(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 103020553 A
(43)申请公布日 2013.04.03

(21)申请号 201210533241.3

(22)申请日 2012.12.11

(71)申请人 广东欧珀移动通信有限公司
地址 523841 广东省东莞市长安镇乌沙海滨路 18 号

(72)发明人 张强

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文

(51)Int.Cl.
G06F 21/88(2013.01)
G06F 21/62(2013.01)

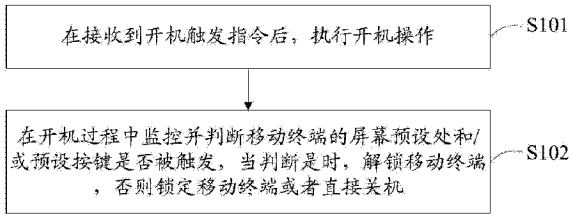
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

一种移动终端防盗保护方法

(57)摘要

本发明适用于移动终端技术领域，提供一种移动终端防盗保护方法及装置，所述方法包括：在接收到开机触发指令后，执行开机操作；在开机过程中监控并判断移动终端的屏幕预设处和/或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。本发明在移动终端被锁定时还没有进入系统，因此移动终端的触摸屏以及按键不响应任何操作，本发明在驱动层面上对用户的解锁操作进行验证，不知道该解锁操作的非法用户是无法进入系统后台查杀进程的，因此本实施例可以有效地保护移动终端不被破解，达到很好的防盗保护效果。



CN 103020553 A

1. 一种移动终端防盗保护方法，其特征在于，所述方法包括：

在接收到开机触发指令后，执行开机操作；

在开机过程中监控并判断移动终端的屏幕预设处和/或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

2. 如权利要求 1 所述方法，其特征在于，所述在开机过程中监控并判断移动终端的屏幕预设处和/或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机步骤，具体包括：

在开机过程中监控移动终端屏幕和/或按键是否被触发；

在接收到屏幕和/或按键的触发信息时，判断该触发信息是否满足预设的开机解锁要求；

当满足所述预设的开机解锁要求时，解锁移动终端，正常进入移动终端的操作界面；

当不满足所述预设的开机解锁要求时，以及在开机过程中并未接收到屏幕和/或按键的触发信息时，锁定移动终端或者直接关机。

3. 如权利要求 2 所述方法，其特征在于，所述在开机过程中监控移动终端屏幕和/或按键是否被触发步骤中，只在开机过程中预设的监控时间段内监控移动终端屏幕和/或按键是否被触发。

4. 如权利要求 3 所述方法，其特征在于，所述在接收到开机触发指令后，执行开机操作步骤之前，还包括：

接收并保存用户设置的开机解锁信息。

5. 如权利要求 4 所述方法，其特征在于，所述接收并保存用户设置的开机解锁信息步骤之后，还包括：

接收并保存用户设置的监控时间段信息。

6. 一种移动终端防盗保护装置，其特征在于，所述装置包括：

开机执行单元，用于在接收到开机触发指令后，执行开机操作；

监控判断执行单元，用于在开机过程中监控并判断移动终端的屏幕预设处和/或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

7. 如权利要求 6 所述装置，其特征在于，所述监控判断执行单元包括：

监控模块，用于在开机过程中监控移动终端屏幕和/或按键是否被触发；

判断模块，用于在接收到屏幕和/或按键的触发信息时，判断该触发信息是否满足预设的开机解锁要求；

解锁模块，用于当满足所述预设的开机解锁要求时，解锁移动终端，正常进入移动终端的操作界面；

锁定模块，用于当不满足所述预设的开机解锁要求时，以及在开机过程中并未接收到屏幕和/或按键的触发信息时，锁定移动终端或者直接关机。

8. 如权利要求 7 所述装置，其特征在于，所述监控模块用于在开机过程中预设的监控时间段内监控移动终端屏幕和/或按键是否被触发。

9. 如权利要求 8 所述装置，其特征在于，所述装置还包括：

解锁信息保存单元，用于接收并保存用户设置的开机解锁信息。

10. 如权利要求 9 所述装置，其特征在于，所述装置还包括：

时间段信息保存单元，用于接收并保存用户设置的监控时间段信息。

一种移动终端防盗保护方法

技术领域

[0001] 本发明属于移动终端领域，尤其涉及一种移动终端防盗保护方法。

背景技术

[0002] 目前包括手机、掌上电脑等移动终端的防盗保护很多都是在开机后通过应用软件来实现，比如可以设置屏幕解锁密码，又如可以使用一些防盗软件对 SIM 卡进行追踪，可以实时定位到移动终端当前所处位置，但所有的这些防盗保护方案都是在移动终端开机后，通过应用软件展开实现，因此这就会给不法者留有软件破解漏洞，移动终端开机后，将关于防盗保护所在的进程关闭即可，比如将锁屏的进程、保护应用杀掉，那么这些保护就失效了，这样就达不到预期的防盗保护效果。

发明内容

[0003] 鉴于上述问题，本发明的目的在于提供一种移动终端防盗保护方法及装置，旨在解决现有移动终端防盗保护方案都是在移动终开机后通过执行应用程序来防盗保护，导致保护安全性不够高的技术问题。

[0004] 一方面，所述移动终端防盗保护方法包括下述步骤：

[0005] 在接收到开机触发指令后，执行开机操作；

[0006] 在开机过程中监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

[0007] 另一方面，所述移动终端防盗保护装置包括：

[0008] 开机执行单元，用于在接收到开机触发指令后，执行开机操作；

[0009] 监控判断执行单元，用于在开机过程中监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

[0010] 本发明的有益效果是：在本发明技术方案中，用户在开机过程中按预设要求触发屏幕和 / 或按键，否则无法解锁开机，触按屏幕和按键都没有任何反应，而其他用户由于不知预设的解锁操作方式来触发屏幕和 / 或按键，由于此时系统没有完全启动，第三方无法进入系统后台查杀进程，本发明从驱动层面上对移动终端进行保护，达到很好的防盗保护效果。

附图说明

[0011] 图 1 是本发明第一实施例提供的移动终端防盗保护方法的流程图；

[0012] 图 2 是本发明第二实施例提供的移动终端防盗保护方法的流程图；

[0013] 图 3 是本发明第三实施例提供的移动终端防盗保护装置的结构方框图；

[0014] 图 4 是本发明第四实施例提供的移动终端防盗保护装置的结构方框图。

具体实施方式

[0015] 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。

[0016] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0017] 实施例一：

[0018] 图 1 示出了本发明第一实施例提供的移动终端防盗保护方法的流程，为了便于说明仅示出了与本发明实施例相关的部分。

[0019] 本实施例提供的移动终端防盗保护方法包括下述步骤：

[0020] 步骤 S101、在接收到开机触发指令后，执行开机操作。

[0021] 本发明实施例只要是完成在开机过程中对用户的操作动作进行判断验证，当符合要求时，才解锁移动终端，正常进入移动终端操作界面，因此用户首先需要在关机状态下开启移动终端，用户触发移动终端上的电源开关后，生成开机触发命令，此时开始进入开机流程。

[0022] 步骤 S102、在开机过程中监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

[0023] 移动终端中保存有用户设置的解锁操作动作对应的解锁信息，比如用户可以设置需要在开机过程中触摸屏幕的四个角才能解锁进入系统，或者也可以设置需要触发音量增减键才能解锁进入系统，所述屏幕的四个角即为屏幕预设处，所述音量增减键即为预设按键，本实施例不具体限定用户设置的解锁操作动作，只要用户在开机过程中按照预先设定的解锁操作动作，触发屏幕预设处和 / 或预设按键即可，当检测到所述屏幕预设处和 / 或预设按键被触发时，才可以完成解锁正常进行操作系统，否则锁定移动终端，此时还没有进入系统，因此移动终端的触摸屏以及按键不响应任何操作，由于还为进入系统，在驱动层面上对用户的解锁操作进行验证，不知道该解锁操作的非法用户是无法进入系统后台查杀进程的，因此本实施例可以有效地保护移动终端不被破解，达到很好的防盗保护效果。

[0024] 实施例二：

[0025] 图 2 示出了本发明实施例提供的移动终端防盗保护方法的流程，为了便于说明仅示出了与本发明实施例相关的部分。

[0026] 本实施例提供的移动终端防盗保护方法包括下述步骤：

[0027] 步骤 S201、接收并保存用户设置的开机解锁信息；

[0028] 步骤 S202、接收并保存用户设置的监控时间段信息。

[0029] 本实施例中，用户可以自行设置开机解锁信息以及监控时段信息，只有在所述监控时间段内完成预设的解锁操作才可以完成解锁，正常进入系统，比如可以设置为开机上电后的 10 秒之内。所述开机解锁信息，是用户在移动状态处于开机状态时，自行设置的解锁操作动作所对应的数据信息，具体实现时，用户可以进入解锁信息录制界面，点击录制后，再在移动终端上做出自己所需的解锁动作，比如触摸屏幕四个角，或者横划屏幕上方，或者双击音量增减等等，在录制的过程中，移动终端会保存此期间产生的操作轨迹信息，所述操作轨迹信息就是所述的开解解锁信息，用户只有在预设的监控时间段内完成先前录制的动作才能完成开机解锁。

[0030] 步骤 S203、在开机过程的预设监控时间段内监控移动终端屏幕和 / 或按键是否被

触发；

[0031] 步骤 S204、在接收到屏幕和 / 或按键的触发信息时，判断该触发信息是否满足预设的开机解锁要求；

[0032] 步骤 S205、当满足所述预设的开机解锁要求时，解锁移动终端，正常进入移动终端的操作界面；

[0033] 步骤 S206、当不满足所述预设的开机解锁要求时，以及在开机过程中并未接收到屏幕和 / 或按键的触发信息时，锁定移动终端或者直接关机。

[0034] 上述步骤 S203-S206 完成了用户解锁操作动作的验证过程，具体的，在触发移动终端的电源开关后，首先获取到所述设置的监控时间段信息，包括起始时间和结束时间，此时启动一个计时器，在到达所述起始时间时开始监控移动终端的屏幕和 / 或按键，直到所述结束时间，比如设置的监控时间段信息为开机上电后的 10 秒，此时启动一个计时器，这里所述计时器为定时器，从开机直到该定时器结束的时间段内监控移动终端的屏幕和 / 或按键。

[0035] 在所述监控时间段内监测到移动终端屏幕和 / 或按键被触发，即接收到屏幕和 / 或按键的触发信息时，继续判断该触发信息是否满足预设的开机解锁要求，具体的，将该触发信息与预设的开机解锁信息进行比对即可，一致时解锁移动终端，正常进入移动终端的操作界面，否者锁定移动终端或者直接关机，在锁定移动终端时，用户无法对移动终端进行任何操作，除非关闭电源。当然如果在所述监控时间段内没有监测到移动终端屏幕和 / 或按键被触发，即并未接收到屏幕和 / 或按键的触发信息时，同样也是锁定移动终端或者直接关机。

[0036] 本实施例在实施例一的基础上，进一步实现了用户可以自行设置开机解锁信息以及监控时间段信息，这样进一步降低了非法用户通过随意解锁操作移动终端完成解锁的可能性，由于开机过程中没有任何解锁提示信息，非法用户不会意识到需要在开机过程中进行解锁操作，即使移动终端被盗，除开用户本人，移动终端基本上没有被解锁开机的可能性，达到了移动终端防盗保护的目的。

[0037] 实施例三：

[0038] 图 3 示出了本发明实施例提供的移动终端防盗保护装置的结构，为了便于说明仅示出了与本发明实施例相关的部分。

[0039] 本实施例提供的移动终端防盗保护装置包括：

[0040] 开机执行单元 301，用于在接收到开机触发指令后，执行开机操作；

[0041] 监控判断执行单元 302，用于在开机过程中监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

[0042] 本实施例提供的各个功能单元 301、302 对应实现了实施例一中的步骤 S101、S102，具体的，开机执行单元 301 在接收到开机触发指令后开机执行单元 301 执行开机操作，在开机过程中监控判断执行单元 302 监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。本实施例中，非法用户由于不知道解锁操作动作，此时还没有进入系统，因此移动终端的触摸屏以及按键不响应任何操作，由于还为进入系统，在驱动层面上对用户的解锁操作进行验证，不知道该解锁操作的第三方用户是无法进入系统后台查杀进程的，因此本实施例可以有效地保护

移动终端不被破解，达到很好的防盗保护效果。

[0043] 实施例四：

[0044] 图 4 示出了本发明实施例提供的移动终端防盗保护装置的结构，为了便于说明仅示出了与本发明实施例相关的部分。

[0045] 本实施例提供的移动终端防盗保护装置包括：

[0046] 解锁信息保存单元 41，用于接收并保存用户设置的开机解锁信息；

[0047] 时间段信息保存单元 42，用于接收并保存用户设置的监控时间段信息；

[0048] 开机执行单元 43，用于在接收到开机触发指令后，执行开机操作；

[0049] 监控判断执行单元 44，用于在开机过程中监控并判断移动终端的屏幕预设处和 / 或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机。

[0050] 其中，所述监控判断执行单元 44 包括：

[0051] 监控模块 441，用于在开机过程中预设的监控时间段内监控移动终端屏幕和 / 或按键是否被触发；

[0052] 判断模块 442，用于在接收到屏幕和 / 或按键的触发信息时，判断该触发信息是否满足预设的开机解锁要求；

[0053] 解锁模块 443，用于当满足所述预设的开机解锁要求时，解锁移动终端，正常进入移动终端的操作界面；

[0054] 锁定模块 444，用于当不满足所述预设的开机解锁要求时，以及在开机过程中并未接收到屏幕和 / 或按键的触发信息时，锁定移动终端或者直接关机。

[0055] 本实施例提供的各个功能单元和功能模块对应实现了实施例二中的各个步骤，另一方面，本实施在实施例三的基础上，增加了解锁信息保存单元 41 以及时间段信息保存单元 42，通过这两个单元，用户可以自行设置开机解锁信息以及监控时间段信息，这样进一步降低了非法用户通过随意解锁操作移动终端完成解锁的可能性，另外本实施例公开了监控判断执行单元 44 的一种具体优选的结构，能够实现对用户所做出的解锁操作动作进行判断，决定是否解锁，本实施例在驱动层面上对用户的解锁操作进行验证，不知道该解锁操作的第三方用户是无法进入系统后台查杀进程，因此本实施例可以有效地保护移动终端不被破解，达到很好的防盗保护效果。

[0056] 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步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以在存储于一计算机可读取存储介质中，所述的存储介质，如 ROM/RAM、磁盘、光盘等。

[0057] 以上所述仅为本发明的较佳实施例而已，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、等同替换和改进等，均应包含在本发明的保护范围之内。

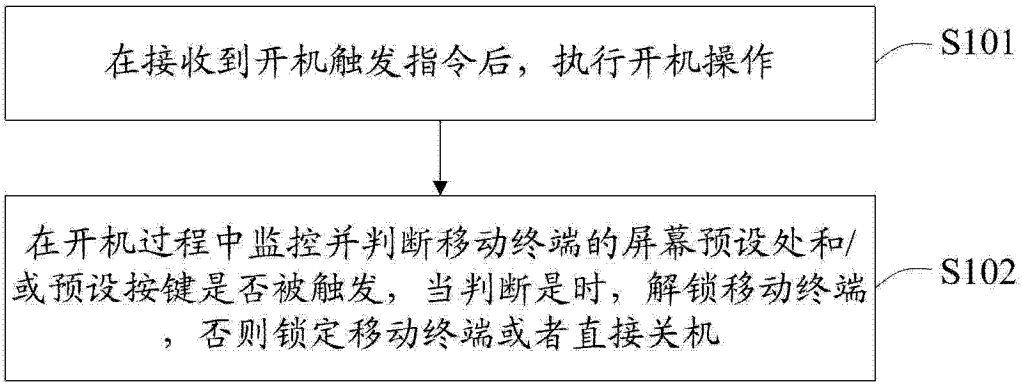

在接收到开机触发指令后，执行开机操作
S101
在开机过程中监控并判断移动终端的屏幕预设处和/或预设按键是否被触发，当判断是时，解锁移动终端，否则锁定移动终端或者直接关机
S102

图 1

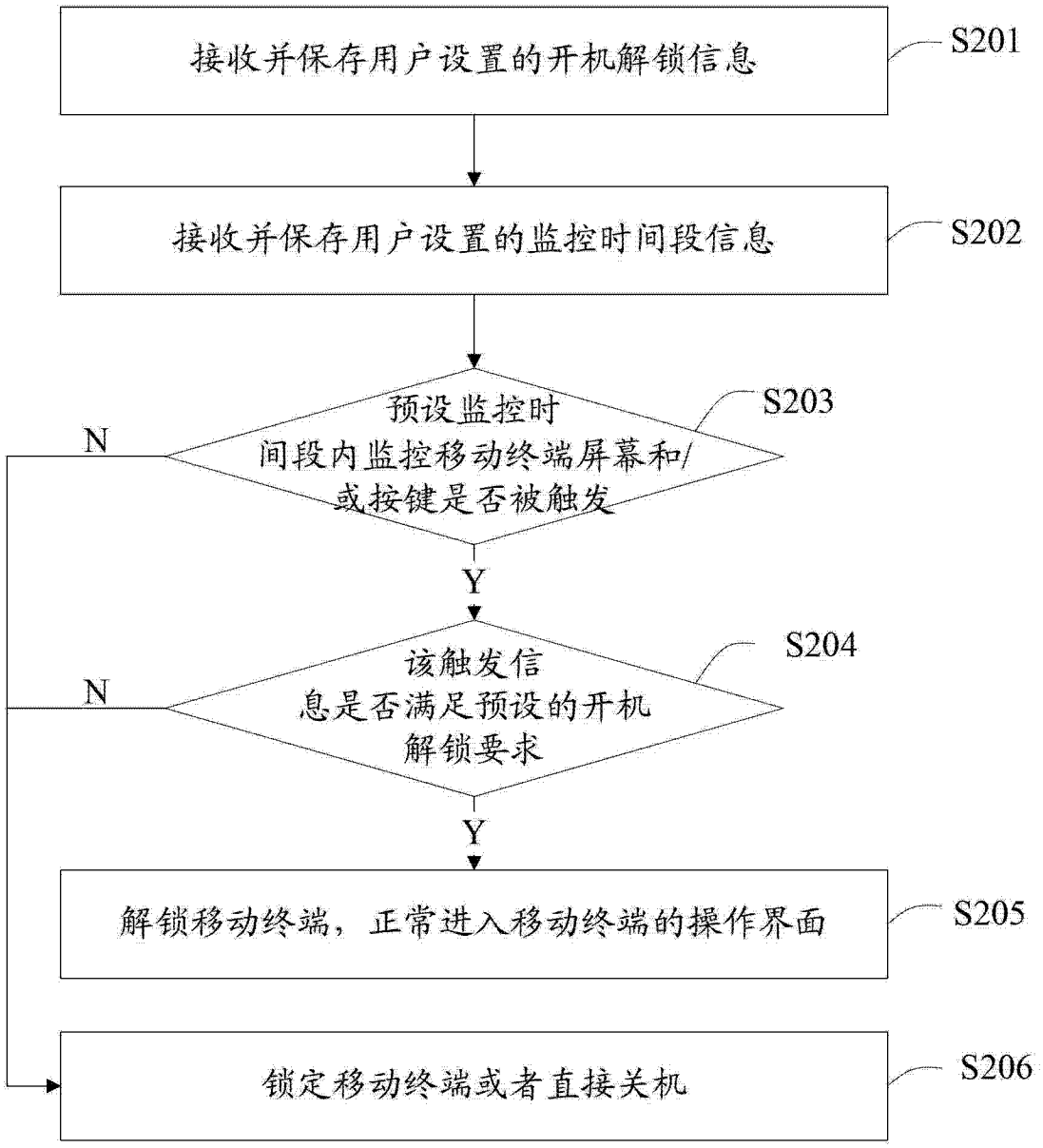

接收并保存用户设置的开机解锁信息
S201
接收并保存用户设置的监控时间段信息
S202
预设监控时间段内监控移动终端屏幕和/或按键是否被触发
S203
N
Y
该触发信息是否满足预设的开机解锁要求
S204
N
Y
解锁移动终端，正常进入移动终端的操作界面
S205
锁定移动终端或者直接关机
S206

图 2

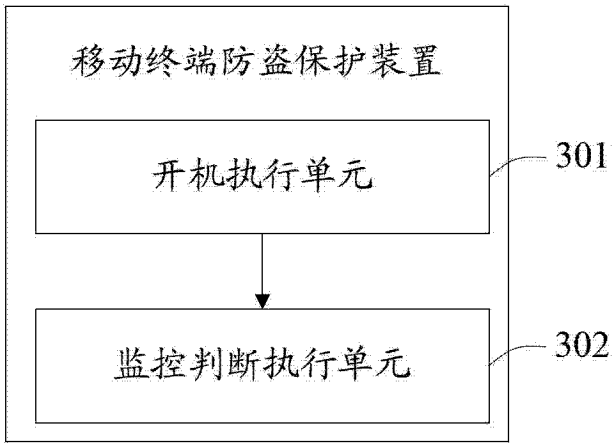

移动终端防盗保护装置
开机执行单元
301
监控判断执行单元
302

图 3

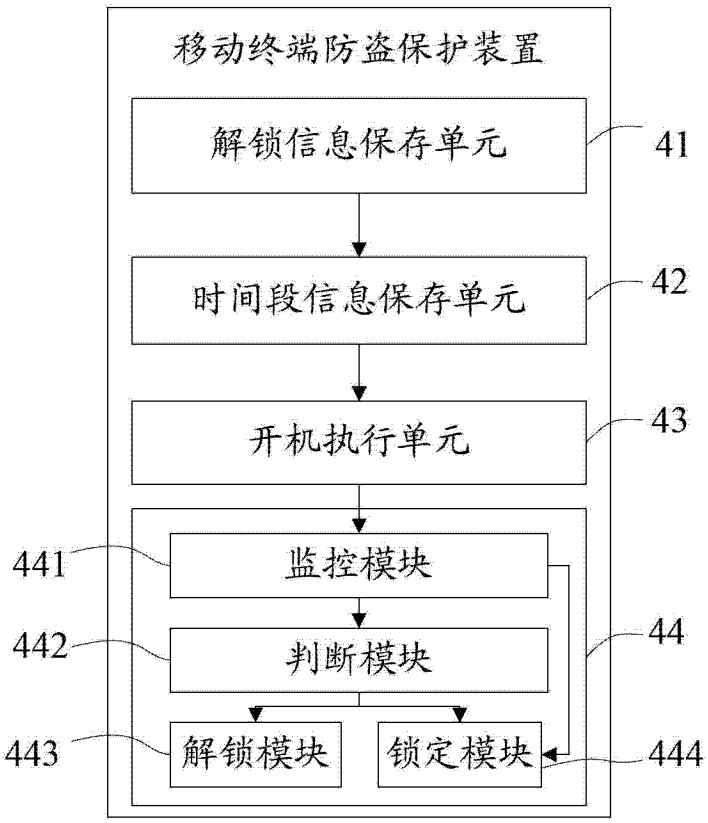

移动终端防盗保护装置
解锁信息保存单元
41
时间段信息保存单元
42
开机执行单元
43
441
监控模块
442
判断模块
44
443
解锁模块
锁定模块
444

图 4