ZHANHAO HU

Tsinghua University, Beijing, China, 100084

+86 18801306893 ⋄ huzhanha17@mails.tsinghua.edu.cn

EDUCATION

Tsinghua University, Beijing *2017 - Present*

Ph.D., Computer Science and Technology

Advisor: Bo Zhang and Xiaolin Hu

Dessertation: The Practicality of Physical Adversarial Examples for Deep Learning Models.

Tsinghua University, Beijing *2013 - 2017*

B.S., Mathematics and Physics

Dessertation: STDP-based learning for spiking neural networks

PUBLICATIONS

Under review & *Preprint*

Qiongxiu Li, Xia Li, **Zhanhao Hu**, Xiao Li, Xiaolin Hu. (under review). On the Hardness of Input Reconstruction Attack via Gradient Sharing in Federated Learning: A Cryptographic View.

Tong Wang, Xiaohui Kuang, Qianjin Du, **Zhanhao Hu**, Huan Deng, Gang Zhao. (under review). Driving into Danger: Adversarial Patch Attack on End-To-End Autonomous Driving Systems Using Deep Learning

Xiao Li, Wei Zhang, Yining Liu, **Zhanhao Hu**, Bo Zhang, Xiaolin Hu. (preprint). Anchor-Based Adversarially Robust Zero-Shot Learning Driven by Language. arXiv:2301.13096.

Xiaopei Zhu, **Zhanhao Hu**, Siyuan Huang, Jianmin Li, Xiaolin Hu. (under review). Hiding from Infrared Detectors in Real World with Adversarial Clothes.

Xiaopei Zhu, Siyuan Huang, **Zhanhao Hu**, Jianmin Li, Xiaolin Hu. (under review). Physical Adversarial Attack to Person Detectors in Infrared Images based on 3D Modeling.

Xiao Li, Qiongxiu Li, **Zhanhao Hu**, Xiaolin Hu. (preprint). On the Privacy Effect of Data Enhancement via the Lens of Memorization. arXiv:2208.08270.

Published

Zhanhao Hu, Wenda Chu, Xiaopei Zhu, Hui Zhang, Bo Zhang, Xiaolin Hu (2023). Physically Realizable Natural-Looking Clothing Textures Evade Person Detectors via 3D Modeling. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).

Zhanhao Hu, Jun Zhu, Bo Zhang, Xiaolin Hu (2022). Amplification trojan network: Attack deep neural networks by amplifying their inherent weakness. Neurocomputing, 505, 142-153.

Zhanhao Hu, Siyuan Huang, Xiaopei Zhu, Fuchun Sun, Bo Zhang, Xiaolin Hu (2022). Adversarial texture for fooling person detectors in the physical world. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR Oral).

Xiaopei Zhu, **Zhanhao Hu**, Siyuan Huang, Jianmin Li, Xiaolin Hu (2022). Infrared invisible clothing: Hiding from infrared detectors at multiple angles in real world. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR Oral).

Zhanhao Hu, Tao Wang, Xiaolin Hu (2017). An stdp-based supervised learning algorithm for spiking neural networks. In Neural Information Processing: 24th International Conference (ICONIP).

TALKS AND SYMPOSIA

Adversarial texture for fooling person detectors in the physical world. Oral Presentation at the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2022/06

Adversarial texture for fooling person detectors in the physical world. Shield Laboratory. 2022/06

Adversarial texture for fooling person detectors in the physical world. Beijing RealAI Intelligent Technology Co., Ltd. 2022/05

Adversarial texture for fooling person detectors in the physical world. Beijing Jiangmen Development Venture Capital Center, L.P. 2022/05

Defend Adversarial Examples by Robust Sparse Coding Neural Networks. Poster Presentation at the McGovern Institutes Joint Neuroscience Symposium, MIT. 2019/03

TEACHING EXPERIENCE

Neural and Cognitive Computation (No.80240642), Tsinghua University *2019 Autumn*
Teaching Assistant

Neural and Cognitive Computation (No.80240642), Tsinghua University *2018 Autumn*
Teaching Assistant

PROFESSIONAL SERVICE

Journal Reviewer

· TNNLS, TPAMI

Conference Reviewer

· CVPR, ECCV, AAAI, ICML, ICIST, ICACI, ICICIP, ISNN

Workshop Reviewer

· ICML2021 adversarial ML workshop