A new DWT-SVD based robust watermarking scheme for real property rights

Sedigeh Razavi Babakalak, Mohammad Ali Balafar, Ali Farzan

MSC Student of computer Science, of Shabestar Branch, Islamic Azad University, Shabestar, Iran, razavi183@gmail.com
Department of Computer, Faculty of Engineering, University of Tabriz, Tabriz, Iran, balafarila@yahoo.com
Department of Computer, Faculty of Engineering, Islamic Azad University of Shabestar, Shabestar, Iran, afs1376@gmail.com

ABSTRACT

In this paper, a new robust digital image watermarking algorithm which was based on singular value decomposition (SVD) and discrete wavelet transform (DWT) was proposed and simulated for protecting real property rights. A gray scale logo image, rather than a randomly generated Gaussian noise type watermark, was used as a watermark. Its embedding algorithm hid a watermark LL sub-band blocks in the low–low (LL) and high-high (HH) sub-bands of a target non-overlapping block of the host image by modifying singular values (SVs) on SVD version of these blocks. A semi-blind watermark extraction algorithm was designed to estimate the original coefficients.

Experimental results showed that the proposed scheme made significant improvements in terms of both transparency and robustness and was superior to the existing methods which were considered in this paper.

Keywords: Watermarking, Singular value decomposition, discrete wavelet transform, false-positive problem, scaling factor.

1. INTRODUCTION

With the rapid spread of multimedia and networking technologies, digital media are easily copied and rapidly distributed over the Internet [1]. Illegal copying and modifying, copyright protection, and property rights of digital media have started to be challenging. Digital watermarking as the process of embedding a secret signal in the original data provides a solution for these problems in multimedia data [2].

There are two main requirements for digital watermarking: transparency and robustness.

Transparency means that human visual system should not be able to take cognizance of the watermark in a watermarked image [3]. In other words, perceptual similarity between the original and watermarked versions of the cover objects is called transparency [4]. Also, watermarks can be removed by intentional and unintentional attacks such as scaling, rotation, or common image processing operations. Therefore, a watermark should be robust and remain detectable after such attacks. In other words, the ability to detect the watermark after performing common operations, such as compression, printing, geometric distortion on watermarked contents, is called robustness [5].

Watermarking can be performed in spatial or transform domains. Spatial domain schemes embed the watermark by directly changing the pixel values of the original image. Examples of spatial domain methods can be found in [6, 7]. On the other hand, transform domain methods embed the watermark by changing the coefficients in a transform domain; for example, discrete cosine transform (DCT) [8], discrete Fourier transform (DFT) [9], discrete wavelet transform (DWT) [10, 11], and singular value decomposition (SVD).

The SVD-based watermarking is one of the most powerful watermarking schemes. In the literature, watermarking algorithms based on SVD insert the watermark in different ways. The simplest embedding scheme consists in adding the SVs of the watermark image by modifying the SVs of the host image. The first SVD-based watermarking algorithm was introduced by Liu et al. [12]. It performs two times of the SVD transformation during embedding phase and hides the watermark in the SVs of the SVD-domain image. Although this method performs well on transparency and robustness but it still has two weaknesses. First, the method needs highly computational complexity due to two times of SVD during the watermark-embedding phase. Second, it requires original images during the watermark-extraction phase. Accordingly, this method fails to overcome the false-positive problem [13]. Chandra [14] introduced a robust method by embedding SVs of the watermark in the SVs of the host image. 1n 2007, Li et al. [15] proposed a hybrid DWT-SVD domain watermarking scheme considering the properties of human visual system (HVS). After decomposing the host image into four sub-bands in the DWT domain, they applied SVD to each sub-band and embedded SVs of the watermark in the sub-bands. The embedding robustness was determined by a human visual model. Bhatnagar et al. [10] introduced a semi-blind reference watermarking scheme based on DWT-SVD for copyright protection and authenticity. They embedded watermark in the reference image by modifying the SVs of reference image using the SVs of the watermark image. Although these methods have high robustness against attacks but still unresolved false-positive problem. To improve robustness of Liu's proposed model, Aslantas [16] and Lai [17] have presented a new model using genetics algorithm, in which watermark embedding is the same as Liu's and only robustness of the mentioned model is increased by genetic algorithm.

All the models investigated here, embed only the SVs of the watermark image into the SVs of the host image. This strategy leads to the false-positive detection problem. False-positive detection problem occurs when a specific watermark is extracted from a content in which a different watermark is embedded and thus an ambiguous situation is developed. This issue does not allow for solving real property rights.

In general, SVD-based watermarking methods which embed the SVs of the watermark into the SVs of the host image are considered invertible schemes [3].

Therefore, this embedding method not only does not solve the property right problem, but also makes another problem. Thus, watermark embedding should be in a way that it would be impossible to extract false-positive watermarks.

As a result, Muhammad et al. [3] proposed a watermarking model which solved the false-positive problem. Given the host image A and visual watermark W, the main step of Mohammad's embedding algorithm can be explained in the following:

1. Perform SVD on the original image A:

$$A = USV^T \qquad (1)$$

2. Add the watermark image W to S, with a scaling factor α as

$$S_n = S + \alpha W \qquad (2)$$

3. Obtain the watermark image A_w:

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

$$A_w = US_nV^T \quad (3)$$

Attend that the scaling factor, α, is a scalar constant value.

To extract the watermark from a possibly distorted watermarked image A_w^*, their algorithm proceeds as follows:

1. Obtain the corrupted matrix S_n^* as (4)

$$S_n^* = U^T A_n^* V \quad (4)$$

2. Reverse step 2 of the embedding procedure to get a possibly distorted watermark W^* as follows:

$$W^* = \frac{1}{\alpha}(S_n^* - S) \quad (5)$$

This method can easily solve the false-positive problem in [12]; but, robustness and transparency are still a big problem.

Watermarking should be solve False-Positive problem in addition to being robust and transparent; in SVD-based watermarking methods, robustness and transparency are controlled by scaling factor (SF). In most of the proposed models, SF is selected as a constant between 0 and 1. Although all watermarks are embedded in a host image, different watermarks need different SFs. Thus, selecting an appropriate SF in SVD-based watermarking is very important and using different SFs for watermarking leads to obtaining transparent and robust watermarks.

Consequently, it motivated us to design a new SVD-DWT based watermarking scheme, which possesses high robustness and high transparency.

In this paper, a combination of SVD and DWT methods is used to present an optimal watermarking method. In this method, first, watermark and host images are taken to discrete wavelet transform domain and then HH and LL sub-bands of the host image are blocked and SVD is applied to each block of the host image. Afterward, blocks of LL sub-band of the watermark image are embedded in the singular values of the blocks of the host image and a different SF is used for each blocks.

Using this method, it was expected to obtain a robust watermark image owing to using DWT and different SFs for each block and, because embedding blocks of LL sub-band of watermark image, forging the watermarked image would be impossible. Therefore, false-positive detection problem was solved. Also, transparency of the watermarked image was expected to increase due to the combination of SVD and DWT and watermark embedding method.

The rest of this paper is organized as follows. Section 2 introduces the background knowledge involved in this paper. Section 3 explains selecting a suitable scaling factor. Section 4 introduces the proposed scheme. The experimental results described in section 5. The comparison and conclusion are discussed in sections 6 and 7, respectively.

2. BACKGROUND

2.1. SINGULAR VALUE DECOMPOSITION

In linear algebra, SVD is a famous method for decomposing a rectangular matrix, real or complex. From the perspective of image processing an image can be viewed as a matrix with non-negative numeric entries. SVD on image A with size L×K is defined in the following way by (6):

$$A = USV^T \quad (6)$$

Where U and V are called left and right singular vectors and T represents the conjugate transpose operation. Matrix S is a singular value and diagonal matrix with non-negative real numbers.

2.2. DWT

One of the main challenges of the watermarking problem is in obtaining a better tradeoff between robustness and perceptivity. DWT is highly preferred, because it provides both simultaneous spatial localization and frequency spread of the watermark within the host image [18]. By applying **the DWT**, an image **is decomposed into four** sub-bands. The most important part of the image resides in **the** LL sub-band **that includes low frequency wavelet coefficients**. **Edges and details are usually in the high frequency sub-bands**. **DWT is superior to other translations due to the characteristics of multi-resolution and excellent image localization, similar to HVS**.

3. SELECTING A SUITABLE SCALING FACTOR

Scaling factor is a numerical factor that controls the transparency and robustness of watermarked images in SVD-based watermarking schemes. The smallest problem which occurs in SVD-based watermarking schemes is related to transparency, because scaling factors have been usually selected in the range of 0 to 1 (0<α<1) in most of the previous studies. Selecting a suitable scaling factor is one of the most challenging steps in SVD-based watermarking and the selected scaling factor is generally a constant scalar number.

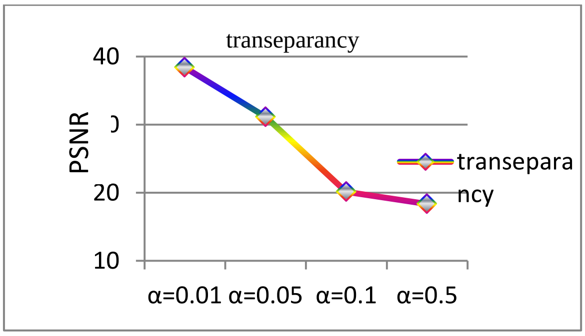


FIGURE 1. Transparency of watermarked image for several scaling factor

FIGURE 1 shows the PSNR of the watermarked image for several different scaling factors and FIGURE 2 demonstrate the correlation coefficient of the extracted watermark for several different scaling factors. These figures represent that the higher the scaling factor, the less the robustness and, consequently, the higher the invisibility of the watermark would be.

Therefore, selecting a suitable scaling factor is one of the major challenges in SVD-based watermarking schemes. A number which could balance the robustness and transparency of the watermarked image and cannot be easily guessed by an attacker should be selected for this factor.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

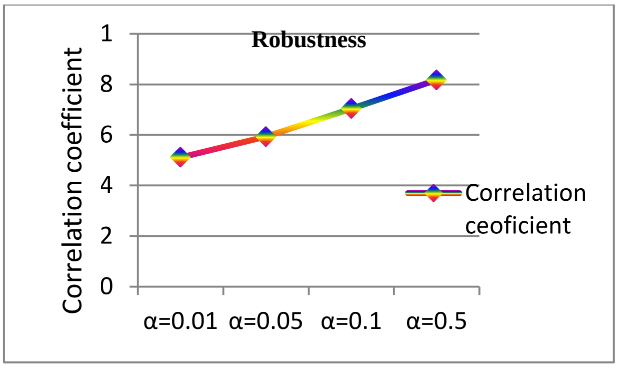


FIGURE 2. Robustness of watermarked image for several Scaling factor

4. PROPOSED METHOD

In this section, we present proposed algorithm. Without less of generality, assume the size of the watermark W to be equal to the size of the original image A.

4.1. WATERMARK EMBEDDING ALGORITHM

The following steps summarize the embedding algorithm for the proposed method:

1) Decomposing the host image A into four sub-bands using DWT: Approximation coefficient LL and detailed coefficients HL, LH, and HH $A \rightarrow \{LL_A, LH_A, HL_A, HH_A\}$.
2) Partitioning LL_A and HH_A sub-bands into M×M blocks: LL_{Aij} and HH_{Aij}.
3) Performing SVD operation for each block of two sub-bands (LL_A and HH_A) of the host image:

$$K_{Aij} = U_{Kij} S_{Kij} V_{Kij}^T \qquad (7),$$

Where $k \in \{LL_A, HH_A\}$.

4) Performing DWT on the watermark image W, $W \rightarrow \{LL_w, LH_w, HL_w, HH_w\}$.
5) Partitioning LL_w sub-band of watermark image into M×M blocks, such as LL_{wij}.
6) Inserting the blocks of LL_w into the singular values of the blocks of LL_A and HH_A sub-bands of the host image (i.e. the proposed scheme embedded the watermark in the host image twice (LL and HH sub-bands)):

$$S_{nKij} = S_{Kij} + \alpha_{ij} LL_{wij} \qquad (8),$$

Where, $k \in \{LL_A, HH_A\}$

Here, α_{ij} demonstrate different scaling factors for each block of the host image.

7) Performing inverse SVD for each block of the mentioned sub-bands of host image and computing the modified coefficients for LL_A and HH_A sub-bands of the host image.
8) Applying the inverse discrete wavelet transform (IDWT) to the modified coefficients to obtain the watermarked image A_w.

4.2. WATERMARK EXTRACTION ALGORITHM

1) Applying DWT to the possibly attacked watermarked image A_w^*:

$$A_W^* \rightarrow \{LL_{A_W^*}, LH_{A_W^*}, HL_{A_W^*}, HH_{A_W^*}\}$$

2) Getting LL_{Aij} and HH_{Aij} blocks of LL_A and HH_A sub-bands of the original image A and applying SVD to each block

$$K_{Aij} = U_{Kij} S_{Kij} V_{Kij}^T \qquad (9),$$

Where, K={LL_A , HH_A}

3) Obtaining the corrupted matrix S^*_{nij} for each block

$$S^*_{nij} = U^T_{K_{Aij}} K^*_{ij} V_{K_{Aij}} \qquad (10),$$

Where, K={LL_A,HH_A} and K^*={$LL_{A^*_W}$, $HH_{A^*_W}$}

4) Reversing Step 2 of the embedding procedure to get a possibly distorted watermark LL_w^* sub-band block as follows:

$$LL_{ext_{ij}}^{w} = {}^{1}\!/_{\alpha}\left(S^{k*}_{n_{ij}} - S^{K}_{ij}\right) \qquad (11)$$

5) Applying inverse discrete wavelet transform (IDWT) to LL-ext coefficient and detailed coefficients HL_w, LH_w, and HH_w to obtain the extracted watermark image W^*.

5. EXPERIMENTAL RESULT

This section presents the experimental setup and results of the SVD-DWT-based image watermarking. In order to investigate the proposed watermarking algorithm, MATLAB platform was used and a number of experiments were performed on different images with the size of 256×256, namely Lena, Baboon and Elaine. The watermark image was a gray scale logo of size 256×256.

(a) (b) © (d)

FIGURE 3. The host images and watermark image. Panel (a)–(c) represent Lena, Baboon, Elaine, respectively; (d) exhibits a watermark

FIGURE 3 (a)-(c) shows 3 host images and FIGURE 3 (d) exhibits a watermark image.

The similarity between W (original watermark) and W^* (extracted watermark) can be measured by means of normalized correlation coefficient, defined as:

$$\mathrm{Corr}(W, W^*) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(W_{ij} - \bar{W}\right)\left(W^*_{ij} - \bar{W}^*\right)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(W_{ij} - \bar{W}\right)^2} \cdot \sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(W^*_{ij} - \bar{W}^*\right)^2}}$$

$$\bar{W} = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N} W_{ij} \qquad (12)$$

$$\bar{W}^* = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N} W^*_{ij}$$

Quality of the watermarked image can be estimated using peak signal-to-noise ratio (PSNR) in (13).

$$\mathrm{PSNR} = 10\log\frac{255^2}{\mathrm{MSE}} \qquad (13)$$

$$MSE = \frac{1}{NN}\sum_{i=1}^{N}\sum_{j=1}^{N}(A - A_w)^2 \qquad ,$$

Where, A and A_w are the original host image and watermarked image, respectively. FIGURE 4 illustrates the results of watermarking using the proposed method and FIGURE 4 (a) and (b) display the original host image and watermark image, respectively. The watermarked image is shown in FIGURE 4 (c). The PSNR value between the original host image and watermarked image was 36.20; i.e. quality of the watermarked image was acceptable and it was invisible for the human vision.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

FIGURE 4 (d) shows the extracted watermark for LL and HH sub-bonds. Since the watermark was embedded for 2 sub-bonds, at the watermark detection stage, two extracted watermarks were obtained. The correlation coefficients of the 1^{st} and 4^{th} quadrant were 1. Based on these values, the extracted watermark was the same as that of the original watermark image.

(a)	(b)	©	(d)

FIGURE 4. Result of proposed method

5.1.FALSE-POSITIVE DETECTION TEST FOR THE PROPOSED METHOD

As stated in [19, 20] the major flaw in the watermarking schemes of SVD-based images occurs by embedding SVs of watermark into host images. Consider two matrices A and B and apply SVD to them; $A = U_A S_A V_A^T$, and $B = U_B S_B V_B^T$. If SVs of these two matrices are replaced, then: $A \cong U_A S_B V_A^T$, and $B \cong U_B S_A V_B^T$. Accordingly, false-positive extraction problem will always occur in SVD-based watermarking schemes that embed only SVs of watermark in the host image. In fact, SVs U and V own a large part of image information [20]. For watermark extraction phase, Liu's algorithm requires SVs of watermark image i.e. U_w and V_w to be available.

It can be shown that, using the pair of SVD reference watermark (U_w, V_w) at extraction stage, false-positive detection will be a probability of one. In other words, SVs of each counterfeit watermark at the extraction stage can be used to claim that this watermark is an embedded one. As can be observed, in Liu and Tan's scheme, an attacker can easily prove its claim.

In this paper, a reliable DWT-SVD-based watermarking scheme was proposed for solving the problem which occurred in [12]. In this scheme, the LH_w, HL_w, and HH_w sub-bands of the embedded watermark were recorded for the extractions stage. If an attacker claimed the ownership of the watermarked image with another counterfeit watermark image, and using the LH, HL, HH sub-bonds of DWT reference counterfeit watermark image, the result of watermark extraction process would be the embedded watermark image and thus the attacker's claim would fail.

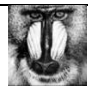
As can be observed, in the proposed method, the attacker's claim was rejected and false-positive extraction became impossible. In this method, only the embedded watermark image was extracted.

5.2. ROBUSTNESS TEST FOR PROPOSED METHOD

In order to demonstrate the robustness of the proposed watermarking algorithm, the watermarked image was attacked by a variety of attacks, namely filtering, noise addition, histogram equalization, cropping, and JPEG compression. After these attacks on the watermarked image, the extracted logo was compared with the original watermark by normalized correlation metric, while PSNR metric was used to analyze perceptual similarity between the original and attacked watermarked images.

TABLE 1 displays some examples for the 7 attacked watermarked images, extracted watermark images, PSNR between attacked-and-watermarked images and the correlations coefficient between extracted watermark images and embedded watermark image.

TABLE 1.
the some attacked watermarked images and extracted watermark images and PSNR value and correlation coefficient values

Attacked / Results	Brighten	Uniform noise (3%)	Sharpening filter	JPEG compression	Cutting 25%	Gaussian filter	Histogram Equalization
Attacked watermarked image							
PSNR	23.5630	33.8092	28.3775	35.0797	11.7296	36.0531	16.8939
Extracted watermark							
Correlation Coefficient	0.9539	0.7010	0.9151	0.6428	0.7156	0.6158	0.7733

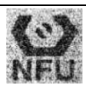
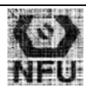
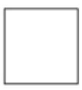
As can be seen, attacks only degrading the watermarked image and extracted watermark images quality and couldn't removed embedded watermark. Therefore proposed method is more robust against attacks.

6. COMPRESSION

This section compares the proposed algorithm with the existing SVD-based methods including two SVD-based methods [3, 21] and Lin's method [8] which was developed in DCT domain. TABLE 2 presents the visual–perception comparison for the extracted watermarks retrieved by the four methods while taking Baboon image as the investigated images. As can be observed in the extracted watermark, the proposed algorithm proved to be much more robust than other three.

FIGURE 5 depicts the comparison result between the correlation coefficient of the proposed method and other three methods [3, 8, 21]. As can be seen in the FIGURE 5 and TABLE 2, the proposed algorithm proved to be much more robust than the Mohammad's method and other two methods.

TABLE 2 .
the visual–perception comparisons for the extracted watermarks retrieved by the six methods while taking Baboon image as the investigated images

Attacks / Methods	Brighten (+20)	Uniform (3%)	Sharpening filter	JPEG compression	Cutting 25%	Gaussian filtering	Histogram equalization
Proposed method							
Lin's method [8]							
Mohammad's method [3]							

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Jain's method [21]	

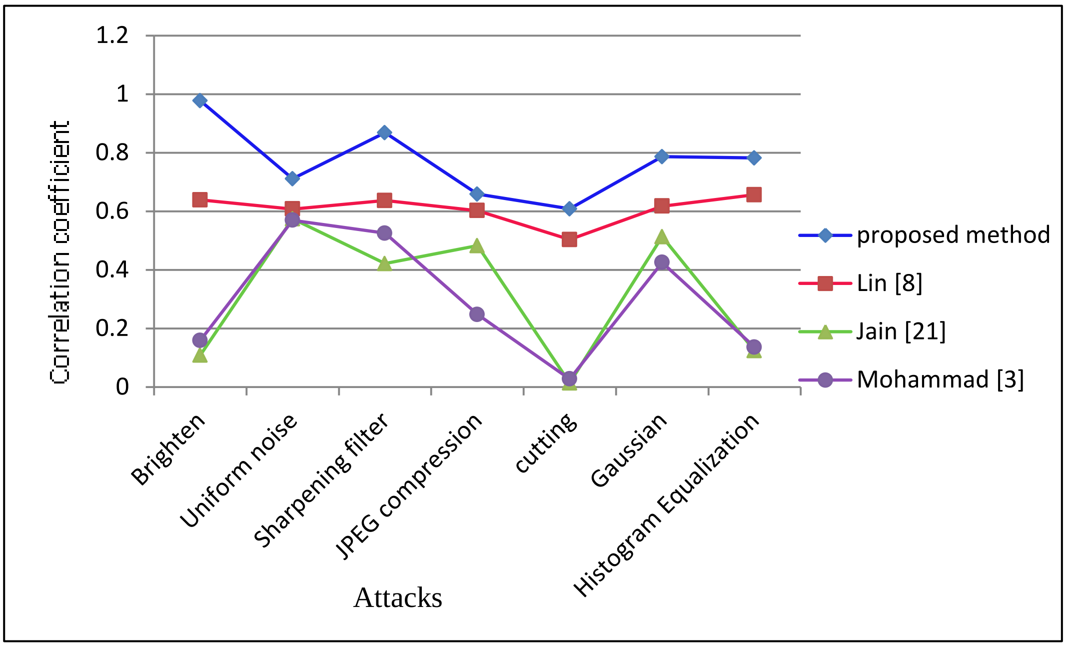


FIGURE 5. Correlation coefficient comparison

7. CONCLUSION

This paper has presented a SVD-DWT scheme, which was a semi-blind block-based watermarking technique for protecting real property rights of images. In this method, first, watermark and host images were taken to discrete wavelet transform domain and then HH and LL sub-bands of the host image were blocked and SVD was applied to each block of the host image. Afterward, LL sub-band blocks of the watermark image were embedded in the singular values of the blocks of the host image and a different SF was used for each block.

Using DWT and different SFs for each block increased its robustness and false-positive detection problem was solved by watermark embedding of LL sub-band blocks. Further, transparency of the watermarked image was improved owing to the combination of SVD and DWT and also using watermark embedding method.

It was shown that the algorithm was reliable. Also, simulations showed that the proposed method was robust against the most common attacks. Additionally, the proposed method solved the false-positive detection problem occurring in most SVD-based methods. Comparison with different algorithms exhibited that the proposed algorithm was more robust.

REFERENCES

[1] C.-Y. Chang, H.-J. Wang, and S.-W. Pan, "A robust DWT-based copyright verification scheme with Fuzzy ART," *Journal of Systems and Software*, vol. 82, pp. 1906-1915, 2009.

[2] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "A State-of-the-Art Overview," *IEEE Signal processing magazine*, 2000.

[3] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," *Signal Processing,* vol. 88, pp. 2158-2180, 2008.
[4] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, *Digital watermarking* vol. 53: Springer, 2002.
[5] H. Suryavanshi, A. Mishra, and S. Kumar, "Digital Image Watermarking in Wavelet Domain," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 3, pp. 1-6, 2013.
[6] J. A. Hussein, "Spatial domain watermarking scheme for colored images based on log-average luminance," *arXiv preprint arXiv:1001.3496,* 2010.
[7] X. Wu, Z.-H. Guan, and Z. Wu, "A chaos based robust spatial domain watermarking algorithm," in *Advances in Neural Networks–ISNN 2007*, ed: Springer, 2007, pp. 113-119.
[8] S. D. Lin, S.-C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Computer Standards & Interfaces,* vol. 32, pp. 54-60, 2010.
[9] T. K. Tsui, X.-P. Zhang, and D. Androutsos, "Color image watermarking using multidimensional Fourier transforms," *Information Forensics and Security, IEEE Transactions on,* vol. 3, pp. 16-28, 2008.
[10] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards & Interfaces,* vol. 31, pp. 1002-1013, 2009.
[11] H. Gao, L. Jia, and M. Liu, "A digital watermarking algorithm for color image based on DWT," *TELKOMNIKA Indonesian Journal of Electrical Engineering,* vol. 11, pp. 3271-3278, 2013.
[12] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *Multimedia, IEEE Transactions on,* vol. 4, pp. 121-128, 2002.
[13] H.-H. Tsai and J.-S. Cheng, "Adaptive signal-dependent audio watermarking based on human auditory system and neural networks," *Applied Intelligence,* vol. 23, pp. 191-206, 2005.
[14] D. S. Chandra, "Digital image watermarking using singular value decomposition," in *Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on*, 2002, pp. III-264-III-267 vol. 3.
[15] Q. Li, C. Yuan, and Y.-Z. Zhong, "Adaptive DWT-SVD domain image watermarking using human visual model," in *Advanced Communication Technology, The 9th International Conference on*, 2007, pp. 1947-1951.
[16] V. Aslantas, "A singular-value decomposition-based image watermarking using genetic algorithm," *AEU-International Journal of Electronics and Communications,* vol. 62, pp. 386-394, 2008.
[17] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Digital Signal Processing*, vol. 21, pp. 522-527, 2011.
[18] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 11, pp. 674-693, 1989.
[19] A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu, and A. Vernone, "A novel block-based watermarking scheme using the SVD transform," *Algorithms,* vol. 2, pp. 46-75, 2009.
[20] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection," *Expert Systems with Applications,* vol. 39, pp. 673-689, 2012.
[21] C. Jain, S. Arora, and P. K. Panigrahi, "A Reliable SVD based Watermarking Schem," *arXiv preprint arXiv:0808.0309,* 2008.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)