International Standard

ISO/IEC 30137-1

Information technology — Use of biometrics in video surveillance systems —

Part 1: System design and specification

Technologies de l'information — Utilisation de la biométrie dans les systèmes de vidéosurveillance —

Partie 1: Conception et spécification

Second edition
2024-03

Reference number
ISO/IEC 30137-1:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **2**
3 Terms and definitions **2**
3.1 Terms related to the target subject 2
3.2 Terms related to VSS 2
3.3 Terms related to biometric systems 4
3.4 Terms related to the environment and scenario 4
3.5 Symbols and abbreviated terms 5
4 Comparison of terms used in biometric systems with those used in video surveillance **5**
5 Architecture **6**
6 Use cases **7**
6.1 General 7
6.2 Post-event use cases 8
6.3 Real-time use cases 8
6.4 Enrolment use cases 9
7 Specification of hardware and software **9**
7.1 General 9
7.2 Physical environment 10
7.3 Illumination environment 10
7.4 Inducing frontal view 10
7.5 Cameras and supporting infrastructure 11
7.5.1 Selection of cameras 11
7.5.2 Positioning of cameras 12
7.5.3 Infrastructure considerations 16
7.6 Biometric software 17
7.6.1 General 17
7.6.2 Face detection software 17
7.6.3 Face comparison software 18
7.6.4 Algorithm selection and testing 18
7.6.5 Other (non-biometric) software 19
7.7 Computational requirements 19
7.7.1 General 19
7.7.2 Core biometric processes 19
7.7.3 Reducing computational expense 20
7.8 Specification for reference image database 21
7.8.1 General 21
7.8.2 Reference database size 21
7.8.3 Reference image quality 21
7.8.4 Reference database maintenance 22
8 Multiple camera operation **22**
9 Interfaces to related software **23**
10 Guidance for operator assistance **23**
11 System design considerations **24**
11.1 General 24
11.2 Establishing the business requirements 24
11.3 Site survey 24
11.4 Size and content of the watchlist 26
11.5 Performance requirements 26

© ISO/IEC 2024 – All rights reserved

11.5.1 General 26
11.5.2 Key metrics of performance 26
11.5.3 PAD performance metrics 27
11.6 Image data and metadata considerations 27
Annex A (informative) **Related (non-biometric) video analytic techniques and applications** **28**
Annex B (informative) **Societal considerations and governance processes** **31**
Annex C (informative) **Case study: The use of AFR with VSS for traveller triaging at the border** **33**
Annex D (informative) **Video acquisition measurements** **35**
Bibliography **45**

© ISO/IEC 2024 – All rights reserved

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 30137-1:2019), of which it constitutes a minor revision. The changes are as follows:

— in the interest of using inclusive language, the terms "black list" and "white list" have been updated to "block list" and "allow list", respectively;

— minor editorial corrections have been made throughout the text, including corrections to cross-referencing within the document itself.

A list of all parts in the ISO/IEC 30137 series can be found on the ISO and IEC websites.

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.

© ISO/IEC 2024 – All rights reserved

Introduction

Considerable improvements in the performance of automatic facial recognition (AFR) technologies have resulted in applications such as automated border control using the facial images encoded in e-passports and implemented in systems whereby the identity of a co-operative traveller is verified in an environment designed for the collection of uniformly illuminated and optimally posed images. The success of these first generation AFR systems has encouraged suppliers to consider other applications where the environment for collection of images may be far from optimal. The inferior performance in such identification applications with less control can necessitate a greater involvement by trained personnel.

The ISO/IEC 30137 series provides guidance on the use of biometric technologies in video surveillance systems (VSSs), a framework for performance testing and reporting of such systems, and procedures for establishing ground truth and annotating video data for testing purposes.

This document provides the architecture, use cases and system design. The use cases include real-time alerting to the presence of individuals of interest, law enforcement applications such as reviewing post-event video footage from one or more cameras against pre-populated watchlists, commercial uses such as the identification of individuals who are to be given preferential service, and faces added to (enrolled in) a watchlist following observation of behaviours in the video material.

Other scenarios include measurement of crowd densities and determining numbers of individuals traversing a given point. While these are not the focus of this document, they are closely related and information on these scenarios is therefore included in Annex A.

© ISO/IEC 2024 – All rights reserved

Information technology — Use of biometrics in video surveillance systems —

Part 1: System design and specification

1 Scope

The ISO/IEC 30137 series is applicable to the use of biometrics in VSSs (also known as closed circuit television or CCTV systems) for a number of scenarios, including real-time operation against watchlists and in post-event analysis of video data. In most cases, the biometric mode of choice will be face recognition, but this document also provides guidance for other modalities, such as gait recognition.

This document:

— defines the key terms for use in the specification of biometric technologies in a VSS, including metrics for defining performance;

— provides guidance on the selection of camera types, placement of cameras, image specification, etc., for the operation of a biometric recognition capability in conjunction with a VSS;

— provides guidance on the composition of the gallery (or watchlist) against which facial images from the VSS are compared, including the selection of appropriate images of sufficient quality, and the size of the gallery in relation to performance requirements;

— makes recommendations on data formats for facial images and other relevant information (including metadata) obtained from video footage, used in watchlist images, or from observations made by human operators;

— establishes general principles for supporting the operator of the VSS, including user interfaces and processes to ensure efficient and effective operation, and highlights the need to have suitably trained personnel;

— highlights the need for robust governance processes to provide assurance that the implemented security, privacy and personal data protection measures specific to the use of biometric technologies with a VSS (e.g. internationally recognizable signage) are fit for purpose, and that societal considerations are reflected in the deployed system.

This document also provides information on related recognition and detection tasks in a VSS, such as:

— estimation of crowd densities;

— determination of patterns of movement of individuals;

— identification of individuals appearing in more than one camera;

— use of other biometric modalities such as gait or iris;

— use of specialized software to infer attributes of individuals, e.g. estimation of gender and age;

— interfaces to another related functionality, e.g. video analytics to measure queue lengths or to provide alerts for abandoned baggage.

© ISO/IEC 2024 – All rights reserved

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 Terms related to the target subject

3.1.1
operator
individual(s) responsible for day-to-day operation of the system

Note 1 to entry: This may include adjustment of the video surveillance cameras, selecting data suitable for use by the biometric application, and acting on the output of the biometric comparison process.

3.1.2
presentation attack
presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion that can interfere with the intended policy of the biometric system

3.1.3
target subject(s)
target(s)
individual(s) of interest

Note 1 to entry: A target subject is normally someone already enrolled in a *watchlist* (3.1.4). However, this is not always the case; in some scenarios they are a target because they are to be enrolled in a watchlist.

3.1.4
watchlist
list of individuals of interest (and their associated reference images) for detection by the video surveillance application

Note 1 to entry: The watchlist may be of individuals for whom an added service level is to be offered (e.g. VIPs or premium customers). This is sometimes referred to as an “allow list”.

Note 2 to entry: The watchlist may be a list of “wanted” individuals, e.g. individuals who should be denied access to premises or services. This is sometimes referred to as a “block list”.

Note 3 to entry: A system may have multiple watchlists of different groups of *target subjects* (3.1.3), and with different performance goals.

Note 4 to entry: In the case of target subject *back-tracking* (3.3.1), the watchlist normally contains only one target subject, or in the case of a group of individuals of interest, a few target subjects.

3.2 Terms related to VSS

3.2.1
codec
computer program capable of encoding or decoding a digital data stream or signal

© ISO/IEC 2024 – All rights reserved