私立東海大學資訊工程與科學研究所

碩士論文

指導教授：林祝興 博士

Dr. Chu-Hsing Lin

一種基於 DDWT 與 SVD 浮水印技術的數位版權保護方法之研究

On Image Watermarking Schemes Based on DDWT and SVD for Copyright Protection

研究生：李衍緯

(Yan-Wei Lee)

中 華 民 國 九 十 七 年 六 月

東海大學碩士學位論文考試審定書

東海大學資訊工程與科學系 研究所

研究生 李 衍 緯 所提之論文

一種基於DDWT與SVD浮水印技術的數位版權保護方法之研究

經本委員會審查，符合碩士學位論文標準。

學位考試委員會
召 集 人 詹進科 簽章

委 員 張添峰

劉榮春

指 導 教 授 林祝興 簽章

中華民國 97 年 6 月 19 日

摘要

在這個資訊化的時代，人們可以藉由快速的網路自由且輕鬆簡單的傳輸數位多媒體資料。但有些不合法或是未經授權下的使用者可以任意複製並且傳送到網路上。保護智慧財產權變成一項重要的課題。

在本篇論文中，我們提出一種基於奇異值分解（Singular Value Decomposition, SVD) 方法和分散式離散小波轉換 (Distributed Discrete Wavelet Transformation, DDWT)方法下的數位浮水印技術來保護數位版權。DDWT 是基於 DWT 上的變化藉由修改基本的運算（水平運算與垂直運算）。DDWT 可以將浮水印均勻的嵌入至整張影像中以抵抗破壞(如：裁切或是旋轉)。

我們利用奇異值分解的浮水印能夠有效的抵擋幾何攻擊（旋轉、縮放等攻擊）與非幾何攻擊（增加高斯雜訊攻擊、銳利化攻擊、提高高斯模糊化等攻擊）。分散式離散小波轉換的浮水印能夠有效的抵抗裁切攻擊。實驗的結果顯示我們的方法能夠有效的抵擋幾何攻擊與非幾何攻擊。

關鍵字： 數位浮水印技術、版權保護、資訊隱藏、奇異值分解、分散式離散小波轉換、影像攻擊。

Abstract

In this digital age, people can use fast speed of internet to transmitted digital multimedia data freely and easily. However some illegal or unauthorized users can duplicate and transmit digital multimedia from the Internet. Protection of the intellectual property right becomes an important topic. In this thesis, we proposed a digital watermark scheme based on Singular Value Decomposition (SVD) method and Distributed Discrete Wavelet Transformation (DDWT) method for copyright protection. DDWT performs similar horizontal and vertical process as discrete wavelet transformation (DWT) to transform data in the spatial domain to the frequency domain and then embed watermark information in the frequency domain. So, DDWT can uniformly distribute watermark information in spatial domain, and is very robust against some image attacks, such as cropping or rotation.

First, we embedded watermark using SVD method and we used 3-scale DDWT method to embed watermark in sub-band LL and HH. The SVD method is robust to against geometric attacks (rotation, rescale) and non-geometric attacks (Gaussian noise, sharp, Gaussian blur). The DDWT method is robust to against cropping attack. Experimental results show our method can be effective to against geometric attacks and non-geometric attacks.

Keywords: Digital watermarking technology, Copyright protection, Data hiding, Singular value decomposition (SVD), Distributed discrete wavelet transformation (DDWT).

致謝

本篇論文能夠順利的完成，要感謝的人很多，首先要感謝我的指導老師　林祝興教授，除了課業上的悉心指導外也教導了我做人做事的道理，使得我在研究所期間有所成長。另外，感謝　劉榮春教授在論文與研究中的指導與啟發，使得本論文得以順利完成，僅向兩位恩師至上學生最高的敬意與謝意。也感謝口試委員們撥冗指證論文並提供寶貴的意見，使得本論文更加完整。

在學期間也感謝實驗室學長姐鎮宇、麗靜、佳男、君維、仁傑、彥菱與嘉仁對於研究所課業上的建議與幫助；實驗室同學懋樺、育瑩在兩年中給我的安慰與打氣，嘉瀚、掄元帶來的活潑生氣與歡樂以及學弟妹建廷、美君的鼓勵。還要感謝一直陪伴在我身邊的惠娟，妳是我最大的推動力。

最後感謝我的家人，在我求學期間給予我最大的包容和支持，讓我順利完成學業。僅將此論文獻給我最敬愛的師長、家人、朋友與實驗室同學們。

九十七年 仲夏　僅識於　私立東海大學資訊工程與科學系

資訊安全實驗室

Contents

Figures

Tables

Chapter 1
Introduction

In this information age, digital multimedia is disseminated rapidly through the Internet. Digital multimedia could be duplicated with very low cost and tampered with simple editing instructions by illegal and non-authentication users. Protection of the intellectual property right becomes an important topic. To protect the intellectual property right and authentication of legitimate owner, watermark information is embedded invisibly in digital multimedia and extracted to claim the ownership of digital multimedia and protect the owner's right. In this way, the watermark technology is applied in copyright protection. In this thesis, we proposed a robust watermark method that combines the Singular Value Decomposition (SVD) [1] and Distributed Discrete Wavelet Transformation (DDWT) methods [2]. We achieve goals of information hiding and robustness of watermark against image attacks. This thesis is organized as follows. Chapter 2 introduces the concept of watermark and related technologies. We describe SVD method and DDWT method in Chapter 3 and Chapter 4, respectively. Chapter 5 describes watermark embedding and extracting schemes. Simulation results are shown in Chapter 6. Conclusions are made in Chapter 7, and future works are discussed in Chapter 8.

Chapter 2
Preliminaries

This chapter is organized as follows. First, we introduce backgrounds of digital watermarks. Then, we describe watermarking technologies in the spatial domain and frequency domain in the following sections.

2.1 Digital watermark

In this section, we will introduce the watermark technology, including general features of watermark, requirements and classification of digital watermark.

2.1.1 General digital watermark

Digital watermark is an important technology to implement copyright protection. In general, digital watermarking is divided into two parts: the watermark embedding process and watermark extracting process.

Watermark embedding process: The watermark embedding process contains an original image (I), the watermark (W), and a secret key (K). The output of the watermark embedding process is called the stego-image (I'). Fig. 1 shows the watermark embedding process.

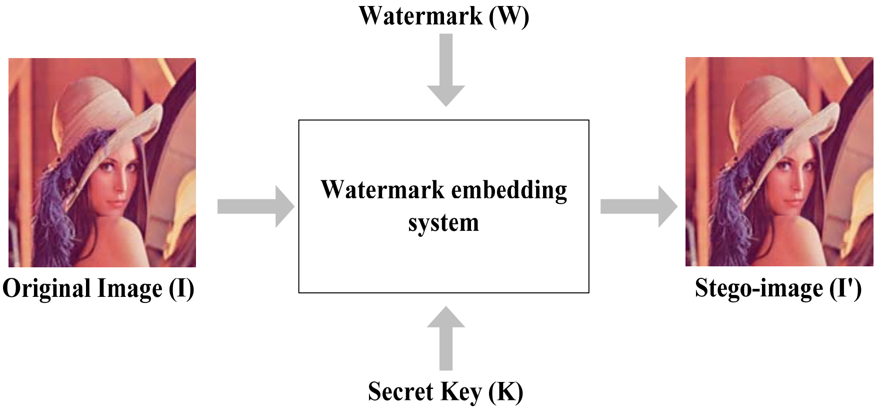


Figure 1. The block diagram of the watermark embedding process

Watermark extracting process: Fig. 2 shows the watermark extracting process. Inputs of the watermark extracting process are the stego- image (I'), the secret key (K), and watermark (W).The output of the watermark extracting process is the extracted watermark (W').

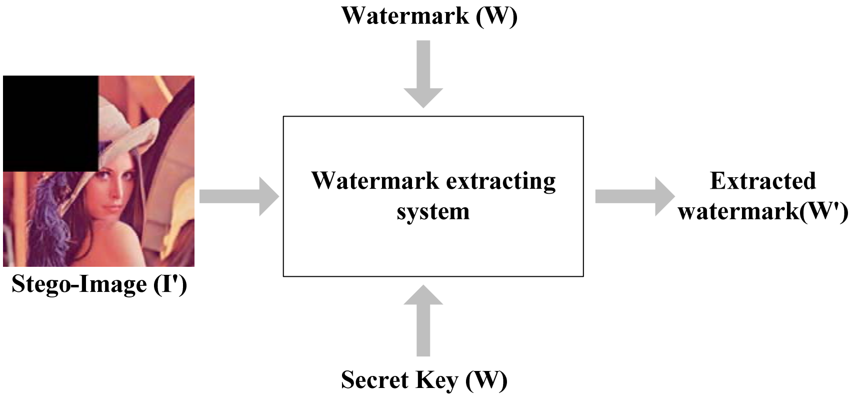


Figure 2. The block diagram of the watermark extracting process

2.1.2 Digital watermark requirements

A good digital watermarking has to satisfy basic requirements as follows:

1. Imperceptibility：Imperceptibility means the embedded digital watermark will not degrade the quality of the original image. In other words, after embedding watermark in the digital cover image to produce the stego-image, the stego-image must have highly visual quality and indistinguishable from the cover image.

2. **Non-removable**：Non-removable means undeletable. When images have not been serious attacked, watermark information should not be removed.
3. **Robustness**：Robustness means the stego-image can resist attacks. Even suffered from attacks, the watermark still can be extracted from the stego-image.
4. **Unambiguousness**：Unambiguousness means that the extracted watermark must be clear, and cannot be equivocal in identification.

2.1.3 Classification of digital watermark

In 1999, Petitcolas et al. [6] classified information hiding by different applications into four branches shown in Fig. 3.

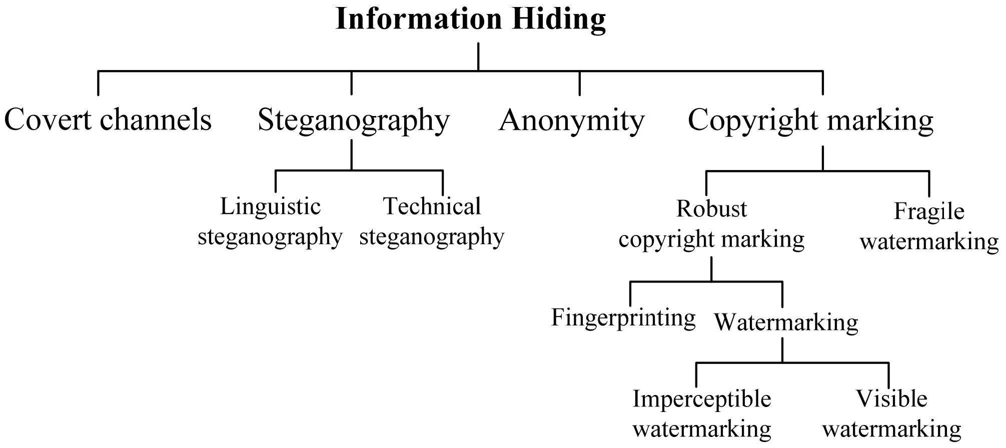


Figure 3. The classification of data hiding

The digital watermark technology is one branch of information hiding. Watermark technology has been developing in years and can be classified in the following three ways.

1. Visual senses: According to the characteristic of human vision, digital watermark technology can divided into visible watermark and invisible watermark.

2. Domain: Digital watermark system can process watermark in two domains: the spatial domain and the frequency domain. To process watermark in spatial domain means to embed watermark in some pixels by using some method. Tp process watermark in frequency domain, we use transformation function to transform original image to the frequency domain, and then embed watermark in the frequency domain, and do the inverse transform to have the stego-image. We will describe spatial domain and frequency domain watermarking technologies watermarking technologies in Section 2.2 and Section 2.3, respectively.

3. Embedding method: Watermarking technology can divided into three classes according to embedding methods: non-blind watermarking, semi-blind watermarking and blind watermarking.

2.2 Spatial domain watermarking technologies

Spatial domain watermarking technology embeds directly the watermark in spatial image without doing any transformation. Eyes of people are not sensitive enough to feel the slight change in image. Therefore, some scheme may be used to embed watermark in image in such a way that eyes cannot feel the minor changes. Least Significant Bits (LSB) [7-10] is a famous spatial domain watermarking technology.

2.2.1 Least significant bits watermarking scheme

In generally [10-12] , a pixel uses 8-bits to express strength of color pixel. Therefore, we can remove all of the least significant bits to embed the data (watermark) that we want to hide in the image. Each pixel can embed 1-bit of data, so the capacity is decided by the image size. To extract watermark, we just combine the data taken from LSBs with the original data. Fig. 4 shows the data flow of LSB watermarking scheme. The disadvantage of LSB is that it is not robust. We can use encoded watermark or pseudo-random permutation of the watermark to enhance robustness of the LSB watermark scheme.

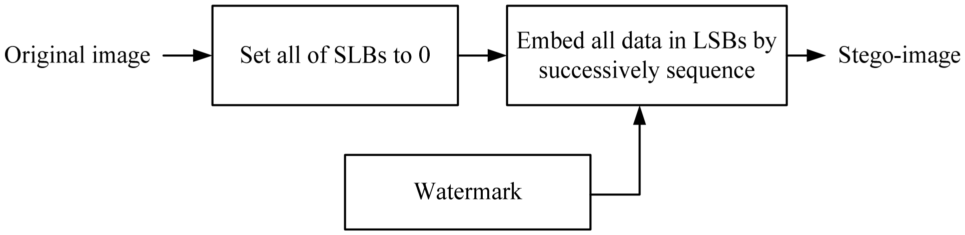


Figure 4. Data flow of Least Significant Bits watermarking scheme

2.3 Frequency domain watermarking technologies

Digital image in the frequency domain is obtained by transforming the spatial image. After transformation, it can be used to embed watermark.

2.3.1 Discrete Cosine Transformation (DCT)

In 1995, Koch and Zhao proposed the Discrete Cosine Transformation (DCT) [13]. Discrete Cosine Transformation processes the spatial domain image to frequency domain by using Forward Discrete Cosine Transformation (FDCT) shown in Equation (1). To process the frequency domain image to spatial domain we use the inverse of Discrete Cosine Transformation (IDCT) shown in eEquation (2).

$$D(i,j)=\frac{1}{\sqrt{2N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(i)C(j)f(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

$$f(x,y)=\frac{1}{\sqrt{2N}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}C(i)C(j)D(i,j)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (2)$$

Where (i,j) means the coefficients of location position in the frequency domain. (x,y) means the coefficients of location position in the spatial domain. $f(x,y)$ is the pixel value of $(x,y)-128$. $D(i,j)$ means the position coefficients (i,j) in frequency domain, and N is the length and the width of 2-dimention array.

2.3.2 Discrete Wavelet Transformation (DWT)

Discrete Wavelet Transformation (DWT) [14-17] was proposed in 1976, DWT technology is a basic method on signal processing. There are many different classes of DWT. Harr DWT [17] scheme is the fastest and is easy to implement. Harr DWT includes two basic processes, namely horizontal process and vertical process. The horizontal process is to separate the original image along the horizontal direction into two equal sub-blocks. Add and subtract corresponding pixels on the two sub-blocks, then replace pixels on the left sub-block with the result of the addition and and pixels on the right sub-block with the result of the subtraction. Denote the processed left sub-block as L and the right sub-block as H. The vertical process is to separate the horizontally processed image along the vertical direction into four equal sub-blocks. Add and Subtract corresponding pixels on the four sub-blocks and replace pixels on the two upper sub-blocks with the result of the addition and pixels on the two lower sub-blocks with the result of the subtraction. Thus, we generate four sub-blocks and denote them as LL, HL, LH, and HH. The example of 1-scale Discrete Wavelet Transformation is shown in Fig. 5.

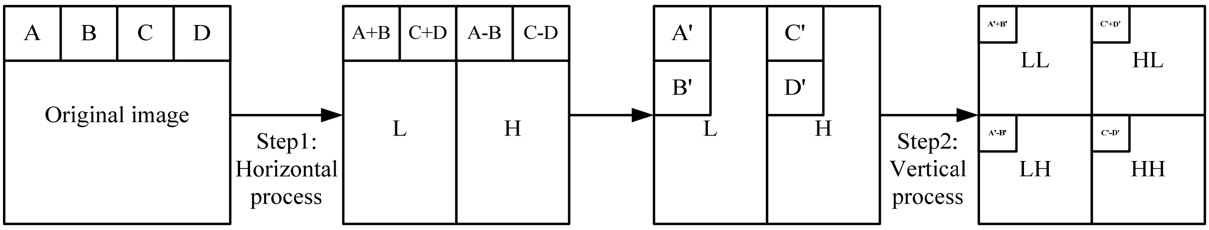


Figure 5. The example for labeling of the 1-scale Discrete Wavelet Transformation

2.3.3 Discrete Fourier Transformation (DFT)

Fourier Transformation not only can be used on the spatial filtering but also can be used to process spatial image to frequency domain. Equations (3) and (4) show the Fourier Transformation (FT) and Inverse Fourier Transformation (IFT), respectively.

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cdot e^{\left[-2\pi i(\frac{xu}{M}+\frac{yv}{N})\right]} \tag{3}$$

$$f(x,y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) \cdot e^{\left[2\pi i\left(\frac{xu}{M}+\frac{yv}{N}\right)\right]} \tag{4}$$

Where (x,y) means the coefficients of location position in the spatial domain. (u,v) means the coefficients of location position in the frequency domain. $f(x,y)$ means the position coefficients (x,y) in the spatial domain. $F(u,v)$ means the position coefficients (u,v) in the frequency domain.

Chapter 3
Background

3.1 Singular Value Decomposition

Singular Value Decomposition (SVD) method is based on linear algebra. Chadra [1] proposed a new digital watermark scheme using singular value decomposition in 2002 to enhance the robustness of watermark against geometric and non-geometric attacks. It is also used in image compression [27-32], watermarking technologies [33-36], signal processing fields [37-43] , noise estimation [44] , ect.

3.1.1 Basic Theory

Singular Value Decomposition is an important topic in linear algebra. SVD decomposes a matrix into three matrixes. Applications of SVD include computing pseudo inverse of a matrix, multivariate analysis and solution of least-squares problems. It is also used in image compression, watermarking technologies, signal processing fields, noise estimation, etc. SVD is described as follows:

Digital image matrix $A \in R^{M \times N}$ with $M \geq N$ and R is the real number, can be represented by SVD as

$$A = U \Sigma V^T \tag{5}$$

where U and V is the $M \times M$ and $N \times N$ orthogonal (unitary) matrix of A,. Σ is the $M \times N$ diagonal matrix, i.e. $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_p)$, $p = \min\{M, N\}$ and $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_p \geq 0$ represent the singular values σ_i of A.

3.1.2 The watermark embedding process

Step 1 Input original image X ($M \times N$) and watermark image W ($P \times Q$), and do SVD to the original image X and the watermark W to obtain：

$$X = U_X \sum_X V_X^T \tag{6}$$

$$W = U_W \sum_W V_W^T \tag{7}$$

Where $\sum_X$ and $\sum_W$ means the singular value of the original image *X* and watermark *W*, respectively. σ_{X_i} are eigenvalues of $\sum_X$, σ_{W_i} are eigenvalues of $\sum_W$. Element of σ_{X_i} is [σ_{X_1} , σ_{X_2} ,…, σ_{X_N}] with $\sigma_{X_1} \geq \sigma_{X_2} \geq \ldots \geq \sigma_{X_N} \geq 0$. Element of σ_{W_i} is [σ_{W_1} , σ_{W_2} ,…, σ_{W_N}] with $\sigma_{W_1} \geq \sigma_{W_2} \geq \ldots \geq \sigma_{W_N} \geq 0$.

Step 2 Embed the singular value of watermark into the singular value of the original image.

$$\sigma_{Y_i} = \sigma_{X_i} + (\alpha_i \times \sigma_{W_i}) \tag{8}$$

Where σ_{X_i} means the element of $\sum_X$ and σ_{W_i} means the element of $\sum_W$. σ_{Y_i} is the element of $\sum_Y$, $\sum_Y$ means the singular matrix of the stego-image *Y*.

Step 3 The stego-image *Y* is obtained by

$$Y = U_X \sum_Y V_X^T \tag{9}$$

3.1.3 The watermark extracting process

Step 1 Input the attacked image Y’, using SVD to obtain:

$$Y' = U' \Sigma_Y' V'^T \tag{10}$$

Step 2 The singular matrix of extracted watermark is obtained as follows:

$$\Sigma'_W = \frac{(\Sigma'_Y - \Sigma'_X)}{\alpha} \tag{11}$$

Step 3 We multiply the three matrices to obtain the extracted watermark *W’*

$$W' = U_W \Sigma'_W V_W \tag{12}$$

3.2 Lin’s Distributed Discrete Wavelet Transformation Scheme

In 2006, Lin et al. [2] proposed the Distributed Discrete Wavelet Transformation Scheme (DDWT) technology [6-8]. DDWT watermark technology is based on DWT watermark technology. DDWT uses two basic processes: the horizontal process and the vertical process. The DDWT watermark technology is different from the DWT watermark technology. The DWT watermark scheme collectedly embed watermark in some sub-band, whereas the DDWT watermark scheme uniformly disperse the watermark over the image. The advantage of DDWT watermark scheme is that it is very robust against cropping and rotation attacks. But the disadvantage of DDWT watermark scheme is not very robust against other geometric attacks such as scaling, and non-geometric attacks such as sharp, Gaussian blur and Gaussian noise.

3.2.1 Multi-scale Distributed Discrete Wavelet Transformation (DDWT)

DDWT is based on Discrete Wavelet Transformation (DWT), which consists of the horizontal process and the vertical process. The steps of multi-scale DDWT transformation are described as follows:

Step 1 **Horizontal process:**

1) Separate the original image along horizontal direction in two equal blocks.

2) Add and subtract corresponding pixels on the two sub-blocks, then replace pixels on the left sub block with the result of the addition and pixels on the right sub-block with the result of the subtraction. Denote the processed left sub block

as L and the right sub-block as H.

Step 2 **Vertical process:**

1) Separate the horizontal processed image along vertical direction into two equal blocks.
2) Add and Subtract corresponding pixels on the two sub-blocks and replace pixels on the upper sub block with the result of the addition and pixels on the lower sub-block with the result of the subtraction. Thus, we generate four sub-blocks and denote them LL, HL, LH, and HH shown in Fig. 6. Fig. 7 shows results of the multiple-scale DDWT. The 1-scale DDWT transform of original image with 4×4 pixels is shown in Fig. 8.

Step 3 **Repeat Step1 and Step2 K times:**

Results of K-scale DDWT transform is generated by doing Step1 and Step 2 operations on the sub-band LL of (K-1)-scale DDWT transform.

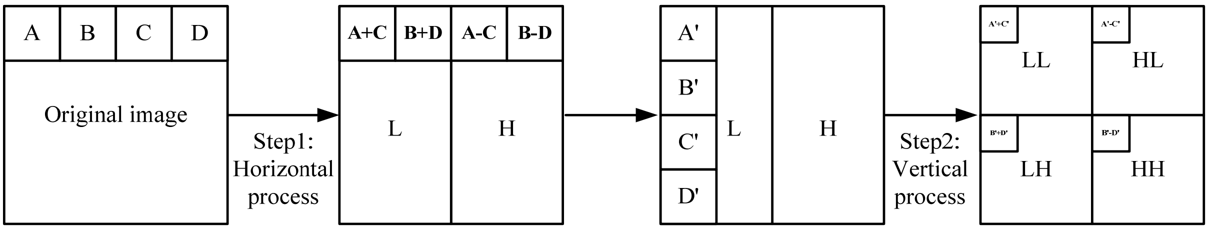


Figure 6. The example for labeling of the 1-scale Distributed Discrete Wavelet Transformation

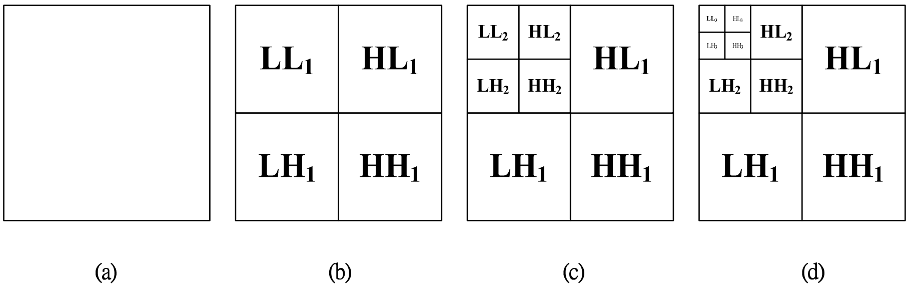
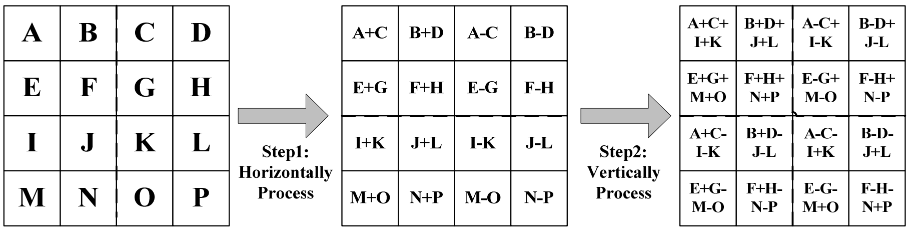


Figure 7. Multiple-scale DDWT processes (a) The original image and results of (b) 1-scale DDWT (c) 2-scale DDWT (d) 3-scale DDWT



A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Step1: Horizontally Process

A+C	B+D	A-C	B-D
E+G	F+H	E-G	F-H
I+K	J+L	I-K	J-L
M+O	N+P	M-O	N-P

Step2: Vertically Process

A+C+ I+K	B+D+ J+L	A-C+ I-K	B-D+ J-L
E+G+ M+O	F+H+ N+P	E-G+ M-O	F-H+ N-P
A+C- I-K	B+D- J-L	A-C- I+K	B-D- J+L
E+G- M-O	F+H- N-P	E-G- M+O	F-H- N+P

Figure 8. The example of 1-scale DDWT on an original image with 4×4 pixels

3.2.2 The watermark embedding process

Step 1 Input original image X ($M \times M$) and watermark image W ($N \times N$)；

Step 2 Using K-scale DDWT transform with *X*, where K is the number of scales and set scaling value t；

Step 3 Take the HL and LH from the K-scale DDWT transform and embed watermark into sub-band HL and LH using following equations:

$$If\ \ W_{(i,j)} = \mathbf{0};\ \ HL_{(i,j)} = t \times (\mathbf{2}^{K})^{2} + HL_{(i,j)} \tag{13}$$

$$If\ \ W_{(i,j)} = \mathbf{1};\ \ LH_{(i,j)} = t \times (\mathbf{2}^{K})^{2} + LH_{(i,j)} \tag{14}$$

Step 4 Repeat step 3, until all of the watermark information are embedded；

Step 5 Do inverse DDWT to obtain the stego-image.

3.2.3 The watermark extracting process

Step 1 Input embedded image *E* and original image *X* ($M \times M$)；

Step 2 Compute the block length *l* of image data for a single extracting process：

$$l = \left(\frac{M}{\mathbf{2}^{K-\mathbf{1}}} \right) \tag{15}$$

Step 3 Divide *E* and *X* with block length *l* into sub-blocks. Each image can be divided into s sub-blocks, $s = ((\mathbf{2}^{K-\mathbf{1}})^{\mathbf{2}})$ to obtain E_i and X_i , where $i \in \{\mathbf{1}, \mathbf{2}, ...s\}$ ；

Step 4 Subtract corresponding subsections from *E* and *X*, resulting in elements of array V_i, where $i \in \{\mathbf{1}, \mathbf{2}, ...s\}$ ；

Step 5 With each block of *V*, divide it into four square subsections with block length of ($l/2$). The sub-blocks are named as LL, HL, LH, and HH.

Step 6 Extract the individual pixel of the embedded watermark by equation (16):

$$W_{(i,j)} = \begin{cases} \mathbf{1}, \ LL_{(i,j)} > \mathbf{0} \ \mathit{and} \ LH_{(i,j)} > \mathbf{0} \\ \mathbf{0}, \ LL_{(i,j)} > \mathbf{0} \ \mathit{and} \ HL_{(i,j)} > \mathbf{0} \end{cases} \tag{16}$$

Step 7 Repeat until all of the pixels in the embedded image are processed.

Chapter 4
Proposed Scheme

We combine the SVD watermark technology and DDWT watermark technology to obtain a novel watermark scheme. Our proposed watermark scheme combines the merits of SVD and DDWT. SVD will provide the robustness against geometric attacks (such as rotation or rescaling) and non-geometric attacks (such as sharp, Gaussian noise and Gaussian blur). DDWT will provide the robustness against cropping attacks. Our proposed watermark scheme is very robust against most kinds of geometric attacks and non-geometric attacks. Our proposed watermark is also robust against special attacks such as waveform, fisheye and mosaic.

4.1 Watermark embedding process

Our digital watermark embedding process is described in the following six steps:

Step 1 Input the original image $X_{M\times M}$ and the watermark $W_{N\times N}$;

Step 2 Apply SVD on *X* and *W*:

$$X = U_X \Sigma_X V_X^T \tag{17}$$

$$W = U_W \Sigma_W V_W^T \tag{18}$$

Step 3 Embed the watermark by processing eigenvalues as follows:

$$\sigma_Y = \sigma_X + (\alpha \times \sigma_W) \tag{19}$$

Where σ_{X_i} are eigenvalues of $\sum_X$, σ_{W_i} are eigenvalues of $\sum_W$, σ_{Y_i} are eigenvalues of $\sum_Y$.

Step 4 Use SVD to obtain Y':

$$Y' = U_X \Sigma_Y V_X^T \tag{20}$$

Step 5 Process Y' with the 3-scale DDWT and embed watermarks in sub-bands LL3 and HH3：

$$If\ W(i,j)=0\ \ then\ Y_{LL_3}(i,j)=Y_{LL_3}(i,j)+\alpha\times(2^K)^2; \tag{21}$$

$$If\ W(i,j)=1\ \ then\ Y_{HH_3}(i,j)=Y_{HH_3}(i,j)+\alpha\times(2^K)^2; \tag{22}$$

Step 6 Apply inverse DDWT to obtain the stego-image *Y*.

4.2 Watermark extracting process

Our digital watermark extracting process is described in the following five steps:

Step 1 Input the stego-image *Y*, the original image *X*, the image Y', and the watermark *W*.

Step 2 Subtract Y' from *Y* to obtain Y_{Diff} , and apply equation (23) to extract the embedded watermark W_{DDWT}

$$W_{DDWT}(i,j)=\begin{cases}0, & if\ Y_{DDWT}(i,j)<0\\ 1, & otherwise\end{cases} \tag{23}$$

Step 3 Apply SVD on *X*, Y' and *W* to find their eigenvalues $\sigma_{X_i}, \sigma_{W_i}, \sigma_{Y_i}$.

$$Y=U_Y\Sigma_Y V_Y^T \tag{24}$$

$$W=U_W\Sigma_W V_W^T \tag{25}$$

$$X=U_X\Sigma_X V_X^T \tag{26}$$

Step 4 Extract Σ_{SVD} by using equation (27):

$$\sigma_{SVD}=\frac{\sigma_{Y_i}-\sigma_{X_i}}{\alpha} \tag{27}$$

Where σ_{SVD} is elements of eigenvalues in Σ_{SVD}.

Step 5 Apply SVD to obtain the SVD watermark W_{SVD}:

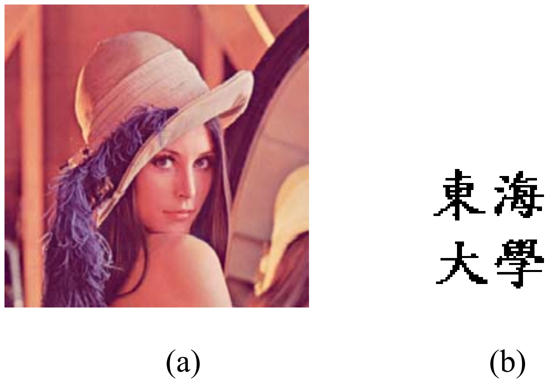
$$W_{SVD}=U_W\Sigma_{SVD}V_W^T \tag{28}$$

Chapter 5
Experimental Results and Analysis

In this chapter, we describe the hardware and software in experimental environment in Section 6.1. We describe the measurement tools to compare the quality of image and the watermark in Section 6.2. Then we show the result of the proposed method in Section 6.3. To test the robustness of our proposed method, we attack the stego-image by means of geometric attacks and non-geometric attacks, including cropping, sharp, Gaussian noise, Gaussian blur, contract adjustment, histogram equalization, rescaling (512→256→512), mosaic (2 pixels), waveform and fisheye.

5.1 Environmental setting

In our experiment, we used the original image of Lena with 512×512 pixels 24-bit full color image shown in Fig. 9(a).The watermark is a binary image with 64×64 pixels binary image shown in Fig. 9(b). The experimental environment was an HP-Compaq Presario V3016 laptop computer, with a Mobile Dual Core AMD Turion 64 X2 TL-52, 1600 MHz CPU, and 1GB RAM. The algorithm implementation software is MATLAB, running on Windows XP. Attacking tests had been done by using Adobe Photo Shop CS version 8.0.



(a) (b)

Figure 9. The experimental setting (a) Original image (b) Watermark

5.2 Measurement tools

To measure the quality of the stego-image, we compute its Peak Signal to Noise Ratios (PSNR) value. A stego-image with higher PSNR value means it is more similar to the original image. The PSNR is defined as below:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} dB \tag{29}$$

Where MSE is the mean square error of the two images:

$$MSE = \left(\frac{1}{m^2}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \left(\alpha_{ij} - \beta_{ij}\right)^2 \tag{30}$$

Where α_{ij} s stand for pixels of original image, β_{ij} s stand for pixels of stego-image.

Pearson's Correlation Coefficient is also used to measure correlation or association between the original watermark (W) and the extracted watermark (W'):

$$Corr\left(W, W'\right) = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \left(W_{(i,j)} - \overline{W}\right)\left(W'_{(i,j)} - \overline{W'}\right)}{\sqrt{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \left(W_{(i,j)} - \overline{W}\right)^2} \sqrt{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \left(W'_{(i,j)} - \overline{W'}\right)^2}} \tag{31}$$

Where W means the original watermark, W' means the extracted watermark, $\overline{W} = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} W_{(i,j)}}{n \times n}$ is the mean value of W, $\overline{W'} = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} W'_{(i,j)}}{n \times n}$ is the mean value of W'. The Pearson's Correlation Coefficient value is between -1 and +1. The value close to +1 indicates positive correlated, while close to -1 indicates negative correlated.

5.3 Experimental results

The results of our proposed watermark method will be shown in Section 6.3.1. Results of the stego-image under attacking tests will be shown in Section 6.3.2. We used geometric attacks and non-geometric attacks (such as cropping, sharp, Gaussian noise, Gaussian blur, contract adjustment, histogram equalization, rescaling (512→256→512), mosaic (2 pixels), waveform and fisheye). The DDWT method watermark W_{DDWT} and the SVD method watermark W_{SVD} extracted from attacked images will be shown in Section 6.3.2. We analyses the quality of attacked images and extracted watermarks in Section 6.4.

5.3.1 The watermark embedding and extracting results

We embed and extract watermarks by the proposed scheme. After the watermark embedding process, we obtain a stego-image with high image quality (PSNR = 43.616) in Fig. 10(a). After the watermark extracting process, we obtain the DDWT watermark, $W_{DDWT,}$ and the SVD watermark, $W_{SVD,}$ shown in Fig. 10(b) and Fig. 10(c), respectively.

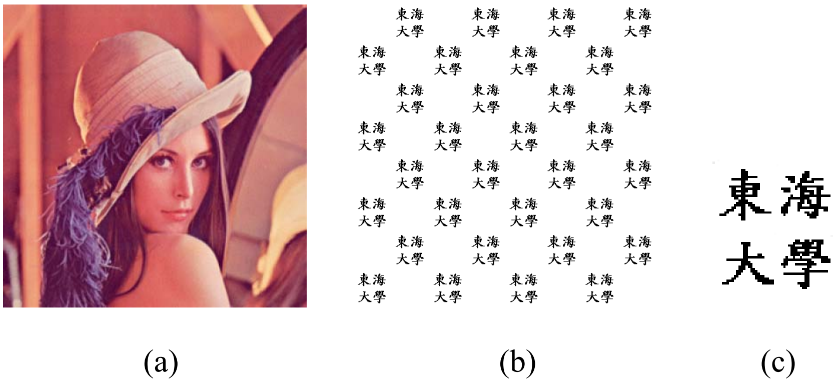


Figure 10. The original results (a) The stego-image Lena (b) The extracted watermark W_{DDWT} (c) The extracted watermark W_{SVD}.

5.3.2 Attacked image and extracted watermark

Attacking tests had been done by using Adobe Photo Shop CS version 8.0. Our image attacks include geometric attacks and non-geometric attacks (such as cropping, sharp, Gaussian noise, Gaussian blur, contract adjustment, histogram equalization, rescaling (512→256→512), mosaic (2 pixels), waveform and fisheye). We will show and analyze results based on attacking methods.

5.3.2.1 Cropping attacks

Cropping attack is one kind of common geometric attacks. The DDWT method is shown very robust to cropping attacks.

Table 1. Cropping attacks:
attacked images, cropping parameter, and image PSNR values

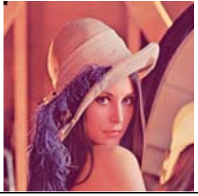
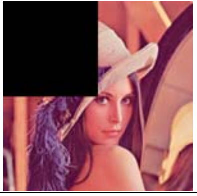
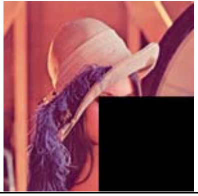
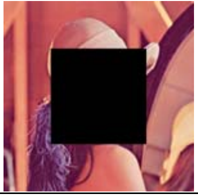
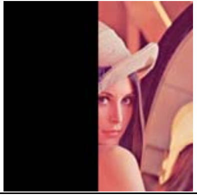
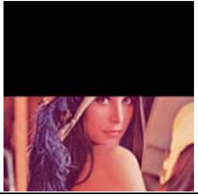
Attacks	**Cropping**		
Parameters	**10×10 pixels**	**25% of upper left corner**	**25% of lower right corner**
Attacked image			
PSNR	34.72	8.46	8.33
Parameters	**25% of middle**	**50% of right side**	**50% of upper side**
Attacked image			
PSNR	8.96	6.27	5.45

Table 2. Extracted DDWT watermark, W_{DDWT}, from image under cropping attacks, and its Pearson's correlation coefficient value

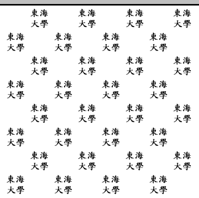
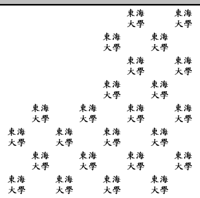
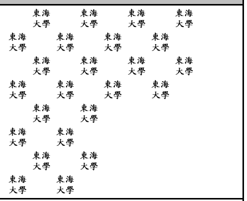
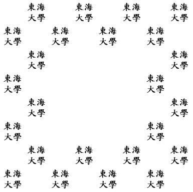
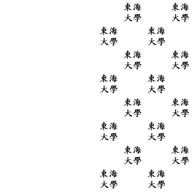
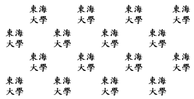
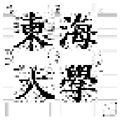
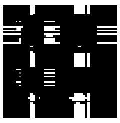
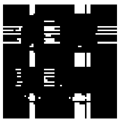
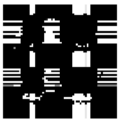
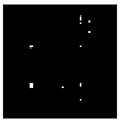
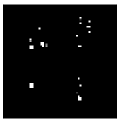
Attacks	**Cropping**		
Parameters	**10×10 pixels**	**25% of upper left corner**	**25% of lower right corner**
W_{DDWT}			
Corr(W,W')	1	1	1
Parameters	**25% of middle**	**50% of right side**	**50% of upper side**
W_{DDWT}			
Corr(W,W')	1	1	1

Table 3. Extracted SVD watermark, W_{SVD}, from image under cropping attacks, and its Pearson's correlation coefficient value

Attacks	**Cropping**		
Parameters	**10×10 pixels**	**25% of upper left corner**	**25% of lower right corner**
W_{SVD}			
Corr(W,W')	0.87	0.09	0.08
Parameters	**25% of middle**	**50% of right side**	**50% of upper side**
W_{SVD}			
Corr(W,W')	0.11	-0.17	-0.23

Cropping is a series attack that might impact the quality of image. The extracted watermarks W_{DDWT} from images under cropping attacks are shown in Table 2. Even after severe image cropping attacks, the extracted watermark, $W_{DDWT,}$ still shows very robust and can be identified with the original watermark.

5.3.2.2 Rotation attacks

Rotation attacks use clockwise direction to rotate images. The rotation attacks have rotation angle from 1° to 30°.

Table 4. Rotation attacks:

attacked images, rotation parameter, and image PSNR values

Attacks	**Rotation (Clockwise direction)**		
Parameters	**1°**	**3 °**	**5 °**
Attacked image			
PSNR	19.69	15.34	13.87
Parameters	**15 °**	**30°**	
Attacked image			
PSNR	11.42	10.35	

Table 5. Extracted DDWT watermark, W_{DDWT}, from images under rotation attacks, and its Pearson’s correlation coefficient value

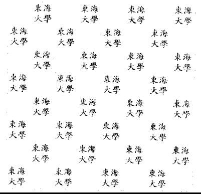
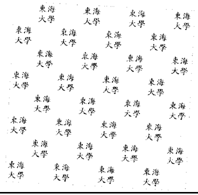
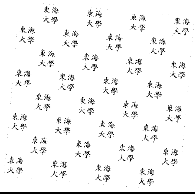
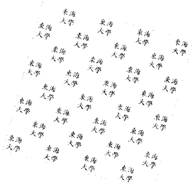
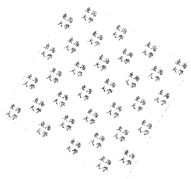
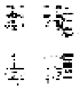
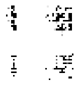
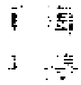
Attacks	**Rotation (Clockwise direction)**		
Parameters	**1°**	**3 °**	**5 °**
W_{DDWT}			
Corr(W,W’)	0.60	0.47	0.63
Parameters	**15 °**	**30°**	
W_{DDWT}			
Corr(W,W’)	0.47	0.21	

Table 6. Extracted SVD watermark, W_{SVD}, from images under rotation attacks, and its Pearson’s correlation coefficient value

Attacks	**Rotation (Clockwise direction)**		
Parameters	**1°**	**3 °**	**5 °**
W_{SVD}			
Corr(W,W’)	0.44	0.44	0.44
Parameters	**15 °**	**30°**	
W_{SVD}			
Corr(W,W’)	0.17	NaN	

From results shown in Table 5 and Table 6, we find that the DDWT watermark, W_{DDWT} is very robust against rotation attacks while the SVD watermark, $W_{SVD,}$ is vulnerable to rotation attacks. After 30 degree rotation, one can hardly extract any embedded watermark information.

5.3.2.3 Sharp attacks

We attack the stego-image with sharpening attacks of intensity from 10% to 80% and 9.4 numbers of pixels. The stego-images after sharpening attacks are shown in Table 7. The extracted DDWT watermarks, W_{DDWT}, and SVD watermarks, W_{SVD}, after sharpening attacks are shown in Table 8 and Table 9, respectively. The extracted watermarks, whether embedded by the DDWT method or SVD method, show robust against sharpening attacks.

Table 7. Sharp attacks:

attacked images, sharpening parameter, and image PSNR values

Attacks	**Sharp**		
Parameters	**10%**	**20%**	**30%**
Attacked image			
PSNR	38.97	34.59	31.65
Parameters	**50%**	**80%**	
Attacked image			
PSNR	27.66	23.97	

Table 8. The DDWT watermark extracted from images after sharpening attacks and its Pearson's correlation coefficient

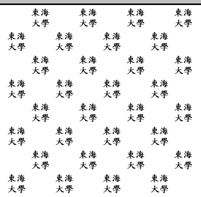
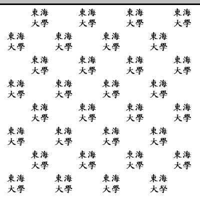
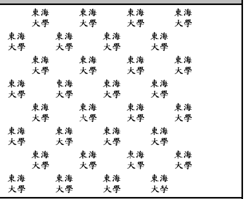
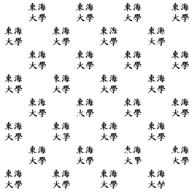
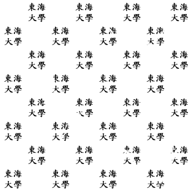
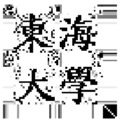
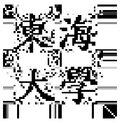
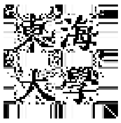
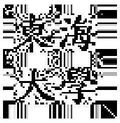
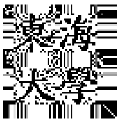
Attacks	Sharp		
Parameters	**10%**	**20%**	**30%**
W_{DDWT}			
Corr(W,W')	1	1	1
Parameters	**50%**	**80%**	
W_{DDWT}			
Corr(W,W')	1	0.99	

Table 9. The SVD watermark extracted from images after sharpening attacks and its Pearson's correlation coefficient value

Attacks	Sharp		
Parameters	**10%**	**20%**	**30%**
W_{SVD}			
Corr(W,W')	0.74	0.62	0.57
Parameters	**50%**	**80%**	
W_{SVD}			
Corr(W,W')	0.48	0.47	

5.3.2.4 Gaussian noise attacks

Gaussian noise attacks mean to add Gaussian noise into the image. In the attacking tests, we added 0.1% to 1% total pixels numbers in the stego-image. The stego-images after Gaussian noise attacks are shown in Ttable 10. The extracted DDWT watermarks, W_{DDWT}, and SVD watermarks, W_{SVD}, after Gaussian noise attacks are shown in Table 11 and Table 12, respectively. The experimental results show that the SVD watermark is robust against Gaussian noise attacks, while the DDWT watermark is vulnerable to Gaussian noise attacks. The Pearson's correlation coefficient of the DDWT watermark decrease sharply for images added with 1% total pixels numbers of Gaussian noise.

Table 10. Gaussian noise attacks:

attacked images, Gaussian noise parameter, and image PSNR values

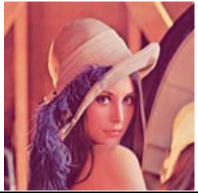
Attacks	**Gaussian Noise**		
Parameters	**0.1%**	**0.3%**	**0.5%**
Attacked image			
PSNR	43.61	42.82	42.77
Parameters	**0.8%**	**1%**	
Attacked image			
PSNR	39.35	37.75	

Table 11. Extracted DDWT watermark from images under Gaussian noise attacks and its Pearson’s correlation coefficient

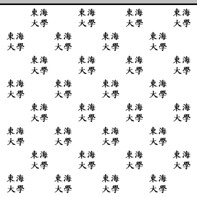
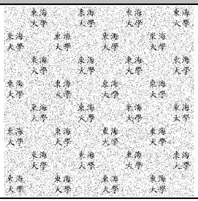
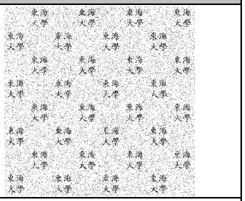
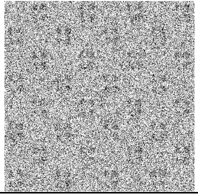
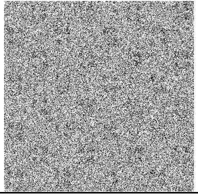
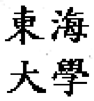
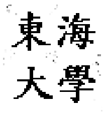
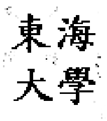
Attacks	**Gaussian Noise**		
Parameters	**0.1%**	**0.3%**	**0.5%**
W_{DDWT}			
Corr(W,W’)	1	0.59	0.55
Parameters	**0.8%**	**1%**	
W_{DDWT}			
Corr(W,W’)	0.19	0.15	

Table 12. Extracted SVD watermark from images under Gaussian noise attacks and its Pearson’s correlation coefficient value

Attacks	**Gaussian Noise**		
Parameters	**0.1%**	**0.3%**	**0.5%**
W_{SVD}			
Corr(W,W’)	0.99	0.99	0.99
Parameters	**0.8%**	**1%**	
W_{SVD}			
Corr(W,W’)	0.99	0.99	

5.3.2.5 Gaussian blurs attacks

We attacked the stego-image by using Gaussian blurs with intensity from 0.1 to 1 numbers of pixels. The stego-images after Gaussian blur attacks are shown in Table 13. The extracted DDWT watermarks, W_{DDWT}, and SVD watermarks, W_{SVD}, after Gaussian blur attacks are shown in Table 14 and Table 15, respectively. From the experimental results, we find that the DDWT watermark is more robust than the SVD watermark. One can still identify the DDWT watermark extracted from stego-images under Gaussian blur with intensity of 1 pixel value, while one cannot tell the identity of the blurry SVD watermark extracted from image under the same intensity of Gaussian blur attacks.

Table 13. Gaussian blur attacks:

attacked images, Gaussian blur parameter, and image PSNR values

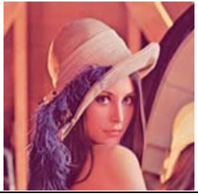
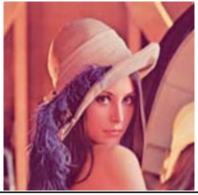
Attacks	**Gaussian Blur**		
Parameters	**0.1**	**0.3**	**0.5**
Attacked image			
PSNR	43.61	37.20	34.30
Parameters	**0.8**	**1**	
Attacked image			
PSNR	32.52	31.56	

Table 14. Extracted DDWT watermark from images under Gaussian blur attacks and its Pearson's correlation coefficient

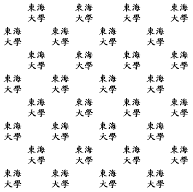
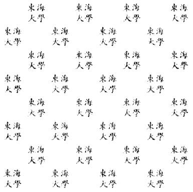
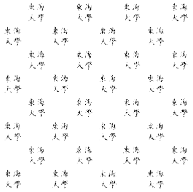
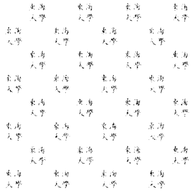
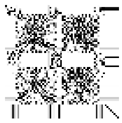
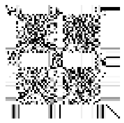
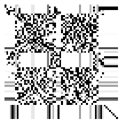
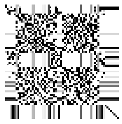
Attacks	Gaussian Blur		
Parameters	**0.1**	**0.3**	**0.5**
W_{DDWT}			
Corr(W,W')	1	0.83	0.73
Parameters	**0.8**	**1**	
W_{DDWT}			
Corr(W,W')	0.57	0.43	

Table 15. Extracted SVD watermark from images under Gaussian blur attacks and its its Pearson's correlation coefficient value

Attacks	Gaussian Blur		
Parameters	**0.1**	**0.3**	**0.5**
W_{SVD}			
Corr(W,W')	0.99	0.26	0.15
Parameters	**0.8**	**1**	
W_{SVD}			
Corr(W,W')	0.04	-0.004	

5.3.2.6 Contrast adjustment attacks

We adjusted the contrast of the foreground and background of image to attack the stego-image, the contrast parameter is adjusted from -40 to +80. The stego-images after contrast adjustment attacks are shown in Table 16. The extracted DDWT watermarks, W_{DDWT}, and SVD watermarks, W_{SVD}, after contrast adjustment attacks are shown in Table 17 and Table 18, respectively. The experimental results show that the SVD watermark is robust against contrast adjustment attacks. The negative contrast adjustment attacks will result in negatively correlated relationship between the extracted SVD watermark and the original watermark, but identity of the extracted SVD watermark is obvious. The positive contrast adjustment (80%) damages the DDWT watermark (Corr = 0.69) more seriously than the SVD watermark (Corr = 0.95).

Table 16. Contrast Adjustment attacks:

attacked images, contrast adjustment parameter, and image PSNR values

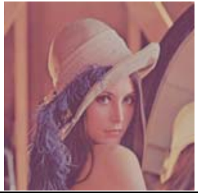
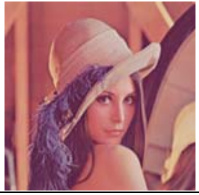
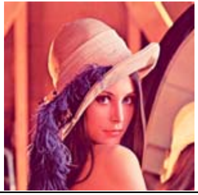
Attacks	**Contrast Adjustment**		
Parameters	**-40**	**-20**	**20**
Attacked image			
PSNR	18.98	25.45	22.73
Parameters	**40**	**60**	**80**
Attacked image			
PSNR	17.43	14.56	12.39

Table 17. Extracted DDWT watermark from images under contrast adjustment attacks and its Pearson's correlation coefficient

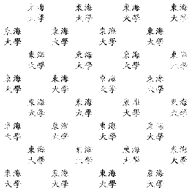
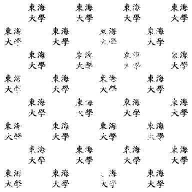
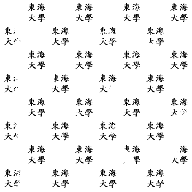
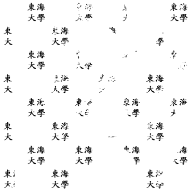
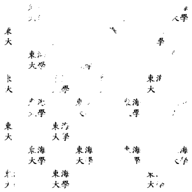
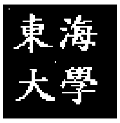
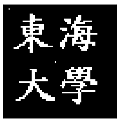
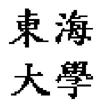
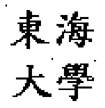
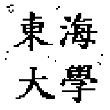
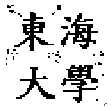
Attacks	**Contrast Adjustment**		
Parameters	**-40**	**-20**	**20**
W_{DDWT}			
Corr(W,W')	0.94	1	1
Parameters	**40**	**60**	**80**
W_{DDWT}			
Corr(W,W')	1	0.97	0.69

Table 18. Extracted SVD watermark from images under contrast adjustment attacks and its Pearson's correlation coefficient value

Attacks	**Contrast Adjustment**		
Parameters	**-40**	**-20**	**20**
W_{SVD}			
Corr(W,W')	-0.99	-0.99	0.99
Parameters	**40**	**60**	**80**
W_{SVD}			
Corr(W,W')	0.99	0.98	0.94

5.3.2.7 Special attacks

Special image attacks in our experiments include Histogram Equalization, Rescale, Mosaic, Waveform, and Fisheye. We utilized the auto functioin provide by Photoshop to do the histogram equalization. The rescaling attacks was done by rescaling the 512x512 image to 256x256 image first, and then rescaling it back to a size of 512x512 again. The mosaic effect was done by forming mosaic square by 2 pixels. The waveform attacks were done by distort the stego-image with 5 waveforms. The fisheye attacks were generated by using the auto function provided by Photoshop to produce a distorted image area as a round circle. The stego-images after special attacks are shown in Table 19. The extracted DDWT watermarks, W_{DDWT}, and SVD watermarks, W_{SVD}, after special attacks are shown in Table 20 and Table 21, respectively. From the experimental results, we observe that

- The experimental results show that both DDWT and SVD watermarks are robust against the histogram attacks.
- The rescaling attacks decrease the quality of both kinds of watermarks, but the identity of the watermark is still discernible.
- The SVD watermark is very robust against mosaic attacks, while the DDWT watermark is degraded but still discernible.
- The waveform attacks degrade the DDWT watermark, but the watermark is still identifiable. The waveform attacks severely damages the SVD watermark.
- The fisheye effect attacks distort the stego-image, but keep intact some of the DDWT watermarks (Corr = 1). The fisheye effect attacks blot out information of the SVD watermark.

Table 19. Special attacks:

attacked images, attacking method and parameter, and image PSNR values

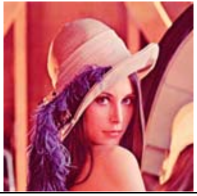
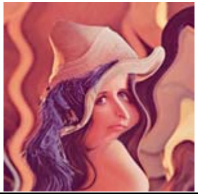
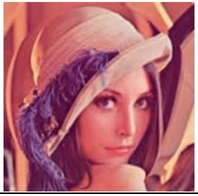
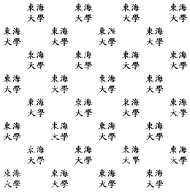
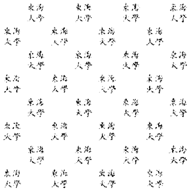
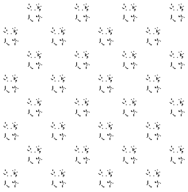
Attacks	**Histogram Equalization**	**Rescale**	**Mosaic**
Parameters	**Auto**	**512→256→512**	**2**
Attacked image			
PSNR	24.02	32.63	43.67
Attacks	**Waveform**	**FishEye**	
Parameters	**Auto**	**Auto**	
Attacked image			
PSNR	15.97	13.98	

Table 20. Extracted DDWT watermark from images under special attacks and its Pearson's correlation coefficient

Attacks	**Histogram Equalization**	**Rescale**	**Mosaic**
Parameters	**Auto**	**512→256→512**	**2**
W_{DDWT}			
Corr(W,W')	1	0.58	0.52

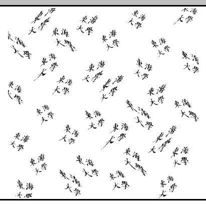
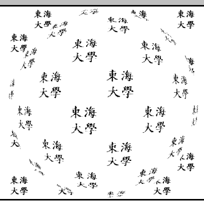
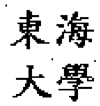
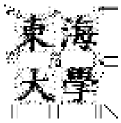
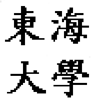
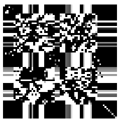
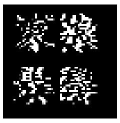
Attacks	**Waveform**	**FishEye**	
Parameters	**Auto**	**Auto**	
W_{DDWT}			
Corr(W,W’)		1	

Table 21. Extracted SVD watermark from images under special attacks and its Pearson’s correlation coefficient value

Attacks	**Histogram Equalization**	**Rescale**	**Masaic**
Parameters	**Auto**	**512→256→512**	**2**
W_{SVD}			
Corr(W,W’)	0.98	0.76	0.99
Attacks	**Waveform**	**FishEye**	
Parameters	**Auto**	**Auto**	
W_{SVD}			
Corr(W,W’)	0.08	0.03	

5.4 Quality analyses of attacked images and extracted watermarks

5.4.1 PSNR of attacked images

Fig. 11 shows the PSNR values of the stego-image after image attacks. We observe a low value of PSNR after cropping, rotation, Gaussian blur, contract adjustment, waveform, fisheye, and histogram equalization attacks, and a high value of PSNR after sharpening, Gaussian noise, rescale, and mosaic attacks. A high PSNR value just indicates high visual quality of the attacked stego-image to the original cover image, and the PSNR cannot be used to estimate the intactness of the embedded watermark information.

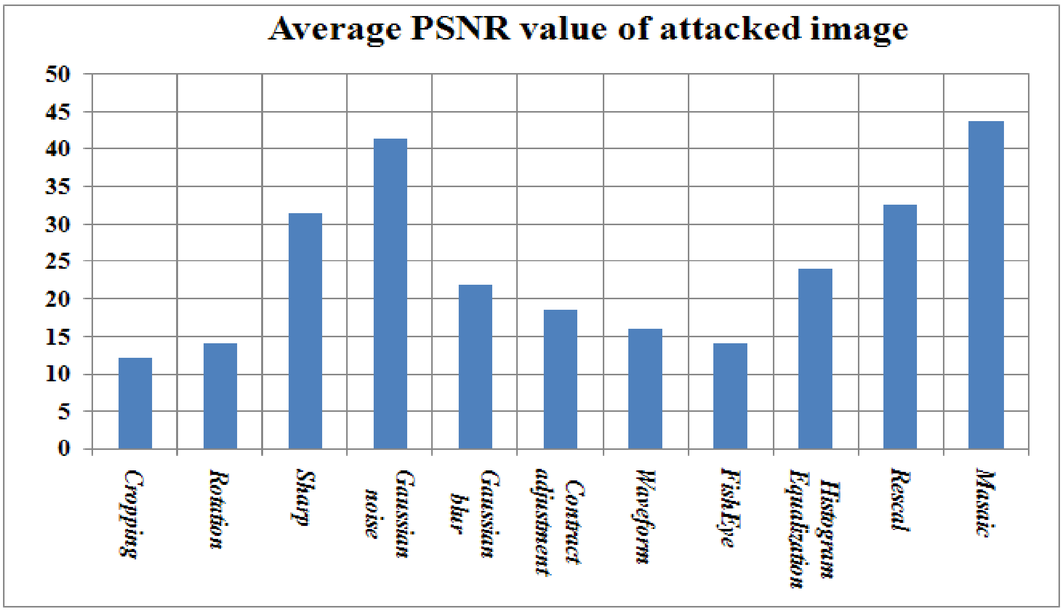


Figure 11. Average PSNR value of attacked image

5.4.2 Pearson's correlation coefficient of extracted DDWT watermarks

Fig. 12 shows the average value of the Pearson's correlation coefficient of DDWT watermark.

We observe that extracted DDWT watermarks from stego-images after attacks have good average Pearson's correlation coefficient. All of them have a mean correlation value around 0.5 or higher, and some of them even have a mean correlation value very close to 1. The DDWT watermark shows very robust against most kind of attacks. Most of the extracted DDWT watermarks are identifiable.

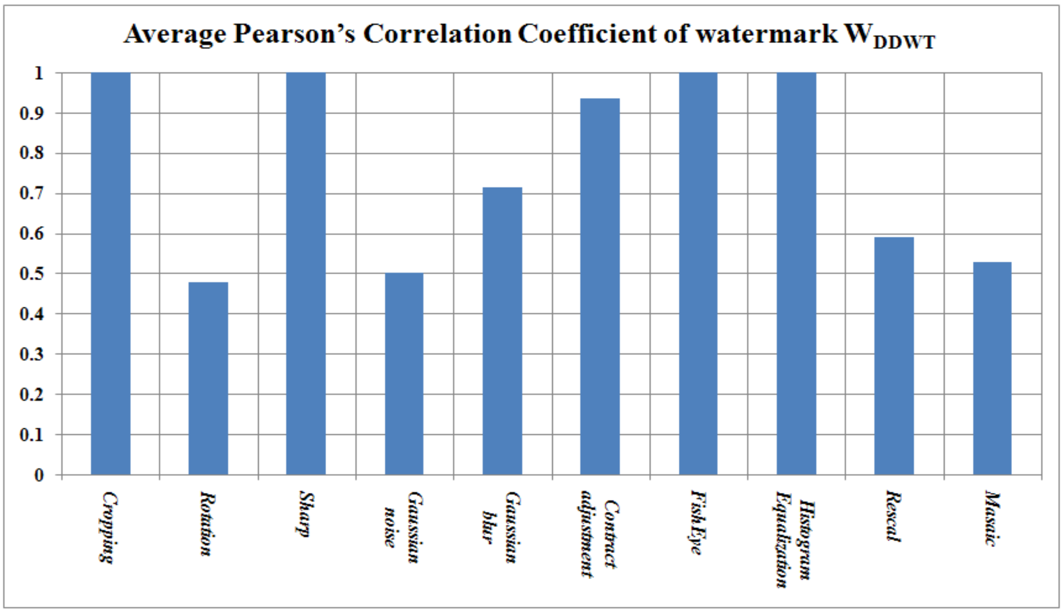


Figure 12. Average Pearson's correlation coefficient of DDWT watermarks

5.4.3 Pearson's correlation coefficient of extracted SVD watermarks

Fig. 13 shows the average value of the Pearson's correlation coefficient of SVD watermark.

We observe very low mean values of the Pearson's correlation coefficient of extracted SVD watermarks from the stego-image under cropping, rotation, Gaussian blur, waveform, and fisheye attacks, and high mean values of the Pearson's correlation coefficient from the other attacks. It shows that the SVD watermark method is robust against many attacks but its robustness can be enhanced by combining it with other watermark method, which is already done in our proposed watermark method.

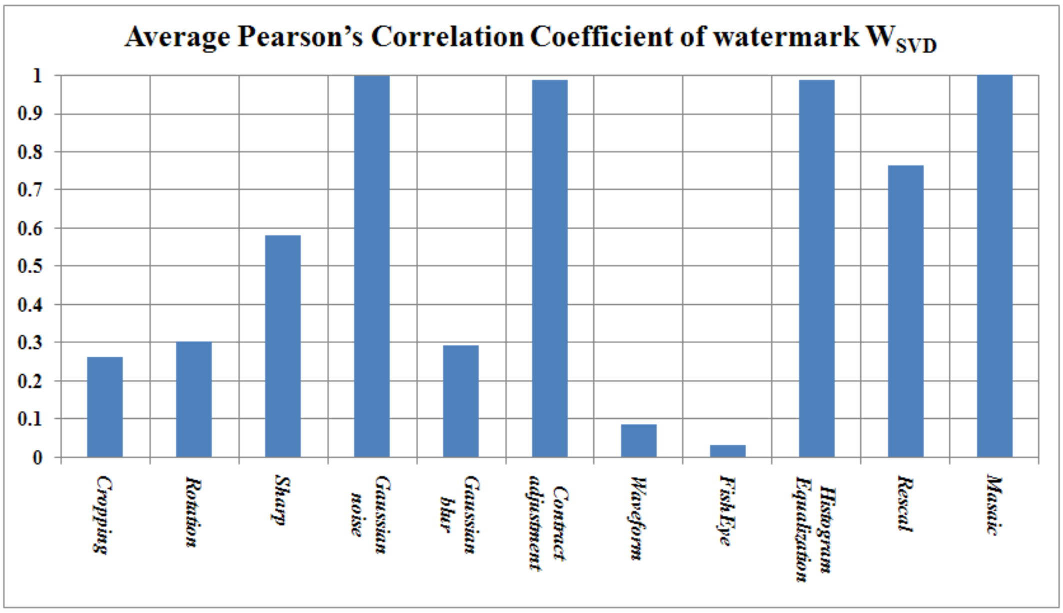


Figure 13. Average Pearson's correlation coefficient of SVD watermarks

Chapter 6
Conclusions

We propose a novel watermark scheme that is very robust and is capable to provide copyright protection. To improve the requirements of watermark security, we successfully take advantage of the merits of Distributed Discrete Wavelet Transformation (DDWT) and Singular Value Decomposition (SVD) watermarking techniques. Although the SVD-based watermark method alone is not efficient against some geometric and non-geometric attacks, and the DDWT-based watermark method alone is not efficient against the other geometric and non-geometric attacks. Our scheme solves problems the disadvantage of DDWT-based and the SVD-based watermark technologies by seamlessly combining the DDWT and SVD methods. The DDWT method enhances robust against attacks such as cropping and rotation attacks. The SVD method enhances robust against other geometric attacks (such as contrast adjustment and histogram equalization) and other non-geometric attacks (such as rescaling).

The robustness of our watermark scheme has been experimentally verified. That it can resist both common geometry and non-geometry attacks such as cropping, rotation, sharp, Gaussian noise, Gaussian blur, contrast adjustment, waveform, fisheye, histogram equalization and rescale. Experimental results show that our scheme is robust and so it can effectively offer copyright protection for legal owners.

Bibliography

[1] H. C. Andrews and C. L. Patterson,“ Singular Value Decomposition (SVD) Image Coding,” IEEE Transactions on Communications, April 1976, pp.425-432.

[2] C. H. Lin, J. S. Jen, and L. C. Kuo, “Distributed Discrete Wavelet Transformation for Copyright Protection,” *The 7th International Workshop on Image Analysis for Multimedia Interactive Services*, Incheon Korea, April 19-21 2006, pp.53-56.

[3] Jung-Chun Liu; Chu-Hsing Lin; Li-Ching Kuo, “A Robust Full-Band Image Watermarking Scheme,**”** The 10th IEEE Singapore International Conference on Communication systems,” Oct. 2006, pp.1 – 5.

[4] Chu-Hsing Lin; Jung-Chun Liu; Chih-Hsiong Shih; Yan-Wei Lee, ”A Robust Watermark Scheme for Copyright Protection,” The International Conference on Multimedia and Ubiquitous Engineering, 24-26 April 2008, pp.132 – 137.

[5] Chu-Hsing Lin, Jung-Chun Liu and Pei-Chen Han, “On the Security of the Full-Band Image Watermark,” *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC2008)*, June 11-13 2008, pp.74-80.

[6] F.A.P Petitcolas; R.J. Anderson; M.G. Kuhn,“Information hiding-a survey,” Proceedings of the IEEE ,Volume 87, Issue 7, July 1999 Page(s):1062 – 1078.

[7] B. Pfitzmann, “Information Hiding Terminology,” *The First Workshop of Information Hiding*, Lecture Notes in Computer Science, Cambridge UK, Vol.1174, May30-June1, 1996, pp 347-350.

[8] K. Dabeer, U. Sullivan, S. Madhow, Chandrasekaran, and B.S. Manjunath “Detection of Hiding in the Least Significant Bit,” *IEEE Transactions on Signal Processing* ,Vol. 52, Issue 10, Part 2, October 2004, pp.3046-3058.

[9] R. Chandramouli. and N. Memon, “Analysis of LSB Based Image Steganography Techniques,” *International Conference on Image Processing*,

Vol. 3, October 7-10, 2001, pp.1019-1022.

[10] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, “Lossless Generalized-LSB Data Embedding,” *IEEE Transactions on Image Processing*, Vol. 14, Issue 2, February 2005, pp.253-266.

[11] N. Cvejic, and T. Seppanen, “Increasing Robustness of LSB Audio Steganography Using A Novel Embedding Method,” *International Conference on Information Technology: Coding and Computing(ITCC 2004)*, Vol. 2, 2004, pp. 533 - 537.

[12] H. C. Wu, N. I. Wu, C. S. Tsai,and M. S. Hwang, “Image Steganographic Scheme Based on Pixel-value Differencing and LSB Replacement Methods,” *IEE Proceedings-Vision, Image and Signal Processing*, Vol. 152, Issue 5, Octobers 2005, pp.611 - 615.

[13] E. Koch and J. Zhao, “Toward Robust and Hidden Image Copyright Labeling,” *IEEE Workshop Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, June 1995, pp. 452–455.

[14] R.A. Gopinath and C.S. Burrus, “Efficient Computation of the Wavelet Transforms,” *International Conference on Acoustics, Speech, and Signal Processing (ICASSP 1990)*, Vol.3, 1990, pp.1599-1601.

[15] I. Daubechies, “The Wavelet Transform: a Method for Time-Frequency Localization,” *IEEE Transactions on Information Theory*, Vol. 36, September 1990, pp. 961–1005.

[16] M. Vetterli and C. Herley, “Wavelet and Filter Banks: Theory and Design,” *IEEE Transactions on Signal Processing*, Vol. 40, No.9, September 1992, pp.2207-2229.

[17] R. S. Stankovic and B. J. Falkowski, “The Haar Wavelet Transform: Its Status and Achievements,” *Computers and Electrical Engineering*, Vol. 29, No. 1, Netherlands, January 2003, pp. 25-44.

[18] Q. Jin, K.M. Wong, and Z. Q. Luo, “Design of an Optimum Wavelet for Cancellation of Long Echoes in Telephone,” *IEEE-SP International Symposium*

on Time-Frequency and Time-Scale Analysis, Philadelphia PA, October 1994, pp.488-491.

[19] S.G. Mallat, “A Theory for Multiresolution Signal Decomposition: The Wavelet Representation,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 11, No. 7, July 1989, pp. 674-693.

[20] V. V. F. Guzman, M. N. Miyatake,and H. M. H. Meana, “Analysis of a Wavelet-based Watermarking Algorithm,” *The 14th International Conference on Electronics, Communications and Computers (CONIELECOMP 2004)*, 16-18 Feb. 2004, pp.283-287.

[21] S. Wang, D. Zheng, J. Zhao, W. J. Tam, and F. Speranza, “A Digital Watermarking and Perceptual Model Based Video Quality Measurement,” *IEEE Instrumentation and Measurement Technology Conference (IMTC 2005)*, Vol. 3, 16-19 May 2005, pp. 1729-1734.

[22] Y. J. Wu and S. himamoto, “A Study on DWT-Based Digital Audio Watermarking for Mobile Ad Hoc Network,” *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Vol. 2, 05-07 June 2006, pp. 247-251.

[23] M. Antonini, M. Barlaud, P. Mathieu and I. Daubechies, “Image Coding Using Wavelet Transform,” *IEEE Transactions on Image Processing*, Vol. 1, No. 2, April 1992, pp. 205-220.

[24] M.Craizer, E. A. B. D. Silva, and E. G.Ramos, “Convergent Algorithms for Successive Approximation Vector Quantization with Applications to Wavelet Image Compression,” *IEE on Image and Signal Processing*, Vol. 146, No.3, June 1999, pp. 159-164.

[25] A. Munteanu, J. Cornelis, G. Van der Auwera and P. Cristea, "Wavelet Image Compression - The Quadtree Coding Approach," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 3, 1999, pp. 176-185.

[26] J.M. Shapiro, “Embedded Image Coding Using Zerotrees of Wavelet Coefficients,” *IEEE Transactions on Signal Processing*, Vol. 41, December 1993, pp. 3445–3463.

[27] H. C. Andrews and C. L. Patterson, “Singular Value Decomposition (SVD) Image Coding,” *IEEE Transactions on Communications*, April 1976, pp.425-432.

[28] N. Garguir, “Comparative Performance of SVD and Adaptive Cosine Transform in Coding Images,” *IEEE Transactions on Communications*, August 1979, pp. 1230-1234.

[29] D. P. O. Leary and S. Peleg, “Digital Image Compression by Outer Product Expansion,” *IEEE Transactions on Communications*, March 1983, pp. 441-444.

[30] C. P. Soo, J. H. Chang, and J. J. Ding, “Quaternion Matrix Singular Value Decomposition and Its Applications for Color Image Processing,” *International Conference on Image Processing (CIP 2003)*, Vol.1, Sept. 14-17, 2003, pp. I-805-I-808.

[31] K. Inoue and K. Urahama, “DSVD: A Tensor-based Image Compression and Recognition Method,” *IEEE International Symposium on Circuits and System (ISCAS 2005)*, Vol. 6, 23-26 May, 2005, pp.6308-6311.

[32] M. Tian, S. W. Luo, and L. Z. Liao, “An Investigation into Using Singular Value Decomposition as A Method of Image Compression,” *International Conference on Machine Learning and Cybernetics*, Vol. 8, 18-21 Aug., 2005, pp.5200-5204.

[33] R. Liu and T. Tan, “An SVD-based Watermarking Scheme for Protecting Rightful Ownership” *IEEE Transactions on Multimedia*, Vol.4, Issue 1, March 2002, pp.121-128.

[34] X. Tang, L. Yang, H. Yue, and Z. Yin, “A Watermarking Algorithm Based on the SVD and Hadamard Transform,” *International Conference on Communications, Circuits and Systems*, Vol. 2, May 27-30, 2005, pp.877.

[35] S. Lee, D. Jang, and C. D. Yoo, “An SVD-Based Watermarking Method for Image Content Authentication with Improved Security,” *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005)*, Vol.2, March 18-23, 2005, pp.525-528.

[36] L. Ma,C. Li, and S. Song, “Digital Watermarking of Spectral Images Using SVD in PCA-Transform Domain,” *IEEE International Symposium on Communications and Information Technology (ISCIT 2005)*, Vol. 2, Oct. 12-14, 2005, pp. 1489-1492.

[37] H. Ozer and B. Sankur, “An SVD Based Audio Watermarking Technique,” *IEEE 13th on Signal Processing and Communications Applications Conference*, May 16-18, 2005, pp. 452-455.

[38] K. Konstantinides and G. S. Yovanof, “Improved Compression Performance Using SVD-Based Filters for Still Images,” *The Society for Imaging Science and Technology (IS&T)/ the International Society for Optical Engineering(SPIE)*, Vol. 2418, San Jose, CA, February 7-8, 1995, pp. 100-106.

[39] T. B. Deng and Y. Nakagawa, “SVD-based Design and New Structures for Variable Fractional-delay Digital Filters,” *IEEE Transactions on Signal Processing*, Vol. 52, Issue 9, Sept. 2004, pp.2513-2527.

[40] S. Redif and T. Cooper, “Paraunitary Filter Bank Design via a Polynomial Singular-Value Decomposition,” *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005)*, Vol. 4, 18-23 March, 2005, pp. iv/613 - iv/616.

[41] R. Karkarala and P. O. Ogunbona, “Signal Analysis Using a Multiresolution Form of the Singular Value Decomposition,” *IEEE Transactions on Image Processing*, Vol. 10, Issue 5, May 2001, pp. 724-735.

[42] T. B. Deng, “Variable Fractional-Delay Filter Design Using Weighted-Least-Squares Singular-Value-Decomposition,” *The 7th International Conference on Signal Processing (ICSP 2004)*, Vol. 1, Aug. 31 –Sept. 4, 2004, pp.54-57.

[43] M. G. Vozalis and K. G. Margaritis, “Applying SVD on Item-Based Filtering,” *The 5th International Conference on Intelligent Systems Design and Applications (ISDA 2005)*, 8-10 Sept., 2005, pp.464-469.

[44] K. Konstantinides, B. Natarajan, G. S. Yovanof, “Noise Estimation and Filtering Using Block-Based Singular Value Decomposition,” *IEEE Transactions on*

Image Processing, Vol.6, Issue 3, March 1997, pp.479 - 483.

[45] E. Ganic and A. M. Eskicioglu, “Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies,” *ACM Multimedia and Security Workshop 2004*, Magdeburg Germany, September 20-21, 2004, pp. 166-174.