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.

Tessellation based methods require robust extraction of the same feature set that was used during embedding. Condition is hard to accomplish from printed and scanned images. Noise added by print–scan process is larger in the edges [7] and features can be lost, especially in textured areas [9].

A pseudorandom watermark is highly sensitive to the synchronization errors [18]. All of the correlation based methods require very high accuracy of the feature point detection method. An accuracy that is impossible to reach from printed and scanned images. To make the issue more complex, the scale-space representation, including automatic scale selection is not repeatable from printed and scanned images. Additionally defining the same set of N most stabile feature points is difficult. Noise added by print–scan process is larger in pixels, which are very bright or very dark [7]. Consequently the response of the features, giving the strongest response is in fact most affected by the print–scan process.

3. Overview of the method

By using a feature-point set, with a two-point basis, invariance to similarity transformation (translation, rotation, and aspect-ratio preserving scaling) can be attained [18]. Accordingly we use a two-point basis to build up a coordinate system. To gain robustness to pixel value distortion during print–scan as well as to the inaccuracy of the feature point detection, a multibit watermarking method resilient to these attacks is used. Reliability of the feature point extraction is ensured with interplay between the watermarking method and the feature point detection.

Embedding steps are iterative as defined below. In the first iteration, the information about the orientation of the feature points is embedded. Then, a multibit message which has been broken to fixed length segments is embedded iteratively one segment at a time. Location of the watermark segments is stored in a secret key.

The steps to embed information are:

1. Use a convex polygon to tile the image to k non-overlapping areas. Offset from the sides is randomized to remove dependence of watermark location from image sides. In Fig. 1(a) the tiling is illustrated with an example.
2. Use Delauney tessellation to divide polygonal areas into triangles as illustrated in Fig. 1(a) with dashed line.
3. Use random permutation to select set of triangles to be watermarked (Fig. 1(b)).
4. Detect feature points as explained in Section 4. For illustration in Fig. 1(c) is shown 35 best results, where ordering is based on the proposed robustness measure.
5. Represent the watermark location in the coordinate system defined by two best feature points (Fig. 1(d)). Selection criteria are based both on robustness and on distance between feature points.
6. Embed one segment of the watermark. Details of the embedding method are explained in Section 5.
7. Repeat Steps 3, 5, 6 while the whole watermark is embedded.

The steps to extract information:

1. Detect feature points using the same method as during embedding (Fig. 2(a)).
2. Use similar criteria as during embedding to select two feature points and built up a coordinate system. (Fig. 2(b))
3. Utilize the secret key, to identify the location of the watermarked triangle areas constituting a piece of information. (Fig. 2(c))
4. Assemble the polygon from triangles (Fig. 2(c)) as shown in Fig. 2(d) so that information can be extracted. Details of the extraction method are explained in Section 6.
5. In the first iteration check that the feature point pair is the correct one: orientation of the feature points should be the same as the embedded information indicates. If the feature point pair is not the correct one, the next feature point pair is checked.
6. Repeat Steps 3 and 4 while the whole message is extracted.

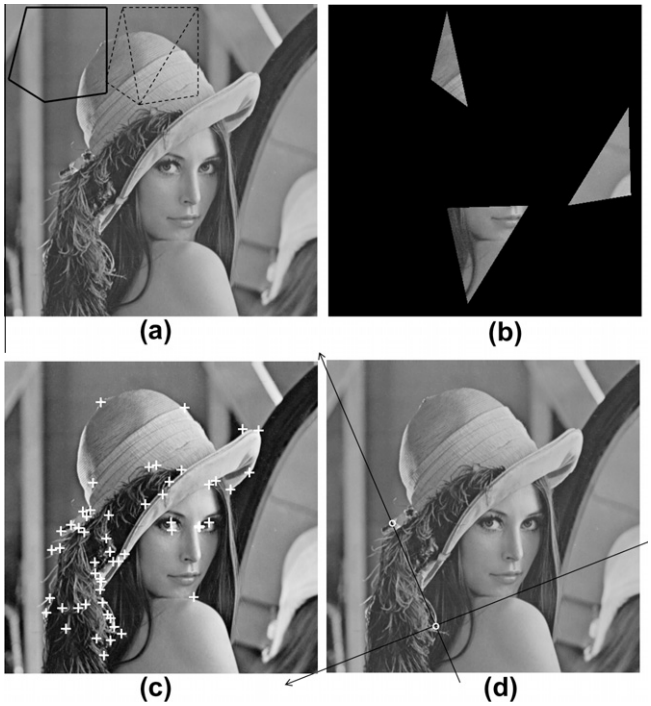

Fig. 1. Embedding overview (a) Step1 and Step2 (b) Step3 (c) Step4 (d) Step5.

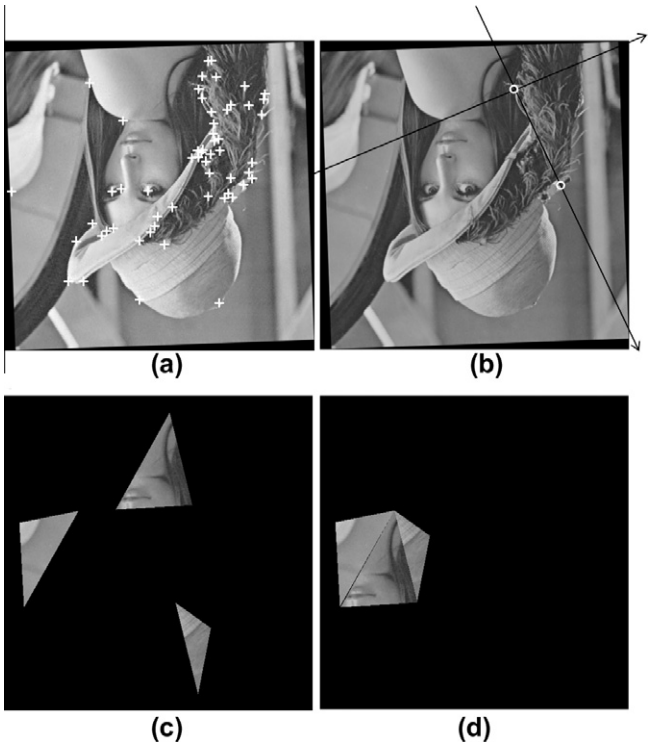

Fig. 2. Extraction overview (a) Step1 (b) Step2 (c) Step3 (d) Step4.

4. Feature extraction

Harris presents in [19] the classical combined corner and edge detector, which has also been used in many of the content based watermarking methods. However the Harris detector is not scale invariant, so scale-space representation and automatic scale selection [20] can be taken advantage of to gain invariance to uniform scaling. More advanced feature point detectors also provide invariance to non-isotropic scaling through shape adaptation, as proposed by Lindeberg and Garding in [22]. Some variants are presented and evaluated in [21]. In [23] Gevrekci and Gunturk present an illumination robust interest point detector.

In the context of the proposed watermarking method, the objectives for the feature point extraction are that, firstly the N points used for building up a coordinate system should belong to the set of extracted feature points, also after attacks. Secondly a descriptor, to describe the robustness of the feature points should be constructed, based on which a sensible ordering of the feature points can be constructed.

In the proposed method we take into account well-known properties. Firstly when no a priori information is available, the only reasonable approach is to treat image structures at all scales simultaneously and as uniformly as possible [22]. Secondly image structures have a varying lifetime in scale-space [20]. Additionally smoothing can affect both shape and the localization of structures [22]. Also, the space of possible photometric transformation can be spanned iteratively, using contrast-stretched images [23], as a result an illumination robust interest point detector.

In [9] and [24] different feature extraction techniques for watermarking has been evaluated. Bas et al. [9] compared the performance of three feature extraction methods, the Harris corner detector, the Susan detector and Achard–Rouquet detector. They found out that from the three tested detectors, the Harris detector preserves points most robustly when the image undergoes a geometrical transformation. Lee et al. [24] compared performance of the Harris corner detector and Mexican Hat wavelet scale interaction method. In their tests Mexican Hat wavelet scale interaction showed severe weakness against scaling attacks. Accordingly in here the Harris detector has been chosen as a basis. The Harris detector is based on the autocorrelation matrix of the image gradients [23]. In the proposed method the autocorrelation matrix is calculated with

$$A(x,y;I_D)=\begin{pmatrix} \sum_{(m,n)\in N}\left(\frac{\partial}{\partial x}I_D(m,n)\right)^2 & \sum_{(m,n)\in N}\frac{\partial}{\partial x}I_D(m,n)\frac{\partial}{\partial y}I_D(m,n) \\ \sum_{(m,n)\in N}\frac{\partial}{\partial x}I_D(m,n)\frac{\partial}{\partial y}I_D(m,n) & \sum_{(m,n)\in N}\left(\frac{\partial}{\partial y}I_D(m,n)\right)^2 \end{pmatrix} \tag{1}$$

In Eq. (1) the transformed coordinates (m,n) are determined by

$$\begin{bmatrix} m \\ n \end{bmatrix}=\begin{bmatrix} t & 0 \\ 0 & t \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}, \tag{2}$$

where t is the detection scale, (x,y) are the original coordinates and I_D, where D stands for detection level, is the function of the transformed coordinates described with

$$f_D(I(m,n))=\left(\frac{I(m,n)-\alpha}{\beta-\alpha}\right)^{\gamma}, \tag{3}$$

γ is the gamma correction factor and α and β define the limits for the contrast stretch. Robustness descriptor for the points is calculated with

$$Rob=\frac{\sum_{i=1}^{n}R_i}{\max(R_i)}, \tag{4}$$

where the Harris response R_i function is calculated with

Fig. 3. Levels for feature point extraction.

$$R_i(m,n,D)=\det A(m,n;I_D)-k(traceA(m,n;I_D))^2 \tag{5}$$

We use $k=0.004$, standard deviation of smoothing Gaussian $\delta_{harris}=2.8$, radius for non-maximum suppression = 8. The normalized cumulative sum (*Rob*) is high when the feature gives high response in each level, where level simulates different scale and contrast conditions. Thus, the calculated robustness descriptor *Rob* gives a measure of the robustness: features which converge and have a long lifetime in scale-contrast-space have a strong value of *Rob*.

In Eq. (4) i describes the Level, where t is defined so that image size changes with a fixed step size between levels. We use 0.02 step size and range from 0.9 to 1.1. Resampling is realized in frequency domain. Simultaneously with geometry transformation, in each Level, α is stepwise (0.035) increased, β stepwise decreased (0.035) and value of gamma correction γ changed in the range of 0.7 to 1.4. This is to conquer nonlinear distortion of pixel values caused by print–scan process. The levelled approach with simultaneous operations is illustrated in Fig. 3. For clarity of illustration in the figure are shown 35 features in each level. *Rob* is calculated over a 4×4 neighborhood, where location of the point is determined by mapping the points to the normalized image scale. During embedding, the normalized scale is the original image scale and during extraction from printed and scanned image approximate given by downsampling with scanning resolution/display resolution.

Consequently to simultaneous operations through the range, we can avoid a number of iterations. Experiments showed that 11 iterations of basic Harris is enough for our purposes. Levelled approach ensures that the N points used for building up a coordinate system belong to the union of extracted feature points also in distorted image. Shape distortion, (wandering of the location of the feature point), is handled through allowing small shift in location.

5. Watermark embedding

Referring to the overview of the method in Section 3, the embedding steps are iterative and during each iteration a piece

of information is embedded. To improve security, the message segments are embedded in permuted triangle areas in the image. A secret key stores the location of the watermark in a coordinate system defined by salient feature points. For message encoding in Step 6, directed periodic pattern method, which is robust to print–scan attack, and additionally to compound attacks is used [25]. In here the patterns carrying the message in the directional angle are shaped to fit to the polygonal shape and furthermore scattered into the triangular Wiener filtered image areas. The dimensions of the triangles are used to adapt the periodicity of the directed periodic patterns, so optimizing security.

A message is encoded by modulating angle θ of the periodic pattern. The original watermark message is divided into shorter message segments m_i, where the message length $|m_i|$ expresses the amount of data bits that are to be embedded in the kth polygon of the image. The quantization step size is calculated with

$$\Delta = 180/2^{|m_i|}, \tag{6}$$

where the constant 180 is defined by the range of θ. A codebook is derived accordingly. The message is expressed by mapping to the codebook values. Consequently, the original message is divided to be spread to image and represented by quantized orientation $Q(\theta)$.

Prior to watermarking Wiener filtering is applied.

$$I_{pre}(u,v) = \begin{cases} I_{wiener}(x,y), & \text{when } r(x,y) = 1 \text{ and} \\ (I(x,y) - I_{wiener}(x,y)) > 0 \\ I(x,y), & \text{otherwise} \end{cases}, \tag{7}$$

where r is a matrix with uniformly distributed values of 0, 1 with a probability(1) + probability(0) = 1. The motivation to Wiener filtering based preprocessing references to the watermark extraction, where the periodicity in the Wiener estimate is calculated as a part of the message extraction process. The calculated $I_{wiener}(x,y)$ for images tend to be substantial in very textured image areas, which with purely addition based watermark embedding approach will cause disturbance in watermark extraction. When with chosen probability a portion of the noise in the image is instead replaced with the watermark, the robustness is increased. By controlling the spatial probability of subtraction, enough image details are left to maintain visual quality.

The embedding proceeds as shown in Fig. 4. The feature points are extracted as explained in Section 4. The feature points are organized according to their *Rob* value, and a feature point pair is selected, to be used to build a coordinate system. An additional conditioning is used according to the distance between the feature points. This is to avoid a situation, where the feature point pair is too close to each other. The coordinates of the permuted triangles, pointing to watermarked location are represented in a new coordinate system using Helmert transformation

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \mu \begin{bmatrix} \cos\theta_f & -\sin\theta_f \\ \sin\theta_f & \cos\theta_f \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} + C, \tag{8}$$

where μ is the scale factor, calculated using image pixel distance, between the feature point pair $\mu = 1/K \cdot (\text{dist}(f1, f2))$. Information about K is shared with the embedding and extraction algorithm. θ_f in the rotation matrix is the angle that a line drawn through feature points makes with x-axis. C is the translation vector to shift the origin to the point $f1$. The result is stored as a key.

When we embed a watermark shaped through the properties of the Human Visual System, the watermark will be enhanced in the edge areas of the image, consequently affecting also the response of feature point detectors. Therefore in here we leave the 8×8 areas, which is also the size for the Harris windowing, around the feature point pair intact.

The embedding of the message in the host image is realized in spatial domain utilizing the equation

$$Y_i^*(x,y) = X_i(x,y) + \lambda_1 \cdot JND_{fb} \cdot W_i^{Q(\theta_k)}(x,y), \tag{9}$$

where Y_i^* is ith watermarked triangle of the image, X_i is corresponding luminance component of the original image. $W_i^{Q(\theta_k)}$ is the corresponding portion of the directed periodic pattern, x and y describe the pixel position, JND_{fb} is the scaling factor attained from a JND profile, and λ_1 is an additional scaling factor calculated by

$$\lambda_1 = \frac{\lambda_t - \lambda_s}{M_t - M_s} \cdot M_b + \lambda_s, \tag{10}$$

where λ_s is the scaling factor for smooth block and λ_t the scaling factor for textured block. M_s and M_t respectively stand for average

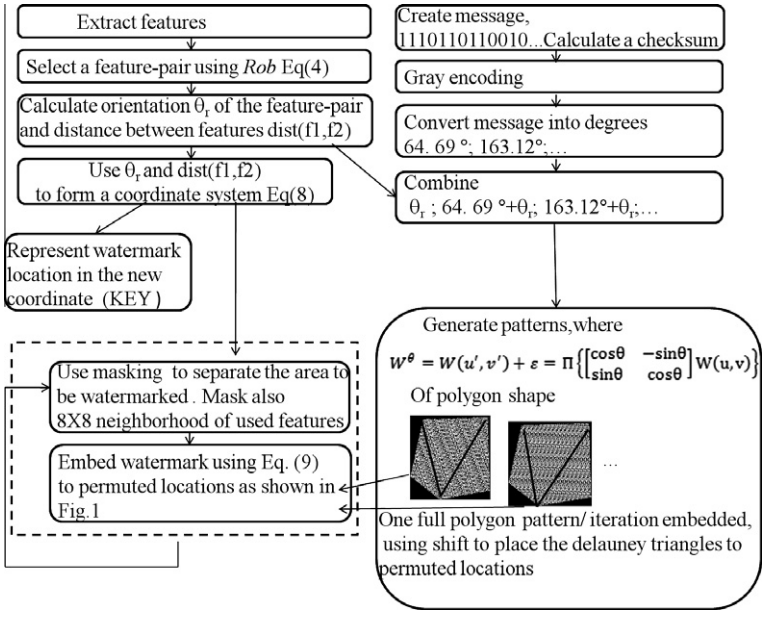

Fig. 4. Embedding block diagram.

gradient magnitude on smooth and textured blocks and have been determined experimentally. Periodicity in $W(u,v)$, where

$$W(x+q_0N_0,y)=W(x,y);\ \ q_0,N_0>1 \tag{11}$$

$$W(x,y+q_1N_1)=W(x,y);\ \ q_1,N_1>1 \tag{12}$$

is defined with the maximum radius of the incircle of Delauney tessellation triangles.

$$N_1>\frac{2A}{a+b+c}, \tag{13}$$

where A is the area of triangle, and a, b and c are the lengths of the sides. N_0 and N_1 determine the periodicity of repetitions, and q_0 and q_1 a repetition number on the horizontal and vertical directions in $W(u,v)$. As a result, single triangle will not carry enough information to detect peak orientation.

6. Watermark extraction

Prior to the watermark extraction process, the watermarked areas have to be located from the distorted image (Fig. 2). The feature pair and the key are used to locate the triangular areas. In each iteration a polygonal area is recomposed from the triangles from which autocorrelation function, filtering, masking, and adaptive line search with Hough transform reveals the alignment of the autocorrelations peaks. The correctness of the feature point pair is first confirmed and the message extraction principle with message interpretation in Step 4 follows the idea presented in [25]. In here however with modifications required by the overall method and to improve robustness. The overall extraction process is shown in Fig. 5.

The same algorithm as during embedding is used to extract feature points and to select a feature point pair. A coordinate system is build similarly using the feature point pair with Helmert transform. The interplay with watermarking ensures that the feature point pair is the correct one.

A Wiener estimate is calculated for the luminance component of the image

$$\tilde{W}(x,y)=Y^*(x,y)-h(k)^*Y^*(x,y), \tag{14}$$

where $Y^*(x,y)$ is the attacked image and $h(k)$ represents the adaptive Wiener filtering. For the polygonal area $\tilde{W}_k(x,y)$, recomposed using a key from permuted triangles $\tilde{W}_i(x,y)$, autocorrelation function is calculated in order to reveal the periodicity in the extracted watermark estimate

$$R_{\tilde{W}_k\tilde{W}_k}(u,v)=\sum_x\sum_y\tilde{W}_k(x,y)\tilde{W}_k(x+u,y+v) \tag{15}$$

The autocorrelation is scaled to the range of [0,1],

$$R^*_{\tilde{W}_k\tilde{W}_k}(u,v)=|R_{\tilde{W}_k\tilde{W}_k}(u,v)|/\max(R_{\tilde{W}_k\tilde{W}_k}(u,v)) \tag{16}$$

In order to enhance peak detection, rotationally symmetric Laplacian of Gaussian filtering operation is performed

$$R^{**}_{\tilde{W}_k,\tilde{W}_k}(u,v)=\frac{\partial^2}{\partial(u,v)^2}h^{T^*}(\frac{\partial^2}{\partial(u,v)^2}h\times R^*_{\tilde{W}_k,\tilde{W}_k}(u,v)) \tag{17}$$

A binary grid image $G^*(u,v)$ is generated

$$G^*(u,v)=\begin{cases}1, & \text{if}\quad M(u,v)\times R^{**}_{\tilde{W}_k,\tilde{W}_k}(u,v)\geqslant\gamma\\ 0, & \text{if}\quad M(u,v)\times R^{**}_{\tilde{W}_k,\tilde{W}_k}(u,v)\geqslant\gamma\end{cases} \tag{18}$$

where $M(u,v)$ denotes masking operation and γ is a threshold. The threshold operation is used to find locations of the maximums of the scaled and filtered autocorrelation function. These peak locations are equidistantly placed with respect to the fundamental periods (N_0,N_1) of the periodic directed watermark pattern. Accordingly information of the direction of the periodicity can be revealed from the peak alignment. The noise reducing mask is a circular mask, where the radius of the mask is maximum of

$$N_1<\frac{2A}{a+b+c}, \tag{19}$$

where A is the area of Delauney triangles, and a, b and c are the lengths of the sides. Attacks may stretch the structure of the peaks, so furthermore we shape grid structures with morphology to radius one disks. We use adaptive line search algorithm [25]. γ value changes stepwise from an initial estimate, until there are enough peaks for detecting lines exceeding a predetermined length.

Finally, the message can be decoded from $\tilde{\theta}_m$ which is calculated utilizing $\tilde{\theta}_m=\tilde{\theta}_k-\tilde{\theta}^*_r$ where $\tilde{\theta}^*_r$ is the orientation of the feature point pair. The message is decoded using the same quantization codebook as during embedding phase.

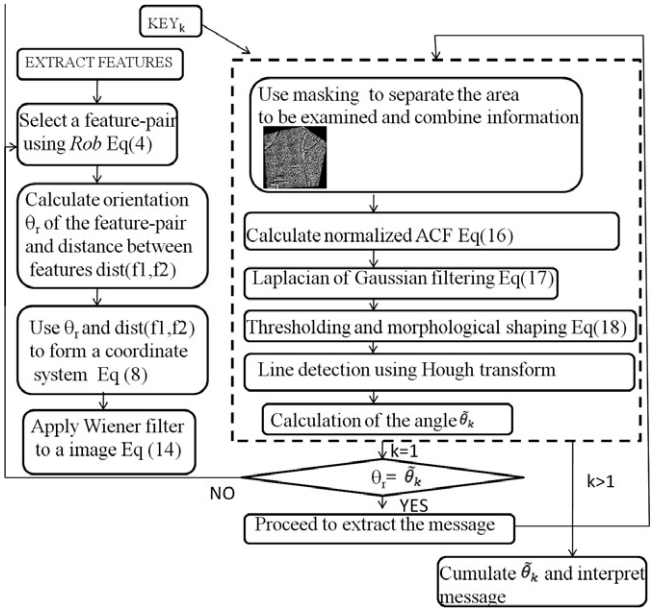

Fig. 5. Extraction block diagram.

7. Experiments

The embedding and extraction algorithms were written in Matlab (registered trademark, The MathWorks, Inc.). In the experiments, we utilized HP Color LaserJet 4650 PCL 6 printer and EPSON perfection, 4180 photo scanner, with scanning resolution of 150 dpi. The experiments were conducted with 16 different images, shown in Fig. 6. For preprocessing with Wiener filtering (Eq. (7)) we use 50% probability of 1 and 0. During embedding, we use $\lambda_s=0.85$ for smooth blocks and $\lambda_t=2.0$ for textured blocks (Eq. (10)). The corresponding values of M_s and M_t are 18 and 180. For searched line length we use fixed value, 45.

First the effect of the distance between the feature-pair was measured. Experiments showed that a reliable coordinate to embed 32 bits robust to print–scan attack can be built when dist($f1$,$f2$) is over 30. In image 2, the dist($f1$,$f2$) if only *Rob* value is used as a selection criteria is just about in the boundary of carrying a coordinate frame. Tests showed that for robustness against compound attacks, it is preferable to choose feature point pair $f1$, $f2$ ordered with *Rob* value and with an additional conditioning on dist($f1$,$f2$). Consequently, we use dist($f1$,$f2$) > 100 in embedding and dist($f1$,$f2$) > 0.8×100 in extraction to ensure extraction reliability also when image is downscaled and distances between feature points change.

Fig. 6. Test images.

Tests in Table 1 show that a 32 bit message can be extracted reliably under a variety of compound attacks. Crop I means that the image has been cropped from the sides and crop II that the portions of the image has been locally cropped. PS indicates printing scanning process. The results are expressed as number of correctly retrieved bits/total amount of embedded bits.

In Table 2 and 3 are depicted the detailed detection results when a message of total length 40 bits, was embedded into images. This is to give more information of how different attack combinations and distance between feature points affect the capacity. In Table 2 column (PS) are depicted the number of correctly retrieved bits, under general print–scan attack. The quality of the watermarked images was measured with PSNR (Table 2).

Feature points and their ordering is computed in ~15 s with unoptimized Matlab code and total execution time of the search succeeded by watermark extraction is depicted in Table 2 column 6 for the general PS process. The results indicate that the *Rob* measure for ordering of feature points is successful. Longer execution time is needed, when the image contains a large number of feature points with a response in a close range to each other.

The results reflect the reduction of the dynamic range of intensity values due to print–scan process. Specially, images containing larger areas of very bright or dark areas are generally more vulnerable to combined attacks. As a confirm in Table 4, are shown the extraction results, where intensity value of im12 has been adjusted to range of 40–200 prior to watermarking (im12_C). The experiment also demonstrates that with contrast adjustment, robustness to combined attacks can be improved significantly for such an image.

The performance of im14, the Baboon image was worse than for other images. Baboon image is highly textured, and so vulnerable to print–scan process and to any interpolation involving attacks, like rotation. In Table 4 are shown how with increasing the preprocessing ratio (im14_Pre80%), the robustness can be improved notably. When ratio of Wiener filtering based noise removal from the cover image (Eq. (7)) is increased, the message extraction reliability increases.

8. Discussion and conclusion

In this paper we proposed a watermarking method robust to compound attacks: print–scan attack combined with an attack on geometry. The Achilles' heel of previously proposed content based watermarking methods is that they are vulnerable to even small changes in aspect ratio. In here we demonstrated that the proposed method is robust when the image has undergone aspect ratio change combined with print scan attack.

In print–scan process geometric distortions cannot be avoided. In tessellation based method, the repeatability of the tessellation is a problem. It is hard to catch all the original feature points, and distortions change the distances between feature points, causing trouble in methods basing ordering on absolute lengths between feature points. In other methods, where a watermark is repeated to non-overlapping regular f. ex circular regions, the problem is defining the same area of correct shape from the distorted image. Also the location of the feature points where the areas are tied to is inaccurate.

We presented a method to order the feature points based on a robustness measure, where the measure was calculated with simultaneous operations for computational efficiency. A feature point pair was selected to be used to form a coordinate system,

Table 1
Robustness to attacks with 32 bit message. (Eight 4 bit message segments embedded.)

	PS	PS & rot 10°	PS & rot 80°	PS & rot 190°	PS & rot 260°	PS & trans	PS & crop I 5%	PS & crop II 7%	PS & scale $x = 0.9$ $y = 0.9$	PS & scale $x = 1.1$ $y = 1.1$	PS & AR $x = 0.98$ $y = 1$	PS & x and y shear 1%
im1	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im2	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im3	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im4	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im5	32/32	32/32	32/32	32/32	No/rec*	32/32	32/32	32/32	32/32	32/32	32/32	32/32
m6	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im7	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im8	32/32	32/32	32/32	32/32	32/32	32/32	32/32	28/32	No	32/32	32/32	32/32
im9	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im10	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	28/32	No	32/32	32/32
im11	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im12	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im13	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im14	32/32	32/32	32/32	24/32	24/32	28/32	32/32	28/32	No	28/32	24/32	24/32
im15	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32
im16	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32	32/32

* Message fully recovered after inverting approximately (accuracy of $-3°\ldots-3°$) the rotation manually.

Table 2
Robustness to attacks with 40 bit message. (Eight 5 bit message segments embedded).

im	Message (CS = checksum)	PSNR	dist_ *f*1_*f*2	PS	Execution time (s)	PS & rot 10°	PS & rot 80°	PS & rot 190°	PS & rot 260°
im1	585339236 + CS	30.8	103.3	40/40	77.3	39/40	40/40	39/40	40/40
im2	998211566 + CS	32.7	230.7	40/40	30.6	40/40	39/40	40/40	40/40
im3	249131326 + CS	32.0	305.2	40/40	20.3	40/40	40/40	39/40	40/40
im4	322636179 + CS	34.6	130.0	40/40	20.5	40/40	40/40	40/40	40/40
im5	947629773 + CS	34.3	173.5	40/40	18.5	40/40	40/40	40/40	No/rec
im6	781792351 + CS	35.5	220.7	40/40	19.4	40/40	40/40	40/40	40/40
im7	321794741 + CS	29.9	101.2	40/40	19.5	40/40	39/40	40/40	40/40
im8	348162886 + CS	34.6	292.7	40/40	17.5	40/40	40/40	40/40	40/40
im9	169785351 + CS	30.0	119.5	40/40	18.1	39/40	40/40	40/40	40/40
im10	621163187 + CS	29.5	105.3	40/40	91.2	40/40	38/40	40/40	40/40
im11	122779134 + CS	34.6	145.7	40/40	18.9	40/40	40/40	40/40	40/40
im12	641272427 + CS	34.6	258.6	40/40	28.2	40/40	No/rec	40/40	40/40
im13	123523415 + CS	35.1	165.0	40/40	22.8	40/40	40/40	38/40	40/40
im14	684635727 + CS	29.0	121.3	40/40	18.9	40/40	39/40	37/40	30/40
im15	728719262 + CS	34.3	180.2	40/40	19.2	40/40	40/40	40/40	40/40
im16	279534762 + CS	33.6	170.4	40/40	18.7	40/40	40/40	40/40	40/40

Table 3
Robustness to attacks with 40 bit message. (Eight 5 bit message segments embedded).

im	PS & trans	PS & crop I 5%	PS & crop I 10%	PS & crop II 7%	PS & scale $x = 0.9$ $y = 0.9$	PS & scale $x = 0.92$ $y = 0.92$	PS & scale $x = 1.1$ $y = 1.1$	PS & AR $x = 0.98$ $y = 1$	PS & AR $x = 0.95$ $y = 1$	PS & x and y shear 1%
im1	40/40	40/40	40/40	40/40	39/40	39/40	40/40	40/40	38/40	40/40
im2	40/40	40/40	40/40	40/40	40/40	39/40	40/40	39/40	38/40	40/40
im3	40/40	40/40	No	40/40	40/40	40/40	40/40	40/40	37/40	40/40
im4	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40	39/40	38/40
im5	40/40	40/40	37/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40
im6	40/40	40/40	39/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40
im7	40/40	40/40	40/40	40/40	38/40	39/40	40/40	40/40	Not	40/40
im8	40/40	39/40	No	37/40	34/40	39/40	40/40	39/40	38/40	39/40
im9	40/40	40/40	38/40	40/40	39/40	40/40	40/40	40/40	39/40	40/40
im10	40/40	40/40	39/40	40/40	36/40	40/40	No	40/40	38/40	40/40
im11	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40	37/40	38/40
im12	39/40	40/40	40/40	40/40	40/40	38/40	40/40	40/40	38/40	40/40
im13	40/40	40/40	40/40	40/40	40/40	39/40	40/40	40/40	39/40	40/40
im14	36/40	39/40	39/40	38/40	No	36/40	38/40	36/40	No	30/40
im15	40/40	39/40	36/40	40/40	40/40	40/40	40/40	40/40	36/40	40/40
im16	40/40	40/40	No	40/40	39/40	40/40	40/40	40/40	39/40	40/40

Table 4
The effect of dynamic range of intensity values and preprocessing ratio.

im	PS & rot 10°	PS & rot 80°	PS & rot 190°	PS & rot 260°	PS & trans	PS & crop I 10%	PS & crop II 7%	PS & scale $x = 0.9$ $y = 0.9$	PS & scale $x = 1.1$ $y = 1.1$	PS & AR $x = 0.95$ $y = 1$	PS & x and y shear 1%
im12	40/40	No/rec	40/40	40/40	39/40	40/40	40/40	40/40	40/40	38/40	40/40
im_12C	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40	40/40
im14	40/40	39/40	37/40	30/40	36/40	39/40	38/40	No	38/40	No	30/40
im14_Pre 80%	40/40	40/40	36/40	40/40	36/40	40/40	40/40	40/40	40/40	39/40	40/40

the reliability of which is ensured with an interplay with the watermarking method. The accuracy of the coordinate system was evaluated with ratio of correctly decoded bits. Also we proposed to spread a piece of watermark information to separate image areas, and with filling up the tiles to embed a multibit message. A secret key, scattering of information, and parameter choices ensures security, making watermark estimation attack complicated.

In tests we demonstrated the effect of contrast adjustment prior to watermarking to improve significantly the robustness to print–scan attack with an example image. However, in images, where the content is richer, there are challenges concerning finding an optimal balance between advantages of the contrast adjustment versus effects on stability of the features. Further development of it is left for the future.

References

[1] Dong Zheng, Yan Liu, Jiying Zhao, Abdulmotaleb El Saddic, A survey of RST invariant image watermarking algorithms, ACM Comput. Surv. 39 (2) (2007) (Article 5).
[2] J.J.K. O' Ruanaidh, T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal Proces. 66 (3) (1998) 303–317.
[3] A. Herrigel, S. Voloshynovskiy, Y. Rytsar, The watermark template attack, in: Proceedings SPIE Security and Watermarking of Multimedia Contents III, 4314 (2001) 394–400.
[4] M. Kutter. Watermarking resistant to translation, rotation and scaling, in: Proceedings SPIE Multimedia Systems and Applications, 3528 (1998) 423–421.
[5] M. Alghoniemy, A.H. Tewfik, Geometric distortion correction through image normalization, in: Proceeding of IEEE International Conference on Multimedia and Expo (ICME 2000), 3 (2000) 1291–1294.
[6] M. Kutter, S.K. Bhattacharjee, T. Ebrehimi, Towards second generation watermarking schemes, in: Proceeding IEEE International Conference Image Processing ICIP, 1 (1999) 320–323.

[7] C-Y Lin, S-F Chang, Distortion modeling and invariant extraction for digital image print–scan process, in: International Symposium on Multimedia Information Processing (ISMIP 99), 1999.
[8] K. Solanki, U. Madhow, B.S. Manjunath, S. Chandrasekaran, I. El- Khalil, Print and scan' resilient data hiding in images, IEEE Trans. Infor. Forensics Security 1 (4) (2006) 464–478.
[9] P. Bas, J-M. Chassery, B. Marq, Geometrically invariant watermarking using feature points, IEEE Trans. Image Proces. 11 (9) (2002) 1014–1028.
[10] S. Hu, Geometric-invariant image watermarking by key-dependent triangulation, Int. J. Comput. Infor. 32 (2) (2008) 169–181.
[11] P. Dong, N. Galatsanos, Affine transformation resistant watermarking based on image normalizaton, in: Proceedings IEEE International Conference Image Processing (ICIP 2002) (2002) 489–492.
[12] B-S. Kim, J-G. Choi, K-H. Park, Image normalization using invariant centroid for RST invariant digital image watermarking, in: International Conference on Digital Watermarking (IWDW 2002), Lecture Notes in Computer Science (LNCS), 2613 (2003) 202–11.
[13] C.W. Tang, H.M. Hang, A feature-based robust digital image watermarking scheme, IEEE Trans. Signal Process. 51 (4) (2003) 950–958.
[14] W. Lu, H. Lu, F-L. Chung, Feature based robust watermarking using image normalization, Comput. Electr. Eng. 36 (1) (2010) 2–18.
[15] X-Y. Wang, J. Wu, P. P Niu, A new digital image watermarking algorithm resilient to desynchronization attacks, IEEE Trans. Inf. Forensics Secur. 2 (4) (2007) 655–663.
[16] X-Y. Wang, Y-P. Yang, H-Y. Yang, Invariant image watermarking using multi-scale Harris detector and wavelet moments, Comput. Electr. Eng. 36 (1) (2010) 31–44.
[17] J.S. Seo, C.D. Yoo, Localized image watermarking based on feature points of scale-space representation, Pattern Recogn. 37 (7) (2004) 1365–1375.
[18] J.S. Seo, C.D. Yoo, Image watermarking based on invariant regions of scale-space representation, IEEE Trans. Signal Process. 54 (4) (2006) 1537–1549.
[19] C. Harris, M. Stephens, A combined corner and edge detector, in: Proceedings of The Fourth Alvey Vision Conference (1988) 147–151.
[20] T. Lindeberg, Feature detection with automatic scale selection, Int. J. Comput. Vision 30 (2) (1998) 77–116.
[21] K. Mikolajczyk, C. Schmid, Scale & affine invariant interest point detectors, Int. J. Comput. Vision 60 (2) (2004) 63–86.
[22] T. Lindeberg, J. Garding, Shape-adapted smoothing in estimation of3-D shape cues from affine deformations of local 2-D brightness structure, Image Vis. Comput. 15 (6) (1997) 415–434.
[23] M. Gevrekci, B.K. Gunturk, Illumination robust interest point detection, Comput. Vis. Image Underst. 113 (4) (2009) 565–571.
[24] H-Y. Lee, I K Kang , H-K. Lee, Y-H. Suh, Evaluation of feature extraction techniques for robust watermarking, in: 4th International Workshop, International Workshop on Digital Watermarking 2005 (IWDW 2005), Lecture Notes in Computer Science, 3710 (2005) 418–431.
[25] A. Keskinarkaus, A. Pramila, T. Seppänen, Image watermarking with a directed periodic pattern to embed multibit messages resilient to print–scan and compound attacks, J. Syst. Softw. 83 (10) (2010) 1715–1725.