基于形态学的电力系统弱口令深度学习检测方案

栗会峰[1] 李铁成[1] 姚启桂[3,4] 栗维勋[2] 杨立波[2] 孙广辉[2]

[1](国网河北省电力有限公司电力科学研究院 河北 石家庄 050021)

[2](国网河北省电力有限公司 河北 石家庄 050021)

[3](全球能源互联网研究院有限公司 江苏 南京 210003)

[4](信息网络安全国网重点实验室 江苏 南京 210003)

摘 要 在电力系统中,口令是身份认证的重要方式之一。传统的弱口令扫描方案主要针对口令长度、相同字母组合、口令与个人信息相关性等因素,未关注用户基于键盘坐标构成具有形态学特征的弱口令。将口令根据键盘位置转化为 28 × 28 的图像,并通过卷积神经网络学习口令的形态学特征,从而有效识别具有形态学特征的弱口令。该方案与基于 N-gram 马尔可夫链模型、卡巴斯基评测器这两种现有口令强度评估方法进行对比,具有更高的准确率和显著的识别精度,更能保障电力系统口令安全。

关键词 形态学弱口令 电力系统 卷积神经网络

中图分类号 TP309 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.10.055

A DEEP LEARNING DETECTION SCHEME FOR WEAK PASSWORD BASED ON MORPHOLOGY IN POWER SYSTEM

Li Huifeng[1] Li Tiecheng[1] Yao Qigui[3,4] Li Weixun[2] Yang Libo[2] Sun Guanghui[2]

[1](*State Grid Hebei Electric Power Research Institute*, *Shijiazhuang 050021*, *Hebei*, *China*)

[2](*State Grid Hebei Electric Power Co., Ltd.*, *Shijiazhuang 050021*, *Hebei*, *China*)

[3](*Global Energy Interconnection Research Institute Co., Ltd.*, *Nanjing 210003*, *Jiangsu*, *China*)

[4](*State Grid Key Laboratory of Information & Network Security*, *Nanjing 210003*, *Jiangsu*, *China*)

Abstract In power system, password is one of the important ways of authentication. The traditional weak password scanning scheme mainly focuses on the password length, the same letter combination, the correlation between password and personal information, but does not pay attention to the weak password with morphological characteristics based on keyboard coordinates. In this paper, the password was transformed into 28 × 28 image according to the position of the keyboard, and the morphological features of the password were learned by convolution neural network, so as to effectively identify the weak password with morphological characteristics. Compared with the existing password strength evaluation methods based on N-gram Markov model method and Kaspersky tester, this scheme has higher accuracy and significant recognition precision, which can guarantee the password security of power system.

Keywords Morphological weak password Power system Convolutional neural network

0 引 言

电力行业是国家重点行业,电力系统安全关乎国家社会安全。随着信息技术的快速发展,人们的生活不可避免使用大量口令注册邮箱、网上购物、网络游戏、电子银行、社交网络、电子商务等与金钱和日常生活挂钩的各种各样互联网服务。与此同时,随着电力系统信息化进程不断深入,生成运维方式不断网络化和数字化,大量储存在各个用户的数据信息被创建,身

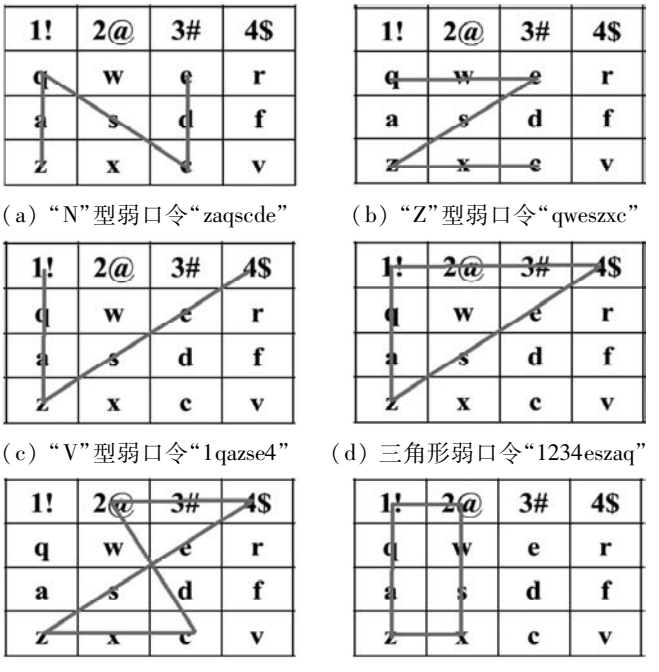
收稿日期:2021 - 04 - 12。国网河北省电力有限公司科技项目(kjcb2020-003)。**栗会峰**,工程师,主研领域:电力监控系统网络安全。**李铁成**,硕士。**姚启桂**,高工。**栗维勋**,硕士。**杨立波**,硕士。**孙广辉**,硕士。

份认证逐渐成为保障用户信息的基本手段。如何管理用户口令,给电力系统信息管理人员和终端用户带来了很大的挑战,其中弱口令的检测也尤为重要。不同的随机字符被认为是弱口令的构造中较为安全的方式,然而人类的大脑能力有限,为了方便记忆,人们常常会构造看似复杂的口令,造成大量根据键盘位置坐标构成的弱口令,而这些基于形态学的弱口令极易被暴力破解和字典攻击。

如果弱口令被内部或外部攻击者有效地利用,那么电力系统将面临巨大的安全风险。例如,2003 年 3 月 8 日,一种名为“口令蠕虫”[1]的网络蠕虫病毒通过系统的弱口令主动传播袭击我国互联网,从而导致了网络通信的明显拥塞。由于弱口令的薄弱性和脆弱性,该病毒极易攻击并猜测出用户口令,例如以连续数字 123456 或者有意义字母 love 所构成的脆弱口令。这次攻击表明,弱口令的管理和整改在越来越多的信息系统应用中需要得到加强。2014 年 1 月 21 日,全球互联网范围的 DNS 流量出现了故障,将近三分之二的网站出现了不同程度的故障,后经证实是通过感染家庭网关、摄像头、路由器等设备,对普遍存在的弱口令(均为系统默认口令)进行口令破解,成为恶意攻击者发起攻击的工具。因此弱口令是网络与信息安全中常见的安全问题,广泛存在于各种场合,且具有相当的危害性,检查系统中的弱口令,对弱口令进行加强管理和整改就成为整个安全电力系统建设中的重要环节。

近年来,口令研究逐渐成了一个热门的话题,研究人员提出了多种定向口令猜测攻击算法[2]。2016 年 7 月,Wang 等[3]提出了一种名为“TarGuess”的框架,该框架系统地描述了典型的目标猜测场景,设计 7 个完整的数学模型,每个模型都基于攻击者利用互联网定向获取用户个人信息中可用的各种数据,经过预处理、训练和猜测三个阶段,以最少尝试次数定向猜测用户的个人口令。通过 10 个真实密码数据集上进行的大量实验训练得到口令组合概率,从而凭借用户个人信息组合出猜测口令字典,尝试破解其他网站所有的用户口令,可以获得高达 73% 的成功率,表明了 TarGuess 的有效性。2016 年 7 月,Li 等[4]提出了概率无上下文无关文法(Probabilistic Context-Free Grammars,PCFG)。在本文中,首先从泄漏的数据集中剖析用户密码,以调查用户个人信息如何较大程度上驻留在密码中。提取最普遍使用的由个人信息组合的密码结构,并显示个人信息的使用情况,其结构包含用户名 A、邮箱前缀 E、姓名 N、生日 B、手机号 P 和身份证 G 这 6 大类。然后,引入了一个新的度量,称为覆盖率,以量化密码和个人信息之间的相关性。其次,扩展了 PCFG 方法,并提出 Personal-PCFG 通过生成个性化猜测来破解密码。本文通过离线和在线攻击场景,证明 Personal-PCFG 比 PCFG 破解密码快得多,使在线攻击更容易成功。

这些传统弱口令的扫描和识别主要针对口令与个人信息的相关性、口令随机性等因素[5],对于基于键盘坐标位置具有形态学特征的弱口令却不能有效检测。如图 1 所示,以部分键盘坐标为基础,构造出“N”型弱口令“zaqscde”,“Z”型弱口令“qweszxc”、“V”型弱口令“1qazse4”、三角形弱口令“1234eszaq”、沙漏型弱口令“234eszxcdw”、长方形弱口令“1qaz2wsx”。为此,本文通过分析提取弱口令的形态学特征,设计基于形态学的弱口令检测方案,根据键盘位置将口令转化为 28 ×28 的图像,基于神经网络模型有效检测传统方案无法检测的形态学弱口令,提升了弱口令检测的覆盖率,更好保护电力系统安全。



(a)“N”型弱口令“zaqscde” (b)“Z”型弱口令“qweszxc”

(c)“V”型弱口令“1qazse4” (d)三角形弱口令“1234eszaq”

(e)沙漏型弱口令“234eszxcdw” (f)长方形弱口令“1qaz2wsx”

图 1 六种形态学弱口令图形组成

1 方案提出

1.1 形态学特征弱口令及分析

弱口令的使用直接导致用户的不安全口令行为。随着信息技术的快速发展,信息化的进程在电力系统的管理中不断深入。此外,不同网站的口令管理策略往往有所差异,用户的精力有限,因此常常会设置方便记忆的口令。

表 1 给出包括 12306、Yahoo、Rockyou 在内的几个知名的真实口令数据集中最常用的口令前 10 名[6]。

表 1　各网站用户最常用口令统计

排名	12306	Rockyou	Yahoo
1	123456	123456	123456
2	a123456	12345	password
3	5201314	123456789	welcome
4	123456a	password	ninja
5	111111	iloveyou	abc123
6	Woaini1314	princess	123456789
7	123123	1234567	12345678
8	000000	rockyou	sunshine
9	qq123456	12345678	princess
10	1qaz2wsx	abc123	qwerty

可以看出,用户在设置口令时,除喜欢使用简单的数字、字母的组合(如 abc123),或有意义的单词、短语外(如 password),根据键盘上字符位置设置口令也占有很大比例,如 123456、1qaz2wsx、qwerty 等。这些通过对键盘上位置相邻的数字、字母、字符进行排列组合而生成的口令,区分于其他口令的形态学特征。

表 1 所展示的形态学弱口令安全性较低,很容易被破解,但是由于容易记忆,这种形态学弱口令构造方式一直被用户沿用,还有很多用户依照这种思路进行口令变形,这些口令统一称为形态学弱口令。

这些形态学弱口令极具有威胁性。对于攻击者而言,利用现有口令猜测技术[7-9],较为迅速地扩展弱口令字典,从而攻破用户口令。对于用户而言,由于这些口令貌似随机,让用户自认为是安全口令,产生麻痹。口令强度评估方法,如基于 N-gram 马尔可夫链方法、卡巴斯基评测器、Google 口令强度评估等,大多基于口令的随机性对口令强度进行评估,无法有效检测出具有形态学特征的弱口令,经常会有较大范围的错漏,甚至被评价为"好密码"。

本文使用两种主流方法评估具有形态学口令的强度,即基于 N-gram 马尔可夫链方法和卡巴斯基测评方法。

1.1.1　基于 N-gram 马尔可夫链方法

针对第一种方法,口令猜测攻击过程包括训练和测试两个阶段[10-11]。首先需要统计序列长度为 N 的项目(item)的每个子串之后紧跟着的字符的频数。以口令 China11 为例,在四阶 Markov 模型中,它的项目(items)依次为"＊＊＊C, ＊＊Ch, ＊Chi, Chin, hina, ina1, na11"[12],需要统计的值为:首字符是 C 的频数,C 后是 h 的频数,Ch 后是 i 的频数,Chi 后是 n 的频数,Chin 后是 a 的频数,hina 后是 1 的频数,ina1 后是 1 的频数。根据上述方式,指定口令的概率等于所有的概率值的乘积。在测试阶段,根据式(1),将计算得到的口令概率按照降序的方式组成口令猜想集。最终,在测试阶段,测试猜测集中的口令便可以评估口令破解的难易程度,如式(2)[13-14]所示。以弱口令"nhy65tgBVfr $"为例,按照式(1),计算得到口令概率 P(nhy65tgBVfr $) = 6.33×10^{-11}。根据式(2),计算口令强度为 33.88。按照上述方法,分别对于基于形态学弱口令和非形态学口令这两种口令计算得到口令强度,如表 2 所示。我们可以看到,形态学口令如"3rgnhy6tfcde"的强度高于其他随机生成的口令。

$$P(c_i \mid c_{i-n+1}, c_{i-n+2}, \cdots, c_{i-1}) = \frac{\mathrm{count}(c_{i-n+1}, c_{i-n+2}, \cdots, c_i)}{\mathrm{count}(c_{i-n+1}, c_{i-n+2}, \cdots, c_{i-1})} \tag{1}$$

$$f(c) = -\log_2(P(x)) \tag{2}$$

表 2　基于 N-gram 马尔可夫链方法评估口令强度

口令	口令	口令类型	口令强度
形态学弱口令	nhy65tgBVfr $	长方形	33.88
	1qaz2wsx3edc	长方形	35.50
	3rgnhy6tfcde	沙漏型	41.50
其他口令	{j = hsb8	随机型	24.05
	＊ywu\l	随机型	26.50
	94ahdb＊u	随机型	33.58

1.1.2　卡巴斯基评测器

第二种方法则是直接通过在卡巴斯基网站输入口令,该网站[15]可以将输入的密码与泄露账户数据库进行匹配,实现自动安全认证。此方法的解决方案之一为 Have I Been Pwned。Have I Been Pwned 由知名网络安全专家 Troy Hunt 创建,近年来已经成为检查口令和用户是否泄露的实际行业标准,是世界上最全面且定期更新的泄露账户集合之一。例如,口令"^&＊90yuioP"通过卡巴斯基网站检测为好密码,如图 2 所示,但是实际上却是长方形的形态学弱口令。

图 2　卡巴斯基网站检测结果

对于这些具有形态学特征的弱口令,却被现有方法判断为非弱口令,错误率很高,这为口令安全带来了极大威胁。本文针对现有口令强度评估方法无法有效检测具有形态学特征的弱口令的问题,提出一种新颖的基于形态学特征的深度学习弱口令检测方案。该方案不同于现有基于随机性或规则的口令强度评估方法,而是根据键盘位置将口令转化为 28 ×28 的图像,并通过卷积神经网络学习口令的形态学特征,从而有效识别具有形态学特征的弱口令,进一步提升弱口令扫描方案的安全性。

1.2 方案设计

形态学弱口令检测方案共包括三个模块:图像预处理模块、形态学弱口令检测模块和口令强度分析与评估模块。形态学弱口令检测方案设计如图 3 所示。

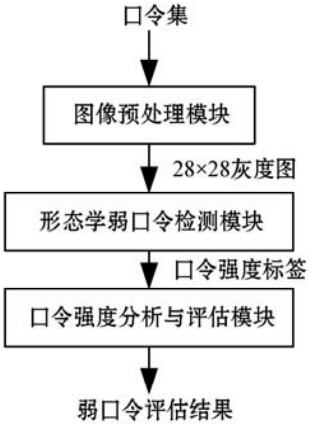


图 3 形态学弱口令检测方案设计

图像预处理模块将口令从文本形态转换为图像形态,通过图像识别的深度学习方法捕捉口令的形态学特征,从而有效检测传统方法无法识别的形态学弱口令。本文将口令转换为 28 ×28 大小的灰度图,该图像可如实反映口令的形态学特征,即口令在键盘上的位置分布信息。得到的 28 ×28 大小的口令灰度图作为形态学弱口令识别模块的输入。

形态学弱口令检测模块是一个具有两层卷积层、一层全连接层和一层 softmax 层的卷积神经网络,它参考手写数字识别网络设计,能有效学习输入的口令图像的形态学特征,准确区分形态学弱口令和其他口令,并将分类结果输出。

口令强度评估与分析模块对检测结果进行分析,确定具有形态学特征的弱口令,并将评估结果与其他口令强度评估方法比较。

下面将对图像预处理模块和形态学弱口令检测模块的功能和设计进行具体描述。

1.2.1 图像预处理

图像预处理模块对口令集进行图像化处理,将口令转化为 28 ×28 大小的灰度图像,该图像可如实反映口令的形态学特征,以便弱口令检测深度学习模型学习。

为将口令的形态学特征可视化,本文定义 4 ×13 大小的口令矩阵 $\boldsymbol{A}$,$\boldsymbol{A}$ 中元素的分布与普通英文键盘上各字符的分布一致,如图 4 所示。

y / x	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1!	2@	3#	4$	5%	6^	7&	8*	9(	0)	-_	=+	
2	q	w	e	r	t	y	u	i	o	p	[{	]}	|
3	a	s	d	f	g	h	j	k	l	;:	'"		
4	z	x	c	v	b	n	m	,<	.>	/?			

图 4 口令矩阵 $\boldsymbol{A}$

对于口令 P,论文做如下处理:依次找到 P 中各个字符在矩阵 $\boldsymbol{A}$ 中的对应位置,并改变该位置的元素值,从而在矩阵中进行标记。将矩阵中各元素位置表示为二维坐标的形式(x,y),如,对于形态学弱口令“1qaz2wsx”,其在矩阵中的分别对应位置坐标为(1,1)、(2,1)、(3,1)、(4,1)、(1,2)、(2,2)、(3,2)、(4,2),图像化后为长方形,再如,弱口令“1234eszxcv”,其在矩阵中的分别对应位置坐标为(1,1)、(1,2)、(1,3)、(1,4)、(2,3)、(3,2)、(4,1),图像化后为“Z”形。表 3 列举了六种典型形态学弱口令对应的形状和位置坐标。

表 3 六种典型形态学弱口令对应的形状和位置坐标

序号	弱口令	形状	位置坐标
1	! qaz2wsX	长方形	(1,1) (2,1) (3,1) (4,1) (1,2) (2,2) (3,2) (4,2)
2	1qazwd4rfv	“Z”型	(1,1) (2,1) (3,1) (4,1) (2,2) (3,3) (1,4) (2,4) (3,4) (4,4)
3	1qazxcvdw	三角形	(1,1) (2,1) (3,1) (4,1) (4,2) (4,3) (4,4) (3,3) (2,2)
4	1234eszxcv	“Z”型	(1,1) (1,2) (1,3) (1,4) (2,3) (3,2) (4,1) (4,2) (4,3) (4,4)
5	4567rtyu	长方形	(1,4) (1,5) (1,6) (1,7) (2,4) (2,5) (2,6) (2,7)
6	qwerty	直线	(2,1) (2,2) (2,3) (2,4) (2,5) (2,6)

然后,将各个位置元素默认值为 255,在灰度图中显示为白色,若口令 P 中字符在矩阵 $\boldsymbol{A}$ 中对应位置出现,则将该位置的元素值设为 0 或 125,其中:0 表示未使用上档键的字符,125 表示使用上档键的字符。经过处理后,每个口令 P 都可表示为 4 ×13 的矩阵,矩阵中各元素的取值共有 0、125、255 三种情况,并以灰度图的形式保存。为使生成的口令图像符合弱口令检测网络输入标准,图像边缘位置使用 255 填充,得到 28 ×28 大小的灰度图像,如图 5 所示,图 5 中口令表

现出明显的形态学特征,如长方形、“N”型、“Z”型、三角形等。为展示图像的灰度效果,对生成的口令进行归一化处理,即原始生成的口令图像范围(0~255)归一化到了(0~1),图 5 如实反映了口令在键盘上的位置关系和是否使用上档键。例如,口令“!qaz2wsX”的第一个字符“!”在坐标位置(1,1)值为 1 上使用了上档键,相对于未使用上档键的字符颜色更浅,为灰色。最后,经过预处理后的口令图像作为弱口令识别模块的输入进行学习。

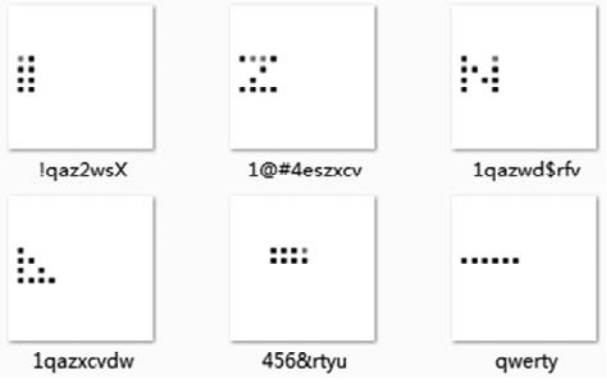


图 5　具有形态学特征的弱口令及对应灰度图像

1.2.2　形态学弱口令检测模型架构

考虑到具有形态学特征的弱口令在视觉上具有与手写数字相似的特征,因此,本文参考手写数字识别网络设计弱口令识别卷积网络模型,如图 6 所示。

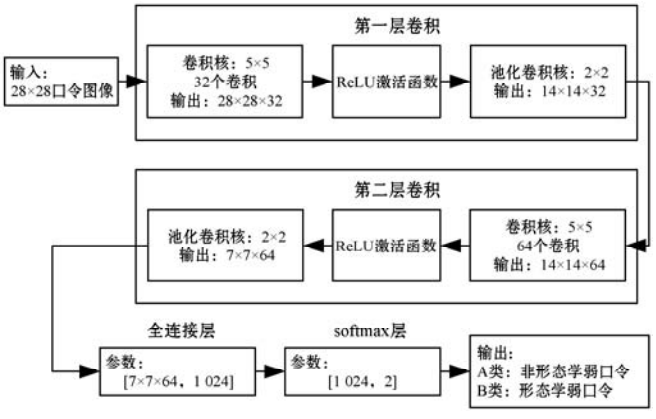


图 6　形态学弱口令检测模型架构

该模型的输入为 28×28 大小的口令灰度图,由图像预处理模块生成。模型包括两个卷积层、一个全连接层和一个 softmax 层,卷积核大小均为 5×5。

第一层卷积层包括 32 个卷积,本方案选择卷积模式为“SAME”,因此,传输过程中特征图的大小与原输入一致。卷积核卷积滑动步长设置为 1,最终,输出图像大小保持不变为 28×28。每个卷积核提取一个特征,本方案采用了 32 个卷积核,最终提取出 32 个特征。因此第一层卷积的输出是 28×28×32。其次,采用 ReLU 激活函数,以提升模型的收敛速度,并添加一个 2×2 的池化层,以更好地保证图像的特征。池化层选择最大池化方式,本方案选择的 2×2 池化核计算图像 2×2 区域上的某个特定特征的最大值,因此,本实验 28×28 的输入经过 2×2 池化后就变成了 14×14。本次特征提取阶段不仅具有更低的维度减少参数,同时防止过拟合现象。

第二个卷积层包括 64 个卷积、ReLU 激活函数、2×2 最大池化。第二层卷积层输出 7×7×64 维的数据。通过全连接层转化为 1 024 维的向量,即将 7×7×64 的三位数组转化成大小 1 024。最后通过 softmax 层输出 2 维的口令强度标签,分别代表形态学弱口令和无形态学特征口令,以便对形态学弱口令进行判别。

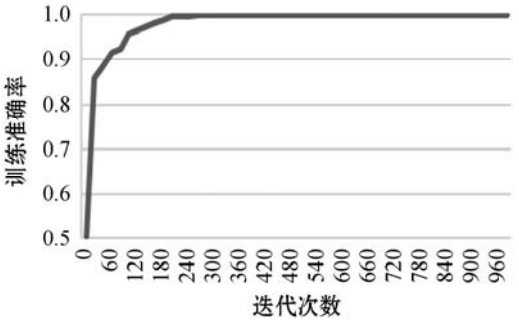
2　实验过程及性能比较

2.1　数据集和实验设置

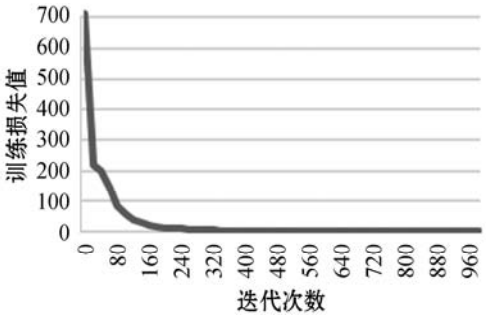
实验数据集主要基于 rockyou 口令数据集生成,包含 10 000 条常用口令,为国外社交网站 www.rockyou.com 泄漏,该数据集为口令强度评估提供了很好的支撑。

本方案采取的数据库划分为两组进行实验。分别设置为 A、B 两类口令图像数据集。A 类包含 300 幅其他类型的口令图像;B 类包含 300 幅具备形态学特征的口令图像,均已经经过预处理模块规范化为 28×28 的灰度图,训练集和测试集随机划分,比例为 7∶3。

实验模型基于 TensorFlow 平台搭建,模型训练时初始化过滤器,标准差为 0.1,初始化偏置为 0.1。为增强泛化能力,在输出层之间加入 dropout。使用 cross-entropy 损失函数加快学习速度,使用 Adam 优化算法调整学习率。图 7 展示的是本方案模型训练过程中准确率变化曲线和损失值变化曲线。此训练过程中,准确率不断上升,迭代到 240 次时,准确率维持在 99.70% 左右,接近于 1。总训练次数为 1 000,此时准确率达到 99.76%。损失值总体呈下降趋势,迭代到 300,损失值下降到 5.65,之后保持稳定下降趋势。最终迭代到 1 000 次时,损失值到 1.70。



(a) 准确率变化曲线



(b) 损失值变化曲线

图 7 模型训练过程

2.2 性能分析和比较

为了分析本方案的性能,实验针对 90 条形态学弱口令和 90 条无形态学特征口令进行检测,比较本文提出的弱口令检测方法(形态学)和基于 N-gram 马尔可夫链口令评估方法、卡巴斯基评测器的检测准确率,图 8 是基于 N-gram 马尔可夫链口令评估方法检测口令强度,同时反映了形态学口令和其他口令的口令强度变化曲线。首先我们可以看出,当形态学弱口令(实线)较低时,强度分别为 9.58、12.89、13.84,计算得到平均值为 12.10。随着长度增加到 12 时,口令强度迅速增加为 32.55、33.89、41.5,平均值达到 35.98,口令强度明显增加。与此同时,其他弱口令的检测强度结果随着口令长度的增加呈上升趋势。除此之外,我们还可以观察到当口令长度较长时,形态学弱口令的强度明显高于其他口令。说明此强度检测方案重点关注口令强度的长短,口令强度随着口令长度的增加而增加,并未关注口令本身的特性,不能精确识别出形态学弱口令,对弱口令扫描带来安全隐患。

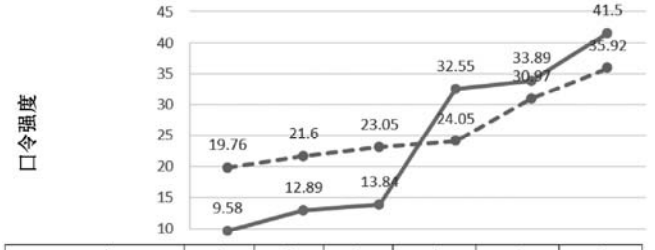
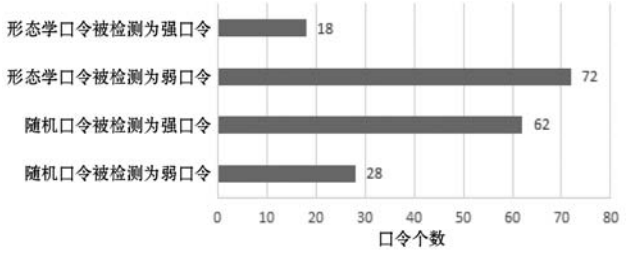


图 8 基于 N-gram 马尔可夫链口令评估方法检测口令强度变化曲线

本文还基于卡巴斯基测评器识别上述 90 条形态学弱口令和 90 条非形态学弱口令,检测结果如图 9 所示。形态学弱口令被检测为弱口令的个数高达 72 个,占口令总数 40%。此方法的准确率为形态学弱口令被检测为弱口令的个数以及随机口令检测为强口令的个数总和与口令总数的占比。计算准确率为 $P=\frac{62+72}{90+90}=74.44\%$。



系列	随机口令被检测为弱口令	随机口令被检测为强口令	形态学口令被检测为弱口令	形态学口令被检测为强口令
系列1	28	62	72	18

图 9 卡巴斯基评测器判别口令类型

将本文提出的形态学弱口令检测方法和基于 N-gram 马尔可夫链口令评估方法、卡巴斯基评测器的检测准确率作对比,由表 4 可知,本文方法对于形态学弱口令有很好的检测效果,准确率达到 99.45%,马尔可夫链方法的准确率为 86.25%[13-14],卡巴斯基测评器准确率为 74.44%。因此,相比现有弱口令检测方法,本文方案基于形态学的弱口令深度学习检测方案具有明显的优势。而现有弱口令检测方法无法有效检测识别出形态学弱口令。

表 4 形态学特征弱口令检测准确率(%)

检测方案	马尔可夫链方法	卡巴斯基评测器	形态学检测方法
准确率	86.25	74.44	97.78

本文方案主要针对具有形态学特征的弱口令进行检测,对于不具有形态学特征的弱口令,可结合其他口令强度评估方法共同分析,实现更完善的弱口令检测。

3 结 语

口令安全是电力系统安全的重要组成部分,弱口令的整改对维护电力系统安全有重要意义。传统口令强度评估方法无法准确识别看似复杂而具有随机性形态学弱口令,这些弱口令在键盘坐标上构成特定的图形形状,例如“Z”型、“V”型、长方形等,为口令安全带来隐患。本文提出的基于形态学特征的弱口令深度学习检测方案,参考手写数字识别网络,重点针对形态学口令构成的 28×28 的图形进行分析研究,实验结果显示本方案的检测准确率达到 99.45%。与此同时,主流检测方法包括基于 N-gram 马尔可夫链口令评估方法、卡巴斯基评测器并不能精确高效识别形态学弱口令,进而证明本方案是切实可行的,可有效检测出具有形态学特征的弱口令,弥补现有弱口令检测方案的不足。接下来,将本方案的研究成果与现有其他弱口令

扫描方案相结合,应用于电力系统,实现更精确更全面的弱口令检测。

参 考 文 献

[1] Sukhram D, Hayajneh T. KeyStroke logs: Are strong passwords enough? [C]//2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference,2017:619 - 625.

[2] 沈瑛,廖刘承,董天阳. 口令强度评估的分级先验模型研究[J]. 计算机科学,2015,42(11):222 - 227.

[3] Wang D, Zhang Z, Wang P, et al. Targeted online password guessing: An underestimated threat [C]//ACM SIGSAC Conference on Computer and Communications Security,2016: 1242 - 1254.

[4] Li Y, Wang H, Sun K. A study of personal information in human-chosen passwords and its security implications[C]// IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications,2016.

[5] Glory F Z, Aftab A U, Tremblay-Savard O, et al. Strong password generation based on user inputs[C]//2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),2019.

[6] 王平,汪定,黄欣沂. 口令安全研究进展[J]. 计算机研究与发展,2016,53(10):2172 - 2187.

[7] Zhang S, Zeng J, Zhang Z. Password guessing time based on guessing entropy and long-tailed password distribution in the large-scale password dataset[C]//2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID),2017.

[8] Guan A, Chen C M. A novel verification scheme for resisting password guessing attacks[C]//2021 IEEE Conference on Dependable and Secure Computing (DSC),2021.

[9] Kanta A, Coisel I, Scanlon M. Smarter password guessing techniques leveraging contextual information and OSINT [C]//2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),2020.

[10] Castelluccia C, Durmuth M, Perito D. Adaptive password-strength meters from Markov models[C]//Network and Distributed System Security Symposium,2012.

[11] 赵琦. 基于 n-gram 模型的中文分词技术研究[D]. 天津:南开大学,2007.

[12] 周环,刘奇旭,崔翔,等. 基于神经网络的定向口令猜测研究[J]. 信息安全科学报,2018,3(5):25 - 37.

[13] Doddington G. Automatic evaluation of machine translation quality using N-gram co-occurrence statistics[C]//2nd International Conference on Human Language Technology Research,2002:138 - 145.

[14] Adewumi S. E, Abdu H. Analysis of N-gram[C]//2nd International Conference on Computer and Information Sciences (ICCIS),2020.

[15] Kaspercky Password Checker. How can I be sure it's safe? [EB/OL]. [2021 - 03 - 15]. https://password. kaspersky. com/.

(上接第 341 页)

[5] 冯登国,吴文玲. 分组密码的设计与分析[M]. 北京:清华大学出版社,2000.

[6] Jakimoski G, Kocarev L. Chaos and cryptography: Block encryption ciphers based on chaotic maps[J]. Ieee transactions on circuits and systems i: fundamental theory and applications, 2001, 48(2): 163 - 169.

[7] Lu Q, Zhu C, Deng X. An efficient image encryption scheme based on the LSS chaotic map and single S-box[J]. IEEE Access, 2020, 8: 25664 - 25678.

[8] 韩妍妍,何彦茹,刘培鹤,等. 一种基于混沌系统的 ZUC 动态 S 盒构造及应用方案[J]. 计算机研究与发展,2020, 57(10):2147 - 2157.

[9] 吕鑫,慕晓冬,张钧,等. 混沌麻雀搜索优化算法[J]. 北京航空航天大学学报,2021,47(8):1712 - 1720.

[10] Ge R, Zhang L, Zhang T, et al. A modified spiking neuron circuit with memory threshold and its application in image encryption[C]//2015 International Conference on Software Engineering and Srevices. IEEE, 2015.

[11] 王光义,袁方. 级联混沌及其动力学特性研究[J]. 物理学报, 2013,62(2):111 - 120.

[12] Chen H, Feng D. An effective evolutionary strategy for bijective S-boxes [C]//Proceedings of the 2004 Congress on Evolutionary Computation . IEEE, 2004.

[13] Çavuşoğlu Ü, Zengin A, Pehlivan I, et al. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system[J]. Nonlinear Dynamics, 2017, 87(2): 1081 - 1094.

[14] Hussain I, Shah T, Mahmood H. A new algorithm to construct secure keys for AES[J]. International Journal of Contemporary Mathematical Sciences, 2010,5(26):1263 - 1270.

[15] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International journal of bifurcation and chaos, 2006, 16(8): 2129 - 2151.

[16] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3D chaotic baker maps[J]. International Journal of Bifurcation and chaos, 2004, 14(10): 3613 - 3624.

[17] Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21(3): 749 - 761.