Research Article

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

Shanshan Shi, Ting Luo, Jiangtao Huang, and Meng Du

Faculty of Information Science and Engineering, Ningbo University, Ningbo 315211, China
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

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 [12–19].

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 matrix [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 non-subsampled 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

\[ S_f = \langle f, \psi_{j,l,k} \rangle, \]

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

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

where \( j \) is a scale parameter, \( l \) is a direction parameter, \( k \) is a translation parameter, \( \text{det} \) represents the determinant of the matrix, \( A \) and \( B \) are \( 2 \times 2 \) invertible matrices, \( A^l \) represents a scale transformation matrix, and \( B^l \) 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 \( 2^j \times 2^l \), which means shearlet has strong selectivity of an-isotropic 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 \( f_{h1} \) and \( f_{h2} \) indicate the high-frequency image and low-frequency image, respectively, after the first layer Laplace pyramid decomposition. \( f_{l1} \) represents the direction subband image after the first layer direction decomposition of \( f_{h1}, f_{h2} \) and \( f_{l2} \) indicate the high-frequency image and low-frequency image, respectively, after the second layer Laplace pyramid decomposition.

To reflect the SIST decomposition process intuitively, Figure 2 shows the low-frequency subband after SIST of the HDR image. 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

\[ x_{k+1} = \mu x_k (1 - x_k), \]

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

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

where \( x_k \in (0,1) \) 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
Parameter \( \mu \) 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 \( f \) be the original HDR image with the size of \( M \times M \) and \( W \) the original binary watermark with the size of \( N \times N \), where \( N = M/2 \). 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 \( W \) is scrambled by the Arnold transform to obtain \( W_1 \) with the private keys \( k_1 \):

\[
W_1 = \text{Arnold}(W),
\]

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

\[
W_2 = \text{XOR}(W_1, G_1).
\]

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 \( f \) was converted to CIELAB color space, and then the luminance component \( L \) is operated by using SIST to compute the low-frequency \( f_{l1} \). \( f_{l1} \) is divided into nonoverlapping blocks \( B \) 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:

\[
T = \begin{pmatrix}
1, & \text{if } S_i(0, 0) > S_j(0, 0), \\
0, & \text{others}
\end{pmatrix},
\]

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 \( W_2 \) and \( T \) to generate zero-watermark \( W^* \).

\[
W^* = \text{XOR}(W_2, T),
\]

**Step 5.** Zero-watermark preservation.

For security, the obtained zero-watermark \( W^* \) 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 \( f^* \) 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 \( f^* \).

Firstly, the HDR image \( f^* \) was converted to CIELAB color space, and then the luminance component \( L^* \) is operated by using SIST to compute the low-frequency \( f_{11}^* \). \( f_{11}^* \) is divided into nonoverlapping blocks \( B^* \) with the size of \( n \times n \).

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

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

**Step 2.** Feature vector construction.

The maximum singular values \( S'(0, 0) \) of all blocks form a vector and then the feature matrix \( T^* \) is constructed by comparing the relative size of the maximum singular value of each block:

\[
T^* = \begin{pmatrix}
1, & \text{if } S_i(0, 0) > S_j(0, 0), \\
0, & \text{others}
\end{pmatrix},
\]

**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:

\[
T^* = \begin{pmatrix}
1, & \text{if } S_i(0, 0) > S_j(0, 0), \\
0, & \text{others}
\end{pmatrix},
\]

**Step 4.** Zero-watermark construction.

To construct the zero-watermark, an exclusive-or operation is performed between the encrypted watermark \( W_2 \) and \( T^* \) to generate zero-watermark \( W^* \).

\[
W^* = \text{XOR}(W_2, T^*).
\]

**Step 5.** Zero-watermark preservation.

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

### 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:

\[
\text{BER} = \frac{N_e}{N_t},
\]

where \( N_e \) represents the error bits number of a watermark and \( N_t \) represents the total bits number of a watermark.
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).

\[
NC = \frac{\sum_i \sum_j W(i, j)W_1(i, j)}{\sqrt{\sum_i \sum_j W^2(i, j)} \sqrt{\sum_i \sum_j W_1^2(i, j)}},
\]

(13)

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

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, LogarithmicTMO, MertensTMO, WardGlobalTMO, WardHistAdjTMO, LischinskiTMO, ReinhardDevlinTMO, RamanTMO, TumblinRushmeierTMO, DurandTMO, and FattalTMO as shown in Table 2.

Table 3 shows BERs of the proposed algorithm for eight attacked images. From Table 3, it is clearly seen that BERs 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 BERs of the proposed algorithm are lower than 0.1, and only, for TM13 and TM14, BERs 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 NCs 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 BERs and NCs of the proposed algorithm are listed as shown in Table 5 and 6, respectively.
Tables 5 and 6 show BERs and NCs 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 1: Similarities between the zero-watermark generated from eight HDR images.

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

### Table 2: Attacks used in experiments.

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

### Table 3: BERs of eight HDR images under different TM attacks.

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

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

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


