LOGO

The Markdown

May 2nd, 2023

Placeholder text until AI introduction writer is implemented.

Recent Research Papers

Attack-SAM: Towards Evaluating Adversarial Robustness of Segment Anything Model

2023-05-01 15:08:17+00:00

['Chenshuang Zhang', 'Chaoning Zhang', 'Taegoo Kang', 'Donghun Kim', 'Sung-Ho Bae', 'In So Kweon']

In recent years, the Segment Anything Model (SAM) has been gaining popularity in the field of computer vision due to its exceptional performance in various downstream tasks. However, like most machine learning models, SAM is vulnerable to adversarial attacks, where imperceptible perturbations can cause the model to make incorrect predictions. This vulnerability raises concerns when using deep learning models for security-sensitive applications. To address this issue, a research team conducted a study called Attack-SAM, aimed at evaluating the adversarial robustness of the SAM model. As far as the team knows, their work is the first to assess how to attack SAM with adversarial examples comprehensively. The study found that SAM is susceptible to white-box attacks, where the attacker has complete knowledge of the model's architecture and parameters. However, the model maintains robustness to some degree in the black-box setting, where the attacker lacks such knowledge. The results of this ongoing project are available through their Github repository: https://github.com/chenshuang-zhang/attack-sam. The findings of this study could contribute to the design and evaluation of more robust computer vision models for security-sensitive applications. As the field of computer vision moves towards foundation models, like in natural language processing, ensuring their robustness against adversarial attacks is critical.

Read more

Patent Mining by Extracting Functional Analysis Information Modelled As Graph Structure: A Patent Knowledge-base

Top Github Repos

1- mlc-llm

2- jsonformer

3- Multimodal-GPT

4- ChatGPT-Prompt-Engineering-for-Developers-in-Chinese

5- bestV8_release

6- FigmaChain

7- datacomp

8- diffusion

9- NakedAttention

10- langchain-cohere-qdrant-doc-retrieval

Top News

1. How ChatGPT and Other LLMs Work—and Where They Could Go Next

Read more

2. NSA Cybersecurity Director Says ‘Buckle Up’ for Generative AI

Read more

3. Tesla’s Magnet Mystery Shows Elon Musk Is Willing to Compromise

Read more

4. How to Hide Your Chats from ChatGPT's Algorithm

Read more

5. Senator Takes the First Step Towards Federal AI Regulation

Read more

6. We Need a Consumer-First Approach to A.I.

Read more

Placeholder text until AI conclusion writer is implemented.