Privacy Preserving Workload Reduction in Biometric Systems

Dailé Osorio-Roig

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

2024-07-08

Agenda

Introduction

Thesis Scope

Biometric Workload Reduction

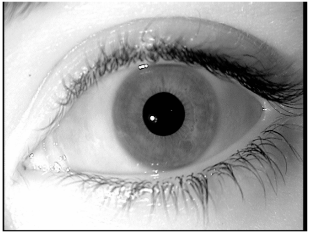
Privacy Protection Analysis

Summary

Biometric recognition

*"Automated recognition of individuals based on their **behavioural** and **biological** characteristics"*

Face



Iris

Fingerprint

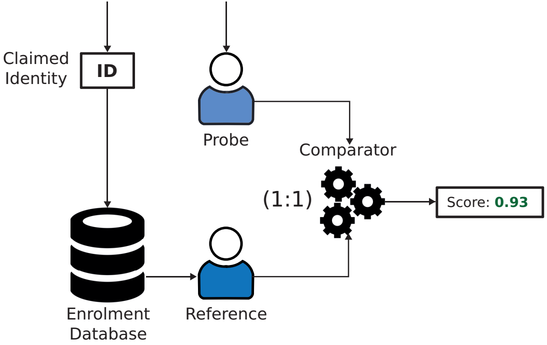
ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37:2022 Information Technology – Vocabulary - Part 37: Biometrics, International Organization for Standardization, 2022

Introduction

Biometric operation modes

- A biometric claim to an identity is made.
- A **1:1 comparison** is performed in order to reach a decision.
- Computational complexity is limited to a **one-to-one comparison**.

⇒ **Computationally** trivial process!



Verification

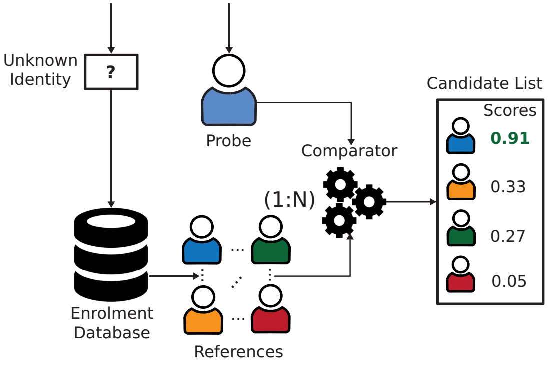
ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37:2022 Information Technology – Vocabulary - Part 37: Biometrics, International Organization for Standardization, 2022

Introduction

Biometric operation modes

- There is no biometric claim.
- **1:N comparisons** are performed to reach a decision using the biometric data alone.
- Computational complexity is limited to the **1:N comparisons** (in worse case: **exhaustive search**).

⇒ **Computationally** non-trivial which leads to different **challenges**.



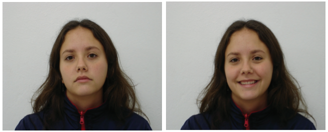
Identification

ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37:2022 Information Technology – Vocabulary - Part 37: Biometrics, International Organization for Standardization, 2022

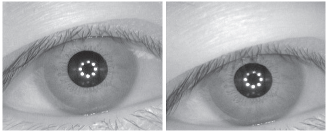
Introduction

Challenges in identification

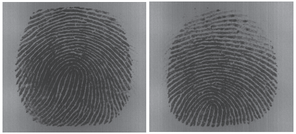
- Computational costs: the computational workload of the biometric system in terms of the number of enrolled subjects.
  ⇒ the **investment** in advanced technologies (e.g. hardware and device investment).
- False positive costs: the cost of a **false match** increases as the number of enrolled subjects increases.
- Biometric data is **fuzzy**.



Faces



Iris



Fingerprint

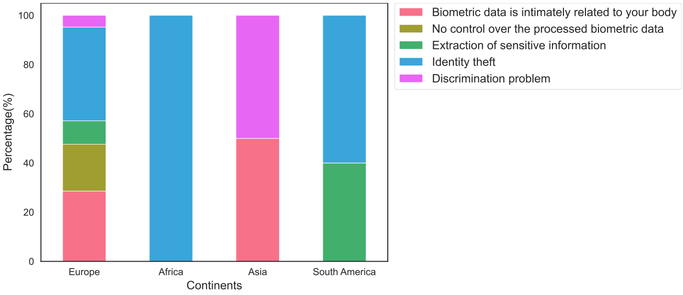
⇒ an inherent order, variance, and variations across different biometric characteristics.

⇒ **Identification** is more challenging than verification!

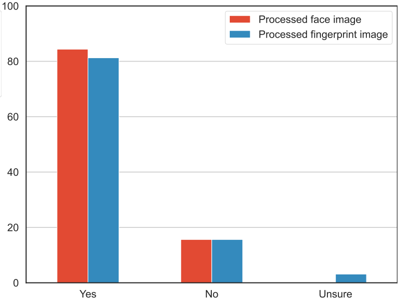
J. Daugman, "Biometric decision landscapes", Tech. rep. University of Cambridge, Computer Laboratory, 2000

Privacy protection

- Questionnaire containing the answers from 32 subjects.
- Privacy depends on human **perception** and **culture**.
- From the legal framework (GDPR), biometric data is defined as **sensitive data**.
- Need for research on **privacy-preserving biometric systems** in compliance with the GDPR.



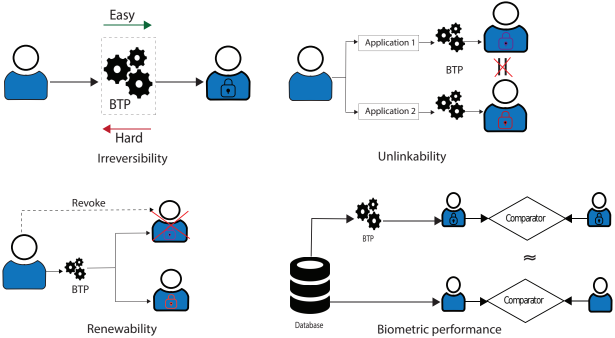
Human Perception and Culture



Level of sensitivity: Face vs Fingerprint

Biometric data protection

- Strong mechanisms for the **full protection** of the biometric reference.
- Requirements defined in ISO/IEC 24745:
  1. Irreversibility
  2. Renewability
  3. Unlinkability
  4. Biometric performance
- Biometric template protection schemes (BTP):
  1. Biometric Cryptosystems
  2. Homomorphic Encryption
  3. Cancelable Biometrics



Irreversibility

Unlinkability

Renewability

Biometric performance

⇒ **High** computational workload on exhaustive searches!

ISO/IEC 24745:2022 Information technology, cybersecurity and privacy protection – Biometric information protection. International Standard. Switzerland, Feb. 2022.

Thesis Scope

Research Questions

1. Is it possible to combine workload-reduction (WR) strategies with BTP schemes while maintaining accuracy and high privacy protection?
   - Is it possible to combine pre-selection strategies (e.g. prefiltering, binning, data structures) with BTP (e.g. cryptobiometrics, homomorphic encryption, and cancelable biometrics)?
2. Is it possible to create a multi-biometric system which combines WR strategies with BTP schemes and demands a low workload, while deploying high privacy protection for the different biometric characteristics (or fusion levels)?
   - Techniques of information fusion at the feature level.
3. How can the trade-offs between biometric performance, template protection, and workload reduction in a biometric identification system be analysed and interpreted?
   - Is it possible to theoretically/formally model the trade-offs between biometric performance, template protection, and workload reduction in a biometric identification system?
   - Is it possible to empirically evaluate these trade-offs?

Thesis Scope

Research Questions

4. Can existing privacy-enhancing technologies (PETs) be successfully employed for privacy protection?
   - Is it possible to design novel attacks that reveal new vulnerabilities of the soft-biometric privacy-enhancing face approaches?

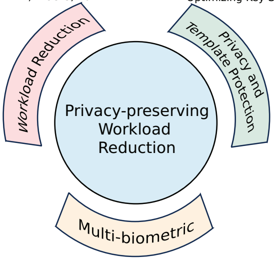
Thesis Scope

Work focus

- **Workload Reduction**: non-exhaustive and stable searches.
- **Template Protection**: combination with template protection.
- **Multi-biometric system**: improvement of the biometric performance, interoperability, usability, and combination.
- **Privacy**: novel vulnerabilities.

“Stable hash generation...”
IEEE T-BIOM, 2021.
“Benchmarking fixed-length Fingerprint...”, BIOSIG, 2023.
“Indexing Protected Deep Face Templates...”, IJCB, 2022.
“Exploring quality scores for WR...”, IWBF, 2022.
“Analysis of Minutiae Quality for WR...”, BIOSIG, 2022.

“An Attack on Facial Soft-Biometric...”
IEEE T-BIOM, 2022.
“Reversing Deep Face Embeddings...”, WIFS, 2023.
“Optimizing Key-Selection...”, WIFS, 2023.



“Privacy-preserving Multi-biometric Indexing...”
IEEE TIFS, 2024.

Biometric Workload Reduction

Biometric WR

WR Methods

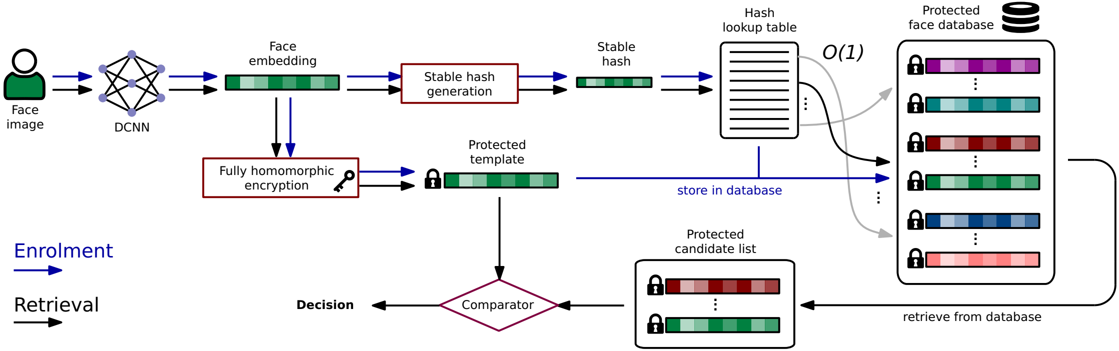
- pre-selection: focused on reducing the number of biometric template comparisons (i.e. search space) by designing e.g. binning schemes, data structures, etc.

Take-away messages

- Homomorphic encryption as BTP scheme.
- Computational complexity O(1) ⇒ non-fuzzy comparison.
- Stable search and specific machine-learning techniques ⇒ without exposing the dimensional biometric feature vector.
- Unsupervised clustering-based approaches with product quantization ⇒ compact hash codes and invalidate any practical security analysis.
- Algorithm agnostic across biometric characteristics ⇒ proof-of-the-concept: Face.

Hash Look-up Table for Indexing Hashed Faces Homomorphically

Overview



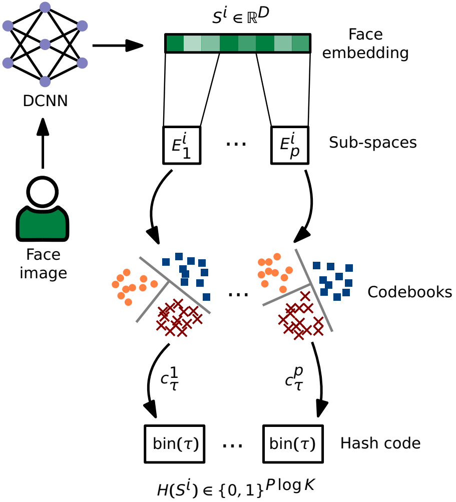
D. Osorio-Roig et al. "Stable Hash Generation for Efficient Privacy-Preserving Face Identification", in Trans. on Biometrics, Behavior, and Identity Science (TBIOM), 2021.

Biometric WR

Hash Generation Scheme

Theory and Computational Workload

- Concatenation of P sub-vectors of equal size.
- P approximated and represented by the nearest cluster.
- $W_{proposed} = N \times p \times \theta + \beta$ (hash look-up table).
- An exact match, i.e. $\beta \ll$ 1.00ms.
- Cost of a one-to-one comparison $\rightarrow \theta$.
- Total of subjects enrolled $\rightarrow N$
- Penetration rate $\rightarrow p = \frac{\gamma}{N}$.
- It is expected $W_{proposed} \ll W_{baseline}$
- $W_{baseline} \rightarrow$ 100%.

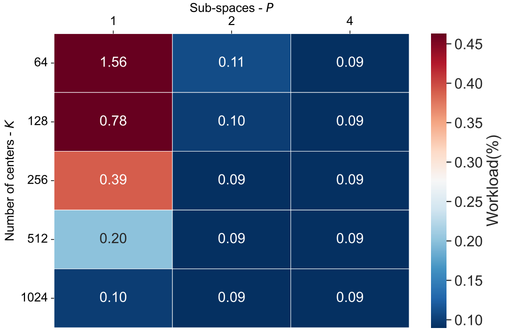


Hash Generation Scheme

Results: workload reduction

Relation between sub-spaces and the number of centres. N=1,177

K	Metrics	$P = 1$	$P = 2$	$P = 4$
64	γ	18.3906	1.3282	1.0020
	p	156×10^{-4}	11×10^{-4}	$\mathbf{9 \times 10^{-4}}$
	W	1.56%	0.11%	**0.09%**
128	γ	9.1953	1.1444	1.0007
	p	78×10^{-1}	10×10^{-4}	$\mathbf{9 \times 10^{-4}}$
	W	0.78%	0.10%	**0.09%**
256	γ	4.5977	1.0815	1.0022
	p	39×10^{-4}	$\mathbf{9 \times 10^{-1}}$	$\mathbf{9 \times 10^{-4}}$
	W	0.39%	**0.09%**	**0.09%**
512	γ	2.2988	1.0591	1.0022
	p	20×10^{-4}	$\mathbf{9 \times 10^{-1}}$	$\mathbf{9 \times 10^{-4}}$
	W	0.20%	**0.09%**	**0.09%**
1024	γ	1.1424	1.0148	1.0012
	p	10×10^{-4}	$\mathbf{9 \times 10^{-1}}$	$\mathbf{9 \times 10^{-4}}$
	W	0.10%	**0.09%**	**0.09%**



⇒ Workload depends on the number of sub-spaces

⇒ Best Workload is 0.09% for a constant N.

⇒ 0.09% → 99% with respect to baseline 100%

Hash Generation Scheme

Results: biometric performance

FPIR and FNIR (in %), Open-set scenario in LFW [1] database.

Approach	**P**	**FPIR=0.1(%)**	**FPIR=1.0(%)**
Unprotected (Exhaustive search) [2]	-	51.58	0.52
Protected (Hash look-up)	$P = 1$	36.40	**2.68**
Protected (Hash look-up)	$P = 2$	**34.99**	2.97
Protected (Hash look-up)	$P = 4$	37.63	3.76

- Robustness analysis ⇒ open-set scenarios.
- High variation of the image quality over LFW.
- Biometric performance in the protected domain is competitive with respect to the unprotected domain.
- Trade-off controlled by the number of sub-spaces.

[1] G. Huang, M. Ramesh, T. Berg, et al. “Faces in the wild: a database for studying face recognition in unconstrained environments.” In: *Technical Report* (2007), pp. 07–49, p. 1.

[2] X. Dong, S. Kim, Z. Jin, et al. “Open-set face identification with index-of-max hashing by learning.” In: *Pattern Recognition* 103 (2020), p. 107277, p. 2.

Biometric WR

Multi-biometric systems

- Combine or fuse multiple sources of information to improve the **overall discriminative power** of a single biometric recognition system.
- Combining biometric data at **different levels** of the processing pipeline:
  Sensor, **Feature**, **Score**, **Rank**, **Decision**

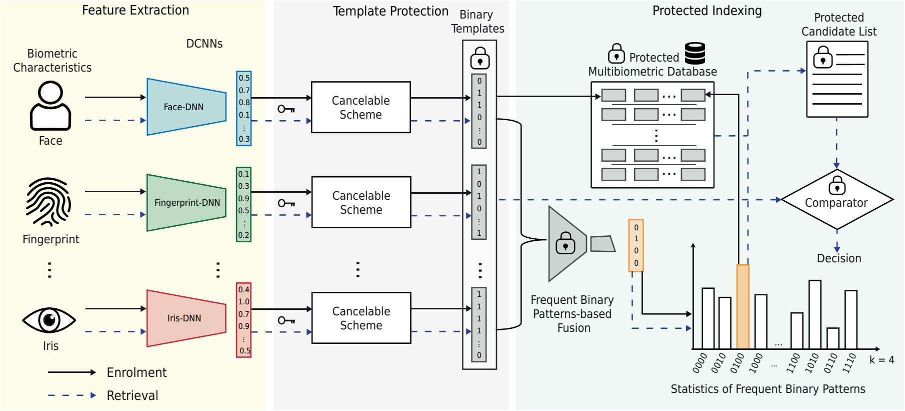
Advantages

- Fusion strategies can be **flexible** to operate at different levels of the biometric processing pipeline.
- Feature-level fusion ⇒ the highest **privacy protection and security** level of a biometric system.
- Protection of the biometric template ⇒ retained at the **feature-level fusion**.
- Application to cancelable approaches as BTP schemes.

⇒ Need for research on **common protected feature** representation!

Privacy-preserving Multi-biometric Indexing based on Frequent Binary Patterns

Overview

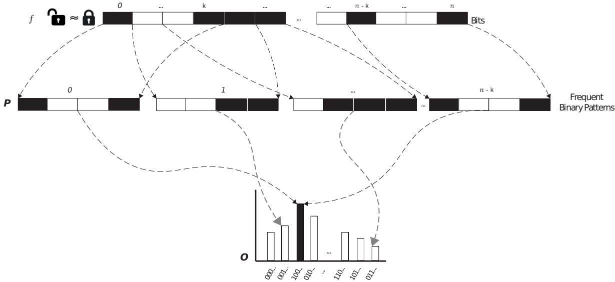


D. Osorio-Roig et al. "Privacy-preserving Multi-biometric Indexing based on Frequent Binary Patterns" submitted to IEEE Trans. on Information Forensics & Security (TIFS), 2023.

Work on Frequent Binary Patterns

Theory

- Sampling and computation of the statistics ($\mathbf{O}$) of the frequent binary patterns extracted (**FBP**).
- Fusion on the feature level taking advantage of the novel concept for retrieval and indexing.
  1. Feature-concatenation (Feature-level)
  2. Ranked-codes (Representation-level based on **FBP**)
  3. XOR-codes (Representation-level based on **FBP**)



Frequent binary pattern extraction.

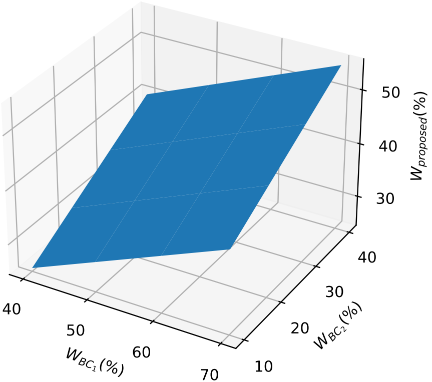
$\Rightarrow$ Data subjects are indexed with at most 2^k bins!
$\Rightarrow$ Search of a threshold $1 \leq t \leq 2^k$ for retrieval!

Work on Frequent Binary Patterns

Computational Workload

$$W_{proposed} = \sum_{i=1}^{t} |b_i| \cdot m, \qquad (1)$$

- Application to single-biometric characteristics and different types of m biometric characteristics.
- Depends on threshold t.
- $W_{proposed}$ depends on the biometric characteristics involved (BC_1 and BC_2).
- $W_{proposed}$ increases with the workloads of the types of BC_1 and BC_2.
- It is expected $W_{proposed} \ll W_{baseline}$



Relation between the $W_{proposed}$ and the BCs involved

Biometric WR

Results in terms of FNIR(%) and WR(%) for single-biometric characteristic

FNIR (%) in FPIR=0.01% and FPIR=0.1%, WR(%)

BC	Search	k	#Bins	WR(%)	FPIR=0.01(%)	FPIR=0.1(%)
Face	exhaustive	-	-	100.00	**33.91**	**21.42**
	indexing	5	25	**75.52**	36.21	33.15
Fingerprint	exhaustive	-	-	100.00	44.43	36.80
	indexing	7	29	**32.23**	**39.57**	**31.21**
Iris	exhaustive	-	-	100.00	**44.60**	**32.52**
	indexing	6	45	**69.04**	74.42	49.42

- Results shown for Biohashing [3] in open-set scenario.
- Workload reductions are remarkable with respect to the baseline workload.
- Differential biometric performance and workload reduction across biometric characteristics utilised.
- Multi-biometric indexing scheme is expected to outperform the biometric performance of the retrieved individual biometric characteristic, while maintaining the overall workload of the system.

[3] ATB. Jin, DNC. Ling, and A. Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." In: *Pattern recognition* 37.11 (2004), pp. 2245–2255, p. 1.

Biometric WR

Results for multi-biometric characteristics: Face(FA), Fingerprint(FP), Iris(IR)

FNIR (%) in FPIR=0.01% and FPIR=0.1%, WR(%)

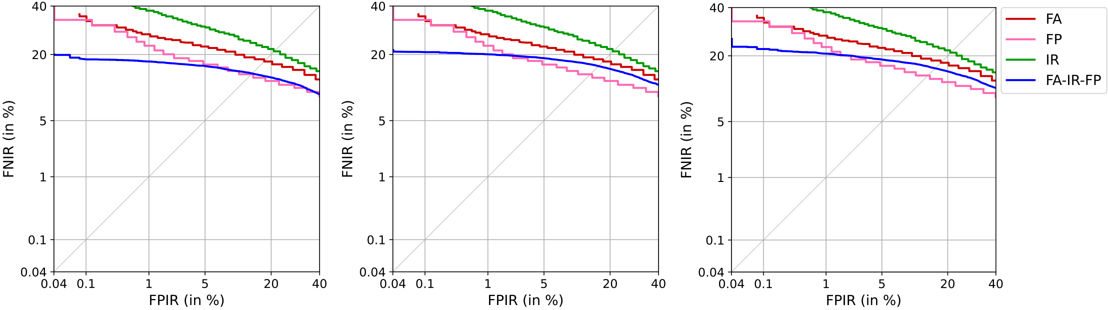
Method	BC	k	#Bins	WR(%)	FPIR=0.01(%)	FPIR=0.1(%)
Single BC	FA	5	25	75.52	36.21	33.15
	FP	7	29	**32.23**	**39.57**	**31.21**
	IR	6	45	69.04	74.42	49.42
Feature-concatenation	IR-FP	6	31	**53.07**	32.20	24.69
	FA-FP-IR	6	38	61.61	**19.81**	**19.36**
Ranked-codes	IR-FP	6	30	**53.40**	32.14	25.36
	IR-FP-FA	6	33	57.40	**21.55**	**20.81**
XOR-codes	IR-FP	5	25	**78.03**	35.25	29.36
	FA-FP-IR	7	63	81.55	**26.24**	**22.38**

- Advantage of the fusion for some biometric characteristics in terms of workload reduction.
- Improvement in biometric performance but the overall computational workload increases for specific biometric characteristics.

Biometric WR

Results for multi-biometric characteristics: Face(FA), Fingerprint(FP), Iris(IR).

Detection Error Trade-off (DET) curves between FPIR and FNIR.



Feature-concatenation

Ranked-codes

XOR-codes

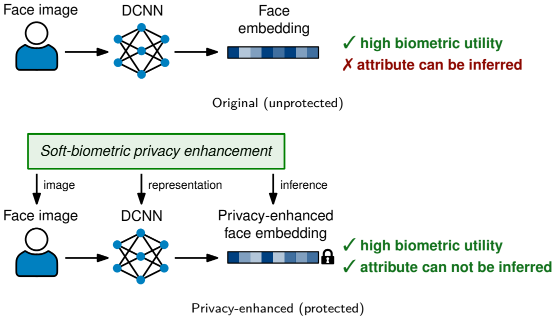
- Biometric performance of the multi-biometric system outperformed at the high-security thresholds: (i.e. FPIR $= 0.01\%$).

Privacy Protection Analysis

Privacy Protection Analysis

Soft-biometric privacy enhancement

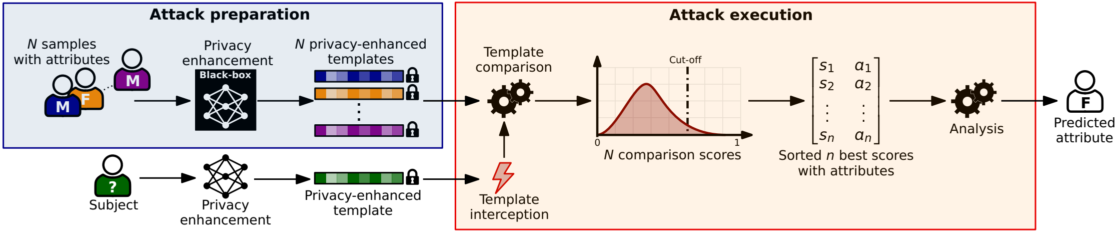
- Facial Soft-biometric Privacy-enhancing technologies (PETs).
- Mechanisms can operate on the feature level by cancelling the attribute or minimizing data.
- High utility on biometric data is preserved, even, when soft-information is cancelled or removed.
- Removal or suppression of facial information yields less discriminative face embeddings?


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

⇒ Need for a closer examination of soft-biometric privacy enhancement methods!

An Attack on Facial Soft-biometric Privacy Enhancement

Overview

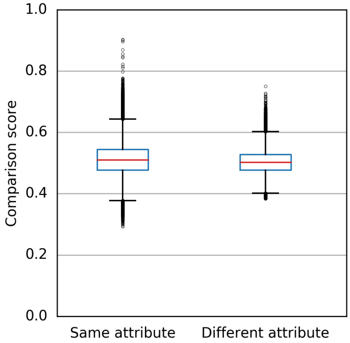

Attack preparation
N samples with attributes
M
F
M
Privacy enhancement
Black-box
N privacy-enhanced templates
Subject
?
Privacy enhancement
Privacy-enhanced template
Attack execution
Template comparison
Template interception
Cut-off
0
1
N comparison scores
$\begin{bmatrix} s_1 & a_1 \\ s_2 & a_2 \\ \vdots & \vdots \\ s_n & a_n \end{bmatrix}$
Sorted n best scores with attributes
Analysis
F
Predicted attribute

D. Osorio-Roig et al. “An Attack on Facial Soft-biometric Privacy Enhancement” Trans. on Biometrics, Behavior, and Identity Science (TBIOM), 2022.

An Attack on Facial Soft-biometric Privacy Enhancement

Execution

- Application of the privacy-enhancing method as black-box.
- Use of a small database of arbitrary face images.
- Two state-of-the-art algorithms for facial soft-biometric privacy enhancement: PFR-Net [4] and PE-MIU [5].
- Predict the soft-biometric attribute gender.
- Analyse the effect of broad homogeneity [6] in privacy-enhanced domains.



Boxplots of similarity scores.

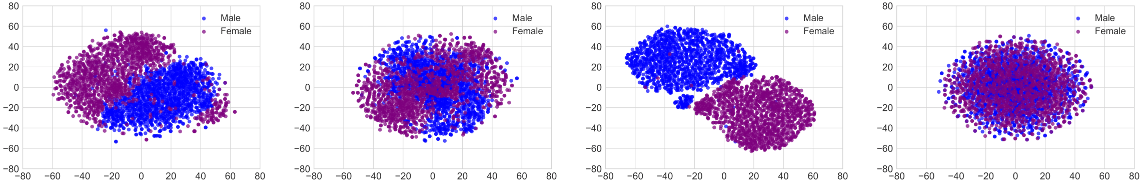
[4] B. Bortolato, M. Ivanovska, P. Rot, et al. “Learning privacy-enhancing face representations through feature disentanglement.” In: *2020 15th IEEE Intl. Conf. on Automatic Face and Gesture Recognition (FG 2020)*. IEEE. 2020, pp. 495–502, p. 1.

[5] P. Terhörst, K. Riehl, N. Damer, et al. “PE-MIU: A training-free privacy-enhancing face recognition approach based on minimum information units.” In: *IEEE Access* 8 (2020), pp. 93635–93647, p. 2.

Privacy Protection Analysis

An Attack on Facial Soft-biometric Privacy Enhancement

Results: performance analysis.



Original – VGGFace2

Privacy-enhanced – PRF-Net

Original – FaceNet

Privacy-enhanced – PE-MIU

- Privacy-enhanced face templates showed similar biometric performance with respect to unprotected templates.
- Privacy is preserved using machine learning technique-based evaluations.
- Visualization through the dimensionality reduction-based tools.
- Machine learning classifiers are not able to learn the pattern of a soft-biometric attribute, it means the pattern does not exist?

Privacy Protection Analysis

An Attack on Facial Soft-biometric Privacy Enhancement

Results: vulnerability analysis.

Summary of the best average attack success rates across all cross-database scenarios (in %).

Method	**Attack success rate**					
	$n = 1$	$n = 5$	$n = 10$	$n = 50$	$n = 100$	$n = 200$
PFRNet	74.92 ± 4.79	79.04 ± 7.08	**79.50 ± 7.42**	78.96 ± 9.06	77.54 ± 9.88	75.63 ± 12.79
PE-MIU	85.23 ± 3.97	88.12 ± 3.28	88.65 ± 3.68	**88.95 ± 3.99**	88.26 ± 4.08	86.91 ± 4.38

- Vulnerability with statistical analysis of the similarity scores: Majority vote, Average, and Weighted Average.
- Best average $\Rightarrow \sim 88\%$ and Best accuracy $\Rightarrow \sim 90\%$.
- Privacy-enhancing face templates retain certain properties of the original face recognition systems.
- The attack can be applied to other biometric characteristics where the effect of broad homogeneity is observed.
- Attack prevention $\Rightarrow$ BTP schemes.

Summary

Take-away Messages and Contributions

In relation to research questions

1. Is it possible to combine workload-reduction (WR) strategies with BTP schemes while maintaining accuracy and high privacy preservation?
   - Proposed indexing methods together with BTP schemes which reduced the computational workload, but do not impair the biometric performance of a biometric identication system.
   - The design of the proposed indexing methods allows the end-to-end protection of the biometric identification transaction, i.e. from the index to the biometric template.
2. Is it possible to create a multi-biometric system which combines WR strategies with BTP schemes and demands a low workload, while deploying high privacy protection for the different biometric characteristics (or fusion levels)?
   - Incorporated the fusion in a common protected feature representation at the feature level across different and protected types of biometric characteristicas maintaining an acceptable overall workload of the biometric system, good biometric performance, and high privacy protection.

Summary

Take-away Messages and Contributions

In relation to research questions

3. How can the trade-offs between biometric performance, template protection, and workload reduction in a biometric identification system be analysed and interpreted?
   - Trade-offs in terms of biometric performance, privacy protection, and workload reduction was evaluated empirically and analysed theoretically.
4. Can existing privacy-enhancing technologies (PETs) be successfully employed for privacy protection?
   - Novel vulnerabilities on facial soft-bimetric privacy-enhancing technologies.

Summary

Future work

- Scalability and Security with homomorphic encryption.
- Multi-biometric fixed-length representations.
- Evaluation of privacy-preserving workload-reduction schemes.
- Privacy analysis in biometric template protection.

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.

Publications (First Author)

Journals

1. **Dailé Osorio-Roig, Lázaro J. González-Soler, Christian Rathgeb and Christoph Busch, "Privacy-preserving Multi-biometric Indexing based on Frequent Binary Pattern", TIFS, 2024.**
2. **Dailé Osorio-Roig, Christian Rathgeb, Pawel Drozdowski, Philipp Terhörst, Vitomir Štruc, Christoph Busch, "An Attack on Facial Soft-biometric Privacy Enhancemen", TBIOM, 2022.**
3. **Dailé Osorio-Roig, Christian Rathgeb, Pawel Drozdowski, Christoph Busch, "Stable Hash Generation for Efficient Privacy-Preserving Face Identification", TBIOM, 2021.**

Conferences

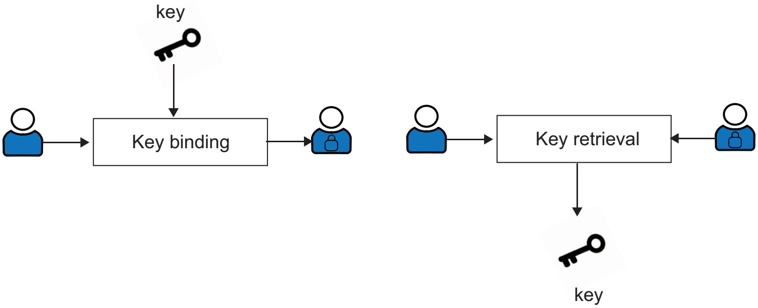
4. Dailé Osorio-Roig, Paul A. Gerlitz, Christian Rathgeb, Christoph Busch, Reversing Deep Face Embeddings with Probable Privacy Protection, in IEEE Intl. Workshop on Information Forensics and Security (WIFS), 2023.
5. Dailé Osorio-Roig, Mahdi Ghafourian, Christian Rathgeb, Ruben Vera-Rodriguez, Christoph Busch, Julian Fierrez, Optimizing Key-Selection for Face-based One-Time Biometrics via Morphing, in IEEE Intl. Workshop on Information Forensics and Security (WIFS), 2023.
6. Dailé Osorio-Roig, Tim Rohwedder, Christian Rathgeb, Christoph Busch, Analysis of Minutiae Quality for Improved Workload Reduction in Fingerprint Identification, in Proc Intl. Conf. of the Biometrics Special Interest Group (BIOSIG), 2022.
7. **Dailé Osorio-Roig, Christian Rathgeb, Hatef Otroshi-Shahreza, Christoph Busch, Sébastien Marcel, Indexing Protected Deep Face Templates by Frequent Binary Patterns, in International Joint Conference on Biometrics (IJCB), 2022.**
8. Dailé Osorio-Roig, Torsten Schlett, Christian Rathgeb, Juan Tapia, Christoph Busch, Exploring Quality Scores for Workload Reductionin Biometric Identification, in International Workshop on Biometrics and Forensics (IWBF), 2022.

Backup

Biometric Template Protection Schemes

Biometric data protection

- Biometric cryptosystems:

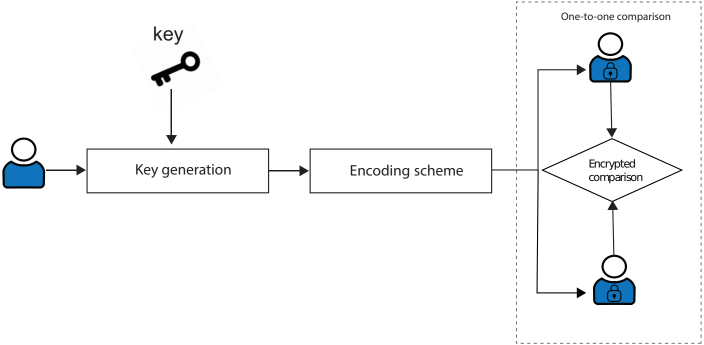


⇒ Enable complex processes of biometric comparison by verifying the correctness of a retrieved key.

⇒ Offering solutions to biometric-dependent key-release and biometric template protection.

Biometric data protection

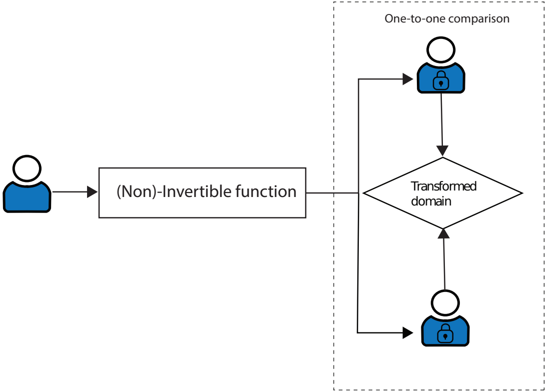
- Homomorphic encryption:



⇒ Optimizations depend on the encoding schemes.
⇒ Limited operations in the encrypted domain.
⇒ Preserving biometric performance.

Biometric data protection

- Cancelable biometrics:



⇒ Retaining efficient biometric comparators.

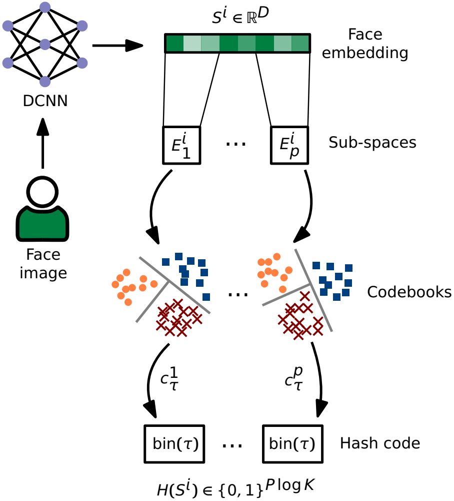
⇒ Degradation of the biometric performance.

Hash Look-up Table

Hash Generation Scheme

Theory

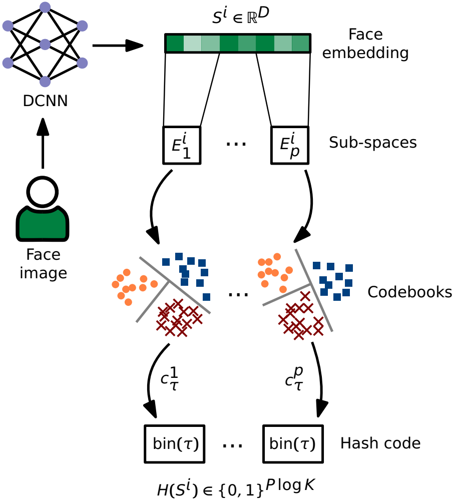
- Each biometric reference is represented for its corresponding face embedding extracted of size D: $\mathbf{S} = \{S^1, \ldots, S^N\}$.
- Each face embedding is divided into P sub-spaces or sub-vectors that are approximated by the nearest cluster.
- Product Quantization is applied on the entire feature vector to represent a concatenation of P sub-spaces of equal size.
- A compact hash code of $P \log_2(K)$ bits is represented for each face embedding.



Hash Generation Scheme

Computational Workload

- $W_{proposed} = N \times p \times \theta + \beta$ (hash look-up table).
- An exact match, i.e. $\beta \ll 1.00$ms.
- Cost of a one-to-one comparison $\rightarrow \theta$.
- Penetration rate $\rightarrow p$.
- Fraction of protected templates indexed in O(1) $\rightarrow \gamma$
- Total of subjects enrolled $\rightarrow N$
- $p = \frac{\gamma}{N}$.
- It is expected $W_{proposed} \ll W_{baseline}$
- $W_{baseline} \rightarrow 100\%$.



Backup

Scenarios of evaluation

- Closed-set scenario: Proposed system is to correctly handle identification transactions with data subjects whose references **are present** in the enrolment database.
- Open-set scenario: Proposed system is to correctly handle identification transactions with data subjects whose references **are not present** in the enrolment database.

Clustering techniques

- Centroid-based clustering techniques (K-means, K-medoids).
- Density-based clustering algorithm (Gaussian mixture model).
- Graph-based clustering algorithm (Affinity propagation)
- Number of clusters and sub-vectors: $\mathbf{K} = \{64, 128, 256, 512, 1024\}$ and $\mathbf{P} = \{1, 2, 4\}$

Backup

Metrics

Closed-set scenario

- Pre-selection error rates: the proportion of subjects for which the corresponding subject identifier is not in the pre- selected subset of candidates.
- Hit-rate: which computes the complement of the preselection error rates: 1 - pre-selection error rates.

Open-set scenario

- The Detection Error Trade-off (DET) curves between false negative identification rate (FNIR) and false fositive fdentification rate (FPIR) .
- The FNIR observed at different FPIR values such as 1% (FNIR100) and 0.1% (FNIR1000).

Computational workload reduction

- Computational Workload: the overall computational workload of a biometric identification transaction as a percentage of the baseline (exhaustive search) workload in terms of the number of template comparisons.

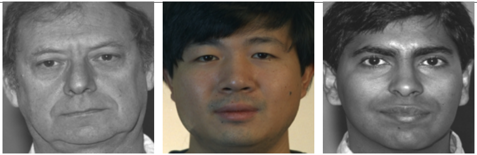
Configurations

Databases

- FERET ⇒ frontal face images with variations of color and expression.
- FEI ⇒ extreme pose variation.
- LFW ⇒ unconstrained face recognition problem in the wild.

Homomorphic encryption

- Brakerski/Fan-Vercauteren (BFV) scheme ⇒ batching technique.
- Security level ⇒ 128 bits.



FERET

FEI

LFW

Security and privacy protection analysis

- Compact hash code of size ⇒ leaks no information about the biometric feature.
- Hash code length is $4\log(1024) = 40$ bits ⇒ not more than 128 bits.
- Non-fuzzy comparison ⇒ a hard task to get similarity information from the indexing scheme.
- Message Authentication Codes (MACs) which may involve the use of cryptographic hash functions (HMACs), e.g., SHA-256 ⇒ prevents cross-matching or reconstruction attacks.
- **Unlinkability**, **Renewability**, **Irreversibility** ⇒ guaranteed by the BTP scheme used.
- The security and privacy protection ⇒ upper-bounded by attackers' effort of being falsely accepted by the system, the so-called **false accept attack**.

Multi-biometric system

Backup

Configuration

- LFW (Face).
- MCYT(Fingerprint).
- CASIA-Iris-Thousand and BioSecure (Iris).
- 1,170 identities for each database.
- Filtering by quality.
- Index-of-Maximum Hashing with Gaussian Random Projection (IoM-GRP) and Bio-Hashing approaches as Cancelable Biometrics.
- Score normalisation $\Rightarrow$ Z-score method
- Score-level fusion $\Rightarrow$ sum-rule fusion

Backup

Privacy Analysis Protection