计算机科学
COMPUTER SCIENCE

基于加性秘密共享的轻量级隐私保护移动传感分类框架

何宇宇, 周凤, 田有亮, 熊伟, 王帅

引用本文

何宇宇, 周凤, 田有亮, 熊伟, 王帅. 基于加性秘密共享的轻量级隐私保护移动传感分类框架[J]. 计算机科学, 2025, 52(11): 415-424.

HE Yuyu, ZHOU Feng, TIAN Youliang, XIONG Wei, WANG Shuai. Lightweight Privacy-preserving Mobile Sensing Classification Framework Based on AddictiveSecret Sharing [J]. Computer Science, 2025, 52(11): 415-424.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241100101

基于加性秘密共享的轻量级隐私保护移动传感分类框架

何宇宇[1,2,3]　周　凤[1]　田有亮[3,4]　熊　伟[1]　王　帅[1,2,3]
1 贵州大学计算机科学与技术学院公共大数据国家重点实验室　贵阳 550025
2 贵州省密码学与区块链技术特色重点实验室　贵阳 550025
3 贵州大学密码学与数据安全研究所　贵阳 550025
4 贵州大学大数据与信息工程学院　贵阳 550025
(heyuyu97@163.com)

摘　要　针对在移动传感设备上部署卷积神经网络模型出现的数据隐私泄露问题,以及隐私保护目标分类框架中服务器交互计算导致通信开销过高的挑战,提出了一种基于加性秘密共享的轻量级隐私保护移动传感目标分类框架(LPMS)。该框架确保移动传感设备在交换数据时不会泄露隐私信息,同时显著降低通信开销和计算开销。首先,利用加性秘密共享技术构建了一系列不依赖计算密集型密码原语的安全计算协议,以实现安全高效的神经网络计算;其次,构建了一种三维混沌加密方案,防止原始数据在上传至边缘服务器的过程中被攻击者窃取;最后,通过理论分析与安全性证明,验证了 LPMS 框架的正确性及安全性。实验结果表明,与 PPFE 方案相比,LPMS 方案将模型计算开销降低了 73.33%,通信开销减少了 68.36%。

关键词:移动传感设备;卷积神经网络;隐私保护;加性秘密共享;混沌加密
中图分类号　TP309.2

Lightweight Privacy-preserving Mobile Sensing Classification Framework Based on Addictive Secret Sharing

HE Yuyu[1,2,3],ZHOU Feng[1],TIAN Youliang[3,4],XIONG Wei[1] and WANG Shuai[1,2,3]
1 State Key Laboratory of Public Big Data,College of Computer Science and Technology,Guizhou University,Guiyang 550025,China
2 Guizhou Provincial Key Laboratory of Cryptography and Blockchain Technology,Guiyang 550025,China
3 Institute of Cryptography & Data Security,Guizhou University,Guiyang 550025,China
4 College of Big Data and Information Engineering,Guizhou University,Guiyang 550025,China

Abstract　To address data privacy leakage in deploying convolutional neural network models on mobile sensing devices,as well as the challenge of excessive communication overhead caused by server interaction computations in privacy-preserving target classification frameworks,a lightweight privacy-preserving mobile sensing object classification framework(LPMS) based on additive secret sharing is proposed. This framework ensures that mobile sensing devices maintain data confidentiality during data exchanges while significantly reducing both communication and computational overhead. Firstly,a series of secure computing protocols are developed using additive secret sharing technology,avoiding reliance on computationally intensive cryptographic primitives to facilitate efficient and secure neural network computations. Secondly,a three-dimensional chaotic encryption scheme is introduced to protect original data from potential attackers during uploads to the edge server. Finally,the correctness and security of the LPMS framework are validated through theoretical analysis and security proofs. Experimental results demonstrate that,compared to the PPFE scheme,the LPMS framework reduces model computation overhead by 73.33% and communication overhead by 68.36%.

Keywords　Mobile sensing devices,Convolutional neural networks,Privacy-preserving,Additive secret sharing,Chaotic encryption

到稿日期:2024-11-18　返修日期:2025-02-21
基金项目:国家重点研发计划(2021YFB3101100);国家自然科学基金(62272123);贵州省高层次创新型人才项目(黔科合平台人才[2020]6008);贵州省科技计划项目(黔科合平台人才[2020]5017,黔科合支撑[2022]一般 065,黔科合战略找矿[2022]ZD001);贵阳市科技计划项目(筑科合[2022]2-4)
This work was supported by the National Key R&D Program of China(2021YFB3101100),National Natural Science Foundation of China(62272123),Project of High-level Innovative Talents of Guizhou Province([2020]6008),Science and Technology Program of Guizhou Province([2020]5017,[2022]065,[2022]ZD001) and Science and Technology Program of Guiyang([2022]2-4).
通信作者:周凤(41544782@qq.com)

1 引言

随着采集技术的快速发展，移动传感设备正逐渐展现出其卓越的传感和计算能力[1]。这些设备配备了多样化的传感器，能够精准捕捉图像信息，进而被应用于各类视觉任务，包括物体识别、目标分类、目标检测和语义分割。因此，移动传感设备在自动驾驶、医学图像分析、虚拟现实、人工智能等领域[2-4]得到了广泛的应用。例如，在自动驾驶中，移动传感设备通过车载摄像头实时捕捉路面图像，辅助障碍物、行人和交通标志的识别，实现自动导航与决策。在深度学习领域的持续突破下，卷积神经网络(Convolutional Neural Network，CNN)[5]在视觉任务中的表现显著提升，尤其是在目标分类任务中，卷积神经网络的分类准确性远超传统的机器学习方法[6]。

在移动传感设备上部署卷积神经网络模型面临计算资源有限和存储开销高的挑战。为了解决这些问题，边缘计算[7]被引入，它是一种优化云计算架构的有效方法，不仅能显著减少向数据中心传输大量数据所需的带宽，还能有效缩短移动设备与数据中心之间的通信延迟。然而，上传至边缘服务器的数据通常包含大量敏感信息，一旦泄露，将对个人隐私构成严重威胁。同时，保护模型数据隐私所引发的高计算和通信开销也是亟待解决的问题。因此，设计面向移动传感体系的隐私保护目标分类方案至关重要。

为了解决神经网络模型中的数据隐私泄露问题，许多研究者利用同态加密(Homomorphic Encryption，HE)[8]和安全多方计算(Multi-party Computation，MPC)[9]构建隐私保护神经网络。Gilad-Bachrach 等[10]提出的 CryptoNets 方案首次将同态加密应用于神经网络，实现了卷积神经网络中涉及的简单计算任务。然而，网络中的非线性函数需要通过低次多项式逼近，这从本质上降低了方案的精度，且会导致计算开销过大。Mohassel 等[11]提出一种隐私保护混合协议框架 ABY3 为不同操作采用最有效的协议，但由于受到计算密集型密码原语的限制，该框架未能充分利用卷积神经网络中的高效并行数据结构，因此扩展性较差。Rathee 等[12]提出的 CrypTFlow2 框架实现了两方隐私保护的安全推理，采用混淆电路(Garbled Circuit，GC)[13]保护计算结果。尽管该框架实现了恒轮通信，但在传输整个加密真值表和执行额外的不经意传输(Oblivious Transfer，OT)[14]操作时，混淆电路的通信开销仍然较高。

上述方案主要针对使用各种加密技术的隐私保护神经网络，但未能有效满足移动传感应用场景下的隐私保护需求。在移动传感设备上部署卷积神经网络模型需要轻量级且通信开销低的解决方案。Xiong 等[15]利用边缘服务器实现了一个隐私保护数据共享框架，该框架不仅可以替代移动传感设备完成目标分类模型的推理和训练任务，还能有效降低通信开销。但该方案难以适应更复杂的神经网络结构，并且在非线性函数计算中开销较大。Huang 等[16]利用加性秘密共享技术，在秘密共享图像上构建了轻量级移动传感神经网络特征提取框架。该框架在保持卷积神经网络模型准确性的同时保护了数据隐私，并有效降低了安全计算协议的计算成本和通信开销。然而，该方案中所设计的安全比较计算协议缺乏自适应循环机制，导致计算精度和效率均产生误差。Yang 等[17]提出了一种高效的隐私保护推理外包方案，利用加性秘密共享为云服务器设计了安全的两方计算协议。该协议避免了线性计算中昂贵的置换操作和非线性计算中的近似操作，从而保证了计算精度，但未能防止潜在敌手对数据通信信道进行破坏。

针对移动传感应用场景下的隐私泄露问题及当前隐私保护目标分类框架中的通信开销优化问题，本文提出了基于加性秘密共享的轻量级隐私保护移动传感目标分类框架(Lightweight Privacy-preserving Object Classification Framework For Mobile Sensing，LPMS)。利用加性秘密共享技术设计了一系列与神经网络各层相匹配的安全计算协议，以此保护数据的隐私性，同时通过一种改进的混沌加密方案，防止潜在敌手破坏数据通信信道。本文的贡献如下：

1)提出了一个轻量级的隐私保护框架 LPMS，旨在实现对移动传感设备的目标分类。利用加性秘密共享技术构建了一系列不依赖计算密集型密码原语的安全计算协议，从而大幅降低了用户的计算和通信开销。

2)构建了一种混沌加密方案，用于保护数据上传过程中的隐私。该方案在有效降低加解密开销的同时具备高安全性，在原始数据上传至边缘服务器的过程中能够有效防止通信信道被攻击者破坏。

3)通过理论分析证明了所提安全计算协议及 LPMS 框架的正确性和安全性。实验结果表明，与 PPFE 方案相比，LPMS 将计算开销减少了 73.33%，通信开销减少了 68.36%。

2 预备知识

2.1 混沌映射

混沌是指一个系统因对初始条件和参数的敏感性而表现出的一种伪随机和不可预测的运动。混沌系统是一种复杂的高动态系统，具有对初始条件敏感、非线性、非周期性等特点。其次，混沌系统还具有其他特征，包括高遍历性、确定性和伪随机性，这对图像加密至关重要。此外，与对称加密相比，混沌加密的计算成本更低，更适合高时效应用场景下的图像加密和传输。

本文引入两个混沌映射，分别是 Henon 映射[18]与 Sine 映射[19]。Sine 映射为单峰映射，定义为 $\boldsymbol{X}_{i+1}=a\sin(\pi\boldsymbol{X}_i)$，其中，$a$ 和 b 表示控制参数，当 $a=0.9$，$b=0.97$ 时，函数映射为混沌状态。Henon 映射是一个经典的二维混沌映射，其定义如下：

$$\begin{cases}\boldsymbol{X}_{n+1}=1+\boldsymbol{Y}_n-a\boldsymbol{Y}_n^2\\ \boldsymbol{Y}_{n+1}=b\boldsymbol{X}_n\end{cases}\tag{1}$$

当 $a=1.4$，$b=0.3$ 时，函数映射为混沌状态。由于单峰映射的加密方案在安全强度上较弱，因此本文在不显著增加计算成本的情况下，在上述两种混沌映射的基础上设计了新的三维混沌映射加密方案。

2.2 加性秘密共享

秘密共享的定义如下：一个可信方将秘密 x 拆分成 N

份，分别分发给 N 个参与方，只需要 $k(k\leqslant N)$ 个参与方即可重构完整秘密。在加性秘密共享中，只有两个参与方，即 $N=k=2$。

在本文中，数组作为最小计算单元，所有元素都在整环 Z_n 中，其中 n 表示 Z_n 的大小。假设有两个参与方 v_1 和 v_2 分别持有 Z_n 内的输入 $\boldsymbol{x}$ 和 $\boldsymbol{y}$，他们想要共同计算 $\boldsymbol{x}+\boldsymbol{y}$，但不向对方暴露 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的值，只需将 $\boldsymbol{x}$ 拆分为 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2$，将 $\boldsymbol{y}$ 拆分为 $\boldsymbol{y}_1$ 和 $\boldsymbol{y}_2$，然后将 $\boldsymbol{x}_i(i=1,2)$ 和 $\boldsymbol{y}_i(i=1,2)$ 发送给参与方 v_i，最后接收方将两个数据进行简单相加即可重构秘密。

3 系统模型和安全模型

3.1 系统模型

在本文框架中，为解决移动传感体系下神经网络目标分类的隐私保护问题，设计了一系列基于加性秘密共享技术的高效安全计算协议，通过混沌加密方案来保护数据发送至边缘服务器之前的通信信道。与之前的秘密共享方案[20-21]不同的是，本文将计算密集型任务下发至两台边缘服务器进行处理，不仅能够减小通信流量，提高传输效率，还能提高抗风险攻击的能力。

本文框架主要由 4 个部分组成，即移动传感设备、两台边缘服务器、可信第三方，以及数据接收方，如图 1 所示。

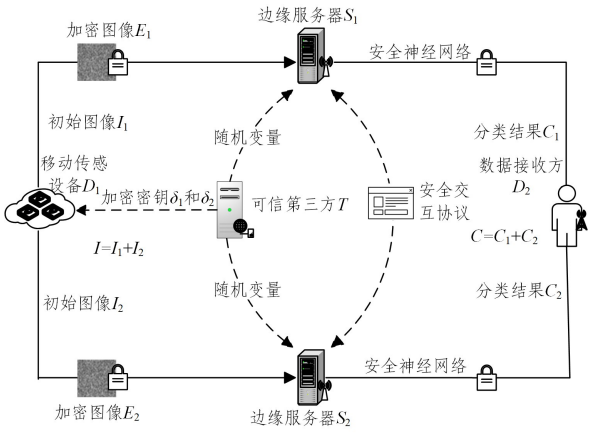

图 1 系统模型图

Fig. 1 Diagram of the system model

1) 移动传感设备 D_1：D_1 使用高清传感器生成图像数据，每个图像 I 被随机拆分成 I_1 和 $I_2(I=I_1+I_2)$。D_1 通过加密密钥 δ_i 将 I_i 加密成加密图像 E_i，分别发送给 S_i，防止 I_i 暴露在通信链路上。

2) 边缘服务器 S_i：S_i 接收到加密图像 E_i 后，会进行两轮解密计算，恢复 I_i。然后，S_i 使用安全计算协议执行保护隐私的神经网络目标分类模型，得到两个分类结果 C_i。

3) 可信第三方 T：T 负责生成图像加密密钥 δ_i，通过安全传输信道发送给 D_1 和 S_i。

4) 数据接收方 D_2：D_2 接收到 C_i 后，将 C_i 进行简单相加得到 $C(C=C_1+C_2)$，即可恢复原始分类结果。

3.2 安全模型

本文讨论了加密图像的隐私保护推理过程。在此过程中，神经网络模型的参数被严格设定为 S_i 私有，以确保 D_1 无法获取到任何相关信息。同时，原始图像、S_i 提取的特征和最终的分类结果均被设定为 D_1 私有，S_i 亦无法获取相关内容。与文献[21-23]一样，本文采用半诚实的安全模型。T 和 S_i 被认为是半诚实实体，严格遵循协议的执行，但试图通过已有数据推测其他信息。其次，假设两个边缘服务器 S_1 和 S_2 是独立的，不相互勾结[15]。可信第三方 T 可以由某个中立机构提供，因为它只负责生成并分发加密密钥和随机值，不参与线上计算过程。因此，T 无法得到任何有意义的图像数据，也不会影响框架的安全性。此外，假设移动传感设备 D_1 与数据接收方 D_2 始终是可靠的，通信链路不中断。

在半诚实模型中，存在概率多项式时间敌手 K，目的是利用设备获取 D_i 的图像隐私。K 具备以下能力和约束条件：1)可以破坏数据发送方和数据接收方以获取存储的加密数据，但无法获取加密密钥；2)可以窃听数据发送方与边缘服务器以及边缘服务器与数据接收方之间的通信信道，从而获取传输信息；3)最多只能破坏并获取两个边缘服务器中其中一个的信息；4) 不能窃听 T，S_1，S_2 之间的安全信道，不能破坏可信第三方 T。K 攻击成功意味着它获取到了完整的原始图像或特征，这在现实场景下是非常困难的。详细证明将在 6.3 节安全性分析中说明。

4 基于秘密共享的高效安全计算

为了实现安全的神经网络目标分类，本文设计了一系列基于加性秘密共享的高效安全计算协议，其中安全与-异或转换协议(STAX)、安全比较协议(SecComp)、安全异或-加法转换协议(STXA)和安全乘法协议(SecMul)[21]是安全激活协议(SecReLU)的组成部分。

4.1 基础安全协议

在本文中，两台边缘服务器 S_1 和 S_2 独立或协作执行协议。用于线性计算的基础安全协议主要包括利用秘密共享的安全加法/减法(SecAdd/SecSub)协议、安全标量乘法协议(SecSMul)和安全异或协议(SecXOR)。

在安全加法/减法协议中，数据发送方 D_1 将输入数组 $(\boldsymbol{u},\boldsymbol{v})\in Z_n$ 拆分为 $(\boldsymbol{u}_1,\boldsymbol{v}_1)$ 和 $(\boldsymbol{u}_2,\boldsymbol{v}_2)$，分别发送给边缘服务器 S_1 和 S_2，S_1 和 S_2 分别独立计算分片结果 $\boldsymbol{f}_1=\boldsymbol{u}_1\pm\boldsymbol{v}_1$ 和 $\boldsymbol{f}_2=\boldsymbol{u}_2\pm\boldsymbol{v}_2$，再发送给数据接收者 D_2，D_2 只需要将数据相加即可得到 $\boldsymbol{f}_1+\boldsymbol{f}_2=\boldsymbol{u}\pm\boldsymbol{v}$。

在安全标量乘法协议中，数据发送方 D_1 将输入数组 $(\boldsymbol{p},\boldsymbol{q})\in Z_n$ 拆分为 $(\boldsymbol{p}_1,\boldsymbol{q})$ 和 $(\boldsymbol{p}_2,\boldsymbol{q})$，分别发送给边缘服务器 S_1 和 S_2，S_1 和 S_2 分别独立计算分片结果 $\boldsymbol{f}_1=\boldsymbol{p}_1\cdot\boldsymbol{q}$ 和 $\boldsymbol{f}_2=\boldsymbol{p}_2\cdot\boldsymbol{q}$，再发送给数据接收者 D_2，D_2 只需要将数据相加即可得到 $\boldsymbol{f}_1+\boldsymbol{f}_2=\boldsymbol{p}\cdot\boldsymbol{q}$。

在安全异或协议中，数据发送方 D_1 将输入数组 $(\boldsymbol{u},\boldsymbol{v})\in Z_n$ 拆分为 $(\boldsymbol{\varepsilon}_1,\boldsymbol{o}_1)$ 和 $(\boldsymbol{\varepsilon}_2,\boldsymbol{o}_2)$，分别发送给边缘服务器 S_1 和 S_2，S_1 和 S_2 分别独立计算分片结果 $\boldsymbol{f}_1=\boldsymbol{\varepsilon}_1\wedge\boldsymbol{o}_1$ 和 $\boldsymbol{f}_2=\boldsymbol{\varepsilon}_2\wedge\boldsymbol{o}_2$，再发送给数据接收者 D_2，D_2 只需要将数据异或即可得到 $\boldsymbol{f}_1\wedge\boldsymbol{f}_2=\boldsymbol{u}\wedge\boldsymbol{v}$。

4.2 安全转换协议

本文将神经网络中的安全比较函数简化为最高有效位(Most Significant Bit，MSB)之间的比较，因此只需要将加法共享转化为异或共享，利用布尔电路实现进位加法运算。

为了处理计算过程中产生的携带位，设计了安全转换协议。

安全与-异或转换协议如协议1所示。给定输入数组 $\boldsymbol{u}_i$ $(i=1,2)$，以补码形式参与计算，安全与-异或转换协议的目标是得到满足 $\boldsymbol{f}_1 \wedge \boldsymbol{f}_2 = \boldsymbol{u}_1 \,\&\, \boldsymbol{u}_2$ 的 $\boldsymbol{f}_i$。T 采用 Beaver 三元组[24]的思想，建立了 $\boldsymbol{\lambda}_i, \boldsymbol{\mu}_i, \boldsymbol{\alpha}_i, \boldsymbol{\beta}_i, \boldsymbol{r}_i, \boldsymbol{\delta}_i$ 之间的关系，它们之间满足 $\boldsymbol{r} \,\&\, \boldsymbol{\delta} = (\boldsymbol{\alpha} \wedge \boldsymbol{\lambda}) \,\&\, (\boldsymbol{\beta} \wedge \boldsymbol{\mu})$，其中 $\boldsymbol{\alpha}$ 代表 $\boldsymbol{u}_1$，$\boldsymbol{\beta}$ 代表 $\boldsymbol{u}_2$，$\wedge$ 代表异或运算，$\&$ 代表与运算。在协议中采用的随机数都是从整环 Z_n 上选择的，其中 n 的位长通常是16位、32位或64位，具体取决于协议的安全需求。S_i 将 $\boldsymbol{u}_i$ 隐藏在中间变量中，然后发送给 S_{3-i}，最后将与共享 $\boldsymbol{u}_i$ 转换成异或共享 $\boldsymbol{f}_i$。

协议1 安全与-异或转换(Secure Transformation From AND to XOR, STAX)

输入：$S_i(i=1,2)$ 拥有 $\mathbf{u}_i \in Z_n$

输出：S_i 返回 $\mathbf{f}_i$

1. T 随机生成 $\boldsymbol{\lambda}_i, \boldsymbol{\mu}_i$，计算
   $\boldsymbol{\lambda} \leftarrow \boldsymbol{\lambda}_1 \wedge \boldsymbol{\lambda}_2, \boldsymbol{\mu} \leftarrow \boldsymbol{\mu}_1 \wedge \boldsymbol{\mu}_2$，随机拆分 $\mathbf{u}_1 \leftarrow \boldsymbol{\alpha}_1 \wedge \boldsymbol{\alpha}_2, \mathbf{u}_2 \leftarrow \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2$；
2. T 计算 $\boldsymbol{\eta} \leftarrow \boldsymbol{\lambda} \,\&\, \boldsymbol{\mu}$，随机拆分 $\boldsymbol{\eta} \leftarrow \boldsymbol{\eta}_1 \wedge \boldsymbol{\eta}_2$，将 $\lambda_i, \boldsymbol{\mu}_i, \boldsymbol{\alpha}_i, \boldsymbol{\beta}_i, \boldsymbol{\eta}_i$ 发送给 S_i；
3. S_i 计算 $\mathbf{r}_i \leftarrow \boldsymbol{\alpha}_i \wedge \boldsymbol{\lambda}_i, \boldsymbol{\delta}_i \leftarrow \boldsymbol{\beta}_i \wedge \boldsymbol{\mu}_i, \mathbf{r} \leftarrow \mathbf{r}_1 \wedge \mathbf{r}_2, \boldsymbol{\delta} \leftarrow \boldsymbol{\delta}_1 \wedge \boldsymbol{\delta}_2$，将 $\mathbf{r}_i, \boldsymbol{\delta}_i$ 发送给 S_{3-i}；
4. S_1 计算 $\mathbf{f}_1 \leftarrow (\boldsymbol{\alpha}_1 \,\&\, \boldsymbol{\delta}) \wedge (\boldsymbol{\beta}_1 \,\&\, \mathbf{r}) \wedge \boldsymbol{\eta}_1$；
5. S_2 计算 $\mathbf{f}_2 \leftarrow (\mathbf{r} \,\&\, \boldsymbol{\delta}) \wedge (\boldsymbol{\alpha}_2 \,\&\, \boldsymbol{\delta}) \wedge (\boldsymbol{\beta}_2 \,\&\, \mathbf{r}) \wedge \boldsymbol{\eta}_2$；
6. S_i 返回 $\mathbf{f}_i$。

为了保护分布隐私，将最高有效位的异或共享转换为加性共享。安全异或-加法转换协议如协议2所示。给定输入数组 $\boldsymbol{u}_i(i=1,2)$，以补码形式参与计算，安全异或-加法转换协议的目标是得到满足 $\boldsymbol{f}_1 + \boldsymbol{f}_2 = \boldsymbol{u}_1 \,\&\, \boldsymbol{u}_2$ 的 $\boldsymbol{f}_i$。单比特位的 $\boldsymbol{u}_1 \,\&\, \boldsymbol{u}_2$ 等价于 $\boldsymbol{u}_1 + \boldsymbol{u}_2 - 2\boldsymbol{u}_1 \cdot \boldsymbol{u}_2$，因此输出 $\boldsymbol{f}_1 + \boldsymbol{f}_2 = \boldsymbol{u}_1 + \boldsymbol{u}_2 - 2\boldsymbol{u}_1 \cdot \boldsymbol{u}_2$。安全乘法(SecMul)[21]协议是基于 Beaver 三元组设计的，给定输入数组 $\boldsymbol{u}_i, \boldsymbol{v}_i(i=1,2)$，通过 $S_i(i=1,2)$ 之间的协同计算 SecMul$(\boldsymbol{u}_1, \boldsymbol{v}_1, \boldsymbol{u}_2, \boldsymbol{v}_2)$ 得到 $\boldsymbol{f}_i$，其中输入输出关系为 $\boldsymbol{f}_1 + \boldsymbol{f}_2 = (\boldsymbol{u}_1 + \boldsymbol{u}_2) \cdot (\boldsymbol{v}_1 + \boldsymbol{v}_2)$。

协议2 安全异或-加法转换(Secure Transformation From XOR to Addition, STXA)

输入：$S_i(i=1,2)$ 拥有 $\mathbf{u}_i \in Z_n$

输出：S_i 返回 $\mathbf{f}_i$

1. S_i 协同计算 $\boldsymbol{\psi}_i \leftarrow \text{SecMul}(\mathbf{u}_1, -2\mathbf{u}_2, -1/2, 1)$；
2. S_i 在本地计算 $\mathbf{f}_i \leftarrow \boldsymbol{\psi}_i + 1/4$；
3. S_i 返回 $\mathbf{f}_i$。

4.3 安全比较协议

安全比较协议如协议3所示。给定输入数组 $\boldsymbol{u}_i(i=1,2)$，以 l 位补码形式 $\boldsymbol{u}_i^{(l-1,\cdots,0)}$ 参与计算，安全比较协议的目标是得到满足 $\boldsymbol{f}_1 \wedge \boldsymbol{f}_2 = \boldsymbol{u}_1 + \boldsymbol{u}_2$ 的 $\boldsymbol{f}_i$。首先，$S_i(i=1,2)$ 协同计算进位结果共享值 $\boldsymbol{\theta}_i^{(l-1,\cdots,0)}$，然后在本地计算最低有效位(Least Significant Bit, LSB)，其中 $\boldsymbol{f}_i^0$ 表示加法结果共享值，$\boldsymbol{c}_i^0$ 表示进位结果共享值。通过从最低位 $j=0$ 迭代到最高位 $j=l-1$，输入共享 $\boldsymbol{u}_i^{(j)}$。加法结果共享 $\boldsymbol{f}_i^{(j)}$ 与进位结果共享 $\boldsymbol{c}_i^{(j)}$ 之间的关系表示为：

$$\boldsymbol{f}_1^{(j)} \wedge \boldsymbol{f}_2^{(j)} \leftarrow (\boldsymbol{u}_1^{(j)} \wedge \boldsymbol{u}_2^{(j)}) \wedge (\boldsymbol{c}_1^{(j-1)} \wedge \boldsymbol{c}_2^{(j-1)}) \tag{2}$$

$$\boldsymbol{c}_1^{(j)} \wedge \boldsymbol{c}_2^{(j)} \leftarrow (\boldsymbol{u}_1^{(j)} \,\&\, \boldsymbol{u}_2^{(j)}) \wedge ((\boldsymbol{u}_1^{(j)} \wedge \boldsymbol{u}_2^{(j)} \,\&\, (\boldsymbol{c}_1^{(j-1)} \wedge \boldsymbol{c}_2^{(j-1)})) \tag{3}$$

S_i 通过调用 STAX 协议计算出进位结果共享 $\boldsymbol{c}_i^{(l-2,\cdots,0)}$，再通过 SecXOR 协议计算得到加法结果 $\boldsymbol{f}_i^{(l-1,\cdots,0)}$。根据最高有效位共享值 $\boldsymbol{f}_i^{l-1}$ 可以推断出输入值的符号，若 $\boldsymbol{f}_1^{l-1} \wedge \boldsymbol{f}_2^{l-1} = 0$，则说明 $\boldsymbol{u}_1 + \boldsymbol{u}_2 \geqslant 0$，否则 $\boldsymbol{u}_1 + \boldsymbol{u}_2 < 0$。

协议3 安全比较(Secure Comparison, SecComp)

输入：$S_i(i=1,2)$ 拥有 $\mathbf{u}_i \in Z_n$

输出：S_i 返回 $\mathbf{f}_i^{(l-1)}$

1. for j=0,…,l−1 do
2. S_i 协同计算 $\boldsymbol{\theta}_i^{(j)} \leftarrow \text{STAX}(\mathbf{u}_1^{(j)}, \mathbf{u}_2^{(j)})$；
3. S_i 在本地计算 $\mathbf{f}_i^0 \leftarrow \mathbf{u}_i^{(0)}$ 和 $\mathbf{c}_i^0 \leftarrow \boldsymbol{\theta}_i^{(0)}$；
4. for j=1,…,l−2 do
5. S_i 协同计算 $\boldsymbol{\varphi}_i^{(j)} \leftarrow \text{STAX}(\mathbf{u}_1^{(j)}, \mathbf{c}_2^{(j-1)})$ 和 $\boldsymbol{\rho}_i^{(j)} \leftarrow \text{STAX}(\mathbf{u}_2^{(j)}, \mathbf{c}_1^{(j-1)})$；
6. S_i 在本地计算 $\mathbf{c}_i^{(j)} \leftarrow (\mathbf{u}_i^{(j)} \,\&\, \mathbf{c}_i^{(j-1)}) \wedge \boldsymbol{\theta}_i^{(j)} \wedge \boldsymbol{\varphi}_i^{(j)} \wedge \boldsymbol{\rho}_i^{(j)}$；
7. for j=0,…,l−1 do
8. S_i 协同计算 $\mathbf{f}_i^{(j)} \leftarrow \text{SecXOR}(\mathbf{u}_i^{(j)}, \mathbf{c}_i^{(j-1)})$；
9. S_i 返回 $\mathbf{f}_i^{(l-1)}$。

5 轻量级隐私保护目标分类框架 LPMS

5.1 图像加密方案

为了保护原始图像隐私，同时防止发送方在上传图像到边缘服务器时数据通信信道被攻击者破坏，本文利用混沌加密技术对原始图像进行加密，整个过程分为初始图像生成、密钥生成、图像加密、图像解密4个阶段。

1)初始图像生成阶段：数据发送方 D_1 使用随机生成器生成一个随机图像 I_1。具体来说，定义 I_1 的随机生成空间为 $[-2^n-1, 2^{n-1}-1]$，其中 $n \geqslant 8$ 为安全参数，因为当 $n \geqslant 8$ 时生成的图像完全无法识别，所以取 $n \geqslant 8$ 随机生成图像 I_1，再用原始图像 I 减去 I_1 得到 I_2。

2)密钥生成阶段：结合 Henon 映射与 Sine 映射构造了一种新的高效三维混沌映射：

$$\begin{cases} \boldsymbol{X}_{n+1} = 1 + \boldsymbol{Y}_n + a\boldsymbol{Y}_n^2 \\ \boldsymbol{Y}_{n+1} = b\sin(\pi \boldsymbol{X}_n) \\ \boldsymbol{Z}_{n+1} = \boldsymbol{X}_n + \boldsymbol{Y}_n + C\boldsymbol{Z}_0 \end{cases} \tag{4}$$

假设图像大小为 (ψ_1, ψ_2, ψ_3)，为了使构造的混沌映射处于混沌状态，将其控制参数元组 (a, b, c) 设为 $(12.56, 0.87, 1)$，使用输入 $(\boldsymbol{X}_0, \boldsymbol{Y}_0, \boldsymbol{Z}_0) = (0.5, 0.5, 0.5)$ 对式(4)中的混沌映射迭代 $\psi_1\psi_2\psi_3$ 次，得到3个长度为 $\psi_1\psi_2\psi_3$ 的混沌序列 $\boldsymbol{X}, \boldsymbol{Y}$ 和 $\boldsymbol{Z}$。为了得到的混沌序列是周期性的，使用正弦函数对上述序列进行处理，得到在区间 $[0,1]$ 以内较长周期的混沌序列 $\boldsymbol{\varphi}_1 = \boldsymbol{Y}^2$ 和 $\boldsymbol{\varphi}_2 = \sin^2(\boldsymbol{X} + \boldsymbol{Z})/2$。为了使随机特性更加理想以及混淆图像像素值，进一步将序列值混淆到 $[0,255]$。执行变换 $\boldsymbol{\delta}_1 = (10^{16}\boldsymbol{\varphi}_1 - round(10^{16}\boldsymbol{\varphi}_1)) \bmod 256$ 和 $\boldsymbol{\delta}_2 = (10^{16}\boldsymbol{\varphi}_2 - round(10^{16}\boldsymbol{\varphi}_2)) \bmod 256$，其中 10^{16} 为延长周期，$round(\cdot)$ 为取最接近整数运算。$\boldsymbol{\delta}_1$ 和 $\boldsymbol{\delta}_2$ 序列的值在像素间隔内近似随机分布 $[0,255]$，因此将 $\boldsymbol{\delta}_1$ 和 $\boldsymbol{\delta}_2$ 序列作为初始加密密钥。

3)图像加密阶段：首先将发送给边缘服务器的图像拉伸成长度为 $\psi_1 \cdot \psi_2 \cdot \psi_3$ 的流序列，然后依次进行两轮加密，如式(5)和式(6)所示：

$$\begin{cases} P_i(1) = I_i(1) \wedge \boldsymbol{\delta}_1(1) \\ P_i(k) = ((I_i(k) + \boldsymbol{\delta}_1(k-1) + P_i(k-1)) \bmod 256) \wedge \boldsymbol{\delta}_1(k) \end{cases} \tag{5}$$

$$\begin{cases} E_i(1)=P_i(1)\wedge\boldsymbol{\delta}_2(1) \\ E_i(k)=(P_i(k))\wedge((E_i(k-1)+\boldsymbol{\delta}_2(k) \bmod 256)\wedge\boldsymbol{\delta}_2(k-1)) \end{cases} \tag{6}$$

其中，$P_i(i=1,2)$为第一轮加密后的加密序列，$E_i(i=1,2)$为第二轮加密后的加密序列。

4）图像解密阶段：边缘服务器 S_1 和 S_2 在接收到加密图像 E_1 和 E_2 之后，首先需要进行逆向加密操作，其中第一轮解密是第二轮加密的逆向操作，第二轮解密是第一轮加密的逆向操作，由可信第三方 T 提供解密密钥 $\boldsymbol{\delta}_1$ 和 $\boldsymbol{\delta}_2$，解密之后得到图像 I_1 和 I_2。解密操作如式(7)和式(8)所示：

$$\begin{cases} P_i(k)=(E_i(k))\wedge((E_i(k-1)+\boldsymbol{\delta}_2(k) \bmod 256)\wedge\boldsymbol{\delta}_2(k-1)) \\ P_i(1)=E_i(1)\wedge\boldsymbol{\delta}_2(1) \end{cases} \tag{7}$$

$$\begin{cases} I_i(k)=((P_i(k)\wedge\boldsymbol{\delta}_1(k))-\boldsymbol{\delta}_1(k-1)-P_i(k-1)) \bmod 256 \\ I_i(1)=P_i(1)\wedge\boldsymbol{\delta}_1(1) \end{cases} \tag{8}$$

然后 S_i 在 I_i 上执行 LPMS 进行目标分类，最终得到两个分类结果 C_i。下面将介绍各个网络层中的实现过程。

5.2 安全的神经网络架构

常见的神经网络架构通常由卷积层、激活层、池化层和全连接层 4 种层组成。为了实现安全的神经网络目标分类，本文在两台边缘服务器之间设计了一系列安全计算协议，整体架构如图 2 所示，每一层的安全协议组成了 LPMS 的构建块。

1）安全卷积层和安全全连接层：由于卷积层只涉及线性运算，即在过滤器和输入之间的局部区域做点积，只涉及加法操作和乘法操作，因此可以直接通过安全加法协议(SecAdd)和安全标量乘法协议(SecSMul)来实现。卷积运算如式(9)所示：

$$\boldsymbol{y}_{m,n}=\sum_{i=0}^{l-1}\sum_{j=0}^{l-1}w_{i,j}\otimes\boldsymbol{x}_{m+i,n+j}+\boldsymbol{b} \tag{9}$$

其中，$\boldsymbol{x}_{m,n}$表示在位置(m,n)处的特征矩阵，$\boldsymbol{w}_{i,j}$表示大小为(l,l)的卷积核权值，$\boldsymbol{b}$表示卷积核偏置，$\boldsymbol{y}_{m,n}$表示该层的卷积结果输出，$\otimes$表示卷积核与特征图进行卷积操作。在 LPMS 中，$\boldsymbol{x}_i$ 被拆分为两个随机份额 $\boldsymbol{x}_1'$和 $\boldsymbol{x}_2'$，$S_i(i=1,2)$在本地计算 $\boldsymbol{y}_i=SecAdd(SecSMul(\boldsymbol{x}_i',\boldsymbol{w}),\boldsymbol{b})$，将计算结果发送给 D_2 即可得到卷积结果 $\boldsymbol{y}(\boldsymbol{y}=\boldsymbol{y}_1+\boldsymbol{y}_2)$。

与卷积层类似，全连接层只涉及线性运算，即点积操作。给定前一层神经元与当前层神经元的连接权值和特征向量，$S_i(i=1,2)$通过调用安全加法协议、安全减法协议和安全标量乘法协议，可以实现矩阵乘法和偏置计算，前向传播过程也可以在本地完成。

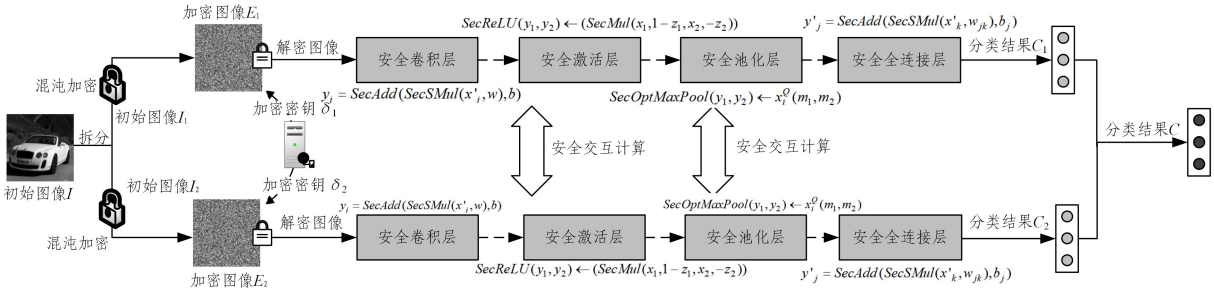

图 2 LPMS 架构

Fig. 2 Architecture of LPMS

2）安全激活层：在卷积神经网络中，ReLU 函数是最常用的激活函数，函数表达式为 $f(\boldsymbol{x})=\max(0,\boldsymbol{x})$，目的是抑制小于 0 的特征输出，可以一定程度上缓解过拟合现象。因此，本文在安全比较协议(SecComp)的基础上设计了安全 ReLU 协议，以实现和普通 ReLU 函数相同的功能效果，如协议 4 所示。

协议 4 安全 ReLU(Secure ReLU，SecReLU)

输入：$S_i(i=1,2)$拥有输入特征 $\mathbf{x}_i\in Z_n$

输出：S_i 返回激活特征 $\mathbf{y}_i$

1. S_1 协同 S_2 计算$(\boldsymbol{\omega}_1,\boldsymbol{\omega}_2)\leftarrow$SecComp$(\mathbf{x}_1,\mathbf{x}_2)$；
2. S_1 协同 S_2 计算$(\mathbf{z}_1,\mathbf{z}_2)\leftarrow$STXA$(\boldsymbol{\omega}_1,\boldsymbol{\omega}_2)$；
3. S_1 和 S_2 协同计算
   $(\mathbf{y}_1,\mathbf{y}_2)\leftarrow$SecMul$(\mathbf{x}_1,1-\mathbf{z}_1,\mathbf{x}_2,-\mathbf{z}_2)$；
4. S_i 返回 $\mathbf{y}_i$。

给定输入特征 $\boldsymbol{x}_1$ 和 $\boldsymbol{x}_2(\boldsymbol{x}=\boldsymbol{x}_1+\boldsymbol{x}_2)$，$S_1$ 和 S_2 通过协同调用安全比较协议获取最高有效位的共享份额 $\boldsymbol{\omega}_i$。同时，为保护激活特征的数据分布隐私，通过安全异或-加法转换协议将最高有效位的异或共享转换为加法共享。最后通过调用安全乘法协议，S_1 和 S_2 可以得到 ReLU 共享 $\boldsymbol{y}_1$ 和 $\boldsymbol{y}_2$，它们之间满足 $\boldsymbol{y}_1+\boldsymbol{y}_2=(\boldsymbol{x}_1+\boldsymbol{x}_2)\cdot(1-(\boldsymbol{z}_1+\boldsymbol{z}_2))$。如果 $\boldsymbol{z}_1+\boldsymbol{z}_2=0$，则 $\boldsymbol{y}_1+\boldsymbol{y}_2=\boldsymbol{x}_1\boldsymbol{x}_2$；否则，$\boldsymbol{y}_1+\boldsymbol{y}_2=0$。

3）安全池化层：在卷积神经网络中，通常使用池化层提高所提取特征的鲁棒性，最大池化可以提取出指定窗口的特征(最大)数据，显著减少特征张量的大小。为了保护特征隐私，本文设计了安全最大池化协议，如协议 5 所示。给定输入特征 $\boldsymbol{x}_i$，S_1 和 S_2 协同计算每一个池化区域 Q 的最大值。在特定的 3×3 的池化区域 Q 内，最大值的二维位置索引初始化为(m_1,m_2)。S_1 和 S_2 之间不能直接交换特征值，而是以差值的形式计算位置索引(m_1,m_2)和(u,v)之间的份额，这样可以避免透露具体的特征值。通过不断更新最大值的索引(m_1,m_2)，S_i 可以得到池化区域 Q 的最大值 $\boldsymbol{y}_i^Q$，依次对每个池化区域进行遍历，S_i 可以安全获取最大池化的特征共享值 $\boldsymbol{y}_i$。

协议 5 安全最大池化(Secure Max Pooling，SecMaxPool)

输入：$S_i(i=1,2)$拥有输入特征 $\mathbf{x}_i\in Z_n$

输出：S_i 返回最大池化特征 $\mathbf{y}_i$

1. foreach 池化区域 Q do
2. S_i 初始化 $m_1,m_2\leftarrow0$；
3. for u，v in(1，1)→(3，3) do
4. S_i 计算 $\delta_i\leftarrow\mathbf{x}_i^Q(m_1,m_2)-\mathbf{x}_i^Q(u,v)$；
5. if $\delta_i<0$ then

S_i 将 δ_i 发送给 S_{3-i}；
S_i 在本地计算 $\delta \leftarrow \delta_i + \delta_{3-i}$；
if $\delta < 0$ then
  S_i 赋值为 $m_1 \leftarrow u, m_2 \leftarrow v$；
  S_i 计算 $\mathbf{y}_i^Q \leftarrow \mathbf{x}_i^Q(m_1, m_2)$；
S_i 返回 $\mathbf{y}_i$。

6 理论分析

6.1 复杂性分析

首先，本文分析了密钥生成，图像加密和解密的计算复杂度。密钥是由几个混沌序列值组成的流序列。为了对大小为 $\psi_1\psi_2\psi_3$ 的图像进行加密，密钥生成的计算复杂度取决于图像大小，即 $O(\psi_1\psi_2\psi_3)$。加密和解密的迭代过程只包含模和异或操作，因此计算复杂度也为 $O(\psi_1\psi_2\psi_3)$。假设输入位宽为 l bit，由于密钥的长度与图像的大小是一一对应的，因此 T 只需要进行一轮离线通信，密钥传输的开销为 $2\psi_1\psi_2\psi_3 l$。

其次，本文详细分析了所提出的安全协议的计算复杂度和通信复杂度。由于 T 可在离线阶段完成计算，其开销可以忽略不计。假设每个安全协议的输入大小为 n，对于安全非交互协议（SecAdd/SecSub，SecSMul，SecXOR），S_i 无需交互通信，仅需在本地完成一些线性计算。因此，这些安全非交互协议的计算复杂度为 $O(n)$。从表 1 可以看出，在安全异或-加法转换和安全与-异或转换中，LPMS 的计算复杂度均为 $O(n)$，这得益于优化的本地计算机制有效提升了转换效率。安全比较协议和安全 ReLU 协议的计算复杂度为 $O(nl)$，与文献[16]和文献[25]中的结果相同，其中 l 表示输入位宽。尽管计算复杂度相同，但在通信开销方面，安全异或-加法转换协议和安全与-异或转换协议减少了每次通信传输的消息量，使得安全比较协议和安全 ReLU 协议的通信开销分别降至 $n(3l-4)$ 和 $n(6l-4)$，显著优于文献[16]（见表 2）。此外，安全比较协议和安全 ReLU 协议还分别减少了一轮通信，从而进一步降低了实际运行的时间成本。

表 1 安全计算协议的计算复杂度对比

Table 1 Comparison of the computational complexity of secure computing protocols

协议	文献[5]	文献[16]	文献[25]	LPMS
安全异或-加法转换	—	—	—	$O(n)$
安全与-异或转换	—	—	$O(n)$	$O(n)$
安全比较	—	$O(nl)$	$O(nl)$	$O(nl)$
安全 ReLU	$O(n)$	$O(nl)$	$O(nl)$	$O(nl)$
安全最大池化	$O(3n/4)$	$O(3nl/4)$	$O(3n/4)$	$O(3n/4)$

表 2 安全计算协议的通信复杂度对比

Table 2 Comparison of the communication complexity of secure computing protocols

协议	文献[16]		LPMS	
	轮数	通信开销	轮数	通信开销
安全异或-加法转换	—	—	1	nl
安全与-异或转换	—	—	1	nl
安全比较	$l+1$	$n(10l-4)$	l	$n(3l-4)$
安全 ReLU	$l+3$	$n(13l-4)$	$l+2$	$n(6l-4)$
安全最大池化	$3n(l+3)/4$	$3n(13l-4)/4$	$3n/4$	$3nl/4$

在卷积层和全连接层中，计算过程仅涉及安全加法和安全标量乘法，无需在 S_i 之间进行交互，计算复杂度为 $O(l^2(m-l+1)(n-l+1))$。在激活层中，为了实现非线性变换，首先通过调用安全比较协议获取输入值的最高有效位，再采用安全异或-加法转换协议将最高有效位的异或共享转换为加性共享，以实现更高效的后续计算。在此基础上，安全 ReLU 协议利用最高有效位作为输入完成非线性激活，其计算复杂度为 $O(nl)$，通信开销为 $3nl$，因为 S_i 需要三轮通信来分别执行安全比较协议、安全异或-加法转换协议以及安全乘法协议。在池化层中，为了对输入数据进行降维处理和特征提取，采用了安全最大池化协议。与基于安全比较协议的设计不同，本文提出的安全最大池化协议使用了交换差策略，避免了复杂的安全比较操作。因此，池化层的通信开销显著低于文献[16]，为 $3nl/4$。

6.2 正确性分析

由于线性计算具有可拆分性，因此安全标量乘法协议（SecSMul）、安全加法协议（SecAdd）、安全减法协议（SecSub）、安全异或协议（SecXOR）显然是正确的。在安全与-异或转换协议（STAX）中，可以将计算过程分解为：由于 $\boldsymbol{\alpha} = \boldsymbol{\alpha}_1 \wedge \boldsymbol{\alpha}_2$，$\boldsymbol{\delta} = \boldsymbol{\beta} \wedge \boldsymbol{\mu}$，所以 $(\boldsymbol{\alpha}_1 \& \boldsymbol{\delta}) \wedge (\boldsymbol{\alpha}_2 \& \boldsymbol{\delta}) = \boldsymbol{\alpha} \& \boldsymbol{\delta} = (\boldsymbol{\alpha} \& \boldsymbol{\beta}) \wedge (\boldsymbol{\alpha} \& \boldsymbol{\mu})$；又由于 $\boldsymbol{\beta} = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2$，$\boldsymbol{r} = \boldsymbol{\alpha} \wedge \boldsymbol{\lambda}$，因此 $\boldsymbol{f}_1 \wedge \boldsymbol{f}_2 = (\boldsymbol{\alpha} \& \boldsymbol{\delta}) \wedge (\boldsymbol{\beta} \& \boldsymbol{r}) \wedge (\boldsymbol{r} \& \boldsymbol{\delta}) \wedge (\boldsymbol{\eta}_1 \wedge \boldsymbol{\eta}_2) = \boldsymbol{\alpha} \& \boldsymbol{\beta}$，因此 $\boldsymbol{f}_1 \wedge \boldsymbol{f}_2 = \boldsymbol{u}_1 \& \boldsymbol{u}_2$，即安全与-异或转换协议是正确的。

在安全异或-加法转换协议（STXA）中，由于 $\boldsymbol{\psi}_1 \cdot \boldsymbol{\psi}_2 = (\boldsymbol{u}_1 - 1/2) \cdot (1 - 2\boldsymbol{u}_2) = \boldsymbol{u}_1 + \boldsymbol{u}_2 - 2\boldsymbol{u}_1\boldsymbol{u}_2 - 1/2$，因此 $\boldsymbol{f}_1 + \boldsymbol{f}_2 = \boldsymbol{\psi}_1 + \boldsymbol{\psi}_2 + 1/2 = \boldsymbol{u}_1 + \boldsymbol{u}_2 - 2\boldsymbol{u}_1\boldsymbol{u}_2$；由于单比特位的 $\boldsymbol{u}_1 \& \boldsymbol{u}_2$ 等价于 $\boldsymbol{u}_1 + \boldsymbol{u}_2 - 2\boldsymbol{u}_1\boldsymbol{u}_2$，因此 $\boldsymbol{f}_1 + \boldsymbol{f}_2 = \boldsymbol{u}_1 \& \boldsymbol{u}_2$。在安全比较协议（SecComp）中，当 $j = 0$ 时，$\boldsymbol{f}^{(0)} = \boldsymbol{u}^{(0)}$；当 $j = 1, \cdots, l-1$ 时，$\boldsymbol{f}_1^{(j)} \wedge \boldsymbol{f}_2^{(j)} = (\boldsymbol{u}_1^{(j)} \wedge \boldsymbol{u}_2^{(j)}) \wedge (\boldsymbol{c}_1^{(j-1)} \wedge \boldsymbol{c}_2^{(j-1)})$。因此，$\boldsymbol{f}_1^{(l-1,\cdots,0)} \wedge \boldsymbol{f}_2^{(l-1,\cdots,0)} = \boldsymbol{u}_1 + \boldsymbol{u}_2$，其中 $\boldsymbol{f}^{(l-1)} = \boldsymbol{f}_1^{(l-1)} \wedge \boldsymbol{f}_2^{(l-1)}$ 为最高有效位的输入。负数以补码形式计算，因此安全异或-加法转换协议和安全比较协议是正确的。

此外，本文使用这些安全计算协议来实现卷积神经网络中的正常计算。调用安全加法/减法协议和安全标量乘法协议能够正常实现卷积层和全连接层。在激活层中，安全比较协议和安全异或-加法转换协议已被证明是正确的，根据最高有效位的异或共享 $\boldsymbol{\omega}_i$，可以通过安全异或-加法转换协议得到加性共性 $\boldsymbol{z}_i$，满足 $\boldsymbol{z}_1 + \boldsymbol{z}_2 = \boldsymbol{\omega}_1 + \boldsymbol{\omega}_2$。激活层中 ReLU 的结果为 $\boldsymbol{y} = \boldsymbol{x} \cdot (1 - \boldsymbol{z})$。如果 $\boldsymbol{x} \geqslant 0$，则 $\boldsymbol{z} = 0, 1 - \boldsymbol{z} = 1, \boldsymbol{y} = \boldsymbol{x}$；当 $\boldsymbol{x} < 0$ 时，则 $\boldsymbol{z} = 1, 1 - \boldsymbol{z} = 0, \boldsymbol{y} = 0$。在池化层中，核心操作为安全最大池化协议中的 3 个比较。$\delta = (\boldsymbol{x}_1(m_1, m_2) - \boldsymbol{x}_1(u, v)) + (\boldsymbol{x}_2(m_1, m_2) - \boldsymbol{x}_2(u, v)) = \boldsymbol{x}(m_1, m_2) - \boldsymbol{x}(u, v)$，如果 $\delta < 0$，则表示 $\boldsymbol{x}(m_1, m_2) < \boldsymbol{x}(u, v)$，索引 (m_1, m_2) 需要更新为 (u, v)，比较后索引 (m_1, m_2) 属于池化区域中 Q 的最大值。因此，激活层和池化层执行过程是正确的。

最后，本文的图像分割和图像加解密涉及的计算显然是正确的，即 $I = I_1 + I_2$ 和 $C = C_1 + C_2$。图像加密和解密是一组逆向操作，对于图像 I_i 的第一个像素值，$P_i(1) = I_i(1) \wedge \boldsymbol{\delta}_1(1)$，$E_i(1) = P_i(1) \wedge \boldsymbol{\delta}_2(1)$，因此 $I_i(1) = P_i(1) \wedge \boldsymbol{\delta}_1(1)$。对于剩余的像素值，第一轮加密 $P_i(k) = ((I_i(k) + \boldsymbol{\delta}_1(k-1) + P_i(k-1)) \bmod 256) \wedge \boldsymbol{\delta}_1(k)$ 对应第二轮解密 $I_i(k) =$

$((P_i(k)\wedge\boldsymbol{\delta}_1(k))-\boldsymbol{\delta}_1(k-1)-P_i(k-1))$ mod 256，而第二轮加密 $E_i(k)=(P_i(k))\wedge((E_i(k-1)+\boldsymbol{\delta}_2(k)\ \text{mod}\ 256)\wedge\boldsymbol{\delta}_2(k-1))$则对应第一轮解密 $P_i(k)=(E_i(k))\wedge((E_i(k-1)+\boldsymbol{\delta}_2(k)\ \text{mod}\ 256)\wedge\boldsymbol{\delta}_2(k-1))$。因此，以上加解密过程是正确的。

6.3 安全性分析

在半诚实模型中，两台边缘服务器 S_1 和 S_2 互不串通，概率多项式时间敌手 K 只能破坏并获取 S_1 和 S_2 中最多一个的特征信息。为更好地证明安全性，本文将定义形式化如下。

定义 1 如果存在一个概率多项式时间模拟器 M，它可以为现实世界中的敌手 K 生成一个视图 $View_{\text{virt}}$，并且该视图在计算上与其真实视图 $View_{\text{real}}$ 无法区分，则协议是安全的。

引理 1 如果一个协议的所有子协议都是完全可模拟的，那么这个协议就是完全可模拟的[26]。

引理 2 如果一个随机元素 a 均匀分布在 Z_n 上且独立于任何变量 $b\in Z_n$，则 $a\pm b$ 也是均匀随机的，且独立于 b[20]。

由于本文协议可以在实践中进行模拟，因此需要引入上述引理以辅助证明过程。

定理 1 安全加法/减法(SecAdd/SecSub)协议、安全异或(SecXOR)协议和安全标量乘法(SecSMul)协议在半诚实模型中是安全的。

证明 对于安全加法/减法(SecAdd/SecSub)协议，S_1 和 S_2 的真实视图 $View_{\text{real}}$ 是$\{\boldsymbol{u}_1,\boldsymbol{v}_1,\boldsymbol{f}_1\}$和$\{\boldsymbol{u}_2,\boldsymbol{v}_2,\boldsymbol{f}_2\}$。概率多项式时间模拟器 M 能够很容易地生成相应的仿真视图 $View_{\text{virt}}$，K 无法在计算上区分 $View_{\text{real}}$ 和仿真视图 $View_{\text{virt}}$。同理，对于安全异或(SecXOR)协议，S_1 和 S_2 的真实视图 $View_{\text{real}}\{\boldsymbol{\varepsilon}_1,\boldsymbol{o}_1,\boldsymbol{f}_1\}$和$\{\boldsymbol{\varepsilon}_2,\boldsymbol{o}_2,\boldsymbol{f}_2\}$。安全标量乘法协议中的 $View_{\text{real}}$是$\{\boldsymbol{p}_1,\boldsymbol{q}\}$和$\{\boldsymbol{p}_2,\boldsymbol{q}\}$，其中 $\boldsymbol{q}$ 是一个公共值。由此证明了安全加法/减法协议、安全异或协议和安全标量乘法协议在半诚实模型中是安全的。证毕。

定理 2 安全与-异或转换(STAX)协议、安全异或-加法转换协议(STXA)和安全比较协议(SecComp)在半诚实模型中是安全的。

证明 对于安全与-异或转换(STAX)协议，输入 $u_i(i=1,2)$是均匀随机的。从 $S_i(i=1,2)$的角度看，$View_{\text{real}}$为$\{\boldsymbol{u}_i,\boldsymbol{\lambda}_i,\boldsymbol{\mu}_i,\boldsymbol{\alpha}_i,\boldsymbol{\beta}_i,\boldsymbol{\eta}_i,\boldsymbol{r}_i,\boldsymbol{\delta}_i,\boldsymbol{f}_i\}$。由于$\{\boldsymbol{\lambda}_i,\boldsymbol{\mu}_i,\boldsymbol{\alpha}_i,\boldsymbol{\beta}_i,\boldsymbol{\eta}_i\}$是由 T 离线生成的随机数，因此根据引理 1 得出 $\boldsymbol{r}_i$ 和 $\boldsymbol{\delta}_i$ 也是均匀随机的。S_i 不能从 $\boldsymbol{r}_1\wedge\boldsymbol{r}_2$ 和 $\boldsymbol{\delta}_1\wedge\boldsymbol{\delta}_2$ 中推断出真实的输入 $\boldsymbol{u}$，但可以得出输出 $\boldsymbol{f}_i$。因此，真实视图 $View_{\text{real}}$对于 M 是可模拟的，并且在计算上 K 无法区分真实视图 $View_{\text{real}}$ 和仿真视图 $View_{\text{virt}}$。由于安全与-异或转换(STAX)协议可以模拟，因此根据引理 1 得出安全比较(SecComp)协议也是可以模拟的，S_i 的 $View_{\text{real}}$为$\{\boldsymbol{u}_i,\boldsymbol{\theta}_i,\boldsymbol{\varphi}_i,\boldsymbol{\rho}_i,\boldsymbol{f}_i\}$，安全与-异或转换(STAX)协议已被证明是安全的，并且$\{\boldsymbol{\theta}_i,\boldsymbol{\varphi}_i,\boldsymbol{\rho}_i\}$是均匀随机的，$S_i$ 可以得到输出 $\boldsymbol{f}_i$，其中 $\boldsymbol{f}_1\wedge\boldsymbol{f}_2=\boldsymbol{u}_1+\boldsymbol{u}_2$。显然，最高有效位 $\boldsymbol{f}_i^{l-1}$ 也是均匀随机的，M 可以生成 S_i 的仿真视图 $View_{\text{virt}}$，在计算上 K 无法区分真实视图 $View_{\text{real}}$ 和仿真视图 $View_{\text{virt}}$。对于安全异或-加法转换(STXA)协议，安全乘法(SecMul)协议在文献[19]中已被证明在半诚实模型中是安全的，S_i 的 $View_{\text{real}}$为$\{\boldsymbol{u}_i,\boldsymbol{\psi}_i,\boldsymbol{f}_i\}$，不能从 $\boldsymbol{\psi}_1+\boldsymbol{\psi}_2$ 中推断出真实的输入 $\boldsymbol{u}$，但可以得出输出 $\boldsymbol{f}_i$，真实视图 $View_{\text{real}}$对于 M 是可模拟的，并且在计算上 K 无法区分真实视图 $View_{\text{real}}$ 和仿真视图 $View_{\text{virt}}$。由此证明了安全与-异或转换(STAX)协议、安全异或-加法转换协议(STXA)和安全比较协议(SecComp)在半诚实模型中是安全的。证毕。

定理 3 安全 ReLU(SecReLU)协议和安全最大池化(SecMaxPool)协议在半诚实模型中是安全的。

证明 由于安全比较(SecComp)协议的安全性在定理 2 中得到了证明，安全乘法(SecMul)协议在文献[16]中得到了证明，因此，$\{\boldsymbol{\omega}_i,\boldsymbol{z}_i,\boldsymbol{y}_i\}$是均匀随机的。由于安全比较协议和安全乘法协议是可以模拟的，因此安全 ReLU(SecReLU)协议可以由 M 根据引理 1 进行模拟，S_i 无法在计算上区分 $View_{\text{real}}$和 $View_{\text{virt}}$。对于安全最大池化(SecMaxPool)协议，输入 $\boldsymbol{x}_i$ 是均匀随机的，S_i 的 $View_{\text{real}}$为$\{\boldsymbol{x}_i,\delta_1,\delta_2,m_1,m_2,\boldsymbol{y}_i\}$。即使 S_i 得到 δ_1 和 δ_2，也无法恢复 $\boldsymbol{x}^Q(u,v)$。因此，对于 K 来说，由 M 生成的 $View_{\text{real}}$ 和 $View_{\text{virt}}$ 在计算上是不可区分的。由此证明了安全 ReLU(SecReLU)协议和安全最大池化(SecMaxPool)协议在半诚实模型中是安全的。证毕。

定理 4 在半诚实模型中，图像加密、图像解密和 LPMS 中的图像处理是安全的。

证明 在图像加密过程中，移动传感设备 D_1 随机将图像 I 拆分为 I_1 和 I_2，并加密成 E_1 和 E_2，然后 D_1 将密文图像 E_1 和 E_2 分别发送给 S_1 和 S_2。如果敌手 K 通过攻击 S_1 或 S_2 获取到 I_1 或 I_2，这样并不能恢复原始图像 I，但如果 K 能够直接破坏 D_1 和 S_1 之间的通信链路以及 D_1 和 S_2 之间的通信链路，甚至直接攻击 D_1，那么 K 就可以很容易地获取到原始图像 I。这是一个非常实际的安全问题，本文描述的图像加密方案就是为了避免这种情况而设计的。由于 $E_1+E_2\neq I$，即使 K 同时获得 E_1 和 E_2 也无法获取任何有意义的信息。在图像解密的过程中，S_1 和 S_2 将提取到的分类特征 C_1 和 C_2 发送给数据接收方 D_2，D_2 通过计算 C_1+C_2 可以安全地得到分类结果 C，不会泄露任何图像隐私。此外，LPMS 使用安全加法(SecAdd)协议、安全减法(SecSub)协议和安全标量乘法(SecSMul)协议实现卷积层和全连接层的操作，使用安全 ReLU(SecReLU)协议和安全最大池化(SecMaxPool)协议实现激活层和池化层的操作。以上协议已被证明是安全的，因此 LPMS 中的图像处理也是安全的。证毕。

7 实验结果

由于本文框架是为移动传感体系设计的，因此选择了 KITTI 数据集[27]来训练和测试本文模型。为了匹配目标分类任务，首先对 KITTI 数据集进行处理，从 KITTI 数据集提供的每一帧图像中手动裁剪出车辆和行人，总共包含 3 000 个训练样本和 750 个测试样本，每个样本的大小都是一张 $3\times224\times224$ 的 RGB 图像。所有实验均在 CPU 为 1.8 GHz，RAM 为 20 GB 的 64 位个人计算机和 PyCharm 仿真平台上进行，Numpy 包被用作数字的多维容器，以

并行执行安全计算协议。

7.1 图像加密方案性能

为了衡量图像加密方案的性能，本文对加密和解密开销进行了评估。在加密阶段，移动传感设备 D_1 将原始图像 I 随机拆分为两个图像 I_1 和 I_2，并对其进行加密，得到加密图像 E_1 和 E_2，两台边缘服务器接收加密图像后分别进行解密。对 KITTI 数据集中的 750 张图像进行加密，通信开销如表 3 所列。

表 3 图像加解密通信开销对比

Table 3 Comparison of communication overhead of image encryption and decryption

方案	加密阶段信息量大小/MB	解密阶段信息量大小/MB
CryptoNets[10]	4306.638	175.781
LPMS	144.51	6.013

在本文加密方案中，每张图像由 224×224 像素组成，每个像素存储为 4 个字节。对于使用同态加密的 CryptoNets 方案，每个像素被加密为 5 个多项式，每个多项式的系数存储为 24 个字节。因此，在加密和解密阶段，CryptoNets 的通信开销分别为 4306.638 MB 和 175.781 MB，而本文方案的通信开销仅为 144.51 MB 和 6.013 MB，明显低于 CryptoNets 方案。

7.2 安全计算协议性能

本文设计的安全计算协议旨在安全实现目标分类任务，影响其通信开销性能的主要因素为输入位宽 l。由图 3(a)可以看出，安全比较协议的通信开销随着输入位宽 l 的增加而增加。与文献[16]的安全比较协议相比，本文的安全比较协议可以减少约 2/3 的通信开销，在输入位宽 l 为 64 时，本文的安全比较协议的通信开销为 22.68 B，远小于文献[16]的安全比较协议的通信开销。由图 3(b)和图 3(c)可以看出，安全 ReLU 协议和安全最大池化协议的通信开销随着输入位宽 l 的增加而增加。本文的安全 ReLU 协议和安全最大池化协议在通信开销方面显著优于文献[16]。

此外，安全比较协议的计算误差可以忽略不计。由于将定点数的小数部分转换为整数域进行计算，因此安全比较协议可以准确地确定输入与 0 之间的关系。因此，安全 ReLU 协议在使用安全比较协议时没有计算误差。由于卷积层、池化层和全连接层不涉及近似计算，因此它们的误差始终保持在 0。

影响本文安全协议计算开销性能的主要因素为并行批大小。从图 3(d)中可以看出，安全比较协议的运行时间随着并行批大小的增加而增加。即使并行处理多个输入，安全比较协议的运行时间也可以控制在 16 ms 以内。与文献[16]的安全协议相比，本文的安全比较协议的效率随着批大小的增加变化得更加明显。

由图 3(e)可以看出，安全 ReLU 协议的运行时间随着并行批大小的增加而增加。当并行批大小在 $10^1 \sim 10^3$ 时，安全 ReLU 协议的运行时间略高于原始 ReLU 函数；当并行批大小增加到 10^5 时，安全 ReLU 协议的运行时间为 20.58 ms，但总体上依旧优于文献[16]。从图 3(f)中可以看出，安全最大池化协议的运行时间随着并行批大小的增加而增加。当并行批大小在 $10^1 \sim 10^4$ 时，安全最大池化协议的运行时间略高于原始最大池化；当并行批大小增加到 10^5 时，安全最大池化协议的运行时间为 3.58 ms，优于文献[16]中的 15.89 ms。此外，安全最大池化协议在最大池化层采用了交换差的贝叶斯方法，而不是使用安全比较协议，降低了计算成本。

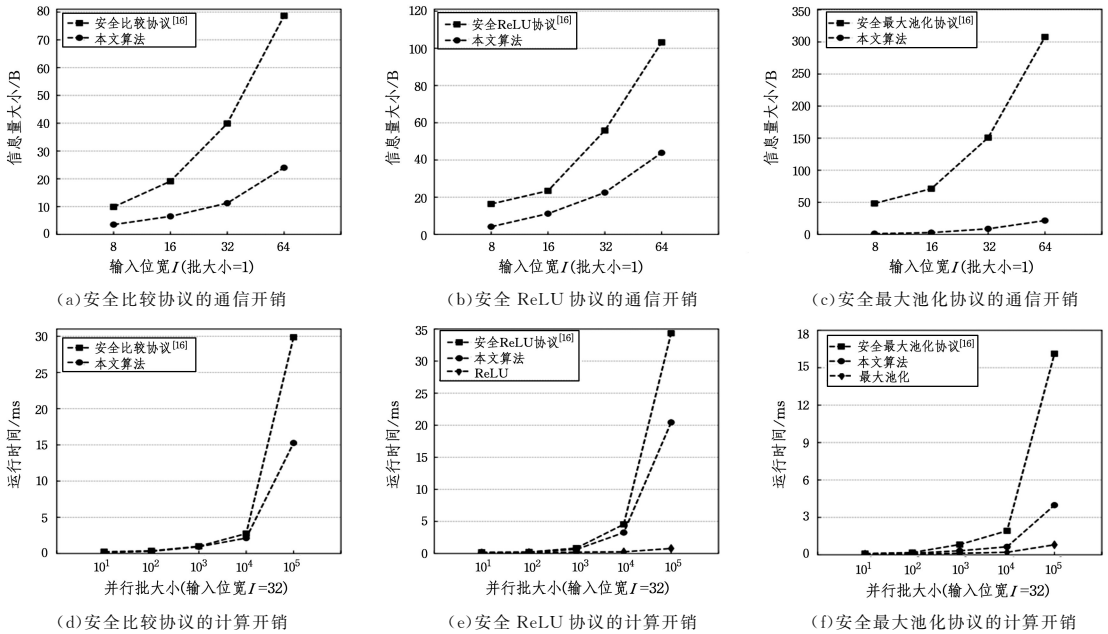

图 3 安全计算协议的性能对比

Fig. 3 Comparison of the performance of secure computing protocols

7.3 目标分类框架性能

隐私保护目标分类框架采用本文设计的安全层协议对加密图像进行隐私计算。为进行性能对比，本文在包含 2 个卷积层、3 个激活层、2 个最大池化层和 2 个全连接层的卷积神经网络上测试了不同的方案，具体网络结构如图 4 所示。

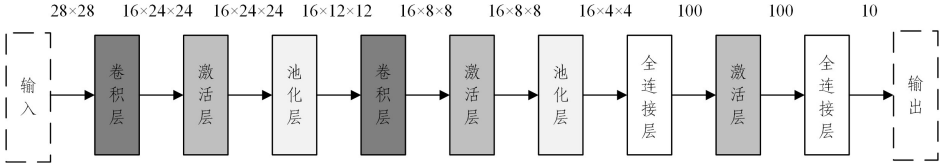

图 4 神经网络架构

Fig. 4 Architecture of neural network

不同方案的性能比较结果如表 4 所列。在相同网络下，LPMS 只需要 0.08 s 的运行时间和 0.81 MB 的通信成本，远小于其他方案的计算开销和通信开销。相比 PPFE 方案，本文方案将计算开销和通信开销降低了 73.33%和 68.36%。

表 4 不同隐私保护方案的性能比较

Table 4 Comparison of performance of different privacy protection schemes

方案	运行时间/s	信息量大小/MB
MiniONN[28]	9.32	657.50
FALCON[29]	0.84	92.50
PPFE[16]	0.30	2.56
LPMS	0.08	0.81

LPMS 方案与其他隐私保护深度学习框架的安全性比较如表 5 所列。MiniONN 和 CryptoNets 方案均基于明文训练出的模型实现隐私保护神经网络，因此无法保障训练数据的隐私安全。同时，在 MiniONN 方案中，每层神经网络都要求客户端与服务器共享输入输出值，因此该方案不支持客户端离线操作，且无法确保模型参数的隐私不被泄露。在 PPFE 方案中，由于发送方仅对初始图像进行简单拆分后便将其发送至边缘服务器，若攻击者同时窃取两个信道的拆分图像，便可恢复出原始图像，故该方案无法抵御双信道攻击。相比之下，本文方案通过混沌加密对初始拆分图像进行加密，能够有效抵御双信道攻击。此外，由于在整个训练和分类过程中，相关数据始终保持拆分状态，单个边缘服务器无法获取完整的数据，因此，本文方案不仅能保护模型参数的隐私，还能实现对推理和训练过程的全方位隐私保护。

表 5 不同隐私保护深度学习框架的安全性比较

Table 5 Comparison of security of different privacy-preserving deep learning frameworks

方案	抵御双信道攻击	客户端离线	模型参数隐私	推理隐私	训练隐私
MiniONN[28]	—	×	×	√	×
FALCON[29]	—	√	—	√	×
PPFE[16]	×	√	√	√	√
LPMS	√	√	√	√	√

结束语 本文提出了一个基于加性秘密共享的轻量级隐私保护移动传感目标分类框架 LPMS，用于实现移动传感设备的目标分类。针对神经网络中的卷积层、池化层、激活层和全连接层的安全性需求构建了高效的安全计算协议，从而大幅降低了用户的计算和资源开销。在原始数据上传至边缘服务器之前，构建了一种混沌加密方案，能够有效防止通信信道被攻击者破坏。仿真实验结果表明，本文方案具有较高的安全性和有效性。

参 考 文 献

[1] LIM W Y B, LUONG N C, HOANG D T, et al. Federated learning in mobile edge networks: A comprehensive survey[J]. IEEE Communications Surveys Tutorials, 2020, 22(3): 2031-2063.

[2] BISWAS A, WANG H C. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain[J]. Sensors, 2023, 23(4): 1963.

[3] WANG Z Y, XIONG H Y, ZHANG J, et al. From personalized medicine to population health: a survey of mHealth sensing techniques[J]. IEEE Internet of Things Journal, 2022, 9(17): 15413-15434.

[4] ZHANG Y M, CHEN Y M, BAI X, et al. Adaptive unimodal cost volume filtering for deep stereo matching[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2020: 12926-12934.

[5] SIMONYAN K, ZISSERMAN A. Very deep convolutional networks for large-scale image recognition[J]. arXiv: 1409.1556, 2014.

[6] LIU B, DING M, SHAHAM S, et al. When machine learning meets privacy: A survey and outlook[J]. ACM Computing Surveys, 2021, 54(2): 1-36.

[7] LI W D, OU J W. Machine scheduling with restricted rejection: An Application to task offloading in cloud-edge collaborative computing[J]. European Journal of Operational Research, 2024, 314(3): 912-919.

[8] GUPTA S, CAMMAROTA R, ŠIMUNIĆ T. Memfhe: End-to-end computing with fully homomorphic encryption in memory [J]. ACM Transactions on Embedded Computing Systems, 2024, 23(2): 1-23.

[9] ZHANG J W, KANG X, LIU Y, et al. A secure and lightweight multi-party private intersection-sum scheme over a symmetric cryptosystem[J]. Symmetry, 2023, 15(2): 319.

[10] GILAD-BACHRACH R, DOWLIN N, LAINE K, et al. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy[C]// International Conference on Machine Learning. PMLR, 2016: 201-210.

[11] MOHASSEL P, RINDAL P. ABY3: A mixed protocol framework for machine learning[C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 35-52.

[12] RATHEE D, RATHEE M, KUMAR N, et al. Cryptflow2: Practical 2-party secure inference[C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 325-342.

[13] DITTMER S, ISHAI Y, LU S, et al. Authenticated garbling from simple correlations[C]// Annual International Cryptology Conference. Cham: Springer, 2022: 57-87.

[14] BORGES R, SEBÉ F. An e-Coin Based Construction for Unlinkable Priced Oblivious Transfer[J]. The Computer Journal, 2023, 67(3): 933-940.

[15] XIONG J B, BI R W, ZHAO M F, et al. Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles[J]. IEEE Wireless Communications, 2020, 27(3): 24-30.

[16] HUANG K, LIU X M, FU S J, et al. A lightweight privacy-preserving CNN feature extraction framework for mobile sensing [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1441-1455.

[17] YANG X, CHEN J, HE K, et al. Efficient privacy-preserving inference outsourcing for convolutional neural networks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4815-4829.

[18] PENG Y X, SUN K H, HE S B. A discrete memristor model and its application in Hénon map[J]. Chaos, Solitons & Fractals, 2020, 137: 109873.

[19] ZHENG Y Z, LI L, QIAN L, et al. Sine-SSA-BP ship trajectory prediction based on chaotic mapping improved sparrow search algorithm[J]. Sensors, 2023, 23(2): 704.

[20] BOGDANOV D, NIITSOO M, TOFT T, et al. High-performance secure multi-party computation for data mining applications[J]. International Journal of Information Security, 2012, 11: 403-418.

[21] ARAKI T, FURUKAWA J, LINDELL Y, et al. High-throughput semi-honest secure three-party computation with an honest majority[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 805-817.

[22] QIN Z, YAN J B, REN K, et al. Towards efficient privacy-preserving image feature extraction in cloud computing[C]// Proceedings of the 22nd ACM International Conference on Multimedia. 2014: 497-506.

[23] WANG J J, HU S S, WANG Q, et al. Privacy-preserving outsourced feature extractions in the cloud: A survey[J]. IEEE Network, 2017, 31(5): 36-41.

[24] BEAVER D. Efficient multiparty protocols using circuit randomization[C]// Advances in Cryptology (CRYPTO'91). Berlin: Springer, 1992: 420-432.

[25] XIONG J B, BI R W, TIAN Y L, et al. Toward lightweight, privacy-preserving cooperative object classification for connected autonomous vehicles[J]. IEEE Internet of Things Journal, 2021, 9(4): 2787-2801.

[26] BOGDANOV D, LAUR S, WILLEMSON J. Sharemind: A framework for fast privacy-preserving computations[C]// Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security. Berlin: Springer, 2008: 192-206.

[27] GEIGER A, LENZ P, STILLER C, et al. Vision meets robotics: The kitti dataset[J]. The International Journal of Robotics Research, 2013, 32(11): 1231-1237.

[28] LIU J, JUUTI M, LU Y, et al. Oblivious neural network predictions via minionn transformations[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 619-631.

[29] LI S H, XUE K P, ZHU B, et al. Falcon: A fourier transform based approach for fast and secure convolutional neural network predictions[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 8705-8714.

HE Yuyu, born in 2000, postgraduate. His main research interests include privacy-preserving machine learning and secure multi-party computation.

ZHOU Feng, born in 1976, postgraduate, associate professor, postgraduate supervisor. Her main research interests include big data security and privacy protection.

(责任编辑:何杨)