ICS 35.240.15
L 71

中华人民共和国国家标准

GB/T 37036.1—2018

信息技术　移动设备生物特征识别 第1部分:通用要求

Information technology—Biometrics used with mobile devices—Part 1:General requirement

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 37036《信息技术　移动设备生物特征识别》分为以下4个部分：

——第1部分：通用要求；

——第2部分：指纹；

——第3部分：人脸；

——第4部分：虹膜。

本部分为GB/T 37036的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：浙江蚂蚁小微金融服务集团股份有限公司、中国电子技术标准化研究院、广州广电运通金融电子股份有限公司、北京旷视科技有限公司、北京中科虹霸科技有限公司、山西天地科技有限公司、北京天诚盛业科技有限公司、北京同方微电子有限公司、北京得意音通技术有限责任公司、长春鸿达光电子与生物统计识别技术有限公司、深圳市汇顶科技股份有限公司、北京海鑫科金高科技股份有限公司、广东远峰汽车电子有限公司、深圳信炜科技有限公司、广东光阵光电科技有限公司、北京集创北方科技股份有限公司、北京巴塔科技有限公司、杭州晟元数据安全技术股份有限公司、智慧海派科技有限公司、惠州市桑莱士智能科技股份有限公司、深圳芯起航科技有限公司、武汉虹识技术有限公司、深圳市一生微电子有限公司、江西合力泰科技有限公司、湖北润宏科技股份有限公司、浙江中正智能科技有限公司、燕南国创科技(北京)有限公司、神思电子技术股份有限公司、大唐微电子技术有限公司、北京曙光易通技术有限公司、广东智冠信息技术股份有限公司、北京中科奥森数据科技有限公司。

本部分主要起草人：胡静宜、落红卫、陈星、高健、孙曦、宋继伟、林冠辰、郑林、张鑫、李星光、冷霜、彭程、丁义民、郑方、李子青。

信息技术　移动设备生物特征识别
第1部分:通用要求

1　范围

GB/T 37036的本部分规定了移动设备生物特征识别的技术架构、通用流程、功能要求和安全要求。

本部分适用于移动设备生物特征识别系统的设计、生产、集成与应用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 26237(所有部分)　信息技术　生物特征识别数据交换格式

GB/T 26238　信息技术　生物特征识别术语

GB/T 33767.1—2017　信息技术　生物特征样本质量　第1部分:框架

GB/T 35273—2017　信息安全技术　个人信息安全规范

ISO/IEC 30107　信息技术　生物特征识别呈现攻击检测(Information technology—Biometric presentation attack detection)

3　术语和定义

GB/T 26238界定的以及下列术语和定义适用于本文件。

3.1

移动设备　mobile device

可接入网络的小型、可手持使用的信息技术产品。

注:移动设备可以包括平板式计算机、移动智能终端。

3.2

用户　user

以任何方式与生物特征识别系统交互的人或组织。

3.3

呈现攻击　presentation attack

以干扰生物特征识别系统的操作为目的,针对生物特征数据采集模块的一种攻击行为。

3.4

呈现攻击检测　presentation attack detection

对呈现攻击的自动检测。

3.5

质量　quality

生物特征样本满足目标应用的指定条件的程度。

注:指定的质量条件可涉及几方面,例如,影像清晰度、分辨率等。隐式质量条件决定获得正确匹配结果的可能性。

[GB/T 33767.1—2017,定义 4.14]

3.6

质量判断　quality judgment

对生物特征样本质量是否满足目标应用指定条件的检验过程。

3.7

执行环境　execution environment

存在于移动设备中的软硬件集合,为应用程序在移动设备中的运行提供必要的能力支持,一般包括硬件处理单元、易失性存储单元、非易失性存储单元、操作系统、调用接口等组件。

3.8

富执行环境　rich execution environment

运行在移动设备中的开放执行环境,为运行其中的应用程序提供开放、丰富的运行能力支持,但安全保护能力相对较弱。

3.9

可信执行环境　trusted execution environment

运行在移动设备中的隔离执行环境,具备较强的安全能力,以确保运行其中的应用程序、敏感数据等在相对可信的环境中得到存储、处理和保护。

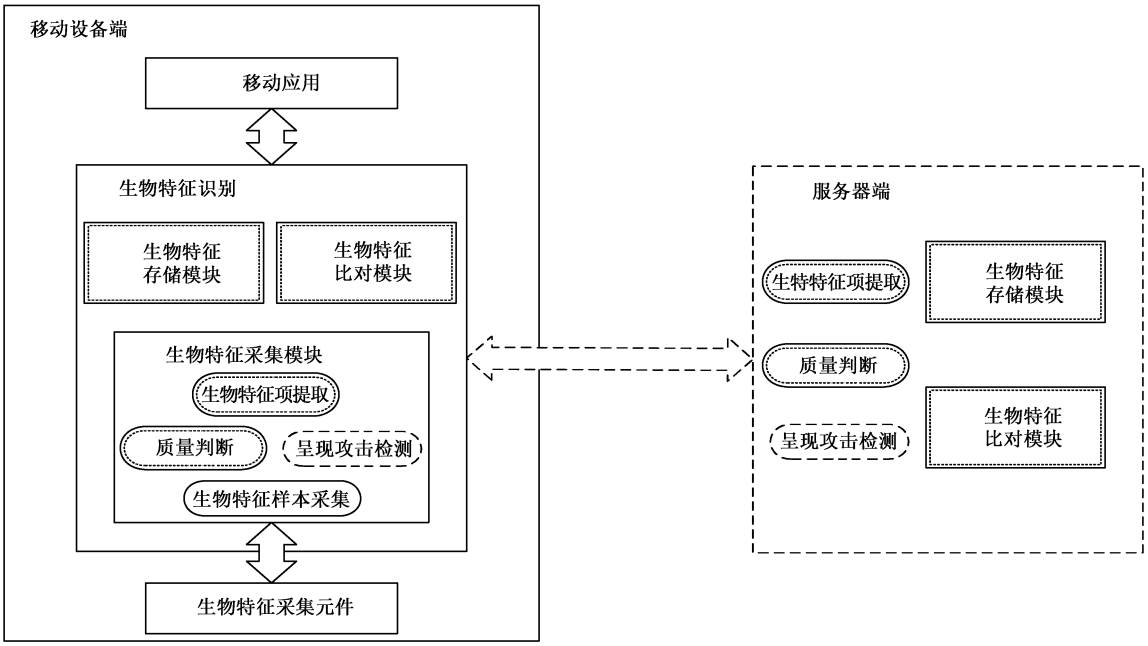
4　技术架构

移动设备上的生物特征识别技术架构主要由移动设备端和服务器端的若干功能模块构成,主要包括生物特征采集模块、生物特征存储模块、生物特征比对模块等。其中,生物特征采集模块包括生物特征样本采集、质量判断、呈现攻击检测、生物特征项提取等子功能模块。生物特征样本采集通过访问移动设备中的生物特征采集元件如图像采集元件、音频采集元件、指纹传感元件等对用户的生物特征样本进行采集。

通常情况下,移动设备上的生物特征识别过程可在移动设备本地完成,并向调用生物特征识别服务的移动应用输出识别结果。移动应用是移动设备中的生物特征识别的服务调用方,可为一个独立的移动应用软件、移动应用软件中的一个功能模块或移动设备操作系统提供的一个系统服务。在某些应用场景中,生物特征识别的部分模块或子模块如质量判断、呈现攻击检测、生物特征项提取等子模块、生物特征存储模块和生物特征比对模块可在服务器端完成相应的功能。

移动设备生物特征识别典型应用场景参见附录 A。

移动设备生物特征识别技术架构如图 1 所示。



说明：

——————— 必须具备的模块

- - - - - - - - - - - - - 可选具备的模块

▒▒▒▒▒▒▒▒▒▒▒▒▒▒▒ 必须具备的模块，根据不同方案，或位于移动设备，或位于选端服务器

图 1　移动设备生物特征识别技术架构

5　通用流程

移动设备生物特征识别通用流程包括登记、识别和注销三个过程：

a）　登记过程包括如下步骤：

1）　用户在移动设备上启动登记过程。

2）　移动设备上的生物特征采集模块采集用户生物特征样本，通过质量判断和呈现攻击检测后进一步提取用户生物特征项。

3）　将该用户生物特征项存储在生物特征存储模块中作为该用户的生物特征模板，并与用户身份标识关联起来。

4）　结束登记过程。

b）　识别过程包括如下步骤：

1）　用户在移动设备上启动识别过程。

2）　移动设备上的生物特征采集模块采集用户生物特征样本，通过质量判断和呈现攻击检测后进一步提取用户生物特征项。

3）　将提取的用户生物特征项与存储在生物特征存储模块中的一个或多个用户生物特征模板进行比对。

4）　根据比对结果进行识别决策并将识别结果输出。

5）　结束识别过程。

c）　注销过程包括如下步骤：

1）　用户在移动设备上启动注销过程。

2） 在移动设备上的生物特征存储模块中删除与待注销用户关联的全部生物特征模板，并删除待注销用户的身份标识。

3） 结束注销过程。

6 功能要求

6.1 一般要求

6.1.1 基本功能

移动设备生物特征识别的基本功能，包括但不限于：

a） 宜适用于不同人种、不同年龄的用户；

b） 宜适用于移动设备用户和生物特征识别系统管理员；

c） 宜支持多模态或多因子的生物特征识别；

d） 生物特征识别服务提供方应支持对错误接受率和错误拒绝率等性能指标的设定；

e） 宜支持对登记时间、识别时间和呈现攻击检测准确率等性能指标进行设定。

6.1.2 功能管理

移动设备生物特征识别应具备功能管理能力，包括但不限于：

a） 应支持新用户登记、已登记用户生物特征模板更新、已登记用户注销等功能；

b） 应支持用户登记生物特征模板到生物特征存储模块中；

c） 应支持用户删除已登记在生物特征存储模块中的生物特征模板；

d） 宜支持用户、生物特征识别系统管理员用户等不同用户使用权限，在生物特征识别中的采集、比对与存储等模块中分别具有相应的权限管理机制；

e） 应具备异常情况处理能力，包括但不限于生物特征采集失败、生物特征模板登记失败、生物特征模板删除失败、生物特征比对失败后的处理机制。

6.2 生物特征采集模块

6.2.1 基本功能

生物特征采集模块的基本功能，包括但不限于：

a） 应能使用移动设备生物特征采集模块采集用户生物特征样本，并将其转化成适合生物特征识别处理的数据格式；

b） 应具有明确的用户提示，告知用户对其生物特征样本进行了采集，若采集过程分为多次进行，宜向用户明示每一次采集的进度；

c） 应能从通过质量判断的用户生物特征样本中提取用户生物特征项，用于后续的生物特征存储或生物特征比对，宜采用不可逆的方式从用户生物特征样本中提取出生物特征项；

d） 应能将提取出的用户生物特征项传输到后续的处理模块，如生物特征存储模块或生物特征比对模块；

e） 应具备异常情况判定及处理能力，如生物特征样本采集失败、生物特征样本未通过质量判断、检测到呈现攻击、生物特征项提取失败等的相应处理机制。

6.2.2 质量判断

应能对采集到的用户生物特征样本进行质量判断，以确定当前生物特征样本是否满足生物特征识别处理的需求。

生物特征样本未通过质量判断时应具备相应的处理机制，如提示用户重新采集或提示失败等。

根据不同生物特征识别模态，质量判断的依据应符合 GB/T 33767.1—2017 对样本质量的要求。

6.2.3 呈现攻击检测

应能对当前被采集的用户生物特征样本进行呈现攻击检测，以防止恶意伪造。检测出呈现攻击时应具备相应的处理机制，如失败/错误提示或进行风险提示等。

呈现攻击检测应依据 ISO/IEC 30107 的方法。

6.2.4 数据交换格式

对成功采集的用户生物特征数据，应在扩展项中包括事件的标识符、唯一的设备标识符、采集日期和时间、生物特征样本的描述等数据。

存储和传输过程应支持 GB/T 26237(所有部分)规定的生物特征数据交换格式。

6.3 生物特征存储模块

生物特征存储模块应提供以下功能，包括但不限于：

a) 应具备生物特征存储模块管理功能，包括但不限于：应只允许具有合法权限的实体录入、访问、读取或删除生物特征存储模块中的用户生物特征数据；
b) 应能够把登记的用户生物特征模板与该用户的身份标识进行关联；
c) 同一用户在同一生物特征存储模块中应只对应唯一的身份标识；不能使用相同的用户身份标识去标识两个或以上不同用户；
d) 宜支持同一用户在生物特征存储模块中登记两个或多个生物特征模板；
e) 应具备异常情况判定及处理能力，如生物特征模板登记、读取或删除失败时的相应处理机制。

6.4 生物特征比对模块

6.4.1 基本功能

生物特征比对模块应提供下述至少一种识别功能：

a) 用户验证，即一对一比对；
b) 用户辨识，即一对多比对。

6.4.2 比对判定及处理

生物特征比对模块应提供以下功能，包括但不限于：

a) 能够将输入的用户生物特征项和已在生物特征存储模块中登记的生物特征模板进行比对，计算出比对得分；
b) 根据比对得分进行识别结果判定，并能够输出识别结果；
c) 应具备异常情况判定及处理功能，包括但不限于比对失败、识别决策失败时的相应处理机制。

7 安全要求

7.1 一般要求

移动设备生物特征识别一般安全要求，包括但不限于：

a) 应具备有效的安全机制，确保当前操作人员拥有合法权限完成用户登记、更新和注销；宜采取适当的机制和程序，在用户登记过程中确认当前登记者的真实身份；

b) 若生物特征识别支持不同用户使用权限，应具备有效的安全机制确保不同权限用户只能在其授权范围内进行相应操作。

7.2 生物特征采集模块安全

移动设备生物特征采集模块安全要求，包括但不限于：

a) 采集过程应在独立的逻辑域或物理域中实现；
b) 应具备有效的安全机制，确保生物特征样本采集、质量判断、呈现攻击检测、生物特征项提取和传输过程中的用户生物特征数据的机密性和完整性；
c) 应及时清除未通过质量判断的用户生物特征样本，并确保其不可恢复；
d) 生物特征项提取结束后应及时清除用户的生物特征样本，并确保其不可恢复；
e) 宜结合移动设备所具有的可信执行环境或安全单元实现上述安全机制。

7.3 生物特征存储模块安全

移动设备生物特征识别存储模块应满足下述安全要求，包括但不限于：

a) 应具备有效的安全机制，防止对生物特征存储模块的非授权访问；
b) 应具有有效的安全机制，确保已登记用户生物特征模板与该用户标识之间的正确关联关系，防止被非法修改；
c) 应具备有效的安全机制，确保在对生物特征存储模块中用户生物特征数据进行操作时，如存储和传输时，用户生物特征数据的机密性和完整性，并在操作完成后对操作过程中的临时数据（如存储或传输过程中，留存在设备动态内存中的生物特征样本等数据），进行及时清除并确保不可恢复；
d) 宜采用加密方式对用户生物特征模板数据进行存储；
e) 对于已删除的用户生物特征模板数据，应及时进行清除并确保不可恢复。
f) 宜结合移动设备所具有的可信执行环境或安全单元实现上述安全机制。

7.4 生物特征比对模块安全

移动设备生物特征识别比对模块应满足下述安全要求，包括但不限于：

a) 比对过程应在独立的逻辑域或物理域中实现；
b) 应具备有效的安全机制，确保在进行生物特征比对操作时：
   1) 生物特征模板读取的准确性；
   2) 生物特征数据不被窃取或篡改；
   3) 相似度计算结果不被窃取或篡改；
   4) 识别决策结果不被窃取或篡改；
   5) 比对结束后，按照 GB/T 35273—2017 规定来处理用户生物特征数据和比对过程中所产生的其他临时数据（如比对得分等）。
c) 应设定比对失败尝试次数限制，比对失败次数超出限制后，应采取相应的失败处理机制；
d) 应采取有效的安全机制，确保识别结果输出时的完整性，不被非法篡改；
e) 宜结合移动设备所具有的可信执行环境或安全单元实现上述安全机制。

7.5 安全环境

若移动设备支持可信执行环境或安全单元等安全环境，在生物特征采集、存储和比对过程中：

a) 宜使用位于可信执行环境中的生物特征采集模块对用户的生物特征样本进行采集；
b) 宜在可信执行环境中对采集的用户生物特征样本进行质量判断、呈现攻击检测和生物特征项提取；
c) 如果生物特征存储和比对模块在移动设备中实现，应在可信执行环境中实现生物特征存储和比对；
d) 宜使用可信执行环境或安全单元中的安全服务，如安全加解密服务、安全时钟服务、随机数服务等；
e) 应通过可信执行环境中可信交互界面实现与用户之间的交互；
f) 应在可信执行环境或安全单元中存储所涉及的密钥；
g) 如需与位于富执行环境的生物特征采集模块或移动应用进行数据交互时，应具备有效的安全机制验证富执行环境中交互对象的合法性，数据交互过程中宜采用安全通道机制以保证交互数据的完整性和机密性。

附 录 A
（资料性附录）
移动设备生物特征识别典型应用场景

A.1 移动设备解锁

生物特征识别用于移动设备解锁一般在移动设备本地实现，用于解锁设备，允许用户访问该设备或远程提供的其他服务和应用。例如：可以通过生物特征取代口令或设备解锁手势。在这种应用场景中，一般对设备、数据以及应用的安全保障要求不高。相对于安全性而言，这种应用场景更注重提高使用的便捷性，主要用于设备用户访问低安全保障水平的服务。

A.2 访问本地应用、服务和/或数据

生物特征识别技术在移动设备上用于对移动设备本地应用、服务和/或数据的访问。设备自行完成生物特征识别判定，并被设备本地应用程序调用，用于连续访问设备上的应用、服务，以及控制对某些特别保护数据的访问。这种应用场景一般在移动设备解锁以后执行，且只能被主屏幕显示的应用程序调用执行，以防止第三方应用或服务越权访问。例如：通过特定文件资源管理器来访问设备内存中受保护文件夹。在这种情况下，安全保障水平取决于具备相应权限用户的应用和访问步骤，根据所需安全保障水平的不同，可启用不同的阈值（如质量阈值或匹配阈值），为了避免第三方应用程序的误用，这些阈值不能持续改变，但可以对阈值加以限制，以确保既不会永远锁死系统也不至于全部通过。

A.3 建立通信信道

当待访问的服务或数据位于远程服务器时，在获得访问授权前，移动设备需先与服务器之间建立通信信道并进行鉴权，在此过程中，生物特征识别可被用来对设备用户进行身份鉴别，以确定是否可以建立通信信道。一些可能的场景为：

a) 在移动设备本地对用户进行生物特征识别并验证通过后，发放用于建立通信信道所需的鉴权令牌；
b) 在移动设备本地生成基于生物特征识别的鉴权令牌，该令牌可由远程服务器进行验证，以确定是否可以建立通信信道；
c) 直接发送生物特征样本到远程服务器，并与位于服务器上的已登记用户生物特征模板进行比对，以确定是否可以建立通信信道。在此过程中，用户可能会声明身份以进行一比一验证，也可能不声明以进行一比多辨识。

A.4 进一步验证/鉴别以访问远程资源

本场景描述的是在移动设备与远程服务器之间建立通信信道后的进一步验证/鉴别。虽然在建立通信信道时已经进行了验证，但远程服务器的数据/服务管理方认为仍有必要进一步验证/鉴别以允许用户获得对相关数据/服务的访问权限。例如：在创建通信信道时并非基于生物特征识别进行验证，根据数据/服务管理方的访问策略和确信等级要求，还需要对设备用户身份进一步进行生物特征识别后才授权进行数据/服务的访问。

参 考 文 献

[1] ISO/IEC TR 30125 Information technology—Biometrics used with mobile devices