Ziyi Yin

+1 8143214788 | zmy5171@psu.edu | https://ericyinyzy.github.io/

EDUCATION

Pennsylvania State University State College, USA

Ph.D. of Information Science and Technology 08/2022 - Now

Directed by *Prof.Fenglong Ma* and *Ting Wang*

Xi'an Jiaotong University Xi'an, China

Master of Science in Control Science and Engineering 09/2019 - 06/2022

Directed by *Prof. Zejian Yuan* at IAIR (Institute of Artificial Intelligence and Robotics)

Xi'an Jiaotong University Xi'an, China

Bachelor of Science in Automation (Honors Youth Program) 09/2015 - 06/2019

PAPER & PATENT

In Submission

- Triggerless Backdoor Attacks on Multimodal Large Language Models
  Ziyi Yin, Muchao Ye, Yuanpu Cao, Aofei Chang, Jiaqi Wang, Han Liu, Jinghui Chen, Ting Wang, Fenglong Ma
- Recent Advances in Predictive Modeling with Electronic Health Records
  Jiaqi Wang, Junyu Luo, Muchao Ye, Xiaochen Wang, Yuan Zhong, Aofei Chang, Guanjie Huang, ***Ziyi Yin****, Can Xiao, Jimena Sun, Fenglong Ma*
- Collaborative Diagnosis: Empowering Underserved Regions with Asymmetrical Reciprocity-based Cross-silo Federated Learning
  Jiaqi Wang*, **Ziyi Yin***, Quanzeng You, Lingjuan Lyu, Fenglong Ma (* denotes equal contribution)

Published Papers

- MedDiffusion: Boosting Health Risk Prediction via Diffusion-based Data Augmentation
  Yuan Zhong, Suhan Cui, Jiaqi Wang, Xiaochen Wang, **Ziyi Yin**, Yaqing Wang, Houping Xiao, Mengdi Huai, Ting Wang and Fenglong Ma
  *Proceedings of the SIAM International Conference on Data Mining (**SDM**), 2024.*
  (*Accepted*)
- VQAttack: Transferable Adversarial Attacks on Visual Question Answering via Pre-trained Models
  Ziyi Yin, Muchao Ye, Tianrong Zhang, Han Liu, Jinghui Chen, Ting Wang and Fenglong Ma
  *Proceedings of the Thirty-Eighth AAAI Conference on Artificial Intelligence (**AAAI**), 2024.*
  (*Accepted*)
- VLATTACK: Multimodal Adversarial Attacks on Vision-Language Tasks via Pre-trained Models.
  Ziyi Yin, Muchao Ye, Tianrong Zhang, Tianyu Du, Jinguo Zhu, Han Liu, Jinghui Chen, Ting Wang and Fenglong Ma
  *Proceedings of the 37th Conference on Neural Information Processing Systems (**NeurIPS**), 2023.*

- UniT: A Unified Look at Certified Robust Training against Text Adversarial Perturbation.
  Muchao Ye, **Ziyi Yin**, Tianrong Zhang, Tianyu Du, Jinghui Chen, Ting Wang and Fenglong Ma
  *Proceedings of the 37th Conference on Neural Information Processing Systems (**NeurIPS**), 2023.*
- Hierarchical Pretraining on Multimodal Electronic Health Records.
  Xiaochen Wang, Junyu Luo, Jiaqi Wang, **Ziyi Yin**, Suhan Cui, Yuan Zhong, Yaqing Wang and Fenglong Ma
  *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing (**EMNLP**), 2023.*
- **Multimodal Transformer Network for Pedestrian Trajectory Prediction.**
  Ziyi Yin, Ruijin Liu, Zhiliang Xiong, Zejian Yuan.
  *International Joint Conference on Artificial Intelligence **(IJCAI),** 2021.*
- Order-independent Matching with Shape Similarity for Parking Slot Detection.
  Ziyi Yin, Ruijin Liu, Zhiliang Xiong, Zejian Yuan.
  *British Machine Vision Conference (**BMVC**), 2021.*
- Attention-Oriented Action Recognition for Real-Time HRI.
  Ziyang Song, **Ziyi Yin**, Zejian Yuan, Chong Zhang, Wanchao Chi, Yonggeng Ling, Shenghao Zhang.
  *International Conference on Pattern Recognition (**ICPR**), 2020*
- Learning to Plan Semantic Free-Space Boundary.
  Ziyi Yin, Ziyang Song, Zejian Yuan.
  *International Conference on Image Processing (**ICIP**), 2019.*

Patent

- *An AI-based action recognition method and related devices*. Chinese Patent, published in 02/2020.

CORE RESEARCH & ENGINEERING PROJECTS

In Progress

Adversarial Robustness in Machine Learning 09/2022 -Now

- **Multimodal Adversarial Attacks on Vision-Language Tasks via Pretrained Models**

To verify adversarial vulnerability on unified multi-modal models, we

- Conduct adversarial attacks on multiple vision language tasks via pertained models, which is a more realistic setting.
- Propose a multi-modal attack strategy to cross-search image and text perturbations from both single-modal and multi-modal levels.

My contributions: proposal providing, paper writing

Finished

Perception of Autonomous Driving 12/2018 - 06/2021

- **Parking Slot Detection**

To detect parking slots in the more general scenarios (variant sizes an shapes), we

- Construct a Large-scale and Remote-view Parking Slot dataset (LRPS).

- Propose a two-level order-independent matching strategy to solve the order induced rotation problem

My contributions: dataset construction, proposal providing, paper writing

- **Pedestrian Trajectory Prediction**

To solve the problems of current CNNs or RNNs in compensating the highly dynamic motion information and massive parameters usages, we

- Introduce specific areas of optical flow to compensate the dynamic motion information, and also propose a compact representation method to improve the computational efficiency.
- Propose a Multimodal Transformer Network (MTN) to integrate distinct modalities in a multi-granularity manner.
- Our method achieves the SOTA performance with 107x fewer parameters on public datasets.

My contributions: investigation of the task, proposal providing, paper writing