

The novel and robust watermarking method based on *q*-logarithm frequency domain

Ta Minh Thanh^{1,2} \cdot Keisuke Tanaka¹

Received: 20 December 2014 / Revised: 2 June 2015 / Accepted: 21 July 2015 © Springer Science+Business Media New York 2015

Abstract In general, watermarking techniques on transform domain are always mainly researched in literature since it is robust against several attacks. In this paper, we continue to focus on the transform domain and extend it to the novel frequency domain, called q-logarithm frequency domain (q-LFD), for robust watermarking. In order to achieve the robustness of embedding method, we embed the scrambled watermark information into the low-band frequency of q-LFD by using the quantization index modulation (QIM) technique. According to the simulation results, our method can improve the quality of embedded image and also the robustness of watermark based on the optimized parameters: q of q-LFD and Q of QIM. Experimental results show that our proposed method is also robust against geometric attacks, processing attacks, filtering attacks, and so on.

Keywords *q*-logarithm frequency domain (q-LFD) $\cdot q$ -logarithm function $\cdot q$ -exponential function \cdot Quantization index modulation (QIM) technique \cdot Image watermarking

1 Introduction

1.1 Background

During the last twenty years, the e-business of digital content has become more popular through the Internet. There have been a number of multimedia contents purchased via

⊠ Ta Minh Thanh taminhjp@gmail.com

> Keisuke Tanaka keisuke@is.titech.ac.jp

¹ Tokyo Institute of Technology and JST CREST, W8-55, 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

network. Owing to the development of computer technique, everyone can easily copy, alter or even stole the digital contents such as picture, audio, and movie. In order to protect the copyright of the producer, a larger of copyright protection researches have been proposed. Among them, digital watermarking is a promising technique to achieve copyright protection which protects the digital content by embedding the secret information directly into the content itself. The secret information, also called watermark information, can be extracted later for authentication, copyright protection, and traitor detection, etc [27, 38]. The important requirements of digital watermarking are invisibility, robustness, and capacity of the embedded information. Namely, the watermark should not be perceived the changes of the digital content to maintain the content quality. It also must be robust against general image processing, such as cropping, noisy addition, JPEG compression, image filtering, and so on. Finally, the watermark should be easily extracted to prove ownership and to detect the traitor.

As presented in literature, the watermark information is normally embedded into several domains, e.g., the spatial domain, the transform domain, and the mixed domain. The watermarking methods using the spatial domain change directly the components of original content, for instance, RGB information, for embedding the watermark [10, 15, 17, 25]. Although watermarking techniques using spatial domain are easy to implement, it is too fragile to resist against common image processing, e.g., JPEG compression, filtering, and noise addition attacks. On the other hand, the watermarking techniques using the transform domain embed the watermark information by adjusting the magnitude of the coefficients of transform domain such as discrete cosine transform (DCT) [8, 26, 34, 35], discrete wavelet transform (DWT) [11, 14, 24, 30], and singular value decomposition (SVD) [16, 21, 28, 29, 40]. Also, there have been a lot of proposals of watermarking method that use the mixed domain. For instance, the combination of DCT and SVD [20, 23, 37], that of SVD and DWT [4, 36, 39], that of DWT and DCT [2, 6, 7] are employed to embed the watermark into the digital content. Most of proposed watermarking techniques focus on the embedding into the low-band of transform domain.

Robustness and imperceptibility are important properties that should be considered in digital watermarking. After choosing the transform domain for embedding, most of previous researches focused on how to achieve the robustness of watermark information. In general, the imperceptibility of watermarking technique depends on the intensity of the embedding strength of watermark. Better imperceptibility, which means the better quality of the digital content, can be achieved with weak embedding strength. However, the robustness of watermark may be low. For increasing the robustness of watermark, a stronger embedding strength is needed in the embedding process. However, it increases the degradation of the digital contents. Therefore, choosing of the optimum embedding strength to find the appropriate balance of the robustness and the imperceptibility properties is very important for the proposed watermarking methods.

1.2 Challenging issues

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

(1) Choosing the appropriate transform domain for embedding.

To ensure the robustness of watermark under common processing attacks, the transform domain should be employed for watermark embedding. Therefore, the first challenging issue is how to find out suitable transform domain for the embedding method.

(2) Choosing the blind embedding technique according to the transform domain.

The choice of the embedding technique is very important for the proposed method because it affects the robustness of the watermark. Normally, the blind embedding techniques are selected for real applications such as copyright protection, ownership proof, and traitor detection. Since our work focuses on these applications, the second challenging issue is how to choose the blind embedding technique that is suitable with the chosen frequency domain.

(3) Optimization of robustness and imperceptibility.

In order to keep the quality of embedded image and the robustness of watermark, the optimum embedding strength should be considered. Most of previous works only focus on optimizing the embedding strength in order to achieve the robustness of method. We think that improving the quality of the embedded content is also important for the proposed method. Therefore, the last challenging issue is how to choose the embedding strength for improving the quality of embedded image and also the robustness of watermark.

1.3 Our contributions

We concentrate to resolve the above challenging issues. Inspired by the advantages of the transform domain for embedding techniques, we continue to focus on transform domain, and extend it to q-logarithm frequency domain (q-LFD) for image watermarking in order to improve the quality of embedded image and also the robustness of watermark. In particular, we make the following contributions in this paper:

To solve the issue (1), we present the novel frequency domain, called *q*-logarithm frequency domain (*q*-LFD), consisting of *q*-DWT and *q*-SVD. By using the *q*-LFD, our method can arbitrarily control the quality of the embedded image while keeping the robustness of watermark by controlling the parameter q of q-LFD.

In order to fulfill the issue (2), we propose the QIM technique on q-LFD, not proposed before, in order to achieve high robustness and blindness. QIM technique is a method that embeds the watermark information into the original image with minimum distortion of the quality of embedded image. We employ the QIM technique proposed in the paper [5]. By the combination of QIM technique and q-LFD, our method can achieve better results. Based on our performances, the proposed method is useful for copyright protection, ownership proof, and traitor detection.

To optimize the parameters for better balance of robustness and imperceptibility, we employ two parameters q of q-LFD and Q of QIM to effectively control the amount of watermark. The embedding strength Q of QIM controls the robustness of watermark information. In order to enhance the quality of embedded image, we propose the way to optimize the parameter q of q-LFD. With the optimum parameters, we can solve the issue (3).

1.4 Roadmap

The rest of this paper is organized as follows. The related studies are discussed in Section 2. The proposal of q-LFD is presented in Section 3. Subsequently, Section 4 describes the proposed watermarking based on the q-LFD. Section 5 gives the experimental results and comparisons with other related methods. Finally, conclusions are made in Section 6.

2 Related studies

Recently, a number of robust watermarking algorithms for digital content have been developed. In this section, we review some representative methods using the traditional transform domain and analyze the weakness of those.

DWT domain has some advanced features that are suitable for the watermarking techniques. Those features are its excellent spatial localization and multi-resolution characteristics. In general, the original image is decomposed into several levels. An appropriate sub-band is chosen for watermark embedding as the method in [24]. Pradhan et al. used the sub-band HL3 for embedding the scrambled watermark based on Arnold transform and cross chaotic map. Though their method is robust against compression attack, cropping, scaling, and noise addition, but non-blind. It is not appropriate for real applications.

With another approach, Huang et al. [11] proposed an adaptive watermarking method based on non-linear wavelet transform (MHWT: Morphological Haar Wavelet Transform). In their technique, the watermark is embedded into the first and the second level of MHWT. Since MHWT employs an erosion (or dilation) for replacing the linear signal analysis filter of the classical linear Haar wavelet, the quality of the embedded image is clearly improved. However, as the method in [24], the method of Huang et al. requires the original image in the extraction process.

Keyvanpour et al. [14] proposed a watermarking scheme using a dynamic blocking of DWT domain. It is better than static blocking of DWT. They claimed that since their method adaptively selects the pixels from the strong edges regions, it is suitable for natural images. By using the QIM technique for embedding the watermark into HL and LH sub-band, they achieved good transparency. However, the robustness of their method was not evaluated enough.

SVD technique is always used to efficiently extract algebraic features from an image. The stable SVD matrices of image can be easily obtained. Therefore, when the embedded image is degraded under several image processing attacks, its singular values (SVs) do not change significantly. This feature is normally used to embed the user's information into the original image with less degradation of image quality. In [21], Liu et al. presented a watermark method which embeds the watermark into SVD domain. They added the watermark bits into the matrix *S*. Three matrices *U*, *S*, and *V* are saved as the secret key. These are required in the watermark extraction. In order to extend the method of [21], Lai [16] demonstrated a watermarking technique using SVD and tiny genetic algorithm to achieve the robustness of watermark information. Unfortunately, both algorithms of [21] and [16] are fundamentally flawed as mentioned in [22]. These algorithms cause the false positive detection even if the attacker uses the different embedded watermark.

With the another motivation, Tsai et al. [30] presented watermarking technique for image copyright protection based on DWT, SVD, and support vector regression (SVR). In their approach, the watermark information is embedded into the low-low level 2 (LL2) sub-band of the DWT domain of the original image by adjusting the coefficients of U component on SVD of the non-overlap block. Their method is blind by using a trained SVR to estimate original coefficients in the extraction process. After estimating, the watermark bits can be extracted correctly from the estimated coefficient. They also utilized the particle swarm optimization (PSO) to optimize the proposed scheme. However, their method is complicated and it suffers from the vulnerability of false positive detection of watermark.

According to the related works, the classical frequency domains are flexibly applied to watermarking researches. In order to increase the robustness of watermark, most of methods

are required to sacrifice the quality of the embedded image. In this work, we focus on how to improve the quality of the embedded image with keeping the robustness of watermark.

3 Proposal of *q*-logarithm frequency domain (*q*-LFD)

In this section, we explain the proposal of novel frequency domain, called q-LFD including q-DWT and q-SVD. The main idea is composition of the classical frequency domain such as DWT and SVD with the q-logarithm function and its inverse, the q-exponential function. By using q-LFD, we easily control the quality of the embedded image with keeping the robustness of watermark extraction.

3.1 *q*-logarithm and *q*-exponential functions

q-logarithm and its inverse, q-exponential, are the concept of non-extensive statistics which is introduced by Tsallis [31], a theory of non-extensive statistics. The q-logarithm function is defined as follows:

$$log_q(x) = \begin{cases} ln(x) & \text{if } q = 1, \\ \frac{x^{1-q}-1}{1-q} & \text{if } q \neq 1, \end{cases}$$
(1)

and its converse, q-exponential is defined as:

$$exp_q(x) = \begin{cases} exp(x) & \text{if } q = 1, \\ (1 + (1 - q)x)^{\frac{1}{1 - q}} & \text{if } q \neq 1, \end{cases}$$
(2)

where the parameter q is a real number that is predetermined and x is also a real number. We notice that the relationship of q-logarithm and q-exponential function can be explained as follows:

$$\lim_{q \to 1} \log_q(x) := \log(x), \lim_{q \to 1} exp_q(x) := exp(x).$$
(3)

Indeed, when q approaches 1, q-logarithm and q-exponential functions approach the exponential and natural logarithmic functions. They are also inverse to each other since $exp_q^{log_q(x)} = log_q(exp_q^x) = x \ (\forall x; \forall q) \ [1].$

In our work, x can be a pixel of image or a coefficient of the frequency domain. The parameter q can be chosen such that the resulting of q-logarithm functions close to the values of the classical frequency domains.

Inspired by the theory of non-extensive statistics, we propose q-LFD to provide a novel frequency domain, which is very flexible by choosing the parameter q to control the quality of image after inverse transform. We employ the feature of q-logarithm and q-exponential in (2) and (1) to construct q-LFD for image processing.

Suppose an image I is given. According to the q-logarithm and the q-exponential function, we propose the forward and the inverse transform of q-DWT and q-SVD.

3.2 Proposal of *q*-DWT domain

DWT is the most promising transformation technique that is useful for signal processing and image compression. Recently, DWT has been attracting researcher due to two excellent features: spatial localization and multi-resolution characteristics.

In case of the image, DWT divides the original image into four multi-resolution subbands low-low frequency (LL), low-high frequency (LH), high-low frequency (HL), and high-high frequency (HH). The coarse scale of the original image is represented in the subband LL. The fine scale of the original image is represented in the subband LL. The fine scale of the original image is represented in the subband LL. The fine scale of the original image is represented in the subband LL. In order to obtain the next *l*-level of DWT coefficients, the sub-band LL is then applied by DWT. Afterwards, the corresponding sub-bands such as *LLl*, *LHl*, *HLl*, and *HHl* of the *l*-level are generated.

Many proposed methods employ the DWT domain for watermark embedding. Generally, the sub-bands LLl consists of most of the information of the image, and other sub-bands include the detail information of the image such as edges, textures. Embedding watermark into the sub-bands LLl may affect significantly the quality of the embedded image, however, can achieve more robustness of the embedding method. Embedding watermark into the other sub-bands can achieve better quality of the embedded image, but the robustness of watermarking method may be sacrificed.

Since q-logarithm function has the feature that the parameter q can be chosen so that the quality of processed image to be close to that of original image, we combine q-logarithm function with DWT in order to minimize the distortion of quality after applying our proposed method.

We employ the Daubechies 9/7 wavelets since its wavelet coefficients are expected to be robust against various processing attacks, especially, lossy compression such as JPEG and JPEG2000 [18].

To implement our proposed q-DWT domain, DWT is performed on the original image I under the l-level of decomposition as follows:

$$I^{l}(u,v) = DWT(I(i,j),l),$$
(4)

where $I^{l}(u, v)$ denotes the coefficient at coordinate (i, j) in the DWT domain and $DWT(\cdot, \cdot)$ is the function of DWT.

The low-frequency LLl of DWT is employed and transformed into q-logarithm domain as below,

$$I_q^{LLl}(u,v) = \log_q \{ I^{LLl}(u,v) \} = \frac{\{ I^{LLl}(u,v) \}^{1-q} - 1}{1-q},$$
(5)

where $I^{LLl}(u, v)$ and $I_q^{LLl}(u, v)$ represent the coefficient at coordinate (u, v) of the low-frequency domain and q-logarithm domain, respectively.

In the inverse transform of q-DWT, the inverse transform of q-logarithm, q-exponential, is performed on the low-frequency *LLl* as follows:

$$I^{LLl}(u,v) = exp_q \left\{ I_q^{LLl}(u,v) \right\} = \left(1 + (1-q) \left\{ I_q^{LLl}(u,v) \right\} \right)^{\frac{1}{1-q}}.$$
 (6)

Finally, after composing *LLl* component with the high-frequency, the inverse image *I* can be obtained by using inverse transform of DWT:

$$I(i, j) = IDWT(Il(u, v), l),$$
(7)

where $IDWT(\cdot, \cdot)$ is the inverse function of DWT.

3.3 Proposal of *q*-SVD domain

In general, A is the matrix that is separated from image I and SVD is used to analyze matrices A. The real matrix A can be decomposed into three matrices $A = USV^T$, where U and V are the orthogonal matrices, $UU^T = E$, $VV^T = E$ and $S = diag(\lambda_1, \lambda_2, \cdots)$. E

is the unit matrix. Here, the singular values $\lambda_1, \lambda_2, \cdots$ of matrices *A* are sorted decreasingly. Note that, the columns of *U* are called the left singular vectors of *A* and the columns of *V* the right singular vectors of *A*. Therefore, the SVD can be formulated as:

$$SVD(A) = U_1\lambda_1V_1^T + U_2\lambda_2V_2^T + \dots + U_r\lambda_rV_r^T,$$
 (8)

where r is the rank of matrix A.

There are the following advantages when using SVD in digital image processing:

- (1) It is not necessary to fix the size of the matrix A beforehand. Its size is $x \times x$ or $x \times y$ for some x, y. Therefore, we can choose the size of A suitable for that of the watermark image.
- (2) SVs of a digital image are less affected under the general image processing such as blurring, noise addition, slight rotation. Therefore, the quality of the watermarked image can be kept after embedding.

To implement the q-SVD, I is transformed into q-logarithm as follows:

$$I_q(i,j) = \log_q\{I(i,j)\} = \frac{\{I(i,j)\}^{1-q} - 1}{1-q},$$
(9)

where I(i, j) and $I_q(i, j)$ represent the pixel (coefficient) at coordinate (i, j) of the spatial domain and the *q*-logarithm domain, respectively. The matrix A_q from I_q can be transformed to *q*-SVD using the original SVD. The *q*-SVD domain of *I* is defined as $SVD(A_q)$. We call the resulting *U*, *S*, and V^T as *q*-SVD domain.

After performing the SVD, we adjust the values of U, S, and V^T to control the quality of image. In order to reconstruct the image I', we apply SVD again to obtain I'_q based on the adjusted values of U, S, and V^T . Finally, we perform the q-exponential function:

$$I'(i,j) = exp_q(I'_q(i,j)) = (1 + (1-q)I'_q(i,j))^{\frac{1}{1-q}}.$$
(10)

Since the values of image pixels are slightly changed after applying the q-logarithm transform, the low-frequency of q-SVD domain is considered to be suitable for the image watermarking method. Therefore, the watermarking based on the q-SVD can be expected not only to improve the quality of the embedded image, but also to keep the robustness of the watermark information.

3.4 Advantage of the *q*-LFD

3.4.1 Quality controlling

In the previous watermarking researches, the watermark is directly added into the coefficients of the frequency domain. Therefore, it causes the distortion in quality of the embedded image. In our proposed frequency domain, q-LFD, the coefficients of the classical frequency domain is then quantized by q-logarithm transformation. The modified coefficients in the q-LFD after watermark embedding slightly affects to the value of coefficient of the classical frequency domain after applying the inverse transform of the qlogarithm transform. Based on this feature, the advantage of the q-LFD is that when the parameter q is changed, the logarithm transformed coefficients are slightly changed.



Fig. 1 The comparison of image quality of the classical frequency domain and the q-LFD

To show the property of controlling the value of frequency coefficients based on q-LFD, we employ the Lena image to implement the classical frequency domain and our q-LFD. In



Fig. 2 Permuted watermark by Torus permutation after p times, where a) p=20, b) p=60, and c) p=96

order to compare the value of frequency coefficients after transformation, we choose 100 frequency coefficients from the sub-band LL3 of the DWT domain and those of the *q*-DWT domain, respectively. We also choose 100 frequency coefficients at the position S(0, 0) from the 100 SVs of the SVD domain and *q*-SVD domain, respectively. The comparison of the values of chosen frequency coefficients is shown in Fig. 1.

As described in Fig. 1, if we change the value of parameter q, the value of frequency coefficients are also changed. Fortunately, the modification based on the parameter q of frequency coefficients affects slightly the quality of image.

3.4.2 Order of application

Our proposed q-LFD can be controlled by the order of application on q-logarithm and q-exponential function in order to minimize the distortion for image quality. We apply these functions only to the region that is employed for watermark embedding.

In particular, since we embed the watermark information into the sub-band LLl, we first apply DWT on the original image to obtain the sub-band LLl. Then, we apply q-logarithm function on the frequency coefficients of LLl. If we apply q-logarithm function on the original image, it also affects the frequency coefficients of sub-bands HLl, LHl, and HHl after applying the DWT.

In the case of the SVD decomposition, we embed the watermark information into entire of the original image. Therefore, we first apply the q-logarithm function to the original image, then the SVD decomposition is applied to all blocks that are divided from the processed image. q-logarithm function adjusts the pixels value of the original image for obtaining various versions of processed image based on the parameter q. These various versions will be the input images for SVD decomposition. Hence, such a feature make the SVD-based watermarking more attractive for real applications.

4 Proposed watermarking method using *q*-LFD

In this section, we present the proposed watermarking method based on the q-LFD using the QIM technique. The detailed processes consist of three processes: the watermark permutation, the embedding method, and the extraction method.

4.1 Watermark permutation

Before embedding, we prepare a watermark information W and obtain a binary sequence bits from W denoted by $w_i \in \{0, 1\}$, *i*-th bit of watermark. In order to achieve more security,



Fig. 3 The watermark embedding process based on q-LFD. The parameters are Q: watermark strength, q: parameter of q-logarithm function, p: the times of permutation transformation

W should be scrambled before embedding into the original image. We employ the Torus permutation function [33] to scramble *W* and obtain the scrambled W' as follows:

$$\binom{x'}{y'} = \binom{1 \quad 1}{k \quad k+1} \binom{x}{y} \mod L.$$
(11)

Here, each pixel at coordinates (x, y) of W is moved to (x', y') of W'. The p times of transformation are performed on the watermark. 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 period P and P depends only upon the parameters $k \in [1, L - 1]$ and L, where $L \times L$ is the size of W and $p \in [1, P]$. Figure 2 shows the periodic property of the Torus permutation where k = 1 and L = 64. It shows that the period P of W is 96.



Fig. 4 The watermark extraction process based on q-LFD

4.2 Watermark embedding based on q-LFD

After scrambling watermark, we implement the embedding algorithm described in Fig. 3. To embed the watermark, the original image I is firstly converted to the YCbCr domain. Y component is utilized to implement our embedding scheme.

In the case of DWT, since we focus on the low-frequency sub-bands LL3, we first apply DWT to the Y component with level l = 3. Afterwards, the coefficients of sub-bands LL3 are transformed to our proposed frequency domain, q-DWT, to obtain I_q .

In the case of SVD, we focus on all of matrices (blocks) that are separated from the Y component. Therefore, we first apply the q-logarithm transform on the Y component. Each matrix (block) is decomposed into the SVD domain, then q-SVD frequency domain is obtained.

We prepare the bit sequences $w'_i \in \{0, 1\}$ from the scrambled watermark W'. It is embedded into the low-frequency of q-DWT and the singular value of q-SVD by QIM method [5]:



Fig. 5 An example of the embedding and extraction of *q*-SVD domain. The parameters in this example are q=1.2, Q=0.4, $w'_{i}=$ "1"

$$\hat{I}_q(u,v) = \begin{cases} \lfloor I_q(u,v)/Q \rfloor \times Q + sgn(3Q/4) \text{ for } w'_i = 1, \\ \lfloor I_q(u,v)/Q \rfloor \times Q + sgn(Q/4) \text{ for } w'_i = 0, \end{cases}$$
(12)

where $I_q(u, v)$ and $\hat{I}_q(u, v)$ are the coefficients of I_q in low-frequency *LL*3 of *q*-DWT domain at coordinate (u, v) (the coefficients S(u, v) of the *S* matrices in *q*-SVD, where u = v) of the original image and the watermarked image, respectively. *sgn* function puts to "+" to the input if $I_q^{LL3}(u, v) > 0$, "-" if $I_q^{LL3}(u, v) < 0$. [] denotes the floor function, and *Q* denotes the embedding strength. Note that, *Q* is defined beforehand.

After embedding, the inverse transformation of q-DWT and q-SVD are performed to obtain the embedded image I'.

According to the above process, we embed the watermark W' into q-LFD of the original image I. That can control the quality of the embedded image based on two parameters: parameter q for q-LFD and parameter Q for watermark strength of QIM. Therefore, our proposed method is more flexible than conventional methods.

The parameters $\{q, Q, p\}$ are saved as the secret key for watermark extraction. We assign the license number (LN) for each combination $\{q, Q, p\}$ and save LN into the database. The embedded watermark can be retrieved only when the user knows the LN and shows it to the authenticator.

4.3 Watermark extraction based on q-LFD

The proposed extraction algorithm is similar to the embedding algorithm. The suspected image I' is first performed to q-LFD, and then the watermark information is extracted from the low-frequency of q-LFD. Since our proposed method is blind, the original image is not required here.

The describer of the watermarking extraction is shown in Fig. 4. First, the suspected image I' is converted to the YCbCr domain. As the embedding process, the Y component is utilized for applying the *q*-DWT and *q*-SVD domain as explained in Section 4.2.

The binary sequence $\{w'_i\}$ of watermark is extracted from the coefficients of I'_q in low-frequency *LL3* of *q*-DWT domain at coordinate (u, v) (the coefficients S(u, v) of the SVs in *q*-SVD, where u = v) based on the following rule:

$$w'_{i} = \begin{cases} 1 \text{ if } I'_{q}(u, v) - \lfloor I'_{q}(u, v)/Q \rfloor \times Q \ge sgn(Q/2), \\ 0 \text{ if } I'_{q}(u, v) - \lfloor I'_{q}(u, v)/Q \rfloor \times Q < sgn(Q/2). \end{cases}$$
(13)

After extracting the binary sequence $\{w'_i\}$, we reconstruct it to obtain the scrambled watermark W_p . Using the Torus permutation, we permute W_p with P - p times to obtain the extracted watermark W''.

Based on our proposed method, if an owner of the registered image I claims that another image I_s is an illegal copy, the corresponding LN is asked to provide for extracting the embedded watermark from I_s . Based on the extracted watermark W'', the authenticator can judge who is the owner of the image.

In order to to help the readers understand how to implement our proposed method, we use the 4 × 4 block with the grayscale values to demonstrate our method. The example is shown in Fig. 5. The parameters used in this example are q=1.2, Q=0.4, and $w'_i =$ "1". We extract 4 × 4 of RGB blocks and convert them to YCbCr components. Only Y component is converted to the q-logarithm frequency before SVD decomposition. In the q-SVD domain, we demonstrate to embed the watermark bit $w'_i =$ "1" into the coefficient S(1, 1) of the matrix S. In the watermark bit $w'_i =$ "1" is extracted from the coefficient S(1, 1) of the matrix S.

5 Experimental results and comparisons

In this section, we provide various experimental results in order to prove the efficiency of the proposed watermarking technique.

5.1 Test images and evaluation measure

We conduct the watermarking experiments on the well-known images of SIDBA (Standard Image DataBAse) database¹. All test images have size 512×512 pixels. In our experiments, 64×64 pixels of a binary logo Fig. 2(c) is first embedded in each of the images and subsequently we try to extract it from the watermarked and attacked image under various attacks. All experiments are performed by the Macbook Air OS 10.9 system.

In order to evaluate the quality of watermarked images, we employ PSNR (Peak Signal to Noise Ratio) criterion [12]. The PSNR of $N \times N$ pixels of the grayscale image I(i, j) and I'(i, j) is calculated with,

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

$$MSE = \sqrt{\frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \{I(i, j) - I'(i, j)\}^2},$$
(15)

¹http://www.vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/

Q	q	0.015	0.025	0.035	0.045	0.055	0.065
10	PSNR	46.73	47.70	49.03	49.52	49.88	50.15
	NC	1.00	1.00	0.995	0.982	0.980	0.963
20	PSNR	47.29	46.78	46.13	45.59	44.92	44.36
	NC	0.9976	1.00	1.00	1.00	1.00	1.00
30	PSNR	43.64	43.15	42.67	42.09	41.33	40.78
	NC	1.00	1.00	1.00	1.00	1.00	1.00
40	PSNR	41.24	40.72	40.16	39.41	38.89	38.39
	NC	1.00	1.00	1.00	1.00	1.00	1.00
50	PSNR	39.21	38.82	38.07	37.55	37.01	36.50
	NC	1.00	1.00	1.00	1.00	1.00	1.00
60	PSNR	37.74	37.13	36.78	35.94	35.36	34.84
	NC	1.00	1.00	1.00	1.00	1.00	1.00
70	PSNR	36.25	35.91	35.31	34.60	34.09	33.30
	NC	1.00	1.00	1.00	1.00	1.00	1.00

Table 1 PSNR[dB] and NC values based on the different q and Q (Lena image)

where MSE is mean square error. In case of color images with three RGB values per pixel, the PSNR is the same except the MSE, which is calculated based on the MSE of RGB values, called MSE_R , MSE_G , and MSE_B . Those can be calculated as follows:

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

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

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

$$MSE = \frac{MSE_{R} + MSE_{G} + MSE_{B}}{3},$$
(16)

where $I_R(i, j)$, $I_G(i, j)$, and $I_B(i, j)$ are the value of pixel of R-, G-, B-component at position (i, j).

To calculate the similarity of the extracted watermark, we use the normalized correlation (NC) value [12] between the original watermark W and the extracted watermark W''.



Fig. 6 Embedded image using q = 0.015, Q = 40: **a**) Baboon: PSNR=41.28dB, **b**) Peppers: PSNR=41.14dB, **c**) Lena: PSNR=41.15dB, **d**) Goldhill: PSNR=41.06dB

The NC value is calculated as follows:

$$NC = \frac{\sum_{i=0}^{L} \sum_{j=0}^{L} [W(i, j) \times W''(i, j)]}{\sum_{i=0}^{L} \sum_{j=0}^{L} [W(i, j)]^2},$$
(17)

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

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 very robust under the attack.

5.2 Experimental results of *q*-DWT

First, we investigate the efficiency of the parameters q and Q for the visual quality of watermarked image and the robustness of watermark information. We try with various values of

ŝ
11 1
à
65,
0.0
=
5)/(0
40
ä
15,
0.0
Ī
<i>b</i>) (<i>d</i>
QF
tor (
fac
lity
qua
vith
v nc
essio
npre
cor
EG
r JP
nde
es u
/alu
ý
A pr
3] ar
[dE
NR
P.
le 2
Tab

				h mu nomodu	(1) internet former	- A formore - A	A trans - Avio	(00-)		
Image	QF	No attack	06	80	70	60	50	40	30	20
Lena	PSNR	41.15/40.56	38.47/38.16	37.26/37.03	36.49/36.31	35.89/35.70	35.42/35.27	34.88/34.75	34.23/34.07	33.07/33.02
	NC	1.00/1.00	1.00/1.00	1.00/1.00	1.00/1.00	0.9909/0.9961	0.9709/0.9841	0.9351/0.9429	0.8621/0.8877	0.7129/0.7444
Peppers	PSNR	41.14/40.80	36.90/36.42	35.48/35.12	34.83/34.50	34.32/34.04	33.89/33.64	33.44/33.22	32.87/32.67	31.91/31.83
	NC	1.00/1.00	1.00/0.9995	1.00/0.9988	0.9998/0.9985	0.9858/0.9905	0.9644/0.9771	0.9324/0.9446	0.8662/0.8884	0.7197/0.7356
Baboon	PSNR	41.28/40.62	34.72/34.76	31.59/31.62	29.83/29.85	28.66/28.68	27.84/27.85	27.06/27.07	26.19/26.20	25.07/25.08
	NC	1.00/1.00	1.00/1.00	1.00/1.00	0.9985/1.00	0.9905/0.9949	0.9689/0.9797	0.9258/0.9492	0.8523/0.8792	0.7144/0.7427
Goldhill	PSNR	41.06/40.67	37.17/37.02	35.26/35.16	34.21/34.14	33.47/33.41	32.89/32.85	32.32/32.27	31.61/31.57	30.50/30.47
	NC	1.00/1.00	1.00/1.00	1.00/1.00	1.001.00	0.9846/0.9949	0.9705/0.9805	0.9382/0.9468	0.8494/0.8743	0.7163/0.7327

QF	100	90	80	70	60	50	40	30
Byun [3]	1	0.99	0.97	0.94	0.90	0.83	0.81	0.77
Hajizadeh [9]	1	1	1	1	1	0.99	0.99	0.91
Ours								
(0.015, 40)	1	1	1	1	0.99	0.97	0.94	0.86
Ours								
(0.065, 30)	1	1	1	1	0.99	0.98	0.94	0.89

Table 3 Comparison of proposed method (q, Q) with others: NC value (Lena image)

q and Q to find out appropriate values for those parameters. The "Titech logo" in Fig. 2 is used as the watermark information. The experimental results of the gray image, Lena, is given in Table 1. In Table 1, the first row shows the various values of parameter q and the first column shows the various values of parameter Q. According to the values of parameters Q and q, the values of PSNR and NC can be obtained. For example, when q = 0.015 and Q = 40, the values of PSNR and NC are 41.24dB and 1.0, respectively.

As shown in Table 1, we can control the visual quality of watermarked image and the robustness of watermark information based on the parameter q of q-DWT domain and the embedding strength parameter Q. When q is larger, PSNR value is smaller. It means that the visual quality of the embedded image becomes low. When Q is larger, NC value is close to 1. It means that the robustness of watermark is high. Therefore, in order to improve the quality of the embedded image and also to increase the robustness of watermark, we can choose small q and larger Q and vice versa for implementation.

In order to specify the the appropriate values for the parameters Q and q, we set the upper bound and the lower bound values of these parameters Q and q. In particular, we

Attacks	Lena	Peppers	Baboon	Goldhill
MF (3×3)	0.94/0.95	0.96/0.96	0.67/0.67	0.88/0.89
MF (5×5)	0.86/0.87	0.85/0.86	0.58/0.59	0.73/0.74
MF (7×7)	0.77/0.78	0.75/0.76	0.53/0.55	0.64/0.65
HE	0.56/0.42	0.52/0.51	0.49/0.50	0.47/0.48
AF (3×3)	0.66/0.66	0.62/0.63	0.52/0.52	0.56/0.57
AF (5×5)	0.55/0.54	0.52/0.53	0.51/0.49	0.52/0.53
AF (7×7)	0.51/0.52	0.51/0.52	0.49/0.49	0.51/0.51
GN(0.001)	1/1	1/0.99	1/1	1/1
GN(0.002)	1/1	1/0.99	1/1	1/1
GN(0.003)	1/1	1/0.99	1/1	1/1
$Scale(256 \times 256)$	0.99/0.99	0.96/0.96	0.96/0.97	0.98/0.99
Crop(1/4)	0.89/0.89	0.89/0.90	0.88/0.89	0.89/0.89
Rotation (-0.3°)	0.72/0.74	0.67/0.67	0.56/0.58	0.63/0.63
Rotation (-0.25°)	0.76/0.77	0.70/0.70	0.60/0.61	0.66/0.67
Rotation(0.25°)	0.74/0.76	0.71/0.71	0.61/0.63	0.68/0.69
Rotation(0.3 ^o)	0.72/0.73	0.69/0.69	0.59/0.60	0.65/0.66

Table 4 NC values (q = 0.015, Q = 40/q = 0.065, Q = 30)

cannot arbitrarily increase the value of Q and the value of q because the quality of the embedded image may become worse (PSNR < 37 dB). We cannot also decrease the value of Q and the value of q to obtain the better quality of the embedded images because this may decrease the robustness of the watermark (NC < 0.9). By considering the upper bound and lower bound values, the appropriate values for the parameters Q and q should be chosen so that the value PSNR of the embedded image is larger than 37dB, and the NC value of the extracted watermark is larger than 0.9.

Since each image has different feature, it is better to choose the appropriate value for the parameters Q and q according to its feature. However, the average values of Q and q can be calculated from various images beforehand in order to be used for all images.

To ensure the quality of the embedded image should be perceptually invisible to human eyes, we must choose the parameters q and Q in order to the PSNR value is larger than 37dB. In this section, we choose $\{q = 0.015, Q = 40\}$ and $\{q = 0.065, Q = 30\}$ to simulate the experimental images. The simulation results of the gray images, Baboon, Peppers, Lena, Goldhill are given in Table 2 and Fig. 6. Figure 6 shows the watermarked images with larger PNSR values. It reveals that good visual quality of watermarked images can be obtained by our proposed method. We also try to attack by JPEG compression with different quality factors (QF). After attacking, the PSNR values of those and the NC values of the extracted watermarks are calculated. Table 2 shows the experimental results. In the JPEG compression, the QF for images is ranged from 1 to 100, which denotes the predefined image quality of JPEG compression. When larger QF is assigned, lower compression ratio of the JPEG image is obtained and better visual quality of the JPEG image is remained. According to the results, we find that even under high compression ratios, high NC values can be obtained. It means that our proposed method is robust against the JPEG compression attack. The proposed method is able to detect watermark for QF greater than 20. Obviously, the image watermarking needs to be robust against, at least, JPEG compression to ensure for image transmission via network. Note that, the image is always compressed to JPEG image with QF equals to 75 before transmission. This is common to many situations. Based on the results of Table 2, our proposed method is useful under the JPEG compression and image transmission via network. Comparing the results of Table 2, we also find that when we use $\{q = 0.015, Q = 40\}$, the visual quality of watermarked images are improved and the robustness of watermark is also improved because the employed parameter Q of QIM is larger than case of $\{q = 0.065, Q = 30\}$. According to the experimental results, it is clear that the choice of parameters q and Q determines the tradeoff of robustness of the watermark and quality of the embedded image.

We compare our proposed method with the algorithms proposed by Byun et al. [3] and Hajizadeh et al. [9] based on Lena image shown in Table 3. According to results, the robustness of the watermark against JPEG compression in our proposed method is better than Byun et al. [3], and is similar to the robustness of Hajizadeh et al. [9].

In addition, in order to show the robustness of our method against other attacks, the watermarked images are exposed to many different attacks such as median filtering (MF), histogram equalization (HE), average filtering (AF), Gaussian noise (GN), scaling, cropping, and rotation.

In general, MF is used to reduce noise and preserve edges in image. By MF process, users expect to remove large amounts of noise while keeping the quality of image. HE is used to adjust the histogram of RGB color information, therefore, the histogram of output image seems uniform. AF is employed to smooth the image and to remove the noise and details of image at the same time. In our experiments, MF and AF are applied with



Overlay logo, NC=0.97

Rotate 40 and re-rotate, NC=0.89

Negate, NC=1

Fig. 7 Examples of the attacked Goldhill and its NC

filtering window size of 3×3 , 5×5 , and 7×7 . GN attacks with zero mean and several variances as 0.001, 0.002, and 0.003. In order to apply scaling attacks to the watermarked images, the scaling and rescaling process are applied. The size 512×512 of the watermarked images are scaled to the size 256×256 . After that, the size 256×256 of images are rescaled back to the size 512×512 . With the cropping attacks, we replace a part of the

Table 5 Comparison, where Ours(1):q = 0.015, Q = 40, Ours(2):q = 0.065, Q = 30

Attacks	Hajizadeh [9]	Lin [19]	Ours(1)	Ours(2)
$MF(3 \times 3)$	0.86	0.90	0.94	0.95
MF (5×5)	0.52	0.53	0.86	0.87
HE	0.89	0.79	0.56	0.42
AF (3×3)	0.88	0.95	0.66	0.66
AF (7×7)	0.44	0.47	0.51	0.52
Scale(256 × 256)	0.73	0.88	0.99	0.99
Crop(1/4)	0.58	0.66	0.89	0.89
Rotation(0.25°)	0.74	0.59	0.74	0.76
Rotation (-0.25°)	0.71	0.60	0.76	0.77
JPEG(QF=10)	0.49	0.34	0.51	0.52
JPEG(QF=20)	0.77	0.67	0.71	0.74
JPEG(QF=30)	0.91	0.82	0.86	0.89
JPEG(QF=50)	0.99	0.96	0.97	0.98
JPEG(QF=70)	1	0.97	1	1
JPEG(QF = 90)	1	0.99	1	1

Q	q	0.2	0.4	0.6	0.8	1.2	1.4	1.6	1.8	2.0
0.30	PSNR	38.4593	40.3052	41.9444	43.2561	45.5018	46.3084	47.0307	47.5226	48.1225
	NC	0.971029	0.964782	0.956682	0.941818	0.918022	0.89495	0.885542	0.862428	0.85067
0.35	PSNR	36.8905	38.7757	40.4758	41.9163	44.2819	45.3985	46.1682	46.8607	47.2839
	NC	0.977358	0.969377	0.963476	0.941196	0.938796	0.910206	0.883629	0.876834	0.860438
0.40	PSNR	35.4971	37.4385	39.1805	40.6326	43.2493	44.1945	45.214	46.0372	46.6467
	NC	0.980723	0.974017	0.968718	0.94935	0.945882	0.92807	0.896696	0.880235	0.85553
0.45	PSNR	34.1959	36.205	37.9389	39.5019	42.0997	43.2704	44.178	45.13	45.8973
	NC	0.984111	0.978365	0.969048	0.962175	0.943057	0.930975	0.903418	0.89034	0.871261
0.50	PSNR	33.0911	35.0678	36.8297	38.4515	41.1907	42.3449	43.3211	44.2749	45.1378
	NC	0.984111	0.982753	0.975685	0.965763	0.94511	0.939008	0.917181	0.891637	0.877551
0.55	PSNR	32.0909	34.0549	35.8289	37.4512	40.2472	41.4019	42.568	43.3395	44.4058
	NC	0.985472	0.985131	0.979374	0.970037	0.945847	0.943396	0.93117	0.900313	0.887457
0.60	PSNR	31.1681	33.1005	34.9007	36.5316	39.3755	40.5954	41.6975	42.716	43.5228
	NC	0.98855	0.985131	0.981737	0.973684	0.945569	0.940174	0.928848	0.911765	0.887944
0.65	PSNR	30.2909	32.2614	34.0562	35.711	38.5476	39.9008	41.0083	42.0944	42.8494
	NC	0.987179	0.985813	0.985131	0.97435	0.949017	0.945729	0.92867	0.913636	0.904137

Table 6 PSNR[dB], NC values using the different q and Q

watermarked image by the black image. We replace the up-left of the quarter part and the center of the embedded image by the black rectangle image and the black circle image with radius equal to 200. For implementing rotation attacks, the watermarked image is rotated with various slight angles ($-0.3^{\circ} \sim +0.3^{\circ}$). The detailed experimental results are shown in Table 4.

We also compare our method with the methods of Hajizadeh et al. [9] and Lin et al. [19] based on Lena image. The comparison is shown in Table 5. According to results in Table 5, except HE and AF, the performance of our algorithm is better than others.

In addition, using the embedded Goldhill image, we apply additional attacks such as center cropping, Barrel, overlay logo, rotate 40° and then re-rotate again, and negate attack. The extracted images and their NC values are given in Fig. 7. Based on those attacks, we confirm that the extracted watermark information has good visual quality except Barrel attack since Barrel is considered as one of the strong attacks.

5.3 Experimental results of *q*-SVD

In our method, by increasing the parameter Q of QIM, we can achieve the robustness of the watermarking method. However, the visible distortion of the embedded image is more conspicuous. Fortunately, by increasing the parameter q of the q-SVD, we can improve the quality of the embedded image with keeping the robustness of the watermark.

	, £)					
Image	Quality factor	No attack	90	80	70	60	50
Lena	PSNR	43.67/41.08	37.04/36.35	32.75/32.47	31.92/31.70	31.37/31.17	30.96/30.78
	NC	0.952/0.951	0.877/0.881	0.808/0.830	0.752/0.786	0.706/0.744	0.667/0.696
F16	PSNR	35.90/32.38	33.85/31.30	31.44/29.80	30.92/29.44	30.41/29.08	29.99/28.81
	NC	0.996/0.994	0.989/0.986	0.982/0.978	0.963/0.974	0.943/0.961	0.919/0.946
Baboon	PSNR	33.39/32.83	29.22/29.00	25.76/25.66	25.12/25.03	24.62/24.54	24.24/24.17
	NC	0.961/0.966	0.906/0.911	0.814/0.823	0.761/0.795	0.725/0.766	0.686/0.725
Scene	PSNR	39.25/35.73	31.82/30.86	28.52/28.00	28.09/27.55	27.77/27.34	27.44/27.17
	NC	0.981/0.980	0.889/0.887	0.811/0.830	0.662/0.762	0.595/0.673	0.576/0.600

Table 7 PSNR[dB], NC values under JPEG compression with different quality factor (q = 1.2, Q = 0.40)/(q = 1.4, Q = 0.60)



Fig. 8 The watermarked color images (q = 1.2, Q = 0.40). **a** Baboon, PSNR=33.39dB, **b** F16, PSNR=35.90dB, **c** Lena, PSNR=43.67dB, and **d** Scene, PSNR=39.25dB

In order to optimize the values of the parameters q and Q, we estimate the parameters q and Q for the visual quality of the embedded image and the robustness of the watermark information. We try with various values of q and Q to find out the appropriate values for those parameters. To compare the average PSNR and average NC values obtained from the embedded images based on $\{Q, q\}$, the watermark strength Q and the parameter q of the q-SVD are increased with uniform steps until we can achieve the minimum acceptable PSNR value that is more than 37 dB, and the minimum acceptable NC value, which is more than 0.9.

The experimental results of the color image, Lena, are given in Table 6. As shown in Table 6, we can also control the visual quality of the watermarked image and the robustness of the watermark information based on the parameter q of q-SVD domain and the embedding strength parameter Q. When q is larger, the PSNR value is lager. It means that the visual quality of the embedded image is better if q increases. When Q is larger, the NC value is close to 1. It means that the robustness of watermark is better if Q increases. Therefore, to achieve high quality of the embedded image and the robustness of watermark, we can choose the appropriate parameters q and Q for the watermarking method. Based on the resulting of the parameters Q and q, we can find out the appropriate region of values for the



(a) F16, JPEG compression with quality 60, PSNR=30.42, NC=0.9426



(d) F16, JPEG compression with quality 30, PSNR=29.05, NC=0.8420



(b) F16, JPEG compression with quality 50, PSNR=29.99, NC=0.9187



(c) F16, JPEG compression with quality 40, PSNR=29.52, NC=0.8869



(f) F16, JPEG compression with quality 10, PSNR=26.44, NC=0.5552

Fig. 9 Watermark extraction from embedded image F16 after JPEG compression with quality factors 60, 50, 40, 30, 20 and 10, respectively, when q = 1.2, Q = 0.40

PSNR=28.16, NC=0.7542

parameters Q and q. We set the upper bound and the lower bound values of these parameters Q and q. In our experiments, we cannot arbitrarily increase the value of Q and decrease the value of q because the quality of the embedded image may become worse (PSNR < 37 dB). We cannot decrease the value of Q and increase the value of q to obtain the better quality of the embedded images because this may decrease the robustness of the watermark (NC < 0.9). By considering the upper bound and lower bound values, the appropriate values for the parameters Q and q are in the gray region shown in Table 6.

Without loss of generality, we choose $\{q = 1.2, Q = 0.40\}$ and $\{q = 1.4, Q = 0.60\}$ to simulate on the experimental images. We embed the watermark into the original image and



Fig. 10 JPEG compression attack



Fig. 11 Geometric attack

try to extract the watermark from the suspected image under intentional and unintentional attacks.

In order to evaluate the robustness of our proposed method, we compare our results with those from the method of Jia [13]. In the case of Jia's method, to be fair, we implement his method employing the grayscale watermark instead of the color watermark.

Robustness against JPEG compression is the most basic requirement for the image watermarking. Therefore, we test our proposed method against several JPEG compression with various quality factors. The simulation results of the color images, Baboon, F16, Lena, and Scene, are given in Fig. 8 and Table 7. Table 7 shows the NC values of the extracted watermarks and the image quality of the watermarked images after attacking by JPEG compression with different quality factors (QF).

According to Table 7, even if under high compression ratios, high NC values can be obtained. It means that our proposed method is robust against the JPEG compression attack. Obviously, the image watermarking needs to be robust against, at least, JPEG compression to ensure for image transmission via network. Note that, image is always compressed to JPEG image with quality equals $75 \sim 80$ before transmission. Figure 9 illustrates the watermarks extraction from the embedded image F16 after the JPEG compression with low quality factors 60, 50, 40, 30, 20, and 10. It is clear that the extracted watermarks can be easily recognized by the human eyes. Additionally, Fig. 10 shows that our methods achieve the better performance compared to the method of Jia [13]. Therefore, according to the results of Table 7 and Fig. 10, our proposed method is useful under the JPEG compression and image transmission via network.

Comparing the results of Table 7, we use $\{q = 1.4, Q = 0.60\}$ instead of $\{q = 1.2, Q = 0.40\}$, the visual quality of watermarked images are almost remained, and the robustness



Fig. 12 Noise addition attack



Fig. 13 Filtering attack

of watermark is improved. Normally, when Q parameter is increased, the quality of the embedded image is degraded. However, by using larger q of the q-SVD domain, the quality of the embedded image is improved. Based on the experimental results, we confirm that the choosing of q and Q decides the tradeoff of robustness of watermark and the quality of the embedded image.

In order to test the robustness of our proposed method against another attacks, in our experiments, the embedded images are subject to the following attacks.

Firstly, the geometric attacks are considered as the first challenge because they destroy the synchronization (the locations of embedded positions) in the embedded image. In our experiments, the embedded images are scaled with different scaling factors (scaling attack) and are 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. In order to obtain the good extraction, the attacked image should be rescaled and re-rotated by an estimated scaling factor or a rotation angle in the opposite direction. To be fair, the estimation method in [32] is performed. Figure 11 shows that our methods are better than the method of Jia [13] in the rotation attacks, however, those performances in the scaling attacks seem to be lower than [13].



Fig. 14 Shearing attack

Attack type	Jia's method	Ours (q=1.4, Q=0.6)	Ours (q=1.2, Q=0.4)
Rotation 40°		 †	†
Scaling 1.5	NC=0.86	NC=0.92	NC=0.91
`Pepper and salt' noise 9%	NC=0.94	NC=0.88	NC=0.86
JPEG QF=50	NC=0.88	NC=0.86	NC=0.85
Median filter 7x7	NC=0.77	NC=0.89	NC=0.86
Shearing 90%	NC=0.69	NC=0.73	NC=0.71
Gaussian noise, variance=0.8	NC=0.95	NC=0.93	NC=0.94

Fig. 15 Comparison of the extracted watermarks in terms of visual perception and NC values for Lena image

Secondly, 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 2 % to 9 % are added into the embedded image. As shown in Fig. 12, our methods are not as robust against Gaussian noise and 'pepper and salt' noise as the method of Jia [13]. However, as we can see the watermark image in Fig. 9 with NC>0.8, the watermark image is still good quality. Hence, our methods are acceptable under the noise addition attacks since the NC values of the extracted watermark are more than 0.8.



Fig. 16 Some examples of simulation results against common image processing attacks on Lena image $(\{q = 1.2, Q = 0.40\})$

Thirdly, the filtering attack is also tested in our experiments. Two kinds of the filtering attacks, median filtering and Gaussian blur filtering, are adopted with the window sizes of 3×3 , 5×5 , 7×7 , 9×9 , 11×11 , 13×13 , and 15×15 . As shown in Fig. 13, we can assert that our proposed methods are better than the method in [13] under strong filtering attacks.

Fourthly, we present the shearing attack on the embedded images. In our experiment, the shearing percentages in x axes with the ranging from 10 % to 90 % are applied. For re-shearing the attacked images, to be fair, we also use the method in [32]. After that, the watermark images are extracted from the the re-sheared images. From the results shown in Fig. 14, it is clear that our methods can achieve the better performance compared to [13] when the shearing percentages becomes higher. It means that, after re-shearing, our method can retain the quality of the embedded image and help us to extract with high extraction results.

For showing the robustness of our proposed method, we pick up several extracted watermark images of the Lena image compared to Jia's method. By Fig. 15, the robustness of watermark in the proposed method is better than [13].

In order to show the robustness of our proposed method against common image processing attacks, we apply several attacks to the embedded Lena image such as tampered attacks by text "TA MINH", quarter of cropping, center cropping with radius of cycle equals to 100, 2/3 of cropping, grayscale, and swirl attack. Here, we extract the watermark image from those attacked images and calculate the NC values. The results are illustrated in Fig. 16. We also can easily recognize the watermark by the human eyes. Therefore, our proposed method seems to be robust against various attacks.

6 Conclusion

We have proposed a new frequency domain for watermarking method, called q-LFD. Based on it, a robust image watermarking using QIM technique and q-LFD have been proposed. The watermark is embedded into the low-frequency of q-LFD in order to achieve the robustness of watermark and to remain the quality of embedded image. According to our experimental results, the embedded watermark can successfully survive after attacked by image processing, especially for the JPEG compression. Moreover, because we employ the QIM method to watermarking method, the watermark embedding and extracting processes are very simple and the watermark can be extracted without the original image. Beside, the tradeoff of robustness and quality can be controlled by Q parameters of QIM and qparameters of logarithm transform. Therefore, we conclude that our new proposed method is suitable for images that will be highly JPEG-compressed and transmitted via network.

Acknowledgments We thank the anonymous reviewers for their helpful comments.

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. Abe S, Okamoto Y (2001) Nonextensive Statistical Mechanics and Its Applications, Series Lectures Notes in Physics. Springer
- Bei Y, Yang D, Liu M, Zhu L (2011) A multi-channel watermarking scheme based on HVS and DCT-DWT. In: Proceedings of CSAE '11, vol 4, pp 305–308
- 3. Byun K, Lee S, Kim H (2005) A watermarking method using quantization and statistical characteristics of wavelet transform. In: Proceedings of IEEE PDCAT, pp 689–693
- Cao W, Yan Y, Li S (2009) Robust image watermarking based on singular value decomposition in DT-CWT domain. In: Proceedings of IST '09, pp 381–384
- Chen B, Wornell GW (2001) Quantization index modulation methods for digital watermarking and information embedding of multimedia. J VLSI Signal Process Syst 27:7–33
- Deb K, Al-Seraj M, Hoque M, Sarkar M (2012) Combined DWT-DCT based digital image watermarking technique for copyright protection. In: Proceedings of ICECE '12, pp 458–461
- Feng LP, Zheng LB, Cao P (2010) A DWT-DCT based blind watermarking algorithm for copyright protection. In: Proceedings of ICCSIT, vol 7, pp 455–458
- 8. Fu Y (2013) Robust oblivious image watermarking scheme based on coefficient relation. J Optik 124(6):517–521

- Hajizadeh M, Helfroush MS, Dehghani MJ, Tashk A (2010) A Robust Blind Image Watermarking Method Using Local Maximum Amplitude Wavelet Coefficient Quantization. Advances in Electrical and Computer Engineering 10(3):96–101
- Huang PS, Chiang CS, Chang CP, Tu TM (2005) Robust spatial watermarking technique for colour images via direct saturation adjustment. In: Proceedings of Vision, Image and Signal Processing, vol 152, no 5, pp 561–574
- Huang X, Zhao S (2012) An Adaptive Digital Image Watermarking Algorithm Based on Morphological Haar Wavelet Transform. Phys Procedia 25:568–575
- Iwakiri M, Thanh TM (2012) Fundamental Incomplete Cryptography Method to Digital Rights Management Based on JPEG Lossy Compression. In: IEEE 26th International Conference on Advanced Information Networking and Applications, pp 755–762
- Jia S (2014) A novel blind color images watermarking based on SVD. Optik International Journal for Light and Electron Optics 125(12):2868–2874
- Keyvanpour M, Merrikh-Bayat F (2011) Robust dynamic block-based image watermarking in DWT domain. Procedia Computer Science 3:238–242
- Kimpan S, Lasakul A, Chitwong S (2004) Variable block size based adaptive watermarking in spatial domain. ISCIT 1:374–377
- Lai CC (2011) A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Process 4(21):522–527
- Lee YK, Chen LH (2000) High capacity image steganographic model. In: Proceedings of Vision, Image and Signal Processing, vol 147, pp 288–294
- Lee H-K, Song G-S, Kim M-A, Yoo K-S, Lee W-H (2004) A Digital Watermarking Scheme in JPEG-2000 Using the Properties of Wavelet Coefficient Sign. In: Proceedings of Computational Science and Its Applications (ICCSA), LNCS, pp 159–166
- Lin WH, Wang YR, Horng S, Kao T, Pan Y (2009) A blind watermarking method using maximum wavelet coefficient quantization. Expert Syst Appl 36(9):11509–11516
- Liu F, Liu Y (2008) A watermarking algorithm for digital image based on DCT and SVD. In: Proceedings of CISP '08, vol 1, pp 380–383
- Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 1(4):121–128
- Loukhaoukha K (2013) Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm". Digital Signal Process 23(4):1334
- Lu Z, Zheng H, Huang J (2007) A digital watermarking scheme based on DCT and SVD. In: Proceedings of IIHMSP '07, vol 1, pp 241–244
- Pradhan C, Rath S, Bisoi AK (2012) Non Blind Digital Watermarking Technique Using DWT and Cross Chaos. Proceedia Technology 6:897–904
- Ren-Junn H, Chuan-Ho K, Rong-Chi C (2002) Watermark in color image. In: Proceedings of the first International Symposium on Cyber Worlds, pp 225–229
- Ruimei Z, Hua L, Huawei P, Boning H (2008) A blind watermarking algorithm based on DCT. In: Proceedings of IITA '08, vol 3, pp 821–824
- 27. Shih FY (ed) (2008) Digital Watermarking and Steganography: Fundamentals and Techniques. Taylor & Francis Group, CRC Press., Inc., Boca Raton
- Stanescu D, Borca D, Groza V, Stratulat M (2008) A hybrid watermarking technique using singular value decomposition. In: Proceedings of IEEE HAVE '08, pp 166–170
- Sun X, Liu J, Sun J, Zhang Q, Ji W (2008) A robust image watermarking scheme based on the relationship of SVD. In: Proceedings of IIHMSP '08, pp 731–734
- Tsai M, Yu K, Chen Y (2000) Joint wavelet and spatial transformation for digital watermarking. IEEE Trans Consum Electron 1(46):241–245
- 31. Tsallis C (1998) Possible generalization of Boltzmann Gibbs statistics. J Stat Phys 52:479-487
- Thanh TM, Hiep PT, Tam TM, Tanaka K (2014) Robust semi-blind video watermarking based on framepatch matching. AEU - International Journal of Electronics and Communications, ISSN:1434–8411

- Voyatzis G, Pitas I (1996) Chaotic mixing of digital images and applications to watermarking. In: European Conference on Multimedia Applications, Services and Techniques (ECMAST '96), vol 2, pp 687–695
- 34. Won C (2010) Boosting robustness against composite attacks for quantization index-modulation algorithms. J Electron Imaging 19(2)
- 35. Xiao J, Wang Y (2008) Toward a better understanding of DCT coefficients in watermarking. Pacific-Asia workshop on computational intelligence and industrial application (PACIIA '08) 2:206–209
- Yavuz E, Telatar Z (2007) Improved SVD-DWT based digital image watermarking against watermark ambiguity. In: Proceedings of SAC '07, pp 1051–1055
- Yavuz E, Telatar Z (2006) SVD adapted DCT domain DC subband image watermarking against watermark ambiguity. In: Proceedings of IW-MRCS2006, LNCS, vol 4105, pp 66–73
- 38. Yeung MM (1998) Digital watermarking. Commun ACM 41(7)
- Zhang L, Li A (2009) Robust watermarking scheme based on singular value of decomposition in DWT domain. In: Proceedings of APCIP '09, vol 2, pp 19–22
- Zhu X, Zhao J, Xu H (2006) Digital watermarking algorithm and implementation based on improved SVD. In: Proceedings of ICPR '06, vol 3, pp 651–656



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.