Logo

AI Newsletter

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']

The Segment Anything Model (SAM) is becoming increasingly popular in the field of computer vision due to its remarkable success across various tasks. However, there is a critical concern- its vulnerability to adversarial attacks. Such attacks can manipulate a model to predict wrongly without being noticed by human beings. This vulnerability can be problematic while using deep models in security-sensitive applications. A research team is exploring this concern and has attempted to identify the adversarial robustness of SAM in an in-depth study. According to the findings, SAM can be easily fooled by white-box attacks while demonstrating resilience to some extent under the black-box setting. This study is the first of its kind to indicate comprehensively the type of adversarial attacks that can subvert the SAM model. While the research is ongoing, more results and findings are anticipated. You can stay up-to-date on the latest developments by visiting the following website: https://github.com/chenshuang-zhang/attack-sam. The results from this study will be useful in further research regarding adversarial attacks and their impact on foundation models.

Read more

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

2023-04-29 17:34:11+00:00

['Manal E. Helal']

Patent mining is an effective technique for extracting

Top Github Repos

1- mlc-llm

2- Multimodal-GPT

3- bestV8_release

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

5- FigmaChain

6- datacomp

7- diffusion

8- NakedAttention

9- langchain-cohere-qdrant-doc-retrieval

10- PandaLM

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