ROTATION AND SCALE INSENSITIVE IMAGE WATERMARKING

Maxime Ossonce, Claude Delpha and Pierre Duhamel*

Laboratoire des Signaux et Systemes
CNRS-UPS-SUPELEC
Supelec 3 rue Joliot Curie 91190 Gif/Yvette - France
{maxime.ossonce, claude.delpha, pierre.duhamel}@lss.supelec.fr

ABSTRACT

Using electronic watermarks as copyright protection for still images requires robustness against attacks. In this paper we propose a watermarking scheme that is robust to rotation, scaling and translation (RST) distortions. The watermark is embedded in a 1-D invariant domain that is a projection of the polar Fourier Transform. Roc curves depicting false positives versus detection probability of the watermark are provided, under various geometrical attacks and JPEG coding.

1. INTRODUCTION

Open networks like internet allow multimedia content to be duplicated, shared or even sold whithout any copyright control. Identifying illegal operations requires media tracking tools like digital watermarking.

Digital watermarking is the communication of information by embbeding it into multimedia data, called *host data*. Many applications, including hidden channel, authentication, copyright protection, represent several applications of digital watermarking. As far as this paper is concerned, copyright protection of still images, robustness of watermark scheme against intentional and unintentional attacks is a main issue. Attacks that have to be prevented against include noise attacks, coding attacks (*e.g.* jpeg coding), and geometrical attacks. Geometrical attacks may be intentional, or, in our specific case, operated by the system which will make use of the watermarking scheme: in our case, it is required that the watermark that is hidden in the plain resolution image should be recovered from a small scale version of it. Several approaches have been developed in recent papers to increase robustness of watermark algorithms to geometrical attacks.

A first approach, used by [1], embeds in the host image two watermarks. The first one, called the template, carries no information. It is a specifically designed registration pattern, easily detected, that allows the detector to estimate which RST distortions have been applied and invert them before detection. A second solution chosen in [2] consists in embedding the same pattern at multiple spatial locations. The autocorrelation function of the watermarked image will be a pattern of peaks that will give information to the detector for identification of the affine distortions to which the watermarked image has been subjected. These approaches have two failure modes, since for successful detection both the identification of the geometric distortion and the detection of the watermark must be successful. A more recent approach, presented in [3] uses salient points in the image. Watermark is not synchronized with an absolute coordinate system but on a content dependent basis. Salient points offer robustness against even local geometrical distortions. A last approach uses invariant domains, like the Fourier-Mellin transform, to embed the watermark. In [4], a 2-D RST-invariant domain, using the Fourier Mellin Transform (the Fourier Transform of the log polar description of the image) is used for watermark embedding. The main limitation of this scheme is the use of strong invariant. Severe difficulties were encountered in the implementation of the watermark embedding process. However, a 1-D projection of a strong invariant, as proposed in [5], offers the possibility of domain inversion. The embedding process is then easier. The domain is obtained from a log polar interpolation of the DFT of the image.

We present here an algorithm that performs digital watermarking in a domain which is invariant under the main geometrical distortions. In previous works [5], the extraction domain was a 1-D projection vector that is a function of interpolated DFT on log-polar grid. The algorithm presented here embeds a watermark (signature) in a domain that is the mean of the polar continuous Fourier Transform (FT) amplitude on the radii at several angles. However, the embedding is performed at the spatial (image) level. No specific interpolation is required.

Our paper is organized as follows: in Section 2 we describe the extraction domain, the embedding and detection processes. We encountered several implementation problems that are described with solutions in Section 3. Section 4 then presents the results obtained on an image database.

2. ALGORITHM

2.1. Algorithm Presentation

The watermarking scheme described in [6], used here, defines two processes. In the detection process the *extraction function* X generates for a given media content c an *extracted vector* $\underline{s} \in \mathcal{S}$, $\mathcal{S}$ being the *extraction domain*. A *detection function* D (generally a correlation function) operates the detection $d = D(\underline{s}, \underline{w})$ and gives either a boolean or a scalar that will have to be thresholded (hard/soft decision) to decide whether the content is watermarked with $\underline{w}$ or not. In the embedding process we have a *mixing function* F that gives for a given extracted vector $\underline{s}$ and a watermark $\underline{w}$ a *mixed signal* $\underline{s}_w = F(\underline{s}, \underline{w})$ which is perceptually similar to $\underline{s}$ and has a high correlation with $\underline{w}$. We then generate a media

This work is funded by the RNRT DIPHONET project on copyright protection of still images

This work is currently subject to patent protection.

content c_w, perceptually close to c

$$c_w = Y(c, \underline{s}_w)$$

so that

$$X(c_w) = \underline{s}_w$$

The function Y is called the the *inverse extraction* function.

In the watermark scheme presented here the extracted vector is the radial mean of the continuous FT modulus of the image, at some directions θ_i, uniformly distributed in $[0, \pi]$. We find an analytic formulation of the variations to carry out to the FFT modulus of the image for the watermark embedding. So we differ from [5] (the closest method we found in the litterature) in two ways: (i) the extraction of the vector does not use a log-polar interpolation grid and (ii) the watermark insertion is done in the spatial domain, in such a way that its signature in the extraction domain has the required form. Thus, this procedure does not require transforming the image from the spatial to the extraction domain back and forth.

2.2. Radial Mean of the FT modulus

The extraction function

$$\underline{s} = X(c)$$

is such that s_i is the radial mean of the continuous FT modulus at direction θ_i. First define the extraction domain in terms of continuous integrals, in order to better understand the method. The implementation of the computation of the extracted vector is addressed in subsection 3.1 below.

Let $c(k, l)$ a $K \times L$ image. It might be defined for $(k, l) \in \mathbb{Z}^2$ with $c(k, l) = 0$ for $(k, l) \notin \mathcal{N} = [-\frac{K}{2} \dots \frac{K}{2}-1] \times [-\frac{L}{2} \dots \frac{L}{2}-1]$. We define its continuous FT for a normalized frequency $(x, y) \in \mathbb{R}^2$, $C(x, y)$, 1-periodic :

$$C(x, y) = \sum_{(k,l) \in \mathcal{N}} c(k, l) e^{-2i\pi(kx+ly)} \tag{1}$$

Through a change of variable, the FT of the image c can be defined on a polar basis

$$C(r, \theta) = C(r \cos\theta, r \sin\theta)$$

The FT modulus of an image has some interesting properties in these polar variables, considering $(r, \theta) \in [-\frac{1}{2}, \frac{1}{2}] \times [0, \pi]$:

- it is translation invariant
- if c' is the rotated image c with an angle α, then we have

$$|C'(r, \theta)| = |C(r, \theta - \alpha)|$$

- if c' is the scaled image c (after anti-alisasing filtering) with a factor $a < 1$ per dimension, we have

$$|C'(r, \theta)| = a^2 \cdot |C(ar, \theta)|$$

For a given angle θ and a $K \times L$ image c, define $s(\theta)$ as the radial mean of its continuous FT modulus so that we have

$$s(\theta) = \int_{-\frac{1}{2}}^{\frac{1}{2}} |C(r, \theta)| \, \mathrm{d}r \tag{2}$$

Referring to properties of the FT of a geometrically distorted image, on the radial mean of the FT modulus, one can easily check that :

- it is translation invariant
- if c' is the image c that has been rotated of an angle α, we have:

$$s'(\theta) = s(\theta - \alpha) \tag{3}$$

- if c' is the image c scaled with a factor $a < 1$

$$s'(\theta) = a^2 \cdot \int_{-\frac{a}{2}}^{\frac{a}{2}} |C(r, \theta)| \, \mathrm{d}r \tag{4}$$

Note that the result (4) would be interesting for images that have no high frequency component (for $|r| > \frac{a}{2}$). In this particular case, we would have

$$s'(\theta) = s(\theta) \tag{5}$$

The goal of our algorithm is to embed a watermark in this invariant domain so that it is robust to geometrical distortions. The embedding process will be described in detail in section 2.4. But, for a proper tuning of the system, it should be remembered that for the embedded watermark to be recovered in a scaled image, the watermark noise should not contain high frequency components.

2.3. Watermark Detection Process

Our watermark detector determines whether or not a given watermark $\underline{w}$ has been embedded in the cover image c_u. The detector output is a binary value indicating whether the image contains $\underline{w}$ or not. We first extract from c_u the vector $\underline{s}_u$ of size M the components of which represent the radial mean of the c_u FT modulus at directions

$$\theta_i = \frac{i\pi}{M} \qquad \text{for} \qquad i = \{0, \dots, M-1\}$$

The extraction computation is operated as described in paragraph 3.1. The detection is a normalized correlation coefficient between $\underline{s}_u$ and $\underline{w}$ [6]. As recommended in [7] we apply a whitening filter to the vector and watermark before correlation. The whitening filter coefficients are computed from a database of extracted vectors. We note $\underline{s}'_u$ and $\underline{w}'$ the output of the whitening filter applied to, respectively, $\underline{s}_u$ and $\underline{w}$. We have then

$$d_u^{(0)} = \frac{< \underline{s}'_u, \underline{w}' >}{\sqrt{< \underline{w}', \underline{w}' >< \underline{s}'_u, \underline{s}'_u >}} \tag{6}$$

If an image has been rotated before detection with an angle $\alpha = \frac{p\pi}{M}$ the extracted vector s_u is cyclically shifted of p elements, according to (3). So, by computing (6) for the M shifted versions of s'_u, we shall be able to detect a rotation attack with an angle multiple of $\frac{\pi}{M}$ rad. Hence, a simple vector shifting allows us to recover the watermark in a rotated image. The correlation (6) becomes

$$d_u = \max_{p=0 \dots M-1} \left\{ \frac{< \underline{s}'^{(p)}_u, \underline{w}' >}{\sqrt{< \underline{w}', \underline{w}' >< \underline{s}'_u, \underline{s}'_u >}} \right\} \tag{7}$$

with $\underline{s}'^{(p)}_u$ is the p-shifted version of $\underline{s}'_u$.

The rotation-invariant correlation coefficient d_u is then thresholded and the detection test is

$$c_u \text{ is watermarked with } \underline{w} \iff d_u > T \tag{8}$$

2.4. Watermark Embedding Process

To embed the watermark, our purpose is to additively modify the FT amplitude of the image c_0, while keeping its phase unchanged, since the phase of the image is perceptually more important [8]. We note c_w the watermarked image and C_w its continuous FT. We have

$$\begin{aligned} |C_w(x,y)| &= |C_0(x,y)| + V(x,y) \\ |C_w(r,\theta)| &= |C_0(r,\theta)| + V(r,\theta) \end{aligned}$$

The *watermark noise* V has to respect symmetry. The mixing function F is a weighting function

$$\underline{s}_w = F(\underline{s}_0, \underline{w}) = \underline{s}_0 + \alpha \underline{w} \tag{9}$$

For a given distortion between c_w and c_0, α has to maximized. Hence we have to find first $\hat{V}$ so that

$$\forall i \qquad \int_{-\frac{1}{2}}^{\frac{1}{2}} \hat{V}(r,\theta_i)\,\mathrm{d}r = w_i \tag{10}$$

and the norm of

$$V = \beta \hat{V} \tag{11}$$

will be maximized for a chosen distortion. In this paper, we have chosen the PSNR as a distortion measure, but other criteria based on vision models are also feasible (and could be more efficient).

The low frequency component being perceptually important, we want them to be preserved (this compensates for the lack of perception model).

$$\hat{V}(r,\theta) = 0 \qquad \text{for} \quad |r| \le f_m \tag{12}$$

Accordingly to (5), we want the watermark noise to have no high frequency component so that it is robust to scaling

$$\hat{V}(r,\theta) = 0 \qquad \text{for} \quad |r| \ge f_M \tag{13}$$

Thus, it is necessary to find a good approximation of a collection $\hat{V}_{j=0\ldots M-1}$, respecting those conditions, verifying

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \hat{V}_j(r,\theta_i)\,\mathrm{d}r = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

Those functions and their approximations are presented at paragraph 3.2.

3. IMPLEMENTATION SOLUTIONS

3.1. Computation of the Radial Mean of the FT modulus

For a $K\times L$ given image c, the 1×1-periodic $\mathbb{R}^2$ function $|C(x,y)|$ might represent the continuous FT of an image c^* defined on $\mathcal{L}_2(\mathbb{Z}^2)$. We have then

$$|C(x,y)| = \sum_{(k,l)\in\mathbb{Z}^2} c^*(k,l) e^{-2i\pi(kx+ly)} \tag{15}$$

and (2) becomes

$$\begin{aligned} s(\theta) &= \sum_{(k,l)\in\mathbb{Z}^2} c^*(k,l) \int_{-\frac{1}{2}}^{\frac{1}{2}} e^{-2i\pi r(k\cos\theta + l\sin\theta)}\,\mathrm{d}r \\ &= \sum_{(k,l)\in\mathbb{Z}^2} c^*(k,l)\,\mathrm{sinc}(k\pi\cos\theta + l\pi\sin\theta) \end{aligned} \tag{16}$$

with

$$c^*(k,l) = \int_{[0,1]^2} |C(x,y)| e^{2i\pi(kx+ly)}\,\mathrm{d}x\,\mathrm{d}y \tag{17}$$

In order to be able to compute (16), we have to restrict the sum to $(k,l) \in \mathcal{N}^* = [-\frac{K^*}{2}\ldots\frac{K^*}{2}-1]\times[-\frac{L^*}{2}\ldots\frac{L^*}{2}-1]$. If we choose $|\mathcal{N}^*| = P^2|\mathcal{N}|$ (*i.e.* $K^* = PK$, $L^* = PL$), we can estimate c^* using FFT : c^* will be the IFFT of the P-padded image c FFT modulus. Padding the image P times before computing its FFT oversamples its continuous FT so that we have a better approximation of its amplitude. Eventually, we have

$$s(\theta) = \sum_{(k,l)\in\mathcal{N}^*} c^*(k,l)\,\mathrm{sinc}(k\pi\cos\theta + l\pi\sin\theta) \tag{18}$$

3.2. Computation of the watermark noise

Since the watermark noise $\hat{V}$ has frequency components only for $f_m \le |r| \le f_M$, we want to find the mimimum energy $\hat{V}_j$ so that

$$2\int_{f_m}^{f_M} \hat{V}_j(r,\theta_i)\,\mathrm{d}r = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

and that respects FT amplitude symmetry and periodicity. If $\hat{v}_j$ is the $\hat{V}_j$ inverse FT, we have to solve

$$\sum_{(k,l)\in Z^2} \hat{v}_j(k,l) p_i(k,l) = \delta ij$$

i.e.

$$< p_i, v_j >= \delta ij \tag{20}$$

where

$$\begin{aligned} p_i(k,l) &= \int_{-f_M}^{f_M} e^{2i\pi r(k\cos\theta_i + l\sin\theta_i)}\,\mathrm{d}r \\ &- \int_{-f_m}^{f_m} e^{2i\pi r(k\cos\theta_i + l\sin\theta_i)}\,\mathrm{d}r \end{aligned}$$

that is

$$\begin{aligned} p_i(k,l) &= f_M\,\mathrm{sinc}(2\pi f_M(k\cos\theta_i + l\sin\theta_i)) \\ &- f_m\,\mathrm{sinc}(2\pi f_m(k\cos\theta_i + l\sin\theta_i)) \end{aligned} \tag{21}$$

We find that for sufficiently large images and $M = 180$, considering $\{p_i\}$ as an orthonormal collection is good approximation.

The embedding process must yield to an image that has the same support as c_0, that is c_w must be a $K\times L$ image. So the modification will be carried out to the FFT of c_0, $C_0^{(\delta)}$. Thus, if $\hat{V}^{(\delta)} = \beta\hat{V}^{(\delta)}$ is the amplitude modification to be carried out to the FFT of c_0, $|C_0^{(\delta)}|$

$$|C_w^{(\delta)}| = |C_0^{(\delta)}| + \beta\hat{V}^{(\delta)}$$

with β being maximized under a PSNR constraint, we have

$$\hat{V}^{(\delta)} = \sum_{i=0}^{M-1} w_i P_i^{(\delta)} \tag{22}$$

where $P_i^{(\delta)}$ is the FFT of the $K\times L$ troncated $p_i(k,l)$. Troncating $p_i(k,l)$ is another lossy approximation in the embedding process. Eventually, if $\Phi_0(m,n)$ is the phase of $C_0^{(\delta)}(m,n)$, we have

$$C_w^{(\delta)}(m,n) = \left(|C_0^{(\delta)}(m,n)| + V^{(\delta)}(m,n)\right) e^{i\Phi_0(m,n)} \tag{23}$$

which is the FFT of an image perceptually close to c_0 and the extracted vector of which has a high correlation with the watermark.

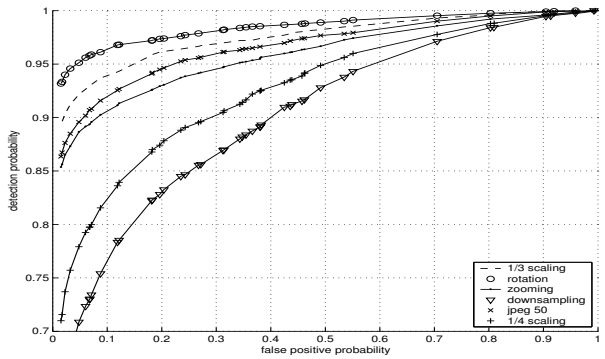

Fig. 1. ROC curves for PSNR=45dB under geometrical attacks and jpeg coding

3.3. Windowing of the image before extraction

Since the image is zero padded in the extraction process, its edges create a cross artifact in its FT, hence bringing irregularities in the extracted vector. The solution we adopted to counter-balance this effect is to multiply the image by a circular window before extraction [9].

4. EXPERIMENTAL RESULTS

The described algorithm has been tested on a large database of 3130 images. The images are taken from a database of press photographs supplied by the press agency ANDIA. The mean size of the images is 2.10^6 pixels. We tested the robustness of the watermark scheme to geometrical attacks and jpeg coding.

Fidelity: In order to avoid degradation of the image in low textured zones, the tests have been carried out with a PSNR of 45 dB.

Algorithm tuning: We chose $M = 180$, hence watermarks in rotated images with an angle of N^o with N integer can be detected. The watermark is embedded at normalized frequencies with norm between f_m and f_M. We chose f_M = 0.25, that allows us by construction to recover watermarks in scaled images of factor 2 per dimension. The test below is concerned with the recovery of the watermark for higher values of the scale factor.

Receiver Operating Characteristic: The ROC curves are presented for JPEG compressed images with quality factor 50. The geometrical attacks are : scaling with factors 3 and 4, a rotation of 6^o (followed by a cropping allowing a natural vision of the picture), a 'zooming' (a 50% per dimension centered cropping followed by a 50% scaling), and a raw downsampling (without anti-aliasing) of the image with a factor 4 per dimension. Note that, due to our applicative constraints (the watermark has to be recovered from small scale versions of the image), the detection process scales down large images before detection, for a faster processing. That is why no results are given for non scaled images.

As a comparison, ref. [5] provides results for 20% scaled down images ($P_d = 0.95$ with $P_{fa} = 0.001$) and cropped rotated images (8^o, $P_d = 0.9$ with $P_{fa} = 0.001$) which corresponds to much easier situations that those reported in this paper.

Figure 1 presents the ROC curve for the different attacks. It gives the detection probability (the probability of detecting the watermark in a watermarked image) yielded for different probability of false positive (P_{fa}, the probability of detecting the watermark in unwatermarked images) that can be tuned with the threshold defined in (8).

We see that even with $f_M = 0.25$ – that is the algorithm is tuned for a maximum factor 2 scaling – a scaling with a factor 3 allows a detection probability of 0.82 with a false positive probability of 0.001. Rotation doesn't affect detection, as expected: a rotation followed by a factor 2 scaling yields $P_d = 0.88$ with $P_{fa} = 0.001$. A cropping of 50% followed by a scaling of a factor 2 yields better detection (0.78 detection probability with $P_{fa} = 0.001$) than a factor 4 scaling ($P_d = 0.55$ with a 0.001 false positive). This is due to the tuning of the method: better detection for higher scaling factors could be obtained with lower f_M. Note that the lower f_M, the more visible will be the watermark noise for a given PSNR. With $P_d = 0.76$ with $P_{fa} = 0.001$, resistance to jpeg coding (the effect of which is more present in high frequencies) can be explained by the fact that watermark is not present in HF components.

5. CONCLUSION

We designed a watermark algorithm robust to various geometrical attacks that occur in current pictures manipulations. Results on watermarks robustness have been presented on a large database of 3130 images. The results are presented for large (2MP) pictures reduced down to 150KP. Further work will consider smaller images. The robustness to rotation can also be improved, since it is currently limited to integer numbers of degrees. Further studies will involve an oversampled detection process, which should improve most of the current characteristics.

6. REFERENCES

[1] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarking," in *Int. Workshop on Info. Hiding*, 1999.

[2] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in *Proc. of SPIE*, november 1998.

[3] P. Bas, Chassery J. M., and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. on Image Proc.*, vol. 11, no. 9, september 2002.

[4] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *Proc. IEEE ICIP*. october 1997, vol. 1, pp. 536–539, IEEE Signal Proc. Society.

[5] C.Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, et al., "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. on Image Proc.*, vol. 10, 2001.

[6] I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proc. of the IEEE (USA)*, vol. 87, no. 7, pp. 1127–1141, 1999.

[7] G. Depovere, T. Kalker, and J.-P. Linnartz, "Improved watrmark detection reliability unsing correlation before correlation," in *IEEE ICIP*, 1998, vol. 1, pp. 430–434.

[8] D. Cochran, "Phase and magnitude in normalized images," *IEEE Trans. IP*, vol. 3, no. 6, pp. 858–862, nov 1994.

[9] E. De Castro and C. Morandi, "Registration of translated and rotated images using fourier finite transforms," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 9, pp. 700–73, 1987.