基于卷积神经网络的车载数字孪生持续认证方案

赖成喆[1]，张鑫伟[1]，李冠颉[2]，郑东[1]
（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；
2. 西安电子科技大学网络与信息安全学院，陕西 西安 710126）

摘 要：为了解决无人驾驶通信过程中存在的车辆身份合法性问题，提出了一种基于卷积神经网络（CNN）的车载数字孪生持续认证方案进行车辆身份合法性验证。具体来说，数字孪生获取车辆传感器收集的数据，用于训练部署在数字孪生上的 CNN，然后执行主成分分析为分类器选择合适的典型特征。利用 CNN 提取的特征，在注册阶段训练一类支持向量机（OC-SVM）分类器，在认证阶段进行数据分类，进而将当前车辆验证为合法或者恶意车辆。仿真结果表明，所提方案在性能和准确率方面优势突出并优于现有方案。

关键词：无人驾驶；车载数字孪生；卷积神经网络；持续认证；分类器
中图分类号：TN92
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023229

CNN-based continuous authentication scheme for vehicular digital twin

LAI Chengzhe[1], ZHANG Xinwei[1], LI Guanjie[2], ZHENG Dong[1]
1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
2. School of Cyber Engineering, Xidian University, Xi'an 710126, China

Abstract: To address vehicle identity legitimacy verification issues, a continuous authentication scheme for vehicular digital twin based on convolutional neural network (CNN) was proposed. Specifically, the digital twin was used to acquire the data collected by the vehicle sensors for training the CNN deployed on the digital twin. Then, principal component analysis was performed to select appropriate typical features for the classifier. Using the features extracted by the CNN, the one-class support vector machine (OC-SVM) classifier was trained in the registration phase and the data was classified in the authentication phase, which consequently verified the current vehicle as a legitimate or malicious vehicle. Simulation results show that the proposed scheme has outstanding advantages and outperforms the existing schemes in terms of performance and accuracy.

Keywords: autonomous vehicle, vehicular digital twin, convolutional neural network, continuous authentication, classifier

0 引言

在移动通信技术的支持下，未来车联网应用将会向协同化和智能化方向发展，为无人驾驶车辆提供安全可信的认证服务至关重要。然而，传统的认证方案在支持车路协同通信时面临一系列新挑战。传统认证技术只能在接入网络时执行身份认证，无法确保在后续的通信过程中持续对用户和设备进行可信验证[1-3]。由于无人驾驶场景对安全性的要求极为苛刻，因此需要进一步研究更安全可靠的认证技术。

收稿日期：2023−07−05；**修回日期：**2023−09−13
通信作者：赖成喆，lcz_xupt@163.com
基金项目：国家自然科学基金资助项目（No.61872293，No.62072371）；陕西省重点研发计划基金资助项目（No.2021ZDLGY06-02）；陕西高校青年创新团队基金资助项目
Foundation Items: The National Natural Science Foundation of China (No.61872293, No.62072371), The Key Research and Development Program of Shaanxi Province (No.2021ZDLGY06-02), The Youth Innovation Team of Shaanxi Universities Foundation

随着人工智能（AI）技术的飞速发展，数字孪生（DT, digital twin）在学术界受到了广泛关注。数字孪生是一种多部署在云端、可以与物理环境协助互通的镜像数字系统，为物理环境活动的监控开辟了新的道路[4]。数字孪生不仅可以进行海量数据的存储和传输，还在云端维护了一个自主应用。数字孪生中的数字代表（DR, digital representative）可以对云上的数据进行清洗、融合、分析处理等，进而能够分析和预测物理实体（PE, physical entity）的活动并做出最优决策[5]。数字孪生的出现为具有传感、计算和通信功能的车辆之间的信息交互提高了效率，并且能够为驾驶员提供预警并规避潜在驾驶风险。在车载数字孪生中，车载传感器等设备将收集到的车辆数据上传到云端，云服务提供商根据收到的数据进行数字孪生系统的创建，数字孪生在云上构建镜像车联网系统。然后，云服务提供商利用云端强大的计算能力，在数字孪生上运行镜像系统，帮助物理环境中的车辆进行最优决策的选择。

利用数字孪生技术，有望实现对车辆身份的持续认证（CA, continuous authentication），即在会话期间对车辆行为活动进行高频率的监视，并持续确定该车辆是否为合法车辆，当确定为恶意车辆时，建立适当的防御机制；数字孪生能够存储并处理海量数据的特点可以满足持续认证的工作方式，因此可以利用数字孪生对车辆进行持续认证，确保车辆身份在会话期间的合法性。

因此，利用数字孪生技术，结合持续认证的思想[6]，设计面向无人驾驶车辆的持续认证方案，同时与传统认证技术有效结合是本文工作的出发点。

作为实现持续认证的关键技术，深度学习尤其是卷积神经网络（CNN, convolutional neural network）在语音、签名、步态和按键的识别等方面表现出了广泛的优势，基于移动感知的活动模式的连续身份验证深度学习方法[7]引入了一种新的连续身份验证框架，该框架根据传感器来测量身体活动模式并识别用户以保证智能手机的数据安全；基于深度学习的持续身份验证用于支持物联网的医疗保健服务[8]提出了一种将用户的行为特征与各种数据增强技术一起使用的持续认证安全框架，该框架通过使用基于长短期记忆深度学习的分类模型来识别攻击者的非法行为。根据现有研究，利用深度学习能够提取更加鲁棒和高辨识度的特征，进而实现对用户身份的持续性认证。

与现有的传统认证方法不同，本文旨在提供一种基于卷积神经网络用于车载数字孪生的持续认证方案，以解决传统车辆认证在网络环境不佳的情况下认证延迟或认证失败的情况。本文基于 shuffleNetV2 结构[9]，设计了一种结合数字孪生及改进的 CNN 的持续认证方案。

本文的主要贡献总结如下。

1) 提出基于 CNN 的车载数字孪生持续认证方案，根据车辆的加速度计、陀螺仪和磁强计收集的传感器数据利用部署在数字孪生上的 CNN 进行持续身份认证。该方案由数据收集、数据预处理、CNN 训练及特征提取、分类器的训练和身份认证五部分组成。

2) 将预处理完成的原始传感器数据用于 CNN 的训练，并根据 shuffleNetV2 结构设计了一个基于基本单元和空间下采样基本单元的 CNN 来学习和提取车辆传感器数据中的特征数据。

3) 仿真结果表明，本文所设计模型的测试损失（Test Loss）和测试准确率（Test Acc）在学习过程中逐渐提高，并且在一定周期后趋于稳定，这表明模型具有一定的泛化能力；所设计模型展现出了比 GoogLeNet 和 DenseNet 更好的性能，实现了更高的准确率。

1 相关工作

本节回顾了持续身份验证中深度学习的最新进展。持续认证是一种通过不断监测和验证用户身份的方法，以确保方案或应用程序在用户会话期间保持安全。传统的身份认证方法，如密码、指纹或面部识别，通常只在用户登录时进行一次认证。然而，这种静态的认证方式存在一些局限性，如用户可以在认证后将设备交给他人使用，或者在认证后自身行为发生变化。如今越来越多智能设备引入机器学习和人工智能来解决传统认证过程中存在的问题和不足。

文献[10]提出了一种基于 AI 的、保护隐私的多设备连续身份验证架构。该架构结合用户与不同设备之间的交互，使用机器学习和深度学习分类器分析了时间对身份验证准确性的影响并通过多设备生成合法配置文件，对单一设备的结果进行了改进。James 等[11]提出了一种通过深度强化学习技术使用高斯加权柯西克里金法的连续 Czekanowski 方法，可对移动设备进行隐式连续身份验证。方案中应用高斯加权非局部均值滤波器预处理模型来降

低原始输入人脸图像中存在的噪声；采用柯西克里金回归函数来降低维数。最后，连续 Czekanowski 分类用于在真实用户和攻击者之间进行熟练的分类。Abuhamad 等[12]提出了一种利用深度学习来主动验证身份的模型，该模型基于深度学习，在用户与智能手机交互或不交互的情况下，根据传感器识别用户的不同行为。Naji 等[13]设计了一个基于 MobileNetV2 的双输入模型来保护移动设备上的敏感数据，使用 2 个公共数据集 BioIdent 和 HMOG，利用滑动手势的图像作为输入，对用户进行连续的身份认证。Chauhan 等[14]提出了一个基于行为的用户认证的持续学习框架，通过融合深度学习模型和在线学习模型来实现动态学习，进而实现会话过程中随着时间的推移认证准确性的下降。Wu 等[15]利用基于 CNN 的特征学习提取独特的触摸特征，通过为被认证为合法用户的行为建模，防止冒名顶替者的攻击。

与上述工作的不同之处在于，本文在车载数字孪生中利用 shuffleNetV2 结构设计了一个二维卷积网络，以提取持续认证系统中的判别车辆行为特征。这有效降低了车载数字孪生的认证开销，对比传统车辆认证方式和持续认证方式，车辆不再被多次要求进行初始认证。持续认证更加便捷，认证频率更高。

2　车载数字孪生系统模型

典型的数字孪生通信系统分为孪生内通信和孪生间通信两部分[16-17]，如图 1 所示。下面详细介绍这 2 种通信模式。

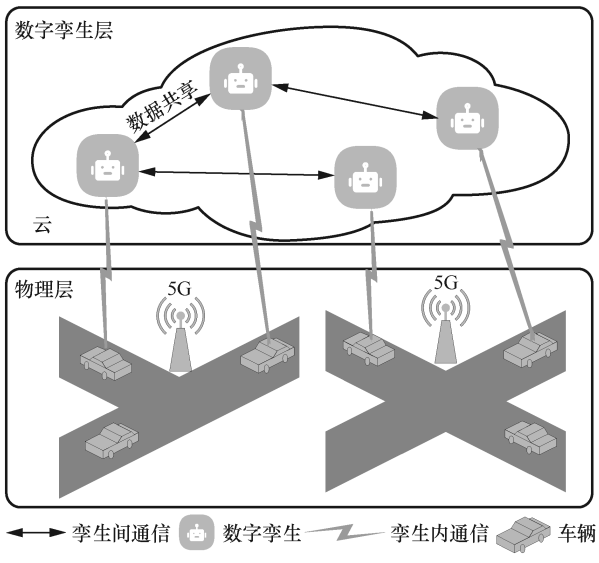


图 1　典型的数字孪生通信系统

1) 孪生内通信

车辆和其云上的镜像数字代表之间的通信称为孪生内通信，包括原始数据传输和处理后的数据传输。其中，原始数据是指从车辆流向数字代表的不同传感器采集到的数据，处理后的数据是指数字代表产生并发送到车辆的分析结果。值得注意的是，车辆与其数字代表之间的链接必须是私有并且完全受保护的，以便在数字代表中共享数据或 AI 模型。车辆和数字代表之间的孪生内通信组成了系统的完整内环，可以在数字孪生内实现有效的仿真、预测和反馈。例如，车辆通过无线通信将车载传感器收集到的数据上传至数字孪生中车辆专有的数字代表。同时，部署在云上的数字代表可以通过孪生内通信将其在云端收集的有效数据传输给车辆，进而帮助车辆在现实中完成决策。孪生内通信具有一致性、实时性、隐私性和专用性等特点。

2) 孪生间通信

孪生间通信主要指的是数字孪生中云端上各个车辆专有数字代表之间的相互通信。云上的数字代表之间可以进行共享信息，并通过专有链路向车辆反馈信息。由此，车辆可以通过其云端上专有的数字代表实现通信中继，与自身通信范围之外的其他车辆进行间接的信息交互，从而帮助车辆在行驶过程中获得更多有意义的路网信息。孪生间通信具有分布式点对点连接、数据私有、多通信代理等特点。

本文主要使用孪生内通信进行数据的传输，车辆的加速度计、陀螺仪和磁强计收集车辆数据，通过孪生内通信利用车辆和数字孪生的私有链路将收集到的原始传感器数据传输给数字孪生，用于 CNN 的训练等活动。

3　车载数字孪生持续认证方案设计

3.1　方案总体描述

本节将介绍基于 CNN 的车载数字孪生持续认证方案的基本架构，这是一个基于 CNN 的持续身份认证方案，使用车载传感器进行数据的收集并传输到数字孪生。方案总体架构如图 2 所示，基于 CNN 的车载数字孪生持续认证方案由 2 个阶段组成。

1) 注册阶段

通过使用训练数据使部署在数字孪生上的 CNN 学习合法用户的特征数据；经过主成分分析（PCA, principle component analysis）选取的具有高辨识度的数据对分类器进行训练，学习并生成合法

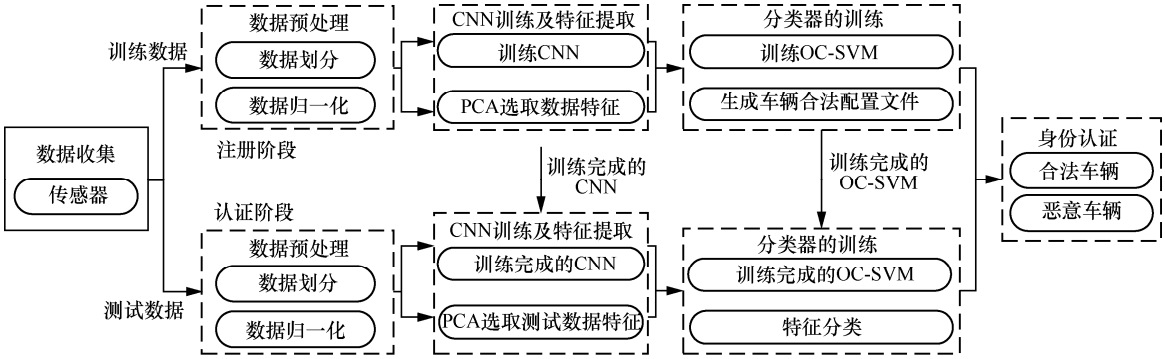


图 2 方案总体架构

车辆的配置文件。

2) 认证阶段

通过利用训练完成的 CNN 来对测试数据进行特征提取；经过主成分分析选取具有高辨识度的测试数据特征并使用训练完成的分类器进行车辆认证。

此外，该方案由五部分组成，包括数据收集、数据预处理、CNN 训练及特征提取、分类器的训练和身份认证。

数据收集部分利用车辆的车载传感器捕捉车辆的行为模式，及时采样车辆相应的行为数据并实时传输到数字孪生。数据预处理部分则对采样的原始传感器数据进行分段和归一化处理。CNN 训练及特征提取部分利用 CNN 学习到的特征数据，通过主成分分析选择具有高识别度的特征数据。分类器的训练部分根据所选择的特征数据，对分类器进行训练，并从训练数据中生成合法车辆的配置文件。认证部分基于训练完成的 CNN 和分类器，对用于测试的车辆数据进行分类，将测试车辆分类为合法车辆或恶意车辆。基于 CNN 的车载数字孪生持续认证方案将允许合法车辆继续访问数字孪生上的云数据并在数字孪生内进行数据的共享；否则，被认定为恶意的车辆将需要车辆的身份标识，例如提供车辆身份标识等。本文工作与其他工作的不同之处在于：1) 在数字孪生中使用持续认证方案对车辆身份在会话过程中进行连续认证；2) 使用轻量级的 CNN 来学习和提取需要鉴别的特征数据并利用一类支持向量机（OC-SVM, one-class support vector machine）分类器进行数据分类。

3.2 改进的 CNN 架构

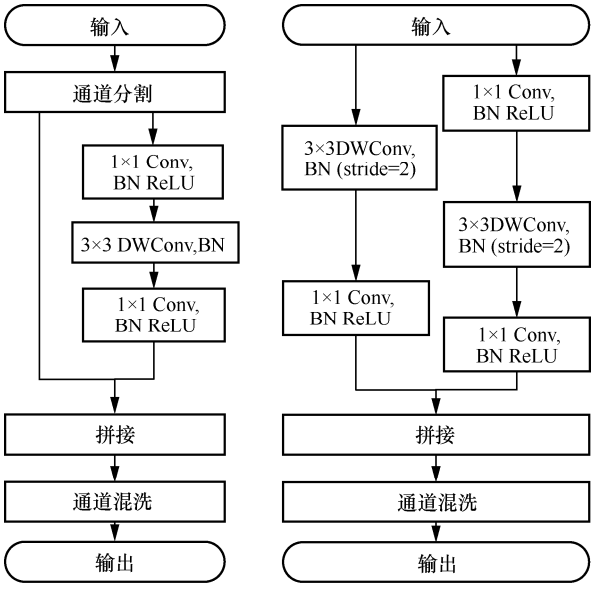
本文根据 shuffleNetV2 结构[9]设计了部署在数字孪生上的 CNN 架构，如图 3 所示。所设计的 CNN 架构主要由 2 个二维卷积层、3 个空间下采样基本单元和 shuffleNetV2 基本单元的堆叠（阶段 2～阶段 4）、一个平均池化层和一个全连接层组成。根据 shuffleNetV2 的结构，在每个二维卷积层后采用批量归一化（BN）和整流线性单元（ReLU），并且将平均池化层（AvgPool）放在在第二个二维卷积层之后。此外，阶段 2～阶段 4 具有相同的架构，由空间下采样基本单元和 shuffleNetV2 基本单元组成。

图 3 CNN 架构

shuffleNetV2 基本单元如图 4(a)所示。首先，将输入的 C 通道分割成 2 个大小相同的分支，即 $C-C'$ 和 C'，其中 $C'=\frac{C}{2}$。一个分支由深度卷积的 bottlenet 单元组成，具体结构由 2 个 1×1 Conv 和一个

3×3 DWConv 组成，每个1×1 Conv 后进行 BN 和 ReLU 操作；在3×3 DWConv 后进行 BN 操作[18]。然后，将 2 个分支与 C 通道进行拼接处理，分成G_b子组，通过将输出通道维度重置为(G_b, n)，转置并整合作为基本单元输出，对其进行通道混洗操作，其中$C = G_b n$。

空间下采样基本单元如图 4(b)所示。从 2 个相同的 C 通道分支开始，其中一个分支由 stride = 2 的 3×3 DWConv 和其后的一个 1×1 Conv 组成，在 3×3 DWConv 后进行 BN 操作，并在1×1 Conv 后进行 BN 和 ReLU 操作。另一个分支由 stride = 2 的深度卷积的 bottlenet 单元组成。然后，将 2 个分支与 2C 通道进行拼接操作，分为G_d子组，并应用通道混洗操作将其作为空间下采样基本单元的输出。



(a) shuffleNetV2基本单元　　(b) 空间下采样基本单元

图 4　shuffleNetV2 基本单元和空间下采样基本单元

3.3　方案细节

3.3.1　数据收集

本文方案中选择车辆的车载传感器来感知车辆的运动行为。利用传感器捕捉车辆的每一个细微操作行为，感知车辆行为运动模式并及时采样行为数据。考虑一般场景，在这项工作中，车辆的行为可以被传感器所捕获。

具体来说，加速度计、陀螺仪传感器能够捕捉车辆的粗粒度和细粒度运动模式，磁强计则能够感知车辆的位置。加速度计、陀螺仪可以通过测量三轴姿态和加速度确定车辆的姿态；磁强计可以确定车辆在真实参照系中的位置。当车辆的行为运动触发数据收集模块时，传感器以 F 为采样率，收集 T 时间段的原始传感器数据。为了收集部署在数字孪生上 CNN 训练的数据，本文设计了一个数据收集程序，产生并记录车辆的行为数据。使用设计的仿真程序在车辆上执行持续 5～15 min 的预计任务（在地图上导航以定位目的地、车辆经常停留的位置以及车辆行驶记录的产生）。这些任务是仿真过程中随机分配的，每个车辆预计执行 24 个随机会话，总共 2～6 h 的行为特征（8 个在地图上导航以定位目的地、8 个车辆经常停留的位置、8 个车辆行驶记录）。

在注册阶段，从车辆中选择加速度计、陀螺仪和磁强计的传感器读数，设置采样率为$F = 100$ Hz，在每个固定时间窗口大小的情况下，选择同样时间段内的训练数据。

在认证阶段，T 时间段内，采集$N = TF$ 个样本，每个同步样本记为$(X_{\mathrm{a}}, X_{\mathrm{g}}, X_{\mathrm{m}}, Y_{\mathrm{a}}, Y_{\mathrm{g}}, Y_{\mathrm{m}}, Z_{\mathrm{a}}, Z_{\mathrm{g}}, Z_{\mathrm{m}})^{\mathrm{T}} \in \mathbb{R}^9$，其中，$X$、$Y$、Z 分别表示传感器的 3 个轴，a、m、g 分别表示加速度计、陀螺仪、磁强计。

最后，将车辆的数据分为两组，其中一组数据用于注册阶段 CNN 和分类器的训练，另一组数据用于认证阶段的CNN特征提取和分类器特征分类。

3.3.2　数据预处理

在 T 时间段内，卷积神经网络可以收集 3 个传感器 $N = TF$ 个时域内的数据样本，收集到的传感器数据可以用$9 \times N$的矩阵表示，即

$$\begin{bmatrix} X_{\mathrm{a}}^{i1} & Y_{\mathrm{a}}^{i1} & Z_{\mathrm{a}}^{i1} & X_{\mathrm{g}}^{i1} & Y_{\mathrm{g}}^{i1} & Z_{\mathrm{g}}^{i1} & X_{\mathrm{m}}^{i1} & Y_{\mathrm{m}}^{i1} & Z_{\mathrm{m}}^{i1} \\ X_{\mathrm{a}}^{i2} & Y_{\mathrm{a}}^{i2} & Z_{\mathrm{a}}^{i2} & X_{\mathrm{g}}^{i2} & Y_{\mathrm{g}}^{i2} & Z_{\mathrm{g}}^{i2} & X_{\mathrm{m}}^{i2} & Y_{\mathrm{m}}^{i2} & Z_{\mathrm{m}}^{i2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ X_{\mathrm{a}}^{in} & Y_{\mathrm{a}}^{in} & Z_{\mathrm{a}}^{in} & X_{\mathrm{g}}^{in} & Y_{\mathrm{g}}^{in} & Z_{\mathrm{g}}^{in} & X_{\mathrm{m}}^{in} & Y_{\mathrm{m}}^{in} & Z_{\mathrm{m}}^{in} \end{bmatrix}$$

根据上述矩阵，传感器收集的数据集可以表示为

$$D_{\mathrm{sensor}} = [D^1, D^2, \cdots, D^{\mathrm{num}}]^{\mathrm{T}}$$

其中，num 是时间段的个数。

对于 CNN 的训练，使用收集到的传感器原始数据，将每个车辆的三轴数据归一化为D_{sensor}并获得预处理完成的传感器原始数据D_{raw}。

3.3.3　特征学习

利用所设计的 CNN 对归一化处理的传感器原始数据D_{raw}进行学习和提取判别特征。具体来说，

将固定时间段内收集到的样本数据进行处理，在首个二维卷积层中设置 24 个 Ksize = 3×3、 stride = 2 的滤波器。在阶段 2 中，模型应用 stride = 2 、$G_d = 2$ 的 2C 个滤波器基本单元进行空间下采样，然后设置 shuffleNetV2 的基本单元为 stride = 1 、G_d=2 的 48 个滤波器。在阶段 3 和阶段 4 中使用与阶段 2 相同的结构，分别使用 96 个滤波器和 192 个滤波器来设置 shuffleNetV2 的基本单元和空间下采样的基本单元。在第二个二维卷积层中，有 1 024 个 Ksize = 1×1 的滤波器在第一个二维卷积层和第二个二维卷积层后都使用 BN 和 ReLU 函数进行处理。平均池化层使用 1 024 个 Ksize = 7×7 的滤波器对通道降维并进行特征的提取。最后，全连接层利用输出层的 Softmax 激活函数将压缩后的特征向量映射到 10 个类别的输出。

3.3.4 CNN 训练及特征选取

1) PCA 降维

PCA[19]利用正交分解法进行数据降维，通过选择空间内新的相互正交的基向量来重新表示原始数据。PCA 降维可以将车辆原始的行为特征向量通过空间变换后映射到新的向量空间内，进而输出新的车辆行为特征向量，由此来达到保护车辆原始数据隐私的目的。简单来说，PCA 就是对于一个多维向量 $\mathbf{nX}=[x_1,x_2,\cdots,x_n]$，在获取一个新的向量空间 **kW** 之后把原始特征向量 **nX** 映射到新的特征向量空间 **kW** 从而得到 k 维向量 $\mathbf{nW}=[w_1,w_2,\cdots,w_k]$。PCA 能够使降维之后的数据特征相互独立。

2) 特征提取

在注册阶段的特征提取部分，CNN 利用训练数据进行特征学习并通过 PCA 对特征进行选取。注册阶段完成后，CNN 为训练完成状态。

在认证阶段的特征提取部分，CNN 已经是训练完成状态，经过训练的 CNN 对测试数据进行特征学习并通过主成分分析在测试数据样本中进行特征选取。

通过 CNN 学习和提取的测试数据的特征，使用 PCA 为 OC-SVM 分类器选择具有高识别度的特征数据，利用分类器对 CNN 所选择的特征数据进行分类。

3.3.5 分类器的训练

数字孪生通过 CNN 学习和提取到的特征数据，利用 OC-SVM 分类器对接入网络的车辆进行身份认证。具体来说，它将数据映射到具有核函数与高维度特征空间中，找到大部分客观数据点的最小超球面[20-21]，通过计算数据点与超球面的距离确定分类数[15,22]。在注册阶段，通过训练数据和径向基函数核来训练 OC-SVM，从而使车载数字孪生根据训练数据学习合法车辆的配置文件；在持续认证阶段，训练完成的分类器对 CNN 提取到的测试数据进行分类，基于选取的测试数据特征和训练完成的 OC-SVM 将想要访问网络的车辆划分为合法车辆或者恶意车辆，并进行如下操作：①若车辆被认定为合法车辆，将被允许访问数字孪生并进行信息传输和共享；②若车辆被认定为恶意车辆，将被禁止继续访问数字孪生并被要求提供合法的车辆身份标识进行车辆合法身份的认证。

无论触发以上何种操作，数字孪生持续认证方案都将持续不断地对车辆进行身份验证，以保证暴露在公共无线网络中数字孪生的安全性和信息数据传输的真实性。

具体来说，本文使用 CNN 和 shuffleNetV2 提取训练数据集中的特征，并使用这些特征来训练 OC-SVM 模型。首先，将这 2 个网络设置为评估模式，以确保在推进过程中不会进行任何训练。然后，进行梯度计算的禁用，以减少内存使用和加速代码。接着，循环训练数据集中的所有批次并将每个批次的输入数据传递给 CNN 和 shuffleNetV2 以提取特征。最后，将这些特征相连并添加到特征列表，使用这些特征来训练 OC-SVM 模型。

3.3.6 身份认证

身份认证是方案的最后一步，传感器数据经过数据预处理后被分训练数据和测试数据。在注册阶段，通过训练数据训练完成的 CNN 和分类器已经能够自主地对数据进行特征学习和特征提取；在测试阶段，CNN 提取的测试数据特征会被 PCA 进行分析，并将选取的特征数据传输给训练完成的分类器，分类器通过这些特征进行异常检测和结果的输出，接着分类器根据输出的结果进行车辆身份认证，最终车辆会被认证为合法车辆或恶意车辆。

3.4 进一步讨论

本节对所提持续认证方案与传统接入认证方案有效结合的可能性进行讨论。

本文所提持续认证方案是一种利用卷积神经网络对车辆进行实时监测和评估的方案，通过提取车辆的行为特征或传感器数据特征并结合训练完成的 CNN，准确评估车辆身份合法性，它可以提供

即时可靠的认证结果，供监管机构检测车辆的身份信息。传统接入认证是指在车辆与某种系统（如车载网络、车载娱乐系统等）之间建立连接时所进行的身份验证和授权过程。这个过程旨在确保只有合法和授权的实体（如车辆用户、制造商、服务提供商）能够访问车辆的功能和数据，以确保车辆的安全性、隐私性和功能完整性。例如，3GPP 中主流的 5G-AKA 认证协议[23]，可以通过利用 5G 网络的安全特性和高速传输能力，使用认证和密钥管理协议来验证车辆身份的合法性，可以有效防止车辆的身份被冒充甚至被非法篡改，以确保网络环境的安全性。然而，传统的认证技术只能在接入网络时执行身份认证，无法确保在后续的通信过程中持续对用户和设备进行可信验证。

通过将这两类方法有效结合，可以充分利用它们各自的优势，进一步提高车辆认证的准确性、实时性和安全性。一种可能的结合方式是在初始接入阶段执行一次完整的接入认证协议，完成身份认证的同时所产生的密钥素材可以保护接下来用于持续认证的数据流的机密性和完整性。而持续认证可以实时监测和评估车辆的性能，提高认证的实时性和准确性。这 2 种认证方法的有效结合可以建立一个更智能、更安全的车联网认证体系，能够提供更全面、更准确和更可靠的车辆认证结果。

4　方案的仿真分析

本节首先对 OC-SVM 分类器的性能进行了分析，接着对方案进行了仿真分析。

4.1　分类器性能分析

为了确定 PCA 为 OC-SVM 分类器选取的最优特征数，本文通过实验来研究不同特征数量对 OC-SVM 的影响，设置特征从 10 个增加到 100 个，计算 OC-SVM 的准确率。不同特征数量的 OC-SVM 准确率如图 5 所示。从图 5 可以看出，OC-SVM 的准确率随着特征数量的增加而增加，当达到最优值后有所下降。从实验结果来看，当 PCA 选取 60 个特征时，OC-SVM 的准确率为最大值 80.76%，这个结果说明在这个数据集上，使用 60 个特征可以获得最佳的分类结果。当特征数量开始增加时，模型的准确率会增加，但是当特征数量超过一定阈值时，模型的准确率会下降。这是因为特征数量过多会导致模型过拟合，而特征数量过少会导致模型欠拟合。通过实验确定 OC-SVM 的最优特征数量为 60 个。

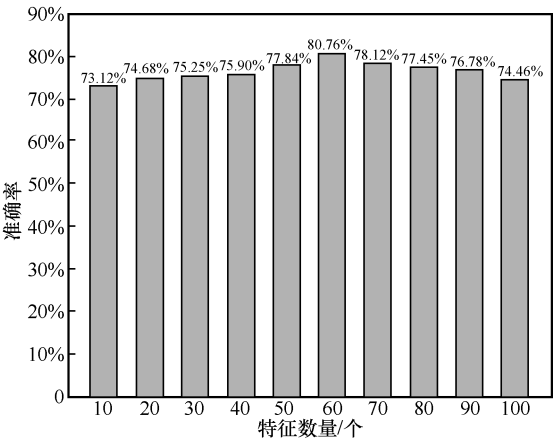


图 5　不同特征数量的 OC-SVM 的准确率

4.2　实验仿真

本节首先描述实验的设置；然后，说明训练损失（Train Loss）、训练准确率（Train Acc）、测试损失、测试准确率评价指标；最后，对设计的方案效率进行详细说明，并将所设计的方案与 GoogLeNet 进行比较。

4.2.1　实验设置

实验中使用 100 个车辆的加速度计、陀螺仪和磁强计所收集的数据作为实验数据集，将收集到的数据通过车辆和数字孪生的专有通信链路传输到部署在数字孪生上的 CNN 中，接着对数据集进行划分。具体来说，从 100 个车辆收集的传感器数据中随机选择 80 个车辆数据来训练 CNN。在训练完成 CNN 的基础上，选择剩下的 20 个用户数据（训练完成的 CNN 提取的特征数据）来训练 OC-SVM 分类器。

对于 CNN 的训练，随机选择 80 个车辆的原始传感器数据，80%用于训练，20%用于验证。对于每个批量大小的训练数据，将它们输入设计的 CNN 中，根据输出利用交叉熵计算损失，然后进行反向传播，最后更新学习率参数；对于分类器的训练，从 20 个实验车辆中随机选择一个作为合法车辆，其余 19 个车辆作为恶意车辆，对合法车辆使用 10 折交叉验证，也就是说，将合法车辆的阳性样本平均分为 10 个子集，其中 9 个子集作为训练集，剩下的一个作为测试集。

4.2.2　评估指标

本节首先对评价指标的变化趋势进行说明，如表 1 所示。

Train Loss 表示训练阶段预测值与实际值之间的误差或差异。训练过程的目标是尽量减少这种损失。Train Loss 通常使用均方误差或交叉熵损失等损失函数进行计算。Train Acc 表示衡量模型对训练

数据集的预测的准确性，通常表示为百分比形式，表示模型在训练期间做出的正确预测的比例。

表 1 评价指标的变化说明

指标	含义
Train Loss 下降 Test Loss 下降	网络仍在学习
Train Loss 下降 Test Loss 不变	网络过拟合
Train Loss 不变 Test Loss 下降	数据集出现问题
Train Loss 不变 Test Loss 不变	学习遇到瓶颈
Train Loss 上升 Test Loss 上升	网络结构设计不当

Test Loss 表示测试数据集上的错误或损失。测试数据集是模型在训练期间未看到的单独数据集。Test Loss 有助于评估模型对未见过的数据的泛化程度。Test Acc 用来衡量模型对测试数据集的预测的准确性，与 Train Acc 类似，它通常表示为百分比形式，表示模型对测试数据做出的正确预测的比例。

4.2.3 方案效率分析

根据上述评价指标，本文进行了实验并评估了所设计的 CNN 的分析特征和认证效率，并对 CNN 训练和测试的全过程进行了分析。

Train Loss 和 Test Loss 随着训练周期的变化情况如图 6 所示。从图 6 可以看出，所设计的 CNN 在初始阶段 Train Loss 较高，Test Loss 也相对较高，并且 Train Loss 和 Test Loss 的差距较大，这可能是由于模型刚开始学习数据中的模式和特征，还没有完全收敛到最优解。随着训练周期的增加，Train Loss 逐渐下降，并在大约 10 个训练周期后趋于稳定。在稳定阶段，Train Loss 约为 210。Test Loss 也随着训练周期的增加而下降，但下降速度较慢。在约 10 个训练周期后，Test Loss 趋于稳定，在稳定阶段约为 45。

根据图 6 可以得出，Train Loss 和 Test Loss 之间存在差距，但它们的整体趋势是相似的。这表明所设计的 CNN 模型在训练过程中能够泛化到未出现过的测试数据，表现出较好的收敛性和泛化性，两者都能够在一定周期后稳定，并且没有出现明显的过拟合现象。随着训练周期的增加，Train Loss 持续下降，这表明模型能够从训练数据中学习到有用的特征和模式。当所设计的 CNN 模型趋于稳定后，Train Loss 和 Test Loss 之间的差距相对较小，这表明模型在训练数据和测试数据上的表现比较一致。

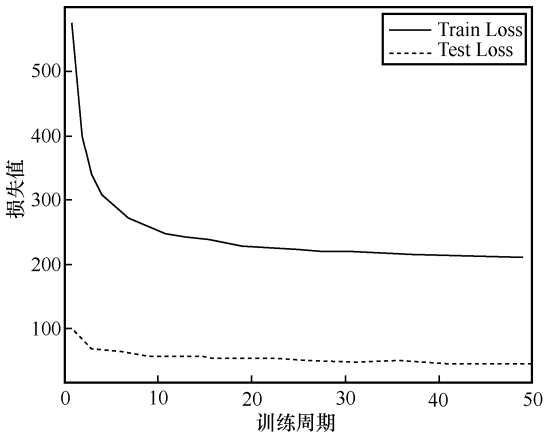


图 6 Train Loss 和 Test Loss 变化情况

Train Acc 和 Test Acc 随着训练周期的变化情况如图 7 所示。从图 7 可以看出，随着训练周期的增加，Train Acc 和 Test Acc 都逐渐提高。在初始阶段，Train Acc 约为 48.2%，Test Acc 约为 60.44%。随着训练周期的增加，Train Acc 逐渐提高，并在大约 40 个周期后超过了 Test Acc。在约 50 个训练周期后，Train Acc 继续提高，而 Test Acc 增长速度放缓，Train Acc 达到了约 83%，而 Test Acc 也在此时达到了约 83.21%。

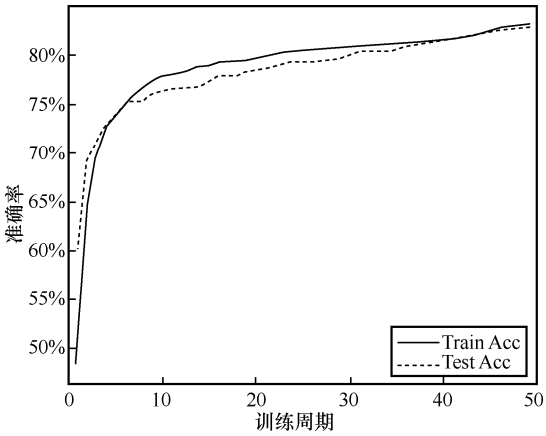


图 7 Train Acc 和 Test Acc 的变化情况

根据图 7 可知，模型的 Train Acc 随着训练周期的增加而逐渐提高，表明模型在训练数据上的表现不断改善，并且能够捕捉到数据中的模式和特征；Test Acc 也随着训练周期的增加而增加，表明模型在未出现过的测试数据上也能够良好地泛化，而不仅仅适用于训练数据。初始阶段，Train Acc 和 Test Acc 之间存在较大的差距。这可能是由于模型刚开始学习数据的特征，还没有完全适应训练和测试数据。随着训练的进行，Train Acc 和 Test Acc 之间的差距逐渐减小。这表明模型在一定程度上避免

了过拟合，即在测试数据上也能够有较好的性能。

总体来看，模型在训练过程中表现出了不错的性能。Train Acc 和 Test Acc 都逐渐提高，并且在一定周期后趋于稳定。这表明模型具有一定的泛化能力，并且能够适应未出现过的数据。

4.2.4　与 GoogLeNet 和 DenseNet 的比较

为了评估所提 CNN 的性能，本节将其与现有流行的网络结构 GoogLeNet[24]和 DenseNet[25]在同平台下利用相同的车辆传感器原始数据集样本进行了比较，结果如图 8 所示。从图 8 可以看出，初始阶段（训练周期为 1～10）GoogLeNet 模型的准确率从约 54.88%快速上升到约 68.89%。这表明模型在初始阶段学习到了有效的特征和模式，并在准确率上取得了显著提升。在稳定阶段（训练周期为 10 之后）GoogLeNet 模型的准确率增长速度减缓，并趋于稳定在 69%～71%。这意味着模型已经接近了在给定数据集上的最优表现，进一步训练对于准确率的提升影响较小。DenseNet 模型的准确率随着训练周期增加而提升。初始阶段，Test Acc 较低（约为 34.48%），随着训练的进行，它逐渐上升，在最初几个训练周期中，Test Acc 提升较快，但之后逐渐提升缓慢，最终达到约 72.89%。与其他 2 个模型相比，DenseNet 的准确率整体上较低。从图 8 可以看出，DenseNet 的准确率增长速度逐渐减缓，说明模型在数据上逐渐达到了一个性能上限，这意味着在同等数据集的情况下，DenseNet 的性能相对较差。

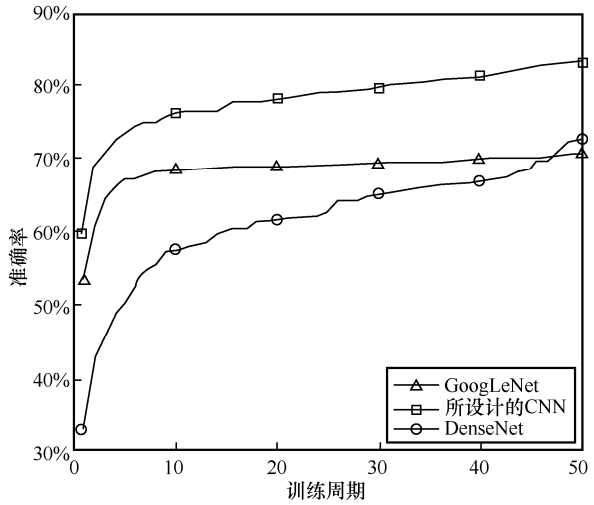


图 8　所设计的 CNN 和 GoogLeNet、DenseNet 准确率的比较

对于所设计的 CNN，在初始阶段（训练周期为 1～10）准确率从约 60.44%迅速上升到约 76.52%，这表明该模型具有较快的学习能力，并能够更快地捕捉到数据中的模式和特征。到达稳定阶段（训练周期为 10 之后）时，模型的准确率增长速度减缓，但仍然持续增长，最终达到约 83.21%。这表明该模型在较长的训练周期内仍然能够进一步提升准确率。

综上所述，在训练开始时，Designed CNN 的 Test Acc 明显优于 GooLeNet 和 DenseNet 的 Train Acc。这表明 Designed CNN 的整体网络结构具有更好的权重初始化，其经过短时间训练后就能表现出较好的性能。Designed CNN 在初始训练周期内快速提高 Test Acc 展示了其学习速率较高，能更快地从数据中学习特征数据。

在整个训练过程中，所设计的 CNN 始终表现出较高的准确率，优于 GoogLeNet 和 DenseNet。图 8 结果表明，所设计的 CNN 在车载数字孪生的持续认证方案上具有更好的性能和学习能力。GoogLeNet 在训练初期的学习速度较快，但在后续阶段的准确率增长相对较慢，趋于稳定。DenseNet 在这个数据集上的 Test Acc 有逐渐提升的趋势，但是整体的性能相对较低。相比之下，尽管增长速度在后期有所减缓，但是所设计的 CNN 在整个过程中都表现出较快的准确率提升。

总体来看，所设计的 CNN 在车载数字孪生的持续认证上展现出了更好的性能，能够更快地学习到数据中的模式和特征，并实现更高的准确率。

5　结束语

本文研究了车载数字孪生系统中车辆身份合法性验证问题，利用主流的 shuffleNetV2 结构改进了部署在数字孪生上的 CNN 架构，进而利用改进的 CNN 架构和 OC-SVM 分类器对车辆的身份进行持续认证。实验分析和比较结果表明，相比于 GoogLeNet 和 DenseNet 模型，所设计的方案具有良好的学习能力和性能。未来，为了提高车载数字孪生持续认证的效率和准确性，将设计用于提取深度特征的数据增强机制对提取的特征数据进行辨识度的优化和提高，进而改进方案的性能和效率。

参考文献：

[1] LAI C Z, MA Y X, LU R X, et al. A novel authentication scheme supporting multiple user access for 5G and beyond[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4): 2970-2987.

[2] ZHANG Y H, DENG R H, BERTINO E, et al. Robust and universal seamless handover authentication in 5G HetNets[J]. IEEE Transac-

tions on Dependable and Secure Computing, 2021, 18(2): 858-874.
[3] FAN C N, HUANG J J, ZHONG M Z, et al. ReHand: secure region-based fast handover with user anonymity for small cell networks in mobile communications[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 927-942.
[4] LI G J, LAI C Z, LU R X, et al. SecCDV: a security reference architecture for cybertwin-driven 6G V2X[J]. IEEE Transactions on Vehicular Technology, 2022, 71(5): 4535-4550.
[5] LAI C Z, WANG M H, ZHENG D. SPDT: secure and privacy-preserving scheme for digital twin-based traffic control[C]//Proceedings of IEEE/CIC International Conference on Communications in China (ICCC). Piscataway: IEEE Press, 2022: 144-149.
[6] GONZALEZ-MANZANO L, FUENTES J M D, RIBAGORDA A. Leveraging user-related Internet of things for continuous authentication: a survey[J]. ACM Computing Surveys, 2020, 52(3): 1-38.
[7] MEKRUKSAVANICH S, JITPATTANAKUL A. Deep learning approaches for continuous authentication based on activity patterns using mobile sensing[J]. Sensors, 2021, 21(22): 7519.
[8] KUMAR A, SAHU S, ROHIT R. Deep learning-based continuous authentication for an IoT-enabled healthcare service[J]. Computers and Electrical Engineering, 2022, 99: 107817.
[9] MA N N, ZHANG X Y, ZHENG H T, et al. ShuffleNetV2: practical guidelines for efficient CNN architecture design[M]. Cham: Springer International Publishing, 2018.
[10] SANCHEZ P M S, MAINO L F, CELDRAN A H, et al. AuthCODE: a privacy-preserving and multi-device continuous authentication architecture based on machine and deep learning[J]. Computers & Security, 2021, 103: 102168.
[11] JAMES J C, RAJASREE M S. Implicit continuous user authentication for mobile devices based on deep reinforcement learning[J]. Computer Systems Science and Engineering, 2023, 44(2): 1357-1372.
[12] ABUHAMAD M, ABUHMED T, MOHAISEN D, et al. AUToSen: deep-learning-based implicit continuous authentication using smartphone sensors[J]. IEEE Internet of Things Journal, 2020, 7(6): 5008-5020.
[13] NAJI Z, BOUZIDI D. Deep learning approach for a dynamic swipe gestures based continuous authentication[C]//Proceedings of the 3rd International Conference on Artificial Intelligence and Computer Vision (AICV2023). Piscataway: IEEE Press, 2023: 48-57.
[14] CHAUHAN J, KWON Y D, HUI P, et al. ContAuth: continual learning framework for behavioral-based user authentication[C]// Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. New York: ACM Press, 2020: 1-23.
[15] WU C, HE K, CHEN J, et al. Liveness is not enough: enhancing fingerprint authentication with behavioral biometrics to defeat puppet attacks[C]//Proceedings of the 29th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2020: 2219-2236.
[16] LUAN T H, LIU R, GAO L, et al. The paradigm of digital twin communications[J]. arXiv Preprint, arXiv: 2105.07182, 2021.
[17] HE C, LUAN T H, LU R X, et al. Security and privacy in vehicular digital twin networks: challenges and solutions[J]. IEEE Wireless Communications, 2023, 30(4): 154-160.
[18] ZHANG X Y, ZHOU X Y, LIN M X, et al. ShuffleNet: an extremely efficient convolutional neural network for mobile devices[C]//Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 6848-6856.
[19] WOLD S, ESBENSEN K, GELADI P. Principal component analysis[J]. Chemometrics and Intelligent Laboratory Systems, 1987, 2(1-3): 37-52.
[20] SHEN C, LI Y X, CHEN Y F, et al. Performance analysis of multi-motion sensor behavior for active smartphone authentication[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 48-62.
[21] SHEN C, LI Y P, YU T W, et al. Motion-senor behavior analysis for continuous authentication on smartphones[C]//Proceedings of 12th World Congress on Intelligent Control and Automation (WCICA). Piscataway: IEEE Press, 2016: 2023-2028.
[22] SENF A, CHEN X W, ZHANG A. Comparison of one-class SVM and two-class SVM for fold recognition[C]//Proceedings of International Conference on Neural Information Processing. Berilin: Springer, 2006: 140-149.
[23] KOUTSOS A. The 5G-AKA authentication protocol privacy[C]//Proceedings of IEEE European Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 464-479.
[24] SZEGEDY C, LIU W, JIA Y Q, et al. Going deeper with convolutions[C]//Proceedings of Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2015: 1-9.
[25] HUANG G, LIU Z, MAATEN L V D, et al. Densely connected convolutional networks[C]//Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2017: 2261-2269.

[作者简介]

赖成喆（1985− ），男，陕西汉中人，博士，西安邮电大学教授，主要研究方向为安全协议设计与分析、车联网安全。

张鑫伟（1998− ），男，陕西咸阳人，西安邮电大学硕士生，主要研究方向为车联网安全和隐私保护技术。

李冠颉（1994− ），男，陕西韩城人，西安电子科技大学博士生，主要研究方向为数字孪生和车联网。

郑东（1964− ），男，山西临汾人，博士，西安邮电大学教授，主要研究方向为编码密码学和网络安全。