基于 Zernike 矩的抗旋转攻击图像感知哈希算法

罗嗣卿，吴 頓

（东北林业大学 信息与计算机工程学院 150040 哈尔滨，luosq@nefu.edu.cn）

摘 要：以 Zernike 矩为特征图像感知哈希算法，由于 Zernike 矩对图像旋转具有不变性，使得算法具备了旋转攻击下的鲁棒性；同时由于 Zernike 矩是图像的正交表示，能够很好地提取图像的内容，使得算法具有良好的区分性. 算法首先将图像归一化，然后提取图像 Zernike 矩作为特征，经过密钥置乱后，对特征进行量化生成哈希串. 算法在 100 幅图像组成的样本集上进行了测试，结果表明本文算法在旋转攻击下误接受率小于 4%，匹配错误率在 10^{-9} 数量级. 说明基于 Zernike 矩的图像哈希算法能够同时满足对旋转攻击鲁棒和区分不同图像的技术要求.

关键词：Zernike 矩；感知哈希；图像归一化；几何失真；图像认证

中图分类号：TP 391.41 **文献标志码**：A **文章编号**：0367－6234(2011)05－0135－04

Zernike moment based image hash algorithm resistant to rotation

LUO Si-qing, WU Di

(Information and Computer Engineering College, Northeast Forestry University, Harbin 150040, China, luosq@nefu.edu.cn)

Abstract: In this paper, we proposed a novel image hash algorithm based on Zernike moments. We employ Zernike moments to represent the image content for the reason that it is the projection of the image under a group of orthogonal basis. Thus, the discrimination of proposed algorithm is improved. Meanwhile, benefited from the invariance property of Zernike moment under affine transform, our algorithm is robust to rotation attack. In the proposed method, the hash string is generated from the Zernike moments of the normalized input image. Secret key is also introduced to ensure the security of the hash method. In the experiments, the method is tested by 100 sample images. The false accept rate under rotation attack is less than 4%. The error recognizing rate between different images is about 10^{-9}. Experimental results prove that our algorithm has great robustness and discrimination.

Key words: Zernike moment (ZM); perceptual Hashing; Image normalization; geometric distortions; image authentication

随着计算机网络和多媒体技术的飞速发展，大量的数字图像广泛的应用于日常生活和工作中. 但由于传播过程中任何人都可以方便地对数字媒体进行修改，使得图像真实性、完整性认证成为多媒体技术领域中的重要课题. 针对这一问题，图像哈希技术近年来迅速发展了起来. 图像哈希将图像转化为一个二进制串，其思想来源于密码学中的哈希函数. 不同的是，密码学哈希要求数据每一位都完全正确，而图像哈希关注图像内容的不变性. 在图像经过内容不变的处理操作后（又称为攻击）哈希算法生成的哈希串，与原图的哈希串相比应当只有少数比特不同，这种性能被称为鲁棒性，而原图的哈希串与不同图像，或原图经过内容篡改的版本生成的哈希串相比，应有 50% 左右的比特不同，这种性能被称为区分性.

在各种图像处理方法中，旋转攻击由于破坏处理前后图像的像素同步关系，尤其难以与内容不同的图像区分. 为在旋转攻击下保证算法的鲁

收稿日期：2010－04－06.
基金项目：黑龙江省自然基金资助项目(F200922).
作者简介：罗嗣卿(1964—)，男，副教授.

棒性和区分性,需要哈希算法所提取的特征具有旋转不变性,并包含图像的总体特征和局部细节特征. 现有哈希算法主要分为:基于矩阵分解的方法(包括奇异值分解,非负矩阵分解等[1-2]);基于细节点的方法[3];基于时频变换的方法(包括傅里叶变换、DCT 变换等[4-5]). 这些算法中使用特征,有的不具备几何不变性,有的没有做到融合图像总体特征和细节特征,所以在旋转攻击下性能不够理想. 为克服现有算法的缺点,本文提出了一种以 Zernike 矩作为图像特征的哈希算法. Zernike 矩是一种正交分解方法,各阶 Zernike 矩分别包含了图像的细节和总体信息,使得它可以灵活提取不同层次的图像特征,保证了算法的良好区分性. 同时由于 Zernike 矩对图像旋转保持不变,保证了算法对于旋转攻击的鲁棒性. 此外,为提高算法安全性,在生成哈希值的过程中,还引入了密钥. 实验结果表明,本文提出的算法对旋转攻击具有良好的鲁棒性,同时具备良好的区分性.

1 Zernike 矩

1.1 Zernike 矩的定义

Zernike 多项式是单位圆内 $(x^2+y^2\leqslant 1)$ 的一组完备的正交基,记为$\{V_{nm}(x,y)\}$,其定义[6]为

$$V_{nm}(x,y)=V_{nm}(\rho,\theta)=R_{nm}(\rho)\mathrm{e}^{\mathrm{j}m\theta}. \quad (1)$$

式中:n 为正整数或零;m 为整数;$n-|m|$ 为偶数,且 $|m|<n$;ρ 为极坐标下原点到(x,y) 的距离,θ 为向量 ρ 与 x 轴的夹角(逆时针方向). $R_{nm}(\rho)$ 为正交的径向多项式,定义为

$$R_{nm}(\rho)=\sum_{k=0}^{(n-|m|)/2}(-1)^k\cdot\frac{(n-k)!}{k!\left[\frac{n+|m|}{2}-k\right]!\left[\frac{n-|m|}{2}-k\right]!}\rho^{n-2k}. \quad (2)$$

Teague 以 Zernike 正交多项式为基础给出二维 Zernike 矩的定义为

$$A_{nm}=\frac{\pi}{n+1}\iint_{x^2+y^2\leqslant 1}V_{nm}^*(x,y)f(x,y)\,\mathrm{d}x\mathrm{d}y. \quad (3)$$

式中:$V_{nm}^*(x,y)$ 为 $V_{nm}(x,y)$ 的共轭. 反之,若已知图像最高 $n_{\max}$ 阶的所有矩,图像重构为

$$\hat{f}(x,y)=\sum_{n=0}^{n_{\max}}\sum_{m}A_{nm}V_{nm}(\rho,\theta). \quad (4)$$

Zernike 矩是连续函数在正交函数基 $\{V_{pq}(x,y)\}$ 上的投影,由式(4) 可以得到:$R_{n,-m}(\rho)=R_{nm}(\rho)$.

1.2 图像 Zernike 矩的计算

根据 Zernike 矩的定义,在计算图像的 Zernike 矩时,需要将图像函数 $f(x,y)$ 转化为标准图像函数 $f_1(x,y)$,这被称为图像的归一化. Abumostafa 等[7]以下列关系式来描述图像归一化过程为

$$f_1(x_2,y_2)=Gf(x_1,y_1)+B.$$

其中:

$$\begin{bmatrix}x_1\\y_1\end{bmatrix}=\begin{bmatrix}x_0\\y_0\end{bmatrix}+\frac{1}{D}\begin{bmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{bmatrix}\begin{bmatrix}x_2\\y_2\end{bmatrix}.$$

式中:x_0 和 y_0 分别为平移量;φ 为旋转角度;D 为缩放比例因子;G 为亮度调整因子;B 为附加直流分量. 选择合适的归一化参数,就可以将图像调整到预定的大小和位置,并使其具备合适的亮度,本文中不对亮度进行调整,即 $G=1,B=0$.

计算图像的 Zernike 矩需要进行离散化处理,数字图像 $f(x,y)$ 的 n 阶 m 重 Zernike 矩定义为

$$A_{nm}=\frac{\pi}{n+1}\sum_{x}\sum_{y}f(x,y)V_{nm}^*(\rho,\theta). \quad (5)$$

式中 V_{nm}^* 为 V_{nm} 的复共轭,且 $x^2+y^2\leqslant 1$. 为计算给定图像的 Zernike 矩,必须将图像中心作为原点并将像素坐标映射到单位圆内,落到单位圆外部的像素不参加计算.

直接按式(5)求 Zernike 矩计算量较大,可以采取文献[8]中提出的快速算法.

1.3 Zernike 矩的旋转不变性

旋转不变性是 Zernike 矩的重要的特性,当图像 $f(x,y)$ 旋转 α 角度时,Zernike 矩变为

$$A'_{nm}=\frac{n+1}{\pi}\int_0^{2\pi}\int_0^1 f(\rho,\theta-\alpha)R_{nm}(\rho)\mathrm{e}^{-\mathrm{j}m\theta}\rho\mathrm{d}\rho\mathrm{d}\theta. \quad (6)$$

设:$\theta_1=\theta-\alpha$,

$$A'_{nm}=\left[\frac{n+1}{\pi}\int_0^{2\pi}\int_0^1 f(\rho,\theta_1)R_{nm}(\rho)\mathrm{e}^{-\mathrm{j}m\theta_1}\rho\mathrm{d}\rho\mathrm{d}\theta_1\right]\mathrm{e}^{-\mathrm{j}m\theta}. \quad (7)$$

从式(7) 可以看出当图像进行旋转后,其幅值保持不变,即 $A_{nm}=A'_{nm}$. 由此证明了 Zernike 矩的具有旋转不变性.

为验证上述结论在离散条件下的有效性,对 Lena 图像以 10° 为步长,旋转 10° ~ 90°,得到 10 幅图像. 分别计算各图像的各阶 Zernike 矩 A_{nm}(n 取 2 ~6,$m<n$),每幅图像共有 14 个独立的 Zernike 矩. 对每个矩求模得 $|A_{nm}|$,并对同阶 $|A_{nm}|$ 进行统计,选取 8 组方差最大的结果,均值和方差如表 1 所示.

表 1　图像旋前后 Zernike 矩变化情况

统计值	$\lvert A_{10}\rvert$	$\lvert A_{22}\rvert$	$\lvert A_{31}\rvert$	$\lvert A_{33}\rvert$	$\lvert A_{42}\rvert$	$\lvert A_{44}\rvert$	$\lvert A_{51}\rvert$	$\lvert A_{62}\rvert$
均值	8.214 667	15.526	19.191	23.240 22	66.255 22	146.356	267.745 6	568.270 8
方差	0.016 132	0.007 348	0.033 589	0.030 103	0.036 204	0.036 377	0.029 615	0.0377 85

从表 1 可以看出，各阶矩统计所得的方差均在 10^{-2} 数量级，说明 Zernike 矩可以抵抗大角度的图像旋转.

2　算法设计

2.1　哈希生成

哈希生成过程包括的步骤为：

1）图像归一化. 将图像统一变成具有 255 阶的灰度图像，并用双三次插值的方法将图像分辨率变为 $m \times m$（m 一般为 8 的倍数）. 此后生成图像的外接圆，图像外的空缺部分用黑色填充，最后对图像进行二值化.

2）特征提取. 计算图像的若干阶 Zernike 矩 A_{nm}. 将矩的幅值构造为特征矢量，即 $\vec{p} = (p_1, p_2, \cdots, p_N) = [\lvert A_{20}\rvert, \lvert A_{22}\rvert, \lvert A_{31}\rvert, \cdots, \lvert A_{n_{\max}n_{\max}}\rvert]$，其中：$N$ 为特征矢量的长度；$n_{\max}$ 为 Zernike 矩的阶，实验中取 $n_{\max} = 20$. 由于矩的共扼对称性，剩下的矩幅度只有 1/2 是独立的. 记最终选取的矩集合为 P，则 $P = \{A_{nm}, n \leqslant N_{\max}, m \geqslant 0\}$.

3）加密. 为了提高算法的安全性，从上述矩集合 P 中通过密钥 K 伪随机选取其中 M 阶 Zernike 矩生成特征向量 $\vec{q} = (q_1, q_2, \cdots, q_M)$ 作为图像的特征信息. 将 q_i 向量中所有不为 0 的幅值平均值作为第 i 个 $hash$ 值，即 $hash_i$ 表示为

$$hash_i = \frac{1}{W}\sum_{n,m}\beta \lvert q_i\rvert .$$

式中：β 为关于 key-dependant 伪随机数，服从均值为 δ，方差为 σ^2 的正态分布；W 为 M 阶 Zernike 矩中幅值不为 0 的个数.

4）量化. 以所有幅值平均值的 1/4 为量化步长，对提取的特征信息进行量化编码，生成二值化的哈希串.

2.2　算法参数选择

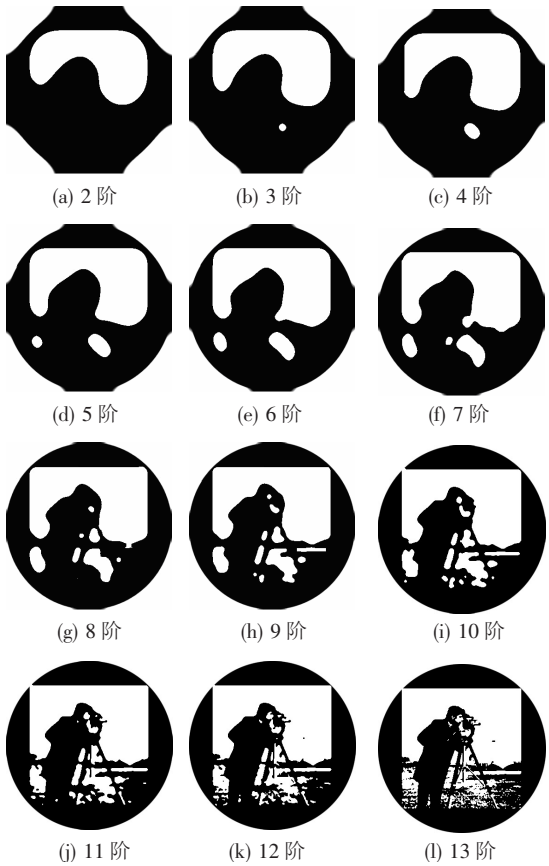
在生成哈希时，需要选取适当阶数的 Zernike 矩作为图像特征，测试图像 Cameraman 如图 1 所示.

利用图 1（b）计算的各阶 Zernike 矩对原图进行重构，2 ~ 13 阶矩的重构图像如图 2 所示.

从图 2 中可以看出，低阶 Zernike 矩包含图像的轮廓信息，高阶矩包含图像的细节信息. 阶数越高，重构图像的效果越好，但是计算的代价也越大. 所以哈希生成时选取 10 阶矩就可以同时提取图像中的整体信息和细节信息.

（a）原始图像　　（b）归一化后的图像

图 1　测试图像



(a) 2 阶　(b) 3 阶　(c) 4 阶

(d) 5 阶　(e) 6 阶　(f) 7 阶

(g) 8 阶　(h) 9 阶　(i) 10 阶

(j) 11 阶　(k) 12 阶　(l) 13 阶

图 2　Zernike 矩重构图像效果

2.3　图像的认证

在认证时，用汉明距离来进行匹配，设 h_1 和 h_2 为 2 个哈希序列，则其汉明距离为

$$D_{\mathrm{H}} = \sum \lvert h_1(i) - h_2(i)\rvert .$$

当 D_{H} 大于设定的阈值时则认为匹配成功，称为接受，反之则为匹配失败，称为拒绝.

2 幅内容不同的图像具有近似的哈希值，将发生错误匹配，这种现象被称为误接受，或称为冲突.

3　实验结果及性能分析

3.1　实验环境

测试图像选自网络图像库，从图像数据库中

随机选取了 100 张不同的图像,包括人物、山水、汽车、动物、花朵、食物、昆虫、天文和纹理等.

3.2 区分性实验

对选出的 100 幅图像计算 Zernike 矩,提取前 10 阶的矩的模作为特征值,即 $A_{00} \sim A_{100}$ 共 20 个特征向量,这样每幅图像有 20 个特征向量,得到 100 组哈希序列. 再对 100 幅图像的特征向量进行相异的两两匹配试验,得到 4 950 组匹配结果,图 3 为不同图像间哈希串汉明距离的统计直方图.

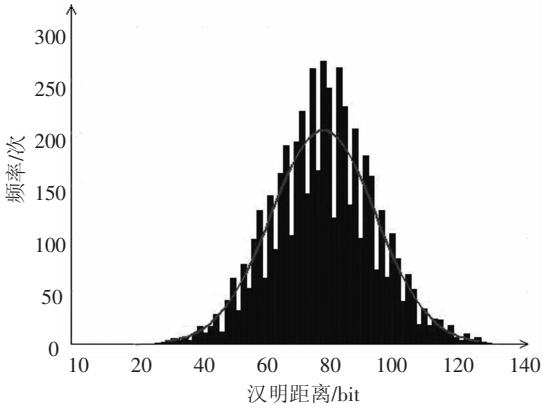


图 3 不同图像间哈希串汉明距离分布

从图 3 中可以看出实验结果基本服从正态分布,求得其数学期望 $\mu = 82.87$,标准差 $\sigma = 9.82$,当选用阈值 $T = 20$ 时,误接受率为

$$P = \int_{-\infty}^{T} \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(x-\mu)^2}{2\sigma^2}} dx = 0.765\ 57e^{-10}.$$

由于冲突率极小,所以说明本文提出的算法具有良好的区分性.

3.3 旋转攻击试验

在 100 幅测试图像中,随机选取 10 幅攻击图像进行图像旋转操作,然后分别选择 30°、60°和 90°旋转. 得到 30 幅攻击图像,用这 30 幅攻击图像与 100 幅测试图像进行汉明距离计算,得到 3 000个匹配结果. 对这些匹配所得的汉明距离进行统计,结果如图 4 所示.

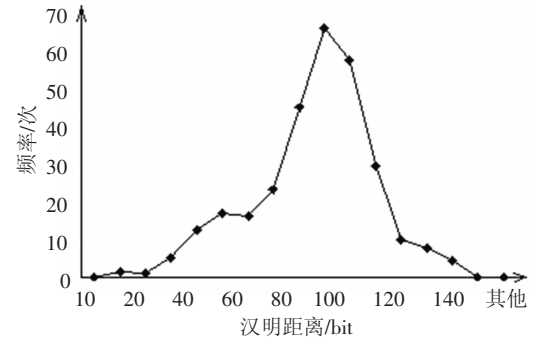


图 4 旋转攻击下测试图像间汉明距离统计

实验结果表明,不同图像间的汉明距离多数分布在 60 ~ 120 的范围内. 根据实验结果统计 ≤20 的值为 29 个. 以 $T = 20$ 为匹配阈值时,误接受率为 3.3%,正确识别率相应的为 96.7%,可以满足图像的抗几何攻击性.

4 结 论

1)利用 Zernike 矩作为图像分层正交表示的特点,同时提取了图像的总体特征和细节特征,具备良好的区分性.

2)利用 Zernike 矩的旋转不变性,提高了图像哈希算法在旋转攻击下的鲁棒性.

3)通过密钥对图像特征进行了置乱,保证了哈希串的随机性,提高了算法的安全性.

4)通过图像旋转实验测试,结果表明该方法对 90°以下图像旋转攻击具有良好的鲁棒性.

参考文献:

[1] KOZAT S S, MIHCAK K, VENKATESAN R. Robust perceptual image hashing via matrix invariants [C]// Proceedings of IEEE Conference on Image Processing. Piscataway, NJ: IEEE, 2004: 3443 - 3446.

[2] MONGA V, MHCAK M K. Robust and secure image hashing via non-negative matrix factorizations [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 376 - 390.

[3] SEBE N, TIAN Q, LOUPIAS E, *et al*. Color indexing using wavelet-based salient points[C]//Proceedings of IEEE Workshop on Content-based Access of Image and Video Libraries. Washington DC: IEEE Computer Society, 2000: 15 - 19.

[4] SWAMINATHAN A, MAO Yinian, WU Min. Robust and secure image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 215 - 230.

[5] 王阿川, 陈海涛. 基于离散余弦变换的鲁棒感知图像哈希技术[J]. 中国安全科学学报, 2009,19(4): 91 - 96.

[6] TEAGUE M R. Image analysis via the general theory of moments [J]. Journal of Optical Society of America, 1980, 7(8): 920 - 930.

[7] ABU-MOSTAFA Y, PSALTIS D. Image normalization by complex moments[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1985, PAMI - 7(1): 46 - 55.

[8] KHOTANZAD A, HONG Y H. Invariant image recognition by Zernike moments [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1990, 12(5): 489 - 497.

(编辑 张 红)