Computer Science and Engineering Department
Michigan State University
East Lansing, MI 48824, USA

Mobile: (+1)-347-574-5875
Email: zhan1853@msu.edu
Website: https://damon-demon.github.io

RESEARCH FOCUSES

Deep learning: Adversarial Learning (adversarial attack & defense), Computer Vision (image classification, object detection/tracking)
Optimization: Sparse optimization for deep model compress, Zeroth-order black-box optimization

EDUCATION

Ph.D. Candidate in Computer Science, Michigan State University Jan. 2021– Present.

M.S. in Electrical Engineering, Columbia University Aug. 2018– Dec. 2019

B.Eng in Electronic and Electrical Engineering, University of Sheffield Sep. 2015– July 2018

PUBLICATIONS

Google Scholar

[1] **Y. Zhang**, Y. Yao, J. Jia, J. Yi, M. Hong, S. Chang, S. Liu, "How to Robustify Black-Box ML Models? A Zeroth-Order Optimization Perspective", International Conference on Learning Representation (*ICLR'22 - Spotlight*)

[2] Y. Gong, Y. Yao, Y. Li, **Y. Zhang**, X. Liu, X. Lin, S. Liu, "Reverse Engineering of Imperceptible Adversarial Image Perturbations", International Conference on Learning Representation (*ICLR'22*)

[3] **Y. Zhang**, X. Liu, B. Wu, A. Walid, "Video Synthesis via Transform-Based Tensor Neural Network", ACM International Conference on Multimedia (*ACM MM'20*)

[4] X. Han, B. Wu, X. Liu, Z. Shou, **Y. Zhang**, L. Kong, "Tensor FISTA-Net for Real-Time Snapshot Compressive Imaging", AAAI Conference on Artificial Intelligence (*AAAI'20*)

RESEARCH EXPERIENCE

Model Compression for Object Tracking [**DARPA IP2 Program**] Sept. 2021 - Present
Supervisor: Sijia Liu (MSU)

- Propose a hardware-friendly pruning scheme for the task of object tracking
- Adopt knowledge distillation to acquire lightweight and high-accuracy model
- Achieve 90% model sparsity without performance loss for ResNet-50 under BDD100K dataset

Robustification of Black-Box ML Models by Zeroth-Order Optimization Jan.2021-Oct.2021
Supervisor: Sijia Liu (MSU) Collaborator: Mingyi Hong (UMN), Shiyu Chang (UCSB)

- Formulate black-box defense problem through the lens of zeroth-order (ZO) optimization
- Propose scalable ZO optimization method to tackle defense challenge in high dimension
- Achieve state-of-the-art certified robustness on CIFAR-10 and STL-10
- Extend black-box defense from image classification to image reconstruction
- **Publications**: [1]

Reverse Engineering of Deceptions (RED) [**DARPA RED Program**] Mar. 2021 - Oct. 2021
Supervisor: Sijia Liu (MSU) Collaborator: Xiaoming Liu (MSU), Xue Lin (NEU)

- Design Reverse Engineering of Deceptions (RED) pipeline to recover adversarial perturbations
- Integrating RED with data augmentation techniques to overcome unforeseen attacks
- Identify RED principles: pixel-level reconstruction, prediction-level alignment, and attribution-level saliency recovery
- **Publications**: [2]

Video Synthesis via Transform-Based Tensor Neural Network Aug. 2019 - May 2020
Supervisor: Anwar Walid (Columbia University)

- Propose an iterative tensor ISTA algorithm for video processing
- Design a Transform-Based Tensor-Net for video frame synthesis task
- Achieve state-of-the-art PSNR on KTH and UCF-101
- **Publications**: [3]

Tensor FISTA-Net for Real-Time Snapshot Compressive Imaging April. 2019 - Oct. 2019
Supervisor: Linghe Kong (SJTU)

- Propose a novel Tensor FISTA-Net for SCI reconstruction
- Utilize tensor form to reduce time and memory consumption significantly
- Achieve state-of-the-art reconstruction accuracy and speed on both synthetic and real datasets
- Small model size (12MB) makes it practical for real-time IoT applications
- **Publications**: [4]

PROGRAMMING SKILLS

- Python, PyTorch, OpenCV, MATLAB, R

SERVICE

- Reviewer for ICASSP, CVPR, ACMMM, ICLR