

Biometric Template Protection: Why and How

Christoph Busch, Marta Gomez-Barrero, Hafez Otroschi Shahreza

Chapter 1, Handbook of Biometric Template Protection (Springer, 2026)



Biometrics: a double-edged property

Advantage

Biometric characteristics are immutable — they cannot be delegated or forgotten.
A non-delegable factor, e.g. for payment services (PSD2).

Disadvantage

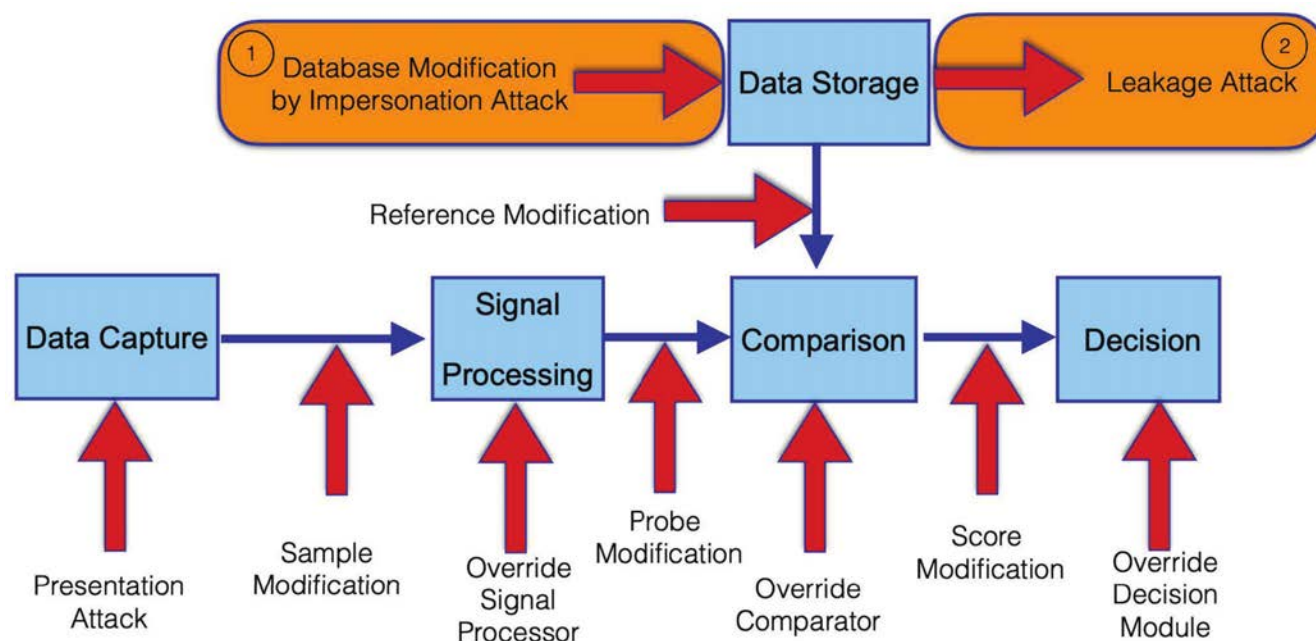
Biometric characteristics are immutable — they cannot be updated once a reference has leaked.

Not “stolen” — *leaked*

The fingerprint stays on the fingertip; what leaks is a representation of it (image, template or protected reference).

Biometric Template Protection (BTP) disentangles the characteristic from the stored record: a pseudonymous identity (PI) that can be re-issued with a new seed if it leaks.

Two attacks on the reference database



1 Impersonation

Replace the victim's reference with the attacker's own sample. Requires missing integrity protection.

2 Leakage

The "silent" attack: copy references without modifying anything.

Fig. 1.1 — attack vectors against the data storage subsystem (after ISO/IEC 30107-1)

Impersonation without being noticed



Fig. 1.2 — parent images (left, right) and morph (centre)

- **Morphing:** a morph verifies against both attacker and victim, and fools face recognition and human examiners.
- **High attack potential:** parents chosen with the same gender, similar age and skin tone.

2.5 M

identity-theft cases per year involve deceased people (Fraud.net)

If the victim is deceased or missing and the records are not maintained, nobody notices the replaced reference.

Why would anyone leak biometric references?

1 Statistics

Draw conclusions on the whole enrolment database, e.g. the distribution of demographic groups (age, gender).

2 Medical data

Derive health information about a person of interest, such as the CEO of the operating organisation.

3 Attack instruments

Derive a digital sample to build a presentation attack instrument (PAI) for impersonation.

Integrity protection stops modification, but not leakage. Leaked references remain a risk.

Incidents in operational systems

5.6 M

fingerprint images

US / DoD breach, 2015.
DoD assessed the “ability to misuse
fingerprint data is limited”.

≈10 M

Afghan citizens enrolled

AABIS and APPS databases (iris,
face, fingerprint) left behind in 2021
came under Taliban control.

AABIS - Automatic Biometric Identification System
APPS - Afghan Personnel and Pay System

**Storing biometric data unprotected cannot be justified.
Use BTP in any system, especially with central storage.**

Biometric samples reveal health information



Fig. 1.3 — same finger: bad (left) and good skin condition



Fig. 1.4 — Simian line (left) vs normal creases

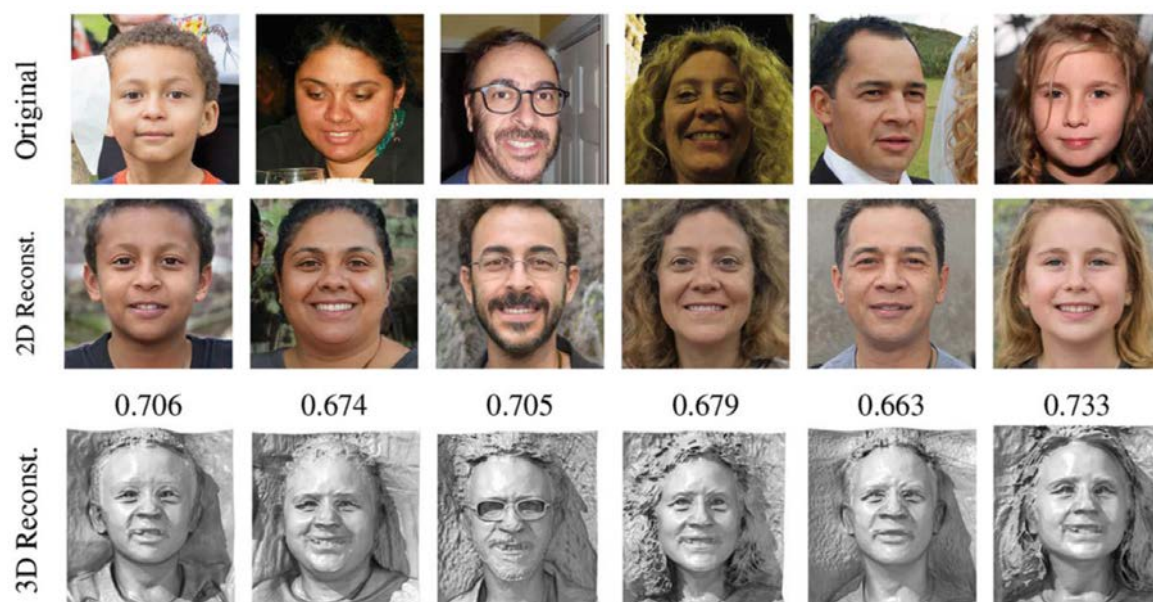
- **Fingerprint:** ~10% of people in Western countries have skin diseases (e.g., atopic eczema), and these effects are shown in the example.
- **Palmprint:** crease patterns can indicate genetic conditions, e.g. Down's syndrome.
- **Iris / face:** iris melanoma progression, skin cancer, emotions and psychological state.

GDPR Art. 9

Biometric and health data are sensitive; processing them is prohibited by default.

BTP is a “safeguard for the fundamental rights and interests of the data subject” (Art. 9.2).

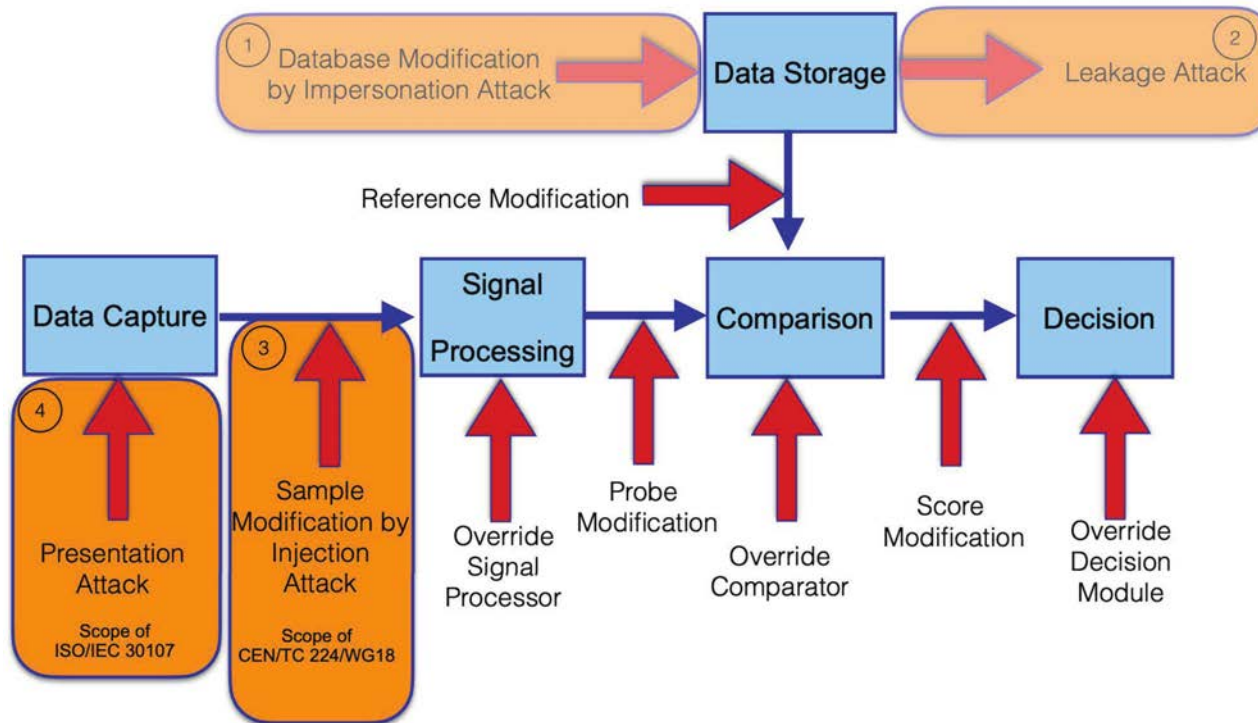
Template inversion: templates do not protect



- **Attack:** invert stored templates to reconstruct the biometric sample.
- **Fingerprint & vein:** images reconstructed from minutiae templates and from binary vein templates.
- **Face:** white-box (extractor known, gradient-based) vs black-box (extractor unknown) attacks.
- **GAN-based:** realistic, high-quality images, now even 3D reconstructions.

Fig. 1.5 — FFHQ originals, 2D and 3D reconstructions from ArcFace templates (cosine similarity shown)

From reconstructed sample to impersonation



3 Injection attack

Bypass the capture device and feed the sample to signal processing.
CEN Standard converted to ISO/IEC Standardisation: ISO/IEC 25456

4 Presentation attack

Turn the sample into a presentation attack instrument (PAI) (printout, display, silicone mask, rubber stamp).
Detection testing: ISO/IEC 30107.

Fig. 1.6 — injection attack (3) and presentation attack (4) with an inverted sample

Protection methods and goals

Turning a biometric template into a renewable biometric reference (RBR)

Four families of template protection

Biometric Template Protection

FT- Feature Transformations

Reproducible, key-controlled distortion of sample or feature vector. Comparison in the protected domain.

BC- Biometric Cryptosystems

Helper-data schemes that bind or (re)generate a key and compensate for intra-class variance.

HE- Homomorphic Encryption

Compute similarity scores on encrypted data. Only the score is decrypted.

LT- Learned Transforms

Neural networks learn the mapping to a protected template.

Bloom filters (FT) and Homomorphic Encryption (HE) can maintain or even improve unprotected accuracy.

ISO/IEC 24745: four requirements for BTP

1 Recognition accuracy

No degradation in FMR / FNMR compared with the unprotected system.

2 Irreversibility

No sample can be reconstructed from the RBR, so no presentation attack (PA), no injection and no demographic statistics.

3 Confidentiality

No leakage of demographic or health data. Comparison runs in the protected domain.

4 Diversification

Unlinkable across applications (space) and renewable after a breach (time), which enables revocability.

Diversification in space: unlinkability

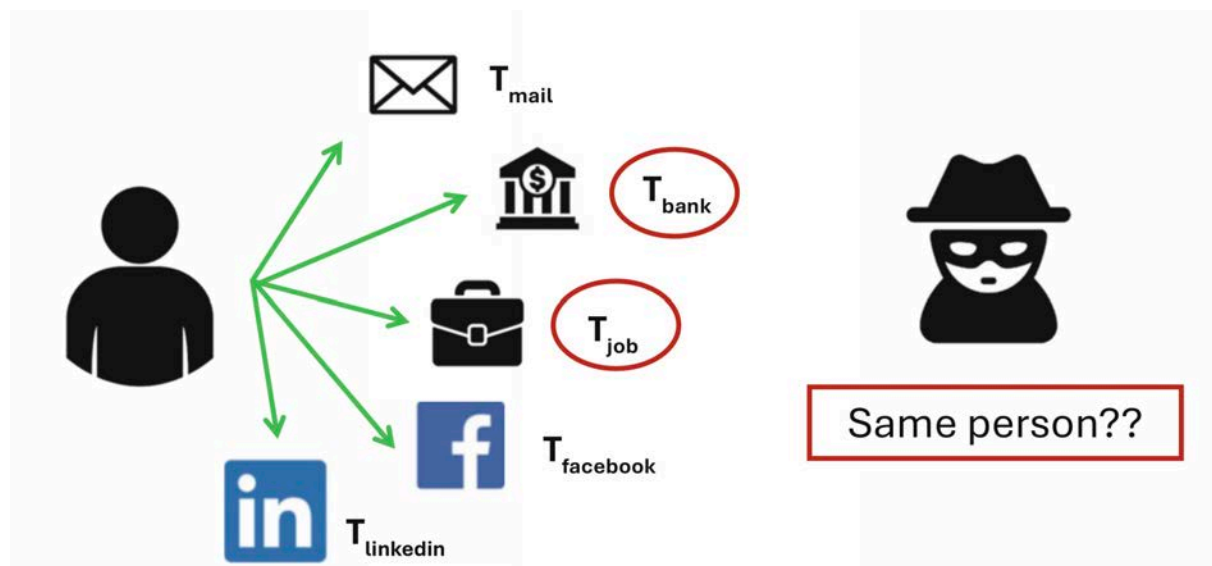
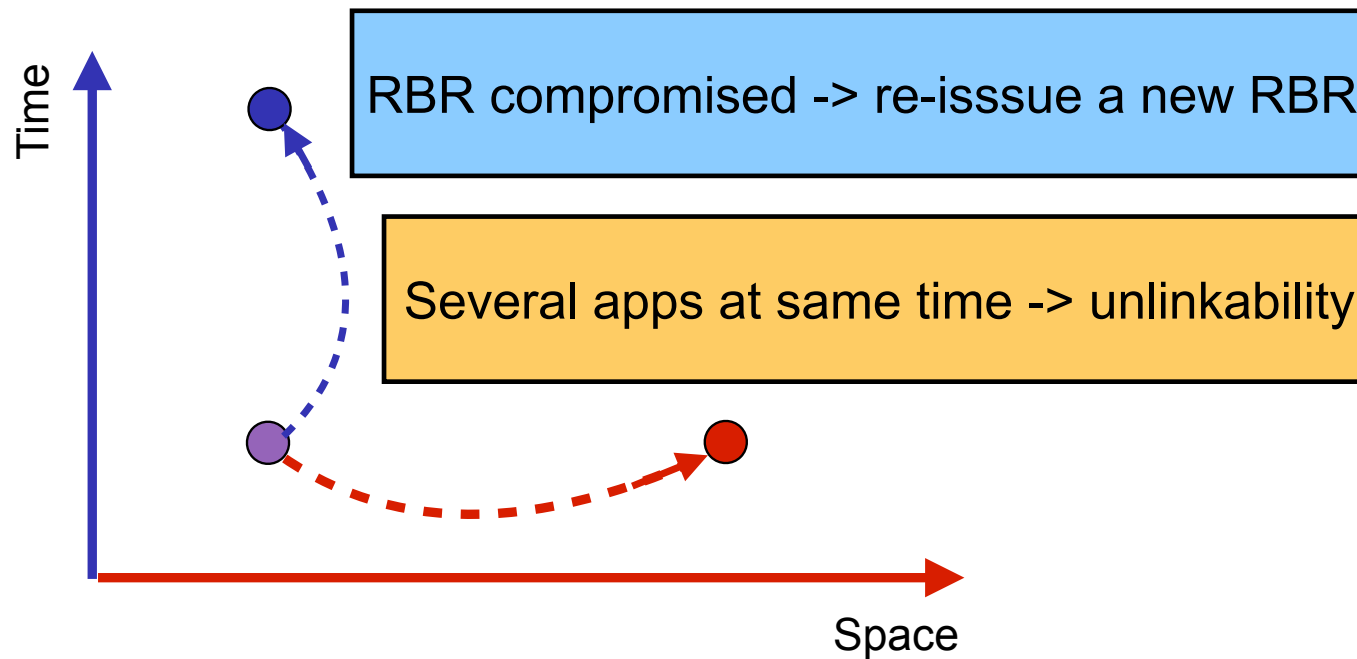


Fig. 1.8 — references T_{bank} and T_{job} cannot be c not allow profiling

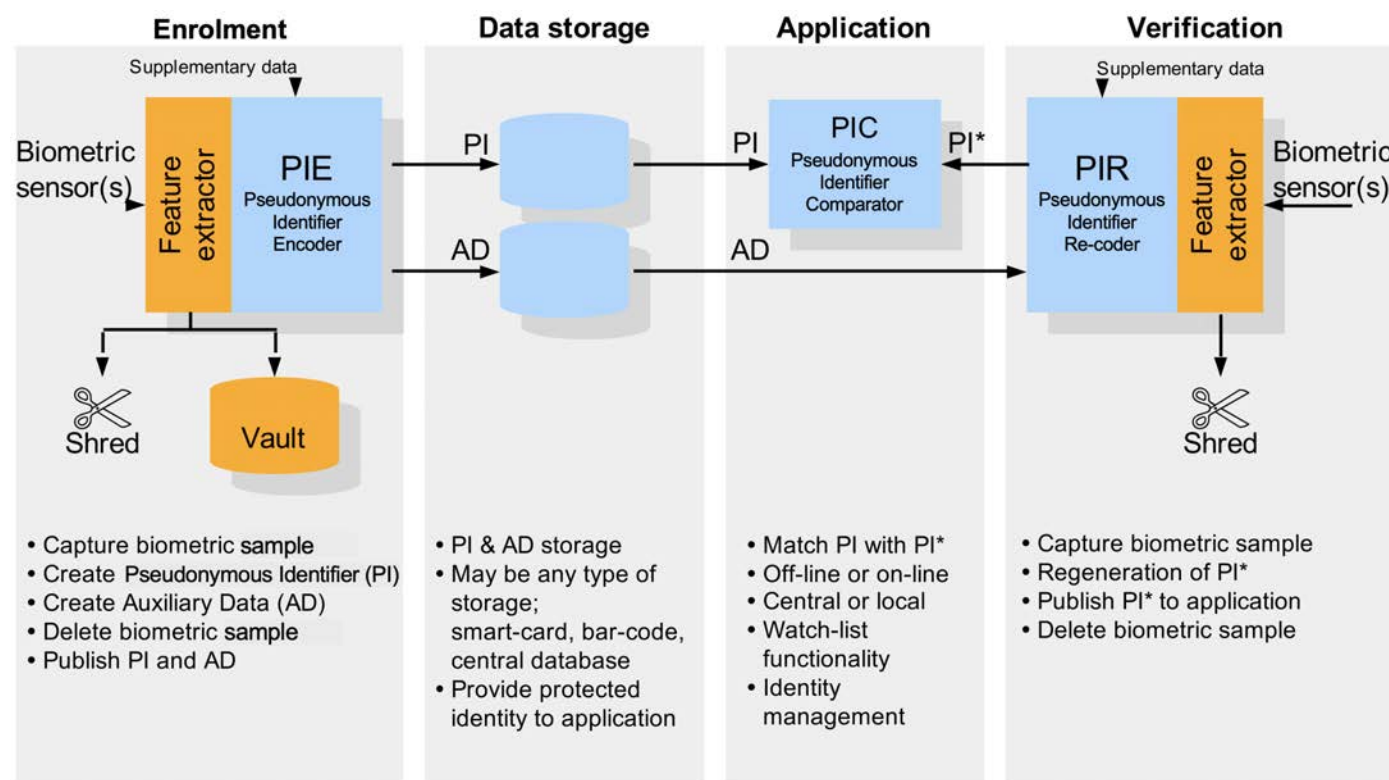
- **Space:** one face, many services, but no cross-matching and therefore no profiling.
- **Time:** after a breach, issue a new reference with new seed values.
- **Testable:** unlinkability is measured under ISO/IEC 30136.

Diversification

Unlinkable across applications (space) and renewable after a breach (time), which enables revocability.



The ISO/IEC 24745 reference framework



- **PIE** encodes features into PI + AD. Then shred the features or keep them in a vault.
- **PIR** re-codes the probe with AD to PI*.
- **PIC** compares PI and PI*, and returns a score.
- **Bilateral control:** Pseudonymous Identity (PI) with the operator, Auxiliary Data (AD) with the subject (e.g., on a card).
Either side can cancel the enrolment

Fig. 1.9 — framework for biometric template protection

Evaluation methodology

ISO/IEC 30136: performance testing of biometric template protection schemes

Benchmarking BTP under explicit threat models

Enrolment & verification performance

Accuracy compared with the unprotected baseline under the same protocol, plus storage (AD and PI bits reported separately) and computational overhead.

Security & privacy protection

Irreversibility, unlinkability and successful attack rates.
Mostly empirical, because biometric data is neither uniform nor easy to model.

Threat models (attacker knowledge ↑)

Naive

Only the protected RBRs, black-box

Collision

Large biometric data set and a BTP of choice

General · standard

Kerckhoffs: algorithm and statistics known, key secret

General · advanced

Can execute the BTP subsystems

General - Full disclosure

Also holds the secret keys

Protection need not cost accuracy

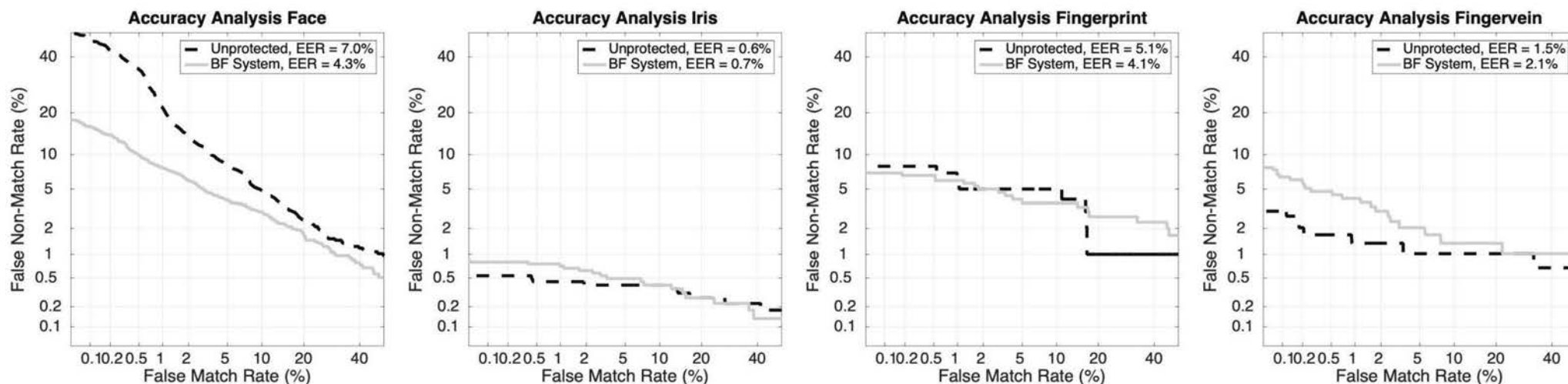


Fig. 1.10 — DET curves for face, iris, fingerprint and finger vein, unprotected vs Bloom-filter BTP

Measured per ISO/IEC 19795-1

FNMR at a fixed FMR, e.g. 0.1% (FRONTEX-rec.).
Mated and non-mated comparison trials.

Identification: $FPIR \approx N \cdot FMR$

Errors scale with database size,
so large systems need workload reduction.

Fairness: an open challenge for BTP

Differential performance

Difference in biometric system metrics across demographic groups (ISO/IEC 19795-10).

- **Acceptance** requires that subjects are treated fairly by both recognition and BTP algorithms.
- **NISTIR 8280** showed demographic differentials in mated and non-mated score distributions.
- **Causes:** unbalanced training data and systematic effects in training.
- **Open:** bias of BTP methods has not been investigated yet. Mitigation is in its infancy.

Anticipate the leak

References may be leaked at some point, so BTP is a necessary part of any biometric system, combined with presentation attack detection.

Design: ISO/IEC 24745 ·

Evaluate: ISO/IEC 30136 + 19795-1 · Criteria: accuracy, irreversibility, confidentiality, diversification

Contact



ATHENE

National Research Center
for Applied Cybersecurity



h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI

Schöfferstr. 3
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-533-30090

<https://dasec.h-da.de>

<https://www.athene-center.de>