Hindawi
Security and Communication Networks
Volume 2021, Article ID 7081194, 12 pages
https://doi.org/10.1155/2021/7081194

*Research Article*

# Color Zero-Watermarking Algorithm for Medical Images Based on BEMD-Schur Decomposition and Color Visual Cryptography

**Deyang Wu**,[1,2,3] **Miaomiao Wang**,[4] **Jing Zhao**,[1,2,3] **Jiayan Wang**,[1,2,3] **Meiyu Zhong**,[1,2,3] **Haichun Zheng**,[1,2,3] **Sen Hu**,[4] **Yong Tang**,[1,2,3] **and Changbo Qu**[4]

[1]*The College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China*
[2]*The Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, Qinhuangdao 066004, China*
[3]*State Key Laboratory of Software Engineering of Hebei Province, Qinhuangdao, Hebei 066004, China*
[4]*College of Software, Liaoning Technical University, Huludao, 125005, China*

Correspondence should be addressed to Miaomiao Wang; wdy_ysu@126.com and Yong Tang; tangyong@ysu.edu.cn

Received 19 July 2021; Revised 21 August 2021; Accepted 11 November 2021; Published 20 December 2021

Academic Editor: Jinwei Wang



With the widespread use of medical images in telemedicine, personal information may be leaked. The traditional zero-watermarking technology has poor robustness under large-scale attacks. At the same time, most of the zero-watermarking information generated is a binary sequence with a single information structure. In order to effectively solve the poor robustness problem of traditional zero-watermarking under large-scale attacks, a color zero-watermarking algorithm for medical images based on bidimensional empirical mode decomposition (BEMD)-Schur decomposition and color visual cryptography is proposed. Firstly, the color carrier image and the color copyright logo are decomposed into R, G, and B three color components, respectively, and the feature value of each sub-block are extracted by wavelet transform, BEMD decomposition, block operation, and Schur decomposition. Then, the R, G, and B components of the copyright logo are scrambled by Arnold scramble and converted into binary watermark information. Finally, a color visual cryptography scheme is proposed to generate two color shared images based on the carrier characteristics and copyright information. One shared image is used to generate a color zero-watermark, and the other is used for copyright authentication phase. Experimental results show that this algorithm has strong robustness and stability in resisting large-scale noise attacks, filtering attacks, JPEG compression, cropping attacks, and translation attacks at different positions. Compared with similar zero-watermarking algorithms, the robust performance is improved by about 10%, and it can adapt to more complex network environments.

## 1. Introduction

With the rapid development of information technology, medical images play an important role in the diagnosis process of telemedicine systems. As the carrier of medical information, medical images usually contain a lot of important personal information [1]. However, that will affect the doctor's diagnosis of diseases and cause the leakage of personal information, when medical images are tampered with by criminals. Therefore, the copyright protection of medical image research is of great significance. As a copyright protection technology, digital watermarking can effectively solve the problems of copyright protection and content authentication and play an important role in protecting the copyright of medical images. Traditional embedding watermarking technology [2] realizes copyright protection by embedding binary watermarking information into the invisible domain of digital images, but the embedded information will destroy the integrity of the image information. Meantime, the amount of embedding information is limited by transparency; therefore, it is not suitable for copyright protection of medical images [3].

To resolve the issue of the integrity of traditional watermarking technology, Wen et al. [4] first presented a zero-watermarking concept; the basic idea of this technique is to generate the unique feature of carrier image and

construct a zero-watermark image by performing an exclusive-or (XOR) operation between the watermark image and the constructed binary feature. Finally, save the zero-watermark information to the copyright protection center. Since the introduction of zero-watermarking technology, it has received extensive attention. Reference [5] analyzes in detail the significance of image encryption in improving watermark performance and security performance in watermark algorithm. Sun et al. [6] proposed a zero-watermarking algorithm based on the generalized Arnold transform, which uses the generalized Arnold transform to scramble the binary copyright to enhance the security of the information. At the same time, the zero-watermark is created through the spread spectrum technology to ensure the completeness of original carrier, but the ability to resist geometric attacks is poor. To this end, Gao and Jiang [7] used the Bessel-Fourier moments of the normalized image to generate feature vectors and generates a zero-watermark image by combining them with a copyright watermark; this algorithm uses the rotation invariance of Bessel–Fourier moments to resist image rotation and image offset operations. Xia et al. [8] proposed a zero watermarking algorithm based on quaternion polar harmonic fourier moments (QPHFM), which improved the antigeometric attack ability of the watermarking algorithm. Rani et al. [9] used discrete wavelet transformation (DWT) [10] to obtain the wavelet coefficients of each sub-block and constructed the feature matrix by singular value decomposition. DWT has sufficient robustness for small-scale nongeometric attacks. But the extracted copyright information contains more noise points when the attack intensity increases. Wang et al. [11] selected the coefficients of polar coordinate complex exponential transformation by using logistic mapping to generate binary feature images and generated zero-watermark information with the copyright watermark encrypted by logistic mapping. This method has a strong robust performance against geometric attack. Thanh and Tanaka [12] proposed a zero-watermarking for visual sharing, which constructed a feature matrix based on the cosine coefficient of each sub-block and then combined it with the copyright watermarking to generate an ownership map. This shared map is characterized by high security and easy authentication, but the robust performance is poor. In terms of resistance to geometric attacks, most existing algorithms use singular values as the decomposition tool for sub-blocks, they can effectively resist small-scale attacks, and singular value decomposition will increase the time complexity of the algorithm. Kang et al. [13] proposed a robust color image zero-watermarking algorithm using polar coordinate transformation and 2D composite chaotic mapping. Firstly, three polar coordinate transformation distances were accurately calculated to enhance the robustness of the algorithm. Then, a binary feature sequence is generated by judging the magnitude relationship of adjacent moments. Finally, Arnold transform is applied to binary feature sequence and copyright watermark to enhance the security of information. As a technical branch of digital watermarking, zero-watermarking solves the imbalance between transparency and robustness of traditional watermarking technology well. Therefore, many scholars have studied the application of zero-watermarking technology to medical images. For example, Xia et al. [14] proposed a medical image zero-watermarking algorithm based on logistic chaotic mapping and quaternion polar coordinate transformation. Firstly, calculate the quantum probability density function of the carrier image and construct the zero-watermark by use qubits to ensure the robustness of the algorithm against geometric attacks. But it can only resist small-scale noise and filtering attacks. To this end, Liu et al. [15] used dual complex tree wavelet transform and discrete cosine transform to extract the visual feature vector of medical images and used chaotic mapping to encrypt the watermark image, in which the logic relationship between three watermarking images and feature vectors is utilized to generate multiple zero-watermark. Since the wavelet transform has strong denoising performance, the extracted low-frequency information can effectively reduce the interference of noise. At the same time, a triple-zero-watermark improves the security of information. Zou et al. [16] proposed a zero-watermarking algorithm for partitionable eye medical images for the problem of inaccurate copyright recognition; the scheme divides the image into several fan-shaped equal parts and then calculates the gray-scale change between the fan-shaped parts to ensure the distinguish ability of the image. Liu et al. [17] proposed a scale-invariant feature transform (SIFT)-discrete cosine transform (DCT) zero-watermarking algorithm for medical images; the algorithm uses SIFT [18] and DCT [19] to extract the features of the carrier images. Since SIFT has a rotation correction function, the algorithm shows strong robustness in resisting rotation attacks, and the logistic chaotic map is used to encrypt the features to improve the concealment of medical images. Xia et al. [20] proposed a robust zero-watermarking algorithm for quaternion polar coordinates and Fourier moments. Firstly, the stable feature points were extracted through speed up robust feature (SURF) [21], and the linear feedback coefficients were determined by the feature scale. Then, the quaternion Fourier moment is calculated using linear feedback coefficients, and the feature vector of the color image is generated. Finally, the feature vector and the copyright image are employed to generate a zero-watermarking by XOR operation. In recent years, with the continuous in-depth study of zero watermarking technology, the synchronization of nongeometric attacks can be improved, but the synchronization of watermark extraction is still poor under geometric attacks. Therefore, researchers try to apply image moments to the copyright protection of digital images to improve the robustness of the algorithm against geometric attacks. For example, reference [22] combined quaternion-type moment invariants (QTMIs) with visual cryptography. QTMIs were used to extract the stable features of the carrier image, and visual cryptography was used to combine features with watermark information to obtain a zero-watermark algorithm that resists geometric attacks. Reference [13] used the invariant features of the three moments of polar complex exponential transformation (PCET), polar cosine transform (PCT), and polar sine transform (PST) to calculate the coefficients of the three moments of the carrier image at the same time. The carrier

feature sequence was constructed by comparing the size relationship of adjacent moments, which improves the robustness of the algorithm. The moment-based watermarking algorithm effectively improves the watermark's ability to resist geometric attacks, but still has problems such as low operating efficiency and inaccurate calculation accuracy. In response to the above problems, Yang et al. [23] proposed a zero-watermark algorithm based on fast quaternion generic polar complex exponential transform (FQGPCET), which fused the low-order coefficients of FGPCET moments and QGPCET moments to improve the calculation efficiency of the moments, and the extracted carrier features are more robust. Reference [24] extended the high-precision generalized orthogonal Fourier Mellin moments (GOFMMs) to accurate quaternion GOFMMs (AQGOFMMs), extracted the 4D features of the carrier image, and the calculation accuracy was improved. Reference [25] proposed a zero-watermark algorithm based on polar complex exponential transform (PCET), which used the relationship between the same moment and repeated moment to simultaneously realize the copyright protection of multiple medical images, which greatly improved the efficiency of the algorithm. Therefore, Honsy et al. [26, 27] and others use the high-precision Gaussian integral method to calculate the multi-channel fractional-order Legendre-Fourier moments (MFrLFMs) to construct the zero watermark, so as to enhance the numerical stability and geometric invariance of the carrier features, so as to improve the performance of the algorithm. Reference [28] proposed a quaternion radial fractional Charlier moments (QRFrCMs) to improve the robustness of the algorithm, which solved the problem of numerical stability to a certain extent and effectively improved the robustness of the zero-watermarking algorithm.

Although the research on zero-watermarking has achieved a lot of results, there still are some problems as follows:

(1) Binary image as watermark information in the existing zero-watermarking schemes, and the generated zero-watermark is binary information, which information structure is relatively simple

(2) Most of the existing zero-watermarking algorithms can only resist small-scale attacks, and the normalized correlation coefficients obtained for large-scale attacks are relatively low, or the extracted copyright information contains more noise points

(3) Existing zero-watermarking algorithms Arnold or chaotic mapping is used alone to encrypt copyright information, and their security is lower

This paper proposes a color zero-watermarking algorithm for medical images based on BEMD-Schur decomposition and color visual cryptography. BEMD [29] decomposition, DWT and Schur decomposition are used to extract the feature information of the carrier image and generate color zero-watermark information by improved visual cryptography. At the same time, Arnold scrambling is utilized to encrypt copyrighted images to improve information security.

The main contributions of this paper are as follows:

(1) Combining empirical mode decomposition, DWT, and Schur decomposition for enhancing the robust performance of the algorithm, while Schur decomposition can effectively improve time efficiency

(2) Based on traditional visual cryptography technology, we propose a color visual cryptography scheme, which generates two color secret shared images to improve authentication efficiency and zero-watermark security

(3) The color zero-watermarking scheme does not require any changes to the medical image, and directly uses improved visual cryptography to generate a color zero-watermarking, which is beneficial to protect the integrity of the color medical image

Given the abovementioned problems and analysis, this paper presents a strong and robust color zero-watermarking algorithm that combines BEMD decomposition and color visual cryptography.

The rest of the organization is as follows: Section 2 describes the principle of BEMD-Schur decomposition and color visual cryptography. In Section 3, we present the proposed color zero-watermarking algorithm in detail. Section 4 reports the robustness test results and security of the color zero-watermarking algorithm. Section 5 gives the conclusions.

## 2. Preliminaries

*2.1. BEMD Decomposition.* BEMD is a two-dimensional linear and nonlinear signal analysis method, it does not need to set the basis function in advance, and it can be decomposed according to the time scale characteristics of the signal itself. Therefore, BEMD is widely used in image denoising, image fusion, and other fields. The purpose of BEMD decomposition is mainly to obtain the intrinsic mode function (IMF). According to the BEMD theory, IMF contains the instantaneous frequency information of each level of the original signal. Therefore, the feature matrix of the original information can be constructed according to the characteristics of the IMF. The BEMD decomposition specific step is as follows [29]:

Step 1: initialize the signal source $\mathbf{x}_i(t)$.

Step 2: find the upper and lower envelopes $\mathbf{x}_{\max}$, $\mathbf{x}_{\min}$ according to the local extreme points of the original information

Step 3: calculate the average value of the upper and lower envelopes $\mathbf{m}_i = \mathbf{x}_{\max} + \mathbf{x}_{\min}/2$.

Step 4: subtract the average value of the envelope from the original signal to get the IMF components $\mathbf{x}_i(x) = \mathbf{x}_{i-1}(t) - \mathbf{m}_{i-1}(t)$.

Step 5: the first component is obtained when $x_i$ satisfies the two conditions of the IMF. Otherwise, the screening continues.

Step 6: repeat Step 2 Step 5 for the remaining signal $x_i$ until the threshold is met to get the first component.

$$S\ D = \sum_{t=0}^{T} \frac{\left|\mathbf{x}_{k-1}(t) - \mathbf{x}_k(t)\right|}{\mathbf{x}_{k-1}(t)} \in \{0.2, 0.3\}. \tag{1}$$

Step 7: subtract the first one **IMF** from the original signal to get the first-order residual amount $\mathbf{r}_i(t) = \mathbf{x}_{i-1}(t) - \mathbf{IMF}_i(t)$, and repeat Step 1–Step 7 with $x$ instead of the original signal. The EMD decomposition model can be obtained through the above decomposition steps as follows:

$$\mathbf{F}(t) = \sum_{i=1}^{k} \mathbf{IMF}_i(t) + \mathbf{r}_k. \tag{2}$$

where, $\mathbf{F}(t)$ is the original signal, **IMF** is the intrinsic modal component, and **r** is the residual term of the difference between the original signal and **IMF**. Since BEMD can adaptively select the basis function according to the characteristics of the signal, it can accurately decompose the signal into different frequency information.

*2.2. Schur Decomposition.* Schur decomposition is a matrix decomposition method, its role directly decomposes the image into two matrices being multiplied [30]. In addition, they also have rotation-invariant, robust characteristics, high speed and so on, and it can effectively reduce the impact of geometric attacks on images. Therefore, it is widely used in the field of image processing. Schur decomposition formula is as follows:

$$\mathbf{I} = \mathbf{UT} = \begin{bmatrix} u_{1,1} & \cdots & u_{1,n} \\ \vdots & \ddots & \vdots \\ u_{m,1} & \cdots & u_{m,n} \end{bmatrix} \begin{bmatrix} \lambda_{1,1} & \cdots & * \\ & \ddots & \vdots \\ & & \lambda_{m,n} \end{bmatrix}, \tag{3}$$

where **U** is the unitary matrix and **T** is the upper triangular matrix.

*2.3. Color Visual Cryptography (CVC).* Visual cryptography is an image encryption method that can be decrypted directly by the human eye, because of its convenience and security, and it is widely used for image encryption. The visual cryptography in document [22] provides a binary visual cryptography scheme based on pixel expansion. In traditional visual cryptography, the original pixels are expanded and cannot maintain the original information structure. At the same time, it is limited to binary pixels. Based on literature [16], this paper introduces the principle of a color visual cryptography into the field of copyright protection to improve the security of watermarking information embedded in the carrier image. The color visual cryptography rules are as follows:

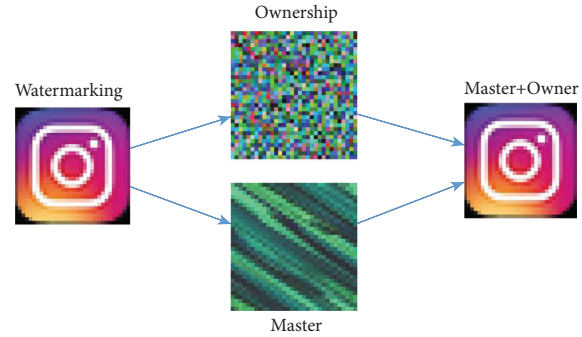


Figure 1: Example of color visual cryptography encryption.

$$1 = \begin{cases} M & O \\ 1 & 1 \\ 0 & 0 \end{cases}, \qquad 0 = \begin{cases} M & O \\ 1 & 0 \\ 0 & 1 \end{cases}. \tag{4}$$

It can be seen from Figure 1, the master share and the ownership share components generated by the copyright image through the principle of color visual cryptography are messy, and it is impossible to identify any copyright-related information. A clear copyright image can be obtained when the master component and the ownership component are superimposed together, and the size is consistent with the original image. Compared with the traditional visual cryptography, the color visual cryptography does not require the original pixels to be expanded, maintaining the original information structure. At the same time, it can be used to encrypt color images with richer content.

## 3. Color Zero-Watermarking Algorithm

*3.1. Color Zero-Watermark Construction.* As the core idea of color zero-watermarking algorithms is to construct color zero-watermark using stable image features and color copyright images encrypted. Let $I = \{f(x, y, 3), 0 \le x < M, 0 \le y < N\}$ be the original color medical image and $W = \{w(x, y, 3), 0 \le x < m, 0 \le y < n\}$ be the color logo image. The color zero-watermarking construction process is shown in Figure 2, and the repetition code in Table 1. Here are the main steps:

Step 1 (color space decomposition): firstly, the color host image $I$ is firstly partitioned into R, G, and B components by dimension-reduction treatment, and the color components $I^R$, $I^G$, and $I^B$ are extracted, which $I^R$, $I^G$, and $I^B$ are uniformly written as $I^c$. The color logo image $W$ is represented by R, G, and B component images, and the color components $W^R$, $W^G$, and $W^B$ are extracted, which $W^R$, $W^G$, and $W^B$ are uniformly written as $W^c$, $c = R, G, B$.

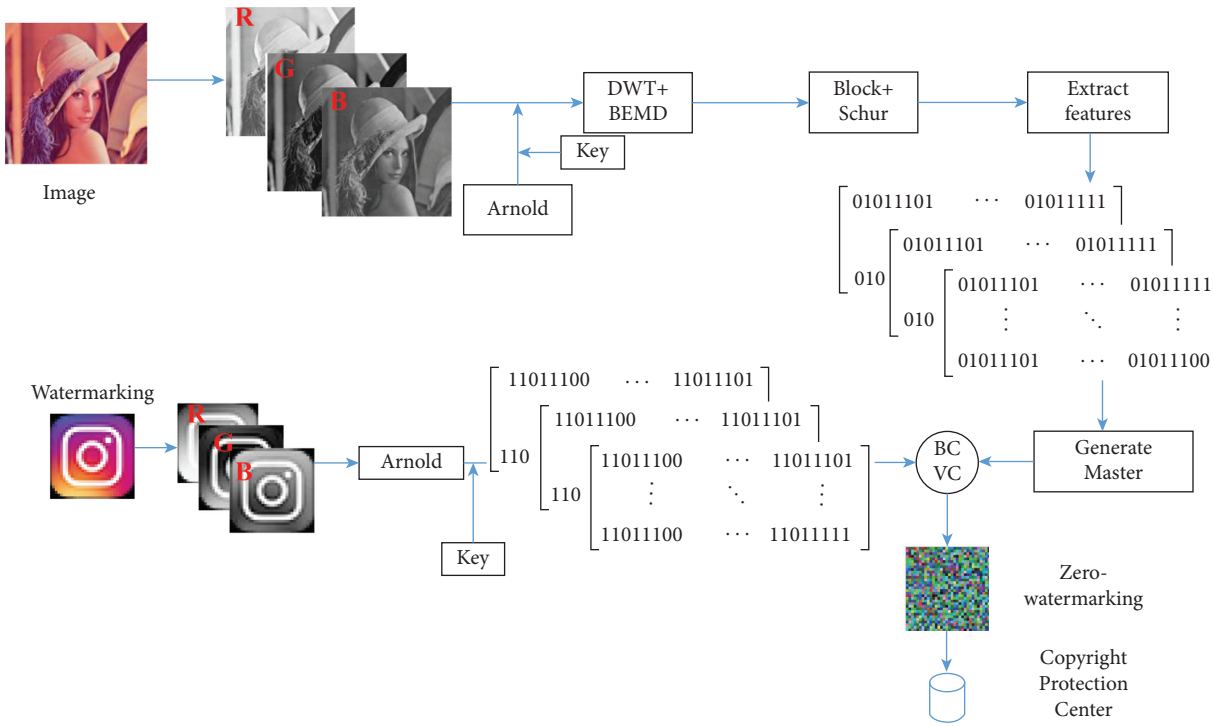


Figure 2: Diagram of the color zero-watermarking generation process.

Table 1: The Repetition code.

**Algorithm 1** Color zero-watermarking algorithm

**Input:** Color host image $\mathbf{I}$ of size $M \times N \times 3$, Color logo $\mathbf{W}$ of size $m \times n \times 3$.
**Output:** Color zero Watermark
1: Read a color host image $\mathbf{I}$ of size $M \times N \times 3$ and a color logo $\mathbf{W}$ of size $m \times n \times 3$.
2: The color host image $\mathbf{I}$ is partitioned into R, G, and B components to obtain $\mathbf{I}^R$, $\mathbf{I}^G$, and $\mathbf{I}^B$. The color logo image $\mathbf{W}$ is extracted into R, G and B components to obtain $\mathbf{W}^R$, $\mathbf{W}^G$, and $\mathbf{W}^B$.
3: **for** $c = R, G, B$ **do**
4: To increase the security of watermark encrypt the watermark $\mathbf{W}^c$ by Arnold scramble using (5).
5: Perform DWT and BEMD on $\mathbf{I}^c$ to obtain $\mathbf{IMF}_k^c$, and sum $\mathbf{IMF}_{k-1}^c$ to obtain $\mathbf{IMF}^c$ using (7).
6: Divide $\mathbf{IMF}^c$ into $m \times n$ nonoverlapping blocks of size $8 \times 8$ to sub-block $\mathbf{B}_{i,j}^c$ using (8).
7: **for** $j = 1$ to $m$ **do**
8: **for** $j = 1$ to $n$ **do**
9: For each sub-block $\mathbf{B}_{i,j}^c$ using Schur decomposition to obtain sub-block max singular value $\lambda_{i,j}^{c\,\max}$ using (9) and (10).
10: **end for**
11: **end for**
12: Convert $\lambda_{i,j}^{c\,\max}$ of each sub-block into a binary form to generate a binary feature matrix $\mathbf{F}^c$ using (11).
13: According to $\mathbf{F}^c$ form gray master share $\mathbf{M}^c$ using (12).
14: Perform the CVC mapping rule on $\mathbf{W}^c$ and $\mathbf{M}^c$ to obtain the gray ownership share $\mathbf{O}_{i,j}^c$ using (14).
15: **end for**
16: Generate color master image $\mathbf{M}^{\mathrm{RGB}}$ by overlapping gray master shares $\mathbf{M}^R$, $\mathbf{M}^G$, $\mathbf{M}^B$ using (13).
17: Generate color ownership share $\mathbf{O}^{\mathrm{RGB}}$ by overlapping gray ownership shares $\mathbf{O}^R$, $\mathbf{O}^G$, $\mathbf{O}^B$ using (15), and as color zero watermark.

Step 2: to improve the security of the watermark information, the Arnold transform [19] is used for a two-dimensional period permutation of the logo image $\mathbf{W}^c$, and it is given as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod (N), \tag{5}$$

where $(x, y)$ and $(x', y')$ are the original logo image pixel and the permuted logo image pixel, respectively.

Step 3: transform the color component $I^c$ using DWT, which is converted from spatial domain to frequency domain and extract approximate components using a low pass filter. It is mathematically expressed as follows:

$$\mathbf{I}_{LL}^{c}(i,j)=\frac{1}{\sqrt{a}}\int_{R}\mathbf{I}^{c}(t)\bullet\Phi\left(\frac{t-b}{a}\right)\mathrm{d}T, \tag{6}$$

where • is the convolution operation, Φ is the wavelet basis function, $a$ is the scaling factor, $b$ is the translation factor, $i\in\{1,2,\ldots P/2\}$, and $j\in\{1,2,\ldots L/2\}$.

Step 4: decompose the approximate components $\mathbf{I}_{LL}^{c}$ of the carrier image by BEMD to extract the intrinsic modal component $\mathbf{IMF}_1^c\sim\mathbf{IMF}_k^c$, remove the component margin of difference, and sum $\mathbf{IMF}_1^c\sim\mathbf{IMF}_{k-1}^c$:

$$\begin{cases}\mathbf{IMF}_k^c=\mathrm{BEMD}\left(\mathbf{I}_{LL}^c\right),\\ \mathbf{IMF}^c=\mathrm{sum}\left(\mathbf{IMF}_{k-1}^c\right),\end{cases} \tag{7}$$

where $k\in\{1,2,\ldots 6\}$.

Step 5: the low frequency sub-band is segmented into nonoverlapping blocks $\mathbf{B}_{i,j}$ of size $8\times 8$. The block method is described as follows:

$$\mathbf{B}_{i,j}^{c}=\frac{\mathbf{IMF}^c}{m\times n}, \tag{8}$$

where $i=1,2,\ldots m,\ j=1,2,\ldots n$.

Step 6: Schur decomposition operation is performed on the nonoverlapping block to acquire the sub-block max singular value.

$$\left[\mathbf{U}^c,\mathbf{T}^c\right]=\mathrm{schur}\left(\mathbf{B}_{i,j}^c\right), \tag{9}$$

$$\lambda_{i,j}^{c}=\max\left(di\ ag\left(\mathbf{T}^c\right)\right), \tag{10}$$

where $\mathbf{U}$ is the unitary matrix and $\mathbf{T}$ is the upper triangular matrix.

Step 7: convert $\lambda_{i,j}^{c}$ into a binary form to generate a binary feature matrix $\mathbf{F}^c$:

$$\mathbf{F}^{c}=\begin{bmatrix}\lambda_{1,1}^{c}\mathrm{bite} & \cdots & \lambda_{1,n}^{c}(1,\mathrm{bite})\\ \vdots & \ddots & \vdots\\ \lambda_{m,1}^{c}(1,\mathrm{bite}) & \cdots & \lambda_{m,n}^{c}(1,\mathrm{bite})\end{bmatrix}. \tag{11}$$

where bite $=1,2,\ldots 8$.

Step 8: for each channel, a gray master shares $\mathbf{M}^c$ is generated by judging the pixel value of each binary bite. Three channels can produce three gray master shares $\mathbf{M}^R$, $\mathbf{M}^G$, and $\mathbf{M}^B$.

$$\mathbf{M}_{i,j}^{c}(1,\mathrm{bite})=\begin{cases}1, & \text{if } \mathbf{F}_{i,j}^{c}(1,\mathrm{bite})==0,\\ 0, & \text{if } \mathbf{F}_{i,j}^{c}(1,\mathrm{bite})==1.\end{cases} \tag{12}$$

Step 9: for an original color image, a color master share $\mathbf{M}^{\mathrm{RGB}}$ can be obtained by overlapping of three gray master shares $\mathbf{M}^R$, $\mathbf{M}^G$, and $\mathbf{M}^B$ according to the following:

$$\mathbf{M}^{RGB}=\mathrm{overlapping}\left(\mathbf{M}^R,\mathbf{M}^G,\mathbf{M}^B\right). \tag{13}$$

Step 10: generate the ownership share denoted as $\mathbf{O}_{i,j}^{c}$ combing color master share $\mathbf{M}^{\mathrm{RGB}}$ and $\mathbf{W}^c$ by using the CVC mapping rule as in (14).

$$\mathbf{O}_{i,j}^{c}(1,\mathrm{bite})=\begin{cases}1, & \text{if } \mathbf{W}_{i,j}^{c}(1,\mathrm{bite})==1\&\mathbf{M}_{i,j}^{c}(1,\mathrm{bite})==0\ ||\mathbf{W}_{i,j}^{c}(1,\mathrm{bite})==0\&\mathbf{M}_{i,j}^{c}(1,\mathrm{bite})==0,\\ 0, & \text{if } \mathbf{W}_{i,j}^{c}(1,\mathrm{bite})==0\&\mathbf{M}_{i,j}^{c}(1,\mathrm{bite})==1||\mathbf{W}_{i,j}^{c}(1,\mathrm{bite})==1\&\mathbf{M}_{i,j}^{c}(1,\mathrm{bite})==1,\end{cases} \tag{14}$$

where $i=1,2,\ldots m$, $j=1,2,\ldots n$, bite $=1,2,\ldots 8$, and $c=R,G,B$.

Step 11: a color ownership share $\mathbf{O}^{RGB}$ can be generated by overlapping of three gray ownership $\mathbf{O}^R$, $\mathbf{O}^G$, and $\mathbf{O}^B$ according to the following:

$$\mathbf{O}^{RGB}=\mathrm{overlapping}\left(\mathbf{O}^R,\mathbf{O}^G,\mathbf{O}^B\right). \tag{15}$$

Finally, the color ownership share $\mathbf{O}^{RGB}$ is treated as color zero-watermarking information, secret key K1 is registered and preserved in the intellectual property database for copyright verification.

*3.2. Copyright Certification Process.* The copyright certification process aims at verifying the copyright logo image. This process needs to extract color zero-watermarking information from intellectual property database and check the validation of the security parameters K1 and K2. The proposed copyright certification steps are similar to the zero-watermarking generation steps, and the corresponding block diagram is given in Figure 3. The steps of the zero-watermark detection process are summarized as follows.

Step 1–Step 6: The steps of the proposed copyright certification process are the same as Steps 1–6 of the zero-watermark generation process, and extracting attacked features $F'^{c}$.

Step 7: generate the master share $\mathbf{M}_{i,j}^{'c}$ referring to formula (16):

$$\mathbf{M}_{i,j}^{'c}(1,\mathrm{bite})=\begin{cases}1, & \text{if } \mathbf{F}_{i,j}^{'c}1,\mathrm{bite}==0,\\ 0, & \text{if } \mathbf{F}_{i,j}^{'c}1,\mathrm{bite}==1.\end{cases} \tag{16}$$

Step 8: an XOR operation is applied on the computed master share $\mathbf{M}_{i,j}^{'c}$ and extracted zero-watermarking $\mathbf{O}_{i,j}^{c}(1,\mathrm{bite})$ from the center of copyright verification in binary bite to retrieve the binary copyright information $\mathbf{W}'^{c}(1,\mathrm{bite})$ as given by (17)

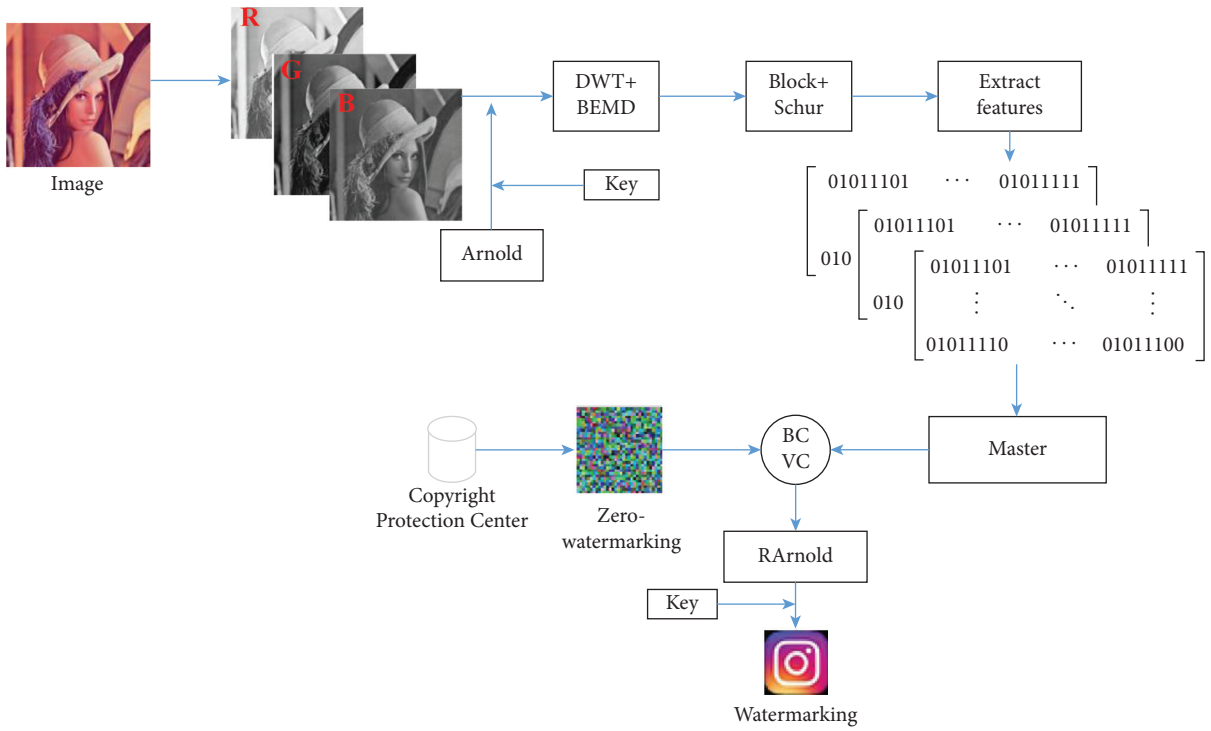


Figure 3: Diagram of the copyright identification process.

$$\mathbf{W}'^{c}(1,\text{bite}) = XOR\left(\mathbf{M}_{i,j}^{'c}(1,\text{bite}), \mathbf{O}_{i,j}^{c}(1,\text{bite})\right). \tag{17}$$

Step 9: convert the binary copyright information $\mathbf{W}'^{c}(1,\text{bite})$ into decimal copyright information $\mathbf{W}''^{c}$.

$$\mathbf{W}_{i,j}^{'c}(1,\text{bite}) \longrightarrow \mathbf{W}''^{c}. \tag{18}$$

Step 10: the encrypted logo image components $\mathbf{W}''^{c}$ are Arnold decryption using the secret key K2 to acquire the three copyright components $\mathbf{W}''^{R}$, $\mathbf{W}''^{G}$, and $\mathbf{W}''^{B}$.

Step 6: A color logo image $\mathbf{W}^{'}$ can be generated by overlapping three copyright components $\mathbf{W}''^{R}$, $\mathbf{W}''^{G}$, and $\mathbf{W}''^{B}$.

$$\mathbf{W}'' = \text{overlapping}\left(\mathbf{W}''^{R}, \mathbf{W}''^{G}, \mathbf{W}''^{B}\right). \tag{19}$$

## 4. Experimental Results and Analysis

*4.1. Experimental Settings.* In the experiments, the used parameters of our algorithm are as follows: the proposed color zero-watermarking scheme is implemented in MATLAB 2016. To evaluate the performance of the proposed color zero-watermarking algorithm, some color fundus images of size $512 \times 512 \times 3$ are chosen as the host images, as shown in Figures 4(a)–4(h), color logo image of size $32 \times 32 \times 3$ shown in Figure 4(i) is selected as the watermark image, and the constructed color zero watermark is shown in Figure 4(j).

*4.2. Robustness Analysis*

*4.2.1. Robustness to Noise Attack.* The robustness of the proposed algorithm is tested in terms of Gaussian noise with noise density in {0.01, 0.03, 0.05}, salt and pepper noise with density in {0.01, 0.03, 0.5}, and speckle noise with density in {0.1, 0.03, 0.5}. The experimental data in Table 2 shows that, with the increase in the noise density, the NC of watermark extracted decreases. However, when the test image is attacked by different Gaussian noise and salt and pepper noise, the watermark NC value is greater than 0.95. The results show that the algorithm has strong robustness against different types of noise attacks.

*4.2.2. Robustness Median, Gaussian, and Mean Filtering.* In this stage, the watermarked image is attacked by median, Gaussian filtering, and mean filtering, respectively. Median filtering replaces the original pixel value of watermarked image with the median value in the window size. Gaussian filtering as a smoothing filter is used to remove high-frequency information from watermarked images. Mean filtering means that the original pixel value of the watermark image is replaced by the mean value of the window size. The NC values are given in Table 3. The overall NC value is above 0.99 for different filtering attacks, which shows that it has strong resistance to different filtering attacks.

*4.2.3. Robustness JPEG Compression.* As the currently international compression standard, JPEG compression is widely used in digital watermarking field. High-intensity JPEG compression may be applied to watermarked images. As shown in Table 4, the NC value remains at 0.99 when

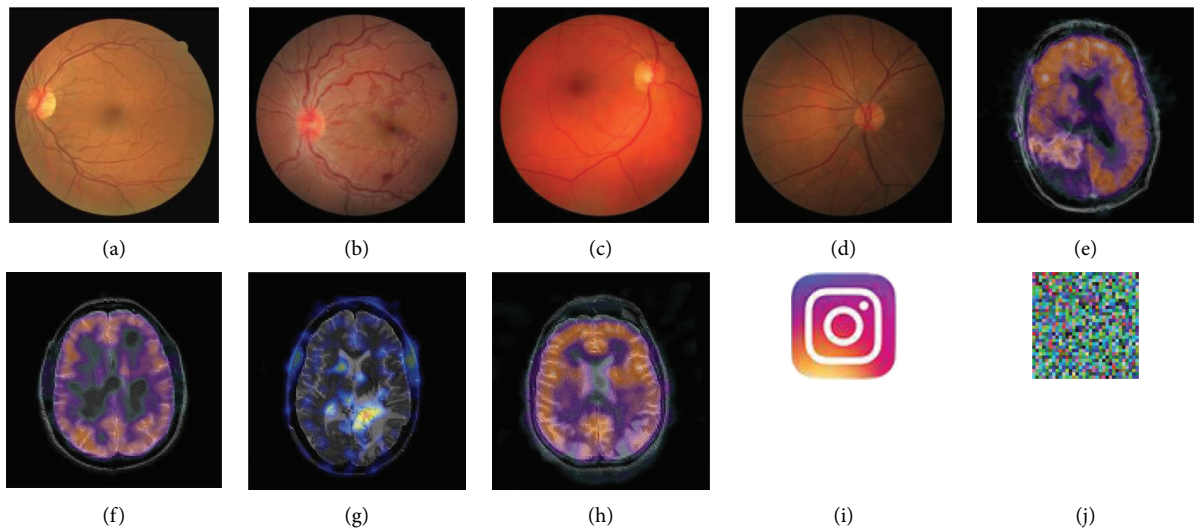

Figure 4: Carrier images and copyright watermark:(a) Fundus1, (b) Fundus2, (c) Fundus3, (d) Fundus4, (e) Cerebral1, (f) Cerebral2, (g) Cerebral3, (h) Cerebral4, (i) Color logo image, (j) Color zero-watermark.

Table 2: NC values under additive Gaussian, salt and pepper, and speckle noise attacks.

| Attack type | Attack intensity | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Gaussian noise | 0.01 | 0.9925 | 0.9916 | 0.9928 | 0.9888 | 0.9911 | 0.9912 | 0.9926 | 0.9909 |
| | 0.03 | 0.9842 | 0.9771 | 0.9789 | 0.9716 | 0.9780 | 0.9800 | 0.9834 | 0.9791 |
| | 0.05 | 0.9768 | 0.9681 | 0.9650 | 0.9517 | 0.9650 | 0.9661 | 0.9723 | 0.9688 |
| Salt and pepper noise | 0.01 | 0.9975 | 0.9951 | 0.9971 | 0.9927 | 0.9955 | 0.9957 | 0.9968 | 0.9954 |
| | 0.03 | 0.9940 | 0.9903 | 0.9909 | 0.9841 | 0.9912 | 0.9913 | 0.9946 | 0.9907 |
| | 0.05 | 0.9903 | 0.9843 | 0.9856 | 0.9777 | 0.9868 | 0.9885 | 0.9907 | 0.9884 |
| Speckle noise | 0.01 | 0.9981 | 0.9974 | 0.9987 | 0.9987 | 0.9974 | 0.9983 | 0.9988 | 0.9989 |
| | 0.03 | 0.9966 | 0.9953 | 0.9990 | 0.9978 | 0.9972 | 0.9969 | 0.9970 | 0.9971 |
| | 0.05 | 0.9961 | 0.9941 | 0.9979 | 0.9961 | 0.9956 | 0.9962 | 0.9964 | 0.9958 |

Table 3: NC values under median, Gaussian, and mean filtering attacks.

| Attack type | Attack intensity | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Median filter | $3\times3$ | 0.9993 | 0.9997 | 0.9997 | 0.9996 | 0.9952 | 0.9974 | 0.9971 | 0.9957 |
| | $5\times5$ | 0.9987 | 0.9986 | 0.9993 | 0.9982 | 0.9919 | 0.9954 | 0.9938 | 0.9909 |
| | $9\times9$ | 0.9986 | 0.9977 | 0.9988 | 0.9972 | 0.9858 | 0.9922 | 0.9897 | 0.9864 |
| Gaussian filter | $3\times3$ | 0.9984 | 0.9991 | 0.9995 | 0.9992 | 0.9992 | 0.9983 | 0.9991 | 0.9993 |
| | $5\times5$ | 0.9982 | 0.9990 | 0.9990 | 0.9991 | 0.9991 | 0.9981 | 0.9991 | 0.9990 |
| | $9\times9$ | 0.9981 | 0.9990 | 0.9990 | 0.9991 | 0.9991 | 0.9980 | 0.9989 | 0.9990 |
| Mean filter | $3\times3$ | 0.9993 | 0.9995 | 0.9991 | 0.9993 | 0.9992 | 0.9993 | 0.9991 | 0.9994 |
| | $5\times5$ | 0.9980 | 0.9985 | 0.9983 | 0.9981 | 0.9982 | 0.9985 | 0.9983 | 0.9988 |
| | $9\times9$ | 0.9974 | 0.9977 | 0.9982 | 0.9981 | 0.9979 | 0.9980 | 0.9978 | 0.9981 |

compressed to 10% of the host image. For different compression attacks, the average NC value is above 0.99. The experimental results show that the algorithm is robust to JPEG compression with different intensity.

*4.2.4. Robustness Rotation Attacks.* To test the algorithm's ability of resistance to geometric attack, we make rotation attacks with rotation angles 5°, 10° and 15°. The experimental results in Table 5 show that the watermarks extracted from images after the rotation attack are all greater than 0.93, indicating the proposed algorithm has a good ability of resistance to rotation attacks.

*4.2.5. Robustness Scaling Attacks.* This part makes a scaling attack test to the host images. The scaling in the paper is to scale the host image with a certain scaling factor, then restore the original size, and attack the host image with a factor of 0.5, 0.75, and 1.5, respectively. It can be seen from Table 6

Table 4: NC values under JPEG compression attacks.

| Attack type | Attack intensity (%) | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| JPEG compression | 10 | 0.9945 | 0.9897 | 0.9949 | 0.9840 | 0.9843 | 0.9906 | 0.9926 | 0.9860 |
| | 30 | 0.9955 | 0.9898 | 0.9952 | 0.9913 | 0.9903 | 0.9954 | 0.9958 | 0.9954 |
| | 50 | 0.9983 | 0.9975 | 0.9973 | 0.9963 | 0.9936 | 0.9971 | 0.9970 | 0.9946 |
| | 70 | 0.9985 | 0.9978 | 0.9978 | 0.9979 | 0.9948 | 0.9969 | 0.9977 | 0.9944 |

Table 5: NC values under geometric rotation attacks.

| Attack type | Attack intensity | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Rotation | 5° | 0.9940 | 0.9877 | 0.9940 | 0.9886 | 0.9631 | 0.9735 | 0.9780 | 0.9697 |
| | 10° | 0.9898 | 0.9837 | 0.9934 | 0.9827 | 0.9461 | 0.9591 | 0.9648 | 0.9553 |
| | 15° | 0.9876 | 0.9780 | 0.9899 | 0.9786 | 0.9340 | 0.9472 | 0.9692 | 0.9465 |

Table 6: NC values under geometric scaling attacks.

| Attack type | Attack intensity | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Scaling | 0.5 | 0.9990 | 0.9995 | 0.9995 | 0.9994 | 0.9918 | 0.9967 | 0.9935 | 0.9929 |
| | 0.75 | 0.9987 | 0.9997 | 0.9992 | 0.9995 | 0.9941 | 0.9972 | 0.9954 | 0.9955 |
| | 1.5 | 0.9992 | 0.9998 | 0.9998 | 0.9999 | 0.9976 | 0.9988 | 0.9981 | 0.9979 |

that the NC values of the watermark are all greater than 0.99, indicating that the algorithm has good performance in resisting image scaling attacks.

*4.2.6. Robustness Translation Attacks.* The host image is translated attack, and the mean value of NC is 0.9804 for all host images when up translated 10 rows. The mean value of NC is 0.9560 when up translated 30 rows. The NC value remains at 0.9118 when up translated 50 rows. Table 7 shows that the proposed algorithm has a fine robustness against translation attacks.

*4.2.7. Robustness Cropping Attacks.* The image cropping is one of the most common geometric attacks. Generally, large-area cropping will cause difficulties in watermark extraction and directly affect the quality of watermarks. In order to verify the effectiveness of the algorithm against cropping attacks, this part performs cropping attacks of different areas on the image (left corner: cropping 1/16, 1/8, and 1/4). The NC of watermarks extracted are shown in Table 8, we can see that the proposed algorithm can extract watermark information perfectly when cropping 1/16 or 1/8. However, when the cropping degree is 1/4, the extracted watermark information deteriorates. The reason is that the feature used in the scheme is based on the sub-block max singular value, and the cropping of image corners does not change the content of all sub-block when the cropping degree is lower.

*4.3. Comparison with Similar Zero-Watermarking Algorithm.* In this section, the performance of the proposed color zero-watermark algorithm is compared with other zero-watermark algorithms [13, 15–17], among which [13] is a binary zero-watermarking algorithm for conventional images; the algorithm in [15–17] are binary zero-watermarking algorithms for medical images. In Table 9, it can be seen that the proposed color zero-watermarking method is superior to the existing representative methods [13, 15–17] in terms of most attacks. Compared with several representative robust zero-watermarking algorithms, the proposed color zero-watermarking algorithm accomplishes better robustness.

In addition to comparing the watermark robustness with the above algorithm, it is also compared with other zero watermarking schemes [24–28]. In the process of extracting the features of the carrier image, the algorithm [24–28] uses the image moment to extract the stable features of the carrier image, which improves the anti-geometric attack ability of the zero-watermarking algorithm. In the algorithm [24–28], the copyright images are binary images, and the color logo is selected as the copyright in this paper. Therefore, when calculating the bit error rate of extracting the watermark, when the value of the color image changes very little, the binary sequence will change greatly. Therefore, the value of the color copyright image is more sensitive, but it can still be seen from Table 10 that the proposed watermarking scheme has better robustness under most attacks.

*4.4. Comparison Time.* In addition to the experiment and comparison of the robustness of the watermark algorithm, in this section, the time of watermark generation and copyright authentication of the algorithm are tested and compared with the algorithm [24–28]. Table 11 shows that the $512 * 512$ carrier image is selected as the test image. In this paper, the zero-watermark generation time and copyright authentication time are less than the algorithms [24–28].

Table 7: NC values under geometric translation attacks.

| Attack type | Attack strength | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Translation | 10 | 0.9802 | 0.9782 | 0.9835 | 0.9816 | 0.9637 | 0.9631 | 0.9761 | 0.9637 |
| | 30 | 0.9564 | 0.9470 | 0.9640 | 0.9604 | 0.9427 | 0.9323 | 0.9534 | 0.9253 |
| | 50 | 0.9359 | 0.9233 | 0.9470 | 0.9415 | 0.9211 | 0.9118 | 0.9443 | 0.9135 |

Table 8: NC values under geometric cropping attacks.

| Attack type | Attack strength | Fundus1 | Fundus2 | Fundus3 | Fundus4 | Cerebral1 | Cerebral2 | Cerebral3 | Cerebral4 |
|---|---|---|---|---|---|---|---|---|---|
| Cropping | 1/16 | 0.9990 | 0.9992 | 0.9992 | 0.9991 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |
| | 1/8 | 0.9962 | 0.9963 | 0.9963 | 0.9965 | 1.0000 | 1.0000 | 1.0000 | 1.0000 |
| | 1/4 | 0.9878 | 0.9880 | 0.9879 | 0.9873 | 0.9998 | 0.9999 | 0.9999 | 0.9998 |

Table 9: Comparison of the robustness (NC) between the proposed scheme and schemes [13, 15–17].

| Attack type | Scheme [13] | Scheme [15] | Scheme [16] | Scheme [17] | Proposed scheme |
|---|---|---|---|---|---|
| Gaussian noise ($\sigma = 0.01$) | 0.9470 | 0.9609 | 0.9264 | 0.9609 | 0.9914 |
| Salt and pepper noise ($\sigma = 0.01$) | 0.9600 | 0.9531 | 0.9416 | 0.9424 | 0.9961 |
| Median filtering ($3 \times 3$) | 0.9818 | 0.9500 | 0.9817 | 0.6200 | 0.9996 |
| Median filtering ($5 \times 5$) | 0.9541 | 0.9600 | 0.9708 | 0.4500 | 0.9992 |
| Gaussian filtering ($3 \times 3$) | 0.9946 | 0.9629 | 0.9803 | 0.9629 | 0.9990 |
| Average filtering ($3 \times 3$) | 0.9785 | 0.9600 | 0.9774 | 0.9721 | 0.9995 |
| JPEG compression (QF = 30) | 0.9762 | 0.9000 | 0.9540 | 0.9000 | 0.9974 |
| Rotation with 5° | 0.9892 | 0.9100 | 0.8851 | 0.8076 | 0.9874 |
| Rotation with 10° | 0.9845 | 0.8700 | 0.8503 | 0.5996 | 0.9833 |
| Scaling 0.75 | 0.9991 | 0.8652 | 0.9901 | 0.7076 | 0.9991 |
| Scaling 1.5 | 0.9878 | 0.8891 | 0.9861 | 0.7900 | 0.9993 |
| Left distance (0, 30) | 0.8203 | 0.5781 | --- | 0.8900 | 0.9459 |
| Cropping (30%) $Y$ direction | 0.9768 | 0.7500 | 0.9839 | 0.7200 | 0.9547 |

--- means no item.

Table 10: Comparison of the robustness (BER) between the proposed scheme and schemes [24–28].

| Attack type | Scheme [24] | Scheme [25] | Scheme [26] | Scheme [27] | Scheme [28] | Proposed scheme |
|---|---|---|---|---|---|---|
| Gaussian noise 0.01 | 0.0024 | 0.0346 | 0.0068 | 0.0021 | 0.0323 | 0.0088 |
| Gaussian noise 0.02 | --- | --- | 0.0088 | --- | 0.0601 | 0.0107 |
| Salt and pepper noise 0.01 | 0.0022 | 0.0190 | 0.0039 | 0.0025 | 0.0067 | 0.0020 |
| Salt and pepper noise 0.02 | --- | 0.0276 | 0.0049 | --- | 0.0093 | 0.0039 |
| Median filtering ($3 \times 3$) | 0.0048 | 0.0055 | 0.0068 | 0.0098 | 0.0075 | 0.0039 |
| Median filtering ($5 \times 5$) | 0.0075 | 0.0194 | --- | 0.0088 | 0.0079 | 0.0039 |
| JPEG compression (QF = 30) | 0.0000 | 0.0143 | 0.0098 | 0.0068 | 0.0193 | 0.0146 |
| JPEG compression (QF = 50) | 0.0019 | 0.0085 | 0.0049 | 0.0049 | 0.0102 | 0.0107 |
| Rotation 5° | 0.0000 | 0.0034 | 0.0059 | 0.0055 | 0.0036 | 0.0025 |
| Rotation 15° | 0.0000 | 0.0055 | 0.0049 | --- | 0.0098 | 0.0045 |
| Scaling 0.75 | 0.0030 | 0.0038 | 0.0049 | 0.0088 | 0.0089 | 0.0029 |
| Scaling 1.5 | 0.0018 | 0.0029 | 0.0020 | 0.0039 | 0.0043 | 0.0014 |

--- means no item.

Table 11: Execution time comparison between the proposed algorithm and other algorithms.

| | Scheme [24] | Scheme [25] | Scheme [26] | Scheme [27] | Scheme [28] | Proposed scheme |
|---|---|---|---|---|---|---|
| Watermark generation time (sec) | 41.7840 | 13.4608 | 10.4270 | 14.2830 | 13,4568 | 5.1761 |
| Copyright authentication time (sec) | 40.6334 | 13.4600 | 11.1830 | 14.7910 | 14,0433 | 4.0378 |

## 5. Conclusion

The traditional embedded watermarking scheme is to embed the watermark information in the host image for copyright protection, but this will affect the visual quality of the host image to a certain extent. In addition, a majority of existing zero-watermarking methods are focused on binary zero-watermark, which single information structure and low security. Most algorithms cannot effectively resist geometric attacks and have poor security. Hence it is quite necessary to devise color image zero-watermarking algorithms with strong robustness and high-level security. In this paper, we proposed a robust color zero-watermarking scheme based on BEMD-Schur decomposition and color visual cryptography. In the proposed algorithm, color zero-watermark is constructed by using color visual cryptography between feature and color logo image to generate ownership share, master share, thus the algorithm has strong robustness against attacks such as noise superposition, filtering, JPEG compression, geometric rotation and scaling, and has high security. The proposed color zero-watermarking algorithm in this paper has strong robustness to geometric attacks and signal processing attacks. At the same time, it is suitable for copyright protection of images with high visual quality. In future work, combining image moments and realizing multiple color copyright image protection will become the focus of research.

## Data Availability

Some or all data, models, or code generated or used during the study are available from the corresponding author by request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References


[1] C. P. Wang, X. Y. Wang, Z. Q. Xia, and C. Zhang, "Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm," *Information Sciences*, vol. 470, pp. 109–120, 2019.

[2] E. Najafi, "A robust embedding and blind extraction of image watermarking based on discrete wavelet transform," *Mathematical Sciences*, vol. 11, no. 4, pp. 307–318, 2017.

[3] S. M. Arora, "A DWT-SVD based robust digital watermarking for digital images," *Procedia computer science*, vol. 132, pp. 1441–1448, 2018.

[4] Q. Wen, T. F. Sun, and S. X. Wang, "Concept and application of zero-watermark," *Acta Electronica Sinica*, vol. 31, no. 2, pp. 214–216, 2003.

[5] T. Lin, X. Y. Wang, and X. K. Wang, "Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 6, pp. 540–547, 2013.

[6] L. Sun, J. C. Xu, X. X. Zhang, W. Dong, and Y. Tian, "A novel generalized Arnold transform-based zero-watermarking scheme," *Appl Math Inf Sci*, vol. 4, no. 4, pp. 2023–2035, 2015.

[7] G. Y. Gao and G. P. Jiang, "Bessel-Fourier moment-based robust image zero-watermarking," *Multimedia Tools And Applications*, vol. 74, no. 3, pp. 841–858, 2015.

[8] Z. Q. Xia, X. Y. Wang, M. Wang et al., "Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments," *IEEE Access*, vol. 7, pp. 122544–122560, 2019.

[9] A. B. Rani, K. D. Amandeep, and K. S. Deepak, "A zero-watermarking scheme using discrete wavelet transform," *Procedia Computer Science*, vol. 70, pp. 603–609, 2015.

[10] X. B. Kang, F. Zhao, G. F. Lin, and Y. J. Chun, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength," *Multimedia Tools And Applications*, vol. 77, no. 11, pp. 13197–13224, 2018.

[11] 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. 26335–26376, 2017.

[12] 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.

[13] X. B. Kang, F. Zhao, Y. J. Chen, G. Lin, and C. Jing, "Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm," *Journal of Visual Communication and Image Representation*, vol. 70, Article ID 102804, 2020.

[14] Z. Q. Xia, X. Y. Wang, W. J. Zhou, R. Li, C. Wang, and C. Zhang, "Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms," *Signal Processing*, vol. 157, pp. 108–118, 2019.

[15] J. Liu, J. B. Li, J. X. Ma, N. Sandiq, U. Bhatti, and Y. Ai, "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map," *Applied Sciences*, vol. 9, no. 4, pp. 1–23, 2019.

[16] B. J. Zhou, J. Y. Du, X. Y. Liu, and Y. Wang, "Distinguishable zero-watermarking scheme with similarity-based retrievol for digital rights Management of Fundus Image," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28685–28708, 2018.

[17] J. L. Liu, J. B. Li, Y. W. Chen et al., "A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain," *Computers, Materials & Continua*, vol. 61, no. 1, pp. 363–378, 2019.

[18] S. Nilkanta and S. Arijit, "SIFT based video watermarking resistant to temporal scaling," *Journal of Visual Communication and Image Representation*, vol. 45, pp. 77–86, 2017.

[19] R. Soumitra and K. P. Arup, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU-International Journal of Electronics and Communications*, vol. 72, pp. 149–161, 2017.

[20] Z. Xia, X. Wang, X. Li et al., "Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments," *Signal Processing*, vol. 164, pp. 368–379, 2019.

[21] H. Bay, A. Ess, T. Tuytelaars, and L. V. Gool, "Speeded-up robust features (SURF)," *Computer Vision and Image Understanding*, vol. 110, no. 3, pp. 346–359, 2008.

[22] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux, and J. Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography," *Signal Processing: Image Communication*, vol. 48, pp. 12–21, 2016.

[23] 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, Article ID 115747, 2020.

[24] X.-Y. Wang, L. Wang, J.-L. Tian, P.-P. Niu, and H.-Y. Yang, "Color image zero-watermarking using accurate quaternion generalized orthogonal fourier–mellin moments," *Journal of Mathematical Imaging and Vision*, vol. 63, no. 6, pp. 708–734, 2021.

[25] W. Wang, Y. Li, and S. Liu, "A polar complex exponential transform-based zero-watermarking for multiple medical images with high discrimination," *Security and Communication Networks*, vol. 2021, no. 2, 13 pages, Article ID 6615678, 2021.

[26] K. M. Hosny and M. M. Darwish, "New geometrically invariant multiple zero-watermarking algorithm for color medical images," *Biomedical Signal Processing and Control*, vol. 70, pp. 1746–8094, 2021.

[27] K. M. Hosny, M. M. Darwish, and M. M. Fouda, "New color image zero-watermarking using orthogonal Multi-Channel fractional-order legendre-fourier moments," *IEEE Access*, vol. 99, p. 1, 2021.

[28] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Robust zero-watermarking scheme based on novel quaternion radial fractional Charlier moments," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 21679–21708, 2021.

[29] N. Bi, Q. Y. Sun, D. Huang, Z. Yang, and J. Huang, "Robust image watermarking based on multiband wavelets and empirical mode decomposition," *IEEE Transactions On Image Processing*, vol. 16, no. 8, pp. 1956–1966, 2007.

[30] A. A. Mohammad, "A new digital image watermarking scheme based on Schur decomposition," *Multimedia Tools and Applications*, vol. 59, no. 3, pp. 851–883, 2012.