International Journal of Innovative Computing, Information and Control
Volume **8**, Number **7(A)**, July **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 4691–4703

ROBUST BLIND DWT BASED DIGITAL IMAGE WATERMARKING USING SINGULAR VALUE DECOMPOSITION

Habibollah Danyali[1], Morteza Makhloghi[2] and Fardin Akhlagian Tab[2]

[1]Department of Electrical and Electronics Engineering
Shiraz University of Technology
P.O.Box 71555-313, Shiraz, Iran
danyali@sutech.ac.ir

[2]Department of Computer Engineering
University of Kurdistan
P.O.Box 416, Sanandaj, Iran
{ m.makhlogi; f.akhlaghian }@uok.ac.ir

Received January 2011; revised June 2011

Abstract. *This paper presents a robust and blind digital image watermarking scheme for copyright protection based on discrete wavelet transform and singular value decomposition (SVD). The basic idea of the proposed method is to embed the singular values (SVs) of the watermark image into the specific values of the SVs of the transformed host image. At the first step, the host image is transformed to wavelet domain and then SVD transform is applied to each sub-band. In the next stage, the SVs of each sub-band and the SVs of the watermark image are converted to new semi-binary arrays form. Finally, using the semi-binary arrays, the values of SVs of the watermark image are inserted into the selected values of SVs of the decomposed host image's sub-bands. The experimental results show clearly high transparency of the watermarked images as well as strong robustness of the proposed watermarking scheme against different geometric and non geometric attacks.*

Keywords: Blind watermarking, Robust watermarking, Discrete wavelet transform, Singular value decomposition

1. **Introduction.**

With the rapid development of computers, digital equipments and internet, the multimedia data can easily be distributed, copied and used legally or illegally. Therefore, copyright protection of multimedia data becomes more essential. One of the best methods to protect copyright and proof of ownership is digital watermarking.

Digital watermarking is a process of modifying the host data with embedding an invisible mark data such as logos, images, texts and audio. The watermarking method is referred to as blind, if the original or reference images are not required during the extraction process, otherwise it is referred to as non-blind [2-4]. There are some important features required for a digital image watermarking system used for copyright protection applications. First, the watermark embedding process should not noticeably degrade the quality of the original image. In other words, the watermarked image should provide a high degree of transparency. Second, the watermarked image should resist against different geometric and non geometric attacks. This feature is known as robustness. Finally, the blindness is necessary especially where obtaining the original image in watermark extracting process is difficult. There is a tradeoff between transparency and robustness; therefore, it is an important issue to solve this problem and introduce an algorithm which provides strong robustness and at the same time offers good transparency.

Watermarking schemes can be divided into two main categories according to the embedding domain: spatial and transform domain schemes [5-7]. In spatial domain, the watermark is embedded into the specific pixels of the host image. In transform domain, the host image is first transformed to a frequency domain and then watermark is embedded into the frequency coefficients [7-10]. Although the transform domain watermarking scheme is more complex than spatial domain watermarking, this kind of watermarking is more robust against different attacks than spatial domain watermarking [1,11]. Discrete wavelet transform (DWT) is more usual than other transforms and used widely in digital image watermarking algorithms.

Raval and Rege [12] presented a multiple watermarking algorithm. After decomposing the original image by applying a discrete wavelet transform, they embed multiple watermarks in low and high frequency subbands to achieve good robustness. Although this method is robust against different attacks, the transparency of the watermarked images is not good enough. Moreover, the method is non-blind and the original image is required for the watermark extraction process.

Lin et al. [9] proposed a wavelet-tree based blind image watermarking scheme using distance vector of binary cluster. The watermark embedding is done by comparing the statistical difference and the distance vector of a wavelet tree to decide about embedding bit 0 or 1. In this scheme, distortion of a watermark image is reduced by quantizing the two smallest coefficients of a wavelet tree. This method preserves strong robustness against filtering attacks, but cannot resist against geometric and JPEG compression attacks. Also, this method cannot preserve very good transparency.

Recently, singular value decomposition (SVD) is used as a new transform for watermarking [13-17]. SVD-based method is introduced by Gorodetski et al. [13]. In their non-blind method, the watermark was embedded into the singular values (SVs) of the host image in spatial domain.

A non-blind digital image watermarking method in spatial domain was proposed by Chandra et al. [18]. They embedded the SVs of the watermark image into the SVs of the host image. However, this method does not offer good transparency and cannot resist against geometric attacks.

Ganic and Eskicioglu [15] introduced a new DWT-SVD based image watermarking method. In this method, they transformed the original image to wavelet domain and then SVs for each frequency sub-band as well as for the watermark image were calculated. Then, the SVs of the watermark image are embedded into the SVs of all sub-bands of the host image. This method is robust against different geometric and non geometric attacks, but the original image is needed during the extracting process and the watermarked image does not offer good transparency.

A robust full-band and non-blind image watermarking scheme using singular value decomposition was proposed by Lin et al. [19]. In this scheme, the original image was transformed into four sub-bands and the SVs of watermark were added into the SVs of HL and LH bands using a small scale factor. In addition, the watermark is embedded into other bands directly. This method preserves good robustness against common attacks but does not offer good transparency and the original image is required during extraction process.

Bhatnagar and Raman [20] suggested a new semi-blind DWT based image watermarking method which used SVD. In their method, first, the original image is transformed into wavelet domain and the HH sub-band is selected. Second, a one-level DWT is applied on this sub-band and all coefficients of the high frequency sub-bands which have lower directive contrast than the given threshold are changed to zero. Then, one-level inverse discrete wavelet transform is applied on changed sub-bands to generate a reference image.

Finally, the SVs of the watermark image are embedded into the SVs of the reference image. This method has good transparency and robustness against non geometric attacks, but it does not offer good robustness against geometric attacks and also needs the reference image for its watermark extraction process.

All of the discussed SVD-based watermarking schemes [13-20] are semi or non-blind methods which do not fulfill both robustness and transparency requirements. In this paper, a new blind digital image watermarking using SVD in wavelet domain is proposed which offers higher degree of transparency and strong robustness against various geometric and non geometric attacks. To have a blind image watermarking, we introduce a novel method to convert the SVs of the grayscale watermark image and the SVs of the decomposed image's sub-bands into a specific semi binary. To achieve strong robustness and at the same time high degree of transparency, the converted SVs of the watermark are embedded into the specific values of the converted SVs of the decomposed host image's sub-bands.

The remainder of this paper is organized as follows. In Section 2, we provide a brief background about singular value decomposition. In Section 3, the proposed watermarking method is described in detail. The experimental results are presented and discussed in Section 4 and finally, some concluding remarks are given in Section 5.

2. **Singular Value Decomposition.**

In algebra, the singular value decomposition (SVD) is known as a powerful technique for factorizing real or complex matrix. SVD is used in different fields of signal processing such as image compression and image watermarking [21,22]. SVD transform decomposes an $M \times N$ image ($C_{M\times N}$) into three matrices, two orthogonal matrices $U_{M\times M}$ and $V_{N\times N}$ (i.e., $U^T.U = I$ and $V^T.V = I$) and one diagonal matrix $S_{M\times N}$ as follows:

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

where, the columns of U and V are called the left and right singular vectors, respectively, and the diagonal entries of S are called the singular values (SVs) of matrix C and:

$$S = diag(\beta_1,\ \beta_2,\ \beta_3,\ \dots) \tag{2}$$

$$C = \sum_{i=1}^{r} \beta_i U_i V_i,\ r = \min(M, N) \tag{3}$$

Utilizing SVD transform has some advantages in image processing. Firstly, the sizes of the matrices in this transform can be a rectangle or a square. Secondly, if the image is changed with general image processing attacks such as compression, noise, etc., the SVs of the image are less affected and then it can be used as a robust feature widely in digital image watermarking. Finally, the SVs contain intrinsic algebraic image properties [20].

3. **The Proposed Watermarking Method.**

The flowchart of the proposed watermarking technique is shown in Figure 1. First, K levels of a discrete wavelet transform (DWT) are applied to the original image. Then, SVD is applied to each subband of the decomposed image as well as to the gray scale watermark image. The SVs of the watermark image are then mapped to real numbers in the range of [0 255]. The SVs of each sub-band of the host image and the mapped SVs of the watermark image are converted to semi-binary arrays. Watermark insertion is done by modifying the special values of converted SVs of different subbands with the values of the SVs of the watermark image (details will be given in the next subsection). Finally, the modified SVs of each sub-band are converted to real numbers and inverse SVD and K levels of inverse DWT are applied to obtain the watermarked image.

Details of the proposed watermarking algorithm are given in the following subsections.

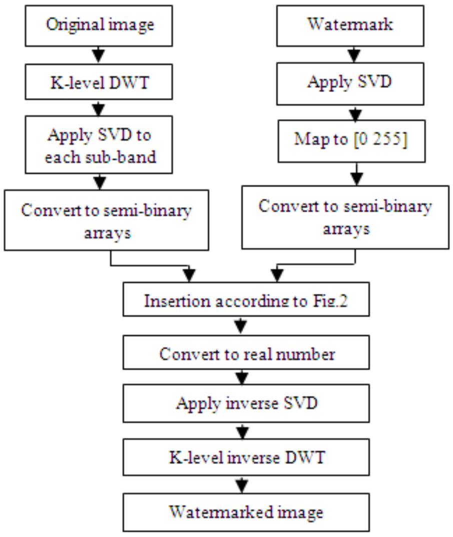


FIGURE 1. Flowchart of the proposed method

3.1. **Semi-binary representation of singular values.** The requirement of the original or reference image in the watermark extraction stage is one of the major problems of the current SVD-DWT based digital image watermarking schemes [13-20]. In this paper, we introduce a novel blind algorithm which replaces the adding of the watermark's singular values with inserting bits of them into the specific bits of the singular values of the decomposed host image's sub bands. Since the singular values of the watermark image and the singular values of the decomposed host image's sub bands are float numbers, for access to different bits of these numbers, they are converted to a new form of semi-binary arrays using Algorithm 1. Algorithm 2 is used to reconstruct a singular values from its semi-binary array.

Algorithm 1

```
$count = 1;$
$while(S \sim= 0)$
  $B(count) = mod(S, 2);$
  $S = fix(S/2);$
  $count = count + 1;$
$end$
```

Algorithm 2

```
$S = 0;$
$k = 1$
$for\ i = 2 : size(B)$
  $S = S + B(i) \times k;$
  $k = k \times 2;$
$end$
```

where S is a SV of the watermark image or a SV of each sub-band of the decomposed host image and B is its semi-binary array representation. The first element of this array is a float number between 0 and 2 (i.e., $0 <= B(1) < 2$) and other elements are binary digits (i.e., 0 or 1).

For example assume S is equal to 205.36. Then B, the semi-binary representation of S would be:

$B(1)$	$B(2)$	$B(3)$	$B(4)$	$B(5)$	$B(6)$	$B(7)$	$B(8)$
1.36	0	1	1	0	0	1	1

FIGURE 2. An example of a semi-binary array representation

3.2. **Watermark embedding algorithm.** Assume $X_{M \times N}$ and $W_{M1 \times N1}$ are the grayscale host and watermark images, respectively. To embed the gray scale watermark image into the host image the following algorithm is formulated:

1. Input host ($X_{M\times N}$) and watermark ($W_{M1\times N1}$) images.
2. Perform K levels of discrete wavelet decomposition on the host image. Each sub-band of the decomposed image is referred to as X_l^θ, where $1 \le l \le K$ and $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.
3. Apply SVD transform to each sub-band's of the decomposed host image,
$$X_K^\theta = U_X^\theta S_X^\theta (V_X^\theta)^T \tag{4}$$
where β_i^θ, $i = 1, \ldots, r$ are SVs of S_X^θ, $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$ and r is the rank of matrix S_X^θ.
4. Apply SVD transform to the watermark image and convert the SVs of the watermark image to real numbers in [0 255] domain,
$$W = U_W S_W (V_W)^T \tag{5}$$
$$\alpha = 255/\ \beta_1^W$$
$$\beta_i^W = \beta_i^W \times \alpha,\ i = 1, \ldots, r \tag{6}$$
where β_i^W are SVs of S_W, r is the rank matrix S_W and α is converting coefficient. Note that β_1^W is the maximum value of β_i^W.
5. Convert the mapped SVs of the watermark image (β_i^W) and the SVs of all sub bands (β_i^θ) to semi-binary arrays using Algorithm 1. The semi-binary arrays for the watermark and the host image's subbands are denoted by $\beta_i^{W^{ar}}$ and $\beta_i^{\theta^{ar}}$, respectively. Where $i = 1, \ldots, r$ and $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.
6. Insert $\beta_i^{W^{ar}}$ values into the specific bits of $\beta_i^{\theta^{ar}}$ as follows (also see Figure 3):
$$\begin{array}{ll} \beta_i^{LL^{ar}}(1) = \beta_i^{W^{ar}}(1) & \beta_i^{HL^{ar}}(2) = \beta_i^{W^{ar}}(5) \\ \beta_i^{LL^{ar}}(2) = \beta_i^{W^{ar}}(2) & \beta_i^{HL^{ar}}(4) = \beta_i^{W^{ar}}(6) \\ \beta_i^{LH^{ar}}(2) = \beta_i^{W^{ar}}(3) & \beta_i^{HH^{ar}}(2) = \beta_i^{W^{ar}}(7) \\ \beta_i^{LH^{ar}}(4) = \beta_i^{W^{ar}}(4) & \beta_i^{HH^{ar}}(4) = \beta_i^{W^{ar}}(8) \end{array} \tag{7}$$

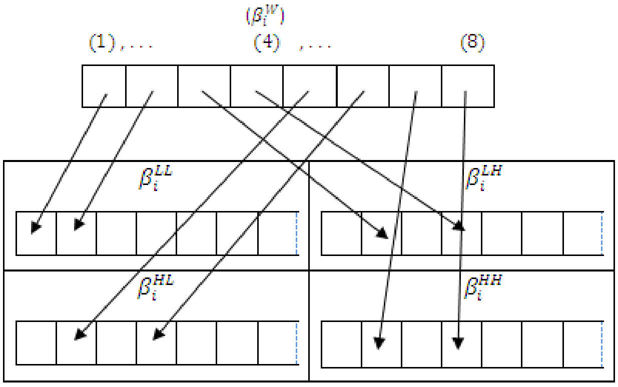


FIGURE 3. The watermark insertion process

7. Reconstruct SVs of each subband, $S_X^{*\theta}$, from their semi-binary arrays using Algorithm 2.
8. Obtain the four sub-bands of the modified decomposed reference image as,
$$X_K^{*\theta} = U_X^\theta S_X^{*\theta} (V_X^\theta)^T,\ \theta \in \{LL_K, LH_K, HL_K, HH_K\} \tag{8}$$
9. Perform K levels of inverse discrete wavelet decomposition to get the watermarked image ($X_{M\times N}^*$).

3.3. Watermark extraction algorithm.

1. Input the watermarked image ($X^*_{M\times N}$).
2. Perform K levels of discrete wavelet decomposition on the watermarked image. The subbands of the decomposed watermarked image are represented by ${X^*}^{\theta}_{l}$, where $1 \le l \le K$ and $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.
3. Apply SVD transform to each sub-band's of the decomposed watermarked image,

$$ {X^*}^{\theta}_{K} = {U^*}^{\theta}_{X} {S^*}^{\theta}_{X} ({V^*}^{\theta}_{X})^T \tag{9} $$

   where ${\beta^*}^{\theta}_{i}$, $i = 1, \dots, r$ are the SVs of ${S^*}^{\theta}_{X}$ and $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.
4. Convert the SVs of all sub bands (${\beta^*}^{\theta}_{i}$) to semi-binary arrays, using Algorithm 1. The semi-binary arrays are denoted by ${\beta^*}^{\theta^{ar}}_{i}$, where $i = 1, \dots, r$ and $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.
5. Extract SVs of the watermark image (i.e., $\beta_i^{ext^{ar}}$) from ${\beta^*}^{\theta^{ar}}_{i}$ to get the reconstructed semi-binary array as follows (see Figure 4):

$$ \begin{array}{ll} \beta_i^{ext^{ar}}(1) = {\beta^*}^{LL^{ar}}_{i}(1) & \beta_i^{ext^{ar}}(5) = {\beta^*}^{HL^{ar}}_{i}(2) \\ \beta_i^{ext^{ar}}(2) = {\beta^*}^{LL^{ar}}_{i}(2) & \beta_i^{ext^{ar}}(6) = {\beta^*}^{HL^{ar}}_{i}(4) \\ \beta_i^{ext^{ar}}(3) = {\beta^*}^{LH^{ar}}_{i}(2) & \beta_i^{ext^{ar}}(7) = {\beta^*}^{HH^{ar}}_{i}(2) \\ \beta_i^{ext^{ar}}(4) = {\beta^*}^{LH^{ar}}_{i}(4) & \beta_i^{ext^{ar}}(8) = {\beta^*}^{HH^{ar}}_{i}(4) \end{array} \tag{10} $$

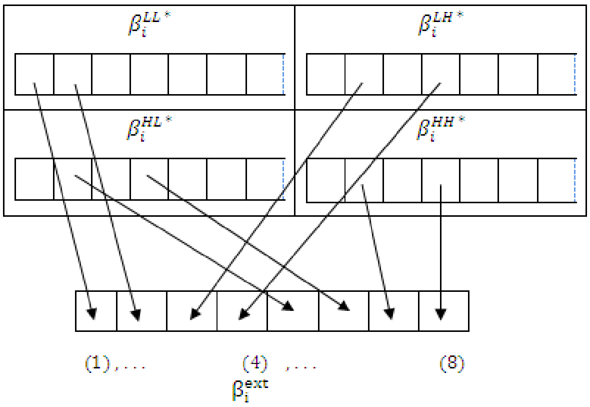


FIGURE 4. The watermark extraction processes

6. Convert the extracted SVs from the subbands ($\beta_i^{ext^{ar}}$) to real numbers, β_i^{ext}, using Algorithm 2, and also map them to their original range as follows:

$$ \beta_i^{ext} = \beta_i^{ext}/\alpha, \; i = 1, 2, \dots, r \tag{11} $$

7. Obtain the reconstructed watermark image by applying inverse SVD:

$$ W^{ext} = U_W S_W^{ext} (V_W)^T \tag{12} $$

4. Simulation Details and Experimental Results.

The proposed watermarking method is fully software implemented in MATLAB. Six gray scale test images with size 512×512 pixels, Plane, Pepper, Lena, Tree, Pirate and House, which are shown in Figure 5, are used as test images. Two 64×64 grey scale watermark images, UOK and IEEE logos shown in Figure 6 are used as watermark images. The SVs of UOK are inserted into the Plane, Pepper and Lena images and the SVs of IEEE are inserted into the Tree, Pirate and House images using the embedding algorithm introduced in the previous section. Three levels of wavelet decomposition with Haar filters is used to decompose the test images.

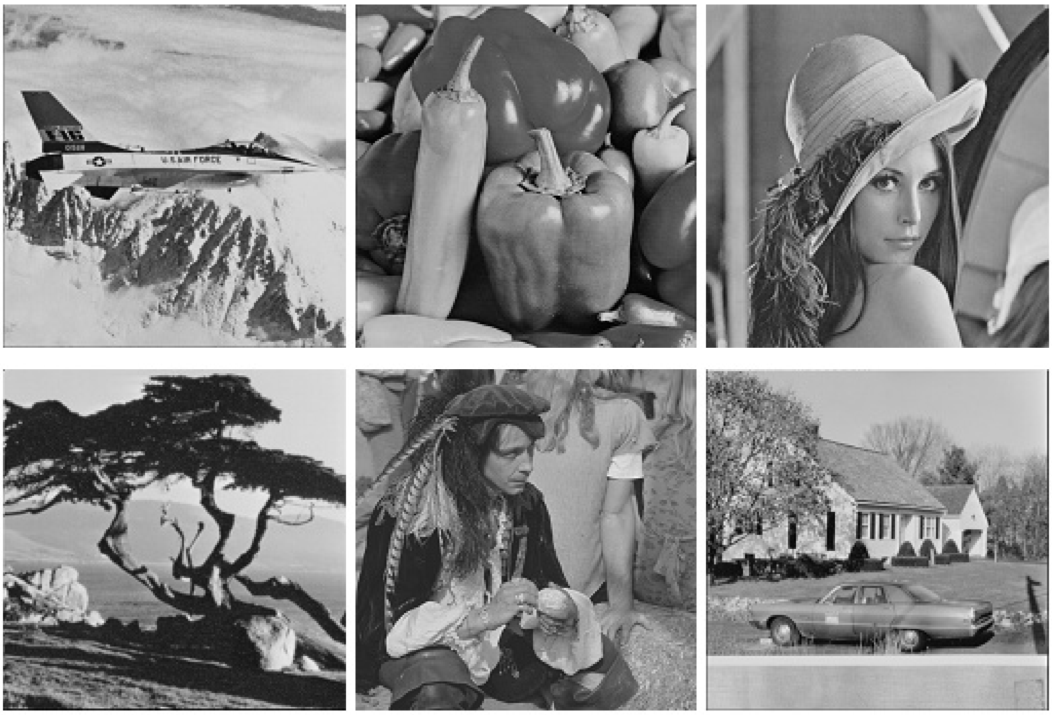
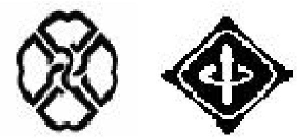


Figure 5. Original test images



(a) (b)

Figure 6. Watermark logos (a) UOK, (b) IEEE

To investigate the performance of the proposed watermarking scheme, several experiments for evaluating of transparency and robustness against different attacks were performed.

4.1. **Transparency results.** We measure the visual quality of watermarked images in compare to the original images using Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity Index Measure (MSSIM). The PSNR is defined as:

$$PSNR = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right)(\text{db}) \tag{13}$$

$$MSE = \frac{\sum_{M,N}\left[X\left(m,n\right) - Y\left(m,n\right)\right]^2}{M * N} \tag{14}$$

where X and Y represent the original and watermarked images, respectively.

The MSSIM is defined as:

$$MSSIM(X,Y) = \frac{1}{M}\sum_{j=1}^{M} SSIM(X_j, Y_j) \tag{15}$$

$$SSIM(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{({\mu_x}^2 + {\mu_y}^2 + C_1)({\sigma_x}^2 + {\sigma_y}^2 + C_2)} \tag{16}$$

where X and Y represent the original and watermarked images, respectively, M denote horizontal dimension of the image, $C_1 = (K_1L)^2$, $C_2 = (K_2L)^2$, $K_1 = 0.01$, $K_2 = 0.03$ and $L = 255$. μ_x and μ_y are the mean values of X and Y respectively and defined as:

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} X_i, \; \mu_y = \frac{1}{N}\sum_{i=1}^{N} Y_i \tag{17}$$

N represents vertical dimension of the image. σ_x and σ_y are the standard deviations (i.e., estimate of the signal contrast) and σ_{xy} is the covariance value:

$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_i)^2\right)^{\frac{1}{2}}, \; \sigma_y = \left(\frac{1}{N-1}\sum_{i=1}^{N}(y_i - \mu_i)^2\right)^{\frac{1}{2}} \tag{18}$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y) \tag{19}$$

The value of MSSIM is in the interval [0, 1]. The value 1 means that the original and watermarked images are exactly the same and 0 means totally unrelated [23].

PSNR and MSSIM are objective criteria for assessment of the quality of digital images. PSNR is widely used by researchers in image processing; however, MSSIM considers some requirements of the human visual system and therefore is closer to the subjective assessment done by human.

Table 1. PSNR and MSSIM values of all test images

	House	Pirate	Tree	Lena	Pepper	Plane
PSNR(dB)	63.78	63.41	63.11	63.44	63.32	63.83
MSSIM	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999

In the first experiment, all test images were watermarked. The watermarked images are shown in Figure 7. As the figure show there is no visual degradation in quality of the watermarked images. Table 1 gives the corresponding MSSIM and PSNR values for the watermarked images. The proposed method provides PSNR higher than 63 dB and MSSIM equal to 0.9999 for all test images, while the PSNR and the MSSIM of the previous works [12-17] were less than 50 and 0.95 respectively. This is mainly due to converting the SVs of the watermark image to real numbers in the range of [0 255] domain and inserting the SVs of the watermark image into the selected bits of SVs of the host images in different wavelet sub-bands. These results confirm very high degree of transparency for the proposed watermarking algorithm.

4.2. **Robustness results.** In this part, we first test the reversibility of the proposed watermarking algorithm in absence of any attack. Watermark extraction process was done for each watermarked image and correlation coefficient measure is used to judge about the extracted watermark. The correlation coefficient is defined as:

$$\rho = \frac{\sum_{i,j=1}^{M_1,N_1}(W(i,j) - \hat{W})(W^*(i,j) - \hat{W^*})}{\sqrt{(\sum_{i,j=1}^{M_1,N_1}(W(i,j) - \hat{W})^2)(\sum_{i,j=1}^{M_1,N_1}(W^*(i,j) - \hat{W^*})^2)}} \tag{20}$$

where W is the original watermark image, W^* is the extracted watermark image and M_1 and N_1 are the height and width of the watermark image, respectively. $\hat{W}$ and $\hat{W}^*$ are mean values of the original watermark and the extracted watermark images, respectively. The correlation coefficients for all extracted watermark logos are equal to 1 (see Table 2)

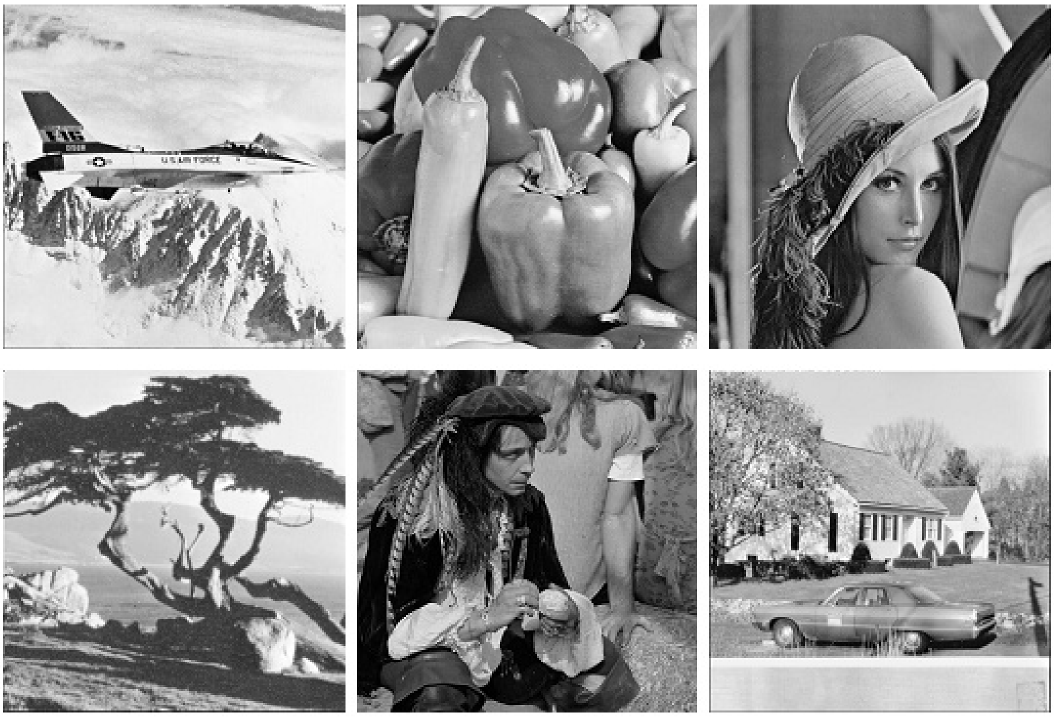


Figure 7. Watermarked test images

which means that the extracted watermark logos are equal to the original ones in absence of attacks. The results prove the complete reversibility of the algorithm while this feature is not fulfilled by the method proposed in [20] and known as a major image watermarking work using SVD in the current literature.

Table 2. Correlation coefficients of all extracted logos

	House	Pirate	Tree	Lena	Pepper	Plane
ρ	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

To test the robustness of the proposed method, several strong geometric and non geometric attacks including cropping (50% of watermarked image), 70° rotation, resizing (512 to 64 to 512), JPEG compression (with low quality factor (QF), e.g., QF=20), additive 75% Gaussian noise, applying 15×15 average and median filters, motion blur, histogram equalization, sharpen and contrast adjustment were applied to the watermarked test images. After applying these attacks, the extracted watermark logos were compared to the original ones. Table 3 shows the correlation coefficients of all extracted watermark logos after applying all mentioned attacks for different test images. According to these results, the proposed method is more robust against all above mentioned attacks than the method introduced in [20].

For further analysis, the visual results of some mentioned attacks into Plane and house images are given in Figures 8 to 12. The extracted watermarks logos after cropping the watermarked images are shown in Figures 8(b) and (d). Although, this attack removes 50% of watermarked image's information, the extracted logos are very clear and recognizable.

Figure 9 shows the results of applying 70° rotation to watermarked images. Again the extracted watermark logos shown in Figures 9(b) and (d) are recognizable. The results

Table 3. Correlation coefficient for the extracted logos after applying attacks to the watermarked images

Attacks	House	Pirate	Tree	Lena	Pepper	Plane
Cropping $(1/4)^{th}$ area remaining	0.6925	0.8213	0.8366	0.9007	0.8844	0.8530
Rotation (70°)	0.7546	0.8693	0.7991	0.7152	0.6769	0.8047
Resizing ($512 \to 64 \to 512$)	0.6674	0.6260	0.7305	0.7868	0.8444	0.7798
JPEG Compression (QF=20)	0.7302	0.7575	0.8735	0.7182	0.8180	0.7825
Additive Gaussian noise (75%)	0.7957	0.7120	0.9100	0.9089	0.8689	0.7174
Average Filtering (15 × 15)	0.8192	0.7191	0.6321	0.8408	0.6880	0.8230
Median Filtering (15 × 15)	0.8250	0.7598	0.7874	0.6957	0.7931	0.8461
Motion Blur	0.7459	0.8912	0.7338	0.7874	0.8048	0.8312
Histogram Equalization	0.6494	0.6410	0.8777	0.7634	0.7022	0.6653
Sharpen	0.7320	0.6470	0.8779	0.6963	0.7127	0.7463
Contrast Adjustment	0.7281	0.6605	0.6729	0.6735	0.7378	0.7583

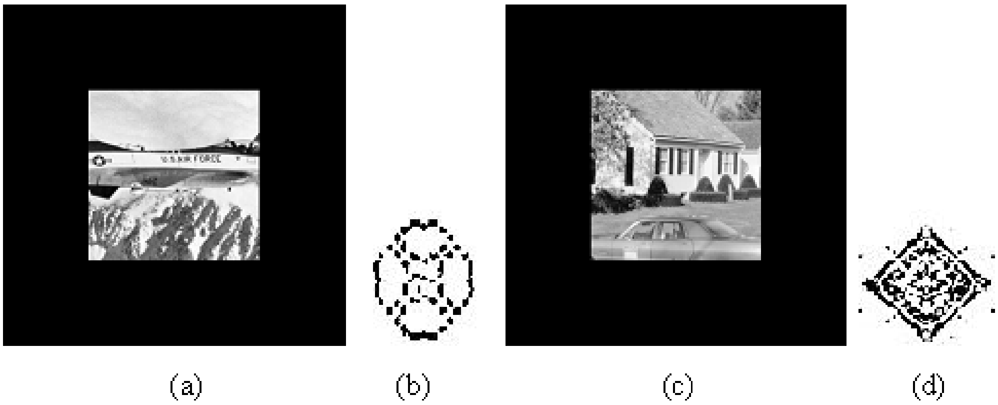


Figure 8. (a) Watermarked plane image after cropping (b) The extracted UOK logo watermark (c) Watermarked house image after cropping (d) The extract IEEE logo watermark

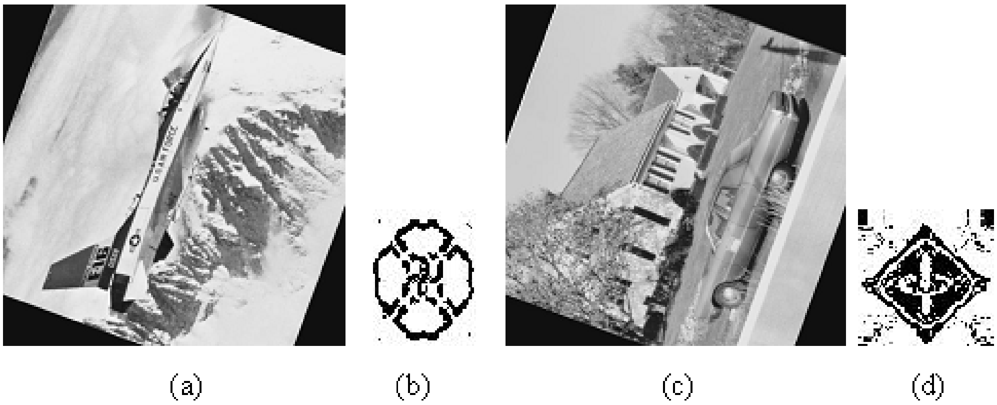


Figure 9. (a) Watermarked plane image after rotation (b) The extracted UOK logo watermark (c) Watermarked house image after rotation (d) The extract IEEE logo watermark

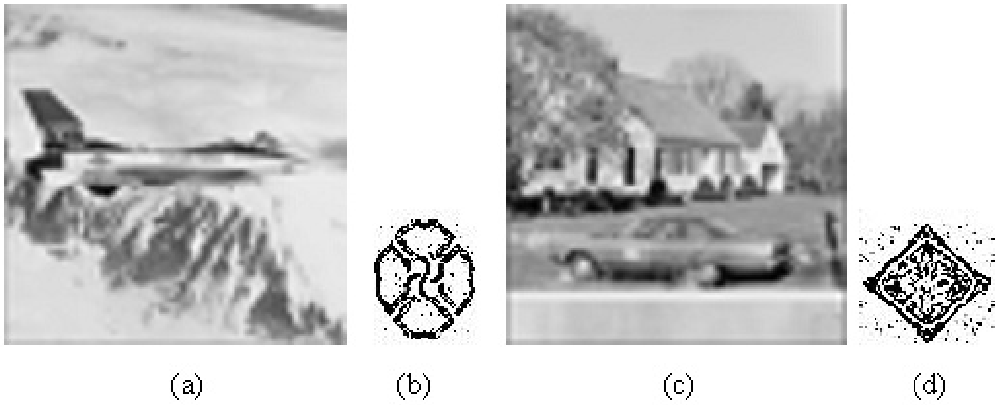


FIGURE 10. (a) Watermarked plane image after resizing (b) The extracted UOK logo watermark (c) Watermarked house image after resizing (d) The extract IEEE logo watermark

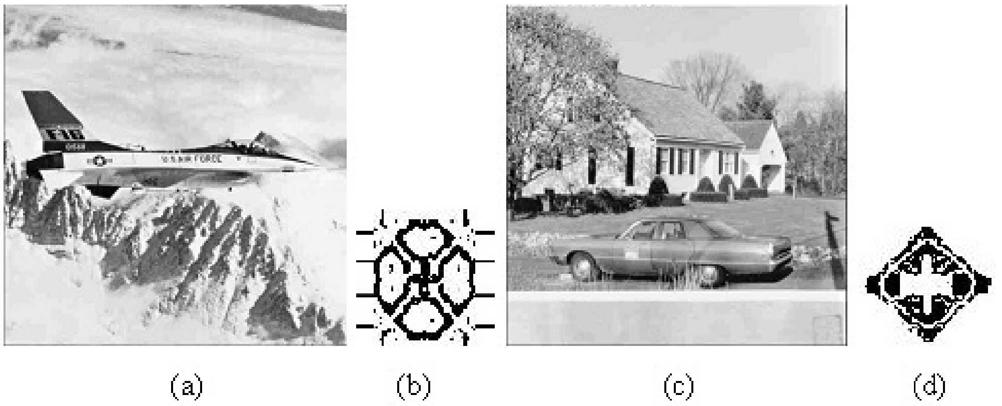


FIGURE 11. (a) Watermarked plane image after JPEG compression (b) Extract watermark (c) Watermarked house image after JPEG compression (d) The extract IEEE logo watermark

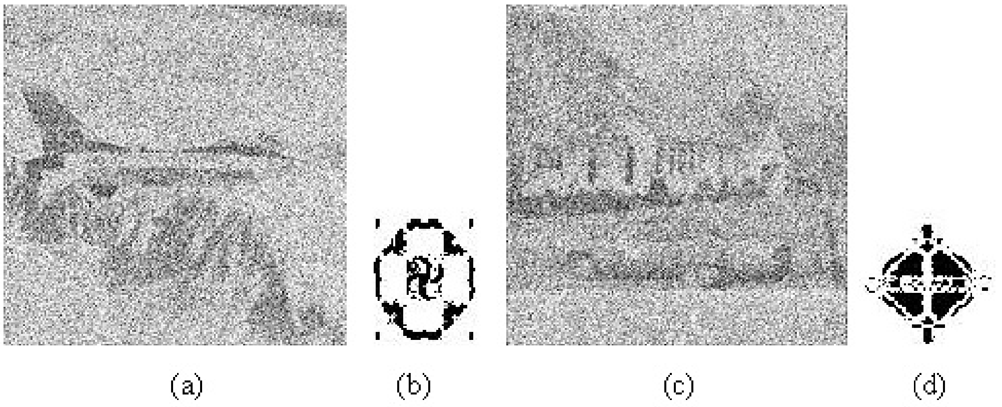


FIGURE 12. (a) Watermarked plane image after adding 75% additive Gaussian noise (b) The extracted UOK logo watermark (c) Watermarked house image after adding 75% additive Gaussian noise (d) The extract IEEE logo watermark

for resizing attack are shown in Figure 10. This attack is performed by reducing the watermarked images of 512×512 pixels to 64×64 and then brought to 512×512 pixels. According to Figures 10(b) and (d), the extracted watermark logos are very clear after applying this attack. The extracted watermarks logos after JPEG compression of the watermarked images by quality factor (QF) equal to 20 are shown in Figure 11(b) and (d). Finally, the results of adding 75% Gaussian noise are given in Figure 12. Although this attack severely degrades the watermarked image, the extracted watermarks are still recognizable.

Note that there is no need to have the original image or even a reference version of it during watermark extraction process in the proposed method. In other words the proposed method is completely blind. The major robust image watermarking methods using SVD in wavelet domain [13-20] in the current are non-blind or semi-blind; therefore, these methods are not comparable to the proposed method.

The proposed watermarking method is a very good candidate for copyright protection and ownership proof applications for digital images even in presence of severe attacks or when the image is transmitted over low bit rate channels that requires high degree of compression for the image or for transmitting visual information over error prone media which degrade the quality of the image in the receiver. For example, if someone intentionally resize the image, rotate it or crops part, still the owner would be able to extract the watermark from the changed version of the image and proves his/her ownership.

5. **Conclusions.** In this paper, a new blind digital image watermarking using SVD in DWT domain is proposed. In the proposed method, grayscale images are used as watermark and watermark embedding is done by inserting the singular values of wavelet decomposed watermark logo into selected singular values of wavelet decomposed image. The proposed method is tested with extensive experiments in terms of transparency and robustness. The experimental results show that the proposed method preserves good transparency for the watermarked images, which is evaluated by PSNR and MSSIM. The proposed method effectively resists against strong geometric attacks such as cropping of the 50% of watermarked image, resizing (512 to 64 and then 512), 70° rotation and non geometric attacks such as applying 15×15 average and median filters, JPEG compression (QF=20), Additive 75% Gaussian noise and common image processing attacks. The proposed method can be effectively used for copyright protection of visual information.

REFERENCES

[1] M. Ouhsain and A. B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform, *Expert Systems with Applications*, vol.36, no.2, pp.2123-2129, 2009.

[2] P. H. W. Wong, O. C. Au and Y. M. Yeung, A novel blind multiple watermarking technique for images, *IEEE Trans. on Circuits and Systems for Video Technology*, vol.13, no.8, pp.813-830, 2003.

[3] Z. Erhu and Z. Fan, Adaptive image blind watermarking method based on zerotree of wavelet, *Proc. of the 8th IEEE Int. Conf. on Electronic Measurement and Instruments*, Xi'an, China, pp.799-802, 2007.

[4] F. T. Alturki and A. F. Almutairi, Analysis of blind data hiding using discrete cosine transform phase modulation, *Signal Processing: Image Communication*, vol.22, no.4, pp.347-362, 2007.

[5] A. G. Bors and I. Pitas, Image watermarking using DCT domain constraints, *Proc. of the IEEE Int. Conf. on Image Processing*, vol.3, pp.231-234, 1996.

[6] R. G. V. Schyndle, A. Z. Tirkel and C. F. Osbrone, A digital watermark, *Proc. of the IEEE Int. Conf. on Image Processing*, Austin, Texas, USA, vol.2, pp.86-90, 1994.

[7] I. Usman, A. Khan, A. Ali and T. S. Choi, Reversible watermarking based on intelligent coefficient selection and integer wavelet transform, *International Journal of Innovative Computing, Information and Control*, vol.5, no.12(A), pp.4675-4682, 2009.

[8] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. on Image Processing*, vol.6, no.12, pp.1673-1687, 1997.

[9] W. H. Lin, Y. R. Wang and S. J. Horng, A wavelet-tree-based watermarking method using distance vector of binary cluster, *Expert Systems with Applications*, vol.36, no.6, pp.9869-9878, 2009.

[10] J. L. Liu, D. C. Lou, M. C. Chang and H. K. Tso, A robust watermarking scheme using self-reference image, *Computer Standards & Interfaces*, vol.28, pp.356-367, 2006.

[11] B. Chandra Mohan, S. S. kumar and B. N. Chatterji, A robust digital image watermarking scheme using singular value decomposition (SVD), dither quantization and edge detection, *International Journal on Graphics, Vision and Image Processing*, vol.8, no.1, pp.17-23, 2008.

[12] M. S. Raval and P. P. Rege, Discrete wavelet transform based multiple watermarking scheme, *Proc. of the IEEE TENCON Conf. for Convergent Technologies for Asia-Pacific Region*, Bangalore, India, vol.3, pp.935-938, 2003.

[13] V. Gorodetski, L. J. Ipopyack and V. Samoilov, SVD-based approach to transparent embedding data into digital images, *Proc. of the Int. Workshop, MMM-ACNS*, St. Petersburg, Russia, pp.263-274, 2001.

[14] R. Liu and T. Tan, A SVD-based watermarking scheme for protecting rightful ownership, *IEEE Trans. on Multimedian*, vol.4, no.1, pp.121-128, 2002.

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

[16] C. C. Lai, H. C. Huang and C. C. Tsai, A digital watermarking scheme based on singular value decomposition and micro-genetic algorithm, *International Journal of Innovative Computing, Information and Control*, vol.5, no.7, pp.1867-1873, 2009.

[17] C. C. Chang, C. C. Lin and Y. S. Hu, An SVD oriented watermark embedding scheme with high qualities for the restored images, *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.609-620, 2007.

[18] D. S. Chandra, Digital image watermarking using singular value decomposition, *Proc. of the 45th Midwest Symposium on Circuits and Systems (MWSCAS'02)*, Tulsa, OK, USA, vol.3, pp.264-267, 2002.

[19] C. H. Lin, J. C. Liu and P. C. Han, On the security of the full-band image watermark for copyright protection, *IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, pp.74-79, 2008.

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

[21] P. Bao and X. Ma, Image adaptive watermarking using wavelet domain singular value decomposition, *IEEE Trans. on Circuits and Systems for Video Technology*, vol.15, no.1, pp.96-102, 2005.

[22] E. Ganic and A. M. Eskicioglu, Robust embedding of visual watermarks using DWT-SVD, *Journal of Electronic Imaging*, vol.14, no.4, (043004), 2005.

[23] R. Amirtharajan and R. J. B. Balaguru, Constructive role of SFC & RGB fusion versus destructive intrusion, *Int. Journal of Computer Applications*, vol.1, no.20, pp.30-36, 2010.