中图法分类号:TP391 文献标识码:A 文章编号:1006-8961(2011)08-1374-05
论文索引信息:徐文娟, 易波. 基于离散曲波变换的图像 Hash 算法[J]. 中国图象图形学报,2011,16(8):1374-1378

基于离散曲波变换的图像 Hash 算法

徐文娟,易波
(湖南大学计算机与通信学院,长沙 410082)

摘 要: 为了提高图像 Hash 算法的鲁棒性,提出一种新的基于离散曲波变换的图像 Hash 算法。该算法首先对图像预处理,再进行基于"打包"的快速离散曲波变换,提取出包含图像主要特征的曲波低频系数和边缘信息较丰富的细节 2 层系数作为特征向量;然后用 Logistic 方程对特征向量加密;最后进行量化压缩得到图像 Hash 序列。实验结果表明,该算法与已有传统算法相比,具有更高的鲁棒性;能有效区分不同图像,具有易碎性;混沌系统的引入使算法具有安全性。

关键词: 图像 Hash;曲波变换;图像认证

Image Hash based on discrete curvelet transform

Xu Wenjuan, Yi Bo
(*Shool of Computer and Communication, Hunan University, Changsha* 410082 *China*)

Abstract: In order to improve the robustness of image Hash algorithm a new image Hash algorithm based on discrete curvelet transform is proposed. The image is firstly preprocessed, and then decomposed with discrete curvelet transform via wrapping. The curvelet coefficients of low frequency contained the main features of image and the coefficient of details of two layer contained rich edge information are as the feature vectors. And Logistic equation is used to encrypt the eigenvector. Finally, the image Hash sequence is obtained by quantization and compression. Experimental results show that the algorithm has better robustness compared to some other Hash method. It is fragility to different images. The chaos system enhances the security.

Keywords: image Hash; curvelet transform; image authentication

0 引 言

在信息技术和互联网高速发展的今天,数字图像广泛应用于各个领域。但是如何检索和认证数字图像的问题也日益凸显。图像 Hash 是根据图像的内容特征提取出来的短序列,可广泛应用于内容认证、图像检索(CBIR)、数字水印[1-2]等领域。传统密码学中的 Hash 算法,如 SHA-1 和 MD5,对输入数据的变化非常敏感,即使 1 bit 输入数据变化也会使 Hash 序列完全改变。因此,它适合于文本信息认证。而对于数字图像而言,经常需要进行多种处理,如压缩、滤波、加噪等,虽然图像有失真,但它代表的内容并没有变,这时要求 Hash 序列不应发生较大范围的变化,因此其认证是基于内容的认证。基于内容认证的图像 Hash 函数应满足 3 个条件:鲁棒性、易碎性(敏感性)和安全性。

近年来,已有不少学者对图像 Hash 进行了研究,并提出了一系列相关算法。现有图像 Hash 算法基本都是分 3 步生成 Hash 序列:特征提取、量化、压缩。在这 3 步中最重要的是特征提取,且要求提取的特征对常用的信号处理具有鲁棒性。现有的特征

收稿日期:2010-08-10;**修回日期:** 2010-10-13

第一作者简介:徐文娟(1985—),女。湖南大学计算机与通信学院信息与通信工程专业硕士研究生,研究方向为图像认证技术、多媒体信息安全。E-mail:xuwenjuan2005@163.com。

提取方法大致可分为以下 4 类:基于图像统计的方法、基于粗略特征描述的方法、基于关系对的方法、基于低层图像特征的方法。Venkatesan 提出在小波域内提取图像统计特征[3],虽然小波系数统计特性较稳健,但不能很好的反映图像内容,因此抵抗攻击的能力有限。Fridrich 等人提出基于 DCT 的图像 Hash 算法[4],使用 DCT 低频系数生成 Hash 值,该算法对滤波操作具有稳健性,但对几何扭曲效果不佳。Swaminathan 等人提出基于 Fourier-Mellin 变换的图像 Hash 算法[5],该算法对 JPEG 压缩和滤波等操作具有稳健性,能抵抗中度几何失真,但算法复杂度较高。Lu 等人提出一种利用图像小波变换后系数间存在的关系生成鲁棒 Hash 方案[6],这种方法可实现图像的多尺度认证,并能对恶意篡改进行定位,但对全局变换和局部几何扭曲很敏感。Monga 等人[7]使用小波变换对图像的角点进行提取,该算法具有很好的鲁棒性,但复杂度较高。

目前图像 Hash 算法涉及的变换域主要是 DCT 域、小波域和傅里叶域,并未考虑利用新一代多尺度分析方法——曲波变换来提取图像的特征。在表示具有点奇异性的目标函数时,小波基是最优基,而在表示图像的边缘时,小波基和傅里叶基均不是最优基。为此,Candes 和 Donoho 提出第 1 代曲波(curvelet)变换[8]和第 2 代曲波变换[9]。曲波变换适合于表达曲线信息和边缘细节信息,考虑到自然图像中包含大量的纹理特征信息,线奇异性和曲线奇异性表现非常突出,提出一种基于快速离散曲波变换的图像 Hash 算法,增强了对 JPEG 压缩、滤波、噪声、剪切、旋转、仿射变换等常见信号处理的鲁棒性;能够区分内容不同的图像,具有易碎性。Hash 序列由密钥控制生成,具有安全性。另外,在算法复杂度方面,由于曲波采用尺度、角度、位置的划分,一次分解就可以得到全部系数,相比基于小波变换和傅里叶变换的图像 Hash 算法,基于曲波变换的 Hash 算法的实现效率更高。

1　曲波变换

新兴的曲波变换理论、脊波变换理论和经典的小波变换理论均属于稀疏理论的范畴,都是采用基函数与信号(函数)的内积形式实现信号(函数)的稀疏表示[8-9],从而曲波变换可表示为

$$c(j,l,k) := \langle f,\varphi_{j,l,k}\rangle \tag{1}$$

式中,$\varphi_{j,l,k}$ 表示曲波函数,j,l,k 分别表示尺度、方向、位置。

曲波变换在频域内实现,采用频域中的窗函数 U 来实现曲波 φ 在频域中的表示,令 $\hat{\varphi}(w) = U(w)$,U 定义为

$$U = WV \tag{2}$$

式中,W 和 V 分别是径向窗函数和角度窗函数,并且都满足允许条件。因此,U 的支撑区间是受 W 和 V 支撑区间限制获得的楔形区域。

定义尺度为 2^{-j},方向为 θ_l,位置为 $x_k^{(j,l)} = R_{\theta_l}^{-1}(k_1\cdot 2^{-j},k_2\cdot 2^{-j/2})$ 的曲波为

$$\varphi_{j,l,k}(x) = \varphi_j(R_{\theta_l}(x - x_k^{(j,l)})) \tag{3}$$

式中,R_θ 表示以 θ 为弧度的旋转量,R_θ^{-1} 是 R_θ 的逆。则曲波变换可表示为

$$c(j,l,k) := \langle f,\varphi_{j,l,k}\rangle = \int_{R^2} f(x)\,\overline{\varphi_{j,l,k}(x)}\,\mathrm{d}x \tag{4}$$

根据帕塞瓦尔定理,由式(4)可得

$$c(j,l,k) := \frac{1}{(2\pi)^2}\int \hat{f}(w)U_j(R_{\theta_l}w)e^{i\langle x(j,l)k,w\rangle}\mathrm{d}w \tag{5}$$

曲波变换由于考虑了尺度、位置、角度信息而使其在对图像中的边缘,如曲线、直线等几何特征表达时优于小波。如果采用逼近误差衡量稀疏表示的效果,假设 f 是沿 C^2 边缘不连续的函数,f_m^C 是曲波变换后 m 个最大的曲波系数对 f 的逼近值,同样 f_m^W 和 f_m^F 是分别经小波变换和傅里叶变换后的逼近值,则

$$\begin{aligned}
&\|f - f_m^C\|_{L^2}^2 \approx C\cdot(\log m)^3\cdot m^{-2} \quad m\to\infty\\
&\|f - f_m^W\|_{L^2}^2 \approx m^{-1} \quad m\to\infty\\
&\|f - f_m^F\|_{L^2}^2 \approx m^{-1/2} \quad m\to\infty
\end{aligned} \tag{6}$$

式(6)从理论上证明了曲波变换要比传统的傅里叶变换、小波变换的逼近误差达到更好的误差衰减级,可以更好地解决沿 C^2 边缘不连续图像的最优稀疏表示问题。因此,相比傅里叶变换和小波变换,利用曲波变换提取的图像特征应具有更高的鲁棒性。

文献[9]介绍了两种快速离散曲波变换(FDCT)算法,第 1 种是基于非等间快速傅里叶变换(USFFT)的快速离散曲波变换算法;第 2 种是基于打包(wrapping)的快速离散曲波变换算法。这两种算法的输出结果相同,但是后者的运算速度比较快,算法效率高,因此,采用第 2 种算法。

2 基于 FDCT 的图像 Hash 算法

2.1 图像鲁棒特征提取

使用基于 Wrapping 的快速离散曲波变换得到图像的概貌层(低频层)、细节层、高频层的系数。概貌层包含图像的主要特征,具有较强的鲁棒性,但曲线特征不明显。而细节 2 层的曲线特征明显,包含图像主要的边缘信息。图 1(b)是使用概貌层和细节 2 层系数重构的图像,可以看出,图(b)包含图像主要的特征,且边缘信息丰富。因此,本文使用概貌层和细节 2 层系数作为图像的特征向量。首先提取出低频层系数 $\boldsymbol{C}_1$ 和细节 2 层系数 $\boldsymbol{C}_2$, 低频系数为 $p \times p$ 矩阵,经变换后形成 $1 \times p^2$ 的子特征矩阵 $\boldsymbol{D}_1$。而细节 2 层的维数很高,为了降低维数,可根据细节 2 层频域角度的划分分块(设细节 2 层频域角度的划分个数为 z),取每块的均值 $M(v)$ 和方差 $\sigma(v)(v = 1,2,3,\cdots,z)$ 分别作为子特征向量 $\boldsymbol{D}_2$ 和 $\boldsymbol{D}_3$。

(a) 原始图像 (b) 重构图像

图 1 原始图像与重构图像

Fig. 1 The original image and the reconstructed image

2.2 Hash 序列的生成方法

Hash 值的生成步骤主要包括预处理、特征提取,以及后处理,具体流程如下。

1)图像预处理:设原始图像 $\boldsymbol{I}$ 大小为 $n \times n$, 首先将图像统一变成灰度图像,再进行低通滤波,然后用双 3 次插值的方法将分辨率统一为 $m \times m$, 使最终的图像 Hash 序列长度统一,最后对图像进行直方图均衡化。

2)图像鲁棒特征提取:对预处理后的图像采用基于 Wrapping 的 FDCT 进行 s 层分解,提取出包含图像主要特征的曲波低频系数 C_1(维数为 $p \times p$)和边缘信息丰富的细节 2 层系数 C_2(频域角度的划分个数为 z)。将矩阵 $\boldsymbol{C}_1$ 转化为 $1 \times p^2$ 的子特征矩阵 $\boldsymbol{D}_1$, 按细节 2 层频域角度的划分分块,取 $\boldsymbol{C}_2$ 每块的均值 $M(v)$ 和方差 $\sigma(v)(v = 1,2,3,\cdots,z)$ 分别作为子特征向量 $\boldsymbol{D}_2$ 和 $\boldsymbol{D}_3$。

3)加密:根据混沌区数据的迭代不重复性和初值敏感性,用 Logistic 方程作为混沌序列发生器进行加密,其数学表达式为

$$x_{n+1} = \mu x_n(1 - x_n) \tag{7}$$

式中,μ 为常数,$\mu \in (3.569\,945,4]$,$x_n \in (0,1)$。由密钥产生加密序列,用此序列对子特征向量 $\boldsymbol{D}_1$, $\boldsymbol{D}_2$ 和 $\boldsymbol{D}_3$ 进行加密,得到加密后的特征向量 $\boldsymbol{E}_1$,$\boldsymbol{E}_2$ 和 $\boldsymbol{E}_3$。

4)量化压缩:选定 3 个量化阈值分别对子特征向量 $\boldsymbol{E}_1$,$\boldsymbol{E}_2$,$\boldsymbol{E}_3$ 进行二值化得序列 $\boldsymbol{H}_1$,$\boldsymbol{H}_2$,$\boldsymbol{H}_3$。

$$H_j(i) = \begin{cases} 0 & \boldsymbol{E}_j(i) < t_j \\ 1 & \boldsymbol{E}_j(i) \geqslant t_j \end{cases} \tag{8}$$

式中,$j = 1,2,3$, 当 $j = 1$ 时,$i = 1,2,3,\cdots,p^2$; 当 $j = 2$ 或 3 时,$i = 1,2,3,\cdots,z$。

选用不同的阈值 t_j 得到的 $\boldsymbol{H}_j$ 不同,本文算法中的 $t_j = \mathrm{mid}(\boldsymbol{E}_j)$, 取中值能确保 $\boldsymbol{H}_j$ 中 0 和 1 几乎等概率出现,使 Hash 序列具有一定的伪随机性。最终的 Hash 序列 $h(I) = (\boldsymbol{H}_1,\boldsymbol{H}_2,\boldsymbol{H}_3)$, 序列长度 $l = p^2 + 2z$。

2.3 图像认证方法

认证阶段按如下步骤进行:

1)将接收到的图像 $\boldsymbol{I}'$ 按 Hash 序列的生成步骤 1)—4)生成哈希值 $h(\boldsymbol{I}')$;

2)计算 $h(\boldsymbol{I})$ 和 $h(\boldsymbol{I}')$ 之间的标准汉明距离 d;

3)设定阈值 τ, 如果 $d \leqslant \tau$, 则通过认证;如果 $d > \tau$, 则认证失败。

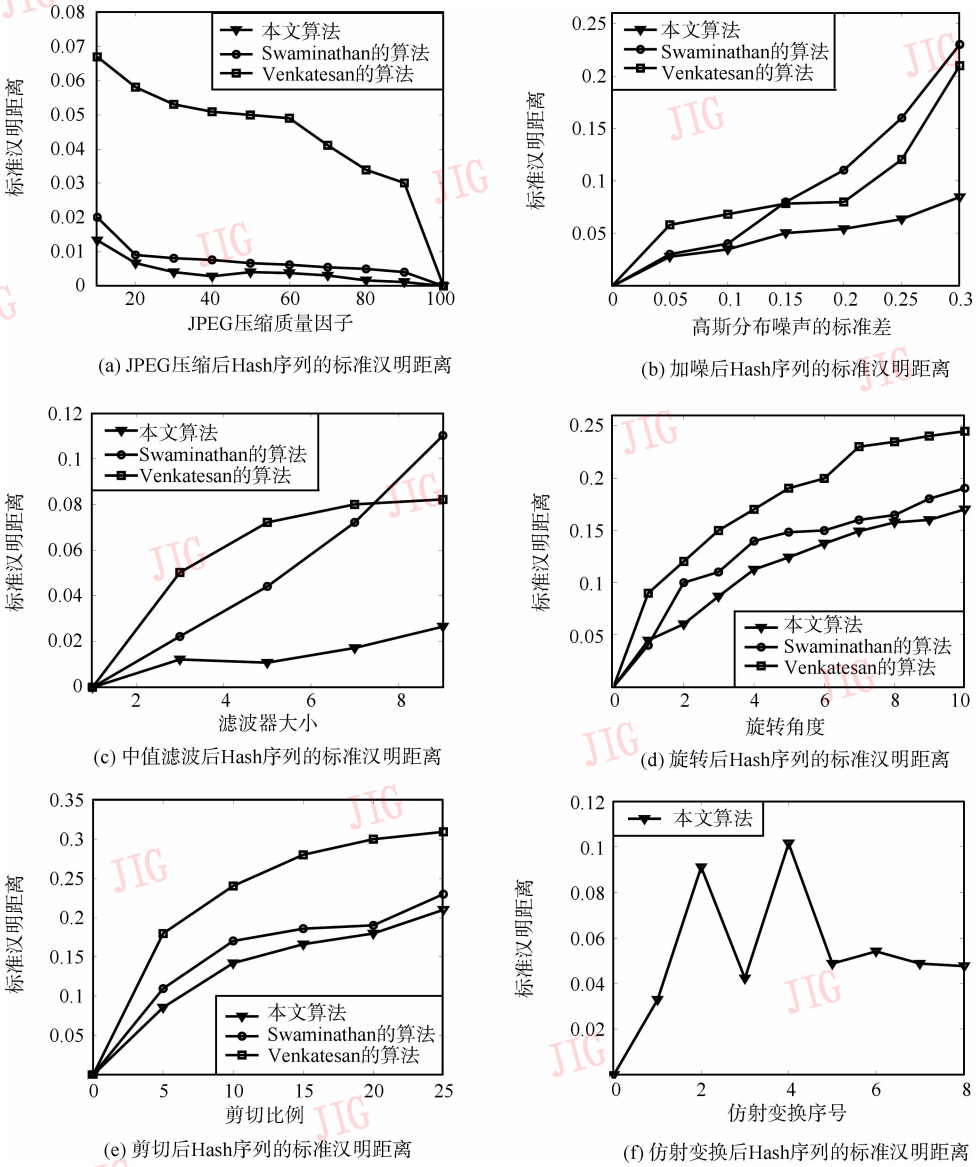
3 实验结果及性能分析

实验中以 512 × 512 大小的标准测试图像 Lena、Peppers、Baboon 作为输入图像,预处理时将图像分辨率统一为 128 × 128, 曲波分解中的参数分别设置为 $s = 4$,$p = 21$,$z = 32$, 混沌系统的初始条件定为 $\mu = 3.92$,$x_1 = 0.32$, 阈值 $\tau = 0.2$, 序列长度 $l = 505$。对本文算法分别进行鲁棒性、安全性及易碎性实验。

3.1 鲁棒性实验

为了对算法的鲁棒性进行评估,将本文算法与已存在的两种比较典型的算法,Venkatesan 的算法[3] 和 Swaminathan 的算法[5] 进行比较。用 StirMark4.0 对各测试图像进行各种内容保持的修改操作,如 JPEG

压缩、加噪、滤波、带剪切的旋转、剪切、仿射变换等,计算操作前后 3 种算法下图像 Hash 算法的平均标准汉明距离,实验结果如图 2 所示。通过曲线可以看出,本文算法在 JPEG 压缩、标准差小于 0.3 的高斯分布噪声、中值滤波、角度小于 10°的旋转、20%以下的剪切、仿射变换等操作下,标准汉明距离基本都小于 0.2。根据此实验结果,可取阈值 τ 为 0.2。通过与其他两种算法的比较可以看出,基于曲波变换的图像 Hash 算法的鲁棒性均优于基于傅里叶变换和基于小波变换的算法。对于 JPEG 压缩,由于曲波变换更好地提取了图像的鲁棒特征,因此比傅里叶域和小波域算法的鲁棒性好。本文算法在预处理阶段进行了低通滤波,所以能很好的抵抗噪声攻击和中值滤波。由于曲波细节 2 层系数具有方向性的特点,本文算法能抵抗大角度旋转攻击。曲波低频系数包含了图像的主要特征,具有较强的鲁棒性,细节 2 层包含了图像的边缘信息,该算法能抵抗 20% 以下的剪切操作。另外,其他两种算法不能抵抗仿射变换,而本文算法能够抵抗仿射变换。因此,本文算法提高了图像 Hash 的鲁棒性。



(a) JPEG压缩后Hash序列的标准汉明距离　(b) 加噪后Hash序列的标准汉明距离

(c) 中值滤波后Hash序列的标准汉明距离　(d) 旋转后Hash序列的标准汉明距离

(e) 剪切后Hash序列的标准汉明距离　(f) 仿射变换后Hash序列的标准汉明距离

图 2　鲁棒性实验结果与比较

Fig. 2　The comparision of robustness experimental results

3.2 安全性实验

本算法的密钥是混沌系统的初值 x_1 和参数 μ，图 3 给出了对于标准测试图像 Lena、Peppers 和 Baboon，改变混沌系统初值 x_1 所引起的图像 Hash 的标准汉明距离，密钥的改变幅度以 10^{-5} 为单位。由图 3 可看出，由于混沌系统对初值的敏感性，初值改变 10^{-5}（如 0.32 变为 0.320 01）所引起的标准汉明距离都在 0.27 以上。因此，攻击者在不知道准确密钥的情况下，很难伪造 Hash 序列，算法具有安全性。另外，攻击者在不知道参数 μ 取值的情况下，也无法得到 Hash 序列，这进一步保证了算法的安全性。

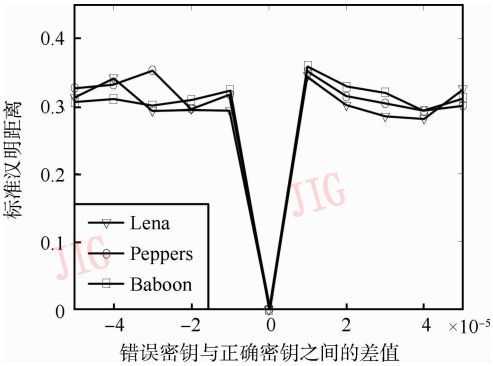


图 3 安全性实验结果

Fig. 3 Security experimental results

3.3 易碎性实验

通过计算测试图像 Lena、Peppers 和 Baboon 之间的标准汉明距离来分析算法的易碎性，不同图像间的标准汉明距离越大，算法的易碎性越高。从表 1 可以看出，不同图像之间的标准汉明距离基本都在 0.29 以上，可以区分内容不同的图像。因而算法具有敏感性。

表 1 测试图像之间的标准汉明距离

Tab. 1 The normalized Haming distance of different images

图像	Lena	Peppers	Baboon
Lena	0	0.356 4	0.340 6
Peppers	0.356 4	0	0.292 1
Baboon	0.340 6	0.292 1	0

4 结 论

提出一种新的基于快速离散曲波变换的图像 Hash 方案，从曲波域中提取图像鲁棒特征并加密，再经过量化压缩得到最终的 Hash 序列。实验结果表明，相比小波域和傅里叶域的图像 Hash 算法，曲波域的 Hash 算法具有更高的鲁棒性，能抵抗大部分内容保持的修改操作。密钥的使用保证了算法的安全性。对于内容不同的图像，算法具有敏感性。另外，由于一次曲波变换就可以得到全部曲波系数，进而得到图像鲁棒特征，因此算法的实现效率较高。

该算法尚未考虑小范围篡改操作下的易碎性，进一步的研究工作将同时结合曲波变换和小波变换的优点来提取图像的鲁棒特征，以及使用更为有效的数据压缩方法以进一步提高图像 Hash 的性能。

参考文献(References)

[1] Zhang C, Cheng L L, Qiu Z D, et al. Multipurpose watermarking based on multiscale curvelet transform[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(4): 611-619.

[2] Fouad Khelifi, Jiang Jianmin. Perceptual image hashing based on virtual watermark detection[J]. IEEE Transactions on Image Processing, 2010, 19(4): 981-994.

[3] Venkatesan R, Koon S M, Jakubowski M H, et al. Robust image hashing[C]//Proceedings of IEEE International Conference on Image Proecssing. Vancouver BC, Canada: IEEE Signal Proessing Society, 2000: 664-666.

[4] Fridrich J, Goljan M. Robust Hash functions for digital watemarking[C]//Proceedings of IEEE International Conference on Information Technology: Coding and Computing. Las Vegas, Nevada, USA: IEEE Computer Society, 2000: 178-183.

[5] Swaminathan A, Mao Yinian, Wu Min. Robust and secure image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 215-230.

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

[7] 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.

[8] Candes E J, Donoho D L. New tight frames of curvelets and optimal representations of objects with C^2 singularities[J]. Commu on Pure and Appl Math, 2004, 57(2): 219-266.

[9] Candes E J, Demanet L, Donoho D L, et al. Fast discrete curvelet transforms[J]. Multiscale Modeling and Simulation, 2006, 5(3): 861-899.