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)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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.

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.

EXAMPLE 2 The reaction of the iris to light and heart activity (pulse) are involuntary reactions (also called physiological functions).

EXAMPLE 3 Squeezing together one's fingers in hand geometry and a biometric presentation in response to a directive cue are both voluntary reactions (also called subject behaviours).

3.3
liveness detection
measurement and analysis of anatomical characteristics or involuntary or voluntary reactions in order to determine whether a biometric sample is being captured from a living subject present at the point of capture

Note 1 to entry: Liveness detection methods are a subset of presentation attack detection methods.

3.4
bona-fide presentation
biometric presentation without the goal of interfering with the operation of the biometric system

[SOURCE: ISO/IEC 2382-37:2022, 37.06.36]

3.5
biometric presentation attack
attack presentation
presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: Biometric presentation attacks can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc.

Note 2 to entry: Biometric presentation attacks can have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: Biometric systems can be unable to differentiate between presentations with the goal of interfering with the systems' operation and non-conformant presentations.

[SOURCE: ISO/IEC 2382-37:2022, 37.06.25, modified — The term "attack presentation", which is frequently used in ISO/IEC 30107-3, has been added as an admitted term.]

3.6
presentation attack detection
PAD
automated discrimination between bona-fide presentations and biometric presentation attacks

Note 1 to entry: PAD cannot infer the biometric capture subject's intent.

[SOURCE: ISO/IEC 2382-37:2022, 37.06.42]

3.7
presentation attack instrument
PAI
biometric characteristic or object used in a biometric presentation attack

Note 1 to entry: The set of PAI includes artefacts but would also include lifeless biometric characteristics, (stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints that are used in an attack).

[SOURCE: ISO/IEC 2382-37:2022, 37.06.44]

4 Characterization of presentation attacks

4.1 General

While attacks on a biometric system can occur anywhere and be instantiated by any actor, the ISO/IEC 30107 series focuses on biometric-based attacks on the data capture subsystem by biometric capture subjects attempting to subvert the intended operation of the system. Attacks by other actors and at other points of the system have previously been considered in documents such as Reference [3]. The ISO/IEC 30107 series does not address protecting the data capture subsystem, including the sensor itself, from modification, replacement or removal, or protecting the communication between the data capture subsystem and other subsystems.

Figure 1 illustrates several generic attacks against a biometric system. The ISO/IEC 30107 series only focuses on attacks pointed out by arrow "1," in which a biometric characteristic or PAI is presented to a sensor that is operating properly within a biometric system.

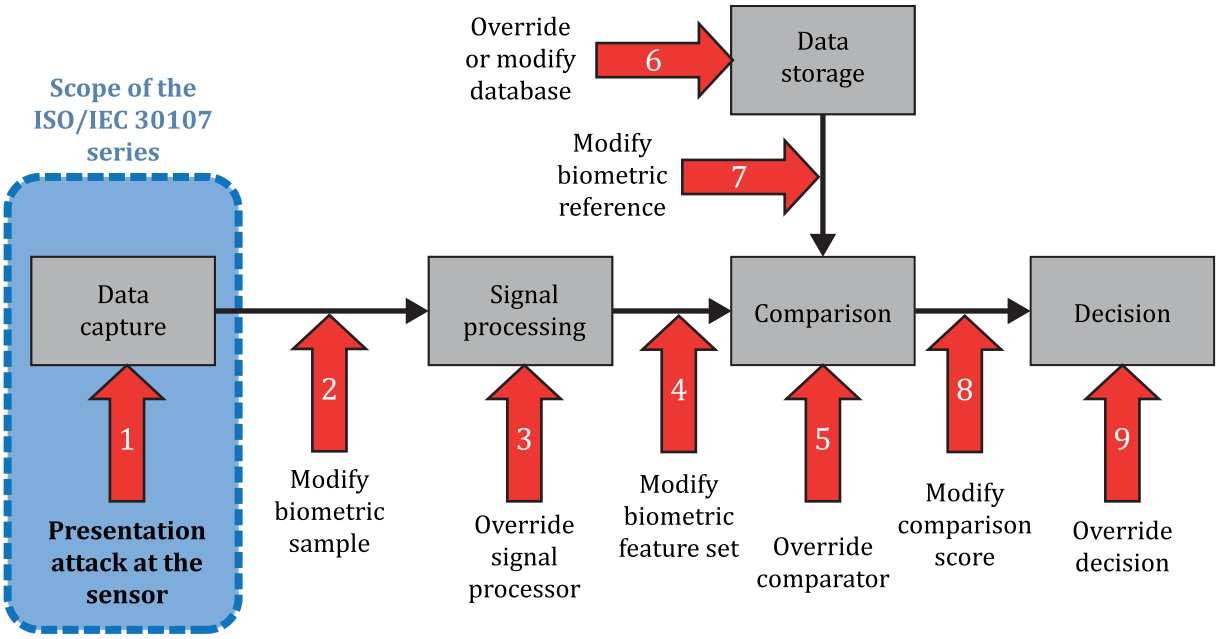


Figure 1 — Examples of points of attack in a biometric system

Presentation attacks can be carried out by two types of subversive biometric capture subjects: a biometric impostor, where the subversive biometric capture subject intends to be recognized as an individual other than themselves, or a biometric concealer, where the subversive biometric capture subject intends to evade being recognized as any individual known to the system.

Biometric impostors can perform attacks in two different ways. In the first sub-type, the subversive data subject intends to be recognized as a specific individual known to the system. In the second sub-type, the subversive data subject intends to be recognized as any individual known to the system, without specification as to which one.

In contrast, biometric concealers seek to conceal their own biometric characteristics, as opposed to modelling the characteristics of known individuals, e.g. using an artefact or through disguise or alteration of natural biometric characteristics.

4.2 Presentation attack instruments

The object or characteristic used in a presentation attack is a PAI. Attacks at the sensor using PAIs generally fall into one of two categories: artificial or human-based characteristics. There is a third category of other natural cases such as animal-based and plant-based PAIs.

Furthermore, the terms conformant and non-conformant are used, but they will not influence the PAD encoding, as their meaning is concerned with the subject-sensor interaction, which is hard to objectively measure and thus cannot be encoded. An example for such non-conformant interaction would be to place the side of a finger on the device instead of the fingerprint pattern.

A detected attack can be due to accessibility or usability issues of a subject and not an attempt to attack the system at all.

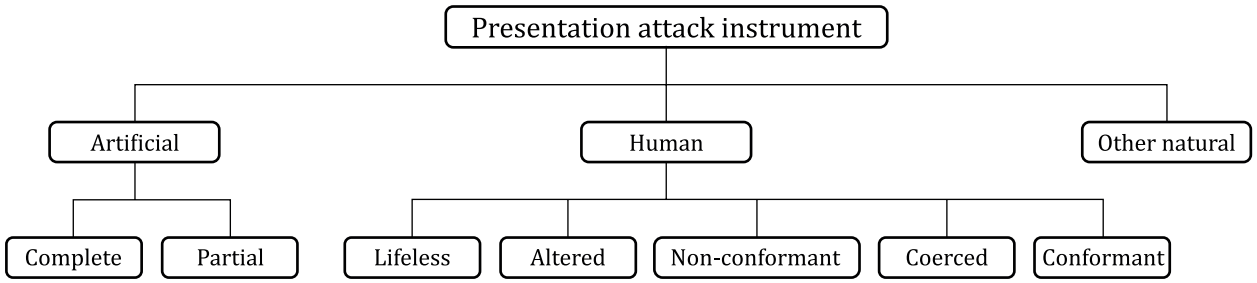


Figure 2 — Types of presentation attacks

Figure 2 shows these categories further broken down in the third row. Table 1 gives examples of each specific PAI type in the bottom tier of Figure 2. This figure can be used to describe a specific PAI by using the adjective in the second column, followed by the word in the first column. For example, a body part from a cadaver would be an example of a "lifeless, human PAI".

Table 1 — Examples of artificial and human presentation attack instruments

Artificial	Complete	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up
Human	Lifeless	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-conform-ant	facial expression/extreme, tip or side of finger
	Coerced[a]	unconscious, under duress
	Conformant	zero effort impostor attempt

[a] Not all coercive presentations are expected to be detectable. Some modalities enable measurement of coercion indicators, such as voice stress analysis, extreme pulse rate, or facial emotion analysis (fear).

5 Framework for presentation attack detection methods

5.1 Types of presentation attack detection

PAD methods fall into two categories, as illustrated in Table 2: those that are based on data captured by the data capture subsystem and those that are based on system-level security measures. PAD methods are not intended to have a one-to-one relationship with PAI categories (shown in Figure 2).

Table 2 — Examples of methods for presentation attack detection

Through data capture subsystem	Artefact detection	Detects features that are indicative of an artefact. EXAMPLE 1 Electrical impedance of "finger" on sensor is outside of the typical range. EXAMPLE 2 Surface and subcutaneous versions of the fingerprint are significantly different.
	Liveness detection	See 3.3 for a definition. See 5.2.2 and 5.2.3 for examples.
	Alteration detection	Detects evidence of attempts to alter biometric characteristics. EXAMPLE Scar tissue on fingerprint.[4]
	Non-conformance detection	Detects abnormalities that would not occur in a proper presentation. EXAMPLE Detection that illumination level is not consistent with normal use.
	Coercion detection	EXAMPLE Stress analysis from voice or facial emotion.
	Obscuration[a] detection	Detects that features have been partially or wholly blocked from the "view" of the sensor. EXAMPLE Detecting an accessory covering part of the face, like a scarf or hat.
Through system-level monitoring	Failed attempt detection counter	EXAMPLE Suspected presentation attack if there is a sequence of similar failed attempts.
	Geographic	Combined geographic/temporal. EXAMPLE Suspected presentation attack if the location or time of use is infeasible or unusual for the identity matched
	Temporal	
	Video surveillance	EXAMPLE Judgement by human operator (or video analytics system).

[a] Obscuration involves a subject presentation containing degraded biometric characteristic utility due to the absence of some portion of the characteristic, an example being a face partially concealed by a hat or scarf. In some cases, obscuration detection can be included in artefact detection.

5.2 The role of challenge-response

5.2.1 General

The concept of challenge-response is widely used in authentication schemes, some of which include biometric aspects and others which have no biometric contribution. This clause provides a structure for examining the overall concept of challenge-response and focuses in more detail on the biometric implementation using challenge-response, and the relationship between liveness and challenge-response.

In this context, a challenge is a purposeful activity that has an expected response when in the presence of the targeted condition.

5.2.2 Challenge-response related to liveness detection

Challenge-response can be used as a tool for determining if a subject's presentation has liveness properties exhibited in the biometric data capture subsystem's acquisition. For example, the live human iris is expected to respond to changes in visible light illumination (the challenge) with changes in pupil size (the expected response if alive).

The framework for categorizing all aspects of challenge-response related to liveness is shown in Table 3. Note that the last column cannot apply to the initial encounter with a subject, or for an enrolment-liveness determination, while the others can apply.

Table 3 — Liveness detection utilizing challenge-response as a tool

	Involuntary response	Voluntary response	Combination of something the subject is and knows
Challenge	Purposeful stimulus focused on known biometric characteristic	Cues (aural, visual, etc.) directing a specific action to be captured by the biometric system	Directions specifying biometric presentation(s) utilizing previously enrolled information
Response	Natural, involuntary, not controllable by the subject	Based on alive human cognition and voluntarily controlled action	Based on alive human cognition, and specific individual biometric enrolment
Examples	Illumination change → Pupil size change	Cue to nod head → head pitch angle changes in the correct direction Cue to close left eye → left iris occlusion	Finger order (random changes by system) → Correct fingers presentation and comparison Digit order → Correct digit utterance and comparison

5.2.3 Liveness detection not related to challenge-response

There are a group of biometric liveness detection approaches that are not enabled by challenge-response and are referred to as "non-stimulated observation of liveness" detection (which can also be referred to as "passive" liveness detection). The liveness is characterized exclusively from what is received by the sensor over some appropriate time period, with no purposeful liveness-related stimuli. Examples of this category are:

— finger perspiration (over time),

— hippus (iris) motion/frequency (over short time),

— pulse (over time), and

— multispectral illumination (blood/tissue light frequency absorption).

5.2.4 Challenge-response not related to biometrics

Some authentication schemes that are not biometrically enabled do utilize the concepts of challenge-response to strengthen their assurance of the authentication, typically with multi-factor authentication (excluding the biometric factor). The challenge in this case can take the form of a device/card authentication using digital certificates or asking for the answer to a security question (secret).

5.3 Presentation attack detection process

PAD may be performed in the following steps. These steps are similar to the biometric recognition processes.

Step 1): Capture raw data for PAD from a subject using the biometric data capture subsystem. The sensors used may be different from the sensors used to capture biometric samples, and the capture

of biometric samples and PAD data may be separate, although divergence in time of measurement between capture of biometric characteristics and PAD data can lead to a vulnerability.

Step 2): Extract features from the PAD data.

Step 3): Compare the PAD features with the criteria.

Step 4): A result (detection, no-detection, score, etc.) is the output of the comparison. These data alone or in combination with other data inform the final decision of the biometric system to accept or reject the sample.

Although these steps shall be performed in this order, they can potentially not be contiguous in time or space.

The decision criteria used in Step 3) can be common for all subjects or specific to each subject. For example, when involuntary reactions or physiological functions, or voluntary reactions or subject behaviours are used to detect presentation attacks, the presentation-attack criteria can be common for all subjects if they are measured roughly. The criteria can be specific to each subject if they are measured precisely.

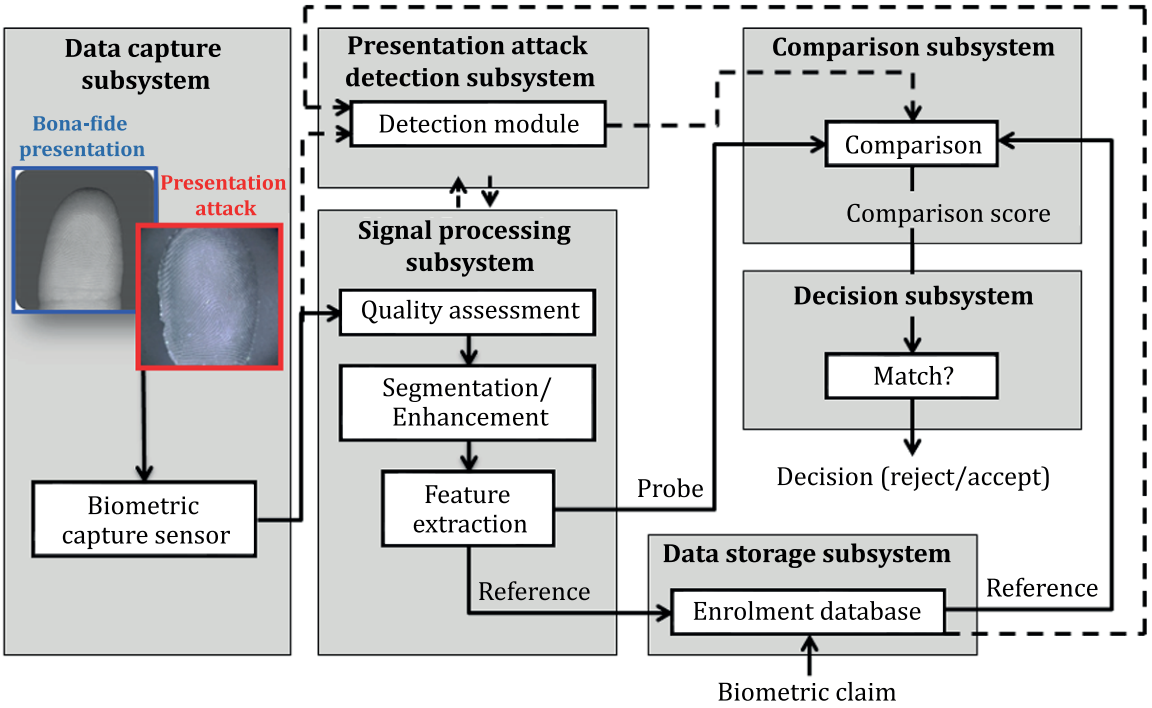
The enrolment process of the criteria is necessary in cases where they are specific to each subject.

5.4 Presentation attack detection within biometric system architecture

5.4.1 Overview in terms of the generalized biometric framework

Although the ISO/IEC 30107 series is concerned only with attacks at the location of the biometric data capture, the PAD function may be performed at any place or time within the biometric system.

Figure 3 shows the PAD subsystem inserted into the general biometric framework in one way, but the PAD subsystem (and its individual processes) may be placed within the generalized framework in several ways. The subsystem which detects presentation attacks may be located following (or within) the data capture subsystem and/or following the signal processing subsystem, indicated by dotted lines in Figure 3. Additionally, PAD may also occur after the comparison or decision subsystems (not shown) or at several points in the system. Also, there may be a physical, temporal, or functional overlap between the process of collecting data for use in determining identity and the process of detecting a presentation attack. See 5.4.2 and 5.4.3 for additional discussion on these variations regarding where and when PAD processes may occur.



NOTE Other configurations are possible.

Figure 3 — A general biometric framework with presentation attack detection

Figure 4 provides additional details for the PAD subsystem. Some PAD subsystems do not need the PAD feature extractor. The PAD comparator and the stored PAD criteria are essential in the subsystems. The PAD criteria are either common for all subjects or are specific to each subject.

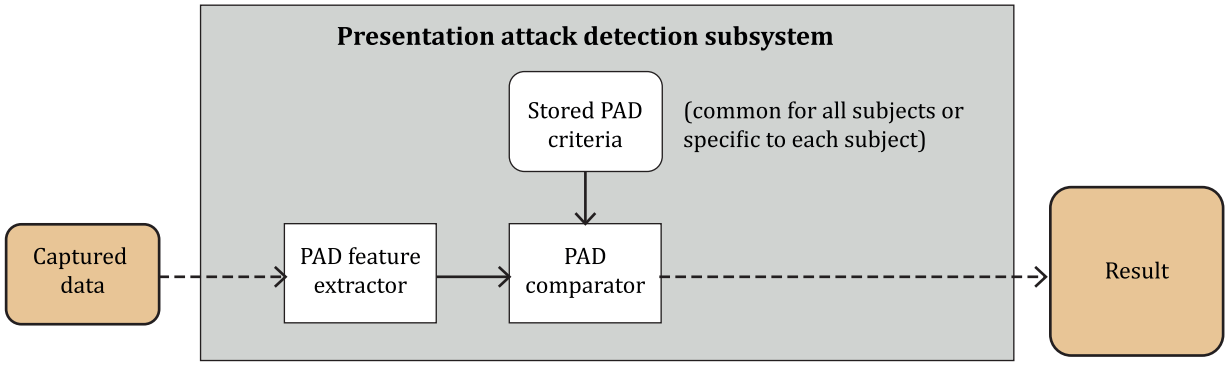


Figure 4 — Components in a general presentation attack detection subsystem

5.4.2 PAD processing considerations relative to the other biometric subsystems

It is instructive to consider the collection and processing of the PAD data and the biometric sample data independently in both time and space. The two forms of data may both exist or either may exist in the absence of the other. The process of PAD can be handled by a biometric system concurrently, before, or after any of the subsystems. The components of the PAD subsystem may even occur separately, between

and/or concurrently with more than one subsystem. PAD output may depend upon multiple captured biometric samples and is not necessarily a simple binary indicator.

EXAMPLE 1 A data capture device can be designed to generate biometric sample data and PAD data for each data capture event. Depending on system design, such a data capture device can output biometric sample data regardless of the outcome of the PAD function, or only in the case that the PAD detects no attack. It is also possible that the PAD data are generated without the acquisition of a biometric sample. In this example, the output of the PAD is a simple binary indicator of detected attack.

EXAMPLE 2 The captured PAD data can be analysed during the signal processing function after the biometric sample has been acquired. In this case, the biometric sample or the biometric features or model resulting from the signal processing subsystem can be accompanied by the PAD metric determined during signal processing.

EXAMPLE 3 The PAD data can be collected but not analysed until much later in the process. In this example, the signal required for PAD processing is stored with the biometric sample, features or model.

NOTE Whilst not every system uses real-time monitoring, video surveillance and other recordings can be an effective post-event detection and analysis mechanism to record the biometric presentation(s) and circumstances around it, just as it is now for automatic teller machines (ATMs) when card data are "skimmed" for the purpose of stealing from accounts. This could increase the detection of the method being used (successfully or not) or coercion of subject. It could allow for the capture of other biometric samples to be used in post event analysis (video surveillance footage for example to collect a face when the original access to ATM funds was via a fingerprint), which could increase the deterrent factor for attacks on such systems. These are real-world solutions that are used to deter and detect misuse of systems and may be best practices for biometric systems.

5.4.3 PAD location implications regarding data interchange

The components of the PAD subsystem may be in different locations (client versus server, front end versus back end, or mobile device versus app software/cloud). Products that support PAD may be in different forms and locations. Several possible approaches, some of which are not related to (or dependent upon) data interchange, are outlined below.

— PAD may be performed on the same device that houses the sensor for data capture. With a sophisticated device that has the computing capabilities to perform PAD, it may be not required to include the PAD data in any data interchange (to send to a back-end machine, server, or an app for example). The output of a biometric sample or granting access rights (or the absence of one of these) may be sufficient to indicate the result.

— Even if all components of a PAD subsystem are performed on the data capture device, higher-risk applications may wish to obtain as much information about the interactions of their sensor and collect data about both failed attempts and how trustworthy a biometric sample is based on available PAD data (e.g. raw data or scores).

— PAD data may be captured on a trusted device and sent to a server or an app (running software developed by a different party) to make a final determination about an identity claim and access rights. Depending on the application, the PAD data included in data interchange for the session may be raw data, sent in the form in which it was captured, or the local device may do feature extraction and send a score or other extracted data.

6 Obstacles to biometric impostor presentation attacks in a biometric system

For a biometric impostor presentation attack to succeed, the following criteria need to be fulfilled:

a) The presentation attack sample is acquired by the data capture subsystem.

b) The presented attack sample is successfully processed to produce a reference or probe.

c) The probe-reference comparison based on the presentation attack matches the target biometric reference.

d) It is possible to make the attack under the system-level security procedures in place.

e) A PAD subsystem, if present, does not classify the presented sample as an attack.

Dependent on the type of biometric system and the sophistication of the presentation attack, the success of the presentation attack can be prevented at any of these stages. For example (corresponding to the order of the stages above):

1) The artefact cannot register due to the design of the biometric sensor and the properties it uses to acquire samples, such as a silicone fake fingerprint on a capacitive fingerprint capture device.

2) The artefact sample can be deemed of insufficient quality during signal processing.

3) Loss of fidelity due to printing a copy of the true biometric image can cause the comparison score to fall outside the threshold value for recognition.

4) A face image impersonation using a life-size mannequin head can be observed by an operator.

Bibliography

[1] ISO/IEC 39794, *Information technology — Extensible biometric data interchange formats*

[2] Ratha N.K., Connell J.H., Bolle R.M., *Enhancing security and privacy in biometrics-based authentication systems*. IBM Syst. J. 2001, **40** (3)

[3] Elliott S.J., Kukula E.P. *A definitional framework for the human-biometric sensor interaction model*. Proc. SPIE. 2010, **7667**, id. 76670H

[4] Feng J., Jain A.K., Ross A. *Detecting altered fingerprints*. In Proc. of Int. Conf. on Pattern Recognition (ICPR), Istanbul, Turkey, August 2010

ICS 35.240.15

Price based on 11 pages