International Standard

ISO/IEC 20059

First edition
2025-08

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

Reference number
ISO/IEC 20059:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **4**
5 Morphing attacks ... **6**
6 Measuring and reporting morphing attack potential ... **7**
6.1 Morphing attack potential ... 7
6.2 Multiple contributing subject generalization ... 9
6.3 Visualisation ... 9
6.4 Benchmarking of morphing methods and impacting factors ... 12
7 Morph detection error rates ... **12**
Annex A (informative) **Reference implementation** ... **13**
Annex B (informative) **Example of morphed sample visualization** ... **14**
Bibliography ... **16**

© ISO/IEC 2025 – 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*.

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 2025 – All rights reserved

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.

© ISO/IEC 2025 – All rights reserved

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 30107-1, ISO/IEC 30107-3, ISO/IEC 39794-5 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
image content
visual information within an image, such as the face of a subject

Note 1 to entry: Artefacts like an iris shadow, caused by a poor quality morphing method, are potentially contained in the image content.

Note 2 to entry: Artefacts by compression also belong to the image content.

© ISO/IEC 2025 – All rights reserved

3.2
image generation
creation of still or animated content with imaging software

Note 1 to entry: For instance, the generation of a synthetic image (e.g. with GANs) and subsequent morphing of the accomplice image with the synthetic.

Note 2 to entry: Morphing can be a part of that process.

3.3 Terms related to image substitution

3.3.1
image substitution attack
replacement of the printed image in the physical passport booklet with the intention to fool the human examiner

Note 1 to entry: Could also be used to fool the face recognition system, if the image from the passport data page is scanned.

Note 2 to entry: The attack takes the target photo and puts parts of it on top of the original printed image on the data page.

Note 3 to entry: The image in the chip is not affected by the attack.

3.3.2
image substitution attack detection
revealing deviations to expected properties of the original portrait image area

Note 1 to entry: An image substitution attack can cause image artefacts in the scanned facial image or its surroundings.

Note 2 to entry: The expected UV pattern cannot be observed.

Note 3 to entry: This is complementary action to other measures, like validating the document numbers.

3.4 Terms related to image manipulation

3.4.1
image modification
act of effect of changing the image content or metadata of an image

Note 1 to entry: Typical signal modifications are beautifications, compression, sharpening, contrast enhancement, cropping, geometry change.

Note 2 to entry: Typical metadata modification could be change of location, date or time of capturing.

3.4.2
image manipulation
act of effect of intentionally altering the visual appearance or specific properties of an image resulting in misrepresentation or misinterpretation

Note 1 to entry: The difference to an image modification is the intention of the malicious actor.

Note 2 to entry: A manipulation is a subset of a modification.

3.4.3
digital image manipulation
act or effect of intentionally altering digitally the visual appearance or specific properties of an image resulting in misrepresentation or misinterpretation

Note 1 to entry: Alteration can be morphing of two parent images or replacing of certain parts/regions of the image.

Note 2 to entry: Manipulation can target elements of metadata (e.g. the capture date field).

© ISO/IEC 2025 – All rights reserved

3.4.4
biometric image manipulation
image modification intended to influence either the output of a biometric system or the decision of a human examiner, or both

Note 1 to entry: Possible intentions are for criminal attacks (impersonation) or for protecting privacy (avoiding recognition by means of de-identification).

Note 2 to entry: Using a filter on the face represented in the image, can influence the error rates of the biometric system (e.g. increased false reject rate or false accept rate, or both)[5].

Note 3 to entry: Alteration before the capture process (e.g. manipulating the facial appearance with makeup) is not a digital manipulation. This is a presentation attack as defined in ISO/IEC 30107-1.

3.4.5
biometric image manipulation attack
submission of an image containing a manipulated representation of a biometric trait to the identity document application process with the goal of interfering with the operation of either the biometric system or the human examiner, or both

3.4.6
image manipulation attack detection
detecting traces of image manipulation conducted by either an algorithm or a human examiner, or both

Note 1 to entry: Detection algorithms typically operate on the suspected images, potentially supported with a trusted live capture image.

Note 2 to entry: The detection algorithm has typically no information about the enrolment process (i.e. the details of the attack vector).

3.5 Terms related to image morphing

3.5.1
biometric morphing
combining two or more biometric samples into one signal

Note 1 to entry: A biometric sample is defined in ISO/IEC 2382-37.

3.5.2
face image morphing
morphing process executed with facial portrait images

3.5.3
face image morphing attack
biometric image manipulation attack based on morphing two or more facial images

Note 1 to entry: The morphing can be executed on the holistic facial image or on selected areas of interest (e.g. the periocular region).

3.5.4
morphing attack detection
MAD
observing a biometric morphing attack through either an algorithmic or a human method, or both

Note 1 to entry: The attack detection can be conducted based on a single image (single image morphing attack detection, i.e. S-MAD) or based on a pair of images (differential image morphing attack detection, i.e. D-MAD).

3.5.5
single image morphing attack detection
S-MAD
morphing attack detection that is based on a single image

© ISO/IEC 2025 – All rights reserved

3.5.6
differential image morphing attack detection
D-MAD
morphing attack detection that is based on a pair of images

Note 1 to entry: D-MAD can be implemented by quantifying the similarity between a suspected morph image and a trusted-capture (i.e. bona fide image).

3.5.7
multiple identity attack
MIA
biometric morphing attack with the intention of obtaining an identity document that can be successfully used by multiple subjects

3.5.8
morphing attack potential
MAP
measure of the capability of a class of morphing attacks to deceive one or more biometric systems using multiple recognition attempts

3.5.9
bona fide sample classification error rate
BSCER
proportion of bona fide samples incorrectly classified as morphed samples in a specific scenario

3.5.10
morphing attack classification error rate
MACER
proportion of morphed samples incorrectly classified as bona fide samples in a specific scenario

3.5.11
morphing attack classification error rate at a given morphing attack potential
$\boldsymbol{MACER}_{\boldsymbol{MAP}}[\boldsymbol{r},\boldsymbol{c}]$
MACER computed on the subset of morphed images that can successfully reach a match decision with both contributing subjects in at least r verification attempts by at least c biometric systems

Note 1 to entry: See Clause 7 for further details.

4 Symbols and abbreviated terms

The following abbreviated terms and symbols are used in this document.

ABC	automated border control
BS	biometric system
BSCER	bona fide sample classification error rate
D-MAD	differential image morphing attack detection
FAR	false accept rate
FRR	false reject rate
FMMPMR	fully mated morph presentation match rate
MACER	morphing attack classification error rate
MAD	morphing attack detection

© ISO/IEC 2025 – All rights reserved