J. Vis. Commun. Image R. 23 (2012) 507–515

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

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

Image watermarking with feature point based synchronization robust to print–scan attack

A. Keskinarkaus *, A. Pramila [1], T. Seppänen [1]

Department of Computer Science and Engineering, University of Oulu, P.O. Box 4500, FI-90014, Finland

ARTICLE INFO

Article history:
Received 18 March 2011
Accepted 16 January 2012
Available online 24 January 2012

Keywords:
Feature points
Second generation watermarking
Multibit watermarking
Periodic patterns
Geometrical attacks
Print–scan attack
Compound attacks
Synchronization

ABSTRACT

In this paper we propose a content based multibit watermarking method robust to print–scan attack. A method to extract feature points, robust in terms of watermarking, is proposed. The location of the watermark is tied to a coordinate system defined by robust feature points. A message sequence is mapped to a directional angle of periodic patterns, which are scattered and embedded into triangles in permuted locations. In watermark extraction, an interplay between feature extraction and watermarking ensures reliability and a multibit message can be decoded blindly from the locations pointed by the key. By detecting the alignment of the autocorrelations peaks and using a coding table, a multibit message can be extracted. Experiments show that the method provides robust and blind extraction of watermark information after a print–scan attack and a set of compound attacks.

1. Introduction

Digital watermarking is a complementary technique for managing special DRM related problems. The owner of an image can embed an invisible watermark, which can be used for authentication and proving ownership. Adding a customer identification helps in tracing how the media moves in the distribution chain, and who is the leakage point, the producer of illegal copies.

Among the most challenging issues in watermarking are geometrical attacks, in which the attack desynchronizes the detection or extraction of the multibit message causing a total failure or fainting of the information. To resolve the synchronization problem different categories of watermarking methods have been proposed, including RST invariant domain-based, radon transform-based, template-based, salient feature-based, image-decomposition based and stochastic-analysis-based algorithms [1].

Ruanaidh and Pun [2] were the first to introduce the idea of transform-based invariants. Fourier Mellin transform was used to gain robustness to RST attacks. Several proposals have followed, to conquer the implementation difficulties and image quality impairment related to the original idea.

In template based approaches a special template watermark is used to detect transformations undergone by the watermarked image. A separate template is however vulnerable to watermark template attack [3]. In [4] Kutter proposes to use a repetitive watermark both as a calibration signal and as a watermark, which makes the method more robust to template attacks [3]. Stochastic-analysis-based algorithms, generated from the original idea of Alghoniemy and Tewfik [5] are based on watermark embedding and detection on a normalized image.

The introduction of second generation watermarking [6] have generated a bunch of techniques, in which the synchronization relies in detecting salient feature points, which determine the location of the watermark or which determine the origin to apply a transform.

In this paper we propose a feature point based watermarking method robust to print–scan attack. Print–scan is a combinatory attack, in which the pixel value distortion is accompanied with geometric distortions. Pixel distortion is caused by luminance, contrast, gamma correction and chrominance variations and blurring of the adjacent pixels [7]. Also, even with most careful scanning procedure, geometric distortions cannot be avoided [8]. Every time an image is printed and scanned, even with proper placement of the paper into the scanner bed, the result image is different. There is always a slight change in rotation and scale, amount of translation and/or cropping.

Consequently to these distortions, applying feature point based methods to gain robustness to print–scan is not straightforward. As well as the print–scan process causes trouble in reading the

* Corresponding author. Fax: +358 8 5532612.
E-mail addresses: anja.keskinarkaus@ee.oulu.fi (A. Keskinarkaus), anu.pramila@ee.oulu.fi (A. Pramila), tapio.seppanen@ee.oulu.fi (T. Seppänen).
[1] Fax: +358 8 5532612.

1047-3203/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.jvcir.2012.01.010

watermark, it also makes the feature point extraction more difficult, and accordingly only a few feature point based watermarking techniques have been tested against print–scan attack.

We propose a technique in which a message sequence is mapped to a directional angle of periodic patterns, which are then embedded into an image. Message segments are embedded to permuted triangular areas in the image, where the triangles are the result of tiling the image with a polygon and using Delauney triangulation on the polygons. The location of the watermark is represented in a coordinate system defined with salient feature points and stored as a key. In the watermark extraction, with utilizing the feature point detection and the key, the multibit message can be decoded from recomposed triangles by estimating the peak alignment of the autocorrelation function. Additionally we propose a measure describing the robustness of the feature points. The measure is utilized to realize interplay with feature point extraction and watermark extraction to ensure reliability. The problem related to the inaccuracy of the feature point location is resolved with a watermarking method, robust to small changes in feature point location.

In Section 2 previous work is described. In Section 3 an overview of the method is presented. In Section 4 a feature extraction method robust to print–scan is described and a robustness measure for the feature points is explained. In Sections 5 and 6 the details of the watermarking algorithm are given. In Section 7 the validity of the proposed method is proven with experiments.

2. Background of second generation watermarking

Roughly the feature point based watermarking techniques can be classified to tessellation based methods [6,9,10], in which $N > 2$ feature points are used to form local regions to which a watermark is embedded. In the other category regions to be watermarked are centered at the extracted feature points. Commonly non-overlapping regular f. ex circular regions are used. The actual embedding methods vary from spatial to transform domain to stochastic-analysis-based methods.

Kutter et al. [6] were the first to propose employing notion of data features to embed watermark. In their work the feature point detection is based on Mexican–Hat wavelet scale interaction and the location of the feature points is used to perform segmentation with Voronoi diagrams. The resulting segments are watermarked using spread spectrum watermarking. Vulnerability to localization inaccuracy (1–2 pixels under attacks) is discussed and limited search is suggested to compensate the misalignment.

Bas et al. [9] use the Harris detector with pre-filtering blur to detect feature points. Delauney tessellation is performed and a triangular shape watermark is shaped through affine transformations to the resulting tessellation triangles. Watermark detection is based on global decision obtained from the sum of the detection results. Repeatability of the tessellation after attacks is important and consequently experiments show better performance on images where the content is well defined.

Hu [10] proposes another scheme based on content based tessellation. The Harris detector is repeatedly used to find feature points in rotated images and robust intersection points are used as a reference for a key-dependent triangulation. The method is workable as long as triangulation is repeatable, so the method is vulnerable to non-uniform attacks, like aspect ratio changes. Unlike the methods above, the actual watermarking method is not based on spread spectrum, but on NPR (neighborhood pixel ratio).

Since the idea of Alghoniemy and Tewfik [5], to use image normalization to conquer geometric attacks, some proposals using the same underlying idea have been proposed. In [11] a CDMA type watermark is embedded to the mid-frequency DCT coefficients on a normalized image. The performance of the image normalization based watermarking is furthermore improved by Kim et al. [12] using an invariant centroid and central region for resiliency against cropping attacks.

Tang and Hang [13] use Mexican Hat wavelet scale interaction method to detect feature points, which are used as centers of disks which are watermarked. Image normalization technique is used for selecting the locations for watermarks. Same watermark is repeated on non-overlapping disks of fixed size radius.

Lu et al. [14] also use disks of fixed size radius centered at feature points. The watermark is embedded in the transform domain of the normalized disks. Since the area to be watermarked is circular, the authors discuss the effect of padding related to both normalization and DFT transform as well as quantization error when watermarked disks are placed back to the image. Watermark detection is based on a local threshold on normalized correlation to detect if a disk has been watermarked, as well as on global threshold to detect if the image has been watermarked.

A fixed size radius is not effective on scale changes, thus Wang et al. [15] propose an improvement. Instead of a fixed sized radius, the radius is calculated using scale-space theory. Accordingly the radius of the disk is dependent on the scale δ over which the Laplacian-of-Gaussians (LOG) attains maximum. Initial feature points are detected with the Harris–Laplace detector. Next, iteration process evaluates feature point properties in accordance with location and characteristic scales, based on which the final set is a subset of the original points. The process favors feature points on textured regions. As well as in [14] DFT domain watermarking is used. A threshold based decision on each disk is made, and a global decision is claimed "success" when at least two disks are claimed watermarked.

In [16] Wang et al. use the same method for feature point selection and adaptive radius as explained above. The watermark is embedded using wavelet moments. Watermark embedding progresses through several steps, including zero padding normalization of the disk area, important area extraction using invariant centroid, wavelet moment calculation and selection, embedding on the moment vector as well as inverse processes of the preceding steps. Watermark detection uses minimum distance decoder from wavelet moment invariants. The gain from using normalization as well as wavelet moments is better robustness to RST attacks as well as to common signal processing attacks.

Seo and Yoo [17] also propose to utilize disks centered at feature points. Scale invariant feature points are detected based on scale selection, (characteristic scale) at Harris corner points. From N strongest corner points, final points are selected by the location and characteristic scales. This is to remove overlapping of the disk areas. The watermark is circularly symmetric and embedded in spatial domain. In detection the feature points are found similarly and the existence of the watermark decided with correlation enhanced with SPOMF (symmetrical phase only filter). Correlation detector of a pseudorandom watermark is highly vulnerable to synchronization errors, so local search is used in the neighborhood of each watermarked feature point.

A feature point gives only position information, so additional means have to be used to gain information about affine and projective transformations. In [18] Seo and Yoo compare different methods; characteristic scale, shape adaptation of the Gaussian kernel and feature-point sets to cope with affine transformations. Characteristic scale has previously been used by Wang et al. [15,16] to attain scale invariance. Tessellation based watermarking methods all use feature-point sets. Three-point set being the constitution which is most common. This is because, in theory, with three-point basis, invariance to affine transformations can be attained. The problems in these kind of approaches are mainly related to the correlation based watermark detector, which is highly sensitive to inaccuracy of feature point location.