On the design of template in the autocorrelation domain

Jin S. Seo and Chang D. Yoo

Department of Electrical Engineering and Computer Science
Korea Advanced Institute of Science and Technology
Daejeon 305-701, Korea

ABSTRACT

This paper proposes a methodology in designing a spatial watermark which is robust to geometrical attacks. The proposed watermarking methodology is based on self-registering watermark that tiles the watermark pattern over the entire image. Thus, the peaks in the autocorrelation domain reveals the information about the geometrical transformations which the image has undergone. However, due to the limited precision of the autocorrelation domain, the template search is not reliable enough. The proposed scheme is based on a novel methodology in designing a watermark that is robust to small geometrical attacks. The watermark pattern is designed such that when the synchronization is off by the small amount of geometrical transformations, it can be identified without any searching. This characteristic of the watermark eventually leads to the reduction in search space of the template and compensation for the limited precision of the autocorrelation domain when the synchronization is off by the large amount. The proposed watermark is generated as a filtered white pattern, and in order for the watermark to be robust against geometrical transformation and lossy compression the filter must be carefully designed. The watermark generated by the filter designed by the proposed method has shown improvement in detection reliability.

Keywords: watermark design, geometrical attack, affine transformation, template search, robustness, optimization

1. INTRODUCTION

For the purpose of copyright protection, broadcast monitoring and copy protection of digital data, an imperceptible signal known as watermark is embedded within the digital data before distribution. A watermark should be perceptually transparent, secure against unauthorized users and robust against various attacks. While most of the attacks such as lossy compression, denoising, noise addition, lowpass filtering, reduce watermark energy, geometrical attacks desynchronize the embedded watermark and can mislead the watermark detector.[1] The purpose of this paper is to improve the detection performance of a spatial watermarking scheme against affine transformations such as translation, rotation, scaling and aspect ratio change.

The proposed watermarking methodology is based on self-registering watermark that tiles the watermark pattern over the entire image. The tiled pattern appears as a lattice of peaks, that is called a template, in the autocorrelation domain and careful analysis of both the orientation of the array and the distance between the peaks can reveal the information about the affine transformations which the watermarked image has undergone. The analysis process is called searching.[2–4] A typical watermark detection scheme that uses the template search is shown in Figure 1. If the watermark detection is failed, the template is searched to reveal the affine transformations. According to the template search result, the affine transformations are reversed.

Since the template search is performed in the autocorrelation domain, the peak positions are an integer value and the affine transformation at the sub-integer level is difficult to search without additional processing. Thus it is desirable to design the watermark pattern with a certain degree of correlation so that it can be identified without searching when the synchronization is off by a small amount. This characteristic of the watermark eventually leads to the reduction in search space of the template and compensation for the limited precision

Further author information: (Send correspondence to Jin S. Seo)
Jin S. Seo: E-mail: pobi@eeinfo.kaist.ac.kr and Chang D. Yoo: E-mail: cdyoo@ee.kaist.ac.kr

Security and Watermarking of Multimedia Contents IV, Edward J. Delp III, Ping Wah Wong,
Editors, Proceedings of SPIE Vol. 4675 (2002) © 2002 SPIE · 0277-786X/02/$15.00

of the autocorrelation domain when the synchronization is off by the large amount. The proposed watermark is generated as a filtered white pattern, and in order for the watermark to be robust against geometrical transformation and lossy compression the filter must be carefully designed. The correlation in the designed watermark pattern can be thought of a form of redundancy embedding or error-correcting scheme from the perspective of communication theory.

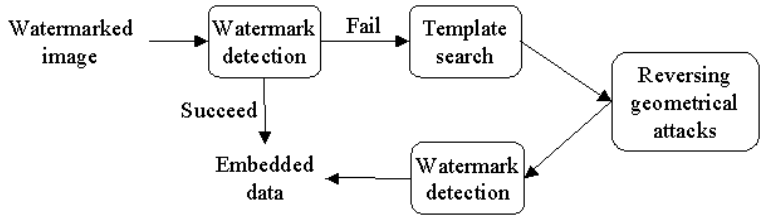


Figure 1: Typical watermark detection scheme with template search

This paper is organized as follows. Section 2 optimizes the watermark pattern to resist small geometrical attacks. Section 3 describes content adaptive watermark embedding and extraction method. Section 4 describes the template peak detection in autocorrelation domain and affine parameter estimation. Section 5 evaluates the performance of the proposed method.

2. OPTIMAL WATERMARK PATTERN GENERATION

The connection between the robustness of the watermark and the watermark pattern itself is generally understood.[5,6] However, few have optimized the connection between the two. This paper proposes a methodology in designing a watermark pattern that is robust to small geometrical attacks and lossy compression. Small geometrical attacks refer to the attacks which include small rotation angle, scaling ratio and translation.

A watermark is generated by passing white pattern through a filter as shown in Figure 2. Thus the design of the watermark pattern becomes an issue of designing a filter with certain requirements. Let the designed watermark and its autocorrelation be w and c, respectively. Then the Fourier transform of c is given by the following relationship.

$$\mathcal{F}(c) = |\mathcal{F}(w)|^2 = |\mathcal{F}(h)|^2 \tag{1}$$

where $\mathcal{F}$ is the Fourier transform and h is the impulse response of the filter. Thus the design of the filter h can be considered as the design of the autocorrelation c. The autocorrelation c should be designed such that the watermark w is robust to small geometrical attacks. The watermark should be also robust against removal attacks such as lossy compression which can be generally considered as highpass filter, and thus for a more robust watermark the watermark pattern should avoid the high frequency range. The watermark should also avoid the low frequency range in order to minimize the image interference so that it can be easily detected. For these reasons the optimization should be based on the objective that the energy in the mid frequency range is maximized while the watermark has proper correlation characteristics so that it is less sensitive to synchronization.

Figure 2: Watermark generation with the designed filter

Let the autocorrelation of watermark $c[m,n]$ have a support in a $(2N+1)$ by $(2N+1)$ square defined by $-N \leq m,n \leq N$. Then the frequency response of the autocorrelation (spectrum of watermark) is given as

follows.

$$C(\omega_x, \omega_y) = \sum_{m=-N}^{N} \sum_{n=-N}^{N} c[m,n] \exp(-j(m\omega_x + n\omega_y)). \tag{2}$$

If the autocorrelation $c[m,n]$ is symmetric, i.e. $c[m,n] = c[-m,-n]$, $c[m,n] = c[m,-n]$, then the frequency response of the autocorrelation can be written as follows.

$$\begin{aligned} C(\omega_x, \omega_y) &= c[0,0] + \sum_{m=1}^{N} 2c[m,0]\cos(m\omega_x) + \sum_{n=1}^{N} 2c[0,n]\cos(n\omega_y) \\ &+ \sum_{m=1}^{N}\sum_{n=1}^{N} 2c[m,n]\cos(m\omega_x + n\omega_y) \\ &+ \sum_{m=1}^{N}\sum_{n=1}^{N} 2c[m,-n]\cos(m\omega_x - n\omega_y) \\ &= c[0,0] + \sum_{m=1}^{N} 2c[m,0]\cos(m\omega_x) + \sum_{n=1}^{N} 2c[0,n]\cos(n\omega_y) \\ &+ \sum_{m=1}^{N}\sum_{n=1}^{N} 2c[m,n]\{\cos(m\omega_x + n\omega_y) + \cos(m\omega_x - n\omega_y)\}. \end{aligned} \tag{3}$$

From the requirements on the autocorrelation and frequency domain, we deduce the following optimization problem. The measure for the energy contained in the frequency band of watermark can be calculated by using a dense grid of frequency bins $\{(\omega_{0x}, \omega_{0y}), (\omega_{1x}, \omega_{1y}), (\omega_{2x}, \omega_{2y}), (\omega_{3x}, \omega_{3y}), \cdots, (\omega_{Mx}, \omega_{My})\}$ covering the whole frequency range. Assume the mid-frequency band of interest to be between ω_{in} and ω_{out}, the average energies at three bands (low-frequency, mid-frequency and high-frequency band) ζ_{in}, ζ_m and ζ_{out} are respectively given by

$$\zeta_{in} = E[C(\omega_{kx}, \omega_{ky})] \text{ for } \sqrt{\omega_{kx}^2 + \omega_{ky}^2} \le \omega_{in} \tag{4}$$

$$\zeta_m = E[C(\omega_{kx}, \omega_{ky})] \text{ for } \omega_{in} < \sqrt{\omega_{kx}^2 + \omega_{ky}^2} < \omega_{out} \tag{5}$$

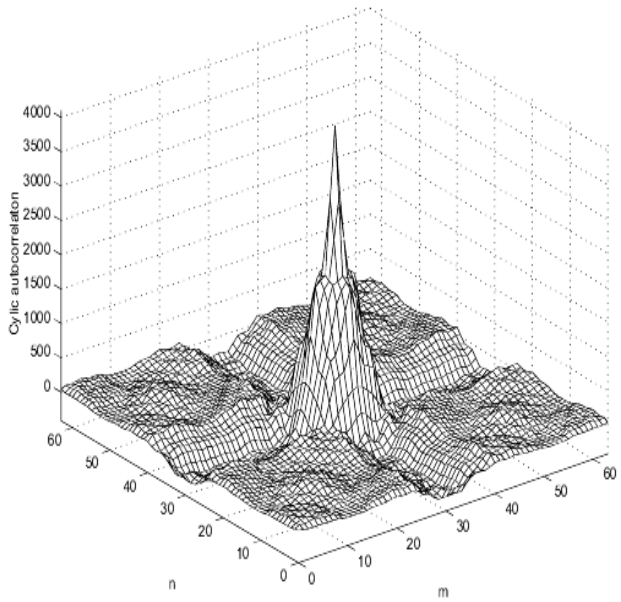
$$\zeta_{out} = E[C(\omega_{kx}, \omega_{ky})] \text{ for } \omega_{out} \le \sqrt{\omega_{kx}^2 + \omega_{ky}^2} \tag{6}$$

The optimization wants to maximize ζ_m while suppressing ζ_{in} and ζ_{out}. At the same time the spectrum $C(\omega_x, \omega_y)$ must be non-negative and the correlation around the origin must be slowly decaying (reducing the sensitivity to synchronization). The above can be summarized into the following optimization problem :

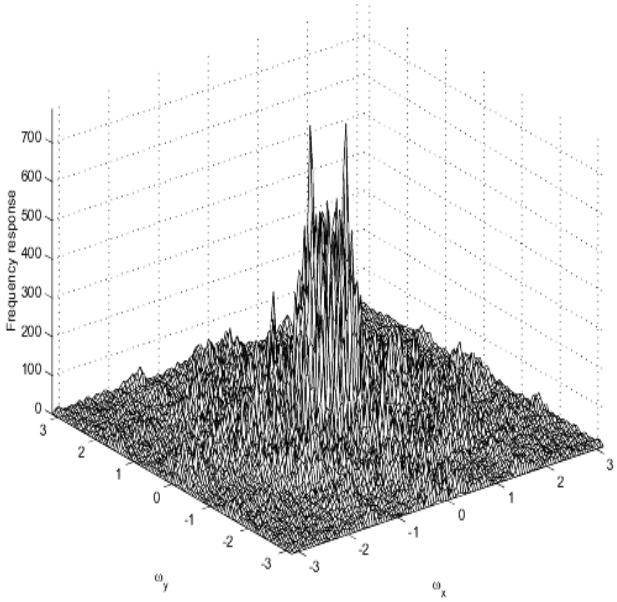
$$\max_{c} \ \zeta_m - \alpha_{in}\zeta_{in} - \alpha_{out}\zeta_{out} \tag{7}$$

$$\text{subject to} \quad \begin{array}{ll} C(\omega_{kx}, \omega_{ky}) \ge \alpha_m \zeta_{in} & \text{for } \omega_{in} < \sqrt{\omega_{kx}^2 + \omega_{ky}^2} < \omega_{out} \\ C(\omega_{kx}, \omega_{ky}) \ge 0 & \text{for all the frequency bins} \\ \alpha_h \le c[m,n] \le 1, & \text{for } \sqrt{m^2+n^2} \le R \\ -\alpha_l \le c[m,n] < \alpha_h, & \text{for } \sqrt{m^2+n^2} > R \end{array} \tag{8}$$

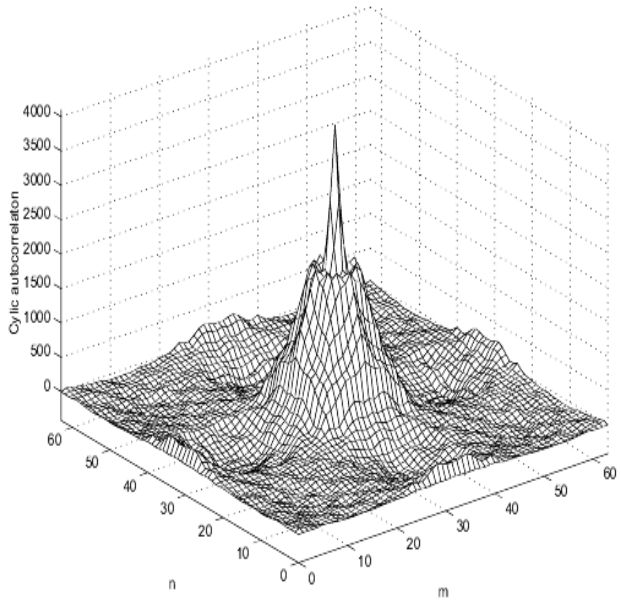
where R represents how much the watermark is robust to the small geometrical attacks. The solution of the above optimization problem can be obtained using a constrained optimization for the sufficiently large frequency bins. The number of frequency bins we used in the optimization was 841. The autocorrelation and frequency response of the optimized watermark pattern is shown in Figure 3 for $R = 3$ and $R = 5$ cases. The parameters we used in the optimization are $\omega_{in} = 0.4\pi$, $\omega_{out} = 0.7\pi$, $N = 32$, $\alpha_{in} = 1$, $\alpha_{out} = 3.5$, $\alpha_m = 0.15$, $\alpha_h = 0.5$ and $\alpha_l = 0.1$.



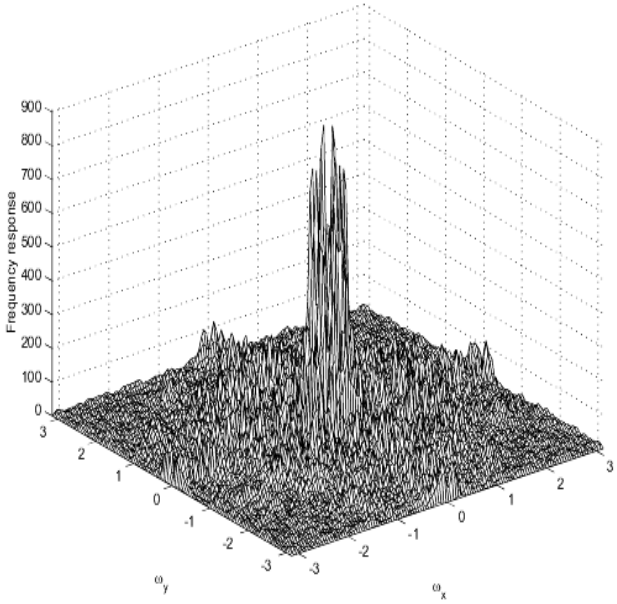
(a) Autocorrelation of the watermark $R = 3$



(b) Frequency response of the watermark $R = 3$



(c) Autocorrelation of the watermark $R = 5$



(d) Frequency response of the watermark $R = 5$

Figure 3: The autocorrelation and frequency magnitude response of the optimized watermark pattern

3. CONTENT ADAPTIVE WATERMARK EMBEDDING AND EXTRACTION

The embedding method should be content adaptive so that the watermark is kept imperceptible while embedding maximum amount of watermark energy for the best possible detection performance. In order to determine the amount of watermark energy that is possible for embedding while being imperceptible, the noise visibility $s(i,j)$ is evaluated.[7] It is given by

$$s(i,j) = \frac{1}{1+\beta\sigma_x^2(i,j)} \tag{9}$$

where $\sigma_x(i,j)$ is the local variance (3x3 or 5x5 block) of the image at (i,j) and β is a constant that depends on the local characteristics of the image ($\beta = 1, 2, 3.5$ for the smooth, edge and texture regions respectively). It is a visibility measure of noise which in this case is the watermark. The amount of watermark that can be embedded with transparency would be inversely proportional to the noise visibility. Using $s(i,j)$, watermark $w(i,j)$ is embedded into the image $x(i,j)$ at pixel (i,j) additively by

$$y(i,j) = x(i,j) + \alpha_1(1-s(i,j))w(i,j) + \alpha_2 s(i,j)w(i,j) \tag{10}$$

where α_1 and α_2 is the global scaling factor.[7]

The extraction method should minimize the watermark impair while suppressing the cover interference. To extract the watermark signal w from the watermarked image, we solve the optimization problem. The objective of the optimization is the minimization of the watermark impair, and the constraint is the suppression of the cover interference. This problem is similar to the signal enhancement problem in noisy speech[8] and image.[9] Let the $\hat{w} = Pz$ be the estimated watermark in each pixel where $z = y - \bar{y}$ and $\bar{y}$ is the local mean. The desired linear estimator P is chosen to minimize the square error of the estimator. The difference between the original watermark and estimated watermark is given by

$$\begin{aligned} r(i,j) &= \hat{w}(i,j) - w(i,j) \\ &= P(x(i,j) - \bar{x}(i,j)) + [\alpha_1 P(1-s(i,j)) + \alpha_2 P s(i,j) - 1]w(i,j) \\ &\triangleq r_x + r_w \end{aligned} \tag{11}$$

where $\bar{x}(i,j)$ is the mean of the block centered at (i,j). The energy of the residual image interference r_x is given by

$$\bar{\epsilon}_x^2 \triangleq E[r_x^2] = P^2\sigma_x^2(i,j). \tag{12}$$

The energy of the watermark estimation error r_w is given by

$$\bar{\epsilon}_w^2 \triangleq E[r_w^2] = [\alpha_1 P(1-s(i,j)) + \alpha_2 P s(i,j) - 1]^2\sigma_w^2 \tag{13}$$

where the variance of watermark signal is σ_w^2. Then the linear estimator P is obtained from the following optimization problem.

$$\begin{aligned} &\min_P \epsilon_w^2 \\ &\text{subject to } \epsilon_x^2 \le \gamma\sigma_x^2. \end{aligned} \tag{14}$$

The solution to above problem can be obtained by introducing a Lagrange multiplier μ, and minimize the unconstrained objective function

$$L(P,\mu) = \bar{\epsilon}_w^2 + \mu(\bar{\epsilon}_x^2 - \gamma\sigma_x^2) \tag{15}$$

The stationary feasible point of P can be found by solving the gradient of $L(P,\mu)$ and $\bar{\epsilon}_x^2 = \gamma\sigma_x^2$. We obtain the following solution.

$$P(i,j) = \frac{[\alpha_1(1-s(i,j)) + \alpha_2 s(i,j)]\sigma_w^2}{[\alpha_1(1-s(i,j)) + \alpha_2 s(i,j)]^2\sigma_w^2 + \mu\sigma_x^2} \tag{16}$$

where $\mu \approx \frac{\alpha_1(1-s(i,j))+\alpha_2 s(i,j)}{\sigma_x}$ to normalize $\bar{\epsilon}_x^2 = \gamma\sigma_x^2 = 1$. It means that the Lagrange multiplier μ is related to the watermark-to-noise ratio.

4. AFFINE PARAMETER ESTIMATION

The search operation to determine the affine transformations which the image has undergone can be performed in the autocorrelation domain. It is based on the fact that the tiled watermark pattern appears in the autocorrelation domain as a lattice of peaks. Since part of peaks may not be detected due to image interference or intentional deletion,[10] reliable parameter estimation is important. Thus we use likelihood method.

In order to reverse the affine transformations, three parameters must be estimated from the autocorrelation of the watermarked image: the angle of rotation which the watermarked image has undergone, the periods of the peaks in both horizontal and vertical directions. After finding peaks as a local maximum in the autocorrelation domain, the Radon transform is evaluated for various angles θ, and the angle that produces the maximum number of peaks is determined to be the rotation angle. For the determined angle, the periods are estimated using the maximum likelihood estimator given by

$$T_{ML} = \arg\max_{T} \left| \sum_{j=1}^{N} e^{2\pi i \frac{t_j}{T}} \right| \tag{17}$$

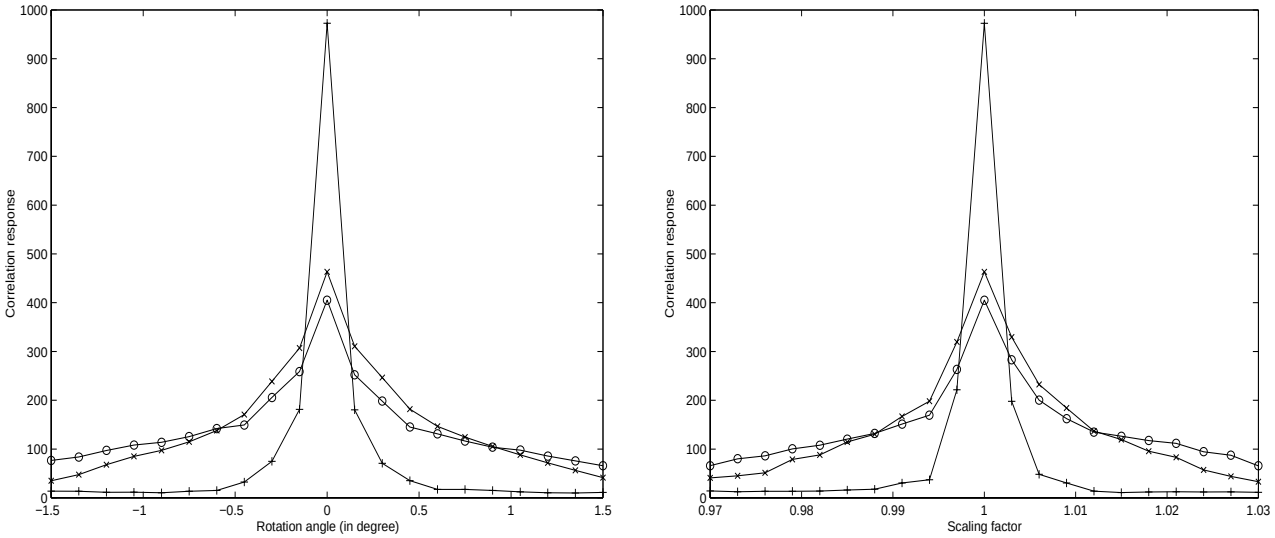
where t_j is the position of the j-th peak in the estimated direction.[11] However, finding peaks in the autocorrelation domain is vulnerable to image interference and compression, thus the maximum likelihood estimation of rotation angle and periods are not sufficiently accurate. We must consider more cases which give high likelihood to improve watermark detection probability.

5. EXPERIMENTAL RESULTS

The performance of the proposed scheme for watermark embedding and detection was evaluated using the 512 by 512 Lena image. The robustness against geometrical attacks was evaluated using the patterns with three different values of correlation parameter $R = 0, 3, 5$. Throughout the evaluation, the 64 by 64 sized watermark pattern was used and the PSNR of the watermarked image was kept constant to 38 dB. With increasing correlation (controlled by the increasing R), the visibility of the watermark is proportionally increased. This phenomenon is especially more noticeable for smooth background. The visibility of the watermark can be adjusted with the parameter α_2 (see Equation 10). In the watermark detection, the tiled watermark is folded to accumulate the watermark power.[12] Then the cross correlation detection of the watermark is performed. The simple linear addition of the tiled watermark pattern was used. Recently various other methods of accumulation have been studied from the perspective of the diversity detection [13,14]; however, these were not used in this experiments.

To evaluate the proposed scheme for small geometrical transformations involving rotation and scaling, the correlation outputs versus rotation angle and scaling factor are obtained without template search. This is shown in Figure 4, and it is noticed that with increasing R the sensitivity to geometrical attacks is proportionally reduced. We also find out the precision of the template search required to detect the watermark from this figure. The watermark without optimization ($R = 0$ case) must have the precision smaller than 0.2 degree of rotation angle and 0.005 of scaling ratio, while the optimized watermarks ($R = 3$ and $R = 5$ cases) require precision in the order of $0.5 \sim 1$ degree of rotation angle and $0.01 \sim 0.02$ of scaling ratio. Thus the complexity of template search can be significantly reduced by the reduced search space.

To compare the detection reliability of the three cases against random affine transformations, we generated twenty images which are randomly rotated and scaled after JPEG compression. Table 1 shows the probability of correct watermark detection after template search with the precision of 0.5 degree of rotation angle and $\frac{1}{64}$ of scaling ratio. We estimated the rotation angle and scaling factor as stated in section 4. The result in Table 1 shows the optimized watermark improves the probability of correct watermark detection. The table also shows the optimized watermark is robust to JPEG compression. This can be attributed to the fact that the watermark design process emphasizes the mid frequency band as stated in section 2.



(a) Correlation response versus rotation angle (b) Correlation response versus scaling factor

Figure 4: Robustness of the watermark against the small geometrical attacks for $R = 0$ (+), $R = 3$ ($\times$), $R = 5$ ($\circ$)

JPEG Quality factor	$R = 0$ case	$R = 3$ case	$R = 5$ case
90 %	40	85	95
80 %	25	70	85
70 %	0	55	70
60 %	0	50	50

Table 1. The probability (%) of correct watermark detection after JPEG compression and randomly chosen affine transforms

6. SUMMARY

This paper showed that the detection reliability against geometrical attacks can be significantly improved by using the optimally designed watermark pattern. The watermark pattern is designed such that when the synchronization is off by the small amount of geometrical transformations, it can be identified without any searching. This characteristic of the watermark eventually leads to the reduction in search space of the template and compensation for the limited precision of the autocorrelation domain when the synchronization is off by the large amount. The proposed watermark is generated as a filtered white pattern, and the filter is designed optimally for the watermark to be robust against geometrical attacks and lossy compression. It has been experimentally verified that the proposed watermark design methodology improves the probability of correct watermark detection for lossy compression and various affine transformations.

REFERENCES

1. S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modeling: towards a second generation watermarking benchmark," *Signal Processing* **81**, pp. 1177–1214, 2001.
2. M. Kutter, "Watermarking resisting to translation, rotation and scaling," in *Int. Symp. on Voice, Video, and Data communication*, *Proc. SPIE* **3528**, 1998.
3. C. W. Honsiner and S. J. Daly, "Method for detecting rotation and magnification in images," *US patent 5835639* , 1998.
4. P.-C. Su and C.-C. J. Kuo, "Synchronized detection of the block-based watermark with invisible grid embedding," in *Security and Watermarking of Multimedia Contents III*, W. Wong and E. J. Delp, eds., *Proc. SPIE* **4314**, 2001.

5. J.-P. M. Linnartz, T. Kalker, G. F. Depovere, and R. Beuker, "A reliability model for the detection of electronic watermarks in digital images," *Proc. IEEE Fifth Symposium on Communications and Vehicular Technology*, 1997.
6. I. Cox and J.-P. M. Linnartz, "Public watermarks and resistance to tampering," *Proc. IEEE Int. Conf. on Image Processing (ICIP 97)*, 1997.
7. S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Int. Workshop on Information Hiding*, *Springer Verlag* **LNCS 1768**, 1999.
8. Y. Ephraim and H. L. V. Trees, "A signal subspace approach for speech enhancement," *IEEE Transactions on Speech and Audio processing* **3**, pp. 251–266, 1995.
9. J. S. Lim, *Two-Dimensional Signal and Image Processing*, Prentice Hall, 1990.
10. A. Herrigel, S. Voloshynovskiy, and Y. Rytsar, "The watermark template attack," in *Security and Watermarking of Multimedia Contents III*, W. Wong and E. J. Delp, eds., *Proc. SPIE* **4314**, 2001.
11. B. M. Sadler and S. D. Casey, "On periodic pulse interval analysis with outliers and missing observations," *IEEE Transactions on Signal Processing* **46**, pp. 2990–3001, 1998.
12. M. Maes, T. Kalker, J.-P. M. Linnartz, J. Talstra, G. F. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protection," *IEEE Signal Processing Magazine* **17**, pp. 47–57, 2000.
13. D. Kundur and D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking," *IEEE Transactions on Signal Processing* **29**, pp. 2383–2396, 2001.
14. S. Voloshynovskiy, F. Deguillaume, S. Pereira, and T. Pun, "Optimal adaptive diversity watermarking with channel state estimation," in *Security and Watermarking of Multimedia Contents III*, W. Wong and E. J. Delp, eds., *Proc. SPIE* **4314**, 2001.