基于局部投影降噪和 FSVDD 的网络流量异常检测*

温祥西[1,2], 孟相如[2], 马志强[2], 康巧燕[2]
(1. 空军工程大学 空管与领航学院, 西安 710051; 2. 空军工程大学 信息与导航学院, 西安 710077)

摘 要: 现有残差比较等异常检测方法只能在突变阶段检测异常,检测率较低。综合考虑网络流量中包含的所有特征,对网络中的多种协议流量指标分别进行局部投影降噪处理,将各流量分解为流量趋势部分和噪声流量部分,以这两部分为参量通过支持向量数据描述建立检测模型,并通过对样本的模糊化处理提高模型的泛化性。实验表明该方法适合于检测拒绝服务攻击引起的流量异常,与传统的阈值比较方法相比能够获得更高的异常检测率和更低的误报率。

关键词: 局部投影降噪; 模糊逻辑; 支持向量数据描述; 异常检测
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)05-1523-04
doi:10.3969/j.issn.1001-3695.2013.05.062

Network traffic anomaly detection based on local projection denoise and FSVDD

WEN Xiang-xi[1,2], MENG Xiang-ru[2], MA Zhi-qiang[2], KANG Qiao-yan[2]
(1. *Air Traffic Control & Navigation College, Air Force Engineering University, Xi'an* 710051, *China*; 2. *Institute of Information & Navigation, Air Force Engineering University, Xi'an* 710077, *China*)

Abstract: The present network traffic anomaly detection methods such as residual detection could detect anomaly at the break moment only, the detection rate was low. This paper denoised the multiple protocols of network traffic by local projection method, it decomposed the traffic into trend part, and noise part and considered them in the detection. It also established the detection model by SVDD, and introduced the fuzzy logic to enhance the model's generalization. The experiments on DoS attacks detection show that the proposed method can detect the anomaly well. Compared to the traditional methods, it gets higher detection rate and lower false alarm rate.

Key words: local projection denoise; fuzzy logic; SVDD; anomaly detection

0 引言

网络流量是记录和反映网络以及用户活动的重要载体,它出现异常主要是由于蠕虫传播、DoS 攻击、DDoS 攻击、僵尸网络等恶意网络攻击行为以及网络配置失误、偶发性线路中断等引起的[1]。对网络流量的异常检测能够准确反映网络的状况,有助于提升网络管理效能,辅助故障定位和故障类别辨识,并预防故障发生,减少损失,成为当前研究的热点。

文献[2]指出流量异常一般会显式地改变流量中 IP 地址或者端口的分布。文献[3]分析了流量信息中的源地址、目的地址、源端口、目的端口出现次数的特征,利用信息熵的变化检测流量异常。这些检测方法均基于流量信息结构,需要对大量的包头和流量信息进行统计,占用资源较多。文献[4,5]基于初级流量的统计特性对网络流量异常进行分析,采用主成分分析(PCA)方法将一组流量测量矩阵分离成正常和异常两个子空间,当异常子空间的值超过一个统计极值时就判定为异常。这些方法是针对大规模网络的全网检测,若要及时处理则需要进一步的分析。在实际应用中,人们更关注关键链路是否安全,这也是当前研究的重点。链路的异常检测主要通过比较流量的 hurst 参数、残差等阈值的方式确定[6,7],这些往往考虑的仅是单一的参数。文献[8]通过对流量中总流量、TCP、UDP 等各部分进行预测,并分别分析判断后综合得出最终的检测结果,获得了比单一阈值检测方法更好的效果。文献[9]通过 SNMP 中 MIB 库统计的 TCP、UDP 等流量信息,并通过支持向量数据描述(SVDD)构建两层模型检测并判别出网络异常类别。这些方法的提出为综合考虑网络流量异常问题提供了新的思路。现有的残差比较和基于预测等异常检测方法是检验一个点与滑动窗之间的异常变化,检测个别和局部之间的变化关系。若流量出现异常,则该时刻值与局部流量之间变化剧烈,可以认为流量与正常的期望值之间出现较大偏差。期望的流量也可视做流量的低频部分或者趋势部分,要得到流量的趋势部分可以通过降噪处理。

本文从降噪的角度分析流量异常问题,采用局部投影降噪处理流量序列,认为异常子空间属于流量的噪声部分。现有的检测方法往往仅考虑异常子空间部分,若攻击持续时间较长,流量序列趋于稳定则无法判断,可见在正常子空间中同样存在着判断流量异常的信息。本文采用局部投影降噪提高了对正常和异常流量部分的区分度,在检测模型构建过程中考虑了正常子空间中的信息,并综合了网络中不同协议的流量变化特征,采用 FSVDD 方法构建异常检测模型。

收稿日期: 2012-09-01; **修回日期**: 2012-10-29 **基金项目**: 国家自然科学基金资助项目(61003252);全军军事学研究生课题资助项目(2011JY002-524);空军工程大学创新基金资助项目(201105)

作者简介:温祥西(1984-),男,江苏连云港人,博士,主要研究方向为网络故障预测与健康管理(wxxajy@163.com);孟相如(1963-),男,陕西西安人,教授,博导,主要研究方向为宽带通信网络技术;马志强(1968-),男,山东威海人,副教授,主要研究方向为视频通信;康巧燕(1980-),女,福建人,讲师,博士,主要研究方向为宽带网络和光通信技术.

1 流量的局部投影降噪分析

局部投影算法是一种子空间去噪方法。它采用局部投影策略来估计噪声:假设在足够小的空间尺度上流量序列足够光滑,在局部邻域内由所有的相点构成协方差矩阵,对这个矩阵进行奇异值分解,将较大的特征值对应的特征向量作为正常子空间 S,将较小的特征值对应的特征向量作为噪声子空间 $\tilde{S}$。将相点向 $\tilde{S}$ 投影,得到噪声分量,用得到的这个分量修正对应的相点即可获得去噪后的轨道,最后将去噪后的相空间还原为时间序列。例如对于一网络流量向量 y,经过子空间映射后分解为两部分:

$$y = \hat{y} + \tilde{y} \tag{1}$$

其中:$\hat{y}$ 为正常流量,$\tilde{y}$ 为噪声部分。$\tilde{y}$ 表示测得流量 y 偏离流量趋势 $\hat{y}$ 的程度,即噪声部分,根据 $\tilde{y}$ 是否超过设定的阈值来判断网络流量异常。在实际中,网络仅在攻击或者异常发生的一小段时间内会产生剧烈的变化,此时可以通过 $\tilde{y}$ 反映。可是当攻击持续一段时间后,网络流量将维持在一个较高的水平,此时的 y 重新稳定在 $\hat{y}$ 附近,$\tilde{y}$ 也变化较小,不会出现大的跳跃,在这种情况下子空间异常检测法将失去检测能力。说明在异常检测中降噪后的纯净流量 $\hat{y}$ 同样包含异常判断的信息。本文在建立异常检测模型时考虑 $\hat{y}$,以提高模型的检测能力。这样,如何准确的提取出 $\hat{y}$ 和 $\tilde{y}$ 成为流量异常检测的关键。

降噪过程中局部邻域的选取直接影响去噪的效果,但是由于受到噪声的影响,相空间中的相点都偏离了各自的初始位置,因此,在所选中的邻域点中势必会包含一些虚假邻域点,降低去噪性能。本文首先对样本进行 PCA 处理,在主元空间中寻找局部邻域以降低邻域虚假率。同时,为了提高降噪性能,采用语音增强领域的频域约束估计(spectrum domain constraint,SDC)方法估计噪声[10]。基于以上思想,本文提出一种改进的降噪方法,具体过程为:a)选择合适的嵌入维数 m(本文选择 6)对已知流量数据进行重构,构建流量样本库并存储;b)对该空间进行 PCA 处理,主成分分量占 80%,并将原相空间中的点映射到低维空间并存储;c)对新到的样本数据进行 PCA 降维处理,在存储的低维样本中找出其邻域集(H),并映射回原相空间找出对应的局部邻域相点;d)对所获得的局部邻域进行投影降噪处理,噪声估计时采用 SDC,获得最新时刻降噪后的流量值,具体过程参见文献[11];e)滑动窗口,获得新的样本数据,重复步骤 c)d)。

2 流量异常检测模型构建

按检测建模方法可以将流量异常检测分为基于误用检测(misuse-based)和基于异常检测(anomaly-based)两类。其中,误用检测是通过建立专家系统和既定规则来描述每一种攻击的特殊模式来检测异常,维护规则的代价比较高,灵活性和自适应性较差。异常检测是通过分析正常时刻的统计特性建立检测模型,将待检测行为与统计模型进行比较,如果能够匹配,则判定该行为是正常行为,不匹配则判定为异常。在目前的网络环境中,流量异常样本的类型众多、数量较少、获取相当困难,且新的异常种类不断出现。基于正常数据的网络流量异常检测具有样本丰富、实现简单,对未知流量异常适应性强等优势。虽然该方法无法判断流量异常的具体原因,但已能对事故的预防起到积极的作用,因此本文选择基于异常检测的方法建立模型。

借鉴文献[5]的方法,本文对总流量、TCP、UDP 和 ICMP 这四种流量序列分别加以降噪并求出对应的 $\hat{y}$ 和 $\tilde{y}$,融合 $\hat{y}$ 和 $\tilde{y}$ 共同决定流量检测模型。文献[5]中采用线性加权的方式融合得到检测模型。但采用线性方式描述各个元素之间的关系,并不能准确地描述它们与最终模型的关系。本文在建立模型过程中摒弃了文献[5]的线性方式,通过 SVDD 建立异常检测模型,采用机器学习隐式地确定各个因素在判决函数中的作用。

2.1 FSVDD 方法

SVDD 是标准 SVM 的扩展,用于解决单分类问题[12]。设目标样本的输入空间为 $X = \{x_i \mid x_i \in \mathrm{R}^d, i = 1, \cdots, n\}$,SVDD 的基本思想是构建一个超球面,通过确定球心 $O \in \mathrm{R}^d$ 和半径 R,使该超球面能以尽量小的半径包含尽可能多的目标样本。传统 SVDD 在训练过程中对所有的数据点采用相同的惩罚因子 C,使得训练模型对野点较敏感。若 C 较大,对野点的惩罚也较大,使得超球面半径较大,导致对异类样本的错判率较高;反之,过小的 C 会增大对目标样本的错判。Lin 等人[13]为了降低野点对 SVM 分类模型的影响,提高泛化性,提出了模糊支持向量机(fuzzy support vector machine,FSVM)。FSVM 通过惩罚系数区分样本的不同贡献,在构造分类模型时对野点赋予较小的权值(模糊隶属度),减小它们对分类模型的影响。本文沿用此思想,对样本点进行模糊化处理,提高模型的泛化性。由此得到的模糊训练样本集合为

$$S_{\text{fuzzy}} = \{(x_1, \mu_1), (x_2, \mu_2), \cdots, (x_n, \mu_n)\} \tag{2}$$

其中:$\mu_i \in [0, 1]$,为样本点 x_i 的模糊隶属度。因此,寻找最优超球面可以归结为求解以下最优化问题

$$\begin{aligned} &\min_{O,R,\xi} \quad R^2 + C\sum_{i=1}^{n}\mu_i\xi_i \\ &\text{s.t.} \quad \| x_i - O \|^2 \leqslant R^2 + \xi_i \\ &\xi_i \geqslant 0 \quad i = 1, \cdots, n \end{aligned} \tag{3}$$

其中:向量 $\xi = [\xi_1, \cdots, \xi_l]^{\mathrm{T}} \in \mathrm{R}^n$ 是为适应野点引入的松弛变量;$\| \cdot \|$ 是欧氏范数;C 是惩罚因子。优化问题式(3)的 Lagrange 函数如式(4)所示。

$$\begin{aligned} &L(R, O, \xi, \alpha, \beta) = \\ &R^2 + C\sum_{i=1}^{n}\mu_i\xi_i - \sum_{i=1}^{n}\alpha_i(R^2 + \xi_i - \| x_i - O \|^2) - \sum_{i=1}^{n}\beta_i\xi_i \end{aligned} \tag{4}$$

其中,α_i 和 $\beta_i (i = 1, \cdots, n)$ 是 Lagrange 乘子。分别对 R、O 和 ξ 求导并进行对偶转换可确定超球球心 O 和半径 R 分别为

$$O = \sum_{i=1}^{n}\alpha_i x_i \tag{5}$$

$$\begin{aligned} R^2 &= \| x_k - O \|^2 = \| x_k - \sum_{i=1}^{n}\alpha_i x_i \|^2 = \\ &x_k \cdot x_k - 2\sum_{i=1}^{n}\alpha_i(x_k \cdot x_i) + \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_j(x_i \cdot x_j) \end{aligned} \tag{6}$$

待测样本 x 如果处于超球内部或超球表面,则接受该样本为目标样本,否则为异类样本。即判断 x 到球心的距离与超球半径 R 的关系,如果:

$$\| x - \sum_{i=1}^{n}\alpha_i x_i \|^2 \leqslant R^2 \tag{7}$$

则接受 x 为目标样本。将式(6)代入式(7)得到目标样本的接受域为

$$x \cdot x - 2\sum_{i=1}^{n}\alpha_i(x \cdot x_i) \leqslant x_k \cdot x_k - 2\sum_{i=1}^{n}\alpha_i(x_k \cdot x_i) \tag{8}$$

FSVDD 通过模糊隶属度体现样本点对分类面的重要程度,减小野点对分类精度的影响,因此隶属度函数的设计是决定 FSVDD 性能好坏的关键。为了描述样本点属于正常类别的可能性,本文采用点到中心的距离 d_i 描述:当样本点距离中心较近时,属于正常样本的可能性较大,因此隶属度较大;当样本

点离中心距离较远时,属于正常样本的可能性变小,而属于野点的可能性变大,因此隶属度快速减小并趋近于 0。本文采用降半高斯函数作为隶属度函数,即

$$\mu_i(d_i)=\begin{cases}1 & d_i\leqslant R'\\ \exp\left[-\dfrac{(d_i-R')^2}{2\varphi^2}\right] & d_i>R'\end{cases} \tag{9}$$

其中:R'为设定值,表示当 $d_i\leqslant R'$时该样本点肯定属于正常样本;设置带宽 $\varphi=0.2R'$,则当 $d_i>1.5R'$后,隶属度将小于 0.05,这些样本点对分类面的影响几乎可以忽略不计。

2.2　流量异常检测模型

SVDD 方法是通过对单类数据样本的描述适用于对网络流量的异常检测,本文采用 FSVDD 方法构建网络流量的异常检测模型,检测流程如图 1 所示。

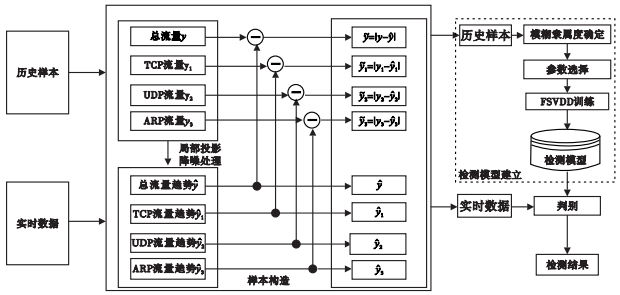

图1　基于FSVDD的流量异常检测流程

具体的步骤如下:a)对正常的历史流量序列分别进行降噪处理,并通过记录降噪后流量和测得流量构建历史样本库(图中样本构造过程);b)计算所得的正常历史样本库类中心,并确定各个训练样本的模糊隶属度;c)选择 FSVDD 训练所需的核参数以及惩罚因子,对正常样本进行 FSVDD 训练获得流量异常检测模型;d)实时地对各个流量进行降噪处理,记录当前流量降噪后的值以及当前的测量值构建检测的实时数据;e)将当前的实时检测数据输入检测模型中,获得检测结果。

3　实验与分析

3.1　实验拓扑

拒绝服务攻击(denial of service,DoS)会造成流量的突变,适合于流量异常检测,本文针对 DoS 攻击造成的流量异常进行检测。为了验证本文方法的有效性,采用网络仿真工具 OPNET 模拟 DoS 攻击并对收集的流量信息进行异常检测。仿真的拓扑如图 2 所示,在该网络中加载多种类型的业务流量,包括 FTP、e-mail、DATA、HTTP 等,为了模拟 DoS 攻击,通过编辑 OPNET 中的 IP-ENCAP 模型构建 Synflood、UDP 以及 ICMP 的攻击节点,并在 subnet1 中加入一些提供 Synflood 攻击的节点,在 subnet2 中加入一些提供 UDP 攻击的节点,在 Subnet3 中加入一些提供 ICMP 攻击的节点,其他正常工作站加载正常的 FTP、e-mail、DATA 等服务。控制攻击节点,在不同的时间段对 database 服务器进行攻击,检测 router2 到 database 服务器之间的链路流量异常,仿真时间为 6 h,激发各种不同攻击强度的 DoS 攻击 40 次,攻击持续时间从 30 s 到 5 min 不等,收集该链路上的流量情况。

3.2　流量降噪分析

对统计的链路流量进行降噪分析,采用本文提出的方法对该段流量进行降噪,其中,前一个小时的流量作为历史流量进行 PCA 处理,局部邻域个数为 10 个。这里以其中的一次攻击的总流量为例,得到的结果如图 3 所示,图中所示为归一化后的流量。

图 3 中测得流量为 y,降噪后的流量趋势为 $\hat{y}$,从得到的降噪结果可以看出本文提出的方法能够很好地反映出网络流量的变化趋势。图 4 为噪声分量 $\tilde{y}$,在流量发生异常时 $\tilde{y}$ 也出现较大的变化,很好地反映了异常。此外,分析框内部分,攻击初期,$|y-\hat{y}|$(即 $\tilde{y}$)变化大,可以判断为发生异常;当流量趋于稳定时,$\tilde{y}$ 起伏变化相对稳定且值较小,若仅通过 $\tilde{y}$ 判断则认为此时流量属于正常,这与实际情况相反,说明前面关于子空间异常检测的分析是正确的。由于本文提出的异常检测方法是为了实现在线检测,对时间需求比较高。每个降噪过程需要涉及的计算包括局部邻域的选择以及奇异值分解,其中邻域选择做的主要是乘、加运算,虽然选择的范围较大,但是耗时并不多;矩阵奇异值分解以及重构大小仅为 6×10,计算复杂度仅为 $O(6^3)$,每一次的降噪过程所需的时间很少(在 MATLAB 7.4.0、Pentium® Dual-Core 2.7 GHz CPU、2 GB 内存条件下平均为 0.024 s),可以很好地满足实时检测的要求。

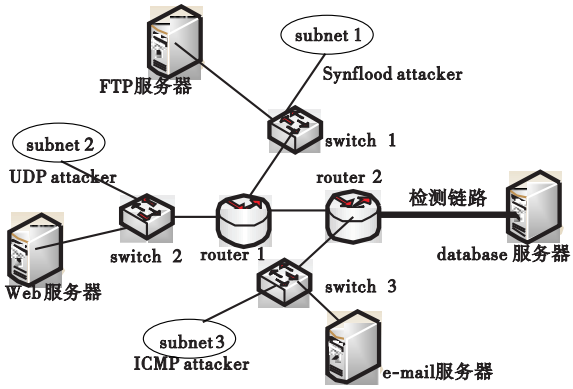

图2　实验拓扑

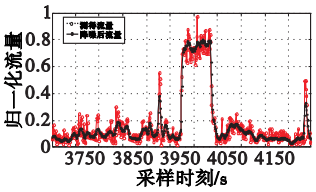

图3　网络流量降噪结果

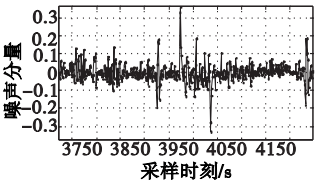

图4　噪声分量时序图

3.3　流量异常检测分析

通过 FSVDD 学习建立网络异常检测模型,需要正常的历史样本建立样本库。以未发生攻击时的各个流量的 $\hat{y}$ 和 $\tilde{y}$ 构建历史样本库(随机选取 2 000 个正常时刻的值),并经过 FSVDD 训练,训练中核函数选择径向基核(高斯核),核带宽为 0.2,惩罚因子为 200。为了衡量本文方法[8]的检测效果,比较本文方法与残差比较、文献[7]以及自适应滤波方法的异常检测率、误检率。其中异常的检测率为序列中实际异常数与检测出的异常总数之比,显然检测率越大,效果越好,它的最大值为 100%;误检率为序列中正常的被判断为异常的数目与正常点数之比,它的值越小越好。检测的结果如表 1 所示。

表 1　不同检测方法的实验结果　　/%

检测方法	残差比较	文献[7]方法	文献[8]方法	本文方法
检测率	87.5	92.5	95	95
误检率	8.4	7.2	6.8	4.3

从实验结果可以看出,这四种方法特别是后三种方法均能很好地检测出 DoS 攻击引起的流量异常,这是由于 DoS 攻击本身引起的流量变化较为明显。分析检测结果可以看出,残差比较检测方法虽然最简单,但是它获得的检测率较低且有较高的误检率,检测效果最差;文献[8]方法优于文献[7]方法的检

测效果,这是由于文献[7]中将流量的各个部分进行了细化分析。相较前三种方法,本文提出的检测方法与文献[7]以及文献[8]的检测效果相当,但是具有最低的误检率,说明通过 FSVDD 隐式地确定各个流量分量的关系较线性的相加更优。表 1 中的检测率检测的仅为是否发生了 DoS 攻击,并不考虑攻击的持续时间,它们所得的检测率是检测出攻击次数占总的攻击次数比例。若考虑攻击持续时间,如图 3 中 4 000 s,通过其他三种方法检测认为此时流量正常,而本文方法仍然可以检测出此时发生攻击,也就是说本文方法可以统计出异常持续时间。另外,从检测方法的反应速度来说,由于某种单一攻击初期引起的变化较弱,往往被背景流量的噪声所覆盖,初期无法检测出来,而本文方法和文献[8]由于分别考虑了各种协议的流量,因此在对攻击的反应速度上优于其他两种方法。

4 结束语

本文从降噪的角度分析考虑了网络流量异常检测,采用局部投影去噪的方式对网络流量进行了实时的降噪处理。在降噪过程中通过 PCA 处理提高选择局部邻域的选择准确率,并引入语音增强中的 SDC 噪声估计方法以提高效果。在构建模型时综合考虑了异常流量、测得流量以及各个协议流量对于模型建立的意义,通过 FSVDD 建立最终异常检测模型,能够更加准确地描述各个因素在异常检测中的相互关系。通过在 OPNET 上模拟攻击的实验说明,本文提出方法能够提供更加准确的流量异常检测和更低的误报率,为流量异常检测和网络的安全防护提供了新的思路。

参考文献:

[1] CASAS P, VATON S, FILLATRE L, *et al*. Optimal volume anomaly detection and isolation in large-scale IP networks using coarse-grained measurements[J]. Computer Networks,2010,54(11):1750-1766.

[2] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions[C]//Proc of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York:ACM Press,2005:217-228.

[3] 朱应武,杨家海,张金祥. 基于流量信息结构的异常检测[J]. 软件学报,2010,21(10):2573-2583.

[4] LAKINA A, CROVELLA M, DIOT C. Diagnosing network-wide traffic anomalies[C]//Proc of Conference on Application,Technologries, Architectures, and Protocols for Computer Communications. New York:ACM Press,2004:219-230.

[5] 侯重远,江汉红,芮万智,等. 工业网络流量异常检测的概率主成分分析法[J]. 西安交通大学学报,2012,46(2):70-75.

[6] 曹敏,程东年,张建辉,等. 基于自适应阈值的网络流量异常检测算法[J]. 计算机工程,2009,35(19):164-166,177.

[7] 邹柏贤. 一种网络异常实时检测方法[J]. 计算机学报,2003,26(8):940-947.

[8] 颜若愚,郑庆华,牛国林. 自适应滤波实时网络流量异常检测方法[J]. 西安交通大学学报,2009,43(2):1-5.

[9] YU J, LEE H, KIM M S, *et al*. Traffic flooding attack detection with SNMP MIB using SVM[J]. Computer Communications,2008,31(17):4212-4219.

[10] EPHRAIM Y, Van TREES H L. A signal subspace approach for speech enhancement[J]. IEEE Trans on Speech and Audio Processing,1995,3(4):251-266.

[11] 韩敏, 项牧. 局部投影去噪的一种改进的邻域选取方法[J]. 系统工程学报,2009,24(4):392-398.

[12] TAX D M J,DUIN R P W. Support vector data description[J]. Machine Learning,2004,54(1):45-66.

[13] LIN Chun-fu, WAN Sheng-de. Fuzzy support vector machines[J]. IEEE Trans on Neural Networks,2002,13(2):464-471.

(上接第 1522 页)m'_1、m'_2 是利用 Duffing 振子检测到的信号调频率。由于本文使用两分量的 Chirp 水印,所以检测到的调频率有两个。“\”表示未能检测出水印。数据表明,Duffing 振子检测性能较 FRFT 方法的检测性能高。

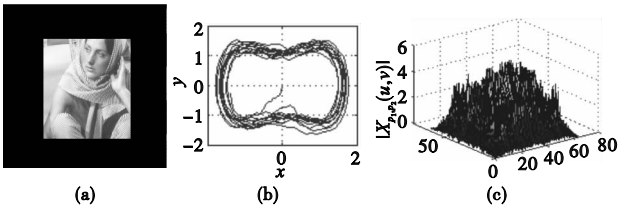

图6 受剪切攻击水印图像和振子因为水印的存在从混沌状态转向大尺度周期状态,而FRFT方法检测失效

表 1 两种检测方法的抗攻击性能比较

嵌入强度 α	水印图像无攻击 $m_1,m_2/m'_1,m'_2$	叠加加性高斯噪声 $m_1,m_2/m'_1,m'_2$	JPEG 压缩(32:1) $m_1,m_2/m'_1,m'_2$	旋转 20° $m_1,m_2/m'_1,m'_2$
0.001	\,\/0.125,0.250	\,\/0.120,0.250	\,\/0.125,0.25	\,\/0.100,0.250
0.003	\,\/0.125,0.250	\,\/0.125,0.250	\,\/0.125,0.25	\,\/0.120,0.250
0.005	\,\/0.125,0.250	\,\/0.125,0.250	\,\/0.125,0.25	\,\0.125,0.250
0.01	0.125,\/0.125,0.25	0.12,\/0.125,0.25	0.120,\/0.125,0.25	\,\/0.125,0.250

4 结束语

本文将 FRFT 和 Duffing 振子在 Chirp 类水印检测中的性能进行比较,首先分析 FRFT 方法检测载体中水印的不足,然后根据微弱信号混沌检测理论,将水印检测问题转换为超低信噪比条件下,载体低频小波系数背景中利用 Duffing 振子滤波器检测周期信号。算法信噪比在低于 -41 dB 时仍能有效地检测到水印,此时 FRFT 方法失效,但 FRFT 方法在信噪比较高时计算较简单。因此,在水印检测时可以综合考虑两种方法,提高水印检测的可靠性。

参考文献:

[1] 杨守义,姬留杰,穆晓敏,等. 基于 FRFT 的数字水印算法分析[J]. 计算机应用与软件,2009,26(1):20-23.

[2] CANDAN C, KUTAY M A, HALDUN M O. The discrete fractional Fourier transform[J]. IEEE Trans on Signal Processing,2000,48(5):1329-1337.

[3] 张峰,穆晓敏,杨守义,等. 基于 FRFT 盲检测 Chirp 类数字水印算法[J]. 计算机工程与应用,2006,42(27):57-61.

[4] WANG Dian-hong, LI Dong-ming, YAN Jun, *et al*. An improved Chirp typed blind watermarking algorithm based on wavelet and fractional Fourier transform[C]//Proc of the 4th International Conference on Image and Graphics. 2007:291-296.

[5] 李东明,王典洪,严军,等. 基于小波与分数傅里叶变换的图像水印算法[J]. 计算机工程,2008,34(8):15-18.

[6] 平先军,陶然,周思永,等. 一种新的分数阶傅里叶变换快速算法[J]. 电子学报,2001,29(3):406-408.

[7] 孙中伟,冯登国,武传坤. 基于弱信号检测理论的离散小波变换域数字水印盲检测算法[J]. 计算机研究与发展,2006,43(11):1920-1926.

[8] STANKOVIC S, DJUROVIC I, PITAS I. Watermarking in the space/spatial-frequency domain using two-dimensional Radon-Wigner distribution[J]. IEEE Trans on Image Processing,2001,10(4):650-658.

[9] 文忠,李立萍. 基于 Duffing 振子的弱 Chirp 信号检测与参数估计[J]. 自动化学报,2007,33(5):536-539.