Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **2**, April **2014**

A Novel SVD-based Watermarking Scheme for Protecting Rightful Ownership of Digital Images

Chia-Chen Lin[1], Chin-Chen Chang[2,4,*], and Yi-Hui Chen[3]

[1]Department of Computer Science and Information Management,
Providence University,
Taichung 43301, Taiwan, R.O.C.
mhlin3@pu.edu.tw

[2,*]Department of Information Engineering and Computer Science,
Feng Chia University,
Taichung 40724, Taiwan, R.O.C.
Correspondence Author
ccc@cs.ccu.edu.tw

[3]Department of Applied Informatics and Multimedia,
Asia University,
Taichung 41354, Taiwan, R.O.C.
chenyh@asia.edu.tw

[4]Department of Computer Science and Information Engineering,
Asia University,
Taichung 43154, Taiwan, R.O.C.

Received May, 2013; revised September, 2013

Abstract. *Watermarking is a data embedding technique widely used to protect rightful ownership of digital images. In recent years, several SVD-based watermarking schemes have been proposed in the literatures. However, although most existing schemes can provide good image quality of the watermarked image and robust embedded watermarks, some still need to store extra data or use an original image in order to extract the watermark. To overcome these drawbacks, in this paper, we propose a novel SVD-based watermarking scheme that contains a recovery mechanism so that the watermarked image can be recovered to satisfactory condition after rightful ownership of an image has been established. To extend the application of the proposed scheme into commercial applications, we also present a variant that inherits the properties of the proposed scheme and provides higher image quality in a restored image after the embedded watermark is extracted. Experimental results confirm that our primary scheme can withstand a variety of image processing techniques and that our variant can successfully reduce the difference between a compressed host image and a restored image to less than 2 dB.*
Keywords: Watermarking, Ownership protection, Singular value decomposition, Robustness, Recovery.

1. **Introduction.** Because the Internet breaks down geographic limitations, it has gained popularity as a data transmission channel in past years. However, while users enjoy the convenience offered by the Internet, transmitted data may suffer attacks by malicious users, forgery, duplication or modification, among other forms of predation. These illegal operations not only violate the intellectual property rights (IPRs) of the digital content but also decrease the intentions of the authors' creations. Watermarking is one approach that

allows a legal owner to claim rightful ownership when it has been violated. Because the ownership protection of digital data has become an important issue, many watermarking schemes have been proposed [1-8, 11-14, 16-24, 26, 27, 29] in past years.

Generally, the taxonomy of watermarking schemes is as shown in Figure 1, ordered according to visibility, embedding approach and robustness of the embedded watermarks.

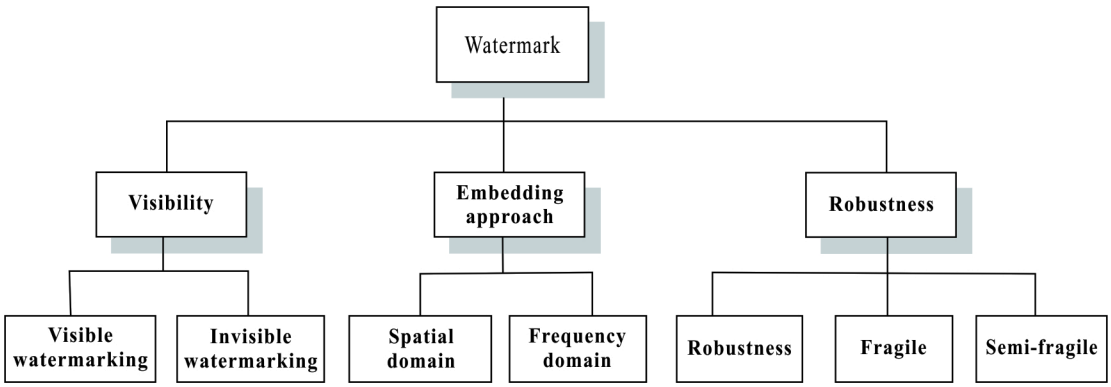


FIGURE 1. Taxonomy of watermarking schemes

As Figure 1 shows, watermarking techniques can be classified into the spatial [19, 21, 23, 26, 27] and frequency domains [10, 11, 13, 15-17, 20]. In the spatial domain approaches, the pixels of the host image are changed directly to hide a watermark. Although the algorithm for spatial domain watermarking is simple and has low computational complexity, it cannot withstand rigorous digital signal processing. In the frequency domain approaches, a watermark is embedded into the coefficients of the frequency domain after the discrete Fourier transform (DFT) [28], discrete cosine transformation (DCT) [10] or discrete wavelet transformation (DWT) [25], and so on. Later, the changed coefficients are inversely transformed back into the spatial manner. Therefore, frequency domain watermarking can withstand digital signal processing at the cost of higher computational complexity as compared with spatial domain watermarking.

In 2002, Liu and Tan proposed a singular value decomposition (SVD)-based watermarking scheme [23] that offers high embedding quality and high robustness. However, for each embedded block, their proposed scheme must store three matrices to be used later for watermark extraction. In the same year, Chandra [4] proposed an effective SVD-based watermarking scheme, but that scheme requires the original image and the watermark for later extraction of the embedded watermark. In 2005, Bao and Ma [3] proposed an SVD-based watermarking scheme that first transforms an image into wavelet subbands. The coefficients in each subband are then segmented into nonoverlapping blocks of size $n \times n$ and the SVDs for each block are computed. The standard deviation and average value for the DWT coefficients of each block are derived as a quantization factor. Finally, Bao and Ma slightly altered the coefficient of the S matrix in each block within the wavelet subbands of the original image based on its corresponding quantization factor to hide one bit of watermark.

Unlike Bao and Ma's watermark embedding strategy, Chang et al. [5] slightly modified the coefficients of the U components in each block of the original image to hide one bit of watermark. To prevent the watermarked image from becoming perceptible, they applied a feature of the S matrix to select the embedding blocks. In addition, they used a magnitude difference threshold to control the robustness of the embedded watermark. Experiments confirmed that their scheme could withstand JPEG, nosing, cropping, sharpening, blurring and tampering attacks. Inspired by Chang et al.'s concept, another

SVD-watermarking was proposed by Chung et al. that contains more watermarks in one host image [12].

Although many scholars have explored the design of watermarking based on SVD schemes, these schemes focus mainly on robustness in withstanding compression, image quality of watermarked images, blind detection of embedded watermarks and sensitivity to malicious manipulation. Only a few schemes consider providing higher image quality of restored images after rightful ownership of an image has been established. In this paper, we propose an SVD-watermarking scheme that involves modifying the coefficients of the S matrices of the original image. In this scheme, multiple copies of watermarks are embedded into an original host image, and a voting strategy is adopted during the extraction phase to increase the accuracy of the extracted watermark. Furthermore, to extend the proposed scheme into commercial applications, we also propose a variant that offers better image quality of restored images than that of the watermarked images, once rightful ownership has been established.

Experimental results confirm that our primarily proposed scheme withstands cropping 50%, brightness adjustment, sharpening, blurring, noising, compression and tampering attacks. Furthermore, on average, the image quality of any restored image generated by using our variant is still 4 *dB* higher than can be achieved by using our primary scheme when the quality factor (QF) of JPEG compression is set at 70.

The rest of this paper is organized as follows. In Section 2, SVD transformation is briefly described. Our primary proposed scheme is presented in Section 3. Several experimental results of our primary scheme are illustrated in Section 4. Our variant, which adds the recovery mechanism, is presented in Section 5. Finally, concluding remarks are given in Section 6.

2. **Singular Value Decomposition (SVD) Transformation.** SVD transformation is a linear algebraic algorithm. Because SVD transformation preserves both one-way and non-symmetric properties that cannot be obtained with the DFT or DCT transformations, SVD has been used in image hiding and image watermarking in recent years. To perform SVD transformation, a grayscale image I is divided into nonoverlapping blocks of size $n \times n$. A block A in image I can be transformed into three matrices, U, S, V, respectively, by using Equation (1).

$$A = USV^T = [u_1, u_2, ..., u_n] \times \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & s_n \end{bmatrix} \times [v_1, v_2, ..., v_n]^T = \sum_{i=1}^{n \times n} s_i u_i v_i^T. \quad (1)$$

Here, U and V are two $n \times n$ orthogonal matrices, and S is an $n \times n$ diagonal matrix. Diagonal components$s_1, s_2, \ldots, s_n$ of matrix S satisfy $s_1 \geq s_2 \geq \ldots \geq s_n$.

3. **Our Proposed Scheme.** This section describes our proposed SVD-based watermarking scheme, which embeds the bits of a watermark into the components of the S matrices in an image. This proposed scheme encompasses both the embedding procedure and the extracting and restoring procedure. The two procedures are described in Subsections 3.1 and 3.2, respectively.

3.1. **Embedding Procedure.** In order to use the characteristics of the SVD domain to embed a watermark into a host image, we explored the coefficients of the S matrix in each block. Based on our observation, we discover that in the non-zero coefficients of S matrices in an image, the larger the value of the coefficient, the greater the effect of the coefficient on image quality. In addition, any alteration to the largest coefficients of the S matrices of an image leads to significant distortions in image quality. These factors support the idea behind developing a robust SVD-watermarking scheme.

An overview of the embedding procedure is shown in Figure 2. The size of host image $I$is $m \times m$. The host image is divided into nonoverlapping blocks B_j of size 4×4, where $1 \leq j \leq (m/4) \times (m/4)$ and $I = B_1 \cup B_2 \cup ... \cup B_{(m/4)\times(m/4)}$. The watermark $W$is a binary image of size $n \times n$ bits, where $W = (w_1, w_2, \ldots, w_n \times_n)$ and$w_i \in \{1,0\}$.

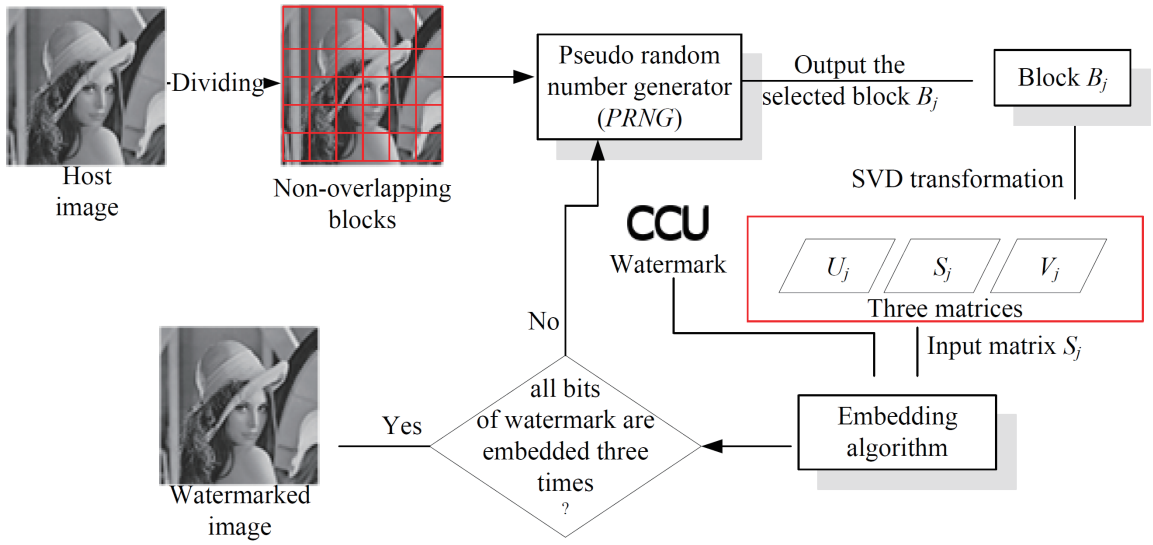


FIGURE 2. Flowchart of the proposed embedding procedure

To increase watermarking security, a pseudo random number generator ($PRNG$) is adopted to select the block in which to hide each bit of watermark. Each selected block B_j is then transformed into three matrices, U_j, S_j and V_j, through SVD transformation. Later, the encoder mixes the components of matrix S_j and watermark bit $w_i$to generate a hidden block WB_j by applying the embedding algorithm. Note that each watermark bit w_i is embedded into three separate blocks of the host image to enhance the robustness of the embedded watermark, and each block of the host image contains only one watermark bit. Therefore, the encoder repeats the embedding algorithm three times until all watermark bits are processed. Finally, all embedded blocks are outputted to generate a watermarked image. In the embedding algorithm, watermark bit w_i is embedded into the second non-zero coefficient of matrix S_j of each block in the host image. The embedding algorithm of our SVD watermarking scheme is as follows.

Embedding Algorithm

Input: The matrix S_j of the selected block and watermark bit w_i.

Output: A watermarked block WB_j.

Step 1: Let $S_j = \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & s_4 \end{bmatrix}$.

Step 2: Let $\bar{s}_4$ be equal to $(s_3 \times 0.1)$. Obtain $\bar{S}_j$ which is $\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & s_3 & 0 \\ 0 & 0 & 0 & \bar{s}_4 \end{bmatrix}$.

Step 3: Let $\bar{s}_3$ be equal to s_2. Obtain $\bar{S}'_j$ which is $\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & 0 & \bar{s}_3 & 0 \\ 0 & 0 & 0 & \bar{s}_4 \end{bmatrix}$.

Step 4: Let $\bar{s}_2$ be equal to $(s_2 + \sigma \times w_i)$ in the matrix $\bar{S}''_j$, where σ is the robustness factor of the embedded watermark. Obtain $\bar{S}''_j$ which is $\begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & \bar{s}_2 & 0 & 0 \\ 0 & 0 & \bar{s}_3 & 0 \\ 0 & 0 & 0 & \bar{s}_4 \end{bmatrix}$. In essence, a higher value of σ makes the embedded watermark more robust, but also results in lower image quality.

Step 5: Perform an SVD inverse operation on matrices U_j, $\bar{S}''_j$ and V_j to reconstruct the watermarked block, WB_j, which is equal to $U_j \times \bar{S}''_j \times V_j^T$.

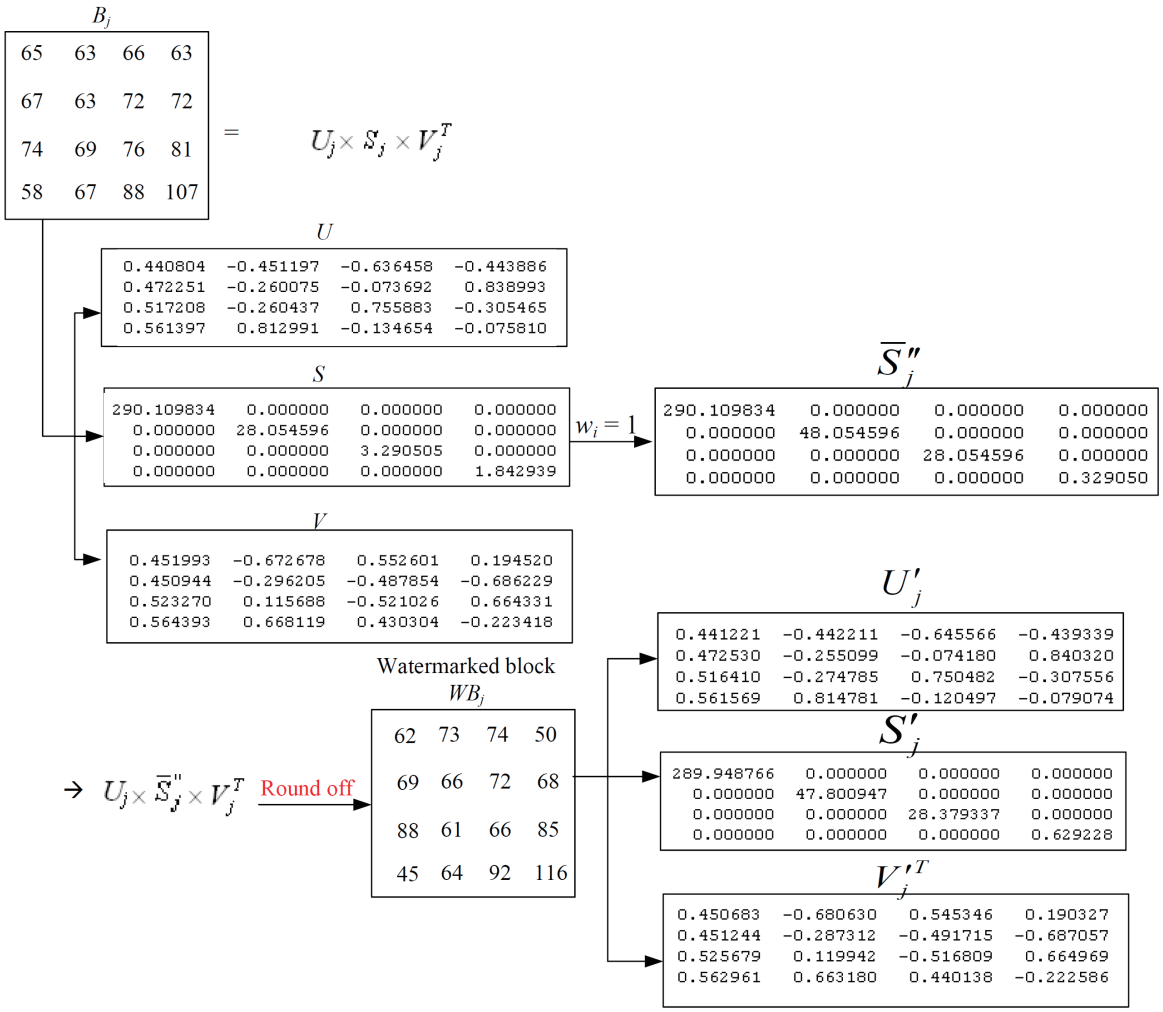


FIGURE 3. Example of embedding algorithm

The example in Figure 3 demonstrates the proposed embedding algorithm. In this figure, we assume that watermark bit w_i is 1 and the value of σ is 20. During watermark embedding, the encoder performs Steps 2 to 4 to hide a watermark bit in current block B_i. In Step 2, the third non-zero coefficient s_4 is replaced by $s_3 \times 0.1$. In Step 3, $s_3$is replaced by the second non-zero coefficient s_2. Finally, in Step 4, s_2 is changed to $s_2 + \sigma \times w_i$=28.054596+20×1 = 48.054596. After watermark embedding is completed, encoder performs the SVD inverse transformation to generate the watermarked block.

Note that each pixel of WB_j is an integer; therefore, a round-off operation is required during the SVD inverse transformation. The round-off operation may cause inevitable distortion between the $\bar{S}''_j$ matrix generated during the embedding procedure and the S'_j matrix of watermarked block WB_j derived during later extracting procedure. However, any resulting distortion is too minor to affect the watermark detection ratio in our proposed scheme. Section 4 presents more detailed experiments that confirm the robustness of the proposed scheme.

3.2. **Extracting and Restoring Procedure.** Generally, a watermarked image cannot be restored to a higher image quality even after the hidden watermark is extracted. Conversely, a more robust watermark may lead to greater distortion of the host image after the watermark is embedded. Thus, once watermarking is applied to commercial products or arts, it will desirable to reduce the distortion caused by an embedded watermark as much as possible. So far, existing SVD-watermark schemes have not yet achieved reversibility. In this paper, we propose an SVD-watermarking approach that promises higher image quality of restored images as a first step to achieving a reversible SVD-watermarking scheme. Therefore, not only can a hidden watermark be extracted correctly from a watermarked image with this procedure, but also a restored image having higher image quality can be reconstructed from the watermarked image after extracting the hidden watermark bits.

Because three copies of a watermark are embedded into three separate blocks of the host image, the final extracted watermark results can be easily derived by applying a majority voting strategy to the three extracted results. Figure 4 presents a flowchart of our extracting and restoring procedure. The watermarked image is first divided into non-

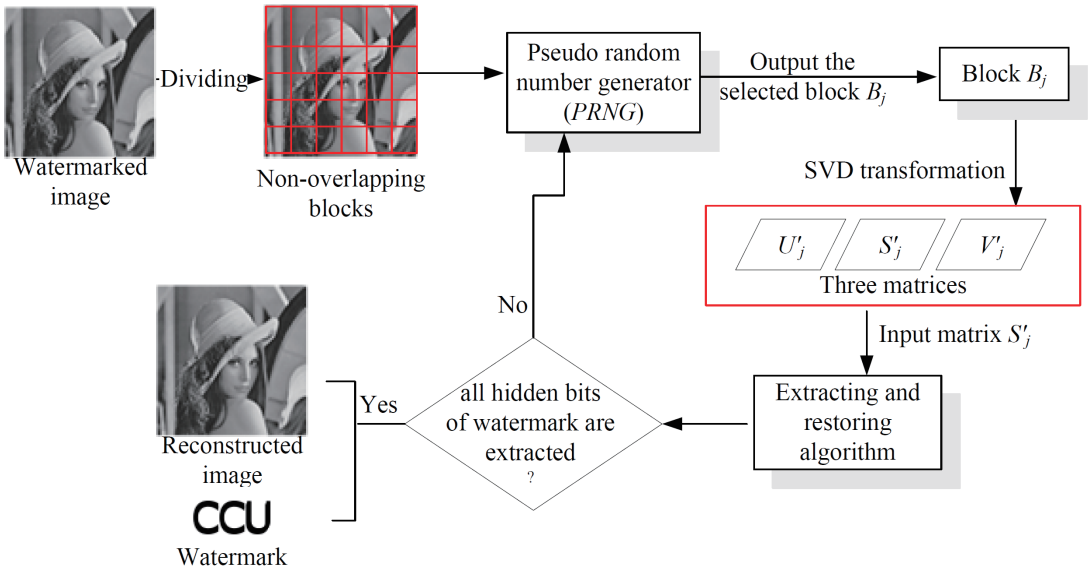


FIGURE 4. Flowchart of extracting and restoring procedure

overlapping blocks of size 4×4. Next, the decoder uses the same seed of the *PRNG* to choose the blocks for extracting. A selected block is SVD transformed into three matrices, U'_j, S'_j and V'_j. Each matrix S'_j of the selected block is processed with the extracting and restoring algorithm to extract the embedded watermark and restore the matrix S'_j. Later, the decoder performs an SVD inverse transformation to generate a restored block RB_j. Finally, the decoder outputs all the restored blocks to generate a restored image after all the embedded blocks of the watermarked image have been processed. Experimental results, derived from our restoring algorithm, presented in Section 4 will prove that the reconstructed image has a higher image quality than its watermarked image does.

Extracting and Restoring Algorithm
Input: Matrix S'_j of an embedded block and variable q, and q's initial value is 0.
Output: A restored block RB_j and an extracted watermark bit w_q.

Step 1: Let $S'_j = \begin{bmatrix} s'_1 & 0 & 0 & 0 \\ 0 & s'_2 & 0 & 0 \\ 0 & 0 & s'_3 & 0 \\ 0 & 0 & 0 & s'_4 \end{bmatrix}$.

Step 2: Extract the hidden watermark by Equation (2).

$$w'_q = \begin{cases} 1, \text{if} s'_2 - s'_3 \geq \sigma/2 \\ 0, \text{otherwise.} \end{cases} \tag{2}$$

Step 3: Let s'_2 be equal to s'_3 and denoted as $\hat{s}_2$. Obtain matrix $\hat{S}_j$ which is $\begin{bmatrix} s'_1 & 0 & 0 & 0 \\ 0 & \hat{s}_2 & 0 & 0 \\ 0 & 0 & s'_3 & 0 \\ 0 & 0 & 0 & s'_4 \end{bmatrix}$.

Step 4: The decoder replaces s'_3 with (s'_4×10) and denoted as $\hat{s}_3$. Obtain matrix $\hat{S}'_j$ which is

$$\begin{bmatrix} s'_1 & 0 & 0 & 0 \\ 0 & \hat{s}_2 & 0 & 0 \\ 0 & 0 & \hat{s}_3 & 0 \\ 0 & 0 & 0 & s'_4 \end{bmatrix}.$$

Step 5: Perform an SVD inverse operation on matrices U'_j, $\hat{S}'_j$ and V'_j to reconstruct the restored block, RB_j, which is equal to $U'_j \times \hat{S}'_j \times V'^T_j \times \hat{S}'_j \times V'^T_j$.

Step 6: Let q be equal to $(q + 1)$.

Step 7: If three copies of a watermarked bit have been extracted, go to Step 8. Otherwise, select the next embedded block to retrieve the next copy of the watermark bit according to the *PRNG* result, and then repeat Steps 1 to 6.

Step 8: Perform the majority voting strategy to decide the final extraction result w'_q of the three copies of a watermarked bit. That is, if $w'_q + w'_{q+n\times n} + w'_{q+2\times n\times n} \geq 2$, where $n \times n$ is the watermark size, let w'_q=1; otherwise, w'_q=0.

Figure 5 gives an example that demonstrates the extracting and restoring procedure.

The difference between the second and third non-zero coefficients is used to extract a watermarked bit from an embedded block. Using our restoring strategy, the third non-zero coefficient is replaced by $(s'_4 \times 10)$. Comparing Figures 3 and 5, we can see that the restored image block using our restoring strategy is very similar to the original one.

4. **Experimental Results.** This section describes several experiments that were conducted to verify the effectiveness of the proposed scheme, which is described in detail in

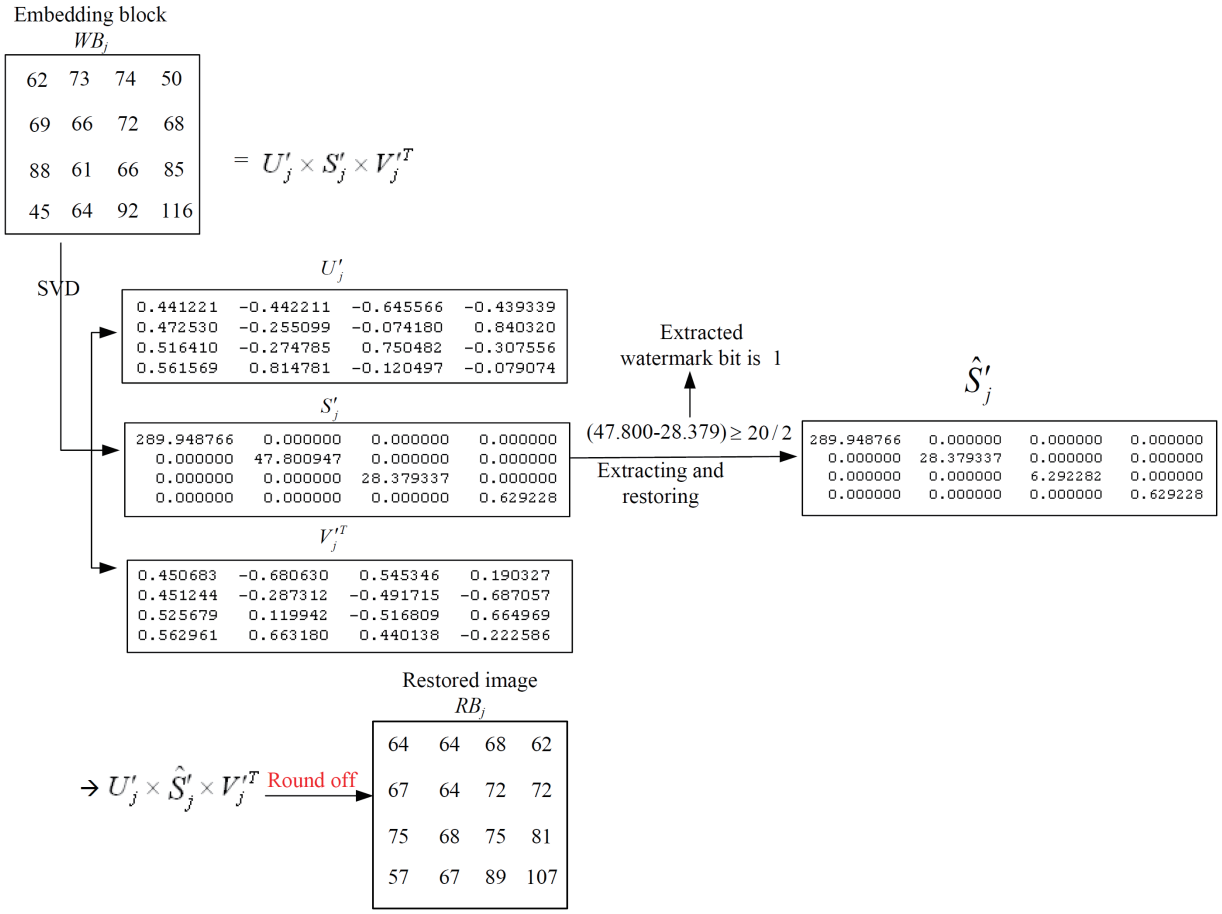


FIGURE 5. Example of extracting and restoring procedure

Section 3. The proposed scheme was developed with Java and the simulation platform is Microsoft Windows XP, Pentium III with 512 MB memory. Seven 512×512 gray-scale images, "Lena", "Pepper", "F16", "Barbara", "Zelda", "Baboon" and "GoldHill", served as host images, and are shown in Figures 6(a) to 6(g), respectively. A 64×64 binary image used as the watermark is shown in Figure 6(h). In addition, in the following experiments, we set content σ, which was used in the embedding, extracting and restoring algorithms, as 20.

Two measures, *PSNR* (peak signal-to-noise ratio) and *BCR* (bit correction ratio), were used to evaluate the performance of our proposed scheme. The *PSNR* value, which is defined in Equation (3), was used to measure the image quality of the watermarked and restored images.

$$PSNR = 10\log_{10}\frac{255^2}{MSE}dB, \tag{3}$$

where 255 represents the maximum pixel value of a gray-level image, and the mean square error (*MSE*) of an image is depicted in Equation (4).

$$MSE = \frac{\sum_{r}^{ht}\sum_{s}^{wd}(x_{rs} - x'_{rs})^2}{H \times W}. \tag{4}$$

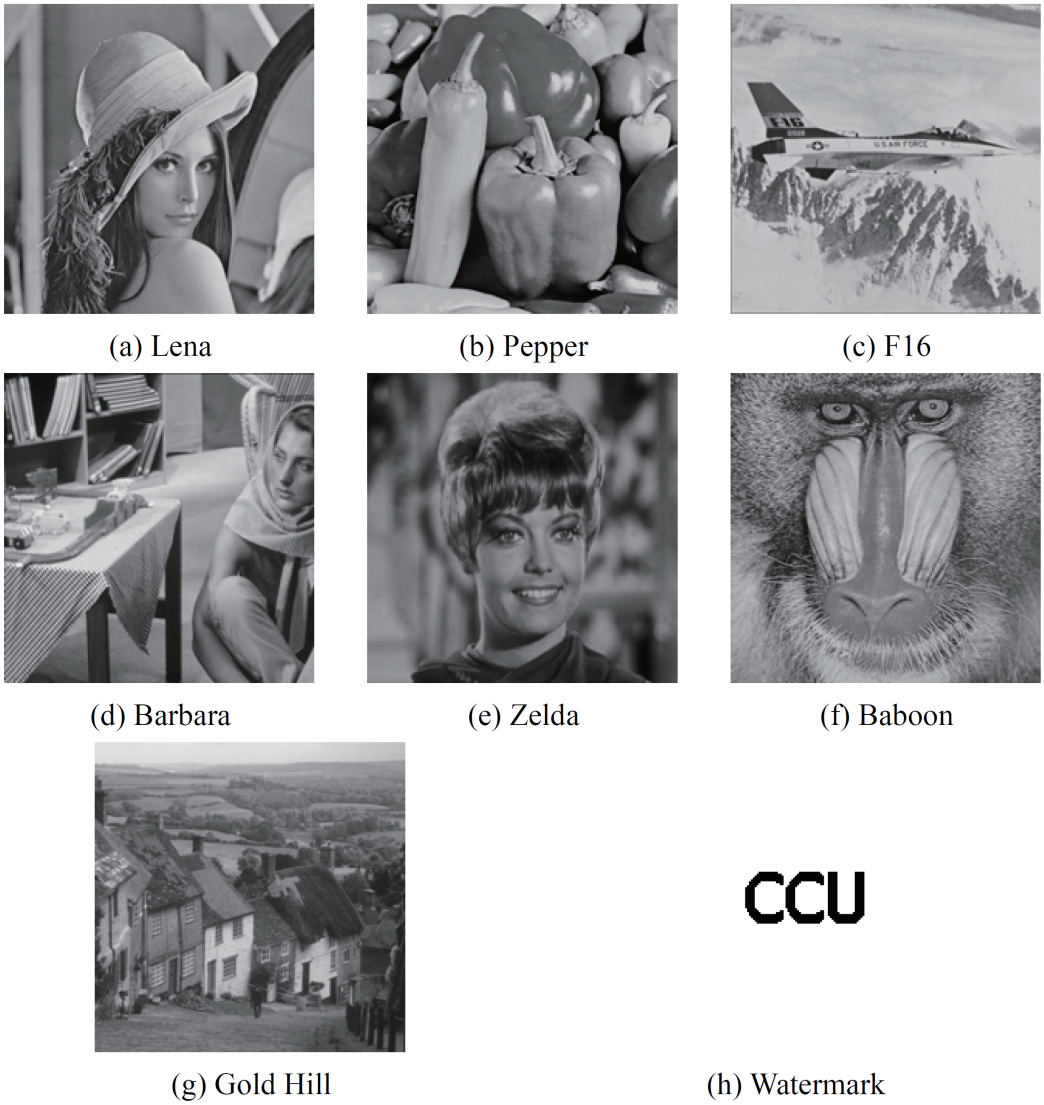


FIGURE 6. Seven 512×512 gray-scale host images and a 64 × 64 binary watermark

Here, the notations *ht* and *wd* represent the height and width of an image, respectively. If *PSNR* is used to measure the image quality of the watermarked image, x_{rs} is the pixel value of the position (r, s)in an original image and x'_{rs} is the pixel value of the watermarked image. Generally, the higher the *PSNR* value of a watermarked image is, the better the image quality will be. In contrast, if the image quality of the watermarked image is worse, its *PSNR* value will be lower. If *PSNR* is used to measure the image quality of the restored image, x_{rs} is the pixel value of the position (r, s)in the watermarked image and x'_{rs} is the pixel value of the restored image. In this case, if the *PSNR* is high, the restoring strategy has successfully restored the image from the watermarked image after the hidden watermark has been extracted. Furthermore, the *BCR* defined in Equation (5) is used to measure the correction ratio of the extracted watermark.

$$BCR = \frac{\sum_{i=1}^{n\times n} \overline{w_i \oplus w'_i}}{n \times n} \times 100\%, \tag{5}$$

where w_i and w'_i are the ith binary value of the original watermark and of the extracted watermark, respectively, and $\oplus$ indicates an exclusive-OR operator. Note that a higher

BCR implies greater similarity between the original watermark and the extracted watermark.

The image quality of the watermarked images and restored images are presented in Table 1 for images not subjected to attack. With the watermark embedding strategy, the average *PSNR* of a watermarked image is 33.91 *dB*. Using the proposed restoring strategy, in the best case, the *PSNR* of the restored "Zelda" image is up to 51.79 *dB*; and in the worse case the restored "Barbara" image stays at 39.71 *dB*. On average, the *PSNR* of the restored image is 10.95 *dB* higher than that of the watermarked image. In other words, the restoring strategy works well. In addition, in the no-attack scenario the *BCR* of each extracted watermark of the seven watermarked images can be as much as 100% with the proposed scheme.

TABLE 1. *PSNR* (*dB*) of watermarked and restored images without any attack

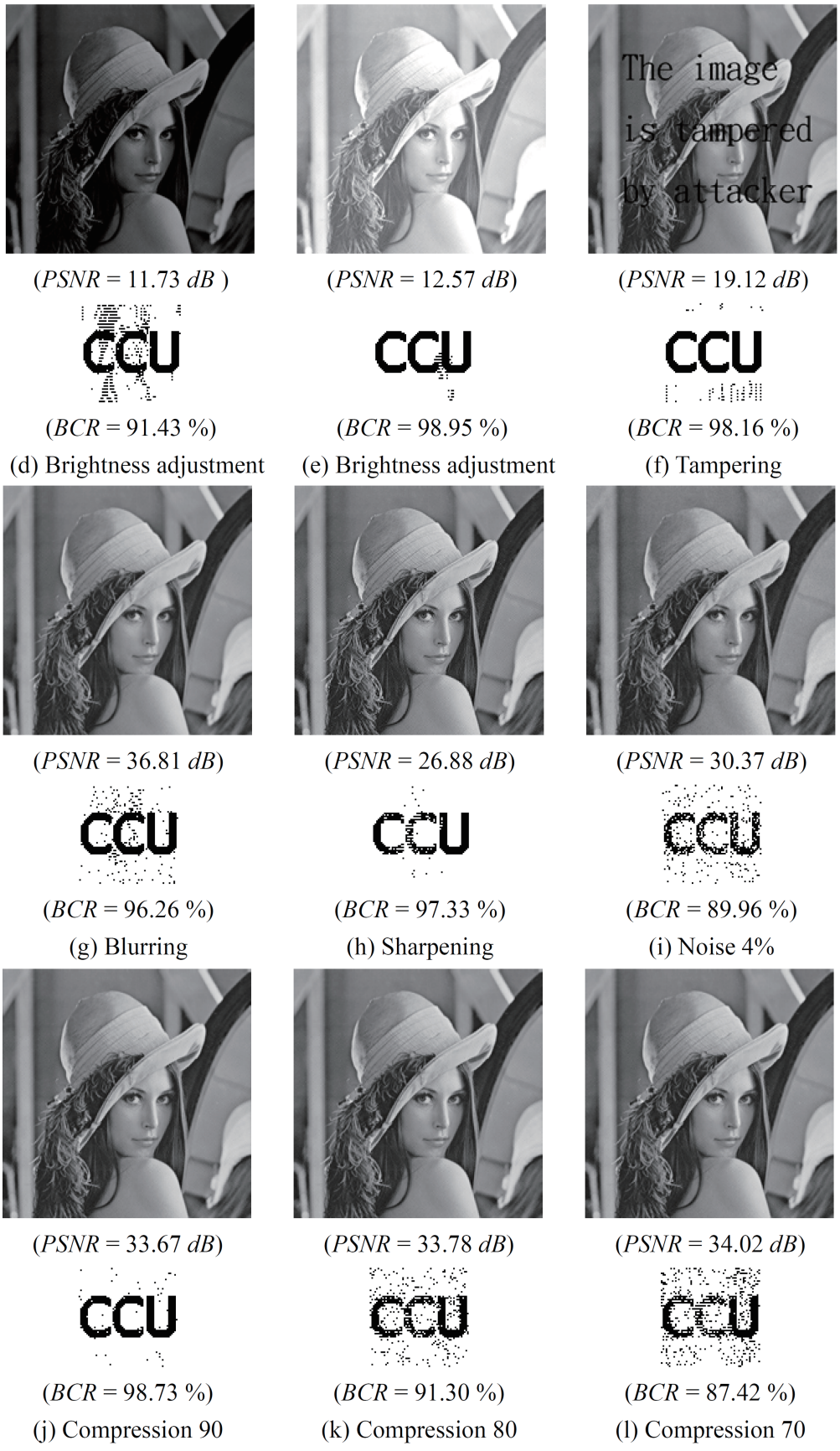
PSNR/*BCR*	Lena	Pepper	F16	Barbara	Zelda	Baboon	Gold Hill
Watermarked image (*dB*)	34.56	35.18	34.36	30.93	35.98	32.13	34.57
Restored image (*dB*)	45.92	46.51	44.27	39.71	51.79	40.94	45.22
BCR	100%	100%	100%	100%	100%	100%	100%

Figure 7 summarizes the performance of the proposed scheme in image quality and *BCR* under various attacks on the test image "Lena". We can see that even though the watermarked image is attacked by JPEG compression with a quality factor (QF) of 70 or noise 4% attacks, the *BCR*s of both extracted watermarks are still 87.42% and 89.96 %, respectively. For the remaining types of attack, the *BCR*s of the extracted watermarks are up to 90%. Moreover, the *BCR*s of the extracted watermarks are as much as 95% when the watermarked images are attacked by cropping 50%, brightness adjustment, tampering, sharpening, blurring or JPEG compression with a quality factor of 90.

(*PSNR* = 17.47 *dB*) (*PSNR* = 11.46 *dB*) (*PSNR* = 8.54 *dB*)

(*BCR* = 100 %) (*BCR* = 99.83 %) (*BCR* = 99.60 %)

(a) Cropping 6.25 % (b) Cropping 25 % (c) Cropping 50 %



(*PSNR* = 11.73 *dB*) (*PSNR* = 12.57 *dB*) (*PSNR* = 19.12 *dB*)

(*BCR* = 91.43 %) (*BCR* = 98.95 %) (*BCR* = 98.16 %)

(d) Brightness adjustment (e) Brightness adjustment (f) Tampering

(*PSNR* = 36.81 *dB*) (*PSNR* = 26.88 *dB*) (*PSNR* = 30.37 *dB*)

(*BCR* = 96.26 %) (*BCR* = 97.33 %) (*BCR* = 89.96 %)

(g) Blurring (h) Sharpening (i) Noise 4%

(*PSNR* = 33.67 *dB*) (*PSNR* = 33.78 *dB*) (*PSNR* = 34.02 *dB*)

(*BCR* = 98.73 %) (*BCR* = 91.30 %) (*BCR* = 87.42 %)

(j) Compression 90 (k) Compression 80 (l) Compression 70

FIGURE 7. *PSNR*s of watermarked images and *BCR*s of extracted watermarks under various types of attack

In Tables 2 to 7, we list the *PSNR*s and *BCR*s of watermarked images after the images are attacked by JPEG compression with a quality factor (QF) of 80, sharpening, blurring, 4% noising, 50% cropping and tampering. Three image processing results with three cropping ratios, 6.25%, 25% and 50%, are listed in Figures 7(a) to 7(c), respectively. Note that the *BCR* of the extracted watermark of the watermarked "Lena" image is very close to 100%. A similar phenomenon also occurs in the other six watermark images, as Table 2 shows. Both of Figure 7(c) and Table 2 demonstrate the robustness of the proposed scheme against a 50% cropping attack.

TABLE 2. Extracting results of seven watermarked images under a 50% cropping attack

Results / Watermarked images	*PSNR* of the noisy image	*BCR* of watermark
Lena	19.12 *dB*	99.60 %
Pepper	19.50 *dB*	99.02 %
F16	16.57 *dB*	98.55 %
Barbara	20.95 *dB*	98.75 %
Zelda	19.20 *dB*	98.77 %
Baboon	17.68 *dB*	98.65 %
Gold Hill	20.02 *dB*	99.26 %

To test whether the proposed scheme can withstand a tampering attack, we added 24 characters to the watermarked "Lena" image shown in Figure 7(f). Note that the *PSNR* of the tampered image is only 19.12 *dB*, but the *BCR* of the extracted watermark is still 98.16%. It is clear that the watermarks have been almost fully extracted. In other words, the difference between the extracted watermark and the original image is almost zero.

TABLE 3. Extracting results of seven watermarked images under tampering attack

Results / Watermarked images	*PSNR* of the noisy image	*BCR* of watermark
Lena	19.12 *dB*	98.16 %
Pepper	19.50 *dB*	99.02 %
F16	16.57 *dB*	98.55 %
Barbara	20.95 *dB*	98.75 %
Zelda	19.20 *dB*	98.77 %
Baboon	17.68 *dB*	98.65 %
Gold Hill	20.02 *dB*	99.26 %

From Table 4, we can see that only three of seven test images show *BCR*s for the extracted watermarks of up to 90%. However, *BCR*s below 90% (the other four images) are still above 86%.

Table 5 presents the experimental results of the robustness test against image blurring for each watermarked image. All *BCR*s listed in Table 5 are higher than 94.84%. Based

TABLE 4. Extracting results of seven watermarked images after JPEG compression with 80% QF

Results / Watermarked images	*PSNR* of the JPEG compressed image	*BCR* of the watermark
Lena	33.78 *dB*	91.30 %
Pepper	34.19 *dB*	90.23 %
F16	33.52 *dB*	87.76 %
Barbara	29.37 *dB*	88.79 %
Zelda	35.81 *dB*	95.11 %
Baboon	30.05 *dB*	86.81 %
Gold Hill	32.38 *dB*	88.40 %

on the *BCR*s listed in Table 5 and in Figure 7(g), we know that our proposed scheme also withstands blurring attack.

TABLE 5. Extracting results of seven watermarked images under blurring processing

Results / Watermarked images	*PSNR* of the blurred image	*BCR* of the watermark
Lena	36.81 *dB*	96.26 %
Pepper	38.15 *dB*	95.65 %
F16	34.36 *dB*	100 %
Barbara	29.10 *dB*	98.09 %
Zelda	39.53 *dB*	94.84 %
Baboon	32.82 *dB*	99.85 %
Gold Hill	36.13 *dB*	99.63 %

Table 6 shows that the *BCR*s of six watermarked images are up to 93%. Even in the worst case, the *BCR* is higher than 88.18%. By looking at Figure 7(f) and Table 6 together, we see the robustness of the proposed scheme on sharpening attack has been proved.

TABLE 6. Extracting results of seven watermarked images under sharpening image processing

Results / Watermarked images	*PSNR* of the sharpened image	*BCR* of the watermark
Lena	26.88 *dB*	97.33 %
Pepper	27.18 *dB*	98.60 %
F16	26.20 *dB*	95.77 %
Barbara	21.67 *dB*	93.53 %
Zelda	29.10 *dB*	99.46 %
Baboon	21.77 *dB*	88.18 %
Gold Hill	25.11 *dB*	93.48 %

Figure 7(i) shows that the *BCR* extracted from watermarked "Lena" is 89.96% and that the visual quality of the extracted watermark is acceptable. In Table 7, we list the *PSNR*s of the remaining six watermarked images and the corresponding *BCR*s of their extracted watermarks. These experimental results confirm the robustness of the proposed scheme in resisting 4% noising image processing.

TABLE 7. Extracting results of seven watermarked images under 4% noising image processing

Results / Watermarked images	*PSNR* of the noisy image	*BCR* of watermark
Lena	30.37 *dB*	89.96 %
Pepper	30.65 *dB*	91.21 %
F16	30.34 *dB*	90.91 %
Barbara	28.21 *dB*	91.16 %
Zelda	30.90 *dB*	89.69 %
Baboon	29.30 *dB*	90.28 %
Gold Hill	30.42 *dB*	91.23 %

TABLE 8. Performance comparisons between other watermark schemes and ours

Performance comparisons	Hwang et al. [19]	Liu and Tan [23]	Chandra [4]	Chang et al. [5]	Bao and Ma [3]	Proposed scheme
Processing domain	Spatial domain	SVD domain	SVD domain	SVD domain	Wavelet and SVD domains	SVD domain
Host image is required for extracting watermark	No	No	Yes	No	No	No
Robustness	Low	High	High	High	High	High
Embedding quality	Very high	High	High	High	High	High
Extra data is required for watermark extraction	No	Three matrices, U_W, S, V_W	The original image and original watermark	No	Quantization factors	No
Restoring mechanism	No	No	No	No	No	Yes

In Table 8, we compare the performance of five similar watermark schemes with that of our proposed scheme. Hwang et al.'s scheme [19] can provide high image quality in watermarked images. However, their robustness is low because their embedded watermark can be extracted clearly only when the least significant three bits of each pixel in the watermarked image are randomly modified. Their scheme cannot work well after the watermarked images are attacked by other image processing attacks. The other SVD-based watermarking schemes and our scheme all have strong robustness and high image quality. Liu and Tan's scheme [23] must store the three matrices whose size is the same as the host image for later extraction of the watermark. Therefore, their scheme requires a large amount of extra information that amounts to three times the host image. As for Chandra's scheme [4], it not only requires the original watermark but also the original image during the watermark extraction procedure. Bao and Ma's scheme [3] successfully uses the quantization parameters to enhance the image quality of the watermarked image. However, the quantization parameters must be stored for later watermark extraction. In addition, their host image must be transformed into the wavelet and SVD domains, which makes the computation complexity higher than with our scheme. In our proposed scheme, neither extra data nor the original host image is required during the extracting procedure. Furthermore, the proposed scheme has a restoring mechanism so that a restored image having better image quality can be produced after the embedded watermark is extracted to establish rightful ownership.

5. **Extension and Discussions.** Although the proposed scheme already provides a restoring mechanism, the image quality of the restored image is not high enough for commercial applications. When we talk about commercial applications, we mean that, to gain the trust of their customers, on-line shops embed their logos into their digital products such as digital images. However, the bandwidth of the transmission channel is limited and digital images are large. To speed up transmission, sellers may provide a compression file for each authorized digital image to allow downloading by legal users. Without applying digital signature techniques, it is difficult for a user to judge whether a compressed file is granted by the seller or not. On the other hand, if a malicious user complains that a seller does not provide the correct compression file, the seller is difficult to prove his innocence. This scenario raises an open problem: how to restore a watermarked image to satisfactory condition after it is compressed by JPEG with a certain level of quality factor. If this problem can be resolved, watermarked images can be reduced to a reasonable size for users to download by JEPG, and second-tier compression is not necessary. In other words, these kinds of disputes can be avoided.

To extend the proposed scheme to the special scenario mentioned above, a variant is proposed in this section. The basic concept of the variant is very simple: to create a space to preserve the third component s_3 of the S matrix of each image block in the host image so that the preserved s_3's can be used to generate a restored image with higher image quality during the extracting and restoring procedure. Here, we call the watermarked image compressed by JEPG *CWI* for short. To achieve our objective, the SVD transformation must be performed twice. The first is conducted on the host image and the second is operated on the *CWI*. All s_3's are recorded after the first SVD transformation. Later, the second SVD transformation is performed on the *CWI*, and the fourth component s_4 of the S matrix of each image block in the *CWI* is replaced by the preserved $s_3 \times 0.1$, individually, as shown in Figure 8.

To prove that this modification can restore the *CWI* to a higher image quality compared with our primary proposed scheme, which is described in Section 3.1, Tables 9, 10, 11 and 12 list the *PSNR*s of the compressed host images in which no watermark is embedded, the

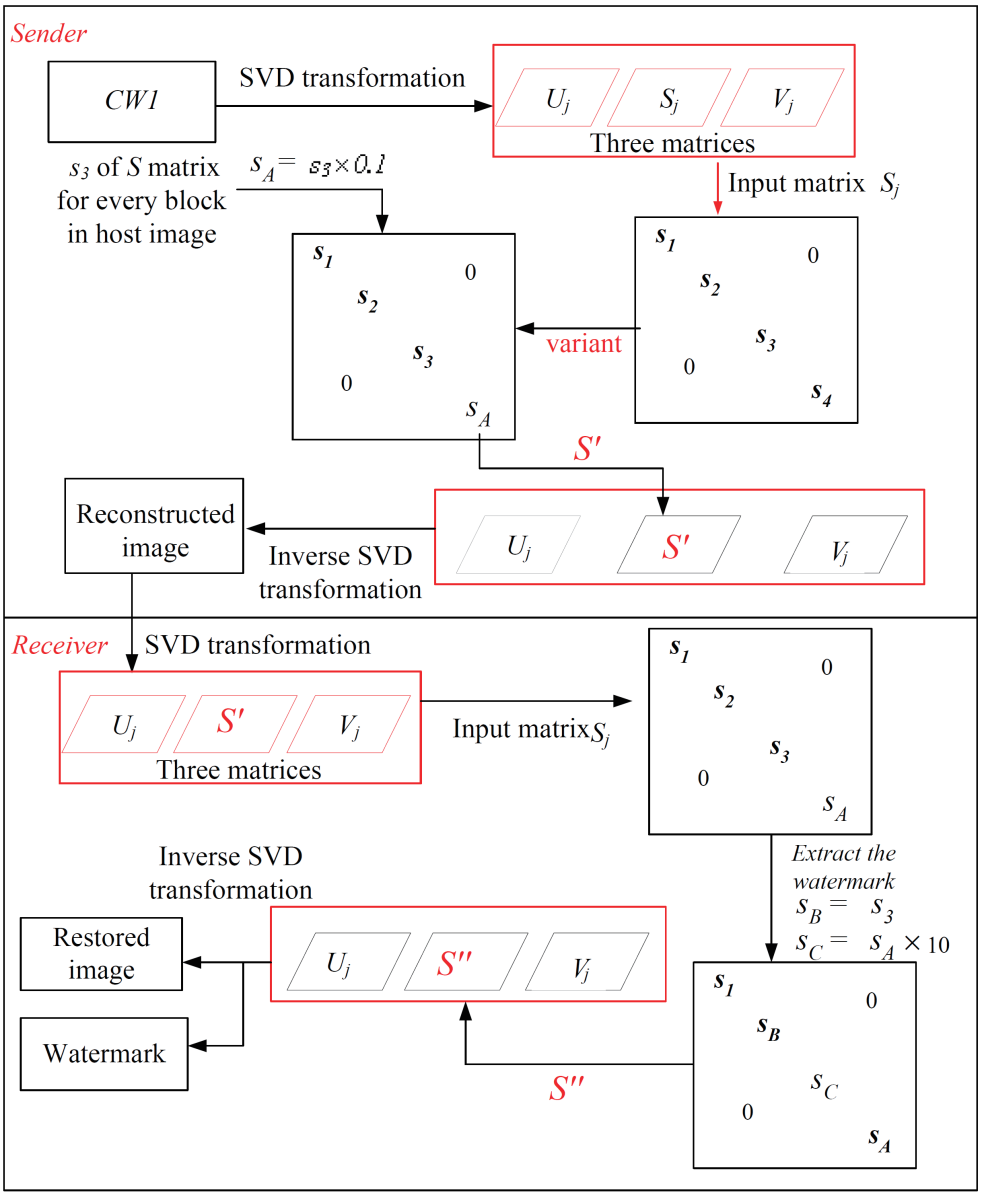


FIGURE 8. Concept of the variant

*PSNR*s of the *CWI* with our primary scheme, the *PSNR*s of the *CWI* with our variant and the *PSNR*s of the restored *CWI* with our variant. We can see that all*PSNR*s listed in Table 11 are higher than those listed in Table 10, which means that the variant improves the image quality of the compressed watermarked images. Comparing Tables 9 and 12, we can see that, on average, the difference between the compressed host image and the

TABLE 9. *PSNR*s (*dB*) of compressed host images

QF	Lena	Pepper	F16	Barbara	Zelda	Baboon	Gold Hill
90	43.13	42.24	42.65	40.51	45.09	38.53	39.44
80	40.68	39.97	40.03	37.26	42.06	34.54	36.69
70	39.31	38.76	38.58	35.53	40.58	32.50	35.37

restored image with our variant is less than 2 *dB*. Furthermore, the restored image quality is up to 39.94 *dB* for "Zelda", even with the quality factor set as 70.

TABLE 10. *PSNRs* (*dB*) of compressed images with primarily proposed scheme

QF	Lena	Pepper	F16	Barbara	Zelda	Baboon	Gold Hill
90	33.67	33.97	33.35	29.67	35.29	31.03	32.96
80	33.78	34.19	33.52	29.37	35.81	30.05	32.38
70	34.02	34.54	33.80	29.13	36.13	29.40	32.32

TABLE 11. *PSNRs* (*dB*) of compressed images with variant

QF	Lena	Pepper	F16	Barbara	Zelda	Baboon	Gold Hill
90	33.71	34.02	33.40	29.70	35.31	31.07	33.02
80	33.80	34.21	33.55	29.41	35.82	30.10	32.43
70	34.03	34.55	33.81	29.18	36.13	29.42	32.34

TABLE 12. *PSNRs* (*dB*) of restored image with variant

QF	Lena	Pepper	F16	Barbara	Zelda	Baboon	Gold Hill
90	40.62	40.65	39.87	35.31	42.24	36.80	39.21
80	38.72	38.67	38.12	33.55	40.90	33.57	36.28
70	37.64	37.68	36.94	32.18	39.94	31.88	34.95

With each preserved s_3 embedded into s_4 after the second SVD transformation, will such a modification affect the *BCR* of the extracted watermark? Table 13 presents the extracted watermarks and their *BCR*s for seven *CWI*s with our variant. Although the *BCR* decreases gradually while the QF of JPEG compression gets lower, the visual quality of the extracted "CCU" logo is still satisfactory when the QF is 70. In the worst case, the extracted "CCU" of "Baboon" still can be verified by the human vision system.

6. **Conclusions.** This paper presents a novel SVD-based watermarking scheme that encompasses a restoring property. The proposed scheme explores features of the S matrix of each block in a host image to provide more robust watermarking that is more resistant to different types of image processing. Experimental results confirm that the performance of our proposed watermarking scheme is better than other similar schemes. To extend the application of the proposed scheme into commercial applications, we also propose a variant which is an extension of the primary scheme. Using our variant, even though a watermarked image is compressed by JEPG with a quality factor of 70, its image quality still can be restored to a higher *PSNR* which is very close to that of JPEG compressed image without watermark. Experiments confirm that our variant successfully reduces the difference between the restored image and its compressed host image to less than 2 *dB*. Even though the QF of JPEG compression is set as 70, the visual quality of each extracted watermark is still acceptable.

TABLE 13.Extracted watermark and its corresponding *BCR* under JPEG compression qualities 90, 80 and 70 with our variant

Watermarked images	The extracted watermark and its corresponding *BCR*		
	90	80	70
Lena	 (*BCR* = 98.73 %)	 (*BCR* = 91.30 %)	 (*BCR* = 87.42 %)
Pepper	 (*BCR* = 98.33%)	 (*BCR* = 90.23 %)	 (*BCR* = 85.27 %)
F16	 (*BCR* = 97.70 %)	 (*BCR* = 87.76 %)	 (*BCR* = 84.17 %)
Barbara	 (*BCR* = 98.68 %)	 (*BCR* = 88.79 %)	 (*BCR* = 85.08 %)
Zelda	 (*BCR* = 97.82 %)	 (*BCR* = 95.11 %)	 (*BCR* = 91.89 %)
Baboon	 (*BCR* = 97.60 %)	 (*BCR* = 86.81 %)	 (*BCR* = 83.88 %)
Gold Hill	 (*BCR* = 97.80 %)	 (*BCR* = 88.40 %)	 (*BCR* = 86.71 %)

So far, our variant works well when the QF of JEPG compression is equal to or greater than 70. To enhance its practicality, improving it to work at a lower QF of JPEG compression will be our future work.

REFERENCES

[1] L. L. An, X. B. Gao, X. L. Li, D. C. Tao, C. Deng, and J. Li, Robust reversible watermarking via clustering and enhanced pixel-wise masking, *IEEE Trans. Image Processing*, vol. 21, no. 8, 2012, pp. 3598-3611.

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

[3] A. Benhocine, L. Laouamer, L. Nana, and A. C. Pascu, New images watermarking scheme based on singular value decomposition, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, No. 1, pp. 9-18, 2013.

[4] D. V. S. Chandra, Digital image watermarking using singular value decomposition, *Proc. of The 45th Midwest Symposium on Circuits and Systems (MWSCAS 2002)*, vol. 3, 2002, pp. 264-267.

[5] C. C. Chang, P. Tsai, and C. C. Lin, SVD-based digital image watermarking scheme, *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577-1586, 2005.

[6] C. C. Chang, and C. Y. Lin, Reversible steganography for VQ-compressed images using side matching and relocation, *IEEE Trans. Information Forensics and Security*, vol. 1, no. 4, pp. 493-501, 2006.

[7] C. C. Chang, W. L. Tai, and C. C. Lin, A reversible data hiding scheme based on side match vector quantization, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 16, no. 10, 2006, pp. 1301-1308.

[8] C. C. Chang, Y. P. Hsieh, and C. Y. Lin, Lossless data embedding with high embedding capacity based on declustering for VQ-Compressed images, appear to *IEEE Trans. Information Forensics and Security*, vol. 2, no. 3, pp. 341-349, 2007.

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

[10] B. Chen, S. Latifi, and J. Kanai, Edge enhancement of remote image data in the DCT domain, *Image and Vision Computing*, vol. 17, no. 12, pp. 913-921, 1999,.

[11] W. C. Chu, DCT-based image watermarking using subsampling, *IEEE Transactions on Multimedia*, vol. 5, no. 1, 2003, pp. 34-38.

[12] K. L. Chung , W. N. Yang, Y. H. Huang, S. T. Wu, and Y. C. Hsu, On SVD-based watermarking algorithm, *Applied Mathematics and Computation*, vol. 188, no. 1, pp. 54-57, 2007.

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

[14] G. H. Golub and C. Reinsch, Singular value decomposition and least squares solutions, *Numerische Mathematik*, vol. 14, pp. 403-420, 1970.

[15] Z. Hou, Adaptive singular value decomposition in wavelet domain for image denoising, *Pattern Recognition*, vol. 36, no. 8, pp. 1747-1763, 2003.

[16] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, pp. 875-882, 2001.

[17] C. T. Hsu, and J. L. Wu, Hidden digital watermarks in images, *IEEE Trans. Image Processing*, vol. 8, no. 1, pp. 58-68, 1999.

[18] Y. Hu, S. Kwong, and J. Huang, An algorithm for removable visible watermarking, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 16, no. 1, pp. 129-133, 2006.

[19] M. S. Hwang, C. C. Chang, and K. F. Hwang, A watermarking technique based on one-way hash functions, *IEEE Trans. Consumer Electronics*, vol. 45, no. 2, pp. 286-294, 1999.

[20] M. Iwata, and A. Shiozaki, Watermarking method for embedding index data into images utilizing features of wavelet transform, *IEICE Trans. Fundamentals*, vol. E84-A, no.7, pp. 1772-1778, 2001.

[21] M. Kutter, F. D. Jordan, and F. Bossen, Digital watermarking of color images using amplitude modulation, *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326-332, 1998.

[22] C. H. Lee, and Y. K. Lee, An adaptive digital watermarking technique for copyright protection, *IEEE Trans. Consumer Electronics*, vol. 45, no. 4, pp. 1005-1015, 1999.

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

[24] Z. M. Lu, and X. W. Liao, Counterfeiting attacks on two robust watermarking schemes, *International Journal of Innovative Computing, Information and Control*, vol. 2, no. 4, pp. 841-848, 2006.

[25] A. Munteanu, J. Cornelis, G. V. D. Auwera and P. Cristea, Wavelet image compression – the quadtree coding approach, *IEEE Trans. Technology in Biomedicine*, vol. 3, no. 3, pp. 176-185, 1999.

[26] N. Nikolaidis and I. Pitas, Robust image watermarking in the spatial domain, *Signal Processing*, vol. 66, no. 3, pp. 385-403, 1998.
[27] M. P. Queluz, Spatial watermark for image content authentication, *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 275-285, 2002.
[28] J. S. Walker, Fast Fourier transforms, 2nd ed., *Boca Raton*, FL: CRC Press, 1996.
[29] X. P. Zhang, S. Z. Wang, Z. X. Qian, and G. R. Feng, Reference sharing mechanism for watermark self-embedding, *IEEE Trans. Image Processing*, vol. 20, no. 2, pp. 485-495, 2011.