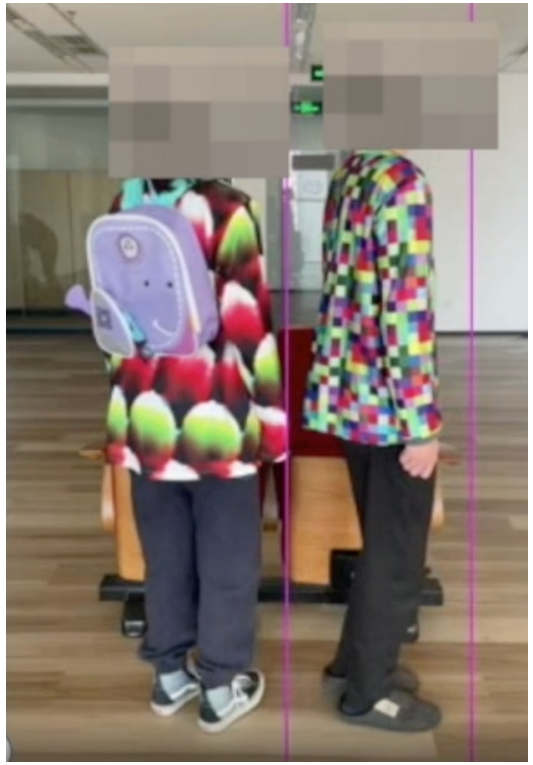
My research interest primarily includes (both digital and physical) adversarial examples and privacy in deep learning models.

- Physical Adversarial Examples:
  We are the first in this field that propose attacking from multiple viewing angles.



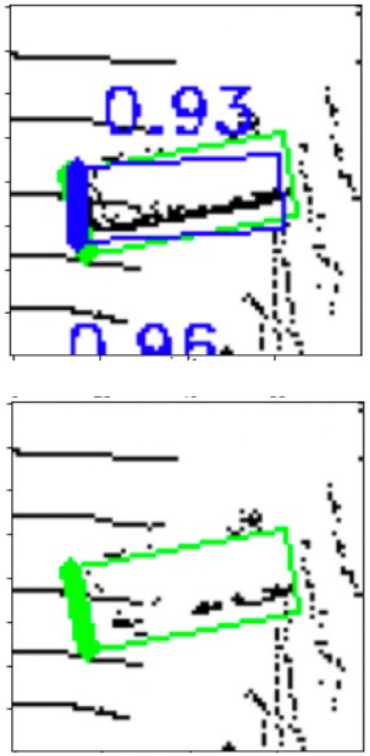
Adversarial textures [1]:

Adversarial camouflage pattern [2]:

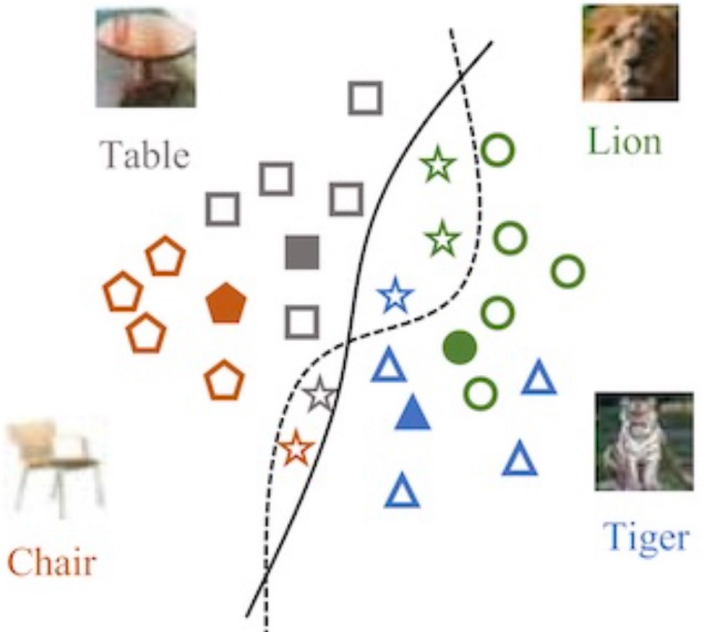
[1] Zhanhao Hu, Siyuan Huang, Xiaopei Zhu, Fuchun Sun, Bo Zhang, Xiaolin Hu (2022). Adversarial texture for fooling person detectors in the physical world. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).
[2] Zhanhao Hu, Wenda Chu, Xiaopei Zhu, Hui Zhang, Bo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

- Physical Adversarial Examples in Various Domains
  Additionally, I conduct research on physical adversarial examples in other domains such as infrared imaging and Lidar point cloud detection.
- Digital Adversarial Examples
  I also explore various aspects of digital adversarial learning.

Adversarial infrared QR pattern [1]:



Lidar point cloud (ongoing)



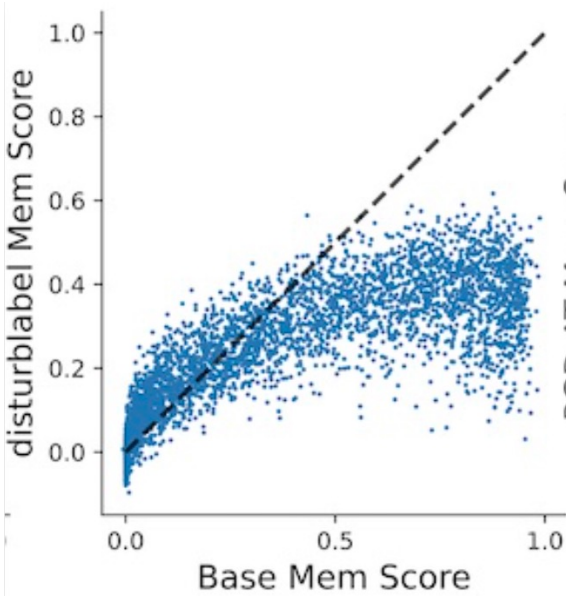
Zero-shot adversarial robustness[2]

[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.

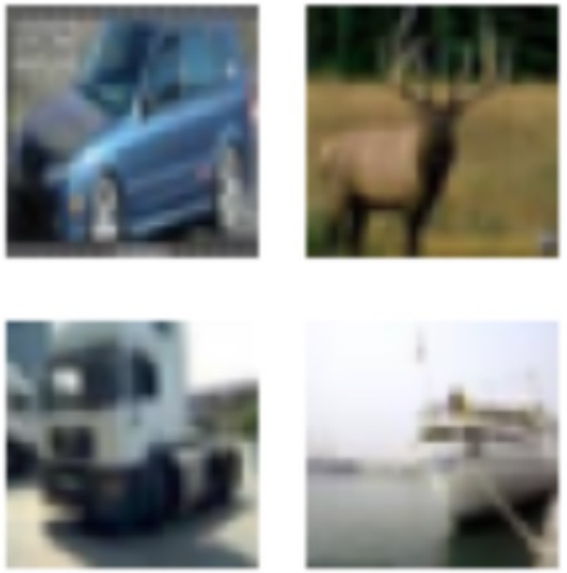
- Privacy in Deep Learning

  I recently focused on membership inference attacks in CV models and privacy in federal learning.
- Learn More

  For more details, please visit my personal website:
  https://whothu.github.io/



Analyzing privacy (by MIA attack) of data augmentation and adversarial training 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.