Leveraging Synthesized N:1 Text-to-Image Relationships for Enhanced CLIP Alignment Stability Against Adversarial Perturbations

Assignee Research

June 11, 2026

Abstract

This comprehensive review delves into the pivotal role of prompt engineering in unleashing the capabilities of Large Language Models (LLMs). The development of Artificial Intelligence (AI), from its inception in the 1950s to the emergence of advanced neural networks and deep learning architectures, has made a breakthrough in LLMs, with models such as GPT-4o and Claude-3, and in Vision-Language Models (VLMs), with models such as CLIP and ALIGN. Prompt engineering is the process of structuring inputs, which has emerged as a crucial technique to maximize the utility and accuracy of these models.

1 Introduction

This paper examines: Unleashing the potential of prompt engineering for large language models. Research question: Does leveraging synthesized N:1 text-to-image relationships in contrastive learning improve the alignment stability of CLIP models against adversarial text perturbations?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.0/10.

3 Results

11 papers retrieved. 8 claims extracted; 8 independently verified. Quality review score: 7.0/10.

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 development of Artificial Intelligence (AI) has made a breakthrough in Large Language Models (LLMs), with models suc	✓	0.35
Prompt engineering is the process of structuring inputs, which has emerged as a crucial technique to maximize the utilit	✓	0.31
Techniques such as self-consistency, chain-of-thought, and generated knowledge significantly enhance model performance.	✓	0.28
Innovative approaches such as Context Optimization (CoOp), Conditional Context Optimization (CoCoOp), and Multimodal Pro	✓	0.34
Adversarial attacks exploit vulnerabilities in prompt engineering, posing risks to AI security.	✓	0.22
Strategies to mitigate risks and enhance model robustness are thoroughly reviewed in the paper.	✓	0.24
The evaluation of prompt methods is addressed through both subjective and objective metrics.	✓	0.23
Prompt engineering plays an essential role in advancing AI capabilities.	✓	0.22

References

- https://doi.org/10.1609/aaai.v38i5.28226
- https://doi.org/10.48550/arxiv.1801.00553
- https://doi.org/10.48550/arxiv.2310.14735