基于深度神经网络的自定义用户异常行为检测

陈 胜 朱国胜 祁小云 雷龙飞 吴善超 吴梦宇
(湖北大学计算机与信息工程学院 武汉 430062)

摘 要 在大数据网络环境下,由于传统用户异常行为检测方法无法满足海量数据检测需求,对不断更新的异常行为和恶意软件无法快速地做出响应,没有考虑用户行为管理等问题,导致异常检测的精度和稳定性都不足。文中结合网络流量分析技术,提出了基于深度神经网络的自定义用户异常行为检测模型,实现了网络流量的细粒度分析,并自定义用户行为管理设定,使用户异常检测与特定网络环境的需要更紧密地结合,将网络流量分析的数据作为深度神经网络算法的输入向量,实现海量数据检测和自定义用户行为管理,同时检测未知异常行为。实验结果表明,所提方法具有较高的准确性及鲁棒性,能有效实现自定义用户行为管理,进而解决传统用户异常行为检测的不足。

关键词 用户异常行为,网络流量,自定义,深度神经网络
中图法分类号 TP181 **文献标识码** A

Custom User Anomaly Behavior Detection Based on Deep Neural Network

CHEN Sheng ZHU Guo-sheng QI Xiao-yun LEI Long-fei WU Shan-chao WU Meng-yu
(School of Computer and Information Engineering, Hubei University, Wuhan 430062, China)

Abstract In the network environment of big data, the method of detecting the abnormal behavior of the traditional user have the question that it can not meet the massive data detection requirements, can not respond to the constantly updated abnormal behavior and malware quickly and does not consider the user behavior management and other issues, so that the accuracy and stability of the abnormal detection is insufficient. Combining the technology of network traffic analysis, this paper proposed a custom model of the abnormal user behavior detection based on deep neural network, which realizes fine-grained analysis of network traffic and customizes user behavior management settings to make user anomaly detection more closely integrated with the needs of specific network environments. The data of network traffic analysis was used as the input vector of the deep neural network algorithm to realize massive data detection and custom user behavior management, and detect unknown abnormal behavior. The experimental results show that the proposed method has high accuracy and robustness, can effectively implement custom user behavior management, and solve the shortage of the traditional user anomalies.

Keywords User anomalous behavior, Network traffic, Custom, Deep neural network

1 引言

随着信息化时代的发展,互联网用户和设备急速增长,网络安全问题也更复杂多变。为了保证网络环境的安全稳定,对大数据时代网络流量数据的监管变得非常重要[1-3]。因此,高效全能地识别网络中的异常行为对网络安全管理起到关键的作用。网络流量具有数据量大、随机性强等特性,传统用户异常行为检测方法不能满足海量数据高效准确检测的要求,对不断更新的异常行为和恶意软件的检测无法迅速地做出裁决和响应,不能准确实现用户行为管理限制等,已经无法满足大数据时代的发展需求,我们需要更加快速准确地检测异常行为[4]。

网络流量分析对用户行为和网络环境的安全维护有着重要作用。早期采用端口扫描、报文特征字段匹配等方法进行异常行为检测[5-6]。但是,随着用户异常行为不断更新变化,特征获取和字段匹配的异常检测方法的代价越来越大,存在无法快速准确检测异常行为等缺点[7]。结合网络流量分析的用户异常检测主要通过网络流量分析提取正常数据并制定规则,能快速地检测出异常行为,但检测精确度不足。随着人工智能技术的发展,机器学习技术被广泛应用到异常行为检测系统[8],对网络层、传输层的流量数据特征进行提取,对检测出的已有异常类型数据进行样本标记,从而自动演变检测规则实现用户异常行为检测。但是其缺少与用户上网行为有密切关系的特征,没有结合自定义用户行为类型的特殊网络环境需要等问题,使用户异常行为检测系统不仅开销大,还会影响实际数据的分析检测,进而影响检测效果。

本文提出了一种基于上层应用特征分析的用户异常行为检测方法,通过网络流量细粒度分析之后,能得到用户行为的规律性、偶然性和多重复性等特征数据[9],提取用户信息进行网络用户画像的构建[10],从而设置自定义用户行为类型特征,满足特殊网络环境的需要。同时采用深度神经网络算法对提取的特征数据进行检测模型的构建,提高网络用户异常

本文受赛尔网络下一代互联网技术创新项目(NGII20170418)资助。

陈 胜(1994—),男,硕士生,主要研究方向为网络流量分析;朱国胜(1972—),男,博士,教授,主要研究方向为下一代互联网、网络安全,E-mail:zhuguosheng@hubu.edu.cn(通信作者)。

行为检测准确性、自定义用户异常行为类型检测系统的效率和适应性。

2　用户异常行为检测模型

2.1　网络流量分析

网络用户流量行为是网络用户在使用网络应用时产生的网络流量特性[11-12]。根据研究目的和网络环境的不同,网络流量行为的分类也不同。从网络安全的角度,网络用户流量行为可以分为正常行为和异常行为。在于用户对象的数量方面,其又可以分为单用户流量行为和海量用户行为;对于单用户流量行为,从行为学角度来看,网络用户存在 3 种特性:规律性、偶然性和多重复性[13]。本文针对单用户和海量用户的流量行为进行分析,挖掘出用户流量行为的内部规则,从而检测网络的异常流量行为。

网络流量分析是研究网络用户流量行为的基础,不仅可以分析网络环境中的异常行为数据,还能分析用户流量行为的详细特征,挖掘用户流量行为的变化规律,并根据上网情况自定义异常类型限制,从而构建用户流量行为。通过网络流量数据来分析整个网络环境的运行状态,对网络负载和环境进行合理用户行为管理,从而达到用户异常行为检测的目的。

2.2　深度神经网络算法

深度神经网络算法(Deep Neural Networks,DNN)是通过模拟人类的认知思维方式,来建立分辨事物的能力,从而得到一个多层的神经网络模型。DNN 具有深层次、非线性和逐层特征提取的特点,能够解决许多浅层神经网络不能解决的复杂问题[14-16]。

DNN 按神经网络层的位置可以分为输入层、隐含层和输出层 3 类,通常第一层为输入层,最后一层是输出层,中间神经元为隐含层。深度神经网络的基本结构如图 1 所示,w_{ij},w_{jk},w_{kl} 是各层之间的权值,b_j,b_k,b_l 为各层的阈值,z_j,z_k,z_l 为节点的输入与权值和阈值计算的结果,a_j,a_k,a_l 是 z_j,z_k,z_l 进行激活函数计算的输出。这种深度神经网络主要是由各层之间的全连接构成,按照误差反向传播来训练迭代,从而更新神经元之间的权值和阈值,进而决定网络的功能。

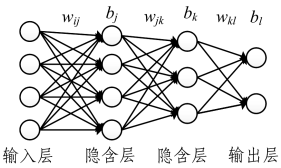

图 1　深度神经网络的基本结构

深度神经网络的具体算法过程如下:

(1)初始化 DNN,设置迭代次数 k 和最小误差 ε;

(2)将样本 $D=\{(x_1,y_1),(x_2,y_2),\cdots,(x_m,y_m)\}$ 作为 DNN 训练数据,其中 x 表示样本的特征向量。根据式(1)、式(2)计算前向传播过程中各层的输出,例第 L 层输出 a^L,w 为权值,b 为阈值,σ 为激活函数。

$$z^l=w^l a^{l-1}+b^l \tag{1}$$

$$a^L=\sigma(z^l)=\sigma(w^l a^{l-1}+b^l) \tag{2}$$

(3)得到输出层的输出后,使用损失函数来度量输出层的结果与实际输出之间的损失,采用均方差 E 来表示整个网络的损失。

$$E=J(w,b,x,y)=\frac{1}{2}\parallel a^L-y\parallel^2 \tag{3}$$

(4)判断迭代次数 k 和误差是否在要求内,若不满足要求则进行反向传播计算,如式(4)计算损失函数对第 L 层隐含层的输出误差,其中⊗表示 Hadamard 积。

$$\delta^L=\frac{\partial J(w,b,x,y)}{\partial z^L}=(a^L-y)\otimes\sigma'(z^L) \tag{4}$$

(5)利用式(5)、式(6)可根据损失函数求得更新权值和阈值的偏导。

$$\frac{\partial J(w,b,x,y)}{\partial w^l}=\frac{\partial(w,b,x,y)}{\partial(z^l)}\frac{\partial z^l}{\partial w^l}=\delta^l(a^{l-1})^{\mathrm{T}} \tag{5}$$

$$\frac{\partial J(w,b,x,y)}{\partial b^l}=\delta^l \tag{6}$$

(6)根据式(7)、式(8)进行各层权值和阈值的参数更新,其中 α 代表学习率。

$$w^l=w^l-\alpha\sum_{i=1}^{m}\delta^{i,l}(a^{i,l-1})^{\mathrm{T}} \tag{7}$$

$$b^l=b^l-\alpha\sum_{i=1}^{m}\delta^{i,l} \tag{8}$$

(7)当误差满足设定要求或达到迭代次数时,可停止训练,得到检测模型,否则跳转到步骤(2)继续迭代。

通过以上的过程分析,DNN 对事物的建模能力或异常行为抽象表现能力更强,能模拟复杂多变的异常行为特征模型,为提高网络流量用户异常行为检测的准确度和适应性。

2.3　自定义行为规则

用户行为管理帮助网络管理者控制和管理互联网的使用,主要包括网页和应用的过滤限制、流量管理、信息审计、行为分析等[17],能防止非法信息传播、信息泄露等各种异常行为的发生,实现网络资源的高效使用,保障网络环境的安全运行。

本文对网络流量进行分析,选用了用户使用的设备、应用程序、浏览器、浏览的网页和舆情关键字等相关信息,包括使用系统、设备、浏览器、网页类型、网页、web 浏览时长、APP、APP 使用时长和舆情关键字等 9 个字段。由于用户访问的网站、APP 和舆情种类过多,因此分析用户使用的网页和 APP 是由预先建立的规则库来确定的,搜集大部分常用的设备、Web、APP 和舆情的信息,能高效地实现自定义用户上网行为管理和用户异常行为检测。

对 user Agent 字段进行分析挖掘,提取相关设备的关键字信息,构建了 1000 多个设备类型信息规则库,其中操作系统包含 Windows,IOS,Android,Linux 4 种,设备关键字主要有 Windows NT 6.1,MHA-AL00,iphone 10_0_2,m1 metal 等。操作系统及设备类型规则库如表 1 所列。

表 1　操作系统与设备类型规则库

操作系统	设备关键字	类型描述
Windows	Windows NT 6.1	Windows7
	Windows NT 6.2	Windows8
	Windows NT 10.0	Windows10
Android	MI NOTE LTE	小米
	MHA-AL00	华为
	m1 metal	魅蓝
IOS	Mac	苹果
	iPhone10_0_2	苹果
	iPad 8_3	苹果
Linux	Linux	Linux

访问网页的信息规则库包含近 3 000 个常用网站,部分样例如表 2 所列。

表 2 Web 标识库

网站名	host	类型
编程中国	bccn. net	IT 网站
阿里巴巴	alibaba. com	B2B 网站
去哪儿	qunar. com	旅行网站
东方财富网	eastmoney. com	财经网站
网易邮件中心	netease. com	电子邮件
房天下	fang. com	房产网站
百姓网	baixing. com	分类广告
快速问医生	120ask. com	健康网站
新浪微博	weibo. com	交友社区
三军网	junshis. com	军事网站

APP 信息规则库部分样例如表 3 所列。根据舆情分析关键字的权重来判断舆情类别，舆情信息库部分样例如表 4 所列。

表 3 APP 标识库

APP	类型
Jike	在线阅读
youdao_dict	教育工具
xiami	在线音乐
wpsoffice	个人工具
wifikey	实用工具
WeRead	在线阅读
Weibo	社区交友
iFLYCloud	个人工具
WeChat	即时通讯
QQ	即时通讯

表 4 舆情标识库

舆情关键字	类型
302	网络错误
403	网络错误
502	网络错误
404	网络错误
湖北大学	教育
百度一下	搜索
CCTV	新闻
学院	教育

在流量采集阶段需要对用户使用的设备、浏览器、网页、APP 和舆情等进行分析挖掘。通过对端口、协议、hosts 字段、user Agent 字段和流量文本重构等方式的各种分析挖掘，将得到的结果与网络环境的需求相结合，实现用户使用的设备、浏览器、网页、APP 和舆情等上网范围规则制定，从而提高了网络用户行为的安全性和可靠性。

在湖北大学校园网实际网络环境下对学生公寓进行流量采集，从网络行为中抽取大量正常数据，并抽选一部分自定义异常行为数据来进行异常检测模型的训练检测。异常行为标记范围如表 5 所列。

表 5 异常行为标记

异常行为	描述
Bro	Bro 识别异常流量和攻击
device	自定义设备类型或型号
duration	自定义上网时间段
APP	自定义应用类型
Web	自定义网页类型
Key	自定义舆情类型或关键主题

2.4 异常行为检测模型

根据所选取的特征、自定义用户异常行为标记训练集和测试集，使用训练集训练深度神经网络的异常用户行为检测模型，利用测试集检验用户异常行为识别的准确率。具体模型检测流程如图 2 所示，首先采用旁路镜像端口的模式对校园网网络流量进行采集，采集使用开源工具 bro[18]，bro 是一个网络分析、信息重构和网络监控的框架，通过 bro 可以获取用户上网的信息，并以日志文件的形式存储。然后，对文件进行细粒度分析挖掘，从而得到用户行为特征[19]，再对用户行为特征进行自定义范围规定，将识别数据用来构建训练集和测试集。最后，使用训练数据来训练深度神经网络的异常用户行为检测模型，并实现检测验证使用。

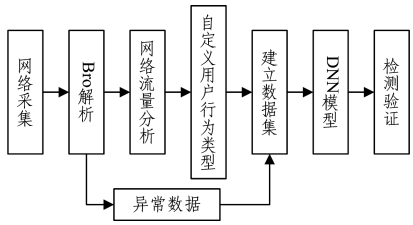

图 2 异常用户行为检测模型流程图

本文模型根据 Bro 工具、user Agent 字段和文本重构等分析方式获取已知异常行为。对一些 Bro 工具未能检测识别的异常、hosts 字段、user Agent 字段不能分析、文本重构和异常行为规则存在检测困难的数据等，通过对分析获取的异常行为数据构建训练集和测试集，然后使用深度神经网络算法建立异常行为检测模型，使整体的异常检测效率大幅度提升，实现异常行为和自定义异常更全面的识别检测。

3 实验部分

3.1 数据说明与处理

本文实验数据采用的网络流量来源于湖北大学校园网，利用旁路端口镜像的方法采集 3 个千兆端口的上下行流量，数据集中的数据是从 2018 年 12 月 18 日到 2018 年 12 月 21 日的流量数据中随机抽取的。

本文基于深度神经网络算法进行用户异常行为检测研究，需要考虑将网络流量中每条连接对应的源 IP 和目标 IP 地址标识为某个用户，进而实现用户的行为检测。由于异常行为连接数据流量大、连接时间长、依赖某种协议或服务等特性，同时设备、网页、应用和用户操作方式不同都会影响网络流量、数据包大小和连接持续时间等，因此异常行为特征与正常行为特征产生了差异。为了使检测模型具有有效性和真实性，从中提取出用户行为检测的所需特征，如表 6 所列，进而得到构建数据集的 10 个特征属性，使训练维度变低，模型建立和检测的效率变高。

表 6 特征属性说明

特征属性	描述
protocol	协议类型
service	网络服务类型
duration	连接持续时间
orig_pkts	源端数据包个数
orig_bytes	源端到目标端的数据字节数
resp_pkts	目标端数据包个数
resp_bytes	目标端到源端的数据字节数
conn_state	连接状态
orig_ip_bytes	源端数据包大小
resp_ip_bytes	目标端数据包大小

根据连接数计算训练集大小，清除无用的连接。本实验从抓取的流量日志中一共提取了 5 个数据集，将工作时间段用户上网使用的爱奇艺、优酷、腾讯视频、QQ 游戏等应用和网页标记为自定义异常行为，分别为 DataSet1－DataSet5。本文建立深度学习模型，使用 10 个与网络流量相关的特征属性，具体说明如表 7 所列。数据集信息说明如表 8 所列。

表 7 深度神经网络训练属性

属性名	protocol	service	duration	orig_pkts	orig_bytes	resp_pkts	resp_bytes	conn_state	orig_ip_bytes	resp_ip_bytes
数据类型	String	String	Time	BigInt	BigInt	BigInt	BigInt	String	BigInt	BigInt

表 8　数据集信息

数据集	时间段	正常数据	异常数据
DataSet1	10:00－11:00	1743	613
DataSet2	16:00－17:00	1517	816
DataSet3	9:00－10:00	1660	701
DataSet4	9:00－10:00	1567	485
DataSet5	15:00－16:00	1445	643

深度神经网络不能处理字符型数据,需要将选择的特征中字符型的数据转变成数字型,然后将离散型数据采用 max-min 标准归一化处理,归一化公式为 $x'=\frac{x-x_{\min}}{x_{\max}-x_{\min}}$,最后将处理过后的数据作为深度神经网络的输入向量。

数据预处理完之后,进行深度神经网络模型的训练。根据本实验选择的特征设定深度神经网络模型的参数:输入层神经元为 10 个,输出层神经元为 2 个,中间隐含层有 3 层,其神经元个数为分别 10,20,10,训练次数为 2000 次。然后初始化深度神经网络模型以进行训练,再使用多个测试集进行模型的准确度对比试验。

3.2　实验平台

本文使用 3 台服务器搭建的 bro 分布式采集系统进行流量采集,使用基于 python3 环境的 TensorFlow、keras 开源深度学习框架来实现模型构建与数据检测预测。本文实验所用实验平台为一台普通 PC 机,内存为 16 GB,处理器为 coreI7-8700,操作系统为 Windows。

3.3　实验结果与分析

将处理过后每个数据集按照各自的正常行为和异常行为比例进行训练,然后使用下一个数据集作为测试集来进行交叉验证。在用户异常行为检测中,为了减弱数据不平衡带来的模型评估的不良影响,本文建立混淆矩阵来验证实验模型[20]。样本测试数据中正确检测用户异常行为、用户正常行为分别由 TP(True Positive)和 TN(True Negative)表示,识别错误的用户异常行为和用户正常行为分别由 FN(False Negative)和 FP(False Positive)表示,具体如表 9 所列。

表 9　混淆矩阵

混淆矩阵		实际样本数	
		Positive	Negative
检测样本数	Positive	*TP*	*FP*
	Negative	*FN*	*TN*

对于用户异常行为检测模型的结果评估,使用准确率、AUC(Area Under Curve)值来评价模型性能。准确率 Accuracy 的计算公式如式(9)所示:

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN} \tag{9}$$

通过混淆矩阵计算各个训练模型的准确率和 AUC 值,如表 10 所列。

表 10　模型评估

训练数据集	测试数据集	准确率/%	AUC
DataSet1	DataSet2	87.75	0.93
DataSet2	DataSet3	82.86	0.89
DataSet3	DataSet4	82.71	0.85
DataSet4	DataSet5	82.36	0.78
DataSet5	DataSet1	87.71	0.90

表 10 是由 TensorFlow 框架构建的自定义用户异常行为检测模型,可以看出深度神经网络的用户异常检测模型的平均准确率可达到84.68%,AUC 值均值大约可达到 0.86,因此基于深度神经网络的用户异常检测方法可以有效地识别网络环境中的异常行为和自定义行为。

本文将 4 个数据集作为训练集,1 个数据集作为测试集,使用 keras 建立深度神经网络模型的参数:Adam 为优化函数(根据推荐参数,学习率为 0.001,β_1 系数为 0.9,β_2 系数为 0.999 等),隐含层激活函数为 sigmoid 函数,dropout 为 0.1 等。

表 11 是由 keras 框架建立的检测模型,准确率的平均值为 87.64%。经过两次实验可得,深度神经网络的自定义用户异常行为检测模型在真实复杂的网络环境中仍具有较好的识别检测率,并保持了较高的效率。

表 11　模型准确率

训练数据集	测试数据集	准确率/%
DataSet2－DataSet5	DataSet1	93.81
DataSet1,DataSet3－DataSet5	DataSet2	86.33
DataSet1,DataSet2,DataSet4,DataSet5	DataSet3	88.36
DataSet1－DataSet3,DataSet5	DataSet4	81.10
DataSet1－DataSet4	DataSet5	88.61

结束语　本文使用网络流量分析技术对上层应用进行分析挖掘,提取出自定义用户异常行为规则特征,结合深度神经网络算法来实现用户异常行为检测方法,弥补了传统异常检测无法满足特定网络环境中数据检测需求、对不断更新的异常行为和恶意软件无法快速做出检测、没有实现用户行为管理等缺点。与其相比,对上层应用进行流量分析,结合深度学习的分类预测使模型更具高效率,能在实际网络环境中准确检测出自定义用户异常行为和未知异常行为。但是算法模型所用特征字段需要与预先建立的标识库进行规则匹配,自定义类型也存在局部性,对数据标识库的拓展和优化变得繁琐,算法的准确性和效率会存在一些影响。不采用繁琐的标识库,对自定义用户行为和未知行为更新实现数据的自动化处理和算法全智能预测识别,是下一步研究的重点。

参 考 文 献

[1] NGUYEN D T,JUNG J E. Real-time event detection for online behavioral analysis of big social data[J]. Future Generation Computer Systems,2017,66:137-145.

[2] JIA Z,SHEN C,YI X,et al. Big-data analysis of multi-source logs for anomaly detection on network-based system[C]// 2017 13th IEEE Conference on Automation Science and Engineering (CASE). IEEE,2017:1136-1141.

[3] HABEEB R A A,NASARUDDIN F,GANI A,et al. Real-time big data processing for anomaly detection:A Survey[J]. International Journal of Information Management,2018.

[4] HAMED T,ERNST J B,KREMER S C. A survey and taxonomy of classifiers of intrusion detection systems[M]// Computer and network security essentials. Springer,Cham,2018:21-39.

[5] BINKLEY J R,Singh S. An Algorithm for Anomaly-based Botnet Detection[J]. SRUTI,2006,6:7-7.

[6] GARCIA-TEODORO P,DIAZ-VERDEJO J,MACIÁ-FERNÁNDEZ G,et al. Anomaly-based network intrusion detection:Techniques,systems and challenges[J]. computers & security,2009,28(1/2):18-28.

[7] ZHU M,YE K,XU C Z. Network Anomaly Detection and Identification Based on Deep Learning Methods[C]// International Conference on Cloud Computing. Springer,Cham,2018:219-234.

(下转第 472 页)

布越均匀，信息熵就越大，信息熵的计算式如下：

$$H(m)=-\sum_{i=0}^{255}p(m_i)\log_2 p(m_i) \tag{16}$$

其中，$p(m_i)$是灰度值为 m_i 出现的概率，那么$\sum_{i=0}^{255}p(m_i)=1$，信息熵越接近于 8，说明它的抗攻击性越好，每个像素值的概率越接近，灰度值分布越均匀，抗统计攻击性就越好。本文加密算法的信息熵是 $H=7.9889$，加密前的信息熵是 $H=7.4416$，可以看出加密后的信息熵更接近于 8，本文算法能够较好地抵抗统计攻击。

4.5 差分分析

NPCR(像素改变率)表示当明文图像中任意像素值发生微小变化或密钥做出微小的变动时，会大幅度改变密文图像的信息，NPCR 越接近理想值，说明密文对明文的敏感性越好；UACI(归一化平均改变强度)，当两个指标的值越接近理想值，说明对明文图像的细微改变越敏感，抗攻击能力越强。

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{17}$$

$$UACI=\frac{1}{M\times N}\left[\sum_i\sum_j\frac{|D_1(i,j)-D_2(i,j)|}{256}\right]\times 100\% \tag{18}$$

其中，D_1 表示密文，D_2 表示明文图像像素值发生改变时的密文。在明文图像中任取两个像素点，由式(17)计算可得，NPCR=99.6414%，NPCR=99.6380%，说明本文算法密文对明文的敏感性较好；由式(18)可得，UACI=33.3869%，UACI=33.3852%，说明本文加密算法可以较好地抵抗差分攻击。

结束语 本文采用 Logistic 混沌系统控制 Tent 混沌映射及 henon 混沌映射将混沌理论应用于图像加密领域。首先，通过构造新的动态参数控制的混沌系统(LCT)对其产生的混沌序列进行排序，从而得到一组序列，对原始位置进行索引，得到一组位置索引序列，将图像矩阵按照得到的索引位置序列进行置乱；其次，应用 henon 混沌映射得到的两个混沌序列，设计了一种新的产生伪随机序列的方法，得到一个新的混沌序列，并将其与得到的置乱图像进行异或处理，从而得到最终的密文图像。本文算法的优势在于得到的混沌序列的随机性更高，消除了其具有周期性的特点及其混沌系统较为复杂，弥补了混沌系统结构单一的缺点，增加了图像置乱与扩散的复杂度，使得其具有良好的安全性。从仿真结果及安全性能分析中可以看出，本文算法的敏感性强，安全性高。

参 考 文 献

[1] WANG X, WANG T. A novel algorithm for image encryption based on couple chaotic systems[J]. International Journal of Modern Physics B, 2012, 26(30): 395.

[2] ZHU C X, SUN K H. Chaos Image Encryption Algorithm by Correlating Keys with Plaintext[J]. China Communications, 2012, 9(1): 73-79.

[3] AKHSHANI A, AKHAVAN A, LIM S, et al. An image encryption scheme based on quantum Logistic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653-4661.

[4] 赵国敏，李国东. 基于广义 Henon 映射以及 CNN 超混沌系统图像加密方案[J]. 信阳师范学院学报(自然科学版)，2015(1)：141-145.

[5] 黄清梅，李国东. 基于 CNN 超混沌特性对图像加密技术的应用研究[J]. 绵阳师范学院学报，2017(2)：60-66.

[6] ZHOU Y, BAO L, CHEN C. A new 1D chaotic system for image encryption[J]. Signal Processing, 2014, 97: 172-182.

[7] 薛伟，王磊. 一种基于新型混沌的彩色图像加密算法[J]. 光学技术，2018，44(3)：263-268.

[8] 平萍，李健华，毛莺池，等. 混沌映射与比特重组的图像加密[J]. 中国图象图形学报，2017，22(10)：1348-1355.

[9] 黄冬梅，耿霞，魏立斐. 基于 Henon 映射的加密遥感图像的安全检索方案 [J]. 软件学报，2016，27(7)：1729-1740.

(上接第 445 页)

[8] BUCZAK A L, GUVEN E. A survey of data mining and machine learning methods for cyber security intrusion detection [J]. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1153-1176.

[9] 宋海涛，韦大伟，汤光明，等. 基于模式挖掘的用户行为异常检测算法[J]. 小型微型计算机系统，2016，37(2)：221-226.

[10] 赵刚，姚兴仁. 基于用户画像的异常行为检测模型[J]. 信息网络安全，2017(7)：18-24.

[11] 丁珊. 基于深度学习的入侵检测关键技术研究[D]. 北京：北京交通大学，2018.

[12] QIAO Y, XING Z, FADLULLAH Z M, et al. Characterizing Flow, Application, and User Behavior in Mobile Networks: A Framework for Mobile Big Data[J]. IEEE Wireless Communications, 2018, 25(1): 40-49.

[13] ALTHOFF T, JINDAL P, LESKOVEC J. Online actions with offline impact: How online social networks influence online and offline user behavior[C]// Proceedings of the Tenth ACM International Conference on Web Search and Data Mining. ACM, 2017: 537-546.

[14] MILLER D J, WANG Y, KESIDIS G. Anomaly detection of attacks (ADA) on DNN classifiers at test time[C]// 2018 IEEE 28th International Workshop on Machine Learning for Signal Processing (MLSP). IEEE, 2018: 1-6.

[15] AMARASINGHE K, KENNEY K, MANIC M. Toward explainable deep neural network based anomaly detection[C]// 2018 11th International Conference on Human System Interaction (HSI). IEEE, 2018: 311-317.

[16] KWON D, KIM H, KIM J, et al. A survey of deep learning-based network anomaly detection[J]. Cluster Computing, 2017: 1-13.

[17] LÓPEZ A U, MATEO F, NAVIO-MARCO J, et al. Analysis of Computer User Behavior, Security Incidents and Fraud Using Self-Organizing Maps[J]. Computers & Security, 2019.

[18] The Bro Network Security Monitor[OL]. http://www.bro.org.

[19] ALJAWARNEH S, ALDWAIRI M, YASSEIN M B. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model[J]. Journal of Computational Science, 2018, 25: 152-160.

[20] HE H, GARCIA E A. Learning from imbalanced data[J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 21(9): 1263-1284.