

说明书

访问应用程序的方法及装置

本申请要求于 2012 年 4 月 26 日提交中国专利局、申请号为 201210126600.3、发明名称为“访问应用程序的方法及装置”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

本发明涉及信息安全技术领域，特别涉及一种访问应用程序的方法及装置。

背景技术

诸如手机、平板电脑或者 PDA（Personal Digital Assistant，个人数字助理）等用户设备作为现代人频繁用来进行信息交流或记事的工具，记录和存储了大量的个人信息，使其在人们的日常生活中扮演着越来越重要的角色。

通常情况下，用户设备所记录和存储的个人信息通常需要所预先安装的应用程序来呈现，如，用户的网络浏览记录需要运行所安装的浏览器客户端来呈现，用户的书籍阅读记录需要运行所安装的阅读器客户端来呈现，用户的游戏等级或者装备等信息需要运行相应的游戏程序客户端来呈现，等等。

现有技术中，自身未提供密码认证流程的应用程序（如浏览器、阅读器或者游戏程序等）可以被随意的打开，使得这类应用程序内的用户信息可能被恶意获取。

发明内容

为了解决现有技术的问题，本发明实施例提供了一种访问应用程序的方法及装置。所述技术方案如下：

一方面，本发明实施例提供了一种访问应用程序的方法，包括：

对用户设备上所安装的应用程序进行监控；

当监控到用户请求访问应用程序时，确定所请求访问的应用程序是否加

密；

当所请求访问的应用程序加密时，请求所述用户输入验证信息，并验证所述验证信息是否正确；

当所述验证信息正确时，运行所请求访问的应用程序，并呈现运行结果；
当所述验证信息错误时，执行对所请求访问的应用程序的保护操作。

5 所述对用户设备上所安装的应用程序进行监控之前，所述方法还包括：

确定应用程序与加密级别间对应关系，所述加密级别用于指示应用程序是否加密，包括未加密、加密、隐藏或者加密且隐藏。

当应用程序的加密级别为隐藏或者加密且隐藏时，隐藏所述应用程序的用户界面接口。

10 所述隐藏所述应用程序的用户界面接口之后，所述方法还包括：

接收用户发送的取消对所述应用程序隐藏的请求，请求用户输入密码，并验证所述密码；

当验证所述密码正确时，重新显示所隐藏的应用程序的用户界面接口。

所述确定所请求访问的应用程序是否加密包括：

15 根据所请求访问的应用程序查询应用程序与加密级别间对应关系，得到所请求访问的应用程序的加密级别，并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密。

所述当所述验证信息错误时，执行对所请求访问的应用程序的保护操作，包括：

20 提示所述用户重新输入验证信息，并返回执行验证所述验证信息是否正确的操作；

如果所述用户输入错误验证信息的次数达到预定值，则禁止运行所述应用程序，或者，输出提示信息，提示无法访问所述应用程序。

所述输出提示信息包括：

语音或者窗口通知所述用户所述应用程序出错。

25

另一方面，本发明实施例还提供了一种访问应用程序的装置，包括：监控模块、第一确定模块、验证模块、第一执行模块和第二执行模块；

所述监控模块，用于对用户设备上所安装的应用程序进行监控；

30 所述第一确定模块，用于当监控到用户请求访问应用程序时，确定所请求访问的应用程序是否加密；

所述验证模块，用于当所请求访问的应用程序加密时，请求所述用户输入

验证信息，并验证所述验证信息是否正确；

所述第一执行模块，用于当所述验证信息正确时，运行所请求访问的应用程序，并呈现运行结果；

5 所述第二执行模块，用于当所述验证信息错误时，执行对所请求访问的应用程序的保护操作。

所述装置还包括：第二确定模块，用于确定应用程序与加密级别间对应关系，所述加密级别用于指示应用程序是否加密，包括未加密、加密、隐藏或者加密且隐藏。

10 第三执行模块，用于当应用程序的加密级别为隐藏或者加密且隐藏时，隐藏所述应用程序的用户界面接口。

第四执行模块，用于接收用户发送的取消对所述应用程序隐藏的请求，请求用户输入密码，并验证所述密码，并当验证所述密码正确时，重新显示所隐藏的应用程序的用户界面接口。

15 所述第二确定模块，具体用于根据所请求访问的应用程序查询应用程序与加密级别间对应关系，得到所请求访问的应用程序的加密级别，并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密。

所述第二执行模块包括：

第一执行单元，用于提示所述用户重新输入验证信息，并返回执行验证所述验证信息是否正确的操作；

20 第二执行单元，用于如果所述用户输入错误验证信息的次数达到预定值，则禁止运行所述应用程序，或者，输出提示信息，提示无法访问所述应用程序。

所述第二执行单元，具体用于语音或者窗口通知所述用户所述应用程序出错。

25 另一方面，还提供了一种终端，所述终端包括：如上所述的访问应用程序的装置。

所述终端包括：手机、平板电脑或者个人数字助理 PDA。

30 本发明实施例提供的技术方案带来的有益效果是：通过当用户请求访问应用程序时，验证用户输入的验证信息，并在验证信息正确时，运行所请求访问的应用程序，并呈现运行结果，当验证信息错误时，执行对所请求访问的应用

程序的保护操作的技术方案的实现，可以有效的防止他人恶意的访问应用程序，从而可以有效保证应用程序内用户信息的安全。

附图说明

5 为了更清楚地说明本发明实施例中的技术方案，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，下面描述中的附图仅仅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。

图 1 是本发明实施例 1 中提供一种访问应用程序的方法流程图；

10 图 2 是本发明实施例 2 中提供一种访问应用程序的方法流程图；

图 3 是本发明实施例 3 中提供一种访问应用程序的装置结构示意图；

图 4 是本发明实施例 3 中提供一种访问应用程序的装置结构示意图；

图 5 是本发明实施例 3 中提供一种访问应用程序的装置结构示意图。

15 具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

实施例 1

参见图 1，一种访问应用程序的方法，包括：

20 步骤 101：对用户设备上所安装的应用程序进行监控；

步骤 102：当监控到用户请求访问应用程序时，确定所请求访问的应用程序是否加密；

步骤 103：当所请求访问的应用程序加密时，请求所述用户输入验证信息，并验证所述验证信息是否正确；

25 步骤 104：当所述验证信息正确时，运行所请求访问的应用程序，并呈现运行结果；

步骤 105：当所述验证信息错误时，执行对所请求访问的应用程序的保护操作。

30 本发明实施例提供的技术方案带来的有益效果是：通过当用户请求访问应用程序时，验证用户输入的验证信息，并在验证信息正确时，运行所请求访问的应用程序，并呈现运行结果，当验证信息错误时，执行对所请求访问的应用

程序的保护操作的技术方案的实现，可以有效的防止他人恶意的访问应用程序，从而可以有效保证应用程序内用户信息的安全。

实施例 2

参见图 2，一种访问应用程序的方法，该方法的执行主体为用户设备，更进一步地，该方法可以由安装在用户设备上的客户端应用程序（如程序锁）实现，其中，该用户设备可以包括但不限于手机、平板电脑或者 PDA（Personal Digital Assistant，个人数字助理）等设备，具体包括如下内容：

步骤 201：确定应用程序与加密级别间对应关系，并保存所述对应关系，其中，所述加密级别用于指示应用程序是否加密，具体可以包括：未加密、加密、隐藏或者加密且隐藏；

本步骤具体实现时可以包括：

接收用户发送的访问程序锁的请求，其中，所述程序锁用于管理用户设备上所安装的应用程序，具体可以包括应用程序加密级别的设置管理等；

本发明实施例中，程序锁可以以快捷图标或者文件夹的形式显示在用户设备上，用户可以通过点击所述快捷图标或者文件夹向用户设备发送访问程序锁的请求；

运行所述程序锁，显示应用程序列表及加密级别设置模版，其中，所述加密级别设置模板提供有应用程序的加密级别，用户便可以通过所显示的应用程序列表及加密级别设置模板来选择设置应用程序的加密级别；

接收用户发送的加密设置请求，所述加密设置请求包括应用程序标识及加密级别；

当接收到的加密级别为加密时，加密所述应用程序标识所标识的应用程序，具体地，请求用户输入所述应用程序标识所标识应用程序的验证信息，接收用户输入的验证信息，并保存所述应用程序标识与验证信息间对应关系，完成对所述应用程序标识所标识应用程序的加密；其中，所述验证信息可以包括：加密密码和用户名中的一个或者全部。

本发明实施例中，可以采用统一的加密密码对加密级别为加密的应用程序进行加密；

本发明实施例通过加密应用程序的实现，达到保护应用程序的目的，避免应用程序被恶意访问。

当接收到的加密级别为隐藏时，隐藏所述应用程序标识所对应的应用程

序，具体地，隐藏所述应用程序标识所标识应用程序的用户界面接口，其中，所述用户界面接口可以是快捷图标或者文件夹；

本发明实施例通过隐藏应用程序的用户界面接口的实现，达到隐藏应用程序的目的，以便非法用户无法查找得到应用程序，避免应用程序被恶意访问，
5 一定程度上保证了应用程序内用户信息的安全性。

当接收到的加密级别为加密且隐藏时，加密并同时隐藏所述应用程序标识所标识的应用程序，具体的加密及隐藏过程参见以上有关加密及隐藏应用程序的描述，此处就不再赘述。

本发明实施例还可以通过加密及隐藏应用程序的实现，达到加密及隐藏
10 双重保护应用程序的目的，提高应用程序被访问的安全性。

通过上述方式可以完成对应用程序的加密级别的设置，之后，本地存储应用程序与其加密级别间对应关系。

步骤 202：对用户设备上所安装的应用程序进行监控；

步骤 203：当监控到用户请求访问应用程序时，确定所请求访问的应用程
15 序是否加密，

当所请求访问的应用程序加密时，执行步骤 204；

当所请求访问的应用程序未加密时，运行所请求访问的应用程序，并呈现运行结果；

本发明实施例在具体实现时，用户可以通过用户设备上所显示的应用程序
20 的用户界面接口来请求访问应用程序；

进一步地，当应用程序的用户界面接口隐藏时，用户通过程序锁来发送取消对应用程序隐藏的请求，当接收到用户发送的取消对应用程序隐藏的请求时，请求用户输入密码，并验证所输入的密码；当验证所述密码正确时，重新显示所隐藏的应用程序的用户界面接口，这样，用户便可以通过所显示的应用
25 程序的用户界面接口来请求访问应用程序。

其中，确定所请求访问的应用程序是否加密可以包括：根据所请求访问的应用程序查询应用程序与加密级别间对应关系，得到所请求访问的应用程序的加密级别，并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密，当所请求访问的应用程序的加密级别为未加密、隐藏时，则所请
30 求访问的应用程序没有加密，当所请求访问的应用程序的加密级别为加密或者加密且隐藏时，则所请求访问的应用程序加密。

步骤 204: 请求用户输入验证信息;

例如, 当用户点击用户设备上应用程序的用户界面接口时, 用户设备的界面上将弹出输入验证信息的窗口, 请求用户输入验证信息, 其中, 该弹出的窗口提供有信息输入接口, 用户便可以在弹出的窗口中输入验证信息。

5 步骤 205: 验证所输入的验证信息是否正确,

当所述验证信息正确时, 执行步骤 206;

当所述验证信息错误时, 执行步骤 207;

本发明实施例中, 用户设备预存储有正确的验证信息, 当接收到用户输入的验证信息时, 将用户输入的验证信息与预存的验证信息进行比对, 当用户输入
10 的验证信息与预存的验证相同时, 则验证用户输入的验证信息成功, 当用户输入的验证信息与预存的验证信息不相同, 则验证用户输入的验证信息错误。

步骤 206: 运行所请求访问的应用程序, 并呈现运行结果;

步骤 207: 执行对所请求访问的应用程序的保护操作;

15 提示所述用户重新输入验证信息, 并返回执行验证所述验证信息是否正确的操作;

如果所述用户输入错误验证信息的次数达到预定值, 则禁止运行所述应用程序, 或者, 输出提示信息, 提示无法访问所述应用程序。

其中, 输出提示信息包括:

20 语音或者窗口通知所述用户所述应用程序出错。

本发明实施例所述的应用程序可以包括存储用户隐私信息的存储空间, 其中, 用户隐私信息可以包括短消息、通话记录、邮件、图片或者视频等信息。

本发明实施例提供的技术方案带来的有益效果是: 通过当用户请求访问应用程序时, 验证用户输入的验证信息, 并在验证信息正确时, 运行所请求访问
25 的应用程序, 并呈现运行结果, 当验证信息错误时, 执行对所请求访问的应用程序的保护操作的技术方案的实现, 可以有效的防止他人恶意的访问应用程序, 从而可以有效保证应用程序内用户信息的安全。

实施例 3

参见图 3, 一种访问应用程序的装置, 包括: 监控模块 301、第一确定模块 302、验证模块 303、第一执行模块 304 和第二执行模块 305;

监控模块 301, 用于对用户设备上所安装的应用程序进行监控;

第一确定模块 302, 用于当监控到用户请求访问应用程序时, 确定所请求访问的应用程序是否加密;

验证模块 303, 用于当所请求访问的应用程序加密时, 请求所述用户输入验证信息, 并验证所述验证信息是否正确;

5 第一执行模块 304, 用于当所述验证信息正确时, 运行所请求访问的应用程序, 并呈现运行结果;

第二执行模块 305, 用于当所述验证信息错误时, 执行对所请求访问的应用程序的保护操作。

参见图 4, 本发明实施例如图 3 所示的第二执行模块 305 包括:

10 第一执行单元 3051, 用于提示所述用户重新输入验证信息, 并返回执行验证所述验证信息是否正确的操作;

第二执行单元 3052, 用于如果所述用户输入错误验证信息的次数达到预定值, 则禁止运行所述应用程序, 或者, 输出提示信息, 提示无法访问所述应用程序。

15 本发明实施例中, 第二执行单元 3052, 具体用于语音或者窗口通知所述用户所述应用程序出错。

更进一步地, 参见图 5, 本发明实施例如图 3 所示的装置还包括:

第二确定模块 306, 用于确定应用程序与加密级别间对应关系, 所述加密级别用于指示应用程序是否加密, 包括未加密、加密、隐藏或者加密且隐藏。

20 第三执行模块 307, 用于当应用程序的加密级别为隐藏或者加密且隐藏时, 隐藏所述应用程序的用户界面接口。

第四执行模块 308, 用于接收用户发送的取消对所述应用程序隐藏的请求, 请求用户输入密码, 并验证所述密码, 并当验证所述密码正确时, 显示所隐藏的应用程序。

25 本发明实施例中, 第二确定模块 306, 具体用于根据所请求访问的应用程序查询应用程序与加密级别间对应关系, 得到所请求访问的应用程序的加密级别, 并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密。

30 另一方面, 本实施例中还提供了一种终端, 所述终端包括: 如上所述的访问应用程序的装置。

可选地, 所述终端包括但不限于: 手机、平板电脑或者个人数字助理 PDA

等。

本发明实施例提供的技术方案带来的有益效果是：通过当用户请求访问应用程序时，验证用户输入的验证信息，并在验证信息正确时，运行所请求访问的应用程序，并呈现运行结果，当验证信息错误时，执行对所请求访问的应用程序的5 保护操作的技术方案的实现，可以有效的防止他人恶意的访问应用程序，从而可以有效保证应用程序内用户信息的安全。

需要说明的是：上述实施例提供的访问应用程序的装置在访问应用程序时，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10 能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的访问应用程序的装置与访问应用程序的方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过15 过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的20 保护范围之内。

权 利 要 求 书

1、一种访问应用程序的方法，其特征在于，所述方法包括：

对用户设备上所安装的应用程序进行监控；

5 当监控到用户请求访问应用程序时，确定所请求访问的应用程序是否加密；
 当所请求访问的应用程序加密时，请求所述用户输入验证信息，并验证所述验证信息是否正确；

 当所述验证信息正确时，运行所请求访问的应用程序，并呈现运行结果；

 当所述验证信息错误时，执行对所请求访问的应用程序的保护操作。

10

2、根据权利要求1所述的方法，其特征在于，所述对用户设备上所安装的应用程序进行监控之前，所述方法还包括：

 确定应用程序与加密级别间对应关系，所述加密级别用于指示应用程序是否加密，包括未加密、加密、隐藏或者加密且隐藏。

15 当所述应用程序的加密级别为隐藏或者加密且隐藏时，隐藏所述应用程序的用户界面接口。

3、根据权利要求2所述的方法，其特征在于，所述隐藏所述应用程序的用户界面接口之后，所述方法还包括：

20 接收用户发送的取消对所述应用程序隐藏的请求，请求所述用户输入密码，并验证所述密码；

 当验证所述密码正确时，重新显示所隐藏的应用程序的用户界面接口。

4、根据权利要求1所述的方法，其特征在于，所述确定所请求访问的应用程序是否加密包括：

25 根据所请求访问的应用程序查询应用程序与加密级别间对应关系，得到所请求访问的应用程序的加密级别，并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密。

30 5、根据权利要求1所述的方法，其特征在于，所述当所述验证信息错误时，执行对所请求访问的应用程序的保护操作，包括：

提示所述用户重新输入验证信息，并返回执行验证所述验证信息是否正确的操作；

如果所述用户输入错误验证信息的次数达到预定值，则禁止运行所述应用程序，或者，输出提示信息，提示无法访问所述应用程序。

5

6、根据权利要求5所述的方法，其特征在于，所述输出提示信息包括：语音或者窗口通知所述用户所述应用程序出错。

7、一种访问应用程序的装置，其特征在于，所述装置包括：监控模块、第一确定模块、验证模块、第一执行模块和第二执行模块；

所述监控模块，用于对用户设备上所安装的应用程序进行监控；

所述第一确定模块，用于当监控到用户请求访问应用程序时，确定所请求访问的应用程序是否加密；

所述验证模块，用于当所请求访问的应用程序加密时，请求所述用户输入验证信息，并验证所述验证信息是否正确；

所述第一执行模块，用于当所述验证信息正确时，运行所请求访问的应用程序，并呈现运行结果；

所述第二执行模块，用于当所述验证信息错误时，执行对所请求访问的应用程序的保护操作。

20

8、根据权利要求7所述的装置，其特征在于，所述装置还包括：

第二确定模块，用于确定应用程序与加密级别间对应关系，所述加密级别用于指示应用程序是否加密，包括未加密、加密、隐藏或者加密且隐藏。

第三执行模块，用于当所述应用程序的加密级别为隐藏或者加密且隐藏时，隐藏所述应用程序的用户界面接口。

25

9、根据权利要求8所述的装置，其特征在于，所述装置还包括：

第四执行模块，用于接收用户发送的取消对所述应用程序隐藏的请求，请求所述用户输入密码，并验证所述密码，并当验证所述密码正确时，重新显示所隐藏的应用程序的用户界面接口。

30

10、根据权利要求 7 所述的装置，其特征在于，所述第二确定模块，具体用于根据所请求访问的应用程序查询应用程序与加密级别间对应关系，得到所请求访问的应用程序的加密级别，并根据所请求访问的应用程序的加密级别确定所请求访问的应用程序是否加密。

5

11、根据权利要求 7 所述的装置，其特征在于，所述第二执行模块包括：

第一执行单元，用于提示所述用户重新输入验证信息，并返回执行验证所述验证信息是否正确的操作；

第二执行单元，用于如果所述用户输入错误验证信息的次数达到预定值，
10 则禁止运行所述应用程序，或者，输出提示信息，提示无法访问所述应用程序。

12、根据权利要求 11 所述的装置，其特征在于，所述第二执行单元，具体用于语音或者窗口通知所述用户所述应用程序出错。

15 13、一种终端，其特征在于，所述终端包括：如权利要求 7-12 任一项所述的访问应用程序的装置。

14、根据权利要求 13 所述的终端，其特征在于，所述终端包括：手机、平板电脑或者个人数字助理 PDA。

20