安全鲁棒的图像感知哈希技术

张维克[1] 孔祥维[1] 尤新刚[1,2]

([1] 大连理工大学信息安全中心, 大连 116024)
([2] 北京电子技术应用研究所, 北京 100091)

摘要: 为了对经过图像处理操作的图像内容进行准确认证,利用图像 DCT 低频系数的感知不变性生成了安全的哈希序列索引. 用标准化后的 DCT 低频系数矩阵和基于密钥种子的随机数矩阵为数字图像生成哈希序列,研究分析了提出算法具有唯一性、鲁棒性和安全性的特性. 实验结果表明,算法可以抵抗内容保持的修改操作,例如格式转换、中度几何变换和滤波失真等,具有较强的鲁棒性. 同时算法具有较强的安全性,在同时得到伪随机序列生成器和密钥的情况下,才能获得图像的哈希值. 另外,算法可为视觉近似图像生成相同或相近的 400 比特哈希值,且冲突率降低到 10^{-8} 数量级. 这种安全鲁棒的图像哈希方法可以用于数字图像认证和大量图像的数据库检索.

关键词: 图像哈希;数据库检索;数字签名
中图分类号: TP391 **文献标识码**: A **文章编号**: 1001 - 0505(2007)增刊(I)-0188-05

Secure and robust image perceptual hashing

Zhang Weike[1] Kong Xiangwei[1] You Xingang[1,2]

([1] Information Security Research Center, Dalian University of Technology, Dalian 116024, China)
([2] Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: Secure hash vector index is generated using perceptual invariance of image DCT (discrete cosine transform) low-frequency coefficients to authenticate content of image which has been processed. A hash vector is generated for digital image using the technique of combining standardized DCT low-frequency coefficients matrix with key based random matrix. The proposed algorithm is shown to be unique, robust and secure. Experimental results indicate that the proposed algorithm is able to resist the content-preserving modifications, such as format change, moderate geometric and filtering distortions. One can only acquire hash value of image while having both pseudo-random generator and key. In addition, the proposed algorithm generates same or similar hash value for perceptual same images, length of the hash value is only about 400 bits, and the collision rate decreases to 10^{-8} level. The proposed robust and secure algorithm can be applied to digital image authentication and retrieval of large image database.

Key words: image hashing; database search; digital signature

随着数字技术的广泛应用,大量的数字图像应用在日常生活和工作中. 数字图像满足了人们的感观需要,也为人们的生活工作提供了便利. 但是如何管理、检索经过图像处理软件处理的图像,以及如何保护图像的版权等问题也相继出现. 图像哈希技术可以将任意分辨率的图像数据转化为几百或几千比特的二值序列,对于大量数据库的图像检索来说,这就意味着极大地减少了搜索的时间,也降低了存储图像的介质成本,同时,其鲁棒性的特点保证了它可以抵抗多种不同类型的攻击,该技术可以面向一些在线图像检索和认证的应用. 另外,图像哈希技术安全性的特点使图像的版权保护成为可能:图像哈希函数可以使用一个密钥为图像生成一个数字签名,数字签名被附加或嵌入在图像中,附加了数字签名的图像被发送给接收者,接收者由相同的密钥得到图像的哈希值与数字签名匹配,从而鉴定图像的版权. 对于图像哈希函数,有如下几方面的要求[1]:

1)复杂度:哈希函数的算法应具有较低的计算复杂度.

收稿日期: 2007-07-20.
基金项目: 国家自然科学基金资助项目(60572111).
作者简介: 张维克(1982—),男,硕士生,dlut_vic@hotmail.com.

2)鲁棒性:相同感知的图像具有相同或相近的哈希值. 传统哈希算法(MD5,SHA-1)对信息变动非常敏感,一个比特的信息变化都会造成生成的哈希序列完全不同. 像数字图像这样的多媒体数据可能会经过压缩增强等操作,这些操作虽然改变了图像信息,但并未影响图像的视觉内容. 因此图像哈希算法需要考虑的是图像视觉域的内容信息改变,也就是说相同内容的图像经过哈希函数运算生成的哈希序列应该相同或相近.

3)惟一性:不同感知的图像经过哈希函数处理产生不同的哈希值.

4)安全性:经过不同的密钥加密后,即使是相同的图像也要产生不同的哈希值.

现有的主要图像哈希方法大多围绕鲁棒性这一特性进行研究. 分为基于图像统计的方法[2-4]、图像的粗略表示[1,5]、基于关系的方法[6-7]和视觉特征点提取[8]4 种. 对于基于图像统计的方法,攻击者可以在不改变图像统计特性的情况下任意改变图像内容,因此不具备鲁棒性;图像的粗略表示方法不能抵抗几何攻击,例如旋转和尺寸变换;基于关系的方法仅仅可以抵抗 JPEG 压缩攻击;视觉特征点提取的方法对于图像内容惟一性并未给出证明,而且算法的复杂度较高.

本文提出了一种满足图像内容惟一性,鲁棒性和安全性的折衷方案. 提出了一种用 DCT 低频系数的标准化矩阵和密钥产生的随机块生成哈希序列的方法,并对生成的哈希序列进行了压缩处理. 实验结果表明,本文的算法可以抵抗仿射变换、20% 以下的剪切、JPEG 压缩、中值滤波、噪声叠加、尺度变换、3 度以下的旋转、格式转换等攻击方式,同时,方法兼具安全性和惟一性,在经过压缩处理后的序列长度较短,仅为 400 比特,可以满足实际应用需要.

1　图像感知哈希的基本框架和相关工作

现有的图像哈希生成方案基本按照如下框架进行[9]:

第 1 步对图像进行 DCT 变换、小波变换等处理,提取部分 DCT 系数或小波系数,对提取的特征进行加密处理. 第 2 步对上一步得到的哈希序列进行量化处理. 考虑到上一步得到的特征具有相当多的冗余,因此必须进行量化处理. 第 3 步对量化后的序列进行压缩编码处理. 数字签名或者图像索引都具有序列长度较短的需求,因此还要进行进一步的压缩处理. 特征提取是图像哈希的关键步骤,下面将对现有的一些主要特征提取方法进行概述.

1)基于图像统计的方法

Schneider 使用图像的亮度直方图统计作为特征,该方法的最大缺陷是:攻击者可以在不改变直方图的情况下,改变图像的内容[3]. Kailasnathan 的方案是使用图像像素的均值、方差等统计特性,但是和上一种方法有近似的缺点[4]. Venkatesan 将图像小波分解的不同子带的统计向量作为特征. 他们认为,小波分解的 DC 子带的均值和细节子带的方差具有基于内容的不变性. 虽然小波系数的统计特性比亮度统计特性鲁棒性更强,但也并不能很好地把握图像的内容变化,尤其是恶意攻击后的图像内容改变[5].

2)图像的粗略表示

Fridrich 利用了低频 DCT 系数对于图像内容有重要影响的特性[1]. 这种哈希提取方法对于 JPEG 压缩,噪声叠加,一般的线性锐化和滤波攻击是鲁棒的. 但方法不能抵抗几何攻击,例如旋转和尺寸变换. Mihcak 和 Venkatesan[6]用一种迭代的方法对 3 级 haar 小波分解的 DC 子带进行二值化,进而得到图像的特征. 到底是 DCT 还是 DWT 更好地保存了图像的主要视觉信息目前仍是个不确定的问题.

3)基于关系的方法

这种方法依然利用了 DCT 和 DWT 变换,但与第 2 种方法不同的是,特征选取使用系数间的不变关系而不是变换系数本身. 一种典型的抵抗 JPEG 压缩的方法由 Lin 和 Chang[7]提出. 他们用不同的 8 × 8DCT 块的相同位置的 DCT 系数间的关系作为特征. 但是这种方法的缺点是仅仅可以抵抗 JPEG 压缩攻击. Lu[8]提出了一种用于图像真实性认证的结构化数字签名. 他们发现图像小波分解的父亲节点和孩子节点是不相关的,但是统计上却是不独立的. 最重要的是,他们发现连续尺度的小波系数的幅度差在不改变内容的操作后也相对稳定. 这种方法和 Chang 的方法差别仅仅是将 DCT 域转化到 DWT 域进行处理.

4)视觉特征点提取

Vishal Monga[9]使用小波变换进行图像的角点提取,实验证明,该方法对不改变内容的攻击具有较强

的鲁棒性,但是他对于图像内容惟一性并未给出证明,因此这种方法只能用于图像的真实性证明,而且算法的复杂度较高.

综合现有的方法,我们认为目前还没有任何一种图像哈希方法可以同时保证鲁棒性,安全性,图像内容惟一性,以及低复杂度的特点,下面我们将提出一种全面的基于密钥的图像感知哈希方法.

2 安全鲁棒的图像感知哈希方法

我们的方法也将按照传统的图像哈希生成方法的步骤进行,即特征提取、量化、压缩编码.

2.1 特征提取

在特征提取阶段,哈希生成算法按照如下步骤进行:

步骤 1 原始图像通过插值处理,分辨率统一变为 32×32.

此步骤的目的之一是对于任何分辨率的图像特征长度是固定的,另一个目的是最大程度地减小索引的长度.

步骤 2 将 32×32 的图像分成 16 个 8×8 的小块,对每小块进行 DCT 变换. 将每个小块相同位置的 4 个低频系数(1 个 DC 分量,3 个 AC 分量)分别组成长为 16 的一维向量 A_i,并计算这 4 组向量的数学期望 m_i,和标准差 σ_i,对 A_i 进行标准化得到 $F_i = (A_i - m_i)/\sigma_i$,再将 F_i 串联成长度为 64 的一维向量 F(以上 $i = 1,2,3,4$). 标准化后的 DCT 矩阵相对稳定,能够增强鲁棒性.

步骤 3 由 $f_{sec}(F,k)$ 生成加密后的特征序列:用密钥生成伪随机序列,用伪随机序列将图像分成伪随机的可重叠矩形区域,将这些矩形块变为列向量组成新的矩阵 T, 则加密后的序列 $H_{sec} = F \times T$. 图 1 和图 2 为采用了不同密钥的随机块生成图. 此步骤的目的是引入密钥,使加密后的序列无法破解.

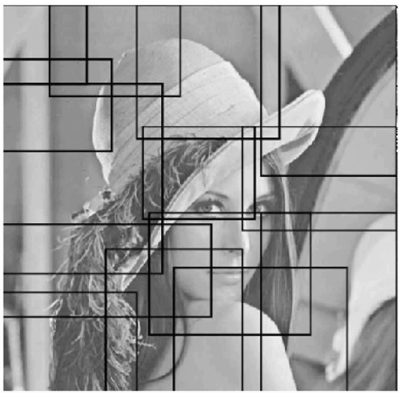

图 1 采用密钥 K_1 的随机块产生图

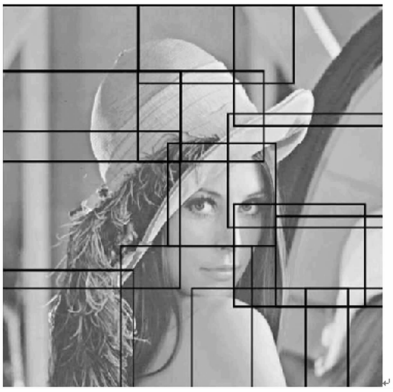

图 2 采用密钥 K_2 的随机块产生图

2.2 量化和压缩编码

步骤 4 量化加密序列 H_{sec}.

将浮点型数据变为二值数据,减少冗余,便于存储.

步骤 5 用 huffman 压缩编码进行压缩,得到最终的哈希值 hash_{origin}.

尽可能地减小哈希序列的长度,以便于应用.

2.3 图像的认证

在认证阶段,按照如下公式计算两哈希序列的距离,即

$$\text{dis} = \text{norm}\frac{|\text{hash}_{new} - \text{hash}_{origin}|}{\sqrt{\text{norm}(\text{hash}_{new})\,\text{norm}(\text{hash}_{origin})}} \tag{1}$$

设定阈值 T,如果 $\text{dis} \leqslant T$,则认为匹配成功;如果 $\text{dis} > T$,则认证失败. 这里的 norm 即 2-范数,也可采用其他的相似度衡量方法.

3 实验结果及性能分析

分别针对此种方法得到的哈希序列进行惟一性、鲁棒性、安全性以及序列长度的实验.

3.1　惟一性实验

首先对冲突下一个定义:冲突就是不同内容的图像产生了近似的哈希值. 实验使用了 1000 张 128 × 128 的彩色 JPEG 图像进行测试,得到 1000 组哈希序列,再对这 1000 组特征进行不同图像的两两匹配,得到 499500 个匹配结果,图 3 为匹配值的统计直方图.

由图4 可以看出,结果可以近似拟合为高斯分布,其中数学期望$\mu = 1.4011$,标准差$\sigma = 0.1549$,我们选用了门限 $T = 0.5$,因此,图像的冲突率为

$$P_F = 1 - \int_T^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(x-\mu)}{2\sigma^2}} dx = 1 - \frac{1}{2}\mathrm{erfc}\left(\frac{T-\mu}{\sigma}\right) = 0.29902e^{-8} \quad (2)$$

由于冲突率极小,因此认为此方法基本可以保证图像的惟一性.

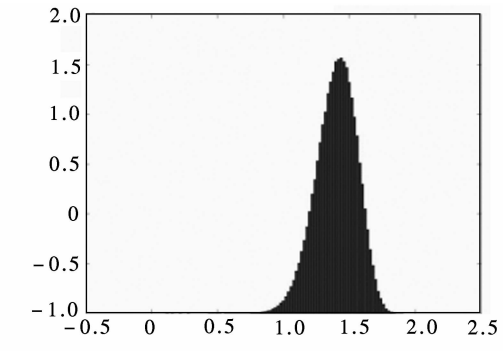

图 3　不同图像匹配值统计直方图

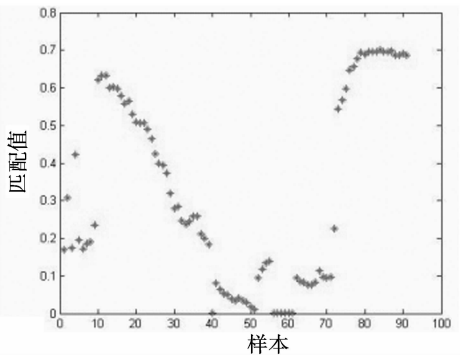

图 4　经图像处理操作后的图像与原图像的匹配图

3.2　鲁棒性实验

在保证了惟一性的前提下,门限应选定为 0.5,为了更具说服力,将门限限定为 0.3. 实验使用 baboon, lena, peppers, fishingboat, f16 标准测试图像作为实验原始图像,用 ACDsee 和 stirmarkbenchmark 处理. 我们分别进行了格式转换,滤波,剪切,比例缩放,JPEG 压缩,叠加噪声,旋转后图像与原图像的哈希序列匹配测试,采用了这几幅图像的匹配值均值作为最终的输出,实验结果见图 5,图中横坐标 1 ~9 为仿射变换,10 ~39 为 1% ~30% 剪切,40 ~51 为 JPEG 压缩,52 ~55 为中值滤波,56 ~60 为叠加噪声,61 ~71 为尺寸变换,72 ~91 为旋转,纵坐标为匹配值. 另外,用 ACDsee 对测试图像进行了格式转换处理,用 bmp 文件与 bmp 格式分别转换为 jpg 和 gif 的图像进行哈希值匹配,匹配结果如表 1 所示.

表 1　不同格式的匹配值

ACDsee 处理	匹配值
bmp 转换为 jpg	0.00141
bmp 转换为 gif	0.08237

从实验数据看得出结论,本算法在保证了图像惟一性的同时,可以抵抗仿射变换,10% 以下的剪切,JPEG 压缩,中值滤波,噪声叠加,尺度变换,3 度以下的旋转等攻击,具有较强的鲁棒性. 同时,也克服了数字水印不能抵抗格式转换攻击的弱点,对于格式转换攻击,此方法具有很好的抵抗效果. 而不能抵抗大角度旋转的原因为:大角度旋转引入了影响图像能量的黑色边框,而我们选用的 DC 分量与能量有关.

3.3　安全性实验

对于分别选用不同密钥后的 1000 组图像进行了不同图像和相同图像间的匹配测试,分别产生 499500 个和 1000 个匹配结果,实验结果如图 6 和图 7 所示.

从图 4 可以看出,所有的匹配值都远远大于阈值 0.5,也就是说无论是否知道密钥,于不同图像产生的哈希序列都不会出现错误匹配的状况. 因此,我们认为,在密钥未知的情况下,即使获得图像,无法进行正确匹配. 即便得到了密钥,也无法得到密钥对应的伪随机序列,也就无法得到图像的哈希值.

3.4　序列长度实验

算法中序列长度由随机块的块数决定,本实验使用了 200 个随机块,因此序列长度达到了 1200bit,如果选用 50 个随机块,哈希序列的安全性会降低,但是哈希序列长度会减少为 300bit,较之原图像,大大减少了存储量,而且此方法不会依据图像的分辨率大小而变化,对于任何图像哈希序列的长度都将固定不变. 对于大量图像数据库应用,我们采用了 huffman 编码对哈希序列压缩,1200bit 的序列可以压缩 400bit 左右.

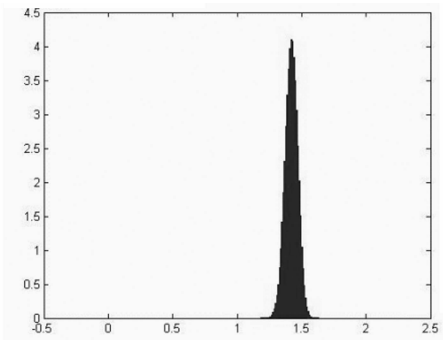

图 6 采用不同密钥的不同图像的匹配值统计直方图

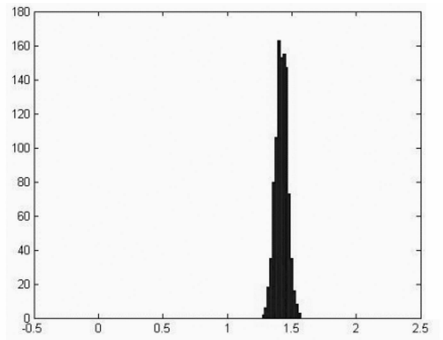

图 7 采用不同密钥的相同图像的匹配值统计直方图

4 结语

提出了一种安全鲁棒的图像哈希生成方法,该方法对于数字图像签名和大量图像数据库检索的应用比较有效,实验结果表明,本文的算法可以抵抗仿射变换,20% 以下的剪切,JPEG 压缩,中值滤波,噪声叠加,尺度变换,3 度以下的旋转等攻击,具有较强的鲁棒性. 同时算法具有较强的安全性,即在密钥未知的情况下,即使获得图像,无法进行正确匹配,即便得到了密钥,也无法得到密钥对应的伪随机序列,也就无法得到图像的哈希值. 这种兼具鲁棒性和安全性的图像哈希算法,可以用于图像的数字签名:图像的接收者通过密钥解密图像的哈希序列,与发送者的哈希值进行匹配,如果匹配成功,则成功地确认了图像的真实性和真实来源. 此外,通过实验证明了每幅图像哈希序列具有惟一性,这就为大量图像数据库检索提供了可能,冲突率达到 10^{-8} 数量级,如果实际应用,还需要减小冲突率. 针对数字水印不能抵抗格式转换攻击的弱点,我们还指出了图像哈希算法完全可以抵抗这种攻击方式,这就为图像的版权保护提出了一种新的途径. 如何进一步增强图像的鲁棒性,降低图像冲突的概率,以及尽可能地减小哈希序列长度,将是下一步的工作.

参考文献 (References)

[1] Fridrich J, Goljan M. Robust hash functions for digital watermarking [C]//*Proc of IEEE Int Conf Information Technology: Coding Computing*. Las Vegas, 2000: 178 - 183.

[2] Schneider M, Chang S F. A robust content based digital signature for image authentication [C]//*Proc of IEEE Conf Image Processing*. Lausanne, Switzerland, 1996, 3: 227 - 230.

[3] Kailasanathan C, Naini R S. Image authentication surviving acceptable modifications using statistical measures and *k*-mean segmentation[C]//*IEEE-EURASIP Workshop Nonlinear Signal and Image*. Baltimore, Maryland, USA. 2001.

[4] Venkatesan R, Koon S M, Jakubowski M H, et al. Robust image hashing[C]//*Proc of IEEE Conf Image Processing*. Vancounver, Canada, 2000: 664 - 666.

[5] Mihcak K, Venkatesan R. New iterative geometric techniques for robust image hashing[C]//*Proc of ACM Workshop on Security and Privacy in Digital Rights Management Workshop*. Paris, 2001: 13 - 21.

[6] Lin C Y, Chang S F. A robust image authentication system distinguishing JPEG compression from malicious manipulation [J]. *IEEE Transaction on Circuits System Video Technology*, 2001, 11(2): 153 - 168.

[7] Lu C-S, Liao H-Y M. Structural digital signature for image authentication [J]. *IEEE Trans Multimedia*, 2003, 5(3): 161 - 173.

[8] Vishal Monga, Brian L Evans. Perceptual Image hashing via feature points: performance evaluation and tradeoffs [J]. *IEEE Transaction on Image Processing*, 2006, 15(11): 3452 - 3465.

[9] Ashwin Swaminathan, Yinian Mao, Min Wu. Robust and Secure Image Hashing [J]. *IEEE Transaction on Information Forensics And Security*, 2006, 1(2): 215 - 230.