

# Mobile Watermarking against Geometrical Distortions

Jing Zhang

School of Electronic Information Engineering  
Tianjin University  
Tianjin,300072,P.R. China  
zhangjing@tju.edu.cn

Yuting Su

School of Electronic Information Engineering  
Tianjin University  
Tianjin,300072, P.R.China  
ytsu@tju.edu.cn

Meili Zhi

School of Electronic Information Engineering  
Tianjin University  
Tianjin,300072, P.R.China  
zhiml@139.com

Qingzhong Liu

Department of Computer Science  
Sam Houston State University  
Huntsville, TX 77341, U.S.A.  
liu@shsu.edu

## ABSTRACT

Mobile watermarking robust to geometrical distortions is still a great challenge. In mobile watermarking, efficient computation is necessary because mobile devices have very limited resources due to power consumption. In this paper, we propose a low-complexity geometrically resilient watermarking approach based on the optimal tradeoff circular harmonic function (OTCHF) correlation filter and the minimum average correlation energy Mellin radial harmonic (MACE-MRH) correlation filter. By the rotation, translation and scale tolerance properties of the two kinds of filter, the proposed watermark detector can be robust to geometrical attacks. The embedded watermark is weighted by a perceptual mask which matches very well with the properties of the human visual system. Before correlation, a whitening process is utilized to improve watermark detection reliability. Experimental results demonstrate that the proposed watermarking approach is computationally efficient and robust to geometrical distortions.

## Categories and Subject Descriptors

K.4.1 [Computers and Society]: Public Policy Issues – *Intellectual property rights, Abuse and crime involving computers, Privacy.*

## General Terms

Algorithms

## Keywords

Geometrical Distortion; Mobile Watermarking; OTCHF Correlation Filter; MACE-MRH Correlation Filter; Perceptual Mask; Whitening.

## 1. INTRODUCTION

Digital watermarking is a process of embedding a hidden signal, *i.e.*, the watermark, into digital multimedia so that the information can be detected for a variety of purposes including copyright protection and digital right management. The requirement of digital watermark surviving geometrical transformations is necessary since such manipulations as global rotation, scaling and translation (RST) transforms are common. Nevertheless, these procedures cause challenging synchronization problems for watermark detection. Special care has to be taken so that the embedded watermark can survive such attacks to achieve the related functionalities in the target application.

Existing methods against geometrical transformations can be classified into the following four types.

### 1) Exhaustive search watermarking

Exhaustive search is a feasible solution if a known hidden signal is the searched target [1], [2]. One challenge is to determine all the possible geometrical distortions in advance. The other challenge is to reduce the computational load. Usually, the searching process should be coupled with certain side information to reduce the computational load.

### 2) Template-based watermarking [3]–[6]

Employing synchronization templates may be a more flexible approach. The template is usually the repeated structure or tiling of signals that will help to reflect the distortion or manipulation applied on the image. The watermark detector can reverse the geometrical operation according to the extracted template for the watermark detection. However, the so-called “template attack” [7] may detect and remove the repeatedly embedded template signal to cause problems for the watermark detection.

### 3) Invariant domain watermarking

In [8], [9], Fourier-Mellin transform based watermarking was proposed by utilizing geometric invariant property of Fourier-Mellin transform. In [10], watermarking in a new feature transform named local daisy feature transform (LDFT) was proposed. Geometrically robust image watermarking using moment invariants was introduced by Alghoneimy and Tewfik [11]. Since then, numerous invariant watermarking schemes have been designed using different moment families such as complex moments [12], wavelet moments [13], Zernike and pseudo-Zernike moments (ZMs/PZMs) [14–18]. Invariant domain watermarking usually suffers from high computational complexity and poor reconstruction quality because of non-linear nature of the invariants.

#### 4) Feature-based watermarking

Recently, the feature-based watermarking have gained more and more attention [19]–[28]. The basic idea of these approaches is resorting to such feature or interest point extraction as Harris corner detection or Scale-Invariant Feature Transform (SIFT), *etc.* to determine the interest areas, which are then transformed into the regions with known shape, size and orientation for the subsequent watermark embedding and detection. Since the interest points are extracted according to the content, the same areas may be identified in both the watermark embedder and detector. But there are usually a lot of feature points in an image found by the interest point extraction algorithms. The watermark embedder and detector have to choose the same points for further processing, which is not a trivial issue.

During the past ten years, mobile devices such as cell phones, PDAs, and music players have become ubiquitous. The use of watermarking for the protection of digital media rights on these devices is becoming more and more important. However, geometrically resilient watermarking algorithms have been designed with little or no consideration for these system constraints such as computational complexity and energy availability.

In [29], a low-complexity watermarking scheme is proposed for mobile devices. The minimum average correlation energy Mellin radial harmonic (MACE-MRH) correlation filter [30] is used for watermark detection. By the scale tolerance property of the correlation filter, the watermark detector can be robust to scaling attacks. It is computationally expensive to generate the MACE-MRH correlation filter. However, the filter can be designed off-line and only one generation is needed during the watermark detection. Once the filter is generated, it only requires a calculation of cross correlation. Enlightened by this scheme, in this paper, we propose a low-complexity geometrically resilient watermarking approach based on the optimal tradeoff circular harmonic function (OTCHF) correlation filter [31] and the MACE-MRH correlation filter. The watermark is embedded into the image spatial domain with a perceptual mask which allows for a significantly increased strength of the watermark as well as remaining its good imperceptibility. Watermark detection accuracy can be further improved by a whitening process before correlation. Experimental results show the feasibility of the proposed approach.

The rest of this paper is organized as follows. In Section 2, we present the proposed watermarking approach, including the scheme diagram, design theory and technique details. Experimental results are shown in Section 3. Finally, we conclude our work in Section 4.

## 2. THE PROPOSED WATERMARKING APPROACH

### 2.1 Problem Formulation

Let  $I$  be a cover image and  $W$  the watermark, which is a Gaussian distributed pseudorandom pattern with zero mean and variance  $\delta_w^2$ . The watermark is of the same size (and uncorrelated) with the cover image. The watermarked image  $I'$  in the most simple case, where the image content is not taken into account (i.e., no perceptual masking is used), can be written as

$$I' = I + W \quad (1)$$

Usually, the blind watermark detection procedure employs a similarity measure based on the correlations between the watermark and the received image. To decide whether an image  $Z$  contains the watermark  $W$  or not, the correlation between the image  $Z$  and the watermark  $W$ , in particular, defined as

$$\rho(Z, W) = \frac{1}{N} \sum_{n=1}^N z_n w_n \quad (2)$$

is used as a measure of the watermark presence.

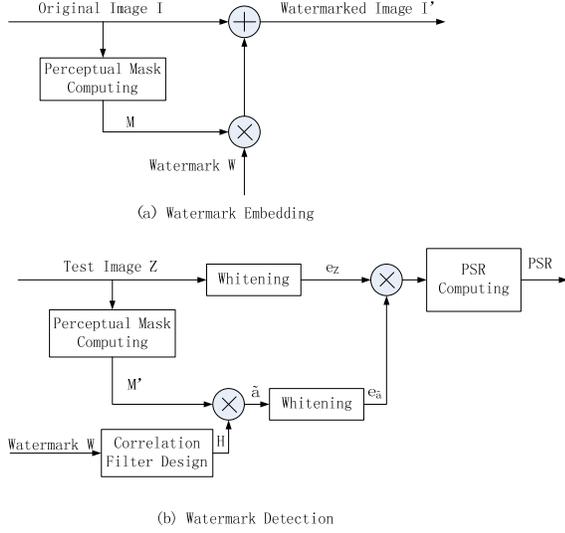
From detection theory it follows that correlation detectors are optimum in the case of a linear time-invariant, frequency non-dispersive, Additive White Gaussian Noise (AWGN) channel. However, this is not the case for real images where the pixels are correlated. In order to resist attacks, many improvements have been made both in watermark embedding and watermark detection. One important development is the application of perceptual masking, such as human visual system models, to the watermark embedding process. These perceptual models allow watermark signals to be added to a source with maximum efficiency. Another area of improvement has been in the development of filters for use prior to watermark detection. In the case of non-white Gaussian noise, it is possible to achieve optimum detection by applying a so-called *whitening filter* at the input of the correlation receiver [32]. Such a filter is designed to suppress the host image and thereby boost the watermark to host signal ratio. Equivalently, this amounts to estimating the host image and subtracting it from the watermarked image under study. The watermark signal has to be filtered in the same way before correlation.

### 2.2 The Diagram of the Proposed Watermarking Scheme

In our proposed watermarking approach, both perceptual masking and whitening are utilized to improve watermark performance. Figure 1 illustrates the diagram of the proposed watermarking scheme.

In the watermark embedding, the perceptual mask  $M$  is computed according to the input image  $I$ , then the masked watermark is generated by  $a = M \bullet W$ , where  $\bullet$  stands for pointwise multiplication. The strength of the watermark (i.e., its standard deviation) is incorporated into  $W$ . The masked watermark  $a$  is a zero mean white process. It depends on  $I$  (via  $M$ ), but is uncorrelated with  $I$  because  $M$  has zero mean. The watermarked image  $I'$  can be written as

$$I' = I + M \bullet W \quad (3)$$



**Figure 1. The diagram of the proposed scheme**

In the watermark detection, Similar to the embedding procedure, the perceptual mask  $M'$  is computed according to the input test image  $Z$ .  $Z$  is whitened before correlation. A specific correlation filter  $H$  (either OTCHF filter or MACE-MRH filter) is designed with the watermark  $W$  as the reference pattern. The correlation filter can provide a user-specified response to in-plane rotation or scale distortion. Thus the watermark detection based on correlation is robust to the specified rotation or scale distortion. The strength of the watermark is incorporated into  $H$  by  $\tilde{a} = M' \bullet H$ . The signal  $\tilde{a}$ , we call it geometrically resilient watermark, is also whitened before correlation. The correlation between the whitened  $Z$  (i.e.,  $e_z$ ) and the whitened  $\tilde{a}$  (i.e.,  $e_{\tilde{a}}$ ) is computed and the peak-to-sidelobe ratio (PSR) is calculated. To determine whether the image  $Z$  contains  $W$  or not, PSR is compared to a predefined threshold  $T_p$ . If it is lower than  $T_p$ , then the decoder decides that  $Z$  does not contain  $W$ , whereas if it is above the threshold, the decoder assumes  $Z$  is marked with  $W$ .

Next, we will detail each step of the design.

### 2.3 Perceptual Masking and Whitening

In our proposed watermarking scheme, the whitening filter is used to estimate the cover image and subtract it from the watermarked image. The estimation of the cover image corresponds to the image denoising problem [33]. When a mask is designed so as to make the embedded watermark resistant against denoising, the way a denoising filter acts on an image should be taken into account. It is well known that the denoising filter mainly affects the high-frequency part of the image (a fact that should be taken into account during watermark embedding), therefore we would like to amplify the watermark in the high frequencies, which correspond to textured image areas and edges, in order to make a watermark robust to the denoising attack. This strategy matches the properties of the human visual system (HVS), since noise is less noticeable in such areas. So, our design is concentrated on finding a proper perceptual mask to compensate for denoising.

In this paper, the denoising attack is assumed to be performed using the adaptive least-squares (LS) prediction error filter. The

improvement of the prediction relates to more accurate estimation of the cover image, thus it is important for watermark detection [34]. Since image statistics change from one region to another, a straightforward idea is to use multiple local predictors instead of a single global predictor. Thus, one can split the image into blocks and compute a distinct LS predictor for each block. The smaller the blocks, the better the prediction. We focus on linear predictors. By linear prediction, image pixels  $x_{i,j}$  are estimated by a weighted sum over a certain neighborhood of  $x_{i,j}$ . In order to simplify the notations, we consider an indexing of the neighborhood (prediction context),  $p = 1, \dots, k$ , namely  $x_{i,j,\dots,i,j}^p$ , where  $k$  is the order of the predictor. Let  $V = [v_1, \dots, v_k]^T$  be the column vector with the coefficients of the predictor. The predicted pixel  $\hat{x}_{i,j}$  can be written as:

$$\hat{x}_{i,j} = v_0 + \sum_{p=1}^k v_p x_{i,j}^p \quad (4)$$

Let  $\mathbf{x}_{i,j}$  be the row vector obtained by ordering the context of  $x_{i,j}$  according to the indexing. Because the constant term is used, the vector  $\mathbf{x}_{i,j}$  is extended by adding a first element,  $x_0=1$ . The predicted pixel  $\hat{x}_{i,j}$  can then be written in closed form as

$$\hat{x}_{i,j} = \mathbf{X}V$$

The predicted value and the prediction error depend on  $\mathbf{v}$ . We shall further write  $x_{i,j}(\mathbf{v})$  and  $e_{i,j}(\mathbf{v})$ .

The LS predictor is the one that provides:

$$\min_{\mathbf{v}} \sum_i \sum_j e_{i,j}(\mathbf{v})^2 \quad (5)$$

Let  $\mathbf{y}$  be the column vector obtained by scanning the image along the rows and let  $\mathbf{X}$  be the matrix whose rows are the corresponding context vectors as defined above. The prediction error vector is  $\mathbf{y} - \mathbf{X}\mathbf{v}$ . Equation (5) corresponds to the minimization of  $(\mathbf{y} - \mathbf{X}\mathbf{v})^T (\mathbf{y} - \mathbf{X}\mathbf{v})$ , where “ $T$ ” denotes vector/matrix transposition. By taking the partial derivatives of the square error with respect to the components of  $\mathbf{v}$  and by setting them equal to zero one gets  $\mathbf{X}\mathbf{X}^T \mathbf{v} = \mathbf{X}^T \mathbf{y}$  and, finally

$$\mathbf{V} = (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \mathbf{Y} \quad (6)$$

Our proposed perceptual mask is a normalized version of the prediction error magnitude, which is defined as:

$$M(i, j) = \frac{|e_x(i, j)|}{\max_x |e_x(i, j)|} \quad (7)$$

### 2.4 Correlation Filter Design

The proposed watermark detection scheme consists of three steps. In the first step, similar to the embedding procedure, the perceptual mask  $M'$  is computed according to the input test image  $Z$ . In the second step, the correlation filter  $H$  is designed with the watermark as the reference image. We utilize two kinds of correlation filter: OTCHF filter and MACE-MRH filter. The design theory is described as follows.

#### 2.4.1 OTCHF Filter

Let  $\hat{f}(x, y)$  denote the reference image with its 2-D Fourier transform (FT) denoted by  $\hat{F}(u, v)$ . By transforming the Cartesian frequencies to polar frequencies, we obtain  $F(\rho, \phi)$ . We can use a Fourier series expansion in  $\phi$  as follows:

$$\begin{aligned}
F(\rho, \phi) &= \sum_k F_k(\rho) e^{jk\phi} \\
F_k(\rho) &= \frac{1}{2\pi} \int_0^{2\pi} F(\rho, \phi) e^{-jk\phi} d\phi \\
(8)
\end{aligned}$$

where  $F_k(\rho)$  is the  $k$ th circular harmonic function (CHF) of  $\hat{F}(u, v)$ .

Let  $\hat{H}(u, v)$  denote the correlation filter in Cartesian frequencies. Its polar coordinate transformed version also lends itself to a CHF decomposition as follows:

$$\begin{aligned}
H(\rho, \phi) &= \sum_k H_k(\rho) e^{jk\phi} \\
H_k(\rho) &= \frac{1}{2\pi} \int_0^{2\pi} H(\rho, \phi) e^{-jk\phi} d\phi \\
(9)
\end{aligned}$$

Let  $c$  denote the correlation value at the origin (from now on referred to as the correlation output or correlation peak) when the input is  $\hat{f}(x, y)$  and the correlation filter is  $\hat{H}(u, v)$ . Using (8) and (9), we obtain the following expression for the correlation peak in terms of the filter and the input CHF's:

$$c = \int_0^{2\pi} d\phi \int_0^{\infty} \rho d\rho F(\rho, \phi) H^*(\rho, \phi) \quad (10)$$

The simpler expression for the correlation output is:

$$c = \sum_{k=-\infty}^{\infty} C_k, \quad C_k = 2\pi \int_0^{\infty} F_k(\rho) H_k^*(\rho) \rho d\rho \quad (11)$$

An input image rotation results in  $\hat{F}(u, v)$  being rotated by angle  $\theta$  leading to  $F(\rho, \phi + \theta)$ . From (8), the CHF's of the FT of this rotated target image are then given by  $F_k(\rho) e^{jk\phi}$ . Since the filter is unchanged, its circular harmonics do not change and the correlation output as a function of input in-plane rotation is given as follows:

$$c(\theta) = \sum_{k=-\infty}^{\infty} C_k e^{jk\theta} \quad (12)$$

Similarly, if a FIR filter has discrete-time impulse response  $a[n]$ , then its frequency response  $A(\omega)$  is given as follows:

$$A(\omega) = \sum_n a[n] e^{jn\omega} \quad (13)$$

Thus, the problem of determining the  $C_k$  to approximate a specified  $c(\theta)$  is equivalent to the FIR filter design problem of finding  $a[n]$  to yield a good approximation to a specified  $A(\omega)$ .

Once the CHF weights  $C_k$  are determined, the next task is to find the filter CHF's  $H_k(\rho)$  so that the correlation filter  $H(\rho, \phi)$  or equivalently  $\hat{H}(u, v)$  can be determined. Three correlation filter performance criteria, i.e., Output Noise Variance (ONV), Average Correlation Energy (ACE) and Average Similarity Measure (ASM) are taken into account in terms of CHF's.

Ideally, we would want a single correlation filter that minimizes ACE, ONV, and ASM while satisfying the constraints in (11). However, not all these correlation performance measures can be simultaneously minimized. Thus, the optimal tradeoff circular harmonic function filter is obtained by minimizing the following

figure of merit (FOM) while satisfying the constraints in (11) obtained from the FIR filter design procedure

$$FOM = 2\pi \sum_{k=-\infty}^{\infty} \left[ \int_0^{\infty} |H_k(\rho)|^2 P_{FOM}(\rho) \rho d\rho \right] \quad (14)$$

where  $P_{FOM}(\rho)$  is defined as:

$$P_{FOM}(\rho) = \alpha P_n(\rho) + \beta P_{avg}(\rho) + \gamma P_{ASM}(\rho) \quad (15)$$

The filter design problem can be rephrased as follows:

Find  $H_k(\rho)$  to

$$\begin{aligned}
&\text{minimize } \int_0^{\infty} |H_k(\rho)|^2 P_{FOM}(\rho) \rho d\rho \\
&\text{subject to } \int_0^{\infty} F_k(\rho) H_k^*(\rho) \rho d\rho = C_k \\
(16)
\end{aligned}$$

The solution to the above optimization problem can be shown to be

$$H_k(\rho) = \lambda_k \frac{F_k(\rho)}{P_{FOM}(\rho)} \quad \text{where } \lambda_k = \frac{C_k}{\int_0^{\infty} \frac{|F_k(\rho)|^2}{P_{FOM}(\rho)} \rho d\rho} \quad (17)$$

Once the filter harmonics are determined using (17), the correlation filter can be obtained using (9).

#### 2.4.2 MACE-MRH Correlation Filter

The MACE-MRH correlation filter is based on the Mellin radial harmonic (MRH) transform, given by the following pair of equations:

$$\begin{aligned}
F(\rho, \phi) &= \sum_{m=-\infty}^{\infty} F_m(\phi) \rho^{j2\pi m-1} \\
F_m(\phi) &= L^{-1} \int_d^R F(\rho, \phi) \rho^{-j2\pi m-1} \rho d\rho \\
(18)
\end{aligned}$$

where  $F_m(\phi)$  is the  $m$ -th MRH function (MRHF) of  $F(\rho, \phi)$ .

Similar to OTCHF filter, the correlation peak  $c$  is:

$$c = L \sum_{m=-\infty}^{\infty} C_m, \quad C_m = 2\pi \int_0^{\infty} F_m(\phi) H_m^*(\phi) d\phi \quad (19)$$

Let  $g_\beta(x, y)$  denote the image that results when image is uniformly scaled by a factor  $\beta$ , i.e.,  $g_\beta(x, y) = f(\beta x, \beta y)$ . Then the 2-D FT of  $g_\beta$  (in polar frequencies) is given by the relation

$$G_\beta(\rho, \phi) = \frac{1}{\beta^2} F\left(\frac{\rho}{\beta}, \phi\right) \quad (20)$$

The  $m$ -th MRHF of  $G_\beta$  can be expressed in terms of the  $m$ -th MRHF of  $F$  as follows:

$$G_{\beta m}(\phi) \approx L^{-1} \beta^{-j2\pi m-1} F_m(\phi) \quad (21)$$

If we take image  $g_\beta(x, y)$  as the input to the filter  $H$ , i.e., we correlate with a scaled version of the reference image, we obtain the following simple expression for the correlation peak as a function of input scale  $\beta$ :

$$c(\beta) = \beta^{-1} \sum_{m=-\infty}^{\infty} C_m e^{-j2\pi m \ln \beta} \quad (22)$$

A new function  $\hat{c}(\beta)$  can be obtained by using a logarithmic transformation  $\Lambda$ :

$$\hat{c}(\beta) = \Lambda\{c(\beta)\} = e^{\frac{L\beta}{2\pi}} c(e^{\frac{L\beta}{2\pi}}) = \sum_{m=-\infty}^{\infty} C_m e^{-j(Lm)\beta} \quad (23)$$

The relationship between the transformed scale response  $c(\beta)$  and the coefficients  $C_m$  is exactly the same as  $A(\omega)$  and  $a[n]$  in (13).

The MACE-MRH correlation filter is designed to minimize the average correlation energy  $ACE_{MRH}$  while satisfying the relationship in (24). The  $ACE_{MRH}$  is equal to the average energy of the correlation filter, defined as:

$$ACE_{MRH} = L \sum_{m=-\infty}^{\infty} \int_0^{2\pi} |H_m(\phi)|^2 P_F(\phi) d\phi \quad (24)$$

where  $P_F(\phi)$  is the average power spectrum of the reference pattern obtained by computing the average of  $|F(\rho, \phi)|^2$  along the radial axis.

The resultant optimization problem can be restated as follows:

Find  $H_m(\phi)$  to

$$\begin{aligned} & \text{minimize} \quad \int_0^{2\pi} |H_m(\phi)|^2 P_F(\phi) d\phi \\ & \text{subject to} \quad \int_0^{2\pi} F_m(\phi) H_m^*(\phi) d\phi = C_m \end{aligned} \quad (25)$$

Using the method of Lagrange multipliers, the solution to the minimization problem of (25) is

$$H_m(\phi) = \lambda_m^* \frac{F_m(\phi)}{P_F(\phi) + \alpha} \quad \text{where} \quad \lambda_m = \frac{F_m(\phi)}{\int_0^{2\pi} \frac{|F_m(\phi)|^2}{P_F(\phi) + \alpha} d\phi} \quad (26)$$

where  $\alpha$  is a small additive constant. Finally, the correlation filter  $H(u, v)$  is found by applying the inverse MRH transforms of  $Hm(\phi)$  and applying a polar-to-cartesian coordinate transform.

## 2.5 Statistical Decision for Correlation Output

In the third step of watermark detection, a whitening procedure is applied to both the received image  $z(i, j)$  and geometrically resilient watermark  $\tilde{a}(i, j)$ . The whitening filter is the LS prediction error filter that has been used for the computation of the perceptual mask.

$$e_z(i, j) = z(i, j) - \hat{z}(i, j) \quad (27)$$

$$e_{\tilde{a}}(i, j) = \tilde{a}(i, j) - \hat{\tilde{a}}(i, j), \quad \tilde{a}(i, j) = M \bullet H \quad (28)$$

Then the correlation between  $e_z(i, j)$  and  $e_{\tilde{a}}(i, j)$  is computed. If the two match, a sharply peaked correlation output will be obtained. When they do not match, a correlation output with less sharp peaks will be obtained.

PSR is computed as follows:

$$PSR = \frac{c(i_p, j_p) - m_{sr}}{\sigma_{sr}} \quad (29)$$

where  $c(i_p, j_p)$  is the peak of the correlation output,  $m_{sr}$  and  $\sigma_{sr}$  are the mean and standard deviation of the sidelobe region respectively.

The watermark detection task can be formulated as the following binary hypothesis testing problem:

$H_0$ : the image  $Z$  is not marked with  $W$ ;

$H_1$ : the image  $Z$  is marked with  $W$ .

To discriminate between  $H_0$  and  $H_1$ , the decoder computes PSR and compares it to  $T_p$ . To determine the value of  $T_p$ , the statistic of PSR must be taken into account. We consider PSR as a random variable and apply the central limit theorem, PSR can then be assumed to be normally distributed. Let  $\mu_0$  and  $\sigma_0$  represent the mean and the variance of PSR under hypotheses 0,  $\mu_1$  and  $\sigma_1$  represent the mean and the variance of PSR under hypotheses 1. The decoder error probability  $P_e$  can be written as

$$P_e = P(0|1)P(1) + P(1|0)P(0) \quad (30)$$

where  $P(0|1)$  is the probability of missing the presence of the watermark (false negative):

$$\begin{aligned} P(0|1) &= p(PSR < T_p | H_1) = \frac{1}{\sqrt{2\pi}\sigma_1} \int_{-\infty}^{T_p} \exp\left(-\frac{(PSR - \mu_1)^2}{2\sigma_1^2}\right) dPSR \\ &= \frac{1}{2} + \frac{1}{2} \operatorname{erf}\left(\frac{T_p - \mu_1}{\sqrt{2}\sigma_1}\right) \end{aligned} \quad (31)$$

and  $P(1|0)$  the probability of revealing the presence of  $W$  when  $W$  is not actually present (false positive):

$$\begin{aligned} P(1|0) &= p(PSR > T_p | H_0) = \frac{1}{\sqrt{2\pi}\sigma_0} \int_{T_p}^{\infty} \exp\left(-\frac{(PSR - \mu_0)^2}{2\sigma_0^2}\right) dPSR \\ &= \frac{1}{2} - \frac{1}{2} \operatorname{erf}\left(\frac{T_p - \mu_0}{\sqrt{2}\sigma_0}\right) \end{aligned} \quad (32)$$

Moreover, by  $P(0)$  and  $P(1)$ , the *a priori* probability of  $H_0$  and  $H_1$  are meant, respectively.

To minimize  $P_e$ , let

$$\frac{dP_e}{dT_p} = 0 \quad (33)$$

Assuming the pdfs of PSR conditioned to  $H_0$  and  $H_1$  have the same variance, i.e.,  $\sigma_0 = \sigma_1 = \sigma$ , the optimum threshold  $T_{opt}$  can be solved:

$$T_{opt} = \frac{\mu_0 + \mu_1}{2} + \frac{\sigma^2}{\mu_0 - \mu_1} \ln\left(\frac{P(1)}{P(0)}\right) \quad (34)$$

By assuming that  $H_0$  and  $H_1$  are equiprobable, i.e.,

$$P(0) = P(1) = \frac{1}{2}, \text{ then we can obtain}$$

$$T_{opt} = \frac{\mu_0 + \mu_1}{2} \quad (35)$$

## 3. EXPERIMENTAL RESULTS

In this section, extensive experiments have been conducted in order to investigate the performance of the proposed watermarking algorithm from the point of view of invisibility, robustness to geometrical attacks and computation complexity.

### 3.1 Watermark Invisibility

To assess the validity of the proposed algorithm in terms of watermark invisibility, we selected a set of standard images and

watermarked each image by using the spatial perceptual mask. We evaluate the performance by the peak of signal-to-noise ratio (PSNR), which is computed as follows:

$$PSNR = 10 \log_{10} \frac{255^2 \times M \times N}{\sum_{x=1}^M \sum_{y=1}^N [I(x, y) - I'(x, y)]^2} \quad (36)$$

The effect of the block size in the local prediction is also investigated. The results on the graylevel set for block sizes varying from  $7 \times 7$  to  $15 \times 15$  are reported in Table 1. As can be readily seen, the proposed approach permits to hide the watermark very well. The optimal block size depends on the test image. We get  $13 \times 13$  for *Lena*,  $12 \times 12$  for *Jetplane*,  $11 \times 11$  for *Barbara*,  $12 \times 12$  for *Tiffany* and  $9 \times 9$  for *Boat*, etc. On the other hand, PSNR is rather robust against moderate variations of the block size. For most test images, the results obtained for blocks in the range  $9 \times 9$  to  $13 \times 13$  are almost indistinguishable. Considering the computation time,  $9 \times 9$  is a good compromise. Thus we use a fixed block of size  $9 \times 9$  for each image.

**Table 1. PSNR (dB) versus block size**

Block size	<i>Lena</i>	<i>Jetplane</i>	<i>Mandrill</i>	<i>Barbara</i>	<i>Tiffany</i>	<i>Boat</i>	<i>Peppers</i>	<i>Lake</i>
$7 \times 7$	49.25	47.15	49.73	49.51	49.02	49.13	48.54	48.32
$8 \times 8$	50.32	48.24	50.52	50.43	50.11	50.23	49.53	49.15
$9 \times 9$	51.11	49.97	50.98	51.02	51.34	51.42	50.89	50.93
$10 \times 10$	51.12	50.11	51.43	51.23	51.36	51.35	51.22	51.02
$11 \times 11$	51.12	50.12	51.42	51.34	51.41	51.23	51.15	51.14
$12 \times 12$	51.13	50.68	51.31	51.13	51.46	51.41	51.32	51.12
$13 \times 13$	51.20	50.42	51.45	51.20	51.40	51.33	51.02	51.10
$14 \times 14$	50.63	49.98	50.56	50.63	50.86	50.25	50.72	50.35
$15 \times 15$	49.79	48.87	50.89	49.79	49.32	49.67	49.83	49.63

## 3.2 Robustness to Geometrical Attacks

Experimental results are based on the full image set of 1338 images in the UCID database. All the test images are turned into grayscale images and cut down to the size of  $256 \times 256$ .

### 3.2.1 Robustness to Rotation and Translation

We design the OTCHF correlation filter that recognizes views of the watermark pattern within an angular range of  $\pm 45^\circ$  and rejects views outside that range, i.e., the filter should provide the following in-plane rotation response

$$c(\theta) = \begin{cases} 1, & |\theta| \leq 45^\circ \\ 0, & \text{otherwise} \end{cases} \quad (37)$$

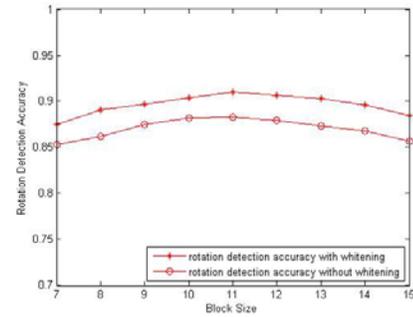
The parameter values we used in (15) are  $\alpha=0.8$ ,  $\beta=0.6$  and  $\gamma=0.1$ .

The performance of the proposed detector with the OTCHF correlation filter was tested. We obtain  $\mu_0=3.94$ , and  $\mu_1=15.81$  by statistical experiments, thus  $T_{opt} = \frac{\mu_0 + \mu_1}{2} = 9.88$ . Rotation

detection accuracy is given in Table 2. The effect of the block size on detection accuracy is also investigated. We use the same block size during watermark embedding and watermark detection. The experimental results are presented in Figure 2. We observe that whitening has a beneficial effect on the detector and detection accuracy can be improved by about 1.8% on average. The block size produce a slight effect on the rotation detection accuracy, especially in the range  $9 \times 9$  to  $13 \times 13$ .

**Table 2. Rotation detection accuracy**

Rotation angle	With whitening	Without whitening
$5^\circ$	92.26%	90.43%
$10^\circ$	91.13%	89.15%
$15^\circ$	90.84%	88.78%
$20^\circ$	90.12%	88.35%
$25^\circ$	89.26%	87.14%
$30^\circ$	89.37%	87.51%
$35^\circ$	88.95%	86.73%
$40^\circ$	86.34%	84.25%
$45^\circ$	84.62%	82.38%



**Figure 2. Rotation detection accuracy versus block size**

Moreover, according to the OTCHF correlation filter design theory, the proposed detector is also robust to translation attack. The translation detection accuracy with whitening and without whitening is both 100% in our experiments. We do not go into details here.

### 3.2.2 Robustness to Scaling

We design the MACE-MRH filter with the following scale response:

$$c(\beta) = \begin{cases} 1, & 0.5 < \beta^{-1} < 1.5 \\ 0, & \text{otherwise} \end{cases} \quad (38)$$

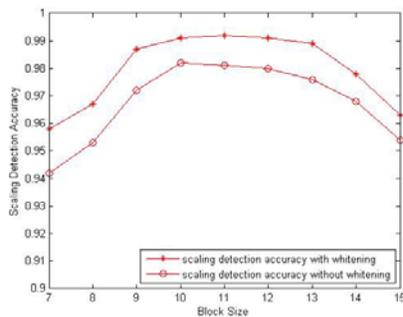
In other words, we want the filter to exhibit a sloped response for scaled versions of the reference pattern between 50% ( $\beta^{-1} = 0.5$ ) smaller and 50% ( $\beta^{-1} = 1.5$ ) larger. Furthermore, we specify that ideally the filter should produce no peak for scaled inputs outside of this range.

The performance of the proposed detector with the MACE-MRH correlation filter was tested based on the UCID images. We obtain  $\mu_0 = 32.86$ , and  $\mu_1 = 7.35$  by statistical experiments, thus  $T_{opt} = \frac{\mu_0 + \mu_1}{2} = 20.11$ . Scaling detection accuracy is shown in

Table 3. The effect of the block size is reported in Figure 3. Similar to rotation detection, we observe that whitening can improve the scaling detection accuracy by about 1% on average, and the block size produce a slight effect on the scaling detection accuracy in the range  $9 \times 9$  to  $13 \times 13$ .

**Table 3. Scaling detection accuracy**

Scaling factor	With whitening	Without whitening
0.6	95.26%	94.31%
0.7	97.13%	96.43%
0.8	98.84%	97.75%
0.9	99.12%	98.34%
1	99.86%	98.56%
1.1	99.31%	97.95%
1.2	98.95%	97.93%
1.3	96.34%	96.28%
1.4	94.97%	94.62%

**Figure 3. Scaling detection accuracy versus block size****Table 4. PSNR (dB) comparison**

	<i>Lena</i>	<i>Jetplane</i>	<i>Mandrill</i>	<i>Barbara</i>	<i>Tiffany</i>	<i>Boat</i>	<i>Peppers</i>	<i>Lake</i>
<b>The scheme in [29]</b>	49.25	47.15	49.25	49.25	49.25	49.25	49.25	49.25
<b>Our scheme</b>	50.32	48.24	50.32	50.32	50.32	50.32	50.32	50.32

**Table 5. Comparison of scaling detection accuracy**

Scaling factor	The scheme in [29]	Our scheme
0.7	94.6%	96.8%
0.85	97.9%	98.9%
1	98.2%	99.7%
1.15	93.6%	98.2%
1.3	92.7%	97.6%

### 3.3 COMPUTATION COMPLEXITY

Compared with the scheme in [29], which only uses a simple  $3 \times 3$  Laplace filter as the perceptual masking filter, perceptual masking and whitening with the local LS prediction in our approach result in the increase of computational complexity, it should be noticed that the cost is still affordable. For the watermarked images, PSNR comparison with the scheme in [29] is presented in Table 4. We also compare the scaling detection accuracy using the

threshold  $T_p$ , which is calculated by setting false positive rate

$P(l|0) = 10^{-3}$  (the same method as adopted in [29]). The detection results are shown in Table 5. Our approach clearly outperforms the scheme in [29] in terms of watermark invisibility and scaling detection accuracy. The average watermark detection time of the proposed scheme on a standard  $256 \times 256$  grayscale image is 2.162 seconds for the Matlab implementation. These results were obtained on a common computer with AMD Athlon(tm) X4 760K Quad Core Processor at 3.8 GHz, 4 GB MB of RAM and a 64 bit operating system. If it is implemented by C++, the average running time will be negligible.

## 4. CONCLUSIONS

Based on the OTCHF correlation filter and the MACE-MRH correlation filter, this paper presents a new mobile watermarking approach for digital images providing robustness to RST distortions. A spatial perceptual mask is computed by using the LS prediction error filter. The watermark is embedded into the cover image with the perceptual mask. In the watermark detection, the OTCHF filter or MACE-MRH filter is designed with the watermark as the reference pattern, and the correlation output is robust to user-specified rotation or scale range. Before final correlation, a whitening filter, i.e., the LS prediction error filter, is adopted to improve the detector performance. Experimental results from a large database of test images indicate that the proposed energy efficient watermarking approach is robust to geometrical distortions, and the detection reliability can be significantly improved by applying whitening filter prior to correlation.

Our previous study shows that image complexity plays an important role in evaluating detection performance [35]. We will carry out the performance study of proposed mobile watermarking under different image complexities in our future study.

## 5. ACKNOWLEDGMENTS

This work was supported by National Natural Science Foundation of China (No. 61170239). The last author highly appreciate the support from the U. S. National Science Foundation under the award CCF-1318688.

## 6. REFERENCES

- [1] Barni, M. 2005. Effectiveness of exhaustive search and template matching against watermark desynchronization, *IEEE Signal Process. Lett.*, 12(2): 158–161.
- [2] Lichtenauer, J., Setyawan, I., Kalker, T. and Lagendijk, R. 2003. Exhaustive geometrical search and the false positive watermark detection probability, *Proc. SPIE*, vol. 5020 (Jan. 2003), Security and Watermarking of Multimedia Contents V, pp. 203–214.
- [3] Pereira, S. and Pun, T. 2000. Robust template matching for affine resistant image watermarks, *IEEE Trans. Image Process.*, 9(6):1123–1129.
- [4] Kutter, M. 1998. Watermarking resisting to translation, rotation and scaling, *Proc. SPIE*, vol. 3528, Multimedia Systems and Applications (Nov. 1998), pp. 423–431.
- [5] Voloshynovskiy, S., Deguillaume, F. and Pun, T. 2001. Multibit digital watermarking robust against local nonlinear geometrical distortions, in *Proc. IEEE Int. Conf. Image Process.*, pp. 999–1002.

- [6] Su, P.-C. and Kuo, C.-C. J. 2001. Synchronized detection of the blockbased watermark with invisible grid embedding, *Proc. SPIE*, vol. 4314, Security and Watermarking of Multimedia Contents III, pp 423–431.
- [7] Herrigel, A., Voloshynovskiy, S. and Rytsar, Y. 2008. The watermark template attack, *Proc. SPIE*, vol. 4314, Security and Watermarking of Multimedia Contents III, pp. 394–405.
- [8] Ruanaidh, J. and Pun, T. 1998. Rotation, scale and translation invariant spread spectrum digital image watermarking, *Signal Process.* 66(3):303–317.
- [9] Lin, C. Y., Wu, M., Bloom, J. A., Cox, I. J., Miller, M. L. and Lui, Y. M., 2001. Rotation, scale, and translation resilient watermarking for images, *IEEE Trans. Image Process.*, 10(5):767–782.
- [10] Tian, H., Zhao, Y., Ni, R., Qin, L. and Li, X. 2013. LDFT-based watermarking resilient to local desynchronization Attacks, *IEEE Trans. Cybernetic*, 43(6):2190–2201.
- [11] Alghoniemy, M. and Tewfik, A.H., 2000. Image watermarking by moment invariants, *Proc. IEEE Int. Conf. Image Processing* (Sept.2000), pp.73–76.
- [12] Zhu, H., Liu, M., Li, Y., 2010, The RST invariant digital image watermarking using Radon transform and complex moments, *Digit. Signal Process.* 20:1612–1628.
- [13] Wang, X.Y., Yang, Y.P., Yang, H.Y., 2010. Invariant image watermarking using multi-scale Harris detector and wavelet moments, *Comput. Electr. Eng.*, 36(1):31–44.
- [14] Farzam, M., Shirani, S., 2001. A robust multimedia watermarking technique using Zernike transform, *Proc. IEEE Fourth Workshop on Multimedia Signal Processing*, 529–534.
- [15] Kim, H.S., Lee, H.-K., 2003. Invariant image watermark using Zernike moments, *IEEE Trans. Circuits Syst. Video Technol.*, 13(8): 766–775.
- [16] Xin, Y., Liao, S., Pawlak, M., 2007. Circularly orthogonal moments for geometrically robust image watermarking, *Pattern Recognition*, 40(12):3740–3752.
- [17] Li, L.-D., Guo, B.-L., Guo, L., 2009. Combining interest point and invariant moment for geometrically robust image watermarking, *J. Inf. Sci. Eng.*, 25:499–515.
- [18] Singhal, N., Lee, Y.-Y., Kim, C.-S., Lee, S.-U., 2009. Robust image watermarking using local zernike moments, *Journal of Visual Communication and Image Representation*. 20(6):408–419.
- [19] Bas, P., Chassery, J. and Macq, B. 2002. Geometrically invariant watermarking using feature points, *IEEE Trans. Image Process.*, 11(9):1014–1028.
- [20] Seo, J. and Yoo, C. 2006. Image watermarking based on invariant regions of scale-space representation, *IEEE Trans. Signal Process.* 54(4): 1537–1549.
- [21] Gao, X., Deng, C., Li, X. and Tao, D. 2010. Geometric distortion insensitive image watermarking in affine covariant regions, *IEEE Trans. Syst., Man Cybern. C, Appl. Rev.*, 40(3):278–286.
- [22] Wang, X., Wu, J. and Niu, P. 2007. A new digital image watermarking algorithm resilient to desynchronization attacks, *IEEE Trans. Inf. Forensics Security*, 2(4): 655–663.
- [23] Deng, C., Gao, X., Li, X. and Tao, D. 2009. A local Tchebichef moments based robust image watermarking, *Signal Process.* 89(8):1531–1539.
- [24] Zheng, D., Wang, S. and Zhao, J. 2009. RST invariant image watermarking algorithm with mathematical modeling and analysis of the watermarking processes, *IEEE Trans. Image Process.*, 18(5): 1055–1068.
- [25] Gao, X., Deng, C., Li, X. and Tao, D. 2010. Local feature based geometric resistant image information hiding, *Cognit. Computat.*, 2(2): 68–77.
- [26] Deng, C., Gao, X., Li, X. and Tao, D. 2010. Local histogram based geometric invariant image watermarking, *Signal Process.* 90(12): 3256–3264.
- [27] Tsai, J.-S., Huang, W.-B. and Kuo, Y.-H. 2011. On the selection of optimal feature region set for robust digital image watermarking, *IEEE Trans. Image Process.*, 20(3): 735–743.
- [28] Su, P.-C., Chang, Y.-C. and Wu, C.-Y. 2013. Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals, *IEEE Trans. Inf. Forensics Security*, 8(12):1897–1908.
- [29] Hyun, D.-K. and Lee, H.-K., 2014. A low-complexity mobile watermarking scheme resisting scale distortions. *Journal of Computer and Communications*, 2: 77–81.
- [30] Ryan A. Kerekes and B. V. K. Vijaya Kumar, 2006. Correlation filters with controlled scale response, *IEEE Trans. Image Process.*, 15(7):1794–1802.
- [31] Kumar, B. V., Mahalanobis, A. and Takessian, A. 2000. Optimal tradeoff circular harmonic function correlation filter methods providing controlled in-plane rotation response, *IEEE Trans. Image Process.*, 9(6):1025–1034.
- [32] Geert Depovere, Ton Kalker, Jean-Paul Linnartz, 1998. Improved watermark detection reliability using filtering before correlation, *Proceedings of ICIP* (1998), 430–434.
- [33] Irene G. Karybali, and Kostas Berberidis, 2006. Efficient spatial image watermarking via new perceptual masking and blind detection schemes, *IEEE Trans. Inf. Forensics Security*, 1(2):256–274.
- [34] Dragoi, I.C. and Coltuc, D. 2014. Local-prediction-based difference expansion reversible watermarking, *IEEE Trans. Image Process.*, 23(4):1779–1790.
- [35] Liu, Q., Sung, A. H., Chen, Z. and Xu, J. 2008. Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images. *Pattern Recognition*, 41(1): 56–66.