



(12) 发明专利申请

(10) 申请公布号 CN 104700050 A

(43) 申请公布日 2015. 06. 10

(21) 申请号 201510115655. 8

(22) 申请日 2015. 03. 17

(71) 申请人 上海天奕达电子科技有限公司

地址 200233 上海市徐汇区桂平路 391 号新  
漕河泾国际商务中心 B 座 21 楼

(72) 发明人 夏宇婷

(74) 专利代理机构 北京品源专利代理有限公司

11332

代理人 路凯 胡彬

(51) Int. Cl.

G06F 21/88(2013. 01)

G06F 21/32(2013. 01)

G01S 19/16(2010. 01)

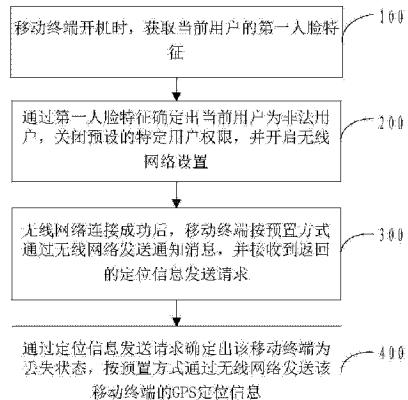
权利要求书2页 说明书6页 附图2页

(54) 发明名称

一种移动终端的安全定位方法及装置

(57) 摘要

本发明涉及一种移动终端的安全定位方法及装置,一种移动终端安全定位方法,包括:移动终端开机时,获取当前用户的第一人脸特征;通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限,并开启无线网络设置;无线网络连接成功后,移动终端按预置方式通过无线网络发送通知消息,并接收到返回的定位信息发送请求;通过定位信息发送请求确定出该移动终端为丢失状态,按预置方式通过无线网络发送该移动终端的 GPS 定位信息。在机主不在的情况下可供他人查询信息并保护机主隐私;在移动终端为丢失状态后,通过无线网络可以得到移动终端的定位信息,加大了找回手机的成功率。



1. 一种移动终端的安全定位方法,其特征在于,包括以下步骤:

移动终端开机时,获取当前用户的第一人脸特征;

通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限,并开启无线网络设置;

无线网络连接成功后,移动终端按预置方式通过无线网络发送通知消息,并接收到返回的定位信息发送请求;

通过所述定位信息发送请求确定出该移动终端为丢失状态,按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

2. 如权利要求 1 所述的方法,其特征在于,所述移动终端按预置方式通过无线网络发送通知消息,包括,所述移动终端通过无线网络发送通知消息到预置的手机号码和 / 或邮箱;所述按预置方式通过无线网络发送该移动终端的 GPS 定位信息,包括:将该移动终端的 GPS 定位信息通过无线网络发送到预置的手机号码和 / 或邮箱。

3. 如权利要求 1 所述的方法,其特征在于,所述按预置方式通过无线网络发送该移动终端的 GPS 定位信息,包括:

按预置方式通过无线网络发送该移动终端的 GPS 定位坐标或包含 GPS 定位坐标的地图。

4. 如权利要求 1 所述的方法,其特征在于,所述按预置方式通过无线网络发送该移动终端的 GPS 定位信息,包括:周期性按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

5. 如权利要求 1 所述的方法,其特征在于,所述移动终端开机时,获取当前用户的第一人脸特征之后,还包括:获取当前用户的人脸图像;无线网络连接成功后,还包括:按预置方式通过无线网络发送该第一人脸图像。

6. 如权利要求 1 所述的方法,其特征在于,所述通过第一人脸特征确定出当前用户为非法用户,包括:

获取第一人脸的视网膜数据,将该视网膜数据与预存的合法视网膜数据进行匹配,确定出当前用户为非法用户;或

获取第一人脸的图像数据,将该图像数据与预存的合法图像数据进行匹配,确定出当前用户为非法用户。

7. 如权利要求 1 所述的方法,其特征在于,通过第一人脸特征确定出当前用户为非法用户之后,还包括:

启动假象关机动画后进入黑屏假关机模式。

8. 如权利要求 1 所述的方法,其特征在于,所述通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限之后,还包括:

移动终端获取输入的特定用户权限解锁数据,将所述权限解锁数据与预存的解锁数据进行匹配,确认开放特定用户权限。

9. 如权利要求 1 所述的方法,其特征在于,所述通过所述定位信息发送请求确定出该移动终端为丢失状态,具体包括:获取定位信息发送请求数据,将该数据与预存的丢失状态下定位信息发送权限密码进行匹配,确定出该移动终端为丢失状态。

10. 一种移动终端的安全定位装置,其特征在于,包括:

人脸特征获取单元,用于移动终端开机时,获取当前用户的第一人脸特征;

非法用户判定单元,用于通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限,并开启无线网络设置;

通知单元,用于无线网络连接成功后,移动终端按预置方式通过无线网络发送通知消息,并接收到返回的定位信息发送请求;

定位信息发送单元,通过所述定位信息发送请求确定出该移动终端为丢失状态,按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

## 一种移动终端的安全定位方法及装置

### 技术领域

[0001] 本发明涉及安全定位技术领域，尤其涉及一种移动终端的安全定位方法及装置。

### 背景技术

[0002] 如今手机、平板电脑等移动终端经常会被盗，而盗贼在盗取手机后会关机并拔掉SIM卡，使得找回手机的难度加大，且很难保护手机内的隐私数据，通常手机中会设置键盘密码锁，虽然加强了的隐私安全系数，但是会导致手机无法联网，降低了手机与外界的通信的可能，从而使找回手机的机率大大降低，且现有的人脸识别解锁系统必须是本人才可以解锁，如手机主人不在的紧急情况下，开不了机，无法拿手机查询重要信息，给使用带来不便。

### 发明内容

[0003] 针对上述缺陷，本发明的目的在于提供一种移动终端的安全定位方法及装置，以解决移动终端被盗后找回几率低的问题。

[0004] 为达此目的，本发明提供了一种移动终端的安全定位方法，包括以下步骤：

[0005] 移动终端开机时，获取当前用户的第一人脸特征；

[0006] 通过第一人脸特征确定出当前用户为非法用户，关闭预设的特定用户权限，并开启无线网络设置；

[0007] 无线网络连接成功后，移动终端按预置方式通过无线网络发送通知消息，并接收到返回的定位信息发送请求；

[0008] 通过所述定位信息发送请求确定出该移动终端为丢失状态，按预置方式通过无线网络发送该移动终端的GPS定位信息。

[0009] 较佳地，所述移动终端按预置方式通过无线网络发送通知消息，包括，所述移动终端通过无线网络发送通知消息到预置的手机号码和 / 或邮箱；所述按预置方式通过无线网络发送该移动终端的GPS定位信息，包括：将该移动终端的GPS定位信息通过无线网络发送到预置的手机号码和 / 或邮箱。

[0010] 较佳地，所述按预置方式通过无线网络发送该移动终端的GPS定位信息，包括：

[0011] 按预置方式通过无线网络发送该移动终端的GPS定位坐标或包含GPS定位坐标的地图。

[0012] 较佳地，所述按预置方式通过无线网络发送该移动终端的GPS定位信息，包括：周期性按预置方式通过无线网络发送该移动终端的GPS定位信息。

[0013] 较佳地，所述移动终端开机时，获取当前用户的第一人脸特征之后，还包括：获取当前用户的人脸图像；无线网络连接成功后，还包括：按预置方式通过无线网络发送该第一人脸图像。

[0014] 较佳地，所述通过第一人脸特征确定出当前用户为非法用户，包括：

[0015] 获取第一人脸的视网膜数据，将该视网膜数据与预存的合法视网膜数据进行匹

配,确定出当前用户为非法用户;或

[0016] 获取第一人脸的图像数据,将该图像数据与预存的合法图像数据进行匹配,确定出当前用户为非法用户。

[0017] 较佳地,通过第一人脸特征确定出当前用户为非法用户之后,还包括:启动假象机关机动画后进入黑屏假关机模式。

[0018] 较佳地,所述通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限之后,还包括:

[0019] 移动终端获取输入的特定用户权限解锁数据,将所述权限解锁数据与预存的解锁数据进行匹配,确认开放特定用户权限。

[0020] 较佳地,所述通过所述定位信息发送请求确定出该移动终端为丢失状态,具体包括:获取定位信息发送请求数据,将该数据与预存的丢失状态下定位信息发送权限密码进行匹配,确定出该移动终端为丢失状态。

[0021] 为达此目的,本发明提供了一种移动终端的安全定位装置,包括:

[0022] 人脸特征获取单元,用于移动终端开机时,获取当前用户的第一人脸特征;

[0023] 非法用户判定单元,用于通过第一人脸特征确定出当前用户为非法用户,关闭预设的特定用户权限,并开启无线网络设置;

[0024] 通知单元,用于无线网络连接成功后,移动终端按预置方式通过无线网络发送通知消息,并接收到返回的定位信息发送请求;

[0025] 定位信息发送单元,通过所述定位信息发送请求确定出该移动终端为丢失状态,按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

[0026] 本发明采用上述技术方案,与现有的技术方案相比,具有以下有益的效果:

[0027] 开机后获取人脸特征,不需要连接网络,在没有插 SIM 卡的情况下仍然可以记录用户的人脸特征;人脸特征与合法人脸特征数据不匹配时,一些特定的用户权限被关闭了,但仍可使用移动终端的部分功能,在机主不在的紧急情况下可供他人查询信息,同时保护机主隐私;启动假象的关机动画,并进入黑屏假关机模式,可防止他人再次关机而失去对移动终端的定位;在移动终端被非法用户操作,可以自动连接无线网络,通过连接无线网络发送寻找通知信息,得到的定位信息发送请求来确定移动终端已经丢失,将定位信息、人脸图像发给预设的手机号码和/或邮箱,加大了找回移动终端的成功率。

## 附图说明

[0028] 图 1 是本发明一种移动终端的安全定位方法的流程图一;

[0029] 图 2 是本发明一种移动终端的安全定位方法的流程图二;

[0030] 图 3 是本发明一种移动终端的安全定位方法的流程图三;

[0031] 图 4 是本发明一种移动终端的安全定位装置的结构框图。

## 具体实施方式

[0032] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。,所述黑屏假关机模式为开启静音模式和来电免提醒模式,熄灭屏幕和

所有指示灯，并关闭所有按键和接口的用户权限

[0033] 附图 1-3 为本发明提供的一种移动终端安全定位方法的流程图，一种移动终端安全定位方法包括以下步骤：

[0034] 100：移动终端开机时，获取当前用户的第一人脸特征，由于开机后手机可能被放置在口袋里或朝向其他方向，开机后是获取用户人脸特征的最佳时机。也可以同时抓拍当前用户的人脸图像，以待后期确认移动终端是否丢失。

[0035] 且开机后可以开启 GPS 功能，在没有网络的情况下仍然可以对手机的位置进行定位，可以采用周期性定位，在开机后立即开始周期性获取移动终端的 GPS 定位信息，将移动终端的移动路径记录下来。

[0036] 200：通过第一人脸特征确定出当前用户为非法用户，关闭预设的特定用户权限，并开启无线网络设置。

[0037] 通过第一人脸特征确定出当前用户为非法用户具体为，获取第一人脸的视网膜数据，将该视网膜数据与预存的合法视网膜数据进行匹配，确定出当前用户为非法用户；或获取第一人脸的图像数据，将该图像数据与预存的合法图像数据进行匹配，确定出当前用户为非法用户。预存的合法视网膜数据和预存的合法图像数据可以为多个亲戚朋友的人脸特征数据，便于他人使用方便。第一人脸特征与预存的合法视网膜数据和预存的合法图像数据逐一进行匹配，如果匹配成功，则当前用户为合法用户；如果匹配失败，则当前用户为非法用户，需要关闭预设的特定用户权限，避免后续用户对移动终端操作过程中泄露机主的隐私，特定用户权限包括特定电话的呼叫权限、特定应用软件的使用权限、向特定联系人发送短信的权限、特定隐私文件的查看权限中的一项或几项，用户可以自定义不希望陌生人使用的权限，如不可以呼叫联系人的电话，但是可以拨打陌生号码，可以查看来电信息、去电信息以及联系人的号码，不可以浏览照片、文档等。为了防止移动终端再次被关机，可以关闭用户的关机权限。

[0038] 开启无线网络设置，一般为开启 WiFi，若移动终端插有上网卡也可以开启蜂窝移动网络。

[0039] 较佳地，在步骤 200 之后，还包括 201：移动终端获取输入的特定用户权限解锁数据，将所述权限解锁数据与预存的解锁数据进行匹配，开放特定用户权限。其中，可以获取到通过移动终端按键和 / 或触屏输入的特定用户权限解锁密码，通过用户通过指定操作找到输入特定用户权限解锁密码的写入窗口，验证特定用户权限解锁密码与预存的权限密码匹配，则开放特定用户权限，此种开放权限的方法可以方便在机主不在的情况下，他人使用移动终端以及查找信息。也可以为通过移动终端获取的第二人脸特征，获取第二人脸的视网膜数据，将该视网膜数据与预存的合法视网膜数据进行匹配，或获取第二人脸的图像数据，将该图像数据与预存的合法图像数据进行匹配，匹配成功，则开放特定用户权限。

[0040] 300：无线网络连接成功后，移动终端按预置方式通过无线网络发送通知消息，并接收到返回的定位信息发送请求。

[0041] 具体为，当移动终端处于无线网络覆盖区域，并连接网络成功，则移动终端通过无线网络发送通知消息到预置的手机号码和 / 或邮箱。

[0042] 当机主发现手机已经丢失，向手机号码和 / 或邮箱写入位信息发送请求数据，此时若手机号码和 / 或邮箱接收到通知消息，则立即将写入的定位信息发送请求返回给移动

终端，并且手机号码和 / 或邮箱提示机主已经找到手机。

[0043] 当机主没有发现手机丢失，移动终端按预置方式通过无线网络发送通知消息，同时也可以通过无线网络发送第一人脸图像到预置的手机号码和 / 或邮箱，此时若手机号码和 / 或邮箱接收到通知消息和人脸图像，可以提示机主是否写入定位信息发送请求数据，如果人脸图像为熟人则可以放弃写入，默认手机不在丢失状态；如果人脸图像为陌生人，则可以写入，并通过手机号码和 / 或邮箱发送给移动终端进行定位请求；也可以不发送第一人脸图像，在确定没有写入定位信息发送请求数据后直接不提示机主，默认手机不在丢失状态。

[0044] 400：通过定位信息发送请求确定出该移动终端为丢失状态，按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

[0045] 定位信息发送请求数据可以为一串预设的密码，可以由机主自定义或者通过移动终端生成，将该定位信息发送请求数据与预存的丢失状态下定位信息发送权限密码进行匹配，若匹配成功，则确定出该移动终端为丢失状态，开启丢失状态下定位信息发送权限，便可以按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

[0046] 按预置方式通过无线网络发送该移动终端的 GPS 定位信息具体为，将该移动终端的 GPS 定位信息通过无线网络发送到预置的手机号码和 / 或邮箱，移动终端的 GPS 定位信息包括该移动终端的 GPS 定位坐标或包含 GPS 定位坐标的地图，通过发送包含 GPS 定位坐标的地图可以更直观的看到当前用户的运动轨迹。可以周期性发送 GPS 定位信息，一般每隔 2-10 秒发送一次，第一次发送的定位信息可以包含自开机到发送时的全部定位坐标以及定位坐标对应的时间点，可以为包含 GPS 定位坐标以及定位坐标对应的时间点的地图。

[0047] 较佳地，通过第一人脸特征确定出当前用户为非法用户之后，还包括：

[0048] 202：启动假象关机动画后进入黑屏假关机模式，防止用户关机而无法获得移动在终端的定位信息，具体为：接收到关机指令，则播放关机动画后进入黑屏假关机模式。关机指令可以为键盘输入或者触屏输入，黑屏假关机模式为黑屏待机并开启静音模式和来电免提醒模式，熄灭屏幕和所有指示灯，并关闭所有按键和接口的用户权限。

[0049] 附图 4 为本发明提供的一种基于人脸识别和 gps 定位的手机安全定位装置的结构框图，该装置包括人脸特征获取单元 500、非法用户判定单元 501 以及通知单元 502 以及定位信息发送单元 503。

[0050] 人脸特征获取单元 500，用于获取当前用户的第一人脸特征，由于开机后手机可能被放置在口袋里或朝向其他方向，开机后是获取用户人脸特征的最佳时机。也可以同时抓拍当前用户的人脸图像，以待后期确认移动终端是否丢失。

[0051] 且开机后可以开启 GPS 功能，在没有网络的情况下仍然可以对手机的位置进行定位，可以采用周期性定位，在开机后立即开始周期性获取移动终端的 GPS 定位信息，将移动终端的移动路径记录下来。非法用户判定单元 501，用于通过第一人脸特征确定出当前用户为非法用户，关闭预设的特定用户权限，并开启无线网络设置。

[0052] 通过第一人脸特征确定出当前用户为非法用户，具体为，获取第一人脸的视网膜数据，将该视网膜数据与预存的合法视网膜数据进行匹配，确定出当前用户为非法用户；或获取第一人脸的图像数据，将该图像数据与预存的合法图像数据进行匹配，确定出当前用户为非法用户。预存的合法视网膜数据和预存的合法图像数据可以为多个亲戚朋友的人脸

特征数据，便于他人使用方便。第一人脸特征与预存的合法视网膜数据和预存的合法图像数据逐一进行匹配，如果匹配成功，则当前用户为合法用户；如果匹配失败，则当前用户为非法用户，需要关闭预设的特定用户权限，避免后续用户对移动终端操作过程中泄露机主的隐私，特定用户权限包括特定电话的呼叫权限、特定应用软件的使用权限、向特定联系人发送短信的权限、特定隐私文件的查看权限中的一项或几项，用户可以自定义不希望陌生人使用的权限，如不可以呼叫联系人的电话，但是可以拨打陌生号码，可以查看来电信息、去电信息以及联系人的号码，不可以浏览照片、文档等。为了防止移动终端再次被关机，可以关闭用户的关机权限。

[0053] 开启无线网络设置，一般为开启 WiFi，若移动终端插有上网卡也可以开启蜂窝移动网络。

[0054] 通知单元 502 用于无线网络连接成功后，移动终端按预置方式通过无线网络发送通知消息，并接收到返回的定位信息发送请求。

[0055] 具体为，当移动终端处于无线网络覆盖区域，并连接网络成功，则移动终端通过无线网络发送通知消息到预置的手机号码和 / 或邮箱。

[0056] 当机主发现手机已经丢失，向手机号码和 / 或邮箱写入位信息发送请求数据，此时若手机号码和 / 或邮箱接收到通知消息，则立即将写入的定位信息发送请求返回给移动终端，并且手机号码和 / 或邮箱提示机主已经找到手机。

[0057] 当机主没有发现手机丢失，移动终端按预置方式通过无线网络发送通知消息，同时也可以通过无线网络发送第一人脸图像到预置的手机号码和 / 或邮箱，此时若手机号码和 / 或邮箱接收到通知消息和人脸图像，可以提示机主是否写入定位信息发送请求数据，如果人脸图像为熟人则可以放弃写入，默认手机不在丢失状态；如果人脸图像为陌生人，则可以写入，并通过手机号码和 / 或邮箱发送给移动终端进行定位请求；也可以不发送第一人脸图像，在确定没有写入定位信息发送请求数据后直接不提示机主，默认手机不在丢失状态。

[0058] 定位信息发送单元 503 用于通过定位信息发送请求确定出该移动终端为丢失状态，按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

[0059] 定位信息发送请求数据可以为一串预设的密码，可以由机主自定义或者通过移动终端生成，将该定位信息发送请求数据与预存的丢失状态下定位信息发送权限密码进行匹配，若匹配成功，则确定出该移动终端为丢失状态，开启丢失状态下定位信息发送权限，便可以按预置方式通过无线网络发送该移动终端的 GPS 定位信息。

[0060] 按预置方式通过无线网络发送该移动终端的 GPS 定位信息具体为，将该移动终端的 GPS 定位信息通过无线网络发送到预置的手机号码和 / 或邮箱，移动终端的 GPS 定位信息包括该移动终端的 GPS 定位坐标或包含 GPS 定位坐标的地图，通过发送包含 GPS 定位坐标的地图可以更直观的看到当前用户的运动轨迹。可以周期性发送 GPS 定位信息，一般每隔 2-10 秒发送一次，第一次发送的定位信息可以包含自开机到发送时的全部定位坐标以及定位坐标对应的时间点，可以为包含 GPS 定位坐标以及定位坐标对应的时间点的地图。

[0061] 较佳地，还包括黑屏假关机单元 511，用于通过第一人脸特征确定出当前用户为非法用户之后，启动假象关机动画后进入黑屏假关机模式，防止用户关机而无法获得移动在终端的定位信息，具体为：接收到关机指令，则播放关机动画后进入黑屏假关机模式。关机

指令可以为键盘输入或者触屏输入,黑屏假关机模式为黑屏待机并开启静音模式和来电免提醒模式,熄灭屏幕和所有指示灯,并关闭所有按键和接口的用户权限。

[0062] 较佳地,还包括权限解锁单元 512,用于关闭预设的特定用户权限之后,移动终端获取输入的特定用户权限解锁数据,将权限解锁数据与预存的解锁数据进行匹配,开放特定用户权限。其中,可以获取到通过移动终端按键和 / 或触屏输入的特定用户权限解锁密码,通过用户通过指定操作找到输入特定用户权限解锁密码的写入窗口,验证特定用户权限解锁密码与预存的权限密码相匹配,则开放特定用户权限,此种开放权限的方法可以方便在机主不在的情况下,他人使用移动终端以及查找信息。也可以为通过移动终端获取的第二人脸特征,如获取第二人脸的视网膜数据,将该视网膜数据与预存的合法视网膜数据进行匹配,或获取第二人脸的图像数据,将该图像数据与预存的合法图像数据进行匹配,匹配成功,则开放特定用户权限。

[0063] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以作出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

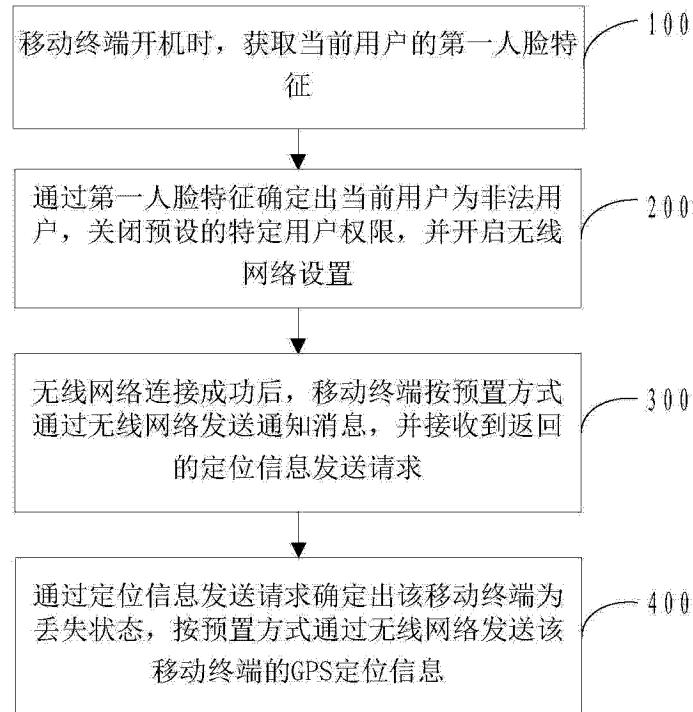


图 1

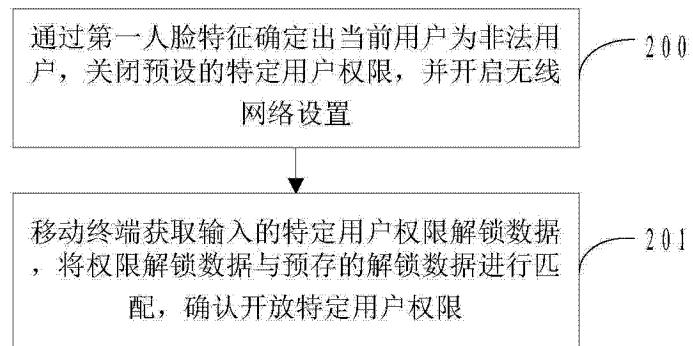


图 2

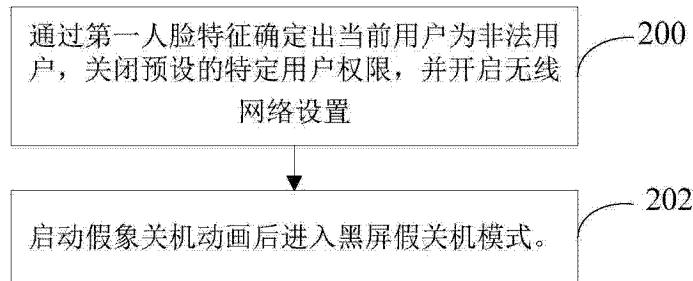


图 3

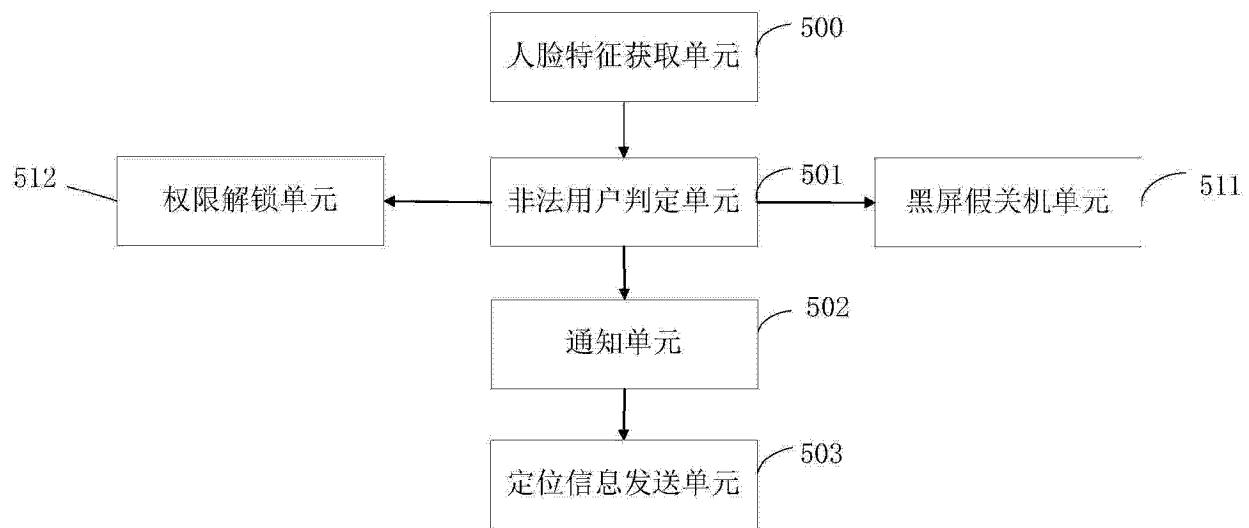


图 4