ICS 35.240.15
L 71

中华人民共和国国家标准

GB/T 37036.2—2019

信息技术　移动设备生物特征识别 第2部分：指纹

Information technology—Biometrics used with mobile devices—Part 2：Fingerprint

2019-10-18 发布　　2020-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 37036《信息技术　移动设备生物特征识别》分为以下4个部分：

——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。

本部分为GB/T 37036的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：长春鸿达光电子与生物统计识别技术有限公司、上海天臣射频技术有限公司、中国电子技术标准化研究院、山西天地科技有限公司、小米通讯技术有限公司、芬普信息科技(上海)有限公司、浙江蚂蚁小微金融服务集团股份有限公司、杭州海康威视数字技术股份有限公司、北京集创北方科技股份有限公司、维沃移动通信有限公司、北京中科虹霸科技有限公司、深圳市亚略特生物识别科技有限公司、深圳市汇顶科技股份有限公司、广州广电运通金融电子股份有限公司、北京曙光易通技术有限公司、OPPO广东移动通信有限公司、北京眼神科技有限公司、中国平安保险(集团)股份有限公司、杭州晟元数据安全技术股份有限公司、西安凯虹电子科技有限公司、山西云时代技术有限公司、北京智慧眼科技股份有限公司、中国信息通信研究院。

本部分主要起草人：佟庆强、高健、秦日臻、王文峰、宋继伟、钟陈、孟凡清、冷霜、朱亚军、胡彬、陈星、赵先林、樊磊、何召锋、邵宇、胡荣英、王江胜、林冠辰、于雪平、郭富豪、宋方方、王衍强、崔新亮、王栋、胥建民、吴斌、傅山、王军、周立雄。

信息技术　移动设备生物特征识别
第2部分：指纹

1　范围

GB/T 37036的本部分给出了应用于移动设备指纹识别系统的技术架构，规定了移动设备指纹识别的业务流程、功能要求、性能要求和安全要求。

本部分适用于移动设备指纹识别系统的设计、生产、集成与应用。

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 26238—2010　信息技术　生物特征识别术语

GB/T 33767.4—2018　信息技术　生物特征样本质量　第4部分：指纹图像数据

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

3　术语和定义

GB/T 26238—2010界定的以及下列术语和定义适用于本文件。

3.1

指纹特征　fingerprint characteristic

可以从个体的指纹信息中提取出的有区别的、可重复的特征信息，从而达到个体识别的目的。

3.2

指纹识别　fingerprint recognition

基于个体的指纹特征，对该个体进行识别的过程。

3.3

指纹采集子系统　fingerprint capture subsystem

收集指纹特征信息并将其转换成指纹采集样本的子系统。

3.4

指纹样本　fingerprint sample

从指纹采集子系统获得的模拟的或数字的指纹特征的表示。

3.5

指纹特征项　fingerprint feature

从指纹样本中提取的，用于比对的数值或标记。

3.6

指纹探针　fingerprint probe

输入到算法的，与指纹参考数据进行比对的指纹数据。

3.7

指纹模板　fingerprint template

参考的或已存储的指纹特征项的集合，可直接与指纹探针样本的指纹特征项进行比对。

3.8

指纹参考　fingerprint reference

用于比对的、属于生物特征数据主体的一个或多个已存储的指纹样本、指纹模板或指纹识别模型等。

3.9

指纹数据　fingerprint data

处于任何处理阶段的指纹样本、指纹参考、指纹特征项或指纹特性。

3.10

指纹登记　fingerprint enrollment

通过一次或多次采集特定已知人的手指指纹图像，抽取其特征并存储的过程。

3.11

识别时间　recognition time

移动设备中完成一次识别过程所需要的时间。

注：识别过程包括图像采集、特征提取和特征比对三个流程。

4　缩略语

下列缩略语适用于本文件。

DPI：每英寸点数(Dots per inch)

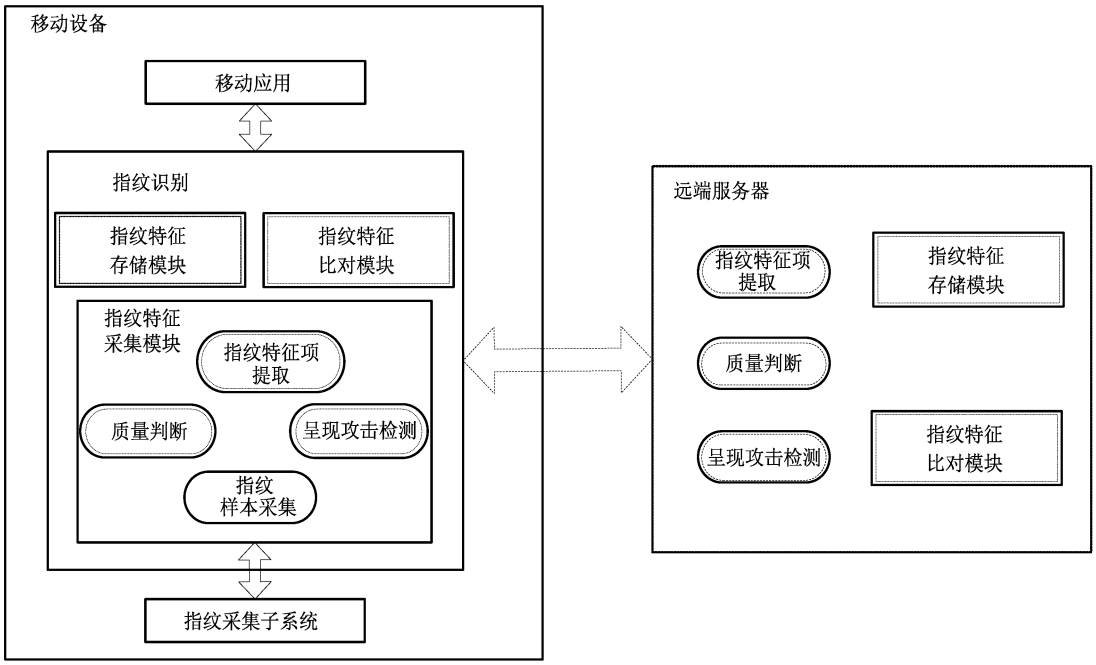
FAR：错误接受率(False acceptance rate)

FRR：错误拒绝率(False rejection rate)

ID：标识符(Identifier)

5　技术架构

本部分给出的移动设备指纹识别技术架构是GB/T 37036.1—2018中描述的通用技术架构在指纹应用领域的具体化，如图1所示。



说明：

——————必须具备的模块；

·····可选具备的模块；

═══必须具备的模块，根据不同方案，或位于移动设备，或位于远端服务器。

图 1　移动设备指纹识别技术架构

图中示出移动设备和远端服务器两大部分。

移动设备包括指纹采集子系统、指纹识别和移动应用三部分。其中，移动应用是移动设备中的指纹识别的服务调用方，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。指纹采集子系统提供现场指纹采集功能。

本部分是对移动设备中的指纹识别和远端服务器进行规定。

指纹识别过程由指纹特征采集模块、指纹特征存储模块和指纹特征比对模块提供的功能予以支持。

指纹特征采集模块的主要作用是通过访问移动设备中的指纹采集子系统采集指纹样本，再进行质量判断、呈现攻击检测和指纹特征项提取。该模块由指纹样本采集、质量判断、呈现攻击检测、指纹特征项提取四个子功能实现，各子功能的作用如下：

a）　指纹样本采集子功能的主要作用是通过访问移动设备中的指纹采集子系统采集指纹样本；

b）　质量判断子功能的主要作用是针对指纹样本进行评估、判断，确认样本数据是否满足质量要求；

c）　呈现攻击检测子功能的主要作用是针对指纹样本进行评判，将非指纹类样本进行屏蔽；

d）　指纹特征项提取子功能的主要作用是针对通过质量判断、呈现攻击检测后的指纹样本进行指纹特征项提取。

指纹特征存储模块的主要作用是将通过指纹特征采集模块验证后的指纹特征形成指纹模板存储在物理芯片上。

指纹特征比对模块的主要作用是将指纹特征采集模块验证后的指纹特征项与指纹特征存储模块的指纹模板进行比对，并将比对结果输出到移动应用。

服务器端包括指纹特征存储模块、指纹特征比对模块以及指纹特征采集模块中的质量判断、呈现攻击检测和指纹特征项提取三个子功能。这些功能和子功能的作用与移动设备端的对应功能和子功能的

作用相同。

移动设备生物特征识别的应用可能有多种模式，主要包括本地识别和远程识别两种模式。

本地识别模式是指，移动设备指纹特征识别过程全部在移动设备本地完成，并向调用指纹识别服务的移动应用输出识别结果。

远程识别模式是指，指纹识别的部分功能（如，指纹特征存储和/或指纹特征比对功能）或子功能（如，质量判断、呈现攻击检测、和/或指纹特征项提取子功能）在远端服务器执行。

一般采用本地识别模式。具体采用何种识别模式，取决于移动设备生物特征识别系统的应用目的和应用环境以及总体设计考虑，在识别系统解决方案中设定。

本地识别和远程识别模式的描述参见附录 A。

6 业务流程

移动设备指纹识别的业务流程一般包括登记过程、识别过程和注销过程。要求如下：

a) 登记过程应包括以下步骤（但不限于）：
   1) 接受指纹识别的人（以下简称用户）在移动设备上启动登记过程；
   2) 用户通过身份验证和权限检查后，移动设备上的指纹采集子系统采集用户指纹样本，通过质量判断进一步提取用户指纹特征项；
   3) 将该用户指纹特征项存储在指纹特征存储模块中作为该用户的指纹特征模板，并与用户身份标识关联起来；
   4) 为每个登记的指纹模板分配一个唯一的 ID；
   5) 结束指纹登记。
b) 识别过程应包括以下步骤（但不限于）：
   1) 用户在移动设备上启动识别过程；
   2) 移动设备上的指纹采集子系统采集用户指纹样本，通过质量判断和呈现攻击检测后进一步提取用户指纹特征项；
   3) 将提取的用户指纹特征项与存储在指纹特征存储模块中的一个或多个用户指纹特征模板进行比对；
   4) 根据比对结果进行识别决策并将识别结果输出给移动应用；
   5) 结束指纹识别。
c) 注销过程应包括以下步骤（但不限于）：
   1) 用户在移动设备上启动指纹注销过程；
   2) 在移动设备上的指纹特征存储模块中删除与待注销用户关联的指纹特征模板；
   3) 结束指纹注销。

7 功能要求

7.1 一般要求

7.1.1 基本功能

应符合 GB/T 37036.1—2018 的 6.1.1 的要求，包括但不限于：

a) 适用于不同人种、不同年龄、不同肤色的用户；
b) 适用于移动设备用户和指纹识别系统管理员；
c) 基于相应的移动设备软硬件条件，能支持多模态或多因子的指纹识别。

7.1.2 功能管理

应符合 GB/T 37036.1—2018 的 6.1.2 的要求，包括但不限于：

a) 指纹登记：
   1) 应能在一次会话内完成指纹登记；
   2) 应能支持超时时间约束。
b) 指纹识别：
   1) 应能支持连续失败次数约束；
   2) 应能输出指纹识别结果。
c) 指纹注销时，注销对象应经过身份验证。
d) 应支持日志管理功能，产生日志记录事件。所要记录的事件包括(但不限于)登记过程和识别过程中的成功或失败事件。每一个事件的日志记录宜包括事件发生时间、事件类型、用户、事件执行结果或失败原因等。

7.2 指纹特征采集模块

7.2.1 基本功能

应符合 GB/T 37036.1—2018 的 6.2.1 的要求，包括但不限于：

a) 应具备手指检测功能，在进行指纹样本采集前应检测手指是否触摸指纹特征采集元件；
b) 应能使用移动设备指纹特征采集模块采集用户指纹样本，并将其转化成适合指纹识别处理的数据格式；
c) 应具备异常情况判定及处理能力，如指纹样本采集失败、指纹样本未通过质量判断、检测到呈现攻击、指纹特征项提取失败等的相应处理机制。

7.2.2 质量判断

应符合 GB/T 37036.1—2018 的 6.2.2 的要求，包括但不限于：

a) 确保不产生完全没有指纹信息的空图；
b) 指纹图像质量判断结果和质量分数满足 GB/T 33767.4—2018 的规定。

7.2.3 呈现攻击检测

应符合 GB/T 37036.1—2018 的 6.2.3 的要求，包括但不限于：

a) 应能对当前被采集的用户指纹样本进行呈现攻击检测，以防止恶意伪造；
b) 检测出呈现攻击时应具备相应的处理机制，如失败/错误提示或进行风险提示等。

注：关于呈现攻击检测的其他要求参考 ISO/IEC 30107 的相关规定。

7.2.4 数据交换格式

基于 GB/T 37036.1—2018 中 6.2.4 的相关规定，对成功采集的用户指纹特征数据，应在扩展项中包括事件的标识符、唯一的设备标识符、采集日期和时间、指纹样本的描述等数据。

7.3 指纹特征存储模块

应符合 GB/T 37036.1—2018 的 6.3 的要求，包括但不限于：

a) 存储的数据不包含指纹原始图像数据；
b) 支持已登记的用户对于指纹特征存储模块中的指纹模板进行增加、注销等操作；

c) 对存储的指纹特征数据进行加密；
d) 凡涉及采用密码技术提供安全(保密性、完整性、真实性、不可否认性)时，遵循密码相关国家标准和行业标准。

7.4 指纹特征比对模块

7.4.1 基本功能

基于 GB/T 37036.1—2018 中 6.4.1 的相关规定，指纹特征比对模块应能支持 1∶N 比对(其中 N 是模板数，取值范围是 1～99 的整数)。

7.4.2 比对判定及处理

应符合 GB/T 37036.1—2018 的 6.4.2 的要求，包括但不限于：
a) 能够将输入的用户指纹特征项和已登记的指纹特征模板进行比对，计算出比对得分；
b) 能根据比对得分进行识别结果判定，并能够输出识别结果；
c) 能执行异常情况判定及处理功能，包括但不限于定义连续错误次数及恢复方式。

8 性能要求

8.1 分辨率

应不小于 300DPI。

8.2 采集时间

从开始发送指纹采集指令到指纹样本数据接收完成的过程，应不超过 250 ms。

8.3 识别时间

应不超过 2 s。

8.4 错误接受率和错误拒绝率

错误接受率和错误拒绝率应符合下列规定：
a) 在 FAR 不大于 0.1%时，FRR 应不大于 5%；
b) 在 FAR 不大于 0.01%时，FRR 应不大于 15%。

9 安全要求

9.1 一般要求

应符合 GB/T 37036.1—2018 的 7.1 的要求，包括但不限于：
a) 应具备有效的安全机制，确保当前操作人员拥有合法权限完成用户登记、更新和注销；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；
b) 若指纹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) 在运行时宜具备运行环境的检查能力，检查范围可包括移动设备系统是否被非法用户获取管理员权限、程序运行环境是否可信等，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) 应采取安全加固措施提升自身安全防护水平；
e) 应采取安全措施确保日志安全；
f) 应采取安全措施确保远程传输模式中的数据安全。

9.2 指纹特征采集模块安全

应符合 GB/T 37036.1—2018 的 7.2 的要求，包括但不限于：

a) 宜设置指纹特征采集超时处理机制，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指纹样本时，模块自动退出运行；
b) 应保护用户输入的敏感数据或采集到的用户指纹数据；
c) 指纹特征采集模块应通过可信环境进行安全保护；
d) 在远程识别模式下，宜在可信环境中存储所涉及的密钥，如与远端服务器之间进行安全通信时所涉及的密钥。

9.3 指纹特征存储模块安全

应符合 GB/T 37036.1—2018 的 7.3 的要求，包括但不限于：

a) 应结合可信环境采取有效的安全方式对存储在指纹特征存储模块中的指纹模板进行安全保护；
b) 在远程识别模式下，应对用户指纹参考进行去标记操作或脱敏处理，并应与用户身份标识信息分库保存。

9.4 指纹特征比对模块安全

应符合 GB/T 37036.1—2018 的 7.4 的要求，包括但不限于：

a) 指纹特征比对模块一般是以软件的形式实现，采取有效的安全措施确保该模块的安全性，并采取有效的安全措施确保比对过程中所使用的用户指纹数据以及识别决策结果的保密性和完整性，不被窃取或篡改；
b) 结合移动设备所具有的可信执行环境或安全单元实现指纹特征比对模块；
c) 在远程识别模式下，结合可信环境增强指纹特征比对模块的安全性，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。

9.5 日志安全

日志安全要求包括但不限于：

a) 日志记录中不应出现明文的指纹数据、秘钥信息或其他安全相关的参数等；
b) 应采取安全措施对日志信息做完整性保护，如数字签名等；
c) 应具备授权管理机制，对日志记录的增加、删除、修改的操作权限进行管理。

9.6 安全环境

应遵循 GB/T 37036.1—2018 中 7.5 的相关规定。

附 录 A
（资料性附录）
移动设备指纹识别应用模式

A.1 模式一 本地识别模式

图 A.1 描述了典型模式一。在该种模式下，指纹特征采集、存储和比对模块都位于移动设备中，出于安全性考虑，指纹识别系统的各模块由移动设备中可信执行环境进行保护。指纹采集子系统仅允许由富执行环境和可信执行环境共享访问，或仅允许由可信执行环境访问。

移动应用一般位于富执行环境，通过可信执行环境提供的对外接口调用指纹识别系统，指纹识别系统调用位于移动设备中的指纹采集子系统采集指纹样本：

a) 在进行质量判断后提取指纹特征，进行指纹登记过程，完成后向调用指纹识别的移动应用反馈结果；

b) 在进行质量判断、呈现攻击检测后提取指纹特征，进行指纹识别过程，完成后向调用指纹识别的移动应用反馈结果。

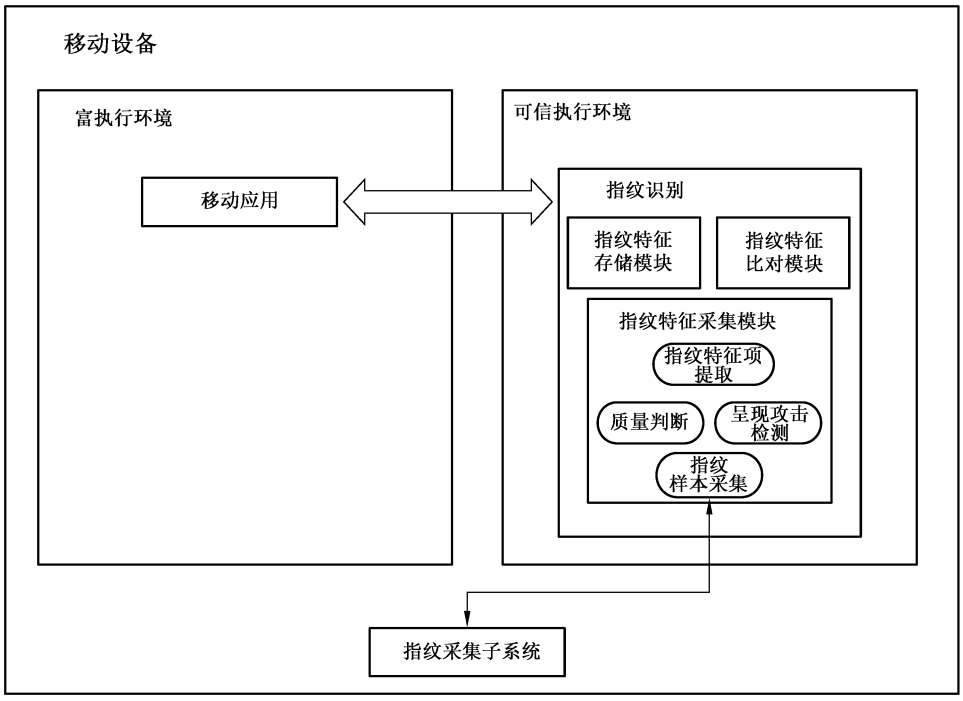


图 A.1 模式一 本地识别模式

A.2 模式二 远程识别模式

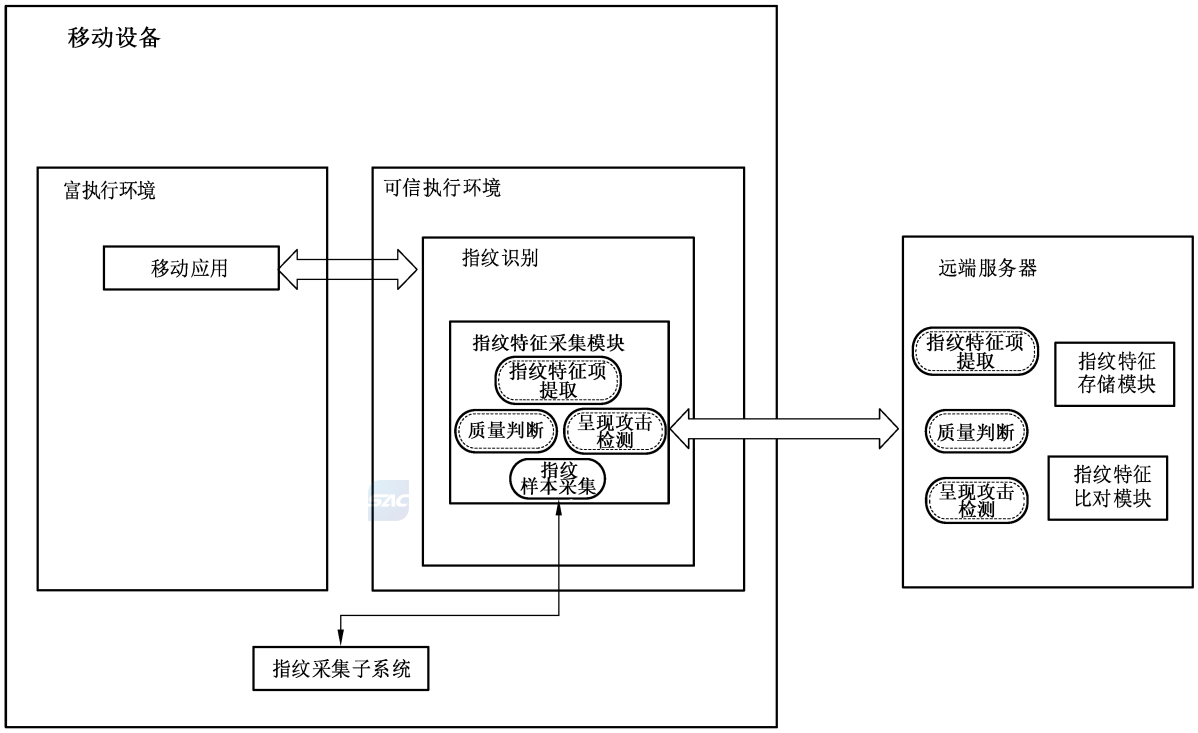
图 A.2 描述了典型模式二。在该种模式下，指纹特征采集模块中指纹样本采集功能在移动设备中完成，质量判断、呈现攻击检测和指纹特征项提取在移动设备或远端服务器中完成，指纹特征存储模块和指纹特征比对模块位于远端服务器。出于安全性增强考虑，位于移动设备中的指纹特征采集模块在可信执行环境中实现。指纹采集子系统允许由富执行环境和可信执行环境共享访问，或仅允许由可信

执行环境访问。

移动应用一般位于富执行环境，通过可信执行环境提供的对外接口调用指纹识别系统，指纹识别系统调用位于移动设备中的指纹采集子系统采集指纹样本：

a) 在进行质量判断后提取指纹特征，在远端服务器进行指纹登记过程，完成后向调用指纹识别的移动应用反馈结果；

b) 在进行质量判断、呈现攻击检测后提取指纹特征，在远端服务器进行指纹识别过程，完成后向调用指纹识别的移动应用反馈结果。



说明：

——————必须具备的模块；

▬▬▬▬▬必须具备的模块，根据不同方案或位于移动设备或位于远端服务器。

图 A.2　模式二　远程识别模式

参 考 文 献

[1] ISO/IEC 30107 Information technology—Biometric presentation attack detection