柯晓鹏

个人主页: <https://sites.google.com/view/xiaopeng-ke>

Github: github.com/mezereonxp

Email: mezereonxp@gmail.com

手机号: +86-130-3249-4890

教育经历

- **东北大学** 沈阳, 中国
工学学士 - 软件工程; *GPA: 3.82*
2015年9月 - 2019年6月
主要课程: 操作系统, 数据结构, 算法分析, 计算机网络, 数据库原理
- **南京大学** 江苏, 中国
硕士 - 计算机科学与技术; *GPA: 4.34*
2019年9月 - 2023年6月
主要课程: 高级机器学习, 分布式系统, 密码学, 计算理论导引

业界经历

- **滴滴出行** 北京, 中国
高级算法工程师
2024年8月 - 至今
 - **花小猪智能呼返策略开发**: 主要负责花小猪自营和三方商家的智能呼返策略开发, 基于因果推断和凸优化的技术, 在千万级冒泡上实现精确的弹性预测,
- **迁移科技** 北京, 中国
算法工程师
2023年7月 - 2024年8月
 - **Atom低代码算法构建模块开发以及Pixel系列结构光相机开发**: 主要负责结构光单目相机三维重建的算法开发, 在工业机械臂抓取领域上的低代码平台的开发构建以及维护。

项目

- **单目结构光相机开发以及结构光条纹研究**: 开发实现了5步相移条纹, 多位的二值高频格雷码条纹以及抗反光物体的线移条纹, 应用在了单目结构光相机上, 在大规模的工业场景上得到应用, 在相机的最佳工作距离下, 三维重建z轴重复精度达到0.1mm, 标准球棒测量球心距误差小于0.1mm, 线移条纹能使得各类反光工件包括反光轴棒等完整成像, 克服了传统相移条纹测量的缺点。
- **针对移动应用中的深度学习模型的自动化切片和测试**: 我们提出了一个自动化切片和测试的框架, 用来针对移动应用中的深度学习模型进行切片和测试。在我们的框架中, 具备两种重建的技术, 分别用来还原不可反向传播的模型到可训练的模型以及重建预处理和后处理的步骤。我们利用该框架, 探究了100个商业应用中的深度学习模型, 并且发现56%的模型具有鲁棒性的问题。
- **隐私保护和鲁棒的联邦深度度量学习**: 在联邦学习场景下, 我们提出了一种新的训练范式用于训练深度度量学习模型。我们对所提出的深度度量学习的联邦训练过程的收敛性进行了分析和证明。同时, 为了保护用户的训练数据, 我们利用差分隐私技术, 在训练的梯度上添加噪声, 实现了隐私保护的联邦训练。
- **高效实用的长视频摘要**: 我们观察到, 当前许多的领先的视频摘要方法都依赖于核时分割 (KTS) 方法。由于KTS方法的复杂度高, 在处理长视频的时候其耗时和内存开销巨大。为了解决这一问题, 我们提出了一种基于长尾分布的D-KTS方法, 给出了一套实用的长视频摘要的流程框架。
- **针对黑盒深度学习服务的推理数据保护**: 深度学习服务通常需要用户上传数据进行云端的推理, 而这些数据容易被二次使用, 比如训练别的任务。因此, 我们提出了一种自动化的特征去除方法, 针对黑盒的深度学习服务, 去除推理数据中不必要的部分特征。使得, 推理数据在被清理特征之后, 难以被用于二次使用。

已发表成果

- 会议论文: **RE-DLC: Learning-driven Reverse Engineering for Deep Learning Compilers** : Minghui Li, Yang Li, Hao Han, Xiaopeng Ke, Tongyu Wang, Fengyuan Xu and Liming Fang. (ISSRE-2024)
- 会议论文: **CAPter: Controllable Data Privacy Enhancement for Deep Learning Inference Services** : Shimao Xu, Xiaopeng Ke, Hao Wu. (UIC-2024)
- 期刊论文: **TIM: Enabling Large-scale White-Box Testing on In-App Deep Learning Models** : Hao Wu, Yuhang Gong, Xiaopeng Ke, Hanzhong Liang, Minghao Li, Fengyuan Xu, Yunxin Liu, Sheng Zhong. (TIFS-2024)
- 会议论文: **GAPter: Gray-box Data Protector for Deep Learning Inference Services at User Side** : Wu Hao, Bo Yang, Xiaopeng Ke, Siyi He, Fengyuan Xu, and Sheng Zhong. (ICASSP-2023)
- 会议论文: **Privacy-Preserving and Robust Federated Deep Metric Learning** : Yulong Tian, Xiaopeng Ke, Zeyi Tao, Shaohua Ding, Fengyuan Xu, Qun Li, Hao Han, Sheng Zhong, Xinyi Fu. (IWQoS-2022)
- 会议论文: **Towards Efficient and Practical Long Video Summary**: Xiaopeng Ke, Boyu Chang, Hao Wu, Fengyuan Xu, and Sheng Zhong. (ICASSP-2022)
- 会议论文: **Efficient Architecture Paradigm for Deep Learning Inference as a Service.**: Jin Yu, Xiaopeng Ke, Fengyuan Xu, and Hao Huang. (IPCCC-2020)

荣誉及奖项

- ATEC 比赛第二季: 数字货币欺诈交易的检测 (第4名), 2021
- ACM MM2021 AIC 第7季: 针对商标检测的鲁棒性防御竞赛 (21/36489), 2021
- 东北大学优秀毕业生, 2019
- 国家数学建模比赛二等奖, 华为命名奖学金, 2018
- 东北大学数学建模比赛一等奖, 中天钢铁数学建模挑战赛一等奖, 2017

开源经历

- **AnomalyDetectTool**
 - 开源了一个名为“AnomalyDetectTool”的异常检测工具库, 用于时序数据的异常检测, 截至2024年获得85星。