

# An improved color image watermarking algorithm based on QR decomposition

Qingtang Su<sup>1</sup> · Gang Wang<sup>1</sup> · Xiaofeng Zhang<sup>1</sup> ·  
Gaohuan Lv<sup>1</sup> · Beijing Chen<sup>2</sup>

Received: 28 April 2015 / Revised: 24 September 2015 / Accepted: 9 November 2015 /  
Published online: 18 November 2015  
© Springer Science+Business Media New York 2015

**Abstract** Most of the existing color image watermarking schemes use binary or grayscale image as watermark, and many of them belong to non-blind watermarking methods. In this paper, an improved color image watermarking algorithm based on QR decomposition is proposed to embed color watermark image into color host image. For embedding watermark, the 24-bits color host image is divided into non-overlapping  $3 \times 3$  pixel blocks and each pixel block is decomposed by QR decomposition, and the 24-bits color watermark image is embedded into the color host image by modifying the relation between the second row first column coefficient and the third row first column coefficient of the orthogonal matrix  $Q$ . For extracting watermark, only the watermarked image is needed. Experimental results show that the proposed color image scheme not only has better watermark performance such as invisibility, robustness, security, capacity, and computation complexity, but also overcomes the false-positive detection problem.

**Keywords** Color watermark image · Matrix decomposition · Orthogonal matrix · Robustness

## 1 Introduction

With the rapid development of computer networks and multimedia technology, humans can easily access or distribute any multimedia data from networks. Hence, multimedia security including illegal copying, tampering, modifying digital copyright etc., has been the focal point of considerable research activity in the last two decades. For solving the problem of copyright protection, digital watermarking technique has been considered as a powerful method [1, 8].

---

✉ Qingtang Su  
sdytsqt@163.com

<sup>1</sup> School of Information Science and Engineering, Ludong University, 264025 Shandong, China

<sup>2</sup> School of Computer & Software, Nanjing University of Information Science & Technology, 210044 Nanjing, China

The main goal of image watermarking is to hide some important information into a host image. The important information includes pseudo random sequence, binary image, grayscale image and color image etc. In the field of image watermarking, researchers have been mainly focusing on grayscale watermarking technique so far, but color image watermark is an important challenge since the color image has more information than the grayscale image or binary image. In widespread multimedia applications, color images are the basic component of multimedia system [13]. Compared with the method of embedding binary or gray images into color image [7, 9, 16], the double color watermarking, i.e., embedding color watermark images into color host image [2, 4, 6, 10], not only has the features of more information and higher fidelity, but also can solve the copyright problems for some corporations which use the unique identifiable color logo as corporation mark.

Among the existing dual color image watermarking schemes, a blind color image watermarking was proposed based on singular value decomposition (SVD) in [6], in which one or more singular values must be modified to keep the order of singular values, which will degrade the quality of the watermarked image. Chou et al. [4] proposed a spatial-domain color image watermarking scheme by the quantization indices of the color host image in the uniform color space, unfortunately the robustness of the color watermark was weaker since this method was based on spatial-domain which has the common feature of lower robustness. Another watermarking method was proposed by Yin et al. [20], in which the singular values of original watermark were required to extract the embedded singular value, and the  $U$  and  $V$  orthogonal matrices of original watermark were also needed to recover the watermark. This method belongs to non-blind watermarking and causes the false-positive detection problem.

Since the QR decomposition is the major intermediate step in SVD, the feature highlights the use of QR decomposition in digital watermarking and a few of methods have been proposed in [11, 19]. Yashar et al. [19] proposed to modify coefficient for embedding watermark bit in the first row of  $R$  matrix after each  $8 \times 8$  block based on QR decomposition. In [11], a  $32 \times 32$  binary image was embedded into the  $512 \times 512$  host image by modifying the elements in the  $Q$  matrix. The common feature in [11, 19] was to use binary image as the watermark.

There are two disadvantages in the aforementioned schemes, e.g., the scheme may be non-blind watermarking method, or the watermark image may be binary or grayscale image. In our previous work [14], the color digital watermark information was embedded into the  $4 \times 4$  block of the color host image, that is, eight pixel values will be modified when embedding one watermark bit, which means the watermark invisibility will be affected. To overcome these drawbacks, a new double color image blind watermarking scheme based on QR decomposition is proposed in this paper. All elements in the first column of orthogonal matrix  $Q$  are very near. The smaller the difference between any two elements in the first column of orthogonal matrix  $Q$ , the smaller the modification for embedding watermark in the first column, which is helpful to improve the watermark invisibility. We use the similarity between  $q_{2,1}$  and  $q_{3,1}$  of  $Q$  matrix after performing QR decomposition on  $3 \times 3$  pixels matrix to represent one kind of embedded watermark information. Hence, the number of the modified pixels will be reduced and the invisibility and robustness of watermark will be better than performing QR decomposition on  $4 \times 4$  pixels matrix. Especially, the false-positive detection problem like in SVD-based algorithm will be overcome since all information of color image watermark can be embedded into the host image. The experimental results show that the proposed scheme can

obtain better invisibility and stronger robustness against many common image processing attacks, and the comparison with the related algorithms also reveals the higher performance of the proposed algorithm.

The rest of this paper is organized as follows. Section 2 describes the QR decomposition theory and its special features, and analyzes the proposed visual compensation method. Section 3 introduces the details of the watermark embedding procedure. Section 4 contains the description of our watermark extraction procedure. Section 5 gives the experimental results. Finally, Section 6 concludes this presentation.

## 2 Methodology

### 2.1 QR decomposition

The QR decomposition, which is a type of matrix decomposition, was formally introduced in [5], and its detailed definition was given as follows.

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

where  $R$  is an  $n \times n$  upper triangular matrix (also called right triangular matrix) and  $Q$  is an  $n \times n$  orthogonal matrix (its columns are orthogonal unit vector).

For example, suppose one matrix  $A$  of size  $3 \times 3$  as follows

$$A = \begin{bmatrix} 255 & 255 & 252 \\ 254 & 251 & 244 \\ 254 & 247 & 230 \end{bmatrix}$$

Using Eq. (1), its upper triangular matrix  $R$  and orthogonal matrix  $Q$  can be obtained as follows

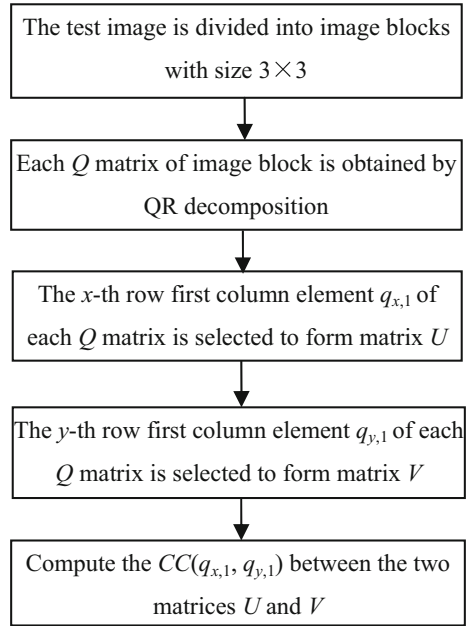
$$R = \begin{bmatrix} 440.5190 & 434.7531 & 419.1783 \\ 0 & 4.9753 & 15.0644 \\ 0 & 0 & 1.6234 \end{bmatrix}, Q = \begin{bmatrix} 0.5789 & 0.6708 & -0.4636 \\ 0.5766 & 0.0652 & 0.8144 \\ 0.5766 & -0.7387 & -0.3490 \end{bmatrix}$$

### 2.2 The special feature in unitary matrix $Q$

As can be seen from the above orthogonal matrix  $Q$ , all elements in the first column of orthogonal matrix  $Q$  are very near. The smaller the difference between any two elements in the first column of orthogonal matrix  $Q$ , the smaller the modification for embedding watermark in the first column, which is helpful to improve the watermark invisibility. In order to select better embedding elements in the first column of  $Q$  matrix on  $3 \times 3$  image block, as shown in Fig. 1, we adopt the following steps to do experiment with many standard images from CVG-UGR image database [15].

- Step 1: The test image is divided into image blocks with size  $3 \times 3$ .
- Step 2: Each image block is decomposed by QR decomposition, and its  $Q$  matrix is obtained.
- Step 3: Matrix  $U_x$  is composed by the  $x$ -th row first column element  $q_{x,1}$  of each  $Q$  matrix, where the size of matrix  $U_x$  is  $m \times n$ , and  $x=1,2,3$  respectively.

**Fig. 1** Compute the Correlation Coefficient (CC) between different elements in the first column of orthogonal matrix  $Q$



- Step 4: Matrix  $V_y$  is composed by the  $y$ -th row first column element  $q_{y,1}$  of each  $Q$  matrix, where the size of matrix  $V_y$  is  $m \times n$ ,  $y=1,2,3$  respectively, and  $y \neq x$ .
- Step 5: Compute the Correlation Coefficient (CC) between the two matrices  $U_x$  and  $V_y$  by the Eq.(2) as follows.

$$CC(q_{x,1}, q_{y,1}) = \min \left( \frac{\sum_{i=1}^n \sum_{j=1}^m U_x(i, j) V_y(i, j)}{\sqrt{\sum_{i=1}^n \sum_{j=1}^m U_x^2(i, j)}}, \frac{\sum_{i=1}^n \sum_{j=1}^m U_x(i, j) \sum_{i=1}^n \sum_{j=1}^m V_y(i, j)}{\sqrt{\sum_{i=1}^n \sum_{j=1}^m V_y^2(i, j)}} \right) \tag{2}$$

where  $m$  and  $n$  are the sizes of the  $U_x$  matrix or  $V_y$  matrix.

- Step 6: Repeat the abovementioned steps to calculate  $CC(q_{1,1}, q_{2,1})$ ,  $CC(q_{1,1}, q_{3,1})$ ,  $CC(q_{2,1}, q_{3,1})$ .

As can be seen from Table 1, the average  $CC(q_{2,1}, q_{3,1})$  value of many standard test images is 0.9746, which shows  $q_{2,1}$  and  $q_{3,1}$  are the closest elements in the first column of  $3 \times 3$  matrix  $Q$ , that is, the difference value between the two elements is very small, which means to slightly modify the two elements can represent one kind of watermark bit ‘1’ or ‘0’. Since the image visual quality will be inevitably affected when modifying  $q_{2,1}$  and  $q_{3,1}$  to embed watermark, the compensation principle proposed in our previous work [14] is used to decrease the negative affection.

**Table 1** The CC values of different elements in first column of  $Q$  matrix after QR decomposition

Image	$CC(q_{1,1},q_{2,1})$	$CC(q_{1,1},q_{3,1})$	$CC(q_{2,1},q_{3,1})$
Lena	0.9891	0.9867	0.9899
Peppers	0.9438	0.9322	0.9708
F16	0.9916	0.9886	0.9917
Baboon	0.9511	0.9424	0.9548
House	0.9973	0.9964	0.9978
Bear	0.8539	0.8388	0.9284
Kid	0.9879	0.9821	0.9891
Couple	0.9010	0.8795	0.9408
Sailboat	0.9873	0.9840	0.9883
Barbara	0.9825	0.9793	0.9844
TTU	0.9833	0.9749	0.9844
Average	0.9608	0.9532	0.9746

## 2.3 The proposed watermarking scheme

In this paper, we propose a new double color image blind watermarking scheme based on QR decomposition, which includes the watermark embedding scheme and watermark extraction scheme.

### 2.3.1 Watermark embedding scheme

In the embedding process, the color watermark image is transformed to binary sequence at first. Then, the host color image is divided into non-overlapping block. Finally, the QR decomposition is performed on the image block and the watermark is embedded into  $Q$  matrix. 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 proposed watermark embedding scheme can be summarized as follows.

Step 1: Transforming the color watermark image to binary formation

Firstly, the original color watermark image  $W$  is also divided into three components R, G, B by dimension-reduction treatment. Then, the component watermarks are obtained corresponding to the R, G and B component, respectively. In order to enhance the security and the robustness of the embedded watermark, each component watermark is permuted by Arnold transform with private key  $KA_i$  ( $i=1, 2, 3$ ) [3, 18]. Arnold transform is also called Cat Face transfer, and it is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (3)$$

where  $(x,y)$  is the pixel of the component watermark image,  $(x',y')$  is the pixel of the component watermark image after permuting,  $N$  is order of watermark image matrix. Since the Arnold transform is periodic, the number of permuting can be considered as the key  $KA_i$  ( $i=1, 2, 3$ ) to enhance the security.

After that, each pixel value is converted to 8-bit binary sequence. Finally, combining all 8-bit binary sequence to form the binary component watermark  $W_i$  ( $i=1, 2, 3$ ).

Step 2: Processing the host image

When more information is embedded into the color host image  $H$ , it is divided into three components  $H_i$  ( $i=1, 2, 3$ ), which represent the R, G and B component respectively, and each component image is divided into  $3 \times 3$  non-overlapping blocks.

Step 3: Selecting the embedding blocks

In order to improve the watermark invisibility and robustness of the cropping attack, all embedded watermark will be uniformly distributed. According to the modified block numbers, the method of embedding interval selection based on private key  $K$  is adopted in this paper. The non-overlapping blocks  $1, 1+K, 1+2 \times K, \dots, 1+n \times K$  in the odd lines and the non-overlapping blocks  $2, 2+K, 2+2 \times K, \dots, 2+n \times K$  in the even lines are selected to embed watermark, where  $n$  is decided by the size of the host image ( $M \times M$ ), the size of the pixel block ( $B \times B$ ) and the private key  $K$ , that is,  $n = \text{floor}(M/(B * K))$ . The private key  $K$  can not only prevent the modified block from getting together, but also improve the invisibility of watermark, but ensure the security of watermark since the attacker cannot know the accurate position of embedding watermark and extracting watermark without the private key  $K$ .

Step 4: Embedding watermark to the orthogonal matrix  $Q$

According to Eq. (1), each selected block is decomposed to obtain the orthogonal matrix  $Q$  by QR decomposition. The elements  $q_{2,1}$  and  $q_{3,1}$  in the first column of  $Q$  matrix will be modified as  $q'_{2,1}$  and  $q'_{3,1}$  by the following rules in Eqs. (4) and (5), respectively.

$$\text{if } w = 1 \text{ and } q_{2,1} - q_{3,1} < (2 * T) / 3, \text{ then } \begin{cases} q'_{2,1} = q_{avg} + T / 2 \\ q'_{3,1} = q_{avg} - T / 2 \end{cases} \quad (4)$$

$$\text{if } w = 0 \text{ and } q_{3,1} - q_{2,1} \leq (2 * T) / 3, \text{ then } \begin{cases} q'_{2,1} = q_{avg} - T / 2 \\ q'_{3,1} = q_{avg} + T / 2 \end{cases} \quad (5)$$

where  $w$  indicates the embedded binary watermark information bit and  $q_{avg} = (q_{2,1} + q_{3,1}) / 2$ . It should be noted that the proposed method is similar to the method in our previous work [14], but the color digital watermark information was embedded into the  $3 \times 3$  block of the host image, that is, only six pixel values instead of eight pixel values will be modified in the new proposed method.

Step 5: Obtaining the watermarked image block

The inverse QR operation is performed to obtain the watermarked image block according to Eq. (6).

$$A' = Q' \times R \quad (6)$$

Step 6: Repetition

Repeating steps 4–5 until all watermark bits are embedded in the host image. Finally, the watermarked R, G, B components are reconstructed to obtain the watermarked image  $H'$ .

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

### 2.3.2 Watermark extraction scheme

In this paper, since the original host image and watermark image are not needed in the procedure, the watermark extraction procedure belongs to blind extraction method. The watermark extraction steps are described as follows.

Step 1: Dividing the watermarked image

The watermarked image  $H'$  is divided into R, G, B component images, and then each component is further divided into watermarked blocks with size of  $3 \times 3$  pixels, respectively.

Step 2: Selecting the watermarked block

The method of embedding interval selection based on private key  $K$  is used to select the watermarked blocks.

Step 3: Extracting watermark

Each watermarked block is decomposed by QR decomposition and its unitary matrix  $Q'$  is obtained. 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. (7).

$$w' = \begin{cases} 1, & \text{if } q'_{2,1} \geq q'_{3,1} \\ 0, & \text{if } q'_{2,1} < q'_{3,1} \end{cases} \quad (7)$$

Step 4: Repetition

The above steps 2–3 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 5: 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.

## 3 Simulation results

### 3.1 Metrics

The main performance of the watermarking methods under consideration is investigated by measuring their invisibility, robustness, execution time, security and embedding capacity. For proving the watermarking performance of the proposed method, all 24-bit  $512 \times 512$  color images in the CVG-UGR image database are used as the host images [15], and two 24-bit  $32 \times 32$  color images showed in Fig. 2a and (b) are used as original watermarks.

In order to evaluate the invisibility capability, not only is the peak signal-to-noise ratio (*PSNR*) used in this paper, but also the structural similarity (*SSIM*) index as a new method is also used to measure the similarity between the original color image *I* and the watermarked image *I'*.

*PSNR* as a good rule for measuring the watermark invisibility [12, 18], it is given by

$$PSNR = 10\lg \frac{255^2}{MSE} \tag{8}$$

where *MSE* is the mean square error given by

$$MSE = \frac{1}{3MN} \sum_{j=1}^3 \sum_{x=1}^m \sum_{y=1}^n [I(x,y,j) - I'(x,y,j)]^2 \tag{9}$$

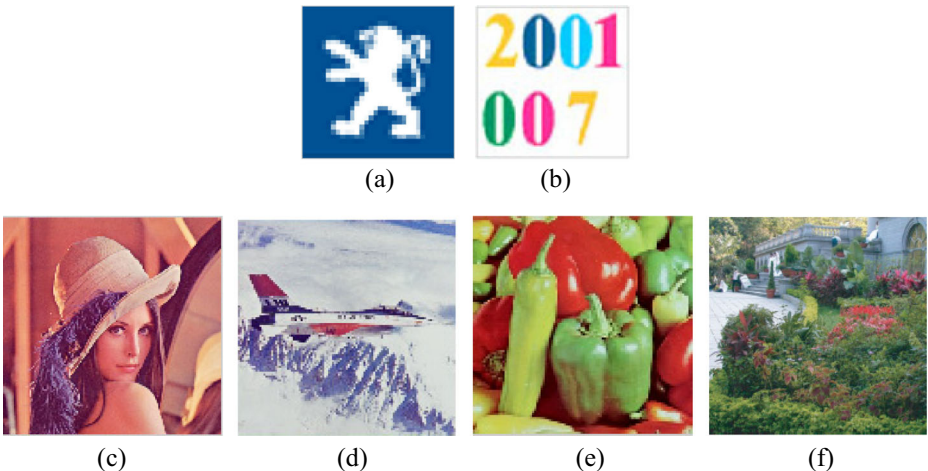
where, *I*(*x*,*y*,*j*), *I'*(*x*,*y*,*j*) present the value of pixel (*x*, *y*) in component *j* of the original image and the watermarked one, and *m*, *n* denote the width and height of the host images, respectively.

Moreover, the *SSIM* developed by Wang et al. [17] was considered to be correlated with the quality perception of the human visual system (*HVS*). The *SSIM* is designed by modeling image distortion that combines three factors: loss of correlation, luminance distortion and contrast distortion. The *SSIM* is defined as:

$$SSIM(I, I') = l(I, I')c(I, I')s(I, I') \tag{10}$$

where

$$\begin{cases} l(I, I') = (2\mu_I\mu_{I'} + C_1) / (\mu_I^2 + \mu_{I'}^2 + C_1) \\ c(I, I') = (2\sigma_I\sigma_{I'} + C_2) / (\sigma_I^2 + \sigma_{I'}^2 + C_2) \\ s(I, I') = (\sigma_{II'} + C_3) / (\sigma_I\sigma_{I'} + C_3) \end{cases} \tag{11}$$



**Fig. 2** Original watermark images: **a** PEUGEOT logo, **b** 8-color image; Original host images: **c** Lena, **d** Avion, **e** Peppers, **f** TTU



The first term in Eq. (10) is the luminance comparison function which measures the closeness of the two images’ mean luminance ( $\mu_I$  and  $\mu_{I'}$ ). This factor is maximal and equal to 1 only if  $\mu_I = \mu_{I'}$ . The second term is the contrast comparison function which measures the closeness of the contrast of the two images. Here the contrast is measured by the standard deviation  $\sigma_I$  and  $\sigma_{I'}$ . This term is maximal and equal to 1 only if  $\sigma_I = \sigma_{I'}$ . The third term is the structure comparison function which measures the correlation coefficient between the two images  $I$  and  $I'$ . Note that  $\sigma_{II'}$  is the covariance between  $I$  and  $I'$ . The positive values of the SSIM index are in  $[0, 1]$ . A value of 0 means no correlation between images, and 1 means that  $I=I'$ . The positive constants  $C_1, C_2$  and  $C_3$  are used to avoid a null denominator.

Besides, in order to measure the robustness of the watermark, we use the normalized correlation (NC) between the original watermark  $W$  and the extracted watermark  $W'$ , which is denoted as follows.

$$NC = \frac{\sum_{j=1}^3 \sum_{x=1}^P \sum_{y=1}^Q (W(x, y, j) \times W'(x, y, j))}{\sqrt{\sum_{j=1}^3 \sum_{x=1}^P \sum_{y=1}^Q W(x, y, j)^2} \sqrt{\sum_{j=1}^3 \sum_{x=1}^P \sum_{y=1}^Q W'(x, y, j)^2}} \tag{12}$$

where  $W(x,y,j), W'(x,y,j)$  present the value of pixel  $(x, y)$  in component  $j$  of the original watermark and the extracted one, and  $P, Q$  denote the row and the column size of the original watermark image, respectively.

Generally, a larger PSNR or SSIM means that the watermarking method has higher invisibility. A higher NC reveals that the watermarking method has more robustness. Table 2 not only shows the watermark invisibility (reflected by average PSNR values) of the embedded host images, but also shows the robustness (measured by the average NC values) of extracted watermark after resisting many attacks with different threshold values  $T$ . The bigger the threshold  $T$  is, the worse the watermark invisibility is and the better the watermark robustness is, vice verse. Considering the tradeoff between the invisibility and robustness of watermarking, the threshold value  $T$  is set to 0.08.

### 3.2 Experiment result

#### 3.2.1 The result of invisibility

For relatively fair comparison, the host images Fig. 2c and d used in [6, 11] and the host images Fig. 2e and f used in [4] are adopted in this experiment. When the different watermark images in Fig. 2a and b were respectively embedded into all  $512 \times 512$  color images of the

**Table 2** The PSNR and NC values with different threshold values  $T$

$T$	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
PSNR(dB)	41.8304	41.2322	40.8443	39.4248	38.1350	36.9701	35.9243	35.0733	34.1043	33.3073
SSIM	0.9779	0.9654	0.9566	0.9559	0.9538	0.9537	0.9514	0.9495	0.9479	0.9422
NC	0.9771	0.9862	0.9894	0.9913	0.9922	0.9929	0.9931	0.9933	0.9933	0.9934

CVG-UGR image database, Fig. 3 not only gives the watermarked color images and their SSIM values, but also shows the extracted watermark and their NC and SSIM values.

### 3.2.2 The result of robustness

In this sub-section, we give the extracted results from the attacked images Lena and F16 after the watermark of Fig. 2a was embedded into.

In the application of real life, storage and transmission of digital data are common operation. For this purpose, a lossy coding operation is often performed on the data to reduce the memory and increase efficiency. Since JPEG and JPEG 2000 standards are widely used formats in image compression, the proposed watermarking system is tested to investigate the robustness of the proposed watermarking system with JPEG and JPEG 2000 standards. JPEG is an image compression standard that supports lossy and lossless compression of grayscale as well as color images. In this experiment, the watermarked images are compressed with different compression factors from 10 to 100 increasing in steps of 10. Figure 4 gives the part of the results. Compared with the methods [6, 14], the proposed scheme achieves better robustness against the JPEG compression.

Meanwhile, JPEG 2000 was developed by the Joint Photographic Expert Group 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 to 10 increasing in steps of 1. Figure 5 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 degrade the watermarked images. Figure 6 shows the quantitative results in terms of the NC, SSIM and visual-perception after adding Salt & peppers noise, respectively. Moreover, the Gaussian noising is also added to corrupt the watermarked images, in which normally distributed noise with mean 0 and standard deviation  $\sigma$  was added to each of the watermarked images. The standard deviation  $\sigma$  of Gaussian parameter is set from 0.1 to 1.0, respectively. The extracted watermarks, NC values and SSIM values are shown in Fig. 7.

In this experiment, the Butterworth low-pass filters are used to corrupt the watermarked images with cut-off frequency 100, and order from 1 to 10, respectively. Figure 8 shows the NC values, SSIM values and visual-perception results after low-pass filters attack.

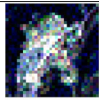











In the procedure of sharpening, the radii are 0.2 and 1.0, respectively. Figure 9 gives the result of sharpening attack. In the blurring attacks, two cases are simulated here to degrade the two watermarked images. The radius in the first case is 0.2, while the second case is 1.0. Figure 10 exhibits the results of visual comparison and quantitative values. It is evident that the proposed method is more robust than the methods [6, 14] in this case.

In addition, scaling operation is performed on the watermarked image from 25 to 800 %, respectively. Figure 11 shows the quantitative results and visual-perception results for the scaling with 400 % and 25 %, respectively. In the cropping attack, two cases are simulated here to crop the two watermarked images. The first case is cropped by 25 %, and the second case is cropped by 50 %. Figure 12 shows the results of anti-cropping attack.

In order to further prove the robustness, the proposed methods are also compared with the spatial domain method [4]. Two color images, as shown in Fig. 2e and f, were used as the host


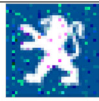
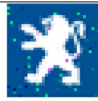









Method	Golea et al. [6]	Song et al.[11]	Su et al.[14]	Proposed method
Watermarked image (PSNR/SSIM)	 39.4358 / 0.9935	 22.5616 / 0.6332	 35.2881 / 0.9589	 35.3414 / 0.9717
Extracted watermark (NC / SSIM)	 0.9937 / 0.9935	 0.8032 / 0.4282	 1.0000 / 0.9999	 1.0000 / 1.0000
Watermarked image (PSNR/SSIM)	 38.3922 / 0.9940	 20.4106 / 0.5411	 32.0662 / 0.9256	 32.4966 / 0.9447
Extracted watermark (NC / SSIM)	 0.9949 / 0.9941	 0.8034 / 0.4282	 1.0000 / 1.0000	 1.0000 / 1.0000
Watermarked image (PSNR/SSIM)	 34.3367 / 0.9279	 23.2864 / 0.7111	 35.8301 / 0.9682	 36.4253 / 0.9783
Extracted watermark (NC / SSIM)	 0.9801 / 0.9298	 0.9293 / 0.3630	 0.9979 / 0.9894	 0.9997 / 0.9940
Watermarked image (PSNR/SSIM)	 35.7817 / 0.9970	 23.6139 / 0.8241	 34.0188 / 0.9854	 35.7281 / 0.9928
Extracted watermark (NC / SSIM)	 0.9919 / 0.9969	 0.9262 / 0.3632	 1.0000 / 1.0000	 1.0000 / 1.0000

Fig. 3 The watermarked color images and the extracted watermarks without any attacks













Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
JPEG 30	Lena	 0.6531 / 0.1861	 0.7530 / 0.3502	 0.7552 / 0.3531
	Avion	 0.8204 / 0.2877	 0.8353 / 0.4975	 0.8488 / 0.5208
JPEG 90	Lena	 0.9712 / 0.4888	 0.9827 / 0.8838	 0.9886 / 0.9024
	Avion	 0.9760 / 0.6806	 0.9910 / 0.9591	 0.9957 / 0.9731

**Fig. 4** The extracted watermarks via using different methods after the JPEG compression operation

image and 8-color image of Fig. 2b was taken as the watermark image in [4]. For fair comparison, we also use these host images and watermark image to carry out the experiment under the same attack styles in [4]. Figures 13 and 14 show the comparison results using Peppers, TTU as the host image respectively.

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
JPEG 2000 (5:1)	Lena	 0.9390 / 0.4097	 0.9836 / 0.9271	 0.9938 / 0.9757
	Avion	 0.9375 / 0.5951	 0.9936 / 0.9834	 0.9977 / 0.9872
JPEG 2000 (10:1)	Lena	 0.8071 / 0.3533	 0.9026 / 0.5807	 0.9564 / 0.8057
	Avion	 0.7951 / 0.3364	 0.9716 / 0.8755	 0.9801 / 0.9023













**Fig. 5** The extracted watermarks via using different methods after the JPEG 2000 compression operation

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Salt & Peppers noise (0.02)	Lena	 0.5698 / 0.3206	 0.9904 / 0.8824	 0.9960 / 0.9071
	Avion	 0.5279 / 0.2504	 0.9846 / 0.9089	 0.9883 / 0.8930
Salt & Peppers noise (0.10)	Lena	 0.3977 / 0.4047	 0.9362 / 0.6931	 0.9428 / 0.6771
	Avion	 0.3968 / 0.3867	 0.9282 / 0.6974	 0.9333 / 0.6614

**Fig. 6** The extracted watermarks via using different methods after the salt & peppers noising operation

### 3.2.3 The result of execution time

In these experiments, a laptop computer with a duo Intel CPU at 2.27GHZ, 2.00GB RAM, Win 7, MATLAB 7.10.0 (R2010a) is used as the computing platform. The embedding time

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Gaussian noise (0.1)	Lena	 0.8600 / 0.3151	 0.8558 / 0.4697	 0.9407 / 0.6653
	Avion	 0.8188 / 0.3296	 0.9222 / 0.6692	 0.9759 / 0.8647
Gaussian noise (0.6)	Lena	 0.3891 / 0.1334	 0.5395 / 0.0405	 0.4327 / 0.4478
	Avion	 0.39604 / 0.1782	 0.5424 / 0.0656	 0.3947 / 0.2626

**Fig. 7** The extracted watermarks via using different methods after the Gaussian noising operation

and extraction time of the proposed methods is 0.546941, 0.410019 s, respectively. Table 3 shows the comparison of execution time between different methods.

## 4 Discussion

### 4.1 Invisibility discussion

By comparison, it can be seen from Fig. 3 that Song et al. [11] based on QR decomposition could not extract good watermark and the host image is obviously modified via embedding the watermark, which cannot meet the need of watermark invisibility. Thus, this method of Song et al. [11] is not suitable for embedding color watermark image into color host image. Golea et al. [6] 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. Based upon this experiment, we draw the conclusion that the proposed method can effectively embed and extract color watermark image.

### 4.2 Robustness discussion

In this paper, various attacks such as JPEG compression, JPEG 2000 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 method [6] based on SVD and method [14] based on QR decomposition.

As can be seen from Figs. 4 and 5, the proposed scheme, compared with the methods [6, 14], achieves better robustness against the compress attacks such as JPEG compression and JPEG 2000 compression.













It is evident from Fig. 6 that the proposed method is more robust against salt & peppers noise attacks than the methods [6, 14]. However, the bigger the Gaussian parameter is, the weaker the robustness is in Fig. 7. Hence, it must be further improved in the future work. Relatively, the robustness of the proposed method is superior to that of other methods under adding Gaussian noising in Fig. 7.

Figure 8 shows the proposed method has better robustness against the low-pass attack. Moreover, the results of visual comparison and quantitative values given in Figs. 9 and 10 prove that the proposed method outperforms the methods [6, 14] in aspects of sharpening and blurring, respectively.

In addition, the proposed method has better robustness as respect of scaling operation and cropping in Figs. 11 and 12, respectively. Because the watermark used in [6] is not permuted,













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

Method	Embedding time	Extraction time	Total time
Golea et al.[6]	1.909066	0.905951	2.815017
Chou et al.[4]	1.406568	1.105751	2.512319
Su et al. [14]	0.829863	0.651540	1.481403
Proposed method	0.546941	0.410019	0.956960













Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Low-pass Filter (100,1)	Lena	 0.5477 / 0.4971	 0.9584 / 0.8451	 0.9765 / 0.8639
	Avion	 0.5855 / 0.4089	 0.9205 / 0.7507	 0.9476 / 0.8038
Low-pass Filter (100,3)	Lena	 0.3818 / 0.1411	 0.7987 / 0.4457	 0.8594 / 0.5465
	Avion	 0.4650 / 0.2687	 0.7779 / 0.4728	 0.8296 / 0.5800

**Fig. 8** The extracted watermarks via using different methods after the low-pass filter operation

the position and size of cropping can fully affect the watermark in the cropped region. In Fig. 12, there is a black region in the extracted watermark, which means the watermark information in this region is fully deleted by cropping attack. Moreover, the method of embedding interval selection replaces the Hash pseudo-random selection in method [14]. Hence, the quality of the proposed method outperforms that of the methods [6, 14].













Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Sharpening (0.2)	Lena	 0.93911 / 0.7705	 0.9991 / 0.9998	 1.0000 / 1.0000
	Avion	 0.9397 / 0.7708	 0.9999 / 0.9999	 1.0000 / 1.0000
Sharpening (1.0)	Lena	 0.9119 / 0.7211	 0.9974 / 0.9997	 1.0000 / 1.0000
	Avion	 0.8135 / 0.5281	 0.9917 / 0.9996	 1.0000 / 1.0000

**Fig. 9** The extracted watermarks via using different methods after the sharpening operation

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Blurring (0.2)	Lena	 1.0000 / 1.0000	 1.0000 / 1.0000	 1.0000 / 1.0000
	Avion	 0.5719 / 0.3143	 0.9994 / 0.9995	 0.9994 / 0.9968
Blurring (1.0)	Lena	 0.2702 / 0.1480	 0.7839 / 0.4631	 0.8361 / 0.4691
	Avion	 0.2702 / 0.1480	 0.7488 / 0.4474	 0.8491 / 0.5201

**Fig. 10** The extracted watermarks via using different methods after the blurring operation

It can be seen from Figs. 13 and 14 that the proposed algorithm is more robust. In most cases, the performance of the proposed method is superior to the method in [4] except adding Gaussian noise with larger parameter. In [4], 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.

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Scaling (4)	Lena	 0.8385 / 0.7083	 0.9823 / 0.9409	 1.0000 / 1.0000
	Avion	 0.8689 / 0.6802	 0.9629 / 0.8619	 1.0000 / 1.0000
Scaling (1/4)	Lena	 0.5699 / 0.3251	 0.8004 / 0.4835	 1.0000 / 1.0000
	Avion	 0.6150 / 0.3476	 0.8180 / 0.5337	 1.0000 / 1.0000

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




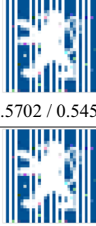








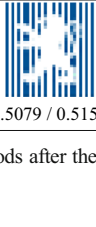

Attack	Image	Extracted watermark (NC / SSIM)		
		Golea et al. [6]	Su et al. [14]	Proposed method
Cropping (25%)	Lena	 0.7361 / 0.6593	 0.5702 / 0.5455	 0.9389 / 0.7183
	Avion	 0.7361 / 0.6593	 0.5702 / 0.5455	 0.9389 / 0.7183
Cropping (50%)	Lena	 0.4478 / 0.4832	 0.5079 / 0.5152	 0.8788 / 0.5958
	Avion	 0.4478 / 0.4832	 0.5079 / 0.5152	 0.8788 / 0.5958

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

### 4.3 Execution time discussion

As can be seen from Table 3, the average execution time of the proposed method is less than that of [6]. This means that SVD is more complex than QR decomposition because the QR decomposition is an intermediate step in SVD and the time complexity for SVD is typically worse than for QR decomposition. Meanwhile, the average execution time of the proposed algorithm is also less than that of [4] 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 [4]. The Hash pseudo-random selection used in [14] needs more time than the interval selection used in this paper. Therefore, one should notice that the proposed algorithm requires much less number of computations.

### 4.4 Security discussion

In this paper, in order to enhance the watermarking security, each component watermark is permuted by Arnold transform with private keys  $KA_i$  ( $i=1, 2, 3$ ) and the watermark embedding block is decided by the private key  $K$ . Firstly, the position of embedding or extraction based on the private key  $K$  is unknown for anybody without the right key  $K$ , which makes it difficult to extract and tamper the embedded watermark; Secondly, when the component watermark is extracted from the watermarked image, nobody can extract and rearrange the watermark without the private keys  $K$  and  $KA_i$  ( $i=1, 2, 3$ ). Kirchhoff’s criterion is often used to assess the usability of cryptograph methods and systems: all algorithms must be public, and only the key is secret. The security of our algorithm only relies on the private keys  $KA_i$  ( $i=1, 2, 3$ ) and  $K$ , which meets Kirchhoff’s criterion. Figure 15 gives the watermark image extracted from the watermarked image Lena. As can be seen from the figure, the right watermark can be extracted only if the private keys  $K$  and  $KA_i$  ( $i=1, 2, 3$ ) are right. Moreover, the attacker without the right

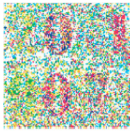



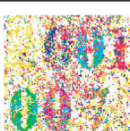


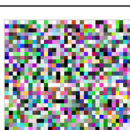
Attack	Chou et al. [4]		Proposed method	
	NC / SSIM	Extracted watermark	NC / SSIM	Extracted watermark
Low-pass filtering	0.539 / 0.0764		0.9704 / 0.6079	
Crop50%	0.553 / 0.2784		0.8733 / 0.3680	
Scaling 1/4	0.536 / 0.0503		0.8064 / 0.2618	
Scaling 4	0.851 / 0.2387		0.9892 / 0.7832	
Rotation 30	–		–	
JPEG 12:1	0.439 / 0.0391		0.9413 / 0.5171	
JPEG 27.5:1	0.343 / 0.0266		0.9205 / 0.4442	

**Fig. 13** The watermarks extracted from the attacked Peppers images via using different methods

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.

#### 4.5 Embedding capacity discussion

In this paper, the 24-bit  $32 \times 32$  color image is embedded into the 24-bit  $512 \times 512$  color host image. The proposed method and the methods [6, 14] have the same watermark capacity



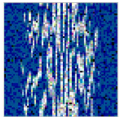

Attack	Chou et al. [4]		Proposed method	
	NC / SSIM	Extracted watermark	NC / SSIM	Extracted watermark
Low-pass filtering	0.423 / 0.0416		0.9412 / 0.5928	
Gaussian noise 4	0.982 / 0.5377		0.9379 / 0.4404	
Gaussian noises 25	0.360 / 0.1120		0.9301 / 0.5063	
Median Filter (3×3)	0.170 / 0.0833		0.4813 / 0.0160	

**Fig. 14** The watermarks extracted from the attacked TTU images via using different methods

0.03125 bpp (bit per pixel). The watermark capacity of Chou et al. [4] can achieve 0.48bpp (bit per pixel) which is more than that of others. In this proposed method, the embedding block with size 3×3 is smaller than that in [14] with size 4×4, in theory, the proposed embedding capacity will be 1.333 times of the [14]. Since the watermarking capacity, invisibility and robustness are in conflict with each other, the watermarking capacity of the proposed method is acceptable in the premise of ensuring the watermarking invisibility and robustness.

### 5 Conclusions

Based on QR decomposition, an improved color image watermarking scheme is proposed in this paper. For embedding watermark, the 24-bits color host image is divided into non-

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

**Fig. 15** The extracted watermark with different keys

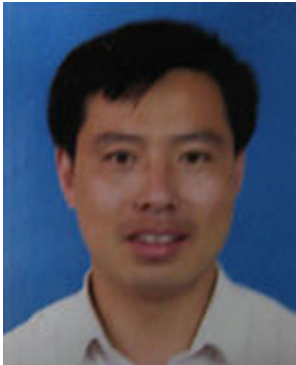
overlapping  $3 \times 3$  pixel blocks and each pixel block is decomposed by QR decomposition, and the 24-bits color watermark image is embedded into the color host image by modifying the relation between the second row first column coefficient and the third row first column coefficient of the orthogonal matrix  $Q$ . When extracting watermark, only the watermarked image is needed. Experimental results have shown that this proposed algorithm not only attains higher invisibility of watermarking, but also has stronger robustness in various distortion operations. In future, we will extend the proposed method to color video watermarking.

**Acknowledgments** The research was partially supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET), Natural Science Foundation of Shandong Province (ZR2014FM005, ZR2013FL008), Shandong Province Higher Educational Science and Technology Program (J14N20), Doctoral Foundation of Ludong University (LY2014034), Shandong Province Science and Technology Plan Projects (2014GGB01944) and Shandong Province Important Research Plan Projects (2015GSF116001). The authors would like to thank anonymous referees for their valuable comments and suggestions which lead to substantial improvements of this paper.

## References

1. An L, Gao X, Li X, Tao D, Deng C, Li J (2012) Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Trans Image Process* 21(8):3598–3611
2. Chen B, Coatrieux G, Chen G, Sun X, Coatrieux JL, Shu H (2014) Full 4-D quaternion discrete Fourier transform based watermarking for color images. *Digital Signal Process* 28(5):106–119
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. Chou CH, Wu TL (2003) Embedding color watermarks in color images. *EURASIP J Appl Signal Process* 32–40
5. De Moor B, Van Dooren P (1992) Generalizations of the singular value and QR decompositions. *SIAM J Matrix Anal Appl* 13(4):993–1014
6. Golea NEH, Seghir R, Benzid R (2010) A bind RGB color image watermarking based on singular value decomposition. *IEEE/ACS Int Conf Comput Syst Appl* 1–5
7. Kuribayashi M (2014) Simplified MAP detector for binary fingerprinting code embedded by spread spectrum watermarking scheme. *IEEE Trans Inf Forensic Secur* 9(4):610–623
8. Li XW, Kim ST (2014) An improved cellular automata-based digital image watermarking scheme combining the use of pixel-wise masking and 3D integral imaging. *Opt Commun* 319(5):45–55
9. Mao L, Fan YY, Wang HQ, Lv GY (2011) Fractal and neural networks based watermark identification. *Multimed Tools Appl* 52(1):201–219
10. Rawat S, Raman B (2010) A new robust watermarking scheme for color images. *IEEE 2nd Int Adv Comput Conf* 206–209
11. 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
12. Su Q, Niu Y, Liu X, Zhu Y (2012) Embedding color watermarks in color images based on Schur decomposition. *Opt Commun* 285(7):1792–1802
13. Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color image blind watermarking scheme based on QR decomposition. *Signal Process* 94(1):219–235
14. Su Q, Niu Y, Zou H, Zhao Y, Yao T (2014) A blind double color image watermarking algorithm based on QR decomposition. *Multimed Tools Appl* 72(1):987–1009
15. University of Granada. Computer Vision Group. CVG-UGR Image Database. [2012-10-22]. <http://decsai.ugr.es/cvg/dbimagenes/c512.php>
16. Urvoy M, Goudia D, Atrousseau F (2014) Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. *IEEE Trans Inf Forensic Secur* 9(7):1108–1119

17. 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
18. Wang X, Wang C, Yang H et al (2013) A robust blind color image watermarking in quaternion Fourier transform domain. *J Syst Softw* 86(2):255–277
19. Yashar N, Saied HK (2014) Fast and robust watermarking in still images based on QR decomposition. *Multimed Tools Appl* 72:2597–2618
20. Yin CQ, Li L, Lv AQ, Qu L (2007) Color image watermarking algorithm based on DWT-SVD. *IEEE Int Conf Autom Log* 2607–2611



**Qingtang Su** received his Master Degree of Engineering from the School of Information and Electronic Engineering, Kunming University of Science and Technology, Kunming, China, in 2005, and his Ph.D. degree in Control Science and Engineering from East China University of Science and Technology, Shanghai, China, in 2013. He is working as an associate professor in Department Information and Electric Engineering of LuDong University, Yantai, China. His research interests include image processing, information security, and etc.



**Gang Wang** received his Master Degree in Optical Engineering from University of Electronic Science and Technology of China, in 2004, and his Ph.D. degree in Optical Engineering from Nanjing University of Science and Technology, Nanjing, China, in 2007. He is working as an professor in Department Information and Electric Engineering of LuDong University, Yantai, China. His research interests include Image processing, Optical information processing, and etc.



**Xiaofeng Zhang** received his master degree from Lanzhou University of Technology in 2005, and received his Ph.D. degree from Shandong University in 2014. Now he is a lecturer in School of Information and Electrical Engineering, Ludong University, China. He has published about 30 papers in international journals and conferences, and his research interest includes medical image segmentation, pattern recognition, and etc.



**Gaohuan Lv** received his B.Sc. degree from the Qufu Normal University, Shandong, China, in 1998, and the M.Sc degree from the Chinese Academy of Engineering Physics(CAEP), Beijing, China, in 2001 and the Ph.D degree from the Shanghai Jiao Tong University, Shanghai, China, in 2013. From 2001 to 2008, he was an Engineer with the institute of electronic engineering at the CAEP, Mianyang, China, where he worked on control system and software engineering. Since 2013, he has been with the school of information and electrical engineering at the Ludong University, Yantai, China. His research interests include radar signal processing, digital image processing, ground moving target indication, and coherent optical signal processing.



**Beijing Chen** received the Ph.D. degree in Computer Science in 2011 from Southeast University, Nanjing, China. Now he is an associate professor in the School of Computer & Software, Nanjing University of Information Science & Technology, China. His research interests include color image processing, information security and pattern recognition.