ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

A new robust color image watermarking using local quaternion exponent moments

Wang Xiang-yang [a,b,*], Niu Pan-pan [a], Yang Hong-ying [a,*], Wang Chun-peng [a], Wang Ai-long [a]

[a] School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, PR China
[b] Jiangsu Key Laboratory of Image and Video Understanding for Social Safety, Nanjing University of Science and Technology, Nanjing 210094, PR China

ARTICLE INFO

Article history:
Received 3 March 2013
Received in revised form 24 February 2014
Accepted 28 February 2014
Available online xxxx

Keywords:
Color image watermarking
Desynchronization attacks
Color invariance model
Probability density
Algebra of quaternions
Exponent moments

ABSTRACT

Desynchronization attacks that cause displacement between embedding and detection are usually difficult for watermark to survive. It is a challenging work to design a robust image watermarking scheme against desynchronization attacks, especially for color host images. In this paper, we propose a robust color image watermarking scheme based on local quaternion exponent moments. The proposed scheme has the following advantages: (1) the stable and uniform color image feature points are extracted by the new color image detector, in which the probability density gradient and color invariance model are used, (2) the affine invariant local feature regions are constructed adaptively according to the variation of local probability density and (3) the effective quaternion exponent moments are derived and introduced to embed watermark in the color image, which consider the correlation between different color channels. Experiments are carried out on a color image set of 100 images collected from Internet, and the preliminary results show that the proposed color image watermarking is not only invisible and robust against common image processing operations such as sharpening, noise adding, and JPEG compression, but also robust against the desynchronization attacks.

1. Introduction

WITH the advances of multimedia and Internet technologies, digital data can be easily reproduced, manipulated and distributed without any quality degradation. This has resulted in strong demand for preventing illegal use of copyrighted data. Digital watermarking is an important technique for copyright protection and integrity authentication in an open network environment [28,17]. Technically speaking, digital watermarking aims to hide watermark data into the actual media object without affecting its normal usage. When necessary, the owners can extract the watermark data to declare their copyright. In general, the watermarking schemes can be classified into three categories: robust, semi fragile, and fragile methods according to their specific applications [14]. Robust watermarking mainly serves for identification purposes, while the fragile and semi fragile watermarking are usually employed in authentication applications. Since a good watermarking scheme should always be able to deal with some kinds of attacks, studies in the watermarking research area mostly target robust watermarking problems.

* Corresponding authors. Address: School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, PR China. Tel./fax: +86 0411 85992415 (X.-y. Wang).
E-mail addresses: wxy37@126.com (X.-y. Wang), yhy_65@126.com (H.-y. Yang).

http://dx.doi.org/10.1016/j.ins.2014.02.158
0020-0255/

Please cite this article in press as: X.-y. Wang et al., A new robust color image watermarking using local quaternion exponent moments, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.158

In recent years, there has been increasing research interest in robust image watermarking, and some robust image watermarking algorithms have been developed. On the other hand, attacks against image watermarking systems have become more sophisticated [2]. In particular, it has been observed that simple desynchronization attacks (including ***global desynchronization attacks***, such as rotation, scaling, translation, and aspect ratio changing, and ***local desynchronization attacks***, such as column or line removal, random cropping, and local random bending) can have a catastrophic impact on the performance of the watermark decoder [3]. Broadly, five types of solutions have been proposed in the literature to address the desynchronization problem: Spread spectrum modulation, Invariant transform, Template insertion, Synchronization correction, and Feature-based algorithm [41].

Spread spectrum modulation: Spread spectrum modulation is probably the most popular approach for data hiding, which spreads the digital watermark over the host image. Spread spectrum embedding could be implemented by two main ways, namely additive and multiplicative spread spectrum embedding [26]. The additive spread spectrum scheme uniformly spreads the watermark bit over the host image while the multiplicative spread spectrum spreads the watermark bit according to the host contents. Since the original host image is generally not available at the watermark decoder side, blind decoders are usually employed. Its robustness against common image processing operations and global desynchronization attacks, such as additional noise and lossy compression, and its simple decoder structure make spread spectrum attractive for image watermarking [36,20]. Despite these advantages of spread spectrum modulation, the interference effect of the host image, which causes the watermark decoding performance degradation, is a major concern of the spread spectrum modulation. Besides, spread spectrum modulations are always fragile to local desynchronization attacks such as column removal and local affine transformation [37].

Invariant transform: The obvious way to achieve resilience against global desynchronization attacks is to use an invariant transform. In [34,25,4,27], the watermark is embedded in an affine-invariant domain by using Fourier-Mellin transform, generalized Radon transform, moment invariants, histogram shape, and singular value vector respectively. Mohammad et al. [21] presented a new digital watermarking algorithm for ownership protection, and the algorithm embeds the watermark in the Schur decomposition components of the cover image. Lai et al. [13] presented a hybrid image-watermarking technique based on DWT and SVD, where the watermark is embedded on the singular values of the cover image's DWT subbands. Li et al. [14] proposed an invariant image watermarking scheme by introducing the Polar Harmonic Transform (PHT), which is a recently developed orthogonal moment method. Similar to Zernike moment and pseudo-Zernike moment approaches, PHT is defined on a circular domain. The magnitudes of PHTs are invariant to image rotation and scaling. Furthermore, the PHTs are free of numerical instability, so they are more suitable for watermarking. In [15], a redistributed invariant wavelet domain is proposed and proved, which is resistant to multiples of 90° rotations and image flipping. On this basis, a novel redesigned method for most wavelet-based watermarking algorithms is presented. Despite that they are robust against global desynchronization attacks, those techniques involving invariant domain suffer from implementation issues and are vulnerable to local desynchronization attacks.

Template insertion: Another solution to cope with desynchronization attacks is to identify the transformation by retrieving artificially embedded references. By focusing on a simple example, Barni et al. [1] investigated the effectiveness of exhaustive watermark detection and resynchronization through template matching against desynchronization attacks. Liu et al. [18] presented a practical robust image watermarking algorithm which combines template embedding and patchwork watermarking in Fourier domain. The embedded template enables the necessary robustness against geometric distortions and the patchwork approach provides a reasonable watermark payload which can meet the requirement of most applications. Kaur [12] proposed an image watermarking technique that incorporates two watermarks in a host image for improved robustness. A watermark, in form of a PN sequence (information watermark), is embedded in the DCT domain of the cover image. The second watermark (synchronization template) is then embedded in the already watermarked image. Synchronization template does not contain any information and is used only to detect and correct any geometrical changes came after the attack on the image. However, the template based image watermarking approaches can be tampered by the malicious attacks. In addition, they are similarly vulnerable to local desynchronization attacks.

Synchronization correction: One of the methods for detecting watermarks after desynchronization attacks is correcting distorted watermarked image before detecting. In [23], the weight Hausdorff distance is defined. It is applied to evaluate the similarity between original and geometric distorted watermarking image. A fast divide and conquer strategy in six dimension is used to search the transformation parameters. The geometric distortion is corrected by the parameters. As a result, a distorted watermarking image could be corrected based on image feature. Based on the Support Vector Machine (SVM) and Gaussian-Hermite Moments (GHMs), Wang et al. [38] proposed a robust image watermarking algorithm in Nonsubsampled Contourlet Transform (NSCT) domain with good visual quality and reasonable resistance toward global desynchronization attacks. Jia et al. [9] proposed an anti-geometric attack SVD digital watermark algorithm based on geometric center and image mass centroid. An improved block-based SVD is employed to embed and extract watermark. Based on the invariance of geometric center and image mass centroid, the conducted geometric transform can be detected, and the attacked image is corrected before extraction according to the detected transformation parameters. Zhang et al. [40] derived the affine invariants from Legendre moments, and exploited the affine Legendre moment invariants for estimating the geometric distortion parameters. But, experimental results show that the synchronization correction schemes are also not robust against the local desynchronization attacks.

Feature-based: The last category is feature-based image watermarking techniques. By binding the digital watermark with the geometrically invariant image features, the watermark synchronization error can be avoided. Moreover, since the

Please cite this article in press as: X.-y. Wang et al., A new robust color image watermarking using local quaternion exponent moments, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.158