Multimedia Tools and Applications (2020) 79:7491–7513
https://doi.org/10.1007/s11042-019-08423-1

A blind color image watermarking scheme with variable steps based on Schur decomposition

Decheng Liu[1] · Zihan Yuan[1] · Qingtang Su[1]

Received: 28 March 2019 / Revised: 30 September 2019 / Accepted: 1 November 2019 /
Published online: 23 December 2019

Abstract
The widespread application of the Internet makes the protection of image copyright face serious challenges. For resolving this problem, this paper designs a blind color digital image watermarking algorithm which meets the requirements of invisibility, security and robustness. The advantages of the proposed method include the following two points: 1) the proposed method uses Affine transformation with large key space to encrypt the watermark information; 2) Schur decomposition with low complexity is selected and performed on the matrix blocks in different color channels of the host image. In this proposed method, the watermark embedding and blind extraction are completed by quantizing the eigenvalues on the diagonal of the decomposed matrix with different quantization steps. Experimental results show that the proposed method not only has good invisibility, but also has high security and strong robustness.

Keywords Color digital watermarking · Schur decomposition · Affine transformation · Security

1 Introduction

With the rapid development of multimedia technology, more and more color digital images, as the main media, are emerging and spreading on the network. At the same times, many illegal behaviors, such as piracy and infringement, are occurrences commonly. Copyright protection has been widely concerned by scholars. In [7], watermarking system can ensure anti-interference and protect the copyright of digital contents by storing, transmitting and processing information. The development of copyright protection technology solution based on watermarking technology has been one of the hot spots in the field of copyright protection in the past two decades [4].

According to the difference of watermarking carrier media, the digital watermarking can be divided into image watermarking, audio watermarking, video watermarking, text watermarking and

✉ Qingtang Su
sdytsqt@163.com

[1] School of Information and Electrical Engineering, Ludong University, Yantai 264025, China

grid watermarking for 3D mesh model [14]. In image watermarking, the redundant space of the carrier image is used to hide the watermark information. When a copyright dispute occurs, the hidden information in the image can be extracted to prove the ownership of the image. At present, although the researches on image digital watermarking technology have greatly exceeded the audio and video digital watermarking technology, the research objects are mostly pseudo-random sequences, binary images or gray images with small information capacity [2, 9, 20]. For example, Chang et al. proposed a watermarking technique by using features classification forest to embed gray image into gray images [2]. A watermarking system is proposed to embed different gray images into gray images by using integer DCT domain [20]. Hsu et al. presented a robust blind image watermarking for gray images using crisscross inter-block prediction in the DCT domain [9]. That is, the methods [2, 9, 20] are applied to gray images. The color image digital watermarking technology has not been fully paid attention, and the indeed requirements of copyright protection are more and more tending to use beautiful and practical color logo as color image digital watermark.

Different detection processes of digital watermarking have great influence on the features of watermarking. Non-blind watermarking need original data or auxiliary information in the detection process, while blind watermarking do not need any original data or auxiliary information. In general, the non-blind watermark is more robust [35], but its application process is limited since it needs the help of the original data. The blind watermarking gets rid of this limitation and has stronger adaptability and wider application. For instance, Su et al. proposed a blind color image watermarking scheme based on QR decomposition using the similarities of the decomposed matrix elements [24]. Liu et al. proposed a blind double watermark authentication and copyright protection for color images [12]. Su et al. used the similarities between the matrix elements in Hessenberg matrix to realize blind detection of watermarks [21]. The above three methods can resist some image processing (such as scaling, compression, filtering, superimposed noise, sharpening, etc.), and these methods can be applied to protect the copyright of digital color image.

The frequency domain watermarking methods [16, 25, 27, 33] can enhance the robustness of watermarking, and expand the scope of its application. On the contrary, the spatial-domain watermarking method [10] is easy to implement, but its robustness is weak. For example, Karybali et al. proposed an efficient spatial-domain image watermarking via new perceptual masking and blind detection method [10]. The spatial perception mask proposed by them matches the features of HVS very well. Meanwhile, the HVS-compliant DCT watermarking technique for still images was proposed by Hernandez et al. which includes detector performance analysis and a new structure [8]. A new watermarking scheme using GABPN hybrid intelligent network and the HVS features of DCT domain to embed binary watermark in gray image was proposed by Agarwal et al. [1]. The reasonable features of HVS can effectively improve the performance of the watermarking algorithm.

With the development of digital watermarking, matrix decomposition has become one of the important tools to protect the copyright. For example, Golea et al. proposed a digital watermarking technique based on singular value decomposition (SVD) [5]. Kincaid et al. pointed out that Schur decomposition is a relatively simple matrix decomposition method in linear algebra [11]. Golub et al. pointed out that Schur decomposition is an intermediate step of SVD decomposition [6]. Hence, Su et al. proposed a watermarking method based on matrix Schur decomposition [23]. It used the similarities of elements in the matrix obtained by Schur decomposition to embed the color watermark image into the color host image. Method [23] has a good invisibility and strong anti-

scaling ability, relatively. However, when the watermarked images obtained by method [23] are attacked, the similarities between the matrix elements are easily broken. Thus, it has weak robust to resist salt & pepper attack, median filtering attack, and cropping attack. After a while, Su et al. continue to study the features of the matrix obtained by Schur decomposition. They found that the maximum energy coefficient contains certain stability, and then a modified color image digital watermarking algorithm based on matrix Schur decomposition was proposed to protect the copyright of the color image [22]. Compared with the method [23], the anti-JPEG compression ability and anti-cropping ability of the method [22] have been improved to some extent, but the method [22] only used the maximum energy coefficient rather than the whole energy coefficient, its anti-cropping ability is not enough strong. In addition, its ability of resisting the median filtering attack is still weak.

Since the computer technology is deeply studied by hackers, the wide transmission of color digital image makes it more easily to be attacked. But the strong robustness of the color watermarking algorithms [30–32, 37] in the frequency domain can resist various attacks. For example, Wan et al. [30] proposed a novel Spread Transform Dither Modulation (STDM) watermarking scheme based on Hybrid just noticeable distortion model for screen content images. The robustness and visual quality of the watermarking scheme are improved by using the AC coefficient feature. The smaller key space of the algorithm is difficult to meet the high safety application demand [36], and the security of the algorithm needs to be improved. For example, when Arnold encryption algorithm is used in color image of size 25×25, its key space is 2^{18} [36]. This key space is not enough to meet people's needs. Shang et al. pointed out that there are many methods to calculate the period of Arnold transform and calculate the inverse transform, and traditional Arnold transform has become unsafe for image scrambling [19]. Thus, Liu et al. proposed a secure and robust digital image watermarking scheme using logistic and RSA encryption to improve the security of the watermarking algorithm [13].

As can be seen from the above discussion, how to use the advantages of the frequency domain watermarking algorithm to design a blind color image watermarking algorithm with strong robustness, high security and large capacity has become one of the urgent problems.

In this paper, a blind color image watermarking scheme with variable steps based on matrix Schur decomposition is proposed in the frequency domain. According to the fact that Schur decomposition is less complex than other matrix decomposition methods in the frequency domain, this scheme carries out Schur decomposition on the image block to obtain the upper triangular matrix. The main diagonal elements of the upper triangular matrix are eigenvalues of the image block, and the embedding and blind extractions of color digital watermarks are completed by quantifying the sum of their eigenvalues. The contributions of this algorithm include three points: 1) Based on the characteristics of the Human Visual System (HVS), the similarity of pixels between color image channels, and the different importance of watermark bits, the different quantization steps are used to the processes of watermark embedding and extraction; 2) Since the high and low bits of the watermark have different importance, the high watermark bits are repeatedly embedded to improve the robustness of watermarking algorithm; 3) Affine transformation algorithm is used to encrypt the color watermark image for improving the watermark security. The proposed algorithm can embed the color image watermark into the color host image, which not only has good watermark invisibility, but also has strong robustness and high security.

The rest of this paper is organized as follows. In the Section 2, the basic theories of Schur decomposition and Affine transformation are introduced. The Section 3 describes the embedding and blind extraction process of the proposed color image digital

watermarking algorithm. In order to show the superiority of the proposed algorithm, the Section 4 evaluates the performance of the proposed algorithm in detail. Finally, the conclusion of the proposed algorithm is summarized in the Section 5.

2 Background

This section introduces the basic theories used in this paper. Firstly, considering the high robustness of the watermarking algorithm in the frequency domain, Schur decomposition of matrix is introduced. Secondly, Affine transform is introduced for ensuring the security of the watermark information.

2.1 Schur decomposition

The feature of Schur decomposition is that all the eigenvalues of the pixel block can be easily obtained. Schur decomposition is defined as follows:

$$A = U \times V \times U^T \tag{1}$$

where, $A \in R^{n \times n}$, and U is an unitary matrix and V is an upper triangular matrix. In order to clearly explain the content of Schur decomposition, Eq. (1) can be described in detail as follows:

$$A = U \times V \times U^T = \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ u_{2,1} & \cdots & u_{2,n} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ u_{2,1} & \cdots & u_{2,n} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \cdots & u_{n,n} \end{bmatrix}^T \tag{2}$$

where, the variable r is the rank of the matrix A, $\lambda_i (i=1,2,\ldots,r)$ is the eigenvalue of matrix A and satisfies the following size relation:

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > \lambda_{r+1} = \cdots = \lambda_n = 0 \tag{3}$$

It can be found from Eq. (3) that the maximum eigenvalue of matrix A is λ_1, and it has the maximum energy coefficient. If you modify it according to certain rules, you can use this fine-tuning relationship to embed the watermark information [23]. But, when the carrier containing watermark information is attacked, it is easy to break the embedding rules, which results in some information extraction errors. In order to reduce the error rate of extraction, all the eigenvalues can be adjust according to the weight of all the eigenvalues. In this way, when the host image is attacked to the same degree, the influence on each eigenvalue will be reduced. Thus, the stability of the embedding rules will be improved, and the accuracy of extracted watermark information will be improved. In other words, the robustness of the algorithm will be improved.

2.2 Affine transformation

In order to ensure the security of watermark information, Affine transformation [3, 34, 36] is adopted in this paper to scramble the watermark image. In scrambling encryption, the transform number of the image is used as the private key Ka_p to ensure the security of the watermark information, where

p=1, 2, 3, and represents red, green and blue color channel, respectively. Affine transformation is defined as an Affine transformation or Affine mapping between two vector spaces, which is composed of a non-singular linear transformation and a translation transformation. The general form of Affine transformation is defined as follows [34]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{cases} Q \times \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} & if \quad x < y-1 \\ Q \times \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ f \end{pmatrix} & if \quad x \geq y-1 \end{cases} \tag{4}$$

where, Q is a nonsingular matrix with size of 4×4, $\begin{pmatrix} x \\ y \end{pmatrix}$ represents the original position of the element (x, y) in the matrix as the x-th row and y-th column, $\begin{pmatrix} x' \\ y' \end{pmatrix}$ represents the new position of the element (x, y) in the matrix as the x'-th row and y'-th column. Both $\begin{pmatrix} e \\ f \end{pmatrix}$ and $\begin{pmatrix} 1 \\ f \end{pmatrix}$ are vectors that represent translation, where e and f are constants.

Since Affine transformation is used for image scrambling, there are special requirements for the general form of Affine transformation. To find the appropriate Affine transformation matrix Q and the constants e and f, Affine transformation should meet the following conditions: 1) the transformation is a single mapping of the region $(x,y)(1 \leq x \leq n, 1 \leq y \leq n)$ to itself; 2) the transformation is a full mapping of the region $(x,y)(1 \leq x \leq n, 1 \leq y \leq n)$ to itself, where n represents the length or width of the image.

Since Affine transformation matrix Q is a non-singular matrix, Q is an invertible matrix. Let the inverse matrix be Q^{-1}. The inverse transformation of Affine transformation is defined as follows [34]:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} Q^{-1} \times \begin{pmatrix} x' \\ y' \end{pmatrix} - Q^{-1} \times \begin{pmatrix} e \\ f \end{pmatrix} & if \quad x' + y' \leq n+1 \\ Q^{-1} \times \begin{pmatrix} x' \\ y' \end{pmatrix} - Q^{-1} \times \begin{pmatrix} 1 \\ f \end{pmatrix} & if \quad x' + y' > n+1 \end{cases} \tag{5}$$

3 Proposed method

In this section, the pre-processing of color host image and color watermark image are described at first. Meanwhile, Fig.1 shows the general processes of embedding watermark and extracting watermark. In which, the top half of Fig. 1 shows the flowchart of embedding watermark, and the bottom half of Fig. 1 shows the flowchart of the watermark extraction.

3.1 The pre-process of embedding watermark

3.1.1 Pre-processing the color host image

The **24-bit** color host image H with size of $M \times M$ is changed to three **8-bit** color channel host images with size of $M \times M$ by dimension reduction, and the red, green and blue color channel

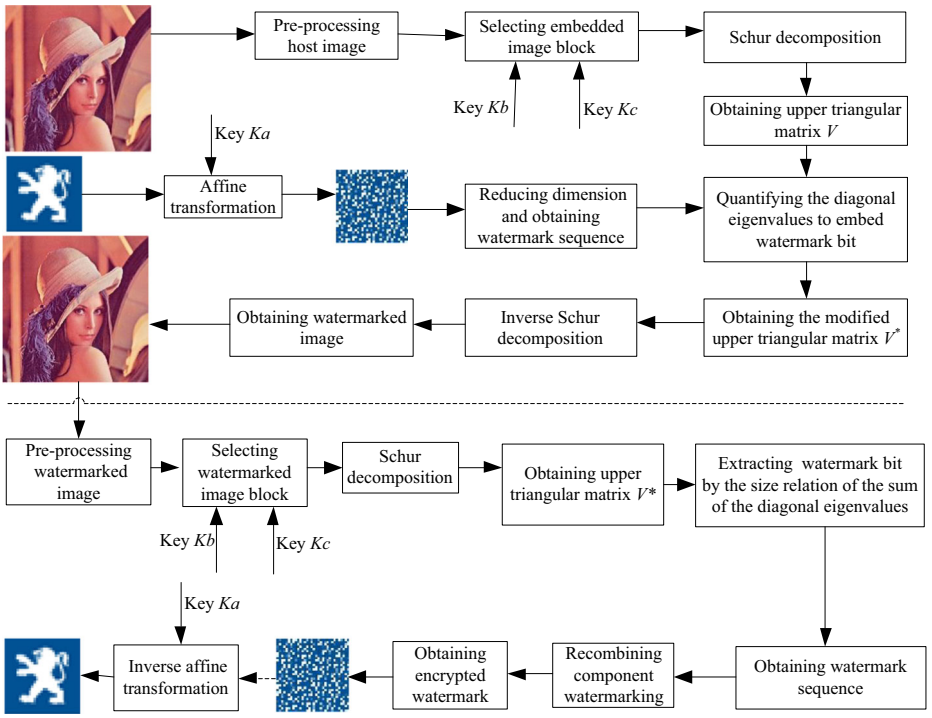

Fig. 1 The flowchart of embedding and extracting watermark

H_p is obtained. Each color channel is divided into non-overlapping pixel blocks with size of 3×3, where p =1, 2, 3, and represents red, green and blue color channel, respectively.

3.1.2 Pre-processing the color watermark image

The **24-bit** color watermark image W with size of $N \times N$ is changed to three **8-bi**t color channel watermark images with size of $N \times N$ by dimension reduction, and the red, green and blue color channel W_p is obtained. Then, Affine transformation based on private key Ka_p is carried out for each color channel to obtain the scrambled color channel, where p =1, 2, 3, and represents red, green and blue color channel, respectively. Afterwards, the decimal pixel value of each color channel is converted into an 8-bit binary sequence. The first two in each 8-bit binary sequence are spliced into string sequence *str*, then the string sequence *str* is copied for three times and saved in the watermark string $wbit_1$. The middle three and the last three of each 8-bit binary sequence are spliced into watermark string $wbit_2$ and $wbit_3$, respectively.

3.2 Embedding watermark

In this process, the watermark information is embedded into the block of the channel host image, and the detailed procedure of embedding the watermark is explained as follows.

- The pseudo-random sequences generated by *randperm* function based on the private keys Kb_p and Kc_p are used to select pixel block *schurblock* from the color channel H_p, where p =1, 2, 3, and represents the red, green and blue color channel, respectively. According to

Eq. (6), Schur decomposition is performed on the pixel block *schurblock*. The former r elements $V(i, i)$ in the upper triangular matrix V are the i-th eigenvalue of the pixel block *schurblock*, respectively. i =1, 2,..., r, r represents the rank of the pixel block *schurblock*.

$$[U, V]=\text{schur}(schurblock) \tag{6}$$

- Selecting the watermark bit wt from the watermark string in sequential order, and calculating the quantization value add by Eq. (7).

$$add = \begin{cases} \lambda_{sum}-\text{mod}\left(\lambda_{sum}, T_p\right) + 0.75 \times T_p, if & wt = '0' \\ \lambda_{sum}-\text{mod}\left(\lambda_{sum}, T_p\right) + 0.25 \times T_p, if & wt = '1' \end{cases} \tag{7}$$

where, the sum of all the eigenvalues of a pixel block $\lambda_{sum} = \sum_{i=1}^{r} \lambda_i$, mod(.) is modulo function, and T_p is quantization step.

- By using Eq. (8) to obtain the eigenvalue λ_i^* and replace the original eigenvalue, the upper triangular matrix V^* is obtained.

$$\lambda_i^* = \lambda_i + (add-\lambda_{sum}) \times \frac{\lambda_i}{\lambda_{sum}} \tag{8}$$

- The watermarked pixel block $schurblock^*$ is obtained by the inverse Schur decomposition as shown in Eq. (9).

$$schurblock^* = U \times V^* \times U^T \tag{9}$$

- Repeating the above steps, three-layer watermarked color channel H_p^* is obtained. Finally, reconstructing the color channel H_p^* to obtain the watermarked color image H^*.

3.3 Extracting watermark

The watermark information is extracted from the watermarked image without the original host image or watermark image. The detailed procedure of extracting watermark is explained as follows.

- Pre-processing the **24-bit** watermarked image. The size of watermarked image H^* is adjusted to $M \times M$ and dimension reduction is performed, and the red, green and blue three **8-bit** color channel images $H_p{}^*$ are obtained. All the pixels in each channel image are divided into non-overlapping pixel blocks of size 3×3, where p =1, 2, 3, and represents red, green and blue color channel, respectively.
- Select the pixels block *schurblock** in the same way as the embedding process. According to Eq. (10), Schur decomposition is performed on the watermarked pixel block *schurblock**. The former r elements $V^*(i, i)$ in the upper triangular matrix V^* are the i-th eigenvalue of the pixel block *schurblock**, respectively. i =1, 2, ..., r, r represents the rank of the pixel block *schurblock**.

$$\left[U^*, V^*\right] = \mathrm{schur}\left(schurblock^*\right) \tag{10}$$

- Eq. (11) is used to extract the watermark bit wt^* from the watermarked pixel block *schurblock**.

$$wt^* = \begin{cases} '0' & if\ \mathrm{mod}\left(\lambda_{sum}{}^*, T_p\right) > 0.5 \times T_p \\ '1' & if\ \mathrm{mod}\left(\lambda_{sum}{}^*, T_p\right) \le 0.5 \times T_p \end{cases} \tag{11}$$

where, mod(.) is modulo function. The sum of all the eigenvalues of a watermarked pixel block is $\lambda_{sum}{}^* = \sum_{i=1}^{r} \lambda_i{}^*$, and T_p is quantization step.

- Repeating above processes, until all the watermarks are extracted. Thus, the watermarked strings str^*, $wbit_2{}^*$, $wbit_3{}^*$ are obtained. Performing the inverse process of pre-processing the color watermark image in Section 3.1 and obtaining the layered color channel $W_p{}^*$. Each layer of color channel is transformed by inverse Affine transformation based on the private key Ka_p, and reorganized into the extracted watermark image W^*.

4 Performance evaluation and analysis

In order to evaluate the invisibility, robustness and security of the proposed scheme, it is necessary to compare this scheme with other related methods [5, 22, 23]. The contents of simulation and analysis are shown as follows.

4.1 Dataset

In the test of the proposed method, the host images are 24-bit color image. They are all selected from the databases CVG-UGR [28] and USC-SIPI [29]. In order to facilitate the experiment, as shown in Fig. 2, the size of the ten host images is resized to 512×512. As shown in Fig. 3, two 24-bit color images with size of 32×32 are used as the watermark

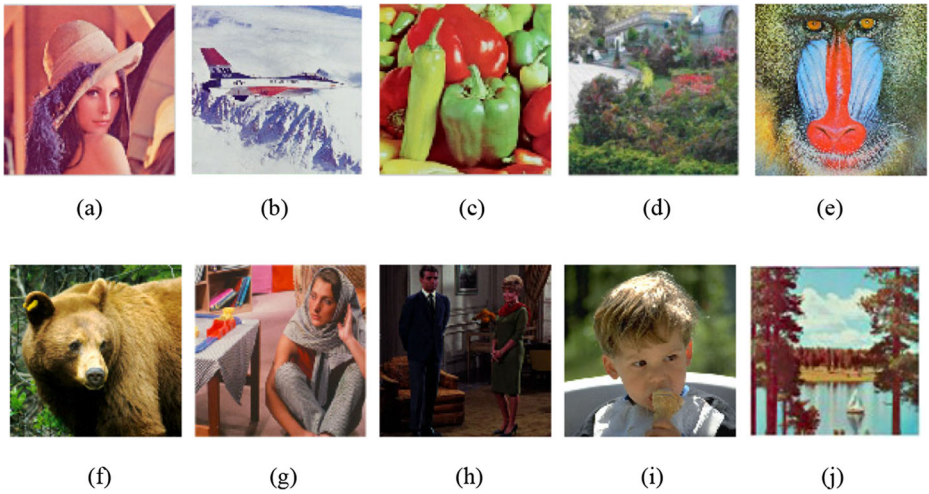

Fig. 2 Host images: (a) Lena, (b) Avion, (c) Peppers, (d) TTU, (e) Baboon, (f) Bear, (g) Barbara, (h) Couple, (i) Kid, and (j) Sailboat

information. All of them are used to test invisibility and compare the robustness of the algorithm with methods [5, 22, 23] in the experiment.

4.2 Metrics

In this section, three measurement indexes, which named peak signal-to-noise ratio (PSNR), structural similarity index metric (SSIM) and normalized cross-correlation (NC), are mainly described and used. PSNR and SSIM can measure the similarity between the original image and the watermarked image, and used to measure the invisibility of watermark. Because NC can measure the fidelity of the extracted watermark, it is often used to measure the robustness of the watermarking. If the NC value is 1, the watermark is regarded as fully extracted. The performance of the watermarking algorithm can be emphasized by the effective use of two types of indicators.

Firstly, PSNR is used to evaluate the invisibility of watermark. The unit of PSNR is dB, and the higher PSNR value is, the better the image quality will be. In general, PSNR value more than 48 dB represents that the image quality is excellent, and image without any noticeable changes. The value of PSNR between 35 dB and 48 dB means good quality and the value of PSNR between 29 dB to 35 dB represents acceptable quality. The critical point of PSNR is 25 dB. If the value of PSNR is smaller than 25 dB, watermark will be obvious [15]. Therefore, the PSNR of watermarking algorithm should be improved as much as possible in a certain range.

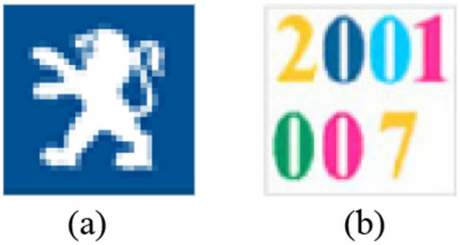

Fig. 3 Watermark images: (a) Watermark image 1, (b) Watermark image 2

PSNR can measure the quality of watermarked image (H^*), and its definition is shown in Eq. (12).

$$PSNR = \left(\sum_{p=1}^{3} PSNR_p \right) / 3 \tag{12}$$

where, p=1, 2, 3, and it represents the red, green and blue color channel of the image respectively, and the $PSNRp$ of each color channel (Hp^*) is shown in Eq. (13).

$$PSNR_p = 10 \times \log_{10} \left(\frac{255^2}{MSE_p} \right) \tag{13}$$

The MSE_p in Eq. (13) is the mean square error of the original image H and the watermarked image H^*. In general, the images H and H^* have the same size of $n \times n$. MSE_p can be defined as Eq. (14).

$$MSE_p = \frac{1}{n \times n} \sum_{i=1}^{n} \sum_{j=1}^{n} \left[H_p(i,j) - H_p{}^*(i,j) \right]^2 \tag{14}$$

where, $H_p(i, j)$ is the pixel value of i-th row and j-th column in the p-th channel, p=1, 2, 3, and it represents the red, green and blue color channel of the image, respectively.

Secondly, SSIM reflects the properties of the structure in the scene and designs the distortion as a combination of brightness, contrast and structural similarity. The mean value between images is used as the measure of brightness, the standard deviation between them is used as the measure of contrast, and the covariance between them is used as the measure of structural similarity. The value range of SSIM is from 0 to 1. When the original image H is exactly the same as the watermarked image H^*, the value of SSIM is 1. SSIM is defined as follows:

$$SSIM(H, H^*) = \frac{(2\mu_H \mu_{H^*} + c_1)(2\sigma_{HH^*} + c_2)}{(\mu_H{}^2 + \mu_{H^*}{}^2 + c_1)(\sigma_H{}^2 + \sigma_{H^*}{}^2 + c_2)} \tag{15}$$

where, μ_H and μ_{H^*} are the mean values of images H and H^*, respectively. σ_H and $\sigma_{H^*}$are the variances of images H and H^* respectively.σ_{HH^*} is the covariance between images H and H^*.

Finally, NC is often used to evaluate the robustness of watermarking [26]. Its principle is to calculate the correlation coefficient matrix between the watermarked image and the original image by using the correlation coefficient formula, and evaluate the correlation degree of two images by analyzing the correlation coefficient matrix. The value range of NC is from 0 to 1. The larger the value of NC is, the stronger the correlation of images will be, and the stronger robustness of the watermarking will be. When the value of NC is 1, two images are exactly the same. Therefore, for the watermarking algorithm, on the premise of ensuring the watermark to meet the requirement of invisibility, the value of NC should be increased as much as possible.

The NC between the original watermark $W$and the extracted watermark W^* can be obtained by using Eq. (16).

$$NC = \frac{\sum_{p=1}^{3} \sum_{x=1}^{n} \sum_{y=1}^{n} \left[W(x,y,p) \times W^*(x,y,p) \right]}{\sqrt{\sum_{p=1}^{3} \sum_{x=1}^{n} \sum_{y=1}^{n} \left[W(x,y,p) \right]^2} \sqrt{\sum_{p=1}^{3} \sum_{x=1}^{n} \sum_{y=1}^{n} \left[W^*(x,y,p) \right]^2}} \tag{16}$$

where, the size of original watermark W and extracted watermark W^* is $n \times n$, $W(x, y, p)$ represents the pixel value of the x-th row and y-th column in the p-th color channel of the original watermark, p=1, 2, 3, and it represents the red, green and blue color channel of the watermark, respectively.

In addition, the quantization step is an important parameter to determine the feature of watermarking algorithm. The proposed algorithm combines the following four features to select the quantization step: 1) the error rates of the extraction in the hundreds, tens and unities have different influences on the robustness of the watermarking algorithm. Assuming that the error rate of watermark extraction is constant, the error extraction in the hundreds has the greatest influence on the robustness of the watermarking, and the error extraction in the tens has the least influence. Similarly, if the decimal pixel of the watermark is represented by an 8-bit binary string, the higher the binary string is, the more important the information is; 2) human eye has the highest sensitivity to red, moderate sensitivity to green and the lowest sensitivity to blue [17]; 3) the quantization step has a great influence on the watermarking algorithm. The larger the step is, the more robust the watermarking will be, but the worse the watermark quality will be; 4) there is usually a strong correlation between three color channels of R, G and B in natural color images, and the correlation coefficients of three color channels are r(B,R)≈0.78, r(R,G)≈0.98 and r(G,B)≈0.94 [18], that is, r(B,R)≈0.78 represents the correlation coefficient between the blue channel and the red one, r(R,G)≈0.98 is the correlation coefficient between the red channel and the green one, and r(G,B)≈0.94 is the correlation coefficient between the green channel and the blue channel, respectively.

Let the step of the watermark embedded in layer B, G, R is T_1, T_2, T_3, respectively. Considering the influence of the above factors on the robustness of watermarking, the quantization step relationships of different color channels are as follows.

$$T_2 = 0.94 \times T_1 \tag{17}$$

$$T_3 = 0.78 \times T_1 \tag{18}$$

For testing the quantization step T_1, the experimental materials are the host image "Lena" in Fig. 2(a) and the watermark image "Watermark image 1" in Fig. 3(a), where the value of SSIM in Fig. 4 shows the watermarked image is not attacked. The NC is the average result obtained by the eight attacks with different parameters, such as JPEG compression, JPEG 2000 compression, Butterworth low-pass filtering, median filtering, scaling, cropping, Gaussian white noise and Salt & Pepper noise. As can be seen from Fig. 4, the quantization step T_1 is selected as 55 in this paper considering the balance of invisibility and robustness of the proposed method.

4.3 Invisibility test and analysis

The invisibility is an important index to test the performance of watermarking algorithm. The method [5] used SVD decomposition to detect and extract watermark. In theory, Schur decomposition is an intermediate process of SVD decomposition. Hence, the proposed method based on Schur decomposition is compared to the method [5]. In addition, the methods [22, 23] all use different methods to embed and extract watermark information based on Schur decomposition. Thus, the proposed method based on Schur decomposition is also compared to the related methods [22, 23].

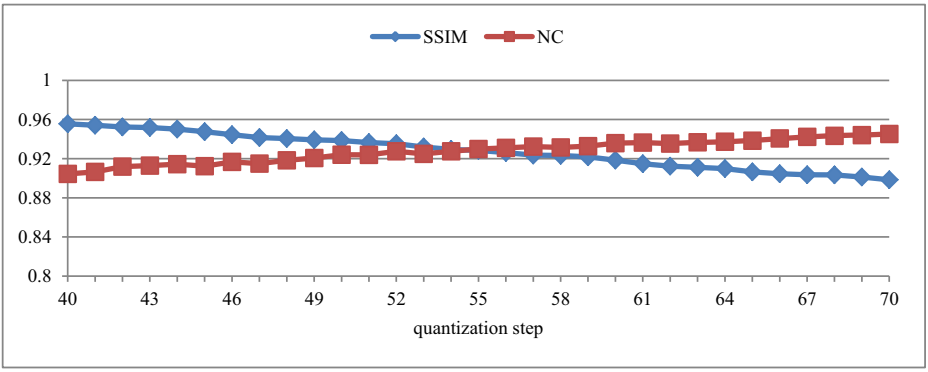

Fig. 4 The different results of SSIM and average NC under different quantization steps

At first, ten 24-bit color host images and two 24-bit color watermark images are selected to evaluate the invisibility of the proposed method. Since the quantization step of the proposed method has been determined, the experimental data for testing the invisibility are obtained on the premise of guaranteeing the complete extraction of the watermark, which can improve the robustness of the algorithm as much as possible. It can be seen from Table 1, the SSIM values are close to 1, and the average SSIM is more than 0.9. In addition, the average PSNR is more than 35 dB. Therefore, the watermarked image has good quality [15], which meets the requirement of watermark invisibility.

Secondly, in order to further measure the invisibility of the proposed method, it is compared with different watermarking methods. Table 2 shows the values of PSNR and SSIM of various watermarking methods. In method [5], not only the values of PSNR and SSIM are higher, but also the average PSNR and SSIM are higher, so their invisibility is stronger. In the original methods [22, 23], most of the PSNR values are more than 33 dB, and each average value is more than 34 dB. Thus, the methods [22, 23] can meet the requirement of invisibility. The proposed method has the same invisibility as methods [22, 23], and the average PSNR are more than 35 dB, which means the proposed method has met the invisibility requirements. Since the fixed quantization step is used to different color channels in [22], which neglects the correlation of different channels and reduces the invisibility of watermarking algorithm. However, the proposed scheme uses the correlation between different color channels and

Table 1 The test results (PSNR/SSIM) of watermark invisibility

Host image	Watermark image 1	Watermark image 2
Lena	36.1046/0.9214	36.1680/0.9294
Avion	36.0268/0.9172	36.0692/0.9266
Baboon	35.7506/0.9701	35.7889/0.9725
TTU	35.9331/0.9526	35.9329/0.9565
Peppers	34.6974/0.8951	34.8798/0.9065
Bear	30.6977/0.8919	31.0841/0.9006
Barbara	35.8287/0.9263	35.8875/0.9332
Couple	34.2514/0.8668	34.7585/0.8814
Kid	35.8629/0.9096	35.7679/0.9154
Sailboat	36.0025/0.9217	36.0354/0.9296
Average	35.1156/0.9173	35.2372/0.9252

Table 2 The values of PSNR (dB)/SSIM of different watermarking methods

Host image	Method [5]	Method [23]	Method [22]	Proposed Method
Lena	39.4358/0.9935	35.4358/0.9767	35.8031/0.9889	36.1046/0.9214
Avion	38.3922/0.9540	38.3922/0.9651	38.3160/0.9705	36.0268/0.9172
Baboon	33.9068/0.9462	28.4332/0.9281	29.5935/0.9572	35.7506/0.9701
TTU	34.3048/0.9532	33.8649/0.9363	33.8603/0.9760	35.9331/0.9526
Average	36.5099/0.9617	34.0315/0.9516	34.3932/0.9732	35.9538/0.9403

HVS to choose different quantization steps, which will improve the invisibility of the watermarking scheme.

4.4 Robustness test and analysis

Robustness is one of the important metrics to evaluate the performance of watermarking algorithm. A robust watermarking algorithm can extract the watermark information from attacked image when the watermarked image is attacked by malicious operation.

When the images are stored on disk, the image may be compressed. JPEG compression, as an image compression standard based on the Discrete Cosine Transform, is widely used in the network, CD and web pages, etc. JPEG 2000, as a new image compression standard based on Wavelet transform, has lower distortion rate. In addition, in the process of transmission, the watermarked images are often affected by noise, such as Gaussian noise and Salt & Pepper noise. The image quality will also be decreased by median filtering, Butterworth low-pass filtering and other filtering technologies. What's more, the image size will be changed and the

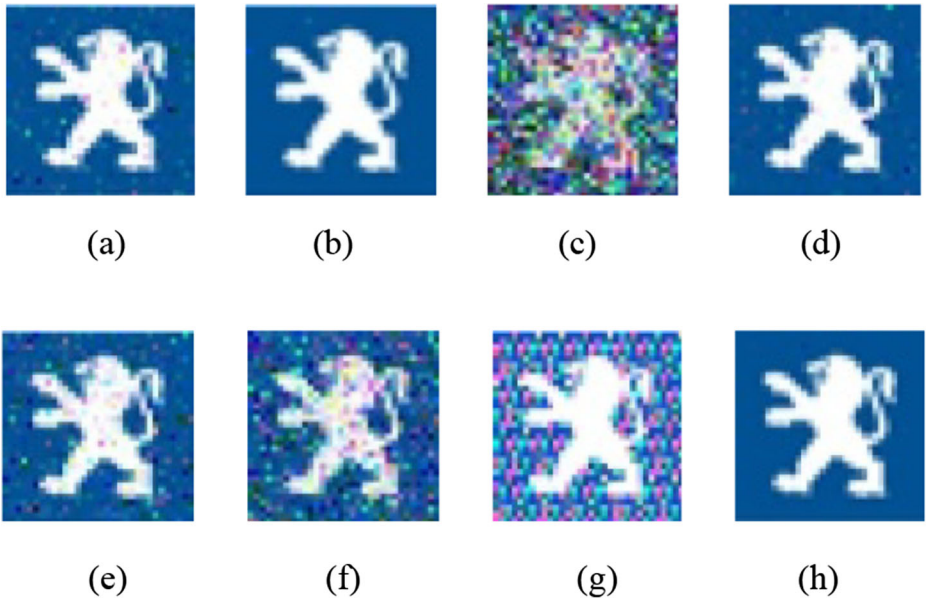

Fig. 5 Extract the "Watermark image 1" from the watermarked image "Lena" after different attacks: (a) JPEG (70) NC = 0.9929, (b) JPEG 2000 (5:1) NC = 0.9997, (c) Gaussian white noise (0, 0.001) NC = 0.7687, (d) Salt & Peppers noise (2%) NC = 0.9947, (e) Butterworth low-pass filtering (100, 20) NC = 0.9756, (f) Median filtering (2 × 2) NC = 0.9179, (g) Cropping (37.5%) NC = 0.6753, and (h) Zoom-in (4:1) NC = 0.9998

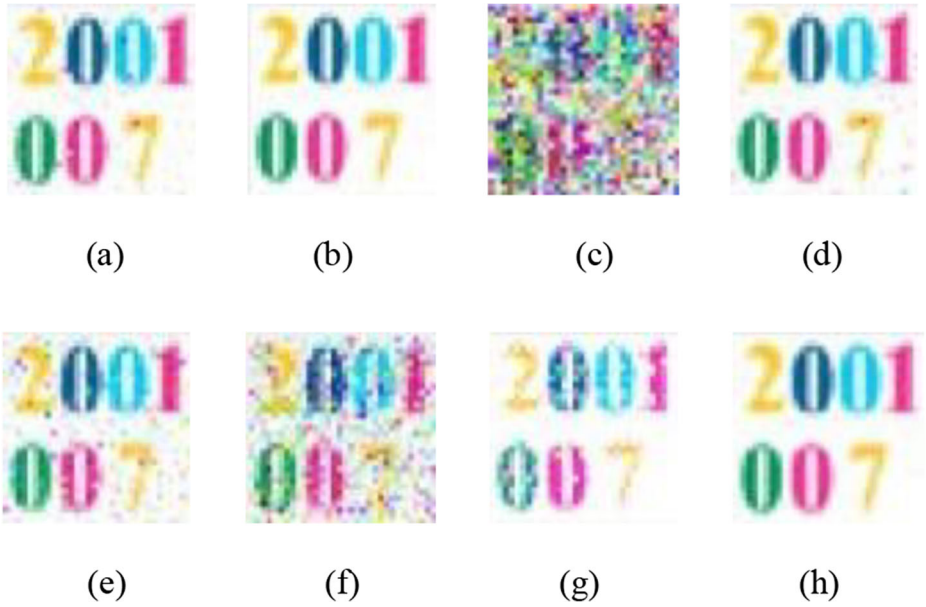

Fig. 6 Extract the "Watermark image 2" from the watermarked image "Lena" after different attacks: (a) JPEG (70) NC = 0.9911, (b) JPEG 2000 (5:1) NC = 0.9999, (c) Gaussian white noise (0, 0.001) NC = 0.7459, (d) Salt & Peppers noise (2%) NC = 0.9942, (e) Butterworth low-pass filtering (100, 20) NC = 0.9746, (f) Median filtering (2 × 2) NC = 0.9078, (g) Cropping (37.5%) NC = 0.9579, and (h) Zoom-in (4:1) NC = 0.9998

image quality will be decreased by rescaling and cropping operation. Therefore, the above attacks are selected to attack the watermarked images.

Two types of experiments are used to discuss the robustness of the proposed algorithm. The first type evaluates the robustness by two different watermark images and the second one evaluates the robustness by comparing with different methods [5, 22, 23].

Firstly, the color image "Lena" in Fig. 2(a) is selected as the host image, and the color image "Watermark image 1" in Fig. 3(a) is selected as the watermark image. In this

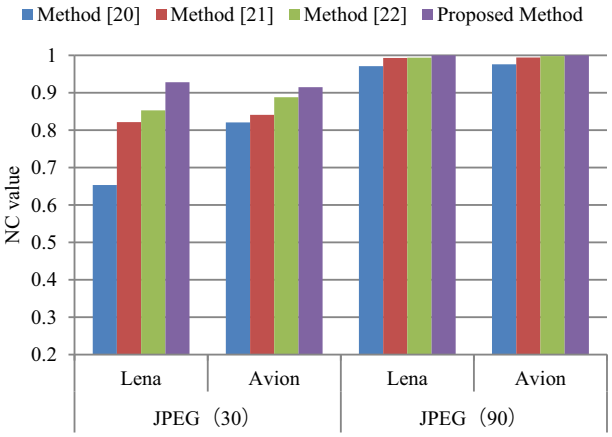

Fig. 7 The NC values obtained by different methods after different JPEG compression attacks

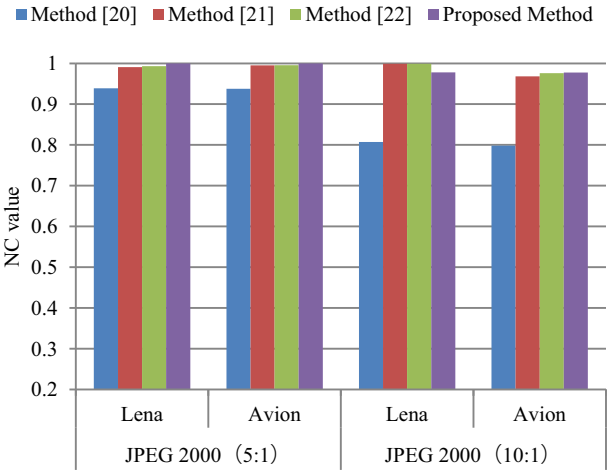

Fig. 8 The NC values obtained by different methods after different JPEG 2000 compression attacks

experiment, various attacks with different parameters are applied to the watermarked image, and the extracted watermark images and NC values are shown in Fig. 5. It can be seen from these results that the proposed method has strong robustness against various attacks. However, due to the strong attack ability of Gaussian white noise, the robustness of the proposed method is weak when Gaussian white noise is added.

Secondly, the host image "Lena" in Fig. 2(a) and the watermark image "Watermark image 2" in Fig. 3(b) are selected as the test images to further test the robustness. The related experimental results are presented in Fig. 6. It can be seen from Fig. 6 that the proposed method has strong robustness to resist various attacks except the attack of adding Gaussian white noise.

In order to further evaluate the robustness of the proposed method, the comparison tests are carried out. The materials of experiments include the host images of Fig. 2(a) "Lena" and Fig. 2(b) "Avion" and the watermark image of Fig. 3(a) "Watermark image 1". The watermarked

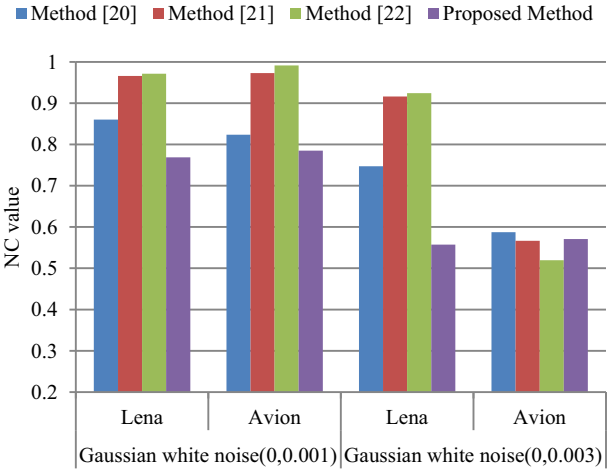

Fig. 9 The NC values obtained by different methods after different Gaussian white noise attacks

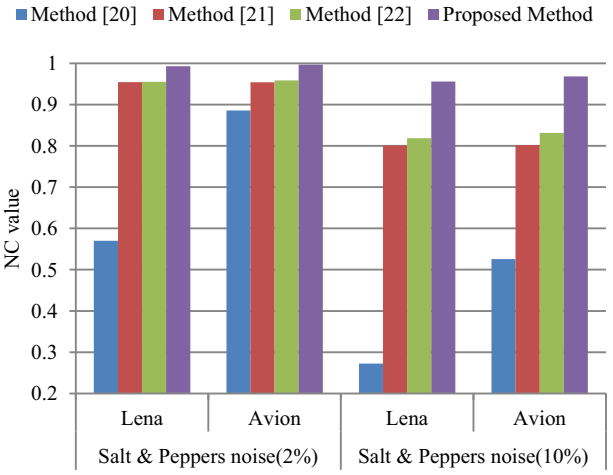

Fig. 10 The NC values obtained by different methods after different Salt & Peppers noise attacks

image is attacked by four attacks with different parameters. At the same time, methods [5, 22, 23] are selected as comparison methods to discuss the robustness of the proposed method in this experiment.

Firstly, JPEG compression experiments with compression ratios from 10 to 100 and step length of 10 are carried out for the watermarked image. In Fig. 7, some experimental results of JPEG compression attack are presented. As can be seen from Fig. 7, the proposed method is more robust when the image compression ratio is lower. Relatively, the NC values of the proposed algorithm are similar to other three methods when the compression ratio is higher. Moreover, Fig. 8 shows part of the experimental results of JPEG 2000 attack. It is seen from the four groups of data in the Fig. 8 that the proposed method is more robust than method [5], and its robustness is similar to the methods [22, 23].

Secondly, different Gaussian white noises, based on different parameters $(0, x)$, $x \in [0.001, 0.005]$, are used to attack the watermarked image. Figure 9 shows some

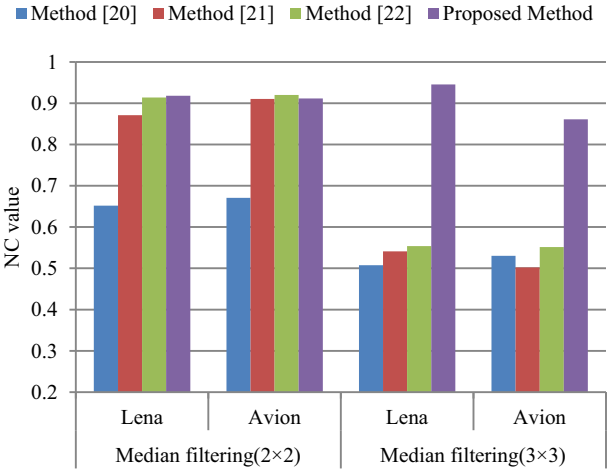

Fig. 11 The NC values obtained by different methods after different median filtering attacks

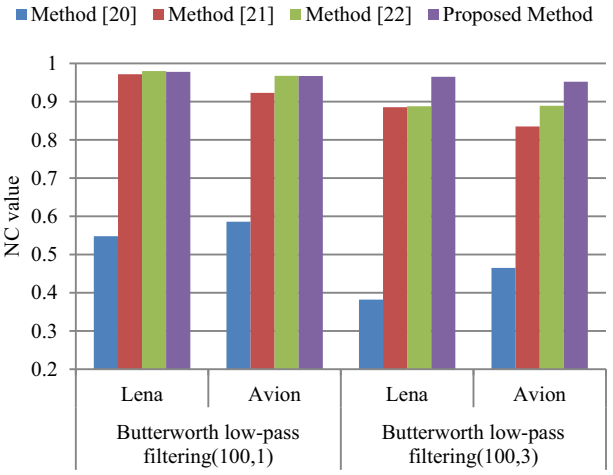

Fig. 12 The NC values obtained by different methods after different Butterworth low-pass filtering attacks

experimental results. The data in the figure shows that the proposed method is weak robust to resist Gaussian noise attacks. In addition, the watermarked image is attacked by adding Salt & Pepper noise with noise intensity from 1% to 10%. Figure 10 shows the comparison results. Experimental results show that the NC values are slightly bigger than the other three methods when the attack intensity is small, but the proposed algorithm has obvious advantage compare to other methods when the attack intensity is big.

Thirdly, the windows of median filtering are set to 2×2 and 3×3 in the experiments, respectively. The data of Fig. 11 shows that the NC values of the proposed method are superior to method [5] and similar to the methods [22, 23] when the window size is 2×2. When the median filtering window is 3×3, the NC value of the proposed method is more than 0.85, which indicates that the proposed algorithm shows strong robustness. At the same time, the watermarked image is attacked by Butterworth low-pass filtering attacks with parameters from (100, 1) to (100, 5), respectively. Some experimental results in

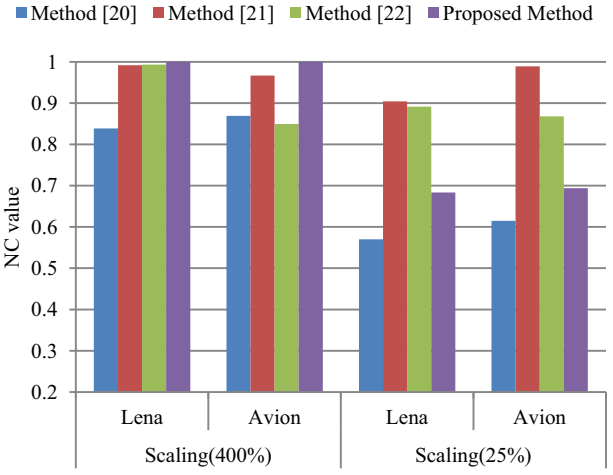

Fig. 13 The NC values obtained by different methods after different Scaling attacks

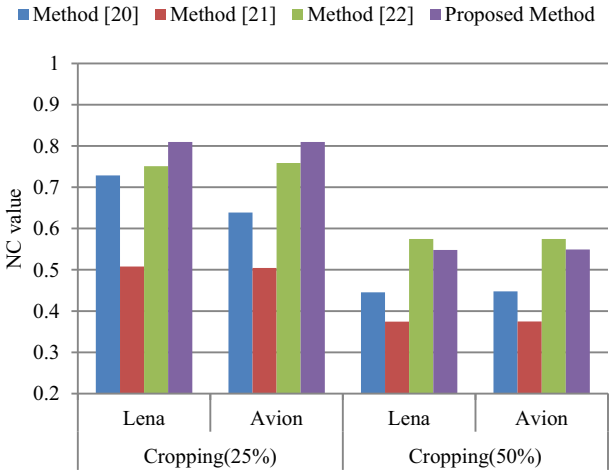

Fig. 14 The NC values obtained by different methods after different Cropping attacks

Fig. 12 show that the proposed method has stronger robustness than other methods when parameter is (100, 3).

Finally, Fig. 13 shows the experimental results of scaling two watermarked images to 400% and 25% of the original size respectively. The proposed method has stronger robustness than other methods when the image is scaled up, while the robustness of the proposed method is weak when the watermarked image is scaled down. As shown in Fig. 14, the NC value of the proposed method is high when the watermarked image is cut off by 25%. When the cut ratio reaches to 50%, the proposed method is weaker than method [22], but is stronger than methods [5, 23].

Since the proposed method uses the whole energy coefficient to complete the processes of embedding watermark and extracting watermark, but the method [22] only used the maximum energy coefficient. Thus, the robustness of the method [22] is weaker than the proposed method. What's more, since the high bits and the low ones of the watermark have different importance, the high watermark bits are repeatedly embedded to improve the robustness of the proposed method, but the methods [22, 23] all ignore this problem.

4.5 Security analysis

The security of watermark is an important prerequisite to ensure the effective implementation of the watermarking algorithm. In this paper, two private keys are used to improve the security

Affine key *Ka*	Right	Wrong	Right	Right
Select block key *Kb*	Right	Right	Wrong	Right
Select block key *Kc*	Right	Right	Right	Wrong
Extracted watermark image				

Fig. 15 The extracted watermark images with different keys

of the algorithm. The first private key *Ka* was used for Affine transformation to encrypt watermark images, and others private keys *Kb* and *Kc* are used to generate the pseudo-random sequences for selecting the pixel blocks from the color channels.

Firstly, Affine transform encryption algorithm has more advantages than the conventional MD5-based Arnold scrambling encryption algorithm, the advantages mainly include the following two aspects: 1) only if the scrambled key is right, Affine transformation can be decrypted immediately without other iterative operations; 2) compared with the Arnold image encryption algorithm, Affine transform has a larger key space. In method [36], the key space of the Arnold transform is only about 2^{18}, while the key space of Affine transform in each channel is more than 2^{84} in this paper. The key space of the whole Affine transform includes three key space of red, green and blue three color channels, and its key space is more than 2^{252}, which is far larger than the key space of Arnold transform.

Secondly, the proposed method uses the pseudo-random sequences generated by *randperm* function based on the private keys *Kb* and *Kc* to select pixel blocks from the color channels. Since the range of positive integer is from 1 to 32,767, the key space of private key *Kb* decided by two integers is 2^{30} and the key space of private key *Kc* decided by two integers is 2^{30}. Then, the key space of each layer color channel of the selected block algorithm determined by the private keys *Kb* and *Kc* is 2^{60}. Hence, the key space of the selected block algorithm includes the key space of red, green and blue three color channels and its key space is 2^{180}.

Therefore, the key space of the proposed method is more than 2^{432}. The larger the key space is, the more the transform times are, the more the chaotic degree is, and the higher the identification is. In this paper, the probability that three keys are cracked at the same time is $1/2^{432}$ when the keys are used in violence. Because of the key space of the private keys *Ka*, *Kb* and *Kc* is big enough, the security of the proposed method is high.

In order to more intuitively reflect the importance of the key, some experiments were carried out. Figure 15 shows the visual effect of extracting watermark images when the key is wrong. As can be seen from Fig. 15, if any key is wrong, the watermark image will not be extracted successfully.

4.6 Watermark embedded capacity analysis

The watermark embedded capacity is an important factor to measure the quality of watermark algorithm. The comparison results of watermark capacity experiments of the methods [5, 22, 23] are shown in Table 3. As can be seen from Table 3, the proposed

Table 3 The comparison of watermark embedded capacity between different methods

	Maximum embedded watermark information (bit)	Real embedded watermark information (bit)	Host image (Pixel)	Embedded watermark capacity(bit/pixel)
Method [5]	24,576	24,576	3 × 1024 × 1024	0.0078125
Method [23]	49,152	24,576	3 × 512 × 512	0.0312500
Method [22]	49,152	24,576	3 × 512 × 512	0.0312500
Proposed method	87,381	24,576	3 × 512 × 512	0.0312500

method can embed the biggest maximum embedded watermark information, which is more applicable than other methods.

5 Conclusion

In order to meet the needs of color image copyright, this paper proposes a color image watermarking technology based on Schur decomposition. The proposed method uses Affine transform algorithm with large key space to encrypt the watermark. In addition, the Schur decomposition with low complexity is also used in this paper. The watermark embedding and blind extraction are completed by quantizing the eigenvalues on the diagonal of the decomposed matrix with different quantization steps. Simulation results show that this method not only meets the requirement of invisibility, but also achieves good performance in terms of security and robustness. In future, we will consider how to develop this method to practical application.

Acknowledgements The research was partially supported by the National Natural Science Foundation of China (No. 61771231, 61772253, 61873117 and 61872170), and Key Research and Development Program of Shandong Province (No. 2019GGX101025).

References

1. Agarwal C, Mishra A, Sharma A (2013) Gray-scale image watermarking using GA-BPN hybrid network. J Vis Commun Image Represent 24(7):1135–1146
2. Chang C, Shen J (2017) Features classification forest: a novel development that is adaptable to robust blind watermarking techniques. IEEE Trans Image Process 26(8):3921–3935
3. Chen H, Du X, Liu Z, Yang C (2013) Color image encryption based on the affine transform and gyrator transform. Opt Lasers Eng 51(6):768–775
4. Cruz-Ramos C, Reyes-Reyes R, Nakano-Miyatake M, Perez-Meana H (2010) A blind video watermarking scheme robust to frame attacks combined with MPEG2 compression. J Appl Res Technol 8(3):323–337
5. Golea N, Seghir R, Benzid R (2010) A bind RGB color image watermarking based on singular value decomposition. IEEE/ACS international conference on computer systems and applications (AICCSA): 1-5
6. Golub G, Van Loan C (1996) Matrix computations. The Johns Hopkins
7. Hai T, Li C, Jasni M, Ahmed N (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12(1):122–138
8. Hernandez J, Amado M, Perez-Gonzalez F (2000) DCT-domain watermarking techniques for still images: detector performance analysis and a new structure. IEEE Trans Image Process 9(1):55–68
9. Hsu L, Hu H (2017) Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. J Vis Commun Image Represent 46:33–47
10. Karybali I, Berberidis K (2006) Efficient spatial image watermarking via new perceptual masking and blind detection schemes. IEEE Trans Inform Forensics Sec 1(2):256–274
11. Kincaid D, Kincaid D R, Cheney E (2009) Numerical analysis: mathematics of scientific computing. American Mathematical Soc
12. Liu X, Lin C, Yuan S (2018) Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans Circ Syst Video Technol 28(5):1047–1055
13. Liu Y, Tang S, Liu R, Zhang L, Ma Z (2018) Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Syst Appl 97:95–105
14. Madine F, Akhaee M, Zarmehi N (2018) A multiplicative video watermarking robust to H.264/AVC compression standard. Signal Process Image Commun 68:229–240
15. Moosazadeh M, Ekbatanifard G (2017) An improved robust image watermarking method using DCT and YCoCg-R color space. Optik 140:975–988

16. Nguyen T, Chang C, Yang X (2016) A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. AEU-Int J Electron Commun 70(8):1055–1061
17. Roy S, Pal A (2017) A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU - Int J Electron Commun 72:149–161
18. Sangwine S, Horne R (1998) The colour image processing handbook. Springer Berlin 29(5):461
19. Shang Z, Ren H, Zhang J (2008) A block location scrambling algorithm of digital image based on Arnold transformation. 2008 the 9th international conference for young computer scientists. IEEE: 2942-2947
20. Singh S, Bhatnagar G (2018) A new robust watermarking system in integer DCT domain. J Vis Commun Image Represent 53:86–101
21. Su Q (2016) Novel blind colour image watermarking technique using Hessenberg decomposition. IET Image Process 10(11):817–829
22. Su Q, Chen B (2017) An improved color image watermarking scheme based on Schur decomposition. Multimed Tools Appl 76(22):24221–24249
23. 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
24. 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
25. Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X (2015) Embedding color image watermark in color image based on two-level DCT. SIViP 9(5):991–1007
26. Su Q, Wang G, Zhang X, Lv G, Chen B (2018) A new algorithm of blind color image watermarking based on LU decomposition. Multidim Syst Sign Process 29(3):1055–1074
27. Su Q, Yuan Z, Liu D (2019) An approximate Schur decomposition-based spatial domain color image watermarking method. IEEE Access 7(1):4358–4370
28. University of Granada. Computer Vision Group. CVG-UGR Image Database, http://decsai.ugr.es/cvg/dbimagenes/c512.php
29. University of Southern California, Signal and Inage Processing Institute. USC-SIPI Image Database, http://sipi.usc.edu/database/
30. Wan W, Wang J, Li J, Meng L, Sun J, Zhang H, Liu J (2018) Pattern complexity-based JND estimation for quantization watermarking. Pattern Recogn Lett. https://doi.org/10.1016/j.patrec.2018.08.009
31. Wan W, Wang J, Li J, Sun J, Zhang H, Liu J (2018) Hybrid JND model-guided watermarking method for screen content images. Multimedia tools and applications: 1-24
32. Wan W, Wang J, Xu M, Li J, Sun J, Zhang H (2019) Robust image watermarking based on two-layer visual saliency-induced JND profile. IEEE Access 7:39826–39841
33. Wang J, Li T, Shi Y, Lian S, Ye J (2017) Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics. Multimed Tools Appl 76(22):23721–23737
34. Wang H, Hu Y, Yu L, Sun W (2018) The research of blind watermarking based on zigzag and affine transformation. 2018 37th Chinese control conference (CCC), IEEE: 9250–9254
35. Yuan X, Li M (2018) Local multi-watermarking method based on robust and adaptive feature extraction. Signal Process 149:103–117
36. Zhu G, Lei B, Quan P, Ye J (2010) Quasi-affine transform over limited integer grids and its application. 2010 third international symposium on information science and engineering. IEEE: 184-187
37. Zou L, Sun J, Gao M, Wan W, Gupta B (2018) A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia tools and applications: 1-16

Decheng Liu received his Bachelor Degree from the School of Information and Electrical Engineering, Ludong University, Yantai, China, in 2018. He is studying for a Master Degree in School of Information and Electrical Engineering of Ludong University, Yantai, China. His research interests include image processing, information security, and etc.

Zihan Yuan received her Bachelor Degree from the School of Computer Science and Technology, Jining Medical University, Jining, China, in 2018.She is studying as a master in School of Information and Electrical Engineering of Ludong University, Yantai, China. Her research interests include image processing, information security, and etc.

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.