Technical Specification

ISO/IEC TS 22604

Second edition
2024-12

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

Reference number
ISO/IEC TS 22604:2024(en)

Contents

Page

Foreword .... **iv**

Introduction .... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Biometric recognition in motion **2**
- 4.1 General 2
  - 4.1.1 Purpose and constraints of in-motion biometric systems 2
  - 4.1.2 Biometric performance and error rate 3
  - 4.1.3 Quality/speed compromise 3
- 4.2 Biometric verification vs. biometric identification 4
  - 4.2.1 Implementing an in-motion verification system 4
  - 4.2.2 Implementing an in-motion identification system 5
- 4.3 Process flows in access-related systems 5
- 4.4 Applicable biometric modalities 5
  - 4.4.1 General 5
  - 4.4.2 Face modality 5
  - 4.4.3 Iris modality 5
  - 4.4.4 Fingerprint modality 6
  - 4.4.5 Palm modality 6
  - 4.4.6 Complementary modalities 6
- 4.5 Enrolment and quality 6
- 4.6 Ergonomics 6
  - 4.6.1 Capture device physical placement 6
  - 4.6.2 Catch attention 7
  - 4.6.3 Feedback signal 7
- 4.7 Biometric information storage 7

5 Accessibility, usability and guidance **7**
- 5.1 General 7
- 5.2 Accessibility 8
- 5.3 Usability 8
- 5.4 Acceptable delay for a user for fluid passage 8
- 5.5 Guidance 9

6 Privacy and security considerations **9**
- 6.1 Data protection 9
- 6.2 Consent 9
- 6.3 Presentation attack detection 10
- 6.4 Security considerations 10

7 Examples of deployment **10**
- 7.1 General 10
- 7.2 Use cases 11
  - 7.2.1 Example of system with fingerprint 11
  - 7.2.2 Example of system with multimodal biometrics 11

Bibliography **15**

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.

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC 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 and https://patents.iec.ch. ISO and IEC 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*.

This second edition cancels and replaces the first edition (ISO/IEC TS 22604:2023), which has been technically revised.

The main change is as follows:

— minor editorial modifications have been made in order to use more inclusive language.

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 management and prior enrolment 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 can 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 and cost effective, maintain security requirements, and provide permission-based access and global interoperability as necessary. Biometric systems should effectively allow access to authorized users, 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 monitoring workplace 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 the 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 who are authorized gain access;

— proximity of capture devices to individuals seeking access for the contactless in-motion capture of the necessary information;

  NOTE 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 those in which:

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

— access is based on credentials presented just prior to interacting with the biometric system (verification) [e.g. wireless technology, radio frequency identification (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 the implementation of state-of-the-art data protection technology and procedures (see ISO/IEC 20889 on privacy-enhancing data de-identification techniques, according to the privacy principles established in ISO/IEC 29100, taking into account legal, common practice, business, industry and privacy considerations).

An important factor in in-motion biometric recognition is the ability to sense/detect presentation attacks according to ISO/IEC 30107-3.

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

1 Scope

This document establishes requirements for the development of biometric solutions for verification and identification processes for secure access without physical contact with any device at any time. The solutions acquire biometric characteristics that are captured while the data subjects are in motion to verify or identify the individuals requiring access, 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 biometric capture subjects in the recognition area that pulls their attention, 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 users, providing them information on the status of their 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 systems

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 function in such a way as to grant access to an area using biometrics without asking 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 for the users (e.g. looking in a specific direction, performing a specific action like removing their glasses). The key concern is 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 being obliged to stop; in-motion systems try to avoid this. But a false rejection of an authorized user is also a very bad experience for them and should also be avoided. Therefore, there is a trade-off to be found between complete freedom of movement and behaviour, and the constraints placed on users to ensure that they are captured with good quality images. One positive aspect is that in scenarios using an authorized user list, the biometric capture subject wants to gain access to the secured area protected by the biometric check and can therefore be expected to be relatively cooperative. In this case, a good user experience can be provided with an in-motion system with low failure to acquire rate (FTAR) and low false reject rate (FRR).

A biometric system can be considered in-motion when subjects do not stop or pause for the biometric capture process. They can slow down and perform a 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 do so. The operator should decide on the trade-off between convenience and security, depending on the application.

Systems for secure and effective recognition of individuals 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 procedures used to recognize users for access-related applications:

— biometric verification of a provided credential;

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

— 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, the following types of identification and verification exist:

— 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, the user 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, e.g. using more robust detection and comparison 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.

As for all biometric systems, biometric accuracy of in-motion systems needs to be expressed in terms of FTAR, a false acceptance metric [false match rate (FMR) for verification system, false positive identification rate (FPIR) for identification] and a false rejection metric [false non-match rate (FNMR) in verification, false negative identification rate (FNIR) for identification]. The specificities of in-motion biometric systems concern the FTAR and the FNMR/FNIR, but should have no impact on the security level, i.e. the FMR/FPIR.

The technical levers include:

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

— dedicating the hardware for in-motion capture (improves FTAR and FNMR/FNIR, see 4.1.3);

EXAMPLE 1 The system uses a camera with a 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 (improves FNMR/FNIR, see 4.5);

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

EXAMPLE 2 With a shutter speed optimized for in-motion capture, an acquisition environment with insufficient lighting results in weak signal.

— optimizing the database size (improves FNIR);

EXAMPLE 3 The 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 (improves FTAR, see Clause 5);

— improving mutual placement of capture device and equipment dedicated to physical access control (e.g. door, barrier, turnstile) (improves 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. At 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 typical 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. One method of achieving brighter images is to illuminate the scene more strongly, but this implies limitations on user acceptance and experience. Another method 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 cm 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 is not moving. On the contrary, with 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.

— As the system is intended to be as seamless as possible, and the user has very limited interaction with the biometric capture device, fewer images that are valid for a biometric comparison are available. Even in a cooperative case, the main purpose of an in-motion system is to have minimal impact on the users' usual behaviour, thus leading to fewer exploitable images.

The challenge for in-motion access-related systems is therefore to limit the increase in the false rejection rate, due to the lower quality of the images captured in motion. Solutions can include the following:

— a more robust algorithm capable of dealing with various acquisition environments and behaviours from data capture subjects;

— improvements in the capture device hardware;

— constraints on the capturing environment;

— improvements in ergonomics/the 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 method of providing the biometric reference shall be specified. The individual can provide the reference biometric data to the system directly (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 access to the reference biometric data stored in a database [using a contactless card or a personal identification number (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 maintain a seamless use of an in-motion access control system in verification mode.

The aim 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 the user is in a predefined area, and 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 can be 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 are captured. When the user moves closer to the access control point, the live user biometrics are captured and compared against the reference data (biometric verification). If access is granted, the user can continue through without stopping and touching anything.