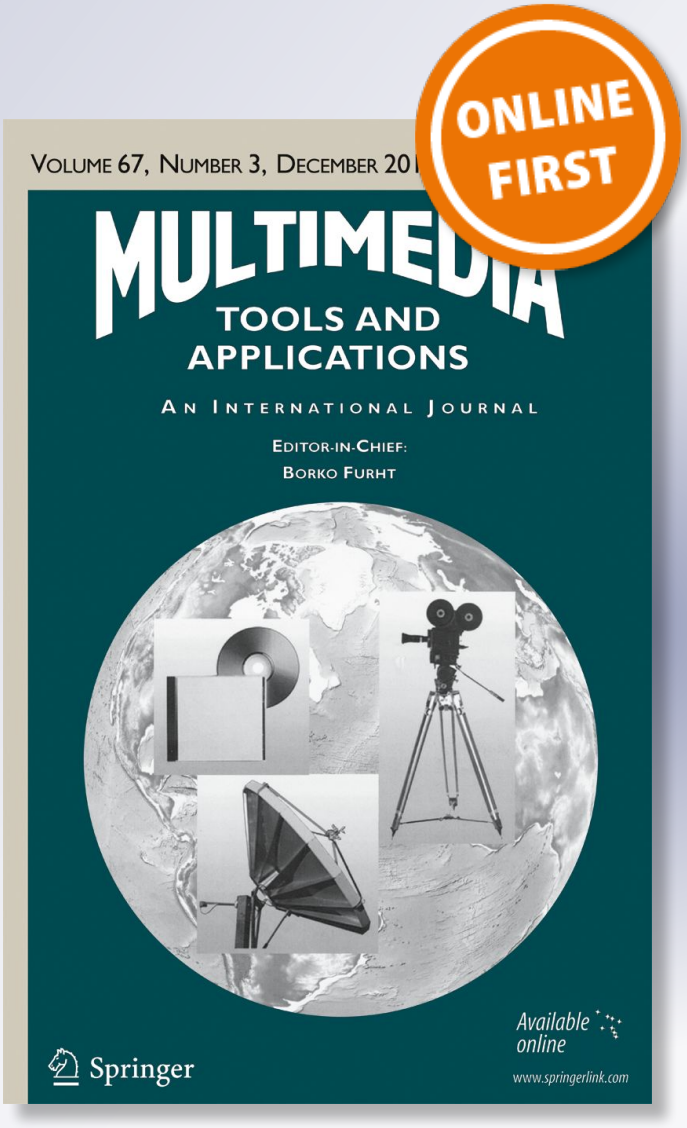
Performance analysis of robust watermarking using linear and nonlinear feature matching

Ta Minh Thanh, Keisuke Tanaka, Luu Hong Dung, Nguyen Tuan Tai & Hai Nguyen Nam

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-017-4435-1



Springer

Multimed Tools Appl
DOI 10.1007/s11042-017-4435-1

Performance analysis of robust watermarking using linear and nonlinear feature matching

Ta Minh Thanh[1] · Keisuke Tanaka[2] · Luu Hong Dung[1] · Nguyen Tuan Tai[3] · Hai Nguyen Nam[4]

Received: 15 July 2016 / Revised: 6 December 2016 / Accepted: 20 January 2017

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 the linear and nonlinear features. In particular, we consider the geometric attacks and the signal processing attacks for the image watermarking. In order to analyze the efficiency of linear and nonlinear features, 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 our performance analysis of watermarking methods using the 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.

✉ Ta Minh Thanh
thanhtm@mta.edu.vn

Keisuke Tanaka
keisuke@is.titech.ac.jp

Luu Hong Dung
luuhongdung@gmail.com

Nguyen Tuan Tai
tainguyen.dlvn@gmail.com

Hai Nguyen Nam
nnhai61@gmail.com

[1] Le Quy Don Technical University, 236 Hoang Quoc Viet Street, Ha Noi City, Vietnam

[2] Tokyo Institute of Technology, 2-12-2, Ookayama, Meguro-ku, Tokyo, 152-8552, Japan

[3] Military Metrology Department (MMD), Ha Noi City, Vietnam

[4] Academy of Cryptography Techniques, Ha Noi City, Vietnam

Published online: 15 February 2017

Keywords Linear feature · Nonlinear feature · Feature point matching · Accelerated KAZE (AKAZE) feature · KAZE feature · SIFT feature · SURF · Rotation-Scaling-Translation (RST) attack · Image watermarking

1 Introduction

1.1 Background

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 [15]. 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 distributors.

Many attack algorithms were also proposed in order to destroy and to evaluate the robustness of watermark information. For example, StirMark benchmark for image http://www.petitcolas.net/fabien/watermarking/stirmark/ and StirMark benchmark for audio [13] are developed to destroy the watermark information in the robustness evaluation. Vidmark [7] 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 those 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 [12].

In the last decade, many methods that resist both the geometric attacks and the signal processing attacks have been reported.

First, 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 [8, 23] 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 distortions.

Second, the watermarking methods using the template were next exploited to resist the geometric attacks. In these approaches, the template information is also embedded with the watermark information into the embedded contents. The extracted template information is used to estimate the parameters of the geometric transformations. Based on the estimated parameters, the attacked image can be restored. The extraction process can be done

successfully. The method of Pereira et al. [11] extracted several points along two lines in the DFT domain as the template and embedded those into the embedded image. Assisted by those points, the watermark synchronization was done before the extraction process. Qi et al. [14] tried to improve the template-based watermarking by proposing an affine resistant watermarking scheme. They used the one-way hash function to generate the embedding positions. They added two lines as a template into the polar coordinate for estimating the parameters of the geometric attacks. Unfortunately, the drawback of their approach is that it is not robust against cropping attack. The template also can be detected and removed easily.

Third, the watermark schemes utilized the contents for embedding, called content-based watermarking, are quite popular recently. For example, Tang et al. [16] introduced to adopt the Mexican hat wavelet scale interaction method for extracting feature points. The disks of fixed radius centered at each feature point are normalized as the patches for watermark embedding and extraction. However, when the images are distorted, the normalized disks cannot be correctly extracted from the image since the normalized disks is sensitive to the image contents. Therefore, the robustness of these patches will decrease when the image is attacked. With another idea, Bas et al. [3] employed the Harris detector to extract the feature points. Based on those points, the Delaunay tessellation is defined for watermark embedding and extraction regions. However, a mis-detection of the feature points may deteriorate the watermark detection performance.

Fourth, in order to eliminate the synchronization process, the histogram-based watermarking techniques [5, 6, 21] were proposed for image, video, and audio. Most of them employed the histogram shape of the low frequency sub-band in the frequency domain to describe the watermark bit ("0" or "1"). Histogram shape is insensitive to processing attacks and geometric distortions. In the histogram-based watermarking, two successive bins or three successive bins of histogram were utilized to embed and to extract the watermark information. However, the limitation of the histogram-based watermarking is that the number of the embedded watermark bits is clearly limited.

Finally, the salient feature points-based watermark was drawn the attention recently. 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, [22] and [10] tried to extract the robust feature points and embedded 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. [18] and Thanh et al. [17] by using scale-invariant feature transform (SIFT) [9] and KAZE feature [2], respectively. However, high computation cost is still the drawback of the watermark schemes employing the robust feature points.

1.2 Our contributions

In this paper, we compare the efficiency of robust image watermarking methods using the linear and nonlinear features. We introduce a novel watermarking method based on the nonlinear scale spaces feature by using the accelerated KAZE (AKAZE) [1]. We also implement the image watermarking method based on the linear scale space feature, such as SIFT and SURF. Our contributions are listed as follows:

(1) The performance evaluation in [1] 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 those.
(3) We compare our embedding method with that based on three different existing features: KAZE, SIFT, SURF. AKAZE and KAZE feature belong to the nonlinear scale space feature. SIFT and SURF belong to the linear scale space feature. We embed the watermark information into the low-frequency of the DCT domain in order to achieve high robustness and blindness.
(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.

In this paper, the state-of-the-art linear and the nonlinear feature matching technique are employed in the experiments. The experiments show the types of the feature points which can survive against several attacks. The feature points surviving the attacks are recommended as reference points. We show the efficiency of linear and the nonlinear feature matching technique in the watermarking method. That makes value for the watermarking researches.

1.3 Roadmap

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.

2 The proposed method

2.1 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. [1] 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.

[1] SURF: Speeded Up Robust Features [4].

When a user claims about the authentication of digital 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.

2.2 Watermark permutation

Before embedding, we prepare a 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' as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod L. \tag{1}$$

Here, each pixel at coordinates (x, y) of W is moved to (x', y') of W'. W' is obtained by applying p times of the Torus permutation to the watermark. k is chosen from 1 to $L - 1$. In our method, the choices of k and p are unknown to the attackers. The Torus permutation is periodic with period P which depends only upon the parameters $k \in [1, L - 1]$ and $N < L < M$, So, we set $p \in [1, P]$. Figure 1 shows the periodic property of the Torus permutation where $k = 1$, $L = 64$, and $M = 97$, $N = 38$. In our permutation method, the period P of W is 96.

2.3 Watermark embedding algorithm

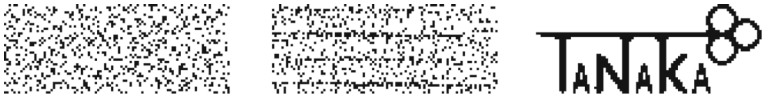
Suppose that the producer wants to deliver the image I with size of $S \times S$ to the user via network. He/she needs to embed the watermark information into the original before delivering. The embedding process shown in Fig. 2a is described in the following.

Step 1. The producer extracts the AKAZE feature points **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 coefficients from the low-band frequency in each block. Assuming that $f_1(u_1, v_1)$ and $f_2(u_2, v_2)$, where $u_1 \neq u_2, v_1 \neq v_2$,



(a) **(b)** **(c)**

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

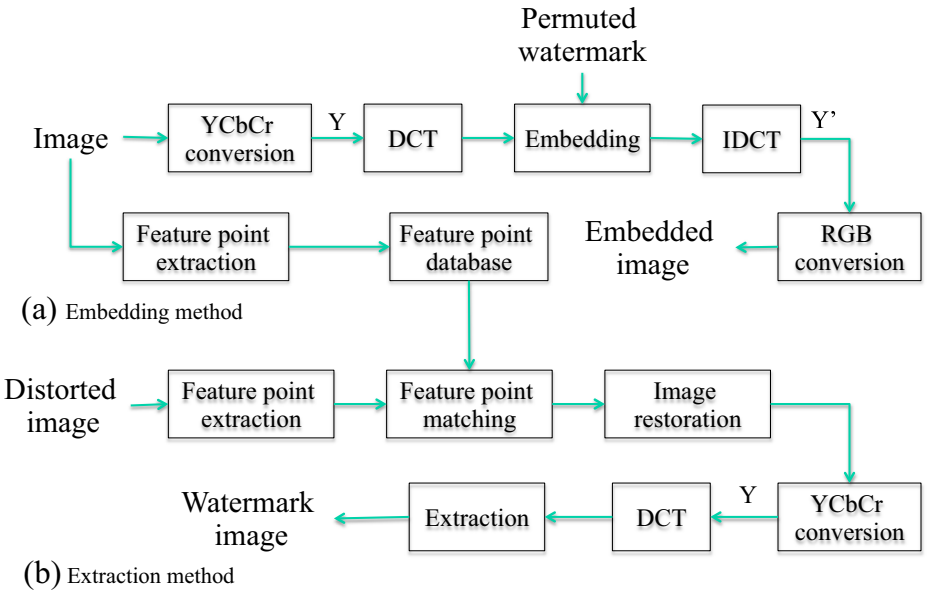


Fig. 2 Proposed embedding and extraction method

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 (2) and (3). One bit $w'(x', y')$ will be embedded into the DCT coefficient of the low-band frequency.

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

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

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

$$\begin{cases} f_1'(u_1, v_1) = sgn(f_1(u_1, v_1)) \times (ave - \frac{\alpha}{2}), \\ f_2'(u_2, v_2) = sgn(f_2(u_2, v_2)) \times (ave + \frac{\alpha}{2}), \end{cases} \tag{3}$$

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 $\mathbf{P}$, 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.

2.4 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 shown in Fig. 2b 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. The matching method is described in Section 2.5.

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. 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 Section 2.6.

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 (4).

$$w^*(x', y') = \begin{cases} 1 & \text{if } f_1^*(u_1, v_1) > f_2^*(u_2, v_2), \\ 0 & \text{if } f_1^*(u_1, v_1) \leq f_2^*(u_2, v_2). \end{cases} \tag{4}$$

Step 6. Repeat Steps 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.

2.5 Feature points matching method

First, the feature points extracted from the distorted image I' are matched with those of original image I.

Suppose that the feature points p_l, q_k are extracted from the distorted image I' and the original image I, respectively:

$$p_l = (x_l, y_l, \lambda_l, o_l, \boldsymbol{f}_l), \text{ for } l \in 1, \ldots, L, \tag{5}$$

$$q_k = (x'_k, y'_k, \lambda'_k, o'_k, \boldsymbol{f}'_k), \text{ for } k \in 1, \ldots, K, \tag{6}$$

where x_l, y_l, λ_l, and o_l are, respectively, the x- and y-position, the scale and the orientation of the l-th detected feature point of I'. The element $\boldsymbol{f}_l$ is the local edge orientation histogram of the l-th point. The symbol " $'$ " denotes the parameters of the feature points in I.

To find the matched points, for each point p_l in I', we compute its distances d_{1l} and d_{2l} to its two nearest neighbors in I as follows:

$$d_{1l} = \underset{k}{\text{argmin}} ||\boldsymbol{f}'_k - \boldsymbol{f}_l||, \tag{7}$$

$$d_{2l} = \underset{k \neq k_{\min}}{\text{argmin}} ||\boldsymbol{f}'_k - \boldsymbol{f}_l||, \tag{8}$$

where $k_{\min}$ is the index of a feature point which had the minimum distance d_{1l}.

Next, a ratio r_l is defined as $r_l = \frac{d_{1l}}{d_{2l}}$. Given a threshold τ, we can obtain a set of the matched points is $\mathbf{M} = \{(p_l, q_k) \mid r_l < \tau\}$. Note that, the matched region is found by the rectangle which covers all matched points in I'.

2.6 Estimation of attacked parameters

According to the feature point matching, the rotation, the scaling, and the translation parameter can be estimated based on some set $\mathbf{M}$ of the matched points.

First, we can estimate the scaling parameter Λ between the distorted image and the original image as follows:

$$\Lambda = \frac{\sum_{i=1}^{M} \lambda'_i}{\sum_{i=1}^{M} \lambda_i}, \tag{9}$$

where λ_i and λ'_i are the scales of matched feature points of I' and I, respectively, and $M = |\mathbf{M}|$.

Next, we estimate the angle θ of rotation by using the feature points matched to each other. The rotation angle is estimated as follows:

$$\theta = \frac{\sum_{i=1}^{M} (\theta'_i - \theta_i)}{M}, \tag{10}$$

where θ_i and θ'_i denote the centre angle of the feature point i of the original image and that of the corresponding feature point i of the distorted image, respectively.

After adjusting the differences of scale and rotation, we calculate the translation parameters δx and δy, which correspond to the differences in width and height, respectively. Let the coordinates of the feature points i is (x_i, y_i) of original image and that of the corresponding distorted image feature points is (x'_i, y'_i). Then, the translation parameters are estimated as follows:

$$\delta x = \frac{\sum_{i=1}^{M} (x'_i - x_i)}{M}, \delta y = \frac{\sum_{i=1}^{M} (y'_i - y_i)}{M}. \tag{11}$$

Based on the estimated parameters, we can restore the distorted image before watermark extraction. That makes our proposed method resist against strong attacks such as geometric attacks.

3 Experimental results

3.1 Test image and evaluational measures

To evaluate the performance of our proposed method, we conduct ten color images of the well known SIDBA (Standard Image Data-BAse) database www.vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/. All these test images are with size 512 × 512

pixels which shown in Fig. 3. The watermark image used in in the experiments is a binary image with size 97 × 38 which is shown in Fig. 1c.

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. The PSNR of $N \times N$ pixels of image $I(i, j)$ and $\dot{I}(i, j)$ is calculated as follows:

$$PSNR = 20 \log \frac{255}{MSE} \quad [\text{dB}]. \tag{12}$$

$$MSE = \sqrt{\frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \{I(i, j) - \dot{I}(i, j)\}^2}.$$

(MSE: Mean Square Error).

To provide objective judgment of the robustness of extraction, we use the normalized correlation (NC) value between the original watermark W and the extracted watermark W''. The NC value is calculated as follows:

$$NC = \frac{\sum_{i=0}^{97} \sum_{j=0}^{38} [W(i, j) \times W''(i, j)]}{\sum_{i=0}^{97} \sum_{j=0}^{38} [W(i, j)]^2}. \tag{13}$$

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

Fig. 3 Test images. Top row, left to right: image 1, image 2, image 3, image 4, image 5. Bottom row, left to right: image 6, image 7, image 8, image 9, image 10

are in [0, 1]. When SSIM value is 0, it means that $I \neq I'$. When SSIM value is 1, it means that $I = I'$.

3.2 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 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 ten 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. 4, when the value of α increases, the value of SSIM decreases, however, the value of NC increases. Therefore, 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 0.975 and the value of SSIM is 0.976. Thus, the embedding strength α is set to 0.11.

3.3 Quality of the embedded image

After choosing the appropriate value of $\alpha = 0.11$, we implement the proposed method and obtain the embedded images and the extracted watermarks. We calculate three parameters of ten images in order to confirm the efficiency of our proposed embedding method. The PSNR and the SSIM value denote the quality of the embedded image. The NC value denotes the robustness of the watermark extraction.

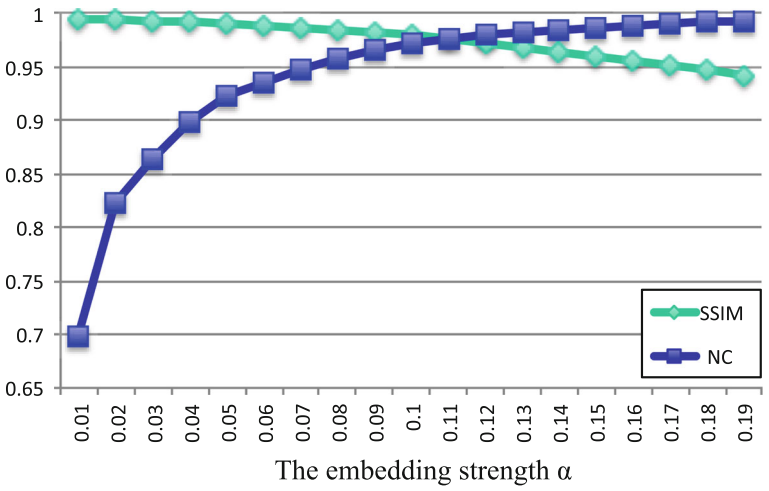


Fig. 4 The values of SSIM and NC with different embedding strength α

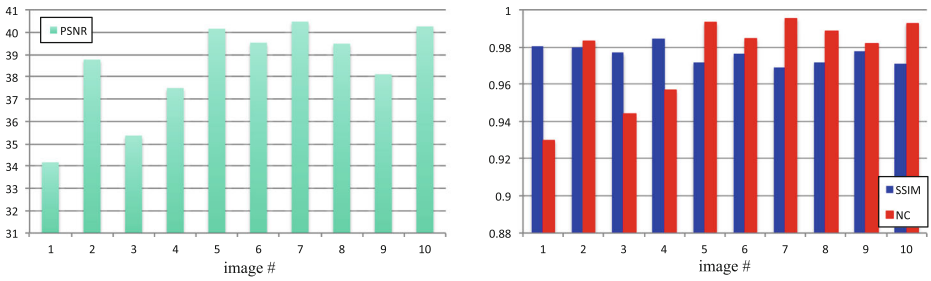


Fig. 5 The quality and robustness of the embedding method

According to the results shown in Fig. 5, we can see that, after embedding the watermark information, the PSNR values are over 34dB, the SSIM values are over 0.97. Therefore, no distortion can be observed in the watermarked images. It means that our embedding method achieves good imperceptibility. Additionally, all NC values are over 0.93. That denotes the robustness of watermark is close to 1.

3.4 Robustness comparison

In order to evaluate the robustness, we compare the experimental results of our proposed method (AKAZE-based) with those of another features based on the watermarking method. In particular, we compare with KAZE-based, SIFT-based, and SURF-based watermarking method. The embedding and extraction method applied on KAZE-based, SIFT-based, and SURF-based watermarking method is similar to the method which is explained in the Sections 2.3 and 2.4.

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

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

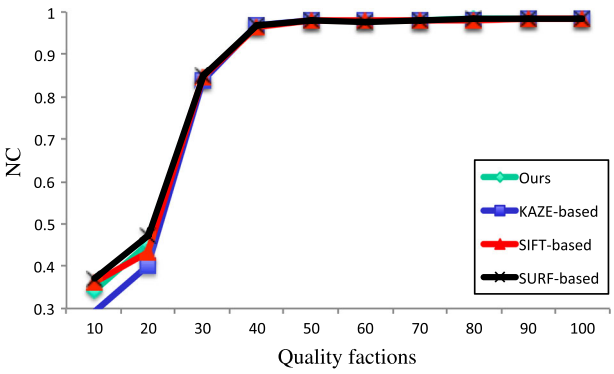


Fig. 6 JPEG attacks

is larger, lower compression ratio of the JPEG image is obtained and better visual quality of the JPEG image is retained.

Figure 6 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, and translation attack. 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

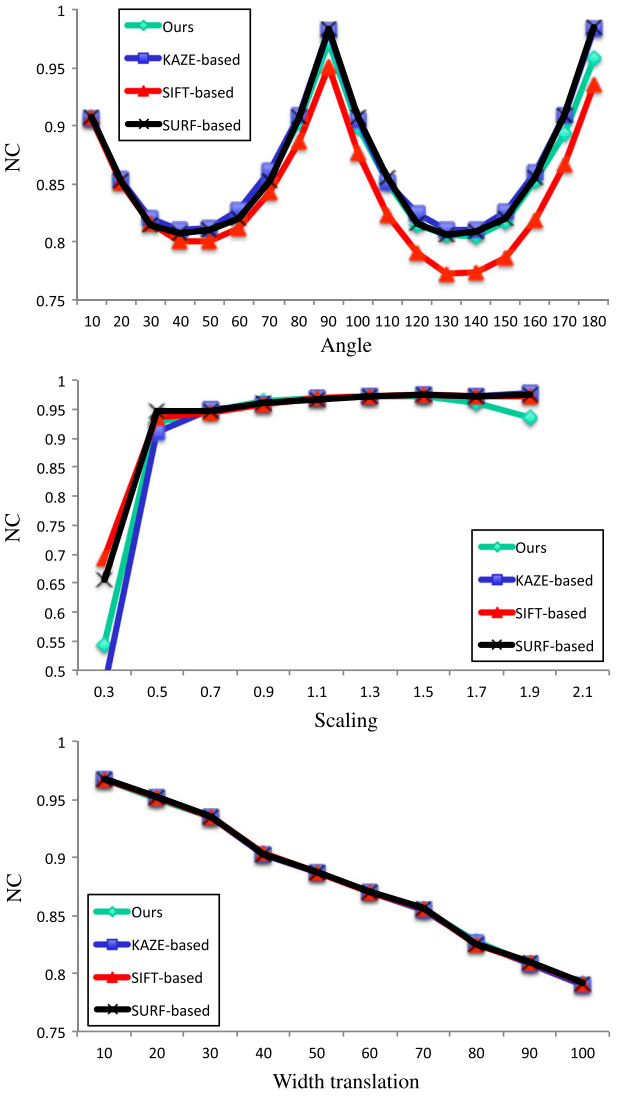


Fig. 7 Geometric attacks

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. The embedded images are also translated along the width of direction by the translation factors from 10 to 100.

Figure 7 shows 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 the values of NC are over 0.95. Finally, all methods present almost the same of robustness in the translation attacks. They seems to be robust with the translations factors belonging to $[0, 70]$ because the according NC values are over 0.85.

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 3×3, 5×5, 7×7, 9×9, 11×11, 13×13, 15×15. According to the results shown in Fig. 8, 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'

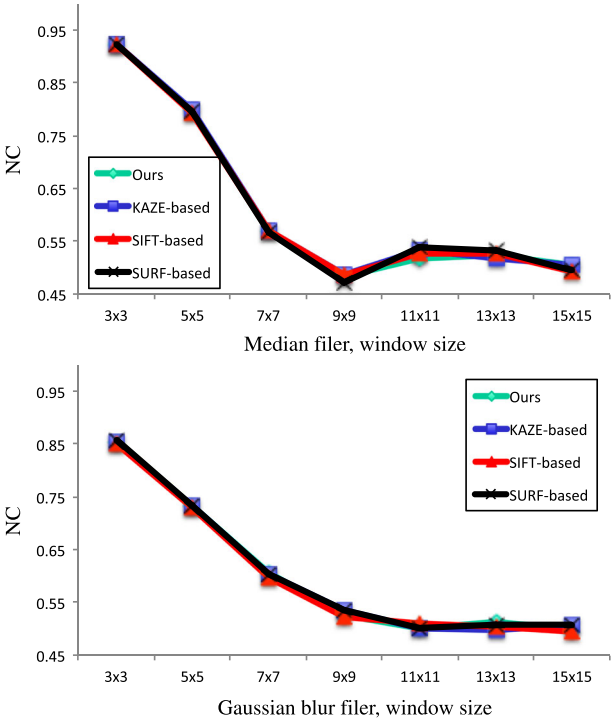


Fig. 8 Filtering attacks

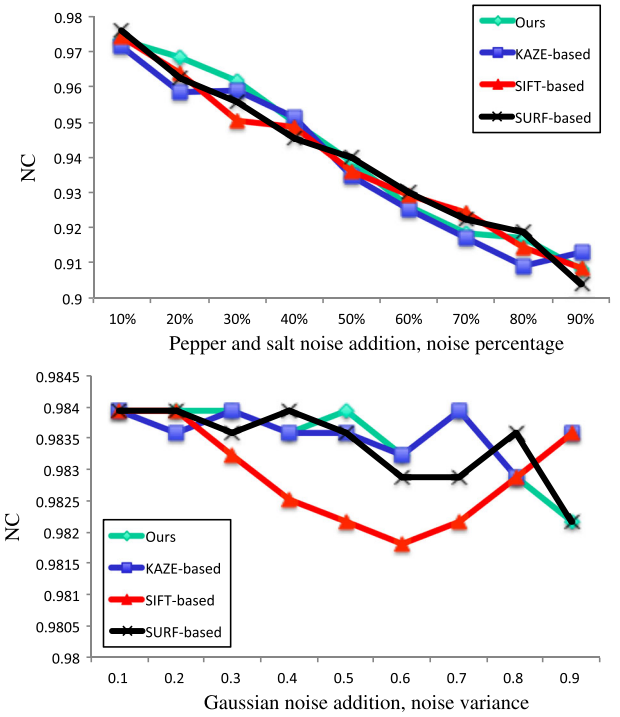


Fig. 9 Noise addition attacks

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. 9, 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

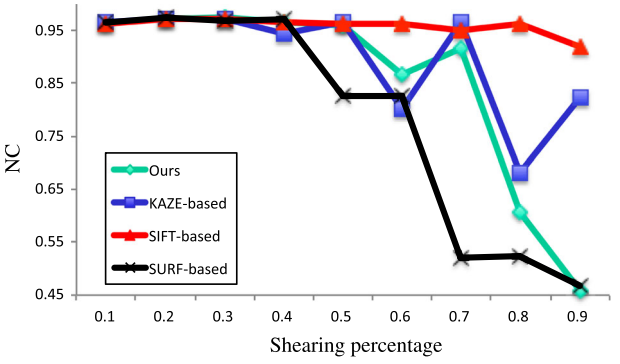


Fig. 10 Shearing attacks

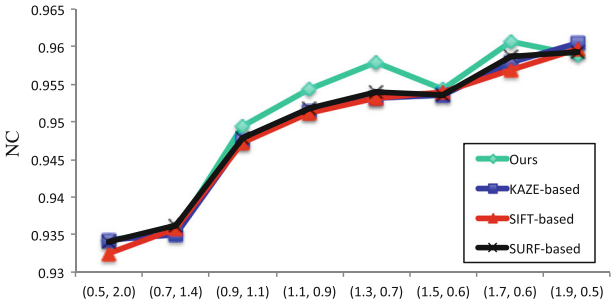


Fig. 11 Downsampling followed by upsampling attacks

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. 10 prove 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

Fig. 12 Comparison of the extracted watermarks in terms of visual perception and NC values

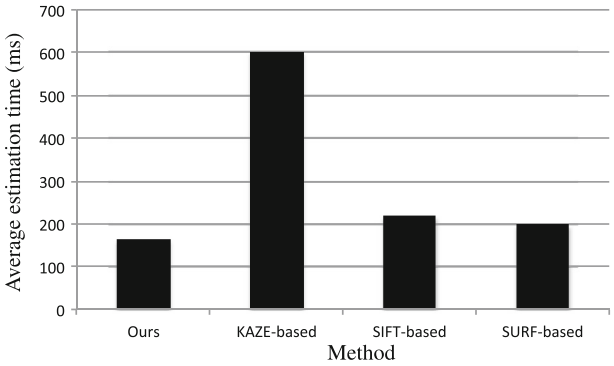


Fig. 13 Computation cost

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. 11. 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 feature, we pick up several watermark images extracted from corresponding attacked images. Those watermark images are described in Fig. 12. It can be seen from Fig. 12, 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.

3.5 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. 13, 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.

4 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. Based on the results, although we cannot conclude that the AKAZE-based method is better than others in all experiments, however,

its advantages can be seen in some cases such as rotation attacks, noise addition attacks, JPEG attacks and so on. The experiments show the types of the feature points which can survive against several attacks. The feature points surviving the attacks are recommended as reference points. The experiments and conclusions of this paper can be used as good reference for both research and engineering purpose. It also has value for the watermarking research.

References

1. Alcantarilla PF, Nuevo J, Bartoli A (2013) Fast explicit diffusion for accelerated features in nonlinear scale spaces british machine vision conference (BMVC)
2. Alcantarilla PF, Bartoli A, Davison AJ (2012) KAZE Features. ECCV, LNCS 7577:214–227
3. Bas P, Chassery J, Macq B (2002) Geometrically invariant watermarking using feature points. IEEE Trans Image Process 11(9):1014–1028
4. Bay H, Ess A, Tuytelaars T, Gool LV (2008) SURF: Speeded Up robust features. Comput Vis Image Underst (CVIU) 110(3):346–359
5. Coatrieux G, Pan W, Cuppens-Boulahia N, Cuppens F, Roux C (2013) Reversible watermarking based on invariant image classification and dynamic histogram shifting. IEEE Trans Inf Forensics Secur 8(1):111–120
6. Hernandez MC, Miyatake MN, Meana HP (2009) Robust watermarking based on histogram modification, IEEE International Conference Multimedia and Expo (ICME), 1748–1751
7. Hernndez-Avalos PA, Feregrino-Uribe C, Cumplido R, Garcia-Hernandez JJ (2010) Towards the Construction of a Benchmark for Video Watermarking Systems: Temporal desynchronization attacks, Proc. of the 53nd MWSCAS, 628–631
8. Lin CY, Wu M, Bloom Cox JA, Ingemar J, Miller ML, Lui YM (2001) Rotation, scale, and translation resilient watermarking for images. IEEE Trans Image Process 10(5):767–782
9. Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110
10. Nikolaidis A (2012) Local distortion resistant image watermarking relying on salient feature extraction, EURASIP Journal on Advances in Signal Processing, 97
11. Pereira S, Pun T (2000) Robust template matching for affine resistant image watermarks. IEEE Trans Image Process 6(9):1123–1129
12. Petitcolas F, Anderson R, Kuhn M (1998) Attacks on copyright marking systems, LNCS, 218–238
13. Petitcolas MS, Fabien AP, Raynal F, Dittmann J, Fontaine C, Seibel S, Fates N, Ferri LC (2001) StirMark benchmark: audio watermarking attacks, Proc. of Coding and Computing, 49–54
14. Qi X, Qi J (2004) Improved affine resistant watermarking by using robust templates, IEEE ICASSP, 495–408
15. Shih FY et al (2008) Digital Watermarking and Steganography: Fundamentals and Techniques, Taylor & Francis Group. CRC Press., Inc., Boca Raton
16. Tang CW, Hang HM (2003) A feature-based robust digital image watermarking scheme. IEEE Trans Signal Process 51(4):950–959
17. Thanh TM, Hiep PT, Tam TM, Tanaka K (2014) Robust semi-blind video watermarking based on frame-patch matching, AEU - International journal of electronics and communications, ISSN, 1434–8411
18. Viet PQ, Miyaki T, Yamasaki T, Aizawa K (2008) Robust object-based watermarking using feature matching. IEICE Trans Inform Syst E91-D(7):2027–2034
19. Voyatzis G, Pitas I (1996) Chaotic mixing of digital images and applications to watermarking. European Conf Multimed Appl Serv Tech (ECMAST96) 2:687–695
20. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: From error visibility to structural similarity. IEEE Trans on Image Process 13(4):600–612
21. Wang L, Ling H, Zou F, Lu Z (2012) Real-Time Compressed domain video watermarking resistance to geometric distortions. IEEE Multimed 19(1):70–79
22. Zhang X, Cao X, Li J (2013) Geometric attack resistant image watermarking based on MSER. Front Comp Sci 7(1):145–156
23. Zheng D, Zhao J, Saddik AE (2003) RST-Invariant digital image watermarking based on log-polar mapping and phase correlation. IEEE Trans Circuits Syst Video Technol 13(8):753–765

Ta Minh Thanh is Lecturer of Faculty of Information Technology, Le Qui Don Technical University, Ha Noi, Vietnam. He is also Postdoctoral Fellow of Department of Mathematical and Computing Sciences at Tokyo Institute of Technology. He received his B.S. and M.S of Computer Science from National Defense Academy, Japan, in 2005 and 2008, and his Ph.D. from Tokyo Institute of Technology, Japan, in 2015, respectively. He is the member of IPSJ Japan and IEEE. His research interests lie in the area of watermarking, network security, and computer vision.

Keisuke Tanaka is Associate Professor of Department of Mathematical and Computing Sciences at Tokyo Institute of Technology. He received his B.S. from Yamanashi University in 1992 and his M.S. and Ph.D. from Japan Advanced Institute of Science and Technology in 1994 and 1997, respectively. For each degree, he majored in computer science. Before joining Tokyo Institute of Technology, he was Research Engineer at NTT Information Platform Labs.

Luu Hong Dung is Lecturer of Faculty of Information Technology, Le Qui Don Technical University, Ha Noi, Vietnam. His research interests lie in the area of cryptography and network security.

Nguyen Tuan Tai is senior technical support of Military Metrology Department (MMD), Hanoi, Vietnam. He received his B.S of Telecommunication Engineering from Le Qui Don Technical University in 2004 and M.S of Telecommunication Engineering and M.S of Business Administration from La Trobe University, Australia in 2012 and 2013. His research interests lie in the areas of watermarking and system security.

Hai Nguyen Nam was born in 1961. He is a Lecturer with the Academy of Cryptography Techniques (Ha Noi, Vietnam). His research interests include cryptography, communication and network security. He has authored or co-authored more than 25 scientific articles, books chapters, reports and patents, in the areas of his research. He received his Ph.D. from the Hanoi University of Science and Technology (1996).