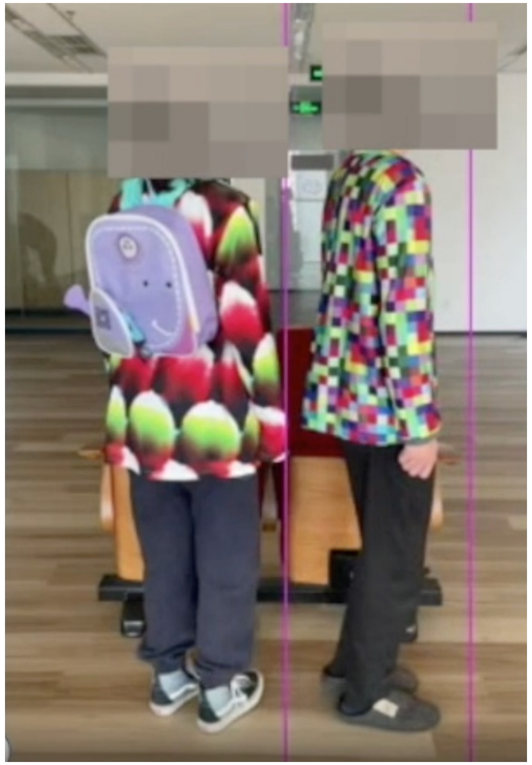
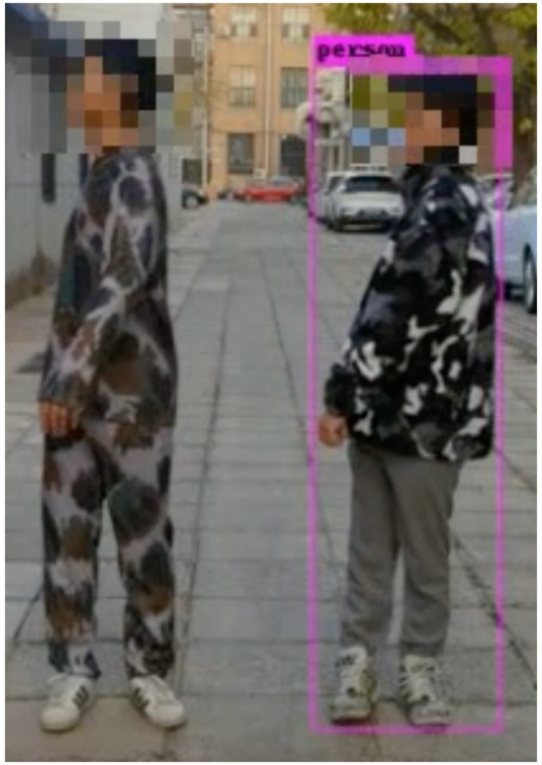
My research interest primarily includes adversarial examples and privacy in deep learning models.

See below for my work on physical adversarial examples. We are the first in this field that propose to attack from multiple viewing angles.



Adversarial textures [1]:

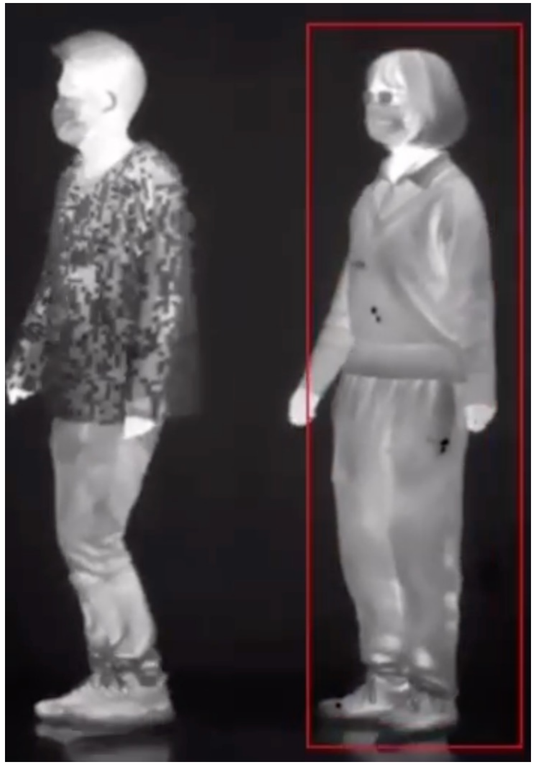


Adversarial camouflage pattern [2]:

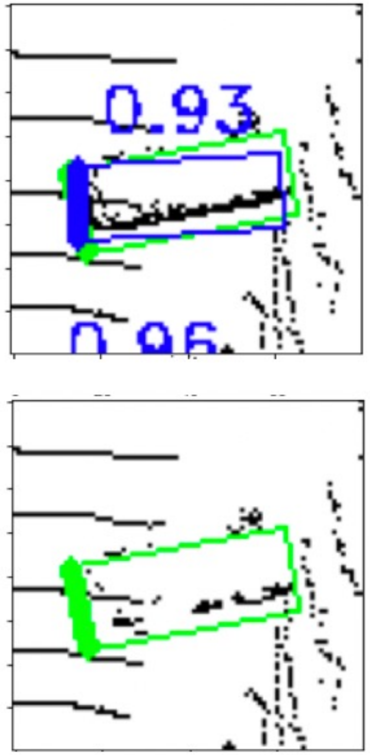
[1] Zhanhao Hu, Siyuan Huang, Xiaopei Zhu, Fuchun Sun, Bo Zhang, Xiaolin Hu (2022). Adversarial texture for fooling person detectors in the physical world. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).

[2] 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).

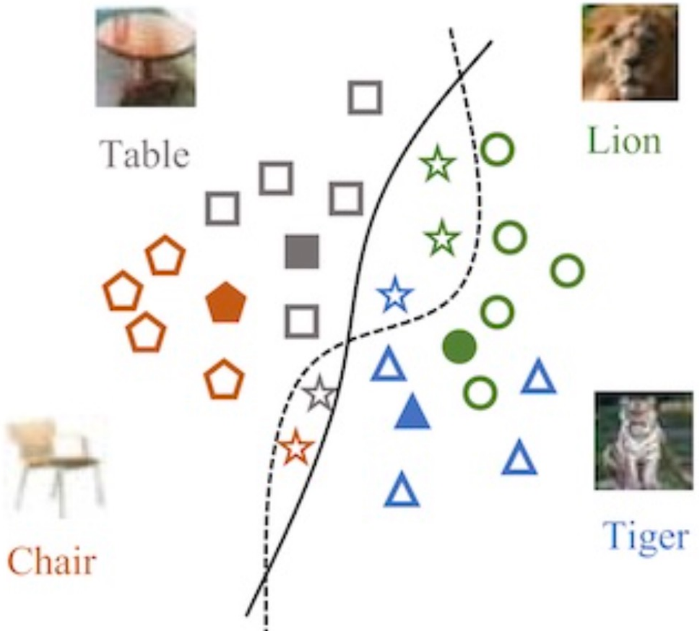
I also worked on physical adversarial examples of other domains, like infrared imaging and Lidar point cloud detection. I am also interested in general adversarial learning topics.



Adversarial infrared QR pattern [1]:



Lidar point cloud (ongoing)

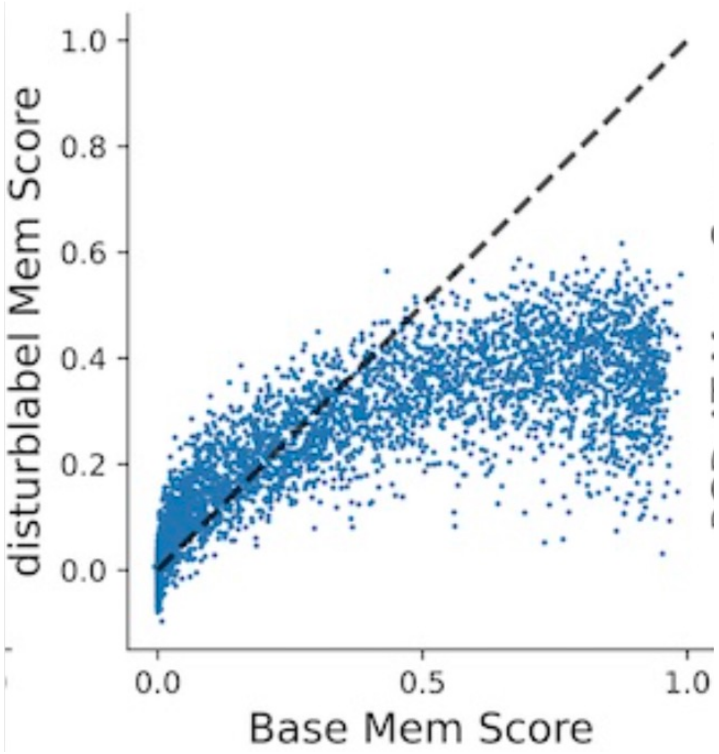


Zero-shot adversarial robustness[2]

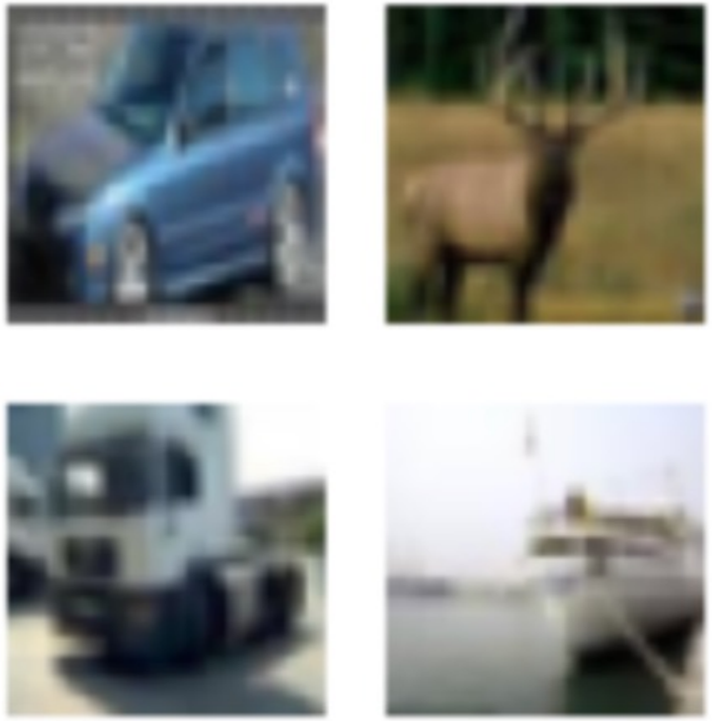
[1] Xiaopei Zhu, Zhanhao Hu, Siyuan Huang, Jianmin Li, Xiaolin Hu (2022). Infrared invisible clothing: Hiding from infrared detectors at multiple angles in real world. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).
[2] Xiao Li, Wei Zhang, Yining Liu, Zhanhao Hu, Bo Zhang, Xiaolin Hu. (preprint). LanguageDriven Anchors for Zero-Shot Adversarial Robustness. arXiv:2301.13096.

Another research interest of mine is privacy in deep learning. I recently mainly focused on membership inference attacks in cv models and privacy in federal learning.

See more details on my personal website: https://whothu.github.io/



Analyzing privacy (by MIA attack) via memorization scores [1]:



Data reconstruction in federal learning via a cryptographic view (under review):

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

[2] Qiongxiu Li, Lixia Luo, Agnese Gini, Zhanhao Hu, Xiao Li, Chengfang Fang, Xiaolin Hu, Jie Shi. (under review). On the Hardness of Input Reconstruction Attack via Gradient Sharing in Federated Learning: A Cryptographic View.