Geometric Attack Resistant Image Watermarking for Copyright Protection

D. E. Koutsonanos, D. Simitopoulos and M. G. Strintzis
Informatics and Telematics Institute, Thermi-Thessaloniki, Greece

Abstract

This paper presents a novel watermarking scheme able to resist geometric attacks. The proposed method performs watermarking of images in the raw domain. A perceptual model is used in order to define the strength of the embedded watermark. For resistance to scaling and rotation attacks, two generalized Radon transformations of the image are introduced, while resistance to translation is accomplished through a localization of the watermarking method based on feature points of the image. Experimental evaluation demonstrates that the proposed scheme is able to withstand a variety of attacks including common geometric attacks.

1. Introduction

Watermarking of images is a technology that has attracted a lot of attention in recent years. In order to verify the robustness of the proposed watermarking schemes, a variety of attacks must be imposed to the image.[1] Among them, geometric attacks such as scaling, rotation and translation are easy to apply and may lead many watermark detectors to total failure due to loss of synchronization between the embedded and the correlating watermark.

Lately, a lot of watermarking methods resistant to geometric attacks were presented in the literature. These may be divided in three categories. In some approaches, the watermark embedding is performed in a domain invariant to geometric attacks,[2,3] while in others an additional pattern is embedded in the image in order to be able to revert the geometric attack.[4] Yet another approach for resisting geometric attacks is based on geometrically transforming a reference watermark both in the embedding and detection (correlation) according to a characteristic of the image content. A similar approach was presented from Bas et al[5] where characteristics of the image content were extracted using Principal Component Analysis.

The watermarking method presented in this paper, is also based on the latter approach to geometric resistant watermarking. First, a corner detection scheme detects corners in the image content and finds the most robust among them. This corner is used as an origin for two one-dimensional generalized Radon transformations that are applied to the image. According to characteristic values extracted from the two transformations during the embedding and detection of the watermark, a reference watermark is scaled and rotated before embedding or correlation based detection respectively. This way, synchronization between the embedding and the correlating watermark is achieved. The experimental results demonstrate the resistance of the proposed scheme to geometric attacks as well as other common attacks.

2. One-Dimensional Generalized Radon Transformations

A generalized Radon transformation[6] of a function $g(x,y)$ is defined as the integral along a curve expressed by the form $\omega(x,y;\mathbf{z})$

$$\check{g}(\mathbf{z}) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} g(x,y)\delta\left(\omega\left(x,y;\mathbf{z}\right)\right)dxdy \tag{1}$$

where $\mathbf{z} = (z_1, z_2,\ldots,z_n)$ is the parameter vector of the transform domain.

We propose the use of two one-dimensional generalized Radon transformations for resistance to scaling and rotation attacks respectively. The Radial Integration Transform (RIT) will be used to deal with rotation attacks, while the Circular Integration Transform (CIT) will be used to cope with scaling attacks.

2.1. Radial Integration Transform (RIT)

The RIT of a function $f(x,y)$ is defined as the integral along a straight line that begins from the origin (x_o,y_o) and has angle θ with respect to the horizontal axis (see Fig. 1). The RIT is given by the following equation

$$R_f(\theta) = \frac{\sin(2\theta)}{|\sin(2\theta)|}\lim_{a\to\infty}\int_{y_o}^{y_o+a\sin\theta}\int_{x_o}^{x_o+a\cos\theta} f(x,y)\cdot \delta((y-y_o)\cos\theta-(x-x_o)\sin\theta)dxdy \tag{2}$$

Another equivalent way of writing equation (2) is

$$R_f(\theta) = \int_0^{+\infty} f(x_o+s\cos\theta, y_o+s\sin\theta)ds \tag{3}$$

where the s-axis, lies along the integration line.

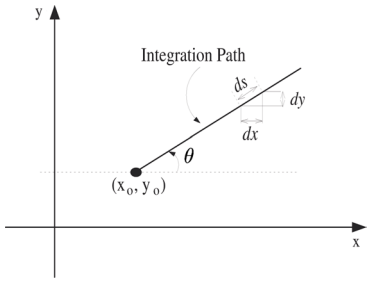

Figure 1. Radial Integration Transform (RIT).

2.2. Scaling and Rotation Properties of the RIT

If $f(x,y)$ is an image and $g(x,y) = f(sx,sy)$ is the image scaled by s in both directions, then the RIT of image $g(x,y)$ is given by

$$R_g(\theta) = \frac{1}{s} R_f(\theta) \tag{4}$$

Therefore, the RIT of the scaled image is multiplied by the factor $1/s$.

If $f(r,\phi)$ is an image written in polar form and $g(r,\phi) = f(r,\phi - \phi_a)$ is the image rotated by ϕ_a around the (r, ϕ_a) system origin, then equation (2) may be rewritten in polar form in the following way for images $f(r,\phi)$ and $g(r,\phi)$ respectively

$$R_g(\theta) = R_f(\theta - \phi_a) \tag{5}$$

Therefore, the RIT of the rotated image is translated by ϕ_a.

2.3. Circular Integration Transform (CIT)

The CIT of a function $f(x,y)$ is defined as the integral along a circle with center (x_o,y_o) and radius ρ (see Fig 2). The CIT is given by the following equation

$$C_f(\rho) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x,y) \cdot \delta(\rho - \sqrt{(y-y_o)^2 + (x-x_o)^2}) dx dy \tag{6}$$

Another equivalent way of writing equation (6) is

$$C_f(\rho) = \int_0^{2\pi} f(x_o + \rho\cos\theta, y_o + \rho\sin\theta) ds \tag{7}$$

where the differential ds lies along the ρ radius circle.

2.4. Scaling and Rotation Properties of the CIT

If $f(x,y)$ is an image and $g(x,y) = f(sx,sy)$ is the image scaled by s in both directions, then the CIT of image $g(x,y)$ is given by

$$C_g(\rho) = \frac{1}{s} C_f(s\rho) \tag{8}$$

Therefore, the CIT of the scaled image is scaled by s and also multiplied by the factor $1/s$.

If $f(r,\phi)$ is an image written in polar form and $g(r,\phi) = f(r,\phi - \phi_a)$ is the image rotated by ϕ_a around the (r,ϕ) system origin, then equation (6) may be rewritten in polar form in the following way for images $f(r,\phi)$ and $g(r,\phi)$ respectively

$$C_g(\rho) = C_f(\rho) \tag{9}$$

Therefore, the CIT of an image is independent of rotation.

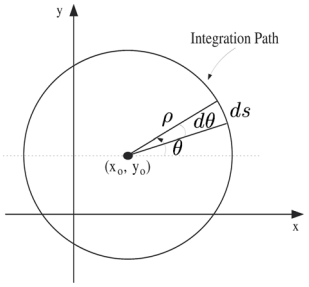

Figure 2. Circular Integration Transform (CIT).

2.5. Discrete RIT and CIT

For the discrete RIT, equation (3) is transformed to

$$R(t\Delta\theta) = \frac{1}{J} \sum_{j=1}^{J} I(x_o + j\Delta s \cdot \cos(t\Delta\theta), y_o + j\Delta s \cdot \sin(t\Delta\theta)), t = 1, \ldots, T \tag{10}$$

where $\Delta\theta$ and Δs are the constant step sizes for the corresponding variables, J is the number of points between the origin and the end of the image $I(x,y)$ on the radius with orientation θ, and $T = 360/\Delta\theta$.

For the discrete CIT, equation (7) is transformed to

$$C(k\Delta\rho) = \frac{1}{T} \sum_{t=1}^{T} I(x_o + k\Delta\rho \cdot \cos(t\Delta\theta), y_o + k\Delta\rho \cdot \sin(t\Delta\theta)), k = 1, \ldots, K \tag{11}$$

where $\Delta\rho$ and $\Delta\theta$ are the step sizes for the corresponding variables, $K\Delta\rho$ is the radius of the smallest circle that encircles the image, and $T = 360/\Delta\theta$. The discrete RIT and CIT ($x_o = 180$, $y_o = 435$) of the original and an attacked Lena image (scaling = 0.6, rotation = 30°, JPEG Q = 70%) are presented in Fig. 3, where the scaling and rotation properties of the proposed transforms can be clearly identified. It should also be noted, that $I(x,y)$ in equations (10) and (11) may never coincide with image samples. This means, that interpolation in both dimensions, like bilinear or cubic interpolation, must be used.

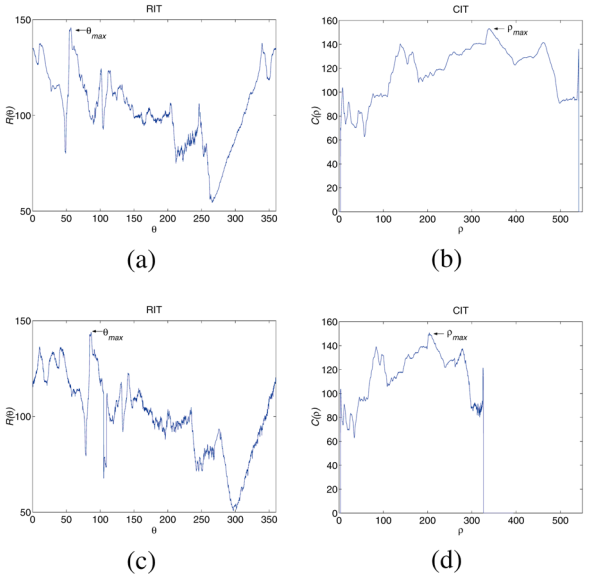

Figure 3. (a) RIT of the original Lena image, (b) CIT of the original Lena image, (c) RIT of the attacked image, (d) CIT of the attacked image.

3. Resisting Geometric Transformations Using RIT and CIT

The RIT and CIT properties given in equations (4), (5), (8) and (9) are very desirable in watermarking applications in which resisting the geometric attacks performed on the watermarked image is required. This can be accomplished by the watermark embedding and detection scheme explained in the following.

First, a two-dimensional watermark is created, to be used as a reference watermark. This watermark corresponds to a reference coordinate θ_r in the RIT domain and a reference coordinate ρ_r in the CIT domain. Then the RIT and CIT of the original image are calculated and the maximum value of each domain is found. The position of the maximum RIT and CIT coefficient, θ_{max} and ρ_{max} respectively, define the geometric transformation that the reference watermark should undergo before additive embedding in the original image is performed. Specifically, the reference watermark is first scaled by $s_w = \rho_{max}/\rho_r$ and rotated by $r_w = \theta_{max} - \theta_r$, and then embedded in the image.

Then, we assume a scaling and a rotation attack to the watermarked image by s_a and θ_a respectively. Based on the RIT and CIT properties, it is obvious that after the attack, the location of the new maximum will be $\theta_{max} + \theta_a$ for RIT and $s_a\rho_{max}$ for CIT. Subsequently, in the detection process, if the reference watermark is scaled by $sw = s_a\ \rho_{max}/\rho_r$ and rotated by $r_w = \theta_{max} - \theta_r + \theta_a$, the embedding and the correlating watermark will be synchronized (same scale and orientation), which is vital for a successful detection.

This concept for resisting geometric attacks can only be applied if the position of the origin (which is the same for both transformations) can be located after the attack. For this reason, the origin is a feature point extracted from the image content.

4. Watermark Embedding

The proposed watermarking scheme, which is based on the concept described in the previous section, performs the watermark embedding in the following steps:

- A random two-dimensional sequence of +1 and –1 is created based on a secret key. Each value of the sequence is spread in blocks sized B x B (B = 2). This block-based watermark will be used as the reference watermark.
- A corner detector is applied in the image and the most robust among the detected corners is extracted.
- Using the location of the most robust corner as the origin, the RIT and CIT are applied to the image. Then, θ_{max} and ρ_{max} are found and the rotation parameter r_w and the scaling parameter s_w are calculated.
- The reference watermark is geometrically transformed using r_w and s_w.
- A perceptual analysis for each image pixel X(i,j) is performed,[7] in order to determine the strength of the watermark.
- Additive embedding of the watermark in the spatial domain is performed.

After experimenting with a set of 500 photographic images where the watermark was embedded, no noticeable degradation of the image quality was observed and the minimum and average PSNR observed were 39.97db and 41.76db respectively.

5. Detection

For the detection of the watermark, a correlation-based detection scheme is applied. The detection process can be divided into the following steps:

- The watermark W is created by using the owner's secret key.
- A corner detector is applied in the image and the most robust among the detected corners is extracted.
- The scaling and rotation parameters s_w and r_w, that will be used to create the correlating watermark W', are estimated by using the detected corner as the origin for RIT and CIT.
- The watermark W is geometrically transformed and the correlating watermark W' is created.
- The correlation value c between the watermarked and possibly distorted N image pixel values $Y(i,j)$ (after the local mean in a 7x7 window is subtracted) and the watermark values $W'(i,j)$ is calculated:

$$c = \frac{1}{N}\sum_i \sum_j Y(i,j)\, W'(i,j)$$

- The correlation value c is compared to the threshold T, which is defined according to the allowed false alarm probability of the detection scheme.

It should be noted, that if the corner with the maximum value in the cornerness function is not the same with the one used as origin in the embedding (detection fails), the described process is repeated starting from the third step. This happens because in some cases of attacks the correct corner may not be detected as the highest local maximum, but an iterative run of the process for a small number of the highest local maximums leads to a correct detection of the watermark.

6. Experimental Results

The experiments presented in the following were all performed using the image Lena, which was watermarked using $W_p = 5$ in the perceptual analysis. The corner detected at ($x_o = 180$, $y_o = 435$) was used as the origin for the RIT and CIT transforms. The parameters of these transforms were set to the following values: $\Delta\theta = 0.01$, $\Delta s = 0.5$, $\theta_r = 0^o$ for the RIT transform and $\Delta\rho = 0.1$, $\Delta\theta = 0.0002$, $\rho_r = 250$ for the CIT transform. Linear interpolation was used for the geometrical transformations of the watermark.

Various attacks were directed on the watermarked image. The corresponding errors of the estimated geometrical transformations of the image, and the corresponding correlator values are presented in Table 1. The RIT and CIT in the case of the attack of the last column are given in Fig. 3c and 3d.

Finally, the correlator value for the watermarked image Lena using 5000 different correlating watermarks is given in Fig. 4. The 1000th watermark is the valid correlating watermark. The experimental mean and variance of the correlator value derived from this test were very close to the corresponding theoretical values which were used to determine the threshold $T = 0.2$ for a given false alarm probability $P_{fa} = 10^{-13}$.

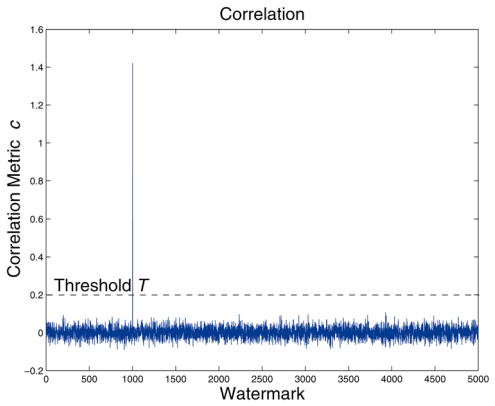

Figure 4. Correlator values for the watermarked image Lena using 5000 different correlating watermarks.

Table 1. Correlator output results for various attacks on the watermarked image Lena.

Attack	Scaling	0.6	-	0.6	0.6
	Rotation	-	30^o	30^o	30^o
	JPEG Q = 70	√	√	-	√
Estimation error	Scaling	0.001	0.004	0.003	0.001
	Rotation	0.03	0.12	0.12	0.06
Correlation value c		0.92	0.50	0.50	0.61

7. Conclusion

A novel watermarking scheme robust to geometrical transformations was presented. The scheme is based on the properties of the RIT and CIT generalized Radon transformations and manages to synchronize the embedding and the correlating watermark in case of geometrical and compression attacks.

References

1. F. A. P. Petitcolas,Watermarking schemes evaluation, IEEE Signal Processing vol. 17, no. 5, pp. 58-64, (2000).
2. C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, Y. M. Lui, Rotation, scale and translation resilient watermarking for images, IEEE Trans. Image Processing vol. 10, no. 5, pp. 767-782, (2001).
3. J. O'Ruanaidh, T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Signal Processing vol. 66, no. 3, pp. 303-317, (1998).
4. S. Pereira, T. Pun, Robust template matching for affine resistant image watermarks, IEEE Trans. Image Processing, vol. 9, no. 6, pp. 1123-1129, (2000).
5. P. Bas, B. Macq, A new video-object watermarking scheme robust to object manipulation, in: ICIP, Thessaloniki, Greece, Vol. 2, pp. 454-457, (2001).
6. P. Toft, The Radon Transform: Theory and Implementation, Ph.D. thesis, Technical University of Denmark, http://www.sslug.dk/~pto/PhD/, (1996).
7. D. Simitopoulos, D. Koutsonanos and M. G. Strintzis, Robust Image Watermarking based on Generalized Radon Transformations, accepted for publication on IEEE Trans. Circuits and Systems for Video Technology.

Biography

Dimitrios Simitopoulos was born in Greece in 1977. He received his Diploma in Electrical and Computer Engineering from Aristotle University of Thessaloniki, Greece, in 1999. He is currently working towards the Ph.D. degree in the same department of Aristotle University of Thessaloniki, where he holds a teaching assistantship position. Since 2000, he is working as a research assistant in Informatics and Telematics Institute. His research interests include watermarking and multimedia security and image indexing and retrieval.