一种新的抗几何攻击的图像认证算法

张汗灵,黄 胜
ZHANG Han-ling,HUANG Sheng

湖南大学 计算机与通信学院,长沙 410082
College of Computer and Communication,Hunan University,Changsha 410082,China
E-mail:husraul@hotmail.com

ZHANG Han-ling,HUANG Sheng.Novel image authentication robust to geometric transformations.Computer Engineering and Applications,2008,44(12):192-195.

Abstract: Robustness against geometric distortion is one of the most important problems in image authentication.In this paper,an image watermarking algorithm robust to geometric transformations is proposed,Radon transformation of edge image is used to detect and invert geometric transformations,then a perceptual hash feature detector is proposed to extract significant geometry preserving feature points,finally compare features from two images by developing a modified Hausdorff distance measure.The experimental results show that the algorithm is robust to image processing,such as JPEG compression,common signal processing operations,global as well as geometric transformations,and it is sensitive to content changing manipulations of image data.

Key words: Radon transformation;perceptual hash;modified Hausdorff distance;authentication

摘 要:提高图像抗几何攻击的能力是当前图像认证算法待解决的重点之一。提出了一种抗几何攻击的图像认证算法,该算法利用图像边界的 Radon 投影变换来实现图像几何失真的矫正,根据感知 hash 方法提取图像的特征点,并通过修正 Hausdorff 距离来实现对图像的认证。实验表明,该算法可以抵抗一定程度的 JPEG 压缩、叠加噪声等图像处理,也能抵抗旋转、缩放等几何变换,并且对于恶意篡改具有较好的敏感性。

关键词: Radon 投影变换;感知 hash;修正 Hausdorff 距离;认证算法
文章编号:1002-8331(2008)12-0192-04 **文献标识码:**A **中图分类号:**TP391

1 引言

随着多媒体和因特网的发展,如何在网络环境中保护多媒体信息的完整性和真实性,是当前面临的一个严峻的现实问题。目前的研究中,多媒体认证已经被认为是保护信息完整性的最有效的手段,其中图像是应用最广的信息载体,所以如何对图像进行认证是当前研究的热点。现在研究中,图像认证包括有脆弱水印和半脆弱水印,脆弱水印要求图像不能经过任何的修改,而半脆弱水印允许图像可以丢失一些不重要的信息。由于图像在网络传输中不免要经历 JPEG 压缩等对图像质量没有影响的失真,如果运用脆弱水印就会造成认证的失败,但此时图像并未被恶意篡改,显然这样的结果是不合理的,比较两种水印的特性,半脆弱水印无疑更符合在现实网络中应用,当前应用于图像认证的半脆弱水印算法有多种,其中一个重要方面是基于 hash 的算法。

由于 hash 函数本身的特性,基于 hash 的水印算法主要应用脆弱水印方面,在半脆弱水印方面应用比较少,主要有下面三种方法:(1)通过保存图像 DCT 或 DWT 变换的低频分量,在低频信息中寻找具有强几何特性的特征点来进行认证,文献[1] K.Mihcak and R.Venkatesan 提出的一种基于小波的图像 hash 算法,通过小波三级分解得到 DC 分量,在 DC 子带中提取具有强几何特性的特征点;文献[2]J.Fridrich 提出选择 DCT 系数来保存的鲁棒 hash 算法,但这些算法对经滤波处理后的图像认证效果并不是很理想。(2)利用图像的相关性的方法,文献[3,4] Lin and Chang 通过两变换系数间的不变关系来认证,这种算法对 JPEG 压缩具有较好的鲁棒性,但对于其他的图像处理依然比较脆弱。(3)文献[5]中 Monga 提出一种通过提取一种有较好鲁棒性的特征点来实现图像感知的 hash 算法,但其对于是否篡改的图像分辨率不是很高。上面文献提到的方法除以上的不足之外,还有一个共同的缺点,就是不具备任何抗几何攻击的能力。在实际应用中,数字图像经常会出现旋转和缩放等几何变换,如何让这类图像通过认证是目前研究待解决的问题。

为了解决上述问题,本文提出一种利用图像边界 Radon 投影变换[11]纠正图像几何失真的、基于感知 hash 的图像认证算法,并在文献[5]的认证算法基础上提出修正的 Hausdorff 距离对图像进行认证,提高了图像的认证效果,同时增强了其抵抗几何攻击的能力。

2 几何失真纠正

本算法是通过图像边界的 Radon 变换来实现图像几何失真矫正,首先用边界检测定位图像的边界,采用图像边界增强

作者简介:张汗灵(1968-),男,博士,副教授,主要研究方向为信号处理,图像处理,信息隐藏等;黄胜(1982-),男,硕士研究生,主要研究方向为图像处理,数字水印。

收稿日期:2007-08-10 **修回日期:**2007-11-26

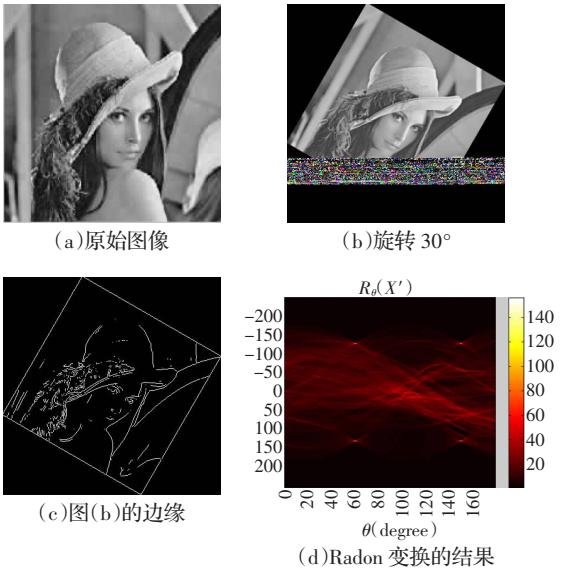
算子“sobel”来提取图像的边缘信息。Radon 函数是用于计算图像数据矩阵沿指定方向的投影，而函数 $f(x,y)$ 的二维投影则为具有一定方向的整合线。图像的 Radon 变换是将原始图像变换为它在各个角度的投影表示。图像 $f(x,y)$ 在任意角度 θ 上的 Radon 投影定义为：

$$R_\theta(x')=\int_{-\infty}^{\infty} f(x'\cos\theta-y'\sin\theta,x'\sin\theta-y'\cos\theta)\mathrm{d}y' \tag{1}$$

其中，

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}\cos\theta & \sin\theta\\-\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} \tag{2}$$

Radon 函数变换与霍夫变换的通用视频操作有着密切的联系，这里可以利用 Radon 函数来实现特定形式的霍夫变换，即解析图像中的直线线条。通过查找 Radon 变换矩阵中的峰值，可得到图像旋转的角度 θ。



(a)原始图像　(b)旋转 30°　(c)图(b)的边缘　(d)Radon 变换的结果

图 1　图像边缘检测及 Radon 变换的结果

3　特征检测及提取

人类的视觉心理学的研究表明人类的视觉皮层中存在 end-stopped 细胞单元，这些细胞对图像中鲁棒性的特征点（如角点、边缘弯曲的点）具有较强的敏感性。Bhattacharjee 等[12]充分利用人类视觉的这一特性构造了 end-stopped 小波来寻找这些特征点。

3.1　End-Stopped 小波

Morlet 小波其频域能量比较集中，具有时域对称和线性相位的特点，可以应用其侦测线性结构的具体方向，所以选择 Morlet 小波作为母小波。

在空间域中，二维 Morlet 小波表示为：

$$\psi_M(\boldsymbol{x})=(e^{i\boldsymbol{k}_0\cdot\boldsymbol{x}}-e^{-\frac{1}{2}(|\boldsymbol{k}_0|^2)})e^{-\frac{1}{2}(|\boldsymbol{x}|^2)} \tag{3}$$

其中，$\boldsymbol{x}=(x,y)$ 代表二维空间坐标，$\boldsymbol{k}_0=(k_0,k_1)$ 表示母小波的波矢量。

在频域中表示为：

$$\hat{\psi}_M(\boldsymbol{k})=(e^{-\frac{1}{2}(|\boldsymbol{k}-\boldsymbol{k}_0|^2)}-e^{-\frac{1}{2}(|\boldsymbol{k}_0|^2)})e^{-\frac{1}{2}(|\boldsymbol{x}|^2)} \tag{4}$$

$\boldsymbol{k}$ 表示二维频域变量 (u,v)。Morlet 小波变换类似于 Gabor 变换，拥有额外的修正容许条件 $e^{-\frac{1}{2}(|\boldsymbol{k}_0|^2+|\boldsymbol{x}|^2)}$，具有最佳时域和频域连接分辨率的特点，能够同时对图像局部结构的方向和空域频率进行解析。其中小波矢量的方向决定滤波调整的方向，Morlet 小波检测的线性结构的方向垂直于小波的方向。

使用 FdoG(First-derivative of Gaussian)来检测线的终端点，在二维结构中，应用 FDoG 滤波器相应的结构方向来检测线性结构的终端点正被研究。其中包括两个滤波步骤，首先检测有具体方向的线，然后检测线的终端点，这样可以组成一个单一的滤波器，结果得到 end-stopped 小波。

end-stopped 小波母小波表示为：

$$\psi_E(x,y)=\frac{1}{4}xe^{-(\frac{x^2+y^2}{4}+\frac{k_1}{4}(k_1-2iy))} \tag{5}$$

在频率域中表示为：

$$\hat{\psi}_E(x,y)=2\pi(e^{-(\frac{u^2+(v-k_1)^2}{4})})(ive^{-(\frac{u^2+v^2}{4})}) \tag{6}$$

式(6)显示了 $\hat{\psi}_E(x,y)$ 产生的两部分，首先是沿着 u 轴方向的 Morlet 小波，第二部分是应用在 v 轴的 FDoG 滤波器，其在方向上垂直于 Morlet 小波。因此，小波检测到的线终端和角点在垂直方向上。

3.2　特征检测方法

特征检测是通过计算以 end-stopped 小波为小波基的小波变换，其实现公式如下：

$$\psi_E(x,y,\theta)=(FDoG)\circ(\psi_M(x,y,\theta)) \tag{7}$$

其中，方向调整 $\theta=\tan^{-1}(\frac{k_1}{k_0})$，$\theta$ 范围$[0,\pi]$离散化为 M 间隔，缩放系数 α 指数化采样，如 $\alpha^i,i\in Z$，可得到：

$$(\psi_E(\alpha^i(x,y,\theta_k))),\alpha\in R,i\in Z \tag{8}$$

其中，$\theta_k=(k\pi)/M,k=0,\cdots,M-1$。取采样系数 α 为 2，变换为：

$$W_i(x,y,\theta)=\int f(x_1,y_1)\psi_E^*(\alpha^j(x-x_1,y-y_1),\theta)\mathrm{d}x_1\mathrm{d}y_1 \tag{9}$$

实现特征检测包括三个步骤：

(1)计算式(8)中的小波变换并取合适的伸缩因子 i，结合其对于失真的敏感性，在这里选取 i=3。

(2)选择图像中被识别的位置为(x,y)的待选择合适的特征点

$$W_i(x,y,\theta)=\max_{(x',y')\in N_{(x,y)}}|W_i(x',y',\theta)| \tag{10}$$

其中，$N_{(x,y)}$表示(x,y)的邻点。

(3)由第(2)步得到待选择的特征点，通过阈值选择得到最后的特征点。

$$\max_\theta W_i(x,y,\theta)>T \tag{11}$$

在检测过程中，通过选择合适的阈值 T 来确定所要提取图像特征点的数目 P，得到长度为 P 的特征矢量 f。这里为了平衡认证水印的鲁棒性和脆弱性，可以通过选取特征点的数目来达到平衡，选取特征点的数量越多特征点对变化失真就越敏感，所以阈值 T 的选取就显得尤为重要。

3.3　特征点处理

通过应用 end-stopped 小波提取得到鲁棒性较好的特征点，为了进一步平衡水印的鲁棒性和脆弱性，可以先对特征点进行相应的处理，并利用图像特征点的 Hausdorff 距离来对图像进行认证。

文献[5]Monga 等运用线性低通移不变滤波器对图像处理再进一步提取特征点，应用特征点 hash 值的 Hamming 距离即

$D_H(H(I),H(I_{sim}))<0.2$ 和 $D_H(H(I),H(I_{diff}))>0.3$ 对图像进行认证，I_{sim} 表示与原图像感知相似的图像，I_{diff} 表示与原图像感知不同的图像，$H(\cdot)$表示图像 hash 值，$D_H(\cdot)$表示两个值的 Hamming 距离。这样的特征点处理其实际认证效果并不是很好，一些经过篡改的图像不能辨别其被篡改，认证的成功率并不高。

如何平衡鲁棒性和脆弱性，在运用修正 Hausdorff 距离进行认证之前，这里先对图像进行处理：(1)非线性空间滤波。首先应用非线性空间滤波对图像滤波处理，使其中心处响应为邻域内值的几何平均，这样可以通过滤波处理减少因为噪声对提取特征点造成的影响。(2)3×3 的中值滤波。中值滤波将像素邻域内灰度的中值代替该像素的值，使拥有不同灰度的点看起来更接近于它的邻近值，可以抵抗椒盐噪声等造成图像非故意篡改的失真，这样可以得到更为鲁棒的特征点，而且并未减弱图像针对恶意篡改的脆弱性。

4 篡改认证

4.1 修正 Hausdorff 距离

Hausdorff 距离[13,14]是用来衡量两个点集间的距离，给定两个点集 $M=\{m_1,m_2,\cdots,m_p\}$，$N=\{n_1,n_2,\cdots,n_q\}$，传统 Hausdorff 距离定义为：

$$H_h(M,N)=\max(h(M,N),h(N,M)) \tag{12}$$

其中 $h(M,N)=\max\limits_{m\in M}\min\limits_{n\in N}\|m-n\|$，$\|\cdot\|$为点集合 M 与 N 的范式。

Hausdorff 距离对篡改的图像的认证能力有限，对于部分篡改并不敏感，为了解决这一问题，这里对 Hausdorff 距离进行修正，增强其对于恶意篡改的敏感性。

为了提高传统 Hausdorff 距离对图像的认证能力，可以通过改进 Hausdorff 距离来实现。通过对图像提取的特征点的观察，可以看出被恶意篡改的图像其特征点的分布具有一定的规律，即是图像被篡改的局部区域的特征点变化很大，而图像其他区域的特征点位置基本没有变化，对于一般的图像处理而言，则没有这一变化特征；根据这个变化特征，在计算两特征点间的距离时，可以提高变化大的特征点距离的比例，减少变化小的特征点距离的比例，达到突出图像局部特征点变化很大这一特征，并减弱一般图像处理(JPEG 压缩等)对图像认证的影响。

因此，这里对传统 Hausdorff 距离进行了修改，提出了修正的 Hausdorff 距离，通过式(13)和式(14)得到 h_{en}，通过设定合适的 α 值(实验中取 α=0.20)，减小一般图像处理对图像的影响，增强算法对恶意篡改的敏感性，最终得到修正 Hausdorff 距离的实现公式(15)。

$$h_q=\sum(\alpha\min_{p/2}\sum_{n\in N}\min\|m_i-n\|+(1-\alpha)\max_{p/2}\sum_{n\in N}\min\|m_i-n\|),\alpha\in(0,1) \tag{13}$$

$$h_{en}=\frac{h_q}{p} \tag{14}$$

$$H(M,N)=\max(h_{en}(M,N),h_{en}(N,M)) \tag{15}$$

在应用修正 Hausdorff 距离来计算原图像和待认证图像的特征点的距离时，要选择合适的阈值 k，使得满足 $H(M,N)<k$，来辨别图像的不可感知失真和恶意篡改的区别。

4.2 水印嵌入及提取

为了实现在一定程度上定位图像的篡改位置，本文在图像中嵌入水印。在水印嵌入时，由于小波变换具有良好的时频特性，其多分辨率分析与人眼视觉特性一致等许多优点，本文选择将水印信息嵌入在DWT域中，其低频子带是图像最重要的信息，集中了图像的大部分能量，比较稳定，所以把水印信息嵌入在三级小波变换的小波低频子带中。

在小波域中，这里采用文献[6]中的嵌入策略，如式(16)，将二值水印图像 W 嵌入到图像低频子带 C 中，得到含水印图像 C'，系数 σ 表示水印的嵌入强度。

$$\begin{cases}C'(i)=C(i)-(C(i)\bmod\sigma)+\frac{3}{4}\sigma,\text{if } x_i=1\ (C(i)\bmod\sigma)\geqslant\frac{1}{4}\sigma\\ C'(i)=[C(i)-\frac{1}{4}\sigma]-[(C(i)-\frac{1}{4}\sigma)\bmod\sigma]+\frac{3}{4}\sigma,\\ \qquad\text{if } x_i=1\ (C(i)\bmod\sigma)<\frac{1}{4}\sigma\\ C'(i)=C(i)-(C(i)\bmod\sigma)+\frac{1}{4}\sigma,\text{if } x_i=0\ (C(i)\bmod\sigma)\leqslant\frac{3}{4}\sigma\\ C'(i)=[C(i)+\frac{1}{2}\sigma]-[(C(i)+\frac{1}{2}\sigma)\bmod\sigma]+\frac{1}{4}\sigma,\\ \qquad\text{if } x_i=0\ (C(i)\bmod\sigma)>\frac{3}{4}\sigma\end{cases} \tag{16}$$

最后为了定位篡改位置，可通过式(17)提取水印。

$$w_i^*=\begin{cases}1 & C^*(i)\bmod\sigma>\frac{\sigma}{2}\\ 0 & \text{otherwise}\end{cases} \tag{17}$$

5 实验结果

本实验采用的是 256×256 的灰度图像，通过在待认证图像中提取 64 个特征点对图像进行认证，经过对多幅图像的实验证明，选取的认证阈值为 0.03，选取这个阈值综合考虑了水印的鲁棒性和脆弱性，此阈值可以较好地辨别图像是否经过恶意篡改，而且可以提高其认证的正确率。如果 $H(M,N)<0.03$，则图像通过认证，否则图像未通过认证。因此，通过判断准则式(18)对图像进行认证：

$$H(M,N)=\max(h_{en}(M,N),h_{en}(N,M))=\begin{cases}<0.03 & \text{authentication success}\\ \text{otherwise} & \text{authentication failure}\end{cases} \tag{18}$$

其中 M 为原始图像的特征点，N 为待认证的图像的特征点；当图像 Hausdorff 距离小于 0.03 时，图像通过认证；当 Hausdorff 距离大于 0.03 时，表明图像被篡改或者剪切了部分信息，提取图像水印可以通过水印图像的失真位置得到图像被篡改或剪切的位置。

表 1 为本文提出的抗几何攻击的认证算法的认证结果，表 2 为原认证算法的认证结果。从实验结果可以看出运用本算法增强了图像抵抗旋转和缩放的能力(原算法没有任何抗几何变换的能力)，并且对于一般的图像处理(包括 JPEG 压缩等)都具有更好的鲁棒性，保持对恶意篡改的敏感性；从实验数据来

表 1 修正的认证算法的实验结果

图像攻击	Lena 图	Man 图	Bridge 图
旋转 30°	0.020 7	0.021 6	0.013 7
放大 1 倍	0.015 3	0.019 5	0.009 1
缩小 25%	0.016 8	0.024 9	0.020 5
JPEG 压缩(Q=70%)	0.023 3	0.020 1	0.004 9
恶意篡改	0.033 9	0.035 6	0.032 3
剪切(12.5%)	0.059 7	0.031 4	0.061 4

表 2　原认证算法的实验结果

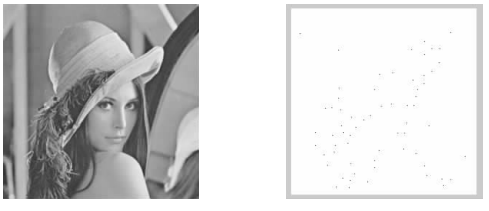
图像攻击	Lena 图	Man 图	Bridge 图
旋转 30°	0.356 5	0.343 4	0.394 5
放大 1 倍	0.037 1	0.030 8	0.052 6
缩小 25%	0.047 3	0.051 8	0.048 3
JPEG 压缩(Q=70%)	0.029 2	0.025 1	0.006 1
恶意篡改	0.032 9	0.044 6	0.037 9
剪切(12.5%)	0.062 5	0.039 3	0.076 7

看修正的算法比原算法有了比较明显的提高。

图 2、图 3 是原始图像和旋转 30°复原的图像所提取的特征点比较,图 2 是提取出原始图像的特征点,图 3 是待认证图像的特征点。由实验结果可以看出,经过旋转复原的图像和原始图像提取的特征点基本一致。

(a)原始图像　　(b)原始图像特征点

图 2　原始图像和其特征点



(a)复原图像　　(b)复原图像特征点

图 3　经过旋转复原的待认证图像和其特征点

图 4 给出了图像经过恶意篡改后提取出的水印和原水印的比较。由水印图像可以看出原图像被恶意篡改的位置,这样可以通过提取的水印定位篡改的位置。

(a)原始图像　　(b)被篡改图像

(c)原始水印　　(d)提取出的水印

图 4　对加水印图像篡改进行和其检测结果

6　小结

本文在原来基于感知 hash 的图像认证算法基础上增强了抗几何攻击(旋转、缩放等)的能力,运用修正 Hausdorff 距离实现图像的认证,在保持其对一般图像处理的鲁棒性基础上,提高了算法对恶意篡改的敏感性。另外,本抗几何攻击的算法计算简单,容易实现,在图像中加入了水印图像能够精确定位图像的篡改位置,其良好的性能进一步增强其适用范围。下一步研究将把重点放在提高算法的安全性,并使得非恶意篡改后的图像依然能被检测器接受,以及提高算法的可靠性。

参考文献:

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

[2] Fridrich J,Goljan M.Robust hash functions for digital watermarking[C]//Proc IEEE Int Conf on Information Technology:Coding and Computing,Mar,2000:178-183.

[3] Lin C Y,Chang S F.Generating robust digital signature for image/video authentication[C]//Proc ACM Multimedia and Security Workshop,Sept 1998.

[4] Lin C Y,Chang S F.A robust image authentication system distinguishing JPEG compression from malicious manipulation[J].IEEE Trans on Circuits and Systems for Video Technology,2001,11:153-168.

[5] Monga V,Evans B L.Robust perceptual image hashing using feature points[C]//Proc IEEE Conf on Image Processing,2004:677-680.

[6] Kang Xian-gui,Huang Ji-wu.A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression[J].IEEE Transactions on Circuits and Systems for Video Technology,2003,13(8).

[7] O'Ruanaidh J J K,Pun T.Rotation,scale and translation invariant spread spectrum digital image watermarking[J].Signal Processing,66(3):303-317.

[8] Lin C Y,Wu M,Bloom J A,et al.Rotation,scale and translation resilient watermarking for images[J].IEEE Trans on Image Processing,2001,10(5):765-782.

[9] Lin C Y.Public watermarking surviving general scaling and cropping:an application for print-and-scan process[C]//Multimedia and Security Workshop at ACM Multimedia 99,USA,1999.

[10] Monga V,Evans B L.Image authentication under geometric attacks via structure matching[C]//IEEE Int Conf Multimedia and Expo,2005.

[11] Wu M,Miller L M,Bloom J A,et al.A rotation,scale and translation resilient public watermark[C]//Proc IEEE Int Conf Acoustics,Speech,and Signal Processing 1999,USA.

[12] Bhatacherjee S,Vandergheynst P.End-stopped wavelets for detecting low-level features[C]//Proc SPIE Wavelet Appl in Sig Image Pro,1999:732-741.

[13] Rucklidge W J.Efficient computation of the minimum Hausdorff distance for visual recognition[D].Cornell University,1995.

[14] 汪亚明.图像匹配的鲁棒型 hausdorff 方法[J].计算机辅助设计与图形学学报,2002,14(3):238-241.