ICS 35.240.01
CCS L 67

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 41815.1-2022

Information technology - Biometric presentation attack detection - Part 1: Framework

Issued on: October 14, 2022 **Implemented on: May 1, 2023**

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

Table of Contents

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 of Standardization Documents"

drafted.

This document is part 1 of GB/T 41815 "Information Technology Biometric Recognition Presentation Attack Detection", GB/T 41815 has been issued

The following parts are distributed.

--- Part 1.Framework;

--- Part 2.Data format.

This document is equivalent to ISO /IEC 30107-1.2016 "Information technology biometric presence attack detection - Part 1.Box

shelf".

Please note that some content of this document may be patented. The issuing agency of this document assumes no responsibility for identifying patents.

Introduction

Biometric identification technology uses people's physiological and behavioral characteristics to identify individuals, so it is often used as a component of security systems.

into parts. Biometrics assist security systems in trying to identify friends or foes, and can also try to identify people unknown to the system.

Since the beginning of biometric identification technology, the possibility of attacking the technology has been recognized, so measures are taken to detect and defend against

Overwhelming identification of attempted and presented attacks is necessary. Attacks on

the intended functionality of biometrics can occur at any point within a security system

Any link occurs at any time, and can also be initiated by any implementer, whether it is an internal or external person in the system. The scope of this document is limited to the presentation

When collecting relevant biometrics, the technology that automatically detects the presence of the biometric collection subject to implement a presence attack is "presence attack detection" (PAD).

method.

Individuals who are the objects of biometric collection have potential security risks during data collection, which limits the use of biometric identification in the system.

use in applications overseen by the system owner agent, such as remote capture over untrusted networks. For example, with regard to electronic authentication

The guidelines do not recommend the use of biometrics as an authentication factor for this purpose. In unattended applications, such as over an open network

remote authentication over the network, the automatic presentation attack detection method can be applied to mitigate the attack risk. Standards, Best Practices and Independent Evaluation

technology can improve the security of all systems that employ biometrics, whether using supervised or unsupervised data collection, including

including systems that use biometrics to secure online transactions.

Like biometrics, PAD technology is subject to errors, including false positives and false negatives. false positives indicate false positives.

Often presentations are classified as attacks, thereby compromising the efficiency of the system, and a false negative indicates that presentation attacks are erroneously classified as normal presentations, without preventing

security breach. Therefore, the decision on which specific PAD implementation to use will depend on the specific application and trade-offs in terms of safety and efficiency

consider.

GB/T 41815 "Information Technology Biometric Recognition Present Attack Detection" stipulates the present attack detection phase in the field of biometric identification.

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

GB/T 41815 is intended 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.

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

The evaluation principles and methods are suitable for the analysis and evaluation of the attack detection capability of the biometric identification system.

To standardize the presentation of attack detection related objects, it is necessary to explicitly present the attack detection framework as a whole to guide the attack detection.

The definition of classification and tools, secondly, in order to exchange and share related data elements, it is necessary to define a clear and unified data format, and finally in the

When evaluating the presentation attack detection capability, it is necessary to clarify the test object, test environment and test indicators to guide the presentation attack detection capability.

scientific and objective assessment.

information technology biometrics presentation attack detection

Part 1.Framework

1 Scope

This document establishes terms and definitions commonly used to present the specification, characterization and evaluation of attack detection methods.

The scope not covered by this document is as follows.

--- Concrete presentation of the standardization of attack detection methods;

--- details about countermeasures (such as anti-spoofing techniques), algorithms or sensors;

--- Biometric system-level security or vulnerability assessment.

The attacks considered in this document are those that occur on sensors during the presentation and collection of biometric features.

Other attacks are outside the scope of this document.

2 Normative references

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, dated citations

documents, only the version corresponding to that date applies to this document; for undated references, the latest edition (including all amendments) applies to

this document.

GB/T 5271.37-2021 Information Technology Vocabulary Part 37.Biometric Identification (ISO /IEC 2382-37.20171),

MOD)

Note. There is no technical difference between the quoted content of GB/T 5271.37-2021 and ISO /IEC 2382-37.2012.

3 Terms and Definitions

The terms and definitions defined in GB/T 5271.37-2021 and the following apply to this document.

3.1

prosthetic artefact

A man-made object or representation that presents a replica of a biometric characteristic or a synthetic biometric modality.

3.2

liveness

Vital sign states that are clearly produced by anatomical features, involuntary responses (or physiological functions), or conscious responses (or subject behavior)

or feature.

Example 1.The absorption of light by skin and blood is an anatomical feature.

Example 2.Iris response to light and heart activity (pulse) are involuntary responses (also known as physiological functions).

Example 3.Gestures by pinching fingers together and biometric presentation by command prompts are conscious responses (also known as subject actions).

3.3

liveness detection