# 基于 PCA-LSTM 的入侵检测研究

高忠石[1] 苏 旸[1,2] 柳玉东[1]
(武警工程大学网络与信息安全武警部队重点实验室 西安 710086)[1]
(武警工程大学密码工程学院 西安 710086)[2]

**摘 要** 目前渗透利用、泛型攻击、SQL 注入和 APT 等隐蔽攻击危害越来越严重,而对于这些隐蔽的攻击形式,浅层的机器学习已经不能很好地对其进行检测。文中设计了一种基于主成分分析优化的长短时记忆网络的入侵检测模型,该模型的主要原理是通过主成分分析去除样本数据中的噪声信息,利用长短时记忆网络的记忆功能和强大的序列数据学习能力进行学习。采用澳大利亚网络安全中心建立的 UNSW-NB15 数据集进行实验,通过对调整关键参数(时间步长、学习率和激活函数)进行模型分析,结果表明该模型比传统模型有更高的准确率。

**关键词** 主成分分析,长短时记忆网络,入侵检测,准确率,UNSW-NB15
**中图法分类号** TP309 **文献标识码** A

## Study on Intrusion Detection Based on PCA-LSTM

GAO Zhong-shi[1] SU Yang[1,2] LIU Yu-dong[1]
(Key Laboratory for Network and Information Security of Chinese Armed Police Force, Engineering University of PAP, Xi' an 710086, China)[1]
(College of Cryptographic Engineering, Engineering College of PAP, Xi'an 710086, China)[2]

**Abstract** At present, concealed attacks such as exploit, generics, SQL injection and APT are becoming more and more serious, and shallow machine learning is no longer a good way to detect these hidden forms of attack. In this paper, an intrusion detection model based on principal component analysis optimization for long and short time memory networks was designed. The main principle is to remove the noise information in the sample data through principal component analysis, and utilize the memory function of long and short memory networks and the powerful sequence data learning ability. The UNSW-NB15 data set established by Australian Network Cyber Center is adopted to conduct experimental analysis by adjusting the key parameters time-steps, learning rate and activation function. The results show that this model has higher accuracy than traditional model.

**Keywords** Principal component analysis, Long short-term memory, Intrusion detection, Accuracy, UNSW-NB15

## 1 引言

随着科技的不断进步,为了增加很多基础设施的实时态势感知和操作效率开放了公共网络,但同时,电脑蠕虫、木马等恶意攻击对信息安全造成了极大威胁[1]。据 2018 年 8 月 CNCERT/CC 发布的《2017 年中国互联网网络安全报告》[2]数据统计,2017 年我国境内木马或僵尸程序受控主机 IP 地址数量为 12 558 412 个,监测到境内 29 396 个网站被植入后门,其中政府网站有 1 339 个。包括漏洞利用、网页仿冒、扫描、渗透测试、点击劫持、SQL 注入、网页挂马、拒绝服务攻击等在内的恶意行为已经成为我国目前面临的最主要的网络问题。

入侵检测[3]系统作为网络安全体系的一个重要组成部分,主要分为误用检测和异常检测。误用检测根据已有的知识构建规则库,对于已知的攻击具有较好的效果,但缺点也很明显,维护频繁并且不能检测未知攻击。异常检测通过对异常行为特征进行训练,能检测已知和未知攻击。虽然异常检测比误用检测的误检率和漏检率都低,但对于用户来说,检测率和误检率依然比较高,为了解决这些问题,数据挖掘和机器学习被引入到网络入侵检测中[4]。随着科技的发展,互联网规模越来越庞大,结构越来越复杂,但是由于计算机网络设计之初没有过多考虑安全问题,一些底层的问题始终困扰着我们,网络攻击者在和安全人员的攻防博弈中提升了相关能力,致使现在的网络攻击趋向于更隐蔽。此外,部分国家为了自身利益有组织地对他国发动高级持续威胁(Advanced Persistent Threat, APT)[5]。针对 0day 漏洞[6],专业性和针对性极强的工具不断被开发出来。随着攻击手段、攻击技术的不断提升和 NSA 黑客武器库中"核武器"级攻击程序的恶意利用,现有的浅层模型学习能力不足,基于浅层模型的入侵检测系统很难对各种类型的攻击进行有效检测。深度学习通过组合低层特征形成更加抽象的高层表示,以发现数据的分布式特征表示,训练出分类效果较高的分类器,从而提高检测系统检测的实时性和准确率[7-8]。

例如,典型 APT 的攻击流程包括情报收集漏洞扫描,针

本文受国家自然科学基金项目(61103231)资助。
**高忠石**(1989—),男,硕士,主要研究方向为网络安全;**苏 旸**(1975—),男,博士,教授,CCF 高级会员,主要研究方向为网络攻防、可信计算,E-mail:15114894304@163.com(通信作者)。

对收集的漏洞信息开发工具进行恶意代码植入，横向提升权限，与外部建立命令和控制通信，潜伏等待执行特定任务。APT 攻击为了执行特定任务，会在目标主机长时间潜伏，从扫描漏洞到最终执行任务有可能需要几个月甚至数年。对于此类攻击，一般的机器学习方法很难学习这么长时间跨度内相关的序列特征。长短时记忆网络(LSTM)非常适合从很长时间跨度内学习序列特征，相对于循环神经网络有更强的学习能力。网络安全数据中，通常异常样本明显少于正常样本，为了避免正负样本数据不均衡影响模型训练，在训练之前利用 smote 合成技术生成异常行为样本。本文在 smote 技术处理数据的基础上，构建了基于 PCA-LSTM 的入侵检测模型，利用 PCA 对高维数据进行降维重构，实验结果表明，本文的方法对异常行为检测有较高的效率和准确率。

## 2 相关工作

王伟[9]采用了一种在数据包和网络流两个层次上使用两阶段 LSTM 的网络流量分类方法。该方法分别使用双向 LSTM 分阶段地学习数据包和网络流的特征，得到比较综合全面的时序特征后进行分类，实现更加准确的网络流量分类效果。该方法充分考虑了网络流量的内部结构组织关系，有效利用了 LSTM 优秀的时序特征学习能力。Wang 等[10]利用当前卷积神经网络(CNN)在图像识别方面成功的应用，将流量特征映射为像素点，进而生成“图片”，将此“图片”作为 CNN 的输入，该方法在二分类、多分类方面都取得了较高的准确率。长短时记忆网络模型将流量特征转化为序列特征在检测渗透利用、泛型攻击和注入攻击等低频攻击方面有更好的适应性。Pektaş等[11]提出了一种将卷积神经网络与长短时记忆相结合的深度学习结构。其原理是从原始网络流量中提取流量特征，对流量进行分组，将连续的 $N$ 条流量记录转换为二维数组，利用卷积神经网络学习空间特征，而长短时记忆网络则从一系列网络原始数据包中学习时间特征，取得了较好的分类结果。

## 3 PCA-LSTM 模型研究

### 3.1 主成分分析

随着大数据技术的发展，网络数据已经从 GB 级向 PB 级发展，面对如此大量高维的数据，当前高速发展的技术手段直接处理起来依旧显得能力不足。主成分分析(Principal Component Analysis，PCA)方法是一种使用最广泛的数据降维算法，由皮尔逊首先使用[12]，PCA 的原理就是从原始的数据中顺序地找一组相互正交的坐标轴，新的坐标轴的选择与数据本身是密切相关的。第一个新坐标轴选择是原始数据中方差最大的方向，后面每次选择的坐标轴均是与已选坐标轴相互垂直的平面内方差最大的方向，可以得到 $n$ 个这样的坐标轴。大部分方差都包含在前面 $k$ 个坐标轴中，后面的坐标轴所含的方差几乎为 0。取前 $k$ 个含有绝大部分方差的坐标轴，这 $k$ 维全新的正交特征即为主成分。事实上，这相当于只保留包含绝大部分方差的维度特征，而忽略包含方差几乎为 0 的特征维度，实现了对数据特征的降维处理。

### 3.2 长短时记忆网络

目前对 web 安全有极大威胁的一句话木马，其获取服务器 shell 的关键是如何绕过系统防护上传代码，常见的是类似于 SQL 注入，将代码嵌入留言板，从而达到欺骗服务器执行恶意代码的目的。如某服务器唯一的上传入口为照片上传，且上传文件类型限制为 JPG 和 JPEG，攻击者为了将〈%eval request(“value”)%〉这个 asp 代码(其中 value 是自己设置的可变的值，request 就是为了得到这个值)通过此入口上传，如果直接上传，服务器会提示文件类型错误。攻击者如果将文件类型改为 cer 证书格式，则可以欺骗服务器，成功上传。一旦上传成功，就可以通过主控端的中国菜刀或者其他主控程序与服务器建立连接，进行后续入侵，一句话木马的核心就是将这句代码添加到数据库中。一句话木马文本内容前后文往往会出现“… eval … request…”和“…execute …request…”等局部关联性较强的内容。对于一句话木马检测识别，可以通过将此过程还原，对尝试登陆后台、尝试上传文件、修改格式属性直至上传成功和与外部加密通信等前后关联的事件进行重点检测，对上传成功的文件文本内容进行前后文关联性检测。

长短时记忆网络是 Sepp Hochreiter 和 Jürgen Schmidhuber[13]于 1997 年提出的一种递归神经网络(RNN)结构。与大多数 RNN 一样，LSTM 网络是通用的，因为只要有合适的权重矩阵，LSTM 网络就可以计算出任何常规计算机可以计算的任意网络单元。与传统的 RNN 不同，LSTM 网络非常适合于从经验中学习，在重要事件之间存在未知大小和界限的时间滞后时，对时间序列进行分类、处理和预测。LSTM 对于间隙长度不敏感，比其他 RNN 和隐马尔可夫模型[14]以及其他序列学习方法在许多应用中都具有优势。通过引入门结构和存储单元，解决了梯度消失和梯度爆炸问题。图 1 显示了单个 LSTM 细胞，$\sigma$ 是一个逻辑函数，tanh 是双曲正切函数，⊕ 表示元素加运算，⊗表示元素乘运算。

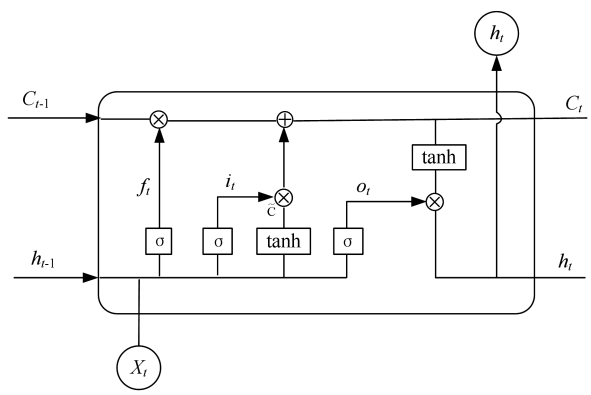


图 1 LSTM 单元结构

LSTM 相对于其他神经网络的优势在于内部复杂的“门”(gates)，LSTM 通过它内部的“门”可以在接下来更新的时候“记住”前几次训练的“残留记忆”[15]。LSTM 的关键就是，怎样控制长期状态 $C$，其分步执行过程如图 1 所示。

(1)遗忘门。该过程决定从单元状态中保留哪些信息，这个决定通过“遗忘门限”sigmoid 层做出决定，在单元状态 $C_{t-1}$ 上，$h_{t-1}$ 和 $x_t$ 输出 0 和 1 之间的一个数字，其中 1 代表保留所有信息，0 代表丢掉所有信息。

$$f_t=\sigma(W_f\cdot[h_{t-1},x_t]+b_f) \tag{1}$$

(2)输入门。该过程要决定在单元状态中存储哪些新的信息，首先被称为“输入门”的 sigmoid 层决定哪些值会更新，接着一个 tanh 层创建新的候选值向量 $C_{t-1}$，这是一个可添加

的状态。单元状态更新，结合 sigmoid 层和 tanh 层创建一个更新的状态，对单元状态进行一次更新。

$$i_t=\sigma(W_i\cdot[h_{t-1},x_t]+b_i) \tag{2}$$

$$\tilde{C}_t=\tanh((W_C\cdot[h_{t-1},x_t]+b_C)) \tag{3}$$

再来更新旧状态 $C_{t-1}$，进入新的单元状态 $C_{t-1}$。对 $C_{t-1}$ 乘以旧状态 $f_t$，丢弃之前我们决定忘记的部分，再加上 $i_t*\tilde{C}_t$ 得到新的候选值。

$$C_t=f_t*C_{t-1}+i_t*\tilde{C}_t \tag{4}$$

(3)输出门。首先运行一个 sigmoid 层决定我们要输出的状态，然后将单元状态通过 tanh 函数和 sigmoid 层的输出相乘，得到目标输出。

$$\sigma_t=\sigma(W_o\cdot[h_{t-1},x_t]+b_o) \tag{5}$$

$$h_t=o_t*\tanh(C_t) \tag{6}$$

### 3.3　算法流程分析

算法流程如图 2 所示，LSTM 的训练算法仍然是反向传播算法，对于该算法，主要有以下 4 个步骤：

(1)前向计算每个神经元的输出值，如式(1)到式(6)所示。

(2)反向计算每个神经元的误差项值。与循环神经网络一样，LSTM 误差项的反向传播也是包括两个方向：1)沿时间的反向传播，即从当前时刻 $t$ 开始，计算每个时刻的误差项；2)将误差项向上一层传播。

(3)根据相应的误差项，计算每个权重的梯度。

(4)根据梯度更新权重。

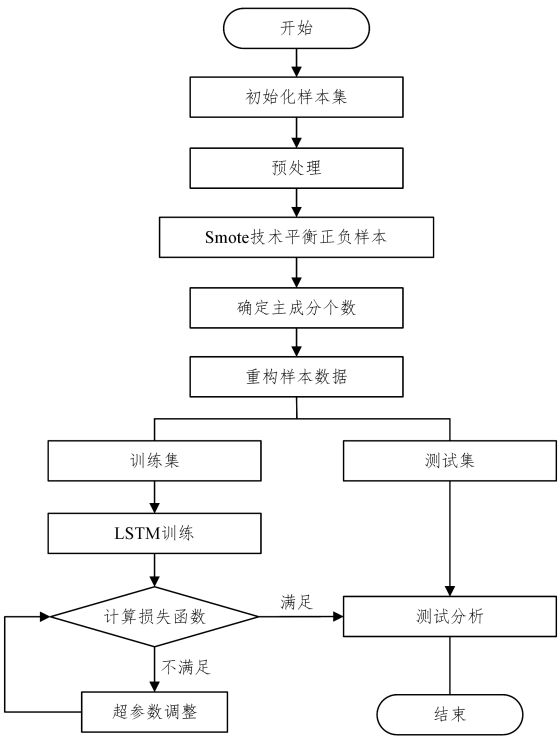


图 2　PCA-LSTM 流程

### 3.4　最优超参数选择

超参数是必须给网络初始化的值，这些数值不能在训练的过程中学到。在神经网络中，这些超参数包括：学习率、神经网络层数、隐藏层大小、激活函数、损失函数、时间步长、所用的优化器、批大小、训练的 epoch 次数等。其中学习率会影响神经网络的收敛，合适的学习率对模型能否收敛到全局最小值至关重要。神经网络层数和隐藏层大小增大时可以提高网络复杂度，降低误差，但是可能出现过拟合现象。合适的激活函数有助于模型更好的学习，现在常用的激活函数有 ReLU、Sigmoid 和 Tanh 函数。epoch 次数应根据计算能力进行合理取值。

### 3.5　PCA 步骤

对一个样本集合进行主成分分析的步骤为：

(1)对原始数据进行规范化；

(2)计算规划后的协方差矩阵 $U$；

(3)对方差矩阵进行特征值分解；

(4)将特征值按照从大到小的顺序为 $\lambda_1,\lambda_2,\cdots,\lambda_k,\cdots,\lambda_n$，取前 $k$ 维实现特征约简。

则前 $k$ 个主成的累计贡献率 $\eta$ 计算式如下：

$$\eta=\frac{\sum_{i=1}^{k}\lambda_i}{\sum_{i=1}^{n}\lambda_i}$$

本文主成分累计贡献率 $\eta$ 不低于 90%。

## 4　实验设计与分析

### 4.1　实验环境

实验所用主机为 Ubantu14.0 操作系统，处理器为 Intel Corel i7-4700MQ@2.4GHz，内存为 16GB。在 Python 2.7 中 tensorflow 平台环境下进行仿真实验。

### 4.2　评价矩阵

分类结果有 4 种情况，如表 1 所列，其中 TP 为真正类，FN 为假负类，FP 为假正类，TN 为真负类。评价分类器性能的指标如下：

准确率 $ACC=\dfrac{TP+TN}{TP+FP+FN+TN}$

误警率 $FPR=\dfrac{FP}{FP+TP}$

漏警率 $FNR=\dfrac{FN}{FN+TN}$

召回率 $DR=\dfrac{TP}{FN+TP}$

表 1　评价矩阵

| | 预测为攻击 | 预测为正常 |
|---|---|---|
| 实际为攻击 | TP | FN |
| 实际为正常 | FP | TN |

### 4.3　实验数据

目前针对入侵检测，绝大多数人均使用的是美国林肯实验室的 KDD CUP99 数据集[16]，该数据集曾经是入侵检测领域的 benchmark，在一定时期内的效果很好。但是该数据集是 20 年前采集到的数据，随着网络的高速发展，当时模拟的实验条件和攻击手段已经无法满足当今的入侵检测系统，不能用来评价今天复杂的网络，如跨站脚本攻击、跨站请求伪造和点击劫持等近年来才出现的攻击形式，即使是在此数据集上测试性能很好的分类器，在实际网络中的效果也大打折扣，主要原因是，一方面互联网高速发展，网络架构向更复杂的方向发展，另一方面网络攻击向着更隐蔽的方向发展，伪装得更加接近正常行为。为此，澳大利亚网络安全中心在 2015 年建立了 UNSW-NB15[17]，它反映了现代网络流量模式，其中包含大量低占用入侵和深度结构化的网络流量信息，该数据集

包含 2540044 个数据实例，包含正常数据和 9 类攻击，攻击类型分别为模糊测试、渗透分析、后门、拒绝服务攻击、漏洞利用、泛型攻击、踩点、shellcode 和蠕虫。该数据集中每条记录共 49 维，其中第 1－5 维为流特征，第 6－18 维为基本特征，第 19－26 维为内容特征，第 27－36 维为时间特征，第 37－47 维为额外生成特征，第 48－49 维为标签特征，前 47 维是数据特征，后 2 维为数据标签特征。由于网络中大量的数据是正常数据，异常数据相对于正常数据的比率很小。在数据集 UNSW-NB15 中，攻击类样本记录 321283 条，正常样本记录 2218761 条。简单地使用欠抽样技术可能会使得多数类样本的关键信息丢失，采用少数类样本过抽样则会导致出现大量的重复样本，容易出现过拟合问题。为了减弱样本不均匀性对分类结果的影响，采用 smote 过抽样技术，smote 过抽样技术在很多方面已经取得了成功[18]，它是利用少数类样本生成人工样本，其原理是利用已有的少数类样本根据相似性原理生成新样本，对于少数类样本 $x$ 寻找其同类样本中的 $k$ 个最近邻，从 $k$ 个近邻中随机选择一个样本 $x_i$，在 $x$ 和 $x_i$ 中随机线性差值生成合成样本 $x_{new}$，如式(7)所示，重复此过程直至样本平衡。

$$x_{new}=x+\delta*(x_i-x) \tag{7}$$

其中，$x_{new}$ 为新生成的样本，$x$ 为已知样本，$x_i$ 为 $x$ 的 $k$ 个同类最近邻样本随机选的一个样本，$\delta$ 为(0,1)之间的一个随机数。

### 4.4 实验设置与分析

在实验中，输入向量为 47 维特征，输出标签中 9 种攻击均用 1 标记，正常用 0 标记，采用二分类形式可以提高模型的训练速度，因为入侵检测对时效性的要求较高，首先判断出这是入侵行为报警之后，再由管理员具体分析入侵属于哪一类，再采取相应的防范措施。因此，输入维度是 47，输出维度是 2。经过 PCA 变换，实验中取不低于 90% 累计贡献率，得到的主成分个数为 17，累计贡献率为 91.03%。LSTM 采用 5 层结构，包括输入层、输出层和 3 层隐藏层，隐藏层神经元个数分别设置为 64，128 和 64，批大小和 epoch 次数分别为 100 和 500，激活函数采用 sigmoid 函数，学习率取 0.01。首先从 UNSW-NB15 中采用 smote 抽样技术选择 10 个测试数据集，每个数据集包含 5000 个随机选择的实例。由于时间步长对系统的性能影响较大，因此首先计算不同时间步长情况下模型的召回率 DR，结果如图 3 所示。

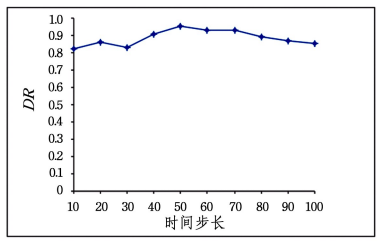


图 3 时间步长对召回率的影响

为了增强模型泛化能力，进行了改变学习率和激活函数的实验，计算不同参数取值情况下分类器的准确率和漏报率。具体实验结果如表 2 所列，由表 2 可知，模型采用 ReLU 函数作为激活函数在学习率为 0.01 时效果最好，这是由于 ReLU 函数相对于 sigmoid 函数和 tanh 函数既不会出现梯度消失问题，同时也有效避免了过拟合问题，而学习率过大会使模型在全局最小值附近来回波动，学习率过小模型易陷入局部最小。

表 2 不同参数条件下准确率和漏警率对比

(单位：%)

| | $r=0.05$ | | $r=0.01$ | | $r=0.05$ | | $r=0.1$ | |
|---|---|---|---|---|---|---|---|---|
| | acc | fnr | acc | fnr | acc | fnr | acc | fnr |
| ReLU | 90.24 | 8.15 | 94.34 | 4.17 | 92.78 | 7.57 | 88.4 | 13.6 |
| Sigmoid | 83.94 | 10.33 | 93.77 | 6.32 | 93.52 | 8.43 | 89.68 | 14.64 |
| tanh | 86.44 | 9.51 | 89.49 | 9.81 | 89.63 | 6.54 | 85.25 | 18.2 |

在上文实验的基础上，选用 ReLU 函数作为激活函数，学习率取 0.01，其他参数同上，研究基于 PCA 降维的 LSTM 和 LSTM 在 UNSW-NB15 上的检测效果，各项评价指标结果如表 3 所列，从结果可以看出，PCA-LSTM 有更好的性能，这是因为高维的网络数据中含有大量的冗余特征，影响分类器对异常行为的检测识别。

表 3 对比 LSTM 和 PCA-LSTM

| | ACC/% | FNR/% | FPR/% | F1/% | 平均训练时间/s |
|---|---|---|---|---|---|
| PCA-LSTM | 94.34 | 4.17 | 8.43 | 95.14 | 21.3 |
| LSTM | 87.52 | 6.21 | 15.16 | 88.5 | 28.5 |

**结束语** 针对当前渗透测试、后门和注入等复杂低频攻击对网络的危害越来越严重，而基于传统的浅层机器学习的入侵检测对此类攻击效果不佳，本文设计了一种基于主成分分析法降噪的长短时记忆网络的入侵检测模型，实验表明该方法对当前复杂的网络攻击有较好的检测效果。

## 参 考 文 献

[1] RASS S,ZHU Q. GADAPT:A Sequential Game-Theoretic Framework for Designing Defense-in-Depth Strategies Against Advanced Persistent Threats[C]// International Conference on Decision and Game Theory for Security. Springer International Publishing,2016:314-326.

[2] http://www.cert.org.cn/publish/main/46/2018/20180802135136854322283/20180802135136854322283_.html.

[3] 卿斯汉，蒋建春，马恒太，等. 入侵检测技术研究综述[J]. 通信学报，2004，25(7)：19-29.

[4] LEE W,STOLFO S J,MOKA K W. Data mining framework for building intrusion detection models[C]// Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344). Oakland,CA,USA,1999,pp. 120-132.

[5] 付钰，李洪成，吴晓平，等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报，2015，36(11)：1-14.

[6] OWEZARSKI P,MAZEL J,LABIT Y. 0day anomaly detection made possible thanks to machine learning[M]// Wired/Wireless Internet Communications. Springer Berlin Heidelberg,2010.

[7] SCHMIDHUBER J. Deep Learning in neural networks:An overview[J]. Neural Netw,2015,61:85-117.

(下转第 492 页)

相应的 NPCR 和 UACI，结果如表 3 所列。可以看出，本文算法的 NPCR 和 UCAI 都能满足算法安全的要求，从而可以较强地抵抗差分攻击。

表 3 密文图像的 NPCI 和 UACI

（单位：%）

| NPCR | UACI |
|---|---|
| 99.8948 | 33.4335 |

**结束语** 本文提出了一种基于分数阶 Chen 超混沌的频域自适应图像加密算法，结合了频域与空域，并且将置乱、代换、扩散 3 种操作有机地结合起来，使它们的优势互相补充。比一般单纯空域加密或普遍使用的置乱-扩散结构更具安性，并且加密效率更高。另外，本文使用高维超混沌系统，生成的伪随机序列不会因为计算机精度有限而导致伪随机序列可能存在短周期，从而产生加密安全性不够高的问题。使用自适应加密，加密过程中不仅依赖于密钥，而且一定程度上依赖于明文和加密过程中产生的中间数据，使选择明文攻击将更难成功，算法的安全性更高。本文扩散使用双向扩散，使扩散速度更快。算法仅通过 3 轮迭代就可达到和以前提出的图像加密算法相同的安全级别，加密效率显著提高。

## 参 考 文 献


[1] 陈翼翔，汪小刚. 基于双随机相位编码的非线性双图像加密方法[J]. 光学学报，2014，34(7)：0710001.

[2] 陈翼翔，汪小刚. 一种基于迭代振幅-相位复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报，2014，34(8)：0810003.

[3] GAO T G，CHEN Z Q. A new image encrypyion algorithm based on hyper-chaos[J]. Physics Letter A，2008(372)：394-400.

[4] CHEN G，ZHAO X Y，LI J L. A Self-Adaptive Algoritthm on image Encryption[J]. Journal of Software，2005，16(11)：1975-1982.

[5] 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003，24(2)：51-57.

[6] ACHARYA B，PATRA S K，PANDA G. Image Encryption by Novel Cryptosystem Using Matrix Transformation[C]// First Internation Conference on Emerging Trends in Engineering and Technology，2008. Washington D C：IEEE Press，2008，77-81.

[7] 朱薇，杨庚，陈蕾，等. 基于混沌的改进双随机相位编码图像加密算法[J]. 光学学报，2014，34(6)：0607001.

[8] 潘泉，张磊，孟晋丽，等. 小波滤波方法及其应用[M]. 北京：清华大学出版社，2005.

[9] 刘钺. 一种小波变换域图像加密技术[J]. 计算工程与应用，2010，46(19)：157-159.

[10] 倪林. 小波变换与图像处理[M]. 合肥：中国科技技术大学出版社，2010.

[11] SCHNEIER B. Applied cryptography：protocols，algorithms，and source code in C[M]. John Wile y& Sons，2007.

[12] 绪其军，李德林，常琛亮，等. 基于 Q-plate 的双图像非对称偏振加密[J]. 物理学报：1-8.[2019-04-16].

[13] 曾健清，王君，吴超. 基于频谱融合和柱面衍射的双图像非对称加密[J]. 光子学报：1-11.[2019-04-16].

[14] 梁锡坤，陶利民，胡斌. 一类广义混沌映射和矩阵非线性变换的图像混合加密[J]. 中国图象图形学报，2019，24(3)：325-333.

[15] 钟艳如，刘华役，孙希延，等. 基于 2D Chebyshev-Sine 映射的图像加密算法[J]. 浙江大学学报(理学版)，2019(2)：131-141，160.

[16] 拜亚萌，张燕玲，邓小鸿. 自适应分块的医学图像混沌加解密算法[J/OL]. [2019-10-25]. https://doi. org/10. 19734/j. issn. 1001-3695. 2018. 10. 0830.

[17] 韩啸，熊礼治，蒋鹏程，等. 一种密文图像安全性评价方案[J]. 计算机应用与软件，2019，36(3)：148-153.

[18] 傅彬. 一种混沌的图像加密算法的研究[J]. 科技通报，2019，35(2)：70-75.

[19] 袁源，和红杰，陈帆. 减少相邻位平面间冗余度的加密图像可逆信息隐藏[J]. 中国图象图形学报，2019，24(1)：13-22.

[20] 程宁，王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报，2019，33(1)：191-202.


(上接第 476 页)


[8] 孙志军，薛磊，许阳明，等. 深度学习研究综述[J]. 计算机应用研究，2012，29(8)：2806-2810.

[9] 王伟. 基于深度学习的网络流量分类及异常检测方法研究[D]. 合肥：中国科学技术大学，2018.

[10] WANG W，ZHU M，ZENG X，et al. Malware traffic classification using convolutional neural network for representation learning[C]// International Conference on Information Networking. IEEE，2017.

[11] PEKTAPS，ABDURRAHMAN，ACARMAN T. A deep learning method to detect network intrusion through flow-based features[J]. International Journal of Network Management，2018.

[12] 冶晓隆，兰巨龙，郭通. 基于 PCA 和禁忌搜索的网络流量特征选择算法[J]. 计算机科学，2014，41(1)：187-191.

[13] HOCHREITER S，SCHMIDHUBER J. Long Short-Term Memory[J]. Neural Computation，1997，9(8)：1735-1780.

[14] ADITYA R，FABIO D T，MARK S. Hidden Markov models with random restarts versus boosting for malware detection[J]. Journal of Computer Virology and Hacking Techniques，2018.

[15] GREFF K，SRIVASTAVA R K，KOUTNÍ K，et al. LSTM：A Search Space Odyssey[J]. IEEE Transactions on Neural Networks & Learning Systems，2015，28(10)：2222-2232.

[16] DAPPA. KDD Cup99 dataset[EB/OL]. [2019-03-10]. http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html.

[17] UNSW-NB15[EB/OL]. [2019-03-10]. http://www. cybersecurity. unsw. adfa. edu. au/ADFA%20NB15%20Datasets/.

[18] 陶新民，刘福荣，杜宝祥. 不均衡数据 SVM 分类算法及其应用[M]. 哈尔滨：黑龙江科学技术出版社，2011：43-45.