一种基于视觉特性的图像摘要算法

秦川 王朔中 张新鹏

（上海大学通信与信息工程学院，上海 200072）

摘 要 提出一种基于视觉特性的图像摘要算法，增大人眼敏感的频域系数在计算图像 Hash 时的权重，使得图像 Hash 更好地体现视觉特征，并提高鲁棒性。将原始图像的分块 DCT 系数乘以若干由密钥控制生成的伪随机矩阵，再对计算的结果进行基于分块的 Watson 人眼视觉特性处理，最后进行量化判决产生固定长度的图像 Hash 序列。本算法比未采用视觉特性的算法相比，提高了对 JPEG 压缩和高斯滤波的鲁棒性。图像摘要序列由密钥控制生成，具有安全性。

关键词 图像摘要 人眼视觉特性 图像认证

中图法分类号: TP391 **文献标识码**: A **文章编号**:1006-8961(2006) -

Image Hashing based on Human Visual System

QIN Chuan, WANG Shuo-zhong, ZHANG Xin-peng

(*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072)

Abstract An HVS-based image hashing method incorporating a Watson's sensitivity matrix is proposed. The transform domain matrix composed of 8-by-8 block DCT coefficients of the image are multiplied by *N* matrices that are pseudo-randomly generated with a key, and divided by the periodically extended Watson matrix. By quantization, an *N*-bit image hash is obtained. Compared to some other hashing methods, the HVS-based hash has better robustness against JPEG compression and low-pass filtering. Since a key is used in the algorithm, the hash is hard to be forged.

Keywords image hashing, human visual system (HVS), image authentication

1 引言

随着信息时代的到来和互联网的飞速发展，多媒体数据呈几何级数增长，如何对多媒体数据的真实性和完整性进行认证成为一个亟待解决的问题。传统密码学中基于 Hash 函数的认证过程是：发送方将原始数据及对该数据计算得到与密钥相关的 Hash 序列即消息认证码（message authentication codes, MAC）发给接收方，接收方对收到的待认证数据再次算出 Hash 序列，与收到的原始数据 Hash 序列比较，若相同则通过认证，反之拒绝。但 Hash 对原始数据的每一个比特都非常敏感，改动一个比特也会使 Hash 发生剧烈变化，使其无法通过认证。

图像、音频、视频等多媒体数据不同于文本，它们在经过有损压缩、滤波、旋转等信号处理后，虽然数据的表示发生了变化但其代表的内容并没有变，根据应用要求仍应通过认证，故传统的 Hash 函数并不适用于多媒体数据的内容认证。

本文讨论用于图像认证的 Hashing 算法。数字水印技术虽然也能实现图像认证，但是水印嵌入会降低图像质量，而基于 Hashing 算法的图像认证没

基金项目：国家自然科学基金(60502039, 60372090)；上海市科委基础研究重点项目(04JC14037)；上海市青年科技启明星计划(06QA14022)

收稿日期：2006-06-30；**改回日期**：2006-08-07

第一作者简介: 秦川（1980~ ），男。2002 年获合肥工业大学信号与信息处理专业硕士学位，现为上海大学通信与信息工程学院博士研究生。主要研究方向为数字图像认证、信息隐藏。E-mail:qcme@163.com

有这个不足。一般而言图像 Hashing 算法 H 应满足如下条件：

(1) 图像$\mathbf{I}_1$和$\mathbf{I}_2$相似时$H(\mathbf{I}_1, K)$和$H(\mathbf{I}_2, K)$相同；

(2) 图像$\mathbf{I}_1$和$\mathbf{I}_2$不相似时$H(\mathbf{I}_1, K)$和$H(\mathbf{I}_2, K)$不同；

(3) K_1不等于K_2时，$H(\mathbf{I}, K_1)$和$H(\mathbf{I}, K_2)$不同。

其中K, K_1, K_2为生成Hash过程中使用的密钥。条件(1)说明图像虽然有失真但视觉上仍然相似时，Hash序列不应发生变化，即图像Hashing算法要具有一定的鲁棒性。条件(2)说明图像在发生明显失真或遭受恶意篡改后Hash应发生明显变化。条件(3)说明图像Hash应基于密钥产生，在没有密钥的情况下，攻击者很难伪造Hash并进行认证，即图像Hashing算法应具有安全性。

近年来已有学者对图像Hashing算法进行了研究[1-7]。目前已报道的图像Hashing算法一般流程如图1所示。首先对图像进行特征提取，该过程可基于密钥，且提取的特征应对常用的信号处理具有鲁棒性，然后对特征值进行基于密钥的量化，得到固定长度的序列，作为最终的图像Hash；当图像Hash用于认证时需计算待认证图像的Hash，并与接收到的原始Hash进行比较，若二者的汉明距离小于预先设定的阈值，则通过认证，反之拒绝。

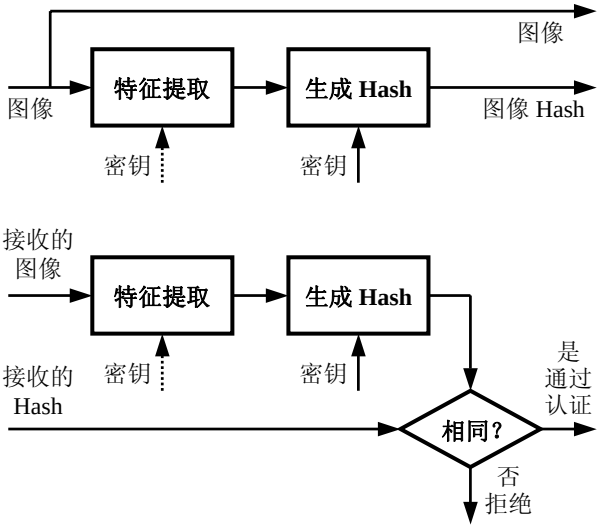


图 1 图像 Hashing 算法流程框图

Fig. 1 Flow chart of hashing algorithm for image authentication

Swaminathan等人给出一种基于Fourier-Mellin变换的图像Hashing算法[1]。该算法首先将图像进行二维Fourier变换，并在极坐标下对每个角度的Fourier系数幅值求和，将结果以密钥产生的随机序列为系数进行线性组合，得到图像特征值即中间Hash，然后量化压缩得到固定长度的图像Hash序列。该算法得到的图像Hash对JPEG压缩和滤波等操作具有鲁棒性，且能够抵抗一定程度的几何失真，并能区分出剪切和替换的恶意篡改操作。

文献[2] 基于原始图像比特平面产生参考图像，根据选定的两个误差参数，保留高位比特平面同时舍弃一些像素的低比特平面，使参考图像能容忍一定程度的失真。对参考图像而不是原始图像进行特征提取并产生最终的 Hash。该方法没有利用密钥计算 Hash，所以不具备安全性，且在认证过程再次计算参考图像特征时需要传送额外信息。

文献[3]在小波域根据密钥将图像各子带伪随机地划分成许多矩形区域，将低频近似子带每个矩形区域系数的平均值和高频细节子带的每个矩形区域系数的方差作为特征值，最后将提取的特征值送入基于密钥的取整量化器，得到最终的图像 Hash。Hash 序列的长度取决于图像大小。

Fridrich[4]指出图像不可能在发生显著变化后仍保持DCT低频系数不变，从而给出一种基于DCT的图像Hashing算法：将图像的DCT系数矩阵分别投影到N个由密钥控制产生并经过低通滤波的光滑随机模板上，通过判断每个投影结果的内积是否大于 0 将其量化成长度为N的二进制序列，作为图像Hash。其中DCT系数矩阵投影到光滑模板得到的是图像的低频特征，有一定的鲁棒性，而模板的生成由密钥控制使得Hashing算法具有安全性。

上述几种图像 Hashing 算法均未考虑到人眼视觉特性（human visual system, HVS）。本文提出在计算图像 Hash 时引入 HVS，使 Hash 能更好地反映图像视觉特征，有效地增强对 JPEG 压缩、滤波等常见信号处理的鲁棒性，该方法还能区分恶意篡改。视觉上完全不同的图像具有显著不同的 Hash，且 Hashing 算法由密钥控制，具有安全性。

后续章节安排如下：第 2 节描述基于人眼视觉特性模型的图像 Hashing 算法；第 3 节给出该算法的实验结果和分析；第 4 节是结论和进一步的工作方向。

2 基于 HVS 的图像 Hashing 算法

从人眼视觉特性来讲，图像中有主要内容和细节之分。一般而言，只要图像的主要内容没有发生变化即可认为图像没有被破坏，可以通过认证，反之拒绝。因而为了使图像 Hash 反映视觉特性，充

分体现图像的主要特征，提高 Hashing 算法对保持图像主要内容不变操作的鲁棒性，本文给出的算法增大人眼敏感的频域系数即图像的主要内容特征在计算图像 Hash 时的权重，较好地体现了视觉特性，增加了 Hash 的鲁棒性。

Watson视觉模型[8]中引入了DCT频率敏感度矩阵$\boldsymbol{m}$，如式(1)。式中的每个元素表示图像分块在没有掩蔽噪声的情况下，对应位置DCT系数可被察觉的最小幅度，这个值越小说明人眼对该频率越敏感，也就是说该频率系数越重要，在频率特征值中占的比例应该越大，因而在计算特征值时可将矩阵$\boldsymbol{m}$中的每个元素的倒数作为对应位置DCT系数的权重。

(1)

我们将原始图像的分块 DCT 系数乘以 N 个由密钥控制生成的伪随机矩阵，再对计算的结果进行基于分块 Watson 人眼视觉特性处理，最后进行量化判决产生 N 比特固定长度的图像 Hash 序列。算法具体步骤如下：

(1) 计算$S_1 \times S_2$图像$\boldsymbol{I}$的 8×8 分块DCT，将每个分块DCT系数矩阵按其在$\boldsymbol{I}$中的对应位置组合，得到与$\boldsymbol{I}$大小相同的矩阵$\boldsymbol{I_C}$，不妨设S_1，S_2均为 8 的整数倍。

(2) 根据密钥K产生与图像$\boldsymbol{I}$大小相同的N个伪随机矩阵，矩阵中的元素互相独立并服从标准正态分布，记为$P_n(i, j)$，其中 $1 \le n \le N$，$1 \le i \le S_1$，$1 \le j \le S_2$。

(3) 求矩阵$\boldsymbol{m}$中每个元素的倒数并乘以常数q = 100 得到$\boldsymbol{m}'$，如式(2)。对$\boldsymbol{m}'$进行周期延拓得到大小为$S_1 \times S_2$的矩阵$\boldsymbol{M}$，将其每个元素作为$\boldsymbol{I_C}$对应位置频率系数在特征值计算中的权。

(2)

(4) 计算

(3)

其中n = 1, 2, … , N。这里不考虑亮度，故在求和时将$\boldsymbol{I_C}$分块位置上的直流系数置 0。

(5) 根据Y_n生成最终的图像Hash序列，其中每一比特由式(4)产生。

(4)

得到的 Hash 序列长度为 N，与图像 $\boldsymbol{I}$ 的尺寸无关，仅与密钥控制生成的高斯模板个数有关。N 值越大 Hash 精度越高，与不同图像 Hash 碰撞的概率就越小，但 Hash 的鲁棒性会降低，因而需要设定合适的 N 值以满足 Hash 在精度和鲁棒性之间的折衷。整个过程均在密钥的控制下完成，使用不同的密钥可得到截然不同的 Hash，攻击者在不知道密钥的情况下无法修改图像而保持 Hash 不变，因而算法具有安全性。

3 实验结果

以 512×512 的标准图像 Lena、Airplane 进行实验，首先计算原始图像的 Hash，系统参数 N 取为 64，即生成的图像Hash长度为64比特。分别在JPEG压缩、低通滤波、剪切替换后及使用错误密钥的情况下计算图像的 Hash，然后与原始 Hash 进行比较，实验结果如图 2 所示。

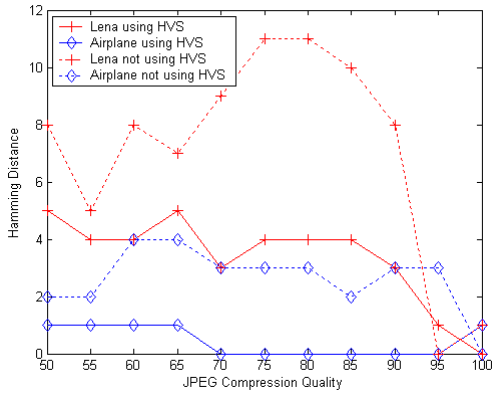
图 2(a), (b), (c), (d)中，纵坐标分别为图像经过 JPEG 压缩、高斯低通滤波、剪切替换及错误密钥计算 Hash 操作后得到的 Hash 序列与原始图像计算出的 Hash 序列的汉明距离。

图 2(a)的横坐标为 JPEG 压缩质量因子，图 2(b)的横坐标表示 3×3 高斯低通滤波掩模的标准差。由图 2(a)和(b)可见采用本文基于 HVS 的 Hashing 算法（图中实线所示）的汉明距离均不超过 5，说明能够容忍 JPEG 有损压缩和低通滤波等保持图像主要内容不变的合理失真。采用本文算法得到 Hash 的汉明距离要小于未采用 HVS 的算法如[4]的方法（图中虚线所示）的汉明距离，表明本文算法提高了 Hash 的鲁棒性。

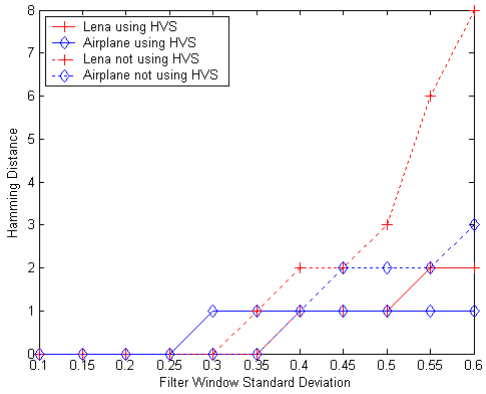
图 2(c)的横坐标为图像被剪切替换像素数占图像总像素数的百分比。由图可知对图像进行较大面积剪切替换的恶意篡改后，得到的 Hash 与原始图

像 Hash 的汉明距离均较大，明显超过 JPEG 压缩和高斯低通滤波等合理失真的情况，因而使用该算法可通过设置合适的汉明距离阈值来判断图像是否经过剪切替换的恶意修改。

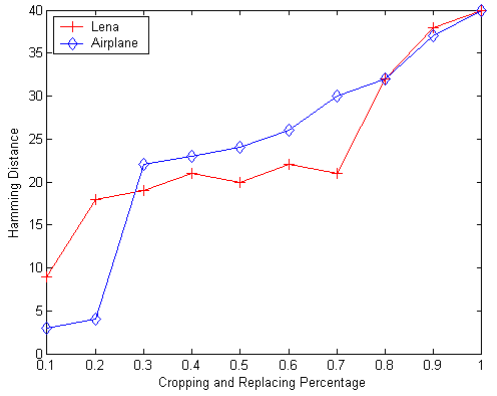
图 2(d)横坐标为不同的错误密钥序号。使用错误密钥得到的图像 Hash 与使用正确密钥得到的 Hash 的汉明距离在 30 左右波动，可见无法得到正确的 Hash 序列，等价于随机猜测，表明本文算法具有安全性。



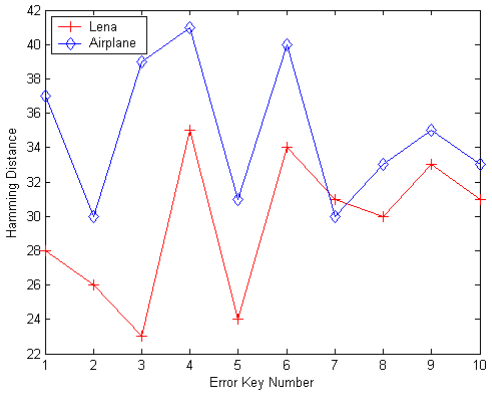
(a) JPEG 压缩后 Hash 的汉明距离



(b) 高斯滤波后 Hash 的汉明距离



(c) 剪切替换后 Hash 的汉明距离



(d) 采用错误密钥 Hash 的汉明距离

图 2 实验结果与比较

Fig. 2 Experimental results and comparison

4 结论

本文给出算法通过引入人眼视觉特性模型有效地提高了 Hash 的鲁棒性，能够容忍 JPEG 有损压缩和高斯低通滤波等合理操作，且可以准确区分出基于剪切替换的恶意篡改。算法生成 Hash 的过程与密钥有关，因而攻击者在不知道密钥的情况下无法伪造 Hash 且不能篡改图像而保持 Hash 不变，因而算法具有安全性。

该算法尚未考虑图像在旋转操作下的鲁棒性。进一步的工作包括设计鲁棒性更好的基于视觉特性的安全图像 Hashing 算法，使算法能抵抗旋转等更多的合理失真。

参考文献 (Reference)

[1] Swaminathan A, MAO Yi-nian, WU Min. Robust and secure image hashing [J]. IEEE Transactions on Information Forensics and Security, 2006, **1**(2): 215 ~ 230

[2] Kobayashi H, Kiya H. Robust image authentication using hash function [A]. In: Proceedings of IEEE Region 10 Conference on Convergent Technologies [C], Chiang Mai, Thailand, 2004, **1**: 435 ~ 438

[3] Venkatesan R, Koon S M, Jakubowski M H, *et al*. Robust image hashing [A]. In: Proceedings of International

Conference on Image Processing [C], Vancover, BC, Canada, 2000, **3**: 664 ~ 666

[4] Fridrich J, Goljan M. Robust hash functions for digital watermarking [A]. In: Proceedings of International Conference on Information Technology: Coding and Computing [C], Las Vegas, Nevada, USA. 2000: 173 ~ 178

[5] Johnson M, Kannan R. Dither-based secure image hashing using distributed coding [A]. In: Proceedings of International Conference on Image Processing [C], Barcelona, Spain, 2003, **2**: 751 ~ 754

[6] 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

[7] Kozat S S, Enkatesan R, Mihcak M K. Robust perceptual image hashing via matrix invariants [A]. In: Proceedings of International Conference on Image Processing [C], Singapore, Republic of Singapore, 2004, **5**: 3443 ~ 3446

[8] Watson A B. DCT quantization matrices optimized for individual images [J]. Proceedings of SPIE Human Vision, Visual Processing, and Digital Display IV, 1993, **1913**: 202 ~ 216