

# Haotian Xue




✉ [htxue.ai@gatech.edu](mailto:htxue.ai@gatech.edu)

🐦 [@Haotianxue\\_GT](https://twitter.com/Haotianxue_GT)

🔗 <https://github.com/xavihart>

🌐 <http://xavihart.github.io/>

## Education

- 2018 – 2022  **B.E. @ Computer Science, Shanghai Jiao Tong University**, Shanghai  
Advisor: *Quanshi Zhang, Zhouhan Lin*
- 2022 – 2024 (expected)  **M.S. @ Computer Science, Georgia Tech**, Atlanta  
Advisor: *Yongxin Chen*
- 2022 – 2027 (expected)  **Ph.D. @ Machine Learning, Georgia Tech**, Atlanta  
Advisor: *Yongxin Chen*

## Employment History

- 2021.9 – 2021.12  **Research Intern**, Microsoft Research Asia  
Advisor: *Lei Cui*  
Project: *Large pretraining for document AI*
- 2021.9 – 2022.12  **Visiting Research Intern**, MIT CSAIL  
Advisor: *Josh Tenenbaum*  
Mentor: *Yunzhu Li, Fish Tung*  
Project: *3D Intuitive Physics*
- 2022.9 – Present  **Graduate Research Assistant**, Georgia Tech  
Advisor: *Yongxin Chen*  
Project: *Generative Models*
- 2024.5 – 2024.8  **Research Intern**, Nvidia Research  
Manager: *Ming-yu Liu*  
Advisor: *Jason(Yao) Lu, Jinwei Gu, Jiaojiao Fan*  
Project: *Embodied AI*

## Machine Learning Conference Papers

I am interested in the broad aspects of machine learning, computer vision and NLP. Currently I am interested in generative models (especially diffusion models), and robust and responsible AI. I am also interested in explainable AI and designing compositional structure and algorithms. Here are some of my research outputs:

\* indicate equal contribution

- 1 Y. Chen\*, **H. Xue\***, and Y. Chen, “Diffusion policy attacker: Crafting adversarial attacks for diffusion-based policies,” *NeurIPS*, 2024.
- 2 J. Fan, **H. Xue**, Q. Zhang, and Y. Chen, “Refdrop: Controllable consistency in image or video generation via reference mixing attention,” *NeurIPS*, 2024.
- 3 A. Mete, **H. Xue**, A. Wilcox, Y. Chen, and A. Garg, “Quest: Self-supervised skill abstractions for continuous control,” *NeurIPS*, 2024.
- 4 **H. Xue**, C. Liang\*, X. Wu\*, and Y. Chen, “Towards effective protection against diffusion-based mimicry through score distillation,” *ICLR*, 2024.

- 5 **H. Xue**, A. Araujo, B. Hu, and Y. Chen, "Diffusion-based adversarial sample generation for improved stealthiness and controllability," *NeurIPS*, 2023.
- 6 **H. Xue**, A. Torralba, J. Tenenbaum, D. Yamins, Y. Li, and H. Tung, "3d-intphys: Towards more generalized 3d-grounded visual intuitive physics under challenging scenes," *NeurIPS*, 2023.
- 7 S. Hou\*, J. Kai\*, **H. Xue\***, *et al.*, "Syntax-guided localized self-attention by constituency syntactic distance," *EMNLP Findings*, 2022.

## Other Preprints

\* indicate equal contribution

- 1 **H. Xue** and Y. Chen, *Pixel is a barrier: Diffusion models are more adversarially robust than we think*, 2024.
- 2 S. Hou, J. Kai\*, Y. Zhang\*, **H. Xue\***, X. Wang, and Z. Lin, *Learning to adaptively incorporate external syntax through gated self-attention*, 2022.
- 3 X. Cheng, X. Wang\*, **H. Xue\***, Z. Liang, and Q. Zhang, *A hypothesis for the aesthetic appreciation in neural networks*, 2021.
- 4 H. Zhang, **H. Xue**, J. Chen, Y. Chen, W. Shen, and Q. Zhang, *Evaluation of attribution explanations without ground truth*, 2021.

## Skills

Coding	Python, C++, $\LaTeX$ , Pytorch, FairSeq, Numpy, Gym, HTML, CSS
Miscs	Piano, Football, Film, MOBA

## Academic Services

Reviewer for ICML2022,2023,2024; NeurIPS2022,2023,2024;ICLR 2024,2025

## Awards

2019	Singapore Tech Engineering Scholarship (Top 10%)
2019-2022	SJTU Zhiyuan Honor Award(Top 5%)
2022	SJTU Outstanding Graduate
2023	NeurIPS Scholar Award
2024	ICLR Travel Award