

A blind double color image watermarking algorithm based on QR decomposition

Qingtang Su · Yugang Niu · Hailin Zou ·
Yongsheng Zhao · Tao Yao

Published online: 10 August 2013

© Springer Science+Business Media New York 2013

Abstract In this paper, a novel blind image watermarking scheme based on QR decomposition is proposed to embed color watermark image into color host image, which is significantly different from using the binary or gray image as watermark. When embedding watermark, the 24-bits color host image with size of 512×512 is divided into non-overlapping 4×4 pixel blocks and each pixel block is decomposed by QR. Then, according to the watermark information and the relation between the second row first column coefficient and the third row first column coefficient in the unitary matrix Q , the 24-bits color watermark image with size of 32×32 is embedded into the color host image. In addition, the new element compensatory method is used in the upper-triangle matrix R for reducing the visible distortion. When extracting watermark, only the watermarked image is needed. Compared with other SVD-based methods, the proposed method does not have the false-positive detection problem and has lower computational complexity, that is, the average running time of the proposed method only needs 1.481403 s. The experimental results show that the proposed method is robust against most common attacks including JPEG compression, JPEG 2000 compression, low-pass filtering, cropping, adding noise, blurring, rotation, scaling and sharpening et al. Compared with some related existing methods, the proposed algorithm has stronger robustness and better invisibility.

Keywords QR decomposition · Color watermark image · Blind extraction · Image watermarking

1 Introduction

In recent years, with more and more color images appearing on the Internet, the problem of copyright protection has been receiving more and more attention. Among the published

Q. Su (✉) · H. Zou · Y. Zhao · T. Yao

School of Information Science and Engineering, Lu Dong University, Yantai 264025 Shandong, People's Republic of China

e-mail: sdysqt@163.com

Q. Su · Y. Niu

Key Laboratory of Advanced Control and Optimization for Chemical Process, Ministry of Education, East China University of Science and Technology, Shanghai 200237, People's Republic of China

copyright protection techniques, digital watermarking is considered as a powerful method. There are still several important issues existing in the watermarking system. Firstly, the embedded watermark should not degrade the quality of the image and should be perceptually invisible to maintain its protective secrecy. Secondly, the watermark must be robust enough to resist common image processing attacks and not be easily removed; only the owner of the image is able to extract the watermark. Thirdly, the blind watermarking technique is necessary since sometimes it is not easy to obtain the original image or original watermark during extraction process. Compared with the method of embedding binary or gray images into color image [2, 4, 6, 9, 14, 18, 19], the double color watermarking, i.e., embedding color watermark images into color host image [5, 7, 25], not only has the features of more information and higher fidelity, but also can solve the copyright problems for some corporations which using the unique identifiable color log as corporation mark.

Recently, some works on the SVD-based watermarking have been published, which sufficiently utilized the stable property of the singular value matrix [7, 11, 13, 22, 24]. For example, Yin et al. [24] proposed a SVD-based color image watermarking, in which the singular values of original watermark were required to extract the embedded singular values, and then the U and V orthogonal matrices of original watermark were utilized to recover the watermark. In [11], two orthogonal matrices U , V and the diagonal matrix S of the original watermark were viewed as the user's secret keys to extract watermark, in which the original host image was needed to extract watermark. The method in [22] also required the singular values of the original watermark to extract the embedded color watermark information. In [13], a hybrid robust digital watermarking algorithm based on finite Radon transform and SVD is proposed. It is noted that in the aforementioned SVD-based methods [13, 24], only the singular values of watermark were embedded in the host image, which might result in the false-positive detection problem such that the attackers can easily prove the ownership of the arbitrary watermarked image without knowing the original watermark embedded in the host image. Although a blind color image watermarking was proposed in [7], one or more singular values must be modified to keep the order of singular values, which might degrade the quality of the watermarked image.

In addition, the SVD has sophisticated computation. Especially, when the problem is of recursive nature, the SVD requires $O(n^3)$ flops for a matrix of order n . As a major intermediate step in SVD, the QR decomposition only needs $O(n^2)$ flops, which is lower than that of SVD [8, 10]. The feature highlights the use of QR decomposition in digital watermarking and a few of methods have been proposed in [16, 23]. Yashar et al. [23] proposed to embed a watermark bit in the first row of R matrix after each 8×8 block was decomposed by QR decomposition, in which the watermark was 88×88 binary image. In [16], by modifying the elements in the Q matrix, a 32×32 binary image was embedded into the 512×512 host image. The common feature in [16, 23] was to use binary image as the watermark. As is well known, the binary information included in the 24-bit color image is twenty-four times more than that of the binary image with same size. When embedding the color image watermark into color host image, the watermark capacity increases by eight times. That is, the method [23] could not be better used to embed large amounts of color watermark information into host image. Meanwhile, in [16], the threshold T and the embedding rules were not suitable for the color watermark image, which can be proved in Fig. 5. Therefore, these mentioned methods [16, 23] cannot be better used to embed the color image watermark into color host image.

Motivated by the above discussion, we propose a new double color image blind algorithm based on QR decomposition. By analysis, it is found that there is a stronger correlation between $q_{2,1}$ and $q_{3,1}$ of Q matrix after performing QR decomposition on 4×4 pixels matrix. Thus, this

relation may be utilized to represent one kind of embedded watermark information, ‘1’ or ‘0’. Hence, the number of modified pixels may be reduced and the invisibility and robustness of watermark can be improved. In this proposed method, the watermark extraction can be performed in a blind manner via the above correlation. Moreover, the presented compensatory method is used in the R matrix to enhance the imperceptibility of watermark. Especially, because all information of color image watermark can be embedded into the host image, the false-positive detection problem like in SVD-based algorithm will not happen. Finally, the experimental results show that the proposed scheme can attain better invisibility and stronger robustness against many common image processing attacks such as image compression, low-pass filtering, cropping, and so on. Meanwhile, the comparisons with related SVD-based algorithm and spatial-domain algorithm also reveal the higher efficiency of the proposed algorithm.

The rest of this paper is organized as follows. The related operations in QR decomposition are described in Section 2. The detailed watermark embedding and extraction procedures are presented in Section 3. Subsequently, Section 4 gives the experimental results and comparisons with other related methods. Finally, conclusions are made in Section 5.

2 Preliminary

2.1 QR Decomposition

In QR decomposition [1], the orthogonal-triangular decomposition of a matrix is performed, which is defined as

$$[Q, R] = qr(A) \quad (1)$$

where an $m \times m$ matrix A produces an $m \times m$ upper triangular matrix R and an $m \times m$ unitary matrix Q so that $A=Q \times R$.

2.2 Selecting the embedding position in unitary matrix Q

Suppose one $m \times n$ image block in RGB color space is $A=[a1, a2, \dots, an]$, any column vector $ai(i=1, 2, \dots, n)$ includes m elements. Since the pixel values of the color image in RGB color space are between 0 and 255, the matrix elements that represent the color image pixels should be non-negative. Thus, any element $a_{j,1}(j=1, 2, \dots, m)$ in the first column $a1$ meets the following condition expression.

$$a_{j,1} \geq 0 \quad (2)$$

Meanwhile, let $Q=[q1, q2, \dots, qn]$ be the unitary matrix of image block A , and the first column vector $q1$ can be described in Eq. (3) according to Gram-Schmidt orthogonalization process.

$$q1 = \frac{a1}{\|a1\|} \quad (3)$$

where $\|\cdot\|$ is the norm operation. According to the Eqs. (2) and (3), any element $q_{j,1}(j=1, 2, \dots, m)$ of the first column $q1$ meets the following condition.

$$q_{j,1} \geq 0 \quad (4)$$

That is, the first column vector in the unitary matrix of image block has stable non-negative feature that can be used to embed watermark in RGB color space.

In order to further determine the accurate embedding position in the first column of Q matrix after performing QR decomposition on $m \times n$ image block, let $m=n=4$ and suppose one matrix includes the x -th row first column element $q_{x,1}$ of each Q matrix and another one includes the y -th row first column element $q_{y,1}$ of each Q matrix, respectively, where $x \neq y$. Now, the similarity degree between the above two matrices is computed by the Normalized cross-Correlation (NC). Table 1 shows the experimental results of many standard test images. As seen from the table, the average value of NC ($q_{2,1}, q_{3,1}$) is 0.9874, which shows $q_{2,1}$ and $q_{3,1}$ are the closest elements in the first column of 4×4 Q matrix. This strong similarity relation can represent one kind of embedded watermark information ‘1’ or ‘0’. Thus, watermark can be embedded by slightly modifying the magnitude relationship between $q_{2,1}$ and $q_{3,1}$.

2.3 Compensating the visual distortion in upper triangular matrix R

When $q_{2,1}$ and $q_{3,1}$ are modified for embedding watermark, the image visual quality will be inevitably affected. Hence, the compensatory method is proposed to possibly decrease the negative affection. For explaining the proposed compensatory method, we assume the original pixel block A is a 4×4 matrix and the QR decomposition of A is performed as follows.

$$\begin{aligned}
 A = [a1, a2, a3, a4] &= \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix} = QR \\
 &= [q1, q2, q3, q4][r1, r2, r3, r4] \\
 &= \begin{bmatrix} q_{1,1} & q_{1,2} & q_{1,3} & q_{1,4} \\ q_{2,1} & q_{2,2} & q_{2,3} & q_{2,4} \\ q_{3,1} & q_{3,2} & q_{3,3} & q_{3,4} \\ q_{4,1} & q_{4,2} & q_{4,3} & q_{4,4} \end{bmatrix} \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} \\ 0 & r_{2,2} & r_{2,3} & r_{2,4} \\ 0 & 0 & r_{3,3} & r_{3,4} \\ 0 & 0 & 0 & r_{4,4} \end{bmatrix}
 \end{aligned}
 \tag{5}$$

Table 1 The NC values of different elements in first column of Q matrix after QR decomposition

Image	NC($q_{1,1}, q_{2,1}$)	NC($q_{1,1}, q_{3,1}$)	NC($q_{1,1}, q_{4,1}$)	NC($q_{2,1}, q_{3,1}$)	NC($q_{2,1}, q_{4,1}$)	NC($q_{3,1}, q_{4,1}$)
Lena	0.9888	0.9827	0.9829	0.9955	0.9845	0.9898
Peppers	0.9643	0.9512	0.9492	0.9902	0.9663	0.9763
F16	0.9890	0.9825	0.9778	0.9965	0.9835	0.9903
Baboon	0.9549	0.9416	0.9367	0.9639	0.9361	0.9552
House	0.9968	0.9945	0.9939	0.9990	0.9953	0.9971
Bear	0.8745	0.8475	0.8494	0.9591	0.9047	0.9313
Kid	0.9898	0.9844	0.9800	0.9942	0.9801	0.9882
Couple	0.8980	0.8669	0.8580	0.9799	0.9153	0.9479
Sailboat	0.9889	0.9822	0.9805	0.9971	0.9823	0.9892
Barbara	0.9880	0.9793	0.9755	0.9954	0.9809	0.9904
TTU	0.9720	0.9554	0.9536	0.9908	0.9773	0.9858
Average	0.9641	0.9517	0.9489	0.9874	0.9642	0.9765

Performing the matrix multiplication for QR, the result is given by Eq. (6).

$$A = \begin{bmatrix} q_{1,1}r_{1,1} & q_{1,1}r_{1,2} + q_{1,2}r_{2,2} & q_{1,1}r_{1,3} + q_{1,2}r_{2,3} + q_{1,3}r_{3,3} & q_{1,1}r_{1,4} + q_{1,2}r_{2,4} + q_{1,3}r_{3,4} + q_{1,4}r_{4,4} \\ q_{2,1}r_{1,1} & q_{2,1}r_{1,2} + q_{2,2}r_{2,2} & q_{2,1}r_{1,3} + q_{2,2}r_{2,3} + q_{2,3}r_{3,3} & q_{2,1}r_{1,4} + q_{2,2}r_{2,4} + q_{2,3}r_{3,4} + q_{2,4}r_{4,4} \\ q_{3,1}r_{1,1} & q_{3,1}r_{1,2} + q_{3,2}r_{2,2} & q_{3,1}r_{1,3} + q_{3,2}r_{2,3} + q_{3,3}r_{3,3} & q_{3,1}r_{1,4} + q_{3,2}r_{2,4} + q_{3,3}r_{3,4} + q_{3,4}r_{4,4} \\ q_{4,1}r_{1,1} & q_{4,1}r_{1,2} + q_{4,2}r_{2,2} & q_{4,1}r_{1,3} + q_{4,2}r_{2,3} + q_{4,3}r_{3,3} & q_{4,1}r_{1,4} + q_{4,2}r_{2,4} + q_{4,3}r_{3,4} + q_{4,4}r_{4,4} \end{bmatrix} \quad (6)$$

Assume $q_{2,1}, q_{3,1}$ are modified by adding $\Delta 1$ and $\Delta 2$, respectively, which will result in the changes of the original pixels $a_{2,n}, a_{3,n}, n=(1,2,3,4)$. Thus, we can modify $r_{1,1}, r_{1,2}, r_{1,3}, r_{1,4}$ for compensating the visible distortion, and assume the modified quantity is $\Delta 3, \Delta 4, \Delta 5, \Delta 6$, respectively.

For example, the following Eq. (7) must be met to compensate the $a_{2,1}$.

$$(q_{2,1} + \Delta 1)(r_{1,1} - \Delta 3) = q_{2,1}r_{1,1} = a_{2,1} \quad (7)$$

That is,

$$\Delta 3 = \frac{\Delta 1 r_{1,1}}{q_{2,1} + \Delta 1} \quad (8)$$

As the same reason, $\Delta 3$ also need to meet the following Eq. (9) for compensating $a_{3,1}$.

$$\Delta 3 = \frac{\Delta 2 r_{1,1}}{q_{3,1} + \Delta 2} \quad (9)$$

In order to keep the robustness of watermark, we adopt the following Eq. (10) to determine $\Delta 3$.

$$\Delta 3 = \frac{1}{2} \left(\frac{\Delta 1 r_{1,1}}{q_{2,1} + \Delta 1} + \frac{\Delta 2 r_{1,1}}{q_{3,1} + \Delta 2} \right) \quad (10)$$

Similarly, $\Delta 4, \Delta 5, \Delta 6$ are determined via the following equations, respectively.

$$\Delta 4 = \frac{1}{2} \left(\frac{\Delta 1 r_{1,2}}{q_{2,1} + \Delta 1} + \frac{\Delta 2 r_{1,2}}{q_{3,1} + \Delta 2} \right) \quad (11)$$

$$\Delta 5 = \frac{1}{2} \left(\frac{\Delta 1 r_{1,3}}{q_{2,1} + \Delta 1} + \frac{\Delta 2 r_{1,3}}{q_{3,1} + \Delta 2} \right) \quad (12)$$

$$\Delta 6 = \frac{1}{2} \left(\frac{\Delta 1 r_{1,4}}{q_{2,1} + \Delta 1} + \frac{\Delta 2 r_{1,4}}{q_{3,1} + \Delta 2} \right) \quad (13)$$

Define the modified $a_{2,n}, a_{3,n}$ as $a_{2,n}', a_{3,n}'$ when embedding operation is performed but compensatory operation is not adopted, and the modified $a_{m,n}$ as $a_{m,n}''$ when compensatory operation is further used, here $m=(1,2,3,4), n=(1,2,3,4)$. Note the compensatory operation may cause larger change than without the compensatory operation. Only the following condition Eq. (14) is true, the compensatory operation is further used; otherwise no modification is performed on $r_{1,1}, r_{1,2}, r_{1,3}, r_{1,4}$.

$$\sum_{m=1}^4 \sum_{n=1}^4 (a''_{m,n} - a_{m,n})^2 < \sum_{m=2}^3 \sum_{n=1}^4 (a'_{m,n} - a_{m,n})^2 \tag{14}$$

3 The proposed watermarking scheme

In this section, a new double color image blind watermarking scheme based on QR decomposition is proposed. As shown in Fig. 1, the color watermark image is embedded into color host image and the final watermark can be extracted from the watermarked image without the original host image or watermark image. Without loss of generality, let the original host image H be 24-bit color image with size of $M \times M$ and the watermark image be 24-bit color image W with size of $N \times N$. The detailed embedding procedures are as follows.

3.1 Watermark embedding process

The summary process of the watermark embedding is shown in Fig. 2 and the detailed steps are listed as follows.

Step 1. Pre-processing on the color watermark image

Since the color image has much more information than the binary or grayscale image, its binarization process is important in that it will directly affect the embedded quality of watermarking. Firstly, 3-D original color watermark image W is divided into three components R, G, B by dimension-reduction treatment. Then, the 2-D component watermarks are obtained corresponding to the R, G and B component, respectively. In order to enhance the security and robustness of the embedded watermark, each component watermark is permuted by Arnold transform with private key KA_i ($i=1, 2, 3$) and each pixel value is converted to 8-bit binary sequence [3]. Finally, combining all 8-bit binary sequence to form the binary component watermark W_i ($i=1, 2, 3$).

Step 2. Block processing of the host image

The host image H is also divided into three components H_i ($i=1, 2, 3$), which represents the R, G and B component respectively, and each component image is divided into 4×4 non-overlapping blocks.

Step 3. Selecting the embedding blocks

The MD5-based Hash pseudo-random replacement algorithm with private key K_i ($i=1, 2, 3$) is used to select the embedding block in H_i for embedding the corresponding component watermark W_i [15]. The MD5 algorithm will be used to randomly select the non-collision embedding blocks to ensure the security of watermark.

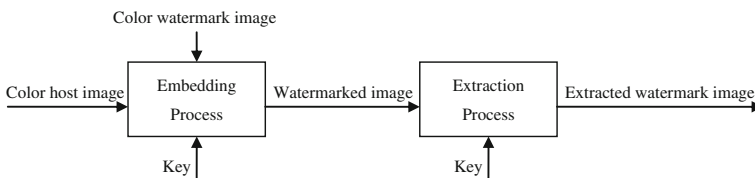


Fig. 1 Block diagram of the proposed watermarking scheme

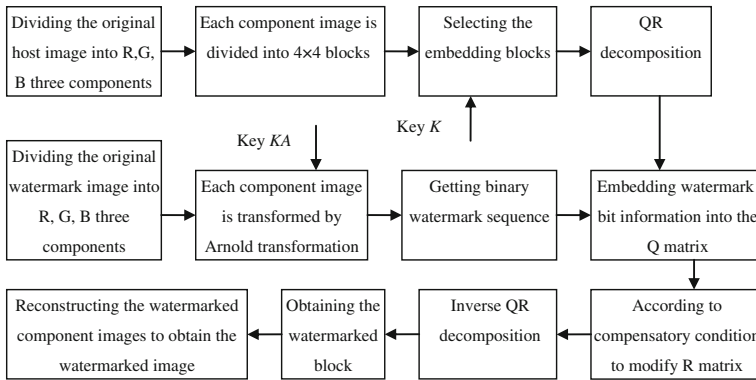


Fig. 2 Watermark embedding process

Step 4. QR decomposition

Each selected block is decomposed by QR decomposition according to Eq. (1) to obtain the unitary matrix Q .

Step 5. Embedding watermark

The watermark is embedded by changing the magnitude relation between the second ($q_{2,1}$) and the third ($q_{3,1}$) elements in the first column of Q matrix. If the embedded watermark information bit is ‘1’, the difference between $q_{2,1}$ and $q_{3,1}$ should be greater than a threshold T . If the embedded binary watermark bit is ‘0’, the difference between $q_{3,1}$ and $q_{2,1}$ should be greater than a threshold T . When these two conditions are violated, $q_{2,1}$ and $q_{3,1}$ should be modified as $q'_{2,1}$ and $q'_{3,1}$ based on the following rules in Eqs. (15) and (16), respectively.

$$\text{if } w = 1 \text{ and } q_{2,1} - q_{3,1} < T, \text{ then } \begin{cases} q'_{2,1} = q_{avg} + T/2 \\ q'_{3,1} = q_{avg} - T/2 \end{cases} \quad (15)$$

$$\text{if } w = 0 \text{ and } q_{3,1} - q_{2,1} \leq T \text{ then } \begin{cases} q'_{2,1} = q_{avg} - T/2 \\ q'_{3,1} = q_{avg} + T/2 \end{cases} \quad (16)$$

where w indicates the embedded binary watermark information bit and $q_{avg} = (q_{2,1} + q_{3,1})/2$.

Step 6. If the condition of Eq. (14) is true, then according to the mentioned compensatory method in Section 2.3 to compensate the related elements in R matrix.

Step 7. Inverse QR operation

The inverse QR operation is performed to obtain the watermarked image block according to Eq. (17).

$$A' = Q' \times R \quad (17)$$

Step 8. Repetition

Repeating steps 4–7 until all watermark bits are embedded in the host image. Finally, the watermarked R, G, B components are reconstructed to obtain the watermarked image H' .

Since all information of color image watermark has been embedded into the host image, which means the final extracted watermark will be decided by the all watermark information bits but is not the partial watermark information, the false-positive detection problem like in SVD-based algorithm will not happen.

3.2 Watermark extraction process

According to whether the original host image and watermark image are needed in the extraction procedure, the watermarking scheme could be categorized into blind scheme or non-blind scheme. As shown in Fig. 3, the watermark extraction procedure belongs to blind extraction method, that is, the original host image and watermark image are not needed in the procedure. The detailed steps of the watermark extraction are described as follows.

Step 1. Pre-processing on the watermarked image

The watermarked image H' is divided into R, G, B component images, which are further divided into watermarked blocks with size of 4×4 pixels, respectively.

Step 2. Select the watermarked block

Using the Hash pseudo-random replacement based on private key K_i ($i=1, 2, 3$) to select the watermarked blocks.

Step 3. QR decomposition

Each watermarked block is decomposed by QR decomposition and its unitary matrix Q' is obtained.

Step 4. Extract watermark

The relation between $q_{2,1}'$ and $q_{3,1}'$ in the first column of Q' is used to extract the watermark information w' , as shown in Eq. (18).

$$w' = \begin{cases} 1, & \text{if } q'_{2,1} \geq q'_{3,1} \\ 0, & \text{if } q'_{2,1} < q'_{3,1} \end{cases} \quad (18)$$

Step 5. Repetition

The above steps 2–4 are repeated until all embedded image blocks are performed. These extracted bit values are partitioned into 8-bit groups and converted to decimal pixel values.

Step 6. Reconstruction

Each component watermark is transformed by the inverse Arnold transformation based on the private key KA_i ($i=1, 2, 3$). Then, the final extracted watermark W' is reconstructed from the extracted watermarks of the three components.

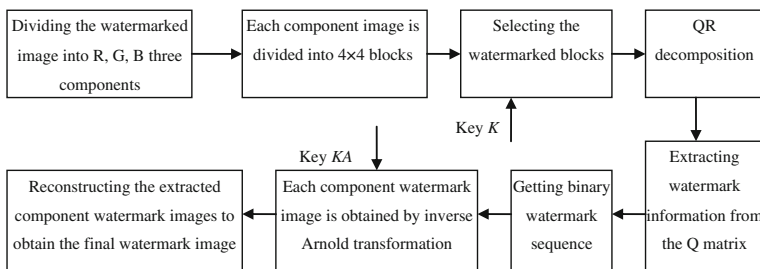


Fig. 3 Watermark extraction process

4 Experimental results and discussion

In this experiment, all 24-bit 512×512 color images in the CVG-UGR image database are used as the host images [20]. Additionally, two 24-bit color images with size of 32×32 , as shown in Fig. 4(a), (b), are used as original watermarks. Generally, the bigger the size of image block is, the smaller the watermark capacity is, the worse the watermark invisibility is and the better the watermark robustness is, vice versa. Meanwhile, the bigger the threshold T is, the worse the watermark invisibility is and the better the watermark robustness is, vice versa. Considering the tradeoff between the invisibility and the robustness of watermarking and based on many experiments, let the size of image block be 4×4 and the threshold T be 0.042.

The performance of the watermarking methods under consideration is investigated by measuring their imperceptible and robust capabilities. For the imperceptible capability, the structural similarity (SSIM) index as a new method is used to measure the similarity between the original color image H and the watermarked image H' . SSIM is designed to improve on traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proved to be inconsistent with human eye perception [21]. For the robust capability, the Normal cross-Correlation (NC) measures the similarity between the original color watermark W and the corresponding extracted watermark W' [17]. Besides NC, the above-mentioned SSIM is also used to evaluate and compare the visual quality of extracted watermarks in section 4.1.

To investigate the robustness of the proposed method, different host images and different watermarks are adopted to compare with the methods of [7] and [5], and several attacks are simulated to degrade the watermarked images.

4.1 The watermark invisibility comparison between different methods

When the different watermark images in Fig. 4(a) and (b) were respectively embedded into all 512×512 color images of the CVG-UGR image database, the average SSIM values of all watermarked images, the average SSIM values and NC values of extracted watermark images were obtained and shown in Table 2. Based upon this experiment, we draw the conclusion that the proposed method can effectively to embed and extract color watermark image.

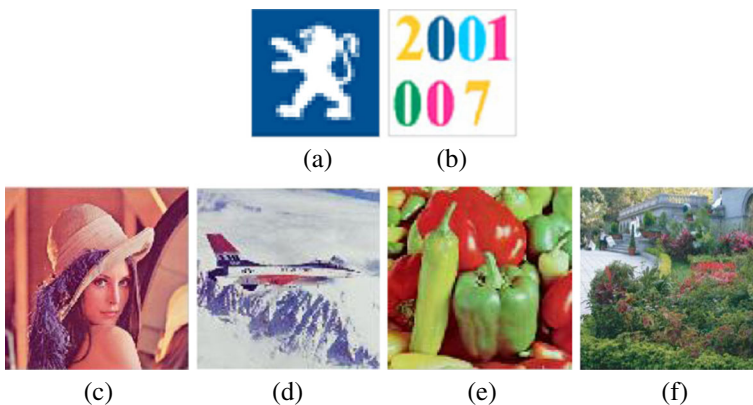


Fig. 4 Original watermark images: **a** PEUGEOT logo, **b** 8-color image; Original host images: **c** Lena, **d** Avion, **e** Peppers, **f** TTTU

Table 2 The average results when the different watermark images are respectively embedded into all 24-bit 512×512 color images of the CVG-UGR image database

Watermark image	Average SSIM values of all watermarked images	Average NC values of all extracted watermarks	Average SSIM values of all extracted watermarks
Fig. 4(a)	0.9682	0.9842	0.9459
Fig. 4(b)	0.9663	0.9964	0.9653

As an example, in order to evaluate the invisibility of the embedded watermark, we embed the watermark of Fig. 4(a) in the host images of Fig. 4(c) and (d), and embed the watermark of Fig. 4(b) in the host images of Fig. 4(e) and (f), respectively. Here, Fig. 4(c), (d) and (e) are three standard images of the CVG-UGR image database, and Fig. 4(f) is a common image that will be used to compare with the method [5] in the following section 4.2.

Figure 5 not only gives the watermarked color images and their SSIM values, but also shows the extracted watermark and their NC and SSIM values. By comparison, it can be seen that Song et al. [16] based on QR decomposition could not extract good watermark and the host image is obviously modified via embedding the watermark, which can not meet the need of watermark invisibility. Thus, this method of Song et al. [16] is not suitable for embedding color watermark image into color host image. Golea et al. [7] and the proposed method have better watermark imperceptibility, but the former has lower NC and SSIM values than the latter. Thus, the proposed method not only has better watermark invisibility, but also can effectively extract the embedded watermark. To further prove the other performances of the proposed method, the different comparisons with the relating methods are made in the following sub-section.

4.2 The watermark robustness comparison between different methods

4.2.1 Comparison with the SVD-based algorithm

In this sub-section, various attacks such as JPEG compression, JPEG2000 compression, cropping, adding noise, scaling, filtering, rotation, blurring et al. are performed on the watermarked image to estimate the robustness of the proposed method, and compare the proposed method with the related work [7]. For saving some space, we give the extracted results from the attacked images Lena and F16 after the watermark of Fig. 4(a) was embedded into.

JPEG is one of the most used formats in the Internet and digital camera. The JPEG quality factor is a number between 0 and 100. When the quality factor is decreased from 100, the image compression is improved, but the quality of the resulting image is significantly reduced. In this experiment, the watermarked images are compressed with different compression factors from 10–100 increasing in steps of 10. Figure 6 gives the part of the results. Compared with the method [7], the proposed scheme achieves better robust against the JPEG compression.

JPEG 2000 is developed by the JPEG in the aim of improving the properties of the JPEG standard. The watermarked images are also performed by JPEG 2000 compression with the compression ratio from 1–10 increasing in steps of 1. Figure 7 gives the NC values, SSIM values and visual-perception results with compression ratios of 5 and 10, respectively.

In addition, a salt & peppers noising scheme is performed by generating noise to corrupt the watermarked images. The noising scheme generates 2 % and 10 % noise, respectively, to

























Method	Golea et al. [7]	Song et al.[17]	Proposed method
watermarked image (SSIM)	 0.9935	 0.6332	 0.9589
Extracted watermark (NC / SSIM)	 0.9937 / 0.9935	 0.8032 / 0.4282	 1.0000 / 0.9999
watermarked image (SSIM)	 0.9940	 0.5411	 0.9256
Extracted watermark (NC / SSIM)	 0.9949 / 0.9941	 0.8034 / 0.4282	 1.0000 / 1.0000
watermarked image (SSIM)	 0.9279	 0.7111	 0.9682
Extracted watermark (NC / SSIM)	 0.9801 / 0.9298	 0.9293 / 0.3630	 0.9979 / 0.9894
watermarked image (SSIM)	 0.9970	 0.8241	 0.9854
Extracted watermark (NC / SSIM)	 0.9919 / 0.9969	 0.9262 / 0.3632	 1.0000 / 1.0000

Fig. 5 The watermarked color images and the extracted watermarks without any attacks

degrade the watermarked images. Figure 8 shows the quantitative results in terms of the NC, SSIM and visual-perception, respectively. It is evident from these results that the proposed method is more robust against salt & peppers noise attacks than the method [7].

Moreover, the Gaussian noising is also added to corrupt the watermarked images. The mean of Gaussian parameters are set to 0.1, 0.3, respectively. The extracted watermarks, NC values and SSIM values are shown in Fig. 9. The robustness of the proposed method is

Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
JPEG 30	Lena	0.6531 / 0.1861			0.7530 / 0.3502
	Avion	0.8204 / 0.2877			0.8353 / 0.4975
JPEG 90	Lena	0.9712 / 0.4888			0.9827 / 0.8838
	Avion	0.9760 / 0.6806			0.9910 / 0.9591

Fig. 6 The extracted watermarks via using different methods after the JPEG compression operation

superior to that of the method [7] when the mean parameter is smaller. However, the bigger the Gaussian parameter is, the weaker the robustness is. Hence, it must be further improved in the future work.

Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
JPEG 2000 (5:1)	Lena	0.9390 / 0.4097			0.9836 / 0.9271
	Avion	0.9375 / 0.5951			0.9936 / 0.9834
JPEG 2000 (10:1)	Lena	0.8071 / 0.3533			0.9026 / 0.5807
	Avion	0.7951 / 0.3364			0.9716 / 0.8755

Fig. 7 The extracted watermarks via using different methods after the JPEG 2000 compression operation

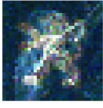






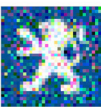
Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Salt & Peppers noise (0.02)	Lena	0.5698 / 0.3206			0.9904 / 0.8824
	Avion	0.5279 / 0.2504			0.9846 / 0.9089
Salt & Peppers noise (0.10)	Lena	0.3977 / 0.4047			0.9362 / 0.6931
	Avion	0.3968 / 0.3867			0.9282 / 0.6974

Fig. 8 The extracted watermarks via using different methods after the salt & peppers noising operation

Figure 10 shows the NC values, SSIM values and visual-perception results after low-pass filters attack. In this experiment, the Butterworth low-pass filters are used to corrupt the watermarked images with cut-off frequency 100, and order 1, 3, respectively.


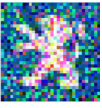



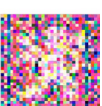


Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Gaussian noise (0.1)	Lena	0.8600 / 0.3151			0.8558 / 0.4697
	Avion	0.8188 / 0.3296			0.9222 / 0.6692
Gaussian noise (0.3)	Lena	0.5919 / 0.3113			0.5090 / 0.2093
	Avion	0.6511 / 0.2044			0.4555 / 0.2178

Fig. 9 The extracted watermarks via using different methods after the Gaussian noising operation



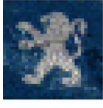

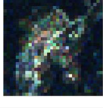
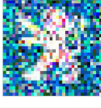


Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Low-pass Filter (100,1)	Lena	0.5477 / 0.4971			0.9584 / 0.8451
	Avion	0.5855 / 0.4089			0.9205 / 0.7507
Low-pass Filter (100,3)	Lena	0.3818 / 0.1411			0.7987 / 0.4457
	Avion	0.4650 / 0.2687			0.7779 / 0.4728

Fig. 10 The extracted watermarks via using different methods after the low-pass filter operation

Figure 11 gives the result of sharpening attack. In the procedure of sharpening, the radii are 0.2 and 1.0, respectively. It is proved that the proposed method outperforms the method [7]. We can notice that the extracted watermarks closely resemble the original watermarks.









Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Sharpening (0.2)	Lena	0.93911 / 0.7705			0.9991 / 0.9998
	Avion	0.9397 / 0.7708			0.9999 / 0.9999
Sharpening (1.0)	Lena	0.9119 / 0.7211			0.9974 / 0.9997
	Avion	0.8135 / 0.5281			0.9917 / 0.9996

Fig. 11 The extracted watermarks via using different methods after the sharpening operation

Figure 12 shows the quantitative results and visual-perception results for the case of scaling, respectively. In this experiment, two scaling operations of 400 % and 25 % are utilized to deteriorate the watermarked image.

In the blurring attacks, two cases are simulated here to degrade the two watermarked images. The radius in the first case is 0.2, while the second case is 1.0. Figure 13 exhibits the results of visual comparison and quantitative values. It is evident that the proposed method is more robust than the method [7] in this case.

In order to test the robustness against rotation attacks, two experiments are investigated. One involves rotating the watermarked image to the right by 5° . The other experiment involves rotating the watermarked image to the right by 30° . The images are first rotated a certain number of degrees clockwise, and then are rotated the same number of degrees counterclockwise. Such rotation attacks are simulated to mimic the occurrence of truncation errors which degrade the image. Consequently, the method [7] is not robust to geometric transform (rotation and scaling) as shown in Fig. 14.

In the cropping attack, two cases are simulated here to crop the two watermarked images. The first case is cropped by 25 %, while the second case is cropped by 50 %. Because the watermark used in [7] is not permuted, the position and size of cropping can fully affect the watermark in the cropped region. In Fig. 15, there is a black region in the extracted watermark, which means the watermark information in this region is fully deleted by cropping attack. Hence, the quality of the proposed method outperforms the method [7].

4.2.2 Comparison with the spatial-domain algorithm

In order to further prove the robustness, the proposed methods are also compared with the spatial domain method [5]. In the spatial domain method, each color pixel's color quantization index, which is modified to carry the watermark in the embedding process, is encoded; however, the color gamut and quantization table are required in the extraction.





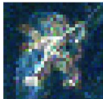

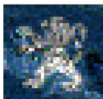
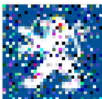
Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Scaling (4)	Lena	0.8385 / 0.7083			0.9823 / 0.9409
	Avion	0.8689 / 0.6802			0.9629 / 0.8619
Scaling (1/4)	Lena	0.5699 / 0.3251			0.8004 / 0.4835
	Avion	0.615 / 0.3476			0.8180 / 0.5337

Fig. 12 The extracted watermarks via using different methods after the scaling operation






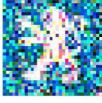
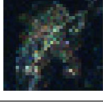

Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Blurring (0.2)	Lena	1.0000 / 1.0000			1.0000 / 1.0000
	Avion	0.5719 / 0.3143			0.9994 / 0.9995
Blurring (1.0)	Lena	0.2702 / 0.1480			0.7839 / 0.4631
	Avion	0.2702 / 0.1480			0.7488 / 0.4474

Fig. 13 The extracted watermarks via using different methods after the blurring operation

Two color images, as shown in Fig. 4(e) and (f), were used as the host image and 8-color image of Fig. 4(b) was taken as the watermark image in [5]. For fair comparison, we also use these host images and watermark image to carry out the experiment under same attack styles in [5]. Figures 16 and 17 respectively shows the comparison results using Peppers, TTU as the host image. These results reveal that the proposed algorithm is more robust. In most

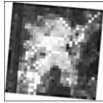

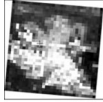
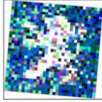
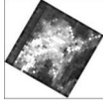
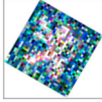
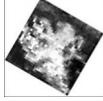
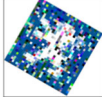
Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Rotation 5 degree	Lena	-			-
	Avion	-			-
Rotation 30 degree	Lena	-			-
	Avion	-			-

Fig. 14 The extracted watermarks via using different methods after the rotation operation









Attack	Image	Golea et al. [7]		Proposed method	
		NC / SSIM	Extracted watermark	Extracted watermark	NC / SSIM
Cropping (25%)	Lena	0.7361 / 0.6593			1.0000 / 1.0000
	Avion	0.7361 / 0.6593			1.0000 / 1.0000
Cropping (50%)	Lena	0.5331 / 0.4710			0.5702 / 0.5455
	Avion	0.4478 / 0.4832			0.5079 / 0.4718

Fig. 15 The extracted watermarks via using different methods after the cropping operation

cases, the performance of the proposed method is superior to the method in [5] except the adding Gausssian noise with larger parameter. In [5], the changed color values for various attacks have directly affected the mapping relation between the original color value and the color table, which results in the degraded quality of extracted watermark.

4.3 The execution time comparison of different algorithms

We carried out the simulations on the platform of 2.27GHZ CPU, 2.00GB RAM, Win 7, MATLAB 7.10.0 (R2010a). After many times running, as can be seen from Table 3, the average execution time of the proposed method is less than that of [7]. This means that SVD is more complex than QR decomposition, which is because the QR decomposition is an intermediate step in SVD and the time complexity for SVD is typically worse than for QR decomposition [10]. Meanwhile, the average execution time of the proposed algorithm is also less than that of [5], which is because the host image needs to be transformed to the CIE-Lab color space for the color quantization and its inverse-transformation is also required in [5]. Therefore, one should notice that the proposed algorithm requires much less number of computations.

4.4 The security of the proposed method

4.4.1 Security analysis

In this paper, in order to enhance the security and robustness of the watermarking, each component watermark is permuted by Arnold transform with private key KA_i ($i=1, 2, 3$). When the component watermark is extracted from the watermarked image, nobody can rearrange the watermark without the private key KA_i ($i=1, 2, 3$).

Attack	Chou et al. [8]		Proposed method	
	NC / SSIM	Extracted watermark	NC / SSIM	Extracted watermark
Low-pass filtering	0.539 / 0.0764		0.9608 / 0.5482	
Crop50%	0.553 / 0.2784		0.8752 / 0.9871	
Scaling 1/4	0.536 / 0.0503		0.8994 / 0.5177	
Scaling 4	0.851 / 0.2387		0.9857 / 0.6288	
Rotation 30	–		–	
JPEG 12:1	0.439 / 0.0391		0.9916 / 0.7809	
JPEG 27.5:1	0.343 / 0.0266		0.9687 / 0.4269	

Fig. 16 The watermarks extracted from the attacked Peppers images via using different methods

Moreover, the MD5-based Hash pseudo-random replacement algorithm with private key K_i ($i=1, 2, 3$) is used to select the random and non-collision embedding blocks. The feature of Hash algorithm is to map the packets of any length into a fixed length of Hash code, which is a function of information in each packet. Any change in the message will result in the change of Hash code. It should be pointed out that, in the proposed method, MD5 is applied to the specific Hash function [15], which makes it difficult for the third party to extract the watermark integrally without the keys. Hence, this proposed algorithm is of higher security.

4.4.2 Security measurement

In order to prove the security of the proposed method, we use different private keys to extract watermark. Figure 18 gives the watermark image extracted from the watermarked

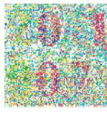







Attack	Chou et al.[8]		Proposed method	
	NC / SSIM	Extracted watermark	NC / SSIM	Extracted watermark
Low-pass filtering	0.423 / 0.0416		0.9078 / 0.4513	
Gaussian noise 4	0.982 / 0.5377		0.9389 / 0.5010	
Gaussian noises 25	0.360 / 0.1120		0.8687 / 0.4456	
Median Filter (3×3)	0.170 / 0.0833		0.3462 / 0.0152	

Fig. 17 The watermarks extracted from the attacked TTU images via using different methods

image Lena. As can be seen from the figure, the right watermark can be extracted only if the private keys K and KA are right. Moreover, the attacker without the right keys can only try all possible forms of the keys until he believes that the original image has been obtained through exhaustive manner, which is an NP-hard problem. If the attacker does not know the range of keys generation, then he needs to try the infinitely many possibility; when attacker tries wrong keys, he will obtain an image that no actual visual significance [12].

4.5 The watermark capacity analysis of the proposed method

In this paper, the 24-bit 32×32 color image is embedded into the 24-bit 512×512 color host image. The proposed method and Golea et al. [7] have the same watermark capacity. The watermark capacity of Chou et al. [5] can achieve 0.48bpp (bit per pixel) that is more than that of [7] or our method. Since the watermarking capacity, invisibility and robustness are contradict, the watermarking capacity of the proposed method is acceptable in the premise of ensuring the watermarking invisibility and robustness.

Table 3 The comparison of execution time between different methods (Second)

Method	Embedding time	Extraction time	Total time
Golea et al.[7]	1.909066	0.905951	2.815017
Chou et al.[5]	1.406568	1.105751	2.512319
Proposed method	0.829863	0.651540	1.481403



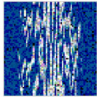
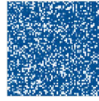
Arnold key KA	Right	Wrong	Right	Wrong
Hash key K	Right	Right	Wrong	Wrong
Extracted watermark				

Fig. 18 The extracted watermark with different keys

5 Conclusions

In this paper, a double color image watermarking scheme has been proposed. The strong correlation, between the second row first column coefficient $q_{2,1}$ and the third row first column coefficient $q_{3,1}$ in the unitary matrix Q of QR decomposition, has been utilized to embed and extract watermark. Watermark invisibility has been achieved by the presented compensatory method in R matrix. Watermark robustness has been ensured by coefficients $q_{2,1}$ and $q_{3,1}$ in the unitary matrix Q . Watermark security has been enhanced by the Arnold transform and the MD5-based Hash pseudo-random replacement algorithm with different private keys. Experimental results have shown that this proposed algorithm not only attains higher invisibility of watermarking, but also has stronger robustness in the various distortion operations. On-going works is to improve this watermarking scheme more robust to add Gaussian noise and extend that to color video watermarking.

Acknowledgments The research was partially supported by NNSF from China (61074041, 61170161), the ‘Twelve Five-Year’ plan major projects supported by National Science and Technology Committee (2011BAD20B01) and the Plan Project of Shandong Province Science and Technology Development Committee (2011YD01079). The authors would like to thank anonymous referees for their valuable comments and suggestions which lead to substantial improvements of this paper.

References

1. Ahn CJ (2008) Parallel detection algorithm using multiple QR decompositions with permuted channel matrix for SDM/OFDM. *IEEE Trans Veh Technol* 57(4):2578–2582
2. Bhatnagar G, Wu QM, Raman B (2012) A new robust adjustable logo watermarking scheme. *Comput Secur* 31(1):40–58
3. Chen W, Quan C, Tay CJ (2009) Optical color image encryption based on Arnold transform and interference method. *Opt Commun* 282(18):3680–3685
4. Chen LF, Zhao DM, Ge F (2010) Gray images embedded in a color image and encrypted with FRFT and region shift encoding methods. *Opt Commun* 283(10):2043–2049
5. Chou CH, Wu TL (2003) Embedding color watermarks in color images. *EURASIP J Appl Signal Process* 2003(1):32–40
6. Findik O, Babaoglu I, Ülker E (2011) A color image watermarking scheme based on artificial immune recognition system. *Expert Syst Appl* 38(3):1942–1946
7. Golea NEH, Seghir R, Benid R (2010) A bind RGB color image watermarking based on singular value decomposition. 2010 IEEE/ACS International Conference on Computer Systems and Applications, pp. 1–5
8. Li XH, Fan H (2000) QR factorization based blind channel identification and equalization with second-order statistics. *IEEE Trans Signal Process* 48(1):60–69

9. Mao L, Fan YY, Wang HQ, Lv GY (2011) Fractal and neural networks based watermark identification. *Multimedia Tools Appl* 52(1):201–219
10. Moor BD, Dooren PV (1992) Generalizations of the singular value and QR decompositions. *SIAM Matrix Anal App* 13(4):993–1014
11. Pei SC, Liu HH, Liu TJ, Liu KH (2010) Color image watermarking using SVD. 2010 I.E. International Conference on Multimedia and Expo (ICME), pp. 122–126
12. Rachlin Y, Baron D (2008) The secrecy of compressed sensing measurements. In: 2008 Proceedings of the 46th Annual Allerton Conference on Communication, Control and Computing, pp. 813–817
13. Rastegar S, Namazi F, Yaghmaie K, Aliabadian A (2011) Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEU Int J Electron Commun* 65(7):658–663
14. Rawat S, Raman B (2010) A new robust watermarking scheme for color images, 2010 I.E. 2nd International Advance Computing Conference, pp. 206–209
15. Rivest RL (April 1992) The MD5 message digest algorithm. Internet RFC(1321)
16. Song W, Hou JJ, Li ZH, Huang L (2011) Chaotic system and QR factorization based robust digital image watermarking algorithm. *J Cent South Univ Technol* 18(1):116–124
17. Su Q, Niu Y, Liu X, Zhu Y (2012) A blind dual color images watermarking based on IWT and state coding. *Opt Commun* 285(7):1717–1724
18. Thorat CG, Jadhav BD (2010) A blind digital watermark technique for color image based on integer wavelet transform and SIFT. *Procedia Comput Sci* 2(9):236–241
19. Tsolis DK, Sioutas S, Papatheodorou TS (2010) A multimedia application for watermarking digital images based on a content based image retrieval technique. *Multimedia Tools Appl* 47(3):581–597
20. University of Granada, Computer Vision Group. CVG-UGR Image Database. [2012-10-22]. <http://decsai.ugr.es/cvg/dbimagenes/c512.php>
21. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* 13(4):600–612
22. Xing Y, Tan J (2007) A color watermarking scheme based on block-SVD and Arnold transformation. 2007 I.E. Second Workshop on Digital Media and its Application in Museum and Heritage, pp.3–8
23. Yashar N, Saied HK (2010) Fast watermarking based on QR decomposition in Wavelet domain. 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.127–130
24. Yin CQ, Li L, Lv AQ, Qu L (2007) Color image watermarking algorithm based on DWT-SVD. 2007 I.E. International Conference on Automation and Logistics, pp. 2607–2611
25. Zhang Y, Lin LC, Li QS, Jiang ZT (200) A blind watermarking algorithm based on block DCT for dual color image 2009 Second International Symposium on Electronic Commerce and Security, pp. 213–217



Qingtang Su received the Master Degree of Engineering from the School of Information and Electronic Engineering, Kunming University of Science and Technology, Kunming, China, in 2005, and is currently pursuing the Ph.D. degree in the School of Information Science and Engineering, East China University of Science and Technology, Shanghai, China. He is working as an instructor in Department Information and Electric Engineering of LuDong University, Yantai, China. His research interests include image processing and information hiding.



Yugang Niu received the B.Sc. degree from Hebei Normal University, Shijiazhuang, China, in 1986, and the M.Sc. and Ph.D. degrees from the Nanjing University of Science & Technology, Nanjing, China, in 1992 and 2001, respectively. His postdoctoral research was carried out in the East China University of Science & Technology, Shanghai, China, between 2001 and 2003. In 2003, He joined the School of Information Science & Engineering, East China University of Science & Technology, where he is currently a Professor and the vice dean. He is now serving as an Associate Editor for IET Control Theory & Applications, International Journal of Systems Science, and the Conference Editorial Board of the IEEE Control Systems Society. His research interests include sliding mode control, stochastic systems, network congestion control, and wireless sensor network.



Hailin Zou is a professor and the dean of Department Information and Electric Engineering of LuDong University, YanTai, China. He received the Ph.D. degree in Electrical Engineering from China University of Mining & Technology, Beijing. His major research interests include wavelets theory and its applications, ground penetrating radar signal processing, data fusion technology and intelligent processing systems.



Yongsheng Zhao received the Master Degree of Engineering from Dalian University of Technology, Dalian, China, in 2007. He is working as a professor in Department Information and Electric Engineering of LuDong University, YanTai, China. His current research interest focuses on digital watermarking and image processing, algorithm analysis and design.



Tao Yao received the Master Degree of Engineering from WuHan University of Technology University, Wuhan, China, in 2006. He is working as an instructor in Department Information and Electric Engineering of LuDong University, Yantai, China. His current research interest focuses on digital watermarking and image processing.