

ICS 35. 240. 01

CCS L 67

团 体 标 准

T/ZSPH ***-2023

智能门锁三维人脸识别应用技术要求

Technical requirements for smart door lock

3D face recognition application

2023-**-**发布

2023-**-** 实施

中关村乐家智慧居住区产业技术联盟 发布

目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 系统组成与业务流程	1
5 三维人脸识别技术要求	3
6 门锁产品要求	6
7 分类和分级	8
8 测试要求	9

前 言

本标准按照GB/1.1-2020给出的规则起草。

本标准由中关村乐家智慧居住区产业技术联盟归口。

本标准起草单位：

本标准主要起草人：

智能门锁三维人脸识别应用技术要求

1 范围

本文件规定了智能门锁三维人脸识别应用的分类分级、技术要求。
本文件适用于智能门锁应用中三维人脸识别技术的设计、检验。

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 7247.1-2012 激光产品的安全
GB/T 35273-2020 信息安全技术 个人信息安全规范
GB/T 35678-2017 公共安全 人脸识别应用图像技术要求
GB/T 38427.1-2019 生物特征识别防伪技术要求 第1部分：人脸识别
GB/T 38671-2020 信息安全技术 远程人脸识别系统技术要求
GB/T 41772-2022 信息技术 生物特征识别 人脸识别系统技术要求
GA 374-2019 电子防盗锁

3 术语和定义

3.1

姿态 pose

[GB/T 35678-2017, 定义3.3]

3.2

错误接受率 false acceptance rate; FAR

将来自非同一个人的样本误认为来自同一人的比率。

[GB/T 38427.1-2019, 定义3.4]

3.3

错误拒绝率 false rejection rate; FRR

将来自同一人的样本误认为来自非同一个人的比率。

[GB/T 38427.1-2019, 定义3.5]

4 系统组成与业务流程

4.1 系统架构

智能门锁三维人脸识别应用系统由视图采集子系统、视图解析子系统、存储子系统、比对子系统、决策子系统、管理子系统以及应用开放接口等组成。智能门锁三维人脸识别应用系统架构见图1。

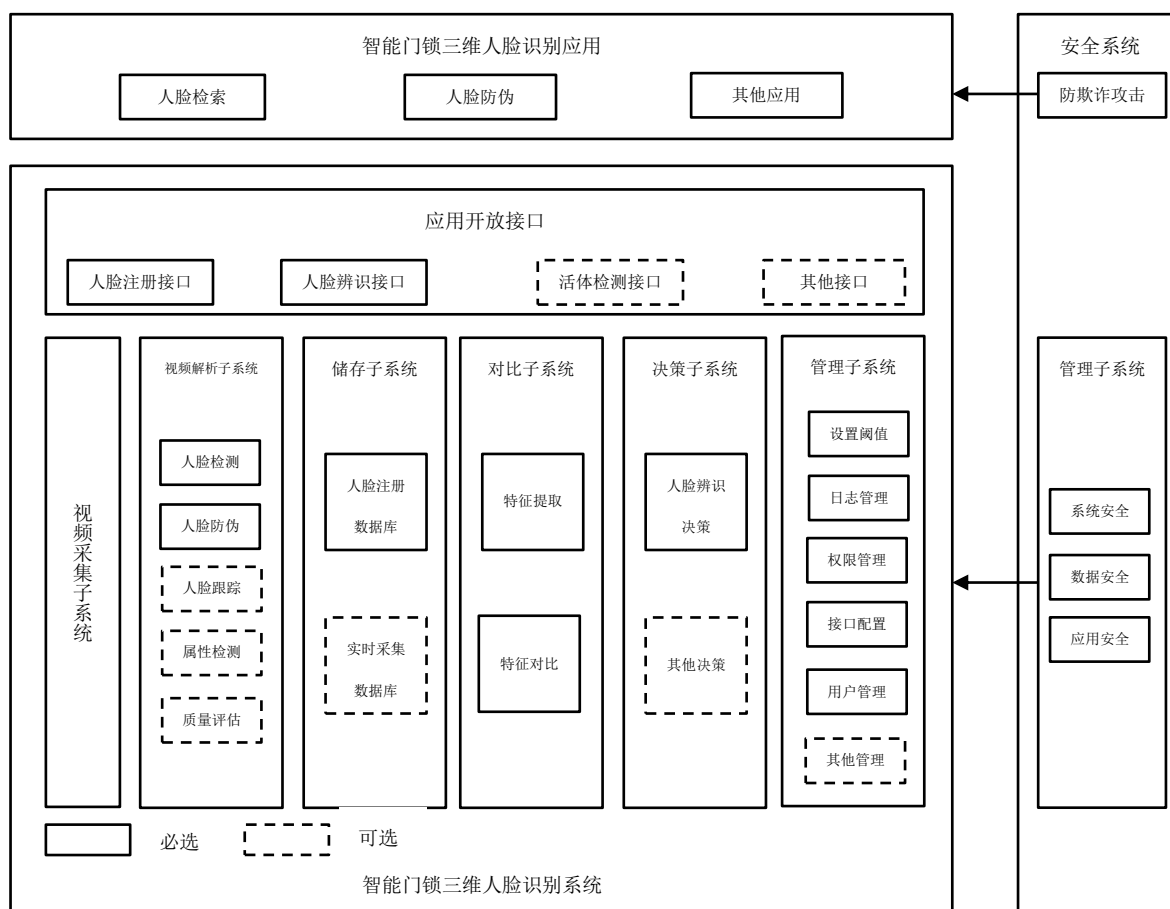


图1 智能门锁三维人脸识别系统架构

智能门锁三维人脸识别应用系统具体组成如下。

- 视图采集子系统：用于人脸图像或视频的采集，包括人脸采集设备以及执行人脸采集过程所需的任何子过程；
- 视图解析子系统：用于人脸图像和/或视频的处理，包括人脸检测、人脸防伪、人脸跟踪、属性检测、质量评估等；
- 存储子系统：用于注册数据及实时采集人脸特征数据的存储，包括：
 - 人脸注册数据库：用于注册人脸特征数据的存储；
 - 实时采集数据库：用于采集人脸特征数据的存储。
- 比对子系统：特征提取模块提取人脸特征，人脸特征同一个或多个人脸参考进行比对，得到相似度得分，并将相似度得分传输到人脸识别决策子系统；
- 决策子系统：根据一个或多个相似度得分，对人脸识别提供决策结果，当相似度得分超过指定的阈值时，对应的人脸参考构成了与人脸参考匹配的潜在候选者；
- 管理子系统：管理人脸识别系统的总体策略、执行和应用，包括但不限于：
 - 设置阈值，例如样本质量阈值，相似度阈值，人脸防伪阈值等；
 - 日志管理：日志生成、查询和导出等；
 - 权限管理：设置不同角色的操作权限等；
 - 接口配置：配置人脸识别系统的视图采集子系统；

- 5) 用户管理：存储或删除用户的人脸参考等注册信息；
- 6) 其它管理：控制工作环境和非生物特征数据的存储、在视图采集时或采集后向用户提供反馈信息、与人脸识别应用进行交互管理等。
- g) 应用开放接口：人脸识别系统和人脸识别应用之间的接口，包括人脸注册接口、人脸辨识接口、活体检测接口等；
- h) 安全系统：用于实现人脸识别相关数据安全、系统安全、应用安全等。

4.2 业务流程

智能门锁三维人脸识别应用系统的业务流程包括人脸注册、人脸识别、人脸更新和人脸注销等。

- a) 人脸注册：
 - 1) 启动人脸注册过程；
 - 2) 根据人脸注册策略，采集用户数据，例如人脸图像、视频和/或非生物特征数据等；
 - 3) 视图解析子系统对采集的视图进行解析，例如质量判断和活体检测等；
 - 4) 将该用户的数据记录存储在人脸注册数据库；
 - 5) 结束注册过程，记录日志。
- b) 人脸识别：
 - 1) 启动人脸识别过程；
 - 2) 采集人脸图像或视频；
 - 3) 视图解析子系统对采集的视图解析，例如质量判断和活体检测等；
 - 4) 比对系统提取视图特征，将人脸特征与一个或多个人脸参考进行比对；
 - 5) 依据系统策略及相似度得分，对人脸识别提供决策结果；
 - 6) 将决策结果传输到人脸识别应用；
 - 7) 结束识别过程，记录日志。
- c) 人脸更新：
 - 1) 启动人脸更新过程；
 - 2) 根据人脸更新策略，使用本次比对通过的人脸参考替换或部分替换之前的人脸参考；
 - 3) 结束更新流程，记录日志。
- d) 人脸注销：
 - 1) 启动人脸注销过程；
 - 2) 根据人脸注销策略，在人脸注册数据库中删除或匿名化与待注销用户关联的全部数据；
 - 3) 结束注销过程，记录日志。

5 三维人脸识别技术要求

5.1 人脸注册

5.1.1 功能要求

应符合如下要求。

- a) 应支持实时人脸注册或者远程人脸注册方式，应具备人脸注册引导和结果提示功能；
- b) 应支持注册库规模大于等于20个ID，宜大于等于50个ID；
- c) 宜支持同一ID多次注册。

5.1.2 光照

注册要求应符合表1的规定。

表 1 注册要求

分类	环境要求
I 类	在光照强度 0~40000 Lux 下，应能注册
II 类	在光照强度 0~100000 Lux 下，应能注册

5.1.3 身高范围

应支持的身高范围为1.35m~1.9m，宜支持1.3m~2.0m。

5.1.4 表情

应支持非夸张表情的人脸注册。

5.1.5 姿态

应支持人脸水平转动角(Yaw)在 $\pm 10^\circ$ 以内，俯仰角(Pitch)在 $\pm 10^\circ$ 以内，倾斜角(Roll)在 $\pm 10^\circ$ 以内。

5.1.6 年龄

应支持成年人和未成年人。

5.1.7 遮挡

宜在人脸无遮挡情况下注册。

5.1.8 注册成功率

在图像质量满足要求的情况下，人脸注册一次成功率 $\geq 99\%$ 。

5.2 人脸识别

5.2.1 光照

识别要求应符合表2的规定。

表 2 识别要求

分类	环境要求
I 类	在光照强度 0~40000 Lux 下，应能识别

II 类	在光照强度 0~100000 Lux 下，应能识别
------	---------------------------

5.2.2 身高范围

应支持的身高范围为1.35m~1.9m，宜支持1.3m~2.0m。

5.2.3 表情

应支持人脸表情微小变化。

5.2.4 姿态

应支持人脸水平转动角(Yaw)在 $\pm 30^\circ$ 以内，倾斜角(Roll)在 $\pm 30^\circ$ 以内，俯仰角(Pitch)在 $\pm 20^\circ$ 以内。

5.2.5 年龄

应支持成年人和未成年人。

5.2.6 遮挡

应支持在不遮挡眼睛、鼻子、嘴巴、眉毛下的人脸识别。

5.2.7 识别距离

应支持识别距离0.4m~0.8m(水平距离)，宜支持0.3m~1m。

5.2.8 时间性能

支持系统触发至验证完成时间 $\leq 2s$ ，宜在1.5s以内。

5.2.9 错误拒绝率与错误接受率

错误拒绝率与错误接受率应满足表3的规定。

表 3 FRR、FAR 要求

等级	条目	指标
A 级	错误拒绝率与错误接受率	$FRR \leq 10\%$ @ $FAR \leq 1e-5$;
B 级	错误拒绝率与错误接受率	$FRR \leq 8\%$ @ $FAR \leq 5e-6$;
C 级	错误拒绝率与错误接受率	$FRR \leq 5\%$ @ $FAR \leq 1e-6$;

5.3 防欺骗攻击

应具备防欺骗攻击能力，至少可防范以下欺骗攻击行为：

二维假体：

- a) 照片：打印的普通人脸照片、纸质高清人脸照片、手机或平板或电脑屏幕重放的人脸照片；
- b) 视频：手机或平板或电脑录制或合成的人脸视频。

三维假体

a) 面具：纸质面具、树脂面具、硅胶面具、乳胶面具、硬泡沫面具、石英砂面具、尼龙面具、塑料面具、铸铜面具、石膏面具、彩色树脂面具、代木面具、陶瓷面具；

b) 头模：泡沫头模、树脂头模、硅胶头模、乳胶头模、硬泡沫头模、石英砂头模、尼龙头模、石膏头模、代木头模、陶瓷头模。

6 门锁产品要求

6.1 门锁产品安全

6.1.1 系统安全

a) 安全启动：智能门锁人脸识别业务在开机和唤醒时设备应提供安全启动校验认证机制，对系统、程序、数据进行完整性校验，保证人脸识别算法和应用相关程序、数据及运行环境等的安全；（A）

b) 固件防逆向保护：应对固件代码采用签名验证，且固件代码应具有反逆向保护；（C）

c) 安全升级：更新固件代码应采用代码签名机制验证代码的完整性和可靠性，且应具有防回滚功能；（A）

d) 人脸面部信息的识别比对应运行在安全环境中（可保证其内部数据的保密性、完整性、可用性等安全性的区域），保证人脸识别运行过程的安全；（C）

e) 人脸面部识别结果信息应通过安全通道（支持防重放攻击、防信息泄露）传输，避免人脸面部识别结果信息在传输过程中泄露。（B）

6.1.2 数据安全

6.1.2.1 人脸数据安全

人脸面部识别信息（面部图像、面部识别特征、面部识别特征的摘要等）属于个人敏感信息，在收集、存储、使用时需进行隐私与安全保护。

a) 收集

智能门锁在使用人脸识别功能时，应将人脸面部识别信息按个人敏感信息处理，应符合GB/T 35273—2020中第5章的要求。（A）

b) 存储

智能门锁如需存储人脸面部识别信息：

- 1) 应将人脸面部识别信息按个人敏感信息处理，符合GB/T 35273—2020中第6章的要求；（A）
- 2) 宜存储在智能门锁设备本体上，若存储在智能门锁设备之外，应告知用户并提供安全传输措施确保数据安全；（A）
- 3) 应存储在安全区域（可保证其内部数据的保密性、完整性、可用性等安全性的区域）；（C）
- 4) 在删除、恢复出厂等情况下，应彻底删除所存储的对应的人脸面部识别信息。（A）

c) 使用

- 1) 智能门锁在使用人脸面部识别信息时，应符合GB/T 35273—2020中第7章的要求；（A）
- 2) 应防止通过入侵设备、安装附加物、替代或修改人脸数据采集模块和相关软硬件的方式以获取或修改人脸数据。（B）

6.1.2.2 人脸数据加密密钥安全

人脸面部识别信息管理密钥应符合以下要求：

a) 加密存储密钥

- 1) 加密密钥不能明文存储，要加密保护；（A）
- 2) 加密密钥应具有唯一性（即每个设备之间不同）；（B）
- 3) 加密密钥应存储在安全区域（可保证其内部数据的保密性、完整性、可用性等安全性的区域）。（C）

b) 加密传输密钥

如果智能门锁与其他设备之间涉及加密传输人脸面部识别信息：

- 1) 如果加密传输所用密钥基于MK/SK密钥体系产生，应由服务器的加密机产生，从服务器下载；在传输过程中，由设备主密钥加密传输；（A）
- 2) 如果加密传输所用密钥通过非对称密钥体系协商产生，应对智能门锁接受到的公钥或证书进行身份验证，防止中间人攻击；（A）
- 3) 不应输出私钥或对称密钥，不应用已经泄密的密钥去加密其他密钥或人脸数据，不应把密钥明文从高安全的组件传送到低安全的组件；（A）
- 4) 加密传输所用密钥不应保存，应每次动态协商产生；（B）
- 5) 加密传输所用密钥应具有更新机制。（C）

c) 密钥与加密算法

- 1) 禁止使用私有加密算法；（A）
- 2) 禁止使用业界已知不安全的加密算法（如DES/3DES（除密钥 $K_1 \neq K_2 \neq K_3$ 外的场景）/SKIPJACK/RC2/RSA（1024位及以下）/MD2/MD4）。（A）

6.1.2.3 关键信息安全

对远程、近端等传送给智能门锁系统的关键信息（如控制信息、配置信息等）应进行身份验证并安全传输。（A）

6.1.3 应用安全

a) 防暴力破解

未授权人脸解锁时，应符合GA374—2019中5.3.3章节的要求。（A）

b) 多机制鉴别

智能门锁应能够提供人脸识别和其它开锁方式相组合的方式来鉴别用户身份，应符合GB/T 38671—2020中6.2.6.5章节的要求。（A）

6.2 OTA 升级

宜支持OTA升级，OTA升级成功率 $\geq 99.9\%$ 。在升级失败时应回退到上一版本且不影响性能。

6.3 环境适应性

整机应符合 GA374-2019 中 5.14 章节的要求。

6.4 电磁兼容

整机应符合 GA374-2019 的 5.15 章节的要求。

7 分类和分级

7.1 三维人脸识别技术分类与分级

7.1.1 三维人脸识别技术分类

通过三维人脸识别技术对环境的适应性，将三维人脸识别技术分为I、II类，如表4所示。

表 4 三维人脸识别技术分类表

分类	环境要求
I 类	在光照强度 0~40000 Lux 下，应能注册与识别
II 类	在光照强度 0~100000 Lux 下，应能注册与识别

7.1.2 三维人脸识别技术分级

根据FAR\FRR、防欺骗攻击能力要求，将三维人脸识别技术分为A、B、C三级，如表5所示。

表 5 三维人脸识别技术分级表

等级	条目	指标
A 级	错误拒绝率与错误接受率	$FRR \leq 10\%$ @ $FAR \leq 1e-5$;
	防欺骗攻击能力	真人正确接受率 > 99%，二维假体错误接受率 < 0.1%，三维假体错误接受率 < 5%;
B 级	错误拒绝率与错误接受率	$FRR \leq 8\%$ @ $FAR \leq 5e-6$;
	防欺骗攻击能力	真人正确接受率 > 99%，二维假体错误接受率 < 0.05%，三维假体错误接受率 < 3%;
C 级	错误拒绝率与错误接受率	$FRR \leq 5\%$ @ $FAR \leq 1e-6$;
	防欺骗攻击能力	真人正确接受率 > 99%，二维假体错误接受率 < $5e-5$ ，三维假体错误接受率 < 1%;

7.2 门锁产品分类与分级

针对安全性要求，将门锁产品分为A、B、C三级，如表6所示。

表6 三维人脸识别门锁分级表

等级	条目	指标
A 级	系统安全要求	满足 6.1.1.a; 6.1.1.c;
B 级	数据安全要求	满足 6.1.2.1.1; 6.1.2.1.2.a; 6.1.2.1.2.b; 6.1.2.1.2.d; 6.1.2.1.3.a; 6.1.2.2.1.a; 6.1.2.2.2.a; 6.1.2.2.2.b; 6.1.2.2.2.c; 6.1.2.2.3.a; 6.1.2.2.3.b; 6.1.2.3;
	应用安全要求	满足 6.1.3

	系统安全要求	满足 6.1.1.e
	数据安全要求	满足 6.1.2.1.3.b; 6.1.2.2.1.b; 6.1.2.2.2.d;
C 级	系统安全要求	满足 6.1.1.b; 6.1.1.d;
	数据安全要求	满足 6.1.2.1.2.c; 6.1.2.2.1.c; 6.1.2.2.2.e;

注：门锁产品A级、B级、C级需满足7.1.2节对应级别的要求。

8 测试要求

8.1 人脸注册

检测目的：被测设备的人脸注册成功率。

测试条件：

- a) 厂商提供样品及使用文档。
- b) 环境条件：测试环境为正常温湿度，环境光线要求如下：
 - 1) 暗光环境：光照强度0~10lux。
 - 2) 正常光环境：
 - 采用D50标准光源，均匀光照，环境光照度10~3000Lux；
 - 采用D75冷色光源，均匀光照，环境光照度10~3000lux；
 - 采用TL83暖色光源，均匀光照，环境光照度10~3000lux。
 - 3) 强光环境：包括侧光和逆光。
 - 对于I类和II类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在3000~40000lux；
 - 对于II类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在40000~100000lux；
 - 在侧光条件下，摄像机、测试对象和光源位置成90度角，在逆光条件下，摄像机、测试对象和光源位置在一条直线上。
- c) 安装条件：由厂商提供设备正常安装条件。
- d) 样本选取条件：人脸测试对象不少于10人，男女比例1:1，年龄小于16占10%，16~60占80%，60以上10%。

测试过程：

- a) 每个测试人员通过模拟手段，从1.35~1.9m逐步增高共模拟10组身高。在不同身高下，执行5次以上人脸注册操作，记录注册成功次数。测试过程中人脸朝向摄像机，保持人脸水平转动角(Yaw)在±10°以内，俯仰角(Pitch)在±10°以内，倾斜角(Roll)在±10°以内，且人脸无遮挡和夸张表情；
- b) 每个测试人员在无眼镜和戴普通眼镜的情况下分别执行25次以上人脸注册操作，记录注册成功次数。测试过程中人脸朝向摄像机，保持人脸水平转动角(Yaw)在±10°以内，俯仰角(Pitch)在±10°以内，倾斜角(Roll)在±10°以内，且人脸无遮挡和夸张表情；
- c) 每个测试人员在不同环境条件下，分别执行1次测试步骤1和测试步骤2。

通过标准：

- a) 人脸注册成功率计算：人脸注册测试中，成功注册的次数占总注册次数的比例，按照式(1)计算。

[illegible]

式中:

S ——人脸注册成功率;

R_1 ——人脸注册成功的次数;

R ——人臉注册次数。

- b) 注册成功率满足5.1.8节要求。

8.2 人脸识别

8.2.1 错误接受率 FAR 测试

检测目的：被测设备的错误接受率。

测试条件:

- a) 厂商提供样品及使用文档;
- b) 厂商额外提供数据采集接口;
- c) 厂商额外提供1:1比对接口, 接口输入两组人脸特征, 输出是否为同一人的结果;
- d) 厂商提供100万组以上人脸特征。
- e) 环境条件: 测试环境为正常温湿度, 环境光线要求如下:
 - 1) 暗光环境: 光照强度0~10lux。
 - 2) 正常光环境:
 - 采用D50标准光源, 均匀光照, 环境光照度10~3000Lux;
 - 采用D75冷色光源, 均匀光照, 环境光照度10~3000lux;
 - 采用TL83暖色光源, 均匀光照, 环境光照度10~3000lux。
 - 3) 强光环境: 包括侧光和逆光。
 - 对于I类和II类算法, 采用全光谱普通照度计测量, 调整光源与测试对象的距离, 使测试对象所在区域光强在3000~40000lux;
 - 对于II类算法, 采用全光谱普通照度计测量, 调整光源与测试对象的距离, 使测试对象所在区域光强在40000~100000lux;
 - 在侧光条件下, 摄像机、测试对象和光源 位置成90度角, 在逆光条件下, 摄像机、测试对象和光源位置在一条直线上。
- e) 安装条件: 由厂商提供设备正常安装条件。
- f) 样本选取条件: 人脸测试对象不少于10人, 男女比例1:1, 年龄小于16占10%, 16~60占80%, 60以上10%。

测试过程:

- 验证厂商提供的人脸特征是否为伪造。
- 测试机构按照如下步骤采集人脸数据：

- 采用 D75 冷色光源，均匀光照，环境光照度 10~3000lux；
- 采用 TL83 暖色光源，均匀光照，环境光照度 10~3000lux；
- 3) 强光环境：包括侧光和逆光。
 - 对于 I 类和 II 类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在 3000~40000lux；
 - 对于 II 类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在 40000~100000lux；
 - 在侧光条件下，摄像机、测试对象和光源 位置成 90 度角，在逆光条件下，摄像机、测试对象和光源位置在一条直线上。
- d) 安装条件：由厂商提供门锁正常安装条件。
- e) 样本选取条件：人脸测试对象不少于10人，男女比例1:1，年龄小于16占10%， 16~60占80%，60以上10%。

测试过程：

- 1) 每个测试人员将人脸注册至人脸数据库；
- 2) 每个测试人员人脸朝向摄像机，保持人脸水平转动角(Yaw)在 $\pm 30^\circ$ 以内，俯仰角(Pitch)在 $\pm 20^\circ$ 以内，倾斜角(Roll)在 $\pm 30^\circ$ 以内，且人脸无遮挡和夸张表情。此时发送开始识别指令，开始计时，等到返回识别结果时，终止计时，并统计耗时；
- 3) 每个测试人员测试10次以上，最终统计平均耗时。

通过标准：人脸识别时间性能满足5.2.8节要求。

8.3 防欺骗攻击

检测目的：

定义一套科学、明确的测试方法来检验智能门锁三维人脸识别技术中的防攻击能力，并且形成规范来指导和约束测试人员执行。人脸防假体攻击测试的光照环境分室内和半室外两种场景，测试样本包括真人、人脸完整照片、人脸抠洞照片、人脸去背景照片、人脸电子照片、人脸视频、仿真人脸面具和仿真人脸头模。

测试条件：

- a) 环境条件：测试环境为正常温湿度，环境光线要求如下：
 - 1) 暗光环境：光照强度0~10lux。
 - 2) 正常光环境：
 - 采用 D50 标准光源，均匀光照，环境光照度 10~3000Lux；
 - 采用 D75 冷色光源，均匀光照，环境光照度 10~3000lux；
 - 采用 TL83 暖色光源，均匀光照，环境光照度 10~3000lux。
 - 3) 强光环境：包括侧光和逆光。
 - 对于 I 类和 II 类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在 3000~40000lux；
 - 对于 II 类算法，采用全光谱普通照度计测量，调整光源与测试对象的距离，使测试对象所在区域光强在 40000~100000lux；
 - 在侧光条件下，摄像机、测试对象和光源 位置成 90 度角，在逆光条件下，摄像机、测试对象和光源位置在一条直线上。

- b) 安装条件:设备正常安装条件由厂家推荐。
- c) 活体人脸测试样本选取
- 1) 活体人脸测试对象不少于 10 人, 男女比例 1:1, 年龄小于 16 占 10%, 16~60 占 80%, 60 以上 10%;
 - 2) 根据眼镜佩戴情况分为无眼镜、佩戴普通眼镜、佩戴黑框眼镜三种场景;
 - 3) 测试距离要求 40cm 和 80cm;
 - 4) 根据人脸角度情况分正脸; yaw 角和 roll 角各 $\pm 10^\circ$ 、 $\pm 20^\circ$ 、 $\pm 30^\circ$; pitch 角各 $\pm 10^\circ$ 、 $\pm 20^\circ$;
 - 5) 根据饰品情况, 分为帽子、围巾、头饰、假发;
 - 6) 测试样本中, 限定表情为中性和微笑表情。
- d) 假体人脸测试样本选取

测试样本类别和样本选取数量要求应符合表 7 的规定。假体人脸身份信息无需与活体人脸一一对应。

表 7 假体人脸测试样本选取

假体人脸样本类型	说明
人脸完整照片	取自不同对象的人脸完整照片, 测试对象戴眼镜和不戴眼镜比例 1: 1, 男女比例 1:1, 年龄小于 16 岁占 10%, 16~60 岁占 80%, 60 岁以上 10%。
人脸抠洞照片	取自不同对象的人脸完整照片, 测试对象戴眼镜和不戴眼镜比例 1: 1, 男女比例 1:1, 年龄小于 16 岁占 10%, 16~60 岁占 80%, 60 岁以上 10%, 并对相关区域进行剪除处理。
人脸去背景照片	取自不同对象的人脸完整照片, 测试对象戴眼镜和不戴眼镜比例 1: 1, 男女比例 1:1, 年龄小于 16 岁占 10%, 16~60 岁占 80%, 60 岁以上 10%。打印在纸上, 并将背景区域剪除。
人脸电子照片	取自不同对象的人脸完整照片, 测试对象戴眼镜和不戴眼镜比例 1: 1, 男女比例 1:1, 年龄小于 16 岁占 10%, 16~60 岁占 80%, 60 岁以上 10%。全屏显示在电子屏幕上。
人脸视频	取自不同对象的人脸视频, 男女比例 1: 1, 年龄小于 16 岁占 10%, 16~60 岁占 80%, 60 岁以上 10%。全屏显示在电子屏幕上。
仿真人脸面具	制作取自不同对象的仿真面具, 每个对象包括睁眼和不睁眼, 两种面具, 材料包括纸质面具、树脂面具、硅胶面具、乳胶面具、硬泡沫面具、石英砂面具、尼龙面具、塑料面具、铸铜面具、石膏面具、彩色树脂面具、代木面具、陶瓷面具等。
仿真人脸头模	制作不同对象的仿真头模, 材料包括泡沫头模、树脂头模、硅胶头模、乳胶头模、硬泡沫头模、石英砂头模、尼龙头模、石膏头模、代木头模、陶瓷头模等。

测试过程:

- a) 人脸活体检测测试
- 1) 安装固定好摄像机, 分别依次设置相应环境, 测试对象面对摄像机;
 - 2) 按顺序从活体测试样本中选择组合方式进行测试;
 - 3) 判定标准: 若出现判断为活体, 则判定成功, 否则判定失败。记录返回结果时间。
- b) 人脸防假体攻击测试
- 1) 人脸完整照片

- 测试前，打印好对应的照片；
- 分别测试 40cm、80cm 两个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

2) 人脸抠洞照片

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 测试前，打印好对应的照片；
- 测试过程中，由测试人员将抠洞的照片戴到脸上露出眼睛、鼻子、嘴巴等部位；
- 分别测试 40cm、80cm 两个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

3) 人脸去背景照片

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 测试前，打印好对应的照片；
- 分别测试 40cm、80cm 两个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

4) 人脸电子照片

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 电子设备分辨率不低于 1920×1080 像素、刷新频率不低于 60Hz；
- 测试 40cm 一个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

5) 人脸视频

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 电子设备分辨率不低于 1920×1080 像素、刷新频率不低于 60Hz；
- 测试 40cm 一个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

6) 仿真人脸面具

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 测试人员佩戴仿真面具，确保能够贴合，无异常；
- 根据眼镜佩戴情况分为无眼镜、佩戴普通眼镜、佩戴黑框眼镜三种场景；
- 测试距离要求 40cm 和 80cm 两个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

7) 仿真人脸头模

- 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 根据眼镜佩戴情况分为无眼镜、佩戴普通眼镜、佩戴黑框眼镜三种场景；
- 测试距离要求 40cm 和 80cm 两个距离，各种角度进行攻击。

判定标准：若出现判断活体，则判定防攻击失败， 否则判定成功，并记录返回结果时间。

c) 人脸防假体系统攻击测试

- 1) 安装固定好摄像机，分别依次设置相应环境，测试对象面对摄像机；
- 2) 在测试假体样本，挑选出根据真人 1: 1 定制的假体样本，或者打印的图片、拍摄的视频等；
- 3) 按照注册要求，注册有对应假体样本的真人；
- 4) 根据不同的假体样本类型、不同的攻击方式进行攻击。

M_1 — 防假体样本攻击失败次数；

M — 防假体样本攻击测试次数。

(5) 测试通过标准

通过 7.1.2 节定义的指标

8.4 安全性测试要求

8.4.1 人脸识别启动安全

检测目的：检测人脸识别业务在启动时是否进行了安全校验。

测试条件：厂商提供设计文档、被测设备、固件烧录工具，未签名的固件镜像。

测试过程：

- a) 查看厂商提供的相关资料，对设计原理和实现方案进行评估。
- b) 使用烧录工具，将未签名的固件镜像加载到设备中。

通过标准：

- a) 设备启动过程中，对系统、程序、数据有完整性校验机制。
- b) 未签名的固件无法写入到设备中，或者写入后人脸识别功能不可用。

8.4.2 人脸识别关键固件防逆向

检测目的：检测人脸识别算法（至少包含人脸比对、活体检测）等关键固件代码镜像是否具备防逆向机制。

评测条件：厂商提供防逆向攻击方案以及代码、被测设备固件包。

评测步骤：使用逆向分析工具，检查人脸识别算法等关键固件代码镜像是否能够解析出来。

通过标准：人脸识别算法等关键固件代码镜像无法解析。

8.4.3 安全升级

检测目的：检测被测设备在更新固件时是否验证了新固件的完整性和真实性，是否具有防回滚机制。

评测条件：被测设备新版本（可更新）、旧版本（不可更新）。

评测步骤：

- a) 在升级服务器上添加旧版本，验证能否升级成功。
- b) 篡改新版本的固件包（篡改签名或签名内容），然后添加到升级服务器上，验证能否升级成功。

通过标准：

- a) 设备拒绝更新到旧版本上。
- b) 新版本被篡改后，设备拒绝更新。
- c) 固件更新失败时，设备可以恢复正常工作，人脸识别功能仍可正常使用。

8.4.4 人脸识别运行环境安全

检测目的：检测人脸识别时运行环境是否安全。

评测条件：厂家已提供被测产品相关安全设计资料或所用的芯片资料。

评测步骤：查看资料，检查人脸识别比对的软硬件运行环境。

通过标准：人脸识别比对程序运行可保证其内部数据保密、完整、可用的安全区域内，如 SE、TEE、TrustZone、物理上独立的人脸识别程序专用运行空间等。

8.4.5 人脸数据收集安全

检测目的：检测收集人脸面部识别信息时是否有隐私保护机制。

评测条件：参考用户手册等资料，将被测设备恢复出厂，使其处于出厂状态（未绑定手机App、未录入人脸等）。

评测步骤：

- a) 参考用户手册等资料对设备进行开机、绑定、配网，录入人脸，开启人脸识别开锁功能。
- b) 查看被测设备是否会告知用户将收集用户的人脸信息。
- c) 查看被测设备是否会告知收集人脸信息的目的、存储位置。
- d) 对于收集人脸信息，查看被测设备是否会征询用户的明示同意。

通过标准：

- a) 被测设备会告知用户将收集人脸信息。
- b) 被测设备会告知用户收集人脸信息的目的、存储位置。
- c) 被测设备会明确询问用户是否同意；当选择不同意时，设备不会启用人脸识别开锁功能。

8.4.6 人脸数据存储安全

a) 人脸面部识别信息存储

检测目的：检测人脸面部识别信息的存储是否安全。

评测条件：厂家已提供被测产品相关安全设计资料。

评测步骤：查看资料，检查人脸面部识别信息的存储区域。

通过标准：人脸面部识别信息存储在了可保证其内部数据保密、完整、可用的安全区域内，如 SE、TEE、TrustZone、物理上独立的个人敏感信息专用存储空间等。

b) 人脸面部识别信息清除

检测目的：检测人脸面部识别信息清除时是否彻底。

评测条件：被测设备上已录入测试人员的人脸。

评测步骤：

- 1) 参考用户手册等资料，将被测设备上已录入的测试人员人脸信息删除。
- 2) 通过手机App等查看被测设备上存储的人脸信息。
- 3) 触发被测设备启动人脸识别。
- 4) 参考用户手册等资料，对被测设备执行恢复出厂操作。
- 5) 重新绑定设备。
- 6) 重复步骤2)、3)。

通过标准：

- 1) 第2)步后，被测设备上已不存在被删除的人脸。
- 2) 第3)步后，对于已删除的人脸，被测设备识别不通过。
- 3) 第6)步后，被测设备上不存在未录入过的人脸。
- 4) 第6)步后，对于未录入过的人脸，被测设备识别不通过。

8.4.7 人脸数据使用安全

a) 人脸面部识别信息使用范围

检测目的：检测人脸面部识别信息的应用范围。

评测条件：被测设备上已录入人脸，已启用人脸识别功能。

评测步骤：通过手机 App、被测设备显示屏等界面，查看在人脸识别之外的场景下，是否有使用人脸面部识别信息。

通过标准：人脸面部识别信息仅用在人脸识别功能上（含人脸录入/识别/更新/删除），与收集时所声明的相符。

b) 人脸面部识别信息和识别结果安全传输

检测目的：检测人脸面部识别信息和识别结果传输时是否安全。

评测条件：厂家已提供被测设备相关安全设计资料，Wi-Fi 和 BLE 空口抓包工具。

评测步骤：

- 1) 查看资料，检查人脸面部识别信息及识别结果的物理传输路径和逻辑传输通道。
- 2) 如果人脸面部识别信息或识别结果传出了被测设备本体，使用空口抓包工具抓取人脸识别过程中Wi-Fi或BLE（取决于被测设备通过哪条链路传输）空口链路上的数据包，检查是否对人脸面部识别信息和识别结果进行了加密保护。

通过标准：

- 1) 人脸面部识别信息和识别结果均没有传出智能门锁设备本体。
- 2) 如果人脸面部识别信息或识别结果传出了被测设备本体，空口报文中人脸面部识别信息和识别结果非明文传输，而是采用了加密保护。

c) 人脸面部识别信息入侵保护

检测目的：检测人脸面部识别信息是否具备入侵保护机制。

测试条件：厂商提供样品。

测试过程：1) 使用仪器设备或软件进行攻击测试。2) 计算攻击分值，分值计算方式应符合 JR/T 0120.5 的要求。

通过标准：被测设备应防止通过入侵设备、安装附加物、替代或修改人脸数据采集模块和相关软硬件的方式以获取或修改人脸数据。攻击总分值至少16分，实施攻击分值至少8分。

8.4.8 人脸数据加密密钥与算法安全

检测目的：检测人脸识别面部信息在加密存储、加密传输时所用的密钥和算法是否安全。

评测条件：厂家已提供被测产品相关安全设计资料以及所用芯片资料。

评测步骤：查看资料，检查人脸识别面部信息加密存储密钥、加密传输密钥的生成机制、存储机制、更新机制，以及所选的加密算法。

通过标准：

a) 加密存储所用密钥

- 1) 加密后存储，非明文存储；
- 2) 每个设备不同；
- 3) 存储在可保证其内部数据保密、完整、可用的安全区域内，如SE、TEE、TrustZone、物理上独立的个人敏感信息专用存储空间等。

- b) 加密传输所用密钥：
 - 1) 如果是基于MK/SK密钥体系产生，则由服务器加密机产生，由设备主密钥加密后传输到智能门锁设备上；
 - 2) 如果是通过非对称密钥体系协商产生，则有对智能门锁接受到的公钥或证书进行身份验证；
 - 3) 没有对外输出私钥和对称密钥，没有使用已经泄密的密钥去加密其他密钥和人脸数据，没有把密钥明文从高安全的组件传送到低安全的组件；
 - 4) 每次动态协商产生，没有进行保存；
 - 5) 提供了更新机制。
- c) 加密算法：
 - a. 使用业界公开的加密算法，没有使用私有算法；
 - b. 没有使用业界已知不安全的加密算法（如DES/3DES（除密钥 $K1 \neq K2 \neq K3$ 外的场景）/SKIPJACK/RC2/RSA（1024位及以下）/MD2/MD4）；
 - c. 若支持国密算法，则应符合国家密码管理机构的相关规定；

8.4.9 人脸识别关键操作安全

检测目的：检测人脸识别功能相关的关键操作是否有安全保护。

测试条件：人脸录入、人脸删除所需的被测设备和工具。

测试过程：

- a) 新录入一个人脸。
- b) 删除一个已录入的人脸。

通过标准：

- a) 录入人脸前，有身份校验机制（如安全校验密码等）；校验通过后，才允许录入。
- b) 删除人脸前，有身份校验机制（如安全校验密码等）；校验通过后，才允许删除。

8.4.10 人脸识别防暴力破解

检测目的：检测人脸识别功能是否具备防暴力尝试机制。

评测条件：测试人员的人脸未注册。

评测步骤：

- a) 触发被测设备对测试人员进行人脸识别开锁；
- b) 在5分钟之内，重复步骤1 N次（N=设备制造商规定的防暴力破解允许尝试次数）。

通过标准：

- a) N次人脸识别均失败；
- b) 连续N次识别失败之后，设备应声音或（和）灯光等提示用户人脸识别功能已禁用；
- c) 连续N次识别失败之后，（在设备没有被其他方式所开锁的情况下）人脸识别功能至少禁用90秒。

8.4.11 人脸与其他方式组合鉴别

检测目的：检测是否支持人脸识别开锁方式与其他开锁方式组合开锁。

评测条件：在被测设备已开启多机制鉴别功能，并已录入开锁方式1（人脸）、开锁方式2（其他某种开锁方式）。

评测步骤：触发被测设备启动开锁识别。

通过标准：开锁方式 1、开锁方式 2 均验证通过后，被测设备才会开锁。
