Robust Wavelet-Based Blind Image Watermarking Against Geometrical Attacks

Gui Xie
Graduate School of Information Science
Japan Advanced Institute of Science and Technology
Tatsunokuchi, Ishikawa, 923-1292, Japan
Email: g-xie@jaist.ac.jp

Hong Shen
Graduate School of Information Science
Japan Advanced Institute of Science and Technology
Tatsunokuchi, Ishikawa, 923-1292, Japan
Email: shen@jaist.ac.jp

Abstract—Given its strong similarity to HVS, wavelet transform has been applied in watermarking successfully. However, due to its sensitivity to rotation, scaling and translation, the wavelet-based watermarking algorithms are vulnerable to geometrical attacks. In this paper, we design a novel wavelet-based watermarking scheme resilient to geometrical attacks using a rotation-invariant log-polar mapping to eliminate all the effects of the geometrical operations in the input image before computing its discrete wavelet transform. A pixel-wise masking method used in the wavelet domain to scale the watermark is applied in order to achieve the best compromise between the requirements of robustness and imperceptibility for the embedded watermark. Experimental results demonstrate the advantages of our scheme, particularly its robustness against geometrical attacks.

I. INTRODUCTION

In recent years, watermarking is finding more and more support as a possible solution for the protection and enforcement of the copyright of digital images. Generally, digital image watermarking has two fundamental requirements: imperceptibility and robustness. As the two requirements are conflicting, a tradeoff based on the human visual system (HVS) [1], [2] is necessary. It is today widely accepted that robust image watermarking techniques should make full use of the characteristics of the HVS, for more effectively hiding a watermark.

The past decade has seen numerous digital watermarking algorithms developed for protection of intellectual property rights, which can be divided into two broad categories by watermark embedding domain: spatial domain and transform domain. Due to its suitability to model the HVS behavior, the wavelet-based watermarking algorithms proposed in the last few years have shown robustness against a variety of attacks such as filtering, addition of noise and compression. However, wavelet-based watermarking schemes are vulnerable to the geometrical attacks because the wavelet transform is sensitive to rotation, scale and translation, which means even very small geometrical distortions can cause big changes in the energy distribution of the wavelet coefficients, and prevent the detection of the embedded watermark. This problem is most pronounced for a blind watermark, as without access to the original unwatermarked image at the end of the detector, it’s difficult, if not possible, to revert the geometrical distortion just based on registration of the watermarked and original images.

To our best knowledge, no blind wavelet-based watermarking algorithms that is able to survive geometrical attacks exist so far.

This paper for the first time proposes a novel wavelet-based blind watermarking scheme resilient to geometrical attacks by integrating a rotation-invariant log-polar mapping (LPM) with the wavelet transform. Traditional LPM eliminates the translation and scale effects, but at the same time produces a row cyclic shifted log-polar image. Because wavelet transform is sensitive to shifts, simply combining LPM and wavelet transform as the Fourier-Mellin transform based watermarking algorithms [3], [4] do cannot guarantee the robustness against geometrical attacks. This paper extends the traditional LPM to a rotation-invariant mapping which produces a geometrical-transform-invariant domain by removing the row cyclic shifted effect in the traditional log-polar image which is then transformed by 2-D DWT. The resulting wavelet domain, which is invariant to all the geometrical operations, is used for the computation of the watermark to be embedded.

The remainder of this paper is organized as follows. The rotation-invariant LPM is presented in Section II. The procedures of watermark embedding and detection are described in Section III and Section IV respectively. Section V gives the experimental results to verify this new watermarking scheme. We conclude the paper in the last section.

II. ROTATION-IN Variant LOG-POLAR MAPPING

LPM transforms the point \((x, y)\) on Cartesian coordinates in the input original image into \((r, w)\) on log-polar coordinates in the output log-polar image. LPM is a well-known space-variant image representation used in some computer vision systems, by which a rotation on Cartesian coordinates is converted into a cyclic shift on log-polar coordinates. If the sampling rate of LPM in the radial and angular directions is constant, and the central point is used as the origin of the Cartesian coordinates, the scale and translation effects in the input image are eliminated.

In log-polar resampling, pixels are indexed by ring number \(r\) and wedge number \(w\), related to ordinary \(x, y\) Cartesian
coordinates by the following mapping
\[
\rho = \sqrt{(x - x_c)^2 + (y - y_c)^2} \quad , \quad \theta = \arctan \frac{y - y_c}{x - x_c} \tag{1}
\]
\[
r = \frac{(N_r - 1) \log(\rho/\rho_{\min})}{\log(\rho_{\max}/\rho_{\min})} \quad , \quad w = \frac{N_w \theta}{2\pi} \tag{2}
\]
where \((\rho, \theta)\) are polar coordinates of the pixel located at \((x, y)\), \((x_c, y_c)\) is the origin of the Cartesian coordinates, \(N_r\) and \(N_w\) are the numbers of rings and wedges respectively (sampling rate in the radial and angular directions), \(\rho_{\min}\) and \(\rho_{\max}\) are the radii of the smallest and largest rings of samples respectively.

Though the above traditional LPM is invariant to scale and shifting of the input image, it is sensitive to rotation since a rotation on Cartesian coordinates results in a cyclic shift on log-polar coordinates, which is illustrated in Fig. 1 where the traditional LPM is applied on two rotated versions of the Barbara image. It is obvious that the rotation sensitivity of the traditional LPM is the main obstacle of designing a robust wavelet-based watermarking scheme. Therefore, an extended LPM is proposed here to further eliminate the rotation effect.

### Theorem 1
The directional line pointing from the geometrical center to the gravity centroid of an image is a rotation-specific axis.

Using some matrix operations, you can easily prove the above theorem.

Fig. 2 illustrates that the rotation has no effect on the rotation-invariant LPM.

![Fig. 2. The effects of geometrical transform on rotation-invariant LPM](image)

To describe the rotation-invariant LPM, we need to give a definition of rotation-specific-axis as follows

**Definition 1:** Let \(f(x, y)\) denote the brightness distribution of a \(2 \times D\) image, \(R\) the rotation operator and \(L\) a procedure which outputs from an image a directional line identified by its starting and ending points. We rotate the input image \(f(x, y)\) by degree \(\theta\), which is denoted by \(\hat{f} = R(f, \theta)\). Applying the procedure \(L\) to \(f\) and \(\hat{f}\), we get two lines \(l\) and \(\hat{l}\): \(l = L(f)\) and \(\hat{l} = L(\hat{f})\). We say \(l\) is a rotation-specific axis of the image \(f(x, y)\) with respect to the procedure \(L\) if and only if \(\hat{l} = R(l, \theta)\).

The underlying idea of the rotation-invariant LPM is to use a dynamic Cartesian coordinate system of the input image based on a rotation-specific axis to compensate the rotation effects. We have observed the fact that given a Cartesian coordinate system in the input original image whose origin is the center of the image and horizontal axis is a rotation-specific axis, the log-polar image using constant sampling rate for rings and wedges based on this system is invariant to rotation, scale and translation.

Obviously, the key to transform the input image through LPM to a new domain that is invariant to geometrical transform is to find a rotation-specific axis. Therefore, we give a theorem here to locate it.

### III. WATERMARK EMBEDDING

The watermark to be embedded is generated by scaling the wavelet coefficients of a random image according to the content of the host image in order to achieve the best tradeoff between robustness and invisibility. As shown in Fig. 3, we have the embedding steps

1. Generate a random image of size \(C_r \times C_w\) from the copyright owner’s key where \(C_r \times C_w\) is the sampling rate of LPM, i.e., the numbers of the rings and wedges in the log-polar mapping respectively.
2. Locate the rotation-specific axis \(\hat{\theta}\).
3. Transform the host image \(I(x, y)\) into \(M_I(r, w)\) using the rotation-invariant LPM.
4. Compute the DWT of \(M_I(r, w)\) and \(R(x, y)\) respectively. Denote the results by two coefficient matrices \(D_I\) and \(D_R\).
5. Scale each coefficient in the matrix \(D_R\) according to the energy distribution in \(D_I\) using a pixel-wise masking method and then inversely transform by the inverse DWT and the inverse log-polar mapping to form the watermark \(\hat{R}\).
6. Add the watermark \(\hat{R}\) to the host image \(I(x, y)\) in the spatial domain with a strength controlling parameter to obtain the watermarked image \(\hat{I}(x, y)\).

The embedded signal should be imperceptible and robust at the same time. This requires the watermark energy to be adapted to the image content. It’s commonly accepted that human visual perception is non-linear and is strongly dependant on the frequency as well as the orientation of the stimuli. Thanks to its excellent spatio-frequency localization property, the DWT is very suitable to identify the image areas where a disturbance can be more easily hidden. In our watermarking embedding procedure, each wavelet coefficient of the random image is scaled before being inversely transformed, by a weighing parameter computed according to the energy distribution of the frequency domain of the host image. We apply a pixel-wise scaling method to do this work, which is proposed in [5] to give the maximum amount of modifications...
Fig. 3. The diagram of watermarking embedding procedure. RSA is the acronym of rotation-specific axis and $\theta$ is the direction of RSA that can be applied to the corresponding DWT coefficient based on the optimum quantization step of each coefficient.

IV. WATERMARK DETECTION

In our watermarking scheme, watermark detection is accomplished without referring to the original host image. It is straightforward to compare a correlation coefficient computed between the test image and the unscaled watermark with a threshold. It is clearly a suboptimal correlator. In our detection procedure, the detector generates an estimated watermark from the test image using the similar scaling procedure as used in the embedder.

![Diagram of watermarking detection procedure](image)

Fig. 4. The diagram of watermarking detection procedure

Obviously, the computation of the gravity centroid is a crucial step in our watermarking scheme to achieve the robustness against the geometrical attacks, so it is a vulnerable attacking target. For example, it is easy to modify the watermarked image slightly to displace the original gravity centroid such that the detection process cannot succeed. In order to make the computation of the gravity centroid robust against this specific attack, we suggest using only the most significant bits of pixels to do the computation so that the position of the gravity centroid depends heavily on the content of the image. To displace it, you have to modify the image significantly to the extent such that the commercial value of the image cannot be maintained.

Note that the correlation between the estimated watermark $\hat{R}$ and the resized test image $\hat{I}$ is computed over the pixels inside the circles tangent to their borders because of the log-polar mapping utilized in our watermarking system.

V. NUMERICAL RESULTS

To evaluate the performance of the proposed watermarking scheme, we conduct experiments using Lena and Barbara images and compare the experimental results of robustness against geometrical attacks between our proposed scheme and Barni’s method [5]. The sampling rate $C_r \times C_w$ for LPM is $512 \times 512$. The strength controlling parameter $\alpha$ is 0.4 in the proposed scheme and 0.25 in Barni’s method so as to get the watermarked images with similar fidelity. As for the computation of the gravity centroid, we use only the first four most significant bits of pixels so as to make the centroid’s position closely related to the significant components of the image, and therefore robust to the attack trying to displace it.

In the experiments of robustness to geometrical attacks, we assume that the image is cropped around the corners only by the rotation operation.

Fig. 5 shows the original, watermarked images and the embedded watermarks. The watermarking key is 500. The watermarked image has the PSNR of 43.32 dB that is sufficient for invisibility requirement. The 500 watermark is embedded in the Lena and Barbara images respectively among 1000 watermarks generated using different keys and the similarities output from the detector are shown in Fig. 6. The results show that the similarities with the 500th watermark are the highest, which also satisfy a predetermined threshold ($T = 0.015$ as the dashed line shows). Therefore, the person with 500th key can insist on their copyright ownership of the images.

Fig. 7 and Fig. 8 show that the proposed scheme is robust to waveform attacks. In Fig. 7, the watermarked Lena image with 500th key was compressed by JPEG and JPEG2000 respectively. Fig. 7(a) shows the similarities in the JPEG compressed Lena image at different quality factors from 0 (best compression) to 100 (best image quality). We can see, the watermark could still be well detected even after the image is compressed by JPEG at the quality factor of 15, at which the image has PSNR of only 31.5 dB. Also in the proposed scheme robustness is found against low pass filtering as shown in Fig. 8. Fig. 8(a) and Fig. 8(b) present the detection responses in the watermarked Lena image after...
averaging and median filtering to size $3 \times 3$. Although the response is lower after filtering, since it is still much higher than the threshold, the owner's copyright can still be protected.

Figs. 9 and Fig. 11 show that the proposed watermarking scheme is robust to geometrical attacks. Fig. 9 represents the results of rotational attacks with cropping around the corners using different rotation degrees ranging from $0^\circ$ to $360^\circ$. Compared with Barni's method that is vulnerable to even a slight rotation, the proposed scheme demonstrates its amazing ability of surviving for all the rotation degrees as the uniform curve of its similarities shows in Fig. 9(b). Note that the peak values of the response curve appear at the degrees of multiples of $90^\circ$ in Fig. 9(b) because there is no information loss due to rotation operations at these special degrees. Fig. 10 shows the similarities computed by different scaling factors. In Fig. 10(a), Barni's method is vulnerable to scaling attacks, while in Fig. 10(b) our proposed scheme demonstrates strong robustness to scaling operations with different scaling factors ranging from 0.5 to 3.5. The robustness of our proposed scheme against the attacks of rotation accompanied with scaling of different degrees and scaling factors is illustrated in Fig. 11.

![Fig. 5. Original, watermarked images and the embedded watermark](image)

![Fig. 6. Similarity in Lena and Barbara images with watermarks of 1000 different keys](image)

![Fig. 7. Similarity in Lena with watermarks of 1000 different keys after compression](image)

![Fig. 8. Similarity in Lena with watermarks of 1000 different keys after suffered filtering attacks](image)

![Fig. 9. Similarity in watermarked Lena image after rotation attacks](image)

![Fig. 10. Similarity in watermarked Lena image after scaling attacks](image)

![Fig. 11. Similarity in the watermarked Lena image after rotation accompanied by scaling.](image)

VI. CONCLUSION

This paper proposed a novel wavelet-based watermarking scheme, which is not only robust to common signal processing operations, but also resilient to geometrical attacks. Our experimental results showed that the performances of our proposed scheme are very impressive, particularly its robustness against geometrical attacks. In our algorithm, we haven’t considered the cropping attack. We assume the images are cropped only around the corners from the rotation operation. The future work should address this cropping attack that might be accompanied with the geometrical transformation.

REFERENCES


