# Maximum Correlation Search Based Watermarking Scheme Resilient to RST

Sergio Bravo and Felix Calderón

Universidad Michoacana de San Nicolás de Hidalgo,
División de Estudios de Posgrado de Ingeniería Eléctrica,
Santiago Tapia 403 Centro,
Morelia, Michoacán, México. CP 58000
sbravo@lsc.fie.umich.mx, calderon@zeus.umich.mx

**Abstract.** Many of the watermarking schemes that claim resilience to geometrical distortions embed information into invariant or semi-invariant domains. However, the discretisation process required in such domains might lead to low correlation responses during watermarking detection. In this document, a new strategy is proposed to provide resilience to strong Rotation, Scaling and Translation (RST) distortions. The proposed detection process is based on a Genetic Algorithm (GA) that maximises the correlation coefficient between the originally embedded watermark and the input image. Comparisons between a previous scheme, based on Log-Polar Mapping (LPM), and the present approach are reported. Results show that even a simple insertion process provides more robustness, as well as a lower image degradation.

## 1 Introduction

Multimedia applications are arising, and technological advances afford faster and cheaper forms of copying and distributing multimedia data, with high quality. Hence, digital watermarking has been proposed to provide suitable alternatives to detect copyright infringements, tampering, and so forth. However, any digital signal might suffer a wide set of accidental and incidental distortions that can severely damage and even destroy the embedded watermarks.

In most watermarking schemes, geometrical distortions, applied on content images, usually lead to wrong detection responses due to synchronisation loss between watermarks and detectors.

When the original (non-watermarked) image is available for the detector, synchronisation might be easily restored by using conventional image registration techniques [1], before testing the presence of a watermark. Yet, detectors will seldom be provided the original image in real applications. Thus, different strategies have been proposed to deal with the effects of geometrical distortions in watermarking schemes that do not require the original image during detection.

Some approaches embed either a template (along with the watermark) or a periodic watermark to generate a defined pattern that is used to effectively invert affine transformations in content images before detection [2,3,4,5]. Both

M. Lazo and A. Sanfeliu (Eds.): CIARP 2005, LNCS 3773, pp. 762–769, 2005.

strategies usually provide robustness against geometrical attacks. However, detectors are unable to restore synchronisation if the templates are removed by using specialised attacks, such as collusion and template removal attacks [6,7].

Another proposed strategy is to embed the watermarks into invariant or semi-invariant domains provided by the Fourier-Mellin transform, or Log-Polar Mapping (LPM) [8,9]. Results show those scheme are robust against RST with and without cropping. Unfortunately, stronger attacks might requiere weighter watermarks, which usually cause visible distortions into the watermarked images. In [10] the watermark is inserted in previously normalised versions of the images, and restored to the original form before distribution. The scheme is robust against some geometrical distortions, but the detection is prone to errors when the normalisation parameters change due to cropping. The schemes based on invariant or semi-invariant domains are usually vulnerable to severe geometrical distortions, because of the discretisation and interpolation processes required in the insertion/extraction processes.

A newer strategy is to embed the watermarks into marking regions near to invariant features of the images [11,12]. However, watermarking retrieval highly depends on the accuracy of the used algorithms for detecting points resilient to geometrical changes.

In this paper we propose a strategy to provide resilience to RST, which is based on Maximum Correlation Seach (MCS). The detection scheme might be thought of as an image registration problem [1], where the correlation between the original watermark and the input image is maximised, instead of minimising the difference between two images. This strategy avoids the security problems found in schemes based on template insertion and auto-synchronisation. Moreover, results show that even a simple insertion scheme could significatively improve the discretisation problems found in schemes based on LPM.

The paper is organised as follows. Sections 2 and 3 describe the proposed insertion and detection process, respectively. The specifications of the Genetic Algorithm (GA), used during the detection process, is presented in Sect. 3.1. Section 3.2 describes the proposed whitening filter, and some experiments and comparisons of the present approach with a previous scheme are shown in Sect. 4. Finally, some conclusions and future work are discussed in Sect. 5.

## 2 Watermark Embedding Process

Let $f(x, y)$ be the pixel intensity of the original image $f$ at $(x, y)$ location, where $0 \leq y \leq M$ and $0 \leq x \leq N$; $M$ and $N$ denote the total number of rows and columns of the image, respectively. The discrete Fourier magnitude, $|F|$, is assessed and a pseudo-random binary watermark, $W_m(x, y) \in \{-1, 1\}$, the same size of the content image, is generated by preserving the symmetry of the Fourier magnitude. Each coefficient of $|F|$ is modified by,

$$|F'(x, y)| = |F(x, y)|\, e^{1+\alpha W_m(x,y)} \quad , \tag{1}$$

where $\alpha$ is a user-defined strength parameter (usually set to 0.1), that controls the tradeoff between robustness and image fidelity.

By using (1), we avoid modifying the phase component of the image in order to preserve a better visual quality. Finally, the inverse discrete Fourier transform is assessed from $F'$ to obtain the watermarked image $f_w$.

## 3 Watermark Detection Process

Translation attacks are implicitly solved by the well known invariance of the Fourier magnitude [13]. In order to find the rotation angle and scale, we propose a novel detection approach based on a GA that aims to maximise the correlation between the originally inserted watermark, $W_m$, and the Fourier magnitude logarithm of the input image.

Let $\tilde{f}$ be the input image, and $\log|\tilde{F}|$ the logarithm of its Fourier magnitude. A whitening filter [14] (see Sect. 3.2) is applied to $\log|\tilde{F}|$ and $W_m$. Then a searching algorithm, based on a GA (see Sect. 3.1), is used to find the scale factor and rotation angle that maximise the correlation between both filtered signals. Finally, a watermark is reported as successfully detected when the best-found correlation value is higher than a predefined threshold $\tau$.

### 3.1 Genetic Algorithm

Several authors have proposed watermarking schemes where the correlation coefficient is used as a detection measure [15,14]. We propose maximising the correlation between the input image, likely distorted, and the originally inserted watermark, which is computed as,

$$C(\theta,\sigma) = \frac{W_m^T(\theta,\sigma)\ \log|\tilde{F}|}{\log|\tilde{F}|^T\ \log|\tilde{F}|}\ . \tag{2}$$

The goal is to achieve the values of scaling, $\sigma$, and rotation, $\theta$, that might have been applied on the watermarked images by using a MCS based on a GA.

A GA is an evolutive algorithm inspired by a biological process, that attempts to optimise a complex function cost, in such a way that given a random initial population, the GA allows this population to reach a state of maximum fitness in many generations. The general optimisation procedure is: 1) Define a cost function and the chromosome, 2) Create a new population, 3) Evaluate the cost function, 4) Select mates, 5) Mating, 6) Mutate, 7) Check convergence.

Haupt [16] describes those previous steps to minimise a continuous parameters function cost using a GA. In our case, we optimise the function cost, given by (2), which depends on the rotation and the scale parameters. A chromosome $\Phi = [\theta, \sigma]$ is created for each member of the population, where $\theta \in [\theta^{min}, \theta^{max})$ and $\sigma \in [\sigma^{min}, \sigma^{max}]$. Based on the symmetry of the Fourier magnitude we set $\theta^{min} = 0$ and $\theta^{max} = \pi$. In addition, it is well known that scaling in time pro-

duces inverse scaling in the Fourier domain [13], hence we set[1] $\sigma^{min} = \frac{1}{1.7}$ and $\sigma^{max} = \frac{1}{0.6}$.

An initial population, of length $N_{pop}$, is created with chromosomes uniformly distributed over the whole space. In this way, we aim to accelerate the convergence, as we cover the entire space and avoid evaluating the cost of very similar chromosomes in the first generation [16].

Once the first generation is computed, the best half is selected for the paring procedure ($N_{good} = N_{pop}/2$) and the other half is discarded. For paring selection, a weighted probability is computed by using a normalised cost, which is estimated for each chromosome, subtracting the highest cost, of the discarded chromosomes, from the cost of all the chromosomes in the mating pool $C_n = cost_n - cost_{N_{good}+1}$. The probability for each mating chromosome is assessed as,

$$P_n = \left| \frac{C_n}{\sum_{p=1}^{N_{good}} C_p} \right| \ , \tag{3}$$

note that the higher an individual's cost is, the higher is the probability of having offsprings.

Mating generates two offsprings by mixing the chromosomes of the couples previously selected. Let $\boldsymbol{\Phi}^{(m)} = \{\phi_1^{(m)}, \phi_2^{(m)}\}$ and $\boldsymbol{\Phi}^{(p)} = \{\phi_1^{(p)}, \phi_2^{(p)}\}$ denote the parents selected by the paring procedure. One of the two genes is randomly selected, and then exchanged, whereas the other one is mixed, by,

$$\boldsymbol{\Phi}^{(offspring_1)} = \{\phi_1^{(m)}, \phi_2^{(new_1)}\} \ \text{ and } \ \boldsymbol{\Phi}^{(offspring_2)} = \{\phi_1^{(p)}, \phi_2^{(new_2)}\} \ ,$$

where $\phi^{(new_1)} = \phi_2^{(m)} - \beta_1(\phi_2^{(m)} - \phi_2^{(p)})$ and $\phi^{(new_2)} = \phi_2^{(p)} + \beta_2(\phi_2^{(m)} - \phi_2^{(p)})$, and $\beta_i$ is randomly selected between the interval [0, 1].

Finally, for the mutation procedure, a percentage of individuals are randomly selected with uniform probability distribution (with the exception of the best individual, which will not be mutated). Then, the gene $j-th$ (randomly selected) of each selected individual is modified by $\phi_j^{(k)} = (\phi_j^{max} - \phi_j^{min})\beta_3 + \phi_j^{min}$.

### 3.2 Whitening Filter

The correlation measure is an optimum method to detect a signal in Additive White Gaussian Noise (AWGN) channels, but it will be suboptimal in the case of non-AWGN channels. Depovere et al. [14] showed that images might be usually thought of as non-AWGN channels. The authors improved the detection response by applying a simple difference filter, known as *whitening filter*, to the rows of an image in order to remove most of the correlation existing between adjacent pixels. Subsequently, Cox et al. [17] proposed a bidimensional whitening filter (size $11 \times 11$), drawn from an elliptical Gaussian distribution, that significatively improved the detection response achieved by Depovere. We propose using a Separable Bidirectional Difference-Whitening Filter (SBD-WF) that computes

[1] We assume that scaling factors out of this range will likely degrade the image quality.

the horizontal and vertical differences. Thus, we aim to decorrelate pixels through both directions, in contrast with the filter proposed by Depovere. In addition, the SBD-WF filter is separable, which can significatively reduce the required computational cost, in comparison with bidimensional Cox's filter.

## 4 Experimental Results

### 4.1 Whitening Filter Test

A random watermark was embedded into 1000 diverse nature images, by using (1), and then, it is detected without applying any prior distortion. We applied and compare the performance of the following whitening filters: the filter proposed by Cox et al. [17], an horizontal difference filter, a vertical difference filter, and the proposed SBD-WF . Figure 1(a) shows the correlation values obtained by using the four different whitening filters. Note that there is no significant difference among the correlation values obtained from non-watermarked images. In the watermarked images, the obtained results are similar after applying both the vertical and horizontal difference filters. Higher correlation values are achieved by using Cox's filter and the proposed SDB-WF. However, the computation cost of the SBD-WF is lower than the filter proposed by Cox, which requieres a 2D convolution of the image with a $11 \times 11$-size kernel.

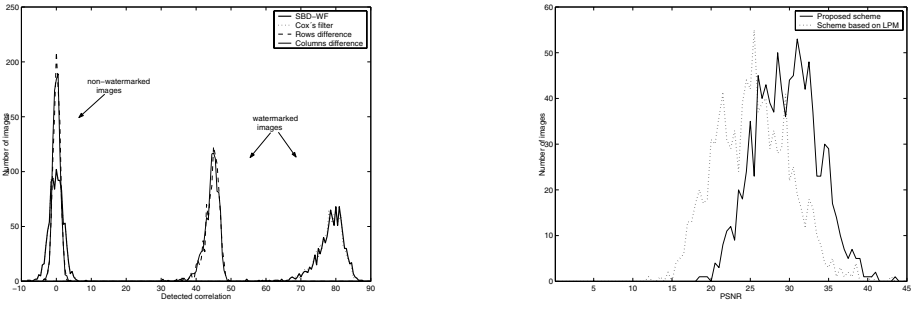


**Fig. 1.** Whitening filter and distortion experiments. (a) Correlation detected from 1000 watermarked and non-watermarked by using different whitening filters. (b) Histograms of PSNR values computed from 1000 watermarked images.

### 4.2 Image Degradation

In order to measure the degradation caused to the watermarked images, 1000 diverse nature test images were watermarked by using the proposed approach (with $\alpha = 0.1$[2]) and Lin's scheme [9]. Figure 1(b) depicts a comparison of the

[2] This is the value used in the experiments discussed in the robustness tests.

Peak Signal-to-Noise Ratio (PSNR) values obtained from the images output by both insertion schemes. Results show that Lin's scheme clearly causes more distortion to the images (lower PSNR values) than the proposed approach.

### 4.3 Robustness

In this section we compare the detection response of Lin's scheme[3] [9] and the proposed approach in images attacked with severe geometrical distortions. We first propose reliable detection thresholds with low false-positive probabilities. Then comparisons between both detection schemes were made.

In this experiment, both detection schemes were applied on 1000 diverse non-watermarked test images. Figures 2(a) and 2(b) show the correlation values detected with the proposed approach and Lin's scheme, respectively. Thus, in order to yield a small false-positive probability, we propose a detection threshold of 9.5 for the proposed scheme and 4.8 for Lin's scheme.

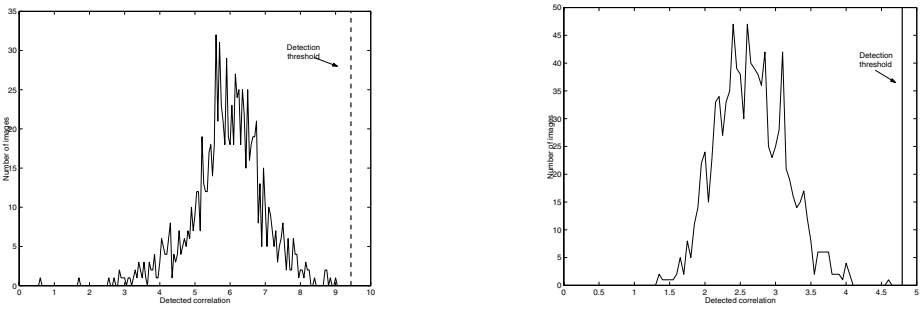


**Fig. 2.** Correlation detected from 1000 non-watermarked images (a) proposed scheme. (b) Lin's scheme.

After defining the detection thresholds, the robustness against strong RST attacks were tested by using the three standard images shown in Figs 3(a)-(c). Figures 3(d)-(e) show the watermarked versions of Lena. Observe that more distortion is perceived when using Lin's scheme. Table 1 shows study cases of the detection responses obtained from both schemes[4], after applying some severe RST attacks on the watermarked test images. Comparatively, the number of faults (printed in bold) detected when using the proposed approach is lower than the faults detected by using Lin's scheme.

Despite the general performance of the proposed scheme is clearly better than Lin's scheme, we think that more robust watermarks and lower impact on human

[3] The original normalised correlation was multiplied by the (constant) watermark magnitude to get higher values.

[4] An initial population of 7,581 was used in our detection scheme, and the reported correlation values required, at most, 15 generations.


**Fig. 3.** Watermarked and non-watermarked images. (a), (b) and (c) Standard test images (Peppers, Lena and Ship). (d) Lena image watermarked with the proposed scheme (e) Lena image watermarked with Lin's scheme.

**Table 1.** Study cases

$\theta$ = rotation angle (grades). $\sigma$ = scale factor.
$T_x$ = horizontal translation. $T_y$ = vertical translation.

| | Tests | | | | Lin's scheme | | | Proposed scheme | | |
|---|---|---|---|---|---|---|---|---|---|---|
| # | $\theta$ | $\sigma$ | $T_x$ | $T_y$ | Peppers | Lena | Ship | Peppers | Lena | Ship |
| 1 | 45.5, | 1.0, | 50.0, | 50.0, | **3.63** | **3.58** | **3.94** | 9.56 | **9.08** | 9.55 |
| 2 | 10.5, | 0.7, | 100.0, | 100.0, | **3.57** | **3.73** | **3.52** | 14.49 | 11.91 | 10.75 |
| 3 | 25.5, | 1.2, | 100.0, | 0.0, | **4.02** | **3.88** | **3.83** | 10.62 | 13.73 | 11.52 |
| 4 | 25.5, | 1.0, | 0.0, | 0.0, | 4.84 | **4.34** | **4.57** | 12.61 | 13.42 | 14.38 |
| 5 | 5.5, | 1.0, | 0.0, | 0.0, | 5.00 | **4.64** | **4.76** | 20.83 | 21.75 | 25.40 |
| 6 | 0.5, | 1.0, | 0.0, | 0.0, | 5.83 | 5.04 | 4.87 | 24.11 | 25.47 | 25.40 |
| 7 | 20.0, | 0.7, | 0.0, | 0.0, | 8.11 | 8.03 | 8.18 | 11.27 | 14.74 | 11.87 |
| 8 | 2.5, | 1.5, | 0.0, | 0.0, | 5.63 | 5.08 | 5.52 | 18.67 | 19.96 | 13.14 |

perception is possible by using an embedding process based on Quantisation Index Modulation (QIM).

## 5 Conclusions

In this paper, a new strategy, based on MCS, is proposed to provide a watermarking scheme resilient to RST. The proposed approach avoid the security problems

found in the schemes basd on auto-synchronisation and template insertion. In addition, comparisons were made to show that even a simple insertion scheme could significatively improve the performance of watermarking schemes based on invariant and semi-invariant domains, such as LPM.

Further research is being done to include an optimised embedding scheme, based on QIM, that will provide stronger watermarks with lower impact in human perception. Additionally, a strong feature extraction algorithm is being designed to provide resilience to local geometrical attacks.

## References


1. Brown, L.G.: A survey of image registration techniques. ACM Computing Surveys **24** (1992) 325–376
2. Fleet, D.J., Heeger, D.J.: Embedding invisible information in color images. In: IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97), Santa Barbara, CA (1997)
3. Pereira, S., Pun, T.: An iterative template matching algorithm using the chirp-z transform for digital image watermarking. Pattern Recognition **33** (2000) 173–175
4. Kutter, M., Hartung, F.: 5. Computer Security Series. In: Introduction to Watermarking Techniques. 1st edn. Artech House (2000) 97–120
5. Deguillaume, F., Voloshynovskiy, S., Pun, T.: A method for the estimation and recovering of general affine transform. US Patent Application (2002)
6. Craver, S., Periig, A., Petitcolas, F.A.P.: 7. Computer Security Series. In: Robustness of copyright marking systems. 1st edn. Artech House (2000) 149–174
7. Herrigel, A., Voloshynovskiy, S., Rytsar, Y.: The watermark template attack (2001)
8. O' Ruanaidh, J.J.K., Pun, T.: Rotation, scale and translation invariant digital image watermarking. In: Proceedings of ICIP 97, IEEE International Conference on Image Processing, Santa Barbara, CA (1997) 536–539
9. Lin, C.Y., Wu, M., Bloom, J.A., Cox, I.J., Miller, M.L., Lui, Y.M.: Rotation, scale, and translation resilient watermarking for images. IEEE Transactions on Image Processing **10** (2001) 767–782
10. Dong, P., Galatsanos, N.P.: Affine transformation resistant watermarking based on image normalization. In: Proceedings of the IEEE International Conference on Image Processing (ICIP-02), Rochester, NY, USA (2002)
11. Feng, Y., Izquierdo, E.: Robust local watermarking on salient image areas. In F.A.P. Petitcolas, H.K., ed.: Digital Watermarking: First International Workshop, IWDW 2002, Seoul, Korea (2002) 180–201
12. Tang, C.W., Hang, H.M.: A feature-based robust digital image watermarking scheme. Signal Processing **51** (2003) 950–959
13. Zelniker, G., Taylor, F.J.: Advanced Digital Signal Processing: Theory and Applications. Marcel Dekker, Inc., New York, NY, USA (1993)
14. Depovere, G., Kalker, T., Linnartz, J.P.M.G.: Improved watermark detection reliability using filtering before correlation. In: ICIP (1). (1998) 430–434
15. Cox, I., Kilian, J., Leighton, T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing **6** (1997) 1673–1687
16. Haupt, R.L., Haupt, S.E.: Practical genetic algorithms. John Wiley & Sons, Inc., New York, NY, USA (1998)
17. Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. 1st edn. Morgan Kaufman (2002)