

# Chumeng Liang

✉ chumengl@usc.edu | 📱 caradryan | 🎓 Chumeng Liang

## Education

### University of Southern California

MASTER STUDENT, COMPUTER SCIENCE

- Major GPA: 3.90/4.00
- Advisor: Jiaxuan You, Ge Liu

Los Angeles, CA, USA

Aug. 2023 - Current

### Shanghai Jiao Tong University

BACHELOR, COMPUTER SCIENCE AND TECHNOLOGY

- Major GPA: 87.6/100
- Advisor: Yang Hua, Guanjie Zheng

Shanghai, China

Sep. 2018 - June. 2022

## Research Interests

I study **interpreting modern generative models**, with applications in 1) addressing **robustness, alignment, and ethical** problems in generative models, and 2) **scaling generative models to handle more complex data, such as protein structures**. In the real world, I am concern about the **societal impacts of Generative AI** and deeply invested in helping **disadvantaged groups**, such as human artists, in the era of Generative AI.

## Publications

(\* means equal contribution)

Adversarial Example Does Good: Preventing Painting Imitation from Diffusion Models via Adversarial Examples

**Chumeng Liang\***, Xiaoyu Wu\*, Yang Hua, Jiaru Zhang, Yiming Xue, Tao Song, Zhengui Xue, Ruhui Ma, Haibing Guan  
Accepted by ICML2023 (**Oral**)

CBLab: Supporting the Training of Large-scale Traffic Control Policies with Scalable Traffic Simulation

**Chumeng Liang**, Zherui Huang, Yicheng Liu, Zhanyu Liu, Guanjie Zheng, Hanyuan Shi, Kan Wu, Yuhao Du, Fuliang Li, Zhenhui Jessie Li  
Accepted by KDD2023

Mist: Towards Improved Adversarial Examples for Diffusion Models

**Chumeng Liang\***, Xiaoyu Wu\*  
Technical Report

Real-world Benchmarks Make Membership Inference Attacks Fail on Diffusion Models

**Chumeng Liang**, Jiaxuan You  
Submitted to ICLR2025

Targeted Attack Improves Protection against Unauthorized Diffusion Customization

**Chumeng Liang\***, Boyang Zheng\*, Xiaoyu Wu  
Submitted to ICLR2025

FDTI: Fine-grained Deep Traffic Inference with Roadnet-enriched Graph

Zhanyu Liu, **Chumeng Liang**, Guanjie Zheng  
Accepted by ECML-PKDD2023

Toward Effective Protection against Diffusion-based Mimicry through Score Distillation

Haotian Xue, **Chumeng Liang\***, Xiaoyu Wu\*, Yongxin Chen  
Accepted by ICLR2024

CGI-DM: Digital Copyright Authentication for Diffusion Models via Contrasting Gradient Inversion

Xiaoyu Wu, Yang Hua, **Chumeng Liang**, Jiaru Zhang, Hao Wang, Tao Song, Haibing Guan  
Accepted by CVPR2024

Online Reward-Weighted Fine-Tuning of Flow Matching with Wasserstein Regularization

Jiajun Fan, Shuaike Shen, Chaoran Cheng, Yuxin Chen, **Chumeng Liang**, Ge Liu  
Submitted to ICLR2025

## Services

### Expert Witness

ZHONGLIANG XUE ET AL V.S. EPSILON TECH

- **The first lawsuit on copyright issues of Generative AI**
- Explained different forms of unauthorized data usage in Generative AI to the plaintiffs (the copyright owners)
- Testified in court about details in the mechanisms and the unauthorized data usage of Generative AI

Beijing Internet Court

Jun, 2024

## Founder & Lead

PSYKER TEAM

Mar,2023 - Current

- A volunteering group focusing on helping **disadvantaged groups** in the age of Generative AI
- Developed software applications to counter the abuse of AI, e.g. protecting private images and detecting unauthorized data usage
- Provided volunteering technical and legal consulting services for disadvantaged groups, such as human artists

## Software

MIST: WATERMARK AGAINST UNAUTHORIZED DIFFUSION CUSTOMIZATION

Oct. 2022 - Sep. 2024

- **The first open-sourced watermark tool for protecting private images from unauthorized customization of diffusion models**
- Authorized **Dropbox** and two other companies for commercial use from March 2024
- **GitHub Stars: 416+310=726**, Media: 16k reposts+20k likes
- Role: team lead + main developer

CBLAB: VERY LARGE SCALE TRAFFIC SIMULATION SYSTEM IN C++

Oct. 2021 - Sep. 2022

- Open-sourced Simulator for urban traffic **with a million vehicles in a real-time/simulation-time ratio of 1:1**
- Role: main developer

## Research Experiences

### Scalable Flow Matching for Protein Generative Modeling with Latent Trees

University of Illinois  
Urbana-Champaign

ADVISOR: GE LIU, JIAXUAN YOU

Jun,2024 - Current

- Designed and implemented scalable latent flow matching for protein generation in PyTorch
- Trained flow matching models on large-scale PDB data with distributed data parallelization

### Real-world Benchmarks Make Membership Inference Attacks Fail on Diffusion Models

University of Illinois  
Urbana-Champaign

ADVISOR: JIAXUAN YOU

Mar,2024 - Sep,2024

- Investigated fatal defects in the previous evaluation of membership inference attacks on diffusion models
- Implemented the first benchmark for membership inference attacks on diffusion models
- Revealed the fact that membership inference attacks on diffusion models are not reliable

### Mist: Watermark against Unauthorized Diffusion-based Artwork Copying

University of Southern California

ADVISOR: YANG HUA

Oct,2022 - Jan,2024

- Designed, implemented, and improved the protection watermark against unauthorized diffusion customization
- Interpreted the mechanism of the protection watermark by analyzing the neural network behaviors of diffusion models
- Open-sourced and maintained the tool

### CBLab: Very Large Scale Traffic Simulation System in C++

Shanghai Jiao Tong University

ADVISOR: GUANJIE ZHENG

Oct. 2021 - Sep. 2022

- Designed and implemented an efficiently multi-thread parallelized traffic simulation system in C++
- Deployed the simulation system on distributed servers as a real-time runtime
- Developed a data transformer in Python to transform OpenStreetMap to simulation input data
- Open-sourced and maintained the scalable simulation system with 10,000 lines of code with documentation

## Teaching & Academic Services

2024 **Reviewer**, NeurIPS2024, ICLR2025, AISTATS2025

2024 **Teaching Assistant**, DSCI352: Applied Machine Learning and Data Mining

2021 **Teaching Assistant**, Introduction to Artificial Intelligence

University of  
Southern California  
Shanghai Jiao Tong  
University