基于角点检测的稳健图像摘要

金秋明 王朔中 李 茜 张新鹏
(上海大学通信与信息工程学院,上海 200072)

摘 要 图像摘要(Hash)是将数字图像映射为一串短的数,在图像认证、图像内容检索、数字水印等方面有广泛应用。提出了应用 Harris 角点检测和奇异值分解的图像 Hash 算法,首先在图像中选取对灰度变化和旋转稳健的 Harris 角点,对这些稳健特征点周围图像块的奇异值进行量化以实现数据压缩,经编码产生图像 Hash。该算法建立在稳健特征点检测基础上,结合了特征点的位置和周围图像信息,得到的 Hash 对视觉可接受的几何变换、亮度和对比度变化、JPEG 压缩具有良好的稳健性,而大幅度扰动或篡改则会改变 Hash 值。密钥的使用保证了 Hash 的安全性。

关键词 图像摘要 Harris 角点 奇异值分解
中图法分类号:TP309 **文献标识码**:A **文章编号**:1006-8961(2008)08-1454-05

Robust Image Hashing Based on Harris Corners

JIN Qiu-ming, WANG Shuo-zhong, LI Xi, ZHANG Xin-peng
(*School of Communications and Information Engineering*, *Shanghai University*, *Shanghai* 200072)

Abstract Perceptual image hashing maps an image to a short data string, applicable to image authentication, content-based image retrieval, digital watermarking, etc. We propose a new image-hashing algorithm using Harris corners and singular value decomposition. Critical feature points robust against gray-level modification and image rotation are identified. A prescribed number of large singular values of the image blocks centered at the robust feature points are quantized to compress the data, which represent positions of the points and information of their neighborhood. The compressed data are then coded to generate the hash. The obtained hash is stable to visually insignificant changes due to normal image processing and JPEG coding, while sensitive to excessive changes and malicious tampering. Security of the hash is guaranteed by using secret keys.

Keywords image hashing, Harris corner, singular value decomposition (SVD)

1 引 言

在互联网和多媒体技术高度发展的今天,数字图像应用极为普遍。数字媒体内容安全一直是学术界和应用部门广泛关注的重要课题。除了已研究多年的数字水印用于保护知识产权以外,数字图像内容安全的其他方面如防伪认证也受到了研究者的重视。由于数字媒体容易被复制和篡改,需要通过技术手段保证其真实性和可信性。此外,多元化的应用领域和迅速增长的需求使图像检索成为迫切需要解决的问题。本文研究针对图像认证和检索的稳健图像摘要或哈希(Hash)。图像 Hash 是多种图像处理技术和信息安全技术的结合,它是一种映射,通过对图像的特征如颜色、纹理、内容等的分析提取对视觉稳健的特征并进行编码,将图像对应于一个短的代码,例如一定长度的二进制串。图像 Hash 在完整性认证、篡改检测、图像索引、数字水印、网络取证等方面有广泛的应用前景。

密码学中代表性的 Hash 算法有 MD5(message digest 5)和 SHA-1(secure hash algorithm 1),其特点是对明文的修改非常敏感,即使 1 比特的变化也会使

基金项目:国家自然科学基金项目(60502039, 60372090);上海市青年科技启明星计划项目(06QA14022)
收稿日期:2007-02-05;**改回日期**:2007-04-03

第一作者简介:金秋明(1983~),女。上海大学通信与信息工程学院通信与信息工程专业硕士研究生。主要从事图像处理及信息安全研究。E-mail:catherine0898@163.com

Hash 完全改变。这样的 Hash 函数并不适用于图像,因为图像常需进行多种处理,如增强和压缩编码,得到的图像应认为还是原来的图像,不应当导致 Hash 发生重大改变。另一方面,图像被篡改后,应使 Hash 完全改变,以达到防伪认证的目的。因此在图像 Hash 研究中应将注意力放在视觉特性,从数字图像中提取基于视觉的特性,然后进行适当的数据压缩和编码。

至今已提出了许多图像 Hash 算法。早期利用图像 Euclid 距离之和以及分块直方图[1]来表示图像的信息,或利用分块统计量如均值、方差等[2]来表示图像块的信息,所产生的 Hash 缺乏安全性,因为可在块内交换像素位置而不影响 Hash。Venkatesan 于 2000 年提出从图像小波分解的子带中提取统计向量,根据密钥随机分割子带,将量化的统计量输入 Reed-Muller 纠错码的解码器产生 Hash[3]。小波系数的统计特性比灰度更加稳健,但不能很好地反映图像内容,特别是恶意添加或删除的内容。

Fridrich 根据图像的粗略特征提出选择 DCT 低频系数的方案[4],因为它们在保持图像基本内容不变的情况下较为稳健。另一种方法是通过迭代将 3 层 Haar 小波分解的最低频分量二值化来表示图像信息[5]。迭代过程强调几何健壮成分而消除柔弱成分。增大对视觉敏感的频域系数在计算图像 Hash 时的权重可更好地体现视觉特征,提高鲁棒性[6]。

基于 DCT/DWT 的另一种思路不是保持某些变换系数不变,而是寻求系数之间近似不变的关系。例如针对 JPEG 压缩,可提取任何两个 DCT 系数之间的不变关系[7,8]:两个 8×8 块同样位置的系数在 JPEG 压缩前后是否相等的性质保持不变,如不相等它们的大小次序也不变。该方法尽管对 JPEG 是稳健的,但对其他不严重影响视觉效果的攻击却缺乏稳健性。Lu 提出了一种结构式数字签名方法[9]。在 DWT 子带分解中父子节点之间虽不相关,但仍有统计依赖关系。在相邻层次上小波系数的大小之差在多种保持视觉性质的改变后维持不变。寻求这些不变的父子系数对可得到稳健数字签名。Monga 提出用迭代法提取对视觉有意义,并能保持几何关系的特征点,通过量化引入随机性从而提高了抗攻击能力,然后比对原始图像和检测对象特征点的 Hausdorff 距离来检测两幅图像是否一致[10,11]。

考虑到图像中线段端点、角点和曲率半径小的局部具有较好的稳健性,提出一种采用 Harris 角点检测的图像摘要算法。取 Harris 角点周围区域进行统计分析,结合位置和灰度信息得到图像的 Hash 值。该方法基于图像中具有代表性的稳健特征点,并通过奇异值分解提取这些特征点周围的图像信息,具有良好的视觉稳定性和对攻击的敏感性。

2　特征点提取

图 1 是算法框架,由图像特征提取和特征量压缩、编码两部分组成。特征点检测采用 Harris 角点算法,然后根据特征点周围的局部图像数据经压缩生成 Hash。

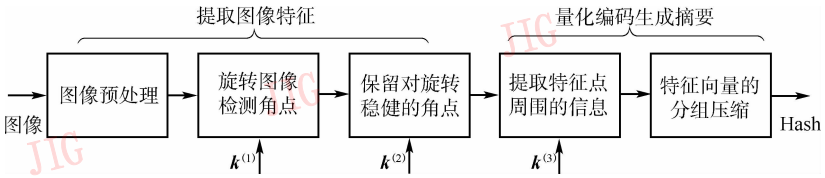


图 1　基于 Harris 角点的图像摘要提取

Fig. 1　Framework of image hashing based on Harris corners

Harris 角点检测是一种基于图像局部区域自相关特性的算法[12,13],由于对旋转、缩放、噪声、亮度变化具有稳健性,故对图像摘要是适用的。考虑一个小窗口 W 和像素位移 $[\Delta x,\Delta y]$,定义局部相关函数:

$$c(x,y) = \sum_{W} [I(x,y) - I(x+\Delta x, y+\Delta y)]^2 \tag{1}$$

式中,$I(x, y)$ 表示像素灰度。Taylor 展开,仅保留一阶项,则局部图像的位移可近似表示为

$$I(x+\Delta x, y+\Delta y) \approx I(x,y) + [I_x(x,y) \quad I_y(x,y)]\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix} \tag{2}$$

下标 x 和 y 分别表示水平和垂直方向的偏微商。于是局部相关函数为

$$c(x,y) = [\Delta x \quad \Delta y]\boldsymbol{C}(x,y)\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix} \tag{3}$$

式中,矩阵 $\boldsymbol{C}(x, y)$ 为

$$\boldsymbol{C}(x,y) = \begin{bmatrix} \sum_{W} [I_x(x,y)]^2 & \sum_{W} I_x(x,y) I_y(x,y) \\ \sum_{W} I_x(x,y) I_y(x,y) & \sum_{W} [I_y(x,y)]^2 \end{bmatrix} \tag{4}$$

令 $\boldsymbol{C}(x, y)$ 的特征值为 λ_1 和 λ_2。若 λ_1 和 λ_2 都很小则为平滑区;λ_1 和 λ_2 一大一小为边缘;λ_1 和 λ_2 都很大即为角点。阈值由实验根据稳健性确定,也可在此引入密钥以提高安全性。

在提取 Harris 角点以前对图像进行的预处理包括低通滤波和直方图均衡,目的是为了提高特征点的稳健性。低通滤波是为了降低高频成分以避免稳健性较差的角点。直方图均衡可看成亮度归一化处理,使提取的特征点不易受反差增强或灰度变换的影响。实际处理中可取小波变换低频分量或将图像下采样后再进行特征点检测以减少计算量。预处理参数和检测 Harris 角点的阈值可在一定范围内由密钥 $\boldsymbol{k}^{(1)}$ 控制。

旋转图像,每隔一定角度检测 Harris 角点,在每个角度都能得到的特征点可认为是稳健的。由密钥 $\boldsymbol{k}^{(2)}$ 控制,保留这些特征点中的一部分用于生成中间 Hash。令保留的 L 个稳健 Harris 角点构成特征点集 H:

$$h_i(x,y) \in \boldsymbol{H} \quad i = 1,2,\cdots,L \tag{5}$$

3 图像摘要算法

在图 1 所示系统的第 2 部分中,由密钥 $\boldsymbol{k}^{(3)}$ 控制,在特征点周围取大小不等的图像块以提取特征向量,再经分组压缩得到最终的 Hash 值。称 $\boldsymbol{H}$ 的重心$[x_0, y_0]$为特征点集的中心。

$$x_0 = \frac{1}{L}\sum_{i=1}^{L} x_i$$

$$y_0 = \frac{1}{L}\sum_{i=1}^{L} y_i \tag{6}$$

计算各特征点到中心的距离。由于离中心较近的区域通常更能反应图像的内容,因此根据到中心的距离由小到大将稳健角点排序。在每个特征点周围定义一个正方形窗口,提取其中像素的统计特性。各窗口的边长 d_i 由密钥 $\boldsymbol{k}^{(3)}$ 所产生的伪随机数 $k_i^{(3)}$ 决定:

$$d_i = \frac{L(M+N)k_i^{(3)}}{\sum_{i=1}^{L} k_i^{(3)}} \qquad i = 1,2,\cdots,L \tag{7}$$

式中,M 和 N 为图像尺寸。由于靠近中心的特征点较密集,为了避免窗口重叠面积过大,使远离中心的窗口较大,所以将 $k_i^{(3)}$ 从小到大排序。由于窗口的具体大小依赖于密钥,因此根据以下方法产生的 Hash 具有良好的安全性,错误的密钥将产生完全不同的 Hash 值。

现在基于奇异值分解(SVD)对所有以稳健角点为中点的正方形块内的图像信息进行压缩和编码。SVD 常被用于特征提取、图像压缩中,因为它反映图像某种内在的不变特征。对图像进行小扰动时奇异值变化不大,转置、旋转、平移、镜像变换后奇异值不变,图像缩放使奇异值以相同倍率改变。一个 $d \times d$ 矩阵 $\boldsymbol{A}$ 的奇异值分解定义如下:

$$\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{V}^{\mathrm{T}} \tag{8}$$

矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 的列向量分别是$(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}})$和$(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})$的特征向量。$\boldsymbol{\Lambda}$ 为 $d \times d$ 矩阵,其前 R 个对角线元素为 $\lambda^{(1)} \geqslant \lambda^{(2)} \geqslant \cdots \geqslant \lambda^{(R)} > 0$,$\lambda^{(n)}$ 是矩阵 $\boldsymbol{A}$ 的奇异值,R 是 $\boldsymbol{A}$ 的秩。前几个奇异值反映图像块的主要特征,在计算 Hash 时仅取前 N 个较大的奇异值($N < R$)组成奇异值向量 $\boldsymbol{S}_i = [\lambda_i^{(1)}, \lambda_i^{(2)}, \cdots, \lambda_i^{(N)}]$ $(i = 1, 2, \cdots, L)$。

由于奇异值 $\lambda_i^{(n)}$ 的取值范围变化较大,因此采用下列方法将它压缩成两位十进制数,其中十位数代表数量级和量化步长,个位数为量化值。

$$\psi_i^{(n)} = 10\lfloor \lg(\lambda_i^{(n)} + 1) \rfloor + [\lambda_i^{(n)} / 10^{\lfloor \lg(\lambda_i^{(n)}+1) \rfloor}]$$
$$i = 1, 2, \cdots, L; n = 1, 2, \cdots, N \tag{9}$$

上式的$\lfloor \cdot \rfloor$表示四舍五入。如 $\lambda_i^{(n)} = 245$,数量级为和量化步长为 $10^2 = 100$,量化值为 2,量化结果为 22;又如 $\lambda_i^{(n)} = 38$,数量级和量化步长为 $10^1 = 10$,量化值为 4,量化结果为 14。

对量化后的奇异值进行编码。将所有 L 个稳健特征点的同序号奇异值编为一组,可得到 N 个长度为 L 的向量:

$$\boldsymbol{\psi}^{(n)} = [\psi_1^{(n)}, \psi_2^{(n)}, \cdots, \psi_L^{(n)}] \quad n = 1, 2, \cdots, N \tag{10}$$

以 $N = 3, L = 6$ 为例,编码情况如表 1 所示。将 $\boldsymbol{\psi}^{(n)}$ 中各元素 $\psi_i^{(n)}$ 减去其中的最小值,将所得结果串接起来,构成 3 个 8 位数 $Z^{(n)}$,其中前两位表示 $\psi_{\min}^{(n)}$。将 3 个 $Z^{(n)}$ 串接就得到所要求的图像 Hash,也可将它转换为 BCD 码然后用游程编码进行无损压缩。

表 1　将量化的奇异值编码得到 Hash

Tab. 1　Encoding the compressed SVD into Hash

n	$\psi^{(n)}$						$Z^{(n)}$	
							$\psi_{\min}^{(n)}$	$\psi^{(n)} - \psi_{\min}^{(n)}$
1	26	24	26	24	24	26	24	202002
2	04	04	02	04	09	11	02	220279
3	01	04	00	01	06	09	00	140169

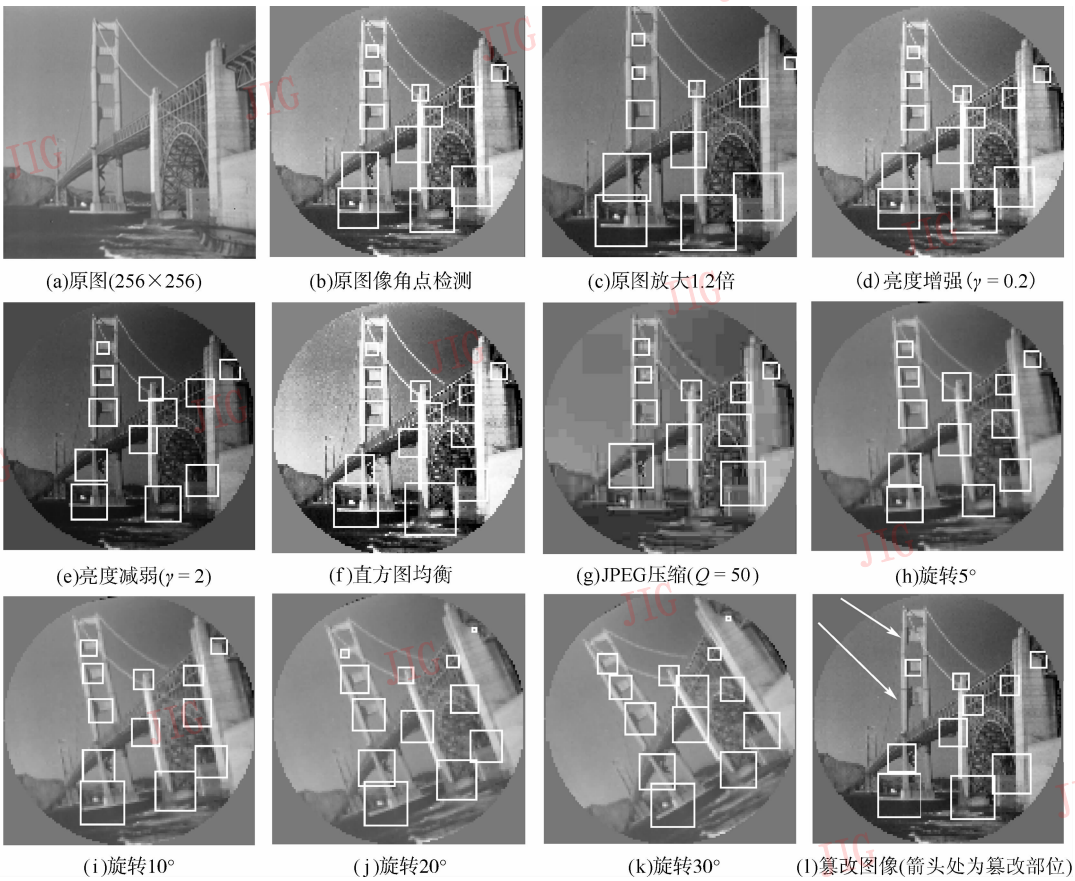
由表 1 可得到 54 比特的 Hash 值。以上编码过程是可逆的,可根据 Hash 求得 N 个量化奇异值向量 $\boldsymbol{\psi}^{(n)}$。对图像进行认证时,可计算待认证图像与原图像 Hash 之间的差异,根据设定的阈值判断真伪。定义两幅图像特征量之间的差异为

$$E = \sum_{i=1}^{L}\sum_{n=1}^{N}\frac{\varphi_i^{(n)}}{\varphi_i^{(1)}}\left|\psi_i^{(n)} - \varphi_i^{(n)}\right| \tag{11}$$

式中,φ 和 ψ 分别表示原始图像和待检测图像特征点周围数据块的奇异值。

4　实验结果

对 55 幅图像进行实验,其中风景 22 幅、人物 22 幅、建筑物 11 幅。以 256 × 256pixel 图像 bridge 为例说明基于 Harris 角点和奇异值编码的 Hash 受各种攻击情况下的性能。经过不同的几何攻击或篡改后的图像以及围绕特征点的正方形窗口如图 2 所示,实验中选取同一密钥来确定窗口大小。



(a)原图(256×256)　(b)原图像角点检测　(c)原图放大1.2倍　(d)亮度增强(γ = 0.2)

(e)亮度减弱(γ = 2)　(f)直方图均衡　(g)JPEG压缩(Q = 50)　(h)旋转5°

(i)旋转10°　(j)旋转20°　(k)旋转30°　(l)篡改图像(箭头处为篡改部位)

图 2　各种情况下的图像特征点和用于提取图像信息的窗口

Fig. 2　Features and windows applied in information extraction under various operations

表 2 列出了图像 bridge 在不同几何攻击或篡改后 Hash 值与原始图像 Hash 值之间的差异,根据 Hash 长度和相对误差和来判别两幅图像视觉上是否可认为是一致的。Hash 的长度是 3 个 $Z^{(n)}$ 长度之和。可见对图像进行一般的亮度改变(图像亮度增强 $\gamma < 1$、图像减弱 $\gamma > 1$)和角度不大的旋转引起的 Hash 改变不大,图像在视觉上并无实质性变化。结合 Hash 长度和 E 值的不同,可反应两幅图像之间的差异。首先,若 Hash 长度不同(特征点数量不同)则认为图像曾被篡改,或者是两幅不同的图像。

实验中对图像关键部位进行篡改,以及进行强度较大的处理如旋转超过 30°、剪切量超过 10%、图像压缩质量因子 Q 小于 20 等都会对 Hash 值产生较大影响,从而检测出与原图像受到了视觉不能接受的攻击。

表 2 各种攻击下的 Hash 性能

Tab. 2 Experiments results under various attacks

	PSNR	Hash 长度	E 值
原图	Inf	33	—
放大 1.2 倍	—	36	0.46
亮度增强(γ = 0.2)	16.1	33	0
亮度减弱(γ = 2)	12.0	33	0
直方图均衡	15.4	36	0.41
旋转 5°	17.8	33	0
旋转 10°	15.7	33	0
旋转 20°	13.7	33	0
旋转 30°	12.6	36	0.41
剪裁 15%	—	42	1.39
JPEG (Q = 95)	43.9	33	0
JPEG (Q = 50)	35.2	36	0.41
JPEG (Q = 10)	29.9	39	0.93
篡改	29.9	39	1.39

注:实验图像 bridge 尺寸为 256×256,取 n = 3

5 结 论

从数字图像中提取的稳健 Harris 角点对于不严重影响视觉效果的改变具有良好的稳定性,将它用于图像 Hash 算法的第 1 阶段。在稳健特征点附近应用 SVD 提取图像特征信息,通过量化进行数据压缩,然后编码实现图像与一个短数字的映射。这种方法提取了图像的主要内容和基本特征,也考虑了特征点的几何位置。实验结果表明,该方法具有抵御一般几何攻击和图像亮度变化的稳健性。对于幅度较大的扰动,该方法给出了明显不同的 Hash 值。

为了保证图像 Hash 的安全性,在算法的不同阶段引入了密钥[14],用以控制 Harris 角点检测中的阈值选取、稳健角点的取舍、图像中代表性窗口的实际尺寸等环节,使 Hash 的检测依赖于密钥,攻击者也难以实施恶意篡改而维持 Hash 不变。进一步将研究对视觉有显著吸引力的特征提取技术和更为有效的数据压缩、编码方法以进一步提高 Hash 性能。

参考文献(References)

1 Schneider M, Chang S F. A robust content based digital signature for image authentication[A]. In: Proceeding of IEEE Conference on Image Processing[C], Lausanne, Switzerland, 1996, **3**:227~230.

2 Kailasanathan C, Naini R S. Image authentication surviving acceptable modifications using statistical measures and k-mean segmentation[EB/OL]. http://citeseer.ist.psu.edu/kailasanathan01image.html.

3 Venkatesan R, Koon S M, Jakubowski M H, *et al*. Robust image hashing[A]. In: Proceedings of Image Processing[C], Vancouver, BC, Canada, 2000, **3**:664~666.

4 Fridrich J, Goljan M. Robust hash functions for digital watermarking [A]. In: Proceeding of IEEE Intevnationac Conference on Information Technology: Coding and Computing[C], Las Vegas, NV, USA, 2000: 178~183.

5 Mihcak K, Venkatesan R. New iterative geometric techniques for robust image hashing[A]. In: Proceeding of ACM Workshop on Security and Privacy in Digital Rights Management[C], Springer Berlin, Heidelberg, 2001: 13~21.

6 Qing Chuan, Wang Shuo-zhong, Zhang Xin-peng. Image hashing based on human vision system[J]. Journal of Image and Graphics, 2006, **11**(11):1678~1681. [秦川,王朔中,张新鹏. 一种基于视觉特性的图像摘要算法[J]. 中国图象图形学报, 2006, **11**(11): 1678~1681]

7 Lin C Y, Chang S F. Generating robust digital signature for image/video authentication[A]. In: Proceeding of ACM Multimedia and Security Workshop[C], Bristol, UK, 1998, 243~246.

8 Lin C Y, Chang S F. A robust image authentication system distinguishing JPEG compression from malicious manipulation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2001, **11**(2): 153~168.

9 Lu C S, Liao H-Y M. Structural digital signature for image authentication[J]. IEEE Transactions on Multimedia, 2003: **5**(2): 161~173.

10 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):3452~3465.

11 Monga V, Banerjee A, Evans B L. A clustering based approach to perceptual image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, **1**(1): 68~79.

12 Harris C, Stephens M J. A combined corner and edge detector[A]. In: Proceedings of Alvey Vision Conference[C], Manchester, UK, 1988: 147~152.

13 Schmid C, Mohr R, Bauckhage C. Evaluation of interest point detectors[J]. International Journal of Computer Vision, 2000, **37**(2): 151~172.

14 Wang S, Zhang X. Attacks on perceptual image hashing[A]. In: Proceedings of 2nd International Conference Technologies & Applications[C], Bail, Indonesia, 2007:199~203.