IIFAA

互联网金融身份认证联盟标准

T/IIFAA 3001.1-2021

远程人脸识别应用技术规范
第 1 部分：金融账户管理

Technical specification for application of remote face recognition—

Part 1: Financial account management

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/IIFAA 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/IIFAA 3001-2021的第1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、冯春培、陈继东、落红卫、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1部分 金融账户管理

1 范围

本文件提出了金融账户管理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的金融机构、设备厂商等开展远程人脸识别应用服务，为金融业务的账户管理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。

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 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

JR/T 0171-2020 个人金融信息保护技术规范

中国人民银行关于改进个人银行账户服务加强账户管理的通知（银发〔2015〕392号）

中国人民银行关于落实个人银行账户分类管理制度的通知（银发〔2016〕302号）

3 术语和定义

GB/T 26238 、GB/T 37036.3 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、GB/T 37036.3 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

下述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LDAFAR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。

在金融账户远程开户、账户解锁、消费金融申请、信用卡申领、业务签约、银行卡业务、核保理赔等金融业务中，均可利用远程人脸识别进行身份的核验。远程人脸识别有两种应用模式，一种是由第三方专业机构负责身份认证，另一种是由金融机构直接进行身份认证。应用远程人脸识别技术对金融账户进行管理，应遵循银发〔2015〕392号、银发〔2016〕302号及其他金融行业监管要求，对账户进行分类管理、严格核验身份信息、管控可采集人脸信息的终端设备。

5.2 总体框架

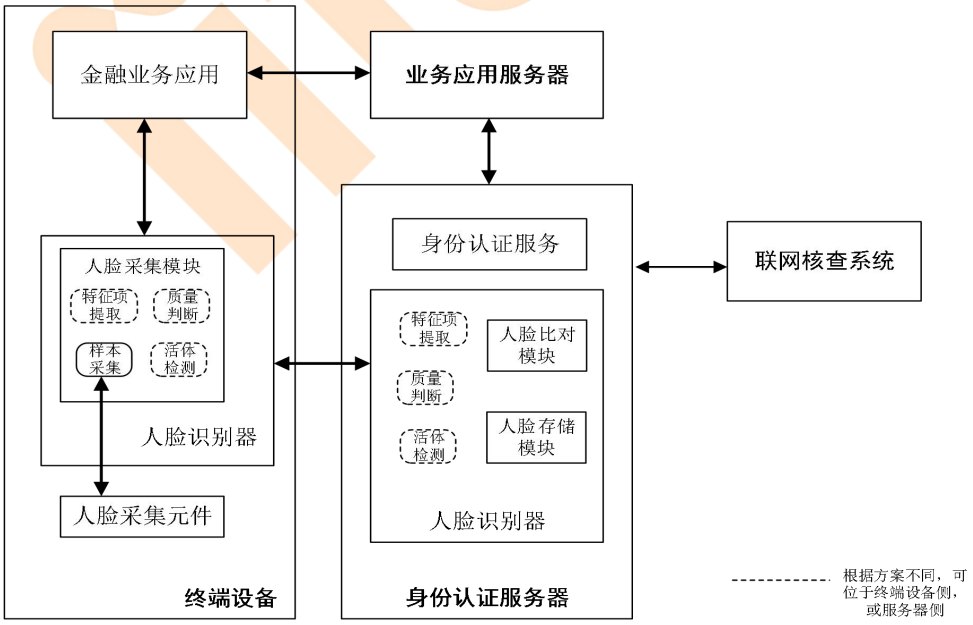

图 1 远程人脸识别金融账户管理应用的总体框架

总体框架如图1所示，详细如下：

终端设备：可提供金融服务的安全可控的移动智能终端（如手机、平板电脑）、自助机具（如远程视频柜员机、智能柜员机）、柜台业务终端等。

金融业务应用：位于终端设备上的独立的金融业务应用程序，或基于浏览器的金融业务网页应用等。通过和金融业务应用服务器的业务交互，实现金融业务场景，通过与金融业务应用服务器和身份认证服务器的交互实现对用户的身份认证。

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。

业务应用服务器：主要负责提供金融业务应用的后台服务，根据用户的身份认证结果提供相应权限的服务或资源。

身份认证服务器：主要对身份认证协议进行解析并验证，以及对身份认证注册关系的管理。在远程模式中，部分人脸识别器的功能模块也在身份认证服务器实现。

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) 用户在安全可控的终端设备中通过金融业务应用向业务应用服务器发起注册请求；
b) 对用户进行的身份信息进行人证比对或联网核查等身份核验，业务应用服务器和身份认证服务器判断是否允许注册请求，并返回给金融业务应用；
c) 金融业务应用直接或间接调用终端设备中的人脸采集模块采集用户人脸样本；
d) 终端设备或身份认证服务器中相关子模块进行质量判断、活体检测、用户人脸特征项提取，生成可更新人脸参考；如有人脸采集失败等异常情况，金融业务应用告知用户并重新进行人脸样本采集；
e) 身份认证服务器将可更新人脸参考存储在人脸存储模块中，并和用户身份标识关联起来；
f) 身份认证服务器经业务应用服务器返回结果至金融业务应用；
g) 结束注册流程。

5.3.2 远程人脸验证

远程人脸验证过程包括但不限于以下步骤：

a) 用户在终端设备侧访问金融业务应用， 金融业务应用转发访问请求至业务应用服务器；
b) 业务应用服务器识别出需要进行身份认证，向金融业务应用发送验证请求；
c) 金融业务应用直接或间接调用终端设备中的人脸采集模块采集用户人脸样本；
d) 终端设备或身份认证服务器中相关子模块进行质量判断、活体检测、用户人脸特征项提取，形成人脸探针；
e) 身份认证服务器中，人脸比对模块将人脸探针与存储在人脸存储模块中的一个或多个可更新人脸参考进行比对，进行决策得到识别结果，并返回身份认证识别结果至业务应用服务器；

f） 业务应用服务器根据识别结果进行后续操作处理， 如允许用户访问相应权限的资源和服务，或要求用户通过其他方式进行身份认证等。

5.3.3 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金融业务应用或系统主动向业务应用服务器发起变更请求；
b） 业务应用服务器和身份认证服务器识别出对应的身份认证注册关系并进行身份验证，判断是否进行此次变更请求；
c） 金融业务应用直接或间接调用终端设备中的人脸采集模块采集新的用户人脸样本；
d） 终端设备或身份认证服务器中相关子模块进行质量判断、活体检测、用户人脸特征项提取，生成新的可更新人脸参考；
e） 身份认证服务器中的人脸存储模块完成该用户可更新人脸参考的更新，并返回结果给业务应用服务器和金融业务应用；
f） 结束变更流程。

5.3.4 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金融业务应用向业务应用服务器发起注销请求；
b） 业务应用服务器和身份认证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，并返回给业务应用服务器和金融业务应用；
d） 结束注销流程。

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） 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。
c） 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。
d） 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。
e） 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。
f） 如采集过程中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、三维假体攻击、AI攻击等。

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、人民银行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生成可更新人脸参考。
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。
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。
e） 宜具备多个渠道接入（柜面、自助机具、电子渠道）进行人脸比对验证能力，能针对不同渠道类型设置不同人脸比对阈值。

6.4 金融业务应用

金融业务应用提供以下功能，包括但不限于：
a） 应能与业务应用服务器进行交互实现金融业务。
b） 应能基于身份认证协议与业务应用服务器和身份认证服务器进行交互，实现注册、验证、变更、注销等业务流程。
c） 应能直接调用相应的人脸识别器实现对用户人脸特征的采集。

6.5 业务应用服务器

业务应用服务器应提供以下功能，包括但不限于：
a） 应能与业务应用进行交互实现金融业务功能。
b） 应能基于身份认证协议与金融业务应用和身份认证服务器进行交互，实现注册、验证、变更、注销等业务流程。
c） 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。
d） 宜具备支持跨通道人脸认证能力，如PC端、自助机具、柜面等发生业务交互时候，可推送至移动终端进行跨通道实现人脸识别与授权。

6.6 身份认证服务器

身份认证服务器应提供以下功能，包括但不限于：
a） 应能基于身份认证协议与业务应用服务器进行交互，实现注册、验证、变更、注销等业务流程。
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人脸比对模块。
d) 应能与公安机关、人民银行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) 应具备多因素组合认证能力（如：用户名口令+人脸、数字证书+人脸等），可基于不同风险级别采用不同认证链流程。
f) 应具备应用人脸业务调用的接口模块，包括人脸注册更新接口、人脸比对接口、人证合一比对接口、人脸搜索接口、人脸回溯查询接口。
g) 应对外提供安全认证协议，保证认证信息的安全传输。
h) 应具备将人脸特征信息进行加密存储及传输的能力，保障人脸特征值存储及认证传输过程的安全性。
i) 应具备人脸识别历史记录查询能力，并可形成分析报表。

7 性能要求

7.1 基本性能要求

对于当错误接受率FAR≤0.001%时，错误拒绝率FRR≤2%。

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 人脸采集元件性能要求

人脸采集元件应满足以下性能要求，包括但不限于：
a) 人脸采集元件在终端设备侧宜以操作系统标准外设的形式存在。

b) 应能够将数字图像信息进行如白平衡、色彩校正、编解码等信息处理。
c) 数据接口应支持MIPI-CS2或者USB接口，控制接口应支持SPI I2C、SPI等接口，应能输出相机数据。
d) 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。
e) 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。
f) 宜有良好的软件兼容性，支持双目深度图像计算，支持OpenNI 、UVC，支持调用API接口升级固件等。
g) 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，RGB和Depth做同步时帧差宜小于1帧。
h) 采集的深度图像分辨率不低于640*400，最大帧率不低于10帧/秒，深度数据的精度不大于3mm（采集物体位于采集单元前50cm处），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%。

8 安全要求

8.1 系统安全

8.1.1 安全物理环境

业务应用服务器、身份认证服务器等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

业务应用服务器、身份认证服务器等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 服务器安全计算环境

业务应用服务器和身份认证服务器的安全计算环境要求包括但不限于：

a) 应符合GB/T 22239-2019 中8.1.4的要求。
b) 业务应用服务器和身份认证服务器接口在被调用时，应对调用方的身份进行确认。
c) 宜具备基于环境感知、风险的动态变化判断是否启用人脸识别（如发现用户异地访问、非正常时间段访问，即使第三方应用程序、未配置人脸识别也可强制要求用户作人脸比对验证）。
d) 宜具备对人脸比对场景进行实时分析判断（异地访问、非常用设备访问、人脸比对错误频率、非常用IP）能力，同时支持黑名单设置（IP过滤、访问时间、访问地点、异常设备、MAC地址）能力，智能提升身份认证安全防护能力。
e) 宜定期对业务应用服务器和身份认证服务器进行第三方安全评测。

8.1.5 终端安全计算环境

终端设备的安全计算环境要求包括但不限于：

a) 针对金融机构提供的自助机具、柜台业务终端等专用终端设备，其承载的操作系统、金融业务应用和数据，应符合GB/T 22239-2019中7.1.4的安全要求。
b) 移动智能终端等承载的金融业务应用和数据，应符合GB/T 22239-2019中7.1.4的安全要求。

8.2 人脸信息安全

8.2.1 概述

在金融账户管理应用中，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，属于C3类别金融个人信息，应符合JR/T 0171-2020中对C3类别信息的要求和GB/T 35237-2020中对个人敏感信息的要求

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) 不应委托或授权无金融业相关资质和机构收集人脸信息。
b) 人脸注册采集人脸信息前，应采用用户名密码、动态密码等方式验证用户身份。
c) 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。
d) 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。
e) 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。
f) 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。
g) 在采集人脸信息后，应对人脸信息进行加密、去标识化处理或脱敏处理，以确保对外不可用。
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) 人脸信息传输前，服务器和终端设备双方应通过有效技术手段进行身份鉴别和认证。
b) 应采用加密通道或数据加密的方式进行传输，保证人脸信息传输时的完整性和保密性。
c) 应采取有效措施保证数据传输可靠性和网络传输服务可用性。
d) 服务器上的人脸识别接口仅限于内部调用，应做好管控。

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) 终端设备上的金融业务应用不应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，保障存储的人脸信息与用户身份信息的对应关系不被篡改。
f) 应采取必要技术和管控措施保证人脸信息存储转移过程中的安全性。

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。
e) 人脸信息的共享和转让、公开披露、委托处理、加工处理、汇聚融合等应满足JR/T 0171-2020中6.1.4的要求；
f) 人脸信息比对后，应确保比对结果输出的数据安全性和完整性。
g) 人脸信息删除后，应确保不可被检索、访问。

附 录 A
（资料性附录）
金融账户管理典型场景应用建议

对典型金融账户管理场景，以下列举人脸识别应用建议：

表 A.1 金融账户管理典型场景应用建议

应用场景	人脸识别应用建议
核保核赔	核保时使用远程人脸识别，由第三方专业机构检验人证合一有效性； 核赔时使用远程人脸识别，可由金融机构直接进行身份认证
消费金融申请	远程人脸识别，由第三方专业机构检验人证合一有效性
业务签约 （包括电子银行签约、快捷支付签约、理财基金签约、代收代付签约、保函审批等）	业务负责人使用本地认证方式； 客户远程人脸识别，由第三方专业机构检验人证合一有效性
银行卡业务 （包括银行卡开户、银行卡解挂、补换卡、密码重置等）	远程人脸识别，由金融机构直接进行身份认证
信用卡申领	申请时使用远程人脸识别，由第三方专业机构检验人证合一有效性； 领取时使用远程人脸识别，可由金融机构直接进行身份认证
网银/APP 登录	本地人脸识别
金融账户远程开户（不含Ⅰ类银行账户）	远程人脸识别，由第三方专业机构检验人证合一有效性
账户解锁	远程人脸识别结合动态验证码

附 录 B
（资料性附录）
金融账户管理典型应用场景流程

B.1 远程开户场景

远程开户是指金融机构在遵守金融监管机构对于开户管理要求的情况下，通过互联网方式远程对客户身份进行确认，并在完成客户身份信息核实后，为客户开立金融账户的行为。

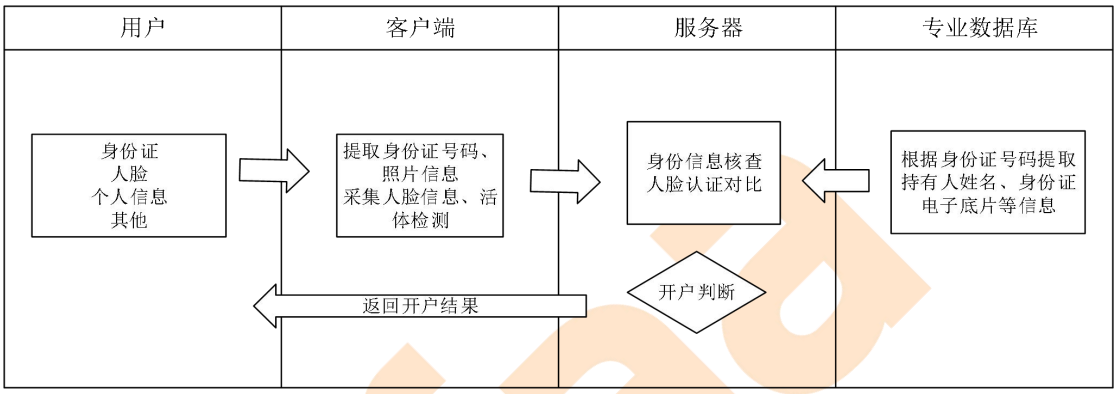

图 B.1 一种远程开户场景流程图

基于远程人脸识别的一种远程开户场景流程主要步骤包括：

a) 用户在客户端中发起开户请求，人工输入相关申请信息；
b) 用户在客户端中拍照扫描二代身份证或者上传二代身份证的正反面照片，客户端快速提取身份证信息和图片；
c) 用户用终端摄像头拍摄人脸图像，客户端进行活体检测、质量判断、采集人脸信息；
d) 服务器根据身份证号码，从公安部或人民银行的数据库调取对应的公民身份信息和二代身份证电子底片；
e) 服务器将专业数据库中的信息与用户提交信息进行核对；
f) 服务器将专业数据库中获取的二代身份证电子底片与现场采集的人脸图像进行认证比对；
g) 服务器进行身份认证和开户判断后，向客户端/用户反馈开户结果。

B.2 互联网账户绑卡

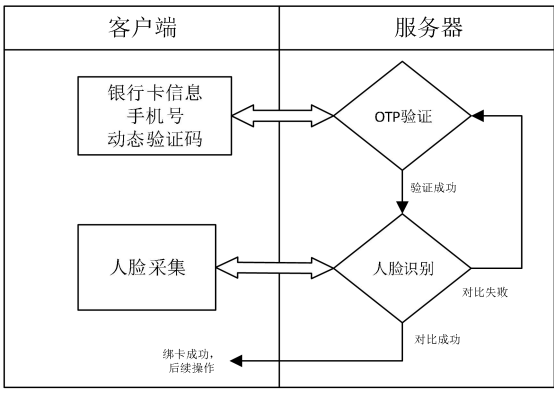

图 B.2 一种互联网账户绑卡场景流程图

基于远程人脸识别的互联网账户绑定第二张银行卡流程如下：

a) 用户在移动应用中进入绑卡界面；

b) 用户输入银行卡号，或移动应用利用OCR识别出银行卡号；

c) 用户输入预留手机号，获取动态密码，进行OTP验证；

d) OTP验证通过后，进行远程人脸识别，移动终端采集人脸信息；

服务器将拍照获取的人脸照片与注册的身份证照片进行比对，如比对通过，则进行后续业务；如比对失败，则返回重新进行 OTP 验证。

B.3 刷脸核身

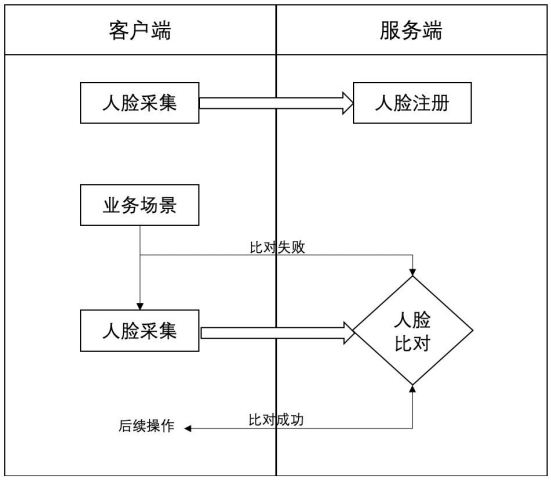

图 B.3 一种互联网刷脸核身场景流程图

基于远程人脸识别的互联网账户刷脸流程如下：

a) 用户在移动应用中采集人脸数据，并存储在服务端，作为人脸的比对源；

b) 当一个业务场景需要核实用户的身份，则用户需要再次采集人脸数据；

c) 系统将获取到的人脸数据与用户原有的比对源数据进行人脸比对，如比对通过则进行后续操作，如果比对失败，用户需要进行重试。