Multimed Tools Appl
DOI 10.1007/s11042-016-3750-2

An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information

Ta Minh Thanh[1,2] · Keisuke Tanaka[1]

Received: 21 November 2015 / Revised: 2 May 2016 / Accepted: 30 June 2016

Abstract We propose a new image zero-watermarking scheme based on the encryption of visual map feature (VMF) and permuted visual map feature (PVMF) of the original image with watermark information. To resist strong attacks, we employ the robust feature extracted from the host image by using the combination of QR decomposition and 1D-DCT. Since the feature extracted from the host image presents the coarse part of the host image, we call it VMF. For enhancing the security of VMF, we apply the permutation method on VMF based on the Torus permutation to obtain PVMF. We construct a new method of image zero-watermarking by the encryption of VMF and PVMF with copyright data, and then generate the master share and the ownership share. The master share is generated by comparison of two consecutive DC coefficients after the QR decomposition is applied. The ownership share is generated by encryption of the master share with copyright data. Experimental results show that the proposed method is robust against common processing and geometric attacks with low consuming time.

Keywords Visual map feature (VMF) · Permuted visual map feature (PVMF) · 1D-DCT · QR decomposition · Image zero-watermarking

✉ Ta Minh Thanh
thanhtm@mta.edu.vn

Keisuke Tanaka
keisuke@is.titech.ac.jp

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

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

Published online: 15 July 2016

1 Introduction

1.1 Background

During the last decade, the exchange of digital contents such as image, video, and music, become more commonly and convenient. It raises the serious piracy problem. Users can use image and video processing softwares (e.g. ImageMagick,[1] GIMP,[2] Photoshop,[3] and Vidmark [4], etc) to make the digital contents easily to copy, modify, and redistribute it via network. Therefore, the illegal copies, modifications, and distributions of the digital contents have become an important issues for the digital content providers.

There have been a lot of solutions for addressing the issue of copyright protection in literature. Those can be classified into four classes: cryptography, invisible watermarking, visual cryptography, and zero-watermarking.

The first solution for this issue is to employ the classical cryptography [2, 3]. The digital content is encrypted before distributing to users. Only users who has the decryption key, can decrypt the encrypted contents. This solution provides the safe way for the distribution of the digital contents via the Internet. However, the decrypted contents can be redistributed without the permission of provider. The redistributed contents do not contain license information, then everyone can use it. Therefore, it causes the illegal distribution even if by the legal users.

Digital watermarking is the second solution for this issue by embedding the copyright information into the digital contents. The embedded information, also called watermark, can be extracted later in order to prove the authentication, ownership, and traitor tracing [12]. The watermark information can be a random number sequence, ownership logo, and user ID. Based on the watermark information, the authenticator can specify the legal user of the watermarked contents.

In general, invisibility, robustness, and capacity of the watermark are important requirements for the watermarking techniques. That means the watermark should not make visible changes on digital contents in order to remain the quality of the original contents. Additionally, the watermark must be robust against the image attacks/distortions applied to the embedded contents. Finally, the watermark must be easily extracted to prove ownership and to detect the traitor. However, the tradeoff between the capacity and invisibility/robustness is always a challenging problem of the watermarking methods. Invisibility/robustness are sacrificed if a larger amount of watermark bits are embedded into the digital contents [1]. That makes hard to control the balance of capacity and the invisibility/robustness in the watermarking researches. Besides, the digital watermarking techniques are required to resist to geometric attack such as rotation, scaling, translation, and so on.

In order to improve capacity and to maintain invisibility/robustness of watermark, our previous works [15–17] had employed the q-logarithm frequency domain (q-LFD) for the watermarking methods. They can successfully improve the quality of the embedded contents with keeping the robustness of watermark extraction. They utilize the human visual characteristics feature of q-logarithm function to control the quality of the embedded contents.

[1] http://www.imagemagick.org/.

[2] http://www.gimp.org/.

[3] http://www.adobe.com/jp/products/photoshop.html.

However, in order to maintain the invisibility of the embedded contents, the appropriate parameter q must be chosen carefully.

To eliminate the controlling of tradeoff among the criteria of traditional watermarking methods, the visual cryptography scheme (VCS) proposed by Naor and Shamir [8] is the third solution. In VCS, some features of content and copyright data are employed to create the master share (M) and the ownership share (O) instead of embedding the copyright into the content itself. Those shares are scrambled images, therefore, they cannot be recognized by human eyes. The copyright data is only retrieved when those shares are superimposed each other.

The VCS scheme in [6] employs the feature of discrete wavelet transform (DWT) and the copyright data to make two share files. Unfortunately, the false alarm of their VCS is not true since the watermark can be retrieved from other contents even if a similar algorithm is used to extract its feature. In order to improve the robustness and security of VCS, Rawat et al. [11] employed fractional Fourier transform and singular value decomposition (SVD) to create the master share and the ownership share. Their method resists various processing attacks but it is complicated.

The fourth solution for this issue is zero-watermarking [9, 10, 22]. Unlike VCS, the features of the content are encrypted with the copyright data to generate ownership share. The master share is the features data of the content itself. The master share is registered to certification authority (CA) for copyright confirmation. When required, the copyright data can be retrieved by decrypting of the master share and the ownership share. Since the zero-watermarking does not embed the watermark information into the digital contents, the quality of the processed content is not degraded. Rani et al. [9] proposed the zero-watermarking in which the combination of the DCT and singular value decomposition are used to extract robust features of the host image. According to the experimental results, the method in [9] proved that it is robust against many strong attacks. However, its drawback is fragile under the center cropping and the tampering attacks. Also, its computation cost is quite high because the overlapping blocks are using for applying the DCT and singular value decomposition.

With another idea, Wanhong et al. [20] employed the highest effective bits (HEBs) of digital content to construct the zero-watermarking algorithm. Since the HEBs of host image presents the major features from image, it is not strongly affected under various attacks, therefore, the robustness of their scheme can be achieved. In the zero-watermarking video, Zhou et al. [21] used the feature of low frequency components achieved by Contourlet transform. Their method is robust against many strong attacks, especially compression attacks. However, its drawback is that it cannot resist the rotation attacks.

Recently, the zero-watermarking is also focused on another fields. For example, Li et al. [5] proposed a zero-watermarking based on QR code image and visual cryptography for identification photos. They extract the face region of the photos then apply the DWT and matrix norm computing to generate the invariant feature. Based on the invariant feature, the M and O can be generated by using the defined codebook beforehand. However, since their method employs the center of the image conveys mainly feature such as face, eyes, nose and mouth of the ID photos as the important region, therefore, it is fragile against center cropping attacks. In the paper [23], Zhou et al. give the idea to use the stroke-width characteristic for generating the zero-watermarking. They use statistics to calculate the stroke-width probability in scalable vector graphics (SVG) vector map, and then generate the zero-watermarking. However, the zero-watermarking algorithm is only appropriate for the scalable vector graphics image. Therefore, its applications is limited.

Although the zero-watermarking can solve the problem of controlling the balance between capacity and invisibility/robustness, the target of this research is that how to extract the important feature of the host image in order to construct the zero-watermarking. In this paper, we propose a robust and fast image zero-watermarking based on the combination of QR decomposition and 1D-DCT. By using the proposed method, we can improve the method in [9] more robustness and faster. Our method exploits the robust features of digital image and encrypts it with the watermark information. By doing so, our method can resist against strong attacks providing popular image processing softwares.

1.2 Challenging issues

Based on the aforementioned explanation, we summarize the following challenging issues:

(1) *Choosing the appropriate feature of image for generation of the master share and the owner share.*

To ensure the robustness of zero-watermarking under common processing attacks, the key point is how to extract the robust features from host image, and thus how to construct a robust zero-watermarking by using its features. Therefore, the first challenging issue is how to find out the suitable features of host image itself for generation of the master share and the owner share.

(2) *Improving the security of zero-watermarking share files.*

The share files of zero-watermarking is commonly registered for the certificate authority in order to confirm the copyright when the dispute happens. However, the master shares may disclosure some informations of the host image to others. According to revealed informations, it also disclosures the informations of the owners such as hobby, achievement, and so on. Therefore, the next challenging issue of our work is how to protect the share files of zero-watermarking method.

(3) *Improving the computation cost of zero-watermarking.*

The conventional methods did not consider the computation cost of proposed methods. Their methods may achieve good performance, but the computation cost is ignored. In the conventional methods, the host image and the host video are normally decomposed into 2D matrices, thus the feature of host image/video is obtained. It causes the problem of high computational cost, therefore, it may not suitable for real applications. For example, the method in [9] has high computational cost. We think that improving the computation cost of the proposed method is also important. Therefore, the last challenging issue is how to improve the computation cost of processes and also retain the robustness of watermark information.

1.3 Our contributions

We concentrate to solve the above challenging issues. We propose a new image zero-watermarking method using the combination of QR decomposition and 1D-DCT. Based on the processed results of QR decomposition and 1D-DCT, we obtain the VMF and PVMF of host image itself for generating the master share and owner share. In particular, we make the following contributions in this paper:

To solve the issue (1), we employ the frequency domain e.g. QR and 1D-DCT since they are robust against the common processing attacks. By using the frequency domains, we expect that the features of the host image are more efficient for the zero-watermarking.The proposed zero-watermarking is constructed by the combination of the QR decomposition and the 1D-DCT, therefore, it can resist against strong attacks.

In particular, we propose the visual map feature (VMF) of the original contents based on the QR decomposition and the 1D-DCT to generate the master share. The ownership share is created by taking bitwise XOR of the master share and the copyright data. The ownership share is registered to certification authority (CA) organization in order to check the authorization of content when digital property dispute happens.

In order to fulfill the issue (2), we propose the permutation technique applied on M file for enhancing its security. In general, M presents the coarse of the host image. That may reveal the important information of the host images. Therefore, the revealed M may show the some clues for the attackers to destroy the zero-watermarking. In order to protect M file, we employ the Torus permutation for randomizing the positions of pixels in M. By doing so, even if M is revealed via network, it does not give any informations of the host images. Therefore, the attackers cannot obtain any clues in order to attack M and O.

We also propose the permuted VMF (PVMF) by using the Torus permutation [19] to improve the security of VMF method. According to the PVMF, the permuted master share and the permuted ownership share are also generated. The advantage of our PVMF is that even if the permuted master share is revealed, it does not give some informations of the original contents for the attackers.

To optimize the computation cost of the zero-watermarking algorithm, we do not use 2D matrices for both QR decomposition and 1D-DCT. The 2D matrices are only used on the QR decomposition to extract the robust feature of QR coefficients. The 1D-DCT is used for decreasing computation cost with keeping the robustness against the compression attacks. With the using of 1D-DCT for decreasing the computation cost, we can solve the issue (3).

In this paper, we also implement various simulation experiments to demonstrate the performance of our proposed methods. Experimental results show that the proposed method has stronger robustness against most common attacks such as the JPEG compression, tamper, cropping, and so on. We can confirm that our performance is better than that of the method proposed by Rani et al. [9].

1.4 Roadmap

The rest of this paper is organized as follows: The conducted techniques are presented in Section 2. The proposal of methods (VMF and PVMF) are presented in Section 3. Subsequently, Section 4 gives experimental results and comparisons with other related methods. Finally, conclusions are made in Section 5.

2 Preliminary

In this paper, we utilize two techniques for preparing the features of the host image. We briefly summarize those in this section.

2.1 QR decomposition

In general, QR decomposition is used to decompose a matrix $\mathbf{B}$ for obtaining two matrices. For example, an $m \times n$ matrix $\mathbf{B}$ can be decomposed by the multiplication of matrix $\mathbf{Q}$ and $\mathbf{R}$. That can be expressed as follows:

$$\mathbf{B} = \mathbf{QR}, \tag{1}$$

where $\mathbf{Q}$ is $m \times n$ matrix and $\mathbf{R}$ is an upper triangular matrix. Let $\mathbf{B}$ and $\mathbf{Q}$ are described as $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n]$ and $\mathbf{Q} = [\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_n]$, respectively, where $\mathbf{b}_i$ and $\mathbf{q}_i$ are column vector. The matrix $\mathbf{R}$ can be calculated as follows:

$$\mathbf{R} = \begin{pmatrix} \langle \mathbf{b}_1, \mathbf{q}_1 \rangle & \langle \mathbf{b}_2, \mathbf{q}_1 \rangle & \ldots & \langle \mathbf{b}_n, \mathbf{q}_1 \rangle \\ 0 & \langle \mathbf{b}_2, \mathbf{q}_2 \rangle & \ldots & \langle \mathbf{b}_n, \mathbf{q}_2 \rangle \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \langle \mathbf{b}_n, \mathbf{q}_m \rangle \end{pmatrix}, \tag{2}$$

where $\langle \mathbf{b}_1, \mathbf{q}_1 \rangle$ is the inner product. Note that, in this paper, $n = m = 8$. As shown in (2), the first row can be obtained as follows:

$$\mathbf{R}_0 = [\mathbf{r}_0, \mathbf{r}_1, ..., \mathbf{r}_n] = [\langle \mathbf{b}_1, \mathbf{q}_1 \rangle, \langle \mathbf{b}_2, \mathbf{q}_1 \rangle, \ldots, \langle \mathbf{b}_n, \mathbf{q}_1 \rangle]. \tag{3}$$

Obviously, the absolute values of elements of $\mathbf{R}_0$ are larger than those of another rows. Compared with other transforms (e.g. DCT, DWT, ...), the QR decomposition can decompose a matrix (block) of pixel into an upper triangular matrix $\mathbf{R}$ and an orthogonal matrix $\mathbf{Q}$. Therefore, the important information of pixel block is concentrated in the upper triangular matrix $\mathbf{R}$, especially in the first row $\mathbf{R}_0$. That is different from other transform because the important information of pixel block is concentrated in the low frequency domain of those. In order to control the quality of the image, we only adjust the in the first row $\mathbf{R}_0$ instead of the low frequency domain.

The first row of matrix $\mathbf{R}$ has values and other rows are nearly zero. So if other rows are selected for the watermark embedding, the distortion of quality may be significant visual perception in the embedded image. If the first row of matrix $\mathbf{R}$ is selected for the watermark embedding, the high quality of the embedded image can be obtained. Therefore, even if the original image is altered, the absolute value of elements of $\mathbf{R}_0$ may not be affected too much [7]. In general, the coefficients $\mathbf{r}_i \, (0 \leq i \leq 3)$ of the matrix $\mathbf{R}_0$ are employed to embed the watermark information since its has the most energy of host image [14].

Inspired of that idea, we also want to employ the QR decomposition for constructing the owner share and master share files. It can be expected more robust comparing the conventional zero-watermarking methods, such as the method of Rani [9].

2.2 1D-DCT

The DCT is known as the basic transform coding technique for the multimedia digital such as JPEG and MPEG standards. The DCT is normally applied on the non-overlapping blocks of the host image, therefore, it respects to the spatial quality of the image. In the DCT, most the signal energy of the host image also lies at low frequency coefficients. To reduce the computation cost of 2D-DCT, we employ 1D-DCT on the same non-overlapping blocks. The 1D-DCT is given as follows:

$$F(u) = C(u) \times \sum_{x=0}^{N-1} f(x) \times cos[\frac{(2x+1)u\pi}{2N}], \tag{4}$$

where $u = 0, 1, \cdots, N-1$. The coefficient $C(u)$ is specified depending on the value of u as follows:

$$\begin{cases} C(u) = \sqrt{\frac{1}{N}} & \text{for } u = 0 \\ C(u) = \sqrt{\frac{2}{N}} & \text{for } u = 1, 2, 3, \cdots, N-1 \end{cases} \tag{5}$$

Here, $f(x)$ can be the 1D row of input pixels with the length is N. $F(u)$ is the 1D-DCT frequency domain. $C(u)$ is called the normalizing factor.

In this paper, we apply the 1D-DCT on the 1D row of the matrix $\mathbf{R}_0$ generated from the QR decomposition. It also generates the low frequency and the high frequency of 1D-DCT output. We use the low frequency coefficients for constructing the zero-watermarking. By doing so, we expect that it can improve the computation cost and we can apply the proposed method for realtime applications.

2.3 Advantages from combination of QR decomposition and 1D-DCT

The proposed method employs the QR decomposition and 1D-DCT to generate the VMF and PVMF. The reasons of choosing the QR decomposition and 1D-DCT are:

(1) The energy of the host image is concentrated in the first row $\mathbf{R}_0$ of matrix $\mathbf{R}$ after the QR decomposition [7, 13]. It is more concentrated in the DC coefficients when the 1D-DCT is applied on $\mathbf{R}_0$.

(2) The computation cost by using the combination of the QR decomposition and 1D-DCT is lower than that in the methods of [9, 10, 22].

By using the combination of the QR decomposition and the 1D-DCT, we can extract the robust VMF and PVMF since $\mathbf{R}_0$ is slightly affected by the processing attacks and the geometric attacks. We also can expect that our proposed method is faster than conventional methods.

3 The proposed zero-watermarking

In this section, we explain the proposal of zero-watermarking using robust VMF and PVMF. The main idea is to combine the QR decomposition with the 1D-DCT for constructing the robust share files of the zero-watermarking. By using the proposed VMF and PVMF, we easily improve the robustness of zero-watermarking and reduce the computation cost of the proposed methods.

Let I and W be the original image with size $N \times N$ and the binary copyright data with size $L \times L$, respectively. We generate two share files based on the feature of I and W. There are two processes in our method: the construction of the share files and copyright identification processes. The construction processes are based on the proposed visual map feature (VMF) and permuted visual map feature (PVMF).

3.1 Proposal of visual map feature (VMF)

The overview of the proposed VMF method is shown in Fig. 1. Suppose $\mathbf{C}$ is image feature generation function. Four steps involved in $\mathbf{C}$ to generate the VMF are explained as follows:

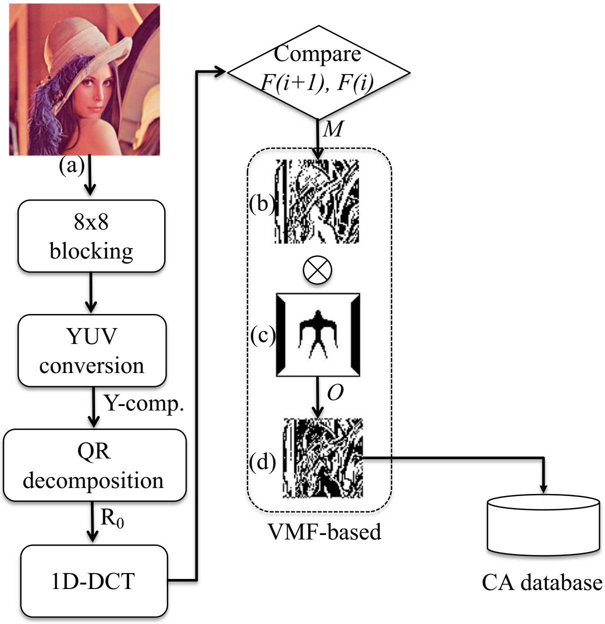


Fig. 1 The proposed VMF method

Step 1. Convert the RGB image I to YUV color space. Divide Y-component into the non-overlapping blocks $\mathbf{B}$ of size 8×8. The number of non-overlapping blocks is $N/8$.

We only use the luminance Y-component to extract the feature of the original more robust since the chrominance (U and V) components is perceptually less sensitive to human visual system compared to the luminance (Y-component)[4]

Step 2. Apply the QR decomposition on each non-overlapping block $\mathbf{B}$ to obtain $\mathbf{R}_0$.

$$\mathbf{B} = \mathbf{QR}, \tag{6}$$

where $\mathbf{Q}$ is $m \times n$ matrix and $\mathbf{R}$ is an upper triangular matrix. Let $\mathbf{B}$ and $\mathbf{Q}$ are described as $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_n]$ and $\mathbf{Q} = [\mathbf{q}_1, \mathbf{q}_2, ..., \mathbf{q}_n]$, respectively, where $\mathbf{b}_i$ and $\mathbf{q}_i$ are column vector. In this paper, we set $m = n = 8$.

Step 3. Apply the 1D-DCT on each $\mathbf{R}_0$ to retrieve the DC coefficients $F(i), i = 0, 1, \cdots, 7$.

Step 4. Two consecutive DC coefficients are compared to generate the VMF of the original image. This VMF is used as the master share M (Fig. 1b) and each point of M is generated by comparison of $F(i)$ and $F(i+1)$:

$$M(x, y) = \begin{cases} 1 & \text{if } F(i+1) > F(i), \\ 0 & \text{otherwise}, \end{cases} \tag{7}$$

where $x, y \in [0, 7)$.

Therefore, M is generated by $M = \mathbf{C}(I)$. The visibility of M can be observed as described in Fig. 1b. M holds the robust edge feature of the original image.

[4] https://en.wikipedia.org/wiki/YUV.

3.2 Proposal of permuted visual map feature (PVMF)

Although the proposed VMF method can generate the robust feature of the host image, however, it reveals the meaning content of the host images. The attackers may utilize the revealed features to destroy the zero-watermarking system.

In order to improve the security of VMF, we include the Torus permutation function [19], called **P**, for VMF to create PVMF. The PVMF method can be shown in Fig. 2.

Step 1. Employ the Step 1 $\sim$ Step 4 of the VMF method in Section 3.1. The file M (Fig. 2b) is generated as follows:

$$M = \mathbf{C}(I). \tag{8}$$

Step 2. Apply the Torus permutation function on M to obtain the permuted feature file M_p (Fig. 2c) of the host image.

$$M_p = \mathbf{P}(\mathbf{C}(I)). \tag{9}$$

The Torus permutation **P** is known as a scrambled function. We employ **P** to scramble M generated by the proposed VMF method. It can be described as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod } L. \tag{10}$$

Here, each pixel at coordinates (x, y) of M is moved to (x', y') of M_p. The p times of transformation are performed on the M. Transformation matrix element k and the number of p are kept as secret keys. In our method, the choices of k and p are unknown to the attackers. The Torus permutation function is periodic with the period P and P depends only upon the parameters $k \in [1, L-1]$ and L, where $L \times L$ is the size of M and $p \in [1, P]$.

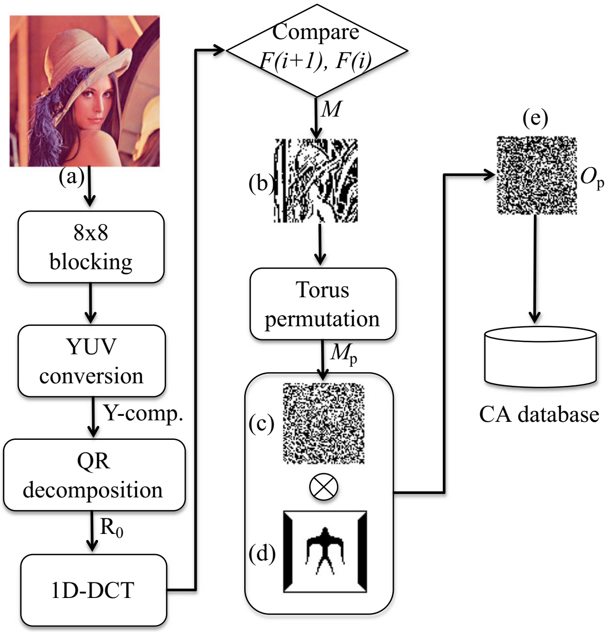


Fig. 2 The proposed PVMF method

Fig. 3 Permuted watermark by Torus permutation after p times, where (**a**) p=20, (**b**) p=60, and (**c**) p=96

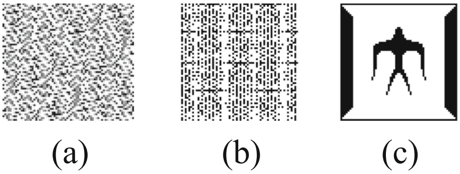


Figure 3 shows the periodic property of the Torus permutation where $k = 1$ and $L = 64$. It shows that the period P of M is 96.

3.3 Construction of ownership share

The ownership share O (Fig. 1d) and the permuted ownership share O_p (Fig. 2e) are generated by encryption of the master share M and M_p with the copyright data W (Fig. 1c), respectively. To obtain the ownership share O and the permuted ownership share O_p, we apply the XOR operation between M and M_p with W as follows:

$$O = M \oplus W, \;\; O_p = M_p \oplus W. \tag{11}$$

Since O_p is scrambled by the Torus permutation, therefore, the security of the original content is improved. The random location k of the permutation matrix, the permuted time p, and the period P of $\mathbf{P}$ are kept as the secret key by the copyright owner. The detailed explanation of k, p, and P can be referred in paper [15, 16]. The owner files O and O_p are registered for CA in order to check the copyright of content.

3.4 Copyright identification

Suppose the property dispute concerning the suspected image I' happens. The CA should judge the rightful owner of the suspected image. The CA asks the owner to provide the secret key and extracts the master share M' and M'_p of I' by using the same algorithm described in Sections 3.1 and 3.2. That means $M' = \mathbf{C}(I')$ and $M'_p = \mathbf{P}(\mathbf{C}(I'))$. Recall that the secret key of the owner is k, p, and P of the Torus permutation function $\mathbf{P}$.

Since CA has the ownership share O and O_p, CA can retrieve the copyright data W' by stacking M' and M'_p with O and O_p.

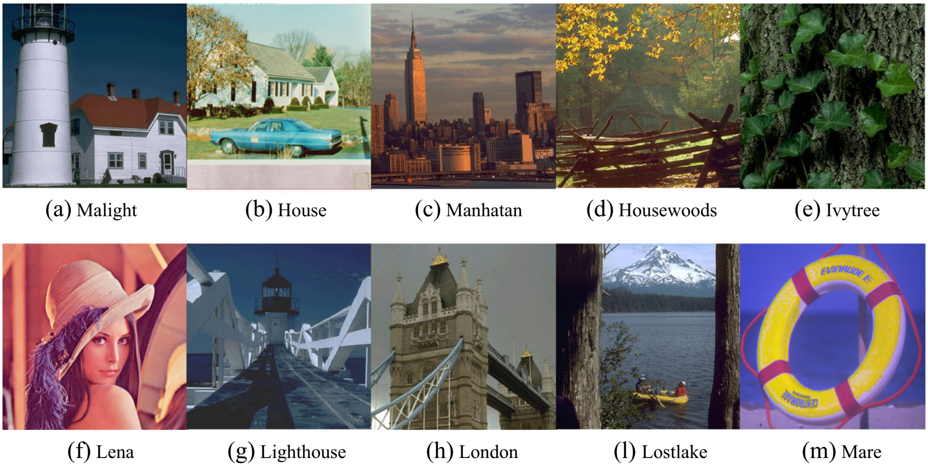
In case of VMF-based method, CA can obtain the watermark W' as follows:

$$\begin{aligned} W' = M' \oplus O &= \mathbf{C}(I') \oplus \{\mathbf{C}(I) \oplus W\} \\ \Rightarrow \;\; W' &= W \text{ if } \mathbf{C}(I') = \mathbf{C}(I). \end{aligned} \tag{12}$$

In case of PVMF-based method, the extracted watermark W' can be obtained as follows:

$$\begin{aligned} W' = M'_p \oplus O_p &= \mathbf{P}(\mathbf{C}(I')) \oplus \{\mathbf{P}(\mathbf{C}(I)) \oplus W\} \\ \Rightarrow \;\; W' &= W \text{ if } \mathbf{P}(\mathbf{C}(I')) = \mathbf{P}(\mathbf{C}(I)). \end{aligned} \tag{13}$$

According to W', CA can judge the rightful owner of the suspected image.


(a) Malight (b) House (c) Manhatan (d) Housewoods (e) Ivytree

(f) Lena (g) Lighthouse (h) London (l) Lostlake (m) Mare

Fig. 4 Experimental images

4 Experimental results

4.1 Test images and evaluational measures

To assess the performance of the proposed algorithm, we conduct ten color images of the well known SIDBA (Standard Image Data-BAse) database.[5] All test images are with size $N \times N = 512 \times 512$ pixels. The conducted images are shown in Fig. 4. The watermark image is a binary image with size $L \times L = 64 \times 64$ which is shown in Fig. 1c.

In order to evaluate the quality of watermarked images, we employ PSNR (Peak Signal to Noise Ratio) criterion [18]. The PSNR of $N \times N$ pixels image of $I(i, j)$ and $I'(i, j)$ is calculated as follows:

$$PSNR = 20 \log \frac{255}{ME} \quad [\text{dB}], \tag{14}$$

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

$$(ME : \text{Mean Square Error}).$$

To judge the robustness, we use the normalized correlation (NC) value between the original watermark W and the extracted watermark W' [18]. The NC value is calculated as follows:

$$NC = \frac{\sum_{i=0}^{L} \sum_{j=0}^{L} [W(i, j) \times W'(i, j)]}{\sum_{i=0}^{L} \sum_{j=0}^{L} [W(i, j)]^2}, \tag{15}$$

where $L \times L$ is the size of W.

[5] http://decsai.ugr.es/cvg/index2.php.

Table 1 Average PSNR[dB] and comparison of average NC values from ours and those of Rani et al. [9]

Attack	Method PSNR	PVMF NC	VMF NC	Rani [9] NC
Scaling	33.20	0.939	0.942	0.978
Rotation and crop	18.81	**0.913**	**0.937**	0.812
Translation	14.51	0.926	0.960	0.999
Gaussian noise	32.05	0.895	0.897	0.984
Pepper and Salt	18.86	0.801	0.803	0.935
Blur	22.79	0.829	0.830	0.931
Shearing	28.39	0.955	0.958	0.989
JPEG	35.56	0.901	0.903	0.978
Brightness	15.24	0.888	0.888	0.972
Cropping	16.04	**0.899**	**0.904**	0.536
Tampering	16.45	**0.943**	**0.943**	0.809
UpDown	31.91	0.947	0.947	0.990

The bold entries describes that the experimental results of our methods are better than Rani et al. [9]

In our experiments, we calculate the PSNR value for each attacked image and the NC value for each watermark extracted from the attacked images. In general, if the PSNR value is larger than 35dB, the quality of the attacked 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 against the attacks.

4.2 Robustness comparisons

In order to evaluate the robustness of the proposed method, we attacked the experimental images by several attacks including processing and geometric attacks. We also compared our NC values with those of the method [9]. In our experiments, the original images are subject to the following attacks.

Geometric attacks are considered as the first challenge because they destroy the feature of images. The images are scaled with different scaling factors (scaling attack). They are also rotated by several angles (rotation attack). The scaling factors with ranging from 0.3 to 1.9 and the rotation angles with ranging from 10° to 100° are employed in our tests. The attacked scaling factors and rotation angles are estimated by the method in [18]. The

Table 2 Center cropping: Average PSNR[dB] and comparison of average NC values from ours and those of Rani et al. [9]

Attack	Method PSNR	PVMF NC	VMF NC	Rani [9] NC
Cropping 1/9	21.59	**0.968**	**0.972**	0.637
Cropping 2/9	15.17	**0.888**	**0.896**	0.503
Cropping 3/9	11.23	**0.769**	**0.730**	0.502
Cropping 4/9	9.59	**0.684**	**0.637**	0.502

The bold entries describe that the experimental results of our methods are better than Rani et al. [9]

attacked images are then rescaled or re-rotated by the estimated scaling factor or the estimated angle in the opposite direction. The images are also translated along the width of direction by the translation factors from 10 to 100 (translation attack). We assume that the size of host image is known beforehand.

Noise addition attack is common distortion in which the noise is added to the images. Gaussian white noise and 'pepper and salt' noise are considered to attack the images. The Gaussian white noise of zero mean and variance ranging from 0.01 to 0.15, and 'pepper and salt' noise with percentage ranging from 1% to 10% are added into the copyrighted images.

Filtering attack is also tested in our experiments. The Gaussian blur filtering attacks are used and are adopted with window sizes of 1 × 1 ∼ 10 × 10.

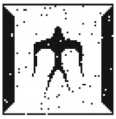
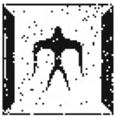
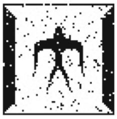
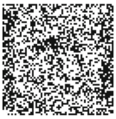
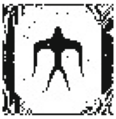
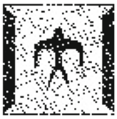
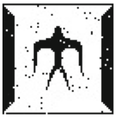
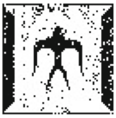
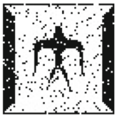
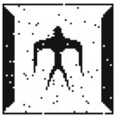
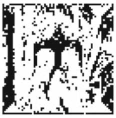
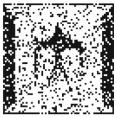
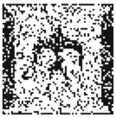
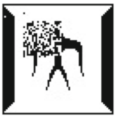
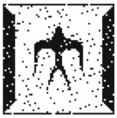
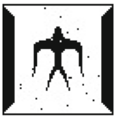
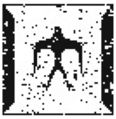
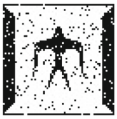
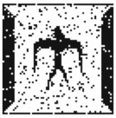
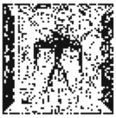
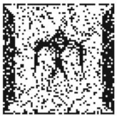
Attack type	Method [14]	Our VMF	Our PVMF
Scaling 0.5	 NC=0.981	 NC=0.989	 NC=0.987
Rotation 50°	 NC=0.624	 NC=0.941	 NC=0.904
Gaussian noise addition Zero mean, variance=0.15	 NC=0.985	 NC=0.942	 NC=0.989
JPEG QF=10	 NC=0.983	 NC=0.848	 NC=0.820
Tampering	 NC=0.794	 NC=0.952	 NC=0.953
Pixelize	 NC=0.994	 NC=0.947	 NC=0.944
Puzzle	 NC=0.916	 NC=0.810	 NC=0.811

Fig. 5 Comparison of our NC values and those of [9]

We also present the *shearing attack* on the copyrighted images. In our experiments, the shearing percentages in x axes with ranging from 10% to 90% are applied. The attacked images are re-sheared at the same time with the estimated sharing factors by the method in [18].

In the *JPEG compression*, the quality factors with range from 90 to 10 are employed to compress the images.

In the *brightness attack*, we change the brightness factors from -127 to +127 with uniform step as 10.

Cropping attack is implemented by cropping 1/9, 2/9, 3/9, and 4/9 of cpyrighted image.

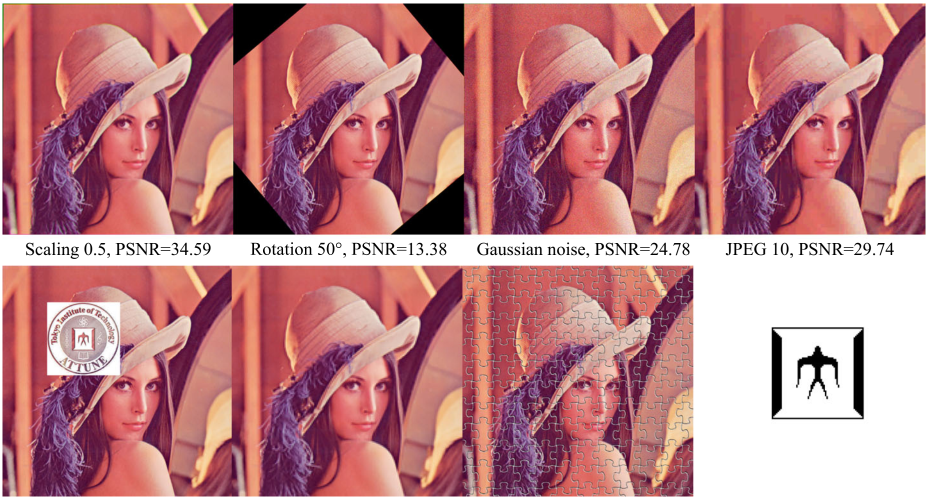
Tampering attack is randomly replaced by a preprepared logo at random position for ten times.

Finally, we apply the downsampling followed by upsampling attacks to the images. We do downsampling to the images and then, do upsampling to inverse to its original size. The downsampling factor is set from 0.3 to 2.0 with uniform step as 0.2.

After applying above attacks, we calculate the PSNR values of the attacked images. The NC values of the extracted watermarks from the attacked images are also calculated. An average PSNR value and an average NC value are retrieved for ten attacked images and for ten extracted watermarks.

Those results are shown in Table 1. The proposed method is robust against almost the attacks in Table 1 since the average NC values are over 0.8. Therefore, our methods can be applied for the copyright protection applications. Although the proposed methods are not better than the method in [9] in some cases, however, ours can improve the consuming cost for real applications. Ours are more robust against only 'rotation and crop', cropping, and tampering attacks as compared to the method of Rani et al. [9]. The reason is that our VMF and PVMF can be remained under those attacks whereas the feature of [9] may be strongly affected.

Especially, the method of [9] is fragile under center cropping whereas our methods are robust. Table 2 shows the comparison results. Rani et al. [9] encrypted the watermark data in the center of image since the center of image is expected to be most significant feature of the



Scaling 0.5, PSNR=34.59 | Rotation 50°, PSNR=13.38 | Gaussian noise, PSNR=24.78 | JPEG 10, PSNR=29.74

Tampering, PSNR=17.63 | Pixelize, PSNR=29.25 | Puzzle, PSNR=18.29 | Original watermark

Fig. 6 Experimental attacked images

Table 3 Comparison of complexity

Operations	The proposed methods	The method of Rani [9]
Blocks	Non-overlapping	Overlapping
Blocks dimension	2D & 1D	2D & 2D
2D DCT $(n \times n)$	N/A	$O(n^2)$
2D SVD $(m \times n)$	N/A	$O(mn^2)$
2D QR $(n \times n)$	$O(n^2)$	N/A
1D DCT	$O(n)$	N/A

images. Our methods do not focus on only the center of image. We encrypt the watermark data with VFM/PVFM which remain the feature of entire image. Therefore, the proposed methods are robust against even if strong center cropping attacks are executed.

Some extracted watermarks using the distorted Lena images are shown in Fig. 5. The corresponding distorted images are shown in Fig. 6. It includes the Photoshop software processing (Pixelize and Puzzle). It is clear that our VMF and PVMF are more superior than the method of Rani et al. [9] in some cases.

4.3 Comparison of computation time

In order to compare the complexity of the proposed methods and that of the method in [9], we analyze the complexity in terms of operations and summarize them in Table 3, where N/A means *not available*. According to Table 3, the proposed methods have less computation cost compared with the method of [9].

We also compare the time consuming of three methods. All experiments are implemented on Macbook Air system with OSX 10.9, memory 4GB 1600Mhz DDR3. Figure 7 shows the comparison results. The VMF demonstrates the best computation cost followed by the PVMF and the method of Rani et al. [9]. The reason is that the VMF does not need to permute or randomize the feature of image.

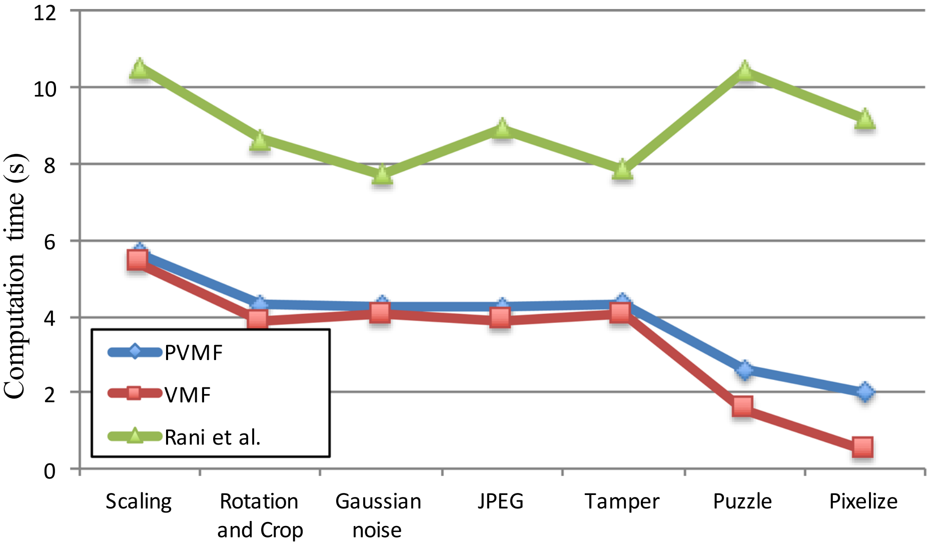


Fig. 7 Comparison of average computation time

5 Conclusion

In this work, we have proposed a zero-watermarking method based on the encryption of VMF with the copyright information. In order to increase the security, we have also proposed the PVMF method. In our methods, the original image is not affected by watermark embedding. The watermark size is also not limited. Since the proposed methods preserve the feature of entire image, therefore, it especially is robust against strong cropping and tampering attacks. Certainly, it can resist against the common processing and geometric attacks. Moreover, the consuming time of our methods is lower than [9].

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.

References

1. Barni M, Bartolini F (2004) Watermarking systems engineering: enabling digital assets security and other applications. Marcel Decker, New York, pp 6–11
2. Ferguson N, Schneier B, Kohno T (2008) Cryptography engineering: design principles and practical applications. Wiley Press, ISBN: 9780470474242
3. Haouzia A, Noumeir R (208) Methods for image authentication: a survey. Multimed Tools Appl 39(1):1–46
4. 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. In: Proc. of the 53nd MWSCAS, pp 628–631
5. Li D, Liu Z, Cui L (2016) A zero-watermark scheme for identification photos based on QR code and visual cryptography. Int J Secur Appl 10(1):203–214
6. Lou DC, Tso HK, Lin JL (2007) A copyright protection scheme for digital images using visual cryptography technique. Comput Standards Interf 29:125–131
7. Naderahmadian Y, Hosseini-Khayat S (2014) Fast and robust watermarking in still images based on QR decomposition. Multimed Tools Appl 72:2597–2618
8. Naor M, Shamir A (1995) Visual cryptography. In: Proc. of the advances in cryptology–EUROCRYPT'94, LNCS, vol 950. Springer-Verlag, pp 1–12
9. Rani A, Balasubramanian R (2014) An image copyright protection scheme by encrypting secret data with the host image. Multimed Tools Appl:1–16
10. Rani A, Balasubramanian R, Kumar S (2013) A robust watermarking scheme exploiting balanced neural tree for rightful ownership protection. Multimed Tools Appl:1–24
11. Rawat S, Raman B (2012) A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. Signal Process 92:1480–1491
12. Shih FY (ed) (2008) Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis Group, CRC Press., Inc., Boca Raton
13. Su Q, Niu Y, Zou H, Zhao Y, Yao T (2014) A blind double color image watermarking algorithm based on QR decomposition. Multimed Tools Appl 72:987–1009
14. Sua Q, Niu Y, Wanga G, Jiac S, Yuea J (2014) Color image blind watermarking scheme based on QR decomposition. Signal Process 94:219–235
15. Thanh TM, Tanaka K (2014) A proposal of novel q-DWT for blind and robust image watermarking. In: Proc. of IEEE 25th International symposium on personal, indoor and mobile radio communications - (PIMRC)
16. Thanh TM, Tanaka K (2015) Blind watermarking using QIM and the quantized SVD domain based on the q-logarithm function. In: Proc. of the 10th International joint conference on computer vision, imaging and computer graphics theory and applications - VISAPP. Germany
17. Thanh TM, Tanaka K (2015) The novel and robust watermarking method based on q-logarithm frequency domain. In: International journal of multimedia tools and applications (MTAP), ISSN: 1573–7721. Springer (to be appeared)

18. Thanh TM, Hiep PT, Tam TM, Tanaka K (2014) Robust semi-blind video watermarking based on frame-patch matching. In: AEU - International journal of electronics and communications, ISSN 1434–8411
19. Voyatzis G, Pitas I (1996) Applications of torus automorphisms in image watermarking. Proc Int Conf Image Processing (ICIP) 3:237–240
20. Wanhong N, Huiqin Y (2009) A zero watermarking algorithm based on the MB construction key. Appl Comput Syst 12(18):66–69
21. Zhou Z, Yang G, Quan T, Wang Z (2010) Digital video zero-watermarking algorithm based on contourlet transform. Microcomput Inform 12(26):82–84
22. Zhou Y, Jin W, Kumar S (2011) A novel image zero-watermarking scheme based on DWT-SVD. In: Proc. of the International conference on multimedia technology (ICMT), pp 2873–2876
23. Zhou L, Huang Y, Chen Z, Li X (2015) A zero-watermarking algorithm of SVG vector map based on stroke-width characteristic. In: The 2nd International conference on intelligent computing and cognitive informatics (ICICCI 2015), pp 34–37

Ta Minh Thanh is Lecturer of Faculty of Information Technology, Le Qui Don Technical University, Ha Noi, Viet Nam. 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.