ICS 35.240.15
CCS L 71

中华人民共和国国家标准

GB/T 37036.4—2021

信息技术　移动设备生物特征识别 第4部分：虹膜

Information technology—Biometrics used with mobile devices—Part 4：Iris

2021-04-30 发布　　2021-11-01 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 37036《信息技术　移动设备生物特征识别》的第4部分。GB/T 37036已经发布了以下部分：

——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。

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：北京中科虹霸科技有限公司、中国电子技术标准化研究院、浙江蚂蚁小微金融服务集团股份有限公司、中科天地科技有限公司、北京眼神智能科技有限公司、OPPO广东移动通信有限公司、北京集创北方科技股份有限公司、深圳市铭图创新科技有限公司、厦门乐翠网络科技有限公司。

本文件主要起草人：何召锋、钟陈、王文峰、宋继伟、高健、孙元博、冷霜、宋方方、欧锦荣、张晋芳、李清顺、李星光、周水子、张慧、刘京、邱显超、马力、吴影。

引　言

GB/T 37036《信息技术　移动设备生物特征识别》拟由九个部分构成。

——第1部分：通用要求，目的在于规定移动设备生物特征识别技术通用要求，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。

——第2部分：指纹，目的在于规定移动设备指纹生物特征识别技术要求，适用于移动设备指纹识别系统的设计、生产、集成与应用。

——第3部分：人脸，目的在于规定移动设备人脸生物特征识别技术要求，适用于移动设备人脸识别系统的设计、生产、集成与应用。

——第4部分：虹膜，目的在于规定移动设备虹膜生物特征识别技术要求，适用于移动设备虹膜识别系统的设计、生产、集成与应用。

——第5部分：声纹，目的在于规定移动设备声纹生物特征识别技术要求，适用于移动设备上声纹生物特征识别的研发、生产、集成和应用。

——第6部分：指静脉，目的在于规定移动设备指静脉生物特征识别技术要求，适用于移动设备指静脉识别系统的设计、生产、集成与应用。

——第7部分：多模态融合，目的在于规定移动设备多模态生物特征识别技术要求，适用于移动设备上生物特征识别多模态融合识别产品设计、研发、生产、集成和应用。

——第8部分：呈现攻击检测，目的在于规定移动设备呈现攻击检测要求，适用于在移动设备上使用生物特征识别技术进行身份鉴别时，对呈现攻击检测系统的设计、生产、应用、评估活动进行指导。

——第9部分：性能测试，目的在于规定移动设备性能测试要求，适用于移动设备上使用生物特征识别系统的性能测试。

虹膜识别基于虹膜的纹理特征，与已知的虹膜参考进行特征比对，从而鉴别用户真实身份。虹膜识别技术具有唯一性、稳定性、非接触式、大容量的特点，在移动设备中具有广泛的应用场景。本文件给出移动设备虹膜生物特征识别技术要求。

信息技术　移动设备生物特征识别
第4部分：虹膜

1　范围

本文件提出了应用于移动设备虹膜识别的系统构成和业务流程，规定了移动设备上虹膜识别的功能要求、性能要求和安全要求。

本文件适用于移动设备虹膜识别系统的设计、生产与应用。

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 20145—2006　灯和灯系统的光生物安全性

GB/T 26237.6—2014　信息技术　生物特征识别数据交换格式　第6部分：虹膜图像数据

GB/T 33767.6—2018　信息技术　生物特征样本质量　第6部分：虹膜图像数据

GB/T 35783—2017　信息技术　虹膜识别设备通用规范

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

ISO/IEC 30107-3：2017　信息技术　生物特征识别呈现攻击检测　第3部分：测试和报告（Information technology—Biometric presentation attack detection—Part 3：Testing and reporting）

3　术语和定义

下列术语和定义适用于本文件。

3.1

虹膜特征　iris characteristic

可以从个体的虹膜信息中提取出的有区别的、可重复的特征信息。

3.2

虹膜识别　iris recognition

基于个体的虹膜特征信息，对该个体进行识别的过程。

3.3

虹膜采集模块　iris capture device

收集虹膜识别特征信息并将其转换成虹膜样本的功能模块组件。

3.4

虹膜样本　iris sample

从虹膜采集模块获得的模拟的或数字的虹膜特征的信息数值。

3.5

虹膜特征项　iris feature

从虹膜样本中提取的，用于比对的数值或标记。

3.6

呈现攻击误判率　attack presentation classification error rate

在特定场景中，采用同类呈现攻击手段进行呈现攻击被误判为真实虹膜呈现的比例。

3.7

真实呈现误判率　bona fide presentation classification error rate

在特定场景中，真实虹膜呈现被误判为呈现攻击的比例。

3.8

呈现攻击无响应率　attack presentation non-response rate

采用同类呈现攻击手段进行呈现攻击的过程中，虹膜识别系统出现无应答响应的比例。

3.9

真实呈现无响应率　bona fide presentation non-response rate

真实虹膜呈现过程中，虹膜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。

APCER　呈现攻击误判率(attack presentation classification error rate)

APNRR　呈现攻击无响应率(attack presentation non-response rate)

BPCER　真实呈现误判率(bona fide presentation classification error rate)

BPNRR　真实呈现无响应率(bona fide presentation non-response rate)

FAR　错误接受率(false accept rate)

FRR　错误拒绝率(false reject rate)

MTF　调制传递函数(modulation transfer function)

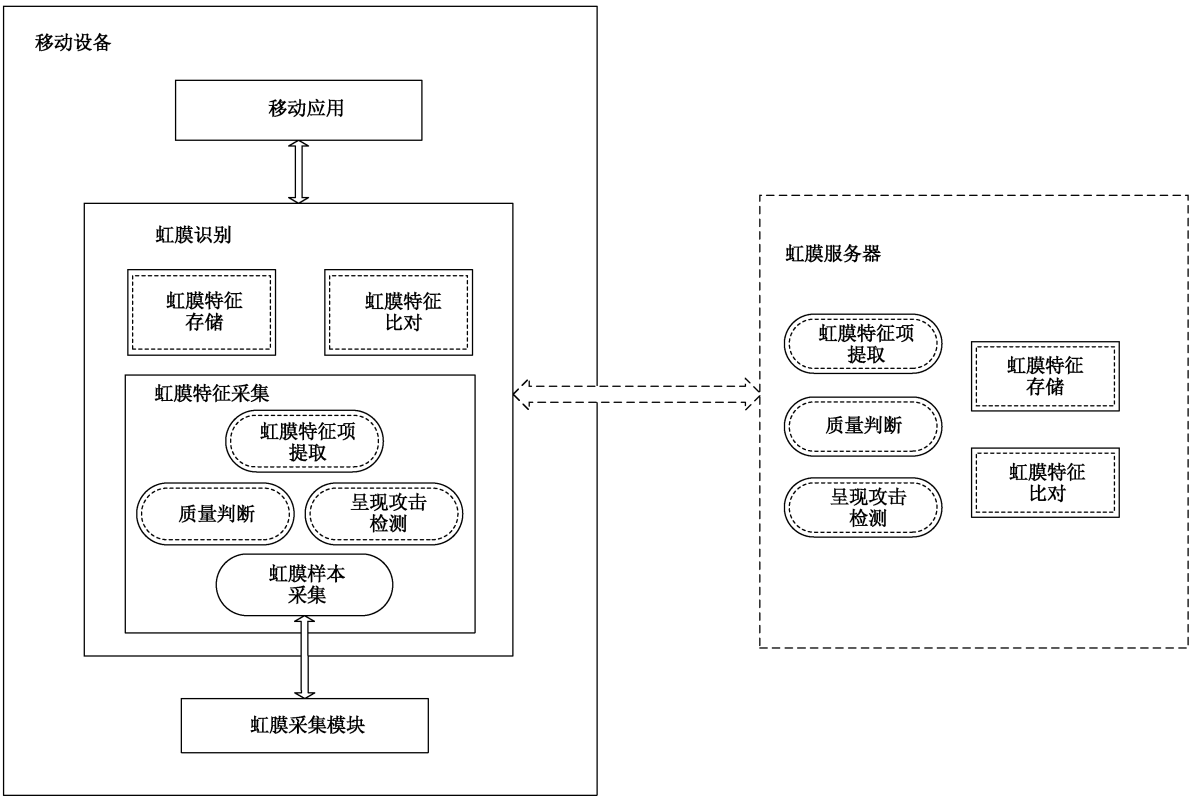
REE　富执行环境(rich execution environment)

SE　安全单元(secure element)

TEE　可信执行环境(trusted execution environment)

5　系统构成

本文件给出的移动设备虹膜识别系统构成是GB/T 37036.1—2018中描述的通用技术架构在虹膜识别应用领域的具体化，见图1。



注：图中线框说明。

——————　应具备的功能；

- - - - - - - - - - - - - -　可选具备的功能；

——————　应具备的功能，根据不同方案，或位于移动设备，或位于虹膜服务器。

图 1　移动设备虹膜识别系统构成

移动设备端包括虹膜采集模块、虹膜识别、移动应用三部分。其中，虹膜采集模块提供现场虹膜采集功能。虹膜识别提供虹膜特征采集、虹膜特征存储和虹膜特征比对功能。移动应用是移动设备中的虹膜识别的服务调用方，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。

注：对虹膜采集模块和移动应用的要求不在本文件规定。

虹膜特征采集的主要作用是通过访问移动设备中的虹膜采集模块采集虹膜样本，再进行质量判断、呈现攻击检测和虹膜特征项提取。虹膜特征存储的主要作用是虹膜模板存储。虹膜特征比对的主要作用是将虹膜特征项与存储的虹膜模板进行比对，并将比对结果输出到移动应用。

其中虹膜特征存储、虹膜特征比对以及虹膜特征采集中的质量判断、呈现攻击检测和虹膜特征项提取等功能可位于移动设备端，也可位于虹膜服务器端，这些功能在移动设备端或者虹膜服务器所起的作用相同。

移动设备虹膜识别的应用有两类模式，包括位于移动设备中的本地识别模式和结合虹膜服务器的远程识别模式。

在本地识别模式中，虹膜特征采集、虹膜特征存储和虹膜特征比对功能均在移动设备中实现，并向调用虹膜识别服务的移动应用输出识别结果。在远程识别模式中，虹膜样本采集在移动设备中实现，虹膜特征项提取、质量判断、呈现攻击检测、虹膜特征存储、虹膜特征比对中的一个或多个功能在虹膜服务器端执行。一些典型应用架构见附录 A。

6 业务流程

移动设备虹膜识别流程主要包括虹膜登记过程、虹膜识别过程和虹膜注销过程。

a) 虹膜登记过程，包括但不限于如下步骤：
   1) 启动虹膜登记过程；
   2) 对用户进行身份鉴别和权限检查，如果鉴别通过则进行虹膜样本采集，否则重新进行身份鉴别和权限检查；
   3) 对采集的虹膜样本进行质量判断、呈现攻击检测，如果检测通过则提取虹膜特征项数据，否则重新进行虹膜样本采集；
   4) 存储虹膜特征项数据，作为该用户的虹膜模板，并与用户身份标识关联；
   5) 结束虹膜登记过程，记录虹膜登记日志。
b) 虹膜识别过程，包括但不限于如下步骤：
   1) 启动虹膜识别过程；
   2) 进行虹膜样本采集；
   3) 对采集的虹膜样本进行质量判断、呈现攻击检测，如果检测通过则提取虹膜特征项数据，否则重新进行虹膜样本采集；
   4) 将提取的虹膜特征项数据与存储的一个或多个虹膜模板进行比对；
   5) 根据比对结果做出判别决策，并传输至移动应用；
   6) 结束虹膜识别过程，记录虹膜识别日志。
c) 虹膜注销过程，包括但不限于如下步骤：
   1) 启动虹膜注销过程；
   2) 删除与待注销用户关联的全部虹膜特征数据以及待注销用户的身份标识；
   3) 结束虹膜注销过程，记录虹膜注销日志。

7 功能要求

7.1 一般要求

7.1.1 基本功能

移动设备虹膜识别应符合 GB/T 37036.1—2018 中 6.1.1 的基本功能要求，包括但不限于：

a) 应适用不同人种、不同年龄的用户；
b) 应支持佩戴无色镜片或无色隐形眼镜的虹膜识别；
c) 应适用移动设备用户和虹膜识别系统管理员；
d) 虹膜识别服务提供方应支持对虹膜比对阈值的设定；
e) 宜支持对登记时间、识别时间和呈现攻击检测阈值等性能指标进行设定。

7.1.2 管理功能

移动设备虹膜识别应符合 GB/T 37036.1—2018 中 6.1.2 的管理功能要求，包括但不限于：

a) 支持新用户登记、已登记用户虹膜模板删除与更新、已登记用户注销等功能；
b) 支持用户登记并存储虹膜模板；
c) 支持用户和虹膜识别系统管理员等不同用户的使用权限，在虹膜特征采集、存储与比对中分别具有相应的权限管理机制；

d) 在远程识别模式中，具有虹膜服务器地址和服务端口设置功能；

e) 具备异常情况处理能力，包括但不限于虹膜样本采集失败、虹膜样本未通过质量判断、呈现攻击检测无响应、虹膜特征项提取失败、虹膜模板登记失败、虹膜模板删除失败、虹膜特征比对失败、识别决策失败、传输失败时的处理机制，如提示用户重新采集或提示失败等。

7.1.3 日志管理功能

移动设备虹膜识别应具备日志管理功能，产生日志记录的事件应包括但不限于：

a) 登记过程中的成功或失败事件；

b) 识别过程中的成功或失败事件；

c) 注销过程中的成功或失败事件；

d) 虹膜模板更新等。

对于每一个事件，日志记录应包括事件发生时间、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 虹膜特征采集

7.2.1 基本功能

虹膜特征采集应符合 GB/T 37036.1—2018 中 6.2.1 的要求，包括但不限于：

a) 支持自然场景中的虹膜样本采集，光源波长应符合 GB/T 35783—2017 中 4.4.1 的要求，也可选用 700 nm～1 000 nm 波长范围的主动光源；

b) 具有适应不同环境光照强度的主动光源光强调节功能；

c) 能使用移动设备虹膜采集模块采集用户虹膜样本，虹膜样本的内容规范应符合 GB/T 26237.6—2014 中第 6 章的要求；

d) 具有明显的用户提示，告知用户对其虹膜样本进行了采集，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；

e) 应从通过质量判断的用户虹膜样本中提取虹膜特征项数据，提取过程宜采用不可逆的方式，提取成功后进行虹膜特征存储或者虹膜特征比对；

f) 宜采取技术手段对采集过程中用户距离远近、双目采集时的偏转角度等进行判断，在不适宜的情况下提示用户配合改进；

g) 远程识别模式中，可采用数据压缩算法处理虹膜特征数据后再传输到虹膜服务器进行处理。

7.2.2 质量判断

虹膜特征采集应具有质量判断功能，应符合 GB/T 37036.1—2018 中 6.2.2 的要求，包括但不限于可用虹膜区域、虹膜-巩膜对比度、虹膜-瞳孔对比度、灰度利用率和虹膜半径等，应分别符合 GB/T 33767.6—2018 中 6.2.1、6.2.2、6.2.3、6.2.5 和 6.2.6 的规定。

7.2.3 呈现攻击检测

虹膜特征采集应具有呈现攻击检测功能，应符合 GB/T 37036.1—2018 中 6.2.3 的要求与 ISO/IEC 30107-3:2017 的相关规定。

应支持二维呈现攻击类型的检测功能，宜支持三维呈现攻击类型的检测功能，见表 1，一些呈现攻击检测实现的示例见附录 B。

宜能提示呈现攻击检测结果。

表 1　虹膜识别呈现攻击类型

呈现攻击类型			样例
二维呈现攻击类型	静态图像	纸质	例如采用普通的复印纸、亚光相纸、高光相纸、绒面相纸等打印的虹膜样本图像
		电子	例如显示设备呈现的虹膜样本图像
	动态图像	录制视频	例如显示设备呈现的录制的虹膜样本视频
		合成视频	例如显示设备呈现的合成的虹膜样本视频
三维呈现攻击类型	美瞳隐形眼镜		例如佩戴带有花纹的美瞳隐形眼镜
	义眼		例如佩戴高分子义眼、玻璃义眼等

7.2.4　虹膜特征项提取

虹膜特征采集应具有虹膜特征项提取功能。

7.2.5　数据交换格式

虹膜特征采集形成的虹膜样本的数据交换格式应符合 GB/T 37036.1—2018 中 6.2.4 的规定，包括但不限于：

a）　对成功采集的虹膜样本数据，在虹膜记录头中应包括事件的标识符、设备标识符、采集日期和时间、虹膜样本的描述等数据；

b）　虹膜数据记录结构应符合 GB/T 26237.6—2014 中 7.3 虹膜图像数据记录结构的规定；

c）　虹膜记录头结构应符合 GB/T 26237.6—2014 中 7.4 虹膜记录头结构的规定。

7.3　虹膜特征存储

虹膜特征存储应符合 GB/T 37036.1—2018 中 6.3 的要求，包括但不限于：

a）　具备虹膜模板存储管理功能，包括但不限于：应只允许具有合法权限的实体录入、访问、读取或删除存储的用户虹膜特征数据；

b）　能将登记的用户虹膜模板与该用户的身份标识进行关联；

c）　支持同一用户登记一个或多个不同光照、不同视角下的虹膜模板；

d）　本地识别模式中，宜能提示已进行虹膜登记的用户数量和最大用户容量；

e）　应具备异常情况判定及处理能力，如虹膜模板存储、读取或删除失败时的相应处理机制。

7.4　虹膜特征比对

虹膜特征比对应符合 GB/T 37036.1—2018 中 6.4 的要求，包括但不限于：

a）　能将输入的用户虹膜特征项和已登记的虹膜模板进行比对，计算出比对得分；

b）　根据比对得分进行识别结果判定，并传输至移动应用；

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。

8　性能要求

8.1　MTF 值

在有效采集距离范围内，分辨力为 2 lp/mm（线对每毫米）时，MTF 值应不小于 50%。

8.2 采集时间

从开始发送虹膜采集指令到虹膜样本数据接收完成的过程，不应超过 200 ms。

8.3 登记时间

虹膜登记过程宜不超过 5 s。

8.4 识别时间

虹膜识别过程应不超过 2 s。

8.5 呈现攻击检测准确率

呈现攻击检测性能指标如表 2 所示。

表 2 呈现攻击检测性能指标

呈现攻击类型	性能指标		
	BPCER/APCER	APNRR	BPNRR
二维呈现攻击类型	当 BPCER 为 3%时，APCER 应低于 3%	计算速率 1 s 的情况下，应低于 5%	计算速率 1 s 的情况下，应低于 3%
三维呈现攻击类型	当 BPCER 为 5%时，APCER 应低于 5%	计算速率 1 s 的情况下，应低于 5%	计算速率 1 s 的情况下，应低于 3%
注：由于部分攻击材料在近红外虹膜采集模块下不成像，因此 APNRR 计算前提是虹膜采集模块切实采集到可检测虹膜的图像。			

8.6 错误接受率和错误拒绝率

应符合在 FAR 为 0.01%时，FRR 低于 1%。

9 安全要求

9.1 人体安全

移动设备虹膜识别的光源安全性应符合 GB/T 20145—2006 中 4.3 辐射危害曝辐限值的规定。

9.2 信息安全

9.2.1 一般要求

移动设备虹膜识别的一般要求除应符合 GB/T 37036.1—2018 中 7.1 的规定外，还应符合如下要求。

a) 具有有效的安全机制，保证用户鉴别授权的安全，应符合如下要求：
   1) 当前操作人员应拥有合法权限完成用户登记、更新和注销；
   2) 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；
   3) 已登记用户虹膜特征数据应与该用户标识之间具有正确关联关系，防止被非法修改。
b) 若虹膜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。

c) 在远程识别模式运行时宜具备运行环境的检查能力，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。

d) 在移动设备支持 TEE 或 SE 等可信环境时，宜结合可信环境增强安全性，包括但不限于：

1) 宜使用 TEE 或 SE 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；

2) 宜通过 TEE 中可信交互界面实现与用户之间的交互；

3) 宜在 TEE 或 SE 中存储所涉及的密钥。

e) 在远程识别模式中，应采取安全措施保护传输数据的安全，包括但不限于：

1) 在移动设备将采集的虹膜样本数据或特征数据传输到虹膜服务器时，应采取有效的安全方式对数据的保密性和完整性进行安全保护；

2) 在虹膜服务器完成识别并返回质量判断、呈现攻击检测、相似度计算、识别决策等结果时，应采取有效的安全方式对数据的保密性和完整性进行安全保护。

f) 应采取安全加固措施增强安全防护水平，包括但不限于：

1) 采取重新编译、加壳保护、修改指令调用顺序等技术手段来增强反破解能力；

2) 在运行时应具备自身代码和文件完整性检查的能力；

3) 对自身代码做防注入处理，防止恶意攻击者对应用进行注入、修改代码逻辑、拦截敏感数据等操作。

g) 具有有效的安全机制，保护数据的机密性和完整性，在进行虹膜识别操作时应满足下列要求：

1) 虹膜特征数据读取的准确性；

2) 虹膜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) 质量判断结果不被窃取或篡改；

6) 呈现攻击检测结果不被窃取或篡改；

7) 比对结束后，即时清除用户虹膜样本数据、虹膜特征数据，以及比对过程中所产生的其他数据如相似度得分等；

8) 被删除的虹膜特征数据不可恢复。

9.2.2 虹膜特征采集

移动设备虹膜特征采集安全要求除应符合 GB/T 37036.1—2018 中 7.2 的规定外，还应符合如下要求：

a) 具备超时处理机制，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虹膜样本时，自动退出运行；

b) 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虹膜数据进行安全保护，确保其保密性和完整性，不被非法窃取或者篡改，例如可结合移动设备中的可信环境实现保护功能；

c) 采用不可逆的计算方式从用户虹膜样本数据中提取出虹膜特征数据，并在特征提取过程结束后对用户的虹膜样本数据进行及时清除并确保不可恢复。

9.2.3 虹膜特征存储

移动设备虹膜特征存储安全要求除应符合 GB/T 37036.1—2018 中 7.3 的规定外，还应符合如下要求：

a) 用户虹膜特征数据仅在身份鉴别通过后可被访问、增加、删除或更新；

b) 在本地识别模式中，应采取有效的安全措施对本地存储的用户虹膜数据进行安全保护，确保其保密性和完整性，不被非法窃取或者篡改，例如可结合移动设备中的可信环境实现保护功能；

c) 远程识别模式中：

1) 宜采用加密的方式存储用户的虹膜模板，并对存储的用户虹膜数据实施访问控制策略；

2) 宜对用户虹膜数据进行匿名化处理，并应与用户身份标识信息采用技术隔离手段存储，如逻辑隔离或物理隔离。

9.2.4 虹膜特征比对

移动设备虹膜特征比对安全要求除应符合 GB/T 37036.1—2018 中 7.4 的规定外，还应符合如下要求：

a) 在本地识别模式中，虹膜特征比对功能一般是以软件的形式实现，应采取有效的安全措施确保其安全性，并采取有效的安全措施确保比对过程中所使用的用户虹膜数据以及识别决策结果的保密性和完整性，如结合移动设备中可信环境实现；

b) 在远程识别模式中：

1) 应在虹膜服务器上采取有效的安全措施对虹膜特征比对功能进行保护，确保比对过程中所使用的用户虹膜数据的保密性和完整性以及识别决策结果的完整性；

2) 宜结合可信环境增强虹膜特征比对功能的安全性，如在可信环境中存储并使用安全通信所涉及的密钥，使用可信交互界面向用户展示识别决策结果等。

9.2.5 日志

应具备授权管理机制，对日志的访问、修改、删除权限进行管理。

应采取安全措施对日志信息做完整性保护，如数字签名等。

日志记录中不应出现明文的虹膜数据、密钥信息或其他安全相关的参数等。

附 录 A
（资料性）
移动设备虹膜识别典型应用架构

A.1 概述

本附录主要是对应用于移动设备上的虹膜识别系统的一些典型技术架构进行描述。在移动设备中，本附录的描述会进一步细分为 REE 和 TEE。

A.2 典型应用架构

A.2.1 本地识别模式

图 A.1 描述了典型模式一。该种模式下，虹膜特征存储和虹膜特征比对功能都位于移动设备中，出于安全性考虑，虹膜识别系统的各种功能应由移动设备中 TEE 进行保护。虹膜采集模块或允许由 REE 和 TEE 共享访问，或仅允许由 TEE 访问。

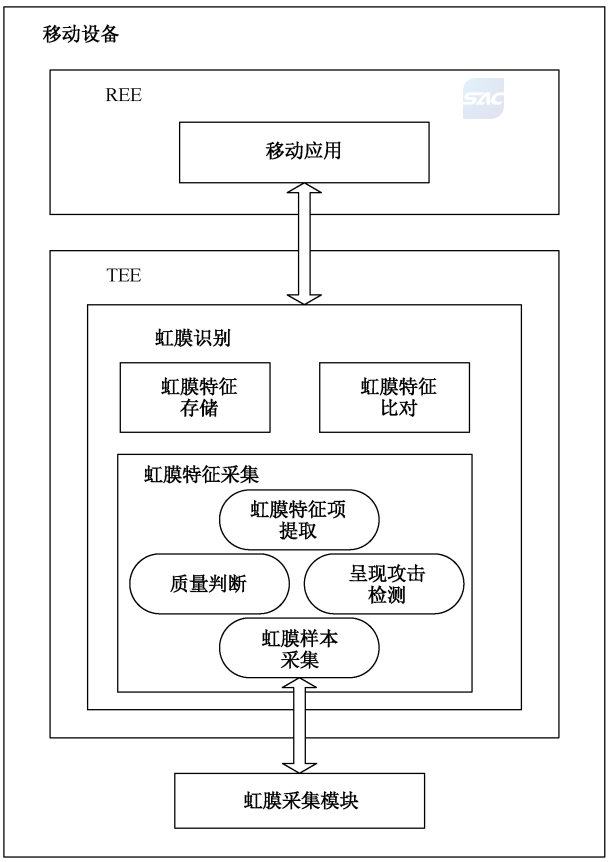


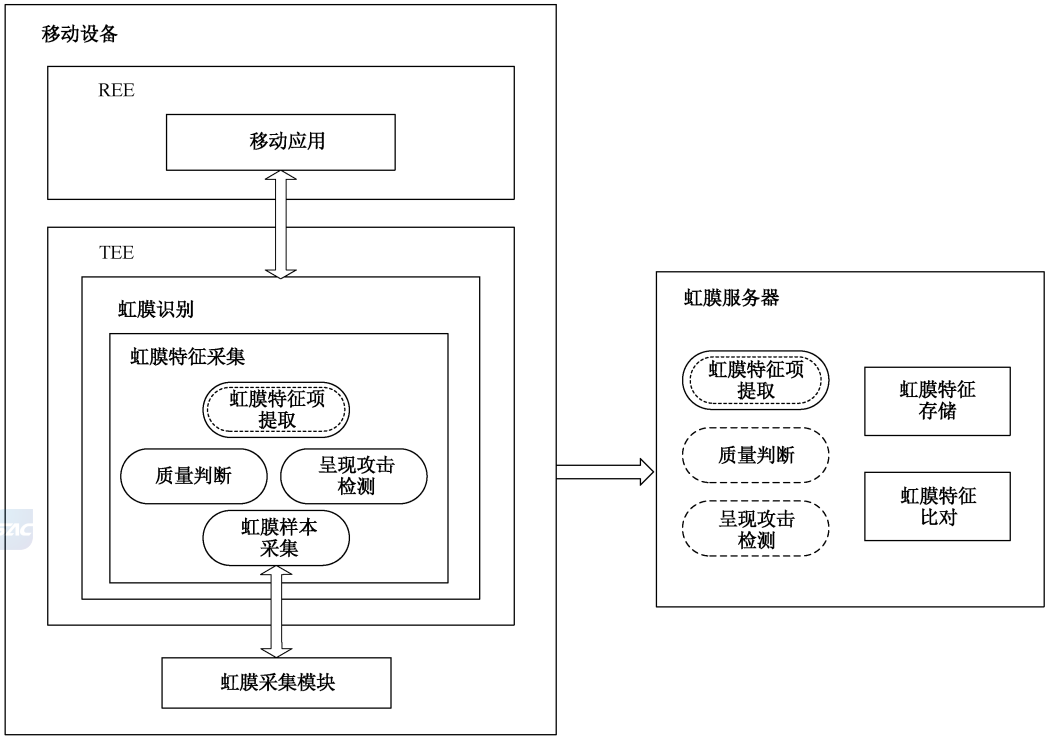
图 A.1 本地识别模式

移动应用一般位于 REE，通过 TEE 提供的对外接口调用虹膜识别系统，虹膜识别系统调用位于移动设备中的虹膜采集模块开展对虹膜样本的采集，在进行质量判断、呈现攻击检测后提取虹膜特征项数据，根据目的不同进行虹膜登记或者识别过程，并将执行结果反馈给移动应用。

A.2.2 结合 TEE 的远程识别模式

图 A.2 描述了典型模式二。这种模式下，虹膜特征采集功能位于移动设备中，虹膜特征存储功能和虹膜特征比对功能在虹膜服务器完成。出于安全性增强考虑，位于移动设备中的虹膜特征采集功能在 TEE 中实现。虹膜采集模块或允许由 REE 和 TEE 共享访问，或仅允许由 TEE 访问。

移动应用一般位于 REE，通过 TEE 提供的对外接口调用虹膜识别系统，虹膜识别系统调用位于移动设备中的虹膜采集模块开展对虹膜样本的采集，在进行质量判断、呈现攻击检测后提取虹膜特征项数据，并访问虹膜服务器进行虹膜登记或识别过程，完成后向调用虹膜识别的移动应用反馈结果。



注：图中线框说明。

——————　应具备的功能；

- - - - - - - - - - - - - -　可选具备的功能；

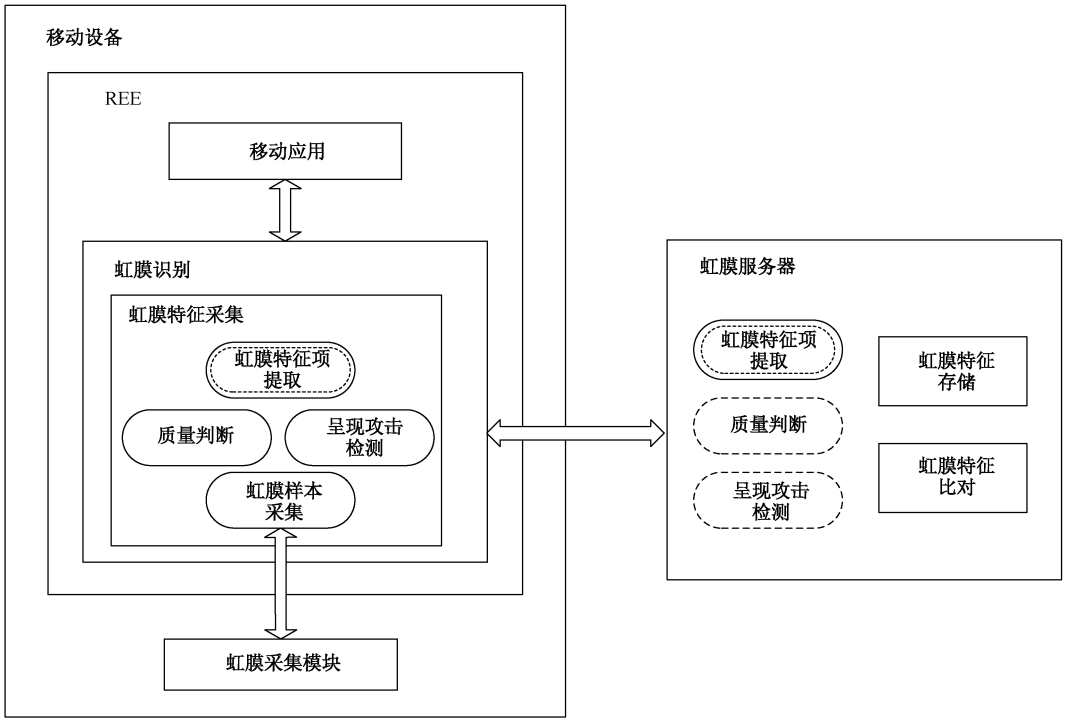
═══════　应具备的功能，根据不同方案，或位于移动设备，或位于虹膜服务器。

图 A.2　结合 TEE 的远程识别模式

A.2.3 未结合 TEE 的远程识别模式

图 A.3 描述了典型模式三。这种模式下，虹膜特征采集功能位于移动设备中，虹膜特征存储功能和虹膜特征比对功能在虹膜服务器完成。位于移动设备中的虹膜特征采集功能在 REE 中实现。虹膜采集模块应允许通过 REE 进行访问。

移动应用一般位于 REE，调用虹膜识别系统后通过位于移动设备中的虹膜采集模块开展对虹膜样本的采集，在进行质量判断、呈现攻击检测后提取虹膜特征项数据，并访问虹膜服务器进行虹膜登记或识别过程，完成后向调用虹膜识别的移动应用反馈结果。



注：图中线框说明。

——————　应具备的功能；

- - - - - - - - - - - - - -　可选具备的功能；

——————
- - - - - - - - - - - - - -　应具备的功能，根据不同方案，或位于移动设备，或位于虹膜服务器。

图 A.3　未结合 TEE 的远程识别模式

附 录 B
（资料性）
移动设备虹膜识别呈现攻击检测实现的示例

移动设备虹膜识别具备的呈现攻击检测功能实现的示例如下：

a） 离散图像检测方法，即利用一幅或多幅图像进行判断，如检测显示器边框、检测纸张及照片边缘、检测屏幕反光、像素点分析、条纹分析、局部纹理分析等；

b） 连续图像检测方法，即采用连续图像序列进行判断，如分析活体特有眼部动作、检测虹膜振颤、异常运动情况分析等；

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进行判断，如眨眼、上下左右转动视线等；

d） 用户被动配合检测方法，即利用瞳孔对不同强度可见光的缩放变化特性进行判断，如增大或减小可见光强度，检查瞳孔是否发生相对应的缩小或放大变化；

e） 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判断依据辅助进行判断，如利用深度摄像头采集眼部区域深度信息；

f） 宜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（如采用与逻辑、或逻辑或置信度加权等方法）后给出呈现攻击检测结果。