Applied Mathematical Sciences, Vol. 8, 2014, no. 60, 2997 - 3008
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2014.4126

A Robust Watermarking Scheme Based on Steerable Pyramid and Singular Value Decomposition

[a,b]Azz El Arab El Hossaini, [b]Mohamed El Aroussi, [a,b]Khadija Jamali
[a]Samir Mbarki, [b]Mohammed Wahbi

[a]Department of Computer Science
Faculty of Science
Ibn Tofail University
Kenitra, Morocco

[b]Department of Electrical Engineering
Hassania School of Public Works
BP 8108 Oasis-Casablanca, Morocco

Abstract

Most of the watermarking schemes that have been proposed until now are based on DCT, DFT, and DWT transformations. For this reason, this paper presents a new robust watermarking scheme based on Steerable Pyramid (SP) wavelet transform and singular value decomposition (SVD) for copyright protection and authenticity. SP transformation is applied to the original image with a number of scales and orientations accurately calculated. Low-pass band is selected and divided into blocks. After applying SVD on each block, watermarking process embeds the watermark by modifying coefficient of S component of each block. For each block we get a secret key that will be used for the extraction of the watermark. Peak signal to noise ratio (PSNR) is used to evaluate the watermarking schemes. Extracted watermark quality is evaluated by Normalized cross correlation (NC). Experimental results show the effectiveness of this method with good visual quality and resistance against several attacks.

Keywords: Robust image watermarking, Steerable pyramid, Singular value decomposition, Geometrical attacks

1 Introduction

With the fast development of data exchange techniques, frauds have increased. Most current information is stored in digital form. Exchange, distribution and processing of these data are becoming easier and out of control. For example, an image on the web can be saved, modified and transmitted over a network or on storage media without consideration of copyrights. For this reason, digital watermarking was born to protect intellectual property against the illegal duplication and manipulation. Watermarking is not only limited to copyright protection. It can be used for the following needs:

- Fingerprinting : used in order to monitor illegal copies of digital documents. The owner can insert various watermarks in the copies of the image. This allows, when an illegal copy is found to determine the identity of the person who violated the license.

- The steganography : used to transmit a secret message in a digital medium. This technique requires a perfect invisibility and solids concepts of cryptography.

- Data authentication : indicates whether the image has undergone change and where the modified regions are.

- Other applications: such as indexing image and monitor programs currently played on TV can be performed by the watermarking techniques.

Digital watermarking involves of embedding some types of digital data (logo, label and name) called watermark representing authors ownership and/or product user in the host image in order to use it if necessary to verify ownership and/or to distinguish product user. In literature, several watermarking techniques were presented and each one of them has its advantages and its inconveniences. A good watermarking approach must meet two main constraints: invisibility of the embedding watermark and robustness against attacks. Indeed, (1) no difference should be detected by human eye between the watermarked image and the original image, (2) as the watermarked image is usable, the watermark must always be detectable regardless of either changes applied to the watermarked image, and finally (3) only authorized persons may extract the watermark. Based on used domain to hide watermark in the host image, image watermarking schemes can be classified into two main categories: spatial domain [1] [2] [3] and frequency domain techniques [4] [5] . Spatial domain

schemes are less complex and not robust against various attacks. Watermark embedding and extracting is performed by manipulating directly the pixel intensity values of the original image. The most common simplest watermarking technique in the spatial domain is performed by manipulating the Least Significant Bit (LSB) of the original image [1][2]. Authors in [6], used human visual effects to adapt watermark embedding in their scheme in spatial domain. Frequency domain schemes are more robust compared to spatial domain schemes. This is due to the fact that watermarking process is performed by manipulating the coefficients of the corresponding transformed domain image of the original image. This technique makes the manipulation of the watermark harder for non authorized persons, because the watermark is distributed irregularly over the original image after the inverse transform. Kundur et al [7], proposed a multiresolution fusion based watermarking technique that incorporates a model of the human visual system (HVS). This watermarking process embeds a gray scale logo into wavelet transformed images. It is a non blind watermarking scheme, in which the original image is necessary to extract the watermark logo.

A few years ago, a new transform for watermarking named singular value decomposition(SVD) was introduced by Liu et al [8]. Makbol et al [9] proposed a watermarking algorithm in which the authors used Redundant Discrete Wavelet Transform (RDWT) and the Singular Value Decomposition (SVD) to embed a gray scale watermark image in the singular values of the RDWT subbands of the host image. Rastegar et al [10] presents a robust watermarking scheme that can survive against several attacks like : filtering, noise addition, and histogram. This method is based on finite Radon transform, singular value decomposition , and Discrete Wavelet Transform to embed Binary watermarrk image using middle frequencies of HL3 and LH3.

This paper is organized as follows. Section 2 describes the proposed method using steerable pyramid and singular value decomposition. Simulation results in Section 3 will show the performance of our scheme against several attacks. Finally, Section 4 concludes this paper.

2 PROPOSED METHOD

The proposed watermarking algorithm consists of two procedures: watermark embedding and watermark extraction procedure using steerable pyramid transform and singular value decomposition.

2.1 Steerable Pyramid Transform

In signal and image processing, recursive multi-scale transforms are widely used. One drawback of this transforms is the lack of translation invariance

especially in two-dimensional (2-D) signals [11]. To overcome this problem, the steerable pyramid wavelet has been proposed by Freeman and Simoncelli [11]. In this transform, an image is subdivided into a number of sub bands with different orientations. The image is decomposed into low pass and high pass sub bands, using steerable filters L0 and H0. Then, the low pass sub band is further decomposed into 1+K oriented sub-bands and a low pass sub band. The later low pass sub band is sub sampled by a factor of 2. A new decomposition is performed by repeating these steps to the later low sub band obtained. Fig. 1 represents System diagram for the first level of the steerable pyramid. Boxes represent filtering and sub sampling operations. H1 is high pass filter, L0 and L1 are low pass filters and Bi are oriented band pass filters.

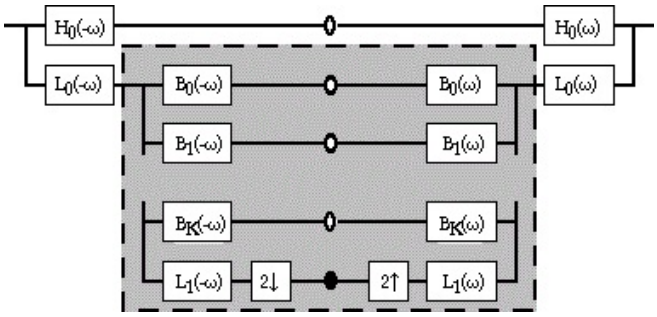

Figure 1: Tree representation of one-level 2D steerable pyramid transform [12]

2.2 Singular Value Decomposition

Singular value decomposition for square matrices was discovered independently by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. Singular value decomposition (SVD) represents useful tools in signal processing and statistics. SVD could be useful in image hiding, image compression [13], noise reduction [14] and image watermarking. SVD is a factorization of real or complex matrix. Applying SVD on a matrix nxn decompose it into three sub matrices [U, S, V] such that:

$$M = U * S * V^T \tag{1}$$

Where U and V are the orthogonal matrices (unitary). They are known as corresponding singular vectors and S is a diagonal matrix. Diagonal elements of S are the singular values and they satisfy the following property

$$S(1,1) > S(2,2) > S(3,3) > ..... > S(n,n) \tag{2}$$

In image processing field, SVD represents some benefits as follows :

- SVD could be applied to square or rectangle matrices.

- U and V matrices represent the geometry of the image and S matrix represents the luminance or color intensity of the image.

- Singular values of the image are less affected when applying general image processing attacks to the image.

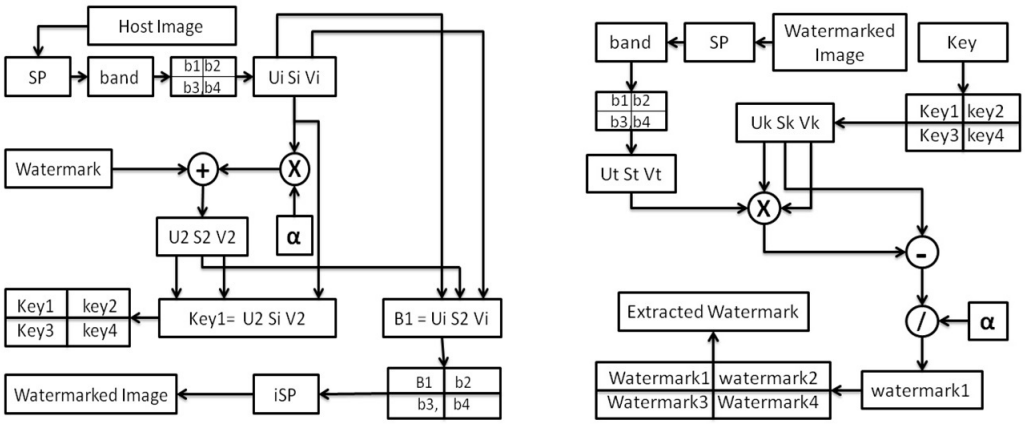

Figure 2: on the left : Proposed watermark embedding scheme; on the right : Proposed watermark extraction scheme

2.3 Watermark Embedding

The watermark embedding scheme is shown in Fig 2. The Steps of watermark embedding are as follow.

Step 1: The host image is transformed into steerable pyramid coefficients by using specific number of scales and orientations defined by the user.

Step 2: The low pass sub band is selected, and then divided into four non-overlapping blocks Bi.

Step 3: SVD is applied on block Bi to get three components Ui, Si, and Vi.

$$Bi = Ui\ Si\ Vi \tag{3}$$

Step 4: Modify the Si with the watermark W.

$$Si = Si + \alpha W \tag{4}$$

Step 5: Apply SVD to the Si.

$$Si = U2\ S2\ V2 \tag{5}$$

Step 6: Key is obtained by applying inverse SVD.

$$Ki = U2\ Si\ V2 \tag{6}$$

Step 7: Watermarked block Bi is obtained by applying inverse SVD.

$$Bi = Ui\ S2\ Vi \tag{7}$$

Step 8: Repeat steps from 3 to 7 four times to get the complete key composed from four keys and to watermark the four blocks Bi.

Step 9: apply inverse SP transform to get the watermarked image.

Figure 3: (a) Cover image Baboon 512x512; (b) Cover image Peppers 512x512; (c) Cover image Lena 512x512; (d) Watermark image Cameraman 128x128; (e) Watermarked image Baboon 512x512; (f) Watermarked image Peppers 512x512; (g) Watermarked image Lena 512x512; (h) Extracted watermark image Cameraman 128x128;

2.4 Watermark Extraction

The watermark extraction scheme is shown in Fig 2. In general, the extraction process is essentially the inverse of the embedding procedure. The Steps of watermark extraction are as follow.

Step 1: The watermarked image is transformed into steerable pyramid coefficients by using specific number of scales and orientations defined for the embedding process.

Step 2: The last low pass sub band B of the last scale is selected, and then divided into four non-overlapping blocks Bi.

Step 3: SVD is applied on block Bi to get three components Ut, St, and Vt.

$$Bi = Ut\ St\ Vt \tag{8}$$

Step 4: Key image is divided into four non-overlapping blocks Ki, and then SVD is applied to the blocks Ki.

$$Ki = Uk\ Sk\ Vk \tag{9}$$

Step 5: Apply inverse SVD to get S2.

$$S2 = Uk\ St\ Vk \tag{10}$$

Step 6: Watermark Wi is obtained as follow.

$$Wi = (S2 - Sk)/\alpha \tag{11}$$

Step 7: Repeat steps from 3 to 6 four times to get the watermark.

3 EXPERIMENTAL RESULTS

Before starting tests, optimal configuration values (scaling factor, Watermark size, number of orientations and number of scales) must be fixed. In our experiments, the scaling factor is 0.035. The size of the watermark depends on number of scales that is shown in Table 1. According to our watermarking scheme, we embed the same watermark with a size of 128x128 four times to produce a watermarking method more robust in case we lost some parts of the watermarked image. Embedding the same watermark image four times means that we embed an image with a size of 256x256. According to table 1, one scale is selected and according to table 2, best optimal value for the watermarked image is one orientation.

Table 1: Size of the watermak image

scales	1	2	3	4
Watermark size	256x256	128x128	64x64	32x32

Table 2: PSNR of the Watermaked images

Orientation	1	2	4	6
Baboon	63.3675	51.8533	51.3009	46.3856
Peppers	58.9436	42.0617	42.0833	42.8689
Lena	59.1271	57.4355	56.2311	48.5623

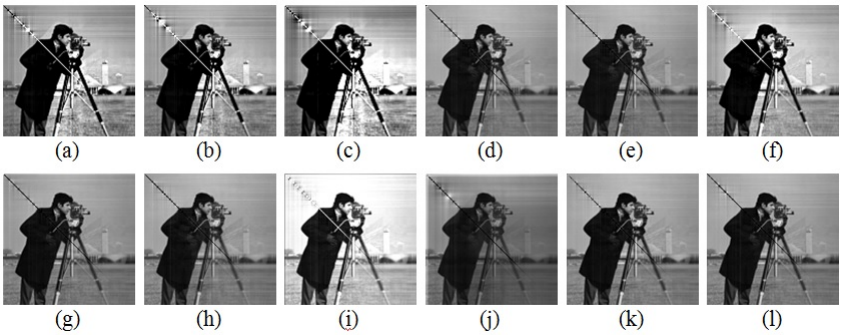

Figure 4: Extracted watermark after (a) Pepper & salt noise (0.1); (b) Speckle noise (0, 1); (c) Gaussian noise (0.1); (d) Median lter (33); (e) Wiener lter (33); (f) Sharpening; (g) Gamma correction (0.8); (h) Resize (256x256); (i) Histogram equalisation; (j) Crop; (k) JPEG compression (Q=30); (l) Rotation (angle 45).

Table 3: The NC of the extracted watermark for Baboon, Pepper and Lena image under different attacks.

Attack	Baboon	Pepper	Lena
Pepper & salt noise (density 0.1)	0.9885	0.9667	0.9687
Pepper & salt noise (density 0.2)	0.9748	0.9424	0.9429
Pepper & salt noise (density 0.3)	0.9601	0.9221	0.9261
Speckle noise (var=0.1)	0.9904	0.9771	0.9738
Speckle noise (var=0.2)	0.9814	0.9614	0.9602
Speckle noise (var=0.3)	0.9744	0.9502	0.9517
Gaussian noise (M=0,var=0.1)	0.9708	0.9409	0.9451
Gaussian noise (M=0,var=0.2)	0.9557	0.9170	0.9265
Gaussian noise (M=0,var=0.3)	0.9487	0.9105	0.9126
Gaussian filtering (3x3)	0.9959	0.9955	0.9955
Gaussian filtering (5x5)	0.9950	0.9955	0.9955
Median filtering (3x3)	0.9932	0.9948	0.9948
Median filtering (5x5)	0.9749	0.9901	0.9891
Median filtering (7x7)	0.9405	0.9833	0.9802
Wiener filtering (3x3)	0.9936	0.9948	0.9946
Wiener filtering (5x5)	0.9838	0.9913	0.9907
Wiener filtering (7x7)	0.9678	0.9869	0.9859
Resize (256x256)	0.9941	0.9944	0.9943
Resize (128x128)	0.9587	0.9705	0.9703
Resize (64x64)	0.8251	0.8566	0.8600
Rotation (angle=10)	0.9968	0.9969	0.9970
Rotation (angle=30)	0.9957	0.9961	0.9958
Rotation (angle=50)	0.9960	0.9961	0.9958
Rotation (angle=70)	0.9959	0.9961	0.9958
Histogram Equalization	0.9902	0.9967	0.9956
Gamma correction 0.8	0.9962	0.9968	0.9958
Gamma correction 0.7	0.9951	0.9960	0.9947
Sharpening	0.9843	0.9913	0.9901
JPEG compression Q=10	0.9979	0.9967	0.9968
JPEG compression Q=20	0.9983	0.9970	0.9970
JPEG compression Q=30	0.9978	0.9970	0.9971
JPEG compression Q=40	0.9976	0.9970	0.9971

To test robustness of the proposed scheme against different attacks, a number of experiments are performed on the watermarked image. Tests are performed to the popular gray scale Baboon, Pepper and Lena images with size 512x512 as cover image and Cameraman image as watermark image.

Our watermarking scheme is evaluated with respect to two metrics: imper-

ceptibility and robustness. Results show that there are no perceptibly visual degradations on the watermarked images as shown in Fig 3. To test the robustness, different intentional and non-intentional attacks are tested on the proposed watermark scheme include pepper & salt, speckle noise, gaussian noise, gaussian filtering, median filtering, wiener filtering, resizing, rotation, cropping, histogram equalization, gamma correction, sharpening and JPEG compression. Table 2 shows Peak signal to noise ratio (PSNR) results obtained with different orientations. The PSNR is used to make sure that the perceptibility property is preserved by the proposed watermarking scheme and it is defined as :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{12}$$

Where MSE (Mean Square Error) is defined as:

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (I_i - \hat{I}_i)^2 \tag{13}$$

Table 3 shows the similarity between the extracted watermark and the original embedded watermark. This similarity is measured using normalized correlation (NC).

$$NC = \frac{\sum_{i=1}^{M} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{M} w_i} \sqrt{\sum_{i=1}^{M} \hat{w}_i}} \tag{14}$$

Where N represents the number of pixels in the original (I) and watermarked ($\hat{I}$) image. M represents the number of pixels in the original (w) and extracted ($\hat{w}$) watermark image. The normalized correlation (NC) may take values between 0 (random relationship) to 1 (perfect linear relationship).

In order to assess the efficiency of the proposed watermarking scheme, three related watermarking schemes are incorporated for the comparison including Makbol et al [9], Lai et al [8] and Rastegar et al [10]. Comparison includes two metrics imperceptibility and robustness as mentioned above for tests.

Table 4: PSNR comparison of the Watermaked image between our proposed method, Makbol et al [9], Lai et al [8] and Rastegar et al [10]

Image	Proposed scheme	Makbol et al	Lai et al	Rastegar et al
Lena	**59.1271**	54.0353	50.89	45.9337
Peppers	**58.9436**	54.1556	-	45.9543
Baboon	**63.3675**	55.9768	-	45.9228

The bold value is the best

Psnr comparison results in table 4 shows that Our proposed scheme achieved a high imperceptibility with all tested images (Pepper, Lena, and Baboon) against other schemes incorporated for the comparisons. In addition to the imperceptibility, our scheme achieved high robustness as shown in table 5 for all tested attacks compared to other schemes except gamma correction (0.7) attack where Lai et al [8] scheme has a better result comparing to us.

Table 5: Normalized correlation comparison of our scheme with Makbol et al [9], Lai et al [8] and Rastegar et al [10]

Attack	Proposed scheme	Makbol et al	Lai et al	Rastegar et al
Pepper & salt noise (density 0.3)	**0.9261**	0.8926	-	0.8258
Speckle noise (var=0.01)	**0.9949**	0.952	-	0.9667
Gaussian noise (M=0,var=0.5)	**0.9058**	0.8935	-	0.82
Gaussian ltering (3x3)	**0.9955**	0.987	-	0.9843
Median ltering (3x3)	**0.9948**	0.982	0.9597	0.9706
Wiener ltering (3x3)	**0.9907**	0.984	-	0.9569
Sharpening	**0.9901**	0.932	-	0.9511
Histogram equalization	**0.9956**	0.990	0.9862	0.9628
Gamma correction (0.7)	0.9947	0.9935	**0.9982**	-
Gamma correction (0.8)	**0.9958**	0.9950	-	0.9217
JPEG compression Q=30	**0.9971**	0.987	-	-
JPEG compression Q=10	**0.9968**	0.972	0.9772	0.9843
JPEG compression Q=5	**0.9962**	0.952	-	0.9354
Rotation (angle=2)	**0.9978**	0.981	-	0.9628
Rotation (angle=30)	**0.9957**	0.9823	0.9780	-

The bold value is the best

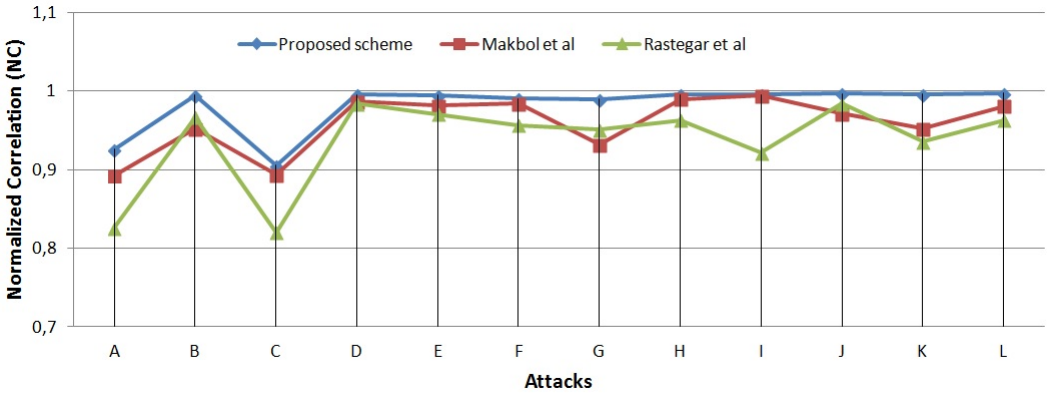

Figure 5: Robustness comparison of the proposed scheme with Rastagar's schemes [10] and Makbol's schemes [9]. (a) Pepper & salt noise (density 0.3); (b) Speckle noise (var=0.01); (c) Gaussian noise (M = 0,var=0.5); (d) Gaussian ltering (33); (e) Median ltering (33); (f) Wiener ltering (33); (g) Sharpening; (h) Histogram equalization; (i) Gamma correction (0.8); (j) JPEG compression Q=10; (k) JPEG compression Q=5; (l) Rotation (angle=2).

4 Conclusion

Due to lack of watermarking schemes based on steerable pyramid in the literature, a new robust watermarking scheme has been proposed based on Steerable Pyramid (SP) wavelet transform and singular value decomposition (SVD) for copyright protection and authenticity. The Experimental results of the proposed scheme have shown high perceptual quality of the watermarked image and excellent robustness against different intentional and non-intentional attacks like pepper & salt, speckle noise, gaussian noise, gaussian filtering, median filtering, wiener filtering, resizing, rotation, cropping, histogram equal-

ization, gamma correction, sharpening and JPEG compression.

References

[1] M. Celik, G. Sharma, E. Saber, A. Tekalp, Hierarchical watermarking for secure image authentication with localization, Image Processing, IEEE Transactions on 11 (6) (2002) 585–595. doi:10.1109/TIP.2002.1014990.

[2] R. van Schyndel, A. Tirkel, C. Osborne, A digital watermark, in: Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference, Vol. 2, 1994, pp. 86–90 vol.2. doi:10.1109/ICIP.1994.413536.

[3] Z.-M. Lu, J.-S. Pan, S. he Sun, Vq-based digital image watermarking method, Electronics Letters 36 (14) (2000) 1201–1202. doi:10.1049/el:20000876.

[4] W. Chu, Dct-based image watermarking using subsampling, Multimedia, IEEE Transactions on 5 (1) (2003) 34–38. doi:10.1109/TMM.2003.808816.

[5] M. Iwata, A. Shiozaki, Watermarking method for embedding index data into images utilizing features of wavelet transform, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 84 (7) (2001) 1772–1778.

[6] C.-C. Chang, K.-F. Hwang, M.-S. Hwang, Digital watermarking scheme using human visual effects, Informatica(Ljubljana) 24 (4) (2000) 505–511.

[7] D. Kundur, D. Hatzinakos, Toward robust logo watermarking using multiresolution image fusion principles, Multimedia, IEEE Transactions on 6 (1) (2004) 185–198. doi:10.1109/TMM.2003.819747.

[8] R. Liu, T. Tan, An svd-based watermarking scheme for protecting rightful ownership, Multimedia, IEEE Transactions on 4 (1) (2002) 121–128. doi:10.1109/6046.985560.

[9] N. M. Makbol, B. E. Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, {AEU} - International Journal of Electronics and Communications 67 (2) (2013) 102 – 112. doi:10.1016/j.aeue.2012.06.008.

[10] S. Rastegar, F. Namazi, K. Yaghmaie, A. Aliabadian, Hybrid watermarking algorithm based on singular value decomposition and radon transform, {AEU} - International Journal of Electronics and Communications 65 (7) (2011) 658 – 663. doi:10.1016/j.aeue.2010.09.008.

[11] W. Freeman, E. Adelson, The design and use of steerable filters, Pattern Analysis and Machine Intelligence, IEEE Transactions on 13 (9) (1991) 891–906. doi:10.1109/34.93808.

[12] E. Simoncelli, A rotation invariant pattern signature, in: Image Processing, 1996. Proceedings., International Conference on, Vol. 3, 1996, pp. 185–188 vol.3. doi:10.1109/ICIP.1996.560415.

[13] A. Ranade, S. S. Mahabalarao, S. Kale, A variation on {SVD} based image compression, Image and Vision Computing 25 (6) (2007) 771 – 777. doi:10.1016/j.imavis.2006.07.004.

[14] P. Sadasivan, D. Dutt, {SVD} based technique for noise reduction in electroencephalographic signals, Signal Processing 55 (2) (1996) 179 – 189. doi:10.1016/S0165-1684(96)00129-6.

Received: January 9, 2014