

# A Novel normalization based schema for digital images watermarking

K.M. Faraoun<sup>1</sup>, A. Rabhi<sup>2</sup>

<sup>1</sup> Evolutionary Engineering and Distributed Information Systems Laboratory, EEDIS  
UDL University- SBA, 22000 - Algeria  
*Kamel\_mh@yahoo.fr*

<sup>2</sup>Laboratoire des mathématiques, UDL University,  
SBA, 22000 - Algeria  
*rabhi\_abbes@yahoo.fr*

Received January 24, 2007 / Accepted July 13, 2007

**Abstract.** Geometric distortions are generally simple and effective attack to many existing watermarking methods that can make detection of the embedded watermark difficult or even impossible. A robust watermarking system must be able to encounter such attacks generally based on rotation, scaling and translation operators (RST attacks). In the present paper, we propose a new robust watermarking schema based on logo embedding in the DCT transformed domain using image normalization techniques. In contrast to existing approaches, the watermark is not embedded directly in the normalized image. The image normalization is just used for calculating the affine transform parameters so that the watermark embedding and detection is performed in the original coordinates system. The performed experiments show that the proposed algorithm is robust against various types of attacks such as low-pass, median, Gaussian noise, aspect ratio change, rotation, scaling, JPEG compression, and their combinations.

**Keywords:** Watermarking, Images normalization, DCT transformation

## 1. Introduction

Over the past few years, there has been tremendous growth in computer networks and more specifically, the World Wide Web. This phenomenon, coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security; images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image.

In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many articles and papers [7]. These properties include: perceptual invisibility to prevent obstruction of the original image, statistical invisibility (so it cannot be

detected or erased), fairly simple extraction (otherwise the detection process requires too much time or computation), robustness to filtering, additive noise, compression, and other forms of image manipulation and finally the ability to determine the owner of the original image.

Many of the current techniques for embedding marks in digital images have been inspired by methods of image coding and compression. Information has been embedded using the Discrete Cosine Transform (DCT) [1, 2], Discrete Fourier Transform magnitude and phase [3], wavelets [6], Linear Predictive Coding [4] and Fractals [5]. The key to making watermark robust has been the recognition that in order for a watermark to be robust it must be embedded in the perceptually significant components of the image [7]. The term "perceptually significant" is somewhat subjective but it suggests that a good watermark is one which takes account of the behavior of human visual system.

In order for a watermark to be useful, it must be robust against a variety of possible attacks by pirates. These include robustness against compression such as JPEG,

scaling and aspect ratio changes, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks. While many methods perform well against compression, they lack robustness to geometric transformations. Rotation and scaling attacks are considered more challenging than other attacks. Usually, the embedding of a strong watermark improves the detectability against the image compression and filtering attacks. However, different from these kinds of attacks, geometric manipulations are difficult to tackle. The main difficulty in geometric attacks is loss of synchronization in the watermark detector. Thus, the detection fails even though the watermark still exists in the watermarked image. Those are challenging attacks in that they do not introduce the quality degradation very much but make the detection process very complex and difficult.

In this paper, we propose a robust logo embedding algorithm that is resistant to geometric attacks. The synchronization is recovered using an image normalization technique for the detection process. Instead of embedding the watermark in the normalized image directly, we use an idea of image normalization just for calculating the affine transform parameters so that the watermark embedding and detection is performed in the original coordinates system. In addition, for a maximum watermark embedding with least perceptual degradation, we use a developed visual masking. The watermarking structure is based on a DCT transform method, and so the watermarking schema is semi-blind and we do not need an original image during the detection process. For robust watermark detection, an optimum threshold with a given false detection error probability is presented so that we can determine the threshold in advance regardless of the attacks that the watermarked image has undergone. It is useful to determine the optimal threshold in advance because the decoder complexity for calculating the threshold can be reduced.

The remaining of this paper is organized as follows. In section 2, a related theory about the DCT block parent-child structure and image normalization is presented. The section 3 present the existing related works to the RST invariants watermarking systems. In section 4, the proposed approach is described including watermark insertion and detection mechanisms. Experimental

results and discussions are given in section 5, and the conclusions are drawn in section 6.

## 2. Related Theory

### 2.1. DCT image transformation

Digital image watermarking technology is closely related to image coding technology. Transform coding is now the de-facto standard in image and video coding, while the Discrete Cosine Transform (JPEG, MPEG-1, 2, H.261, H.263) and the Discrete Wavelet Transform (JPEG2000) are mostly used. Given an image  $A$  of size  $M \times N$ , the DCT of the image is defined as [8]:

$$B(k_1, k_2) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} 4 \cdot A(i, j) \cdot \cos\left[\frac{\pi \cdot k_1}{2 \cdot M} (2i + 1)\right] \cdot \cos\left[\frac{\pi \cdot k_2}{2 \cdot N} (2j + 1)\right]$$

$B(k_1, k_2)$  is the DCT coefficient of the image in row  $k_1$  and column  $k_2$ . Larger DCT coefficients are usually located at low frequencies (upper left corner), while coefficients at high frequencies are very small. That is, DCT puts most of an image's energy at low frequencies. DWT separates an image into several sub-images corresponding to horizontal, vertical and diagonal details at each resolution level and a coarsest resolution level. Like DCT, most energy of an image is put in the coarsest sub-image.

### 2.2. Image Normalization

The typical geometrical attacks include rotation, scaling and translation of the image. These kinds of attacks can be represented by affine transform. The affine transform with scaling parameters  $(a, b)$ , rotation angle  $\varphi$  and translational parameters  $(T_x, T_y)$  can be defined as:

$$\begin{bmatrix} x_a \\ y_a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} T_x \\ T_y \end{bmatrix} \quad (1)$$

where  $(x, y)$  are the pixel coordinates of an input image and  $(x_a, y_a)$  are the pixel coordinates of a transformed image. The affine transform parameters can be estimated using image moments. The image moment of order  $p+q$  is defined in the two dimensional Cartesian coordinates as:

$$m_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} x^p y^q \cdot I(x, y) \quad (2)$$

The centroid of the image can be calculated using the zeroth and the first moments:

$$\bar{x} = m_{10}/m_{00}, \quad \bar{y} = m_{01}/m_{00}$$

The translational effect in the image can be removed by setting the transform center as  $(\bar{x}, \bar{y})$ . The central moments of order  $p+q$  is defined as:

$$\mu_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} (x - \bar{x})^p (y - \bar{y})^q I(x, y) \quad (3)$$

Now, we can normalize the input image of size  $l_x \times l_y$  using the image moments. Let the width and the height of the normalized image  $\check{l}_x = a.l_x$  and  $\check{l}_y = b.l_y$  so that the aspect ratio of the normalized image should be one.

$$\check{y} = b.l_y / a.l_x = 1 \quad (4)$$

If the aspect ratio of the input image is  $y = l_y/l_x$  we can get by replacing the relation into equation:

$$a = b.y \quad (5)$$

Let  $I(x/a, y/b)$  be the normalized image of the input image  $I(x, y)$ . Then, the zeroth moment of the normalized image can be obtained by changing the variables in equation (2)

$$\check{m}_{00} = a.b.m_{00}, \quad (6)$$

By solving the simultaneous equations of (5) and (6), finally we can calculate scaling parameters.

$$a = \sqrt{y.\check{m}_{00}/m_{00}} \quad , \quad b = \sqrt{\check{m}_{00}/y.m_{00}} \quad (7)$$

The image normalization against rotation can be performed using tensor theory defined in [9]. The rotation angle  $\varphi$  for image normalization can be calculated using following equations:

$$t^1 = \mu_{21} + \mu_{30} \text{ and } t^2 = \mu_{03} + \mu_{21}$$

$$\varphi = \tan^{-1} \left( -t^1 / t^2 \right) \quad (8)$$

Equation (8) has two possible solutions, thus, we choose  $\varphi$  such that  $-t^1 \sin \varphi + t^2 \cos \varphi > 0$  to insure a unique solution.

We can transform any input image to a normalized form by identifying the transform parameters,  $(a, b), \varphi$  and  $(\bar{x}, \bar{y})$ . If two different images are an affine transform pair, the normalized form of these images will be same.

### 3. Related Works

Recently, major of the researches concerning watermarking robustness improvement are interested to RST invariants metodes. O'Ruanaidh et al. [10] first have outlined the theory of integral transform invariants and showed that this can be used to produce watermarks that are resistant to rotation, scaling, and translation. In their approach the discrete Fourier transform (DFT) of an image is computed and then the Fourier-Mellin transform is performed on the magnitude, the watermark is embedded in the magnitude of the resulting transform. The watermarked image is reconstructed by performing the inverse transforms (an inverse DFT and an inverse Fourier-Mellin transform) after considering the original phase [11][10]. Fourier-Mellin transform is a log-polar mapping (LPM) followed by a Fourier transform, while an inverse Fourier-Mellin transform is an inverse log-polar mapping (ILPM) followed by an inverse Fourier transform. In the scheme, the embedded watermark may be extracted by transforming the watermarked image into RST invariant domain. However, they noted very severe implementation difficulties which might have hampered further work in this area. Pereira et al. [13] proposed to embed two watermarks, a template and a spread spectrum message containing the information or payload. The template contains no information itself, but is used to detect transformations undergone by the image. One problem with this solution is that, because it requires the insertion of a registration watermark in addition to the data-carrying watermark, this approach is likely to reduce the image quality. Lin et al. [12] proposed a method that develops a watermark invariant to geometric distortions, and that eliminates the need to identify and invert them. The watermark is embedded into a translation and scaling invariant one-dimensional signal obtained by taking the Fourier transform of the image, re-sampling the Fourier magnitudes into log-polar coordinates, and then summing a function of those magnitudes along the log-radius axis.

In [14, 15], Z. Dong has proposed to embed watermark in the log-polar mappings of Fourier magnitude spectrum of original image, and use the phase correlation between the LPM of the original image and the LPM of the watermarked image to calculate the displacement of watermark positions in LPM domain.

The scheme preserves the image quality by avoiding computing inverse log-polar mapping (ILPM)

In [16], a watermarking scheme is implemented by improving image normalization based watermarking (INW). Image normalization is based on the moments of the image, Invariant Centroid (IC) is proposed and the only central region(R), which has less cropping possibility by RST, is used for normalization.

J. Xuan and H.Zhang [17] proposed a rotation, scaling and translation (RST) resilient watermarking method through embedding watermark in RST invariant derived from Radon transform and Fourier transform. Based on the translation and rotation properties of Radon transform and the translation invariant property of Fourier magnitude, the RST invariant is obtained.

#### 4. Proposed Approach

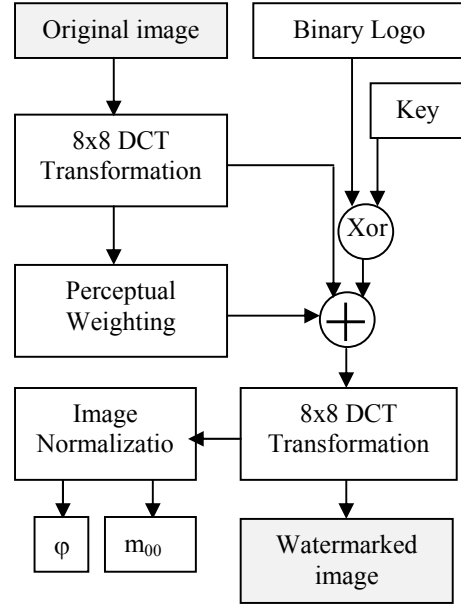
In the following, details of the proposed watermarking schema are explained. The two main phases of any watermarking system are embedding of the watermark and its extraction (detection process).

In the proposed method, the embedded watermark is a Logo binary image of size 64x64, where the host images used for benchmarking are gray scale 512x512 bitmaps.

##### 4.1. Watermark embedding

The block diagram for watermarks embedding is shown in Figure.1. The original image is transformed to  $8 \times 8$  block DCT domain. Then, the robust and the fragile watermarks are embedded in the DCT block. For robust logo embedding, the perceptual weighting for each block is calculated using spatio-frequency localization property of the  $8 \times 8$  DCT block. Two randomly selected groups of coefficients in each block are modified to embed one bit of information. The fragile watermark is embedded into the high frequency DCT coefficients which are vulnerable to the image modifications. To cope with geometric manipulations, the zeroth moment ( $m_{00}$ ) of the watermarked image and rotation angle ( $\varphi$ ) between the watermarked image and its normalized image are calculated. For the security of the embedding procedure, the binary logo  $S = \{s_0, s_1, \dots, s_{M-1}\}$  is modulated with the pseudorandom bit sequence  $R = \{r_0, r_1, \dots, r_{M-1}\}$  to generate the modulated watermark sequence  $P = \{p_0, p_1, \dots, p_{M-1}\}$ , where  $s_i, r_i, p_i \in \{0, 1\}$ . The modulation is based on the bit-wise logical XOR operation :

$$p_i = s_i \oplus r_i$$



**Figure 1:** General block diagram for the watermark (logo) embedding process

The embedding is based on the two set operation, *i.e.*, we embed one bit of watermark according to the sign of difference between two groups of randomly selected coefficients in the  $8 \times 8$  block. Let  $G_X$  and  $W_X$  be coefficients and their corresponding weighting values of a group X respectively. Then, the two groups  $G_A$  and  $G_B$  can be represented as:

$$\begin{aligned} G_A &= \{a_1, a_2, \dots, a_{N-1}\} & W_A &= \{u_0, u_1, \dots, u_{N-1}\} \\ G_B &= \{b_1, b_2, \dots, b_{N-1}\} & W_B &= \{v_0, v_1, \dots, v_{N-1}\} \end{aligned}$$

where N is the number of elements in each group.

When we embed  $p_j = '1'$  into the block  $j$ , we increase the absolute values of the coefficients in  $G_A$  by an amount of corresponding scaled (with  $\alpha$ ) weights in  $W_A$  and decrease the absolute values of the coefficients in  $G_B$  by an amount of corresponding scaled weights in  $G_B$  until  $ASD_j(G_A, G_B)$  (Absolute Sum Difference between  $G_A$  and  $G_B$ ) is greater than zero or predefined iteration is reached. On the other hand, when we embed "0" we decrease the absolute values of the coefficients in  $G_A$  by an amount of corresponding scaled weights in  $W_A$  and increase the absolute values of the coefficients in  $G_B$  by an amount of corresponding scaled weights in  $W_B$  until  $ASD_j(G_A, G_B)$  is smaller than zero, or predefined iteration is reached. The  $ASD_j(G_A, G_B)$  in the block  $j$  is defined as:

$$ASD_j(G_A, G_B) = \sum_{i=0}^{N-1} |a_i| - \sum_{i=0}^{N-1} |b_i| \quad (9)$$

pseudo-code for the embedding procedure is depicted in Figure 2. In the code, the functions  $\text{sgn}(x)$  and  $\text{step}(x)$  are well-known *signum* and *unit step* functions respectively.

$$\text{sgn}(x) = \begin{cases} 1 & \text{when } x > 0 \\ 0 & \text{when } x = 0 \\ -1 & \text{when } x < 0 \end{cases}$$

$$\text{step}(x) = \begin{cases} 1 & \text{when } x \geq 0 \\ 0 & \text{when } x < 0 \end{cases}$$

```

If  $P_j=1$  then {
  Itr:=0;
  Repeat
  { For  $i=0$  to  $N-1$ 
    { $a_i' := (|a_i| + \alpha \cdot u_i) \cdot \text{sgn}(a_i)$ ;
     $c := |b_i| - \alpha \cdot v_i$ ;
     $b_i' := c \cdot \text{sgn}(b_i) \cdot \text{step}(c)$ ;
    }
     $ASD_j(G_A', G_B') = \sum_{i=0}^{N-1} |a_i'| - \sum_{i=0}^{N-1} |b_i'|$ 
    Itr:=itr+1;
  }
  Until ( $ASD > 0$ ) or ( $\text{itr} > \text{max\_iteration}$ ); }
Else {
  Itr:=0;
  Repeat { For  $i=0$  to  $N-1$ 
    { $c := |b_i| - \alpha \cdot v_i$ ;
     $a_i' := c \cdot \text{sgn}(a_i) \cdot \text{step}(c)$ ;
     $b_i' := c \cdot \text{sgn}(b_i) \cdot \text{step}(c)$ ;
    }
     $ASD_j(G_A', G_B') = \sum_{i=0}^{N-1} |a_i'| - \sum_{i=0}^{N-1} |b_i'|$ 
    Itr:=itr+1;
  }
  Until ( $ASD < 0$ ) or ( $\text{Itr} > \text{max\_iteration}$ ); }

```

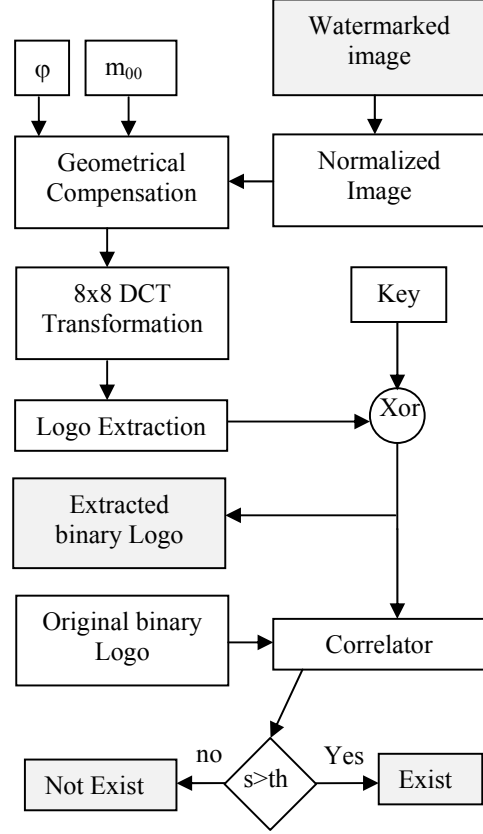
**Figure 2:** The used bit embedding algorithm

Three transform parameters have to be identified to invert the geometric manipulations. The translation can be compensated by calculating the image centroid  $(\bar{x}, \bar{y})$ . The scale and rotation can be compensated by using equation (7) and (8). Thus, we need  $m_{00}$  and  $\varphi$  of the watermarked image in watermark detection process.

#### 4.2. Watermark extraction process

The logo extraction is a reverse process of embedding. The image that is watermarked and possibly corrupted by attacks is normalized, and then scale parameters and rotation angles are calculated using equation (7) and (8) respectively. After inverting the geometric transform, the image is transformed into 8x8 DCT domain. Then, the block by block bit extraction is performed. For each

block  $j$ ,  $ASD_j(G_A, G_B)$  is calculated. If  $ASD_j(G_A, G_B) \geq 0$  then, we can decode  $p_j$  as '1' else decode  $p_j$  as '0'. The Figure.3 illustrate the general schema of the logo detection process.



**Figure 3:** Block diagram for watermark detection process

Apart from extracted logo, we can calculate the matching score using traditional normalized cross correlation between the original watermark and the decoded watermark [18]. The score is computed like the following:

$$s = \frac{\sum_{i=0}^{M-1} (2p_i - 1) \cdot (2p'_i - 1)}{\sqrt{\sum_{i=0}^{M-1} (2p_i - 1)^2 \cdot \sum_{i=0}^{M-1} (2p'_i - 1)^2}} \quad (10)$$

$$= \frac{1}{M} \cdot \sum_{i=0}^{M-1} (2p_i - 1) \cdot (2p'_i - 1)$$

where  $p_i$  and  $p'_i$  are the original and the extracted watermarks respectively.  $M$  is the length of watermark. If the score  $s$  is higher than a certain threshold  $T_s$ , we can say that the watermark is present in the image.

However, how much higher response is required for the watermark to exist? To solve this problem we present a method to calculate an optimal threshold for declaring the existence of the watermark with a given probability of false detection. To do this, we assume that  $s$  is normally distributed with a mean and a variance of  $\mu_s$  and  $\sigma_s^2$  respectively. The detection of watermark is modeled as a hypothesis testing problem. We have two cases for the null hypothesis ( $H_0$ : an image  $I(x,y)$  is not watermarked with  $X$ ). The first case is that the image,  $I(x,y)$  is not watermarked. The second case is that the image  $I(x,y)$  is watermarked with  $Y$  other than  $X$ . In our problem, the both cases are same because regardless of other watermark embedding, the distributions of  $p_i$  are same, *i.e.* in any case  $p_i$  is uniformly distributed with equal probabilities of  $\Pr(p_f=0)=0.5$  and  $\Pr(p_f=1)=0.5$ .

With the assumption that  $s$  is normally distributed, we can calculate false detection probability as:

$$P_f = \frac{1}{2} \operatorname{erfc} \left( \frac{T_s - \mu_s}{\sqrt{2}\sigma_s} \right) \quad (11)$$

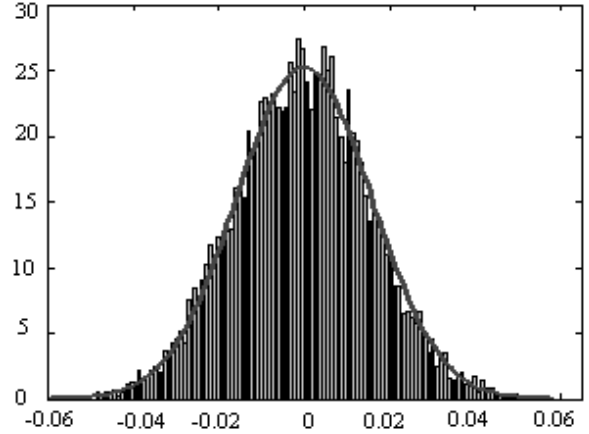
The statistics are easily calculated as  $\mu_s=0$  and  $\sigma_s^2=1/M$ . The derivation of these statistics is given in Appendix. A threshold with  $P_f \leq 10^{-10}$  can be calculated using equation (11):

$$T_s = 4.5\sqrt{2\sigma_s^2} \quad (12)$$

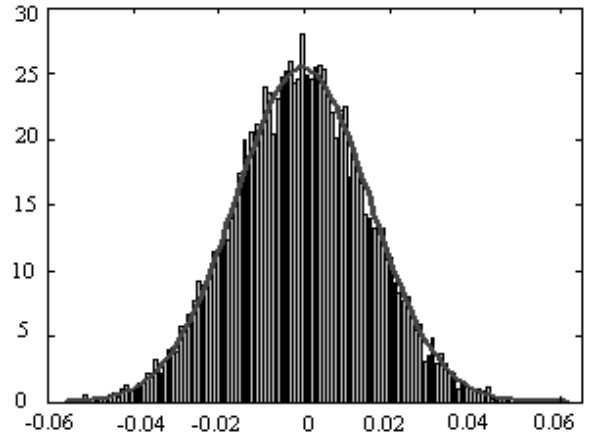
The final threshold can be calculated by replacing the  $\sigma_s^2=1/M$  into equation (13):

$$T_s = 4.5\sqrt{2/M} \quad (13)$$

The threshold only depends on the length of the embedded bits. The result has a meaning that we can use the consistent threshold regardless of the original image and embedded watermark strength in the detection process. Figure.4 and Figure.5 show the experimental distribution and theoretical pdf (with  $\mu_s=0$  and  $\sigma_s^2=1/M$ ) of the detector output  $s$ .



**Figure 4:** Distribution of the detector  $10^4$  output for unwatermarked image and its theoretical pdf



**Figure 5:** Distribution of the detector  $10^4$  output for the second case and its theoretical pdf

## 5. Results and Discussion

The proposed algorithm was tested on the popular  $512 \times 512$  Lena image as shown in Figure 6.(a). The image is watermarked with the logo shown in Figure 8.(a). The size of logo is  $64 \times 64$  so that one bit of information can be embedded into  $8 \times 8$  block. The watermarked version of Figure 6.(a) is shown in Figure 6.(b). The PSNR (Peak Signal to Noise Ratio) between these two images was 42.0885dB with embedding parameter  $\alpha=2.5$ . As can be seen from Figure 6.(a) and Figure 6.(b), the original and the watermarked image are perceptually indistinguishable. It means that the watermark is effectively masked.



(a)



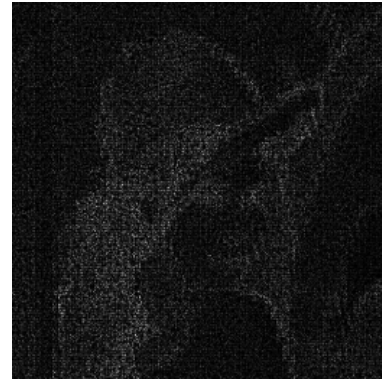
(b)

**Figure 6:** (a) Original Lena image and (b) watermarked image

Figure 7.(a) shows the absolute difference between the original and the watermarked image. The difference was scaled up for the illustrative purpose. The figure indicates that the watermark is mainly embedded into the highly active region of the image, which is less sensitive to human eyes. Several signal processing attacks as well as geometric attacks were simulated to demonstrate the robustness of the algorithm. Figure 7.(b) shows the image attacked with 30° rotation and 0.8 scaling.

The extracted logos from lowpass filtering, median filtering, and Gaussian noise attacks with 30° rotation and 1.5 times scaling are shown in Figure 8(c), Figure 8.(d) and Figure 8.(e) respectively. The extracted logos from aspect ratio change of 0.5 and 2 are shown in Figure 8.(f) and Figure 8.(g) respectively. Figure 7.(b) shows the image attacked with 30° rotation and 0.8 scaling. Figure 8.(h) shows extracted logos from

Figure 7(b). Figure 9 shows the corresponding matching score for extracted logos in Figure 8 with 1000 different keys. The horizontal line in the figures indicates the threshold with false detection probability of  $P_f < 10^{-10}$ .



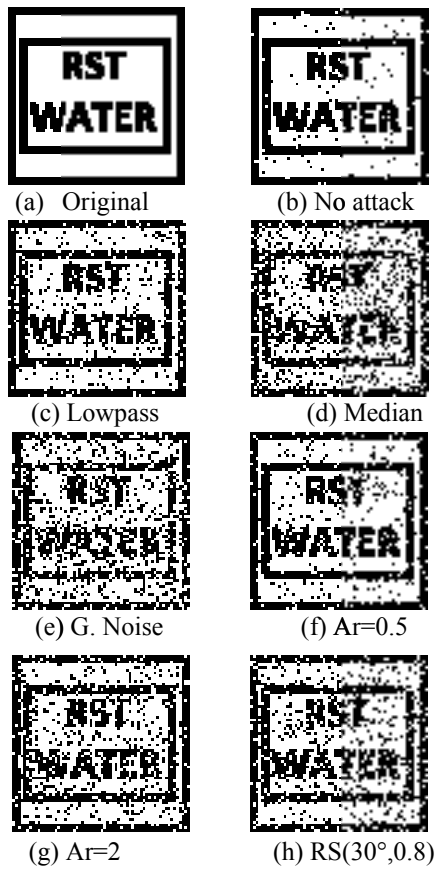
(a)



(b)

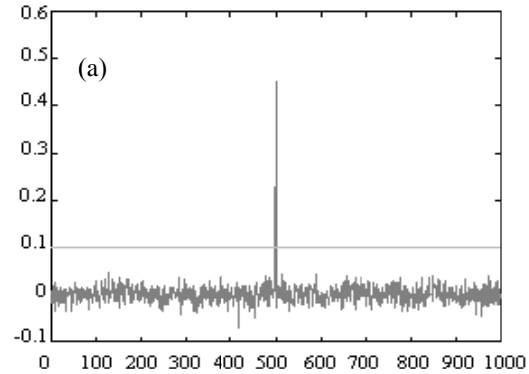
**Figure 7:** (a) absolute difference between 6.(a) and 6.(b), (b) rotated (30°) and scaled (0.8) version of 6.(b)

We can see that even if the attack is a combination of signal processing and geometrical transform, the detector output is reliable. Figure 10 shows that our scheme can resist rotation attacks of any angle, by illustrating the detector response intensity against various possible attacks. The detector output for the scaling with varying magnification is shown in Figure 11. As can be seen from the figure, the response has a local maximum at the integer multiples of magnifications. This is due to the interpolation in calculation of the magnifications. Figure 12 and Figure 13 show the detector response for rotation attacks with fixed magnification and scaling attacks with fixed rotation angle respectively. The detector is reliable for any combination of rotation and scaling.

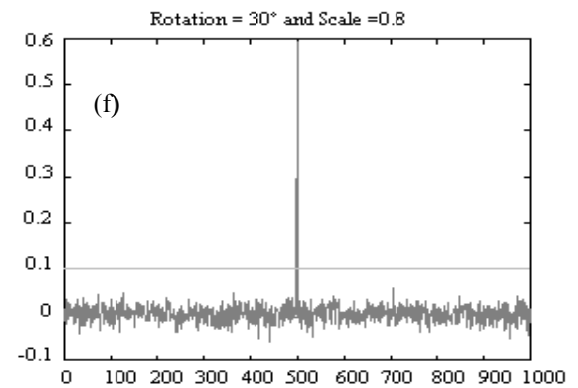
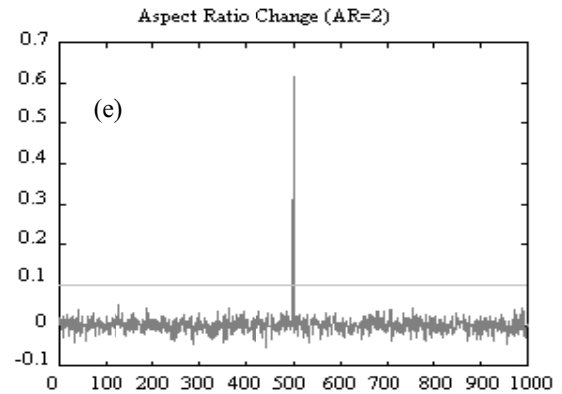
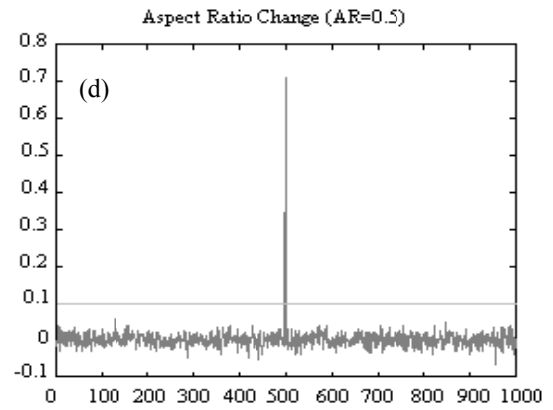
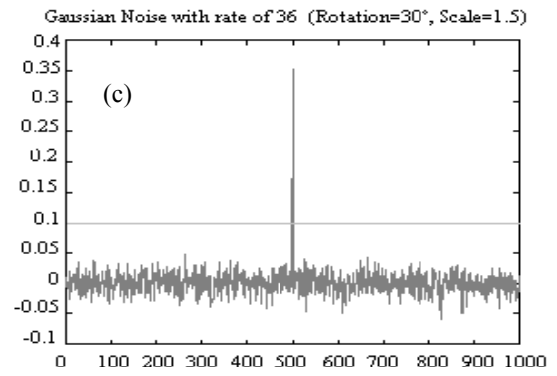
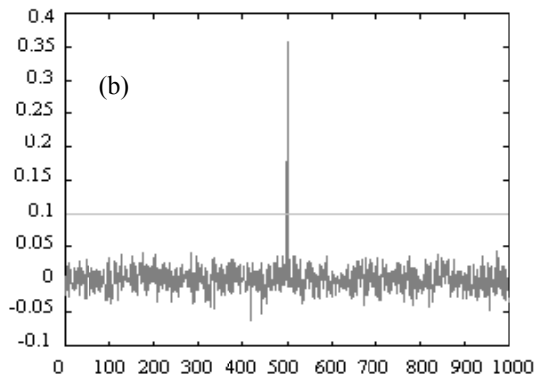


**Figure 8:** Extracted logos from attacked images

Lowpass Filtering with matrix size 3x3 (Rotation=30°, scale=1.5)



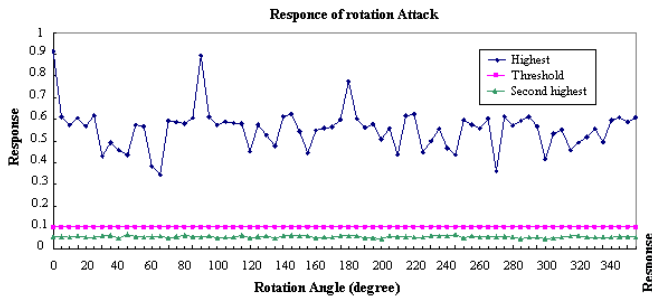
Median filtering with matrix size 3x3(Rotation=30°,scale=1.5)



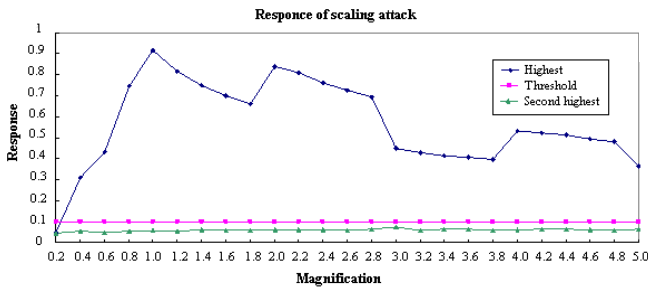
**Figure 9:** Detector response for various attacks

(a)Lowpass filter, (b) Median Filter, (c) G. Noise, (d) As. Ratio 0.5, (e) As. Ratio 2, (f) Rotation 30° and scale 0.8

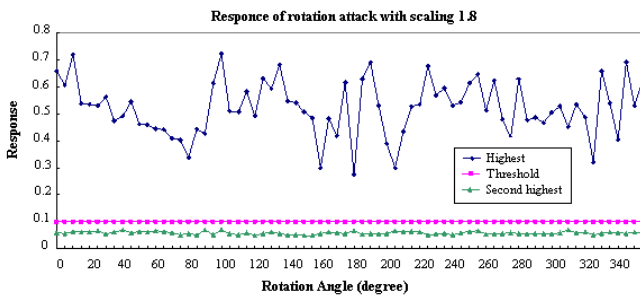




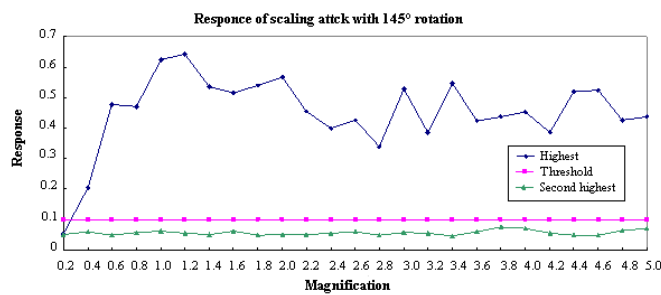
**Figure 10:** Detector response for the rotation with varying angles



**Figure 11:** Detector response for the scaling with varying magnification



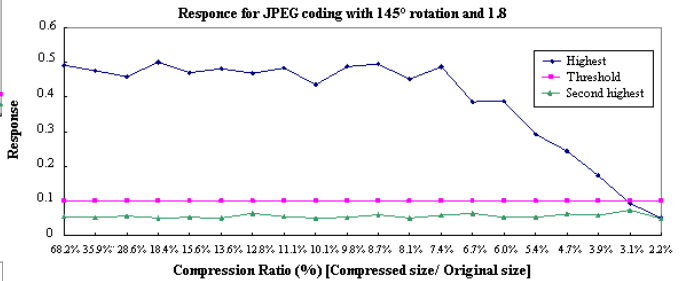
**Figure 12 :** Detector response for the rotation with scaling of 1.8 and varying angles



**Figure 13:** Detector response for the scaling with 145° rotation and varying magnification

The robustness for image compression is very important in image watermarking because almost all images are distributed in coded format. The detector response for JPEG compression with fixed rotation and scaling is shown in Figure 14, where compression ratios are varying. Even if the image undergoes combination of

geometric manipulation and compression, the detector shows robust performance until the compression ratio reaches 3.1% of the original size.



**Figure 14:** Detector response for the JPEG coding with 145° rotation, scaling of 1.8 and varying compression ratios

## 6. Conclusion

In this paper, we proposed a robust watermark embedding scheme using image normalization. To avoid the quality degradation caused by interpolation in image normalization, we do not embed the watermark in the normalized image. Instead, we use the idea of image normalization just for calculating the affine transform parameters so that the watermark embedding and detection can be performed in the original coordinates system. The robustness of the algorithm came from the utilization of the HVS property. The optimum threshold with a given false detection probability was presented so that we can determine the threshold in advance regardless of the attacks that watermarked image has undergone. We tested algorithm for various types of attacks such as lowpass, median, Gaussian noise, aspect ratio change, rotation, scaling, JPEG compression, and their combinations. Simulation results showed that the proposed algorithm is robust and reliable against various attacks and geometric transformation.

## References

- [1]. A. Bors, I. Pitas. "Image Watermarking using DCT Domain Constraints", IEEE International Conference on Image Processing (ICIP'96), Lausanne, Switzerland, vol. III, pp. 231-234, 16-19 September 1996.
- [2]. M.Barni, F. Bartolini, V. Cappellini, A. Piva. "A DCT Domain System for Robust Image

- Watermarking”, *Signal Processing*, vol.66, pp 357-372, 1998.
- [3]. J.J.K.O Ruanaidh, W.J.Dowling and F.M.Boland. “Phase watermarking of digital images”. In *proceeding of the IEEE International conference of Image Processing ICIP-96*, pages 239-242, Lausanne , Switzerland, September 1996.
- [4]. K. Matsui and K.Tanaka. “Video-Steganography :How to secretly embed a signature in a picture”. In *IMA Intellectual Property Project Proceeding*, pages 187-206, January 1994.
- [5]. P.Devern and M.Scott. “Fractal based images steganography” . In Ross Anderson Editor, *Proceeding of the First International Workshop in Information Hiding , Lecture notes in computer sciences*, pages 279-294, Cambridge, UK, May/June 1996.
- [6]. R. Eslami and H. Radha, “New Image Transforms Using Hybrid Wavelets and Directional Filter Banks: Analysis and Design,” in *proc. of IEEE International Conference on Image Processing*, vol. 1, pp. 733-736, Italy, 2005.
- [7]. A.Michael, M.Schmucker and D.Wolthusen. “Techniques and applications and Digital Watermarking and content protection”. *Brithich library Cataloguing in publication data*, Artech House computer security series, ISBN 1-58053-111-3. 685 Canton Street – Norwood, MA 02062.
- [8]. Z.Xiong, K.Ramchandran, M.T.Orchard and Y.Zhang, “A comparative study of DCT- and wavelet-based image coding”, *IEEE Trans. on Circutis and Systems for Video Technology*, Vol.9, No.5, August, 1999
- [9]. S. C. Pei and C. N. Lin, “Image Normalization for Pattern Recognition,” *Image and Vision Computing*, vol. 13, no. 10, pp. 711-723, December 1995.
- [10]. J. O’Ruanaidh and T. Pun, Rotation, Scale, and Translation Invariant Digital Image Watermarking, *Signal Processing*, Vol.66, No.3, pp. 303-317, 1998.
- [11]. M. Alghoniemy and A. Tewfik. “Progressive Quantized Projection Watermarking Scheme”, *Proceedings of ACM Multimedia 99*, Vol.1, pp. 295-298, 1999.
- [12]. C. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y Lui, Rotation, Scale, and Translation Resilient Watermarking for Images, *IEEE Transactions on Image Processing*, Vol.10, No.5, pp. 767-782, 2001.
- [13]. S. Pereira and T. Pun, Robust Template Matching for Affine Resistant Image Watermarks, *IEEE Transactions on Image Processing*, Vol.9, No.6, pp. 1123-1129, 2000.
- [14]. D. Zheng, J.zhao, a.el saddik, RST invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE transactions on circuits and systems for video technology*, vol. 9, no.6, September 2003.
- [15]. D. Zheng, J.zhao. “A novel RST-invariant digital image watermarking scheme”. *Third International Symposium on Multispectral Image Processing and Pattern Recognition*. Edited by Lu, Hanqing; Zhang, Tianxu. *Proceedings of the SPIE*, Volume 5286, pp. 477-480 (2003).
- [16]. B.Kim, J.Choi , K.Park, F.Petitcolas, K.Hyoung Joong, “Image normalization using Invariant Centroid for RST Invariant digital image watermarking” . *First International workshop on digital watermarking*, Seoul. vol. 2613, pp. 202-211. 2002.
- [17]. J. Xuan ; H.Zhang and L.Wang. “Rotation, scaling and translation invariant image watermarking based on Radon transform” *Visual Communications and Image Processing*. Edited by Li, Shipeng; Pereira, Fernando; Shum, Heung-Yeung; Tescher, Andrew G. *Proceedings of the SPIE*, Volume 5960, pp. 1499-1505, 2005.
- [18]. P. H. Wong, O. C. Au and Y.M. Yeung, “A Novel Blind Multiple Watermarking Technique for Images,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 813-830, August 2003.