

(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
2024 年 12 月 19 日 (19.12.2024)



(10) 国际公布号
WO 2024/255336 A1

(51) 国际专利分类号:
G06F 9/445 (2018.01)

(21) 国际申请号: PCT/CN2024/080037

(22) 国际申请日: 2024 年 3 月 5 日 (05.03.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310695930.2 2023年6月12日 (12.06.2023) CN

(71) 申请人: 荣耀终端有限公司 (HONOR DEVICE CO., LTD.) [CN/CN]; 中国广东省深圳市福田区香蜜湖街道红荔西路 8089 号深业中城 6 号楼 A 单元 3401, Guangdong 518040 (CN)。

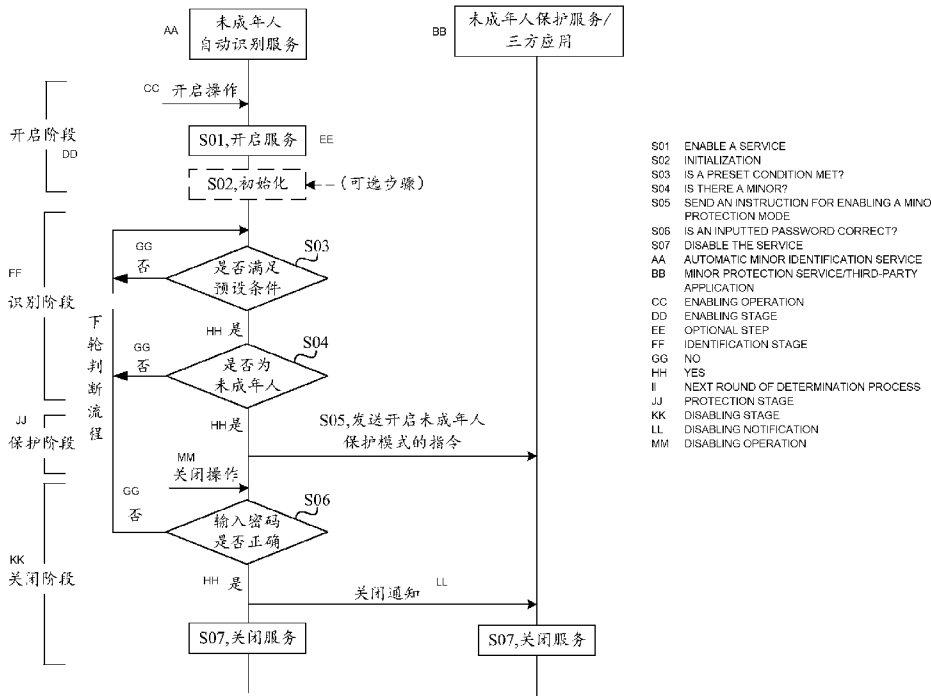
(72) 发明人: 赵晓娜 (ZHAO, Xiaona); 中国广东省深圳市福田区香蜜湖街道红荔西路 8089 号深业中城 6 号楼 A 单元 3401, Guangdong 518040 (CN)。曾勇波 (ZENG, Yongbo); 中国广东省深圳市福田区香蜜湖街道红荔西路 8089 号深业中城 6 号楼 A 单元 3401, Guangdong 518040 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司 (SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市福田区莲花街道紫荆社区深南大道 6008 号深圳特区报业大厦 33 层, Guangdong 518034 (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,

(54) Title: AUTOMATIC MINOR IDENTIFICATION AND PROTECTION METHOD, AND TERMINAL DEVICE AND STORAGE MEDIUM

(54) 发明名称: 未成年人自动识别和保护方法、终端设备及存储介质



(57) Abstract: The present application relates to the technical field of terminals. Provided are an automatic minor identification and protection method, and a terminal device and a storage medium. In the solution of the present application, a terminal device provides a user with a configuration switch of an automatic minor identification service. After the user triggers the enabling of the automatic minor identification service by means of an operation on an automatic minor identification service option, the automatic minor identification service can detect whether a preset condition for triggering minor identification is met, when the preset condition is met, whether the current user is a minor is identified, and when it is identified that the current user is a minor, a minor protection service or a three-party

CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, IE, IS, IT, LT, LU, LV, MC, ME, 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))。

application is triggered to execute a minor protection operation. In this way, a guardian only needs to perform one operation of enabling the automatic minor identification service, such that when it is identified that the current user is a minor, the minor protection operation can be automatically executed, and there is no need to manually and frequently enable or disable a minor protection mode.

(57) 摘要: 本申请提供一种未成年人自动识别和保护方法、终端设备及存储介质, 涉及终端技术领域。在本申请方案中, 终端设备向用户提供了未成年人自动识别服务的配置开关。在用户通过对未成年人自动识别服务选项的操作触发启用未成年人自动识别服务后, 未成年人自动识别服务可以检测是否满足触发未成年人识别的预设条件, 当满足预设条件时会识别当前用户是否为未成年人, 并在识别到当前用户为未成年人的情况下触发未成年人保护服务或三方应用执行未成年人保护操作。如此, 监护人仅需要一次开启未成年人自动识别服务的操作, 就可以在识别到当前用户为未成年人的情况下自动执行未成年人保护操作, 不用手动频繁开启或关闭未成年人保护模式。

说明书

未成年人自动识别和保护方法、终端设备及存储介质

本申请要求于 2023 年 06 月 12 日提交国家知识产权局、申请号为 202310695930.2、申请名称为“未成年人自动识别和保护方法、终端设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及终端技术领域，尤其涉及一种未成年人自动识别和保护方法、终端设备及存储介质。

背景技术

随着终端制造技术的发展，终端设备的普及率越来越高。未成年人逐渐成为使用终端设备的重要群体。未成年人的自制力薄弱，容易长时间沉溺网络游戏等移动互联网服务，或者在未得到家长授权的情况下对游戏充值、直播打赏等，不良的网络环境影响到了未成年人的健康成长。

目前，法律要求对终端产品及服务提供者、个人信息处理者、智能终端制作者提出安装未成年人保护软件或设置未成年人保护模式的要求。在常规的产品设计方案中，监护人需要在孩子使用终端设备时手动开启未成年人保护模式，再在自己使用终端设备时手动关闭未成年人保护模式。手动频繁开启或关闭未成年人保护模式，操作繁琐，降低使用体验。

发明内容

本申请提供一种未成年人自动识别和保护方法、终端设备及存储介质，解决了手动频繁开启或关闭未成年人保护模式导致操作繁琐的技术问题。

为达到上述目的，本申请采用如下技术方案：

第一方面，本申请实施例提供一种未成年人自动识别和保护方法。该方法可以应用于终端设备，该终端设备设置有未成年人自动识别服务、未成年人保护服务和三方应用。该方法可以包括：响应于用户的第一操作，终端设备开启未成年人自动识别服务；未成年人自动识别服务检测是否满足触发未成年人识别的条件；在确定终端设备满足触发未成年人识别的条件的前提下，未成年人自动识别服务识别使用终端设备的用户是否为未成年人；若使用终端设备的用户为未成年人，则未成年人自动识别服务向未成年人保护服务或三方应用发送开启未成年人保护模式的指令。

在上述方案中，未成年人自动识别服务可以为在终端设备中预先设置的一个系统级服务，或者为应用商店提供的一个可供下载安装的应用，用于在满足预设条件时触发未成年人识别。应理解，通过在终端设备中预先设置一个未成年人自动识别服务的配置开关，可以供用户选择是否开启该服务。如此，监护人仅需要一次开启未成年人自动识别服务的操作，就可以在在某些情况下自动识别当前正在使用终端设备的用户是否为未成年人，并在识别到该用户为未成年人的情况下触发未成年人保护服务或三方应用自动执行未成年人保护操作，用户不用手动频繁开启或关闭未成年人保护模式，简化了用户操作，提高了用户的使用体验。

在一种可能的实现方式中，上述触发未成年人识别的条件可以包括下述至少一项：

终端设备的亮屏时长大于或等于第一时长；

终端设备在第一时段内亮屏；

应用程序的运行时长大于或等于第二时长；

终端设备在第二时段内运行应用程序；

终端设备正在运行的应用程序属于白名单；

未成年人自动识别服务接收到来自三方应用的未成年人识别请求；

使用终端设备的用户不是机主；

终端设备的使用时长达到固定周期的整数倍。

在上述方案中，触发未成年人识别的条件可以为未成年人自动识别服务的默认设置，也可以为用户的手动设置。当预设条件的数量为多个时，预设条件分析模块可以依次遍历每个条件，以确定是否满足任意一个预设条件，如此，未成年人自动识别服务能够在满足一项或多项预设条件时触发未成年人识别。

在一种可能的实现方式中，白名单包括多个类别的应用程序，该多个类别中的每个类别分别对应一个时长。相应地，终端设备满足触发未成年人识别的条件，包括：终端设备正在运行的第一应用程序属于第一类别，且第一应用程序的运行时长大于或等于与第一类别对应的时长。其中，该第一类别为该多个类别中的任意一个类别。

在上述方案中，白名单由多个待监测应用类别组成。待监测应用可以为支付、游戏和视频播放等各类需要加强未成年人监管的应用。如果在终端设备安装的某个应用属于某个待监管的应用类别，那么这个应用将被自动加入到白名单。当然，未成年人自动识别服务也可以为用户提供一个自定义白名单的功能，方便监护人自行添加应用。应理解，在将白名单作为触发未成年人识别的条件后，只要终端设备检测到正在使用的应用属于白名单，且运行时长达到对应的时长，则可以自动触发未成年人识别。

在一种可能的实现方式中，未成年人自动识别服务和三方应用之间采用预设格式发送预设内容。当触发未成年人识别的条件包括终端设备正在运行的应用程序属于白名单时，未成年人自动识别服务检测是否满足触发未成年人识别的条件，包括：三方应用检测是否满足触发发送未成年人识别请求的条件；三方应用在满足触发发送未成年人识别请求的条件的前提下，向未成年人自动识别服务发送未成年人识别请求；未成年人自动识别服务基于未成年人识别请求判断是否满足触发未成年人识别的条件。相应地，确定终端设备满足触发未成年人识别的条件，包括：若未成年人自动识别服务确定未成年人识别请求符合预设格式，且未成年人识别请求携带预设内容，则未成年人自动识别服务确定满足触发未成年人识别的条件。

在一种可能的实现方式中，在三方应用检测是否满足触发发送未成年人识别请求的条件之前，该方法还可以包括：未成年人自动识别服务向三方应用发送初始化参数，该初始化参数用于指示已开启未成年人自动识别服务。

示例性地，上述触发发送未成年人识别请求的条件可以包括下述至少一项：

三方应用的运行时长大于或等于第三时长；

三方应用的运行时段为预设时段；

三方应用调用支付类应用；

三方应用使用非常用功能；

三方应用的输入密码错误；

三方应用接收到用户关闭未成年人保护模式的操作。

应理解，有些应用不具备自动开启未成年人保护模式的功能，这些应用不能很好的保护未成年人。当某个请求未成年人识别的三方应用满足运行达到预设时长、调用支付类应用、运行时段为预设时段、使用非常用功能和/或输入密码错误等条件时，可以初步确定当前用户

不是监护人。该三方应用通过向未成年人自动识别服务发送请求，可以触发进一步精确识别当前用户是否为未成年人。

在一种可能的实现方式中，未成年人自动识别服务向三方应用发送开启未成年人保护模式的指令，包括：未成年人自动识别服务采用预设格式，向三方应用发送开启未成年人保护模式的指令；三方应用响应于该指令，开启未成年人保护模式。

应理解，在确定当前用户是未成年人的情况下，如果三方应用设置有未成年人保护模式，那么未成年人自动识别服务可以通知三方应用开启未成年人保护模式。

在一种可能的实现方式中，未成年人自动识别服务可以采用下述至少一种方式，识别使用终端设备的用户是否为未成年人：未成年人自动识别服务调用年龄识别接口，由年龄识别接口根据使用终端设备的用户的生物特征信息和设备使用习惯信息中的至少一项确定该用户的年龄；未成年人自动识别服务调用系统账号识别接口，由系统账号识别接口提示用户输入密码，并判断用户输入的密码与预设密码是否匹配；未成年人自动识别服务调用问卷识别接口，由问卷识别接口提示用户回答预设问题，并判断用户的答案与预设答案是否匹配。

其中，通过生物信息验证该用户的年龄的方式，可以包括但不限于：基于人脸、指纹、声音、虹膜等生物特征信息识别年龄的算法来实现，将人脸、指纹等生物特征信息发送给权威身份认证机构平台进行年龄查验等。

应理解，与传统手动频繁开启或关闭未成年人保护模式相比，通过生物特征信息、设备使用习惯信息、密码识别、问卷识别及三方平台识别等方式可以自动识别未成年人，并在识别到当前用户为未成年人的情况下自动开启未成年人保护模式，从而提高了设备智能化程度，简化用户操作步骤。

在一种可能的实现方式中，未成年人自动识别服务向未成年人保护服务发送开启未成年人保护模式的指令，包括：未成年人自动识别服务检测终端设备是否已安装未成年人保护服务。在已安装未成年人保护服务的情况下，未成年人自动识别服务执行下述步骤：直接向未成年人保护服务发送开启未成年人保护模式的指令；或者，在获得监护人的即时授权后，向未成年人保护服务发送开启未成年人保护模式的指令。在未安装未成年人保护服务的情况下，未成年人自动识别服务执行下述步骤：直接向终端设备请求下载安装未成年人保护服务，之后向未成年人保护服务发送开启未成年人保护模式的指令；或者，在获得监护人的即时授权后，向终端设备请求下载安装未成年人保护服务，之后向未成年人保护服务发送开启未成年人保护模式的指令。其中，即时授权为未成年人自动识别服务向终端设备绑定的监护设备发送预警消息后由监护设备返回的授权信息。

应理解，根据终端设备是否已绑定监护设备、是否安装未成年人保护软件，可以执行不同的未成年人保护策略。通过绑定监护设备，可以在识别到使用终端设备的用户为未成年人时，及时向监护人使用的监护设备发出预警消息。需要说明的是，绑定监护设备可以通过蓝牙或 WLAN 等短距离通信技术实现，如，将监护设备的蓝牙媒体接入控制（media access control, MAC）地址或无线局域网（wireless local area network, WLAN）MAC 地址等设备标识符保存或关联到终端设备本地；也可以通过设置监护账号实现，如，将终端设备所登录的账号与监护账号进行关联，从而将监护账号所登录的另一个终端设备作为监护设备。另外，通过安装未成年人保护软件，可以由未成年人保护软件提供过滤不良信息、阻止未经授权购买、拦截欺诈网站等未成年人保护服务。

应理解，上述未成年人自动识别服务在未安装未成年人保护服务的情况下可自动执行上述操作步骤，通过向用户提供配置未成年人自动识别服务的功能开关来实现，若用户打开开

关，表示用户允许未成年人自动识别服务在识别出未成年人后可以自行决定执行上述未成年人保护服务操作。

在一种可能的实现方式中，响应于用户的第一操作，终端设备开启未成年人自动识别服务，包括：响应于用户的第一操作，终端设备判断第一操作是否为首次开启未成年人自动识别服务的操作。当第一操作为首次开启未成年人自动识别服务的操作时，终端设备提示用户输入身份验证信息，并保存用户输入的第一身份验证信息，以及开启未成年人自动识别服务。其中，该身份验证信息包括以下至少一项：用户密码和生物特征识别信息。

相应地，开启未成年人自动识别服务之后，该方法还包括：响应于用户的第二操作，终端设备再次提示用户输入身份验证信息，第二操作为触发关闭未成年人自动识别服务的操作；当用户输入的第二身份验证信息与第一身份验证信息相同时，未成年人自动识别服务向未成年人保护服务或三方应用发送关闭未成年人保护模式的指令。终端设备关闭未成年人自动识别服务。

应理解，在首次开启未成年人自动识别服务时，监护人通过设置独立密码，可以仅授权知道独立密码的监护人关闭未成年人自动识别服务。对于不知道独立密码的未成年人，不能通过对允许自动启动未成年人识别开关的操作关闭该服务，从而更好地起到未成年人保护的作用。另外，在接收到关闭未成年人自动识别服务的操作时，说明监护人可能不需要使用未成年人保护模式，因此可以将未成年人保护模式一并关闭。当然，也可以通过设置生物特征识别信息（如人脸、指纹等）作为一种身份验证方式，仅允许拥有该生物特征识别信息的用户关闭未成年人自动识别服务。

在一种可能的实现方式中，在未成年人自动识别服务识别使用终端设备的用户是否为未成年人之后，该方法还包括：若使用终端设备的用户为成年人，则在已开启未成年人保护模式的情况下，未成年人自动识别服务向未成年人保护服务或三方应用发送关闭未成年人保护模式的指令。

应理解，如果已开启未成年人保护模式，但当前用户为成年人，那么可能对当前用户造成使用不便，因此通过自动关闭未成年人保护模式，简化了操作步骤，方便成年人获得在普通模式（非未成年人保护模式）下的更多使用权限。

第二方面，本申请提供一种装置，该装置包括用于执行上述第一方面中的方法的单元。该装置可对应于执行上述第一方面中描述的未成年人自动识别和保护方法，该装置中的单元的相关描述请参照上述第一方面的描述，为了简洁，在此不再赘述。

其中，上述第一方面描述的未成年人自动识别和保护方法可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的模块或单元。例如，处理模块或单元、显示模块或单元等。

第三方面，本申请提供一种终端设备，该终端设备包括存储器和一个或多个处理器。其中，存储器用于存储计算机程序代码，计算机程序代码包括计算机指令。当计算机指令被处理器执行时，使得终端设备执行第一方面中任一项提供的未成年人自动识别和保护方法。

第四方面，本申请提供一种计算机可读存储介质。该计算机可读存储介质包括计算机指令。当计算机指令在终端设备上运行时，使得该终端设备执行如第一方面及其任一种可能的实现方式提供的未成年人自动识别和保护方法。

第五方面，本申请提供一种计算机程序产品。当计算机程序产品在计算机上运行时，使得计算机执行如第一方面及其任一种可能的实现方式提供的未成年人自动识别和保护方法。

第六方面，本申请提供一种芯片系统。该芯片系统包括一个或多个接口电路和一个或多

个处理器。该接口电路和处理器通过线路互联。该芯片系统可以应用于包括通信模块和存储器的终端设备。该接口电路用于从终端设备的存储器接收信号，并向处理器发送接收到的信号，该信号包括存储器中存储的计算机指令。当处理器执行该计算机指令时，终端设备可以执行如第一方面及其任一种可能的实现方式提供的未成年人自动识别和保护方法。

可以理解，上述提供的第二方面的装置，第三方面的终端设备，第四方面的计算机可读存储介质，第五方面的计算机程序产品及第六方面的芯片系统所能达到的有益效果，可参考如第一方面及其任一种可能的实现方式中的有益效果，此处不再赘述。

附图说明

图1为本申请实施例提供的终端设备的硬件结构示意图；

图2为本申请实施例提供的终端设备的架构示意图；

图3A~图3F为本申请实施例提供的一组开启未成年人自动识别服务的界面示意图；

图4A~图4J为本申请实施例提供的一组设置独立密码的界面示意图；

图5A~图5T为本申请实施例提供的一组设置触发未成年人识别的条件条件的界面示意图；

图6A~图6D为本申请实施例提供的一组设置未成年人识别的条件条件的界面示意图；

图7A~图7H为本申请实施例提供的一组设置未成年人保护操作的界面示意图；

图8为本申请实施例提供的未成年人自动识别和保护方法的总流程示意图；

图9为本申请实施例提供的判断是否满足预设条件的一个示例的流程图；

图10为本申请实施例提供的判断是否满足预设条件的另一个示例的流程图；

图11为本申请实施例提供的判断当前用户是否为未成年人的一个示例的流程图；

图12A~图12D为本申请实施例提供的一组用户输入密码的界面示意图；

图13A~图13D为本申请实施例提供的一组用户回答问题的界面示意图；

图14为本申请实施例提供的开启未成年人保护的一个示例的流程图；

图15为本申请实施例提供的三方应用请求未成年人自动识别的一个示例的流程图。

具体实施方式

为了使本申请实施例的目的、技术方案和优点更加清楚，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，所描述的实施例是本申请一部分实施例，而不是全部的实施例。

在本申请的描述中，除非另有说明，“/”表示或的意思，例如，A/B可以表示A或B。在本申请的描述中，“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。

在本申请的说明书和权利要求书中的术语“第一”和“第二”等是用于区别不同的对象，或者用于区别对同一对象的不同处理，而不是用于描述对象的特定顺序。例如，第一时长和第二时长等是用于区别不同的时长，而不是用于描述时长的特定顺序。在本申请实施例中，“多个”是指两个或两个以上。

本申请提供了一种未成年人自动识别和保护方法。该方法可以应用于终端设备，该终端设备向用户提供了未成年人自动识别服务。在该方法中，在用户通过对未成年人自动识别服务选项的操作触发终端设备启用未成年人自动识别服务后，终端设备可以检测是否满足触发未成年人识别的预设条件，当满足预设条件时识别当前用户是否为未成年人，并在识别到当前用户为未成年人的情况下执行未成年人保护操作。如此，监护人仅需要一次开启未成年人自动识别服务的操作，就可以在识别到当前用户为未成年人的情况下自动执行未成年人保护

操作，不用手动频繁开启或关闭未成年人保护模式，从而简化了操作步骤。

在一些实施例中，终端设备也称为终端（terminal）或用户设备（user equipment, UE）。比如，终端设备可以是手机、个人计算机（personal computer, PC）、平板电脑（Pad）、智慧屏、穿戴式设备、带无线收发功能的电脑、虚拟现实（virtual reality, VR）设备、增强现实（augmented reality, AR）设备、智慧家庭（smart home）中的无线终端或运输安全（transportation safety）中的无线终端等，或者其他具备显示功能的设备或装置。对于终端设备的具体类型，本申请实施例不作任何限制。

为了更好地理解本申请实施例，下面对本申请实施例的终端设备的结构进行介绍。

图1示出了本申请实施例提供的终端设备的硬件结构示意图。

以终端设备为手机100为例。如图1所示，手机100可以包括处理器110，外部存储器接口120，内部存储器121，通用串行总线（universal serial bus, USB）接口130，充电管理模块140，电源管理模块141，电池142，传感器模块150，无线通信模块160，移动通信模块161，天线1，天线2，音频模块170，扬声器170A，受话器170B，麦克风170C，耳机接口170D，按键180，触控屏190，用户标识模块（subscriber identification module, SIM）卡接口191，摄像头192等。

处理器110可以包括一个或多个处理单元，例如，处理器110可以包括中央处理器（central processing unit, CPU）、图形处理器（graphics processing unit, GPU）、应用处理器（application processor, AP）、图像信号处理器（image signal processor, ISP）、神经网络处理器（neural-network processing unit, NPU）、视频编解码器、调制解调处理器（modem），和/或基带处理器（baseband processor）等。在一些实施例中，不同的处理单元可以是独立的器件，也可以集成在一个或多个处理器中。

其中，CPU是信息处理、程序运行的最终执行单元，其主要工作包括处理指令、执行操作、控制时间和处理数据等。CPU可以包括控制器、运算器、高速缓冲存储器，以及用于连接这些部件的总线。控制器是手机100的神经中枢和指挥中心。控制器可以根据指令操作码和时序信号，产生操作控制信号，完成取指令和执行指令的控制。运算器是指进行各种算术和逻辑运算操作的部件。高速缓冲存储器可以保存处理器110刚用过或循环使用的指令或数据。如果处理器110需要再次使用该指令或数据，可从高速缓冲存储器中直接调用。避免了重复存取，减少了处理器110的等待时间，因而提高了系统的效率。

外部存储器接口120可以用于连接外部存储卡，例如Micro SD卡，实现扩展手机100的存储能力。外部存储卡通过外部存储器接口120与处理器110通信，实现数据存储功能。例如，将游戏账号等保存在外部存储卡中。

内部存储器121可以用于存储计算机可执行程序代码，可执行程序代码包括指令。处理器110通过运行存储在内部存储器121的指令，从而执行手机100的各种功能应用以及数据处理。内部存储器121可以包括存储程序区和存储数据区。其中，存储程序区可以存储操作系统，至少一个功能所需的APP，比如，游戏APP、支付APP和视频播放APP等。存储程序区还可以存储安卓应用程序包（Android application package, APK），比如未成年人自动识别服务和未成年人保护服务等。存储数据区还可以存储手机100使用过程中所创建的数据，比如手机100的系统账号、监护人账号等性能参数。此外，内部存储器121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、闪存器件和/或通用闪存存储器（universal flash storage, UFS）等。

USB接口130是符合USB标准规范的接口，具体可以是Mini USB接口、Micro USB接

口和 USB Type C 接口等。USB 接口 130 可以用于连接充电器为手机 100 充电，也可以用于手机 100 与外围设备之间传输数据，还可以用于连接耳机，通过耳机播放音频。USB 接口 130 还可以用于连接其他设备，例如有线鼠标、无线鼠标等。

充电管理模块 140 用于从充电器接收充电输入。其中，充电器可以是无线充电器，也可以是有线充电器。在一些有线充电的实施例中，充电管理模块 140 可以通过 USB 接口 130 接收有线充电器的充电输入。在一些无线充电的实施例中，充电管理模块 140 可以通过手机 100 的无线充电线圈接收无线充电输入。充电管理模块 140 为电池 142 充电的同时，还可以通过电源管理模块 141 为手机 100 供电。

电源管理模块 141 用于连接电池 142、充电管理模块 140 与处理器 110。电源管理模块 141 接收电池 142 和/或充电管理模块 140 的输入。电源管理模块 141 还可以用于监测电池容量，电池循环次数，电池健康状态等参数。

无线通信模块 160 可以提供应用在手机 100 上的包括无线局域网（wireless local area networks, WLAN）（如无线保真（wireless fidelity, Wi-Fi）网络），蓝牙（bluetooth, BT），全球导航卫星系统（global navigation satellite system, GNSS），调频（frequency modulation, FM），近距离无线通信技术（near field communication, NFC），红外技术（infrared, IR）等无线通信的解决方案。无线通信模块 160 可以是集成至少一个通信处理模块的一个或多个器件。无线通信模块 160 经由天线 1 接收电磁波，将电磁波信号调频以及滤波处理，将处理后的信号发送到处理器 110。无线通信模块 160 还可以从处理器 110 接收待发送的信号，对其进行调频，放大，经天线 1 转为电磁波辐射出去。

移动通信模块 161 可以提供应用在手机 100 上的包括 2G/3G/4G/5G 等无线通信的解决方案。移动通信模块 161 可以包括至少一个滤波器，开关，功率放大器，低噪声放大器（low noise amplifier, LNA）等。移动通信模块 161 可以由天线 2 接收电磁波，并对接收的电磁波进行滤波，放大等处理，传送至调制解调处理器进行解调。移动通信模块 161 还可以对经调制解调处理器调制后的信号放大，经天线 2 转为电磁波辐射出去。

手机 100 可以通过音频模块 170，扬声器 170A，受话器 170B，麦克风 170C，耳机接口 170D 等实现音频功能。比如，在用户通过对未成年人自动识别服务选项的操作触发手机 100 启用未成年人自动识别服务后，处理器调用音频模块 170、受话器 170B 和麦克风 170C 等采集当前用户的声音，以根据声纹确定当前用户是否为未成年人。

按键 180 包括开机键，音量键等。按键 180 可以是机械按键或触摸式按键。手机 100 可以接收按键输入，产生与用户设置以及功能控制有关的键信号输入。

触控屏 190 包括触控模块和显示面板。触控模块包括多个压力传感器，用于检测用户触控操作，比如采集用户指纹以确定当前用户是否为未成年人。显示面板可以显示图像和视频等，比如强制关闭当前应用的弹窗等提示消息、与未成年人自动识别服务对应的操作界面。

SIM 卡接口 191 用于连接 SIM 卡。SIM 卡可以通过插入 SIM 卡接口 191，或从 SIM 卡接口 191 拔出，实现和手机 100 的接触和分离。

摄像头 192 可以捕获静态图像或视频。比如，在用户通过对未成年人自动识别服务选项的操作触发手机 100 启用未成年人自动识别服务后，处理器调用摄像头 192 采集当前用户的图像，以确定当前用户是否为未成年人。

上述终端设备的软件系统可以采用分层架构，事件驱动架构，微核架构，微服务架构，或云架构。本发明实施例以分层架构的 Android 系统为例，示例性说明终端设备的软件结构。

图 2 为本申请实施例提供的终端设备的架构示意图。

分层架构将软件分成若干个层，每一层都有清晰的角色和分工。层与层之间通过软件接口通信。在一些实施例中，从上至下将 Android 系统分为：应用程序（application，APP）层和硬件抽象（hardware abstract layer，HAL）层。上述软件架构在硬件层之上运行，硬件层可以包括摄像头、传感器、受话器及麦克风等。

应用程序层，简称为应用层，可以包括一系列的应用程序，比如支付 APP、游戏 APP、视频播放 APP、理财 APP 等三方应用。另外，应用程序层还可以包括未成年人自动识别服务和未成年人保护服务等 APK。需要说明的是，未成年人保护服务也可以是三方应用，应理解，无论是系统应用还是三方应用，未成年人保护服务均具备对终端设备的所有应用程序和进程进行监管的能力。当这些应用程序被运行时，可以通过应用编程接口（application programming interface，API）访问应用程序框架层提供的各个服务模块，并且执行相应的智能化业务。另外，APP 层还可以包括应用监测进程（apTouchDaemon）、桌面启动器（launcher）和系统用户界面（systemUI）等核心应用。

HAL 层是对 Linux 内核驱动程序的封装，向上提供接口，它隐藏了特定平台的硬件接口细节，为操作系统提供了虚拟硬件平台，使其具有硬件无关性，可在多种平台上进行移植。例如，HAL 层可以包括人脸识别年龄算法、指纹识别年龄算法和声纹识别年龄算法等年龄识别算法，采用这些算法可以识别出正在使用终端设备的当前用户的年龄，进而判断当前用户是否为未成年人。需要说明的是，图 2 是以采用 HAL 层包括的年龄识别算法进行识别为例进行说明的，其并不对本申请实施例形成限定，在实际实现时，未成年人自动识别服务也可以调用其他分层的未成年人识别功能，或者未成年人自动识别服务也可以请求第三方平台进行未成年人识别。

在本申请实施例中，未成年人自动识别服务可以为终端设备制造商/生产商在终端设备中预先设置的一个系统级服务，用于在满足预设条件时触发未成年人识别。用户可以通过对未成年人自动识别服务选项的操作，触发手机启用未成年人自动识别服务。然后，未成年人自动识别服务可以执行下述逻辑：

未成年人自动识别服务的预设条件分析模块，分析是否满足下述至少一个条件：亮屏时长是否超过预设时长、应用运行时长是否超过预设时长、正在使用应用是否属于白名单应用、是否接收到三方应用发送的未成年人识别请求、是否检测到当前用户不是机主，终端设备的使用时长是否达到固定周期的整数倍。

如果分析结果指示满足预设条件，那么未成年人自动识别服务的未成年人识别模块调用年龄识别接口、问卷识别接口和/或系统账号识别接口等，由这些接口检测当前用户是否为未成年人。比如，年龄识别接口可以调用在终端设备本地存储的年龄识别算法或第三方平台进行年龄识别。未成年人识别算法包括但不限于基于人脸特征、指纹特征、声纹特征、设备使用习惯等信息的年龄识别算法。其中，基于人脸特征的年龄识别算法用于对摄像头采集的人脸图像进行分析，以确定当前用户的年龄；基于指纹特征的年龄识别算法用于对传感器采集的指纹数据进行分析，以确定当前用户的年龄；基于声纹特征的年龄识别算法用于对受话器和/或麦克风采集的声纹数据进行分析，以确定当前用户的年龄；基于设备使用习惯信息的年龄识别算法用于对用户使用终端设备过程中产生的数据（如使用时间或时长，使用应用偏好，触控区域面积或速度，握持手机角度或力度或区域面积等）进行分析，以确定当前用户的年龄。

当识别结果为年龄小于 18 周岁时，可以确定当前用户是未成年人。未成年人自动识别服务向三方应用发送通知，以便三方应用根据自身业务情况进行监控；或者，未成年人自动识

别服务可以向未成年人保护服务发送开启指令，以便未成年人保护服务对终端设备中的全部或指定应用进行监控。

需要说明的是，图 2 示出的软件结构中的层以及各层中包含的部件，并不构成对终端设备的具体限定。在另一些实施例中，终端设备可以包括比图示更多的层，比如、应用程序框架（framework，FWK）层及内核层等。每个层中可以包括比图示更多或更少的部件。另外，上述各个功能模块也可能合成为一个功能模块，一个功能模块也可能由多个功能模块组成。

可以理解的是，终端设备为了实现本申请实施例中的未成年人自动识别和保护方法，其包含了执行各个功能相应的硬件和/或软件模块。结合本文中所公开的实施例描述的各示例的算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。本领域技术人员可以结合实施例对每个特定的应用来使用不同方法来实现所描述的功能。

下面结合界面示意图介绍本申请提供的设置未成年人自动识别服务的场景。

本申请的说明书和权利要求书及附图中的术语“界面”和“用户界面”，是应用程序或操作系统与用户之间进行交互和信息交换的介质接口，它实现信息的内部形式与用户可以接受形式之间的转换。示例性地，界面的表现形式可以是用户体验（user experience，UX）界面。它可以是在电子设备的显示屏中显示的一个图标、窗口、控件等界面元素，其中，控件可以包括图标、按钮、菜单、选项卡、文本框、对话框、状态栏、导航栏等可视的界面元素。

1、开启未成年人自动识别服务（图 3A~图 3F）。

图 3A 示出了一个系统桌面，该系统桌面包括了荣耀视频、运动健康、天气、浏览器、智慧生活和设置等应用程序的图标（icon）。用户可以通过对任意一个图标的点击操作，触发终端设备显示应用程序的操作界面。比如用户可以点击设置 201。

在终端设备检测到用户对设置 201 的点击操作后，终端设备显示如图 3B 所示的设置界面。该设置界面包括未成年人识别功能开关、蓝牙、无线局域网、电话、信息和飞行模式等功能选项，每个功能选项对应一个系统级服务。用户可以通过对某个选项的点击操作，触发终端设备显示与这个选项对应的服务设置界面。比如用户可以点击未成年人识别功能开关 202。

在终端设备检测到用户对未成年人识别功能开关 202 的点击操作后，终端设备显示如图 3C 所示的未成年人识别功能开关设置界面。该设置界面包括一个允许自动启动未成年人识别开关。允许自动启动未成年人识别开关由圆形控件 203 和滑动条 204 组成。作为一种场景示例，在默认情况下，圆形控件 203 位于滑动条 204 的左侧，此时未成年人识别功能处于关闭状态，没有开启未成年人自动识别服务。当然，本申请文件对此开关的默认状态配置并不进行限定，比如，在另一种场景示例中，未成年人识别功能默认处于开启状态。

如图 3D 所示，当用户想要使用未成年人自动识别服务时，用户可以按照箭头所示方向沿着滑动条 204 向右滑动圆形控件 203，使圆形控件 203 滑动至滑动条 204 的右侧，从而开启未成年人自动识别服务。在开启未成年人自动识别服务后，终端设备可以检测是否满足预设条件，当满足条件时将识别当前用户是否为未成年人，并在识别到当前用户为未成年人的情况下执行未成年人保护操作。

作为一种实现方式，在用户通过如图 3D 所示的操作开启未成年人自动识别服务后，终端设备更新显示为如图 3E 所示的界面，该界面可以包括三个设置选项：触发未成年人识别的条件选项、未成年人识别方式选项、未成年人保护操作选项。这些设置选项处于可操作状态。其中，触发未成年人识别的条件选项用于用户设置触发未成年人识别的预设条件，未成年人

识别方式选项用于用户设置未成年人识别的方式，未成年人保护操作选项用于用户设置未成年人保护的方式。

作为另一种实现方式，如图 3F 所示，在“允许自动启用未成年人识别”开关处于关闭状态时，界面也可以包括三个设置选项：触发未成年人识别的条件选项、未成年人识别方式选项、未成年人保护操作选项。这些设置选项默认无法操作。只有在将如图 3F 所示的“允许自动启用未成年人识别”开关更新为如图 3E 所示的开启状态时，这三个设置选项才变为可操作状态。

作为又一种实现方式，终端设备也可以不向用户提供这三个设置选项，而是直接在算法逻辑中固化下来。

本申请实施例对三个设置选项的具体设置方式不进行限定，可以根据使用需求进行调整。

应理解，监护人仅需要一次开启未成年人自动识别服务的操作，终端设备就可以在满足条件时进行未成年人自动识别，并在识别到当前用户为未成年人的情况下自动执行未成年人保护操作，从而监护人不用手动频繁开启或关闭未成年人保护模式，提高了使用体验。

2、首次开启未成年人自动识别服务需设置身份验证信息（图 4A~图 4J）。

在监护人触发终端设备开启未成年人自动识别服务后，未成年人可能会通过关闭该允许自动启动未成年人识别开关来关闭该服务，从而无法起到未成年人保护的作用。为了解决此问题，图 4A~图 4F 所示，本申请提供一种首次开启未成年人自动识别服务需设置独立密码的方案。

在用户执行如图 3D 所示的开启操作后，如果终端设备检测到这次开启操作属于首次开启未成年人自动识别服务的操作，那么终端设备显示如图 4A 所示的密码输入框 205 和首次开启需设置独立密码的提示信息。如图 4B 所示，用户可以在密码输入框 205 中设置四位密码 206，然后，终端设备保存四位密码 206。

在开启未成年人自动识别服务后，用户还可能想要关闭未成年人自动识别服务。如图 4C 所示，用户可以按照箭头所示方向沿着滑动条 204 向左滑动圆形控件 203。在终端设备检测到滑动操作后，暂时不关闭未成年人自动识别服务，而是显示如图 4D 所示的密码输入框 205，并提示用户再次输入先前设置的四位密码。

在一些实施例中，如图 4E 所示，用户可以在密码输入框 205 中输入四位密码 207。如果本次输入的四位密码 207 与先前设置的四位密码 206 匹配，那么说明当前用户为先前设置四位密码的监护人，关闭未成年人自动识别服务符合监护人的真实意图，此时如图 4F 所示终端设备可以关闭未成年人自动识别服务。

在另一些实施例中，如果用户在密码输入框 205 中输入的四位密码与先前设置的四位密码 206 不匹配，那么为了避免用户操作失误导致密码错误，终端设备可以再次提示用户输入四位密码。当用户连续 N 次输入的四位密码与先前设置的四位密码 206 不匹配，说明当前用户不是先前设置四位密码的监护人，可能是未成年人，其中，N 为大于或等于 2 的整数。此时，终端设备可以无需检测是否满足预设条件，也无需识别当前用户是否为未成年人，而是直接向三方应用发送通知，以便三方应用根据自身业务情况进行监控，或者，开启未成年人保护服务，以便未成年人保护服务对各个应用情况进行监控。

应理解，在首次开启未成年人自动识别服务时，监护人通过设置独立密码，可以仅授权知道独立密码的监护人关闭未成年人自动识别服务。对于不知道独立密码的未成年人，不能通过对允许自动启动未成年人识别开关的操作关闭该服务，从而更好地起到未成年人保护的作用。

需要说明的是，上述图 4A~图 4F 仅以设置四位密码的方案为例进行描述，其并不对本申请形成限定。应理解，终端设备还可以采用其他设置用户身份验证信息的方案，比如，基于指纹、声纹或人脸识别等身份验证方案。

作为另一种示例，图 4G~图 4J 示出了一种首次开启未成年人自动识别服务后采集人脸信息的方案。如图 4G 所示，如果终端设备检测到首次开启未成年人自动识别服务的操作，那么弹出提示信息“首次开启需采集人脸信息，请正视屏幕”。在成功采集到人脸信息后，终端设备显示如图 4H 所示的“已成功采集人脸信息”，保存人脸信息，并成功开启未成年人自动识别服务。在开启未成年人自动识别服务后，用户还可能想要关闭未成年人自动识别服务。如图 4I 所示，用户可以按照箭头所示方向，沿着滑动条向左滑动圆形控件。在终端设备检测到滑动操作后，终端设备暂时不关闭未成年人自动识别服务，而是显示如图 4J 所示的提示信息“关闭该功能需采集人脸信息，请正视屏幕”。当首次采集的人脸信息与关闭未成年人自动识别服务时采集的人脸信息为同一个用户时，关闭未成年人自动识别服务；否则，禁止关闭未成年人自动识别服务，从而更好地起到未成年人保护的作用。

当然，在终端设备检测到首次开启未成年人自动识别服务的操作时，终端设备也可以无需采集人脸图像，而是直接将先前已经采集的用于解锁屏幕或电子支付的人脸图像，作为关闭未成年人自动识别服务时的授权人脸图像；或者，在获得用户授权后，将先前已经采集的用于解锁屏幕或电子支付的人脸图像，作为关闭未成年人自动识别服务时的授权人脸图像。

另外，在图 4A~图 4J 中，终端设备是以显示提示信息的方式通知用户输入身份验证信息的，其并不对本申请实施例形成限定。在实际实现时，终端设备可以通过语音等方式通知用户输入身份验证信息，比如通过语音提示用户录入声纹信息。

3、设置触发未成年人识别的条件（图 5A~图 5T）。

在用户执行如图 3D 所示的开启操作后，如果该操作属于首次开启未成年人自动识别服务的操作，那么用户可以执行如图 4A 和图 4B 所示的设置独立密码操作，然后终端设备保存用户设置的独立密码，并显示如图 5A 所示的设置界面。或者，在用户执行如图 3D 所示的开启操作后，如果该操作不属于首次开启未成年人自动识别服务的操作，那么终端设备可以直接显示如图 5A 所示的设置界面。

如图 5A 所示，在开启未成年人自动识别服务后，设置界面包含三个设置选项：触发未成年人识别的条件选项 208、未成年人识别方式选项、未成年人保护操作选项。这些设置选项处于可操作状态。对于这三个设置选项的实现方式，可以参照上述实施例的描述，此处不再赘述。

下面对设置触发未成年人识别的条件进行示例说明。

在用户点击如图 5A 所示的触发未成年人识别的条件选项 208 后，终端设备显示如图 5B 所示的设置界面。该设置界面可以包括默认条件开关和手动设置条件开关。

如果用户选择开启默认条件开关，则终端设备会将未成年人自动识别服务的默认设置作为触发未成年人识别的条件。比如，默认设置为接收到三方应用的未成年人识别请求。再比如，默认设置为每隔 1 小时检测一次亮屏时长超过预设时长、应用持续时长超过预设时长、正在使用属于白名单应用。又例如，默认设置为终端设备的使用时长达到固定周期的整数倍。其中，检测时长、预设时长、固定周期和白名单应用均为未成年人自动识别服务预先设定的。

如果用户选择开启手动设置条件开关，则如图 5B 所示，终端设备显示可供用户选择的设置条件：亮屏时长/时段 209、应用持续运行时长/时段 210、白名单应用 211、请求未成年人识别的应用 212、机主检测 213、固定周期检测。当然，终端设备还可以显示其他可供用户

选择的设置条件，或者，终端设备也可以不向用户提供以上所有或部分设置选项，而是在算法逻辑中直接固化下来，本申请实施例不作限定。

(1) 设置亮屏时长/时段（图 5C~图 5D）。

如图 5C 所示，用户可以点击亮屏时长/时段 209。响应于该点击操作，终端设备显示如图 5D 所示的设置界面。该设置界面可以包括两个部分：一个部分是亮屏时长，另一个部分是亮屏时段。

在一些实施例中，用户可以沿着滑动条 214 向右滑动圆形控件 215，使圆形控件 215 滑动至滑动条 214 的右侧，从而开启亮屏时长。在开启亮屏时长之后，用户可以在输入框 216 中输入预设时长。以预设时长是 30 分钟为例，当终端设备持续亮屏的时长超过 30 分钟时，将确定满足预设条件，并触发未成年人自动识别。需要说明的是，当输入框 216 中的预设时长为 0 时，终端设备可以将亮屏确定为满足预设条件，即，只要检测到终端设备亮屏则立即触发未成年人自动识别。

在另一些实施例中，用户可以沿着滑动条 217 向右滑动圆形控件 218，使圆形控件 218 滑动至滑动条 217 的右侧，从而开启亮屏时段。在开启亮屏时段之后，用户可以在输入框 219 中输入亮屏时段的起始时刻，在输入框 220 中输入亮屏时段的截止时刻。以亮屏时段的起始时刻是 18:00、亮屏时段的截止时刻是 24:00 为例，当终端设备在时段 18:00~24:00 的任意时刻点亮屏幕时，终端设备可以确定满足预设条件，并触发未成年人自动识别。

在某些情况下，用户可能同时开启亮屏时长和亮屏时段。在一些实施例中，只要终端设备持续亮屏的时长超过预设时长，或在亮屏时段的任意时刻点亮屏幕，则触发未成年人自动识别。在另一些实施例中，如果在亮屏时段内持续亮屏的时长超过预设时长，那么触发未成年人自动识别。

(2) 设置应用持续运行时长/时段（图 5E~图 5F）。

如图 5E 所示，用户可以点击应用持续运行时长/时段 210。响应于该点击操作，终端设备显示如图 5F 所示的设置界面。该设置界面可以包括两个部分：一个部分是应用持续运行时长，另一个部分是应用持续运行时段。

在一些实施例中，用户可以沿着滑动条 221 向右滑动圆形控件 222，使圆形控件 222 滑动至滑动条 221 的右侧，从而开启应用持续运行时长。在开启应用持续运行时长之后，用户可以在输入框 223 中输入预设时长。以预设时长是 45 分钟为例，当终端设备持续亮屏的时长超过 45 分钟时，确定满足预设条件，并触发未成年人自动识别。需要说明的是，当输入框 223 中的预设时长为 0 时，终端设备将应用启动确定为满足预设条件，即只要终端设备启动应用则立即触发未成年人自动识别。

在另一些实施例中，用户可以沿着滑动条 224 向右滑动圆形控件 225，使圆形控件 225 滑动至滑动条 224 的右侧，从而开启应用持续运行时段。在开启应用持续运行时段之后，用户可以在输入框 226 中输入应用持续运行时段的起始时刻，在输入框 227 中输入应用持续运行时段的截止时刻。以应用持续运行时段的起始时刻是 18:00、应用持续运行时段的截止时刻是 24:00 为例，当终端设备在时段 18:00~24:00 的任意时刻启动应用时，终端设备可以确定满足预设条件，并触发未成年人自动识别。

在某些情况下，用户可能同时开启应用持续运行时长和应用持续运行时段。作为一个示例，只要应用持续运行时长超过预设时长，或在应用持续运行时段的任意时刻启动应用，则触发未成年人自动识别。作为另一个示例，如果在应用持续运行时段内应用持续运行时长超过预设时长，那么触发未成年人自动识别。

需要说明的是，上述应用可以是终端设备中的任意一个应用，也可以是预设类别的应用，还可以是用户指定的某些应用。如图 5F 所示，用户可以打开指定运行应用开关 228，并根据实际需求对某些应用程序进行选择操作，对于指定运行应用的实现方式可以参照下述实施例选择白名单应用的相关描述，此处不予赘述。

应理解，当上述应用的数量为多个时，与各个应用对应的应用持续运行时长可以相同或不同，与各个应用对应的应用持续运行时段也可以相同，也可以不同。比如，与游戏类对应的应用持续运行时长为 15 分钟，与娱乐类对应的应用持续运行时长为 30 分钟，与社交类对应的应用持续运行时长为 1 小时。

(3) 设置白名单应用（图 5G~图 5J）。

白名单由至少一个待监测应用组成。待监测应用可以为支付 APP、游戏 APP 和视频播放 APP 等需要加强未成年人监管的应用。在将白名单作为触发未成年人识别的条件后，只要终端设备检测到正在使用/正在运行的应用属于白名单，就可以触发未成年人识别。

在一些实施例中，上述白名单为未成年人自动识别服务提供的名单。智能终端制作商可以根据政策要求在未成年人自动识别服务中预先设定一些应用类别。如果在终端设备安装的某个应用属于某个应用类别，那么这个应用将被自动加入到白名单。或者，也可以在算法逻辑中固化一些应用作为白名单应用，本申请实施例对此不进行限定。

在另一些实施例中，用户可以手动为白名单添加应用。

如图 5G 所示，用户可以点击白名单应用 211。响应于该点击操作，终端设备显示如图 5H 所示的设置界面。该设置界面可以包括白名单应用开关。用户可以沿着滑动条 229 向右滑动圆形控件 230，使圆形控件 230 滑动至滑动条 229 的右侧，从而开启白名单应用开关。在开启白名单应用开关后，终端设备还可以显示如图 5H 所示的应用名单 231。该应用名单 231 可以包括所有 APP 与类别、社交、游戏、娱乐、支付、教育、旅游和购物等选项。

作为一个示例，用户可以选择所有 APP 与类别选项。如此，当终端设备运行任何一个应用时都会触发未成年人识别。

作为另一个示例，用户可以选择与一个或多个类别选项对应的全部应用。比如，如图 5I 所示，用户可以点击与社交选项对应的选择控件 232。如此，当终端设备运行任何一个社交类应用时，都会触发未成年人识别。

作为又一个示例，用户可以选择与一个或多个类别选项对应的部分应用。比如，如图 5J 所示，用户可以点击与社交选项对应的展开控件 233，并选择社交 1 和社交 2。如此，当终端设备运行社交 1 或社交 2 时会触发未成年人识别。另外，如图 5J 所示，在用户选择社交 1 和社交 2 后，终端设备还可以展示与社交 1 对应的输入框 2331、与社交 2 对应的输入框 2332，其中，输入框 2331 用于输入与社交 1 对应的预设时长，输入框 2332 用于输入与社交 2 对应的预设时长。以输入框 2331 中的时长为 10 分钟为例，当检测到社交 1 持续运行时长大于或等于 10 分钟时，触发未成年人识别。

需要说明的是，上述实施例是以为白名单应用设置预设时长为例进行说明的，其并不对本申请实施例形成限定。在实际实现时，也可以不设置预设时长，这样只要检测到当前运行应用属于白名单则触发未成年人识别。

需要说明的是，上述实施例是以应用类别展示并提供用户设置入口的，其并不对本申请实施例形成限定。在实际实现中，也可以直接将该终端设备上所有已安装应用直接以列表形式展示给用户进行设置。

(4) 设置请求未成年人识别的应用（图 5K~图 5N）。

上述请求未成年人识别的应用为与未成年人自动识别服务签订协议的应用。当请求未成年人识别的应用按照协商的消息格式向未成年人自动识别服务发送请求时，未成年人自动识别服务响应于该请求，触发未成年人自动识别。

如图 5K 所示，用户可以点击请求未成年人识别的应用 212。响应于该点击操作，终端设备显示如图 5L 所示的设置界面。该设置界面可以包括请求未成年人识别的应用开关。用户可以沿着滑动条 234 向右滑动圆形控件 235，使圆形控件 235 滑动至滑动条 234 的右侧，从而开启请求未成年人识别的应用开关。在开启请求未成年人识别的应用开关后，终端设备还可以显示如图 5L 所示的添加请求未成年人识别的 APP 选项 236、APP 发送未成年人识别请求的条件 237。

如图 5M 所示，用户可以点击与添加请求未成年人识别的 APP 选项 236 对应的展开控件 238，从而终端设备可以显示所有 APP 与类别、社交、游戏、娱乐、创意、教育、旅游和购物等选项。然后，用户可以通过对这些选项的操作，选择一个或多个请求未成年人识别的应用。对于用户选择请求未成年人识别的应用的实现方式，可以参照上述实施例中选择白名单应用的相关描述，此处不再赘述。需要说明的是，也可以不为用户提供设置请求未成年人识别的应用，而是在算法逻辑中直接以预置白名单等形式实现，允许未成年人自动识别服务与预置白名单内应用以预设消息格式和内容进行交互。

如图 5N 所示，用户可以点击与 APP 发送未成年人识别请求的条件 237 对应的展开控件 239，从而终端设备可以显示下述可选择条件：APP 运行达到预设时长、调用支付类 APP、运行时段为预设时段、使用非常用功能、输入密码错误。用户可以从这些条件中选择一个或多个条件，从而当满足选择的任意一个条件时均会触发未成年人自动识别。需要说明的是，终端设备也可以不为用户提供针对每个 APP 设置发送未成年人识别请求的条件，而是在 APP 算法逻辑中固化预设条件，允许 APP 在检测到满足预设的条件时能自行向未成年人自动识别服务以预设消息格式和内容方式发送未成年人识别请求。

其中，“APP 运行达到预设时长”中的 APP 为用户选择的“请求未成年人识别的 APP”。比如，假设用户添加了游戏类作为“请求未成年人识别的 APP”，且“APP 运行达到预设时长”中的预设时长为 15 分钟，那么当任意一个游戏类 APP 的运行时长大于或等于 15 分钟时，该游戏类 APP 会向未成年人自动识别服务发送请求，从而未成年人自动识别服务响应于该请求，触发未成年人自动识别。

“调用支付类 APP”是指在运行用户设定的某个“请求未成年人识别的 APP”的过程中，如果这个 APP 检测到用户触发该 APP 调用支付类 APP，那么该 APP 会向未成年人自动识别服务发送请求，从而未成年人自动识别服务响应于该请求，触发未成年人自动识别。

“运行时段为预设时段”中的预设时段可以为用户设定的一个时段或终端设备自行设定的一个时段（比如节假日）。以用户设定的预设时段是 18:00~24:00 为例，如果用户设定的某个“请求未成年人识别的 APP”在时段 18:00~24:00 内运行，那么该 APP 会向未成年人自动识别服务发送请求，从而未成年人自动识别服务响应于该请求，触发未成年人自动识别。

“使用非常用功能”中的非常用功能为用户不经常使用的功能。对于用户设定的“请求未成年人识别的 APP”，未成年人自动识别服务可以根据每款 APP 的日志文件统计出使用频率相对较低的功能，并将其标记为该 APP 的非常用功能。以某一款视频 APP 为例，假设非常用功能为直播功能和动漫功能，如果该视频 APP 检测到用户使用直播功能或动漫功能，那么该 APP 会向未成年人自动识别服务发送请求，从而未成年人自动识别服务响应于该请求，触发未成年人自动识别。

“输入密码错误”中的密码可以为用户设定的“请求未成年人识别的 APP”的账号密码、支付密码或登录密码等。以某一款社交 APP 为例，在登录时会提示用户输入登录密码，如果输入的登录密码与预设密码不匹配，那么该 APP 会向未成年人自动识别服务发送请求，从而未成年人自动识别服务响应于该请求，触发未成年人自动识别。

“接收到用户关闭未成年人保护模式的操作”是指在某个自身具备未成年人保护功能的三方应用运行过程中，用户关闭了该三方应用的未成年人保护模式，那么存在未成年人擅自关闭的风险，因此该 APP 会向未成年人自动识别服务发送请求，然后未成年人自动识别服务响应于该请求，触发未成年人自动识别。

需要说明的是，上述这些条件设置选项，也可以在每个 APP 的界面内提供用户入口，本申请实施例对此不进行限定。

另外，当用户设定多个“请求未成年人识别的 APP”时，这些 APP 对应的“APP 运行达到预设时长”中的预设时长可以相同，也可以不同，这些 APP 对应的“运行时段为预设时段”中的预设时段可以相同也可以不同。

应理解，有些应用没有设置未成年人保护模式，或者不具备自动开启未成年人保护模式的功能，这些应用不能很好的保护未成年人。本申请向用户提供了可设置“请求未成年人识别的 APP”的能力。当用户设定的某个“请求未成年人识别的 APP”满足 APP 运行达到预设时长、调用支付类 APP、运行时段为预设时段、使用非常用功能和/或输入密码错误等条件时，可以初步确定当前用户不是监护人，因此该 APP 通过向未成年人自动识别服务发送请求，可以触发进一步精确识别当前用户是否为未成年人。在确定当前用户是未成年人的情况下，如果该 APP 没有设置未成年人保护模式，那么未成年人自动识别服务可以触发开启成年人保护服务；如果该 APP 设置有未成年人保护模式，那么未成年人自动识别服务可以通知该 APP 开启未成年人保护模式。

(5) 设置机主检测（图 5O~图 5R）。

上述设置机主检测中的机主为终端设备的拥有者或监护人。当使用终端设备的当前用户不是机主时，该用户是未成年人的概率较大，因此通过开启机主检测，可以触发未成年人自动识别。

如图 5O 所示，用户可以点击机主检测 213。响应于该点击操作，终端设备显示如图 5P 所示的设置界面。该设置界面可以包括允许自动识别使用用户是否为机主开关。用户可以沿着滑动条 240 向右滑动圆形控件 241，使圆形控件 241 滑动至滑动条 240 的右侧，从而开启允许自动识别使用用户是否为机主开关。在开启请求未成年人识别的应用开关后，终端设备还可以显示如图 5P 所示的机主检测手段选项 242、机主检测触发条件选项 243。

如图 5Q 所示，用户可以点击与机主检测手段选项 242 对应的展开控件 2421，从而终端设备可以显示默认、人脸、指纹、声纹和输入密码错误等选项。其中，默认选项用于指示未成年人自动识别服务预置的机主检测手段，该检测手段可以为人脸、指纹、声纹和输入密码错误中的一项或多项；人脸选项用于指示通过人脸识别年龄方式；指纹选项用于指示通过指纹识别年龄方式；声纹选项用于指示通过声纹识别年龄方式；输入密码错误选项用于指示通过密码检测年龄方式，当用户输入支付密码或登录密码等任意密码时，未成年人自动识别服务会识别输入密码与存储的预设密码是否匹配，并根据匹配结果确定当前用户是否为机主。用户可以通过对这些选项的操作，选择一个或多个机主检测手段。当用户选择多个检测手段时，若多个检测手段中的任意一个检测手段的检测结果显示当前用户不是机主，则触发未成年人识别。应理解，除了如图 5Q 所示的检测手段，终端设备还可能采用虹膜等其他检测手

段，本申请实施例不作限定。

如图 5R 所示，用户可以点击与机主检测触发条件选项 243 对应的展开控件 2431，从而终端设备可以显示默认、固定频率检测、亮屏时长满足条件时检测、应用持续运行时长满足条件时检测和当前应用属于白名单时检测等选项。其中，默认选项用于指示未成年人自动识别服务预置的机主检测触发条件，该触发条件可以为固定频率检测、亮屏时长满足条件时检测、应用持续运行时长满足条件时检测和当前应用属于白名单时检测中的一项或多项；固定频率检测选项用于指示按照预设频率检测当前用户是否为机主，比如每隔 10 分钟检测一次当前用户是否为机主；亮屏时长满足条件时检测选项用于指示在终端设备持续亮屏时长大于或等于预设时长的情况下触发检测当前用户是否为机主；应用持续运行时长满足条件时检测选项用于指示在某应用持续运行的时长大于或等于预设时长的情况下触发检测当前用户是否为机主；当前应用属于白名单时检测选项用于指示在当前运行的应用属于白名单时触发检测当前用户是否为机主。用户可以通过对这些选项的操作，选择一个或多个触发条件。当用户选择多个触发条件时，若满足多个触发条件中的任意一个触发条件，则触发检测当前用户是否为机主，在检测结果不是机主时进一步触发未成年人识别。

需要说明的是，本申请实施例是以人脸、指纹和声纹这三种生物特征识别方式为例进行示例说明的，其并不对本申请实施例形成限定。在实际实现时，还可以采用虹膜或体态等其他生物特征识别方式。另外，上述实施例中展示的机主检测手段、机主检测触发条件设置选项，也可以不直接向用户提供，而是在直接在算法逻辑中固化明确，本申请实施例对此不进行限定。

应理解，未成年人自动识别服务为用户提供了一个可配置触发未成年人识别的预设条件的入口。用户可以实际需要进行上述设置操作，从而终端设备能够在满足一项或多项预设条件时触发未成年人识别。

(5) 设置固定周期检测（图 5S~图 5T）。

上述固定周期可以为机主根据实际使用需求设置的任意时长，比如 10 分钟、半小时或 3 小时等。

如图 5S 所示，用户可以点击固定周期检测。响应于该点击操作，终端设备显示如图 5T 所示的设置界面。该设置界面可以包括允许自动按照固定周期检测开关。用户可以沿着滑动条向右滑动圆形控件，使圆形控件滑动至滑动条的右侧，从而开启允许自动按照固定周期检测开关。在开启允许自动按照固定周期检测开关后，终端设备还可以显示如图 5T 所示的固定周期设备选项。以用户设备的固定周期为 1 小时为例，终端设备可以每隔 1 小时检测一次当前用户是否为未成年人。

需要说明的是，上述实施例中展示的固定周期设置选项，也可以不直接向用户提供，而是在直接在算法逻辑中固化明确，本申请实施例对此不进行限定。

4、设置未成年人识别的条件（图 6A~图 6D）。

参照上述实施例的描述，在用户开启未成年人自动识别服务后，设置界面包含三个设置选项：触发未成年人识别的条件选项、未成年人识别方式选项、未成年人保护操作选项。这些设置选项处于可操作状态。对于这三个设置选项的实现方式，可以参照上述实施例的描述，此处不再赘述。

下面对设置未成年人识别方式进行示例说明。

如图 6A 所示，用户可以点击未成年人识别方式选项 244。响应于该点击操作，终端设备显示如图 6B 所示的设置界面。该设置界面可以包括默认识别方式开关和手动设置识别方式

开关。

作为一种示例，如图 6B 所示，当圆形控件 246 位于滑动条 245 的右侧时，默认识别方式开关处于开启状态。终端设备会按照未成年人自动识别服务的默认设置进行未成年人识别。比如，默认设置为生物信息识别、系统账号识别、问卷识别和身份验证平台识别中的一项或多项。当按照默认识别到当前用户为未成年人时，执行未成年人保护操作。

作为另一种示例，如图 6C 所示，用户可以沿着滑动条 247 向右滑动圆形控件 248，使圆形控件 248 滑动至滑动条 247 的右侧，从而开启手动设置识别方式开关。在开启手动设置识别方式开关后，终端设备还可以显示如图 6C 所示的基于生物特征信息、系统账号、问卷、身份验证平台和设备使用习惯信息等可选择的年龄识别方式。用户可以从这些可选择的年龄识别方式中选择一种或多种识别方式，作为未成年人识别的方式。

其中，生物信息识别方式，用于计算采集的生物特征信息与监护人在终端设备中预先录入的未成年人生物特征模板的匹配度，以判断当前用户是否为未成年人；或者，用于基于人工智能（artificial intelligence, AI）算法对采集的生物特征信息进行年龄识别，以判断当前用户是否为未成年人。

系统账号识别方式，用于提示当前用户输入终端设备的系统账号和/或系统密码，或者输入在上述实施例中为未成年人自动识别服务设置的独立密码。当用户输入密码不正确时，确定当前用户为未成年人，执行未成年人保护操作。

问卷识别方式，用于提示当前用户回答预设问题。未成年人自动识别服务可以提供多个年龄阶段的题库，比如，题库 1 中的题目难度与 1~6 岁年龄阶段的认知水平对应，题库 2 中的题目难度与 7~9 岁年龄阶段的认知水平对应，题库 3 中的题目难度与 10~12 岁年龄阶段的认知水平对应，题库 4 中的题目难度与 13~15 岁年龄阶段的认知水平对应，题库 5 中的题目难度与 16~18 岁年龄阶段的认知水平对应。监护人可以根据被监护人的年龄，选择题目难度超出被监护人的认知水平的题库。当被监护人使用终端设备时，终端设备可以从监护人设定的题库中随机选择一个或多个题目，并提示被监护人进行回答。若被监护人答错题目的数量超过预设数量或预设比例，将触发未成年人保护操作。

身份验证平台识别方式，用于通过与第三方平台交互，由第三方平台对采集的生物特征信息进行识别。应理解，在某些场景下，终端设备提供的 AI 算法存在一定的误识别率，而第三方平台对未成年人识别的准确性较高，因此可以借助第三方平台对采集的生物特征信息进行识别。

示例性地，以用户选择的手动设置识别方式为生物信息识别方式为例进行说明。如图 6C 所示，用户可以点击与生物信息识别选项对应的展开控件 249，从而终端设备可以显示通过人脸识别年龄、通过指纹识别年龄和通过声纹识别年龄等选项。其中，通过人脸识别年龄选项用于选中通过人脸识别年龄方式，当用户选中通过人脸识别年龄方式时，未成年人自动识别服务会调用人脸识别算法识别与当前用户的人脸图像对应的年龄；通过指纹识别年龄选项用于选中通过指纹识别年龄方式，当用户选中通过指纹识别年龄方式时，未成年人自动识别服务会调用指纹识别算法识别与当前用户的指纹信息对应的年龄；通过声纹识别年龄选项用于选中通过声纹识别年龄方式，当用户选中通过声纹识别年龄方式时，未成年人自动识别服务会调用声纹识别算法识别与当前用户的声纹信息对应的年龄。用户可以通过对这些选项的操作，选择一种或多种生物信息识别方式，作为未成年人识别的方式。如图 6D 所示，用户可以选择通过人脸识别年龄选项。应理解，当按照用户选择的任意一种生物信息识别方式识别到未成年人时，均会触发执行未成年人保护操作。需要说明的是，上述年龄识别算法可以

为在终端设备本地存储的，也可以为第三方平台提供的，本申请实施例不作限定。

设备使用习惯信息是根据机主使用终端设备的历史记录统计出来的。设备使用习惯信息可以用于表征用户的习惯行为或高频行为，比如，这些行为包括机主经常使用手机的时段、机主经常使用的应用、机主经常使用应用的具体功能、用户习惯设置的屏幕亮度、用户习惯设置的音量等。如果实时采集的终端设备使用数据与预先统计的机主的使用习惯不相符，那么确定当前用户不是机主而是未成年人。

除了上述识别方式，终端设备还可能采用其他识别方式，本申请不作具体限定。

应理解，与传统手动频繁开启或关闭未成年人保护模式相比，通过自动识别未成年人，可以在识别到当前用户为未成年人的情况下自动开启未成年人保护模式。

5、设置未成年人保护操作（图 7A~图 7H）。

在用户开启未成年人自动识别服务后，设置界面包含三个设置选项：触发未成年人识别的条件选项、未成年人识别方式选项、未成年人保护操作选项。这些设置选项处于可操作状态。对于这三个设置选项的实现方式，可以参照上述实施例的描述，此处不再赘述。

下面对设置未成年人保护操作进行示例说明。

如图 7A 所示，用户可以点击未成年人保护操作选项 250。在终端设备接收到点击操作时，可能已经安装未成年人保护软件，具备提供未成年人保护服务的能力，也可能尚未安装未成年人保护软件，不具备提供未成年人保护服务的能力。此时，终端设备响应于该点击操作，根据未成年人保护软件的安装情况，显示与未成年人保护操作对应的不同设置界面。

作为一种示例，如图 7B 所示，如果在终端设备接收到点击操作时，已经安装了未成年人保护软件，具备提供未成年人保护服务的能力，那么与未成年人保护操作对应的设置界面可以仅包括绑定设备开关 251。在绑定设备开关 251 处于开启状态时，用户可以将终端设备与监护设备绑定，从而在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会向监护设备发送预警消息，并在接收到监护设备返回的授权应答的情况下，开启未成年人保护软件，以提供未成年人保护服务。

作为另一种示例，如图 7C 所示，如果在终端设备接收到点击操作时，尚未安装未成年人保护软件，不具备提供未成年人保护服务的能力，那么与未成年人保护操作对应的设置界面可以包括绑定设备开关 251 和安装保护软件开关 252。用户可以打开绑定设备开关 251 和安装保护软件开关 252 中的至少一者。

如果用户打开绑定设备开关 251，不打开安装保护软件开关 252，那么用户可以将终端设备与监护设备绑定，从而在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会向监护设备发送预警消息。

如果用户打开安装保护软件开关 252，不打开绑定设备开关 251，那么在未成年人自动识别服务识别到当前用户是未成年人之后，直接下载并安装未成年人保护软件，以提供未成年人保护服务。

如果用户打开绑定设备开关 251 和安装保护软件开关 252，那么用户可以将终端设备与监护设备绑定。在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会下载并安装未成年人保护软件，并向监护设备发送预警消息，以提供未成年人保护服务。或者，终端设备也可以在开启安装保护软件开关 252 后立即安装未成年人保护软件。

示例性地，如图 7D 所示，用户可以沿着滑动条 2511 向右滑动圆形控件 2512，使圆形控件 2512 滑动至滑动条 2511 的右侧，从而开启绑定设备开关 251。在开启绑定设备开关 251 后，终端设备还可以显示如图 7D 所示的二维码和提示信息，以提示监护人通过使用监护人

扫描二维码，来绑定终端设备和监护设备。如图 7E 所示，在终端设备与至少一台监护设备成功绑定后，终端设备可以显示已绑定设备列表 253。然后，如图 7F 所示，用户可以沿着滑动条 2521 向右滑动圆形控件 2522，使圆形控件 2522 滑动至滑动条 2521 的右侧，从而开启安装保护软件开关 252。如此，在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会向监护设备发送预警消息，以提供未成年人保护服务。需要说明的是，绑定监护设备也可以通过蓝牙或 WLAN 等短距离通信技术实现，比如，将监护设备的蓝牙 MAC 地址或 WLAN MAC 地址等设备标识符保存或关联到终端设备本地；绑定监护设备还可以通过设置监护账号实现，比如，将终端设备所登录的账号与监护账号进行关联，从而将监护账号所登录的另一个终端设备作为监护设备。

作为又一种示例，如果在终端设备接收到点击操作时，尚未安装未成年人保护软件，不具备提供未成年人保护服务的能力，那么如图 7B 所示，终端设备可以仅显示绑定设备开关 251，而不显示安装保护软件开关 252。在用户打开绑定设备开关 251 并绑定设备的情况下，可以采用线上方式向监护设备发送安装未成年人保护软件的请求，在获得监护人实时授权后在终端设备本地下载与安装相应软件。

作为再一种示例，如图 7G 所示，如果在终端设备接收到点击操作时，尚未安装未成年人保护软件，不具备提供未成年人保护服务的能力，那么与未成年人保护操作对应的设置界面可以包括绑定设备开关 251 和自动安装保护软件开关 254。用户可以打开绑定设备开关 251 和自动安装保护软件开关 254 中的至少一者。

如果用户打开绑定设备开关 251，不打开自动安装保护软件开关 254，那么用户可以将终端设备与监护设备绑定，从而在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会向监护设备发送预警消息。

如果用户打开自动安装保护软件开关 254，不打开绑定设备开关 251，那么在未成年人自动识别服务识别到当前用户是未成年人之后，直接下载并安装未成年人保护软件，以提供未成年人保护服务。

如果如图 7H 所示，用户打开绑定设备开关 251 和自动安装保护软件开关 254，那么用户可以将终端设备与监护设备绑定，从而在未成年人自动识别服务识别到当前用户是未成年人之后，终端设备会向监护设备发送预警消息，同时直接下载并安装未成年人保护软件，以提供未成年人保护服务。

应理解，通过绑定监护设备，可以在识别到使用终端设备的用户为未成年人时，及时向监护人使用的监护设备发出预警消息。另外，通过安装未成年人保护软件，可以由未成年人保护软件提供过滤不良信息、阻止未经授权购买、拦截欺诈网站等未成年人保护服务。

上述实施例已经完成对如何设置、开启未成年人自动识别服务的介绍。在设置、开启未成年人自动识别服务之后，终端设备可以执行本申请下述实施例提供的未成年人自动识别和保护方法。

下面将以未成年人自动识别和保护方法的执行主体为如图 2 所示的软件结构示意图中的模块为例，对本申请实施例提供的未成年人自动识别和保护方法进行示例性说明。

图 8 为本申请实施例提供的未成年人自动识别和保护方法的总流程示意图。

如图 8 所示，该方法可以分为四个阶段：未成年人自动识别服务的开启阶段、未成年人的识别阶段、未成年人的保护阶段、未成年人自动识别服务的关闭阶段。其中，未成年人自动识别服务的开启阶段包括下述 S01~S02，未成年人的识别阶段包括下述 S03~S04，未成年人的保护阶段包括下述 S05，未成年人自动识别服务的关闭阶段包括下述 S06~S07。

S01, 响应于用户对允许自动启动未成年人识别开关的开启操作, 开启未成年人自动识别服务。

其中, 未成年人自动识别服务为在终端设备中预先设置的一个系统级服务, 或者为应用商店提供的一个可供下载安装的应用。未成年人自动识别服务用于在满足预设条件时触发未成年人识别。

以未成年人自动识别服务提供了用户设置入口为例, 在 S01 之后可以执行下述 S02。应理解, 当未成年人自动识别服务没有提供用户设置入口时, 在 S01 之后可直接执行 S03, 而无需执行 S02, 即, S02 为一个可选步骤。

S02, 未成年人自动识别服务进行初始化。

结合上述实施例的描述, 用户可以通过对未成年人识别功能的操作, 设置触发未成年人识别的条件、未成年人识别的方式及未成年人保护操作, 然后未成年人自动识别服务可以在本地保存配置参数。在每次接收到开启操作后, 未成年人自动识别服务可以按照这些配置参数进行初始化。另外, 未成年人自动识别服务还可以向 FWK 层、HAL 层等相关的算法接口和通道接口下发对应的初始化参数, 然后各个接口根据初始化参数进行初始化, 并向未成年人自动识别服务返回初始化成功消息。

S03, 未成年人自动识别服务分析终端设备是否满足预设条件。

其中, 预设条件为预先设置的用于触发开始未成年人识别的条件, 即, 在满足预设条件时会触发开始未成年人识别。

上述预设条件可以为未成年人自动识别服务的默认设置, 也可以为用户的手动设置。

示例性地, 上述预设条件可以包括下述至少一项:

终端设备的亮屏时长大于或等于第一时长;

终端设备在第一时段内亮屏;

应用程序的运行时长大于或等于第二时长;

终端设备在第二时段内运行应用程序;

终端设备正在运行的应用程序属于白名单;

未成年人自动识别服务接收到来自某应用的未成年人识别请求, 该应用为预先与未成年人自动识别服务签订协议的应用;

使用终端设备的当前用户不是机主;

终端设备的使用时长达到固定周期的整数倍。

对于上述预设条件可以参照上述实施例的具体描述, 此处不再赘述。

示例性地, 假设预设条件的数量为多个, 未成年人自动识别服务的预设条件分析模块可以依次遍历每个条件, 以确定是否满足任意一个预设条件。

如果分析结果为不满足所有预设条件, 那么未成年人自动识别服务的预设条件分析模块可以继续下轮判断流程。如果分析结果为满足至少一个预设条件, 那么执行下述 S04。

S04, 未成年人自动识别服务判断当前用户是否为未成年人。

具体地, 未成年人自动识别服务的未成年人识别模块可以判断当前用户是否为未成年人。

作为一种可能的实现方式, 未成年人识别模块可以基于本地存储的年龄识别算法判断当前用户是否为未成年人。比如, 年龄识别算法可以为通过人脸识别年龄算法、通过指纹识别年龄算法和通过声纹识别年龄算法等。这些生物信息识别算法用于计算采集的生物特征信息与监护人在终端设备中预先录入的未成年人生物特征模板的匹配度, 以判断当前用户是否为未成年人; 或者, 用于基于 AI 算法对采集的生物特征信息进行计算, 以判断当前用户的年龄。

再例如，终端设备可以基于设备使用习惯信息判断当前用户是否为未成年人。

作为一种可能的实现方式，未成年人识别模块可以调用第三方的身份验证平台提供的未成年人识别算法，通过识别当前用户的年龄来确定当前用户是否为未成年人。比如，未成年人识别模块可以向身份验证平台识别接口发送调用请求，以由身份验证平台识别接口与第三方平台交互，由第三方平台对终端设备采集的生物特征信息进行识别。

作为又一种可能的实现方式，未成年人识别的条件还可以是系统账号识别。当未成年人识别的条件包括系统账号识别时，未成年人识别模块可以向系统账号识别接口发送调用请求，以由系统账号识别接口提示当前用户输入终端设备的系统账号和/或系统密码，或者输入在上述实施例中为未成年人自动识别服务设置的独立密码。当用户输入密码不正确时，确定当前用户为未成年人。需要说明的是，该系统账号注册时可能已通过年龄选择、实名身份验证或者实名身份验证等方式确认其所有者为成年人。

作为又一种可能的实现方式，未成年人识别的条件还可以是问卷识别。当未成年人识别的条件包括问卷识别时，未成年人识别模块可以向问卷识别接口发送调用请求，以由问卷识别接口提示当前用户回答预设问题。问卷识别接口可以从监护人设定的题库中随机选择一个或多个题目，并提示当前用户进行回答。若当前用户答错题目的数量超过预设数量或预设比例，确定当前用户为未成年人。

对于上述未成年人识别的条件可以参照上述实施例的具体描述，此处不再赘述。

如果识别结果指示当前用户是成年人，那么未成年人自动识别服务可以继续从 S03 开始下轮判断流程。进一步地，在识别结果指示当前用户是成年人时，若终端设备已经处于未成年人保护模式，则需要从未成年人保护模式切换到普通模式，即关闭未成年人保护模式；若终端设备处于普通模式，则需要保持普通模式，即无需开启未成年人保护模式。

如果识别结果指示当前用户是未成年人，那么执行下述 S05。

S05，未成年人自动识别服务向未成年人保护服务或三方应用发送开启未成年人保护模式的指令。

相应地，未成年人保护服务开启未成年人保护模式，执行未成年人保护操作。

作为一种实现方式，未成年人保护服务可以直接开启未成年人保护模式，执行未成年人保护操作。作为另一种实现方式，未成年人保护服务可以先获得监护人的即时授权后，再开启未成年人保护模式，执行未成年人保护操作。其中，该即时授权为未成年人自动识别服务向终端设备绑定的监护设备发送预警消息后由监护设备返回的授权信息。

在本申请实施例中，上述触发开始未成年人识别的预设条件分为两类：

第一类条件包括：接收到来自三方应用的未成年人识别请求，该三方应用为与未成年人自动识别服务签订协议的应用。

示例性地，如果触发开始未成年人识别的预设条件为第一类条件，即接收到与未成年人自动识别服务签订协议的某个三方应用的识别请求，那么在识别到未成年人后，未成年人自动识别服务向该三方应用发送通知消息，从而该三方应用根据自身业务情况进行监控。示例性地，该应用先判断是否自身配置未成年人保护模式，如果配置了未成年人保护模式，那么该应用开启未成年人保护模式，可以理解为三方应用能从应用使用时长、提供服务内容类型或数量、使用功能类型或数量等角度针对未成年人用户进行使用限制或保护。如此，三方应用会开启对自身的保护。

第二类条件包括：亮屏时长大于或等于第一时长、在第一时段内亮屏、应用程序的运行时长大于或等于第二时长、在第二时段内运行应用程序、正在运行的应用程序属于白名单、

当前用户不是机主、终端设备的使用时长达到固定周期的整数倍。

示例性地，如果触发开始未成年人识别的预设条件为第二类条件，那么在识别到未成年人后，未成年人自动识别服务向未成年人保护服务发送开启指令。如此，未成年人保护服务会开启对所有应用的保护。

S06，未成年人自动识别服务响应于用户对允许自动启动未成年人识别开关的关闭操作，显示密码输入框，以提示用户输入密码，之后判断用户在密码输入框中输入的密码是否正确。

如果密码正确，那么执行 S07。

如果密码不正确，那么可以继续从 S03 开始下轮判断流程。

需要说明的是，S06 是以提示用户输入密码为例进行示例说明的。参照上述实施例的描述，终端设备也可以采集当前用户的生物特征识别信息，然后通过比对该生物特征识别信息与预先存储的生物特征识别信息是否匹配，来确定是否允许关闭成年人自动识别服务和未成年人保护服务。

S07，未成年人自动识别服务向未成年人保护服务或三方应用发送关闭通知。然后，关闭未成年人自动识别服务和未成年人保护服务。

在本申请提供的未成年人自动识别和保护方法中，通过在终端设备中预先设置一个未成年人自动识别服务的配置开关，可以供用户选择是否开启该服务。在用户通过对未成年人自动识别服务选项的操作触发终端设备启用未成年人自动识别服务后，未成年人自动识别服务可以检测是否满足预设条件，当满足预设条件时将识别当前用户是否为未成年人，并在识别到当前用户为未成年人的情况下触发未成年人保护服务执行未成年人保护操作。如此，监护人仅需要一次开启未成年人自动识别服务的操作，就可以在识别到当前用户为未成年人的情况下自动执行未成年人保护操作，不用手动频繁开启或关闭未成年人保护模式，简化了用户操作，提高了用户的使用体验。

图 9 为本申请实施例提供的判断是否满足预设条件的一个示例的流程图。

在该示例中，预设条件包括亮屏时长大于第一时长、在第一时段内亮屏、应用程序的运行时长大于第二时长、在第二时段内运行应用程序、正在运行的应用程序属于白名单、接收到来自应用的未成年人识别请求、当前用户不是机主。如图 9 所示，在接收到用户对允许自动启动未成年人识别开关的操作后，未成年人自动识别服务的预设条件分析模块可以执行下述 S11~S18。

S11，预设条件分析模块判断终端设备是否在第一时间段内亮屏。

如果终端设备在第一时间段内亮屏，那么执行下述 S12。

如果终端设备没有在第一时间段内亮屏，那么执行下述 S13。

S12，预设条件分析模块判断终端设备在第一时间段内的亮屏时长是否大于第一时长。

如果终端设备在第一时间段内的亮屏时长大于第一时长，那么开始未成年人识别流程。

如果终端设备在第一时间段内的亮屏时长小于或等于第一时长，那么执行下述 S13。

S13，预设条件分析模块判断终端设备是否在第二时段内运行应用。

如果终端设备在第二时段内运行应用，那么执行下述 S14。

如果终端设备没有在第二时段内运行应用，那么执行下述 S15。

S14，预设条件分析模块判断在第二时段内应用的运行时长是否大于第二时长。

如果在第二时段内应用的运行时长大于第二时长，那么开始未成年人识别流程。

如果在第二时段内应用的运行时长小于或等于第二时长，执行下述 S15。

S15，预设条件分析模块判断终端设备正在运行的应用是否属于白名单。

如果终端设备正在运行的应用属于白名单，那么开始未成年人识别流程。

如果终端设备正在运行的应用不属于白名单，那么执行下述 S16。

S16，预设条件分析模块判断终端设备是否接收到来自某应用的未成年人识别请求，该应用为与未成年人自动识别服务签订协议的应用。

如果未成年人自动识别服务接收到来自任意一个签订协议应用的预设消息格式的识别请求，那么开始未成年人识别流程。

如果未成年人自动识别服务没有接收到来自任意一个签订协议应用的识别请求，或者，接收到来自签订协议应用的识别请求不符合预设消息格式，那么执行下述 S17。

S17，预设条件分析模块判断使用终端设备的当前用户是否为机主。

如果使用终端设备的当前用户是机主，那么执行下述 S18。

如果使用终端设备的当前用户不是机主，那么开始未成年人识别流程。

S18，预设条件分析模块等待第三时长，并在计时时长达到第三时长后，从 S11 开始下轮判断流程。其中，第三时长为未成年人自动识别服务的默认设置，也可以为用户的手动设置。

图 10 为本申请实施例提供的判断是否满足预设条件的另一个示例的流程图。

在该示例中，预设条件包括亮屏时长大于第一时长、在第一时段内亮屏、应用程序的运行时长大于第二时长、在第二时段内运行应用程序、正在运行的应用程序属于白名单、接收到来自应用的未成年人识别请求、当前用户不是机主。如图 10 所示，在接收到用户对允许自动启动未成年人识别开关的操作后，可以执行下述 S11'~S18'。

S11'，预设条件分析模块判断终端设备是否在第一时间段内亮屏。

如果终端设备在第一时间段内亮屏，那么执行下述 S12'。

如果终端设备没有在第一时间段内亮屏，那么执行下述 S13'。

S12'，预设条件分析模块判断终端设备在第一时间段内的亮屏时长是否大于第一时长。

如果终端设备在第一时间段内的亮屏时长大于第一时长，那么执行下述 S17'。

如果终端设备在第一时间段内的亮屏时长小于或等于第一时长，那么执行下述 S13'。

S13'，预设条件分析模块判断终端设备是否在第二时段内运行应用。

如果终端设备在第二时段内运行应用，那么执行下述 S14'。

如果终端设备没有在第二时段内运行应用，那么执行下述 S15'。

S14'，预设条件分析模块判断在第二时段内应用的运行时长是否大于第二时长。

如果在第二时段内应用的运行时长大于第二时长，那么执行下述 S17'。

如果在第二时段内应用的运行时长小于或等于第二时长，执行下述 S15'。

S15'，预设条件分析模块判断终端设备正在运行的应用是否属于白名单。

如果终端设备正在运行的应用属于白名单，那么执行下述 S17'。

如果终端设备正在运行的应用不属于白名单，那么执行下述 S16'。

S16'，预设条件分析模块判断终端设备是否接收到来自某应用的识别请求，该应用为与未成年人自动识别服务签订协议的应用。

如果未成年人自动识别服务接收到来自任意一个签订协议应用的预设消息格式的识别请求，那么执行下述 S17'。

如果未成年人自动识别服务没有接收到来自任意一个签订协议应用的识别请求，或者，接收到来自签订协议应用的识别请求不符合预设消息格式，那么执行下述 S18'。

S17'，预设条件分析模块判断使用终端设备的当前用户是否为机主。

如果使用终端设备的当前用户是机主，那么执行下述 S18'。

如果使用终端设备的当前用户不是机主，那么开始未成年人识别流程。

S18'，未成年人自动识别服务等待第三时长，并在计时时长达到第三时长后，从 S11' 开始下轮判断流程。其中，第三时长为未成年人自动识别服务的默认设置，也可以为用户的手动设置。

应理解，与图 9 对应的示例相比，在图 10 对应的示例中，在确定满足在第一时段内亮屏时长大于第一时长、在第二时段内应用的运行时长大于第二时长、正在运行的应用程序属于白名单、或接收到来自应用的未成年人识别请求后，增加一个判断当前用户是否为机主的步骤，如此在一定程度降低了误触发未成年人识别的可能性。

需要说明的是，上述图 9 或图 10 的示例仅是一种可能的实现方式，并不对本申请实施例如何判断终端是否满足预设条件的实现逻辑造成限定。

图 11 为本申请实施例提供的判断当前用户是否为未成年人的一个示例的流程图。

在该示例中，未成年人识别方式包括生物信息识别和系统账号识别，或者，包括生物信息识别和问卷识别。如图 11 所示，开始未成年人识别后，未成年人自动识别服务的未成年人识别模块可以执行下述 S21~S29。

S21，未成年人识别模块开始计时。

S22，未成年人识别模块采集使用终端设备的当前用户的生物特征信息。

S23，未成年人识别模块判断该生物特征信息是否符合未成年人特征。

如果该生物特征信息符合未成年人特征，那么执行下述 S24。

如果该生物特征信息不符合未成年人特征，那么执行下述 S25。

S24，未成年人识别模块判断在开始计时后是否第 N 次符合未成年人特征。N 为大于或等于 2 的整数。

如果已经达到第 N 次符合未成年人特征，那么说明误判为未成年人的概率较低，可以执行下述 S26 或 S28。

如果尚未达到第 N 次符合未成年人特征，那么说明存在误判为未成年人的可能性，可以返回继续执行上述 S22。

S25，未成年人识别模块判断计时时长是否大于预设时长。

如果计时时长尚未达到预设时长，那么可以返回继续执行上述 S22。

如果计时时长已经达到预设时长，仍不能达到第 N 次符合未成年人特征，那么说明当前用户是未成年人的概率非常低，可以从上述实施例的 S03 开始执行下轮判断流程。

S26，未成年人识别模块提示当前用户输入密码。该密码可以为用户设定的“请求未成年人识别的 APP”的账号密码、支付密码、登录密码和系统密码等。

S27，未成年人识别模块判断用户输入的密码与预设密码是否匹配。

如果用户输入的密码与预设密码匹配，那么说明当前用户是未成年人的概率非常低，可以从上述实施例的 S03 开始执行下轮判断流程。

如果用户输入的密码与预设密码不匹配，说明当前用户是未成年人的概率较高，可以执行未成年人保护操作。

示例性地，图 12A~图 12D 为本申请实施例提供的一组用户输入密码的界面示意图。如图 12A 所示，终端设备正在运行视频 APP。如果终端设备检测到视频 APP 属于白名单应用，那么终端设备可以显示如图 12B 所示的提示消息 255 和密码输入框 256。如图 12C 所示，用户可以在密码输入框 256 中输入四位密码 257。由于本次输入的四位密码 257 与先前设置的四位密码 206 不匹配，那么说明当前用户为未成年人，可以开启未成年人保护模式，比如强

制关闭视频 APP。另外，终端设备还可以显示如图 12D 所示的“密码错误，已开启未成年人保护模式”的提示消息 258。

S28，未成年人识别模块提示当前用户回答预设问题。

该预设问题可以为监护人设定的题库中随机选择一个或多个题目。

S29，未成年人识别模块判断用户回答的答案与预设答案是否匹配。

如果用户回答的答案与预设答案匹配，那么说明当前用户是未成年人的概率非常低，可以从上述实施例的 S03 开始执行下轮判断流程。

如果用户回答的答案与预设答案不匹配，说明当前用户是未成年人的概率较高，可以执行未成年人保护操作。

示例性地，图 13A~图 13D 为本申请实施例提供的一组用户回答问题的界面示意图。如图 13A 所示，终端设备正在运行视频 APP。如果终端设备检测到视频 APP 属于白名单应用，那么终端设备可以显示如图 13B 所示的问卷框 259。如图 13C 所示，问卷框 259 的待回答试题可以依次更新显示，直至用户完成所有题目作答。若当前用户答错题目的数量超过预设数量或预设比例，那么说明当前用户为未成年人，可以开启未成年人保护模式，比如强制关闭视频 APP。另外，终端设备还可以显示如图 13D 所示的“密码错误，已开启未成年人保护模式”的提示消息 260。

需要说明的是，上述图 11 所述示例仅是一种可能的实现方式，并不对本申请实施例如何进行未成年人识别的实现逻辑造成限定。

应理解，与传统手动频繁开启或关闭未成年人保护模式相比，通过生物信息识别、密码识别、问卷识别等方式可以自动识别未成年人，并在识别到当前用户为未成年人的情况下自动开启未成年人保护模式，简化了用户操作。

图 14 为本申请实施例提供的开启未成年人保护的一个示例的流程图。如图 14 所示，开始未成年人识别后，可以执行下述 S401~S414。

S401，未成年人自动识别服务判断是否已安装未成年人保护软件。

如果已安装未成年人保护软件，那么执行下述 S402~S405。

如果未安装未成年人保护软件，那么执行下述 S406~S410，或执行下述 S411~S414。

需要说明的是，上述 S402~S405、S406~S410、S411~S414 仅是一种示例性的实现方案，其并不对本申请实施例形成限定。

S402，未成年人自动识别服务判断是否已绑定监护设备。

如果已绑定监护设备，那么执行下述 S403。

S403，未成年人自动识别服务通过通信模块向监护设备发送预警消息。

示例性地，未成年人自动识别服务可以根据监护设备的电话号码、邮箱地址或系统账号等，向监护设备发送预警消息。该预警消息用于向使用监护设备的监护人进行提示，被监护人正在使用终端设备，是否授权被监护人继续使用终端设备。相应地，监护设备收到预警消息后，可以以图片、文字或声音等形式提示监护人。如果监护人输入授权操作，那么监护设备向终端设备返回授权信息。

S404，未成年人自动识别服务判断是否接收到来自监护设备的授权信息。

如果接收到来自监护设备的授权信息，那么执行下述 S405。

S405，未成年人自动识别服务向未成年人保护服务发送开启指令。相应地，未成年人保护服务开启未成年人保护模式，执行未成年人保护操作。

S406，未成年人自动识别服务判断是否已绑定监护设备。

如果已绑定监护设备，那么执行下述 S407。

如果没有监护设备，那么执行下述 S409。

S407，未成年人自动识别服务通过通信模块向监护设备发送预警消息。

示例性地，未成年人自动识别服务可以根据监护设备的电话号码、邮箱地址或系统账号等，向监护设备发送预警消息。该预警消息用于向使用监护设备的监护人进行提示，被监护人正在使用终端设备，是否授权被监护人继续使用终端设备，以及是否授权下载安装未成年人保护软件。

S408，未成年人自动识别服务判断是否接收到来自监护设备的授权信息。

如果接收到来自监护设备的授权信息，那么执行下述 S409。

S409，从应用商店下载未成年人保护软件，并安装该软件。

S410，开启未成年人保护模式，执行未成年人保护操作。

S411，从应用商店下载未成年人保护软件，并安装该软件。

S412，开启未成年人保护模式，执行未成年人保护操作。

S413，未成年人自动识别服务判断是否已绑定监护设备。

如果已绑定监护设备，那么执行下述 S414。

S414，未成年人自动识别服务通过通信模块向监护设备发送预警消息。

示例性地，未成年人自动识别服务可以根据监护设备的电话号码、邮箱地址或系统账号等，向监护设备发送预警消息。该预警消息用于向使用监护设备的监护人进行提示，被监护人正在使用终端设备，已开启未成年人保护模式。

需要说明的是，终端设备与监护设备之间的消息格式为预先协定的。

另外，监护设备除了向终端设备返回授权信息，还可以返回拒绝信息，或不返回任何信息。如果返回拒绝信息，或不返回任何信息，那么不开启未成年人保护模式，也不会下载安装未成年人保护软件。

需要说明的是，上述图 14 所述示例仅是一种可能的实现方式，并不对本申请实施例如何进行未成年人保护的实现逻辑造成限定。

应理解，根据终端设备是否已绑定监护设备、是否安装未成年人保护软件，可以执行不同的未成年人保护策略。通过绑定监护设备，可以在识别到使用终端设备的用户为未成年人时，及时向监护人使用的监护设备发出预警消息。另外，通过安装未成年人保护软件，可以由未成年人保护软件提供过滤不良信息、阻止未经授权购买、拦截欺诈网站等未成年人保护服务。

图 15 为本申请实施例提供的三方应用请求未成年人自动识别的一个示例的流程图。如图 15 所示，该方法可以包括下述 A01~A17。

A01，响应于用户对允许自动启动未成年人识别开关的开启操作，开启未成年人自动识别服务。

以未成年人自动识别服务提供了用户设置入口为例，在 A01 之后可执行下述 A02。应理解，当未成年人自动识别服务没有提供用户设置入口时，在 A01 之后可直接执行 A05，而无需执行 A02。

A02，未成年人自动识别服务进行初始化。

对于 A01 和 A02 的实现方式，可以参照上述实施例对 S01~S02 的具体描述。

需要说明的是，在 A02 中，未成年人自动识别服务还向与其预先签订协议的各个三方应用下发初始化参数，用于指示已开启未成年人自动识别服务，从而各个三方应用可以开始判

断是否满足发送未成年人识别请求的条件，即执行下述 A03。对于未成年人自动识别服务与三方应用签订协议的方式可以参照上述实施例对图 5K~图 5N 的描述，此处不再赘述。

A03，三方应用判断是否满足发送未成年人识别请求的条件。

在三方应用完成初始化后，可以检测是否满足下述条件：APP 运行达到预设时长、调用支付类 APP、运行时段为预设时段、使用非常用功能、输入密码错误、接收到用户关闭三方应用所配置未成年人保护模式的操作。当某个应用满足这些条件中的任意一个条件时均会触发未成年人自动识别，即执行下述 A04。对于这些条件，可以参照上述实施例对图 5K~图 5N 的描述，此处不再赘述。

A04，该三方应用向未成年人自动识别服务发送未成年人识别请求。

A05，未成年人自动识别服务响应于该未成年人识别请求，分析在本轮判断中是否接收到来自三方应用的未成年人识别请求。

如果分析结果为没有接收到来自三方应用的未成年人识别请求，且不满足其他预设条件，那么未成年人自动识别服务可以继续从 A05 开始下轮判断流程。如果分析结果为接收到来自三方应用的未成年人识别请求，那么执行下述 A06。

示例性地，未成年人自动识别服务和三方应用可以预先协定双方发送消息时的格式和内容。若三方应用发送的未成年人识别请求符合预设格式，且该未成年人识别请求携带预设内容，则未成年人自动识别服务确定终端设备满足预设条件。

A06，未成年人自动识别服务判断当前用户是否为未成年人。

示例性地，未成年人自动识别服务向年龄识别算法发送未成年人识别请求。年龄算法计算用户年龄以判断当前用户是否为未成年人。然后，年龄算法将未成年人识别结果返回至自动识别服务。之后，未成年人自动识别服务根据识别结果，判断当前用户是否为未成年人。

如果识别结果指示当前用户不是未成年人，那么未成年人自动识别服务可以继续从 A05 开始下轮判断流程。

如果识别结果指示当前用户是未成年人，那么执行下述 A07。

A07，未成年人自动识别服务向三方应用发送开启指令，以指示开启未成年人保护模式。

A08，三方应用判断自身是否具备未成年人保护能力。

如果三方应用具备未成年人保护能力，那么执行下述 A09~A12。

如果三方应用不具备未成年人保护能力，那么执行下述 A13~A15。

A09，三方应用判断该应用是否绑定监护设备。

如果三方应用绑定了监护设备，那么执行下述 A10~A11。

如果三方应用没有绑定监护设备，那么执行下述 A12。

A10，三方应用向绑定的监护设备发送预警消息。

三方应用可以根据监护设备的电话号码、邮箱地址或系统账号等，向监护设备发送预警消息。该预警消息用于向使用监护设备的监护人进行提示，被监护人正在使用终端设备，是否授权被监护人继续使用终端设备。相应地，监护设备收到预警消息后，可以以图片、文字或声音等形式提示监护人。如果监护人输入授权操作，那么执行下述 A11。

A11，监护设备向终端设备返回授权信息。

A12，三方应用开启自身的未成年人保护模式。

其中，三方应用自身携带的未成年人保护模式用于过滤该应用内的、不适宜未成年人观看的部分内容，限制当前用户使用应用内部分功能（如支付功能），以及管理该应用的使用时间等。

上述 A11 和 A12 是以先获取监护人的即时授权，再开启未成年人保护模式为例进行示例说明的，其并不对本申请实施例形成限定。在实际实现时，也可以直接开启未成年人保护模式，执行未成年人保护操作。

需要说明的是，上述 A09~A12 仅是一种示例性的实现方案，其并不对本申请实施例形成限定。在实际实现时，也可以采用其他实现方案。比如，三方应用本身可以直接进行未成年人保护。再例如，三方应用可以通知系统开启系统级未成年人保护功能，以通过系统级未成年人保护功能对该应用的使用时长进行管控或限制。

A13，三方应用向未成年人自动识别服务发送请求消息，以请求开启未成年人保护服务。

A14，未成年人自动识别服务向未成年人保护服务发送开启指令。

A15，未成年人保护服务开启未成年人保护模式，执行未成年人保护操作。

其中，未成年人保护服务为一款专门的未成年人保护软件，用于对终端设备中的所有应用或指定应用进行未成年人保护。比如，建立适宜青少年访问的网站库，过滤掉广告弹窗和骚扰拦截信息，时间管理和绿色护眼功能等。在该实施例中，未成年人保护服务也可以仅针对该三方应用的使用进行管控。

A16，未成年人自动识别服务响应于用户对允许自动启动未成年人识别开关的关闭操作，显示密码输入框，以提示用户输入密码，之后判断用户在密码输入框中输入的密码是否正确。

如果密码正确，那么执行 A17。

如果密码不正确，那么可以继续从 A05 开始下轮判断流程。

A17，关闭未成年人自动识别服务。

如果先前开启了三方应用的未成年人保护模式，那么未成年人自动识别服务向三方应用发送关闭通知，以关闭三方应用的未成年人保护模式。

如果先前开启了未成年人保护服务的未成年人保护模式，那么未成年人自动识别服务向未成年人保护服务发送关闭通知，以关闭未成年人保护服务的未成年人保护模式。

需要说明的是，上述实施例是以当识别到未成年人后，优先向请求未成年人识别的三方应用发送开启指令为例进行说明的，其并不对本申请实施例形成限定。在实际实现时，也可以直接向未成年人保护服务发送开启指令，以对所有应用或指定应用进行未成年人保护。

在本申请提供的未成年人自动识别和保护方法中，尽管一部分三方应用具备未成年人保护能力，但是需要用户手动开启，特别是当开启未成年人保护模式的三方应用较多时，操作特别繁琐。本申请提供的未成年人自动识别服务为一个对三方应用统一管理的平台，可以在识别到当前用户为未成年人的情况下，自动触发开启未成年人保护模式，不用手动频繁开启或关闭未成年人保护模式，提高了使用体验。另外，为了简化三方应用，某些三方应用可能并不具备未成年人保护能力，本申请提供的未成年人自动识别服务也能够为这些三方应用提供未成年人保护。

本申请实施例还提供了一种终端设备，包括处理器，处理器与存储器耦合，处理器用于执行存储器中存储的计算机程序或指令，以使得终端设备实现上述各实施例中的方法。

本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有计算机指令：当该计算机可读存储介质在终端设备上运行时，使得该终端设备执行如上所示的方法。该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机指令可以从一个网站站点、计算机、服务器或者数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进

行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可以用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质（例如，软盘、硬盘或磁带），光介质或者半导体介质（例如固态硬盘（solid state disk, SSD））等。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机程序代码，当计算机程序代码在计算机上运行时，使得计算机执行上述各实施例中的方法。

本申请实施例还提供了一种芯片，该芯片与存储器耦合，该芯片用于读取并执行存储器中存储的计算机程序或指令，以执行上述各实施例中的方法。该芯片可以为通用处理器，也可以为专用处理器。需要说明的是，该芯片可以使用下述电路或者器件来实现：一个或多个现场可编程门阵列（field programmable gate array, FPGA）、可编程逻辑器件（programmable logic device, PLD）、控制器、状态机、门逻辑、分立硬件部件、任何其他适合的电路、或者能够执行本申请通篇所描述的各种功能的电路的任意组合。

上述本申请实施例提供的终端设备、计算机可读存储介质、计算机程序产品以及芯片均用于执行上文所提供的方法，因此，其所能达到的有益效果可参考上文所提供的方法对应的有益效果，此处不再赘述。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以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，模块或单元的划分，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装置，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，机械或其它的形式。

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一个物理单元或多个物理单元，即可以位于一个地方，或者也可以分布到多个不同地方。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。

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。上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。

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，可以存储在一个可读存储介质中。基于这样的理解，本申请实施例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，该软件产品存储在一个存储介质中，包括若干指令用以使得一个设备（可以是单片机，芯片等）或处理器（processor）执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read only memory, ROM）、随机存取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上内容，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何在本申请揭露的技术范围内的变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1. 一种未成年人自动识别和保护的方法，其特征在于，所述方法应用于终端设备，所述终端设备设置有未成年人自动识别服务、未成年人保护服务和三方应用，所述方法包括：

响应于用户的第一操作，所述终端设备开启所述未成年人自动识别服务；

所述未成年人自动识别服务检测是否满足触发未成年人识别的条件；

在确定所述终端设备满足所述触发未成年人识别的条件的前提下，所述未成年人自动识别服务识别使用所述终端设备的用户是否为未成年人；

若使用所述终端设备的用户为未成年人，则所述未成年人自动识别服务向所述未成年人保护服务或所述三方应用发送开启未成年人保护模式的指令。

2. 根据权利要求1所述的方法，其特征在于，所述触发未成年人识别的条件包括下述至少一项：

所述终端设备的亮屏时长大于或等于第一时长；

所述终端设备在第一时段内亮屏；

应用程序的运行时长大于或等于第二时长；

所述终端设备在第二时段内运行应用程序；

所述终端设备正在运行的应用程序属于白名单；

所述未成年人自动识别服务接收到来自所述三方应用的未成年人识别请求；

使用所述终端设备的用户不是机主；

所述终端设备的使用时长达到固定周期的整数倍。

3. 根据权利要求2所述的方法，其特征在于，所述白名单包括多个类别的应用程序，所述多个类别中的每个类别分别对应一个时长；

所述终端设备满足所述触发未成年人识别的条件，包括：

所述终端设备正在运行的第一应用程序属于第一类别，且所述第一应用程序的运行时长大于或等于与所述第一类别对应的时长，其中，所述第一类别为所述多个类别中的任意一个类别。

4. 根据权利要求2所述的方法，其特征在于，

所述未成年人自动识别服务检测是否满足触发未成年人识别的条件，包括：

所述三方应用检测是否满足触发发送所述未成年人识别请求的条件；

所述三方应用在满足触发发送所述未成年人识别请求的条件的前提下，向所述未成年人自动识别服务发送所述未成年人识别请求；

所述未成年人自动识别服务基于所述未成年人识别请求判断是否满足所述触发未成年人识别的条件；

所述确定所述终端设备满足所述触发未成年人识别的条件，包括：

若所述未成年人自动识别服务确定所述未成年人识别请求符合预设格式，且所述未成年人识别请求携带预设内容，则所述未成年人自动识别服务确定满足所述触发未成年人识别的条件。

5. 根据权利要求4所述的方法，其特征在于，在所述三方应用检测是否满足触发发送所述未成年人识别请求的条件之前，所述方法还包括：

所述未成年人自动识别服务向所述三方应用发送初始化参数，所述初始化参数用于指示已开启所述未成年人自动识别服务。

6. 根据权利要求4或5所述的方法,其特征在於,所述触发发送所述未成年人识别请求的条件包括下述至少一项:

所述三方应用的运行时长大于或等于第三时长;

所述三方应用的运行时段为预设时段;

所述三方应用调用支付类应用;

所述三方应用使用非常用功能;

所述三方应用的输入密码错误;

所述三方应用接收到用户关闭未成年人保护模式的操作。

7. 根据权利要求4至6中任一项所述的方法,其特征在於,所述未成年人自动识别服务向所述三方应用发送开启未成年人保护模式的指令,包括:

所述未成年人自动识别服务采用所述预设格式,向所述三方应用发送开启所述未成年人保护模式的指令;

所述三方应用响应于所述指令,开启所述未成年人保护模式。

8. 根据权利要求1至7中任一项所述的方法,其特征在於,所述未成年人自动识别服务采用下述至少一种方式,识别使用所述终端设备的用户是否为未成年人:

所述未成年人自动识别服务调用年龄识别接口,由所述年龄识别接口根据使用所述终端设备的用户的生物特征信息和设备使用习惯信息中的至少一项确定所述用户的年龄;

所述未成年人自动识别服务调用系统账号识别接口,由所述系统账号识别接口提示用户输入密码,并判断用户输入的密码与预设密码是否匹配;

所述未成年人自动识别服务调用问卷识别接口,由所述问卷识别接口提示用户回答预设问题,并判断用户的答案与预设答案是否匹配。

9. 根据权利要求1至8中任一项所述的方法,其特征在於,所述未成年人自动识别服务向所述未成年人保护服务发送开启未成年人保护模式的指令,包括:

所述未成年人自动识别服务检测所述终端设备是否已安装所述未成年人保护服务;

在已安装所述未成年人保护服务的情况下,所述未成年人自动识别服务执行下述步骤:直接向所述未成年人保护服务发送开启所述未成年人保护模式的指令;或者,在获得监护人的即时授权后,向所述未成年人保护服务发送开启所述未成年人保护模式的指令;

在未安装所述未成年人保护服务的情况下,所述未成年人自动识别服务执行下述步骤:直接向所述终端设备请求下载安装所述未成年人保护服务,之后向所述未成年人保护服务发送开启所述未成年人保护模式的指令;或者,在获得监护人的即时授权后,向所述终端设备请求下载安装所述未成年人保护服务,之后向所述未成年人保护服务发送开启所述未成年人保护模式的指令;

其中,所述即时授权为所述未成年人自动识别服务向所述终端设备绑定的监护设备发送预警消息后由所述监护设备返回的授权信息。

10. 根据权利要求1至9中任一项所述的方法,其特征在於,所述响应于用户的第一操作,所述终端设备开启所述未成年人自动识别服务,包括:

响应于用户的所述第一操作,所述终端设备判断所述第一操作是否为首次开启所述未成年人自动识别服务的操作;

当所述第一操作为首次开启所述未成年人自动识别服务的操作时,所述终端设备提示用户输入身份验证信息,并保存用户输入的第一身份验证信息,以及开启所述未成年人自动识

别服务；其中，所述身份验证信息包括以下至少一项：用户密码和生物特征识别信息。

11. 根据权利要求 10 所述的方法，其特征在于，所述开启所述未成年人自动识别服务之后，所述方法还包括：

响应于用户的第二操作，所述终端设备再次提示用户输入身份验证信息，所述第二操作为触发关闭所述未成年人自动识别服务的操作；

当用户输入的第二身份验证信息与所述第一身份验证信息相同时，所述未成年人自动识别服务向所述未成年人保护服务或所述三方应用发送关闭所述未成年人保护模式的指令；

所述终端设备关闭所述未成年人自动识别服务。

12. 根据权利要求 1 至 11 中任一项所述的方法，其特征在于，所述未成年人自动识别服务识别使用所述终端设备的用户是否为未成年人之后，所述方法还包括：

若使用所述终端设备的用户为成年人，则在已开启所述未成年人保护模式的情况下，所述未成年人自动识别服务向所述未成年人保护服务或所述三方应用发送关闭所述未成年人保护模式的指令。

13. 一种终端设备，其特征在于，包括处理器，以及与所述处理器耦合的存储器；其中，所述存储器中存储有指令，所述处理器执行所述指令时，使得所述终端设备执行如权利要求 1 至 12 中任一项所述的未成年人自动识别和保护方法。

14. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，当所述计算机程序在终端设备上运行时，使得所述终端设备执行如权利要求 1 至 12 中任一项所述的未成年人自动识别和保护方法。

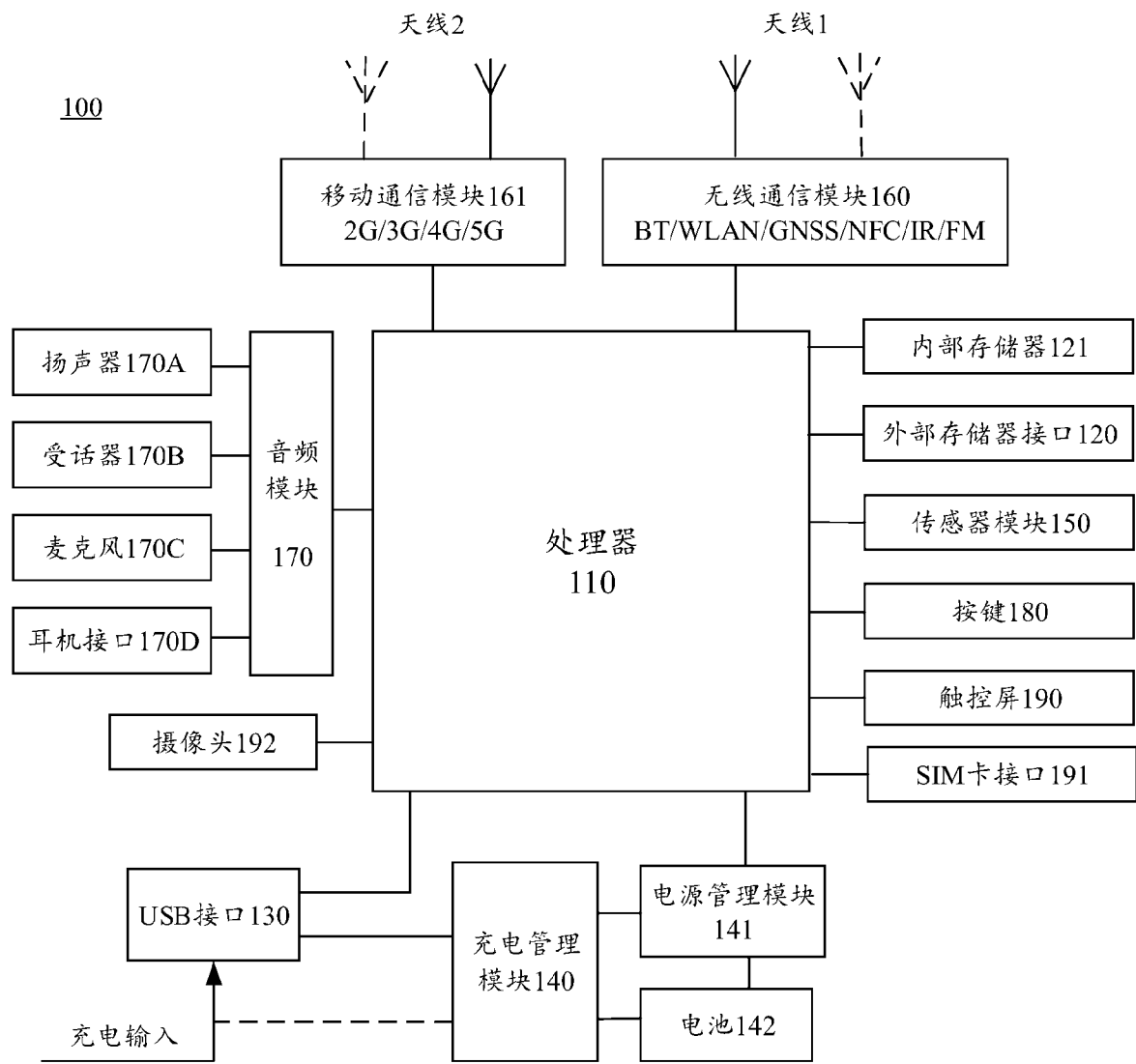


图 1

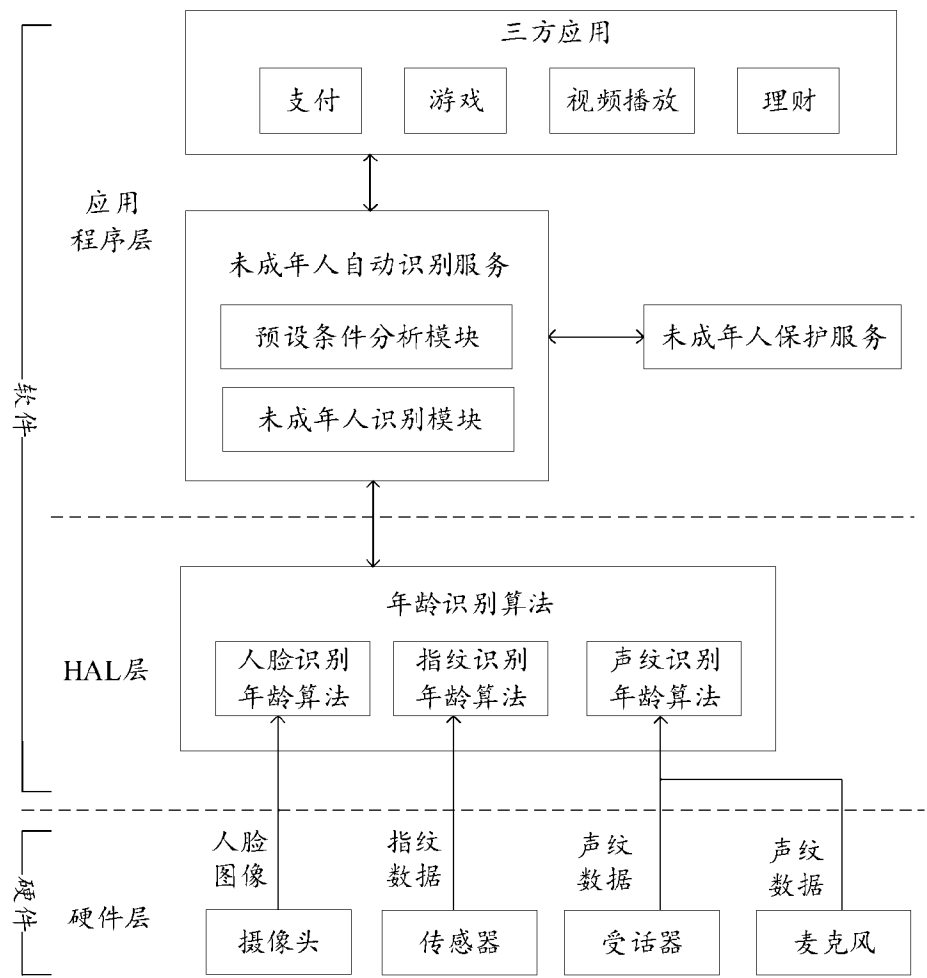


图 2

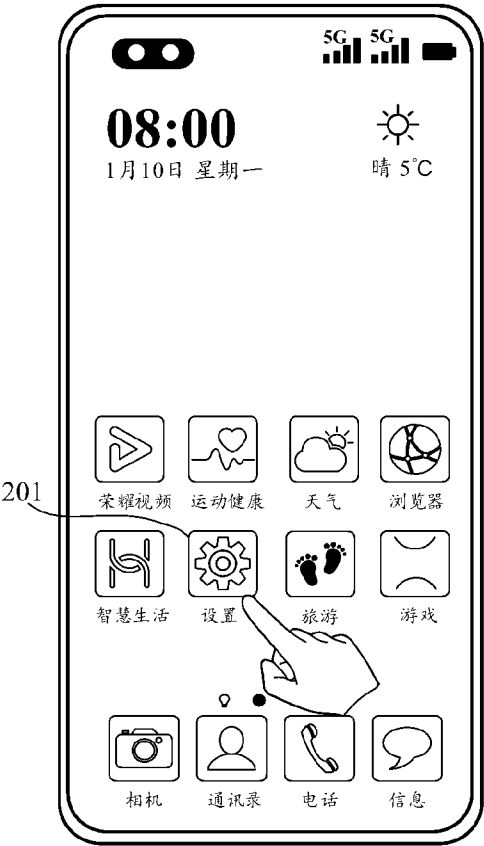


图3A

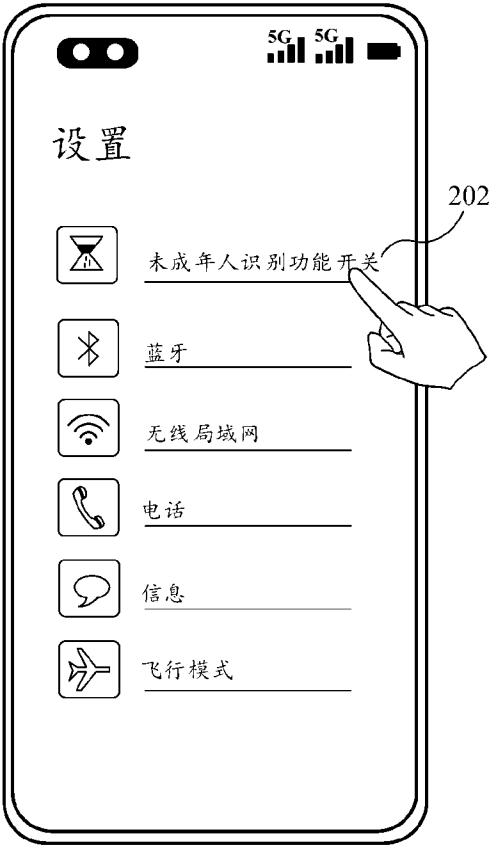


图3B

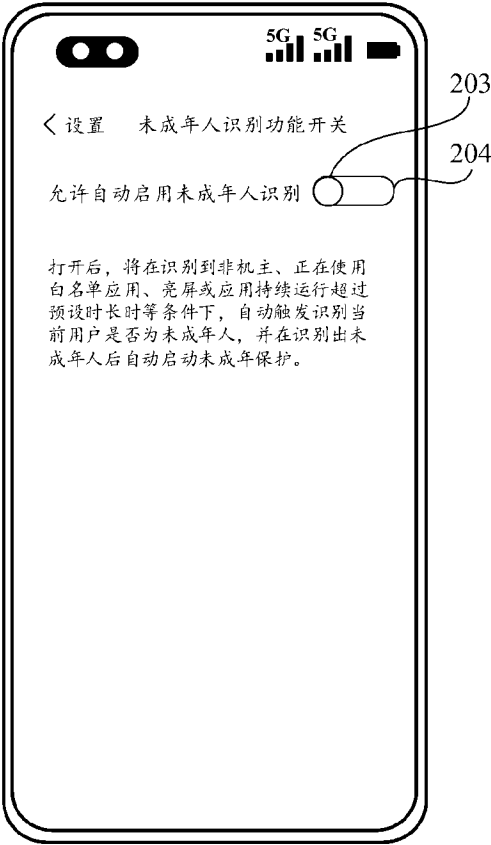


图3C

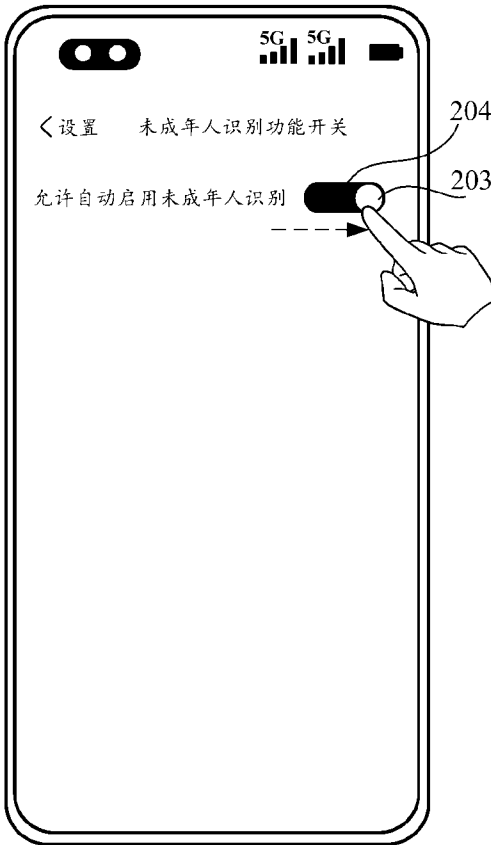


图3D

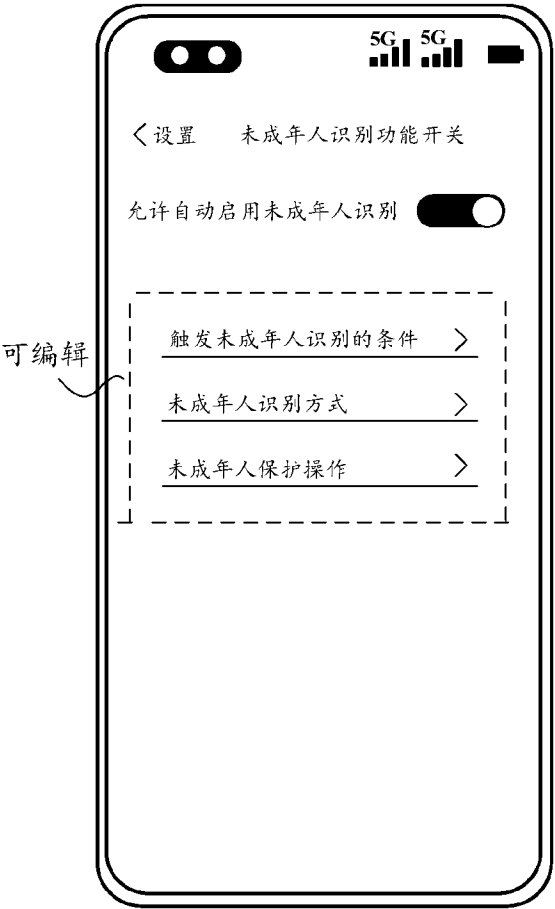


图3E

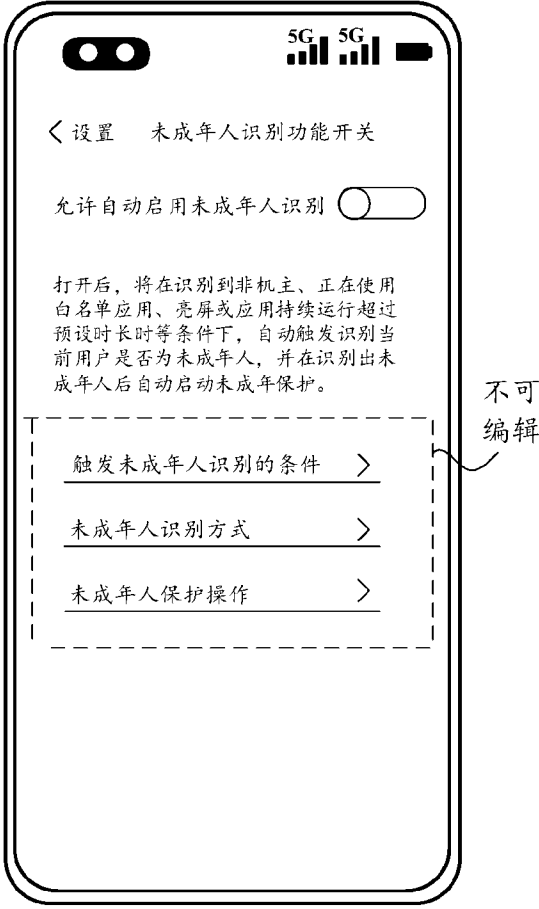
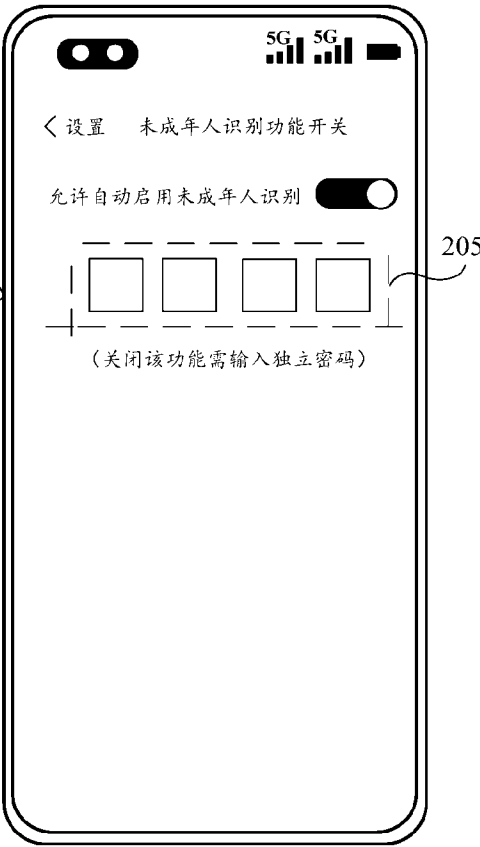
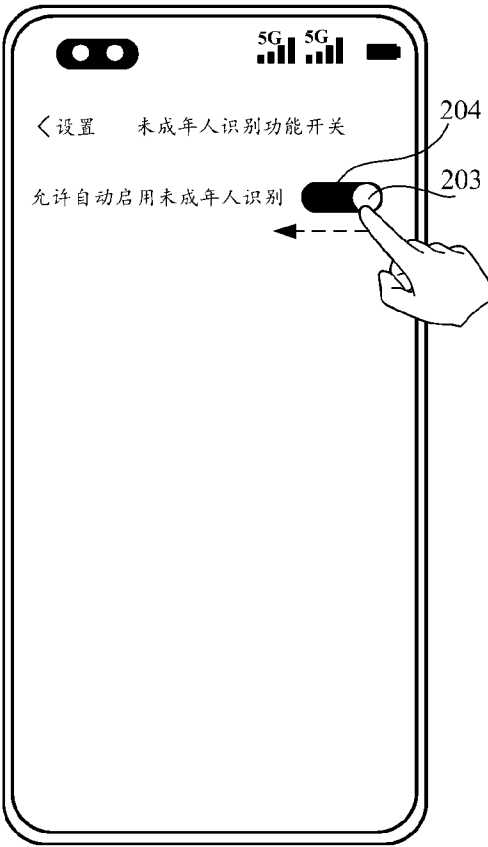
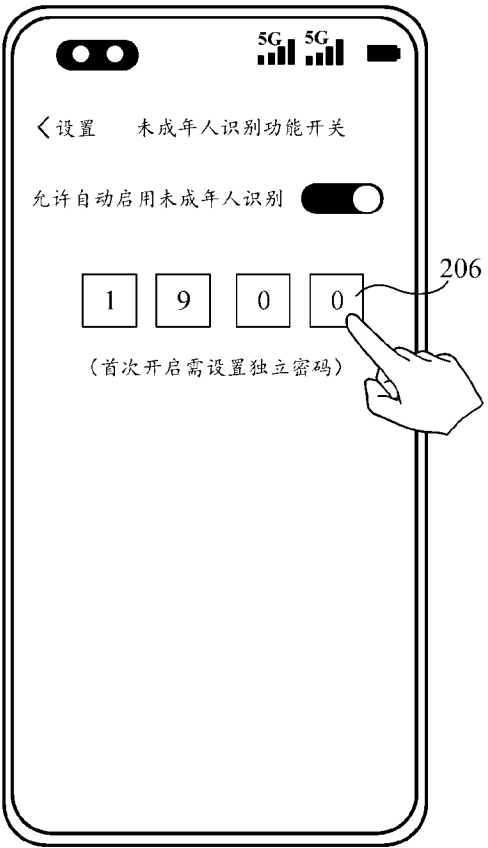
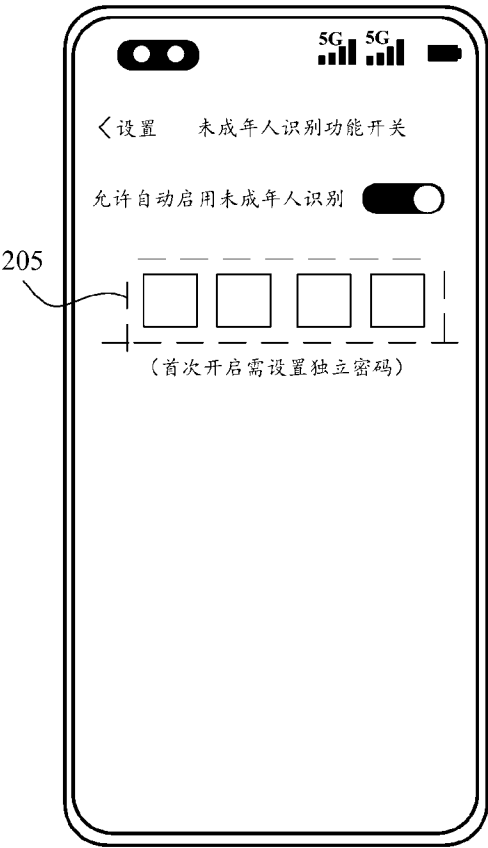


图3F



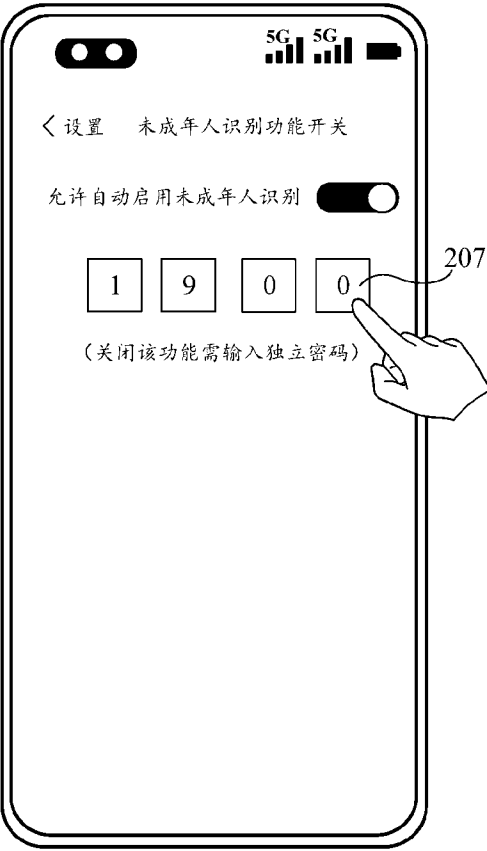


图4E

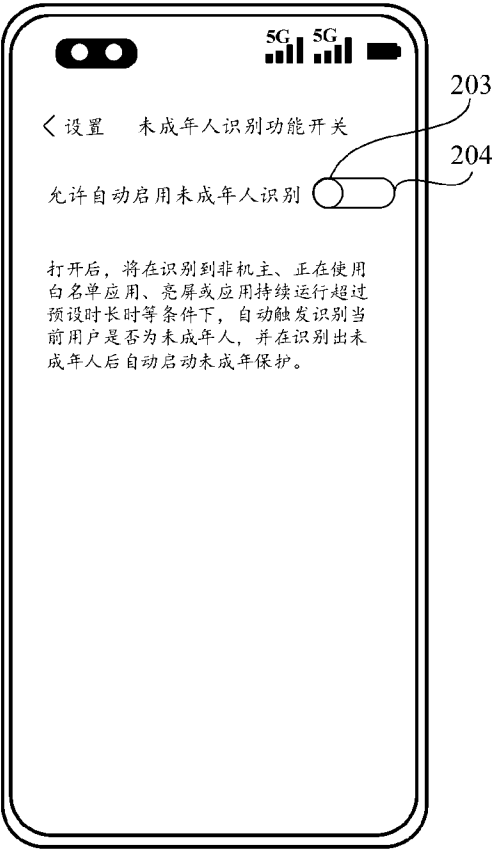


图4F



图4G

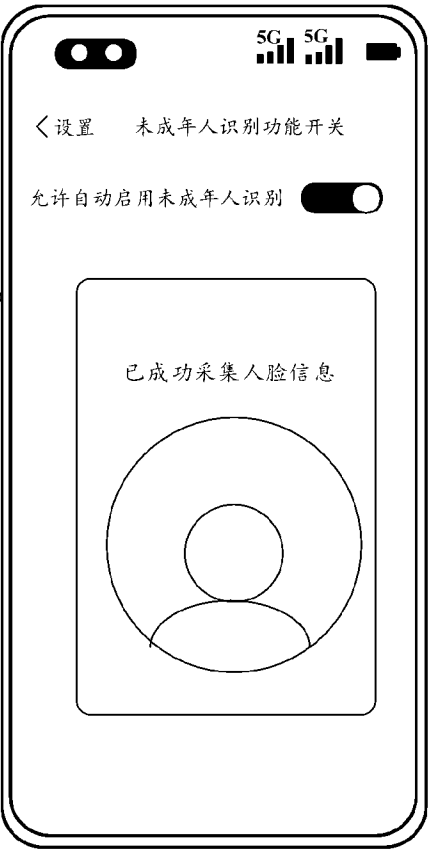


图4H

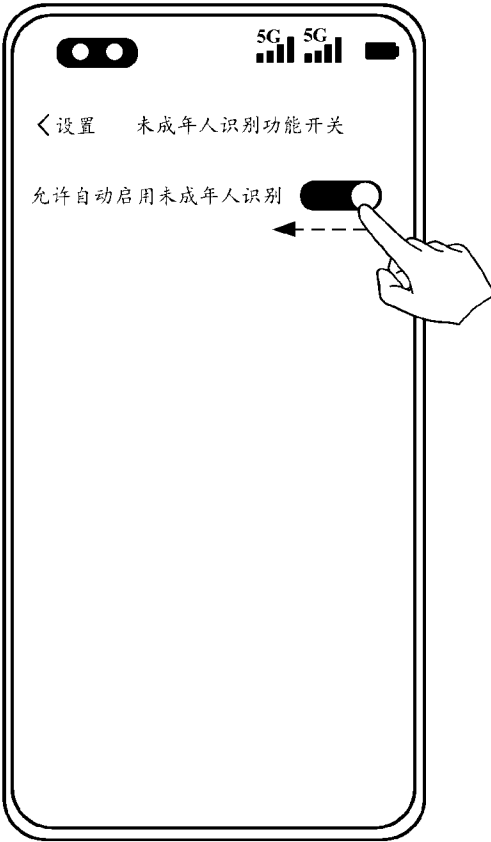


图4I



图4J

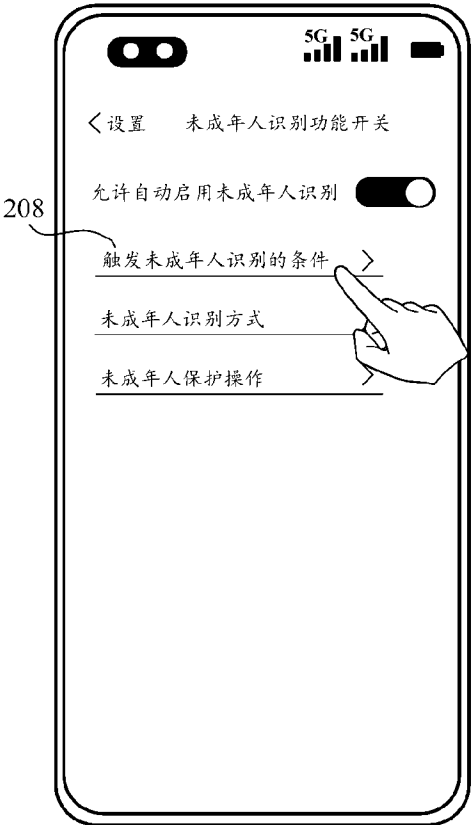


图5A

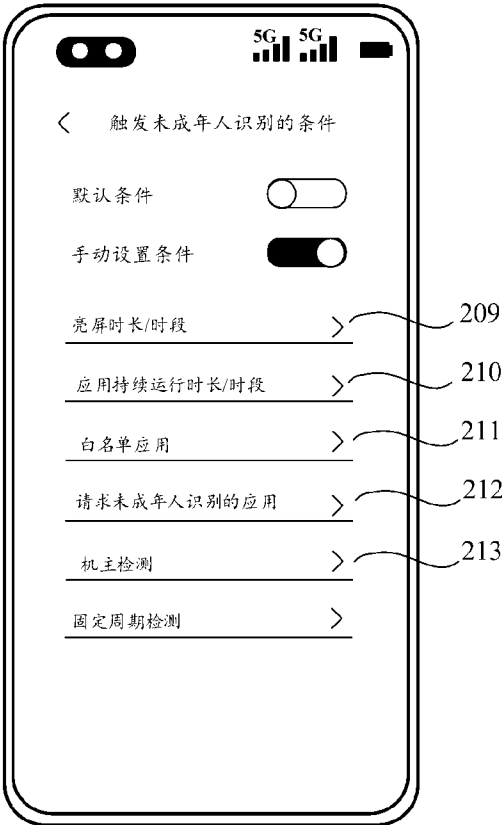


图5B

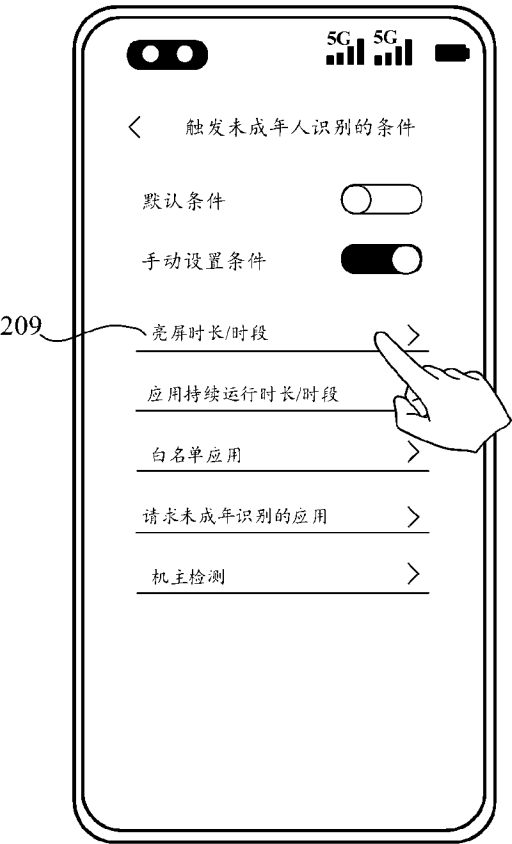


图5C

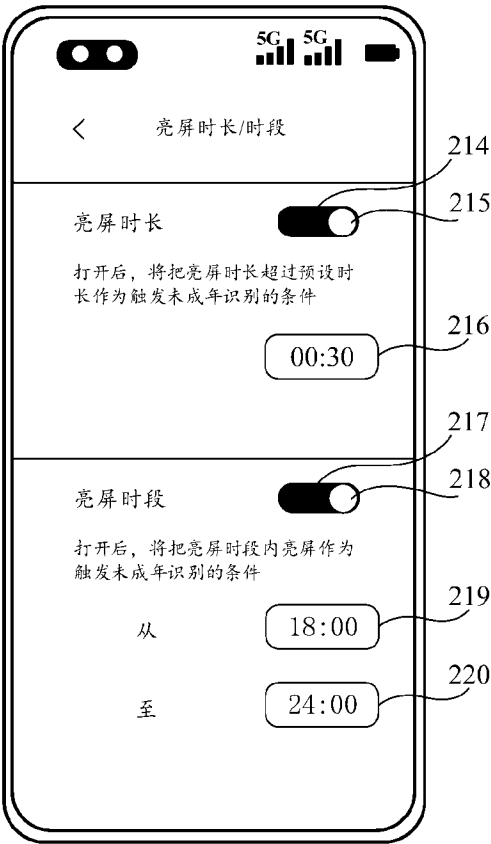


图5D

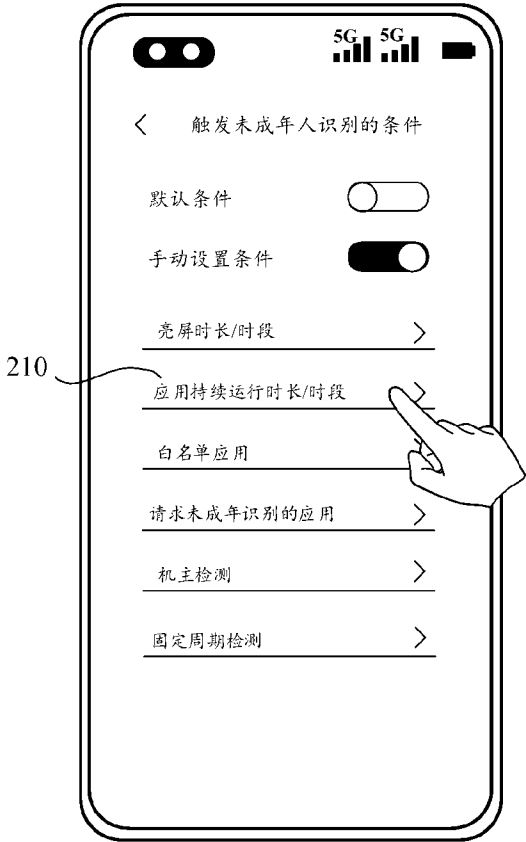


图5E

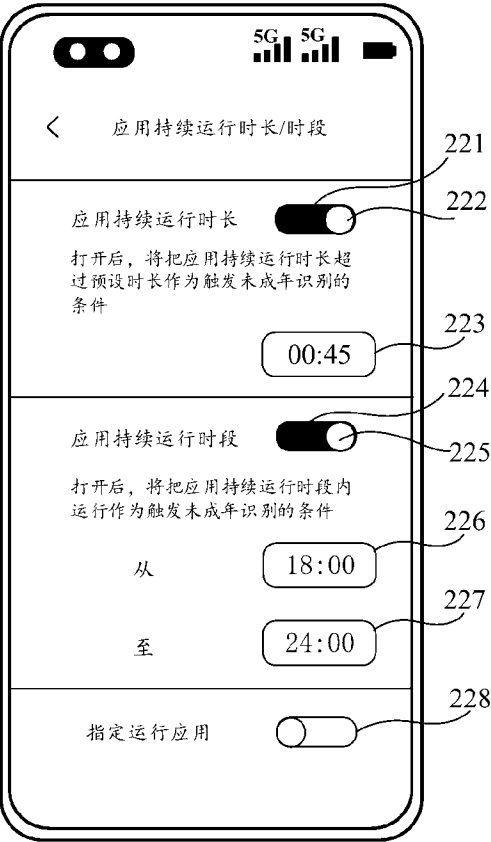


图5F

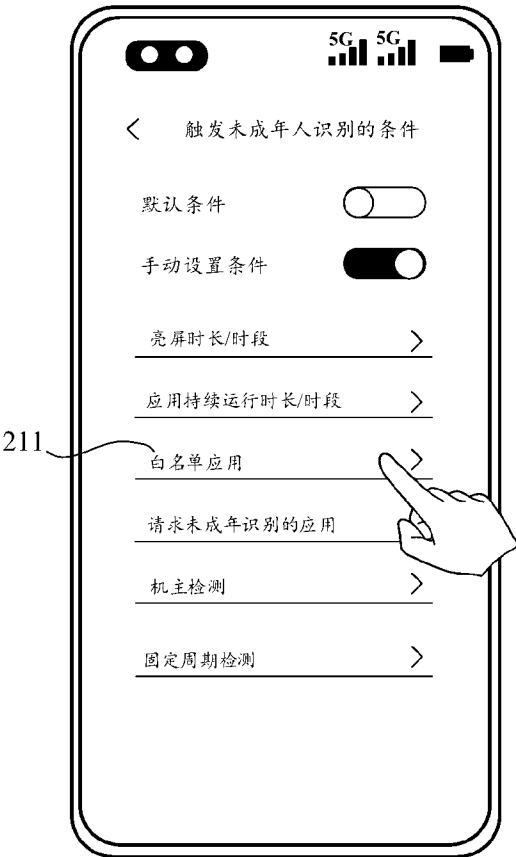


图5G

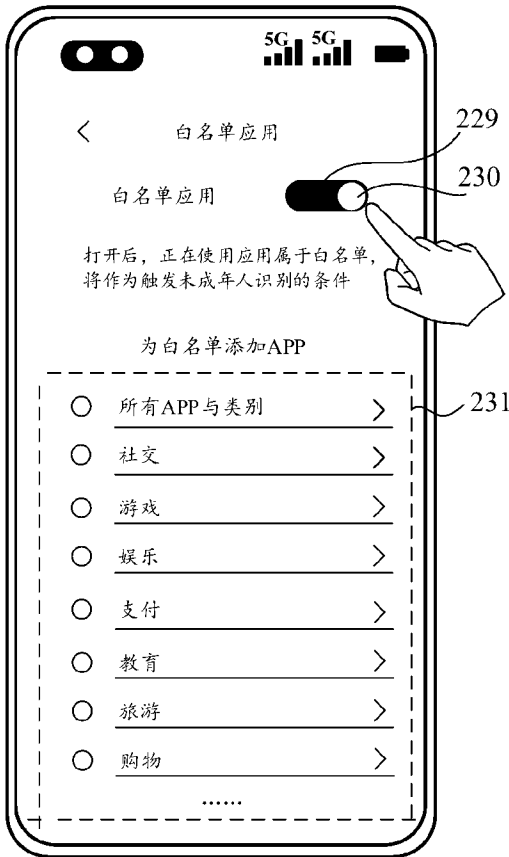


图5H

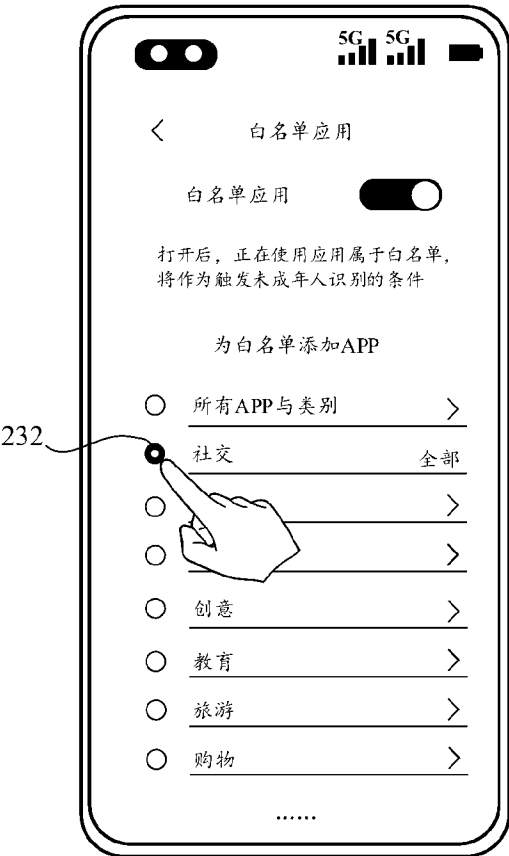


图5I

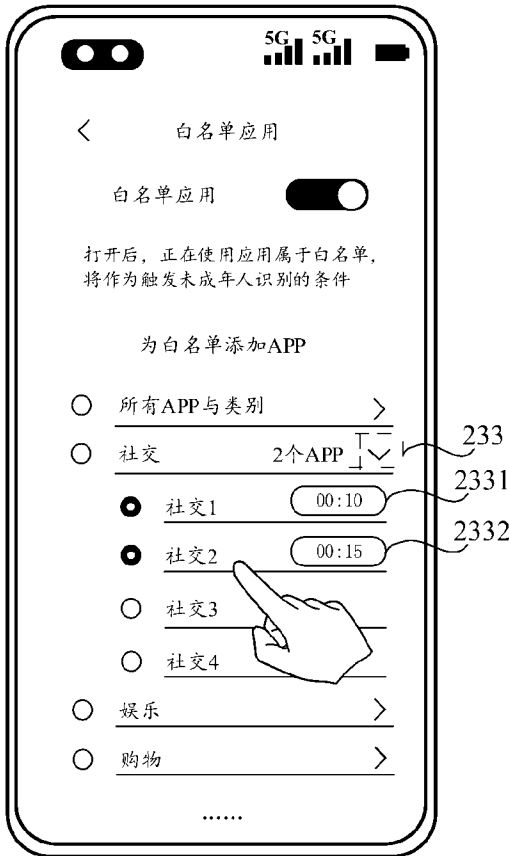


图5J

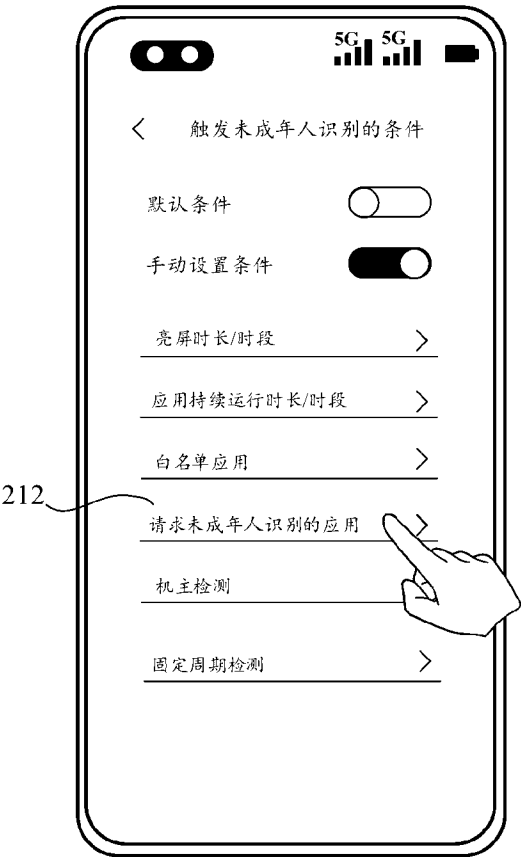


图5K

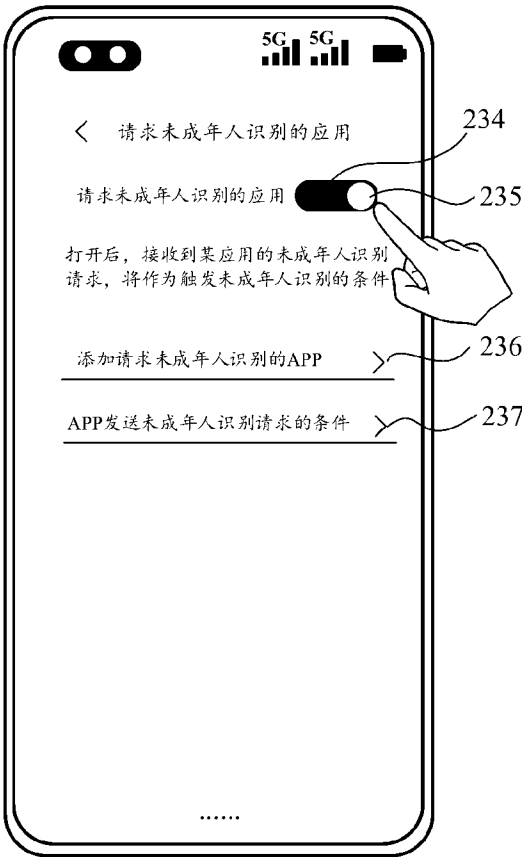


图5L

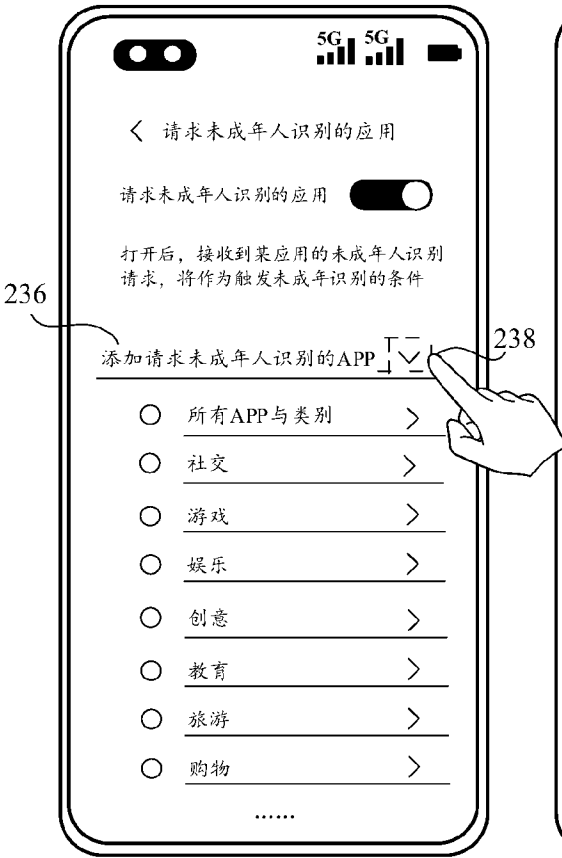


图5M

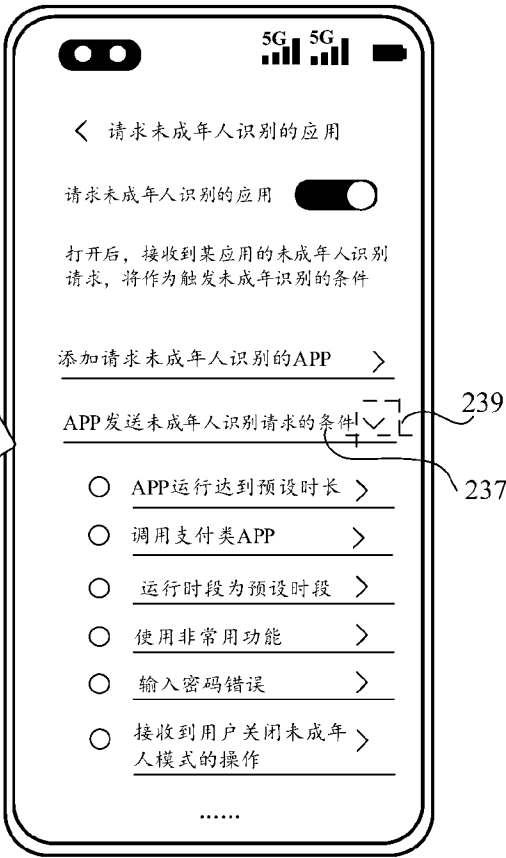


图5N

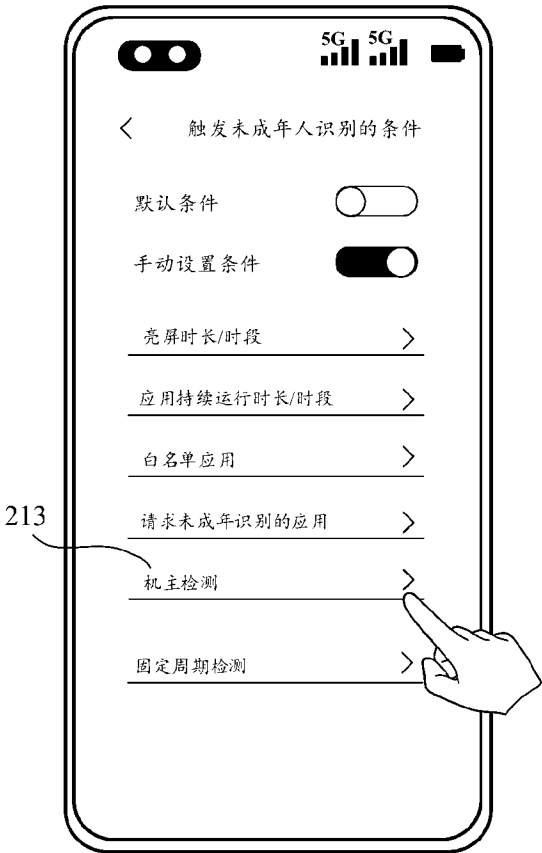


图5O

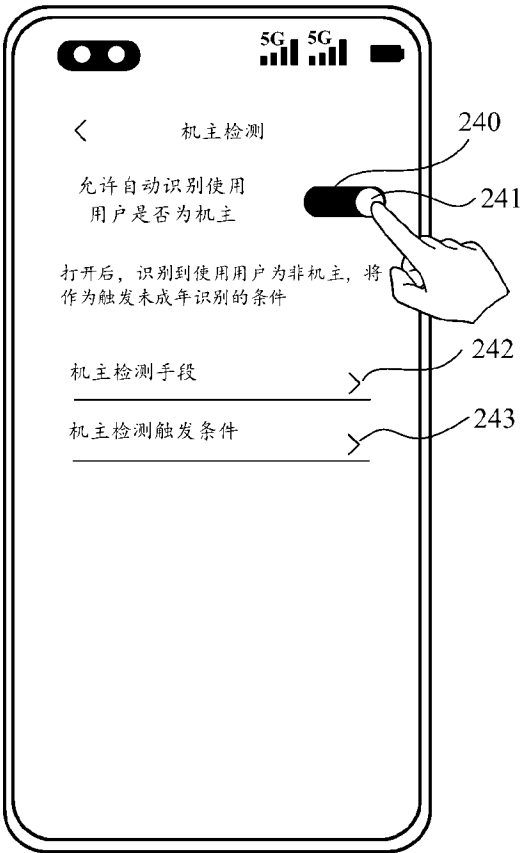


图5P

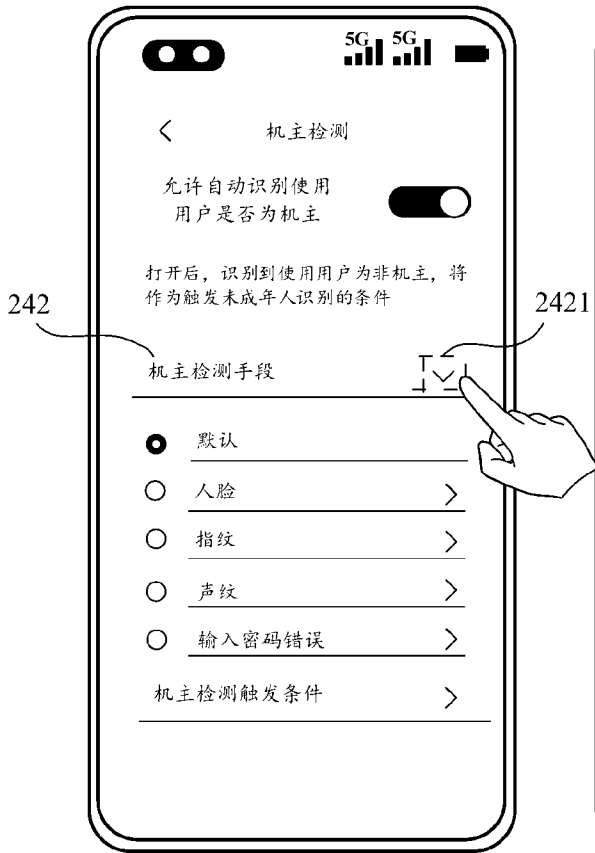


图5Q

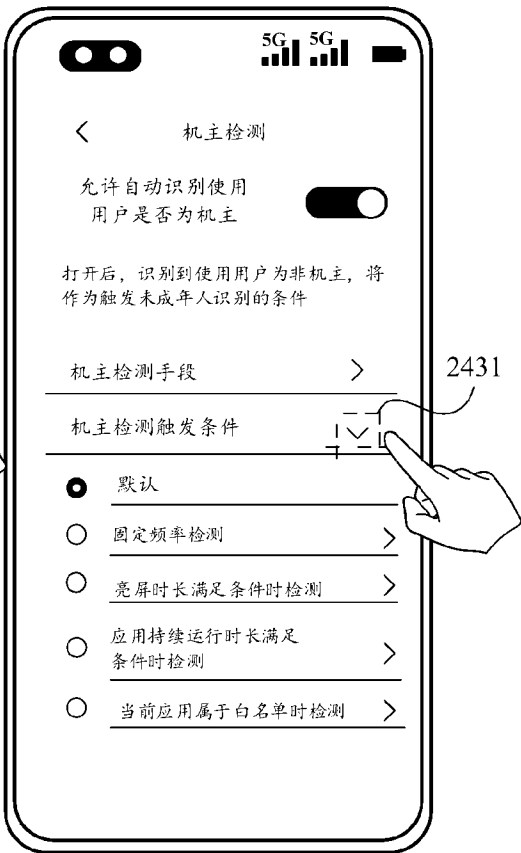


图5R

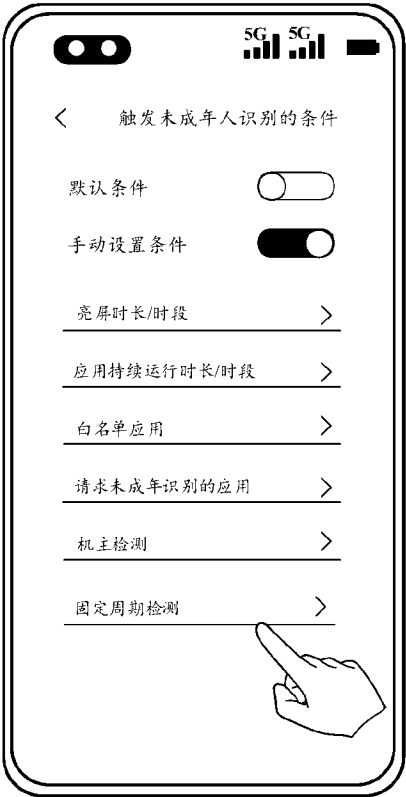


图5S



图5T

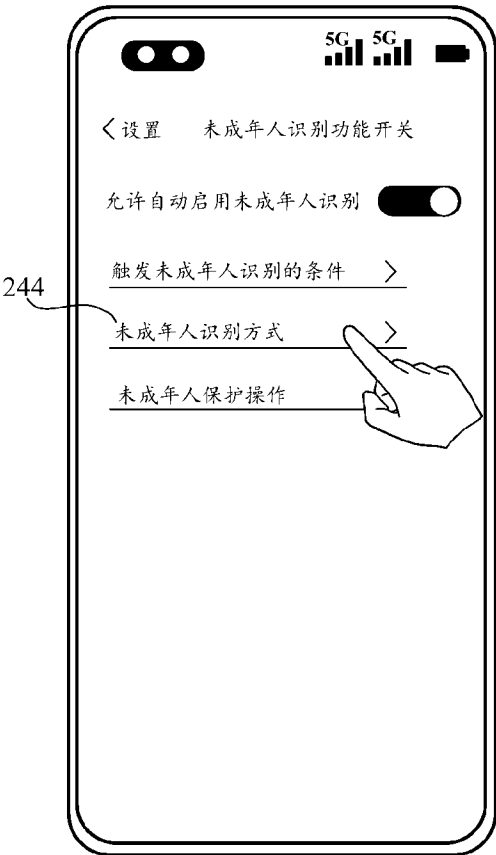


图6A

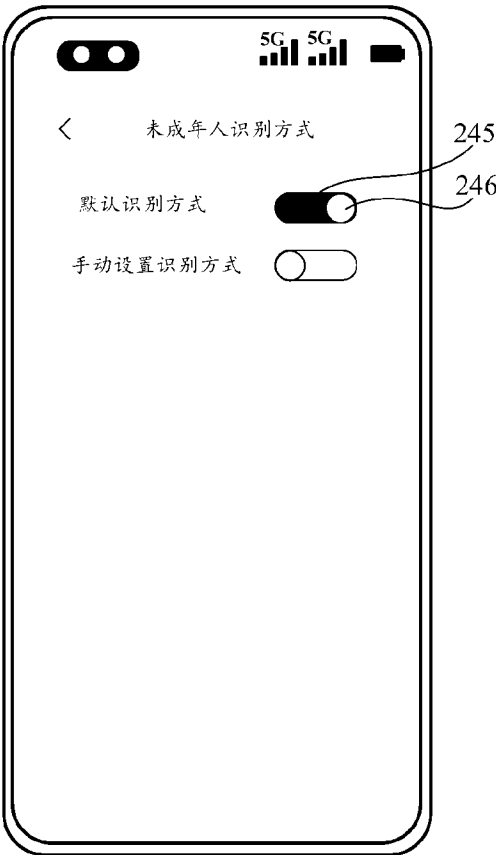


图6B

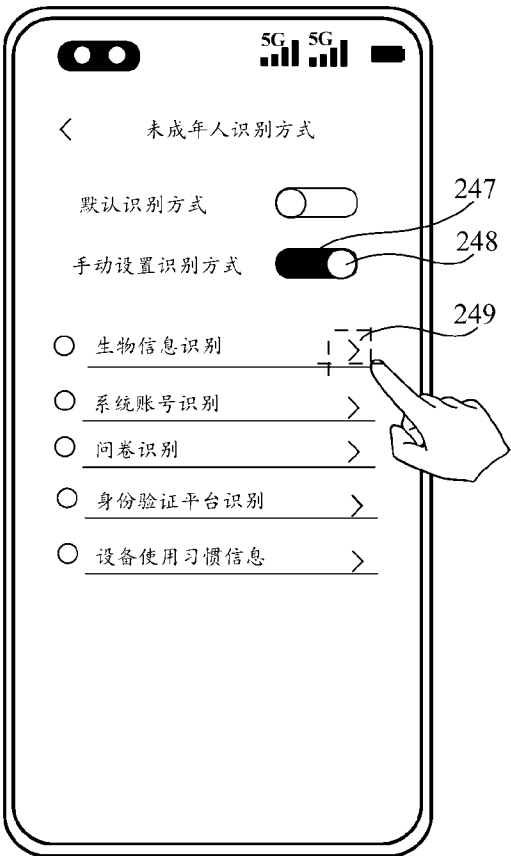


图6C

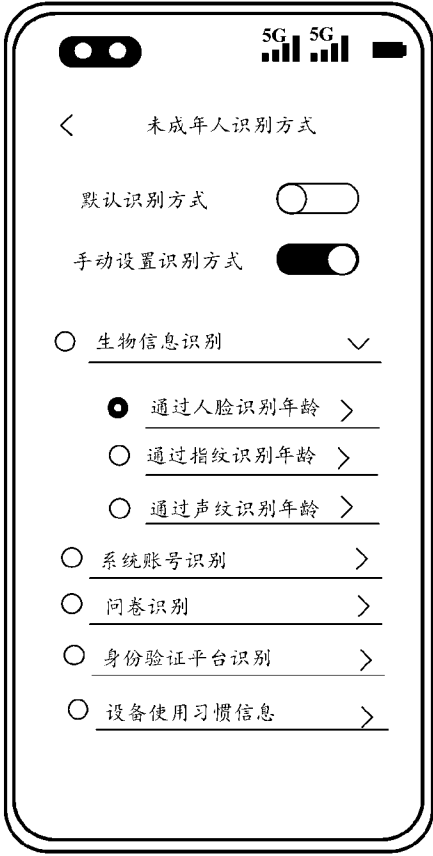


图6D

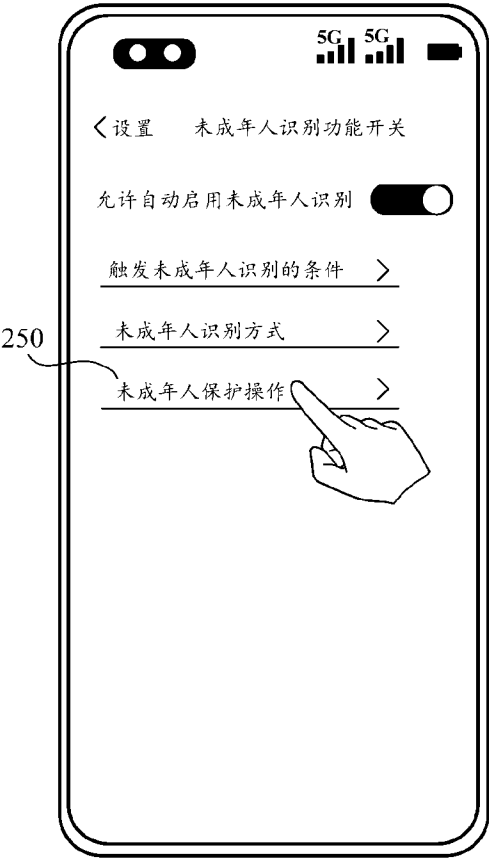


图7A

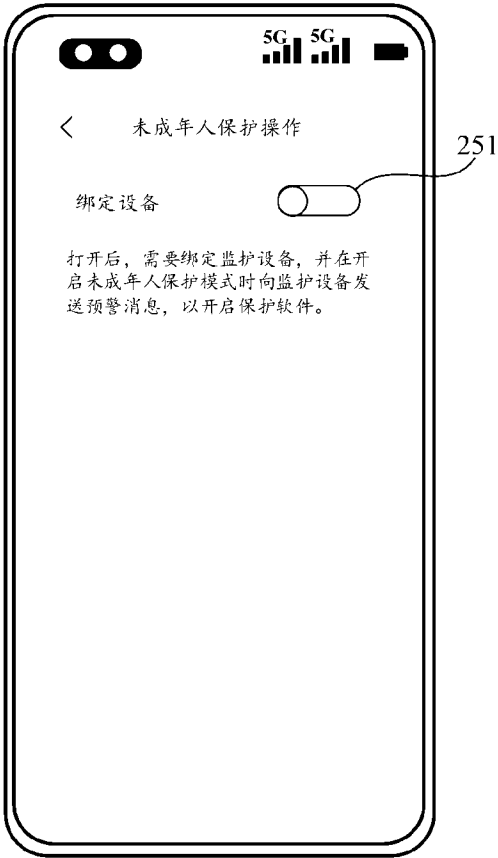


图7B

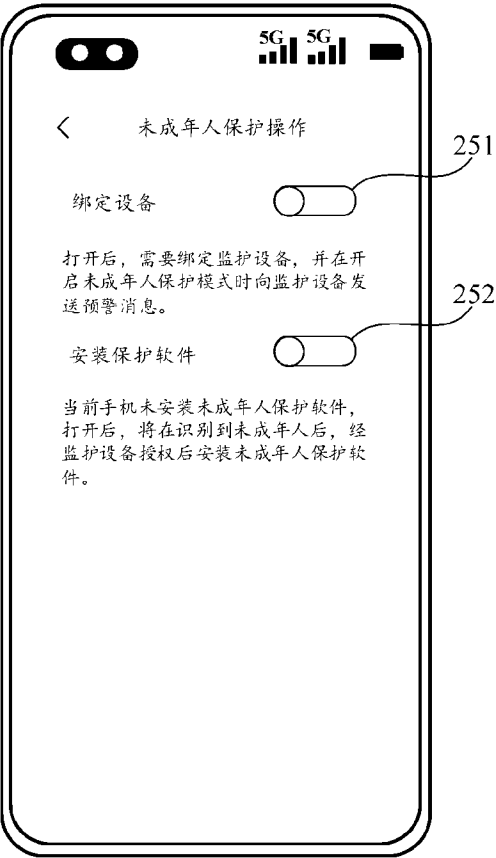


图7C



图7D

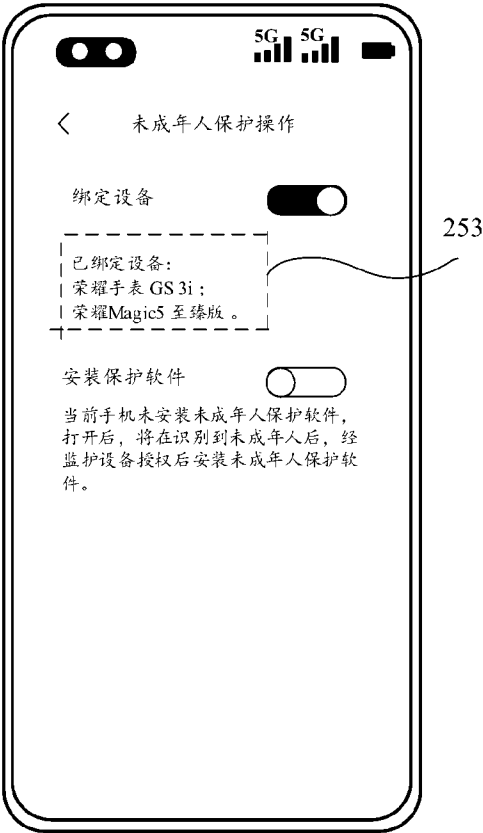


图7E

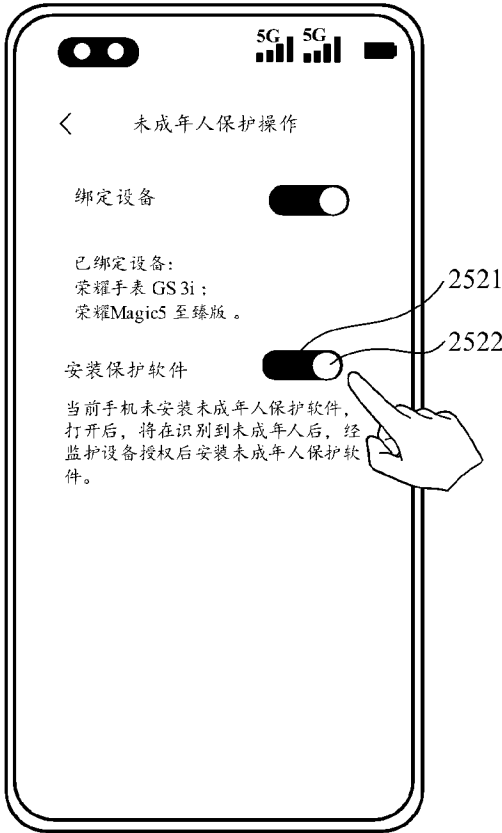


图7F

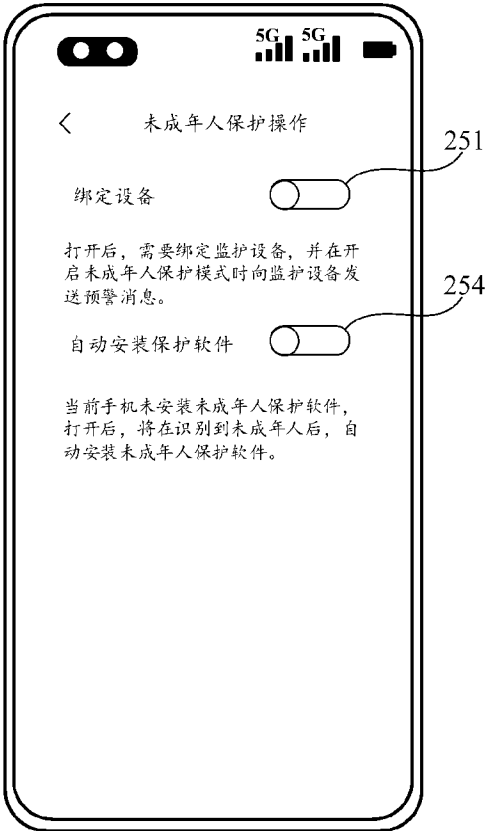


图7G

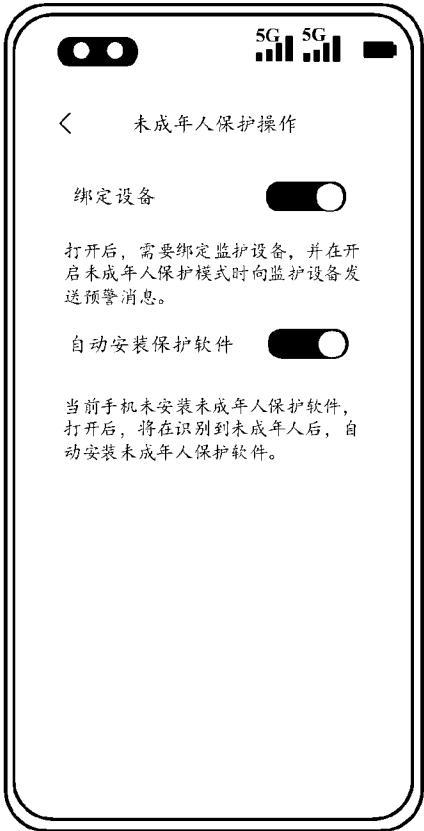


图7H

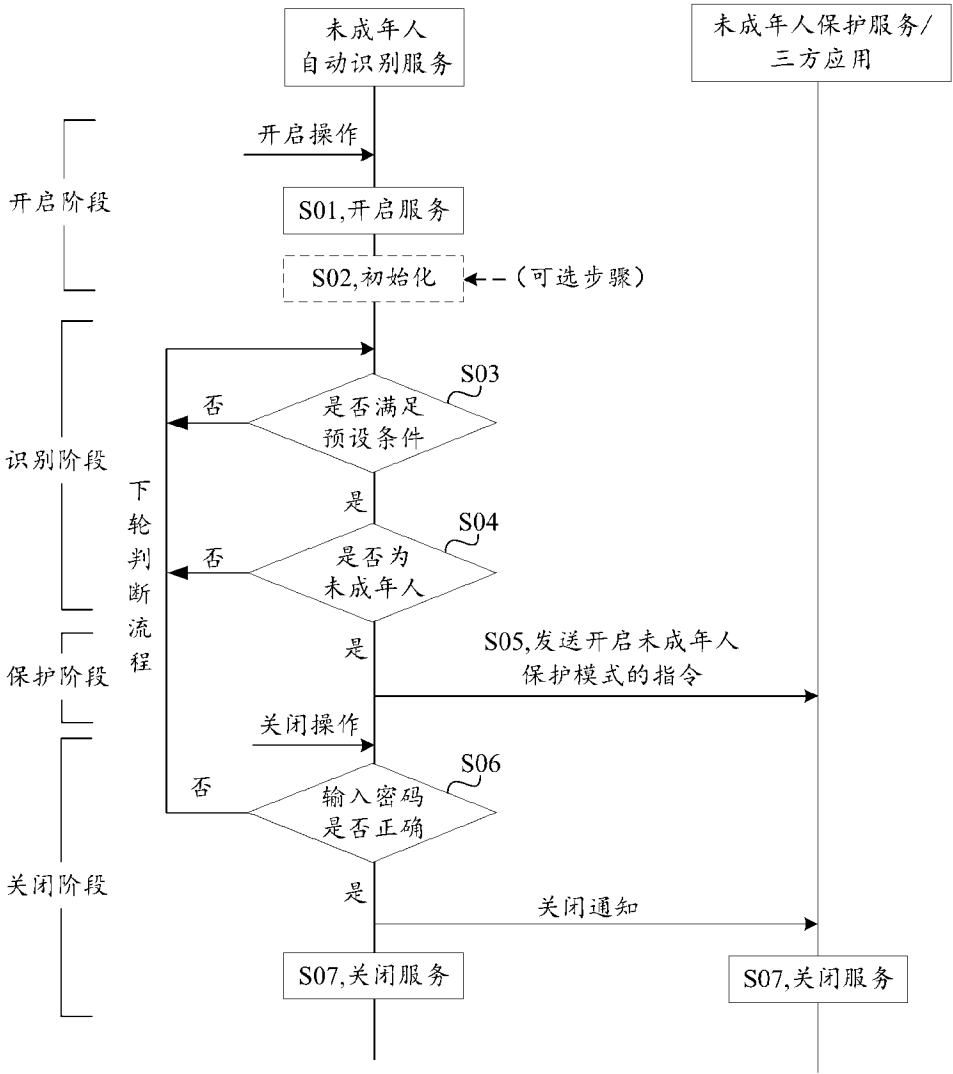


图 8

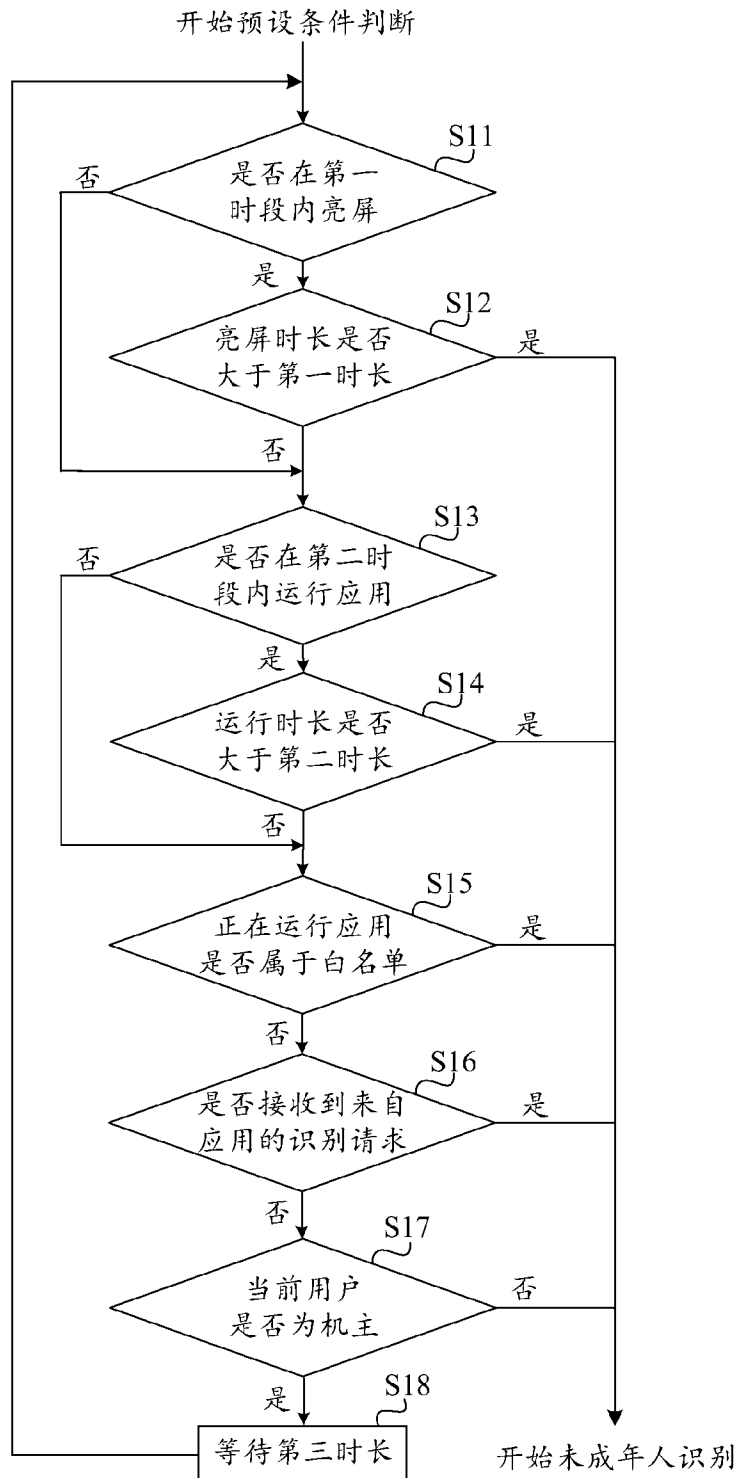


图 9

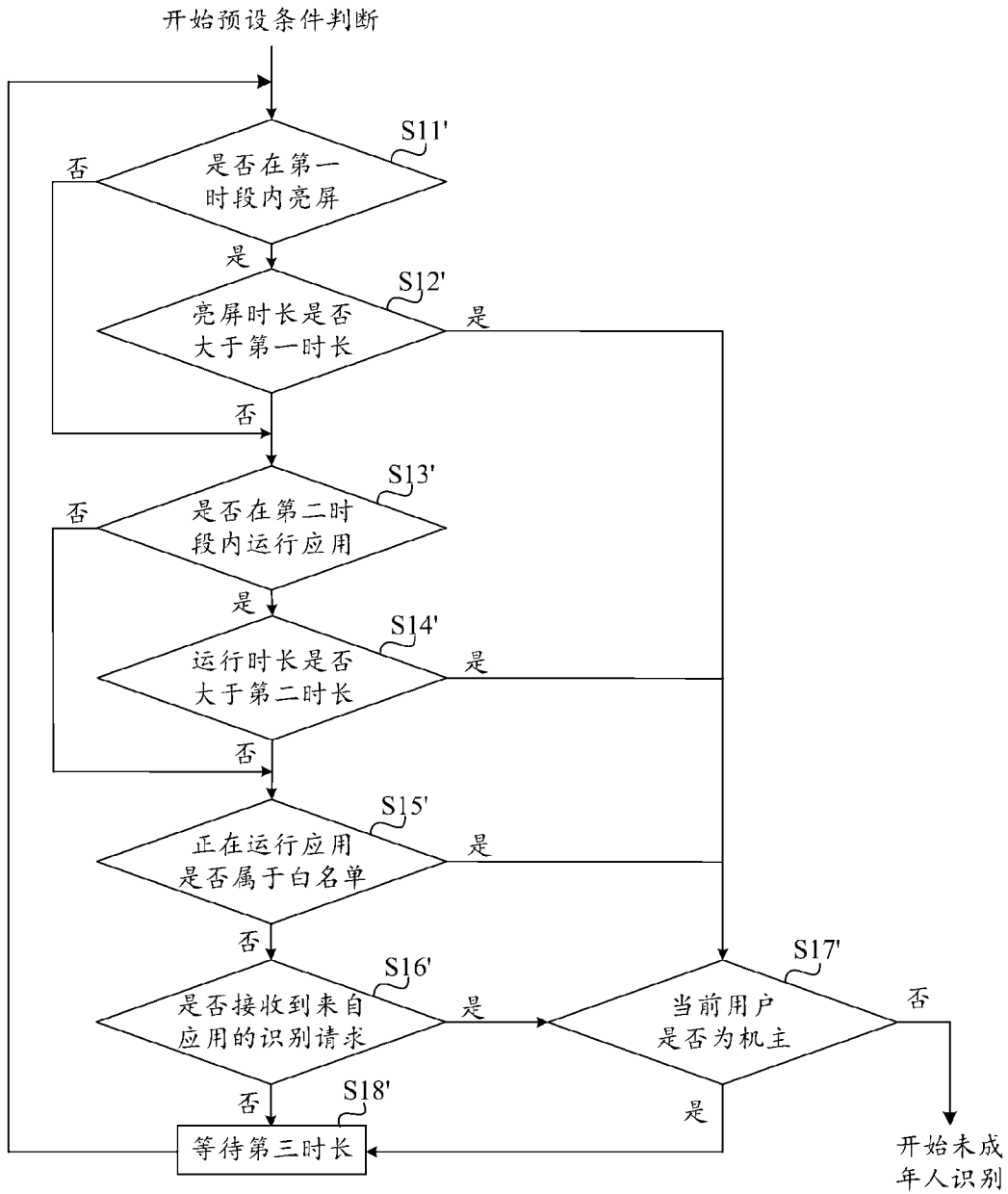


图 10

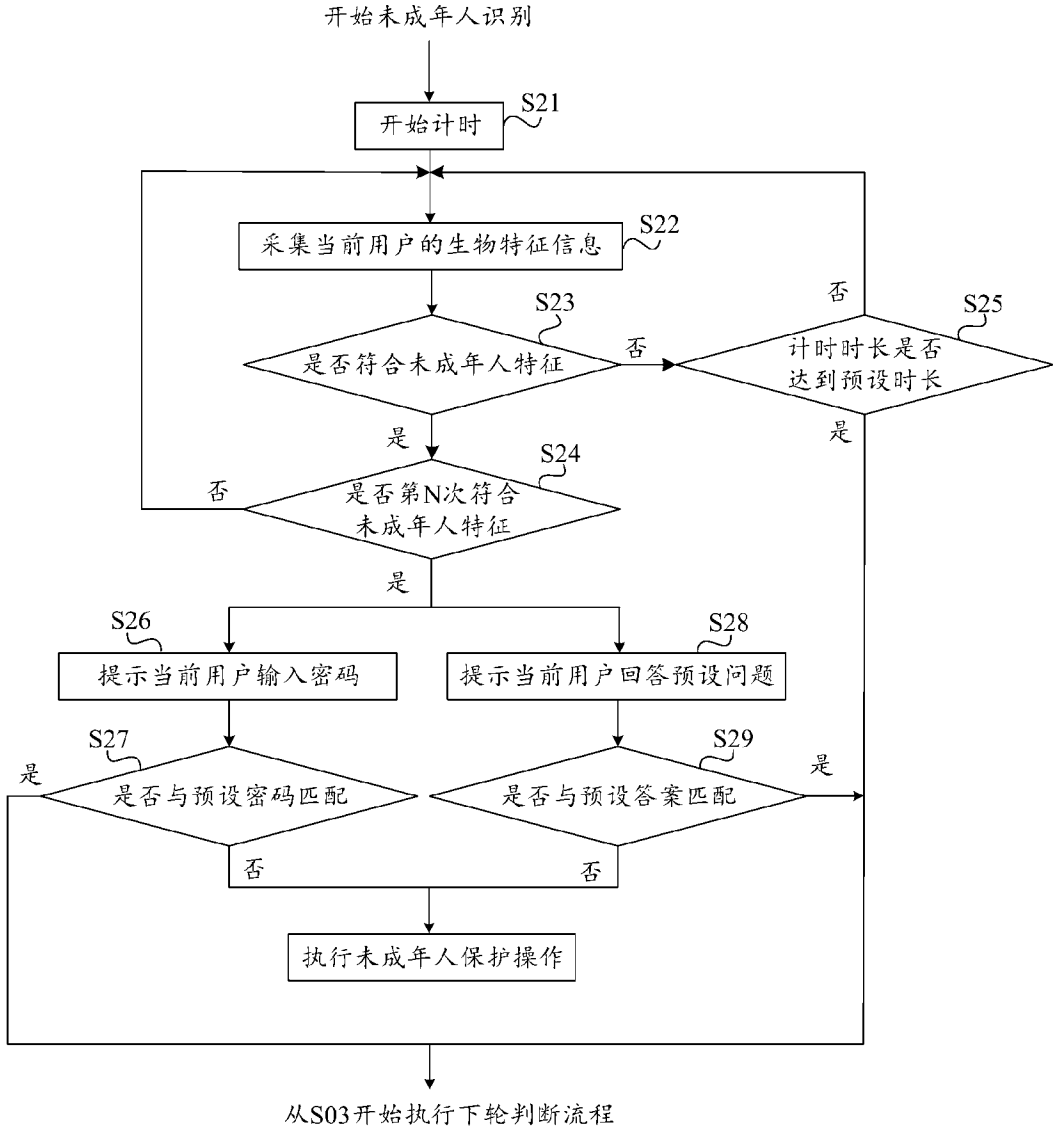


图 11

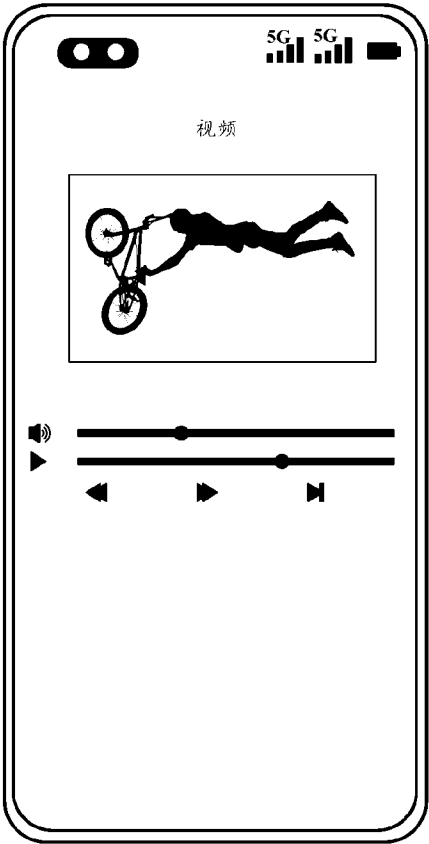


图12A

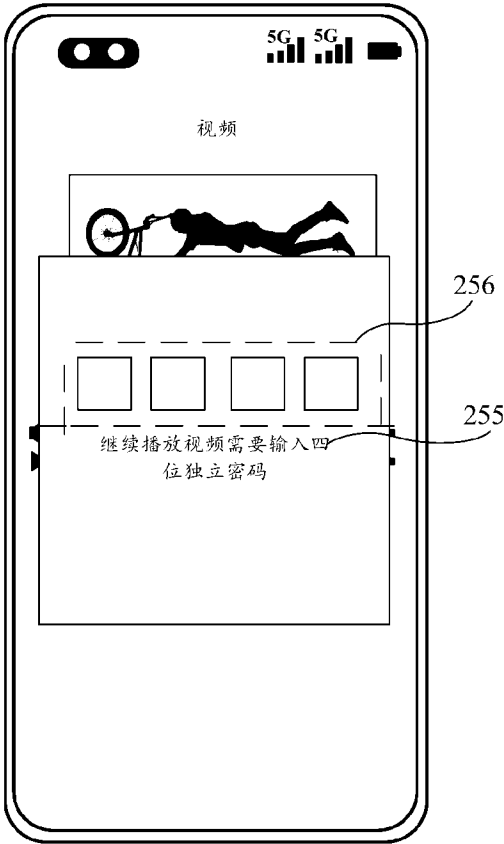


图12B

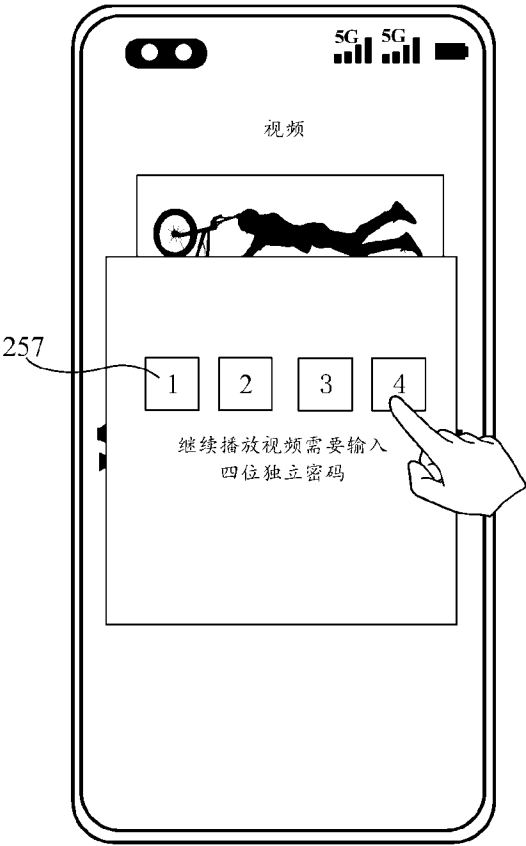


图12C

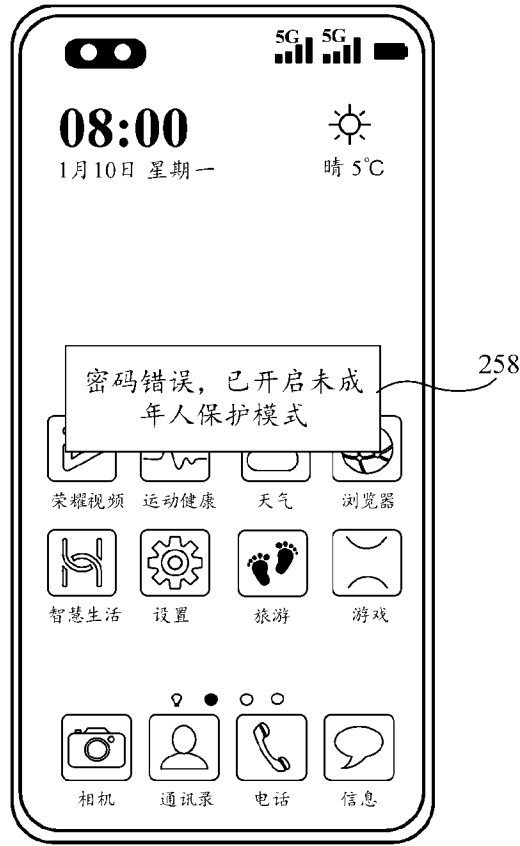


图12D

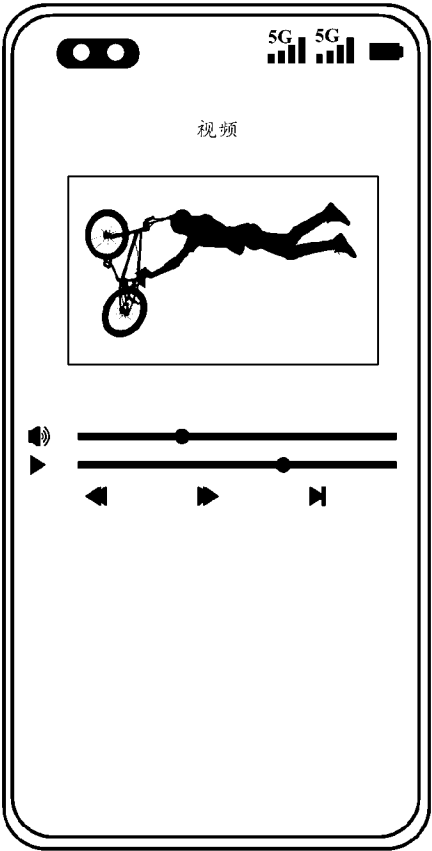


图13A

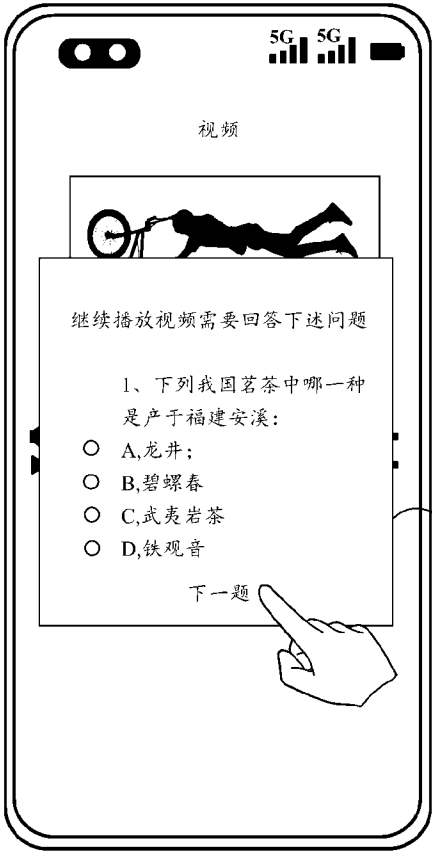


图13B

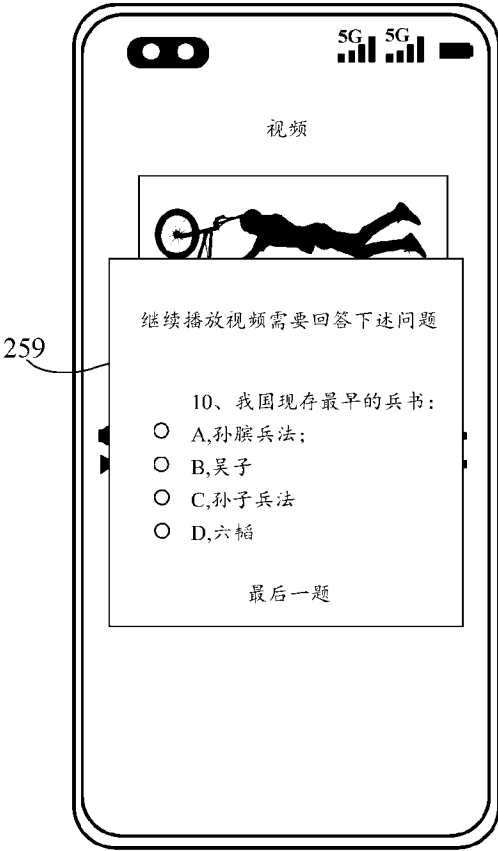


图13C

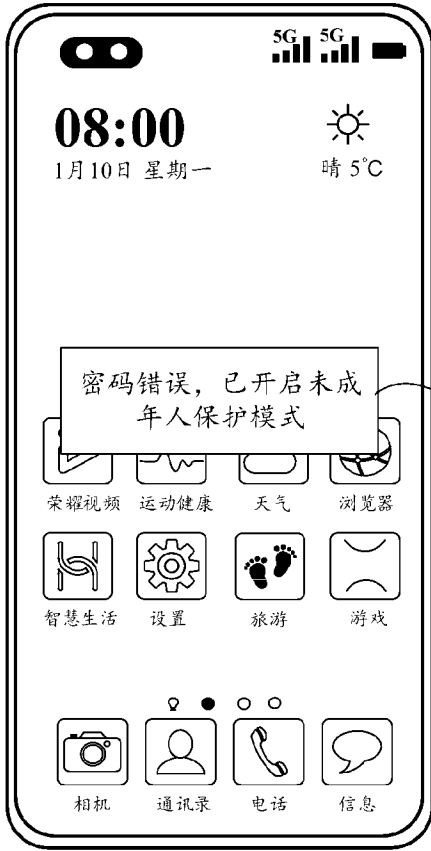
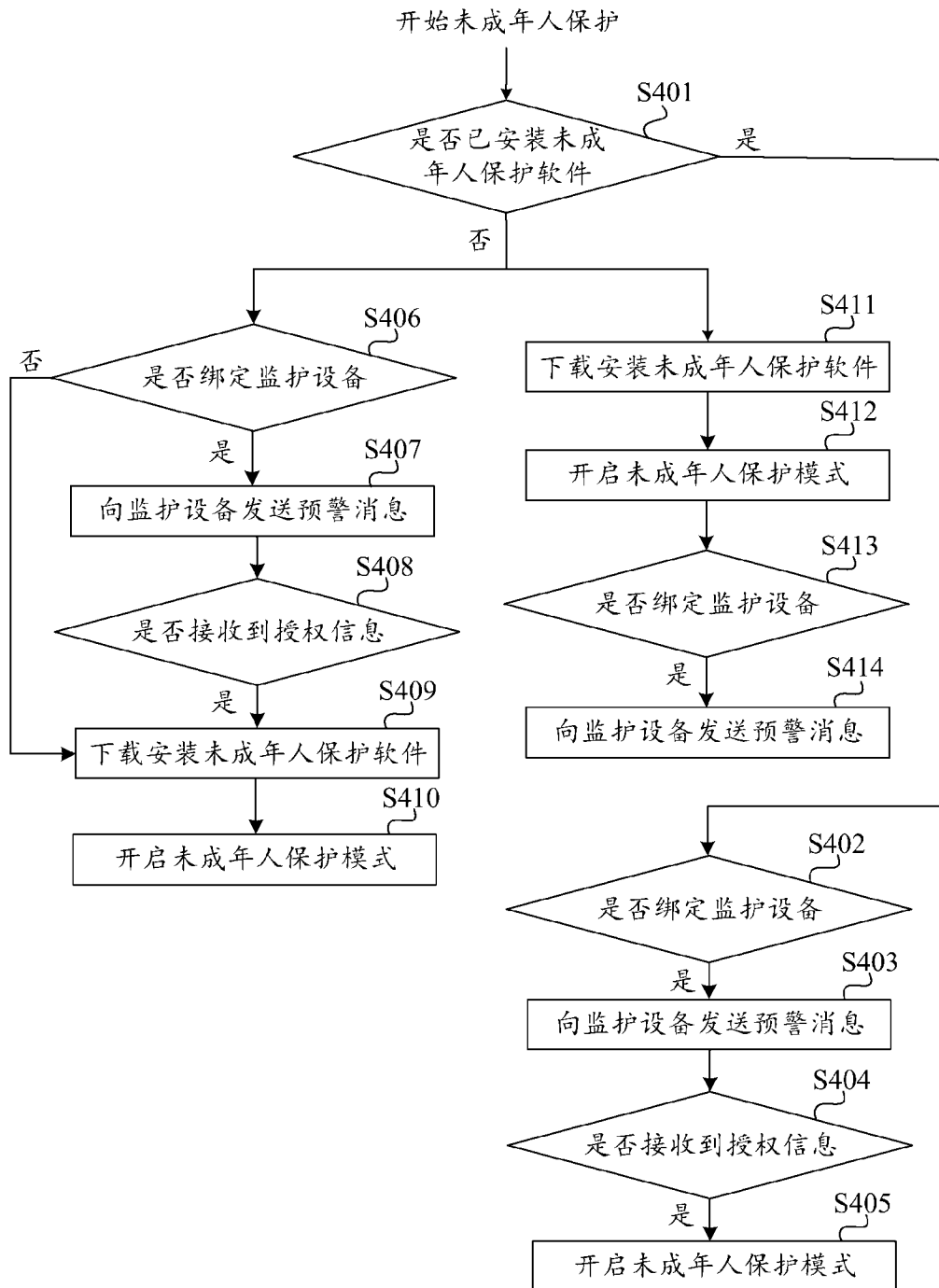


图13D



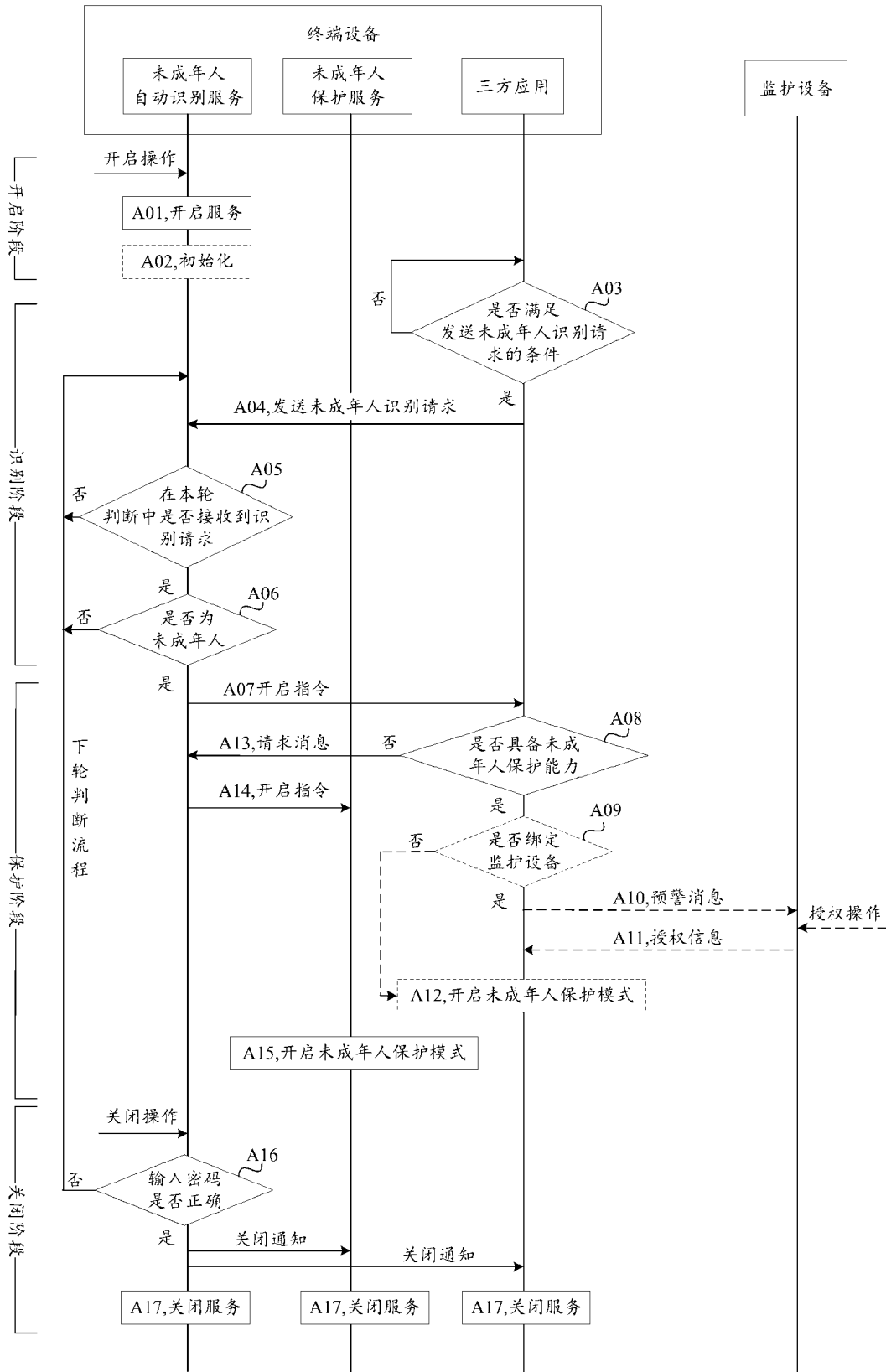


图 15

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/080037

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/445(2018.01)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)

IPC: 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)

VEN, CNABS, CNTXT, WOTXT, EPTXT, CNKI, IEEE, ISI: 未成年, 儿童, 识别, 应用, 时长, 保护, 名单, 触发, 开启, 启动, 条件, 下载, 安装, minor, child, identification, application, duration, time, protection, list, trigger, start, condition, download, install

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 111198724 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) 26 May 2020 (2020-05-26) description, paragraphs [0028]-[0142]	1-14
Y	CN 105224838 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) 06 January 2016 (2016-01-06) description, paragraphs [0029]-[0059]	1-14
A	CN 111935351 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) 13 November 2020 (2020-11-13) entire document	1-14
A	CN 108900719 A (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD.) 27 November 2018 (2018-11-27) entire document	1-14
A	EP 3629278 A1 (INFOCERT S.P.A.) 01 April 2020 (2020-04-01) entire document	1-14



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

“D” document cited by the applicant in the international application

“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

09 May 2024

Date of mailing of the international search report

22 May 2024

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/080037

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111198724	A	26 May 2020	None	
CN	105224838	A	06 January 2016	None	
CN	111935351	A	13 November 2020	None	
CN	108900719	A	27 November 2018	None	
EP	3629278	A1	01 April 2020	None	

国际检索报告		国际申请号 PCT/CN2024/080037
A. 主题的分类 G06F 9/445(2018.01)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) IPC: 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)) VEN, CNABS, CNTXT, WOTXT, EPTXT, CNKI, IEEE, ISI: 未成年, 儿童, 识别, 应用, 时长, 保护, 名单, 触发, 开启, 启动, 条件, 下载, 安装, minor, child, identification, application, duration, time, protection, list, trigger, start, condition, download, install		
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
Y	CN 111198724 A (宇龙计算机通信科技(深圳)有限公司) 2020年5月26日 (2020 - 05 - 26) 说明书第[0028]-[0142]段	1-14
Y	CN 105224838 A (广东欧珀移动通信有限公司) 2016年1月6日 (2016 - 01 - 06) 说明书第[0029]-[0059]段	1-14
A	CN 111935351 A (OPPO广东移动通信有限公司) 2020年11月13日 (2020 - 11 - 13) 全文	1-14
A	CN 108900719 A (惠州TCL移动通信有限公司) 2018年11月27日 (2018 - 11 - 27) 全文	1-14
A	EP 3629278 A1 (INFOCERT S.P.A) 2020年4月1日 (2020 - 04 - 01) 全文	1-14
☐ 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 “D” 申请人在国际申请中引证的文件 “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 2024年5月9日		国际检索报告邮寄日期 2024年5月22日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088		授权官员 周亚楠 电话号码 (+86) 010-53961530

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/080037

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	111198724	A	2020年5月26日	无	
CN	105224838	A	2016年1月6日	无	
CN	111935351	A	2020年11月13日	无	
CN	108900719	A	2018年11月27日	无	
EP	3629278	A1	2020年4月1日	无	