Privacy-preserving Workload Reduction of Biometric Systems

ESR1 Daile Osorio-Roig

da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt

2023-09-13

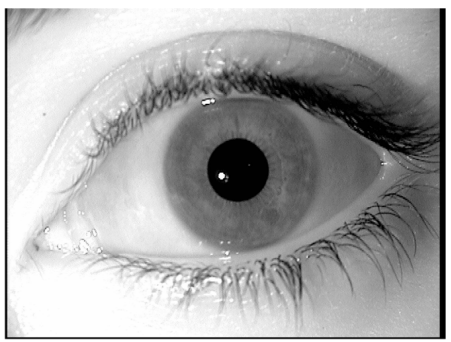
Introduction

Biometric Operation Mode: Identification

- There is **no biometric claim**.
- The decision has to be reached using **the biometric data alone**.
- Computationally **expensive** (in worst scenario, exhaustive search).

Problems and Motivation

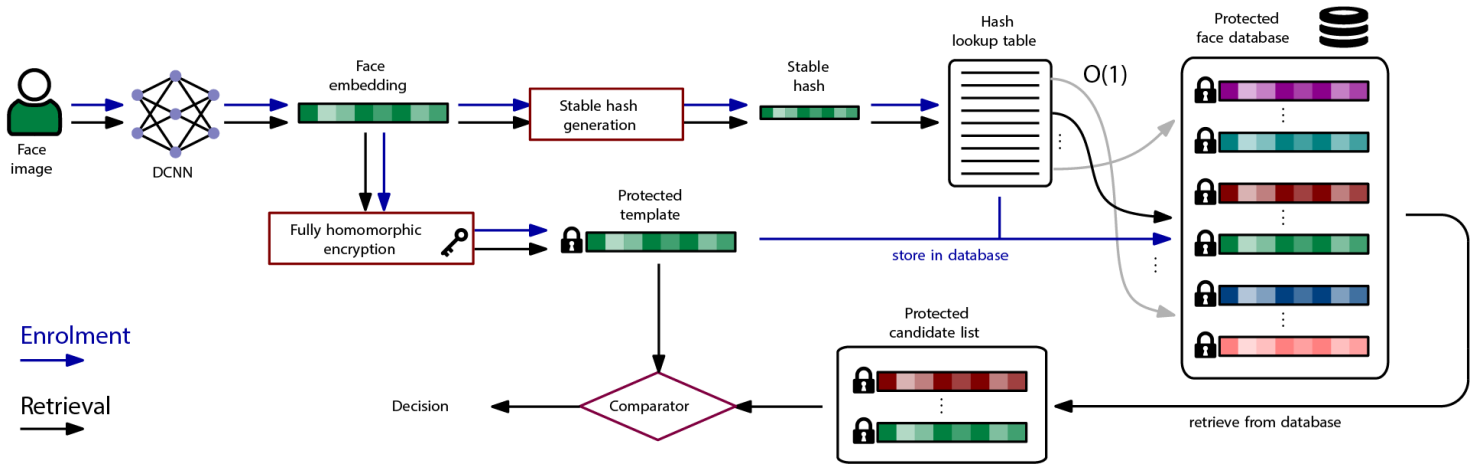
- Exhaustive **searches** together with the **protection** scheme.
- Biometric deployments require **interoperability** and **usability** by including efficient **multi-modal** solutions.
- **Vulnerabilities** on the privacy protection schemes.
  1. Unauthorised subjects breaking into biometric systems.
  2. Breach of protected privacy information.


Stable Search

Privacy-preserving face identification system for indexing and retrieval of protected face templates.

1. Application to Homomorphic encryption.
2. Stable search in the encrypted domain.
3. Not to the exhaustive searches: search in O(1) with a look-up hash table.
4. Generation of stable face hashes (non-fuzzy comparison).
5. Workload reduction down to 0.1% of a baseline approach (i.e. an exhaustive search).

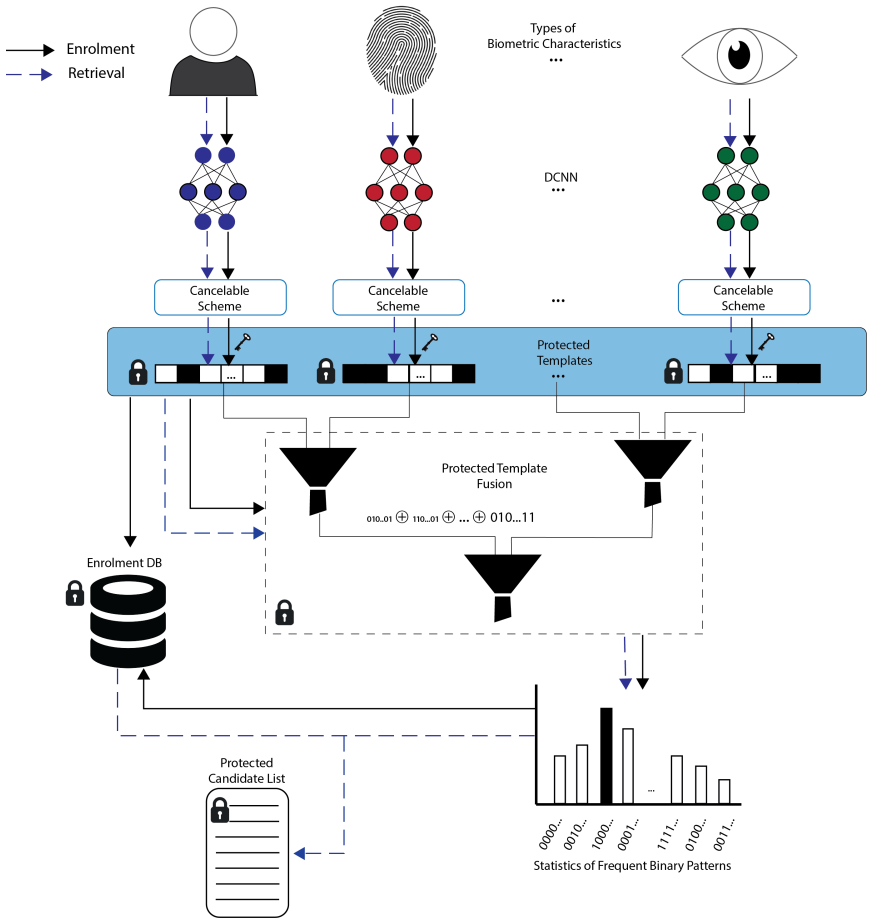


Indexing encrypted templates through a look-up hash table.

Multi-biometric Indexing

Concept of Frequent Binary Patterns

- Application to Cancelable schemes.
- Solution agnostic with respect to biometric modality and protection scheme.
- Application to Face, Iris, and Fingerprint.
- Working on the most secure level of the biometric system: feature level.

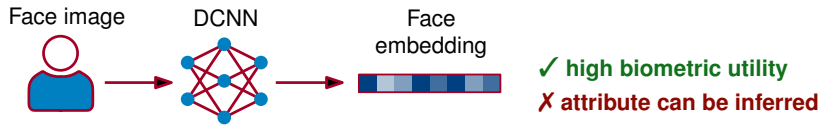


Privacy-preserving multi-biometric indexing scheme.

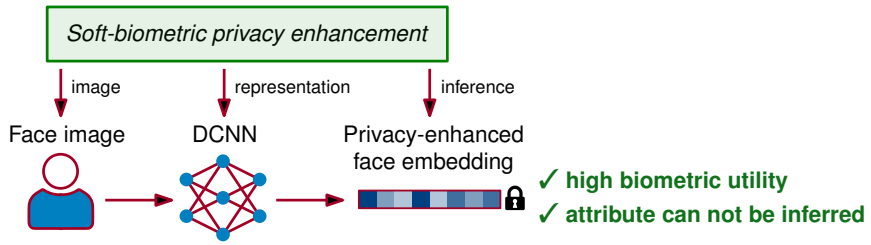
Privacy Protection

Vulnerabilities and Strengths on Privacy Protection Schemes.

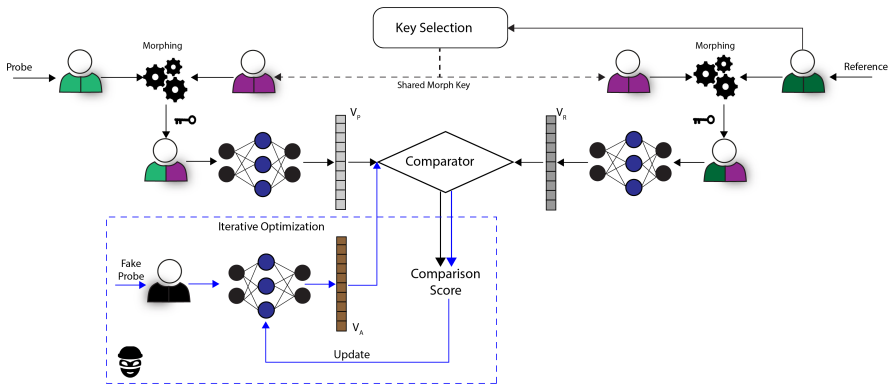
- Novel attacks on protected information: e.g. demographic information.
- Need of novel protocols and evaluations to consider the highest security and privacy.
- Chance of the false match increased.
- Attacks led to novel insights against adversarial attacks.



(a)Unprotected domain



(b)Protected domain



Scheme against adversarial attacks

Final Remarks

Take-away message

- We need to make efficient multi-biometric deployments while maintaining the highest privacy, security, and biometric performance.
- There is a need for indexing solutions that work by a trade-off between privacy and efficiency.
- It has been argued that a more rigorous analysis is necessary to measure the actual privacy enhancement provided by privacy-enhancing technologies.

Achievments

- 11 peer-reviewed publications.
- Multidisciplinary research through collaborations with lawyers and academic institutions.
- Skills in teaching at one university and supervision of 1 BSc and 2 MSc theses.

Thank you for listening!

This work is supported by the TReSPAsS-ETN project funded from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860813.