da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

ATHENE
National Research Center
for Applied Cybersecurity

Privacy-preserving Workload Reduction of Biometric Systems

Dailé Osorio-Roig

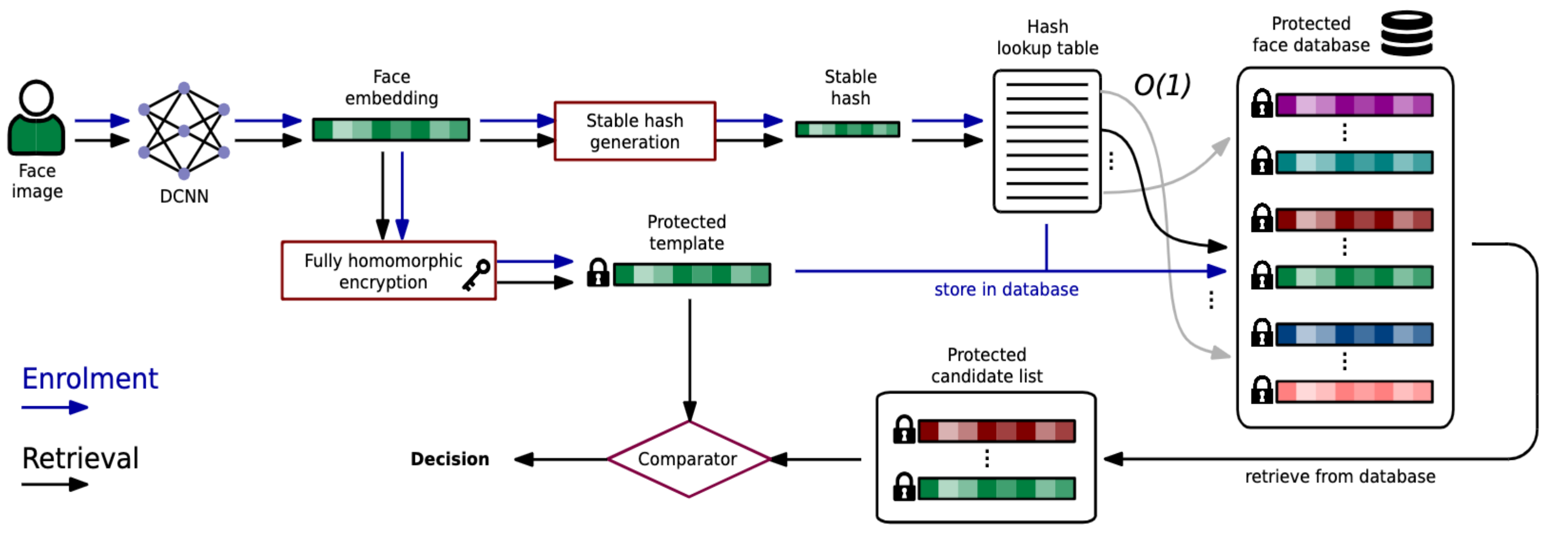
Darmstadt University of Applied Sciences

Introduction

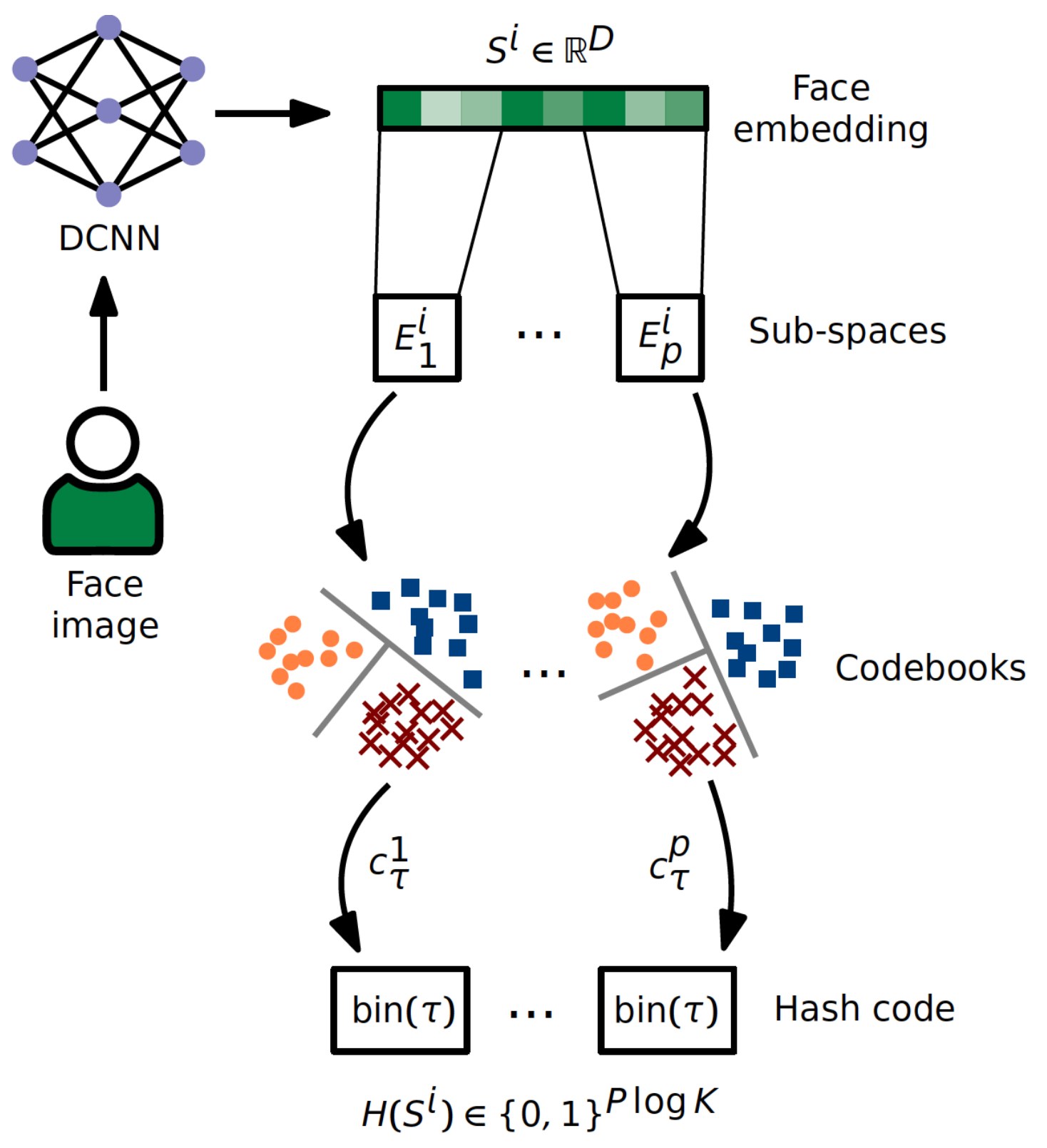
- **Identification scenario**: The "process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual" (1:many).
- Time-consuming tasks dominated by the number of comparisons.
- Biometric technologies demand interoperability and deployment assuring maximum usability by including multi-modal biometric solutions.
- Biometric template protection schemes (BTPs) appear to be unsuitable for indexing in biometric identification systems.
- Need of BTP- and modality-agnostic indexing schemes.

- **Security and data privacy**
- Findings on new vulnerabilities in facial soft-biometric privacy enhancement.
- Privacy-preserving indexing schemes are designed to offer an end-to-end protection (i.e. from the template to the indexing scheme).

Selected Results



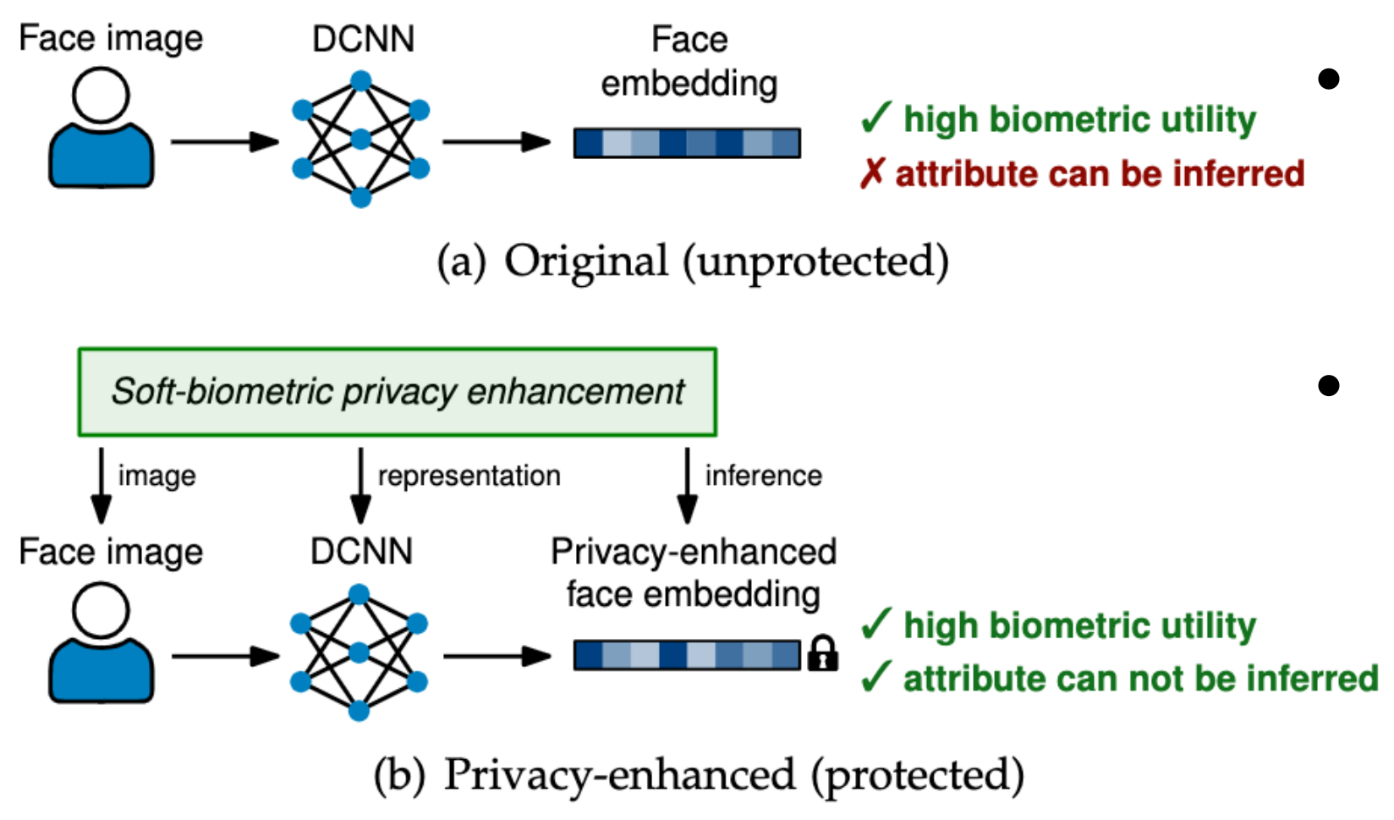
Identification system with Stable Hashes and Fully Homomorphic Encryption



Hash Generation Scheme

- Privacy-preserving face identification system for indexing and retrieval of protected face templates [1].
- Application of *Fully Homomorphic Encryption* in identification scenarios.
- *Not* to the exhaustive searches: search in O(1), *Not* to the dimensionality reduction.
- *Stable face hashes* through the Product Quantisation-based and clustering-based look-up table are analysed.
- Application of *conventional cryptographic methods* is feasible since the system enables an *exact match* (*non-fuzzy* comparison) of hash codes.
- *Workload reduction* down to 0.1% of a baseline approach (i.e. exhaustive search).

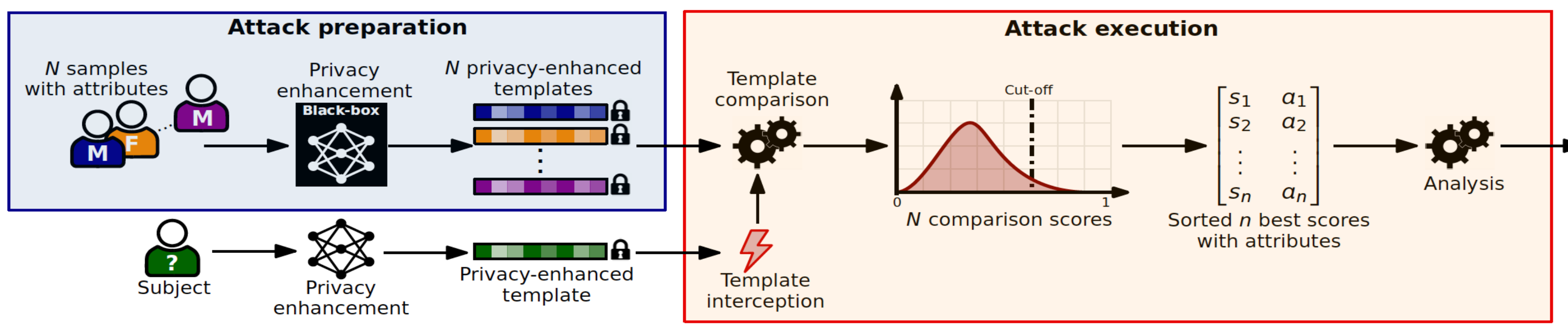
- An attack on Facial Soft-biometric Privacy Enhancement is shown in [2].


Face image
DCNN
Face embedding
✓ high biometric utility
✗ attribute can be inferred
Soft-biometric privacy enhancement
image
representation
inference
Face image
DCNN
Privacy-enhanced face embedding
✓ high biometric utility
✓ attribute can not be inferred

(a) Original (unprotected)

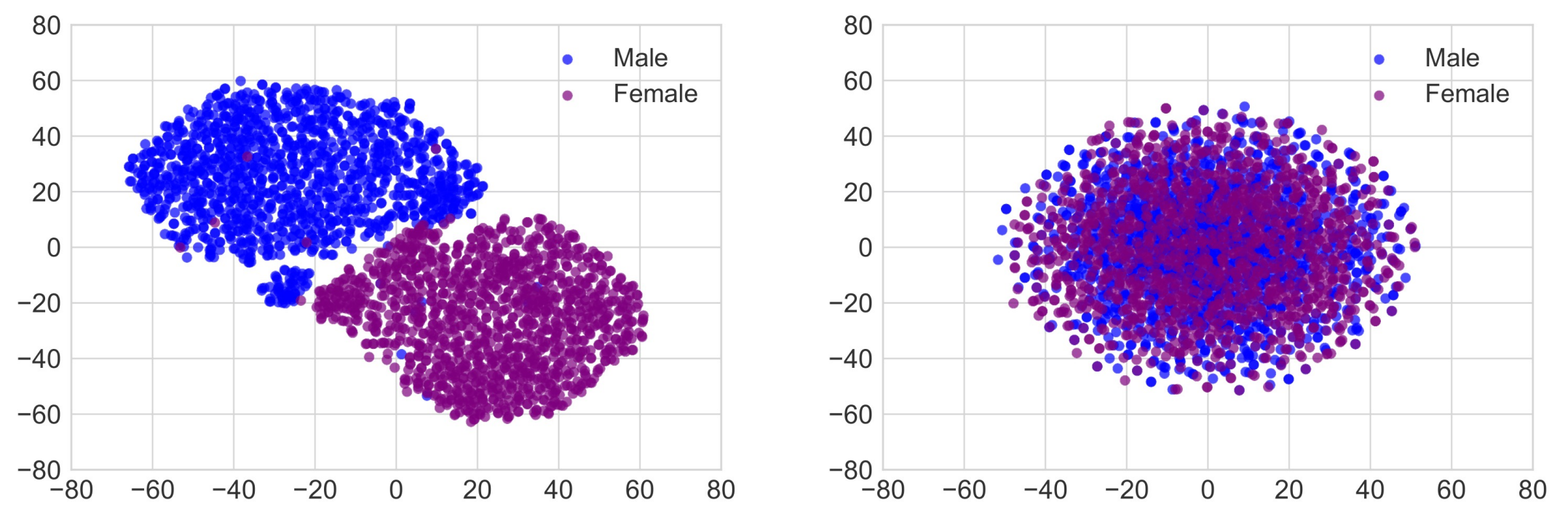
(b) Privacy-enhanced (protected)

- Exploiting the effect of broad homogeinity and demographic differential in face recognition.
- Analysis of the false match chances leading to the execution/design of these attacks.



Overview of the attack

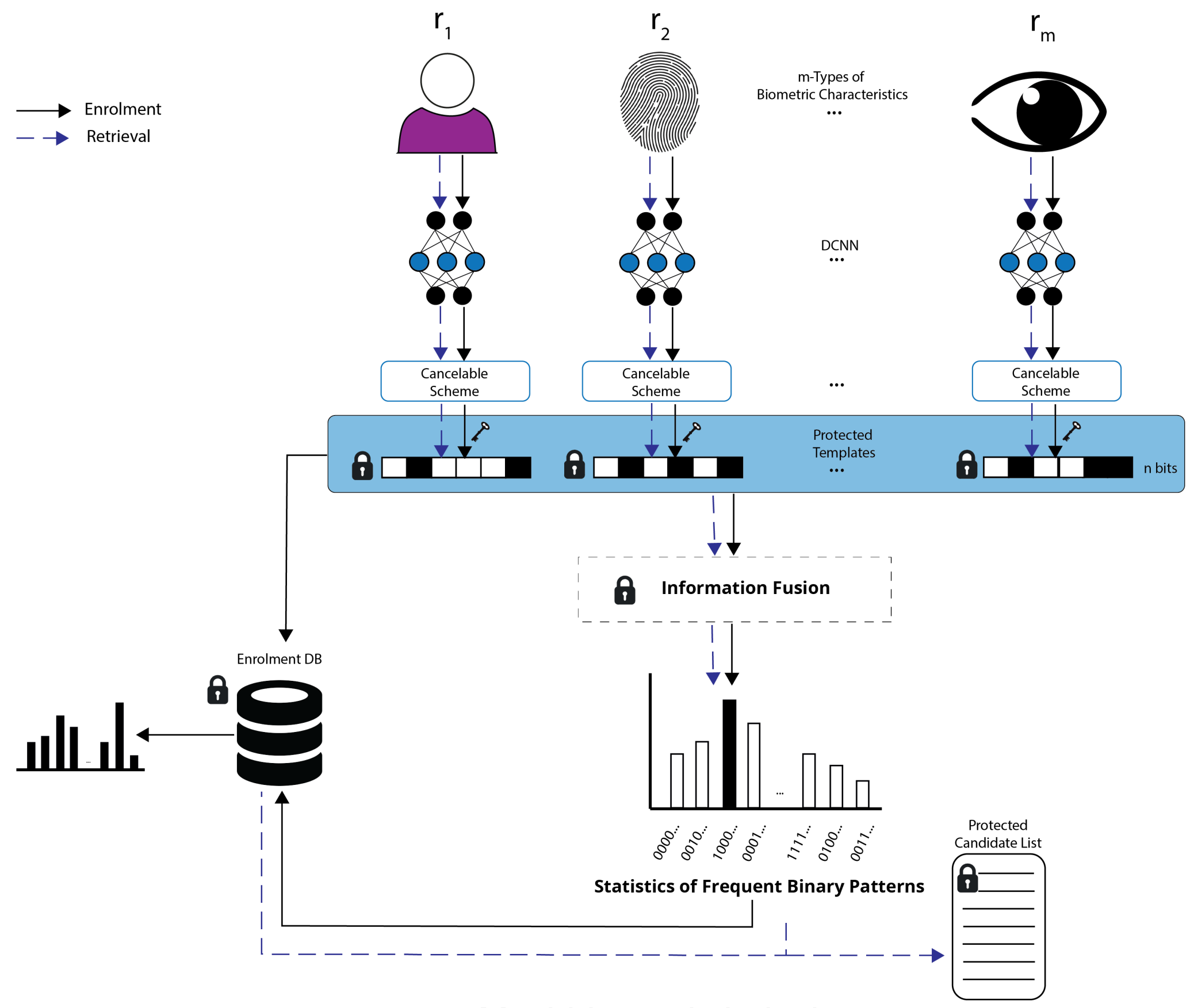
- Unknown attribute is inferred from the attributes associated with the highest obtained similarity scores.
- Classification on gender with an accuracy of up to approximately 90%.
- Rigorous analysis is necessary to measure the actual privacy enhancement provided by such techniques.



Unprotected space

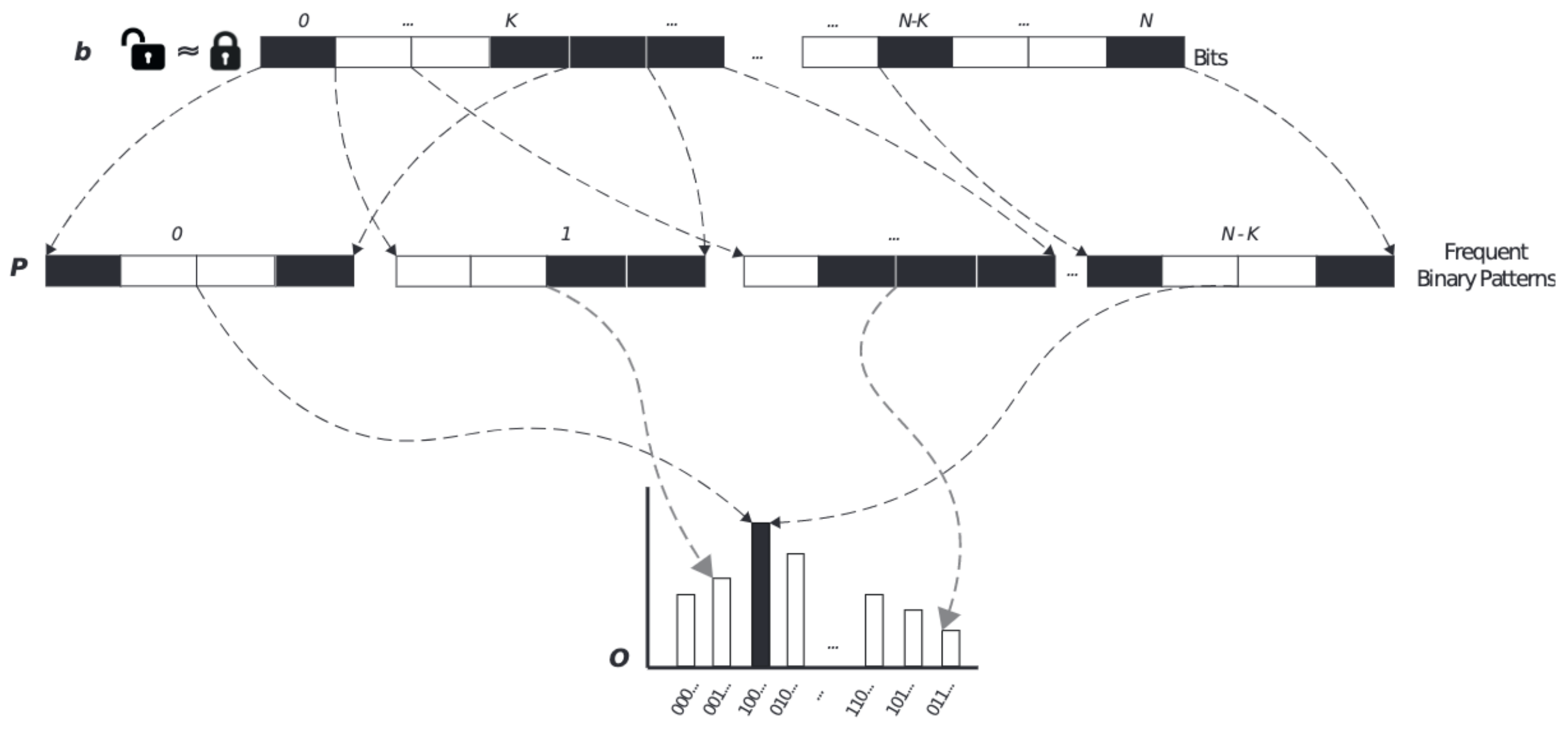
Protected space

- Protection capabilities are tested using machine learning-based classifiers and dimensionality reduction tools.
- They are not enough!



Multi-biometric indexing

- Cancelable schemes with base of binary representation: BioHashing and IoM-GRP.
- State-of-the-art DNN-based embedding extractors with 512-floating values.
- Evaluation on the three most commonly used biometric modalities (Face, Iris, and Fingerprint).



Frequent binary pattern extraction

- Cancelable biometric template protection scheme- and modality-agnostic indexing scheme.
- Successful application of the proof-of-concept of frequent binary patterns on individual biometric characteristics.
- Fusion strategies on the concept of frequent binary patterns at two steps: the representation- and feature-based step.
- Computational workload reduction is reduced to approximately 57% (indexing up to 3 modalities) and 51% (indexing up to 2 modalities).
- Improvement of the biometric performance at the high-security thresholds of a baseline biometric system.

Own Publications

[1] Dailé Osorio-Roig, Christian Rathgeb, Pawel Drozdowski, Christoph Busch, “Stable Hash Generation for Efficient Prvacy-Preserving Face Identification”, in Transactions on Biometrics, Behavior, and identity Science (TBIOM), July 2021.

[2] Osorio-Roig D, Rathgeb C, Drozdowski P, Terhörst P, Štruc V, Busch C. An Attack on Facial Soft-biometric Privacy Enhancement. IEEE Transactions on Biometrics, Behavior, and Identity Science. 2022 May 9.

[3] D.Osorio-Roig, T.Schlett, C.Rathgeb, J.Tapia, C.Busch “Exploring Quality Scores for Workload Reduction in Biometric Identification”, International Workshop on Biometrics and Forensics (IWBF), Salzburg, Austria,2022.

[4] D. Osorio-Roig, C. Rathgeb, H. Otroshi-Shahreza, C. Busch, S. Marcel, Indexing Protected Deep Face Templates by Frequent Binary Patterns, in International Joint Conference on Biometrics (IJCB), 2022.

[5] D. Osorio-Roig, T. Rohwedder, C. Rathgeb, C. Busch, Analysis of Minutiae Quality for Improved Workload Reduction in Fingerprint Identification, in Proc Intl. Conf. of the Biometrics Special Interest Group (BIOSIG), 2022.

[6]Tim Rohwedder and Daile Osorio-Roig and Christian Rathgeb and Christoph Busch, “Benchmarking fixed-length Fingerprint Representations across different Embedding Sizes and Sensor Types”, in Proc Intl. Conf. of the Biometrics Special Interest Group (BIOSIG), 2023.

[7] Reversing Deep Face Embeddings with Probable Privacy Protection (under revision).

[8] Optimizing Key-Selection for Face-based One-Time Biometrics via Morphing (under revision).

[9] Privacy-preserving Multi-biometric Indexing based on Frequent Binary Patterns (under revision).

EAB - Protecting Your Data in Biometric Systems

Participate in the survey “*Protecting your data in biometric systems*”

Acknowledgment: This work has in part received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 860813 - TReSPAsS-ETN and the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE..

TReSPAsS-ETN