

Adversarial Perturbation Alignment and Model Robustness Across CIFAR-10 and MNIST

Assignee Research

June 9, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: How does the alignment of adversarial perturbations across domains affect the robustness of discriminative models compared to generative models, as measured by accuracy on the CIFAR-10 and MNIST. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Cross-Domain Transferability of Adversarial Perturbations. Research question: How does the alignment of adversarial perturbations across domains affect the robustness of discriminative models compared to generative models, as measured by accuracy on the CIFAR-10 and MNIST benchmarks?.

2 Methodology

Systematic literature search across multiple databases yielded 12 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.2/10.

3 Results

12 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 7.2/10.

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.

References

- <http://arxiv.org/abs/1905.11736v5>
- <http://arxiv.org/abs/2311.18495v2>
- <http://arxiv.org/abs/2310.04414v3>