# A Novel Image Zero-watermarking Scheme Based on DWT-SVD

Yaxun Zhou, Wei Jin
College of Information Science and Engineering, Ningbo University
Ningbo, China
zhouyaxun@nbu.edu.cn

*Abstract*—**In this paper, a novel copyright protection zero-watermarking scheme that combines the discrete wavelet transform (DWT) and the singular value decomposition (SVD) is proposed. Instead of modifying the original image data, which inevitably causes some permanent quality degradation, to embed a watermarking, the proposed scheme constructs a watermarking from the image features which extracts from the original image by applying the DWT and the SVD. Firstly, the original image is decomposed into the appropriate levels by the DWT, and the obtained approximation image is divided into non-overlapping blocks. The SVD is then applied to the each block to obtain the singular values. Finally, the embedding of zero-watermarking is realized through the exclusive or (XOR) operation between the first singular value of the each block and the pixel value of the actual binary character watermarking sequentially. The simulation results demonstrate that the proposed zero-watermarking scheme not only ensures the watermarked image quality without any distortion, but also has very good robustness to resist the common image processing attacks such as noise addition, filtering, compression and geometric cutting.**

***Keywords-zero-watermarking; digital image; DWT; SVD; robustness***

## I. INTRODUCTION

With the rapid development of computer networks and multimedia technology, digital multimedia such as audio, image and video are being widely and easily transmitted over the Internet. Duplication, modification and forgery of these multimedia contents have become difficult to detect and prevent. However, the ease of such manipulations may encourage the violation of intellectual property rights. As a result, the copyright protection has become a very important issue [1, 2]. To address this issue, a wide variety of techniques for the copyright protection of digital multimedia have been proposed. Among these techniques, digital watermarking has attracted considerable attention and been regarded as one of the most promising technique solutions to the problem of copyright protection of multimedia documents [3, 4].

Digital watermarking refers to embedding the copyright information such as copyright logo, signature, serial number, date, or icon, etc. into the original multimedia body that can be detected or extracted later by means of some operations in order to assert the rightful ownership of the multimedia. However, the conventional digital watermarking embedding procedure inevitably brings some permanent distortion to the original multimedia object. To solve this problem, a new zero-watermarking technique has been proposed in recent years, and has become a research hot of digital watermarking technology [5-7]. The basic idea of zero-watermarking technique is to construct a watermarking key directly from its own features of digital multimedia, combine it with an actual digital watermarking to form some zero-watermarking information, and then store them in the intellectual property databases to achieve the aim of copyright protection. Obviously, the zero-watermarking technique breaks through the conventional idea of embedding watermarking through modifying the spatial values or transform domain coefficients of the original multimedia. As the digital watermarking in the zero-watermarking technique is stored in the watermarking database, not embedded in the multimedia body, it has not the quality degradation problem of host digital multimedia. Because of this, the zero-watermarking scheme arrives at a good balance between the watermarking robustness and the imperceptibility.

Therefore, it is important for a zero-watermarking scheme to find or determine the internal stability feature information of digital multimedia and then construct a robust zero-watermarking from them. In this paper, a novel image zero-watermarking scheme based on the combined domain of discrete wavelet transform (DWT) and singular value decomposition (SVD) is proposed. A series of simulation results indicate that the proposed scheme has good robustness to resist some common image processing attacks.

## II. THEORETICAL BACKGROUND

There are two theories relevant to the proposed zero-watermarking copyright protection scheme, namely the discrete wavelet transform (DWT) and the singular value decomposition (SVD).

### A. *Discrete Wavelet Transform*

The DWT is a powerful multi-resolution decomposition tool which has been applied to a variety of image processing such as noise reduction, edge detection, and data compression. The characteristic of wavelet multi-resolution decomposition is consistent with the human eye's visual perception process [8]. After the DWT, an image is decomposed into four sub-bands $LL_1$, $HL_1$, $LH_1$, and $HH_1$, where $HL_1$, $LH_1$, and $HH_1$ represent the finest scale wavelet coefficients, i.e. the detailed image, while $LL_1$ stands for the coarse level coefficients, i.e. the approximation image. To obtain the next coarse level of wavelet coefficients, the sub-band $LL_1$ can be further decomposed into four sub-bands $LL_2$, $HL_2$, $LH_2$, and $HH_2$

978-1-61284-774-0/11/$26.00 ©2011 IEEE

again. This decomposition process continues until a certain final scale is reached. Compared to the detailed image, the low frequency approximation image has better stability against the image distortion.

### B. Singular Value Decomposition

The SVD is a powerful matrix decomposition tool which has also been used in a variety of applications, such as signal processing and pattern analysis. From the viewpoint of linear algebra, a discrete image can be regarded as a matrix with non-negative scalar entries. The SVD of an $N \times N$ image matrix $F$ has a decomposition form:

$$F = U \times S \times V^{\mathrm{T}} \tag{1}$$

where $U$ and $V$ are $N \times N$ orthogonal matrices, the superscript T denotes matrix transposition, and $S$ is an $N \times N$ matrix containing singular values on the diagonal and zeros off the diagonal. The singular values ($s_i$) of $F$ are arranged in a decreasing order $s_i > s_{i+1}$. The SVD can effectively reveal the essential property of image matrix, the main property of SVD relevant to digital watermarking is that the larger singular values of an image do not change significantly when common image processing attacks are performed on this image.

## III. DIGITAL ZERO-WATERMARKING SCHEME

The DWT-SVD based zero-watermarking embedding and extracting processes can be described as follows:

### A. Watermarking Embedding

The digital watermarking is a binary character image denoted as $W=\{\omega(i, j)=0/1,\ 1 \le i \le M_1,\ 1 \le j \le M_2\}$. The original digital image is a gray-level normalized image denoted as $F=\{0 \le f(i, j) \le 1,\ 1 \le i \le N_1,\ 1 \le j \le N_2\}$, where $\omega(i, j)$ and $f(i, j)$ represent the pixel value of coordinates $(i, j)$ of character watermarking and original image, with size of $M_1 \times M_2$ and $N_1 \times N_2$, respectively. Without loss of generality, the size of $M_1 \times M_2$ and $N_1 \times N_2$ satisfies $N_1/M_1=r$, $N_2/M_2=p$, $r$ and $p$ are integers.

Step 1: Decompose the original image $F$ by the $L$-level DWT, and obtain a $L$-level approximation image $F_L$.

Step 2: Divide the approximation image $F_L$ into multiple non-overlapping blocks of size $n_1 \times n_2$.

Step 3: Apply the SVD to each block and obtain the singular values of each block.

Step 4: Instead the each block with its first singular value and obtain a reduced matrix $B$ with size equal to the binary character watermarking. The sizes of original image, binary watermarking and block are requested to satisfy $N_1=2^L \times n_1 \times M_1$, $N_2=2^L \times n_2 \times M_2$.

Step 5: Compare the pixel value of matrix $B$ based on the following algorithm and return a binary embedding key $K$:

```
for i=1: M1, for j=1: M2
    if B(i,j)>B(i,j+1)
        K(i,j)=1;
    else
        K(i,j)=0;
    end
end, end.                                    (2)
```

Step 6: Construct a zero-watermarking information matrix $ZW$ from the binary embedding key $K$ and the actual binary character watermarking $W$ based on the following XOR operation:

$$ZW = \mathrm{XOR}\ (K, W) \tag{3}$$

Finally, store the zero-watermarking information matrix $ZW$ in the intellectual property databases so that it can be extracted to assert the rightful ownership or copyright of the image when needed.

### B. Watermarking Extraction

The watermarking extraction process is similar to the embedding process.

Step 1: Decompose the tested image $T\_F$ with size of $N_1 \times N_2$ by the $L$-level DWT, and obtain an approximation image $T\_F_L$.

Step 2: Divide the approximation image $T\_F_L$ into multiple non-overlapping blocks of size $n_1 \times n_2$.

Step 3: Apply the SVD to each block and obtain the singular values of each block.

Step 4: Instead the each block with its first singular value and obtain a reduced matrix $T\_B$.

Step 5: Compare the pixel value of matrix $T\_B$ based on the following algorithm and return a binary extraction key $T\_K$:

```
for i=1: M1, for j=1: M2
    if T_B (i,j)> T_B (i,j+1)
        T_K(i,j)=1;
    else
        T_K(i,j)=0;
    end
end, end.                                    (4)
```

Finally, recover the watermarking $T\_W$ from the binary extraction key $T\_K$ and the zero-watermarking information matrix $ZW$ stored in the intellectual property databases based on the following XOR operation:

$$T\_W = \mathrm{XOR}\ (T\_K, ZW) \tag{5}$$

## IV. EXPERIMENTAL SIMULATION RESULTS

The original image is a normalized grayscale 8-bit Lena image of size 512×512 and the digital watermarking is a binary character image of size 32×32. The original Lena image and watermarking are shown in Fig.1. For embedding the watermarking, a 2-level wavelet decomposition and reconstruction was applied to the original image, and the block size is taken as 4×4. The quality of the watermarked image is evaluated by peak signal to noise ratio ($PSNR$), and the objective evaluation of watermarking extraction results uses the error rate $\rho_{\mathrm{b}}$ defined as below:

$$PSNR = 10 \times \log_{10} \frac{1^2}{MSE} \ \text{(dB)} \tag{6}$$

$$MSE = \frac{1}{N_1 \times N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \left( f(i,j) - f^*(i,j) \right)^2 \tag{7}$$

$$\rho_{\mathrm{b}} = T_{\mathrm{error}} / T_{\mathrm{b}} \tag{8}$$

where $f(i, j)$ and $f^*(i, j)$ represent the pixel values of the original and watermarked image, respectively. $T_b$ represents the total pixel number of the embedded digital watermarking, $T_{error}$ represents the total error pixel number occurred in the extracted watermarking.

(a) (b)

Fig.1. (a) The original Lena image, and (b) the binary character watermarking

For the proposed zero-watermarking scheme in this paper, the watermarked Lena image presented in Fig.2 (a) has *PSNR* of infinite value, indicating that no degradation occurs in the watermarked Lena image any all. It can also be seen that any perceptual distortion cannot be found, revealing the unique advantage of zero-watermarking scheme. The extracted watermarking is presented in Fig. 2 (b), it can be seen that the embedded watermarking can be fully recovered when the watermarked Lena image is not affected, and the error rate $\rho_b$ is 0%.

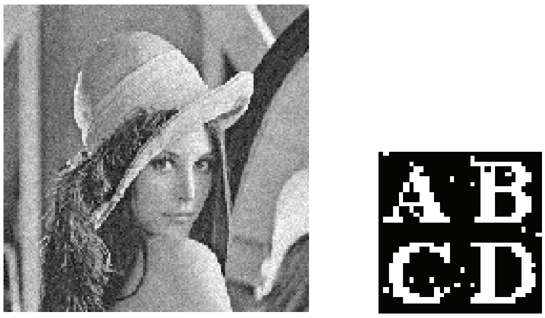
(a) (b)

Fig.2. (a) The watermarked Lena image, and (b) the extracted watermarking

An effective copyright protection scheme should provide good robustness against different types of attacks. In the following experiments, the robustness of the proposed zero-watermarking scheme is evaluated by performing several common image processing attacks.

*A. Noise Addition*

Generally, addition of noise is responsible for the degradation and distortion of the image. The watermark information is also degraded by noise addition and results in difficulty in watermarking extraction. Fig.3 (a) is the watermarked Lena image added by the Gaussian noise with mean of 0 and variance of 0.002. As a result, the watermarked Lena image looks noisy, the perceptual quality degrades obviously and its *PSNR* reduces to 26.9dB. However, the extracted watermarking shown in Fig.3 (b) is clearly recognizable, and the error rate $\rho_b$ is only about 2.6%.



(a) (b)

Fig. 3. (a) The noised watermarked Lena image and (b) the extracted result

*B. Median Filtering*

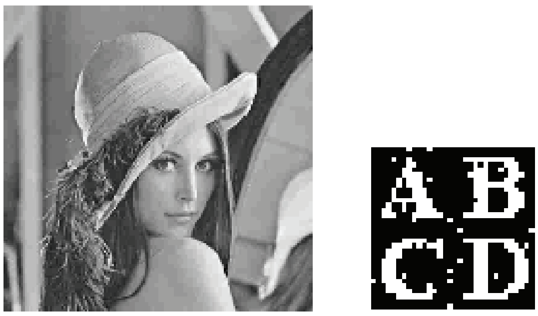
Fig.4 (a) is the watermarked Lena image acquired by performing median filtering with filter window of [5×5] size. It can be observed that after median filtering, lot of detail data is lost and the *PSNR* of the watermarked image reduces to 29.3dB. Fig.4 (b) is the corresponding extracted watermarking ($\rho_b$=2.1%) and it is clearly recognizable. The test result shows that the proposed algorithm can resist a filtering attack.

(a) (b)

Fig. 4. (a) The filtered watermarked Lena image and (b) the extracted result

*C. JPEG Compression*

Fig.5 (a) is the JPEG compressed version of the watermarked Lena image with a quality factor of 15%. Its *PSNR* reduces to 30.8dB and the extracted watermarking is shown in Fig.5 (b). Although the compression ratio is very high and the box compression effect is obvious, the extracted watermarking is still good ($\rho_b$=3.1%).



(a) (b)

Fig. 5. (a) The compressed watermarked Lena image and (b) the extracted result

### D. *Geometric crop*

Image cropping is very frequently used in real life. Cropping is the process of removing a portion of an image and thus is a lossy operation. Fig.6 (a) is the watermarked Lena image with parts of component has been cropped randomly (*PSNR*=16.7dB) and the extracted result is shown in Fig.6 (b) ($\rho_b$=4.7%). It is shown again that the proposed scheme has better robustness against the geometric distortion, and the watermarking can be recovered relatively satisfied from the parts of image.

(a) (b)

Fig. 6. (a) The cropped watermarked Lena image and (b) the extracted result

## V. CONCLUSION

In this paper, a novel image zero-watermarking scheme based on DWT-SVD is presented. The scheme fully exploits the respective characteristics of the DWT which achieves multi-resolution decomposition and the SVD which efficiently represents intrinsic algebraic properties of an image. The use of DWT-SVD combined domain helps to extract stable image internal features and then construct a robust zero-watermarking. Simulation results of the proposed scheme have shown the robustness under common image manipulation attacks.


## ACKNOWLEDGMENT

This work was financially supported by the Natural Science Foundation of Zhejiang Province, China (Y1080778), Ningbo Optoelectronic Materials and Devices Creative Team (2009B21007), and was sponsored by K. C. Wong Magna Fund and Hu Lan Outstanding Doctoral Fund in Ningbo University.


## REFERENCES


[1] J. C. Patra, J. E. Phua, and C. Bornand, “A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression,” Digital Signal Processing, vol. 20, pp. 1597-1611, December 2010

[2] 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, September 2008

[3] M. S. Wang, and W. C. Chen, “A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography,” Computer Standards & Interfaces, vol. 31, pp. 757-762, June 2009

[4] G. Bhatnagar, and B. Raman, “A new robust reference watermarking scheme based on DWT-SVD,” Computer Standards & Interfaces, vol. 31, pp. 1002-1013, September 2009

[5] Q. Wen, T. F. Sun, and S. X. Wang, “Concept and application of zero-watermark,” Acta Electronica Sinica, vol. 31, pp. 214-216, February 2003 (In Chinese)

[6] J. H. Ma, and J. X. He, “A wavelet-based method of zero-watermark,” Journal of Image and Graphics, vol. 12, pp.581-585, April 2007 (In Chinese)

[7] W. Song, J. J. Hou, Z. H. Li, and L. Huang, “A novel zero-bit watermarking algorithm based on Logistic chaotic system and singular value decomposition,” Acta Physica Sinica, vol. 58, pp. 4449-4456, July 2009 (In Chinese)

[8] X. H. Sun, J. M. Lu, and X. M. Niu, “Digital watermarking technology and applications,” Beijing: Science Press, pp. 11-191, 2004 (In Chinese)