

(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
2016 年 10 月 20 日 (20.10.2016)



(10) 国际公布号
WO 2016/165161 A1

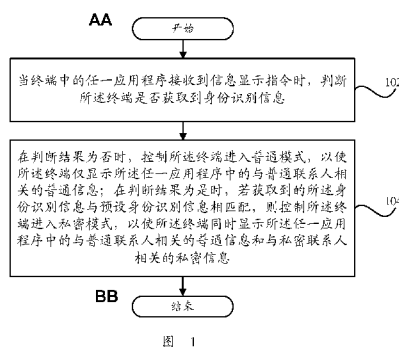
- (51) 国际专利分类号:
H04L 29/06 (2006.01) G06F 21/62 (2013.01)
G06F 21/31 (2013.01)
- (21) 国际申请号: PCT/CN2015/077953
- (22) 国际申请日: 2015 年 4 月 30 日 (30.04.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510179281.6 2015 年 4 月 15 日 (15.04.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
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: 郭雄伟 (GUO, Xiongwei); 中国广东省深圳
市南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 傅文治 (FU, Wenzhi); 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: 广州三环专利代理有限公司 (GUANG-
ZHOU SCIHEAD PATENT AGENT CO., LTD); 中
国广东省广州市越秀区先烈中路 80 号汇华商贸大厦
1508 室, Guangdong 510070 (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, 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, 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,
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)。

[见续页]

(54) Title: INFORMATION DISPLAY METHOD, INFORMATION DISPLAY DEVICE, AND TERMINAL

(54) 发明名称: 信息显示方法、信息显示装置和终端



102 When any application program in terminal receives information display command, determine whether terminal has obtained identity identification information

104 When determination result is no, control terminal to enter common mode, so that terminal only displays common information in any application program, common information being related to common contacts; when determination result is yes, and if obtained identity identification information matches preset identity identification information, control terminal to enter private mode, so that terminal simultaneously displays common information and private information in any application program, common information being related to common contacts, the private information being related to private contacts

AA Start

BB End

(57) Abstract: Provided are an information display method, an information display device, and a terminal. The method comprises: when any application program in a terminal receives an information display command, determining whether the terminal has obtained identity identification information; when a determination result is no, controlling the terminal to enter a common mode, so that the terminal only displays common information in any application program, the common information being related to common contacts; when the determination result is yes, and if the obtained identity identification information matches preset identity identification information, controlling the terminal to enter a private mode, so that the terminal simultaneously displays common information and private information in any application program, the common information being related to common contacts, the private information being related to private contacts. Via the present technical solution, a private mode in a terminal may be hidden, preventing an illegal user from attempting to crack a key of a private space after becoming aware that the private space corresponding to the private mode is present in the terminal, thereby increasing the security of using the terminal.

(57) 摘要:

[见续页]



WO 2016/165161 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明提出了一种信息显示方法、一种信息显示装置和一种终端，方法包括：当终端中的任一应用程序接收到信息显示指令时，判断终端是否获取到身份识别信息；在判断结果为否时，控制终端进入普通模式，以使终端仅显示任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的身份识别信息与预设身份识别信息相匹配，则控制终端进入私密模式，以使终端同时显示任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。通过本发明的技术方案，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，提高了终端的使用安全性。

信息显示方法、信息显示装置和终端

本申请要求于 2015 年 04 月 15 日提交中国专利局，申请号为 CN 201510179281.6、发明名称为“信息显示方法、信息显示装置和终端”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。

5

技术领域

本发明涉及终端技术领域，具体而言，涉及一种信息显示方法、一种信息显示装置和一种终端。

10 背景技术

目前，为了提高手机的使用安全性，一些手机上设置有私密模式，其作用是把设置好的私密联系人的信息都隐藏起来，这样，即使有人发现了私密模式也可以通过假私密密码进入假私密模式中，而真正的私密联系人的私密信息是不会被看到的，且私密模式的功能非常强大，除了假密码外，
15 还可以将来电、短信进行伪装。

另外，目前对私密模式的使用，基本依赖用户手动拉起私密模式入口，然后输入密码进到私密模式，在私密模式里进行查看私密联系人的私密信息等操作。但是，这个切换模式的入口和操作过程很容易告诉别人手机上有一个私密空间，也容易让人产生试图破解密码，反而给手机的使用安全性带来一定威胁；而且，用户设置好私密模式后，手机需要对于私密联系人的来电进行伪装，对私密联系人的短息信提示进行伪装，对私密的蓝牙信息进行伪装，而这么多的伪装，弹出的提示可能会与手机的实际状态矛盾，例如，手机会把来电伪装成闹钟，但其他用户在查看闹钟，就会发现并没有闹钟，这就导致用户的私密模式很容易被他人知晓。

25 因此，如何隐藏终端中的私密模式，保护私密联系人的私密信息，提高终端的使用安全性，成为亟待解决的问题。

发明内容

本发明正是基于上述问题，提出了一种新的技术方案，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，而降低终端的使用安全性，进而保护了私密联系人的私密信息，提高了终端的使用安全性。

有鉴于此，本发明的一方面提出了一种信息显示方法，包括：当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，由于在终端中设置身份识别信息接收模块，以使任一应用程序（如联系人应用程序、通讯记录应用程序、微信应用程序、QQ应用程序等）在接收到信息显示指令或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作时，必须向身份识别信息接收模块输入与存储的预设身份识别信息相匹配的身份识别信息，才能获取查看任一应用程序中的私密联系人的私密信息或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作的权限的这一事实，只有终端的合法用户知晓，而非法用户并不知道终端中设置身份识别信息接收模块，且该身份识别信息接收模块具有辨别用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、删除、修改等任一操作的权限，因而，当终端中的任一应用程序接收到信息显示指令时，若终端未获取到身份识别信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，或者是终端的合法用户，但终端的合法用户不希望查看该任一应用程序中的与私密联系人相关的私密信息，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，

从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性；当然，若终端获取到与预设身份识别信息相匹配的身份识别信息，则说明终端的当前操作者是终端的合法用户，则可以控制终端进入私密模式，以使终端的合法用户既可以查看任一应用程序中的与普通联系人相关的普通信息又可以查看与私密联系人相关的私密信息，避免对终端的合法用户带来不便。其中，身份识别信息接收模块可以为设置在终端背部的指纹识别模块，相应地，该预设身份识别信息可以为终端的合法用户的指纹信息。

另外，用户可以根据个人需求，在任一应用程序中任意设置私密联系人，则该私密联系人的所有信息就会变为私密信息，而私密联系人的私密信息与普通联系人的普通信息由于字段的区别，其在终端上的显示方式也有区别，例如：普通联系人的普通信息的字体为黑色字体时，而私密联系人的私密信息的字体就可以能为红色字体，或私密联系人的私密信息上携带有※号，而普通联系人的普通信息不携带有※号等。

在上述技术方案中，优选地，还包括：在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

在该技术方案中，当终端中的任一应用程序接收到信息显示指令时，若接收到身份识别信息与预设身份识别信息不匹配，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而实现避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性。

在上述技术方案中，优选地，还包括：在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；在判断结果为是时，控制所述终端由所述普通模式切换为

所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

- 5 在该技术方案中，在终端进入普通模式后，若接收到正确的私密模式切换密钥（如正确的指纹信息、声音识别特征，预设手势等），则仍然可以使用户进入私密模式下查看私密联系人的私密信息，从而防止用户在多次误输入错误的身份识别信息无法查看任一应用程序中的私密联系人的私密信息。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。
- 10

- 在上述技术方案中，优选地，所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及当所述身份识别信息为所述第二指纹信息时，所述判断所述终端是否获取到身份识别信息，具体包括：判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及所述在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，具体包括：在判断结果为是时，若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。
- 15
- 20

- 在该技术方案中，当身份识别信息为第二指纹信息时，通过判断终端背面的指纹识别模块是否接收到与第二指纹信息相匹配的预设指纹信息，可以对是否进入私密模式进行有效控制，以及在第二指纹信息与预设指纹信息相匹配时，才控制终端进入私密模式，可以控制只有合法用户才能查看任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，确保了私密联系人的私密信息的安全性。其中，身份识别信息
- 25

包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

在上述技术方案中，优选地，当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

在该技术方案中，当任一应用程序接收到与私密联系人相关的私密信息（如私密联系人的来电等）时，若终端的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以将私密信息伪装为与私密信息相对应的虚拟信息进行显示，以防止非法用户查看该任一应用程序的私密信息，同时，禁止该非法用户对该私密信息进行删除、复制、修改等任何操作，从而有效地确保了终端中的任一应用程序中的与私密联系人相关的私密信息不会被非法用户进行操作；反之，若终端的指纹识别模块获取到与预设指纹信息相匹配的指纹信息，则说明终端的当前操作者是终端的合法用户，则终端无需将该任一应用程序的私密信息伪装为虚拟信息，以方便合法用户直接查看该任一应用程序的真实的私密信息，同时，也允许合法用户对该私密信息进行删除、复制、修改等任何操作，从而确保了只有合法用户才能对私密信息进行各种操作。例如：当联系人应用程序接收到私密联系人的来电时，若终端中的指纹识别模块获取到与预设指纹信息相匹配的第二指纹信息，则将该私密联系人的姓名和手机号码进行正常显示，若终端中的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则可以将该私密联系人的姓名和手机号码分别伪装为“未知联系人”、“未知联系电话”或将该私密联系人的姓名“张三”和手机号码“18611114936”分

别伪装为“李四”和“18511114937”等进行显示，从而防止非法用户查看私密联系人的真实私密信息。

另外，为了进一步确保私密联系人的真实私密信息的安全性，当合法用户对任一应用程序的真实的私密信息进行查看、接听、修改、复制等操作后，若使终端灭屏，则终端重新亮屏后，可以判断重新判断指纹识别模块是否获取到与预设指纹信息相匹配的第二指纹信息，若获取到，则终端可以重新回到终端灭屏前的私密模式的显示界面，以使合法用户继续查看该任一应用程序在私密模式下的私密联系人的私密信息；否则，则终端进入普通模式，显示普通模式下的界面，从而使非法用户无法知晓私密模式的存在，而提高终端中的私密信息的安全性。

本发明的另一方面提出了一种信息显示装置，包括：判断单元，当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；控制单元，在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，由于在终端中设置身份识别信息接收模块，以使任一应用程序（如联系人应用程序、通讯记录应用程序、微信应用程序、QQ应用程序等）在接收到信息显示指令或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作时，必须向身份识别信息接收模块输入与存储的预设身份识别信息相匹配的身份识别信息，才能获取查看任一应用程序中的私密联系人的私密信息或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作的权限的这一事实，只有终端的合法用户知晓，而非法用户并不知道终端中设置身份识别信息接收模块，且该身份识别信息接收模块具有辨别用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、删除、修改等任一操作的权限，因而，当终端中的任一应用程序接收到信息显示指令时，若终端未获取到身份识别信息，

则说明终端的当前操作者是非法用户，并不是终端的合法用户，或者是终端的合法用户，但终端的合法用户不希望查看该任一应用程序中的与私密联系人相关的私密信息，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知

5 晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性；当然，若终端获取到与预设身份识别信息相匹配的身份识别信息，则说明终端的当前操作者是终端的合法用户，则

10 可以控制终端进入私密模式，以使终端的合法用户既可以查看任一应用程序中的与普通联系人相关的普通信息又可以查看与私密联系人相关的私密信息，避免对终端的合法用户带来不便。其中，身份识别信息接收模块可以为设置在终端背部的指纹识别模块，相应地，该预设身份识别信息可以为终端的合法用户的指纹信息。

15 另外，用户可以根据个人需求，在任一应用程序中任意设置私密联系人，则该私密联系人的所有信息就会变为私密信息，而私密联系人的私密信息与普通联系人的普通信息由于字段的区别，其在终端上的显示方式也有区别，例如：普通联系人的普通信息的字体为黑色字体时，而私密联系人的私密信息的字体就可以能为红色字体，或私密联系人的私密信息上携

20 带有※号，而普通联系人的普通信息不携带有※号等。

在上述技术方案中，优选地，所述控制单元还用于：在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

25 在该技术方案中，当终端中的任一应用程序接收到信息显示指令时，若接收到身份识别信息与预设身份识别信息不匹配，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密

空间的密钥，进而实现避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性。

在上述技术方案中，优选地，所述判断单元还用于：在所述终端进入
5 所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；所述控制单元还用于：在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第
10 一预设手势和第一预设密码中的至少一种信息。

在该技术方案中，在终端进入普通模式后，若接收到正确的私密模式切换密钥（如正确的指纹信息、声音识别特征，预设手势等），则仍然可以
15 使用户进入私密模式下查看私密联系人的私密信息，从而防止用户在多次误输入错误的身份识别信息无法查看任一应用程序中的私密联系人的私密信息。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

在上述技术方案中，优选地，所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设
20 手势和第二预设密码中的至少一种信息，以及所述判断单元具体用于：当所述身份识别信息为所述第二指纹信息时，所述判断所述终端是否获取到身份识别信息，具体包括：判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及所述控制单元具体用于：在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进
25 入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，当身份识别信息为第二指纹信息时，通过判断终端背面的指纹识别模块是否接收到与第二指纹信息相匹配的预设指纹信息，可以对是否进入私密模式进行有效控制，以及在第二指纹信息与预设指纹

信息相匹配时，才控制终端进入私密模式，可以控制只有合法用户才能查看任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，确保了私密联系人的私密信息的安全性。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

在上述技术方案中，优选地，所述判断单元还用于：当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；所述控制单元还用于：在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

在该技术方案中，当任一应用程序接收到与私密联系人相关的私密信息（如私密联系人的来电等）时，若终端的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以将私密信息伪装为与私密信息相对应的虚拟信息进行显示，以防止非法用户查看该任一应用程序的私密信息，同时，禁止该非法用户对该私密信息进行删除、复制、修改等任何操作，从而有效地确保了终端中的任一应用程序中的与私密联系人相关的私密信息不会被非法用户进行操作；反之，若终端的指纹识别模块获取到与预设指纹信息相匹配的指纹信息，则说明终端的当前操作者是终端的合法用户，则终端无需将该任一应用程序的私密信息伪装为虚拟信息，以方便合法用户直接查看该任一应用程序的真实的私密信息，同时，也允许合法用户对该私密信息进行删除、复制、修改等任何操作，从而确保了只有合法用户才能对私密信息进行各种操作。例如：当联系人应用程序接收到私密联系人的来电时，若终端中的指纹识别模块获取到与预设指纹信息相匹配的第二

指纹信息，则将该私密联系人的姓名和手机号码进行正常显示，若终端中的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则可以将该私密联系人的姓名和手机号码分别伪装为“未知联系人”、“未知联系电话”或将该私密联系人的姓名“张三”和手机号码“18611114936”
5 分别伪装为“李四”和“18511114937”等进行显示，从而防止非法用户查看私密联系人的真实私密信息。

另外，为了进一步确保私密联系人的真实私密信息的安全性，当合法用户对任一应用程序的真实的私密信息进行查看、接听、修改、复制等操作后，若使终端灭屏，则终端重新亮屏后，可以判断重新判断指纹识别模块是否获取到与预设指纹信息相匹配的第二指纹信息，若获取到，则终端
10 可以重新回到终端灭屏前的私密模式的显示界面，以使合法用户继续查看该任一应用程序在私密模式下的私密联系人的私密信息；否则，则终端进入普通模式，显示普通模式下的界面，从而使非法用户无法知晓私密模式的存在，而提高终端中的私密信息的安全性。

15 本发明的又一方面提出了一种终端，所述终端包括通信总线、输入装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、存储器以及处理器之间的连接通信；

所述输入装置，用于接收信息显示指令；

20 所述存储器中存储一组程序代码，且处理器调用存储器中存储的程序代码，用于执行以下操作：

当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；

在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示
25 所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在上述技术方案中，优选地，所述处理器还用于执行以下操作：

在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

在上述技术方案中，优选地，所述处理器还用于执行以下操作：

- 5 在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；

在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、
10 第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

在上述技术方案中，优选地，所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及

- 15 当所述身份识别信息为所述第二指纹信息时，所述处理器判断所述终端是否获取到身份识别信息，具体包括：

判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及

- 所述在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的
20 私密信息，具体包括：

在判断结果为是时，若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

- 25 在上述技术方案中，优选地，所述处理器还用于执行以下操作：

当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；

在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密

信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

5 在该技术方案中，通过在终端上设置信息显示装置，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，而降低终端的使用安全性，进而保护了私密联系人的私密信息，提高了终端的使用安全性。

10 通过本发明的技术方案，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，而降低终端的使用安全性，进而保护了私密联系人的私密信息，提高了终端的使用安全性。

附图说明

15 图 1 示出了根据本发明的一个实施例的信息显示方法的流程示意图；
图 2 示出了根据本发明的一个实施例的信息显示装置的结构示意图；
图 3 示出了根据本发明的一个实施例的终端的结构示意图；
图 4 示出了根据本发明的一个实施例的另一种终端的结构示意图。

具体实施方式

为了可以更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

25 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的信息显示方法的流程示意图。

如图 1 所示，示出了本发明的一个实施例的信息显示方法，包括：步骤 102，当终端中的任一应用程序接收到信息显示指令时，判断所述终端

是否获取到身份识别信息；步骤 104，在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，由于在终端中设置身份识别信息接收模块，以使任一应用程序（如联系人应用程序、通讯记录应用程序、微信应用程序、QQ 应用程序等）在接收到信息显示指令或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作时，必须向身份识别信息接收模块输入与存储的预设身份识别信息相匹配的身份识别信息，才能获取查看任一应用程序中的私密联系人的私密信息或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作的权限的这一事实，只有终端的合法用户知晓，而非法用户并不知道终端中设置身份识别信息接收模块，且该身份识别信息接收模块具有辨别用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、删除、修改等任一操作的权限，因而，当终端中的任一应用程序接收到信息显示指令时，若终端未获取到身份识别信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，或者是终端的合法用户，但终端的合法用户不希望查看该任一应用程序中的与私密联系人相关的私密信息，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性；当然，若终端获取到与预设身份识别信息相匹配的身份识别信息，则说明终端的当前操作者是终端的合法用户，则可以控制终端进入私密模式，以使终端的合法用户既可以查看任一应用程序中的与普通联系人相关的普通信息又可以查看与私密联系人相关的私密信息，避免对终端的合法用户带来不便。其中，身份识别信息接收模块可

以为设置在终端背部的指纹识别模块，相应地，该预设身份识别信息可以为终端的合法用户的指纹信息。

另外，用户可以根据个人需求，在任一应用程序中任意设置私密联系人，则该私密联系人的所有信息就会变为私密信息，而私密联系人的私密信息与普通联系人的普通信息由于字段的区别，其在终端上的显示方式也有区别，例如：普通联系人的普通信息的字体为黑色字体时，而私密联系人的私密信息的字体就可以能为红色字体，或私密联系人的私密信息上携带有※号，而普通联系人的普通信息不携带有※号等。

在上述技术方案中，优选地，还包括：在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

在该技术方案中，当终端中的任一应用程序接收到信息显示指令时，若接收到身份识别信息与预设身份识别信息不匹配，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而实现避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性。

在上述技术方案中，优选地，还包括：在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

在该技术方案中，在终端进入普通模式后，若接收到正确的私密模式切换密钥（如正确的指纹信息、声音识别特征，预设手势等），则仍然可

以使用户进入私密模式下查看私密联系人的私密信息，从而防止用户在多次误输入错误的身份识别信息无法查看任一应用程序中的私密联系人的私密信息。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

在上述技术方案中，优选地，所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及当所述身份识别信息为所述第二指纹信息时，所述判断所述终端是否获取到身份识别信息，具体包括：

10 判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及所述在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，具体包括：在判断结果为是时，若所述指纹识别模块获取到的所述第

15 二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，当身份识别信息为第二指纹信息时，通过判断终端背面的指纹识别模块是否接收到与第二指纹信息相匹配的预设指纹信息，

20 可以对是否进入私密模式进行有效控制，以及在第二指纹信息与预设指纹信息相匹配时，才控制终端进入私密模式，可以控制只有合法用户才能查看任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，确保了私密联系人的私密信息的安全性。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

25

在上述技术方案中，优选地，当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二

指纹信息；在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

在该技术方案中，当任一应用程序接收到与私密联系人相关的私密信息（如私密联系人的来电等）时，若终端的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以将私密信息伪装为与私密信息相对应的虚拟信息进行显示，以防止非法用户查看该任一应用程的私密信息，同时，禁止该非法用户对该私密信息进行删除、复制、修改等任何操作，从而有效地确保了终端中的任一应用程序中的与私密联系人相关的私密信息不会被非法用户进行操作；反之，若终端的指纹识别模块获取到与预设指纹信息相匹配的指纹信息，则说明终端的当前操作者是终端的合法用户，则终端无需将该任一应用程序的私密信息伪装为虚拟信息，以方便合法用户直接查看该任一应用程序的真实的私密信息，同时，也允许合法用户对该私密信息进行删除、复制、修改等任何操作，从而确保了只有合法用户才能对私密信息进行各种操作。例如：当联系人应用程序接收到私密联系人的来电时，若终端中的指纹识别模块获取到与预设指纹信息相匹配的第二指纹信息，则将该私密联系人的姓名和手机号码进行正常显示，若终端中的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则可以将该私密联系人的姓名和手机号码分别伪装为“未知联系人”、“未知联系电话”或将该私密联系人的姓名“张三”和手机号码“18611114936”分别伪装为“李四”和“18511114937”等进行显示，从而防止非法用户查看私密联系人的真实私密信息。

另外，为了进一步确保私密联系人的真实私密信息的安全性，当合法用户对任一应用程序的真实的私密信息进行查看、接听、修改、复制等操作后，若使终端灭屏，则终端重新亮屏后，可以判断重新判断指纹识别模块是否获取到与预设指纹信息相匹配的第二指纹信息，若获取到，则终端

可以重新回到终端灭屏前的私密模式的显示界面，以使合法用户继续查看该任一应用程序在私密模式下的私密联系人的私密信息；否则，则终端进入普通模式，显示普通模式下的界面，从而使非法用户无法知晓私密模式的存在，而提高终端中的私密信息的安全性。

5 图 2 示出了根据本发明的一个实施例的信息显示装置的结构示意图。

如图 2 所示，示出了本发明的一个实施例的信息显示装置 200，包括：判断单元 202，当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；控制单元 204，在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与
10 普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，由于在终端中设置身份识别信息接收模块，以使任一应用程序（如联系人应用程序、通讯记录应用程序、微信应用程序、QQ
15 应用程序等）在接收到信息显示指令或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作时，必须向身份识别信息接收模块输入与存储的预设身份识别信息相匹配的身份识别信息，才能获取查看任一应用程序中的私密联系人的私密信息或对任一应用程序中的私密联系人的私密信息进行删除、修改等任一操作的权限的这一事实，只有终端的合法
20 用户知晓，而非法用户并不知道终端中设置身份识别信息接收模块，且该身份识别信息接收模块具有辨别用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、删除、修改等任一操作的权限，因而，当终端中的任一应用程序接收到信息显示指令时，若终端未获取到身份识别信息，
25 则说明终端的当前操作者是非法用户，并不是终端的合法用户，或者是终端的合法用户，但终端的合法用户不希望查看该任一应用程序中的与私密联系人相关的私密信息，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进

而避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性；当然，若终端获取到与预设身份识别信息相匹配的身份识别信息，则说明终端的当前操作者是终端的合法用户，则可以控制终端进入私密模式，以使终端的合法用户既可以查看任一应用程序中的与普通联系人相关的普通信息又可以查看与私密联系人相关的私密信息，避免对终端的合法用户带来不便。其中，身份识别信息接收模块可以为设置在终端背部的指纹识别模块，相应地，该预设身份识别信息可以为终端的合法用户的指纹信息。

- 5 可以控制终端进入私密模式，以使终端的合法用户既可以查看任一应用程序中的与普通联系人相关的普通信息又可以查看与私密联系人相关的私密信息，避免对终端的合法用户带来不便。其中，身份识别信息接收模块可以为设置在终端背部的指纹识别模块，相应地，该预设身份识别信息可以为终端的合法用户的指纹信息。
- 10 另外，用户可以根据个人需求，在任一应用程序中任意设置私密联系人，则该私密联系人的所有信息就会变为私密信息，而私密联系人的私密信息与普通联系人的普通信息由于字段的区别，其在终端上的显示方式也有区别，例如：普通联系人的普通信息的字体为黑色字体时，而私密联系人的私密信息的字体就可以能为红色字体，或私密联系人的私密信息上携带有※号，而普通联系人的普通信息不携带有※号等。
- 15 带有※号，而普通联系人的普通信息不携带有※号等。

在上述技术方案中，优选地，所述控制单元 204 还用于：在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

- 20 在该技术方案中，当终端中的任一应用程序接收到信息显示指令时，若接收到身份识别信息与预设身份识别信息不匹配，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以控制终端进入普通模式，而使终端仅显示任一应用程序中的与普通联系人相关的普通信息，从而避免使非法用户知晓终端中存在与私密模式对应的私密空间而试图破解私密空间的密钥，进而实现避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性。
- 25 空间的密钥，进而实现避免非法用户查看该任一应用程序中的与私密联系人相关的私密信息，从而使得该任一应用程序中的私密联系人的私密信息得到有效的保护，并最终提高了终端的使用安全性。

在上述技术方案中，优选地，还包括：所述判断单元 202 还用于：在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则

判断是否获取到正确的私密模式切换密钥；所述控制单元 204 还用于：在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

在该技术方案中，在终端进入普通模式后，若接收到正确的私密模式切换密钥（如正确的指纹信息、声音识别特征，预设手势等），则仍然可以使用户进入私密模式下查看私密联系人的私密信息，从而防止用户在多次误输入错误的身份识别信息无法查看任一应用程序中的私密联系人的私密信息。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操作权限的信息均可。

在上述技术方案中，优选地，所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及所述判断单元 202 具体用于：当所述身份识别信息为所述第二指纹信息时，所述判断所述终端是否获取到身份识别信息，具体包括：判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及所述控制单元 204 具体用于：在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

在该技术方案中，当身份识别信息为第二指纹信息时，通过判断终端背面的指纹识别模块是否接收到与第二指纹信息相匹配的预设指纹信息，可以对是否进入私密模式进行有效控制，以及在第二指纹信息与预设指纹信息相匹配时，才控制终端进入私密模式，可以控制只有合法用户才能查看任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，确保了私密联系人的私密信息的安全性。其中，身份识别信息包括但不限于上述信息，所有可以标识用户身份以判断用户是否具有对任一应用程序中的私密联系人的私密信息进行查看、接听、修改、复制等操

作权限的信息均可。

在上述技术方案中，优选地，所述判断单元 202 还用于：当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与预设指纹信息相匹配的所述第二指纹信息；所述控制单元 204 还用于：在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

在该技术方案中，当任一应用程序接收到与私密联系人相关的私密信息（如私密联系人的来电等）时，若终端的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则说明终端的当前操作者是非法用户，并不是终端的合法用户，则可以将私密信息伪装为与私密信息相对应的虚拟信息进行显示，以防止非法用户查看该任一应用程序的私密信息，同时，禁止该非法用户对该私密信息进行删除、复制、修改等任何操作，从而有效地确保了终端中的任一应用程序中的与私密联系人相关的私密信息不会被非法用户进行操作；反之，若终端的指纹识别模块获取到与预设指纹信息相匹配的指纹信息，则说明终端的当前操作者是终端的合法用户，则终端无需将该任一应用程序的私密信息伪装为虚拟信息，以方便合法用户直接查看该任一应用程序的真实的私密信息，同时，也允许合法用户对该私密信息进行删除、复制、修改等任何操作，从而确保了只有合法用户才能对私密信息进行各种操作。例如：当联系人应用程序接收到私密联系人的来电时，若终端中的指纹识别模块获取到与预设指纹信息相匹配的第二指纹信息，则将该私密联系人的姓名和手机号码进行正常显示，若终端中的指纹识别模块未获取到与预设指纹信息相匹配的第二指纹信息，则可以将该私密联系人的姓名和手机号码分别伪装为“未知联系人”、“未知联系电话”或将该私密联系人的姓名“张三”和手机号码“18611114936”分别伪装为“李四”和“18511114937”等进行显示，从而防止非法用户查

看私密联系人的真实私密信息。

另外，为了进一步确保私密联系人的真实私密信息的安全性，当合法用户对任一应用程序的真实的私密信息进行查看、接听、修改、复制等操作后，若使终端灭屏，则终端重新亮屏后，可以判断重新判断指纹识别模块是否获取到与预设指纹信息相匹配的第二指纹信息，若获取到，则终端可以重新回到终端灭屏前的私密模式的显示界面，以使合法用户继续查看该任一应用程序在私密模式下的私密联系人的私密信息；否则，则终端进入普通模式，显示普通模式下的界面，从而使非法用户无法知晓私密模式的存在，而提高终端中的私密信息的安全性。

图 3 示出了根据本发明的一个实施例的终端的结构示意图。

如图 3 所示，示出了本发明的一个实施例的终端 300，包括：如上述技术方案中任一项所述的信息显示装置 200。

在该技术方案中，通过在终端 300 上设置信息显示装置 200，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，而降低终端的使用安全性，进而保护了私密联系人的私密信息，提高了终端的使用安全性。

本发明实施例还提供了一种终端，图 4 为本发明实施例中另一种终端的结构示意图，如图所示，所述终端可以包括：至少一个输入装置 403，至少一个处理器 401，例如 CPU，存储器 404 和至少一个总线 402，处理器 401 可以结合图 2 所示的信息显示装置。

其中，上述总线 402 用于连接上述输入装置 403、处理器 401 和存储器 404。

其中，上述输入装置 403 具体可为终端的通信接口，例如网络接口，网络接口可以包括标准的有线接口或者无线接口（如 WI-FI 接口）。又如用户接口，用户接口可以包括键盘或者显示屏等。

上述存储器 404 可以是高速 RAM 存储器，也可为非不稳定的存储器（non-volatile memory），例如磁盘存储器。上述存储器 404 还用于存储一组程序代码，上述处理器 401 用于调用存储器 404 中存储的程序代码，执行如下操作：

当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否

获取到身份识别信息;

在判断结果为否时, 控制所述终端进入普通模式, 以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息; 在判断结果为是时, 若获取到的所述身份识别信息与预设身份识别信息相匹配, 则控制所述终端进入私密模式, 以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

可选的, 所述处理器 401 还用于执行以下操作:

在所述判断结果为是时, 若获取到的所述身份识别信息与所述预设身份识别信息不匹配, 则仍然控制终端进入普通模式, 以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

可选的, 所述处理器 401 还用于执行以下操作:

在所述终端进入所述普通模式后, 若所述终端接收到私密模式切换指令, 则判断是否获取到正确的私密模式切换密钥;

在判断结果为是时, 控制所述终端由所述普通模式切换为所述私密模式; 否则, 控制所述终端继续停留在所述普通模式, 其中, 所述私密模式切换密钥包括: 第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

可选的, 所述身份识别信息包括: 第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息, 以及

当所述身份识别信息为所述第二指纹信息时, 所述处理器判断所述终端是否获取到身份识别信息, 具体包括:

判断设置在终端背面的指纹识别模块是否接收到第二指纹信息; 以及

所述在判断结果为是时, 若获取到的所述身份识别信息与预设身份识别信息相匹配, 则控制所述终端进入私密模式, 以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息, 具体包括:

在判断结果为是时, 若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配, 则控制所述终端进入私密模式, 以使所述终端同

时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

可选的，所述处理器 401 还用于执行以下操作：

5 当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；

10 在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

具体的，本发明实施例中介绍的终端可以用以实施本发明结合图 1 介绍的方法实施例中的部分或全部流程。

15 以上结合附图详细说明了本发明的技术方案，可以隐藏终端中的私密模式，避免非法用户在知晓终端中存在私密模式对应的私密空间后，试图破解私密空间的密钥，而降低终端的使用安全性，进而保护了私密联系人的私密信息，提高了终端的使用安全性。

20 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求

1. 一种信息显示方法，其特征在于，包括：

当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否
5 获取到身份识别信息；

在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通
10 联系人相关的普通信息和与私密联系人相关的私密信息。

2. 根据权利要求 1 所述的信息显示方法，其特征在于，还包括：

在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

15 3. 根据权利要求 1 所述的信息显示方法，其特征在于，还包括：

在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；

在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式
20 切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

4. 根据权利要求 1 至 3 中任一项所述的信息显示方法，其特征在于，

所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少
25 一种信息，以及

当所述身份识别信息为所述第二指纹信息时，所述判断所述终端是否获取到身份识别信息，具体包括：

判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及
所述在判断结果为是时，若获取到的所述身份识别信息与预设身份识

别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，具体包括：

5 在判断结果为是时，若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

5. 根据权利要求4所述的信息显示方法，其特征在于，还包括：

10 当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；

在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

6. 一种信息显示装置，其特征在于，包括：

判断单元，当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；

20 控制单元，在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

25 7. 根据权利要求6所述的信息显示装置，其特征在于，

所述控制单元还用于：

在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

8. 根据权利要求 6 所述的信息显示装置，其特征在于，
所述判断单元还用于：

在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；以及

5 所述控制单元还用于：

在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

10 9. 根据权利要求 6 至 8 中任一项所述的信息显示装置，其特征在于，
所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及

所述判断单元具体用于：

15 当所述身份识别信息为所述第二指纹信息时，判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及

所述控制单元具体用于：

在判断结果为是时，若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。
20

10. 根据权利要求 9 所述的信息显示装置，其特征在于，
所述判断单元还用于：

25 当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的第二指纹信息；

所述控制单元还用于：

在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用

户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

11. 一种终端，其特征在于，所述终端包括通信总线、输入装置、存储器以及处理器，其中：

所述通信总线，用于实现所述输入装置、存储器以及处理器之间的连接通信；

所述输入装置，用于接收信息显示指令；

所述存储器中存储一组程序代码，且处理器调用存储器中存储的程序代码，用于执行以下操作：

当终端中的任一应用程序接收到信息显示指令时，判断所述终端是否获取到身份识别信息；

在判断结果为否时，控制所述终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息；在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

12. 根据权利要求 11 所述的终端，其特征在于，所述处理器还用于执行以下操作：

在所述判断结果为是时，若获取到的所述身份识别信息与所述预设身份识别信息不匹配，则仍然控制终端进入普通模式，以使所述终端仅显示所述任一应用程序中的与普通联系人相关的普通信息。

13. 根据权利要求 11 所述的终端，其特征在于，所述处理器还用于执行以下操作：

在所述终端进入所述普通模式后，若所述终端接收到私密模式切换指令，则判断是否获取到正确的私密模式切换密钥；

在判断结果为是时，控制所述终端由所述普通模式切换为所述私密模式；否则，控制所述终端继续停留在所述普通模式，其中，所述私密模式切换密钥包括：第一指纹信息、第一声音识别特征信息、第一面部特征信

息、第一身份证信息、第一预设手势和第一预设密码中的至少一种信息。

14. 根据权利要求 11 至 13 中任一项所述的终端，其特征在于，

所述身份识别信息包括：第二指纹信息、第二声音识别特征信息、第二面部特征信息、第二身份证信息、第二预设手势和第二预设密码中的至少一种信息，以及

当所述身份识别信息为所述第二指纹信息时，所述处理器判断所述终端是否获取到身份识别信息，具体包括：

判断设置在终端背面的指纹识别模块是否接收到第二指纹信息；以及

所述在判断结果为是时，若获取到的所述身份识别信息与预设身份识别信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息，具体包括：

在判断结果为是时，若所述指纹识别模块获取到的所述第二指纹信息与预设指纹信息相匹配，则控制所述终端进入私密模式，以使所述终端同时显示所述任一应用程序中的与普通联系人相关的普通信息和与私密联系人相关的私密信息。

15. 根据权利要求 14 所述的终端，其特征在于，所述处理器还用于执行以下操作：

当所述身份识别信息为所述第二指纹信息时，若所述任一应用程序接收到与所述私密联系人相关的私密信息，则判断所述指纹识别模块是否获取到与所述预设指纹信息相匹配的所述第二指纹信息；

在判断结果为否时，控制所述终端将所述任一应用程序中的所述私密信息显示为与所述私密信息相对应的虚拟信息，同时，禁止所述终端的用户对所述私密信息进行任何操作；在判断结果为是时，控制所述终端将所述任一应用程序中的所述私密信息进行正常显示，同时，允许所述终端的用户对所述私密信息进行任何操作。

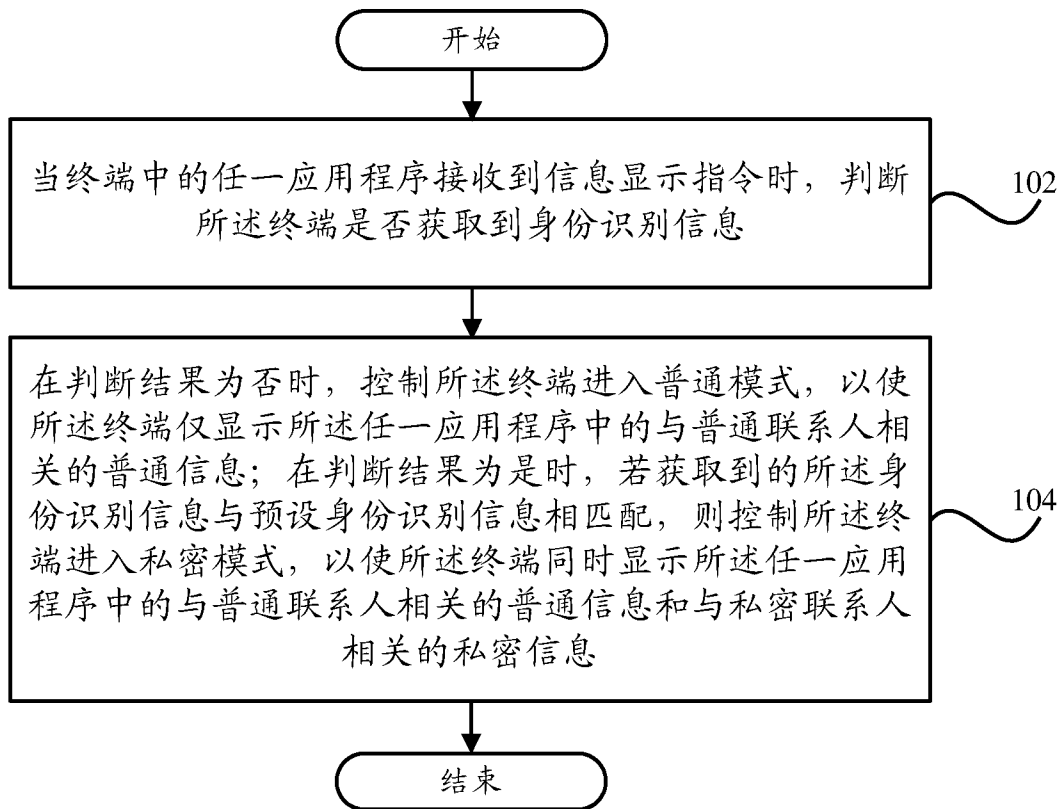


图 1



图 2



图 3

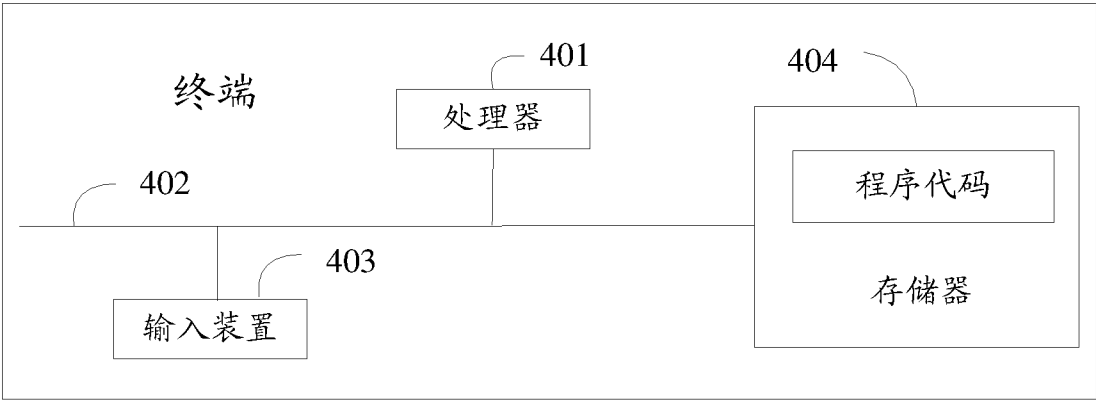


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/077953

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; G06F 21/31 (2013.01) i; G06F 21/62 (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)

IPC: H04L; G06F

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)

CNABS; CNKI; SIPOABS; VEN: safe+, security, private, mode, user, authenticat+, identif+, display+; CPC: G06F21/31, G06F21/32, G06F21/62, G06F3/0481, G06F3/0482, G06F3/04842

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to
Y	CN 104036160 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 10 September 2014 (10.09.2014) description, paragraphs [0004] to [0047]	1-15
Y	WO 2014050949 A1 (KYOCERA CORP.) 03 April 2014 (03.04.2014) description, paragraphs [0002] to [0004]	1-15
Y	CN 104036159 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 10 September 2014 (10.09.2014) description, paragraphs [0004] to [0047]	1-15
Y	CN 103942476 A (YULONG COMPUTER TELECOM TECHNOLOGY SHENZ) 23 July 2014 (23.07.2014) description, paragraphs [0025] to [0047]	1-15
A	CN 103532938 A (DONGGUAN YULONG COMMUNICATION TECHNOLOGY et al.) 22 January 2014 (22.01.2014) the whole document	1-15

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

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 05 January 2016	Date of mailing of the international search report 27 January 2016
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 XUE, Yu Telephone No. (86-10) 62089405

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/077953

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104036160 A	10 September 2014	US 2014325680 A1	30 October 2014
		WO 2014134945 A1	12 September 2014
WO 2014050949 A1	03 April 2014	US 2015208244 A1	23 July 2015
		JP 2014071476 A	21 April 2014
CN 104036159 A	10 September 2014	US 2015332065 A1	19 November 2015
		WO 2014135085 A1	12 September 2014
CN 103942476 A	23 July 2014	None	
CN 103532938 A	22 January 2014	None	

A. 主题的分类 H04L 29/06 (2006.01)i; G06F 21/31 (2013.01)i; G06F 21/62 (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) H04L; G06F 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)) CNABS; CNKI; SIPOABS; VEN: 私密, 隐私, 安全, 模式, 普通, 用户, 身份, 识别, 认证, 显示, safe+, security, private, mode, user, authenticat+, identif+, display+; CPC: G06F21/31, G06F21/32, G06F21/62, G06F3/0481, G06F3/0482, G06F3/04842																				
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 104036160 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段</td> <td>1-15</td> </tr> <tr> <td>Y</td> <td>WO 2014050949 A1 (KYOCERA CORP) 2014年 4月 3日 (2014 - 04 - 03) 说明书第0002-0004段</td> <td>1-15</td> </tr> <tr> <td>Y</td> <td>CN 104036159 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段</td> <td>1-15</td> </tr> <tr> <td>Y</td> <td>CN 103942476 A (宇龙计算机通信科技深圳有限公司) 2014年 7月 23日 (2014 - 07 - 23) 说明书第0025-0047段</td> <td>1-15</td> </tr> <tr> <td>A</td> <td>CN 103532938 A (东莞宇龙通信科技有限公司等) 2014年 1月 22日 (2014 - 01 - 22) 全文</td> <td>1-15</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 104036160 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段	1-15	Y	WO 2014050949 A1 (KYOCERA CORP) 2014年 4月 3日 (2014 - 04 - 03) 说明书第0002-0004段	1-15	Y	CN 104036159 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段	1-15	Y	CN 103942476 A (宇龙计算机通信科技深圳有限公司) 2014年 7月 23日 (2014 - 07 - 23) 说明书第0025-0047段	1-15	A	CN 103532938 A (东莞宇龙通信科技有限公司等) 2014年 1月 22日 (2014 - 01 - 22) 全文	1-15
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
Y	CN 104036160 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段	1-15																		
Y	WO 2014050949 A1 (KYOCERA CORP) 2014年 4月 3日 (2014 - 04 - 03) 说明书第0002-0004段	1-15																		
Y	CN 104036159 A (腾讯科技深圳有限公司) 2014年 9月 10日 (2014 - 09 - 10) 说明书第0004-0047段	1-15																		
Y	CN 103942476 A (宇龙计算机通信科技深圳有限公司) 2014年 7月 23日 (2014 - 07 - 23) 说明书第0025-0047段	1-15																		
A	CN 103532938 A (东莞宇龙通信科技有限公司等) 2014年 1月 22日 (2014 - 01 - 22) 全文	1-15																		
☐ 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 2016年 1月 5日		国际检索报告邮寄日期 2016年 1月 27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 薛钰 电话号码 (86-10) 62089405																		

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/077953

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	104036160	A	2014年 9月 10日	US	2014325680	A1	2014年 10月 30日
				WO	2014134945	A1	2014年 9月 12日
WO	2014050949	A1	2014年 4月 3日	US	2015208244	A1	2015年 7月 23日
				JP	2014071476	A	2014年 4月 21日
CN	104036159	A	2014年 9月 10日	US	2015332065	A1	2015年 11月 19日
				WO	2014135085	A1	2014年 9月 12日
CN	103942476	A	2014年 7月 23日	无			
CN	103532938	A	2014年 1月 22日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)