

# A Geometric Distortion Resilient Image Watermark Algorithm Based on DWT-DFT

Yuping Hu, Zhijian Wang

<sup>1</sup>Guangdong Province Key Lab of EC Market Application Technology, GuangDong University of Business Studies  
Guangzhou, 510320, China

<sup>2</sup>Hangzhou Key Lab of E-Business and Information Security, Hangzhou Normal University  
Hangzhou, 310036, China

okhyp@yahoo.com.cn, zjian@gdcc.edu.cn

Hui Liu

Department of Electronics and Communication Engineering, Changsha College, Changsha  
Hunan 410003, China

Email: liuhui8037@yahoo.com.cn

Guangjun Guo

Department of Computer Science and Technology, Hunan Institute of Humanities, Science and Technology  
Loudi, Hunan 41700, China

Email: gguo@163.com

**Abstract**—In this paper, a robust watermarking algorithm against geometric distortions and common signal processing is proposed. This algorithm is based on two method to solve the synchronization of the original watermarking images and test images in the wavelet domain watermarking. One method, which estimates rotation and scaling based on embedding a template in a circle of middle frequency in DFT, One method which estimates translation based on extracting an invariant centroid from a restricted area inside the image. In the embedding process, a watermark is embedded adaptively in low band of DWT domain, according to the conceal quality of Human Visual System (HVS).The experiment results show robustness against common signal processing attacks , several geometric distortions and some combination attacks, Also the comparison with the prior algorithms shows the better performance of the proposed algorithm.

**Index Terms**—Digital watermarking; Wavelet transform; Direct Fourier transform; Geometric distortions

## I. INTRODUCTION

With the development of the Internet, more and more Digital media products become available through different on line services. The rapid growth of the multimedia services has created a potential demand for the protection of ownership since digital media is easily reproduced and manipulated. Digital watermarking has been introduced for solving such problems. One of the most prominent applications. of watermarking is using robust and practical watermarking to protect image and video data<sup>[1]</sup>.

In the past ten years, attacks against image watermarking systems have become more and more complicated with the development of watermarking techniques<sup>[2]</sup>. In a desired watermarking system, the

watermark should be robust to content-preserving attacks including geometric deformations and image processing operations. From the image watermarking point of view, geometric attacks mainly introduce synchronization errors between the encoder and decoder. The watermark is still present, but the detect or is no longer able to extract it. Different from geometric attacks, the content preserving image processing operations(such as addition of noises, common compression and filtering operations) do not introduce synchronization problems, but will reduce watermark energy. Most of the previous watermarking schemes have shown robustness against common image processing operations by embedding the watermarking to the low-frequency component of images, such as the low-frequency subbands of discrete wavelet transform<sup>[3]</sup>. In the literature, only a few algorithms have presented the topic of the robustness against geometric attacks. When the original image (not watermarked) is available in the detection, the cost for resynchronization can be reduced by comparing the original image with the watermarked image(which has undergone some geometric attacks), such as [4]-[7].Because the nonblind watermarking schemes are limited for most practical applications, researchers paid little attention to them. The nonblind schemes are effective to compensate for small local distortion, but the computation cost is dramatically increased under global affine transform<sup>[8]</sup>.When the original image is not available during the detection, several specialized methods have addressed the issue against geometric attacks by relying on exhaustive search<sup>[3]</sup>, template-based re-synchronization<sup>[9]</sup>, self-synchronizing watermarks<sup>[10]</sup> and watermarking in invariant domains<sup>[11]</sup>.In all the methods, the watermark embedding domain was always selected as spatial domain, DFT<sup>[12]</sup> domain or DFT-SVD domain .However

the wavelet transform has no ability to resist to geometric distortion, so the wavelet domain watermarking resisting to geometric distortion is a very difficult and challenging subject.

In this paper a watermarking algorithm robust to geometric distortion in DWT domain is proposed. In the algorithm, a watermark is embedded adaptively in low band of DWT domain, according to the conceal quality of Human Visual System (HVS), especially, the geometric transformation can be corrected before the watermarking detection, owing to embedding a template in a circle of middle frequency in DFT and extracting a invariant centroid from a restricted area inside the image. The paper is organized as follows: Section II reviews some necessary background on the wavelet tree and the properties of 2-D DFT, Section III and section IV describe the proposed watermark embedding and detection algorithm respectively in detail. In section V, experimental results of algorithm performance are presented. Finally conclusions are drawn in Section VI.

II. THE ANALYSES OF DWT AND DFT

A. The Wavelet trees and Human Visual System

For convenience, we will use 4-level wavelet transform of a  $256 \times 256$  image as example. With 4-level decomposition, we have 13 subbands as shown Fig 1, The coefficients are grouped according to wavelet trees except the coefficients of band LL band ( $d_4^0$ ). We will use the coefficients in subband  $d_4^1, d_4^2, d_4^3$  as roots to form wavelets trees. At the fourth level, the subbands  $d_4^1, d_4^2, d_4^3$  have  $3 \times 256 = 768$  trees. Each tree  $d_l^\theta(x, y)$  ( $\theta = 1, 2, 3$ ) consists of  $1+4+16+64=85$  coefficients, it can be defined as follow:

$$tree(d_4(x, y)) = \bigcup_{\theta=1}^3 tree(d_3^\theta(x, y))$$

$$tree(d_l^\theta(x, y)) = \bigcup_{i=1}^2 \bigcup_{j=1}^2 tree(d_{l-1}^\theta(2x-2+i, 2y-2+j)) \quad (l=4, 3, 2)$$

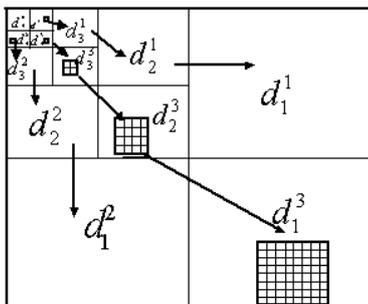


Fig.1 Tree structure of wavelet coefficients

The visual models provide thresholds (JND thresholds) for how much a given transform coefficient can change, before such changes are noticeable under

standard viewing conditions. JND threshold was determined for each coefficient, based on the literature[13], we are using this model in the paper, This model is as follows:

$$JND_l^\theta = \Theta(l, \theta) \Lambda(l, x, y) \Xi(l, x, y)^{0.2} \quad (2)$$

there into :

$$\Theta(l, \theta) = \begin{cases} 1.00, l=1 \\ \sqrt{2}, \theta=3 \\ 1, \theta=0, 1, 2, 3 \end{cases} \begin{cases} 0.32, l=2 \\ 0.16, l=3 \\ 0.10, l=4 \end{cases}$$

$$\Lambda(l, x, y) = 1 + \frac{1}{256} d_3^0 \left( 1 + \frac{x}{2^{3-l}}, 1 + \frac{y}{2^{3-l}} \right)$$

$$\Xi(l, x, y) = \sum_{k=1}^{3-l} \frac{1}{16^k} \sum_{\theta} \sum_{i=0}^1 \sum_{j=1}^1 [d_{k+l}^\theta \left( i + \frac{x}{2^k}, j + \frac{y}{2^k} \right)]^2$$

$$\frac{1}{16^{3-l}} Var \{ d_3^0 \left( 1 + i + \frac{x}{2^{3-l}}, 1 + j + \frac{y}{2^{3-l}} \right); i=0,1; j=0,1 \}$$

$\Theta(l, \theta)$  takes into account how sensitivity to noise changes depending on the band (in particular depending on the orientation and on the level of detail),  $\Lambda(l, x, y)$  takes into account the local brightness based on the gray level values of the low pass version of the image,  $\Xi(l, x, y)$  gives a measure of texture activity in the neighborhood of the pixel. In particular, this term is composed by the product of two contributions: the first is the local mean square value of the DWT coefficients in all detail subbands, while the second is the local variance of the low-pass subband. Both these contributions are computed in a small  $2 \times 2$  neighborhood corresponding to the location of the pixel.

B. Properties of 2-D DFT and LPM

An important property of DFT is translation invariance of its magnitude. Shifts in the spatial domain only cause a linear shift in the phase component. If a 2-D signal  $f(x, y)$  in the spatial domain is shifted, while the magnitude remains as follows :

$$f(x, y) \leftrightarrow F(\mu, \nu)$$

$$f(x+a, y+b) \leftrightarrow F(\mu, \nu) \exp[-j(a\mu + b\nu)] \quad (3)$$

Where a and b are the amount of shifts on the x- and y-axis respectively, and  $F(\mu, \nu)$  is 2-D DFT of  $f(x, y)$ .

The rotation of  $f(x, y)$  is represented by the rotation of  $F(\mu, \nu)$ , that is

$$f(x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta)$$

$$\leftrightarrow F(\mu \cos \theta - \nu \sin \theta, \mu \sin \theta + \nu \cos \theta) \quad (4)$$

and the scale change in the spatial domain increase the resolution of the spectrum and reduces the magnitude inverse proportionally as follows;

$$f(ax, by) \leftrightarrow \frac{1}{ab} F(\mu/a, \nu/b) \quad (5)$$

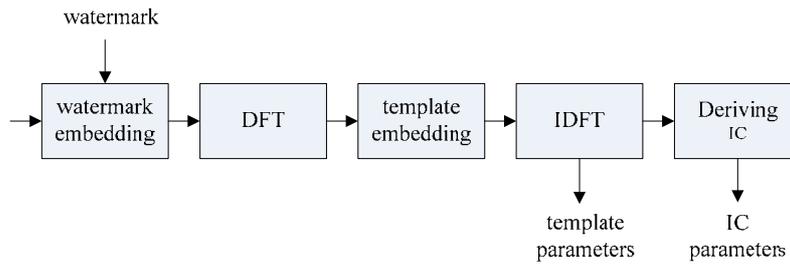


Fig.2 watermark embedding scheme

The properties of LPM include scaling invariance and the conversion of a rotation on Cartesian coordinates into a cyclic shift on log-polar coordinates. The scale of an image on log-polar coordinates is not changed, if the sampling rates  $N_r$  and  $N_\theta$  of LPM on the radial and angular direction, are constant. Eq.(6) represents the use of LPM to transform the point  $(x, y)$  on Cartesian coordinates into  $(r, \theta)$  on log-polar coordinates as follows:

$$\begin{aligned} x - x_0 &= \exp(r\Delta_r) \cos(\theta\Delta_\theta), \\ y - y_0 &= \exp(r\Delta_r) \sin(\theta\Delta_\theta) \end{aligned} \quad (6)$$

Where  $(x - x_0)$  are the Cartesian coordinates used as the origin of the log-polar coordinates,  $\Delta_r = \ln(\max(\text{distance from origin}) / N_r - 1)$  and  $\Delta_\theta = 2\pi / N_\theta$  are the sampling step size for the  $r$  and  $\theta$  axis, respectively, and  $r = \{0, 1, \dots, N_r\}$ ,  $\theta = \{0, 1, \dots, N_\theta\}$ .

### III. WATERMARK EMBEDDING SCHEME

The proposed algorithm provides a method to embed a watermark that consists of a sequence of 64 bits into a gray-scale image. The basic idea of the proposed watermark embedding scheme, which consists of three parts, the watermark embedding part, the template embedding part and the deriving IC (invariant centroid) part as shown Fig2.

#### A. Watermark Embedding

In the first of the watermarking embedding process, the wavelet tree quantization is used to embed the formatted watermark into the image. The wavelet coefficients of the host image are grouped into wavelet trees. It's corresponding mask controls the characteristic and tree structure relation of wavelet coefficients confirms a correlation mask for every lowest coefficient, then the quantization step of every lowest coefficient. Each watermark bit is embedded using a pair of wavelet lowest coefficients. The pair of wavelet lowest coefficients are so quantized that they exhibit a large enough statistical difference, which will later be used for watermark extraction.

The processes of the algorithm can be described in detail as follows: consider a  $256 \times 256$ , 8-bpp gray-scale images and

a readable watermark (W) of 128 bits that contains some meaningful information to embed into the image.

Step1: A 4-level DWT decomposition of the original I is performed using Daubechies-8 filters. According to formula (1), The coefficients are grouped according to wavelet trees except the coefficients of band LL band( $d_4^0$ ). We will use the coefficients in subband  $d_4^1, d_4^2, d_4^3$  as roots to form wavelets trees.

Step2: To guarantee the algorithm security, we use a key  $K_1$  to choose a tree pairs, say tree  $A_i$  and tree  $B_i$  for each bit  $w_i$  to be embedded.

Step3: All wavelet coefficients of tree  $A_i$  or tree  $B_i$  will be quantized depending the watermark bit  $W_i$ . the quantization of  $d_l^\theta(x, y)$  is given by:

$$d_l^{\theta'}(x, y) = \text{Sign}(d_l^\theta(x, y)) * \lfloor \text{floor}(d_l^\theta / JNd_l^\theta(x, y) * W_i + 0.5) * d_l^\theta(x, y) \rfloor \quad (7)$$

$d_l^{\theta'}$  is the wavelet coefficient after quantized,  $\text{floor}(X)$  denotes the integer of X,  $JNd_l^\theta(x, y)$  is JND of coefficient  $d_l^\theta(x, y)$ .

if  $w_i=1$  All wavelet coefficients of tree  $A_i$  is quantized, if  $w_i=0$  All wavelet coefficients of tree  $B_i$  is quantized.

Step4: step-2 and step-3 is done repeatedly till all  $w_i$  is embedded.

Finally the IDWT is applied using modified coefficients, resulting in the watermarked image.

#### B. Template embedding

According to the magnitude property of an image DFT, the magnitude of its 2-D DFT remains invariant after the image is shifted, rotates  $\theta$  after the image rotated  $\theta$ , reduces  $1/\rho$  after the image reduced  $\rho$ . Making use of these properties, we will embed a template in the magnitude of an image DFT, which can embody the RST attack to the watermarking image.

Because of the low frequency coefficient of DFT includes the main energy of the magnitude, it can not reflect on the rotation attack of small angle, at one time, the high frequency coefficient of DFT is influenced by the common image processing easily. So, we select the intermediate frequency domain of DFT for template

embedding. The template embedding algorithm is described as following.

Step1: Use key  $K_2$  to choose NUM template points uniformly on a circle region with radius R in the intermediate frequency domain of DFT (the experiment indicates that if NUM=15, it can assure the better matching precision and efficiency in the detection)

Step2: Select a appropriate circle window(always  $r=6-8$ ) with the template point as a center, and augment its magnitude value to the biggest value in the local region(the biggest magnitude value always equals to 2-3 times of the average of the local region)

Step3: Considering on the conjugate of 2-D DFT, the magnitude of coefficients in the descend plane is modified symmetrically.

Step4: the IDFT is applied using modified coefficients, resulting in the final watermarked image

C. Deriving Invariant Centroid

The IC (invariant centroid) is defined as an invariant point that is not changed by geometrical transformations, image processing e.g. JPEG compression and noise addition etc. If we can derive an invariant centroid from a watermarking image, the change coordinate of its invariant centroid will reflect on the translation of watermarking image.

A simple method is that the center of an image is used as the origin, but this can cause different results if the image is cropped for some reason. Therefore, an invariant point that remains unchanged after geometrical or waveform attacks is needed. In conventional feature point finding techniques, it is difficult to find an invariant point that is not changed by geometrical transformations, image processing, and compression. Therefore, in the proposed scheme, an invariant centroid derived by an iterative method is used as the origin.

The centroid  $C = (C_x, C_y)$  of an image  $I(x, y)$  is calculated as follows:

$$C_x = \frac{\sum_x \sum_y I(x, y) x}{\sum_x \sum_y I(x, y)}$$

$$C_y = \frac{\sum_x \sum_y I(x, y) y}{\sum_x \sum_y I(x, y)}$$

(8)

Where  $x, y \in \mathbb{R}^2$  is the region of the image  $I(x, y)$ .

The method of deriving the invariant centroid is depicted in Fig. 3, the algorithm is described as following.

Step1: Perform low pass filtering on the image so as to reduce the effects of waveform attacks,

Step2: The initial centroid of the image  $C_0$  is calculated using Eq. (8)

Step3: Eq. (8) is used to calculate the centroid  $C_1$  based on a circular region with radius r and center point  $C_0$ . The region used to calculate the centroid position must be circular so that it will not change although rotation occurs.

Step4: If  $C = C_1$ , go to step 5 else suppose  $C = C_1$  and go to step3.

Step5: C is the obtained invariant centroid.

Geometrical or waveform attacks will have no effect on the location of this point due to the use of low pass filtering and the fact that the point was not extracted from the entire image but rather from a restricted area inside the image.

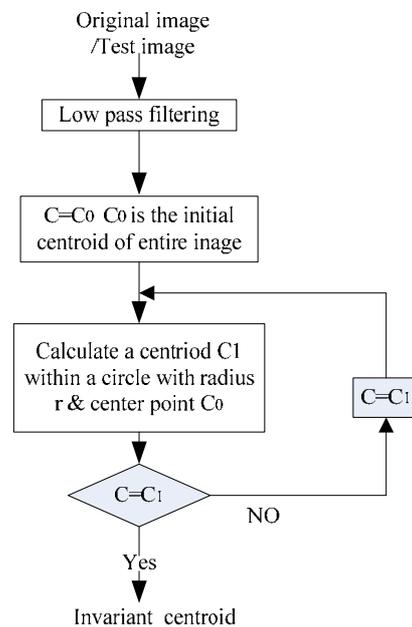


Fig.3. Sketch map for deriving invariant centroid.

The proposed method which identified an invariant centroid as the origin of LPM, was found to be efficient and robust to various attacks, see Fig.4. Fig.4(a) shows the invariant centroid of the original image, while Fig.4(b)-(g) represents the robustness of the invariant centroid to various attacks. including  $3 \times 3$  average filtering(Fig.4(b)), addition of 5% Gaussian noise(Fig.4(c)), JPEG compression based on compression ratio of 70 (Fig.4(d)), clockwise rotation  $20^\circ$  with cropping(Fig.4(e)), translation of 30 pixels along x-axis(Fig.4(f)), and scale changing based on scaling factor 0.5(Fig.4(g)), respectively. In Fig. 7(a)-(g) invariant centroid is marked as cross and we can see that although various geometrical attacks are given, each centroid in Fig. 7(a)-(g) are positioned on the similar point which is on the band of hat.



Fig.4. Invariant centroids which are marked as cross: (a)original image;(b)  $3 \times 3$  average filtered;(c) 5% Gaussian noise added;(d) JPEG compressed image with compression ratio of 70;(e)  $20^\circ$  clockwise rotation of image plus cropping;(f) 30 pixels translated along x-axis;(g) scaled based on scaling factor of 0.5.

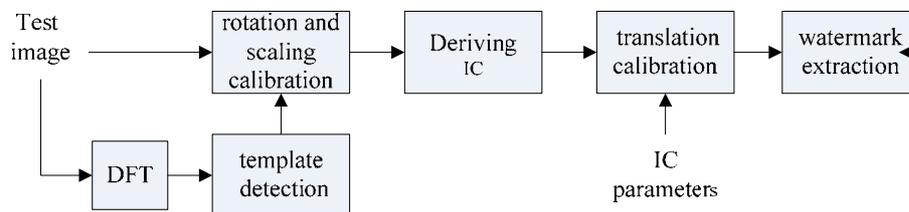


Fig.5. The watermarking detection scheme

IV. WATERMARKING DETECTION SCHEME

The basic idea of the proposed watermark detection scheme, which consists of two parts, the Template detection& image recovery part, and the watermark extraction part as shown Fig.5.

A. Template detection and image recovery

The aim of template detection is to calculate on the rotation  $\theta$  and the scaling  $\rho$ , the detection algorithm is described as follows:

Step1: Perform 2-D DFT to the test image.

Step2: Search on the circle window with radius  $r'$  ( $r' > r$ ,  $r$  is the embedding radius), so as to derive the collection points which have the biggest magnitude values on the local location.

Step3: Perform LPM transformation to all collection points and obtain corresponding points collection  $P_{LMP}$

Step4: Use key  $K_2$  to produce the same points collection  $Q$  as the template embedding process. Perform LPM transformation to all points and obtain corresponding points collection  $Q_{LMP}$ . As the template embedding on the same circle, all points of  $Q_{LMP}$  have the same  $\lambda$  coordinate value  $Q_\lambda$ .

Step5: Classify the collection points  $P_{LMP}$  according to the same  $\lambda$  coordinate, and obtain the child points

collections  $P_{LMPi}$  ( $i=1, 2, 3 \dots$ ).then, set the numbers of each child point collections  $P_{LMPi}$ , save the child point collection  $P_{LMPj}$  that the  $\lambda$  coordinate is value  $P_\lambda$ , and the numbers are most.

Step6: The scaling is Calculate on as follows:  
 $\rho = e^{Q_\lambda - P_\lambda}$

Step7: Point collection  $Q_{LMPi}$  is produced by adding  $\varphi$  coordinate  $0.5i$  ( $i=0, 1, \dots, 719$ ) to all points in points collection  $Q_{LMP}$ , and set the suited points of same  $\varphi$  coordinate between  $Q_{LMPi}$  and  $P_{LMPj}$ . While  $i=k$ , the suited points are most, the rotation angle of the detection image is  $0.5k$  degree.

After the detection image is calibrated by the rotation and scaling parameter through template detection, we derive an invariant centroid  $C' = (C'_x, C'_y)$  from the calibration image. Comparing with the invariant centroid of the original image, the translation of the detection image to the original image is obtained as follow:

$$\begin{aligned} \Delta x &= C'_x - C_x \\ \Delta y &= C'_y - C_y \end{aligned} \tag{9}$$

Finally, The synchronization is implemented, after performing translation calibration to the detection image.

B. Watermark Extraction

Step 1: A 4-level DWT decomposition of the test image is performed using Daubechies-8 filters. According to formula(1), The coefficients are grouped according to wavelet trees as the step 1 of watermark embedding.

Step2: Use the same key  $K_1$  to choose a tree pairs , say tree  $A'_i$  and tree  $B'_i$  for each bit  $w'_i$  to be extracted.

Step3: For each watermark bit  $w'_i$  embedded in tree  $A'_i$  and tree  $B'_i$ , we determine which one is a quantized

tree .In particular, a coefficient  $d_i^\theta(x, y)$  is a watermark coefficient if

$$|d_i^\theta(x, y) / JNd_i^\theta(x, y) - \text{floor}(d_i^\theta(x, y) / JNd_i^\theta(x, y))| \leq 0.25 \tag{10}$$

$JNd_i^\theta(x, y)$  is the JND of coefficient  $d_i^\theta(x, y)$ . We use majority rule in the decision of each watermark bit. We count the number of watermark coefficients in tree A and B. Let the numbers be respectively  $N_A$  and  $N_B$ . If  $N_A > N_B$  then  $w'_i$ , otherwise ,  $w'_i = 0$ .

A threshold value T must be defined to determine if the watermark is present or not into the image. Hence, if the number of correct extracted bits exceeds T, the watermark sequence is extracted correctly from the image. The false alarm probability  $P_{fa}$  for n bits embedded watermark data is given by (11)<sup>[14]</sup>, and the value T must be controlled in order that Pfa is smaller than a predetermined value.

$$P_{fa} = \sum_{i=T}^n \left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{i! (n-i)!}\right) \tag{11}$$

where n is the total number of watermark data bits.

IV. EXPERIMENT RESULTS

Several experiments were performed to verify the validity of the proposed watermarking scheme .A set of gray-level images of  $256 \times 256$  image pixels was used as host images, the simulation results for image ‘‘Lena’’ are described as follows.

A. Imperceptibility

The quality metric is based on the Peak Signal to Noise Ratio (PSNR).The watermarked image in this experiment has PSNR=38.2db which means the watermark is almost imperceptible .This can be also seen in Fig.6 which shows the original and the watermarked image ‘Lena’.



Fig.6 Invisible of watermark : (a)Original image (b) Containing watermark image

B. Robustness

Different sets of tests have been performed to assess the algorithm robustness against lossy image compression, common image-processing operations, and geometric operations. These operations were applied to a watermarked image and then the embedded watermark was extracted. The Bit Error Rate (BER) of the extracted watermark bits (128bits) is used as a measure of the algorithm robustness .

Lossy image compression: The algorithm robustness is examined against JPEG and JPEG2000, For JPEG , quality factor of 40, 50, 70, 90 are used , and the results are shown in Table 1, the number of errors in the watermark extracted from the compressed image is zero. The proposed method can detect the existence of watermark for quality factor greater than 40. Usually for images with quality factor smaller than 40, there are visible artifacts. Even if the detector fails to confirm the existence of watermark, it is apparent that the image has been distorted. The results of attacks using JPEG2000 compression are also shown in table 1, while in JPEG-2000 compression, when the compression is 0.4 bpp or higher, the numbers of errors in the watermarked extracted from the compressed image is zero.

Image-processing: The algorithm robustness is examined against image filtering and noise addition. The watermarked image ‘‘Lena’’ is filtered using average and median filters with increasing window-size. Table 2 reports the obtained results against image filtering .It can be seen that watermarks survive average and median filtering of window size  $3 \times 3$ . The watermarked images are corrupted by adding Gaussian noise with variance 10, 15,20, 30, Table 2 reports the obtained results against adding Gaussian.

Geometric operations: The algorithm robustness against geometric operations, in particular rotation, scaling and cropping, is examined using StirMark 3.1<sup>[9]</sup>. Table 3 reports the obtained results, which are attacked by most common geometrical distortions, and combined attacks, respectively. The experimental results show the watermark robustness of the proposed method against these attacks. Also, a performance comparison between the proposed method and previous works, such as the color histogram method proposed by [15], the histogram oriented watermarking algorithm proposed by[16], the template-based scheme proposed by [17] and the image normalization based scheme proposed by [18]. This comparison includes JPEG compression, scaling, cropping, aspect ratio change, rotation, shearing, Gaussian noise, and median filtering. Table 4 shows the performance comparisons together with watermark detection methods (blind or original image is required) and the watermark data length associated with each scheme. These results show better performance of the proposed method compared with prior methods against most common geometric and signal processing attacks.

Table 1. Bit Error Ratio) versus JPEG and JPEG2000 compression to the image ‘Baboon’

JPEG compression (quality factor)	JPEG2000 compression/(bits per pixel)	BER(%)
90		0.8
70		1.6
50		4.7
40		5.5
	0.70	1.6
	0.60	2.3
	0.40	4.7
	0.30	8.7

Table 2. Bit Error Rate) versus Filtering and adding Gaussian noise in the image ‘Baboon’

Average Filter (size)	Median filter (size)	Added Gaussian noise (Variance)	BER/%
2×2			1.6
3×3			3.1
4×4			11.1
	2×2		1.6
	3×3		3.1
	4×4		15.9
		10	1.6
		15	3.1
		20	4.7
		30	5.5

Table 3. Bit Error Rate ) versus Geometric operations and combined attacks

Attack	BER%
Rotation by 55°	0.8
Cropping 40 %	2.3
Scale 0.75	1.6
Affine Transformation	11.1
Aspect ratio (1.0, 1.2)	1.6
JPEG 70 + Rotation 15 °	7.9
JPEG 70 + Cropping 10 %	6.3
JPEG 70 + median filter 3 x 3	7.1
JPEG70 + Flipping horizontal and vertical.	9.5

VI. CONCLUSION

A robust watermarking algorithm against geometric distortions and common signal processing attacks, The algorithm is based on two method to solve the synchronization of the original watermarking images and test images in the wavelet domain watermarking. One method, which estimates rotation and scaling based on embedding a template in a circle of middle frequency in DFT, One method which estimates translation based on extracting an invariant centroid from a restricted area inside the image. In the embedding process, a watermark is embedded adaptively in low band of DWT domain, according to the conceal quality of Human Visual System (HVS). The experimental results show a better performance compared with the prior methods against most common geometric and signal processing attacks, such as aspect ratio, rotation, cropping, scaling, median filtering and Gaussian noise.

Table 4 Performance Comparison

Comparison	Zheng et al.[17]	Roy et al.[15]	C.H. Lin et al.[16]	M.Cedillo et al.18	Proposed method
JPEG(QF)	10-100	50-100	20-100	20-100	20-100
Scaling	0.6-1.3	1.2-1.4	0.75-1.5	0.4-2	0.3-2.0
Cropping	detected	Up to 60%	Up to 15%	-	Up to 60%
Aspect Ratio	—	—	detected	detected	detected
Rotation(with Autocrop and Scale)	0° -360°	0° -40°	1° - 15°	detected	0° -360°
Shearing	10 columns or 10 rows	—	X5% Y5%	X5% Y5%	X5% Y5%
Median Fitering	detected	—	4×4	3×3	4×4
Gaussian Noise	detected	detected	—	detected	detected
Original Image for detection	Need or exhaustive search	blind	blind	blind	blind
Watermark length	64 bits	256 bits	128 bits	64 bits	128 bits

ACKNOWLEDGMENTS

This work was supported by Guangdong Provincial Science and Technology Planning Project of China (2010B0106003620); Natural Scientific Research Fund of Guangdong China (2011023960) ; Research Fund of

HangZhou Key Lab of E-Business and Information Security;(HZEB201003).

REFERENCE

[1] Thomas, T., Emmanuel, S., Subramanyam, A.V., Kankanhalli, M.S..Joint Watermarking Scheme for

- Multiparty Multilevel DRM Architecture. *IEEE Transactions on Information Forensics and Security*, vol.4, no.4, 2009, pp. 758 – 767
- [2] Shijun Xiang, Jiwu Huang. Invariant Image Watermarking Based on Statistical Features in the Low-Frequency Domain. *IEEE Transactions on Circuits and Systems for Video Technology*, vol.18, No.6, 2008, pp.777-784
- [3] X.Kang, J.Huang, Y.Shi, and Y.Lin. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Transactions on Circuits and Systems for Video Technology*, vol.13, No.8, 2003, pp.776-778.
- [4] N.Johnson, Z. Duric, and S.Jajodia. Recovery of watermarks from distorted images. in *Proc.3rd Int. Workshop Inf. Hiding*, 1999, vol.1768, LNCS, pp.318-332.
- [5] F.Davoine, . Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares. in *Proc. EURASIP Signal Process. Conf.*, 2000, vol.3, pp.493-496.
- [6] P.Dong, J. Brankov, N. Galatsanos, and Y.Yang.. Geometric robust watermarking based on a new mesh model correction approach. in *Proc. IEEE Int. Conf. Image Process.*, 2002, pp.493-496.
- [7] P.Bas, J.-M. Chassery, and B.Macq., Geometrically invariant watermarking using feature points. *IEEE Trans. Image Process.*, vol.11, no.9, pp.1014-1028, Sep.2002.
- [8] M.Barni, . Effectiveness of exhaustive search and template matching against watermark desynchronization. *IEEE Signal Process. Lett.*, vol.12, no.2, pp.158-161, Feb.2005.
- [9] Tang C W and Hang H M. A feature-based robust digital image watermarking scheme. *IEEE Trans. on Signal Processing*, vol, 51, No 4, 2003, pp. 950-959.
- [10] Emir Ganic, Ahmet M. Eskicioglu. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. *Proceedings of the 2004 Workshop on Multimedia and Security*.Magdeburg, Germany: ACM Special Interest Group on Multimedia, 2004, pp.166-174.
- [11] Hartung F, Girod. B. Fast public-key watermarking of compressed vide. In: *Proc.of the IEEE Int. Conf. on Image Processing*, vol, 1, 1997, pp.528-531
- [12] Boo-Soo Kim, Jae-Gark, etc. Robust digital image watermarking method against geometrical attacks, *Real Time Imaging*, 2003, 9: 139-149
- [13] Yuping Hu, Ming Zhang and Dezhi Han, "Image-adaptive watermark based on wavelet transform", *Journal of central china normal university*, vol36, No 4, pp.451-454, 2002
- [14] C.Tang and H.M.Hang. A Feature-Based robust digital image watermarking scheme, *IEEE Trans on signal processing*, vol.51, no.4, 2003, pp.950-959
- [15] Roy, S., and Chang, E.C. Watermarking color histogram. *Proc IEEE Int. Conf. on Image Processing*, Singapore, 2004.
- [16] C.H. Lin, D.Y. Chan, H. Su and W.S. Hsieh. Histogram Oriented watermarking Algorithm: colour image watermarking scheme robust against geometric attacks and signal processing. *IEE Proc.-Vis. Image Signal Process.*, Vol. 153, No. 4, pp. 483-492, 2006.
- [17] Kang, X., Huang, J., Shi, Y. Q., and Lin, Y. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Trans. Circuits Syst. Video Technol.*, 13, (8), pp. 776-786, 2003.
- [18] M. Cedillo, M. Nakano and H. Perez. Robust watermarking to geometric distortion based on image normalization and texture classification. in *Proc IEEE Midwest Symposium CAS 2008*, Knoxville, Tennessee, pp. 245-248.

**Yuping Hu:** Male, born in 1969, he received his B.S. degree in celestial survey from Chinese Academy of Science, China, in 1996 and his Ph.d. degree in computer science from Huazhong University of Science and Technology, Wuhan, China in 2005. He is currently pursuing the postdoctoral research in computer applications from Central South University, Changsha, China.

Dr. Hu is a professor in the Guangdong Province Key Lab of EC Market Application Technology, Guangdong University of Business Studies, Guangzhou, China. His current research interests include digital watermarking, image processing, multimedia and network security.