LAP Pre-Training Enhances Robustness to Visual Domain Shifts in Sim-to-Real Transfer

Assignee Research

June 7, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: Does the LAP pre-training recipe improve robustness to visual domain shifts in sim-to-real transfer tasks as measured by success rate degradation on the CALVIN benchmark. 15 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Using Pre-Training Can Improve Model Robustness and Uncertainty. Research question: Does the LAP pre-training recipe improve robustness to visual domain shifts in sim-to-real transfer tasks as measured by success rate degradation on the CALVIN benchmark?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.7/10.

3 Results

10 papers retrieved. 15 claims extracted; 0 independently verified. Quality review score: 3.7/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Adversarially trained high-capacity networks exhibit greater adversarial robustness.	×	0.04
Nearly all adversarial defenses fail, and even some adversarial training methods can fail too.	×	0.05
CIFAR-10 Wide ResNets are made so wide that their adversarial train accuracies are 100% but their adversarial test accur	×	0.03
Adversarial pre-training, where representations transfer across data distributions robustly, can reduce the generalizati	×	0.06
Choosing to use targeted adversaries or no adversaries during pre-training does not provide substantial robustness.	×	0.05
Adversarially pre-training a Downsampled ImageNet model against an untargeted adversary improves adversarial robustness.	×	0.10
An adversarially pre-trained network can surpass the long-standing state-of-the-art model by a significant margin.	×	0.09
By pre-training a Downsampled ImageNet classifier against an untargeted adversary, then adversarially fine-tuning on CIF	×	0.07
Pre-trained models have comparable clean accuracy to adversarially trained models from scratch, but pre-training can mar	×	0.11
Normal Training on CIFAR-10 achieves 96.0% clean accuracy and 0.0% adversarial accuracy.	×	0.03
Normal Training on CIFAR-100 achieves 81.0% clean accuracy and 0.0% adversarial accuracy.	×	0.02
Adversarial Training on CIFAR-10 achieves 87.3% clean accuracy and 45.8% adversarial accuracy.	×	0.04
Adversarial Training on CIFAR-100 achieves 59.1% clean accuracy and 24.3% adversarial accuracy.	×	0.02
Adversarial Pre-Training and Tuning on CIFAR-10 achieves 87.1% clean accuracy and 57.4% adversarial accuracy.	×	0.07
Adversarial Pre-Training and Tuning on CIFAR-100 achieves 59.2% clean accuracy and 33.5% adversarial accuracy.	×	0.06

References

- http://arxiv.org/abs/2508.11117v1
- http://arxiv.org/abs/1901.09960v5
- http://arxiv.org/abs/2306.02623v1