Biometric Systems

Script from the Course

Christoph Busch

January 19, 2021

Contents

1 Introduction to Biometrics

Biometric applications have the primary purpose, to provide access control with a non-delegable authentication factor. These applications are more convenient for users of an IT system on the one hand and increase the security of access control on the other hand. This manuscript covers a some aspects discussed in the course *Biometric Systems* and will look at how these techniques work, and what their strengths is. We also take a look at the weaknesses to learn how to prevent bypassing a security system. The compliance of biometric systems with European data protection regulations is of particular importance, which is why we will work Privacy Enhancing Technologies (PET) for biometric methods.

1.1 Overview

The International Standardisation defines the term *biometrics* as follows: *automated recognition of individuals based on their behavioral and biological characteristics* [5][1]. Biometric methods thus analyze human behavior and/or their biological characteristics. The biological characteristics are categorized into anatomical characteristics, which are shaped by structures of the body, and physiological characteristics, which are characterized by body functions such as the voice. The process of biometric authentication provides a unique link between an individual (i.e. the natural person) and their identity, regardless of where that identity is stored.

For more than a hundred years, criminal investigators have been using fingerprints to catch suspects on the basis of evidence at the scene of the crime. Today, computers speed up identification both online and at the scene: Automated Fingerprint Identification Systems (AFIS) compare traces found at the scene of a crime with millions of stored fingerprint images in just a few seconds. Nowadays the police has already introduced in some cities a mobile AFIS, which enables investigators to initiate this comparison even over mobile communication networks such as UMTS or GSM. But in addition to fingerprints, facial and iris images or representation of the hand geometry can be used as means of identification in a biometric process. It is no longer just criminal investigation offices that apply these technologies many commercial access control systems are now using biometrics for identification purposes. Biometrics, which is understood as the automated recognition of individuals based on their behavioural and biological characteristics, on the one hand exploits the rich set of anatomical characteristics related to the structure of the body (finger pattern, iris pattern etc.). These characteristics can be measured more or less directly. On the other hand behavioural or physiological characteristics are related to the function of the body such as the written signature, the

[1] you can find the definition online under `http://www.christoph-busch.de/standards.html\#370103`

voice or the typing pattern on the keyboard. Those functions create a signal, where Biometrics observes the emitted body signal.

1.2 Biometric Recognition

A biometric recognition process requires that an individual (i.e. the natural person) is known by the system in advance (enrolment) to create the necessary reference data. This is done in the enrolment procedure. Biometric systems can either be designed as verification systems or as identification systems.

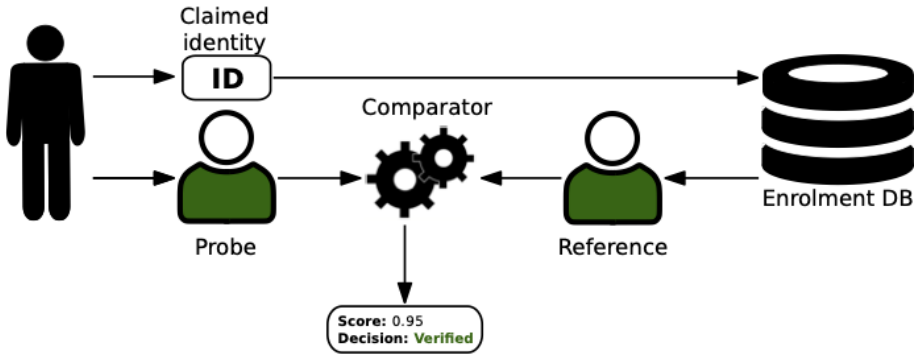

Figure 1.1: Biometric verification: confirming a biometric claim in a 1:1 comparison

In a verification system, the user specifies an identity to which - he claims - exists a reference in the system. If biometric systems are combined with an authentication document (e.g. a loyalty card), the biometric reference (e.g. a passport photo) may be stored on this document. At the time of verification, a comparison with exactly this one reference image is performed (1:1 comparison).

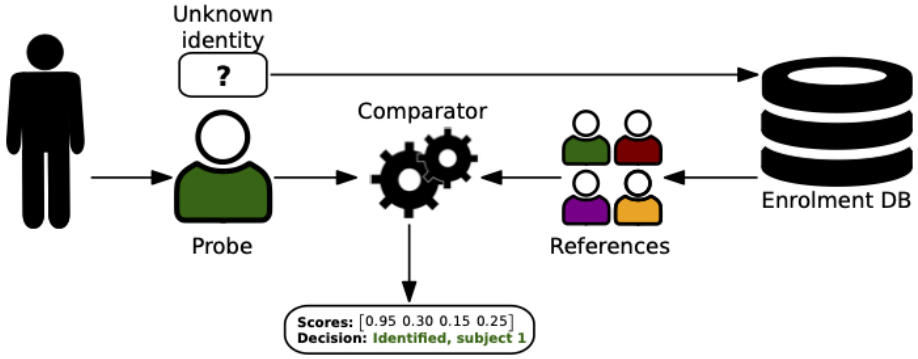

Figure 1.2: Biometric identification: searching a reference in a 1:n search

In the case of an identification system, on the other hand, the captured image is compared with many images that have been enrolled, and the most similar reference

record is determined from this set (1:n comparison). However, the similarity between two images must reach a pre-defined threshold, so that a reliable assignment of the identity associated with the most similar reference image can be done.

The biometric recognition process can be described with the following steps:

- **Acquisition:** Biometric characteristics are captured: a sensor, camera or other integrated capture device such as microphones observes the subject's characteristic and creates a digital representation, which is defined as the biometric sample (a scanned fingerprint, a digital portrait photo etc.)

- **Feature extraction:** This is a mathematical transformation applied to a biometric sample to derive distinguishing and repeatable numbers from the representation. These numbers are defined as biometric features, namely a concise representation of the original information. A biometric template is then understood to be a set of biometric features, which can be compared directly to biometric features from other presented biometric samples.

- **Enrolment:** In the enrolment process a biometric reference is created that is that one or more biometric samples or biometric templates are stored (in a database or in an ePass) and at the same time attributed to a subject. The reference can from then on be used for comparison.

- **Comparison:** This is a process in which probe sample stemming from the live biometric characteristic of one individual is compared against the biometric references of one or more individuals. The result of such comparison is a score that indicates the similarity (a value close but seldom identical to one) or dissimilarity (a value close to zero) of two samples.

Only after the comparison the recognition system is capable to decide on the comparison score, whether a presented sample matches or non-matches to a stored reference. The principle of biometric recognition is the same in all systems regardless of their particular technological design. In any case a biometric system must "learn" the biometric characteristic of the subject, before it can "recognize" an individual. Thus the information describing those biometric characteristics must be recorded and stored in data records. If a capture subject is asking for access authorization, the system compares current data with the data in the records. If they match to a specified level of certainty, the system recognizes the person and grants access.

The process steps are illustrated in figure 1.3, which provides a reference architecture for a biometric system [3].

1.2.1 Criteria for Biometric Characteristics

The procedure of enrolment, verification and identification are shown in Figure 1.3, from which also the essential components of a biometric system become apparent [3]. When constructing a biometric system, it is important to not only select appropriate technical components (i.e. capture device and embedded sensors, signal processing subsystem,

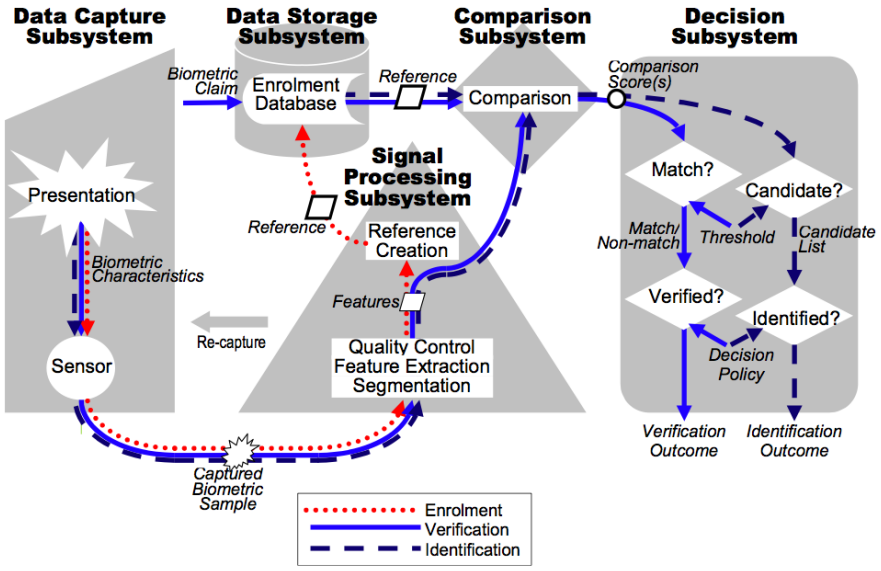

Figure 1.3: ISO/IEC reference architecture of a biometric system [3].

comparison subsystem, and decision subsystem) but also choose a suitable biometric characteristic for the target group that meets the following criteria:

- **Universality:** every individual should have it.
- **Uniqueness:** is the characteristic distinctive such that any two individuals are sufficiently different.
- **Performance:** does a recognition system based on this biometric characteristic provide a reasonable biometric performance (low errors). Furthermore this property is associated with the throughput time (how does it take to capture the biometric characteristic and to extract features from the captured sample.
- **Permanence:** the characteristic should be invariant over time and features extracted thereof should be persistent and not be mutable over time. The ageing of the individual should not affect the feature vector.
- **Collectability:** the characteristic is measurable and the quantitative result is reproducible.
- **Acceptability:** the capture process provides a convenient measurement at low cost and is considered unobtrusive for the data subjects.
- **Security:** intended impostor attacks are hard, as it is difficult to collect the biometric characteristic and replicate a fake biometric characteristic, which would be capable to fool a sensor. Thus the security of a captures device measuring this biometric characteristic can be considered high.

Factors → / Biometric identifier ↓	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	Circumvention
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Figure 1.4: Comparison of biometric modalities [7].

If individual criteria are not met in a mono-modal system, multi-modal systems can be a solution. For example, a face recognition is combined with an iris recognition in order to achieve a sufficient recognition performance of the biometric system.

Biometric characteristics always arise under the influence of genes received from the parents. The face often resembles the face of the parents. Also, a certain behavior (e.g. the gait, the way of speaking) is often taken over from the parents or has been adapted from role models in the course of life. To a certain extent, characteristics are therefore genetically determined or characterized by behavior and the environment. However, a good and suitable biometric characteristic is primarily characterized by random factors. This property applies, for example, to the formation of a fingerprint or the pattern of the iris, which occur randomly during pregnancy. These patterns remain consistent and do not change when developing from child to adult.

1.2.2 Categories of Biometric Methods

In addition to the criteria of the biometric characteristics, we can also look at the categories for biometrics methods and then sort or benchmark biometric technology. The consideration of said categories makes it possible to evaluate certain products in a technology selection procedure. These are some examples of categories:

- **static / dynamic** - is a characteristic captured as a snapshot (e.g. photo of the face), or is a continuous measurement of a signal (e.g. recording of the voice or keyboard interaction) necessary.
- **cooperative / non-cooperative** - this category, which is for simplicity often referred to as *active / passive*, distinguishes between those methods of measurement in which the individual (i.e. *biometric capture subject*[2]) is aware that he/she

[2]biometric capture subject is defined `www.christoph-busch.de/standards.html\#370703`

interacts with a capture device (for instance the fingerprint sensor) versus such applications in which the affected individual is not aware of the data acquisition (e.g. video surveillance)

- **contact-free / contact-based** - for some modalities (such as fingerprints) the recording can be both contactless, i.e. using a digital photo, or contact-based, i.e. via a dedicated fingerprint sensor. The choice of the capture device has influence on any potential deformation of the finger (e.g. by the pressure applied during placement) and also on the acceptance of the procedure with regards to the subjects's concern about the transmission of diseases.

- **open / closed** - large biometric systems, such as the forensic applications of law enforcement agencies, are usually open so that data can be exchanged between different departments in a uniform standardized format. Even today's border control applications such as the one *EasyPASS*[3] at German Airports are open systems because identity documents which may have been produced outside of Germany must be able to be read when entering (see more in the chapter on **??**). For this, storing biometric data in the passport in a standard format [1, 2] is a mandatory prerequisite. On the contrary an operator that wants to ensure access control through biometrics can use a closed and *proprietary* storage format, but with a high risk: if the system vendor leaves the market, the reference data must be recoded or, if necessary, re-coded or recorded again.

- **supervised / unsupervised** - some biometric systems such as border control are deliberately operated under supervision only. For some biometric capture devices good robustness against attacks can be assumed, i.e. a sensor is not deceived by artefacts (i.e. counterfeit or plagiarized characteristics) [4]. Such capture devices are suitable for unattended systems in the physical access control to buildings, which can mean significant potential for savings in terms of staff. An online banking system with biometrics is another example of an unsupported application with high relevance.

- **positive identification / negative identification** - in the case of positive identification, the biometric statement consists of the statement *"I have a reference record in the company's database because I am an employee"*. In the case of negative identification, the biometric statement consists of the statement *"I have no reference record in the criminal records database because I am not a criminal"*.

- **environment sensitive** - performance of biometric techniques may be severely impacted by environmental factors. A facial recognition system is difficult to operate in direct sunlight whereas a speaker recognition system faces difficulties in the vicinity of a busy street.

[3] The EasyPASS application is a Biometric Border control: `https://www.easypass.de/EasyPass/DE/Was_ist_EasyPass/home_node.html`

In addition to the criteria discussed above, there are other obvious factors such as cost of procurement and cost and effort of operating the biometric system. Very relevant is also the question of familiarization of the affected person to the interaction with the capture device. A facial recognition photo can be taken without much instruction. If necessary, the supervisor must be trained, so that attention is paid to good lighting conditions. Training of the capture subject themself, however, is necessary for example for a signature recognition system. The "blind" writing on a tablet PC takes getting used to, and only over time a largely error-free interaction will be possible. From a technical point of view, it is particularly important for us to observe errors and to measure the recognition performance, which we will explore in chapter **??**.

Strengths of Biometric Authentication

What are the strengths of biometric authentication? The classical authentication mechanisms, such as the knowledge authentication (password), authentication via tokens (keys) or the like are provided with distinct disadvantages. You can usually pass on your password and token in violation of a security guideline; you can forget about it or lose it. To prevent loss in the increasing number of logical and physical access controls, inappropriate storage locations or identical passwords are regularly used. In contrast, we cannot forget biometric characteristics and we cannot delegate them. Biometric applications allow identification of an individuals's identity in logical and physical access control, and biometrics can solve problems of other authentication methods. Furthermore, in biometric authentication equality of security across different users prevails, as opposed to, for example, knowledge-based authentication in which "strong" or "weak" passwords can be chosen.

Weaknesses of Biometric Authentication

Biometric methods are usually used to either improve the usability of a technical system (e.g. fingerprint authentication on the iPhone or Samsung smartphone) or to improve the security of a technical system. However, it must be taken into account that the introduction of a biometric user recognition potentially introduces new security risks. Many attacks can be intercepted by cryptographic protocols and secure transmission of biometric data (see chapter **??**).

1.3 Vocabulary

Literature and science specifically in a multi-disciplinary community as in biometrics tends to struggle with a clear and non-contradictonary use and understanding of its terms. Thus ISO/IEC has undertaken significant efforts to develop a Harmonized Biometric Vocabulary (HBV) [5] that contains terms and definitions useful also in the context of discussions about presentation attacks. Without going into detail of the terminology definition process it is important to note that biometric *concepts* are always discussed in context (e.g. of one or multiple biometric subsystems) before a *term* and

its *definition* for said concept can be developed. Thus terms are defined in groups and overlap of groups ("concept clusters") and the interdependencies of its group members necessarily lead to revision of previously found definitions. The result of this work is published as ISO/IEC 2382-37:2017 [5]

The following list contains definitions of interest:

- **biometric characteristic** : biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition (37.01.02)
- **biometric feature** : numbers or labels extracted from biometric samples and used for comparison (37.03.11)
- **biometric capture subject** : individual who is the subject of a biometric capture process (37.07.03)
- **biometric capture process** : collecting or attempting to collect a signal(s) from a biometric characteristic, or a representation(s) of a biometric characteristic(s,) and converting the signal(s) to a captured biometric sample set (37.05.02)
- **impostor** : subversive biometric capture subject who attempts to being matched to someone else's biometric reference (37.07.13)
- **identity concealer** : subversive biometric capture subject who attempts to avoid being matched to their own biometric reference (37.07.12)

The use of biometric terms in a term paper **must** be compliant with the ISO/IEC SC37 Biometric Harmonized Vocabulary (ISO/IEC 2382-37:2012). In consequence replace for instance any occurrence of the term *matching* with *comparison* and use the term *template* only in a context, where you actually refer to a set of extracted biometric features.

1.4 Reading

Complementary reading for an introduction on biometrics is the overview provided with [8]. A tutorial on biometrics has been published as technical report of ISO/IEC JTC1 SC37 [6]. A general biometric system architecture is described in the ISO/IEC SC37 Standing Document 11[3]. The ISO/IEC SC37 Standardised Vocabulary [5] provides a Harmonized Biometric Vocabulary, which is available online version at:
`http://www.christoph-busch.de/standards.html`

Bibliography

[1] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19794-4:2005 Information Technology – Biometric Data Interchange Formats – Part 4: Finger Image Data.* International Organization for Standardization, July 2005.

[2] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19794-5:2005. Information Technology - Biometric Data Interchange Formats - Part 5: Face Image Data.* International Organization for Standardization, June 2005.

[3] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC SC37 SD11 General Biometric System.* International Organization for Standardization, May 2008.

[4] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 30107-1. Information Technology - Biometric presentation attack detection - Part 1: Framework.* International Organization for Standardization, 2016.

[5] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 2382-37:2017 Information Technology - Vocabulary - Part 37: Biometrics.* International Organization for Standardization, 2017.

[6] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC TR 24741 Biometrics Tutorial.* International Organization for Standardization, 2018.

[7] Jain, A., Ross, A., and Pankanti, S. Biometrics: A tool for information security. *IEEE Trans. on Information Forensics and Security* (2006).

[8] Jain, A. K., Flynn, P., and Ross, A. A. *Handbook of Biometrics.* Springer, July 2007.