INTERNATIONAL STANDARD

ISO/IEC 30107-1

First edition
2016-01-15

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 30107-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/IEC 30107-1 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 30107 consists of the following parts, under the general title *Information technology — Biometric presentation attack detection*:

— *Part 1: Framework*

— *Part 2: Data formats*

— *Part 3: Testing and reporting*

Introduction

Biometric technologies are used to recognize individuals based on biological and behavioural characteristics and, consequently, are often used as a component in security systems. A biometric technology assisted security system may attempt to recognize persons who are known as either friends or foes, or may 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. This International Standard (ISO/IEC 30107) will be limited in scope, however, focusing on techniques for the automated detection of presentation attacks undertaken by biometric capture subjects at the point of presentation and collection of the relevant biometric characteristics. We will call these automated techniques "Presentation Attack Detection" (PAD) methods.

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 could be applied to mitigate the risks of attack. Standards, best practices and independently evaluated techniques could 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 techniques are subject to errors, both false positive and false negative: false positive indications wrongly categorize routine presentations as attacks, thus impairing the efficiency of the system, and false negative indications wrongly categorize presentation attacks as routine, not preventing a security breach. Therefore, the decision to use a specific implementation of PAD will depend upon the requirements of the application and consideration of the trade-offs with respect to security and efficiency.

The purpose of this part of ISO/IEC 30107 is to provide a foundation for PAD through 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 standards projects in ISO/IEC committees and sub-committees. This International Standard does not advocate a specific technique as a standard PAD tool.

There are two other parts of ISO/IEC 30107. Part 2 defines data formats for conveying the type of approach used in biometric presentation attack detection and for conveying the results of presentation attack detection methods. Part 3 establishes principles and methods for performance assessment of presentation attack detection algorithms or mechanisms.

Information technology — Biometric presentation attack detection —

Part 1: Framework

1 Scope

This part of ISO/IEC 30107 establishes terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods.

Outside the scope are

— standardization of specific PAD detection methods;

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

— overall system-level security or vulnerability assessment.

The attacks to be considered in ISO/IEC 30107 are those that take place at the sensor during the presentation and collection of the biometric characteristics.

Any other attacks are considered outside the scope of ISO/IEC 30107.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*

NOTE The electronic version of ISO/IEC 2382-37:2012 can be downloaded for free from the ISO/IEC Information Technology Task Force (ITTF) web site: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012 and the following apply.

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 or physiological functions, or voluntary reactions or subject behaviours

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 if 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
normal presentation
interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

Note 1 to entry: The term "normal" is analogous to "routine" when referring to a "normal presentation." Any type of presentation that is not an attack is considered a "normal presentation."

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

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

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

Note 3 to entry: Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations.

3.6
presentation attack detection
PAD
automated determination of a presentation attack

Note 1 to entry: PAD cannot infer the subject's intent. In fact it may be impossible to derive that difference from the data capture process or acquired sample.

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

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

4 Symbols and abbreviated terms

PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument

5 Characterisation of presentation attacks

5.1 General

Although attacks on a biometric system can occur anywhere and be instantiated by any actor, ISO/IEC 30107 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 [2]. ISO/IEC 30107 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. ISO/IEC 30107 only focuses on attacks pointed out by arrow "1," in which a biometric characteristic or PAI is presented to a sensor which is operating properly within a biometric system.

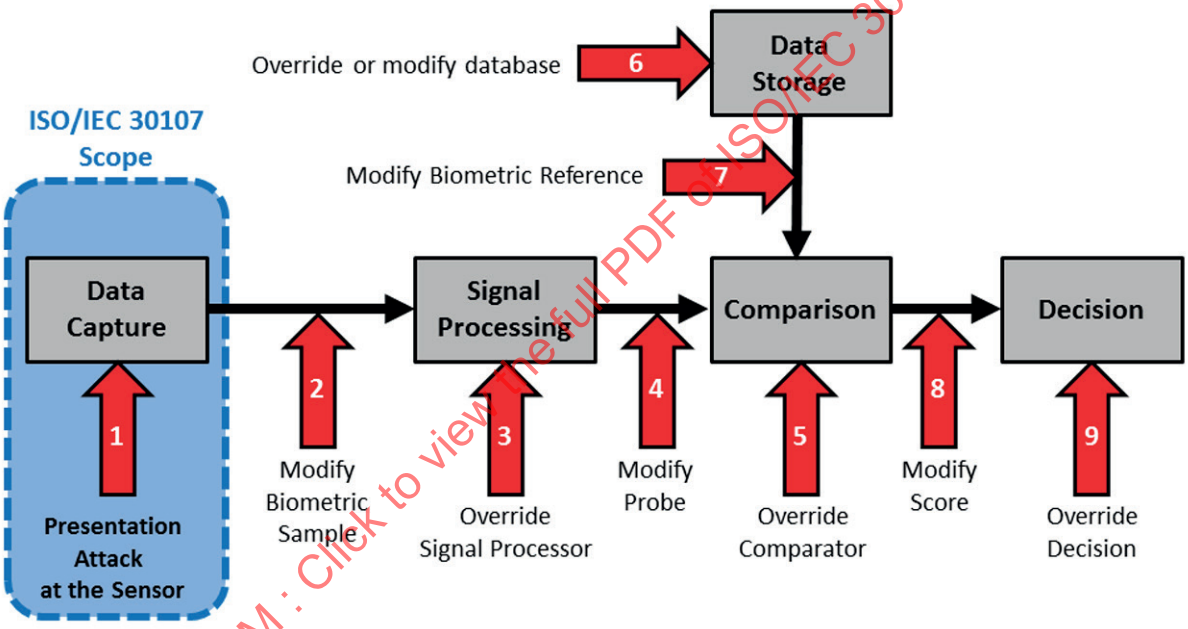

Figure 1 — Examples of points of attack in a biometric system (inspired by [1])

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

Biometric imposters may 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 will be seeking to conceal his/her 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.

5.2 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. Note that 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 in this clause and specifically in Table 1, 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.

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

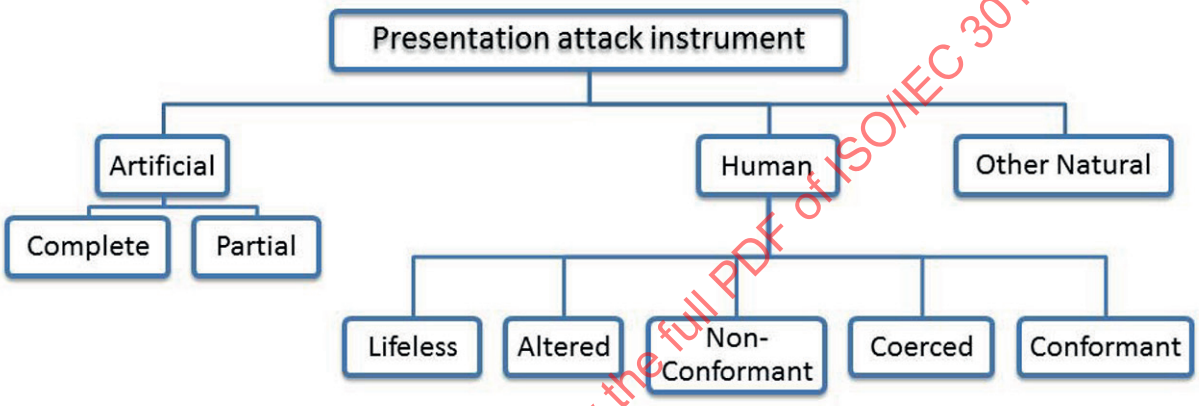

Figure 2 — Types of presentation attacks

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-Conformant	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 may enable measurement of coercion indicators, such as voice stress analysis, extreme pulse rate, or facial emotion analysis (fear).		

6 Framework for presentation attack detection methods

6.1 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. Note that 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 detecting presentation attacks

Through data capture subsystem	Artefact detection	Detects features that are indicative of an artefact. Examples: (i) electrical impedance of "finger" on sensor is outside of the typical range, (ii) surface and subcutaneous versions of the fingerprint are significantly different
	Liveness detection	See 3.3 for a definition. See 6.2.1 and 6.2.2 for examples.
	Alteration detection	Detects features characteristic of attempts to alter biometric feature. Example: scar tissue on fingerprint.
	Non-conformance detection	Detects abnormalities that should not occur in a proper presentation. Example: detection that illumination level not consistent with normal use
	Coercion detection	Examples: stress analysis from voice or facial emotion
	Obscuration 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)

NOTE 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 may be included in artefact detection.

6.2 The role of challenge-response

The concept of challenge-response is widely used in authentication schemes, some of which include biometric aspects and others with no biometric contribution. This clause provides a structure for examining the overall concept of challenge-response, and will focus 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.

6.2.1 Challenge-response related to liveness

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

	1. Involuntary response	2. Voluntary response	3. Combination of something you are and know
Challenge	Purposeful stimulus focused on known biometric characteristic	Cues (aural, visual,...) 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 & comparison Digit order --> Correct digit utterance & comparison

6.2.2 Liveness 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 could 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).

6.2.3 Challenge-response not related to biometrics

Some authentication schemes which 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).

6.3 Presentation attack detection process

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

Step 1): Capture raw data for PAD from a subject using the biometric data capture subsystem.

Note that the sensors used may be different from the sensors used to capture the biometric characteristics and the capture of biometric and PAD data might not be simultaneous, 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. This data alone or in combination with other data will inform the final decision of the biometric system to accept or reject the sample.

Although these three steps must be performed in this order, they might not be performed contiguously in time or space.

The decision criteria used in Step 3) may 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 may be common for all subjects if they are measured roughly, while the criteria may be specific to each subject if they are measured precisely.

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

6.4 Presentation attack detection within biometric system architecture

6.4.1 Overview in terms of the generalized biometric framework

Although ISO/IEC 30107 is concerned only with attacks at the location of the biometric data capture, the PAD function might 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) could be placed within the generalized framework in a number of ways. The subsystem which detects attack presentations 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 could 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 6.4.2 and 6.4.3 for additional discussion on these variations regarding where and when PAD processes may occur.

Figure 4 provides additional details for the PAD subsystem. Some PAD subsystems may 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 of subjects or are specific to each subject.

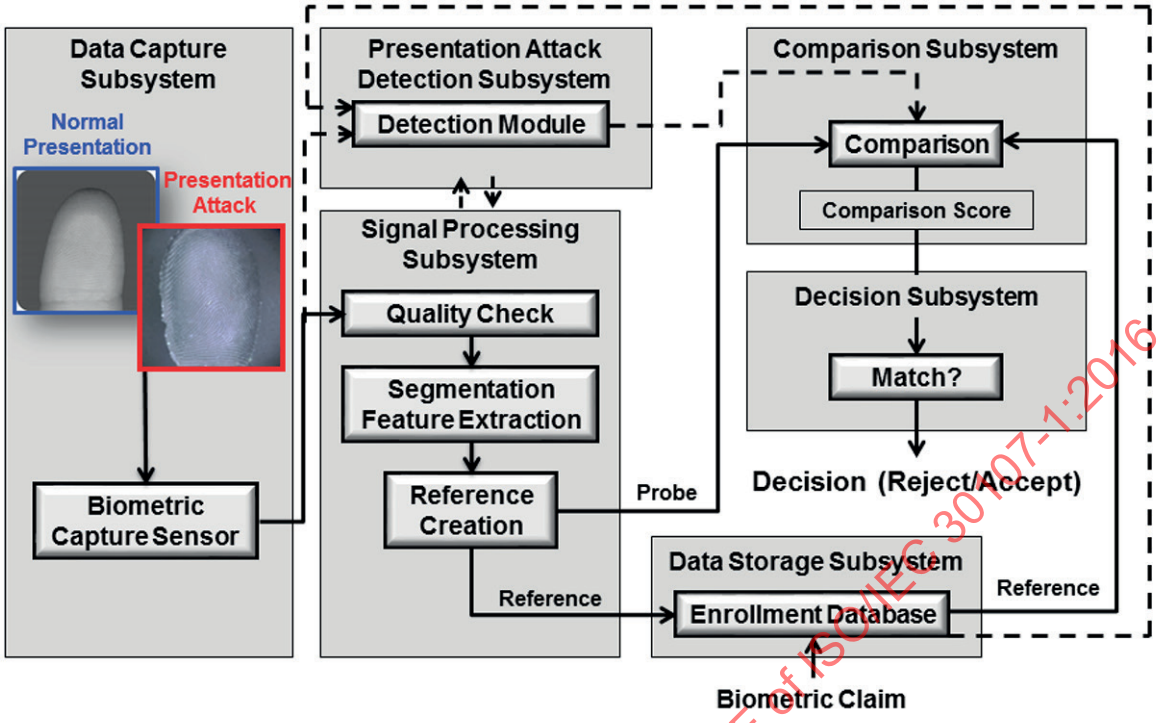

Figure 3 — A general biometric framework with presentation attack detection (other configurations are possible)

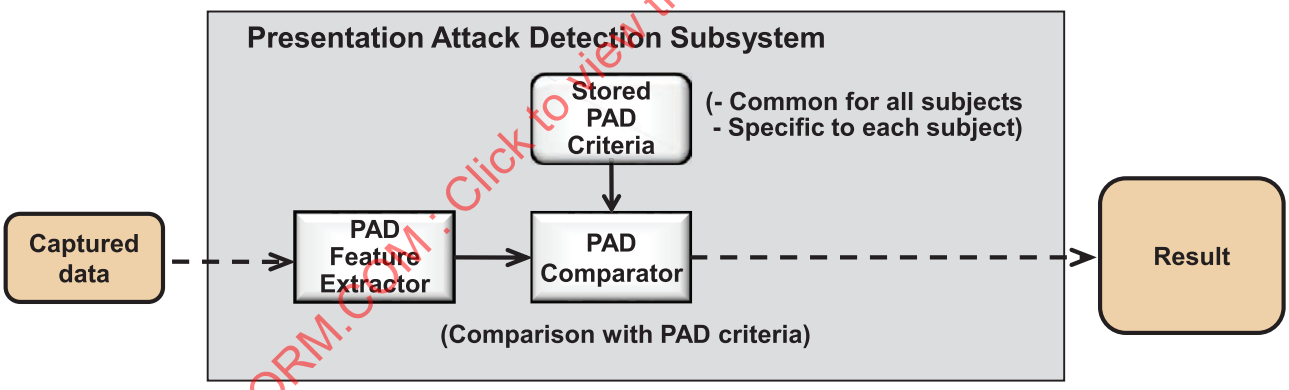

Figure 4 — Components in a general presentation attack detection subsystem

6.4.2 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 might 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 As a first example, a data capture device may be designed to generate biometric sample data and PAD data for each data capture event. Depending upon system design, such a data capture device may 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 is generated without the

