



# (12)发明专利申请

(10)申请公布号 CN 107895116 A

(43)申请公布日 2018.04.10

(21)申请号 201711230899.6

(22)申请日 2017.11.29

(71)申请人 山东渔翁信息技术股份有限公司  
地址 264200 山东省威海市高区初村镇初  
河北路-12-1号

(72)发明人 宋志华 徐波

(74)专利代理机构 北京超凡志成知识产权代理  
事务所(普通合伙) 11371  
代理人 逯恒

(51)Int.Cl.

G06F 21/53(2013.01)

G06F 21/60(2013.01)

G06F 21/62(2013.01)

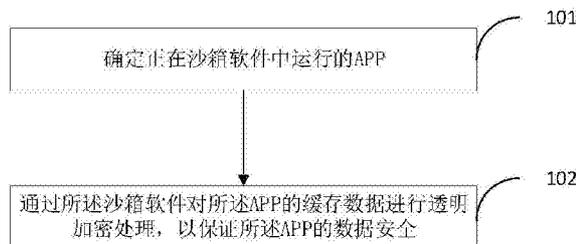
权利要求书1页 说明书6页 附图3页

## (54)发明名称

APP数据保护方法、设备、移动终端及计算机  
可读存储介质

## (57)摘要

本发明实施例提出了APP数据保护方法、设备、移动终端及计算机可读存储介质,其中,该方法包括:确定正在沙箱软件中运行的APP;通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。以此通过沙箱软件构建一个独立的运行环境,且通过沙箱软件对经过APP的数据进行加密处理,从而提高了数据的安全性,提高了用户的使用体验。



1. 一种APP数据保护方法,其特征在于,包括:  
确定正在沙箱软件中运行的APP;  
通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。
2. 根据权利要求1所述的一种APP数据保护方法,其特征在于,还包括:  
当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;  
展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。
3. 根据权利要求2所述的一种APP数据保护方法,其特征在于,所述“确定正在沙箱软件中运行的APP”包括:  
在所述运行界面获取运行APP的指令;  
基于所述指令确定所运行的APP。
4. 如权利要求2所述的一种APP数据保护方法,其特征在于,还包括:  
获取用户的账户信息;  
对所述账户信息进行验证;  
若验证通过,则授予所述用户执行权限,其中所述执行权限不低于运行所述沙箱软件,以及在所述沙箱软件的运行界面运行APP所需要的权限。
5. 如权利要求1所述的一种APP数据保护方法,其特征在于,还包括:  
当接收到用于关闭所述APP的指令时,基于所述指令清除所保存的缓存数据。
6. 一种APP数据保护设备,其特征在于,包括:  
确定模块,用于确定正在沙箱软件中运行的APP;  
保护模块,用于通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。
7. 根据权利要求6所述的一种APP数据保护设备,其特征在于,还包括:  
展示模块,用于当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;  
展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。
8. 根据权利要求7所述的一种APP数据保护设备,其特征在于,所述确定模块,用于:  
在所述运行界面获取运行APP的指令;  
基于所述指令确定所运行的APP。
9. 一种移动终端,其特征在于,包括存储器和处理器,所述存储器用于存储计算机程序,所述处理器运行所述计算机程序以使所述移动终端执行根据权利要求1至5中任一项所述的内容推荐方法。
10. 一种计算机可读存储介质,其特征在于,其存储有权利要求9所述的移动终端中所使用的计算机程序。

## APP数据保护方法、设备、移动终端及计算机可读存储介质

### 技术领域

[0001] 本发明涉及数据保护的技术领域,具体而言,涉及APP数据保护方法、设备、移动终端及计算机可读存储介质。

### 背景技术

[0002] 目前随着移动终端,例如手机平板等的迅速发展,人们使用手机上的APP(Application,应用程序)的频率越来越高,且各种APP的数量也呈现爆发式的增长,APP的使用越来越与人们的生活工作息息相关,导致在使用APP时会有大量的个人数据,而目前在使用APP时,非常容易导致个人数据被窃取,导致个人隐私被侵犯,进而导致用户的使用体验不够好。

[0003] 由此,目前需要一种可以有效保护APP的数据的方法。

### 发明内容

[0004] 有鉴于此,本发明提出了APP数据保护方法、设备、移动终端及计算机可读存储介质,通过沙箱软件构建一个独立的运行环境,且通过沙箱软件对经过APP的数据进行加密处理,从而提高了数据的安全性,提高了用户的使用体验。

[0005] 具体的,本发明提出了以下具体的实施例:

[0006] 本发明实施例提出了一种APP数据保护方法,包括:

[0007] 确定正在沙箱软件中运行的APP;

[0008] 通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。

[0009] 在一个具体的实施例中,该方法还包括:

[0010] 当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;

[0011] 展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。

[0012] 在一个具体的实施例中,所述“确定正在沙箱软件中运行的APP”包括:

[0013] 在所述运行界面获取运行APP的指令;

[0014] 基于所述指令确定所运行的APP。

[0015] 在一个具体的实施例中,该方法还包括:

[0016] 获取用户的账户信息;

[0017] 对所述账户信息进行验证;

[0018] 若验证通过,则授予所述用户执行权限,其中所述执行权限不低于运行所述沙箱软件,以及在所述沙箱软件的运行界面运行APP所需要的权限。

[0019] 在一个具体的实施例中,该方法还包括:

[0020] 当接收到用于关闭所述APP的指令时,基于所述指令清除所保存的缓存数据。

- [0021] 本发明实施例还提出了一种APP数据保护设备,包括:
- [0022] 确定模块,用于确定正在沙箱软件中运行的APP;
- [0023] 保护模块,用于通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。
- [0024] 在一个具体的实施例中,该设备还包括:
- [0025] 展示模块,用于当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;
- [0026] 展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。
- [0027] 在一个具体的实施例中,所述确定模块,用于:
- [0028] 在所述运行界面获取运行APP的指令;
- [0029] 基于所述指令确定所运行的APP。
- [0030] 在一个具体的实施例中,该设备还包括:
- [0031] 验证模块,用于获取用户的账户信息;
- [0032] 对所述账户信息进行验证;
- [0033] 若验证通过,则授予所述用户执行权限,其中所述执行权限不低于运行所述沙箱软件,以及在所述沙箱软件的运行界面运行APP所需要的权限。
- [0034] 在一个具体的实施例中,该设备还包括:
- [0035] 清除模块,用于当接收到用于关闭所述APP的指令时,基于所述指令清除所保存的缓存数据。
- [0036] 本发明实施例还提出了一种移动终端,包括存储器和处理器,所述存储器用于存储计算机程序,所述处理器运行所述计算机程序以使所述移动终端执行根据上述任一方法项所述的步骤。
- [0037] 本发明实施例还提出了一种计算机可读存储介质,其存储有上述的移动终端中所使用的计算机程序。
- [0038] 以此,本发明实施例提出了APP数据保护方法、设备、移动终端及计算机可读存储介质,其中,该方法包括:确定正在沙箱软件中运行的APP;通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。以此通过沙箱软件构建一个独立的运行环境,且通过沙箱软件对经过APP的数据进行加密处理,从而提高了数据的安全性,提高了用户的使用体验。

## 附图说明

[0039] 为了更清楚地说明本发明实施例的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本发明的某些实施例,因此不应被看作是对范围的限定,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相关的附图。

- [0040] 图1为本发明的一个实施例提出的一种APP数据保护方法的流程示意图;
- [0041] 图2为本发明的一个实施例提出的一种APP数据保护方法的流程示意图;
- [0042] 图3为本发明的一个实施例提出的一种APP数据保护设备的结构示意图;

- [0043] 图4为本发明的一个实施例提出的一种APP数据保护设备的结构示意图；  
[0044] 图5为本发明的一个实施例提出的一种APP数据保护设备的结构示意图；  
[0045] 图6为本发明的一个实施例提出的一种APP数据保护设备的结构示意图。

### 具体实施方式

[0046] 在下文中,将更全面地描述本公开的各种实施例。本公开可具有各种实施例,并且可在其中做出调整和改变。然而,应理解:不存在将本公开的各种实施例限于在此公开的特定实施例的意图,而是应将本公开理解为涵盖落入本公开的各种实施例的精神和范围内的所有调整、等同物和/或可选方案。

[0047] 在本公开的各种实施例中使用的术语仅用于描述特定实施例的目的并且并非意在限制本公开的各种实施例。如在此所使用,单数形式意在也包括复数形式,除非上下文清楚地另有指示。除非另有限定,否则在这里使用的所有术语(包括技术术语和科学术语)具有与本公开的各种实施例所属领域普通技术人员通常理解的含义相同的含义。所述术语(诸如在一般使用的词典中限定的术语)将被解释为具有与在相关技术领域中的语境含义相同的含义并且将不被解释为具有理想化的含义或过于正式的含义,除非在本公开的各种实施例中被清楚地限定。

#### [0048] 实施例1

[0049] 本发明实施例1公开了一种APP数据保护方法,如图1所示,包括以下步骤:

[0050] 步骤101、确定正在沙箱软件中运行的APP;

[0051] 步骤102、通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。

[0052] 上述,值得指出的是,通过沙箱软件对APP的缓存数据进行透明加密处理,具体可以为,当沙箱软件中的APP正在运行时,沙箱软件对该APP运行的缓存数据通过透明加密的方式进行保存;当该APP需要读取其缓存数据时,沙箱软件获取该APP读取缓存数据的请求,并采用透明解密的方式将缓存数据解密返回给该APP。

[0053] 在一个具体的实施例中,还包括:

[0054] 当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;

[0055] 展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。

[0056] 具体的,为了便于用户进行操作,可以沙箱软件中的所安装的APP可以以图标的方式显示给用户,用户通过点击即可在沙箱软件中运行该APP。

[0057] 在一个具体的实施例中,所述“确定正在沙箱软件中运行的APP”包括:

[0058] 在所述运行界面获取运行APP的指令;

[0059] 基于所述指令确定所运行的APP。

[0060] 具体的,事先沙箱软件中的各APP与图标是有关联的,运行APP的指令是通过点击运行界面的APP图标产生的,因此可以基于指令确定所点击的APP,也即确定所运行的APP。

[0061] 在一个具体的实施例中,为了进一步提高安全性,该方法还包括:

[0062] 获取用户的账户信息;

- [0063] 对所述账户信息进行验证；
- [0064] 若验证通过，则授予所述用户执行权限，其中所述执行权限不低于运行所述沙箱软件，以及在所述沙箱软件的运行界面运行APP所需要的权限。
- [0065] 具体的，除了本身对APP的数据进行加密处理，以保证安全外，还可以对启动沙箱软件以及运行APP的权限进行设置，只有用户的账户信息经过验证，才会授予权限。具体的验证例如可以以指纹验证，或者人脸识别以及密码等方式来进行。
- [0066] 在一个具体的实施例中，为了保证数据的安全，该方法还包括：
- [0067] 当接收到用于关闭所述APP的指令时，基于所述指令清除所保存的缓存数据。
- [0068] 具体的，在关闭了所运行的APP后，为了避免数据被盗用后可能存在的解密，之间删除所保存的缓存数据，增强数据的安全性。
- [0069] 具体的，如图2所示，在一个具体的应用场景下，以手机为例来进行说明，事先在手机中运行一套带有密码运算功能的沙箱软件；后续需要运行的手机APP安装到该沙箱软件中；
- [0070] 由此，当用户需要运行APP时，首先运行沙箱软件，登陆沙箱软件成功后完成沙箱软件的启动，并显示虚拟手机画面，并显示用户应用APP图标。
- [0071] 在此情况下，用户点击用户应用APP图标，运行所点击的APP，该APP运行过程中的数据到存放到该沙箱软件中。
- [0072] 而当缓存数据写入沙箱中时，沙箱软件采用透明加密方式自动将数据加密存放；对应的当用户APP读取缓存数据时，沙箱软件获取用户APP读取数据的请求，采用透明解密的方式将缓存数据解密返回给用户APP。
- [0073] 后续当用户关闭用户APP时，沙箱软件将该用户APP对应的缓存数据删除。
- [0074] 以此，采用沙箱方式将用户APP运行封闭在沙箱的虚拟环境中。且采用透明加密方式。并当用户APP软件关闭后能自动清除残留的数据。最大限度增强了APP数据的安全性。
- [0075] 实施例2
- [0076] 本发明实施例2还提出了一种APP数据保护设备，如图3所示，包括：
- [0077] 确定模块201，用于确定正在沙箱软件中运行的APP；
- [0078] 保护模块202，用于通过所述沙箱软件对所述APP的缓存数据进行透明加密处理，以保证所述APP的数据安全。
- [0079] 在一个具体的实施例中，如图4所示，该设备还包括：
- [0080] 展示模块203，用于当获取到运行所述沙箱软件的第一请求时，基于所述第一请求运行所述沙箱软件；
- [0081] 展示所述沙箱软件的运行界面，其中所述运行界面中包括所述沙箱软件中所有APP的图标。
- [0082] 在一个具体的实施例中，所述确定模块201，用于：
- [0083] 在所述运行界面获取运行APP的指令；
- [0084] 基于所述指令确定所运行的APP。
- [0085] 在一个具体的实施例中，如图5所示，该设备还包括：
- [0086] 验证模块204，用于获取用户的账户信息；
- [0087] 对所述账户信息进行验证；

[0088] 若验证通过,则授予所述用户执行权限,其中所述执行权限不低于运行所述沙箱软件,以及在所述沙箱软件的运行界面运行APP所需要的权限。

[0089] 在一个具体的实施例中,如图6所示,该设备还包括:

[0090] 清除模块205,用于当接收到用于关闭所述APP的指令时,基于所述指令清除所保存的缓存数据。

[0091] 实施例3

[0092] 本发明实施例3还公开了一种移动终端,包括存储器和处理器,所述存储器用于存储计算机程序,所述处理器运行所述计算机程序以使所述移动终端执行根据实施例1中的方法;具体的,所述处理器运行所述计算机程序用于:

[0093] 确定正在沙箱软件中运行的APP;

[0094] 通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。

[0095] 在一个具体的实施例中,所述移动终端还用于:

[0096] 当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;

[0097] 展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。

[0098] 在一个具体的实施例中,所述“确定正在沙箱软件中运行的APP”包括:

[0099] 在所述运行界面获取运行APP的指令;

[0100] 基于所述指令确定所运行的APP。

[0101] 在一个具体的实施例中,所述移动终端还用于:

[0102] 获取用户的账户信息;

[0103] 对所述账户信息进行验证;

[0104] 若验证通过,则授予所述用户执行权限,其中所述执行权限不低于运行所述沙箱软件,以及在所述沙箱软件的运行界面运行APP所需要的权限。

[0105] 在一个具体的实施例中,所述移动终端还用于:

[0106] 当接收到用于关闭所述APP的指令时,基于所述指令清除所保存的缓存数据。

[0107] 实施例4

[0108] 本发明实施例4还公开了一种计算机可读存储介质,其存储有实施例3中所述的移动终端中所使用的计算机程序;具体的,所使用的计算机程序用于执行以下流程:

[0109] 流程A、确定正在沙箱软件中运行的APP;

[0110] 流程B、通过所述沙箱软件对所述APP的缓存数据进行透明加密处理,以保证所述APP的数据安全。

[0111] 在一个具体的实施例中,计算机程序还用于执行以下流程:

[0112] 当获取到运行所述沙箱软件的第一请求时,基于所述第一请求运行所述沙箱软件;

[0113] 展示所述沙箱软件的运行界面,其中所述运行界面中包括所述沙箱软件中所有APP的图标。

[0114] 在一个具体的实施例中,所述“确定正在沙箱软件中运行的APP”包括:

- [0115] 在所述运行界面获取运行APP的指令；
- [0116] 基于所述指令确定所运行的APP。
- [0117] 在一个具体的实施例中, 计算机程序还用于执行以下流程：
- [0118] 获取用户的账户信息；
- [0119] 对所述账户信息进行验证；
- [0120] 若验证通过, 则授予所述用户执行权限, 其中所述执行权限不低于运行所述沙箱软件, 以及在所述沙箱软件的运行界面运行APP所需要的权限。
- [0121] 在一个具体的实施例中, 计算机程序还用于执行以下流程：
- [0122] 当接收到用于关闭所述APP的指令时, 基于所述指令清除所保存的缓存数据。
- [0123] 以此, 本发明实施例提出了APP数据保护方法、设备、移动终端及计算机可读存储介质, 其中, 该方法包括: 确定正在沙箱软件中运行的APP; 通过所述沙箱软件对所述APP的缓存数据进行透明加密处理, 以保证所述APP的数据安全。以此通过沙箱软件构建一个独立的运行环境, 且通过沙箱软件对经过APP的数据进行加密处理, 从而提高了数据的安全性, 提高了用户的使用体验。
- [0124] 本领域技术人员可以理解附图只是一个优选实施场景的示意图, 附图中的模块或流程并不一定是实施本发明所必须的。
- [0125] 本领域技术人员可以理解实施场景中的装置中的模块可以按照实施场景描述进行分布于实施场景的装置中, 也可以进行相应变化位于不同于本实施场景的一个或多个装置中。上述实施场景的模块可以合并为一个模块, 也可以进一步拆分成多个子模块。
- [0126] 上述本发明序号仅仅为了描述, 不代表实施场景的优劣。
- [0127] 以上公开的仅为本发明的几个具体实施场景, 但是, 本发明并非局限于此, 任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

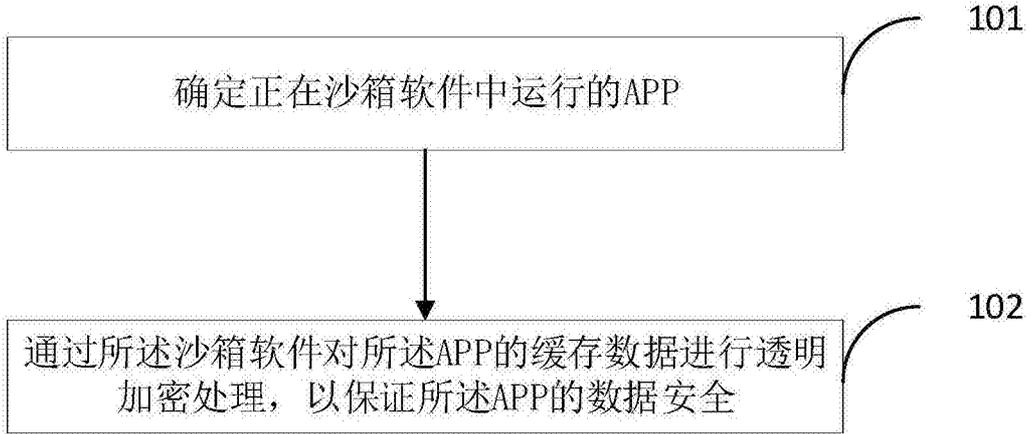


图1

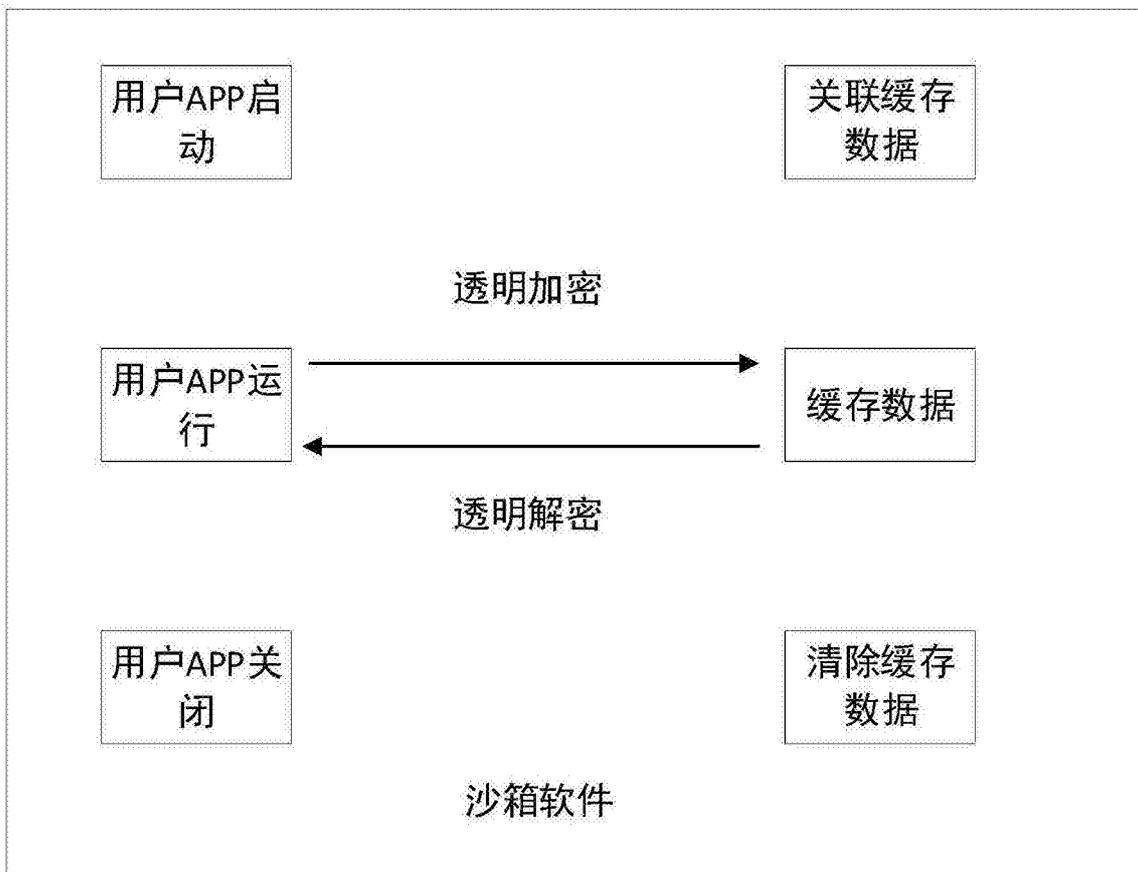


图2



图3

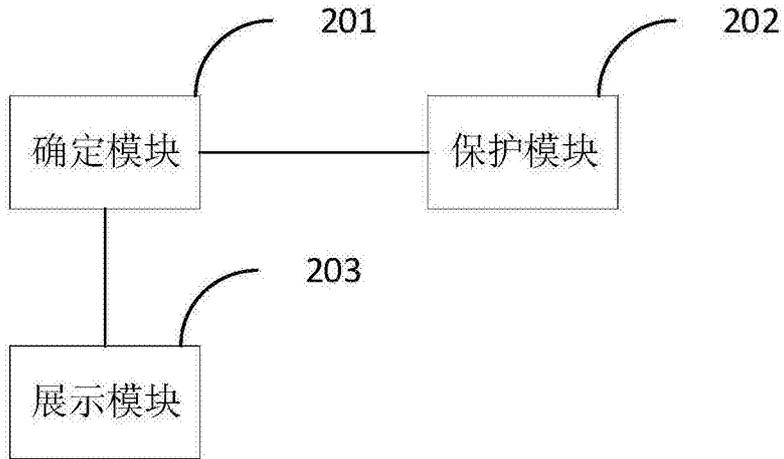


图4

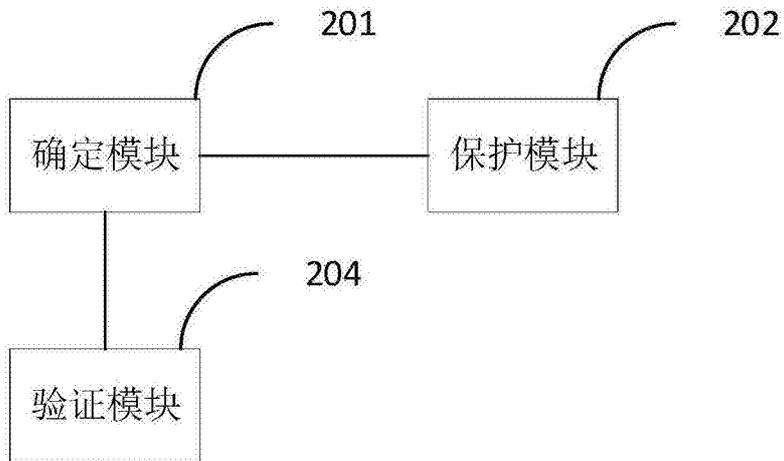


图5

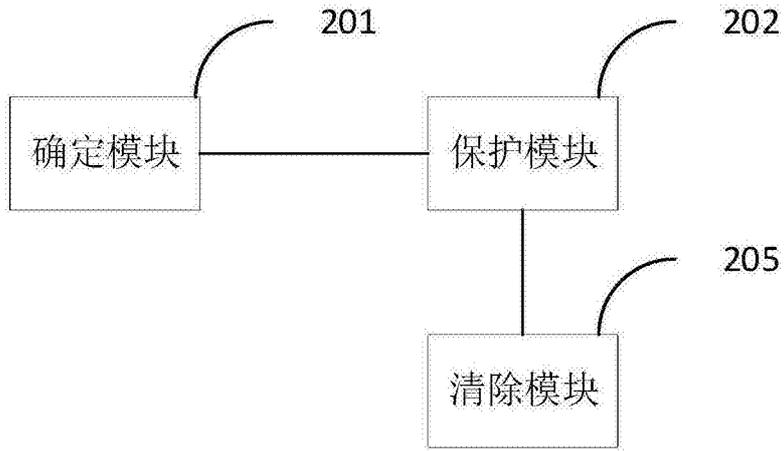


图6