h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

ATHENE
National Research Center
for Applied Cybersecurity

– Master Thesis –

Investigating Embedding Reconstruction in FHE-based Biometric Template Protection Systems

da/sec

da/sec is the biometrics and Internet 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 and Prof. Dr. Christian Rathgeb. 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

Biometric reference data contains discriminative and sensible information and therefore must be protected. Fully Homomorphic Encryption (FHE) has emerged as a valuable tool to secure such sensitive data. However, despite operating on encrypted data, score leakage may enable attackers to accurately recover protected templates. This work aims to assess the practical feasibility of such attacks and to develop and evaluate countermeasures.

Tasks

- Design and implement a basic FHE-based BTP scheme, including a complete feature extraction pipeline, subject enrolment, and verification
- Conduct template recovery/inversion attacks: (1) with a known identity (non-reference photo), and (2) using a blind/black box approach with randomized embeddings and reconstruct decision boundaries
- Propose and implement countermeasures against template inversion attacks
- Evaluate and analyze the efficacy of these countermeasures, discussing practical feasibility and security implications

Requirements

- High motivation
- Strong programming skills

By Date

By now / by appointment

Contact

Florian Bayer
florian.bayer@h-da.de

h_da
Faculty of
Computer Science

ATHENE–National Research Center for Applied Cybersecurity
da/sec – biometrics and internet security research group
Schöfferstraße 8b
64295 Darmstadt