(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105701420 B
(45)授权公告日 2019.05.14

(21)申请号 201610098934.2

(22)申请日 2016.02.23

(65)同一申请的已公布的文献号
申请公布号 CN 105701420 A

(43)申请公布日 2016.06.22

(73)专利权人 深圳市金立通信设备有限公司
地址 518040 广东省深圳市福田区深南大道7028号时代科技大厦东座21楼

(72)发明人 刘立荣

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

(51)Int.Cl.
G06F 21/62(2013.01)

(56)对比文件
CN 1425157 A,2003.06.18,
CN 1425157 A,2003.06.18,
CN 104036202 A,2014.09.10,
CN 103634482 A,2014.03.12,

审查员 刘义乐

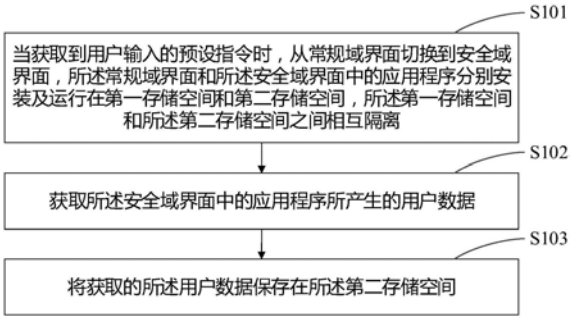
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种用户数据的管理方法及终端

(57)摘要

本发明实施例公开了一种用户数据的管理方法，包括：当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离；获取所述安全域界面中的应用程序所产生的用户数据；将获取的所述用户数据保存在所述第二存储空间。相应的，本发明实施例还公开了一种终端。采用本发明实施例，可以实现将应用程序所产生的用户数据隔离到独立的存储空间，从而避免用户数据被泄露。



CN 105701420 B

1.一种用户数据的管理方法,其特征在于,所述方法包括:

当获取到用户输入的预设指令时,从常规域界面切换到安全域界面,所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间,所述第一存储空间和所述第二存储空间之间相互隔离;

获取所述安全域界面中的应用程序所产生的用户数据;

将获取的所述用户数据保存在所述第二存储空间,所述用户数据被存储至所述第二存储空间中的隐藏文件夹中,在安全域界面接收到用户针对拨号盘APP输入的正确的字符信息时,允许读取所述隐藏文件夹中所保存的所述用户数据。

2.如权利要求1所述的方法,其特征在于,所述当获取到用户输入的预设指令时,从常规域界面切换到安全域界面之后,还包括:

当获取到用户输入的身份验证信息时,判断所述身份验证信息是否与预设的验证信息匹配;

若是,则在所述安全域界面中显示预先隐藏的应用程序。

3.如权利要求2所述的方法,其特征在于,所述判断所述身份验证信息是否与预设的验证信息匹配之后,还包括:

若是,则允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据。

4.如权利要求1所述的方法,其特征在于,所述当获取到用户输入的预设指令时,从常规域界面切换到安全域界面之后,还包括:

当获取到用户针对拨号盘应用程序输入的字符信息时,判断所述字符信息是否与预设的模板信息匹配;

若是,则打开保存在所述第二存储空间的隐藏文件夹。

5.如权利要求2或3所述的方法,其特征在于,所述身份验证信息包括指纹信息、虹膜信息或人脸信息。

6.一种终端,其特征在于,所述终端包括:

界面切换单元,用于当获取到用户输入的预设指令时,从常规域界面切换到安全域界面,所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间,所述第一存储空间和所述第二存储空间之间相互隔离;

数据获取单元,用于获取所述安全域界面中的应用程序所产生的用户数据;

数据保存单元,用于将获取的所述用户数据保存在所述第二存储空间,所述用户数据被存储至所述第二存储空间中的隐藏文件夹中,在安全域界面接收到用户针对拨号盘APP输入的正确的字符信息时,允许读取所述隐藏文件夹中所保存的所述用户数据。

7.如权利要求6所述的终端,其特征在于,所述终端还包括:

身份验证单元,用于当获取到用户输入的身份验证信息时,判断所述身份验证信息是否与预设的验证信息匹配;

应用显示单元,用于若是,则在所述安全域界面中显示预先隐藏的应用程序。

8.如权利要求7所述的终端,其特征在于,所述终端还包括:

数据调用单元,用于若是,则允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据。

9.如权利要求6所述的终端，其特征在于，所述终端还包括：

文件夹解密单元，用于当获取到用户针对拨号盘应用程序输入的字符信息时，判断所述字符信息是否与预设的模板信息匹配；若是，则打开保存在所述第二存储空间的隐藏文件夹。

10.如权利要求7或8所述的终端，其特征在于，所述身份验证信息包括指纹信息、虹膜信息或人脸信息。

一种用户数据的管理方法及终端

技术领域

[0001] 本发明涉及安全技术领域，尤其涉及一种用户数据的管理方法及终端。

背景技术

[0002] 随着电子技术的不断发展，如智能手机和平板电脑等的终端已成为用户必不可少的随身物品。与此同时，终端也成为了用户的私有物品，用户在使用终端所安装的APP(Application，应用程序)时，会产生一些涉及隐私的用户数据，例如短消息、聊天记录、通话记录、图片和视频等的数据。

[0003] 这些用户数据，若被他人翻看到，将会严重影响用户的情绪，甚者影响到财产安全和家庭幸福。因此，如何避免用户数据被泄露已成为目前亟需解决的问题。

发明内容

[0004] 本发明实施例提供一种用户数据的管理方法及终端，可以避免用户数据被泄露。

[0005] 本发明实施例提供的一种用户数据的管理方法，包括：

[0006] 当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离；

[0007] 获取所述安全域界面中的应用程序所产生的用户数据；

[0008] 将获取的所述用户数据保存在所述第二存储空间。

[0009] 相应的，本发明实施例还提供了一种终端，包括：

[0010] 界面切换单元，用于当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离；

[0011] 数据获取单元，用于获取所述安全域界面中的应用程序所产生的用户数据；

[0012] 数据保存单元，用于将获取的所述用户数据保存在所述第二存储空间。

[0013] 本发明实施例中，终端包括常规域界面和安全域界面，常规域界面和安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，且这两个存储空间相互隔离，在终端从常规域界面切换到安全域界面之后，当获取到安全域界面中的应用程序所产生的用户数据时，将该用户数据保存在第二存储空间，可以实现将应用程序所产生的用户数据隔离到独立的存储空间，从而避免用户数据被泄露。

附图说明

[0014] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0015] 图1是本发明实施例提供的一种用户数据的管理方法的流程示意图；

[0016] 图2是本发明实施例提供的另一种用户数据的管理方法的流程示意图；

[0017] 图3是本发明实施例提供的一种终端的结构示意图；

[0018] 图4是本发明实施例提供的另一种终端的结构示意图；

[0019] 图5是本发明实施例提供的一种终端系统架构的示意图。

具体实施方式

[0020] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0021] 本发明实施例提供的用户数据的隔离方法实现于终端，所述终端包括智能手机、平板电脑、数字音视频播放器、电子阅读器、手持游戏机或车载电子设备等电子设备，所述终端可以运行APP。

[0022] 图1是本发明实施例中一种用户数据的管理方法的流程示意图。如图所示本实施例中的用户数据的隔离方法的流程可以包括：

[0023] S101，当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离。

[0024] 本发明实施例中，终端的系统设置有至少两个域环境(简称为“域”)，包括常规域和安全域，安全域的访问权限相比常规域要高一些，故常用于存放一些相对重要的数据和APP。需要说明的是，域面向用户的操作界面被称为域界面，也就是说，安全域面向用户的操作界面称为安全域界面，常规域面向用户的操作界面称为常规域界面。常规域界面和安全域界面中的APP分别安装及运行在第一存储空间和第二存储空间，其中第一存储空间和第二存储空间之间相互隔离。具体实现过程中，本发明实施例中终端的架构如图5所示自下而上包括硬件、核心(kernel)层、操作系统和域，其中硬件由处理器和存储器等的硬件资源组成，核心层由操作系统中用于管理存储器、文件、外设和系统资源等的软件资源组成，操作系统是管理硬件资源与软件资源的计算机程序，常规域和安全域设立于操作系统之上，分配有独立的存储空间，相互隔离。可见，所述隔离既包括物理存储上的隔离，也包括软件逻辑上的隔离，即硬件和软件两个维度上的隔离。

[0025] 具体的，终端当获取到用户输入的预设指令时，从常规域界面切换到安全域界面。其中，所述预设指令可以由设备商在出厂前设定，也可以由用户预先设定，这里不做限定。例如：终端处于常规域界面时，当获取到用户长按home键以及在触摸屏上向右滑动的操作时，从常规域界面切换到安全域界面。进一步的，终端在切换到安全域界面之前，向用户请求输入密码，使得只有终端所属用户本身才有权限访问安全域，避免其他用户非法访问。

[0026] S102，获取所述安全域界面中的应用程序所产生的用户数据。

[0027] 应理解的，用户在使用APP时，APP会产生一些涉及隐私的用户数据，例如：短信APP会产生短消息数据、社交APP会产生聊天记录数据、拨号APP会产生通话记录数据、图库APP会产生图片数据以及播放器APP会产生视频数据。

[0028] 具体的，在用户使用安全域界面的APP的过程中，终端获取被使用的APP所产生的

一切用户数据。

[0029] S103,将获取的所述用户数据保存在所述第二存储空间。

[0030] 具体的,终端将获取的用户数据保存在第二存储空间。应理解的,由于第二存储空间与第一存储空间是相互隔离,常规域界面只能访问第一存储空间,不能访问第二存储空间,因而其他用户在没有权限访问安全域界面时,只能处于常规域界面,无法翻看到安全域界面中APP所产生用户数据,提高了安全性和对隐私的保护。

[0031] 作为一种可选的实施方式,终端从常规域界面切换到安全域界面之后,当获取到用户输入的身份验证信息时,判断身份验证信息是否与预设的验证信息匹配。可选的,所述身份验证信息可以是字符密码、图形密码和手势密码等的验证信息,本发明实施例不做限定。优选的,所述身份验证信息为利用生物识别技术的验证信息,如指纹信息、虹膜信息和人脸信息,优点在于,指纹信息、虹膜信息和人脸信息可以作为人的唯一识别标识,其他用户无法盗取这类身份验证信息。进一步的,终端若判定身份验证信息与预设的验证信息匹配,则在安全域界面中显示预先隐藏的APP。本实施方式的优点在于,用户可以在安全域中预先将一些APP设置为隐藏状态,即使其他用户访问了安全域界面,若未通过身份验证,仍是不能翻看到被隐藏的APP中的用户数据,进一步提高了安全性和对隐私的保护。

[0032] 更进一步的,终端若判定身份验证信息与预设的验证信息匹配,则允许安全域界面中的APP调用保存在第二存储空间中的加密数据。其中,所述加密数据可以是短消息、聊天记录、通话记录、图片和视频等的数据,由用户预先设置为加密状态,在未通过身份验证之前,即使是安全域界面中的APP也不能访问加密数据。例如:假设加密数据为某图片,终端处于安全域界面,那么在通过身份验证之前,图库APP不能从第二存储空间中调出并显示该图片,在通过身份验证之后,图库APP才能从第二存储空间中调出并显示该图片。

[0033] 作为又一种可选的实施方式,终端从常规域界面切换到安全域界面之后,当获取到用户针对拨号盘APP输入的字符信息时,判断该字符信息是否与预设的模板信息匹配,例如:用户启动安全域界面中的拨号盘APP后,输入“12345#”的字符,终端判断“12345#”是否与预设的模板信息匹配。进一步的,终端若判定输入的字符信息与预设的模板信息匹配,则打开保存在第二存储空间的隐藏文件夹,例如:输入的字符信息为“12345#”,模板信息也为“12345#”,终端判定两者相匹配,此时打开保存在第二存储空间的隐藏文件夹,该隐藏文件夹中存放有文档、图片和视频数据。本实施方式的优点在于,用户可以通过安全域界面中的拨号盘APP访问隐藏文件夹,该操作隐秘而不容易被发现,进一步提高了安全性和对隐私的保护。

[0034] 本发明实施例中,终端包括常规域界面和安全域界面,常规域界面和安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间,且这两个存储空间相互隔离,在终端从常规域界面切换到安全域界面之后,当获取到安全域界面中的应用程序所产生的用户数据时,将该用户数据保存在第二存储空间,可以实现将应用程序所产生的用户数据隔离到独立的存储空间,从而避免用户数据被泄露。

[0035] 图2是本发明实施例中另一种用户数据的管理方法的流程示意图。如图所示本实施例中的用户数据的隔离方法的流程可以包括:

[0036] S201,当获取到用户输入的预设指令时,从常规域界面切换到安全域界面,所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空

间，所述第一存储空间和所述第二存储空间之间相互隔离。

[0037] 本发明实施例中，终端的系统设置有至少两个域环境(简称为“域”)，包括常规域和安全域，安全域的访问权限相比常规域要高一些，故常用于存放一些相对重要的APP。需要说明的是，域面向用户的操作界面被称为域界面，也就是说，安全域面向用户的操作界面称为安全域界面，常规域面向用户的操作界面称为常规域界面。常规域界面和安全域界面中的APP分别安装及运行在第一存储空间和第二存储空间，其中第一存储空间和第二存储空间之间相互隔离。具体实现过程中，本发明实施例中终端的架构如图5所示自下而上包括硬件、核心(kernel)层、操作系统和域，其中硬件由处理器和存储器等的硬件资源组成，核心层由操作系统中用于管理存储器、文件、外设和系统资源等的软件资源组成，操作系统是管理硬件资源与软件资源的计算机程序，常规域和安全域设立于操作系统之上，分配有独立的存储空间，相互隔离。可见，所述隔离既包括物理存储上的隔离，也包括软件逻辑上的隔离，即硬件和软件两个维度上的隔离。

[0038] 具体的，终端当获取到用户输入的预设指令时，从常规域界面切换到安全域界面。其中，所述预设指令可以由设备商在出厂前设定，也可以由用户预先设定，这里不做限定。例如：终端处于常规域界面时，当获取到用户长按home键以及在触摸屏上向右滑动的操作时，从常规域界面切换到安全域界面。进一步的，终端在切换到安全域界面之前，向用户请求输入密码，使得只有终端所属用户本身才有权限访问安全域，避免其他用户非法访问。

[0039] S202，当获取到用户输入的身份验证信息时，判断所述身份验证信息是否与预设的验证信息匹配。

[0040] 具体的，终端若判定身份验证信息与预设的验证信息匹配，则执行步骤S203和/或步骤S204，若否，则不做任何处理。

[0041] 可选的，所述身份验证信息可以是字符密码、图形密码和手势密码等的验证信息，本发明实施例不做限定。优选的，所述身份验证信息为利用生物识别技术的验证信息，如指纹信息、虹膜信息和人脸信息，优点在于，指纹信息、虹膜信息和人脸信息可以作为人的唯一识别标识，其他用户无法盗取这类身份验证信息。

[0042] S203，在所述安全域界面中显示预先隐藏的应用程序。

[0043] 本实施方式的优点在于，用户可以在安全域中预先将一些APP设置为隐藏状态，即使其他用户访问了安全域界面，若未通过身份验证，仍是不能翻看到被隐藏的APP中的用户数据，进一步提高了安全性和对隐私的保护。

[0044] S204，允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据。

[0045] 其中，所述加密数据可以是短消息、聊天记录、通话记录、图片和视频等的数据，由用户预先设置为加密状态，在未通过身份验证之前，即使是安全域界面中的APP也不能访问加密数据。例如：假设加密数据为某图片，终端处于安全域界面，那么在通过身份验证之前，图库APP不能从第二存储空间中调出并显示该图片，在通过身份验证之后，图库APP才能从第二存储空间中调出并显示该图片。

[0046] S205，当获取到用户针对拨号盘应用程序输入的字符信息时，判断所述字符信息是否与预设的模板信息匹配。

[0047] 具体的，终端若判定字符信息与预设的模板信息匹配，则执行步骤S206，否则不做

任何处理。

[0048] 例如:用户启动安全域界面中的拨号盘APP后,输入“12345#”的字符,终端判断“12345#”是否与预设的模板信息匹配。

[0049] S206,打开保存在所述第二存储空间的隐藏文件夹。

[0050] 例如:输入的字符信息为“12345#”,模板信息也为“12345#”,终端判定两者相匹配,此时打开保存在第二存储空间的隐藏文件夹,该隐藏文件夹中存放有文档、图片和视频数据。本实施方式的优点在于,用户可以通过安全域界面中的拨号盘APP访问隐藏文件夹,该操作隐秘而不容易被发现,进一步提高了安全性和对隐私的保护。

[0051] 本发明实施例中,终端包括常规域界面和安全域界面,常规域界面和安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间,且这两个存储空间相互隔离,在终端从常规域界面切换到安全域界面之后,当获取到用户输入的身份验证信息时,判断身份验证信息是否与预设的验证信息匹配,若是,则开放更多的权限,可以实现为安全域界面设置更多的权限,进一步提高安全性和对隐私的保护。

[0052] 图3是本发明实施例中一种终端的结构示意图。如图所示本发明实施例中的终端至少可以包括界面切换单元310、数据获取单元320以及数据保存单元330,其中:

[0053] 界面切换单元310,用于当获取到用户输入的预设指令时,从常规域界面切换到安全域界面,所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间,所述第一存储空间和所述第二存储空间之间相互隔离。

[0054] 本发明实施例中,终端的系统设置有至少两个域环境(简称为“域”),包括常规域和安全域,安全域的访问权限相比常规域要高一些,故常用于存放一些相对重要的APP。需要说明的是,域面向用户的操作界面被称为域界面,也就是说,安全域面向用户的操作界面称为安全域界面,常规域面向用户的操作界面称为常规域界面。常规域界面和安全域界面中的APP分别安装及运行在第一存储空间和第二存储空间,其中第一存储空间和第二存储空间之间相互隔离。具体实现过程中,本发明实施例中终端的架构如图5所示自下而上包括硬件、核心(kernel)层、操作系统和域,其中硬件由处理器和存储器等的硬件资源组成,核心层由操作系统中用于管理存储器、文件、外设和系统资源等的软件资源组成,操作系统是管理硬件资源与软件资源的计算机程序,常规域和安全域设立于操作系统之上,分配有独立的存储空间,相互隔离。可见,所述隔离既包括物理存储上的隔离,也包括软件逻辑上的隔离,即硬件和软件两个维度上的隔离。

[0055] 具体的,界面切换单元310当获取到用户输入的预设指令时,从常规域界面切换到安全域界面。其中,所述预设指令可以由设备商在出厂前设定,也可以由用户预先设定,这里不做限定。例如:终端处于常规域界面时,界面切换单元310当获取到用户长按home键以及在触摸屏上向右滑动的操作时,从常规域界面切换到安全域界面。进一步的,界面切换单元310在切换到安全域界面之前,向用户请求输入密码,使得只有终端所属用户本身才有权限访问安全域,避免其他用户非法访问。

[0056] 数据获取单元320,用于获取所述安全域界面中的应用程序所产生的用户数据。

[0057] 应理解的,用户在使用APP时,APP会产生一些涉及隐私的用户数据,例如:短信APP会产生短消息数据、社交APP会产生聊天记录数据、拨号APP会产生通话记录数据、图库APP会产生图片数据以及播放器APP会产生视频数据。

[0058] 具体的，在用户使用安全域界面的APP的过程中，数据获取单元320获取被使用的APP所产生的一切用户数据。

[0059] 数据保存单元330，用于将获取的所述用户数据保存在所述第二存储空间。

[0060] 可选的，请参阅图3，如图所示本发明实施例中的终端还可以包括身份验证单元340和应用显示单元350，其中：

[0061] 身份验证单元340，用于当获取到用户输入的身份验证信息时，判断所述身份验证信息是否与预设的验证信息匹配。

[0062] 可选的，所述身份验证信息可以是字符密码、图形密码和手势密码等的验证信息，本发明实施例不做限定。优选的，所述身份验证信息为利用生物识别技术的验证信息，如指纹信息、虹膜信息和人脸信息，优点在于，指纹信息、虹膜信息和人脸信息可以作为人的唯一识别标识，其他用户无法盗取这类身份验证信息。

[0063] 应用显示单元350，用于若是，则在所述安全域界面中显示预先隐藏的应用程序。

[0064] 本实施方式的优点在于，用户可以在安全域中预先将一些APP设置为隐藏状态，即使其他用户访问了安全域界面，若未通过身份验证，仍是不能翻看到被隐藏的APP中的用户数据，进一步提高了安全性和对隐私的保护。

[0065] 进一步的，请参阅图3，如图所示本发明实施例中的终端还可以包括数据调用单元360，用于若是，则允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据。

[0066] 其中，所述加密数据可以是短消息、聊天记录、通话记录、图片和视频等的数据，由用户预先设置为加密状态，在未通过身份验证之前，即使是安全域界面中的APP也不能访问加密数据。例如：假设加密数据为某图片，终端处于安全域界面，那么在通过身份验证之前，图库APP不能从第二存储空间中调出并显示该图片，在通过身份验证之后，图库APP才能从第二存储空间中调出并显示该图片。

[0067] 又可选的，请参阅图3，如图所示本发明实施例中的终端还可以包括文件夹解密单元370，用于当获取到用户针对拨号盘应用程序输入的字符信息时，判断所述字符信息是否与预设的模板信息匹配；若是，则打开保存在所述第二存储空间的隐藏文件夹。

[0068] 例如：用户启动安全域界面中的拨号盘APP后，输入“12345#”的字符，文件夹解密单元370判断“12345#”是否与预设的模板信息匹配。进一步的，文件夹解密单元370若判定输入的字符信息与预设的模板信息匹配，则打开保存在第二存储空间的隐藏文件夹，例如：输入的字符信息为“12345#”，模板信息也为“12345#”，文件夹解密单元370判定两者相匹配，此时打开保存在第二存储空间的隐藏文件夹，该隐藏文件夹中存放有文档、图片和视频数据。本实施方式的优点在于，用户可以通过安全域界面中的拨号盘APP访问隐藏文件夹，该操作隐秘而不容易被发现，进一步提高了安全性和对隐私的保护。

[0069] 图4是本发明实施例中的另一种终端的结构示意图，如图4所示，该终端可以包括：至少一个处理器401，例如CPU，至少一个通信总线402，至少一个用户接口403，存储器404。其中，通信总线402用于实现这些组件之间的连接通信；用户接口403可以包括触摸显示屏、按键以及指纹识别模块或摄像头，用于与用户进行交互，以及获取用户的身份验证信息；存储器404可以是高速RAM存储器，也可以是非易失的存储器(non-volatile memory)，例如至少一个磁盘存储器。可选的，存储器404还可以是至少一个位于远离前述处理器401的存储

装置。存储器404中存储一组程序代码，处理器401用于调用存储器404中存储的程序代码，执行以下操作：

[0070] 当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离；

[0071] 获取所述安全域界面中的应用程序所产生的用户数据；

[0072] 将获取的所述用户数据保存在所述第二存储空间。

[0073] 可选的，处理器401当获取到用户输入的预设指令时，从常规域界面切换到安全域界面之后，还执行：

[0074] 当获取到用户输入的身份验证信息时，判断所述身份验证信息是否与预设的验证信息匹配；

[0075] 若是，则在所述安全域界面中显示预先隐藏的应用程序。

[0076] 进一步的，处理器401判断所述身份验证信息是否与预设的验证信息匹配之后，还执行：

[0077] 若是，则允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据。

[0078] 又可选的，处理器401当获取到用户输入的预设指令时，从常规域界面切换到安全域界面之后，还执行：

[0079] 当获取到用户针对拨号盘应用程序输入的字符信息时，判断所述字符信息是否与预设的模板信息匹配；

[0080] 若是，则打开保存在所述第二存储空间的隐藏文件夹。

[0081] 又可选的，所述身份验证信息包括指纹信息、虹膜信息或人脸信息。

[0082] 本发明实施例中，终端包括常规域界面和安全域界面，常规域界面和安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，且这两个存储空间相互隔离，在终端从常规域界面切换到安全域界面之后，当获取到安全域界面中的应用程序所产生的用户数据时，将该用户数据保存在第二存储空间，可以实现将应用程序所产生的用户数据隔离到独立的存储空间，从而避免用户数据被泄露。

[0083] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0084] 本发明实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[0085] 本发明实施例装置中的单元，可以根据实际需要进行合并、划分和删减。

[0086] 本发明实施例中所述单元，可以通过通用集成电路，例如CPU(Central Processing Unit，中央处理器)，或通过ASIC(Application Specific Integrated Circuit，专用集成电路)来实现。

[0087] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

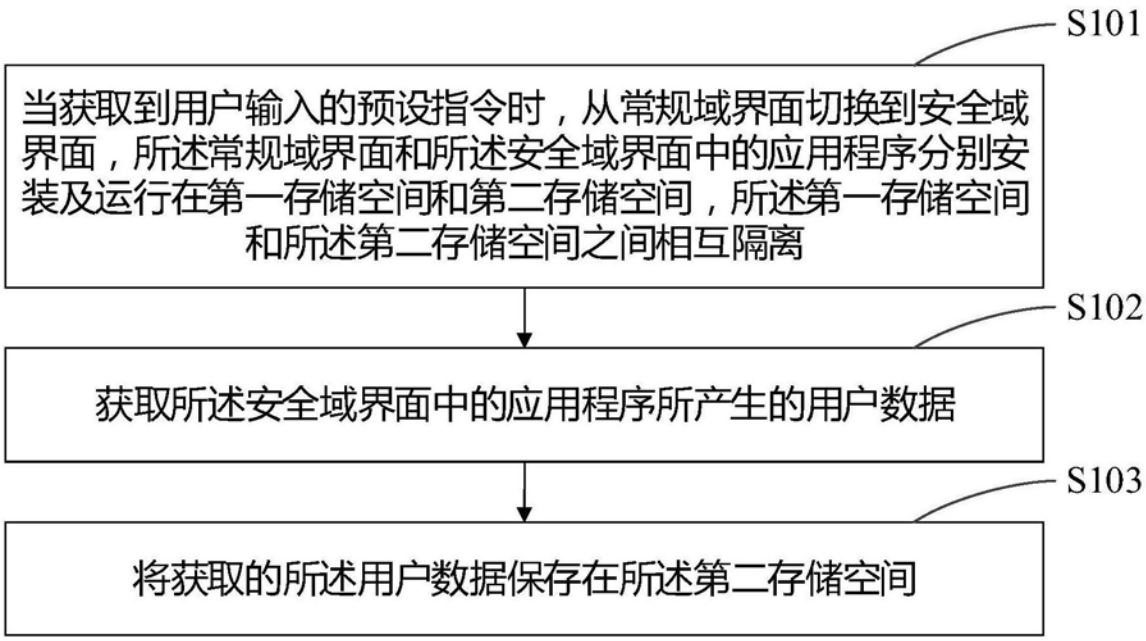

S101
当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离
S102
获取所述安全域界面中的应用程序所产生的用户数据
S103
将获取的所述用户数据保存在所述第二存储空间

图1

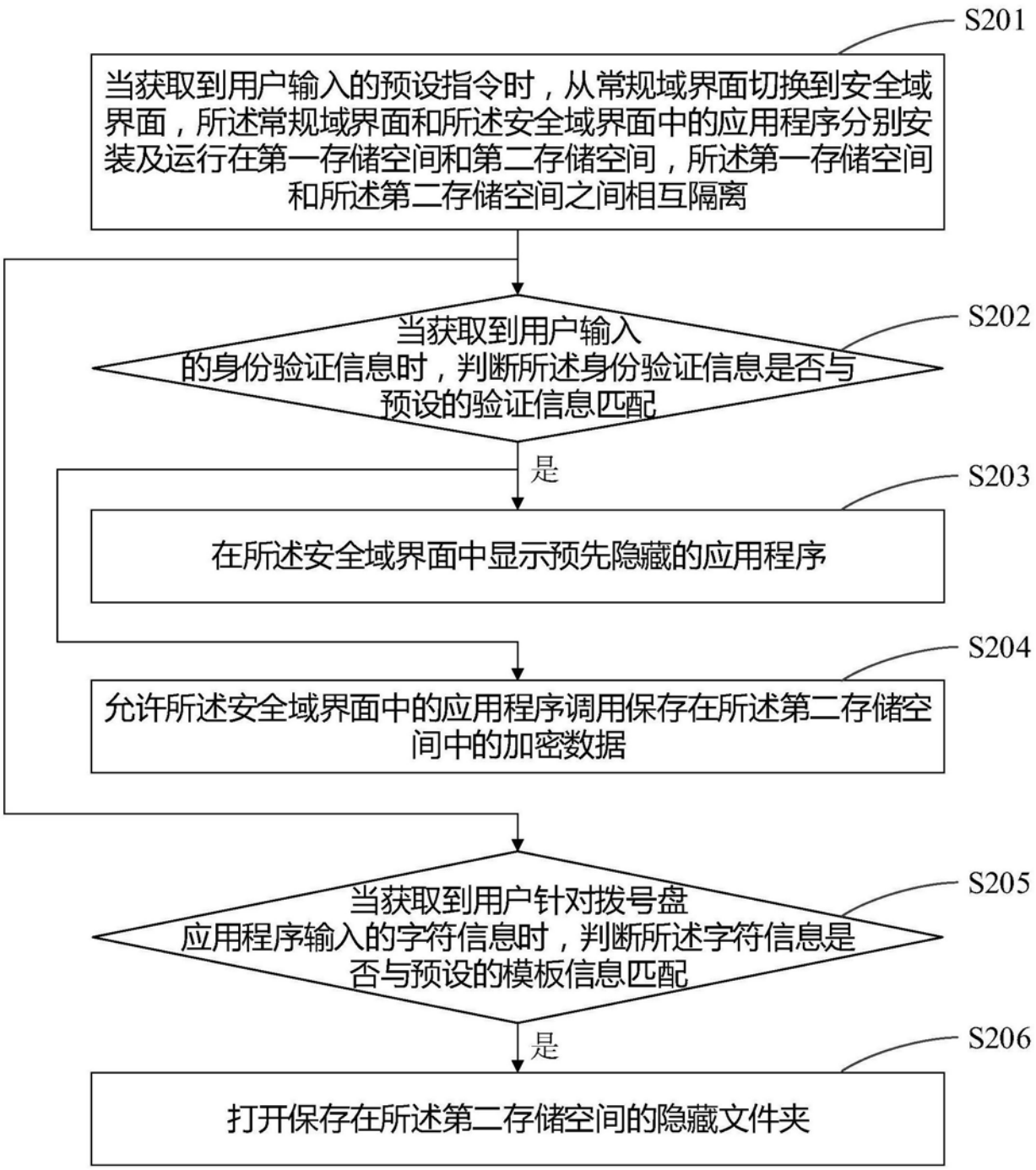

S201
当获取到用户输入的预设指令时，从常规域界面切换到安全域界面，所述常规域界面和所述安全域界面中的应用程序分别安装及运行在第一存储空间和第二存储空间，所述第一存储空间和所述第二存储空间之间相互隔离
S202
当获取到用户输入的身份验证信息时，判断所述身份验证信息是否与预设的验证信息匹配
是
S203
在所述安全域界面中显示预先隐藏的应用程序
S204
允许所述安全域界面中的应用程序调用保存在所述第二存储空间中的加密数据
S205
当获取到用户针对拨号盘应用程序输入的字符信息时，判断所述字符信息是否与预设的模板信息匹配
是
S206
打开保存在所述第二存储空间的隐藏文件夹

图2

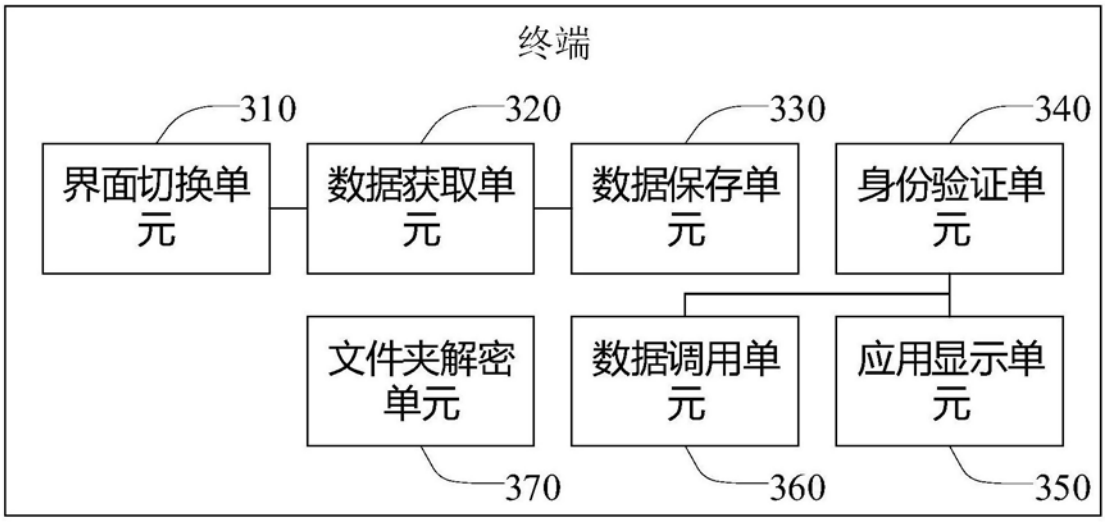

终端
310
320
330
340
界面切换单元
数据获取单元
数据保存单元
身份验证单元
文件夹解密单元
数据调用单元
应用显示单元
370
360
350

图3

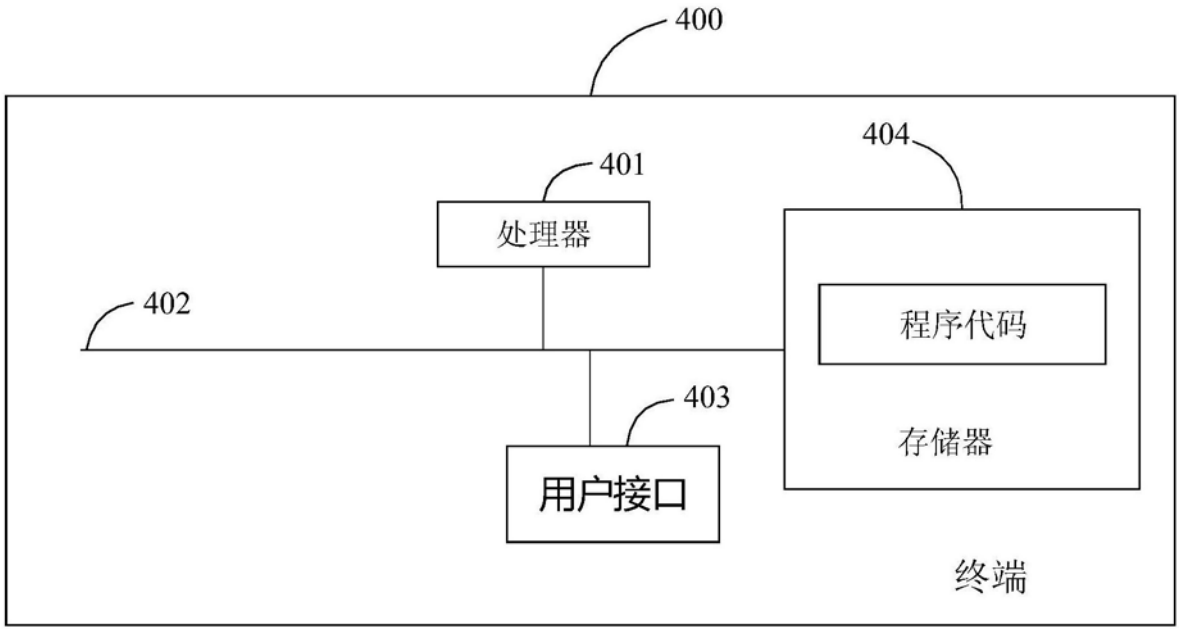

400
401
处理器
404
程序代码
402
403
用户接口
存储器
终端

图4

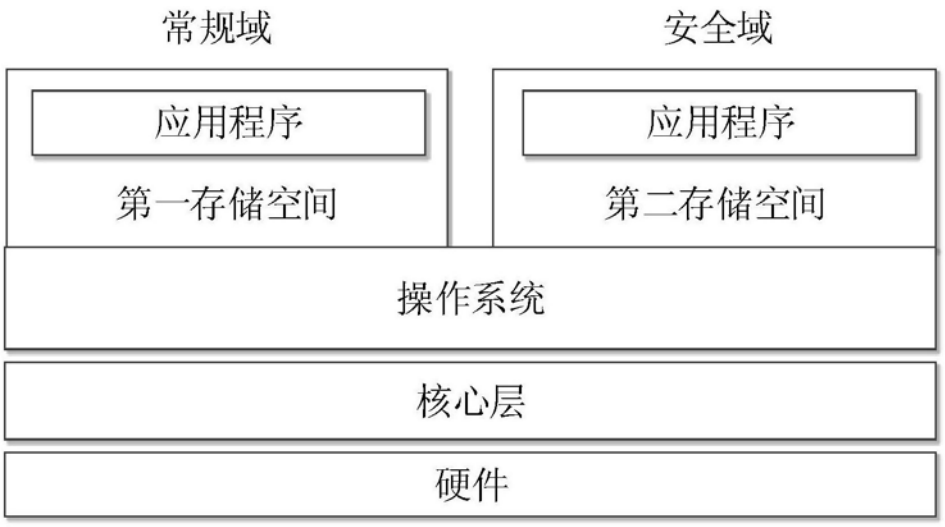


图5