Multimodal vs. Text-Only Code Generation Models in Adversarial Robustness Benchmarks

Assignee Research

June 9, 2026

Abstract

This report synthesises findings from 15 peer-reviewed papers addressing the following research question: How do multimodal code generation models perform on adversarial robustness metrics compared to text-only models like Code Llama when tested on perturbed MBPP samples. 15 claims were extracted from source literature; 1 was independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.5/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Multimodal Adversarial Defense for Vision-Language Models by Leveraging One-To-Many Relationships. Research question: How do multimodal code generation models perform on adversarial robustness metrics compared to text-only models like Code Llama when tested on perturbed MBPP samples?.

2 Methodology

Systematic literature search across multiple databases yielded 15 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 4.5/10.

3 Results

15 papers retrieved. 15 claims extracted; 1 independently verified. Quality review score: 4.5/10.

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
The study evaluates defense methods against the multimodal adversarial attack SGA with perturbation constraints of ϵI =	×	0.11
FARE is an unsupervised unimodal adversarial fine-tuning scheme for CLIP that focuses on obtaining a robust CLIP vision	×	0.05
TeCoA-ITR fine-tunes all parameters using a cross-modal objective to generate adversarial images, whereas the original T	×	0.04
The models CLIP-ViT-B/16, ALBEF-14M, and BLIP w/ ViT-B were fine-tuned using the proposed Multimodal Adversarial Trainin	×	0.09
Adversarial images in the training process were generated via 2-step-PGD with a perturbation size of 2/255 in l∞-norm.	×	0.04
Adversarial texts in the training process were generated using BERT-attack with a 1-token perturbation.	×	0.05
Intra-modal augmentation enhances data points without considering image-text interactions (text $\rightarrow$ text, image $\rightarrow$ image).	×	0.08
Cross-modal augmentation enhances data points by leveraging the other modality (image $\leftrightarrow$ text).	×	0.09
EDA is used as an intra-modal text augmentation technique for basic word-level edits.	×	0.02
MAT consistently achieves significantly greater robustness against multimodal attacks than the unimodal AT methods FARE	×	0.07
MAT consistently achieves significantly greater robustness against multimodal attacks than unimodal AT methods on ALBEF	×	0.08
Unimodal attacks perturb a single modality to mislead models, while multimodal attacks perturb both image and text modal	×	0.13
Multimodal attacks are significantly more effective than unimodal attacks.	×	0.11
Existing defense strategies for Vision-Language models mainly focus on vision robustness where adversarial attacks pertu	✓	0.25
The proposed method leverages one-to-many (1:N) image-text relationships via4augmentations to enhance robustness.	×	0.11

References

- http://arxiv.org/abs/2405.18770v6
- http://arxiv.org/abs/2212.10264v1
- http://arxiv.org/abs/2511.18488v2