소유권 확인을 위한 향상된 고신뢰성 SVD 기반 워터마킹기법

융 녹 투이 덩, 손원
경희대학교

banhbao1986@khu.ac.kr, wsohn@khu.ac.kr

Improved Reliable SVD-Based Watermark Scheme For Ownership Verification

Luong Ngoc Thuy Dung, Won Sohn
Kyung Hee University

Abstract

We propose a new reliable SVD-based watermarking scheme having high fidelity and strong robustness with no false-positive problem. Each column of the principal component of a watermark image is embedded into singular values of LL, LH, HL and HH sub-bands of cover image with different scale factors. Each scale factor is optimized by trading-off fidelity and robustness using Differential Evolution (DE) algorithm. The proposed scheme improves fidelity and robustness of existing reliable SVD based watermarking schemes without any false-positive problem.

Index Terms – watermarking, reliable SVD, DWT, principal component, Differential Evolution.

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.

Singular value decomposition (SVD) is widely used in digital watermarking schemes because its features are not affected much by common attacks, and there are many studies about hybrid usages of SVD and transformation techniques for digital watermarking applications. E. Ganic *et al.* [6] and G. Bhatnagar *et al.* [7] proposed a scheme of embedding singular values of the watermark image into the singular values of the cover image based on DWT. The schemes shows high fidelity but they are not robust to general attacks by adversaries. Chih-Chin Lai and Cheng-Chih Tsai proposed a scheme of embedding watermark image directly into the singular values of the DWT transformed cover image to improve the false positive problem [8]. Nasrin et al. applied SVD to the RDWT transformed cover image [9], and they achieved better fidelity and robustness to general attacks than the works using DWT by using more data, but their work is not robust to noise addition attack and has a computational complexity.

The previously mentioned studies [6–9] are similar to each other in the point that singular values are employed in the embedding and extracting processes. The singular values are rarely changed to a small change in image intensity and the values are unique to each image, but they are not much different among different images. Therefore a scheme using singular values can cause the false positive problem which adversaries can extract their fake watermark images to prove their copyright ownership. If adversaries use the singular values from the watermarked image and combine them with the singular vectors of the fake watermark image, they can extract the fake watermark image successfully. Jain et al. proposed a reliable SVD based watermarking scheme without false-positive problem by embedding principal component of the watermark image into the cover image [10-11]. Using this scheme, only a set of right singular vectors are required to extract a watermark image at the detector. However, the drawback of this scheme is its low performance of fidelity and robustness. Guo *et al.* [12] proposed a scheme based on Jain *et al.* scheme to avoid the false-positive problem by embedding principal component of watermark image directly into the cover image. The DWT LL sub-band is divided into several blocks and the maximal singular values of each block are chosen to embed the principal component of watermark image. Finding the optimal scale factor is also a drawback of this scheme.

In this paper, we proposed an improved reliable SVD-based watermark scheme based on DWT and SVD. The scheme embeds the principal component of the watermark image into singular values of four DWT sub-bands: LL, LH, HL, and HH. Moreover, we use a different scale factor for each sub-band. The differential evolution (DE) algorithm is used adaptively to obtain four optimal scale factors by considering robustness and fidelity.

The paper is organized as follows: in section 2, the reliable SVD-based algorithm and the problem to solve through this study are presented. The proposed scheme based on DWT/SVD is illustrated in section 3, and section 4 shows the experimental results and the comparison with existing systems.

2. Reliable SVD-Based Watermarking Algorithm and Problem Formulation

The reliable SVD-based watermarking scheme was first proposed by Jain *et al.* to overcome the false-positive problem. The principal component of the watermark image is embedded into the singular values of the cover image. By using the scheme, only a set of singular vectors are required to extract the watermark image.

A. Embedding process

i) Apply SVD to cover image A:

$$A = USV^T \tag{1}$$

ii) Apply SVD to watermark image W:

$$\mathrm{W} = \mathrm{U_w S_w V_w^T} = A_{Wa}\mathrm{V_w^T} \tag{2}$$

where $\mathrm{A_{Wa}} = \mathrm{U_w S_w}$ is known as a principal component.

iii) Embed A_{Wa} into a diagonal matrix S of the cover image and get the watermarked image $\mathrm{A_w}$:

$$\mathrm{S_1} = \mathrm{S} + \alpha \mathrm{A_{Wa}} \tag{3}$$

$$\mathrm{A_w = US_1V^T} \tag{4}$$

B. Extraction process

i) Subtract the cover image from the distorted watermarked image, $\mathrm{A_w^*}$:

$$A_1 = A_w^* - A \tag{5}$$

ii) Extract the principal component from $\mathrm{A_1}$:

$$A_{wa}^* = \frac{U^{-1}A_1(V^T)^{-1}}{\alpha} \tag{6}$$

iii) Recover watermark image $\mathrm{W^*}$:

$$W^* = A_{wa}^* V_w^T \tag{7}$$

C. Problem formulation

It is observed that the reliable SVD-based watermarking algorithm does not have a false positive problem as shown in Figure 1. Adversaries cannot extract a fake watermark image as shown in Figure 1.e.

Although the reliable SVD watermark scheme overcomes the false-positive problem, it shows not high fidelity and not strong robustness as shown in Table 1. The principal component of the watermark image is embedded into the singular values of the cover image, and the updated singular values are used directly to modify the watermarked image. Because of that, it decreases fidelity greatly. To improve the fidelity, it is necessary to decrease the scale factor α in an embedding process, but it will weaken robustness as shown in Table 1. Through our study we would like to improve both of fidelity and robustness.

3. Proposed Scheme Based on DWT/SVD and DE

A. Embedding process

(i) Apply DWT to cover image A, and define each sub-band as A^i , $i = LL, LH, HL, HH$.

(ii) Apply SVD to A^i and watermark image W:

$$A^i = U^i S^i \left(V^i\right)^T ; W = U_\psi S_\psi V_\varphi^T = P_W V_\varphi^T \tag{8}$$

where $\mathrm{P_w = U_\psi S_\psi}$ is a principal component of W.

(iii) Modify the singular values of the cover image $(\lambda_j^i), j = 1,2, \cdots ,2N$ by embedding P_w to update singular values of the four sub-bands, S_W^i.

$$\lambda_j^i = \lambda_{0,j}^i + \alpha_i P_{w,j} \ . \tag{9}$$

(iv) Obtain the modified DWT coefficients by

$$\left(A^i\right)^+ = U^i S_W^i \left(V^i\right)^T . \tag{10}$$

(v) Obtain the watermarked image A_W by applying the inverse DWT to $\left(A^i\right)^+$.

B. Extraction process

(i) Apply DWT to the received watermarked image $\mathrm{A_W^*}$ to decompose it into four sub-bands, A_W^{*i}.

(ii) Subtract four sub-bands of cover image from the distorted watermarked image:

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

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

$$P_{W,j}^* = \frac{\left(\left(U^i\right)^{-1} A_1^i \left(\left(V^i\right)^T\right)^{-1}\right)}{\alpha_i} \tag{12}$$

(iv) The extracted principal component of watermark image, $\mathrm{P_W^*}$ is obtained through $\mathrm{P_{W,j}^*}$.

(v) Get the extracted watermark image by

$$W^* = P_W^* V_\varphi^T . \tag{13}$$

The DE algorithm [15] is applied to find out the near optimal scale factors α_i in Eq.9 which give the maximum objective function f.

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

where NC denotes the two-dimensional normalized correlation value and n 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. The watermark image was tested against several attacks, and the attacks include salt and pepper noise (Noise density, $N = 0.001$), Gaussian noise ($\mu = 0, \sigma^2 = 0.005$), Speckle noise ($N = 0.001$), Gaussian filter ($3 \times 3$), rotation ($45^0$), JPEG compression (Q=50, 70). Figure 2 shows the watermarked image at 30dB, 35dB, and 40dB.

We use the DE algorithm to find out the optimal scale factors α_i which gives the best fidelity and robustness as in Table 2.

Table 3 and 4 show the comparison between the proposed scheme, false-free method by Guo *et al*., and the reliable SVD by Jain *et al.* It can be observed clearly that our proposed scheme shows stronger robustness at PSNR values of 30dB, 35dB, and 40dB than the reliable SVD scheme. The proposed scheme has better robustness than Guo *et al.* for additional noise attack. A weak point of the proposed scheme is not robust to rotation attack.

5. Conclusion

This paper proposed an improved scheme to the existing reliable SVD-based watermark schemes without a false-positive problem for the ownership verification applications. 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. The proposed scheme improves fidelity and robustness of the reliable SVD based watermarking schemes without any false-positive problem. A weak point of the proposed scheme is not robust to rotation attack, but this can be solved by employing a compensation algorithm to the rotation.

6. References

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "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, J. G. Brankov, N. P. Galatsanos, Y. Yang, F. Davoine, "Digital Watermarking Robust to Geometric Distortions," IEEE Transactions on Image Processing, Vol.14, No.12, December 2005.

[4] M. Alghoniemy, Ahmed 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] E. Ganic, A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding data in all frequencies," in Proc. Workshop Multimedia and Security, Magdeburg, Germany, 2004, pp. 166-174.

[7] G. Bhatnagar, B. Raman, “A new robust reference watermarking scheme based on DWT-SVD,” Computer Standards & Interfaces, vol.31, no.5, pp.1002-1013, Sep.2009.

[8] Chih-Chin Lai, Cheng-Chih Tsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition,” IEEE Transactions on instrumentation and measurement, Vol.59, No.11, November 2010.

[9] Nasrin M.Mkbol, Bee Khoo, “Robust Blind image watermarking scheme bases on Redundant Discrete Wavelet Transform and Singular Value Decomposition,” Int J Electron Commun(AEU); 67(2013) 102-112.

[10]. C.Jain, S.Arora, P. K. Panigrahi, “A Reliable SVD based Watermarking Scheme,” August 2008.

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

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

[13]. S.G.Mallat, “ A Theory for Multiresolution Signal Decomposition: The Wavelet Representation,” IEEE Trans on Pattern Analysis and Machine Intelligence, Vol. 11, No.7, July 1989.

[14]. M.E.Wall, A.Reachtseiner, L.M.Rocha, “Singular Value Decomposition and Principal Component Analysis in a Practical approach to Microarray Data Analysis,” D.P Berrar, W. Dubitzky, M.Granzow, eds.) Kluwer: Norwell, MA, 2003. pp. 91-109. LANL LA-UR-02-4001.

[15]. 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.

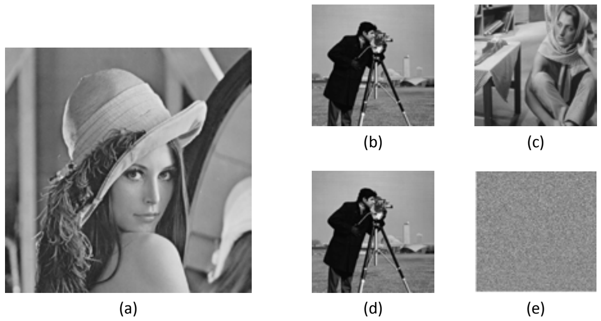

Figure 1. Results by the reliable SVD watermarking scheme; (a) Watermarked image PSNR=57.31dB; (b) Watermark image; (c) Fake watermark image; (d) Extracted watermark image; (e) Extracted fake watermark image.

Figure 2. Watermarked image at (a) PSNR=30 dB; (a) PSNR=35 dB; (a) PSNR=40 dB.

Table 1. PSNR and robustness (normalized correlation) of the reliable SVD watermark scheme for Salt and Peppers attack.

Scale Factor	PSNR [dB]	Robustness
0.03	39.98	0.4478
0.06	35.52	0.6500
0.10	31.30	0.8281
0.50	17.31	0.8504

Table 2. The optimal scale factors for PSNR values.

PSNR [dB]	α_1	α_2	α_3	α_4
30	-0.8951	3.2722	6.0624	5.3419
35	-0.4959	-2.2342	3.7828	5.4992
40	-0.2718	-1.3176	3.9000	6.5000

Table 3. Comparison between the proposed scheme and the reliable SVD scheme.

Attacks	**30dB**			**35dB**		
	Proposed scheme	Guo et al.	Reliable SVD	Proposed scheme	Guo et al.	Reliable SVD
Salt and pepper	0.9989	0.9760	0.8466	0.9959	0.9609	0.6500
Gaussian noise	0.9996	0.9450	0.9307	0.9988	0.8880	0.8197
Speckle	0.9904	0.9788	0.4324	0.9722	0.9597	0.2520
Gaussian filter	0.9625	0.9784	0.8424	0.9137	0.9673	0.6967
Rotation 45^0	0.3416	0.0358	0.1061	0.3431	0.0354	0.0892
JPEG compression Q=50	0.9618	0.9770	0.4704	0.9222	0.9559	0.3023
JPEG compression Q=70	0.9806	0.9840	0.6368	0.9590	0.9794	0.4252

Table 4. Comparison between the proposed scheme and the reliable SVD scheme.

Attacks	**40dB**		
	The proposed scheme	Guo et al.	The reliable SVD
Salt and pepper	0.9894	0.8742	0.4478
Gaussian noise	0.9960	0.7159	0.6426
Speckle	0.9081	0.8812	0.1467
Gaussian filter	0.7975	0.9084	0.5400
Rotation 45^0	0.3433	0.0352	0.0650
JPEG compression Q=50	0.7379	0.8722	0.1830
JPEG compression Q=70	0.8258	0.9395	0.2705