J. Vis. Commun. Image R. 31 (2015) 75–85

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Digital watermark extraction using support vector machine with principal component analysis based feature reduction ☆

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:
Received 13 August 2014
Accepted 1 June 2015
Available online 9 June 2015

Keywords:
Lifting wavelet transform
Support vector machine
Coefficient difference
Feature reduction
Watermarking
Attacks
PCA
Digital image watermarking

ABSTRACT

This paper proposes a new approach for watermark extraction using support vector machine (SVM) with principal component analysis (PCA) based feature reduction. In this method, the original cover image is decomposed up to three level using lifting wavelet transform (LWT), and lowpass subband is selected for data hiding purpose. The lowpass subband is divided into small blocks, and a binary watermark is embedded into the original cover image by quantizing the two maximum coefficients of the block. In order to extract watermark bits with maximum correlation, SVM based binary classification approach is incorporated. The training and testing patterns are constructed by employing a reduced set of features along with block coefficients. Firstly, different features are obtained by evaluating the statistical parameters of each block coefficients, and then PCA is utilized to reduce this feature set. As far as security is concerned, randomization of coefficients, blocks, and watermark bits enhances the security of system. Furthermore, energy compaction property of LWT increases the robustness in comparison to conventional wavelet transform. A comparison of the proposed method with some of the recent techniques shows remarkable improvement in terms of robustness and security of the watermark.

1. Introduction

The ease of illegal reproduction of multimedia contents has seriously affected the protection of multimedia intellectual property rights. Currently, digital watermarking has enlisted considerable prominence within the research community due to its remarkable benefits over the traditional data hiding techniques. Watermarking technique should at least satisfy the following requirements: (1) Imperceptible. (2) Without seriously affecting the image quality it is difficult to remove/alter the watermark. (3) Robust against various image processing operations, or attacks. Broadly, watermarking techniques are developed either in the spatial domain or in transform domain. A review of literature reveals that transform domain techniques are typically 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 [1–10]. Numerous transform domain based watermarking schemes have also been proposed and the greater part of these methods is to investigate watermark detectable quality against different signal processing attacks (see for example, [11–21]). Recently, Fu [21] proposed a novel discrete cosine transform (DCT) based image watermarking scheme. Using Bose–Chaudhuri–Hocquenghem (BCH) code, the watermark bits are embedded into the host by modulating the relationships between the selected DCT coefficients. Modulation is similar to the JPEG compression and improves the robustness against JPEG compression but not more effectively.

In order to achieve more robustness against geometrical attacks, various content-based synchronization schemes have been proposed. Recently, Deng et al. [22] presented a content-based watermarking scheme that combines the invariant feature extraction with watermark embedding by using Tchebichef moments (TM). In this approach, Harris Laplace detector is utilized to generate feature point based local disk which is invariant to the geometric distortions whereas, TMs are employed to describe the global characteristics of the local invariant region. More recently, Gao et al. [23] have proposed another variant of feature-based image watermarking by incorporating the advantages of affine invariant point detector, the image normalization, and orientation alignment. To improve the robustness, this scheme includes mainly three components: feature selection procedure, geometrically invariant region, and indirect inverse normalization. Although both

☆ This paper has been recommended for acceptance by M.T. Sun.

* 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.jvcir.2015.06.001
1047-3203/

the methods have exhibited robustness against various important attacks, their performance is not so good in case of geometrical distortions and multiple attacks.

In recent years, there has been a trend of using machine learning and soft computing approaches to design more robust and intelligent watermarking techniques. Yu et al. [24] proposed a digital watermarking method in spatial domain based on artificial neural networks (ANNs), where employing multi-layer perceptrons (MLPs) based neural networks to learn the characteristics of the embedded watermark related to the watermarked image. Shieh et al. [25] presented a genetic algorithm (GA) based optimization scheme in watermarking, where GA was applied to find optimal frequency bands for watermark embedding. Another adaptive scheme based on fuzzy-ART was proposed by Chang et al. in [26] using DCT domain. Adapting discrete wavelet transform (DWT) and GA, Ramanjaneyulu et al. [27] have recently proposed a copyright protection scheme which outperforms the previous methods. In this approach, the watermark embedding and extraction processes are characterized with parameters and GA is utilized for parameter optimization. Though, this method provides more robustness against various types of image processing operations, but, fails to achieve efficient robustness against JPEG compression and sharpening operation.

A systematic review of literature indicates that the performance of SVM based schemes are superior compared to that of traditional learning methods. Particularly, the SVM based solution for the classification problem outperforms the solutions of traditional neural networks, such as MLPs and radial basis functions [28]. Taking the advantages of SVM, significant work has been done on watermark insertion and extraction. Tsai and Sun [28] proposed a color image watermarking approach in spatial domain based on SVM, where watermark extraction was considered as a binary classification problem. Wang et al. [29] presented an image watermarking approach using SVM to resist desynchronization attacks. In another SVM based scheme proposed by Peng et al. [30], the special frequency band and the property of image in multiwavelet domain are utilized for watermarking. Though, the technique is quite robust against several attacks, but, fails to resist JPEG compression, median filtering, average filtering, and scaling attacks effectively. Using regression of SVM, Wang et al. [31] and Shen et al. [32] presented robust watermarking schemes. Recently, Wang et al. [33] proposed a robust image watermarking scheme based on the SVM and Gaussian Hermite moments (GHMs). The original image is transformed using non-subsampled contourlet transform (NSCT) and corresponding lowpass subband is selected to embed a binary watermark. During the watermark extraction, low-order GHMs of training image are computed and watermark bits are extracted from the watermarked image which is corrected by well trained SVM model. The scheme is shown to be robust against different geometric attacks, but, fails to resist JPEG compression attacks effectively. More recently, Yang et al. [34] have also proposed a robust image watermarking technique in undecimated discrete wavelet transform (UDWT) domain. The scheme uses a fuzzy support vector machine (FSVM) to learn geometric distortion parameters by using low order Zernike moments. Watermark extraction is carried out after watermarked image has been synchronized without the original cover. One of the main drawback of this scheme is excessive computational time in extraction. It is also fragile to local geometrical distortions, such as random bending, and column or line removal, and fails to resist JPEG compression attacks more effectively.

Researchers have already done lots of noteworthy work in the field of digital image watermarking. Even though, it is interesting to point out that current methods designed for image integrity may not be perfect. The proposed method provides more robustness in all aspects of image integrity and outperforms especially in case of JPEG compression with high compression ratio.

1.1. Key contribution

Main aim of this paper is to design a system with enhanced features of robustness and extraction of the watermark with maximum possible correlation. With this concern, the watermark embedding and extraction procedures are designed in such a way that maximum performance balance between capacity and robustness could be achieved. In this scheme, the watermark embedding is based on quantization of maximum coefficients of the block; and, the watermark extraction is treated as binary classification based. The novelty of the proposed work is that it uses computationally simple features set for training and testing the SVM, and PCA is utilized to generate an optimally reduced set, which is not experienced in existing schemes. In place of conventional wavelet transform, lifting wavelet transforms have been used in the proposed approach, as it is fast and requires less memory, and the transform can be modified locally while preserving invertibility. The motivation of using SVM is owing to the good learning capability and generalization performance even when the watermarked image is vigorously distorted [28,30]. Well established statistical parameters such as Kurtosis, Skewness, and Entropy are used to generate features set. Key features of the proposed scheme include

1. Using standard statistical parameters and PCA based feature reduction makes the technique computationally more efficient.
2. Energy compaction property of LWT and good learning ability of SVM can tolerate more image distortions.
3. Key based randomization of coefficients, blocks and watermark bits enhances the security of the system.
4. In case of watermark extraction, neither original image nor original watermark image is required.

Rest of the paper is organized as follows: In Section 2, we have briefly sketched the concept of LWT and PCA based feature reduction. Section 3 is devoted to the proposed watermarking technique detailing embedding and extraction of watermark. While in Section 4, experimental results and comparisons with different existing techniques are shown, conclusion and future scope are discussed in Section 5.

2. Preliminaries

This section presents the background material for subsequent sections. We begin with a brief introduction to LWT then illustrate the general concept of PCA based dimensionality reduction (or feature reduction).

2.1. Lifting wavelet transform

Lifting wavelet transform was introduced by Sweldens [35]. The lifting scheme conquers the limitations of the traditional wavelet transform by reducing the computation time and memory requirements. By directly analyzing the problem in integer domain the lifting wavelet simplifies the problem of reversibility which is not experienced in conventional wavelet transform due to the floating point coefficients, we get after transformation. Various advantages of LWT over traditional wavelet transform helps on developing watermarking schemes with increase of computational efficiency.

In general, the lifting scheme includes three basic steps that are splitting, prediction, and update [36,37].