基于特征点的抗几何攻击零水印

王 忠，叶雄飞
（武汉工程大学 计算机科学与工程学院，湖北 武汉 430205）

摘 要：提出了最小偏离度的概念，根据IPR库中的特征点信息和待测图像自身的特征点信息分别构造Delaunay三角网，并以此计算两张三角网中三角形的最小偏离度值。若该值低于预先设定的阈值，则可以确认待测图像的版权归属。实验表明，该算法对各种几何攻击甚至是组合几何攻击均具有较强的鲁棒性。

关键词：几何攻击；零水印；最小偏离度；特征点；版权
中图分类号：TP39　　**文献标识码**：A

Geometrical zero watermarking based on feature points

WANG Zhong, YE Xiong Fei
(School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan 430205, China)

Abstract: The Delaunay triangular nets will be created with the feature points in IPR library and the feature points of checked image itself respectively. The least deviation is proposed to calculate the least deviation value between the two triangular nets. If the value is less than the gate value which is set in advance, the ownership of checked image will be confirmed. The experiments have indicated that the scheme in this paper is robust to many kinds of geometrical attacks, even the compound geometrical attacks.

Key words: geometrical attacks; zero watermark; least deviation; feature points; ownership

数字水印技术是为了解决互联网上数字作品的版权保护和认证等问题而提出来的。由于数字水印技术在抗几何攻击方面遇到的巨大挑战，众多研究者们开始关注抗几何攻击的数字水印技术，并发现图像的特征点信息在经受了各种仿射变换之后，仍然具有良好的稳定性。此外，温泉等人[1]于2003年首次提出了零数字水印的概念，即不修改原图像来构造水印。本文提出了以图像特征点和尺寸构造零水印并保存到IPR(Intellectual Property Right)中作为数据版权凭据的算法。对于攻击后的图像，算法提取出特征点，利用Delaunay分割法把这些特征点组成1张Delaunay三角网。用同样的办法，把IPR中零水印保存的特征点也组成1张Delaunay三角网。最后，计算2个三角网的最小偏离度值。如果此项指标低于设定的阈值，就可以断定被检测图像和原始图像具有相同的版权，从而达到抗几何攻击的目的。

1 图像特征点提取及Delaunay分割

特征点就是图像中的明显点，如角点、圆点等。数字图像理想的特征点应当是几何不变的[2]，即一旦图像受到了几何攻击，特征点仍然能指出相同的局部特征，同时，当只有部分信息可用时，特征点的信息并不受损。

特征点的提取有很多种办法。本文采用Harris角点检测器来提取图像的特征点信息，以图像的角点作为特征点。

设定矩阵M，其特征值是图像自相关函数的一阶曲率，对图像中任意一点，如果水平曲率和垂直曲率都高于局部邻域中的其他点，则认为该点是角点。M的定义如下[3-4]：

$$M=G(s)\otimes\begin{bmatrix} g_x^2 & g_x g_y \\ g_x g_y & g_y^2 \end{bmatrix} \tag{1}$$

其中，g_x为x方向的梯度，g_y为y方向的梯度，$G(s)$为高斯模板，起到平滑噪声的作用。

对M求取特征值λ_1和λ_2，建立如下的度量函数：

$$R=\det M-k(\text{trace } M)^2 \tag{2}$$

其中，$\det M=\lambda_1\lambda_2$表示矩阵$M$的行列式值，$\text{trace } M=\lambda_1+\lambda_2$表示矩阵$M$的迹，$k$为常数，根据经验，一般取为0.04[5]。

如果R超过某一预先设定的阈值，即可认为该点为角点[3]。

参考文献[4]对Delaunay分割的特性进行了说明，并

强调这种分割具有唯一性，因而在基于图像特征点的研究中占有重要地位。

2 零水印技术

作为一种新颖的数字水印技术，零数字水印利用图像的重要特征来构造水印，而不需要修改图像信息[6-7]，因此不存在媒体质量下降或水印量受限制等问题。另外，由于构造的零水印因宿主媒体而异，不像常规水印那样具有特定的内容，所以需要建立零水印信息库(IPR)作为数据版权的凭证。

零水印算法的主要技术难点：(1)构造比宿主媒体小得多的数字水印来标识该媒体的版权；(2)解决被篡改媒体的认证问题，即零水印的鲁棒性要强；(3)解决内容相似的媒体的版权识别，即零水印的唯一辩识性能要强。

本文基于这些考虑，提出以图像的特征点信息和尺寸信息作为零水印，在一定程度上克服了这些困难。

3 算法原理及仿真实验

本文仿真实验由三部分组成，第一部分是利用特征点构造零水印；第二部分是通过鉴别零水印信息的唯一独特性来确定版权阈值；第三部分是各种攻击实验及其对应的数据分析。

3.1 零水印的构造与检测

实验过程分两步完成，第一步完成对零水印的构造；第二步对各种攻击实验进行零水印的检测，包括确定版权阈值。

在构造零水印时，从原始图像中提取特征点的坐标位置信息，然后与原始图像尺寸组成零水印信息并存入IPR 库中作为版权依据。

在零水印的检测过程中，首先要确定一个版权阈值作为判断版权归属的标准。然后根据这个阈值判断受攻击图像的版权归属问题。判断受攻击图像(又称为受测图像)的版权过程为：首先按照 IPR 库中零水印的获取方法提取受测图像的零水印，然后以该零水印中的特征点构造出 Delaunay 三角网，最后计算这两个三角网的最小偏离度值，若该值小于预先设定的版权阈值，则可以确定受测图像的版权。

3.2 特征点提取的参数确定

本文的特征点提取通过 Harris 角点检测器实现。角点就是图像的一种特征点。在提取角点时，需要考虑的一个问题就是确定 Harris 角点检测的邻域大小。如果邻域太小，则在纹理复杂区域上会遍布特征点，将来在对这些特征点进行 Delaunay 分割的时候，生成的三角形会非常密集，使得三角形的尺寸变得很小。这样，即使两个完全不一样的小三角形，也会由于它们的尺寸较小而得到较小的偏离度，从而干扰实验的最终结果判断；而如果邻域太大，则特征点的数目会非常少，由此通过 Delaunay 分割所生成的三角形个数又非常少，容易造成三角形匹配的失败。因此，为了获得相对比较均匀的特征点分布，实验在利用 Harris 角点提取算法时，选择的邻域是以当前待考察点为中心的圆形，该圆的直径由受测图像的宽 W 和高 H 以及常量 γ 确定[4]，即：

$$D=\frac{W+H}{\gamma} \tag{3}$$

本文经过反复实验，最终确定了 $\gamma=25$。

3.3 版权阈值的确定

本文提出以最小偏离度作为版权阈值，依据是不相干图像之间具有较高的最小偏离度。

(1)最小偏离度计算

设 1 个三角形的三边长分别为：x_1, y_1, z_1 且 $x_1 \le y_1 \le z_1$；另 1 个三角形的三边长分别为：x_2, y_2, z_2 且 $x_2 \le y_2 \le z_2$。则称 $\Delta=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2+(z_1-z_2)^2}$ 为这 2 个三角形的偏离度。

如果 2 个三角形的偏离度为 0，则表示这 2 个三角形全等。偏离度越小，说明 2 个三角形的三边尺寸越相近；反之，则越不相近。

有了三角形之间的偏离度定义，最小偏离度则很容易定义了：

设一个三角形的集合 $A=\{A_1, A_2, \cdots, A_n\}$，则该集合中的三角形两两之间计算偏离度，一共可得 $k=C_n^2$ 个偏离度，记为：$\Delta=\{\Delta_1, \Delta_2, \cdots, \Delta_k\}$，则称 $\Delta_{\min}=\min\{\Delta_1, \Delta_2, \cdots, \Delta_k\}$ 为集合 A 的最小偏离度。

实验中，由于需要计算最小偏离度值的 2 个三角形集合实际上是 2 个 Delaunay 三角网，组成这 2 张网的每 1 个三角形顶点是图像的特征点。特别要注意的是，许多图像的端点(即 4 个角落或者与 4 个角落紧邻的 1 个像素位置上的点)往往是图像的特征点。对于完全不相关的两幅图像来说，这些端点将极有可能成为彼此关联性很强的特征点，如果它们参与构造三角形，很容易导致两幅图像三角网中三角形的偏离度变小，这显然不合理。为此，实验在计算最小偏离度值的时候，一律剔除含有端点的三角形。

(2) 版权阈值确定

为了能有效地确定合适的版权阈值，本文通过实验进行了分析。实验中以标准的 Lena 灰度图(256×256)作为研究对象，以标准的 Cameraman 灰度图 (256×256)和 Goldhill 灰度图(256×256)作为干扰图像。实验结果显示 Lena 图与 Cameraman 图的最小偏离度值为 8.148 5，Lena 图与 Goldhill 图的最小偏离度值为 6.099 6。据此，本文确定版权阈值为 5。

3.4 仿真实验及结果分析

仿真实验主要针对各种几何攻击，包括组合形式的几何攻击的情况。这些几何攻击限定于 RST(Rotation, Scaling and Translation)攻击。

实验中以 Lena 灰度图(256×256)作为研究对象。针

对对 Lena 图的每一种攻击，均做反复实验，各自列出具体数据进行分析。

(1) 旋转攻击

图 1 为 Lena 图在遭受旋转角度为 5°的攻击之后的 Delaunay 三角分割情况。

图 1 旋转 5°后的 Delaunay 三角网图

表 1 给出了 Lena 图在遭受各种程度的旋转攻击后，与 IPR 中零水印保存的信息对比而得到的最小偏离度值。旋转的角度数直接用数字表示，最小偏离度值用 Delta 表示(以下所有攻击实验中均采用此记法)。

通过表 1 可以看出，本文的算法对旋转攻击的鲁棒性比较好，尽管中间有个别角度的最小偏离度值相对其他值而言有些偏高，但保持在阈值以下，在零水印检测的时候，仍然可以确认版权。

(2) 缩放攻击

针对各种具体的缩放攻击，表 2 给出了 Lena 图在遭受这些缩放攻击后，与 IPR 中保存的零水印信息对比而得到的最小偏离度值。

通过表 2 可以看出，大幅度的缩放攻击对 Lena 图造成的质量损伤要普遍大于小幅度攻击造成的损伤。因为对 Lena 图的缩放幅度越大，其丢失的信息就越多，原来的特征点失去也多，最终导致了偏离度增大。

(3) 平移攻击

图像在平移攻击后，各实验中最小偏离度值均为 0，表现出了该方案对平移攻击有极强的鲁棒性。原因是图像的平移不会导致图像特征点之间的相对距离出现变化。

(4) 旋转与平移组合攻击

旋转和平移组合起来的几何攻击可以分为先旋转后平移与先平移后旋转 2 种类型。表 3 给出了各种情形下的最小偏离度值。为了数据表述简单起见，类似地简称“平移幅度为[x,y]的攻击”为“移[x,y]”，“旋转 x 度”简称为“旋 x”。以下所有攻击实验中均采用此记法。

表 3 旋转和平移组合攻击下的最小偏离度值

攻击类型	先旋 5 再移 [5,10]	先旋 5 再移 [10,10]	先旋 10 再移 [5,10]	先旋 10 再移 [10,10]
Delta	0.556 0	0.556 0	1.122 7	1.122 7
攻击类型	先移[5,10] 再旋 5	先移[10,10] 再旋 5	先移[5,10] 再旋 10	先移[10,10] 再旋 10
Delta	0.175 4	0.175 4	0.672 5	1.006 2

由表 3 中的数据可以看出，先对 Lena 图进行旋转攻击再进行平移攻击，所得到的最小偏离度值不依赖于平移幅度；而反过来，先平移再旋转的最小偏离度值却与平移的幅度有关。这是因为，先对图像进行旋转攻击后，特征点之间的相对位置由于旋转的关系，已经出现了扭曲(由计算旋转位置的误差所致)，但这种扭曲不会随着平移的进行而发生任何改变，因此，最终得到的结果必然与平移无关。而先对图像进行平移再进行旋转时，尽管特征点之间的相对位置不变，但是其绝对位置已经变化，这时再经过旋转变换，势必会使得最小偏离度值的结果同时依赖于平移和旋转 2 种操作。同时，表中的数据也表明，本文对旋转和平移组合攻击是鲁棒性的。

(5) 旋转与缩放组合攻击

旋转和缩放组合起来的几何攻击也可以分为先旋转后缩放和先缩放后旋转两种类型。表 4 给出了各种情形下的最小偏离度值。为了数据表述简单起见，将“缩放因子为 x 的缩放攻击”简称为“缩 x”，以下所有攻击实验中均采用此记法。

表 4 中的数据表明了本文对抗旋转和缩放联合攻击的鲁棒性。表中的数据还说明，尽管旋转角度和缩放因子一定，先对图像进行旋转攻击再进行缩放攻击与先对图像进行缩放攻击再进行旋转攻击，对图像质量造成的损伤是不一样的。

(6) 缩放与平移组合攻击

缩放与平移组合起来的几何攻击同样可以分为先缩放、后平移及先平移后缩放两种类型。表 5 给出了各种情况下的最小偏离度值。

由表 5 中的数据可以发现，当对 Lena 图先进行缩放攻击再进行平移攻击时，所得的最小偏离度值与平移的幅度没有关系。其原因与旋转平移相

表 1 旋转攻击下的最小偏离度值

旋转角度	1	2	3	4	5	10	15	20
Delta	0.295 4	0.032 2	0.534 3	0.128 9	0.556 0	1.122 7	1.146 0	0.782 3
旋转角度	25	30	35	40	45	50	55	60
Delta	0.688 2	0.972 4	0.203 5	3.225 2	0.730 0	0.462 7	0.841 4	0.512 2

表 2 缩放攻击下的最小偏离度值

缩放因子	0.4	0.5	0.6	0.8	1.2	1.5	1.8	2.0
Delta	4.920 4	3.413 1	4.224 1	2.100 8	0.281 1	1.139 0	3.973 5	3.983 7

表 4 旋转和缩放组合攻击下的最小偏离度值

攻击类型	先旋 5 再缩 1.2	先旋 4 再缩 0.8	先旋 4 再缩 1.5	先旋 2 再缩 1.2	先旋 2 再缩 0.8
Delta	0.550 8	3.940 8	2.206 6	0.731 1	3.417 8
攻击类型	先缩 1.2 再旋 5	先缩 0.8 再旋 5	先缩 1.5 再旋 2	先缩 1.2 再旋 2	先缩 0.8 再旋 2
Delta	0.789 2	1.347 5	1.420 6	0.848 2	2.450 7

表 5 缩放与平移组合攻击下的最小偏离度值

攻击类型	先缩 0.8 再移[5, 10]	先缩 0.8 再移[10, 10]	先缩 1.2 再移[5, 10]	先缩 1.2 再移[10, 10]
Delta	2.245 8	2.245 8	0.730 5	0.730 5
攻击类型	先移[5, 10] 再缩 1.2	先移[10, 10] 再缩 1.2	先移[5, 10] 再缩 0.8	先移[10, 10] 再缩 0.8
Delta	0.730 5	0.730 5	1.048 2	1.048 2

表6 RST 综合攻击下的最小偏离度值

攻击类型	先旋 5 再缩 1.2 后移[5,10]	先移[5,10]再旋 5 后缩 1.2	先移[10,10]再旋 5 后缩 0.8
Delta	0.550 8	2.551 7	2.480 3
攻击类型	先旋 5 再移[5,10]后缩 1.2	先缩 0.8 再移[10,10]后旋 5	先缩 1.2 再移[5, 10]后旋 5
Delta	0.550 8	3.135 3	0.997 5
攻击类型	先移[5,10]再缩 1.2 后旋 5	先缩 1.2 再移[10,10]后旋 10	先缩 0.8 再旋 5 后移[10,10]
Delta	0.789 2	2.050 8	1.347 5

组合的情况是一样的，即凡是平移攻击在最后的组合攻击中，最小偏离度值都与平移幅度没有关系。

(7) RST 综合攻击

RST 综合的几何攻击可以分为先旋转再缩放后平移、先旋转再平移后缩放、先缩放再旋转后平移、先缩放再平移后旋转、先平移再旋转后缩放和先平移再缩放后旋转 6 种类型。表 6 给出了各种情况下的最小偏离度值。

由表 6 中的数据可以看出，本文对抗 RST 综合攻击这类复杂的攻击组合具有较强的鲁棒性。

通过实验可以看出，本文算法对各类常见的几何攻击具有非常强的鲁棒性，特别是对于组合性的几何攻击也体现出了鲁棒性。这些成果归功于图像特征点的稳定性和算法对特征点的选取所采用的策略，有了比较合理的零水印，就能对各种 RST 攻击做出正确的回应。此外，提出了最小偏离度的概念，在此基础上确定的零水印版权阈值也对实验结果起到了至关重要的作用。

参考文献

[1] 温泉，孙锬锋，王树勋. 零水印的概念与应用[J]. 电子学报，2003，31(2): 214-216.

[2] 金聪，叶俊民，许凯华，等. 具有抗几何攻击能力的盲数字图像水印算法[J].计算机学报，2007，30(3):474-482.

[3] 闫龙，赵正旭，周以齐. 图像质量对 Harris 角点检测的影响研究[J]. 山东大学学报(工学版)，2006，36(5): 21-24.

[4] 邓峰森，王炳锡. 基于特征点的抗几何失真数字图像水印[J]. 信号处理，2005，21(1):12-16.

[5] XIAO Jun Qi, JI Qi. A robust content-based digital image watermarking scheme[J]. Signal Processing，2007，87(6):1264-1280.

[6] 马建湖，何甲兴. 基于小波变换的零水印算法[J]. 中国图像图形学报[J]，2007，12(4):581-585.

[7] 杨素敏，王嘉祯，彭德云，等. 基于 HVS 和小波变换的零水印数字图像算法[J]. 计算机工程与应用，2006，42(12): 63-65.

(收稿日期：2009-11-10)

作者简介：

王忠，男，1968 年生，副教授，博士研究生，主要研究方向：图像处理与数字水印技术。

叶雄飞，男，1983 年生，硕士研究生，主要研究方向：图像处理与数字水印技术。