

# 基于颜色矢量角度直方图与 DCT 压缩的鲁棒哈希算法

万兵<sup>1</sup>, 李威<sup>2</sup>

(1.重庆水利电力职业技术学院 智能制造学院, 重庆 402160;

2.吉安职业技术学院 机械与电子工程学院, 吉安 343000)

**摘要:** **目的** 为了改善哈希序列对篡改内容的正确识别率和鲁棒性, 提出基于颜色矢量角度直方图耦合离散余弦变换压缩的鲁棒哈希算法。**方法** 结合插值运算和 Gaussian 滤波器, 对图像实施预处理, 使其对于任意的认证目标均可产生一个固定长度的哈希序列; 引入极坐标变换 LPT (Log-polar transform), 对规范尺寸图像完成坐标变换, 输出二次图像; 借助 SVD (Singular Value Decomposition) 方法来处理二次图像, 输出全局鲁棒特征; 提取规范尺寸图像中所有像素分量的颜色矢量角度, 并计算其对应的直方图, 形成色彩感知特征; 将全局与色彩感知特征组合, 将其视为 1D 哈希序列; 基于离散余弦变换 DCT (Discrete Cosine Transform), 对 1D 哈希序列实施压缩, 输出一组交流系数; 引入 Logistic 映射, 根据其输出的混沌序列来设计差异加密方法, 对交流系数实施扩散, 从而形成目标哈希序列。基于  $l_2$  范数距离和优化的识别阈值, 对待检测图像内容的真伪实施判别。**结果** 试验结果显示, 相对于已有的哈希机制而言, 所提方案具备更强的鲁棒性, 对各类几何攻击均有更高的检测准确度。**结论** 所提哈希方法具有较高的鲁棒性与识别正确率, 对商标检索、信息防伪等领域具有较好的参考价值。

**关键词:** 图像哈希; 颜色矢量角度; 直方图; 极坐标变换; 离散余弦变换; 差异加密方法;  $l_2$  范数距离  
**中图分类号:** TP391 **文献标识码:** A **文章编号:** 1001-3563(2019)07-0229-10

**DOI:** 10.19554/j.cnki.1001-3563.2019.07.035

## Image Robust Hashing Algorithm Based on Color Vector Angle Histogram and DCT Compression

WAN Bing<sup>1</sup>, LI Wei<sup>2</sup>

(1.School of Intelligent Manufacturing, Chongqing Water Resources and Electric Engineering College, Chongqing 402160, China; 2.School of Mechanical and Electronic Engineering, Ji'an College, Ji'an 343000, China)

**ABSTRACT:** to the work aims to improve the correct recognition rate and robustness of hash sequences for tampered content by proposing a robust hash algorithm based on color vector angle histogram and coupled discrete cosine transform compression. Combining interpolation operation with Gauss filter, the image was preprocessed to produce a fixed-length hash sequence for any authentication target. The polar coordinate transformation LPT (Log-polar transform) was introduced to transform the coordinates the image in standard size to output the secondary images. SVD method (Singular Value Decomposition) was used to process the secondary image to output global robust features. Subsequently, the color vector angles of all the pixel components in the normalized size image were extracted, and the corresponding histograms were calculated to form color perception features. Combined global and color perception features were regarded as 1D

收稿日期: 2018-11-19

基金项目: 重庆市 2017 年度教委科学技术研究项目 (KJ1752486, KJ1752485)

作者简介: 万兵 (1970—), 男, 硕士, 重庆水利电力职业技术学院副教授, 主要研究方向为图形图像处理、计算机应用技术。

hash sequences. Based on discrete cosine transform (DCT Discrete Cosine Transform), the 1D hash sequence was compressed to get a set of AC coefficients. By introducing the logistic map, the differential encryption method was designed by the chaotic sequence to diffuse the AC coefficients to form the target hash sequence. Based on the optimal decision threshold and  $l_2$  norm distance, the authenticity of detected image content was discriminated. From the test results, the proposed scheme had stronger robustness and higher detection accuracy for various geometric attacks than the current hash mechanism. This hash method has high robustness and recognition accuracy, which has good reference value for trademark retrieval, information anti-counterfeiting and other fields.

**KEY WORDS:** image hashing; color vector angle; histogram; polar coordinate transformation; discrete cosine transformation; differential encryption;  $l_2$  norm distance

近年来,许多功能强大的图像编辑软件可以免费使用,导致图像可被非用户进行肆意修改,给信息安全带来了一定的威胁<sup>[1-2]</sup>,因此,为了实现对图像内容实施认证,较为流行的方案有图像取证和哈希方法。对于取证机制而言,虽然它可以定位出伪造内容,但其效率不理想<sup>[3]</sup>。哈希方法主要是利用图像中的鲁棒特征来生成相应的哈希序列,可作为图像的唯一表示而用于信息的真假判别<sup>[3-5]</sup>。如金晓民等<sup>[3]</sup>利用SVD方法来处理尺寸规范图像的鲁棒特征,并计算了二次图像的颜色矢量角度,并定义2个鲁棒特征提取方法来获取Y分量的感知特征,将三者组合,形成了哈希序列,并对其实施加密,改善算法的安全性。该方案是直接颜色矢量角度作为哈希序列,而且只考虑了Y分量的目标边缘特征,忽略了其他有用信息,使其对旋转篡改的鲁棒性有待提高。Tang等<sup>[6]</sup>利用PHT方法来处理图像,并联合Fourier方法,从二次图像中提取目标的鲁棒特征,将其视为哈希序列,并利用量化压缩方法,对其实施降维处理,输出紧凑的哈希序列。该方案虽然采用了PHT机制,但其忽略了图像色彩信息,不能充分提取图像的鲁棒特征,使其对篡改攻击的稳健性不理想。Qin等<sup>[7]</sup>设计了基于感知特征与结构特征的鲁棒哈希方案,利用高斯滤波器与线性插值来归一化图像尺寸,并对二次图像实施编码,输出不同方向上的编码映射,基于直方图合成机制,提取感知特征,同时,从包含最丰富角点的选择性采样块所对应的频率系数和位置信息中提取结构特征,将二者组合,并进行降维处理,输出紧凑哈希序列。但是,此方案没有考虑彩色图像的色彩特征,对颜色与亮度调整修改的鲁棒性较低,削弱了哈希敏感性。

为了充分利用图像的色彩特征,提高哈希对旋转、亮度等操作的鲁棒性,文中设计了基于颜色矢量角度直方图耦合离散余弦变换压缩的鲁棒哈希算法。利用LPT方法来生成抗旋转操作的二次图像;并借助SVD(Singular Value Decomposition)机制,克服二次图像在水平方向的不稳定性,将其生成的奇异值当作全局鲁棒特征。提取规范尺寸图像的颜色矢量角度,通过计算其对应的直方图来获取色彩感知特征,

增强其对亮度与色彩修改的鲁棒性。组合全局与色彩感知特征,形成一维哈希序列;再使用DCT方法来压缩一维哈希序列,降低其维数,改善哈希生成效率。同时,为了提高哈希安全性,利用差异加密方法对DCT方法产生的交流系数完成扩散,以生成所需的哈希序列。通过计算真实图像与可疑目标的哈希序列对应的 $l_2$ 范数距离来实施真伪判别。最后,在多种几何变换下,测试了所提哈希方案的鲁棒性。

### 1 所提的鲁棒哈希算法

所提的基于颜色矢量角度直方图耦合离散余弦变换压缩的鲁棒哈希算法过程见图1。由图1可知,该哈希方案主要有5个阶段:预处理;基于LPT与

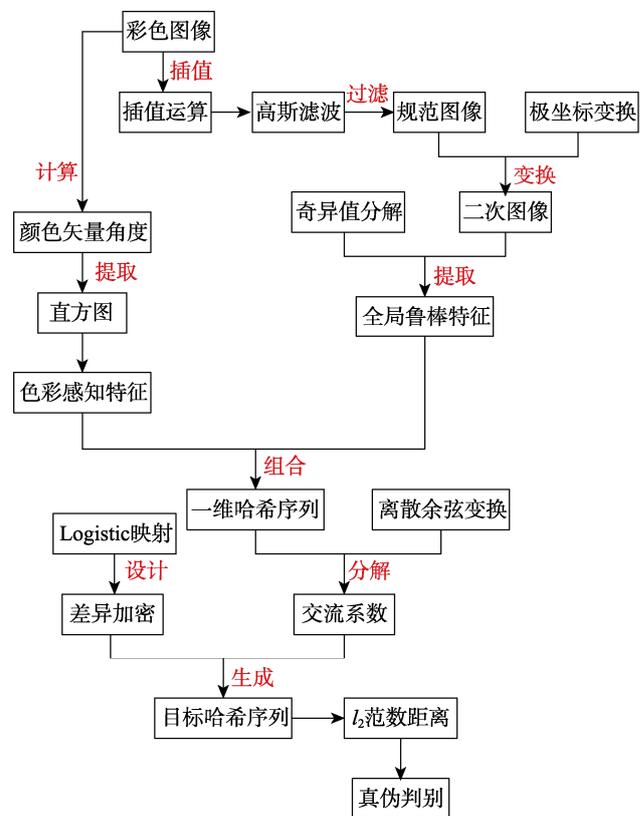


图1 文中鲁棒哈希算法的过程  
Fig.1 Process of proposed robust hashing algorithm

SVD 的全局特征提取；基于颜色矢量角度的感知特征提取；基于离散余弦变换的哈希压缩；哈希加密与认证。

### 1.1 彩色图像的预处理

为了增强哈希算法对缩放、噪声等内容修改的鲁棒性<sup>[2]</sup>，文中首先采用 2D 插值运算<sup>[2]</sup>来规范彩色图像的尺寸，使其对于任意的目标均可生产固定长度的哈希序列：

$$z_X = y_0 + \frac{y_1 - y_0}{x_1 - x_0} (z_Y - x_0) \tag{1}$$

$$z_Y = x_0 + \frac{x_1 - x_0}{y_1 - y_0} (z_X - y_0) \tag{2}$$

式中： $x_0, x_1$  为插值运算的起点； $y_0, y_1$  为  $x_0, x_1$  的插值运算结果； $x_0 \leq z_X \leq x_1, y_0 \leq z_Y \leq y_1$ 。

再借助 Gaussian 滤波器<sup>[8]</sup>来过滤规范图像中的噪声。若  $G(i, j)$  是卷积掩码中位于  $(i, j)$  处的元素，则根据式 (3) 函数来完成 Gaussian 滤波处理<sup>[8]</sup>：

$$\begin{cases} G(i, j) = \frac{g(i, j)}{\sum_{i=1}^M \sum_{j=1}^N g(i, j)} \\ g(i, j) = e^{-\frac{(i^2 + j^2)}{2\sigma^2}} \end{cases} \tag{3}$$

式中： $\sigma$  为  $G(i, j)$  对应的标准偏差。

选择图 2a 所示的彩色图像作为样本，通过式 (1—3) 插值与滤波后，输出的预处理结果分别见图 2b—c。根据输出结果发现，初始彩色经插值与滤波处理后，可得到一个无噪声干扰的尺寸规范图像。



图 2 彩色图像的预处理  
Fig.2 Preprocessing of color images

### 1.2 基于 LPT 与 SVD 的全局特征提取

上述尺寸规范图像对抗旋转操作能力较低，因此，文中借助 LPT 方法<sup>[9]</sup>来增强其抗旋转操作的能力。若  $(x_0, y_0)$  为尺寸规范图像的中心坐标，则  $(x, y)$  是规范图像在 Cartesian 内特定像素的坐标。对于大小为  $M \times M$  的规范图像，有  $1 \leq x \leq M, 1 \leq y \leq M$ 。令  $(\rho, \theta)$  为  $(x, y)$  的对数极坐标，见图 3，则  $\rho, \theta$  对应的计算模型为：

$$\begin{cases} x = e^\rho \cos \theta \\ y = e^\rho \sin \theta \end{cases} \tag{4}$$

$$\rho = \ln \sqrt{(x - x_0)^2 + (y - y_0)^2} \tag{5}$$

$$\theta = \arctan \frac{y - y_0}{x - x_0} \tag{6}$$

式中： $\rho$  为像素  $(x, y)$  与  $(x_0, y_0)$  之间的距离； $\theta$  为旋转角度。

通过式 (4) 发现，LPT 充分考虑了旋转角度  $\theta$ ，从而可以增强其对任意角度的旋转操作的鲁棒性。令规范图像为  $f(x, y)$ ，则其形成的二次图像为<sup>[10]</sup>：

$$f_1(\rho, \theta) = f_0[\rho, (\theta + \theta_0)] \tag{7}$$

式中： $f_0$  为  $Y$  分量； $f_1(\rho, \theta)$  为经过 LPT 处理所形成的二次图像。

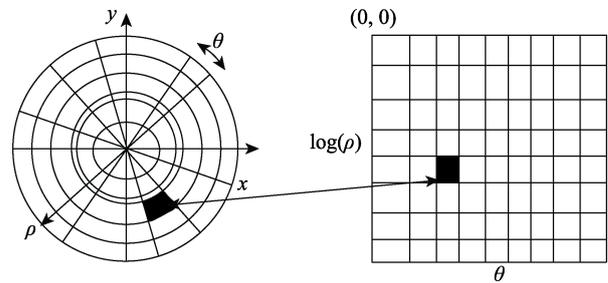


图 3 Cartesian 坐标演变成对数极坐标  
Fig.3 Evolution of Cartesian coordinates into log polar coordinates

以图 2c 为样本，对其实施 90° 旋转后，结果见图 4b。借助 LPT 方法对其处理后，对应的结果见图 4c—d。根据 2 个不同样本的 LPT 变换结果发现，即使规范图像旋转了 90°，在二次图像中，其内容也只在水平方向出现周期性变化，剩余内容均不变。

根据上述描述可知，LPT 方法对角度旋转具备较高的鲁棒性。根据图 3 发现，当规范图像发生  $\theta$  角度旋转后，其内容会引起圆形漂移，此处特征的稳健性不理想。故利用奇异值分解<sup>[11]</sup>SVD (Singular Value Decomposition) 来解决此问题，以获取二次图像中的鲁棒特征。令二次图像为  $X$ ，则其 SVD 变换函数为<sup>[11]</sup>：

$$X = S \cdot V \cdot D \tag{8}$$

式中： $S, D$  为  $X$  的正交矩阵； $V$  为  $X$  的对角矩阵，包含了  $m$  个奇异值。



图4 二次图像的形成  
Fig.4 Formation of secondary image

随后，把式(8)输出的对角矩阵中的所有奇异值组合成一个向量  $\beta = \{\beta_1, \beta_2 \dots \beta_m\}$ ，将其视为全局鲁棒特征。根据上述过程发现， $\beta = \{\beta_1, \beta_2 \dots \beta_m\}$ 是经过LPT与SVD方法共同处理后得到的数据，充分结合了SVD与LPT的优势。

### 1.3 基于颜色矢量角度的感知特征提取

在已有的彩色图像哈希方法中，主要是提取亮度分量的特征，使其不能较好地捕获图像的颜色信息<sup>[12]</sup>，因此，文中引入颜色矢量角度<sup>[12]</sup>CVA (Color Vector Angle) 来生成哈希。虽然CVA对于强度变化是稳定的，但是当改变图像的色度时，可以采用CVA来捕获色调与饱和度之间的差异。对于2个不同的像素，其相应的CVA值存在巨大差异，因此，与Euclidean距离相比，CVA能更充分地表征图像的感知特征。如图5所示， $(C_1, C_2)$ ， $(C_3, C_4)$ 这2对颜色像素存在视觉差异，但其Euclidean距离时相等的，均为8.944；二者的CVA值有较大差别， $(C_1, C_2)$ ， $(C_3, C_4)$ 的CVA值分别为0.034 86, 0.6193 rad。对于彩色图像，CVA能够有效体现不同目标的颜色差异。

令  $P_1 = [R_1, G_1, B_1]^T$  与  $P_2 = [R_2, G_2, B_2]^T$  是2个不同的RGB颜色。其中， $R_v, G_v, B_v, v=1, 2$  分别代表彩色图像的红、绿、蓝成分，因此，可以计算  $P_1$  与  $P_2$  之间的CVA值。

$$\theta = \arcsin \left( 1 - \frac{(P_1^T P_2)^2}{P_1^T P_1 P_2^T P_2} \right)^{1/2} \quad (9)$$

在所提方案中，为了方便计算，采用CVA的余弦值来代替CVA自身，从而将式(9)变换成：

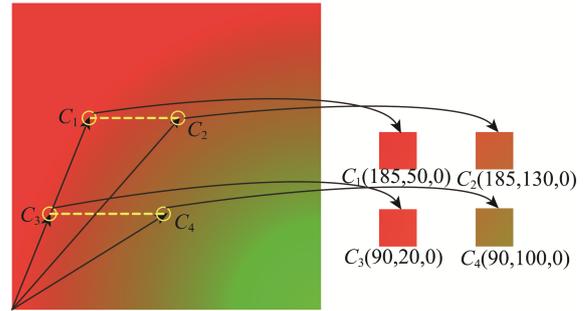


图5 不同的2对颜色像素对应的CVA值与Euclidean距离  
Fig.5 CVA value and Euclidean distance for different two pairs of color pixels

$$\sin \theta = \left( 1 - \frac{(P_1^T P_2)^2}{P_1^T P_1 P_2^T P_2} \right)^{1/2} \quad (10)$$

最后，借助式(10)，提取彩色图像中全部像素的CVA值，从而获取CVA的特征矩阵：

$$A = \begin{bmatrix} \sin \theta_{1,1}, \sin \theta_{1,2} \dots \sin \theta_{1,M} \\ \sin \theta_{2,1}, \sin \theta_{2,2} \dots \sin \theta_{2,M} \\ \vdots \\ \sin \theta_{M,1}, \sin \theta_{M,2} \dots \sin \theta_{M,M} \end{bmatrix} \quad (11)$$

以图2c为样本，基于上述过程，输出其对应的颜色矢量角度，见图6a。一般而言，旋转是以图像中心为坐标原点来实现的，在旋转操作后，内切圆中的图像像素被很好地保存。另外，对于不同的图像，其直方图也存在较大差异。基于这些考虑，所提方案通过提取内切圆中的图像CVA对应的直方图来生成哈希。令  $(x_c, y_c)$  为彩色图像的中心，其尺寸为  $M \times M$ ，则  $(x_c, y_c)$  的计算函数如下：

$$\begin{cases} x_c = y_c = M/2 & \text{if } M \text{ 为偶数} \\ x_c = y_c = (M+1)/2 & \text{if } M \text{ 为奇数} \end{cases} \quad (12)$$

若彩色图像中位于坐标  $(x, y)$  处的像素满足如下条件，则提取其CVA值对应的直方图：

$$(x - x_c)^2 + (y - y_c)^2 \leq r^2 \quad (14)$$

其中， $r$  为内切圆半径。

由于式(10)的取值范围在  $[0,1]$  内，因此，在提取CVA对应的直方图之前，必须对其采样。为此，文中以步长  $\Delta=0.005$ ，对  $[0,1]$  实施采样，从而可输出  $V=201$  个离散值。随后，对每个CVA的余弦值实施量化，使其与这些离散值相等。最后，根据每个像素的CVA值，提取对应的直方图。令  $f(t), t=0,1,2 \dots V-1$  是第  $(t+1)$  个直方图 bin 值，因此，对于内切圆图像而言，总共可以生产  $V$  个直方图 bin，将这些  $f(t)$  视为感知特征，记为  $z = \{z_1, z_2 \dots z_V\}$ 。以图6a为例，其对应的内切圆结果见图6b，最终形成的CVA直方图见图6c。

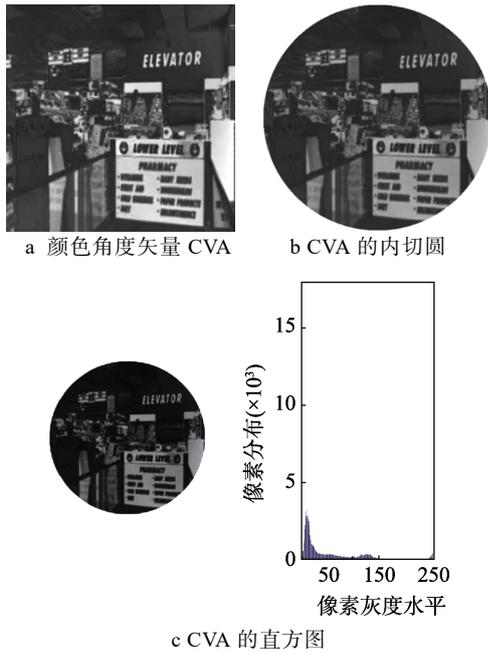


图 6 CVA 直方图的提取  
Fig.6 Extraction of CVA histogram

### 1.4 基于离散余弦变换的哈希压缩

将上述过程提取的特征  $\beta = \{\beta_1, \beta_2 \dots \beta_m\}$  与  $z = \{z_1, z_2 \dots z_V\}$  实施组合, 记为  $q = \{q_1, q_2 \dots q_k\}$ ,  $k = V + m$ 。若直接将  $q = \{q_1, q_2 \dots q_k\}$  作为最终的哈希序列, 会使其维度较高, 易增大算法的复杂度。故借助离散余弦变换 DCT<sup>[13]</sup> 来实现  $q = \{q_1, q_2 \dots q_k\}$  的压缩。对于 1D 数据  $q = \{q_1, q_2 \dots q_k\}$ , 其对应的一维 DCT 函数为:

$$C(u) = a(u) \sum_{t=0}^{N-1} f(t) \cos \left[ \frac{(2t+1)u\pi}{2N} \right], u = 0, 1, 2 \dots N-1 \quad (15)$$

式中:  $C(u)$  为一维 DCT 变换系数;  $\cos$  为余弦变换;  $a(u)$  为  $C(u)$  的核变换, 其模型为:

$$a(u) = \begin{cases} \sqrt{\frac{1}{N}} & u = 0 \\ \sqrt{\frac{2}{N}} & u = 1, 2 \dots N-1 \end{cases} \quad (16)$$

数据  $q = \{q_1, q_2 \dots q_k\}$  经过式 (15) 变换后, 可输出  $V+m$  个 DCT 系数。由于初始数据的主要能量集中在 DCT 变换的交流系数上, 能充分反映其特征, 因此, 文中将所有的交流系数作为哈希序列, 记为  $h^t = \{h^t_1, h^t_2, h^t_3 \dots h^t_n\}$ ,  $n \ll V + m$ 。其中,  $n$  为交流系数的数量。

### 1.5 哈希加密与认证

为了改善哈希方案的防碰撞性, 引入 Logistic 映射<sup>[14]</sup>, 设计差异加密方法, 实现  $h^t = \{h^t(1), h^t(2), h^t(3) \dots h^t(m)\}$  的加密。首先, 借助彩色图像的总像素量来估算 Logistic 映射的初值  $x_0$ :

$$x_0 = T / 10^7 \quad (17)$$

式中:  $T$  为彩图的总像素量。

再设置  $\gamma$ , 对 Logistic 映射实施迭代<sup>[14]</sup>:

$$x_{n+1} = \gamma x_n (1 - x_n) \quad (18)$$

其中,  $\gamma \in (0, 4)$  为混沌窗口变量。

构建密钥量化方法, 对式 (18) 输出的随机序列实施处理, 以获取加密密钥  $\{k_i\}$ :

$$k_i = \text{mod}(\text{floor}(x_i \times 10^{14}), 256) \quad (19)$$

其中,  $\text{mod}$  为求余运算。

基于  $\{k_i\}$ , 计算 2 个扩散引擎  $kt_1, kt_2$ :

$$kt_1 = \text{floor} \left( \frac{\text{mod}(P_{(i-1)} + k_i, 256)}{256 \times (i-1)} \right) + 1 \quad (20)$$

$$kt_2 = \text{floor} \left( \frac{\text{mod}(P_{(i-1)} + k_i, 256)}{256 \times (M \times N - i - 1)} \right) + 1 \quad (21)$$

联合  $kt_1, kt_2$  与  $\{k_i\}$ , 设计差异加密函数, 对  $h^t = [h^t_1, h^t_2, h^t_3 \dots h^t_n]$  中的元素实施扩散:

$$h_i = h^t_i \oplus k_i \oplus P_{kt_1} \oplus P_{kt_2}, i = 1, 2 \dots n/2 \quad (22)$$

$$h_i = h^t_i \oplus k_i \oplus P_{kt_1}, i = n/2 + 1, n/2 + 2 \dots n \quad (23)$$

通过对  $h^t = [h^t_1, h^t_2, h^t_3 \dots h^t_n]$  完成加密, 可获取一组安全哈希序列  $h = [h_1, h_2, h_3 \dots h_n]$ 。随后, 借助  $l_2$  范数距离<sup>[15]</sup> 来实现可疑图像的判别。令真实彩图的哈希序列为  $H_0 = \{h^0_1, h^0_2, h^0_3 \dots h^0_n\}$ ; 可疑图像经过上述哈希算法后, 输出的哈希序列为  $H_1 = \{h^1_1, h^1_2, h^1_3 \dots h^1_n\}$ 。计算 2 个哈希之间的  $l_2$  范数距离<sup>[15]</sup>  $d$  来评估  $H_0, H_1$  的相似性:

$$d(H_0, H_1) = \sqrt{\sum_{i=1}^n [h^0_i - h^1_i]^2} \quad (24)$$

一般而言,  $d$  值越小, 说明  $H_0$  与  $H_1$  之间的相似性越高。再借助实验优化的阈值  $W$ , 若  $d \leq W$ , 则可将二者作为一对相似图像; 否则, 二者为差异图像。

## 2 实验结果与分析

为了验证所提哈希方案的鲁棒性与判别准确度, 从 UCID 图像集<sup>[16]</sup> 中任意选择图像来完成试验, 并且将哈希鲁棒性较好的方案当作此次试验的对比组, 分别是文献[5]、文献[6]中的方案, 从而反映出所提方案的优势。就整个哈希方案而言, 阈值  $W$  直接影响了对可疑图像的判别准确性, 是一个非常重要的参数, 因此, 首先要优化该  $W$  值。剩余的实验参数具体值为: 图像尺寸  $M \times M = 512 \times 512$ 、标准偏差  $\sigma = 1$ 、混沌窗口变量  $\gamma = 3.73$ 、内切圆半径  $r = 256$  像素。

### 2.1 阈值 $W$ 的优化

在 UCID 图像集<sup>[16]</sup> 中任意确定 50 幅目标图像, 然后根据表 1 中的几何攻击对其实施操作, 借助 PS

软件,最终输出 800 对感知相似图像;随后,在此图像集中选择 200 幅不同的图像,再次利用 PS 软件,通过复制-粘贴、裁剪以及组合恶意攻击,输出 1600 对视觉差异图像。按照式(24)计算源图像与可疑目标间的  $l_2$  范数距离。通过观察每个  $l_2$  范数距离对应的频数变化来找出一个较优的  $W$ 。

图 7 显示了源图像与可疑目标间的  $l_2$  范数距离分布状况。由图 7a 发现,就这些感知相似图像对而言,当  $d < 25.5$  时,其产生的频率变化很集中;再基于图 7b 发现,就视觉差异图像对而言,在  $d > 27$  时,产生的

频率变化很集中。根据这个测试结果,文中取  $W=25$  为最优阈值。

表 1 不同攻击类型及其参数  
Tab.1 Different attack types and parameters

操作类型	参数
椒盐噪声	0.01, 0.03, 0.05, 0.08
亮度调整	0.8, 1.6, 2.2, 2.8
旋转	15°, 45°, 75°, 125°
缩放	0.4, 0.9, 1.2, 1.5

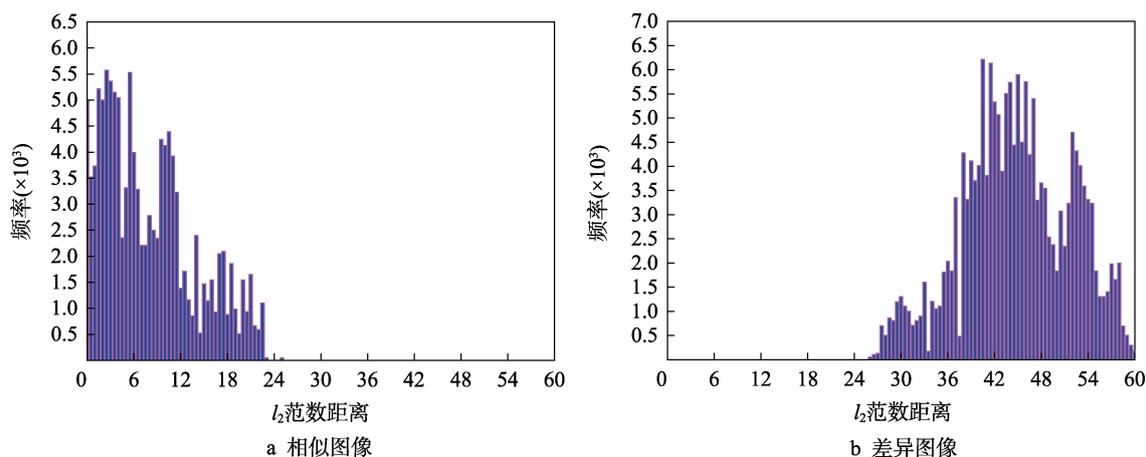


图 7 阈值  $W$  的优化  
Fig.7 Optimization of threshold  $W$

## 2.2 鲁棒性测试

鲁棒性是客观衡量哈希方案的重要指标<sup>[3]</sup>。故从 UCID 图像库随机选择 4 幅图像作为样本来进行实验,见图 8a—d;并把表 2 中的内容修改类型作用于图 8a—d;基于所提方案的哈希过程,使用式(24)计算内容修改前后目标对应的  $l_2$  范数距离,形成的曲线见图 8e—h。根据输出数据发现,利用表 2 中的修改类型来篡改样本,其生产的哈希与初始图像之间的  $l_2$  范数距离  $d$  均低于 25。例如,对于噪声与尺度缩放,所提方案的  $l_2$  范数距离  $d$  值远低于 25, Sea 图像的最大  $d$  值仅为 14.3,见图 8e;面对缩放修改时,其最大  $d$  值为 21.7 左右,见图 8h;对于亮度修改,利用所提哈希方案得到的最大  $d$  值为 22.3(Barbara 图像),见图 8f;对于旋转修改,其最大  $d$  值为 23.8(Peppers 图像),见图 8g。这说明文中方案对表 2 中的内容修改类型具备理想的鲁棒性,将其全部当作视觉相似图像,判别正确。原因是所提哈希方案对初始图像进行了插值与 Gaussian 滤波操作,增强哈希序列对噪声和缩放操作的稳健性,并且联合 LPT 与 SVD 方法来提取图像的全局特征,改善其对任意角度旋转的判别准确性,与此同时,提取规范尺寸图像的颜色矢量角度,利用其对应的直方图来生成感知特征,使其对亮度调整等操作具备理想的鲁棒性。

## 2.3 敏感性测试

敏感性是评估哈希方案的经典指标,在初始图像内容遭遇恶意修改时,其产生的哈希序列与真实图像截然不同<sup>[17]</sup>。在此次测试中,将图 9a 为样本,并施加 4 种篡改类型,分别见图 9b—e;随后,基于该哈希方法,联合再利用所提式(24),计算恶意攻击前后图像的  $l_2$  范数距离,输出数据见表 2。由数据发现,所提哈希方案可以实现对不同篡改类型的准确判别,当样本遭遇复制-粘贴以及其他组合恶意篡改时,得到的  $l_2$  范数距离都要高于 25。例如,对于图 9c—e,三者的  $l_2$  范数距离分别为 28.51, 31.29, 28.07,此时将其判别为伪造图像;而图像遇到噪声修改时,输出的  $l_2$  范数距离为 12.65,远低于 25,此时可判别为真实图像。这些测试结果显示文中哈希方法具备强烈的敏感性,可以准确完成各种攻击类型下的图像判别。原因是文中哈希方案计算了彩色图像的颜色角度矢量,并提取其直方图来生成哈希序列,当图像受到恶意篡改时,其直方图内容会发生较大变化,从而使得最终形成的哈希序列也存在较大差异。

## 2.4 不同哈希算法的鲁棒性测试

为了反映出所提方案的优势,测试了其文献[5]、文献[6]三者对应的 ROC 曲线。ROC 曲线<sup>[3]</sup>由正

确识别率  $P_{TPR}$ 、虚警率  $P_{FPR}$  构成，相应的模型为：

$$P_{TPR} = \frac{n_1}{M_1}, P_{FPR} = \frac{n_2}{M_2} \quad (25)$$

式中： $n_1$  为正确判别的图像总量； $n_2$  为错误决策的图像总量； $M_1, M_2$  分别为真实图像与可疑图像的

总和<sup>[3]</sup>。

所提方案与 2 种对照组的 ROC 曲线见图 10。通过观察这些 ROC 曲线发现，所提技术与文献[5]、文献[6]方法对任意参数的缩放、噪声等内容修改均有较强的鲁棒性，所得到的 ROC 曲线状态较为理想，准

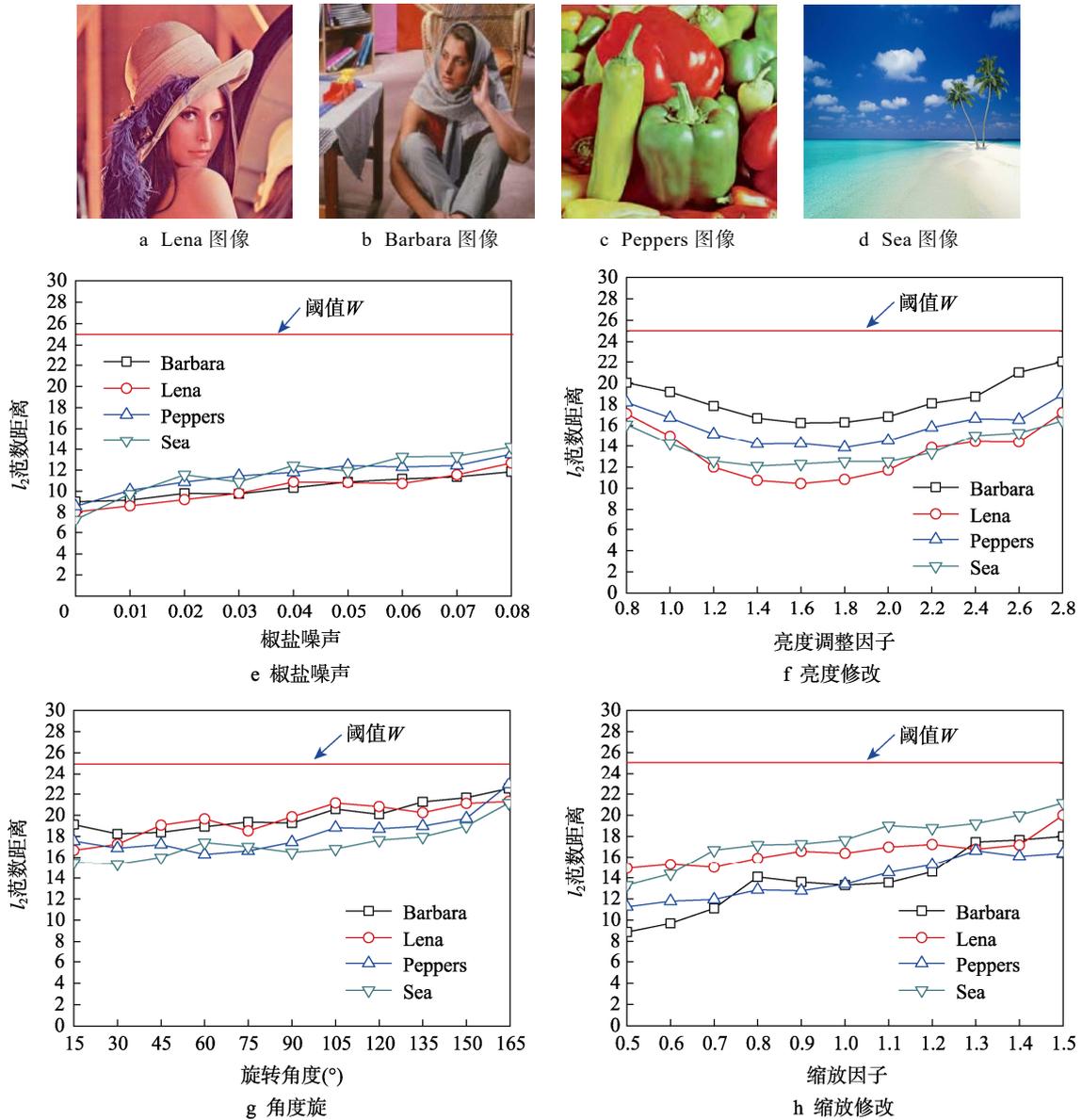


图 8 文中哈希算法的鲁棒性测试  
Fig.8 Robustness test of proposed hash algorithm



图 9 内容修改图像  
Fig.9 Content modification image

表2 篡改前后图像间的  $l_2$  范数距离  
Tab.2  $l_2$  normal distance between images before and after Tamper

名称	范数距离
图 9b	12.65
图 9c	28.51
图 9d	31.29
图 9e	28.07

确识别率维持在 0.95 以上,对于噪声修改。当  $P_{FPR}=0$  时,所提方案、文献[6]和文献[5]的  $P_{TPR}$  分别为 0.957, 0.955, 0.954, 继续增大虚警率  $P_{FPR}$  至 0.3 时,其  $P_{TPR}$  分别为 0.999, 0.998, 0.998, 三者非常接近,对于尺度攻击,也有相似的鲁棒性能,见图 10a 与图 10b。但是,面对亮度与大角度旋转操作时,所提方案表现出更大的优势。文献[5]虽然对亮度具备较高的稳健性,但其对大角度旋转的鲁棒性欠佳,见图 10c、图 10d。文献[6]对大角度旋转攻击具备较好的鲁棒性,但是对亮度修改的鲁棒性较低。例如,就大角度旋转操作而言,当  $P_{FPR}=0$  时,文献[5]、文献[6]与所提方案的  $P_{TPR}$  分别为 0.902, 0.920, 0.941。面对亮度操作攻击时,当  $P_{FPR}=0$  时,所提哈希方案的  $P_{TPR}=0.932$ , 文献[5]、文献[6]的  $P_{TPR}$  分别为 0.913, 0.818; 当

$P_{FPR}=0.3$  时,三者的  $P_{TPR}$  分别为 0.999, 0.993, 0.971。原因是所提方案与文献[5]、文献[6]方法均采用了插值与 Gaussian 滤波器对初始图像实施了预处理,使得这三者对于噪声与缩放均有理想的稳健性。文献[5]考虑了彩色图像的颜色矢量角度,使其对亮度修改也具有理想的鲁棒性,并充分利用奇异值分解 SVD 的稳定性来提高哈希算法对旋转的鲁棒性,但是,这种 SVD 对大角度旋转的鲁棒性不佳,且该技术只利用了 Y 分量来生成哈希序列,忽略了其他分量的特征信息,使其对彩色图像的描述能力不足,导致其鲁棒性有待提高。文献[6]则是联合 PHT 方法与 Fourier 变换来提取彩色图像的全局特征,利用其来生成哈希序列,使其对任意角度的旋转操作均有较高的鲁棒性,但是其忽略了图像色彩信息,不能充分提取图像的鲁棒特征,使其对亮度调整的鲁棒性较弱。文中哈希方案不仅采用了与文献[5]、文献[6]相同的预处理方法,而且还充分结合 PHT 与 SVD 方法的优势,使其生成的哈希对任意角度旋转操作均表现出理想的鲁棒性,并且还计算了彩色图像所有分量的颜色矢量角度,通过提取其对应的直方图来做为感知特征,并联合全局与感知特征来生成哈希,使其对彩色图像的描述更为充分,从而使其对亮度与大角度旋转操作的鲁棒性均要优于文献[5]、文献[6]。

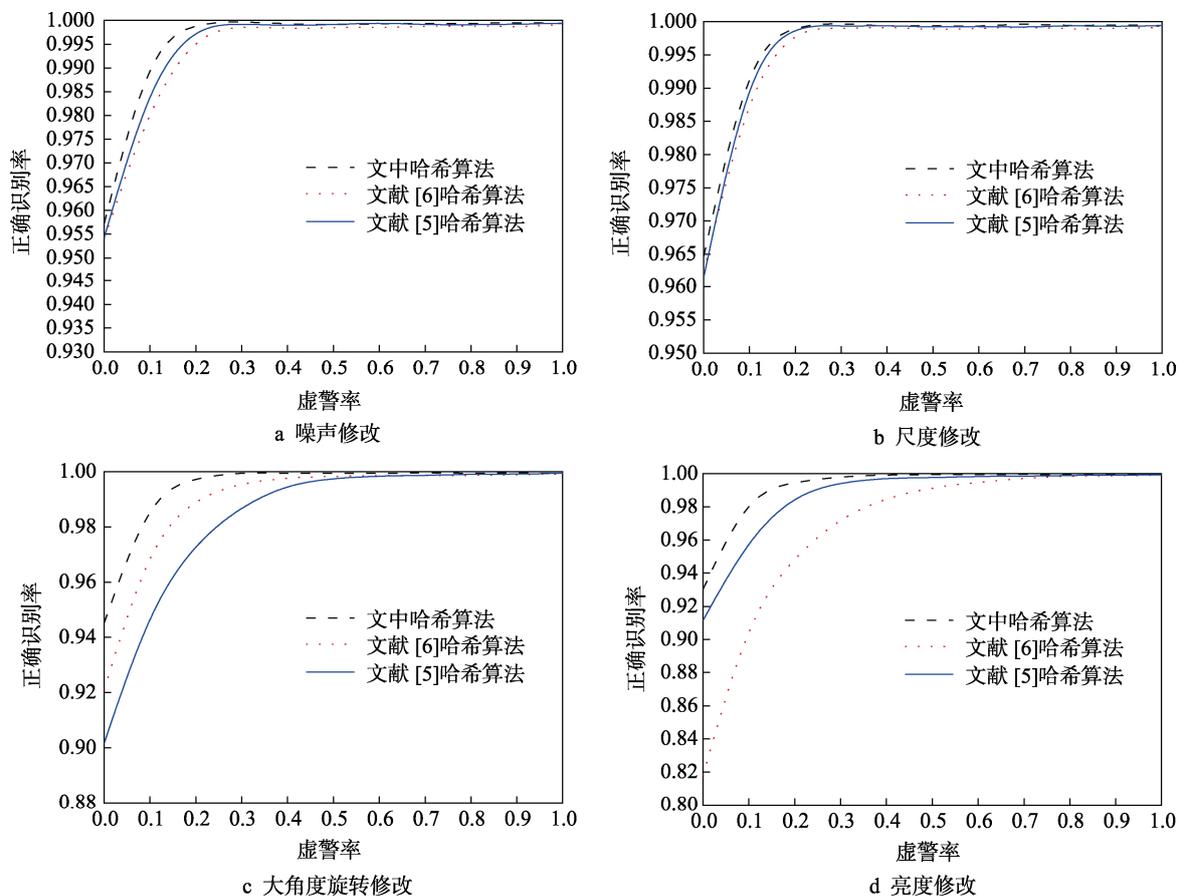


图 10 3 种算法的鲁棒性测试  
Fig.10 Robustness test of three algorithms

## 2.5 所提算法在商标检索领域中的应用测试

随着市场与包装行业的繁荣发展，各式各样的产品也相继被生产加工出来，为了保护公司与产品的属性，人们通常会向相关部门注册商标，通常，商标图像包含了文字、符号、各种形状、颜色等信息<sup>[18]</sup>。为了准确地从大型数据库中准确检索到目标图像，诸多学者们利用哈希技术来实现该目的<sup>[19-20]</sup>。文献[19]是一种典型的基于哈希算法的商标检索方案，其检索过程为：根据设计的哈希方法来获取待查询商标图像的哈希序列；利用支持向量机哈希序列实施处理，输出二进制哈希序列；最后通过计算查询目标与图像库中的目标之间的汉明距离来完成检索。

为了测试所提哈希在商标检索中的应用效果，利用所提哈希方案替换文献[19]中哈希算法（也就是改变步骤 1），其余检索过程保持不变，从而得到文中哈希对应的检索步骤如下所述。

1) 利用所提哈希算法替换文献[19]的哈希方案，输出查询商标图像对应的哈希序列。

2) 再按照文献[19]的方法，利用支持向量机对所提算法的哈希序列实施处理，输出二进制哈希序列。

3) 最后通过计算查询目标与图像库中的目标之间的汉明距离来完成检索。

以图 11 所示的“adidas 商标”为样本，利用 PS 软件，通过对其施加噪声、旋转、缩放、JPEG 压缩、模糊、内容复制-粘贴、亮度调整以及裁剪等不同参数的几何攻击，输出 850 幅图像，再额外添加 150 幅其他商标图像，自行构建一个含有 1000 幅图像的数据库。在返回检索结果时，设置返回数量为 10 幅。在利用所提哈希的检索过程与文献[19]对其实施检索，结果分别见图 12 和图 13。依图 12—13 可知，利用所提哈希算法来替换文献[19]的哈希方案后，输出的检索结果中，只有 1 幅图像是错误的，见图 12 中的最后一幅图像“华为”商标；而文献[19]的检索方法在面对这种复杂数据库时，其返回结果中有 3 幅图像是错误的，见图 13 中的方框标识。这说明所提哈希方案可以用于商标图像的检索，而且也显示了所提哈希方案要优于文献[19]中的哈希方法，使其呈现出较好的检索精度。



图 11 待查询的商标图像  
Fig.11 Trademark image to be queried



图 12 文中哈希方案的检索结果  
Fig.12 Retrieval results of the proposed hash scheme



图 13 文献[19]的检索结果  
Fig.13 Retrieval results of reference [19]

## 3 结语

为了改善哈希方案对各种内容修改类型的鲁棒性，文中通过提取图像的颜色矢量角度对应的直方图来形成鲁棒哈希方案。通过对初始彩色图像实施预处理，可固定哈希长度，增强哈希算法对噪声的抗干扰能力。并联合 PHT 与 SVD 方法，充分利用二者的优势，从规范尺寸图像中提取出全局鲁棒特征。另外，由于所提方案考虑了颜色矢量角度的直方图，图像进行旋转时，因其不改变图像内接圆中的像素，因此该直方图也不变。这 2 个过程保证所提哈希方案可以抵抗任意角度的旋转。颜色矢量角度可以很好地测量彩色图像中的色调与饱和度的差异，从而有效增强其敏感性，改善哈希对图像内容的辨别能力。利用 Logistic 映射输出的混沌序列来设计差异加密机制，以提高哈希方案的防碰撞性能。测试数据验证了所提哈希方案对不同类型的内容修改均有理想的鲁棒性，尤其是对

亮度与角度旋转, 呈现出更大的优势。

所提虽然采用了离散余弦变换来对其实施压缩, 但其哈希长度仍有 189 bits, 后续将引入多维尺度变换, 设计一种新的量化压缩机制, 以改善所提方案的哈希生成效率。

#### 参考文献:

- [1] QU Wen, WANG Da-ling, FENG Shi. A Novel Cross-Modal Hashing Algorithm Based on Multimodal Deep Learning[J]. Science China Information Sciences, 2017, 60(9): 156—167.
- [2] RAM K K. Robust Image Hashing Through DWT-SVD and Spectral Residual Method[J]. EURASIP Journal on Image and Video Processing, 2017, 9(1): 1—17.
- [3] 金晓民, 张丽萍. 基于混合特征与颜色矢量角度的鲁棒彩色图像哈希认证算法[J]. 计算机科学与探索, 2018, 12(10): 1672—1683.  
JIN Xiao-min, ZHANG Li-ping. Image Hash Authentication Algorithm Based on Mixed Feature and Color Vector Angle[J]. Computer Science and Exploration, 2018, 38(7): 1102—1115.
- [4] 王彦超, 郭静博, 周丽宴. 基于数据投影降维机制与对称局部二值模式的紧凑图像哈希算法[J]. 激光与光电子学进展, 2017, 54(2): 4—16.  
WANG Yan-chao, GUO Jing-bo, ZHOU Li-yan. Compact Image Hashing Algorithm Based on Data Projection Dimensionality Reduction Mechanism and Symmetrical Local Binary Mode[J]. Progress in laser and Optoelectronics, 2017, 54(2): 4—16.
- [5] 张勇, 黄家荣. 非负矩阵分解耦合环形分割的图像哈希认证算法[J]. 计算机工程与设计, 2018, 38(9): 2464—2471.  
ZHANG Yong, HUANG Jia-rong. Image Hash Authentication Algorithm Based on Negative Matrix Factorization Coupled with Ring Division[J]. Computer Engineering and Design, 2018, 38(9): 2464—2471.
- [6] TANG Zhen-jun, HUANG Zi-qing, ZHANG Xian-quan. Robust Image Hashing with Multidimensional Scaling[J]. Signal Processing, 2017, 137(22): 240—250.
- [7] QIN Chuan, CHEN Xue-qin, LUO Xiang-yang. Perceptual Image Hashing Via Dual-Cross Pattern Encoding and Salient Structure Detection[J]. Information Sciences, 2018, 423(19): 284—302.
- [8] SEBASTIAN S C, JUAN R A. Image Dehazing Using Morphological Opening, Dilation and Gaussian Filtering[J]. Signal, Image and Video Processing, 2018, 12(7): 1329—1335.
- [9] SONDOS M F, NOURA A S. Robust Copy-move Forgery Revealing in Digital Images Using Polar Coordinate System[J]. Neurocomputing, 2017, 265(11): 57—65.
- [10] 冯贺, 常国权, 郭晓波. 超复数 Fourier 变换耦合位  
置扰乱的彩色图像哈希算法[J]. 计算机科学与探索, 2016, 11(11): 1837—1848.  
FENG He, CHANG Guo-quan, GUO Xiao-bo. Hash Algorithm for Color Image Based on Super Complex Fourier Transform and Position Disturbance[J]. Journal of Frontiers of Computer Science & Technology, 2016, 11(11): 1837—1848.
- [11] NEELIMA A, SINGHI K M. Perceptual Hash Function Based on Scale-Invariant Feature Transform and Singular Value Decomposition[J]. The Computer Journal, 2016, 59(9): 1275—1281.
- [12] KIM N W, KIM T Y, CHOI J S. Edge-Based Spatial Descriptor for Content-based Image Retrieval[J]. Image and Video Retrieval, 2005, 3568(12): 454—464.
- [13] 汤武. 基于几何不变性鲁棒哈希的重复视频检测算法研究[D]. 广州: 华南理工大学, 2018.  
TANG Wu. Research on Repeated Video Detection Algorithm Based on Geometric Invariance Robust Hashing[D]. Guangzhou: South China University of Technology, 2018.
- [14] LI Bo, LIAO Xiao-feng, JIANG Yan. A Novel Image Encryption Scheme Based on Logistic Map and Dynamotic Modular Curve[J]. Multimedia Tools and Applications, 2018, 77(7): 8911—8938.
- [15] YE Qiao-lin, FU Li-yong, ZHANG Zhao. Lp- and Ls-Norm Distance Based Robust Linear Discriminant Analysis[J]. Neural Networks, 2018, 39(8): 1017—2028.
- [16] SCHAEFER G, STICH M. UCID-an Uncompressed Colour Image Database[M]. Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multi-media, 2004.
- [17] 王彦超. 基于联合特征与中心方向信息的图像哈希算法[J]. 西南大学学报(自然科学版), 2018, 40(2): 113—124.  
WANG Yan-chao. Image Hashing Algorithm Based on Joint Feature and Center Direction Information[J]. Journal of Southwestern University (Natural Science Edition), 2018, 40(2): 113—124.
- [18] 钟瑞泽. 基于多尺度特征变换与颜色相关性的商标检索算法[J]. 包装工程, 2018, 39(23): 200—209.  
ZHONG Rui-ze. Trademark Retrieval Algorithms Based on SIFT and Color Correlation[J]. Packaging Engineering, 2018, 39(23): 200—209.
- [19] 孙奇平. 融合多特征和哈希算法的图像检索研究[J]. 淮阴工学院学报(自然科学版), 2018, 27(1): 38—42.  
SUN Qi-ping. Research on Image Retrieval Based on Fusion of Multi-feature and Hash Algorithms[J]. Journal of Huaiyin Institute of Technology (Natural Science Edition), 2018, 27(1): 38—42.
- [20] ZHANG Xiao-fan, LIU Wei, DUNDAR M. Towards Large-Scale Histopathological Image Analysis: Hashing-Based Image Retrieval[J]. IEEE Transactions on Medical Imaging, 2015, 34(2): 496—506.