h_da hochschule darmstadt
fachbereich informatik

member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

ATHENE
National Research Center
for Applied Cybersecurity

– Master-/Bachelor Thesis –

Hallucination Prevention on Explainable Biometric Systems

da/sec

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

Motivation & Goal

Explainable biometric systems are necessary to improve trust in users and to comply with incoming government regulations regarding High-Risk AI systems. LLMs have become a common resource to provide explanations regarding biometric identification decisions. However, LLMs tend to provide confident yet incorrect answers (aka hallucinations) that can harm users by giving false information to reviewers. This project aims to find and implement solutions that flag hallucinations coming from explainable face reconition systems to improve the quality of LLM responses.

Tasks

- Implement a face recognition explainable system
- Implement a "reviewer" that checks for hallucination prevention and flag wrong answers.
- Evaluate the improvement achieved by the "reviewer".

We offer

- Work on solving current scientific problems.
- International colleagues and collaboration.

Requirements

- High motivation and creativity.
- Familiarity with computer vision algorithms.
- Self organized and good communication.

By Date

By now / by appointment

Contact

Ana Real
ana.estrada-real@h-da.de

h_da
PhD Candidate
Computer Science

da/sec
BIOMETRICS & SECURITY
RESEARCH GROUP

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