doi:10.3969/j.issn.1000-436x.2012.11.023

对局部内容篡改敏感的感知图像散列

倪丽佳，王朔中，吴曾珉，裴蓓
（上海大学 通信与信息工程学院，上海 200072）

摘 要：提出了一种基于图像内容和颜色分布的感知图像散列。先将图像尺寸规格化并分成小块，根据各块亮度矩阵的奇异值判断其是否属于复杂区域，由此得到复杂区分布索引表。计算各图像块 Y 分量的均值和 R、G、B 均值两两之差的最小值，构成表征亮度和颜色分布的特征向量，将它与复杂区索引组合并加密得到图像散列。实验结果表明，由此提取的图像散列对保持图像内容不变的 JPEG 压缩、平滑滤波、缩放等处理具有良好的稳健性，而对内容篡改敏感并能准确定位篡改部位。

关键词：图像认证；图像散列；奇异值分解；篡改定位
中图分类号：TP391.41 **文献标识码**：A **文章编号**：1000-436X(2012)11-0177-08

Perceptual image hashing sensitive to content modification

NI Li-jia, WANG Shuo-zhong, WU Qiu-min, PEI Bei
(School of Communication and Information Engineering, Shanghai University hanghai 200072, China)

Abstract: A perceptual image hashing method based on the image content and color distribution was proposed. The image was scaled to a fixed size and divided into blocks. Each block was then classified semantically into complex or plain according to the ratio of the first two singular values of its luminance matrix so as to give a table of complexity indices. RGB components of each complex block were used to form a color-feature vector, which was combined with the complexity table and encrypted to produce the image hash. Experiments show that the hash is robust against content-preserving image manipulations such as JPEG compression, smoothing and re-scaling, and sensitive to tampering of the image content.

Key words: image authentication; image hashing; singular value decomposition; tampering localization

1 引言

随着数字技术和计算机网络的发展，数字图像的应用日益广泛，随之而来的侵权、篡改、伪造等问题也越来越严重，因此人们着手研究图像认证方法用以验证图像内容的完整性和真实性。一类重要的图像认证方案是主动认证（active authentication），即对要保护的图像采取特定的防范措施，如嵌入脆弱水印，或提取反映图像内容的认证码而不对图像进行任何修改。后者称为图像散列（image hash），可用于篡改和侵权检测、图像检索等领域，是数字内容安全和多媒体应用的前沿研究课题。

不同于密码学中对明文数据微小变化高度敏感的散列函数，图像散列对于不改变图像内容的正常处理具有稳健性，故常被称感知图像散列（perceptual image hash）。图像散列是图像到认证码的单向映射，应代表图像的本质内容并满足下列基本要求：1）感知稳健性，即 2 幅图像视觉无差异时，其散列值相同的概率趋于 1；2）抗碰撞性，图像间有重要视觉差异时散列相同的概率趋于 0；

收稿日期：2011-04-19；**修回日期**：2011-07-23
基金项目：国家自然科学基金资助项目（60773079, 60872116, 60832010）
Foundation Item: The National Natural Science Foundation of China (60773079, 60872116, 60832010)

3）安全性，根据媒体内容能正确估计散列的概率趋于 0；4）对篡改的敏感性，如用于篡改检测，应对局部内容的变化高度敏感。

早期图像散列方法缺乏安全性，抵抗攻击的能力较弱，例如根据图像块灰度均值和方差生成的散列[1]，或在小波域随机分割子带，提取统计量进行量化后输入 Reed-Muller 解码器产生散列[2]。一些基于 DCT 的方法如选用 DCT 低频系数[3]或利用 JPEG 图像块相同位置 DCT 系数间的不变性关系[4]，可使散列对 JPEG 压缩稳健，但对其他感知差异不明显的修改却很脆弱。Mihcak[5]用迭代法将小波低频分量二值化得到散列。利用变换系数对的不变关系也可生成图像散列，如用 DWT 分解中父子节点间的统计依赖关系得到稳健的结构式数字签名[6]。使用其他方法如保留图像块奇异值分解（SVD）中最大奇异矢量也可构造图像散列[7]。

Monga 等[8]提出了提取图像散列的 2 步框架，第 1 步先提取特征向量得到反映视觉特性的中间散列，视觉相似的图像特征向量相近，视觉差异大的图像其特征向量之间距离大。例如可用 Morlet 小波检测线状目标，再以 Gauss 函数一阶微商为滤波器来检测端点，取强度较大的小波系数构成特征向量。第 2 步是对中间散列进行量化和压缩得到最终的散列，包括输入图像中间散列向量和视觉相似图像中间散列的聚类[9]。为提高图像散列性能，研究者提出了一系列方法，如通过 Fourier-Mellin 变换中的旋转不变性矢量生成图像散列[10]。Monga 等采用非负矩阵分解（NMF, non-negative matrix factorization），将散列生成看作图像矩阵的降维[11]。利用 NMF 提取图像散列的方法近年来又有所发展。将图像进行伪随机分割可得到许多高维向量，用以组成二次图像并进行非负矩阵分解，再用 NMF 系数矩阵构造散列[12]，以及将 NMF 用于构建词典式结构的图像散列系统[13]，性能优于前期的 NMF 方法。

近来 Kheli?[14]基于虚水印检测得到了图像散列，Lei[15]提取图像 Radon 变换后的不变量，接着在这些不变量上进行 DFT 变换，量化后得到最终图像散列，这些方法具有良好的抗碰撞性和安全性。

本文提出一种结合图像局部区域复杂性结构的感知散列方法，使散列更集中地体现图像的实质内容。通过定位图像中具有足够信息量的区域，得到反映图像总体结构的索引，同时提取亮度和颜色分布特征参数，据此得到图像散列。该方法可有效区分图像是曾被恶意篡改还是仅经过了常规的处理，并可准确定位篡改部位，具有良好的感知稳健性和安全性。

2 图像散列提取和图像认证

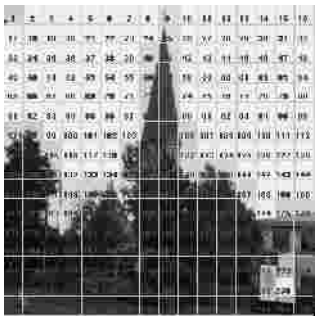
2.1 图像复杂区识别

图像篡改一般总是针对有意义区域进行的，或者用信息量极少的平坦块覆盖本来有意义的目标。可检测图像中有一定复杂度的区域，从中提取特征并结合复杂区域的分布来构成散列。为此将图像分成小块，通过奇异值分解（SVD）得到各图像块亮度矩阵的奇异值，以最大的 2 个奇异值 V_1 和 V_2 之比作为块的复杂性测度[16]

$$U = \frac{V_1}{V_2} \tag{1}$$

若 U 值很大，则最大的一个奇异值已包含块中绝大部分能量，说明是平坦块，包含信息量极少。相反，U 值较小说明图像块复杂，包含丰富的信息。极端情况下，完全平坦的块 $U\to\infty$，纯噪声块 U=1。用一个阈值 $?$ 来判定该图像块是否为复杂块，取 $?$=30 可得到满意的结果，如图 1 所示，可见平坦的块都被正确识别出来。实验表明本文方法对阈值的要求不苛刻，$?$ 在 20~40 范围内对散列的性能没有影响。

(a)原始图像



(b)复杂性判别结果

图 1 平坦图像块的识别

2.2　特征提取和散列的构成

直接取每个图像块 R、G、B 分量的均值构成颜色特征向量需要 24bit，考虑到各颜色分量之间并不完全独立，可取颜色分量之差来减少比特数。本文采用$|\overline{R}-\overline{G}|$、$|\overline{G}-\overline{B}|$、$|\overline{B}-\overline{R}|$中的最小值表示图像块的颜色特征

$$C=\min\left(|\overline{R}-\overline{G}|,|\overline{G}-\overline{B}|,|\overline{B}-\overline{R}|\right) \tag{2}$$

对 2 000 幅图像进行测试，计算每幅 256 块的 C 值，得到的数据分布情况如图 2 所示，其中，C >31 部分占总数的 5.9%。将 C 值限幅到 31，仅用 5bit 表示以缩短散列长度。

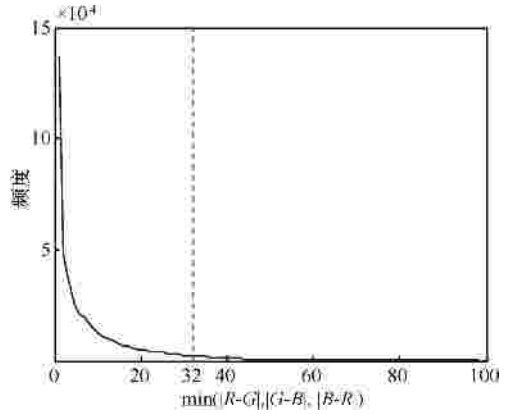


图 2　根据 2 000 幅图像得到的图像块 C 值分布

按下列步骤从图像中提取特征构成散列，用于图像认证。

1) 将图像规格化为统一的大小 256×256，然后进行 RGB→YUV 转换，以便根据亮度 Y 和 R、G、B 分量得到代表内容结构和颜色的特征。

2) 将规格化后的图像分割为 16×16 的块，共得 256 块。对每块的亮度矩阵进行奇异值分解，由式(1)计算块的复杂性参数 U。取阈值 ?=30，若 U<?，则认为该块位于复杂区域，记为 1；否则是平坦的，记为 0。代表所有块复杂性的记号形成一个长度为 256 的二进制序列 S，称为索引表。

3) 分别计算每个图像块 Y、R、G、B 分量，用 Y 分量的均值和由式(2)得到的 C 值构成反映图像亮度和颜色分布的特征 F，用 8bit 表示亮度特征 Y，用 5bit 表示颜色特征 C，因此 F 有 13bit。

4) 将反映亮度和颜色分布的特征 F 和反映复杂度结构的索引表 S 串接起来构成散列，即 H=[FS]，长度为 256×13+256=3 584bit。

5) 根据密钥用 AES[17]算法将 H 序列加密，认证时先用密钥解密。AES 是常用的对称加密算法，至今未有破解方法，可保证算法安全性。

2.3　图像认证过程

令原图像散列解密后为 H_1=[F_1S_1]，对于待认证图像根据上述特征提取步骤求得 H_2=[F_2S_2]。

1) 记录索引表 S_1 和 S_2 中取值为 1 的图像块编号，得到复杂块的指针序列 p_1 和 p_2。分别对 F 中的亮度特征 Y 分量和颜色特征 C 分量计算距离。

2) 考虑 Y 分量，取出 p_1 和 p_2 中的相同部分，记为 p_S，其长度为 K_S；不同部分为 p_D，长度为 K_D。将 p_S 和 p_D 串接，并按图像块编号排列，得到长度为 K=K_S+K_D 的指针序列 p（如 p_1 和 p_2 相同则没有 p_D，p=p_1=p_S）。求得 p_S 所指的两图像对应块的 Y 分量距离 $d_S(1),d_S(2),\cdots,d_S(K_S)$，统计其中为 0 的个数 z。根据 p_D 中的指针得到两图像对应块的 Y 分量，计算距离 $d_D(1),d_D(2),\cdots,d_D(K_D)$。将 2 个距离序列组合起来得到 [$d_S(1)$, $d_S(2)$, … ,$d_S(K_1)$,$d_D(1)$,$d_D(2)$, … , $d_D(K_2)$]，记为{$d(k)$},k=1,…,K。记录其中的最大值 m，并计算下列距离测度

$$D_Y^{(1)}=\sqrt{\sum_{k=1}^{K}[d(k)]^2} \tag{3}$$

为说明上述步骤，如图 3 所示。设阴影块是复杂图像块，数字为编号，左边为原始图像，复杂块指针 p_1=[3 17 18 19 32 34 243]，右边为待认证图像，指针 p_2=[3 17 18 19 32 48 52 243]。两指针序列不同，得到 p_S=[3 17 18 19 32 243]，K_S=6，对应块 Y 分量距离为 $d_S(1)$~$d_S(6)$；p_D=[344 852]，K_D=3，对应块 Y 分量距离为 $d_D(1)$~$d_D(3)$。由此可求得 m、z 和 $D_Y^{(1)}$。

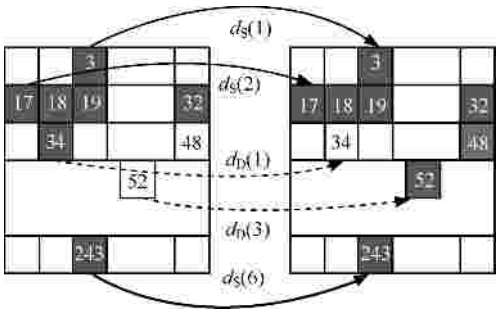


图 3　认证过程图解

3) 根据上述参数分几种情况计算特征 F 中的 Y 分量距离 D_Y。

① 若 m 和 z 足够大（m>μ，z>?），说明较多的块没有发生变化，同时又存在变化幅度较大的块，

因此可认为图像曾被篡改，Y 分量距离由 p 中所有指针所指 2 图像对应块 Y 分量之间的欧氏距离得到，记 $D_{\mathrm{Y}}=D_{\mathrm{Y}}^{(1)}$。根据实验，取 μ=18，?=0.65×K_{S}。

② 若 $D_{\mathrm{Y}}^{(1)}$ 大于某一阈值 ?，可认为是不同图像。也将 Y 分量的距离记为 $D_{\mathrm{Y}}=D_{\mathrm{Y}}^{(1)}$。根据实验，取 ? 为 500。

③ 若上述 2 个条件都不满足，计算序列 p 中相邻指针所指的 2 图像中块的 Y 分量值之差，分别记为 $f_1(1), f_1(2),\cdots, f_1(K-1)$和 $f_2(1), f_2(2),\cdots, f_2(K-1)$。以图 3 为例，$p$=[3 17 18 19 32 34 48 52 243]，K=9，则 $f_1(1)$为原始图像第 3 块和第 17 块的 Y 分量值之差。此时应按下式计算 2 幅图像 Y 分量之间的距离

$$D_{\mathrm{Y}}=D_{\mathrm{Y}}^{(2)}=\sqrt{\sum_{k=1}^{K-1}\left[f_1(k)-f_2(k)\right]^2} \tag{4}$$

这样求得的距离考虑了图像块之间的关系，若待认证图像经过常规处理后图像块 Y 分量值发生变化，通过计算 Y 分量值差可在一定程度上减弱这种变化，提高稳健性。

4) 用同样的方法计算颜色特征 C 的距离 D_{C}。C 分量的取值范围较小，阈值也应较低。通过实验将阈值 μ 取为 8，? 取 250。

5) 以 D_{Y} 和 D_{C} 中较大者为 2 图像的距离

$$D=\max(D_{\mathrm{Y}}, D_{\mathrm{C}}) \tag{5}$$

用 D 衡量 2 幅图像之间的差异能有效区分常规处理和篡改。经过常规处理的图像与原图像距离较小，而被篡改后与原图像距离明显变大，2 幅完全不同图像之间的距离更大。设定 2 个阈值 T_1 和 T_2 可判断一幅图像是原始图像经正常处理的结果，被篡改的版本，还是完全不同的图像。

6) 篡改定位。通过上述 5 步得到原始图像和待认证图像间的散列距离 D，若 $T_1<D<T_2$，认为待认证图像经过篡改。对于两图像的 256 块逐一计算相对应块的 Y 分量之差 $E_1(i)$和 C 分量之差 $E_2(i)$，i=1,…,256。若 $E_1(i)>t_1$ 或 $E_2(i)>t_2$，则认为该图像块被篡改。这里取 t_1=10，t_2=5。

3 实验结果

将图像库 UCID[18]和 McGill Calibrated[19]中各 200 幅图像用于实验，对 400 幅图像进行不同类型和不同程度的处理，包括以下 6 类，22 种。

1) JPEG 压缩，质量因子 20、40、60、80、100；

2) 缩放，倍率 0.75、0.9、1.1、1.5；

3) 中值滤波，窗口尺寸 3×3、5×5；

4) 行列删除，间隔行列数 30、20、10；

5) 添加高斯白噪声，信噪比 50dB、40dB、30dB、20dB；

6) 低通滤波，模板高斯函数标准差 0.3、0.5、0.7、0.9。

其中，前 4 类用 Stirmark4.0 实现[20]，后 2 类用 MATLAB 实现。这些处理均不改变图像的实质内容，为了便于叙述，统称常规处理。

再用不同的图像局部代替原始图像中的特定区域，得到篡改后的 400 幅图像（图 8 给出几个实例）。计算常规处理和篡改后图像散列与原图像散列之间的距离，结果如图 4 所示，其中，横坐标为

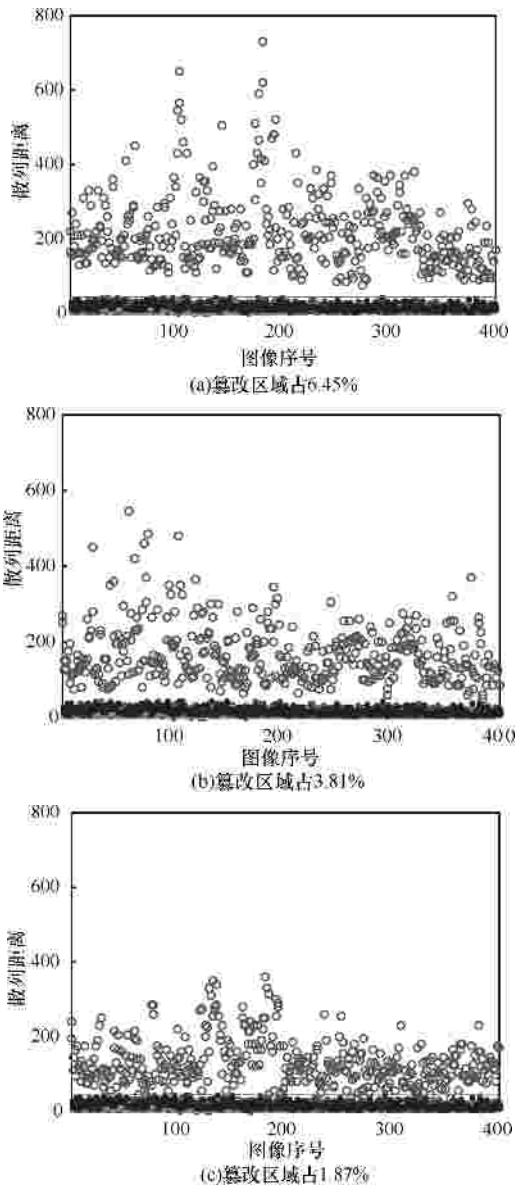


图 4 对 400 幅图像进行不同处理后与原图的散列距离

图像序号，纵坐标是散列之间的距离。图 4 中位于下部的实心小点为常规处理的结果，小圆圈表示篡改图像的结果，给出了 3 种不同篡改面积的情况，如图 4(a)、图 4(b)、图 4(c)所示。在常规处理中，低质量因子的 JPEG 压缩和中值滤波造成散列之间距离较大，但仍在水平线 45 以下。篡改后图像的散列与原图像散列的距离明显较大，绝大多数超过 45。实验中篡改区域小到 1.87%时也能与常规处理明确区分。

图 5 给出正常处理、局部内容篡改、不同图像 3 种情况下散列距离的分布。每个图中左边曲线表示

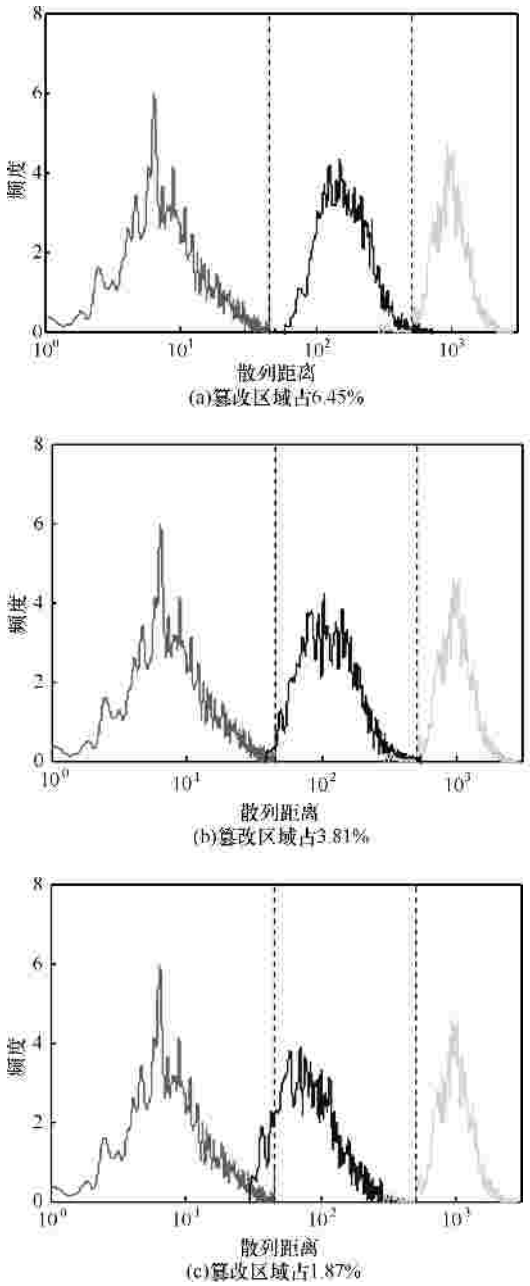


图 5　分辨常规处理、内容篡改、不同图像的实验结果

对 400 幅图像进行 5 种常规处理（标准差为 0.9 的高斯滤波、质量因子 60 的 JPEG 压缩、3×3 中值滤波、缩小到 90%、每 10 行 10 列删除 1 行 1 列），提取处理前后的散列，得到 2 000 个距离的统计结果。中间的曲线表示每幅图像经过 5 种不同位置，不同内容的篡改得到 2 000 个散列距离的分布。篡改比例分别为 6.45%、3.81%和 1.87%(图 5(a)、图 5(b)和图 5(c))。右边则是 2 000 对不同图像的散列距离的统计分布。可见常规图像处理引起散列的改变较小，不同图像间散列距离很大，局部内容篡改则介于两者之间。当篡改区域较大时，与常规处理的曲线相交部分很小，随着篡改比例减小两者相交部分随之增大，意味着误判增加，但大多数仍能正确区分。根据大量实验，取 T_1=45 为常规处理和内容篡改的分界，T_2=500 为篡改和不同图像的分界，可得到满意的结果。

篡改比例为 6.45%、3.81%、1.87%时，对常规处理和内容篡改的结果取不同阈值得到如图 6 所示 ROC 曲线，横坐标是虚警率，表示常规处理被误判为篡改的概率，纵坐标是正确检测率，表示篡改图像被正确检测的概率。图 6 中三角、圆圈、十字符号标出的点分别为阈值取 40、45、50 时的结果，具体数据如表 1 所示。可见，取 45 为常规处理和篡改的分界较为合理，当篡改比例为 6.45%时全部正确检测，无虚警。随着篡改面积减小，正确检测率仅略有下降，同时虚警率也开始上升。同样，也可根据图像篡改和不同图像的检测结果得到 ROC 曲线，当阈值为 500 时区分篡改和不同图像的效果优良。

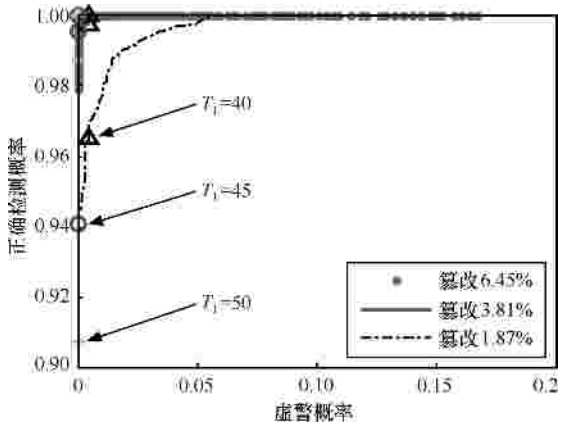


图 6　篡改区占整个图像 3.81%和 1.87%时的 ROC 曲线

为检验散列的抗碰撞性能，取 1 000 幅图像，计算两两之间的散列距离，得到 499 500 个数据。

表 1 取不同阈值时的 2 类错误概率

概率	篡改 6.45%			篡改 3.81%			篡改 1.87%		
	T_1=40	T_1=45	T_1=50	T_1=40	T_1=45	T_1=50	T_1=40	T_1=45	T_1=50
虚警概率 P_f	0.004 5	0.000 0	0.000 0	0.004 5	0.000	0.000 0	0.004 5	0.000 0	0.000 0
正确检测概率 P_d	1.000 0	1.000 0	1.000 0	0.998 0	0.996 0	0.987 5	0.965 5	0.941 0	0.907 5

图 7 给出散列距离的分布。参照文献[12]采用的方法，可知散列距离服从伽玛分布

$$P(T)=\int_0^T \frac{1}{b^a\Gamma(a)}D^{a-1}\exp\left(-\frac{D}{b}\right)\mathrm{d}D \qquad (6)$$

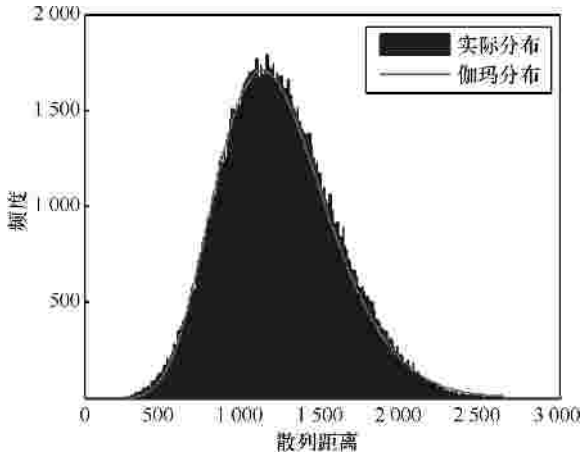


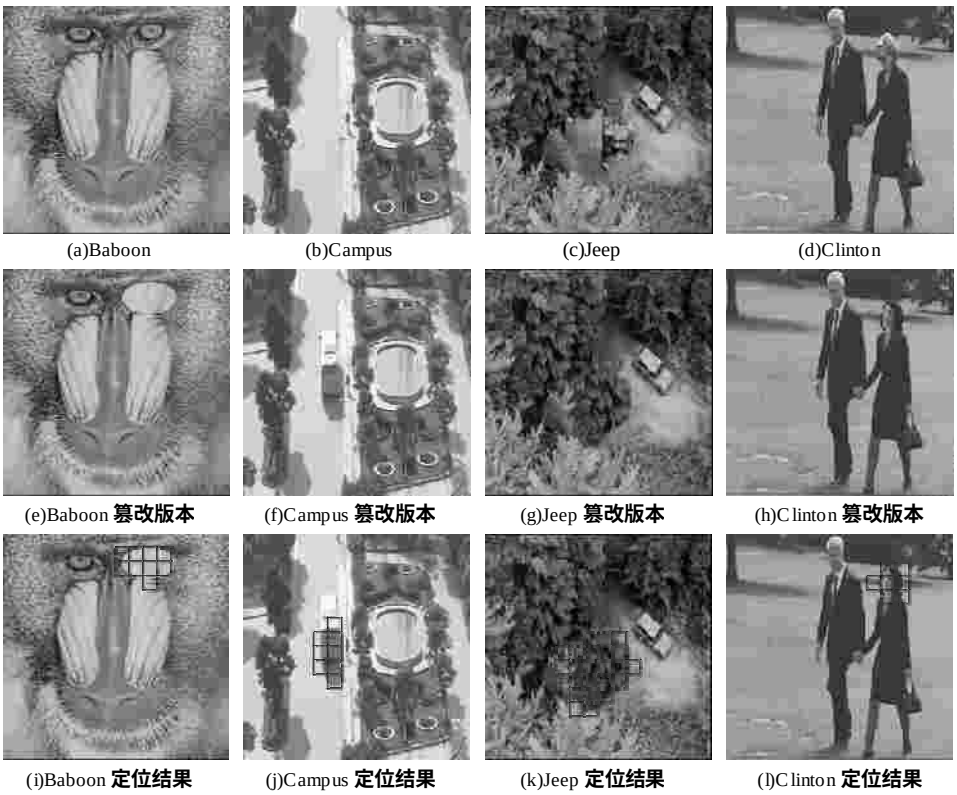
图 7 1 000 幅图像两两间散列距离的分布

其中，G(a)为伽玛函数，a=11.441，b=107.798。由此可计算不同阈值下的冲突概率,以 T_1=45 与常规处理的图像相区分，碰撞概率 2.63×10^{-13}；若以 T_2=500 与局部内容篡改（面积 6.45%~1.87%）的图像相区分，碰撞概率 5.4×10^{-3}。可见该算法抗碰撞性优良。

用本文方法还可定位被篡改区域。如图 8 所示，检测结果中方框标识的块为定位的篡改块。表 2 为检测所得各篡改图像散列与原始图像散列之间的距离，它们都明显高于阈值 45。图 8 及表 2 表明了本文方法的有效性。

表 2 图 7 中篡改图像与原图像散列的距离均大于阈值 45

图像	距离 D
Baboon	167.9
Campus	186.2
Jeep	175.4
Clinton	67.4



(a)Baboon (b)Campus (c)Jeep (d)Clinton

(e)Baboon 篡改版本 (f)Campus 篡改版本 (g)Jeep 篡改版本 (h)Clinton 篡改版本

(i)Baboon 定位结果 (j)Campus 定位结果 (k)Jeep 定位结果 (l)Clinton 定位结果

图 8 测试图像 Baboon、Campus、Jeep 和 Clinton 篡改检测及定位结果

将本文提出的方法与 Wavelet[2]、SVD-SVD[7]、NMF-NMF-SQ[11]比较。用同样的 400 幅图像进行测试，处理类型与图 5 一致，计算处理前后的散列距离。根据文献[2]中的定义，Wavelet 法用归一化距离度量，SVD-SVD 和 NMF-NMF-SQ 用欧氏距离。实验中用双线性插值将图像转换成 256×256，3 种方法具体参数设置如表 3 所示。

表 3　　文献[2,7,11]方法的实验参数

散列方法	参数
Wavelet	三级 dB 4 小波，N=150，量化步长=100
SVD-SVD	p=100，m=64，r=20，d=40
NMF-NMF-SQ	p=10，m=100，r_1=2，r_2=1

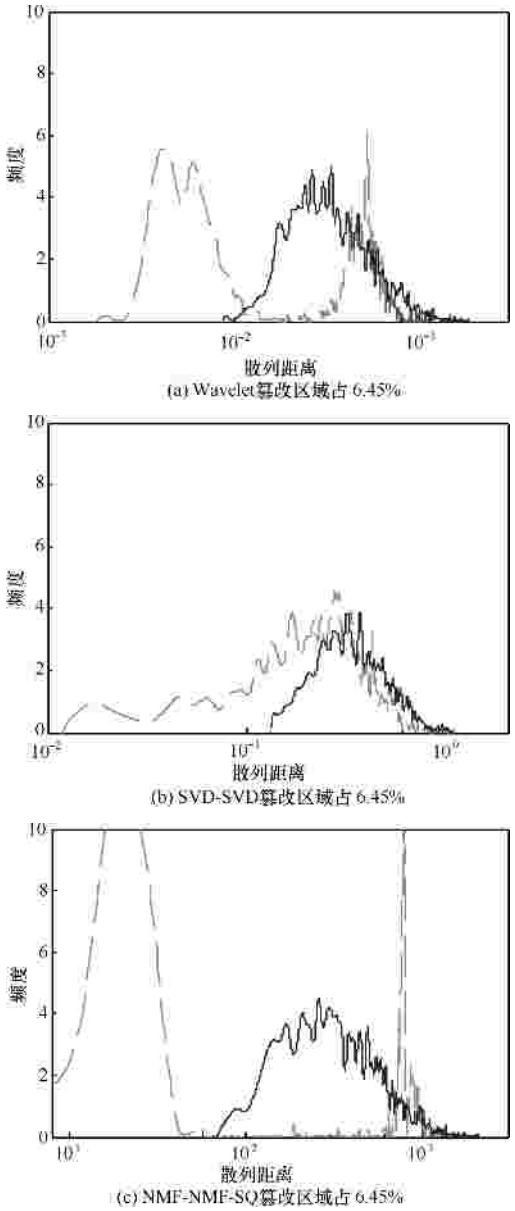


图 9　文献[2,7,11]的方法对常规处理和内容篡改的性能

图 9 分别给出文献中 3 种方法在常规处理和 6.45%内容篡改情况下图像散列距离的分布，每个图中 2 条曲线均重叠，可见都不能检测图像局部区域篡改。本文方法对局部内容篡改很敏感（如图 5 所示），性能优于这 3 种方法。

再与文献[14]和文献[15]比较。文献[14]给出了 2 幅篡改面积达 50%的实例，未给出小面积的篡改的检测结果。在文献[15]中，篡改面积为 10%时将“篡改”误判为“常规处理”的概率高达 60%，而用本文方法，在篡改面积仅有 6.45%时也未发生误判。可见本文方法的性能优于文献[14]和文献[15]。

4　结束语

本文提出的感知散列图像认证方法兼顾了图像内容和颜色特征的分布。对图像尺寸的规格化预处理使生成的散列对缩放稳健。通过将规格化图像分块，并由各块亮度矩阵的奇异值得到反映总体轮廓的结构信息，然后提取块的亮度和颜色特征构成散列。利用各颜色分量之间的相关性选择 R、G、B 均值的最小值为颜色特征，得到了反映图像块颜色的足够信息，同时又有效地压缩了散列长度。对于结合复杂度结构信息和亮度、颜色分布特征的序列进行加密，得最终长度为 3 584bit 的图像散列。

实验表明，用上述方法提取的图像散列对于缩放、JPEG 压缩、行列删除和高斯滤波等常规处理具有良好的稳健性，对局部内容篡改则十分敏感。对小面积篡改的敏感性是本文方法的优势所在。此外，不同图像之间散列发生碰撞的概率极低。同时因为系统中引入了加密环节，所产生的散列满足感知稳健性、抗碰撞性、安全性、对篡改敏感的基本要求，可用于图像防伪认证。

参考文献：

[1] SCHNEIDER M, CHANG S F. A robust content based digital signature for image authentication[A]. Proceedings of Inter ional Conference on Image Processing[C]. Lausanne, Switzerland, 1996. 227-230.

[2] VENKATESAN R, KOON S M, JAKUBOWSKI M H. Robust image hashing[A]. Proceedings of International Conference on Image Processing[C]. Vancouver, BC, Canada, 2000. 664-666.

[3] FRIDRICH J, GOLJAN M. Robust hash functions for digital watermarking[A]. Proceedings of International Conference on Information Technology: Coding and Computing[C]. Las Vegas, USA, 2000. 178-183.

[4] LIN C Y, CHANG S F. A robust image authentication method distinguishing JPEG compression from malicious manipulation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2001, 11(2): 153-168.

[5] MIHCAK K, VENKATESAN R. New iterative geometric methods for robust perceptual image hashing[A]. Proceedings of ACM Workshop on Security and Privacy in Digital Rights Management[C]. Philadelphia, PA, USA, 2001.13-21.

[6] LU C S, LIAO H Y M. Structural digital signature for i ge authentication: an incidental distortion resistant scheme[J]. EEE Transactions on Multimedia, 2003, 5(2):161-173.

[7] KOZAT S S, VENKATESAN R, M K MIHCAK. Robust perceptual image hashing via matrix invariants[A]. Proceedings of International Conference on Image Processing[C]. Singapore, 2004.3443-3446.

[8] MONGA V, EVANS B L. Perceptual image hashing via feature points: performance evaluation and trade-offs[J]. IEEE Transactions on Image Processing, 2006, 15(11):3453-3466.

[9] MONGA V, BANERJEE A, EVANS B L. A clustering based approach to perceptual image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, 15(11):3453-3466.

[10] SWAMINATHAN A, MAO Y, WU M. Robust and secure image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(1): 68-79.

[11] MONGA V, MIHCAK M K. Robust and secure image hashing v non-negative matrix factorizations[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3):376-390.

[12] TANG Z J, WANG S Z, ZHANG X P. Robust image hashing for tamper detection using non-negative matrix factorization[J]. Journal of Ubiquitous Convergence Technology, 2008, 2(1):18-26.

[13] TANG Z J, WANG S Z, ZHANG X P. Structural feature-based image hashing and similarity metric for tampering detection[J]. Fundamenta Informaticae, 2011, 106(1):75-91.

[14] KHELIFI F, JIANG J M. Perceptual image hashing based on virtual watermark detection[J]. IEEE Transactions on Image Processing, 2010, 19(4):981-994.

[15] LEI Y Q, WANG Y G, HUANG J W. Robust image hash in Radon transform domain for authentication[J]. Signal Processing:Image Communication, 2011, 26(6):280-288.

[16] WANG S Z, LU X, SU S J. Image block feature vectors based on a singular-value information metric and color-texture description[J]. Journal of Shanghai University, 2007, 11(3):205-209.

[17] DAEMEN J, RIJMEN V. The Design of Rijndael: AES-the Advanced Encryption Standard[M]. Berlin: Springer-Verlag, 2002.

[18] SCHAEFER G, STICH M. UCID-an uncompressed color image database[A]. Proceedings of the SPIE, Storage and Retrieval Methods and Applications for Multimedia[C]. San Jose, USA, 2004.472-480.

[19] OLMOS A, KINGDOM F A A. McGill calibrated color image database[EB/OL]. http://tabby.vision.mcgill.ca.

[20] PETITCOLAS F A P. Watermarking schemes evaluation[J]. E Signal Processing Magazine, 2000, 17(5):58-64.

作者简介：

倪丽佳（1986-），女，上海人，上海大学硕士生，主要研究方向为图像认证、图像处理。

王朔中（1943-），男，江苏苏州人，上海大学教授、博士生导师，主要研究方向为水声学、图像处理、信息安全。

吴酋珉（1987-），男，上海人，上海大学硕士生，主要研究方向为数字图像认证、图像处理。

裴蓓（1986-），女，上海人，上海大学硕士生，主要研究方向为图像检索。