INTERNATIONAL STANDARD

ISO/IEC 30107-1

Second edition
2023-08

Information technology — Biometric presentation attack detection —

Part 1: **Framework**

Technologies de l'information — Détection d'attaque de présentation en biométrie —

Partie 1: Structure

Reference number
ISO/IEC 30107-1:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Characterization of presentation attacks ... **3**
4.1 General ... 3
4.2 Presentation attack instruments ... 3
5 Framework for presentation attack detection methods ... **4**
5.1 Types of presentation attack detection ... 4
5.2 The role of challenge-response ... 5
5.2.1 General ... 5
5.2.2 Challenge-response related to liveness detection ... 6
5.2.3 Liveness detection not related to challenge-response ... 6
5.2.4 Challenge-response not related to biometrics ... 6
5.3 Presentation attack detection process ... 6
5.4 Presentation attack detection within biometric system architecture ... 7
5.4.1 Overview in terms of the generalized biometric framework ... 7
5.4.2 PAD processing considerations relative to the other biometric subsystems ... 8
5.4.3 PAD location implications regarding data interchange ... 9
6 Obstacles to biometric impostor presentation attacks in a biometric system ... **9**
Bibliography ... **11**

© ISO/IEC 2023 – 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 30107-1:2016), which has been technically revised.

The main changes are as follows:

— the terms and definitions have been harmonized with the other parts of the ISO/IEC 30107 series.

A list of all parts in the ISO/IEC 30107 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 2023 – All rights reserved

Introduction

Biometric technologies are used to recognize individuals based on biological and behavioural characteristics. Consequently, they are often used as a component in security systems. A biometric technology assisted security system can attempt to recognize persons who are known as either friends or foes or can attempt to recognize persons who are unknown to the system as either.

Since the beginning of these technologies, the possibility of subversion of recognition by determined adversaries has been widely acknowledged, as has the need for countermeasures to detect and defeat subversive recognition attempts, or presentation attacks. Subversion of the intended function of a biometric technology can take place at any point within a security system and by any actor, whether a system insider or an external adversary. However, the ISO/IEC 30107 series is limited in scope, focusing on mechanisms for the automated detection of presentation attacks undertaken by biometric capture subjects at the capture device during the presentation of the biometric characteristics. These automated mechanisms are referred to as "presentation attack detection" (PAD) methods. Morphing attacks, where biometric samples that are manipulated to match two or more biometric data subjects are submitted during enrolment, are not considered in the ISO/IEC 30107 series, though the performance assessment methods are similar for PAD and morphing attack detection mechanisms.

The potential for subversion of biometric systems at the point of data collection by determined individuals acting as biometric capture subjects has limited the use of biometrics in applications which are unsupervised by an agent of the system owner, such as remote collections over untrusted networks. Guidelines on e-authentication, for example, do not recommend the use of biometrics as an authentication factor for this reason. In unattended applications, such as remote authentication over open networks, automated presentation attack detection methods can be applied to mitigate the risks of attack. Standards, best practices and independently-evaluated mechanisms can improve the security of all systems employing biometrics, whether using supervised or unsupervised data capture, including those using biometric recognition to secure online transactions.

As is the case for biometric recognition, PAD mechanisms are subject to errors, both false positive and false negative: false positive indications wrongly categorize bona-fide presentations as attacks, thus impairing the efficiency of the system, and false negative indications wrongly categorize presentation attacks as bona fide, not preventing a security breach. Therefore, the decision to use a specific implementation of PAD depends upon the requirements of the application and consideration of the trade-offs with respect to security and efficiency.

The purpose of this document is to provide a foundation for PAD by defining terms and establishing a framework through which presentation attack events can be specified and detected so that they can be categorized, detailed, and communicated for subsequent biometric system decision-making and performance assessment activities. This foundation will also benefit other standardization projects in ISO/IEC committees and subcommittees. This document does not advocate a specific mechanism as a standard PAD tool.

There are currently three other parts in the ISO/IEC 30107 series. ISO/IEC 30107-2 defines data formats for conveying the type of approach used in biometric presentation attack detection and for conveying the results of PAD methods. The data formats defined in ISO/IEC 30107-2 are integrated into the extensible biometric data interchange formats defined in the ISO/IEC 39794 series. ISO/IEC 30107-3 establishes principles and methods for performance assessment of PAD mechanisms. ISO/IEC 30107-4 provides requirements for assessing the performance of PAD mechanisms on mobile devices with local biometric recognition.

© ISO/IEC 2023 – All rights reserved

Information technology — Biometric presentation attack detection —

Part 1: Framework

1 Scope

This document establishes terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection (PAD) methods.

This document does not provide the following:

— standardization of specific PAD detection methods;

— detailed information about countermeasures (i.e. anti-spoofing mechanisms), algorithms or sensors;

— overall system-level security or vulnerability assessment.

The attacks to be considered in this document are those that take place at the capture device during the presentation and collection of the biometric characteristics. Any other attacks are considered outside the scope of this document.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 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
artefact
artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

3.2
liveness
quality or state of being alive, made evident by anatomical characteristics, involuntary reactions, physiological functions, voluntary reactions, subject behaviours, or any combination of these

EXAMPLE 1 Absorption of illumination by the skin and blood are anatomical characteristics.

© ISO/IEC 2023 – All rights reserved