(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112637195 B
(45)授权公告日 2022.11.11

(21)申请号 202011519330.3

(22)申请日 2020.12.21

(65)同一申请的已公布的文献号
申请公布号 CN 112637195 A

(43)申请公布日 2021.04.09

(73)专利权人 维沃移动通信(杭州)有限公司
地址 311100 浙江省杭州市余杭区仓前街道龙泉路20号2幢305室

(72)发明人 刘绪森

(74)专利代理机构 北京远志博慧知识产权代理事务所(特殊普通合伙) 11680
专利代理师 李翠雅

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 110336720 A,2019.10.15
CN 109981747 A,2019.07.05
CN 103118032 A,2013.05.22
CN 109413006 A,2019.03.01
CN 110738499 A,2020.01.31
CN 105306407 A,2016.02.03
CN 102025648 A,2011.04.20
US 2001032232 A1,2001.10.18

审查员 申杨

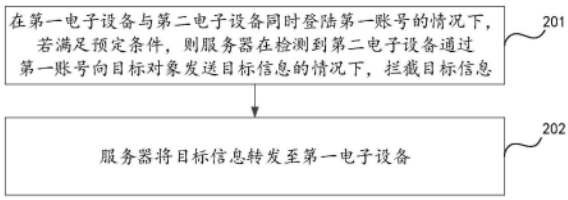
权利要求书2页 说明书11页 附图3页

(54)发明名称

控制电子设备的方法、装置及电子设备

(57)摘要

本申请公开了一种控制电子设备的方法、装置及电子设备，属于通信技术领域，能够解决在多个电子设备中登陆同一账号的场景下，账号安全性低的问题。该方法包括：在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则在检测到第二电子设备通过第一账号向目标对象发送目标信息的情况下，拦截目标信息，并将目标信息转发至第一电子设备；其中，上述满足预定条件包括以下至少一项：检测到登陆第一账号的目标应用处于安全模式，或者，检测到目标用户与第二电子设备间的距离超过预定阈值。



CN 112637195 B

1.一种控制电子设备的方法,应用于服务器,其特征在于,该方法包括:

在第一电子设备与第二电子设备同时登陆第一账号的情况下,若满足预定条件,则在检测到所述第二电子设备通过所述第一账号向目标对象发送目标信息的情况下,拦截所述目标信息,并将所述目标信息转发至所述第一电子设备;

其中,所述满足预定条件包括以下至少一项:检测到登陆所述第一账号的目标应用处于安全模式,或者,检测到目标用户与所述第二电子设备间的距离超过预定阈值。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在接收到所述目标对象对应的第二账号向所述第一账号发送第一信息的情况下,对所述第一信息进行加密处理以得到第二信息;

将所述第二信息发送至所述第二电子设备中的所述第一账号。

3.根据权利要求2所述的方法,其特征在于,所述将所述第二信息发送至所述第二电子设备中的所述第一账号之后,所述方法还包括:

将所述第一信息发送至所述第一电子设备的所述第一账号。

4.一种控制电子设备的方法,应用于第一电子设备,其特征在于,该方法包括:

在所述第一电子设备与第二电子设备同时登陆第一账号的情况下,若满足预定条件,接收服务器向所述第一电子设备发送的目标信息;

其中,所述目标信息为:所述第二电子设备通过所述第一账号向目标对象发送的信息;

其中,所述满足预定条件包括以下至少一项:检测到登陆所述第一账号的目标应用处于安全模式,或者,检测到目标用户与所述第二电子设备间的距离超过预定阈值。

5.根据权利要求4所述的方法,其特征在于,所述接收服务器向所述第一电子设备发送的目标信息之后,所述方法还包括:

接收用户的第一输入;

响应于所述第一输入,控制所述第二电子设备开启摄像头进行图像采集。

6.根据权利要求4所述的方法,其特征在于,所述接收服务器向所述第一电子设备发送的目标信息之后,所述方法还包括:

接收用户的第二输入;

响应于所述第二输入,向所述服务器发送第一指令,所述第一指令用于指示所述服务器将所述目标信息发送至第二账号。

7.一种控制电子设备的装置,其特征在于,该装置包括:

处理模块,用于在第一电子设备与第二电子设备同时登陆第一账号的情况下,若满足预定条件,则在检测到所述第二电子设备通过所述第一账号向目标对象发送目标信息的情况下,拦截所述目标信息;

发送模块,用于将所述处理模块拦截的所述目标信息转发至所述第一电子设备;

其中,所述满足预定条件包括以下至少一项:检测到登陆所述第一账号的目标应用处于安全模式,或者,检测到目标用户与所述第二电子设备间的距离超过预定阈值。

8.根据权利要求7所述的装置,其特征在于,所述处理模块,还用于在接收到第二账号向所述第一账号发送第一信息的情况下,对所述第一信息进行加密处理以得到第二信息;

所述发送模块,还用于将所述处理模块得到的所述第二信息发送至所述第二电子设备中的所述第一账号。

9.根据权利要求8所述的装置,其特征在于,所述发送模块,还用于将所述第一信息发送至所述第一电子设备的所述第一账号。

10.一种控制电子设备的装置,其特征在于,该装置包括:

接收模块,用于在第一电子设备与第二电子设备同时登陆第一账号的情况下,若满足预定条件,接收服务器向所述第一电子设备发送的目标信息;

其中,所述目标信息为:所述第二电子设备通过所述第一账号向目标对象发送的信息;

其中,所述满足预定条件包括以下至少一项:检测到登陆所述第一账号的目标应用处于安全模式,或者,检测到目标用户与所述第二电子设备间的距离超过预定阈值。

11.根据权利要求10所述的装置,其特征在于,所述装置,还包括:处理模块,其中:

所述接收模块,还用于接收用户的第一输入;

所述处理模块,还用于响应于所述接收模块接收到的所述第一输入,控制所述第二电子设备开启摄像头进行图像采集。

12.根据权利要求10所述的装置,其特征在于,所述装置还包括:发送模块,其中:

所述接收模块,还用于接收用户的第二输入;

所述发送模块,还用于响应于所述接收模块接收到的所述第二输入,向所述服务器发送第一指令,所述第一指令用于指示所述服务器将所述目标信息发送至第二账号。

13.一种电子设备,其特征在于,包括处理器,存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令,所述程序或指令被所述处理器执行时实现如权利要求1至3任一项或者权利要求4至6所述的控制电子设备的方法的步骤。

控制电子设备的方法、装置及电子设备

技术领域

[0001] 本申请属于通信技术领域，具体涉及一种控制电子设备的方法、装置及电子设备。

背景技术

[0002] 随着移动互联网的发展，人们可以通过同时在多个电子设备(如，智能手机或电脑)中登陆同一账号来实现电子设备间的通讯。

[0003] 在现有技术中，当用户在多个电子设备中登陆同一账号a后，若账号a接收到联系人1发送的信息，则该信息会被同步至上述多个电子设备中。

[0004] 如此，在多个电子设备中登陆同一账号的场景下，由于该多个电子设备均会同步显示该账号所接收到的信息，则会导致账号被冒用或导致信息泄露，安全性低。

发明内容

[0005] 本申请实施例的目的是提供一种控制电子设备的方法、装置及电子设备，能够解决在多个电子设备中登陆同一账号的场景下，账号安全性低的问题。

[0006] 为了解决上述技术问题，本申请是这样实现的：

[0007] 第一方面，本申请实施例提供了一种控制电子设备的方法，应用于服务器，该方法包括：在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则在检测到上述第二电子设备通过上述第一账号向目标对象发送目标信息的情况下，拦截上述目标信息，并将上述目标信息转发至上述第一电子设备；其中，上述满足预定条件包括以下至少一项：检测到登陆上述第一账号的目标应用处于安全模式，或者，检测到目标用户与上述第二电子设备间的距离超过预定阈值。

[0008] 第二方面，本申请实施例提供了一种控制电子设备的方法，应用于第一电子设备，该方法包括：在上述第一电子设备与第二电子设备同时登陆第一账号的情况下，接收服务器向上述第一电子设备发送的目标信息；其中，上述目标信息为：上述第二电子设备通过上述第一账号向第二账号发送的信息。

[0009] 第三方面，本申请实施例提供了一种控制电子设备的装置，该装置包括：处理模块，用于在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则在检测到上述第二电子设备通过上述第一账号向目标对象发送目标信息的情况下，拦截上述目标信息；发送模块，用于将上述处理模块拦截的上述目标信息转发至上述第一电子设备；其中，上述满足预定条件包括以下至少一项：检测到登陆上述第一账号的目标应用处于安全模式，或者，检测到目标用户与上述第二电子设备间的距离超过预定阈值。

[0010] 第四方面，本申请实施例提供了一种控制电子设备的装置，该装置包括：接收模块，用于在上述第一电子设备与第二电子设备同时登陆第一账号的情况下，接收服务器向上述第一电子设备发送的目标信息；其中，上述目标信息为：上述第二电子设备通过上述第一账号向第二账号发送的信息。

[0011] 第五方面，本申请实施例提供了一种服务器，该电子设备包括处理器、存储器及存

储在所述存储器上并可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第一方面所述的方法的步骤。

[0012] 第六方面，本申请实施例提供了一种电子设备，该电子设备包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第二方面所述的方法的步骤。

[0013] 第七方面，本申请实施例提供了一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如第一方面或第二方面所述的方法的步骤。

[0014] 第八方面，本申请实施例提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如第一方面或第二方面所述的方法。

[0015] 第九方面，本申请实施例提供了一种计算机程序产品，该程序产品被存储在非易失的存储介质中，该程序产品被至少一个处理器执行以实现如第一方面或第二方面所述的方法。

[0016] 在本申请实施例中，在第一电子设备与第二电子设备同时登陆第一账号的情况下，在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件(即检测到登陆上述第一账号的目标应用处于安全模式，和/或，检测到目标用户与上述第二电子设备间的距离超过预定阈值)，则服务器可以在检测到第二电子设备通过该第一账号向目标对象发送目标信息的情况下，则确认当前的第二电子设备中登陆的第一账号存在安全隐患，从而拦截目标信息，并停止目标信息的传输。同时，为了提醒使用第一电子设备的用户当前的第二电子设备中登陆的第一账号存在安全隐患，服务器会将原本需要发送给第二账号的目标信息转发至第一电子设备，从而避免了账号被不法分子冒用，提高了信息的安全性。

附图说明

[0017] 图1是本申请实施例提供的控制电子设备的方法应用的一种通信系统架构图；

[0018] 图2是本申请实施例提供的一种控制电子设备的方法的方法流程图之一；

[0019] 图3是本申请实施例提供的一种控制电子设备的方法的方法流程图之二；

[0020] 图4是本申请实施例提供的一种控制电子设备的装置的结构示意图之一；

[0021] 图5是本申请实施例提供的一种控制电子设备的装置的结构示意图之二；

[0022] 图6是本申请实施例提供的一种控制电子设备的装置的结构示意图之三；

[0023] 图7是本申请实施例提供的一种控制电子设备的装置的结构示意图之四；

[0024] 图8是本申请实施例提供的一种电子设备的结构示意图；

[0025] 图9是本申请实施例提供的一种电子设备的硬件示意图。

具体实施方式

[0026] 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。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施

例,都属于本申请保护的范围。

[0027] 本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象,而不用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外,说明书以及权利要求中“和/或”表示所连接对象的至少其中之一,字符“/”,一般表示前后关联对象是一种“或”的关系。

[0028] 下面结合附图,通过具体的实施例及其应用场景对本申请实施例提供的控制电子设备的方法进行详细地说明。

[0029] 本申请实施例提供的控制电子设备的方法可以应用于通信系统,如图1所示,该通信系统包括:服务器11、第一电子设备12及第二电子设备13,其中:

[0030] 在第一电子设备12与第二电子设备13同时登陆第一账号的情况下,若满足预定条件,则在检测到第二电子设备13通过第一账号向目标对象发送目标信息的情况下,服务器11拦截上述目标信息,并将上述目标信息转发至上述第一电子设备12。相应的,在第一电子设备12与第二电子设备13同时登陆第一账号的情况下,接收服务器11向第一电子设备12发送的目标信息。

[0031] 其中,上述满足预定条件包括以下至少一项:检测到登陆该第一账号的目标应用处于安全模式,或者,检测到目标用户与第二电子设备间的距离超过预定阈值。

[0032] 需要说明的是,上述服务器11可以是一台服务器,也可以是由多台服务器组成的服务器集群,或者是一个云计算服务中心。

[0033] 在本申请实施例中,在第一电子设备与第二电子设备同时登陆第一账号的情况下,在第一电子设备与第二电子设备同时登陆第一账号的情况下,若满足预定条件(即检测到登陆上述第一账号的目标应用处于安全模式,和/或,检测到目标用户与上述第二电子设备间的距离超过预定阈值),则服务器可以在检测到第二电子设备通过该第一账号向目标对象发送目标信息的情况下,则确认当前的第二电子设备中登陆的第一账号存在安全隐患,从而拦截目标信息,并停止目标信息的传输。同时,为了提醒使用第一电子设备的用户当前的第二电子设备中登陆的第一账号存在安全隐患,因此,服务器会将原本需要发送给第二账号的目标信息转发至第一电子设备,从而避免了账号被不法分子冒用,提高了信息的安全性。

[0034] 可选地,在本申请实施例中,服务器11在检测到第二电子设备13通过上述第一账号向目标对象发送目标信息的情况下,拦截目标信息的过程包括:在接收到第二电子设备13通过该第一账号向目标对象发送目标信息的情况下,拦截目标信息;或者,在接收到第二电子设备13通过改第一账号在与目标对象的对话框中输入信息的情况下,拦截目标信息。

[0035] 可选地,在本申请实施例中,服务器11在检测到第二电子设备13通过上述第一账号向目标对象发送目标信息的情况下,会向上述第一电子设备12发送目标提示信息,其中,上述目标提示信息用于提示用户,上述第二电子设备13通过上述第一账号发送上述目标信息。而第一电子设备12在接收到目标提示信息后,便可基于该提示获知该目标信息的来源。

[0036] 如此,当其他用户使用第二电子设备中的第一账号向其他电子设备发送信息时,服务器在接收到该信息后,会向第一电子设备发送提示信息,以提示用户当前有其他用户使用第一账号,提高了信息的安全性,避免账号被冒用或导致信息泄露。

[0037] 可选地，在本申请实施例中，服务器11在接收到第二账号向第一账号发送第一信息的情况下，对第一信息进行加密处理以得到第二信息，然后，将上述第二信息发送至第二电子设备13中的第一账号。进一步的，服务器在将上述第二信息发送至第二电子设备13中的第一账号之后，还可以将上述第一信息发送至第一电子设备的第一账号。

[0038] 如此，在第二账号向第一账号发送第一信息时，服务器将对第一信息进行加密，提高了信息传输的安全性，避免了隐私信息的泄露。

[0039] 可选地，在本申请实施例中，第一电子设备12在接收到服务器发送的目标信息之后，接收用户的第一输入，响应于该第一输入，控制第二电子设备开启摄像头进行图像采集。或者，接收到用户的第二输入，响应于第二输入，向服务器11发送第一指令，上述第一指令用于指示服务器11将上述目标信息发送至第二账号，即取消拦截操作，继续将上述目标信息发送至第二账号。

[0040] 如此，便可通过第一电子设备实现对登陆同一账号的其他电子设备的控制。

[0041] 本申请实施例提供一种控制电子设备的方法，如图2所示，该控制电子设备的方法可以包括如下步骤：

[0042] 步骤201：在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则服务器在检测到第二电子设备通过第一账号向目标对象发送目标信息的情况下，拦截目标信息。

[0043] 步骤202：服务器将目标信息转发至第一电子设备。

[0044] 在本申请实施例中，上述满足预定条件包括以下至少一项：检测到登陆该第一账号的目标应用处于安全模式，或者，检测到目标用户与第二电子设备间的距离超过预定阈值。

[0045] 需要理解的是，上述目标对象可以包括以下至少一项：其他账号，其他电子设备对应的使用用户。

[0046] 在本申请实施例中，上述登陆该第一账号的目标应用处于安全模式是指：登陆该第一账号的目标应用的当前使用环境安全。可以理解，当某一应用处于该安全模式下时，可以认为登录或使用该第一账号的使用者为该电子设备的持有者，或被持有者授权允许使用。上述目标用户与第二电子设备间的距离超过预定阈值是指：目标用户离开第二电子设备的使用范围，例如，在第二电子设备为电脑的情况下，用户从电脑前离开至较远的距离。

[0047] 可选地，在本申请实施例中，在多台电子设备同时登陆同一账号的场景下，用户可以从中选择一台或多台电子设备开启安全模式，或直接将该账号对应的目标应用设置为安全模式，此时安全模式对应的设备可以由用户自己选定。在该安全模式下的电子设备均可以通过该账号正常查看、接收、发送消息，而其他电子设备通过该账号发送的信息会被服务器拦截。

[0048] 示例性的，在第一电子设备中登录第一账号的目标应用处于安全模式时，与第一电子设备登陆同一账号的其他电子设备仅仅处于账号登陆状态，不能通过该账号与其他账号联络，也不会收到其他账号所发的新信息。即，当第一电子设备中登录第一账号的目标应用处于安全模式时，如果有用户使用第二电子设备中的第一账号向其他账号发送信息时，服务器在接收到该信息后，会直接拦截该信息，并将该信息全部转移至第一电子设备中。

[0049] 可选地，在本申请实施例中，服务器可以默认特定设备类型的电子设备中的目标

应用一直处于安全模式，例如，智能手机以第一账号登陆目标应用之后，其一直处于安全模式。或者，在第一电子设备开启安全模式时，该第一电子设备会向服务器发送信息，来告知服务器其已经开启安全模式。

[0050] 可选地，在本申请实施例中，上述服务器在检测到第二电子设备通过上述第一账号向目标对象发送目标信息的情况下，拦截目标信息的过程包括：在接收到第二电子设备通过该第一账号向目标对象发送目标信息的情况下，拦截目标信息；或者，在接收到第二电子设备通过该第一账号在与目标对象的对话框中输入信息的情况下，拦截目标信息。

[0051] 具体地，在本申请实施例中，可以在服务器上设立好一些相关的隐私关键字(该隐私关键字可以是用户根据实际场景自主设置的)，例如：转账、汇款等，如此，当服务器接检测到第二电子设备中的第一账号向目标对象发送的目标信息、且该目标信息中包含上述隐私关键字，则拦截上述目标信息，并将上述目标信息转发至第一电子设备。在检测到在对话框中输入信息(发送后即为目标消息)中包含这些隐私关键字的时候，在发送目标消息之后，拦截目标信息。

[0052] 可选地，在本申请实施例中，上述步骤201之后，本申请实施例提供的控制电子设备的方法还可以包括如下步骤：

[0053] 步骤A：在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则在检测到第二电子设备通过第一账号向目标对象发送目标信息的情况下，则向上述第一电子设备发送目标提示信息。

[0054] 其中，上述目标提示信息用于提示用户上述第二电子设备通过上述第一账号向目标对象发送上述目标信息。

[0055] 可以理解的，在通信会话场景中，目标对象可以指的是第一账号中任意好友或者陌生人，只要是能于第一账号对应的用户进行会话即可。

[0056] 进一步，上述目标提示信息还用于提示用户是否关闭第一电子设备中的目标应用的安全模式，以及还用于提示该目标信息已被服务器拦截。例如，用户1同时在手机和电脑上登陆了账号1，用户1从电脑前离开后，开启了手机的安全模式，此时，若有其他用户在电脑上使用账号1向其他账号发送信息，该信息经过服务器时，会被服务器直接拦截，并向手机发送提示信息，如“你刚刚在电脑端给“XXX”发送了一条信息，服务器已为您拦截，请问是否取消手机模式?”。

[0057] 此外，针对第二电子设备，该第二电子设备在通过第一账号向目标对象发送完目标信息后，服务器会向该第二电子设备发送第一提示信息，该第一提示信息用于向第二电子设备的使用者提示以下至少一项信息：消息发送失败，退出第一电子设备的安全模式，输入解密信息解锁。

[0058] 例如，用户1同时在手机和电脑上登陆了账号1，用户1从电脑前离开后，开启了手机的安全模式，此时，若有其他用户在电脑上使用账号1向目标对象(其他账号)发送信息，该信息经过服务器时，会被服务器直接拦截，并向电脑提示“消息发送失败，请在手机上退出手机模式，或输入隐私密码解锁”。

[0059] 在本申请实施例中，在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件(即检测到登陆上述第一账号的目标应用处于安全模式，和/或，检测到目标用户与上述第二电子设备间的距离超过预定阈值)，则服务器可以在检测到第二电子

设备通过该第一账号向目标对象发送目标信息的情况下，则确认当前的第二电子设备中登陆的第一账号存在安全隐患，从而拦截目标信息，并停止目标信息的传输。同时，为了提醒使用第一电子设备的用户当前的第二电子设备中登陆的第一账号存在安全隐患，因此，服务器会将原本需要发送给第二账号的目标信息转发至第一电子设备，从而避免了账号被不法分子冒用，提高了信息的安全性。

[0060] 可选地，在本申请实施例中，服务器可以对目标应用中的账号发送的信息进行加密处理，从而增加信息传输的安全性。

[0061] 示例性的，在上述第一电子设备与上述第二电子设备同时登陆上述第一账号的情况下，本申请实施例提供的控制电子设备的方法还可以包括如下步骤：

[0062] 步骤B1：服务器在接收到第二账号向第一账号发送第一信息的情况下，对第一信息进行加密处理以得到第二信息。

[0063] 步骤B2：服务器将第二信息发送至第二电子设备中的第一账号。

[0064] 示例性的，服务器可以对上述第一信息进行加密，得到第二信息，并将上述第二信息发送至上述第一账号，并在第二电子设备中显示。如此，第二电子设备作为对端，其使用者需要对第二信息进行解密才可得到第一信息。

[0065] 可以理解的，所述第二信息可以是对关键词(例如：数字、身份证号、姓名等)进行模糊处理、马赛克处理后的信息等等，第二电子设备接收到的信息在未解密的情况下，无法真实的获取信息内容，防止陌生人对于消息的偷看。

[0066] 进一步可选地，在上述步骤B2之后，本申请实施例提供的技术方案还可以包括：将所述第一信息发送至第一电子设备的第一账号。

[0067] 进一步可选地，服务器在接收到目标对象对应的第二账号向第一账号发送第一信息的情况下，可以在第一电子设备中登录该第一账号的目标应用处于安全模式时，对第一信息进行加密处理以得到第二信息。

[0068] 示例性的，在多台电子设备同时登陆同一账号的场景下，用户可以从中选择一台或多台电子设备开启安全模式，在该安全模式下的电子设备中的目标应用中登录的账号均可正常查看、接收、发送消息，其他电子设备中的目标应用中登录的账号则需要执行相应的安全操作才可通过该账号查看消息。

[0069] 如此，服务器通过对所有登陆第一账号的电子设备进行安全评估，按照不同的安全等级，采用不同的信息传输方式发送信息，在避免隐私信息被泄露的情况下，保证安全性高的电子设备可以直接查看到该信息。

[0070] 本申请实施例提供一种控制电子设备的方法，应用于第一电子设备，如图3所示，该控制电子设备的方法可以包括如下步骤：

[0071] 步骤301：在第一电子设备与第二电子设备同时登陆第一账号的情况下，第一电子设备接收服务器向第一电子设备发送的目标信息。

[0072] 其中，上述目标信息为：第二电子设备通过第一账号向目标对象发送的信息。进一步的，上述目标信息可以是：服务器在接收到第二电子设备发送的目标信息时转发给第一电子设备的。

[0073] 可选地，在本申请实施例中，在第一电子设备与第二电子设备同时登陆第一账号的情况下，本申请实施例提供的控制电子设备的方法还可以包括如下步骤：

[0074] 步骤302:第一电子设备接收服务器向第一电子设备发送的目标提示信息。

[0075] 其中,上述目标提示信息用于提示用户第二电子设备通过第一账号向目标对象发送目标信息。

[0076] 可选地,在本申请实施例中,本申请实施例提供的控制电子设备的方法还可以包括如下步骤C1或步骤C2:

[0077] 步骤C1:第一电子设备接收用户的第一输入。

[0078] 步骤C2:第一电子设备响应于第一输入,控制第二电子设备开启摄像头进行图像采集。

[0079] 可以理解的,第一电子设备在接收到第一输入后,会向第二电子设备发送控制指令,以指示第二电子设备开启摄像头进行图像采集,从而获取此时在使用第二电子设备的人员,以保障隐私安全。

[0080] 可选地,在本申请实施例中,本申请实施例提供的控制电子设备的方法还可以包括如下步骤D21或步骤D22:

[0081] 步骤D1:第一电子设备接收用户的第二输入。

[0082] 步骤D2:第一电子设备响应于第二输入,向服务器发送第一指令,该第一指令用于指示服务器将目标信息发送至第二账号。

[0083] 可以理解的,上述第一指令还用于指示服务器取消拦截操作,继续将上述目标信息发送至第二账号。即,在目标消息不含有一些隐私内容,或者知晓当前使用用户为安全用户(熟人)的时候,可以开启权限,允许当前使用第二电子设备的用户通过第一账号进行一系列操作。

[0084] 进一步的,第一电子设备在接收到该目标提示信息后,可以先控制第二电子设备开启摄像头以采集第二电子设备端当前的具体环境,即采集当前使用的人员图像,若确定第二电子设备的使用人员为安全用户,便向服务器发送第一指令,来指示服务器不要拦截上述目标信息;若确定第二电子设备的使用者为非法用户,则对该非法用户的样貌进行记录,并保持拦截(禁止通过第一账号进行操作),极大程度的降低了用户隐私不被窃取的隐患。

[0085] 在一种示例中,第一电子设备在关闭安全模式时,该第一电子设备会自动向服务器发送第一指令,以指示服务器不要拦截上述目标信息。

[0086] 此外,在第一电子设备处于安全模式的情况下,第一电子设备可以设置部分隐私账号,当第一电子设备通过第一账号与隐私账号联系时,该第一账号与隐私账号间的信息不会显示在第二电子设备上。如果需要在第二电子设备中查看该第一账号与隐私账号间的信息,则用户可以进行相应的安全操作,才可查看消息。例如,输出用户在手机上设置的安全密码。

[0087] 需要说明的是,本申请实施例提供的控制电子设备的方法,执行主体可以为控制电子设备的装置(该装置可以为电子设备或服务器),或者,该控制电子设备的装置中的用于执行加载控制电子设备的方法的控制模块。本申请实施例中以服务器或电子设备执行控制电子设备的方法为例,说明本申请实施例提供的控制电子设备的方法。

[0088] 本申请实施例提供一种控制电子设备的装置,如图4所示,该装置包括:处理模块401以及发送模块402,其中:

[0089] 处理模块401，用于在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则在检测到上述第二电子设备通过上述第一账号向目标对象发送目标信息的情况下，拦截上述目标信息；发送模块402，用于将上述处理模块401拦截的上述目标信息转发至上述第一电子设备；其中，上述满足预定条件包括以下至少一项：检测到登陆上述第一账号的目标应用处于安全模式，或者，检测到目标用户与上述第二电子设备间的距离超过预定阈值。

[0090] 可选地，上述处理模块401，还用于在接收到第二账号向上述第一账号发送第一信息的情况下，对上述第一信息进行加密处理以得到第二信息；上述发送模块402，还用于将上述处理模块401得到的上述第二信息发送至上述第二电子设备中的上述第一账号。

[0091] 可选地，上述发送模块402，还用于将上述第一信息发送至上述第一电子设备的上述第一账号。

[0092] 在本申请实施例提供的控制电子设备的装置中，在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件(即检测到登陆上述第一账号的目标应用处于安全模式，和/或，检测到目标用户与上述第二电子设备间的距离超过预定阈值)，该控制电子设备的装置在检测到上述第二电子设备通过上述第一账号向目标对象发送目标信息的情况下，确认当前的第二电子设备中登陆的第一账号存在安全隐患，从而拦截目标信息，并停止目标信息的传输。同时，为了提醒使用第一电子设备的用户当前的第二电子设备中登陆的第一账号存在安全隐患，因此，该控制电子设备的装置会将原本需要发送给第二账号的目标信息转发给第一电子设备，从而避免了账号被不法分子冒用，提高了信息的安全性。

[0093] 本申请实施例提供一种控制电子设备的装置，如图5所示，该装置包括：接收模块501，其中：

[0094] 接收模块501，用于在第一电子设备与第二电子设备同时登陆第一账号的情况下，接收服务器向第一电子设备发送的目标信息；其中，上述目标信息为：第二电子设备通过第一账号向第二账号发送的信息。

[0095] 可选地，如图6所示，该装置还包括：处理模块502，其中：上述接收模块501，还用于接收用户的第一输入；处理模块502，还用于响应于接收模块501接收到的所述第一输入，控制第二电子设备开启摄像头进行图像采集。

[0096] 可选地，如图7所示，该装置还包括：发送模块503，其中：接收模块501，还用于接收用户的第二输入；发送模块503，用于响应于接收模块501接收到的第二输入，向服务器发送第一指令，上述第一指令用于指示服务器将目标信息发送至第二账号。

[0097] 在本申请实施例提供的控制电子设备的装置中，在第一电子设备与第二电子设备同时登陆第一账号的情况下，服务器将原本需要发送给第二账号的目标信息转发给第一电子设备。如此，该控制电子设备的装置在接收到该目标信息后，便可提醒使用第一电子设备的用户当前的第二电子设备中登陆的第一账号存在安全隐患，从而避免了账号被不法分子冒用，提高了信息的安全性。

[0098] 需要说明的是，上述控制电子设备的装置可以是装置，也可以是电子设备中的部件、集成电路、或芯片。该装置可以是移动电子设备，也可以为非移动电子设备。示例性的，该移动电子设备可以为手机、平板电脑、笔记本电脑、掌上电脑、车载电子设备、可穿戴设

备、超级移动个人计算机(ultra-mobile personal computer,UMPC)、上网本或者个人数字助理(personal digital assistant,PDA)等,非移动电子设备可以为服务器、网络附属存储器(Network Attached Storage,NAS)、个人计算机(personal computer,PC)、电视机(television,TV)、柜员机或者自助机等,本申请实施例不作具体限定。

[0099] 本申请实施例中的控制电子设备的装置可以为具有操作系统的装置。该操作系统可以为安卓(Android)操作系统,可以为iOS操作系统,还可以为其他可能的操作系统,本申请实施例不作具体限定。

[0100] 本申请实施例提供的控制电子设备的装置能够实现图2或图3的方法实施例中控制电子设备的装置实现的各个过程,为避免重复,这里不再赘述。

[0101] 本实施例中各种实现方式具有的有益效果具体可以参见上述方法实施例中相应实现方式所具有的有益效果,为避免重复,此处不再赘述。

[0102] 可选的,本申请实施例还提供一种电子设备,如图8所示,包括处理器801,存储器802,存储在存储器802上并可在所述处理器801上运行的程序或指令,例如,该电子设备为服务器时,该程序或指令被处理器801执行时实现上述图2对应方法实施例的各个过程,且能达到相同的技术效果。该电子设备为上述第一电子设备时,该程序或指令被处理器801执行时实现上述图3对应方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0103] 需要注意的是,本申请实施例中的电子设备包括上述所述的移动电子设备和非移动电子设备。

[0104] 图9为实现本申请实施例的一种电子设备的硬件结构示意图。该电子设备为第一电子设备,该电子设备100包括但不限于:射频单元101、网络模块102、音频输出单元103、输入单元104、传感器105、显示单元106、用户输入单元107、接口单元108、存储器109、以及处理器110等部件。

[0105] 本领域技术人员可以理解,电子设备100还可以包括给各个部件供电的电源(比如电池),电源可以通过电源管理系统与处理器110逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。图9中示出的电子设备结构并不构成对电子设备的限定,电子设备可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置,在此不再赘述。

[0106] 其中,上述射频单元101,用于在第一电子设备与第二电子设备同时登陆第一账号的情况下,接收服务器向第一电子设备发送的目标信息;其中,上述目标信息为:第二电子设备通过第一账号向第二账号发送的信息。

[0107] 可选地,上述射频单元101,还用于接收用户的第一输入;上述处理器110,还用于响应于射频单元101接收到的所述第一输入,控制第二电子设备开启摄像头进行图像采集。

[0108] 可选地,上述射频单元101,还用于接收用户的第二输入;上述处理器110,用于响应于射频单元101接收到的第二输入,向服务器发送第一指令,上述第一指令用于指示服务器将目标信息发送至第二账号。

[0109] 在本申请实施例提供的第一电子设备中,在第一电子设备与第二电子设备同时登陆第一账号的情况下,服务器将原本需要发送给第二账号的目标信息转发给第一电子设备中的第一账号。如此,第一电子设备在接收到该目标信息后,便可提醒使用第一电子设备的

用户当前的第二电子设备中登陆的第一账号存在安全隐患,从而避免了账号被不法分子冒用,提高了信息的安全性。

[0110] 应理解的是,本申请实施例中,输入单元104可以包括图形处理器(Graphics Processing Unit,GPU)1041和麦克风1042,图形处理器1041对在视频捕获模式或图像捕获模式中由图像捕获装置(如摄像头)获得的静态图片或视频的图像数据进行处理。显示单元106可包括显示面板1061,可以采用液晶显示器、有机发光二极管等形式来配置显示面板1061。用户输入单元107包括触控面板1071以及其他输入设备1072。触控面板1071,也称为触摸屏。触控面板1071可包括触摸检测装置和触摸控制器两个部分。其他输入设备1072可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆,在此不再赘述。存储器109可用于存储软件程序以及各种数据,包括但不限于应用程序和操作系统。处理器110可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器110中。

[0111] 本申请实施例还提供一种可读存储介质,所述可读存储介质上存储有程序或指令,该程序或指令被处理器执行时实现上述控制电子设备的方法的方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0112] 其中,所述处理器为上述实施例中所述的电子设备中的处理器。所述可读存储介质,包括计算机可读存储介质,如计算机只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等。

[0113] 本申请实施例另提供提供了一种芯片,所述芯片包括处理器和通信接口,所述通信接口和所述处理器耦合,所述处理器用于运行程序或指令,实现上述控制电子设备的方法的方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0114] 应理解,本申请实施例提到的芯片还可以称为系统级芯片、系统芯片、芯片系统或片上系统芯片等。

[0115] 本申请实施例提供了一种计算机程序产品,该程序产品被存储在非易失的存储介质中,该程序产品被至少一个处理器执行以实现上述控制电子设备的方法的方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0116] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。此外,需要指出的是,本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能,还可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,例如,可以按不同于所描述的次序来执行所描述的方法,并且还可以添加、省去、或组合各种步骤。另外,参照某些示例所描述的特征可在其他示例中被组合。

[0117] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本申请的技术方案本质上或者说对现有技术做

出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

[0118] 上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本申请的保护之内。

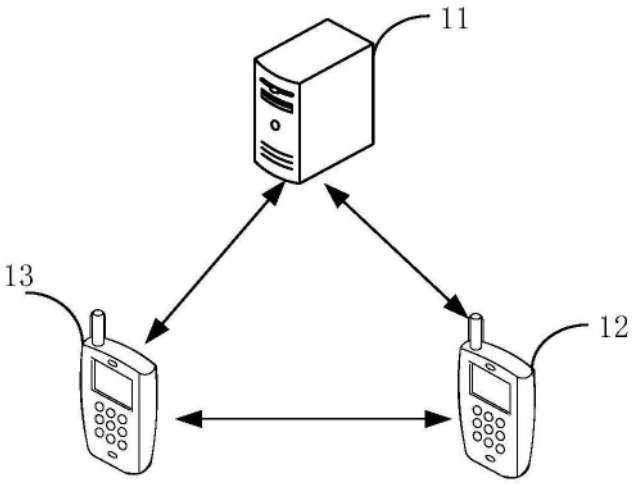

11
13
12

图1

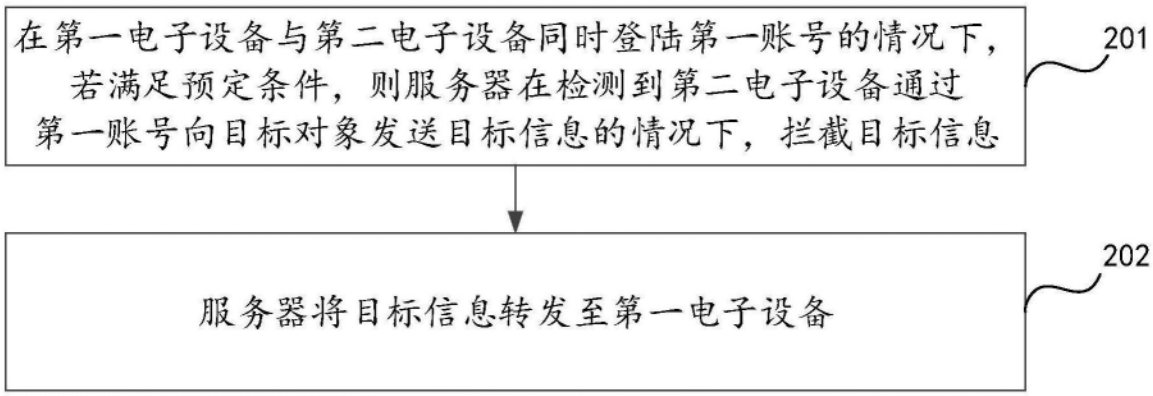

在第一电子设备与第二电子设备同时登陆第一账号的情况下，若满足预定条件，则服务器在检测到第二电子设备通过第一账号向目标对象发送目标信息的情况下，拦截目标信息
201
服务器将目标信息转发至第一电子设备
202

图2

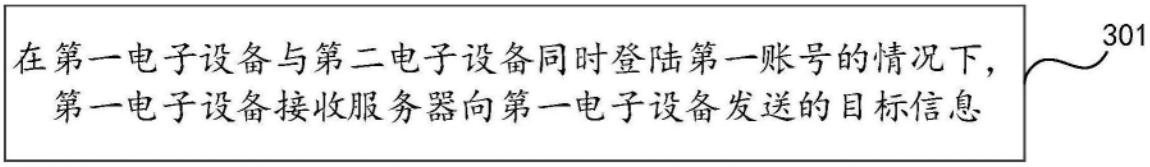

在第一电子设备与第二电子设备同时登陆第一账号的情况下，第一电子设备接收服务器向第一电子设备发送的目标信息
301

图3

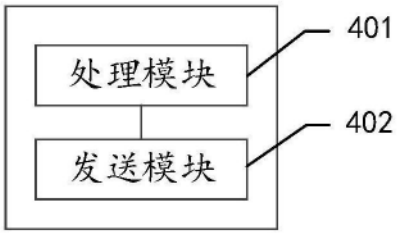


图4

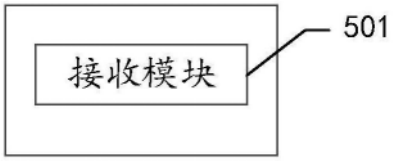


图5

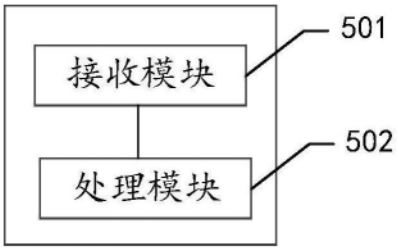


图6

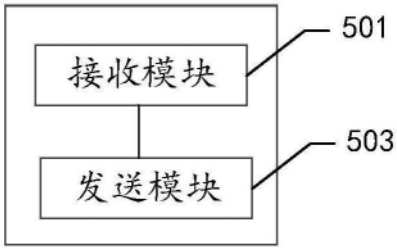


图7

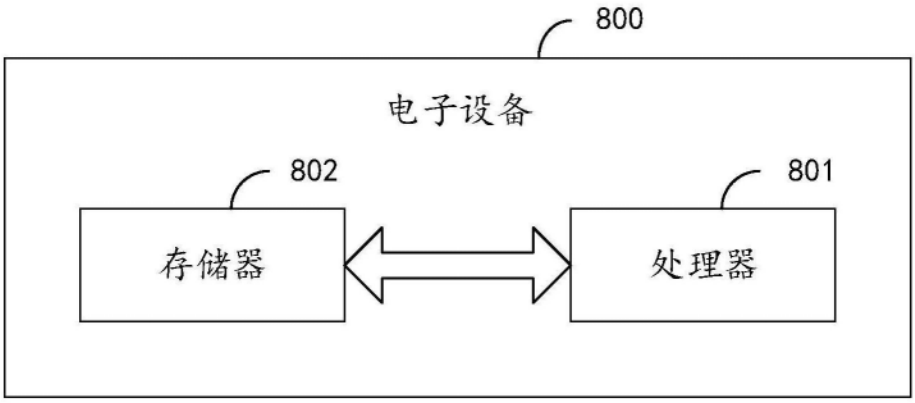

800
电子设备
802
存储器
801
处理器

图8

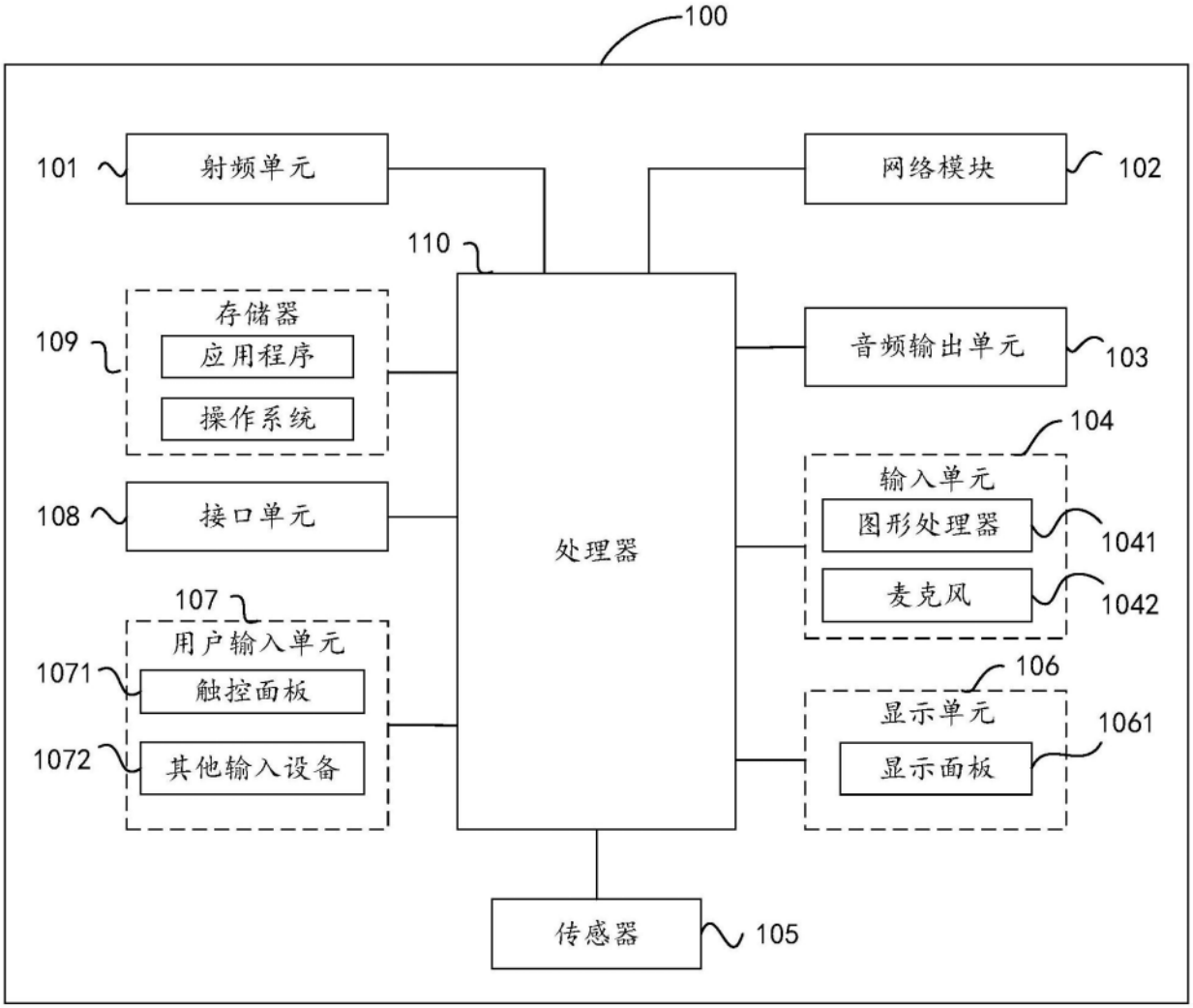

100
101
射频单元
网络模块
102
110
存储器
109
应用程序
操作系统
音频输出单元
103
104
输入单元
108
接口单元
处理器
图形处理器
1041
麦克风
1042
107
用户输入单元
106
1071
触控面板
显示单元
1061
1072
其他输入设备
显示面板
传感器
105

图9