International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.04,Issue.20,
December-2016,
Pages:3855-3859

Block Based Image Watermarking Through Wavelet Transform and Arnold Transform

MOUNIKA JOGU[1], VENKATA SUBBA REDDY K[2]

Abstract: This Paper proposes a new image watermarking approach based on the discrete wavelet transform and Arnold transform. Along with DWT, this approach also combines the discrete cosine transform and singular value decomposition. The low frequency band of host image is chosen for watermarking and before embedding, the LF band is divided into equal sized non-overlapping blocks. The watermark image is initially transformed through Arnold transform and then embedded into the host image. Normalized Correlation and Peak signal to noise ratio are used to measure the performance of proposed approachat various attacks like Gaussian noise attack, Salt & pepper noise attack, Rotation Attack, Crop attack, median filter attack, Contrast Enhancement, JPEG compression, Mosaicking and translation.

Keywords: Image Watermarking, SVD, Arnold Transform, DWT, PSNR, NC, DCT.

I. INTRODUCTION

Nowadays, digital image watermarking has been developed to solve the problem for copyright protection and content verification of multimedia data. It allows owners to hide their ownership rights and access controls into their original images. The ownership rights or access controls are called watermarks which can be various data formats such as logos, tags, sound or any other copyright information. Image watermarking can be roughly classified into several categories according to the domain they are developed, reference to host image, visibility, and robustness. For the case of watermark embedding, watermarking techniques can be developed in three domains, spatial, frequency and blend domains. Spatial domain methods embed a watermark via modifications to the pixel values of an original image. Frequency-domain schemes embed a watermark via modifications to the coefficients of the corresponding transformed-domain image of an original image. In the existing approach, the developed digital image watermarking scheme is combined with discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD). To improve the security of the watermark, the encrypted watermark is acquired by Arnold transform before watermark embedding.

The performance of proposed scheme is evaluated with respect to the normalized correlation (NC) and peak signal-to noise ratio (PSNR).However the main drawbacks are, 1. Reduced image quality due to the information loss at image reconstruction because of discrete wavelet transform. 2. Low PSNR and low NC between the original and extracted watermark images.3. Less Security due to the Arnold transform. This paper proposed a new digital image watermarking scheme based on the Multi Spectral features of host image. Discrete Wavelet Transform (DWT) is applied to the host image to find the pixels with less correlation. If the watermark is embedded at the pixels with less correlation, the quality of host image won’t be affected. Then the watermark image is subjected to normal DWT followed by DCT and SVD. PSNR and NC are used to measure the performance of proposed approach at various attacks like Gaussian noise attack, Salt & pepper noise attack, Rotation Attack, Crop attack, median filter attack, Contrast Enhancement, JPEG compression, Mosaicking and translation. Rest of the paper is organized as follows: section II gives the details of literature survey. Section III illustrates the complete details of proposed approach. Section IV gives the details of implementation results and finally the conclusions are given in section V.

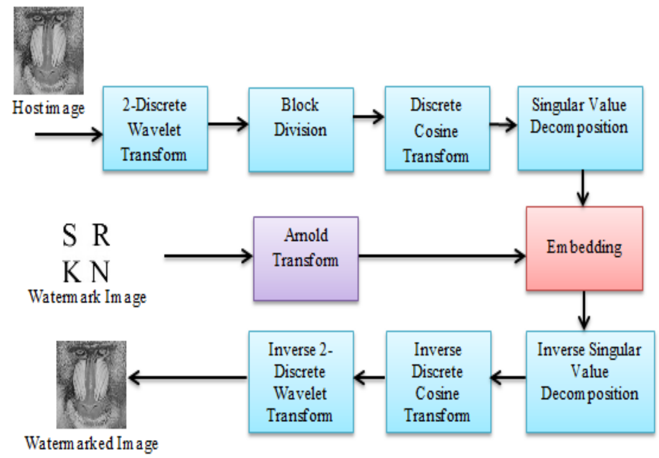
II. LITERATURE SURVEY

Based on the domain in which the watermark inserted, the watermarking techniques are classified into two classes such as spatial domain watermarking techniques and frequency domain watermarking techniques. In spatial domain techniques, the watermark is directly inserted into the cover image by altering the pixel values [4, 5, 6]. The simplest technique in this category is to modify the least significant bits (LSB) of the host image pixels by watermark image pixels [3]. The spatial domain methods have the advantages of easy implementation and low cost of operation but are generally not robust to geometrical and image processing attacks. In contrast, frequency domain methods transform the representation of spatial domain into the frequency domain and then modify its frequency coefficients to embed the watermark. There are many transform domain watermarking techniques such as discrete cosine transforms (DCT) [7, 8], singular value decomposition (SVD) [9,10], discrete Fourier transforms (DFT) [11], and discrete wavelet transforms (DWT) [12,13,14]. These techniques are more robust against many signal and image processing attacks in comparison to the spatial domain techniques but generally require higher computational cost. Another way to increase the performance of watermarking approaches is to use Artificial Intelligence techniques. Since the watermarking can be viewed as an optimization technique, the AI techniques such as Genetic

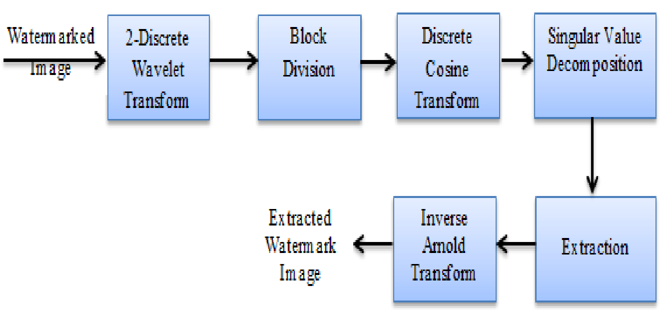
Algorithm and Particle Swarm Optimization can be used for the purpose of optimization. In earlier various watermarking approaches are proposed based on the GA [15-17] and PSO [18-20]. But all these works have been dedicatedly designed for gray scale image watermarking and the extension of these types of bio-inspired optimization methods to the field of color image watermarking has been neglected.

III. PROPOSED APPROACH

The architecture of proposed watermarking system is shown in fig.1. Fig.1(a) is of embedding and (b) is of extraction.



(a)



(b)

Fig.1. (a) Embedding Unit (b) Extraction Unit.

The watermarking scheme proposed in this approach includes two main procedures: watermark embedding and watermark extraction, which is similar to the watermarking scheme in [2]. However, unlike the watermark embedding procedure and watermark extraction process in [2], the Arnold transform is applied to guarantee the security of watermarking.

A. Watermark Embedding Procedure

Step 1: One-level MWT transform using 'Haar' wavelet is applied on the host grayscale image **I** with size of M×M . The four frequency components of size M / 2×M / 2 are obtained as follows: LL, HL, LH, and HH .

Step 2: The low resolution approximation matrix LLis partitioned into 8×8 non-overlapping image blocks.

Step 3: The watermark W is encrypted by Arnold transform with secret key K, and the encrypted watermark is represented as W^0.

Step 4: DCT is executed on each image block, and the 4×4 matrix in the up-left transformed coefficient matrix is performed by secondary DCT. According to watermark capacity, at the up-left of each coefficient matrix block, the 1×1, 2×2, or 4×4 matrix are extracted to organize a new matrix B , respectively.

Step 5: SVD is performed on the matrix B: $B=U_1S_1V_1^T$.By $S_1+\alpha W^0=U_2S_2V_2^T$, the matrix $W^0$is embedded into the singular value matrix 1 S , where α is scale factor to regulate the embedding intensity of watermark. Finally, the matrix B* $=U_1S_2V_1^T$is calculated. In this approach, the watermark embedding intensity α is set as 0.01.

Step 6: After embedding process, the modified low frequency sub-band is acquired by performing twice inverse DCT. After inverse DWT transform, the watermarked image I∗ is obtained.

B. Watermark Extraction Procedure

Step 1: One-level MWT using 'Haar' wavelet is performed on the watermarked image I *. Then the low frequency matrix LL is partitioned into 8×8 non-overlapping image blocks.

Step 2: DCT is applied on each image block. Then the 4×4 matrix in the up-left transformed coefficient matrix is performed by secondary DCT. According to the watermark capacity, at the up-left of each coefficient matrix block, the 1×1, 2×2, or 4×4 matrix is extracted to organize the matrix B*, respectively.

Step 3: The SVD transform is applied on the matrix $B^*=U_1^*S_1^*V_1^{*T}$, S_2^*, U_2 and $V_2$are used to obtain the matrix $E=U_2S_2^*V_2^T$. At last, the extracted watermark W∗ is obtained by $W^*=(E-S_1)/\alpha$. The real watermark W ' is recovered after inverse Arnold transform.

IV. SIMULATION RESULTS

A Performance Metrics

In this chapter, we use the PSNR to assess the imperceptibility of the watermarked image, and the NC to test the similarity between the original watermark and the extracted watermark. Besides that, the false positive problem and the comparison with other schemes are also presented. After extracting the watermark image, the PSNR and NC were evaluated as

$$PSNR = 10 * \log\left({255^2}/{MSE}\right) \quad (1)$$

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(w(i,j)-w^*(i,j)\right)^2 \quad (2)$$

Where

w=original watermark image

w^* = extracted watermark image

Generally, the larger the PSNR value is, the better its imperceptibility between the original and watermarked image would be.

$$NC = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{w(i,j)*w^*(i,j)}{(w(i,j))^2*w^*((i,j))^2} \quad (3)$$

The NC is a positive number which is less than or equal to 1. A larger NC signifies that the extracted watermark is much closer to the original watermark.

B. Experimental Results

For performance evaluation, three host images and three watermark images are considered and shown in fig.2 and fig.3 respectively. To investigate the robustness of proposed approach, the watermarked image was subjected to eight attacks such as: (1) Gaussian noise Attack (GNA), (2) salt & pepper noise attack (SPA), (3) Median Filtering attack (MFA) with average window size of 3X3, (4) Crop attack (1-upper left, 2-upper right, 3-bottom left, 4-bottom right, 5-middle), (5) Rotation attack (RA) with rotation of 45^0,90^0 and 135^0 (6) Contrast Enhancemnet attack (CEA), (7) radiation transformation attack, (8) JPEG compression, (9) Translation and (10) Mosaic.

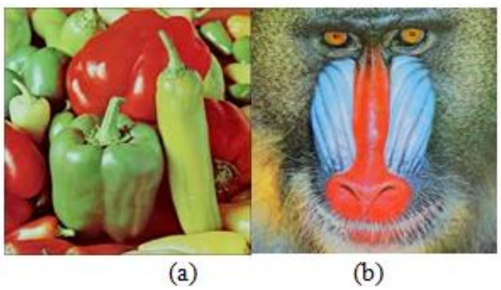
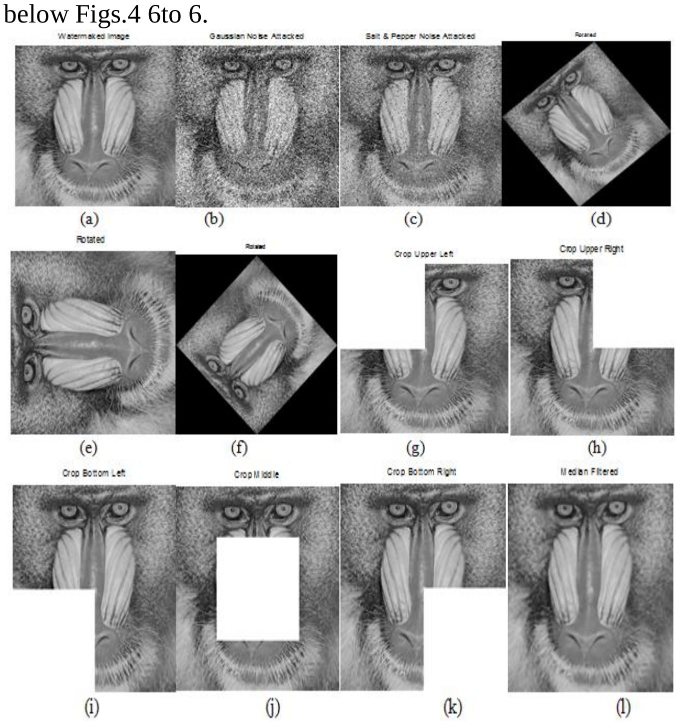


Fig.2. Host images.

Fig.3. Watermark Images.

The obtained results for lena as a host image are shown below Figs.4 6to 6.



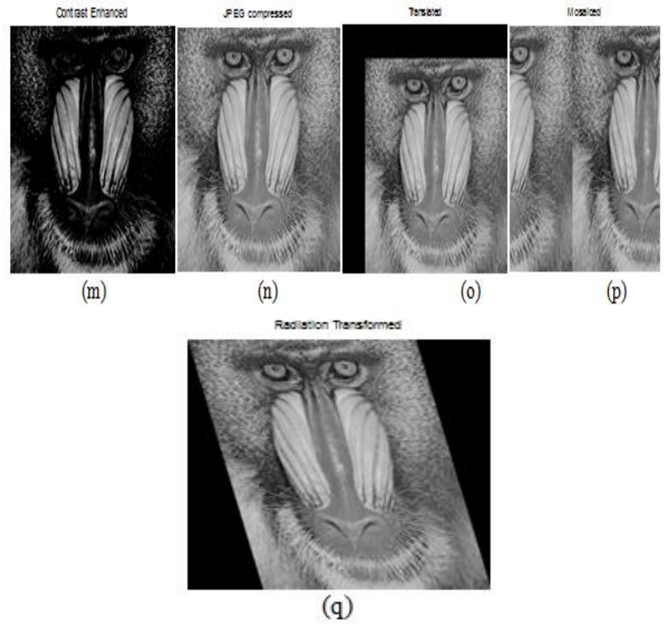


Fig.4. Watermarked Image under different attacks (a) Watermarked Image (b) Gaussian noise (0, 0.1); (c) Salt and pepper noise (0.5); (d) Rotate 45°; (e) Rotate 90°; (f) Rotate 135°; (g) Crop up-left; (h) Crop up-right; (i) Crop down-left; (j) Crop down-right; (k) Crop middle; (l) Median filter (3×3); (m) Contrast-enhanced; (n) JPEG compression (QF = 10); (o) Translation; (p) Mosaic and (q) Radiation transformation.

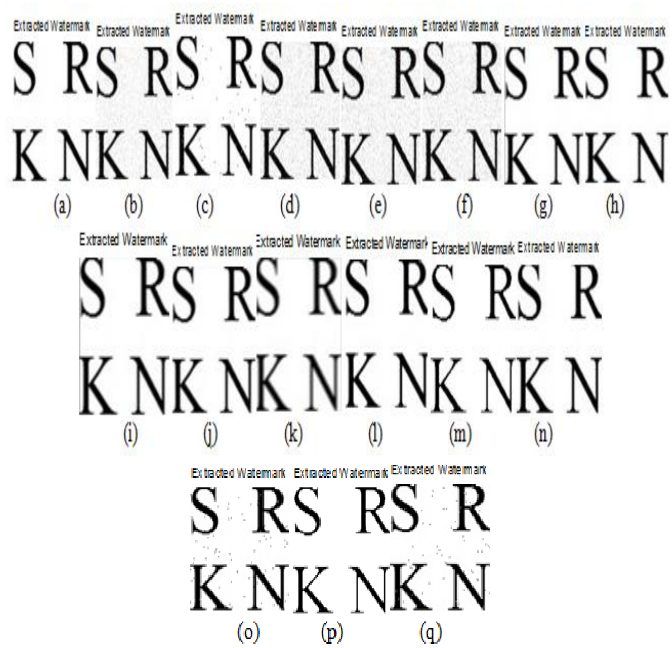


Fig.5. Extracted Watermark (64*64) under different attacks (a) Watermarked Image (b) Gaussian noise (0, 0.1); (c) Salt and pepper noise (0.5); (d) Rotate 45°; (e) Rotate 90°; (f) Rotate 135°; (g) Crop up-left; (h) Crop up-right; (i) Crop down-left; (j) Crop down-right; (k) Crop middle; (l) Median filter (3×3); (m) Contrast-enhanced; (n) JPEG compression (QF = 10); (o) Translation; (p) Mosaic and (q) Radiation transformation.

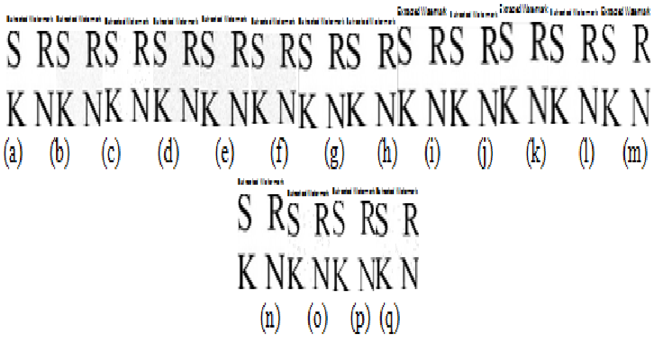


Fig.6. Extracted Watermark (32*32) under different attacks (a) Watermarked Image (b) Gaussian noise (0, 0.1); (c) Salt and pepper noise (0.5); (d) Rotate 45^o; (e) Rotate 90^o; (f) Rotate 135^o; (g) Crop up-left; (h) Crop up-right; (i) Crop down-left; (j) Crop down-right; (k) Crop middle; (l) Median filter (3×3); (m) Contrast-enhanced; (n) JPEG compression (QF = 10); (o) Translation; (p) Mosaic and (q) Radiation transformation.

Further the obtained PSNR and NC results of the above test cases are described in table.1 and figs.7, 8 and 9 below;

TABLE I: PSNR and NC Results

Attack	PSNR	NC
No Attack	51.7163	0.9953
Gaussian Noise	34.2356	0.9770
Salt & Pepper Noise	35.3325	0.9752
Rotation (45^0)	34.1458	0.9730
Rotation (90^0)	34.2589	0.9750
Rotation (135^0)	34.7415	0.9741
Crop (upper-left)	36.8865	0.9810
Crop (upper-right)	36.1123	0.9860
Crop (bottom-left)	35.5202	0.9863
Crop (bottom-right)	35.7452	0.9871
Crop (middle)	33.5326	0.9820
Median Filter	40.3369	0.9774
Contrast Enhanced	33.7852	0.9612
JPEG compression	52.6689	0.9722
Translation	52.7741	0.9757
Mosaic	32.9958	0.9552
Radiation transformation	52.4412	0.9741

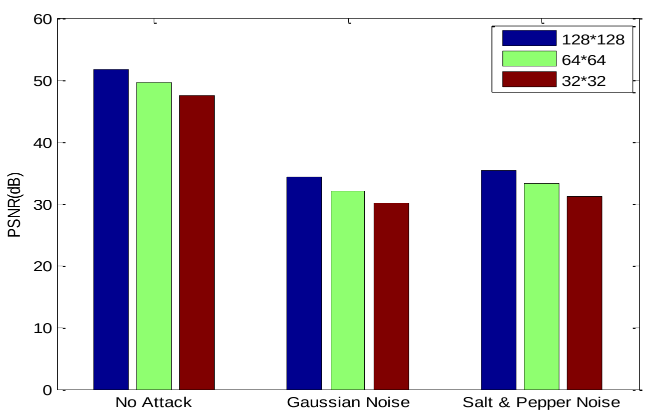


Fig.7. PSNR observations for various watermark sizes for no attack and noise attacks.

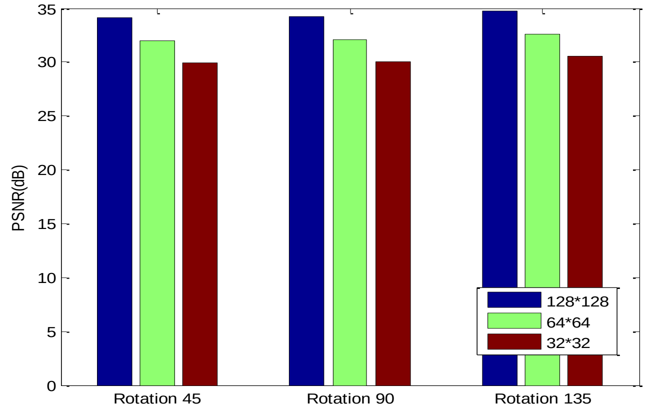


Fig.8. PSNR observations for rotation attacks.

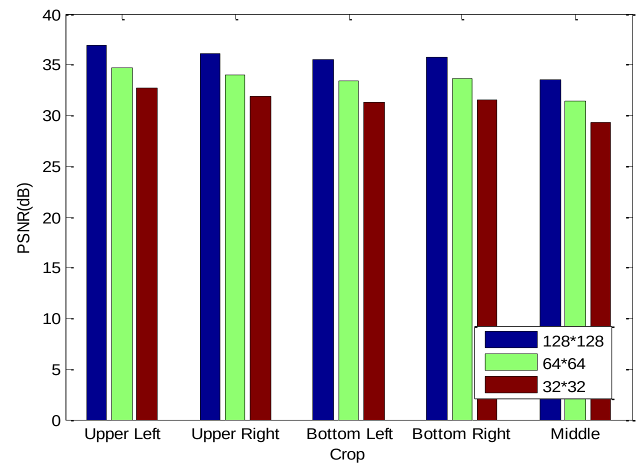


Fig.9. PSNR observation for various crop attacks.

V. CONCLUSION AND FUTURE SCOPE

Digital image watermarking must be needed in today's digitized world where digital image is most widely transferred file over the internet. In previous work, there are so many techniques in spatial and frequency domain for image watermarking from which DCT, DWT and SVD are most widely used techniques. SVD provides better noise immunity but the main drawback is that it cannot be used alone because of its large computations requirements. DWT provides good robustness but the visibility is average. In case of DCT, we can attempt acceptable visibility and average robustness. So, Hybridization of DCT and DWT gives much better result than independent DCT or DWT because it overcomes the drawbacks of each other. Thus, here we used hybridize concept of DCT, DWT & SVD to overcome the problems faced at earlier stage of research. By implementing proposed system in matlab and tested it with different kind of attacks, we say that the proposed system is more robust than earlier system with full proof of implementation results.There is scope of improvement in quality of watermarked image and elapsed time taken by proposed approach. In future, this technique can be further improved by reducing processing time as well we can also hybridize other techniques than these three to make more robust system. We can also use semantic key encryption algorithm to make the system more secure.

VI. REFERENCES

[1] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process 6 (12) (1997) 1673–1687.

[2] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 4 (1) (2002) 121–128.

[3] I.J. Cox, M.L. Miller, J.A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, San Francisco, CA, 2002.

[4] P.S. Huang, C.S. Chiang, C.P. Chang, T.M. Tu, Robust spatial watermarking technique for color images via direct saturation adjustment, IEE Proc., Vis. Image Signal Process. 152 (5) (2005) 561–574.

[5] I.G. Karibali, K. Berberidis, Efficient spatial image watermarking via new perceptual masking and blind detection scheme, IEEE Trans. Inform. Forensics Secur. 1 (2) (2006) 256–274.

[6] N. Nikolaidis, I. Pitas, Robust image watermarking in spatial domain, Signal Process. 66 (1998) 385–403.

[7] G.L. Varco, W. Puech, DCT-based data hiding for securing ROI of color images, in: Proc. of the IEEE Int. Conf. on Image Processing (ICIP), Genova, Italy, vol. 2, 2005, pp. 1086–1089.

[8] A. Phadikar, S.P. Maity, B. Verma, Region based QIM digital watermarking scheme for image database in DCT domain, Comput. Electr. Eng. 37 (2011) 339–355.

[9] J.-M. Shieh, D.-C.Lou, M.-C. Chang, A semi-blind digital watermarking scheme based on singular value decomposition, Comput. Stand. Interfaces 28 (4) (2006) 428–440.

[10] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Process. 88 (9) (2008) 2158–2180.

[11] W. Lu, H. Lu, F.-L. Chung, Feature based robust watermarking using image normalization, Comput. Electr. Eng. 36 (2010) 2–18.

[12] L. Ghouti, A. Bouridane, M. Ibrahim, S. Boussakta, Digital image watermarking using balanced multiwavelets, IEEE Trans. Signal Process. 54 (4) (2006) 1519–1536.

[13] M. Ouhsain, A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform, Expert Syst. Appl. 36 (2) (2009) 2123–2129.

[14] G. Bhatnagar, R. Balasubramanian, A new robust reference watermarking scheme based on DWT-SVD, Comput. Stand. Interfaces 31 (5) (2009) 1002–1013.

[15] P. Kumsawat, K. Attakitmongcol, A. Srikaew, A new approach for optimization in image watermarking by using genetic algorithms, IEEE Trans. Signal Process. 53 (12) (2005) 4707–4719.

[16] F.Y. Shih, Y.-T. Wu, Enhancement of image watermark retrieval based on genetic algorithms, J. Vis. Commun. Image Represent 16 (2) (2005) 115–133.

[17] V. Aslantas, A singular-value decomposition-based image watermarking using genetic algorithm, Int. J. Electron. Commun. (AEÜ) 62 (5) (2008) 386–394.

[18] O. Fındık, I. Babaoˇglu, E. Ülker, A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm, Opt. Commun. 283 (24) (2010) 4916–4922.

[19] Y.-R. Wang, W.-H. Lin, L. Yang, An intelligent watermarking method based on particle swarm optimization, Expert Syst. Appl. 38 (7) (2011) 8024–8029.

[20] H.-H. Tsai, Y.-J.Jhuang, Y.-S.Lai, An SVD-based image watermarking in wavelet domain using SVR and PSO, Appl. Soft Comput.J. (2012).