

SIT799 Human Aligned Artificial Intelligence

Distinction Task 4.2: Adversarial Attacks on Computer Vision

Overview

During week 4, you have been introduced to: Adversarial attacks against AI; Real-world examples of adversarial attacks on AI; Some solutions to fight against adversarial attacks on AI. To better understand Adversarial attacks against AI, in this assignment, we will look at a Computer Vision use case.

To complete this assignment, you need to refer back to Week 4 lecture material.

Submission Details

Convert the Jupyter Notebook to a **PDF** and submit that document. Also, include a URL link to a GitHub repo containing the Notebook file and make sure you complete all the tasks.

You may have to install *pandoc* to convert a Jupyter Notebook to a PDF document:

<http://pandoc.org/installing.html>

Instructions

Download the Jupyter Notebook from the task resources and complete all the tasks.