Xindi (Cindy) Wu

+1 (412)-726-0470 | xindiw@andrew.cmu.edu | Google Scholar | Github | Linkedin

Education

Carnegie Mellon University *Pittsburgh, PA*
Master of Science in Computer Vision, School of Computer Science *Aug. 2020 - Dec. 2021*
- Selected Courses: Introduction to Machine Learning, Computer Vision, Math foundation for Robotics

Xi'an Jiaotong University *Xi'an, China*
Bachelor of Computer Science, Honors Youth Program *Sept. 2016- July 2020*

Experience

Megvii (Face++) *Beijing, China*
Computer Vision research developer Intern w/ Banghuai Li *June 2020 - Sept. 2020*
- Researched & designed few shot learning models built on Detectron2 with metric learning based methods for object detection
- Provided a loosened embedding method to map every training image to its most similar examples with the same label
- Implemented mixup data augmentation and contrastive loss to help build the relation graph after Region Proposal Networks

Carnegie Mellon University, Language Technology Institute Pittsburgh, PA
Research Assistant w/ Haohan Wang & Prof. Eric P. Xing *Apr. 2019 - June 2020*
- Demonstrated a relationship between frequency spectrum of image data and generalization behavior of CNNs
- Tested hypothesis used ResNet-18 for MNIST/CIFAR10/FashionMNIST. Indicated that natural prefers to pick up at he Low Frequency Components (LFC), yet lable-shuffled data can be pick up at either LFC or High Frequency Components (HFC)[1]

Carnegie Mellon University, Computational Biology Department *Pittsburgh, PA*
Research Assistant w/ Prof. Min Xu *Mar. 2019 - June 2020*
- Proposed Regularized Adversarial Training to push decision boundary away from training data while maximizing accuracy on unperturbed examples to improved the robustness of subtomogram SoTA classification models [3]

Xi'an Jiaotong University, Institute of Artificial Intelligence and Robotics *Xi'an, China*
Research Assistant w/ Prof. Jinjun Wang & Prof. Pengju Ren *Dec. 2017 - Feb.2019*
- Introduced a self-paced regularizer to select reliable samples for fine-tuning each CNNs and implemented multi-view self-paced clustering by minimizing ranking loss and identification loss. Alternative optimization strategy (AOS) is adopted to optimize.
- Achieved higher mAP & Rank-1 by 4.44% & 2.2% on ResNet50; improved 6.04% & 4.6% at mAP & Rank-1 on DenseNet121[4]

Projects

Transferable Adversarial Attacks on Deep Reinforcement Learning Link Jan. 2020 - March 2020
- Implemented the attacks to minimize the rewards of substitute target policies against DRL
- Outperforms the existing attacks when the system dynamics or the action space changes in both HalfCheetah and Walker2d

Robustifying Trained Models by Reducing Exploitation of Data Idiosyncrasy Link March 2019 - May 2019
- Developed a rigorous mathematical framework to put bounds on previously-identified trade-off between robustness & accuracy
- Implemented three lightweight methods to increase model robustness to verify the framework's implications
- Improved robustness by perturbing weights after the models are trained with barely any computational efforts

Multitask Learning With Enhanced Modules [5] *Jan. 2018 - May 2018*
- Applied scale parameters for each module in the multi-layer structure and trained multitask learning models
- Used x5.23 fewer generations to achieve 99% accuracy on a source-to-target MNIST classification task compared with DeepMind's PathNet. Increased the accuracy of CIFAR- SVHN transfer task by x1.9. Achieved 70.75% accuracy on miniImageNet

Smooth Kernels Improve Adversarial Robustness Link *Aug. 2019 - Oct. 2019*
- Designed a regularization scheme that penalizes large differences between adjacent components within kernels
- Achieved numerically the best adversarially robustness across most settings, suggesting the effective of smooth regularization

Publications

[1] High Frequency Component Helps Explain the Generalization of Convolutional Neural Networks.
H. Wang, **X. Wu**, Z. Huang, EP. Xing *Conference on Computer Vision and Pattern Recognition (CVPR) 2020*

[2] Transferable Adversarial Attacks on Deep Reinforcement Learning
X. Pan, Y. Cao, **X. Wu**, E. Zelikman, C. Xiao, Y. Sui, R. Chakraborty, RS. Fearing *Workshop on Adversarial ML at CVPR, 2020*

[3] Regularized Adversarial Training (RAT) for Robust Cellular Electron Cryo Tomograms Classification
X. Wu, Y. Mao, H. Wang, X. Zeng, X. Gao, EP. Xing, M. Xu *IEEE Int. Conf. on Bioinformatics and Biomedicine, 2019*

[4] Deep Self-Paced Learning for Semi-supervised Person Re-identification Using Multi-View Self-Paced Clustering
X. Xin, **X. Wu**, Y. Wang, J. Wang *IEEE 26th Int. Conf. on Image Processing (ICIP), 2019*

[5] Multitask Learning With Enhanced Modules
Z. Zheng, Y. Wei, Z. Zhao, **X. Wu**, Z. Li and P. Ren *IEEE 23rd Int. Conf. on Digital Signal Processing (DSP) 2018*

Skills

Languages: Python, C/C++/C#, Matlab, R, SQL, Bash, HTML/CSS
Development Tools: Spark, Hadoop, RabbitMQ, Celery; Docker;
Deep Learning Tools: PyTorch, TensorFlow, Keras, Caffe; OpenCV; MuJoCo, OpenAI Gym