基于数据降维与对称二值模式的图像 Hash 算法

王彦超[1], 郭静博[1], 周丽宴[2]

[1]平顶山教育学院计算机系, 河南 平顶山 467000;

[2]郑州大学信息工程学院, 河南 郑州 450001

摘要 为了解决当前图像 Hash 算法难以兼顾较高的感知稳健性与篡改识别率的不足,提出了基于数据投影降维机制与对称局部二值模式的紧凑图像 Hash 算法。利用双线性插值来预处理图像,使 Hash 具有固定的长度;引入对数极坐标变换,将其转变为二次图像;利用 Gabor 滤波器平滑二次图像;基于模糊集理论,设计对称局部二值模式算子,获取稳健特征;定义数据投影降维机制与量化规则,生成紧凑的中间 Hash 比特序列;构造一维组合混沌映射,建立加密模型,完成比特序列扩散,以生成图像 Hash;并引入汉明距离,估算初始图像与接收端图像的 Hash 相似度,联合决策阈值,完成图像认证。测试数据表明,与当前图像 Hash 技术相比,该算法的 Hash 更紧凑,且其感知稳健性与敏感性更高。

关键词 图像处理; 图像 Hash; 数据投影降维; 对称局部二值模式; 量化规则; 一维组合混沌映射; 决策阈值

中图分类号 TP391.4 **文献标识码** A

doi: 10.3788/LOP54.021004

Image Hash Algorithm Based on Data Dimension Reduction and Symmetric Binary Pattern

Wang Yanchao[1], Guo Jingbo[1], Zhou Liyan[2]

[1] *Department of Computer, Pingdingshan College of Education, Pingdingshan, Henan* 467000, *China*;

[2] *College of Information Engineering, Zhengzhou University, Zhengzhou, Henan* 450001, *China*

Abstract In order to solve the problem of difficulty of both the high perception robustness and tampering identification rate in the current image Hash algorithm, the compact image Hash algorithm based on data projection dimension reduction mechanism and fuzzy symmetric local binary pattern is proposed. The generated Hash has a fixed length by introducing the bilinear interpolation mechanism to preprocess the image. And the pretreatment image is transformed into the secondary image by the log polar transformation. The secondary image is smoothed by Gabor filter. The fuzzy symmetric local binary pattern operator is designed based on the fuzzy theory. And the compact intermediate Hash sequence is got by defining the data projection dimension reduction mechanism. The image Hash is generated by diffusing the bit Hash based on designing the one-dimensional combined chaotic map. The similarity between the original image and the image of the receiving end is estimated by introduction the Hamming distance and decision threshold to finish the authentication of image. Testing data show that this algorithm has stronger perception robust and sensitivity with tighter Hash length than the current image Hash technologies.

Key words image processing; image Hash; data projection dimension reduction; symmetric local binary pattern; quantization rule; one dimensional combined chaotic map; decision threshold

OCIS codes 100.4994; 110.2960; 110.2970

1 引 言

随着计算机技术的日益完善,各种图像编辑软件也不断升级,其编辑功能越来越强大,可以对图像进行

收稿日期: 2016-09-22; **收到修改稿日期**: 2016-10-10

基金项目: 河南省科技计划重点项目(102102210416)、河南省软科学研究计划项目(152400410323)

作者简介: 王彦超(1975—)男,硕士,副教授,主要从事图像图形处理、模式识别、虚拟化技术方面的研究。

E-mail: WangYchao1975pds@163.com

任意修改,而不留下任何篡改痕迹,仅凭人眼无法识别图像的真伪,严重威胁着图像信息安全[1-2]。为了应对这种图像篡改,有效识别图像信息的真伪,国内外学者提出了诸多图像内容认证方法,其中,常用的技术是图像 Hash 技术,该技术对图像内容具有强烈的敏感性,当图像内容发生极其微小变化时,所产生的 Hash 值与初始图像存在巨大差异[3-4]。在已有的图像 Hash 算法中,其主要包括三个过程:图像预处理、特征提取以及 Hash 生成。其中,图像特征提取是整个 Hash 算法的核心,其特征的稳健性直接影响了 Hash 算法的认证精度[3]。如 Choi 等[5]设计了基于层次直方图的图像 Hash 算法,通过预处理与联合子块直方图,提高 Hash 算法对缩放、JPEG 压缩的稳健性,实验结果验证了该算法的有效性。但是由于依据直方图特性来生成 Hash,因此其对旋转攻击的敏感性不高。曾勇等[6]提出了基于图像归一化和离散余弦变换(DCT)的感知图像 Hash 算法,通过 DCT 变换提取其低频系数,从而生成图像 Hash,仿真结果显示该技术具有良好的感知稳健性。但是该算法属于时频变换,难以有效抵御旋转攻击,且 Hash 维数较高,算法复杂度较大。Sun 等[7]设计了基于压缩感知与傅里叶-梅林变换的图像 Hash 算法,通过傅里叶-梅林变换,增强算法对缩放与过渡攻击的稳健性,基于压缩感知对所提取的特征进行压缩,形成紧凑的 Hash,实验结果验证了该算法的有效性,但是,该技术对篡改攻击的误识别率较高。

对此,基于数据降维思想,本文提出了一种新的紧凑图像 Hash 算法。该算法通过设计对称局部二值模式算子,能够较好地获取稳健特征,从而提高了算法的感知稳健性,再结合数据投影降维机制与加密机制,使得 Hash 算法兼顾了较高的安全性与生成效率,尤其是对数极坐标变换与对称局部二值模式算子,增强了该算法对旋转篡改的识别正确率。最后,对所提 Hash 算法的稳健性及其受试者工作(ROC)特性曲线进行了测试。

2 本文图像 Hash 算法

本文紧凑图像 Hash 生成算法流程见图 1,主要分为:1)基于双线性插值算子的图像预处理;2)基于对数极坐标变换的二次图像生成;3) 基于模糊对称局部二值模式算子的抗旋转特征提取;4)基于数据投影降维机制与

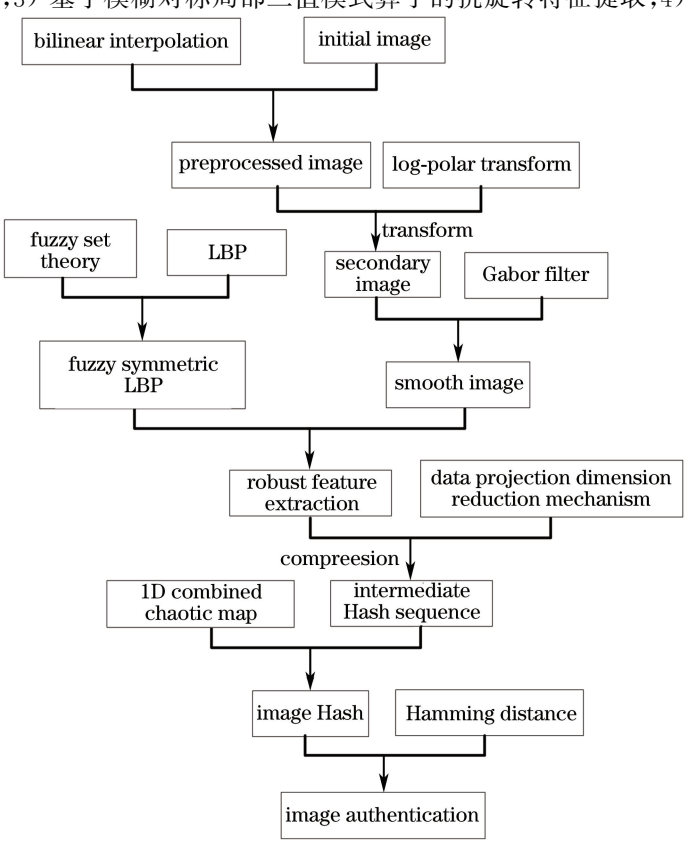

图 1 本文图像 Hash 认证算法过程

Fig. 1 Process of proposed image Hash authentication algorithm

量化规则的紧凑中间 Hash 比特序列生成;5)基于一维组合混沌映射与汉明距离的 Hash 加密与认证。

2.1 图像预处理

为了提高 Hash 对缩放的稳健性,使得对于任意尺寸的初始图像,其 Hash 长度具有固定值,本文引入双线性插值技术[8],结合卷积掩模对初始图像完成预处理。若 $T_G(i,j)$ 为卷积掩模中位于(i,j)处的元素,则其计算函数为

$$\begin{cases} T_G(i,j)=\dfrac{T(i,j)}{\sum_i\sum_j T(i,j)} \\ T(i,j)=\exp\left[\dfrac{-(i^2+j^2)}{2\sigma^2}\right] \end{cases}, \tag{1}$$

式中 σ 是卷积掩模的标准差。

同时,为了充分兼顾图像的色度信息与亮度,本文将 RGB 转换为 YCbCr 空间,将图像信息丢失对算法的影响最小化,从而提高算法的稳健性[9],即

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix}=\begin{bmatrix} 65.481 & 128.553 & 24.996 \\ -37.797 & -74.203 & 112 \\ 112 & -93.786 & -18.214 \end{bmatrix}\begin{bmatrix} R \\ G \\ B \end{bmatrix}+\begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix}, \tag{2}$$

式中 R、G、B 是彩图的红、绿、蓝三分量,Y、Cb、Cr 是亮度、蓝色浓度偏移量、红色浓度偏移量。

2.2 基于对数极坐标变换的二次图像生成

图像预处理增强了算法对缩放的敏感性,随后引入对数极坐标变换[10],获取抗旋转的的二次图像。若初始图像为 $f_0(x,y)$,$f_1(x,y)$ 为 $f_0(x,y)$ 的旋转版本,令其旋转角度为 θ,则 $f_1(x,y)$ 为

$$f_1(x,y)=f_0[(x\cos\theta-y\sin\theta),(x\sin\theta+y\cos\theta)]。 \tag{3}$$

对数极坐标变换对抗旋转与缩放性具有理想的敏感性[10],其变换机制见图 2。利用该机制将预处理图像转换成二次图像。设 (x,y) 为图像笛卡尔空间内的像素点;而 ρ 是对数极坐标变换的极径,θ 代表幅角,则其对数极坐标[10]为

$$\begin{cases} x=\exp(\rho)\cos\theta \\ y=\exp(\rho)\sin\theta \end{cases}, \tag{4}$$

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

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

式中(x_0,y_0)是图像中心点。

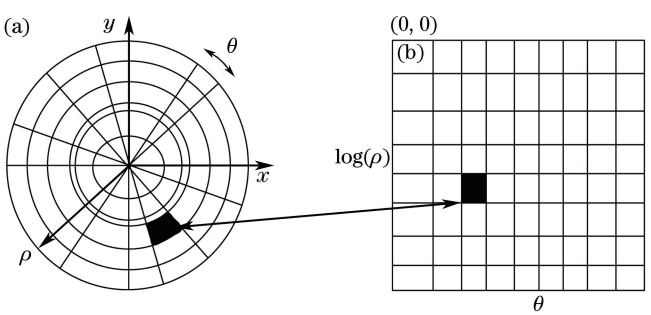

图 2 笛卡儿坐标映射为对数极坐标。(a)笛卡儿平面;(b)对数极坐标

Fig. 2 Cartesian coordinate mapping for log polar coordinates. (a) Cartesian plane; (b) log polar coordinate

联合(3)~(6)式,可得二次图像为

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

以图 3(a)为例,经过双线性插值技术预处理后,其结果见图 3(b),图像细节得到了较好地保留;在经过(4)式处理后,生成的二次图像如图 3(c)所示。

图 3 二次图像的生成及其 Gabor 滤波器处理。(a)初始图像;(b)双线性插值的平滑处理;(c)对数极坐标变换的二次图像;(d) Gabor 滤波器的过滤结果

Fig. 3 Secondary image generation and Gabor filter processing. (a) Initial image; (b) bilinear interpolation smoothing processing; (c) secondary image of the log polar coordinate transformation; (d) Gabor filter result

2.3 基于 Gabor 滤波器的二次图像过滤

为了增强 Hash 算法对噪声与几何变换攻击的稳健性,本文引入 Gabor 滤波器对二次图像进行滤波处理,该滤波器是在 Gabor 变换基础上扩展得到的二维信号处理技术,其模型为[11]

$$G(x,y,\lambda,\theta_f,\sigma_x,\sigma_y)=\frac{1}{2\pi\sigma_x\sigma_y}\exp\left[-\pi\left(\frac{x_{\theta_j}}{\sigma_x}\right)^2-\pi\left(\frac{y_{\theta_j}}{\sigma_y}\right)^2\right]\exp\left(\frac{2\pi\mathrm{j}x_{\theta_j}}{\lambda}\right), \tag{8}$$

$$\begin{cases}x_{\theta_j}=x\cos\theta_j+y\cos\theta_j\\ y_{\theta_j}=x\sin\theta_j+y\sin\theta_j\end{cases}, \tag{9}$$

式中 x、y 代表 Gabor 滤波器的窗口尺寸,σ_x、σ_y 分别是 x、y 的标准差,λ 为正弦波的波长,θ_j 代表正弦波的方向,其计算模型为

$$\theta_j=\frac{\pi}{n}(k-1),\qquad k\in N_+, \tag{10}$$

其中,k 为 Gabor 滤波方向数量。

依据(8)~(10)式可知,参数 σ_x、σ_y 与 λ 体现了 Gabor 滤波器的多尺度性;并且通过调整正弦波方向 θ_j,能够获取多方向的 Gabor 滤波,使其与人类视觉系统相接近,从而提取图像不同方向与尺度的稳定特征,如图 3(b)所示。在本文算法中,(8)式的核函数为[11]

$$G(x,y,\lambda,\theta_f,\sigma_x,\sigma_y)=\frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)\exp\left[\frac{2\pi\mathrm{j}(x\cos_{\theta_j}+y\cos_{\theta_j})}{\lambda}\right]。 \tag{11}$$

可见,利用 Gabor 滤波器对二次图像进行滤波处理,能够增强 Hash 算法对噪声与亮度调整的稳健性,同时对图像常见的几何变换攻击(平移、缩放以及旋转)也具有良好的敏感性。

2.4 基于模糊对称局部二值模式算子的稳健特征提取

图像经过 Gabor 滤波器处理后,有效降低了噪声干扰,再通过设计模糊对称局部二值模式算子,提取图像的稳健特征。局部二值模式算子局部二值模式(LBP)[12]具有较强的旋转和灰度不变性等显著优点,常用于图像特征提取。但是,传统的 LBP 只考虑一个 3×3 的窗口,并以矩形中心点的灰度值为阈值,对矩形内其他像素作二值化处理,并根据像素的不同位置进行加权求和得到该窗口的 LBP 值[12],其过程如图 4 所示。给定图像的中心像素,则 LBP 描述子为[12]

$$V_{\mathrm{LBP}}=\sum_{P=0}^{P-1}h_P\times w_P, \tag{12}$$

$$h(x)=\begin{cases}1, & x\geqslant 0\\ 0, & x<0\end{cases}, \tag{13}$$

式中 P 代表领域像素格式,$w_P=2^P$ 为权重,$h_P=(d_n-d_c)$ 是中心像素与领域像素的灰度差。

可见,传统的 LBP 算子是利用中心像素的领域像素的硬阈值来提取特征,当时攻击者对初始图像进行微小篡改时,LBP 算子难以识别这种差较小的像素,降低了其描述能力。

对此,本文基于模糊集理论,设计模糊对称局部二值模式算子,其典型的 8 邻域结构如图 5 所示。令

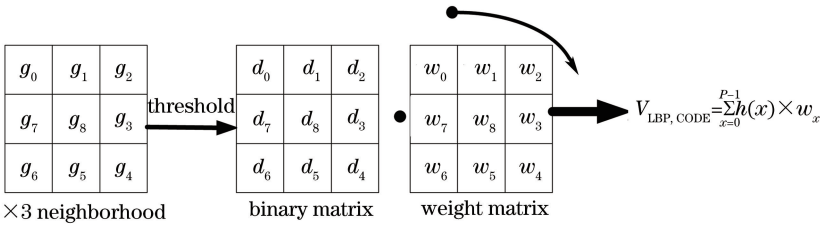

图 4 传统 LBP 算子的计算

Fig. 4 Traditional LBP operation calculation

$I(x,y)$ 代表图像，g_c 为位于 (x_c,y_c) 处像素的灰度值，即 $g_c=I(x_c,y_c)$。且令 $B\in[g_{\mathrm{ref}},g_{\max}]$ 代表 P_x 的模糊集合，而 $S\in[0,g_{\mathrm{ref}}]$ 是该范围内所有像素 P_x 的模糊集合。其中，$g_{\max}$ 为最大灰度，g_{ref} 是参考灰度。则 B、S 模型为

$$B=\{\langle P_i,u_B(x)\rangle,x\in H\}, \tag{14}$$

$$S=\{\langle P_x,u_S(x)\rangle,x\in H\}, \tag{15}$$

式中 u_B、u_S 分别为模糊集合 B、S 的模糊隶属度函数，代表着每个像素属于闭区间 $[0,1]$ 的程度；$H=\{0,1,2,\cdots,n-1\}$ 为 n 个领域像素数量。其中，u_B、u_S 的定义为[13]

$$u_B(x)=\begin{cases}1, & \text{if } g_{\max}-g_{\mathrm{ref}}\geqslant A\\ \dfrac{A+g_{\max}-g_{\mathrm{ref}}}{2_A}, & \text{if } g_{\max}-g_{\mathrm{ref}}<A,A\neq 0\\ 0, & \text{if } g_{\max}-g_{\mathrm{ref}}\leqslant -A,\ A\neq 0\\ 0, & \text{if } g_{\max}-g_{\mathrm{ref}}<A,\ A=0\end{cases}, \tag{16}$$

$$u_S(x)=1-u_B(x), \tag{17}$$

式中 $A\in[0,g_{\max}]$ 是控制模糊度的参数。

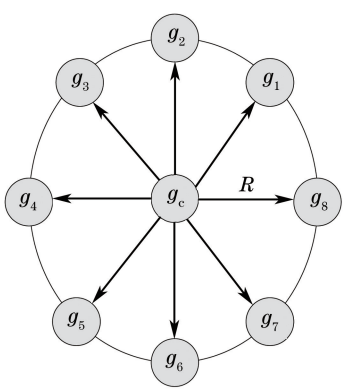

图 5 模糊对称局部二值模式算子

Fig. 5 Fuzzy symmetric partial binary pattern operator

根据(12)～(13)式，则模糊对称局部二值模式算子为

$$V_{\mathrm{FS\text{-}LBP}}(x_c,y_c)=\sum_{P=0}^{P/2-1}h_P\times w\,[g_P+g_{P+(P/2)}]^{2P}, \tag{18}$$

$$h_P=\begin{cases}1, & \text{if } Z\equiv B\\ 0, & \text{if } Z\equiv S\end{cases}, \tag{19}$$

式中 FS-LBP 为模糊对称局部二值模式(FS-LBP)算子。

随后，利用该糊对称局部二值模式算子来计算其归一化直方图，将其视为特征矢量，表示为

$$H(b)=\frac{1}{(M\times N)}\sum_{i=1}^{M}\sum_{j=1}^{N}f\,[V_{\mathrm{FS\text{-}LBP}}(i,j),b], \quad b\in[0,S], \tag{20}$$

$$f(x,y)=\begin{cases}1, & x=y\\ 0, & \text{otherwise}\end{cases}。 \tag{21}$$

将(20)式得到的直方图连接起来,得到了特征矢量 $\boldsymbol{V}_{\mathrm{F}}=\{v_1,v_2,v_3,\cdots,v_N\}$。

2.5 基于数据投影降维机制的中间 Hash 压缩量化

由于本文得到的 $\boldsymbol{V}_{\mathrm{F}}=\{v_1,v_2,v_3,\cdots,v_N\}$ 的维数较高,增加了算法的复杂度,为此,本文设计了数据投影降维机制,对特征矢量 $\boldsymbol{V}_{\mathrm{F}}=\{v_1,v_2,v_3,\cdots,v_N\}$ 进行压缩,以生产紧凑的 Hash 序列。本文数据投影降维机制的核心就是确定一个矢量 $\boldsymbol{M}$,将高维特征矢量 $\boldsymbol{V}_{\mathrm{F}}=\{v_1,v_2,v_3,\cdots,v_N\}$ 映射为低维矢量 $\boldsymbol{V}'_{\mathrm{F}}$。

为了确保数据映射前后所对应的元素有较近的距离,可最小化目标函数,表示为

$$\min\Big[\sum_{i,j}(y_i-y_j)^2\boldsymbol{w}_{ij}\Big], \tag{22}$$

$$\boldsymbol{w}_{ij}=\exp\left(\frac{-\|y_i-y_j\|^2}{\sigma^2}\right), \tag{23}$$

式中 $\boldsymbol{w}_{ij}$ 是权重矢量,以评估映射前后对应的元素 y_i 与 y_j 的紧密度。

假设特征矢量 $\boldsymbol{V}_{\mathrm{F}}=\{v_1,v_2,v_3,\cdots,v_N\}$ 中的每列向量为 $\boldsymbol{v}_i=\{a_1,a_2,\cdots,a_N\}$,对其进行数据降维,就是将特征矢量 $\boldsymbol{V}_{\mathrm{F}}$ 映射为 $\boldsymbol{V}'_{\mathrm{F}}=\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{V}_{\mathrm{F}}$,其中,$y_i$ 是降维矢量 $\boldsymbol{V}'_{\mathrm{F}}$ 中的元素。因此,对(22)式进行推导,得

$$\frac{1}{2}\sum_{i,j}(y_i-y_j)^2\boldsymbol{w}_{ij}=\frac{1}{2}(\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{v}_i-\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{v}_j)\boldsymbol{w}_{ij}=\sum_i\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{v}_i\boldsymbol{D}_{ii}\boldsymbol{v}_j^{\mathrm{T}}\boldsymbol{\beta}-\sum_{i,j}\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{v}_i\boldsymbol{w}_{ij}\boldsymbol{v}_j^{\mathrm{T}}\boldsymbol{\beta}=\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{V}_{\mathrm{F}}\boldsymbol{L}\boldsymbol{V}_{\mathrm{F}}^{\mathrm{T}}\boldsymbol{\beta}, \tag{24}$$

式中 $\boldsymbol{L}$ 代表拉普拉斯矩阵,$\boldsymbol{D}_{ii}$ 代表对角矩阵,

通过求解(24)式的最小特征值矢量 $\boldsymbol{\beta}$,可获得对应的低维矢量 $\boldsymbol{V}'_{\mathrm{F}}$,再依次连接 $\boldsymbol{V}'_{\mathrm{F}}$ 中的元素,形成中间 Hash $\boldsymbol{h}=\{h_1,h_2,h_3,\cdots,h_L\}$。

根据上述描述可知,本文定义的数据投影降维机制为

1) 通过最邻近域思想,对特征矢量 $\boldsymbol{V}_{\mathrm{F}}$ 中的元素进行相似度搜索链接,b_1、b_2 是 $\boldsymbol{V}_{\mathrm{F}}$ 中的相邻元素,若 $\|b_1-b_2\|^2<\varepsilon$($\varepsilon$ 为一个非常小的实数),则 b_1 是 b_2 的局部邻近点,用边将 b_1 与 b_2 连接起来,反复执行此操作,形成加权邻接图。

2) 依据加权邻接图,联合(23)式,确定该图中邻近两点的相似度权重。

3) 依据步骤 2)中的权重,对 $\boldsymbol{V}_{\mathrm{F}}$ 进行数据投影,降低数据维数。本文引入拉格朗日乘数法[14],对(24)式的进行转换,即

$$\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{V}_{\mathrm{F}}\boldsymbol{L}\boldsymbol{V}_{\mathrm{F}}^{\mathrm{T}}\boldsymbol{\beta}-\boldsymbol{\mu}\times\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{V}_{\mathrm{F}}\boldsymbol{D}_{ii}\boldsymbol{V}_{\mathrm{F}}^{\mathrm{T}}\boldsymbol{\beta}=0, \tag{25}$$

式中 $\boldsymbol{\mu}$ 为实数。

通过(25)式即可获得对应的矢量 $\boldsymbol{\beta}$,将其代入 $\boldsymbol{V}'_{\mathrm{F}}=\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{V}_{\mathrm{F}}$ 中,得到低维特征矢量 $\boldsymbol{V}'_{\mathrm{F}}$。

随后,对低维特征矢量 $\boldsymbol{V}'_{\mathrm{F}}$进行压缩量化。若 $\boldsymbol{v}_i$,$1\leqslant i\leqslant L$ 是其第 i 列向量。首先,根据矢量 $\boldsymbol{v}_i$ 的元素,计算其方差 δ_i;随后,再计算所有列向量的方差均值 t,即

$$t=\frac{\delta_1+\delta_2+\cdots+\delta_L}{L}, \tag{26}$$

式中 L 为 Hash 长度。

根据方差均值 t,定义量化规则:若矢量 $\boldsymbol{v}_i\geqslant t$,则 $B_i=1$;反之将 $B_i=0$。根据该规则,将紧凑的中间 Hash 序列量化为比特数组 $\boldsymbol{B}=\{B_1,B_2,\cdots,B_L\}$。

2.6 基于一维组合混沌映射的图像 Hash 生成与认证

为了增强 Hash 的安全性,对三个低维 1D 混沌映射,通过其中的逻辑映射来控制其他两个映射的迭代,从而设计组合混沌映射,其结构见图 6,对比特数组 $\boldsymbol{B}=\{B_1,B_2,\cdots,B_L\}$ 完成加密,以生成图像 Hash。组合混沌映射模型为

$$y_{i+1}=\begin{cases}P(y_i), & u_i\geqslant 0.5\\ T(y_i), & u_i<0.5\end{cases}, \tag{27}$$

式中 y_{i+1} 是组合映射的第 $i+1$ 个输出值,$P(y_i)$ 是切比雪夫混沌映射,$T(y_i)$ 是 Tent 映射,u_i 为逻辑映射的输出值。

对于(27)式中的切比雪夫混沌映射、Tent 映射、逻辑映射,其模型[15]分别为

$$P(x_{i+1})=\cos(k\sec x_i), \tag{28}$$

$$T(x_i)=\begin{cases}\beta x_i, & x_i<0.5\\ \beta(1-x_i), & x_i\geqslant 0.5\end{cases},\tag{29}$$

$$u_{i+1}=\lambda u_i(1-u_i),\tag{30}$$

式中 x_i 为系统变量；k 为混沌参数，当 $k=4$ 时，(28) 式具有理想的混沌行为；$\lambda\in[0,4]$，$\beta\in[0,2]$ 均为混沌控制参数。

根据(27)～(30)式，以及图 6 可知，其混沌序列输出规则为：

1) 当 $\lambda\in[0,2]$，且 $0\leqslant u_i<0.5$，则组合混沌映射的输出序列由(29)式决定；

2) 当 $\lambda\in[2,3]$，且 $0.5\leqslant\mu_i<1$，则组合混沌映射的输出序列由(28)式决定；

3) 当 $\lambda\in[3,4]$，且 $0\leqslant\mu_i<1$，则组合混沌映射的输出序列由(27)式决定。

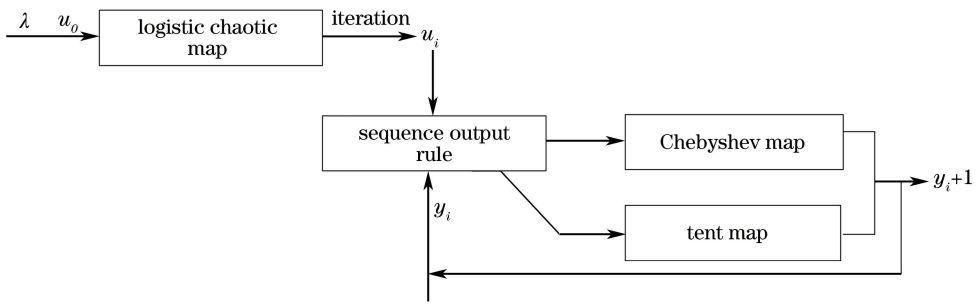

图 6 一维组合混沌映射

Fig. 6 One dimensional combined chaotic map

通过设置好参数 k、λ、β 以及初始变量 x_0，迭代设计组合混沌映射，输出混沌序列 $\{y_1,y_2,\cdots,y_k\}$，k 为迭代次数，本文取 k 等于 Hash 长度 L。

根据输出混沌序列 $\{y_1,y_2,\cdots,y_k\}$，构建加密模型为

$$\begin{cases}H_i=B_i\oplus Y_i\\ Y_i=\mathrm{mod}[\mathrm{round}(y_i\times 2^8),2]\end{cases},\tag{31}$$

式中 H_i 为图像 Hash 序列，mod 为求余计算，round 代表取整计算，⊕为异或运算。

依据(31)式，即可得到加密的 Hash $\boldsymbol{H}=\{H_1,H_2,\cdots,H_L\}$。

为了对接收端的图像进行认证，令初始图像为 I_0、用户接收图像为 I_1，利用本文 Hash 算法生成 I_0、I_1 对应的 Hash 序列 $\boldsymbol{H}_0=\{H_1^0,H_2^0,H_3^0,\cdots,H_L^0\}$ 与 $\boldsymbol{H}_1=\{H_1^1,H_2^1,H_3^1,\cdots,H_L^1\}$。并引入归一化汉明距离 D 来评估 H_0 与 H_1 的相似度[4]：

$$D=d(H_0,H_1)=\frac{1}{L-1}\sum_{i=1}^{L-1}(H_0\oplus H_1),\tag{32}$$

由(32)式可知，当 D 值小于用户设置的阈值 W 时，则可将图像视为视觉相同图像；反之，则视为差异图像。

3 实验结果与分析

为了测试所提 Hash 算法的稳健性与安全性，在 UCID 图像库[16]进行测试。另外，为彰显本文 Hash 技术的优异性，将文献[5]中基于层次直方图、文献[7]中基于压缩感知的 Hash 算法视为对照组。并引入 ROC 曲线来衡量算法的认证性能，由正确识别率 P_{TPR} 与虚警率 P_{FPR} 组成，其所对应 Hash 算法的感知稳健性与认真性能[17]，表达式为

$$\begin{cases}P_{\mathrm{TPR}}(\lambda)=\dfrac{n_1(D_1<\lambda)}{M_1}\\ P_{\mathrm{FPR}}(\lambda)=\dfrac{n_2(D_1<\lambda)}{M_2}\end{cases},\tag{33}$$

式中 n_1 为正确决策图像数量，n_2 为误判图像数量，M_1、M_2 分别为视觉相同与差异图像数量。

利用 Hash 算法对图像进行认证时，其阈值 W 对算法的稳健性具有重要影响。为了将所提 Hash 技术

的稳健性最大化，需确定出一个最优的认证阈值 W。其余参数为 $k=4$，$\lambda=3.5$，$\beta=1.5$，$u_0=0.35$。

3.1 认证阈值的优化

在 UCID 库[16]中随机选取 600 幅图像作为初始图像，对其完成表 1 中的数字操作。

表 1 不同参数值的图像数字操作

Table 1 Image digital operation with different parameter values

Operation type	Parameter
Salt-pepper noise	0.01, 0.04, 0.07, 0.1
Brightness adjustment	0.4, 0.8, 1.6, 1.9
Gamma correction	0.2, 0.4, 0.6, 1
JPEG compress	10, 20, 40, 90
Rotation /(°)	15, 35, 75, 105
Scale	0.2, 0.6, 1.4 1.7

图 7 为归一化汉明距离及其频数的整体分布。由图 7 可知，当归一化汉明距离低于 0.45 时，其频数分布异常突变，故本文将认证阈值 $W=0.45$。

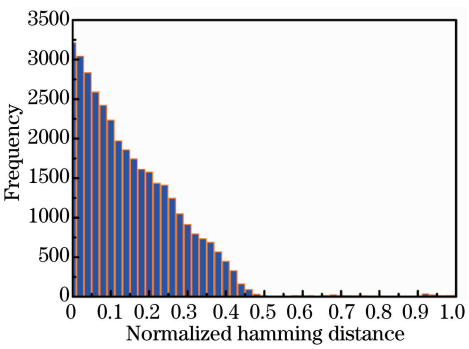

图 7 600 幅图像的识别测试

Fig. 7 Identification test with 600 images

3.2 Hash 算法的稳健性测试

1) 感知稳健性测试

感知稳健性是衡量 Hash 算法的重要指标[14]，故本文从 UCID 库中随机选择 4 个目标，如图 8(a)～(d)所示，依据表 1 中的 6 种内容篡改操作方式处理每幅图像，并联合(32)式获取其归一化距离 D，结果见图 8(e)～(k)。由测试数据可知，对于表 1 中的 6 种图像内容操作而言，本文 Hash 算法的归一化距离 D 都低于 0.45。可见，本文算法对椒盐噪声、旋转以及伽马校正等攻击具有较高的感知稳健性。原因是本文联合了对数极坐标变换与 Gabor 滤波器来处理二次图像，使其对亮度、对比度以及旋转、缩放具有较强的识别能力，且设计了模糊局部二值算子来提取稳健特征，增强算法对噪声以及压缩的敏感性。

2) 敏感性测试

当传输图像经过篡改攻击时，其 Hash 序列会产生截然不同的变化[7]。为了验证所提 Hash 算法的敏感性，将复制－粘贴的组合篡改攻击图像为目标，如图 9 所示，并依据(32)式计算其与初始图像的归一化距离，如表 2 所示。根据计算数据可知，这些篡改攻击图像经过所提 Hash 算法处理后，其归一化距离 D 都高于 0.4，可见，所提 Hash 技术可精确对这些篡改图像完成认证，将其决策为视觉差异图像。

表 2 数字操作图像与初始图像的相关系数

Table 2 Correlation coefficient between digital operation image and initial image

Name	Fig. 9(b)	Fig. 9(c)	Fig. 9(d)	Fig. 9(e)	Fig. 9(f)
Normalized distance	0.478	0.519	0.533	0.601	0.584

3) 安全性测试

优异的 Hash 算法应具备理想的安全性[6]，为此，本文测试 3000 组错误密钥，其归一化距离分布如图 10 所示。依图可知，本文算法对应的归一化距离都在认证阈值上方。在图像发送过程中，若攻击者不知道

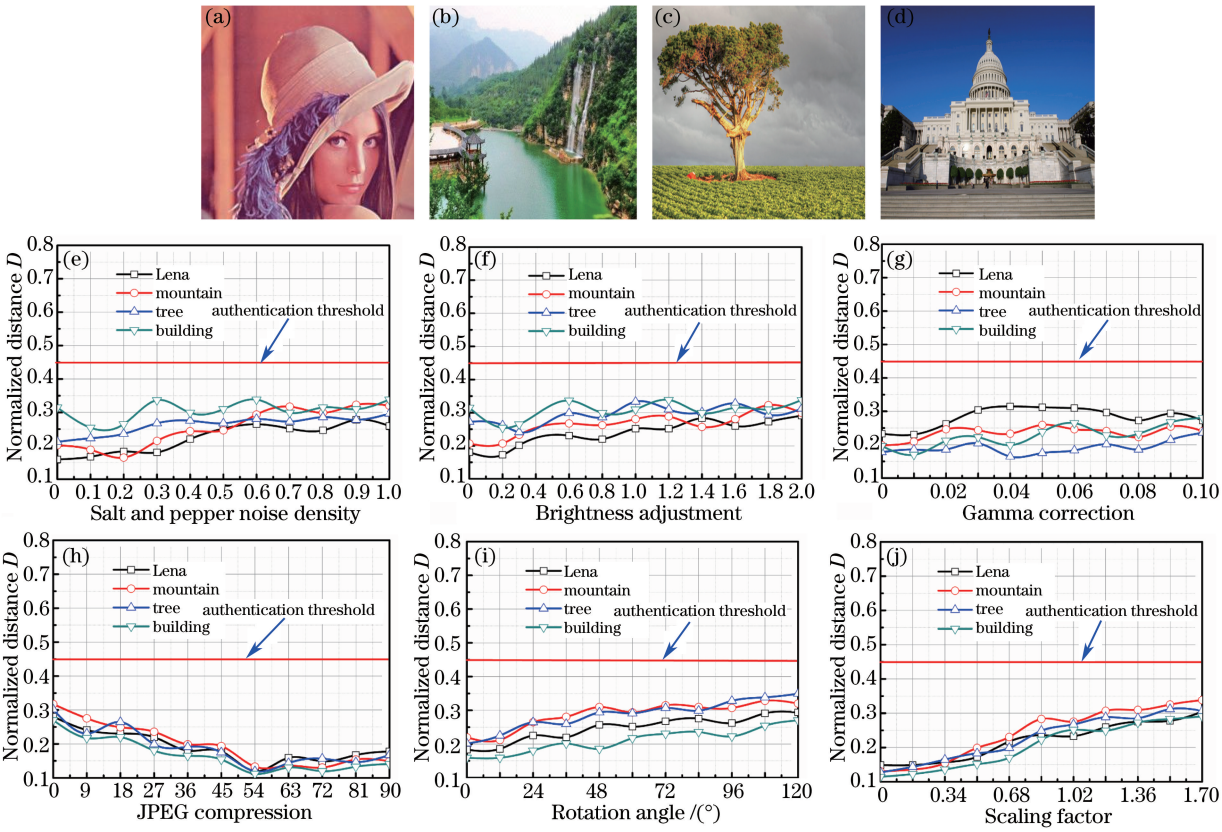

图 8 本文 Hash 算法的感知稳健性测试。(a) Lena;(b) mountain;(c) tree;(d) building;(e)椒盐噪声;(f)亮度调整;(h)伽马校正篡改下的相关系数;(i) JPEG 压缩下的相关系数;(j)旋转角度操作下的相关系数;(k)缩放操作下的相关系数

Fig. 8 Perceptual robustness testing of the proposed Hash algorithm. (a)Lena; (b)mountain; (c)tree; (d) building; (e) salt and pepper noise; (f) brightness adjustment; (h) correlation coefficient with Gamma correction; (i) correlation coefficient under JPEG compression; (j) correlation coefficient of rotation angle of operation; (k) correlation coefficient of the zoom operation

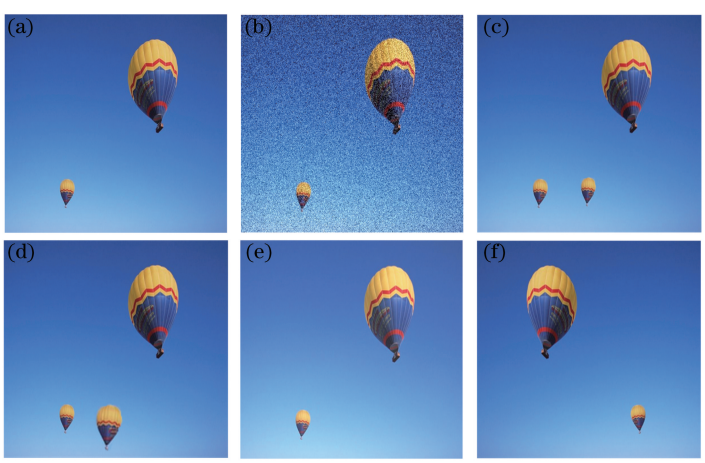

图 9 初始图像与数字操作图像。(a)初始图像;(b)施加 8%的椒盐噪声;(c)复制-粘贴;(d)复制-粘贴+缩放;(e)亮度调整;(f)旋转

Fig. 9 Initial image and digital operation image. (a) Original image; (b) applying 8% salt and pepper noise; (c) copy-paste; (d) copy-paste + zoom; (e) brightness adjustment; (f) rotation

Hash 密钥与整体的 Hash 算法,而本文算法 Hash 长度为 156 位,则攻击者对图像完成篡改的概率为 $(1/2)^{156}$。可见,本文 Hash 算法具有较高的安全性。

4) 不同 Hash 算法的稳健性对比测试

为了验证该算法、文献[5]与文献[7]算法的感知稳健性,本文在 UCID 库[16]中选择 500 幅图像来获取

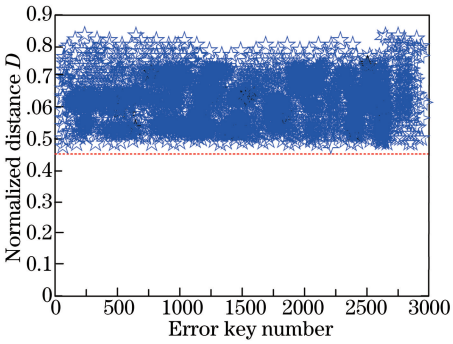

图 10 本文 Hash 算法的安全性测试

Fig. 10 Security test of the proposed hash algorithm

ROC 曲线,结果如图 11 所示。由图可知,对于表 1 中的篡改手段,本文算法的 ROC 特性更好,特别是在旋转操作下,当 $P_{FPR}=0$ 时,本文 Hash 算法的 $P_{TPR}=0.946$,当虚警率 $P_{FPR}=0.3$ 时,其 $P_{TPR}=0.997$。而对照组的感知性不佳,文献[5]在旋转操作下的稳健性最差,文献[7]的稳健性略低于本文算法,在旋转干扰下,当 $P_{FPR}=0$ 时,二者的 P_{TPR} 分别为 0.633,0.841,当虚警率 $P_{FPR}=0.3$ 时,其 P_{TPR} 约为 0.868,0.923。原因是本文算法利用双线性插值算子对其完成预处理,兼顾彩图的亮度与色度信息,通过对数极坐标变换与 Gabor 滤波器处理二次图像,增强 Hash 算法的抗旋转特性,再设计模糊对称局部二值模式,提取抗旋转与噪声的稳健特征。而文献[5]是单纯依赖图像的灰度直方图来生成 Hash,使其直方图对旋转与 JPEG 压缩的敏感性较低;文献[7]通过利用压缩感知与傅里叶-梅林变换来生成 Hash,虽然能够获取紧凑 Hash,但压缩感知丢失了图像部分特征,使得整个 Hash 算法识别旋转攻击的精度不佳。

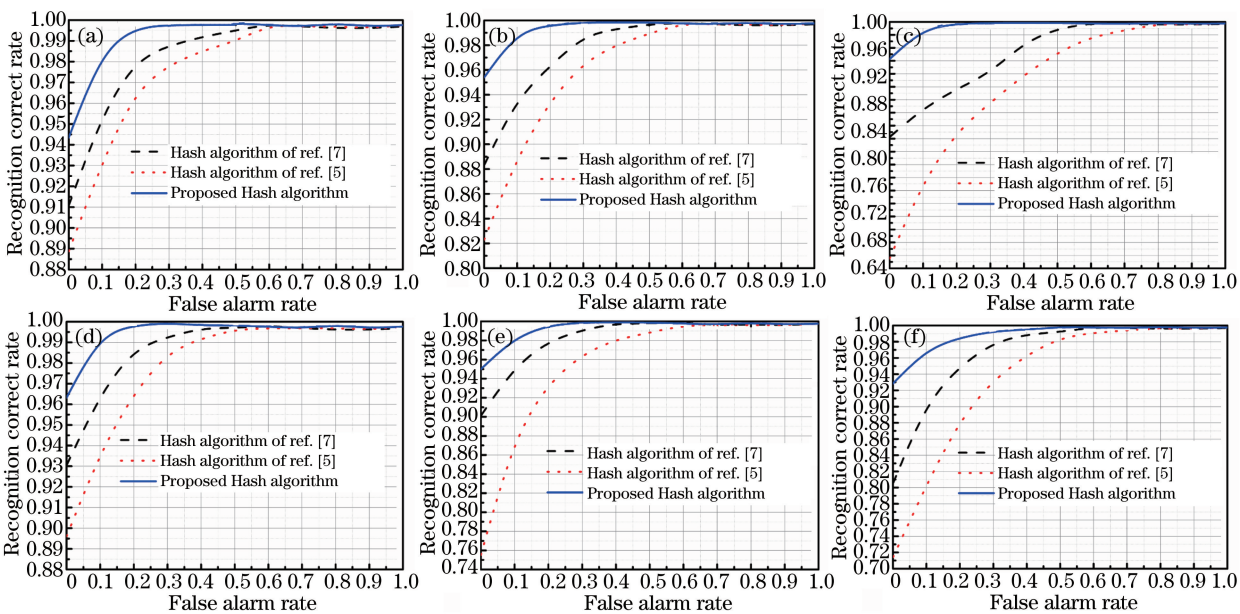

图 11 三种算法的 Hash ROC 曲线测试。(a)椒盐噪声;(b)亮度调整;(c)旋转操作;(d)缩放操作;(e) JPEG 压缩操作;(f)伽马校正

Fig. 11 Hash ROC curves test of the three algorithms. (a) Salt and pepper noise; (b) brightness adjustment; (c) rotation operation; (d) zoom operation; (e) JPEG compression operation; (f) Gamma correction

5) Hash 算法效率对比测试

为了测试本文算法、文献[5]与文献[7]三种算法的 Hash 生成效率,利用 Matlab 平台进行测试,条件为 DELL3.5 Hz 双核, 4 GB 的内存,各算法的效率见表 3。依据表中数据可知,本文算法由于设计了数据投影降维机制,对将高维 Hash 进行降维,使得 Hash 序列更为紧凑,其 Hash 长度为 126 位,显著降低了所提 Hash 算法的复杂度,其时耗为 0.17 s;而文献[5]通过层次直方图来生成 Hash,需要对每个特征的直方图进

行分层,且其提取的特征维数较高,增加了 Hash 算法的复杂度,其 Hash 长度为 334 位,其时耗最高,约为 0.46 s;文献[7]利用了压缩感知对 Hash 序列进行压缩,但压缩感知仍然是无法对其特征进行降维处理,使其时耗要高于本文算法,约为 0.26 s,其长度为 272 位。

表 3 三种算法的 Hash 性能与效率测试

Table 3 Hash performance and efficiency test of three algorithms

Name	Proposed algorithm	Ref. [5]	Ref. [7]
Hash length /bits	126	334	272
Time consumption of Hash generation /s	0.17	0.46	0.26
Identification noise tampering	YES	YES	YES
Identification rotation tampering	YES	NO	YES
Identification brightness adjustment tampering	YES	YES	YES
Identification JPEG compression tampering	YES	NO	NO
Identification Gamma correction tampering	Yes	No	No
Identification scale tampering	Yes	Yes	Yes

4 结 论

为了提高 Hash 算法的安全性与稳健性,提出了一种紧凑图像 Hash 算法,有效地实现了图像 Hash 的快速生成。该算法充分融合双线性插值机制与对数极坐标变换的优势,使得生成的二次图像具有更强的抗缩放与抗旋转能力;通过设计模糊对称局部二值模式算子,可以较好地提取图像的稳健特征;利用这些稳健特征,基于数据投影降维机制与量化规则,可生成维数较低的 Hash 比特序列;同时,还设计 1D 组合混沌映射,以此构建加密模型,从而进一步提高了 Hash 序列的安全性。并利用实验验证了所提 Hash 技术的有效性与优异性。由于彩色图像涉及到 RGB 三分量,后续将引入超复数理论,同步提取 RGB 三分量的稳健特征,进一步提高 Hash 生成效率。

参 考 文 献

[1] Lin Chao, Shen Xueju, Lei Ming, *et al*. Optical security validation based on orthogonal polarization multiplexing in three-dimensional space[J]. Acta Optica Sinica, 2016, 36(3): 0307001.
林 超, 沈学举, 雷 鸣, 等. 基于三维空间正交偏振态复用的光学认证技术研究[J]. 光学学报, 2016, 36(3): 0307001.

[2] Oommen R S, Jayamohan M, Sruthy S. Using fractal dimension and singular values for image forgery detection and localization [J]. Procedia Technology, 2016, 24: 1452-1459.

[3] Liu Z, Li Q, Niu X. Improve the security of image robust hash using fuzzy commitment scheme[J]. Neural Computing and Applications, 2013, 23(1): 67-72.

[4] Li Xinwei, Li Leida. Robust image hashing algorithm based on polar harmonic transform[J]. Computer Simulation, 2014, 31(5): 293-296.
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, 2014, 31(5): 293-296.

[5] Choi Y S, Park J H. Image hash generation method using hierarchical histogram [J]. Multimedia Tools and Applications, 2012, 61(1): 181-194.

[6] Zeng Yong, Sun Shusen, Xia Aijun. Image perceptual hashing based on image normalization and DCT[J]. Journal of Zhejiang Sci-Tech University, 2012, 29(1): 84-88.
曾 勇, 孙树森, 夏爱军. 基于图像归一化和 DCT 的感知图像哈希算法[J]. 浙江理工大学学报, 2012, 29(1): 84-88.

[7] Sun R, Zeng W. Secure and robust image hashing via compressive sensing[J]. Multimedia Tools and Applications, 2014, 70(3): 1651-1665.

[8] Cheng Xiangzheng, Zeng Chaoyang, Chen Hang, *et al*. Calibration method of low-resolution sensor based on bilinear interpolation strategy[J]. Laser & Optoelectronics Progress, 2013, 50(7): 071501.
程相正, 曾朝阳, 陈 杭, 等. 基于双线性插值算法的低分辨率传感器标定方法[J]. 激光与光电子学进展, 2013, 50

(7): 071501.

[9] Fang Wangsheng, Li Yunan, Zhang Rong. Blind watermarking algorithm for color image guided by visual model[J]. Application Research of Computers, 2011, 28(7): 2719-2722.
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.

[10] Zhang Z, Chen J, Li X, *et al*. An image matching method based on Fourier and LOG-polar transform[J]. Sensors & Transducers, 2014, 169(4): 61-66.

[11] Ye Zhen, Bai Lin, Nian Yongjian. Hyperspectral image classification based on Gabor feature and local protection dimension reduction[J]. Acta Optica Sinica, 2016, 36(10): 1028003.
叶 珍, 白 璘, 粘永健. 基于 Gabor 特征与局部保护降维的高光谱图像分类[J]. 光学学报, 2016, 36(10): 1028003.

[12] Tiwari D, Tyagi V. A novel scheme based on local binary pattern for dynamic texture recognition[J]. Computer Vision and Image Understanding, 2016, 150: 58-65.

[13] Zhang Zhifeng, Pei Zhili. Image forgery detection based on fuzzy local binary pattern operator [J]. Computer Engineering and Design, 2015, 36(12): 3284-3290.
张智丰, 裴志利. 基于模糊局部二值模式算子的图像伪造检测[J]. 计算机工程与设计, 2015, 36(12): 3284-3290.

[14] Brinkhuis J, Protasov V. A new proof of the Lagrange multiplier rule[J]. Operations Research Letters, 2016, 44(3): 400-402.

[15] Zhao Xin. Research on the optimization performance comparison of different one-dimensional chaotic maps [J]. Computer Application of Research, 2012, 29(3): 913-915.
赵 欣. 不同一维混沌映射的优化性能比较研究[J]. 计算机应用研究, 2012, 29(3): 913-915.

[16] Schaefer G, Stich M. UCID-an uncompressed colour image database[C]. SPIE, 2004, 5307: 472-480.

[17] Tang Z, Zhang X, Zhang S. Robust perceptual image hashing based on ring partition and nonnegative matrix factorization[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(3): 711-724.