

基于人脸与虹膜的面部多模态识别设备 技术规范

Technical specifications for facial multi-modal recognition device based on face
and iris

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 产品构成	3
6 技术要求	5
7 试验方法	9
附录 A（资料性）人脸与虹膜融合识别应用实践	16
附录 B（规范性）测试数据集要求	24
附录 C（资料性）比对结果记录文件	26
参考文献	28

基于人脸与虹膜的面部多模态识别设备技术规范

1 范围

本文件确立了基于人脸与虹膜的面部多模态识别设备的产品构成，规定了基于人脸与虹膜的面部多模态识别设备的技术要求，描述了试验方法。

本文件适用于基于人脸与虹膜的面部多模态识别设备(以下简称产品)的研制、生产和检验等。

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
- GB/T 20145—2006 灯和灯系统的光生物安全性
- GB/T 33767.6 信息技术 生物特征样本质量 第6部分：虹膜图像数据
- GB/T 35678 公共安全 人脸识别应用 图像技术要求
- GB/T 36460—2018 信息技术 生物特征识别 多模态及其他多生物特征融合

3 术语和定义

GB/T 5271.37—2021和GB/T 36460—2018中界定的以及下列术语和定义适用于本文件。

3.1

多模态 multi-modal

单个生物特征识别系统中，一个模式的三个组成成分中至少有两个是多重的。

注1：多重意味着类型的差异。

注2：三个组成成分指生物特征特性的类型、传感器类型和处理方法。

[来源：GB/T 5271.37—2021，3.2.6]

3.2

面部多模态识别 facial multi-modal recognition

基于个体人脸与虹膜的生物学特性进行身份识别的技术。

3.3

面部样本 facial sample

在面部特征提取之前的人脸与虹膜的生物特征特性的模拟表示或数字表示。

注：在本文件中指人脸样本和虹膜样本或人脸与虹膜融合后样本。

3.4

面部特征 facial feature

从面部样本中提取的用于比对的数值或标记。

注：在本文件中指人脸特征和虹膜特征或人脸与虹膜融合后特征。

3.5

面部特征模板 facial template

可直接与待识别的面部特征进行比对的已存储的面部特征的集合。

注：在本文件中指人脸特征模板和虹膜特征模板或人脸与虹膜融合后特征模板。

3.6

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，以确定面部样本是否来自于有生命体征的人。

3.7

生物特征融合 biometric fusion

多来源（如：传感器、模态、算法、实例或呈现等）的信息的组合。

[来源：GB/T 36460—2018，3.3]

3.8

融合模块 fusion module

具备一种或多种生物特征融合的功能模块。

注：融合模块支持采集融合、样本融合、特征融合、分数融合和决策融合中的至少一种融合方式。

3.9

采集融合 fusion in capturing

人脸与虹膜采集过程中的生物特征融合（如：算法、传感器等）方式。

注：人脸与虹膜的采集融合过程，可通过人脸检测等算法为虹膜采集和处理提供人眼位置，或者，根据人脸姿态调节虹膜传感器拍摄角度等。

3.10

首选识别率 identification rate at rank 1

生物特征辨识中正确识别结果处于首位的比率。

注：首选识别率又称为首位命中率，排名首位的识别结果也称为TOP1。

3.11

注册集 enroll set

已知身份并作为生物特征模板的面部样本（测试对象）集合。

3.12

探针集 probe set

由已知测试样本根据一定规则组成的待识别面部样本集合。

3.13

样本主体 sample subject

生物特征样本所关联的自然人。

1 缩略语

下列缩略语适用于本文件。

FAR: 错误接受率 (False Acceptance Rate)

FRR: 错误拒绝率 (False Rejection Rate)

FTER: 注册失败率 (Failure-To-Enrol Rate)

LDFAR 活体检测错误接受率 (Liveness Detection False Acceptance Rate)

LDFRR 活体检测错误拒绝率 (Liveness Detection False Rejection Rate)

2 产品构成

2.1 概述

按照GB/T 36460—2018的规定，面部多模态识别设备包括采集融合、样本融合、特征融合、分数融合及决策融合等五种融合方式：

——采集融合即通过算法、传感器等软硬件协同，同时采集并输出多种生物特征样本；

——样本融合即每个单一生物特征识别过程输出一组样本，将多组生物特征样本数据融合为一个样本；

——特征融合即每个单一生物特征识别过程输出一组特征，将多组生物特征融合为一个特征集或者特征向量；

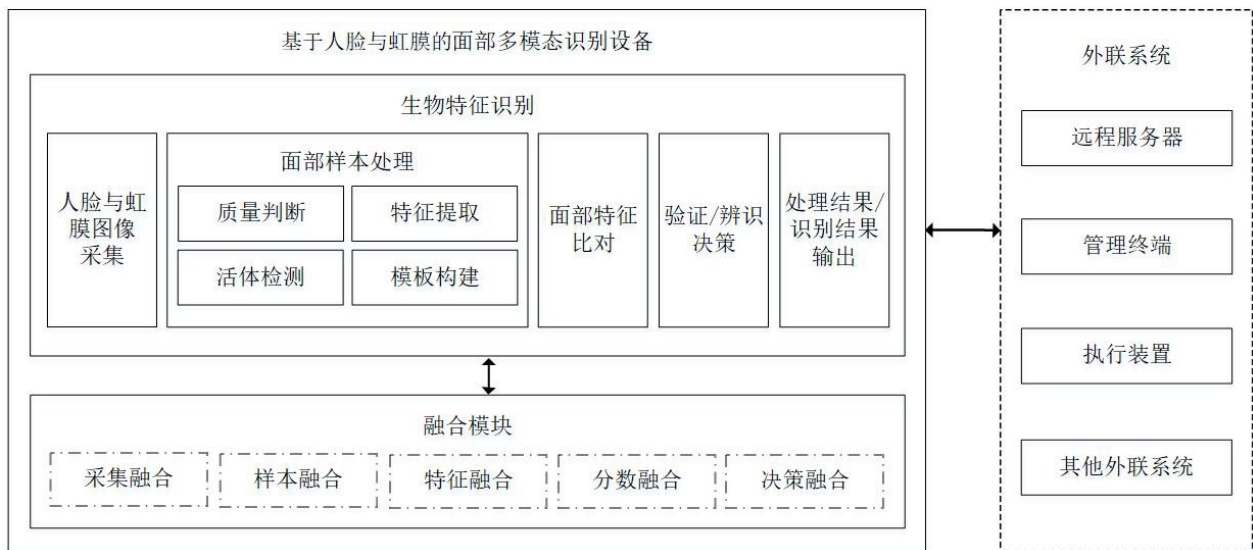
——分数融合即每个单一生物特征识别过程通常输出单一匹配分数，也可能是多个分数。将多个生物特征识别分数融合成一个分数或决策，然后与系统接受阈值进行比较；

——决策融合即每个单一生物特征识别过程输出一个布尔值。利用“或规则”或“与规则”的逻辑运算，或者采用更多参数，如输入样本质量分数将结果进行融合。

注：采集融合是新增融合方式，该方式利用人脸与虹膜的物理相关性同时获取面部样本。

2.2 组成框图

产品由人脸与虹膜的图像采集、样本处理、特征比对、决策及输出等功能模块组成，并通过融合模块实现生物特征融合。外联系统是与产品相关的系统或装置，可用于面部生物特征远程识别、产品管理以及控制门禁、闸机等执行装置。产品组成框图见图1。



线框说明：

—— 必选

----- 可选

- - - - - 任选其一或多项

图1 产品组成框图

产品由以下功能模块组成：

- 人脸与虹膜图像采集：用于人脸图像和虹膜图像的获取并形成面部样本，包括图像获取所需的采集装置或组件等；
- 面部样本处理：对面部样本进行质量判断、活体检测、特征提取及面部特征模板构建等处理，可生成面部特征，或者，构建并存储用户的面部特征模板；
- 面部特征比对：将面部特征与面部特征模板进行比对，计算相似度得分，包括验证（1:1比对）和辨识（1:N比对）两种比对方式；
- 验证/辨识决策：根据相似度得分和决策逻辑给出决策结果，包括验证决策和辨识决策两种，其中，验证决策结果将给出成功匹配者的用户标识，辨识决策结果将给出成功匹配候选者的用户标识（集）；

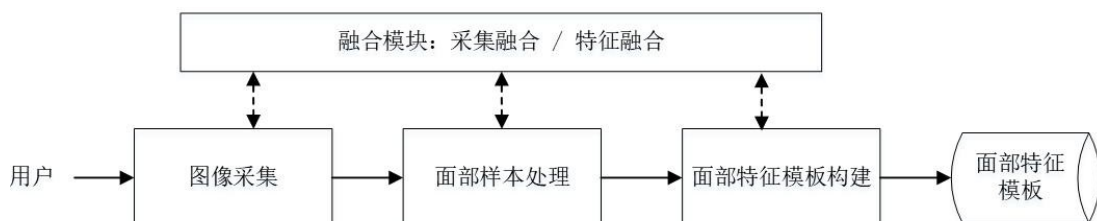
注：决策逻辑与系统设计相关，如“阈值动态调整”、“首位命中”等。

- 融合模块：用于人脸与虹膜识别过程中生物特征融合的实现，至少支持一种融合方式，或者，支持两种及以上融合方式的结合，融合可能发生在采集、处理、比对或决策等阶段；
- 处理结果/识别结果输出：输出所采集的面部样本或面部特征信息，或者，验证/辨识决策结果等。

2.3 功能实现逻辑模型

注册和识别为产品的必备功能，其中，注册分为现场注册和非现场注册两种方式。现场注册的人脸和虹膜样本来自现场图像采集，而非现场注册的人脸和虹膜样本来自图像文件的输入或导入。

产品功能实现逻辑模型见图2。



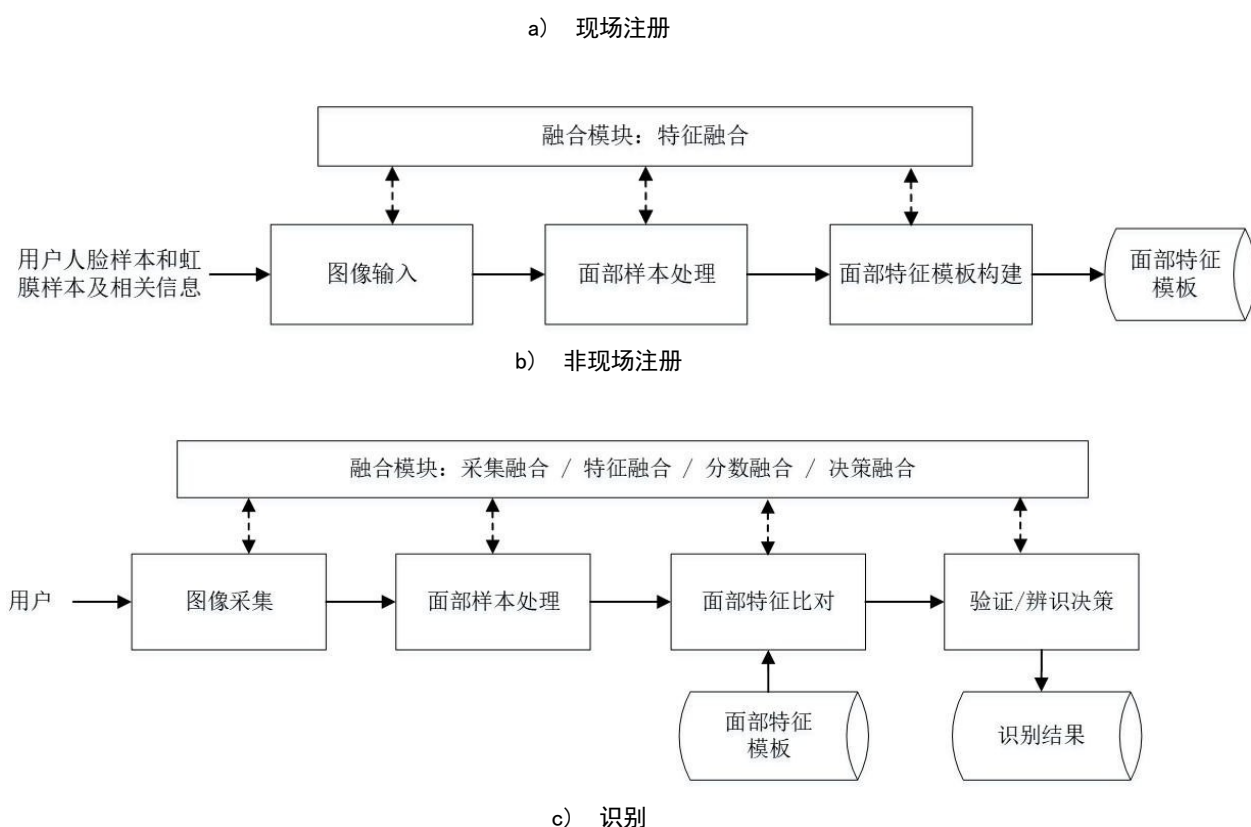


图 2 产品功能实现逻辑模型图

在用户注册和识别过程中，可在图像采集、样本处理、特征比对和决策等阶段进行融合，如：图像采集阶段采用采集融合方式、样本处理阶段采用特征融合方式、特征比对阶段采用分数融合方式、决策阶段采用决策融合方式。相关融合方式的实现参考GB/T 36460—2018的第5章。融合方式的选择取决于产品设计需要，附录A给出了人脸与虹膜融合识别的应用实践。

3 技术要求

3.1 外观和结构

3.1.1 外观

产品外观符合以下要求：

- 结构完整、外观洁净，表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂镀层应均匀、不应起泡、龟裂、脱落和磨损。金属零部件不应有锈蚀及其他机械损伤；
- 在无遮挡位置具有生产者的专用标志以及产品型号，外部接口处应有明确标识，且标志标识不易被擦除。

3.1.2 结构

产品的零部件应紧固无松动，安装可抽换部件的接插件应能可靠连接，键盘、开关按钮和其他控制部件的控制应灵活可靠，布局应方便使用。

3.2 功能

3.2.1 基本功能

3.2.1.1 图像采集

产品具有人脸与虹膜图像的采集和传输功能，包括但不限于：

- a) 应具有自适应补光功能。虹膜采集宜使用波长为700 nm~900 nm的近红外主动光源； b
-) 应能自动感知人体身高和位置，身高适应范围至少在1.3m~1.9m之间；
- c) 应能通过图像采集获取采集区域内的包含人脸和虹膜的面部图像；
- d) 应能处理眼镜反光等因素造成的光斑遮挡虹膜问题，处理方式包括但不限于调整补光角度、变换补光位置等；
- e) 宜能进行口罩佩戴检测，并对佩戴口罩的面部样本进行处理；
- f) 宜采用采集融合方式，具体实现过程可参见附录A.2.1；
- g) 宜支持通过通信接口输出当前采集的面部样本或面部特征等信息。

3.2.1.2 质量判断

应对面部样本进行质量判断并给出判断结果。面部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，并通过语音、图形文字、灯光等方式提示用户进行交互。

3.2.1.3 活体检测

应对面部样本进行活体检测并给出检测结果，包括但不限于：

- a) 应能对二维或三维的假体人脸和假体虹膜攻击进行活体检测；
- b) 应具备防假体攻击的处理机制，如假体提示或终止采集等；
- c) 应利用虹膜隐蔽性强、不易获取、伪造成本高等特性，做为活体检测的首选。

注：对于假体攻击的防范，除了活体检测功能外，有时也需要通过识别功能来做进一步的确认，如：攻击者佩戴祛除眼部区域的人脸面具的情形，就需要“全系统”级的呈现攻击检测。

3.2.2 用户注册

用户注册包括面部样本的采集、处理、模板构建和用户身份绑定等功能，支持以下两种注册方式： a

-) 现场注册：通过现场图像采集获得面部样本，并进行面部样本处理，完成用户注册；
- b) 非现场注册：从外部批量输入/导入面部样本或面部特征模板，在产品内完成用户注册。

用户注册按照产品注册策略进行，满足以下要求：

- a) 应能进行图像采集/输入、质量判断、活体检测等处理，且注册用样本不宜佩戴口罩；
- b) 应能对面部样本进行特征项提取、面部特征模板构建，并形成模板标识符；
- c) 应为用户分配唯一身份标识，并将模板标识符与用户身份标识进行关联；
- d) 应能给出注册成功的提示，未注册成功时应有相应的处理机制，如提示重新注册。

示例：

采用分数融合或决策融合方式时，分别提取人脸特征和虹膜特征，注册为人脸特征模板和虹膜特征模板。

3.2.3 用户识别

用户识别包括面部样本采集、处理、比对及决策输出等功能，满足以下要求： a

-) 应支持验证和辨识中的至少一种比对方式：
 - 验证方式：通过 1:1 比对来确认用户的真实身份是否与其声称的身份一致；
 - 辨识方式：通过 1:N 比对来辨认已注册用户身份，并能拒绝未注册用户。
- b) 应能进行图像采集、质量判断、活体检测等处理，其中，对假体攻击的防范，除活体检测功能外，还应结合面部特征比对来完成进一步的确认；

- c) 应能对面部样本进行特征项提取，并将提取的面部特征与面部特征模板进行比对，计算相似度得分；
- d) 在验证方式下，若比对相似度得分大于指定阈值，则应判定为匹配成功并输出对应用户身份标识；在辨识方式下，若比对相似度得分集合中存在大于指定阈值的候选者，则应判定最大相似度得分的候选者为成功匹配者并输出对应用户身份标识；
- e) 应能通过屏幕提示、声光提示或其他方式，输出决策结果；
- f) 当用户识别操作时间达到最大识别时间或识别失败次数达到尝试识别次数后，应暂停用户识别功能。

示例 1：

采用分数融合方式时，分别进行人脸比对和虹膜比对，并将二者的相似度得分进行融合，然后将融合分数与阈值进行比较，根据决策逻辑输出识别结果。

示例 2：

采用决策融合方式时，分别进行人脸比对和虹膜比对，并将二者的比对结果进行决策融合，根据决策逻辑输出识别结果。

3.2.4 用户注销

产品应能对已注册的用户信息进行删除操作。

3.2.5 用户查询

产品具有信息查询功能，包括但不限于：

- a) 应能对已注册的用户信息进行查询操作；
- b) 应能显示已注册用户和模板的数量，以及最大用户和模板容量。

3.2.6 参数设置

产品应能设置控制参数，如网络、日期和时间、比对方式、最大识别时间或尝试识别次数等。

3.2.7 日志管理

产品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注册、识别、注销及参数设置等事件；
- b) 对于每一个事件，日志记录宜包括事件发生时间、事件类型、用户、事件内容、设备信息及操作人员等；
- c) 具有查询权限的管理员可以查看日志事件记录；
- d) 不应提供对日志内容的修改功能；
- e) 日志中不应出现明文的生物特征数据、密钥信息或其他安全相关的参数等。

3.2.8 指示/显示

产品应能通过显示屏、声音、灯光或其它显示装置指示/显示设备的状态。

3.2.9 节能

产品宜具有睡眠、休眠或其它自动节能功能。

3.2.10 其他功能

应支持其他非生物特征识别方式，如刷卡、密码验证等。

3.3 性能

3.3.1 面部样本质量

面部样本质量满足以下要求：

- a) 人脸样本满足GB/T 35678中要求；
- b) 虹膜样本满足GB/T 33767.6中要求。

3.3.2 注册失败率

FTER是指注册不成功的样本在总注册样本中所占的比例，FTER应不大于1%。

3.3.3 注册时间

产品从开始采集到完成注册之间的时间应不超过5s。

3.3.4 识别时间

产品从开始采集到比对结果输出之间的时间要求如下：

- a) 验证方式下，系统平均识别时间应不超过 2s；
- b) 辨识方式下，系统平均识别时间宜不超过 2s。

3.3.5 验证性能

在FAR不大于 0.001%时，FRR应不大于1%。

3.3.6 辨识性能

在注册用户为1万时，首选识别率应不小于99%。

3.3.7 活体检测

在LDFAR不大于1%时，LDFRR应不大于1%。

3.4 安全要求

3.4.1 数据安全

产品应符合以下数据安全要求：

- a) 应将面部特征识别信息与用户身份相关信息隔离存储；
注 1：面部特征识别信息包含面部样本、面部特征模板等。
注 2：隔离方式包括逻辑隔离、物理隔离。
- b) 面部特征应具有可更新、不可逆的特性；
- c) 应防止采集、处理、注册、识别及传输过程中的信息外泄及篡改；
- d) 用户注销后，应删除用户所有数据，并确保其不可恢复；
- e) 具有识别操作时间超时或尝试识别超次等安全处理措施，对失败操作进行警告或报警；
- f) 具有加载、导出过程中的数据安全保护机制；
- g) 产品应具有唯一设备编号。

3.4.2 权限管理

产品应具有不同使用权限管理功能，在注册、注销、查询、参数设置等操作中具有相关的授权机制。

3.4.3 掉电保护

在电源掉电或更换电池时，产品已存储的信息不应丢失或受到破坏。

3.4.4 设备安全

设备指示灯的安全性应符合 GB/T 20145—2006 中 4.3 辐射危害曝辐限值的规定。

3.5 光照适应性

产品的光照适应性应符合以下要求：

- a) 在均匀光照环境下，产品的最高适应光照大于等于3000 lux；
- b) 在均匀光照环境下，产品的最低适应光照小于等于100 lux。

包装表面或产品使用说明书中应标注产品的光照适应性。

3.6 通信接口

产品宜具有Wi-Fi、网口，以及韦根、开关量等数据通信接口。

4 试验方法

4.1 试验条件

4.1.1 试验环境条件

本文件中除环境适应性试验外，其他试验均在下述条件下进行。

- 环境温度：15℃～35℃；
- 相对湿度：25%～75%；
- 大气压：86 kPa～106 kPa；
- 环境光照：100 lux～3000 lux。

4.1.2 测试平台

测试平台由硬件平台和软件平台组成：

- a) 硬件平台：中央处理器主频 2.0GHz 以上、内存不小于 1GB；
- b) 软件平台：主流操作系统。

4.1.3 测试数据库

准备测试数据库，数据库的面部样本组成和规模要求应符合附录 B 的规定。

4.1.4 受试样品与辅助工具

受试方应提供带包装和使用说明书的受试样品，以及用于辅助测试的软硬件工具，包括但不限于：

- a) 若需要，则由受试方提供功能验证软件及说明文件，用于完成产品相关功能的测试；
- b) 识别性能测试软件。用于验证性能和辨识性能的测试，主要功能包括测试数据的导入、导出及算法调用等。考虑到产品容量、运行效率及通信开销等因素，识别性能测试软件可设计为以下两种形式：

- 识别性能测试软件通过接口与受试样品进行通信，通过接口调用，以实现算法运行比对并输出比对结果记录文件（见附录 C）；
- 由 PC 端的算法动态库模拟受试样品，并由识别性能测试软件调用算法动态库，以实现算法运行比对并输出比对结果记录文件。

c) 识别性能指标统计软件。用于统计分析比对结果记录表并计算识别性能指标。一般由检测机构或第三方提供。

4.2 外观和结构

4.2.1 外观

用目测方法进行外观检查，判断是否符合6.1.1 a)的要求。

用白色棉布蘸水或蘸酒精擦拭产品标识15s，判断是否符合6.1.1 b)的要求。

4.2.2 结构

用目测手动方法进行结构检查，判断是否符合6.1.2的要求。

4.3 功能试验

4.3.1 基本功能

4.3.1.1 图像采集

受试样品加电启动后，按照产品使用说明书中规定的步骤，检查受试样品是否能进行样本采集，并输出面部样本或面部特征等信息。

采集不少于10名测试人员的面部样本，采集过程中，检查产品以下功能是否符合要求：

- a) 将受试样品移至暗处（低于100 lux），检查样品是否自动补光且正常工作。采用分析光谱仪测试样品的光谱中心波长，重复测试三次，统计其平均值，是否符合6.2.1.1 a)的要求；
- b) 检查受试样品是否自动感知、判断人体身高和位置，且适应身高范围符合6.2.1.1 b)的要求；
- c) 检查受试样品是否能够通过调整补光灯角度、变换补光位置等方式处理光斑遮挡虹膜问题；
- d) 测试人员佩戴口罩时，检查受试样品是否能够进行人脸检测及面部识别；
- e) 检查受试样品是否使用采集融合方式；
- f) 检查受试样品是否能够输出面部样本或面部特征等信息

4.3.1.2 质量判断

执行用户注册或识别功能，测试人员通过超出采集区域、面部遮挡、增大姿态角、佩戴墨镜等方法，检查受试样品是否能通过质量判断或合格性判定，并以语音、图形文字、灯光等方式提示失败或重新采集。

4.3.1.3 活体检测

执行用户识别功能，按照表1选择假体攻击类型进行测试，检查受试样品是否能进行活体检测，并输出相关提示信息。

未注册的测试人员佩戴抠除眼部区域的人脸面具，执行用户识别操作，检查是否匹配通过，如果匹配不通过，则活体检测成功，否则，活体检测失败。

4.3.2 用户注册

现场注册方式下，按照产品使用说明书中规定的步骤，10名测试人员依次注册，检查受试样品的

注册相关功能是否符合要求：

- a) 执行现场注册时，检查受试样品是否符合图像采集、质量判断、活体检测等基本功能的要求，并进行面部特征提取、模板构建及存储等，操作完成时是否给出注册成功或失败的提示；
- b) 注册过程中，检查受试样品是否具备异常情况判定及处理能力，包括但不限于面部样本采集失败、样本质量不合格、检测到假体攻击、面部特征提取失败、模板构建及存储失败等异常情况的相应处理机制；
- c) 注册成功后，检查系统内所注册人员的身份信息及面部特征模板是否存在。

非现场注册方式下，将不少于100个测试样本及身份信息批量导入受试样品，检查受试样品的注册相关功能是否符合要求：

- a) 批量导入过程中，检查受试样品是否具备异常情况判定及处理能力，包括但不限于样本质量不合格、面部特征提取失败、模板构建及存储失败等异常情况的相应处理机制；
- b) 批量导入完成后，检查系统内所注册人员的身份信息及面部特征模板是否存在。

4.3.3 用户识别

完成注册功能试验后，对已注册人员进行识别，检查测试人员是否被正常识别并给出识别结果。未注册人员进行识别时，检查该人员是否被拒绝。

按照验证和辨识两种方式分别进行试验：

- a) 验证方式：已注册或未注册的测试人员通过刷卡或输入编号等形式进行 1:1 比对，检查测试人员的真实身份与其声称的身份是否一致；
- b) 辨识方式：已注册人员进行 1:N 比对，检查受试样品是否能正确辨认该人员并输出对应的用户身份信息；未注册人员进行 1:N 比对，检查受试样品是否能拒绝该人员；
- c) 进行防假体攻击的面部识别试验，由未注册人员佩戴抠除眼部区域的人脸面具，并尝试进行识别，检查受试样品是否给出假体攻击或识别失败的提示；
- d) 识别过程中，检查受试样品是否具备异常情况判定及处理能力，包括但不限于样本质量不合格、检测到假体攻击、面部特征提取失败、识别时间超时或尝试识别超次等情况的处理机制。

4.3.4 用户注销

按照产品使用说明书中规定的步骤，对已注册人员的面部特征模板进行删除操作，检查受试样品在删除操作完成时是否有删除成功的提示，并检查受试样品是否不再识别该测试人员。

4.3.5 用户查询

按照产品使用说明书中规定的步骤，执行相关的用户查询操作：

- a) 对已注册人员的数据进行查询操作，检查受试样品在查询操作完成时是否有查询结果的显示；
- b) 检查是否能查看已注册的用户数量，以及最大容量。如果超过最大容量，则不能再次进行注册，并有相应提示。

4.3.6 参数设置

按照产品使用说明书中规定的步骤，检查受试样品是否能查看和修改网络、日期和时间、比对方式、最大识别时间或尝试识别次数等控制参数。

4.3.7 日志管理

按照产品使用说明书进行操作，检查受试样品在注册、识别、注销及参数设置等过程中，是否能按规定产生日志记录，日志中不能有生物特征数据的明文、密钥信息或安全参数，并检查是否禁止修改和删除日志。

4.3.8 指示/显示

在进行注册、识别、注销等操作过程中，检查受试样品是否能通过显示屏、声音、灯光或其它显示装置指示/显示其状态。

4.3.9 节能

按产品使用说明书的设置，在开启节能功能后，检查受试样品是否可以进入节能状态。

4.3.10 其他功能

检查受试样品是否支持刷卡、密码验证等其他非生物特征识别方式，并按照产品使用说明书中规定的步骤进行操作和查验。

4.4 性能试验

4.4.1 注册失败率

将符合6.3.1中面部样本质量要求的M (M≥3000) 个样本批量导入受试样品，受试样品给出成功注册数量S，按照公式 (1) 计算FTER。

$$FTER = (M - S) / M \times 100\% \dots\dots\dots (1)$$

式中：

M——批量导入样本量；

S——注册成功样本量。

注：对于产品容量不足3000的情况，测试分批进行。

4.4.2 注册时间

按照产品使用说明书规定进行现场注册，记录开始注册时间与注册完成时间，将二者的差值作为注册时间。10名测试人员依次注册，记录每个测试人员的注册时间，统计平均值。

4.4.3 识别时间

按照产品使用说明书规定进行面部识别，记录开始识别时间与识别完成时间，将二者的差值作为识别时间。10名测试人员依次识别，记录每个测试人员的识别时间，统计平均值。

验证方式下，识别时间试验按以下步骤进行：

- a) 清空受试样品中的所有注册数据；
- b) 执行注册功能，注册一个用户；
- c) 执行验证功能，记录产品从开始采集到识别结果输出之间的时间；
- d) 重复 c) 20 次，计算平均识别时间，判断是否满足要求。

辨识方式下，识别时间试验按以下步骤进行：

- a) 清空受试样品中的所有注册数据；
- b) 将注册集中的测试样本依次注册进入受试样品，直到注册用户达到最大容量为止；
- c) 执行辨识功能，记录产品从开始采集到识别结果输出之间的时间；
- d) 重复 c) 20 次，计算平均识别时间，判断是否满足要求。

4.4.4 验证性能

按照附录B的要求构建用于测评FRR和FAR的测试数据集，测试数据集包括注册集和探针集，本文件的FRR和FAR测评采用同一对注册集和探针集。测试样本包含从测试数据库中抽取的面部样本，且应包含使用受试样品在测试现场采集至少10名测试人员的面部样本。

测试数据集构建完成后，提取注册集和探针集中测试样本的面部特征。

当进行FRR测试时，将注册集和探针集中同一样本主体的面部特征进行比对，共计S（ $S \geq 3,000$ ）次，记录提示错误拒绝的次数 N_1 ，按照公式（2）计算FRR。

$$FRR = N_1 / S \times 100\% \dots\dots\dots (2)$$

当进行FAR测试时，将注册集和探针集中不同样本主体的面部特征进行特征比对，共计W（ $W > 3,000,000$ ）次，记录提示错误识别的次数 N_2 ，按照公式（3）计算FAR。

$$FAR = N_2 / W \times 100\% \dots\dots\dots (3)$$

验证性能测试步骤如下：

- a) 准备测试，如清空受试样品中的所有注册数据；
- b) 从注册集中导入面部样本或面部特征作为注册面部特征模板；
- c) 从探针集中输入面部样本或面部特征作为待验证样本，并由识别性能测试软件调用受试样品或算法动态库进行特征与模板间的特征比对；
- d) 输出或导出特征比对结果记录文件，文件中的比对记录包括：两个比对样本的标识和比对结果，具体参见附录C中的表C.1；
- e) 待所有特征比对完成，根据比对结果记录文件，按照公式（2）和公式（3）分别统计FRR和FAR。

4.4.5 辨识性能

按照附录B的要求构建用于测评首选识别率的测试数据集，测试数据集包括注册集和探针集，注册集的样本主体数量不低于10,000人，探针集的样本主体数量不低于3,000人，且探针集的样本主体在注册集中已存在。测试样本包含从测试数据库中抽取的面部样本，且应包含使用受试样品在测试现场采集至少10名测试人员的面部样本。

测试数据集构建完成后，提取注册集和探针集中测试样本的面部特征。使用探针集中的面部特征到注册集中进行特征比对搜索，共计搜索Q轮（ $Q \geq 3,000$ ）次，记录TOP1的次数 N_{top1} ，按照公式（4）计算首选识别率。

$$\text{首选识别率} = N_{top1} / Q \times 100\% \dots\dots\dots (4)$$

辨识性能测试步骤如下：

- a) 准备测试，如清空受试样品中的所有注册数据；
- b) 从注册集中导入面部样本或面部特征作为注册面部特征模板；
- c) 从探针集中输入面部样本或面部特征作为待辨识样本，并由识别性能测试软件调用受试样品或算法动态库进行特征与模板库的特征比对搜索；
- d) 输出或导出比对结果记录文件，文件中的比对记录包括候选者列表的模板标识和比对得分（可选），具体参见附录C中的表C.2；
- e) 待所有特征比对搜索完成，根据比对结果记录文件，按照公式（4）统计首选识别率。

4.4.6 活体检测

4.4.6.1 活体检测错误接受率

采用表1中一类或多类假体，对受试样品进行不少于3000次的识别攻击试验，记录误判为活体的次数A和总测试次数B，按照公式（5）计算受试样品LDFAR。

$$\text{LDFAR} = A/B \times 100\% \dots\dots\dots (5)$$

在攻击试验过程中，可根据不同应用情况，采取不同策略进行测试，包括但不限于：

- a) 变换假体样本的位置、角度及环境光照等进行测试；
- b) 将人脸假体样本与虹膜假体样本进行组合测试；
- c) 假体样本与真人进行组合测试，如：测试人员佩戴剔除眼部区域的人脸面具。

表 1 面部识别假体攻击类型

假体攻击类型		样例	样本数量≥
假体人脸	二维假体攻击类型	静态纸质图像：采用不同材质的A4、A3 打印纸、相纸及胶片等，印制或绘制人脸图像，含剔除眼部区域或眼鼻区域或眼鼻嘴区域的样品； 静态电子图像：移动终端、微型计算机等显示人脸图像； 动态图像：录制视频、合成视频等。	100
	三维假体攻击类型	3D 人脸仿真面具、3D 头模，含剔除眼部区域或眼鼻区域或眼鼻嘴区域的样品。	10
假体虹膜	二维和三维假体攻击类型	虹膜照片、虹膜视频； 复制虹膜纹理的眼镜（含隐形）； 仿真人造眼。	10

4.4.6.2 活体检测错误拒绝率

测试人员不少于10人，站在受试样品前，总共进行不少于3000次的测试，记录受试样品给出无法识别/非活体的次数C，以及总测试次数D，按照公式（6）计算受试样品的LDFRR。

$$\text{LDFRR} = C/D \times 100\% \dots\dots\dots (6)$$

4.5 安全试验

4.5.1 数据安全

数据安全试验按照以下方法进行：

- a) 通过数据库查询或文件查询，检查面部特征识别信息与用户身份相关信息是否隔离存储；
- b) 比较重新注册前后的特征模板，检查面部特征是否可更新、不可逆特性；
- c) 在采集、处理、注册、识别及传输过程中，处理用户敏感数据（如用户名、生物特征、密码等）时，通过数据抓包、文件查看等手段检查敏感数据是否进行加密；
- d) 在用户注销后，通过查询功能、数据库查询等手段检查用户数据是否被删除或匿名化；
- e) 识别时使用非注册用户，检查受试样品是否具有识别时间超时或尝试识别超次等处理措施，对失败操作是否进行警告或报警；
- f) 通过数据抓包、文件查看等手段检查敏感数据在加载、导出过程中是否进行加密和校验；
- g) 检查受试样品是否具有唯一设备编号。

4.5.2 权限管理

受试样品在注册、注销、查询、参数设置等过程中，检查是否具有相应的授权机制。

4.5.3 掉电保护

受试样品加电启动后，按照产品说明书的有关规定进行各项功能测试，检测正常后，切断电源，然后重新加电启动，检查受试样品在断电前存储的数据是否丢失或受到破坏。

4.5.4 设备安全

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/787145062031010032>