Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A robust watermarking algorithm based on QR factorization and DCT using quantization index modulation technique*

Hong-yuan CHEN, Yue-sheng ZHU†‡

(*Communication and Information Security Lab, Shenzhen Graduate School, Peking University, Shenzhen 518055, China*)

†E-mail: zhuys@pkusz.edu.cn

Received Nov. 16, 2011; Revision accepted Apr. 9, 2012; Crosschecked July 6, 2012

Abstract: We propose a robust digital watermarking algorithm for copyright protection. A stable feature is obtained by utilizing QR factorization and discrete cosine transform (DCT) techniques, and a meaningful watermark image is embedded into an image by modifying the stable feature with a quantization index modulation (QIM) method. The combination of QR factorization, DCT, and QIM techniques guarantees the robustness of the algorithm. Furthermore, an embedding location selection method is exploited to select blocks with small modifications as the embedding locations. This can minimize the embedding distortion and greatly improve the imperceptibility of our scheme. Several standard images were tested and the experimental results were compared with those of other published schemes. The results demonstrate that our proposed scheme can achieve not only better imperceptibility, but also stronger robustness against common signal processing operations and lossy compressions, such as filtering, noise addition, scaling, sharpening, rotation, cropping, and JPEG/JPEG2000 compression.

Key words: Digital watermarking, QR factorization, Quantization index modulation (QIM), Discrete cosine transform (DCT)
doi:10.1631/jzus.C1100338 **Document code:** A **CLC number:** TP309.2

1 Introduction

Digital techniques have greatly facilitated data representation and data storage. However, digital media are easy to edit and copy without distortion, and this has resulted in a series of security problems over the widespread network. For example, people can easily access, edit, or distribute any digital media from a network. Therefore, how to guarantee copyright protection and the integrity of the content of digital media has become an emergent issue. Digital watermarking has been developing rapidly as a solution to this problem.

Digital watermarking (Chandramouli *et al*., 2002) is the process of embedding information in digital media content such that the information which we call the watermark can later be extracted or detected for a variety of purposes including copyright protection and integrity authentication. Digital watermarking techniques can be classified into two types, namely robust watermarking and fragile watermarking. Robust watermarking is resilient to intentional or un-intentional attacks, and is used mainly for copyright protection. Fragile watermarking is designed to indicate any modification made to the digital media, and is used mainly for integrity authentication. In this paper, we will focus on robust watermarking techniques.

Existing robust watermarking algorithms can be further classified into two categories, spatial domain methods and transform domain methods. In a spatial domain watermarking system (Zeki *et al*., 2011), the watermark is embedded by directly modifying the pixel values. This is easy to implement; however, many of such schemes are not robust enough against attacks. In a transform domain watermarking system, the host image is presented in a transformed domain where the embedding is performed. The commonly

‡ Corresponding author

* Project supported by the "Shuang Bai Plan" and "Shenzhen–Hong Kong Innovation Circle" Research Program of Shenzhen, China

used transform methods include discrete cosine transform (DCT) (Barni *et al*., 1998; Gupta and Shrivastava, 2010; Won, 2010; Phadikar *et al*., 2011; Sakib *et al.*, 2011), discrete wavelet transform (DWT) (Liu *et al.*, 2003; Shen *et al*., 2009; Su *et al*., 2009; Hu *et al.*, 2011), discrete Fourier transform (DFT) (Wang *et al*., 2009), independent component analysis (ICA) (Murillo-Fuentes, 2007), singular value decomposition (SVD) (Mohammad *et al*., 2008; Liu *et al*., 2009; Lai, 2011a; 2011b; Rastegar *et al.*, 2011), and QR factorization (or QR decomposition) (Naderahmadian and Hosseini-Khayat, 2010; Song *et al*., 2011). In the transform domain, more stable characteristics and the human visual system (HVS) can be exploited. Therefore, better robustness and imperceptibility are expected to be achieved. Several typical watermarking algorithms in the transform domain are reviewed briefly below.

Won (2010) proposed a DCT-based watermarking algorithm. The watermark is embedded by modifying the DC coefficient of a block using the quantization index modulation (QIM) technique (Chen and Wornell, 2001). This algorithm can achieve strong robustness against severe composite attacks and JPEG compression.

Liu *et al.* (2003) proposed a robust watermarking algorithm combining DWT and DCT, and by using the ICA technique, the performance of watermark detection is greatly improved.

Hu *et al*. (2011) proposed a robust digital watermarking scheme based on DWT and DFT, in which the watermark is embedded adaptively in the low band of the DWT domain according to the HVS. To enhance robustness, a template is embedded in the DFT domain and good performances can be achieved.

Murillo-Fuentes (2007) proposed a new blind robust watermarking scheme based on ICA, in which the watermark is embedded into some statistically independent transform coefficients obtained by applying ICA to the host image. By utilizing the property that some of the transformed coefficients have noise-like spectra, a spread spectrum watermark is used to enhance the robustness of the scheme and the watermark can be detected blindly with a simple matched filter.

Rastegar *et al*. (2011) proposed a hybrid robust digital watermarking algorithm based on finite Radon transform (FRAT), SVD, and DWT techniques. To achieve a tradeoff between robustness and imperceptibility, watermark embedding is done by using middle frequencies of HL3 and LH3. This method can survive filtering, noise addition, and gamma correction attacks.

Song *et al.* (2011) proposed a watermarking scheme based on QR factorization. The first column coefficients in the obtained $\boldsymbol{Q}$ matrix of blocks are modified to embed the watermark. To enhance the security of the scheme, a pseudorandom circular chain generated by logistic mapping is applied to select the embedding blocks. This scheme can survive such attacks as cropping and noise pollution.

Naderahmadian and Hosseini-Khayat (2010) embedded a watermark image by directly modifying the first row elements in the obtained $\boldsymbol{R}$ matrix after performing QR factorization in the DWT domain. Experimental results demonstrated that their scheme can achieve low computational complexity and good robustness against some image processing operations.

Inspired by the latter two schemes, a novel robust digital watermarking algorithm based on QR factorization for copyright protection is proposed in this paper. We combine QR factorization and DCT techniques to derive the DC coefficients, which are used as the stable features and modified for embedding the watermark by using the QIM technique. Meanwhile, an embedding location selection method similar to that adopted by Huang *et al*. (2010) is exploited to select blocks with small modifications to embed the watermark. Our experimental results show two remarkable features of the proposed scheme. One is its strong ability to survive common signal processing operations and lossy compressions. The other is effective minimization of the embedding distortion introduced by watermarking and significant improvement on the imperceptibility of the algorithm.

2 Related techniques

2.1 QR factorization

In linear algebra, given an $M\times N$ matrix $\boldsymbol{A}$, its QR factorization (also called QR decomposition) can be formulated as

$$\boldsymbol{A}_{M\times N}=\boldsymbol{Q}_{M\times M}\boldsymbol{R}_{M\times N}, \tag{1}$$

where $\boldsymbol{R}$ is an upper triangular matrix and $\boldsymbol{Q}$ is an orthogonal matrix, i.e., $\boldsymbol{Q}^{\mathrm{T}}\boldsymbol{Q}=\boldsymbol{I}$. The M columns of $\boldsymbol{Q}$

form an orthonormal basis for the column space of $\boldsymbol{A}$. This confers an interesting property that when a small perturbation is added to the matrix, large variation in the elements in the first column does not occur. Therefore, the matrix can be used for designing robust watermarking schemes, such as in the algorithm proposed by Song *et al*. (2011). The first row elements in matrix $\boldsymbol{R}$ have much larger absolute values than others and dominate most of the energy of $\boldsymbol{A}$; meanwhile, these elements are resistant to several signal processing operations, such as lossy compressions, noise addition, and filtering. Based on this property, several robust watermarking schemes utilizing $\boldsymbol{R}$ have been proposed, such as that proposed by Naderahmadian and Hosseini-Khayat (2010).

2.2 1D-DCT model

Discrete cosine transform (DCT) is a decomposition that converts signals from the time domain to the frequency domain. For a vector $\boldsymbol{X}=(x_0, x_1, \ldots, x_{N-1})$, its discrete cosine transform, denoted by $\boldsymbol{Y}=(y_0, y_1, \ldots, y_{N-1})$, can be calculated as

$$y_u = C(u)\sqrt{\frac{2}{N}}\sum_{n=0}^{N-1} x_n \cos\left(\frac{2n+1}{2N}u\pi\right),\ u=0,1,...,N-1, \tag{2}$$

where

$$C(u)=\begin{cases}1/\sqrt{2}, & u=0,\\ 1, & u=1,2,...,N-1.\end{cases} \tag{3}$$

The corresponding inverse discrete cosine transform (IDCT) can be calculated as

$$x_n = \sqrt{\frac{1}{N}}y_0 + \sqrt{\frac{2}{N}}\sum_{u=1}^{N-1} y_u \cos\left(\frac{2n+1}{2N}u\pi\right),\ n=0,1,...,N-1. \tag{4}$$

2.3 Quantization index modulation

Chen and Wornell (2001) introduced a class of embedding methods, termed the quantization index modulation (QIM) technique, which can achieve efficient tradeoffs among information-embedding capacity, caused embedding distortion, and robustness of embedding. Some schemes based on this technique have been proposed (Seo *et al*., 2007; Huang *et al*., 2010; Phadikar *et al*., 2011). As presented by Seo *et al*. (2007), the technique embeds signal-dependent watermarks based on the quantization technique. A particular quantizer is chosen from a set of possible quantizers by using the watermark information as an index, and then applied to the host data to embed the watermark information.

Assume one bit $m\in\{0, 1\}$ is to be embedded and s denotes the host signal. Two quantizers $Q_i(s)$, i=0, 1 will be generated and the watermark bit determines the selection of the quantizer $Q_i(s)$ with a step size Δ, which can be formulated as follows:

$$Q_i(s)=Q(s-d_i)+d_i,\ i=0, 1, \tag{5}$$

where $Q(s)=\Delta\times\text{round}(s/\Delta)$, $d_0=-\Delta/4$, $d_1=\Delta/4$, and round(x) rounds x to the nearest integer.

The watermarked signal s' can be calculated based on the two quantizers Q_0 and Q_1 using Eq. (6). Fig. 1 illustrates the watermark embedding process.

$$s'=\begin{cases}Q_0(s), & m=0,\\ Q_1(s), & m=1.\end{cases} \tag{6}$$

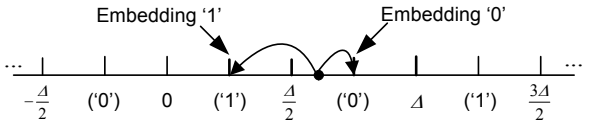


Fig. 1 Quantization index modulation embedding process

In the watermark extraction process, the decoded bit m' can be extracted from the received signal s'' by solving the optimization problem:

$$m'=\arg\min_{m\in\{0,1\}} \| s''-Q_m(s'') \|. \tag{7}$$

From the QIM embedding process we can see that, the larger is Δ, the more serious will be the caused embedding distortion, and on the contrary, the stronger will be the robustness of the embedding method. Therefore, an efficient tradeoff between the caused embedding distortion and robustness can be achieved by adjusting Δ.

3 The proposed algorithm

The proposed watermarking algorithm comprises two processes, watermark embedding and watermark extraction. Sections 3.1 and 3.2 are dedicated

to detailed descriptions of the two processes respectively, and in Section 3.3, an estimation method of the threshold T adopted in the embedding location selection method will be briefly described.

3.1 Watermark embedding

The watermark embedding framework is illustrated in Fig. 2. First, the host image is divided into non-overlapping blocks. Before embedding the watermark, we first apply QR factorization to each block, obtain the matrix $\boldsymbol{R}$, and perform DCT on the first row elements of $\boldsymbol{R}$. Then a 1-bit watermark is embedded in the block by modifying the value of the obtained DC coefficient using the QIM technique. There were two reasons which prompted us to select the DC coefficient of the first row elements in $\boldsymbol{R}$ to embed the watermark. First, the absolute values of the first row elements of $\boldsymbol{R}$ are much larger than others, and most of the energy of the block is evenly distributed on these elements. Therefore, they are expected to be robust against noise addition attacks and lossy compressions. Second, the DC coefficient of the first row elements is obtained by averaging the elements, which can further enhance the robustness against such attacks. Furthermore, to reduce the caused embedding distortion and improve the imperceptibility of this algorithm, an embedding location selection method similar to that adopted by Huang *et al*. (2010) is utilized to give priority to the blocks with small modifications to embed the watermark. Before the watermark is embedded, it is scrambled using Arnold transform with a private key K_p to enhance the security of the watermark.

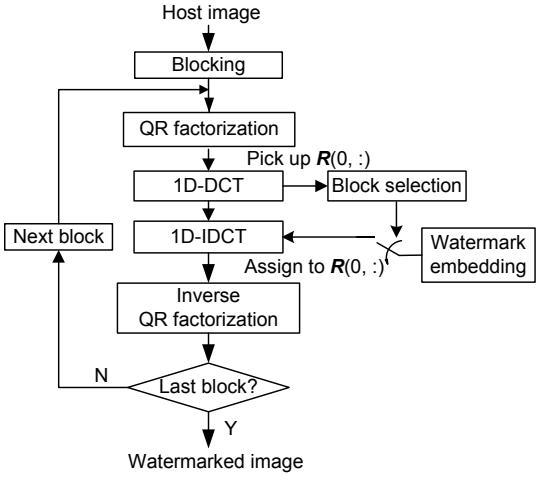


Fig. 2 Watermark embedding framework

The detailed embedding steps are as follows:

Step 1: Divide the host image into non-overlapping blocks of size $M\times N$.

Step 2: Select one block denoted by $\boldsymbol{B}$ sequentially and perform QR factorization on it as follows:

$$\boldsymbol{B}=\boldsymbol{QR}. \tag{8}$$

Step 3: Pick up the first row elements of $\boldsymbol{R}$, which form a vector denoted by $\boldsymbol{V}_{\boldsymbol{R}1}=\boldsymbol{R}(0, :)$.

Step 4: Perform 1D-DCT on $\boldsymbol{V}_{\boldsymbol{R}1}$ and obtain the transformed vector denoted by $\boldsymbol{V}_{\boldsymbol{R}1\text{-DCT}}$.

Step 5: Determine whether the block can be embedded with a 1-bit watermark, according to the DC coefficient of $\boldsymbol{V}_{\boldsymbol{R}1\text{-DCT}}$ (denoted by DC) and the watermark bit w to be embedded. If a 1-bit watermark can be embedded into this block, the embedded DC coefficient denoted by DC′ will be computed using the QIM method as follows:

$$\mathrm{DC}'=\begin{cases}\Delta\cdot\mathrm{round}((\mathrm{DC}+\Delta/4)/\Delta)-\Delta/4, & w=0,\\ \Delta\cdot\mathrm{round}((\mathrm{DC}-\Delta/4)/\Delta)+\Delta/4, & w=1,\end{cases} \tag{9}$$

where Δ is the adopted step size.

Calculate the absolute difference d between DC and DC′, i.e., d=abs(DC−DC′). The larger is d, the more serious will be the caused embedding distortion. Therefore, once the step size Δ is determined, we can calculate a threshold T for the image. The estimation procedure of T will be described in Section 3.3. If the calculated d is not larger than T, the block will be selected to embed the watermark by Eq. (9) and the modified $\boldsymbol{V}_{\boldsymbol{R}1\text{-DCT}}$ is denoted by $\boldsymbol{V}'_{\boldsymbol{R}1\text{-DCT}}$. Otherwise, no watermark is embedded and $\boldsymbol{V}'_{\boldsymbol{R}1\text{-DCT}}$ is equal to $\boldsymbol{V}_{\boldsymbol{R}1\text{-DCT}}$.

Step 6: Perform 1D-IDCT on $\boldsymbol{V}'_{\boldsymbol{R}1\text{-DCT}}$, and assign the transformed vector to the first row elements of $\boldsymbol{R}$. We denote the modified matrix $\boldsymbol{R}$ by $\boldsymbol{R}'$.

Step 7: Perform inverse QR factorization to reconstruct the block denoted by $\boldsymbol{B}'$, which can be formulated as

$$\boldsymbol{B}'=\mathrm{round}(\boldsymbol{QR}'). \tag{10}$$

Step 8: Repeat Steps 2–7 until all the blocks have been examined, and the watermarked image can be obtained.

If the size of the host image is $W\times H$, a binary embedding location matrix (denoted by $\boldsymbol{M}_{\mathrm{EL}}$) with a

size $(W/M)\times(H/N)$ can be formed in the embedding process. The embedding location matrix $\boldsymbol{M}_{\mathrm{EL}}$, the block size $M\times N$, and the step size Δ along with the key K_{p} used to perform Arnold transform will be used as the private keys. Only with the knowledge of the private keys, can the embedded watermark be extracted, which can enhance the robustness and security of this algorithm.

3.2 Watermark extraction

The watermark extraction process is the reverse procedure of watermark embedding (Fig. 3). With the knowledge of the private keys, the watermark extraction process can be performed as follows:

Step 1: Divide the watermarked image into non-overlapping blocks of size $M\times N$.

Step 2: Select one block sequentially, and determine whether a 1-bit watermark is embedded in it, according to the embedding location matrix $\boldsymbol{M}_{\mathrm{EL}}$. If yes, go to Step 3; otherwise, select the next block and repeat Step 2.

Step 3: Perform QR factorization on the block and pick up the first row elements of $\boldsymbol{R}$, which form a vector denoted by $\boldsymbol{V}_{\boldsymbol{R}1}$.

Step 4: Perform 1D-DCT on $\boldsymbol{V}_{\boldsymbol{R}1}$ and obtain the DC coefficient denoted by DC.

Step 5: Extract a 1-bit watermark w' from the block by Eqs. (11)–(13).

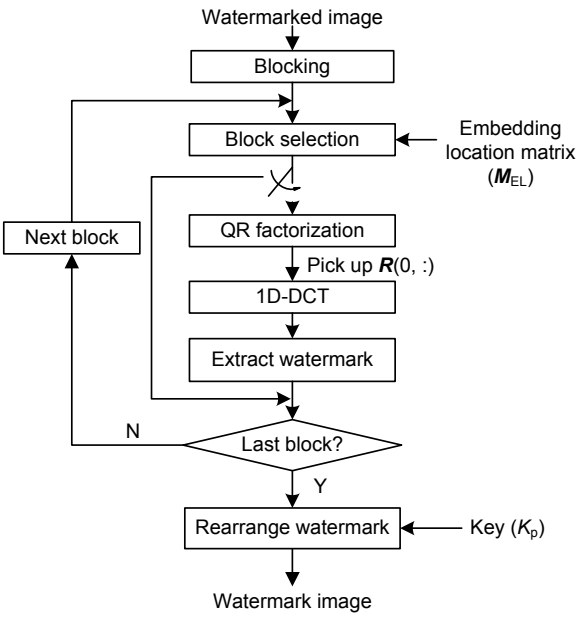


Fig. 3 Watermark extraction framework

$$w' = \arg\min_{m\in\{0,1\}} \|\mathrm{DC} - Q_m(\mathrm{DC})\|, \tag{11}$$

where

$$Q_0(\mathrm{DC})=\Delta\cdot\mathrm{round}((\mathrm{DC}+\Delta/4)/\Delta)-\Delta/4, \tag{12}$$

$$Q_1(\mathrm{DC})=\Delta\cdot\mathrm{round}((\mathrm{DC}-\Delta/4)/\Delta)+\Delta/4. \tag{13}$$

Step 6: Repeat Steps 2–5 until all the watermark bits have been extracted.

Step 7: Recover the watermark image from the extracted watermark bits by performing inverse Arnold transform with the key K_{p}.

3.3 Estimation of threshold T

As mentioned in Section 3.1, once the step size Δ for QIM is determined, we can calculate a threshold T for the host image according to the watermark information and the characteristics of the host image. The steps to determine the value of T are briefly described as follows:

Step 1: Randomly assign one value to T.

Step 2: Embed the watermark information using the proposed method with the selected parameter T.

Step 3: If the watermark information can be completely embedded in the host image, reduce the value of T. Otherwise, increase the value.

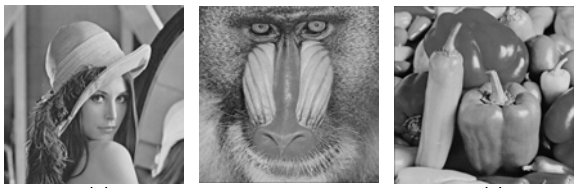
Step 4: Repeat Steps 2 and 3 until T satisfies the condition that the total bits of the watermark can be only just completely embedded in the host image. In other words, once the value of T is reduced, the watermark information can no longer be completely embedded in the host image.

With the selected threshold T, the blocks with small modifications will be selected as the embedding locations. This can minimize the embedding distortion, and the imperceptibility of the algorithm can be greatly improved. Note that, even if the adopted step size Δ and the watermark are the same for two different images, the calculated threshold T may be different due to the different characteristics of the two images. Therefore, for different images, an adaptive threshold T should be separately estimated.

4 Experimental results

To test and evaluate the performance of our algorithm, 10 standard gray-scale images (512×512) were used. Three samples of them are illustrated in

Fig. 4. The watermark was a binary image of size 32×32 (Fig. 5), and therefore the total amount of bits in the watermark image was 32×32 (1024). In this study, the selected step size Δ for QIM was 320, and the host image was divided into blocks of size 4×4. Thus, 128×128 (16384) blocks were generated and up to 16384 bits could be embedded in the host image. Therefore, only 6.25% of the generated blocks were used to embed the watermark and these blocks could be selected using the embedding location selection method with a specific threshold T for each test image.



(a) (b) (c)

Fig. 4 Test images: (a) Lena; (b) Baboon; (c) Pepper

Fig. 5 Watermark image (32×32)

For a digital watermarking system, two aspects, imperceptibility and robustness, are often used as the performance metrics. For imperceptibility, we used the peak signal-to-noise ratio (PSNR) defined by Eqs. (14) and (15) as the measure criterion:

$$\mathrm{PSNR}=10\lg\frac{255^2}{\mathrm{MSE}}, \tag{14}$$

$$\mathrm{MSE}=\frac{1}{W_I\times H_I}\sum_{i=0}^{W_I-1}\sum_{j=0}^{H_I-1}(I_{i,j}-I'_{i,j})^2, \tag{15}$$

where $I_{i,j}$ and $I'_{i,j}$ denote the value of the pixel with coordinate (i, j) in the host image I and watermarked image I', respectively, and $W_I\times H_I$ is the size of I. The larger is PSNR, the better will be the imperceptibility.

For robustness, we used the bit error ratio (BER) and the normalized correlation (NC) to evaluate the performance of our scheme. The BER essentially measures the ratio of error bits to the total watermark bits and can be defined by Eq. (16), while the NC measures the correlation between the extracted and the original watermark which can be calculated by Eq. (17).

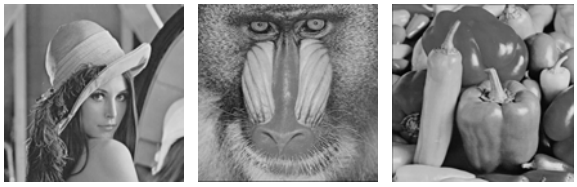
$$\mathrm{BER}(W,W')=\frac{1}{X\times Y}\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}W(i,j)\otimes W'(i,j), \tag{16}$$

$$\mathrm{NC}(W,W')=\frac{\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}W(i,j)W'(i,j)}{\sqrt{\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}W^2(i,j)}\sqrt{\sum_{i=0}^{X-1}\sum_{j=0}^{Y-1}W'^2(i,j)}}, \tag{17}$$

where W and W' denote the original and the extracted watermark images, respectively, $X\times Y$ is the size of the watermark image, and $\otimes$ is the exclusive-or (XOR) operator.

4.1 Performance comparison based on imperceptibility

The corresponding watermarked images for test images illustrated in Fig. 4 are shown in Fig. 6. From Figs. 4 and 6 we can see that no visible artifacts can be observed in the watermarked images, and that good imperceptibility can be achieved by our scheme.



(a) (b) (c)

Fig. 6 Watermarked images

(a) Lena with 54.4173 dB; (b) Baboon with 55.5757 dB; (c) Pepper with 54.9082 dB

Besides subjective observation, we compared our results with three previous schemes (Liu *et al*., 2009; Naderahmadian and Hosseini-Khayat, 2010; Song *et al*., 2011). The selected parameters for the four schemes and the corresponding average PSNR of the watermarked images obtained by averaging the results for the 10 test images are listed in Table 1. An average PSNR of 53.7661 dB can be achieved by our scheme. This value is much larger than those obtained by the other schemes, which further demonstrates the better imperceptibility of our scheme.

Table 1 Comparison of results on imperceptibility

Reference	Parameter	Average PSNR (dB)
Liu *et al.* (2009)	Q=30	46.9983
Naderahmadian and Hosseini-Khayat (2010)	S=32	46.9088
Song *et al*. (2011)	T=0.042	41.9602
This paper	Δ=320	53.7661

4.2 Performance comparison based on robustness

To evaluate the robustness of our algorithm, we compared our results with those from the previous three schemes listed in Table 1. In the experiment, the watermarked images were subject to the following attacks, which were implemented using MATLAB R2011a and VS2005. The 10 watermarked test images were used to test the robustness of our scheme.

1. Filtering attack: three kinds of filtering attacks, namely Wiener filtering, median filtering, and average filtering, were used and the adopted window size was 3×3.

2. Scaling attack: each watermarked image was scaled with different scaling factors using a bilinear interpolation method, and the values of the scaling factor in our experiment were taken as 0.1, 0.5, and 0.9. Since the original size of the watermarked image can be derived from the sizes of the embedding location matrix and each divided block, in the experiment the attacked image was resized to the original size using a bilinear interpolation method before the watermark was extracted.

3. Noise addition attack: two types of noise, namely Gaussian white noise and 'pepper & salt' noise, were added to each watermarked image separately until the corresponding attacked image had a PSNR of 20 dB.

4. Sharpening attack: a 3×3 unsharp contrast enhancement filter created from the Laplacian filter with parameter α was used to sharpen the watermarked images. The values of α were taken as 0.1 and 0.9.

5. Rotation attack: each watermarked image was rotated through a given angle and resized to the original size using a bilinear interpolation method. Before extracting the watermark, the following preprocessing actions were performed to the attacked image: re-rotating it by an estimated rotation angle in the opposite direction, cutting the margin region, and resizing it using the above-mentioned interpolation method. Since the estimation method is not the focus of this work, in the experiment we just used the same rotation angle as that adopted in the embedding process to re-rotate the attacked image.

6. Cropping attack: the cropping attack was carried out in three different ways, namely center-, side-, and corner-cropping. For center-cropping, a square with a size of 200×200 was cropped from the center of each watermarked image. For side-cropping, a 20-pixel narrow band was cropped from each side of one watermarked image. For corner-cropping, a square with a size of 256×256 was cropped from the upper left corner of each watermarked image.

7. Lossy compression: Two typical compression standards, JPEG and JPEG2000, were selected. JPEG is implemented based on the DCT technique while JPEG2000 is based on the DWT technique. For JPEG compression, the compression qualities (CQs) were selected from 10 to 90 to compress the watermarked images. The larger is the value of CQ, the better will be the quality of the compressed image. The valid value that CQ can be set to is in the range [0, 100]. For JPEG2000 compression, the compression ratios (i.e., the storage size of the raw image to that of the compressed image) were taken from 10 to 90 in our experiment.

The comparison results based on robustness against attacks 1–6 between our scheme and the three other schemes are listed in Table 2. The values of BER and NC listed in this table were obtained by averaging the results for the 10 test images. For subjective comparison, we took the Lena image as an example. The watermarked image was subjected to attacks 1–6 with a specific parameter. The attacked image and the extracted watermark image obtained by our scheme and the scheme with the best performance among the three previous schemes are illustrated in Fig. 7.

From Table 2 we can see that, for all attacks mentioned above except for sharpening and cropping attacks, the performance of our scheme was always superior to those of others. For cropping attacks, since our scheme is block-based, only part of the watermark image is hidden in the blocks located in the cropped region. Although some watermark bits embedded in the cropped region cannot be correctly extracted, the rest of the watermark bits distributed in other blocks can be successfully extracted. Therefore, a high NC value between the extracted watermark image and the

original watermark image can still be obtained and the watermark image can be successfully detected. Similar to our scheme, the schemes of Liu *et al.* (2009) and Song *et al.* (2011) are block-based, and strong robustness against cropping attacks can be achieved by the two schemes for the same reason mentioned above. For the scheme of Naderahmadian and Hosseini-Khayat (2010), because the watermark is embedded in the LL (low-low) sub-band obtained by performing DWT on the host image, the stability of the coefficients in the LL sub-band gives their scheme certain robustness against cropping attacks. Comparable robustness against cropping attacks can be achieved by the four schemes (Table 2). Due to the stability of the first column coefficients of the matrix $\boldsymbol{Q}$ obtained by performing QR factorization, the scheme of Song *et al.* (2011) can achieve a good performance on 'pepper & salt' noise and scaling attacks and a slightly better performance than our scheme on sharpening attack. However, the robustness against other attacks is not strong enough. The schemes of Liu *et al.* (2009) and Naderahmadian and Hosseini-Khayat (2010) can both achieve good robustness against filtering, scaling, and cropping attacks, but their performances on noise and sharpening attacks need improvement. For our scheme, the performances on scaling, noise, and rotation attacks are much better than those of the three other schemes. For example, even though the watermarked image is scaled with a lower scaling factor of 0.1, a high NC value of 0.7808 can still be obtained by our scheme. As for Gaussian noise attacks, our scheme can achieve a higher NC value of 0.9934, while the best result of the other three schemes is only 0.6758. For rotation attacks, when the watermarked image is rotated by a large angle of 20°, our scheme can achieve an NC value of 0.8812, while the best performance of the other schemes is only 0.5654. The better performance of our scheme can be further demonstrated from the extracted watermark image illustrated in Fig. 7. Even though the watermarked image has undergone severe distortion due to different attacks, the extracted watermark image still has a strong correlation with the original watermark image and is distinctly recognizable.

Fig. 8 shows the results of a comparison based on robustness against lossy compressions. The scheme of Song *et al.* (2011) does not work well on JPEG compression (Fig. 8a). The schemes of Liu *et al.* (2009) and Naderahmadian and Hosseini-Khayat (2010) can achieve good performances when the compression quality for JPEG compression is high.

Table 2 Results of a comparison between different schemes based on robustness against different attacks

Attack	BER				NC			
	Ours	Liu *et al.* (2009)	Naderahmadian and Hosseini-Khayat (2010)	Song *et al.* (2011)	Ours	Liu *et al.* (2009)	Naderahmadian and Hosseini-Khayat (2010)	Song *et al.* (2011)
No attack	0	0	0	0	1	1	1	1
Wiener filtering	0.0004	0.0088	0.0534	0.3962	0.9996	0.9913	0.9470	0.6443
Media filtering	0.0018	0.1288	0.1031	0.5000	0.9983	0.8728	0.8982	0.5626
Average filtering	0.0012	0.0379	0.1099	0.4984	0.9988	0.9622	0.8917	0.5558
Scaling_0.1	0.2212	0.4944	0.5025	0.4941	0.7808	0.5101	0.4942	0.6023
Scaling_0.5	0.0018	0.1195	0.1963	0.2688	0.9983	0.8809	0.8053	0.7497
Scaling_0.9	0.0007	0.0647	0.0628	0.1156	0.9993	0.9354	0.9376	0.8880
Gaussian noise	0.0066	0.4896	0.4861	0.3266	0.9934	0.5100	0.5163	0.6758
Pepper & salt	0.0337	0.4852	0.3806	0.0348	0.9664	0.5150	0.6237	0.9656
Sharpening_0.1	0.0468	0.2972	0.5087	0.0218	0.9537	0.7051	0.4926	0.9786
Sharpening_0.9	0.0367	0.2797	0.4972	0.0163	0.9636	0.7237	0.5043	0.9840
Rotation_5°	0.0893	0.4248	0.4077	0.4789	0.9110	0.5747	0.5897	0.5611
Rotation_10°	0.0816	0.4168	0.4001	0.4393	0.9186	0.5840	0.5986	0.5966
Rotation_20°	0.1196	0.4494	0.4386	0.4887	0.8812	0.5451	0.5624	0.5654
Center-cropping	0.1007	0.0932	0.0889	0.0905	0.9116	0.9148	0.9199	0.9206
Side-cropping	0.0920	0.0964	0.0748	0.1092	0.9166	0.9048	0.9283	0.9043
Corner-cropping	0.1427	0.1231	0.1242	0.1190	0.8833	0.8963	0.8955	0.8993

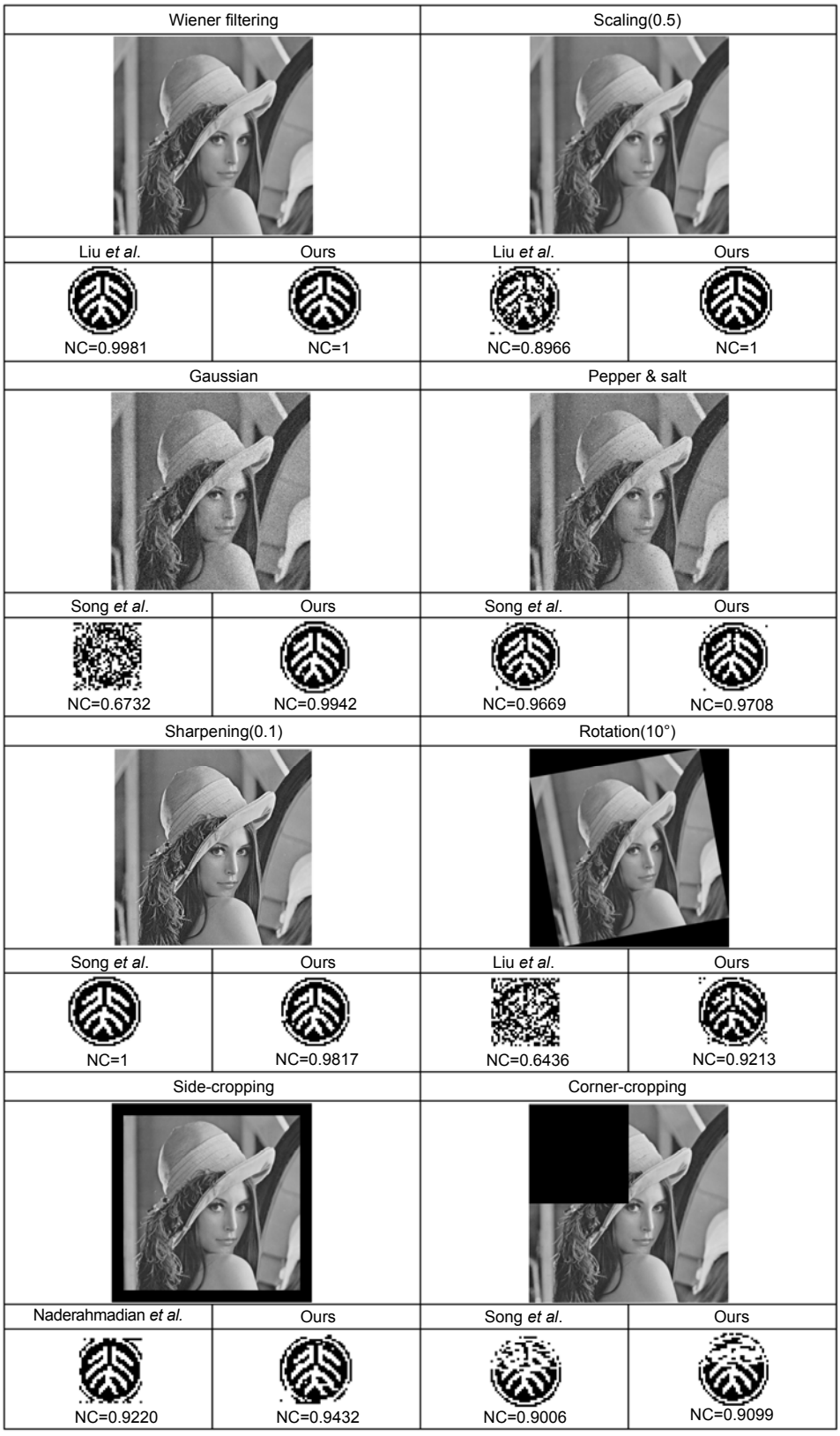


Fig. 7 Comparison of results for different attacks between our scheme and the scheme with the best performance among the three schemes of Liu *et al.* (2009), Naderahmadian and Hosseini-Khayat (2010), and Song *et al.* (2011)

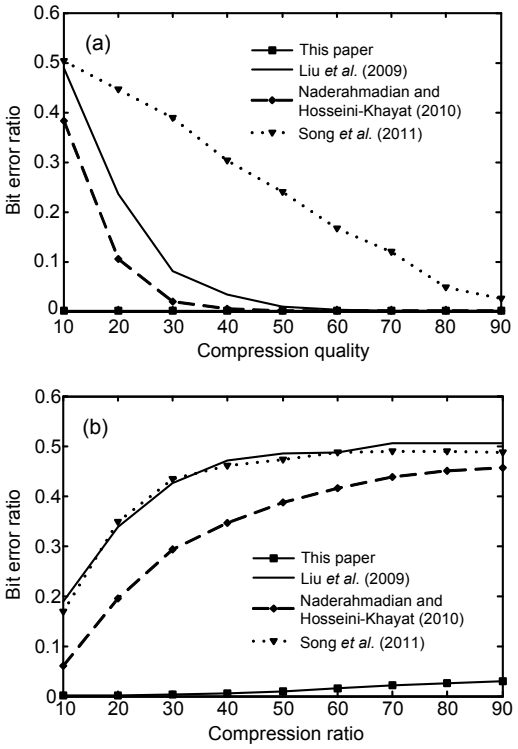


Fig. 8 Performance comparison based on robustness against compression attacks

(a) BER with JPEG compression; (b) BER with JPEG2000 compression

However, with a decrease in the compression quality, their performances deteriorate. For our scheme, when the compression quality varied from 10 to 90, the average BER of the extracted watermark was always equal or close to 0, which demonstrates the strong robustness of our scheme against JPEG compression. For JPEG2000 compression attacks (Fig. 8b), when the compression ratio was larger than 40, the average BERs of the extracted watermark images using the three previous schemes were all higher than 0.3. The schemes of Liu *et al*. (2009) and Song *et al*. (2011) could no longer survive such an attack when the compression ratio grew above 60, since both the obtained average BERs were approaching 0.5. However, even if the watermarked image was compressed by JPEG2000 with a compression ratio of 90, the average BER of our scheme was only about 0.03. Therefore, our scheme can achieve strong robustness against lossy compressions.

To test the robustness of our scheme when the watermarking method is known, we performed Wiener filtering on the DC coefficients obtained by our scheme. Because the private keys are unknown, we cannot obtain the embedding location information, and it cannot be effectively estimated without knowledge of the adopted step size Δ for QIM embedding. Therefore, all the DC coefficients in all blocks were subject to this Wiener filtering attack in this experiment. The average result for the 10 test images is shown in Fig. 9 and we compare it with the result obtained by our method when the watermarking method is unknown. Although the robustness of our scheme is reduced when the watermarking method is known, good performance can still be achieved. For example, even if the PSNR of the attacked watermarked image is only 20 dB, the calculated average BER of the extracted watermark image approaches only 0.4, and we can still successfully detect the existence of the watermark. Therefore, no matter whether the watermarking algorithm is known, strong robustness can be achieved by our scheme.

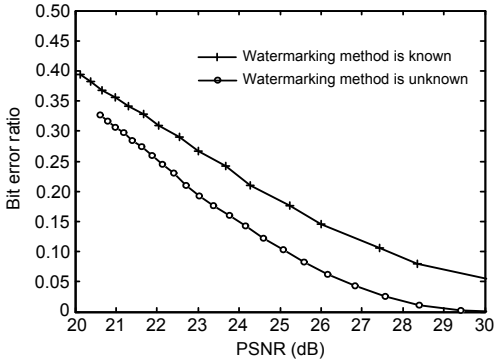


Fig. 9 BER after Wiener filtering based attacks vs. PSNR for our scheme on the condition that the watermarking method is known or unknown

4.3 Discussions

The experimental results described above show that good imperceptibility and strong robustness can be achieved by our scheme, and the performance is better than those of the other schemes selected for comparison. The following three aspects contribute most to the superiority of our scheme:

1. The selected feature used to embed the watermark is resilient to common signal processing operations and lossy compressions.

2. The embedding location selection method can greatly improve the imperceptibility of our scheme.

3. A larger step size Δ for QIM embedding is selected to enhance the robustness of our scheme.

Similar to our scheme, the schemes of Liu *et al*. (2009) and Naderahmadian and Hosseini-Khayat (2010) adopt a quantization-based embedding method to embed the watermark. For such a method, the larger is the selected step size for quantization, the stronger will be the robustness of the embedding, but the more serious will be the caused embedding distortion. Therefore, the schemes of Liu *et al*. (2009) and Naderahmadian and Hosseini-Khayat (2010) select a smaller step size to balance the robustness and imperceptibility of their watermarking methods. However, although a larger step size for QIM is selected by our scheme, the caused embedding distortion can be effectively minimized by using the embedding location selection method to select the blocks with small modifications as the embedding locations. Therefore, compared with the schemes of Liu *et al.* (2009) and Naderahmadian and Hosseini-Khayat (2010), a better performance can be achieved by our scheme. Song *et al*. (2011) used a relation-based method to embed the watermark by adjusting the distance between two selected feature coefficients, and a threshold T is used to control the maximum modification to one feature coefficient. A larger T will improve the robustness of the watermarking scheme, but more serious embedding distortion will be caused. Similar to the schemes of Liu *et al*. (2009) and Naderahmadian and Hosseini-Khayat (2010), the value of T should not be set too large to make an efficient tradeoff between the robustness and imperceptibility of their scheme. Therefore, although a good performance can be achieved by their method, the performance is inferior to that of our scheme.

5 Conclusions

This paper describes a robust watermarking scheme which combines the techniques of QR factorization, DCT, and QIM, and results in a good performance on imperceptibility and robustness. Two aspects contribute most to the strong robustness of our scheme. First, the DC coefficient of the first row elements in the matrix $\boldsymbol{R}$ obtained by performing QR factorization to one block is used as the stable feature, which is resilient to certain attacks. Second, the QIM technique is utilized to embed the watermark, and a larger step size is selected to enhance the robustness of our scheme. Generally speaking, more serious embedding distortion can be caused due to the QIM embedding with a larger step size. However, this can be minimized in our work by using the embedding location selection method to select the blocks with small modifications as the embedding locations, and therefore the imperceptibility of our scheme is greatly improved. Experimental results demonstrate that our scheme can achieve not only good imperceptibility but also strong robustness against common signal processing operations and lossy compressions, like filtering, noise addition, scaling, sharpening, rotation, cropping, and JPEG/JPEG2000 compression. Therefore, our scheme can be used as a good solution for copyright protection of digital images.

References

Barni, M., Bartolini, F., Cappellini, V., Piva, A., 1998. A DCT-domain system for robust image watermarking. *Signal Process.*, **66**(3):357-372. [doi:10.1016/S0165-1684(98)00015-2]

Chandramouli, R., Nasir, M., Majid, R., 2002. Digital Watermarking. *In*: Hornak, J.P. (Ed.), Encyclopedia of Imaging Science and Technology. Wiley, New York, p.226-239.

Chen, B., Wornell, G., 2001. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory*, **47**(4):1423-1443. [doi:10.1109/18.923725]

Gupta, P.K., Shrivastava, S.K., 2010. Improved RST-Attacks Resilient Image Watermarking Based on Joint SVD-DCT. Int. Conf. on Computer and Communication Technology, p.46-51. [doi:10.1109/ICCCT.2010.5640409]

Hu, Y., Wang, Z., Liu, H., Guo, G., 2011. A geometric distortion resilient image watermark algorithm based on DWT-DFT. *J. Softw.*, **6**(9):1805-1812. [doi:10.4304/jsw.6.9.1805-1812]

Huang, H., Yang, C., Hsu, W., 2010. A video watermarking technique based on pseudo-3-D DCT and quantization index modulation. *IEEE Trans. Inf. Forens. Secur.*, **5**(4):625-637. [doi:10.1109/TIFS.2010.2080675]

Lai, C.C., 2011a. An improved SVD-based watermarking scheme using human visual characteristics. *Opt. Commun.*, **284**(4):938-944. [doi:10.1016/j.optcom.2010.10.047]

Lai, C.C., 2011b. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Dig. Signal Process.*, **21**(4):522-527. [doi:10.1016/j.dsp.2011.01.017]

Liu, F., Han, K., Wang, C.Z., 2009. A Novel Blind Watermark Algorithm Based on SVD and DCT. IEEE Int. Conf. on Intelligent Computing and Intelligent Systems, p.283-286. [doi:10.1109/ICICISYS.2009.5357687]

Liu, J., Zhang, X., Sun, J., Lagunas, M.A., 2003. A Digital Watermarking Scheme Based on ICA Detection. 4th Int.

Symp. on Independent Component Analysis and Blind Signal Separation, p.215-220.

Mohammad, A.A., Alhaj, A., Shaltaf, S., 2008. An improved SVD-based watermarking scheme for protecting rightful ownership. *Signal Process.*, **88**(9):2158-2180. [doi:10.1016/j.sigpro.2008.02.015]

Murillo-Fuentes, J.J., 2007. Independent component analysis in the blind watermarking of digital images. *Neurocomputing*, **70**(16-18):2881-2890. [doi:10.1016/j.neucom.2006.06.011]

Naderahmadian, Y., Hosseini-Khayat, S., 2010. Fast Watermarking Based on QR Decomposition in Wavelet Domain. 6th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, p.127-130. [doi:10.1109/IIHMSP.2010.39]

Phadikar, A., Maity, S.P., Verma, B., 2011. Region based QIM digital watermarking scheme for image database in DCT domain. *Comput. Electr. Eng.*, **37**(3):339-355. [doi:10.1016/j.compeleceng.2011.02.002]

Rastegar, S., Namazi, F., Yaghmaie, K., Amir, A., 2011. Hybrid watermarking algorithm based on singular value decomposition and Radon transform. *AEU Int. J. Electron. Commun.*, **65**(7):658-663. [doi:10.1016/j.aeue.2010.09.008]

Sakib, M.N., Alam, S.B., Sazzad, A.B.M.R., Shahnaz, C., Fattah, S.A., 2011. A Basic Digital Watermarking Algorithm in Discrete Cosine Transformation Domain. 2nd Int. Conf. on Intelligent Systems, Modelling and Simulation, p.419-421. [doi:10.1109/ISMS.2011.72]

Seo, Y., Kim, W., Suh, Y., Oh, W., Hwang, C., 2007. QIM Watermarking for Image with Two Adaptive Quantization Step-Sizes. 9th Int. Conf. on Advanced Communication Technology, p.797-800. [doi:10.1109/ICACT.2007.358470]

Shen, Z.W., Liao, W.W., Shen, Y.N., 2009. Blind Watermarking Algorithm Based on Henon Chaos System and Lifting Scheme Wavelet. Int. Conf. on Wavelet Analysis and Pattern Recognition, p.308-313. [doi:10.1109/ICWAPR.2009.5207447]

Song, W., Hou, J., Li, Z., Huang, L., 2011. Chaotic system and QR factorization based robust digital image watermarking algorithm. *J. Cent. South Univ. Technol.*, **18**(1):116-124. [doi:10.1007/s11771-011-0668-8]

Su, Q., Liu, X., Yang, W., 2009. A Watermarking Algorithm for Color Image Based on YIQ Color Space and Integer Wavelet Transform. Int. Conf. on Image Analysis and Signal Processing, p.70-73. [doi:10.1109/IASP.2009.5054573]

Wang, W., Men, A., Chen, X., 2009. Robust Image Watermarking Scheme Based on Phase Features in DFT Domain and Generalized Radon Transformations. Int. Congress on Image and Signal Processing, p.1510-1514. [doi:10.1109/CISP.2009.5303553]

Won, C.S., 2010. Boosting robustness against composite attacks for quantization index-modulation algorithms. *J. Electron. Imag.*, **19**(2):023010. [doi:10.1117/1.3427158]

Zeki, A.M., Manaf, A.A., Mahmod, S.S., 2011. High watermarking capacity based on spatial domain technique. *Inf. Technol. J.*, **10**(7):1367-1373. [doi:10.3923/itj.2011.1367.1373]