

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 3 月 1 日 (01.03.2018)



(10) 国际公布号
WO 2018/035930 A1

(51) 国际专利分类号:
G06F 21/31 (2013.01)

(21) 国际申请号: PCT/CN2016/100778

(22) 国际申请日: 2016 年 9 月 29 日 (29.09.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610718935.2 2016 年 8 月 24 日 (24.08.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

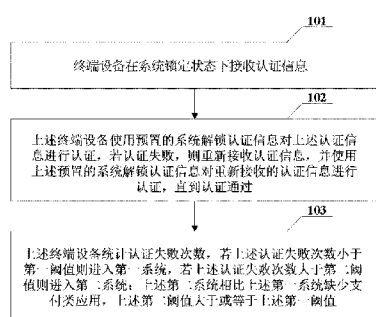
(72) 发明人: 卢乐金 (LU, Lejin); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司等 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD. et al.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST,

(54) Title: SYSTEM UNLOCKING METHOD AND DEVICE

(54) 发明名称: 一种系统解锁方法和设备



[Fig. 1]

- 101 A terminal device receives authentication information in a locked state of a system
- 102 The terminal device authenticates the authentication information by using preset system unlocking authentication information, again receives the authentication information if the authentication fails, and authenticates the again-received authentication information by using the preset system unlocking authentication information, until the authentication passes
- 103 The terminal device counts the number of times of authentication failures, the terminal device enters a first system if the number of times of authentication failures is less than a first threshold, and the terminal device enters a second system if the number of times of authentication failures is greater than a second threshold, the second system not having a payment application in comparison with the first system, and the second threshold being greater than or equal to the first threshold

(57) Abstract: A system unlocking method and device. The method comprises: a terminal device receives authentication information in a locked state of a system (101); the terminal device authenticates the authentication information by using preset system unlocking authentication information, again receives the authentication information if the authentication fails, and authenticates the again-received authentication information by using the preset system unlocking authentication information, until the authentication passes (102); and the terminal device counts the number of times of authentication failures, the terminal device enters a first system if the number of times of authentication failures is less than or equal to a first threshold, and the terminal device enters a second system if the number of times of authentication failures is greater than a second threshold, the second system not having a payment application in comparison with the first system, and the second threshold being greater than or equal to the first threshold (103). By means of the device and the method, the safety of personal property can be protected in a case in which an owner of a terminal device is forced to unlock the terminal device of the owner.

(57) 摘要: 一种系统解锁方法和设备。该方法包括: 终端设备在系统锁定状态下接收认证信息(101); 所述终端设备使用预置的系统解锁认证信息对所述认证信息进行认证, 若认证失败, 则重新接收认证信息, 并使用所述预置的系统解锁认证信息对重新接收的认证信息进行认证, 直到认证通过(102); 所述终端设备统计认证失败次数, 若所述认证失败次数小于等于第一阈值则进入第一系统, 若所述认证失败次数大于第二阈值则进入第二系统; 所述第二系统相比所述第一系统缺少支付类应用, 所述第二阈值大于或等于所述第一阈值(103)。该设备和方法使得终端设备拥有者被迫对其终端设备进行解锁的情况下可以保护其个人财产的安全。

SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

一种系统解锁方法和设备

- [1] 本申请要求于2016年8月24日提交中国专利局，申请号为201610718935.2、发明名称为“一种系统解锁方法和设备”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

- [2] 本发明涉及通信技术领域，特别涉及一种系统解锁的方法和设备。

背景技术

- [3] 随着通信技术的发展，各种终端设备已经越来越普及，例如手机、平板电脑等已经成为日常生活中必不可少的部分。同时，越来越多的人喜欢使用通信终端设备上的微信支付、手机银行、支付宝等应用进行支付。
- [4] 为了保护用户在使用中的信息的安全和支付安全，很多终端设备安装了相关的锁屏以及解锁程序，锁屏以及解锁程序在终端屏幕上运行，显示相关的解锁界面，用户输入的认证信息通过认证后才能成功进入系统。
- [5] 在现有技术中，通常通信终端设备只能设置一个解锁界面以及对应的密码，当终端设备的拥有者在人身安全受到限制和威胁的情况下，可能会被迫说出密码或对终端设备进行解锁。当受侵害人被迫解锁终端设备后，侵害人就可以操作受侵害人的终端设备登陆支付应用程序进行转账等操作。目前终端设备采用的解锁方式有：数字密码、手势图案、滑动解锁等，这些解锁方式在终端设备的拥有者被迫对其终端设备进行解锁的情况下不能有效阻止不法者进行转账等操作。

对发明的公开

发明内容

- [6] 本发明实施例提供了一种系统解锁的方法和设备，以期在终端设备拥有者被迫对其终端设备进行解锁的情况下保护其个人财产的安全。
- [7] 本发明实施例一方面提供了一种系统解锁的方法，包括：
- [8] 终端设备在系统锁定状态下接收认证信息；

- [9] 所述终端设备使用预置的系统解锁认证信息对所述认证信息进行认证，若认证失败，则重新接收认证信息，并使用所述预置的系统解锁认证信息对重新接收的认证信息进行认证，直到认证通过；
- [10] 所述终端设备统计认证失败次数，若所述认证失败次数小于第一阈值则进入第一系统，若所述认证失败次数大于第二阈值则进入第二系统；所述第二系统相比所述第一系统缺少支付类应用，所述第二阈值大于或等于所述第一阈值。
- [11] 在一个可选的实现方式中，所述终端设备在系统锁定状态下接收认证信息之前，所述方法还包括：
- [12] 所述终端设备接收到解锁指令后显示认证界面。
- [13] 在一个可选的实现方式中，若所述认证失败次数大于所述第二阈值则进入第二系统之前，所述方法还包括：
- [14] 所述终端设备冻结并隐藏所述支付类应用。
- [15] 在一个可选的实现方式中，在认证失败之后，所述方法还包括：
- [16] 输出提示信息，提示是否更换认证方式；
- [17] 若接收到更换指令，则将当前使用的认证方式更换为所述更换指令所指定的认证方式，然后执行所述重新接收认证信息。
- [18] 在一个可选的实现方式中，所述终端设备进入第二系统之后，所述方法还包括：
- [19] 所述终端设备向预置的目标终端发送所述终端设备的位置信息和报警信息。
- [20] 相应地，本发明实施例还公开了一种终端设备，包括：
- [21] 接收单元，设置为终端设备在系统锁定状态下，接收认证信息；在认证失败后，重新接收认证信息；
- [22] 认证单元，设置为使用预置的系统解锁认证信息对所述认证信息进行认证；
- [23] 统计单元，设置为统计认证失败次数；
- [24] 执行单元，设置为若所述认证失败次数小于第一阈值则进入第一系统，若所述认证失败次数大于所述第二阈值则进入第二系统；所述第二系统相比所述第一系统缺少支付类应用，所述第二阈值大于或等于所述第一阈值；
- [25] 在一个可选的实现方式中，所述接收单元，还设置为接收解锁指令；所述设备

还包括：

- [26] 显示单元，设置为在所述接收单元接收到解锁指令之后显示认证界面。
- [27] 在一个可选的实现方式中，所述设备还包括：
- [28] 应用控制单元，设置为若所述认证失败次数大于所述第二阈值则进入第二系统之前冻结并隐藏所述终端设备中的支付类应用。
- [29] 在一个可选的实现方式中，所述设备还包括：
- [30] 输出单元，设置为认证失败之后输出提示信息，提示是否更换认证方式；
- [31] 所述接收单元，还设置为接收更换指令；
- [32] 认证控制单元，设置为若所述接收单元接收到所述更换指令，则将当前使用的认证方式更换为所述更换指令所指定的认证方式；
- [33] 所述接收单元，还设置为在当前使用的认证方式更换为所述更换指令所指定的认证方式之后，重新接收认证信息。
- [34] 在一个可选的实现方式中，所述设备还包括：
- [35] 定位单元，设置为定位所述终端设备的位置信息。
- [36] 发送单元，设置为在所述终端设备进入第二系统之后，向预置的目标终端发送所述终端设备的位置信息和报警信息。
- [37] 可以看出，本实施例的方法提供了一种可以冻结并隐藏支付类应用的解锁方法。在终端设备拥有者被迫对其终端设备进行解锁的情况下通过简单的操作就可以冻结并隐藏支付类应用进而保护其个人财产的安全。

附图说明

- [38] 为了更清楚地说明本发明实施例中的技术方法，下面将对实施例中所需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它的附图。
- [39] 图1是本发明实施例系统解锁方法的流程示意图；
- [40] 图2为本发明实施例终端设备结构示意图；
- [41] 图3为本发明实施例终端设备结构示意图；
- [42] 图4为本发明实施例终端设备结构示意图；

[43] 图5为本发明实施例终端设备结构示意图；

[44] 图6为本发明实施例终端设备结构示意图；

[45] 图7为本发明实施例终端设备结构示意图；

[46] 图8为本发明实施例终端设备结构示意图。

具体实施方式

[47] 为了使本发明的目的、技术方法和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部份实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[48] 本发明实施例提供了一种系统解锁方法，如图1所示，包括：

[49] 101：终端设备在系统锁定状态下接收认证信息；

[50] 其中，终端设备例如可以是手机、平板电脑、笔记本电脑、掌上电脑等。

[51] 系统锁定状态是终端设备未解锁的状态，在该状态下终端设备通常处于待机状态。认证信息是解除终端设备的锁定状态所需的验证信息。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。认证方式例如可以是滑动解锁、指纹解锁、语音解锁等。例如终端设备的认证方式是指纹解锁，则对应的认证信息就是指纹。认证方式和对应的认证信息本发明实施例不作唯一性限定。

[52] 终端设备在系统锁定状态下接收认证信息可以没有认证界面即手机处于黑屏状态。用户可以在终端设备处于黑屏状态的时候输入认证信息进行认证，例如在黑屏状态下通过指纹解锁。

[53] 102：上述终端设备使用预置的系统解锁认证信息对上述认证信息进行认证，若认证失败，则重新接收认证信息，并使用上述预置的系统解锁认证信息对重新接收的认证信息进行认证，直到认证通过。

[54] 预置的系统解锁认证信息是在终端设备本地存储的认证信息，用于对用户输入的认证信息进行认证。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。本发明实施例并不重点关注如何进行认证，因此在此对此不作详述。若认证失败，用户需要重新输入认证信息，终

端设备对重新接收的认证信息进行认证，认证失败一次用户需要重新输入一次，直到认证通过。若在认证成功前不再输入认证信息，则终端设备等待一定时间之后，进入待机状态。

[55] 103: 上述终端设备统计认证失败次数，若上述认证失败次数小于第一阈值则进入第一系统，若上述认证失败次数大于第二阈值则进入第二系统；上述第二系统相比上述第一系统缺少支付类应用，上述第二阈值大于或等于上述第一阈值。

[56] 第一系统是正常启动之后的系统，第二系统中的支付类应用处于冻结并隐藏的状态，也就是终端设备系统中的支付类应用是冻结的且在系统中找不到。

[57] 支付类应用指的是支付宝、微信支付、手机银行等在通信终端设备上使用的应用程序。

[58] 第一阈值例如可以是2、3、4、5、6等正整数，第二阈值例如可以是2、3、4、5、6、7等正整数。第二阈值大于或等于第一阈值，若第二阈值等于第一阈值，例如第一阈值和第二阈值都是3，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于3则进入第二系统，如果认证失败次数等于3则不作限定，既可以进第一系统也可以进第二系统；若第二阈值大于第一阈值，例如第一阈值是3，第二阈值是4，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于4则进入第二系统，如果认证失败次数是3或4时则不作限定，既可以进第一系统也可以进第二系统。

[59] 举例来说，当第一阈值和第二阈值都是3时，如果第4次认证成功，则进入第二系统，在此系统中可以看到并操作除支付类外的所有应用；如果第2次认证成功，则进入第一系统即正常启动系统。

[60] 可以看出，本实施例提供了可以冻结并隐藏支付类应用的解锁方法。在终端设备拥有者被迫对其终端设备进行解锁的情况下通过简单的操作就可以冻结并隐藏支付类应用进而保护其个人财产的安全。

[61] 为了进一步方便用户解锁终端设备和支持多种认证方式，本发明实施例在前实施例的基础上提供了另一种接收认证信息的方法，具体如下：在上述终端设备在系统锁定状态下接收认证信息之前，上述方法还包括：

[62] 上述终端设备接收到解锁指令后显示认证界面。

[63] 本发明实施例提供的接收认证信息的方法是为了方便用户解锁终端设备和支持多种认证方式。本发明实施例中的终端设备在接收到解锁指令后显示认证界面，认证界面可以有多种形式，例如可以是指纹解锁、图案解锁、语音解锁等。

[64] 举例来说，用户在终端设备的显示屏上显示出认证界面后，根据认证界面的情况输入相应的认证信息，若认证失败则重新输入认证信息。例如，用户点亮终端设备显示屏后，通过相应解锁操作，终端设备就可以显示出解锁界面，然后用户就可以输入相应认证信息进行认证。若认证成功之后，则进入相应系统；若认证不成功，重新输入认证信息进行认证。

[65] 本发明实施例提供的接收认证信息的方法更加简单且支持多种认证方式。

[66] 本发明实施例在前述实施例基础上提供了配置安全系统的方法，具体如下：若上述认证失败次数大于上述第二阈值则进入第二系统之前，上述方法还包括：

[67] 上述终端设备冻结并隐藏上述支付类应用。

[68] 上述第二系统就是配置后的安全系统，在第二系统中的支付类应用处于冻结并隐藏的状态，在第二系统中找不到支付类应用，因此就算终端设备解锁成功也不能进行转账等操作。

[69] 举例来说，如果用户的认证失败次数大于第二阈值，终端设备先将支付类应用冻结并隐藏起来，然后再进入认证成功后的第二系统。在实际的认证过程中，第二系统的配置过程即终端设备中支付类应用的冻结并隐藏的过程非常快，用户不会注意到这一过程。以手机为例，认证成功之后，如果手机统计的认证失败的次数大于第二阈值时，那么手机中的支付宝、手机银行、微信支付等支付类应用冻结并且在手机中是找不到的。

[70] 本发明实施例提供的配置安全系统的方法十分隐蔽迅速并能有效阻止用户被迫解锁终端设备后的非法转账等操作。

[71] 本发明实施例在前实施例的基础上还提供了一种更换认证方式的方法，具体如下：在认证失败之后，上述方法还包括：

[72] 输出提示信息，提示是否更换认证方式；

[73] 若接收到更换指令，则将当前使用的认证方式更换为上述更换指令所指定的认

证方式，然后执行上述重新接收认证信息。

[74] 认证方式可以有多种，例如指纹解锁、图案解锁、语音解锁等。终端设备中可以设置多种认证方式，一方面用户如果忘记终端设备当前的认证信息还可以更换另外的认证方式；另一方面用户在被迫解锁终端设备的时候可以选择更容易认证失败的认证方式。对于本发明实施例来说，认证方式至关重要，如果终端设备只有一种认证方式且认证方式很难故意认证失败，本发明实施例的方法就失去了意义。例如，如果终端设备只有指纹解锁这一种认证方式并且指纹认证十分准确，用户在被迫解锁终端设备时很难使得认证失败的次数达到上述第二阈值。

[75] 举例来说，终端设备中可以设置图案解锁、指纹解锁和语音解锁等三种认证方式，默认的认证方式是指纹解锁。若用户在安全的情况下，他可以选择使用指纹解锁也可以在认证失败后选择另外的认证方式；若用户在被迫解锁的情况下，他可以故意认证失败再选择容易故意认证失败的图案解锁方式。

[76] 本发明实施例中认证失败的次数是累加的，认证失败次数是不同认证方式下认证失败次数的总和。这样更容易达到上述第二阈值，导致终端设备进入第二系统。

[77] 本发明实施例提供的更换认证方式的方法，不仅丰富了认证方式，也提高了本发明实施例方法的实用价值。

[78] 本发明实施例在前实施例的基础上还提供了一种报警方法，具体如下：上述终端设备进入第二系统之后，上述方法还包括：

[79] 上述终端设备向预置的目标终端发送上述终端设备的位置信息和报警信息。

[80] 其中，预置的目标终端可以是用户预先设置的警察局等机构的终端设备也可以是其它终端设备。报警信息用来说明终端设备的用户处于危险之中且需要帮助。报警信息可以包括用户的身份信息、体征信息、相貌信息等。位置信息准确定位终端设备的位置。终端设备定时向预置的目标终端设备发送位置信息，不断通知预置的目标终端终端设备的位置信息。

[81] 上述终端设备向预置的目标终端发送上述终端设备的位置信息和报警信息通过隐蔽的方式进行，终端设备并不显示相应信息。

- [82] 本发明实施例提供的报警方法可以隐蔽的将终端设备的位置信息和报警信息发送给预置的目标终端，从而帮助受害者及时被解救。
- [83] 本发明实施例还提供了一种终端设备，如图2所示，包括：
- [84] 接收单元201，设置为终端设备在系统锁定状态下，接收认证信息；在认证失败后，重新接收认证信息；
- [85] 认证单元202，设置为使用预置的系统解锁认证信息对上述认证信息进行认证；
- [86] 统计单元203，设置为统计认证失败次数；
- [87] 执行单元204，设置为若上述认证失败次数小于第一阈值则进入第一系统，若上述认证失败次数大于上述第二阈值则进入第二系统；上述第二系统相比上述第一系统缺少支付类应用，上述第二阈值大于或等于上述第一阈值。
- [88] 其中，终端设备例如可以是手机、平板电脑、笔记本电脑、掌上电脑、MID等。
- [89] 系统锁定状态是终端设备未解锁的状态，在该状态下终端设备通常处于待机状态。认证信息是解除终端设备的锁定状态所需的验证信息。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。认证方式例如可以是滑动解锁、指纹解锁、语音解锁等。例如终端设备的认证方式是指纹解锁，则对应的认证信息就是指纹。认证方式和对应的认证信息本发明实施例不作唯一性限定。接收单元201设置为接收认证信息，认证信息可以是多种形式。
- [90] 终端设备在系统锁定状态下接收认证信息可以没有认证界面即手机处于黑屏状态。用户可以在终端设备处于黑屏状态的时候输入认证信息进行认证，例如在黑屏状态下通过指纹解锁。
- [91] 预置的系统解锁认证信息是在终端设备本地存储的认证信息，用于与用户输入的认证信息进行认证。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。认证单元202使用预置的系统解锁认证信息与上述认证信息进行认证。本发明实施例并不重点关注如何进行认证，因此在此对此不作详述。若认证失败，用户需要重新输入认证信息，终端设备对

重新接收的认证信息进行认证，认证失败一次用户需要重新输入一次，直到认证通过。若在认证成功前不再输入认证信息，则终端设备等待一定时间之后，进入待机状态。

[92] 第一系统是正常启动之后的系统，第二系统中的支付类应用处于冻结并隐藏的状态，也就是终端设备系统中的支付类应用是冻结的且在系统中找不到。

[93] 支付类应用指的是支付宝、微信支付、手机银行等在通信终端上使用的应用程序。

[94] 第一阈值例如可以是2、3、4、5、6等正整数，第二阈值例如可以是2、3、4、5、6、7等正整数。第二阈值大于或等于第一阈值，若第二阈值等于第一阈值，例如第一阈值和第二阈值都是3，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于3则进入第二系统，如果认证失败次数等于3则不作限定，既可以进第一系统也可以进第二系统；若第二阈值大于第一阈值，例如第一阈值是3，第二阈值是4，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于4则进入第二系统，如果认证失败次数是3或4时则不作限定，既可以进第一系统也可以进第二系统；

[95] 举例来说，当第一阈值和第二阈值都是3时，如果第4次认证成功，则进入第二系统，在此系统中可以看到并操作除支付类外的所有应用；如果第2次认证成功，则进入第一系统即正常启动系统。

[96] 可以看出，本实施例的方法提供了一种可以冻结并隐藏支付类应用的解锁方式。在移动终端拥有者被迫对其移动终端进行解锁的情况下通过简单的操作就可以冻结并隐藏支付类应用进而保护其个人财产的安全。

[97] 本发明实施例在前实施例的基础上还提供了另一种接收认证信息的方法，具体如下：进一步地，如图3所示，上述设备还包括：

[98] 所述接收单元，还设置为接收解锁指令；

[99] 显示单元301，设置为在上述接收单元接收到上述解锁指令之后显示认证界面。

[100] 本发明实施例提供的接收认证信息的方法是为了方便用户解锁终端设备和支持多种认证方式。本发明实施例中的终端设备在接收到指令后显示认证界面，认

证界面可以有多种形式，例如可以是指纹解锁、图案解锁、语音解锁等。

[101] 举例来说，用户在终端设备的显示屏上显示出认证界面后，根据认证界面的情况输入相应的认证信息，若认证失败则重新输入认证信息。例如，用户点亮终端设备显示屏后，通过相应解锁操作，终端设备就可以显示出解锁界面，然后用户就可以输入相应认证信息进行认证。若认证成功之后，则进入相应系统；若认证不成功，重新输入认证信息进行认证。

[102] 本发明实施例提供的接收认证信息的方法更加简单且支持多种认证方式。

[103] 本发明实施例在前实施例的基础上还提供了一种配置安全系统的方法，具体如下：进一步地，如图4所示，上述终端设备还包括：

[104] 冻结与隐藏单元401，设置为若上述认证失败次数大于上述第二阈值则进入第二系统之前冻结并隐藏上述终端设备中的支付类应用。

[105] 上述第二系统就是配置的安全系统，在第二系统中的支付类应用处于冻结并隐藏的状态，在第二系统中找不到支付类应用，因此就算终端设备解锁成功也不能进行转账等操作。

[106] 举例来说，如果用户的认证失败次数大于第二阈值，终端设备先将支付类应用冻结并隐藏起来，然后再进入认证成功后的第二系统。在实际的认证过程中，第二系统的配置过程即终端设备中的支付类应用的冻结并隐藏的过程非常快，用户不会注意到这一过程。以手机为例，认证成功之后，如果手机统计的认证失败的次数大于第二阈值时，手机中的支付宝、手机银行、微信支付等支付类应用在手机中是找不到的。

[107] 本发明实施例提供的配置安全系统的方法十分隐蔽迅速并能有效阻止用户被迫解锁终端设备后的非法转账等操作。

[108] 本发明实施例在前实施例的基础上还提供了一种更换认证方式的方法，具体如下：进一步地，如图5所示，上述设备还包括：

[109] 输出单元501，设置为认证失败之后输出提示信息，提示是否更换认证方式；

[110] 所述接收单元201，还设置为接收更换指令；

[111] 更换单元502，设置为若接收到上述更换指令，则将当前使用的认证方式更换为上述更换指令所指定的认证方式；

- [112] 上述接收单元201，还设置为当前使用的认证方式更换为上述更换指令所指定的认证方式之后重新接收认证信息。
- [113] 认证方式可以有多种，例如指纹解锁、图案解锁、语音解锁等。终端设备中可以设置多种认证方式，一方面用户如果忘记终端设备当前的认证信息还可以更换另外的认证方式；另一方面用户在被迫解锁终端设备的时候可以选择更容易认证失败的认证方式。对于本发明实施例来说，认证方式至关重要，如果终端设备只有一种认证方式且认证方式很难故意认证失败，本发明实施例的方法就失去了意义。例如，如果终端设备只有指纹解锁这一种认证方式并且指纹认证十分准确，用户在被迫解锁终端设备时很难使得认证失败的次数达到上述第二阈值。
- [114] 举例来说，终端设备中可以设置图案解锁、指纹解锁和语音解锁等三种认证方式，默认的认证方式是指纹解锁。若用户在安全的情况下，他可以选择使用指纹解锁也可以在认证失败之后选择另外的认证方式；若用户在被迫解锁的情况下，他可以故意认证失败选择容易故意认证失败的图案解锁方式。
- [115] 本发明实施例中认证失败的次数是累加的，认证失败次数是不同认证方式下认证失败次数的总和。这样更容易达到上述第二阈值，导致终端设备进入第二系统。
- [116] 本发明实施例提供的更换认证方式的方法，不仅丰富了认证方式，也提高了本发明实施例方法的实用价值。
- [117] 本发明实施例在前实施例的基础上提供了一种报警方法，具体如下：进一步地，如图6所示，上述设备还包括：
- [118] 发送单元601，设置为上述终端设备进入第二系统之后，向预置的目标终端发送上述终端设备的位置信息和报警信息。
- [119] 定位单元602，设置为定位上述终端设备的位置信息。
- [120] 其中，预置的目标终端可以是用户预设置的警察局的终端设备也可以是其它终端。报警信息用来说明终端设备的用户处于危险之中需要帮助，可以包括用户的身份信息、体征信息、相貌信息等。位置信息准确定位终端设备的位置。终端设备定时向预置的目标终端发送位置信息，不断通知预置的目标终端终端设

备的位置信息。

[121] 上述终端设备向预置的目标终端发送上述终端设备的位置信息和报警信息通过隐蔽的方式进行，终端设备并不显示相应信息。

[122] 本发明实施例提供的报警方法可以隐蔽的将终端设备的位置信息和报警信息发送给预置的目标终端，帮助受害者及时脱离危险。

[123] 本发明实施例还提供了一种终端设备，如图7所示，包括：处理器701以及存储器702、输入设备703、输出设备704；其中存储器702可以用于提供处理器701执行数据处理所需要的缓存和预置的系统解锁认证信息的本地缓存，还可以用于提供处理器701执行数据处理调用的数据以及获得的结果数据的存储空间；其中输入设备703用于在终端设备处于锁定状态下接收认证信息，还用于认证失败后重新接收认证信息和接收更改指令；输出设备704用于输出提示消息和认证界面，还用于向预置的目标终端发送上述终端设备的位置信息和报警信息。

[124] 其中，上述处理器701，用于在终端设备处于锁定状态下，获取认证信息；使用预置的系统解锁认证信息对上述认证信息进行认证，若认证失败，则重新接收认证信息，并使用上述预置的系统解锁认证信息对重新接收的认证信息进行认证，直到认证通过；统计认证失败次数，若上述认证失败次数小于第一阈值则进入第一系统，若上述认证失败次数大于第二阈值则进入第二系统；上述第二系统相比上述第一系统缺少支付类应用，上述第二阈值大于或等于上述第一阈值。

[125] 其中，终端设备例如可以是手机、平板电脑、笔记本电脑、掌上电脑、MID等。

[126] 系统锁定状态是终端设备未解锁的状态，在该状态下终端设备通常处于待机状态。认证信息是解除终端设备的锁定状态所需的验证信息。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。认证方式例如可以是滑动解锁、指纹解锁、语音解锁等。例如终端设备的认证方式是指纹解锁，则对应的认证信息就是指纹。认证方式和对应的认证信息本发明实施例不作唯一性限定。

[127] 终端设备在系统锁定状态下接收认证信息可以没有认证界面即手机处于黑屏状

态。用户可以在终端设备处于黑屏状态的时候输入认证信息进行认证，例如在黑屏状态下通过指纹解锁。

[128] 预置的系统解锁认证信息是在终端设备本地存储的认证信息，用于与用户输入的认证信息进行认证。认证信息可以是字符串、指纹、语音等中的一种或多种，它与终端设备解锁的认证方式相对应。本发明实施例并不重点关注如何进行认证，因此在此对此不作详述。若认证失败，用户需要重新输入认证信息，终端设备对重新接收的认证信息进行认证，认证失败一次用户需要重新输入一次，直到认证通过。若在认证成功前不再输入认证信息，则终端设备等待一定时间之后，进入待机状态。

[129] 第一系统是正常启动之后的系统，第二系统中的支付类应用处于冻结并隐藏的状态，也就是终端设备系统中的支付类应用是冻结的且在系统中看不到。

[130] 支付类应用指的是支付宝、微信支付、手机银行等在通信终端上使用的应用程序。

[131] 第一阈值例如可以是2、3、4、5、6等正整数，第二阈值例如可以是2、3、4、5、6、7等正整数。第二阈值大于或等于第一阈值，若第二阈值等于第一阈值，例如第一阈值和第二阈值都是3，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于3则进入第二系统，如果认证失败次数等于3则不作限定，既可以进第一系统也可以进第二系统；若第二阈值大于第一阈值，例如第一阈值是3，第二阈值是4，如果认证失败次数小于3则进入第一系统，如果认证失败次数大于4则进入第二系统，如果认证失败次数是3或4时则不作限定，既可以进第一系统也可以进第二系统；

[132] 举例来说，当第一阈值和第二阈值都是3时，如果第4次认证成功，则进入第二系统，在此系统中可以看到并操作除支付类外的所有应用；如果第2次认证成功，则进入第一系统即正常启动系统。

[133] 可以看出，本实施例的方法提供了一种可以冻结并隐藏支付类应用的解锁方式。在终端设备拥有者被迫对其终端设备进行解锁的情况下通过简单的操作就可以冻结并隐藏支付类应用进而保护其个人财产的安全。

[134] 本发明实施例还进一步提供了一种接收认证信息的实现方法，具体如下：上述

处理器701，还用于在上述接收单元接收到解锁指令之后显示认证界面。

[135] 本发明实施例提供的接收认证信息的方法是为了方便用户解锁终端设备和支持多种认证方式。本发明实施例中的终端设备在接收到指令后显示认证界面，认证界面可以有多种形式，例如可以是指纹解锁、图案解锁、语音解锁等。

[136] 举例来说，用户在终端设备的显示屏上显示出认证界面后，根据认证界面的情况输入相应的认证信息，若认证失败则重新输入认证信息。例如，用户点亮终端设备显示屏后，通过相应解锁操作，终端设备就可以显示出解锁界面，然后用户就可以输入相应认证信息进行认证。若认证成功之后，则进入相应系统；若认证不成功，重新输入认证信息进行认证。

[137] 本发明实施例提供的接收认证信息的方法更加简单且支持多种认证方式。

[138] 本发明实施例还提供了一种配置安全系统的方法，具体如下：上述处理器701，还用于若上述认证失败次数大于上述第二阈值则进入第二系统之前冻结并隐藏上述终端设备中的支付类应用。

[139] 上述第二系统就是配置的安全系统，在第二系统中的支付类应用处于冻结并隐藏的状态。在第二系统中找不到支付类应用，因此就算终端设备解锁成功也不能进行转账等操作。

[140] 举例来说，如果用户的认证失败次数大于第二阈值，终端设备先将支付类应用冻结并隐藏起来，然后再进入认证成功后第二系统。在实际的认证过程中，第二系统的配置过程即终端设备中的支付类应用的冻结并隐藏的过程非常快，用户不会认为会有这一过程。以手机为例，认证成功之后，如果手机统计的认证失败的次数大于第二阈值时，手机中的支付宝、手机银行、微信支付等支付类应用在手机中是找不到的。

[141] 本发明实施例提供的配置安全系统的方法十分隐蔽迅速并能有效阻止用户被迫解锁终端设备后的非法转账等操作。

[142] 本发明实施例还提供了一种更换认证方式的方法，具体如下：上述处理器701，还用于认证失败之后输出提示信息，提示是否更换认证方式以及接收到更换指令后将当前使用的认证方式更换为上述更换指令所指定的认证方式并重新接收认证信息。

- [143] 认证方式可以有多种，例如指纹解锁、图案解锁、语音解锁等。终端设备中可以设置多种认证方式，一方面用户如果忘记终端设备当前的认证信息还可以更换另外的认证方式；另一方面用户在被迫解锁终端设备的时候可以选择更容易认证失败的认证方式。对于本发明实施例来说，认证方式至关重要，如果终端设备只有一种认证方式且认证方式很难故意认证失败，本发明实施例的方法就失去了意义。例如，如果终端设备只有指纹解锁这一种认证方式并且指纹认证十分准确，用户在被迫解锁终端设备时很难使得认证失败的次数达到上述第二阈值。
- [144] 举例来说，终端设备中可以设置图案解锁、指纹解锁和语音解锁等三种认证方式，默认的认证方式是指纹解锁。若用户在安全的情况下，他可以选择使用指纹解锁也可以故意认证失败选择另外的认证方式；若用户在被迫解锁的情况下，他可以故意认证失败选择容易故意认证失败的图案解锁方式。
- [145] 本发明实施例中认证失败的次数是累加的，认证失败次数是不同认证方式下认证失败次数的总和。这样更容易达到上述第二阈值，导致终端设备进入第二系统。
- [146] 本发明实施例提供的更换认证方式的方法，不仅丰富了认证方式，也提高了本发明方法的实用价值。
- [147] 本发明实施例还提供了一种报警方法，具体如下：上述处理器701，还用于在上述终端设备进入第二系统之后，向预置的目标终端发送上述终端设备的位置信息和报警信息。
- [148] 其中，预置的目标终端可以是用户预设置的警察局的终端设备也可以是其它终端。报警信息用来说明终端设备的用户处于危险之中需要帮助，可以包括用户的身份信息、体征信息、相貌信息等。位置信息准确定位终端设备的位置。终端设备定时向预置的目标终端发送位置信息，不断通知预置的目标终端终端设备的位置信息。
- [149] 上述终端设备向预置的目标终端发送上述终端设备的位置信息和报警信息通过隐蔽的方式进行，终端设备并不显示相应信息。
- [150] 本发明实施例提供的报警方法可以隐蔽的将终端设备的位置信息和报警信息发

送给预置的目标终端，能够帮助受害者及时被解救。

[151] 本发明实施例还提供了另一种终端设备，如图8所示，为了便于说明，仅示出了与本发明实施例相关的部分，具体技术细节未揭示的，请参照本发明实施例方法部分。该终端设备可以为包括手机、平板电脑、车载电脑等任意终端设备，以终端设备为手机为例。

[152] 图8示出的是与本发明实施例提供的终端设备相关的手机的部分结构的框图。参考图8，手机包括：射频（Radio Frequency，RF）电路810、存储器820、输入单元830、显示单元840、传感器850、音频电路860、无线保真（wireless fidelity，WiFi）模块870、处理器880、以及电源890等部件。本领域技术人员可以理解，图8中示出的手机结构并不构成对手机的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[153] 下面结合图8对手机的各个构成部件进行具体的介绍：

[154] RF电路810可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，给处理器880处理；另外，将设计上行的数据发送给基站。通常，RF电路810包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器（Low Noise Amplifier，LNA）、双工器等。此外，RF电路810还可以通过无线通信与网络和其它设备通信。上述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统（Global System of Mobile communication，GSM）、通用分组无线服务（General Packet Radio Service，GPRS）、码分多址（Code Division Multiple Access，CDMA）、宽带码分多址（Wideband Code Division Multiple Access，WCDMA）、长期演进（Long Term Evolution，LTE）、电子邮件、短消息服务（Short Messaging Service，SMS）等。

[155] 存储器820可用于存储软件程序以及模块，处理器880通过运行存储在存储器820的软件程序以及模块，从而执行手机的各种功能应用以及数据处理。存储器820可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据手机的使用所创建的数据（比如音频数据、电话本等）等。

此外，存储器820可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其它易失性固态存储器件。

- [156] 输入单元830可用于接收输入的数字或字符信息，以及产生与手机的用户设置以及功能控制有关的键信号输入。具体地，输入单元830可包括触控面板831以及其它输入设备832。其它输入设备832可用于接收输入的指纹、语音等信息。触控面板831，也称为触摸屏，可收集用户在其上或附近的触摸操作（比如用户使用手指、触笔等任何适合的物体或附件在触控面板831上或在触控面板831附近的操作），并根据预先设定的程式驱动相应的连接装置。可选的，触控面板831可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器880，并能接收处理器880发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板831。除了触控面板831，输入单元830还可以包括其它输入设备832。具体地，其它输入设备832可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。

- [157] 显示单元840可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元840可包括显示面板841，可选的，可以采用液晶显示器（Liquid Crystal Display, LCD）、有机发光二极管（Organic Light-Emitting Diode, OLED）等形式来配置显示面板841。进一步的，触控面板831可覆盖显示面板841，当触控面板831检测到在其上或附近的触摸操作后，传送给处理器880以确定触摸事件的类型，随后处理器880根据触摸事件的类型在显示面板841上提供相应的视觉输出。虽然在图8中，触控面板831与显示面板841是作为两个独立的部件来实现手机的输入和输出功能，但是在某些实施例中，可以将触控面板831与显示面板841集成而实现手机的输入和输出功能。

- [158] 手机还可包括至少一种传感器850，比如光传感器、运动传感器以及其它传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示面板841的亮度，接近传感器可在手机移动

到耳边时，关闭显示面板841和/或背光。作为运动传感器的一种，加速计传感器可检测各个方向上（一般为三轴）加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用（比如横竖屏切换、相关游戏、磁力计姿态校准）、振动识别相关功能（比如计步器、敲击）等；至于手机还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其它传感器，在此不再赘述。

[159] 音频电路860、扬声器861、传声器862可提供用户与手机之间的音频接口。音频电路860可将接收到的音频数据转换后的电信号，传输到扬声器861，由扬声器861转换为声音信号输出；另一方面，传声器862将收集的声音信号转换为电信号，由音频电路860接收后转换为音频数据，再将音频数据输出至处理器880处理后，经RF电路810以发送给比如另一手机，或者将音频数据输出至存储器820以便进一步处理。

[160] WiFi属于短距离无线传输技术，手机通过WiFi模块870可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图8示出了WiFi模块870，但是可以理解的是，其并不属于手机的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[161] 处理器880是手机的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器820内的软件程序和/或模块，以及调用存储在存储器820内的数据，执行手机的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器880可包括一个或多个处理单元；优选的，处理器880可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器880中。

[162] 手机还包括给各个部件供电的电源890（比如电池），优选的，电源可以通过电源管理系统与处理器880逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

[163] 尽管未示出，手机还可以包括摄像头、蓝牙模块等，在此不再赘述。

[164] 前述实施例中，各步骤方法流程可以基于该终端设备的结构实现。其中传感器

850或者触控面板831可以作为指纹采集设备使用。

[165] 值得注意的是，上述指纹解锁控制设备实施例中，所包括的各个单元只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本发明的保护范围。

[166] 另外，本领域普通技术人员可以理解实现上述各方法实施例中的全部或部分步骤是可以通过程序来指令相关的硬件完成，相应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。

[167] 以上仅为本发明实施例较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明实施例揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

权利要求书

- [权利要求 1] 一种系统解锁方法，其特征在于，包括：
- 终端设备在系统锁定状态下接收认证信息；
- 所述终端设备使用预置的系统解锁认证信息对所述认证信息进行认证，若认证失败，则重新接收认证信息，并使用所述预置的系统解锁认证信息对重新接收的认证信息进行认证，直到认证通过；
- 所述终端设备统计认证失败次数，若所述认证失败次数小于第一阈值则进入第一系统，若所述认证失败次数大于第二阈值则进入第二系统；所述第二系统相比所述第一系统缺少支付类应用，所述第二阈值大于或等于所述第一阈值。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，所述终端设备在系统锁定状态下接收认证信息之前，所述方法还包括：
- 所述终端设备接收到解锁指令后显示认证界面。
- [权利要求 3] 根据权利要求2所述的方法，其特征在于，若所述认证失败次数大于所述第二阈值则进入第二系统之前，所述方法还包括：
- 所述终端设备冻结并隐藏所述支付类应用。
- [权利要求 4] 根据权利要求1至3任意一项所述的方法，在认证失败之后，所述方法还包括：
- 输出提示信息，提示是否更换认证方式；
- 若接收到更换指令，则将当前使用的认证方式更换为所述更换指令所指定的认证方式，然后执行所述重新接收认证信息。
- [权利要求 5] 根据权利要求1至3任意一项所述的方法，其特征在于，所述终端设备进入第二系统之后，所述方法还包括：
- 所述终端设备向预置的目标终端发送所述终端设备的位置信息和报警信息。
- [权利要求 6] 一种终端设备，其特征在于，包括：
- 接收单元，设置为终端设备在系统锁定状态下，接收认证信息；

在认证失败后，重新接收认证信息；
认证单元，设置为使用预置的系统解锁认证信息对所述认证信息进行认证；
统计单元，设置为统计认证失败次数；
执行单元，设置为若所述认证失败次数小于第一阈值则进入第一系统，若所述认证失败次数大于所述第二阈值则进入第二系统；
所述第二系统相比所述第一系统缺少支付类应用，所述第二阈值大于或等于所述第一阈值。

[权利要求 7] 根据权利要求6所述的设备，其特征在于，
所述接收单元，还设置为接收解锁指令；所述设备还包括：
显示单元，设置为在所述接收单元接收到所述解锁指令之后显示认证界面。

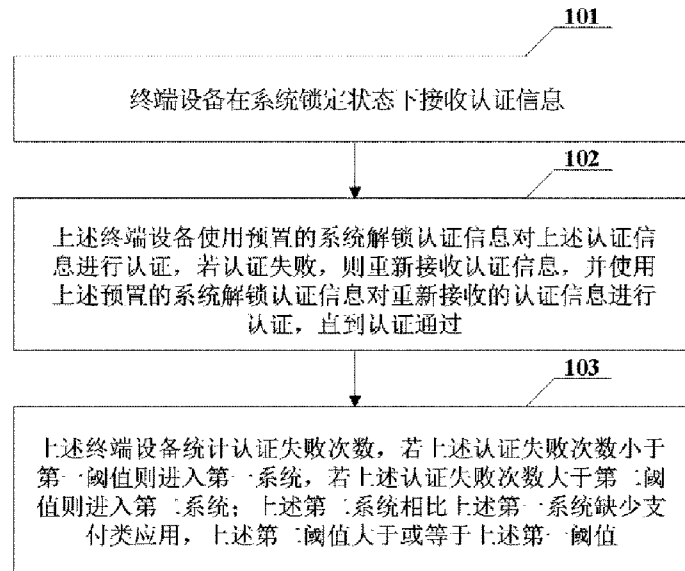
[权利要求 8] 根据权利要求7所述的设备，其特征在于，所述设备还包括：
应用控制单元，设置为若所述认证失败次数大于所述第二阈值则进入第二系统之前冻结并隐藏所述终端设备中的支付类应用。

[权利要求 9] 根据权利要求7至8任意一项所述的设备，其特征在于，所述设备还包括：
输出单元，设置为认证失败之后，输出提示信息，提示是否更换认证方式；
所述接收单元，还设置为接收更换指令；
认证控制单元，设置为若所述接收单元接收到所述更换指令，则将当前使用的认证方式更换为所述更换指令所指定的认证方式；
所述接收单元，还设置为在当前使用的认证方式更换为所述更换指令所指定的认证方式之后，重新接收认证信息。

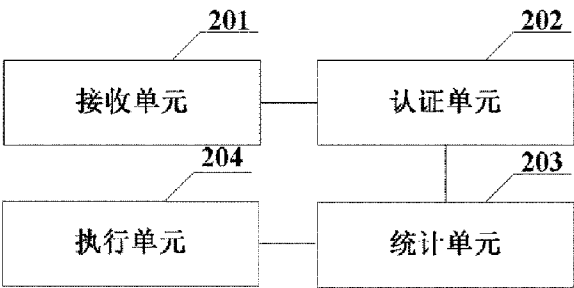
[权利要求 10] 根据权利要求7至8任意一项所述的设备，其特征在于，所述设备还包括：
定位单元，设置为定位所述终端设备的位置信息。
发送单元，设置为在所述终端设备进入第二系统之后，向预置的

目标终端发送所述终端设备的位置信息和报警信息。

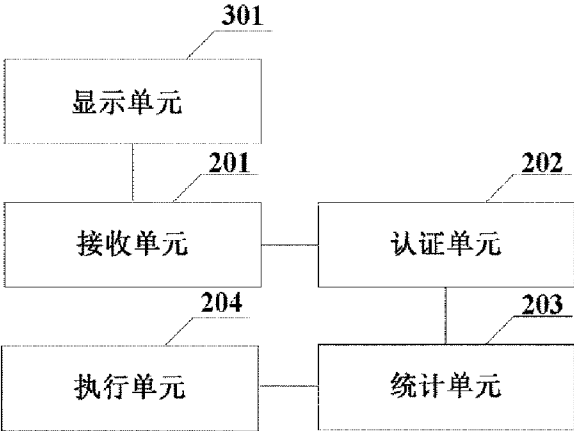
[Fig. 1]



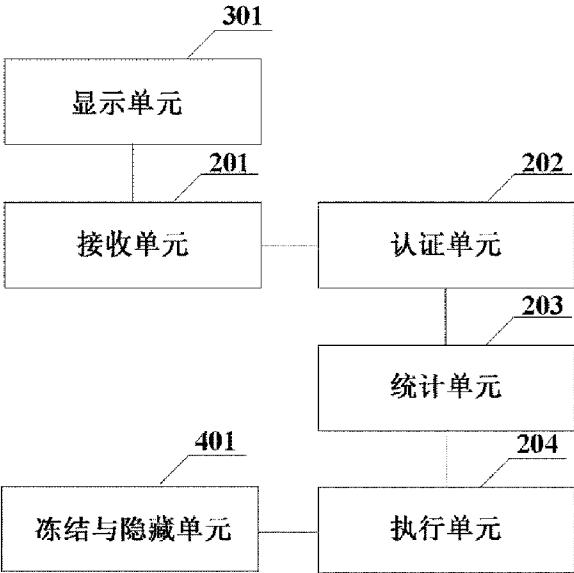
[Fig. 2]



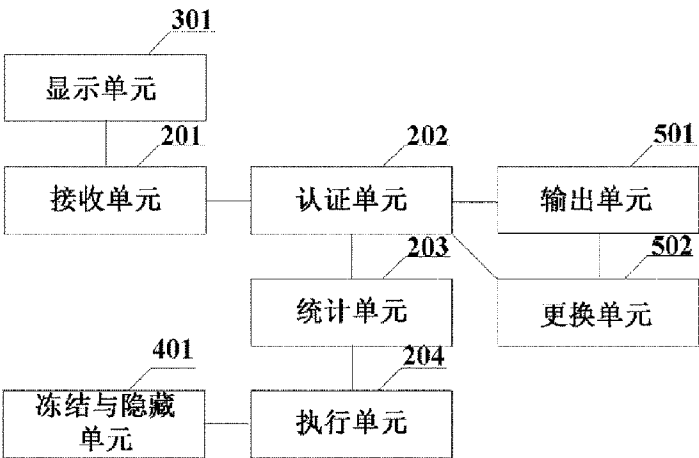
[Fig. 3]



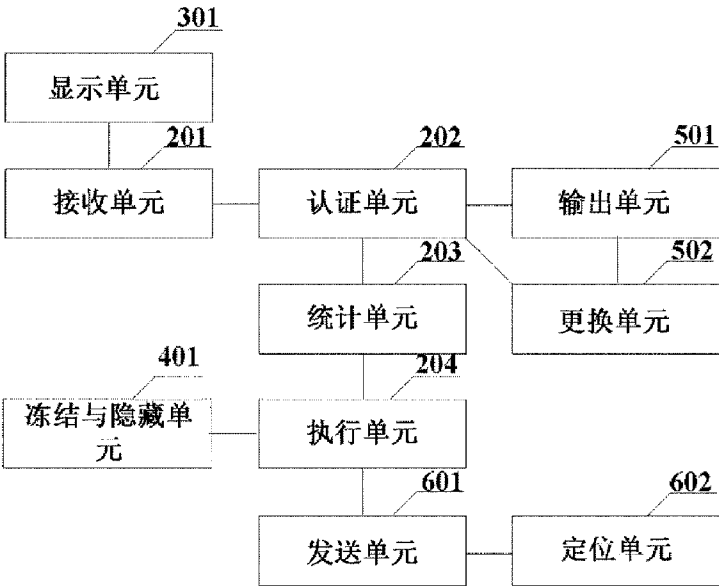
[Fig. 4]



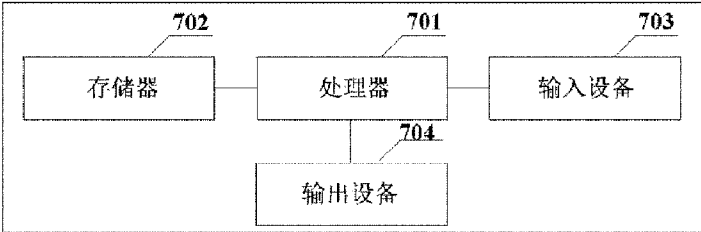
[Fig. 5]



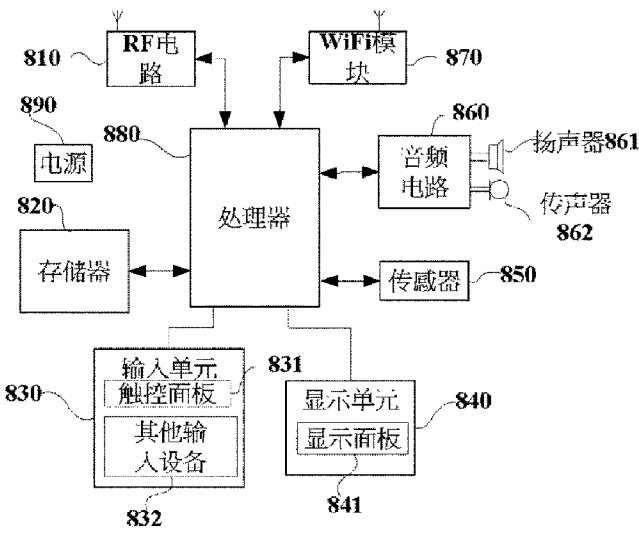
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/100778

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, IEEE: 支付, 校验, 权限, 应用受限, 限制, 功能受限, 锁屏, 鉴权, 计数, 次数, 失败, 阈值, 认证, 受限系统, 解锁, pay, count, lock, threshold, verify, function, customization

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 105574378 A (XIAOMI TECHNOLOGY CO., LTD.), 11 May 2016 (11.05.2016), description, pages 6-9, and figures 2-3	1-10
Y	CN 104361303 A (XIAOMI TECHNOLOGY CO., LTD.), 18 February 2015 (18.02.2015), description, pages 3-7, and figures 2-4 and 6-9	1-10
A	CN 101345967 A (SHENZHEN HUAWEI COMMUNICATION TECHNOLOGIES CO., LTD.), 14 January 2009 (14.01.2009), entire document	1-10
A	CN 104253818 A (HUAWEI DEVICE CO., LTD.), 31 December 2014 (31.12.2014), entire document	1-10
A	CN 1472952 A (SHARP KABUSHIKI KAISHA), 04 February 2004 (04.02.2004), entire document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

01 April 2017

Date of mailing of the international search report

16 May 2017

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer

LI, Fuyong

Telephone No. (86-10) 62413682

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/100778

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105574378 A	11 May 2016	None	
CN 104361303 A	18 February 2015	KR 20160059454 A	26 May 2016
		JP 2017500833 A	05 January 2017
		RU 2015114997 A	10 November 2016
		EP 3012766 A1	27 April 2016
		US 2016117500 A1	28 April 2016
		WO 2016061929 A1	28 April 2016
		IN 201500733 P2	26 August 2016
CN 101345967 A	14 January 2009	None	
CN 104253818 A	31 December 2014	None	
CN 1472952 A	04 February 2004	US 2004034792 A1	19 February 2004
		JP 2004032403 A	29 January 2004

A. 主题的分类 G06F 21/31 (2013.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																				
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06F, H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, CNKI, WPI, EPDOC, IEEE: 支付, 校验, 权限, 应用受限, 限制, 功能受限, 锁屏, 鉴权, 计数, 次数, 失败, 阈值, 认证, 受限系统, 解锁, pay, count, lock, threshold, verify, function, customization																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 105574378 A (小米科技有限责任公司) 2016年 5月 11日 (2016 - 05 - 11) 说明书第6-9页, 图2-3</td> <td>1-10</td> </tr> <tr> <td>Y</td> <td>CN 104361303 A (小米科技有限责任公司) 2015年 2月 18日 (2015 - 02 - 18) 说明书第3-7页, 图2-4、6-9</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 101345967 A (深圳华为通信技术有限公司) 2009年 1月 14日 (2009 - 01 - 14) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 104253818 A (华为终端有限公司) 2014年 12月 31日 (2014 - 12 - 31) 全文</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 1472952 A (夏普株式会社) 2004年 2月 4日 (2004 - 02 - 04) 全文</td> <td>1-10</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	CN 105574378 A (小米科技有限责任公司) 2016年 5月 11日 (2016 - 05 - 11) 说明书第6-9页, 图2-3	1-10	Y	CN 104361303 A (小米科技有限责任公司) 2015年 2月 18日 (2015 - 02 - 18) 说明书第3-7页, 图2-4、6-9	1-10	A	CN 101345967 A (深圳华为通信技术有限公司) 2009年 1月 14日 (2009 - 01 - 14) 全文	1-10	A	CN 104253818 A (华为终端有限公司) 2014年 12月 31日 (2014 - 12 - 31) 全文	1-10	A	CN 1472952 A (夏普株式会社) 2004年 2月 4日 (2004 - 02 - 04) 全文	1-10
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
Y	CN 105574378 A (小米科技有限责任公司) 2016年 5月 11日 (2016 - 05 - 11) 说明书第6-9页, 图2-3	1-10																		
Y	CN 104361303 A (小米科技有限责任公司) 2015年 2月 18日 (2015 - 02 - 18) 说明书第3-7页, 图2-4、6-9	1-10																		
A	CN 101345967 A (深圳华为通信技术有限公司) 2009年 1月 14日 (2009 - 01 - 14) 全文	1-10																		
A	CN 104253818 A (华为终端有限公司) 2014年 12月 31日 (2014 - 12 - 31) 全文	1-10																		
A	CN 1472952 A (夏普株式会社) 2004年 2月 4日 (2004 - 02 - 04) 全文	1-10																		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																				
国际检索实际完成的日期 2017年 4月 1日		国际检索报告邮寄日期 2017年 5月 16日																		
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 李福永 电话号码 (86-10) 62413682																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/100778

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105574378	A	2016年 5月 11日	无			
CN	104361303	A	2015年 2月 18日	KR	20160059454	A	2016年 5月 26日
				JP	2017500833	A	2017年 1月 5日
				RU	2015114997	A	2016年 11月 10日
				EP	3012766	A1	2016年 4月 27日
				US	2016117500	A1	2016年 4月 28日
				WO	2016061929	A1	2016年 4月 28日
				IN	201500733	P2	2016年 8月 26日
CN	101345967	A	2009年 1月 14日	无			
CN	104253818	A	2014年 12月 31日	无			
CN	1472952	A	2004年 2月 4日	US	2004034792	A1	2004年 2月 19日
				JP	2004032403	A	2004年 1月 29日