Gao, Ruiyuan

Email: rygao [AT] cse.cuhk.edu.hk
Tel: +86 15652580190
Homepage: gaoruiyuan.com
Shatin, Hong Kong, China

Research Interest

My current research interests span **data generation**, including generative models and synthetic data for perception tasks; and **trustworthy AI**, including adversarial attack/defence and AI privacy.

Education

The Chinese University of Hong Kong — Hong Kong, China
PhD of Computer Science and Engineer (PhD candidate) — *Oct. 2020 – Present*

Beihang University — Beijing, China
B.E. in Computer Science and Technology from SHENYUAN Honors College — *Sep. 2016 – Jun. 2020*

Experience

Research Intern — Dec. 2022 – Present
AI Theory, Huawei Noah's Ark Lab — *Hong Kong, China*
- Conducted research on data synthesis for perception in autonomous vehicles.

Research Intern — Mar. 2022 – Aug. 2022
Digital Twin, SenseTime — *Beijing, China*
- Conducted research on Neural Radiance Field (NeRF) for animatable human.

Research Intern — Jul. 2019 – Nov. 2019
Institute of Automation, Chinese Academy of Sciences — *Beijing, China*
- Conducted research on Network Architecture Search (NAS) algorithm.
- Conducted research on 3D Object Detection with Point Clouds and Images.
- Implemented parallel code framework design on Pytorch from GPU; data visualization and analysis.

Research Intern — Sep. 2018 – Jun. 2019
State Key Laboratory of Software Development Environment, Beihang University — *Beijing, China*
- Conducted research on few-shot learning and object detection.

Publication

[1] **Ruiyuan Gao***, Kai Chen*, Enze Xie, Lanqing Hong, Zhenguo Li, Dit-Yan Yeung, and Qiang Xu. "MagicDrive: Street View Generation with Diverse 3D Geometry Control". In: *International Conference on Learning Representations*. 2024.

[2] Yibo Wang*, **Ruiyuan Gao***, Kai Chen*, Kaiqiang Zhou, Yingjie Cai, Lanqing Hong, Zhenguo Li, Lihui Jiang, Dit-Yan Yeung, Qiang Xu, and Kai Zhang. "DetDiffusion: Synergizing Generative and Perceptive Models for Enhanced Data Generation and Perception". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2024.

[3] Yijun Yang, **Ruiyuan Gao**, Xiaosen Wang, Tsung-Yi Ho, Nan Xu, and Qiang Xu. "MMA-Diffusion: MultiModal Attack on Diffusion Models". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2024.

[4] **Ruiyuan Gao**, Chenchen Zhao, Lanqing Hong, and Qiang Xu. "DiffGuard: Semantic Mismatch-Guided Out-of-Distribution Detection using Pre-trained Diffusion Models". In: *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 2023.

[5] Minhao Liu, Ailing Zeng, Qiuxia Lai, **Ruiyuan Gao**, Min Li, Jing Qin, and Qiang Xu. "T-WaveNet: A Tree-Structured Wavelet Neural Network for Time Series Signal Analysis". In: *The Tenth International Conference on Learning Representations*. 2022.

[6] Yijun Yang, **Ruiyuan Gao**, Yu Li, Qiuxia Lai, and Qiang Xu. "What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction". In: *Network and Distributed System Security Symposium (NDSS)*. 2022.

[7] Yijun Yang, **Ruiyuan Gao**, and Qiang Xu. "Out-of-Distribution Detection with Semantic Mismatch under Masking". In: *European Conference on Computer Vision*. Springer. 2022.

[8] Ailing Zeng, Xuan Ju, Lei Yang, **Ruiyuan Gao**, Xizhou Zhu, Bo Dai, and Qiang Xu. "DeciWatch: A Simple Baseline for 10x Efficient 2D and 3D Pose Estimation". In: *European Conference on Computer Vision*. Springer. 2022.

[9] Yaran Chen*, **Ruiyuan Gao***, Fenggang Liu, and Dongbin Zhao. "ModuleNet: Knowledge-Inherited Neural Architecture Search." In: *IEEE transactions on cybernetics* PP (2021). ISSN: 2168-2275 2168-2267. DOI: 10.1109/TCYB.2021.3078573. pmid: 34097629.

[10] **Ruiyuan Gao**, Hailong Yang, Shaohan Huang, Ming Dun, Mingzhen Li, Zerong Luan, Zhongzhi Luan, and Depei Qian. "PriPro: Towards Effective Privacy Protection on Edge-Cloud System running DNN Inference". In: *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. IEEE. 2021, pp. 334–343.

[11] Yijun Yang, **Ruiyuan Gao**, Yu Li, Qiuxia Lai, and Qiang Xu. "MixDefense: A Defense-in-Depth Framework for Adversarial Example Detection Based on Statistical and Semantic Analysis". In: *arXiv preprint arXiv:2104.10076* (2021).

[12] Ailing Zeng, Minhao Liu, Zhiwei Liu, **Ruiyuan Gao**, and Qiang Xu. "Hop-Aware Dimension Optimization for Graph Neural Networks". In: *arXiv preprint arXiv:2105.14490* (2021).

[13] Yaran Chen, Haoran Li, **Ruiyuan Gao**, and Dongbin Zhao. "Boost 3-D Object Detection via Point Clouds Segmentation and Fused 3-D GIoU-L_1 Loss". In: *IEEE Transactions on Neural Networks and Learning Systems* (2020).

[14] **Ruiyuan Gao**, Ming Dun, Hailong Yang, Zhongzhi Luan, and Depei Qian. "Privacy for Rescue: A New Testimony Why Privacy is Vulnerable In Deep Models". In: *arXiv preprint arXiv:2001.00493* (2019).

(* for equal contribution)

Competition

International Algorithm Case Competition (Huangpu) | *Distributed Training* Aug. 2022 – Nov. 2022

- As the **team leader** on the team of CURE Lab from CUHK.
- **2nd place** in competition problem of Adversarial Robustness Defense Algorithm of Deep Learning Models.

ASC Student Supercomputer Challenge | *Python, Docker, Distributed Programming* Jan. 2018 – Apr. 2019

- As a core member on the team of Beihang University, responsible for AI topics.
- **1st place** in tasks of Single Image Super Resolution (1/300+) and Face Super Resolution (1/20).
- First Prize & Highest LINPACK awards.

Awards & Scholarships

- Full Postgraduate Studentship, The Chinese University of Hong Kong.
- Outstanding Graduate in Beijing.
- Second-class Undergraduate Merit Scholarship, Beihang University.
- Special Undergraduate Merit Scholarship for Discipline Competition, Beihang University.
- Meritorious Winner, American College Students Mathematical Modeling Competition.

Technical Skills and Other

Languages: Python, C/C++, Java, Verilog
Frameworks: Pytorch, Tensorflow, Rails
Developer Tools: Linux and shell, Git, Docker, VS Code, Visual Studio, PyCharm, LaTeX
English: TOEFL 102, GRE V151 Q168 W4.0