Logo

AI Newsletter May 2nd, 2023

Paragraph 1 Lorem ipsum dolor sit amet, consectetur adipiscing elit. In tempus adipiscing felis, sit amet blandit ipsum volutpat sed. Morbi porttitor, eget accumsan dictum, nisi libero ultricies ipsum, in posuere mauris neque at erat.

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 the world of deep learning and computer vision, the Segment Anything Model (SAM) has been making waves due to its impressive performance on various downstream tasks. However, with the rise of adversarial attacks, it's important to evaluate the robustness of these models. That's where Attack-SAM comes in. In a recent research paper, the authors introduce Attack-SAM, a method for evaluating the adversarial robustness of SAM. Adversarial attacks are essentially when a model is fooled into making the wrong prediction with imperceptible perturbations. This is a serious concern, particularly in security-sensitive applications. As SAM is a foundation model for computer vision, it's important to know how vulnerable it is to adversarial attacks. The authors found that SAM is indeed vulnerable to white-box attacks, where the adversary has access to the model and its parameters. However, SAM maintains robustness to some extent in the black-box setting, where the adversary has limited or no access to the model. This is valuable information for those using SAM in real-world applications. The authors note that this is an ongoing project, and more results and findings will be continually updated on their GitHub page. As deep learning models become more prevalent in various applications, it's crucial to understand their vulnerabilities to adversarial attacks. The work done in the Attack-SAM project helps shed light on SAM's robustness and sets the foundation for future research on the topic.

Read more

Patent Mining by Extracting Functional Analysis Information Modelled As Graph

Top Github Repos

1- mlc-llm

2- Multimodal-GPT

3- jsonformer

4- bestV8_release

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

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

Paragraph 4 Duis sit amet accumsan nibh, varius tincidunt lectus. Quisque commodo, nulla ac feugiat cursus, arcu orci condimentum tellus, vel placerat libero sapien et libero. Suspendisse auctor vel orci nec finibus.

f t