

ICS 35.240.15

CCS L 67



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 41815.3-2023

**Information technology - Biometric presentation attack
detection - Part 3: Testing and reporting**

Issued on: May 23, 2023

Implemented on: December 1, 2023

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface	
Introduction	
1 Scope	1
2 Normative references	1
3 Terms and Definitions	2

foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents"

drafting:

This document is part 3 of GB/T 41815 "Information Technology Biometric Recognition Presentation Attack Detection", GB/T 41815 has been issued

Published the following sections:

--- Part 1: Framework;

--- Part 2: Data format;

--- Part 3: Testing and reporting:

This document is equivalent to ISO /IEC 30107-3:2023 "Information Technology Biometric Recognition Presentation Attack Detection Part 3: Testing

Test and Report":

Please note that some contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents:

Introduction

To standardize the presentation of attack detection-related objects, it is necessary to first clearly present the attack detection framework as a whole to guide the detection of attacks:

Definition of classification and tools, secondly, in order to exchange and share relevant data elements, a clear and unified data format needs to be defined, and finally in

When evaluating the ability to detect attack on display, it is necessary to specify the test object, test environment and test indicators to guide the detection ability of attack on display:

Scientific and objective evaluation:

GB/T 41815 "Information Technology Biometric Feature Recognition Attack Detection" stipulates that the field of biometric feature recognition presents attack detection

The relevant framework, data format, and test-related content are used to facilitate the design of the attack detection function and the evaluation of its capabilities:

GB/T 41815 is proposed to consist of 3 parts:

--- Part 1: Framework: The purpose is to establish an overall framework related to attack detection in the biometric identification system, which is suitable for biometric identification systems:

Design and use of object feature recognition systems:

--- Part 2: Data format: The purpose is to standardize the data format related to attack detection, which is suitable for biometric identification systems

data exchange between them:

--- Part 3: Testing and reporting: The purpose is to clearly present the various factors that need to be considered in the evaluation of attack detection capabilities and the evaluation methods:

It is applicable to the analysis and evaluation of the attack detection capability of the biometric system:

The process of presenting a prosthetic or human body feature to a biometric acquisition subsystem in a manner intended to interfere with the system's policies is called a presentation attack:

hit: GB/T 41815 (all parts) presents techniques for automatic detection of attacks: These techniques are called Presence Attack Detection (PAD)

mechanism:

As in the case of biometric identification, the PAD mechanism is subject to false positive and false negative errors: False positive errors will be rendered as normal

Misclassified as an offensive presentation, which may draw attention to or inconvenience legitimate users: False negative errors will present an attack

Attacks (also known as attack renderings) are misclassified as normal renderings, which can lead to security breaches:

Therefore, which PAD implementation to use depends on the requirements of specific applications and the trade-off considerations of safety, strength and efficiency:

The purpose of preparing this document is to:

---Defining the terms of testing and reporting related to biometric identification presenting attack detection;

---Specify the performance evaluation principles and methods of biometric recognition presenting attack detection, including indicators:

This document is intended for suppliers or laboratories that need to evaluate the PAD mechanism:

Biometric performance testing terminology, practices, and methods of statistical analysis have been standardized: Wide range of indicators such as FAR, FRR and FTE

It is widely used to characterize the performance of biometric identification systems:

Due to the obvious difference between the biometric performance test and the PAD mechanism test, the biometric performance test technique

Language, practice, and statistical analysis methods are only partially applicable to the assessment of PAD mechanisms:

The differences between biometric performance tests and PAD mechanism tests can be grouped into the following categories:

a) Statistical significance

Biometric performance testing utilizes a statistically significant number of test subjects representative of the target user group: When adding more tests

There is no appreciable change in the error rate when using different subjects or using completely different test groups: In general, taking more measurements increases the error rate

accuracy:

In the PAD test, many biometric modalities can be attacked by a large or indeterminate number of potential PAI types: In these

case, it is difficult or even impossible to have all possible PAI synthesis models: So it is impossible to find a representative set of PAI types to

to evaluate: Therefore, it cannot be assumed that the error rate measured for one set of PAIs also applies to the other set:

PAI types were derived from systematic variation across trials: Different PAIs may have significantly different error rates: Furthermore, at any given

In the PAI type, the differences between PAI series instances will change randomly: The number of presentations required to test for statistical significance versus the number of concerns

The number of PAI types is linear: Within each PAI type, the uncertainty in the PAD error rate depends on the number of prostheses tested and on the individual

quantity:

Example 1: In fingerprinting, many effective prosthetic materials are known, but any material that can present the characteristics of a fingerprint to a biometric sensor

Or mixtures of materials are possible candidates: Due to the characteristics of the prosthesis, such as age, thickness, humidity, temperature, mixing rate and manufacturing specifications will affect the PAD mechanism:

Output has a significant impact, so tens of thousands of PAI types are easily identified using current materials: Thousands of presentations are required for proper statistical analysis

analysis: Even then, the resulting error rate cannot be applied to the next set of new materials:

b) Comparability of test results across systems

In biometric performance testing, the specific error rate based on the same biometric sample library can be used to compare different biometric characteristics:

sign recognition system or a different configuration: "Better" and "worse" are what people usually understand:

In contrast, when benchmarking PAD mechanisms using error rates, words such as "better" can be highly dependent on the expected

application:

Example 2: In a given test scenario, there are 10 types of PAI (occurring 100 times), System 1 detects 90% of attack presentations, System 2 detects

85%: System1 detected all presentations of 9 PAIs but failed to detect all presentations of the 10th PAI: System 2 detects all PAI types

85%: Which is better question, in security analysis, system 1 will be worse than system 2, because exposing the 10th PAI type will lead the attacker to use this method

Has been conquering the acquisition equipment: However, if an attacker could be prevented from using a 10th PAI type, then System 1 would be better than System 2, since individual rates show that,

All PAI types have the potential to overcome System 2:

c) cooperation

In many biometric performance testing applications, the main body is cooperative, such as