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 & PROJECT EXPERIENCE

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

• **Research on SSL backdoor attack:** Investigating the data poisoning based backdoor attacks (DPBAs) against self-supervised learning (SSL): 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 an "immune system" and improve the attack performance (claims state-of-the-art performance over widely-used datasets like ImageNet-100). The corresponding paper, "Backdoor Contrastive Learning via Bi-level Trigger Optimization", is under review in ICLR 2024.

• **Research on targeted attack in the SSL chain:** Investigated the white / black-box targeted attack in downstream fine-tuning scenarios, explored multiple forms of adversarial pattern designs (e.g., frequency domain adversarial perturbation, dynamic patch) to challenge a higher attack success rate. The corresponding paper is under drafting.

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

• **DOHA-rPPG:** 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. DOHA claims state-of-the-art performance over widely-used datasets like VIPL-HR and PURE. The corresponding paper, "Resolve Domain Conflicts for Generalizable Remote Physiological Measurement", is accepted by ACM MM 2023.

• **SSPD-rPPG:** Explored the self-supervised way to efficiently and conveniently train the rPPG DNN model via the label representation proposed in DOHA-rPPG, accomplished the paper "Self-similarity Prior Distillation for Unsupervised Remote Physiological Measurement" as the 2nd author.

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

• **Programmings on healthcare applications:** Developed and optimized the rPPG algorithm to precisely extract physiological information (e.g., heart rate, respiratory rate) from facial video. Developed two versions (C++ and Python, respectively) of rPPG-algorithm-based software with UI interface (gadget code here), integrated the rPPG algorithm into the online health monitoring platform of Nanjing University workshops, then drafted a patent enunciating the label conflict issues within rPPG DNN training (one contribution in DOHA-rPPG). Invited by some companies (Samsung, Huawei) to integrate these algorithms into their products.

• **Wearable devices for ECG measurement:** Investigated the capacitor-based electrode to measure the subject's electrocardiogram (ECG) without the necessity of electrode-skin contact (i.e., can measure ECG through clothes); then concluded it in my undergraduate dissertation.

• **Research on DNN-assisted liver cancer diagnosis:** Cooperated with lab peers on developing the DNN model to assist in the diagnosis of liver cancer (whether it belongs to hepatocellular carcinoma (HCC), intrahepatic cholangiocarcinoma (ICC), or benign tumor). This project won the prize in the Microsoft Innovation Cup that year and drafted a patent, "A Method of Image Classification Based on SCCNN Network", about 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] Yan Zhang, Han Zhou, Kaiyue Chu, Chuanfeng Wu, Yun Ge, Guoping Shan, Jundong Zhou, Jing Cai, Jianhua Jin, **Weiyu Sun**, Ying Chen, Xiaolin Huang. 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; arXiv here).

[3] Xinyu Zhang, **Weiyu Sun**, Ying Chen. "Tackling the Non-IID Issue in Heterogeneous Federated Learning by Gradient Harmonization." Submitted to the IEEE Signal Processing Letters (SPL), currently under review (for already 2 months arXiv here).

ADDITIONAL INFO AND SELECTED HONERS / AWARDS

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

- GRE(325): w3.5, v157, q168

- People's Scholarship of China, 2017-2018

- Academic Scholarship of Nanjing University × 3, 2019-2022

- China national patents × 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.