IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 7, 2018, accepted December 16, 2018, date of publication December 27, 2018,
date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2888857

An Approximate Schur Decomposition-Based Spatial Domain Color Image Watermarking Method

QINGTANG SU, ZIHAN YUAN, AND DECHENG LIU
School of Information Science and Engineering, Ludong University, Yantai 264025, China

Corresponding author: Qingtang Su (sdytsqt@163.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61771231, in part by the Natural Science Foundation of Shandong Province under Grant ZR2017MF010, in part by the Natural Science Foundation of China under Grant 61772253, Grant 61873117, and Grant 61872170, and in part by the Natural Science Foundation of Shandong Province under Grant ZR2016FM21, Grant ZR2016FM13, and Grant ZR2017MF062.

ABSTRACT In this paper, an approximate Schur decomposition-based spatial domain blind color image watermarking method is proposed to protect the copyright of color images, which has low computation complexity similiar to the watermarking technique in the spatial domain and strong robustness similiar to the watermarking technique in the transform domain. First, the approximate maximum eigenvalue of Schur decomposition is calculated in the spatial domain by the proposed method. Second, the approximate maximum eigenvalue is used to embed and extract the color watermark image in the spatial domain without the true Schur decomposition. Moreover, the procedures of the proposed watermarking method are given in detail. The proposed technique is performed on the spatial domain based on the approximate Schur decomposition and belongs to blind watermarking technique. The experimental results on two publicly available image databases (CVG-UGR and USC-SIPI) have demonstrated the effectiveness of the proposed method in terms of invisibility, robustness, and the real-time feature.

INDEX TERMS Color image watermark, real-time feature, spatial domain, Schur decomposition.

I. INTRODUCTION

With the rapid development of the Internet, the security of multimedia big data has been becoming one of the research hotspots. Many techniques about information security, such as copy detection [1]–[4], steganography [5], [6], digital watermarking [7]–[19], have been proposed in the past two decades. Among these information security techniques, digital watermarking has become a necessary technique in many applications such as data authentication, broadcast monitoring on the Internet and ownership identification [7]. According to the types of carrier data, the watermarking methods include image watermarking [24], video watermarking [25], [26], text watermarking [27], audio watermarking [28], and so on. According to the processing domains of watermarking methods, the existing watermarking methods may be roughly classified into two types: spatial domain watermarking [9] and frequency domain watermarking [10]. The spatial domain watermarking is usually embedded watermark into the least significant bit (LSB) of the original image. Any changes in the watermarked image will affect the LSB of watermarked image, and the spatial watermarking method shows weak robustness but low computation complexity. Since the frequency components of the image can be used to embed and extract watermark, many frequency domain watermarking methods have been proposed [10], [15]–[17]. Generally, the frequency domain watermarking method has high computation complexity but good invisibility and robustness compared with the spatial domain watermarking method [9], [16]. It is necessary to find a new watermarking method which has the advantages of the spatial watermarking method and the frequency domain watermarking method for protecting the color image copyright in the multimedia big data era.

Recently, some watermarking research results for cloud computing have been proposed. For example, Singh *et al.* [8] proved that the digital watermarking could significantly improve the data security in cloud computing. Wang *et al.* [11] applied multi-watermarking in cloud environment, and found that the secure media distribution models are suitable for cloud-based platform. Ren *et al.* [12]

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

proposed a provable data possession model for multimedia files, and a framework based on digital watermarking for multimedia data storages audit service. Cao *et al.* [13] proposed a privacy-preserving and auditing-supporting outsourcing data storage scheme by using encryption and digital watermarking. Logistic map-based chaotic cryptography algorithm was used to preserve the privacy of outsourcing data [13], whose computation time is low and the encryption performance is good. These above-mentioned watermarking methods are mainly used to protect big data of images with respect to data storage, data access, data audit service, and so on. However, how to protect the copyright of big data of images using real-time watermarking method is still an open problem.

Since the image and video have occupied by more than 80% of big data and the color images are the main parts of images, to protect the copyright of color images is a key problem for the multimedia big data [14]. In the last two decades, a few of color image watermarking techniques have been proposed. For example, Chou *et al.* [9] proposed a method to embed color watermark into color host image with the quantization indices of the host image in the uniform color space; the application of this method is simple, but its robustness is weak. Recently, many matrix decomposition methods, such as Schur decomposition, singular value decomposition (SVD), LU decomposition, and so on, have been widely applied to the digital watermarking. In [15], a SVD-based robust watermarking method was proposed to embed color image to color host image. In [16], the similarity correlation based Schur decomposition method was used to embed color watermark image into color host image. For further enhancing the watermarking performance of the method [16], an improved watermarking technique [17] was proposed. The difference between the methods [16] and [17] is the embedding position of watermark. In the method [17], the embedding block is selected randomly, and the watermark is embedded into the elements $U_{2,\mathrm{c}}$ and $U_{3,\mathrm{c}}$ instead of the elements $U_{2,1}$ and $U_{3,1}$ that used in [16], where c is the column of the maximum eigenvalue in upper triangular matrix and U is an unitary matrix of Schur decomposition. Simulation results have shown that the proposed scheme [17] has better performance in terms of invisibility and robustness than that of method [16]. The common feature of the methods [16] and [17] is that the watermark is embedded into the unitary matrix of Schur decomposition. In which, twelve elements will be changed with more modification when embedding one watermark bit, and the total execution time cannot meet the real-time requirement for protecting the copyright of multimedia big data. Since Schur decomposition is an intermediate step in SVD decomposition, it could be further studied and applied to meet the real-time requirement in cloud computing. Theoretically, as a major intermediate step of SVD decomposition, Schur decomposition requires about $8n^3/3$ flops, where n is an iterator [18]. That is, Schur decomposition is less than one third numbers of computations required in SVD decomposition since SVD decomposition requires about $11n^3$ flops, and it means that the Schur decomposition based watermarking method is more effective to achieve the real-time feature than that of the SVD-based watermarking method. However, the average execution times of the methods [16] and [17] are 1.855042 seconds and 2.472367 seconds, respectively, which cannot be acceptable to protect the copyright of the color image. Hence, it is necessary to further reduce the computation time of watermarking method based on Schur decomposition.

In this paper, a new watermarking method based on the principle of Schur decomposition in the spatial domain is proposed. The maximum eigenvalue of Schur decomposition is obtained by the algebra operations in the spatial domain. And then, the watermark is embedded into the maximum eigenvalue in the spatial domain not in the frequency domain. This method belongs to blind watermarking method. Experimental results on two publicly available image databases (CVG-UGR and USC-SIPI) have demonstrated the effectiveness of the proposed method in terms of invisibility, robustness, and the real-time feature.

This paper is organized as follows. Section II introduces the preliminaries, which include Arnold transform and Schur decomposition. The method to get and use the approximate maximum eigenvalue of Schur decomposition in the spatial domain is proposed in Section III. The detailed procedures of watermark embedding and extraction are presented in Section IV. Simulation results and discussions are shown in Section V. At last, Section VI gives the conclusions.

II. GUIDELINES FOR MANUSCRIPT PREPARATION

In order to improve the robustness and security of the watermarking method, Arnold transform is explained in this section. In addition, the basic theory of Schur decomposition is introduced for further to research the feature of approximate maximum eigenvalue.

A. ARNOLD TRANSFORM

Arnold transform has been widely used to permute watermark image with size of $P \times P$ for watermark security [19], and its permutation can be realized by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod \quad P, \tag{1}$$

where x, y, x' and y' are four integer variables between 0 and P-1, and mod is modular operation. The image pixel at the coordinate (x, y) of original image will be permuted to a new coordinate (x', y') by (1), which disorganizes the pixels of watermark image and enhances the security in visual identification of watermark images and the number of permutations is the secret key. Correspondingly, the inverse transform formula of Arnold transform defined in (2) can be used to restore the original information.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} + \begin{bmatrix} P \\ P \end{bmatrix} \right) \bmod \quad P. \tag{2}$$

B. SCHUR DECOMPOSITION

As an important tool in numerical linear algebra, Schur decomposition has been widely used in watermarking techniques [16], [17].

Schur Theorem: If A is $n \times n$ unitary space, then the unitary matrix U exists and makes

$$UAU^T = D, \tag{3}$$

where D is an upper triangular matrix, and the elements on the D diagonal are the eigenvalues of A, and the matrix U^T represents the transposed unitary matrix U.

When A is a real matrix, its Schur decomposition can be performed by

$$[U, D] = schur(A), \tag{4}$$

where $schur(.)$ is the Schur decomposition function. Based on (4), the upper triangular matrix D can be obtained, and the maximum eigenvalue of A can be found on the diagonal of the matrix D, whose computation complexity is $O(n^2)$.

The matrix A can be reconstructed by the inverse Schur decomposition:

$$A = UDU^T, \tag{5}$$

where the matrix U^T represents the transposed unitary matrix U.

III. A NEW APPROXIMATE MAXIMUM EIGENVALUE OF SCHUR DECOMPOSITION IN THE SPATIAL DOMAIN

Eigenvalues are very important to the matrix characteristics, and the maximum eigenvalue plays important roles in Schur decomposition and it has great effect on the performance of watermarking in the spatial domain. It takes more time to obtain the maximum eigenvalue of Schur decomposition by the Schur decomposition. This section proposes a new method to obtain the approximate maximum eigenvalue of Schur decomposition in the spatial domain, and then investigates the effects using the proposed method.

A. THE APPROXIMATE MAXIMUM EIGENVALUE OF SCHUR DECOMPOSITION IN THE SPATIAL DOMAIN

In Schur decomposition, the diagonal components of the upper triangular matrix consist of the real eigenvalues of Schur decomposition. Generally, the smaller the image block is, the closer the pixel values are, which because the changes of neighbor pixel values in one small image block are not obvious. The maximum eigenvalue of image block can be obtained by 2-norm form in Singular Value Decomposition (SVD), but how to calculate the maximum eigenvalue of Schur decomposition in the spatial domain is an open problem [20]. Here, we propose an approximate method to calculate the maximum eigenvalue of Schur decomposition in the spatial domain based on data statistical analysis as follows:

$$F_{\max} \approx \sum_{i=1}^{M}\sum_{j=1}^{M} a_{i,j}/M, \tag{6}$$

where $F_{\max}$ denotes the approximate maximum eigenvalue of the matrix A with size of $M \times M$, $a_{i,j} \in A$, and $1 \leq i, j \leq M$, whose computation complexity is $O(n)$.

Here one 4 × 4 matrix is used to explain how the proposed method can be used to find the maximum eigenvalue. The matrix A and its upper triangular matrix D are obtained by Schur decomposition as (7). It can be seen from (7) that the maximum eigenvalue of the upper triangular matrix D of Schur decomposition is 896.2491. When the proposed approximate method (6) is used to calculate the maximum eigenvalue in the spatial domain, the maximum eigenvalue is 896.25, which shows the proposed approximate method is effective.

$$A = \begin{bmatrix} 225 & 224 & 224 & 223 \\ 224 & 224 & 224 & 224 \\ 224 & 224 & 225 & 223 \\ 224 & 225 & 225 & 223 \end{bmatrix} = UDU^T, \tag{7}$$

where,

$$D = \begin{bmatrix} 896.2491 & -1.7673 & -1.0215 & -1.1547 \\ 0 & -0.9994 & -0.0004 & -0.6121 \\ 0 & 0 & 1.0000 & -0.3536 \\ 0 & 0 & 0 & 0.7503 \end{bmatrix},$$

$$U = \begin{bmatrix} -0.4999 & 0.0001 & 0.8165 & -0.2890 \\ -0.4999 & 0.7074 & -0.4082 & -0.2883 \\ -0.4999 & 0.0001 & 0.0006 & 0.8661 \\ -0.5004 & -0.7068 & -0.4084 & -0.2885 \end{bmatrix}.$$

For further validating the proposed approximate method, we use SIM to calculate the similarity between the approximate maximum eigenvalue VS and the maximum eigenvalue VA obtained by Schur decomposition, that is,

$$\text{SIM} = VS/VA. \tag{8}$$

In here, all test images are selected from the standard image databases [23], [29] and used to test the similarity SIM. Table 1 gives the test results. As can be seen from Table 1, the similarity of the proposed approximate method is near to 1, which means the proposed approximate method has good performance and can be used to calculate the maximum eigenvalue in the spatial domain instead of using Schur decomposition. In Table 1, $M = n$ represents the size of image block is $n \times n$.

B. MODIFY THE MAXIMUM EIGENVALUE OF SCHUR DECOMPOSITION IN THE SPATIAL DOMAIN

In general, when the watermark information is embedded into the image block, the maximum eigenvalue will be modified and the pixels of image block will be changed slightly at same time, which can improve the invisibility of watermarked image. Now, the key problem is to analyze the pixel changes of image block in the spatial domain when the watermark information is embedded into the maximum eigenvalue of Schur decomposition.

Suppose A is the original image block of size $M \times M$, A^* is the watermarked image block, $a_{i,j}$ is the i-th row the

TABLE 1. The similarity values of different maximum eigenvalues that obtained by schur decomposition and the propsosed approximate method.

Image	M=2	M=3	M=4	M=5	M=6
Lena	1.000312	1.000727	1.001385	1.001474	1.001594
Peppers	1.003375	1.008831	1.005762	1.006967	1.006661
Avion	0.999937	0.999981	1.000032	1.000110	1.000770
Baboon	0.999853	1.000072	1.000160	1.000185	1.000365
House	0.999999	0.999972	0.999938	0.999940	0.999908
Bear	1.013214	1.026602	1.012303	1.019199	1.017786
Kid	1.000704	1.000856	1.001122	1.001221	1.001140
Couple	1.003283	1.007920	1.005117	1.006168	1.005691
Sailboat	1.000127	1.000552	1.000093	1.000149	1.000154
Barbara	1.000647	1.002354	1.002869	1.002702	1.002262
Average	1.002145	1.004787	1.002878	1.003812	1.003633

j-th column element in the matrix A, $a^*_{i,j}$ is the i-th row the j-th column element in the matrix A^*, $F_{\max}$ represents the approximate maximum eigenvalue of A, and $F^*_{\max}$ represents the approximate maximum feature value of A^*.

According to (6), one can obtain

$$F^*_{\max} \approx \sum_{i=1}^{M}\sum_{j=1}^{M} a^*_{i,j}/M. \tag{9}$$

Suppose E is the change quantity of the approximate maximum eigenvalue of upper triangular matrix when embedding watermark, that is,

$$F^*_{\max} = F_{\max} + E; \tag{10}$$

i.e.

$$\sum_{i=1}^{M}\sum_{j=1}^{M} a^*_{i,j}/M = \sum_{i=1}^{M}\sum_{j=1}^{M} a_{i,j}/M + E, \tag{11}$$

$$\sum_{i=1}^{M}\sum_{j=1}^{M} a^*_{i,j}/M - \sum_{i=1}^{M}\sum_{j=1}^{M} a_{i,j}/M = E, \tag{12}$$

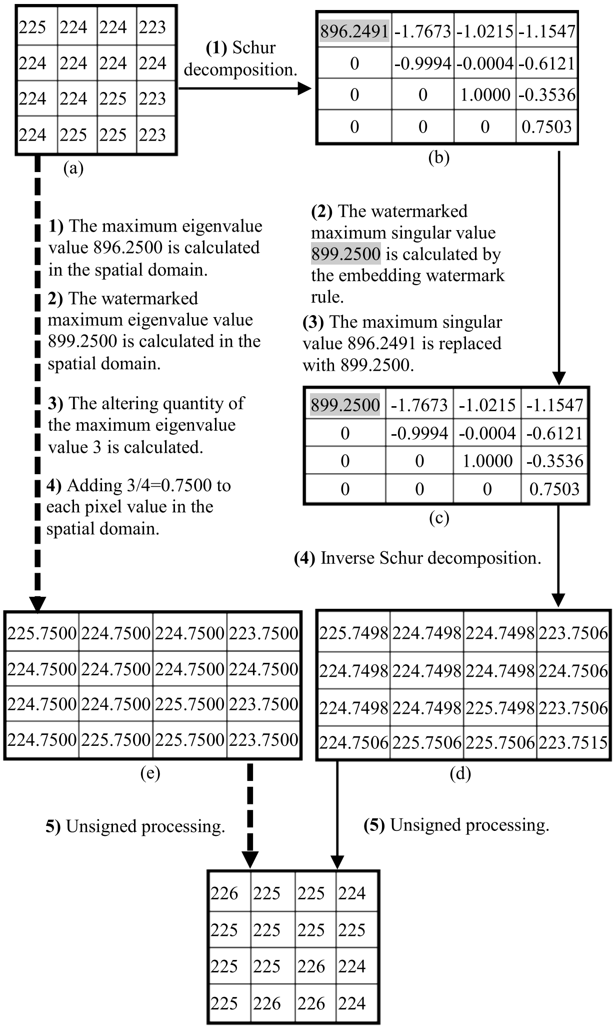
$$\sum_{i=1}^{M}\sum_{j=1}^{M} a^*_{i,j} - \sum_{i=1}^{M}\sum_{j=1}^{M} a_{i,j} = M \times E. \tag{13}$$

Let Δ be the average change quantify of each pixel in the image block of size $M \times M$, then

$$\Delta = (M \times E)/(M \times M) = E/M. \tag{14}$$

That is, adding E/M to each pixel in the spatial domain equals to embedding watermark information into the approximate maximum eigenvalue of Schur decomposition in the frequency domain. Moreover, the proposed method has simpler algebra operation than the Schur decomposition, and it can reduce the computation time which is important for the real-time watermarking.

Here, the comparison of the Schur decomposition based watermarking method and the approximate Schur decomposition based watermarking method is explained by Fig. 1. The original image block of size 4 × 4 is shown in Fig. 1(a).



(a)

225	224	224	223
224	224	224	224
224	224	225	223
224	225	225	223

(1) Schur decomposition.

(b)

896.2491	-1.7673	-1.0215	-1.1547
0	-0.9994	-0.0004	-0.6121
0	0	1.0000	-0.3536
0	0	0	0.7503

1) The maximum eigenvalue value 896.2500 is calculated in the spatial domain.

2) The watermarked maximum eigenvalue value 899.2500 is calculated in the spatial domain.

3) The altering quantity of the maximum eigenvalue value 3 is calculated.

4) Adding 3/4=0.7500 to each pixel value in the spatial domain.

(2) The watermarked maximum singular value 899.2500 is calculated by the embedding watermark rule.

(3) The maximum singular value 896.2491 is replaced with 899.2500.

(c)

899.2500	-1.7673	-1.0215	-1.1547
0	-0.9994	-0.0004	-0.6121
0	0	1.0000	-0.3536
0	0	0	0.7503

(4) Inverse Schur decomposition.

(e)

225.7500	224.7500	224.7500	223.7500
224.7500	224.7500	224.7500	224.7500
224.7500	224.7500	225.7500	223.7500
224.7500	225.7500	225.7500	223.7500

(d)

225.7498	224.7498	224.7498	223.7506
224.7498	224.7498	224.7498	224.7506
224.7498	224.7498	225.7498	223.7506
224.7506	225.7506	225.7506	223.7515

5) Unsigned processing.

(5) Unsigned processing.

(f)

226	225	225	224
225	225	225	225
225	225	226	224
225	226	226	224

FIGURE 1. The comparison of modifying the maximum eigenvalue of Schur decomposition in the spatial domain: (a) the original image block, (b) the upper triangular matrix, (c) the watermarked upper triangular matrix, (d) the results of inverse Schur decomposition, (e) the results of obtained in the spatial domain, and (f) the final same unsigned watermarked matrix by two different methods.

The upper triangular matrix of Schur decomposition is displayed in Fig. 1(b).

Supposing the watermarked maximum eigenvalue should be 899.2500 when the embedding watermark is “0”. As shown in Fig. 1(c), the maximum eigenvalue value 896.2491 is replaced with 899.2500. Fig. 1(d) shows the watermarked image block after inverse Schur decomposition. Fig. 1(e) shows the obtained watermarked image in spatial domain, and the final watermarked block is given in Fig. 1(f). It is noted that the difference of each corresponding pixel pair between Fig. 1(a) and Fig. 1(e) is $\Delta = E/M = 3/4 = 0.7500$, that is, Fig. 1(e) can also be directly obtained from Fig. 1(a) in the spatial domain by (14), which is one of the important innovations in this paper.

As can be seen from Fig.1, it is very clear that the embedding procedure of the proposed approximate method (dot line flow) is simpler than that of normal Schur decomposition (solid line flow), which shows the proposed method can be realized in the spatial domain.

IV. THE PROPOSED WATERMARKING METHOD

The proposed watermarking method is shown by Fig. 2. As shown in Fig. 2(a), the detailed steps for embedding watermark are explained as follows.

A. THE PROCEDURE FOR EMBEDDING WATERMARK

Step 1: Transforming the color watermark image to the binary watermark array.

At first, the original watermark image W is divided into R, G and B layers W_i by dimension-reduction treatment. Then, each layer watermark is permuted by Arnold transform with the private key Ka_i and converted every pixel value to 8-bit binary information, where $i = 1, 2, 3$, respectively. At last, all 8-bit binary information is sequentially linked to the watermark array.

Step 2: Selecting the embedding block of the host image.

The host image is also divided into R, G and B layer images and each layer image H_i is partitioned into non-overlapping blocks of size 4×4. For improving the anti-cropping robustness of the proposed method, the embedding blocks are dispersedly selected instead of centralized embedding. The Hash pseudo-random replacement algorithm, which is based on MD5 with private key Kb_i, is used to randomly select the embedding image blocks from image layer [21], where $i = 1, 2, 3$, respectively.

Step 3: Calculating the approximate maximum eigenvalue of embedding block.

The approximate maximum eigenvalue $F_{\max}$ of embedding block is calculated by (6) in the spatial domain.

Step 4: Embedding watermark.

The watermark information w is embedded into the approximate maximum eigenvalue $F_{\max}$ by the following four substeps.

Step 4.1: The watermarked approximate maximum eigenvalue $F^*_{\max}$ is calculated by the following rules.

$$F^*_{\max} = \begin{cases} F_{\max} - \mathrm{mod}(F_{\max}, T) + 0.75 \times T, & \text{if } w = 1 \\ F_{\max} - \mathrm{mod}(F_{\max}, T) + 0.25 \times T, & \text{if } w = 0, \end{cases} \tag{15}$$

where mod(.) represents the modular function, and T is quantization step.

Step 4.2: The changed quantity E of the approximate maximum eigenvalue is gotten by (16).

$$E = F^*_{\max} - F_{\max}. \tag{16}$$

Step 4.3. According to (14), the average changed quantity Δ of each pixel in the embedding block is gotten by

$$\Delta = E/4. \tag{17}$$

Step 4.4: The average changed quantity Δ is added to each pixel of the embedding block, which means that the watermark is embedded into the approximate maximum eigenvalue of the image block in the spatial domain.

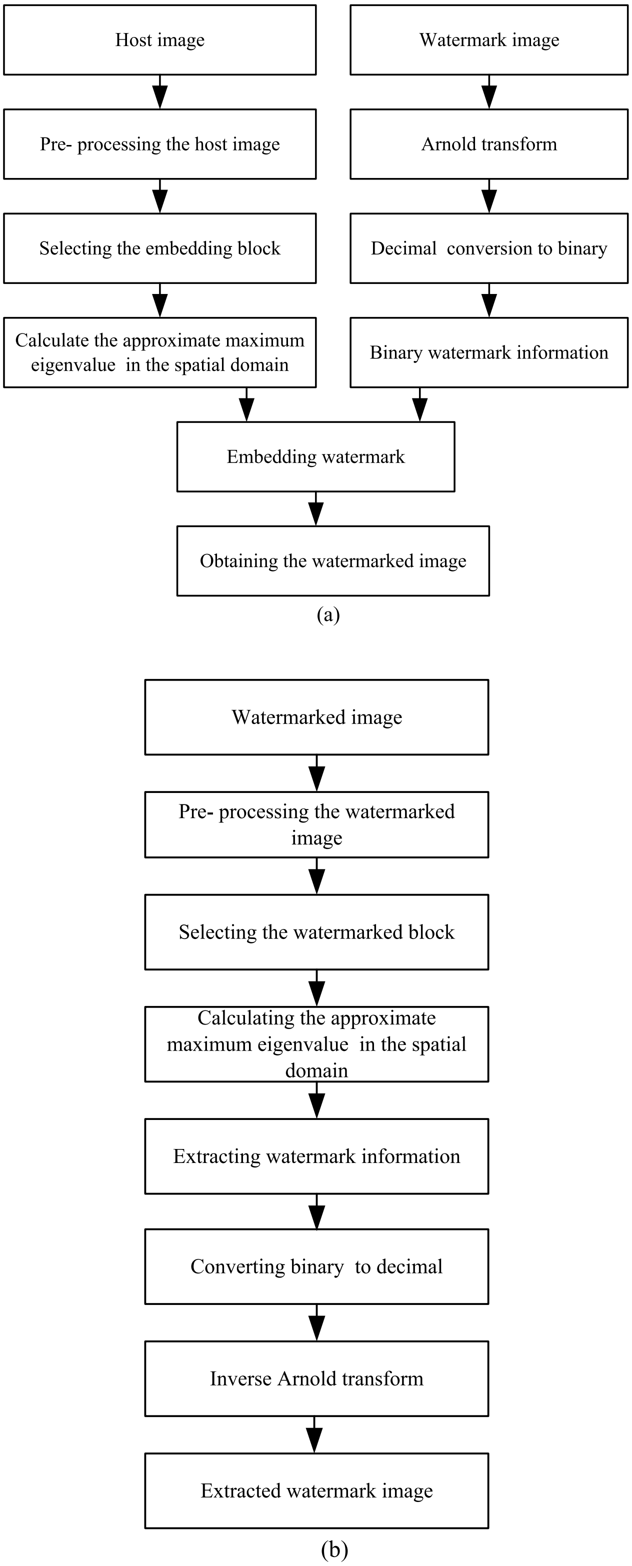

Host image
Pre- processing the host image
Selecting the embedding block
Calculate the approximate maximum eigenvalue in the spatial domain
Watermark image
Arnold transform
Decimal conversion to binary
Binary watermark information
Embedding watermark
Obtaining the watermarked image
(a)
Watermarked image
Pre- processing the watermarked image
Selecting the watermarked block
Calculating the approximate maximum eigenvalue in the spatial domain
Extracting watermark information
Converting binary to decimal
Inverse Arnold transform
Extracted watermark image
(b)

FIGURE 2. The proposed watermarking frameworks: (a) embedding watermark, and (b) extracting watermark.

Step 5: Repetition.

The above-mentioned Steps 3-4 are repeated to embed all binary watermark information into the host color image.

Step 6: Combining the R, G and B watermarked layer images to obtain the watermarked image H^*.

B. THE PROCEDURE FOR EXTRACTING WATERMARK

As shown in Fig. 2(b), the watermark is extracted from the watermarked image without the original host image or original watermark image. The detailed extraction procedures of the proposed watermarking method are explained as follows.

Step 1: Obtaining the watermarked image block.

At first, the watermarked image H^* is divided into R, G and B three layer images; then, each layer image is further divided into image blocks of size 4×4, and the watermarked image blocks are selected by the MD5-based Hash pseudo-random replacement algorithm with private key Kb_i, where $i = 1, 2, 3$, respectively.

Step 2: Calculating the approximate maximum eigenvalue $F^*_{\max}$ of the watermarked block based on the proposed method.

The approximate maximum eigenvalue $F^*_{\max}$ of watermarked block is calculated by (6) in the spatial domain.

Step 3: Extracting the watermark information w^*.

The embedded watermark w^* is extracted by the following rules.

$$w^* = \begin{cases} 0, & if \quad \bmod\,(F^*_{\max}, T) < 0.5 \times T \\ 1, & if \quad \bmod\,(F^*_{\max}, T) \geq 0.5 \times T. \end{cases} \tag{18}$$

Step 4: Repetition.

The above-mentioned Steps 2-3 are repeated to extract watermark information from the watermarked image blocks. All extracted bit values are partitioned into 8-bit groups, and each group is converted to decimal pixel value, then the inverse-Arnold transformation based on the private key Ka_i is executed and each extracted layer watermark is reconstructed, where $i = 1, 2, 3$, respectively.

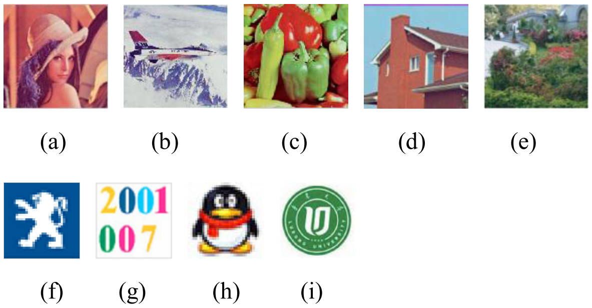
Step 5: Obtaining the extracted watermark.

The extracted three layer watermarks are rearranged to form the final extracted watermark W^* by R, G, and B order.

V. EXPERIMENTAL RESULTS

In this proposed method, the color images of the image databases CVG-UGR [23] and USC-SIPI [29] are used as the host images to evaluate the performance of the proposed method. In which, the CVG-UGR image database contains 135 color images and the USC-SIPI image database contains 53 color image.

For fair comparison, four color standard images of Figs. 3(a)-(d) and one common image Fig. 3(e), whose sizes are 512 × 512 pixels, are adopted as host images in here, and four 24-bit color images of size 32 × 32, as shown in Figs. 3 (f) - (i), are adopted as original color image watermarks in this experiment. In the following experiment, we select some color image watermarking methods as compared methods: an image SVD-based watermarking method [15], a novel blind image watermarking based on Schur decomposition [16], an improved color image watermarking scheme based on Schur decomposition [17], a classic color image watermarking method in the spatial domain [9], and so on.


(a) (b) (c) (d) (e)

(f) (g) (h) (i)

FIGURE 3. Host images: (a) Lena, (b) Avion, (c) Peppers, (d) House, and (e) TTU; Watermark images: (f) watermark 1, (g) watermark 2, (h) watermark 3, and (i) watermark 4.

For evaluating the imperceptibility, two indicators, i.e. the peak signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM), are adopted as the performance metrics [17].

As a good measurement for estimating the similarity between the watermarked image H^* and host image H, PSNR can be defined as follows:

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE}), \tag{19}$$

where the mean square error (MSE) for color image can be defined by

$$MSE = \frac{1}{3 \times m \times n} \sum_{z=1}^{3} \sum_{x=1}^{m} \sum_{y=1}^{n} [H(x, y, z) - H^*(x, y, z)]^2, \tag{20}$$

where m and n are the sizes of the testing image, and $H^*(x, y, z)$ and $H(x, y, z)$ are the pixel values at the coordinates (x, y, z) of watermarked image H^* and host image H, respectively.

SSIM, as a new evaluation method that has more correlation with HVS than PSNR [22], is defined as follows:

$$SSIM(H, H^*) = l(H, H^*)c(H, H^*)s(H, H^*), \tag{21}$$

where $l(H, H^*)$ is the luminance comparison function, $c(H, H^*)$ is the contrast comparison function, and $s(H, H^*)$ is the structure comparison function.

Moreover, the normalized cross-correlation (NC) is an effective way to measure the robustness, and NC is also adopted in this experiment, which is defined as follows:

$$NC = \frac{\sum\limits_{z=1}^{3} \sum\limits_{x=1}^{p} \sum\limits_{y=1}^{q} (W(x, y, z) \times W^*(x, y, z))}{\sqrt{\sum\limits_{z=1}^{3} \sum\limits_{x=1}^{p} \sum\limits_{y=1}^{q} W(x, y, z)^2} \sqrt{\sum\limits_{z=1}^{3} \sum\limits_{x=1}^{p} \sum\limits_{y=1}^{q} W^*(x, y, z)^2}}, \tag{22}$$

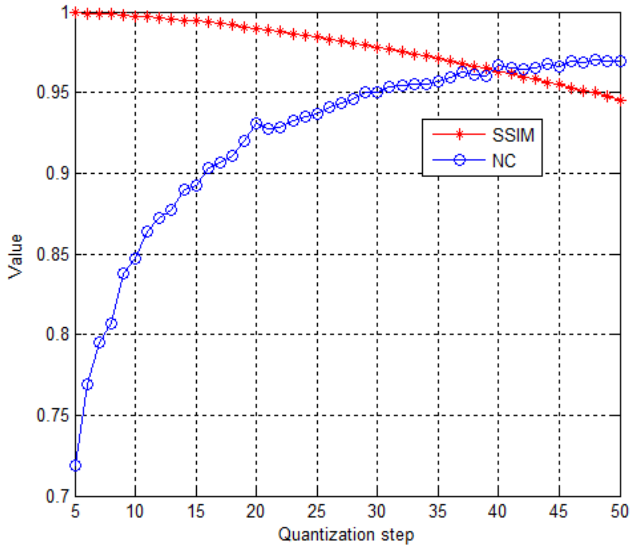


FIGURE 4. The average values of NC and SSIM under different quantization steps.

where p and q are the sizes of the watermark image, and $W^*(x, y, z)$ and $W(x, y, z)$ are the pixel values at the coordinates (x, y, z) of the extracted watermark W^* and original watermark W, respectively.

For selecting the suitable quantization step, the color image watermarks are embedded into the host images with different quantization steps T. The average SSIM values, the average NC values for different quantization steps T are given in Fig. 4, in which the quantization step T is increased from 5 to 50 with a step of 1. As can be seen from Fig. 4, when the quantization step T is increasing, the value of SSIM is decreasing and the value of NC is increasing, which means the invisibility is worse but the robustness is better when T is increasing. So, considering the balance between the robustness and invisibility of watermark, the quantization step T can be selected as 40.

A. IMPERCEPTIBILITY TEST

Table 2 gives the average PSNR values, the average SSIM values and the average NC values of the extracted watermark images when embedding four watermark images in Fig. 3 into all 512 × 512 color images of the CVG-UGR and USC-SIPI image databases, respectively. As can be seen from Table 2, the average PSNR values between the original host image and the watermarked image are more than 40 dB, and the SSIM values are near to 1. It is noted that the watermarked image is similar with the original host image when PSNR value is big or SSIM is nearer to 1. Hence, the watermarked image and the original host image are indistinguishable, which shows the effectiveness of the proposed watermarking scheme in term of the invisibility of watermark image.

For providing the invisibility comparison of different methods, we embed the color image watermark 1 of Fig. 3(f) into the color host images of Figs. 3(a) and (b), and embed the color image watermark 2 of Fig. 3(g) into the color host images of Figs. 3(c) and (e), respectively. Table 3 gives the values of PSNR and SSIM of watermarked images with different methods. It can be seen from Table 3 that the proposed method has the better visual quality of watermarked images than other methods.

TABLE 2. The quality comparison of the watermarked image and the extracted ONR when using the different color watermark images.

Watermark image	PSNR(dB)	SSIM	NC
Watermark 1	40.1565	0.9681	0.9964
Watermark 2	40.0691	0.9675	0.9912
Watermark 3	40.5405	0.9594	0.9988
Watermark 4	40.6450	0.9660	1.0000

TABLE 3. The imperceptibility comparison between different methods.

Method	Metric	Lena	Avion	Peppers	TTU
Method [15]	PSNR(dB)	38.3965	35.3004	38.9360	37.2120
	SSIM	0.9968	0.9954	0.9773	0.9854
Method [16]	PSNR(dB)	35.4358	38.3922	35.831	34.1080
	SSIM	0.9767	0.9540	0.9319	0.9788
Method [17]	PSNR(dB)	35.8031	38.3160	35.9869	37.3255
	SSIM	0.9889	0.9705	0.9709	0.9864
Proposed method	PSNR(dB)	40.6976	40.5906	40.5428	40.6095
	SSIM	0.9971	0.9957	0.9963	0.9893

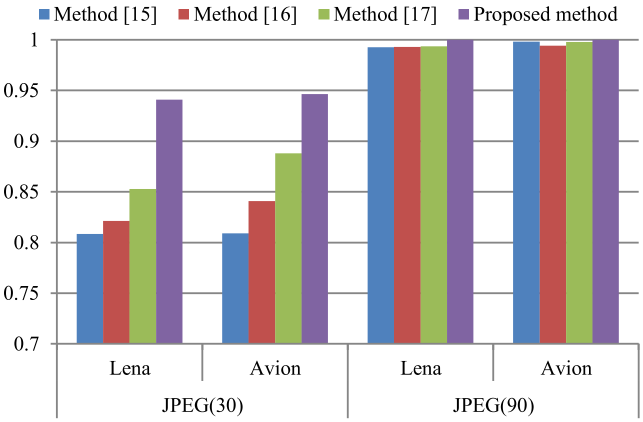


FIGURE 5. The comparison results of resisting the JPEG compression attack.

B. ROBUSTNESS TEST

For testing the robustness of the proposed method, the color image watermark 1 is embedded into the color host images Figs. 3(a) and (b), i.e. “Lena” and “Avion”, then several typical image attacks are performed on the watermarked images, and the extracted watermarks are compared to the related works [15]–[17].

Image compression, such as JPEG compression or JPEG 2000 compression, is one of the common image processes. In this experiment, the watermarked image is attacked by JPEG compression with an increment step 10; Fig. 5 gives parts of the experimental results with different compression

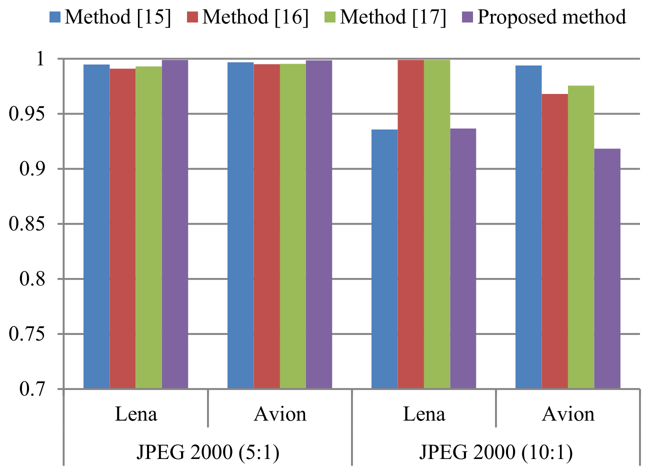


FIGURE 6. The comparison results of resisting the JPEG 2000 compression attack.

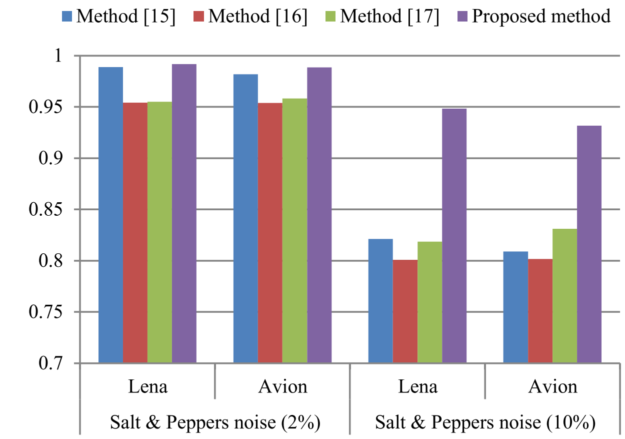


FIGURE 7. The comparison results of resisting the Salt & Peppers noising attack.

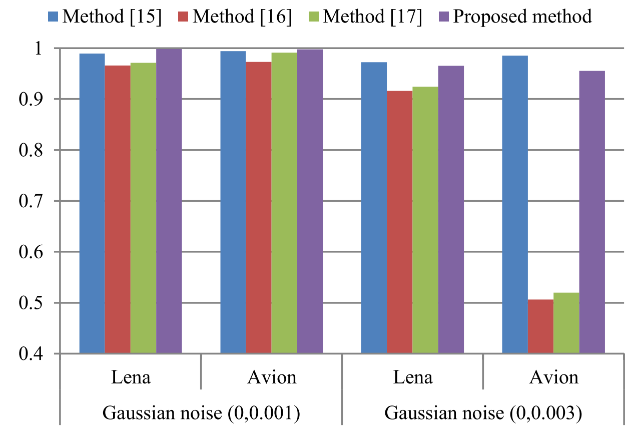


FIGURE 8. The comparison results of resisting the Gaussian noising attack.

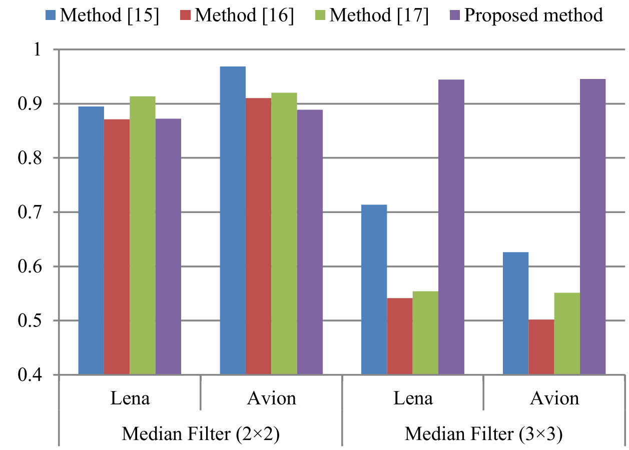


FIGURE 9. The comparison results of resisting the median filtering attack.

factors, respectively. In addition, the watermarked image is also attacked by JPEG 2000 compression with the compression ratio from 1 to 10 with an increment step 1, and Fig. 6 gives parts of the comparison results. As can be seen from Figs. 5 and 6, the proposed method has good robustness against image compression attack, especially in the common JPEG compression.

Adding noise is one common operation in image attacks, and there are many types of noise. In this experiment, we select the Salt & Peppers noising and Gaussian white noising as the typical noises. In the adding Salt & Peppers noise, the noise quantity is from 1% to 10% with an increment size 1%, and Fig. 7 shows the comparison results.

Moreover, Gaussian white noise of mean 0 and variances from 0.001 to 0.005 with an increment size 0.001 is used to attack the watermarked image. Fig. 8 shows the comparison results of extracted watermark after adding Gaussian white noise of mean 0 and different variances (0.001 and 0.003), respectively. As can be seen from Figs. 7 and 8, the proposed method has good robustness to against the noise attack.

In the filtering attack, at first, the median filtering with different windows sizes from 2 × 2 to 7 × 7 with an increment size 1 are used to process the watermarked images. Fig. 9 shows the comparison results of the filtering sizes of 2 × 2 and 3 × 3, respectively. It can be seen from Fig. 9 that as the window size changes bigger and bigger, the robustness of the proposed watermarking becomes stronger and stronger, which because the modified quantity of embedding watermark is well-distributed to each image pixel in the spatial domain.

In the second filtering experiment, Butterworth low-pass filtering attacks with cut-off frequency 100 and different orders are also performed on the watermarked images. Here, the orders are between 1 and 5 with interval of 1. Fig. 10 shows the comparison results of the attacked images with cut-off frequency 100 and orders 1 and 3, respectively. Obviously, the proposed method can effectively to against this filtering attack.

There are many sharpening methods in image processing. In this experiment, the watermarked image is attacked by sharpening with different pixel radii from 0.1 to 2 with an increment size 0.1. Fig.11 shows the comparison results of the

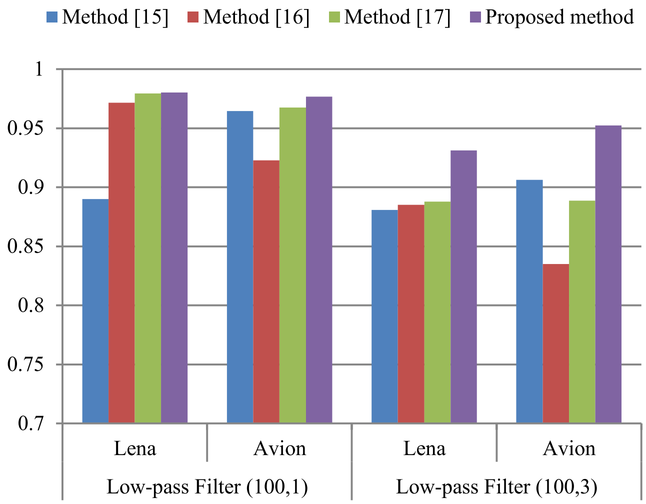


FIGURE 10. The comparison results of resisting the low-pass filtering attack.

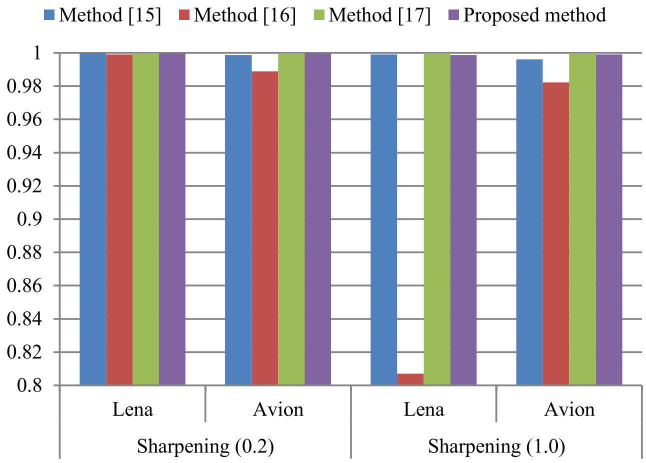


FIGURE 11. The comparison results of resisting the sharpening attack.

attacked image with different radii 0.2 and 1.0, respectively. As can be seen from the results, the proposed method has similar robustness compared with other methods.

In the blurring attack, the blurring radii are from 0.1 to 2 with an increment size 0.1. Fig.12 gives partial results with visual comparison and NC values. As can be seen from Fig.12, the proposed method is more robust than the other methods when the blurring radius is increasing.

In the common image processing, zoom in or zoom out of image will directly affect the image size and change the image pixels. At first, the watermarked image is scaled from 25% to 400% with an increment size 25%, respectively. Then, each scaled image is restored to the original size of 512 × 512 for extracting the watermark from the attacked image. Here, we give the comparison results with the scaling operations of 400% and 25% in Fig.13. As can be seen from Fig.13, the proposed method has stronger robustness than other methods when the watermarked image is magnified, however, the proposed method has weaker robustness when the watermarked image is reduced since the part of pixel values of watermarked image are deleted.

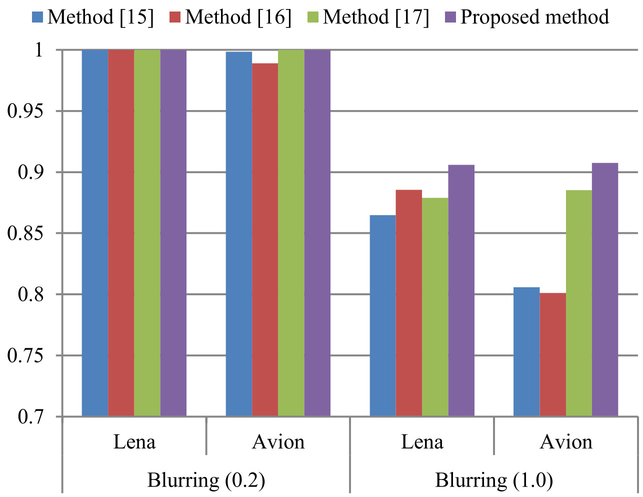


FIGURE 12. The comparison results of resisting the blurring attack.

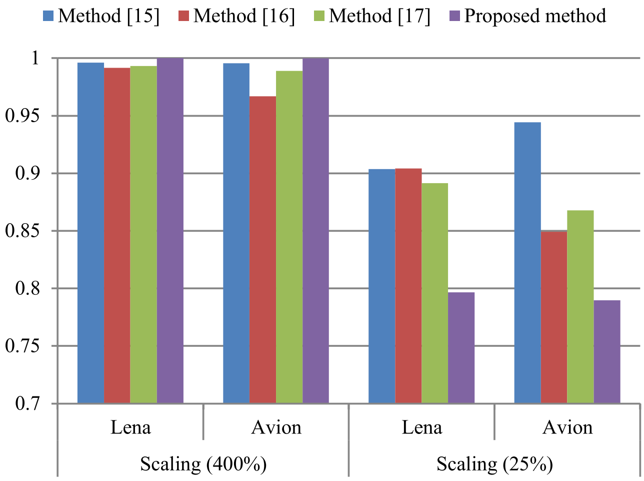


FIGURE 13. The comparison results of resisting the scaling attack.

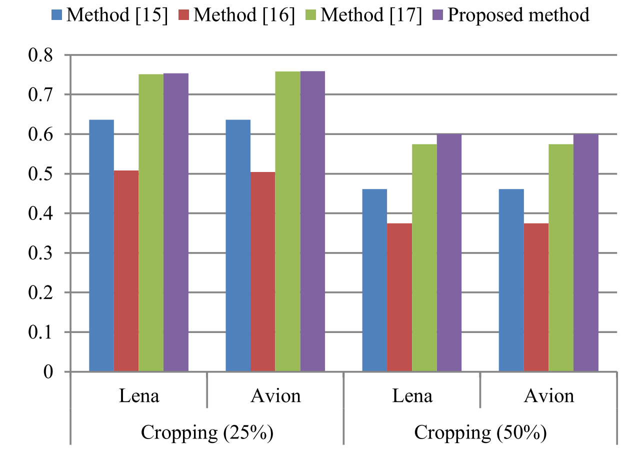


FIGURE 14. The comparison results of resisting the cropping attack.

Image cropping, as an image geometric attack, is often happened in the digital world. Here, the watermarked image is cropped from 5% to 50% with an increment size 5%.

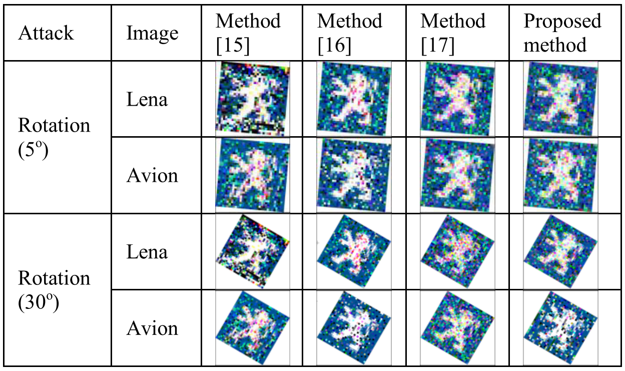


FIGURE 15. The comparison results of resisting the rotation attack.

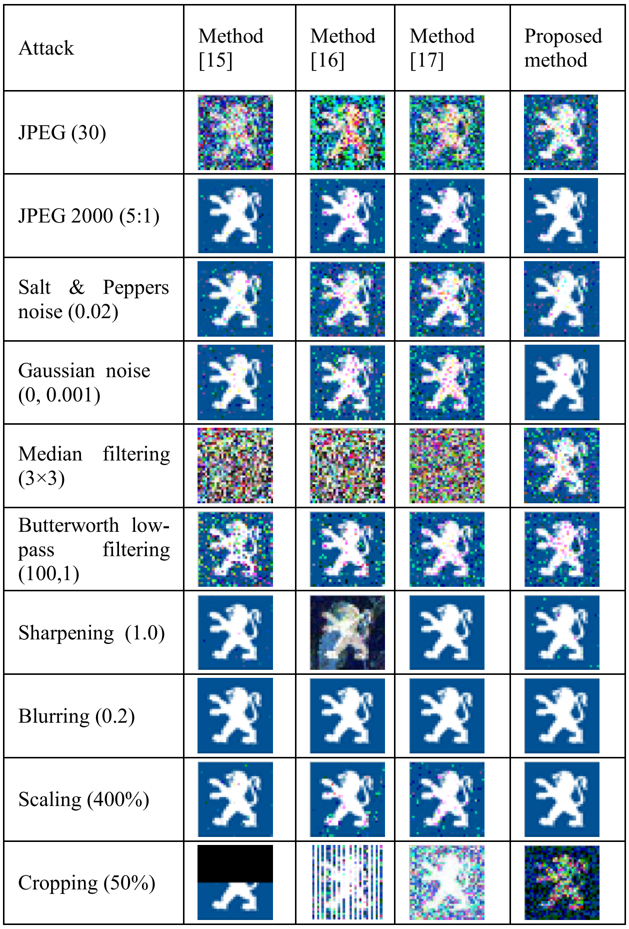


FIGURE 16. Robustness test results of "Lena" image.

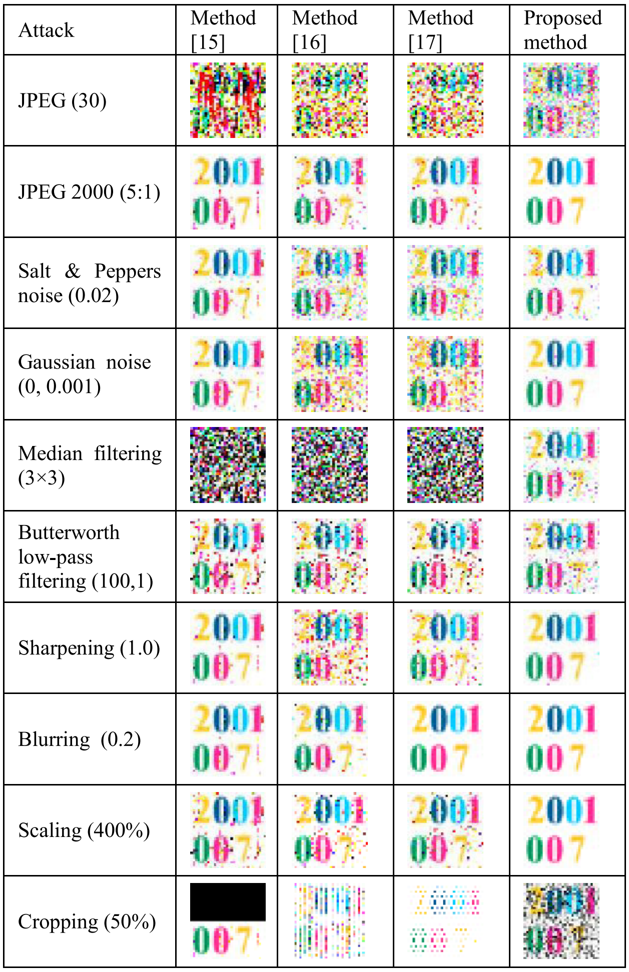


FIGURE 17. Robustness test results of "Peppers" image.

Fig. 14 gives the comparison results with cropping ratios 25% and 50%, respectively. These results show that the proposed method has stronger robustness than other methods under the different cropping operations, which because the embedding image blocks are randomly selected by the Hash pseudo-random replacement algorithm in this proposed method.

The average NC values of the different methods in Figs. 5-14 are 0.890365, 0.846005, 0.888197, and 0.925860, respectively. These results show that the proposed spatial method not only keep the robustness as the method in frequency domain, but also has stronger robustness than other methods in most cases.

As another kind of the image geometric attack, the image rotation is performed on the watermarked images. Firstly, the watermarked image is rotated with different degrees clockwise with 5° to 45° increasing with 5°. Secondly, each rotated image is resized to the original size 512 × 512 for extracting the watermark from the attacked image. Fig. 15 gives the comparison results with different rotation degrees. It is seen from the Fig. 15, the proposed method has similar robustness to other methods except the method [15].

Moreover, Fig. 16 gives the visual result of extracted watermark 1 with the host image "Lena", Fig. 17 gives the visual result of extracted watermark 2 with the host image "Peppers", Fig. 18 gives the visual result of extracted watermark 3 with the host image "House", and Fig. 19 gives the visual result of extracted watermark 4 with the host image "Avion". From these results, it can be concluded that the proposed method is more robust than the related methods, relatively.

In order to further prove the robustness, the proposed methods are also compared with the classic spatial domain

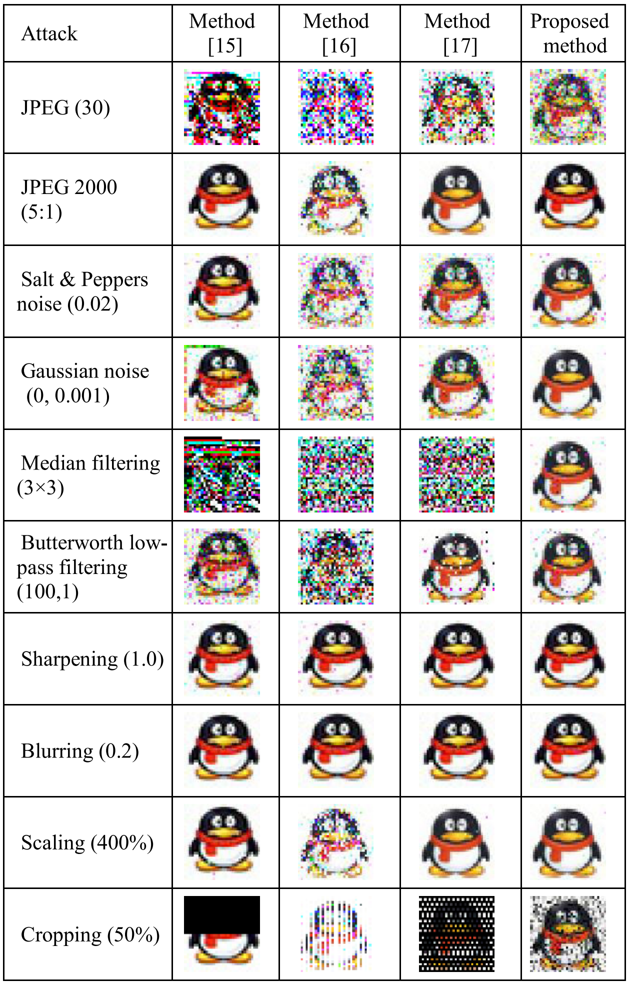


FIGURE 18. Robustness test results of "House" image.

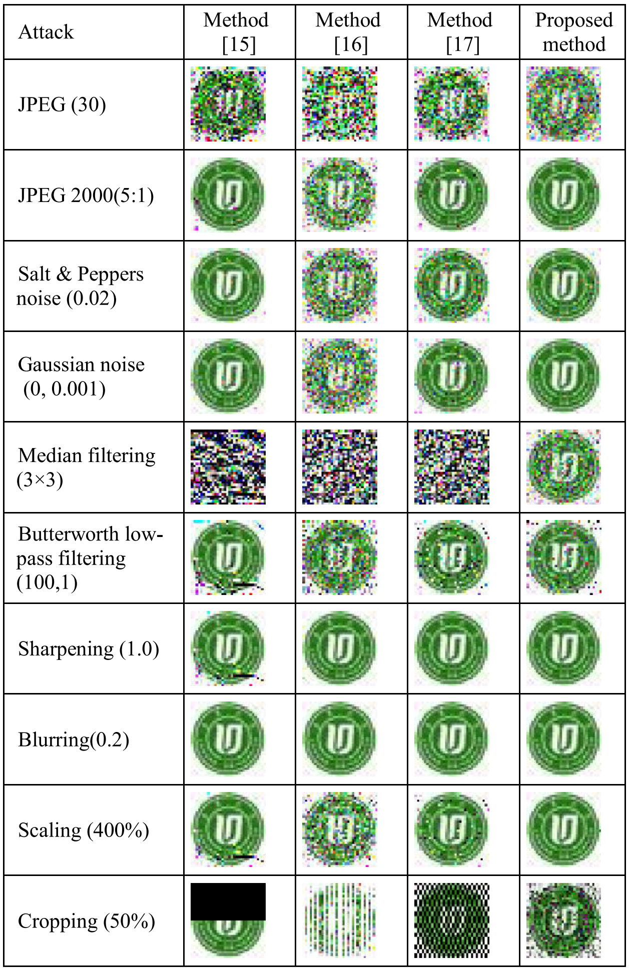


FIGURE 19. Robustness test results of "Avion" image.

TABLE 4. The comparison of execution times of the different methods (second).

Method	Embedding time	Extraction time	Total time
Method [9]	1.406568	1.105751	2.512319
Method [15]	0.979948	0.436173	1.416121
Method [16]	1.263168	0.591873	1.855041
Method [17]	1.736693	0.735674	2.472367
Proposed method	0.274117	0.238315	0.512432

method [9]. In method [9], the watermark image of Fig. 3(g) was taken as the watermark image. For fair comparison, we also use the watermark image to carry out the experiment with same attack styles in method [9]. Fig. 20 shows the comparison results using "Peppers", "TTU" as the host images. These results reveal that the proposed algorithm is more robust. In most cases, the performance of the proposed method is superior to that of the method in [9]. In [9], 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.

C. THE REAL-TIME FEATURE COMPARISON OF DIFFERENT METHODS

In this experiment, all methods are performed on the same platform of 2.27GHZ CPU, 2.00GB RAM, Win 7 and MATLAB 7.10.0 (R2010a). To compare the computation complexity of the different methods, the executive times of different methods are given in Table 4.

As can be seen from Table 4, the proposed method has shorter running time than other methods since the proposed method performs on the spatial domain, which only includes the simple algebra operation, although the proposed method uses the approximate maximum eigenvalue of Schur decomposition to embed and extract watermark. Hence, the main advantage of the proposed method is its real-time feature, which is more suitable to protect the copyright of multimedia big data.

D. THE SECURITY ANALYSIS

According to Kirchhoff's criterion, the security of information system relies on keys instead of privacy of scheme. In the

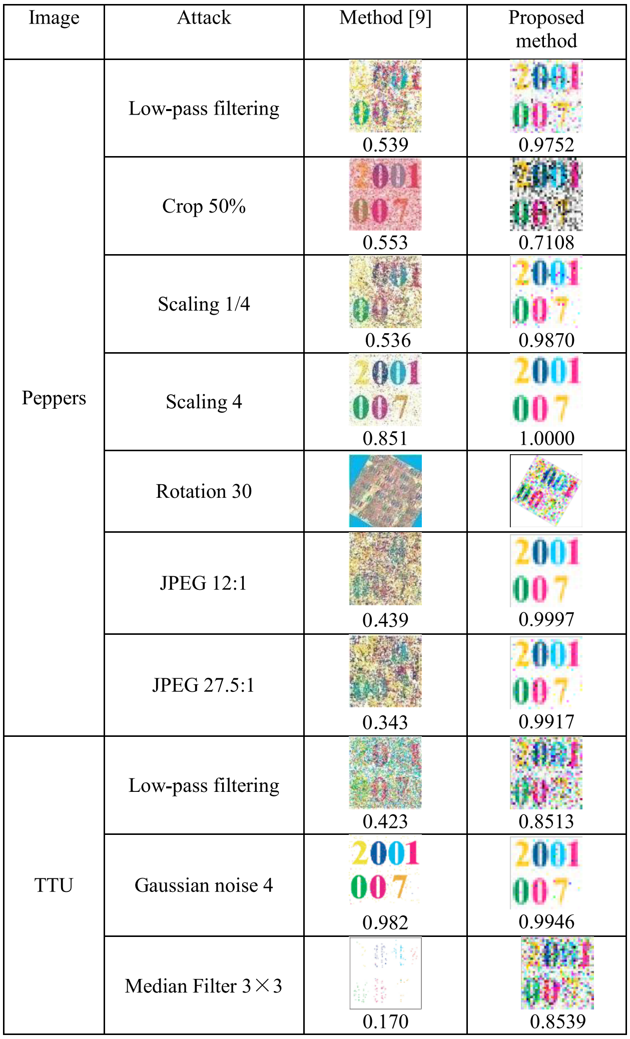


Image	Attack	Method [9]	Proposed method
Peppers	Low-pass filtering	0.539	0.9752
	Crop 50%	0.553	0.7108
	Scaling 1/4	0.536	0.9870
	Scaling 4	0.851	1.0000
	Rotation 30		
	JPEG 12:1	0.439	0.9997
	JPEG 27.5:1	0.343	0.9917
TTU	Low-pass filtering	0.423	0.8513
	Gaussian noise 4	0.982	0.9946
	Median Filter 3×3	0.170	0.8539

FIGURE 20. Robustness results compared to the classic spatial domain method.

proposed method, the security relies on the private keyKa_i and key Kb_i, $i \in \{1, 2, 3\}$.

The key Ka_i is used to select the permutation times, and it is determined by the memory type of integer number ($1 \sim 32768$), hence the length of each key Ka_i is 16, its key space of each key Ka_i is 2^{16}. So the permutation key space of the color watermark image is 2^{48}.

The key Kb_i is used to select the embedding image block, and it is determined by three factors: the host image size, the image block size, and the key of MD5, the key space of each factor is 2^9, 2^2, and 2^{16}, hence the key space of key Kb_i is 2^{27}. Hence, the key space of embedding image block is 2^{81}.

Hence the key space of the whole watermarking method is 2^{129}. Enough large key space can ensure the high security of the proposed color watermarking method.

E. EMBEDDING CAPACITY ANALYSIS

For comparing the embedding capacity of the proposed method with other related methods, we calculated their reality embedding capacity as shown in Table 5. The spatial domain method [9] has higher capacity than other methods. This is because this method [9] employs color quantization to all image pixels, while other methods use non-overlapping block technique and one block contains only 1 bit watermark information. Since one watermark bit can be embedded in each 4 × 4 image block in this paper, the maximum embedding capacity of the algorithm is $((512/4) \times (512/4) \times 3)/(512 \times 512 \times 3) = 0.0625$(Bit/Pixel). In fact, the 24-bit color watermark image of sized 32 × 32 is embedded to the host color image of sized 512 × 512, so the reality embedding capacity of this paper is $(32 \times 32 \times 24)/(512 \times 512 \times 3) = 0.03125$(Bit/Pixel). It is seen from the Table 5, the capacity of the proposed method is same as other methods [15]–[17] because the block size is 4 × 4.

TABLE 5. The comparison of reality embedding capacity between different methods.

Method	Watermark Lengt	Host image (Pixel)	Bit/Pixel
Method [9]	128×128×24	512×512×24	0.50000
Method [15]	32×32×24	512×512×3	0.03125
Method [16]	32×32×24	512×512×3	0.03125
Method [17]	32×32×24	512×512×3	0.03125
Proposed method	32×32×24	512×512×3	0.03125

VI. CONCLUSION

In order to protect the copyright of color images in multimedia big data, an approximate Schur decomposition-based watermarking technique was proposed in this paper. Firstly, a new approximate method was proposed to obtain the maximum eigenvalue of Schur decomposition in the spatial domain. Then, the approximate maximum eigenvalue was used to embed and extract watermark in the spatial domain not in the frequency domain. The highlight of this paper is that the watermarking technique was fulfilled in the spatial domain using the feature of Schur decomposition. Experimental results show that the proposed method not only has the real-time advantage as same as the watermarking technique in the spatial domain, but also has strong robustness advantage as same as the watermarking technique in the transform domain. In the future, we will consider how to extent this method to practical application.

REFERENCES

[1] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[2] Z. Zhou, Y. Wang, Q. M. J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 48–63, Jan. 2017.

[3] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 507–518, Mar. 2015.

[4] Z. Zhou, C.-N. Yang, B. Chen, X. Sun, Q. Liu, and Q. M. J. Wu, "Effective and efficient image copy detection with resistance to arbitrary rotation," *IEICE Trans. Inf. Syst.*, vol. E99-D, no. 6, pp. 1531–1540, Jun. 2016.

[5] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *J. Internet Technol.*, vol. 18, no. 2, pp. 435–442, Mar. 2017.

[6] Z. Xia, X. Wang, X. Sun, and B. Wang, "Steganalysis of least significant bit matching using multi-order differences," *Secur. Commun. Netw.*, vol. 7, no. 8, pp. 1283–1291, Aug. 2014.

[7] Q. Su, *Color Image Watermarking: Algorithms and Technologies*. Berlin, Germany: Walter de Gruyter, 2017, pp. 1–26.

[8] N. Singh and S. Singh, "The amalgamation of digital watermarking & cloud watermarking for security enhancement in cloud computing," *Int. J. Comput. Sci. Mobile Comput.*, vol. 2, no. 4, pp. 333–339, Apr. 2013.

[9] C.-H. Chou and T.-L. Wu, "Embedding color watermarks in color images," *EURASIP J. Adv. Signal Process.*, vol. 2003, no. 1, pp. 32–40, Jan. 2003.

[10] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *Int. J. Electron. Commun. AEU*, vol. 72, pp. 149–161, Feb. 2017.

[11] J. Wang and S. Lian, "On multiwatermarking in cloud environment," *Concurrency Comput. Pract. Exper.*, vol. 24, no. 17, pp. 2151–2164, Dec. 2012.

[12] Y. Ren, J. Shen, J. Wang, J. Xu, and L. Fang, "Security data auditing based on multifunction digital watermark for multimedia file in cloud storage," *Int. J. Multimedia Ubiquitous Eng.*, vol. 9, no. 9, pp. 231–240, Sep. 2014.

[13] X. Cao, Z. Fu, and X. Sun, "A privacy-preserving outsourcing data storage scheme with fragile digital watermarking-based data auditing," *J. Elect. Comput. Eng.*, vol. 2016, no. 4, pp. 1–7, Apr. 2016.

[14] X. Kong, B. Wang, and X. Li, "Multimedia information security: A review," (in Chinese), *J. Inf. Secur. Res.*, vol. 1, no. 1, pp. 44–53, Oct. 2015.

[15] S.-L. Jia, "A novel blind color images watermarking based on SVD," *Optik*, vol. 125, no. 12, pp. 2868–2874, Jun. 2014.

[16] Q. Su, Y. Niu, X. Liu, and Y. Zhu, "Embedding color watermarks in color images based on Schur decomposition," *Opt. Commun.*, vol. 285, no. 7, pp. 1792–1802, Apr. 2012.

[17] Q. Su and B. Chen, "An improved color image watermarking scheme based on Schur decomposition," *Multimedia Tools Appl.*, vol. 76, no. 22, pp. 24221–24249, Nov. 2017.

[18] G. H. Golub and C. F. Van Loan, *Matrix Computations*. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 1989, pp. 1–30.

[19] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 987–1009, Sep. 2014.

[20] A. Ostrowski, "Bounds for the greatest latent root of a positive matrix," *J. London Math. Soc.*, vol. 27, no. 2, pp. 253–256, Apr. 1952.

[21] R. L. Rivest, *The MD5 Message-Digest Algorithm*, document RFC 1321, Apr. 1992.

[22] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[23] University of Granada. *Computer Vision Group. CVG-UGR Image Database*. Accessed: Mar. 13, 2017. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/

[24] Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "A new algorithm of blind color image watermarking based on LU decomposition," *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1055–1074, Jul. 2018.

[25] A. Cedillo-Hernandez, M. Cedillo-Hernandez, M. N. Miyatake, and H. P. Meana, "A spatiotemporal saliency-modulated JND profile applied to video watermarking," *J. Vis. Commun. Image Represent.*, vol. 52, pp. 106–117, Apr. 2018.

[26] X.-W. Li, S.-T. Kim, and Q.-H. Wang, "Designing three–dimensional cellular automata based video authentication with an optical integral imaging generated memory-distributed watermark," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 7, pp. 1200–1212, Oct. 2017.

[27] R. A. Alotaibi and L. A. Elrefaei, "Improved capacity Arabic text watermarking methods based on open word space," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 30, no. 2, pp. 236–248, Apr. 2018.

[28] H.-T. Hu, J.-R. Chang, and S.-J. Lin, "Synchronous blind audio watermarking via shape configuration of sorted LWT coefficient magnitudes," *Signal Process.*, vol. 147, pp. 190–202, Jun. 2018.

[29] University of Southern California. *Signal and Image Processing Institute. USC-SIPI Image Database*. Accessed: Mar. 15, 2017. [Online]. Available: http://sipi.usc.edu/database/

QINGTANG SU received the master's degree in engineering from the School of Information and Electronic Engineering, Kunming University of Science and Technology, Kunming, China, in 2005, and the Ph.D. degree in control science and engineering from the East China University of Science and Technology, Shanghai, China, in 2013. He is currently an Associate Professor with the Department Information and Electric Engineering, Ludong University, Yantai, China. His research interests include image processing and information security.

ZIHAN YUAN received the bachelor's degree from the School of Computer Science and Technology, Jining Medical University, Jining, China, in 2018. She is currently pursuing the master's degree with the School of Information and Electrical Engineering, Ludong University, Yantai, China. Her research interests include image processing and information security.

DECHENG LIU received the bachelor's degree from the School of Information and Electrical Engineering, Ludong University, Yantai, China, in 2018, where he is currently pursuing the master's degree. His research interests include image processing and information security.