DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19795-1

ISO/IEC JTC **1**/SC **37**

Secretariat: **ANSI**

Voting begins on:
2019-11-27

Voting terminates on:
2020-02-19

Information technology — Biometric performance testing and reporting —

Part 1:
Principles and framework

Technologies de l'information — Essais et rapports de performance biométriques —

Partie 1: Principes et canevas

ICS: 35.240.15

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 19795-1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, Biometrics.

This second edition cancels and replaces the first edition (ISO/IEC 19795-1:2006), which has been technically revised.

The main changes compared to the previous edition are as follows:

— Terminology is updated to follow the biometrics vocabulary of ISO/IEC 2382-37:2017;

— Additional detail on testing and reporting of transaction times and computational workload, and on graphical representation of results.

A list of all parts in the ISO 19795 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is concerned solely with the scientific “technical performance testing” of biometric systems and devices. Technical performance testing seeks to determine error and throughput rates, with the goal of understanding and predicting the real-world error and throughput performance of biometric systems. The error rates include both false-positive and false-negative rates, as well as failure-to-enrol and failure-to-acquire rates across the test population. Throughput rates refer to the number of individuals processed per unit time based both on computational speed and human–machine interaction. These measures are generally applicable to all biometric systems and devices. Technical performance tests that are modality-specific — for example, fingerprint scanner image quality — are not considered in this part of ISO/IEC 19795.

The purpose of this part of ISO/IEC 19795 is to present the requirements and best scientific practices for conducting and reporting technical performance testing. It is acknowledged that technical performance testing is only one form of biometric testing. Other types of testing not considered in this part of ISO/IEC 19795 include:

— reliability, availability and maintainability;

— security, including vulnerability;

— conformance;

— safety;

— human factors, including user acceptance;

— cost/benefit;

— privacy regulation compliance.

Biometric technical performance testing can be of three types: technology, scenario and operational evaluation. Each type of test requires a different protocol and produces different types of results. Other parts of ISO/IEC 19795 will provide specific advice and requirements for the development and use of such different test protocols. This part of ISO/IEC 19795 addresses specific philosophies and principles that can be applied over a broad range of test conditions.

Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

1 Scope

This part of ISO/IEC 19795:

— establishes general principles for testing the performance of biometrics systems in terms of error rates and throughput rates for purposes including measurement of performance, prediction of performance, comparison of performance, and verifying compliance with specified performance requirements;

— specifies performance metrics for biometric systems;

— specifies requirements on the recording of test data and reporting of test results; and

— specifies requirements on test protocols in order to:

  — reduce bias due to inappropriate data collection or analytic procedures;

  — help achieve the best estimate of field performance for the expended effort;

  — improve understanding of the limits of applicability of the test results.

This part of ISO/IEC 19795 is applicable to empirical performance testing of biometric systems and algorithms through analysis of the comparison scores and decisions output by the system, without requiring detailed knowledge of the system's algorithms or of the underlying distribution of biometric characteristics in the population of interest.

Not within the scope of this part of ISO/IEC 19795 is the measurement of error and throughput rates for people deliberately trying to subvert the intended operation of the biometric system (e.g., by presentation attacks).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 2382-37:2017 *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2017 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
channel effect
variation of the biometric sample due to sampling, noise and frequency response characteristics of the sensor and transmission channel

3.2
presentation effect
variation of the biometric sample due to the way that biometric characteristics are presented to the sensor

EXAMPLE In facial recognition, this could include pose angle and illumination; in fingerprinting, finger rotation and skin moisture. In many cases, the distinction between changes in the fundamental biometric characteristic and the presentation effects may not be clear (e.g. facial expression in facial recognition or pitch change in speaker verification systems).

3.3
enrolment attempt
sequence of one or more capture attempts with the aim of producing a biometric reference for a capture subject

Note 1 to entry: An enrolment attempt can require a specific number of capture attempts (e.g. three separate placements of a finger on a sensor within a set period), from which the highest quality sample(s) is/are selected for further processing.

3.4
enrolment transaction
one or more enrolment attempts with the aim of producing a biometric reference for a capture subject

Note 1 to entry: If an enrolment attempt fails, further enrolment attempts can be performed within the same enrolment transaction until an attempt succeeds or enrolment is given up.

3.5
test subject
individual whose biometric data is intended to be enrolled or compared as part of the evaluation

3.6
test crew
set of test subjects utilized in an evaluation

3.7
target population
set of biometric data subjects of the application for which performance is being evaluated

3.8
test organization
functional entity under whose auspices the test is conducted

3.9
experimenter
person responsible for defining, designing and analysing the test

3.10
test administrator
person performing the testing

EXAMPLE Staff conducting enrolments or overseeing verification or identification transactions

3.11
test observer
person recording test data or monitoring the test crew

3.12
technology evaluation
offline evaluation of one or more algorithms for the same biometric modality using a pre-existing or specially-collected corpus of samples

3.13
scenario evaluation
evaluation that measures end-to-end system performance in a prototype or simulated application with a test crew

3.14
operational evaluation
evaluation that measures the performance of a biometric system in a specific application environment using a specific target population

3.15
online
pertaining to execution of biometric enrolment or comparison at the time of biometric sample capture

3.16
offline
pertaining to execution of biometric enrolment or comparison of stored biometric data subsequent to biometric sample capture

Note 1 to entry: Collecting a corpus of images or signals for offline enrolment and calculation of comparison scores allows greater control over which probe and reference images are to be used in any transaction.

3.17
closed-set test
test in which the test crew comprises only individuals known to have a reference in the enrolment database

Note 1 to entry: Closed-set tests are a specific type of test for showing performance of identification systems in terms of a cumulative match characteristic (CMC) plot.

3.18
false reject rate
FRR
proportion of biometric transactions with true biometric claims erroneously rejected

3.19
false accept rate
FAR
proportion of transactions with false biometric claims erroneously accepted

3.20
false-negative identification rate
FNIR
FNIR(N,R,T)
proportion of identification transactions by capture subjects enrolled in the system in which the subject's correct identifier is not among those returned

Note 1 to entry: The false-negative identification rate can be expressed as a function of parameters of the identification process for returning matched reference identifiers including rank (R), comparison score threshold (T), and the number of enrolees in the system (N).

3.21
false-positive identification rate
FPIR
FPIR(N,T)
proportion of identification transactions by capture subjects not enrolled in the system, where an identifier is returned

Note 1 to entry: The false-positive identification rate can be expressed as a function of parameters of the identification process for returning matched reference identifiers including comparison score threshold (T), and the number of enrolees in the system (N).

3.22
identification rank
smallest value *k* for which a subject's correct identifier is in the top *k* identifiers returned by an identification system

Note 1 to entry: Identification rank is dependent on size of the enrolment database, and should be quoted "rank *k* out of *n*".

3.23
rank R identification rate
proportion of identification transactions by capture subjects enrolled in the system in which the subject's correct identifier is returned at rank R or stronger

Note 1 to entry: Rank *R* identification rate is dependent on factors including the decision threshold (T) for comparison scores and the number of enrolees in the system (N).

Note 2 to entry: The rank R identification rate and false-negative identification rate FNIR(N,R,T) for the same rank, threshold and number of enrolees in the system sum to 1.

3.24
selectivity
SEL(N,T)
expected number of candidates returned above threshold T in a non-mated search

3.25
computational workload
total computational effort of a single transaction (or set of transactions) in a biometric system, including number of intrinsic operations, execution time, memory requirements, etc.

Note 1 to entry: Computational workload is dependent on the hardware on which the biometric system is operating.

3.26
detection error trade-off
DET
relationship between false-positive and false-negative errors of a binary classification system as the discrimination threshold varies

Note 1 to entry: The DET may be represented as a DET table or a DET plot.

Note 2 to entry: The Receiver Operating Characteristic (ROC) curve was used in the previous version of this part. The ROC is unified with the DET.

3.27
cumulative match characteristic plot
CMC plot
graphical presentation of results of a closed-set test, plotting rank values on the x-axis and the identification rate at each rank on the y-axis

3.28
pre-selection algorithm
algorithm to reduce the number of comparisons that need to be made in an identification search of the enrolment database

3.29
pre-selection error
(pre-selection algorithm) error that occurs when the corresponding subject identifier is not in the pre-selected subset of candidates

Note 1 to entry In binning pre-selection, pre-selection errors happen when the data subject's enrolment reference and a subsequent sample from the same biometric characteristic are placed in different partitions.

3.30
penetration rate
(pre-selection algorithm) average proportion of the total number of references that is pre-selected

4 Conformance

To conform to this part of ISO/IEC 19795, a biometric performance test shall be planned, executed and reported in accordance the mandatory requirements contained herein.

5 General biometric system

5.1 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.* In other cases, the sample itself (without feature extraction) may be stored as the reference. A subsequent *query* or *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.

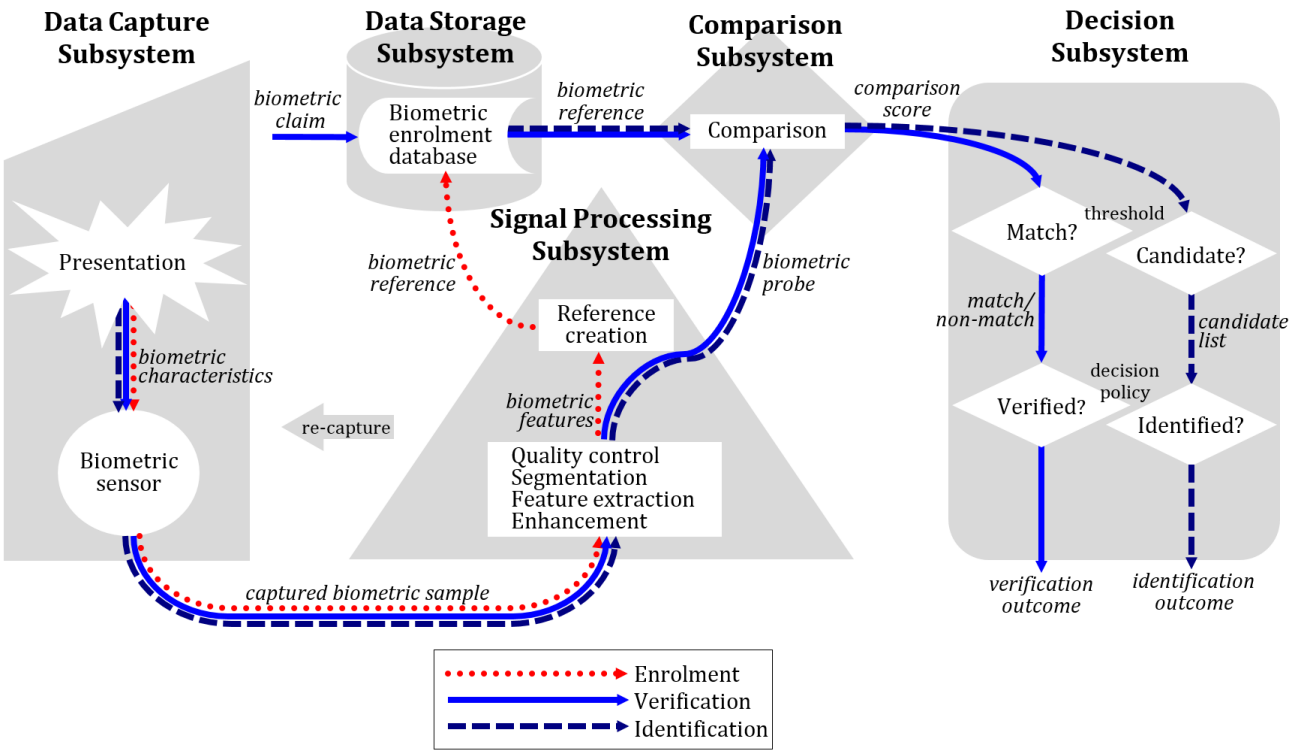

Figure 1 – Components of a general biometric system

Figure 1 illustrates the information flow within a general biometric system 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.

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* presented to the *biometric sensor*, and outputs this image/signal as a *captured biometric sample*.

5.2.2 Transmission subsystem

NOTE Transmission subsystem not portrayed in Figure 1.

The transmission subsystem (not always present or visibly present in a biometric system) will transmit *samples, features, probes, references, comparison scores* and *outcomes* 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.

5.2.3 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 (*recapture*); 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.

5.2.4 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 enrolment 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.

5.2.5 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 *probe(s)* and *reference(s)* compared. 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 *probes*, and output a *comparison score* for each comparison.

5.2.6 Decision subsystem

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

In the case of verification, the *probes* 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.