ICS 35.240.01
CCS L 67

中华人民共和国国家标准

GB/T 41815.1—2022/ISO/IEC 30107-1:2016

信息技术　生物特征识别呈现攻击检测　第1部分:框架

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

（ISO/IEC 30107-1:2016,IDT）

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 41815《信息技术　生物特征识别呈现攻击检测》的第1部分,GB/T 41815已经发布了以下部分:

——第1部分:框架;

——第2部分:数据格式。

本文件等同采用ISO/IEC 30107-1:2016《信息技术　生物特征识别呈现攻击检测　第1部分:框架》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位:中国电子技术标准化研究院、联想中天科技有限公司、平安科技(上海)有限公司、上海商汤智能科技有限公司、厦门市熠成信息技术有限公司、深圳赛西信息技术有限公司、北京旷视科技有限公司、北京万里红科技股份有限公司、北京眼神智能科技有限公司、北京中科虹霸科技有限公司、中国科学院自动化研究所、北京集创北方科技股份有限公司、云从科技集团股份有限公司、天津中科虹星科技有限公司、广州麦仑信息科技有限公司、杭州景联文科技有限公司、中国信息通信研究院、新大陆数字技术股份有限公司、蚂蚁科技集团股份有限公司、惠州学院、天复(东莞)标准技术有限公司、西安交通大学、北京邮电大学、广州广电运通金融电子股份有限公司、上海依图网络科技有限公司、北京澎思科技有限公司、深圳市腾讯计算机系统有限公司、国网区块链科技(北京)有限公司。

本文件主要起草人:钟陈、王思翔、史春腾、冷霜、王文峰、宋继伟、刘倩颖、王衍强、蒋慧、石红岩、何智勇、梅敬青、张小亮、杨春林、李星光、何召锋、雷震、樊磊、李军、李海青、崔峰科、刘云涛、傅山、宁华、李霖、林冠辰、罗中良、王成、蔺琛皓、张玮、张辰宇、谢佩博、王力宽、蒋增增、张慧、张默男、黄剑锋、秦日臻。

引　言

生物特征识别技术利用人的生理和行为特征对个人身份进行识别，因此经常被用作安全系统的组成部分。生物特征识别技术辅助安全系统以尝试识别朋友或敌人，也可以尝试识别系统未知的人。

从生物特征识别技术开始使用以来，该技术被攻击的可能性已被公认，因此采取措施检测和防御颠覆性的识别企图和呈现攻击是必要的。对生物特征识别技术预期功能的攻击可以在安全系统内的任何时刻任何环节发生，也可以由任何实施者发起，无论是系统内部或外部人员。本文件的范围限制在呈现和采集相关生物特征时，自动检测生物特征采集主体实施呈现攻击的技术即“呈现攻击检测”（PAD）方法。

作为生物特征采集对象的个人在数据采集时存在潜在安全隐患，这限制了生物特征识别在不受系统所有者代理监督的应用程序中的使用，例如在不受信任的网络上进行远程采集。例如，关于电子认证的准则不建议为此使用生物特征识别技术作为认证因素。在无人值守的应用程序中，例如通过开放网络进行远程身份验证，可以应用自动呈现攻击检测方法来减轻攻击风险。标准、最佳实践和独立评估的技术可以提高所有采用生物特征识别技术的系统的安全性，无论是使用有监督或无监督的数据采集，包括使用生物特征识别技术来确保在线交易安全的系统。

与生物特征识别技术一样，PAD 技术也会出现错误，包括假阳性和假阴性：假阳性指示错误地将正常呈现归类为攻击，从而损害了系统的效率，假阴性指示错误地将呈现攻击归类为正常呈现，没有防止安全漏洞。因此，决定采用何种具体 PAD 实施方式将取决于具体应用以及在安全和效率方面的权衡考虑。

GB/T 41815《信息技术　生物特征识别呈现攻击检测》规定了生物特征识别领域呈现攻击检测相关的框架、数据格式、测试相关的内容，以便于对呈现攻击检测功能的设计及其能力的评估。GB/T 41815拟由 3 部分构成。

——第 1 部分：框架。目的在于建立生物特征识别系统中呈现攻击检测相关的整体框架，适用于生物特征识别系统的设计和使用。

——第 2 部分：数据格式。目的在于规范呈现攻击检测相关的数据格式，适用于生物特征识别系统间的数据交换。

——第 3 部分：测试与报告。目的在于明确呈现攻击检测能力评估时需要考虑的各种因素以及评估原则和方法，适用于生物特征识别系统呈现攻击检测能力的分析与评估。

对呈现攻击检测相关对象进行标准化，需要首选从整体上明确呈现攻击检测框架以指导对攻击的分类及工具的定义，其次为了将相关数据元素进行交换和共享，需要定义明确、统一的数据格式，最后在对呈现攻击检测能力进行评估时需要明确测试对象、测试环境以及测试指标，指导对呈现攻击检测能力的科学、客观评估。

信息技术　生物特征识别呈现攻击检测 第1部分:框架

1　范围

本文件确立了常用于呈现攻击检测方法的规范、特性描述与评价的术语和定义。

本文件不涉及的范围如下:

——具体呈现攻击检测方法的标准化;

——关于对策(如反欺骗技术)、算法或传感器的详细信息;

——生物特征识别系统级安全或漏洞评估。

本文件中所要考虑的攻击是在呈现和采集生物特征识别特性期间发生在传感器上的攻击。

其他攻击不在本文件的范围内。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.37—2021　信息技术　词汇　第37部分:生物特征识别(ISO/IEC 2382-37:2017[1)],MOD)

注:GB/T 5271.37—2021被引用的内容与ISO/IEC 2382-37:2012被引用的内容没有技术上的差异。

3　术语和定义

GB/T 5271.37—2021界定的以及下列术语和定义适用于本文件。

3.1

假体　artefact

呈现生物特征识别特性副本或合成生物特征识别模态的人造物体或表现形式。

3.2

活体　liveness

明显由解剖特征、无意识的反应(或生理功能)、或有意识的反应(或主体行为)产生的生命体征状态或特性。

示例1:皮肤和血液对光照的吸收是解剖特征。

示例2:虹膜对光的反应和心脏活动(脉搏)是无意识的反应(也称为生理功能)。

示例3:将手指捏在一起做出手势以及按指令提示做出的生物特征识别呈现是有意识的反应(也称为主体行为)。

3.3

活体检测　liveness detection

对解剖学特征、无意识或有意识的反应的度量和分析,以确定采集到的生物特征样本是否来自在采集端的活人。

---

1)　ISO/IEC 2382-37的最新版本为2022年修订的版本,本文件涉及的相关内容没有技术性的修订。