INTERNATIONAL STANDARD

ISO/IEC 19794-1

First edition
2006-04-01

Information technology — Biometric data interchange formats —

Part 1: Framework

Technologies de l'information — Formats d'échange de données biométriques —

Partie 1: Cadre général

Reference number
ISO/IEC 19794-1:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19794 consists of the following parts, under the general title *Information technology — Biometric data interchange formats*:

— *Part 1: Framework*

— *Part 2: Finger minutiae data*

— *Part 3: Finger pattern spectral data*

— *Part 4: Finger image data*

— *Part 5: Face image data*

— *Part 6: Iris image data*

— *Part 7: Signature/sign time series data*

— *Part 8: Finger pattern skeletal data*

— *Part 9: Vascular image data*

— *Part 10: Hand geometry silhouette data*

The following part is under preparation:

— *Part 11: Signature/sign processed dynamic data*

Introduction

This part of ISO/IEC 19794 is intended to describe the general aspects and requirements for defining biometric data interchange formats.

The notation and transfer formats provide platform independence and separation of transfer syntax from content definition. This part of ISO/IEC 19794 defines what is commonly applied for biometric data formats, i.e. the standardization of the common content, meaning, and representation of biometric data formats of biometric types considered in the specific parts of ISO/IEC 19794.

Figure 1 shows the interrelation of biometric-related ISO/IEC standardization fields. Biometric data complying with a biometric data interchange format of ISO/IEC 19794 represent the core component of biometric interoperability. Biometric formats frameworks such as ISO/IEC 19785 (CBEFF) serve as a wrapper around biometric data. Since biometric data are sensitive data and subject to attack, cryptographic protection is required in interchange environments. Biometric properties with respect to profiles, security evaluation and performance also play an important role. Biometric interfaces are essential to facilitate easy integration and usage of biometric components. The emerging harmonized vocabulary is recommended for use in describing biometric technology. The deployment of applications using biometric verification or identification takes place within the context of societal and cross-jurisdictional requirements.

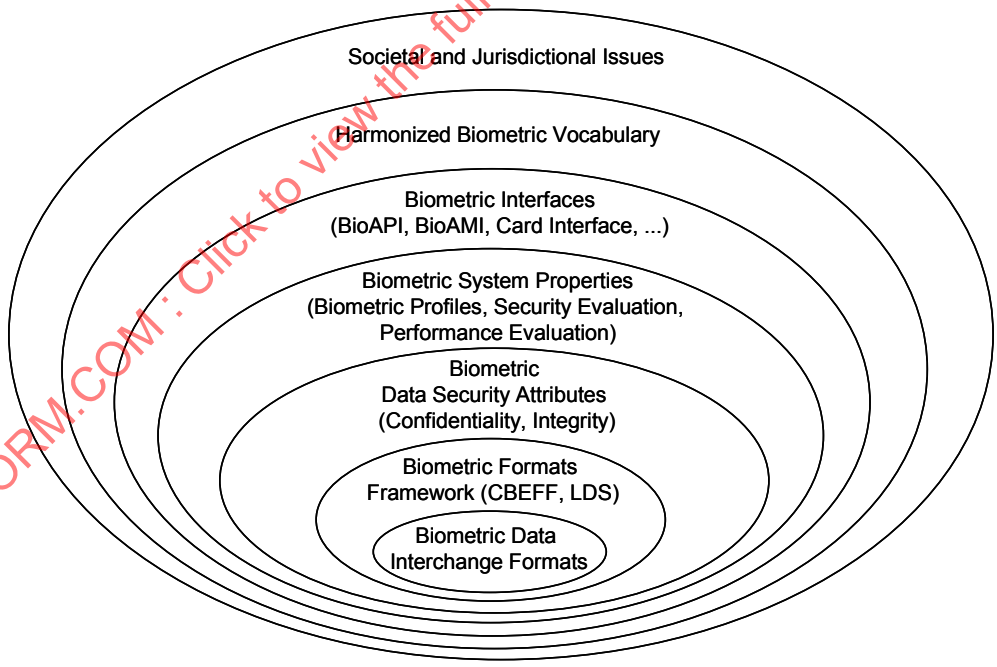

Figure 1 — General interrelation model of biometric issues

Information technology — Biometric data interchange formats —

Part 1: Framework

1 Scope

This part of ISO/IEC 19794 specifies

— general aspects for the usage of biometric data structures,

— the types of biometric data structure,

— a naming concept for biometric data structures,

— a coding scheme for format types.

Biometric data include but are not limited to finger minutiae, finger pattern, finger image, face image, iris image and signature/sign behavioural data.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-11:2004, *Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods*

ISO/IEC 19785-1:—, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification* [1]

ISO/IEC 19785-3:—, *Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specifications* [1]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
biometric
pertaining to the field of biometrics

[1] To be published.

3.2
biometrics
automated recognition of living persons based on observation of behavioural and biological (anatomical and physiological) characteristics

3.3
biometric algorithm
sequence of instructions that tell a biometric system how to solve a particular problem

NOTE A biometric algorithm will have a finite number of steps and is typically used by the biometric system software to decide whether biometric verification or identification data and a biometric template match.

3.4
biometric behavioural data
biometric data resulting from a dynamic action of the user

EXAMPLE data resulting from writing, speaking, or typing

3.5
biometric data
any data representing a biometric characteristic

EXAMPLE sensor data, image data, behavioural data, feature data

3.6
biometric feature
representation of a biometric characteristic that can be used by a biometric algorithm for the purpose of comparing data sets of the same biometric type with each other

NOTE The biometric feature may be composed of individual biometric feature data units.

3.7
biometric feature data unit
smallest individual unit of extracted feature data

EXAMPLE minutia of a fingerprint

3.8
biometric feature extraction
process of converting pre-processed sensor data into a biometric template, verification or identification data so that it can be compared with other extracted feature data

3.9
biometric identification
one-to-many process of comparing submitted biometric data against all records of a database to determine whether it matches and, if so, to identify the respective person

3.10
biometric identification data
data acquired during an identification process for comparison with several biometric templates

3.11
biometric image data
pre-processed biometric data that result from the presentation of a physiological (i.e. static) biometric feature of a user and are represented by pixels in a spatial coordinate system

EXAMPLE fingerprint image data

3.12
biometric information
information needed by the feature extraction and data formatting components of a biometric system to construct the biometric verification or identification data

3.13
biometric template
biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

3.14
biometric sample
information obtained from a biometric device, either directly or after processing

3.15
biometric system
automated system capable of capturing biometric sensor data from a user, extracting feature data from that processed acquired data, comparing the processed feature data with those contained in one or more biometric templates, deciding how well they match, and indicating whether or not an identification or verification of identity has been achieved

3.16
biometric type
type of biometric technology

EXAMPLE fingerprint

3.17
biometric verification
automated process of assessing a claim that submitted biometric sample(s) and a stored biometric template are from the same source

3.18
biometric verification data
data acquired during a verification process for comparison with the biometric template

3.19
enrolment
process of collecting biometric data from a person and the subsequent preparation and storage of biometric templates representing that person's identity

3.20
intermediate biometric sample
biometric sample obtained by processing an acquired biometric sample, intended for further processing

3.21
matching
process of comparing biometric data with a previously stored biometric template and scoring the level of similarity

NOTE An accept or reject decision is then based on whether this score exceeds the given threshold.

3.22
processed biometric sample
biometric sample suitable for comparison

3.23
acquired biometric sample
raw biometric sample
biometric sample obtained directly from an individual by means of a biometric capture device

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

API	Application Programming Interface
BDB	Biometric Data Block
CBEFF	Common Biometric Exchange Formats Framework
IBIA	International Biometric Industry Association
LDS	Logical Data Structure
SB	Signature Block
SBH	Standard Biometric Header

5 General biometric system

5.1 Conceptual diagram 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. Biometric samples are acquired from a subject by a sensor. The sensor output is sent to a processor which extracts the distinctive but repeatable measures of the sample (the "features"), discarding all other components. The resulting features can be stored in the database as a "template", or compared to a specific template, many templates or all templates already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarity between the sample features and those of the template or templates compared.

Figure 2 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, storage, matching and decision subsystems. This diagram

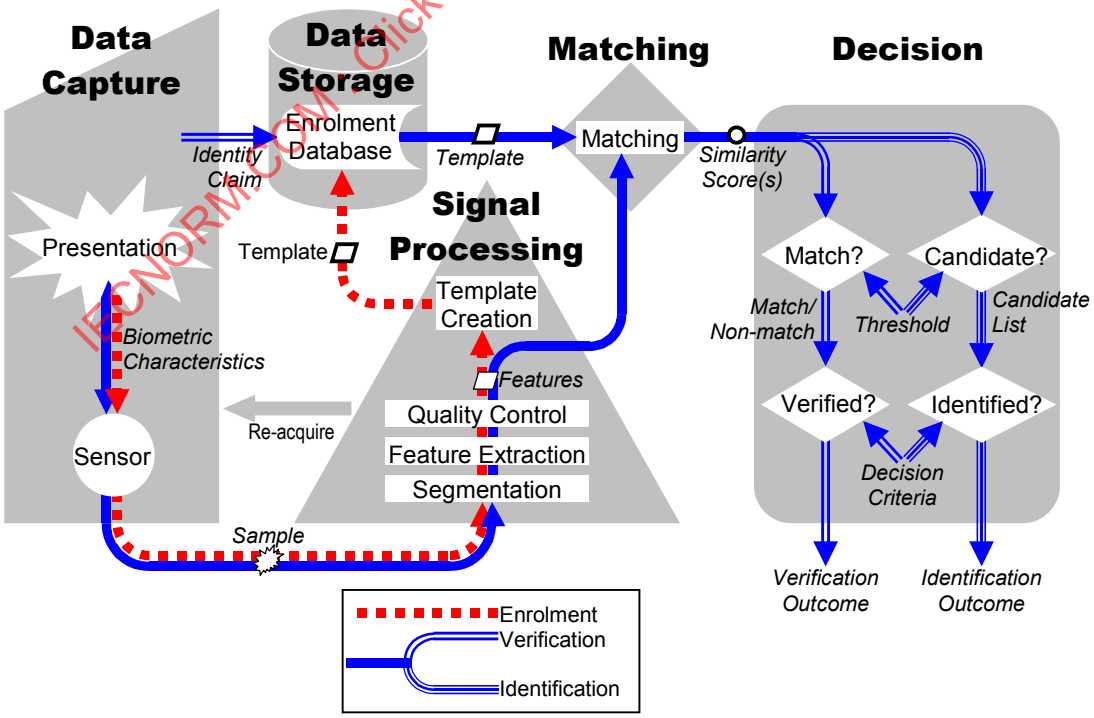

Figure 2 — Components of general biometric system

illustrates both enrolment, and the operation of verification and identification systems. The following subclauses describe each of these subsystems in more detail. It should be noted that, in any real biometric system, these conceptual components may not exist or may not directly correspond to the physical components.

5.2 Conceptual components of a general biometric system

5.2.1 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 *biometric sample*.

5.2.2 Transmission subsystem

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

5.2.3 Signal processing subsystem

The signal processing subsystem extracts the distinguishing *features* from a biometric *sample*. This may involve locating the signal of the subject's *biometric characteristics* within the received *sample* (a process known as *segmentation*), *feature extraction*, and *quality control* to ensure that the extracted features are likely to be distinguishing and repeatable. Should *quality control* reject the received *sample/s*, control may return to the data capture subsystem to collect a further *sample/s*.

In the case of enrolment, the signal processing subsystem creates a *template* from the extracted biometric *features*. Often the enrolment process requires *features* from several presentations of the individual's *biometric characteristics*. Sometimes the *template* comprises just the *features*.

5.2.4 Data storage subsystem

Templates are stored within an *enrolment database* held in the data storage subsystem. Each *template* is associated with details of the enrolled subject. It should be noted that prior to being stored in the *enrolment database*, *templates* may be re-formatted into a biometric data interchange format. *Templates* 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.

5.2.5 Matching subsystem

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

5.2.6 Decision subsystem

The decision subsystem uses the *similarity 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 *template* when the *similarity score* exceeds a specified *threshold*. A claim about the subject's enrolment can then be verified on the basis of the *decision policy*, which may allow or require multiple attempts.

In the case of identification, the enrolee identifier or *template* is a potential *candidate* for the subject when the *similarity score* exceeds a specified *threshold*, and/or when the *similarity score* is among the highest k values generated for a specified value k. The *decision policy* may allow or require multiple attempts before making an identification decision.

NOTE Conceptually, it is possible to treat multi-biometric systems in the same manner as uni-biometric systems, by treating the combined biometric *samples/templates/scores* as if they were a single *sample/template/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate.

5.2.7 Administration subsystem

The administration subsystem (not portrayed in diagram) 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;

— storage and format of the biometric *templates* and/or biometric interchange data;

— provide final arbitration on output from decision and/or scores;

— set *threshold* values;

— set biometric system acquisition settings;

— control the operational environment and non-biometric data storage;

— provide appropriate safeguards for end-user privacy;

— interact with the application that utilizes the biometric system.

5.2.8 Interface

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

5.3 Functions of general biometric system

5.3.1 Enrolment

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

Enrolment typically involves:

— sample acquisition;

— segmentation and feature extraction;

— quality checks, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples);

— template creation (which may require features from multiple samples), possible conversion into a biometric data interchange format and storage;

— test verification or identification attempts to ensure that the resulting enrolment is usable;

— should the initial enrolment be deemed unsatisfactory, repeated enrolment attempts may be allowed (dependent on the enrolment policy).

5.3.2 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"). Verification 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 end-user to enrol more than one instance of a biometric characteristic (for example, an iris system may allow end-users to enrol both iris images, while a fingerprint system may have end-users enrol two or more fingers as backup, in case one finger gets damaged).

Verification typically involves:

— sample acquisition,

— segmentation and feature extraction,

— quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),

— comparison of the sample features against the template for the claimed identity producing a similarity score,

— judgement on whether the sample features match the template based on whether the similarity score exceeds a threshold,

— a verification decision based on the match result of one or more attempts as dictated by the decision policy.

EXAMPLE In a verification system allowing up to three attempts to be matched to an enrolled template, 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 template for the claimed identity on any of three attempts.

5.3.3 Identification

In identification, a transaction by a subject is processed by the system in order to find an identifier of the subject's enrolment. Identification provides a candidate list of identifiers that may be empty or contain only one identifier. 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;

— segmentation and feature extraction;

— quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples);

— comparison against some or all templates in the enrolment database, producing a similarity score for each comparison;

— judgement on whether each matched template is a potential candidate identifier for the user, based on whether the similarity score exceeds a threshold and/or is among the highest k scores returned, producing a candidate list;

— an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

6 Usage context of biometric data interchange formats

The structure and content of biometric data structures for interchange depend on the intended usage context. There may be

— self-contained data structures providing all necessary information;

— data structures designed for the biometric data block of CBEFF not duplicating information which is present in the CBEFF standard biometric header;

— data structures for usage in a Biometric Information Template as defined in ISO/IEC 7816-11 and ISO/IEC 19785-3;

— data structures designed for on-card matching.

CBEFF defines a common set of data elements to support multiple technologies. It describes a biometric information record (BIR) consisting of a standard biometric header (SBH), a biometric data block (BDB) and a security block (SB) as Figure 3 shows. The BDB is the structural unit for the insertion of biometric data interchange formats as defined in ISO/IEC 19794.

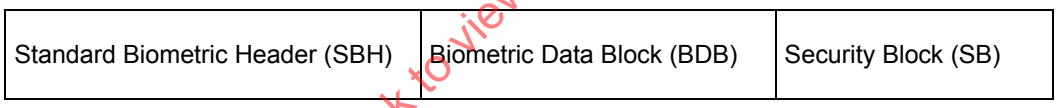

Figure 3 – CBEFF biometric information record (source: ISO/IEC 19785-1)

CBEFF supports patron formats to meet specific application environments. When using smart cards, data structures as defined in ISO/IEC 7816-11 and in the smart card related clauses of ISO/IEC 19785-3 should be used.

7 General aspects of the usage of biometric data for interchange

7.1 Introduction

When using biometric data, the general aspects specified in the following clauses should be taken into consideration.

7.2 Natural variability

Verification data and reference data are generally not identical when performing a matching process. A person will never be able to present exactly the same data again since they depend on a lot of factors where smallest changes (e.g. translation, rotation and distortion of fingers) already result in different data. Therefore it may be necessary to specify together with the biometric data structure specific parameters such as tolerances.

7.3 Aging and usage duration

A couple of biometric features (e.g. facial image or signature dynamics) undergo changes with increasing age of the person. Therefore it is important to specify the principle usage period of biometric reference data or to provide means for adaptation, if appropriate. A validation period as defined by an application provider should be less than or equal to the principle usage period.

7.4 Enrolment conditions

In order to achieve good matching results, it is important to specify enrolment conditions with respect to the minimum quality of the biometric reference data, e.g. minimum number of minutiae or, in the case of image data, minimum focus quality, contrast, resolution, etc.

7.5 Feature extraction algorithms

If biometric data formats for interchange are specified on the feature level (e.g. finger minutiae), then the way for deriving these features shall be specified to the extent necessary to facilitate interoperability, i.e. the matching results of different implementations shall be within the range of allowed differences.

7.6 Feature matching algorithms

If biometric data formats for interchange are specified on the feature level (e.g. finger minutiae), then the means for comparing the biometric verification data against the biometric reference data generated in an enrolment process shall be specified to the extent necessary to facilitate interoperability, i.e. the matching results of different implementations shall be within the range of allowed differences.

7.7 Capture device type ID

The capture device type ID shall be a unique identifier for the type of capture device deployed to acquire a biometric sample. The capture device type ID shall be recorded in two bytes. A value of all zeros indicates that the capture device type ID is unreported. The value "unreported" may not be allowable in some applications. The value field is determined by the vendor possibly depending on requirements for the respective application.

7.8 Multi-modal data structures

If multi-modal biometric systems are used, data structures of several parts of ISO/IEC 19794 may be involved in a verification or identification process.

8 Processing level of data formats for interchange

8.1 Processing levels according to ISO/IEC 19785-1

The processing levels of biometric data as defined in ISO/IEC 19785-1 are the following.

— Acquired data: the data in their raw form as delivered by the sensor.

— Intermediate data: the data have been processed from the form delivered by the sensor, but is not in a form usable for matching – these data are addressed as image data or behavioural data.

— Processed data: the data are in a form that can be used for matching - these data are addressed as feature data.

For interchange, intermediate data (image or behavioural data) and feature data as shown in Figure 4 are of special relevance.

Examples of scenarios using biometric data of different processing level are shown in Annex A.

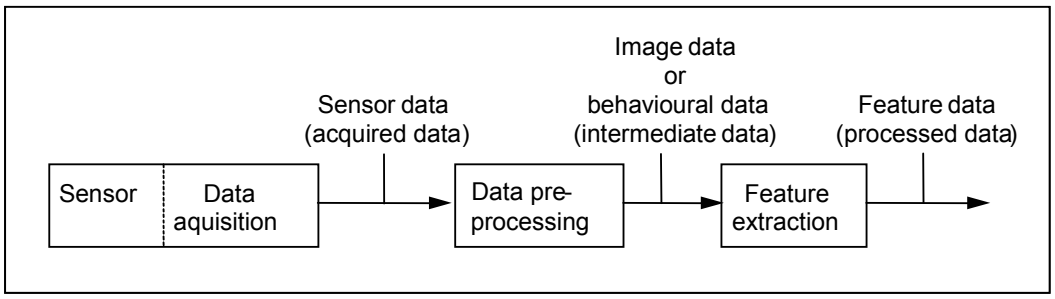

Figure 4 – Sensor data, image/behavioural data and feature data

8.2 Sensor data

The acquired biometric data is influenced by some or all of the following:

— underlying biometric feature;

— presentation of the biometric feature to the sensor;

— data pre-processing (as part of data acquisition) within the sensor device;

— performance of the sensor and sensor device;

— environmental conditions (e.g. lighting, background noise).

Sensor data are usually not used for interchange.

8.3 Image data

In many cases, the acquired biometric data of a static biometric feature delivered by a biometric sensor is sub-sampled, scaled, interpolated, compressed or otherwise processed to produce an image of the feature. The first important convention to be made concerns the general image file format (e.g. BMP, TIFF, GIF, JPEG, JPEG-LS, JPEG2000) and the compression level to make images readable for all systems. Further conventions are needed for certain parameters concerning the image capturing process and the hardware to be used which have a strong impact on the resulting image e.g. grey levels (e.g. 8 bit, 16 bit), image resolution, position of biometric object to be presented, and lighting conditions during image capture process. Each pixel in a monochrome image shall be presented by one or more bytes, so that at least 256 grey levels can be provided. Colour images shall be presented as three or more bytes per pixel, representing red, green, and blue intensities, in that order.

8.4 Behavioural data

In contrast to the acquisition of image data, which captures a static physiological feature like a fingerprint, a behavioural biometric feature is a dynamic action with contributions of conditioned behaviour patterns and physiological features. For behavioural biometric characteristics, common acquisition methods are provided by time based and frequency based analysis. Therefore, the standardization has concentrated on data formats for these approaches.

8.5 Feature data

Feature data may consist of several feature data units. A feature data unit may consist of several data elements, e.g. coordinates and angle. The structure and content of a feature data unit depends on the biometric type.

8.6 Naming concept for biometric data structures

The name of the data structure should contain the information, whether it is related to

— image data, e.g. face image data;

— behavioural data, e.g. signature behavioural data;

— feature data.

Since there may be different feature data structures for the same biometrics, it is recommended to denote the respective feature in the name, e.g. finger minutiae data.

8.7 Requirements for standardizing biometric data formats

The standardization of biometric data formats is intended to provide interoperability. Thus the number of standardized formats should be kept small and manageable. The following qualifications should be considered before a new data format may enter a standardization process:

— the data format represents the basic data of an alternative mathematical approach of feature extraction and/or matching;

— the data format is a prevalent alternative representation of data that is not defined in ISO/IEC 19794;

— the data format represents data of a widely-used biometric type not considered in ISO/IEC 19794 yet;

— the data format represents data of a different processing level and has become widely-used for data interchange or has the potential for it;

— the data format enables interoperability among algorithms that use individual non-standardized data formats of a more advanced processing level;

— the data format drastically reduces the size of data of an already standardized data format and is suitable for usage on card;

— the data format has the potential to be used for different biometric types, e.g. an image format;

— the data format combines existing formats without increasing size;

— the data format allows increase in biometric performance (improvements in terms of error rates).

9 Multi-biometrics

Multi-biometrics can be divided in 3 sub-categories:

— multi-modal – usage of different biometric types such as face and fingerprint;

— multi-algorithmic – usage of two or more distinct algorithms for processing the same biometric sample;

— multi-instance – usage of at least two instances of the same biometric type e.g. left and right iris or left and right pointer finger.

Multi-biometrics may be used to improve the performance of biometric systems in terms of error rates.