Xutao Henry Mao

xutao.mao@vanderbilt.edu | +1 857-869-6559

EDUCATION

Bachelor of Science, Vanderbilt University **Aug 2022 - Dec 2025**

- *Grade: 3.867/4.0*
- Key courses: AI, Foundation of Machine Learning, Data Mining and AI, Privacy & Security (PhD-Level)
- Awards: Dean's List for all semesters (Fall 2022-Spring 2025); Vanderbilt University Summer Research Scholarship (2025)

RESEARCH EXPERIENCE

Research on Fake Voice Generation and Fake Voice Detection **Sept 2023 - May 2025**

Leader & First Author, Supervised by Dr. Dan (Linda) Lin, Vanderbilt University

- Objective: Conduct a large-scale, cross-domain evaluation to understand the evolving arms race between fake voice generation and detection, identifying vulnerabilities and guiding the development of more robust detection systems.
- Contribution 1**:** Benchmarked 20+ state-of-the-art fake voice generators and 8 leading fake voice detectors using a one-to-one evaluation protocol, revealing unique acoustic artifacts, method-specific vulnerabilities, and detector performance variations across generator types.
- Contribution 2: Performed explainability-driven analysis of generator–detector interactions to uncover the root causes of detection failures, and proposed actionable practices to enhance the robustness, generalization, and transparency of fake voice detection technologies.

Research on Personalization Imputation on Textual Edge Graph **Oct 2024 - July 2025**

Key Contributor & Co-first Author, Supervised by Dr. Tyler Derr, Vanderbilt University

- Objective: Design and evaluate a scalable framework for leveraging large language models to perform accurate, context-aware imputation on multivariate time series, addressing challenges of missing data in real-world applications.
- Contribution 1: Designed and implemented a graph-aware LLM aggregator that captures higher-order context through line-graph views, enabling the generation of coherent, personalized reviews that are more helpful, authentic, and specific.
- Contribution 2: Conducted comprehensive evaluations on Amazon and Goodreads benchmarks, demonstrating superior performance over numeric, graph-based, and LLM baselines in both recommendation quality and review generation.

Research on Opinion Distribution Prediction in social media (MindVote) **April 2025-June 2025**

Leader & First Author

- Objective: Build and use a realistic, context-rich benchmark to evaluate how LLMs predict distributions of public opinion in social media, closing the gap left by survey-based evaluations.
- Constructed MindVote, a 3,918-poll dataset from Reddit and Weibo (English & Chinese) spanning 5 major topics / 23 subtopics, with rich platform, topical, and temporal annotations and a multi-stage quality pipeline; released in CSV/JSON for reproducible evaluation.
- Revealed substantial performance gaps and systematic biases invisible to traditional benchmarks, including domain-specific knowledge limitations, source of origin bias, and social media context dependencies, enabling authentic assessment of LLM social reasoning capabilities.

Research on Text-to-SQL Optimization via Graph-guided Reasoning **June 2025-Aug 2025**

Key Contributor & Co-first Author, Supervised by Dr.Hongying Zan, Zhengzhou University

- Objective: Unify mathematical reasoning and schema navigation in complex Text-to-SQL by reformulating both as a single graph-guided optimization: decompose math requirements, connect the required tables via a Steiner tree on the schema graph, and ensure correctness with multi-level validation.
- Developed SteinerSQL, a novel three-stage framework that reformulates complex mathematical Text-to-SQL generation as a unified graph optimization problem.
- Addressed the dual challenge of multi-step computation decomposition and intricate database schema navigation, achieving state-of-the-art performance with 36.10% execution accuracy on LogicCat and 36.75% on Spider2.0-Lite.

Ongoing Research on Hierarchical Red Teaming of Vision-Language Models **Aug 2025-Now**

Leader, Supervised by Dr.Cong Wang, City University of Hong Kong

- Objective: To develop a novel hierarchical reinforcement learning framework, Flow-RTPO, for the red teaming of Vision-Language Models (VLMs) to identify and address safety vulnerabilities. This framework is designed to generate realistic and subtle adversarial images that can expose critical failures in VLM safety protocols, providing a structured method for model improvement.

- Current Process: Currently designing the core Flow-RTPO algorithm. The initial training process is underway, focusing on implementing the Group Relative Policy Optimization (GRPO) to do reinforcement learning against the LLaVA model using the RTP-challenge benchmark.

PROFESSIONAL EXPERIENCE

Cloud Engineer Intern **May 2024-Aug 2024**

Pegasystems, Boston, MA

- Migrated and refactored automation deployment pipeline from manual deployment using Go in AWS Lambda and Jenkins, reducing deployment time by 40% and increasing reliability in staging/integration environments.
- Designed an automated security alert system for CI/CD pipelines using AWS CloudWatch, Lambda, and Elasticsearch, generating over 10 monthly security reports and reducing vulnerability exposure by 40% through AWS IAM role enforcement and proactive early-stage issue detection.

PUBLICATIONS

[1] **Xutao Mao**, Ezra Xuanru Tao, Leyao Wang. MindVote: When AI Meets the Wild West of Social Media Opinion. (Pre-print in Arxiv, Under Review)

[2] **Xutao Mao**, Ke Li, Ezra Xuanru Tao, Cameron Baird, Dan Lin. SoK: Benchmarking Fake Voice Detection in the Voice Arms Race. (Under Review)

[3**] Xutao Mao**, Tao Liu, Hongying Zan. Building Bridges Where Rivers Run: Graph-Guided Reasoning for Complex SQL Generation. (Under Review)

[4] Leyao Wang***, Xutao Mao***, Tyler Derr, et al. Towards Bridging Review Sparsity in Recommendation with Textual Edge Graph Representation. (Pre-print in Arxiv, Under Review, * = Equal Contribution.)

[5] Tao Liu*, **Xutao Mao***, Hongying Zan, et al. LogicCat: Text-to-SQL Benchmark for Multi-Domain Reasoning Challenges. (Pre-print in Arxiv, Under Review, * = Equal Contribution.)

SKILLS

LLM & AI: Transformers, Instruction-tuning & alignment, Parameter-efficient finetuning, Chain-of-Thought Reasoning, Reinforcement Learning
ML/DL: Classical ML (regression, tree ensembles, clustering), Deep Learning, GNN, Hyper-parameter Tuning
Language/Technologies: Python, Go, Java, C++, SQL, Bash, PyTorch, AWS, Git, Linux