KSE 2015 8-10 October 2015

The Seventh International Conference on Knowledge and Systems Engineering

Ho Chi Minh City, Vietnam

UIT

JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY

IEEE

IEEE Vietnam Section

MMLAB Multimedia Communications Laboratory

Published by CPS Conference Publishing Services

CONFERENCE INFORMATION

PAPERS BY SESSION

PAPERS BY AUTHOR

GETTING STARTED

TRADEMARKS

SEARCH

Proceedings

2015 IEEE International Conference on Knowledge and Systems Engineering

8–10 October 2015
Ho Chi Minh City, Vietnam

Editors
Bernard Mérialdo
Minh Le Nguyen
Duy-Dinh Le
Duc Anh Duong
Satoshi Tojo

Organized by
University of Information Technology (UIT), VNU-HCM, Vietnam
Japan Advanced Institute of Science and Technology (JAIST), Japan

CPS
Conference Publishing Services

Los Alamitos, California

Washington • Tokyo

IEEE
computer
society

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number E5621
BMS Part Number CFP1503I-ART
ISBN 978-1-4673-8013-3

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Lisa O'Conner
Cover Design by Mark Bartosik

IEEE Computer Society
Conference Publishing Services **(CPS)**
http://www.computer.org/cps

2015 Seventh International Conference on Knowledge and Systems Engineering

KSE 2015

Table of Contents

Long Papers

Short Papers

Comparison of Watermarking Schemes using Linear and Nonlinear Feature Matching

Ta Minh Thanh$^{(1,2)}$, Keisuke Tanaka$^{(1)}$
$^{1)}$*Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology,*
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan. Email: thanh4@is.titech.ac.jp
$^{2)}$*Dept. of Network Security, Le Quy Don Technical University, 236 Hoang Quoc Viet,*
Cau Giay, Ha Noi, Viet Nam. Email: thanhtm@mta.edu.vn.

***Abstract*—Recently, the feature point matching based watermarking techniques have been paying attention for resisting the geometric attacks. We present a performance analysis of robust watermarking using linear and nonlinear feature. In particular, we consider the geometric attacks and the signal processing attacks for image watermarking. In order to analyze the efficiency of linear and nonlinear feature, we employ the linear and the nonlinear feature matching technique in the image watermarking. The extracted feature points can survive against several attacks, therefore, those can be used as reference points for restoration before the extraction of the watermark information. For blindness and robustness, we embed the watermark into the low-band of the discrete cosine transform (DCT) domain. Experimental results show that our performance analysis of watermarking methods using linear and nonlinear feature matching against the geometric attacks and the signal processing attacks. These include the JPEG compression, the filtering attacks, and so on.**

***Keywords*-Accelerated KAZE (AKAZE) feature, rotation-scaling-translation (RST) attack, image watermarking.**

I. Introduction

In order to protect the copyright of digital content, the efficient techniques are required recently due to rapid distribution of digital contents. Among them, digital watermarking is attracted attention recent years. Many digital watermark schemes have been proposed for various formats of digital contents such as image, audio, and video. In digital watermarking techniques, the watermark information is embedded into the digital content without distortion. The watermark information is extracted later by using the special algorithm for some purposes such as authentication, claiming the legal copyright, and detecting the illegal redistribution source [1]. The invisibility, robustness, and capacity of watermark information are required for the proposed watermarking method. Namely, after embedding, the existence of watermark should not be perceived in the embedded content. It must be robust against general image processing such as cropping, noisy addition, JPEG compression, image filtering, and so on. Finally, amount of the embedded watermark must be enough for distinguishing users and detecting the illegal distributor.

Many attack algorithms were also proposed in order to destroy and to evaluate the robustness of watermark information. For example, StirMark benchmark for image [2] and StirMark benchmark for audio [3] are developed to destroy the watermark information in the robustness evaluation. Vidmark [4] provides a benchmark that can attack the video watermarking by a set of the temporal attacks such as frame dropping, frame inserting, frame rate changes, and these combinations. In general, these benchmarks employ roughly two kinds of attacks that are the geometric attacks and the signal processing attacks. The geometric attacks are difficult to tackle because they change the embedded locations in the embedded content, therefore, they induce the error of watermark extraction [5].

In the last decade, many methods that resist both the geometric attacks and the signal processing attacks have been reported. Some previous works mainly focused on the geometric invariant frequency domain for watermark embedding and extraction because it is invariant under rotation, scaling, and translation attacks. The authors of [6], [7] employed the log-polar mapping (LPM) of discrete Fourier transformation (DFT) domain to embed the watermark information and achieved the robustness against the RST attacks. However, their algorithms induce the degradation because the transformation of LPM and inverse LPM distort the embedded image. It is also vulnerable to the cropping and the random bending attacks known as the combined geometric distortion.

Recently, the salient feature points-based watermark was drawn the attention. Our proposed method also belongs to this category. The main idea is that the watermark information is embedded into the geometrically invariant regions. Those regions are specified by the extracted feature points from the image. For example, [8] and [9] tries to extract the robust feature points and embeds the watermark information into the normalized regions. In the extraction process, with the help of the invariant feature points, the watermark information can be successfully retrieved. Another merit of the salient feature points is that the parameters of the geometric attack can be estimated by using a set of feature points. This idea was introduced in the methods of Viet $et\ al.$ [10] and Thanh $et\ al.$ [13] by using scale-invariant feature transform (SIFT) [15] and KAZE feature [16], respectively.

978-1-4673-8013-3/15 $31.00 © 2015 IEEE
DOI 10.1109/KSE.2015.67

However, high computation cost is still the drawback of the watermark schemes employing the feature points.

In this paper, we introduce a novel watermarking method based on the nonlinear scale spaces feature by using the accelerated KAZE (AKAZE) [17]. Our contributions are listed as follows:

(1) The performance evaluation in [17] showed that AKAZE performs better than SIFT, SURF[1], and KAZE feature in the most of attacks such as blur, zoom and rotation, JPEG compression, viewpoint change, noise addition, light change, and so on. We successfully apply AKAZE feature to watermarking methods, such that its the good performances of AKAZE feature are retained.

(2) We propose AKAZE feature points for restoring the suspected image before extracting the watermark. Since AKAZE feature points can be extracted stably under most of the geometric attacks, we can use AKAZE feature points in order to estimate the parameters of the geometric attacks such as rotation, scaling, translation, and the combinations of these.

(3) We compare the robustness of watermarking methods using the linear feature (SIFT and SURF) and nonlinear feature (AKAZE and KAZE) matching in order to show the efficiency of those for watermarking methods.

(4) Various simulation experiments are conducted to demonstrate the performance of our proposed method. With the comparison results of KAZE-based, SIFT-based, SURF-based watermarking methods, we find that the AKAZE feature is very appropriate for robust watermarking method.

The remainder of this paper is organized as follows. In Section 2, the details of our proposed method, consisting of the embedding method and extraction method, are described. Section 3 presents our simulation results and those discussions. Section 4 concludes our paper.

II. The proposed method

A. Overview

As far as we know, the AKAZE feature is employed in watermarking method for the first time. Before embedding the watermark information, a detection algorithm of Alcantarilla $et\ al.$ [17] is adopted to extract the AKAZE feature points. Those feature points are saved into the database of the producer to restore the suspected image before watermark extraction.

In the embedding process, the original watermark image is first permuted to obtain the scrambled watermark image. The scrambled watermark is embedded into the low-band frequency of DCT domain of the original image. The embedded image can be used to send the legal user via network.

When a user claims about the authentication of the image, the producer has to judge it. He/she uses the same detection algorithm as used in the embedding process, and detects the AKAZE feature points from the suspected image. Based on those feature points and the feature points from his/her database, he/she can restore the suspected image. Then, a watermark image is extracted from the restored image. Here, the producer can distinguish the watermark image and can judge the right authentication of the image.

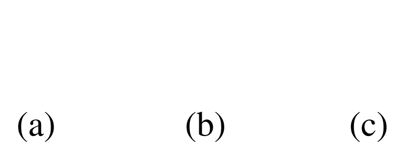


Figure 1. Permuted watermark by the Torus permutation after p times, where a) p=20, b) p=60, and c) p=96.

B. Watermark permutation

Before embedding, we prepare watermark information W with the size $M \times N$ and obtain the binary sequence bits from W denoted by $w(x,y) \in \{0,1\}, 1 \leq x \leq M, 1 \leq y \leq N$, i-th bit of watermark. In order to achieve more security, W should be scrambled before embedding into the original image.

We employ the Torus permutation [19] to scramble W and obtain the scrambled W' with the period P and p times of permutation. The detail of the watermark permutation can be seen in [11]. Fig. 1 shows some examples of permutation process.

C. Watermark embedding algorithm

Suppose that the producer wants to deliver the image I with size of $S \times S$ to the user via network. He/she needs to embed the watermark information into the original before delivering. The embedding process is described in following.

Step 1. The producer extracts the AKAZE feature points $\mathbf{P}$ from I and saves it in his/her database. These feature points are used to restore the suspected image when a user claims the authentication.

Step 2. Convert the RGB image I to YCbCr color space.

Step 3. Transform Y-component to frequency domain by using DCT transform and obtain $Y' = \{f(u,v), 1 \leq u,v \leq S\}$. Divide Y' into non-overlapping blocks. The size of each block is 8×8.

Step 4. In order to embed the watermark information, a secret key k_s is used to select two arbitrary coordinates of the DCT coefficient from the low-band frequency in each block. Assuming that $f_1(u_1,v_1)$ and $f_2(u_2,v_2)$, where $u_1 \neq u_2, v_1 \neq v_2$, are selected by k_s. The watermark is embedded by adjusting the relation among the selected DCT coefficients. These two coefficients are changed to $f_1'(u_1,v_1)$ and $f_2'(u_2,v_2)$ according to the modification in Eq. (1) and (2). One bit $w'(x',y')$ will be embedded into the DCT coefficient of the low-band frequency.

When $w'(x',y') = 0$,

$$\begin{cases} f_1'(u_1,v_1) = sgn(f_1(u_1,v_1)) \times (ave + \dfrac{\alpha}{2}), \\ f_2'(u_2,v_2) = sgn(f_2(u_2,v_2)) \times (ave - \dfrac{\alpha}{2}). \end{cases} \quad (1)$$

[1] SURF: Speeded Up Robust Features [18].

When $w'(x',y')=1$,

$$\left\{\begin{array}{l} f_1'(u_1,v_1)=sgn(f_1(u_1,v_1))\times(ave-\frac{\alpha}{2}),\\ f_2'(u_2,v_2)=sgn(f_2(u_2,v_2))\times(ave+\frac{\alpha}{2}), \end{array}\right. \tag{2}$$

where $sgn(X)$ function equals to "+" if $X>0$, "−" if $X<0$ and $ave=(|f_1(u_1,v_1)|+|f_2(u_2,v_2)|)/2$, which is the average value of the absolute value of $f_1(u_1,v_1)$ and $f_2(u_2,v_2)$, α is the embedding strength.

Step 5. Compute the inverse DCT to obtain the modified Y-component and compose it with the Cb and Cr components.

Step 6. Convert the modified YCbCr image to obtain the modified RGB image.

Repeat Step 3 to Step 5 until all bits $w'(x',y')$ are embedded into I, we obtain the watermarked image I'.

According to the above process, we embed the watermark W' into the DCT domain of Y component in order to achieve the blindness and robustness. The embedding strength α, the parameter k and p used to perform the Torus permutation, the extracted AKAZE feature points **P**, and the secret key k_s will be used as the private keys. Therefore, only producer who knows the private keys, can extract correctly the watermark information from the embedded image. From this point, our proposed method can be expected more security.

D. Watermark extraction algorithm

The extraction algorithm is to extract the watermark information from the suspected image for authentication. The producer uses the private keys to extract the watermark information from the suspected image. Our extraction method is performed without using the original image and those steps are described in following.

Step 1. The producer extracts the AKAZE feature points **P'** from the suspected image I'. He/she uses the AKAZE feature points **P** from his/her database to compare with **P'** and to match them each other.

Step 2. Based on the matched feature points, the rotation, scaling, and translation (RST) parameters of the distorted image can be calculated. Then, the distorted image is restored. Note that, we employ the estimation algorithm presented in paper [13]. The authors used the resulted matching of the KAZE feature points to derive the RST parameters. In our paper, we use the AKAZE feature instead of the KAZE feature and obtain better performance results. The detailed estimation algorithm can be referred in the paper [13].

Step 3. After restoration, convert the restored image to YCbCr color space.

Step 4. Transform Y-component to a frequency domain using DCT. Divide the transformed Y-component into non-overlapping blocks with the same size of those in the embedding process.

Step 5. From each block, an embedded bit $w^*(x',y')$ can be retrieved based on the following rule in Eqs. (3).

$$w^*(x',y')=\left\{\begin{array}{ll} 1 & \text{if } f_1^*(u_1,v_1)>f_2^*(u_2,v_2),\\ 0 & \text{if } f_1^*(u_1,v_1)\le f_2^*(u_2,v_2). \end{array}\right. \tag{3}$$

Step 6. Repeat Step 5 until all the watermark bits have been extracted.

Step 7. From $w^*(x',y')$, we can obtain the permuted W^*. Permute W^* with $P-p$ times using the Torus permutation, we can obtain the extracted watermark W''.

With the help of the AKAZE feature points, the producer can easily restored the distorted image. As the result, the watermark information is correctly extracted from the distorted image when it is attacked by geometric transformations.

III. Experimental results

A. Test image and evaluational measures

To evaluate the performance of our proposed method, we conduct four gray-scale images of the well known SIDBA (Standard Image Data-BAse) database [14]. All these test images (Lena, Pirate, Airplane, Peppers) are with size 512×512 pixels. The watermark image used in in the experiments is a binary image with size 97×38 which is shown in Fig. 1(c). All experiments are implemented on Macbook Air system with OSX 10.9, memory 4GB 1600Mhz DDR3. We use the GCC version 4.2.1 to compile the programming. Additionally, the ImageMagick version 6.8.8-10 is used to convert and to view the experimental images.

In order to evaluate the quality of watermarked images, we employ PSNR (Peak Signal to Noise Ratio) criterion [12]. To provide objective judgment of the robustness of extraction, we use the normalized correlation (NC) value [13] between the original watermark W and the extracted watermark W''.

In our experiments, we calculate the PSNR values for each embedded image and NC values for each watermark extracted from the embedded images and the attacked images. In general, if the PSNR value is over 37dB, the quality of the embedded image is considered to be close to the original image. When the NC value is close to 1, it means that the watermarking method is robust under the attacks.

Additionally, we also include the structural similarity (SSIM) [20] index to measure the similarity between the original image I and the embedded image I'. The values of SSIM are in $[0,1]$. When SSIM value is 0, it means that $I\neq I'$. When SSIM value is 1, it means that $I=I'$.

B. Estimation of the embedding strength α

Generally, in order to achieve the robustness of watermark, the quality of the embedded image (also called imperceptibility) should be sacrificed. Therefore, the tradeoff of robustness and imperceptibility must be considered in the proposed watermarking method. If the robustness of

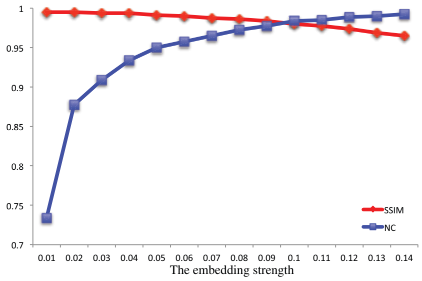


Figure 2. The values of SSIM and NC with different embedding strength α.

watermark is increased (the values of the embedding strength α and NC are increased), the imperceptibility of the embedded image is degraded (the value of SSIM is reduced). Conversely, if the robustness of watermark is reduced (the values of the embedding strength α and NC are reduced), the imperceptibility of the embedded image is improved (the value of SSIM is increased).

In order to determine the appropriate embedding strength α, we repeat the experiments based on the test images. We increase the value of α and run the experiment according to its value. After embedding, we try to calculate the SSIM value and the NC value for each test images. Finally, the average values of the SSIM values and the NC values are obtained.

As shown in Fig. 2, when the value of α increases, the value of SSIM decreases, however, the value of NC increases. Such, to consider the tradeoff of the imperceptibility and robustness of watermark, we choose the value of α at the point of intersection of the curves of SSIM and NC, where the average value of NC is 0.983 and the value of SSIM is 0.980. Thus, the embedding strength α sets to 0.1.

C. Quality of the embedded image

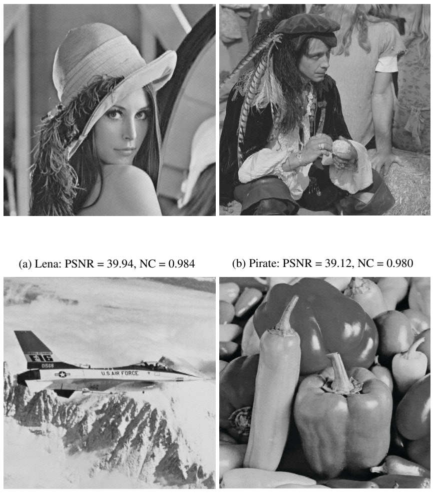
After choosing the appropriate value of $\alpha = 0.1$, we implement the proposed method and obtain the embedded images, then the extracted watermarks. The corresponding embedded images for test images are shown in Fig. 3. The extracted watermark images of the corresponding embedding images are also shown in Fig. 3.

According to the results shown in Fig. 3, we can see that, after embedding the watermark information, no distortion can be observed in the watermarked images. It means that our proposed method achieves good imperceptibility.

D. Robustness comparison

In order to evaluate the robustness, we compare the experimental results of our proposed method with those of another features based on the watermarking method. In particular, we compare with KAZE-based, SIFT-based, and SURF-based watermarking method.

In our experiments, the embedded images are attacked by the following processing attacks and the geometric attacks.



(a) Lena: PSNR = 39.94, NC = 0.984 (b) Pirate: PSNR = 39.12, NC = 0.980

(c) Airplane: PSNR = 39.22, NC = 0.980 (d) Peppers: PSNR = 40.38, NC = 0.989

Figure 3. The watermarked images and the extracted watermark from those.

Firstly, JPEG compression is tested on the embedded images because robust against JPEG compression is the most basic requirement for the image watermarking. After embedding, the embedded images are compressed with different quality factors (QF) with ranging from 10 to 100. Note that, in the JPEG compression, the QF for images is ranged from 1 to 100, which denotes the predetermined image quality of the JPEG compression. When QF is larger, lower compression ratio of the JPEG image is obtained and better visual quality of the JPEG image is retained.

Fig. 4(a) presents the results of our experiments. We can notice that the performance of our method is a litter bit better than the KAZE-based and the SIFT-based method. However, it is lower than SURF-based method when the QF is lower than 30. For higher QF values, the NC values of all methods are close to 1 since the distortions of JPEG images are smaller.

Secondly, we test the robustness of the embedded images under the geometric attacks such as rotation, scaling. The geometric attacks are considered as a difficult challenge because they destroys the synchronization in the embedded image. In our experiments, the embedded images are scaled with the different scaling factors (scaling attack). They are rotated by several angles (rotation attack). The scaling factors with ranging from 0.1 to 1.9 and the rotation angles with ranging from 10^o to 180^o are employed in our tests.

Fig. 4(b) and Fig. 4(c) show the results of the geometric attacks. In the rotation attacks, ours and the KAZE-based method achieve better performance than others. The SIFT-based method achieves the worse performance. In the scaling attacks, SIFT-based and SURF-based methods demonstrate the better performance followed by ours and KAZE-based method. From these results, most of them are robust against the scaling attacks with scaling factors in $[0.5, 2.0]$ because

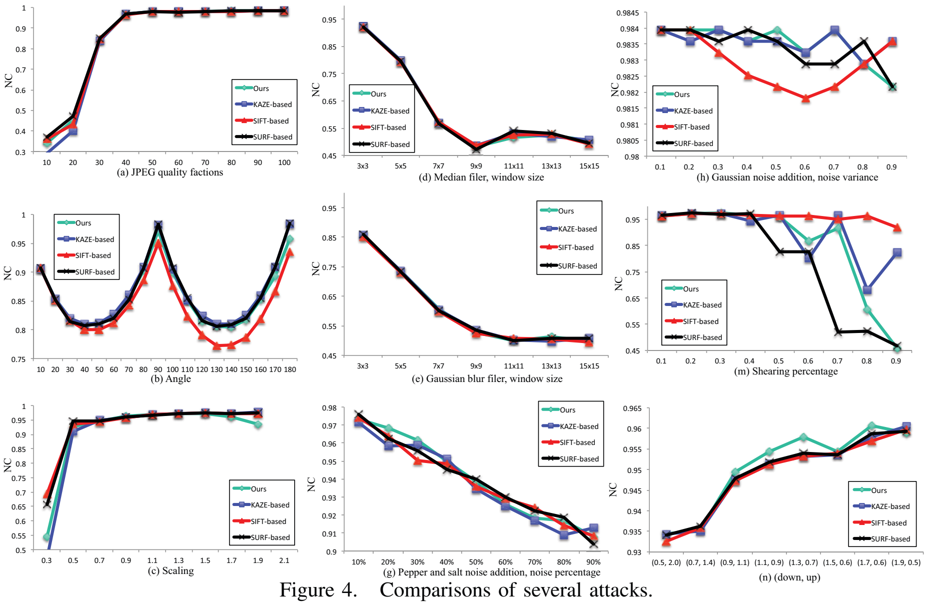


Figure 4. Comparisons of several attacks.

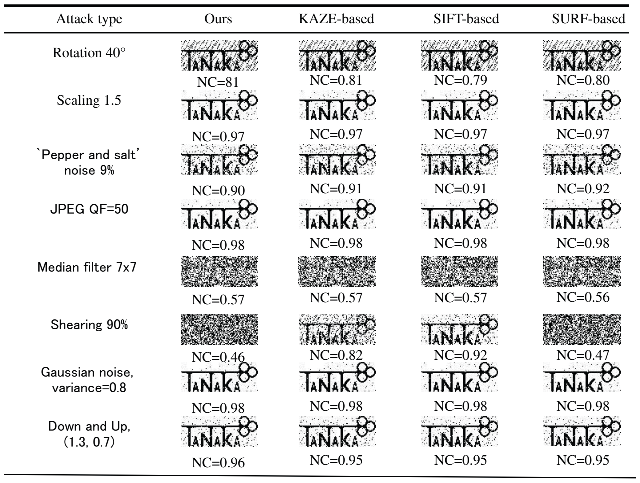
the values of NC are over 0.95.

Thirdly, the next considered attacks are filtering attack. There are two kinds of the filtering attacks, median filtering and Gaussian blur filtering, are used and adopted with the window sizes are $3{\times}3, 5{\times}5, 7{\times}7, 9{\times}9, 11{\times}11, 13{\times}13, 15\times 15$. According to the results shown in Fig. 4(d) and Fig. 4(e), we can see that most of methods have not good performance when the window size is larger than 5. Although all methods obtain similar performance, our method slightly appears to prevail.

Fourthly, noise addition attack is common distortion in which the noise is added to the embedded image. There are two types of noise, Gaussian white noise and ‘pepper and salt’ noise, which are normally added into the embedded images. For the purpose of our experiments, Gaussian white noise of zero mean and variance ranging from 0.1 to 0.9, and ‘pepper and salt’ noise with percentage ranging from 10% to 90% are added into the embedded image.

As presented in Fig. 4(g) and Fig. 4(h), our method is robust against the Gaussian white noise and ‘pepper and salt’ noise addition attacks because the NC values are always larger than 0.9 and 0.98, respectively. Compare to another methods, our method can slightly improve the robustness of watermark extraction. In the ‘pepper and salt’ noise addition attacks, KAZE-based method exhibits the lowest robustness. In the Gaussian noise addition attacks, SIFT-based method achieves the lower performance than others.

Fifthly, we present the shearing attacks on the embedded images. The shearing percentages in x axes with the ranging from 10% to 90% are applied. The results in Fig. 4(m) proves that SURF-based method is not resistant against the shearing attacks, which is expected that SURF feature points maybe lose after shearing the image. The performance of our method is better than SURF-based method, but it become worse when the shearing percentages are over 60%. In this experiment, SIFT-based method achieves the best performance, followed by KAZE-based method.



Attack type	Ours	KAZE-based	SIFT-based	SURF-based
Rotation 40°	NC=81	NC=0.81	NC=0.79	NC=0.80
Scaling 1.5	NC=0.97	NC=0.97	NC=0.97	NC=0.97
`Pepper and salt' noise 9%	NC=0.90	NC=0.91	NC=0.91	NC=0.92
JPEG QF=50	NC=0.98	NC=0.98	NC=0.98	NC=0.98
Median filter 7x7	NC=0.57	NC=0.57	NC=0.57	NC=0.56
Shearing 90%	NC=0.46	NC=0.82	NC=0.92	NC=0.47
Gaussian noise, variance=0.8	NC=0.98	NC=0.98	NC=0.98	NC=0.98
Down and Up, (1.3, 0.7)	NC=0.96	NC=0.95	NC=0.95	NC=0.95

Figure 5. Comparison of the extracted watermarks in terms of visual perception and NC values.

Finally, we apply the downsampling followed by upsampling attacks to the embedded images. In this experiments, we do downsampling to the embedded images and then, do upsampling to inverse to the original size of the embedded images. Those results can be seen in Fig. 4(n). We notice that all methods present similar performance and robust against such kind of attacks. Our method achieves the best performance among all methods.

In order to show the robustness of the watermark of the methods using the AKAZE (Ours), KAZE, SIFT, and SURF

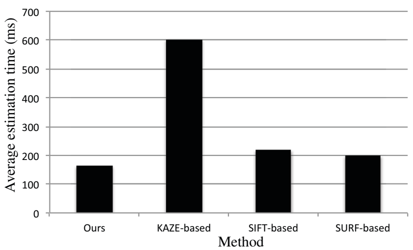


Figure 6. Computation cost.

feature, we pick up several watermark images extracted from corresponding attacked images. Those watermark images are described in Fig. 5. It can be seen from Fig. 5, our proposed method can achieve the good performance comparing to other features. In some cases, our method can improve the robustness of watermark better than others.

E. Computation cost

In this kind of watermarking method, the suspected images should be restored before watermark extraction. Therefore, the computation cost of the restoration process is very important in this method. As shown in Fig. 6, our method spend the smallest of time for restoration the suspected image. The largest of time consuming for restoring image is KAZE-based method. The next ones are SIFT-based and SURF-based methods.

IV. Conclusion

We have introduced a watermarking method based on the nonlinear scale spaces feature by using the AKAZE feature. With the help of the good performances of AKAZE feature, when we employed the AKAZE feature in watermarking method, our proposed method can resist some geometric attacks and some processing attacks. These include the JPEG compression, the filtering attacks, and so on. Four different features such as AKAZE, KAZE, SIFT, SURF are alternatively used in our proposed method and those of experimental results are compared. With the comparison results of KAZE-based, SIFT-based, SURF-based watermarking methods, we conclude that the AKAZE feature is very appropriate for robust watermarking method.

V. Acknowledgments

This work is supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A) No.24240001, a grant of I-System Co. Ltd., NTT Secure Platform Laboratories and CREST, JST.

This work was also funded by the Research Fund RF@K12, Faculty of Information Technology, Le Quy Don Technical University.

References

[1] F. Y. Shih (eds.), “Digital Watermarking and Steganography: Fundamentals and Techniques,” Taylor & Francis Group, CRC Press., 2008.

[2] http://www.petitcolas.net/fabien/watermarking/

[3] M. Steinebach, Petitcolas, A. P. Fabien, F. Raynal, J. Dittmann, C. Fontaine, S. Seibel, N. Fates, L. C. Ferri, “StirMark benchmark: audio watermarking attacks,” Proc. of Coding and Computing, pp. 49–54, 2001.

[4] P. A. H. Avalos, C. F. Uribe, R. Cumplido, J. J. G. Hernandez, “Towards the Construction of a Benchmark for Video Watermarking Systems: Temporal Desynchronization Attacks,” Proc. of the 53nd MWSCAS, pp. 628–631, 2010.

[5] F. Petitcolas, R. Anderson, M. Kuhn, “Attacks on copyright marking systems,” LNCS, pp. 218–238, 1998.

[6] C. Y. Lin, M. Wu, J. A. Bloom Cox, J. Ingemar, M. L. Miller, Y. M. Lui, “Rotation, scale, and translation resilient watermarking for images,” IEEE Trans. on Image Processing, vol. 10, no. 5, pp.767–782, 2001.

[7] D. Zheng, J. Zhao, A. E. Saddik,“RST-invariant digital image watermarking based on log-polar mapping and phase correlation,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no. 8, pp.753–765, 2003.

[8] X. Zhang, X. Cao, J. Li, “Geometric attack resistant image watermarking based on MSER, ” Frontiers of Computer Science, vol. 7, issue 1, pp. 145–156, 2013.

[9] A. Nikolaidis, “Local distortion resistant image watermarking relying on salient feature extraction,” EURASIP Journal on Advances in Signal Processing, vol. 97, 2012.

[10] P. Q. Viet, T. Miyaki, T. Yamasaki, K. Aizawa, “Robust Object-based Watermarking Using Feature Matching,” IEICE Trans. Infor. and Sys., vol. E91-D, no. 7, pp. 2027–2034, 2008.

[11] T. M. Thanh, K. Tanaka, “Blind watermarking using QIM and the quantized SVD domain based on the q-logarithm function,” Proc. of the 10th Conf. on VISAPP, pp. 14–25, 2015.

[12] M. Iwakiri, T. M. Thanh, “Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management,” The 26th IEEE International Conf. on AINA, pp. 763–770, 2012.

[13] T. M. Thanh, P. T. Hiep, T. M. Tam, K. Tanaka, “Robust semi-blind video watermarking based on frame-patch matching,” J. of Electronics and Communications, ISSN 1434-8411, 2014.

[14] www.vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/

[15] D. Lowe,“Distinctive image features from scale-invariant keypoints,”J. of Computer Vision, vol.60, no.2, pp.91–110, 2004.

[16] P. F. Alcantarilla, A. Bartoli, A. J. Davison, “KAZE Features,” ECCV, LNCS, vol. 7577, pp. 214–227, 2012.

[17] P. F. Alcantarilla, J. Nuevo, A. Bartoli, “Fast Explicit Diffusion for Accelerated Features in Nonlinear Scale Spaces,” British Machine Vision Conference (BMVC), 2013.

[18] H. Bay, A. Ess, T. Tuytelaars, L. Gool,“SURF: Speeded Up Robust Features,”J. of CVIU, vol.110, no.3, pp.346–359, 2008.

[19] G. Voyatzis, I. Pitas, “Chaotic mixing of digital images and applications to watermarking,” European Conf. on ECMAST, vol. 2, pp.687–695, 1996.

[20] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. on Image Processing, vol. 13, no. 4, pp. 600–612, 2004.