(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105956487 A
(43)申请公布日 2016.09.21

(21)申请号 201610282530.9

(22)申请日 2016.04.29

(71)申请人 乐视控股(北京)有限公司
地址 100025 北京市朝阳区姚家园路105号3号楼10层1102
申请人 乐视移动智能信息技术(北京)有限公司

(72)发明人 许帅群

(74)专利代理机构 北京市惠诚律师事务所 11353
代理人 刘子敬

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 11/14(2006.01)

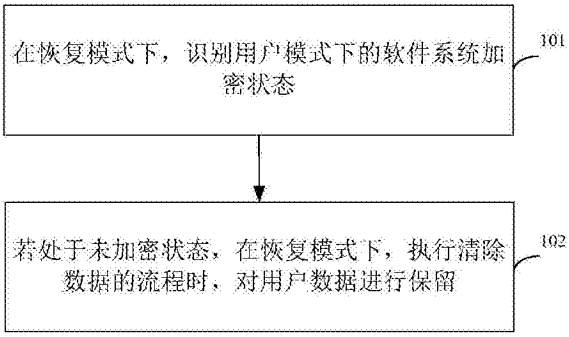
权利要求书1页 说明书4页 附图2页

(54)发明名称

数据清除方法和装置

(57)摘要

本发明实施例提供了一种数据清除方法和装置，通过在恢复模式下，识别用户模式下的软件系统加密状态，若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留，从而用户无需预先对所需保留的用户数据进行拷贝，解决了现有技术中由于在进行数据清除时是对全部的用户数据进行删除所导致的用户需要预先拷贝用户数据，操作不便捷的技术问题。同时，由于仅在用户模式下为未加密状态时，才保留用户数据，也就是说，当用户数据为无需进行加密的常规数据时，对用户数据进行保留，若用户数据为敏感数据依旧采用安全性较高的全部清除以避免外泄的处理方式，降低了敏感的用户数据外泄的风险性。



CN 105956487 A

1.一种数据清除方法,其特征在于,包括:

在恢复模式下,识别用户模式下的软件系统加密状态;

若处于未加密状态,在恢复模式下,执行清除数据的流程时,对用户数据进行保留。

2.根据权利要求1所述的数据清除方法,其特征在于,所述识别用户模式下的软件系统加密状态包括:

在恢复模式下,读取预设状态位;其中,所述预设状态位是用户模式下设置所述软件系统的加密状态时所写入的,用于指示用户模式下所述软件系统的加密状态;

根据所读取的预设状态位,确定用户模式下的所述软件系统加密状态。

3.根据权利要求1所述的数据清除方法,其特征在于,所述识别用户模式下的软件系统加密状态包括:

在恢复模式下,访问用户数据;

若访问成功,确定用户模式下的所述软件系统加密状态为未加密;

若访问失败,确定用户模式下的所述软件系统加密状态为已加密。

4.根据权利要求1-3任一项所述的数据清除方法,其特征在于,所述识别用户模式下的软件系统加密状态之后,还包括:

若处于已加密状态,在恢复模式下,执行清除数据的流程时,对外接存储设备中的用户数据进行清除。

5.根据权利要求1-3任一项所述的数据清除方法,其特征在于,所述用户数据存储于外接存储设备中。

6.一种数据清除装置,其特征在于,包括:

识别模块,用于在恢复模式下,识别用户模式下的软件系统加密状态;

保留模块,用于若处于未加密状态,在恢复模式下,执行清除数据的流程时,对用户数据进行保留。

7.根据权利要求6所述的数据清除装置,其特征在于,所述识别模块,包括:

读取单元,用于在恢复模式下,读取预设状态位;其中,所述预设状态位是用户模式下设置所述软件系统的加密状态时所写入的,用于指示用户模式下所述软件系统的加密状态;

确定单元,用于根据所读取的预设状态位,确定用户模式下的所述软件系统加密状态。

8.根据权利要求7所述的数据清除装置,其特征在于,所述识别模块,包括:

访问单元,用于在恢复模式下,访问用户数据;

处理单元,用于若访问成功,确定用户模式下的所述软件系统加密状态为未加密;若访问失败,确定用户模式下的所述软件系统加密状态为已加密。

9.根据权利要求6-8任一项所述的数据清除装置,其特征在于,所述装置,还包括:

清除模块,用于若处于已加密状态,在恢复模式下,执行清除数据的流程时,对外接存储设备中的用户数据进行清除。

10.根据权利要求6-8任一项所述的数据清除装置,其特征在于,所述用户数据存储于外接存储设备中。

数据清除方法和装置

技术领域

[0001] 本发明涉及信息技术，尤其涉及一种数据清除方法和装置。

背景技术

[0002] 在移动终端的软件系统中，例如安卓系统，恢复(Recovery)模式指的是一种可以对移动终端内部的数据或系统进行修改的模式。在这个模式下可以写入新的软件系统，或者对已有的软件系统进行备份或升级，也可以进行恢复出厂设置。对于移动终端的软件系统来说，在恢复模式下能够实现软件系统升级和数据清除的功能。

[0003] 发明人在实现本发明的过程中，发现现有技术存在如下缺陷：

[0004] 在进行数据清除时是对全部的用户数据进行删除，从而用户需要将需要保留的用户数据预先进行备份，例如对通信录、照片等文件进行拷贝操作不够便捷。

发明内容

[0005] 本发明提供一种数据清除方法和装置，用于解决现有技术中由于在进行数据清除时是对全部的用户数据进行删除所导致的用户需要预先拷贝用户数据，操作不便捷的技术问题。

[0006] 为达到上述目的，本发明的实施例采用如下技术方案：

[0007] 第一方面，提供了一种数据清除方法，包括：

[0008] 在恢复模式下，识别用户模式下的软件系统加密状态；

[0009] 若处于未加密状态，在恢复模式下，执行清除数据的流程时，对外接存储设备中的用户数据进行保留。

[0010] 第二方面，提供了一种数据清除装置，包括：

[0011] 识别模块，用于在恢复模式下，识别用户模式下的软件系统加密状态；

[0012] 保留模块，用于若处于未加密状态，在恢复模式下，执行清除数据的流程时，对外接存储设备中的用户数据进行保留。

[0013] 本发明实施例提供的数据清除方法和装置，通过在恢复模式下，识别用户模式下的软件系统加密状态，若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留，从而用户无需预先对所需保留的用户数据进行拷贝，解决了现有技术中由于在进行数据清除时是对全部的用户数据进行删除所导致的用户需要预先拷贝用户数据，操作不便捷的技术问题。同时，由于仅在用户模式下为未加密状态时，才保留用户数据，也就是说，当用户数据为无需进行加密的常规数据时，对用户数据进行保留，若用户数据为敏感数据依旧采用安全性较高的全部清除以避免外泄的处理方式，降低了敏感的用户数据外泄的风险性。

[0014] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0015] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0016] 图1为本发明实施例一提供的一种数据清除方法的流程示意图；

[0017] 图2为本发明实施例二提供的一种数据清除装置的结构示意图；

[0018] 图3为本发明实施例三提供的一种数据清除装置的结构示意图；

[0019] 图4为本发明实施例三提供的另一种数据清除装置的结构示意图；

[0020] 图5为本发明实施例三提供的又一种数据清除装置的结构示意图。

具体实施方式

[0021] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0022] 下面结合附图对本发明实施例提供的数据清除方法和装置进行详细描述。

[0023] 实施例一

[0024] 图1为本发明实施例一提供的一种数据清除方法的流程示意图，如图1所示，本实施例所提供的方法可以由移动终端执行，方法包括：

[0025] 步骤101、在恢复模式下，识别用户模式下的软件系统加密状态。

[0026] 具体的，软件系统具有用户模式和恢复模式，下面分别对两种模式进行简要的介绍。

[0027] 其中，用户模式指的是一种用于用户通常情况下，使用移动终端的模式，用户模式具有两种加密状态，一种为加密状态，另一种为非加密状态。在加密状态下，需要首先进行解密，才能够访问用户数据；另一种为非加密状态，无需解密，便可以访问用户数据。通常情况下，若用户数据涉及较为敏感的信息，则可以将用户模式设置为已加密状态。相反的，若用户数据为一般信息，无需进行加密，则可以将用户模式设置为未加密状态，从而节省加解密所带来的运行开销，提高运行速度。

[0028] 恢复模式指的是一种可以对安卓机内部的数据或系统进行修改的模式。在这个模式下我们可以写入新的安卓系统，或者对已有的系统进行备份或升级，也可以进行恢复出厂设置以及数据清除等。

[0029] 作为一种可能的实现方式，在恢复模式下，读取预设状态位，其中，预设状态位是用户模式下设置软件系统的加密状态时所写入的，用于指示用户模式下所述软件系统的加密状态。具体来说，用户模式下，可以对软件系统是否进行加密进行设置，在对加密状态设置完成之后，在预设状态位写入用于指示是否加密的值，进而在恢复模式下，通过对该预设状态位进行读取，根据该用于指示是否加密的值确定用户模式是否进行了加密。

[0030] 作为另一种可能的实现方式，在恢复模式下，访问用户数据，若访问成功，确定用户模式下的软件系统加密状态为未加密，若访问失败，确定用户模式下的软件系统加密状

态为已加密。这是由于当用户模式处于加密状态下时，恢复模式下的进程是不能够直接读取用户数据的，必须对其进行解密后才能够对用户数据进行访问，因而可以据此确定用户模式下的软件系统加密状态。

[0031] 步骤102、若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留。

[0032] 具体的，根据加密状态，对用户数据进行保留。若处于未加密状态，在恢复模式下，执行清除数据的流程时，对外接存储设备中的用户数据进行保留。

[0033] 进一步，若处于已加密状态，在恢复模式下，执行清除数据的流程时，对外接存储设备中的用户数据进行清除。

[0034] 其中，外接存储设备可以为安全数码卡(Secure Digital Memory Card,SD卡)。

[0035] 通过在恢复模式下，识别用户模式下的软件系统加密状态，若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留，从而用户无需预先对所需保留的用户数据进行拷贝，解决了现有技术中由于在进行数据清除时是对全部的用户数据进行删除所导致的用户需要预先拷贝用户数据，操作不便捷的技术问题。

[0036] 同时，由于仅在用户模式下为未加密状态时，才保留用户数据，也就是说，当用户数据为无需进行加密的常规数据时，对用户数据进行保留，若用户数据为敏感数据依旧采用安全性较高的全部清除以避免外泄的处理方式，降低了敏感的用户数据外泄的风险性。

[0037] 因此，本发明实施例所提供的方法，在保证了用户操作便捷性的同时，提高了用户数据的安全性。

[0038] 实施例二

[0039] 图2为本发明实施例二提供的一种数据清除装置的结构示意图，本实施例所提供的数据清除装置可以设置于移动终端中，如图2所示，该装置包括：识别模块31和保留模块32。

[0040] 识别模块31，用于在恢复模式下，识别用户模式下的软件系统加密状态。

[0041] 保留模块32，用于若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留。

[0042] 本实施例所提供的装置通过识别模块31在恢复模式下，识别用户模式下的软件系统加密状态，若处于未加密状态，在恢复模式下，执行清除数据的流程时，保留模块32对用户数据进行保留，从而用户无需预先对所需保留的用户数据进行拷贝，解决了现有技术中由于在进行数据清除时是对全部的用户数据进行删除所导致的用户需要预先拷贝用户数据，操作不便捷的技术问题。

[0043] 同时，由于保留模块32仅在用户模式下为未加密状态时，才保留用户数据，也就是说，当用户数据为无需进行加密的常规数据时，对用户数据进行保留，若用户数据为敏感数据依旧采用安全性较高的全部清除以避免外泄的处理方式，降低了敏感的用户数据外泄的风险性。

[0044] 因此，本发明实施例所提供的装置，在保证了用户操作便捷性的同时，提高了用户数据的安全性。

[0045] 实施例三

[0046] 图3为本发明实施例三提供的一种数据清除装置的结构示意图，如图3所示，在图2

所提供的数据清除装置的基础上，该装置进一步包括：清除模块33。

[0047] 清除模块33，用于若处于已加密状态，在恢复模式下，执行清除数据的流程时，对外接存储设备中的用户数据进行清除。

[0048] 进一步，为了清楚说明本实施例所提供的数据清除装置，本实施例中提供了数据清除装置的两种可能的实现方式。

[0049] 作为一种可能的实现方式，图4为本发明实施例三提供的另一种数据清除装置的结构示意图，如图4所示，在图3的基础上，识别模块31，进一步包括：读取单元311和确定单元312。

[0050] 读取单元311，用于在恢复模式下，读取预设状态位。

[0051] 其中，预设状态位是用户模式下设置所述软件系统的加密状态时所写入的，用于指示用户模式下所述软件系统的加密状态。

[0052] 确定单元312，用于根据所读取的预设状态位，确定用户模式下的所述软件系统加密状态。

[0053] 作为另一种可能的实现方式，图5为本发明实施例三提供的又一种数据清除装置的结构示意图，如图5所示，在图3的基础上，识别模块31，进一步包括：访问单元313和处理单元314。

[0054] 访问单元313，用于在恢复模式下，访问用户数据。

[0055] 处理单元314，用于若访问成功，确定用户模式下的所述软件系统加密状态为未加密；若访问失败，确定用户模式下的所述软件系统加密状态为已加密。

[0056] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0057] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

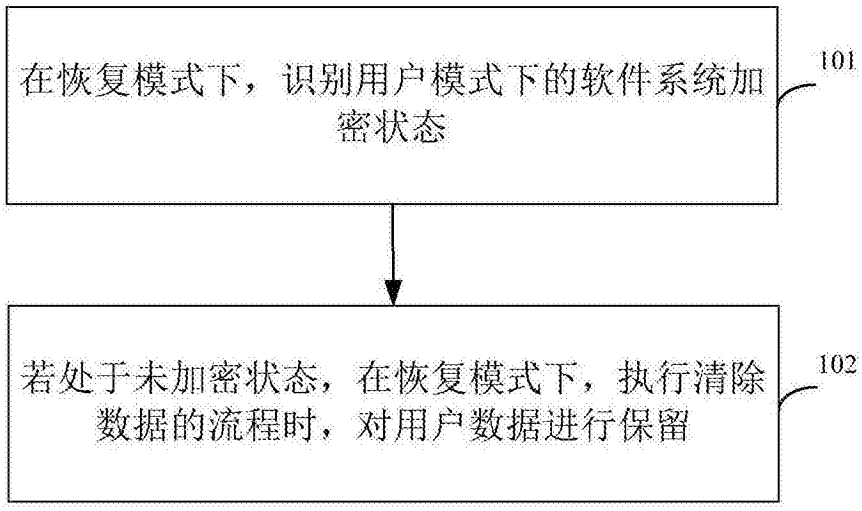

在恢复模式下，识别用户模式下的软件系统加密状态
101
若处于未加密状态，在恢复模式下，执行清除数据的流程时，对用户数据进行保留
102

图1

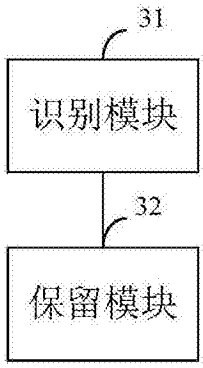

31
识别模块
32
保留模块

图2

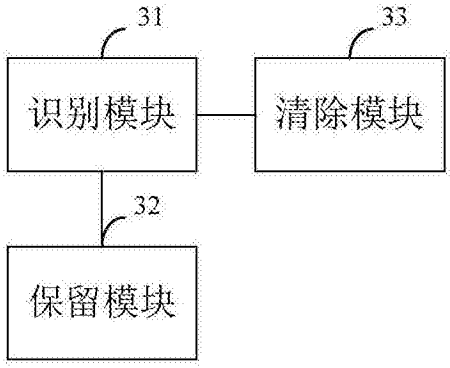

31
识别模块
33
清除模块
32
保留模块

图3

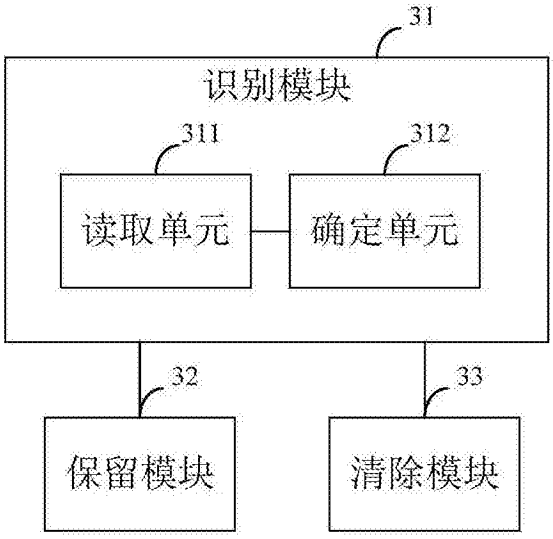

31
识别模块
311
读取单元
312
确定单元
32
保留模块
33
清除模块

图4

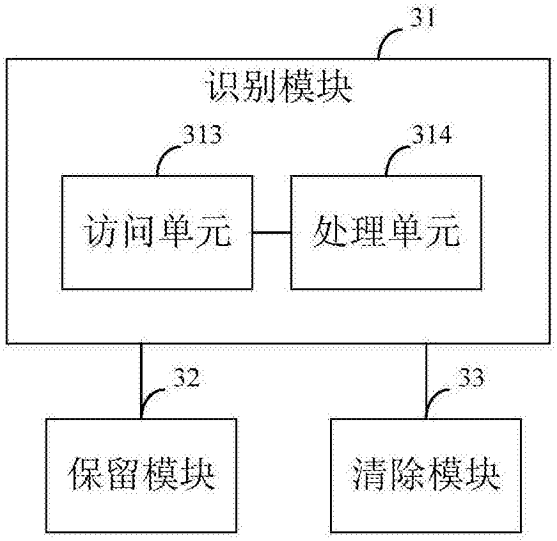


图5