WEIYU SUN

Tel: (+86) 15050551145 Email: weiyusun@smail.nju.edu.cn Personal Web: swy666.github.io

EDUCATION EXPERIENCE

Nanjing University, Jiangsu, China B.S. in Electronic and Computer Engineering 2015.9-2019.6
Selected high-scored courses:
Numerical Analysis: [98/100], C++ Programming: [93/100]

Nanjing University, Jiangsu, China M.S. in Electronic and Computer Engineering 2019.9-2022.6
Selected high-scored courses:
Matrix Theory: [96/100]

RESEARCH EXPERIENCE

Pennsylvania State University - University Park *Research Internship 2022.June - present*
Computer Science & Trustworthy AI *Tutor: Jinghui Chen*

- Explored the backdoor security issues on self-supervised learning (SSL) scenarios: revealed the natural "immune system" (e.g., negative pairs in SimCLR) of SSL against the backdoor threat, then proposed a bi-level optimization paradigm to compromise such a "immune system" and enhance the backdoor attack success rate.

- Conducted extensive experiments on various datasets (e.g., ImageNet-100) and SSL methods (e.g., SimCLR and BYOL) to verify the effectiveness of our paradigm, and the corresponding paper "Backdoor Contrastive Learning via Bi-level Trigger Optimization", which is currently under review in ICLR 2024.

- Investigated the white / black-box targeted attack issues within the self-supervised learning chain (i.e., downstream train via the pre-trained encoder) and explored multiple forms of adversarial pattern designs (e.g., adversarial perturbation over the frequency domain) to challenge a higher attack success rate.

The Hong Kong University of Science and Technology (HKUST) *Research Internship 2023.Feb-2023.June*
Algorithm research for Healthcare *Tutor: Yingcong Chen*

- Explored the label and attribute conflicts problem within the remote photoplethysmography (rPPG) DNN model training; developed a new label representation and gradient-level optimization paradigm (namely DOHA, DOmain-HArmonious framework) to mitigate these conflicts.

- Conducted extensive experiments to verify the effectiveness of DOmain-HArmonious framework, including different cross-datasets scenarios and inner-dataset scenarios; then drafted the paper "Resolve Domain Conflicts for Generalizable Remote Physiological Measurement." which can refer to my published works below.

- Explored the self-supervised way to efficiently train the rPPG DNN model via the new label representation (proposed in DOHA), then accomplished on the paper "Self-similarity Prior Distillation for Unsupervised Remote Physiological Measurement" with co-workers.

Nanjing University - Jiangsu, China *Postgraduate & Research Assistant 2019.Sep-2023.Feb*
Algorithm development & Computer Programming *Tutor: Ying Chen*

- Developed the rPPG algorithm to precisely extract physiological information (e.g., heart rate) from facial video.

- Develop two versions (C++ and Python, respectively) of rPPG-algorithm-based software with UI interface (code here), which then got integrated into the online health monitoring platform of Nanjing University workshops.

- Drafted the patent investigating the label issues (temporal misalignment) for rPPG DNN model training.

- Cooperated with lab peers on developing the DNN algorithm to assist the diagnosis on liver cancer, then drafted a patent "A Method of Image Classification Based on SCCNN Network" on it.

PAPERS (PUBLISHED)

[1] **Weiyu Sun**, Xinyu Zhang, Hao Lu, Ying Chen, Yun Ge, Xiaolin Huang, Jie Yuan, and Yingcong Chen. 2023. Resolve Domain Conflicts for Generalizable Remote Physiological Measurement. In Proceedings of the 31st ACM International Conference on Multimedia (MM '23). Association for Computing Machinery, New York, NY, USA, 8214–8224. https://doi.org/10.1145/3581783.3612265. (project website)

[2] Zhang, Yan & Zhou, Han & Chu, Kaiyue & Wu, Chuanfeng & Ge, Yun & Shan, Guoping & Zhou, Jundong & Cai, Jing & Jin, Jianhua & **Sun, Weiyu** & Chen, Ying & Huang, Xiaolin. (2022). Setup error assessment based on "Sphere-Mask" Optical Positioning System: Results from a multicenter study. Frontiers in Oncology. 12. 10.3389/fonc.2022.918296.

PAPERS (UNDER REVIEW & ARXIV)

[1] **Weiyu Sun**, Jinghui Chen, Lin Lu, et. al. "Backdoor Contrastive Learning via Bi-level Trigger Optimization." Submitted to the Twelfth International Conference on Learning Representations (ICLR 2024), currently under review, nevertheless the latest reviews and pdf can refer to this website.

[2] Xinyu Zhang, **Weiyu Sun**, Hao Lu, Yingcong Chen, et. al. "Self-similarity Prior Distillation for Unsupervised Remote Physiological Measurement." Submitted to the IEEE Transactions on Multimedia (TMM), currently under review (for already 6 months, really painful, man).

ADDITIONAL INFO AND SELECTED HONERS / AWARDS

- Skilled in Python (pycharm, cross programming with C++, cython), C++ (UI interface, multiprocessing programming), Matlab, Latex.

- TOFEL(100): r29, l26, s20, w25; GRE(325): w3.5, v157, q168

- People's Scholarship of China, 2017-2018

- Academic Scholarship of Nanjing University $\times$ 3, 2019-2022

- China national patents $\times$ 2

- National Second Prize (top 10%) in China Post-graduate Mathematical Contest in Modeling, 19th, 2022

- Rank No.2 in Jiangsu Province, Microsoft Innovation Cup Global Student Technology Competition, 2022.