Journal of Korea Multimedia Society Vol. 16, No. 5, May 2013(pp. 591-600)
http://dx.doi.org/10.9717/kmms.2013.16.5.591

A Feature-Based Robust Watermarking Scheme Using Circular Invariant Regions

Munkhbaatar Doyoddorj[†], Kyung-Hyung Rhee[††]

ABSTRACT

This paper addresses a feature-based robust watermarking scheme for digital images using a local invariant features of SURF (Speeded-Up Robust Feature) descriptor. In general, the feature invariance is exploited to achieve robustness in watermarking schemes, but the leakage of information about hidden watermarks from publicly known locations and sizes of features are not considered carefully in security perspective. We propose embedding and detection methods where the watermark is bound with circular areas and inserted into extracted circular feature regions. These methods enhance the robustness since the circular watermark is inserted into the selected non-overlapping feature regions instead of entire image contents. The evaluation results for repeatability measures of SURF descriptor and robustness measures present the proposed scheme can tolerate various attacks, including signal processing and geometric distortions.

Key words: Robust Watermarking, Local Invariant Feature, Optimized Location, Repeatability, Distinctiveness

1. INTRODUCTION

Digital watermarking is a promising way to protect the copyright of digital products. The ownership can be established by extracting previously embedded information or watermarks. Therefore the protection of the ownership of multimedia data against various attacks has become a very challenging issue. In many applications, the effectiveness of a digital watermarking algorithm depends on its ability to resist attacks. According to different intention of attacks, robustness and security should be considered in the design of digital watermarking schemes [1,2]. Robustness deals with blind attacks that try to destroy or invalidate hidden watermarks without exploiting knowledge of the watermarking algorithm. The robustness measurement for watermarking schemes is to evaluate their ability to successfully detect the hidden watermark after blind attacks. In general, these attacks can be classified into two broad categories: signal processing and geometrical distortions. While signal processing attacks attempt to reduce the watermark energy, geometrical distortions may induce synchronization error between the encoder and decoder of the watermark. But, security denotes the ability of a watermarking scheme to prevent hidden watermarks from being accessed by unauthorized users. For the attacks to security, it is usually assumed that the unauthorized users know all knowledge about the watermarking algorithm except the secret key and they try to estimate the hidden watermarks through observing the

※Corresponding Author : Kyung-Hyung Rhee, Address : (608-737) 45, Yongso-ro, Nam-Gu. Busan, Korea. TEL : +82-51-629-6247, FAX : +82- 51-626-4887, E-mail : khrhee@pknu.ac.kr

Receipt date : Jan. 31, 2013, Revision date : Mar. 22, 2013
Approval date : Mar. 24, 2013

[†] Department of Information Security, Pukyong National University
(E-mail: d_mbtr@pknu.ac.kr)
[††] Department of IT Convergence and Application Engineering, Pukyong National University

※ This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by Ministry of Education, Science and Technology(2012-0001331).

watermarked images. The security of a watermarking scheme can be measured by analyzing the leakage of information about the hidden watermarks from observations.

Local features representing image structures, ranging from points to regions, have been adopted in many applications, such as object recognition, image retrieval, and data hiding [2-4]. These features, which are powerful references, have also been applied successfully in feature-based watermarking methods since they can be preserved after suffering distortion such as scaling, rotation, or illumination changes. In general, a feature detector performs a specific transformation on an image to extract local features for watermark embedding and detection. However, a feature region extracted by a detector is not directly applicable to digital watermarking. Because, the locations and sizes of extracted features can be publicly found by the attackers. Also, the watermark embedding into all regions will also cause heavy image degradation and low robustness since most of features are overlapped. Although many new feature detectors have been proposed to enhance the robustness of feature-based watermarking [5,6], most of them are still vulnerable to geometrical distortions. Therefore, a qualified feature-based watermarking scheme should examine the robustness of the adopted feature detector, avoid the information leakage of secret parameters, and determine an appropriate non-overlapping feature region set.

1.1 Related Work

Many digital watermarking schemes have been proposed for copyright protection and several watermarking methods have been developed to overcome the problem caused by geometric distortions. These methods can be roughly classified into template-based, invariant-transform domain-based, moment-based, histogram-based and feature-based methods.

The template-based watermarking methods are based on embedding a template in addition to the watermark to assist the watermark synchronization in the detection process. This may be achieved using a structured template embedded in the discrete Fourier transform (DFT) domain [7] or by embedding the watermark several times at different location [8]. In invariant-transform domain-based methods [9], watermarks are embedded in affine-invariant domains such as the Fourier - Mellin transform or log-polar domain to achieve robustness against affine transforms. However, watermarking methods involving invariant domains are usually vulnerable to cropping and they are difficult to implement because of the log-polar mapping [10]. In moment-based watermarking methods [11,12], watermarks are embedded into normalization-based moments robust against affine transforms. Using the fact that image histograms are independent of the positions of pixels, the authors in [13,14] presented a histogram-based watermarking approach. However, these approaches suffer from robustness limitations under histogram enhancement and equalization attacks. Another way to reduce or remove the synchronization issue caused by geometric attacks is to extract feature points, which represent invariant references to geometric transformations.

Recently, image feature-based watermarking methods have been widely exploited to overcome the watermark synchronization issue [15-17]. In [15], the Harris detector is used to extract feature points, which are combined with a Delaunay Tessellation to define a number of triangular regions for embedding the watermark. The drawback of this method is that extracted features points from the original and attacked images are not matched. Therefore the sets of triangles generated during watermark embedding and detection are different. Furthermore, this method is not robust to most signal processing attacks except JPEG compression [17]. In [16], a Mexican hat wavelet scale interaction method is used to extract feature points and then the watermark is embedded in normalized disks centered at the extracted feature points. In [17], the authors proposed a method similar to that presented in [15], in which the adaptive Harris corner detector is used to extract feature points and the Delaunay Tessellation-based triangle matching method is used to reduce the watermark synchronization problem and resist geometric distortions. Moreover, the methods reported in [11,12,15] are not robust to local geometric attacks such as cropping. This is because the normalization process is applied into the entire image. Indeed, the removal of any part of an image will result in significant distortion of the moment values.

1.2. Our Contributions

In this paper, we propose a robust feature-based watermarking scheme using circular invariant regions of SURF descriptor [18]. The watermark is bound with circular areas and inserted into extracted invariant feature regions that using an additive watermark embedding method. High repeatability of these feature regions offers robustness against signal processing and geometrical distortions, while secrecy of the region size makes it difficult for an attacker to estimate exact range of feature region. The non-overlapping region selection process further incorporates randomization to avoid an attacker correctly identifying the watermarked regions. According to local invariance of such feature, our scheme provides efficient feature computation and comparison with respect to repeatability, distinctiveness and robustness. The most desirable property of any detector is its repeatability, that is, its ability to detect a given feature when it appears in different images. But, the distinctiveness offers that an individual features can be matched to a large database of object. Moreover, our scheme is blind as the original image is not required at the watermark detection.

The rest of this paper is structured as follows. Section 2 introduces a preliminaries used in our proposed scheme. Section 3 covers the details of our watermark embedding and detection process. Experimental results are shown in Section 4. Conclusions and discussions are drawn in Section 5.

2. PRELIMINARIES

2.1 Speeded-Up Robust Features (SURF)

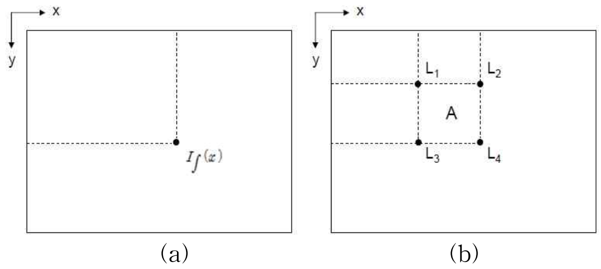
The SURF [18] approach describes a keypoint detector and descriptor. Keypoints are found by using a so called Fast-Hessian Detector that bases on an approximation of the Hessian matrix for a given image point. The responses to Haar wavelets are used for orientation assignment, before the keypoint descriptor is formed from the wavelet responses in a certain surrounding of the keypoint. The main process of SURF algorithm is as below.

1) **Integral Images.** The concept of integral images allow for fast computation of box type convolution filters. The entry of an integral image $I_{\int}(x)$ at a location $x=(x,y)^T$represents the sum of all pixels in the input image I within a rectangular region formed by the origin and x.

$$I_{\int}(x)=\sum_{i=0}^{i\leq x}\sum_{j=0}^{j\leq y}I(i,j) \tag{1}$$

Once the integral image has been computed, it takes three additions to calculate the sum of the intensities over any upright, rectangular area as shown in Fig. 1. Hence, the calculation time is independent of its size.

2) **Feature detection.** It is mainly about accelerating image convolution operation by the use of box filter and integral image, establishing the scale space and extracting the location and scale of feature points according to Hessian matrix. To speed up the convolution operation, Bay proposed a method of using box filter to approximate Gaussian



(a) (b)

Fig. 1. Integral image representation. (a) Integral image and (b) Region A can be computed using the following four array references: $L_4+L_1-(L_2+L_3)$.

filter. The achieved approximation L_{xx}, L_{xy}, L_{yy} will be noted as D_{xx}, D_{xy}, D_{yy}. Then the determinant of Hessian matrix can be calculated through it, see in [1].

SURF scale space is also divided by group. Each group is obtained by gradually up-scaling the filter size on input image. Filter size used in the first layer of the first group is 9×9. The initial scale is $s=1.2$, corresponding to $\sigma=1.2$ in Gaussian function. The filter size of other layers expands at a unit of 6 pixels and the filter sizes are 15×15, 21×21, 27×27 one by one. It is similar to other groups. The filter sizes in each group form an arithmetic progression, and the relationship between tolerance and group number is $6\times2^{n-1}$. From the second group, the filter size of the first layer in each group is the same with the filter size of the second layer in last group. On this basis, SURF algorithm greatly improves the computational efficiency by the use of box filter and integral image.

After obtaining the extreme value using Hessian matrix, we need to use non-maximum suppression in a 3×3×3 neighborhood to accurately position key points. Then to get stable location and scale of a key point, interpolation operator is used in scale space [19].

3) **Generating SURF descriptor.** The main task is to generate a feature vector based on local image information around the key point. The first step is to get the main direction of the key point. It mainly relies on the calculation of Haar wavelet responses in x and y direction and the summation of them within a range of 60° to form a new vector after weighted and traverse all the circular area. Then, the second step is generating SURF descriptor. We also need to calculate the Haar-wavelet responses in certain size of region and add up the weighted responses and their absolute values to get a four-dimensional vector over each sub-region. The specific method can be seen in [20]. Finally, we can obtain a 64 dimensional descriptor vector. Through converting the descriptor to a unit vector, we can achieve invariance to illumination.

2.2 Polar Mapping

To assign the insertion location of extracted circular SURF feature, we consider the transforms between the rectangular watermark and the circular watermark, and vice versa. Let (x,y) be the coordinates of $M\times N$ dimensions of the rectangular watermark. To generate the circular watermark, the coordinates (x,y) of the rectangular watermark are inversely transformed to the radius and angle directions of the circle, as shown in Fig. 2. The relations between two coordinates are represented as follows:

$$\begin{cases} x=\dfrac{r_i-r_0}{r_M-r_0}\bullet M,\ y=\dfrac{\theta}{\pi}\bullet N, & \text{if } 0\le\theta\le\pi; \\ x=\dfrac{r_i-r_0}{r_M-r_0}\bullet M,\ y=\dfrac{\theta-\pi}{\pi}\bullet N, & \text{if } 0\le\theta\le2\pi. \end{cases} \quad (2)$$

where x and y are the rectangular watermark co-

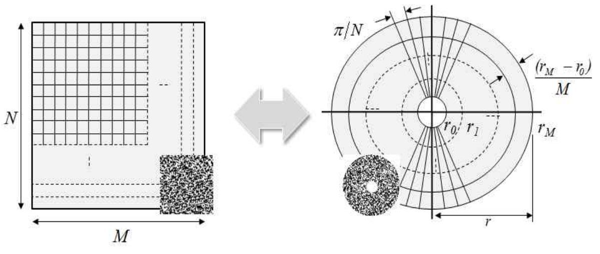


Fig. 2. Polar mapping structure.

ordinates, r_i and θ are the coordinates of the circular watermark, r_M is equal to the radius of circle, and r_0 is a fixed fraction of r_M.

3. THE PROPOSED SCHEME

3.1 Watermark Embedding

We apply the SURF descriptor to detect the local invariant features of input image. A single image may contain a number of circular feature regions, as shown in Fig. 3(b). Among the detected feature regions, non-overlapped regions are selected to use our watermarking scheme. We generate a circular watermark dependent on the radius (size) of each region, using the method described in Fig. 3(c) and (d). respectively. The insertion of the watermark must not affect the perceptual quality of image. Therefore, we apply the perceptual masking as follows:

$$P^{mask} = \alpha \cdot (1 - NVF) + \beta \cdot NVF, \quad (3)$$

where α is lower bound of visibility in flat and smooth regions and β is the upper bound in edged and texture regions. The noise visibility function (NVF) is calculated as follows:

$$NVF(i,j) = \frac{1}{1 + \theta \cdot \sigma_x^2(i,j)}, \quad \theta = \frac{D}{\sigma_{xmax}^2}, \quad (4)$$

where $\sigma_x^2(i,j)$ and σ_{xmax}^2 denote the local variance and maximum of neighboring pixels, respectively. D is a scaling constant. Finally, we embed the circular watermark additively into the extracted feature regions, as follows:

$$w_i = I_i + P_i^{mask} w_i^{cir}. \quad (5)$$

where I_i and w_i^{cir} denote the pixels of image and of the circular watermark, respectively. P_i^{mask} is the perceptual mask that controls the insertion strength of the watermark.

3.2 Watermark Detection

Similarly to watermark embedding, non-overlapped regions are selected from the watermarked image based on the SURF descriptor. The additive watermark embedding method inserts the watermark into the image as noise. Therefore, we apply a Wiener filter to extract this noise by calculating the difference between the watermarked and its Wiener filtered image, which regard the difference as the retrieved watermark. As with the watermark embedding, we compensate for the modification by perceptual masks, such compensation does not greatly affect the performance of watermark detection. Then the retrieved circular watermark w^{cir} is converted into a rectangular watermark w^{rec} by applying the polar mapping. To measure the similarity between the reference watermark w^{ref} and the retrieved watermark w^{rec}, the Normalized Hamming Similarity (NHS) is applied, as follows:

$$NHS = \frac{1 - D^{HD}(w^{ref}, w^{rec})}{N}. \quad (5)$$

where D^{HD} denotes Hamming distance between the original watermark sequence and the extracted

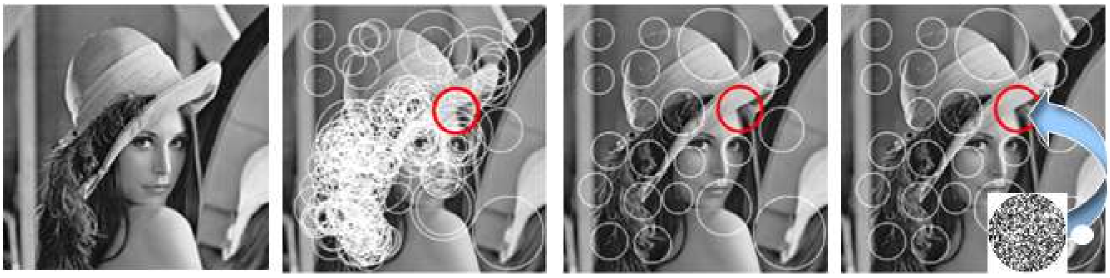

(a) (b) (c) (d)

Fig. 3. Illustration of detection and embedding stages. (a) Input image (b) Detected SURF features (c) Selected circular feature regions (d) Additive watermarking as noise.

watermark sequence, and N denotes the total number of the watermark bit .

Finally, to determine the presence of watermark, the NHS will be compared with a predefined threshold value τ^{pre}.

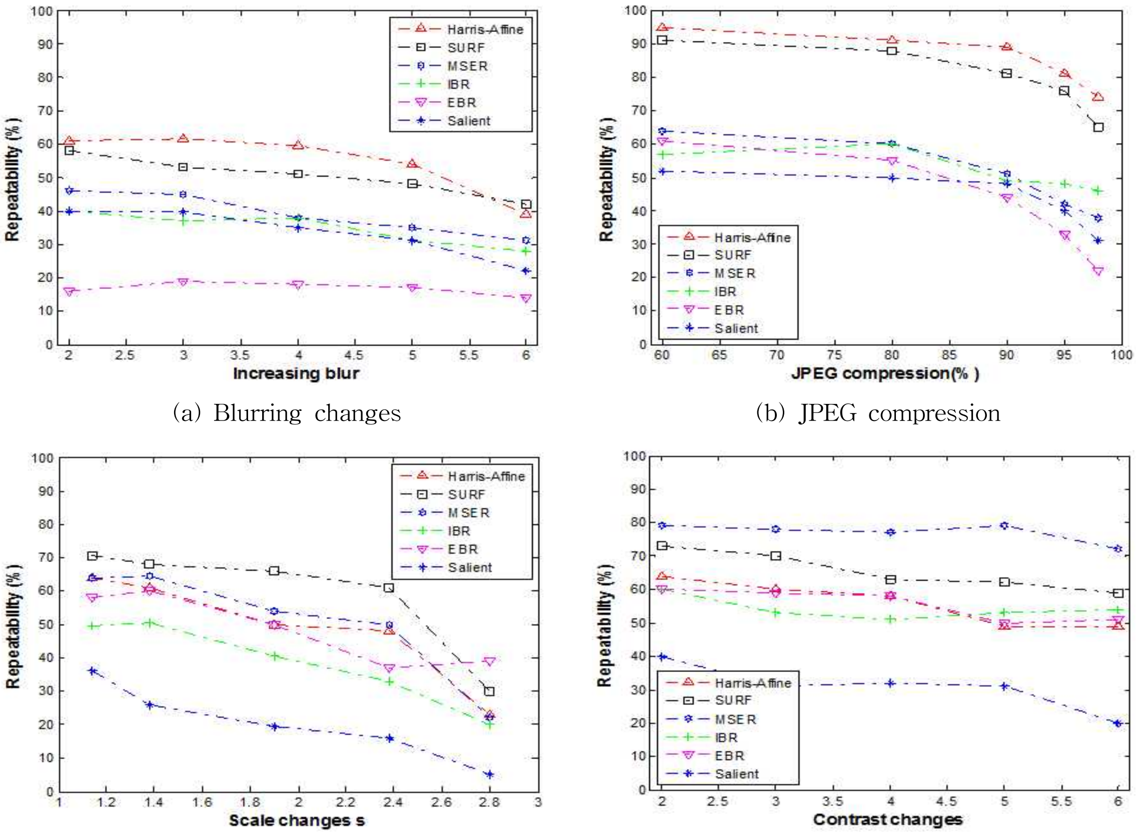
4. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, we describe our experiments and discuss the results. The simulation was carried out using Matlab version R2008a. In order to evaluate the performance of our proposed scheme, we considered eight commonly used grayscale images with the size of 512×512.

4.1 Evaluation of SURF descriptor

In this section, we introduce a repeatability measure of local invariant features and comparison between different feature descriptors. In general, in order to design a robust feature based watermarking scheme, extraction of the local invariant features should provide highly distinctive and repeatability properties. These aspects are important factors for extracting robust image space. In this sense, we are evaluated the repeatability measure of our chosen SURF descriptor and compared its performance between other image feature descriptors.

We attached some evaluation results for repeatability measure in Fig. 4, such as commonly applied image distortion operations, blurring, contrast and scale changes, and JPEG compression. Fig. 4(a) shows the results of blurring changes undergoing increasing amount of image blur. All detectors are middle level (nearly 50%) of invariance to image blur, except for the EBR detector, which is clearly more sensitive to this type of transformation. In



(a) Blurring changes

(b) JPEG compression

(c) Contrast changes

(d) Scale changes

Fig. 4. Comparisons for repeatability measures.

Fig. 4(b), the SURF descriptor has achieved higher level of invariance with Harris-Affine descriptor. In case of contrast and scale changes, all descriptors have good robustness to scale and contrast, except the salient feature descriptor, as shown in Fig. 4(c) and (d), respectively. Although the SURF descriptor obtains the highest repeatability score for scale changes.

4.1 Performance of the proposed scheme

We evaluated the robustness of our scheme against several image processing and geometrical operations. To assess the performance of the proposed scheme, a variety of experiments were carried out. Length of watermark is depending on the extracted non-overlapped feature regions, and different for each test images. First, we calculated the Peak Signal to Noise Ratio (PSNR) values between cover image and its watermarked image, where the cover images watermarked by the proposed method as shown in Fig. 5. Here, it is difficult to visually distinguish the cover image from the watermarked image. Furthermore, the maximum *NHS*=1, which reveals we can extract the watermark accurately.

The robustness in watermarking is the process of extraction the correct data after compression or any other alteration applied on the watermarked image. Hence, for fair benchmarking and performance evaluation, the robustness due to the embedding is an important issue. Since there is no universal metric, we review in this section the most popular pixel-based distortion criteria and introduce one metric which makes use of effect in the human visual system. Most distortion measures used in visual information processing belong to the group of difference distortion measures, such as similarity measure of Normalized Hamming Similarity (*NHS*). The maximum *NHS*=1, which reveals we can extract the watermark accurately.

To confirm the efficiency and robustness, well-known attacks such as rotation, cropping, JPEG compression and Gaussian noise are applied to our scheme in Fig. 6. For each attack, we computed a similarity measure between an original embedded data and attacked embedded data according to the percentage. This percentage is number of equal bits between original and extracted embedded data. A result less than or equal to 50% implies that the cover image has probably not been hidden.

To evaluate the robustness of the proposed scheme against various attacks, the experimental results on signal processing and geometric oper-

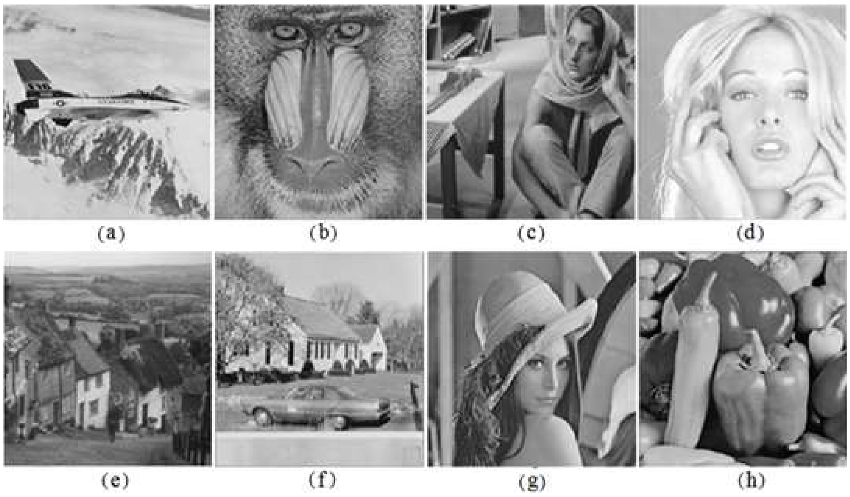


Fig. 5. Watermarked images (512×512). (a) Airplane (48.35 dB), (b) Baboon (47.51 dB), (c) Barbara (48.32 dB), (d) Tiffany (49.18 dB), (e) Goldhill (48.44 dB), (f) House (49.62 dB), (g) Lena (49.34 dB), (h) Pepper (47.52 dB).

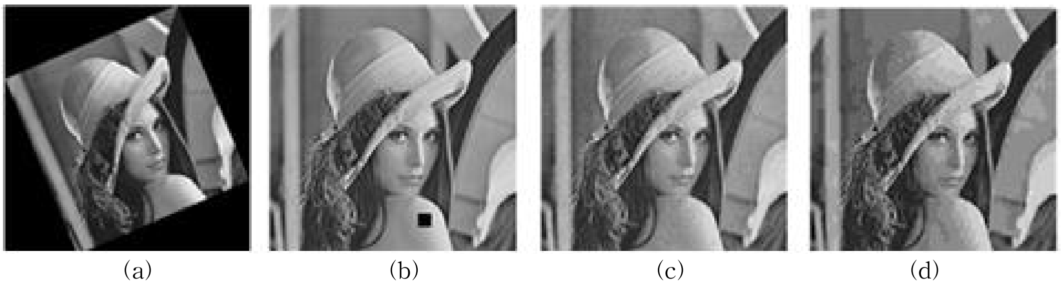


Fig. 6. An attacked images by various image processing and geometrical distortions. (a) Rotation (α=10°), (b) Cropping (50 blocks), (c) Gausian noise (dev.=2), (d) JPEG compression (60%).

Table 1. Comparison and the robustness against image processing operations (*NHS*)

	Proposed scheme	Proposed (*NHS*)	Zhang's scheme	Li's scheme
No attack	9/9	1	1	1
Median filtering	5/9	0.97	0.95	0.860
Added noise	6/8	0.89	-	-
JPEG 60%	5/9	0.91	0.88	0.977
JPEG 70%	7/10	0.95	0.98	0.992
JPEG 80%	8/10	0.93	1	1

Table 2. Comparison and the robustness against desynchronization operations (*NHS*)

	Proposed scheme	Proposed (*NHS*)	Zhang's scheme	Li's scheme
Rotation (5°)	4/9	0.45	0.56	1
Rotation (10°)	3/8	0.58	-	-
Scaling (0.7)	4/10	0.96	0.98	1
Scaling (0.9)	8/10	0.98	1	1
Scaling (1.1)	8/10	0.97	1	1
Cropping 50 bl.	8/10	0.94	1	1

ations are listed in Table 1 and 2, respectively. We compared the performance of the proposed scheme with that of Zhang's scheme [21] and Li's scheme [22]. Where the denominator denotes the number of synchronized interest regions during watermark detection and the numerator denotes the number of matched interest regions from which the watermark can be successfully determined after various attacks, respectively. Compared with Zhang's and Li's schemes, our scheme is more robust against a variety of attacks in feature-based domain. On the other hand, the robustness against rotation attack in our scheme is relatively weak. But our scheme can provide higher robustness on the median filtering and scaling operations.

5. CONCLUSION

This paper presents a feature-based robust watermarking scheme, which is designed to be robust against both signal processing and geometrical attacks. In order to increase the robustness, certain non-overlapping circular feature regions were extracted and the watermark were inserted into it by additive watermarking way. The evaluation results for repeatability measure of SURF descriptor demonstrates that extracted circular regions can effectively resist against set of geometrical distortions.

In addition to, according to ability of SURF descriptor, our embedded circular watermarks are respect to repeatability, distinctiveness and robustness yet can be computed and compared much faster.

REFERENCES

[1] F. Cayre, C. Fontaine, and T. Furon, "Watermarking Security: Theory and Practice," *IEEE Transactions on Signal Processing*, Vol. 53, No. 10, pp. 3976-3987, 2005.

[2] L. Pérez-Freire, P. Comesaña, J.R.T.Pastoriza, and F. Pérez-González, "Watermarking Security: A Survey," *Transactions on Data Hiding and Multimedia Security I*, Vol. 4300, pp. 41-72, 2006.

[3] K. Mikolajczyk, T. Tuytelaars, and L.V. Gool, "A Comparison of Affine Region Detectors," *International Journal of Computer Vision*, Vol. 65, No. 2, pp. 43-72, 2005.

[4] D. Munkhbaatar, Y. Park, and K.-H. Rhee, "A Robust Reversible Data Hiding Scheme with Large Embedding Capacity and High Visual Quality," *Journal of Korea Multimedia Society,* Vol. 15, No. 7, pp. 891-902, 2012.

[5] C. Deng, X. Gao, X. Li, and D. Tao, "Local Histogram based Geometric Invariant Image Watermarking,“ *Signal Processing,* Vol. 90, No. 12, pp. 3256-3264, 2010.

[6] J.S. Tsai, W.B. Huang, and Y.H. Kuo, "On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking," *IEEE Transactions on Image Processing,* Vol. 20, No. 3, pp. 735-743, 2011.

[7] S. Pereira and T. Pun, "Robust Template Matching for Affine Resistant Image Watermarks," *IEEE Transactions on Signal Processing*, Vol. 9, No. 6, pp. 1123-1129, 2000.

[8] 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 Transactions Circuits System & Video Technology,* Vol. 13, No. 8, pp. 776- 786, 2003.

[9] D. Zheng, J. Zhao, and S. El Saddik, "RST-Invariant Digital Correlation," *IEEE Transactions Circuits Systems & Video Technology,* Vol. 13, No. 8, pp. 753-765, 2003.

[10] 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 Transactions on Image Processing*, Vol. 10, No. 5, pp. 767-782, 2001.

[11] M. Alghoniemy and A.H. Tewfik, "Geometric Invariant in Image Watermarking," *IEEE Transactions on Image Processing*, Vol. 13, No. 2, pp. 145-153, 2004.

[12] P. Dong, J.G. Brankov, N.P. Galatsanos, Y.Y. Yang, and F. Davoine, "Affine Transformation Resistant Watermarking Based on Image Normalization," *IEEE Transactions on Image Processing*, Vol. 14, No. 12, pp. 145-153, 2005.

[13] S. Roy and E.C. Chang, "Watermarking Color Histograms," *Proc. Int. Conf. Image Processing,* pp. 2191-2194, 2004.

[14] S. Xiang, H. Joong, and J. Huang, "Invariant Image Watermarking Based on Statistical Features in Low-Frequency Domain," *IEEE Transactions on Circuit and System Video Technology,* Vol. 18, No. 6, pp. 777-789, 2008.

[15] P. Bas, J.M. Chassery, and B. Macq, "Geometrically Invariant Watermarking using Feature Points," *IEEE Transactions on. Image Processing*, Vol. 11, No. 9, pp. 1014-1028, 2002.

[16] C.W. Tang and H.M. Hang, "A Feature-Based Robust Digital Image Watermarking Scheme," *IEEE Transactions on Signal Processing,* Vol. 51, No. 4, pp. 950-959, 2003.

[17] X. Qi and J. Qi, "A Robust Content-Based Digital Image Watermarking Scheme," *Signal*

Processing, Vol. 87, No. 6, pp. 1264-1280, 2007.

[18] H. Bay, A. Ess, T. Tuytelaars, and L.V. Gool, "SURF: Speeded Up Robust Features," *Computer Vision and Image Understanding (CVIU)*, Vol. 110, No. 3, pp. 346-359, 2008.

[19] M. Brown and D. Lowe, "Invariant Features from Interest Point Groups," *Proc. Conf. British Machine Vision, British*, pp. 656-665, 2002.

[20] P. Shao, L. Yang, and Y. Zeng, "An Improved Algorithm of Integral Image for Computing Rotated Harr-Like Features," *Computer Technology and Development*, Vol. 12, No.3, pp. 34-42, 2006.

[21] Y. Zhang, H. Bi, and H. Zhang, "Robust Watermarking Scheme by Harris Interest Regions," *Journal of Computational Information Systems*, Vol. 8, No. 20, pp. 8421-8429, 2012.

[22] L. Li, B. Guo, and L. Guo, "Rotation, Scaling and Translation Invariant Image Watermarking using Feature Points," *The Journal of China Universities of Posts and Telecommunications*, Vol. 15, No. 2, pp. 82-87, 2008.

Munkhbaatar Doyoddorj

2003 B.S. degree from National University of Mongolia
2011 M.S. degree from Dept. of Information Security, Pukyong National University
2011~onward Ph.D. course in Information Security, Pukyong National University
Interesting : Steganography, Watermarking, Image Forensics

Kyung-Hyune Rhee

1982 B.S. degree in Mathematics Education from Kyungpook National University
1985 M.S. degree in Applied Mathematics from KAIST
1992 Ph.D. in Mathematics from KAIST
1993~onward Professor at Pukyong National University
Interesting : Information Security, Cryptography, Communication Security, Multimedia Security