Privacy-Preserving Biometrics

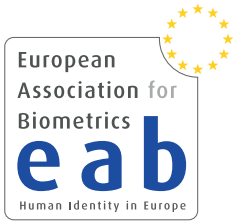
Christoph Busch

22nd Int.l Summer school for advanced studies on biometrics
2025-06-05

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

ATHENE



Overview

Structure of this session

- Privacy and data protection culture
- Data protection principles
- Non-discriminatory biometric system and additional information in biometric samples
- Biometric template protection

Privacy and Data Protection Culture

What is the Perspective?

Privacy and data protection culture differs

- European Countries:
  - Biometric data is owned by the data subjects, who determine the use and disclosure of their personal data (right of informational self-determination)
- Non-European Countries (e.g. USA):
  - Biometric data is owned by the organization that processed the data

Source: Hoan Ton-That (Clearview 2021)

https://weta.org/watch/shows/amanpour-and-company/clearview-ai-ceo-defends-facial-recognition-software-nuyagm

Erik Carter

China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment

Even children are pressed into giving blood samples to build a sweeping genetic database that will add to Beijing's growing surveillance capabilities, raising questions about abuse and privacy.

What is the Difference?

Privacy is not data protection

- Privacy refers to a personal sphere, whereas
- Data protection refers to control over or protection of personal information

Examples

- Unwanted physical contact falls under privacy but not under data protection.
- When someone gives her address to a hotel for billing purposes data protection rules apply, but it will generally not be a privacy matter.

Source: https://www.hiig.de/en/why-privacy-%E2%89%A0-data-protection-and-how-they-overlap/ (2024)

Fundamental Rights in EU Treaties

Council of Europe (~~47~~ 46 member states)

- European Convention on Human Rights (ECHR), 1950
  - Art. 8 ECHR : Right to respect for private and family life

(1) Everyone has the right to respect for his private and family life, his home and his correspondence

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Image Source: Atle Arnes (2019)

Fundamental Rights in EU Treaties

European Union

- Charter of Fundamental Rights, 2000 (last updated 2012)
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT
  - Entry into force with the treaty of Lisbon (December 2009)
  - The charter is the „constitution of the EU“

Fundamental Rights in EU Treaties

European Union

- Charter of Fundamental Rights
  - Article 7: Respect for private and family life
    Everyone has the right to respect for his or her private and family life, home and communications.
  - Article 8: Protection of personal data
    (1) Everyone has the right to the protection of personal data concerning him or her.
    (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
    (3) Compliance with these rules shall be subject to control by an independent authority.

Legal & Regulatory Framework for Biometrics

Council of Europe

- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981
  - Article 2 - Definitions:
    - *personal data means any information relating to an identified or identifiable individual ("data subject")*
    - *automatic processing includes the following operations if carried out in whole or in part by automated means: storage of data, ... retrieval or dissemination;*
    - *controller of the file means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, ... which operations should be applied to them.*

Legal & Regulatory Framework for Biometrics

EU legal Framework

- General Data Protection Regulation (GDPR)
  - Regulation 2016/679
- Reform aimed to make the rules clearer and more consistent by replacing the former patchwork of national laws with one, common EU-law.
- Rules apply to all companies targeting EU consumers, regardless of whether they are established inside or outside the EU
- Obligations of data controllers and processors are adjusted to the size of the business and/or the nature of the data being processed, in order to avoid burden for smaller companies.

Image Source: https://www.flaticon.com (2020)

Legal & Regulatory Framework for Biometrics

What is biometric data from a data protection perspective?

- Biometric data in whatever form (captured sample, template) is clearly personal data
- It may be sensitive data?

Sensitive Data

- Article 9.1 of GDPR listed the following special categories.
  - racial or ethnic origin,
  - political opinions, religious or philosophical beliefs,
  - or trade union membership,
  - the processing of genetic data,
  - biometric data for the purpose of uniquely identifying a natural person,
  - data concerning health or data concerning a natural person's sex life or sexual orientation
- Processing of sensitive data shall be prohibited.

Legal & Regulatory Framework for Biometrics

Processing of sensitive data in the GDPR

- Article 9.1 prohibits the processing of
  - biometric data for the purpose of uniquely identifying a natural person,
- Article 9.2.g states that paragraph 1 shall not apply if one of the following applies:
  - …
  - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Legal & Regulatory Framework for

GDPR Recital 51:

- *Personal data which are, …The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.*
- The operation of surveillance systems is addressed in the AI-Act

Image Source: https://www.tfeconnect.com (2020)

Image Source: https://www.verwaltung-der-zukunft.org/ (2020)

Data Protection Principles

EU - Data Protection Principles

Criteria for processing biometric data:

- Proper processing basis must exists
  - For example, data subject has unambiguously given consent
    OR
    compliance with legal obligation

Image Source: https://www.flaticon.com (2020)

- Fallback principle
  - Non-discriminatory systems
  - The data controller shall not condition the access to its services to the acceptance of the biometric processing
  - When used for authentication purpose, the data controller must offer an alternative solution (without biometrics)

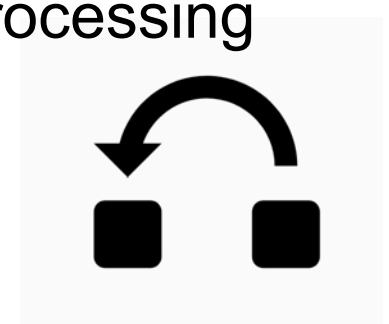


Image Source: https://thenounproject.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Purpose binding / finality principle
  - Personal data may be used only for the purpose they were originally collected for
  - Personal data shall not further be processed in a manner that is incompatible with those purposes
- Accuracy principle
  - Personal data shall be accurate and kept up to date

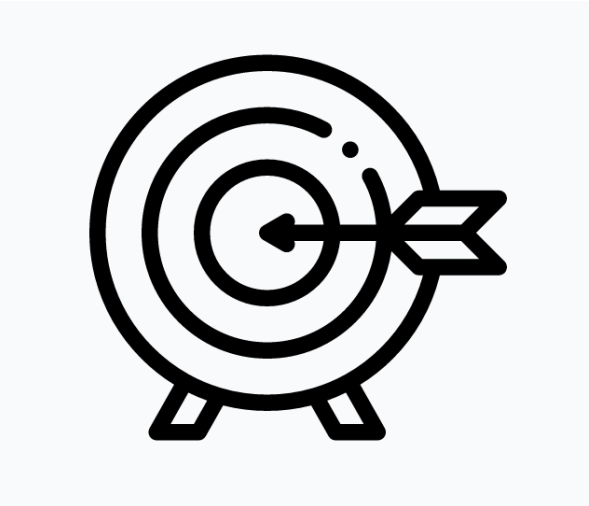


Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Proportionality in relation to interference
  - Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected
  - Process is necessary to fulfill the purpose of the system

Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Data minimization principle
  - Storage limitation with automatic routines for deletion
  - Personal data to be deleted or anonymized as soon as possible:
    data must be kept ... for no longer than is necessary
    for the purposes for which the data were collected

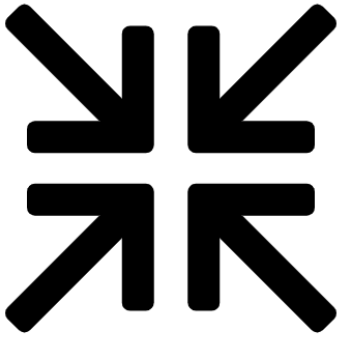


Image Source: https://www.flaticon.com (2020)

EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Transparency principle
  - Transparency for the data subject is needed, when and which data are collected and processed and for which purposes
  - Data subjects should be informed, who is collecting their data
- Accountability principle
  - Controller is responsible for, and must be able to document, compliance with the regulations.

Image Source: https://www.flaticon.com (2020)

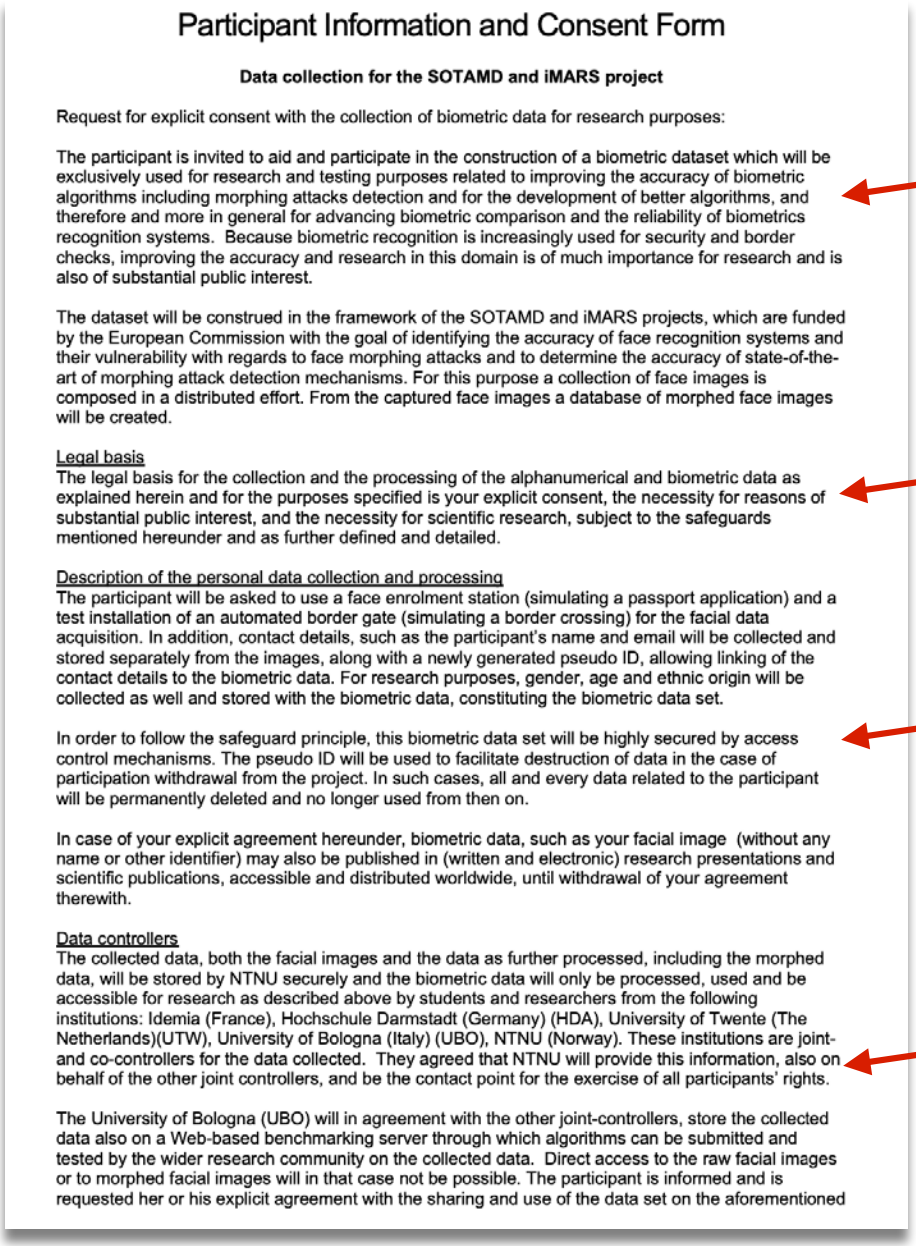
EU - Data Protection Principles

Criteria for processing biometric data (cont.):

- Protection of sensitive personal data
  - Processing of sensitive data (e.g. concerning health) prohibited
- Integrity and confidentiality
  - Personal data shall be secured against unauthorized or illegal access and against accidental loss, destruction or damage.
- Safeguard principle
  - *Controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access*

Image Source: https://www.flaticon.com (2020)

A Consent Form - Example



Participant Information and Consent Form

Data collection for the SOTAMD and iMARS project

Request for explicit consent with the collection of biometric data for research purposes:

The participant is invited to aid and participate in the construction of a biometric dataset which will be exclusively used for research and testing purposes related to improving the accuracy of biometric algorithms including morphing attacks detection and for the development of better algorithms, and therefore and more in general for advancing biometric comparison and the reliability of biometrics recognition systems. Because biometric recognition is increasingly used for security and border checks, improving the accuracy and research in this domain is of much importance for research and is also of substantial public interest.

The dataset will be construed in the framework of the SOTAMD and iMARS projects, which are funded by the European Commission with the goal of identifying the accuracy of face recognition systems and their vulnerability with regards to face morphing attacks and to determine the accuracy of state-of-the-art of morphing attack detection mechanisms. For this purpose a collection of face images is composed in a distributed effort. From the captured face images a database of morphed face images will be created.

Legal basis
The legal basis for the collection and the processing of the alphanumerical and biometric data as explained herein and for the purposes specified is your explicit consent, the necessity for reasons of substantial public interest, and the necessity for scientific research, subject to the safeguards mentioned hereunder and as further defined and detailed.

Description of the personal data collection and processing
The participant will be asked to use a face enrolment station (simulating a passport application) and a test installation of an automated border gate (simulating a border crossing) for the facial data acquisition. In addition, contact details, such as the participant's name and email will be collected and stored separately from the images, along with a newly generated pseudo ID, allowing linking of the contact details to the biometric data. For research purposes, gender, age and ethnic origin will be collected as well and stored with the biometric data, constituting the biometric data set.

In order to follow the safeguard principle, this biometric data set will be highly secured by access control mechanisms. The pseudo ID will be used to facilitate destruction of data in the case of participation withdrawal from the project. In such cases, all and every data related to the participant will be permanently deleted and no longer used from then on.

In case of your explicit agreement hereunder, biometric data, such as your facial image (without any name or other identifier) may also be published in (written and electronic) research presentations and scientific publications, accessible and distributed worldwide, until withdrawal of your agreement therewith.

Data controllers
The collected data, both the facial images and the data as further processed, including the morphed data, will be stored by NTNU securely and the biometric data will only be processed, used and be accessible for research as described above by students and researchers from the following institutions: Idemia (France), Hochschule Darmstadt (Germany) (HDA), University of Twente (The Netherlands)(UTW), University of Bologna (Italy) (UBO), NTNU (Norway). These institutions are joint- and co-controllers for the data collected. They agreed that NTNU will provide this information, also on behalf of the other joint controllers, and be the contact point for the exercise of all participants' rights.

The University of Bologna (UBO) will in agreement with the other joint-controllers, store the collected data also on a Web-based benchmarking server through which algorithms can be submitted and tested by the wider research community on the collected data. Direct access to the raw facial images or to morphed facial images will in that case not be possible. The participant is informed and is requested her or his explicit agreement with the sharing and use of the data set on the aforementioned

what is it about

the legal basis

purpose and safeguard

the data controller

A Consent Form - Example (cont.)

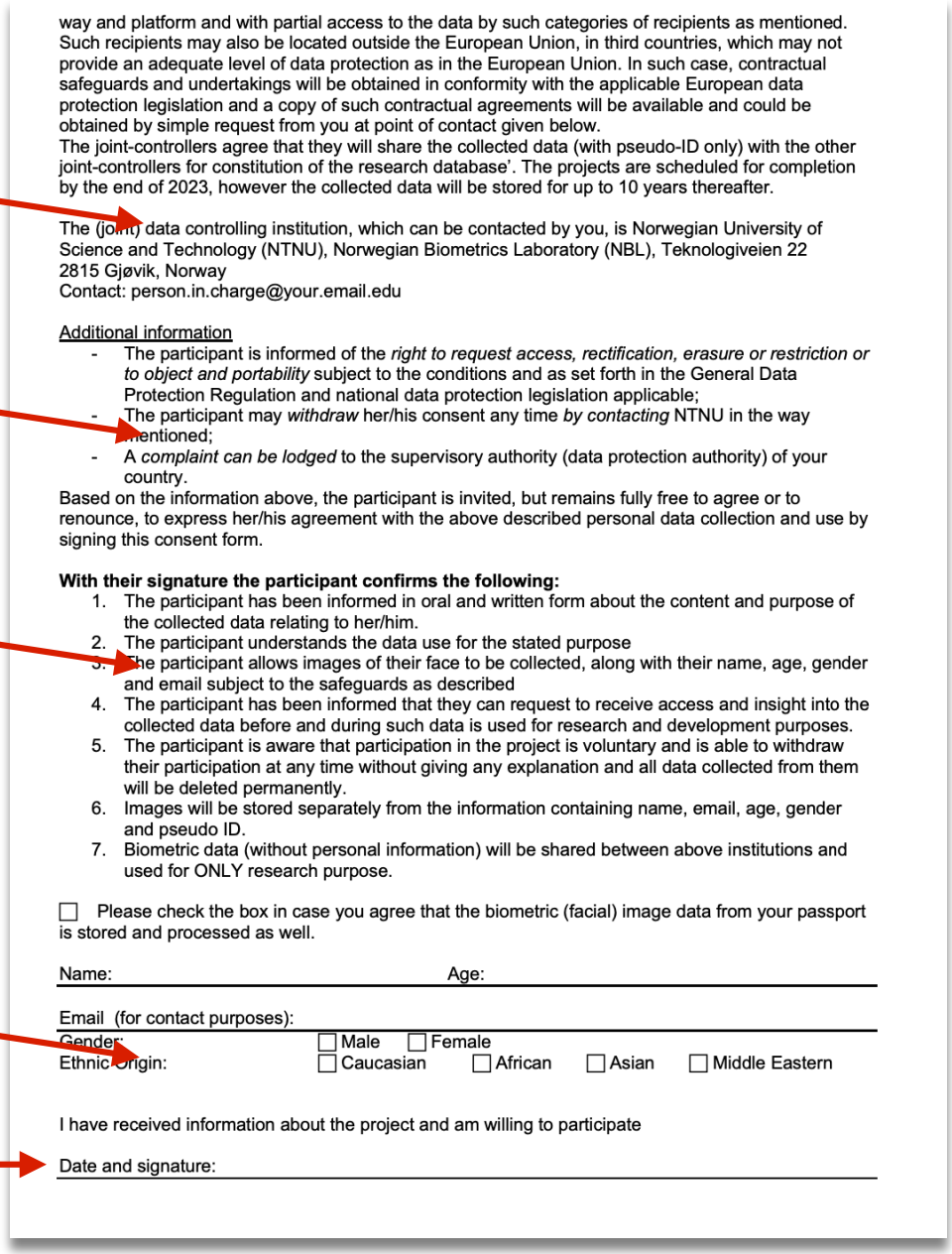
point of contact

right to withdraw

scope of agreement

alphanumerical data

signature



way and platform and with partial access to the data by such categories of recipients as mentioned. Such recipients may also be located outside the European Union, in third countries, which may not provide an adequate level of data protection as in the European Union. In such case, contractual safeguards and undertakings will be obtained in conformity with the applicable European data protection legislation and a copy of such contractual agreements will be available and could be obtained by simple request from you at point of contact given below.
The joint-controllers agree that they will share the collected data (with pseudo-ID only) with the other joint-controllers for constitution of the research database'. The projects are scheduled for completion by the end of 2023, however the collected data will be stored for up to 10 years thereafter.

The (joint) data controlling institution, which can be contacted by you, is Norwegian University of Science and Technology (NTNU), Norwegian Biometrics Laboratory (NBL), Teknologiveien 22 2815 Gjøvik, Norway
Contact: person.in.charge@your.email.edu

Additional information

- The participant is informed of the *right to request access, rectification, erasure or restriction or to object and portability* subject to the conditions and as set forth in the General Data Protection Regulation and national data protection legislation applicable;
- The participant may *withdraw* her/his consent any time *by contacting* NTNU in the way mentioned;
- A *complaint can be lodged* to the supervisory authority (data protection authority) of your country.

Based on the information above, the participant is invited, but remains fully free to agree or to renounce, to express her/his agreement with the above described personal data collection and use by signing this consent form.

With their signature the participant confirms the following:

1. The participant has been informed in oral and written form about the content and purpose of the collected data relating to her/him.
2. The participant understands the data use for the stated purpose
3. The participant allows images of their face to be collected, along with their name, age, gender and email subject to the safeguards as described
4. The participant has been informed that they can request to receive access and insight into the collected data before and during such data is used for research and development purposes.
5. The participant is aware that participation in the project is voluntary and is able to withdraw their participation at any time without giving any explanation and all data collected from them will be deleted permanently.
6. Images will be stored separately from the information containing name, email, age, gender and pseudo ID.
7. Biometric data (without personal information) will be shared between above institutions and used for ONLY research purpose.

☐ Please check the box in case you agree that the biometric (facial) image data from your passport is stored and processed as well.

Name: Age:

Email (for contact purposes):

Gender: ☐ Male ☐ Female
Ethnic Origin: ☐ Caucasian ☐ African ☐ Asian ☐ Middle Eastern

I have received information about the project and am willing to participate

Date and signature:

Non-discriminatory Biometric System and additional Information in Biometric Samples

Operational Risk

Limited universality of a biometric characteristic may result in:

- Discriminatory situation for the capture subject
- Operational risk

Jan 2, 2004

Faded fingerprints cost former welder a job

ASSOCIATED PRESS

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

Strickler

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

But because of his welding work, Strickler has only about 30 of the identification points.

Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.

Demographic Effects

- Dermatologists estimate that up to 11% of the population suffers from skin diseases, which will directly impact fingerprint recognition
  - Atopic eczema
  - Atopic hand eczema
  - Hyper ceratotic hand eczema
  - Thrombangitis obliterans etc.

- Operational systems must provide non-discriminatory fallback procedures!

Additional Information from Hand Patterns

Limited intellectual capabilities are correlated with a certain hand pattern

- Down syndrome (aka Trisomy 21) - Simian crease
  "*A simian crease is defined as fusion of the proximal and distal transverse palmar creases into single transfers palmar crease.*" [Pur1972]
- Roseola - Sydney line
  "*A sydney line occurs where the proximal transverse crease extends beyond the midline axis of the fifth finger towards the ulnar border of the palm.*" [Pur1972]

Normal flexion crease

Simian crease

Sydney line

[Pur1972] S.G. Purvis-Smith: „The Sydney Line: A significant Sign in Downs Syndrome", Australian Paediatric Journal, 8:198-200, (1972)

Additional Information from Face Samples

We can detect the mood of an individual without a biometric system.

- … and we can keep a record of it with a sample

Other critical issues?

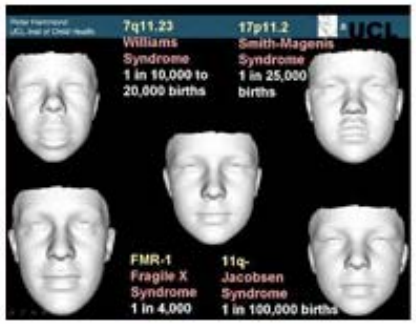
medGadget
internet journal of emerging medical technologies

Tuesday, September 11, 2007

3D Face Scan for Diagnosis of Genetic Syndromes

Filed under: Pediatrics

Professor Peter Hammond from the Institute of Child Health at the University College London has developed software that can scan facial features of children, and offer a likely diagnosis from over 700 genetic conditions. According to Dr. Hammond's report, presented at the ongoing BA Festival of Science by the British Association for the Advancement of Science, his software is pretty accurate in making the diagnosis:



Additional Information from Iris Samples

Malign melanom of the iris

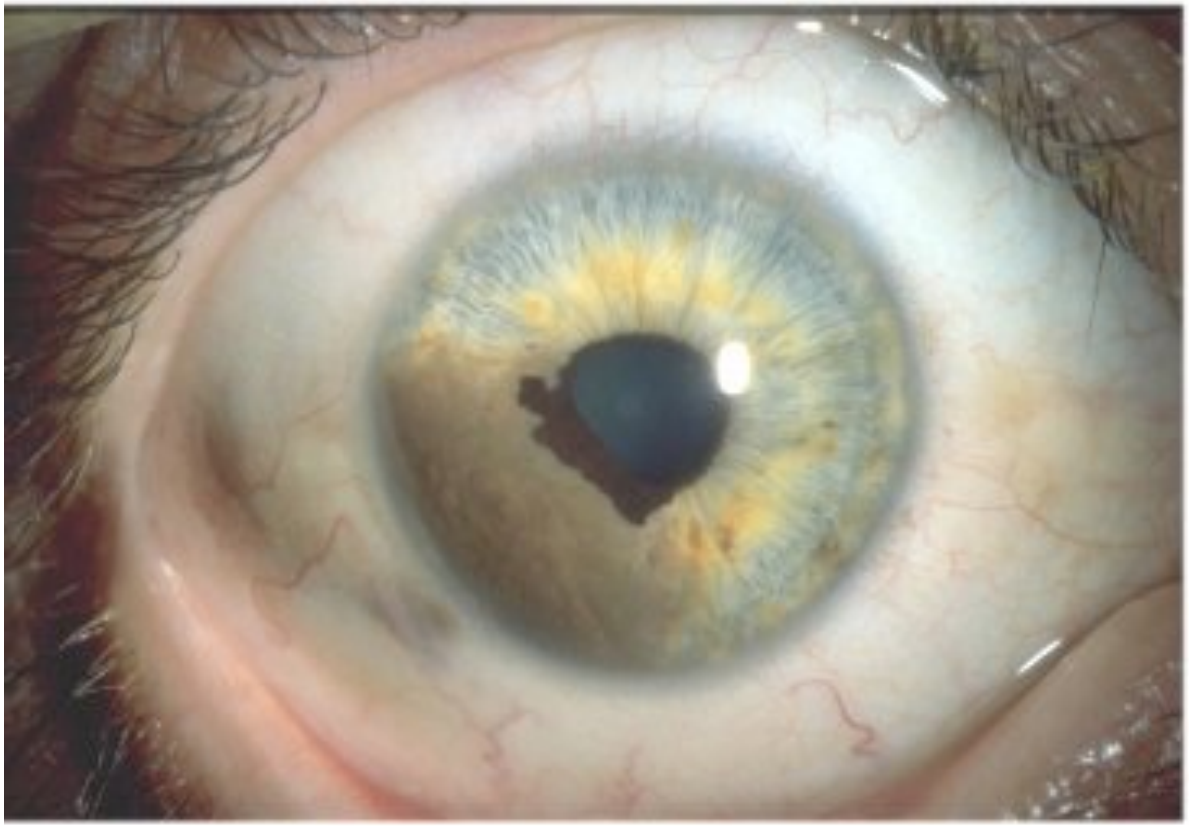
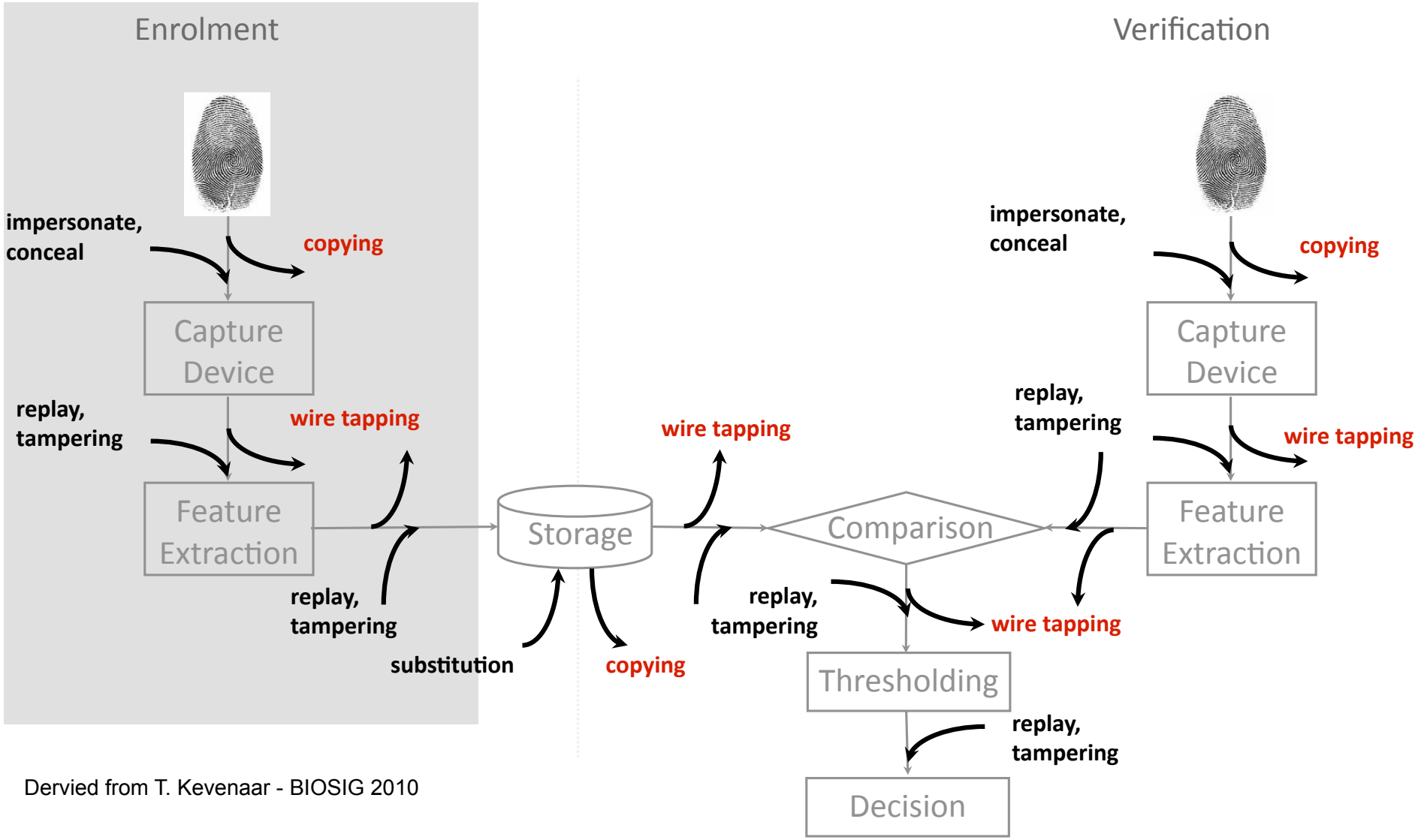


Image Source: Online Journal of Ophthalmology

Biometric Template Protection

Security versus Data Protection

Security and data leaking attacks



Dervied from T. Kevenaar - BIOSIG 2010

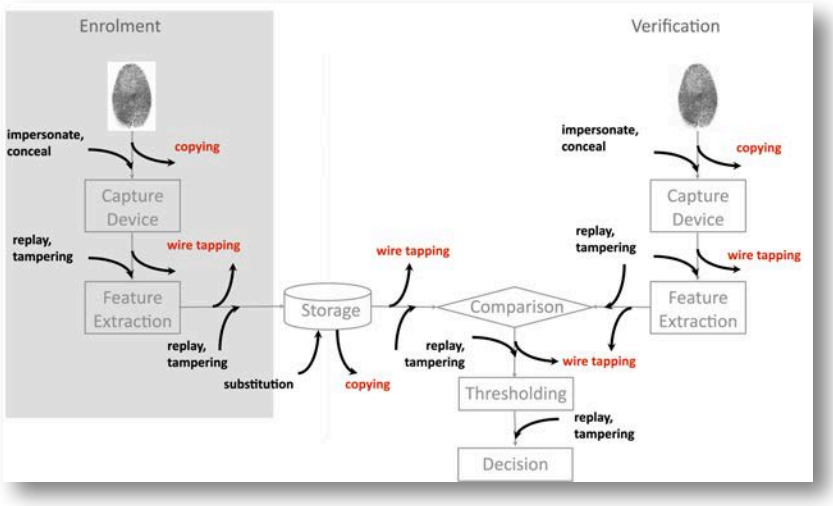
Security versus Data Protection

Protection goals

- Security (ingoing arrows) defines how difficult it is to illegitimately be accepted by the system.
- Data protection (outgoing arrows) is related to the difficulty to obtain any relevant information from a provided biometric characteristic other than a verification decision.

Protect the data storage

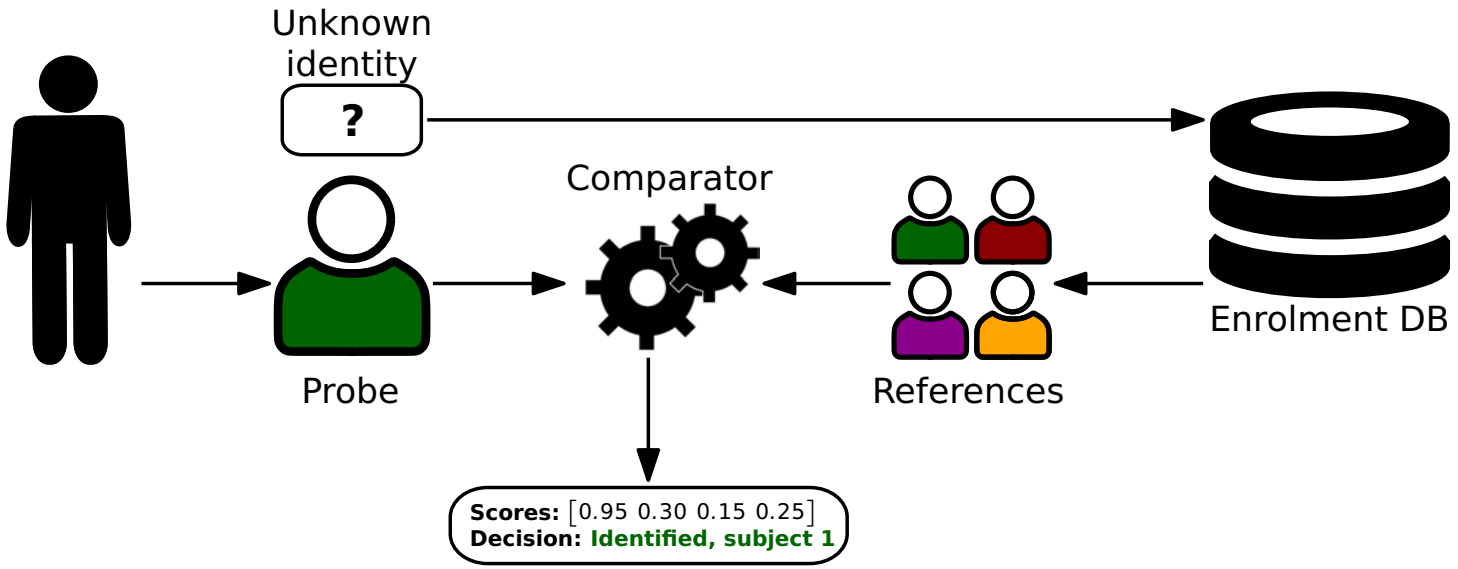
- Database modification
  - Impersonation attack
- Leakage attack
  - Need for template protection



Secure Data Storage

Two architectures to investigate

- Personal Card (RFID)
  - Store on Card
  - on Card Comparison
  - Sensor on Card
- Central databases
  - Identification systems



Secure Data Storage?

An incident: https://www.opm.gov/news/releases/2015/09/cyber-statement-923/

OPM.gov Main > News > Latest News > News Archives > Releases > 2015 > September > Cyber Statement 9.23

Statement

FOR IMMEDIATE RELEASE
Wednesday, September 23, 2015

Contact: Office of Communications
Tel: (202) 606-2402

Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident

As part of the government's ongoing work to notify individuals affected by the theft of background investigation records, the Office of Personnel Management and the Department of Defense have been analyzing impacted data to verify its quality and completeness. During that process, OPM and DoD identified archived records containing additional fingerprint data not previously analyzed. Of the 21.5 million individuals whose Social Security Numbers and other sensitive information were impacted by the breach, the subset of individuals whose fingerprints have been stolen has increased from a total of approximately 1.1 million to approximately 5.6 million. This does not increase the overall estimate of 21.5 million individuals impacted by the incident. An interagency team will continue to analyze and refine the data as it prepares to mail notification letters to impacted individuals.

Secure Data Storage?

An incident - function creep:

https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans

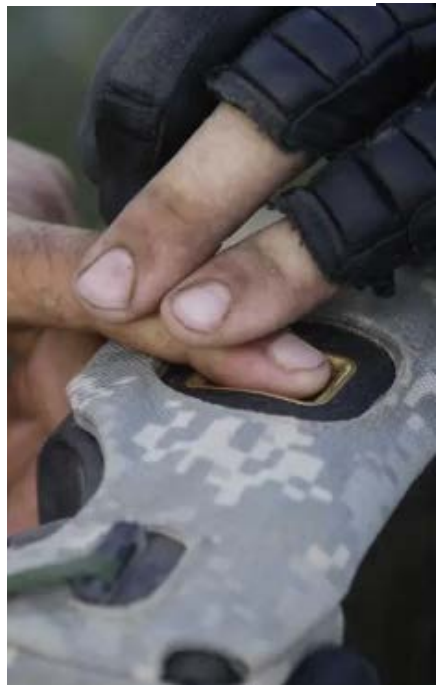
March 30, 2022 1:30AM EDT

New Evidence that Biometric Data Systems Imperil Afghans

The Taliban control systems holding sensitive biometric data that Western donor governments left behind in Afghanistan in August 2021, putting thousands of Afghans at risk, Human Rights Watch said today.

These digital identity and payroll systems contain Afghans' personal and biometric data, including iris scans, fingerprints, photographs, occupation, home addresses, and names of relatives. The Taliban could use them to target perceived opponents, and Human Rights Watch research suggests that they may have already used the data in some cases.

"Governments and organizations that helped amass vast quantities of personal data on large numbers of Afghans may be inadvertently assisting the Taliban repression," said Belkis Wille, senior crisis and conflict researcher at Human Rights Watch. "Data collection's highly intrusive nature and inadequate protections could put people at heightened risk of Taliban abuse."



Sample Reconstruction

Biometric inversion attacks are an underestimated risk

- It was a common belief that the stored templates reveal no information about the biometric characteristics

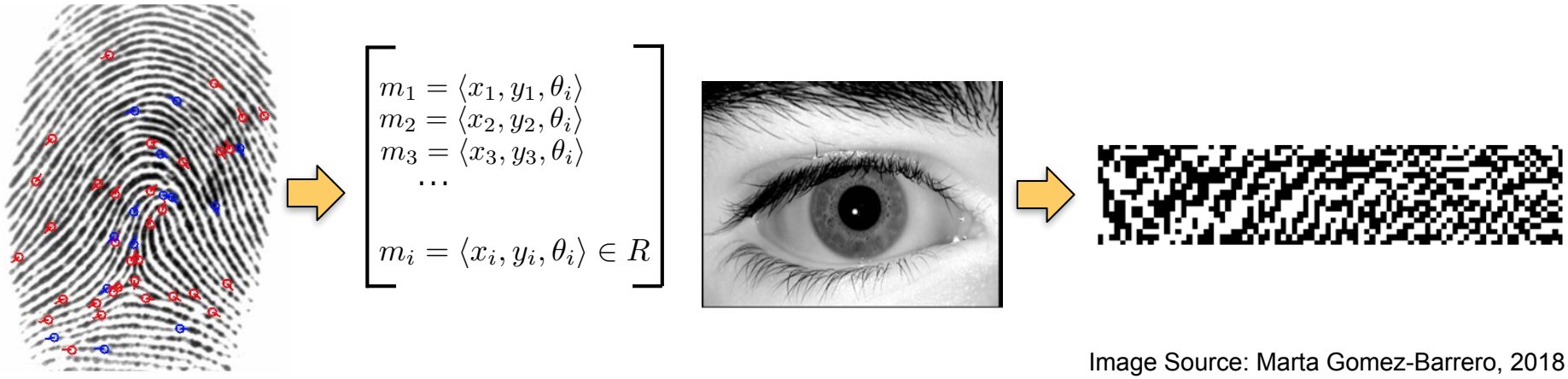


Image Source: Marta Gomez-Barrero, 2018

- Vendor's statement (some years back):
  "Our product is secure since it does store fingerprint minutiae and not fingerprint-image"
- However, biometric samples can be recovered from the stored unprotected templates

Sample Reconstruction

Biometric inversion attacks on minutia templates

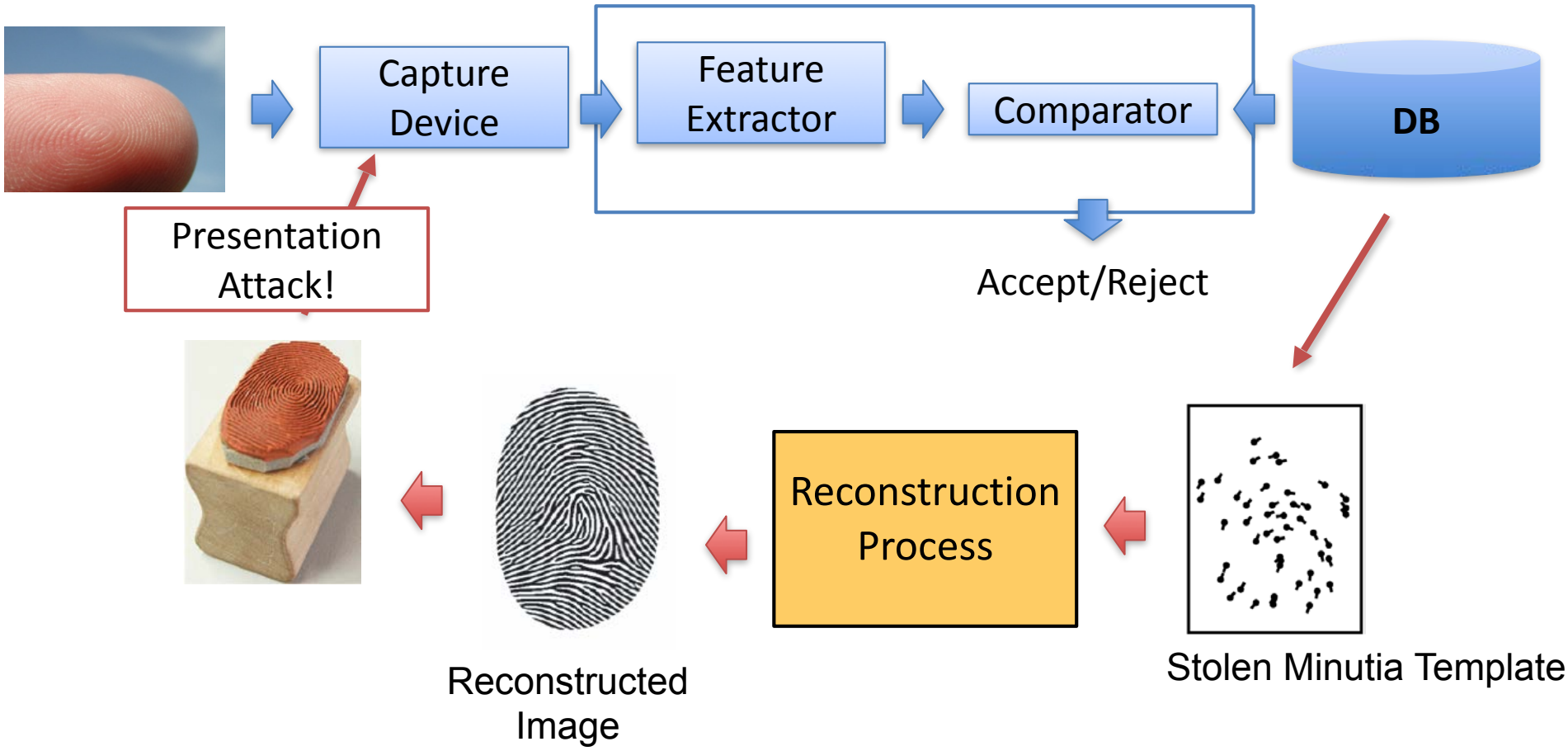


Image Source: Marta Gomez-Barrero, 2018

[Cappelli2007] R. Cappelli et al. „Fingerprint Image Reconstruction from Standard Templates“, in IEEE PAMI, (2007)

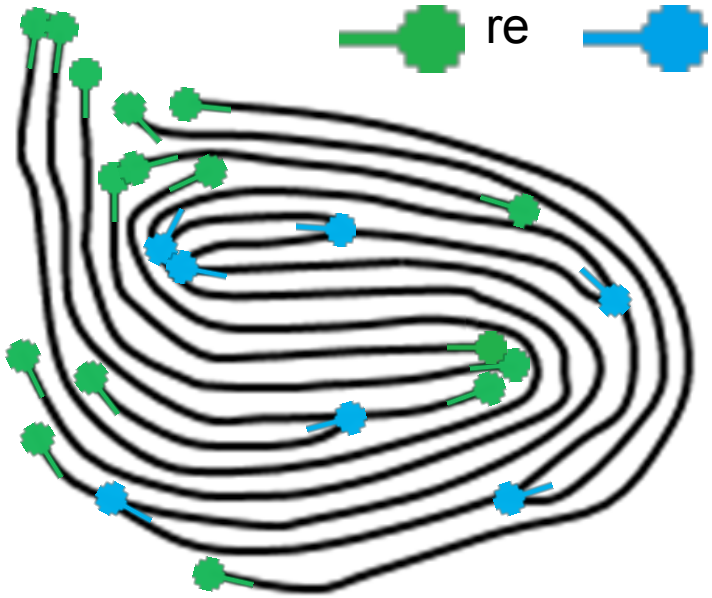
[Galbally2009] J. Galbally et al. „Template Reconstruction“, in Pattern Recognition Letters, (2009)

Sample Reconstruction

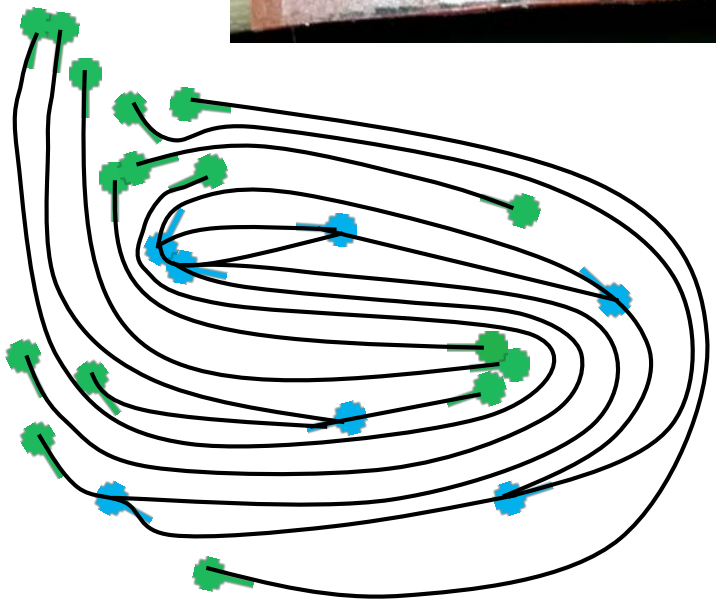
Processing the attack

We invert from fingerprint-minutia to a sample that will grant access!

Sample reconstruction!



original sample

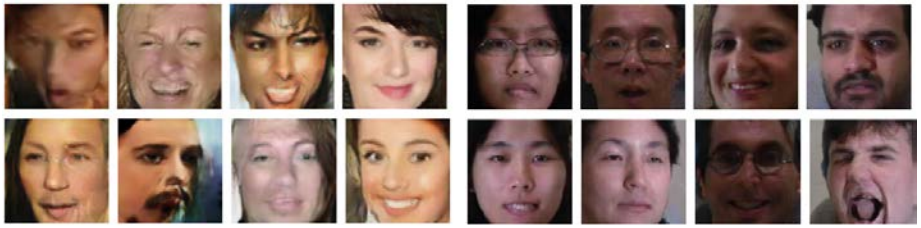


reconstructed sample

Sample Reconstruction

Early approaches for face image reconstruction:

- A neighbourly de-convolutional network can be used to reconstruct facial templates from FaceNet [Schroff2015]
- Over large open access databases, success rates over 73% and 95% are achieved [Mai2018]



Nowadays reconstruction of face images from latent space is state of the art [Kabb2022]

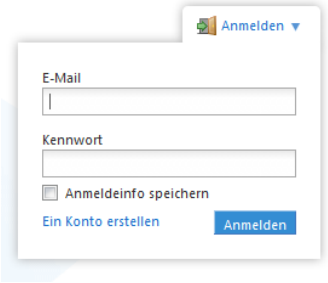
original image

reconstructed image

[Schroff2015] Schroff et al. „FaceNet: A Unified Embedding for Face Recognition and Clustering“, in CVPR, (2015)
[Mai2019] Mai et al. „On the Reconstruction of Face Images from Deep Face Templates“, in IEEE T-PAMI, (2019)
[Kabb2022] Kabbani et al. „EGAIN: Extended GAN Inversion Architecture“, (2022)

Biometric Template Protection (BTP)

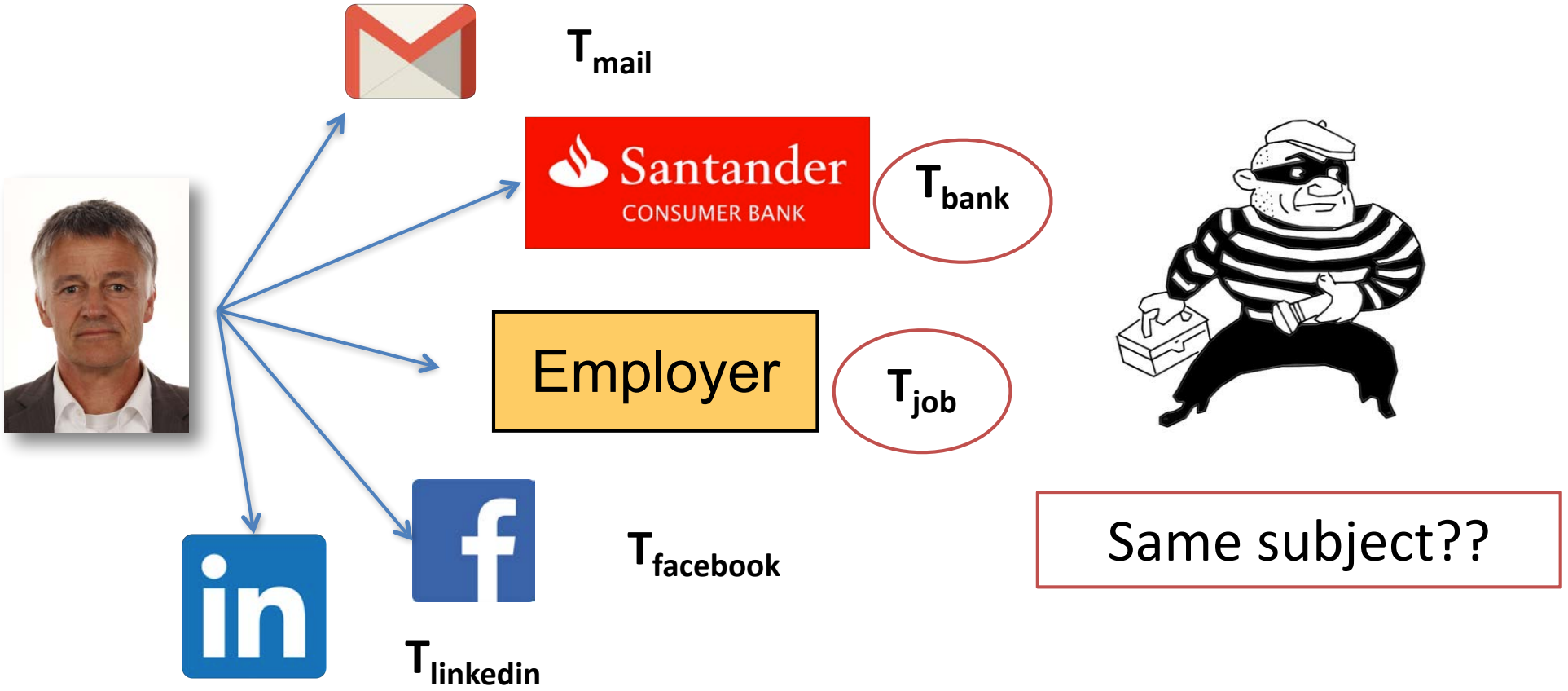
Benchmark of Authentication Methods

	Non-Invertibility from the reference	Revocability and Renewability	Strong link to the data subject
	✓ (?)	✓	✗
	✓	✓	✗
	✗	✗	✓

Further Risks for Biometric References

Cross-Comparison attacks

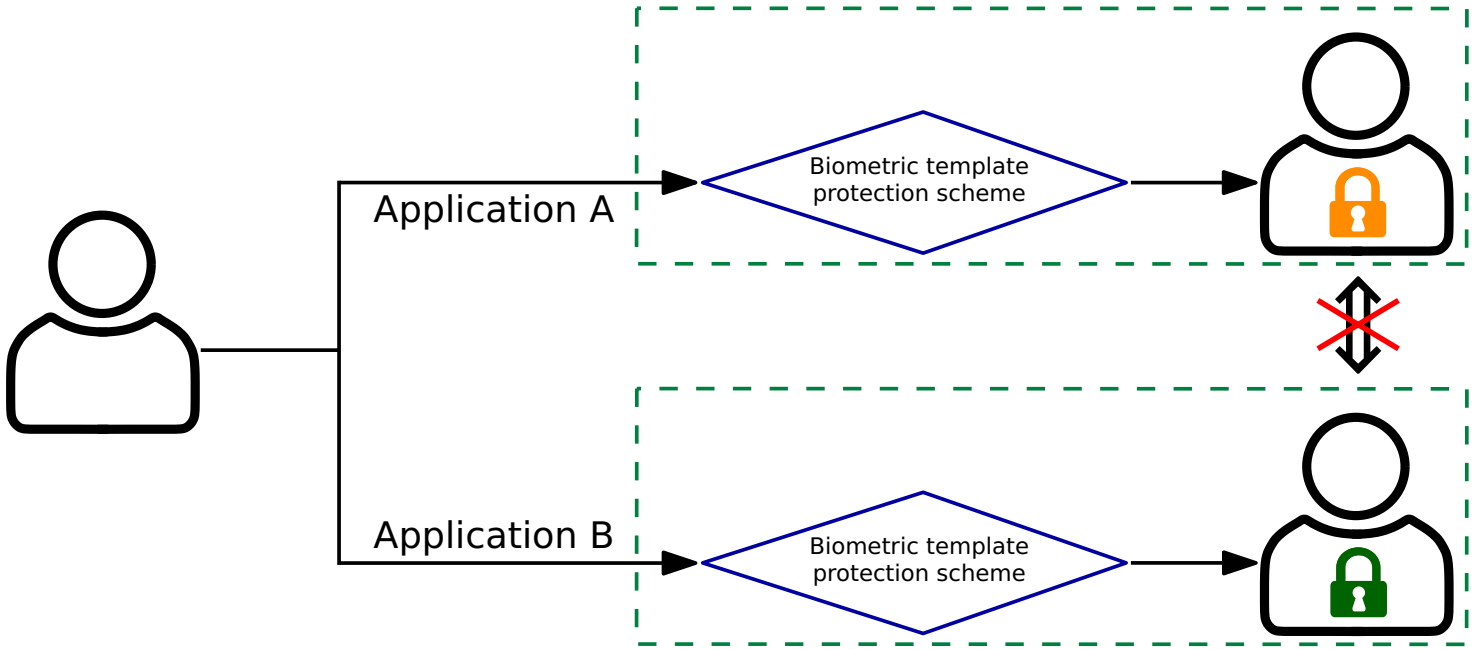
- We want to enrol with a single biometric characteristic in different applications



Further Risks for Biometric References

Cross-Comparison attacks

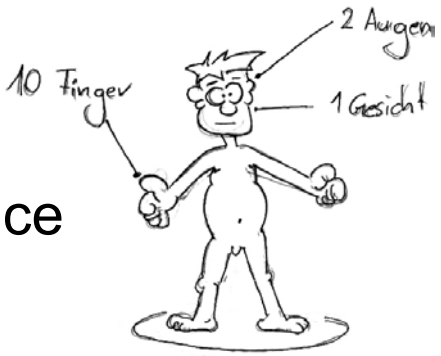
- Enrol with a single biometric characteristic in different applications
- Prevent the generation of profiles
  - Cross-correlating protected templates across different systems and databases must not be possible to avoid profiling



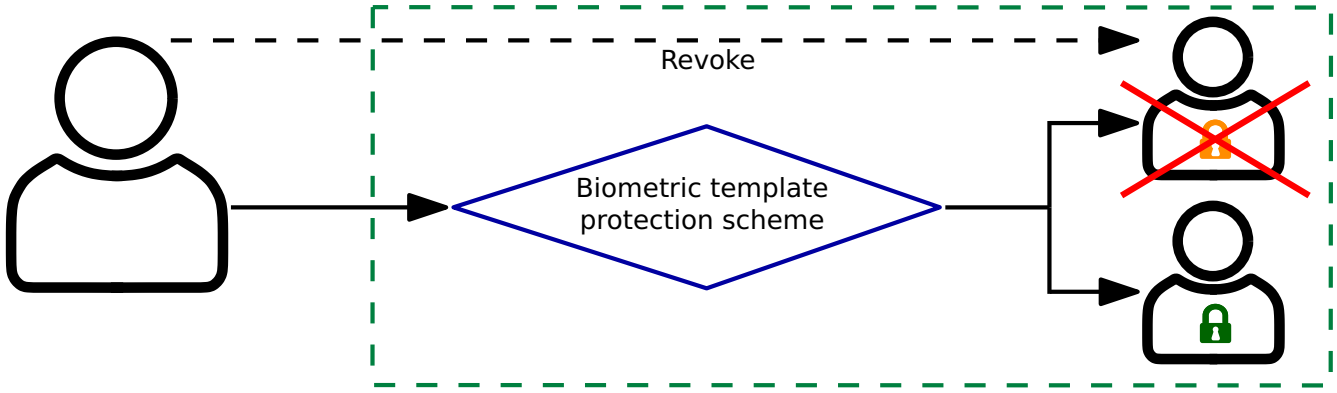
Further Risks for Biometric References

Leaking attacks against the reference data

- The biometric characteristic as such can not be revoked
  - only 10 finger, 2 eyes, 1 face, ...
  - in case of being compromised, revoking and reissuing a new (different) protected biometric reference should be possible and straightforward.
  - for PW-based system you would expect renewal frequently (e.g. every 3 month)



We need renewability!



Risks for Biometric References

Summary: Possible attacks on reference data

- Cross-Comparison: Identical template can establish unwanted links for one individual between several databases
- Leaking references: The biometric characteristic can not be revoked
  - only 10 finger, 2 eyes, 1 face, ...
  - we need to revoke and renew the biometric reference
- Disclosing additional information
  - almost for each biometric characteristic

Normal flexion crease

Simian crease

Is encryption of biometric references a sufficient level of template protection?

Biometric Template Protection (BTP)

Encryption of the biometric reference?

Conventional cryptography yields two main drawbacks

- Shift of problem: the encrypted template will be secure only as long as the decryption key is unknown to the attacker.
- Decryption at authentication: the template needs to be decrypted during every verification attempt since comparison cannot be directly performed in the encrypted domain.
  - Adversary can observe the biometric template by simply launching a verification attempt!

Classical crypto / encryption does not solve the problem

Biometric Template Protection

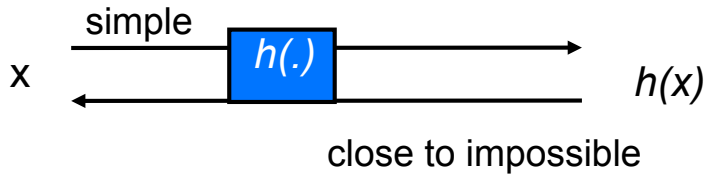
Hashing the reference?

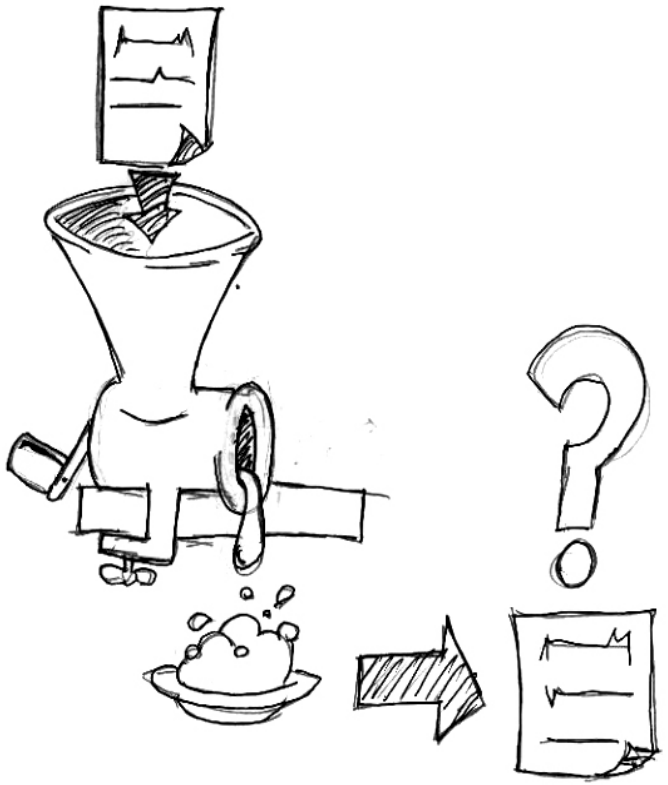
- Approach analog to UNIX Password authentication
- Public assessable file: /etc/passwd

```
id:<login_name>:hash(password)
```

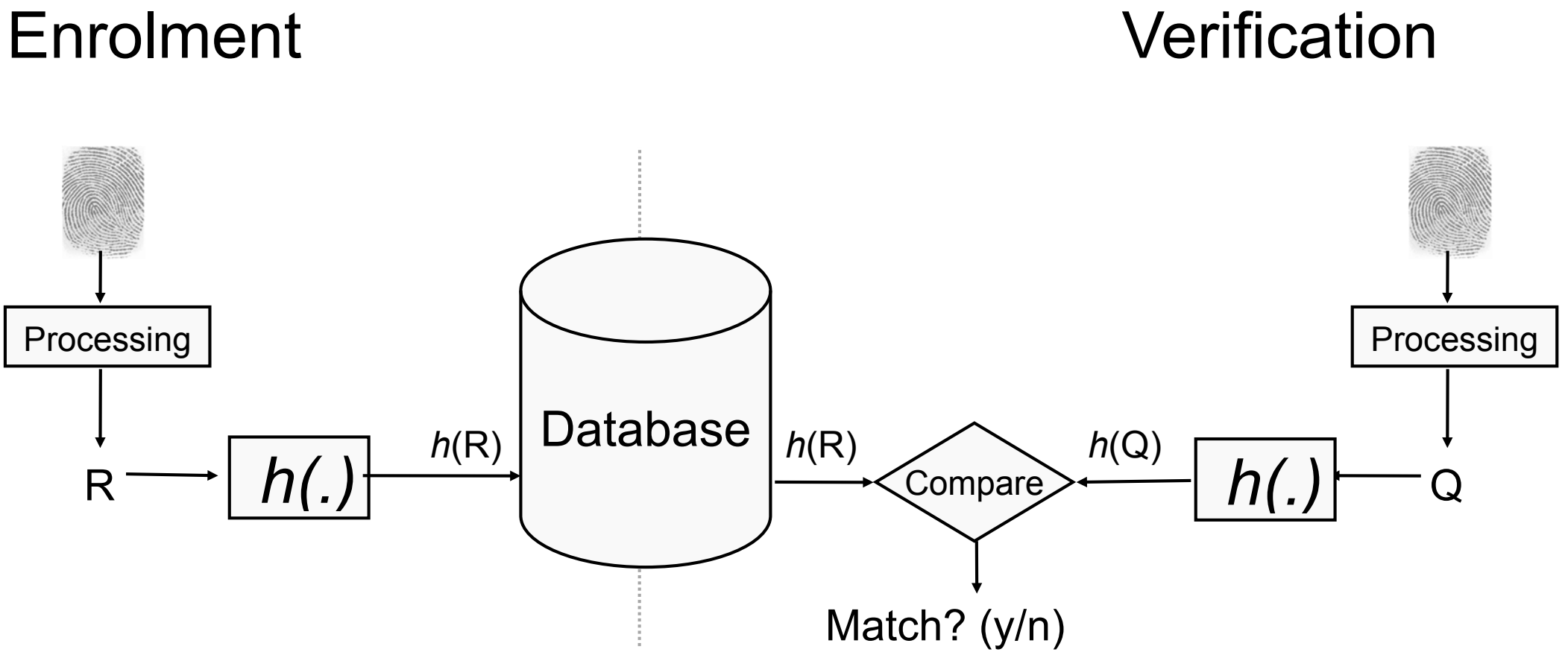
- Authentication:

```
hash(input) =?= hash(password)
```





Template Protection with Hash functions



h(.) = one-way hash function

Challenges

Difference between passwords and biometric samples

`h(01000101)` is not similar to `h(01010101)`

- Biometric measurements are influenced by noise
- Cryptographic one way functions are (by purpose) extremely sensitive to small changes in the input data

Classical crypto hashing does not solve the problem either

Biometric Template Protection

Preliminary conclusion

- We do NOT store fingerprint, iris or face images
- We do NOT store fingerprint, iris or face templates

But

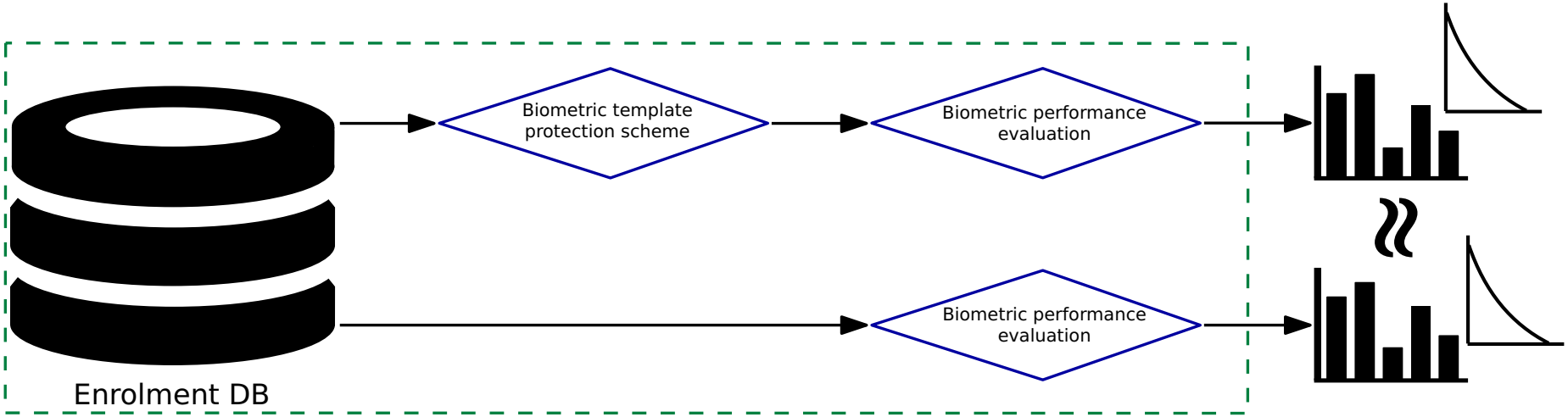
- We transform templates to pseudonymous identifiers (PI)
- We reach renewable biometric references (RBR)
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversification in space: unlinkability: unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Diversification in time: renewability: we can revoke and renew the reference data.
  - Non-invertibility: original biometric sample can **not** be reconstructed

[Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)

Biometric Template Protection

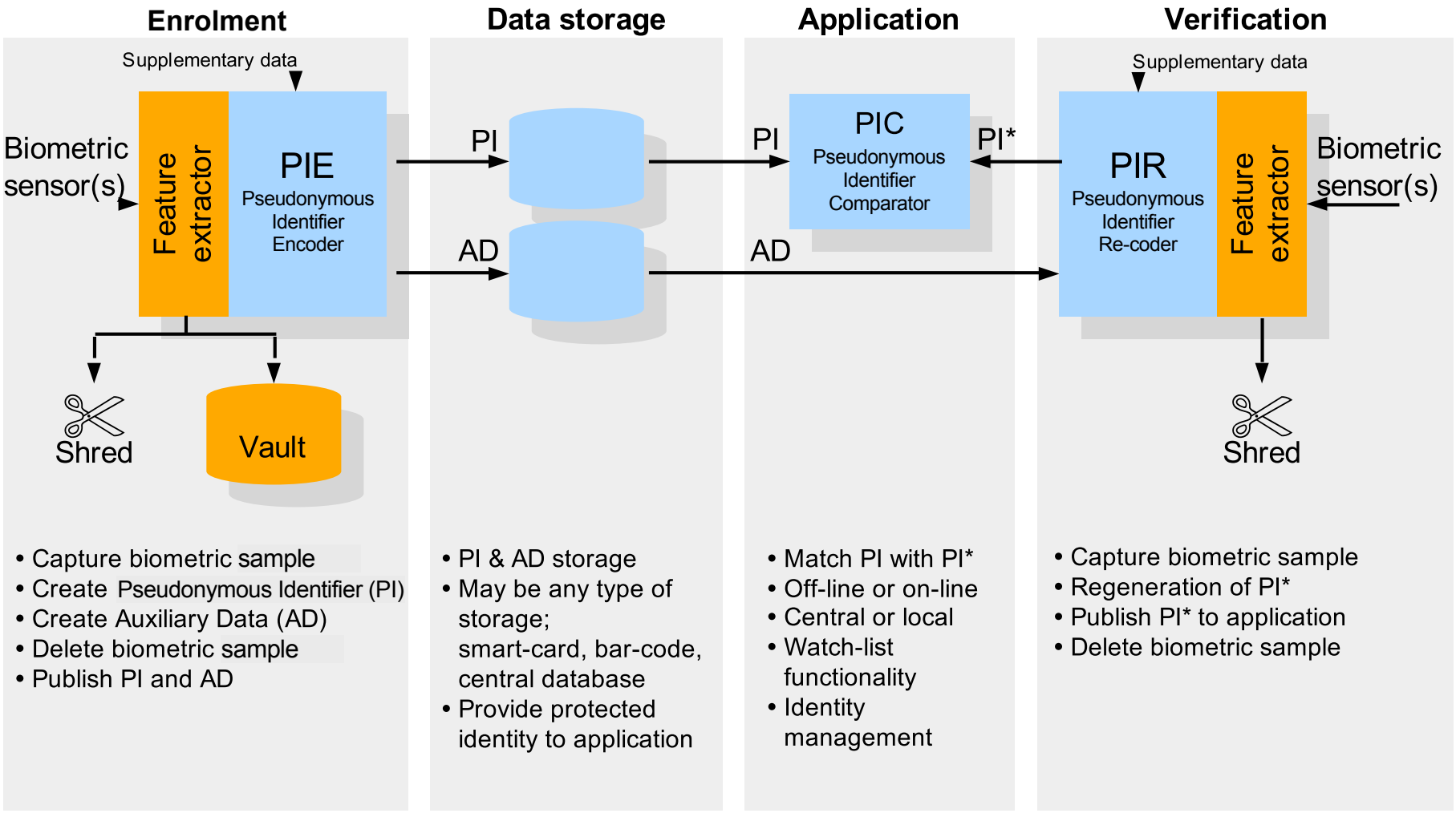
Expectation

- The biometric performance of the protected system must not be (severely) impaired by the template protection scheme.



Framework in ISO/IEC 24745

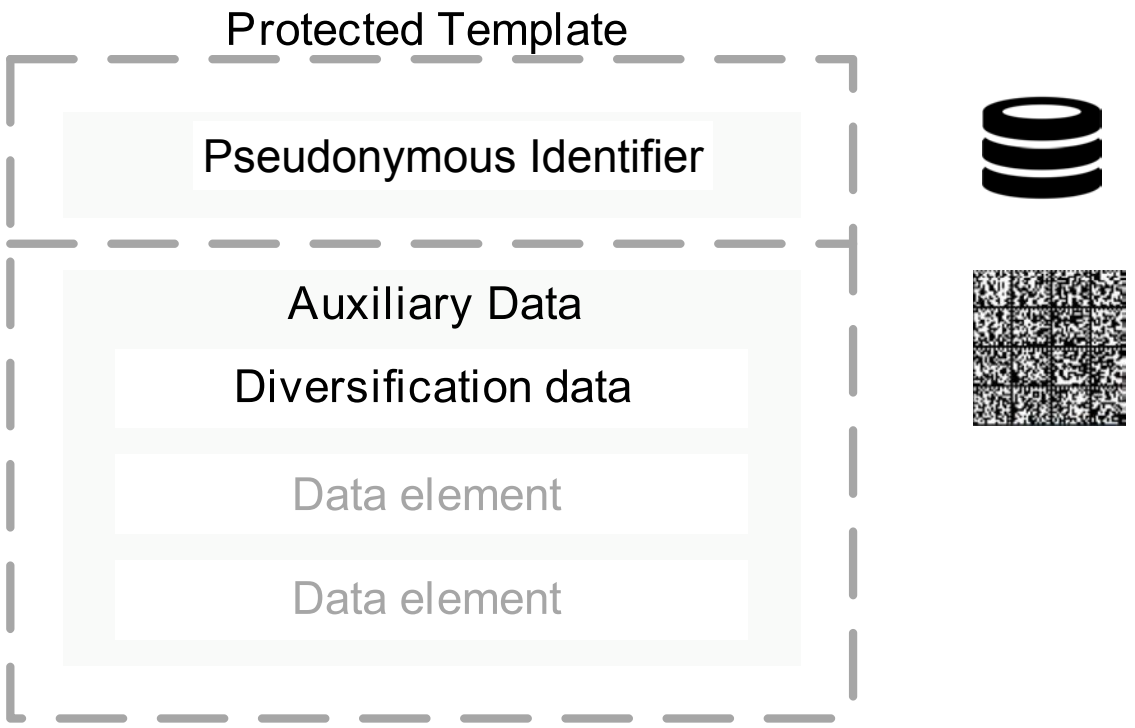
- Standardized architecture for renewable biometric references



Protected Template Structure

Resulting Protected Template

- Consists of two parts
  - Pseudonymous Identifier
  - Auxiliary Data
- Bi-lateral security
  - Capture subject
  - Service operator
- Balance of revocation power



Survey of BTP Algorithms

BTP approaches: Cancelable biometrics

- Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the protected domain.
- Two types:
  - Non-reversible transformations
    of the biometric data or unprotected templates.
  - Biometric salting, in which Auxiliary Data (AD)
    is blended with biometric data to derive a distorted version
    of the biometric template.

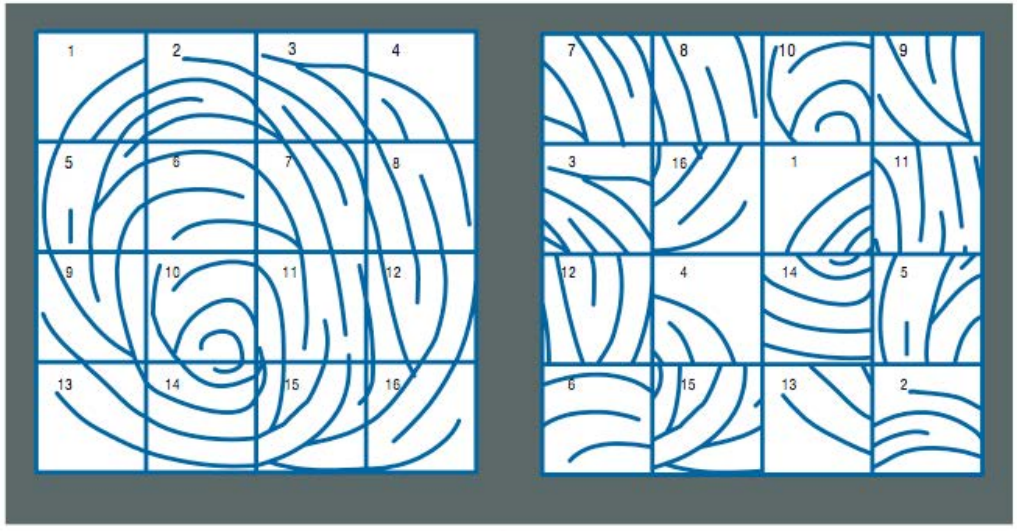
Cancelable Biometrics

Transformation of a signal prior to feature extraction

- Grid morphing

  [Ratha2001]

Block permutation

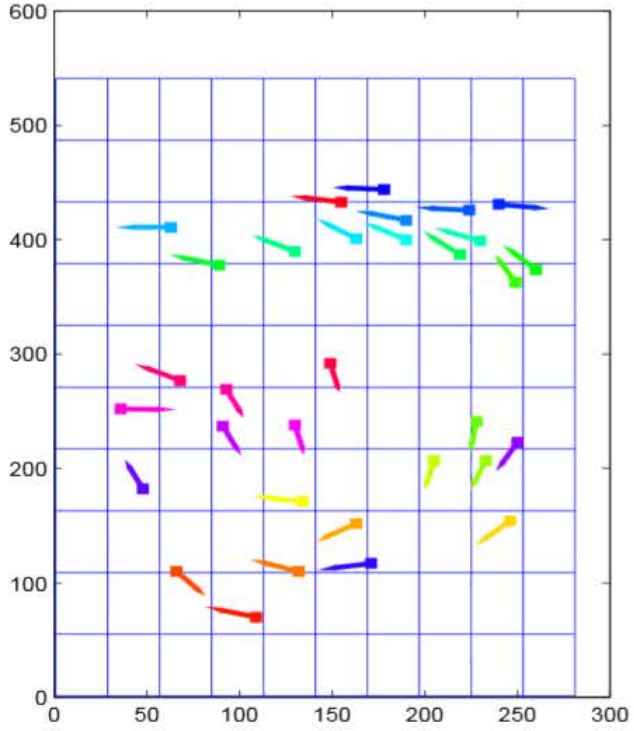


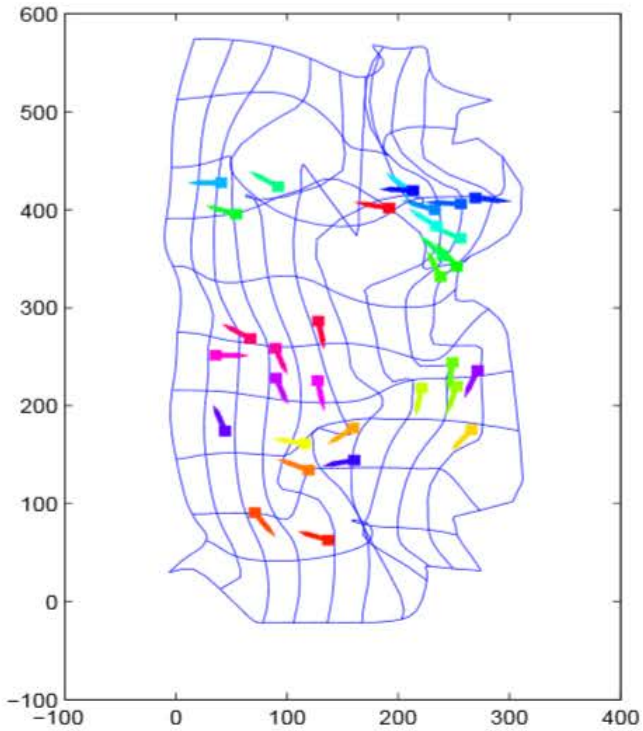
Cancelable Biometrics

Transformation of a signal prior to feature extraction

- Non-invertible transformation based algorithm: Cancelable biometrics [Ratha2007]

X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

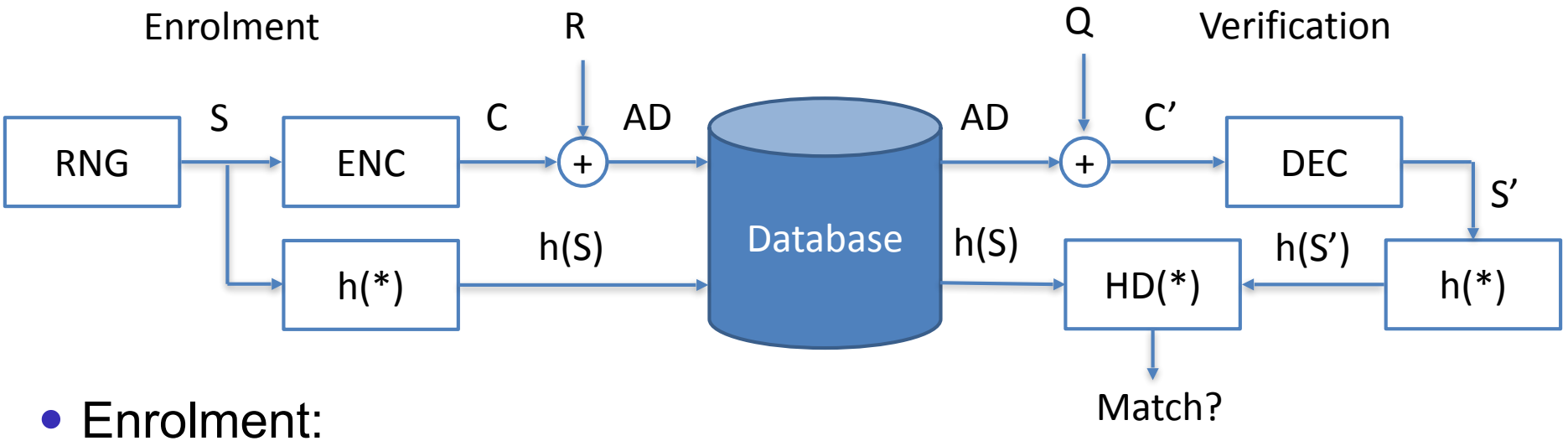




Non-invertibility introduced by “folding” operations

Cryptobiometrics - Fuzzy Commitment

- Hashed secret can ECC code words [Jules1999]



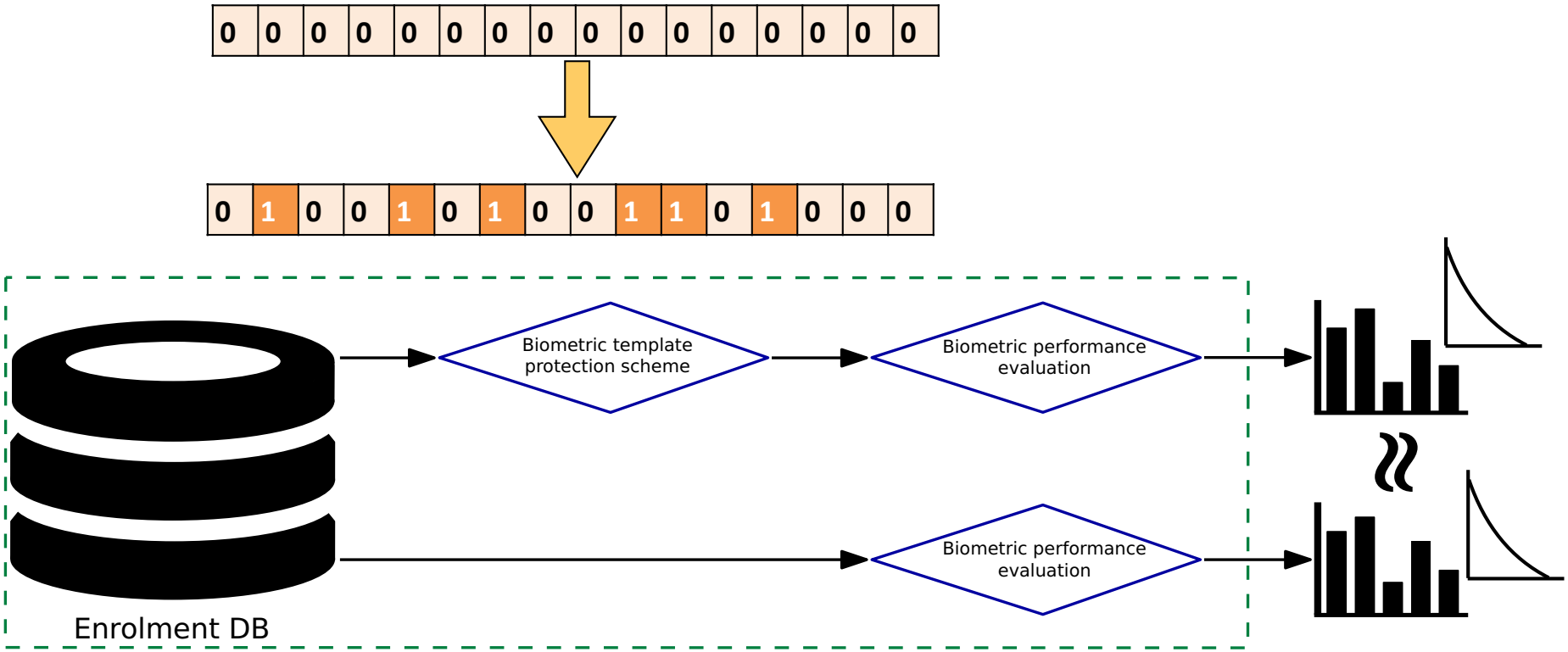
- Enrolment:
  - C is the codeword generated for the random string S
  - R is the binary extract of the reference vector
  - AD = C XOR R is the public AD
  - {h(S), AD} are stored as reference
- Verification:
  - C' = AD XOR Q (query vector)
  - HD(C, C') needs to be smaller than the error correction capabilities

[Juels1999] A. Jules and M. Wattenberg: „A Fuzzy Commitment Scheme“, in ACM CCS, (1999)

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers



[Ra2014] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: „On the Application of Bloom Filters to Iris Biometrics“, in IET Journal on Biometrics 3(1), (2014)
http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Bloom filters

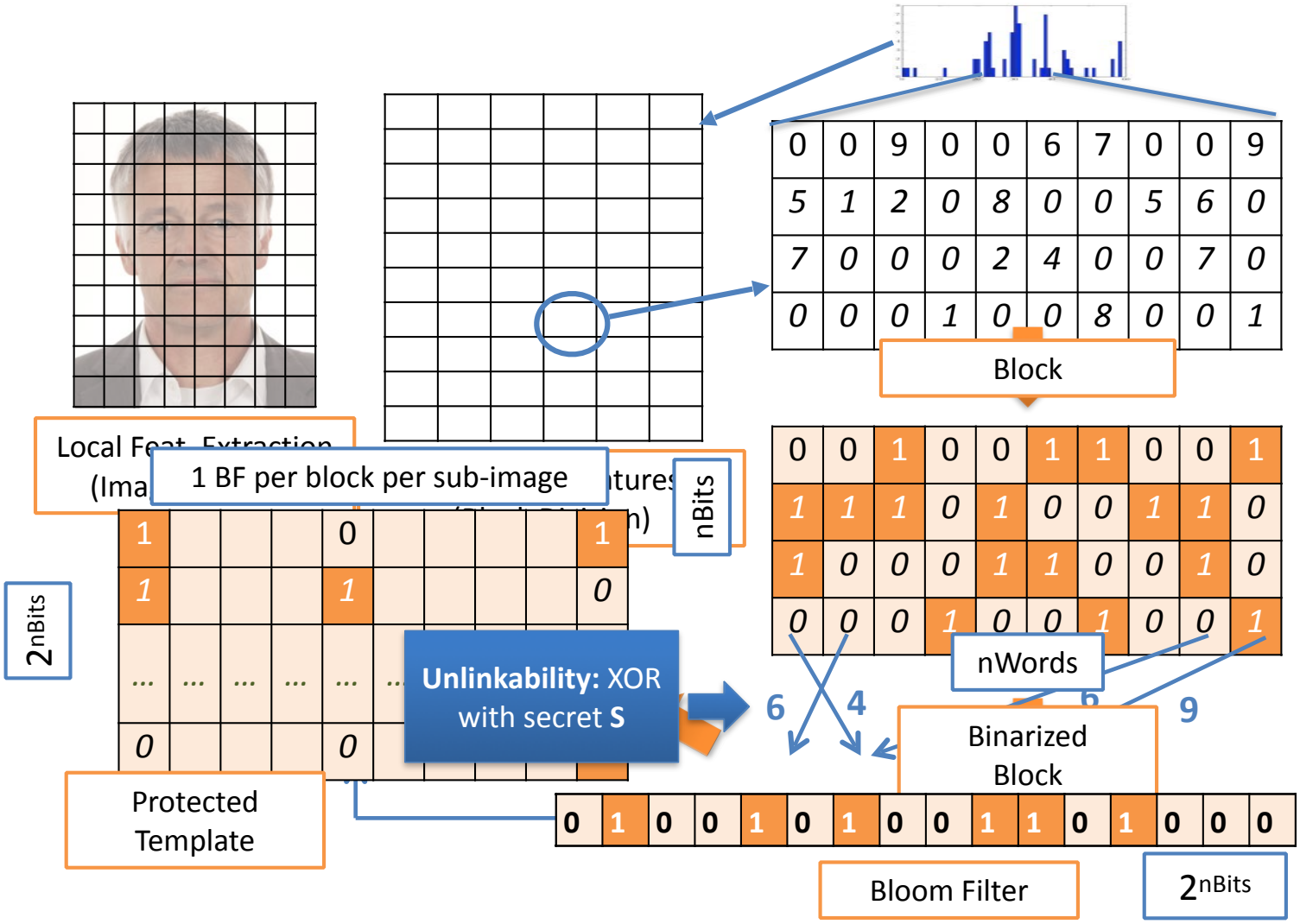
- A Bloom filter b is a space-efficient data structure representing a set S to support membership queries
  - b is a simple bit array of length n (initially all bits are set to 0)
- To represent $S = \{x_1, x_2, \ldots, x_m\}$, k independent hash functions $h_1, h_2, \ldots, h_k$ with range $[0, n-1]$ are utilized
  - For each element $x \in S$, bits $h_i(x)$ of b are set to 1, for $1 \leq i \leq k$
- Indices can be set to 1 multiple times (but only the first change has an effect!)
- Let $|b|$ denote the amount of bits within a Bloom filter b, which are set to 1. Then the dissimilarity score DS between two Bloom filters b_i and b_j is defined as

$$DS(b_i, b_j) = \frac{HD(b_i, b_j)}{|b_i \cup b_j|}$$

Bloom Filter Biometric Template Protection

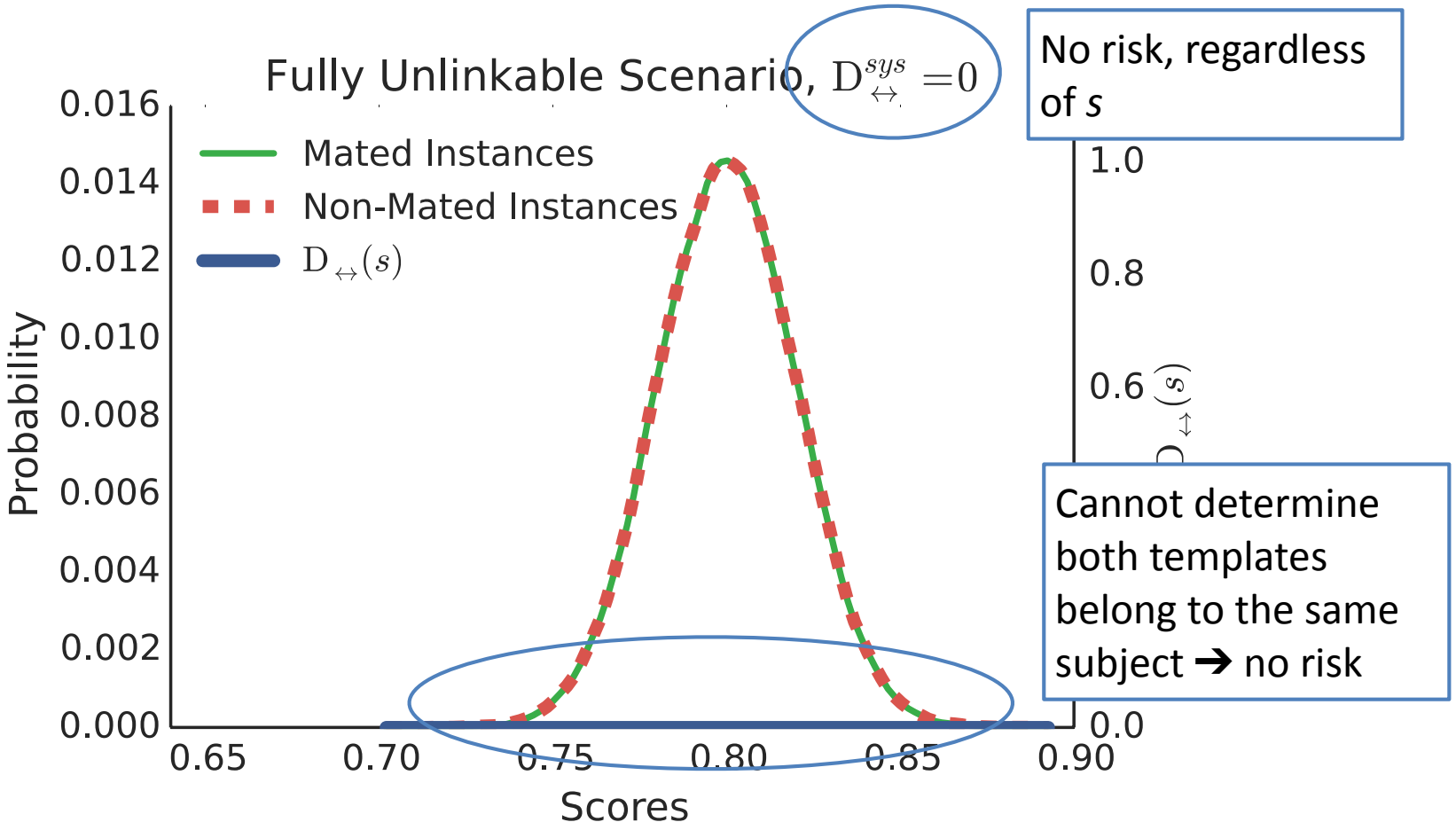
Protection at the same accuracy level is possible

- Generating bloom filter-based pseudonymous identifiers



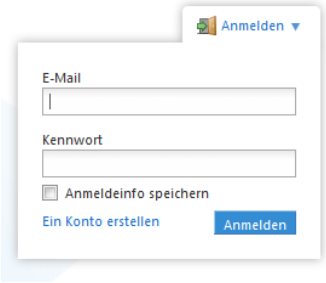
BTP Unlinkability Evaluation

Full Unlinkability



[Gomez2018] M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch: "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems", in IEEE Transactions on Information Forensics and Security (TIFS), (2018)

Revised Benchmark of Authentication

	Non-Invertibility from the reference	Revocability and Renewability	Strong link to the data subject
	✓	✓	✗
	✓	✓	✗
	✓	✓	✓

BTP Approaches

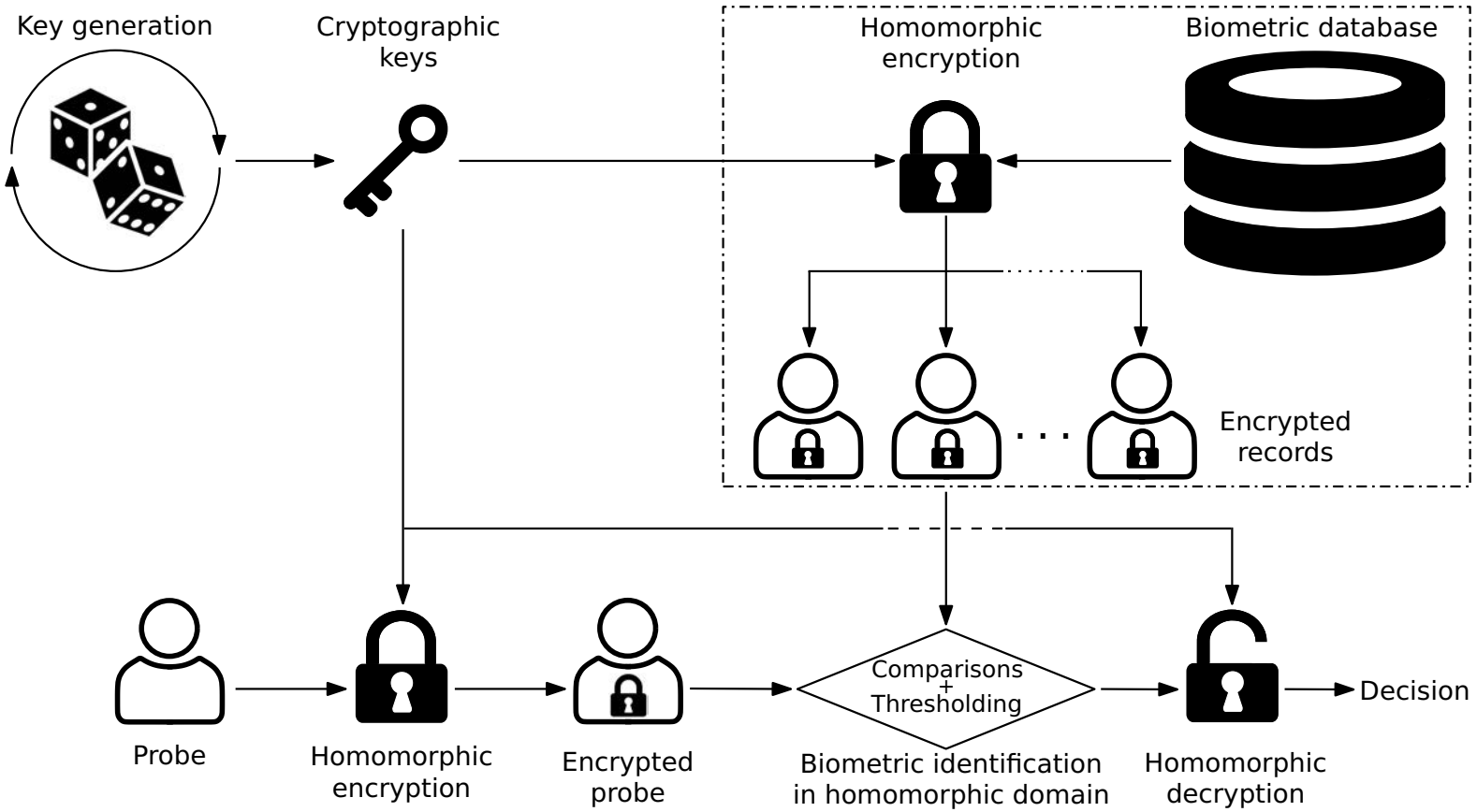
Biometrics in the Encrypted Domain

- Homomorphic Encryption (HE) schemes allow for computations to be performed on ciphertexts,
  - with no additional AD,
  - and which generate encrypted results
  - which decrypt to plaintexts
  - that match the result of the operations carried out on the original plaintext
- This solves the issue of decryption before authentication...

BTP Approaches

Biometrics in the Encrypted Domain

- Homomorphic Encryption (HE) schemes allow for computations to be performed on ciphertexts



BTP Approaches

Biometrics in the Encrypted Domain

- Partially Homomorphic Encryption (PHE) schemes
  - Are defined as allowing only a single operation type an unlimited number of times.
  - PHE schemes have been around for over 30 years supporting only either addition or multiplication.
- Somewhat Homomorphic Encryption(SHE) schemes
  - Allow multiple operation types, but only a limited number of times.
- Fully Homomorphic Encryption (FHE) schemes
  - Support an unlimited number of operations.

BTP Approaches

Homomorphic Encryption

- Assymmetric Cryptosystem (pk/sk)
- Post-quantum secure
- Homomorphic Properties:

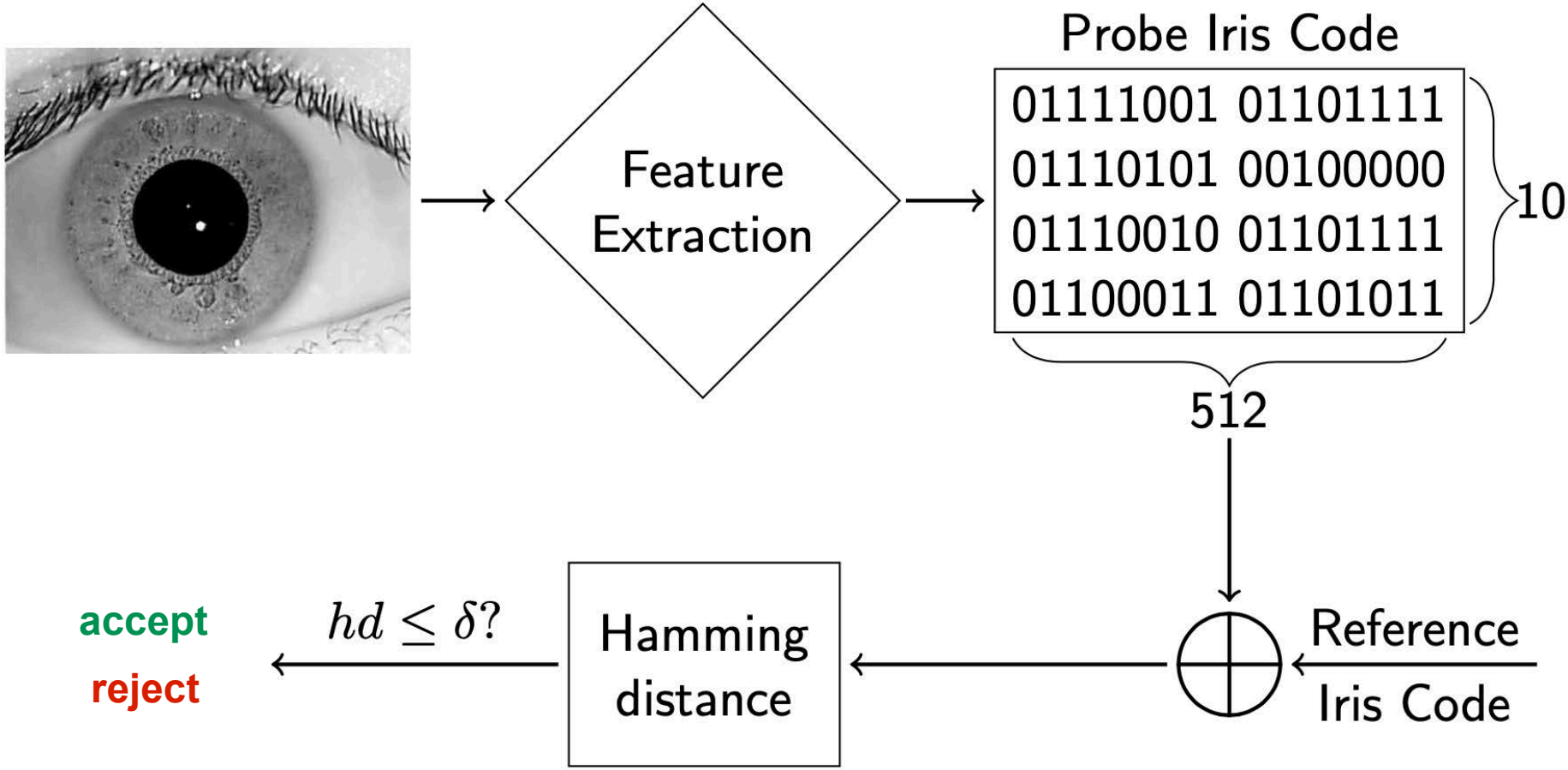
$$\mathsf{Enc}_{pk}(A) + \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A + B)$$
$$\mathsf{Enc}_{pk}(A) \cdot \mathsf{Enc}_{pk}(B) = \mathsf{Enc}_{pk}(A \cdot B)$$

[Kolb2019] J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE WIFS, Delft, NL, (2019)
[Dro2019] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, (2019)

BTP Approaches

Homomorphic Encryption

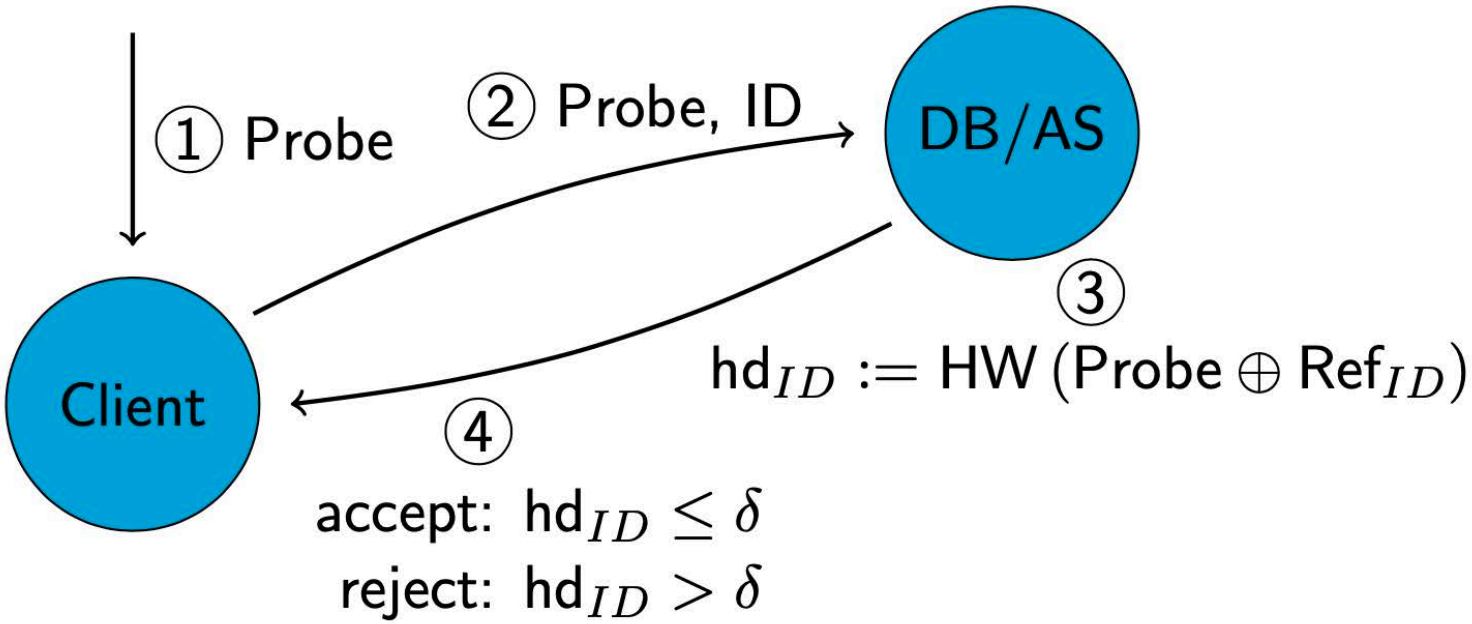
- Example: Iris Recognition
  - unprotected system



BTP Approaches

Homomorphic Encryption

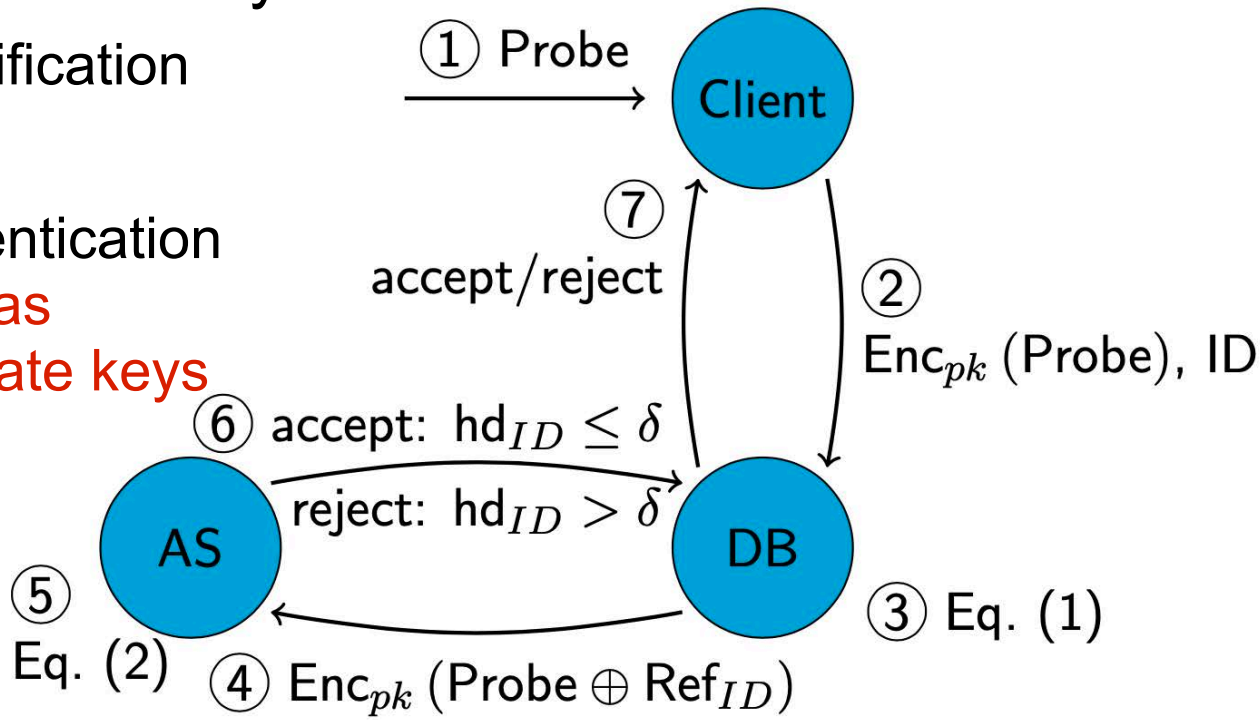
- Example: Iris Recognition
  - unprotected verification



BTP Approaches

Biometrics in the Encrypted Domain

- A protected biometric system
  - NTRU HE verification
  - additive HE
  - only the Authentication Server (AS) has access to private keys



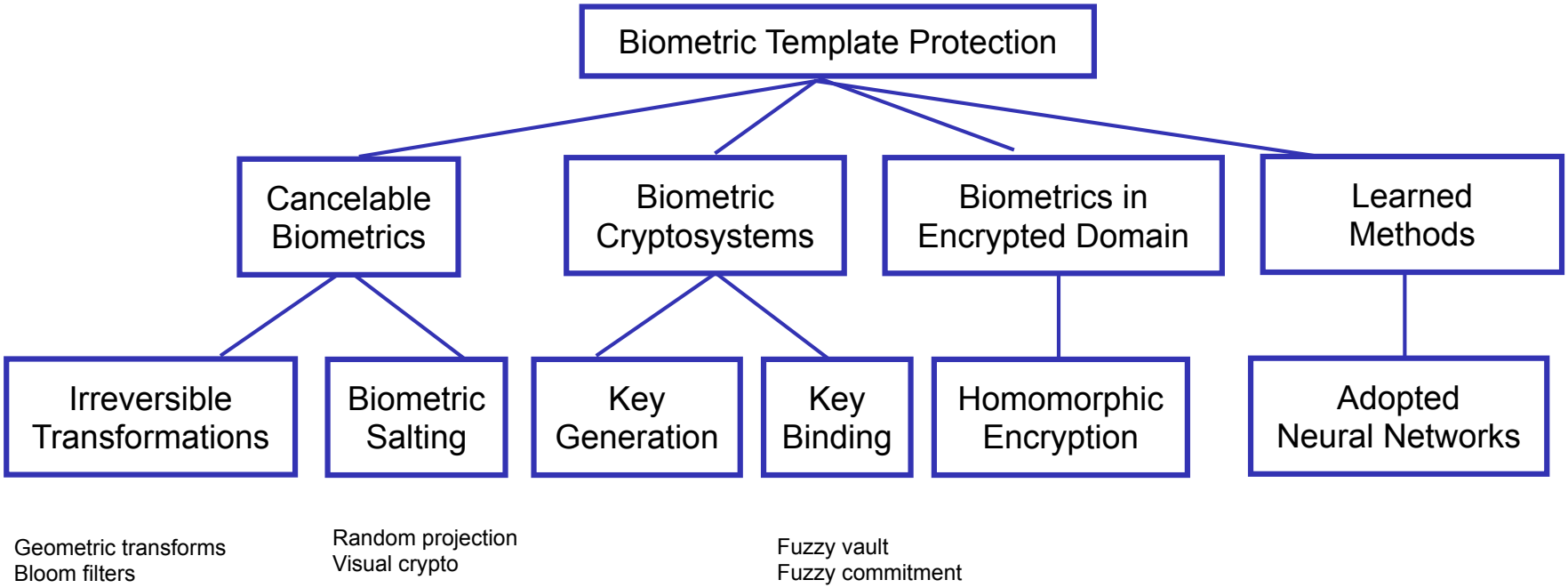
$$\text{Enc}_{pk}(\text{Probe} \oplus \text{Ref}_{ID}) := \text{Enc}_{pk}(\text{Probe}) \oplus \text{Enc}_{pk}(\text{Ref}_{ID}) \quad (1)$$

$$\text{hd}_{ID} := \text{HW}(\text{Dec}_{sk}(\text{Enc}_{pk}(\text{Probe} \oplus \text{Ref}_{ID}))) \quad (2)$$

[NTRU1998] J. Hoffstein, J. Pipher, J. Silverman: NTRU: A Ring-Based Public Key Cryptosystem, in Int. Algorithmic Number Theory Symposium. Springer, (1998)

Overview

BTP approaches: summary



Conclusion

Integration of privacy and security is technically possible

- Biometric data is sensitive data, which needs to be protected, providing irreversibility, unlinkability, renewability and accuracy preservation.
- Unprotected templates can be reconstructed using inverse biometrics methods, where only access to similarity scores is required.
- Privacy Enhancing Technology (PET) will increase the likelihood that individuals will effectively consent in using the biometric system
- Cross-comparison-resistant renewable biometric references prevent from tracking without consent in case biometric databases are compromised

References

Web

- General Data Protection Regulation (GDPR)
  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- European Convention on Human Rights (ECHR)
  http://www.echr.coe.int/Documents/Convention_ENG.pdf
- European Convention 108
  http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- Ann Cavoukian: „Privacy by Design“;
  https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

Complementary reading

- M. Meints et al.: „Biometric Systems and Data Protection Legislation in Germany“, 2008
- ISO/IEC 24714-1: „Guide to the accessibility, privacy and health and safety issues in the deployment of biometric systems for commercial application”

References

Publications

- N.K. Ratha, J.H. Cornell, R.M. Bolle: „Enhancing security and privacy in biometrics-based authentication systems“, (2001)
- M. Veen, T. Kevenaar, G.J. Schrijen, T.H. Akkermans. F. Zuo "Face Biometrics with Renewable Templates", SPIE Conference Multimedia and Security, (2006)
- C. Rathgeb, A. Uhl: „A survey on biometric cryptosystems and cancelable biometrics“, Springer, (2011)
- C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014)
- M. Gomez-Barrero, C.Rathgeb, J. Galbally, J. Fierrez, C. Busch: „Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters“, in Proceedings ICPR, Stockholm, Sweden, (2014)
- G. Li, B. Yang, C. Rathgeb, C. Busch: "Towards Generating Protected Fingerprint Templates based on Bloom Filters", in Proceedings IWBF, Gjøvik, Norway, (2015)
- M. Gomez-Barrero, et al: "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters“, in Journal Information Sciences, (2016)
- M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch: "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems“, in IEEE Transactions on Information Forensics and Security (TIFS), (2018)

References

Standard

- ISO/IEC 24745:2022, Security techniques – Biometric information protection, (2022)
- ISO/IEC 30106:2018 Performance testing of biometric template protection schemes, in revision

Publications HE

- J. Kolberg, et al.: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE WIFS, Delft, NL, (2019)
- P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, (2019)
- M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez: Multi-Biometric Template Protection Based on Homomorphic Encryption. Pattern Recognition, (2017)

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
Schoefferstr. 3
64295 Darmstadt, Germany
christoph.busch@h-da.de
Telefon +49-6151-533-30090
https://dasec.h-da.de
https://www.athene-center.de