Boming Miao

202322011154@mail.bnu.edu.cn — +86 13358855689 — Homepage

EDUCATION

Beijing Normal University Sep 2023 - Jun 2025
Master of Science, School of Statistics
GPA: 3.65/4.00
Thesis Supervisor: *Xiaoyi Wang* Co-supervised by: *Chuanlong Xie*

Northeastern University Sep 2019 - Jun 2023
Bachelor of Science, Department of Mathematics
GPA: 90.32/100

RESEARCH INTERESTS

- Trustworthy AI: adversarial machine learning and explainable machine learning.
- Generative Models: LLMs, VLMs and their application in various fields.
- Statistical Learning: learning theory and probabilistic models.

PAPERS AND WORK IN PROGRESS

AdvLogo: Adversarial Patch Attack based on Diffusion Models [arXiv] [Code]
Submitted and reviewed by TNNLS, September 2024

An Efficient Framework for Enhancing Discriminative Models via Diffusion Techniques
Submitted and reviewed by AAAI, August 2024 [OpenReview]

Robust LLMs

- Studing the vulnerability of large language models (LLMs) and investigating multi-modal perturbation techniques.
- Enhancing perturbation efficacy by applying reinforcement learning to prompt-tuning.

OOD Dection, with *Andi Zhang* at University of Cambridge

- Investigating novel methods for calculating in-distribution and out-of-distribution probabilities using generative and reconstructive techniques based on generative models.

ACADEMIC EXPERIENCE

Department of Automation, Tsinghua University Beijing, China
Research Assistant Oct 2023 - Present

- Researched the robustness and vulnerabilities of deep learning models.
- Enhanced the stealthiness of adversarial examples using generative models.
- Explored the explainability of deep neural networks through gradient maps and local masks.

Department of Computer Science, North Carolina State University Raleigh, USA
Summer Exchange Reseach Program [Poster] [Project Report] Jul 2022 - Aug 2022

- Investigated the effectiveness of several modern classifiers under a semi-supervised learning framework in the context of missing labels.

- Applied the Expectation-Maximization (EM) algorithm to generate pseudo labels during the training stage of Naive Bayes and BERT classifiers.
- Found that while the EM algorithm enhances the accuracy of the Naive Bayes classifier, it does not improve the performance of the BERT classifier due to BERT's reliance on accurate labels.

PROJECTS

Randomized learning for vision tasks Shenyang, China
Undergraduate Dissertation (Distinct) Supervised by Xuefeng Zhang Dec 2022 - Jun 2023

- Designed the framework of Matrix Configuration Networks (MSCN) and solved the computational problem caused by low rank with shifting window mechanism.
- Introduced convolution to MSCN, extending it to a deep architecture, and proposed a method for incremental weight construction in convolutional neural networks.
- Applied MSCN to vision tasks based on patch embedding, and demonstrated the great potential of randomized learning in vision tasks such as image denoising.

Soliton solutions for curve shortening flow on the pseudo-sphere Shenyang, China
NEU CN, Department of Mathematics, Research Assistant Sep 2020 - Dec 2021

- Proved that a curve is a soliton solution to the curve shortening flow if and only if its geodesic curvature is proportional to the inner product between its tangent vector and a fixed vector.
- Described the geometric properties of curves on the pseudo-sphere and further studied their qualitative behavior.
- Proved that these curves converge to the equator orthogonal to the fixed vector, providing new insights into the behavior of the curve shortening flow on the pseudo-sphere.

AWARDS

- 2024, Second Prize in the Graduate Market Research Competition
- 2023, First-class Scholarship, Beijing Normal University
- 2023, Second-class Scholarship, Northeastern University
- 2022, Third-class Scholarship, Northeastern University
- 2021, Third-class Scholarship, Northeastern University
- 2021, First Prize, Mathematics Competition of Chinese College Students (CMC)

MEMBERSHIPS

- Student Member, Chinese Association for Applied Statistics
- President, Debate Association of College of Science, Northeastern University

SKILLS

- **Programming:** Python, R, C++, Matlab
- **Language:** Chinese (Native), English (TOEFL 99)