TECHNICAL SPECIFICATION

ISO/IEC TS 22604

First edition

Information technology — Biometric recognition of subjects in motion in access-related systems

Technologies de l'information — Reconnaissance biométrique de sujets en mouvement dans les systèmes d'accès

PROOF/ÉPREUVE

Reference number
ISO/IEC TS 22604:2023(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO 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) or www.iec.ch/members_experts/refdocs).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents or the IEC list of patent declarations received (see patents.iec.ch). ISO shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

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 and www.iec.ch/national-committees.

Introduction

The purpose of this document is to provide guidance on the use of in-motion biometric recognition technologies in access-related systems, where the previous enrolment and management of the identity of individuals needing access is required.

To satisfy increasing security demands, biometric recognition technologies are used in access-related systems to provide a more robust approach to identity authentication, and to mitigate security risks. However, this can come at a cost of increased processing times and lead to delays in user identification or verification.

Biometric identification and verification should be comprehensive and flexible for effective use in an access-related environment. Solutions should reduce user burden, be easy to manage, cost effective, maintain the security requirements, and provide permission-based access and global interoperability as necessary. Biometric systems should effectively allow authorized users' access, incorporate mechanical and behavioural mechanisms to refer unenrolled persons to human personnel and alert facilities to unauthorized users attempting to gain access. Systems should also provide a seamless, accurate and non-invasive user experience.

Considerable improvements in the performance of in-motion biometric recognition, have resulted in applications that enable automated, convenient and non-intrusive face, iris or fingerprint recognition across a range of scenarios including border control, passenger flow facilitation, access control and work place time and attendance. This provides a positive and non-intrusive user experience, as the user does not need to carry anything or stop and stand still to be recognized and does not need to touch anything.

There are several considerations that are unique to in-motion biometric solutions for design of contactless biometric recognition systems. Design considerations include:

— Selection and placement of biometric data capturing devices (e.g. cameras).

— Control of the flow of individuals requiring access to ensure that only those that are authorized gain access.

— Proximity of capture devices to individuals seeking access for the contactless in-motion capture of the needed information. The proximity of the biometric capture devices can depend on the employed biometric modalities.

— Management of exceptions.

— Mutual placement of capture devices and equipment dedicated to physical access-control (e.g. door, barrier, turnstile).

A number of use cases involving in-motion biometrics address different scenarios including:

— where access is on the basis of the prior enrolment of all individuals well in advance of interacting with the biometric system (identification);

— where access is on the basis of credentials presented just prior to interacting with the biometric system (verification) (e.g. wireless technology, RFID token or a vehicle number plate or any other token available without any interruption to the person's flow of movement).

These scenarios present different challenges to in-motion verification and identification processes.

Critical to the success of biometrics-based secure access is implementation of state-of-the-art data protection technology and procedures (see ISO/IEC 20889[1] on privacy enhancing data de-identification techniques, according to the privacy principles established in ISO/IEC 29100,[3] taking into account legal, common practice, business, industry and privacy considerations).

An important factor in in-motion biometric recognition is its ability to sense/detect presentation attacks per ISO/IEC 30107-3.[5]

Information technology — Biometric recognition of subjects in motion in access-related systems

1 Scope

This document establishes requirements for development of biometric solutions for verification and identification processes for secure access without physical contact with any device at any time. The solution acquires the biometric characteristics that are captured while the data subjects are in motion to verify or identify the individuals requiring access, and thus controlling access using contactless biometrics.

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, *Information technology — Vocabulary — Part 37: Biometrics*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1 and the following apply.

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

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

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

3.1
in-motion identification
identification for which a person in motion can be identified without physical contact with any device at any time

3.2
non in-motion identification
identification for which a person needs to stop to be identified

3.3
in-motion verification
verification for which a person in motion can be verified without physical contact with any device at any time

3.4
recognition area
area where biometric characteristics are captured and biometric recognition can be performed

3.5
attraction point
distraction in the field of view of the people in the recognition area that pulls the attention of the people making them look in a specific direction

3.6
access point
location, typically with a physical barrier, where users are identified and pass through to enter an access-controlled area

3.7
feedback signal
signal for the identified user providing him or her information on the status of his or her access authorization

3.8
authorized user list
list containing the information and biometrics for identifying authorized users

3.9
unauthorized user list
list containing the information and biometrics for identifying unauthorized users

3.10
alert list
list containing the information and biometrics for identifying unauthorized users for which an alert needs to be raised in case of identification

4 Biometric recognition in motion

4.1 General

4.1.1 Purpose and constraints of in-motion biometric system

In-motion access-related systems allow users to be identified without stopping and without any physical contact with any device. The targeted optimal solution should be handled to grant access to an area using biometrics without asking the users to perform any specific action and without any additional constraint on them compared to a crossing without biometric identification. However, the live biometric data needed to identify the users should be as good as possible to avoid a false rejection, and this tends to add constraints on the users (e.g. look in a specific direction, perform a specific action like removing their glasses). At the end, it is all about the user experience; additional constraints on how to behave while crossing the access control point are bad for the user experience. One of these constraints is to be obliged to stop, and in-motion systems try to remove it. But a false rejection of an authorized user is also a very bad experience for them and should be avoided in any case. Therefore, there is a trade-off to find between a complete freedom of movement and behaviour and the constraints added to the user to get captured with good quality images. One positive aspect is that, in the authorized user list use case, the biometric capture subject wants to get access to the secured area protected by the biometric check and can be expected to be more or less cooperative. In this case, there is definitely a way to provide a good user experience with an in-motion system with low FTA and low FRR.

A biometric system can be considered in-motion when subjects do not stop/pause for the biometric capture process. They can slow down and perform few actions (without any physical contact with a sensor). It is not required that all authorized users cross the access control point without stopping but most of them should be able to. The operator should decide the trade-off between convenience and security depending on the application.

Systems for secure and effective recognition of individual people are essential for the management of many types of facilities, including office buildings, residential facilities, private clubs, campuses and other locations that include sensitive and/or private assets. They are also needed to secure borders.

There are three cases used to recognize users for access-related applications:

— biometric verification of a provided credential;

— biometric identification against a database of pre-enrolled people;

— multi-factor authentication using biometrics for identification and for verification and a token as a secondary means of authentication.

From the viewpoint of user actions, there are:

— non in-motion identification or verification – the user is required to stop in the recognition area to be properly identified or verified;

— in-motion identification or verification - as the user is approaching an access point from a distance, he or she is identified or verified without any stop or physical contact with any device.

4.1.2 Biometric performance and error rate

The challenge for in-motion access-related systems is to limit the increase of false rejection due to the lower quality of the images captured in motion compared to non in-motion systems. This can be achieved by different means like using more robust detection and matching algorithms, dedicating the hardware to in-motion capture, ensuring the quality of the enrolment data, putting constraints on the environment, improving the user interface and overall ergonomics or even limiting the database size.

Like for all biometric systems, biometric accuracy of in-motion system needs to be expressed in terms of failure to acquire rate (FTAR), a false acceptance metric (FMR for verification system, FPIR for identification) and a false rejection metric (FNMR in verification, FNIR in identification). The specificities of in-motion biometric systems actually concern the FTAR and the FNMR/FNIR, but should have no impact on the security level, meaning the FMR/FPIR.

The technical levers include:

— more robust detection (improve FTAR) and biometric comparison algorithms (improve FNMR/FNIR);

— dedicating the hardware to in-motion capture (improve on FTAR and FNMR/FNIR, see 4.1.3);

EXAMPLE The system uses camera with smaller shutter speed or higher frame per second rate. The camera is motorized to focus on a refined region of interest.

— ensuring the quality of the enrolment data (improve on FNMR/FNIR, see 4.5);

— putting constraints on the environment as lighting (improve on FTAR and FNMR/FNIR);

EXAMPLE With a shutter speed optimized for in-motion capture, a too dark acquisition environment results in weak signal.

— optimizing the database size (improve FNIR);

EXAMPLE Dataset is carefully maintained in order to only have the relevant and current users registered for a specific access control point.

— improving the user interface and overall ergonomics (improve FTAR, see Clause 5);

— improving mutual placement of capture device and equipment dedicated to physical access control (e.g. door, barrier, turnstile) (improve FTAR, see 4.6.1).

4.1.3 Quality/speed compromise

For many biometric modalities, the quality of a sample captured in motion is lower than that of a sample captured without motion. This assumption is valid for several reasons:

— For photographic reasons, images taken in motion can be darker, less contrasted, with lower resolution, and noisier than the static images. For instance, for in-motion biometric capture, it is interesting to have a large depth of field (get a focused image in a wide depth range in order to maximize the number of images that can be used for biometric feature extraction) and then decrease

the aperture. In the same time, motion blur should be avoided, and a small shutter value should be used.

EXAMPLE 1 When the acquisition is performed in motion for face recognition modality, good practice to prevent motion blur is to use a shutter speed from 1/125 s to 1/50 s for a normal walking rate of around 1 m/s to 1,5 m/s. These two settings decrease the amount of light coming on the photographic sensor and then produce darker and less contrasted images. A way to get brighter images is to illuminate the scene more strongly but there are limitations on user acceptance and experience. Another way is to use higher ISO values, but this will bring electronic noise on the captured image. As the images can be captured from a longer distance than in static mode where the user is standing in front of the biometric capture device, resolution can also be smaller, decreasing the global quality of the biometric data.

EXAMPLE 2 For face recognition modality, good practice regarding resolution is 10 pixels per centimetre on the face.

— Time to acquire a valid image is much smaller in motion than statically. When the user stops and looks at the device, or places their finger on a sensor, there is time to choose images of sufficient quality while the user doesn't move. In opposite, in the in-motion biometric capture, the user is moving during the acquisition and the biometric decision should be taken at the latest when the biometric capture subject reaches the access point.

— Considering that the system should be as seamless as possible, the available images that are valid for a biometric comparison are much fewer because the user has very limited interaction with the biometric capture device. Even in a cooperative case, the main purpose of an in-motion system is to have as low impact as possible on the user normal behaviour, thus leading to few exploitable images.

The challenge for in-motion access-related systems is then to limit the increase of false rejection rate, due to the lower quality of the images captured in motion:

— more robust algorithm able to deal with various acquisition environments and behaviours from data capture subject;

— capture device hardware improvement;

— constraints on the capturing environment;

— ergonomics/user interface;

— limitation of the database size.

4.2 Biometric verification vs. biometric identification

4.2.1 Implementing an in-motion verification system

When implementing biometric verification, the way to provide the biometric reference shall be specified. The individual can provide directly the reference biometric data to the system (for instance, presenting a smartcard or other token where the biometric reference is stored or scanning a 2D barcode containing a biometric template), or use credentials allowing the access to the reference biometric data stored in a database (using a contactless card or a PIN code). These examples show interactions of the user with a reading device, which is not compatible with a fully contactless and in-motion access control system. However other solutions can be implemented to keep a seamless use of an in-motion access control system in verification mode.

The idea is to design an access control system which is able to retrieve biometric reference data from the user without any action from the user approaching the system. Such a system should be able to sense the user when he/she is in a predefined area around, and to retrieve the necessary reference data for future use. This can be achieved by a wireless connection between the system and a token possessed by the user, which can be any connected device.

EXAMPLE The token is a smartphone.

When the user approaches the system, the token is detected and starts communicating with the system, exchanging the necessary data even before the live user biometrics is captured. When closer to the access control point, the live user biometrics is captured, and compared against the reference data (biometric verification). If access is granted, the user can go through without stopping and touching anything.

If multiple tokens can be present and detected at the same time with ambiguity about which one belongs to the individual trying to gain access, some mechanisms need to be implemented.

The live biometrics should be matched against the closest one, but can also be matched against the reference data of all detected present users, giving access if one of them is considered as genuine. The sensing area should be small enough to avoid that too many users are considered as possible candidates, but needs to be large enough to detect users as early as possible to allow in-motion, no stop access.

4.2.2 Implementing an in-motion identification system

When the biometric capture subject approaches the access point, biometric probes are captured and searched against the reference database (biometric identification). The identification system should be configured such that the candidate list includes only candidates whose similarity score exceeds an acceptance threshold. If access is granted, the user can go through the access point without stopping and touching anything.

4.3 Process flow in access-related systems

Possible process flows include:

- All users are authorized if the biometric data quality is good and the user was not identified in the unauthorized user list.
- Only users in the authorized user list are accepted.
- Both authorized and unauthorized user lists exist in the system. Operators should decide what to do when a user is identified in both lists.
- Users on an alert list signal an alert. Additionally, system operator can treat alert list as authorized user list or as unauthorized user list.

For unattended systems, it should be defined by system policy whether alerts should be raised to an operator, just logged in a system log or both.

4.4 Applicable biometric modalities

4.4.1 General

In-motion biometric recognition can be based on any information obtained in a contactless/touchless way and supporting natural human behaviour. Different biometric modalities can be used, such as for example face, periocular region, hand/finger, iris, gait/anthropometrics, voice or a combination of modalities.

4.4.2 Face modality

The use of the face for in-motion biometric recognition is natural and contactless, with no physical interaction with the sensors, as a simple glance in the general direction of the capture device is generally enough.

This is the most common biometric modality for such a system. Facial image capture is non-intrusive, quite easy to achieve, and user acceptance is high.