A Robust and Removable Watermarking Scheme Using Singular Value Decomposition

Ya-Feng Di[1], Chin-Feng Lee[2], Zhi-Hui Wang[1], Chin-Chen Chang[3] and Jianjun Li[4]
[1] School of software, Dalian University of Technology
Dalian, China 116620
[e-mail: wangzhihui1017@gmail.com]
[2] Department of Information Management, Chaoyang University of Technology
Taichung, Taiwan
[e-mail: amylee.cf168@gmail.com]
[3] Department of Information Engineering and Computer Science, Feng Chia University
Taichung, Taiwan
[e-mail: alan3c@gmail.com]
[4] School of Computer Science and Technology, Hangzhou Dianzi University
Hangzhou, China
[e-mail: lijjcan@gmail.com]
*Corresponding author: Zhi-Hui Wang

Received May 23, 2016; revised October 2, 2016; accepted October 24, 2016; published December 31, 2016

Abstract

Digital watermarking techniques are widely applied to protect the integrity and copyright of digital content. In a majority of the literature for watermarking techniques, the watermarked image often causes some distortions after embedding a watermark. For image-quality-concerned users, the distortions from a watermarked image are unacceptable. In this article, we propose a removable watermarking scheme that can restore an original-like image and resist signal-processing attacks to protect the ownership of an image by utilizing the property of singular value decomposition (SVD). The experimental results reveal that the proposed scheme meets the requirements of watermarking robustness, and also reestablishes an image like the original with average PSNR values of 59.07 dB for reconstructed images.

***Keywords*:** Removable watermarking, copyright protection, robust watermark, singular value decomposition (SVD)

http://dx.doi.org/10.3837/tiis.2016.12.008 **ISSN : 1976-7277**

1. Introduction

Digital watermarking is the process of embedding information and is widely employed to protect the integrity and copyright of digital content [1-2]. The owner embeds the ownership or other descriptive information into digital content such as audio [3-4], images [5-8], video [9], etc., which is difficult to remove. Subsequently, an authenticated receiver verifies the source of this digital content by extracting the hidden information. Today, watermarking technology is used in many areas including, but not limited to copyright enforcement, tamper detection, broadcast monitoring and fingerprinting. The requirements of watermarking design depend on the specific needs of the applications. However, some common requirements for the design of watermarks should include satisfying visual fidelity, embedding rate, and robustness against common signal processing attacks, such as cropping, noising and compressing, or malicious processing. There is a dilemma in that watermarking approaches have to sacrifice image quality in order to achieve watermarking robustness. Therefore, demands for watermarking with reversibility has gradually increased for high image quality requirement applications, such as military and medical images. To guarantee the quality of a restored image, a series of removable watermarking schemes that can restore the original image have been proposed.

Removable watermarking approaches derived from reversible data hiding (RDH) schemes [10-15], are characterized by their prominent contribution, which is the ability to extract the hidden information and recover the original image without any distortion. However, although RDH can realize reversible data hiding, these kinds of methods cannot endure against certain attacks, i.e., if the secret-embed image was attacked in some way, the authorized receiver cannot extract the embedded secret information in a lossless way. Since reversible approaches must be manipulated thru pixel computing; image recovery will fail and the embedded image cannot be restored to the original data if pixels have been modified by any image processing. Like reversible approaches, the removable watermarking techniques can embed the watermark into an original image by the owner and then the authenticated receiver can extract the watermark and restore the original-like image with wispy distortion. More importantly, removable watermarking schemes can extract the watermark after suffering various kinds of attacks in a satisfactory way.

Some removable watermarking techniques had been proposed over the past several years. Hu *et al*. [16] proposed a scheme to embed a visible watermark into the host image in a removable way in 2006. However, the scheme did not have good behavior in terms of robustness, that is, it cannot resist heavy attacks. In 2009, Chang *et al*. proposed a removable watermarking scheme [17] that transfers the spatial domain to a frequency domain by DCT transformation, and then proceeds with the removable watermark embedding procedure. The method of Chang *et al*. can recover an original-like image of satisfactory quality and is able to resist malicious attacks. However, Chang *et al.*'s scheme adopts a voting mechanism to guarantee robustness which means the same watermark bit needs to be embedded at least three times. Thus, the visual quality of the restored image will be influenced by this expense. To achieve a watermark approach considering both robustness and high visual quality of the restored images, we propose a removable and

robust watermarking scheme by utilizing the property of singular value decomposition (SVD). The produced singular values are appropriated to embed the watermark and resistant against malicious attacks; therefore, a quantization method on singular values and an exchange mechanism on the quantization residues are designed to embed the watermark bits. The experimental results show the proposed scheme is superior to the scheme of Chang *et al.*, both in the quality of the reconstructed image and robustness to common signal processing attacks.

The rest of the paper is organized as follows. A common matrix transformation method of singular value decomposition (SVD) and a related removable watermarking scheme is elaborated in Section 2. Section 3 demonstrates the proposed scheme. The experimental results and analysis follow in Section 4. Finally, we make conclusions in Section 5.

2. Related Work

In this section, we introduce singular value decomposition (SVD) and the removable and robust watermarking scheme proposed by Chang *et al*.

2.1 SVD

Singular value decomposition (SVD), a factorization of a matrix, is used to analyze matrices in a number of effective numerical analysis tools. By applying a SVD transformation on a matrix, three matrices will be obtained. Suppose A is an $m \times n$ matrix, the singular value decomposition of A is formulized as $A = U \sum V^T$, where U and V^T are orthogonal matrices of which the size are $m \times m$ and $n \times n$, respectively. The most important matrix $\sum$ is an $m \times n$ diagonal matrix, whose diagonal elements are non-negative real numbers. The specific matrix of $\sum$ is shown as follows:

$$\sum = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & \cdots & 0 \\ 0 & 0 & \sigma_r & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where the singular values satisfy $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0, \sigma_{r+1} = \cdots = 0$ and $r = \text{rank}\,(A)$.

The properties of SVD transformation provide benefits that can be applied in digital image processing. First, the original matrix can be square or rectangle; that is, the SVD transformation is suitable for any image whose height and weight are not equal. Second, the singular values in D matrix of a digital image are embedded watermark bits for accomplishing the robustness of the inserted watermark. The changes of singular values are not quite significant if the image is performed through typical image processing operations. Moreover, these small changes in the singular values after a watermark is inserted would not perceptually affect an image. Due to its character, there are plenty of watermarking

schemes applying this technique in recent years. Zheng *et al.* proposed a blind watermarking scheme by applying SVD and a least squares support vector machine [18]. Guo *et al.* embedded the principal component of the watermark into the host image using a spread spectrum concept [19].

2.2 Chang *et al.* scheme

In 2009, Chang *et al.* [17] proposed a novel watermarking scheme based on pair-difference correlations upon subsampling and the technique of Just Noticeable Distortion (JND) on the DCT domain. Chang *et al.*'s method on the one hand can guarantee the watermarking robustness; and on the other hand, the restored images after watermark has been removed preserve satisfactory visual quality. The Chang *et al.* scheme consists of three phases, a preliminary phase, a low-frequency, and a middle-frequency watermarking phase.

In the preliminary phase, the authors adopted the subsampling method in [20] to obtain four sub-images, O_1, O_2, O_3 and O_4. Then the DCT operation is manipulated on the 8×8 non-overlapping block in each sub-image. Thus four sets of DCT coefficients can be obtained naturally, of which each set represents one sub-image. Last, a sequence of random number pairs $\{(\alpha, \beta)\}$ is generated by a secret key *SK* and the random number pairs are used to choose two blocks from the four DCT-coefficient sets, where α, $\beta \in \{1, 2, 3, 4\}$ and $\alpha \neq \beta$.

The low-frequency watermarking phase mainly obtains exchange records $s, s \in \{0, 1\}$. Specifically, assume the random number pair is (α, β), so two DCT coefficient blocks B_α and B_β can be obtained. Let $B_\alpha(u)$ and $B_\beta(u)$ be the u-th zigzag scan order coefficients corresponding to blocks B_α and B_β, respectively, and w be the watermark bit to be embedded. If $w = 0$ and $B_\alpha(u) \geq B_\beta(u)$, exchange $B_\alpha(u)$ and $B_\beta(u)$ then set $s = 1$; otherwise, set $s = 0$. If $w = 1$ and $B_\alpha(u) < B_\beta(u)$, exchange $B_\alpha(u)$ and $B_\beta(u)$ then set $s = 1$; otherwise, set $s = 0$. Then a simple operation of enhancement between $B_\alpha(u)$ and $B_\beta(u)$ is done.

Due to the middle-frequency watermarking phase, the job is to embed the exchange records in the middle-frequency subband, which is used to restore the modified coefficients in the low-frequency subband. Assume $B_\alpha(v)$ is the v-th zigzag scan ordered coefficient of the block B_α. The embedding method is based on the least significant bit (LSB). Specifically, the exchange records are embedded into the l-th LSB of the coefficient $B_\alpha(v)$, which is represented in a bitstream. To guarantee the robustness of the watermarking scheme, the authors embed each watermark bit into the same block at r times.

An authorized user is permitted to verify the watermark and restore the original-like image with the secret information {*SK*, *u*, *v*, *r*, *l*}. When the user owns all of the secret information, they can extract the watermark and restore the original-like image.

3. Proposed Scheme

This section proposes a robust and removable watermarking scheme exploiting the singular value decomposition (SVD) and introduces the approach in three subsections. The preliminary phase is for preprocessing before watermark embedding, the purpose of which is to generate two block sets. The watermark embedding phase is introduced in the next subsection, and the last subsection describes how to extract the watermark and restore the original-like image.

3.1 Preliminary phase

In the preliminary phase, two sets of blocks are selected for the watermark embedding phase. First, the original image will be divided into non-overlapping blocks of which the size is 8×8. Then, the SVD transformation is applied on each block. According to a comparison between a threshold T_{svd} and the largest singular value of each block, we can obtain an eligible set S from which two sets SA and SB are generated using a private key Key_1. The detailed operations are shown in the following steps:

Step 1. Divide an input image O of size $W\times H$ into non-overlapping 8×8 blocks.

Step 2. Apply the SVD transformation on each block B such that $B=UDV^T$ and obtain a set of eight singular values σ_j from the diagonal matrix D, $j=1,\ 2,\ ...,\ 8$, where the singular value entries satisfy $\sigma_1\geq\sigma_2\geq\cdots\geq\sigma_8$.

Step 3. Let S be a collection of blocks where their first singular values are greater than a predetermined threshold. That is, $S=\{\,B\,|\,\sigma_1\geq T_{svd}\,\}$.

Step 4. Use a private key Key_1 to randomly choose two equal-sized subsets SA and SB from S. The number of blocks in SA is $m\times n$, where $m\times n$ represents the size of watermark image. Similarly, the number of blocks in SB is $m\times n$.

3.2 Watermark embedding phase

After two sets of blocks SA and SB are obtained, this subsection describes how to embed a watermark bit into each block pair which comes from SA and SB, respectively. Let w_i be a watermark bit in an $m\times n$ binary watermark image, such that $w_i\in\{0,\ 1\}$, and $i=1,\ 2,\ ...,\ m\times n$. Assume A_i and B_i are a pair of blocks belonging to the sets of SA and SB, respectively, and a_i and b_i are the first singular values of A_i and B_i, respectively.

Detailed operations of the watermark embedding process are described by the following steps:

Step 1. Compute x_i and y_i by quantizing a_i and b_i, respectively, using the following Equation (1)

$$\begin{cases} x_i = a_i \bmod f \\ y_i = b_i \bmod f \end{cases}, \tag{1}$$

where the factor value f is an adjustable integer that controls robustness and image quality.

Step 2. If $w_i = 0$ and $x_i \geq y_i$, exchange x_i and y_i, then set $r_i = 1$; otherwise, set $r_i = 0$.

If $w_i = 1$ and $x_i < y_i$, exchange x_i and y_i, then set $r_i = 1$; otherwise, set $r_i = 0$.

Step 3. If $|x_i - y_i| < adj$, enlarge the difference between x_i and y_i by the following equation:

$$\text{When } w_i = 0, \begin{cases} y_i = y_i + adj & x_i \leq adj/2, \\ x_i = x_i - adj & \text{if } y_i \geq f - (adj/2), \\ x_i = x_i - (adj/2),\ y_i = y_i + (adj/2) & \text{otherwise,} \end{cases}$$

$$\text{When } w_i = 1, \begin{cases} x_i = x_i + adj & y_i \leq adj/2, \\ y_i = y_i - adj & \text{if } x_i \geq f - (adj/2), \\ x_i = x_i + (adj/2),\ y_i = y_i - (adj/2) & \text{otherwise,} \end{cases} \tag{2}$$

where the adjustment value adj is an adjustable integer that controls robustness and image quality.

Step 4. Compute the new largest singular values a_i' and b_i' according to Equation (3).

$$\begin{cases} a_i' = (a_i - a_i \bmod f) + x_i, \\ b_i' = (b_i - b_i \bmod f) + y_i. \end{cases} \tag{3}$$

Then retrieve the watermarked block by using an inverse SVD transformation.

Step 5. Combine all blocks to obtain image O'.

Step 6. Construct the watermarked image O_w by selecting $m \times n$ pixels from O' with a secret key Key_2 and embed the exchange information r_i using a LSB replacement algorithm.

An instance of watermark embedding is described below. Assume the quantization factor f is 91, where the adjustment value adj is set as 8 and two largest singular values of A_1 and B_1 are a_1 and b_1. For simplicity in notation, we omit the subscript i from further illustrations. In the preliminary phase, two blocks as shown in **Fig. 1**(a) are selected for the watermark embedding phase. Afterwards, apply the SVD transformation on each block to obtain a set of eight singular values from the diagonal matrix as shown in **Fig. 1**(b). $a = 1231$ and $b = 1512$, respectively, represent the largest singular values greater than a predetermined threshold. According to the embedding steps, first apply a modular operation such that the dividends are 1231 and 1512, respectively, and the divisor is 91; namely, "1231 mod 91", which is equal to 48, while "1512 mod 91", which is equal to 56. According to Equation (1), $x = 48$ and $y = 56$. The difference between x and y is $56 - 48 = 8$ which equals the adjustment value adj, so that there is no need to enlarge the

difference. Assume that the to-be-embedded watermark bit is 1. According to Equation (3), compute the new singular values a' and b' again; therefore, $a'=1239$ and $b'=1504$. Finally, set the exchange information r as 1 and the watermarked blocks are obtained by the inverse SVD transformation. **Fig. 1**(c) shows the result after embedding the watermark bit as 1. Otherwise, if the watermark bit is 0, x and y are kept unchanged and set the exchange information r as 0.

157	154	152	149	148	151	150	149
161	157	153	149	150	153	148	145
159	155	153	152	150	150	150	150
158	155	152	153	151	147	147	150
161	156	155	153	152	152	151	151
159	156	156	155	153	152	152	152
165	161	157	158	155	153	152	151
160	161	160	160	161	158	156	155

193	192	192	194	193	190	190	190
191	192	194	194	193	190	190	191
190	191	194	194	192	189	186	187
189	191	192	191	192	189	188	188
186	190	190	189	188	189	186	186
189	189	189	188	187	186	185	186
187	187	187	187	186	185	188	188
186	188	185	184	184	185	187	187

(a) Two blocks of size 8×8

1231	0	0	0	0	0	0	0
0	9	0	0	0	0	0	0
0	0	6	0	0	0	0	0
0	0	0	5	0	0	0	0
0	0	0	0	2	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0

1512	0	0	0	0	0	0	0
0	9	0	0	0	0	0	0
0	0	4	0	0	0	0	0
0	0	0	3	0	0	0	0
0	0	0	0	2	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(b) The diagonal matrixes from SVD transformation on each block of (a)

1239	0	0	0	0	0	0	0
0	8	0	0	0	0	0	0
0	0	6	0	0	0	0	0
0	0	0	5	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

1504	0	0	0	0	0	0	0
0	8	0	0	0	0	0	0
0	0	4	0	0	0	0	0
0	0	0	2	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(c) The results after the third step of watermark embedding procedure

Fig. 1. An example illustrating watermark embedding

3.3 Watermark extraction and image reconstruction phase

An authorized user can confirm the copyright of the watermarked image by extracting the watermark and recover the watermarked image to an original-like image after receiving the watermarked image from the sender. The watermark extracting phase is quite similar to the watermark embedding phase, except that the exchange records of x and y should be obtained before extracting the watermark. Assume the watermarked image is O_w, and exchange records are $r_1, r_2, \ldots, r_{1024}$. . Detailed operations of procedure "watermark extraction and original-like image restoration" is described in the following steps:

Step 1. Select 1024 pixels from O_w by secret key Key_2 and extract the exchange record from the LSB of those pixels to obtain r_i, $i = 1, 2, ..., 1024$.

Step 2. Divide the watermarked image O_w into 8×8 non-overlapping blocks B_m, where $0 \le m \le (W \times H) / 64$.

Step 3. Apply the singular value decomposition on each block B_m such that $B_m = U_m D_m V_m^T$ and obtain singular values σ_j in matrix D_m, $j = 1, 2, ..., 8$.

Step 4. Select blocks whose first singular value σ_1 is greater than T_{svd} and collect them into set S.

Step 5. Choose 1024 blocks of SA and 1024 blocks of SB with secret key Key_1.

Step 6. Let x_i and y_i be the quantized residuals of $a_i \bmod f$ and $b_i \bmod f$, where a_i and b_i are the largest singular values of blocks in SA and SB, respectively, $i = 1, 2, ..., 1024$.

Step 7. Compare x_i and y_i, if $x_i < y_i$ then extracted watermark $w_i = 0$; otherwise, $w_i = 1$.

Step 8. Read the exchange records r_i, if $r_i = 1$, then exchange x_i and y_i, otherwise, keep unchanged.

Step 9. Restore the first singular value a_i and b_i according to Equation (4).

$$\begin{cases} a_i = (a_i - a_i \% f) + x_i, \\ b_i = (b_i - b_i \% f) + y_i. \end{cases} \tag{4}$$

Step 10. Combine all blocks to restore the original-like image.

4. Experimental Results

In this section, we use several simulations to demonstrate the advantages of our proposed method compared with state-of-art schemes. Image visual quality of a watermarked and restored image and the robustness of an extracted watermark are two major requirements for a removable watermarking scheme. In this section, we compare our image quality with the Chang *et al.* [17] scheme and simulated several common signal processing techniques to evaluate the robustness of the proposed scheme. Specifically, we use PSNR (peak signal-to noise ratio) to evaluate the visual quality of the restored image. AR (accuracy rate) is used to assess the robustness of the watermarking scheme. The evaluation of PSNR is

defined as below:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB .$$

The mean square error (MSE) of an image with $W \times H$ pixels is defined as

$$MSE = \frac{1}{W \times H}\sum_{u=1}^{W}\sum_{v=1}^{H}(p_{uv} - p'_{uv})^2 ,$$

where p_{uv} is the original pixel value and p'_{uv} is the pixel value of the shadow image.

The evaluation of AR is defined as below:

$$AR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\overline{w_{ij} \oplus w'_{ij}}}{m \times n} ,$$

where m and n mean the length and width of the watermark image, w_{ij} and w'_{ij} are the value of original watermark bit and extracted watermark bit, respectively.

4.1 Experimental results

To test our proposed scheme and also obtain a comparison with the scheme of Chang *et al*. [17], eight images as used in the Chang *et al*. studies were selected as test images. **Fig. 2** (a1)-(h1) show the eight test images. The corresponding watermarked images are demonstrated in **Fig. 2** (a2)-(h2). **Fig. 2** (a3)-(h3) show the restored images from the watermarked images. The visual quality of each watermarked image is satisfactory and the restored images are almost the same as the original images. From our literature review, there were only a few studies related to "removable" watermarking, and as such we only compare with the Chang *et al*. method [17].

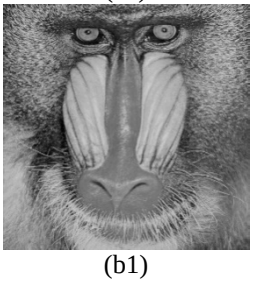
Airplane

(a1)

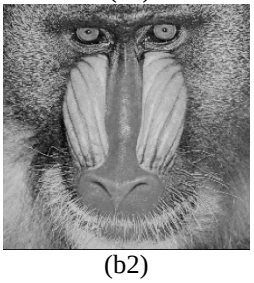
(a2)

(a3)

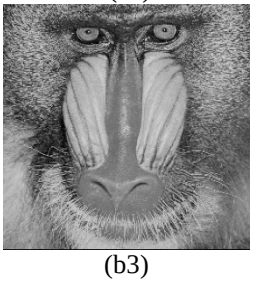
Baboon



(b1)



(b2)



(b3)

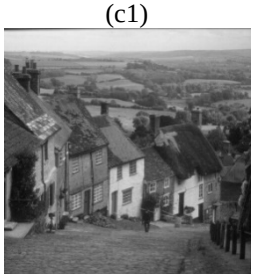
Girl

(c1)

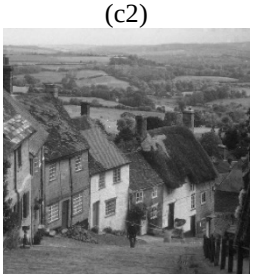
(c2)

(c3)

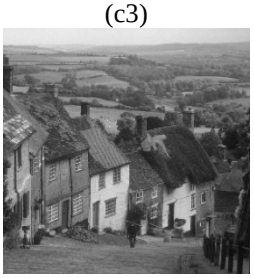
Goldhill



(d1)

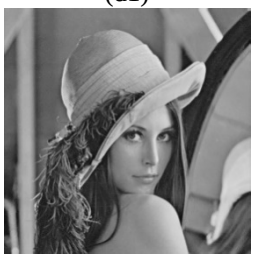


(d2)



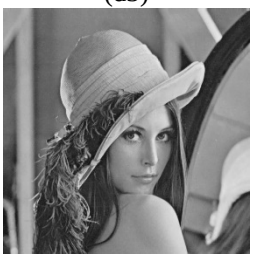
(d3)

Lena



(e1)

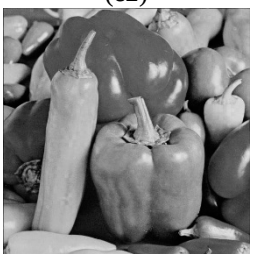
(e2)



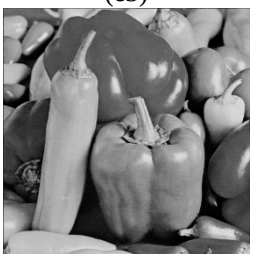
(e3)

Pepper

(f1)



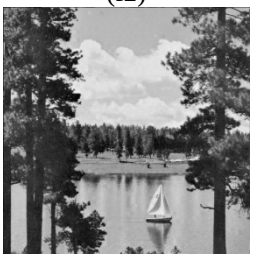
(f2)



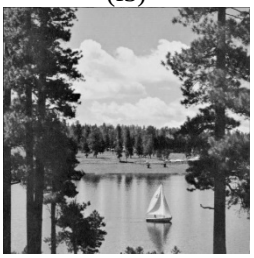
(f3)

Sailboat

(g1)

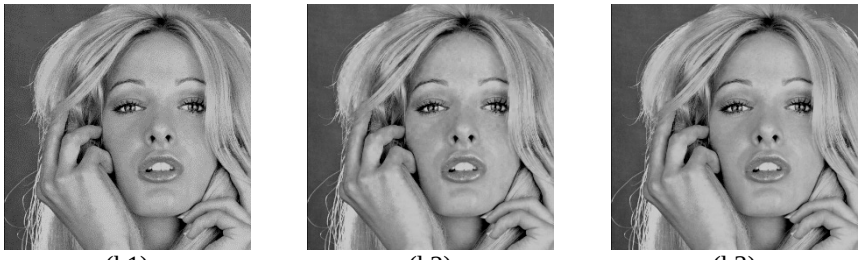


(g2)



(g3)

Tiffany



(h1) (h2) (h3)

Fig. 2. Test images, watermarked images, and restored images

From the watermark embedding phase, we can see that the parameters T_{svd}, f and adj are set to 750, 91 and 8, respectively. **Table 1** shows the PSNR values of watermarked images and restored images compared with the scheme of Chang *et al*. From the table we can see that the PSNR value of each watermarked image is larger than that of Chang *et al*. and the average difference value is more than 2dB. As for the PSNRs for the restored images, almost all PSNRs for the images are larger than that of Chang *et al*.'s method except for Lena, which is a bit smaller. The proposed scheme is about 4.2 dB larger on average than that of Chang *et al*.'s scheme.

Table 1. The image quality of watermarked and restored images (T_{svd} =750)

Test image	Image PSNR (dB)			
	Watermarked		Restored	
	Chang *et al*. [17]	This study	Chang *et al*. [17]	This study
Airplane	40.24	43.56	56.60	57.87
Baboon	35.06	42.51	49.68	59.72
Girl	40.87	43.15	56.36	59.03
Goldhill	41.23	43.21	56.10	58.75
Lena	42.66	42.73	59.88	58.68
Pepper	41.99	42.76	55.37	59.68
Sailboat	39.07	42.29	54.59	58.48
Tiffany	41.81	41.93	50.38	60.36
Average	40.37	42.77	54.87	59.07

In terms of robustness, we tested several well-known signal processing attacks on the watermarked image, such as blurring, noising, sharpening, scaling, changing brightness and contrast, cropping in different percentages and JPEG compressing at different compression degrees. **Fig. 3** shows the attacked watermarked images and corresponding extracted watermarks. From the figure we can see that the proposed scheme has good performance in terms of robustness; that is, our scheme can resist common signal processing attacks. **Table 2** and **Table 3** demonstrate the results compared with the schemes of Chang *et al*. and Lu *et al*. in terms of the PSNR values of the restored original-like image and AR values of the attacked watermark from each specific attack. The tables reveal that the proposed scheme has better performance in terms of the quality of

the restored image as well as in robustness to signal attacks. Moreover, a significant feature deserves mention. Chang *et al.*'s scheme embeds the watermark bits into the same block for five times, i.e., the parameter $r = 5$ while in our proposed scheme, we only embed the watermark bits into the block one time, i.e., $r = 1$. **Table 3** demonstrates that our scheme still has satisfactory performance about robustness compared with that of the scheme by Chang *et al*.

(a) Blurring (b) GaussNoise(3%) (c) Cropping 10% (d) Cropping 20%

(e) Cropping 30% (f) Cropping 40% (g) Cropping 50% (h) Cropping center

(i) JPEG Q = 6 (j) JPEG Q = 8 (k) JPEG Q = 10 (l) Scaling 75%

(m) Scaling 200% (n) Sharpening (o) USM50% (p) White Noise

Fig. 3. Common signal-processing attacks

Table 2. Comparison of *PSNR* after attack by various signal-processing attacks.

Attack	PSNR		
	Lu *et al.* [20]	Chang *et al.* [17]	This study
Blurring (Gaussian 0.5)	38.98	38.83	36.37
Gaussian Noising (3%)	30.13	29.84	30.36
Scaling (75%)	25.28	25.21	35.55
Scaling (200%)	25.64	25.56	36.65
JPEG (Q = 6)	39.62	38.59	41.51
JPEG (Q = 8)	40.04	38.62	41.79
JPEG (Q = 10)	41.66	38.94	42.78
Sharpening	33.55	26.19	34.12
Cropping (10%)	15.29	15.29	15.62
Cropping (20%)	12.39	12.38	12.64
Cropping (30%)	10.58	10.58	10.78
Cropping (40%)	9.41	9.41	9.72
Cropping (50%)	8.34	8.33	8.59
Cropping (60%)	7.36	7.35	7.53

Table 3. Comparison of *AR* after attacks by various signal-processing attacks.

Attack	AR		
	Lu *et al.* [20]	Chang *et al.* [17]	This study
Blurring (Gaussian 0.5)	59.47	90.34	97.56
Gaussian Noising (3%)	80.96	97.95	87.41
Scaling (75%)	66.21	95.90	99.81
Scaling (200%)	89.36	100	99.71
JPEG (Q = 6)	67.38	92.29	99.51
JPEG (Q = 8)	72.26	97.27	100
JPEG (Q = 10)	86.62	100	100
Sharpening	91.40	100	95.7
Cropping (10%)	82.42	95.02	97.85
Cropping (20%)	78.22	87.50	91.9
Cropping (30%)	75.10	81.84	87.01

Cropping (40%)	70.02	76.86	80.57
Cropping (50%)	64.65	72.56	74.51
Cropping (60%)	59.77	66.31	70.02

4.2 Experimental analysis

A. Parameters in the watermark embedding phase

In the watermark embedding phase, the parameters T_{svd}, f and adj are set to 750, 91 and 8, respectively. To test what effect this has on the results, we provide a brief discussion in this subsection. To ensure consistency in the testing, we choose *Lena* as the sample.

For threshold T_{svd}, first, it can control the number of blocks that are used to embed a watermark. For different images, threshold T_{svd} can select a different number of eligible blocks to embed watermark bits. For example, for image *Pepper* and image *Lena*, if T_{svd} is 900, *Lena* has 2096 blocks while *Pepper* only has 1855 blocks, which is not enough to embed the watermark bits in the experiment. As such, threshold T_{svd} needs to be carefully selected in order to allow each image enough eligible blocks to carry the watermark bits. This can also influence the visual quality of a watermarked image and robustness of the watermarking scheme to some degree. We evaluate the performance of the threshold T_{svd} by fixing the other two parameters, set f = 91 and adj = 8. **Fig. 4** demonstrates the effect.

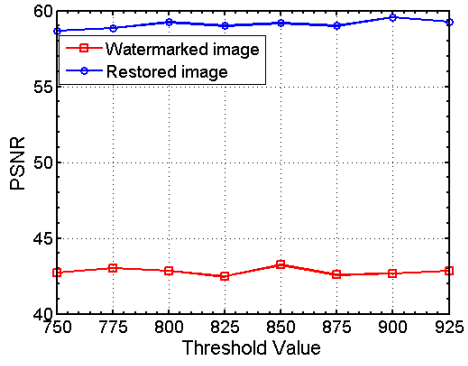


Fig. 4. The effect of threshold T_{svd}

Due to quantization factor f and adjustment value adj, the former can control the range of x and y, while the latter controls robustness and image quality. **Fig. 5** and **Fig. 6** demonstrate the effects, respectively. **Fig. 5** and **Fig. 6** show that different values of f and adj can result in different PSNRs for the watermarked image and restored image, as well as different ARs for the extracted watermark. When threshold value T_{svd} is fixed, finding a best pair for quantization factor f and the adjustment value adj is significant to the experimental results. Therefore, in the watermark embedding phase, f =91 and adj =8 were chosen as the optimal value for the quantization factor and the adjustment value, respectively.

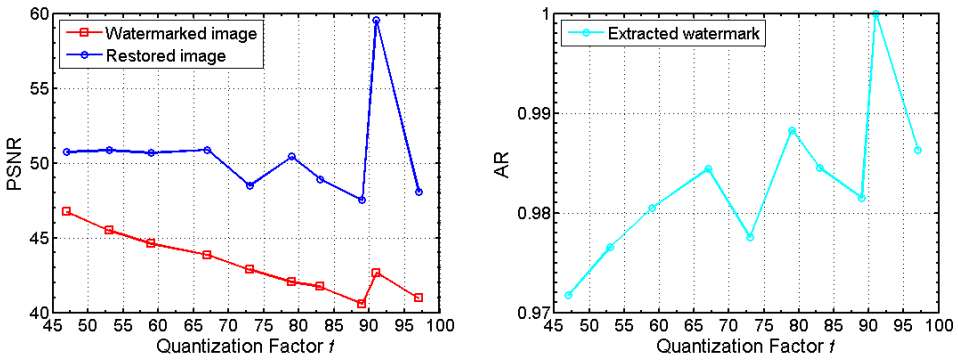


Fig. 5. The effect of quantization factor *f*.

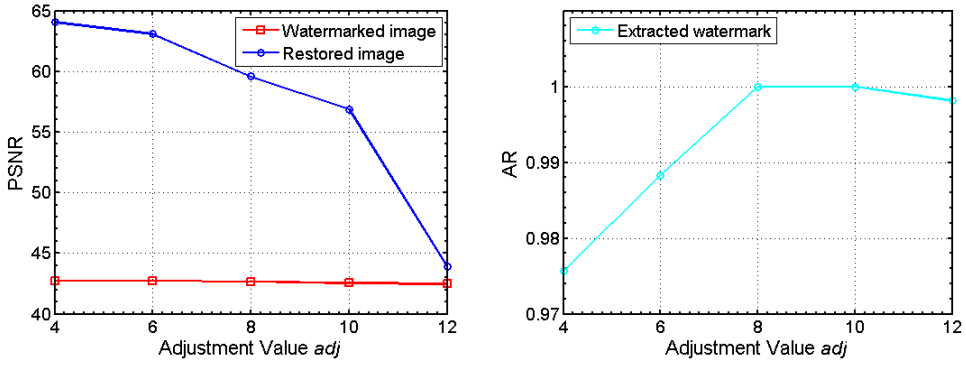


Fig. 6. The effect of adjustment value *adj*.

B. Ttruncation errors

Apart from the parameters discussed previously, there was overflow and underflow as a result of truncation errors. Because of adjustment value *adj* and truncation when writing into an image, there may be errors in the watermark bit when extracting the watermark from the watermarked image.

Detecting overflows/underflows is relatively straightforward by using the following condition in the Preliminary phase to omit some blocks that may result in overflow and underflow. Assume the block's largest single value as a, and if it satisfies the condition $\left|\mathrm{mod}(a, f)\right| \le adj$, the the block needs to be omitted; otherwise, it may probably cause overflow and underflow.

5. Conclusion

This article proposed a novel removable watermarking algorithm based on singular value decomposition. By exchanging the quantization residues of a block's largest singular values, watermark bits can be embedded. To satisfy high image quality requirements, the experimental results show the restored image of the proposed scheme achieves a high PSNR value of around 59.07 dB, which is an improvement compared to the method by Chang *et al*. Additionally, adjustment of the exchanged values enhances the robustness of the proposed scheme. For copyright protection of important images, the experimental results show that the watermarked image can resist a majority of signal processing attacks and modifications, such as JPEG, Gaussian blurring, cropping, scaling and several noise attacks, etc. Therefore, the proposed scheme is effective in protecting valuable images.

References

[1] M.U. Celik, G. Sharma, and A.M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," *IEEE Transactions on Image Processing*, vol. 15, no.4, pp. 1042-1049, April, 2006. Article (CrossRef Link)

[2] C.C. Chang, K.F. Hwang, and M.S. Hwang, "Robust authentication Scheme for protecting copyrights of images and graphics," *IEE Proceedings – Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43-50, February, 2002. Article (CrossRef Link)

[3] Lei, B., Soon, Y., Zhou, F., Li, Z., & Lei, H. "A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition," *Signal Processing*, vol. 92, no. 9, pp. 1985-2001, September, 2012. Article (CrossRef Link)

[4] Hu, H. T., & Hsu, L. Y. "Robust, transparent and high-capacity audio watermarking in DCT domain," *Signal Processing*, vol. 109, pp. 226-235, April, 2015. Article (CrossRef Link)

[5] Khan, A., & Malik, S. A. "A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection," *Information Sciences*, vol. 256, pp. 162-183, January, 2014. Article (CrossRef Link)

[6] Lee, T. Y., & Lin, S. D. "Dual watermark for image tamper detection and recovery," *Pattern recognition*, vol. 41, no. 11, pp. 3497-3506, November, 2008. Article (CrossRef Link)

[7] Di Martino, F., & Sessa, S., "Fragile watermarking tamper detection with images compressed by fuzzy transform," *Information Sciences*, vol. 195, pp. 62-90, July, 2012. Article (CrossRef Link)

[8] Parah, S. A., Sheikh, J. A., Loan, N. A., & Bhat, G. M. "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digital Signal Processing*, vol. 53, pp. 11-24, June, 2016. Article (CrossRef Link)

[9] Dutta, T., & Gupta, H. P. "A robust watermarking framework for high efficiency video coding (HEVC)–Encoded video with blind extraction process," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 29-44, July, 2016. Article (CrossRef Link)

[10] Nguyen, T. S., Chang, C. C., & Huynh, N. T., "A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm," *Journal of Visual Communication and Image Representation*, vol. 33, pp. 389-397, November, 2015. Article (CrossRef Link)

[11] Wang, X., Ding, J., & Pei, Q., "A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition," *Information Sciences*, vol. 310, pp. 16-35, July, 2015. Article (CrossRef Link)
[12] Nguyen, T. S., & Chang, C. C. "A reversible data hiding scheme based on the Sudoku technique," *Displays*, vol. 39, pp. 109-116, October, 2015. Article (CrossRef Link)
[13] Ou, B., Li, X., & Wang, J. "Improved PVO-based reversible data hiding: A new implementation based on multiple histograms modification," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 328-339, July, 2016. Article (CrossRef Link)
[14] Pan, Z., Hu, S., Ma, X., & Wang, L., "Reversible data hiding based on local histogram shifting with multilayer embedding," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 64-74, August, 2015. Article (CrossRef Link)
[15] Rad, R. M., Wong, K., & Guo, J. M., "Reversible data hiding by adaptive group modification on histogram of prediction errors," *Signal Processing*, vol. 125, pp. 315-328, August, 2016. Article (CrossRef Link)
[16] Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recovery of original images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 11, pp.1423-1429, November, 2006. Article (CrossRef Link)
[17] C. C. Chang, P. Y. Lin, and J.S. Yeh, "Preserving robustness and removability for digital watermarks using subsampling and difference correlation," *Information Sciences*, vol. 179, no.13, pp. 2283-2293, June, 2009. Article (CrossRef Link)
[18] P. P. Zheng, J. Feng, Z. Li, & M. Q. Zhou, "A novel SVD and LS-SVM combination algorithm for blind watermarking," *Neurocomputing*, vol. 142, pp. 520-528, October, 2014. Article (CrossRef Link)
[19] J. M. Guo, H. Prasetyo, "False-positive-free SVD-based image watermarking," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1149-1163, July, 2014. Article (CrossRef Link)
[20] W. Lu, H. Lu, and F. L. Chung, "Robust digital image watermarking based on subsampling," *Applied Mathematics and Computation*, vol. 181, no. 2, pp. 886-893, October, 2006. Article (CrossRef Link)

Ya-Feng Di received the B.S. degree in software engineering in 2014 from the Dalian University of Technology, Dalian, China. Since September 2014, he has been studying for his MS degree in software engineering in Dalian University of Technology, Dalian, China. His current research interests include information hiding and image processing.

Chin-Feng Lee received Ph.D. degree in Computer Science and Information Engineering in 1998 from National Chung Cheng University in Taiwan. She is currently a professor in the Department of Information Management at Chaoyang University of Technology, Taiwan. Her research interests include steganography, image processing, and data mining.

Zhi-Hui Wang received the BS degree in software engineering in 2004 from the North Eastern University, Shenyang, China. She received her MS degree in software engineering in 2007 and the PhD degree in software and theory of computer in 2010, both from the Dalian University of Technology, Dalian, China. Since November 2011, she has been a visiting scholar of University of Washington. Her current research interests include information hiding and image compression.

Chin-Chen Chang received his Ph. D in computer engineering in 1982 from the National Chiao Tung University, Taiwan. He was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. Since February 2005, he has been a Chair Professor of Feng Chia University. He is currently a Fellow of IEEE and a Fellow of IEE, UK. He also published several hundred papers in Information Sciences. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.

Jian-Jun Li received the B.S. degree in information engineering from Xi'an University of Electronic Science and Technology, Xi'an, China, and the M.Sc. and Ph. D degrees in electrical and computer from The University of Western Ontario and University of Windsor, Canada separately. He is currently working at HangZhou Dianzi University as a chair professor. His research interests include micro-electronics, audio, video and image processing algorithms and implementation.