(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 10 月 17 日 (17.10.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/196792 A1

(51) 国际专利分类号:
G06F 21/12 (2013.01)

(21) 国际申请号: PCT/CN2019/081739

(22) 国际申请日: 2019 年 4 月 8 日 (08.04.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810326273.3 2018年4月12日 (12.04.2018) CN
201810327440.6 2018年4月12日 (12.04.2018) CN

(71) 申请人: **OPPO 广东移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: **郭子青 (GUO, Ziqing)**; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。 **周海涛 (ZHOU, Haitao)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 **惠方方 (HUI, Fangfang)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 **谭筱 (TAN, Xiao)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

(74) 代理人: 北京清亦华知识产权代理事务所 (普通合伙) **(TSINGYIHUA INTELLECTUAL PROPERTY LLC)**; 中国北京市海淀区清华园清华大学照澜院商业楼301室, Beijing 100084 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,

(54) **Title:** SECURITY CONTROL METHOD AND APPARATUS FOR APPLICATION PROGRAM, AND MOBILE TERMINAL AND COMPUTER-READABLE STORAGE MEDIUM

(54) **发明名称**: 应用程序的安全控制方法及装置、移动终端及计算机可读存储介质

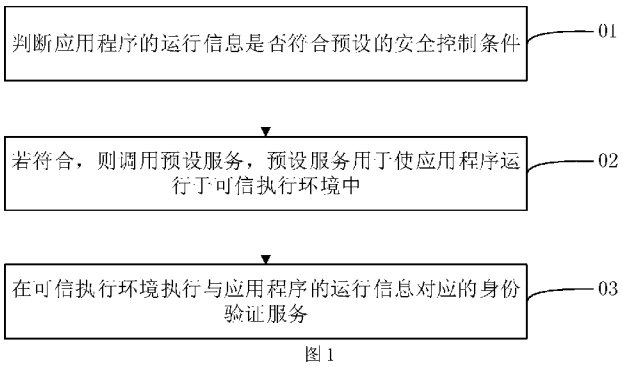

图 1

01 Determine whether running information of an application program satisfies a pre-set security control condition

02 If so, invoke a pre-set service, wherein the pre-set service is used for enabling the application program to be run in a trusted execution environment

03 Execute, in the trusted execution environment, an identity verification service corresponding to the running information of the application program

(57) **Abstract:** A security control method for an application program. The method comprises: determining whether running information of an application program satisfies a pre-set security control condition (01); if so, invoking a pre-set service, wherein the pre-set service is used for enabling the application program to be run in a trusted execution environment (02); and executing, in the trusted execution environment, an identity verification service corresponding to the running information of the application program (03).

(57) **摘要**: 一种应用程序的安全控制方法, 方法包括: 判断应用程序的运行信息是否符合预设的安全控制条件 (01); 若符合, 则调用预设服务, 预设服务用于使应用程序运行于可信执行环境中 (02); 在可信执行环境执行与应用程序的运行信息对应的身份验证服务 (03)。

WO 2019/196792 A1

[见续页]

IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

应用程序的安全控制方法及装置、移动终端及计算机可读存储介质

优先权信息

本申请请求 2018 年 04 月 12 日向中国国家知识产权局提交的、专利申请号为 201810326273.3 及 201810327440.6 的专利申请的优先权和权益，并且通过参照将其全文并入此处。

技术领域

本申请涉及移动终端技术领域，尤其涉及一种应用程序的安全控制方法、应用程序的安全控制装置及移动终端、计算机可读存储介质。

背景技术

在许多应用场景下，均需要在应用程序中的进行身份验证服务，身份验证服务例如为对使用该应用程序所属终端的用户的身份进行验证，例如通过人脸识别等进行身份验证，在验证通过后，执行后续的终端解锁、电子支付等操作。

发明内容

本申请实施方式提供一种应用程序的安全控制方法、应用程序的安全控制装置及移动终端、计算机可读存储介质。

本申请实施方式的应用程序的安全控制方法包括步骤：判断所述应用程序的运行信息是否符合预设的安全控制条件；若符合，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中；及在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务。

本申请实施方式的应用程序的安全控制装置包括判断总模块、调用总模块及执行总模块。判断总模块用于判断所述应用程序的运行信息是否符合预设的安全控制条件；调用总模块用于若判断符合所述安全控制条件，则调用预设服务，所述预设服务用于使所述应用程序运行于所述可信执行环境中；执行总模块用于在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务。

本申请实施方式的终端包括成像传感器、存储器、微处理器单元 MCU、处理器及存储在所述存储器上并可在所述处理器的可信执行环境下运行的可执行程序代码；所述 MCU，为所述可信执行环境的专用硬件，与所述成像传感器和所述处理器连接，用于控制所述成像传感器进行成像，并将成像数据发送至所述处理器；所述处理器执行所述可执行程序代码时，实现上述的应用程序的安全控制方法。

本申请实施方式的计算机可读存储介质上存储有计算机程序，该程序被处理器执行时实现上述的应用程序的安全控制方法。

本申请的实施方式的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实施方式的实践了解到。

附图说明

本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图；

图 2 为本申请实施例提供的一种应用程序的安全控制装置的结构示意图；

图 3 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图；

图 4 为本申请实施例提供的一种电子设备的结构示意图；

图 5 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图；

图 6 为本申请实施例提供的一种根据红外图像进行活体识别的方法的流程示意图；

图 7 为本申请实施例提供的一种根据红外图像和可见光图像进行活体检测的方法的流程示意图；

图 8 为本申请实施例提供的一种应用程序的安全控制装置的结构示意图；
图 9 为本申请实施例提供的一种应用程序的安全控制装置的结构示意图；
图 10 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图；
图 11 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图；
图 12 为本申请实施例提供的一种应用程序的安全控制装置的结构示意图；
图 13 为本申请实施例提供的一种应用程序的安全控制装置的结构示意图；
图 14 为本申请实施例提供的一种移动终端的结构示意图；
图 15 为本申请实施例提供的一种计算机可读存储介质的结构示意图。

具体实施方式

下面详细描述本申请的实施例，实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本申请，而不能理解为对本申请的限制。相反，本申请的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

下面参考附图描述本申请实施例的应用程序的安全控制方法、装置及移动终端、存储介质。

目前，在许多应用场景下，均需要在应用程序中的进行身份验证服务，身份验证服务例如为对使用该应用程序所属终端的用户的身份进行验证，例如通过应用程序的安全控制等进行身份验证，在验证通过后，执行后续的终端解锁、电子支付等操作。

请参阅图 1，本申请实施方式提供一种应用程序的安全控制方法，安全程序的应用方式包括步骤：

01：判断应用程序的运行信息是否符合预设的安全控制条件；
02：若符合，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中；及
03：在可信执行环境执行与应用程序的运行信息对应的身份验证服务。

请参阅图 2，本申请实施方式提一种应用程序的安全控制装置 60，安全控制装置 60 具有可信执行环境，安全控制装置 60 包括判断总模块 61、调用总模块 62 及执行总模块 63。判断总模块 61 用于判断应用程序的运行信息是否符合预设的安全控制条件。调用总模块 62 用于若判断符合安全控制条件，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中。执行总模块 63 用于在可信执行环境执行与应用程序的运行信息对应的身份验证服务。

即，判断总模块 61 可用于实施步骤 01，调用总模块 62 可用于实施步骤 02，执行总模块 63 可用于实施步骤 03。

本申请实施方式的应用程序的安全控制方法及控制装置 60 中，若应用程序的运行信息符合预设的安全控制条件，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中，以及在可信执行环境中执行与应用程序的运行信息对应的身份验证服务，能够从运行环境上提高身份验证服务的安全性。

下面将以两部分实施例展开本申请实施方式的应用程序的安全控制方法及控制装置。

第一部分实施例：

相关技术中，应用程序在执行身份验证服务时的软件环境安全性不高。

针对这一问题，本申请实施例提出一种应用程序的安全控制方法，该方法在进行身份验证服务之前，首先确定应用程序是否为预设应用程序；若为预设应用程序，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中；在可信执行环境中执行应用程序中的身份验证服务，提高了应用程序在执行身份验证服务时的软件环境安全性，以及从另外一个维度提升身份验证的安全性和可靠性。

图 3 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图。

该应用程序的安全控制方法可应用电子设备 70，电子设备的结构可参见图 4。

图 4 为本申请实施例提供的一种电子设备 70 的结构示意图。

如图 4 所示，该电子设备 70 包括：激光摄像头 71、泛光灯 72、可见光摄像头 73、镭射灯 74 以及微控制器单元（Microcontroller Unit，MCU）75。其中，MCU75 包括脉冲宽度调制（Pulse Width

Modulation，PWM）751、深度引擎 752、总线接口 753 以及随机存取存储器 RAM754。

其中，PWM751 用于调制泛光灯 72 以使其发出红外光，以及调制镭射灯 74 以使其发出激光，激光可以带有特定图案；激光摄像头 71 用于采集成像对象的结构光图像或可见光图像，结构光图像为激光被成像对象调制后形成的图像；深度引擎 752 用于根据结构光图像，计算获得成像对象对应的深度数据；总线接口 753 用于将深度数据发送至处理器，并由处理器上运行的可执行程序代码利用深度数据执行相应的操作。其中，总线接口 753 包括 MIPI 总线接口、I2C 同步串行总线接口、SPI 总线接口。

如图 3 所示，步骤 01 包括步骤 101：确定应用程序是否为预设应用程序。

应用程序的运行信息包括应用程序的类型，其中的预设应用程序为需要在可信执行环境 76 中执行相关服务的应用程序，预设应用程序可以例如为安全类应用程序，或者需要进入保护状态的应用程序，对此不作限制。

本申请实施例中的预设应用程序可以由用户根据自身的需求进行设定，或者，也可以由电子设备 70 的出厂程序预先设定，对此不作限制。

本申请实施例在具体执行的过程中，可以预先建立一个预设应用程序标识库，该库中记录有多个预设应用程序的标识，通过电子设备 70 的操作系统读取当前进行安全控制的应用程序的标识，并在预设应用程序标识库中进行查询，若查询到预设应用程序标识库包含有该标识，则可以确定应用程序为预设应用程序，否则，确定其不为预设应用程序，在确定应用程序为预设应用程序之后，可以触发步骤 102 及步骤 103。

步骤 02 包括步骤 102：若为预设应用程序，则调用预设服务，预设服务用于使应用程序运行于可信执行环境 76 中。

步骤 03 包括步骤 103：在可信执行环境 76 中执行应用程序中的身份验证服务。

其中，与应用程序的运行信息对应的身份验证服务可以是应用程序中的身份验证服务。

可选地，一些实施例中，参见图 5，步骤 103：在可信执行环境 76 中执行应用程序中的身份验证服务，可以包括：

步骤 301，通过可信执行环境 76 的专用硬件，控制图像传感器进行成像，其中，图像传感器包括结构光传感器。

可信执行环境 76 是电子设备（包含智能手机、平板电脑等）主处理器上的一个安全区域，其可以保证加载到该环境内部的代码和数据的安全性、机密性以及完整性。可信执行环境 76 提供一个隔离的执行环境，提供的安全特征包含：隔离执行、可执行程序代码的完整性、可信数据的机密性、安全存储等。总之，可信执行环境 76 提供的执行空间比常见的移动操作系统，如 ISO、Android 等，提供更高级别的安全性。

本实施例中，预设服务用于使应用程序运行于可信执行环境 76 中，从运行环境上提高了身份验证服务的安全性。

当在可信执行环境 76 中执行应用程序中的身份验证服务时，如进行电子支付、电子设备解锁时，可通过可信执行环境 76 的专用硬件，控制开启图像传感器进行成像。其中，专用硬件可以为 MCU，图像传感器可包括结构光传感器。

为了进一步提高安全性，可将结构光图像发送至 MCU75，在硬件的 MCU75 中对结构光图像进行处理，相比于直接发送给应用程序处理，数据已经在硬件中运算，黑客无法获取原始的数据，因此更加安全。

本实施例中，结构光传感器可包括激光摄像头 71 和镭射灯 74。MCU 75 可以调制电子设备 70 上的镭射灯 74 发出激光，激光投射到成像对象。激光受到成像对象的阻碍和调制，被成像对象反射，激光摄像头 71 捕获成像对象反射的激光进行成像。

本实施例中，由于每个人的身体部分的特征一般是不相同的，可以选取身体部位作为成像对象，例如，成像对象可以为人脸、面部器官（眼睛、鼻子、嘴巴）或者手部等身体部位。

步骤 302，通过专用硬件，获取图像传感器成像得到的成像数据。

本实施例中，可通过专用硬件，获取图像传感器成像的得到的成像数据，如结构光传感器成像得到的深度数据。

步骤 303，根据成像数据，对成像对象进行活体检测。

本实施例中，可利用成像数据中的深度数据，对成像对象进行活体检测。

具体而言，根据深度数据构建结构光深度模型，并从结构光深度模型中识别目标器官，具体地，将结构光深度模型与预存的脸部器官的结构光深度模型进行比对，以从结构光深度模型中识别出目标器官。

由于成像对象为活体时，成像对象不可能始终保持静止，当某器官处于运动状态时，其深度数据也会发生变化，因此本实施例中对目标器官进行跟踪，以确定目标器官是否处于运动状态。

在识别出目标器官后，继续采集成像对象的深度图，获取连续的多帧深度图。通过比较同一器官在连续的多帧深度图中的深度数据，以确定该器官是否处于运动状态。当同一器官在连续的多帧深度图中的深度数据发生了变化，可以确定该器官处于运动状态。

当目标器官处于运动状态时，说明成像对象不是仿照物，如照片等，可以确定该成像对象为活体。当目标器官处于静止状态时，可以确定该成像对象不是活体，可能为照片等仿照物。

本实施例中，通过从结构光深度模型中识别出目标器官，对目标器官进行跟踪，以确定目标器官是否处于运动状态，进而确定成像对象是否为活体，活体检测的准确率高。

步骤 304，若活体检测通过，将依据成像数据中的深度数据构建的结构光深度模型，与预设人脸深度模型进行匹配。

如果成像对象通过活体检测，将成像对象的结构光深度模型与预设的人脸深度模型进行匹配。

作为一种可能的实现方式，可将构建的结构光深度模型中脸部各个器官的结构光深度模型，与预设的人脸深度模型中各个器官的深度模型进行比对，当相似度超过预设阈值时，可以认为结构光深度模型与预设的人脸深度模型匹配。

可以理解的是，这里预设的人脸深度模型，是预先存储的利用结构光图像传感器对电子设备 70 的机主的人脸进行成像得到的结构光图像，利用结构光图像中深度数据构建得到的预设的人脸深度模型，以用于身份验证。

步骤 305，当结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

当结构光深度模型与预设人脸深度模型匹配时，确定通过了身份验证，可以进行后续的操作，如完成电子支付、电子设备解锁等等。

当未通过活体检测时，可返回未通过活体检测的消息，或者当结构光深度模型与预设人脸深度模型不匹配时，返回身份验证失败的信息。

本实施例中，先根据成像数据对成像对象进行活体检测，在活体检测通过后，再根据结构光深度模型进行身份验证，从而可以避免利用仿照物如照片身份验证通过的情况，提高了用人脸进行身份验证的安全性和可靠性。

上述实施例中，通过专用硬件，控制进行成像的图像传感器还可包括红外传感器，红外传感器包括激光摄像头 71 和泛光灯 72。在控制红外传感器进行成像时，PWM 751 可以调制电子设备 70 上的泛光灯 72 发出红外光，投射到成像对象。红外光受到成像对象的阻碍，被成像对象反射，激光摄像头 71 捕获成像对应反射的红外光进行成像。

在进行活体检测时，可通过红外传感器成像得到的红外图像，识别红外图像的成像对象是否为活体。

图 6 为本申请实施例提供的一种根据红外图像进行活体识别的方法的流程示意图。

如图 6 所示，该活体检测方法包括：

步骤 401，从红外图像中提取成像轮廓。

本实施例中，可根据红外图像中的边缘像素点，提取得到成像轮廓。

步骤 402，根据处于成像轮廓内部的局部红外图像，确定红外图像的成像对象的温度。

本实施例中，可将成像轮廓划分多个部分，确定每个局部红外图像对应的温度，将每个局部红外图像对应的温度相加求出平均值，将平均值作为红外图像的成像对象的温度。

步骤 403，若成像轮廓与预设人脸轮廓匹配，且红外图像的成像对象的温度处于体温范围内，确定红外图像的成像对象为活体。

本实施例中，将成像轮廓与预设人脸轮廓进行匹配。作为一个示例，在进行成像轮廓匹配时，

可分段进行匹配，当每个分段相似程度均超过每个分段的预设阈值时，可以认为该成像轮廓与预设的成像轮廓匹配，即成像对象为预存的成像对象。

在将成像轮廓与预设的人脸轮廓进行比对时，可将人脸轮廓分以眉毛为分界分为上半部分和下半部分，分段进行比对。由于上半部分（包括眉毛），受到眉形、发型的影响，相对变化比较大，可信度比较低，而下半部分，如眼睛、眉毛、鼻子、嘴巴等比较固定，因此上半部分对应的相似度的预设阈值，相对下半部分相对较小。

针对两个部分分别进行比对，当成像轮廓的上半部分与预存的人脸轮廓的上半部分的相似度超过对应的预设阈值，且成像轮廓的下半部分与预存的人脸轮廓的下半部分的相似度超过对应的预设阈值时，可以认为成像轮廓与预存的人脸轮廓匹配。

若成像轮廓与预设的人脸轮廓匹配，且红外图像的成像对象的温度处于人体体温范围内，可以确定红外图像的成像对象为活体。否则，可以认为红外图像的成像对象不是活体。

本实施例中，通过成像轮廓是否与预设人脸轮匹配，以及成像对象的温度是否在人体体温范围内，判断成像对象是否为活体，从而提高了活体识别的准确率。

上述实施例中，通过专用硬件，控制开启的图像传感器可包括红外传感器和可见光传感器，通过红外传感器和可见光传感器成像得到红外图像和可见光图像。在进行活体检测时，可通过红外图像和可见光图像，对成像对象进行活体检测。

图 7 为本申请实施例提供的一种根据红外图像和可见光图像进行活体检测的方法的流程示意图。

如图 7 所示，该活体检测方法包括：

步骤 501，在可见光图像中识别人脸区域，并在红外图像中，确定与人脸区域相对应的第一目标区域。

本实施例中，在可见光图像上，检测人脸区域，如果没有检测到人脸区域，重新采集可见光图像和红外图像。如果检测到人脸，则在红外图像中识别出人脸轮廓，确定与可见光图像中人脸区域对应的第一目标区域。可以理解的是，这里第一目标区域为红外图像中的人脸区域。

步骤 502，根据第一目标区域，确定包含第一目标区域且大于第一目标区域的第二目标区域。

在红外图像上在第一目标区域的基础上扩大范围，得到第二目标区域。可以理解的是，第二目标区域包含第一目标区域且大于第一目标区域。

步骤 503，在第二目标区域内统计直方图，并根据直方图计算对比度。

在红外图像上的第二目标区域内统计直方图，如公式（1）所示。

$$C=\sum_{\delta}\delta(\mathrm{i},j)^{2}p_{\delta}(\mathrm{i},j) \quad (1)$$

其中，$\delta(\mathrm{i},j)=|i-j|$，即相邻像素间灰度差，$p_{\delta}(\mathrm{i},j)$ 为相邻像素间的灰度差的像素分布概率。

步骤 504，若对比度大于阈值，确定红外图像和可见光图像的成像对象为活体。

当对比度大于一定的阈值时，可以确定红外图像和可见光图像的成像对象为活体，否则为仿照物。

本实施例中，通过红外图像和可见光图像两种图像，确定成像对象是否活体，提高了活体检测的准确率。

进一步地，在提高身份验证的安全性和可靠性的情况下，能够节省电子设备 70 的能量，提高续航能力。

本申请实施例中，若控制成像的图像传感器中还包括红外传感器，则通过专用硬件，控制开启红外传感器进行成像。若根据红外传感器成像得到的红外图像确定成像对象为活体，控制结构光传感器进行成像。

具体而言，通过专用硬件 MCU 75 调整泛光灯以发出红外光，红外光照射至成像对象。红外光受到成像对象的阻碍，反射红外光，红外传感器接收到成像对象反射的红外光，进行成像。

通过 MCU 75 获取红外传感器成像得到的红外图像，并根据红外图像对成像对象进行活体检测，具体的检测方法可参见上述实施例中描述的方法，在此不再赘述。

若根据红外图像确定成像对象为活体，再控制结构光传感器进行成像，以根据结构光深度模

型进行身份验证。

本实施例中，先控制红外传感器进行成像，在根据红外图像确定成像对象为活体后，再控制结构光传感器进行成像，从而使得结构光传感器不需要一直处于工作状态，可以很好地节省电子设备 70 的电量，提高电子设备 70 的续航能力。

可以理解的是，为了提高身份验证的速度，可同步控制图像传感器中的红外传感器和结构光传感器进行成像，从而在根据红外图像确定成像对象为活体后，直接根据结构光传感器成像得到的成像数据进行身份验证，提高了身份验证的速度。

上述实施例中，若通过专用硬件控制成像的图像传感器中包括可见光传感器、红外传感器、结构光传感器，为了节省电子设备 70 的能量，可先控制可见光传感器和红外传感器进行成像。若根据红外传感器成像得到的红外图像和可见光传感器成像得到的可见光图像确定成像对象为活体，控制结构光传感器进行成像。

其中，根据可见光图像和红外图像，检测成像对象是否为活体的过程，可参见上述实施例中的方法，在此不再赘述。

本实施例中，通过确定应用程序是否为预设应用程序，若为预设应用程序，则调用预设服务，预设服务用于使应用程序运行于可信执行环境 76 中，以及在可信执行环境 76 中执行应用程序中的身份验证服务，能够从运行环境上提高了身份验证服务的安全性。

本申请实施例还提出一种应用程序的安全控制装置。

图 8 为本申请第一部分实施例提供的一种应用程序的安全控制装置 60 的结构示意图。

如图 8 所示，确定总模块 61 包括第一确定模块 601，用于确定应用程序是否为预设应用程序。

调用总模块 62 包括第一调用模块 602，用于在为预设应用程序时，调用预设服务，预设服务用于使应用程序运行于可信执行环境中。

执行总模块 63 包括第一执行模块 603，用于在可信执行环境中执行应用程序中的身份验证服务。

可选地，一些实施例中，参见图 9，第一执行模块 603，包括：

第一控制子模块 6031、第一获取子模块 6032、第一检测子模块 6033、第一匹配子模块 6034。其中，

第一控制子模块 6031，用于通过可信执行环境的专用硬件，控制图像传感器进行成像，其中，图像传感器包括结构光传感器。

第一获取子模块 6032，用于通过专用硬件，获取图像传感器成像得到的成像数据。

第一检测子模块 6033，用于根据成像数据，进行活体检测。

第一匹配子模块 6034，用于若活体检测通过，将成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；当结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

在本实施例一种可能的实现方式中，图像传感器还包括红外传感器，成像数据包括红外图像，第一检测子模块 6033 还用于：

根据成像数据中的红外图像，识别红外图像的成像对象是否为活体。

进一步地，在本实施例一种可能的实现方式中，第一检测子模块 6033 还用于：

从红外图像中提取成像轮廓；

根据处于成像轮廓内部的局部红外图像，确定红外图像的成像对象的温度；

若成像轮廓与预设人脸轮廓匹配，且红外图像的成像对象的温度处于体温范围内，确定红外图像的成像对象为活体。

在本实施例一种可能的实现方式中，图像传感器还包括红外传感器和可见光传感器，成像数据包括红外图像和可见光图像，第一检测子模块 6033 还用于：

在可见光图像中识别人脸区域，并在红外图像中，确定与人脸区域相对应的第一目标区域；

根据第一目标区域，确定包含第一目标区域且大于第一目标区域的第二目标区域；

在第二目标区域内统计直方图，并根据直方图计算对比度；

若对比度大于阈值，确定红外图像和可见光图像的成像对象为活体。

在本实施例一种可能的实现方式中，第一控制子模块 6031 还用于：

控制图像传感器中的红外传感器进行成像；

若根据红外传感器成像得到的红外图像确定成像对象为活体，控制结构光传感器进行成像。

在本实施例一种可能的实现方式中，第一控制子模块 6031 还用于：

同步控制图像传感器中的红外传感器和结构光传感器进行成像。

在本实施例一种可能的实现方式中，第一控制子模块 6031 还用于：

控制图像传感器中的红外传感器和可见光传感器进行成像；

若根据红外传感器成像得到的红外图像和可见光传感器成像得到的可见光图像确定成像对象为活体，控制结构光传感器进行成像。

上述应用程序的安全控制装置中各个模块的划分仅用于举例说明，在其他实施例中，可将应用程序的安全控制装置按照需要划分为不同的模块，以完成上述应用程序的安全控制装置的全部或部分功能。

需要说明的是，前述对应用程序的安全控制方法实施例的解释说明，也适用于该实施例的应用程序的安全控制装置，故在此不再赘述。

本申请实施例的应用程序的安全控制装置 60，通过确定应用程序是否为预设应用程序，若为预设应用程序，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中，以及在可信执行环境中执行应用程序中的身份验证服务，能够从运行环境上提高了身份验证服务的安全性。

第二部分实施例：

相关技术中，身份验证服务和后续的终端解锁、电子支付等操作均对应执行于同一级别的安全环境中，这种方式下，相关操作的执行效率不高。

针对这一问题，本申请实施例提出一种应用程序的安全控制方法，该方法首先确定当前对应用程序操作的操作类型，判断操作类型是否为预设操作类型，若为预设操作类型，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中，以及在可信执行环境中控制应用程序执行与预设操作类型对应的身份验证服务，能够在保障对设备操作安全性的同时，提升一些操作类型对应服务的执行效率，提升用户使用体验度。

图 10 为本申请实施例提供的一种应用程序的安全控制方法的流程示意图。

该应用程序的安全控制方法可应用电子设备 70，电子设备 70 的结构可参见图 4。

图 4 为本申请实施例提供的一种电子设备 70 的结构示意图。

如图 4 所示，该电子设备 70 包括：激光摄像头 71、泛光灯 72、可见光摄像头 73、镭射灯 74 以及微控制器单元（Microcontroller Unit，MCU）75。其中，MCU75 包括脉冲宽度调制（Pulse Width Modulation，PWM）751、深度引擎 752、总线接口 753 以及随机存取存储器 RAM754。

其中，PWM751 用于调制泛光灯 72 以使其发出红外光，以及调制镭射灯 74 以使其发出激光，激光可以带有特定图案；激光摄像头 71 用于采集成像对象的结构光图像或可见光图像，结构光图像为激光被成像对象调制后形成的图像；深度引擎 752 用于根据结构光图像，计算获得成像对象对应的深度数据；总线接口 753 用于将深度数据发送至处理器，并由处理器上运行的可执行程序代码利用深度数据执行相应的操作。其中，总线接口 753 包括 MIPI 总线接口、I2C 同步串行总线接口、SPI 总线接口。

如图 10 所示，步骤 01 包括步骤 201：确定当前对应用程序操作的操作类型；及步骤 202：判断操作类型是否为预设操作类型。

应用程序的运行信息包括对应用程序操作的操作类型，其中的预设操作类型为需要在可信执行环境 76 中进行执行的操作类型，预设操作类型可以例如为电子支付类操作，而非预设操作类型的操作类型可以例如为解锁类操作，对此不作限制。

本申请实施例中的预设操作类型可以由用户根据自身的需求进行设定，或者，也可以由电子设备 70 的出厂程序预先设定，对此不作限制。

本申请实施例在具体执行的过程中，可以预先建立一个预设操作类型标识库，该库中记录有多个预设操作类型的标识，通过电子设备 70 的操作系统读取当前对应用程序进行操作的操作类型标识，并在预设操作类型标识库中进行查询，若查询到预设操作类型标识库包含有该操作类型标识，则可以确定当

前对应用程序操作的操作类型为预设操作类型，否则，确定其不为预设操作类型，在确定当前对应用程序操作的操作类型为预设操作类型之后，可以触发下述步骤 203 及步骤 204。

步骤 02 包括步骤 203：若为预设操作类型，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中。

进一步，如图 11，可选地，步骤 02 包括步骤 205：若不为预设操作类型，则在第一执行环境中控制应用程序执行与操作类型对应的服务，第一执行环境为与可信执行环境 76 不同的执行环境。

请结合图 4，本申请实施例中，第一执行环境例如为普通执行环境 77，具体如富媒体执行环境，对此不作限制。

本申请实施例若不为预设操作类型，则在第一执行环境中控制应用程序执行与操作类型对应的服务，第一执行环境为与可信执行环境 76 不同的执行环境，能够有效提升该种操作类型（例如，解锁类操作）的执行效率，提升用户使用体验度。而在可信执行环境 76 中控制应用程序执行与预设操作类型对应的身份验证服务，能够保障对设备操作的软件环境的安全性和可靠性。

步骤 03 包括步骤 204：在可信执行环境 76 中控制应用程序执行与预设操作类型对应的身份验证服务。

请参阅图 4 至图 7，上述第一部分实施例的部分也可以用于本申请第二部分实施例中，例如对步骤 301、步骤 302、步骤 303、步骤 304、步骤 305、步骤 401、步骤 402、步骤 403、步骤 501、步骤 502、步骤 503、步骤 504 的描述及其相关的技术细节，因此，在此不再赘述。

本实施例中，通过确定当前对应用程序操作的操作类型，在操作类型为预设操作类型时，调用预设服务，预设服务用于使应用程序运行于可信执行环境 76 中，以及在可信执行环境 76 中控制应用程序执行与预设操作类型对应的身份验证服务，能够在保障对设备操作安全性的同时，提升一些操作类型对应服务的执行效率，提升用户使用体验度。

本申请实施例还提出一种应用程序的安全控制装置。

图 12 为本申请第二部分实施例提供的一种应用程序的安全控制装置 60 的结构示意图。

如图 8 所示，确定总模块 61 包括第二确定模块 611，用于确定当前对应用程序操作的操作类型及判断模块 612，用于判断操作类型是否为预设操作类型；

第二调用模块 613，用于在为预设操作类型时，调用预设服务，预设服务用于使应用程序运行于可信执行环境中；

第二执行模块 614，用于在可信执行环境中控制应用程序执行与预设操作类型对应的身份验证服务。

可选地，一些实施例中，第二执行模块 614，还用于：

若不为预设操作类型，则在第一执行环境中控制应用程序执行与操作类型对应的服务，第一执行环境为与可信执行环境不同的执行环境。

可选地，一些实施例中，参见图 13，第二执行模块 614，包括：

第二控制子模块 6141、第二获取子模块 6142、第二检测子模块 6143、第二匹配子模块 6144。其中，

第二控制子模块 6141，用于通过可信执行环境的专用硬件，控制图像传感器进行成像，其中，图像传感器包括结构光传感器。

第二获取子模块 6142，用于通过专用硬件，获取图像传感器成像得到的成像数据。

第二检测子模块 6143，用于根据成像数据，进行活体检测。

第二匹配子模块 6144，用于若活体检测通过，将成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；当结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

在本实施例一种可能的实现方式中，图像传感器还包括红外传感器，成像数据包括红外图像，第二检测子模块 6143 还用于：

根据成像数据中的红外图像，识别红外图像的成像对象是否为活体。

进一步地，在本实施例一种可能的实现方式中，第二检测子模块 6143 还用于：

从红外图像中提取成像轮廓；

根据处于成像轮廓内部的局部红外图像，确定红外图像的成像对象的温度；

若成像轮廓与预设人脸轮廓匹配，且红外图像的成像对象的温度处于体温范围内，确定红外图像的成像对象为活体。

在本实施例一种可能的实现方式中，图像传感器还包括红外传感器和可见光传感器，成像数据包括红外图像和可见光图像，第二检测子模块 6143 还用于：

在可见光图像中识别人脸区域，并在红外图像中，确定与人脸区域相对应的第一目标区域；

根据第一目标区域，确定包含第一目标区域且大于第一目标区域的第二目标区域；

在第二目标区域内统计直方图，并根据直方图计算对比度；

若对比度大于阈值，确定红外图像和可见光图像的成像对象为活体。

在本实施例一种可能的实现方式中，第二控制子模块 6141 还用于：

控制图像传感器中的红外传感器进行成像；

若根据红外传感器成像得到的红外图像确定成像对象为活体，控制结构光传感器进行成像。

在本实施例一种可能的实现方式中，第二控制子模块 6141 还用于：

同步控制图像传感器中的红外传感器和结构光传感器进行成像。

在本实施例一种可能的实现方式中，第二控制子模块 6141 还用于：

控制图像传感器中的红外传感器和可见光传感器进行成像；

若根据红外传感器成像得到的红外图像和可见光传感器成像得到的可见光图像确定成像对象为活体，控制结构光传感器进行成像。

上述应用程序的安全控制装置中各个模块的划分仅用于举例说明，在其他实施例中，可将应用程序的安全控制装置按照需要划分为不同的模块，以完成上述应用程序的安全控制装置的全部或部分功能。

需要说明的是，前述对应用程序的安全控制方法实施例的解释说明，也适用于该实施例的应用程序的安全控制装置，故在此不再赘述。

本申请实施例的应用程序的安全控制装置 60，通过确定当前对应用程序操作的操作类型，在操作类型为预设操作类型时，调用预设服务，预设服务用于使应用程序运行于可信执行环境中，以及在可信执行环境中控制应用程序执行与预设操作类型对应的身份验证服务，能够在保障对设备操作安全性的同时，提升一些操作类型对应服务的执行效率，提升用户使用体验度。

本申请实施例还提出一种移动终端 80。

图 14 为本申请实施例提供的一种移动终端 80 的结构示意图。

本实施例中，移动终端 80 包括但不限于手机、平板电脑等设备。

如图 14 所示，该移动终端 80 包括：成像传感器 810、存储器 820、MCU 830、处理器 840 以及存储在存储器 820 上并可在处理器 840 的可信执行环境下运行的可执行程序代码（图 14 中未示出）。

其中，MCU 830 为可信执行环境的专用硬件，与成像传感器 810 和处理器 840 连接，用于控制成像传感器 810 进行成像，并将成像数据发送至处理器 840。

处理器 840 执行可执行程序代码时，实现前述实施例的应用程序的安全控制方法。

在本实施例一种可能的实现方式中，MCU 830 与处理器 840 之间通过加密方式进行通信。

本实施例中，MCU 830 可采取行列像素点置乱方法对图像进行加密。具体而言，MCU 830 可将原图中的像素信息进行了重新排布，处理器可通过一一对应的关系可以恢复原来的图像。

MCU 830 也可采用基于混沌的图像加密方法，具体地，产生 2 个 Logistic 混沌序列，改造 2 个 Logistic，得到两个 y 序列，由 y1 和 y2 序列对原图像进行值替代加密。其中，秘钥为混沌系统的初始状态值。

在本实施例一种可能的实现方式中，成像传感器 810 可包括：红外传感器、结构光图像传感器和可见光图像传感器。

其中，红外传感器包括激光摄像头和泛光灯；结构光图像传感器包括：镭射灯，以及与红外传感器共用的激光摄像头，可见光图像传感器包括：可见光摄像头。

在本实施例一种可能的实现方式中，MCU 830 包括 PWM、深度引擎、总线接口以及 RAM。

其中，PWM 用于调制泛光灯以使发出红外光，以及调制镭射灯以发出激光；

激光摄像头，用于采集成像对象的结构光图像；

深度引擎，用于根据结构光图像，计算获得成像对象对应的深度数据；以及

总线接口，用于将深度数据发送至处理器 840，并由处理器 840 在可信执行环境中执行应用程序中的身份验证服务。

例如，可根据深度数据进行身份验证，具体过程可参见上述实施例，在此不再赘述。

如图 15，本申请实施例还提出一种计算机可读存储介质 1000，其上存储有计算机程序 2000，该程序 2000 被处理器 3000 执行时实现如前述任意实施例的应用程序的安全控制方法。

需要说明的是，在本申请的描述中，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。此外，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本申请的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本申请的实施例所属技术领域的技术人员所理解。

应当理解，本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

此外，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模块中，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模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请的限制，本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。

权利要求书

1. 一种应用程序的安全控制方法，其特征在于，所述方法包括步骤：

判断所述应用程序的运行信息是否符合预设的安全控制条件；

若符合，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中；及

在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务。

2. 根据权利要求 1 所述的应用程序的安全控制方法，其特征在于，

所述判断所述应用程序的运行信息是否符合预设的安全控制条件，包括：确定所述应用程序是否为预设应用程序；

所述若符合，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中，包括：若为所述预设应用程序，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中；

所述在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务，包括：在所述可信执行环境中执行所述应用程序中的身份验证服务。

3.根据权利要求 2 所述的应用程序的安全控制方法，其特征在于，所述在所述可信执行环境中执行所述应用程序中的身份验证服务，包括：

通过所述可信执行环境的专用硬件，控制图像传感器进行成像，其中，所述图像传感器包括结构光传感器；

通过所述专用硬件，获取图像传感器成像得到的成像数据；

根据所述成像数据，对成像对象进行活体检测；

若活体检测通过，将所述成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；

当所述结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

4. 根据权利要求 3 所述的应用程序的安全控制方法，其特征在于，所述图像传感器还包括红外传感器，所述成像数据包括红外图像，所述根据所述成像数据，对成像对象进行活体检测，包括：

根据所述成像数据中的红外图像，识别所述红外图像的成像对象是否为活体。

5. 根据权利要求 4 所述的应用程序的安全控制方法，其特征在于，所述根据所述成像数据中的红外图像，识别所述红外图像的成像对象是否为活体，包括：

从所述红外图像中提取成像轮廓；

根据处于所述成像轮廓内部的局部红外图像，确定所述红外图像的成像对象的温度；

若所述成像轮廓与预设人脸轮廓匹配，且所述红外图像的成像对象的温度处于体温范围内，确定所述红外图像的成像对象为活体。

6. 根据权利要求 3 所述的应用程序的安全控制方法，其特征在于，所述图像传感器还包括红外传感器和可见光传感器，所述成像数据包括红外图像和可见光图像，所述根据所述成像数据，对成像对象进行活体检测，包括：

在所述可见光图像中识别人脸区域，并在所述红外图像中，确定与所述人脸区域相对应的第一目标区域；

根据所述第一目标区域，确定包含所述第一目标区域且大于所述第一目标区域的第二目标区域；

在所述第二目标区域内统计直方图，并根据所述直方图计算对比度；

若所述对比度大于阈值，确定所述红外图像和所述可见光图像的成像对象为活体。

7. 根据权利要求 3-6 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像传感器进行成像，包括：

控制图像传感器中的红外传感器进行成像；

若根据所述红外传感器成像得到的红外图像确定成像对象为活体，控制结构光传感器进行成像。

8. 根据权利要求 3-6 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像传

感器进行成像，包括：

同步控制图像传感器中的红外传感器和结构光传感器进行成像。

9. 根据权利要求 3-6 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像传感器进行成像，包括：

控制图像传感器中的红外传感器和可见光传感器进行成像；

若根据所述红外传感器成像得到的红外图像和所述可见光传感器成像得到的可将图像确定成像对象为活体，控制结构光传感器进行成像。

10. 根据权利要求 1 所述的应用程序的安全控制方法，其特征在于，

所述判断所述应用程序的运行信息是否符合预设的安全控制条件，包括：确定当前对所述应用程序操作的操作类型；及判断所述操作类型是否为预设操作类型；

所述若符合，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中，包括：若为所述预设操作类型，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中；

所述在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务，包括：在所述可信执行环境中控制所述应用程序执行与所述预设操作类型对应的身份验证服务。

11. 根据权利要求 10 所述的应用程序的安全控制方法，其特征在于，在所述判断所述操作类型是否为预设操作类型之后，所述安全控制方法还包括：

若不为所述预设操作类型，则在第一执行环境中控制所述应用程序执行与所述操作类型对应的服务，所述第一执行环境为与所述可信执行环境不同的执行环境。

12. 根据权利要求 10 所述的应用程序的安全控制方法，其特征在于，所述在所述可信执行环境中控制所述应用程序执行与所述预设操作类型对应的身份验证服务，包括：

通过所述可信执行环境的专用硬件，控制图像传感器进行成像，其中，所述图像传感器包括结构光传感器；

通过所述专用硬件，获取图像传感器成像得到的成像数据；

根据所述成像数据，对成像对象进行活体检测；

若活体检测通过，将所述成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；

当所述结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

13. 根据权利要求 12 所述的应用程序的安全控制方法，其特征在于，所述图像传感器还包括红外传感器，所述成像数据包括红外图像，所述根据所述成像数据，对成像对象进行活体检测，包括：

根据所述成像数据中的红外图像，识别所述红外图像的成像对象是否为活体。

14. 根据权利要求 13 所述的应用程序的安全控制方法，其特征在于，所述根据所述成像数据中的红外图像，识别所述红外图像的成像对象是否为活体，包括：

从所述红外图像中提取成像轮廓；

根据处于所述成像轮廓内部的局部红外图像，确定所述红外图像的成像对象的温度；

若所述成像轮廓与预设人脸轮廓匹配，且所述红外图像的成像对象的温度处于体温范围内，确定所述红外图像的成像对象为活体。

15. 根据权利要求 12 所述的应用程序的安全控制方法，其特征在于，所述图像传感器还包括红外传感器和可见光传感器，所述成像数据包括红外图像和可见光图像，所述根据所述成像数据，对成像对象进行活体检测，包括：

在所述可见光图像中识别人脸区域，并在所述红外图像中，确定与所述人脸区域相对应的第一目标区域；

根据所述第一目标区域，确定包含所述第一目标区域且大于所述第一目标区域的第二目标区域；

在所述第二目标区域内统计直方图，并根据所述直方图计算对比度；

若所述对比度大于阈值，确定所述红外图像和所述可见光图像的成像对象为活体。

16. 根据权利要求 12-15 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像

传感器进行成像，包括：

控制图像传感器中的红外传感器进行成像；

若根据所述红外传感器成像得到的红外图像确定成像对象为活体，控制结构光传感器进行成像。

17. 根据权利要求 12-15 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像传感器进行成像，包括：

同步控制图像传感器中的红外传感器和结构光传感器进行成像。

18. 根据权利要求 12-15 任一项所述的应用程序的安全控制方法，其特征在于，所述控制图像传感器进行成像，包括：

控制图像传感器中的红外传感器和可见光传感器进行成像；

若根据所述红外传感器成像得到的红外图像和所述可见光传感器成像得到的可将图像确定成像对象为活体，控制结构光传感器进行成像。

19. 一种应用程序的安全控制装置，其特征在于，所述装置具有可信执行环境，所述装置包括：

判断总模块，用于判断所述应用程序的运行信息是否符合预设的安全控制条件；

调用总模块，用于若判断符合所述安全控制条件，则调用预设服务，所述预设服务用于使所述应用程序运行于所述可信执行环境中；及

执行总模块，用于在所述可信执行环境执行与所述应用程序的运行信息对应的身份验证服务。

20. 根据权利要求 19 所述的应用程序的安全控制装置，其特征在于，所述判断总模块包括：第一确认模块，用于确定所述应用程序是否为预设应用程序；

所述调用总模块包括：第一调用模块，用于在为所述预设应用程序，则调用预设服务，所述预设服务用于使所述应用程序运行于可信执行环境中；

所述执行总模块包括：第一执行模块，用于在所述可信执行环境中执行所述应用程序中的身份验证服务。

21. 根据权利要求 20 所述的应用程序的安全控制装置，其特征在于，所述第一执行模块，包括：

第一控制子模块，用于通过所述可信执行环境的专用硬件，控制图像传感器进行成像，其中，所述图像传感器包括结构光传感器；

第一获取子模块，用于通过所述专用硬件，获取图像传感器成像得到的成像数据；

第一检测子模块，用于根据所述成像数据，进行活体检测；

第一匹配子模块，用于若活体检测通过，将所述成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；当所述结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

22. 根据权利要求 19 所述的应用程序的安全控制装置，其特征在于，所述判断总模块包括：第二确认模块及判断模块，所述第二确认模块用于确定当前对所述应用程序操作的操作类型，所述判断模块用于判断所述操作类型是否为预设操作类型；

所述调用总模块包括：第二调用模块，用于在为所述预设操作类型时，调用预设服务，所述预设服务用于使所述应用程序运行于所述可信执行环境中；

所述执行总模块包括：第二执行模块，用于在所述可信执行环境中控制所述应用程序执行与所述预设操作类型对应的身份验证服务。

23. 根据权利要求 22 所述的应用程序的安全控制装置，其特征在于，所述第二执行模块，还用于：

若不为所述预设操作类型，则在第一执行环境中控制所述应用程序执行与所述操作类型对应的服务，所述第一执行环境为与所述可信执行环境不同的执行环境。

24. 根据权利要求 22 或 23 所述的应用程序的安全控制装置，其特征在于，所述第二执行模块，包括：

第二控制子模块，用于通过所述可信执行环境的专用硬件，控制图像传感器进行成像，其中，所述图像传感器包括结构光传感器；

第二获取子模块，用于通过所述专用硬件，获取图像传感器成像得到的成像数据；

第二检测子模块，用于根据所述成像数据，进行活体检测；

第二匹配子模块，用于若活体检测通过，将所述成像数据中的结构光深度模型，与预设人脸深度模型进行匹配；当所述结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过。

25. 一种移动终端，其特征在于，包括：成像传感器、存储器、微处理器单元 MCU、处理器及存储在所述存储器上并可在所述处理器的可信执行环境下运行的可执行程序代码；所述 MCU，为所述可信执行环境的专用硬件，与所述成像传感器和所述处理器连接，用于控制所述成像传感器进行成像，并将成像数据发送至所述处理器；所述处理器执行所述可执行程序代码时，实现如权利要求 1-18 中任一项所述的应用程序的安全控制方法。

26. 根据权利要求 25 所述的移动终端，其特征在于，所述 MCU 与所述处理器之间通过加密方式进行通信。

27. 一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求 1-18 中任一项所述的应用程序的安全控制方法。

附图

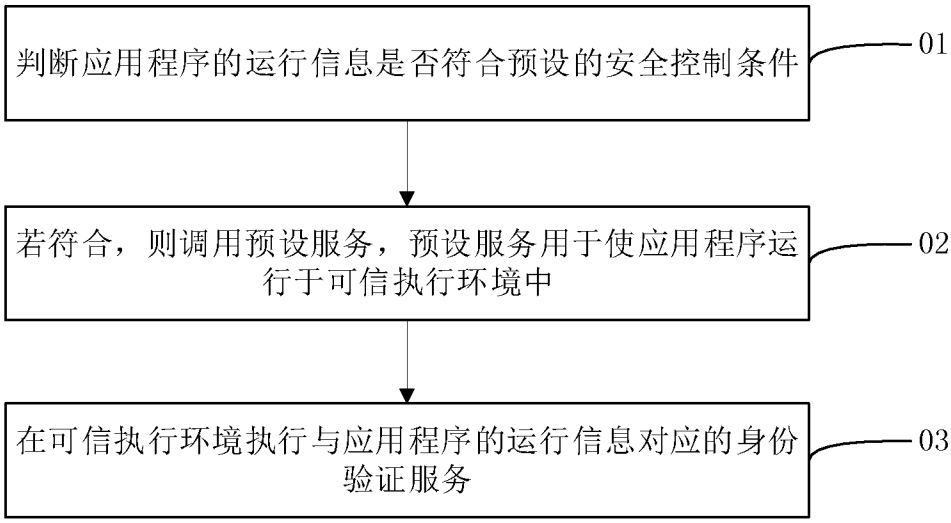
判断应用程序的运行信息是否符合预设的安全控制条件
01
若符合，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中
02
在可信执行环境执行与应用程序的运行信息对应的身份验证服务
03

图 1

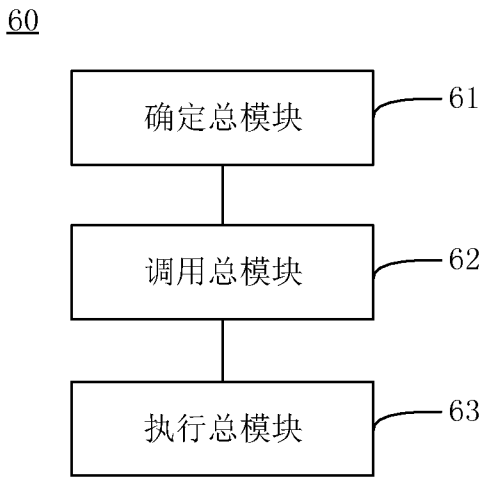
60
确定总模块
61
调用总模块
62
执行总模块
63

图 2

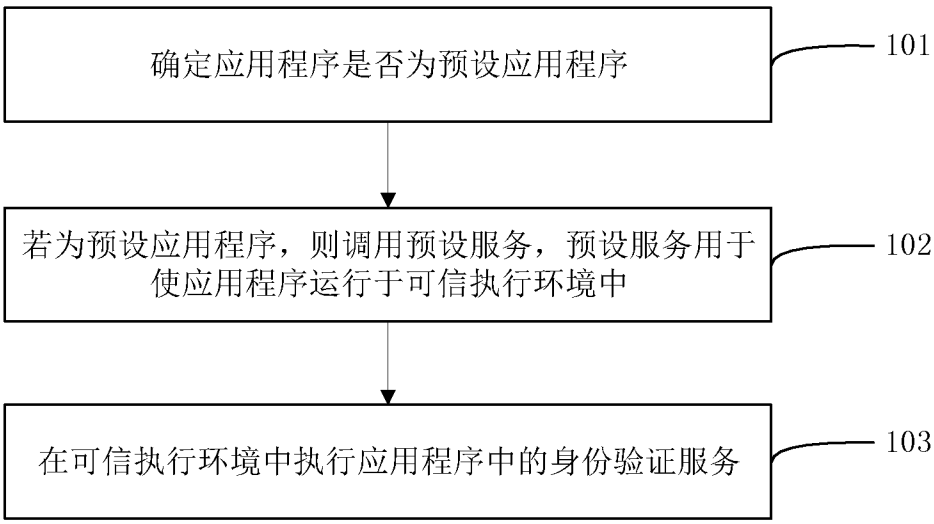
确定应用程序是否为预设应用程序
101
若为预设应用程序，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中
102
在可信执行环境中执行应用程序中的身份验证服务
103

图 3

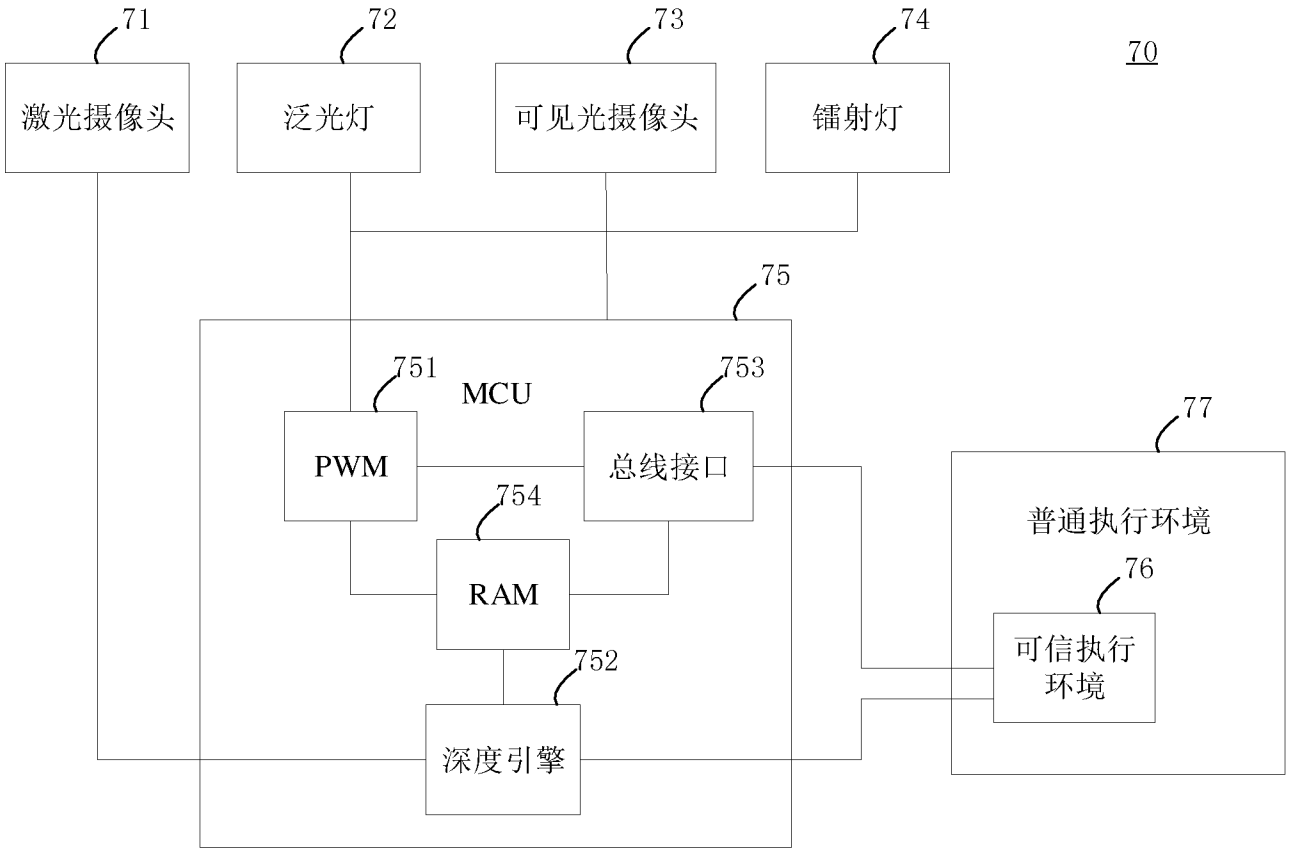
71
72
73
74
70
激光摄像头
泛光灯
可见光摄像头
镭射灯
75
751
MCU
753
PWM
总线接口
77
普通执行环境
754
RAM
76
可信执行环境
752
深度引擎

图 4

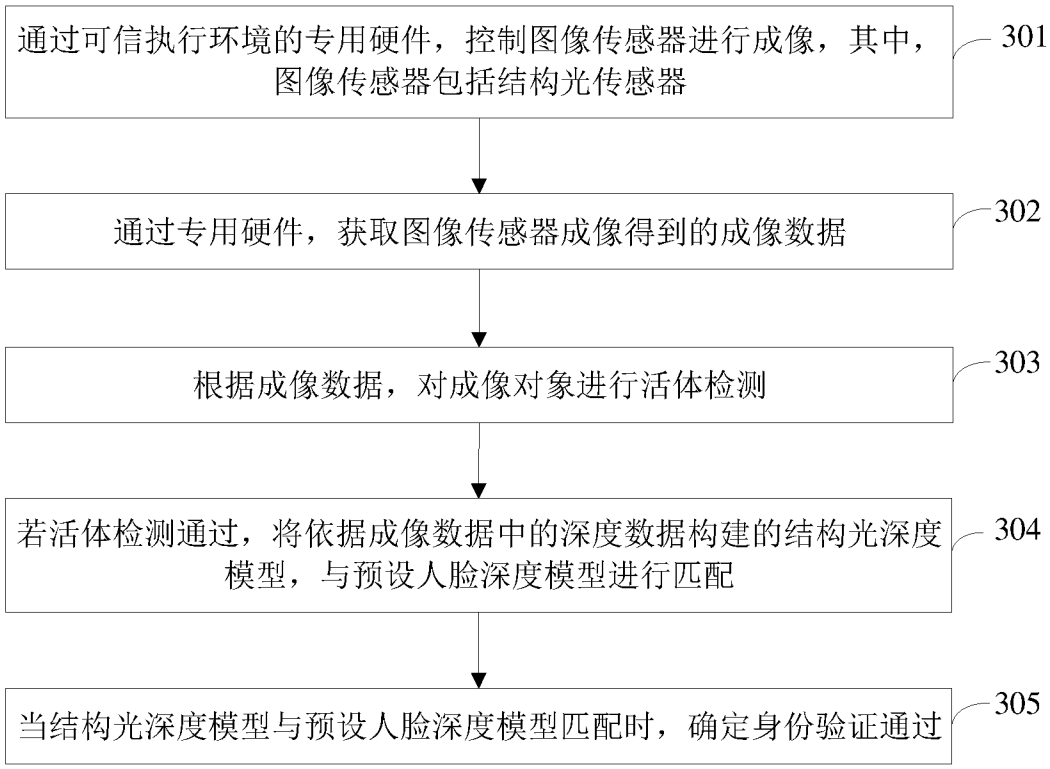
通过可信执行环境的专用硬件，控制图像传感器进行成像，其中，图像传感器包括结构光传感器
301
通过专用硬件，获取图像传感器成像得到的成像数据
302
根据成像数据，对成像对象进行活体检测
303
若活体检测通过，将依据成像数据中的深度数据构建的结构光深度模型，与预设人脸深度模型进行匹配
304
当结构光深度模型与预设人脸深度模型匹配时，确定身份验证通过
305

图 5

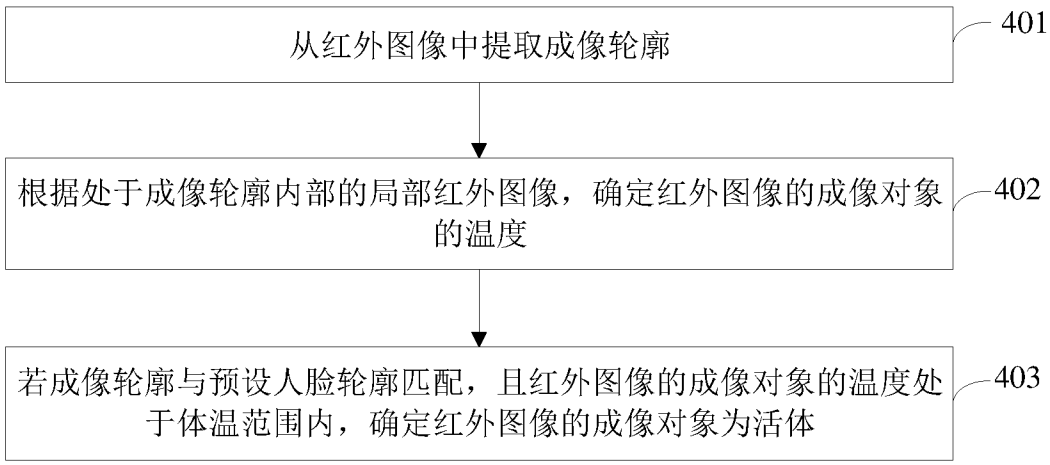
从红外图像中提取成像轮廓
401
根据处于成像轮廓内部的局部红外图像，确定红外图像的成像对象的温度
402
若成像轮廓与预设人脸轮廓匹配，且红外图像的成像对象的温度处于体温范围内，确定红外图像的成像对象为活体
403

图 6

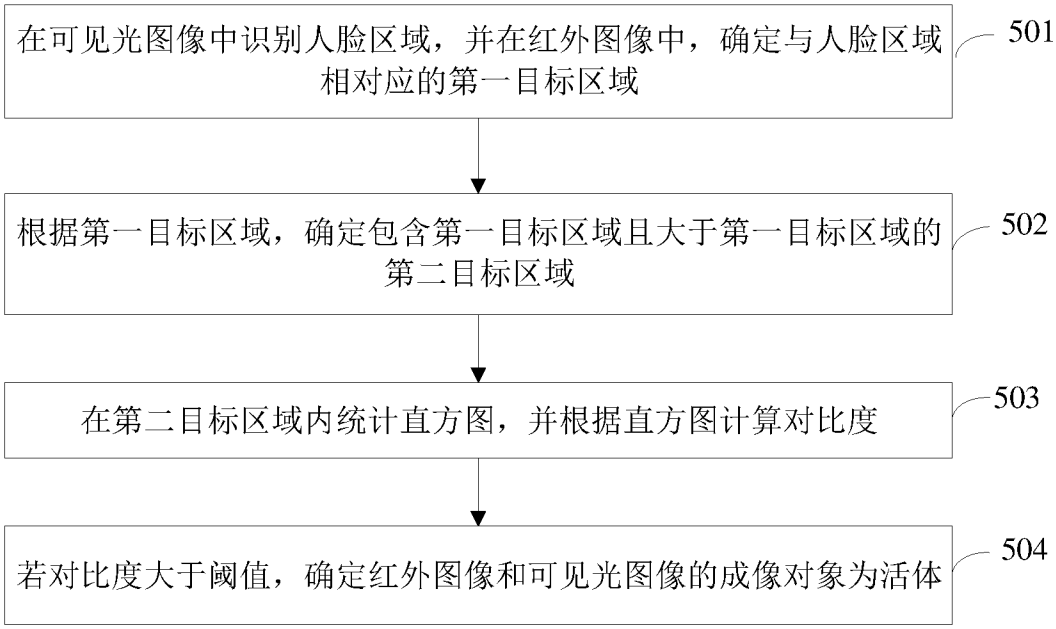
在可见光图像中识别人脸区域，并在红外图像中，确定与人脸区域相对应的第一目标区域
501
根据第一目标区域，确定包含第一目标区域且大于第一目标区域的第二目标区域
502
在第二目标区域内统计直方图，并根据直方图计算对比度
503
若对比度大于阈值，确定红外图像和可见光图像的成像对象为活体
504

图 7

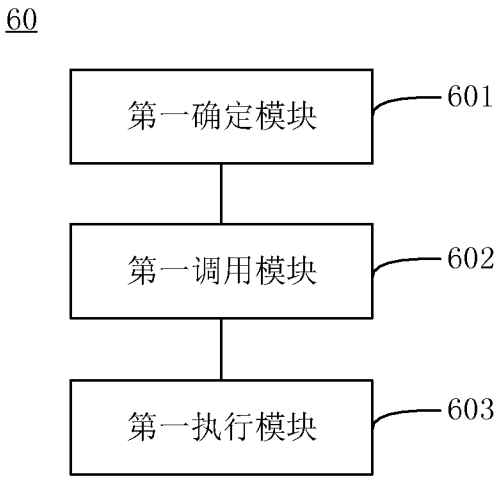
60
第一确定模块
601
第一调用模块
602
第一执行模块
603

图 8

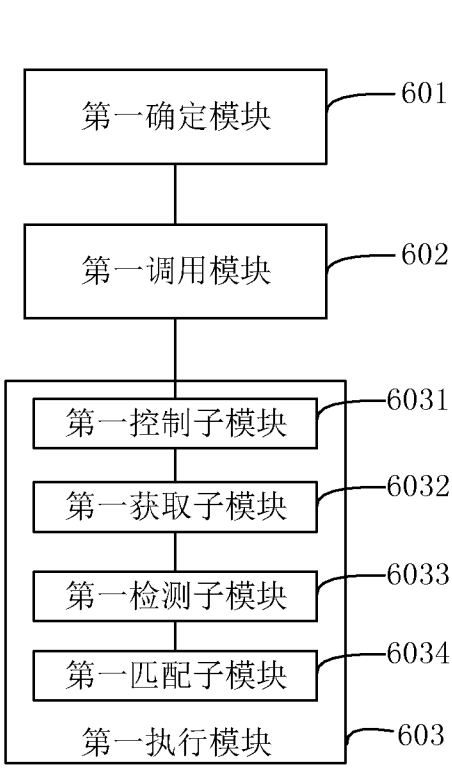
60
第一确定模块
601
第一调用模块
602
第一控制子模块
6031
第一获取子模块
6032
第一检测子模块
6033
第一匹配子模块
6034
第一执行模块
603

图 9

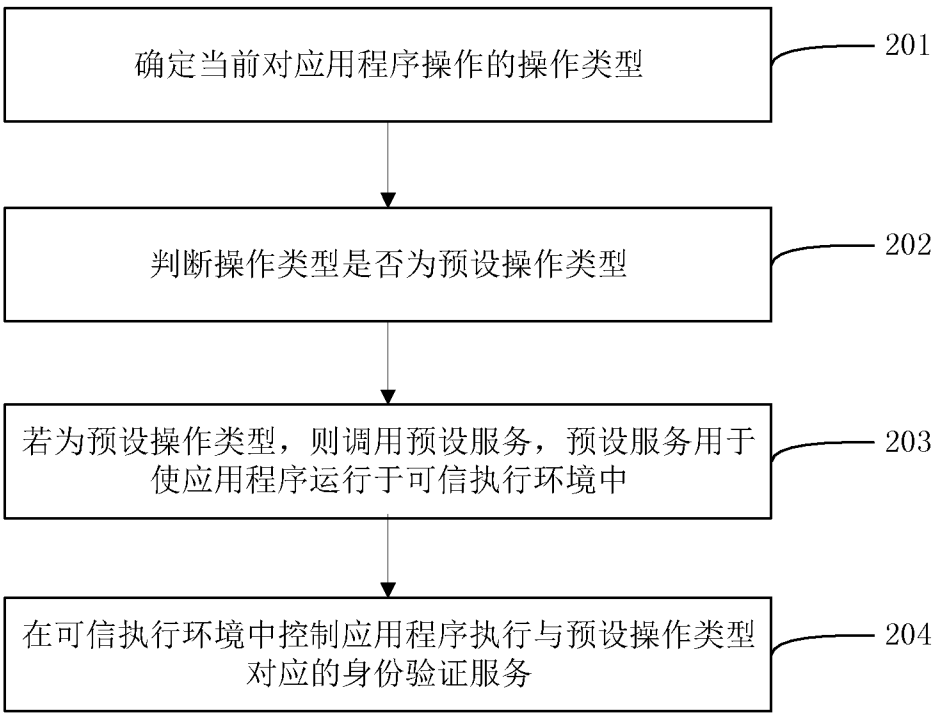
确定当前对应用程序操作的操作类型
201
判断操作类型是否为预设操作类型
202
若为预设操作类型，则调用预设服务，预设服务用于使应用程序运行于可信执行环境中
203
在可信执行环境中控制应用程序执行与预设操作类型对应的身份验证服务
204

图 10

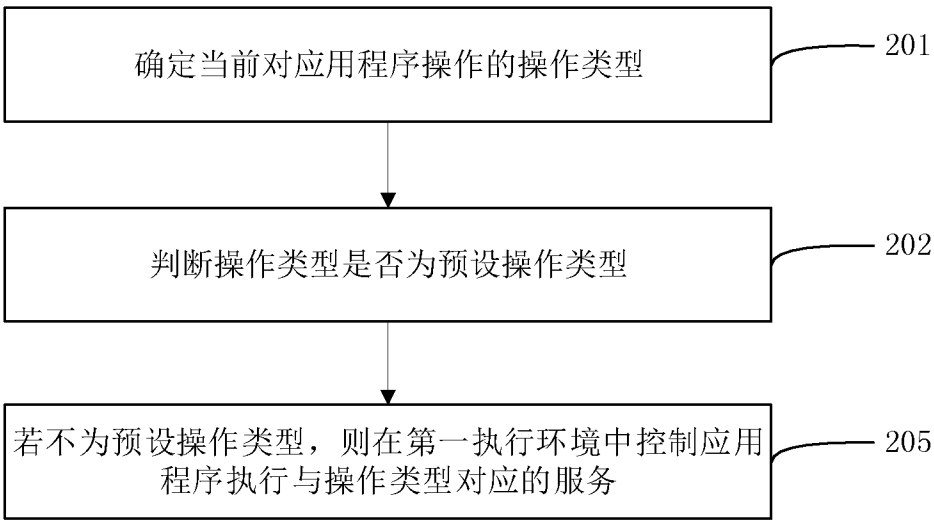
确定当前对应用程序操作的操作类型
201
判断操作类型是否为预设操作类型
202
若不为预设操作类型，则在第一执行环境中控制应用程序执行与操作类型对应的服务
205

图 11

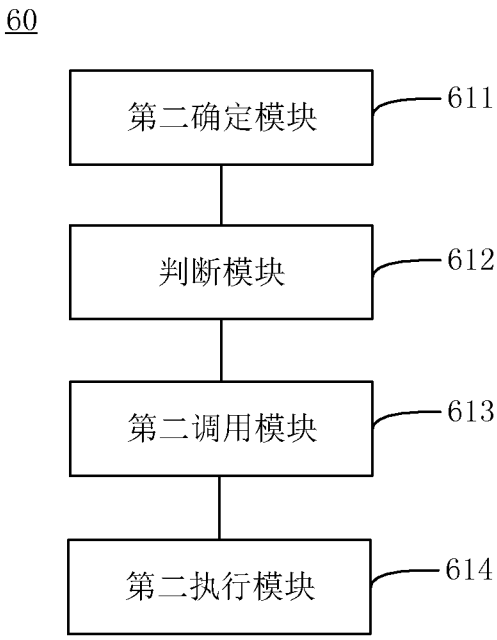
60
第二确定模块
611
判断模块
612
第二调用模块
613
第二执行模块
614

图 12

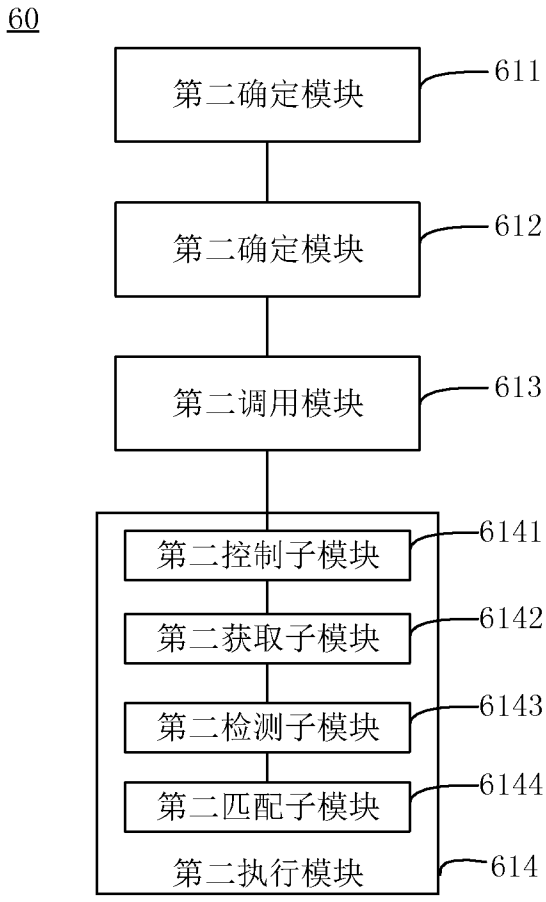
60
第二确定模块
611
第二确定模块
612
第二调用模块
613
第二控制子模块
6141
第二获取子模块
6142
第二检测子模块
6143
第二匹配子模块
6144
第二执行模块
614

图 13

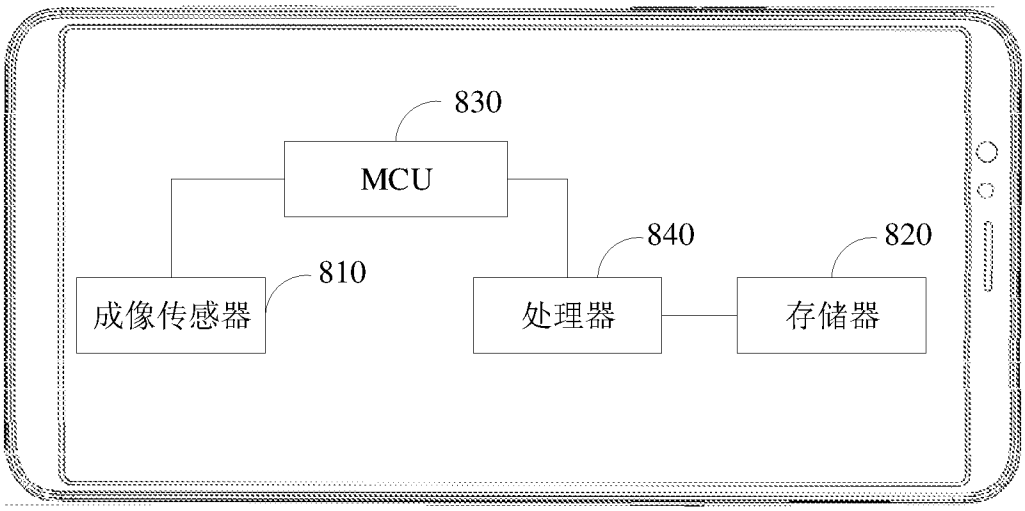
80
830
MCU
840
820
810
成像传感器
处理器
存储器

图 14

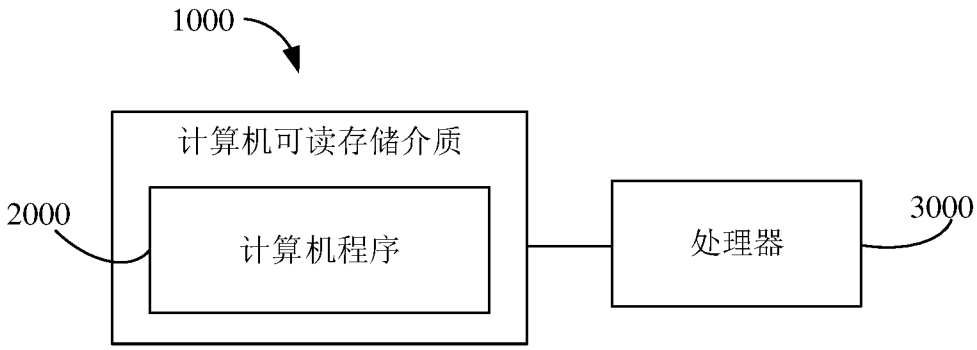
1000
计算机可读存储介质
2000
计算机程序
处理器
3000

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/081739

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/12(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI, IEEE: 应用程序, 可信, 安全, 环境, 身份验证, 身份认证, 人脸, 识别, 活体, 红外, 可见光, trust, security, safe, zone, environment, identity, verification, authentication, validation, facial, recognition, biometric, infrared, image

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108595942 A (OPPO (GUANGDONG) MOBILE COMMUNICATION CO., LTD.) 28 September 2018 (2018-09-28) claims 1-13	1-9, 19-21, 25-27
PX	CN 108614958 A (OPPO (GUANGDONG) MOBILE COMMUNICATION CO., LTD.) 02 October 2018 (2018-10-02) claims 1-15	1, 10-19, 22-27
X	CN 106027257 A (BEIJING YUANXIN TECHNOLOGY CO., LTD.) 12 October 2016 (2016-10-12) description, paragraph [0009]	1, 19, 25-27
Y	CN 106027257 A (BEIJING YUANXIN TECHNOLOGY CO., LTD.) 12 October 2016 (2016-10-12) description, paragraph [0009]	2-18, 21-24
Y	CN 106529275 A (VIVO MOBILE COMMUNICATION CO., LTD.) 22 March 2017 (2017-03-22) description, paragraphs [0007]-[0010]	2-9, 20-21

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 2019	**09 July 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106778607 A (GUOZHENGTONG TECHNOLOGY CO., LTD.) 31 May 2017 (2017-05-31) description, paragraphs [0044]-[0048]	3-9, 12-18
Y	CN 107392055 A (GIONEE COMMUNICATION EQUIPMENT CO., LTD.) 24 November 2017 (2017-11-24) description, paragraph [0042]	10-18, 22-24
A	CN 101047701 A (WATCHDATA SYSTEM CO., LTD.) 03 October 2007 (2007-10-03) entire document	1-27
A	US 2015254622 A1 (PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.) 10 September 2015 (2015-09-10) entire document	1-27
A	US 2018053005 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 22 February 2018 (2018-02-22) entire document	1-27

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/081739

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108595942	A	28 September 2018	None			
CN	108614958	A	02 October 2018	None			
CN	106027257	A	12 October 2016	None			
CN	106529275	A	22 March 2017	None			
CN	106778607	A	31 May 2017	None			
CN	107392055	A	24 November 2017	None			
CN	101047701	A	03 October 2007	None			
US	2015254622	A1	10 September 2015	JP	2015171105	A	28 September 2015
US	2018053005	A1	22 February 2018	WO	2018039099	A1	01 March 2018

国际检索报告

国际申请号
PCT/CN2019/081739

A. 主题的分类

G06F 21/12(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,EPODOC,CNPAT,CNKI,IEEE: 应用程序，可信，安全，环境，身份验证，身份认证，人脸，识别，活体，红外，可见光， trust, security, safe, zone, environment, identity, verification, authentication, validation, facial, recognition, biometric, infrared, image

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 108595942 A (OPPO广东移动通信有限公司) 2018年 9月 28日 (2018-09-28) 权利要求1-13	1-9，19-21，25-27
PX	CN 108614958 A (OPPO广东移动通信有限公司) 2018年 10月 2日 (2018-10-02) 权利要求1-15	1，10-19，22-27
X	CN 106027257 A (北京元心科技有限公司) 2016年 10月 12日 (2016-10-12) 说明书第[0009]段	1，19，25-27
Y	CN 106027257 A (北京元心科技有限公司) 2016年 10月 12日 (2016-10-12) 说明书第[0009]段	2-18，21-24
Y	CN 106529275 A (维沃移动通信有限公司) 2017年 3月 22日 (2017-03-22) 说明书第[0007]-[0010]段	2-9，20-21
Y	CN 106778607 A (国政通科技股份有限公司) 2017年 5月 31日 (2017-05-31) 说明书第[0044]-[0048]段	3-9，12-18
Y	CN 107392055 A (深圳市金立通信设备有限公司) 2017年 11月 24日 (2017-11-24) 说明书第[0042]段	10-18，22-24

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 6月 27日	2019年 7月 9日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 曾璇 电话号码 86-(10)-53961373

国际检索报告

国际申请号
PCT/CN2019/081739

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 101047701 A (北京握奇数据系统有限公司) 2007年 10月 3日 (2007 - 10 - 03) 全文	1-27
A	US 2015254622 A1 (PANASONIC INTELLECTUAL PROPERTY MANAGEMENT CO., LTD.) 2015年 9月 10日 (2015 - 09 - 10) 全文	1-27
A	US 2018053005 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2018年 2月 22日 (2018 - 02 - 22) 全文	1-27

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/081739

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108595942	A	2018年 9月 28日	无			
CN	108614958	A	2018年 10月 2日	无			
CN	106027257	A	2016年 10月 12日	无			
CN	106529275	A	2017年 3月 22日	无			
CN	106778607	A	2017年 5月 31日	无			
CN	107392055	A	2017年 11月 24日	无			
CN	101047701	A	2007年 10月 3日	无			
US	2015254622	A1	2015年 9月 10日	JP	2015171105	A	2015年 9月 28日
US	2018053005	A1	2018年 2月 22日	WO	2018039099	A1	2018年 3月 1日