基于 CNN 的国产商用分组密码算法识别研究

刘节威[1],王　钢[2],颜培志[2],方一格[1],荆　浩[3]
(1.内蒙古工业大学 数据科学与应用学院,内蒙古 呼和浩特 010051;
2.内蒙古工业大学 信息化建设与管理中心,内蒙古 呼和浩特 010051;
3.内蒙古工业大学 信息工程学院,内蒙古 呼和浩特 010051)

摘　要:随着国产商用密码算法的应用普及与商密应用测评工作的推进,商密算法的应用合规性备受关注。尝试针对商用分组密码算法开展识别研究,将其应用到密评工作中。提出了一种基于自动编码器和卷积神经网络结合的分组密码算法识别方案,将商密 SM4 算法与国际主要标准分组密码算法进行识别。利用 NIST 随机性测试方法对密文进行特征提取,最后借助卷积神经网络对密文特征进行训练和测试。实验表明,密码算法的密钥长度是否一致是影响识别准确率的重要因素,SM4 与其他算法两两识别的准确率可达 80%之上,并且识别效果与现有方案相比具有较高的准确率和稳定性。

关键词:随机性测试;密码算法识别;卷积神经网络;自动编码器;SM4 算法
中图分类号:TP391　　**文献标识码**:A　　**DOI**:10.20044/j.csdg.2097-1788.2022.03.006
引用格式:刘节威,王钢,颜培志,等. 基于 CNN 的国产商用分组密码算法识别研究[J].网络安全与数据治理,2022,41(3):33-39.

Research on identification of domestic commercial block cipher algorithms based on CNN

Liu Jiewei[1], Wang Gang[2], Yan Peizhi[2], Fang Yige[1], Jing Hao[3]
(1.College of Data Science and Applications, Inner Mongolia University of Technology, Hohhot 010051, China;
2.Information Construction and Management Center, Inner Mongolia University of Technology, Hohhot 010051, China;
3.College of Information Engineering, Inner Mongolia University of Technology, Hohhot 010051, China)

Abstract: With the popularization of domestic commercial cryptographic algorithms and the advancement of commercial cryptographic application evaluation, the application compliance of commercial cryptographic algorithms has attracted much attention. This paper attempts to carry out identification research on commercial block cipher algorithms and apply them to the evaluation of commercial cipher applications. In this paper, a block cipher algorithm identification scheme based on the combination of autoencoder and Convolutional Neural Networks(CNN) is proposed. The NIST randomness test method is used to extract the features of the ciphertext, and finally the ciphertext features are trained and tested by means of CNN. Experimental results show that whether the key lengths of the cryptographic algorithms are consistent is an important factor affecting the recognition accuracy. The accuracy of SM4 and other algorithms can reach more than 80%, and compared with the existing schemes, the recognition effect has higher accuracy and stability.

Key words: randomness test; cryptographic algorithm identification; convolutional neural network; autoencoder; SM4 algorithm

0 引言

在商用密码应用安全性评估工作中,要求对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性与正确性进行评估[1]。分析与识别安全系统所采用的密码算法,对于评估信息系统安全性、密码使用合规性与正确性、中间人攻击等方面有着重要的现实意义。同时,密码算法识别是开展密码分析的前提条件,也是密码分析的一个重要组成部分。无论是对信息系统或网络设备中商用密码算法的应用合规性进行评估还是开展

www.pcachina.com

密码分析工作,对密文进行密码算法识别都是至关重要的前提。目前对密码算法的识别方向主要有两个:(1)逆向分析技术[2-4];(b)唯密文特征识别技术。在密评工作中,由于密码算法应用合规性检测多采用逆向分析技术,存在耗时和安全性等问题,利用唯密文特征识别密码算法可以缓解上述问题的存在。同时,唯密文方法是目前主流的研究方向,也是本文所采用的方法。

由于密码轮函数、密钥长度和加密结构等加密条件的不同,明文经过不同密码算法加密而来的密文在空间分布上也会存在差异,且加密后的密文数据也并未达到真正的随机性,彼此之间尚存微小差异。因此可通过提取密文数据隐藏的特征关系作为密码算法识别的依据。虽然利用统计学的方法对古典密码算法进行识别取得了不错的成绩,但对现代密码算法识别工作却收效甚微[5]。随着机器学习在其他领域的成熟应用发展,其逐渐被研究者引入密码算法识别任务中。利用机器学习算法对唯密文开展密码算法识别可以将其视为模式识别问题,通过某种方式对密文提取特征,并对提取到的密文特征进行选择和机器学习模型训练,最终识别出其所属的密码算法。当前常见的密文特征提取方式有:(1)NIST 随机性测试返回 p_value 特征值[6-7];(2)特定字符、字节或比特的熵;(3)特定字符、字节或比特的概率;(4) 将密文看成可变长的文档向量[8];(5)以上几种特征提取方式组合[9-10]。本文采用 NIST 随机性测试方法提取密文特征,通过分析特征分布情况选择合适的随机性测试方法。

1 相关研究

如今,将机器学习方式运用到密码算法识别领域的研究日渐增多。2010 年,Kuncheva 等人[11]对 DES、IDEA、RC2、AES 共 4 种分组密码算法进行识别,研究了 8 种机器学习模型在密码算法识别中的效果。2011 年,Manjula 等人[12]基于决策树算法,对 11 种加密算法进行识别,识别的密码体制包括分组密码、公钥密码、序列密码与古典密码。2012 年,Chou 等人[13]设计了基于支持向量机的识别模型,对 ECB 模式与 CBC 模式下的 AES、DES、RC4 三种分组密码算法生成的密文进行加密算法识别。2015 年,吴杨等人[6]基于 NIST 的随机性测试方法,选取三种测试方法设计密文特征,对 AES、DES、3DES、Camellia、SM4 五种分组密码算法使用 K-mean 聚类算法进行两两聚类。2018 年,黄良韬等人[9]综合已有的密码算法识别研究成果,给出了密码算法识别系统的一个形式化定义,然后对古典密码、流密码、分组密码、公钥密码四种体制,通过簇分和单分两个阶段划分识别阶段,然后基于随机森林算法进行分层识别。同年,赵志诚等人[14]结合随机性测试方法、比特熵和不定长文本向量等方法,设计密文特征,将 Grain-128 密码算法分别与 11 种其他对称密码算法进行了两两区分。2019 年,赵志诚等人[7]基于 NIST 随机性测试标准重新设计密文特征提取方法,基于随机森林算法完成对 AES、DES、3DES、IDEA、Blowfish 和 Camellia 六种分组密码算法的两两区分实验。2021 年,纪文桃等人[15]针对分组密码算法进行识别,利用三种随机测试方法对密文提取特征,训练 C4.5 决策树分类模型将商密 SM4 算法与国际主要标准分组密码算法进行两两识别。同年,曹莉茹[16]使用随机性测试方法选择密文特征,使用深度学习方法对密码算法体制进行识别,分别将 BP 神经网络、卷积神经网络和循环神经网络算法应用于密码算法识别任务中,确定了合适的网络参数,构建相应的密码算法识别分类器,对 8 种密码算法进行识别。

分组密码算法是现代密码学中的一个重要研究分支,其诞生和发展有着广泛的实用背景和重要的理论价值,同样在众多网络设备和信息系统中广泛应用,针对国产商用分组密码算法 SM4 开展识别研究,对密评工作也具有促进作用。目前,在密码算法识别领域很少有研究者主要针对国产商用密码进行识别研究,且研究选择识别的加密算法没有考虑密钥长度等影响识别效果的变量信息。同时,深度学习技术因其拥有处理和分析大量复杂数据的能力,在图像、自然语言处理和加密流量识别等众多领域取得显著成果,其研究对人工智能技术的发展意义重大。基于此,本文提出了一种基于自动编码器(Autoencoder,AE) 和卷积神经网络(Convolutional Neural Networks,CNN)结合的分组密码算法识别方案,利用 NIST 随机性方法提取密文潜在的整体和局部特征,研究识别的密码算法是在尽量控制密钥长度一致的基础上选择,对商密 SM4 算法与 AES、Camellia、DES、IDEA 分组密码算法进行两两区分识别。

2 识别方案

密码算法识别首先要提取密文特征,然后通过

www.pcachina.com

各类密文特征之间的差异进行分类。据此，本文首先使用 NIST 随机性测试方法对密文数据提取特征，然后对特征进行数据预处理生成规则的灰度图，以便后续卷积神经网络完成分类识别任务。在特征提取阶段，选择组内频率测试、最长 1 游程测试和二元矩阵秩测试等 9 种方法体现密文数据整体特征，选择非重叠模板匹配方法体现密文数据局部特征。由于局部特征维度与整体特征维度不匹配，使用自动编码器对局部特征降维，然后对整体特征和降维后的局部特征融合处理生成对应的灰度特征图，之后将它们输入到卷积神经网络模型进行训练。该方法的结构如图 1 所示。

2.1 特征提取

由于 NIST 随机性测试众多方法对序列的整体或局部随机性均有针对性的测试，针对这一特性，本文将整体和局部特征融合共同作为密文特征来突出各种加密算法密文之间的差异性。同样，选择合适的随机性测试方法反映密文整体特征也是至关重要的。通过对各类加密算法的密文文件进行特征分布统计分析，选择了 9 种随机性测试方法反映密文整体特征，分别是频率测试(Frequency test)、组内频率测试(Frequency test within a block)、游程测试(Runs test)、最长 1 游程测试(Longest run of ones test)、二元矩阵秩测试(Binary matrix rank test)、离散傅里叶变换测试(Discrete Fourier transform test)、序列测试(Serial test)、近似熵测试(Approximate entropy test)、累加和测试(Cumulative sums test)。而反映密文局部特征的方法选择的则是非重叠模块匹配测试(Non overlapping template matching test)。

在待提取特征的密文文件统一大小的基础上，将密文文件分割为数份固定大小的二进制密文块，分别基于上述 10 种随机性测试方法提取密文特征。密码算法集合为 $M=\{m_1, m_2, m_3, \cdots, m_k\}$，其中 k 代表密码算法的数量。每种密码算法 m_i 分别加密明文文件 F 得到密文文件 C，每个密文文件 C_i 分割为一定数量等长的密文块 C_{ij}。每个密文块 C_{ij} 基于反映密文文件整体特征的 9 种随机性方法提取特征，可得特征向量 $\mathbf{Afea}_{ij}=\{\mathrm{Afea}_{ij\_1}, \mathrm{Afea}_{ij\_2}, \cdots, \mathrm{Afea}_{ij\_d}\}$；基于反映密文局部特征的非重叠模块匹配测试方法提取特征，可得特征向量 $\mathbf{Bfea}_{ij}=\{\mathrm{Bfea}_{ij\_1}, \mathrm{Bfea}_{ij\_2}, \cdots, \mathrm{Bfea}_{ij\_q}\}$。在对特征向量 $\mathbf{Afea}_{ij}$ 和 $\mathbf{Bfea}_{ij}$ 融合之前，首先需要对 $\mathbf{Bfea}_{ij}$ 进行数据降维处理。

2.2 自动编码器数据降维

自动编码器[17]是一种无监督机器学习算法，其基本思想是直接使用一层或者多层的神经网络对输入数据进行关系映射，得到输出向量作为从输入数据中提取的特征。自动编码器广泛用于数据降维[18]和特征学习[19]，与主成分分析(PCA)算法相比，自动编码器具有更好的灵活性和处理非线性特征的能力。图 2 所示为三层自动编码器模型，从图中可以看出自动编码器分为三部分：输入层、隐藏层和输出层。其中输入层向隐藏层的低维映射被称为编码器，得到输入数据的高效表征；从隐藏层到输出层的高维映射被称为解码器，对输入数据进行重构。一般情况下隐藏层的维度比输入层的维度要小，由于隐藏层抽取了输入层的有效信息，因此自动编码器可用于数据降维[20]。由于 2.1 节中特征向量 $\mathbf{Bfea}_{ij}$ 维度过高且 $\mathbf{Afea}_{ij}$ 维度过低，如果未经

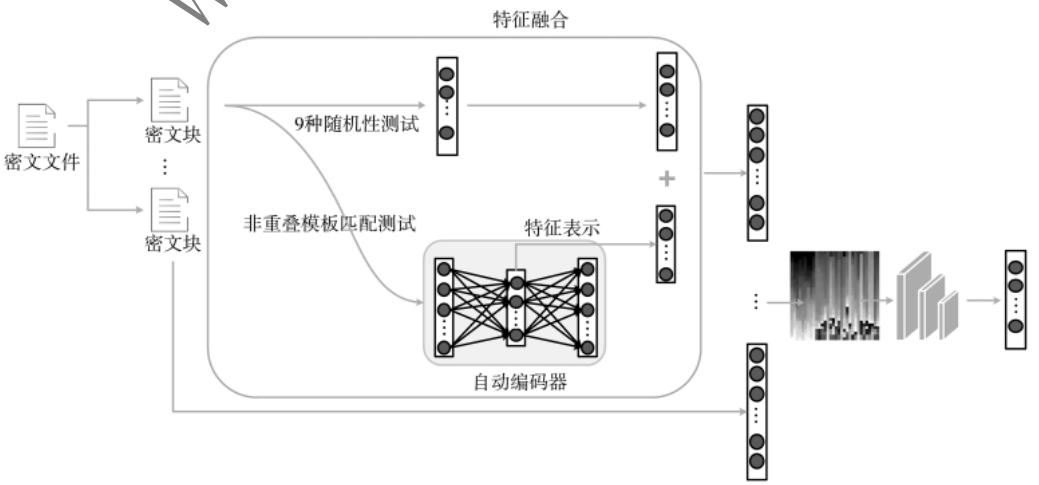


图 1 基于自动编码器和卷积神经网络的密码算法识别模型

www.pcachina.com

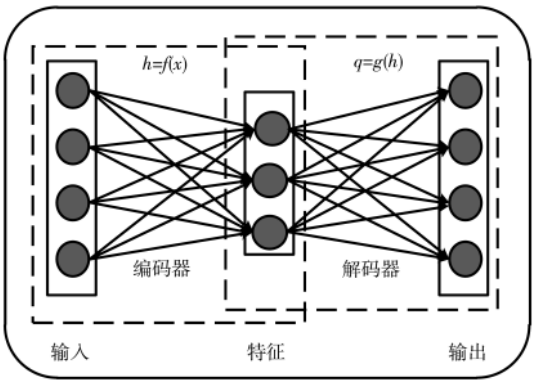


图 2　三层自动编码器模型

过任何降维处理直接融合特征向量，就会造成两个特征向量维度不匹配的问题。在分类模型训练过程中，高维度特征向量会压制低维度向量，导致训练效果不理想。

为了将密文整体和局部特征更高效地融合，使用自动编码器对特征向量 $\mathbf{Bfea}_{ij}$ 降维。以处理 16 KB 密文块为例，自动编码器模型包括 1 个输入层、4 个线性隐藏层+激活层、1 个输出层，如图 3 所示。

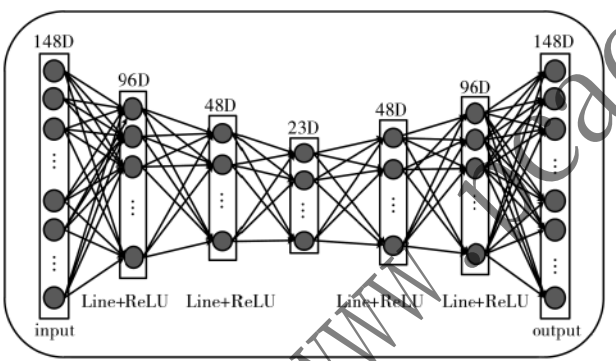


图 3　自动编码器模型

2.3 卷积神经网络模型

卷积神经网络[21]由于善于提取数据局部特征和下采样特性，相比其他机器学习模型更适合处理特征维度较高和具有空间特征的数据，如图像、文本和本文中使用的密文数据空间特征。不同结构的加密算法生成的密文文件在空间分布上存在信息差异性，这种空间信息差异性很难用传统机器学习算法分析，故本文使用卷积神经网络对密码算法展开识别研究。卷积神经网络识别模型如图 4 所示，以 16 KB 密文块为例，包括一个输入层、三个卷积+最大池化连接层、两个全连接层以及一个输出层，其中输入层为预处理过之后的灰度特征图。

基于卷积神经网络模型的识别方案，具体流程如下：

(1)训练阶段

①随机抽取密码算法已知的一组密文文件 C_1，C_2，…，C_s，其中 s 为文件个数；

②对每个密文文件 C_i 按固定大小分割为二进制密文块 C_{i1}，C_{i2}，…，C_{it}，其中 t 为密文块个数；

③对密文块 C_{ij} 数据内容进行特征提取，得到两组特征向量 $\mathbf{Afea}_{ij}$ 和 $\mathbf{Bfea}_{ij}$，对 $\mathbf{Bfea}_{ij}$ 特征降维，然后融合特征向量 $\mathbf{Afea}_{ij}$ 和 $\mathbf{Bfea}_{ij}$ 得到 $\mathbf{fea}_{ij}=\{\mathrm{fea}_{ij-1},\mathrm{fea}_{ij-2},\cdots,\mathrm{fea}_{ij-d}\}$，其中 d 为特征维数，其维数由具体选择的采集方式确定；

④每个密文文件组成一个大小为 $t\times d$ 的特征矩阵，转换为灰度特征图；

⑤s 个密文文件则构成 s 个灰度特征图且特征标签已知为 $\mathrm{Lab}=\{\mathrm{lab}_1,\mathrm{lab}_2,\cdots,\mathrm{lab}_s\}$，每个密文文件构成二元组$(\mathrm{fea}_i,\mathrm{lab}_i)$；

⑥将带标签的数据$(\mathrm{fea}_i,\mathrm{lab}_i)$提交到神经网络分类算法，进行分类模型的训练。

(2)测试阶段

①从网络设备或信息系统中获取密文文件。对一个待识别的密文文件 C 按固定大小分割为二进

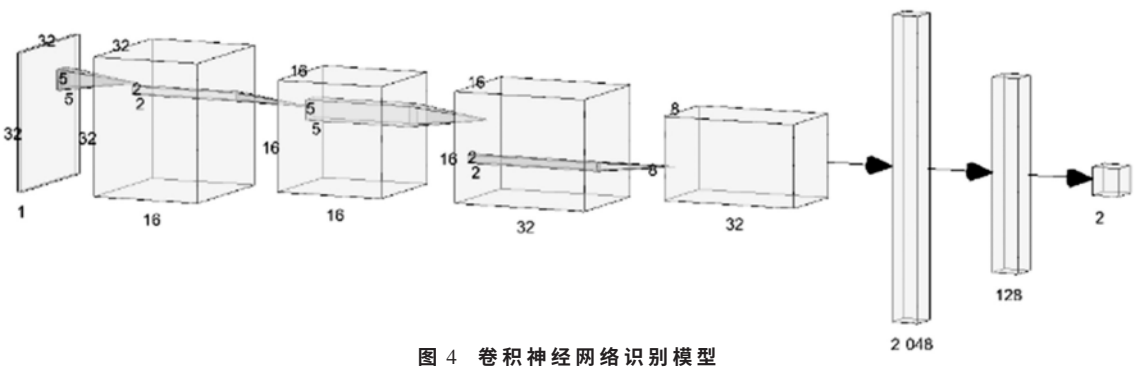


图 4　卷积神经网络识别模型

www.pcachina.com

制密文块，对每个密文块进行特征提取和特征降维，拼接每个密文块的特征向量 $\mathbf{fea}_i$，得到一个二维矩阵并转换为灰度特征图。

②将灰度特征图输入到在训练阶段训练好的分类器模型中，模型给出密码算法识别结果，即密码算法标签 lab。

3 实验结果与分析

本文实验使用 OpenSSL 和 GmSSL 密码库工具中实现的 SM4、AES、Camellia、DES 和 IDEA 密码算法加密明文文件，使用 NIST 随机性测试工具包提取密文特征，以 PyTorch 深度学习框架和 PyCharm 软件为模型训练环境，实验测试环境如表 1 所示。

表 1 实验测试环境

项目	描述
显卡	RTX A5000
内存	30 GB
CPU	AMD EPYC 7543 32-Core Processor
操作系统	Ubuntu
Python	3.8 版本
PyTorch	1.7.0 版本
PyCharm	Professional 2020.1 版本

明文数据来源于网上爬取的图片，将所有图片拼接成大小为1 024 MB 的明文文件，再将其平均分割为 2 000 份小文件，每份大小均为 512 KB。设置对应的固定密钥和分组密码 ECB 工作模式，每份小文件经过不同密码算法加密后获得对应的密文文件共计 10 000 份。对实验数据灰度特征图进行随机抽样训练，随机抽样 70%作为训练集，其余30%作为测试集，以 10 折重复随机抽样数据集的平均准确率作为识别效果的度量值。后续模型训练阶段和测试阶段都是在此基础上完成。有关各类密码算法的设置情况和实现方式如表 2 所示。

表 2 5 种加密算法的具体参数列表

密码算法	密钥长度/bit	分组长度/bit	密钥方式	加密结构	实现方式
SM4	128	128	固定	Feistel 网络	GmSSL
AES	128	128	固定	SP 网络	OpenSSL
Camellia	128	128	固定	Feistel 网络	OpenSSL
DES	56	64	固定	Feistel 网络	OpenSSL
IDEA	128	64	固定	Lai-Massey	OpenSSL

10 种随机性测试方法的参数设置对返回值 p_value 的大小和数量均有影响。表 3 为实验所用随机性测试方法的参数设置情况[22]，未说明实验取参均使用 NIST 随机性测试包默认设置。

为了验证密文块大小对实验效果是否有影响，本文采用两种密文分块方案，分别将密文文件划分为 32 块和 128 块，则密文文件大小为 16 KB 和 4 KB。对每种分块方案的密文块分别记为 C_{ij}^{32} 和 C_{ij}^{128}，密文文件提取特征生成 32×32 维和 128×128 维的特征灰度图。图 5 和图 6 所示分别为基于某种加密算法的 C_{ij}^{32} 和 C_{ij}^{128} 密文块方案的特征灰度图。

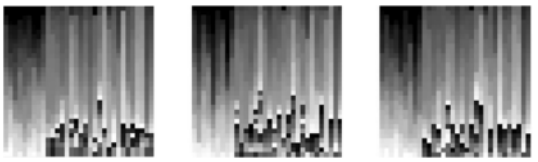
完成以上工作，将得到的特征灰度图输入到卷积神经网络模型中训练分类。首先将商密 SM4 算法与 AES、Camellia、DES、IDEA 算法之间两两区分识别，其准确率都在 80%以上，如表 4 所示。

根据实验结果可知，C_{ij}^{128} 密文分块方案的密码算法识别效果总体优于 C_{ij}^{32} 方案，且其中 SM4 算法

表 3 10 种随机性测试参数范围列表

随机性测试方法	参数要求	实验取参	返回值数量
频率测试	--	--	1
组内频率测试	$m>0.01n$(其中 $n=C_{ij}\times 8$ bit)	$m=128$	1
游程测试	--	--	1
最长 1 游程测试	--	--	1
二元矩阵秩测试	$n\geqslant 38MQ$	$M=Q=16$	1
离散傅里叶变换测试	--	--	1
序列测试	$m<\lfloor \log_2 n \rfloor -2$	$m=4$	1
近似熵测试	$m<\lfloor \log_2 n \rfloor -5$	$m=10$	1
累加和测试	--	--	1
非重叠模块匹配测试	$2\leqslant m\leqslant 10$	$m=9$	148

www.pcachina.com



(a)AES (b)DES (c)SM4

图 5 C_{ij}^{32} 密文块方案特征灰度图

(a)AES (b)DES (c)SM4

图 6 C_{ij}^{128} 密文块方案特征灰度图

表 4 SM4 与 4 种分组密码算法识别准确率

密码算法识别场景	密文块方案	准确率/%	随机分类/%
SM4 与 AES	C_{ij}^{128}	82.41	50
SM4 与 Camellia	C_{ij}^{128}	83.49	50
SM4 与 DES	C_{ij}^{128}	88.45	50
SM4 与 IDEA	C_{ij}^{128}	80.36	50
SM4 与 AES	C_{ij}^{32}	80.11	50
SM4 与 Camellia	C_{ij}^{32}	81.25	50
SM4 与 DES	C_{ij}^{32}	87.31	50
SM4 与 IDEA	C_{ij}^{32}	82.93	50

与 DES 算法识别准确率最高。为了进一步验证分组密码密钥长度是否对密码算法识别产生影响,本文还在 C_{ij}^{128} 密文分块方案的基础上对 DES 算法和其他算法两两识别。识别结果如表 5 所示。

表 5 DES 与 4 种分组密码算法识别准确率

密码算法识别场景	密文块方案	准确率/%	随机分类/%
DES 与 AES	C_{ij}^{128}	85.16	50
DES 与 Camellia	C_{ij}^{128}	86.41	50
DES 与 IDEA	C_{ij}^{128}	86.18	50
DES 与 SM4	C_{ij}^{128}	88.45	50

DES 算法与其他算法识别准确率均在 85%以上,具有较高的识别准确率,这说明密钥长度不同确实会影响密码算法之间识别的效果。研究识别的密码算法在密钥长度一致的基础上,与其他相关文献相比,本文提出的基于自动编码器和卷积神经网络的密码算法识别方案取得了不错的准确率和稳定性,对比结果如表 6 所示。

表 6 分组密码算法识别方案对比

识别方案	密钥长度是否一致	识别准确率/%
文献[6]	否	40~80
文献[14]	否	81~94
文献[23]	否	45~95
本文	是	80~89

4 结论

本文利用 NIST 随机性方法对密文文件提取整体和局部特征,使用自动编码器对数据降维,提出一种基于自动编码器和卷积神经网络模型的分组密码算法识别方案。所选密码算法在控制密钥长度这一变量的基础上开展研究,实验结果表明,密钥长度不同的两种分组密码算法,识别准确率相对较高,说明算法密钥长度不同对识别结果的准确率确实有影响。同时,SM4 与其他算法两两识别的准确率可达 80%之上,DES 与其他算法两两识别的准确率可达 85%之上。本文主要针对分组密码 ECB 工作模式进行识别研究,在后续的工作中,将尝试对 CBC、CFB 等复杂工作模式开展研究,对多种不同密钥长度的密码算法进行识别,优化密文特征选择和特征处理过程。同时,对国产商用序列密码体制和公钥密码体制识别展开研究。

参考文献

[1] 邓福彪.信息系统密码应用安全性评估与测评实践[J].福建电脑,2020,36(1):27-29.

[2] 李继中.基于相似性判定的密码算法识别技术研究[D].郑州:解放军信息工程大学,2009.

[3] 李继中.密码算法识别与分析关键技术研究[D].郑州:解放军信息工程大学,2014.

[4] 张经纬,舒辉,蒋烈辉,等.公钥密码算法识别技术研究[J].计算机工程与设计,2011,32(10):3243-3246,3273.

[5] POOJA M.Classification of ciphers[D].Kanpur:Indian Institute of Technology,2001.

[6] 吴杨,王韬,邢萌,等.基于密文随机性度量值分布特征的分组密码算法识别方案[J].通信学报,2015,36(4):147-155.

[7] 赵志诚,赵亚群,刘凤梅.基于随机性测试的分组

www.pcachina.com

密码体制识别方案[J].密码学报,2019,6(2):177-190.

[8] DILEEP A D,SEKHAR C C.Identification of block ciphers using support vector machines[C]//Proceedings of the 2006 IEEE International Joint Conference on Neural Network Proceedings,2006.

[9] 黄良韬,赵志诚,赵亚群.基于随机森林的密码体制分层识别方案[J].计算机学报,2018,41(2):382-399.

[10] 王旭,陈永乐,王庆生,等.结合特征选择与集成学习的密码体制识别方案[J].计算机工程,2021,47(1):139-145,153.

[11] SHARIF S O,KUNCHEVA L I,MANSOOR S P.Classifying encryption algorithms using pattern recognition techniques[C]//Proceedings of the 2010 IEEE International Conference on Information Theory and Information Security.IEEE,2010:1168-1172.

[12] MANJULA R,ANITHA R.Identification of encryption algorithm using decision tree[C]//Proceedings of the International Conference on Computer Science and Information Technology.Berlin:Springer,2011:237-246.

[13] CHOU J W,LIN S D,CHENG C M.On the effectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks[C]//Proceedings of the 5th ACM Workshop on Security and Artificial Intelligence,2012:105-110.

[14] ZHAO Z C,ZHAO Y Q,LIU F M.Research on Grain-128's cryptosystem recognition[C]//Proceedings of the 2018 IEEE 3rd Advanced Information Technology,Electronic and Automation Control Conference(IAEAC),2018.

[15] 纪文桃,李媛媛,秦宝东.基于随机性特征的SM4分组密码体制识别[J].计算机应用技术,2021,38(9):2821-2824,2830.

[16] 曹莉茹.基于深度学习的密码算法识别研究[D].成都:电子科技大学,2021.

[17] BENGIO Y.Learning deep architectures for AI[M].Now Publishers Inc.,2009.

[18] HINTON G E,SALAKHUTDINOV R R.Reducing the dimensionality of data with neural networks[J].Science,2006,313(5786):504-507.

[19] HASSAIRI S,EJBALI R,ZAIED M.A deep stacked wavelet auto-encoders to supervised feature extraction to pattern classification[J].Multimedia Tools and Applications,2018,77(5):5443-5459.

[20] 刘会芸,侯志平.基于自动编码器数据降维的滚动轴承故障诊断研究[J].现代制造工程,2022(1):148-153,160.

[21] KRIZHEVSKY A,SUTSKEVER I,HINTON G E.Imagenet classification with deep convolutional neural networks[C]//Advances in Neural Information Processing Systems,2012,2:1097-1105.

[22] RUKHIN A,SOTO J,NECHVATAL J,et al.A statistical test suite for random and pseudorandom number generators for cryptographic applications[Z].National Institute of Standards & Technology,2010.

[23] TAN C,JI Q.An approach to identifying cryptographic algorithm from ciphertext[C]//Proceedings of the 2016 8th IEEE International Conference on Communication Software and Networks(ICCSN),2016.

(收稿日期:2022-06-17)

作者简介:

刘节威(1998-),男,硕士研究生,主要研究方向:国产商用密码算法识别。

王钢(1971-),通信作者,男,硕士,正高级工程师,主要研究方向:网络与信息安全。E-mail:wg@imut.edu.cn。

颜培志(1981-),男,硕士,高级工程师,主要研究方向:网络安全、教育管理信息化。

www.pcachina.com

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com