

Zihao (Philip) DONG

Email: zihadong@g.ucla.edu Phone: +1 3102546253 Github: <https://github.com/ZHDphilip>

Education

University Of California,, School Of Engineering

Bachelor in Computer Science

Los Angeles, LA

2019/09 - 2023/06(expected)

- **GPA:** 3.93/4.0, departmental honor
- **Relevant coursework:** Machine Learning, Algorithms, DL CV, NLP, GNN, Theoretical ML, Adversarial Robustness, OS
- **Technical Skills:** Python, C++, Torch, OpenCV, Linux, Javascript, PHP

Industry Experience

Amazon (Java, AWS) SDE Summer Intern

Bellevue, WA, 2022/06 - 2022/09

- **Individually designing** an api for team's dynamodb tables capable of recording changes in the tables and writing to designated history tables, and querying the results through RESTful API Gateway. Separated design into Listener module and Inspector module.
- Implementing both modules using AWS Lambda function and using AWS API GW to invoke the lambdas to query for events in a specific region in a given time period.
- Testing the functions with unit tests, reached 100% line coverage; Tested the lambdas in AWS console and made sure the api is able to **process ≈ 1000 TPS of incoming events** from around the globe, and **serve desired query/invoke rate of > 1 TPS**.
- Implemented **additional features** other than asked in the project spec, and saved them remotely for further development.
- Presented my work in front of a team of 50+ engineers and responded to all questions and concerns successfully with reasoning

Agile Robotics (C++, cmake, opencv, halcon) Summer Intern

Beijing, 2021/06 - 2021/09

- Improved robot camera calibration process by implementing image acquisition using camera SDK, allowing for automatic image acquisition and reducing unnecessary step (using separate software to take image and copy to the calibration folder)
- Work Individually on Robot hand-eye-calibration, 3D reconstruction through Triangulation and object pose estimation through Coordinate Matrix Calculation for a FoxConn iPhone Assembling Project. Reached ≤ 0.5 mm accuracy. **The product was bought as part of an assembly robot by FoxConn for 250,000 RMB ($\sim \$40,000$) per set * 20 sets.**
- Tested the accuracy of the calibration by calculating the distance between 2 feature points (originally 10cm away from each other) after undistorting 2 test images, one from left cam, the other from the right camera.
- Extended the project into a general C++ Class capable of calibrating Intrinsic Parameters and/or External Parameters of any single camera, stereo camera, and hand-eye system.

Jiefeng Institute (Python, NLP) Summer Algorithm Intern,

Beijing, Remote, 2020/07 - 2020/09

- Implemented Python programs to extract keywords from 100,000+ JSON format bid contracts in the MySQL database using Jieba Library for Chinese sentence segmentation for further analysis and model training, and recommending companies based on their respective professional fields and the customers' project requirements
- Improved the accuracy of Jieba Library on recognizing compound words. Optimized the data structure of new word detection using Trie, achieved 20+ x speedup on average. Ranked the key words by frequency and removed those with \leq threshold appearances to avoid selecting words like location, company name as professional field. Compared the generated keywords with human labeled keywords and achieved +30% relevance.

Research and Projects

Robustness of Network Trained on Condensed Dataset

with Prof. Chojui Hsieh, 2022/10-present

- Investigating Dataset Condensation methods and re-generating their results using existing code on github

Adversarial Attack on ViT (Python, Vision, Adversarial Attack)

with Prof. Chojui Hsieh, 2022/03-2022/06

- Noticed the preconditioning matrices of Shampoo Optimizer has resemblance to patch characteristic of ViT, developed a new adversarial attack method using Matrix Form Shampoo
- Determining the best perturbation budget and learning rate for Shampoo Attack by considering success rate and perturbation percentage such that the attack converges. Achieved similar SR (99%+) and time comparing to state-of-the-art PGD baseline
- Experiments on attacking robust-trained ViT, success rate was not as good as non-robust trained ViT.

3D Generative Model Research (Python, ML, Vision)

with Prof. Bolei ZHOU, 2022/03-2022/09

- Exploring generative models related to Neural Radiance Field, like NeRF and StyleNeRF. Try to extract 3D shapes using these models from the CARLA dataset for [MetaDrive](#).
- Noticed artifacts in the extracted shapes, especially near the bottom of the car, concluded the artifacts come from dataset bias
- Improving UNICORN by leveraging images from consecutive frames. Calculating the camera extrinsic param and use 3d mesh normal vectors with camera position to compute the weight for each image to update the mesh

Hard Label Node Injection Attack GNN (Python, Attack, GNN)

with Prof. Yizhou SUN, 2022/03-2022/06

- Expanding an existing hard label edge attack on GNN to a node injection attack by expanding the perturbation matrix and inject isolated new nodes into the graph, hoping that the new nodes can be connected into the graph to create adversarial instance
- Do experiments on the new node feature initialization, and found mean (of all other nodes) initialization works the best
- Found that cannot guarantee all new nodes are injected, and isolated nodes may still perturb the model prediction
- Proposed an iterative approach where we gradually increase the number of nodes injected until reaching the budget. Experiments shown this method decreases perturbed edge count by around 3, and also mitigated the perturbation from unconnected new nodes
- Overall our method achieved 51% success rate on a budget of perturbing 10% nodes on COIL-DEL dataset.