# 기하학적 공격에 강한 고신뢰성 SVD 기반 워터마킹방안

융 녹 투이 덩, 손원
경희대학교
banhbao1986@khu.ac.kr, wsohn@khu.ac.kr

# A Reliable SVD Based Watermarking Scheme Resistant to Geometric Attacks

Luong Ngoc Thuy Dung, Won Sohn
Kyung Hee University

## Abstract

We proposed an improved reliable SVD-based watermarking scheme resistant to geometric attacks while having high fidelity with no false-positive problem. Principal components of a watermark image are embedded into singular values of LL, LH, HL, and HH sub-bands of a transformed cover image by RDWT(redundant discrete wavelet transform) with optimal scale factors. Each scale factor is generated by trading-off fidelity and robustness using Differential Evolution (DE) algorithm. Zernike Moment (ZM) is used to estimate the geometric distortion and to correct the watermarked image before extracting watermark. The proposed scheme improves fidelity and robustness of existing reliable SVD based watermarking schemes while resisting to geometric attacks.

Index Terms – watermarking, SVD, principal component, RDWT, Zernike moment.

## 1. Introduction

Currently multimedia contents are distributed more and more over the Internet, and protecting their legal copyright ownership becomes gradually important. There have been many studies about using digital watermarks to solve the protection problem [1-5], and contents owners can embed their logos or personal information into the multimedia contents to protect their copyrights.

Several watermarking schemes have been proposed to resist geometric attacks. Ruanaidh and Pun proposed a watermarking scheme based on Fourier-Melilin transform (FMT) to resist the geometric attacks such as rotation, scaling and translation [6]. The scheme decreased the image quality steeply. Kim and Lee suggested a semi-blind watermarking scheme based on the invariant image feature vector using Zernike moments [7]. It needs a lot of information to extract watermark and has high computational complexity. Fazli and Moeini proposed a watermarking scheme combining DWT, DCT and SVD domains to resist geometric attacks [8]. The scheme proposed an inventional synchronization technique to recover geometrically attacked image by detecting desired image corners, but it has a false positive problem.

Reliable SVD-based watermarking schemes are proposed to overcome the problem [9-11], but they have low performance in fidelity and robustness, and weak robustness to geometric attacks.

In this paper, we proposed an improved reliable SVD-based watermark scheme which can resist to geometric attacks without a false positive problem. Principal component of a watermark image is embedded into singular values decomposed from the LL, LH, HL, and HH sub-bands of the central part of the cover image with optimal scale factors. Moreover, we use different scale factors for each sub-band. The differential evolution algorithm (DE) is applied adaptively to obtain the four optimal scale factors by considering robustness and fidelity. Zernike Moment (ZM) is used to estimate the geometric distortion and correct the watermarked image before extracting watermark.

The paper is organized as follows: in section 2, the background of Zernike Moment is reviewed. The proposed scheme based on RDWT/SVD is illustrated in section 3, and section 4 shows the experimental results and the comparison with existing systems.

## 2. Zernike moment

Zernike Moment (ZM) is popularly used in image processing, pattern recognition [12], and it is insensitive to geometrical attacks such as rotation and scaling. The geometrically attacked image can be corrected by using ZM.

The form of complex polynomials which are introduced by Zernike and form a complete orthogonal set over the interior of the unit circle is defined as

$$V_{nm}(x,y) = V_{nm}(r,\theta) = R_{nm}(r)e^{jm\theta}, \qquad (1)$$

where $r = \sqrt{x^2+y^2}$, $\theta = \tan^{-1}\left(\frac{y}{x}\right)$, $n$ is a nonnegative integer, and $m$ is an integer subject to constraints $n-|m|$ even, $|m| \le n$. $R_{nm}(r)$, radial polynomial is defined as

$$R_{nm}(r) = \sum_{s=0}^{\frac{(n-|m|)}{2}} (-1)^s \cdot \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!} r^{n-2s}. \qquad (2)$$

ZMs are the projection of the image function $f(x,y)$ onto the orthogonal basis polynomials. The ZM of order $n$ with $m$ repetition is defined as

$$z_{n,m} = \frac{n+1}{\pi}\sum_x\sum_y f(x,y) \times V_{nm}^*(x,y). \qquad (3)$$

### 2.1 Rotation correction

If an image has been rotated by $\varphi$ degrees, the ZM connection between the original image and the rotated image becomes

$$z'_{nm} = z_{nm}e^{-jm\varphi} \qquad (4)$$

and the angle $\varphi$ can be computed by

$$\varphi = \frac{\arg(z'_{nm}) - \arg(\mathrm{z_{nm}})}{m}. \qquad (5)$$

### 2.2 Scaling correction

Let $f\left(\frac{x}{a},\frac{y}{a}\right)$ represent a scaled version of the original image $f(x,y)$. The ZM connection between the magnitudes of original image and the attacked watermarked image are obtained as given

$$|z'_{nm}| = a^2|z_{nm}|, \qquad (6)$$

And the scale factor can be computed by

$$a = \sqrt{\frac{|z'_{nm}|}{|z_{nm}|}}. \qquad (7)$$

## 3. Proposed Scheme

The proposed scheme is based on RDWT, SVD, DE and ZM, and its embedding and extraction processes are illustrated as follows.

### A. Embedding process

(i) Apply RDWT to the $\frac{N}{2}\times\frac{N}{2}$ central part of the cover image A, and define each sub−band as $A^i$, $i = LL, LH, HL, HH$.
(ii) Apply SVD to $A^i$ and the $M\times L$ watermark image $W$ to get

$$A^i = U^iS^i\left(V^i\right)^T, W = U_\psi S_\psi V_\psi^T = P_w V_\psi^T \qquad (8)$$

where $M\times L = 2N$, $P_w = U_\psi S_\psi$ is a principal component of $W$. The matrix $P_w$ is mapped into a vector $p_W$, and $p_W$ is partitioned into 4 vectors, $\boldsymbol{p}_W^i, i = LL, LH, HL, HH$.
(iii) Modify the singular values of $A^i$ by embedding $\boldsymbol{p}_W^i$ to update singular values of each sub−band,

$$\lambda_j^i = \lambda_j^i + \alpha_i p_W^i(j) \qquad (9)$$

where $p_W^i(j)$ is a j$^{\text{th}}$ element of $p_W^i$.
(iv) Obtain the modified DWT coefficients by

$$B^i = U^iS_W^i\left(V^i\right)^T \qquad (10)$$

where $S_W^i = \mathrm{diag}\left(\lambda_1^i, \lambda_2^i, \cdots, \lambda_{N/2}^i\right)$.
(v) Obtain the watermarked image $A_W$ by applying the inverse RDWT to $B^i$.

### B. Extraction process

First, we apply ZM to the watermarked image to apply geometric attacks and correct it into the right form $A_W^*$.
(i) Apply RDWT to the central part of the received watermarked image $A_W^*$ to decompose it into four sub−bands, $A_W^{*i}$.
(ii) Subtract each sub−band of cover image from $A_W^{*i}$:

$$A_1^i = \left(A_w^{*i} - A^i\right). \qquad (11)$$

(iii) Obtain the principal component from $A_1^i$:

$$P_{W,i}^* = \frac{\left(U^i\right)^T A_1^i V^i}{\alpha_i}. \qquad (12)$$

(iv) The extracted principal component of watermark image, $P_W^*$ is obtained through $P_{W,i}^*$.
(v) Get the extracted watermark image by

$$W^* = P_W^* V_\psi^T. \qquad (13)$$

The DE algorithm [13] is applied to find out the nearest optimal scale factors $\alpha_i$'s in (9) which give the maximum objective function $f$.

$$\max f = \frac{\sum_{k=1}^{\mathrm{num}} \mathrm{NC}(W, W_k^*) + \mathrm{NC}(A, A_W)}{\mathrm{num}} \qquad (14)$$

where $\mathrm{NC}(Y,Z)$ denotes the normalized correlation value between $Y$ and $Z$, and num is the number of attacks.

## 4. Experimental Results

We use 'Lena' image with a 512×512 resolution as a cover image, and 'cameraman' image with a 32×32 resolution as a watermark image as shown in Fig. 1. The watermarked image is tested against several attacks, and the attacks include salt and pepper noise (Noise density, $\mathrm{N} = 0.001$), Gaussian noise $\left(\mu = 0, \sigma^2 = 0.005\right)$, speckle noise $(\mathrm{N} = 0.001)$, Gaussian filter (3×3), JPEG compression (Q=50, 70), and geometric attacks. Fig. 1(d) shows that the PSNR of the watermarked image is 40 dB.

We use the DE algorithm to find out the optimal scale factors $\alpha_i$ which gives the best fidelity and robustness as shown in Table 1. Table 1 also shows robustness of the proposed scheme, Guo's [11] and Jain's schemes [9] to common attacks for PSNR=40 dB. It is observed clearly that our proposed scheme shows stronger robustness than the other schemes for most of attacks.

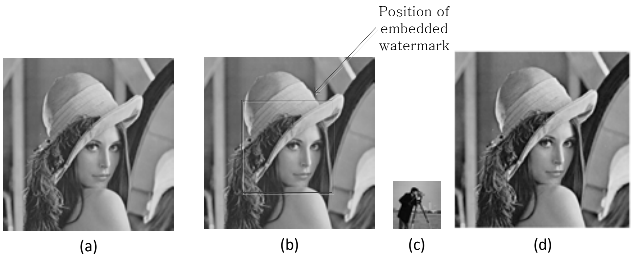

Figure 1. (a) Cover image; (b) Position of embedded

watermark; (c) watermark image; (d) watermarked image.

Through Table 2, it can be observed that the proposed scheme achieves the strongest robustness under rotation attack for except 90° rotation attack but Guo's and Jain's schemes show a little better robustness for 90° rotation attack than the proposed scheme. For Guo's and Jain's schemes, the cropping rotation leads to losing some data of the watermarked image and the embedded principal component of watermark. For the scaling attack Guo's scheme shows the best robustness and the Jain's scheme the worst robustness. The proposed scheme shows moderate robustness for the attack, and the robustness is stronger when the scaling factor is greater than 1.

Table 1. Comparison among the proposed scheme, Guo's and Jain's schemes for common attacks. ($\alpha_1 = -0.4959$, $\alpha_2 = -5.2342$, $\alpha_3 = 9.7828, \alpha_4 = 8.4992$)

| | Proposed scheme | Guo | Jain |
|---|---|---|---|
| Salt and pepper | **0.9466** | 0.8742 | 0.4478 |
| Gaussian noise | **0.9300** | 0.7159 | 0.6426 |
| Speckle noise | **0.9467** | 0.8812 | 0.1467 |
| Gaussian filter | 0.8467 | **0.9084** | 0.5400 |
| JPEG Q=50 | **0.8776** | 0.8722 | 0.1830 |
| JPEG Q=70 | 0.9223 | **0.9395** | 0.2705 |

Table 2. Comparison among the proposed scheme, Guo's and Jain's schemes for geometric attacks.

| Attacks | | Proposed scheme | Guo | Jain |
|---|---|---|---|---|
| Rotation | 30° | **0.9232** | 0.0609 | 0.1913 |
| | 45° | **0.9222** | 0.0207 | 0.1979 |
| | 60° | **0.9241** | 0.0181 | 0.2070 |
| | 90° | 0.9512 | **0.9896** | 0.9578 |
| Scaling | 0.5 | 0.6775 | **0.9782** | 0.0192 |
| | 0.85 | 0.8939 | **0.9868** | 0.2541 |
| | 1.5 | 0.9268 | **0.9885** | 0.5193 |
| | 2.0 | 0.9253 | **0.9887** | 0.5130 |

## 5. Conclusion

This paper proposed a new scheme resisting to geometric attacks, and its robustness to the common attacks is better than the existing reliable SVD-based watermark schemes for most of attacks. The proposed scheme shows the best robustness for the rotation attack, but it shows moderate robustness for the scaling attack. The scheme embedded the principal component of the watermark image into singular values of the four DWT sub-bands: LL, LH, HL, and HH with four optimal scale factors obtained by the DE algorithm, and it improves fidelity and robustness of the reliable SVD based watermarking schemes without any false-positive problem. Moreover, using Zernike Moment helps our scheme to resist geometric attacks.

## 6. References

[1] I. J. Cox, et al, "Secure spread spectrum watermarking for multimedia", IEEE Trans. on Image Processing, 6(12):1673-1687, 1997.

[2] C. H. Huang, J.-L. Wu, "Attacking Visible Watermarking Schemes", IEEE Transactions on Multimedia, Vol.6, No.1, February 2004.

[3] P. Dong, *et al*, "Digital Watermarking Robust to Geometric Distortions," IEEE Transactions on Image Processing, Vol.14, No.12, December 2005.

[4] M. Alghoniemy, A. H. Tewfik, "Geometric Invariance in Image Watermarking", IEEE Transactions on Image Processing, Vol.13, No.2, February 2004.

[5] C. H. Huang, S. C. Chuang, J. L. Wu, "Digital-Invisible-Ink Data Hiding Based on Spread-Spectrum and Quantization Techniques", IEEE Transactions on Multimedia, Vol.10, No.4, June 2008.

[6] O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking", Signal Processing, Vol 66, pp. 303-317, 1998.

[7] H. S. Kim, H. K. Lee, "Invariant Image Watermarking Using Zernike Moments, IEEE Transactions on Circuits and System for Video Technology 13 (2003).

[8] S. Fazli, M. Moeini, "A Robust Image Watermarking Method Based On DWT, DCT, and SVD Using A New Technique For Correction of Main Geometric attacks", Optik 127 (2016) 964-972.

[9] C. Jain, S. Arora, P. K. Panigrahi, "A Reliable SVD based Watermarking Scheme," August 2008.

[10] S. R. Moulick, S. Arora, C. Jain, P. K. Panigrahi, "Reliable SVD Based Semi-Blind and Invisible Watermarking Schemes," 6 Mar 2015.

[11] J. M. Guo, H. Prasetyo, "False-positive-free SVD-based image watermarking", J. Vis. Commun. Image R.25 (2014) 1149-1163.

[12] A. Khotanzad, Y. H. Hong, "Invariant Image Recognition by Zernike Moments", IEEE Transactions on Pattern Analysis and Machine Intelligence, 1990.

[13]. R. Storn, K. Price, "Differential Evolution – A simple and Efficient Heuristic for Global Optimization over Continuous Spaces", Journal of Global Optimization 11 (4) (1997) 341-359.