IIFAA

互联网金融身份认证联盟标准

T/IIFAA 3001.2-2021

远程人脸识别应用技术规范
第 2 部分：自助通关

Technical specification for application of remote face recognition—

Part 2: Self-service entrance

2021－01－22 发布　　2021－01－22 实施

互联网金融身份认证联盟　发布

目　　次

前　言

T/IFAA 3001-2021《远程人脸识别应用技术规范》分为以下部分：

——第1部分 金融账户管理；

——第2部分 自助通关。

本部分为T/IFAA 3001-2021的第2部分。

本部分按照GB/T 1.1—2020给出的规则起草。

本部分由互联网金融身份认证联盟提出和归口

本部分起草单位：平安科技（深圳）有限公司、蚂蚁科技集团股份有限公司、银行卡检测中心、中国电信综合平台开发运营中心、深圳蚂里奥技术有限公司、深圳竹云科技有限公司、航天信息股份有限公司、深圳奥比中光科技有限公司、深圳市耐能人工智能有限公司、楚天龙股份有限公司、长春吉大正元信息技术股份有限公司、北京安御道合科技有限公司、深圳市汇顶科技股份有限公司、北京的卢深视科技有限公司、上海申石软件有限公司。

本部分主要起草人：倪春娟、王磊、于惊涛、林冠辰、杨波、王鑫、潘浩、张力文、江隆业、张兼、戴立伟、向韬、周珅珅、张宇驰、张安定、郝康立、王晓松、崔明伟、杨宏英、陈鑫、方宏俊、赵所峰、户磊、朱海涛、汪建仁、周毅华。

远程人脸识别应用技术规范 第2部分 自助通关

1 范围

本文件提出了自助通关应用中远程人脸识别技术应用的功能要求、性能要求和安全要求等内容。

本文件适用于IIFAA的系统和设备厂商、服务提供商、管理单位等开展远程人脸识别应用服务，在自助通关服务中提供基于远程人脸识别应用的服务参考和技术指导。

本文件不适用于火车站、机场、海关、酒店等只能调用相关主管机构专业数据或利用证件图像本地认证的场景。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 26238-2010 信息技术 生物特征识别术语

GB/T 33767.5-2018 信息技术 生物特征样本质量 第5部分：人脸图像数据

GB/T 35273-2020 信息安全技术 个人信息安全规范

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

3 术语和定义

GB/T 26238-2010 、GB/T 37036.3-2019 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 26238-2010、GB/T 37036.3-2019 中的某些术语和定义。

3.1

人脸识别 face recognition

以人脸特征作为识别个体身份的一种个体生物特征识别方法。通过分析提取人脸样本的人脸特征，并将其与已存储的可更新人脸参考进行比对，用以识别用户身份。依据应用方式不同，人脸识别可分为人脸验证和人脸辨识。

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。

[来源：GB/T 37036.3-2019，3.2]

3.3

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表示。
[来源：GB/T 37036.3-2019，3.5]

3.4

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。
[来源：GB/T 37036.3-2019，3.6]

3.5

人脸探针 face probe

输入到算法的、与可更新人脸参考数据进行比对的人脸数据。

3.6

可更新人脸参考 renewable face reference

基于人脸数据生成的不可逆脱敏的、可更新、可撤销的识别码。

3.7

活体检测 liveness detection

用于判断人脸采集设备捕捉到的人脸图像是否来源于活体的行为。

3.8

错误接受率 false acceptance rate

人脸验证过程中错误接受的数目占测试集合中应被拒绝的测试数目的百分率。

3.9

错误拒绝率 false rejection rate

人脸验证过程中错误拒绝的数目占测试集合中应被接受的测试数目的百分率。

3.10

活体检测错误接受率 liveness detection attack false acceptance rate

活体检测过程中误判为人脸活体的数目占测试集合中应被识别为假体的测试数目的百分率。

3.11

活体检测错误拒绝率 liveness presentation false rejection rate

活体检测过程中误判为人脸假体的数目占测试集合中应被识别为活体的测试数目的百分率。

4 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）

LDAFAR:活体检测错误接受率(Liveness detection attack false acceptance rate)

LPFRR:活体检测错误拒绝率（Liveness presentation false rejection rate）

5 应用框架

5.1 概述

远程人脸识别，是基于人脸识别的远程身份认证技术。远程人脸识别的完整过程需在终端设备侧和远端服务器侧共同完成。在终端设备侧对用户的人脸样本进行采集，并传递到远端服务器侧，完成对用户人脸特征的存储和比对，输出识别结果。

在写字楼、智能社区以及园区的自助进出等场景中，均可运用远程人脸识别进行身份的认证和核验。可更新人脸参考是由在用户注册时，机构自身采集的人脸信息生成。

自助通关应用中，进行人脸注册、更改和注销的终端设备可以为智能移动终端、带摄像设备的计算机设备等，终端设备通过移动APP、H5、Web等不同客户端形式提供人脸信息注册、更改和注销服务。进行人脸验证和辨识的终端设备为专用设备，与闸机等机具集成，一般不提供除验证外的其他人脸识别服务。

5.2 总体框架

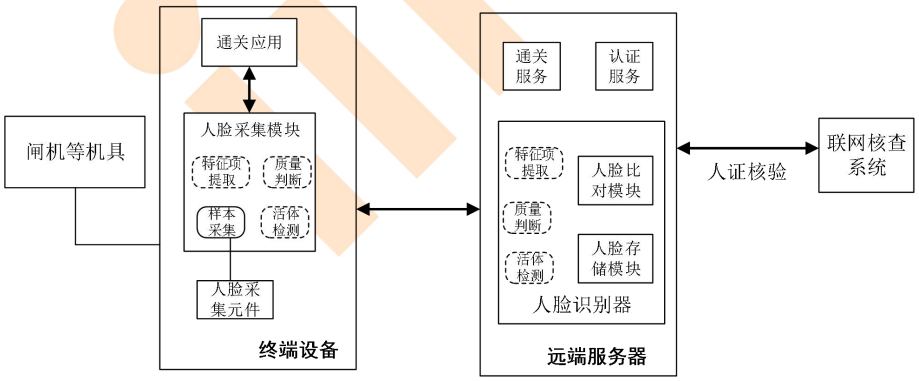

图 1 远程人脸识别自助通关应用的总体框架

远程人脸识别自助通关应用的总体框架如图1所示。

终端设备：自主通关应用场景中，终端设备主要包含2类：一类是进行人脸注册、更改和注销的通用终端设备，如手机、平板、笔记本电脑等；另一类是与闸机等机具相连，通关时进行人脸验证和辨识的专用终端设备。

通关应用：通关应用也包含2类：一类是在通用终端设备提供人脸信息注册、更改和注销服务的移动APP、H5、Web等不同客户端，面向用户可操作；另一类是在专用终端上提供对外服务的应用，面向用户不可操作。

人脸识别器：基于人脸识别技术对用户进行身份验证，一般由人脸采集模块、人脸存储模块和人脸比对模块等组成。在远程模式中，一般人脸采集模块位于终端设备侧，人脸存储模块和人脸比对模块位于服务器侧。

人脸采集模块包括人脸样本采集、质量判断、活体检测、特征项提取等子功能模块，根据方案的不同，质量判断、活体检测、特征项提取等子模块可位于终端设备侧，也可位于服务器侧。

人脸采集元件：用于采集人脸的传感器，一般为摄像头等图像采集装置。

远端服务器：后台实现部分通关服务、身份认证服务和人脸识别过程部分功能的服务器，并能其他服务器进行对接。

5.3 应用流程

5.3.1 远程人脸注册

远程人脸注册过程包括但不限于以下步骤：

a) 用户在移动设备或其他终端设备中通过通关应用移动APP、H5、Web等不同客户端向远端服务器发起注册请求；

b) 服务器对用户进行的身份信息进行认证和核查，判断是否允许注册请求；

c) 终端设备中的人脸采集模块采集用户人脸样本；

d) 终端设备或服务器中的相关子模块进行质量判断、活体检测、用户人脸特征项提取，形成可更新人脸参考；如有人脸采集失败等异常情况，应告知用户并采取重新进行人脸样本采集等处理手段；

e) 服务器将可更新人脸参考存储在人脸存储模块中，把用户可更新人脸参考和用户身份标识关联起来；

f) 结束注册流程。

5.3.2 远程人脸变更

远程人脸变更过程包括但不限于以下步骤：

a) 用户主动在终端设备侧通过客户端、或系统主动向服务器发起变更请求；

b) 服务器识别出对应的身份认证注册关系并判断是否进行此次变更请求；

c) 终端设备中的人脸采集模块采集用户人脸样本；

d）终端设备或服务器中相关子模块进行质量判断、活体检测、以及用户人脸特征项提取，形成新的可更新人脸参考；

e) 服务器的人脸存储模块完成该用户可更新人脸参考的更新，并返回结果给客户端；

f) 结束变更流程。

5.3.3 远程人脸注销

远程人脸注销过程包括但不限于以下步骤：

a) 用户在终端设备侧通过客户端主动向服务器发起注销请求；

b) 服务器识别出对应的身份认证注册关系并判断是否进行此次注销请求；

c) 在服务器的人脸存储模块中删除该身份相关联的可更新人脸参考、身份标识和其他注册信息等，并返回给客户端；

d) 结束注销流程。

5.3.4 远程人脸辨识和验证

远程人脸辨识和验证过程包括但不限于以下步骤：

a) 用户进入识别区域，或请求验证操作后，专用终端设备发送访问请求至远端服务器；
b) 远端服务器识别出需要进行身份认证，向终端设备发送验证或辨识请求；
c) 专用终端设备中的人脸采集装置采集用户人脸样本；
d) 专用终端设备和远端服务器中相关子模块进行质量判断、活体检测，提取用户人脸特征项，形成人脸探针；
e) 远端服务器中，人脸比对模块将人脸探针与存储在人脸存储模块中的可更新人脸参考进行比对，并进行决策得到识别结果，并返回身份认证识别结果至专用终端设备；
f) 专用终端设备将识别根据识别结果进行后续操作处理，如闸机等机具打开允许人员进入，或要求用户重新进行人脸识别；
g) 结束辨识或验证过程，闸机等机具和专用终端设备恢复到默认状态。

6 功能要求

6.1 人脸采集模块

6.1.1 基本功能

人脸采集模块应能实现人脸信息的采集和传输，基本功能包括但不限于：

a) 应能使用终端设备上的人脸采集模块采集人脸特征样本，并将其转化为适合人脸识别处理的数据格式；
b) 专用终端设备中的采集模块应能对进入识别区域的人脸图像进行主动辨识；
c) 应具有明确的用户提示，告知用户对其人脸样本进行了采集，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；
d) 应能将提取出的用户人脸特征项传输到后续的处理模块，如人脸存储模块或人脸比对模块；
e) 应具备异常情况判定及处理能力，如人脸样本采集失败、人脸样本未通过质量判断、检测到假体攻击、 人脸特征项提取失败等的相应处理机制；
f) 宜采用技术手段对采集过程中环境光照情况、人脸区域遮挡情况、姿态等进行判断，在光照条件不适宜、用户姿态不适宜、人脸有遮挡等情况下提示用户配合改进；
g) 采集区域内出现多人脸或无人脸的情况，宜提示用户配合改进或技术上设定规则选择主要人脸区域进行合理处理。

6.1.2 活体检测子模块

人脸采集模块应具有活体检测功能，活体检测子模块的功能包括但不限于：

a) 应能防范二维假体攻击和三维假体攻击；
b) 检测到假体攻击时，应具备相应的处理机制，如失败/错误提示或风险提示等；
c) 能防范的二维假体攻击包括但不限于二维静态纸质图像攻击、二维静态电子图像攻击、二维动态图像攻击等；
   ——活体检测防范二维静态纸质图像攻击时，宜考虑的因素包括但不限于：人脸图像材质、人脸图像质量、呈现方式、裁剪方式；
   ——活体检测防范二维静态电子图像攻击时，宜考虑的因素包括但不限于：显示设备类型、显示设备能力、人脸图像质量、呈现方式；
   ——活体检测防范二维动态图像攻击时，宜考虑的因素包括但不限于：二维动态图像类型、显示设备类型、显示设备能力、二维动态图像质量、呈现方式。

d) 能防范的三维假体攻击包括但不限于三维面具攻击、三维头模攻击、化妆修饰的三维头模攻击等；
——活体检测防范三维面具攻击时，宜考虑的因素包括但不限于：面具材质、呈现方式、光线条件、裁剪方式；
——活体检测防范三维头模攻击时，宜考虑的因素包括但不限于：头模材质、呈现方式、光线条件。
e) 宜采用RGB和深度数据同时进行判断。

6.1.3 质量判断子模块

人脸采集模块应具有质量判断功能，质量判断子模块的功能包括但不限于：
a) 应对用于人脸识别的当前人脸样本质量进行评估，判断是否符合人脸识别算法要求，质量判断的依据符合GB/T 33767.5-2018的要求；
b) 人脸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；
c) 人脸样本质量判断功能应包括不限于：
——人脸区域大小评估，判断检测到的人脸区域大小是否符合人脸识别算法要求；
——清晰度评估，判断检测到的人脸区域清晰程度是否符合人脸识别算法要求；
——完整度评估，判断检测到的人脸区域完整程度是否符合人脸识别算法要求；
——表情评估，判断人脸表情是否合理；
——姿态角度评估，判断人脸姿态的旋转角度、俯仰角度和倾斜角度是否在合理；
——眼睛闭合程度评估，对眼睛的闭合程度进行评估并判断是否合理；
——嘴巴闭合程度评估，对嘴巴的闭合程度进行评估并判断是否合理；
——光照度评估，判断检测到的人脸区域光照情况是否合理。
d) 宜结合RGB和深度图对样本质量进行评估，判断人脸完整、五官及面部轮廓特征是否明显，无明显空洞，人脸无异常点。

6.2 人脸存储模块

人脸存储模块，应能实现人脸信息的存储，基本功能包括但不限于：
a) 应具备人脸存储模块管理功能， 包括但不限于： 应只允许具有合法权限的实体录入、访问、读取或删除人脸存储模块中的用户人脸数据；
b) 应把登记的用户可更新人脸参考与该用户的身份标识进行关联；
c) 不应使用相同的用户身份标识去标识两个或以上不同用户，同一用户在同一人脸存储模块中应只对应唯一的身份标识；
d) 应具备异常情况判定及处理能力，如可更新人脸参考登记、读取或删除失败时的相应处理机制；
e) 应具备动态存储能力，人脸存储库初始化数据支持从公安机关等权威机构批量存入，并支持动态更新，能根据比对结果动态调整可更新人脸参考；
f) 宜允许同一用户在人脸存储模块中登记一个或多个不同条件下提取的可更新人脸参考；
g) 宜支持已登记用户对人脸存储模块中属于该用户的可更新人脸参考进行增加、删除等操作。

6.3 人脸比对模块

人脸比对模块，应能实现人脸特征的比对，基本功能包括但不限于：

a) 应提供一对一比对的用户验证功能和一对多的用户辨识功能；
b) 应能够将输入的用户人脸特征项和已在人脸存储模块中登记的可更新人脸参考特征项进行比对， 计算出相似度比对得分；
c) 应能够根据比对得分进行识别决策， 并能够输出识别结果；
d) 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。

6.4 远端服务器

远端服务器提供以下功能，包括但不限于：
a) 应能实现人脸的注册、验证、变更、注销等业务功能；
b) 应能够对身份认证注册关系进行管理，包括注册、维护和注销等；
c) 应具备人脸存储模块和比对模块；
d) 应能与公安或出入境等权威第三方的身份核查系统进行交互，实现联网身份核验；
e) 应具备对人脸信息进行备份的能力以及相应的恢复控制措施，应采用技术措施保证备份数据的保密性和完整性；
f) 通过权威第三方身份核查系统核查的记录，可被记录到人脸存储模块，并记录第三方身份核查系统的相关信息，便于以后本地认证；
g) 应对外提供安全认证协议，保证认证信息的安全传输；
h) 具备多因素组合认证能力（人脸+指纹、人脸+声纹等），提升认证强度，确保业务安全性；
i) 应具备人脸识别历史记录和通关记录查询能力，并可形成分析报表。

7 性能要求

7.1 基本性能要求

远程人脸识别应用的基本性能应满足以下要求：
a) 一对一人脸验证时，当错误接受率FAR≤0.001%时，错误拒绝率FRR≤3%；
b) 一对多人脸辨识时，应满足：
——人脸库的数量N ≤ 500，当错误接受率FAR≤0.001%时，错误拒绝率FRR≤5%；
——500<N≤100000 ，当错误接受率FAR≤0.001%时，错误拒绝率FRR≤6%。

7.2 响应时间要求

远程人脸识别应用的系统响应时间应满足以下要求：
a) 人脸注册时，系统响应时间（完成人脸样本采集流程总时间）≤3000ms；
b) 人脸验证时，系统响应时间（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）≤2000ms。

7.3 活体检测性能要求

当活体检测错误接受率LDAFAR为0.1%时，活体检测错误拒绝率LPFRR应≤2%。

7.4 质量判断性能要求

人脸样本应满足以下质量要求：
a) 人脸全景图分辨率应不低于 640*480 像素；
b) 人脸全景图应采用标注人脸区域等方式准确确定人脸识别对象；

c) 人脸全景图几何失真应小于等于 10%；
d) 人脸区域应完整，无编辑修改性处理，眼镜框不遮挡眼睛，镜片无色无反光，美瞳镜片不遮挡干扰人眼球区域的纹理成像；
e) 人脸区域应清晰，轮廓和五官清晰，无浓妆；
f) 人脸图像的瞳间距应不小于 60 像素，宜大于 90 像素；
g) 人脸图像的表情宜合理，中性或微笑，眼睛自然睁开，嘴唇自然闭合或微张；
h) 人脸姿态应在合理范围内，人脸图像的旋转角、俯仰角、倾斜角应在±20° 以内；
i) 人脸区域光照光源应为自然光、白炽灯光、或钨丝灯光，光源非彩色光；
j) 人脸区域光照均匀，对比度适中，脸部无明显阴影、无过曝光和无欠曝光，图像灰度化后脸部区域动态范围主要分布在 85～200 间，灰度级应为 256 级。

7.5 专用设备性能要求

7.5.1 专用终端设备要求

通关时进行人脸验证和辨识的专用终端设备应满足以下性能要求，包括但不限于：
a) 专用终端设备应支持与证件信息采集装置、指纹等其他生物特征采集装置集成，支持相机参数的输出；
b) 专用终端设备应在温度-10~60℃的条件下正常工作；
c) 终端应具备通讯能力，可支持以下全部或部分类型的接口：串行通讯接口、USB接口、红外通讯接口、以太网通讯接口、蓝牙通讯接口、WIFI通讯接口、4G及以上无线网络通讯接口等；
d) 人脸采集单元在终端侧宜以操作系统标准外设的形式存在，不依赖第三方驱动、定制API、SDK等方式进行开发支持。

7.5.2 人脸采集元件要求

专用终端设备上的人脸采集单元应满足以下性能要求，包括但不限于：
a) 在终端设备高度固定下，人脸采集单元应能识别身高在1米4~1米9范围内的人，视场角FOV不应低于60度；
b) 应具有良好的光照环境适应性，在人脸脸部光照强度为15Lux-7500Lux、色温2300K-7500K的条件下，采集的人脸图像符合质量要求；
c) 应具有良好的运动场景能力，在人体慢速行走或站立晃动下情况下能够对正脸人脸正常识别；
d) 人脸采集单元应能够将图像采集单元传递过来的数字图像信息进行如白平衡、色彩校正、编解码等信息处理；
e) 人脸采集单元可以基于包括但不限于单目摄像头、红外可见光双目摄像头、可见光双目摄像头、结构光摄像头、TOF（Time Of Flight）摄像头的形态；
f) 人脸采集单元应有多码流，能够同时输出深度图、IR图和彩色图像，宜有深度图、IR图及彩色图对齐功能；
g) 采集的深度图像分辨率不低于640*400像素，深度数据的精度不大于3mm（采集物体位于采集单元前50cm处），人脸深度数据完整性大于80%，在五官等关键位置附近完整性大于95%；
h) 深度数据采集同步性宜不大于60ms，最大帧率宜不低于10帧/秒。

8 安全要求

8.1 系统安全

8.1.1 安全物理环境

远端服务器所在的物理环境安全应符合GB/T 22239-2019中8.1.1的要求。

8.1.2 安全通信网络

通信网络安全应符合GB/T 22239-2019中8.1.2的要求。

8.1.3 安全区域边界

远端服务器区域边界安全应符合GB/T 22239-2019中8.1.3的要求。

8.1.4 安全计算环境

远端服务器和终端设备的安全计算环境要求包括但不限于：

a) 远程服务器的操作系统以及所承载的应用和数据，应符合GB/T 22239-2019 中8.1.4的要求；
b) 终端设备中所承载的应用和数据，应符合GB/T 22239-2019 中7.1.4的要求。

8.2 人脸信息安全

8.2.1 概述

人脸信息，包括处于任何阶段的人脸样本、可更新人脸参考、人脸探针、人脸特征或人脸特征项等，均属于个人敏感信息，应符合GB/T 35273-2020中的相关要求。

8.2.2 人脸信息采集安全

人脸信息采集安全技术要求包括但不限于：

a) 人脸注册采集人脸信息前，应验证用户身份；
b) 人脸注册采集人脸信息前，应单独向被采集用户告知人脸信息收集、使用人脸信息的目的、方式和范围，以及存储时间等规则，征得用户明示同意后方可进行采集；
c) 人脸信息采集完成后，应立即对人脸信息进行加密处理；
d) 应采取安全措施保证人脸信息不被其他设备或程序非授权获取；
e) 应采取防篡改机制保证人脸信息不被其他设备或程序篡改；
f) 在采集人脸信息后，应对人脸信息进行去标识化处理或脱敏处理，以确保对外不可用；
g) 人脸采集过程应在终端设备内的独立的逻辑域或物理域中实现；
h) 在人脸信息采集结束后，应及时清除采集的人脸样本，并确保其不可恢复。

8.2.3 人脸信息传输安全

人脸信息传输安全技术要求包括但不限于：

a) 应采用安全传输协议，保证人脸信息传输时的完整性和保密性；
b) 人脸信息传输前，服务器需对采集终端设备进行身份确认，以确保终端设备的身份合法性。

8.2.4 人脸信息存储安全

人脸信息存储安全技术要求包括但不限于：

a) 终端设备上应禁止以任何形式留存人脸信息，包括但不限于人脸采集、验证等过程中使用的人脸信息；
b) 应采用技术措施确保人脸信息安全后再进行存储，例如将人脸信息的原始信息和摘要分开存储，或仅存储摘要信息；
c) 应加密存储人脸信息，并防止人脸信息的未授权访问、泄露、篡改或损毁；
d) 人脸信息保存期限应为实现用户授权使用的目的所需的最短时间，超出上述保存期限后，应对人脸信息进行删除或匿名化处理；
e) 应采取关联校验技术，保障存储在服务器中的人脸信息与用户身份信息的对应关系不被篡改。

8.2.5 人脸信息使用安全

人脸信息使用安全技术要求包括但不限于：

a) 使用人脸信息时，不得超出与收集时所声称的目的具有直接或合理关联的范围；
b) 在人脸信息注册、验证、变更和注销各个环节，应对关键操作信息进行日志记录；
c) 用户主动发起人脸信息变更或注销时，应采用使用两种以上要素验证用户身份；
d) 应具有失败处理措施，在人脸识别失败时进行相应提示并限制失败次数，超过限制次数时触发相应的失败控制机制；人脸信息的委托处理、共享、转让和公开披露，应符合GB/T 35273-2020中第9章的相关要求。
e) 人脸信息比对后，应确保比对结果输出的数据保密性和完整性；
f) 人脸信息删除后，应确保不可被检索、访问。