Hindawi
Security and Communication Networks
Volume 2021, Article ID 3803481, 13 pages
https://doi.org/10.1155/2021/3803481

Research Article

Robust Image Hashing Based on Cool and Warm Hue and Space Angle

Yan Zhao and Shuai Liu

College of Electronics & Information Engineering, Shanghai University of Electric Power, Shanghai 200090, China

Correspondence should be addressed to Yan Zhao; yanzhao79@hotmail.com

Received 19 May 2021; Revised 18 June 2021; Accepted 7 July 2021; Published 20 July 2021

Academic Editor: Vincenzo Conti

Image hashing has attracted more and more attention in the field of information security. In this paper, a novel hashing algorithm using cool and warm hue information and three-dimensional space angle is proposed. Firstly, the original image is preprocessed to get the opposite color component and the hue component H in HSV color space. Then, the distribution of cool and warm hue pixels is extracted from hue component H. Blocks the hue component H, according to the proportion of warm hue and cool hue pixels in each small block, combined with the quaternion and opposite color component, constructed the cool and warm hue opposite color quaternion (CWOCQ) feature. Then, three-dimensional space, opposite color, and cool and warm hue are combined to obtain the three-dimensional space angle (TDSA) feature. The CWOCQ feature and the TDSA feature are connected and disturbed to obtain the final hash sequence. Experimental results show that the proposed algorithm has good security and has better image classification performance and shorter computation time compared with some advanced algorithms.

1. Introduction

With the rapid development of science and technology, more and more digital images appear on the Internet. In the transmission process, these digital images may be edited, for example, image zooming and adding watermarks. These edited images have some differences from the original images, but they are similar images. These edited images exist in large quantities on the Internetand are difficult to be recognized by the naked eye in a short time. Therefore, how to recognize a target image and distinguish a similar image from different images quickly is a problem worth addressing. Image hashing is an important and effective method to solve this kind of problem.

Image hashing refers to the one-way mapping of a digital image to a string of binary or decimal numbers, which is called the hash sequence of the digital image. Image hashing should possess robustness, discrimination, and key security.

(1) Robustness: robustness means that the hash sequence obtained after the original image is processed to keep the digital content should be the same or similar to the hash sequence of the original image

(2) Discrimination: discrimination means that the hash sequences of different images under the same hash algorithm should be significantly different; that is, the probability of similarity of hash sequences of different images under the same hash algorithm is extremely small

(3) Key security: key security means that an attacker cannot obtain the correct hash sequence without knowing the correct key

Therefore, image hashing can be applied to image retrieval, image classification, and image copy detection.

2. Related Works

In recent years, different scholars have put forward different hashing algorithms by using a variety of technologies. These algorithms can be roughly divided into transform domain methods and spatial domain methods as follows:

(1) Transform domain methods: Qin et al. [1] proposed a kind of image hashing scheme based on significant structural features. To obtain the final hash sequence, discrete cosine transform (DCT) and other processing ones are done according to the result of edge detection by using some information that contains a rich image block. This algorithm has good robustness against attacks, such as Gaussian filtering and mean filtering, but it only uses partial boundary information, and some local information will be missed, thus affecting the robustness of the algorithm. Tang et al. [2] proposed to construct image hashes using multidimensional scaling analysis (MDS). The algorithm is robust to rotation at any angle of the image, but there is still room for efficiency improvement. In another study [3], an image hashing algorithm based on the color vector angle (CVA) and discrete wavelet transform (DWT) was proposed. This algorithm has good robustness for JPEG compression and small-angle rotation. Tang et al. [4] proposed an image hashing algorithm based on DCT and local linear embedding (LLE). The scheme has good robustness for most image transformations, but it is not robust enough for the rotation transformation of large angles. Tang et al. proposed a robust image hashing based on the CVA [5]. The algorithm has good security, but its limitation is that different color pairs may produce the same CVA, which affects the robustness of the algorithm.

(2) Spatial domain methods: Liu et al. [6] proposed combining the RGB channel with quaternion and then using the local binary pattern (LBP) to obtain image hashing. Their scheme has good robustness against attacks, such as brightness adjustment and Gaussian low-pass filtering, and it has good key security. However, the algorithm is less robust against large angle rotation. Moreover, in another work [7], an image hashing scheme combining CVA and Canny operator was proposed. The algorithm has good robustness against image rotation, brightness, contrast adjustment, and other attacks, but the discrimination is not ideal. Tang et al. [8] proposed an image hashing scheme based on a visual attention model and invariant moments. This method shows good robustness against conventional attacks, such as brightness and contrast, but poor robustness against rotation and cropping attacks. Tang et al. [9] also proposed an image hashing method based on ring segmentation and the invariant vector distance. Since the features extracted within the image segmentation ring are independent of the image rotation, this scheme extracts statistical features from the image segmentation ring to construct the image hashing. This algorithm has good robustness, but there is still room for improvement in discrimination enhancement. Based on the hybrid structure of the color image perception hash algorithm, Qin and others [10] proposed an algorithm in the preprocessing step for image normalization, Gaussian low-pass filtering, and singular value decomposition (SVD); then, after pretreatment, based on a ring and a method based on a block, a Canny operator is used for edge sampling, and the CVA is calculated and combined with the feature of edge information and vector angle to generate the hash sequence. Compared with the previous algorithms based on CVA, this algorithm has better robustness and discrimination, but its robustness to brightness is slightly reduced. Moreover, Zhao et al. [11] proposed an image hashing algorithm based on the Zernike moment and significant region. This scheme has a good effect on image authentication and can also be used for tampering and positioning. Shen and Zhao [12] put forward a method based on the color of opposites and the quadtree decomposition of the image hashing algorithm. The algorithm uses the opposite color component information extraction color features, and color changes in the brightness of the image component are utilized to extract features of the quadtree. The two kinds of features are combined to obtain the hash sequence. This algorithm has good tamper localization capability, but it lacks robustness for large angle rotation. Davarzani et al. [13] proposed a hashing scheme based on the center-symmetrical local binary pattern (CS-LBP) and SVD. Their scheme has good robustness against attacks, such as luminance and JPEG compression, and it can also locate tampers, but the algorithm has poor robustness against rotation. Hosny et al. [14] proposed a hashing scheme based on quaternion polar complex exponential transform, which has good robustness and image authentication ability. Hosny et al. [15] proposed a hashing scheme based on Gaussian–Hermite moments. And this algorithm has robustness not only to some common noises, but also to rotation attacks.

Furthermore, there are other types of image hashing algorithms, such as those based on a structure and gradient hashing algorithm [16], based on a tensor decomposition (TD) hashing algorithm [17], based on binary multiview [18], based on a two-dimensional principal component analysis (PCA) hashing algorithm [19], based on hierarchical ordinal pattern [20], and based on Laplacian Pyramids [21]. These algorithms all have good image discrimination performance, among which the algorithm in [18, 21] has a good ability of tampering detection.

Most of the existing algorithms above were based on the two-dimensional plane of the image for feature extraction, and they all ignore the influence of the cool and warm hue information of the image. Moreover, the features of three-dimensional space of image are also extremely important, and the cool and warm hue [22] information of the image reflects people's intuitive sense of the image color, which should not be ignored. The robustness and discrimination of the algorithm can be improved by adding the features of cool and warm hue and three-dimensional space. Therefore, in this paper, we fully consider the two-dimensional global features of the image and the local features of the three-dimensional space. The image components in the three-dimensional space of each small block build specific three-dimensional space coordinates, and the features of the three-dimensional space angle are extracted, both of which improve the robustness and the discrimination of the algorithm. The main contributions can be summarized as follows:

(1) This algorithm introduces the feature of the cool and warm hue, cool and warm hue reflect people's intuitive perception of the image color, and different hues give people different feelings, which is something that was never used in the previous hashing algorithm.

(2) A three-dimensional space with image components is constructed, and the local features of the three-dimensional space are obtained by extracting angle features. The local features with three-dimensional space are not used in past hashing algorithms. Compared with global features of three-dimensional space, local features of the three-dimensional space can describe image feature in more detail. As a result, the image classification performance of hashing algorithm can be improved.

In this paper, feature extraction is carried out by combining two-dimensional global features and three-dimensional local features to make the extracted features more comprehensive. The experimental result shows that the performance of our algorithm is better with regard to discrimination, and the receiver operating characteristic (ROC) curve is better than that of the algorithm based on the global features of three-dimensional space [16] or the algorithm based on the two-dimensional plane features alone [6, 7, 12, 17, 21]. Compared with the comparison algorithm, the proposed hashing algorithm had higher efficiency, with good security.

3. Proposed Image Hashing

A flow chart of the image hashing based on cool and warm hue information and the space angle is shown in Figure 1, including three parts: image preprocessing, feature extraction, and generation of hash sequence.

3.1. Image Preprocessing. Firstly, the original size of the input image $\mathbf{I}$ is adjusted to the size of $N \times N$ by bilinear interpolation. In this way, images of different sizes can have the same hash length, and the robustness of the algorithm to image scaling is improved. Then, the image is processed with a Gaussian low-pass filter to reduce the influence of subtle operations, such as noise and compression, on the image. The preprocessed image is then obtained as $\mathbf{I}_0$.

3.2. Cool and Warm Hue Information Extraction. Cool and warm hue information in images refers to dividing hues into cool and warm according to people's cool and warm feelings in color psychology [22]. In the image, those with cool hues (green, blue, purple, etc.) give people a feeling of coolness, while those with warm hues (red, orange, yellow, etc.) give people a feeling of warmth. The image in Figure 2 contains many cool hues, which give people a feeling of being cool. The image in Figure 2 contains more warm hues, which give people a feeling of being warm.

In this method, red, green, and blue (RGB) images are converted into the hue, saturation, value (HSV) color space, and the hue component H is extracted [23, 24]. As shown in Figure 2, in this paper, it is stipulated that, in the counterclockwise direction, the pixels in the hue component H between 1/3 (green) and 5/6 (magenta) are cool hue pixels, and the pixels in the hue component H between 5/6 (magenta) and 1/3 (green) are warm hue pixels. These values refer to the values of the normalized hue component H in MATLAB.

As Figure 3 shows, hue component H is divided into $M \times M$ small blocks, the proportion of cool hue pixels in each small block is $\mathbf{b}_{m,n}$, the proportion of warm hue pixels in each small block is $\boldsymbol{c}_{m,n}$, and the cool and warm hue quaternion $\mathbf{CWQ}_{m,n} = i\ \mathbf{a}_{m,n} + j\ \mathbf{b}_{m,n} + k\ \mathbf{c}_{m,n}$ is constructed. Here, $\mathbf{a}_{m,n} = \mathbf{b}_{m,n} - \mathbf{c}_{m,n}$, and m and n are, respectively, the number of rows and columns of each small block in the $M \times M$ small blocks of the hue component H.

3.3. Extraction of the Cool and Warm Hue Opposite Color Quaternion Features. In this section, opposite color red-green (RG) and blue-yellow (BY) are introduced for calculation [25,26]. The RG and BY are the opposite color red-green and blue-yellow found in the human retina; the RG and BY can be calculated by equations (1) and (2), respectively.

$$\mathrm{RG} = T_{\mathrm{R}}(x, y) - T_{\mathrm{G}}(x, y), \tag{1}$$

$$\mathrm{BY} = T_{\mathrm{B}}(x, y) - T_{\mathrm{Y}}(x, y). \tag{2}$$

Here, $T_{\mathrm{R}}(x, y)$,$T_{\mathrm{G}}(x, y)$, $T_{\mathrm{B}}(x, y)$and $T_{\mathrm{Y}}(x, y)$ are functions defined in equations (3) to (6), respectively.

$$T_{\mathrm{R}}(x, y) = f_r(x, y) - \frac{f_g(x, y) + f_b(x, y)}{2}, \tag{3}$$

$$T_{\mathrm{G}}(x, y) = f_g(x, y) - \frac{f_r(x, y) + f_b(x, y)}{2}, \tag{4}$$

$$T_{\mathrm{B}}(x, y) = f_b(x, y) - \frac{f_r(x, y) + f_g(x, y)}{2}, \tag{5}$$

$$T_{\mathrm{Y}}(x, y) = -T_{\mathrm{B}}(x, y) - \frac{\left|f_r(x, y) - f_g(x, y)\right|}{2}. \tag{6}$$

Here, $f_r(x,y)$, $f_g(x,y)$, and $f_b(x,y)$ are the red, green, and blue channels of the RGB color space, respectively.

As Figure 4 shows, the RG component and BY component of the obtained opposite colors are divided into $M \times M$ small blocks, respectively, and the average

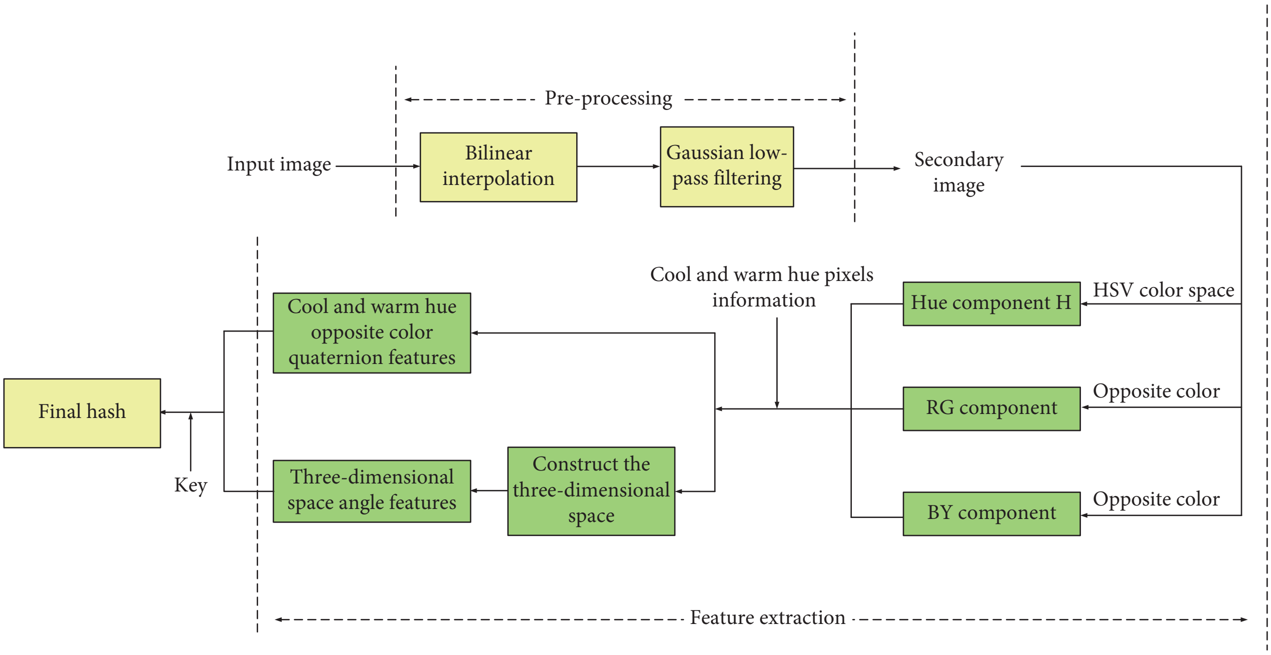
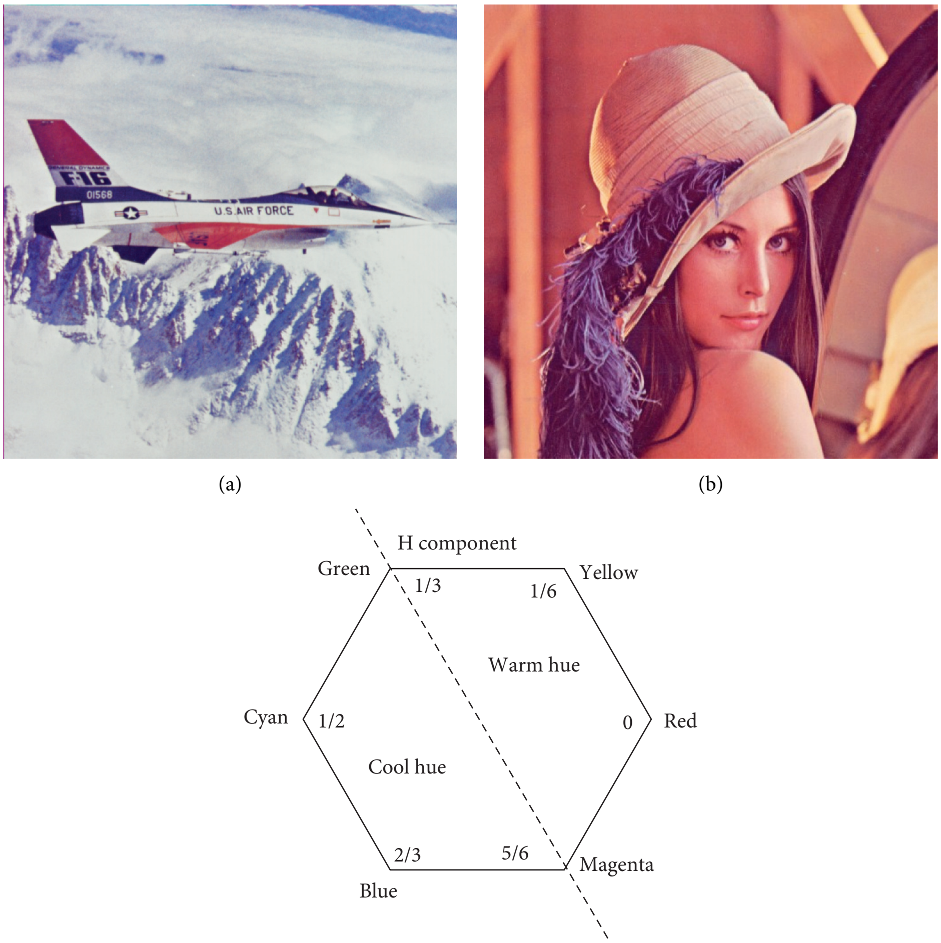

Pre-processing
Input image
Bilinear interpolation
Gaussian low-pass filtering
Secondary image
Cool and warm hue pixels information
Cool and warm hue opposite color quaternion features
Hue component H
HSV color space
Final hash
RG component
Opposite color
Key
Three-dimensional space angle features
Construct the three-dimensional space
BY component
Opposite color
Feature extraction

FIGURE 1: A flowchart of the image hashing.



(c)

FIGURE 2: Cool and warm hue image and hue division.

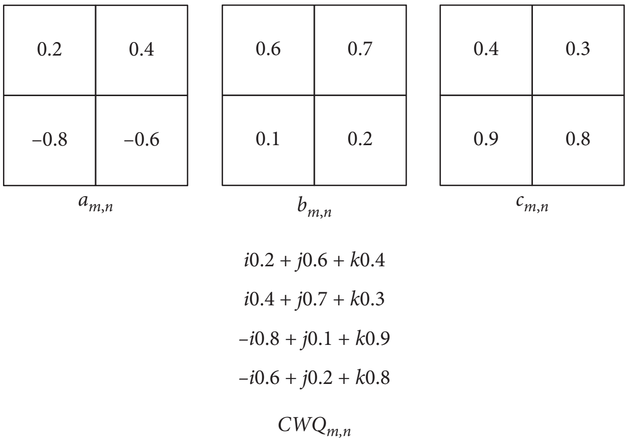


Figure 3: The formation of the cool and warm hue quaternion $\mathbf{CWQ}_{m,n}$.

value of the rounded pixels of each small block is $\mathbf{d}_{m,n}$ and $\mathbf{e}_{m,n}$. During hue information extracting process, hue H is also divided into $M \times M$ small blocks, and the average of the pixels of each small block is $\mathbf{h}_{m,n}$. Thus, you get the opposite color quaternion $\mathbf{OCQ}_{m,n} = i\ \mathbf{h}_{m,n} + j\ \mathbf{d}_{m,n} + k\ \mathbf{e}_{m,n}$, where m and n are, respectively, the hue component H and the number of rows and columns in each of the $M \times M$ blocks of the opposite color component RG and BY.

The cool and warm hue quaternion $\mathbf{CWQ}_{m,n} = i\ \mathbf{a}_{m,n} + j\ \mathbf{b}_{m,n} + k\ \mathbf{c}_{m,n}$ from Section 3.2 and the opposite color quaternion $\mathbf{OCQ}_{m,n} = i\ \mathbf{h}_{m,n} + j\ \mathbf{d}_{m,n} + k\ \boldsymbol{e}_{m,n}$ in this section are used to construct the cool and warm hue opposite color quaternion $\mathbf{CWOCQ}_{m,n}$ as follows:

$$\begin{aligned}\mathbf{CWOCQ}_{m,n} &= \mathbf{CWQ}_{m,n}\mathbf{OCQ}_{m,n} = \left(i\mathbf{a}_{m,n} + j\mathbf{b}_{m,n} + k\mathbf{c}_{m,n}\right)\left(i\mathbf{h}_{m,n} + j\mathbf{d}_{m,n} + k\mathbf{e}_{m,n}\right)\\ &= -\left(\mathbf{a}_{m,n}\mathbf{h}_{m,n} + \mathbf{b}_{m,n}\mathbf{d}_{m,n} + \mathbf{c}_{m,n}\mathbf{e}_{m,n}\right) + i\left(\mathbf{b}_{m,n}\mathbf{e}_{m,n} - \mathbf{c}_{m,n}\mathbf{d}_{m,n}\right) + j\left(\mathbf{c}_{m,n}\mathbf{h}_{m,n} - \mathbf{a}_{m,n}\mathbf{e}_{m,n}\right) + k\left(\mathbf{a}_{m,n}\mathbf{d}_{m,n} - \mathbf{b}_{m,n}\mathbf{h}_{m,n}\right).\end{aligned} \tag{7}$$

Finally, the magnitude of $\mathbf{CWOCQ}_{m,n}$ is $\mathbf{Q}_{m,n}$.

$$\mathbf{A}_{m,n} = -\left(\mathbf{a}_{m,n}\mathbf{h}_{m,n} + \mathbf{b}_{m,n}\mathbf{d}_{m,n} + \mathbf{c}_{m,n}\mathbf{e}_{m,n}\right), \tag{8}$$

$$\mathbf{B}_{m,n} = \mathbf{b}_{m,n}\mathbf{e}_{m,n} - \mathbf{c}_{m,n}\mathbf{d}_{m,n}, \tag{9}$$

$$\mathbf{C}_{m,n} = \mathbf{c}_{m,n}\mathbf{h}_{m,n} - \mathbf{a}_{m,n}\mathbf{e}_{m,n}, \tag{10}$$

$$\mathbf{D}_{m,n} = \mathbf{a}_{m,n}\mathbf{d}_{m,n} - \mathbf{b}_{m,n}\mathbf{h}_{m,n}, \tag{11}$$

$$\mathbf{Q}_{m,n} = \sqrt{\left(\mathbf{A}_{m,n}\right)^2 + \left(\mathbf{B}_{m,n}\right)^2 + \left(\mathbf{C}_{m,n}\right)^2 + \left(\mathbf{D}_{m,n}\right)^2}. \tag{12}$$

The matrix $\mathbf{Q}$ composed of the magnitude is obtained as follows:

$$\begin{bmatrix} \mathbf{Q}_{1,1} & \cdots & \mathbf{Q}_{1,M} \\ \vdots & \ddots & \vdots \\ \mathbf{Q}_{M,1} & \cdots & \mathbf{Q}_{M,M} \end{bmatrix}. \tag{13}$$

In matrix $\mathbf{Q}$, each column is connected end to end and transposed to obtain the cool and warm hue opposite color quaternion (CWOCQ) feature sequence $\mathbf{Q}_1(s_1)$, with one row and $M \times M$ columns, where $1 \le s_1 \le M \times M$.

3.4. Extracting the Three-Dimensional Space Angle Features.

Let (x, y) represent the pixel location, and let z represent the value of the pixel at location (x, y). Then, the image can be represented in a three-dimensional space considering the location variables (x, y) and the value variable z. The RG images in the three-dimensional space are presented in Figure 5(a).

In this paper, the RG image and BY image are divided into $M \times M$ blocks and nonoverlapping. To build the three-dimensional coordinates, the rows are divided into small blocks in the RG image, and the BY image is taken as the x-axis coordinate, and the number of columns is divided into small blocks in the RG image, and the BY image is taken as the y-axis coordinate. The z-axis coordinates are $\mathbf{L}_1(m, n)$ and $\mathbf{L}_2(m, n)$, where $\mathbf{L}_1(m, n)$ and $\mathbf{L}_2(m, n)$ are the rounding averages of the pixels in each small block off the RG image and BY image, respectively, and the three-dimensional coordinate is established accordingly. Then, the coordinates of $\mathrm{RG}(m, n)$ and $\mathrm{BY}(m, n)$ in the mth row and the nth column of the RG image and BY image in the three-dimensional space are $(m, n, \mathbf{L}_1(m, n))$ and $(m, n, \mathbf{L}_2(m, n))$. The coordinates of the small blocks of the RG image in three-dimensional space are shown in Figure 5(b), and the same is true for the BY image.

Because cool and warm hues give people different feelings in the image, the concept of cool and warm hue dominant blocks is added in the construction of three-dimensional space in this method. As Figure 6 shows, in the small blocks of each hue component H, if the proportion of cool hue pixels $\mathbf{b}_{m,n} \ge 0.5$, then the small block is called a cool hue dominant block; otherwise, it is a warm hue dominant block. Besides, $\mathrm{RG}(m, n)$ and $\mathrm{BY}(m, n)$ in the RG image and BY image with the same coordinates are also accordingly called a cool hue dominant block or a warm hue dominant block. In the three-dimensional space coordinates formed by the small blocks of the RG image and BY image, the z-axis

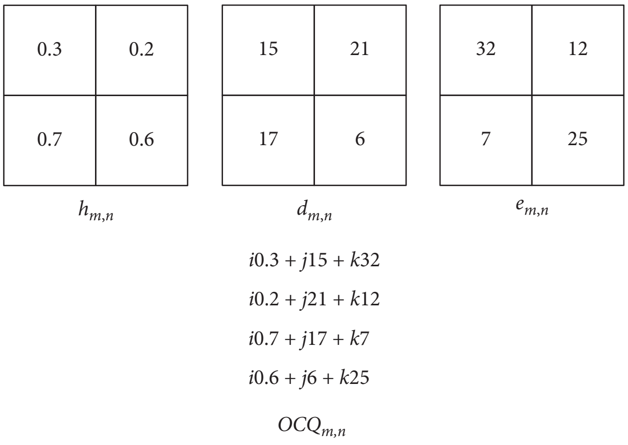
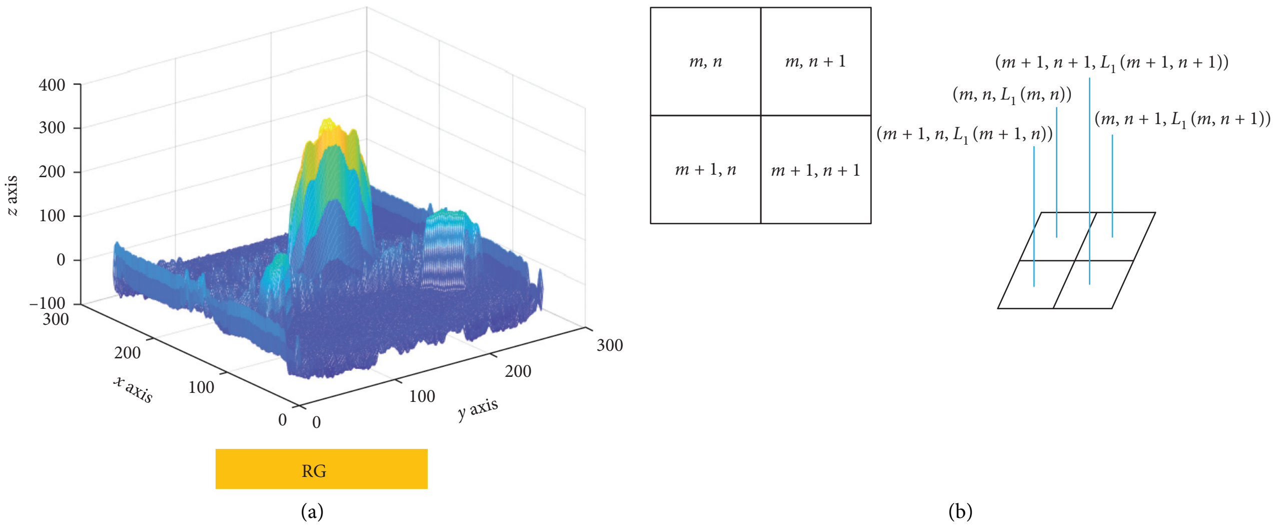


FIGURE 4: The formation of opposite color quaternion $\mathbf{OCQ}_{m,n}$.



(a)

(b)

FIGURE 5: (a) The RG images in the three-dimensional space. (b) The coordinates of RG's blocks of the image in the three-dimensional space.

coordinate of the dominant block of cool hue is specified as the opposite number of the mean value of the coordinates of the block. In other words, if a small block with a coordinate (m, n) of hue H is a dominant block with cool hues, then the coordinates of the RG image and BY image of the small block RG(m, n) and BY(m, n) in the $M \times M$ small block in the three-dimensional space are $(m, n, -\mathbf{L}_1(m, n))$ and $(m, n, -\mathbf{L}_2(m, n))$, respectively. If it is a warm hue dominant block, then the coordinates in the three-dimensional space will not change.

As shown in Figure 7, RG's three-dimensional space angle features of the image are extracted from the small blocks with a position in (m, n) and its four adjacent positions. First, the coordinates of (m, n), $(m, n-1)$, and $(m, n+1)$ for the block $\mathbf{O}_{m,n} = (m, n, \mathbf{L}_1(m, n))$, $\mathbf{E}_{m,n} = (m, n-1, \mathbf{L}_1(m, n-1))$ and $\mathbf{F}_{m,n} = (m, n+1, \mathbf{L}_1(m, n+1))$ are found, and it is judged whether the corresponding small block is a cool hue dominant block. If the block is a cool hue dominant block, then the z-axis coordinate takes the negative number; if the block is a warm hue dominant block, then it remains unchanged. Moreover, the two vectors that are formed by these three coordinates $\mathbf{EO}_{m,n} = \mathbf{E}_{m,n} - \mathbf{O}_{m,n}$, $\mathbf{FO}_{m,n} = \mathbf{F}_{m,n} - \mathbf{O}_{m,n}$ can then be discovered. Next, vector $\mathbf{EO}_{m,n}$ and vector $\mathbf{FO}_{m,n}$ form an included angle $\boldsymbol{\alpha}_{m,n}$, and, in three dimensions, the included angle cosine $\mathbf{cos}\boldsymbol{\alpha}_{m,n}$ is as follows:

$$\mathbf{cos\alpha}_{m,n} = \frac{\mathbf{EO}_{m,n}\mathbf{FO}_{m,n}}{|\mathbf{EO}_{m,n}||\mathbf{FO}_{m,n}|}. \tag{14}$$

The matrix $\mathbf{K}$ is composed of $\mathbf{cos}\boldsymbol{\alpha}_{m,n}$, where $2 \leq m \leq M$-1 and $2 \leq n \leq M$-1, so the matrix $\mathbf{K}$ has M-2 rows and M-2 columns.

Similarly, in Figure 7(b), the coordinates of (m, n), $(m-1, n)$, and $(m+1, n)$ for the block $\mathbf{O}_{m,n} = (m, n, \mathbf{L}_1(m, n))$, $\mathbf{G}_{m,n} = (m-1, n, \mathbf{L}_1(m-1, n))$ and $\mathbf{P}_{m,n} = (m+1, n, \mathbf{L}_1(m+1, n))$ are found, and it is judged whether the corresponding small block is a cool hue dominant block. If it is a cool hue dominant block, then the z-axis coordinate takes the negative number; if it is a warm hue dominant block, then it remains unchanged. Then, the two vectors that are formed by these three coordinates $\mathbf{GO}_{m,n} = \mathbf{G}_{m,n} - \mathbf{O}_{m,n}$,

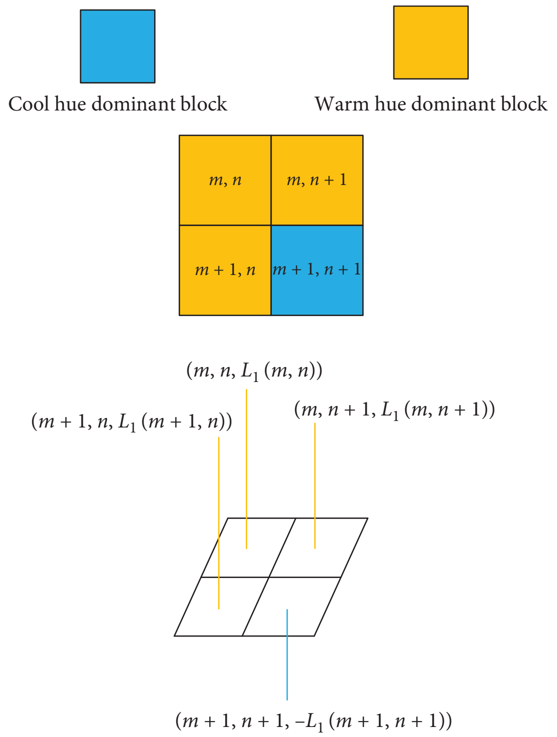


Figure 6: The coordinates of the cool color dominant blocks and the warm color dominant blocks of the image in the three-dimensional space.

$\mathbf{PO}_{m,n} = \mathbf{P}_{m,n} - \mathbf{O}_{m,n}$ can be found. Next, vector $\mathbf{GO}_{m,n}$ and vector $\mathbf{PO}_{m,n}$ form an included angle $\boldsymbol{\beta}_{m,n}$, and, in three dimensions, the included angle cosine $\mathbf{cos}\boldsymbol{\beta}_{m,n}$ is as follows:

$$\cos \beta_{m,n} = \frac{\mathbf{GO}_{m,n}\mathbf{PO}_{m,n}}{|\mathbf{GO}_{m,n}||\mathbf{PO}_{m,n}|}. \tag{15}$$

The matrix $\mathbf{U}$ is composed of $\mathbf{cos}\boldsymbol{\beta}_{m,n}$, where $2 \leq m \leq M\text{-}1$ and $2 \leq n \leq M\text{-}1$, so the matrix $\mathbf{U}$ has $M\text{-}2$ rows and $M\text{-}2$ columns.

Finally, the two matrices of $\mathbf{K}$ and $\mathbf{U}$ are added to obtain matrix $\mathbf{J}$. Matrix $\mathbf{J}$ is a matrix with $M\text{-}2$ rows and $M\text{-}2$ columns, each row is connected, the vector $\mathbf{J}(s_2)$ that produces the one row $(M\text{-}2) \times (M\text{-}2)$ columns is obtained, the BY image is extracted in the same way to obtain the three-dimensional space angle eigenvector $\mathbf{J}_1(s_2)$, and $\mathbf{J}(s_2)$ add $\mathbf{J}_1(s_2)$ obtains the three-dimensional space angle (TDSA) feature sequence $\mathbf{J}_2(s_2)$, where $1 \leq s_2 \leq (M\text{-}2)^2$.

3.5. Hash Generation. The feature sequence $\mathbf{Q}_1$ of CWOCQ and the TDSA feature sequence $\mathbf{J}_2$ combine to form the sequence $\mathbf{Z} = [\mathbf{Q}_1\ \mathbf{J}_2]$.

$$\mathbf{H}_1(s) = \begin{cases} 1, & \mathbf{Z}(s) \geq \mathbf{Z}(s+1), \\ 0, & \text{else}, \end{cases} \tag{16}$$

where $1 \leq s \leq M^2 + (M-2)^2 - 1 = 2M^2 - 4M + 3$.

The hash of the hashing algorithm in this study had a length of $\mathbf{L}_\mathrm{H} = 2M^2 - 4M + 3$ bits. The key was used to scramble the intermediate hash sequence $\mathbf{H}_1$ to obtain the final hash $\mathbf{H}$.

4. Experimental Results and Analysis

For the experiment, the parameters of the algorithm were set as follows: 3×3 Gaussian low-pass filtering with normalized size $N = 256$ and a standard deviation 1. The number of image subblocks was $M \times M = 16 \times 16 = 256$, and thus the hash length $\boldsymbol{L}_\mathrm{H} = M^2 + (M\text{-}2)^2 - 1 = 2M^2 - 4M + 3$ was 451 bits. All the experiments were implemented with MATLAB 2018b on a computer with an Inter Core i5-8300H CPU, 8 GB of memory, and Windows 10 operating system.

4.1. Robustness Experiment. To evaluate the robustness of the algorithm, 20 images were used as test samples, and Figure 8 shows one of the sample images. Similar images were generated for each test image according to the attack types that are given in Table 1. The algorithm was used to extract the hash sequence of the original image and the similar image, and the Hamming distance between them was calculated. Hamming distance graphs are drawn according to different attack categories. The robustness experimental results of five images are shown in Figure 9. As shown, the curve fluctuation range of attacks, such as JPEG compression, brightness adjustment, contrast adjustment, pepper and salt noise, image zoom, and Gaussian filtering, was small, and the Hamming distances were all less than 84. In the robustness experiment results of the rotation attack, the Hamming distance of the rotation attack within 1° is small, and the Hamming distance increased gradually with the increase of the angle. This is because the algorithm blocks the image, and thus, it is more sensitive to a rotation attack. Table 2 shows the Hamming distance statistical results of 20 images under different attacks. The JPEG compression, brightness adjustment, contrast, salt and pepper noise, image scaling, and Gaussian filtering are shown. The maximum Hamming distance was less than 84. The mean and standard deviation (SD) were less than 32, and the rotation attack had both a maximum and an average of more than 121. The maximum Hamming distance, except for the rotation attack, was less than 84. Except for large angle rotation, all distance is less than the threshold value 160 selected in Section 4.2 (shown by the red line in Figure 9). This indicates that, except for large angle rotation attacks, the algorithm in this paper has good robustness against attacks, such as JPEG compression, brightness adjustment, and contrast adjustment.

4.2. Discrimination Experiment. One thousand images were downloaded from the network to form the image test library, in which 700 images were taken from the Ground Truth database [27], and 300 images were taken from the VOC2007 database [28]. The hash sequence of 1000 images were extracted by using the algorithm in this paper, and the Hamming distance between the 1000 images was calculated to generate a total of $\mathbf{C}_{1000}^2 = 499500$ different image pairs. The attacks are given in Table 3, so each image generated

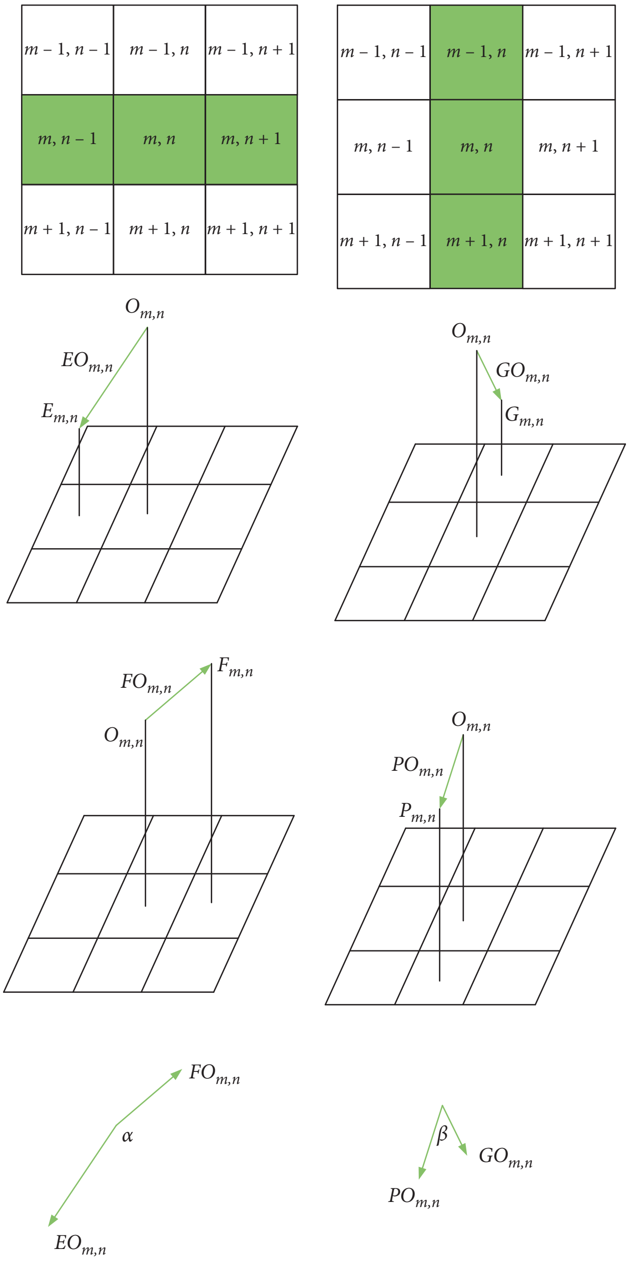


Figure 7: Extracted three-dimensional space angle features.

$2 \times 10 = 20$ similar image pairs, and the Hamming distance between the similar image and the original image was calculated. There were a total of $(21 \times 20) \div 2 \times 1000 = 210000$ image similarity pairs. The similar and different images of the Hamming distance of the distribution are shown in Figure 10. The abscissa diagram shows the different Hamming distances, and the ordinate diagram shows the the different frequencies of the Hamming distance, 127, which was found by calculating the minimum. The minimum Hamming distance between different images was 127.

The maximum Hamming distance between similar images was 168, and similar and different images of the Hamming distance intersection appeared between 127 and 168. To obtain the optimal threshold value to distinguish similar image pairs from different image pairs, the collision rate and error detection rate were introduced to analyze the differences between the algorithms in this study. The calculation formulas are

$$P_C = \frac{N_C}{N_D}, \tag{17}$$

$$P_E = \frac{N_E}{N_S}, \tag{18}$$

where N_C and N_D represent the number of different image pairs detected as similar image pairs and the total number of

Figure 8: Color image in robustness experiment.

Table 1: Attack setting in robustness experiment.

Operation	Parameter	Parameter values
JPEG compression	Quality	30, 40, ..., 100
Brightness adjustment	Level	−20, −10, 10, 20
Contrast adjustment	Level	−20, −10, 10, 20
Salt & pepper	Noise level	0.002, 0.004, ..., 0.01
Image resizing	Ratio	0.6, 0.8, 1.2, 1.4, 1.6, 1.8
3 × 3 Gaussian filter	Standard deviation	0.1, 0.2, ..., 1
Rotation	Angle	1, 2, 3, ..., 7, 8
Watermark embedding	Transparency	3, 4, ..., 7, 8
Gamma correction	Gamma	0.75, 0.9, 1.1, 1.25
speckle	Noise variance	0.002, 0.004, ..., 0.01

different image pairs, respectively; similarly, N_E and N_S represent the number of similar image pairs detected as different image pairs and the total number of similar image pairs, respectively; and P_C and P_E represent the collision rate and error detection rate, respectively.

The calculation results are shown in Table 4. According to the data, when the threshold value was selected to be 160, the algorithm had a low collision rate and error detection rate at the same time, with good discrimination.

4.3. Key Detection Experiment. Hashing algorithm security means that different hash sequences are generated by different keys. The key security of the proposed hashing algorithm is illustrated in Figure 11. The x-axis is the index of 1,000 error keys, and the y-axis is the Hamming distance. As shown, the minimum Hamming distance value was 190, and the average value was 225.6040 for all error keys, which was significantly greater than the threshold value of 160 that was selected in Section 4.2 (shown by the red line in Figure 11). This means that it would be difficult for an attacker to generate the correct hash sequence without the correct key, and thus, the hashing algorithm in this paper meets the security requirements.

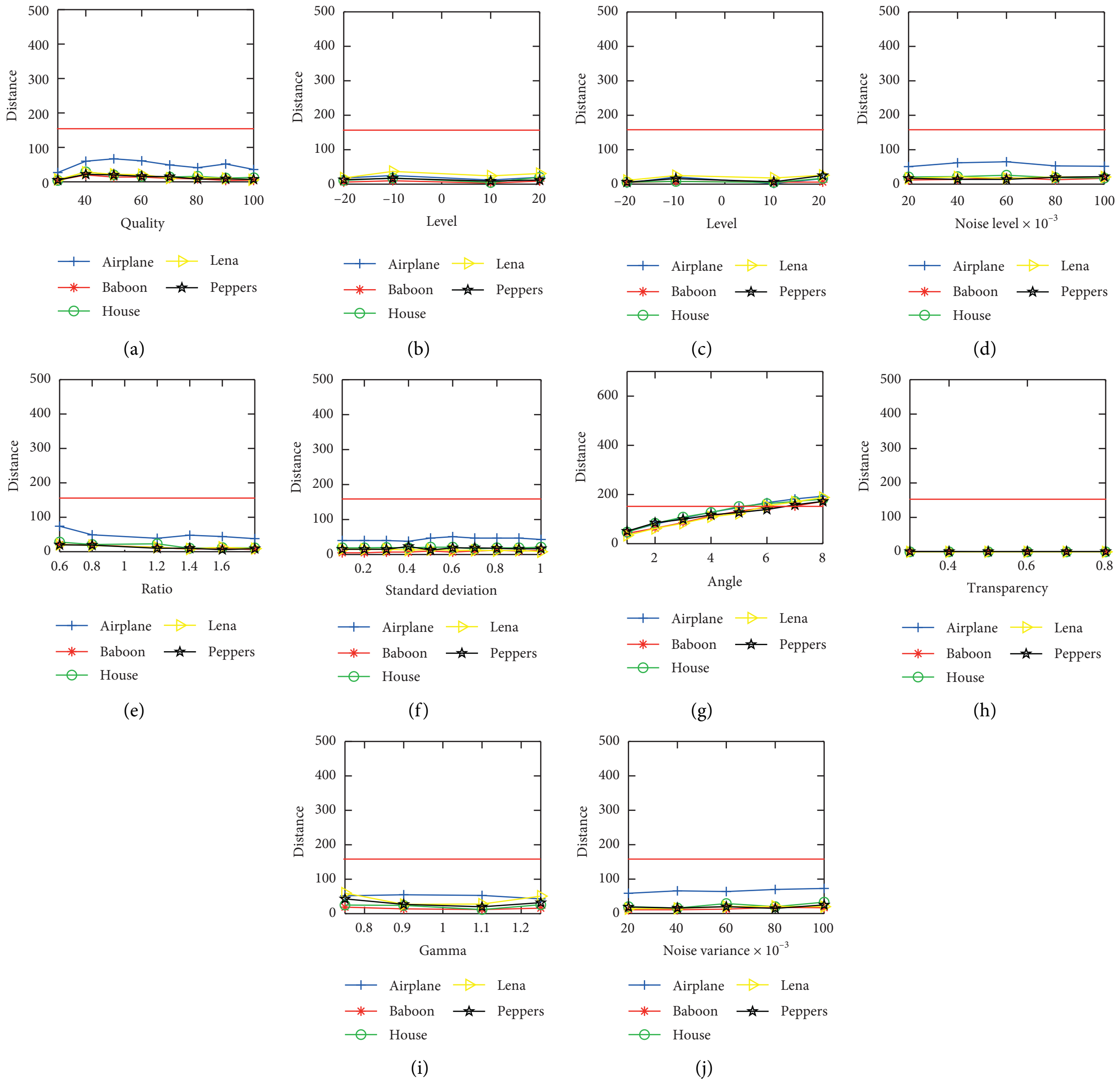
4.4. Performance Comparison of Different Blocks and Different Components. To analyze the influence of the number of blocks on the performance of the algorithm, the ROC curve was introduced to compare the performance, which mainly included robustness and discrimination. A series of different thresholds were set to obtain a series of false positive rate (P_{FPR}) and the true positive rate (P_{TPR}) to draw the ROC curve. The experimental results are shown in Figure 12. As shown, the abscissa is the P_{FPR}, the ordinate is the P_{TPR}, and the calculation formula can be expressed as

$$P_{\text{FPR}} = \frac{n_1}{N_1}, \tag{19}$$

$$P_{\text{TPR}} = \frac{n_2}{N_2}, \tag{20}$$

where n_1 represents the number of different image pairs misjudged as similar image pairs; n_2 represents the number of similar image pairs correctly judged; and N_1 and N_2 denote the total number of different image pairs and similar image pairs, respectively. The horizontal axis represents the distinctiveness performance, while the vertical axis represents the robust performance. The closer the ROC curve to the upper left corner, the better the performance of the proposed algorithm.

In the experiment, 1,000 images were used for the discrimination test. Visually similar images could be generated according to the attack settings in Section 4.2. Each image could generate 20 similar images. Therefore, the total number of similar image pairs was 210,000, and the number of different image pairs was 499,500. When the image was divided into 8 × 8, 16 × 16 and 32 × 32 blocks, the lengths of hash code were 99 bits, 451 bits, and 1,923 bits, respectively. When the image was divided into 32 × 32 blocks, the hash code length was too long. Therefore, in the experiment, only



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Figure 9: Robustness experiment. (a) JPEG compression. (b) Brightness adjustment. (c) Contrast adjustment. (d) Salt & Pepper. (e) Image resizing. (f) 3 × 3 Gaussian low-pass filter. (g) Rotation. (h) Watermark embedding. (i) Gamma correction. (j) Speckle.

the performance of the hashing algorithm whose image was divided into 8 × 8 blocks, 16 × 16 blocks, and 16 × 16 blocks, but the hue component H is replaced by the value component V, was selected for comparison. As shown in Figure 12, the ROC curve of the hashing algorithm divided into 16 × 16 blocks was closer to the upper left corner than that of the hash algorithm with other curves, and thus, the performance was better. In this study, the hashing algorithm divided the image into 16 × 16 blocks, combined with cool and warm hue and hue component H, which was a better choice for a balance between robustness and discrimination.

4.5. Performance Comparison with the Different Algorithms. As shown in Table 5, the algorithm in this paper was compared with the Quaternion LBP algorithm [6], the CVA-Canny algorithm [7], the Quadtree algorithm [12], the Color Structure algorithm [16], the TD algorithm [17], and the LP algorithm [21]. The parameters for the comparison were the same as those set in their respective published papers, and the hash lengths of the compared algorithms were 256 bits, 40 decimal numbers, 452 decimal numbers, 354 bits, 96 bits, and 1024 decimal numbers, respectively. The hash code length of the proposed hashing algorithm was 451 bits.

In this experiment, as in Section 4.4, the hashing algorithm was used to extract the hash sequences of similar image pairs and different image pairs, and the Hamming distance between these image pairs was calculated. The attack settings for similar images were also the same as those in visually similar images that could be generated according to the attack settings in Section 4.2. Among them, there were

Table 2: Hamming distance in different attacks.

Operation	Min	Max	Mean	SD
JPEG compression	4	67	20.4250	16.7912
Brightness adjustment	3	37	15.9000	8.7232
Contrast adjustment	2	26	11.8500	7.9092
Salt & pepper	12	83	28.8800	22.1384
Image resizing	6	74	20.9667	16.0763
3 × 3 Gaussian filter	5	51	20.3200	12.8372
Rotation	34	193	121.5250	45.8649
Watermark embedding	0	1	0.3000	0.4661
Gamma correction	12	60	31.9500	15.6692
Speckle	11	73	28.2000	20.2279

Table 3: Attack setting in discrimination experiment.

Operation	Parameter	Parameter values
JPEG compression	Quality factor	40, 80
Brightness adjustment	Level	−20, 20
Contrast adjustment	Level	−20, 20
Salt & pepper	Noise level	0.002, 0.006
Image resizing	Ratio	0.8, 1.6
3 × 3 Gaussian filter	Standard deviation	0.2, 0.6
Rotation	Angle	1, 2
Watermark embedding	Transparency	0.3, 0.8
Gamma correction	Gamma	0.75, 1.25
speckle	Noise variance	0.002, 0.006

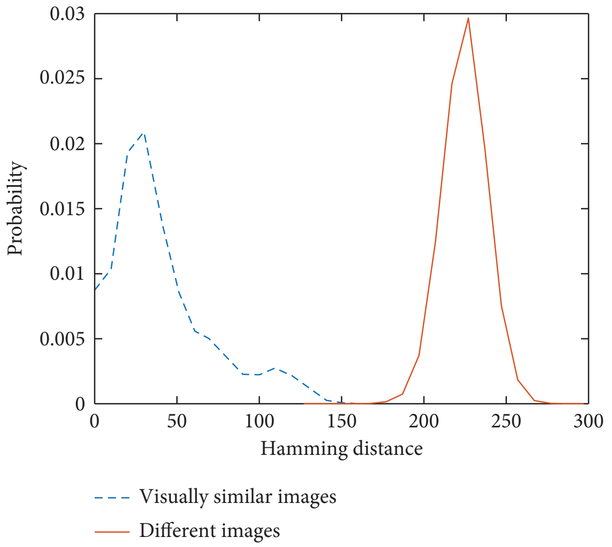


Figure 10: The Hamming distance distribution of similar image pairs and different image pairs.

Table 4: Threshold selection.

Threshold	Collision rate	Error detection rate
127	0	1.38×10^{-2}
140	4.00×10^{-6}	2.06×10^{-3}
150	1.00×10^{-5}	2.62×10^{-4}
160	4.60×10^{-5}	1.43×10^{-5}
168	1.76×10^{-4}	0

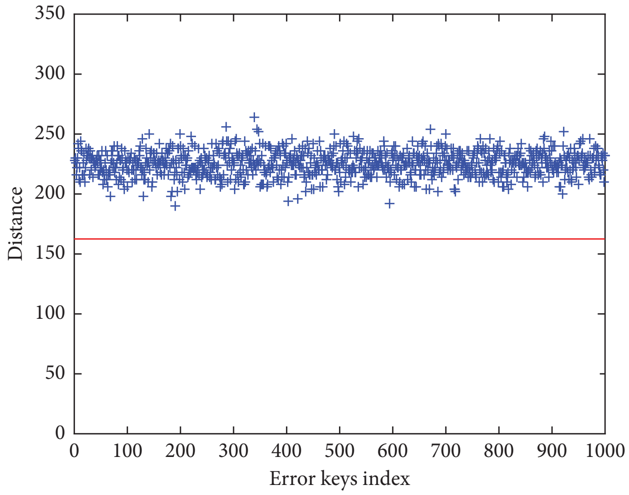


Figure 11: The Hamming distance between hashes with the correct secret key and wrong secret key.

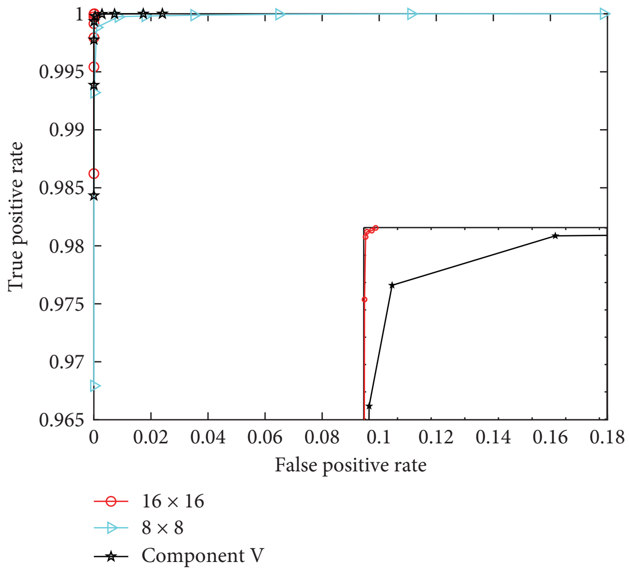


Figure 12: The ROC curves of different blocks and different components.

Table 5: Performance comparison of the different algorithms.

Algorithm	Average time (s)	Hash length
Proposed algorithm	0.021	451 bits
QLBP [6]	0.036	256 bits
CVA-canny [7]	0.288	40 decimal numbers
Quadtree [12]	0.042	452 decimal numbers
Color structure [16]	0.019	354 bits
TD [17]	0.101	96 bits
LP [21]	0.028	1024 decimal numbers

210,000 similar image pairs and 499,500 different image pairs. A series of different thresholds were set to obtain a series of false positive rate (P_{FPR}) and the true positive rate (P_{TPR}) to draw the ROC curve. The experimental results are shown in Figure 13. As shown, the proposed algorithm is

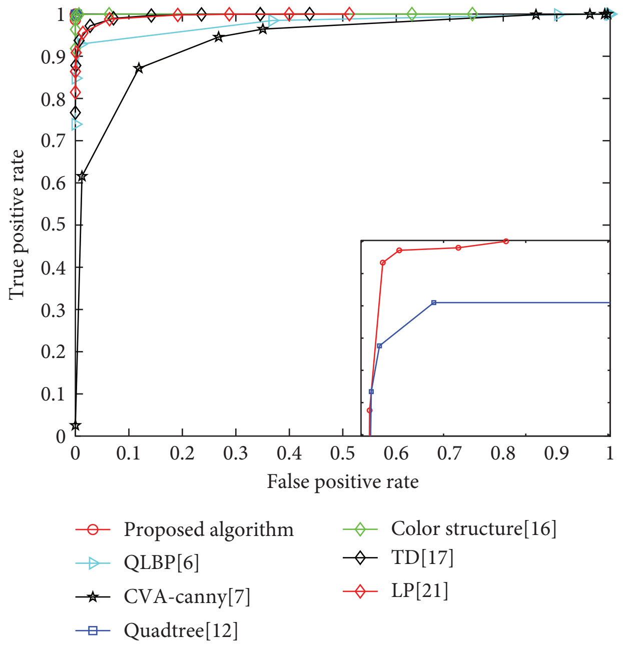


Figure 13: The ROC curves of different algorithms.

closer to the upper left corner than other algorithms, indicating that the classification effect of the proposed algorithm was better.

As for the hash length, the proposed algorithm extracted the hue component H and the opposite color component RG and BY block for feature extraction, and thus, the hash code length was relatively long. However, as shown in Table 5, the average calculation time of this algorithm was 0.021 s, which was only longer than the Color Structure algorithm and superior to the other algorithms.

5. Conclusions

This work proposes an image hashing algorithm based on cool and warm hue information and the space angle. This algorithm extracts the features of cool and warm hue opposite color quaternion and the three-dimensional space angle. Finally, the algorithm combines them and scrambles to obtain the final hash sequence. Experimental results show that the proposed algorithm is robust to brightness adjustment, contrast attacks, and other attacks. ROC curves show that this algorithm has better discrimination performance, better key security, and shorter calculation time compared with the comparison algorithms. The algorithm in this paper does not have tampering detection performance, but it will be further studied in the future, so that warm and cold hue can be applied to tampering detection and location.

Data Availability

The image datasets used to support the findings of this study can be downloaded from the public websites whose links are provided in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61802250 and Local College Capacity Building Project of Shanghai Municipal Science and Technology Commission (20020500700).

References

[1] C. Qin, X. Chen, J. Dong, and X. Zhang, “Perceptual image Hashing with selective sampling for salient structure features,” *Displays*, vol. 45, pp. 26–37, 2016.

[2] Z. Tang, Z. Huang, X. Zhang, and H. Lao, “Robust image hashing with multidimensional scaling,” *Signal Processing*, vol. 137, pp. 240–250, 2017.

[3] Z. Tang, Y. Dai, X. Zhang, L. Huang, and F. Yang, “Robust image hashing via colour vector angles and discrete wavelet transform,” *IET Image Processing*, vol. 8, no. 3, pp. 142–149, 2014.

[4] Z. Tang, H. Lao, X. Zhang, and K. Liu, “Robust image hashing via DCT and LLE,” *Computers & Security*, vol. 62, pp. 133–148, 2016.

[5] Z. Tang, X. Li, X. Zhang, S. Zhang, and Y. Dai, “Image hashing with color vector angle,” *Neurocomputing*, vol. 308, pp. 147–158, 2018.

[6] E. Liu, H. Yao, Y. Hu, and F. Cao, “Perceptual color image hashing based on quaternionic local ranking binary pattern,” *IETE Technical Review*, vol. 38, no. 1, pp. 158–171, 2021.

[7] Z. Tang, L. Huang, X. Zhang, and H. Lao, “Robust image hashing based on color vector angle and Canny operator,” *AEU - International Journal of Electronics and Communications*, vol. 70, no. 6, pp. 833–841, 2016.

[8] Z. Tang, H. Zhang, C. M. Pun, M. Yu, C. Yu, and X. Zhang, “Robust image hashing with visual attention model and invariant moments,” *IET Image Processing*, vol. 14, no. 5, pp. 901–908, 2020.

[9] Z. Tang, X. Zhang, X. Li, and S. Zhang, “Robust image hashing with ring partition and invariant vector distance,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 200–214, 2016.

[10] C. Qin, M. Sun, and C.-C. Chang, “Perceptual hashing for color images based on hybrid extraction of structural features,” *Signal Processing*, vol. 142, pp. 194–205, 2018.

[11] Y. Zhao, S. Wang, X. Zhang, and H. Yao, “Robust Hashing for image authentication using zernike moments and local features,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 55–63, 2013.

[12] Q. Shen and Y. Zhao, “Perceptual hashing for color image based on color opponent component and quadtree structure,” *Signal Processing*, vol. 166, Article ID 107244, 2020.

[13] R. Davarzani, S. Mozaffari, and K. Yaghmaie, “Perceptual image hashing using center-symmetric local binary patterns,” *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4639–4667, 2016.

[14] K. M. Hosny, Y. M. Khedr, W. I. Khedr, and E. R. Mohamed, “Robust color image hashing using quaternion polar complex exponential transform for image authentication,” *Circuits, Systems, and Signal Processing*, vol. 37, no. 12, pp. 5441–5462, 2018.

[15] K. M. Hosny, Y. M. Khedr, W. I. Khedr, and E. R. Mohamed, "Robust image hashing using exact Gaussian-Hermite moments," *IET Image Processing*, vol. 12, no. 12, pp. 2178–2185, 2018.

[16] Y. Zhao and X. Yuan, "Perceptual image hashing based on color structure and intensity gradient," *IEEE Access*, vol. 8, pp. 26041–26053, 2020.

[17] Z. Tang, L. Chen, X. Zhang, and S. Zhang, "Robust image hashing with tensor decomposition," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 3, pp. 549–560, 2019.

[18] L. Du, Z. Chen, and A. T. S. Ho, "Binary multi-view perceptual hashing for image authentication," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 22927–22949, 2020.

[19] X. Liang, Z. Tang, X. Xie, J. Wu, and X. Zhang, "Robust and fast image hashing with two-dimensional PCA," *Multimedia Systems*, vol. 27, no. 3, pp. 389–401, 2020.

[20] A. Neelima and K. Singh, "Perceptual hash function for images based on hierarchical ordinal pattern,," in *Handbook of Multimedia Information Security: Techniques and Applications*, A. Singh and A. Mohan, Eds., Springer, Cham, Switzerland, 2019.

[21] H. Hamid, F. Ahmed, and J. Ahmad, "Robust image hashing scheme using laplacian Pyramids," *Computers & Electrical Engineering*, vol. 84, Article ID 106648, 2020.

[22] G. T. Sigurdson, P. Tang, and M. M. Giusti, "Natural colorants: food colorants from natural sources," *Annual Review of Food Science and Technology*, vol. 8, no. 1, pp. 261–280, 2017.

[23] M. Riaz, G. Kang, Y. Kim, S. Pan, and J. Park, "Efficient image retrieval using adaptive segmentation of HSV color space," in *Proceedings of International Conference on Computational Sciences and its Applications*, Perugia, Italy, June 2008.

[24] M. Loesdau, S. Chabrier, and A. Gabillon, "Hue and saturation in the RGB color space," in *Proceedings of Paper Presented at the 6th International Conference on Image and Signal Processing*, ICISP, Cherbourg, France, June 2014.

[25] S. Engel, X. Zhang, and B. Wandell, "Colour tuning in human visual cortex measured with functional magnetic resonance imaging," *Nature*, vol. 388, no. 6637, pp. 68–71, 1997.

[26] C. P. Yan, C. M. Pun, and X. C. Yuan, "Quaternion-based image hashing for adaptive tampering localization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2664–2677, 2016.

[27] "Ground truth database," October 2017, http://www.cs.washington.edu/research/imagedatabase/groundtruth/.

[28] "Pascal VOC 2007 data set," October 2017, https://pjreddie.com/projects/pascal-voc-dataset-mirror/.