© 2017 IJSRST | Volume 3 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Novel Hybrid Digital Image Watermarking Scheme based on IWT and SVD

K. Basavaraju
Department of ECE, Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India

ABSTRACT

In this paper, A Hybrid Digital Image Watermarking method using IWT and SVD is presented which can be used for copyright protection through owner identification. The watermark pixel values are directly embedded into the singular values of 1-level IWT decomposed sub-bands. Digital signature based authentication mechanism is used to solve the false positive problem faced by most of the SVD-based watermarking methods. The digital signature mechanism consists of signature generation, embedding after embedding the watermark and extraction. The ownership is then authenticated before extraction of watermarks. Hence the scheme attains security. The experimental results reveal the superiority of the proposed method in terms of imperceptibility, robustness and capacity due to the properties of IWT and SVD. To verify the feasibility of the proposed scheme, MATLAB simulation is used.

Keywords : Integer wavelets transform, Singular value decomposition, Imperceptibility, Robustness, Security.

I. INTRODUCTION

Digital watermarking is a process of hiding some useful information in to the digital data. In the digital world the digital content can be easily controlled, so the authentication is necessary to check the completeness of the data. Digital watermarking is the optimum technique to provide authentication. Apart from authentication digital watermarking also used for the fingerprinting, broadcast monitoring and authentication applications. In the digital image watermarking process some image is embedded into the original image which allows it to be extracted later for security purpose.

Most of the existing methods are of invisible type of digital image watermarking are concentrated. Transform domain watermarking techniques such as Discrete wavelet transform (DWT) [3], Redundant discrete wavelet transform (RDWT) [1,2], Lifting wavelet transform (LWT) [4] are employed to perform digital image watermarking due to their features. The challenges related to any watermarking scheme are imperceptibility, robustness, security and data payload. Robustness is the techniques resistance against image processing and geometrical attacks. All methods don't resist all attacks which depend on application [9]. Data payload refers to number of watermarking bits ciphering in a message [10]. The similarity measurement between the original image and the watermarked image is called as imperceptibility. Imperceptibility is evaluated through PSNR and high PSNR refers to high imperceptibility. Generally for any watermarking scheme the minimum PSNR is 38 dB [5]. Security indicates resistance against hostile attacks with respect to the technique.

A number of robust watermarking methods using SVD were developed [11,12,13,14]. The existing hybrid methods can be improved in terms of many factors include imperceptibility, robustness and security are major concerned. To improve these factors of watermarking, a new hybrid technique employed in the proposed scheme called IWT-SVD scheme to overcome the existing schemes [2, 3, 4] drawbacks. Integer wavelet transform (IWT) is a reversible lifting wavelet transform which is lifted to another transform with particular properties and which maps integers to integers without rounding errors [19], allowing the custom design of filters. It is provided that all classical transforms implemented using lifting schemes [6], possessing a number of advantages over the classical wavelet transforms. Transform is easy to understand, easy to implement and easy to invert [7, 8] and also very

fast because all calculations are performed in-place and auxiliary memory isn't required [7]. The implementation steps of LWT involve splitting, predicting and updating.
The singular value decomposition (SVD) is a numerical analysis technique is effective and widely used in image processing applications [2,4]. Applying SVD on any medium, such as image results into three matrices. SVD of any matrix B is defined as follows:

$$\text{SVD}(\mathbf{B}) = \boldsymbol{USV^T} \quad (1)$$

$$\mathbf{U} = [\mathbf{u_1}, \mathbf{u_2}, \ldots \mathbf{u_N}] \quad (2)$$

$$\mathbf{V} = [\mathbf{v_1}, \mathbf{v_2}, \ldots \mathbf{v_N}] \quad (3)$$

$$\mathbf{S} = \begin{bmatrix} S_1 & & \\ & S_2 & \\ & & S_N \end{bmatrix} \quad (4)$$

where **U** and **V** are $N \times N$ orthogonal matrices and their column vectors are Eigen vectors and **S** represents $N \times N$ diagonal matrix including the singular values S_i in decreasing order [4]. The SVD technique is popular in image processing applications due to its features which are in the following [1,4]:

- SVD can be applied on rectangle or square matrices.
- Good stability of the singular values S_i of any image.
- The **S** of an image indicates it algebraic properties, represents an image's luminance, where the singular vectors represent the geometry properties of an image.
- Singular values are in descending order.

The rest of the paper as organized as follows, Section 2 contains the detailed explanation of proposed algorithm, Section 3 contains the implementation steps. The experimental results are given in Section 4, and finally conclusion in Section 5.

II. PROPOSED ALGORITHM

In this paper, the process of proposed algorithm is explained. The algorithm has two processes include watermark embedding and extracting. Before going to explain the processes, authentication procedure will be explained in the following.

A. Authentication process

The Authentication procedure is proposed as one of the solution for the false positive detection suggested by [18] and the problem has occurred in number of SVD-based watermarking schemes [15]. The flaw in such schemes due to **U** and **V** which preserves the most information of the image, therefore the attacker can claim ownership using forged singular vectors to obtain a unique forged watermark regardless of the extracted singular values [16,17]. The authentication process consists of signature generation, embedding and extraction procedures. Signature based authentication mechanism involves unique generation of signature from orthogonal **U** and **V** matrices and embedded into the watermarked image to have watermarked image with sign encryption seems to as same as original image. In detection side, the decoder extracts the signature and compares it with the signature generated at the person side based on received **U** and **V**. If the signatures matched after authentication, watermark extraction process is continued otherwise the extraction process is halted.

1) Signature generation procedure :

The signature has distinct binary digits generated using **U** and **V** matrices. The digital signature generation steps listed in the below:

- Transform the orthogonal matrices U and V from 2-D to 1-D arrays.
- Hash U and V using Secure Hash Algorithm-1.

$$\text{Digest}_{\mathbf{U}} = \text{Hashing}_{(\text{SHA}-1)}(\mathbf{U}) \quad (5)$$

$$\text{Digest}_{\mathbf{V}} = \text{Hashing}_{(\text{SHA}-1)}(\mathbf{V}) \quad (6)$$

- Convert the Digest_U and Digest_V into their corresponding binary digits, and then do XORing between them, assume the result as R_1.
- Convert the selected secret key into binary digits, assume the result as R_2.
- Perform an Exclusive-OR operation between R_1 and $R2_.$.
- For authentication purposes, select the first 8-bits of the result (R) as a digital signature bits stream.

2) Signature embedding procedure :

Embed the the 8-bit digital signature stream into pixels that are robust against attacks which doesn't modify the image quality. The SVD technique offers to embed the signature. The signature embedded through modifying the elements of a **U** matrix. DWT technique carried out for simplicity and better security to decompose the watermarked image before embedding the signature. The following are steps of signature embedding:

- Perform the 1-level DWT on to the watermarked image.
- Divide the LL sub-band into 8 × 8 blocks.
- Randomly select eight blocks with the help of the secret key.
- For each selected block, perform SVD.
- Round each element of **U** to the nearest integer less than or equal to its integer part after multiplying **U** by 10, as follows:

$$\boldsymbol{U_{modified}} = \lfloor \boldsymbol{U} \times 10 \rfloor \quad (7)$$

- Examine the $\boldsymbol{U_{modified}}$ based on the digital signature bits stream (Sig):

If sign bit = 1 and $\boldsymbol{U_{modified}}$ = even or sign bit = 0 and $\boldsymbol{U_{modified}}$ = odd then increase $\boldsymbol{U_{modified}}$ by 1 and divide results by 10. Otherwise keep $\boldsymbol{U_{modified}}$ unchanged.

- Perform inverse SVD and DWT for all selected blocks.
- The Signed watermarked image is obtained.

3) Signature extracting procedure :

The signature extraction process is exactly the reverse process of signature embedding. The following are steps of signature extraction:

- Perform the 1-level DWT on the received image (watermarked image).
- Divide the LL sub-band into 8 × 8 blocks.
- Select the blocks based on the secret key.
- Perform SVD for all the selected blocks.
- Examine **U**, if the mod($\lfloor \boldsymbol{U} \times 10 \rfloor$, 2) = = 0 then Sig(i) = 1 Otherwise Sig(i) = 0.
  where i =1, ...,8 is the digital signature length.

III. IMPLEMENTATION

A. Embedding Process

The complete embedding process is explained in Figure 2. The embedding process consists the following steps:

- Apply 1-level IWT to decompose the host image into four frequency bands, includes low, high and middle frequency bands.
- Apply SVD on four frequency bands as mentioned below:

$$\mathbf{B_i} = \mathbf{U_i S_i V_i^T} \quad (8)$$

where i = LL, HL, LH, HH.

- Embed the watermark directly to modify the singular values (S_i) of each sub-band.

$$\mathbf{S_i} + \alpha \mathbf{W} = \mathbf{U_i^W S_i^W V_i^{TW}} \quad (9)$$

where α is a scaling factor

- Perform the above signature generation procedure to the four corresponding sets ($\mathbf{U_i^W}$ and $\mathbf{V_i^{TW}}$) of the four sub-bands. Therefore, four 8-bit digital signatures are generated.
- Finally, the 8-bit digital signature obtained by doing XOR operation on four generated signatures.
- Modified IWT coefficients for each frequency band obtained by:

$$\mathbf{B_i} = \mathbf{U_i S_i^W V_i^T} \quad (10)$$

- Apply the inverse IWT to get the watermarked image by:

$$B_W = IW\ T^{-1} \quad (11)$$

- Digital signature is embedded into the watermarked image through the above mentioned signature embedding procedure.

B. Extraction Process

The Extraction process is reverse process of the embedding process as shown in Figure 3. The extraction process consists of the following steps:

- Apply 1-level IWT on a watermarked image $\mathbf{B_i}^{*\mathbf{W}}$ (barely distorted) to decompose into four frequency bands.
- Perform SVD operation on four sub-bands :

$$\mathbf{B_i}^{*\mathbf{W}} = \mathbf{U_i^* S_i^* V_i^{*T}} \quad (12)$$

- Estimate the detection by

$$\mathbf{D_i^*} = \mathbf{U_i^W S_i^* V_i^{TW}} \quad (13)$$

- Extract the watermarks from each sub-band:

$$\boldsymbol{W_i^*} = {}^{(\boldsymbol{D_i^*} - \boldsymbol{S_i})}/_{\boldsymbol{\alpha}} \quad (14)$$

(a) (b) (c) (d)

Figure 1: (a) Host image, (b) Watermark, (c) Watermarked image, (d) Signed watermarked image.

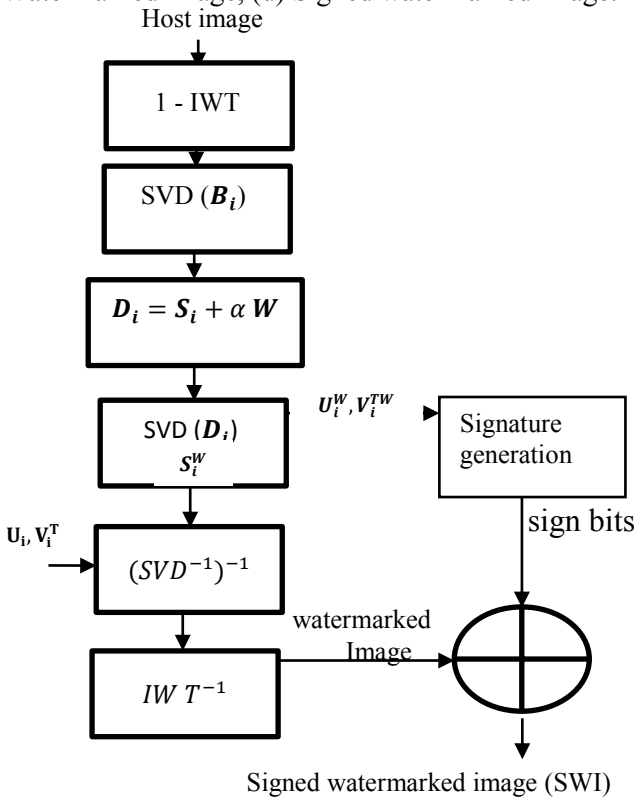

Figure 2 : The watermark embedding process

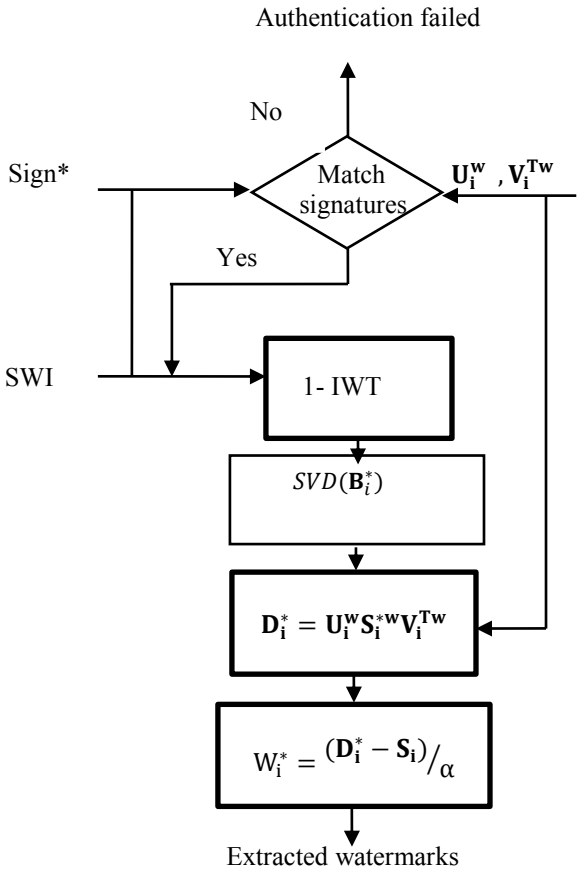

Figure 3: The watermark extracting process

IV. EXPERIMENTAL RESULTS

The proposed scheme is implemented using MATLAB and tested on standard images considered as a host image of size 128×128 and the Cameraman for watermark image of size is half of the size of host image due to decomposition analysis. There are two scaling factors are used, it is for 0.05 for LL sub-band and 0.005 for remaining sub-bands to have a fair comparison with existing schemes [2,3]. Figure 1 shows host image, watermark image, watermarked image and signed watermarked image. The PSNR is used to estimate the imperceptibility as similarity between the host image and watermarked image because the host image is affected due to the embedding process by small margin. The PSNR can be calculated as follows:

$$PSNR = 10log_{10}\left(\frac{\max(X(i,j))^2}{MSE}\right) \quad (15)$$

Where the Mean Square Error (MSE) between the host image X and the watermarked image Y is defined in the following:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j) - Y(i,j)]^2 \qquad (16)$$

The Imperceptibility comparison using PSNR (dB) is shown in Table 1. The minimum acceptable PSNR value in the watermarking world is 38dB[5]. The achieved PSNR value is considered to be good and high value even though it is lower than the existing scheme [1] and higher than the reported [2].

The robustness can be evaluated by calculating the Normalized Cross-Correlation (NC) which indicates the similarity between the original watermark and the extracted watermark after an attack. Generally, the NC value is acceptable if it is greater than or equal to 0.75. The NC is defined as:

$$NC(w,\bar{w}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j)-\mu_w][\bar{w}(i,j)-\mu_{\bar{w}}]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j)-\mu_w]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[\bar{w}(i,j)-\mu_{\bar{w}}]^2}} \qquad (17)$$

where M and N indicate the number of rows and columns of watermark image, w and $\bar{w}$ indicate the original watermark and the extracted watermark respectively.The μ_w and $\mu_{\bar{w}}$ indicate the mean of the original watermark and the mean of the extracted watermark respectively. The NC value in Table 2 shows that the proposed scheme is robust against the number of attacks with respect to existing scheme. The noise addition attacks such as salt and pepper noise, speckle noise and Gaussian noise with noise density are tested. Other attacks include filtering, JPEG compression and scaling attacks are performed. The implemented scheme exhibited a higher resistance against attacks with respect to the existing scheme. The capacity in the proposed scheme is 64×64 considered to be high but the existing scheme achieved twice this capacity due to RDWT decomposition analysis. Thus the trade-off between the conflicting parameters is compromised in the implemented scheme. Figure 4 shows Lena watermarked image under different attacks and Figure 5 shows the extracted watermarks under different attacks.

Table1: Imperceptibility comparison values using PSNR (dB)

Image name	**IWT-SVD (this paper)**	**RDWT-SVD[1]**	**RDWT-SVD**[2]
Lena	43.9861	54.0353	38.52

Table 2 : Comparison of the robustness of proposed scheme with the existing scheme.

Attacks		**LL**	**LH**	**HL**	**HH**
Salt & pepper noise 0.001	RDWT IWT	0.9750 0.9897	0.8699 0.9717	0.8680 0.9674	0.8571 0.9322
Speckle noise 0.001	RDWT IWT	0.9720 0.9907	0.8391 0.9727	0.8516 0.9684	0.7973 0.9332
Gaussian noise 0.001	RDWT IWT	0.9790 0.9901	0.8675 0.9721	0.8853 0.9678	0.7807 0.9326
Wiener filter (7,7)	RDWT IWT	0.9640 0.9719	0.9384 0.9608	0.9545 0.9584	0.9492 0.9586
JPEG Compr-ession Q=30	RDWT IWT	0.9870 0.9928	0.9327 0.9649	0.9222 0.9721	0.8498 0.8915
Scaling(0.5,2)	RDWT IWT	0.9480 0.9790	0.8094 0.8945	0.7467 0.8703	0.8605 0.8993

Figure 4 : Lena image under different attacks (a) Salt & pepper noise 0.001, (b) Speckle noise 0.001, (c) Gaussian noise 0.001, (d) Wiener filter (7, 7), (e) JPEG compression Q=30, (f) Scaling (0.5, 2)

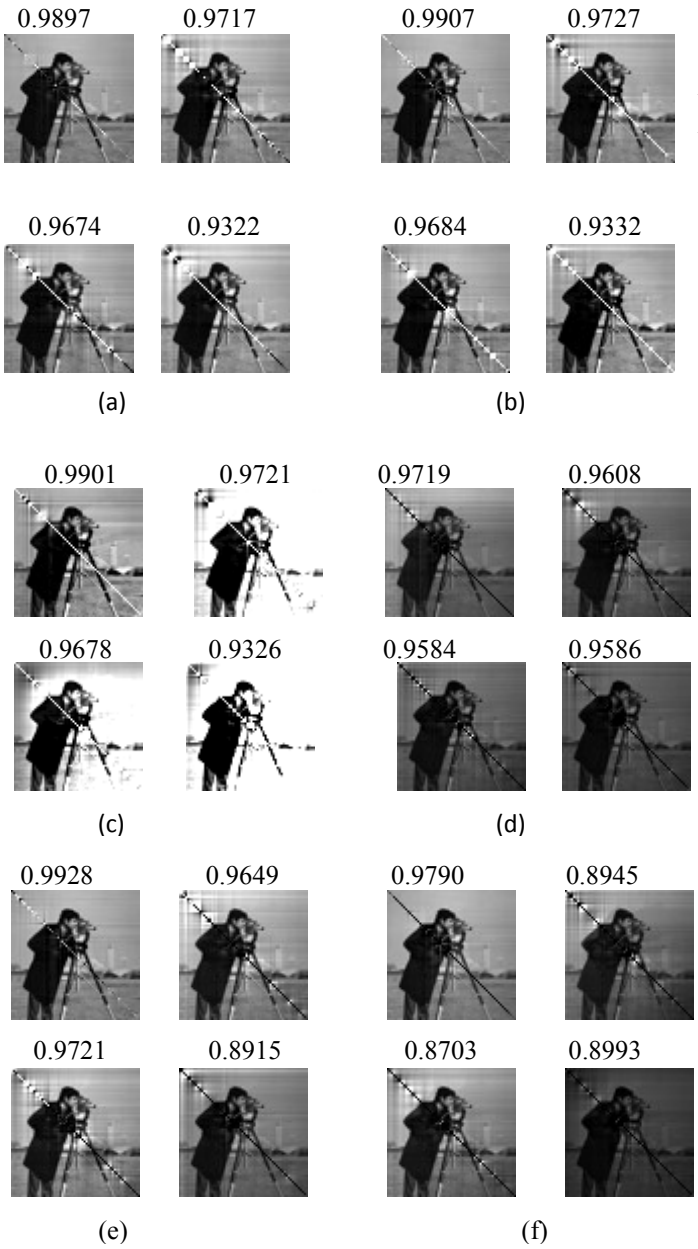

Figure 5 : Extracted watermarks from four sub-bands under the mentioned attacks

V. Conclusion and Future Scope

In this paper, a novel hybrid, secure and robust image watermarking scheme based on the IWT and SVD is implemented. Hybrid scheme employs properties of IWT and SVD transforms to get the requirements of watermarking. These properties include perfect reconstruction due to IWT in which integers are mapped to integers and the good stability of the SVD. In addition to that security is improved due to a digital signature authentication mechanism. Hybrid scheme shows high resistance against attacks. Our proposed scheme performs better compared to the existing schemes in terms of Imperceptibility, robustness, security and capacity. Future work will continue to improve a robust SVD-based watermarking scheme through embedding the watermark into the singular vectors which improves the robustness and security additionally.

VI. REFERENCES

[1]. N. M. Makbol, B.E. Khoo, Robust blind image watermarking scheme based on RDWT and SVD, AEÜ,Int. J. Electron. Commun. 67 (2) (2013) 102-112.

[2]. S. Lagzian, M. Soryani, M. Fathy, Robust watermarking scheme based on RDWT-SVD: embedding data in all subbands, in: International Symposium on Artificial Intelligence and Signal Processing (AISP), 2011, pp. 48-52

[3]. E. Ganic, A.M. Eskicioglu, Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition, J. Electron. Imaging 14 (4) (2005) 043004.

[4]. K. Loukhaoukha, J.Y. Chouinard, Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification, in: Canadian Workshop on Information Theory, 2009, pp. 177-182.

[5]. Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, C.P. Chang, High-payload image hiding with quality recovery using tri-way pixel-value differencing, Inf. Sci. 191 (2012) 214-225.

[6]. W. Sweldens, The lifting scheme: aconstruction of second generation wavelets,SIAM J. Math. Anal. 29 (2) (1998) 511-546.X.P. Zhang, K. Li, Comments on "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimed. 7(3) (2005) 593-594.

[7]. I. Daubechies, W. Sweldens, Factoring wavelet transforms into lifting steps,J. Fourier Anal. Appl. 4(3) (1998) 245-267.H. Chao and P. Fisher, An approach of fast integer reversible wavelet transform for image compression, preprint, Infinop, Deaton, TX 76208 1996.

[8]. Z.-z. Jia, H.-Y. Zhu, W.-s. Cheng, Ablind watermarking algorithm based on lifting wavelet transform and scrambling technology, in: International Conference on Electrical and Control Engineering (ICECE), 2010, pp. 4576-4579.G. Strang, T. Nguyen. Wavelets and Filter Banks.Wellesley-Cambridge Press, 1996.

[9]. A. Koz, Digital watermarking based on human visual system, Master's thesis, Dept. of Electrical and Electronics Engineering, Orta Dogu Teknik University,2002.
[10]. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd ed., Morgan Kaufmann Publishers Inc., San Francisco, CA,USA, 2007.
[11]. R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimed. 4(1) (2002) 121-128.
[12]. S. Lagzian, M. Soryani, M. Fathy, Anew robust watermarking scheme based on RDWT-SVD, Int. J. Intell. Inf. Process. 2(1) (2011) 22-29.
[13]. S. Rastegar, F. Namazi, K. Yaghmaie, A. Aliabadian, Hybrid watermarking algorithm based on singular value decomposition and radon transform, AEÜ, Int. J.Electron. Commun. 65 (7) (2011) 658-663.
[14]. C.C. Lai, C.C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE Trans. Instrum. Meas. 59 (11) (2010) 3060-3063.
[15]. L. Xiao, Z. Wei, J. Ye, Comments on "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition" and theoretical analysis, J. Electron. Imaging 17 (4) (2008) 040501.
[16]. X.P. Zhang, K. Li, Comments on "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimed. 7(3) (2005) 593-594.
[17]. H.C. Ling, R.C.W. Phan, S.H. Heng, On the security of a hybrid watermarking algorithm based on singular value decomposition and radon transform, AEÜ,Int. J. Electron. Commun. 65 (11) (2011) 958-960.
[18]. A. Gupta, M. Raval, A robust and secure watermarking scheme based on singular values replacement, Sadhana 37 (2012) 425-440.
[19]. A. Calderbank, I. Daubechies, W. Sweldens, B.L. Yeo, and Wavelet transforms that map integers to integers, Appl. Comput. Harmon. Anal. 5(3) (1998) 332-369.