基于伪 Zernike 的归一化分形水印算法研究 *

张语涵, 苗锡奎, 孙劲光
(辽宁工程技术大学 电子与信息工程学院, 辽宁 葫芦岛 125105)

摘 要: 以归一化技术,分形编码技术及伪 Zernike 矩相关知识为基础,提出一种可有效抵抗几何攻击的鲁棒数字水印新算法。算法首先利用归一化技术和不变质心理论在图像中提取出重要区域;然后利用分形编码及设置的阈值将重要区域分成自相似性块和非自相似性块并计算自相似性块的伪 Zernike 矩,从中选出最鲁棒的矩;最后通过量化调制伪 Zernike 矩幅值将水印嵌入其中。仿真实验表明,算法不仅具有较好的透明性,而且对常规信号处理(滤波、锐化、加噪和 JPEG 压缩等)和几何攻击(全局仿射变换、局部失真等)均具有较好的鲁棒性。

关键词: 分形水印; 几何攻击; 图像归一化; 分形编码; 伪 Zernike 矩
中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1863-04
doi:10.3969/j.issn.1001-3695.2010.05.073

New normalized fractal watermarking scheme based on pseudo-Zernike moments

ZHANG Yu-han, MIAO Xi-kui, SUN Jin-guang
(*Shool of Electronics & Information Engineering, Liaoning Technical University, Huludao Liaoning* 125105, *China*)

Abstract: This paper proposed a new image watermarking scheme robust to geometric attacks. Firstly, extracted significant region by using normalization and invariant centroid theory. Then, divided significant region into two groups: self-similarity and non-self-similarity blocks by fractal coding and pre-set threshold, picked up the robustest pseudo-Zernike moments among the pseudo-Zernike moments of the self-similarity blocks. Finally, embedded the watermark by quantizing the magnitudes of the robustest pseudo-Zernike moments. Experimental results show that the scheme is not only invisible and robust against common signals processing such as median filtering, sharpening, noise adding, JPEG compression, etc, but also robust against the geometric attacks such as affine transform, local geometric distortion, etc.

Key words: fractal watermarking; geometric attacks; image normalization; fractal coding; pseudo-Zernike moment

0 引言

目前,人们主要采用三种措施设计抗几何攻击的图像水印方案,分别为构造几何不变量、隐藏模板、利用原始图像重要特征。Dong 等人[1]利用基于矩的图像归一化将水印信号嵌入到几何不变量内,实现了水印系统对几何攻击的鲁棒性,但该方案仅能抵抗简单的全局仿射变换(即旋转、缩放和平移),尚无法有效抵抗,诸如行列去除、剪切、镜像翻转、随机扭曲等几何攻击,同时还普遍具有透明性较差等弱点。Chen 等人[2]计算水印图像的 Zernike 矩,重构后直接嵌入到原始图像中,但其无法有效抵抗缩放和平移等攻击。Li 等人[3]利用 SIFT 提取出图像的尺度不变特征区域,然后利用 Zernike 矩从特征区域中提取出不变水印嵌入其中,有效抵抗剪切攻击。李雷达等人[4]利用图像伪 Zernike 矩的幅度具有旋转不变的性质提出了一种抗几何攻击图像水印算法。文献[5]以 Zernike 矩理论为基础,提出了一种可有效抵抗几何攻击的数字水印新方案。文献[6]通过在图像 DFT 中频区域嵌入模板信息的方式来估计并校正图像所经历的几何变换,从而实现水印的同步。但其无法有效抵抗行列去除、剪切、镜像翻转、随机扭曲等几何攻击,而且水印容量受到限制。文献[7]提出了基于图像特征的数字水印方案,然而目前该类方法普遍存在特征点稳定性差且分布极不均匀等问题,严重影响了水印对常规信号处理的抵抗能力,水印容量有限(仅 16 bit)。

与传统的水印方案相比,分形技术为抗几何攻击的水印方案注入了新的活力。文献[8]是最早的分形水印文献,嵌入水印的策略是依靠改变定义域块的搜索范围实现的。相继利用分形技术又有很多新分形算法[9,10]。

鉴于此,针对不少抗几何攻击水印算只对小角度或特定角度的旋转具有鲁棒性,能够抵抗任意角度旋转的算法相对较少的问题。本文受到文献[4,5,8]的启发,以图像归一化和分形技术为基础,结合伪 Zernike 矩相关知识,提出一种可以有效抵抗几何攻击的强鲁棒数字图像水印算法,很好地解决了上述问题。

1 归一化重要区域与水印嵌入块

1.1 归一化图像重要区域的确定

图像归一化[1]过程是寻找一些合适的变换参数,将原始图像变换为惟一的标准形式,而且即使原始图像经过某种不可预测的几何仿射变换,仍然能够利用这些参数把经过仿射变换的图像归一化到这个惟一的标准形式。

收稿日期: 2009-07-12; **修回日期**: 2009-09-07 **基金项目**: 辽宁省高校重点实验室资助项目(2008s115)

作者简介:张语涵(1984-),女,硕士研究生,主要研究方向为数字水印、图形图像处理;苗锡奎(1984-),男,工程师,硕士研究生,主要研究方向为数字水印、图形图像处理(miaoxikui@163.com); 孙劲光(1962-),女,教授,博导,博士,主要研究方向为数字水印、图形、图像、多媒体技术.

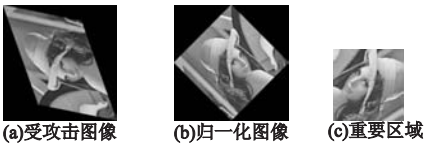
由于归一化图像带有黑边，不能将水印直接嵌入到整个归一化图像内，否则逆归一化过程将会导致部分水印信息丢失。为此，本文将利用区域不变质心理论，从归一化图像中提取出重要区域并用于水印嵌入。

设原始宿主图像的归一化图像为 $G=\{g(i,j),1\leqslant i\leqslant M,1\leqslant j\leqslant N\}$，$R$ 是归一化图像 G 的某个区域，则图像区域 R 的不变质心可以定义为

$$x_R=\frac{\sum_{x\in R}\sum_{y\in R}g(x,y)\cdot x}{\sum_{x\in R}\sum_{y\in R}g(x,y)},y_R=\frac{\sum_{x\in R}\sum_{y\in R}g(x,y)\cdot y}{\sum_{x\in R}\sum_{y\in R}g(x,y)}$$

归一化图像重要区域的确定方法步骤如下：a）利用高斯滤波器对归一化图像进行平滑处理，以消除噪声干扰；b）根据图像区域不变质心定义，计算整个归一化图像的质心 $C_0=(x_C,y_C)$，为不变质心初值；c）根据图像区域不变质心定义，计算出以 (x_C,y_C) 为圆心 r 为半径的圆形区域的不变质 $C_1=(x_C,y_C)$；d）若 $C_1=C_0$，则转 e），否则，令 $C_0=C_1$，并转 c）；e）C_0 为最终的不变质心。

最后，以整个归一化图像的不变质心为中心点，选取大小为 $S_1\times S_2$ 的矩形区域作为整个归一化图像的重要区域，如图 1 所示。采用此方法提取的质心不是由整幅图像提取而是由图像内部的一个限定区域来提取，这样可以避免图像受到剪切攻击后在图像中相对位置的变化。另外，由于不变质心将在滤波后的图像中进行，这样可以减小提取的不变质心受到 JPEG 压缩、加噪等攻击的影响。



(a)受攻击图像　(b)归一化图像　(c)重要区域

图1　归一化图像的重要区域

1.2　分形水印

通过对大量数字图像的分析和研究，笔者发现，一幅图像的不同部分之间、部分与整体之间存在着某种程度的相似，这种自相似性是图像本身所固有的属性，具有良好的稳定性，在一般的图像处理中是不容易被破坏的，自相似分形集的精细结构所蕴涵的自相似性，不会因几何失真操作而改变，具有很好的抗几何失真特性。这就给水印抗几何攻击提供了良好的思路，即可利用图像的自相似特性来实现水印的嵌入。

1.3　分形水印嵌入块的确定

按照一定的规则将图像分成若干个（设为 M）互相不重叠大小为 $B\times B$ 的值域块 $R_i(1\leqslant i\leqslant M)$ 和若干个（设为 N）可以互相重叠大小为 $2B\times 2B$ 的定义域块 $D_j(1\leqslant j\leqslant N)$。根据分形编码的原理，对每个值域块 R_i 寻找一个最佳匹配的定义域块 D_j，该定义域块通过收缩仿射变换 τ_{ik}（缩放、平移、旋转、灰度拉伸等）后能够以最小的误差逼近 R_i，即 $R_i\approx\tau_{ik}(D_j)$。误差大小反映了 R_i 与 D_j 的相似程度。本文用最小均方误差（MSE）$d(R_i,\tau_{ij}(D_j))$ 来衡量值域块与定义域块的相似程度。

$$d(R_i,\tau_{ik}(D_k))=\min d(R_i,\tau_{ij}(D_j))$$

然后，可以事先设定一个误差阈值 ε_0（仍然作为密钥），对于最小均方误差小于给定域值的值域块笔者称之为自相似性块，反之，称之为非自相似性块。显然，误差阈值决定了值域块的分类，为满足嵌入水印容量的需要，其选择应根据要嵌入水印的容量和值域块容量的比较来确定，总的原则是在误差阈值的控制下，各嵌入块的容量总和不小于水印的总容量。为使水印的不可见性最佳，本文每个自相似性块仅嵌入 1 bit 水印。另外，由于将自相似性块作为水印嵌入块也能很好地抵抗剪切攻击。

2　伪 *Zernike* 矩及其性质

2.1　伪 *Zernike* 矩的计算

图像的伪 Zernike 矩是将图像映射到一组基函数上得到的，称伪 Zernike 矩的基，记为 $\{V_{nm}(x,y)\}$。这组基构成了单位圆 $(x^2+y^2\leqslant 1)$ 内的一组完备正交集，其定义为

$$V_{nm}(x,y)=V_{nm}(\rho,\theta)=R_{nm}(\rho)\exp(jm\theta)$$

其中：n 为非负整数，m 为整数，$|m|\leqslant n$；分别为极坐标下像素的半径和角度；$R_{nm}(\rho)$ 为径向多项式，定义为

$$R_{nm}(\rho)=\sum_{s=0}^{n-|m|}\frac{(-1)^s(2n+1-s)!\ \rho^{n-s}}{S!\ (n+|m|+1-s)!\ (n+|m|-S)!}$$

这些多项式相互正交，满足：

$$\iint_{x^2+y^2\leqslant 1}V_{nm}^*(x,y)\cdot V_{pq}(x,y)\,\mathrm{d}x\mathrm{d}y=\frac{\pi}{n+1}\delta_{np}\delta_{mq}。$$

对于一幅数字图像 $f(x,y)$，阶数为 n，重复度为 m 的伪 Zernike 矩定义如下：

$$Z_{nm}=\frac{\pi}{n+1}\sum_{\rho\leqslant 1}\sum_{0\leqslant\theta\leqslant 2\pi}f(\rho,\theta)R_{nm}(\rho)\exp(jm\theta)\rho$$

若已知图像最高 $n_{\max}$ 阶的伪 Zernike 矩，由其完备性和正交性，有如下的重构公式：

$$f'(x,y)=\sum_{n=0}^{n_{\max}}\sum_{m=-n}^{n}Z_{nm}V_{nm}(x,y)$$

2.2　伪 *Zernike* 矩的性质

伪 Zernike 矩的幅度具有旋转不变性。另外，与 Zernike 矩相比，其不仅具有旋转不变性、更低的噪声敏感性，而且还具有表达有效性、计算快速性以及多级表达性等特点，故更加适合于设计抗几何攻击图像水印。

3　伪 Zernike 矩归一化分形水印算法

3.1　水印的产生

由密钥 key1 产生一个伪随机序列 $W=\{w_i\in\{0,1\},i=1,2,\cdots,L\}$ 作为数字水印信息。其中：L 为水印的长度，本文 $L=128$。

3.2　矩的选择

由伪 Zernike 矩相关理论得知，部分伪 Zernike 矩存在微小的计算误差。也就是说，必须合理选择伪 Zernike 矩用于水印嵌入。总体说来，选择伪 Zernike 矩应该考虑如下两个方面：

a）选择阶数较低的伪 Zernike 矩。因为当阶数高于某一数值 $N_{\max}$ 时，伪 Zernike 矩计算将不再准确。本文选取 $N_{\max}=20$；

b）重复度为 $m=4i(i=0,1,2,\cdots)$ 的伪 Zernike 矩存在微小计算误差，故不适合嵌入水印。显然，可用于数字水印嵌入的伪 Zernike 矩集合为

$$E=\{Z_{nm},n\leqslant N_{\max},m\geqslant 0,m\neq 4i\}$$

3.3　数字水印的嵌入

设原始载体图像为 $512\times 512\times 8$ bit 标准灰度 Lena 图像 $I=\{f(i,j),1\leqslant i\leqslant 512,1\leqslant j\leqslant 512\}$。归一化图像的重要区域大小为 256×256，值域块、定义域块大小分别为 8×8、16×16，误差阈值 $\varepsilon_0=4.3$。水印的嵌入过程可描述如下：

a）提取图像归一化重要区域，参考文献[1]和 1.1 节。

b)自相似性块(水印嵌入块)的确定。按照误差阈值 ε_0,在重要区域中提取自相似性块 $S_i(1\leqslant i\leqslant 128)$。

c)计算每个自相似性块的伪 Zernike 矩[11],并按照 3.2 节矩的选择原则得到集合 $E_i(1\leqslant i\leqslant 128)$。

d)对集合 E_i 中的矩进行幅度改变量测试,得到最优矩集合 E_{opt},作为最终修改的矩,供水印嵌入与提取时使用。

需要注意的是,在修改的矩数目较少时,被修改矩的幅度变化很明显,对其他矩幅度的影响较小。然而,当修改的矩数目较多时,这种影响会累积,从而使得未修改的矩幅度变化也比较明显,这对于水印检测是很不利的。为了减小这种影响,对集合中 E_i 的矩进行预修改测试,即对 E_i 中的所有矩进行修改,并进行重构图像;再次计算重构图像的伪 Zernike 矩,求两次计算矩的幅度差,并从中选出至少 128 个幅度改变较大的矩(每个 E_i 中至少选择一个),作为最终修改的矩集合,记这个集合为 E_{opt}。

为了提高系统安全性能,本文利用密钥 key2 从 E_{opt} 中随机选择 128 个伪 Zernike 矩 $Z=(Z_{p_1q_1},\cdots,Z_{p_Lq_L})$ 用于水印嵌入。设其对应的幅值为 $A=(A_{p_1q_1},\cdots,A_{p_Lq_L})$。

e)量化嵌入。本文采用量化调制伪 Zernike 矩幅值的方法实现水印信号嵌入,量化规则如下:

$$A'_{p_iq_i}=\left[\frac{A_{p_iq_i}-d(w_i)}{\Delta}\right]\cdot\Delta+d(w_i);i=1,2,\cdots,L$$

其中:[·]表示四舍五入;Δ 是量化步长;$d(\cdot)$ 是通过密钥 key3 产生的量化函数,而且满足 $d(1)=\frac{\Delta}{2}+d(0)$,$d(0)\in[0,1]$。需要说明的是量化伪 Zernike 矩幅值 $A_{p_iq_i}$ 时,如果 $q_i\neq 0$,应该同时量化它的共轭幅值 $A_{p_i-q_i}$,以保证其具有相同幅值。另外,考虑到算法效率与嵌入水印的质量,量化步 Δ 长大小很重要。经过实验确定,对于灰度图像 $\Delta=[0.3\times\text{gray}]$ 或 $[0.4\times\text{gray}]$ 比较适宜。其中 gray 是整幅图像平均灰度值。

f)含水印自相似性块图像的获得。将自相似性块中未被修改的伪 Zernike 矩与已被修改的伪 Zernike 矩合并,并重构图像,便得到含水印自相似性块图像。

g)含水印图像重要区域获得。将 f)得到的含水印自相似性块与非自相似性块合并即得到重要区域。

h)将含水印图像重要区域与非重要区域合并作逆归一化处理即得到含水印图像。

3.4　数字水印的提取

水印提取是水印嵌入的逆过程。整个数字水印的检测关键步骤如下:

a)提取图像归一化[1]重要区域。

b)在重要区域中提取自相似性块 $S_i(1\leqslant i\leqslant 128)$。

c)计算 S_i 伪 Zernike 矩得到集合 $E_i(1\leqslant i\leqslant 128)$。

d)按照 3.3 节 e)的方法得到最优矩集合 E_{opt}。

e)利用密钥 key2 选择 128 个伪 Zernike 矩 $Z'=(Z'_{p1q1},\cdots,Z'_{pLqL})$ 用于水印提取。设其对应的幅值为 $A'=(A'_{p1q1},\cdots,A'_{pLqL})$。具体过程如下:

利用密钥 key3 产生量化函数 $d(\cdot)$,采用与嵌入过程相同的量化公式用 $d(0)$,$d(1)$ 分别量化 $A'_{piqi}(i=1,2,\cdots,L)$。

$$(A'_{piqi})_j=\left[\frac{A'_{piqi}-d(j)}{\Delta}\right]\cdot\Delta+d(j)\quad(j=0,1)$$

通过上面的公式,可以得到两组向量式 $(A'_{piqi})_0$ 和 $(A'_{piqi})_1$,$i=1,2,\cdots,L$。

通过如下关系即可获取水印。

$$k=((A'_{piqi})_0-A'_{piqi})^2-((A'_{piqi})_1-A'_{piqi})^2$$

如果 $k>0$ 则 $w'_i=1$,否则 $w'_i=0$。

f)将提取水印与原始水印比较,计算失真率 BER。

其中 BER 的大小主要受图像质心和伪 Zernike 矩的稳定性的影响。本文利用归一化和分形编码技术在图像中提取出具有抗几何失真特性的归一化自相似性块作为水印嵌入块,同时在自相似性块中利用幅度改变量测试,计算出最适合嵌入水印的伪 Zernike 矩,使水印具有更好的鲁棒性。另外借助伪 Zernike 矩的旋转不变性,使水印的鲁棒性得到巩固,从而有效地降低了失真率。

4　仿真实验结果

为了验证本文数字图像水印算法的有效性,以下分别给出了透明性测试、水印容量对比、抗攻击能力(鲁棒性)测试的实验结果,并与文献[1,5]算法进行了对比。其中算法的鲁棒性本文选用失真率(BER)来衡量。实验中,宿主图像为 512×512×8 bit 标准灰度 Lena,水印是由密钥 key1 产生一个长度为 128 B 的伪随机序列,量化步长 $\Delta=3$,如图 2 为重要区域自相似性块,图 3 为含有水印图像。表 1 给出了两种水印方案的透明性和水印容量的对比实验结果。

图2　重要区域自相似性块

图3　含水印图像

表 1　透明性与容量对比实验

	本文算法	Dong[3]	Xin[7]
PSNR/dB	44.45	35.07	44.367
capacity/bit	128	50	64

为了检测算法的鲁棒性,仿真实验分别对本文算法、文献[5]算法的含水印图像进行了一系列攻击,对比结果如表 2、3 所示。

表 2　水印对常规信号处理的抵抗能力(失真率 BER)

攻击方式		本文算法	Xin[5]
JPEG 压缩	90	0	0
	70	0	15.62
	30	4.56	16.13
高斯滤波	3×3	10.86	15.62
	5×5	17.78	53.12
高斯噪声	0;0.01	14.48	42.18
	0;0.002	10.73	53.56
椒盐噪声	0.01	9.18	51.56
	0.002	1.24	2.34

5　结束语

本文将归一化技术,分形技术及伪 Zernike 矩相结合,将水印嵌入到归一化自相似性块中,有效地解决了剪切攻击。利用归一化和伪 Zernike 矩的良好性质,有效地弥补了分形技术的不足,从而使所设计的算法对几何攻击具有高度的鲁棒性。从以上实验可以看出,本方案不但在水印的容量和透明性方面优于其他水印方案,而且失真率(BER)也优于其他水印方案。算法的主要特点:a)基于归一化技术和分形编码技术在图像中

提取出具有抗几何失真特性的归一化自相似性块作为水印嵌入块。b)利用伪 Zernike 矩的良好性质,有效地弥补了分形的不足,从而使所设计的算法对几何攻击具有高度的鲁棒性。c)利用幅度改变量测试,在自相似性块中计算出最适合嵌入水印的伪 Zernike 矩,使水印提取更加准确。此外,本方案还具有容易实现、提取水印时无须原始载体等优点,这大大增强了其用于数字图像作品版权保护的实用性,具有一定的应用价值。

表 3 算法对几何攻击及联合的抵抗能力(失真率 BER)

攻击方式		本算法	Xin[5]
旋转单位(度)	5	2.03	6.25
	10	0.98	1.56
	15	2.12	7.81
	20	0	3.12
	25	2.18	4.68
	30	3.09	5.12
	45	4.87	9.76
	60	2.08	6.02
	90	0	0
缩放	0.8	3.86	7.81
	0.9	1.08	1.56
平移(水平、垂直方向)	10	19.54	48.43
	20	12.62	43.75
	30	10.83	42.18
垂直翻转		0	0
水平翻转		0	0
缩放 1.2 + 旋转 10		3.86	4.68
缩放 1.2 + 平移 10		11.97	50.00
旋转 10 度 + 平移 20		11.04	45.31

参考文献:

[1] DONG P, BRANKOV J. G, GALATSANOS N P, *et al*. Digital watermarking robust to geometric distortions[J]. IEEE Trans on Image Processing, 2005, 12(14): 2140-2150.

[2] CHEN Qing, YANG Xiao-li, ZHAO Ji-ying. Robust image watermarking with Zernike moments[C]//Proc of CCECE 2005. Canada: IEEE, 2005: 1340-1343.

[3] LI Lei-da, GUO Bao-long, SHAO Kai. Geometrically robust image watermarking using scale-invariant feature transform and Zernike moments[J]. Chinese Optics Letters, 2007, 5(6): 332-335.

[4] 李雷达,郭宝龙,刘雅. 基于伪 Zernike 矩的抗几何攻击图像水印[J]. 光电子· 激光,2007,18(2):231-235.

[5] XIN Yong-qing, LIAO S, PAWLAK M. A multibit geometrically robust image watermark based on Zernike moments[C]// Proc of the 17th International Conference on Pattern Recognition. Cambridge, UK: IEEE Press, 2004: 861-864.

[6] KANG Xian-gui, HUANG Ji-wu, YUN Shi, *et al*. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression,[J]. IEEE Trans on Circuits and Systems for Video Technology, 2003, 13(8): 776-786.

[7] JIN S S, CHANG D Y. Image watermarking based on invariant regions of scale-space representation[J]. IEEE Trans on Signal Processing, 2006, 54(4): 1537-1549.

[8] PAUTE J, JORDAN F. Using Fractal compression scheme to embed a digital signature into an image[C]// Proc of SPIE Photonics East Symposium. Boston: [s. n], 1996: 108-118.

[9] PI Ming-hong, LI Chun-hung, LI Hua. Anovel fractal image watermarking watermarking[J]. IEEE Trans on Multimedia, 2006, 8(3): 488-499.

[10] XIE Rong-sheng, YANG Shu-guo. A digital image watermarking method based on fractal transform in DWT domain[C]// Proc of the 1st International Conference on Modelling and Simulation. 2008.

[11] HADDADNIA J, AHMADI M, FAEZ K. An efficient feature extraction method with Pseudo-Zernike moment in RBF neural network-based human face recognition system[J]. EURASIP Journal on Applied Signal Processing, 2003, 2003(9): 890-901.

(上接第 1849 页)节点依据相关信任模型降低其信任度。为了提高检测的精确度,TEBA 参考使用了多节点协作检测思想。仿真结果表明,TEBA 能对 Sybil 节点作出有效检测,且在仿真条件相近的情况下较之于 CRSD 检测方案具有更高的系统吞吐量。事实上,为了验证其正确性和有效性,本文对于 TEBA 检测方案仅仅是做出了初步的调查结果。如何使其更为适用于普遍的路由协议如 AODV、DSDV 等和提高安全防范性能将是未来研究的工作重点。

参考文献:

[1] AYDAY E, DELGOSHA F, FEKRI F. Location-aware security services for wireless sensor networks using network coding [J]. IEEE International Conference on Computer Communications, 2007 (6-7): 1226-1234.

[2] 王晓东,孙言强,孟祥旭. WSN 中基于簇的 Sybil 攻击防御机制[J]. 计算机工程,2009,35(15):129-131.

[3] 冯涛, 马建峰. 防御无线传感器网络 Sybil 攻击的新方法[J]. 通信学报,2008,29(6):13-19.

[4] 聂晓文, 卢显良, 唐晖. 基于洗牌策略的 Sybil 攻击防御[J]. 电子学报,2008,36(11): 2144-2149.

[5] WEN M, LI H, ZHENG Y, *et al*. TDOA-based Sybil attack detection scheme for wireless sensor networks [J]. Journal of Shanghai University: English Edition, 2008, 12 (1): 66-70.

[6] DEMIRBAS M, SONG Y. An RSSI-based scheme for Sybil attack detection in wireless sensor networks[C]// Proc of International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2006: 568-570.

[7] PRIYANTHA N B, MIU A K L, BALAKRISHNAN H, *et al*. The cricket compass for context-aware mobile applications[C]// Proc of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM). New York: ACM Press, 2001: 1-14.

[8] LV Shao-he, WANG Xiao-dong, ZHAO Xin, *et al*. Detecting the Sybil attack cooperatively in wireless sensor networks[C]// Proc of International Conference on Computational Intelligence and Security. 2008: 442-446.

[9] DAI Hong-jun, JIA Zhi-ping, DONG Xiao-na. An entropy-based trust modeling and evaluation for wireless sensor networks[C]// Proc of International Conference on Embedded Software and Systems. Washington DC: IEEE Computer Society, 2008: 27-34.

[10] 朱运波,胡向东. WSN 中防御 Sybil 病毒攻击的密钥预分配方案[J]. 通信技术,2008,41(8).

[11] BOUKERCH A, XU L, EL-KHATIB K. Trust-based security for wireless Ad hoc and sensor networks [J]. Computer Communications, 2007, 30(11-12): 2413-2427.

[12] ATAKLI I M, HU Hong-bing, CHEN Yu, *et al*. Malicious node detection in wireless sensor networks using weighted trust evaluation [C]// Proc of Spring Simulation Multi Conference. 2008: 1066-1069.