(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107786341 B
(45)授权公告日 2019.11.29

(21)申请号 201710941771.4

(22)申请日 2017.10.11

(65)同一申请的已公布的文献号
申请公布号 CN 107786341 A

(43)申请公布日 2018.03.09

(73)专利权人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 王健

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04L 9/32(2006.01)
H04M 1/67(2006.01)
H04M 1/725(2006.01)
G06K 9/00(2006.01)
G06F 21/32(2013.01)

(56)对比文件
CN 103164710 A,2013.06.19,全文.
CN 104376270 A,2015.02.25,全文.
CN 102035849 A,2011.04.27,全文.
US 2015147045 A1,2015.05.28,全文.
US 2003154406 A1,2003.08.14,全文.

审查员 王亭

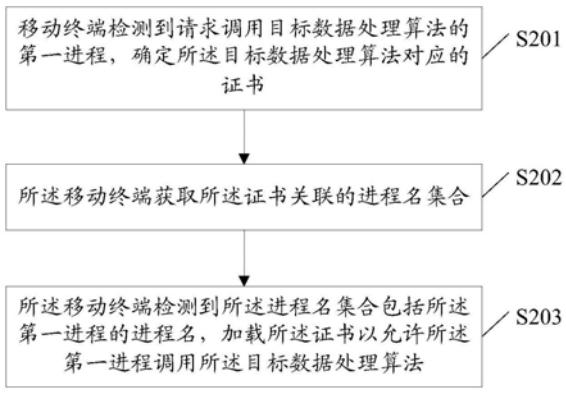
权利要求书2页 说明书11页 附图5页

(54)发明名称

证书加载方法及移动终端和计算机可读存储介质

(57)摘要

本申请实施例公开了一种证书加载方法及相关产品，包括：检测到请求调用目标数据处理算法的第一进程，确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；获取证书关联的进程名集合；检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。本申请实施例有利于提升移动终端进行人脸识别的安全性。



CN 107786341 B

1.一种移动终端,其特征在于,包括处理器,连接所述处理器的人脸图像采集装置和存储器,其中:

所述人脸图像采集装置,用于采集人脸图像;

所述存储器,用于存储目标数据处理算法和所述目标数据处理算法对应的证书;

所述处理器,用于导入面部识别应用程序关联的多个数据处理算法对应的多个证书;以及确定每个证书关联的进程名集合;检测到请求调用目标数据处理算法的第一进程,确定导入的所述多个证书中的所述目标数据处理算法对应的证书,所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法;以及获取所述证书关联的进程名集合;以及检测到所述进程名集合包括所述第一进程的进程名,加载所述证书以允许所述第一进程调用所述目标数据处理算法。

2.根据权利要求1所述的移动终端,其特征在于,在所述加载所述证书以允许所述第一进程调用所述目标数据处理算法方面,所述处理器具体用于:调用所述证书解析处于加密状态的所述目标数据处理算法;以及通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据,所述第一进程关联的参考数据是摄像头采集的当前用户的人脸图像数据或者人脸图数据中的人脸特征数据。

3.根据权利要求1所述的移动终端,其特征在于,所述处理器在检测到请求调用目标数据处理算法的第一进程之前,还用于:检测到所述面部识别应用程序的启用指令,验证所述面部识别应用程序的签名证书和导入证书为同个证书;以及启用所述面部识别应用程序。

4.根据权利要求2所述的移动终端,其特征在于,所述处理器在检测到请求调用目标数据处理算法的第一进程之前,还用于:检测到所述面部识别应用程序的启用指令,验证所述面部识别应用程序的签名证书和导入证书为同个证书;以及启用所述面部识别应用程序。

5.根据权利要求1-4任一项所述的移动终端,其特征在于,在导入面部识别应用程序关联的多个数据处理算法对应的多个证书;以及确定每个证书关联的进程名集合的方面,所述处理器具体用于:在检测到所述移动终端的开机事件的情况下,导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书;以及确定每个证书关联的进程名集合。

6.根据权利要求5所述的移动终端,其特征在于,在所述确定每个证书关联的进程名集合方面,所述处理器具体用于:根据当前用户录入的进程名确定所述每个证书关联的进程名集合;或者,查询预设的证书与进程名集合之间的映射关系,确定所述每个证书关联的进程名集合。

7.一种证书加载方法,其特征在于,包括:导入面部识别应用程序关联的多个数据处理算法对应的多个证书,确定每个证书关联的进程名集合;

检测到请求调用目标数据处理算法的第一进程,确定导入的所述多个证书的所述目标数据处理算法对应的证书,所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法;

获取所述证书关联的进程名集合;

检测到所述进程名集合包括所述第一进程的进程名,加载所述证书以允许所述第一进程调用所述目标数据处理算法。

8.根据权利要求7所述的方法,其特征在于,所述加载所述证书以允许所述第一进程调用所述目标数据处理算法,包括:

调用所述证书解析处于加密状态的所述目标数据处理算法；

通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据，所述第一进程关联的参考数据是摄像头采集的当前用户的人脸图像数据或者人脸图数据中的人脸特征数据。

9.根据权利要求7所述的方法，其特征在于，所述检测到请求调用目标数据处理算法的第一进程之前，所述方法还包括：

检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书；

启用所述面部识别应用程序。

10.根据权利要求8所述的方法，其特征在于，所述检测到请求调用目标数据处理算法的第一进程之前，所述方法还包括：

检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书；

启用所述面部识别应用程序。

11.根据权利要求7-10任一项所述的方法，其特征在于，所述导入面部识别应用程序关联的多个数据处理算法对应的多个证书，确定每个证书关联的进程名集合，包括：

在检测到移动终端的开机事件的情况下，导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书；确定每个证书关联的进程名集合。

12.根据权利要求11所述的方法，其特征在于，所述确定每个证书关联的进程名集合，包括：

根据当前用户录入的进程名确定所述每个证书关联的进程名集合；或者，

查询预设的证书与进程名集合之间的映射关系，确定所述每个证书关联的进程名集合。

13.一种移动终端，其特征在于，包括导入单元、确定单元、获取单元和加载单元，其中，

所述导入单元，用于导入面部识别应用程序关联的多个数据处理算法对应的多个证书；所述确定单元，用于确定每个证书关联的进程名集合，检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；

所述获取单元，用于获取所述证书关联的进程名集合；

所述加载单元，用于检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

14.一种移动终端，其特征在于，包括处理器、存储器、通信接口，以及一个或多个程序，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行如权利要求7-12任一项所述的方法中的步骤的指令。

15.一种计算机可读存储介质，其特征在于，存储用于电子数据交换的计算机程序，其中，所述计算机程序被计算机执行，以实现如权利要求7-12任一项所述的方法，所述计算机包括移动终端。

证书加载方法及移动终端和计算机可读存储介质

技术领域

[0001] 本申请涉及移动终端技术领域，具体涉及一种证书加载方法及移动终端和计算机可读存储介质。

背景技术

[0002] 随着智能手机的大量普及应用，智能手机能够支持的应用越来越多，功能越来越强大，智能手机向着多样化、个性化的方向发展，成为用户生活中不可缺少的电子用品。

[0003] 目前，随着智能手机越来越高的安全性需求，多种生物信息解锁方案应运而生，例如指纹解锁，人脸解锁，虹膜解锁等，其中，由于人脸解锁的解锁速度较快，识别成功率较高，使其成为众多智能手机的首要选择。

发明内容

[0004] 本申请实施例提供了一种证书加载方法及相关产品，以期提升移动终端的人脸识别的安全性。

[0005] 第一方面，本申请实施例提供一种移动终端，包括处理器，连接所述处理器的人脸图像采集装置和存储器，其中：

[0006] 所述人脸图像采集装置，用于采集人脸图像，所述人脸图像用于提取面部特征数据；

[0007] 所述存储器，用于存储目标数据处理算法和所述目标数据处理算法对应的证书；

[0008] 所述处理器，用于检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；以及获取所述证书关联的进程名集合；以及检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0009] 第二方面，本申请实施例提供一种证书加载方法，包括：

[0010] 检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；

[0011] 获取所述证书关联的进程名集合；

[0012] 检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0013] 第三方面，本申请实施例提供一种移动终端，包括确定单元、获取单元和加载单元，其中，

[0014] 所述确定单元，用于检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；

[0015] 所述获取单元，用于获取所述证书关联的进程名集合；

[0016] 所述加载单元，用于检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0017] 第四方面，本申请实施例提供一种移动终端，包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行本申请实施例第二方面任一方法中的步骤的指令。

[0018] 第五方面，本申请实施例提供了一种计算机可读存储介质，其中，所述计算机可读存储介质存储用于电子数据交换的计算机程序，其中，所述计算机程序使得计算机执行如本申请实施例第二方面任一方法中所描述的部分或全部步骤，所述计算机包括移动终端。

[0019] 第六方面，本申请实施例提供了一种计算机程序产品，其中，所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，所述计算机程序可操作来使计算机执行如本申请实施例第二方面任一方法中所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包，所述计算机包括移动终端。

[0020] 可以看出，本申请实施例中，移动终端在检测到请求调用目标数据处理算法的第一进程，首先确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；其次，获取证书关联的进程名集合；最后，检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法，那么这些第三方数据处理算法的安全性就显得尤为重要，故而通过证书鉴权机制以确保调用目标数据处理算法的安全性，能够避免非法进程调用该算法来破解该算法的情况发生，有利于提高移动终端进行人脸识别的安全性。

附图说明

[0021] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0022] 图1是本申请实施例提供的一种移动终端的结构示意图；

[0023] 图2A是本申请实施例公开的一种证书加载方法的流程示意图；

[0024] 图2B是本申请实施例公开的一种安卓系统和安全系统的架构示例图；

[0025] 图3是本申请实施例公开的另一种证书加载方法的流程示意图；

[0026] 图4是本申请实施例公开的另一种证书加载方法的流程示意图；

[0027] 图5是本申请实施例公开的一种移动终端的结构示意图；

[0028] 图6是本申请实施例公开的一种移动终端的功能单元组成框图。

具体实施方式

[0029] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员

在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0030] 本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其他步骤或单元。

[0031] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0032] 本申请实施例所涉及到的移动终端可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其他处理设备，以及各种形式的用户设备(User Equipment，UE)，移动台(Mobile Station，MS)，终端设备(terminal device)等等。为方便描述，上面提到的设备统称为移动终端。

[0033] 本申请实施例所描述的移动终端设置有人脸图像采集装置，人脸图像采集装置可以是通用摄像头模组，如前置摄像头。下面对本申请实施例进行详细介绍。

[0034] 请参阅图1，图1是本申请实施例提供了一种移动终端100的结构示意图，所述移动终端100包括：壳体、触控显示屏、主板、电池和副板，主板上设置有处理器110、存储器120、前置摄像头130和SIM卡槽等，副板上设置有振子、一体音腔、VOOC闪充接口，所述前置摄像头130组成该移动终端100的人脸图像采集装置，所述人脸图像采集装置可以包括摄像头，其中，

[0035] 所述人脸图像采集装置130，用于采集人脸图像；

[0036] 所述存储器120，用于存储目标数据处理算法和所述目标数据处理算法对应的证书；

[0037] 所述处理器110，用于检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；以及获取所述证书关联的进程名集合；以及检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0038] 其中，所述第一进程为移动终端的应用程序的进程，该应用程序包括移动终端安装的第三方应用程序，或者安装的系统应用程序等，如支付类应用、锁屏应用等，此处不做限定。

[0039] 其中，目标数据处理算法至少包括人脸特征数据的提取算法、人脸特征数据的匹配算法等，此处不做唯一限定。

[0040] 其中，证书是指移动终端预存的用于验证目标对象的身份的电子标签或者随机数等，目标对象例如可以是上述目标数据处理算法等。

[0041] 其中，所述证书可以存储在所述安全系统中。所述移动终端调用该证书时，需要从安全系统中提取该证书。

[0042] 其中，处理器110是移动终端的控制中心，利用各种接口和线路连接整个移动终端

的各个部分，通过运行或执行存储在存储器120内的软件程序和/或模块，以及调用存储在存储器120内的数据，执行移动终端的各种功能和处理数据，从而对移动终端进行整体监控。可选的，处理器110可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，所述调制解调处理器也可以不集成到处理器110中。

[0043] 其中，存储器120可用于存储软件程序以及模块，处理器110通过运行存储在存储器120的软件程序以及模块，从而执行移动终端的各种功能应用以及数据处理。存储器120可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序等；存储数据区可存储根据移动终端的使用所创建的数据等。此外，存储器120可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0044] 可以看出，本申请实施例中，移动终端在检测到请求调用目标数据处理算法的第一进程，首先确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；其次，获取证书关联的进程名集合；最后，检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法，那么这些第三方数据处理算法的安全性就显得尤为重要，故而通过证书鉴权机制以确保调用目标数据处理算法的安全性，能够避免非法进程调用该算法来破解该算法的情况发生，有利于提高移动终端进行人脸识别的安全性。

[0045] 在一个可能的示例中，在所述加载所述证书以允许所述第一进程调用所述目标数据处理算法方面，所述处理器110具体用于：调用所述证书解析处于加密状态的所述目标数据处理算法；以及通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0046] 可见，本示例中，移动终端需要基于证书验证机制，在检测到调用目标处理算法的第一进程身份合法的情况下，才允许通过目标数据处理算法处理所述第一进程关联的参考数据，有利于提高移动终端进行人脸识别的安全性。

[0047] 在一个可能的示例中，所述处理器110在检测到请求调用目标数据处理算法的第一进程之前，还用于：检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书；以及启用所述面部识别应用程序。

[0048] 可见，本示例中，签名证书和导入证书的验证机制可以有效防止面部识别应用程序被掉包，有利于提高移动终端进行人脸识别的安全性。

[0049] 在一个可能的示例中，所述处理器110还用于：检测到所述移动终端的开机事件，导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书；以及确定每个证书关联的进程名集合。

[0050] 可见，本示例中，移动终端在开机时既可以同步导入数据处理算法的证书，以及确定每个证书关联的进程名集合，使得后续使用过程中移动终端无需再次导入证书，提高鉴权速度。

[0051] 在一个可能的示例中，在所述确定每个证书关联的进程名集合方面，所述处理器110具体用于：根据当前用户录入的进程名确定所述每个证书关联的进程名集合；或者，查

询预设的证书与进程名集合之间的映射关系，确定所述每个证书关联的进程名集合。

[0052] 可见，本示例中，移动终端提供了灵活的进程集合确定机制，有利于提高进程集合设置的便捷性和灵活性。

[0053] 请参阅图2A，图2A是本申请实施例提供了一种证书加载方法的流程示意图，如图所示，本证书加载方法包括：

[0054] S201，移动终端检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法。

[0055] 其中，所述第一进程为移动终端的应用程序的进程，该应用程序包括移动终端安装的第三方应用程序，或者安装的系统应用程序等，如支付类应用、锁屏应用等，此处不做限定。

[0056] 其中，目标数据处理算法至少包括人脸特征数据的提取算法、人脸特征数据的匹配算法等，此处不做唯一限定。

[0057] 其中，证书是指移动终端预存的用于验证目标对象的身份的电子标签或者随机数等，目标对象例如可以是上述目标数据处理算法等。

[0058] 其中，如图2B所示，移动终端运行有富执行环境(Rich Execution Environment，REE，REE)和可信执行环境(Trust Execution Environment，TEE)，TEE具有其自身的执行空间，也就是说在TEE的环境下也有一个操作系统。TEE环境比Rich OS(普通操作系统)的安全级别更高。TEE所能访问的软硬件资源是与Rich OS分离的。TEE提供了可信应用TA的安全执行环境，同时也保护TA的资源和数据的保密性、完整性和访问权限。为了保证TEE本身的可信根，TEE在安全启动过程中是要通过验证并且与安卓操作系统隔离的。在TEE中，每个TA是相互独立的，而且不能在未授权的情况下互相访问。所述人脸识别TA是所述移动终端的安全系统对应的可信执行环境(Trust Execution Environment，TEE)所支持的应用中的可信应用。

[0059] 其中，所述证书可以存储在所述安全系统中。所述移动终端调用该证书时，需要从安全系统中提取该证书。

[0060] S202，所述移动终端获取所述证书关联的进程名集合。

[0061] S203，所述移动终端检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0062] 可以看出，本申请实施例中，移动终端在检测到请求调用目标数据处理算法的第一进程，首先确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；其次，获取证书关联的进程名集合；最后，检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法，那么这些第三方数据处理算法的安全性就显得尤为重要，故而通过证书鉴权机制以确保调用目标数据处理算法的安全性，能够避免非法进程调用该算法来破解该算法的情况发生，有利于提高移动终端进行人脸识别的安全性。

[0063] 在一个可能的示例中，所述移动终端加载所述证书以允许所述第一进程调用所述目标数据处理算法，包括：所述移动终端调用所述证书解析处于加密状态的所述目标数据

处理算法;以及通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0064] 其中,所述第一进程关联的参考数据例如可以是摄像头采集的当前用户的人脸图像数据,还可以是人脸图数据中的人脸特征数据,此处不做唯一限定。

[0065] 可见,本示例中,移动终端需要基于证书验证机制,在检测到调用目标处理算法的第一进程身份合法的情况下,才允许通过目标数据处理算法处理所述第一进程关联的参考数据,有利于提高移动终端进行人脸识别的安全性。

[0066] 在一个可能的示例中,所述移动终端检测到请求调用目标数据处理算法的第一进程之前,所述方法还包括:所述移动终端检测到所述面部识别应用程序的启用指令,验证所述面部识别应用程序的签名证书和导入证书为同个证书;以及启用所述面部识别应用程序。

[0067] 可见,本示例中,签名证书和导入证书的验证机制可以有效防止面部识别应用程序被掉包,有利于提高移动终端进行人脸识别的安全性。

[0068] 在一个可能的示例中,所述方法还包括:所述移动终端检测到所述移动终端的开机事件,导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书;以及确定每个证书关联的进程名集合。

[0069] 可见,本示例中,移动终端在开机时既可以同步导入数据处理算法的证书,以及确定每个证书关联的进程名集合,使得后续使用过程中移动终端无需再次导入证书,提高鉴权速度。

[0070] 在一个可能的示例中,所述移动终端确定每个证书关联的进程名集合,包括:所述移动终端根据当前用户录入的进程名确定所述每个证书关联的进程名集合;或者,所述移动终端查询预设的证书与进程名集合之间的映射关系,确定所述每个证书关联的进程名集合。

[0071] 其中,预设的证书与进程名集合之间的映射关系可以由服务器下发给移动终端。

[0072] 可见,本示例中,移动终端提供了灵活的进程集合确定机制,有利于提高进程集合设置的便捷性和灵活性。

[0073] 与所述图2A所示的实施例一致的,请参阅图3,图3是本申请实施例提供的一种证书加载方法的流程示意图,应用于移动终端,所述移动终端运行有安卓系统和安全系统,所述安卓系统中运行有人脸识别服务Service,所述安全系统中运行有人脸识别可信应用TA。如图所示,本证书加载方法包括:

[0074] S301,移动终端检测到请求调用目标数据处理算法的第一进程,确定所述目标数据处理算法对应的证书,所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法;

[0075] S302,所述移动终端获取所述证书关联的进程名集合;

[0076] S303,所述移动终端检测到所述进程名集合包括所述第一进程的进程名,调用所述证书解析处于加密状态的所述目标数据处理算法;

[0077] S304,所述移动终端通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0078] 可以看出,本申请实施例中,移动终端在检测到请求调用目标数据处理算法的第一进程,首先确定目标数据处理算法对应的证书,目标数据处理算法为当前启用的面部识

别应用程序关联的多个数据处理算法中的数据处理算法;其次,获取证书关联的进程名集合;最后,检测到进程名集合包括第一进程的进程名,加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法,那么这些第三方数据处理算法的安全性就显得尤为重要,故而通过证书鉴权机制以确保调用目标数据处理算法的安全性,能够避免非法进程调用该算法来破解该算法的情况发生,有利于提高移动终端进行人脸识别的安全性。

[0079] 此外,移动终端需要基于证书验证机制,在检测到调用目标处理算法的第一进程身份合法的情况下,才允许通过目标数据处理算法处理所述第一进程关联的参考数据,有利于提高移动终端进行人脸识别的安全性。

[0080] 与所述图2A所示的实施例一致的,请参阅图4,图4是本申请实施例提供的一种证书加载方法的流程示意图,应用于移动终端,所述移动终端运行有安卓系统和安全系统,所述安卓系统中运行有人脸识别服务Service,所述安全系统中运行有人脸识别可信应用TA。如图所示,本证书加载方法包括:

[0081] S401,所述移动终端检测到所述移动终端的开机事件,导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书;

[0082] S402,所述移动终端确定每个证书关联的进程名集合。

[0083] S403,移动终端检测到所述面部识别应用程序的启用指令,验证所述面部识别应用程序的签名证书和导入证书为同个证书;

[0084] S404,所述移动终端启用所述面部识别应用程序。

[0085] S405,所述移动终端检测到请求调用目标数据处理算法的第一进程,确定所述目标数据处理算法对应的证书,所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法;

[0086] S406,所述移动终端获取所述证书关联的进程名集合;

[0087] S407,所述移动终端检测到所述进程名集合包括所述第一进程的进程名,调用所述证书解析处于加密状态的所述目标数据处理算法;

[0088] S408,所述移动终端通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0089] 可以看出,本申请实施例中,移动终端在检测到请求调用目标数据处理算法的第一进程,首先确定目标数据处理算法对应的证书,目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法;其次,获取证书关联的进程名集合;最后,检测到进程名集合包括第一进程的进程名,加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法,那么这些第三方数据处理算法的安全性就显得尤为重要,故而通过证书鉴权机制以确保调用目标数据处理算法的安全性,能够避免非法进程调用该算法来破解该算法的情况发生,有利于提高移动终端进行人脸识别的安全性。

[0090] 此外,移动终端需要基于证书验证机制,在检测到调用目标处理算法的第一进程身份合法的情况下,才允许通过目标数据处理算法处理所述第一进程关联的参考数据,有利于提高移动终端进行人脸识别的安全性。

[0091] 此外,签名证书和导入证书的验证机制可以有效防止面部识别应用程序被掉包,

有利于提高移动终端进行人脸识别的安全性。

[0092] 此外，移动终端在开机时既可以同步导入数据处理算法的证书，以及确定每个证书关联的进程名集合，使得后续使用过程中移动终端无需再次导入证书，提高鉴权速度。

[0093] 此外，移动终端提供了灵活的进程集合确定机制，有利于提高进程集合设置的便捷性和灵活性。

[0094] 与所述图2A、图3、图4所示的实施例一致的，请参阅图5，图5是本申请实施例提供的一种移动终端的结构示意图，如图所示，该移动终端包括处理器、存储器、通信接口以及一个或多个程序，其中，所述一个或多个程序被存储在所述存储器中，并且被配置由所述处理器执行，所述程序包括用于执行以下步骤的指令；

[0095] 检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；

[0096] 获取所述证书关联的进程名集合；

[0097] 检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0098] 可以看出，本申请实施例中，移动终端在检测到请求调用目标数据处理算法的第一进程，首先确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；其次，获取证书关联的进程名集合；最后，检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法，那么这些第三方数据处理算法的安全性就显得尤为重要，故而通过证书鉴权机制以确保调用目标数据处理算法的安全性，能够避免非法进程调用该算法来破解该算法的情况发生，有利于提高移动终端进行人脸识别的安全性。

[0099] 在一个可能的示例中，在所述加载所述证书以允许所述第一进程调用所述目标数据处理算法方面，所述程序中的指令具体用于执行以下操作：调用所述证书解析处于加密状态的所述目标数据处理算法；以及通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0100] 在一个可能的示例中，所述程序还包括用于执行以下操作的指令：在所述检测到请求调用目标数据处理算法的第一进程之前，检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书；以及启用所述面部识别应用程序。

[0101] 在一个可能的示例中，所述程序还包括用于执行以下操作的指令：检测到所述移动终端的开机事件，导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书；以及确定每个证书关联的进程名集合。

[0102] 在一个可能的示例中，在所述确定每个证书关联的进程名集合方面，所述程序中的指令具体用于执行以下操作：根据当前用户录入的进程名确定所述每个证书关联的进程名集合；或者，查询预设的证书与进程名集合之间的映射关系，确定所述每个证书关联的进程名集合。

[0103] 与上述实施例一致的，图6是本申请实施例提供的一种移动终端的功能单元组成

框图，所述移动终端运行有安卓系统和安全系统，所述安卓系统中运行有人脸识别服务Service，所述安全系统中运行有人脸识别可信应用TA，该移动终端600包括：确定单元601、获取单元602和加载单元603，其中，

[0104] 所述确定单元601，用于检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书，所述目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；

[0105] 所述获取单元602，用于获取所述证书关联的进程名集合；

[0106] 所述加载单元603，用于检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法。

[0107] 可以看出，本申请实施例中，移动终端在检测到请求调用目标数据处理算法的第一进程，首先确定目标数据处理算法对应的证书，目标数据处理算法为当前启用的面部识别应用程序关联的多个数据处理算法中的数据处理算法；其次，获取证书关联的进程名集合；最后，检测到进程名集合包括第一进程的进程名，加载证书以允许第一进程调用目标数据处理算法。由于面部识别应用程序在进行人脸识别过程中会调用第三方数据处理算法，那么这些第三方数据处理算法的安全性就显得尤为重要，故而通过证书鉴权机制以确保调用目标数据处理算法的安全性，能够避免非法进程调用该算法来破解该算法的情况发生，有利于提高移动终端进行人脸识别的安全性。

[0108] 在一个可能的示例中，在所述加载所述证书以允许所述第一进程调用所述目标数据处理算法方面，所述加载单元603具体用于：调用所述证书解析处于加密状态的所述目标数据处理算法；以及通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据。

[0109] 在一个可能的示例中，所述移动终端还包括验证单元和启动单元，

[0110] 所述验证单元，用于在所述确定单元601在检测到请求调用目标数据处理算法的第一进程之前，检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书；

[0111] 所述启动单元，用于启用所述面部识别应用程序。

[0112] 在一个可能的示例中，所述移动终端还包括导入单元，

[0113] 所述导入单元，用于检测到所述移动终端的开机事件，导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书；

[0114] 所述确定单元601，还用于确定每个证书关联的进程名集合。

[0115] 在一个可能的示例中，在所述确定每个证书关联的进程名集合方面，所述确定单元601具体用于：根据当前用户录入的进程名确定所述每个证书关联的进程名集合；或者，查询预设的证书与进程名集合之间的映射关系，确定所述每个证书关联的进程名集合。

[0116] 需要注意的是，本申请装置实施例所描述的移动终端是以功能单元的形式呈现。这里所使用的术语“单元”应当理解为尽可能最宽的含义，用于实现各个“单元”所描述功能的对象例如可以是集成电路ASIC，单个电路，用于执行一个或多个软件或固件程序的处理器(共享的、专用的或芯片组)和存储器，组合逻辑电路，和/或提供实现上述功能的其他合适的组件。

[0117] 其中，确定单元601和加载单元603可以是处理器或控制器，获取单元602可以通信

接口等。

[0118] 本申请实施例还提供一种计算机存储介质，其中，该计算机存储介质存储用于电子数据交换的计算机程序，该计算机程序使得计算机执行如所述方法实施例中记载的任一方法的部分或全部步骤，所述计算机包括移动终端。

[0119] 本申请实施例还提供一种计算机程序产品，所述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质，所述计算机程序可操作来使计算机执行如所述方法实施例中记载的任一方法的部分或全部步骤。该计算机程序产品可以为一个软件安装包，所述计算机包括移动终端。

[0120] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请并不受所描述的动作顺序的限制，因为依据本申请，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本申请所必须的。

[0121] 在所述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0122] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

[0123] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0124] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。所述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0125] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储器中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储器中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本申请各个实施例上述方法的全部或部分步骤。而前述的存储器包括：U盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0126] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储器中，存储器可以包括：闪存盘、只读存储器(英文：Read-Only Memory，简称：ROM)、随机存取器(英文：Random Access Memory，简称：RAM)、磁盘或光盘等。

[0127] 以上对本申请实施例进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

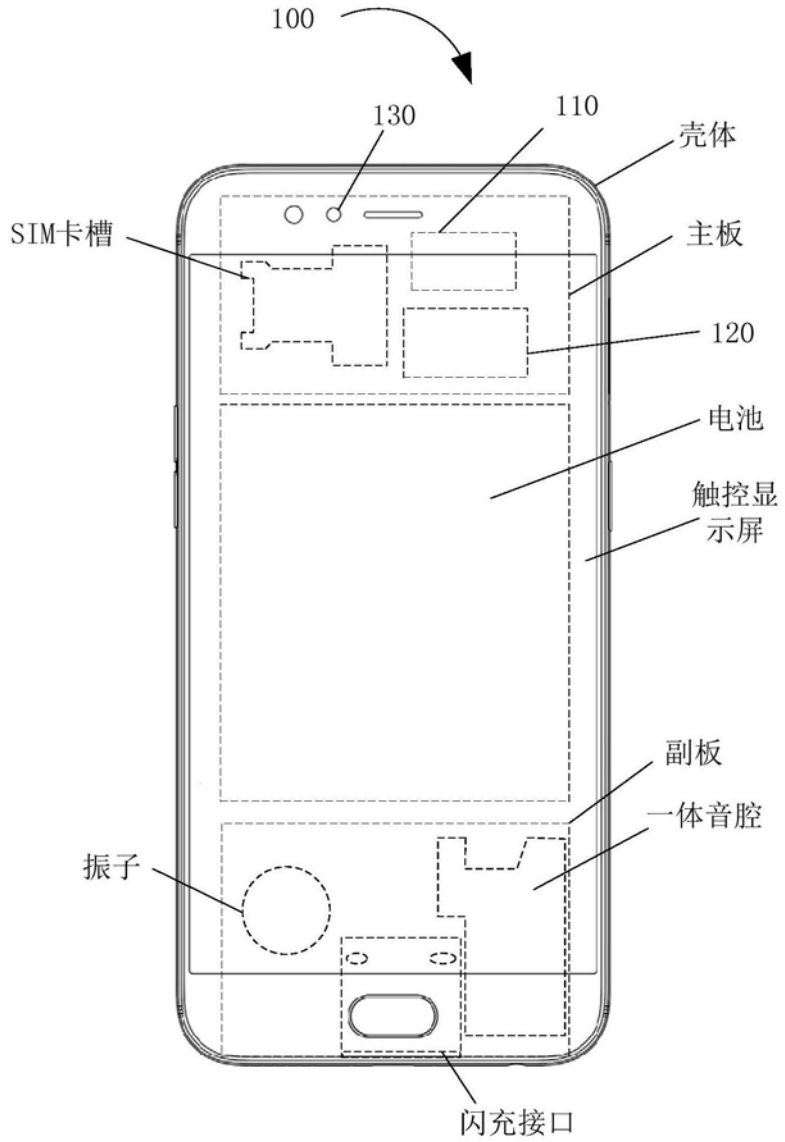


图1

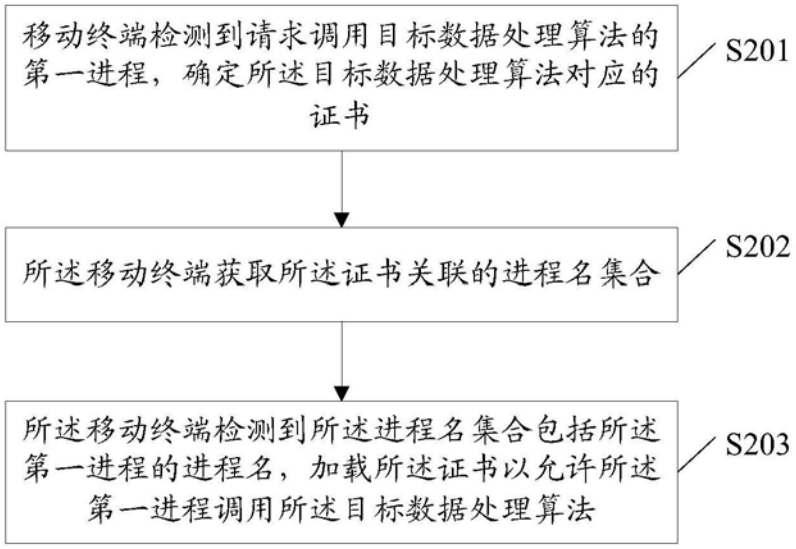

移动终端检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书
S201
所述移动终端获取所述证书关联的进程名集合
S202
所述移动终端检测到所述进程名集合包括所述第一进程的进程名，加载所述证书以允许所述第一进程调用所述目标数据处理算法
S203

图2A

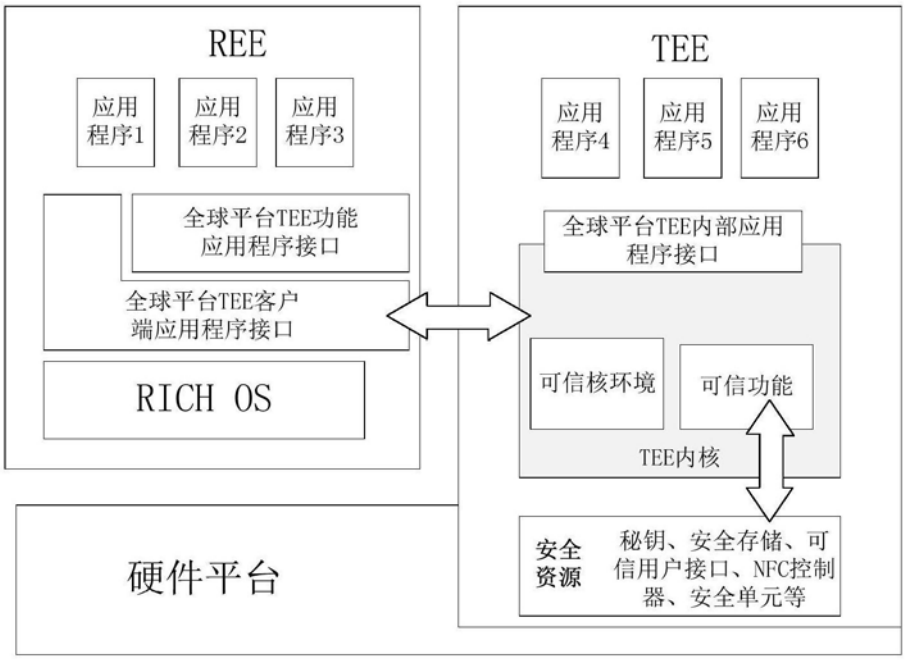

REE
应用程序1
应用程序2
应用程序3
全球平台TEE功能应用程序接口
全球平台TEE客户端应用程序接口
RICH OS
TEE
应用程序4
应用程序5
应用程序6
全球平台TEE内部应用程序接口
可信核环境
可信功能
TEE内核
安全资源
秘钥、安全存储、可信用户接口、NFC控制器、安全单元等
硬件平台

图2B

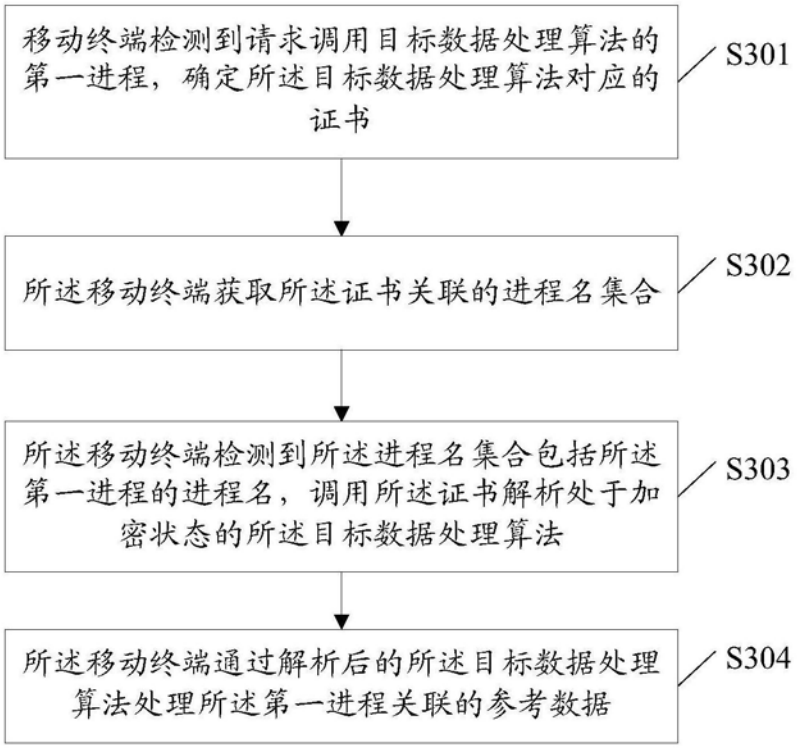

移动终端检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书
S301
所述移动终端获取所述证书关联的进程名集合
S302
所述移动终端检测到所述进程名集合包括所述第一进程的进程名，调用所述证书解析处于加密状态的所述目标数据处理算法
S303
所述移动终端通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据
S304

图3

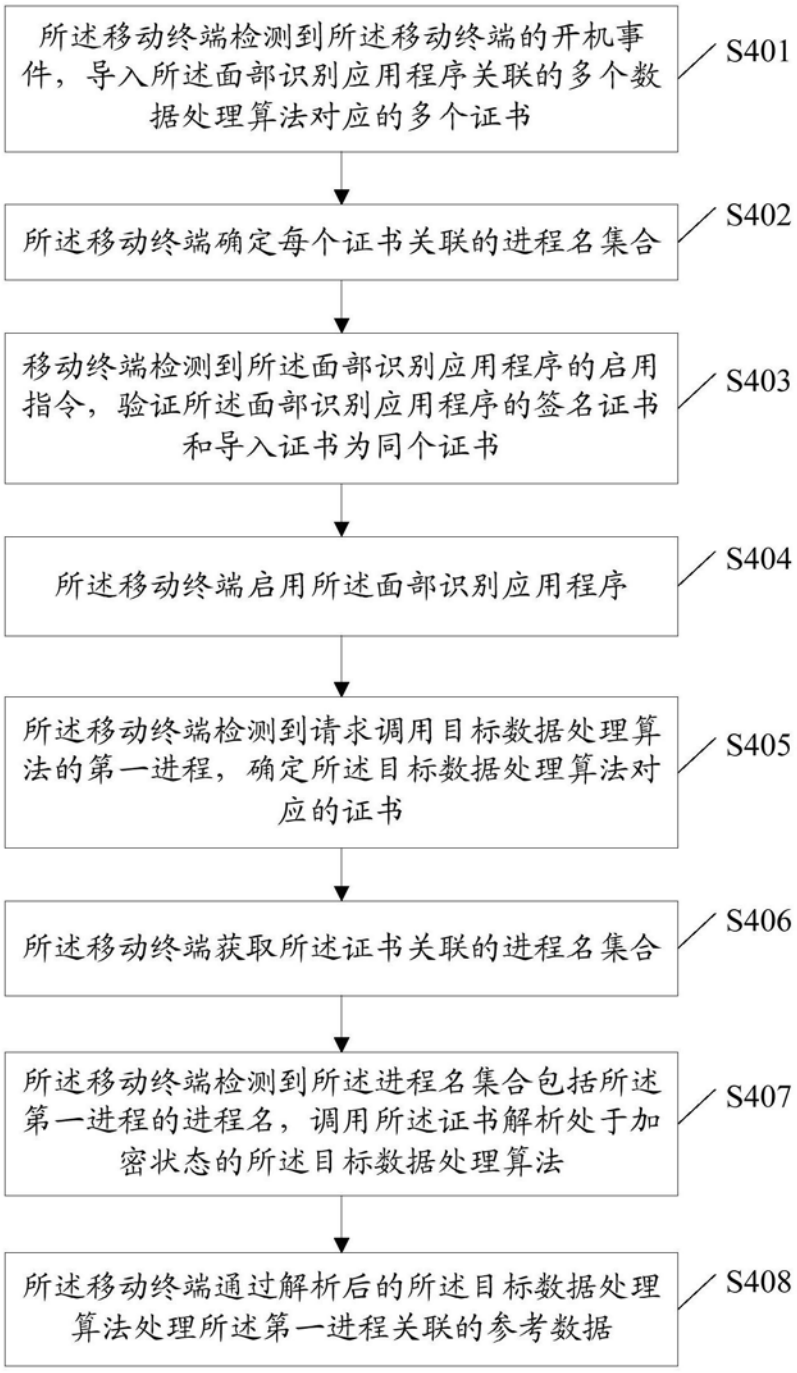

所述移动终端检测到所述移动终端的开机事件，导入所述面部识别应用程序关联的多个数据处理算法对应的多个证书
S401
所述移动终端确定每个证书关联的进程名集合
S402
移动终端检测到所述面部识别应用程序的启用指令，验证所述面部识别应用程序的签名证书和导入证书为同个证书
S403
所述移动终端启用所述面部识别应用程序
S404
所述移动终端检测到请求调用目标数据处理算法的第一进程，确定所述目标数据处理算法对应的证书
S405
所述移动终端获取所述证书关联的进程名集合
S406
所述移动终端检测到所述进程名集合包括所述第一进程的进程名，调用所述证书解析处于加密状态的所述目标数据处理算法
S407
所述移动终端通过解析后的所述目标数据处理算法处理所述第一进程关联的参考数据
S408

图4

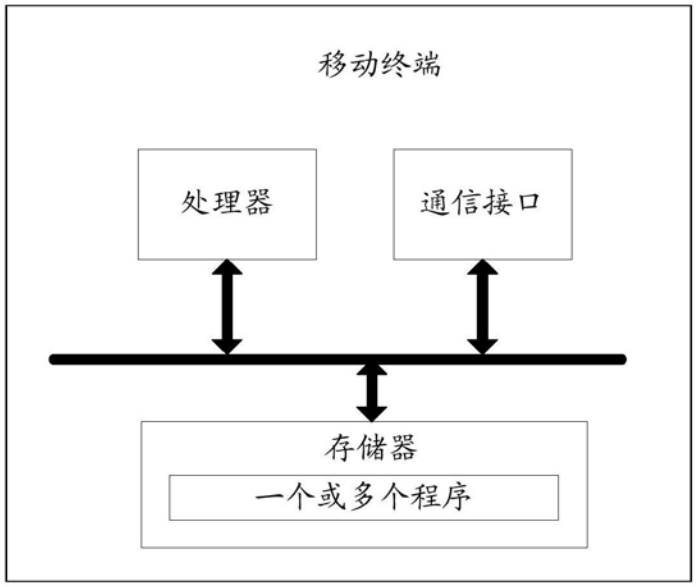


图5

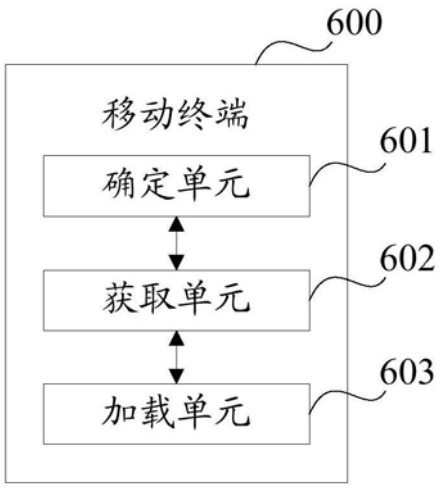


图6