基于融合鲁棒特征与多维尺度变换的紧凑图像哈希算法

余震[1]，何留杰[1]，吴婷[2]
（1.黄河科技学院，郑州 450063；2.中原工学院，郑州 450007；3.郑州大学，郑州 450001）

摘要：目的 为了增强哈希序列对任意旋转角度的鲁棒性与识别能力，提出一种基于融合鲁棒特征与多维尺度变换的紧凑图像哈希算法。**方法** 首先，利用双线性插值来固定图像的哈希序列长度，获取规则尺寸的图像；借助高斯低通滤波对规则图像完成过滤操作，消除噪声污染和插值误差对哈希生成的影响；将滤波图像转换到 YCbCr 颜色空间，提取亮度 *Y* 分量，增强哈希对亮度调整的鲁棒性；利用极坐标变换 LPT 方法处理亮度 *Y* 分量，输出二次图像；引入 SVD 机制来分解二次图像，获取其抗旋转的鲁棒特征；同时，根据 Fourier 变换与残差机制，获取 *Y* 分量的局部显著特征；随后，将这 2 种特征组合，形成融合鲁棒特征，将其视为中间哈希序列；引入多维尺度变换，对中间哈希序列完成压缩，获取紧凑哈希；基于 Logistic 映射，完成紧凑哈希序列的加密，形成目标哈希；通过计算真实图像与待认证图像之间哈希序列对应的 Hamming 距离，根据预设阈值，完成图像识别。**结果** 测试数据表明，较已有的哈希方案而言，所提方案拥有更高的鲁棒性和更紧凑的哈希长度，呈现出更为理想的 ROC 曲线，在多种攻击下，其稳定的正确识别率保持在 96%以上。**结论** 所提哈希方案拥有良好的鲁棒性与敏感性，在包装图标检索、信息水印等行业具备较好的应用价值。

关键词：图像哈希；融合鲁棒特征；多维尺度变换；双线性插值；YCbCr 颜色空间；Fourier 变换；残差机制
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2019)01-0186-10
DOI：10.19554/j.cnki.1001-3563.2019.01.029

Compact Image Hash Algorithm Based on Fusion Robust Features and Multidimensional Scaling

YU Zhen[1], *HE Liu-jie*[1], *WU Ting*[2]
(1.Huanghe S & T University, Zhengzhou 450063, China; 2.Zhongyuan University of Technology, Zhengzhou 450007, China; 3.Zhengzhou University, Zhengzhou 450001, China)

ABSTRACT: The work aims to propose a compact image hash algorithm based on fusion robust features and multidimensional scaling transform, in order to enhance the robustness and recognition ability of hash sequences for arbitrary rotation angles. Firstly, bilinear interpolation was used to fix the hash sequence length of the image for obtaining images of regular size. The Gauss low-pass filtering was used to filter regular images to eliminate the influence of noise pollution and interpolation error on the hash generation. Then, the filtered image was transformed into YCbCr color space for extracting the brightness *Y* component, so as to enhance the hash robustness with brightness adjustment. Then, the log-polar transform LPT was used to process the brightness *Y* component for outputting the secondary image. The SVD mechanism was introduced to decompose the secondary image for obtaining the robust features of its anti-rotation. At the same time,

收稿日期：2018-08-28
基金项目：国家自然科学基金（61379079）；河南省国际科技合作基金（144300510007）；河南省产学研合作计划（152107000093）
作者简介：余震（1980—），男，硕士，黄河科技学院讲师，主要研究方向为图像信息处理、计算机算法。

the local salient features of the *Y* component were obtained based on Fourier transform and residual mechanism. Subsequently, the two features were combined to form a fusion robust feature, which was regarded as an intermediate hash sequence. The multidimensional scaling was introduced to compress the intermediate hash sequence for obtaining compact hash. The compact hash sequence was encrypted base on Logistic map to form the target hash. By calculating the Hamming distance of hash sequence between the real image and the image to be authenticated, the image recognition was determined according to the preset threshold. Experimental results showed that, the proposed algorithm had stronger robustness and more compact hash length, as well as more ideal ROC curve, compared with the existing hash scheme, and its correct recognition rate of stability was over 96% under a variety of attacks. Featured by good robustness and sensitivity, the proposed hash scheme has better application value in packaging icon retrieval, information watermarking and other industries.

KEY WORDS: image hashing; fusion robust features; multidimensional scaling; bilinear interpolation; YCbCr color space; Fourier transform; residual mechanism

随着数字信号处理的发展，多媒体内容的可靠性和可信度已成为人们普遍关注的问题，而图像作为多媒体技术中常用的介质，因其具有理想的直观表达能力，在众多领域得到了广泛引用[1]。近年来，随着图像编辑软件的迅速普及，极大地提高了数字图像真实性的风险，攻击者可以随意使用这些编辑软件对图像完成修改，而且不留篡改痕迹，导致人眼难以对其内容的真假进行识别，对图像内容造成了威胁[2]。对此，诞生了图像认证方案，图像哈希算法作为有效的决策介质，它是从短的二进制或实数序列来提取图像特征，是一种基于图像视觉内容的压缩表达，可作为图像的唯一表示方式而用于其信息的真伪决策，该技术对其内容具有强烈的敏感性，当图像内容发生极其微小变化，所产生的哈希值与初始图像存在巨大差异[3]。目前，哈希技术已经在商标检索、版权保护等领域得到了广泛应用，例如，为了快速地从大型数据库中准确检索到相似商标，可以利用哈希算法生成商标图像对应的低维哈希矩阵，然后根据初始商标图像与数据库中商标对应的哈希矩阵，计算二者之间的 Hamming 距离，以此来输出检索商标[4]。在版权保护领域中，图像哈希是鲁棒水印方法的重要过程，利用哈希算法生成宿主图像的哈希序列，将其与待嵌入水印进行异或运算，可以生成检测水印的密钥，从而增强水印系统的安全性[5]。

一般而言，图像哈希序列的生成主要分为图像预处理、特征提取与哈希序列的生成 3 个过程，其中，特征检测是其关键内容，其鲁棒性的高低对整个哈希算法具有重要影响[3]。如 Qin 等[6]为了实现对图像内容的快速认证，提出了基于显著结构特征的图像哈希算法，通过对图像完成预处理，固定哈希序列的长度，并提取滤波图像的边缘特征，并从中选择出包含结构信息最多的子块作为样本，并利用 DCT（Discreet Cosine Transform）机制对其完成分解，并联合 PCA（Principal Component Analysis）来生成对应的哈希序列，测试数据表明该方案对诸如尺度缩放、噪声干扰等常规的内容保留操作具有理想的鲁棒性。但是，此技术仅利用了图像的边缘特征，对旋转攻击的鲁棒性较弱，导致其认证准确度较低。Tang 等[7]为了增强哈希序列的鲁棒性，提出了基于张量分解的紧凑图像哈希算法，利用插值运算与低通滤波来完成图像的预处理，并将滤波图像的 L 分量分割为一系列的子块，再组合每个子块的灰度均值，形成特征矩阵，以此构造张量，通过对该特征矩阵完成三阶张量分解，形成哈希序列。该技术只是选择尺寸较小的子块（2×2）来构建特征矩阵，且张量分解难以有效充分获取 L 分量的抗旋转鲁棒特征，使其对角度旋转的正确识别率不高。Pun 等[8]为了改善哈希算法的感知鲁棒性，提出了基于渐进特征选择的鲁棒哈希算法，联合 SIFT 算子与特征匹配方法，构建渐进特征选择机制，从图像中提取高鲁棒的特征点，同时，使用特征点描述符来提取图像的局部特征与颜色特征，将三者进行组合，构成了复合特征，通过对其完成量化，输出哈希序列。实验结果表明该方案对于任意角度旋转、噪声污染等篡改操作具有良好的鲁棒性与识别能力。SIFT 算子容易检测到图像中较多的伪特征点，限制了其鲁棒性，而且对亮度调整等攻击的识别准确度较低。

为了提高哈希生成效率与对任意角度旋转攻击的鲁棒性，文中提出基于融合鲁棒特征与多维尺度变换的紧凑图像哈希算法。利用双线性插值与高斯低通滤波作为预处理机制，对于任意尺寸的图像，可固定其哈希长度；将预处理图像的 RGB 空间转换到 YCbCr 颜色空间，利用其亮度 Y 分量来生成哈希，可以增强哈希对亮度调整的鲁棒性；通过联合 LPT 方法与 SVD 机制，提取抗旋转的鲁棒特征；基于 Fourier 变换与残差机制，获取 Y 分量的局部显著特征；通过组合这些特征，形成中间哈希序列；为了压缩哈希长度，提高效率，利用多维尺度变换，对中间哈希序列完成压缩，并利用 Logistic 映射对压缩后的哈希序列实施加密，形成目标哈希；通过计算真实图像与待

认证图像之间哈希序列对应的 Hamming 距离来实现对图像判别；最后测试所提哈希算法的鲁棒性与识别精度。

1　所提紧凑哈希算法

所提的基于融合鲁棒特征与多维尺度变换的紧凑图像哈希算法过程见图 1。根据图 1 可发现，整个哈希的生成有 4 个阶段：初始图像的预处理；图像的鲁棒特征提取；基于多维尺度变换的哈希序列压缩；哈希序列的生成及图像认证。

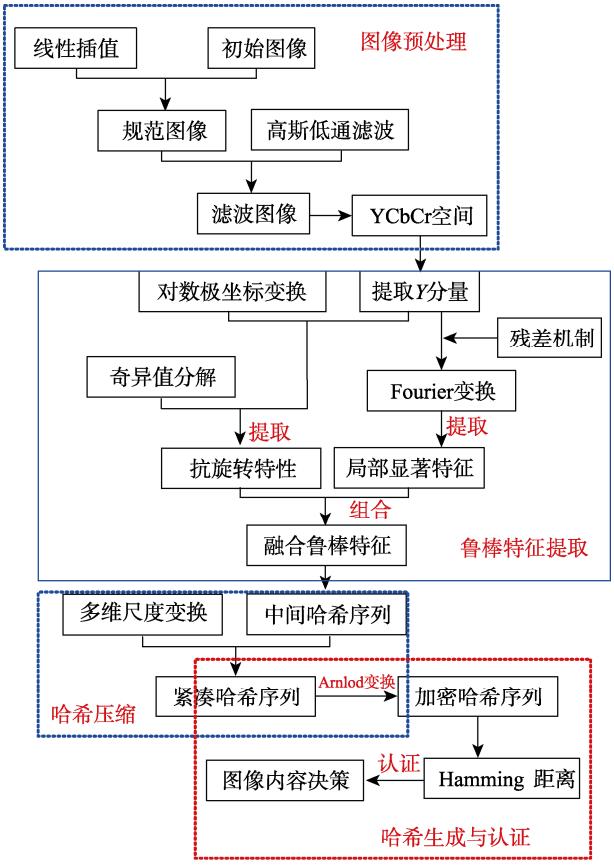


图 1　所提哈希算法的生成过程

Fig.1 Generation process of the proposed hash algorithm

1.1　初始图像的预处理

图像预处理是哈希生成的不可或缺的过程，可以有效改善哈希机制对缩放与噪声等常规内容保留操作的鲁棒性[1]。首先，利用双线性插值运算[9]来规范初始图像的尺寸，确保对于不同尺寸的待认证图像时，均可产生一个固定长度的哈希序列。然后，利用带卷积掩模的高斯低通滤波[1]来过滤规范图像，消除噪声污染和插值误差对哈希序列的影响。对于（x,y）处的高斯低通滤波，其卷积掩码的元素计算函数为[1]：

$$\begin{cases} G(i,j)=\dfrac{g(i,j)}{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N}g(i,j)} \\ g(i,j)=e^{\dfrac{-\left(i^2+j^2\right)}{2\sigma^2}} \end{cases} \tag{1}$$

式中：σ 为卷积掩码中所有元素的标准偏差。

由于规范图像的尺寸对整个哈希序列的长度影响较大。一般而言，规范化图像的尺寸越小，则哈希序列长度也就越短，反之，则哈希序列长度更大。若规范图像的尺寸过小，会丧失图像的部分主要特征信息，反而会影响鲁棒特征的提取，因此，对于规范化图像的尺寸，需要兼顾图像质量与哈希长度。为此，在文中算法中，其规范化原则：规范化图像的信息熵不能低于 7.63；或者峰值信噪比不能低于 40 dB。

为了提高哈希算法对亮度修改的鲁棒性，将滤波图像转换到 YCbCr 空间，并提取相应的 Y 分量来描述图像，因为 Y 分量包含了图像的大部分几何与视觉上的重要信息[10]：

$$\begin{bmatrix} Y \\ C_{\mathrm{b}} \\ C_{\mathrm{r}} \end{bmatrix}=\begin{bmatrix} 65.481 & 128.553 & 24.996 \\ -37.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix}\begin{bmatrix} R \\ G \\ B_{\mathrm{r}} \end{bmatrix}+\begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \tag{2}$$

式中：R, G, B_{r} 为预处理图像的红、绿、蓝分量；Y, C_{b}, C_{r} 分别为图像的亮度、蓝色与红色浓度偏移量[2]。

上述任意图像的预处理过程见图 2。其中，图 2a 是不规则图像，其尺寸为 $M\times N$（$M\neq N$）；图 2b 是经过插值操作后的规范图像，其尺寸为 $m\times m$。利用高斯滤波处理图 1b 后，形成的滤波图像见图 2c；经过式（2）计算后，提取的 Y 分量见图 2d。

a 初始图像　　b 规范图像

c 滤波图像　　d 亮度 Y 分量

图 2　图像的预处理过程

Fig.2 Image preprocessing

1.2　图像的鲁棒特征提取

1.2.1　二次图像的形成

根据上述过程提取的 Y 分量虽然对于常规的噪声与亮度修改等具有较高的鲁棒性，但是，抗旋转攻击性能较弱。对此，文中引入极坐标变换[11]LPT 来处理 Y 分量。LPT 是一种将图像从笛卡尔空间转换为对数极坐标的常用方法[11]。令（x_0,y_0），（x,y）分别是 Y 分量的中心坐标、笛卡尔空间内给定像素的坐标。显然，对于尺寸为 $m\times m$ 的 Y 分量，有 $1\leqslant x\leqslant m$，$1\leqslant y\leqslant m$。假设（ρ,θ）是像素（x,y）的对数极坐标，其中 ρ 为从像素到图像中心的距离，θ 为 x 轴与通过 Y 分量中心和像素（x,y）的直线之间的角度，则 ρ 与 θ 的计算函数为：

$$\begin{cases} x = \mathrm{e}^{\rho}\cos\theta \\ y = \mathrm{e}^{\rho}\sin\theta \end{cases} \tag{3}$$

$$\rho = \ln\sqrt{(x-x_0)^2+(y-y_0)^2} \tag{4}$$

$$\theta = \arctan\frac{y-y_0}{x-x_0} \tag{5}$$

由式（5）发现，极坐标变换考虑了旋转角度 θ，使其对任意角度的旋转攻击具有较强的鲁棒性。在笛卡尔空间内的旋转修改，可视为对数极坐标内的水平、垂直方向上的平移操作[10]，见图 3。Y 分量经过 LPT 处理后，其对应的结果为：

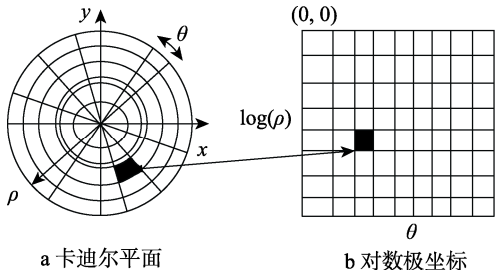
$$f_1(\rho,\theta) = f_0\left[\rho,(\theta+\theta_0)\right] \tag{6}$$

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

Y 分量的 LPT 变换过程见图 4。其中，图 4a，b 分别是初始的 Y 分量和经过旋转 90°后的图像。二者经过 LPT 变换后，结果分别见图 4c，d。通过对比图 4c 与图 3d 可发现，虽然 Y 分量经过 90°攻击，但其 LPT 变换结果中，只有 x 轴方向存在周期性变动，其他位置的信息保持变。

1.2.2　融合鲁棒特征的提取

虽然 LPT 变换对任意角度旋转具有理想的鲁棒性，但是通过对比图 3c 与图 3d 可知，Y 分量经过旋转后，其图像列之间产生了圆形移位，这些位置的特



a 卡迪尔平面　　b 对数极坐标

图 3　卡迪尔坐标变换成极坐标的过程
Fig.3 Process of transforming Cartier coordinates into polar coordinates

a 初始 Y 分量　　b 90°旋转后的 Y 分量

c Y 分量的 LPT 结果　　d 旋转 Y 分量的 LPT 结果

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

征不稳定。为此，文中引入奇异值分解[12]SVD，根据其较好的稳定性来处理二次图像，充分提取整个二次图像中的抗旋转特征。若二次图像为 X，根据 SVD 方法，可得[12]：

$$X = \boldsymbol{S}\cdot\boldsymbol{V}\cdot\boldsymbol{D} \tag{7}$$

式中：$\boldsymbol{S}$，$\boldsymbol{D}$ 分别为二次图像的正交矩阵；$\boldsymbol{V}$ 为二次图像的对角矩阵，其含有 m 个奇异值。

通过式（7）处理二次图像，可以获取一个 $m\times m$ 维对角矩阵 $\boldsymbol{V}$；并将 $\boldsymbol{V}$ 中的奇异值组合为矢量 $\boldsymbol{\beta}=\{\beta_1,\beta_2\ldots\beta_m\}$。可见，矢量 $\boldsymbol{\beta}=\{\beta_1,\beta_2\ldots\beta_m\}$是在 LPT 变换与 SVD 基础上形成的，不仅保持了 SVD 的稳定性，而且继承了 LPT 的抗任意角度旋转的特性。

显著性特征对于图像内容的真伪决策具有重要作用。为此，文中联合残差方法与 Fourier 变换来充分获取 Y 分量的显著特征。若 Y 分量为 f（x,y），大小为 $m\times m$，则对应的 Fourier 变换为[13]：

$$f(x_0,y_0) = F^{\alpha}\left[f(x,y)\right](x_0,y_0) = \int_{-\infty}^{+\infty} f(x,y)K_{\alpha}(x,y;x_0,y_0)\mathrm{d}x\mathrm{d}y \tag{8}$$

式中：K_{α} 为变换核；（x,y），（x_0,y_0）分别为输入、输出坐标；a 为 Fourier 变换的阶数。

根据式（8），可形成 Y 分量的 Fourier 频谱，从而得到相应的幅度 $B(f)=\left|f(x_0,y_0)\right|$。

随后，利用 B（f）来估计相应的对数谱 L（f）：

$$L(f) = \log\left(B(f)\right) \tag{9}$$

通过式（9）输出的 L（f），可得到 Y 分量的平均谱 E（f）：

$$\begin{cases} E(f) = \boldsymbol{g}_q(f) * L(f) \\ \boldsymbol{g}_q(f) = \dfrac{1}{q}\begin{bmatrix} 1\cdots\cdots 1 \\ \vdots\ \ddots\ \vdots \\ 1\cdots\cdots 1 \end{bmatrix} \end{cases} \tag{10}$$

式中：*为卷积运算；$\boldsymbol{g}_q$（f）为经过局部滤波[14]处理 Y 分量后所输出的 $q\times q$ 维矩阵。

利用 $L(f)$ 和 $B(f)$ 来获取 Y 分量的频谱残差 $R(f)$：

$$R(f)=L(f)-E(f) \tag{11}$$

通过可逆 Fourier 变换处理 $R(f)$ 与相位频谱 $P(f)=\arg\left|I(x_0,y_0)\right|$，可形成 Y 分量的显著映射：

$$S(f)=F^{-1}\left[\exp\left(R(f)+P(f)\right)\right]^2 \tag{12}$$

最后，基于阈值分割[15]，得到 $S(f)$ 的显著区域；利用与 LBP 机制[16]，从区域中获取局部特征 $\boldsymbol{s}=\{s_1, s_2\ldots s_m\}$。通过将 $\boldsymbol{\beta}=\{\beta_1, \beta_2\ldots\beta_m\}$ 与 $\boldsymbol{s}=\{s_1, s_2\ldots s_m\}$ 进行组合，形成融合鲁棒特征，将其视为中间哈希序列 $\boldsymbol{h}=(\boldsymbol{\beta}, \boldsymbol{s})$。为了便于后续描述，将中间哈希序列 $\boldsymbol{h}=(\boldsymbol{\beta}, \boldsymbol{s})$ 记为 $\boldsymbol{h}=\{h_1, h_2\ldots h_{2m}\}$。

1.3 基于多维尺度变换的哈希序列压缩

直接从图像中提取的哈希序列维度较高，易增大算法的复杂度。为此，文中引入多维尺度变换[17]MS（Multidimensional scaling），对 $\boldsymbol{h}=(\boldsymbol{\beta}, \boldsymbol{s})$ 完成压缩。经典的 MS 方法是一种有效的数据压缩技术，主要有 3 个过程[17]。

1）距离矩阵 $\boldsymbol{D}$ 的构建。对于序列 $\boldsymbol{h}=\{h_1, h_2\ldots h_{2m}\}$，计算 2 个元素 h_i 与 h_j 之间的欧式距离 $d_{i,j}$，从而得到距离矩阵 $\boldsymbol{D}$：

$$\boldsymbol{D}=\begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,2m} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,2m} \\ \vdots & \vdots & \vdots & \vdots \\ d_{2m,1} & d_{2m,2} & \cdots & d_{2m,2m} \end{bmatrix} \tag{13}$$

2）内积矩阵 $\boldsymbol{B}$ 的计算。根据距离矩阵 $\boldsymbol{D}$，按照如下函数，对其完成内积运算：

$$\begin{cases} \boldsymbol{B}=\dfrac{1}{2}\boldsymbol{JDJ} \\ \boldsymbol{J}=\boldsymbol{E}-\dfrac{1}{2m}\boldsymbol{ee}^{\mathrm{T}} \end{cases} \tag{14}$$

式中：$\boldsymbol{J}$ 为集中矩阵；$\boldsymbol{E}$ 为 $2m\times 2m$ 维的单位矩阵；$\boldsymbol{e}$ 为 $2m\times 1$ 维的单位矢量。

3）低维表示 $\boldsymbol{G}$ 计算。由于内积矩阵 $\boldsymbol{B}$ 是对称半正定矩阵，因此将其变换为：

$$\boldsymbol{B}=\boldsymbol{SVS}^{\mathrm{T}} \tag{15}$$

式中：$\boldsymbol{V}$ 为 $\boldsymbol{B}$ 的对角矩阵；$\boldsymbol{S}$ 为 $\boldsymbol{B}$ 对应的特征向量所构成的矩阵。

由此，低维表示 $\boldsymbol{G}$ 可以从矩阵 $\boldsymbol{z}$ 中前 $d(d<2m)$ 列元素来生成：

$$\boldsymbol{Z}=\boldsymbol{SV}^{1/2} \tag{17}$$

为了压缩低维矩阵 $\boldsymbol{G}$，文中首先计算矩阵 $\boldsymbol{G}$ 中每一行元素的方差，并使用这些统计特征来表示。令 $\boldsymbol{G}=\{g_1, g_2\ldots g_{2m}\}^{\mathrm{T}}$，且 $g_i(j)$ 是矢量 $\boldsymbol{g}_i$（$1\leqslant i\leqslant 2m$）中的第 j（$1\leqslant j\leqslant d$）个元素。则 $\boldsymbol{g}_i$（$1\leqslant i\leqslant 2m$）的方差 σ 为：

$$\begin{cases} \sigma=\dfrac{1}{d-1}\sum\limits_{j=1}^{d}\left[g_i(j)-u\right]^2 \\ u=\dfrac{1}{d}\sum\limits_{j=1}^{d}g_i(j) \end{cases} \tag{18}$$

由于方差可以有效地测量矢量元素的波动，因此文中将式（18）得到的方差 σ 视为描述低维向量的特征。随后，为了缩小哈希的存储空间，借助一维 DWT 处理方差矢量 $\boldsymbol{p}=\left\{\sigma_{g_1}, \sigma_{g_2}\cdots\sigma_{g_{2m}}\right\}$，从而得到了相应的 DWT 系数矩阵 $\boldsymbol{q}=[q_1, q_2\ldots q_m]^{\mathrm{T}}$。其中，$q_i$（$1\leqslant i\leqslant m$）是 DWT 变换的近似系数。可见，经过 DWT 处理后，统计特征的维度降低至原来的一半左右，从而有助于获得一个紧凑哈希。随后，根据如下函数，对系数 q_i 实施量化：

$$h'(i)=\mathrm{Round}(q_i) \tag{19}$$

利用式（19）量化所有的系数 q_i 后，可输出紧凑哈希 $\boldsymbol{h'}=\left\{h'(1), h'(2), h'(3)\cdots h'(m)\right\}$。

1.4 哈希序列的加密及图像认证

为了提高哈希序列的防碰撞性，文中利用 Logistics 映射对 $\boldsymbol{h'}=\left\{h'(1), h'(2), h'(3)\cdots h'(m)\right\}$ 实施加密。首先，根据 Y 分量的像素总和来计算 Logistics 映射[18]的初值 x_0：

$$x_0=n/10^6 \tag{20}$$

式中：n 为 Y 分量图像的像素总和。

并设置 μ，对 Logistics 映射迭代 m 次，输出随机序列 $\{x_1, x_2\ldots x_m\}$：

$$x_{k+1}=\mu x_k(1-x_k) \tag{21}$$

随后，利用如下函数对 $\{x_1, x_2\ldots x_m\}$ 实施量化，产生一组密钥流 $\{k_i\}$：

$$k_i=\mathrm{mod}\left(floor\left(x_i\times 10^{14}\right), 256\right) \tag{22}$$

再根据 $\{k_i\}$，对哈希 $\boldsymbol{h'}=\left\{h'(1), h'(2), h'(3)\cdots h'(m)\right\}$ 完成加密：

$$H(i)=h'(i)\oplus k_i \tag{23}$$

式中：$H(i)$ 为加密后的哈希元素。

利用式（23）加密所有的哈希元素 h'_i，最终可获取目标哈希序列 $\boldsymbol{H}=\left\{H(1), H(2)\cdots H(m)\right\}$。随后，基于 Hamming 距离[19]，对可疑图像进行认证。令真实图像的哈希序列 $\boldsymbol{H}_0=\left\{H_0(1), H_0(2)\cdots H_0(m)\right\}$；可疑图像的哈希序列为 $\boldsymbol{H}_1=\left\{H_1(1), H_1(2)\cdots H_1(m)\right\}$。二者之间的 Hamming 距离 $D(H_0, H_1)$ 为[19]：

$$D(H_0, H_1)=\frac{1}{L-1}\sum_{i=1}^{L-1}\left(H_0(i)\oplus H_1(i)\right) \tag{24}$$

式中：L 为哈希序列的长度；$\oplus$ 为异或运算。

再根据预设阈值 T，若 $\rho(H_0, H_1)\geqslant T$，则可

将这 2 幅图像视为相似图像；否则，其为差异图像。

2　实验结果与分析

为了验证文中哈希算法的鲁棒性，从 UCID 图像库[20]中任意挑选 4 幅图像来完成实验。另外，为了突出所提哈希方案的优势，将鲁棒性较好的哈希机制作为对照组：文献[7]、文献[8]。在整个哈希算法过程中，预设阈值 T 对其识别准确率具有重要影响，为此，首先需对 T 完成优化，确定最佳值。剩余测试参数值见表 1。

表 1　实验参数设置

Tab.1 Setting of experimental parameters

哈希生成阶段	参数名称	参数值
预处理	初始图像尺寸 $M\times N$	512×1024
	规范图像尺寸 $m\times m$	360×360
	标准偏差 σ	1
	高斯滤波器尺寸	3×3
特征提取	Fourier 变换阶数 a	2
	LBP 算子的半径	1
	领域的像素个数	8
哈希压缩	d	40
	哈希长度	360
哈希认证	混沌参数 μ	3.2

2.1　最佳阈值 T 的确定

首先，从 UCID 图像库[20]挑选 50 幅目标图像，借助 StirMark 4.0[21]平台生成 3850 对感知相似图像；另外，再从 UCID 库中挑选 100 幅不同的图像，形成 7300 对差异图像。然后，按照表 2 的内容攻击类型，对这些图像完成相应的修改。最后，统计初始图像与内容修改图像之间的 Hamming 距离。根据频数变化强烈程度，确定合适的阈值。

表 2　不同攻击类型及其参数

Tab.2 Different attack types and parameters

操作类型	参数
椒盐噪声	0.02, 0.04, 0.06, 0.08
亮度调整	1, 1.5, 2, 2.4
旋转	30°, 60°, 90°, 100°
缩放	0.5, 0.8, 1, 1.5

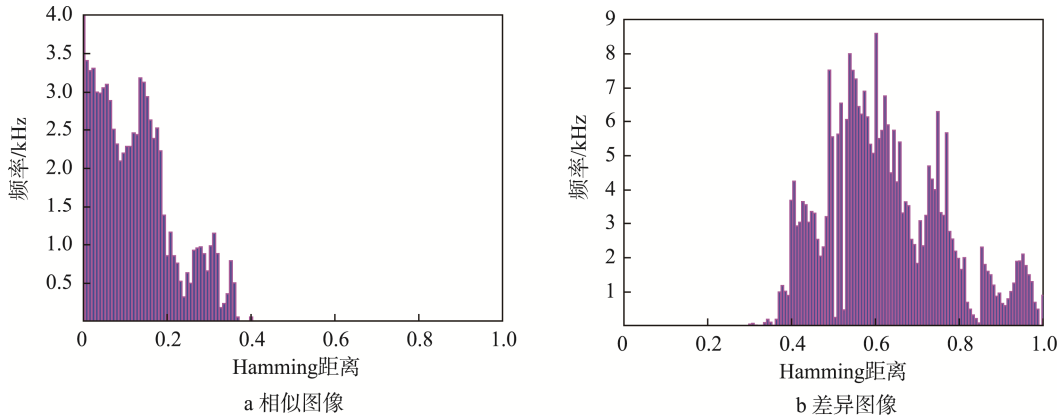
统计相应的初始图像与内容修改图像之间的 Hamming 距离分布情况见图 5。根据图 5a 发现，利用表 1 的攻击类型来修改感知相似图像对时，当 $D<0.34$ 时，对应的频数变化较为强烈；通过观察图 5b 发现，面对这些差异图像，在 $D>0.36$ 时，频数变化较大。为此，文中将预设阈值 T 取为 0.34。

2.2　鲁棒性测试

鲁棒性是衡量哈希算法的重要指标[2]，为此，以图 6a—d 为测试样本，并把表 2 中的 4 种篡改类型来修改样本；再利用文中方案的哈希过程，根据式（24）计算修改前后样本对应的 Hamming 距离，结果见图 6e—h。根据输出数据发现，对于表 1 中的任意修改类型，其对应的 Hamming 距离均低于 0.34。这显示文中哈希方案对表 1 中的所有攻击类型拥有理想的识别正确度。原因是所提哈希方案对初始图像实施了预处理，使其对常规的噪声、缩放和亮度具有较强的鲁棒性；利用 LPT 与 SVD 机制，充分提取其抗旋转的鲁棒特征，同时联合 Fourier 变换与来 DWT 方法来检测其局部显著特征，使得所提算法产生的哈希序列拥有优异的感知鲁棒性。

2.3　敏感性测试

敏感性是评估哈希算法的常用指标，当图像遭遇某种类型的篡改时，其产生的哈希序列与真实图像截然不同[3]。为此，以图 7a 为目标，对其进行 4 种不同类型的内容修改，见图 7b—e；再利用所提方案的



a 相似图像　　b 差异图像

图 5　预设阈值的优化

Fig.5 Optimization of preset threshold

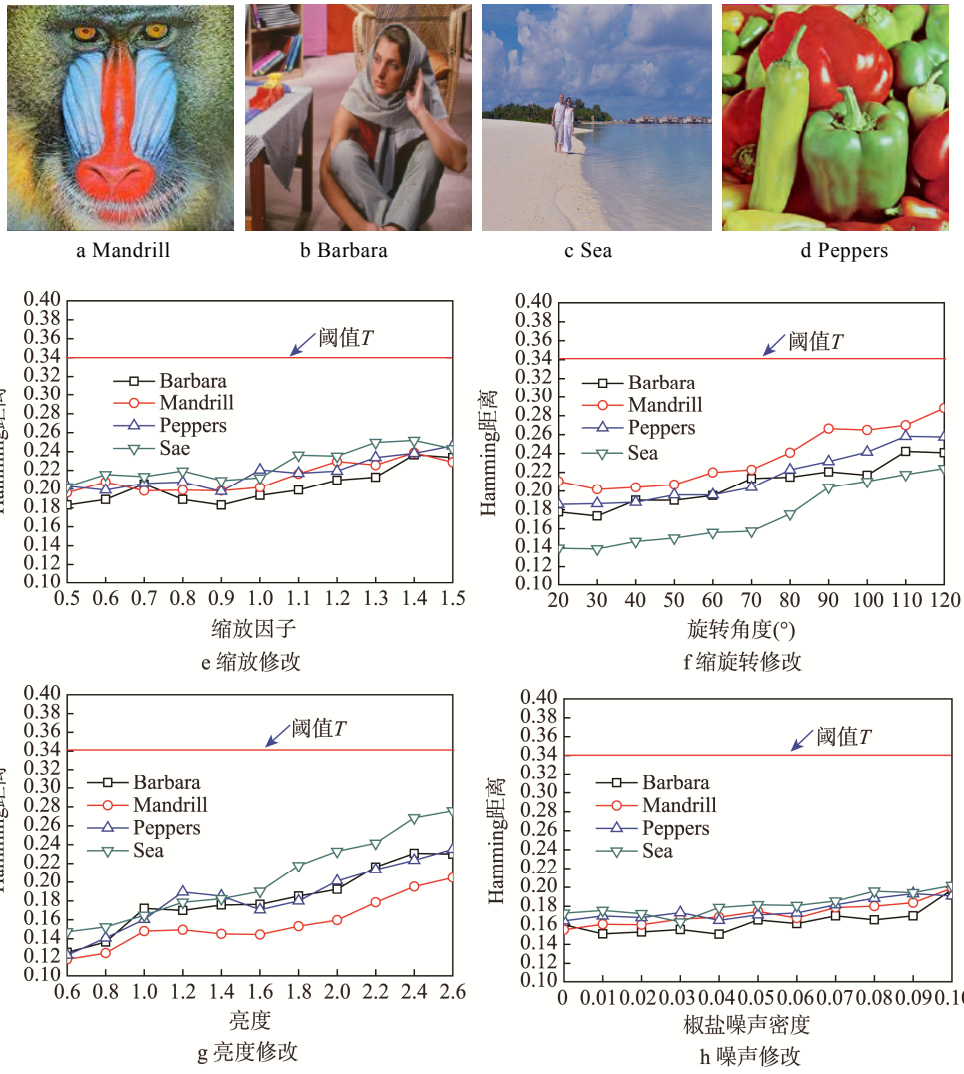


图 6　所提哈希算法的鲁棒性测试

Fig.6 Robustness test of the proposed hash algorithm

图 7　不同内容修改后的图像

Fig.7 Images with different contents modified

哈希生成过程，根据式（24）获取二者的 Hamming 距离，结果见表 3。通过测试数据发现，所提哈希方案能够准确对各种图像完成准确识别，当图像遇到复制，以及组合篡改手段时，二者对应的 Hamming 距离均显著大于 0.34。当图像遇到噪声修改时，其 Hamming 距离要小于 0.34。这表明了所提哈希方案满足严格的敏感性，能够对各类攻击做出准确的判别。主要是因为所提方案通过提取图像的抗旋转特征与局部显著特征来生成哈希，当图像遇到攻击时，其特征描述就会发生明显的变化，导致提取的鲁棒特征存在较大差异。

2.4　不同算法的鲁棒性测试

为了突出文中哈希方案的优异性，测试了所提算法、文献[7]与文献[8]的 ROC 曲线。ROC 曲线[1]由正确识别率 P_{TPR}、虚警率 P_{TPR} 组成，其计算函数为：

表 3　内容修改前后图像之间的 Hamming 距离

Tab.3 Hamming distance between images before and after content modification

图像	汉明距离
图 7b	0.479
图 7c	0.653
图 7d	0.614
图 7e	0.226

$$P_{\mathrm{TPR}}=\frac{n_1}{M_1},\ P_{\mathrm{FPR}}=\frac{n_2}{M_2} \tag{25}$$

式中：n_1 为正确决策的图像数量；n_2 为误判的图像数量；M_1，M_2 分别为完好图像与可疑图像的总和[1]。

2 种不同哈希算法的 ROC 曲线见图 8。由图 8 可发现，3 种算法对缩放、噪声修改都拥有理想的鲁棒性，呈现出良好的 ROC 特性曲线，见图 8a—b。然而，对于亮度与旋转修改，3 种算法表现出不同的特征。对于文献[8]，其对亮度修改的鲁棒性不佳，但是对旋转具有良好的识别准确率，见图 8c 和图 8d。文献[7]则对于亮度调整具有理想的鲁棒性，但是对于旋转修改的识别准确率不理想。对于旋转修改，当 P_{TPR}=0 时，文献[7]、文献[8]与所提方案的 P_{TPR} 分别为 0.763，921，0.943；P_{TPR}=0.3 时，三者的 P_{TPR} 分别达到 0.958，0.986，0.992。对于亮度修改，当 P_{TPR}=0，P_{TPR}=0.3 时，文中哈希技术的 P_{TPR}=0.946，P_{TPR}=0.995；当 P_{TPR}=0 时，文献[7]、文献[8]的 P_{TPR} 分别为 0.923，0.845。在 P_{TPR}=0.3 时，二者的 P_{TPR} 分别为 0.983，0.974。原因是文献[7]与文献[8]均采用了线性插值与滤波的预处理方法，消除了缩放与噪声对哈希生成的影响。文献[7]是将图像转换到 Lab 空间后，利用张量分解来提取亮度 L 分量的特征，而张量分解具有一定的稳定性，因此，其对亮度修改具有较好的鲁棒性，但是其只采用了 L 分量的全局特征，使其对图像的描述能力不足，导致其对角度旋转的稳定性有待进一步提升。文献[8]则是主要是通过 SIFT 算子与特征匹配方法，从图像中提取鲁棒性较高的特征点，而且使用了特征点描述符来提取图像的局部特征与颜色特征，将这种复合特征视为哈希，相对于文献[7]而言，其提取的鲁棒特征更加充分，使其对于任意角度的旋转都具有较高的鲁棒性。此哈希序列是在图像的 RGB 颜色空间内生成的，对于亮度修改，表现的 ROC 特性曲线不理想。所提哈希方案除了与文献[7]、文献[8]采用了相同的预处理方法之外，其哈希生成是在 YCbCr 空间内，利用抗旋转的 LPT 机制与较为稳定的奇异值分解来充分获取亮度 Y 分量的鲁棒特征，而且还根据 Fourier 变换与残差机制来获取 Y 分量的局部显著特征，使其对 Y 分量特征的描述较为充分，提高了所提哈希算法对任意角度旋转与亮度修改的鲁棒性。

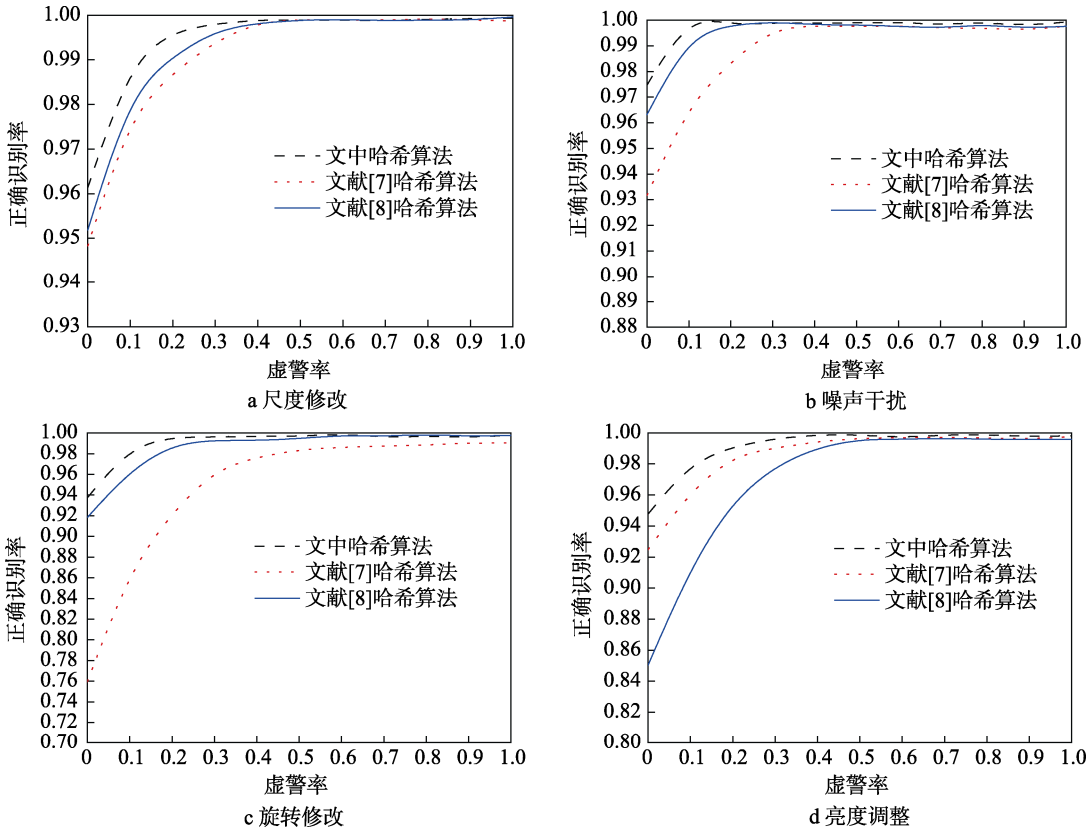


图 8　3 种算法的鲁棒性测试

Fig.8 Robustness test of three algorithms

2.5 哈希生成效率测试

为了客观评估 3 种方案输出的哈希序列长短以及效率，借助 Matlab 软件，在测试条件为 DELL 3.5 Hz，8 GB 内存的工作机上完成验证，数据见表 4。根据表 4 可发现，所提方案因采用了多维尺度变换与 DCT 机制，对提取的融合鲁棒特征完成了压缩，显著降低了哈希的维度，其哈希长度较为紧凑，为 360 位，所用时间为 0.27 s；文献[7]只提取了图像的全局特征，并利用张量分解来获取相应的哈希序列，使其哈希长度最短，约为 255 位，时耗为 0.18 s；文献[8]充分利用了提取了图像 SIFT 特征、局部特征与颜色特征，虽然增强了鲁棒性，但是缺乏数据压缩过程，使其维度最高，约 960 位，时耗为 0.51 s。

表 4 哈希长度和生成效率

Tab.4 Hash length and generation efficiency

算法	哈希长度/bits	哈希生成时耗/s	识别噪声篡改	识别旋转篡改	识别亮度调整篡改	识别 JPEG 压缩篡改	识别伽马校正篡改	识别缩放篡改
文中	360	0.27	YES	YES	YES	YES	YES	YES
文献[7]	255	0.18	YES	NO	YES	NO	NO	YES
文献[8]	960	0.51	YES	YES	NO	YES	YES	YES

3 结语

为了获取紧凑哈希，兼顾其对旋转篡改的鲁棒性，文中提出了基于融合鲁棒特征和多维尺度变换的紧凑图像哈希算法。利用 LPT 方法对图像的亮度 Y 分量进行变换，获取抗旋转修改的二次图像；根据 SVD 来提取二次图像的鲁棒特征；通过联合 Fourier 变换与残差机制，提取 Y 分量的局部显著特征；将二者视为中间哈希序列；利用多维尺度变换对中间哈希序列完成压缩，降低哈希维度，提高生成效率；为了提高哈希序列的安全性，文中利用 Logistic 映射来对其加密。测试数据显示了所提哈希方案对于常规的数字修改与恶意篡改均具有较好的鲁棒性，所生成的哈希序列较为紧凑，对于尺寸为 512×1024 的图像，其时耗仅为 0.27 s。

参考文献：

[1] 金晓民, 张丽萍. 混合特征与颜色矢量角度的图像哈希认证算法[J]. 计算机科学与探索, 2018, 38(7): 1102—1115.
JIN Xiao-min, ZHANG Li-ping. Image Hashi Authentication Algorithm Based on Mixed Feature and Color Vector Angle[J]. Computer Science and Exploration, 2018, 38(7): 1102—1115.

[2] 王彦超. 基于压缩量化与邻域空间 LBP 算子的图像哈希算法[J]. 包装工程, 2017, 38(21): 191—198.
WANG Yan-chao. Image Hashing Algorithm Based on Compressed Quantization and Neighborhood Space LBP Operator[J]. Packaging Engineering, 2017, 38(21): 191—198.

[3] 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 Bnary Mode[J]. Progress in laser and Optoelectronics, 2017, 54(2): 4—16.

[4] 苏毅娟, 余浩, 雷聪. 基于 PCA 的哈希图像检索算法[J]. 计算机应用研究, 2017, 35(11): 1011—1017.
SU Yi-juan, YU Hao, LEI Cong. Hash Image Retrieval Algorithm Based on PCA[J]. Computer Application Research, 2017, 35(11): 1011—1017.

[5] 余波. 基于 DWT-PCA 和感知哈希的鲁棒零水印算法[J]. 电视技术, 2016, 40(1): 25—30.
YU Bo. Robust Zero Watermarking Algorithm Based on DWT-PCA and Perceptual Hash[J]. Video Engineering, 2016, 40(1): 25—30

[6] QIN Chuan, CHEN Xue-qin, DONG Jing. Perceptual Image Hashing With Selective Sampling for Salient Structure Features[J]. Displays, 2016, 45(9): 26—37.

[7] TANG Zhen-jun, CHEN Lv, ZHANG Xian-quan. Robust Image Hashing with Tensor Decomposition[J]. IEEE Transactions on Knowledge & Data Engineering, 2018, 121(99): 1—12.

[8] PUN C M, YAN Cai-ping, YUAN Xiao-chen. Robust Image Hashing Using Progressive Feature Selection for Tampering Detection[J]. Multimedia Tools & Applications, 2018, 77(10): 11609—11633.

[9] 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 Hashi Authentication Algorithm Based on Negative Matrix Factorization Coupled with Ring Division [J]. Computer Engineering and Design, 2018, 38(9): 2464—2471.

[10] 方旺盛, 李玉南, 张蓉. 一种视觉模型引导的小波域彩色图像盲水印算法[J]. 计算机应用研究, 2011, 28(7): 2719—2722.
FANG Wang-sheng, LI Yu-nan, ZHANG Rong. A Vis-

ual Model Guided Color Image Blind Watermarking Algorithm in Wavelet Domain[J]. Computer Application Research, 2011, 28(7): 2719—2722.

[11] NIRMAL S, ALOKA S. Optics Based Bbiometric Encryption Using Log Polar Transform[J]. Optics Communications, 2010, 28(7): 34—43

[12] QIN Chuan, SUN Mei-hui, CHANG Chin-chen. Perceptual Hashing for Color Images Based on Hybrid Extraction of Structural Features[J]. Signal Processing, 2018, 142(7): 194—205.

[13] ZHAO Meng-dan, GAO Xu-zhen, PAN Yue. Image Encryption Based on Fractal-Structured Phase Mask in Fractional Fourier Transform Domain[J]. Journal of Optics, 2018, 20(4): 1—12.

[14] 赵爱罡, 王宏力, 杨小冈. 基于非线性局部滤波的红外小目标检测方法[J]. 工程科学学报, 2016, 38(11): 1652—1658.
ZHAO Ai-gang, WANG Hong-li, YANG Xiao-gang. Infrared Small Target Detection Method Based on Nonlinear Local Filtering[J]. Journal of Engineering Science, 2016, 38(11): 1652—1658.

[15] ZHENG Xin, LEI Qin-yi, YAO Run. Image Segmentation Based on Adaptive K-means Algorithm[J]. EURASIP Journal on Image and Video Processing, 2018, 1(7): 1201—1209.

[16] REZA D, SAEED M, KHASHAYAR Y. Perceptual Image Hashing Using Center-Symmetric Local Binary Patterns[J]. Multimedia Tools and Applications, 2016, 75(8): 4639—4667.

[17] TENREIRO J A, ERDAL E D. Analysis of UV Spectral Bands Using Multidimensional Scaling[J]. Signal, Image and Video Processing, 2015, 9(3): 573—580.

[18] LIU Jing-yi, YANG Ding-ding, ZHOU Hong-bo. A Digital Image Encryption Algorithm Based on Bit-Planes and An Improved Logistic Map[J]. Multimedia Tools and Applications, 2018, 77(8): 10217—10233.

[19] 李新伟, 李雷达. 基于极谐变换的鲁棒图像哈希算法[J]. 计算机仿真, 2013, 31(5): 293—296.
LI Xin-wei, LI Lei-da. Robust Image Hashing Algorithm Based on Polar Harmonic Transformation[J]. Computer Simulation, 2013, 31(5): 293—296.

[20] SCHAEFER G, STICH M. UCID-an Uncompressed Colour Image Database[M]. Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multi-media, 2004.

[21] FAP P. Watermarking Schemes Evaluation[J]. IEEE Signal Proc Magazine, 2000, 17(5): 1—4.