Pre-print version

E. Micheli-Tzanakou, K. Plataniotis, R. Donida Labati, "Biometrics: Terms and Definitions", in Encyclopedia of Cryptography, Security and Privacy, S. Jajodia, P. Samarati, M. Yung (eds.), Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1-5, January, 2021. ISBN: 978-3-642-27739-9.

[DOI: 10.1007/978-3-642-27739-9_730-2]]

Biometrics: Terms and Definitions

Evangelia Micheli-Tzanakou, Konstantinos N. Plataniotis, and
Ruggero Donida Labati [*]

Definition

Biometrics is defined as the "Automated recognition of individuals based on their behavioral and biological characteristics."

Background

The interest in biometric recognition technologies has grown significantly in the last four decades, and academic as well as corporate research units have devoted a lot of resources to study and develop accurate, user friendly, unconstrained, and cost-effective biometrics. As a result, biometric authentication systems are in use today in a wide range of applications, including physical access control, surveillance, network security, online transactions, attendance control, and authentication technologies for mobile devices and personal computers, as described in Blackburn et al (2009).

From the technological point of view, biometric systems can be considered as pattern recognition systems (please refer to Goodfellow et al (2016)). However, they present specific problems and peculiarities that are commonly described by the research and industrial communities using a set of specific terms and definitions, which are frequently defined by international standards.

Theory

Biometric systems

Biometric can be seen as a general term used alternatively to describe

[*] corresponding author

a characteristic or a process, as described in Blackburn et al (2009).

- *As a characteristic*
  "A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition."
- *As a process*
  "Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."

Biometric traits are behavioral or biological characteristics of the individuals used by deployable biometric systems (as described in Boulgouris et al (2009)). Some widely used biometric traits are the following: face, fingerprints, iris, voice, gait, and signature. Many other modalities, such as soft biometrics and ear biometrics, are in various stages of development and assessment. Factors such as device location, security risks, task (identification or verification), expected number of users, user circumstances, and existing data must be taken into consideration when a biometric trait is selected as input to a recognition system.

Biometric Trait – Characteristics (Table 1):

- *Universality* refers to the fact that everyone should have this trait.
- *Uniqueness* refers to the fact that no two persons should be the same in terms of this trait.
- *Collectability* refers to the fact that the characteristic can be measured quantitatively.
- *Permanence* refers to the fact that the characteristic should be invariant with time.
- *Performance* refers to the achievable accuracy, resource requirements, robustness.
- *Acceptability* refers to the grade in which people are willing to accept using the biometric system.
- *Circumvention* refers to how easy it is to fool the system, as detailed in Jain et al (2004).

Biometric system refers to a pattern recognition system which can be used to identify and / or verify a person's identity. A biometric system is usually comprised of five integrated modules:

- *Sensor module* collects the data and converts the information to a digital format.
- *Signal processing module* performs quality control activities and develops the biometric template.
- *Data-storage module* keeps information to which new biometric templates will be compared.
- *Matching algorithm module* compares the new biometric template to one or more templates kept in data storage.
- *Decision module* (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

Biometric templates are files derived from the unique features of a biometric sample. Biometric vendors' templates are usually proprietary and not interoperable (for more details, please refer to Boulgouris et al (2009)).

Biometric system – operations:

- *Enrollement* is the process of collecting a biometric sample from an individual (“end-user”), converting it into a biometric template, and storing it in the biometric system’s database for later comparison.
- *Matching* is the process of comparing a biometric sample against a previously stored template and scoring the level of similarity or difference between the two. Biometric systems then make decisions based on this score and its relationship against a predetermined threshold (above or below the threshold).

Biometric systems – recognition tasks:

- *Authentication / verification* involves a one-to-one match that compares a query sample against a template of the claimed biometric identity in the database. The claim is either accepted or rejected.
- *Identification / recognition* involves one-to-many matching that compares a query sample against all the biometric templates in the database to output the identity or the possible identity list of the input query. In this scenario, it is often assumed that the query sample belongs to the persons who are registered in a database.
- *Watch list* involves one-to-few matching that compares a query sample against a list of suspects. In this task, the size of database is usually very small compared to the possible queries and the identity of the probe may not be in the database. Therefore, the recognition system should first detect whether the query is on the list or not and if yes, correctly identify it.

Biometric system – performance are generally measured using two quantities (as described in Blackburn et al (2009)): False Acceptance Rate (FAR) and False Rejection Rate (FRR) which are defined as follows:

- *False acceptance rate* (FAR) is the percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual’s existing biometric.
- *False rejection rate* (FRR) is the percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his / her own existing biometric template.

These values can generally be varied by way of system parameter choices. The plot of FAR vs. FRR using different parameters generates what is known as the Receiver Operating Characteristic (ROC) curve. The term is used to define a method of showing the measured accuracy performance of a biometric system. A verification ROC compares false accept rate vs. verification rate. An open-set identification (watch-list) ROC compares false alarm rates vs. detection and identification rate.

Multi-biometric systems attempt to enhance the authentication performance of single biometric systems by combining multiple evidences of the same

Table 1 Comparison of different biometric technologies, from Jain et al (2004)

Biometric	Universality	Accuracy	Stability	User acceptability	Cost	Circumvention (difficulty)
Face	H	L	M	H	L	L
Fingerprint	M	H	H	H	L	L
Voice	M	L	L	H	L	L
Iris	H	H	H	L	H	H
Signature	L	L	L	H	L	L
Gait	M	L	L	H	L	M
Palmprint	M	H	H	M	M	M

identity, obtained from multiple biometric samples and / or sensors.

Privacy

Privacy is a major concern in the use of biometric systems (Donida Labati et al (2012)). There are two main categories of privacy risks posed by biometric systems:

- *Personal privacy* relates to privacy of the individual user, the infringement of which relates to coercion or physical or emotional discomfort when interacting with a biometric system.
- *Informational privacy* relates to the misuse of biometric information or of data associated with biometric identifiers.

Depending on how biometric systems are used and what protections are in place to prevent their misuse, biometric systems can be categorized as:

- *Privacy-protective* is a system in which biometric data is used to protect or limit access to personal information.
- *Privacy-sympathetic* is a system in which protections are established and enforced to limit the access to and usage of biometric data.
- *Privacy-neutral* is a system in which privacy simply is not an issue, or in which the potential privacy impact is very slight. These are generally closed systems in which data never leaves the biometric device.
- *Privacy-invasive* is a system that is used in a fashion inconsistent with generally accepted privacy principles. Privacy-invasive systems may include those that use data for purposes broader than originally intended.

Application

As an example, we consider a face identification systems.

As described in Sundararajan and Woodard (2018), face recognition technologies can be divided into approaches based on handcrafted features (Boulgouris et al (2009)) and approaches based on deep learning strategies (Goodfellow et al (2016)) .

In this appliction scenario, the system must attempt to detect whether a given subject entering the premises (termed a “probe” subject) is enrolled in the system and, if he or she is enrolled, identify that subject. When a positive detection and identification is achieved, this is considered “acceptance” in the system. Conversely, if detection fails, then “rejection” has occurred.

The identification performance is affected by means of a ranking threshold, r, which determines how many of the enrolled subjects (which achieved positive detection when compared to the probe subject) may achieve positive identification. For example, if $r = 1$, then only the (one) enrolled subject exhibiting the highest similarity compared to the probe subject is considered a candidate identity; if $r = 2$, then the two enrolled subjects exhibiting the highest similarities compared to the probe subject, and so on. Increasing r weakens the criterion for identification and increases the likelihood that the subject will be correctly identified in this ranked list context.

This leads to a definition of correct detection and identification, which is achieved when:
Correct Detection and Identification (Acceptance)

$$s_{ij} \geq t_s \quad \mathrm{rank}(p_j) \leq r \quad \mathrm{id}(p_j) = \mathrm{id}(g_i) \tag{1}$$

where p_j is a given probe subject, and g_i is a subject enrolled in the system (termed a “gallery” subject); the ranking is performed across all gallery (enrolled) subjects.

Hence, a false detection and identification is achieved when:
False Detection and Identification (Acceptance)

$$s_{ij} \geq t_s \quad \mathrm{rank}(p_j) \leq r \quad \mathrm{id}(p_j) \neq \mathrm{id}(g_i) \tag{2}$$

where p_j is a given probe subject, and g_i is a subject enrolled in the system; the ranking is performed across all gallery (enrolled) subjects.

Conversely, correct rejection occurs when:
Correct Rejection

$$s_{ij} < t_s \quad \mathrm{id}(p_j) \neq \mathrm{id}(g_i) \quad \forall g_i \in G \tag{3}$$

where p_j is a given probe subject, g_i is a subject enrolled in the system, and Grepresents the set of all enrolled subjects (“gallery” set).

And finally, false rejection occurs when:
False Rejection

$$\begin{gathered}[(s_{ij} < t_s) \text{ or } (s_{ij} \geq t_s \text{ and } \mathrm{rank}\,(p_j) > r)] \\ \text{and } \mathrm{id}\,(p_j) = \mathrm{id}\,(g_i)\end{gathered} \tag{4}$$

where p_j is a given probe subject, and gi is a subject enrolled in the system; the ranking is performed across all gallery (enrolled) subjects.

This leads to the measure of probability of correct detection and identification as follows:

$$\begin{gathered}P_{DI}(t_s, r) = \\ \frac{\left|\left\{p_j : s_{ij} \geq t_s, \mathrm{rank}(p_j) \leq r, \mathrm{id}(p_j) = \mathrm{id}(g_i)\right\}\right|}{|P_G|}, \\ \forall p_j \in P_G\end{gathered} \tag{5}$$

where P_G is the set of probe subjects, all of which are enrolled in the system. In other words, measuring across a set of subjects which are all enrolled in the system, determined the fraction of them which will be correctly detected and identified.

The fractions of those which are rejected constitute false rejections, leading to the probability of false rejection or false rejection rate (FRR):

$$P_{FR}(t_s, r) = 1 - P_{DI}(t_s, r) \tag{6}$$

We note that P_{FR} is completely dependent on P_{DI}.

The other measure of performance is the probability of false acceptance (also known as false acceptance rate (FAR)).This is measured as follows:

$$P_{FA}(t_s) = \frac{\left|\left\{p_j : \max_i s_{ij} \geq t_s\right\}\right|}{|P_N|}, \quad \forall p_j \in P_N \; \forall g_i \in G \tag{7}$$

where P_N is a set of "impostor" subjects not enrolled in the system. In other words, measuring across a set of subjects which are not enrolled in the system, determines the fraction of those subjects exhibiting a similarity with an enrolled subject (the gallery set G) greater than the threshold t_s.

Open problems and Future directions

The research community is constantly active in designing novel solutions for improving heterogeneous aspects of current biometric systems. In this context, novel terms and definitions are constantly presented by researchers to describe the innovative aspects of their works. Therefore, selecting the most appropriate terms and definitions for new research fields in biometrics can still be considered as an open problem. To avoid possible ambiguities and redefinitions of terminologies accepted by the research community, it is necessary to have a deep knowledge of the state of the art, in order to consider all the international standards and the previously published works. Furthermore, as a future direction, standards should be promptly realized for defining commonly accepted terminologies for every novel research context.

Summary

The research community working in biometrics use a specific set of terms and definitions to univocally describe different aspects of biometric systems. For example, there are specific terms for describing technological features, performance metrics, and privacy-related aspects.

References

Blackburn DM, Miles C, Wing B (2009) Biometrics foundation documents

Boulgouris N, Plataniotis K, Micheli-Tzanakou E (2009) Biometrics: Theory, Methods, and Applications. IEEE Press Series on Computational Intelligence, Wiley

Donida Labati R, Piuri V, Scotti F (2012) Biometric privacy protection: Guidelines and technologies. In: Obaidat MS, Sevillano JL, Filipe J (eds) E-Business and Telecommunications, Springer Berlin Heidelberg, pp 3–19

Goodfellow I, Bengio Y, Courville A (2016) Deep Learning. MIT Press

Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 14(1):4–20

Sundararajan K, Woodard DL (2018) Deep learning for biometrics: A survey. ACM Computing Surveys 51(3)