基于压缩量化与邻域空间 LBP 算子的图像哈希算法

王彦超
（平顶山教育学院，平顶山 467000）

摘要：目的 为了解决哈希算法的感知鲁棒性与伪造检测能力不高的问题，提出基于特征压缩机制与邻域空间局部二值模式的紧凑图像哈希算法。**方法** 首先利用 2D 线性插值技术，对输入图像进行预处理；嵌入 Ring 分割技术，将其变为二次图像；再利用 Gabor 滤波技术对其完成过滤；考虑到图像的颜色特征与其内在的空间关系，基于局部二值模式 LBP 设计邻域空间 LBP 算子，提取滤波图像的特征；构建特征压缩量化准则，输出紧凑的哈希二值数组；迭代 Logistic 映射，输出随机序列，通过量化每个序列值输出密钥流，通过构建动态引擎设计分段异加密模型，实现紧凑哈希序列的加密，获取图像哈希；最后计算原始哈希序列与待检测哈希序列的 Hamming 距离，实现图像信息的安全认证。**结果** 与已有的哈希生成机制相比，文中算法所输出的哈希序列更紧凑，对旋转、伽马校正等篡改操作具有更好的感知鲁棒。**结论** 所提哈希技术具备较高的安全性，在包装图标检索、信息检测等领域具有较好的价值。

关键词：图像哈希；特征压缩量化规则；邻域空间局部二值模式；分段异加密；Gabor 滤波；决策阈值
中图分类号：TS801.3; TP391 **文献标识码：**A **文章编号：**1001-3563(2017)21-0191-08

Image Hashing Algorithm Based on Compression Quantization and Neighborhood Space LBP Operator

WANG Yan-chao
(Pingdingshan Institute of Education, Pingdingshan 467000, China)

ABSTRACT: The work aims to solve the problem of low perceptual robustness and forgery detection ability of Hash algorithm and propose the compact image Hash algorithm based on the feature compression mechanism and local binary pattern (LBP) in the neighborhood space. Firstly, the 2D liner interpolation was introduced to preprocess the input image and such image was changed into a secondary image with the Ring segmentation technology. Then, the Gabor filter technique was used to filter the image. LBP operator in the neighborhood space was designed based on LBP by considering the color feature and the intrinsic spatial relationship of image for extracting the feature of the filter image. The ture compression quantization rule was constructed to output the compact Hash binary array. The Logistic mapping was iterated to output the random sequence. The key stream was generated by quantifying each sequence value to design the segment diffusion model by constructing the dynamic engine, so as to realize the encryption of compact Hash sequence and obtain the image Hash. Finally, the Hamming distance between the original Hash sequence and the Hash sequence to be detected was calculated, and the security authentication of the image information was realized. The test results showed that, compared with the existing Hash generation mechanism, the proposed algorithm was more compact and more robust to rotation, gamma correction and other tampering operations. The proposed Hash technique has higher security and better value in the fields of packaging icon retrieval and information detection, etc.

KEY WORDS: image Hash; feature compression quantization rule; local binary pattern in neighborhood space; segment diffusion; Gabor filter; decision-making threshold

强大的图像编辑工具能够随意篡改图像而且无明显的痕迹，对图像信息造成了巨大威胁[1—2]。为了能够对图像的真伪实行准确检测，研究人员设计了图像内容认证技术，其中之一就是图像哈希技术[3—4]。

收稿日期：2017-03-13
基金项目：河南省科技计划（102102210416）；河南省软科学研究计划（152400410323）
作者简介：王彦超（1975—），男，硕士，平顶山教育学院副教授，主要研究方向为图像图形处理、模式识别、虚拟化技术。

如张秋余等[5]提出了基于非下采样轮廓波变换的彩色图像感知哈希算法。此技术忽略了图像的颜色特征与其内在的空间关系，且其输出的哈希序列维数较高。Yong Soo 等[6]提出了基于层次直方图的图像哈希算法。此哈希技术主要是利用了图像的直方图分布特性，导致其对旋转篡改的识别能力较弱。余俊伟等[7]提出了基于局部不变矩和 DWT 特征矩阵的图像哈希算法。由于旋转操作会导致子块与其旋转版本会存在较大的内容差异，且单纯利用图像的 V 分量来生产哈希序列，忽略了图像的颜色特征。为了提高哈希算法的感知鲁棒性与紧凑度，文中提出基于特征压缩机制与邻域空间局部二值模式的紧凑图像哈希算法。

1　文中图像哈希算法

所提的紧凑图像哈希算法过程见图 1。

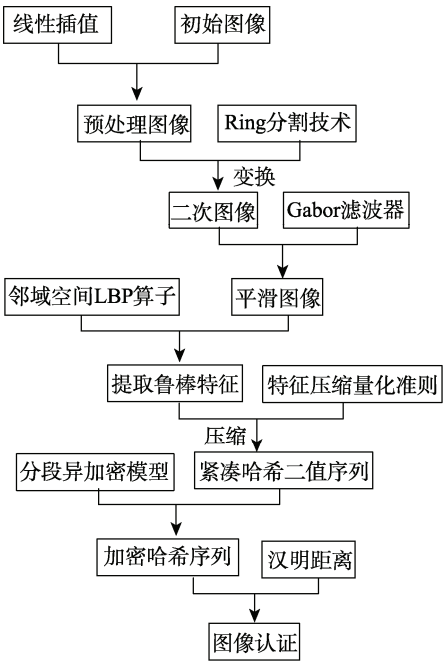


图 1　文中图像哈希认证算法过程

Fig.1 The propsoed image Hash authentication algorithm process

1.1　基于 2D 线性插值的图像预处理

首先，引入 2D 线性插值技术[8]，固定哈希尺寸：

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

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

式中：x_0, x_1 为初始起点；y_0, y_1 为 x_0, x_1 的插值结果；$x_0 \leqslant z \leqslant x_1$, $y_0 \leqslant z \leqslant y_1$。

再利用式（1）与式（2），联合卷积掩模[3]来实现初始图像的预处理。令 $T_G(i,j)$ 为卷积掩模中 (i,j) 处的元素，其模型为：

$$\begin{cases} T_G(i,j) = \dfrac{T(i,j)}{\sum_i \sum_j T(i,j)} \\ T(i,j) = \exp\dfrac{-\left(i^2 + j^2\right)}{2\sigma^2} \end{cases} \tag{3}$$

式中：σ 为卷积掩模的标准差；

另外，文中将图像 RGB 变为 YC_bC_r 空间[9]：

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 65.481 & 128.553 & 24.996 \\ -37.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \tag{4}$$

式中：R, G, B 为输入图像的红、绿、蓝三分量；Y, C_b, C_r 为亮度、蓝色与红色浓度偏移量。以图 2a 为例，利用式（1—3）对其插值后，输出结果见图 2b。

a 输入图像　　b 预处理结果

图 2　图像预处理结果

Fig.2 Image preprocessing results

1.2　基于 Ring 分割的二次图像输出

文中基于 Ring 分割技术[10]输出二次图像。令 f_0（x,y）的尺寸为 $m \times m$；n 为环形数量；$\boldsymbol{R}_k$ 是像素值集合。通过计算每个像素与图像中心之间的距离以及计算环形半径来对输入图像实施合理的 Ring 分割，其示意见图 3。令为第 k（k=1,2,3…n）个环形的半径，那么，对于 $m \times m$ 的图像 $f_0(x,y)$，其令 r_n 的计算函数为：

$$r_n = \left\lfloor \frac{m}{2} \right\rfloor \tag{5}$$

式中：$\lfloor\ \rfloor$ 为向下取整运算。

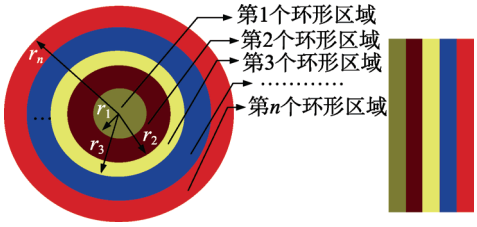


图 3　Ring 分割过程

Fig.3 Ring segmentation process

为了确定其他环形半径，首先计算内接圆 A 的面积以及每个环形的平均面积 u_A 见式（6）。

$$\begin{cases} A = \pi r_n^{\,2} \\ u_A = \left\lfloor \dfrac{A}{n} \right\rfloor \end{cases} \tag{6}$$

则最内环形区域的面积 r_1 为：

$$r_1 = \left\lfloor \frac{u_A}{\pi} \right\rfloor \tag{7}$$

对于其他环形区域 r_k（k=1,2,3…n−1）的面积，其计算模型为：

$$r_k=\sqrt{\frac{u_{\mathrm{A}}+\pi_{k-1}{}^2}{\pi}} \tag{8}$$

接下来，需估算其他位置像素与图像中心间的距离。令（x_c,y_c）代表图像中心位置，当 m 为偶数时，x_c=y_c=m/2+0.5；若 m 为奇数，则 x_c=y_c=（m+1）/2+0.5。则任意像素与中心像素的距离 d 为：

$$d_{x,y}=\sqrt{(x-x_c)^2+(y-y_c)^2} \tag{9}$$

根据式（5）、式（7）、式（8）以及式（9），获取距离 d 后，文中将这些像素值变为 n 个集合：

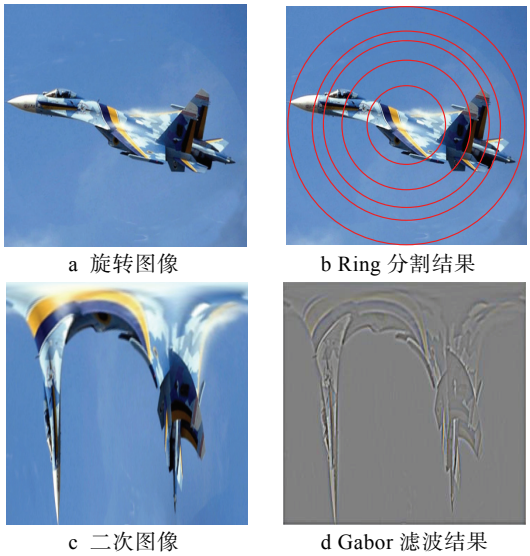
$$\boldsymbol{R}_1=\left\{p(x,y)\middle|d_{x,y}\leqslant r_1\right\} \tag{10}$$

$$\boldsymbol{R}_k=\left\{p(x,y)\middle|r_{k-1}<d_{x,y}\leqslant r_k\right\}(k=1,2....n) \tag{11}$$

随后，将 $\boldsymbol{R}_k$（k=1,2,3…n）中的元素按照从小到大的顺序重排，生成新的矢量 $\boldsymbol{u}_k$，确保 $\boldsymbol{u}_k$ 与旋转操作无关。再利用线性插值技术，将 $\boldsymbol{u}_k$ 映射为矢量 $\boldsymbol{v}_k$，其尺寸为 $\boldsymbol{u}_{\mathrm{A}}$×1。那么，对 $\boldsymbol{v}_k$ 进行重排，生成二次图像 V。

$$V=[v_1,v_2,v_3...v_n] \tag{12}$$

以图 2c 为例，对其进行逆时针旋转 32°，得到其旋转版本，见图 4a；并利用 Ring 分割对其分环处理，结果见图 4b，最终生成的二次图像见 4c。



a 旋转图像　　b Ring 分割结果

c 二次图像　　d Gabor 滤波结果

图 4　二次图像的生成

Fig.4 Secondary image generation

1.3　基于 Gabor 滤波器的二次图像平滑处理

利用 Gabor 滤波技术来平滑二次图像，其模型为[11]：

$$G(x,y,\lambda,\theta_f,\sigma_x,\sigma_y)=$$

$$\frac{1}{2\pi\sigma_x\sigma_y}\exp\left[-\pi\left(\frac{x_{\theta_j}}{\sigma_x}\right)^2-\pi\left(\frac{y_{\theta_j}}{\sigma_y}\right)^2\right]\exp\left(\frac{2\pi jx_{\theta_j}}{\lambda}\right) \tag{13}$$

$$\begin{cases}x_{\theta_j}=x\cos\theta_j+y\cos\theta_j\\ y_{\theta_j}=x\sin\theta_j+y\sin\theta_j\end{cases} \tag{14}$$

式中：x,y 为 Gabor 滤波的窗口尺寸；σ_x, σ_y 分别为 x,y 的标准差；λ 为正弦波的波长；θ_j 为正弦波的方向。

$$\theta_j=\frac{\pi}{n}(k-1),k\in\mathbf{N}_+ \tag{15}$$

式中：k 为 Gabor 滤波的方向数目。

利用式（13）处理二次图像，结果见图 4d。由图 4d 可知，Gabor 滤波图像可显著改善哈希序列对噪声、光照亮度干扰的鲁棒性。

1.4　基于领域空间 LBP 算子的特征提取

文中考虑图像的颜色特征与其内在的空间关系，并基于局部二值模式[12]，设计了邻域空间 LBP 算子。传统的 LBP 仅依靠单个像素区域内的特征，其模型为[12]：

$$L_{R,P}=\sum_{P=0}^{P-1}S(g_i-g_c)\times 2^i \tag{16}$$

$$S(x)=\begin{cases}1 & x\geqslant 0\\ 0 & x<0\end{cases} \tag{17}$$

式中：S（x）为中心和领域点的灰度差值；g_c, g_i 分别为中心像素及其邻域像素点；$L_{R,P}$ 为半径为 R 且存在 P 个邻域点的 LBP 算子。这种 LBP 算子没有考虑图像色彩与空间结构关，为此，文中设计邻域空间 LBP 算子。

首先，依据式（4），将 RGB 变为 YC_bC_r 空间；并利用 YC_bC_r 中任意 2 个分量 p_1, p_2 来估算 2 个领域与中心像素的偏差 $D_{p_{1i}}$, $D_{p_{2i}}$。

$$\begin{aligned}D_{p_{1i}}&=I_{p1}(g_i)-I_{p1}(g_c)\\ D_{p_{2i}}&=I_{p2}(g_i)-I_{p2}(g_c)\end{aligned} \tag{18}$$

式中：$I_{p1}(g_i)$ 为分量 p_1 中的第 i 个领域值；$I_{p1}(g_c),I_{p2}(g_c)$ 分别为分量 p_1, p_2 的中心领域值。

通过对比 $D_{p_{1i}}$, $D_{p_{2i}}$，得到新的灰度差值：

$$s(p_{1i}\times p_{2i})=\begin{cases}1 & D_{p_{1i}}>0\,\&\,D_{p_{2i}}>0\\ -1 & D_{p_{1i}}<0\,\&\,D_{p_{2i}}<0\\ 0 & \text{else}\end{cases} \tag{19}$$

为了与式（17）对应，文中将式（19）进行分割，得到子灰度差：

$$\begin{aligned}s_1(p_{1i}\times p_{2i})&=\begin{cases}1 & D_{p_{1i}}>0\,\&\,D_{p_{2i}}>0\\ 0 & \text{else}\end{cases}\\ s_2(p_{1i}\times p_{2i})&=\begin{cases}1 & D_{p_{1i}}<0\,\&\,D_{p_{2i}}<0\\ 0 & \text{else}\end{cases}\end{aligned} \tag{20}$$

随后，根据式（16）对 s_1（p_{1i}×p_{2i}），s_2（p_{1i}×p_{2i}）完成编码：

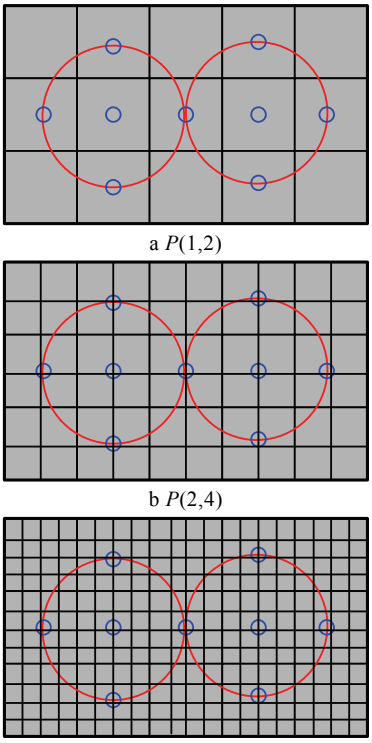
$$\begin{aligned}F_1(p_1\times p_2)&=\sum_{i=0}^{N-1}s_1(p_{1i}\times p_{2i})\times 2^i\\ F_2(p_1\times p_2)&=\sum_{i=0}^{N-1}s_2(p_{1i}\times p_{2i})\times 2^i\end{aligned} \tag{21}$$

再结合 F_1（$p_1\times p_2$），F_2（$p_1\times p_2$），获取色彩 LBP 算子 LBP（$p_1\times p_2$）。将空间结构关系引入到 LBP（$p_1\times p_2$）中，得到邻域空间 LBP 机制。为了充分利用相邻区域的空间结构特性，文中考虑图像中 2 个相邻的像素区域：

$$P(r,\Delta)=\left[L_{(c)},L_{(c+\Delta)}\right] \tag{22}$$

式中：Δ 为 2 个 LBP 中心像素点的距离；r 为 LBP 像素区的半径；c 为左侧 LBP 中心位置。

由于 LBP 提取的特征维数较高。为了降低特征维数，文中在任意一个 LBP 区域择取 4 个相邻像素点，见图 5。



a $P(1,2)$　b $P(2,4)$　c $P[4,8]$

图 5　不同（r,Δ）下的 $P(r,\Delta)$

Fig.5 $P(r,\Delta)$ with different (r,Δ)

通过考虑色彩 R，G，B，C_r 这 4 个分量，联合式（22），得到邻域空间 LBP 算子见式（23）。

$$L(r,\Delta)=\left[L(R\times C_r)_{(r,\Delta)},L(G\times C_r)_{(r,\Delta)},L(B\times C_r)_{(r,\Delta)}\right] \tag{23}$$

利用文中设计的邻域空间 LBP 算子提取 Gabor 滤波图像的特征，输出特征矢量 $\boldsymbol{F}_V=\{v_1,v_2,v_3...v_N\}$。以图 2a 为目标，利用式（24）对其处理，获取 LBP 特征图像，见图 6。由图 6 可知，目标的鲁棒特征被充分提取出来，无背景干扰特征。

1.5　基于特征压缩量化准则的低维哈希序列形成

文中构建了压缩量化准则，以降低 $\boldsymbol{F}_v=\{v_1,v_2,v_3\cdots v_N\}$的维数，输出紧凑哈希 $\boldsymbol{F}_v'=\{v_1',v_2',v_3'\cdots v_N'\}$。其步骤如下所述。

图 6　邻域空间 LBP 算子的输出结果

Fig.6 Output results of LBP operator in neighborhood space

1）引入最邻近域思想[13]，对 $\boldsymbol{F}_v=\{v_1,v_2,v_3\cdots v_N\}$中的每个元素完成相似性连接；若 b_1,b_2 为 F_V 的相邻两元素，且$\|b_1\square b_2\|^2<\varepsilon$ 时，将 b_1 认为是 b_2 的邻近点，再将二者进行连接。通过对 $\boldsymbol{F}_v=\{v_1,v_2,v_3\cdots v_N\}$中的每个元素完成该过程，则可输出邻接图。

2）计算邻接图中任意 2 个邻近点的相似度权重：

$$w_{ij}=\exp\left(\frac{-\|v_i-v_j\|^2}{\sigma^2}\right) \tag{24}$$

3）根据式（24）计算的权重，将 $\boldsymbol{F}_v=\{v_1,v_2,v_3\cdots v_N\}$完成映射，对其维数进行压缩：

$$\beta^{\mathrm{T}}(\boldsymbol{F}_V)L(\boldsymbol{F}_V)^{\mathrm{T}}\beta-\mu\times\beta^{\mathrm{T}}(\boldsymbol{F}_V)D_{ii}(\boldsymbol{F}_V)^{\mathrm{T}}\beta=0 \tag{25}$$

式中：μ 为实数。

得到式（25）的特征矢量β后，将β代入 $\boldsymbol{F}_{V'}=\beta^{\mathrm{T}}(\boldsymbol{F}_V)$中，可输出压缩特征矢量 $\boldsymbol{F}_V'$。随后，对低维特征矢量 $\boldsymbol{F}_V'$进行量化，输出紧凑哈希序列 $B=(B_1,B_2,B_3\ldots B_L)$。

$$B_i=\begin{cases}1 & v_i>t\\ 0 & v_i\leqslant t\end{cases} \tag{26}$$

式中：t 为阈值，其计算函数见式（27）。

$$t=\frac{\delta_1+\delta_2+\ldots+\delta_L}{N} \tag{27}$$

式中：N 为哈希长度；δ_i 为矢量 v_i 中所有元素的方差。

1.6　基于分段异加密模型与 Hamming 距离的哈希认证

为了改善哈希序列的安全度，文中设计哈希加密机制。删除哈希数组 $B=(B_1,B_2,B_3\ldots B_N)$ 中的 B_1 元素，再统计其他元素值之和：

$$s_{\mathrm{um}}=\sum_{i=2}^{N}B_i \tag{28}$$

再根据 S_{um} 值，估算初值 E_0：

$$E_0=\mathrm{mod}(s_{\mathrm{um}},256) \tag{29}$$

同时，引入 Logistic 映射[14]，设置初值 x_0, λ 进行迭代 N 次，生成混沌数组$\{x_1,x_2,x_3\ldots x_N\}$。

$$x_{i+1}=\lambda x_i(1-x_i) \tag{30}$$

并对$\{x_1,x_2,x_3\ldots x_N\}$进行量化，输出混沌密钥流$\{k_i\}$。

$$k_i=\mathrm{mod}\left(\mathrm{floor}\left(x_i\times10^{14}\right),256\right) \tag{31}$$

根据 E_0 与 k_i，对 $B=(B_1, B_2, B_3 \ldots B_N)$ 中的首个元素完成加密。

$$B_1 = E_0 \oplus B_1 \oplus k_1 \tag{32}$$

再构建 2 个引擎 q_1, q_2 来对哈希序列中其他元素进行加密：

$$q_1 = \text{floor}\left(\frac{\text{mod}\left(B_{i-1}+k_i, 256\right)}{256\times(i-1)}\right)+1 \tag{33}$$

$$q_2 = \text{floor}\left(\frac{\text{mod}\left(B_{i-1}k_i, 256\right)}{255\times(L-i-1)}\right)+i+1 \tag{34}$$

式中：$q_1 \in [1, i-1]$, $q_2 \in [i+1, N]$均为动态引擎；N 为哈希序列长度。

利用 q_1, q_2，设计了哈希加密机制：

$$B'_i = B_i \oplus k_i \oplus B_{q_1} \tag{35}$$

式中：B'_i 为加密哈希值。

反复执行上述哈希加密过程，当 $i=N-1$ 时结束。对于哈希 B_N，根据引擎 q_2 对其进行加密：

$$B'(N) = B(N) \oplus k(N) \oplus B_{q_2} \tag{36}$$

执行整个加密机制后，可输出最终的哈希序列 $H=\{H_1, H_2, H_3 \ldots H_N\}$。

完成哈希加密后，再对其实施认证。若初始图像对应的哈希序列 $\boldsymbol{H}_0 = \left\{H_1^0, H_2^0, H_3^0 \ldots H_N^0\right\}$，待检测图像的哈希序列是 $\boldsymbol{H}_1 = \left\{H_1^1, H_2^1, H_3^1 \ldots H_N^1\right\}$。文中利用 Hamming 距离[15] D 来计算 H_0, H_1 的相似度：

$$D = d(H_0, H_1) = \frac{1}{N-1}\sum_{i=1}^{N-1}(H_0 \oplus H_1) \tag{37}$$

式中：$\oplus$ 为异或运算。

根据式（37），若 D 值低于用户阈值 W 时，认为接收到的图像的内容为真实；反之，其内容被篡改。

2　实验结果与分析

借助 UCID 数据库[16]对所提哈希认证算法完成安全性测试，同时为了体现所提哈希技术的优异性，将文献[6，18]视为对照组，并利用 ROC 曲线[17]对 3 种哈希技术进行评估。关键实验参数为：x_0=1.5, λ=3.2, n=8, k=6。

2.1　阈值 W 的优化

在 UCID 图像库[16]中选择 1500 幅图像视为样本，将如下内容操作赋予每一幅图像：椒盐噪声分别为 0.01, 0.03, 0.05, 0.1；亮度调整因子为 0.6, 0.8, 1.2, 2.6；伽玛校正因子为 0.1, 0.4, 0.6, 1；JPEG 压缩因子为 0.6, 0.8, 1.4, 1.6；旋转角度为 10°, 30°, 60°, 110°；缩放尺度为 0.5, 0.9, 1.2 1.5。

不同图像的 Hamming 距离以及频数分布情况见图 7。根据图 7 中数据可知，就相同图像而言，当 Hamming 距离小于 0.53 时，其频数变化较大。对于不同的图像对，其 Hamming 距离大于 0.53，频数变化剧烈，因此，在文中哈希技术中，取阈值 W=0.53 进行鲁棒性与安全性实验测试。

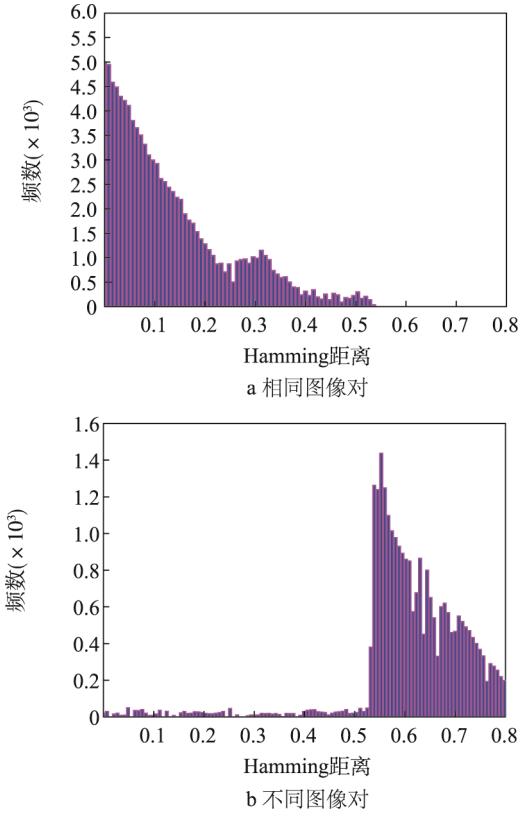


图 7　阈值的优化测试结果

Fig.7 Threshold optimization test results

2.2　哈希算法的鲁棒性测试

鲁棒性是哈希序列的重要评估指标[6]，为此，从 UCID 图像库中任意选择 4 幅图像，见图 8a—d，并上述的篡改内容对其进行处理；同时，利用式（37）输出其 Hamming 距离，测试数据见图 9a—9f。根据图 9 中显示的 Hamming 距离，所提哈希技术的 Hamming 距离 D 均要小于 0.53。

2.3　哈希算法的敏感性测试

若图像在网络传输中遭遇攻击使其数据被篡改，则攻击前后的图像哈希序列时存在较大差异[3]。文中对图像施加 6 种攻击，见图 10。同时估算二者的 Hamming 距离，图 10b—f 的 Hamming 距离分别为 0.543, 0.591, 0.637, 0.564, 0.602。利用文中哈希技术对其进行检测后，它们所对应的 Hamming 距离均超过阈值 0.53，这显示文中哈希算法对上述 6 种攻击具有强烈的敏感性，可对图像内容信息的真伪进行准确认证。

2.4　哈希算法的安全性测试

理想的哈希算法是具有的较高的安全性[7]，因此文中对 2400 组错误密钥进行测试，统计其对应的 Hamming

a Lena　b Pepper　c Scenery　d Panda

图 8　测试图像

Fig.8 Test image

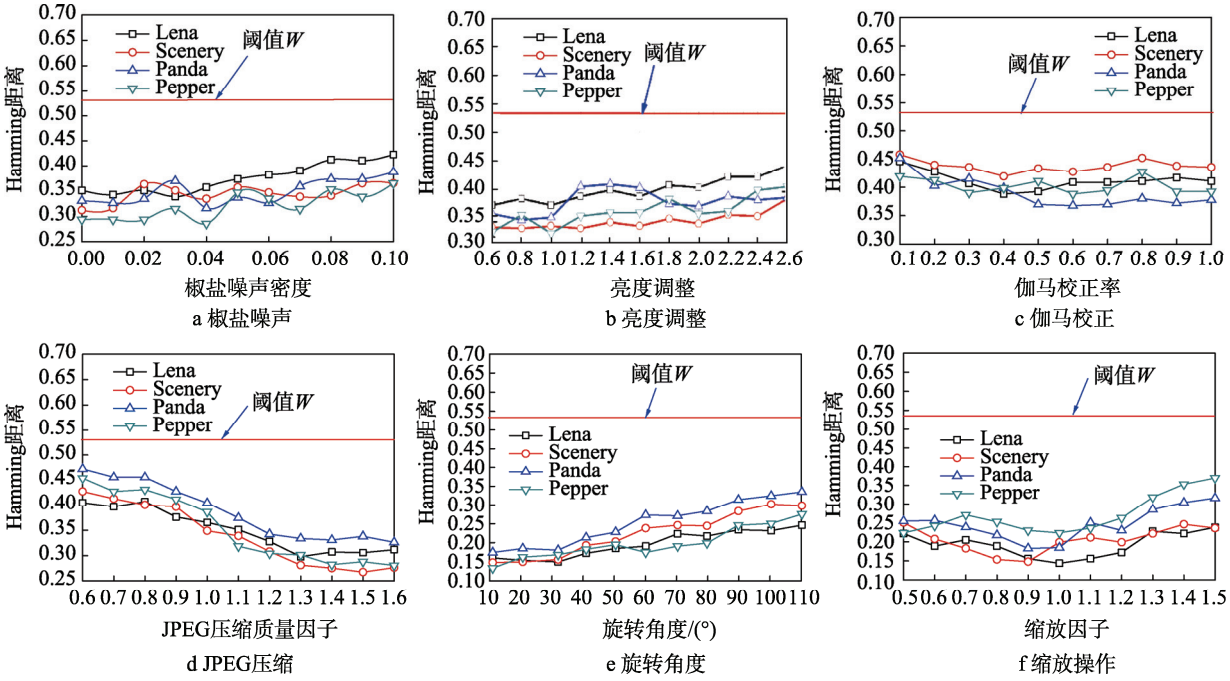
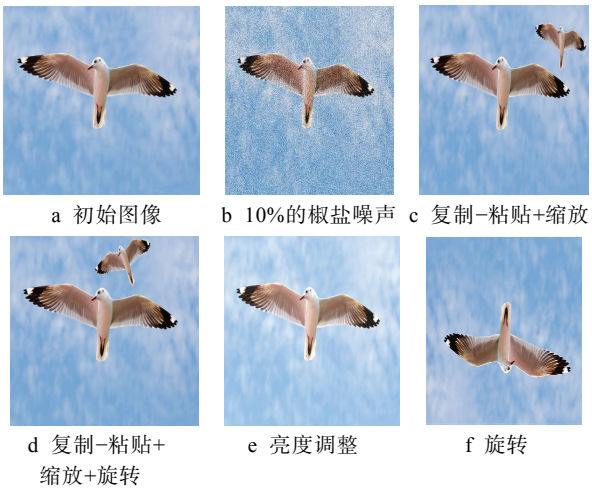


图 9　文中哈希技术的感知鲁棒性测试

Fig.9 Perceptual robustness test of the proposed Hash technique



a 初始图像　b 10%的椒盐噪声　c 复制−粘贴+缩放

d 复制−粘贴+缩放+旋转　e 亮度调整　f 旋转

图 10　6 种数字操作对应的图像

Fig.10 Images corresponding to six digital operations

距离，结果见图 11。由统计结果可知，对于这 2400 组错误密钥，所提哈希算法产生的 Hamming 距离值均超过了阈值 0.53。这显示了所提哈希技术具备理想的安全性。

2.5　不同哈希算法的鲁棒性分析

在 UCID 图像库[16]中任意选择 800 幅图像作为测试样本，利用文中算法、文献[6，18]对其进行处理，得到 ROC 曲线见图 12。根据 ROC 曲线可知，所提哈希算法对应的 ROC 特性最佳，尤其是面对旋转与伽马校正攻击，在 P_{FPR}=0.2 时，所提哈希技术对应的 P_{TPR}=0.983。文献[6，18]的感知鲁棒性均要低于所提哈希技术，其中，文献[6]对旋转攻击的识别能力最弱，文献[18]的鲁棒性虽然要优于文献[6]，但是仍然不理想，在 P_{FPR}=0.2 时，二者的 P_{TPR} 分别为 0.861, 0.925。

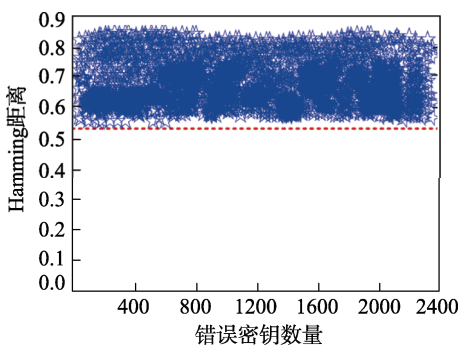


图 11　所提哈希算法的安全性测试

Fig.11 Security test of the proposed Hash algorithm

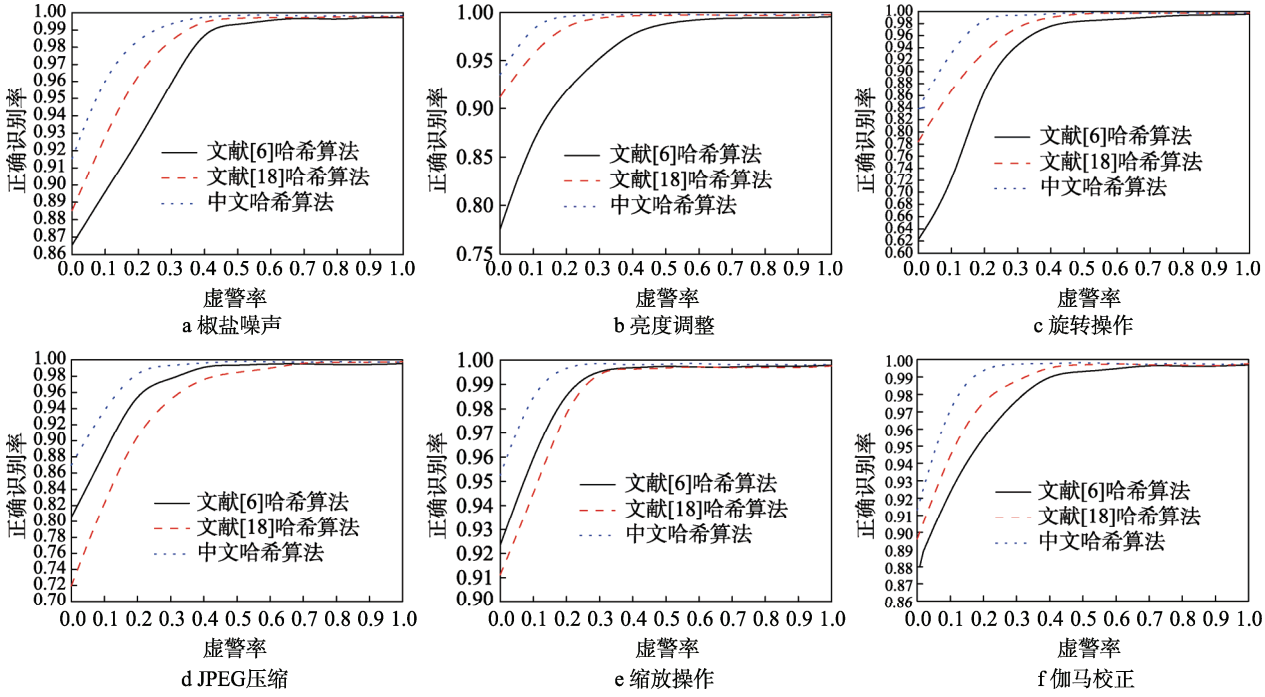


图 12　3 种算法的 ROC 曲线测试

Fig.12 ROC curve test of three algorithms

3　结语

提出了一种新的紧凑图像哈希算法来压缩哈希序列长度与提高其感知鲁棒性。联合 Ring 分割与 Gabor 滤波技术，将输入图像转变为抗旋转的二次图像，并基于经典的 LBP 算子，考虑图像的颜色特征与其内在的空间关系，设计了邻域空间 LBP 算子，增强其特征描述能力，有效提取鲁棒特征。另外，通过设计相应的加密函数来进一步改善哈希序列的安全性。实验结果显示所提哈希算法的认证能力更好，具有理想的 ROC 特性曲线。

参考文献：

[1] ÇAVUŞOĞLU Ü, KAÇAR S, PEHLIVAN I. Secure Image Encryption Algorithm Design Using A Novel Chaos Based S-Box[J]. Chaos, Solitons and Fractals, 2017, 95(16): 92—101.

[2] 郭静博, 孙琼琼. 改进的引力模型耦合明文像素相关交叉机制的图像加密算法[J]. 包装工程, 2016, 37(13): 165—172.
GUO Jing-bo, SUN Qiong-qiong. Image Encryption Algorithm Based on Improved Gravity Model Coupled with Plain Pixel Correlation Crossing Mechanism[J]. Packaging Engineering, 2016, 37(13): 165—172.

[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 Symmetric Local Two Value Model[J]. Laser & Optoelectronics Progress, 2017, 54(2): 4—16.

[4] SUN Rui, ZENG Wen-jun. Secure and Robust Image Hashing Via Compressive Sensing[J]. Multimedia Tools and Applications, 2014, 70(3): 1651—1665.

[5] 张秋余, 杨子, 李凯. 基于非下采样轮廓波变换的彩色图像感知哈希算法[J]. 兰州理工大学学报(自然科学版), 2016, 42(5): 95—101.
ZHANG Qiu-yu, YANG Zi, LI Kai. Color Image Perception Hash Algorithm Based on Non-sampling Contourlet Transform[J]. Journal of Lanzhou University of Technology(Natural Science Edition), 2016, 42(5): 95—101.

[6] YONG S C, PARK J H. Image Hash Generation Method Using Hierarchical Histogram[J]. Multimedia Tools and Applications, 2015, 61(1): 181—194.

[7] 余俊伟. 基于局部不变矩和DWT特征矩阵的图像哈希算法[D]. 广西: 广西师范大学, 2015.
YU Jun-wei. Image Hashing Algorithm Based on Local Moment Invariants and DWT Feature Matrix[D]. Guangxi: Guangxi Normal University, 2015.

[8] ROSŁONIEC S. An Example of Two-Dimensional Interpolation Using a Linear Combination of Bicubic B-Splines[J]. International Journal of Electronics and Telecommunications, 2012, 45(6): 109—118.

[9] 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 Blind Watermarking Algorithm for Color Image Guided by Visual Model[J]. Computer Application

Research, 2011, 28(7): 2719—2722.

[10] TANG Zhen-jun, ZHANG Xian-quan. Robust Perceptual Image Hashing Based on Ring Partition and NMF[J]. IEEE Transactions on Knowledge & Data Engineering, 2014, 26(3): 711—724.

[11] 王延年, 牛飞婷, 刘婷. 基于 Gabor 滤波的指纹图像增强方法[J]. 激光杂志, 2016, 11(1): 117—119.
WANG Yan-nian, NIU Fei-ting, LIU Ting. Fingerprint Image Enhancement Method Based on Gabor Filter[J]. Journal of Laser, 2016, 11(1): 117—119.

[12] 李春利, 沈鲁娟. 基于改进 LBP 算子的纹理图像分类方法[J]. 计算机工程与设计, 2016, 37(1): 232—236.
LI Chun-li, SHEN Lu-juan. Texture Image Classification Method Based on Improved LBP Operator[J]. Computer Engineering and Design, 2016, 37(1): 232—236.

[13] LIU Yang, LI Mei-dong, BI Xiao-ru. An Improved Location Difference of Multiple Distances Based Nearest Neighbors Searching Algorithm[J]. Optik-International Journal for Light and Electron Optics, 2016, 127(22): 10838—10843.

[14] 胡春杰, 陈晓, 陈霞. 基于改进广义 Arnold 映射的多混沌图像加密算法[J]. 包装工程, 2017, 38(3): 144—149.
HU Chun-jie, CHEN Xiao, CHEN Xia. Multi Chaotic Image Encryption Algorithm Based on Improved Generalized Arnold Map[J]. Packaging Engineering, 2017, 38(3): 144—149.

[15] 付海燕. 基于图像哈希的大规模图像检索方法研究[D]. 辽宁: 大连理工大学, 2015.
FU Hai-yan. Research on Image Retrieval Based on Image Hash[D]. Liaoning: Dalian University of Technology, 2015.

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

[17] 夏蕾, 周冰. 像素预测误差耦合似然映射的移动-复制图像伪造检测算法[J]. 量子电子学报, 2016, 33(2): 153—161.
XIA Lei, ZHOU Bing. A motion Detection Algorithm Based on Pixel Prediction Error Coupled Likelihood Mapping[J]. Quantum Electronics Journal, 2016, 33(2): 153—161.

[18] 刘凯. 基于压缩感知的图像哈希算法[D]. 广西: 广西师范大学, 2016.
LIU Kai. Image Hashing Algorithm Based on Compressed Sensing[D]. Guangxi: Guangxi Normal University, 2016.