INTERNATIONAL STANDARD

ISO/IEC 30136

First edition
2018-03

Information technology — Performance testing of biometric template protection schemes

Technologies de l'information — Essais de performance des systèmes de protection par modèle

Reference number
ISO/IEC 30136:2018(E)

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 on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

In conventional biometric access control systems, an adversary who compromises an enrolment database may gain access to the generative biometric data of the individuals enrolled therein. This is undesirable because, if the biometric system is vulnerable to presentation attacks or replay attacks, the adversary could impersonate an individual and gain access to the system after gaining access to the enrolment database. Furthermore, if the biometric enrolment databases contain unprotected templates and the same biometric modality is adopted in multiple applications, the adversary could link the accounts of the individual across those applications (cross-matching).

A biometric template stored in an enrolment database is a reference set of biometric features derived from the biological and behavioural characteristics of an individual. If the system implementation allows it, a biometric enrolment that is known to have been compromised may be revoked and renewed a limited number of times. However, the number of unique biometrics that can be extracted from an individual is limited and thus biometric enrolments cannot be revoked and then re-issued an unlimited number of times like new credit card numbers or passwords. The compromise of biometric enrolment records stored in an enrolment database is a serious issue. Therefore, methods and procedures to mitigate the risk of compromise are needed.

Secure biometric verification

The biometrics research community has invested significant effort in enabling biometric verification without directly needing to store an individual's biometric features in the clear at the access control device. This has led to the development of new methods referred to as “biometric template protection”, “biometric information protection”, or simply “secure biometrics”. In this document, the term “biometric template protection” is used.

The rationale behind this strategy is that, instead of storing the biometric features directly, the access control system derives some data from the biometric features and stores this derived data on the device. During the biometric verification phase, the system receives a probe biometric sample from the individual seeking access. Then, the system combines the probe biometric sample and the derived data and generates a biometric verification decision. The main property of the derived data is that it reveals little or no information about the underlying biometric characteristic that was captured during the enrolment phase.

Thus, if the access control device is compromised by an adversary, only the derived data falls into the hands of the adversary, but this does not enable the adversary to recover the biometric characteristics of the individuals enrolled in the database. Clearly, this strategy protects the privacy of the individuals enrolled in the database.

Further, if an adversary attempts to gain access, i.e. to log in, to the system by providing a fake probe biometric sample, then in a well-designed secure biometric system, combining the fake probe biometric sample with the derived stored data results in biometric verification failure. Thus, this strategy protects the secrecy of the individuals enrolled in the database.

Rationale for new metrics

There are several ways in which biometric template protection can be realized. Some of these methods are described in ISO/IEC 24745:2011. Regardless of the method employed to construct the derived data, the following questions must be asked when evaluating a biometric template protection system:

a) What is the probability that the system rejects genuine individuals and accepts imposters? This is a natural question to ask of *any* biometric verification system. The metrics, False Non-Match Rate (FNMR) and False Match Rate (FMR) measure this performance [ISO/IEC 19795-1] for the conventional biometric system in which enrolment biometric features are matched against probe biometric features. A biometric template protection system will also inherit these metrics, though the method of measuring them may vary depending upon the particular realization of the template protection algorithm.

b) What is the probability that an adversary enhanced with some knowledge about the database of enrolled individuals can be successfully verified as one of those enrolled?

c) How much information can an adversary obtain by compromising an access control device and stealing the derived (stored) enrolment information? In conventional biometric systems, the adversary may obtain significant information, in the form of the stored biometric template, or the stored feature vector. The goal of biometric template protection systems is to ensure that the stored derived data does not leak much information about the enrolled individuals.

d) What is the probability that an adversary, having successfully compromised one or more access control devices and having stolen the data stored on them, uses the information gained to be successfully verified at an access control device?

These questions form the basis for evaluating the accuracy, secrecy, and privacy of a biometric template protection system, which introduces a new set of metrics not previously associated with evaluating traditional biometric systems.

Necessity for standardization

There are several architectures under the umbrella of biometric template protection, e.g., fuzzy vault-based systems, secure sketch-based systems, cancellable biometric systems, secure multiparty computation-based systems, etc. It is necessary to define key metrics that not only answer the questions posed above, but also apply to a wide variety of biometric template protection architectures, thereby providing a common basis for comparison of systems based on different architectures. The goal of this document is to specify new metrics for evaluating template protection-based biometric verification and identification systems. Theoretical and empirical definitions are provided for each metric in Clause 8.

Information technology — Performance testing of biometric template protection schemes

1 Scope

This document supports evaluation of the accuracy, secrecy, and privacy of biometric template protection schemes. It establishes definitions, terminology, and metrics for stating the performance of such schemes. Particularly, this document establishes requirements for the measurement and reporting of:

- theoretical and empirical accuracy of biometric template protection schemes,
- theoretical and empirical probability of a successful attack on biometric template protection schemes (single or multiple), and
- the information leaked about the original biometric when one or more biometric template protection schemes are compromised.

This document also gives guidance on measuring and reporting diversity and unlinkability of templates.

This document does not:

- establish template protection schemes;
- address testing of traditional encryption schemes.

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 19795-1, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 24745:2011, *Information technology — Security techniques — Biometric information protection*

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 24745 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
accuracy degradation
difference in FNMR/FMR (or FAR/FRR) for a biometric system tested both with and without template protection schemes

3.2
adversary
one who compromises an enrolment database and may gain access to the generative biometric data of the individuals enrolled therein

3.3
biometric template protection
protection of biometric references under various requirements for secrecy, irreversibility, and renewability during storage and transfer

3.4
generative biometric data
biometric data (sample(s) or features) used as primary input to the biometric template protection scheme

3.5
irreversibility
property of a transform that creates a biometric reference from generative biometric data such that knowledge of the transformed biometric reference cannot be used to determine any information about the generative biometric data

Note 1 to entry: Metrics introduced by this document aim to measure irreversibility by the degree of difficulty faced by an adversary in recreating an original unprotected version of the biometric data.

3.6
privacy compromise
event in which an adversary discovers part of the generative biometric data of an individual enrolled in the database of a biometric verification or identification system

Note 1 to entry: Discovery of part of the generative biometric data does not mean that successful biometric recognition is achieved, i.e. biometric system secrecy is not compromised by the discovery itself.

3.7
privacy leakage
<template protection scheme> amount of information about an individual‘s generative biometric data which an adversary can learn from the stored reference data

3.8
pseudonymous identifier comparator
system, process or algorithm that compares the pseudonymous identifier generated during enrolment by the pseudonymous identifier encoder and the pseudonymous identifier reconstructed during verification by the pseudonymous identifier recoder, and returns a similarity score representing the similarity between the two

3.9
pseudonymous identifier recoder
system, process or algorithm that reconstructs a pseudonymous identifier based on the provided auxiliary data and the extracted features

3.10
secrecy
degree of difficulty faced by an adversary in determining input data, from a protected biometric template, that achieves biometric recognition, when impersonating an individual enrolled in the biometric enrolment database of a template protection system

3.11
secrecy compromise

event in which an adversary achieves biometric recognition when impersonating an individual enrolled in the biometric enrolment database of a template protection system

Note 1 to entry: Secrecy compromise includes the case in which the adversary gains unlawful access without necessarily discovering the generative biometric data of the individual being impersonated, i.e. the case in which the adversary remains unable to cause a privacy compromise.

3.12
successful attack rate

probability that an informed adversary can obtain a false accept result in a biometric system

Note 1 to entry: An informed adversary is one that has compromised (gained access to) a subset of the biometric enrolment database and the secret parameters (if any) associated with one or more biometric recognition systems (potentially including the target system under consideration) in which common individuals are enrolled.

3.13
template diversity

expected value of the number of independent protected templates that can be generated from a given generative biometric data by a biometric template protection scheme

3.14
template size

size of stored reference data

3.15
unlinkability

property of two or more biometric references that they cannot be linked to each other or to the subject(s) from which they were derived

4 Abbreviated terms

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

AD	Auxiliary Data
BTP	Biometric Template Protection
ECC	Error Correcting Code, or Error Correction Coding
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
H(X)	Information-theoretic Entropy of a random variable X
H(X | Y)	Conditional entropy of random variable X given random variable Y
I(X; Y)	Mutual information between random variables X and Y
PI	Pseudonymous Identifier
PIC	Pseudonymous Identifier Comparator
PIE	Pseudonymous Identifier Encoder

PIR	Pseudonymous Identifier Recoder
RBR	Renewable Biometric Reference
SAR	Successful Attack Rate

5 Conformance

To conform to this document, evaluations of the accuracy, secrecy and privacy of biometric template protection schemes shall conform to Clause 8.

6 Methods for biometric template protection (informative)

6.1 General

In this document, biometric template protection refers to the category of techniques that perform biometric verification or identification without storing the enrolment template, whether “in the clear” or encrypted via traditional means. Instead, the captured biometric sample is transformed in an irreversible fashion and the transformed result is stored in the database of enrolled individuals. If an adversary gains access to the database, only the transformed data is accessible, which has two beneficial properties:

a) The stored data for an enrolled individual may reveal partial information about the features extracted from the individual’s biometric sample, but it does not contain enough to reconstruct the individual’s biometric characteristics.

b) It is more difficult for the adversary to achieve biometric recognition when impersonating an individual enrolled in the enrolment database compared to systems that do not employ template protection schemes. Thus, biometric template protection provides improved secrecy for individuals enrolled in the system.

The extent of irreversibility and secrecy depends on a variety of factors, such as the type of biometric characteristic used, the feature extraction algorithm employed to extract a digital representation of the biometric signal, the mechanism used to provide template protection, and the use of optional secret keys as a second factor of secrecy. Providing increased irreversibility and secrecy may come at the cost of reduced biometric verification accuracy. In order to be able to study and analyze the various performance aspects of biometric template protection systems, it is necessary to precisely characterize the various dimensions of accuracy, secrecy and irreversibility. In this clause, a generalized architecture for biometric template protection systems is presented. Using this generalized architecture, metrics that quantify the accuracy, secrecy and irreversibility are defined in Clause 8.

Figure 1 illustrates the information flow within a general unprotected-template biometric system, from ISO/IEC/TR 24741:2018, Clause 6. Explanations about subsystems can be found in ISO/IEC/TR 24741:2018, Clause 6.

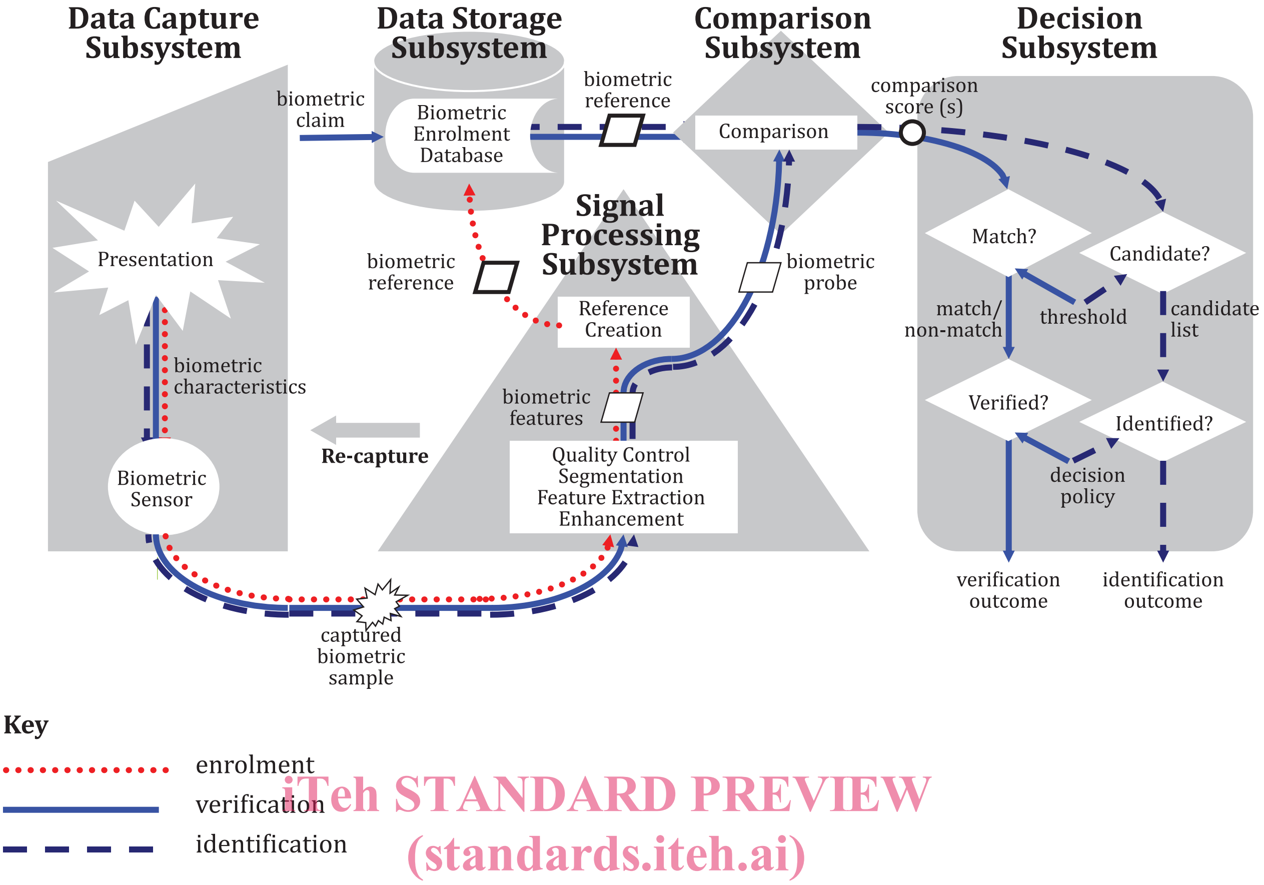

Figure 1 — Components of a conventional biometric system

6.2 Generalized architecture for biometric template protection system

Figure 2 illustrates the information flow within a general template protection biometric system, which can be regarded as an extended system of an unprotected-template biometric system described in Figure 1.

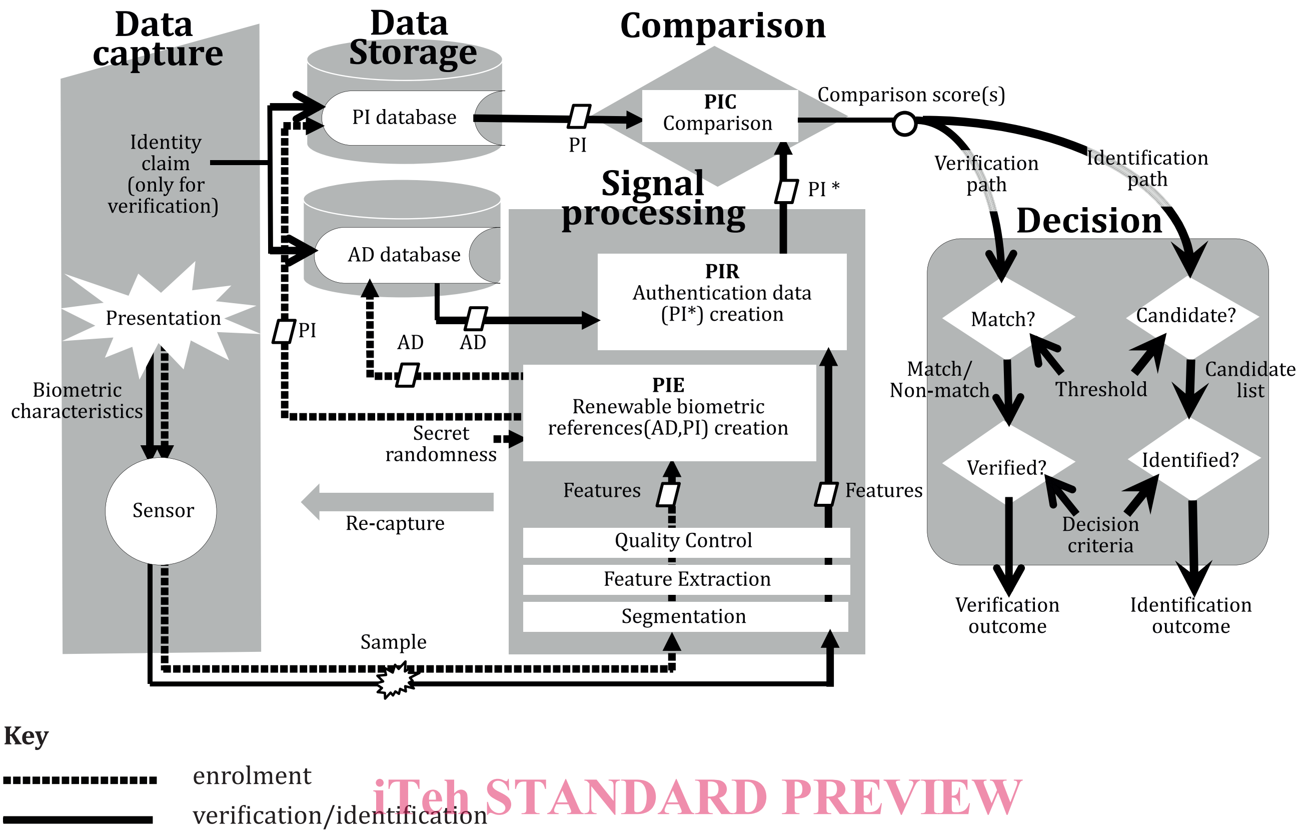

Figure 2 — Components of a general biometric template protection system

NOTE Figure 2 represents components for typical verification/identification systems and does not cover a general identification scenario that could directly execute a 1 vs N comparison (not N times 1 vs 1). In a general 1 vs N identification system, the algorithm PIR can take multiple ADs as input and output multiple PI*s, and the algorithm PIC can take multiple PIs or PI*s as input.

The main difference between the conventional biometric system in Figure 1 and the template protection system in Figure 2 is that the Pseudonymous Identifier Encoder (PIE) generates Auxiliary Data (AD) and Pseudonymous Identifier (PI) from the extracted biometric features during enrolment. A pair of AD and PI is called a Renewable Biometric Reference (RBR). A Pseudonymous Identifier Recoder (PIR) generates a different PI (labelled PI*) from an enrolled AD and the extracted biometric features during verification or identification. A Pseudonymous identifier Comparator (PIC) compares PI and PI*. The definitions of AD, PI, RBR, PIE, PIR and PIC can be found in ISO/IEC 24745:2011, Clause 2 and 5.2.3.

In the following, the algorithms executed in the PIE, PIR and PIC modules are formally redefined in compliance with ISO/IEC 24745:2011[18]. Let U be a set consisting of all individuals' biometric characteristics. Assuming that biometric features are extracted from an acquired sample during enrolment, verification/identification can be represented as an element $\boldsymbol{x}$ of a space M and PI, AD and PI* are represented elements of spaces M_{PI}, M_{AD} and M^{*}_{PI}.

A tuple of the three algorithms, PIE, PIR and PIC, described below, is then called a biometric template protection (BTP) algorithm.

- A PIE that takes generative biometric data $\boldsymbol{x} \in M$ and a randomness as input and returns a pair (α, π) of an AD $\alpha \in M_{\mathrm{AD}}$ and a PI $\pi \in M_{\mathrm{PI}}$. In Figure 2, the PIE can be regarded as a creation module for the Renewable biometric references (AD, PI).

- A PIR that takes as input an auxiliary data α and generative biometric data $\boldsymbol{x}' \in M$ and returns a PI $\pi' \in M^{*}_{\mathrm{PI}}$ for verification or identification. In Figure 2, the PIR can be regarded as a creation module for the authentication data (PI*) creation module.