h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

– Master-/Bachelor Thesis –

Large Language Models for Digital and Physical Attack Detection

da/sec

da/sec is the biometrics and security research group and is affiliated with University of Applied Sciences Darmstadt and the National Research Center for Applied Cybersecurity (ATHENE). The group is led by Prof. Dr. Christoph Busch. The focus of the group is on highly innovative and applied IT security research in the special fields of biometrics. Read more on www.dasec.h-da.de.

Motivation & Goal

Large language models (LLMs) are a category of foundation models trained on huge amounts of data that make them capable of understanding and generating natural language and other types of content to perform a wide range of tasks. LLMs can be also used for image classification. The goal of this project is to explore LLMs for detecting digital (e.g., morphing) and physical (e.g., attack presentations) attacks.

Tasks

- Explore the capability of LLMs for attack detection.
- Implement finetune strategies for LLMs to avoid the training from scratch.

We offer

- Incentives for the student to work on this project (work within scientific context, international collaboration, work on project in collaboration with companies)

Requirements

- High motivation and creativity
- Programming skills
- Good analytical skills
- Interest in biometric recognition

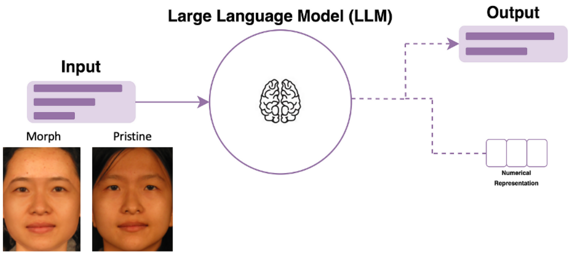
By Date

By now / by appointment

Contact

Dr. Lazaro Janier Gonzalez-Soler
Lazaro-janier.gonzalez-soler@h-da.de

h_da
Faculty of
Computer Science
ATHENE – National Research Center for Applied Cybersecurity
da/sec – Biometrics and Security Research Group
Schöfferstraße 8b
64295 Darmstadt


Large Language Model (LLM)
Output
Input
Morph
Pristine
Numerical
Representation