

赵嘉乐

2005.06.02 | 广东

15626006790 | zh2841871831@gmail.com

[Google Scholar](#) | [Homepage](#)



教育经历

广东工业大学 计算机科学与技术 本科 2023.09 - 2027.06
GPA:4.12/5.0 (学院前 2.7%) | CET-6 | 核心课程：程序设计(96)、高等数学(90)、线性代数(100)、离散数学(97)、数据结构(99)
个人技能：熟练掌握 Python 及常用数据分析库，具备数据处理、分析与可视化能力；熟悉 PyTorch 深度学习框架，能够进行模型构建、训练、优化及调参；熟悉 Linux 开发环境及常用命令，具备程序编译、调试与部署能力；掌握 LaTeX 学术论文排版。

项目经历

言华——基于 AI 多模型部署的中华文化体验教育平台 2024.09 - 2025.03

- 负责平台核心功能开发与模型部署，结合计算机视觉、NLP 和生成式 AI 技术，实现多元化汉语学习模块；
- 使用 Stable Diffusion 与 LoRA 微调技术优化大语言模型在古诗词生成与意境图像创作任务中的表现，并提升模型推理效率；

科研经历

我的研究方向聚焦深度伪造检测、对抗性攻击与 AI 安全，同时覆盖高效深度学习算法、生成式模型可靠性评测、隐私安全计算等交叉领域。围绕物理域 AI 对抗鲁棒性这一核心问题，我原创提出 ISPCloak 物理伪装攻击框架，首次揭示现有深度伪造检测器过度依赖数字频域伪影的决策惯性缺陷，验证其在真实相机 ISP 成像链路中物理噪声干扰下决策边界将显著崩塌；该框架无需迭代优化，即可实现高效、普适的物理域对抗伪装攻击。应用层面，重点围绕文本生成视频、Transformer 大模型等主流 AI 体系，从物理一致性、文本可控性、推理效率、隐私安全等现实维度，开展深度学习与生成式模型的安全、效率与可靠性评估，搭建专项评测基准与高效算法框架，系统剖析 AI 模型在复杂实际场景下的性能短板。代表性成果（*表示共同第一作者，按字母序排序）：

- 《ISPCloak: Weaponizing ISP for Optimization-Free Physical Camouflage against Deepfake Detectors》(一作), ACM MM 2026

Jiale Zhao, Jiajun Wan, Lei Tang, Ye Qin, Kebing Jin, Jinghui Qin, 提出一种无需迭代优化的对抗攻击框架，通过将真实相机的物理噪声与 ISP 成像统计特性嵌入生成图像，在保持视觉质量的同时，快速且普遍地使现有深度伪造检测器失效，揭示了当前检测范式在物理域鲁棒性上的根本漏洞。

- 《Fast Sampling for Privacy-Preserving Lazy Multiplicative Weight Update》(*), ICDM 2025, Xiaoyu Li*, Zhao Song*, Jiale Zhao*

提出一种子线性时间的 MWU 近似算法，用于加速大规模决策问题中的专家权重更新，并在计算效率与差分隐私之间取得理论保证。

- 《EP-MAE: A Resource-Efficient Masked Autoencoding Framework for 3D Neural Representation Learning》(二作), Neural Networks

Jian Zhu, Jiale Zhao, Chengxing Lin, Luan Lyu, Ruichu Cai, Xiaohua Ren, Enhua Wu

提出一种高效自监督学习框架 EP-MAE，通过序列化建块、上下文感知令牌丢弃和轻量动量教师三大策略，在保持性能的同时加速预训练。

- 《Conv-Basis: A New Paradigm for Efficient Attention Inference and Gradient Computation in Transformers》(*), EMNLP 2025 Findings

Yingyu Liang*, Heshan Liu*, Zhenmei Shi*, Zhao Song*, Zhuoyan Xu*, Jiale Zhao*, Zhen Zhuang*

提出基于卷积基表示的注意力近似方法，将自注意力分解为结构化卷积形式，从而实现近线性复杂度的高效推理与梯度计算。

- 《T2VPhysBench: A First-Principles Benchmark for Physical Consistency in Text-to-Video Generation》(*), Preprint

Xuyang Guo*, Jiayan Huo*, Zhenmei Shi*, Zhao Song*, Jiahao Zhang*, Jiale Zhao*

提出基于第一性原理的文本生成视频物理一致性评测基准，衡量模型在核心物理定律上的遵循能力，并揭示当前架构在物理建模上的系统性缺陷。

- 《T2VTextBench: A Human Evaluation Benchmark for Textual Control in Video Generation Models》(*), Preprint

Xuyang Guo*, Jiayan Huo*, Zhenmei Shi*, Zhao Song*, Jiahao Zhang*, Jiale Zhao*

提出首个面向文本生成视频模型中屏幕内文本保真度与时间一致性的人类评估基准，用于衡量模型在复杂动态场景下精确渲染文字与公式的能力。

奖项荣誉

2023-2024 年校级一等奖学金

2024 华为昇腾 AI 创新大赛广州赛区金奖

2024 蓝桥杯 c++赛道广东省一等奖

2024 高教社杯全国大学生数学建模竞赛广东省三等奖

校园经历

2023 级计算机科学与技术伏羲班（前 6%尖子班）班长

负责班级日常事务管理与学术组织工作，协调课程学习进度与小组合作安排，保障班级整体学习效率与运行秩序。