POSTER SESSION

Gatherly Link : https://app.gather.town/invite?token=qxUbJwYD-8ZyBMYP0pqA5kZJaIJF6F6G

1. The Risk and Opportunity of Adversarial Example in Military Field
2. Towards Comprehensive Testing on the Robustness of Cooperative Multi-agent Reinforcement Learning
3. Robustness and Adaptation to Hidden Factors of Variation
4. PAT: Pseudo-Adversarial Training For Detecting Adversarial Videos
5. Adversarial Robustness through the Lens of Convolutional Filters
6. Strengthening the Transferability of Adversarial Examples Using Advanced Looking Ahead and Self-CutMix
7. AugLy: Data Augmentations for Adversarial Robustness
8. RODD: A Self-Supervised Approach for Robust Out-of-Distribution Detection
9. An Empirical study of Data-Free Quantization's Tuning Robustness
10. Exploring Robustness Connection between Artificial and Natural Adversarial Examples
11. Generalizing Adversarial Explanations with Grad-CAM
12. CorrGAN:Input Transformation Technique Against Natural Corruptions
13. Poisons that are learned faster are more effective
14. Adversarial Machine Learning Attacks Against Video Anomaly Detection Systems
15. Understanding CLIP Robustness
16. On Fragile Features and Batch Normalization in Adversarial Training
17. Sparse Visual Counterfactual Explanations in Image Space
18. Efficient and Effective Augmentation Strategy for Adversarial Training
19. Towards Data-Free Model Stealing in a Hard Label Setting
20. Transferability of ImageNet Robustness to Downstream Tasks