# 基于参数优化 SVM 融合的网络异常检测

陈 烨[1,2] 刘 渊[1]
[1](江南大学数媒学院 江苏 无锡 214122)
[2](江苏省信息融合软件工程技术研发中心 江苏 江阴 214405)

**摘 要** 网络异常检测技术是入侵检测系统中不可或缺的部分。然而目前的入侵检测系统普遍存在检测率不高,误报率过高等问题,从而难以在实际的企业中大规模采用。针对之前的检测技术检测效果不佳的问题,提出基于 SVM 回归和改进 D-S 证据理论的入侵检测方法。该方法是将支持向量机回归的分类融合应用到网络异常行为分析中,在 SVM 参数选择时采用交叉验证和深度优先搜索算法进行优化选择,并通过融合证据理论,建立网络异常检测模型。通过仿真实验表明,该模型能够有效地提高入侵检测性能,缩短检测时间。

**关键词** 异常行为分析 支持向量机 回归 参数优化 交叉验证

**中图分类号** TP393 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2013.09.012

# NETWORK ANOMALY DETECTION BASED ON PARAMETERS OPTIMISED SVM FUSION

Chen Ye[1,2] Liu Yuan[1]
[1](*School of Digital Media, Jiangnan University, Wuxi 214122, Jiangsu, China*)
[2](*Jiangsu Engineering R&D Center for Information Fusion Software, Jiangyin 214405, Jiangsu, China*)

**Abstract** Network anomaly detection technology is an indispensable part in intrusion detection system. However, currently the poor detection rate and high false positive rate in intrusion detection systems are widely existed, so the large-scale use of it is difficult in practical enterprises. Aiming at the poor detection effect in previous detection technologies, we propose an intrusion detection method which is based on SVM recession and improved D-S evidence theory. This method applies the classifier fusion of support vector machine's regression to network abnormal behaviour analysis, and uses cross-validation and depth-first search algorithm for optimised selection when choosing the SVM parameters; it builds a network abnormal detection model with D-S evidence theory. Through the experiment it is proved that this method can effectively improve the intrusion detection performance and shorten the detection time.

**Keywords** Abnormal behaviour analysis Support vector machine Regression Parameters optimisation Cross-validation

## 0 引 言

随着互联网的高速发展,各种针对计算机的网络入侵行为日渐频繁。为了有效地遏制这些网络入侵行为,在上世纪 80 年代初提出了网络入侵检测系统。入侵检测系统作为网络安全防御系统不可或缺的组成部分,它通过各种机器学习的方法,建立在正常情况下数据的网络异常检测模型,将当前收集到的网络数据在模型中进行决策,发现异常并进行报警。

到目前为止,针对入侵检测提出的方法有概率统计分析方法[1]、数据挖掘方法[2]、人工神经网络方法[3]、模糊数学理论[4]等。但是,单一的检测性能和较长的训练时间,限制了入侵检测系统在实际中的应用。

本文把基于参数优化的 SVM 和 DS 证据理论融合,解决了单一分类器对所有攻击检测率不高的问题,又用交叉验证和深度优先搜索算法为 SVM 回归找到最优参数,并得出寻优后的 SVM 回归结果,将其作为证据理论中的参数,建立分类融合模型并采用 KDD99 数据集进行仿真实验,实验结果表明,本文提出的入侵检测模型缩短了融合分类器的检测时间,提高了融合分类器的准确率。

## 1 支持向量机

### 1.1 支持向量机回归的基本原理

支持向量机 SVM 采用统计学习理论中的 VC 维理论和结构风险最小原理,在解决小样本、非线性及高维模式识别中表现出许多特有的优势。

设训练样本$\{x_i, y_i\}$(其中 $i=1,2,\cdots,n$,$x_i$ 是输入模式的第 $i$ 个样本,$y_i \in \{+1, -1\}$)。在线性条件下,SVM 回归使用线性

收稿日期:2012-08-12。国家自然科学基金项目(61103223);江苏省自然科学基金重点研究专项项目(BK2011003);江苏省信息融合软件工程技术研究开发中心开放基金项目(SR-2011-05)。**陈烨**,硕士生,主研领域:网络流量与网络安全技术。**刘渊**,教授。

函数 $f(x,w)=(w,x)+b$ 对样本点进行拟合;在非线性条件下,SVM 回归则是将样本映射到高维特征空间,并在高维特征空间中建立线性模型 $f(x,w)=(w,\varphi(x))+b$,其中 $\varphi(x)$ 是将样本点映射到高维空间的非线性变换,SVM 回归可以表示为:

$$\min \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{l}(\xi_i + \xi_i^*) \tag{1}$$

$$\text{s.t.} \quad f(x_i,w) - y_i \leqslant \varepsilon + \xi_i$$

$$y_i - f(x_i,w) \leqslant \varepsilon + \xi_i^*$$

$$\xi_i,\xi_i^* \geqslant 0 \quad i=1,\cdots,l$$

其中:$\|w\|^2$ 表示与模型复杂度相关的因素;$C>0$ 为一个常数,称为惩罚参数 $C$;$\varepsilon$ 表示不敏感损失函数;$\xi_i,\xi_i^*$ 表示样本偏离 $\varepsilon$ 区域的程度,称为松弛变量。

对于优化问题式(1),用 Lagrange 乘子法可以解决二次最规划问题,最终转化为其对偶问题,则判断函数为:

$$f(x) = \left(\sum_{i=1}^{l}(-\alpha_i + \alpha_i^*)K(x_i,x) + b\right) \tag{2}$$

其中 $K(x_i,x_j)$ 称为核函数,满足 Mercer 条件。惩罚参数 $C$ 以及核函数的选择与检测模型的成功存在一定关系[7]。

### 1.2 核函数和参数的选择

1.2.1 RBF 核

本文选取径向基核(RBF)函数作为 SVM 回归的核函数,径向基核(RBF)函数定义为:

$$K(x_i,x_j) = \exp(-\gamma\|x_i - x_j\|^2) \quad \gamma>0 \tag{3}$$

把式(3)带入式(2),得到 SVM 回归判断函数:

$$f(x) = \left(\sum_{i=1}^{l}(-\alpha_i + \alpha_i^*)\right)\exp(-\gamma\|x_i - x_j\|^2) + b) \tag{4}$$

因此,为了使 SVM 回归的性能最优,需要确定不敏感损失函数 $\varepsilon$、惩罚参数 $C$ 以及核参数 $\gamma$。

1.2.2 交叉验证和深度优先搜索算法

交叉验证:将训练数据集分成相等的 $k$ 个子集,其他 $k-1$ 个子集用来训练,交叉验证重复 $k$ 次,每个子样验证一次,$k$ 次迭代后的 MSE 值来估计期望泛化误差,最后选择一组最优的参数。

深度优先搜索算法:假设图中所有顶点都未被访问过,任选顶点 i 为出发点,然后依次搜索 $i$ 的未被访问的邻接点,直到图中所有与 $i$ 有相连的顶点都被访问为止。如果图中尚有顶点还未被访问,那么就另外选图中未曾访问的顶点作为起始点,重复上述步骤,直到图中所有顶点都被访问为止。

在参数 $C$ 和 $\gamma$ 上使用深度优先搜索的方式进行交叉验证,并找出 MSE 值最小的参数对作为最终参数进行训练。但完全的深度优先搜索会比较耗时,因此可采用启发式在上一轮参数对的附近重新定义范围,加快搜索速度。

对参数进行寻优(交叉验证和深度优先搜索算法):

① 根据以往研究经验设置参数的范围(参数 $C$ 的范围为 $2^{-5}\sim2^5$,步长为 2,$\gamma$ 的范围为 0.1 到 1,步长为 0.1),并按步长对进行均匀划分,并采用 10 折交叉验证方法,统计每组参数的均方根误差,选择均方根误差最小对应的参数为本轮 SVM 的最佳参数组合。

② 将本轮 SVM 最优参数和上一轮最优参数的均方根误差进行对比,如果小于上一轮均方根误差,那么就跳转步骤③,否则寻优结束,找到最优参数。

③ 根据上一轮 SVM 参数,采用启发式在该参数附近重定义范围,进行局部搜索。具体修改方式为:上阶段的步长范围改变,$C$ 的步长变为 1,$\gamma$ 的步长变为 0.1,参数范围上限 = 最优参数-步长,下限 = 最优参数 + 步长。然后跳转步骤①,重新进行递归运算。

使用深度优先搜索算法对 SVM 回归进行训练,得出最优参数。

## 2 Dempster-Shafer 证据理论基础

### 2.1 经典的 D-S 理论

D-S 证据理论是建立在非空有限域 $\Theta$ 上的理论,表示有限个系统状态 $\{A1,A2,\cdots,An\}$,$\Theta$ 称为辨识框架,而系统状态 $\Theta$ 的幂集 $P(\Theta)$ 中的一个元素称为系统状态假设 $Hi$。为了推测出当前系统所处的状态,D-S 证据理论通过一些对系统状态的观察 $E1,E2,\cdots Em$,来实现。证据理论中的三个重要函数如下:

**定义 1** 基本置信分配函数 BPA(basic probability assignment),设函数 $m$:设函数 $m:2^\Theta\to[0,1]$,且满足:$m:(\varnothing)=0$,$\sum_{A\in2\Theta}m(A)=1$,$m(A)\to[0,1](A\in2^\Theta)$,$m(A)$ 称为焦元 $A$ 的基本概率数,表示依据当前的环境对焦元 $A$ 的信任程度。

**定义 2** 信任函数 Bel(Belief Function):

$$Bel(A) = \sum_{B|B\in A} m(B) \tag{5}$$

表示对焦元 $A$ 的信任程度。

**定义 3** D-S 证据理论的合成规则:

$$\begin{cases} m(A) = m_1 \oplus m_2 \oplus \cdots m_n(A) = \dfrac{\sum\limits_{A_1\cap A_2\cap\cdots A_n=A}\prod\limits_{i=1}^{n}m_i(A_i)}{1-k} & A\neq\varnothing \\ m(\varnothing) = m_1 \oplus m_2 \oplus \cdots m_n(\varnothing) = 0 & \\ k = \sum\limits_{A_1\cap A_2\cap\cdots A_n=\varnothing}\prod\limits_{i=1}^{n}m_i(A_i) & k\neq1 \end{cases} \tag{6}$$

### 2.2 经典证据理论的缺陷

在实际运用中,经典 D-S 理论存在如下不足:当各证据间的基本概率分配函数存在严重冲突时,融合后得到的结果明显不合理;而且焦元的基本信任分配发生的极其微小变化会带来组合结果剧烈的变化。这些不足很可能导致判断错误,从而影响入侵检测系统的检测性能。

### 2.3 组合规则改进

针对各证据间的冲突问题,文中应用一种基于加权的 D-S 证据合成方法[2]:考虑到各证据之间、焦元之间的相关性,引入平均证据距离,计算各证据的可信度并作为该证据的权值。该方法通过平均证据,计算平均证据距离,并得出加权系数,区分各证据在 D-S 融合中的影响程度,从而解决冲突证据的组合问题。

首先,计算各证据的平均值:

$$\overline{m} = \frac{m_1 + m_2 + \cdots + m_n}{n} \tag{7}$$

然后,计算各证据到平均证据的距离:

$$d_i = e^{-|m_i(A)-\overline{m}(A)|} + e^{-|m_i(B)-\overline{m}(B)|} + \cdots \quad i=1,2,\cdots,m \tag{8}$$

由式(6)知两个证据体中相似性程度与对应概率的距离成反比,距离小的相似性程度就大,可令该距离为证据体的支持度,即 $s(m_i)=d_i$。

最后,计算各证据的可信度:

$$c(m_i) = \frac{s(m_i)}{\sum_{i=1,2,\cdots,3} s(m_i)} \tag{9}$$

其中,$c(m_i)$作为证据 $m_i$的权重,满足 $\sum_{i=1,\cdots,n} c(m_i) = 1$,其他证据体对证据的支持程度表现在该证据的权值上。证据的权值高,则其支持程度高,对组合结果影响大;反之亦然。

那么,可以得出加权 D-S 证据的合成规则是:

$$(m_i \oplus m_j)(A) = \frac{\sum_{A_k \cap A_{k'} = A} [c_i m_i(A_k) \cdot c_j m_j(A_{k'})]}{1 - \sum_{A_k \cap A_{k'} = \phi} [c_i m_i(A_k) \cdot c_j m_j(A_{k'})]} \tag{10}$$

## 3　基于参数优化的 SVM 融合

### 3.1　基于参数优化的 SVM 融合模型

基于参数优化的 SVM 融合的网络异常行为检测模型如图 1 所示。

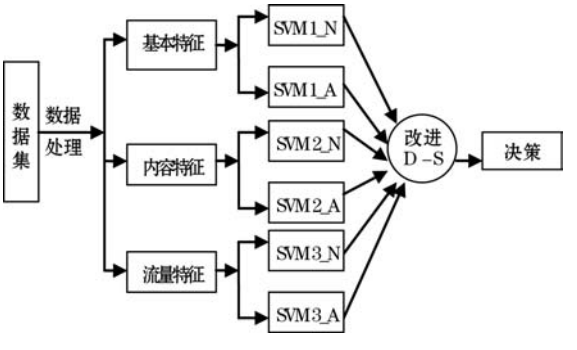


图 1　基于参数优化的 SVM 融合模型

将采集的数据集进行数据预处理,用训练数据集训练模型,在建立好的检测模型上用测试数据集进行决策,对于当前的一条网络连接,按基本特征、流量特征和内容特征进行特征分类提取。将基本特征分别通过训练好的 SVM1_N 和 SVM1_A 进行预测,将结果存入 $m1(N)$和 $m1(A)$中;将流量特征分别通过 SVM2_N 和 SVM1_A 进行预测,将结果存入 $m2(N)$和 $m2(A)$中;将内容特征分别通过 SVM3_N 和 SVM3_A 进行预测,将结果存入 $m3(N)$和 $m3(A)$中。即可得到各个 SVM 分类器对 $A$、$N$、$\{N,A\}$的可信度。代入 D-S 合成规则式(10),最终得出检测结果。至此,决策阶段完毕。

### 3.2　基于参数优化的 SVM 融合检测模型的实现

**步骤 1**　底层各个 SVM 分类器部分的实现:将训练数据集,按其特征属性分为三类,分别使用交叉验证和深度优先搜索算法对 SVM 回归进行训练,得出最优参数。

**步骤 2**　基于参数优化的 SVM 融合部分的实现:

基本置信分配函数的确定:

首先令识别框架 $\Theta$ 为$\{N,A\}$,$N$ 表示正常,$A$ 表示异常,且 $N \cap A = \phi$。定义基本置信分配函数 $m: P(\{N,A\}) \rightarrow [0,1]$,$m(\phi) = 0$,$m(\{N,A\}) + m(N) + m(A) = 1$,其中 $m(N)$表示当前特征支持正常行为的可信度,$m(A)$表示当前特征异常行为的可信度,而 $m(\{N,A\})$表示不能确定当前行为属于正常或者异常行为的可信度。

融合模型中采用了一对 SVM_N 和 SVM_A 分类器来对一类特征进行回归。N 分类器给出了在该特征下的正常行为的可信度,A 分类器给出了在该特征下的异常行为的可信度。首先分别计算出正常行为的聚类中心 DN 和异常行为的聚类中心 DA。在训练 $N$ 分类器时,计算正常行为 $N$ 到 $DN$ 的距离 $DN\_N$ 并取正值,同理计算异常行为的距离 $DN\_A$ 取负值,都保存到 $N\_L$ 中,并进行[0,1]范围内的归一化,作为 $N$ 分类器的训练标签。同理,$A$ 分类器,计算异常行为到 $DA$ 的距离 $DA\_A$ 取负值,正常行为到 $DA$ 的距离取正值,都保存到 $A\_L$ 中,并进行[0,1]范围内的归一化,作为 $A$ 分类器的训练标签。这样图 1 中的 6 个分类器转化为 $N$ 和 $A$ 分类器,并用相应有 $N\_L$ 与 $A\_L$ 的标签进行回归训练。

将上述分类器训练好,将测试数据集分别采用上面训练好的 6 个分类器的回归功能对测试数据集进行估计。这样分别利用 SVM1,SVM2,SVM3 对测试数据集进行基本置信值预测。保存结果到 $m1(N)$,$m1(A)$,$m2(N)$,$m2(A)$,$m3(N)$,$m3(A)$,即可得到各个 SVM 分类器对 $A$、$N$、$\{N,A\}$的可信度,即确定了基本置信分配函数中的基本置信值,再根据式(9)确定权重,代入 D-S 合成规则式(10),最终得出检测结果。

## 4　仿真实验

### 4.1　实验环境

该模块的核心分类器是使用林智仁编写的 libsvm 2.8.9 版并在 Matlab 2009b 下完成的。该模块中使用的数据集是麻省理工 Lincoln 实验室提供的 DARPA1998 数据集 KDD CUP 99,该数据集可分为基本特征、流量特征和内容特征。由于原数据集较庞大,不便实验,本文实验使用了 10% KDD99 数据集中的部分数据作为训练数据集和测试数据集。

### 4.2　数据的预处理

因为 KDD99 数据集的 41 个特征类型比较复杂,有符号型,连续型和离散型,所以在实验之前需要对所有的特征属性统一。其中,连续型特征采用 Rosetta[9] 软件中的 Naïve 算法进行离散化,而符号型特征则通过一般的映射将符号映射到离散型的数值。最后,使用 Matlab 中自带的映射函数 mapminmax,将数据集归一化,使所有属性的度量得到统一。

### 4.3　实验结果及分析

为了评价本文提出的融合模型的检测性能,本文使用以下检测参数:

检测率(Precision):指被检测出来的真正是异常记录的数目在总的入侵记录数中所占的比例;

Recall 是真正的攻击记录中被检测出来的占所有攻击记录的比例;

*F-Score* 是用来评估一个异常检测系统的好坏,*F-Score* 值越大,说明该系统越好,*F-Score* 的计算公式如下:

$$F\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{11}$$

ROC 曲线的横坐标是误报率,纵坐标是检测率,曲线下的面积是 *AUC* 值,*AUC* 值越大说明性能越好。

首先,本文做了一下 3 组实验。实验数据集中 Normal 为

4 000条,probing 攻击,DOS 攻击,R2L 攻击数均为 2 000 条,U2R 攻击数为 249 条,实验结果如表 1 - 表 4 所示。

**表 1 单个 SVM 参数优化对各种攻击类型的检测结果**
**(虚警率 =3.06%)**

| 攻击类型 | 总攻击数 | 被检测出的攻击数 | 检测率(%) |
|---|---|---|---|
| DOS | 2 000 | 1 958 | 97.9% |
| Probe | 2 000 | 1 992 | 99.6% |
| U2R | 249 | 201 | 80.72% |
| R2L | 2 000 | 1 656 | 82.8% |
| Total | 6 249 | 5 807 | 92.93% |

**表 2 经典 D-S 证据理论对各种攻击类型的检测结果**
**(虚警率 =1.38%)**

| 攻击类型 | 总攻击数 | 被检测出的攻击数 | 检测率(%) |
|---|---|---|---|
| DOS | 2 000 | 1 995 | 99.75% |
| Probe | 2 000 | 1 994 | 99.7% |
| U2R | 249 | 232 | 93.2 % |
| R2L | 2 000 | 1 844 | 92.2% |
| Total | 6 249 | 6 065 | 97.06% |

**表 3 基于参数优化的 SVM 融合模型对各种入侵行为类型的检测结果**
**(虚警率 =0.60%)**

| 入侵类型 | 攻击总数 | 被检测出的攻击数 | 检测率(%) |
|---|---|---|---|
| DOS | 2 000 | 1 975 | 98.75% |
| Probe | 2 000 | 1 972 | 98.6% |
| U2R | 249 | 233 | 93.57% |
| R2L | 2 000 | 1 996 | 99.8% |
| Total | 6 249 | 6 176 | 98.83% |

**表 4 SVM、经典 D-S 和基于参数优化的 SVM 融合在所有攻击类型上的整体比较**

| 检测方法 | Precision | Recall | F-Score | AUC |
|---|---|---|---|---|
| SVM | 0.9293 | 0.9222 | 0.9257 | 0.9476 |
| 经典 D-S | 0.9706 | 0.9650 | 0.9678 | 0.9770 |
| 基于参数优化的 SVM 融合 | 0.9883 | 0.9847 | 0.9865 | 0.9903 |

从表 1 和表 2 两组实验可以看出,实验 1 对 Probe 攻击和 DOS 攻击的检测率都还可以,相对而言,对 U2R 和 R2L 的检测效果要差一些,这说明了单个 SVM 对 Probe,Dos 的检测效果要比对 U2R 和 R2L 的检测效果要好。实验二和实验一相比,使用经典 D-S 算法进行融合之后,能够得到良好的检测效果。从表 3 可以看出本文提出的入侵检测模块,和经典 D-S 算法比不仅能够提高对各攻击的检测性能,而且还能够有效地降低系统的误报率。由表 3 可以看出,本文提出的入侵检测模块,对 U2R 和 R2L 攻击,也有着较高的检测率,说明了该模块具有良好的适用性和推广性。

而从表 4 可以直观地看出本文的入侵检测模块在与其他模型在整体性能上的比较,*F-Score* 也说明了本文的 SVM 回归融合在检测性能上更甚一筹。

图 2 中,实线是单个 SVM 对 test 集总体检测的 ROC 曲线,点线则是 SVM 结合经典 D-S 算法的分类器对 test 集总体检测的 ROC 曲线,点划线则是本文提出的检测模块对 test 集总体检测的 ROC 曲线。其中实线下的面积,*AUC* 值为 0.9476,而点线下的面积,*AUC* 值为 0.9770,而点划线下的面积,*AUC* 值为 0.9903。从上图显示的来看,D-S 算法能够有效地提高检测系统的检测性能,而本文提出的使用的检测模块,能够得到比 D-S 算法更好的检测性能。

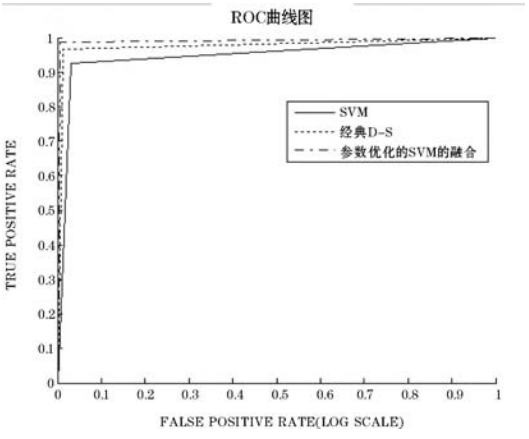


图 2 单个 SVM、经典 D-S 融合方法和参数优化的 SVM 融合的 ROC 曲线图

接着,为了更好地说明采用深度优先搜索算法的 SVM 融合模型的高性能,本文分别与非启发式的网格搜索和启发式的 GA 算法的 SVM 融合做了对比实验。实验数据集:(1) 4 000 条 Normal,Probing 攻击、DOS 攻击、R2L 攻击数均为 2 000 条,U2R 有 249 条;(2) 1 000 条 Normal,Probing 攻击、DOS 攻击、R2L 攻击数和攻击数均为 500 条,U2R249 条。

由表 5 和表 6 可知,不管采用较大样本数据集还是较小样本数据集,三种算法的检测率都差不多,但还是采用交叉验证和深度优先搜索的 SVM 融合要略胜一筹。从花费的时间来看,采用交叉验证和深度优先搜索的 SVM 融合所花费的时间明显优于其他,而且随采用样本的数据集增大,花费时间的优势更明显。可见不管从检测性能上还是花费时间上,采用启发式深度优先搜索的 SVM 融合具有不错的检测性能。

**表 5 采用数据集(1)的检测率和花费时间比较**

| 参数优化方法 | 检测率 | 时间 |
|---|---|---|
| 网格搜索 | 98.80% | 58 023.18s |
| GA 算法 | 98.83% | 25 042.14s |
| 深度优先搜索 | 98.83% | 4 005.57s |

**表 6 采用数据集(2)的检测率和花费时间比较**

| 参数优化方法 | 检测率 | 时间 |
|---|---|---|
| 网格搜索 | 98.99% | 8 044.17s |
| GA 算法 | 99.02% | 3 063.26s |
| 深度优先搜索 | 99.03% | 1 005.57s |

## 5 结 语

通过实验证明,本文提出的采用交叉验证和深度优先搜索的 SVM 融合算法在网络异常行为检测系统中提高了检测率,减少了时间的花费,确实是一个可行有效的入侵检测算法。

## 参 考 文 献

[1] Staniford S,Hoagland J A,McAlerney J M. Practical automated detection of stealthy portscans [J]. Journal of Computer Security,2002,10(1):105 - 136.

[2] Bridges S M,Rayford M Vaughn. Fuzzy data mining and genetic algorithms applied to intrusion detection [C]//Proceedings 23rd National Information Systems Security Conference, Baltimore,MD,2000:13 - 31.

[3] Sung A H,Mukkamala S. Identify important features for intrusion detection using support vector machines and neural networks [C]//IEEE

Proceedings of the 2003 Symposium on Application and the Internet, 2003:209 - 216.
[4] Zhu Ming, Liao Junguo. Research of Intrusion Detection Based on Support Vector Machine[C]//Advanced Computer Theory and Engineering, 2008:434 - 438.
[5] Maheshkumar Sabhnani, Gürsel Serpen. Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context[C]//Proceedings of the International Conference on Machine Learning, Models, Technologies andAp2plications. MLMTA'03, June, Las Vegas, Nevada, USA, 2003:209 - 215.
[6] http://www.csie.ntu.edu.tw/~cjlin/libsvm/.
[7] 刘靖旭,蔡怀平,谭跃进. 支持向量机回归参数调整的一种启发式算法[J]. 系统仿真学报,2007,19(7):1540 - 1543.
[8] Hsu Chihwei, Chang Chihchung, Lin Chihjen. A practical guide to SVM classification [EB/OL]. [2008 - 07 - 03]. http://www.csie.ntu.edu.tw/-cjlin/papers/guide/guide.pdf.
[9] The ROSETTA Homepage[EB/OL]. (1998 - 04 - 02). http://www.idi.ntnu.no/~aleks/rosetta/.
[10] 诸葛建伟,王大为, 陈昱,等. 基于 D-S 证据理论的网络异常检测方法[J]. 软件学报,2006,17(3):463 - 471.
[11] Josef Kittler, Mohamad Hatef, Robert P W Duin, et al. On Combining Classifiers[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(3):226 - 238.
[12] Peng Xiang, Irwin King. Robust {BMPM} Training Based on Second Order Cone Programming and Its Application in Medical Diagnosis Tasks[J]. Neural Networks, 2008, 21(2):450 - 457.
[13] Peng Xiang, Irwin King. A Biased Minimax Probability Machine-based Scheme for Relevance Feedback in Image Retrieval[J]. Neurocomputing, 2009, 72(7):2046 - 2051.
[14] 李立红,许元飞. 深度优先搜索的支持向量机参数优化算法[J]. 计算机仿真,2010,28(7).
[15] 王宏,刘渊. 扩展 D-S 证据理论在网络异常检测中的研究[J]. 计算机工程与应用,2011,47(34).

(上接第 3 页)

### 3.4　同步攻击鲁棒性测试

旋转、缩放、平移、剪切等空间域同步攻击是鲁棒性水印算法面临的最大挑战。表 3 所示是各种几何攻击下的水印提取结果。从表中可以看出,在鲁棒性角点检测、筛选和具有统计意义的水印嵌入/检测算法的共同作用下,本算法对于各种几何攻击及其组合攻击均具有很强的鲁棒性。

**表 3　几何攻击实验结果**

| 攻击类型 | Lena (*NHS*) | Baboon (*NHS*) | Peppers (*NHS*) |
|---|---|---|---|
| 旋转 5 度 | 1 | 1 | 1 |
| 旋转 10 度 | 1 | 1 | 1 |
| 旋转 15 度 | 1 | 1 | 1 |
| 旋转 30 度 | 1 | 1 | 1 |
| 旋转 60 度 | 1 | 1 | 0.875 |
| 旋转 90 度 | 1 | 1 | 1 |
| 缩放 0.8 倍 | 1 | 0.7083 | 1 |
| 缩放 0.9 倍 | 1 | 1 | 1 |
| 缩放 1.2 倍 | 1 | 1 | 1 |
| 缩放 1.5 倍 | 1 | 1 | 1 |
| 向右下平移 5 像素 | 1 | 1 | 1 |
| 向右下平移 10 像素 | 1 | 1 | 1 |
| 向右下平移 20 像素 | 1 | 1 | 1 |
| 中心剪切 5% | 1 | 1 | 1 |
| 中心剪切 10% | 1 | 1 | 1 |
| 旋转 20 度 + 缩放 0.8 倍 | 1 | 1 | 0.625 |
| 旋转 40 度 + 缩放 1.5 倍 | 1 | 1 | 1 |
| 旋转 15 度 + 中心剪切 10% | 1 | 1 | 0.625 |
| 缩放 0.8 倍 + 中心剪切 10% | 1 | 0.7083 | 1 |

## 4　结　语

本文提出了一种基于隐含同步思想,使用鲁棒角点进行重同步的空间域局部化鲁棒数字图像盲水印算法。其主要创新点包括:(1) 首次利用 CSS 算法检测出的鲁棒角点作为稳定特征点,基于熵筛选后得到具有几何不变性的圆形特征区域;(2) 在特征区域设计了一种圆环形的水印模式,并在空间域采用具有统计意义的奇偶量化方法嵌入/检测水印。算法计算量小,嵌入水印后能够保持较高的视觉质量,对常见信号处理攻击和空间域同步攻击均具有较强的鲁棒性。

不足之处是对于较高强度的压缩比较敏感,这主要是由于空间域算法本身特点引起的。

今后的工作包括:(1) 采用更稳定的特征点来进一步增加水印同步的准确性;(2) 使用变换域算法用于水印的嵌入/检测以增强对高强度信号处理的鲁棒性。

## 参　考　文　献

[1] Licks V, Jordan R. Geometric attacks on image watermarking systems [J]. IEEE Multimedia, 2005, 12(3): 68 - 78.
[2] Kutter M, Bhattacharjee S K, Ebrahimi T. Towards second generation watermarking scheme[C]//IEEE International Conference on Image Processing, 1999, 1: 320 - 323.
[3] Bas P, Chassery J M, Macq B. Geometrically invariant watermarking using feature points[J]. IEEE Transactions on Image Processing, 2002, 11(9): 1014 - 1028.
[4] Tang C W, Hang H M. A feature-based robust digital image watermarking scheme[J]. IEEE Transactions on Signal Processing, 2003, 51(4): 950 - 959.
[5] Weinheimer J, Qi X J, Qi J. Towards a robust feature-based watermarking scheme[C]//IEEE International Conference on Image Processing, 2006: 1401 - 1404.
[6] Lee H Y, Kim H S, Lee H K. Robust image watermarking using local invariant features[J]. Optical Engineering, 2006, 45(3):1 - 10.
[7] Parthasarathy A K, Kak S. An improved method of content-based image watermarking[J]. IEEE Transactions on Broadcasting, 2007, 53(2): 468 - 479.
[8] He X C, Yung N H C. Curvature scale space corner detector with adaptive threshold and dynamic region of support[C]//IEEE International Conference on Pattern Recognition, 2004, 2:791 - 794.
[9] Hu S Y. Geometric-invariant image watermarking by key-dependent triangulation[J]. Informatica, 2008, 32:169 - 181.
[10] Lin Y T, Wu J L, Kuo Y F. Geometric-invariant image watermarking by object-oriented embedding[J]. IJCSNS International Journal of Computer Science and Network Security, 2006, 6(3B).