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)

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 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*