Hanxiu Zhang

Research Interest: Computer Vision, Deep Learning, Adversarial Robustness

Email: hanxiu_zhang@stu.ecnu.edu.cn Tel: (+86)18332247567
Homepage: hanxiuzhang.github.io

Education

East China Normal University (ECNU, 985 Project) Sep. 2021 - Present
Master's degree student | Software Engineering | GPA: 3.86/4 (WES: 3.88/4) *Shanghai, China*

Northeastern University (NEU, 985 Project) Sep. 2017 - Jun. 2021
Bachelor's degree | Software Engineering | GPA: 4.03/5 (WES: 3.86/4) *Shenyang, China*

Research Experience

Adversarial frequency domain watermarking algorithm for image security (Pytorch/OpenCV)
Jun. 2022 - Dec. 2022

- Computer Vision | Adversarial Example | Image Frequency
- Propose a novel adversarial frequency watermark framework
- Combine frequency watermark and gradient-based adversarial perturbation to protect images
- Optimize perturbation to improve attack imperceptibility
- "Making Adversarial Attack Imperceptible in Frequency Domain: A Watermark-based Framework" accepted as oral in ICME2023

Radar signal classification model adversarial robustness analysis (Pytorch)
Oct. 2021 - Dec. 2021

- Computer Vision | Adversarial Example
- Evaluate radar signal spectogram classification model robustness with adversarial attacks

Zero-shot learning algorithm for radar signal (Matlab/Pytorch/Sklearn)
Nov. 2020 - Jun. 2021

- Computer Vision | Zero-shot Learning | Signal Frequency
- Convert radar signals into frequency spectral maps and extract their fractal dimensional features
- Train ResNet to extract frequency spectral maps' representations
- Classify the signals with SVM/Random Forest/Bayesian classifiers
- Construct signal zero-shot classification model based on DAP algorithm

Real-time strip defect monitoring system (OpenCV)
Sep. 2018 - Jun. 2020

- Computer Vision | Defect Detection
- Denoise and identify edge defect for surveillance video of strip rolling
- Locate edge defect using convex hull detection algorithm

Publications

1. **Hanxiu Zhang**, Guitao Cao*, Xinyue Zhang, Jing Xiang, Chunwei Wu. Making Adversarial Attack Imperceptible in Frequency Domain: A Watermark-based Framework. ICME2023 (CORE-A)

2. Jing Xiang, Xinyue Zhang, Chunwei Wu, **Hanxiu Zhang**, Guitao Cao*, Hong Wang. Discriminative Feature Mining and Alignment for Unsupervised Domain Adaptation. IJCNN2023 (CORE-B)

Awards & Honors

- Nezha Technology Outstanding Student Scholarship 2023
- Northeastern University Outstanding Graduates 2021
- Northeastern University Outstanding Student Scholarship 2018/2019/2020/2021
- National Inspirational Scholarship of China 2018/2019/2020/2021
- National Outstanding University Student Innovation Training Program 2020
- Honorable Mention of Mathematical Contest In Modeling 2020
- Second Prize of National University Mathematics Competition in China 2018

Specialized Skills

Programming language:	Python, Matlab, Java, JavaScript, HTML, SQL
English proficiency:	TOEFL iBT 95 (Reading 29/ Listening 23/ Speaking 22/ Writing 21)