

Amber Yijia Zheng

✉ zheng709@purdue.edu • 🏠 amberyzheng.com

Education

Purdue University

Doctor of Philosophy in Computer Science

Advisor: Raymond A. Yeh

West Lafayette, IN

2022–present

Shanghai University of Finance and Economics

Bachelor of Science in Data Science

Major GPA – 3.9/4.0, Ranking – 1/41

Advisor: Yixuan Qiu

Shanghai, China

2018–2022

Research & Work Experience

Apple

Research Intern

Mentor: Chen Chen

Seattle, WA

Apr. - Sept. 2024

- Researched **diffusion-based** low-light image denoising, proposing a controllable module for image-to-image diffusion models that preserves content details during the denoising process.

Purdue University — Department of Computer Science

Research Assistant

West Lafayette, IN

Mar. 2023–present

- Researched and proposed a novel task to **protect pre-trained Stable Diffusion models** from malicious adaptation, for example, against DreamBooth, LoRA, and Custom Diffusion, which can be exploited to learn harmful content.
- Researched the removal of concepts from **pre-trained Stable Diffusion models** using influence functions. This algorithm can effectively erase artistic styles and unsafe content from the model.

Amazon Web Service

Applied Scientist Intern

Mentor: David P. Wipf, Tong He

Shanghai, China

Feb. 2022 - Apr. 2024

- Researched **deep generative model** on manifold data.
- Investigated graph machine learning from a bilevel optimization perspective.

Kafang Tech

Quantitative Research Intern

Shanghai, China

Aug. - Dec. 2021

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

Shanghai University of Finance and Economics

Research Assistant

Shanghai, China

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)

Publications

- [1] **Amber Yijia Zheng** and Raymond A. Yeh. Multi-concept model immunization through differentiable model merging. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2025.
- [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 AI for Content Creation in CVPR Workshop 2024.
- [3] **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.
- [4] **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.
- [5] **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.

Honors & Awards

- | | |
|---|------------------|
| Best Paper Runner-up in AI for Content Creation Workshop 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)
- Conference Reviewer:** International Conference on Computer Vision (ICCV)