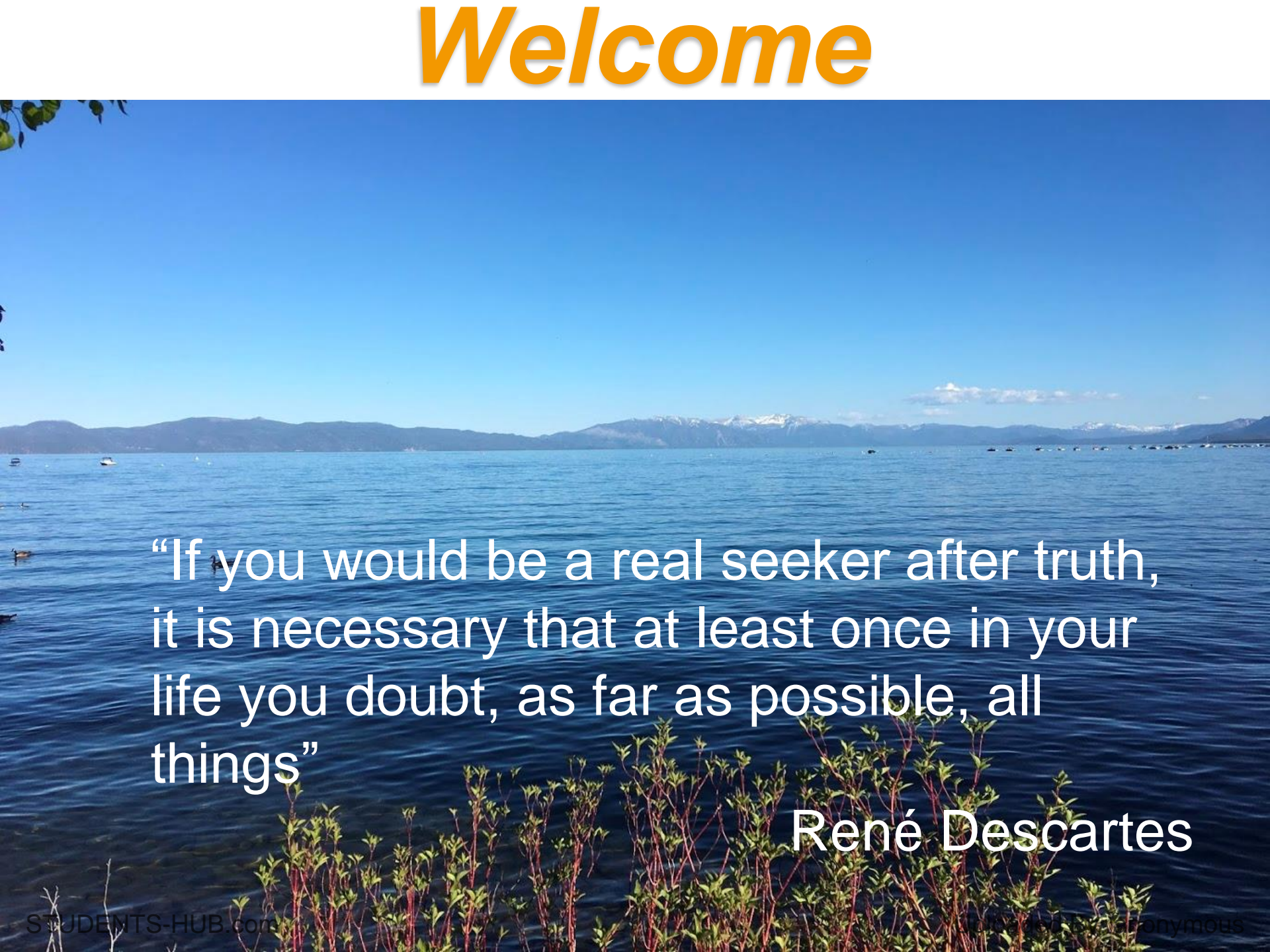


Welcome



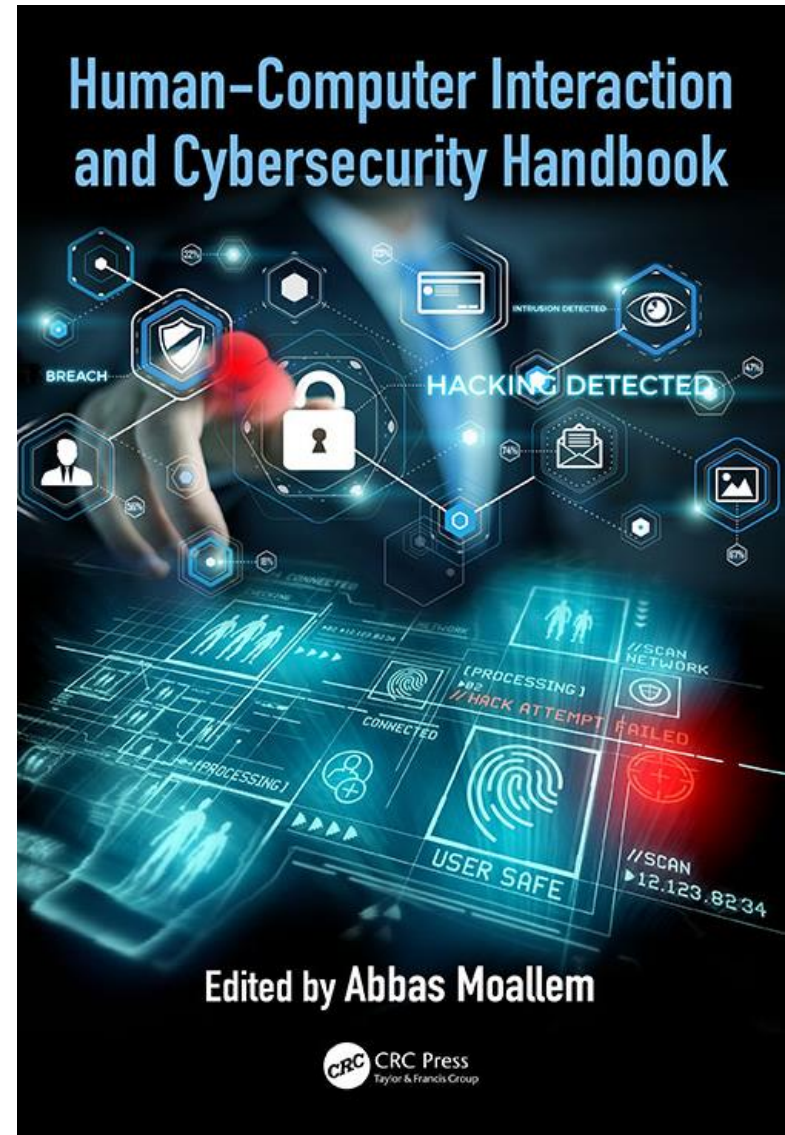
“If you would be a real seeker after truth,
it is necessary that at least once in your
life you doubt, as far as possible, all
things”

René Descartes

Chapter 2-Biometrics-Overview

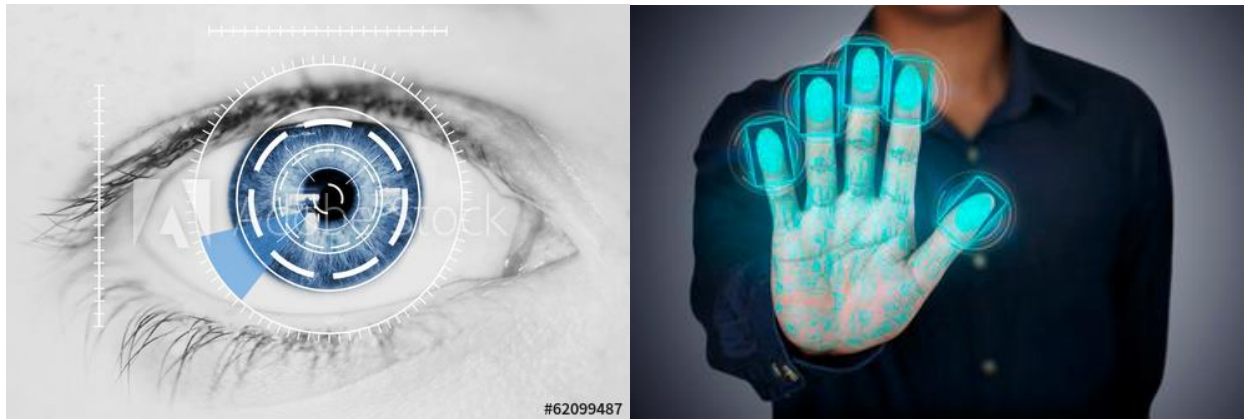
Human-Computer Interaction and Cybersecurity Handbook

- *Introduction*
- *Biometric verification*
- *Biometric matching paradigms*
- *Biometric security*
- *Biometric modalities*
- *Conclusion*



Introduction

- **Biometric usage for human–computer interaction is mostly concerned with biometric recognition, or matching.**
- **Biometric recognition can be divided into two categories:**
 - one-to- many matching, also called identification,
 - one-to-one matching, also called verification.

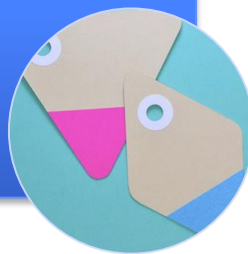


Biometric Recognition Categories

Human-Computer Interaction and Cybersecurity Handbook

- One-to-many matching

Identification



- one-to-one matching

Verification



Biometric verification is the one most relevant to human-computer interaction

Use cases of Biometric Recognition

Human-Computer Interaction and Cybersecurity Handbook

Forensics

Surveillance

Photo Tagging

identification of Customers

Use cases: physical access control, authentication of automated teller machine customers, phone unlocking, remote identity proofing, authentication, and privilege escalation.



Biometric Verification Concepts

Human-Computer Interaction and Cybersecurity Handbook

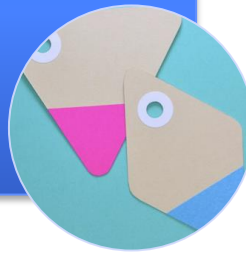
- **A biometric characteristic, or trait, is a measurable aspect of the human body that can be used to distinguish individuals from each other, such as a fingerprint, an iris image, a facial image, or acoustic features of the human voice.**
- **A biometric sample is a sample of a biometric characteristic.**
- **A biometric modality is a class of biometric systems that deal with a particular biometric characteristic.**
- **In biometric verification, a verifier compares two biometric samples and decides whether they come from the same individual.**

Biometric Verification is a two-phase protocol

Human-Computer Interaction and Cybersecurity Handbook

- Enrollment phase, an enrollment sample is acquired from a subject.

Phase 1



- Verification phase, the subject provides biometric input comprising a verification sample to a verifier, which compares it to the enrollment sample or to data derived from the enrollment sample.

Phase 2



Two kinds of biometric verification

Human-Computer Interaction and Cybersecurity Handbook

- **Authentication**
 - the subject presents the enrollment sample to the verifier. If the verification sample later matches the enrollment sample (or a template or other enrollment data derived from the enrollment sample), the verifier learns that the individual presenting the verification sample is the same subject who provided the enrollment sample, but nothing else.
- **Identity proofing**
 - In identity proofing, the verifier, which may have no prior relationship with the subject, obtains the enrollment sample or other enrollment data from an identification authority with which the subject has enrolled earlier, together with a binding of the enrollment data to attributes of the subject.

Biometric Matching Paradigms

Human-Computer Interaction and Cybersecurity Handbook

Templates

Statistical Models

Deep Neural Network

Biometric Cryptosystem

Biometric Templates

Human-Computer Interaction and Cybersecurity Handbook

- **A biometric template is derived from the enrollment sample and matched against the verification sample or against a template derived from the verification sample.**
- **A biometric template is an encoding of characteristic features of a biometric sample.**
- **The order of the features encoded in the template may or may not be significant. If it is significant, the template is a feature vector, or an encoding of a feature vector.**

Statistical Models

Human-Computer Interaction and Cybersecurity Handbook

- Multiple enrollment samples are used to construct a statistical model of the subject's biometric characteristic.
- A general model of the biometric characteristic is also constructed using samples from a large number of individuals, and
- A statistical test is used to estimate the likelihood that the verification sample comes from the subject rather than a random individual.





A Deep Neural Network

Human-Computer Interaction and Cybersecurity Handbook

- **Enrollment and verification samples are separately input to the network, which produces a mathematical output for each sample.**
- **The outputs are then compared according to some similarity metric and deemed to belong to the same person if their similarity metric is above a certain threshold. In the case of Google's FaceNet**
- **The output is a vector with 128 coordinates, each of which is a single byte, and the similarity metric used to compare the vectors derived from enrollments and verification samples is the Euclidean distance between the two vector**



A Biometric Cryptosystem

Human-Computer Interaction and Cybersecurity Handbook

- **A biometric cryptosystem error correction techniques are used to consistently generate a biometric key from varying but genuine biometric samples.**
- **At enrollment time, an enrollment biometric template is derived from an enrollment sample, and a random biometric key and helper data are generated from the enrollment template and random bits produced by a random or pseudorandom bit generator (NIST 2016).**
- **At verification time, a verification biometric template is derived from a verification sample, and an error correction algorithm attempts to recover the biometric key from the verification template and the helper data.**
 - **If the verification sample is genuine, the error correction algorithm is able to recover the key with a probability equal to the complement of the FRR, $1 - \text{FRR}$.**

Confidentiality of the Subject's Biometric

Human-Computer Interaction and Cybersecurity Handbook

- Randomization makes it computationally unfeasible to derive any useful biometric information from it.
- By contrast, traditional biometric templates reveal biometric information.





Different Kinds of Biometric Key

Human-Computer Interaction and Cybersecurity Handbook

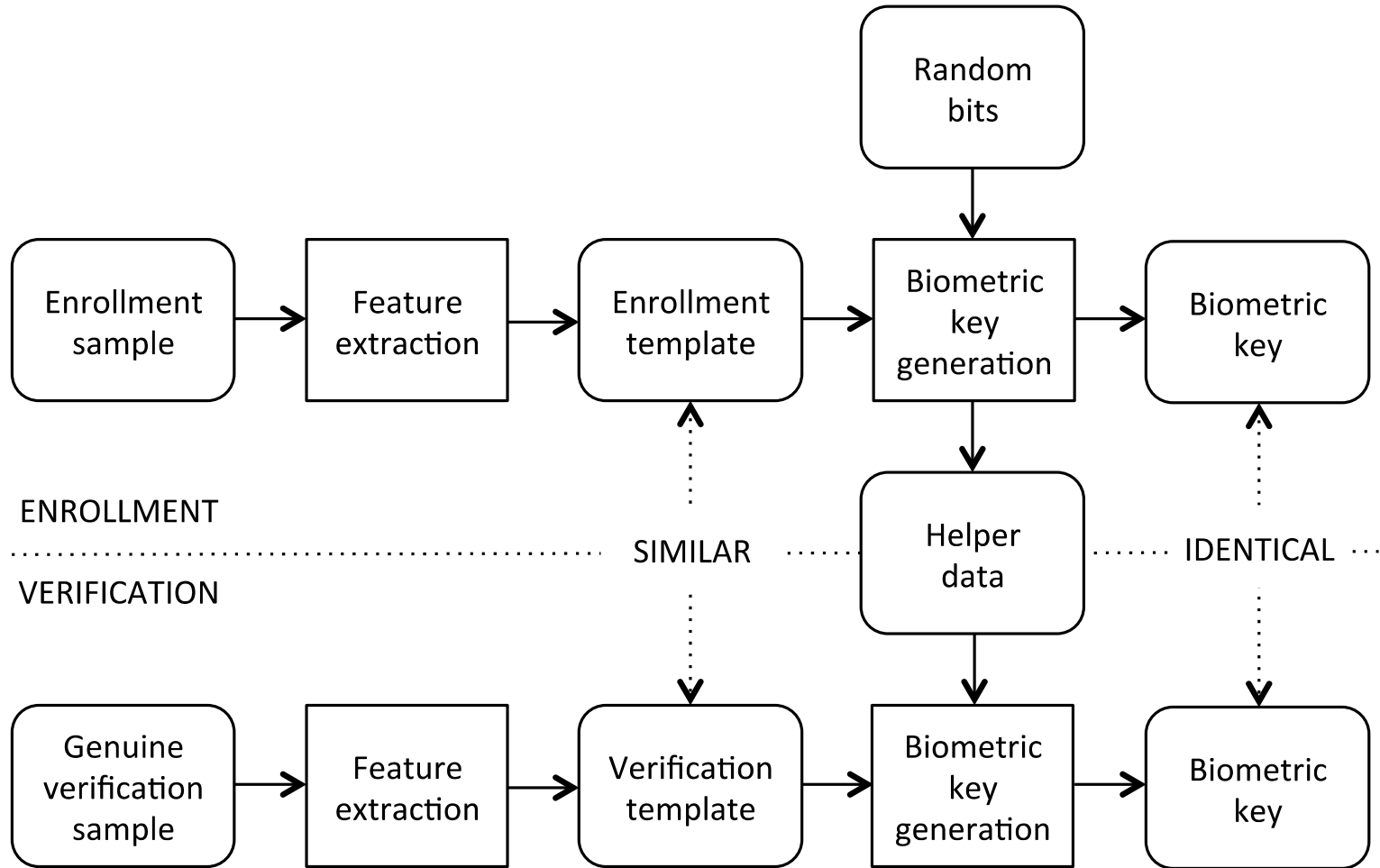
Key generation techniques are used with different kinds of biometric templates.

Techniques based on the concept of a fuzzy commitment may be used with feature vectors, where the order of the features matters,

Techniques based on the concept of a fuzzy vault may be used with feature sets, where the order does not matter.

Biometric System

Human-Computer Interaction and Cybersecurity Handbook





Biometric Cryptosystem

Human-Computer Interaction and Cybersecurity Handbook

- **A biometric cryptosystem can be used for a variety of purposes. For example, the biometric key can be used to encrypt data.**
- **In such a use case, if the biometric key is compromised, it can be replaced with a different random key generated from the same biometric characteristic of the subject, and the data can be encrypted anew with the replacement key.**
- **The biometric key is said to be revocable, and this motivates referring to biometric crypto- system technology as revocable biometrics, or cancelable biometrics.**



Biometric Cryptosystem

Human-Computer Interaction and Cybersecurity Handbook

- **When a biometric cryptosystem is used for biometric matching as discussed here,**
 - **the biometric key is not used for encryption or any other cryptographic use.**
 - **It is used to check whether the verification sample is genuine, by verifying that the error correction algorithm is able to produce the same key that was generated at enrollment time.**
 - **The biometric key cannot be stored along with the helper data for that purpose, because the helper data and the biometric key together do reveal biometric information.**
 - **But a cryptographic hash of the biometric key can be stored together with the helper data, and the biometric key produced at verification time can be verified by hashing it and comparing the resulting hash to the stored hash.**

Biometric Cryptosystem

Human-Computer Interaction and Cybersecurity Handbook

- **The use of a biometric cryptosystem for biometric matching raises a practical difficulty.**
 - **Neither the enrollment sample nor the enrollment template is available at verification time.**
 - **It is not possible to perform any geometric alignment of the enrollment and verification samples or templates, in modalities that require such alignment.**



Biometric Security

Human-Computer Interaction and Cybersecurity Handbook

- **The goal of biometric verification is to prevent the impersonation of the subject by an adversary, and that requires protecting against a variety of attacks that may be carried out by the adversary.**
- **The adversary may carry out a zero-effort attack by presenting a bio- metric sample from his or her own body and hoping that it will be accepted as genuine.**

Biometric Security

Human-Computer Interaction and Cybersecurity Handbook

- **Biometric accuracy mitigates zero-effort attacks.**
However,
 - The sample presented by the adversary may not come straight from the adversary's body.
 - It may come from an artifact, or the adversary may wear a disguise, or the sample may be a digital transformation of a sample originating from the adversary, or it may be a digital copy of a genuine sample coming from the subject's body.
 - Attacks with such samples are presentation attacks, informally known as spoofing attacks.



Presentation Attacks

- May be physical or digital, according to whether it is performed before or after a sensor has digitized the biometric sample.
- The presented sample may be artificial,
 - if it is produced by a physical artifact or is digitally generated; disguised, if it comes from a physically or digitally disguised adversary; or genuine, if it originates from the impersonation victim.
- The target, i.e., the biometric characteristic of the subject that the adversary wants to impersonate, may be known or unknown.

Presentation Attacks

- When a fake finger is used to hack the fingerprint sensor of a smart phone, or a photo of the impersonation victim is presented to a smart phone camera in an attack against face verification, the attack is *physical*, the sample is *artificial*, and the target is *known*.
- When a MasterPrint is used to make a fake finger that is presented to a partial fingerprint sensor, the attack is *physical*, the sample is *artificial*, and the target is *unknown*.
- When a wig, a fake nose, and makeup are used to disguise an adversary against face verification, the attack is *physical*, the sample is *disguised*, and the target is *known*.

Presentation Attacks

- When colored eyeglass frames are used in a perturbation attack against a deep neural network (Sharif et al. 2016), the attack may be *physical* or *digital*, the sample is *disguised*, and the target is *known*.
- When voice morphing is used to disguise the voice of an adversary reading prompted text in an attack against speaker verification, the attack is *digital*, the sample is *disguised*, and the target is *known*.
- When a video of the impersonation victim is obtained by a malicious verifier and replayed to another verifier, the attack is *digital*, the sample is *genuine*, and the target is *known*.

Protection against Presentation Attacks

Human-Computer Interaction and Cybersecurity Handbook

*Biometric
confidentiality*

*Combination
with a password*

*Presentation
attack detection*

*Remark:
Liveness
detection*



Security and Privacy Implications of Biometric Verification Architecture

Human-Computer Interaction and Cybersecurity Handbook

- **Biometric verification for human–computer interaction involves components, such as a sensor, enrollment data, and biometric matching software, and devices such as a smart phone, a personal computer, a smartcard, or a server.**
- **A biometric verification architecture determines what components reside on what device.**
- **There is a wide variety of possible architectures, ranging from an old-fashioned one where a fingerprint is obtained by a sensor attached to a desktop and compared to a template stored in a smartcard plugged into a card reader also attached to the desktop to more recent ones such as where a credit card is equipped with a fingerprint sensor.**



Security and Privacy Implications of Biometric Verification Architecture

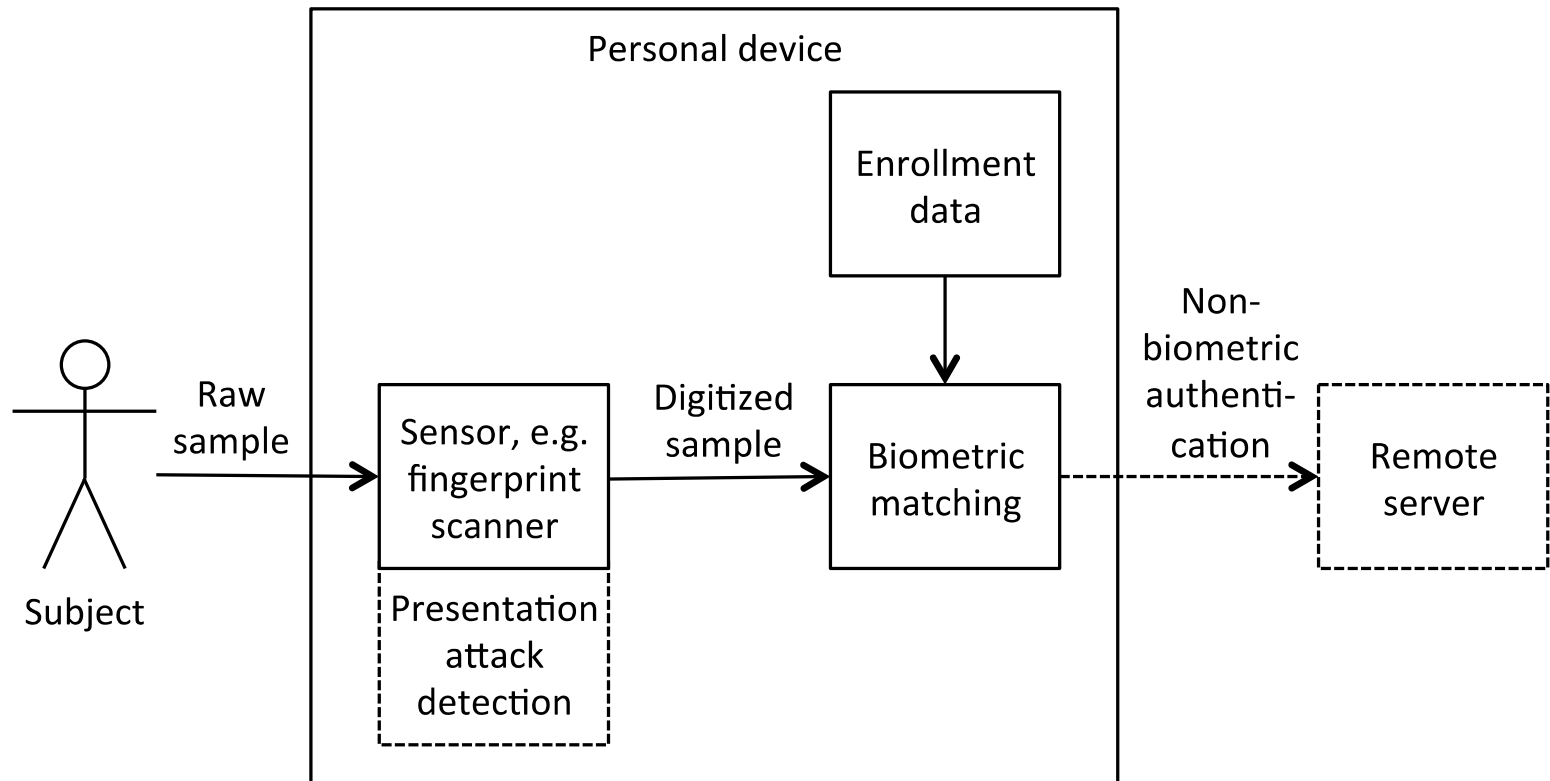
Human-Computer Interaction and Cybersecurity Handbook

The purpose of the authentication may be to unlock the device or to authorize a secondary nonbiometric authentication to a remote server. The latter purpose is the goal of the Fast IDentity Online (FIDO) Universal Authentication Framework (FIDO Alliance 2016), where the secondary authentication to the remote server is by means of an uncertified key pair.

Local Authentication

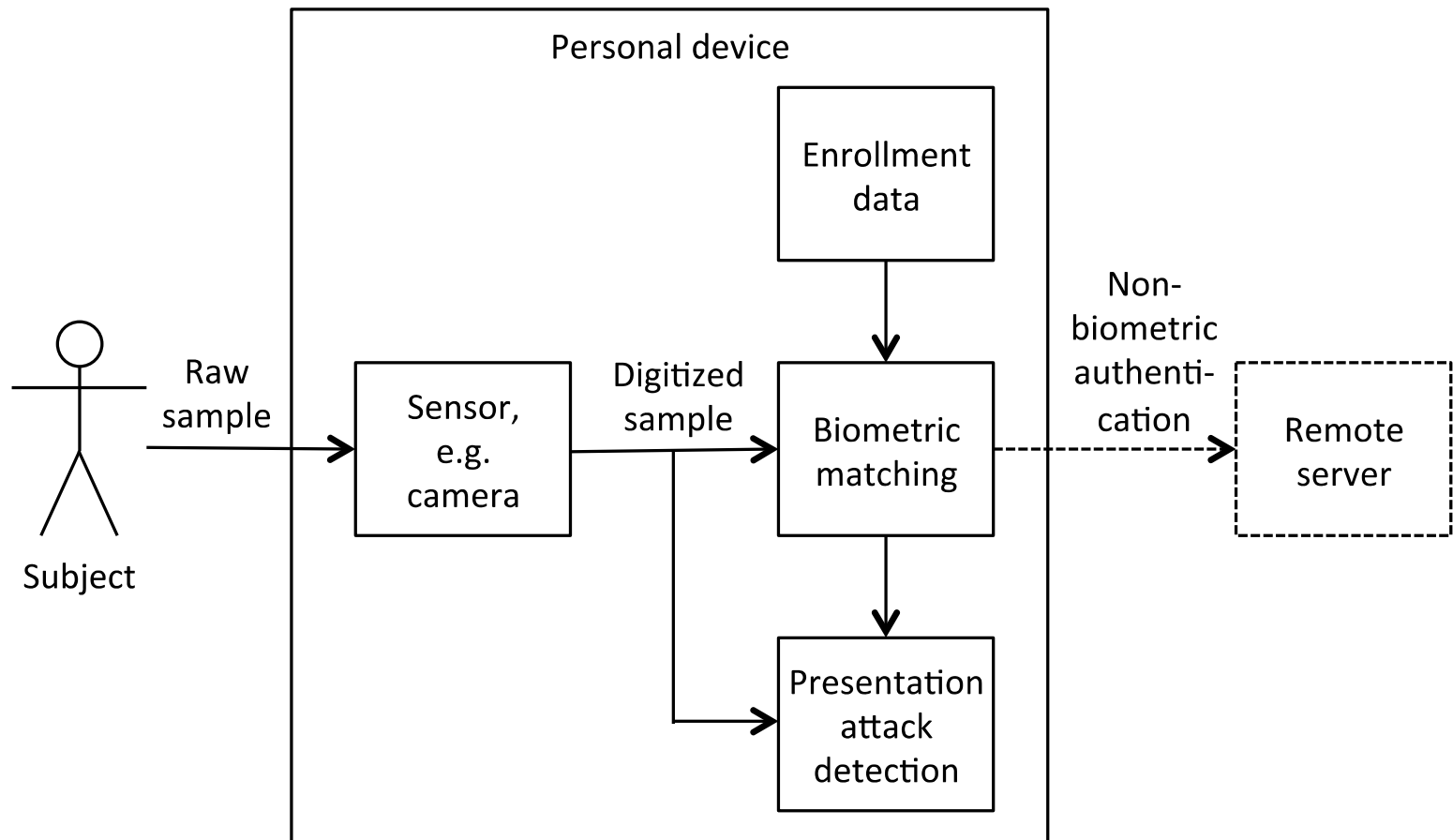
Human-Computer Interaction and Cybersecurity Handbook

Local authentication with Presentation attack detection by sensor



Local authentication

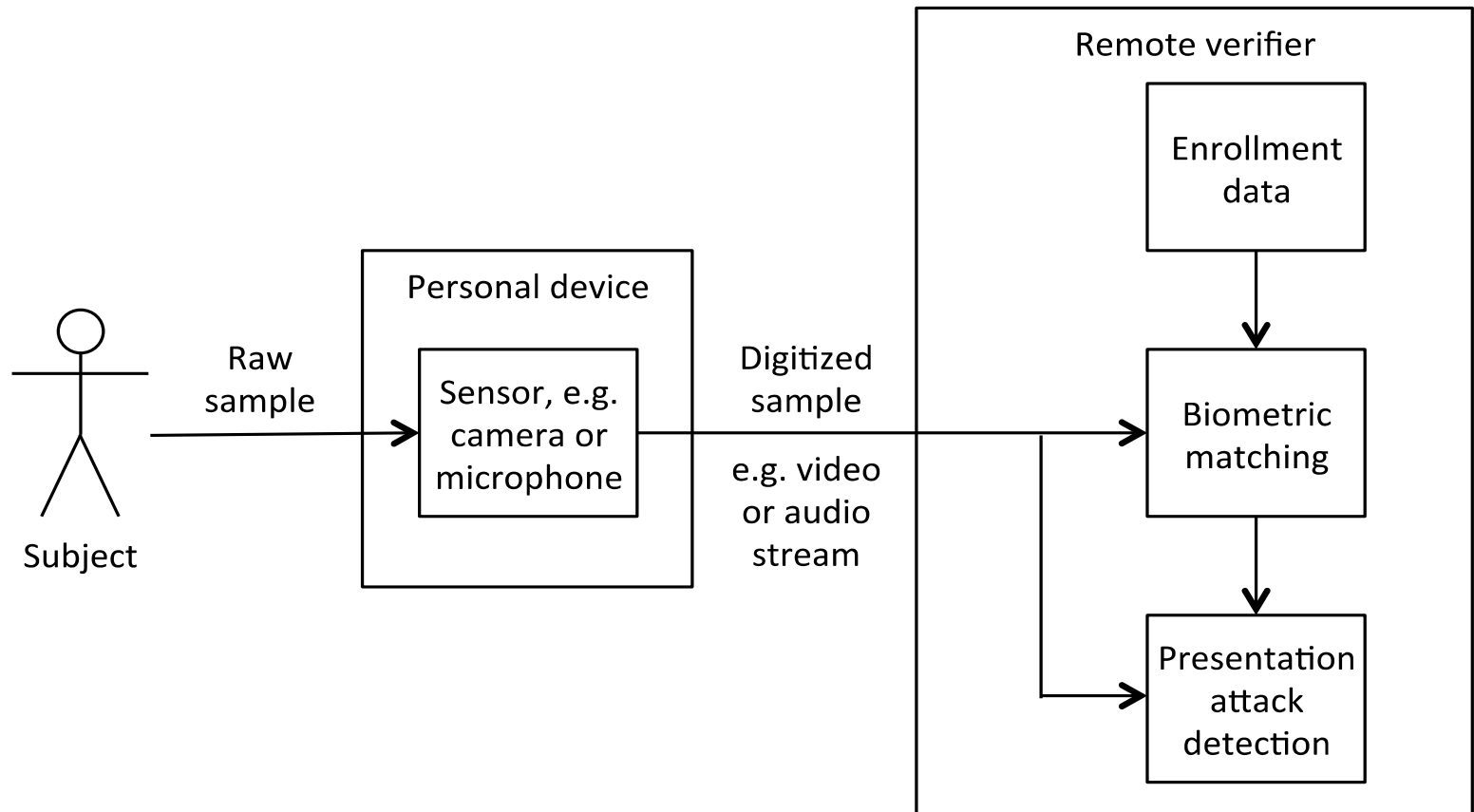
Local authentication with presentation attack detection by sensor.



Remote Authentication

Human-Computer Interaction and Cybersecurity Handbook

Remote authentication or identity proofing against a database.



Presentation Attack Detection

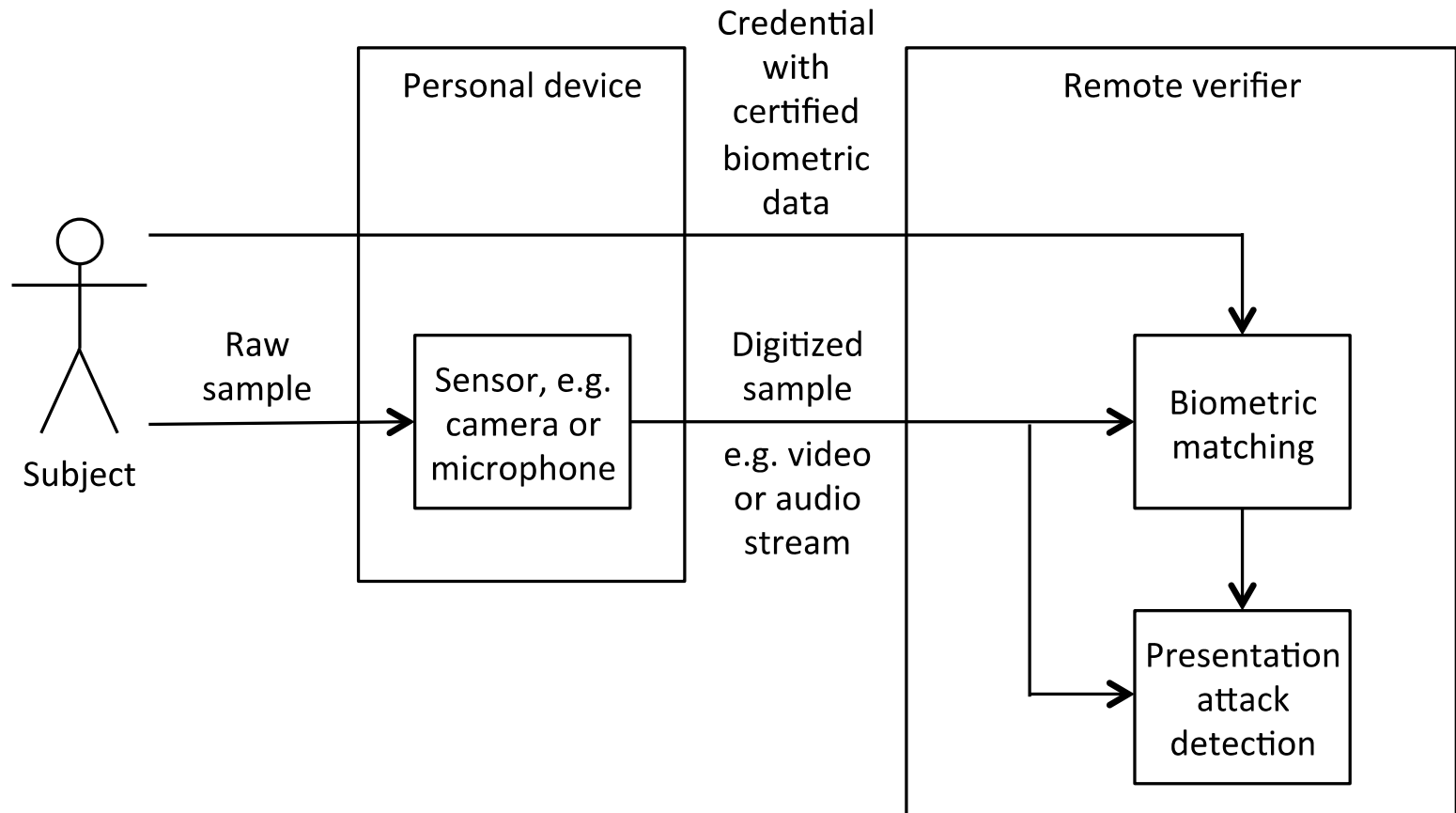
Human-Computer Interaction and Cybersecurity Handbook

- **Carried out by a sensor such as a fingerprint scanner, or is omitted.**
 - **Today, fingerprint scanners found on smart phones do not perform any presentation attack detection, but they may do so in the future,**
 - **Presentation attack detection is carried out on the digitized output of the sensor, which may be, for example, a video captured by a camera.**

Remote Authentication

Human-Computer Interaction and Cybersecurity Handbook

Remote authentication or identity proofing against certified enrollment data.



Biometric Modalities

Human-Computer Interaction and Cybersecurity Handbook

Fingerprint verification

Iris verification

Face verification

Speaker verification

Other Biometric Modalities

- **Retinal scanning is based on the pattern of blood vessels in the retina, observed using a beam of IR light that scans the retina as the subject looks into the scanner.**
- **Eye vasculature biometrics is based on the pattern of veins in the sclera (the white part of the eye).**
- **Finger vein recognition is based on the pattern of surface veins in the finger, imaged with IR light while the finger is inside a scanner.**
- **Electrocardiogram biometrics is based on the cardiac rhythm, which may be measured by an NFC-enabled wristband.**



Biometric Fusion

Human-Computer Interaction and Cybersecurity Handbook

Biometric fusion refers to the observation of multiple biometric characteristics, resulting in multiple biometric samples, for biometric verification.



Biometric Fusion

Human-Computer Interaction and Cybersecurity Handbook

- **There are many ways of combining the multiple samples to reach a decision as to whether they are genuine or not.**
- **The samples may be different instances of the same biometric modality, such as fingerprints from multiple fingers or images of both irises, or pertain to different modalities.**
- **They may be acquired by one sensor or multiple sensors.**



Conclusion

- **The security challenge is the need to provide protection against presentation attacks.**
- **There are two aspects to this challenge.**
 - **One is the need to spread awareness of the threat of presentation attacks among implementers and users of biometric verification systems.**
 - **The other is the need to address presentation attacks that are particularly difficult to cope with.**
- **Biometric cryptosystems can be used to protect biometric information against hackers in the architecture , but little work has been done on biometric cryptosystems for face or voice verification.**
- **More research is needed in those areas**

Questions

Human-Computer Interaction and Cybersecurity Handbook





Thank You For Your Participation