WEIDI LUO

Ohio State University, 100 Lane Ave., Columbus, OH 43210
(+1)614.477.3643 (+86)18990600198 luo.1455@buckeyemail.osu.edu https://eddyluo1232.github.io/

EDUCATION

School of Advanced Technology, Xi'an Jiao Tong Liverpool University Aug 2020-Jul 2022

B.SC. in Information and Computing Science, Overall GPA: 3.79/4.0, Major GPA: 3.92/4.00

Core Course: Artificial Intelligence(4.0), Computer System(4.0), Discrete Mathematics(4.0), Java Programming(4.0), Algorithmic Foundation and Problem Solving(4.0), Linear Algebra(4.0), Calculus(4.0), Multivariable Calculus(4.0)

Art and Science College, The Ohio State University Aug 2022-Jul 2025

B.A. in Computer and Information Science, Overall GPA: 3.63/4.0

Core Course: Introduction to Data Mining(A-), Introduction to Statistics(A-), Introduction to Linguistics(A), Survey on Bias in Artificial Intelligence(A), Computer and Linguistics(A), Conlangs(A), Language and Mind(A), Language and Ethic(A)

PUBLICATION

Siyuan Ma*, **Weidi Luo***, Yu Wang, Xiaogeng Liu, Muhao Chen, Bo Li, Chaowei Xiao, "*Visual-RolePlay: Universal Jailbreak Attack on MultiModal Large Language Models via Role-playing Image Character*", on Arxiv.

Weidi Luo*, Siyuan Ma*, Xiaogeng Liu*, Xiaoyu Guo, Chaowei Xiao, "*JailBreakV-28K: A Benchmark for Assessing the Robustness of MultiModal Large Language Models against Jailbreak Attacks*", Accepted by COLM'2024.

Vardaan Pahuja, **Weidi Luo**, Yu Gu, Cheng-Hao Tu, Hong-You Chen, Tanya Berger-Wolf, Charles Stewart, Song Gao, Wei-Lun Chao, Yu Su, "*Bringing Back the Context: Image Classification as Link Prediction on Multimodal Knowledge Graphs*", Accepted by CIKM'2024.

RESEARCH EXPERIENCES

Multimodal Large Language Model Attack | University of Wisconsin-Madison | Research Assistant. Dec 2023- Apr 2024

Advisor: Chaowei Xiao, Assistant Professor at Information School, University of Wisconsin-Madison

- Developed and tested a universal MLLM jailbreak attack, "Visual Role-Playing," which surpassed all benchmarks for multimodal large language models, and threw insight into converting query-specific settings to universal settings.
- Improved evaluation metrics for relevance plus toxic evaluation and accurately assessed the robustness of multimodal large language models including the closed source models against role-playing jailbreak attacks.
- Conducted detailed statistical analysis and sample learning of experimental results for paper writing.

Multimodal Large Language Model Safety | University of Wisconsin-Madison | Research Assistant. Dec 2023- Apr 2024

Advisor: Chaowei Xiao, Assistant Professor at Information School, University of Wisconsin-Madison

- Specialized in data mining and development of high-quality, diverse benchmark JailBreakV-28K and RedTeam-2K, which is A Benchmark for Assessing the Robustness of MultiModal Large Language Models(MLLMs) against Jailbreak Attacks.
- Expertise in deployment, training, and evaluating of the state of art Multimodal Large Language Models and Advanced Language Models. Proficient in Utilizing Hugging Face and GitHub for Advanced Model Development and Collaboration
- Implemented Jailbreak Attack Strategies on Various Large Language Models for Security Analysis, and proved the transferability of LLM jailbreak attack on MLLMs.

Machine Learning on Camera Trap | ICICLE Institute | Research Assistant Aug 2022- Dec 2023

Advisor: Yu Su, Distinguished Assistant Professor at College of Engineering, Ohio State University

- Expertise in leveraging traditional knowledge graph embedding techniques for refined classification of biological species, ensuring high-precision taxonomic categorization for Out-of-distribution detection.
- Developed and introduced COSMO, an innovative framework for image classification that harnesses multi-modality knowledge graphs, achieving benchmark-setting performance surpassing current state-of-the-art methodologies.
- Proficient in the deployment of the XGBoost machine learning algorithm, augmented with incremental learning strategies, for advanced multi-modal image recognition across extensive datasets.
- Demonstrated proficiency in the design, implementation, and operational deployment of Knowledge Graph Embedding algorithms (including TransE, TransH, Distmult, ConvE), coupled with the application of sophisticated Deep Learning models.

Machine Learning based on Data Mining | North Carolina State University | Research Assistant Jane 2022-Feb 2022

Advisor: Min Chi, Associate professor at department of Computer Science, North Carolina State University

- Demonstrated expertise in the execution of complex data mining algorithms, paired with a sophisticated application of feature engineering techniques to extract and enhance predictive model performance.
- Executed a comprehensive analytical project utilizing the NBA dataset from Kaggle; skillfully integrated a suite of machine learning algorithms (XGBoost, Random Forest, SVM, PCA, Isolation Forest) with deep learning architectures (LSTM, MLP) to forecast NBA All-Star Game selections with high accuracy.
- Acquired advanced skills in the design and composition of academic posters, effectively synthesizing and presenting research findings for scholarly communication.

Deep Learning based on Computer Vision | Xi'an Jiao Tong Liverpool University | Research Assistant Dec 2022-May 2022

Advisor: Erick Purwanto, lecturer in School of Advanced Technology, Xi'an Jiaotong liverpool University

- Advanced proficiency in deep learning computer vision tasks, including nuanced approaches to image segmentation and classification, demonstrating the ability to extract significant insights from visual data.
- In-depth knowledge and hands-on experience in deploying and fine-tuning state-of-the-art computer vision models such as Swin Transformer and the U-Net series, ensuring cutting-edge outcomes in model performance.
- Skilled in the preprocessing of image datasets, implementing innovative data augmentation techniques like Cut-Out, Mix-up, and Test-Time Augmentation (TTA) to enhance model robustness and data diversity.
- Awarded First Prize in the Xi'an Jiao Tong Liverpool University Data Science Competition 2022 for the Classification task on Hep-2 cells, where I employed advanced models like CoAtNet and ConvNeXt, setting a new benchmark that exceeded the existing state-of-the-art performance.

Computer Vision on Data Acquisition | North Carolina State University | Research Assistant June 2021-Aug 2021

Advisor: Andre Mazzoleni, Professor in Engineering Department, North Carolina State University

- Proficient in utilizing Matlab for a comprehensive range of image analysis tasks: from acquisition and camera calibration to processing, segmentation, ground truth annotation, and advanced 3D reconstruction, ensuring high fidelity in visual data manipulation and interpretation.
- Cultivated expertise in the practical application of sophisticated computer vision algorithms, including but not limited to R-CNN for object detection, ACF for feature detection, OCR for text recognition, and SFM for 3D imaging from 2D data, reflecting a robust understanding of image analysis and pattern recognition.

SKILL

Programming Languages: C/C++, Matlab, Java, Python, SQL, CQL

Strong skills in Pytorch. Numpy, Pandas, Matplotlib, Sklearn, Java Programming, C Programming, Database, Neo4j, Linux

Strong skills in teamwork and cooperation

Office Applications: Microsoft Office, Team, Letax