# A Color Image Watermarking Scheme Resistant against Geometrical Attacks

*Yan XING*[1,2], *Jieqing TAN*[1,2]

[1] School of Mathematics, Hefei University of Technology, Hefei 230009, China
[2] School of Computer and Information, Hefei University of Technology, Hefei 230009, China

xy1128@126.com, jieqingtan@yahoo.com.cn

**Abstract.** *The geometrical attacks are still a problem for many digital watermarking algorithms at present. In this paper, we propose a watermarking algorithm for color images resistant to geometrical distortions (rotation and scaling). The singular value decomposition is used for watermark embedding and extraction. The log-polar mapping (LPM) and phase correlation method are used to register the position of geometrical distortion suffered by the watermarked image. Experiments with different kinds of color images and watermarks demonstrate that the watermarking algorithm is robust to common image processing attacks, especially geometrical attacks.*

## Keywords

Digital watermarking, geometrical attacks, LPM, phase correlation.

## 1. Introduction

With the development of network and multimedia technology, more and more digital multimedia data can be transmitted through Internet. This has made multimedia data vulnerable to various attacks. Watermarking is a kind of important multimedia authentication techniques among today's information security methods. Watermarks, such as text or images, which carry ownership information, are inserted in multimedia data to protect the copyright. Robustness and invisibility are two important features of a watermarking scheme [1].

In recent years, great progress has been made in digital image watermarking technology. Still, most image watermarking schemes cannot effectively resist geometrical attacks such as rotation and scaling, and the resistance to geometrical attacks is still a hotspot and difficulty in this field [2]-[9]. Conventional image watermarking algorithms are sensitive to geometrical distortions. Even a slight geometric distortion may significantly influence the extraction of watermark because the synchronization of watermark is destroyed [10].

To solve the problem, we use the LPM and phase correlation method to estimate the geometric transformation parameters to re-synchronize the watermarked image. The watermark embedding and extraction method adopt the method in [10]. Experimental results indicate that the scheme proposed in this paper is robust to rotation and scaling attacks.

## 2. Log-Polar Mapping

Consider a point $(x, y) \in R^2$and define:

$$x - x_0 = e^{\mu}\cos\theta\,,\ y - y_0 = e^{\mu}\sin\theta \tag{1}$$

where $\mu \in R$, $0 \le \theta \le 2\pi$, and $(x_0,\ y_0)$ are the Cartesian coordinates used as the origin of the log-polar coordinates. One can see that for every point $(x, y)$ there is a point $(\mu,\ \theta)$ that uniquely corresponds to it.

The new coordinate system has the following properties:

- Scaling is converted to a translation in the radial direction

$$(\rho x, \rho y) \leftrightarrow (\mu + \log\rho, \theta)\ . \tag{2}$$

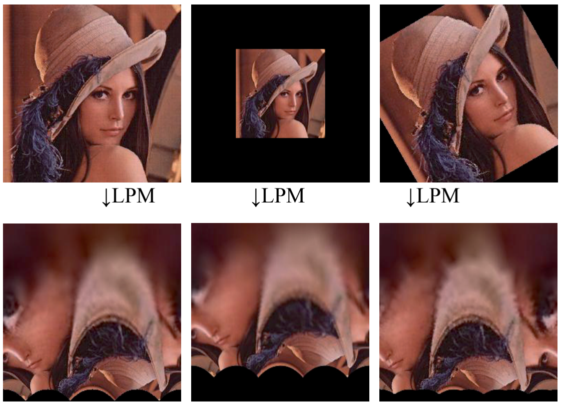
- Rotation on Cartesian coordinates is also converted to a cyclic translation/shift in the angular direction on log-polar coordinates.

$$(x\cos\delta - y\sin\delta, x\sin\delta + y\cos\delta) \leftrightarrow (\mu, \theta + \delta)\,. \tag{3}$$

The value of the image at the nearest valid coordinate point can be estimated by interpolation. Fig. 1 and Fig. 2 exhibit a visual representation of the properties of LPM. In Fig. 1 and Fig. 2, the original image is shown in (a), the scaling- and rotation- attacked images are shown in (b) and (c). LPM results of (a), (b) and (c) are also shown, respectively.

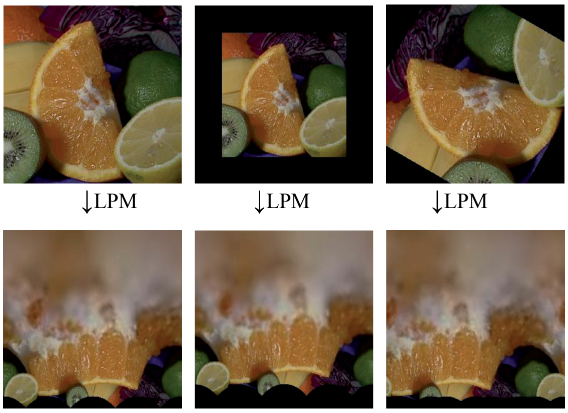
## 3. Phase Correlation

It is widely accepted that phase plays an important, and often crucial role in vision and image representation.



(a) Original (b)Scaled by 0.5 (c)Rotated by ***30***°

**Fig. 1.** Lena and LPM.



(a)Original (b)Scaled by 0.7 (c)Rotated by ***60***°

**Fig. 1.** Fruits and LPM.

In image processing, phase correlation is a fast frequency-domain approach to estimate the relative translatory movement between two images. Phase correlation based methods have been proposed to align two images which are shifted relative to each other [11]-[14], [6].

Given two $M \times N$ input images $f_1(x, y)$ and $f_2(x, y)$, satisfying $f_2(x, y) = f_1(x - x_0, y - y_0)$.

Suppose $F_1(u, v)$ and $F_2(u, v)$ are the discrete 2D Fourier transforms of both images. Then we have

$$F_2(u,v) = e^{-j2\pi\left(\frac{ux_0}{M}+\frac{vy_0}{N}\right)} F_1(u,v) . \tag{4}$$

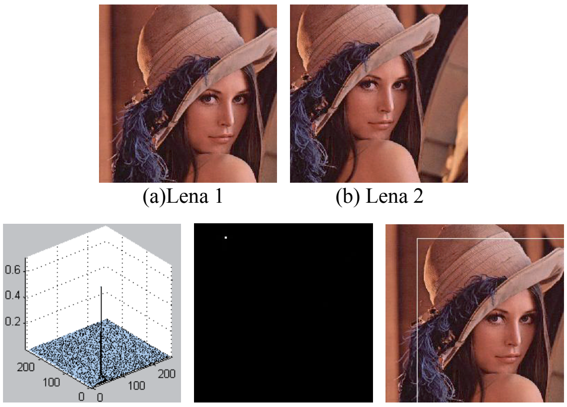
The cross-power spectrum is defined as follows:

$$R(u,v) = \frac{F_1(u,v)F_2^*(u,v)}{\left|F_1(u,v)F_2^*(u,v)\right|} = e^{j2\pi\left(\frac{ux_0}{M}+\frac{vy_0}{N}\right)} \tag{5}$$

where $F_2^*(u, v)$ is the complex conjugate of $F_2(u, v)$. Applying the inverse Fourier transform to R gives the normalized cross-correlation as follows

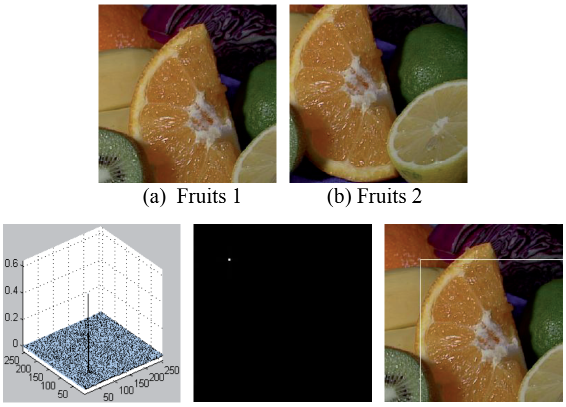
$$r(x,y) = F^{-1}(R(u,v)) = F^{-1} e^{j2\pi\left(\frac{ux_0}{M}+\frac{vy_0}{N}\right)} . \tag{6}$$

The inverse Fourier transform of a complex exponential is a Kronecker delta, i.e., a single peak:



(c) (d) (e)

**Fig. 3.** Phase correlation between Lena images.



(c) (d) (e)

**Fig. 4.** Phase correlation between Fruits images.

$$r(x,y) = \delta\left(x - x_0, y - y_0\right) . \tag{7}$$

Determine the location of the peak in $r$, and it is the translation parameter between two images:

$$\left(x_0, y_0\right) = \arg\max_{(x,y)}(r) . \tag{8}$$

Examples are shown in Fig. 3 and Fig. 4.

## 4. The Proposed Watermarking Scheme and Experiments

The proposed watermarking scheme is based on the work of paper [10], which gives a color watermarking algorithm not only robust to waveform attacks such as Gaussian noise addition, lossy JPEG compression, low pass filtering, etc. due to the use of block-SVD, but also robust to cropping because of the watermark Arnold transformation preprocessing. But as was said in its conclusion, the scheme only survives very small angle rotation. To improve its resistance to geometrical attacks, we add a step before watermark extracting, that is, calculating phase correlation in image LPM domain to estimate the geometrical distortion parameters to resynchronize the watermark position destroyed by geometrical distortion.

Assume that original image $A$ is a RGB color image of size $N \times N$ where $N = 2^n$, watermark $W$ is also a recognizable and meaningful color image of size $M \times M$ where $M = 2^m$, and $n \geq m$. The watermarking procedures can be described as follows:

## 4.1 Watermark Embedding

**(A)** Color watermark preprocessing.

To enhance the security and the robustness to cropping operation, color watermark $W$ is spatially scrambled using Arnold transformation [10] before embedding: $W \Rightarrow \hat{W}$ . We shuffle the color watermark $k$ times, where the parameter $k$ can later be used as the secret key during watermark recovery.

**(B)** Block-SVD of the host color image.

The original color image is divided into $M \times M$ non-overlapping blocks of size $(N/M) \times (N/M)$ pixels. A block is denoted by the location of its starting pixel $(i, j)$. Perform SVD (Singular Value Decomposition) on each block $B_{ij}$ in each RGB channel: $B_{ij} \Rightarrow U_{ij} S_{ij} V_{ij}^H$. The notation $^H$ denotes the conjugate transpose.

**(C)** Watermark embedding.

We add every pixel value of the scrambled watermark $\hat{W}$ to the maximum SV (Singular Value) of every corresponding block obtained from block-SVD on the host image. This can be expressed as $S + \alpha\hat{W}$ , where $S$ is an $M \times M$ matrix composed of all blocks' maximum SVs, $\alpha$ is the scale factor which controls the strength of the watermark to be embedded and $\hat{W}$ is the scrambled watermark.

According to the luminance masking property and texture masking property of the HVS, we can embed watermark signal to host image with different strength factor $\alpha$ to avoid the damage to the visual quality. For simplicity, we select a constant as the scaling factor.

**(D)** In the end, we obtain the watermarked image $A_W$ by inversing the block-SVD transformation:

$$U_{ij}\widetilde{S}_{ij}V_{ij}^H \Rightarrow \widetilde{B}_{ij} \tag{9}$$

where $\widetilde{S}_{ij}$ is obtained by modifying the maximum SV of $S_{ij}$ with the corresponding pixel value of the scrambled watermark with scale factor $\alpha$ and $\widetilde{B}_{ij}$ is the non-overlapping block in the final watermarked image, which will constitute the watermarked image $A_W$ finally.

Of course, the Arnold transformation times $k$ (as secret key) during watermark scrambling, the host image block size $(N/M) \times (N/M)$ and the strength factor $\alpha$ of watermark embedding should be saved in the intermediate file and are required for watermark detection.

## 4.2 Watermark Extraction

Watermark extraction process is the reverse of watermark embedding procedure. A step is added to combat against the geometric attack before watermark extracting. The possibly corrupted watermark $W^*$ could be extracted as follows:

**(A)** First, calculate phase correlation between LPM domain of the possibly attacked watermarked image $A_W^{*\prime}$ and LPM of the original image $A$, from which we can estimate the geometrical distortion parameters including rotation angle and scaling ratio. If the watermarked image was rotated or scaled, we can retrieve it according to the geometrical distortion parameters to resynchronize the watermark position destroyed by geometrical distortion. $A_W^{*\prime} \Rightarrow A_W^*$, $A_W^*$ still possibly underwent waveform attacks.

**(B)** Then, the possibly waveform attacked watermarked image $A_W^*$ is partitioned into non-overlapping blocks of size $(N/M) \times (N/M)$ pixels. Then block-SVD is performed in each RGB channel:

$$\widetilde{B}_{ij}{}^* \Rightarrow U_{ij}{}^* \widetilde{S}_{ij}{}^* V_{ij}{}^{*H} . \tag{10}$$

**(C)** Maximum SV of every block $\widetilde{S}_{ij}{}^*$ is picked up to constitute a new matrix $\widetilde{S}^*$ of size $M \times M$. The possibly distorted scrambled watermark $\hat{W}^*$ can be obtained by computing $(\widetilde{S}^* - S)/\alpha \Rightarrow \hat{W}^*$ .

**(D)** At last, the spatially scrambled watermark is once again permuted using Arnold transformation with the permutation times $P - k$, where $P$ is the Arnold transformation period of $M \times M$ matrix. The possibly distorted watermark $W^*$ in original form is thus obtained.

Experimental results and explanation are shown in Figs. 5, 6, 7 and Tab. 1.

The similarity of original image $A$ and watermarked image $A_W$ can be measured by peak signal-to-noise ratio (PSNR), and PSNR in this paper is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{L^2}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[A(i,j) - A_W(i,j)\right]^2}\right)(\text{dB}) \tag{11}$$

where $M \times N$ is the input image size, and $L$ is the maximum fluctuation in the input image data type. For example, if the image has a double-precision floating-point data type, then $L$ is 1. If it has an 8-bit unsigned integer data type, $L$ is 255, etc.

The degree of similarity between the extracted watermark $W^*$ and the original watermark $W$ may be expressed by the normalized cross-correlation (NC):

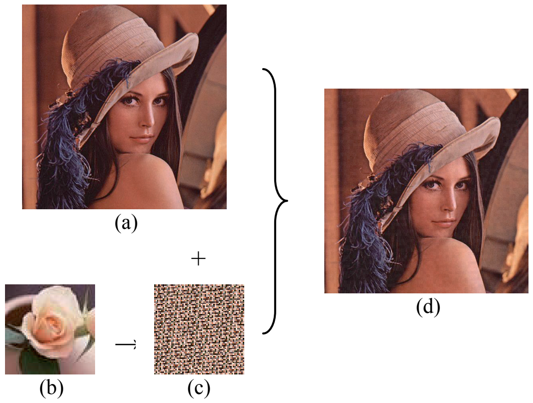


**Fig. 5.** (a)Lena of size 512 × 512 as host image. (b) Flower of size 64 × 64 as watermark. (c)The scrambled watermark Flower after 9 times permutation. (d)The watermarked image Lena with $\alpha = 0.3$ (PSNR = 33.4874).

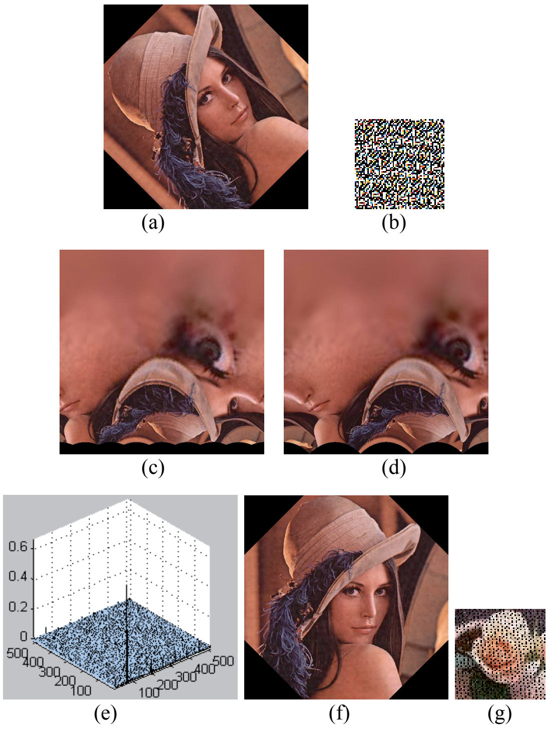


**Fig. 6.** (a)Rotated watermarked image with cropping. (b) Watermark extracted from (a) with NC = 0.4840. (c) LPM of (a). (d) LPM of the original image. (e) Phase correlation between (c) and (d). The peak is 0.6571 at (1,65) from which we can calculate the rotation angle is 45°, and the scaling ratio=1. (f)The resynchronized watermarked image according to the geometrical transformation parameters from (e). (g) The extracted watermark from (f) with NC=0.8557.

$$NC(W,W^*)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{ij}-\overline{W}\right)\left(W_{ij}^*-\overline{W^*}\right)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{ij}-\overline{W}\right)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(W_{ij}^*-\overline{W^*}\right)^2}} \qquad (12)$$

where

$$\overline{W}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}W_{ij}\ ,$$

| Rotation angle (degree) | Peak position | Estimated angle (degree) |
|---|---|---|
| 0 | (1,1) | 0 |
| 10 | (1,15) | 9.8438 |
| 22 | (1,32) | 21.7969 |
| 30 | (1,44) | 30.2344 |
| 45 | (1,65) | 45 |
| 60 | (1,86) | 59.7656 |
| 78.5 | (1,113) | 78.75 |
| 90 | (1,129) | 90 |
| 120 | (1,172) | 120.2344 |
| 135 | (1,193) | 135 |
| 150 | (1,214) | 149.7656 |
| 180 | (1,257) | 180 |
| 270 | (1,385) | 270 |

**Tab. 1.** Rotation (with cropping) angle estimation (image size 512 × 512).

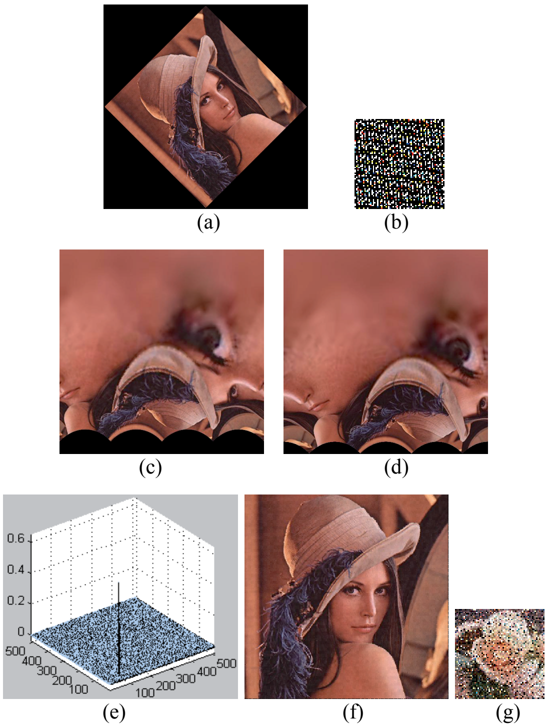


**Fig. 7.** (a)The watermarked image which was scaled by 0.7 and rotated by 45° (PSNR = 9.4150). (b) Watermark extracted from (a) with NC = 0.3772. (c) LPM of (a). (d) LPM of the original Lena image. (e) Phase correlation between (c) and (d). The peak is 0.6141 at (32,65) from which we can calculate the rotation angle is 45°, and the scaling ratio = 0.7000. (f)The resynchronized watermarked image according to the geometrical distortion parameters from (e). (g) The extracted watermark from (f) with NC = 0.8565.

$$\overline{W^*}=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}W_{ij}^*\ ,$$

and $M \times N$ is the size of watermark image.

The geometrical distortion parameters estimation equations can be deduced from equations given in Sec. 2 and 3. For example, the rotation angle can be calculated by $(y_0-1)/N\times 360$.

To verify the robustness of the proposed scheme, extensive experiments have been carried out, including traditional signal processing attacks and geometric attacks. We also compared our results with those of [15]. Simulation results on the signal processing attacks and geometric attacks are listed in Tab. 2.

| Attack Type | | Similarity $(W,W^*)$ | | |
|---|---|---|---|---|
| | | Lee's method | Original method in [10] | Proposed method |
| No attack | | 0.727 | 1 | 1 |
| median filtering | 2X2 | 0.611 | 0.8773 | 0.8773 |
| | 3X3 | 0.629 | 0.9672 | 0.9672 |
| | 4X4 | 0.609 | 0.8473 | 0.8473 |
| Gaussian filtering | ([3,3],0.5) | 0.671 | 0.9897 | 0.9897 |
| Lossy JPEG compression (Quality factor) | 80 | 0.660 | 0.9648 | 0.9648 |
| | 70 | 0.623 | 0.9537 | 0.9537 |
| | 60 | 0.579 | 0.9361 | 0.9361 |
| | 50 | 0.532 | 0.9100 | 0.9100 |
| | 40 | 0.477 | 0.8776 | 0.8776 |
| Centered Cropping | 5% | 0.703 | 0.9633 | 0.9633 |
| | 25% | 0.621 | 0.7985 | 0.7985 |
| | 50% | 0.446 | 0.5870 | 0.5870 |
| Rescaling (Estimated scaling ratio) | 1.5X | 0.524 | 0.9984 | (1.4945X)<br>0.9984 |
| | 1.3X | 0.594 | 0.9714 | (1.2953X)<br>0.9714 |
| | 1.1X | 0.606 | 0.9221 | (1.1004X)<br>0.9221 |
| | 0.9X | 0.605 | 0.9807 | (0.90162X)<br>0.9807 |
| | 0.8X | 0.539 | 0.9443 | (0.80361X)<br>0.9443 |
| | 0.7X | 0.472 | 0.9058 | (0.69996X)<br>0.9058 |
| Rotation with cropping (Estimated rotation angle) | 0.25° | 0.682 | 0.8950 | (0°)<br>0.8950 |
| | 0.5° | 0.673 | 0.8037 | (0.70313°)<br>0.8898 |
| | 0.75° | 0.662 | 0.7335 | (0.70313°)<br>0.9615 |
| | 1° | 0.643 | 0.6770 | (0.70313°)<br>0.8536 |
| | 2° | 0.550 | 0.5585 | (2.1094°)<br>0.9322 |
| | 5° | 0.641 | 0.5211 | (4.9219°)<br>0.9283 |
| | 10° | 0.600 | 0.4962 | (9.8438°)<br>0.8750 |
| | 15° | 0.538 | 0.4985 | (14.7656°)<br>0.8347 |
| | 30° | 0.514 | 0.4825 | (30.2344°)<br>0.8079 |
| | 45° | 0.550 | 0.4840 | (45°)<br>0.8557 |

**Tab. 2.** Comparison of Lee's method [15], the original method in [10] and the proposed improved scheme.

## 5. Conclusions

In this paper, we give a new watermarking scheme that uses the log-polar mapping and phase correlation method to get the geometric transform parameters. The geometrically distorted image can be realigned with original image accordingly. The test results demonstrate that the scheme is very reliable in geometric transform parameters calculation, and very robust to both geometric attacks and waveform attacks. As for our future work, we will improve our algorithm to give a more accurate computation of the geometric transform parameters.

## Acknowledgements

Research described in the paper was financially supported by the National Natural Science Foundation of China under Grant No. 60773043 and No. 60473114, the Doctoral Program Foundation of Ministry of Education of China under Grant No. 20070359014, Anhui Provincial Natural Science Foundation under Grant No. 070416273X, ARO (DAAD19-03-1-0375), USA, the Science Research and Development Foundation of Hefei University of Technology under Grant No. 2009HGDXJ0054 and in part by the Research Funds for Young Innovation Group, Education Department of Anhui Province under Grant No. 2005TD03.

## References

[1] SWANSON M. D., KOBAYASHI, M., TEWFIK, A. H. Multimedia data-embedding and watermarking technologies. *Proceedings of the IEEE*, 1998, vol. 86, no.6, p. 1064 − 1087.

[2] O'RUANAIDH, J. J. K., PUN, T. Rotation, scale and translation invariant digital image watermarking. In *Proceedings of the 1997 International Conference on Image Processing*. Washington DC (USA), 1997, vol.1, p. 536 − 539.

[3] ÓRUANAIDH, J. J. K., PUN, T. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 1998, vol. 66, no. 3, p. 303-317.

[4] AGUNG I.W., SWEENEY P. Method for combating random geometric attack on image watermarking. *Electronics Letters*, 2001, vol.37, no.7, p. 420 − 421.

[5] KIM B.S., et al. Robust digital image watermarking method against geometrical attacks. *Real-Time Imaging*, 2003, vol. 9, no. 2, p. 139 − 149.

[6] ZHENG, D., ZHAO, J., SADDIK, A. EL. RST invariant digital image watermarking based on log-polar mapping and phase correlation. *IEEE Transactions on Circuits and Systems for Video Technol*ogy. , 2003, vol. 13, no. 8, p. 753 – 765 (Special Issue on Authentication, Copyright Protection and Information Hiding).

[7] ZHENG, D., LIU, Y., ZHAO, J. RST invariant digital image watermarking based on a new phase-only filtering method. *Signal Processing*, 2005, vol. 85, no. 12, p. 2354 − 2370.

[8] LICKS, V., JORDAN, R. Geometric attacks on image watermarking systems. *IEEE Multimedia*, 2005, vol.12, no.3, p. 68 − 78.

[9] RIDZOŇ, R., LEVICKÝ, D. Robust digital watermarking based on the log-polar mapping. *Radioengineering*, 2007, vol. 16, no. 4, p. 76 − 81.

[10] XING, Y., TAN, J. Q. A color watermarking scheme based on block-SVD and Arnold transformation. In *Proceedings of the 2$^{nd}$ Workshop on Digital Media and its Application in Museum & Heritage.* Chongqing (China), 2007, p. 3 - 8.

[11] KUGLIN C.D., HINES D.C. The phase correlation image alignment method. In *Proc. of the IEEE International Conference on Cybernetics and Society, San Francisco, CA, USA*, 1975, p. 163 − 165.

[12] CASTRO, E. D. E., MORANDI, C. Registration of translated and rotated images using finite fourier transforms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1987, vol. 9, no. 5, p. 700 − 703.

[13] BRWON, L. G. A survey of image registration techniques. *ACM Computing Surveys*, 1992, vol. 24, no. 4, p. 325 − 376.

[14] REDDY, B. S., CHATTERJI, B. N. A FFT-based technique for translation, rotation, scale-invariant image registration. *IEEE Transactions on Image Processing*, 1996, vol. 5, no. 8, p. 1266 − 1271.

[15] LEE, H. Y., KIM, H. S., LEE, H. K. Robust image watermarking using local invariant features. *Optical Engineering*, 2006, vol. 45, no. 3, p. 9056 − 9064.

## About Authors...

**Yan XING** was born in Anhui (China) in 1977. She graduated from the School of Computer Science, Northeast Normal University at Changchun, China. She is now a PhD. student at the School of Computer and Information, Hefei University of Technology and a lecturer at the School of Mathematics, Hefei University of Technology. Her research is focusing on multimedia and digital image processing.

**Jieqing TAN** was born in Anhui (China) in 1962. He got his computational mathematics PhD degree from Jilin University in 1990, and worked in Fachbereich Mathematik, Universität Dortmund, Germany as a post-doctoral from 1992 to 1993. He is professor of Hefei University of Technology, director of Inst. of Applied Mathematics from 1996 and supervisor of doctoral students from 1998. His research interests include nonlinear numerical approximation, scientific computing, computer aided geometric design, computer graphics and digital image processing.