International Standard

ISO/IEC 20059

Information technology — Methodologies to evaluate the resistance of biometric systems to morphing attacks

Technologies de l'information — Méthodologies pour l'évaluation de la résistance des systèmes biométriques aux attaques par morphing

First edition
2025-08

Reference number
ISO/IEC 20059:2025(en)

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

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*.

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

Many application processes for ID documents do not implement trusted capture. For example, as long as printed biometric samples (e.g. face images) are accepted, morphing attacks, where biometric references are manipulated to match two or more biometric data subjects submitted during enrolment, pose a threat to image-based biometric systems (BSs). Morphing attack detection is possible, though the ability to detect morphing attacks can differ based on the morphing attack techniques.

Not all morphing techniques pose the same risk for an operational BS. This document establishes morphing attack potential (MAP) as a measure of the capability of a class of morphing attacks to deceive one or more BSs.

The user of this document can simulate a real use case such as issuance of documents or border control. The use case can consider a variable number of attempts and BSs to determine the MAP against automated border control (ABC) gates from different vendors.

NOTE The evaluation of the resistance of a BS is not a security evaluation.

Information technology — Methodologies to evaluate the resistance of biometric systems to morphing attacks

1 Scope

This document establishes a methodology to evaluate the resistance of BSs to morphing attacks, including multiple identity attacks. The document is limited to image-based morphing attacks. The term "image-based" includes modalities such as face, iris and finger image data.

The document establishes:

— a definition of biometric sample modifications and manipulation with a specific focus on manipulations that constitute a multiple identity attack. This can be, for instance, an enrolment attack with face image morphing;

— a methodology to measure the morphing attack potential of a morphing method.

The document also describes how morphing algorithms can be used for system evaluation.

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 30107-1, *Information technology — Biometric presentation attack detection — Part 1: Framework*

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*