

1 General Biometric System

1.1 Conceptual representation of general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. *Captured biometric samples* are acquired from a subject by a sensor. The sensor output is sent to a processor that extracts the distinctive but repeatable measures of the sample (the *biometric features*), discarding all other components. The resulting features can be stored in the *biometric enrolment database* as a *biometric reference* or (in this case) a *biometric template*. In other cases the sample itself (without feature extraction) may be stored as the reference. A subsequent *probe* biometric sample can be compared to a specific reference, to many references or to all references already in the database to determine if there is a match. A decision regarding the *biometric claim* is made based upon the similarities or dissimilarities between the features of the *biometric probe* and those of the reference or references compared.

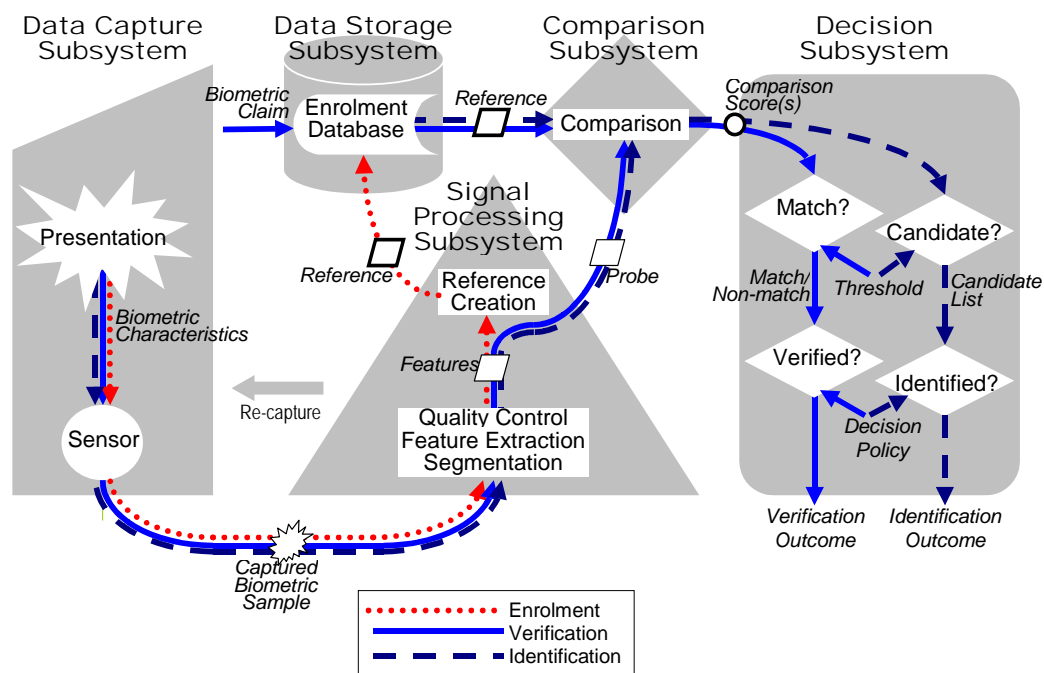


Figure 1 — Components of a general biometric system

Figure 1 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, data storage, comparison and decision subsystems. This diagram illustrates both enrolment, and the operation of verification and identification systems. The following sub-clauses describe each of these subsystems in more detail. However, it should be noted that in any implemented system, some of these conceptual components may be absent, or may not have a direct correspondence with a physical or software entity.

1.2 Conceptual components of a general biometric system

1.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's *biometric characteristics* that they have presented to the *biometric sensor*, and outputs this image/signal as a *captured biometric sample*.

1.2.2 Transmission subsystem (Not portrayed in diagram)

The transmission subsystem (not always present or visibly present in a biometric system) will transmit *samples*, *features*, *probes* and *references* between different subsystems. The captured biometric sample may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A captured biometric sample may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. Data may be transmitted using standard biometric data interchange formats, and cryptographic techniques may be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

1.2.3 Signal processing subsystem

Signal processing may include processes such as:

- *enhancement*, i.e. improving the quality and clarity of the captured biometric sample,
- *segmentation*, i.e., locating the signal of the subject's biometric characteristics within the captured biometric sample,
- *feature extraction*, i.e., deriving the subject's repeatable and distinctive measures from the captured biometric sample, and
- *quality control*, i.e., assessing the suitability of samples, features, references, etc. and possibly affecting other processes, such as returning control to the data capture subsystem to collect further *samples*; or modifying parameters for segmentation, feature extraction, or comparison.

In the case of enrolment, the signal processing subsystem creates a biometric reference. Sometimes the enrolment process requires features from several presentations of the individual's biometric characteristics. Sometimes the *reference* comprises just the *features*, in which case the reference may be called a "template". Sometimes the reference comprises just the sample, in which case feature extraction from the reference occurs immediately before comparison.

In the case of verification and identification, the signal processing subsystem creates a biometric probe.

Sequencing and iteration of the above-mentioned processes are determined by the specifics of each system.

1.2.4 Data storage subsystem

References are stored within an *enrolment database* held in the data storage subsystem. Each reference might be associated with some details of the enrolled subject or the enrollment process. It should be noted that prior to being stored in the *enrolment database*, *references* may be reformatted into a biometric data interchange format. *References* may be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer or local server, or in a central database.

1.2.5 Comparison subsystem

In the comparison subsystem, *probes* are compared against one or more *references* and *comparison scores* are passed to the decision subsystem. The *comparison scores* indicate the similarities or dissimilarities between the *features* and *reference/s* compared. In some cases, the *features* may take the same form as the stored *reference*. For verification, a single specific claim of subject enrolment would lead to a single *comparison score*. For identification, many or all *references* may be compared with the *features*, and output a *comparison score* for each comparison.

1.2.6 Decision subsystem

The decision subsystem uses the *comparison scores* generated from one or more attempts to provide the decision *outcome* for a verification or identification transaction.

In the case of verification, the *features* are considered to *match* a compared *reference* when (assuming that higher scores correspond to greater similarity) the *comparison score* exceeds a specified *threshold*. A biometric claim can then be verified on the basis of the *decision policy*, which may allow or require multiple attempts.

In the case of identification, the enrollee reference is a potential *candidate* for the subject when (assuming that higher scores correspond to greater similarity) the *comparison score* exceeds a specified *threshold*, and/or when the *comparison score* is among the highest ranked values generated during comparisons across the entire database. The *decision policy* may allow or require multiple attempts before making an identification decision.

NOTE Conceptually, it is possible to treat multibiometric systems in the same manner as unibiometric systems, by treating the combined captured biometric *samples/references/scores* as if they were a single *sample/reference/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. (See also ISO/IEC TR 24722:2007 Multimodal and other multibiometric fusion.)

1.2.7 Administration subsystem (Not portrayed in diagram)

The administration subsystem governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

- providing feedback to the subject during and/or after data capture,
- requesting additional information from the subject,
- storing and formatting of the biometric *references* and/or biometric interchange data,
- providing final arbitration on output from decision and/or scores,
- setting *threshold* values,
- setting biometric system acquisition settings,
- controlling the operational environment and non-biometric data storage,
- providing appropriate safeguards for subject privacy, and
- interacting with the application that utilizes the biometric system.

1.2.8 Interface (Not portrayed in diagram)

The biometric system may or may not interface to an external application or system via an Application Programming Interface, a Hardware Interface or a Protocol Interface.

1.3 Functions of general biometric system

1.3.1 Enrolment

In enrolment, a transaction by a biometric capture subject is processed by the system in order to generate and store an enrolment reference for that individual.

Enrolment typically involves:

- sample acquisition,
- sample restoration or enhancement,
- segmentation,
- feature extraction,
- quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require acquisition of further samples),

- reference creation (which may require features from multiple samples), possible conversion into a biometric data interchange format,
- storage,
- test verification or identification attempts to ensure that the resulting enrolment is usable, and
- allowing repeat enrollment attempts, should the initial enrollment be deemed unsatisfactory (dependent on the enrolment policy).

1.3.2 Verification

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g., "I am enrolled as subject X"). The verification function will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). Note that some biometric systems will allow a single subject to enrol more than one instance of a biometric characteristic (for example, an iris system may allow subjects to enrol both iris images, while a fingerprint system may require enrolment of additional fingers for fallback in case a primary finger is damaged).

Verification typically involves:

- sample acquisition,
- sample restoration or enhancement,
- segmentation,
- feature extraction,
- quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- probe creation (which may require features from multiple samples), possible conversion into a biometric data interchange format,
- comparison of the probe against the reference for the claimed identity producing a comparison score,
- determination of whether the biometric features of the probe match those of the reference based on whether the comparison score exceeds a threshold (higher scores correspond to greater similarity), and
- decision to verify claim based on the comparison result of one or more attempts as dictated by the decision policy.

EXAMPLE In a verification system allowing up to three attempts to be compared with an enrolled reference, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled reference for the claimed identity on any of three attempts.

1.3.3 Identification

In identification, a transaction by a subject is processed by the system and the enrolment database is searched to find similar references. Identification provides a candidate list of identifiers that will contain zero, one, or more identifiers. Identification is considered correct when the subject is enrolled, and an identifier for their enrolment is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error).

Identification typically involves:

- sample acquisition,

- sample restoration or enhancement,
- segmentation,
- feature extraction,
- quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- probe creation (which may require features from multiple samples), possible conversion into a biometric data interchange format),
- comparison against some or all references in the enrolment database, producing a score for each comparison,
- determination of whether each compared reference is a potential candidate identifier for the user, based on whether the comparison score exceeds a threshold and/or is among the highest ranked scores returned, producing a candidate list (higher scores correspond to greater similarity), and
- an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.