Amber Yijia Zheng

✉ zheng709@purdue.edu • 🏠 amberyzheng.com

Education

Purdue University   **Indiana, IN**
Doctor of Philosophy in Computer Science   *2022–present*
Advisor: Raymond A. Yeh

Shanghai University of Finance and Economics   **Shanghai, China**
Bachelor of Science in Data Science   *2018–2022*
Major GPA – 3.9/4.0, Ranking – 1/41
Advisor: Yixuan Qiu

Publications

[1] **Amber Yijia Zheng***, Chiao-An Yang*, and Raymond A. Yeh. Learning to obstruct few-shot image classification over restricted classes. *European Conference on Computer Vision (ECCV)*, 2024.

[2] **Amber Yijia Zheng** and Raymond A. Yeh. Imma: Immunizing text-to-image models against malicious adaptation. *European Conference on Computer Vision (ECCV)*, 2024.
Best Paper Runner-up at AI4CC in CVPR Workshop 2024.

[3] **Amber Yijia Zheng**, Tong He, Yixuan Qiu, Minjie Wang, and David P Wipf. Graph machine learning through the lens of bilevel optimization. *Artificial Intelligence and Statistics (AISTATS)*, 2024.

[4] **Amber Yijia Zheng**, Tong He, Yixuan Qiu, and David P Wipf. Learning manifold dimensions with conditional variational autoencoders. *Advances in Neural Information Processing Systems (NeurIPS)*, 35, 2022.

Research & Work Experience

Apple   **Seattle, WA**
Research Intern   *Summer 2024*
Mentor: Chen Chen
○ Researched Diffusion-based low-light image denoising.

Purdue University — Department of Computer Science   **West Lafayette, IN**
Research Assistant   *2023-present*

○ Researched algorithms in protecting stable diffusion from malicious adaptation.
○ Researched erasing concepts from generative AI via influence functions.

Amazon Web Service   **Shanghai, China**
Applied Scientist Intern   *2022-2024*
Mentor: David P. Wipf, Tong He
○ Researched deep generative model on manifold data.
○ Investigated graph machine learning from a bilevel optimization perspective.

Kafang Tech   **Shanghai, China**
Quantitative Research Intern   *Fall 2021*

- Researched deep-learning-based trading strategy on high-frequency trading data.

Shanghai University of Finance and Economics **Shanghai, China**
Research Assistant *2019-2021*

- Researched deep generative models and proposed a mutual-information-based lower bound that provides more interpretability than a variational lower bound. (2021)
- Researched and proposed discriminator-driven energy-based latent space model. (2020 - 2021)
- Researched Kaplan-Meier precedence test based on ranked set progressively type-II censored data. (2020)
- Investigated residuals of SVM prediction on time series data. (2019)

Shanghai Jiao Tong University — John Hopcroft Center for Computer Science **Shanghai, China**
Research Assistant *Fall 2020*

- Researched overfitting in image classification via entropy theory.

Ping An **Shanghai, China**
Algorithm Engineering Intern *Summer 2020*

- Worked on the NER model in optimizing the labeled corpus of legal documents.

Teaching Experience

Purdue University **West Lafayette, IN**
Teaching Assistant - STAT 350: Introduction To Statistics *Spring 2023*

Purdue University **West Lafayette, IN**
Teaching Assistant - STAT 511: Statistical Methods *Fall 2022*

Honors & Awards

Best Paper Runner-up in AI for Content Creation at CVPR *2024*
- Recognized among the top 3% of papers.

NeurIPS Travel Award *2022*
- Awarded to support the travel of graduate students and post-doctoral fellows and junior faculty to attend NeurIPS 2022.

Shanghai Outstanding Graduate *2022*
- Recognized as an Outstanding Graduate by the Shanghai Municipal Government for academic excellence.

First-class People's Scholarship *2020, 2021, 2022*
- Awarded to top 2% students in academic in the department.

Talks

Imma: Immunizing text-to-image models against malicious adaptation (link)
- Invited keynote speaker in T2MM workshop at ICME *2024*

Towards Safer AI Content Creation by Immunizing Text-to-image Models
- Oral presentation in AI4CC workshop at CVPR *2024*

Learning Manifold Dimensions with Conditional Variational Autoencoders (link)
- Invited speaker for Rising Star Lecture Series in Center for Frontier AI Research – Singapore *2023*

Academic Services

Conference Reviewer: Neural Information Processing Systems (NeurIPS)
Conference Reviewer: International Conference on Learning Representations (ICLR)
Conference Reviewer: Computer Vision and Pattern Recognition (CVPR)

References

Raymond A. Yeh, Assistant Professor
Department of Computer Science
Purdue University
rayyeh@purdue.edu

Yixuan Qiu, Associate Professor
School of Statistics and Management
Shanghai University of Finance and Economics
qiuyixuan@sufe.edu.cn

David Wipf, Principle Research Scientist
Amazon Web Service
Amazon, Inc
daviwipf@amazon.com