Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-08459-3

# A robust zero-watermarking algorithm for color image based on tensor mode expansion

Feifeng Jiang [1] · Tiegang Gao [1] · De Li [2]

Received: 31 July 2018 / Revised: 20 May 2019 / Accepted: 12 November 2019
Published online: 02 January 2020


**Abstract**
Digital zero-watermarking technology is an effective measure to protect image copyright, and many algorithms have been proposed based on zero-watermark. However, most of the existing zero-watermarking algorithms are designed for grayscale images. In this paper, a new zero-watermarking algorithm for color image based on tensor mode expansion is proposed. In the proposed scheme, four images of R, G, B, and gray are firstly generated from the original image. Then, the four images are appropriately combined to construct two three-dimensional tensors, and tensor expansion is performed on the obtained tensors. By performing singular value decomposition (SVD) and discrete cosine transform (DCT) on the expanded data, a feature image containing the main information of the host image can be generated. Finally, the feature image is fused with the specified logo image to obtain a zero-watermark image. Experimental results show that the proposed algorithm is robust to noise attacks and common image processing attacks, and better performances compared with some existing algorithms are also achieved. In addition, since the proposed algorithm is based on color images, it can make full use of all aspects of color images.

**Keywords** Zero-watermark · Tensor mode expansion · Singular value decomposition · Discrete cosine transform

✉ Tiegang Gao
gaotiegang@nankai.edu.cn

Feifeng Jiang
1036779510@qq.com

De Li
leader1223@ybu.edu.cn

[1] College of Software, Nankai University (Jinnan), Tianjin 300350, China

[2] Department of Computer Science, Yanbian University, Yanji 133000, China

## 1 Introduction

In recent years, the rapid development of technology has promoted the use of the Internet. This also allows multimedia data to be distributed in digital form via the Internet regardless of time or place. However, such data has certain security risks, because the internet users can download, modify, and copy multimedia data. These various actions described above make the copyright protection behavior of the owner difficult. As one of the information security technologies, digital zero-watermarking technology is an effective measure to guarantee the security of multimedia data.

The digital zero-watermarking technology is evolved from digital watermarking technology [1, 2]. And both have similarities in function and processing. The traditional digital watermarking technology mainly embeds some custom data into the carrier data, so as to achieve copyright protection of the original carrier data. In general, an effective digital watermarking algorithm needs to meet the demand of invisibility, and it's also necessary to have strong robustness against some common noise attacks and image processing attacks. At present, people have presented many digital watermarking algorithms with good performance. In [3], Wang et al. described a geometrically invariant image watermarking method using Radial Harmonic Fourier Moments (RHFMs). After analyzing the computing method of RHFMs and doing some research on the relationship between reconstruction performance and the number of RHFM, the proposed method uses a fast and precise method based on Fast Fourier Transformation (FFT) to calculate the RHFMs of the original image. And the next step is to modify the magnitudes of RHFMs for watermark embedding. Shao et al. constructed a watermarking algorithm for color image based on quaternion moment invariants and visual cryptography [4]. In their scheme, the quaternion representation is used to represent the color image as a quaternary matrix, such that each channel of the color image can be processed in a holistic manner. Moreover, the invariant features of the host image can be extracted by using the quaternion moment, so the proposed algorithm can be resilient to geometric attacks and common image processing attacks effectively. In [5], a watermarking method using discrete cosine transform was proposed. And it works on the YCoCg-R color space. The YCoCg-R color space is a reversible integer version of the YCoCg (Luminance Chrominance Orange Chroma Green) color space, while the YCoCg color space breaks down color images into Luminance (Y), Chrominance Orange (Co), and Chroma Green (Cg). Due to the good decorrelation of the YCoCg-R color space, the algorithm is robust to various attacks, and it is also highly resistant to JPEG compression. In [6], a robust watermarking system was showed, which was based on integer discrete cosine transform, non-linear chaotic map and dynamic stochastic resonance (DSR). The algorithm in that article combines the advantages of the above three techniques to make the algorithm relatively robust.

Although digital watermarking technology can provide security for multimedia data, embedding additional data into the host image will change the host image. For a good watermarking algorithm, it is necessary to ensure that there is no obvious visual difference between the host image before and after embedding the watermarking, so the less the embedded watermarking data, the less the impact on the host image, the higher the invisibility of the watermarking. However, considering the robustness of the algorithm, there is no doubt that the more the watermarking data, the better. In that way, when the host image is attacked, even if the extracted watermarking is not complete, effective information can be extracted from some correct data. Considering the above two aspects, it is difficult to satisfy both invisibility and robustness when designing a watermarking algorithm.

Due to the above shortcomings of digital watermarking technology, the digital zero-watermarking technology [7] was first proposed by Wen et al. in the early twenty-first century. The digital zero-watermarking technology [8] overcomes the limitation of digital watermarking technology, since invisibility and robustness can coexist in a zero-watermarking scheme. The key point of the digital zero-watermarking technique is "zero", which means that there is no modification and embedding of the host image throughout the process. The digital zero-watermarking technology mainly constructs a zero-watermark based on the feature data, which is extracted from a certain aspect of the host image. One aspect to note is that the feature data is usually unique and robust. This ensures that meaningful watermark images cannot be extracted using unrelated images.

### 1.1 Related works

In general, digital zero-watermarking technology can be divided into two categories according to its watermarking content, one is that only the feature data extracted from the host image is used to construct the zero-watermark; the second one is that the zero-watermark image contains two parts, a specific logo image and the feature data extracted from the host image, and most of zero-watermarking algorithms use the second scheme. In [9], a zero-watermarking method based on discrete wavelet transform (DWT) and edge detection was introduced. This method uses two-level DWT to extract the main information from the original image, and then performs edge detection to obtain the edge image. At last, the edge image is segmented and processed to obtain an encoding matrix for constructing a zero-watermark. In [10], Han et al. proposed a zero-watermarking algorithm combining lower-upper (LU) decomposition with Non-Subsampled Shearlet Transform (NSST). The proposed algorithm first converts the original image into the NSST domain, and randomly selects a sub-image using the logistic chaotic system; then, the sub-image is subjected to block processing, and each sub-block is further subjected to LU decomposition processing to complete the zero-watermark construction task. Experiments have proved that this zero-watermarking method has good robustness against enhanced noise, filtering, JPEG compression, cropping, etc. In [11], an image zero-watermarking scheme based on DWT and boost normed singular value decomposition (BN-SVD) was presented. In view of the fact that this method can eliminate the false positive problem and diagonal line problem found in traditional singular value decomposition, the robustness of this algorithm has been improved. In the zero-watermarking algorithm proposed in [12], DWT is also used as a key technique to process the host image. The paper shows two schemes, and the main difference between the two kinds of schemes is the order of block processing and DWT processing. However, the core idea of both is to use DWT and SVD to extract the feature data of the host image. At present, many digital zero-watermarking technologies with good performance are based on grayscale images. However, a color image contains more information available than a grayscale image, the focus of this paper is on color image.

### 1.2 Motivations and contributions

In order to make better use of the information in the host image, this paper proposes a robust zero-watermarking algorithm based on tensor mode expansion for color image. According to the proposed algorithm, a set of images are obtained at first, including three images corresponding to the three channels (R, G, B) and one gray image. Then, the proper combination based on this set of images is given so as to construct two three-dimensional tensors. Use

tensor expansion for both tensors and process the expanded data using singular value decomposition (SVD) and discrete cosine transform (DCT), respectively. After those operations, the feature image corresponding to the host image can be obtained. Using exclusive OR (XOR) processing, combining the feature image with the preprocessed logo image to construct a zero-watermark is the last step of the algorithm. Experimental results show that the proposed algorithm has good uniqueness, can resist noise attacks well, and has good robustness against other types of attacks such as image processing attacks.

### 1.3 Paper organization

The rest of the paper is organized as follows: tensor, tensor mode expansion, SVD and DCT are presented in section 2. Section 3 explains the proposed algorithm in detail. In section 4, the uniqueness and robustness of the algorithm are tested, and comparative experiments is also given in this part. The entire experiment is summarized in section 5.

## 2 Preliminaries

### 2.1 Tensor and tensor mode expansion

Tensor is an organization form of high-dimensional data, which can be regarded as a generalization of vectors [13, 14]. The scalar is zero-dimension, the vector is one-dimension, and the matrix is two-dimensional one. When the dimension of data is greater or equal to three, it's a very common choice to use the tensor for data representation.

When defining an n-dimensional tensor, first assign more than one position per dimension. At the same time, what needs to be done is to determine how the data of each dimension changes with the change of the coordinate system. In order to deal with a tensor of three or more dimensions easily, it is usually necessary to perform tensor mode expansion on the tensor.

Tensor mode expansion is the operation of converting high-dimensional tensor to matrix in accordance with the specified dimension. In the dimension reduction process, instead of reading data in order, the data of different dimensions is simultaneously read in a mixed interleaving manner. For example, a three-dimensional tensor A is shown in Fig. 1, and the corresponding module-expansion matrices are shown in formulas (1), (2), (3). When the scale of tensor A is $3 \times 2 \times 3$, the matrix of $3 \times 6$ can be obtained by expanding in the first dimension (keeping the first dimension unchanged). If you expand it by the second dimension, you can get a 2 by 9 matrix with keeping the second dimension constant. If you expand it by the third dimension, you keep the third dimension the same, and you will get a 3 by 6 matrix.

$$A_{(1)} = \begin{pmatrix} 1 & 2 & 7 & 8 & 13 & 14 \\ 3 & 4 & 9 & 10 & 15 & 16 \\ 5 & 6 & 11 & 12 & 17 & 18 \end{pmatrix} \tag{1}$$

$$A_{(2)} = \begin{pmatrix} 1 & 7 & 13 & 3 & 9 & 15 & 5 & 11 & 17 \\ 2 & 8 & 14 & 4 & 10 & 16 & 6 & 12 & 18 \end{pmatrix} \tag{2}$$

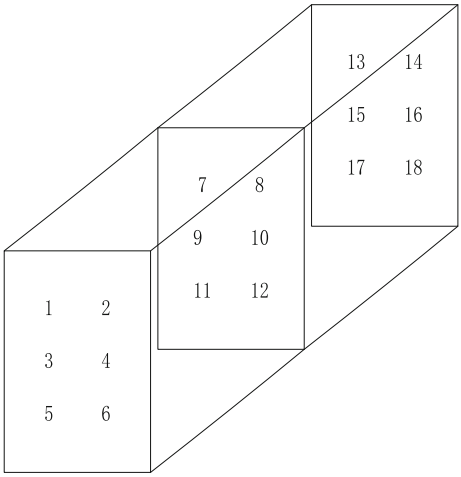



**Fig. 1** An example of three-dimensional tensor

$$A_{(3)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \end{pmatrix} \tag{3}$$

In the proposed algorithm, the tensor mode expansion is mainly used to reduce the dimensions of the three-dimensional data to obtain a two-dimensional matrix for processing. In terms of data distribution, the tensor mode expansion operation disturbs the data to a certain extent, but there is no loss of data, and the structural information between the data is also retained. Therefore, using the tensor mode expansion operation in the proposed algorithm has some positive effects on improving the robustness of the algorithm.

## 2.2 Singular value decomposition (SVD)

The definition of Singular Value Decomposition (SVD) can be described as follows (referring to the Fig. 2) [15–17]. Given a non-negative matrix M, the singular value decomposition of matrix M is given in the following formula:

$$M = U\Sigma V^T \tag{4}$$

where, U is called the left singular matrix, V is called the right singular matrix, and the former satisfies the condition that $UU^T = I$, the latter satisfies the condition that $VV^T = I$ (that is, U and V are both unitary matrices). $\Sigma$ is an m × n diagonal matrix, that is, only the elements on the diagonal are non-zero, and the elements on the diagonal are also the singular values of the matrix M. Similar to the eigenvalues in the eigen-decomposition, the elements in the $\Sigma$ matrix have only the data of the previous part being non-zero. Besides, $\Sigma$ satisfies the condition: $\Sigma_{1,1} \geq \Sigma_{2,2} \geq \cdots \geq \Sigma_{r,r} > 0$.

Singular value decomposition can transform a complex matrix into the product of several simpler matrices, and extract the important information (i.e. non-zero singular value) from the original matrix. By applying singular value decomposition, it can simplify the processing of large-scale data in the image. Besides, the extracted singular values are capable of demonstrating the intrinsic characteristics of the image, and they have high stability, which can help to improve the robustness of the algorithm [18].

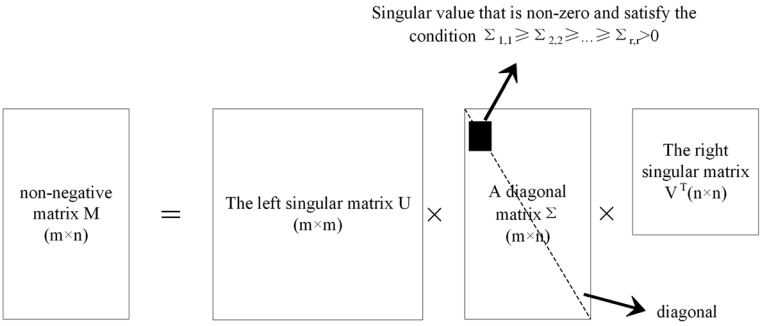



**Fig. 2** Singular value decomposition

### 2.3 Discrete cosine transform (DCT)

Discrete Cosine Transform (DCT) is a transformation method that takes Cosine Transform as the kernel of transformation [19, 20]. It can compress data or images mainly by adjusting the distribution density of data. This method enables the energy to be concentrated in the upper left corner, while most of the rest is close to zero. According to the different signal dimensions, it can be divided into one-dimensional discrete cosine transform and two-dimensional discrete cosines transform, and the former is the basis of the latter.

The most common form of one-dimensional discrete cosine transform is as follows:

$$F(u) = c(u)\sum_{i=0}^{N-1} f(i)\cos\left[\frac{(i+0.5)\pi}{N}u\right] \tag{5}$$

$$c(u) = \begin{cases} \sqrt{\frac{1}{N}}, u=0 \\ \sqrt{\frac{2}{N}}, u\neq 0 \end{cases} \tag{6}$$

where, f represents the original input signal, F(u) represents the coefficient output after the discrete cosine transform, N is the number of points of the original input signal, and c(u) here can be considered as a compensation coefficient, whose purpose is to make the DCT transform matrix an orthogonal matrix.

The two-dimensional discrete cosine transform is based on the one-dimensional discrete cosine transform. The difference between the two is that the discrete cosine transform is performed in the case of two dimensions once more than in the case of one dimension. The transformation form of two-dimensional discrete cosine transform is as follows.

$$F(u,v) = c(u)c(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cos\left[\frac{(i+0.5)\pi}{N}u\right]\cos\left[\frac{(j+0.5)\pi}{N}v\right] \tag{7}$$

$$c(u) = \begin{cases} \sqrt{\frac{1}{N}}, u=0 \\ \sqrt{\frac{2}{N}}, u\neq 0 \end{cases} \tag{8}$$

Similarly, f(i, j) is the original input signal, and F(u, v) is the coefficient output after the two-dimensional discrete cosine transform.

Discrete cosine transform will concentrate data energy on the low-frequency part and reduce the correlation between data. Therefore, when the discrete cosine transform is used in the proposed algorithm, and only low-frequency data are selected to construct the zero-

watermark, it will not affect the extraction of the main features, but reduces the amount of data and facilitates subsequent processing. In addition, since the discrete cosine transform is the basis of JPEG compression, the resistance of the algorithm to JPEG compression attacks can be enhanced due to the use of the discrete cosine transform.

## 3 Robust zero-watermarking algorithm

### 3.1 Processing of host images

As Shown in Fig. 3, the detailed processing of the host image $\boldsymbol{I}$ can be described in the following steps:

(1) Transform the original RGB host image $\boldsymbol{I}$ into some images of different channels, they are images of R, G and B channels and grayscale image, marked as $\boldsymbol{R}$, $\boldsymbol{G}$, $\boldsymbol{B}$ and $\boldsymbol{Gray}$.
(2) Combine image data in $\boldsymbol{G}$, $\boldsymbol{Gray}$ and $\boldsymbol{G}$ order to construct a three-dimensional tensor $\boldsymbol{T_1}$. The second three-dimensional tensor $\boldsymbol{T_2}$ is constructed in the order of $\boldsymbol{R}$, $\boldsymbol{R}$ and $\boldsymbol{B}$.

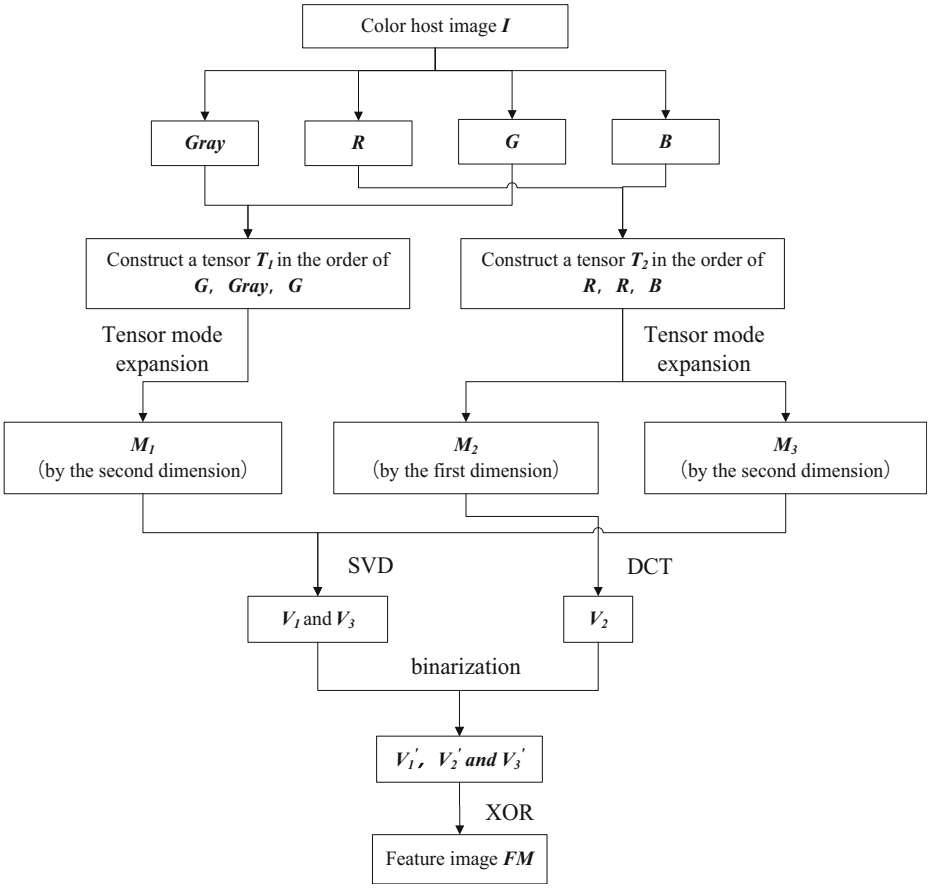



**Fig. 3** Processing of host images

(3) Expand $T_1$ according to the second dimension to obtain $M_1$ matrices; $T_2$ is expanded according to the first and the second dimension, and $M_2$ and $M_3$ matrices are obtained.
(4) $M_1$ and $M_3$ are processed by SVD, respectively, to obtain $V_1$ and $V_3$.
(5) Perform 2*2 block DCT transform on $M_2$, extract low frequency part of the frequency domain to obtain a matrix, labeled as $V_2$.
(6) Calculate the mean of the matrices $V_1$, $V_2$, and $V_3$, respectively, and binarize the three matrices according to the mean. After the binarization process, the results are labeled $V_1'$, $V_2'$, and $V_3'$.
(7) By performing XOR operation on $V_1'$, $V_2'$, and $V_3'$, a final feature image $FM$ can be obtained for subsequent steps.

One thing to note here is that there are many ways to combine the four graphs $R$, $G$, $B$, and $Gray$ when constructing two three-dimensional tensors. After some experiments, it is found that the combination of $G$, $Gray$, $G$ and $R$, $R$, $B$ is better. In addition, in this experiment, the tensor expansion of $T_1$ is performed, but only the data of the second dimension is selected, because the experimental results are not good if the data of the first dimension is added.

### 3.2 Zero-watermark generation

Zero- watermark generation includes the following steps, as shown in Fig. 4:

(1) The host image $I$ and the logo image $L$ are separately preprocessed to obtain the feature image $FM$ and the processed logo image $L'$. The preprocessing of the host image $I$ is according to 3.1, and the preprocessing of the logo image $L$ is Hadamard spread spectrum and Logistic scrambling.
(2) Apply an XOR operation between the feature matrix $FM$ and $L'$ to generate the zero-watermark image named $W$.

### 3.3 Zero-watermark extraction

The following two steps can be used to describe the zero-watermark extraction, as shown in Fig. 5:

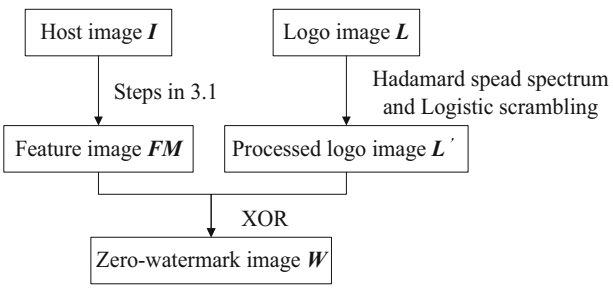



**Fig. 4** Zero-watermark generation

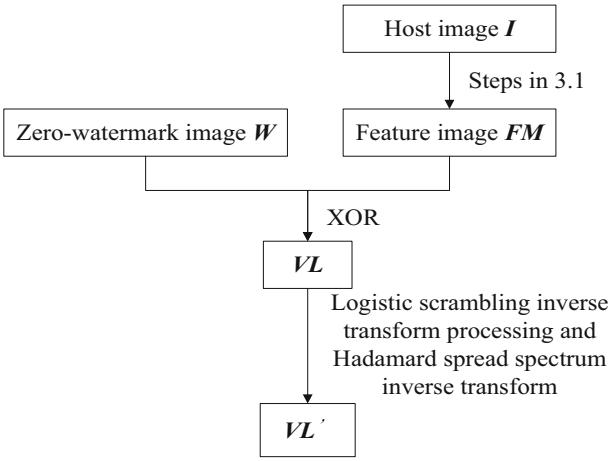



**Fig. 5** Zero-watermark extraction

(1) Perform XOR on the feature image ***FM*** and the zero-watermark image ***W*** to generate the ***VL***. Here, ***FM*** is derived from the host image ***I*** according to the steps in 3.1.
(2) Perform preprocessing inverse transformation (Logistic scrambling inverse transform processing and Hadamard spread spectrum inverse transform) on ***VL*** to obtain a logo image named ***VL***', and ***VL***' is used to verify the performance of the algorithm by comparing it to the correct logo image.

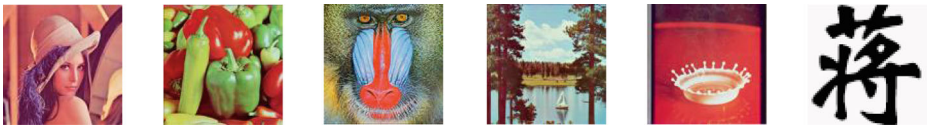
## 4 Experimental results and analysis

As shown in the Fig. 6, the original host images [21] used in the experiment are color images with 512 × 512 pixels, including Lena, Pepper, Mandrill, Sailboat on lake and Splash. The logo image is a binary image of the Chinese character "jiang" with 64 × 64 pixels. In this paper, the Bit Error Ratio (BER) and the Normalized Correlation Coefficient (NC) are selected to evaluate the uniqueness and robustness of the proposed algorithm. In general, BER refers to the proportion of erroneous bits in the extracted logo image, based on the correct logo image. It is defined in formula (9)

$$\mathrm{BER} = \frac{\mathrm{B}}{\mathrm{P} \times \mathrm{Q}} \times 100\% \tag{9}$$

where B is the number of erroneously detected bits,P × Qis the size of the extracted logo image. NC refers to the degree of similarity between the extracted logo image and the correct logo image. And the formula for NC is given by:

$$\mathrm{NC} = \frac{\sum_x \sum_y W(wx, wy) W'(wx, wy)}{\sqrt{\sum_x \sum_y W^2(wx, wy)} \sqrt{\sum_x \sum_y W'^2(wx, wy)}} \tag{10}$$



(a) Lena (b) Pepper (c) Mandrill (d) Sailboat on lake (e) Splash (f) Jiang

**Fig. 6** Images used in the experiment

where W($wx$, $wy$) means the correct logo image, and W'($wx$, $wy$) means the extracted logo image.

### 4.1 Uniqueness detection

Since the feature images generated from different host images are different, the zero-watermarks derived from different images should also be different, that is, the correlation between zero-watermarks generated by different images should be relatively small. In addition, in theory, if you use other images to extract the logo image instead of using the original host image, the correlation between the extracted logo image and the correct logo image should be relatively low. So the uniqueness test is firstly carried out, and the performance of the proposed scheme is shown in the Table 1. According to the data in Table 1, the NC has a maximum of 0.7289, and its corresponding logo image is shown in Fig. 7. Even if the NC is 0.7289, it is difficult to obtain useful information from the extracted logo image, so the algorithm has good uniqueness.

### 4.2 Robustness detection

For digital zero-watermarking scheme, it is necessary to make the algorithm robust while ensuring good uniqueness. When testing the robustness of the algorithm, the attack types include Gaussian noise, salt and pepper noise, speckle noise, Poisson attack, etc. Detailed experimental data are shown in the Tables 2 and 3. Tables 2 and 3 recorded BER and NC respectively, and the five host images mentioned above are tested. In Table 2, the BER higher than 0.0100 is thickened, and similarly, in Table 3, the NC below 0.9900 is thickened.

According to the horizontal analysis results of the data in the two tables, if the Gaussian noise (mean = 0, variance = 0.01), JPEG (QF = 10) and the cropping attack of each orientation are used for the host image, in the five experiments corresponding to the five host images, there are more than three experiments, in which the NC is less than 0.9900 and the BER is

**Table 1** NC values obtained after extracting zero-watermark using different images based on five host images

| | Lena | Pepper | Mandrill | Sailboat on lake | Splash |
|---|---|---|---|---|---|
| Lena | 1 | 0.5996 | 0.6156 | 0.6116 | **0.7289** |
| Pepper | 0.5996 | 1 | 0.5680 | 0.6063 | 0.5911 |
| Mandrill | 0.6156 | 0.5680 | 1 | 0.5633 | 0.4899 |
| Sailboat on lake | 0.6116 | 0.6063 | 0.5633 | 1 | 0.6507 |
| Splash | 0.7289 | 0.5911 | 0.4899 | 0.6507 | 1 |

**Fig. 7** The logo image associated with the NC value equal to 0.7289 in Table 1

greater than 0.0100. The above phenomenon shows that under these three types of attacks, the robustness of the algorithm is relatively weak.

Next, by observing the data in the two tables in a longitudinal view, it can be found that if Mandrill.jpg is used as host images, the experiment does not achieve relatively good robustness.

Although this experiment has the above shortcomings, according to the data of the two tables, most of the BER is still less than 0.0100, and most of the NC is close to 1.0000,

**Table 2** BER of five host images under different attacks

| Attacking description | | Lena | Pepper | Mandrill | Sailboat on lake | Splash |
|---|---|---|---|---|---|---|
| Gaussian noise (mean = 0, variance = 0.01) | | 0.0059 | **0.0171** | **0.0325** | **0.0103** | **0.0146** |
| Salt and pepper noise (intensity = 0.01) | | 0.0017 | 0.0015 | **0.0144** | 0.0081 | 0.0007 |
| Speckle noise (intensity = 0.01) | | 0.0015 | 0.0020 | **0.0168** | 0.0020 | 0.0015 |
| Poisson attack | | 0.0037 | 0.0006 | **0.0127** | 0.0032 | 0.0007 |
| 4-neibourhood filtering | | 0.0002 | 0.0004 | 0.0049 | 0.0017 | 0.0004 |
| 8-neibourhood filtering | | 0.0002 | 0.0009 | 0.0044 | 0.0024 | 0.0004 |
| Median filtering (window size = 3 × 3) | | 0.0017 | 0.0007 | 0.0059 | 0.0054 | 0.0015 |
| Scaling attack | scaling ratio = 2 | 0.0006 | 0.0020 | **0.0129** | 0.0022 | 0.0017 |
| | scaling ratio = 1.5 | 0.0012 | 0.0004 | 0.0076 | 0.0061 | 0.0006 |
| | scaling ratio = 1.2 | 0.0015 | 0.0015 | 0.0054 | 0.0032 | 0.0002 |
| | scaling ratio = 0.8 | 0.0017 | 0.0004 | 0.0063 | 0.0024 | 0.0002 |
| | scaling ratio = 0.5 | 0.0022 | 0.0007 | 0.0090 | 0.0042 | 0.0002 |
| | scaling ratio = 0.25 | 0.0037 | 0.0027 | **0.0181** | 0.0059 | 0.0020 |
| JPEG | QF = 90 | 0 | 0 | 0.0012 | 0.0012 | 0 |
| | QF = 70 | 0 | 0 | 0.0037 | 0.0024 | 0.0007 |
| | QF = 50 | 0.0006 | 0.0024 | 0.0049 | 0.0015 | 0.0004 |
| | QF = 40 | 0.0012 | 0.0020 | 0.0090 | 0.0022 | 0.0007 |
| | QF = 30 | 0.0007 | **0.0256** | **0.0105** | 0.0034 | 0 |
| | QF = 20 | 0.0032 | 0.0027 | **0.0186** | 0.0051 | 0.0004 |
| | QF = 10 | **0.0151** | **0.0308** | **0.0669** | 0.0071 | 0.0020 |
| cropping attack (32 × 32) | Upper left corner | **0.0144** | **0.0525** | **0.0454** | **0.0754** | 0.0095 |
| | Lower left corner | **0.0117** | **0.0381** | **0.0479** | **0.0251** | **0.0769** |
| | Upper right corner | **0.0112** | **0.0122** | **0.0366** | **0.0234** | **0.0227** |
| | Lower right corner | **0.1042** | **0.0100** | **0.1089** | **0.0281** | **0.0217** |

**Table 3** NC values of five host images under different attacks

| Attacking description | | Lena | Pepper | Mandrill | Sailboat on lake | Splash |
|---|---|---|---|---|---|---|
| Gaussian noise (mean = 0, variance = 0.01) | | 0.9955 | **0.9869** | **0.9750** | 0.9921 | **0.9888** |
| Salt and pepper noise (intensity = 0.01) | | 0.9987 | 0.9989 | **0.9890** | 0.9938 | 0.9993 |
| Speckle noise (intensity = 0.01) | | 0.9989 | 0.9985 | **0.9871** | 0.9985 | 0.9989 |
| Poisson attack | | 0.9972 | 0.9994 | 0.9903 | 0.9976 | 0.9993 |
| 4-neibourhood filtering | | 0.9998 | 0.9996 | 0.9963 | 0.9987 | 0.9996 |
| 8-neibourhood filtering | | 0.9998 | 0.9991 | 0.9966 | 0.9981 | 0.9996 |
| Median filtering (window size = 3 × 3) | | 0.9987 | 0.9993 | 0.9955 | 0.9959 | 0.9989 |
| Scaling attack | scaling ratio = 2 | 0.9994 | 0.9985 | 0.9901 | 0.9983 | 0.9987 |
| | scaling ratio = 1.5 | 0.9991 | 0.9996 | 0.9942 | 0.9953 | 0.9994 |
| | scaling ratio = 1.2 | 0.9989 | 0.9989 | 0.9959 | 0.9976 | 0.9998 |
| | scaling ratio = 0.8 | 0.9987 | 0.9996 | 0.9951 | 0.9981 | 0.9998 |
| | scaling ratio = 0.5 | 0.9983 | 0.9993 | 0.9931 | 0.9968 | 0.9998 |
| | scaling ratio = 0.25 | 0.9972 | 0.9979 | **0.9861** | 0.9955 | 0.9985 |
| JPEG | QF = 90 | 1 | 1 | 0.9991 | 0.9991 | 1 |
| | QF = 70 | 1 | 1 | 0.9972 | 0.9981 | 0.9993 |
| | QF = 50 | 0.9994 | 0.9981 | 0.9963 | 0.9989 | 0.9996 |
| | QF = 40 | 0.9991 | 0.9985 | 0.9931 | 0.9983 | 0.9993 |
| | QF = 30 | 0.9993 | **0.9803** | 0.9920 | 0.9974 | 1 |
| | QF = 20 | 0.9976 | 0.9979 | **0.9858** | 0.9961 | 0.9996 |
| | QF = 10 | **0.9884** | **0.9763** | **0.9481** | 0.9946 | 0.9985 |
| cropping attack (32 × 32) | Upper left corner | **0.9889** | **0.9595** | **0.9650** | **0.9414** | 0.9927 |
| | Lower left corner | 0.9910 | **0.9706** | **0.9630** | **0.9807** | **0.9402** |
| | Upper right corner | 0.9914 | 0.9907 | **0.9718** | **0.9820** | **0.9826** |
| | Lower right corner | **0.9185** | 0.9923 | **0.9149** | **0.9784** | **0.9833** |

indicating that the proposed algorithm is still effective against various types of attacks. In addition, it should be noted that since the original host image lacks a part of the data due to the

**Table 4** The comparison on BER between the proposed algorithm and Wang's method

| Attacking description | the proposed algorithm | Wang's method [22] |
|---|---|---|
| Median filtering (window size = 3 × 3) | **0.0030** | 0.0049 |
| Gaussian noise (mean = 0, variance = 0.01) | 0.0160 | **0.0131** |
| pepper and salt noise (intensity = 0.01) | **0.0052** | 0.0088 |
| Scaling attack (scaling ratio = 0.25) | **0.0064** | 0.0151 |
| Scaling attack (scaling ratio = 0.5) | **0.0032** | 0.0115 |
| Scaling attack (scaling ratio = 0.8) | **0.0022** | 0.0068 |
| Scaling attack (scaling ratio = 1.2) | **0.0023** | 0.0056 |
| Scaling attack (scaling ratio = 1.5) | 0.0031 | **0** |
| Scaling attack (scaling ratio = 2.0) | 0.0038 | **0** |
| Rotation without cropping (angle = 0.25°) | **0.0037** | 0.0122 |
| Rotation without cropping (angle = 0.5°) | **0.0027** | 0.0254 |
| Rotation without cropping (angle = 0.75°) | **0.0034** | 0.0378 |
| Rotation without cropping (angle = 1°) | **0.0029** | 0.0466 |
| Rotation without cropping (angle = 2°) | **0.0039** | 0.0750 |
| JPEG (QF = 90) | 0.0004 | **0** |
| JPEG (QF = 70) | **0.0013** | 0.0034 |
| JPEG (QF = 50) | **0.0019** | 0.0056 |
| JPEG (QF = 40) | **0.0030** | 0.0066 |
| JPEG (QF = 30) | 0.0080 | **0.0075** |
| JPEG (QF = 10) | 0.0243 | **0.0156** |

**Table 5** The comparison on BER between the proposed algorithm and Shen's algorithm

| Attacking description | the proposed algorithm | Shen's method [23] |
|---|---|---|
| JPEG (QF = 90) | **0.0004** | 0.0078 |
| JPEG (QF = 70) | **0.0013** | 0.0127 |
| JPEG (QF = 50) | **0.0019** | 0.0166 |
| JPEG (QF = 30) | **0.0080** | 0.0361 |
| JPEG (QF = 25) | **0.0041** | 0.0420 |
| JPEG (QF = 15) | **0.0077** | 0.0850 |
| JPEG (QF = 10) | **0.0243** | 0.1094 |
| Gaussian noise (mean = 0, variance = 0.05) | **0.0560** | 0.0791 |
| pepper and salt noise (intensity = 0.01) | **0.0052** | 0.0283 |
| Median filtering (window size = 3 × 3) | **0.0030** | 0.0488 |

cropping attack, the BER is greater than 0.0100 and the NC is less than 0.9900 regardless of which image is used as the host image in the experiment. But even so, most of the BER is still maintained below 0.0500, and most of the NC is above 0.9500.

### 4.3 Comparisons with some existing schemes

In view of the following facts: first, most of the existing zero-watermarking algorithms are based on grayscale images; secondly, there are almost no zero-watermarking algorithms using tensors, so it is difficult to find some similar algorithms for comparison. In order to make the algorithm proposed in this paper more convincing, this paper selects three algorithms with good performance for comparison experiments. Among these three zero-watermarking algorithms, the zero-watermarking algorithm in [22] is most similar to the algorithm proposed in this paper, both of which are designed for color images, while the zero-watermarking algorithms in [23, 24] are both applied to grayscale images. Therefore, compared with the algorithm in [23, 24], the proposed algorithm has obvious advantages, that is, it uses color images as the host image. This measure can make full use of all aspects of color images. For the sake of achieving more precise results, the results are obtained by averaging the BER of five experimental groups based on five host images. The detailed comparison results are shown in Tables 4, 5, and 6. Analysis of the above three tables can lead to the following conclusions: The proposed algorithm is

**Table 6** The comparison on BER between the proposed algorithm and Wang's algorithm

| Attacking description | the proposed algorithm | Wang's method [24] |
|---|---|---|
| Median filtering (window size = 3 × 3) | **0.0030** | 0.0098 |
| Gaussian noise (mean = 0, variance = 0.001) | 0.0461 | **0.0020** |
| pepper and salt noise (intensity = 0.001) | **0.0006** | 0.0020 |
| Scaling attack (scaling ratio = 0.5) | **0.0032** | 0.0078 |
| Scaling attack (scaling ratio = 0.8) | **0.0022** | 0.0049 |
| Scaling attack (scaling ratio = 1.3) | **0.0023** | 0.0049 |
| Scaling attack (scaling ratio = 1.5) | **0.0031** | 0.0049 |
| JPEG (QF = 30) | 0.0080 | **0.0049** |
| JPEG (QF = 40) | **0.0030** | 0.0059 |
| JPEG (QF = 50) | **0.0019** | 0.0059 |
| JPEG (QF = 70) | **0.0013** | 0.0020 |
| JPEG (QF = 90) | 0.0004 | **0** |

weaker than the algorithms in [22, 24], when resisting some attacks, but the proposed algorithm is significantly more robust than the algorithm in [23].

## 5 Conclusion

Different from most of the zero-watermarking algorithms which are based on gray images, a new zero-watermarking algorithm based on tensor mode expansion for color image is proposed. As the three channel images R, G, and B and the grayscale image are combined and utilized, the information of each aspect of the color image is comprehensively used. Moreover, by using the tensor mode expansion operation, data of different dimensions can be transmitted and fused, so that the image data can be scrambled to some extent. After doing tensor mode expansion, some of the data are processed by extracting the singular value with high stability and the other part are processed with DCT to extract the low frequency part containing a large amount of energy. Then, the two parts of data are merged to generate a feature image corresponding to the original host image for subsequent operations. In the experiment, the characteristics of SVD, tensor mode expansion and DCT are fully utilized, which makes the algorithm have better performance than most existing algorithms.

**Acknowledgements** The work was supported by the Program of Natural Science Fund of Tianjin, China (Grant NO. 16JCYBJC15700).

## References

1. Potdar VM, Han S, Chang E (2005) A survey of digital image watermarking techniques. https://doi.org/10.1109/INDIN.2005.1560462
2. Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12(1):122–138. https://doi.org/10.1016/s1665-6423(14)71612-8
3. Wang CP, Wang XY, Xia ZQ (2016) Geometrically invariant image watermarking based on fast radial harmonic fourier moments. Signal Process Image Commun 45(C):10–23. https://doi.org/10.1016/j.image.2016.03.007
4. Shao Z, Shang Y, Rui Z, Shu H, Coatrieux G, Wu J (2016) Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography. Signal Process Image Commun 48:12–21. https://doi.org/10.1016/j.image.2016.09.001
5. Moosazadeh M, Ekbatanifard G (2017) An improved robust image watermarking method using dct and ycocg-r color space. Optik Int J Light Electron Opt 140:975–988. https://doi.org/10.1016/j.ijleo.2017.05.011
6. Singh SP, Bhatnagar G (2018) A new robust watermarking system in integer dct domain. J Vis Commun Image Represent 53:86–101. https://doi.org/10.1016/j.jvcir.2018.03.006
7. Quan W, Tanfeng S, Shuxun W (2003) Concept and application of zero-watermark. Acta Electron Sin 31(2):214–216. https://doi.org/10.3321/j.issn:0372-2112.2003.02.015
8. Leng XX, Xiao J, Li DY, Shen ZY (2013) Study on the digital image zero-watermarking technology. Adv Mater Res 5:765–767. https://doi.org/10.4028/www.scientific.net/AMR.765-767.1113
9. Li Z, Peng C, Tian X, Xia S (2011) A novel zero-watermarking algorithm based on DWT and edge detection. Int Congr Image Signal Process. https://doi.org/10.1109/CISP.2011.6100325
10. Han SC, Zhang ZN (2013) A novel zero-watermark algorithm based on LU decomposition in NSST domain. IEEE Int Conf Signal Process. https://doi.org/10.1109/ICoSP.2012.6491884
11. Rao YR, Nagabhooshanam E (2015) A novel image zero-watermarking scheme based on DWT-BN-SVD. Int Conf Inf Commun Embed Syst. https://doi.org/10.1109/ICICES.2014.7034073
12. Rani A, Bhullar AK, Dangwal D, Kumar S (2015) A zero-watermarking scheme using discrete wavelet transform. Procedia Comput Sci 70:603–609. https://doi.org/10.1016/j.procs.2015.10.046

13. Qiang Z, Wang Y, Levine MD, Yuan X, Long W (2015) Multisensor video fusion based on higher order singular value decomposition. Inf Fusion 24(C):54–71. https://doi.org/10.1016/j.inffus.2014.09.008
14. Luo X, Zhang Z, Zhang C, Wu X (2017) Multi-focus image fusion using hosvd and edge intensity. J Vis Commun Image Represent 45(C):46–61. https://doi.org/10.1016/j.jvcir.2017.02.006
15. Ali M, Chang WA, Pant M (2014) A robust image watermarking technique using svd and differential evolution in dct domain. Optik Int J Light Electron Opt 125(1):428–434. https://doi.org/10.1016/j.ijleo.2013.06.082
16. Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on dwt-svd. Comput Stand Interfaces 31(5):1002–1013. https://doi.org/10.1016/j.csi.2008.09.031
17. Goléa EH, Seghir R, Benzid R (2010) A bind RGB color image watermarking based on singular value decomposition. IEEE/ACS Int Conf Comput Syst Appl. https://doi.org/10.1109/AICCSA.2010.5586967
18. Andrews HC, Patterson CL (1976) Singular value decompositions and digital image processing. IEEE Trans Acoust Speech Signal Process 24(1):26–53. https://doi.org/10.1109/TASSP.1976.1162766
19. Zhi Z, Wang C, Xiao Z (2017) Image watermarking scheme based on Arnold transform and DWT-DCT-SVD. IEEE Int Conf Signal Proces. https://doi.org/10.1109/ICSP.2016.7877942
20. Umaroh L, Sari CA, Astuti YP, Rachmawanto EH (2017) A robust image watermarking using hybrid DCT and SLT. Technol Inf Commun. https://doi.org/10.1109/ISEMANTIC.2016.7873857
21. USC-SIPI Image Database, Volume 3: Miscellaneous. Available: http://sipi.usc.edu/database/database.php?volume=misc&image=13#top
22. Wang CP, Wang XY, Xia ZQ, Zhang C, Chen X (2016) Geometrically resilient color image zero-watermarking algorithm based on quaternion exponent moments. J Vis Commun Image Represent 41: S1047320316302103. https://doi.org/10.1016/j.jvcir.2016.10.004
23. Shen Z, Kintak U (2017) A novel image zero-watermarking scheme based on non-uniform rectangular. Int Conf Wavelet Anal Pattern Recogn. https://doi.org/10.1109/ICWAPR.2017.8076667
24. Wang CP, Wang XY, Chen XJ, Zhang C (2016) Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. Multimed Tools Appl:1–22. https://doi.org/10.1007/s11042-016-4130-7



**Feifeng Jiang** is a M.S. candidate in College of Software, Nankai University, China. Her current research interests include digital watermarking, software engineering and text detection and recognition.

**Tiegang Gao** is a professor in College of Software, Nankai University, China since 2006. His interests are in information security, multimedia information processing and software engineering. He has published or co-authored more than 100 papers in relation areas.

**De Li** received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.