

Zero-Watermarking Algorithm in Transform Domain Based on RGB Channel and Voting Strategy

Qiumei Zheng*, Nan Liu*, Baoqin Cao*, Fenghua Wang**, and Yanan Yang*

Abstract

A zero-watermarking algorithm in transform domain based on RGB channel and voting strategy is proposed. The registration and identification of ownership have achieved copyright protection for color images. In the ownership registration, discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) are used comprehensively because they have the characteristics of multi-resolution, energy concentration and stability, which is conducive to improving the robustness of the proposed algorithm. In order to take full advantage of the characteristics of the image, we use three channels of R, G, and B of a color image to construct three master shares, instead of using data from only one channel. Then, in order to improve security, the master share is superimposed with the copyright watermark encrypted by the owner's key to generate an ownership share. When the ownership is authenticated, copyright watermarks are extracted from the three channels of the disputed image. Then using voting decisions, the final copyright information is determined by comparing the extracted three watermarks bit by bit. Experimental results show that the proposed zero watermarking scheme is robust to conventional attacks such as JPEG compression, noise addition, filtering and tampering, and has higher stability in various common color images.

Keywords

Color Image, Transform Domain, Voting Strategy, Zero Watermarking

1. Introduction

In recent decades, the production and dissemination of digital works have become more and more convenient due to the rapid development of computer technology and the internet. Simply copying and modifying existing digital works have become a quick and easy way to "own" them. However, it is also accompanied by a lot of serious copyright problems, such as malicious tampering and arbitrary embezzlement. Therefore, digital watermarking, which refers to the embedding of copyright information such as random sequences, copyright logos and owner identities into digital works to effectively protect their copyright, emerged as an indispensable technology [1-3]. Digital watermarking can be used not only in image, text and video but also in medical domain such as medical image [4,5]. Images are one of the most commonly used digital works, and its copyright problems cannot be more overstated [6,7]. Therefore, embedding digital watermarking has become one of the important methods for protecting

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received November 27, 2018; first revision July 10, 2019; second revision April 13, 2020; third revision May 26, 2020; accepted May 29, 2020.

Corresponding Author: Fenghua Wang (fenghuawang@upc.edu.cn)

* College of Computer Science and Technology, China University of Petroleum Huadong, China (zhengqm@upc.edu.cn, 17854227923@163.com, caobaoqin2302@163.com, yangyanan0309@gmail.com)

** College of Computer and Communication Engineering, China University of Petroleum Huadong, Qingdao, China (fenghuawang@upc.edu.cn)

image copyright. However, the embedded digital watermarking will affect image quality, that is, its invisibility will be poor [8-11].

The watermarking has two characteristics: invisibility and robustness. Invisibility refers to the visual effect of the embedded watermark on the original image. The effect is the optimal when it is completely invisible. Robustness refers to the ability of the protected image embedded with watermark to extract the watermark after compression, noise addition, and other attacks. Zero-watermarking is a method for protecting copyright by displaying the watermark information in the host image, so it avoids the dilemma the traditional digital watermarking is difficult to achieve a balance between invisibility and robustness [12-16].

“Zero” in the “zero-watermarking” means that the host image is no longer embedded with a watermark and is no longer encrypted by the copyright watermark provided by the owner, such as random sequence of copyright information, ownership mark or user identity [17-19]. More specifically, this encryption method uses the rich and stable features of the original image to construct the master share, and the master share and the copyright watermark superimpose to generate a zero watermark, which is called ownership share [20]. The two shares do not provide any information about the host image and copyright watermark separately, and the copyright watermark will be displayed only when they are superimposed [21,22], thus making zero-watermark reliable and secure in copyright protection. A zero-watermarking scheme divides digital copyright protection into two processes, namely registration and identification. Upon registration, the ownership share is registered with an intellectual property database of the third-party certification authority (CA). When a copyright dispute arises, identification process is required. Firstly, the master share is extracted from the disputed image, and then the ownership share is taken out from the third-party CA. Finally, the copyright watermark is retrieved under the joint action of two shares to determine the ownership of the digital work [23].

The zero-watermarking scheme proposed by Rani and his colleagues in [24,25], first implements discrete cosine transform (DCT) and singular value decomposition (SVD) for overlapping block sub-images of the host image, and then constructs the master share according to the relation of coefficients. This method is robust to many attacks. However, the test image used in Rani’s study is gray image, which is not applicable to more mainstream applications of color images. In [26], the authors proposed two zero-watermarking schemes based on visual mapping, which combined QR decomposition with DCT to generate master share. Although this method is robust to common attacks, when the color image is used as the test image to construct the master share in the experimental scheme, the image is converted to the YUV color space, and only Y-component is used, and the characteristics of the image are not fully utilized. Similarly, the zero-watermarking algorithm for color images based on DWT-DCT-SVD proposed by Jiang and Chen [27] converts the image from the RGB color space to the YCbCr color space. Then the master share is constructed using only the luminance component (Y), and the characteristics of the image are not fully utilized. In the robust zero-watermarking algorithm for color images in the spatial domain proposed by Xiong [28], master share is constructed directly in the spatial domain using the relationship between the mean value of the pixel and that of the block. This method can resist common attacks because it uses voting policy to extract copyright watermarks in authentication, but it is not robust to rotation attacks because the coefficients in spatial domain are easily interfered by attacks.

It can be seen from the above literature that only by using the features of the image can the watermarking algorithm have strong robustness, and the host image must be color image rather than gray image. In order to address these issues, a zero-watermarking algorithm in transform domain based on

RGB channel and voting strategy (RGB-CV) is proposed in this paper, which can be applied to color images. The robustness of the algorithm is improved by fully utilizing the RGB channel features of the image and using voting decision in the identification process.

2. The Proposed Zero-Watermarking (RGB-CV)

The RGB-CV algorithm achieves copyright protection for color images with ownership registration and identification, as shown in Fig. 1. In the registration phase, the master share of the image is constructed firstly, and then the ownership share generated by the interaction of master share and copyright watermark is registered to a CA. In the identification phase, the master share of the image with copyright dispute is constructed and superposed with the registered ownership share to restore the copyright watermark.

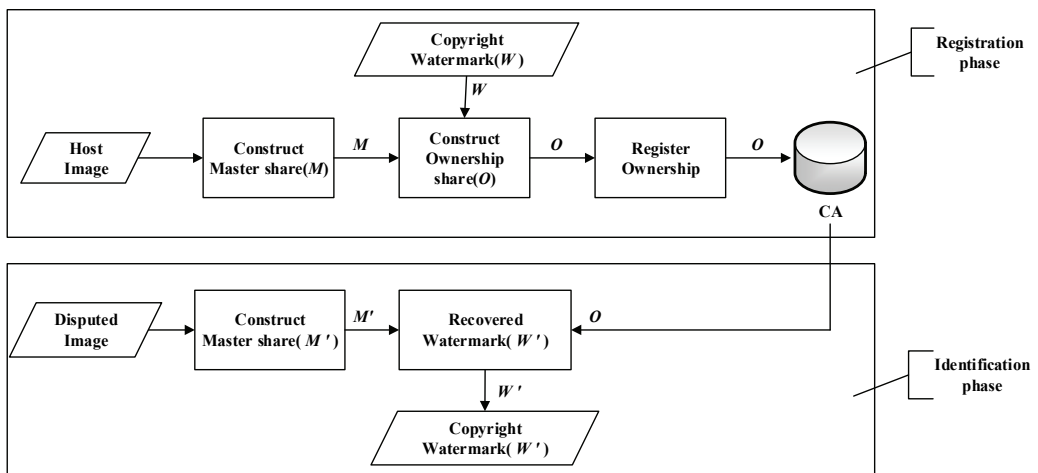


Fig. 1. Flow chart of the RGB-CV algorithm for protecting image copyright.

2.1 Overview of RGB-CV

In the phase of zero watermark identification, in order to improve the robustness of the algorithm, the algorithm makes full use of image features to construct the master share, namely the transformation domain coefficients of the three channels in the construction of color image. When constructing the master share with the host image, the low-frequency approximate sub-image of the host image is divided into three channels of R, G, and B in the RGB color space, and three master shares are constructed from the three channels by applying the same rule. The rules for constructing the master share are as follows: firstly divide a channel into non-overlapping 8×8 sub-blocks and perform 1-level wavelet transform on the sub-block to obtain a low-frequency block. Secondly, perform discrete cosine transform and singular value decomposition on the low-frequency block. Finally, construct a singular value coefficient matrix using the maximum singular value of each sub-block, and generate a master share by comparing the relationship between the maximum singular value of each block and the mean value of the singular value coefficient matrix.

We use host image and copyright watermark image to generate ownership share. In the experimental method of this paper, the copyright watermark is simply referred to as Watermark (W). Firstly, the watermark is encrypted by using the double-chaos scrambling method and the three-master sharing X-OR method, respectively. The three watermark bits obtained are used as the R, G and B channel data of ownership share respectively. When the watermark is encrypted by double chaos scrambling method, relevant data such as the initial value of the chaos and the encryption control rate are used as the owner's key.

In the phase of zero watermark registration, when master share and ownership share are separated, neither of them will display any relevant information about watermark. Only when the two are superimposed (that is, X-OR operation) can the encrypted watermark bits be displayed. Therefore, when retrieving copyright information of disputed images, it is necessary to construct three master shares, respectively, corresponding to R, G, and B channels. The channels corresponding to R, G, and B of the master share and ownership share are respectively subjected to X-OR operations to obtain three encrypted watermarks which should theoretically be identical. In order to further improve the robustness of the algorithm, the watermark bits are determined bit by bit using voting decisions on the three obtained watermarks. Finally, under the effect of the legitimate owner's key, the watermark bits are inverted to obtain the copyright watermark. The key further guarantees the reliability and security of the zero watermark.

Therefore, this study improves the robustness of the algorithm in two ways: (1) more stable transform domain coefficients are used, and the master share is constructed from three channels; (2) in the phase of copyright identification, the final watermark is obtained through the bit-by-bit voting decision of the watermark obtained from the three channels.

2.2 Implementation of RGB-CV

This section describes the implementation of RGB-CV algorithm used in the phase of ownership registration and identification. A color image I with a size of $L \times L$ is used as a host image, and a binary image W with a size of $N \times N$ as a watermark image.

2.2.1 Ownership registration phase

There are two main steps in the phase of ownership registration, namely the construction of master share and the construction of ownership share, which are discussed as follows.

(1) Construction of master share

The construction of the master share (M) of the original image I is divided into in the following four steps, as shown in Fig. 2.

Step 1 (Acquisition of approximate sub-image): Using Haar filter, 1-level wavelet decomposition is performed on the original image I to obtain a low-frequency approximation sub-image ILF of size $\frac{L}{2} \times \frac{L}{2} \times 3$.

Step 2 (Separation of three channels): The RGB channels of the low frequency approximation sub-image ILF are separated to obtain I_R , I_G , and I_B of size $\frac{L}{2} \times \frac{L}{2}$.

Step 3 (Construction of master shares): The master shares M_R , M_G , and M_B of $N \times N$ size are constructed by the same series of processing for the three channels. Taking R channel construction M_R as an example, the construction process is introduced.

- After I_R is performed with non-overlapping partitions with a block size of $\frac{L}{2 \times N} \times \frac{L}{2 \times N}$, the block matrix $\{B_{lc_R_{ij}}\}$ is obtained, where $i, j = 1, \dots, N$.
- After each block $B_{lc_R_{ij}}$ is subjected to 1-level DWT, the low-frequency sub-band is obtained, and then the obtained low-frequency coefficients are subjected to DCT. Finally, the DCT coefficients are further subjected to singular value decomposition to obtain the maximum singular values.
- The matrix $\{S_{_R_{ij}}\}$ is constructed with s taken from each block, and the mean $savg$ of the matrix is calculated.
- The master share M_R of the R channel is constructed using the method shown in (1).

$$M_{R_{ij}} = \begin{cases} 1, S_{_R_{ij}} \geq savg \\ 0, S_{_R_{ij}} < savg \end{cases} \quad (1)$$

Step 4 (Construction of master share M): The M_R , M_G , and M_B are used as the data for the three channels R, G, and B, respectively, to generate the master share M of the image I .

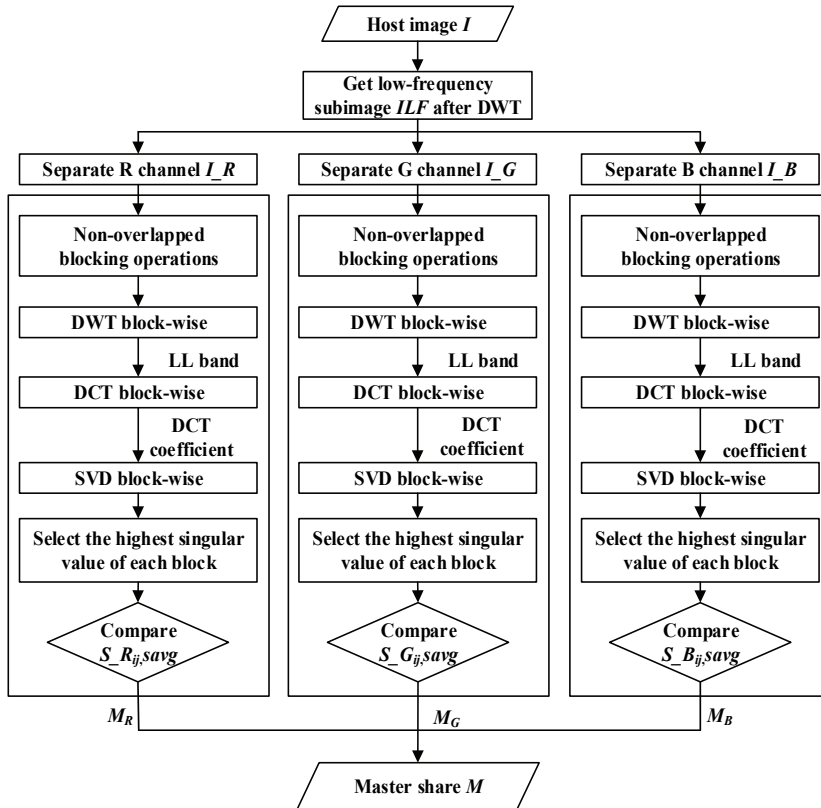


Fig. 2. Flow chart for constructing the master share (M).

(2) Ownership share construction

The construction of the ownership share (O) is divided into the following two steps. The construction flow chart is shown in Fig. 3.

Step 1 (Preprocessing of watermark image): The Arnold scrambling encryption has periodic characteristics and is easy to be broken by force. Therefore, chaotic scrambling technique sensitive to initial value is used in this paper to encrypt the watermark image. In order to obtain the encrypted watermark W' , the odd and even columns of the watermark images are encrypted by using the mapping sequence with different initial chaotic values and encryption control rates respectively, and the initial values of the chaos and the control rate are stored as part of the secret key, Key .

Step 2 (Construction of ownership share O): The three channels of O are composed of O_R , O_G , and O_B . The O_R , O_G , and O_B are generated by X-OR operations between the M_R , M_G , and M_B and the encrypted secret watermark SW , respectively, as shown in (2).

$$\begin{cases} O_R = M_R \oplus SW \\ O_G = M_G \oplus SW \\ O_B = M_B \oplus SW \end{cases} \quad (2)$$

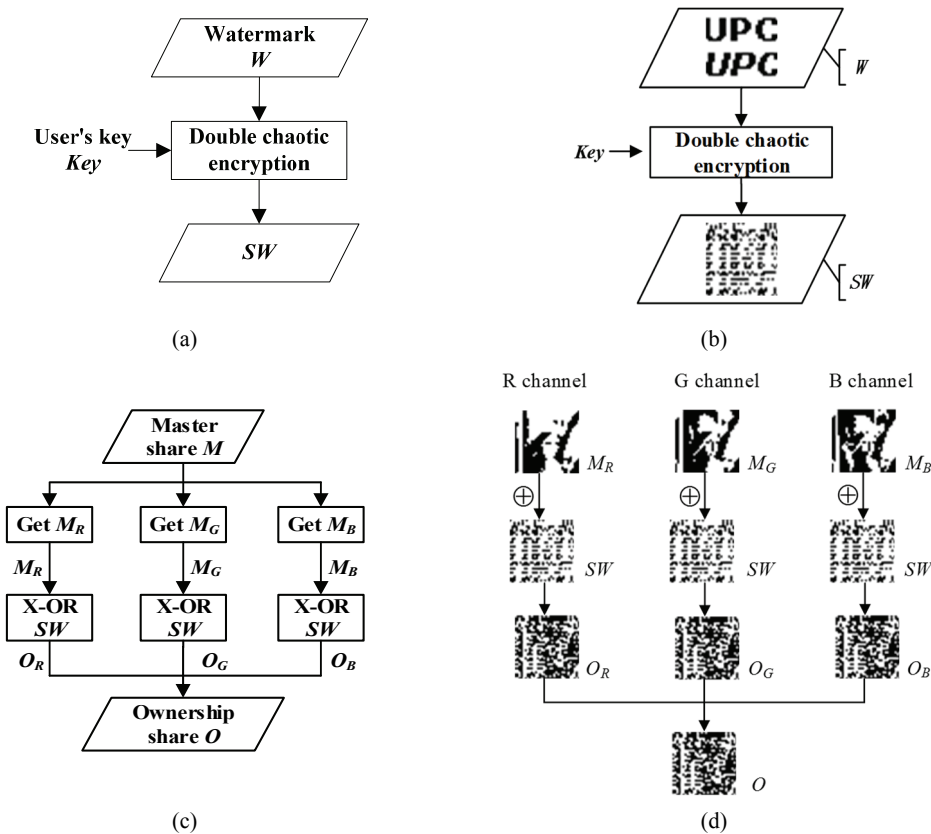


Fig. 3. Flow chart for constructing the ownership share (O): (a) watermark encryption (b) zero-watermark construction, (c) data of watermark encryption, and (d) data of zero-watermark construction.

2.2.2 Ownership identification phase

When a copyright dispute arises, the master share (M') is firstly “extracted” from the disputed digital image I' in the same way as the master share in the registration phase. Then, the registered ownership share is then taken out from the CA’s IPR database. Finally, the watermark bit is obtained by the X-OR operation of M' and O , and the copyright watermark W' of the legal person is decrypted by the key, Key . The process is specifically divided into the following five steps and its flow chart is shown in Fig. 4.

Step 1: According to the construction process of master share, the master shares M_R' , M_G' , and M_B' of the R, G, and B channels of the disputed image I' are constructed.

Step 2: O_R , O_G , and O_B are separated from the R, G, and B channels of the ownership share O that has been taken out.

Step 3: Watermarks W_R' , W_G' , and W_B' are respectively “extracted” from the three channels. The specific method is shown in (3).

$$\begin{cases} W_R' = M_R' \oplus O_R \\ W_G' = M_G' \oplus O_G \\ W_B' = M_B' \oplus O_B \end{cases} \quad (3)$$

Step 4: The watermark bit WMB is calculated by using the Voting decision.

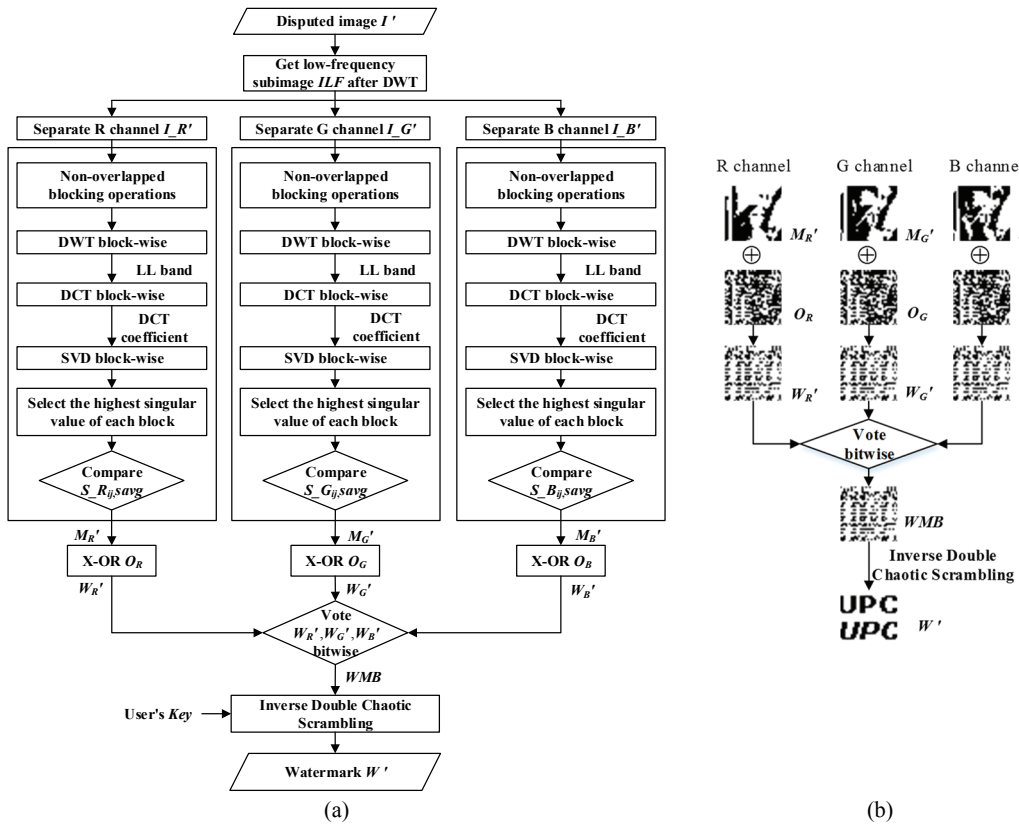


Fig. 4. Flow chart for extracting copyright watermarks from disputed images: (a) zero-watermark extraction and (b) data of zero-watermark extraction.

According to the construction process, the theoretical values of W_R' , W_G' and W_B' at the same pixel position are equal, but the actual values of WR, WG and WB obtained from the image to be detected after the attack are not equal at the same pixel position. Therefore, if the i -th row and the j -th column on the watermark image are regarded as the position P, where $i, j=1, \dots, N$, the watermark value of the WMB at the P position can be determined according to the voting decision theory. The three channels are treated as three voters, and the watermark value of each channel at the P position is regarded as a vote. In other words, if the watermark value is 1, the number of vote for a channel at the P position is considered to be 1; conversely, if the watermark value is 0, the number of votes is 0. And then the total number of votes from the three channels at the P position is calculated. If the total number of votes is more than half, the watermark value of the WMB at that position is considered to be 1, otherwise, it is considered to be 0. The specific calculation method of the watermark bit WMB is as shown in (5).

$$WBit_{ij} = W_{R_{ij}}' + W_{G_{ij}}' + W_{B_{ij}}' \quad (4)$$

$$WMB_{ij} = \begin{cases} 1, WBit_{ij} \geq 2 \\ 0, WBit_{ij} < 2 \end{cases} \quad (5)$$

Step 5: With decryption using the owner's key, the watermark bit WMB is subjected to inverse double chaos scrambling to obtain the decrypted watermark image W' .

3. Experimental Results and Analysis

In order to verify the effectiveness of the proposed watermarking algorithm, simulation experiments are carried out in MATLAB R2017b. In the experiments, 10 color images of 512×512 size are selected from the Standard Image Database (SIDBA) as the test images, as shown in Fig. 5. A 32×32 binary image is used as the watermark image, as shown in Fig. 6. In this paper, peak signal-to-noise ratio (PSNR) is used to describe the peak signal-to-noise ratio between the post-attack test image I' and the original image I , i.e., PSNR is used to express the amplitude of the attack on the test image. The larger the PSNR value, the smaller the attack on the image to be detected. The similarity between the extracted watermark W' and the copyright watermark W is expressed with the normalization coefficient (NC). The larger NC value is, the higher similarity between W' and W , the more effective the proposed zero watermarking algorithm. The PSNR value of the test image $I'(i, j)$ with a size of $L \times L$ is calculated according to (6). The NC value of the extracted watermark $W'(i, j)$ with a size of $N \times N$ is calculated according to (8).

$$PSNR(I, I') = 20 \log_{10} \frac{255}{MSE} \quad (6)$$

$$MSE = \sqrt{\frac{1}{L \times L} \sum_{i=1}^{L-1} \sum_{j=1}^{L-1} [I(i, j) - I'(i, j)]^2} \quad (7)$$

$$NC(W, W') = \frac{\sum_{i=1}^{N-1} \sum_{j=1}^{N-1} W(i, j) \times W'(i, j)}{\sqrt{\sum_{i=1}^{N-1} \sum_{j=1}^{N-1} W(i, j)^2} \times \sqrt{\sum_{i=1}^{N-1} \sum_{j=1}^{N-1} W'(i, j)^2}} \quad (8)$$

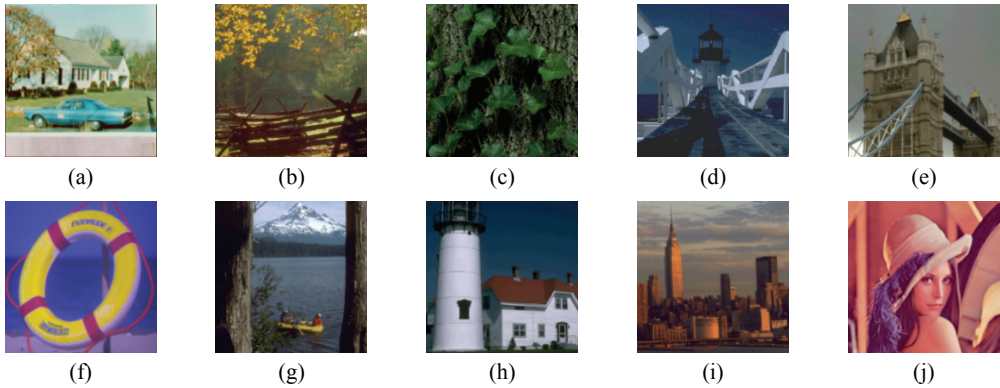


Fig. 5. The test images: (a) house, (b) housewoods, (c) ivytree, (d) lighthouse, (e) london, (f) life, (g) lostlake, (h) malight, (i) manhatan, and (j) Lena.



Fig. 6. The watermark image.

3.1 Robustness Comparison

Since the zero watermarking algorithm proposed in this paper targets at color images, 10 pairs of color images, which are different in color, contrast, texture, etc. (shown in Fig. 5), are selected as test images in this paper so as to better demonstrate the robustness of the proposed algorithm. In order to verify the effectiveness of the proposed algorithm, the common attack methods in the watermark algorithm are used to attack the test image to varying degrees. NC is used to evaluate the robustness of the algorithm, the larger value of NC, the more robust the proposed algorithm:

(1) Common attack. Common attacks include noise addition, compression, and filter. The image is attacked by noise addition, which includes Salt-and-Pepper noise and Gaussian noise. Both attacks are carried out 10 times. The range of the effect factor of Salt and Pepper noise is from 1% to 10%, the mean value of added Gaussian noise is 0, and the variance range is from 1% to 15%. In 10 compression attack tests, the range of image quality factor after compression is 90–10. In Gaussian filter experiment, a Gaussian filter is used to blur the image and the filter window size is set as 1×1 to 10×10 .

(2) Geometric attack. Geometric attacks include shear attack, translation, rotation, and scaling. In shear attack, 10% to 90% of the image is cut in the x-axis direction. In the Center crop attack on the image, 1/9, 2/9, 3/9, 4/9 of the image center are cut off respectively. In the translation attack, the image is shifted by 10 to 100 pixels in the width direction. In the rotation attack, the rotation angle ranges from 10° to 100° . And in terms of scaling attacks, the zoom factor ranges from 0.3 to 1.9. According to the experimental method of Thanh in [29], the rotated and scaled images are inversely transformed according to the attacking factor, namely the image is re-rotated and re-scaled.

(3) Other attack. In the brightness attack, the image brightness changes from -127 to +127. In the tampering attack, a label is placed anywhere 10 times in the image.

The robustness of the proposed algorithm is detailed as follows.

Table 1. The attacked images




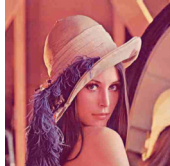



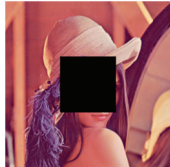

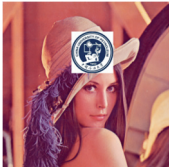
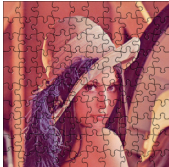
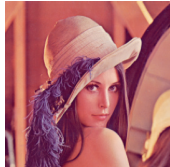












 Salt&Pepper noise 0.05 PSNR=13.424	 Gaussian noise 0.05 PSNR=9.080	 Shearing 0.3 PSNR=11.017	 JPEG 20 PSNR=25.061
 Gaussian filter 10×10 PSNR=24.673	 Rotation 80° PSNR=12.082	 Scaling 0.3 PSNR=21.639	 Center crop 1/9 PSNR=9.600
 Brightness -16 PSNR=13.659	 Tampering [157,275] PSNR=13.860	 Puzzle PSNR=14.110	 Pixelize PSNR=26.354

Table 2. The watermark extracted from Table 1

 Salt&Pepper noise 0.05 NC=1	 Gaussian noise 0.05 NC=0.998	 Shearing 0.3 NC=0.958	 JPEG 20 NC=0.998
 Gaussian filter 10×10 NC=0.999	 Rotation 80° NC=0.970	 Scaling 0.3 NC=0.992	 Center crop 1/9 NC=0.922
 Brightness -16 NC=0.996	 Tampering [157,275] NC=0.986	 Puzzle NC=0.995	 Pixelize NC=1

3.1.1 Analysis of the results of “Lena”

“Lena” image is selected to display the attacked image and the extracted watermark. The PSNR of the image to be measured after attack and the non-original image under different attacks are calculated, and the NC between the extracted watermark and the copyrighted watermark is also calculated. The results are shown in Tables 1 and 2, respectively, and the comparison of NC values with different degree of attack factors is shown in Table 3.

In addition, the NC values of the watermarks extracted from the attacked “Lena” image are compared, as shown in Table 4.

To further verify the robustness of the algorithm, the bit error rate (BER) values of the watermarks extracted from the attacked “Lena” image are compared, as shown in Table 5.

Table 3. Comparison of NC values with different degree of attack factors

	Factor	RGB-CV	Jiang and Chen [27]
Salt and Pepper	0.01	0.99986	0.998
	0.05	0.998	0.996
	0.2	0.989	0.987
Shearing	1/4	0.871	0.892
	1/9	0.973	0.949
	1/16	0.981	0.969
Rotation	1	0.983	0.980
	3	0.936	0.936
	10	0.817	0.823
	20	0.773	0.773
Median filtering	3×3	1	0.999
	5×5	0.999	0.997
	7×7	0.998	0.995
JPEG	10%	0.997	0.991
	30%	0.999	0.998
	50%	0.9997	0.998

Table 4. Comparison of NC values obtained using different algorithms

	PSNR (dB)	RGB-CV	Rani and Raman [25]	Thanh and Tanaka [26]	
				PVMF	VMF
Gaussian noise (mean=0, variance=0.15)	5.583	0.995	0.985	0.989	0.942
JPEG QF=10	22.758	0.997	0.983	0.820	0.848
Rotation 50°	8.507	0.862	0.624	0.904	0.941
Scaling 0.5	28.225	1	0.981	0.987	0.989
Tampering	13.925	0.987	0.794	0.953	0.952
Puzzle	14.110	0.995	0.916	0.811	0.810
Pixelize	26.354	1	0.994	0.944	0.947

Table 5. Comparison of BER values with different degree of attack factors

	Factor	RGB-CV	Yang et al. [16]	Zhou et al. [11]
Salt and Pepper	0.01	0	0	0.002
Rotation	1	0.017	0.011	-
Median filtering	3×3	0	0	0.021
	5×5	0.001	-	0.028
JPEG	10%	0.003	0.003	0.030
	20%	0.002	0	0.040
	30%	0.001	0	0.032
	50%	0	0.0011	0.029
Scaling	0.3	0.008	0.003	-
	0.5	0	0.001	0.033
Shearing	0.3	0.042	0.104	-
Gaussian filter	3×3	0.001	0	-
Gaussian noise	0.01	0.002	0.004	0.002
Brightness	16	0.004	-	0.026

The NC and BER values are used to evaluate the robustness of RGB-CV. It can be seen that the proposed algorithm is highly robust to conventional attacks such as noise, filtering, and JPEG compression. In addition, the RGB-CV algorithm is robust to the distortion of filter Puzzle and Pixelize in Photoshop software. The RGB-CV is more robust not only than current zero watermarking algorithms but also than traditional robust watermarking algorithms.

3.1.2 Analysis of the results of 10 images

In the robustness comparison experiment, 10 images suffered from 10 different attacks such as noise addition, compression, and rotation. When an image is attacked, the image is subjected to 10 attacks of different intensities, and the values of the action factors of different intensities are evenly distributed and changed 10 times within the attack range described in Section 3.1. Table 6 shows the comparison of the NC values obtained by the RGB-CV algorithm and other algorithms under the premise of the same PSNR value. Among them, the data of each line is the average value obtained after 10 different attacks on 10 images.

Table 6. Comparison of average NC values obtained using different algorithms

	PSNR	RGB-CV	Rani and Raman [25]	Thanh and Tanaka [26]	
				PVMF	VMF
Salt&Pepper noise	13.669	0.999	0.935	0.801	0.803
Gaussian noise	9.228	0.995	0.984	0.895	0.897
Shearing	11.307	0.811	0.989	0.955	0.958
JPEG	24.773	0.999	0.978	0.901	0.903
Gaussian filter	24.149	1	0.931	0.829	0.830
Rotation	10.811	0.928	0.812	0.913	0.937
Translation	8.119	0.784	0.999	0.926	0.960
Scaling	23.225	0.998	0.978	0.939	0.942
Center crop	9.199	0.821	0.536	0.899	0.904
Brightness	11.324	0.948	0.972	0.888	0.888
Tampering	13.152	0.960	0.809	0.943	0.943

PVMF=permuted visual map feature, VMF=visual map feature.

In order to illustrate the stability of the RGB-CV algorithm proposed in this paper for color images with large differences in hue, texture, etc., under certain attack of certain strength, the 10 images shown in Fig. 5 are used as test images, and the variance of the NC values of the watermarks detected by the 10 images after the attack is calculated. Since the magnitude of the fluctuation of the NC value is not an order of magnitude in the case of common attacks and geometric attacks, the two-line charts shown in Figs. 7 and 8 are used to respectively represent the variance of the NC values in the conventional attack and geometric attack. The horizontal coordinates in the line chart represent the action factors of a certain attack at 10 levels, with action factors increasing from 1 to 10 and attack intensity increasing.

It can be seen from the NC average comparison in Table 6 that the watermarking algorithm proposed in the paper has good robustness to common attacks such as noise addition, JPEG compression, filtering, scaling, tampering, etc. In the JPEG compression and Gaussian filtering, the watermarking NC reached 0.999. Moreover, as can be seen from Fig. 7, when the attack strength is enhanced, the variance of the NC values for extracting watermarks from different images is mostly less than 0.003, and only fluctuates

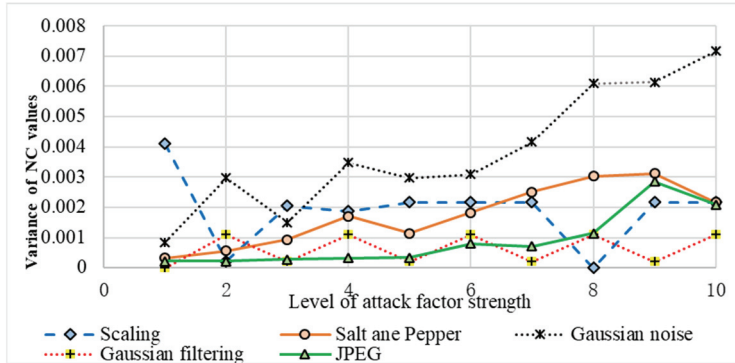


Fig. 7. Comparison of NC variance in common attacks.

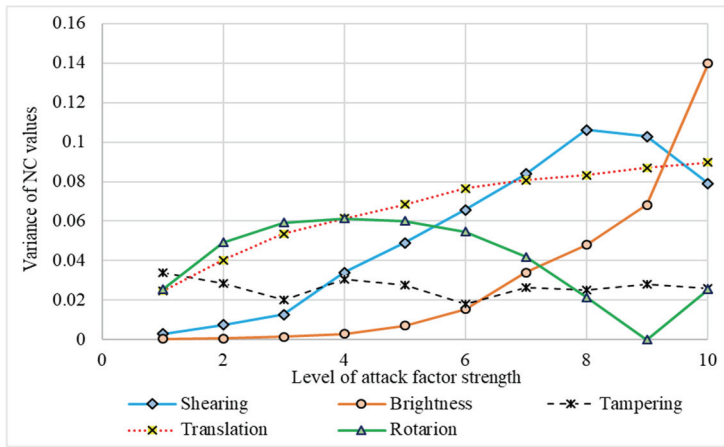


Fig. 8. Comparison of NC variance in geometric attacks.

slightly in scaling attacks and Gaussian noise attacks. Among them, when the scaling attack factor is 0.3, the maximum variance of the watermark NC value obtained by 10 images is only 0.004. When Gaussian noise with a mean of 0 and a variance of 0.13 is added, the maximum variance of the NC value of the watermark obtained from 10 images is only 0.007. Therefore, the zero-watermarking algorithm proposed in this paper is suitable for color images with common hue and texture, and is very robust to conventional attacks.

According to Table 6, we can conclude that the algorithm is less robust to shear and translation in geometric attacks. The main reason is that the watermark bit is constructed in blocks when the master share is constructed. From the line chart shown in Fig. 8, we can see that the influence of the image difference on the extraction of the watermark gradually increases as the attack intensity increases, and the shear and translation also have a large fluctuation in the NC value, namely the stability of the algorithm is weakened. However, in the labeling attack, the attack that tampers with the image content is not affected by the image difference, and the NC value does not fluctuate greatly, but basically remains around 0.96.

Although the robustness to shear and translation is relatively weak due to the influence of the block structure master share method, the proposed algorithm is superior to Rani and Raman [25] and Thanh and Tanaka [26] in noise addition, filtering JPEG compression, scaling, tampering, Puzzle and Pixelize.

Table 7. Comparison of complexity

	RGB-CV	Rani and Raman [25]	Thanh and Tanaka [26]
Image size	512×512	512×512	512×512
Copyright image size	32×32	128×128	64×64
Ownership share size	32×32	128×128	64×64
Image properties	Color	Gray	Color
Domain	DWT/DCT/SVD	DCT/SVD	DCT/SVD/QR
Security	Double chaos scrambling	Pseudo-random number key	Torus permutation
Complexity of algorithm	$O(n^2)$	$O(n^3)$	$O(n^2)$

3.2 Complexity Analysis Comparison

The complexity of the proposed algorithm is also compared from the perspectives of copyright watermark size, algorithm scope and security, as shown in Table 7. We can conclude from the comparison results that the zero-watermark algorithm proposed in this paper is applied to color images, which requires a small third-party database to preserve the copyright watermark. And when the complexity is equal to other algorithms, it has higher security.

4. Conclusion

In this paper, a zero-watermarking algorithm in transform domain based on RGB-CV is proposed. RGB-CV extracts the transform domain features that can resist various kinds of attacks, and DWT, DCT and SVD are used comprehensively because they have the characteristics of multi-resolution, energy concentration and stability, which is conducive to improving the robustness of proposed algorithm. In the identification phase, voting decision is used to obtain the watermark bit of the three channels so as to accurately obtain copyright watermark. Experimental results show that the proposed watermarking algorithm is very robust to common attacks such as compression, noise addition, and filtering when used in common color images. The NC of the extracted watermark is more than 0.99. However, its robustness to shear attack and translation attack needs to be improved. In the future research, we hope that the global features of the image can be used for constructing master share to improve the robustness of the algorithm to geometric attacks.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 51274232, 61305008); the Natural Science Foundation of Shandong Province of China (No. ZR2018MEE004); and the Fundamental Research Funds for the Central Universities (No. 19CX02030A).

References

[1] H. Berghel and L. O’Gorman, “Protecting ownership rights through digital watermarking,” *Computer*, vol. 29, no. 7, pp. 101-103, 1996.

[2] C. I. Podilchuk and E. J. Delp, “Digital watermarking: algorithms and applications,” *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, 2001.

- [3] M. Barni, F. Bartolini, I. J. Cox, J. Hernandez, and F. Perez-Gonzalez, "Digital watermarking for copyright protection: a communications perspective," *IEEE Communications Magazine*, vol. 39, no. 8, pp. 90-91, 2001.
- [4] X. Y. Yu, C. Y. Wang, and X. Zhou, "A hybrid transforms-based robust video zero-watermarking algorithm for resisting high efficiency video coding compression," *IEEE Access*, vol. 7, pp. 115708-115724, 2019.
- [5] Z. Ali, M. S. Hossain, G. Muhammad, and M. Aslam, "New zero-watermarking algorithm using Hurst exponent for protection of privacy in telemedicine," *IEEE Access*, vol. 6, pp. 7930-7940, 2018.
- [6] S. Roy and A. K. Pal, "An SVD Based location specific robust color image watermarking scheme using RDWT and Arnold scrambling," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2223-2250, 2018.
- [7] Q. T. Su, Y. G. Niu, G. Wang, S. L. Jia, and J. Yue, "Color image blind watermarking scheme based on QR decomposition," *Signal Processing*, vol. 94, pp. 219-235, 2014.
- [8] Q. Wen, T. Sun, and S. Wang, "Concept and application of zero-watermark," *Acta Electronica Sinica*, vol. 31, no. 2, pp. 214-216, 2003.
- [9] J. H. Ma and J. X. He, "A wavelet-based method of zero-watermark," *Journal of Image and Graphics*, vol. 12, no. 4, pp. 581-585, 2007.
- [10] H. Q. Cao, H. Xiang, X. T. Li, M. Liu, S. Yi, and F. Wei, "A zero-watermarking algorithm based on DWT and chaotic modulation," in *Proceedings of the SPIE 6247: Independent Component Analyses, Wavelets, Unsupervised Smart Sensors, and Neural Networks IV*. Bellingham, WA: International Society for Optics and Photonics, 2006.
- [11] X. Zhou, H. Zhang, and C. Wang, "A robust image watermarking technique based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 3, article no. 77, 2018.
- [12] X. L. Liu, B. J. Chen, G. Coatrieux, and H. Z. Shu, "Color image zero-watermarking based on SVD and visual cryptography in DWT domain," in *Proceedings of SPIE 10225: Eighth International Conference on Graphic and Image Processing (ICGIP 2016)*. Bellingham, WA: International Society for Optics and Photonics, 2017.
- [13] Y. Zhao and X. Wang, "Multipurpose zero watermarking algorithm for color image based on SVD and DCNN," *Journal of Shandong University (Engineering Edition)*, vol. 48, no. 3, pp. 25-33, 2018.
- [14] Y. Yu, M. Lei, X. Liu, Z. Qu, and C. Wang, "Novel zero-watermarking scheme based on DWT-DCT," *China Communications*, vol. 13, no. 7, pp. 122-126, 2016.
- [15] C. P. Wang, X. Y. Wang, X. J. Chen, and C. Zhang, "Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping," *Multimedia Tools and Applications*, vol. 76, no. 24, pp. 26355-26376, 2017.
- [16] H. Y. Yang, S. R. Qi, P. P. Niu, and X. Y. Wang, "Color image zero-watermarking based on fast quaternion generic polar complex exponential transform," *Signal Processing: Image Communication*, vol. 82, pp. 115747-115763, 2020.
- [17] Y. Hu, S. A. Zhu, and D. Zhang, "A novel zero-watermark algorithm in image subspace domain," in *Proceedings of IEEE International Conference on Control and Automation*, Guangzhou, China, 2007, pp. 2744-2748.
- [18] Y. R. Rao and E. Nagabhooshanam, "A novel image zero-watermarking scheme based on DWT-BN-SVD," in *Proceedings of International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, 2014, pp. 1-6.
- [19] D. Xiao, M. Deng, and X. Zhu, "A reversible image authentication scheme based on compressive sensing," *Multimedia Tools and Applications*, vol. 74, no. 18, pp. 7729-7752, 2015.
- [20] T. Ye, "A robust zero-watermark algorithm based on singular value decomposition and discreet cosine transform," in *Parallel and Distributed Computing and Networks*. Heidelberg, Germany: Springer, 2011, pp. 1-8.
- [21] H. Pan, G. Chen, Y. Ding and F. Li, "A zero-watermarking algorithm of color image based on SVD and DWT," *Microelectronics & Computer*, vol. 29, no. 5, pp. 50-53, 2012.
- [22] T. Sun, W. Quan and S. Wang, "Zero-watermark watermarking for image authentication," in *Proceedings of the 4th IASTED International Conference on Signal and Image Processing*, Kauai, HI, 2002, pp. 503-508.

- [23] M. Sui and J. B. Li, "Robust watermarking for medical images based on Arnold scrambling and DCT," *Application Research of Computers*, vol. 30, no. 5, pp. 2552-2556, 2013.
- [24] A. Rani, A. K. Bhullar, D. Dangwal, and S. Kumar, "A zero-watermarking scheme using discrete wavelet transform," *Procedia Computer Science*, vol. 70, pp. 603-609, 2015.
- [25] A. Rani and B. Raman, "An image copyright protection scheme by encrypting secret data with the host image," *Multimedia Tools and Applications*, vol. 75, no. 2, pp. 1027-1042, 2016.
- [26] T. M. Thanh and K. Tanaka, "An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13455-13471, 2017.
- [27] Z. T. Jiang and W. Chen, "Zero-watermarking algorithm for color image based on DWT-DCT-SVD," *Microelectronics & Computer*, vol. 33, no. 8, pp. 107-111, 2016.
- [28] X. G. Xiong, "A robust zero-watermarking algorithm for spatial domain color images," *Computer Engineering and Science*, vol. 39, no. 1, pp. 103-110, 2017.
- [29] T. M. Thanh, P. T. Hiep, T. M. Tam, and K. Tanaka, "Robust semi-blind video watermarking based on frame-patch matching," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 10, pp. 1007-1015, 2014.



Qiumei Zheng <https://orcid.org/0000-0002-5901-6205>

She is a Professor of College of Computer & Communication Engineering at China University of Petroleum (East China). She received the B.S. degrees from East China Petroleum Institute, Dongying, China, in 1986. She received the M.E. degrees from China University of Petroleum (East China), Dongying, China, in 1999. She has published more than 40 journal papers, of which more than 20 have been retrieved by EI et al. She is the editor of two books and the associate editor of one. Her research interests lie in watermarking, image processing.



Nan Liu <https://orcid.org/0000-0001-7785-3587>

She received the B.S. degree from China University of Petroleum (East China), Qingdao, China, in 2018. She is currently working toward the M.E. degree in China University of Petroleum (East China), Qingdao, China. Her research interest is in image processing and copyright protection.



Baoqin Cao <https://orcid.org/0000-0002-1651-1126>

She received the B.S. degree from China University of Petroleum (East China), Qingdao, China, in 2016. She is currently working toward the M.E. degree in China University of Petroleum (East China), Qingdao, China. Her research interest is in image processing and copyright protection.



Fenghua Wang <https://orcid.org/0000-0002-4656-2629>

He received the Ph.D. degree from Xi'an Jiaotong University, Xi'an in 2009. Currently he works in College of Computer & Communication Engineering at China University of Petroleum (East China). His research interests include Digital watermarking, Pattern Recognition, Computer Vision.



Yanan Yang <https://orcid.org/0000-0002-6237-5452>

She received the B.S. degree from University of Jinan, Jinan, China, in 2017. She is currently working toward the M.E. degree in China University of Petroleum (East China), Qingdao, China. Her research interest is in video watermarking.