



中华人民共和国国家标准

GB/T 37036.3—2019

信息技术 移动设备生物特征识别 第3部分：人脸

Information technology—Biometrics used with mobile devices—
Part 3: Face

2019-10-18 发布

2020-05-01 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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 技术架构	2
6 业务流程	3
7 功能要求	4
7.1 一般要求	4
7.2 人脸特征采集模块	5
7.3 人脸特征存储模块	6
7.4 人脸特征比对模块	7
8 性能要求	7
8.1 呈现攻击检测性能要求	7
8.2 识别性能要求	7
8.3 人脸识别响应速度	7
8.4 人脸登记失败率	7
9 安全要求	7
9.1 基本要求	7
9.2 人脸特征采集模块安全	8
9.3 人脸特征存储模块安全	8
9.4 人脸特征比对模块安全	8
9.5 传输安全	9
9.6 日志安全	9
附录 A (资料性附录) 移动设备人脸识别典型应用架构	10
附录 B (资料性附录) 移动设备人脸识别呈现攻击检测方法	14

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 3 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、北京中科虹霸科技有限公司、北京旷视科技有限公司、山西天地科技有限公司、广州广电运通金融电子股份有限公司、北京眼神科技有限公司、北京深醒科技有限公司、北京中科奥森科技有限公司、OPPO 广东移动通信有限公司、中国平安保险(集团)股份有限公司、北京智慧眼科技股份有限公司、山西平安谷信息技术有限公司、中科博宏(北京)科技有限公司、维沃移动通信有限公司、小米通讯技术有限公司、公安部第一研究所、北京市商汤科技开发有限公司、深圳市汇顶科技股份有限公司、北京曙光易通技术有限公司、杭州晟元数据安全技术有限公司、北京集创北方科技股份有限公司、上海聚虹光电科技有限公司、西安凯虹电子科技有限公司、山西云时代技术有限公司、中国信息通信研究院、杭州海康威视数字技术股份有限公司、北京清微智能科技有限公司、新大陆数字技术股份有限公司。

本部分主要起草人：冯春培、陈星、孙曦、高健、钟陈、王文峰、宋继伟、秦日臻、何召锋、李星光、吕盟、冷霜、宁静、林冠辰、杨春林、袁培江、贺兵、李子青、方攀、王衍强、王栋、陈永华、翁斌、王江胜、朱亚军、郑征、蒋慧、王浩、于雪平、胥建民、吴斌、樊磊、宫雅卓、刘敏、傅山、任文奇、王博、蔡春水。

信息技术 移动设备生物特征识别

第3部分：人脸

1 范围

GB/T 37036 的本部分给出了移动设备人脸识别系统的技术架构,规定了移动设备人脸识别的业务流程、功能要求、性能要求和安全要求。

本部分适用于移动设备人脸识别系统的设计、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 26238—2010 信息技术 生物特征识别术语

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

3 术语和定义

GB/T 26238—2010 界定的以及下列术语和定义适用于本文件。

3.1

人脸识别 face recognition

基于个体的人脸特征,对个体进行识别的过程。

3.2

人脸特征 face characteristic

可以从个体的人脸信息中提取出的有区别的、可重复的特征信息,从而达到个体自动识别的目的。

注：人脸特征可包括：人脸面部的解剖学特征、五官形态特征、特殊标记特征及人脸部因为手术或整容等人为形成的其他特征等。

3.3

人脸数据 face data

对处于任何处理阶段的人脸样本、人脸参考、人脸特征项或人脸特性的通称。

3.4

人脸采集装置 face capture device

收集人脸识别特征信息并将其转换成人脸样本的装置。

注：人脸采集装置可由若干部件组成,例如,发光源、一个或多个图像传感器等。

3.5

人脸样本 face sample

从人脸采集装置获得的模拟的或数字的人脸特征的代表。

3.6

人脸特征项 face feature

从人脸样本中提取的,用于比对的数值或标记。

3.7

人脸探针 face probe

输入到算法的、与人脸参考数据进行比对的人脸数据。

3.8

人脸模板 face template

参考的人脸特征项的集合,已存储的人脸特征项的集合,可直接与人脸探针的人脸特征项进行比对。

3.9

人脸参考 face reference

用于比对的、属于人脸数据主体的一个或多个已存储的人脸样本、人脸模板或人脸识别模型等。

3.10

用户主观配合度 user subjective cooperation level

在用户知情情况下,通过主动调整姿势、表情等方式力图通过人脸识别以获得身份授权。

3.11

攻击呈现错误接受率 attack presentation false acceptance rate

在特定场景中,采用攻击呈现手段进行呈现攻击被错误接受为真实人脸呈现的比例。

3.12

善意呈现错误拒绝率 bona fide presentation false rejection rate

在特定场景中,真实人脸呈现被错误判定为攻击呈现并被拒绝的比例。

3.13

攻击呈现无响应率 attack presentation non-response rate

采用攻击呈现手段进行呈现攻击的过程中,人脸识别系统出现无应答响应的比例。

3.14

善意呈现无响应率 bona fide presentation non-response rate

真实人脸呈现过程中,人脸识别系统出现无应答响应的比例。

4 缩略语

下述缩略语适用于本文件。

APFAR:攻击呈现错误接受率(Attack presentation false acceptance rate)

APNRR:攻击呈现无响应率(Attack presentation non-response rate)

BPFRR:善意呈现错误拒绝率(Bona fide presentation false rejection rate)

BPNRR:善意呈现无响应率(Bona fide presentation non-response rate)

FAR:错误接受率(False acceptance rate)

FRR:错误拒绝率(False rejection rate)

5 技术架构

移动设备人脸识别系统主要由移动设备端和远端服务器的若干功能模块构成,主要包括人脸特征采集模块、人脸特征存储模块、人脸特征比对模块等。其中,人脸特征采集模块包括人脸样本采集、质量判断、呈现攻击检测、人脸特征项提取等子功能模块。人脸识别系统通过访问移动设备中的人脸采集装

置对用户的人脸样本进行采集。

移动设备人脸识别主要包括本地识别和远程识别两种模式。

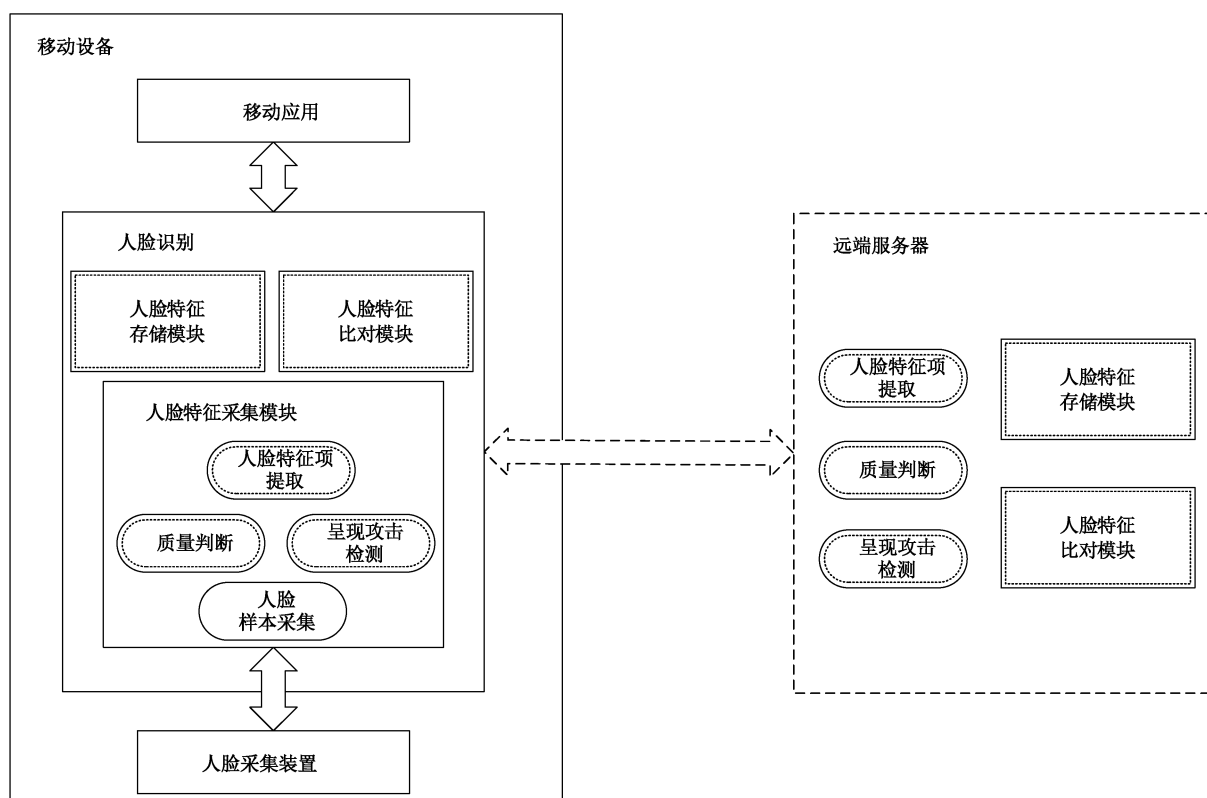
在本地识别模式中,人脸特征采集模块、人脸特征存储模块和人脸特征比对模块均在移动设备中实现,并在人脸特征采集模块中进行质量判断和呈现攻击检测。

在远程识别模式中,人脸特征采集模块在移动设备中实现,通过调用移动设备中存在的人脸采集装置(如摄像头、发光源等)采集人脸样本(如图像、视频、深度信息等),用于后续的人脸特征项提取、人脸特征存储或人脸特征比对;质量判断、呈现攻击检测和人脸特征项提取可在移动设备中实现,也可在远端服务器实现;人脸特征存储模块和人脸特征比对模块一般在远端服务器中实现。

一些可能的具体应用架构参见附录 A。

注:远端服务器用于比对的人脸模板可来自于其他已存在的且符合质量要求的人脸特征数据源。呈现攻击检测子模块可存在于人脸识别系统任意模块中。

移动设备人脸识别技术架构如图 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,或位于远端服务器。

图 1 移动设备人脸识别技术架构

6 业务流程

移动设备人脸识别的业务流程一般包括登记过程、识别过程和注销过程,要求如下:

- a) 登记过程应包括但不限于如下步骤：
 - 1) 移动应用在移动设备中启动登记过程；
 - 2) 移动设备中的人脸采集装置采集用户人脸样本；
 - 3) 进行质量判断、呈现攻击检测及用户人脸特征项提取；
 - 4) 将该用户人脸特征项存储在人脸特征存储模块中作为该用户的人脸模板，并与用户身份标识关联起来；
 - 5) 完成后结束登记过程。
 - b) 识别过程应包括但不限于如下步骤：
 - 1) 移动应用在移动设备中启动识别过程；
 - 2) 移动设备中的人脸采集装置采集用户人脸样本；
 - 3) 进行质量判断、呈现攻击检测及用户人脸特征项提取；
 - 4) 将提取的用户人脸特征项作为人脸探针，与存储在人脸特征存储模块中的一个或多个用户人脸模板进行比对；
 - 5) 根据比对结果进行识别决策并将识别结果输出，结束识别过程。
- 注：移动设备人脸识别系统可使用识别通过的人脸探针对存储在人脸特征存储模块中的用户人脸模板进行更新。
- c) 注销过程应包括但不限于如下步骤：
 - 1) 移动应用在移动设备中启动注销过程；
 - 2) 在人脸特征存储模块中删除与待注销用户关联的全部人脸参考，并在人脸识别中删除待注销用户的身份标识；
 - 3) 完成后结束注销过程。

7 功能要求

7.1 一般要求

7.1.1 基本功能

应符合 GB/T 37036.1—2018 的 6.1.1 的要求，包括但不限于：

- a) 适用于不同人种、不同年龄的用户；
- b) 结合其他生物特征识别技术形成多模态方案；
- c) 人脸识别系统服务提供方宜支持对错误接受率和错误拒绝率等性能指标的设定；
- d) 人脸识别系统服务提供方宜支持对呈现攻击检测性能指标进行设定。

7.1.2 功能管理

应符合 GB/T 37036.1—2018 的 6.1.2 的要求，包括但不限于：

- a) 支持新用户登记、已登记用户人脸模板更新、已登记用户注销等功能；
- b) 支持用户登记人脸模板到人脸特征存储模块中；
- c) 支持用户删除已登记在人脸特征存储模块中的人脸模板；
- d) 支持用户、人脸识别系统管理员用户等不同用户使用权限，在人脸识别中的采集、比对与存储等模块中分别具有相应的权限管理机制；
- e) 具备异常情况处理能力，包括但不限于人脸样本采集失败、人脸模板登记失败、人脸模板删除

失败、人脸特征比对失败后的处理机制。

7.1.3 日志管理

移动设备人脸识别应具备日志管理功能,包括但不限于:

- a) 产生日志记录的事件包括但不限于:
 - 1) 登记过程中的成功或失败事件;
 - 2) 识别过程中的成功或失败事件;
 - 3) 注销过程中的成功或失败事件;
 - 4) 人脸模板更新等。
- b) 对于每一个事件,日志记录包括事件发生时间、事件类型、用户、事件执行结果或失败原因、日志有效时间等。

7.2 人脸特征采集模块

7.2.1 基本功能

人脸特征采集模块提供人脸特征数据采集与传输的功能,包括但不限于:

- a) 应符合 GB/T 37036.1—2018 的 6.2.1 的要求;
- b) 宜采取技术手段对采集过程中用户所处的环境光照条件进行判断,在环境光照条件不适宜(如环境光照过亮或过暗等)的情况下宜提示用户配合改进;
- c) 宜采取技术手段对采集过程中用户在采集区域中出现的人脸区域遮挡情况、姿态等进行判断,在人脸区域不全(如有饰物遮挡或只有部分人脸在视频采集区域内)或姿态不适宜(人脸旋转、俯仰或倾斜角度过大)的情况下宜提示用户配合改进;
- d) 采集过程中视频区域内如出现多人脸或无人脸的情况,宜根据当前业务场景进行合理处置,如提示用户配合改进或设定规则选择主要人脸区域进行处理等。

7.2.2 质量判断

移动设备人脸特征采集模块应具备质量判断功能,且应符合 GB/T 37036.1—2018 的 6.2.2 的要求。

人脸样本质量判断功能:

- a) 应包括但不限于:
 - 1) 区域大小评估:判断样本中检测到的人脸区域大小是否符合人脸识别算法要求;
 - 2) 清晰度评估:判断样本中检测到的人脸区域清晰程度是否符合人脸识别算法要求;
 - 3) 完整度评估:判断样本中检测到的人脸区域完整程度是否符合人脸识别算法要求;
 - 4) 姿态角度评估:判断样本中检测到的人脸姿态的旋转角度、俯仰角度和倾斜角度是否在合理范围内。
- b) 宜包括但不限于:
 - 1) 眼睛闭合程度评估:对眼睛的闭合程度进行量化评估并判断是否符合人脸识别算法要求;
 - 2) 嘴巴闭合程度评估:对嘴巴的闭合程度进行量化评估并判断是否符合人脸识别算法要求;
 - 3) 光照度评估:判断样本中检测到的人脸区域光照情况是否符合人脸识别算法要求;
 - 4) 用户主观配合度评估:判断用户是否具备主观意愿配合进行人脸识别。

7.2.3 呈现攻击检测

移动设备人脸识别应具备呈现攻击检测功能,且应符合 GB/T 37036.1—2018 的 6.2.3 的要求。移动设备人脸识别呈现攻击检测功能,宜能支持对下述呈现攻击类型的检测,如表 1 所示。一些可用的移动设备人脸识别呈现攻击检测方法参见附录 B。

表 1 移动设备人脸识别呈现攻击类型及检测条件因素

呈现攻击类型		呈现攻击检测条件因素	
二维呈现攻击类型	静态图像	纸质	检测条件因素包括但不限于: a) 图像材质如普通的 A4、A3 打印纸、亚光相纸、高光相纸、绒面相纸等; b) 人脸区域的分辨率、清晰度、大小、脸部拍摄角度、光照条件以及人脸区域占据纸面比例等; c) 攻击者尝试通过不同距离、不同角度、不同方向移动纸质图像,以及弯曲纸质图像等方式进行攻击
		电子	检测条件因素包括但不限于: a) 电子图像的显示设备类型; b) 显示设备的分辨率、亮度、对比度等; c) 人脸区域清晰度、分辨率、脸部占屏幕比例、脸部拍摄角度、光照条件等; d) 攻击者尝试通过不同距离、不同角度及不同方向移动电子图像进行攻击等
	动态图像	录制视频	检测条件因素包括但不限于: a) 视频图像的显示设备类型; b) 显示设备的分辨率、亮度、对比度; c) 视频图像的清晰度、分辨率、帧率等; d) 视频图像中人脸占屏幕比例、脸部的拍摄角度、光照条件等
		合成视频	检测条件因素包括但不限于: a) 视频图像的显示设备类型; b) 显示设备的分辨率、亮度、对比度; c) 视频图像的分辨率、帧率、逼真程度等; d) 视频图像中人脸占屏幕比例、光照条件等
三维呈现攻击类型	面具	塑料面具	检测条件因素包括但不限于: a) 攻击距离、攻击角度、移动方向; b) 面具的俯仰、旋转、倾斜角度; c) 攻击者佩戴已去除眼部、鼻子或嘴巴等区域的面具进行攻击等
		纸面具	
		硅胶面具	
	头模	泡沫头模	检测条件因素包括但不限于: a) 攻击距离、攻击角度、移动方向; b) 头模的俯仰、旋转、倾斜角度; c) 环境背景光照的强弱、冷温、色彩等
树脂头模			

7.3 人脸特征存储模块

人脸特征存储模块应提供以下功能,包括但不限于:

- a) 支持将登记的用户人脸特征模板与该用户的身份标识进行关联;
- b) 支持已登记用户对人脸特征存储模块中属于该用户的人脸模板进行增加、删除等操作;

- c) 支持同一用户在人脸特征存储模块中登记一个或多个在不同光照或不同姿态下提取的人脸模板；
- d) 具备异常情况判定及处理能力,如人脸模板登记、读取或删除失败时的相应处理机制。

7.4 人脸特征比对模块

人脸特征比对模块应提供以下功能,包括但不限于:

- a) 将输入的用户人脸特征项和已在人脸特征存储模块中登记的人脸模板进行比对,计算出比对得分;
- b) 根据比对得分进行识别决策,并能够输出识别结果;
- c) 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。

8 性能要求

8.1 呈现攻击检测性能要求

移动设备人脸识别系统的呈现攻击检测性能要求如表 2 所示。

表 2 呈现攻击检测性能要求

攻击类型	性能要求		
	BPFRR 和 APFAR	APNRR	BPNNR
二维呈现攻击类型	在 APFAR 为 3% 时, BPFRR 应不高于 3%	在响应时间为 1 s 的情况下 APNRR 应不高于 5%	在响应时间为 1 s 的情况下 BPNNR 应不高于 3%
三维呈现攻击类型	在 APFAR 为 5% 时, BPFRR 应不高于 5%		

8.2 识别性能要求

移动设备人脸识别系统的识别性能要求为:在 FAR 不高于 0.01% 时 FRR 不高于 10%。

8.3 人脸识别响应速度

移动设备人脸识别系统完成人脸特征项提取、人脸特征比对并输出识别结果的流程总时间应不超过 2 s。

8.4 人脸登记失败率

移动设备人脸识别系统的用户人脸登记失败率应不高于 1%。

9 安全要求



9.1 基本要求

基本安全要求包括但不限于:

- a) 应符合 GB/T 37036.1—2018 的 7.1 的要求;
- b) 在采集用户人脸样本前,应向用户明确告知所提供的产品或服务收集、使用用户人脸数据的规

则,并获得用户的授权同意;

- c) 人脸识别注销发起前应对操作者身份进行鉴别和权限确认,在人脸识别注销完成后,应确保所有关联人脸数据被删除并不可恢复;
- d) 位于移动设备中的功能模块在运行时宜具备运行环境的检查能力,检查范围可包括移动设备系统是否被非法用户获取管理员权限、程序运行环境是否可信等,在发现运行环境异常时应具备相应处理措施,如提示用户安全风险、关闭应用等;
- e) 位于移动设备中的功能模块应采取安全措施确保只有具备调用权限的调用方才能调用该模块;
- f) 位于移动设备中的功能模块应采取安全加固措施如反编译、完整性检查等提升自身安全防护水平。

9.2 人脸特征采集模块安全

人脸特征采集模块安全要求包括但不限于:

- a) 应符合 GB/T 37036.1—2018 的 7.2 的要求;
- b) 应设置人脸特征采集超时处理机制,即在设置的有效时长内,如无法采集到符合质量要求的且通过呈现攻击检测的人脸样本时,模块自动退出运行;
- c) 应采取有效的安全措施对用户输入的敏感数据或采集到的用户人脸数据进行安全保护,确保其保密性和完整性,不被非法窃取或者篡改,如结合移动设备中可信环境实现;
- d) 人脸特征项提取结束后应在移动设备中及时清除用户的人脸样本,并确保其不可恢复。

9.3 人脸特征存储模块安全

9.3.1 一般要求

应符合 GB/T 37036.1—2018 的 7.3 的要求。

9.3.2 远程识别模式

远程识别模式中,人脸特征存储模块安全要求包括但不限于:

- a) 应将用户人脸参考与用户身份标识信息分库保存,并宜对用户人脸参考进行伪名化处理;
- b) 宜采用加密的方式在人脸特征存储模块中存储用户的人脸参考,并对存储的用户人脸数据实施严格的访问控制策略。

9.3.3 本地识别模式



本地识别模式中,应采取有效的安全措施对本地存储的用户人脸数据进行安全保护,确保其保密性和完整性,不被非法窃取或者篡改,如结合移动设备中可信环境实现。

9.4 人脸特征比对模块安全

9.4.1 一般要求

应符合 GB/T 37036.1—2018 的 7.4 的要求。

9.4.2 远程识别模式

远程识别模式中,应在远端服务器上采取有效的安全措施对人脸特征比对模块进行保护,确保比对过程中所使用的用户人脸数据的保密性和完整性以及识别决策结果的完整性。

9.4.3 本地识别模式

本地识别模式中,人脸特征比对模块一般是以软件的形式在移动设备中实现,应采取有效的安全措施确保该模块的安全性,并确保比对过程中所使用的用户人脸数据的保密性和完整性以及识别决策结果的完整性,如结合移动设备中可信环境实现。

9.5 传输安全

在人脸识别不同模块间传递人脸数据时:

- a) 传输过程中应对通信对方的真实身份进行鉴别,鉴别通过后应建立安全通道对人脸数据在传输过程中的保密性和完整性进行保护;
- b) 应采取有效措施防范重放攻击,如不可预测随机数、时间戳或挑战/应答等方式;
- c) 远程识别模式中,从移动设备中传输人脸数据到远端服务器进行比对并返回识别决策结果时,应采取有效的安全方式对传输的人脸数据以及识别决策结果进行安全保护,确保其保密性和完整性,不被窃取或篡改;
- d) 应采取有效的安全措施对传输过程使用的密钥进行安全保护,如结合移动设备中可信环境实现。

9.6 日志安全

日志安全要求包括但不限于:

- a) 日志记录中不应出现明文的人脸数据、密钥信息或其他安全相关的参数等;
- b) 应采取安全措施对日志信息做完整性保护,如数字签名等;
- c) 应具备授权管理机制,对日志记录的增加、删除、修改的操作权限进行管理。

附录 A
(资料性附录)

移动设备人脸识别典型应用架构

A.1 概述

本附录主要对应用于移动设备上的人脸识别系统的典型应用架构模式进行描述。移动设备的操作环境又可进一步细分为富执行环境和可信环境。

A.2 典型应用架构

A.2.1 结合可信环境的本地识别模式

图 A.1 描述了典型模式一。这种模式下,人脸特征存储和比对模块都位于移动设备中,出于安全性考虑,人脸识别系统的各模块应由移动设备中可信环境进行保护。人脸采集装置支持通过可信环境访问。

移动应用一般位于富执行环境中,通过可信环境提供的对外接口调用人脸识别系统,人脸识别系统调用人脸采集装置开展对人脸样本的采集,在进行质量判断、呈现攻击检测后提取人脸特征项,根据目的不同进行人脸登记或者识别过程,并将执行结果反馈给移动应用。

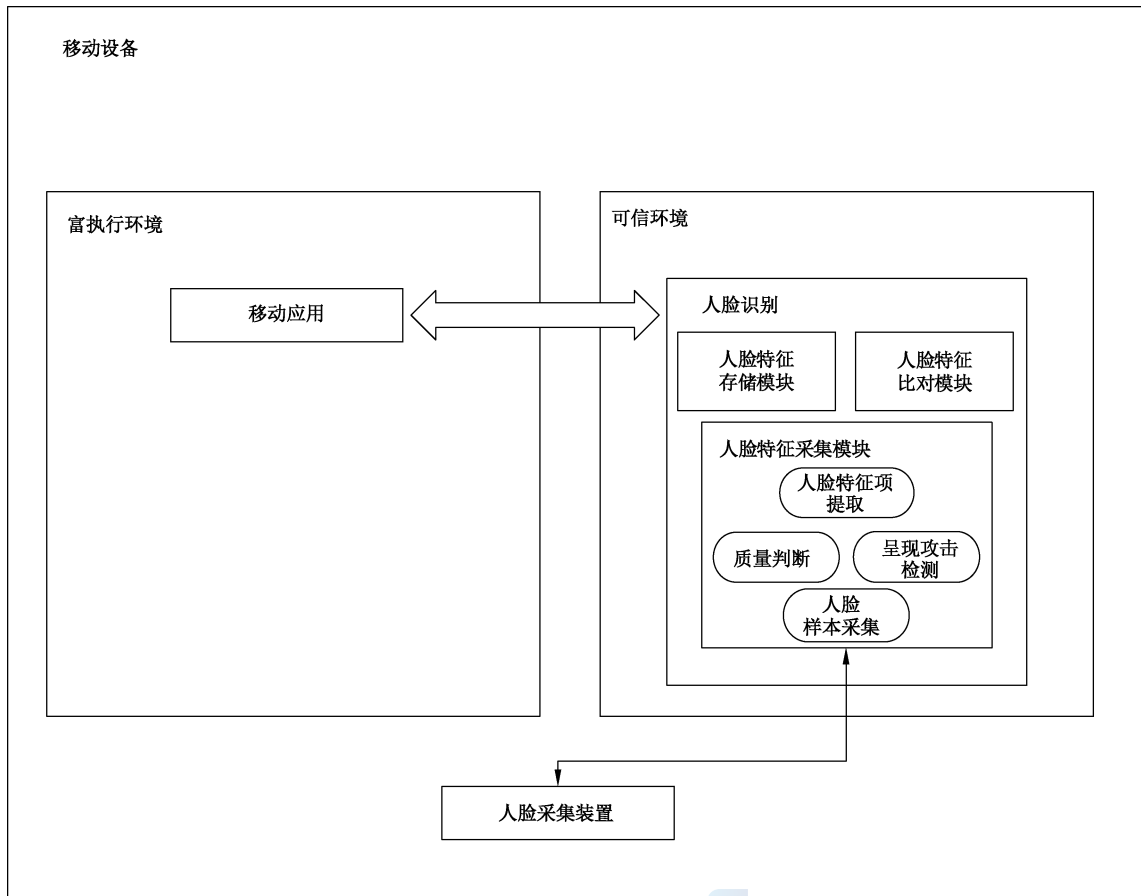
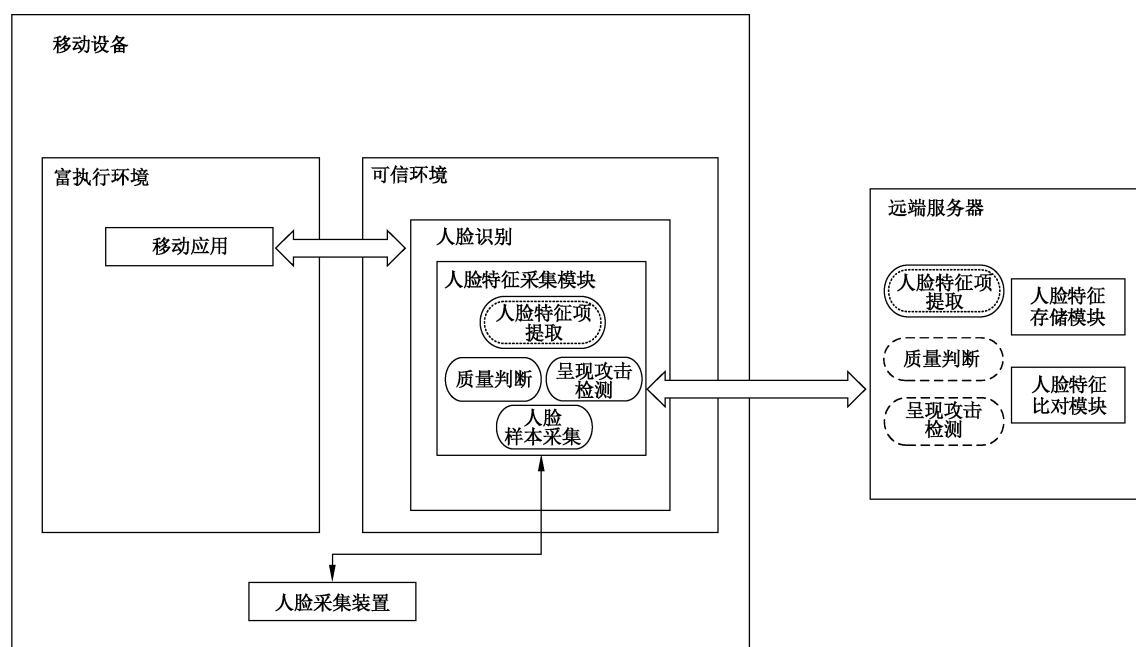


图 A.1 模式一 结合可信环境的本地识别模式

A.2.2 结合可信环境的远程识别模式

图 A.2 描述了典型模式二。这种模式下,人脸特征采集模块位于移动设备中,人脸特征存储模块和人脸特征比对模块在远端服务器完成。为提升安全性,位于移动设备中的人脸特征采集模块在可信环境中实现。人脸采集装置支持通过可信环境访问。

移动应用一般位于富执行环境,通过可信环境提供的对外接口调用人脸识别系统,人脸识别系统调用人脸采集装置开展对人脸样本的采集,并访问远端服务器进行人脸登记或识别过程,完成后向调用人脸识别的移动应用反馈结果。



说明：

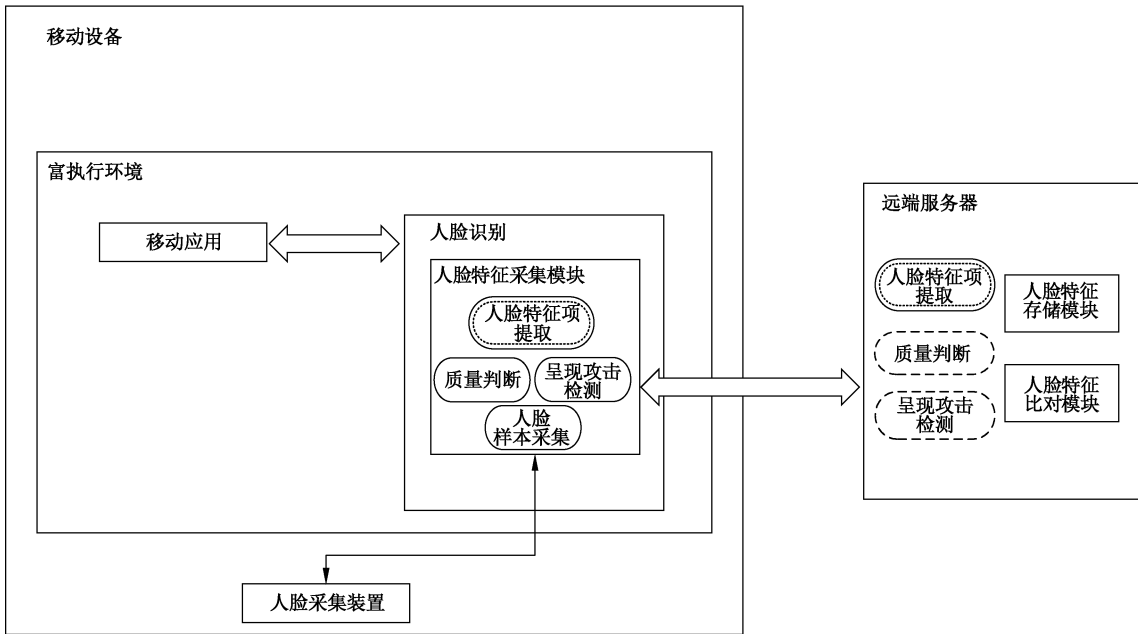
- 必须具备的模块；
- 可选具备的模块；
- ===== 必须具备的模块,根据不同方案,或位于移动设备,或位于远端服务器。

图 A.2 模式二 结合可信环境的远程识别模式

A.2.3 未结合可信环境且在移动设备中进行呈现攻击检测的远程识别模式

图 A.3 描述了典型模式三。这种模式下,人脸特征采集模块位于移动设备中,人脸特征存储模块和人脸特征比对模块在远端服务器完成。位于移动设备中的人脸特征采集模块在富执行环境中实现。人脸采集装置支持通过富执行环境进行访问。

移动应用一般位于富执行环境,调用人脸识别系统后通过人脸采集装置开展对人脸样本的采集,在进行质量判断、呈现攻击检测后,访问远端服务器进行人脸登记或识别过程,完成后向调用人脸识别的移动应用反馈结果。



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，或位于远端服务器。

图 A.3 模式三 未结合可信环境且在移动设备中进行呈现攻击检测的远程识别模式

A.2.4 未结合可信环境且在远端服务器进行呈现攻击检测的远程识别模式

图 A.4 描述了典型模式四。这种模式下，人脸特征采集模块位于移动设备中，但仅实现了人脸样本采集功能。质量判断、呈现攻击检测、人脸特征项提取以及人脸特征存储模块和人脸特征比对模块在远端服务器完成。移动设备中的人脸特征采集模块在富执行环境中实现，人脸采集装置支持通过富执行环境进行访问。

移动应用一般位于富执行环境，调用人脸识别系统后通过人脸采集装置采集人脸样本，再送至远端服务器对人脸样本进行质量判断、呈现攻击检测后提取人脸特征，并根据需要进行人脸登记或识别过程，完成后向调用人脸识别的移动应用反馈识别结果。



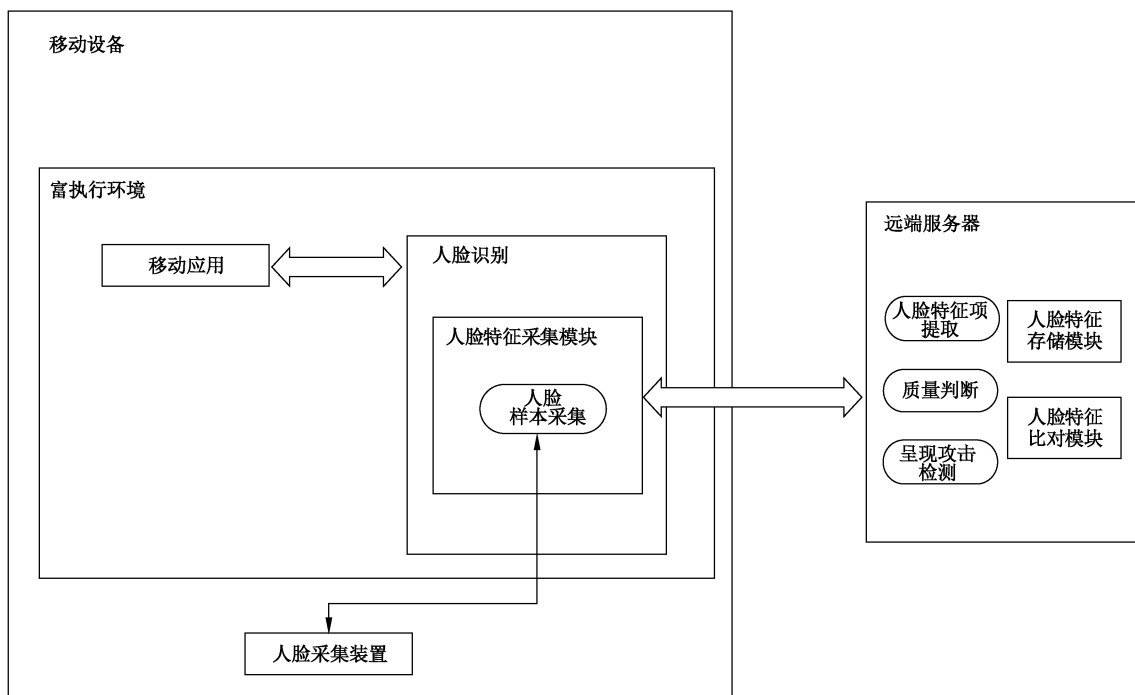


图 A.4 模式四 未结合可信环境且在远端服务器进行呈现攻击检测的远程识别模式

附 录 B
(资料性附录)

移动设备人脸识别呈现攻击检测方法

移动设备人脸识别具备的呈现攻击检测功能可采用以下方法实现：

- a) 离散图像检测方法,即利用一幅或多幅图像进行判断;
 - b) 连续图像检测方法,即采用连续图像序列进行判断,如检测显示器边缘、边框、屏幕反光、像素点、条纹分析等进行判断;
 - c) 用户主动配合检测方法,即通过指令要求用户完成相应动作如点头、抬头、左右转头、张嘴、眨眼、跟读屏显提示信息等进行判断;
 - d) 基于辅助硬件设备的检测方法,即利用辅助硬件设备获取更多信息辅助进行判断,如利用深度摄像头采集人脸深度信息、或利用特定波长光源投射人脸并检测材质发射率差异等;
 - e) 用户被动配合检测方法,如:
 - 1) 利用静脉血管、肌肉、骨骼、静脉血液中脱氧血色素对红外线的吸收特性,判断其是否来自活体;
 - 2) 通过特定指令引导用户眼睛运动,并通过跟踪眼睛运动以判断是否为真实活体;
 - f) 结合多种方法进行呈现攻击检测,并对不同方法计算得出的检测结果置信度进行综合处理(如采用置信度加权等方式)后给出呈现攻击检测结果。
-

