汪心成

182-7937-3593
seymour2003@qq.com
推荐算法实习生
isSeymour.github.io

教育背景

硕士，上海交通大学，人工智能学院，人工智能　　预计 2026.09—2029.01

本科，同济大学，计算机学院，信息安全　　2021.09—2026.06

排名: 2 / 34　GPA: 4.82 / 5.0　CET-6: 522　国家励志奖学金 2 次 (1 / 34 ,2024 | 1 / 34 ,2023)

学术成果

TKDE（CCF-A 类期刊） Defending Attacks on Anti-fraud Model with Generative Graph Representations

- **第二作者**，主要承担模型代码实现、实验性能测试、论文初稿部分撰写等工作。　　2025.02—2025.11
- **研究背景**：金融欺诈检测领域现有对抗攻击方法多局限于理想环境、且在数据处理时容易丢失原始图重要信息。
- **创新方案**：提出 GSRGNN 图神经网络框架。①特征净化重构：通过生成模块获取增强的干净节点特征；②局部高阶邻居结构增强：使用节点阶数作为信赖值，以获得在各自局部图上的稳定结构；③上述形成一张新的生成图，将生成图和原始图一并作为输入进入下一层生成得到综合图特征。
- **实验效果**：在 Amazon 和 Yelp 的一般数据集、攻击数据集上的检测性能 (AUC 指标) 比 SOTA 分别高出 **1.94%**、**1.95%** 和 **1.95%**、**6.87%**；在真实 WeChat Pay 上性能位居前列，AUC 高达 **90.24%**、**88.87%**。

项目经历

阿里云天池新闻推荐 Top 7 方案 | 竞赛项目　　2025.12—2026.03

- **验证体系**：采样 5w / 20w 用户构建 Leave-one-out 离线评估体系，预测最后一次点击，确保离线指标对齐线上。
- **数据处理**：统一时间戳表示形式、缺失值按用户分桶填充处理等，逐十分钟滑动窗口统计新闻热榜。
- **召回策略**：基于 ItemCF、BiNetwork、Word2Vec、Hot-Items、DSSM、SASRec-3000 六路召回，分析召回重合度。
- **特征工程**：挖掘用户画像特征、文章质量特征、交叉匹配特征、召回源衍生特征、文章间相似性特征等 30 余项。
- **排序策略**：将排序建模为二分类任务，采用 XGBoost 与 DIN 并联融合架构，最终选出排序评分 Top5 作为结果。
- **涨点技巧**：指标 MRR@5 通过引入点击敏感性 ↑ 1.2%，差异化模型集成 ↑ 1.1%，SASRec 负采样优化 ↑ 0.2%。
- **性能优化**：采用缓存、预排序、向量化计算、多进程并行等手段优化代码，全流程耗时约从 6h 压缩至 4h 。
- **阿里云长期赛 MRR@5 得分 0.3188（最高 0.3199），位列总榜第 7 名（7 / 16000+）。**[1]

强网拟态人脸识别攻击 | 竞赛项目　　2024.12—2025.02

- **数据处理**：根据人脸显著性热图仅在人眼、鼻梁、嘴角等关键语义区域施加稀疏扰动 (扰动面积仅占图像 5.2%)。
- **攻击策略**：设计分层特征扰动损失，同时约束浅层边缘纹理、中层结构和高层语义特征，梯度多样性提升。
- **集成优化**：采用动态权重集成策略，在代理模型 ResNet50 和 ArcFace 上协同优化，黑盒 ASR 提升至 78.3%。
- **团队荣获 AI 安全初赛第一名（1 / 586）和总决赛第八名（8 / 40）。**

全栈专业推荐与学业规划系统 | 开发项目　　2024.01—2024.09

- **全栈架构**：采用 Vue3 + Element Plus 构建响应式前端界面，配合 Django REST Framework 打造标准化后端接口。
- **数据驱动**：利用 Scrapy/Requests 自动化构建高校专业数据库；基于课程兴趣量化匹配度输出专业建议得分。
- **功能集成**：集成 Qwen API，通过 Prompt Engineering 构建专家级咨询模块，为用户提供学业路径规划。
- **安全存储**：基于 JSON Web Token 实现无状态身份验证机制；优化 MySQL 数据库表结构设计，确保高效查询。
- **独立负责从需求分析、数据库建模、前后端开发、在线部署的全流程，获课程设计“优秀”评定。**[2]

专业技能

- 熟悉 Python 编程语言，熟练使用 PyTorch 进行深度学习模型开发，具备 Linux 环境下开发与调试经验。
- 熟悉 C/C++ 编程语言，掌握常见数据结构及其 STL 容器，了解部分底层实现原理。
- 熟悉推荐系统全链路流程，掌握 CTR 预估相关模型，如 LR、FM、Wide & Deep、DeepFM、DIN 等。
- 熟悉常见评估指标，如 AUC、Precision、Recall 等；熟悉推荐系统评价指标，如 HitRate、NDCG、MRR 等。
- 了解 Transformer 架构，如注意力机制 MHA / GQA、归一化层 LayerNorm / RMSNorm、门控 FFN、MoE 等。

[1] 在线榜单：https://tianchi.aliyun.com/competition/entrance/531842/rankingList
[2] 效果展示：https://isseymour.github.io/butterflyblog/2024/03/29/AAMS/