Image Watermarking Scheme Based on Scale-Invariant Feature Transform

Wan-Li Lyu [1, 2], Chin-Chen Chang [2, 3], Thai-Son Nguyen [2, 4] and Chia-Chen Lin[5]
[1] Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University
Hefei 230039, China
[e-mail: wanly_lv@163.com]
[2] Department of Information Engineering and Computer Science,Feng Chia University
Taichung 40724, Taiwan, R.O.C
[e-mail: ccc@cs.ccu.edu.tw]
[3] Department of Computer Science and Information Engineering,
Asia University
Taichung 41354, Taiwan, R.O.C
[4] Department of Information Technology, Tra Vinh University
Tra Vinh Province, Vietnam
[e-mail: thaison@tvu.edu.vn]
[5] Department of Computer Science and Information Management,
Providence University
Taichung 43301, Taiwan, R.O.C
[e-mail: mhlin3@pu.edu.tw]
*Corresponding author: Chin-Chen Chang

Received June 3, 2014; revised August 20, 2014; accepted September 10, 2014; published October 31, 2014

Abstract

In this paper, a robust watermarking scheme is proposed that uses the scale-invariant feature transform (SIFT) algorithm in the discrete wavelet transform (DWT) domain. First, the SIFT feature areas are extracted from the original image. Then, one level DWT is applied on the selected SIFT feature areas. The watermark is embedded by modifying the fractional portion of the horizontal or vertical, high-frequency DWT coefficients. In the watermark extracting phase, the embedded watermark can be directly extracted from the watermarked image without requiring the original cover image. The experimental results showed that the proposed scheme obtains the robustness to both signal processing and geometric attacks. Also, the proposed scheme is superior to some previous schemes in terms of watermark robustness and the visual quality of the watermarked image.

Keywords: Geometric attack, high quality, image watermarking, SIFT

http://dx.doi.org/10.3837/tiis.2014.10.018

1. Introduction

With the rapid developments in multimedia technology and the Internet over the last decade, digital data, i.e., images, videos, audio, and text, can be easily copied and altered when they are transmitted via the Internet. Hence, protection of the ownership of digital data has become a very essential issue. Many solutions have been proposed to solve this issue, and digital watermarking is one of the most promising. Watermarking schemes can embed specific data, also referred to as a 'watermark,' into the original image. The watermark cannot be easily seen, which means that an unauthorized person cannot visually detect that embedded data in the content of the watermarked image. To prove the ownership of the image, the embedded watermark is extracted and detected. In watermarking applications, it is most important that the watermark must be sufficiently robust to withstand different attacks. There are two types of watermark attacks, i.e., signal processing and geometric attacks. Watermarking schemes [1-17, 20-25] can be classified into template-based [1,2], invariant transform domain-based [3-5], histogram-based [6,7], moment-based [8,9], and feature-based schemes [10-17].

Many feature-based image watermarking algorithms [10-17] have been introduced in the literature. This is because these algorithms can resist signal processing attacks, and they are robust against geometric attacks. In [13], Bas et al. utilized the Harris detector technique to determine the feature points from the original image. A Delaunay Tessellation technique is implemented to divide the image into a set of disjointed triangles. Then, the watermark is embedded into each triangle of the tessellation. However, in this scheme, the feature points extracted from the original image and from the attacked image are not the same. In other words, their schemes cannot extract exactly the embedded watermark once the watermarked image is attacked. In [11], Li and Guo applied the Harris detector to determine the non-overlapped circular areas and embedded the watermark into the spatial domain of these areas. However, in using the spatial domain for embedding the watermark, their scheme had limited robustness against both signal processing attacks and geometric attacks. In [14,15], Seo and Yoo proposed two watermarking schemes using a multi-scale Harris detector. In their schemes, the image is decomposed into disjointed, local circular regions. In [14], a circular, symmetric watermark was embedded after scale normalization processing according to the local characteristic scale, whereas, in [15], Seo and Yoo extract the selected regions and the watermark is embedded in these regions after geometric normalization processing adopting to the shapes of these regions. In [12], Lee et al. extracted local circular regions by using scale-invariant feature transform (SIFT). In the extracted local circular regions, pixel values are modified to embed the watermark. Because the watermark is embedded in spatial domain in these schemes [11, 12, 14, 15], their embedded watermarks are less robust. To further improve the robustness of watermarking schemes, Wang et al. [17] proposed the feature-based watermarking scheme in the transform domain. Their scheme achieved high robustness of the watermark against signal processing attacks. However, the size of the watermark is quite small, i.e., only32 bits. To enhance the watermark's robustness and size, Li et al. [16] proposed a new watermarking scheme in the DWT domain. The watermark is first resized to the size of the horizontal and vertical high-frequency DWT subbands of the images. Then, the difference between the horizontal and vertical high-frequency DWT coefficients is expanded to embed the watermark. Their scheme outperformed schemes proposed by Lee et al. [12] and Wang et al. [17].

In this paper, a new, robust, watermarking scheme is proposed. The proposed scheme uses the SIFT algorithm to extract the feature areas for embedding the watermark. To achieve better robustness, the DWT coefficients of the SIFT areas is utilized for carrying the watermark. Our experimental results showed that the proposed scheme is resilient to both signal processing attacks and geometric attacks, e.g., Salt and Pepper noise, Gaussian filtering, rotation, and cropping. In addition, the visual quality of the watermarked image is excellent in the proposed scheme.

The rest of this paper is organized as follows. Section 2 provides the concept of the SIFT algorithm [18] to give readers sufficient background knowledge. Section 3 describes the proposed scheme, consiting of the watermark embedding and extracting phases. Section 4 presents the experimental results and illustrates the superiority of the proposed scheme. Finally, we present our conclusions in Section 5.

2. SIFT Algorithm

In 2004, Lowe [18] first introduced the scale-invariant feature transform (SIFT) algorithm, which proved that the extracted feature points are stable to geometric transformations, i.e., scaling, rotation, and translation transformation. The SIFT algorithm extracts the feature points from the scale space of the image. The scale space of image is denoted as L(x, y, α), and is defined in Equation (1):

$$L(x, y, \alpha) = I(x, y) * Gau(x, y, \alpha), \tag{1}$$

where $I(x, y)$ is the digital image, * denotes the convolution operation, and $Gau(x, y, \alpha)$ is the variable-scale Gaussian kernel with a standard deviation α. $Gau(x, y, \alpha)$ is defined in Equation (2):

$$Gau(x, y, \alpha) = \frac{1}{2\pi\alpha^2} e^{-(x^2+y^2)/2\pi^2}. \tag{2}$$

To detect the SIFT feature points, scale-space extrema in the difference-of-Gaussian (DoG) function, $D(x, y, \alpha)$ is applied, and it can be computed using Equation (3):

$$\begin{aligned} D(x, y, \alpha) &= I(x, y) * (Gau(x, y, k\alpha) - Gau(x, y, \alpha)) \\ &= L(x, y, k\alpha) - L(x, y, \alpha), \end{aligned} \tag{3}$$

where k is a constant, multiplicative factor; $Gau(x, y, k\alpha)$ is the variable-scale Gaussian kernel with the standard deviation α and the constant multiplicative factor k; and $L(x, y, k\alpha)$ is the scale space of the image with the constant multiplicative factor k. To determine the candidates of the difference-of-Gaussian function, $D(x, y, \alpha)$, each point is first compared with its eight neighbors points in the current image. Then, it is also compared to the nine neighbors in the scale above and below. The point is selected only when its value is larger or smaller than the value of all of these neighbors. In addition, the positions that have low contrast or are poorly localized are deleted by stability function.

After obtaining the feature points, one or more orientations are assigned to each point on the basis of the local image gradient directions. Let the gradient magnitude be gm(x, y), and orientation of the feature point (x, y) be $O(x, y)$, which are calculated using Equations (4)-(5), respectively.

$$gm(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x, y+1) - L(x, y-1))^2} \tag{4}$$

$$O(x,y)=\tan^{-1}((L(x+1,y)-L(x-1,y))/(L(x,y+1)-L(x,y-1))), \quad (5)$$

where L is the Gaussian smoothed image [3]. The descriptor of feature area is constructed by first calculating the gradient magnitude and orientation at each image sample point in an area around the feature point location. Then, these samples are accumulated into orientation histograms that summaries the contents over 4 × 4 sub-areas, with the length of each orientation bin corresponding to the sum of the gradient magnitudes near that direction within the area. The feature area is formed with containing the values of all the orientation histograms entries, corresponding to the lengths of the orientation bins. In the SIFT feature descriptor, the radius of an area around the feature point is determined as a constant times the detection scale of the feature point, which can be motivated by the property of the scale selection mechanism in the feature point detector of returning a characteristic size estimate associated with each feature point [26].The reader can refer to [18] for the detailed algorithms that are used to extract the features of SIFT. In the research reported in this paper, the SIFT algorithm was used to extract the feature areas of the image in which the watermark was embedded.

3. The Proposed Schemes

After applying the SIFT algorithm, several SIFT feature areas were determined in an image. However, a problem arises if the SIFT feature areas are generated by using the SIFT algorithm, since some of the feature areas may overlap. In order to hide the watermark, some local areas must be removed. If two areas are overlapped, only the area whose size is larger than or equal to 60 × 60 pixels is reserved. The main reason is that areas of these sizes are most suitable for embedding watermark sizes of 32 × 32 pixels in the proposed scheme. In addition, if two areas larger than 60 × 60 pixels are overlapped, only the one that has the larger *DoG* function value, calculated by Equation (3), is reserved because the larger *DoG* value offers the better stability. **Fig. 1** shows examples of the extracted SIFT feature areas using SIFT.

Fig. 1. Example of extracted SIFT feature areas from the image Lena

Each extracted SIFT area is processed independently for embedding the watermark. To further improve the robustness of the watermark, N extracted SIFT areas are used to carry the same copy of the watermark. Notably, since all circular SIFT areas larger than 60 × 60 pixels are selected for embedding the watermark, then N is equal to 20 if there are 20 areas having the size larger than 60 × 60 pixels. In addition, watermark embedding and watermark detection are performed in the DWT domain. DWT is a mathematical technique that can be used to transform the image in the spatial domain into the frequency domain. Basically, the DWT image is obtained repeatedly by filtering the current image on a row-by-row and a

column-by-column. After each level DWT transformation, four sub-bands, i.e., *CAi*, *CHi*, *CVi*, and *CDi*, are generated. **Fig. 2** shows an example of one-level DWT transformation.

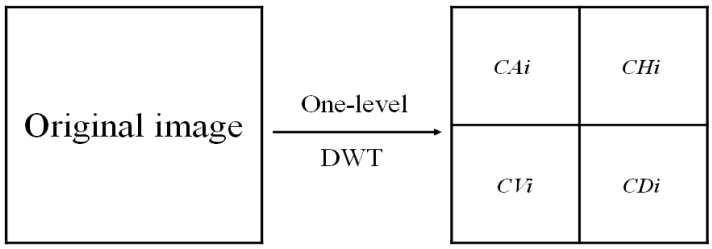

Fig. 2. Example of one-level DWT transformation

In the DWT domain, the *CAi* sub-band is not used for carrying a watermark. It is because *CAi* is a low-frequency sub-band, and this sub-band will contain essential information about the image. Therefore, small modifications in this sub-band can easily cause the image to be distorted. Similarly, embedding the watermark into sub-band *CDi* also is not applied, because this sub-band can be eliminated easily, for example, via JPEG compression. Thus, in the work described in this paper, the *CHi* and *CVi* sub-bands were used to carry the watermark. In addition, since the watermark W is partitioned and embedded into both the horizontal and vertical frequency sub-bands, i.e., CH_i, and CV_i, of the selected SIFT areas. Therefore, the size of watermark W that is used should be the smaller or equal to the half size of the horizontal and vertical frequency sub-bands, i.e., CH_i, and CV_i, of the selected SIFT areas. The main reason is to guarantee robustness of watermark when the watermark with the original size is completely embedded into these sub-bands.

In this paper, to resist the geometric attacks, i.e. scaling and rotation, the circular feature area is used for watermarking. As a result, scaling invariance can be obtained because the radius of area is directly proportional to the scale of feature area. Moreover, to achieve the rotation invariance, circular area should be required. **Fig. 3** shows how pixels present in the circular are and rectangle area. The proposed scheme contains two phases, i.e., the embedding phase and the extracting phase, and these two phases are described in Subsections 3.1 and 3.2, respectively.

(a) Rectangle area (b) Circular area

Fig. 3. Different shapes of feature areas

3.1 Watermark Embedding Phase

In this subsection, the same watermark is embedded repeatedly into N extracted SIFT areas. **Fig. 4** shows the flowchart of watermark embedding phase. Then the watermark embedding algorithm is described.

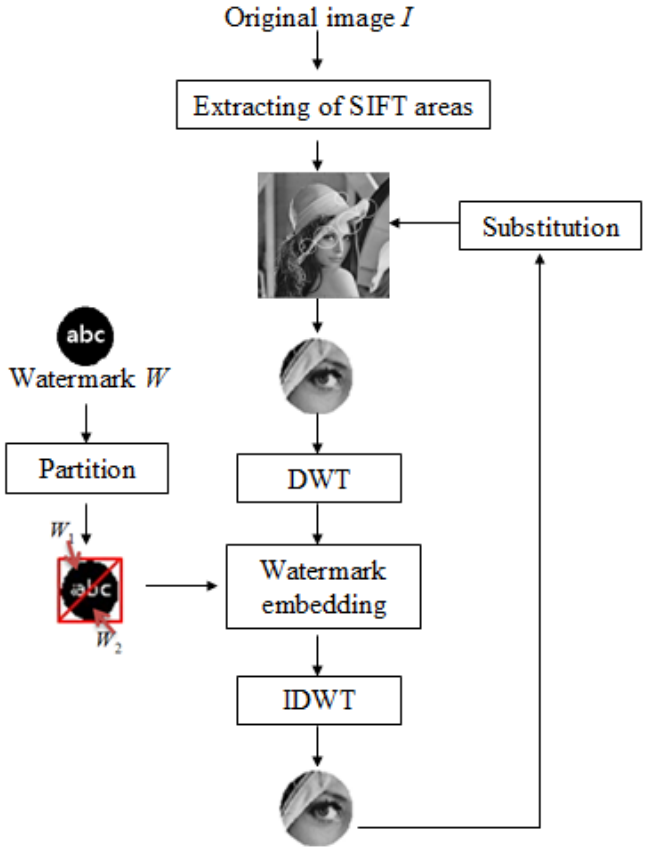

Fig. 4. Flowchart of watermark embedding phase

Step 1: First, N SIFT areas having its size larger than 60 × 60 pixels are selected from the original image, and the size of the SIFT area is determined by the size of the watermark. In this paper, the size of the SIFT area is larger than 60 × 60 pixels, and the size of the image is 512 × 512 pixels; the size of the watermark can be 32 × 32 pixels.

Step 2: Each selected SIFT area is resized to 64 × 64 pixels, and one-level DWT is applied to yield four frequency sub-bands $\{CA_i, CH_i, CV_i, CD_i\}$.

Step 3: Partition the watermark image W into two parts, W_1 and W_2, as shown in **Fig. 4**.

Step 4: Embed the two parts of the watermark image, W_1 and W_2, by modifying the coefficients in the horizontal and vertical frequency sub-bands, i.e., CH_i, and CV_i, respectively, as shown in **Fig. 5.** It is noticeable that only the DWT coefficients locate inside the left, upper half of the inscribed circle, which is modified for embedding the watermark.

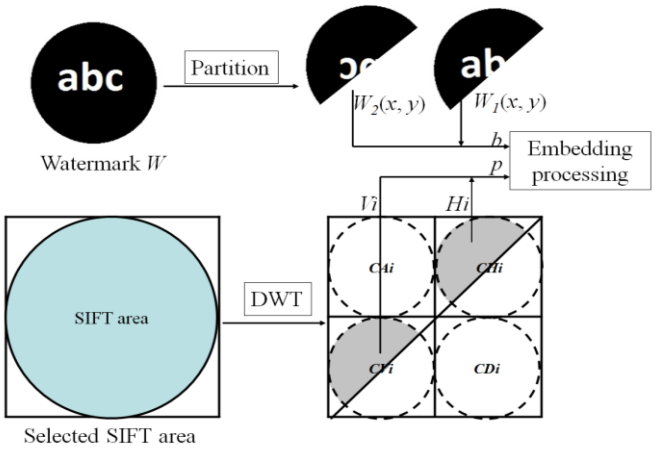

Fig. 5. Demonstration of watermark embedding

In the proposed scheme, W_1 is embedded into the horizontal frequency sub-band CH_i, and W_2 is embedded into the vertical frequency sub-band CV_i. To embed watermark bit $W_1(x, y)$, the corresponding horizontal, high-frequency coefficient, that has the similar coordinates are selected as $CHi(x, y)$, is used. Then, the two digits Hi of the fractional portion of $CHi(x, y)$ are extracted to embed watermark bit W_1 (x, y). Notably, the value of Hi is extracted from the value of CHi, and Hi is the two digits that are selected starting from the first non-zero digit of the fractional portion of CHi. For example, if $CHi(x, y) = 0.00\mathbf{10}52$, the value of Hi will be **10**. Similarly, $W_2(x, y)$ is embedded into the two digits Vi that are selected starting from the first non-zero digit of the fractional portion of $CVi(x, y)$. To explain further, let b denote $W_1(x, y)$ (or W_2 (x, y)) and let p denote the result of $Hi \bmod T$ (or $Vi \bmod T$). Note that Hi (or Vi) is two digits that are selected starting from the first non-zero digit of the fractional portion of $CHi(x, y)$ (or $CVi(x, y)$), hence, Hi (or Vi) is in range [10, 99]. Notably, the value of Vi is extracted from the value of CVi, and Vi is first two non-zero digits of the fractional portion of CVi. Here, T is the threshold value. Therefore, $p = Hi \bmod T$ (or $Vi \bmod T$) must be in the range $[0, T)$. The watermark bit b is embedded into the value p using Equation (6):

$$p' = \begin{cases} \left\lfloor \dfrac{p + \frac{T}{4}}{2} \right\rfloor & \text{if } b = 0 \text{ and } p \le \dfrac{T}{2} \\ \left\lfloor \dfrac{p - \frac{T}{4}}{2} \right\rfloor & \text{if } b = 0 \text{ and } p > \dfrac{T}{2}, \\ \left\lfloor \dfrac{p + \frac{5T}{4}}{2} \right\rfloor & \text{if } b = 1 \text{ and } p \le \dfrac{T}{2} \\ \left\lfloor \dfrac{p + \frac{3T}{4}}{2} \right\rfloor & \text{if } b = 1 \text{ and } p > \dfrac{T}{2} \end{cases} \tag{6}$$

where T is the threshold value; p is the result value of $Hi \bmod T$ if CHi is used to embed watermark $W_1(x, y)$ (or $Vi \bmod T$, if CVi is used to embed watermark $W_2(x, y)$); and b is the watermark bit $W_1(x, y)$ (or $W_2(x, y)$). **Fig. 6** shows the value of p and the value of p' based on the threshold T after embedding watermark bit b.

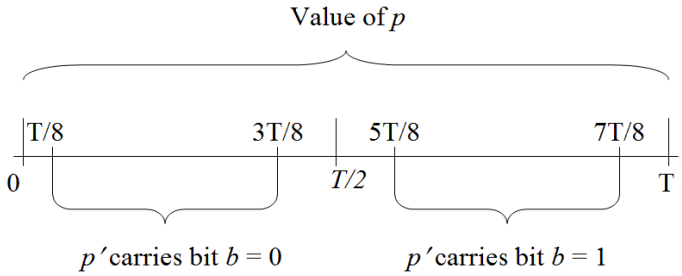

Fig. 6. Value of p' after embedding the watermark

Step 5: If CHi is used to embed watermark $W_1(x, y)$, set CHi' to the value of $Hi' = p'$. Otherwise, if CVi is used to embed watermark $W_2(x, y)$, set CVi' to the value of $Hi' = p'$.

Step 6: Utilize one-level IDWT to reconstruct the watermarked SIFT area. This area is resized to its original size and is used to substitute for the original SIFT area in the image.

Step 7: Repeat Steps 2 through 5 until N SIFT areas have been completely processed.

3.2 Watermark Extracting Phase

This Subsection describes how watermark W is extracted from the watermarked image. The extracting algorithm is implemented without requirement of the original image. Therefore, the proposed scheme meets the condition of blindness. Some of the steps in the watermark extracting algorithm are exactly the same as those used in watermark embedding phase. Specifically, SIFT algorithm is used to extract N watermarked SIFT areas from the watermarked image and resized them to 64 × 64 pixels. Then, the watermark is extracted from each watermarked SIFT area. **Fig. 7** shows the watermark extracting processes and the watermark extracting algorithm is performed in each SIFT area, as shown below.

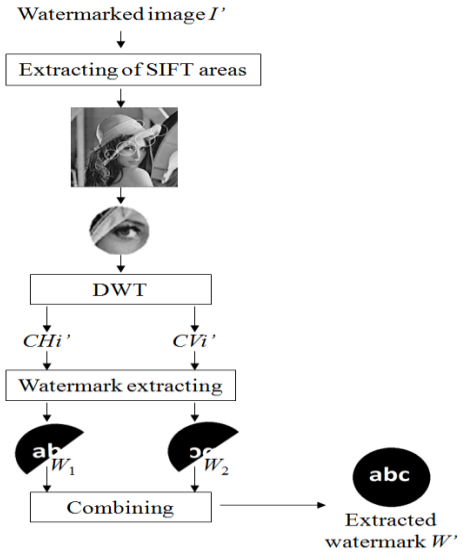

Fig. 7. Watermark extracting procedure

Step 1: Utilize one-level DWT on each watermarked SIFT area to produce four frequency sub-bands {*CAi'*, *CHi'*, *CVi'*, *CDi'*}.

Step 2: For the coefficients in two sub-bands, i.e., *CHi'* or *CVi'*, the value *p'* is determined as first two non-zero digits of the fractional portion of *CHi'* or *CVi'* to extract watermark bit *b'*. Note that only coefficients inside the left, upper half of the inscribed circle of sub-bands, *CHi'* and *CVi'*, are processed. In this scenario, if *b'* is extracted from *CHi'* coefficients (or *CVi'* coefficients), it belongs to W_1 (or W_2), respectively. Watermark bit *b'* is extracted using Equation (7).

$$b' = \begin{cases} 0 & if \quad T/8 \le p' \le 3T/8 \\ 1 & if \quad 5T/8 \le p' \le 7T/8 \end{cases}. \tag{7}$$

Step 3: Combine two watermarks W_1 and W_2 to obtain the extracted watermark *W'*. Then, based on the demonstration of the extracted watermark, the final decision will be made. In addition, the watermark similarities should be calculated to judge objectively.

4. Experimental Results

In this section, the performance of the proposed scheme in terms of the watermark's being invisible and robustness is demonstrated. The experiments were performed on a standard image with the size of 512 × 512 pixels. The watermark is a circular binary image size of 32 × 32 pixels. *N* SIFT areas were selected for embedding the watermark. In this experiment, three different values of *N*, i.e. 3, 4, and 5, are used.

The peak signal-to-noise ratio (PSNR) was used to estimate the visual qualiy of the watermark. The PSNR was computed using Equation (8):

$$PSNR = 10\log_{10}\left(\frac{255^2}{(1/M)\sum_{i=1}^{M}(I_i - I'_i)}\right), \tag{8}$$

where *M* is the size of the original image, and I_i and I'_i are the pixel values before and after embedding the watermark, respectively. **Table 1** lists the PSNRs of the watermark image with different values of threshold *T*. It is apparent that the proposed scheme provided watermarked images with high visual quality and different values of threshold *T*. **Fig. 8** shows image Lena before and after the watermark was embedded. **Fig. 8** clearly shows that the proposed scheme made the watermark invisible when the value of PSNR is greater than 84 dB.

Table 1.. PSNR of the watermarked image with different values of threshold *T*

Values of threshold *T*	20	30	40	50
PSNR	84. 70	84.69	84.68	84.67

(a) Original image (b) Watermarked image (84.69 dB)

Fig. 8. Watermark's invisibility

To demonstrate the robustness of the proposed scheme, we use the normalized correlation coefficient (*NC*) to measure the similarity between the embedded watermark *W* and the extracted watermark *W'*. *NC* is calculated using Equation (9):

$$NC = \frac{1}{W_h \times W_w} \sum_{i=0}^{W_{h-1}} \sum_{j=0}^{W_{w-1}} W(i,j) \times W'(i,j), \tag{9}$$

where W_h and W_w are the height and width of the embedded watermark, respectively. Note that, in this experiment, the highest NC value from *N* SIFT areas is selected for comparisons.

Fig. 9 shows performance of the proposed scheme with several thresholds *T*, i.e., 20, 30, 40, and 50. To obtain the tradeoff between visual quality of the watermarked image and robustness, the threshold $T = 30$ was selected in the proposed scheme.

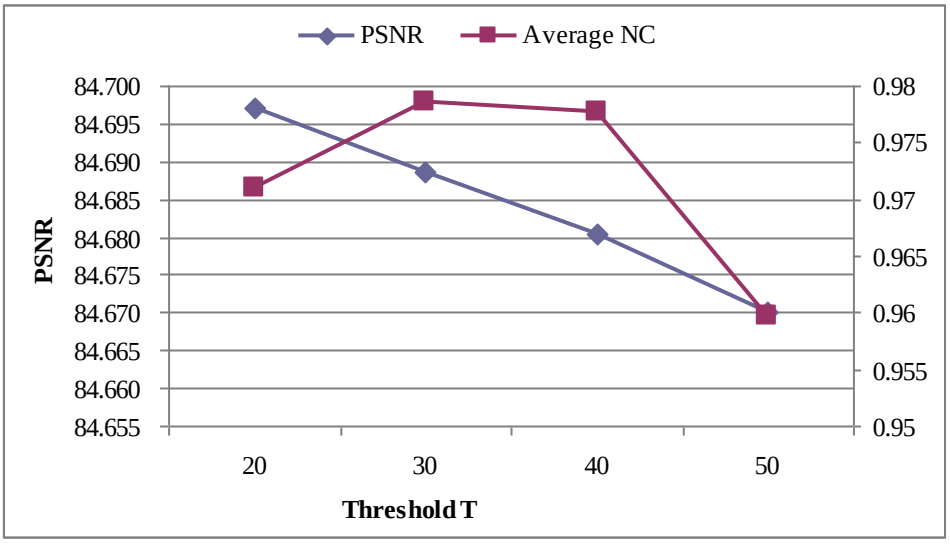

Fig. 9. Performance of the proposed scheme with several thresholds

Signal processing and geometric attacks listed in the benchmark software, Stirmark 4.0 [19], were used on the watermarked images. These attacks try to weaken or remove the embedded

watermark from the watermarked images. **Fig. 10** shows that the embedded watermark can be extracted clearly from all watermarked images under Salt and Pepper noise, JPEG 100, and Gaussian attacks with different parameters. As can be seen in **Fig. 10,** the proposed scheme obtained a high value of *NC*, i.e., greater than 0.9. This indicates that our proposed scheme was resilient against these attacks and that it ensured the high visual quality of the embedded watermarked images, as shown in **Table 1**.

Fig. 10. Watermarked images, extracted watermarks, and *NC* values for Salt and Pepper noise, JPEG 100, and Gaussian attacks

Fig. 11 shows the results of the proposed scheme for rotation attacks and cropping attacks. In the rotation attacks, three cases of rotating the watermarked images were simulated, i.e., 2^{o}, 5^{o}, and 10^{o}. In the cropping attacks, three different cases were performed to crop three watermarked images. In the first case, the corner of the watermarked image was cropped by 25%. In the second and the third cases, the outsides of the watermarked images were cropped by 50% and 75%, respectively. **Fig. 11** shows that the watermark was extracted completely from the watermarked images.

Fig. 10. Watermarked images, extracted watermarks, and *NC* values for rotation and cropping attacks

To further validate the proposed scheme, we compared it with two previous schemes [12, 16]. These schemes were selected to estimate the proposed scheme because they are similar to the proposed scheme in terms of using invariant feature points to conceal the watermark. **Table 2** shows that our proposed scheme obtained much higher PSNR than those of the previous schemes [12, 16], even though the proposed scheme and Li et al.'s scheme both used the DWT domain to embed the watermark. However, in [16], Li et al. modified the horizontal and the vertical high-frequency DWT coefficients to hide the watermark bits. Whereas, the proposed scheme only hides the watermark bits into the fractional portion of the horizontal or the vertical high-frequency DWT coefficients. Consequently, more distortions of the watermarked images occurred in Li et al.'s scheme than in our proposed scheme.

Table 2. PSNR of watermarked and original images (dB)

Schemes	Li et al.'s scheme [16]	Lee et al.'s scheme [12]	Proposed scheme
PSNRs	36.2	40.8	84.6

Table 3 compares the robustness of the watermarks for Li et al.'s scheme, Lee et al.'s scheme, and our proposed scheme, and it shows that the proposed scheme had greater robustness. In Lee et al.'s scheme, the pixels in the SIFT regions are modified to embed the watermark. Hence, since more pixels have their values altered in an attack, the extracted watermark will have more distortion. Instead of embedding the watermark in the spatial domain, Li et al.'s scheme embeds watermark into the DWT domain. As a result, their scheme obtained higher robustness than Lee et al.'s scheme. However, in Li et al.'s scheme, the difference between the horizontal and vertical high frequency DWT coefficients was expanded to embed the watermark. Therefore, if the value of one of the horizontal or the vertical high frequency DWT coefficients is modified, the extracted watermark bit will be changed. Conversely, in the proposed scheme, only the value of the horizontal or vertical high frequency DWT coefficient is altered to embed the watermark bit. **Table 4** shows the robustness of the proposed scheme with different values of N.

Table 3. Comparisons of the robustness of the watermark among Li et al.'s scheme, Lee et al.'s scheme, and the proposed scheme

Attacks	Li et al.'s scheme [16]	Lee et al.'s scheme [12]	Proposed scheme
No attack	0.963	0.728	0.982
JPEG 100	0.942	0.715	0.982
Median filter (3×3)	0.644	0.629	0.645
Shearing x-0%, y-5%	0.672	0.418	0.672
Center cropping (50%)	0.860	0.453	0.980
Scaling 0.9x	0.739	0.605	0.956
Scaling 1.2x	0.881	0.632	0.982
Rotation 2°	0.863	0.556	0.940
Rotation 5°	0.708	0.645	0.931
Rotation 10°	0.693	0.608	0.886

Table 4. Robustness of the proposed scheme with different values of N

Attacks	Proposed scheme		
	$N = 3$	$N = 4$	$N = 5$
No attack	0.982	0.982	0.982
JPEG 100	0.982	0.982	0.982
Median filter (3×3)	0.645	0.645	0.645
Shearing x-0%, y-5%	0.672	0.672	0.672
Center cropping (50%)	0.980	0.980	0.980
Scaling 0.9x	0.956	0.956	0.956
Scaling 1.2x	0.982	0.982	0.982
Rotation 2°	0.940	0.940	0.940
Rotation 5°	0.931	0.931	0.931
Rotation 10°	0.886	0.886	0.886

Based on experimental results we can see same results were obtained the same with different *N*s. This is because only the highest NC results are selected in our scheme, and the highest results can be obtained when N=3. Therefore, we set N as 3 here.

5. Conclusions

In this paper, a new image watermarking scheme was proposed to obtain high visual quality of the watermarked image and resistance against various attacks. In the proposed scheme, the SIFT feature areas are extracted, and a watermark image in binary form is embedded repeatedly into the horizontal and vertical high-frequency DWT coefficients of the selected SIFT feature areas. The experimental results showed that the proposed scheme is resilient to various attacks, i.e., signal processing and geometric attacks. In addition, the proposed scheme achieved better visual quality of the watermarked image and stronger robustness to various attacks than some previous schemes. It can be concluded that our watermarking scheme satisfied the demand of real-time applications. In some attacks, i.e. Median filter and Shearing, the robustness of the proposed scheme is not truly high. Therefore, to achieve better robustness to these attacks can be the future work.

References

[1] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermark," *IEEE Trans. Image Processing,* vol. 9, no. 6, pp. 1123-1129, 2000. Article (CrossRef Link)

[2] X. Kang, J. Huang, Y. Q. Shi and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuit Syst. Video Technol.*, vol. 13, no. 8, pp. 776-786, 2003. Article (CrossRef Link)

[3] Y. T. Lin, C. Y. Huang and G. C. Lee, "Rotation, scaling, and translation resilient watermarking for images," *IET Image Processing*, vol. 5, no. 4, pp. 328-340, 2011. Article (CrossRef Link)

[4] D. Zheng, J. Zhao and A. ElSaddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation," *IEEE Trans. Circuit Syst. Video Technol.*, vol. 13, no. 8, pp. 753-765, 2003. Article (CrossRef Link)

C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Proc.*, vol. 10, no. 5, pp. 767-782, 2001. Article (CrossRef Link)

[5] S. Roy and E. C. Chang, "Watermarking color histograms," *Proc. ICIP*, pp. 2191-2194, 2004. Article (CrossRef Link)

[6] S. Xiang, H. Joong and J. Huang, "Invariant image watermarking based on statistical feature in low-frequency domain," *IEEE Trans. Circuit and Syst. Video Technol.*, vol. 18, no. 6, pp. 777-790, 2008. Article (CrossRef Link)

[7] M. Alghoniemy and A. H. Tewfik, "Geometric invariant in image watermarking," *IEEE Trans. Image Processing*, vol.13, no. 2, pp. 145-153, 2004. Article (CrossRef Link)

[8] P. Dong, J. G. Brankow, N. P. Galatsanos, Y. Y. Yang and F. Davoine, "Digital watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2140-2150, 2005. Article (CrossRef Link)

[9] C. Deng, X. B. Gao, X. L. Li and D. C. Tao, "A Local Tchebichef moments-based robust image watermarking," *Signal Processing*, vol. 89, no.8, pp. 1531-1539, 2009. Article (CrossRef Link)

[10] L. D. Li and B. L. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks," *AEU-Int. J. Electron. Commun.*, vol. 63, no. 2, pp. 123-131, 2009. Article (CrossRef Link)

[11] H. Y. Lee, H. Kim and H. K. Lee, "Robust image watermarking using local invariant features," *Optical Engineering*, vol. 45, no.3, pp. 1-10, 2007. Article (CrossRef Link)

[12] P. Bas, J. Chassery and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans Image Processing*, vol. 11, no.9, pp. 1014-1028, 2002. Article (CrossRef Link)
[13] J. Seo and C. Yoo, "Localized image watermarking based on feature points of scale space representation," *Pattern Recognition*, vol. 37, no.7, pp. 1365-1375, 2004. Article (CrossRef Link)
[14] J. Seo and C. Yoo, "Image watermarking based on invariant region of scale-space representation," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1537-1549, 2006. Article (CrossRef Link)
[15] L. Li, J. S. Qian and J. S. Pan, "Characteristic region based watermark embedding with RST invariance and capacity," *AEU-Int. J. Electon. Commun.*, vol. 65, no. 5, pp. 435-442, 2011. Article (CrossRef Link)
[16] X. Y. Wang, J. Wu and P. P. Niu, "A new digital image watermarking algorithm resilient to desynchronization attacks," *IEEE Trans. Inf. Forensics Secur.*, vol.2, no. 4, pp. 655-663, 2007. Article (CrossRef Link)
[17] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004. Article (CrossRef Link)
[18] F. A. Petitcolas, "Watermarking scheme evaluation," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 58-64, 2000. Article (CrossRef Link)
[19] Abdelhamid Benhocine, Lamri Laouamer, Laurent Nana, and Anca Christine 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, January 2013. Article (CrossRef Link)
[20] Alimohammad Latif, "An Adaptive Digital Image Watermarking Scheme using Fuzzy Logic and Tabu Search," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 4, pp. 250-271, October 2013. Article (CrossRef Link)
[21] Hsiang-Cheh Huang and Feng-Cheng Chang, "Robust Image Watermarking Based on Compressed Sensing Techniques," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 2, pp. 275-285, April 2014. Article (CrossRef Link)
[22] H. W. Tian, Y. Zhao, R. R. Ni, L. M. Qin, X. L. Li, "LDFT-Based Watermarking Resilient to Local Desynchronization Attacks," *IEEE Trans. on Cybernetics*, vol. 43, no. 6, pp. 2190-2201, 2013. Article (CrossRef Link)
[23] J. S. Tsai, W. B. Huang, Y. H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," *IEEE Trans. on Image Process.*, vol. 20, no. 3, pp. 735-743, 2011. Article (CrossRef Link)
[24] X. B. Gao, C. Deng, X. L. Li, D. C. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," *IEEE Trans. Systems, Man, and Cybernetics - Part C: Applications and Reviews*, vol. 40, no. 3, pp. 278-286, 2010. Article (CrossRef Link)
[25] T. Lindeberg, "Feature detection with automatic scale selection," *International Journal of Computer Vision,* vol. 30, no. 2, pp. 79-116, 1998. Article (CrossRef Link)

Wan-Li Lyu was born in Anhui province, China, in 1974. She received the M.S. degree in computer science and technology with Guangxi University and the Ph.D. degree in computer science and technology with Anhui University. Since July 2004, s he is a Lecturer in School of Computer Science and Technology, Anhui University. Currently, she is a postdoctoral research fellow in Department of Information Engineering and Computer Science at Feng Chia University from August. 2013. Her current research interests include image processing, computer cryptography and information security.

Chin-Chen Chang received the B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from National Tsing Hua University, Hsinchu, Taiwan, and the Ph.D. degree in computer engineering from National Chiao Tung University, Hsinchu, in 1982. From 1980 to 1983, he was with the faculty of the Department of Computer Engineering, National Chiao Tung University. From 1983 to 1989, he was with the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the Head and a Professor with the Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the Dean of the College of Engineering, National Chung Cheng University. From August 1995 to October 1997, he was the Provost with National Chung Cheng University. From September 1996 to October 1997, he was the Acting President with National Chung Cheng University. From July 1998 to June 2000, he was the Director of the Advisory Office of the Ministry of Education of Taiwan. From 2002 to 2005, he was a Chair Professor with National Chung Cheng University. Since February 2005, he has been a Chair Professor with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung. He is also with the Department of Computer Science and Information Engineering, Asia University, Taichung. He has served as a Consultant with several research institutes and government departments. His current research interests include database design, data structures, computer cryptography, and image processing.

Thai-Son Nguyen received the bachelor degree in information technology from Open University, HCM city, Vietnam, in 2005. From December 2006, he has been lecturer of TraVinh University, TraVinh, Vietnam. In 2011, he received M.S. degree in computer sciences from FengChia University, TaiChung, Taiwan. He is currently pursuing the Ph.D. degree with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan. His current research interests include data hiding, image processing, database security and information security.

Chia-Chen Lin received the B. S. degree in information management from the Tamkang University, Taipeo, Taiwan, R.O.C., in 1992. She received the M.S. degree in information management and the Ph.D. degree in information management from Chiao Tung University, Hsinchu, Taiwan, in 1994 and 1998, respectively. She was a Visiting Associate Professor at Business School, University Illinois at Urbana Champain, during August 2006 to July 2007. She is currently a Professor in the Department of Computer and Information Management, Providence University, Sha-Lu, Taiwan. Her research interests include image and signal processing, image data hiding, mobile agent, and electronic commerce.