Hindawi
Security and Communication Networks
Volume 2021, Article ID 6662700, 12 pages
https://doi.org/10.1155/2021/6662700

Research Article

A Novel HDR Image Zero-Watermarking Based on Shift-Invariant Shearlet Transform

Shanshan Shi,[1] **Ting Luo**,[2] **Jiangtao Huang**,[1] **and Meng Du**[1]

[1]*Faculty of Information Science and Engineering, Ningbo University, Ningbo 315211, China*
[2]*College of Science and Technology, Ningbo University, Ningbo 315212, China*

Correspondence should be addressed to Ting Luo; luoting@nbu.edu.cn

Received 30 December 2020; Revised 5 March 2021; Accepted 17 March 2021; Published 26 March 2021

Academic Editor: Sen Bai

In this paper, a novel high dynamic range (HDR) image zero-watermarking algorithm against the tone mapping attack is proposed. In order to extract stable and invariant features for robust zero-watermarking, the shift-invariant shearlet transform (SIST) is used to transform the HDR image. Firstly, the HDR image is converted to CIELAB color space, and the $\boldsymbol{L}$ component is selected to perform SIST for obtaining the low-frequency subband containing the robust structure information of the image. Secondly, the low-frequency subband is divided into nonoverlapping blocks, which are transformed by using discrete cosine transform (DCT) and singular value decomposition (SVD) to obtain the maximum singular values for constructing a binary feature image. To increase the watermarking security, a hybrid chaotic mapping (HCM) is employed to get the scrambled watermark. Finally, an exclusive-or operation is performed between the binary feature image and the scrambled watermark to compute robust zero-watermark. Experimental results show that the proposed algorithm has a good capability of resisting tone mapping and other image processing attacks.

1. Introduction

Recently, people have more extreme requirements for image quality and visual perception. Traditional low dynamic range (LDR) images have a very limited ability to record the wide dynamic range, which causes that the light area is overexposed and the dark area is underexposed in the real scene [1,2]. Compared with the LDR imaging, the high dynamic range (HDR) imaging technology emerges in order to describe the real scene more accurately and record more detailed information in the light and dark areas [3,4]. As HDR images become more and more common in practical applications [5,6], the copyright protection of the HDR image has received increasing attention. Watermarking technology can effectively protect the copyright of multimedia data and it plays an important role in the field of information security [7–10].

Since the existing LDR display device has a limited dynamic range, the tone mapping (TM) process is required when HDR images are to be displayed on the LDR display device [11]. Thus, different from LDR images, the TM process is an inevitable form of attack for considering the copyright protection of HDR images. However, only a few HDR image watermarking algorithms have been proposed for decades [12–19]. Some watermarking algorithms mainly paid attention to invisibility and embedding capacity and embedded the watermark in the spatial domain of images. Yu et al. [12] and Wang et al. [13] directly used the exponential channel of HDR image with RGBE storage format to guide the lossless watermark embedding. Cheng et al. [14] and Li et al. [15] combined the least significant bit (LSB) technique to embed the watermark with RGBE storage format and LogLuv (TIFF) storage format, respectively. Lin et al. used the 10-digit mantissa in OpenEXR format to convey secret data [16]. Besides, other HDR watermarking algorithms mostly considered the structural features of the HDR image itself and completed the watermark embedding in the transform domain. Guerrini et al. embedded watermark in the low-frequency band of the discrete wavelet transformation (DWT) domain by

using quantization index modulation (QIM) [17]. This algorithm achieved good imperceptibility, but the bit error rate (*BER*) of watermark extraction was high. Solachidis et al. decomposed the HDR image into a set of LDR images with different exposure by using a bracketing process, and the watermark was embedded into the DWT domain of the image sequence [18]. However, the corresponding imperceptibility was not satisfied. In order to preserve strong relationships of three color channels of HDR images, Luo et al. proposed a HDR image watermarking method based on feature map extraction by using Tucker decomposition [19], which can resist different TM attacks and most common image processing attacks.

In order to improve the watermarking robustness, the above HDR watermarking algorithms will increase the watermarking strength for robustness, which leads to image distortion. Thus, it is a contradiction between watermarking imperceptibility and robustness. Moreover, minor modification is not required for some HDR medical images and HDR remote sensing images, and it is necessary to design an algorithm that has no damage to the image at all. To solve this problem, Wen et al. proposed a zero-watermarking algorithm, which was a lossless watermarking algorithm and overcame the image quality degradation for traditional watermarking algorithms [20]. In general, the zero-watermarking algorithm extracts the intrinsic features of the original image to compute the robust zero-watermark without affecting the image quality and obtains a balance between invisibility and robustness of watermarking. Similar to zero-watermarking, image hashing is also a process of extracting features from the original image and converts the image into a short numeric representation. However, it is mainly used for integrity verification of images [21,22]. Moreover, the image hashing provides effective support for the content of the image, which can be used to assist the zero-watermarking [23,24].

To our knowledge, HDR image zero-watermarking algorithms were rarely reported, and only some LDR image zero-watermarking algorithms were presented. The zero-watermarking is mainly classified into spatial domain based and transform domain based watermarking algorithms. In the spatial domain based algorithm, the feature matrix is obtained by extracting the characteristics from the spatial domain directly. Xiong et al. proposed a robust zero-watermarking based on the spatial domain by comparing the size between the whole mean of the image and the block mean to construct the feature matric [25]. The transform domain based zero-watermarking algorithm is more robust than the spatial domain based algorithm, and different transform domains are used to design robust zero-watermarking. Pan et al. proposed a color image zero-watermarking algorithm based on DWT and singular value decomposition (SVD) [26]. Cui et al. presented a zero-watermarking algorithm based on DWT by selecting image wavelet coefficients to construct zero-watermark [27], which was robust to various image attacks. To get high watermarking robustness, some multiscale transforms are regarded as the extension of the wavelet transform and have been applied to zero-watermarking, such as Contourlet and Shearlet. Zhu et al. presented a color image zero-watermarking algorithm based on Schur decomposition and contour-let transform [28], which was good at resisting rotation and compression attacks. The shearlet transform has its advantage of optimal sparse representations for multidimensional data and is a compactly supported transform. Mardanpour et al. designed a watermarking based on shearlet transform and bidiagonal singular value decomposition [29], which was robust to most of image attacks, including rotation and translation. Subramani et al. presented a robust watermarking algorithm based on shearlet transform and QR matrix decomposition for resisting various attacks [30]. Wang et al. presented a zero-watermarking algorithm based on nonsubsampled pyramid decomposition (NSPD) and discrete cosine transform (DCT) but was not robust to combined image attacks [31]. Though shearlet transform is used in watermarking frequently, it lacks strong shift-invariant. To efficiently analyze the geometric structure of HDR image and achieve the shift-invariant of the geometric structure, the shift-invariant shearlet transform (SIST) as an advanced multiscale geometric analysis is employed. SIST can extract stable information from images efficiently and has no downsampling process when it is multiscale decomposed. For the copyright protection of the HDR image, we can apply the SIST to extract the stable and invariant structure features to construct robust zero-watermark.

This paper proposes a HDR image zero-watermarking algorithm based on SIST, DCT, and SVD [32]. The SIST is operated on the HDR image for computing the low-frequency subband, and the invariant geometrical structures of the HDR image are extracted. To obtain the stability of the feature matrix, the DCT and SVD are used to decompose the low-frequency subband successively. To enhance the robustness of zero-watermarking, an adjacent comparison is designed to construct a binary feature image. A hybrid chaotic mapping (HCM) is used to generate the scrambled watermark for security, and an exclusive-or operation is performed between the binary feature image and the scrambled watermark to obtain zero-watermark. The experimental results show that the proposed algorithm can effectively resist different TM attacks and most of the common image attacks. The contributions of this paper are listed as follows:

(1) A novel robust HDR image zero-watermarking algorithm based on SIST is proposed

(2) In order to extract stable and invariant features from the HDR image, the SIST is applied to transform the HDR image

(3) Experimental results show that the proposed HDR image zero-watermarking algorithm is more robust than some existing HDR image zero-watermarking algorithms

The rest of this paper is organized as follows: Section 2 briefly introduces the ST, SIST, and the HCM system. Section 3 explains the proposed HDR image zero-watermarking scheme. Section 4 provides the experimental results and analysis. Section 5 draws a conclusion.

2. Theoretical Basis

In this section, shearlet transform (ST), shift-invariant shearlet transform (SIST), and hybrid chaotic mapping (HCM) used in the proposed algorithm are briefly introduced.

2.1. Shearlet Transform (ST). ST is a basic function generated by an affine transformation and expresses the characteristics of a curve in two-dimensional or even multidimensional space for achieving optimal linear error approximation. A continuous ST is represented as

$$S_\psi = \langle f, \psi_{j,l,k} \rangle, \tag{1}$$

where **f** is the signal and $\psi_{j,l,k}$ is shearlet basis function and defined as

$$\psi_{j,k,l}(x) = |\det A|^{j/2} \psi\left(B^l A^j x - k\right) \tag{2}$$

where **j** is a scale parameter, **l** is a direction parameter, **k** is a translation parameter, *det* represents the determinant of the matrix, **A** and **B** are 2×2 invertible matrices, $\mathbf{A^j}$ represents a scale transformation matrix, and $\mathbf{B^l}$ means the geometric transformation matrix when the area is constant. In the transform domain, shearlet $\psi_{j,l,k}$ with different characteristics represents a trapezoidal pair of relative origin symmetry. Each shearlet is supported on a pair of trapezoids, and each one contains a box with the size of approximately $2^j \times 2^{2j}$, which means shearlet has strong selectivity of anisotropic directionality [33].

2.2. SIST. SIST is designed on the basis of shearlet transform and can be completed by using multiscale partition and directional localization [34].

In the multiscale partition, the shift-invariant means little sensitivity to the image shift and can be achieved by the nonsubsampled pyramid filter. In the directional localization, the frequency plane is decomposed into a low-frequency subband and several trapezoidal high-frequency subbands by SIST. SIST removes the subsampling operation from the traditional ST, and the decomposed subband image is the same size as the original image. SIST has a good localization in the transform domain and shift-invariant property, and its process can be summarized as illustrated in Figure 1. In Figure 1, **f** represents the original image, and $\mathbf{f_{h1}}$ and $\mathbf{f_{l1}}$ indicate the high-frequency image and low-frequency image, respectively, after the first layer Laplace pyramid decomposition. $\mathbf{f_{s1}}$ represents the direction subband image after the first layer direction decomposition of $\mathbf{f_{h1}}$.$\mathbf{f_{h2}}$ and $\mathbf{f_{l2}}$ indicate the high-frequency image and low-frequency image, respectively, after the second layer Laplace pyramid decomposition.

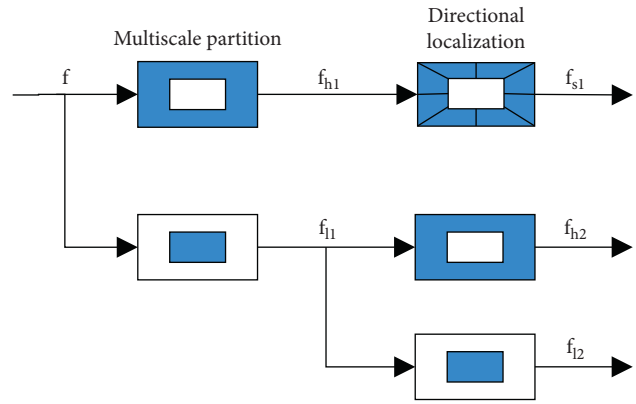


Figure 1: The process of SIST.

To reflect the SIST decomposition process intuitively, Figure 2 shows the low-frequency subband after SIST of the HDR image Rend10. From Figure 2, we can see the low-frequency subband mainly includes approximate structure information of the HDR image.

2.3. HCM. The HCM mainly includes two typical chaotic systems: the logistic mapping (LM) [35] and the piecewise linear chaotic mapping (PWLCM) [36]. The LM is defined as

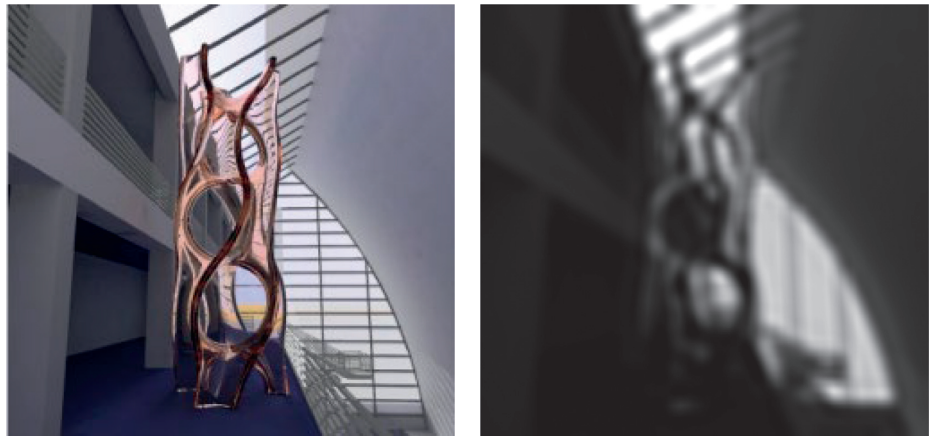
$$x_{k+1} = \mu x_k (1 - x_k), \tag{3}$$

where $x_0 \notin \{0, 0.25, 0.5, 0.75\}$, $\mu \in [0, 4]$ is the control parameter, and x_k is the chaos sequence of the map. Furthermore, since PWLCM has properties including uniform distribution, good ergodicity, confusion, and diffusion, it is also utilized for encrypting watermark. PWLCM can be described as

$$x_{k+1} = F(x_k, p) = \begin{cases} \dfrac{x_k}{p}, & x_k \in [0, p], \\ \dfrac{(x_k - p)}{(0.5 - p)}, & x_k \in [p, 0.5], \\ F(1 - x_k, p), & x_k \in [0.5, 1], \end{cases} \tag{4}$$

where $x_k \in (0, 1)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $p \in (0, 0.5)$ is the control parameter.

To enhance the security of the proposed algorithm, we replace the control parameter p of the above PWLCM system with a variable parameter p_k, and p_k depends on the random sequence generated from x_k. To satisfy $p \in (0, 0.5)$, we make p_k to be a third of x_k. The mixed chaos mapping system can be presented as



(a) (b)

Figure 2: The HDR image Rend10 and the low-frequency subband. (a) Rend10. (b) Low-frequency subband.

$$\begin{cases} x_{k+1} = \mu x_k(1-x_k), p_k = x_k/3, \\ \quad \dfrac{y_k}{p_k}, \qquad y_k \in [0, p], \\ y_{k+1} = \dfrac{(y_k - p_k)}{(0.5 - p_k)}, \qquad y_k \in [p_k, 0.5], \\ \quad F(1 - y_k, p_k), \quad y_k \in [0.5, 1]. \end{cases} \tag{5}$$

Parameter μ is regarded as a private key. In the proposed watermarking algorithm, equation (5) is used to generate hybrid sequences for watermark image encryption.

3. Proposed Zero-Watermarking Algorithm

In this section, we present a zero-watermarking by using SIST, DCT, and SVD. In the following, processes of zero-watermark generation and verification are described in detail.

3.1. Zero-Watermark Generation. Let $\boldsymbol{f}$ be the original HDR image with the size of $M \times M$ and $\mathbf{W}$ the original binary watermark with the size of $N \times N$, where $N = M \div n$. Figure 3 shows the process of zero-watermark generation, and the main steps are described in detail as follows:

Step 1. Original watermark scrambling and encryption.

To enhance the security of the watermark, the watermark is scrambled and encrypted. The original watermark $\mathbf{W}$ is scrambled by the Arnold transform to obtain $\boldsymbol{W_1}$ with the private keys $\boldsymbol{k_1}$:

$$W_1 = \text{Arnold}(W), \tag{6}$$

where Arnold (•) means Arnold transform and a random sequence $\mathbf{Y_1} = \{\mathbf{y_n} \,|\mathbf{n = 1, 2, \ldots, N^2}\}$ is generated by using equation (9). $\mathbf{Y_1}$ is converted into a binary image denoted by $\boldsymbol{G}$. An exclusive-or operation is performed between $\mathbf{G_1}$ and $\mathbf{W_1}$ to obtain the encrypted watermark $\mathbf{W_2}$:

$$W_2 = XOR(W_1, G_1). \tag{7}$$

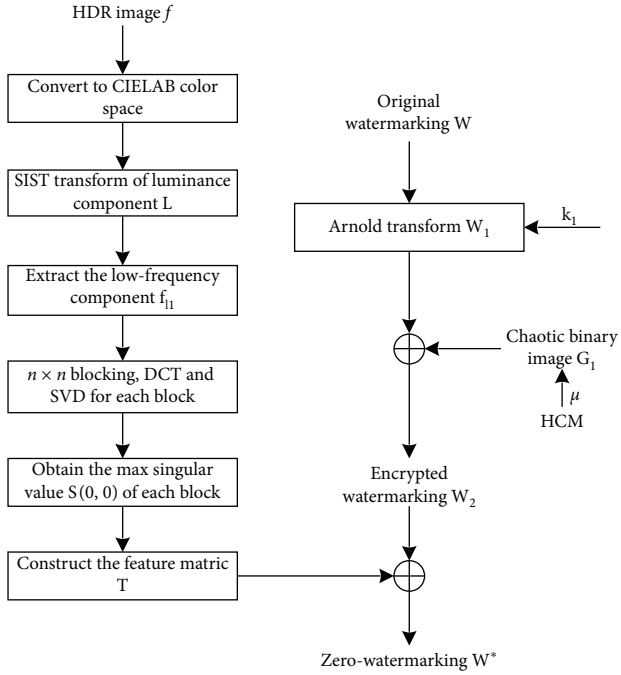


Figure 3: The process of zero-watermark generation.

Step 2. Robust feature extraction.

To obtain the optimal representation of the HDR image and resist different types of image attacks, robust image features are extracted. Firstly, the HDR image $\mathbf{f}$ was converted to CIELAB color space, and then the luminance component $\mathbf{L}$ is operated by using SIST to compute the low-frequency $\mathbf{f_{l1}}$. $\mathbf{f_{l1}}$ is divided into nonoverlapping blocks $\mathbf{B}$ with the size of $n \times n$.

Secondly, apply DCT on **B** to retrieve the DC coefficients **F(u, v)**, where **u, v** = 0, 1, 2, ..., n-1.

Thirdly, apply SVD on **F(u, v)** to obtain the diagonal matrix **S(u, v)**; the maximum singular value **S(0, 0)** is extracted.

Step 3. Feature vector construction.

To compute zero-watermark, the robust binary vector is computed by comparing the maximum singular values of each block. The maximum singular values **S(0, 0)** of all blocks are arranged in a vector and then the feature matrix **T** is constructed by comparing the relative size of the maximum singular value of each block:

$$T = \begin{pmatrix} 1, & if\ S_{i+1}(0,0) > S_i(0,0), \\ 0, & \text{others}, \end{pmatrix}, \tag{8}$$

where $i = 0, 1, 2, 3, ..., n-1$.

Step 4. Zero-watermark construction.

To construct the zero-watermark, an exclusive-or operation is performed between the encrypted watermark $\boldsymbol{W_2}$ and $\boldsymbol{T}$ to generate zero-watermark $\mathbf{W}^*$.

$$W^* = XOR(W_2, T). \tag{9}$$

Step 5. Zero-watermark preservation.

For security, the obtained zero-watermark $\mathbf{W}^*$ and secret key k_1 were registered in a third-party intellectual property rights (IPR) database for copyright protection.

3.2. Zero-Watermark Verification. Suppose $\mathbf{f}^*$ is the image to be verified, and it may have undergone certain TM attacks. Figure 4 shows the process of zero-watermark extraction for copyright verification, and the detailed steps are depicted as follows:

Step 1. Feature extraction from $\mathbf{f}^*$.

Firstly, the HDR image $\mathbf{f}^*$ was converted to CIELAB color space, and then the luminance component $\mathbf{L}^*$ is operated by using SIST to compute the low-frequency $\mathbf{f_{l1}}^*$. $\mathbf{f_{l1}}^*$ is divided into nonoverlapping blocks $\mathbf{B}^*$ with the size of $n \times n$.

Secondly, apply the DCT on $\mathbf{B}^*$ to retrieve the DC coefficients $\mathbf{F}^*$**(u, v)**, where **u,v** = 0, 1, 2, ..., n-1.

Thirdly, apply the SVD on $\mathbf{F}^*$**(u, v)** to obtain the diagonal matrix $\mathbf{S}^*$**(u, v)**; the maximum singular value $\mathbf{S}^*$**(0, 0)** is extracted.

Step 2. Feature vector construction.

The maximum singular values $\mathbf{S}^*$**(0, 0)** of all blocks form a vector and then the feature matrix $\boldsymbol{T}^*$ is constructed by comparing the relative size of the maximum singular value of each block:

$$T* = \begin{cases} 1, & \text{if } S_{i+1} * (0,0) > S_i(0,0), \\ 0, & \text{others}. \end{cases} \tag{10}$$

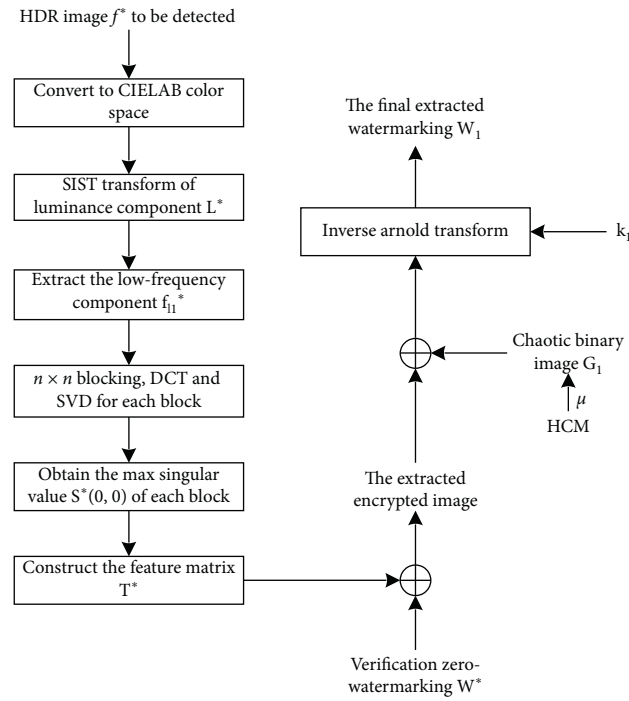


Figure 4: The process of zero-watermark verification.

Step 3. Final watermark extraction.

Then, an exclusive-or operation and the inverse Arnold transform are performed to extract the final watermark $\mathbf{W_1}$:

$$W_1 = \text{Arnold}^{-1}(XOR(T*, W*), G_1). \tag{11}$$

The extracted $\mathbf{W_1}$ and the original binary watermark $\mathbf{W}$ are compared, and if they are similar, the certification is accomplished.

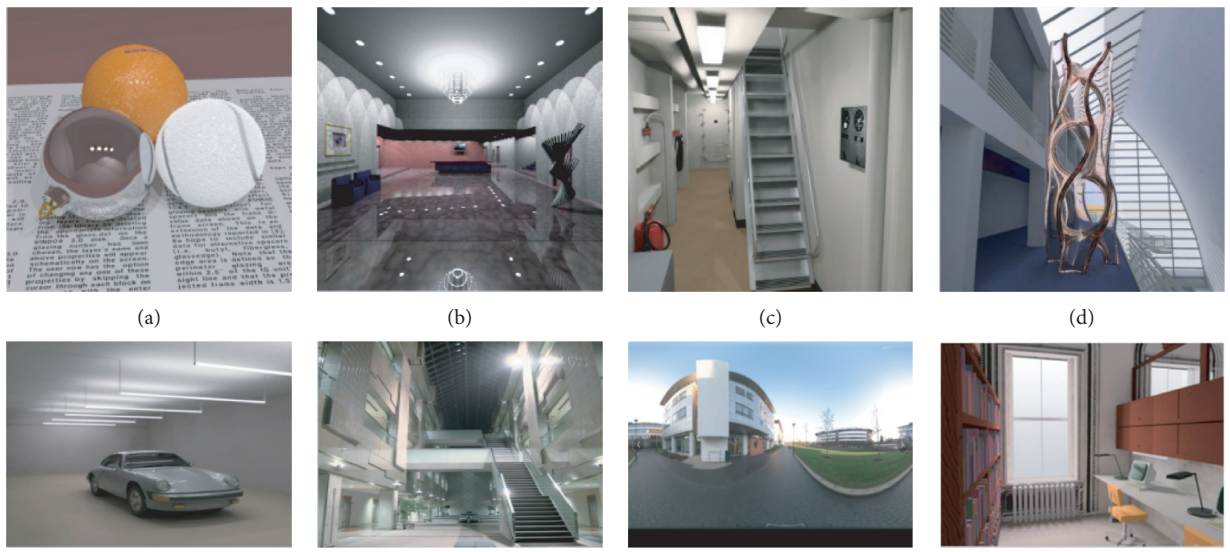
4. Experimental Results and Analysis

Eight HDR images are selected from the website Gred Ward for testing as illustrated in Figure 5. 14 typical TM attacks are selected to evaluate the watermarking robustness. Watermark is a binary image with the word "NB," as illustrated in Figure 6 and the Arnold scrambling secret key $k_1 = 29$.

The robustness of watermarking means the capability of withstanding various unintentional attacks, including TM attacks and common image processing attacks. The robustness is evaluated by the bit error rate (*BER*) [35] and normalized cross-correlation (*NC*) [9] between the original watermark and extracted watermark. They are defined as equations (12) and (13), respectively:

$$BER = \frac{N_e}{N_t}, \tag{12}$$

where $\mathbf{N_e}$ represents the error bits number of a watermark and $\mathbf{N_t}$ represents the total bits number of a watermark.



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

(e) (f) (g) (h)

Figure 5: Original HDR images. (a) Rend01 (1024 × 1024). (b) Rend07 (575 × 575). (c) Rend09 (1024 × 1024). (d) Rend10 (1024 × 1024). (e) Rend13 (1024 × 1024). (f) AtriumNight (1016 × 760). (g) CS_Warwick (512 × 1024). (h) Rend11 (735 × 1024).

Figure 6: Original watermark (64 × 64).

$$NC = \frac{\sum_i \sum_j W(i,j) W_1(i,j)}{\sqrt{\sum_i \sum_j W^2(i,j)} \sqrt{\sum_i \sum_j W_1^2(i,j)},} \quad (13)$$

where $\mathbf{W(i, j)}$ and $\mathbf{W_1(i, j)}$ represent the original watermark and extracted watermark, respectively.

4.1. Uniqueness Verification of Zero-Watermarking. In this subsection, we discuss the uniqueness verification of zero-watermark, and zero-watermark constructed from an image should only be relevant to this image. In other words, zero-watermark generated from different original images should be different. Table 1 exhibits the similarities between the zero-watermark binary images generated from eight original HDR images, and the similarity calculation is based on equation (13).

From Table 1, the maximum and minimum similarities are 0.5903 and 0.7014, respectively, which are far less than 1. Thus, it can be easily seen that the zero-watermark from different original HDR images has a low similarity and is distinguishable.

4.2. Robustness of Zero-Watermarking. In this subsection, the robustness of the proposed algorithm under TM attacks and common image processing attacks is tested, and corresponding *NC* and *BER* are computed.

4.2.1. Robustness Test for TM Attacks. In order to evaluate the robustness of the proposed algorithm on TM attacks, 14 TM attacks are selected to attack the original HDR images. The TM attacks are consisting of KrawczykTMO, GammaTMO, AshikhminTMO, DragoTMO, Logarithmic TMO, MertensTMO, WardGlobalTMO, WardHistAdj TMO, LischinskiTMO, ReinhardDevlinTMO, RamanTMO, TumblinRushmeierTMO, DurandTMO, and FattalTMO as shown in Table 2.

Table 3 shows *BER*s of the proposed algorithm for eight attacked images. From Table 3, it is clearly seen that *BER*s of eight HDR images are higher than 0.75, which means the copyright of the HDR image can be declared. For most of the TM attacks, the corresponding *BER*s of the proposed algorithm are lower than 0.1, and only, for TM13 and TM14, *BER*s are a little higher but still lower than 0.75. The average *BERs* of different TM attacks are lower than 0.1, and they show that the proposed algorithm is robust to different TM attacks. Table 4 also shows similar results, and *NC*s of the proposed algorithm are higher than 0.8, which proves the robustness.

4.2.2. Robustness Test for Common Image Processing Attacks. Besides resisting TM attacks, the proposed algorithm is also robust to common image processing attacks. 10 different common image processing attacks are operated on the original HDR images, such as adding noise, filtering, scaling, cropping, rotation, and *BER*s and *NC*s of the proposed algorithm are listed as shown in Table 5 and 6, respectively.

Table 1: Similarities between the zero-watermark generated from eight HDR images.

Image	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
Rend01	1	0.6672	0.6528	0.5927	0.6402	0.6521	0.6824	0.6154
Rend07	0.6672	1	0.6376	0.6089	0.6809	0.6138	0.6536	0.6346
Rend09	0.6528	0.6376	1	0.6273	0.6338	0.6072	0.7014	0.6417
Rend10	0.5927	0.6089	0.6273	1	0.6238	0.6105	0.6117	0.6438
Rend13	0.6402	0.6809	0.6338	0.6238	1	0.6569	0.6478	0.6505
Rend11	0.6521	0.6138	0.6072	0.6105	0.6569	1	0.5958	0.6547
CS_Warwick	0.6824	0.6536	0.7014	0.6117	0.6478	0.5958	1	0.5903
Rend11	0.6154	0.6346	0.6417	0.6438	0.6505	0.6547	0.5903	1

Table 2: Attacks used in experiments.

Number	TM attacks	Number	Common attacks
TM1	KrawczykTMO	CA1	'Salt&Pepper' (0.001)
TM2	GammaTMO	CA2	Median filter (3×3)
TM3	AshikhminTM0	CA3	Median filter (5×5)
TM4	LogarithmicTMO	CA4	Scaling (4)
TM5	MertensTMO	CA5	Scaling (1/4)
TM6	WardGlobalTMO	CA6	Gaussian low-pass filter (3×3)
TM7	WardHistAdjTMO	CA7	Poisson noise
TM8	LischinskiTMO	CA8	Image sharpen (0.5)
TM9	ReinhardDevlinTMO	CA9	Average filter (4×4)
TM10	RamanTMO	CA10	Imrotate (10)
TM11	DragoTMO		
TM12	TumblinRushmeierTMO		
TM13	DurandTMO		
TM14	FattalTMO		

Table 3: *BER*s of eight HDR images under different TM attacks.

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
TM1	0.0198	0.0796	0.0161	0.0698	0.0359	0.0195	0.0503	0.0862
TM2	0.0142	0.0698	0.0208	0.0291	0.0393	0.0220	0.0474	0.0698
TM3	0.0417	0.0850	0.0527	0.0737	0.0457	0.0713	0.0496	0.0718
TM4	0.0085	0.0303	0.0078	0.0205	0.0115	0.0115	0.0078	0.0232
TM5	0.0730	0.1040	0.0796	0.0908	0.0823	0.0862	0.0732	0.1309
TM6	0.0112	0.0059	0.0042	0.0081	0.0027	0.0059	0.0049	0.0203
TM7	0.0254	0.0728	0.0383	0.0291	0.0610	0.0356	0.0439	0.0457
TM8	0.0032	0.0718	0.0120	0.0269	0.0244	0.0217	0.0862	0.0586
TM9	0.0146	0.0569	0.0349	0.0317	0.0342	0.0325	0.0271	0.0522
TM10	0.0337	0.1006	0.0632	0.0688	0.0344	0.0608	0.0527	0.0857
TM11	0.0161	0.0627	0.0232	0.0278	0.0356	0.0317	0.0300	0.0420
TM12	0.0088	0.0190	0.0100	0.0132	0.0076	0.0110	0.0156	0.0225
TM13	0.1663	0.2690	0.1548	0.2327	0.1707	0.1550	0.1814	0.1506
TM14	0.1956	0.0811	0.0972	0.1501	0.0862	0.1047	0.2178	0.1775
Average	0.0451	0.0791	0.0439	0.0623	0.0479	0.0478	0.0634	0.0740

Tables 5 and 6 show *BER*s and *NC*s of the proposed algorithm when the HDR image is attacked by ten common image processing attacks as listed in Table 2. From the two tables, we can see that the averages of *BER* of eight HDR images are all below 5%, and the minimum value is 2.18%. The averages of *NC* of eight HDR images are all higher than 96%, and the maximum value is 98.58%. It denotes that the proposed algorithm is robust to common image processing attacks.

In order to present watermark extraction visually, Figure 7 shows watermark extraction from *Rend01* under different attacks. The most reconstructed watermark can be seen clearly, which means the watermark can be extracted for copyright protection. Similar results can be obtained from other HDR images, and it is proved that the proposed algorithm is robust to TM attacks and common image processing attacks.

In order to test the robustness of the proposed algorithm again, a pseudorandom code is used as a watermark. BERs of the proposed algorithm for resisting TM attacks are shown in Table 7. From Table 7, we can see that most BERs of eight HDR images are below 5%, which denotes the robustness of the proposed algorithm. Moreover, for resisting common image processing attacks, BERs are all below 5% and the

Table 4: *NC*s of eight HDR images under different TM attacks.

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
TM1	0.9874	0.9486	0.9898	0.9550	0.9771	0.9876	0.9678	0.9442
TM2	0.9910	0.9551	0.9868	0.9815	0.9749	0.9861	0.9697	0.9550
TM3	0.9733	0.9451	0.9662	0.9525	0.9708	0.9542	0.9683	0.9537
TM4	0.9944	0.9807	0.9951	0.9870	0.9927	0.9927	0.9951	0.9853
TM5	0.9529	0.9324	0.9486	0.9412	0.9469	0.9443	0.9529	0.9144
TM6	0.9929	0.9963	0.9974	0.9949	0.9983	0.9963	0.9969	0.9871
TM7	0.9839	0.9531	0.9755	0.9815	0.9608	0.9773	0.9719	0.9708
TM8	0.9980	0.9538	0.9924	0.9829	0.9845	0.9862	0.9443	0.9624
TM9	0.9907	0.9636	0.9777	0.9798	0.9782	0.9793	0.9828	0.9665
TM10	0.9785	0.9347	0.9593	0.9557	0.9781	0.9611	0.9662	0.9446
TM11	0.9898	0.9597	0.9852	0.9823	0.9773	0.9798	0.9809	0.9732
TM12	0.9944	0.9879	0.9937	0.9916	0.9952	0.9930	0.9901	0.9857
TM13	0.8899	0.8164	0.8981	0.8426	0.8869	0.8978	0.8796	0.9009
TM14	0.8923	0.9478	0.9370	0.9011	0.9443	0.9320	0.8538	0.8823
Average	0.9721	0.9482	0.9716	0.9592	0.9690	0.9691	0.9586	0.9519

Table 5: *BER*s of eight HDR images under common image processing attacks.

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
CA1	0.0400	0.0479	0.0132	0.0298	0.0376	0.0149	0.0374	0.0776
CA2	0.0168	0.0044	0.0049	0.0076	0.0017	0.0093	0.0024	0.0098
CA3	0.0510	0.0098	0.0107	0.0151	0.0032	0.0200	0.0042	0.0215
CA4	0.0027	0.0115	0.0012	0.0344	0.0007	0.0020	0	0.0015
CA5	0.0046	0.0437	0.0029	0.0491	0.0027	0.0046	0	0.0042
CA6	0.0081	0.0046	0.0032	0.0137	0.0037	0.0046	0.0009	0.0042
CA7	0.0017	0.0461	0.0081	0.0137	0.0247	0.0107	0.0288	0.0461
CA8	0.0073	0.0544	0.0142	0.0249	0.0305	0.0259	0.0295	0.0542
CA9	0.0273	0.0083	0.0073	0.0300	0.0105	0.0122	0.0042	0.0083
CA10	0.2261	0.2122	0.1523	0.2021	0.1465	0.2102	0.1506	0.2122
Average	0.0386	0.0443	0.0218	0.0420	0.0261	0.0314	0.0258	0.0439

Table 6: *NC*s of eight HDR images under common image processing attacks.

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
CA1	0.9745	0.9694	0.9916	0.9810	0.9760	0.9906	0.9762	0.9499
CA2	0.9893	0.9972	0.9969	0.9952	0.9989	0.9941	0.9985	0.9938
CA3	0.9674	0.9938	0.9932	0.9904	0.9980	0.9873	0.9974	0.9864
CA4	0.9983	0.9927	0.9992	0.9781	0.9995	0.9988	1	0.9991
CA5	0.9971	0.9721	0.9981	0.9686	0.9983	0.9971	1	0.9974
CA6	0.9949	0.9971	0.9980	0.9913	0.9977	0.9971	0.9994	0.9974
CA7	0.9989	0.9705	0.9949	0.9913	0.9843	0.9932	0.9817	0.9705
CA8	0.9954	0.9653	0.9910	0.9842	0.9806	0.9832	0.9812	0.9668
CA9	0.9826	0.9947	0.9954	0.9809	0.9933	0.9923	0.9974	0.9923
CA10	0.8480	0.8579	0.8996	0.8648	0.9036	0.8590	0.9011	0.8293
Average	0.9746	0.9710	0.9858	0.9726	0.9830	0.9793	0.9833	0.9683

minimum is 2.13% as shown in Table 8. Thus, the proposed algorithm is still robust when the watermark is a pseudo-random code.

4.3. Robustness Comparison. In order to ensure the rationality of the comparative experiment, the proposed algorithm is compared with Wang's zero-watermarking algorithm [37] and Bai's watermarking algorithm [38] in terms of robustness against different TM attacks. HDR images and TM attacks used in this experiment are consistent with the two comparative algorithms. The comparison results are given in Table 9, in which the bold font indicates the best one.

Table 9 shows *BER*s of three comparison algorithms for resisting TM attacks, and we can see most of *BER*s of the proposed algorithm are lower than those of Wang's and Bai's. Moreover, average *BER* of the proposed algorithm being 4.51% is much lower than those of Wang's and Bai's, thus the above comparative experiments prove the robustness of the proposed algorithm again.

4.4. Computation Time of Zero-Watermarking. In order to verify the efficiency of the proposed zero-watermarking algorithm, the average computation time of the zero-watermark generation and extraction for the eight HDR images are tested.

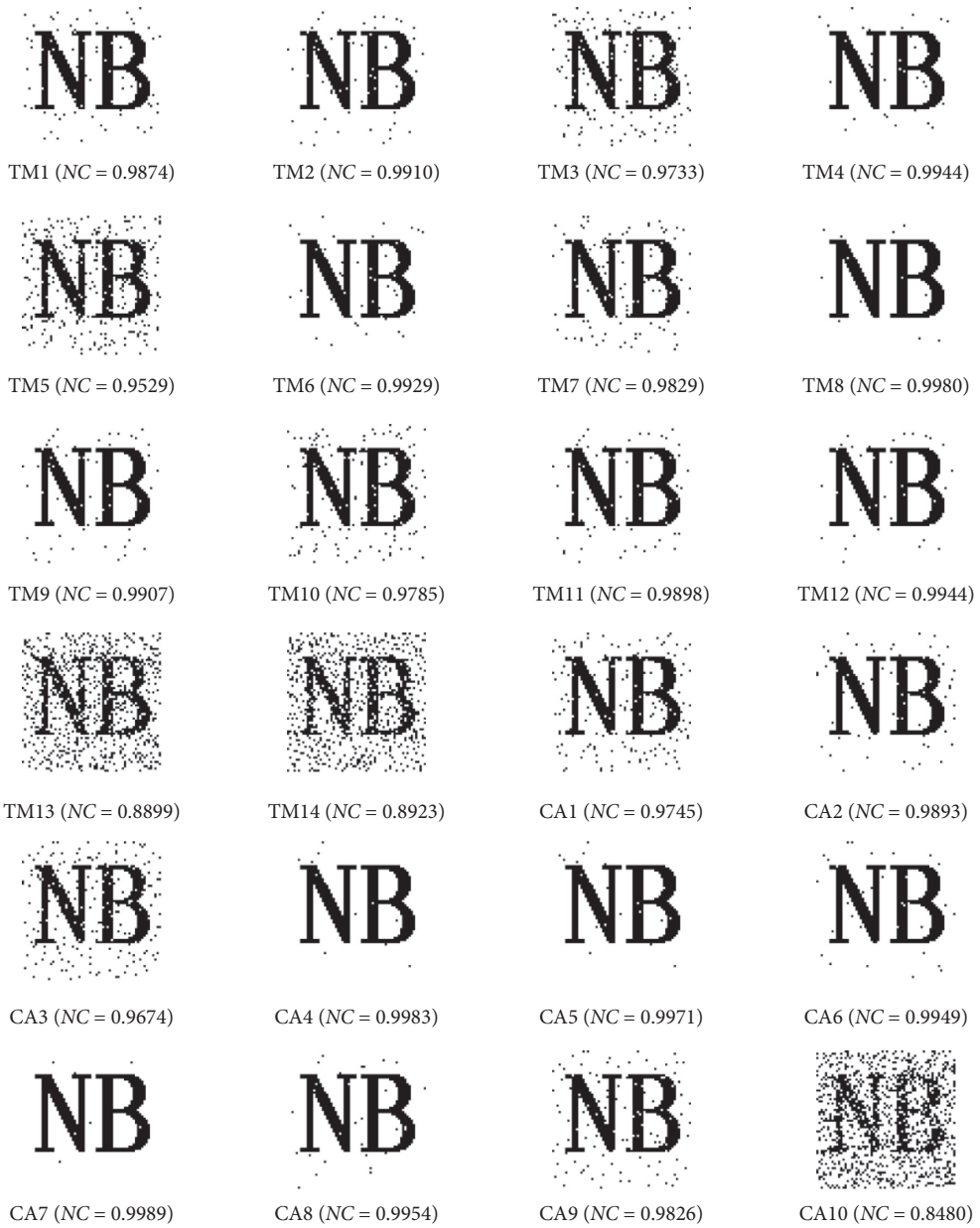


Figure 7: Extracted watermarks for Rend01 image under different attacks.

Table 7: *BER*s of eight HDR images under different TM attacks (a pseudorandom code as a watermark).

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
TM1	0.0174	0.0763	0.0157	0.0682	0.0363	0.0176	0.0500	0.0850
TM2	0.0153	0.0676	0.0211	0.0310	0.0385	0.0218	0.0477	0.0686
TM3	0.0407	0.0844	0.0520	0.0732	0.0368	0.0710	0.0480	0.0706
TM4	0.0090	0.0297	0.0089	0.0201	0.0116	0.0113	0.0065	0.0240
TM5	0.0619	0.1035	0.0776	0.0909	0.0830	0.0854	0.0702	0.1297
TM6	0.0080	0.0047	0.0040	0.0085	0.0020	0.0048	0.0038	0.0200
TM7	0.0310	0.0732	0.0378	0.0311	0.0558	0.0360	0.0430	0.0453
TM8	0.0024	0.0724	0.0125	0.0270	0.0236	0.0229	0.0854	0.0580
TM9	0.0152	0.0574	0.0352	0.0322	0.0359	0.0336	0.0263	0.0529
TM10	0.0368	0.1001	0.0622	0.0658	0.0325	0.0600	0.0532	0.0838
TM11	0.0101	0.0630	0.0231	0.0304	0.0349	0.0305	0.0298	0.0418
TM12	0.0082	0.0187	0.0110	0.0143	0.0062	0.0112	0.0158	0.0228
TM13	0.1572	0.2649	0.1561	0.2330	0.1711	0.1540	0.1804	0.1500
TM14	0.1902	0.0802	0.0970	0.1508	0.0840	0.1043	0.2162	0.1769
Average	0.0431	0.0782	0.0438	0.0626	0.0465	0.0474	0.0626	0.0735

Table 8: *BER*s of eight HDR images under common image processing attacks (a pseudorandom code as a watermark).

	Rend01	Rend07	Rend09	Rend10	Rend13	AtriumNight	CS_Warwick	Rend11
CA1	0.0402	0.0473	0.0130	0.0290	0.0370	0.0144	0.0366	0.0770
CA2	0.0170	0.0040	0.0044	0.0066	0.0012	0.0090	0.0020	0.0094
CA3	0.0510	0.0096	0.0102	0.0144	0.0030	0.0198	0.0035	0.0213
CA4	0.0020	0.0116	0.0008	0.0336	0.0003	0.0022	0	0.0016
CA5	0.0045	0.0433	0.0026	0.0487	0.0039	0.0041	0	0.0040
CA6	0.0078	0.0038	0.0030	0.0130	0.0035	0.0044	0.0007	0.0042
CA7	0.0010	0.0460	0.0079	0.0135	0.0244	0.0101	0.0287	0.0457
CA8	0.0066	0.0538	0.0140	0.0250	0.0301	0.0247	0.0286	0.0540
CA9	0.0275	0.0081	0.0064	0.0297	0.0102	0.0120	0.0040	0.0082
CA10	0.2250	0.2120	0.1505	0.2017	0.1460	0.2008	0.1537	0.2113
Average	0.0382	0.0439	0.0213	0.0415	0.0259	0.0302	0.0258	0.0436

Table 9: Robustness comparisons in resisting TM attacks.

Number	Attack type	Wang's [37] *BER*	Bai's [38] *BER*	Proposed *BER*
1	TM1	0.0456	0.1104	**0.0198**
2	TM2	0.0387	0.1234	**0.0142**
3	TM3	0.0723	0.0697	**0.0417**
4	TM4	0.0237	0.0687	**0.0085**
5	TM5	0.1010	**0.0615**	0.0730
6	TM6	0.0254	0.0560	**0.0112**
7	TM7	0.0431	0.0707	**0.0254**
8	TM8	0.0391	0.0538	**0.0032**
9	TM9	0.0488	0.1199	**0.0146**
10	TM10	0.0940	0.0964	**0.0337**
11	TM11	0.0413	0.0685	**0.0161**
12	TM12	0.0364	0.0809	**0.0088**
13	TM13	0.2044	**0.0666**	0.1663
14	TM14	0.1410	**0.1389**	0.1956
Average	0.0682	0.0847	**0.0451**	

Table 10: Average running time of the proposed algorithm for eight HDR images.

	Zero-watermark generation	Zero-watermark extraction under TM attacks				
		TM1	TM2	TM3	TM4	TM5
Time (s)	1.4125	1.3500	1.3341	1.5160	1.3126	1.2982

The computer used for our experiments had a 1.50 GHz processor, 4 GB RAM, and a Microsoft Windows 7 operating system with 64 bits. The experiments were completed in the environment of MATLAB 2019a. The average running time of the zero-watermark generation and extraction for the eight HDR images is less than 2 seconds as shown in Table 10, which denotes the proposed algorithm is acceptable in real applications.

5. Conclusion

In this paper, a novel HDR image zero-watermarking algorithm based on shift-invariant shearlet transform (SIST), discrete cosine transform (DCT), and singular value decomposition (SVD) is proposed. In order to extract the invariant information of the HDR image, the SIST technique is used to transform the $\boldsymbol{L}$ component of CIELAB color space. To obtain the stability of the characteristic matrix, the DCT and SVD are used to decompose the low-frequency image successively. To enhance the robustness of zero-watermarking, an adjacent comparison is designed to construct a binary feature image. Finally, an exclusive-or operation is performed between the binary feature image and scrambled watermark image to obtain a zero-watermark. Moreover, in order to ensure watermarking security, a hybrid chaotic mapping (HCM) is used to get the scrambled watermark. Experimental results show that the proposed algorithm can effectively protect the copyright of the HDR images and is robust to a variety of TM attacks and most of the common image processing attacks. However, the proposed algorithm cannot resist rotate attacks. In the future work, we will explore robust characteristics of the HDR image to improve it.

Data Availability

The datasets used in this paper are mainly obtained through open-source channels and can be downloaded from the dataset website http://www.anyhere.com/gward/hdrenc/pages/originals.html.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant nos. 61971247 and 61501270 and Zhejiang Provincial Natural Science Foundation of China under Grant nos. LY19F020009 and LQ20F010002. It was also sponsored by the K. C. Wong Magna Fund at Ningbo University.

References

[1] R. Aakanksha, "Deep tone mapping operator for high dynamic range images," *IEEE Transactions on Image Processing*, vol. 29, pp. 1285–1298, 2019.

[2] Y. Huang, S. Qiu, C. Wang et al., "Learning representations for high dynamic range image color transfer in a self-supervised way," *IEEE Transactions on Multimedia*, vol. 29, pp. 176–188, 2020.

[3] Z. Pan, M. Yu, G. Jiang, H. Xu, Z. Peng, and F. Chen, "Multi-exposure high dynamic range imaging with informative content enhanced network," *Neurocomputing*, vol. 386, pp. 147–164, 2020.

[4] S. Xie, W. Wu, R. Chen, and H.-Z. Tan, "Reduced-dimensional capture of high-dynamic range images with compressive sensing," *Discrete Dynamics in Nature and Society*, vol. 2020, pp. 1–13, 2020.

[5] V. Hulusic, K. Debattista, G. Valenzise, and F. Dufaux, "A model of perceived dynamic range for HDR images," *Signal Processing: Image Communication*, vol. 51, pp. 26–39, 2017.

[6] Y. Song, G. Jiang, H. Jiang, M. Yu, F. Shao, and Z. Peng, "A new tone-mapped image quality assessment approach for high dynamic range imaging system," in *Proceedings of the. IEEE International Conference on Image Processing*, pp. 1012–1016, Beijing, China, September 2017.

[7] G. Bhatnagar, Q. M. J. Wu, and P. K. Atrey, "Secure randomized image watermarking based on singular value decomposition," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 10, no. 1, pp. 1–21, 2013.

[8] H.-Y. Yang, X.-Y. Wang, P.-P. Niu, and A.-L. Wang, "Robust color image watermarking using geometric invariant quaternion polar harmonic transform," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 11, no. 3, pp. 1–26, 2015.

[9] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal Fourier-Mellin moments and chaotic map for double images," *Signal Processing*, vol. 120, pp. 522–531, 2016.

[10] M. Amirmazlaghani, "Additive watermark detection in the wavelet domain using 2D-GARCH model," *Information Sciences*, vol. 370-371, pp. 1–17, 2016.

[11] D. Kundu, D. Ghadiyaram, A. C. Bovik, and B. L. Evans, "Large-scale crowdsourced study for tone-mapped HDR pictures," *IEEE Transactions on Image Processing*, vol. 26, no. 10, pp. 4725–4740, 2017.

[12] C. Yu, K. Wu, and C. Wang, "A distortion-free data hiding scheme for high dynamic range images," *' Journal of Electronic Science and Technology of China*, vol. 11, pp. 20–26, 2013.

[13] Z. Wang, T. Lin, and C. Chang, "A novel distortion-free data hiding scheme for high dynamic range images," in *Proceeding of the Fourth International Conference On Digital Home*, Guangzhou, China, September 2012.

[14] Y.-M. Cheng and C.-M. Wang, "A novel approach to steganography in high- dynamic-range images," *IEEE Multimedia*, vol. 16, no. 3, pp. 70–80, 2009.

[15] M. Li, N. Huang, and C. Wang, "A data hiding scheme for high dynamic range images," *International Journal of Innovative Computing, Information & Control*, vol. 7, pp. 2021–2035, 2011.

[16] Y.-T. Lin, C.-M. Wang, W.-S. Chen, F.-P. Lin, and W. Lin, "A novel data hiding algorithm for high dynamic range images," *IEEE Transactions on Multimedia*, vol. 19, no. 1, pp. 196–211, 2017.

[17] F. Guerrini, M. Okuda, N. Adami, and R. Leonardi, "High dynamic range image watermarking robust against tone-mapping operators," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 283–295, 2011.

[18] V. Solachidis, E. Maiorana, and P. Campisi, "HDR image multi-bit watermarking using bilateral-filtering-based masking," *Proceeding of SPIE*, vol. 5, no. 8655, 2013.

[19] T. Luo, G. Jiang, M. Yu, H. Xu, and W. Gao, "Robust high dynamic range color image watermarking method based on feature map extraction," *Signal Processing*, vol. 155, pp. 83–95, 2019.

[20] Q. Wen, T. Sun, and S. Wang, "Concept and application of zero-watermark," *Acta Electron Sin*, vol. 31, pp. 214–216, 2003.

[21] I. Bashir, F. Ahmed, J. Ahmad, W. Boulila, and N. Alharbi, "A secure and robust image hashing scheme using Gaussian pyramids," *Entropy*, vol. 21, no. 11, p. 1132, 2019.

[22] S. Qasim Abbas, F. Ahmed, and Y. Chen, "Perceptual image hashing using transform domain noise resistant local binary pattern," *Multimedia Tools and Applications*, vol. 14, pp. 1–27, 2020.

[23] B. Han, J. Li, and Y. Li, "Zero-watermarking algorithm for medical volume data based on difference hashing," *International Journal of Computers Communications & Control*, vol. 10, no. 2, pp. 188–199, 2015.

[24] X. Wang and Y. Zhan, "A zero-watermarking scheme for three-dimensional mesh models based on multi-features," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27001–27028, 2017.

[25] X. Xiong, "A strong robust zero-watermarking scheme based on spatial domain," *Automatic Chemical Report*, vol. 44, pp. 160–175, 2018.

[26] H. Pan, G. Chen, and Y. Ding, "One color image zero-watermarking algorithm based on DWT and SVD," *Journal of Guilin University of Electronic Science and Technology*, vol. 29, pp. 50–53, 2011.

[27] D. Cui, ""Zero-watermarking technology for digital image based on DWT," *Journal of Chengdu Institute of Information Engineering*, vol. 3, pp. 306–308, 2007.

[28] C. Zhu, Y. Li, W. Chi, S. Gao, and D. Fan, "Zero-watermarking algorithm for Contourlet domain color images based on Schur decomposition," *Information Technology and Information*, vol. 2, pp. 89–93, 2019.

[29] M. Mardanpour and M. A. Z. Chahooki, "Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition," *AEU-International Journal of Electronics and Communications*, vol. 70, no. 6, pp. 790–798, 2016.

[30] S. Subramani, L. Omprakash Narayanan, C. Kamalanathan, S. Panda, and B. Sreenivas, "Design of robust image

watermarking technique based on shearlet transform and QR matrix decomposition," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 1, pp. 163–174, 2020.

[31] L. Wang and L. Zhang, "A kernel-learning-based fusion scheme for multi-modal medical image fusion in shift-invariant shearlet transform domain," *Journal of Medical Imaging and Health Informatics*, vol. 8, no. 4, pp. 855–861, 2018.

[32] A. Musrrat, A. C. Wook, P. Millie et al., "A reliable image watermarking scheme based on redistributed image normalization and svd," *Discrete Dynamics In Nature and Society*, vol. 2016, Article ID 326358, 15 pages, 2016.

[33] J. Zhao, W. Xu, S. Zhang, S. Fan, and W. Zhang, "A strong robust zero-watermarking scheme based on shearlets' high ability for capturing directional features," *Mathematical Problems in Engineering*, vol. 2016, Article ID 2643263, 11 pages, 2016.

[34] P. Wang, X. Luo, X. Li et al., "Image fusion based on shift-invariant shearlet transform and stacked sparse autoencoder," *Journal of Algorithms & Computational Technology*, vol. 12, 2018.

[35] 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.

[36] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *The Scientific World Journal*, vol. 2014, no. 4, Article ID 275818, 2014.

[37] R. Wang, S. Han, P. Zhang et al., "A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain," *IEEE Access*, vol. 4, p. 1, 2020.

[38] Y. Bai, G. Jiang, M. Yu, Z. Peng, and F. Chen, "Towards a tone mapping robust watermarking algorithm for high dynamic range image based on spatial activity," *Signal Processing Image Communication*, vol. 77, no. 18, pp. 24521–24535, 2018.