(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 107846517 A
(43)申请公布日 2018.03.27

(21)申请号 201711117672.0

(22)申请日 2017.11.13

(71)申请人 维沃移动通信有限公司
地址 523857 广东省东莞市长安镇乌沙步步高大道283号

(72)发明人 林松杰

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 许志勇

(51)Int.Cl.
*H04M 1/725*(2006.01)
*H04M 1/67*(2006.01)

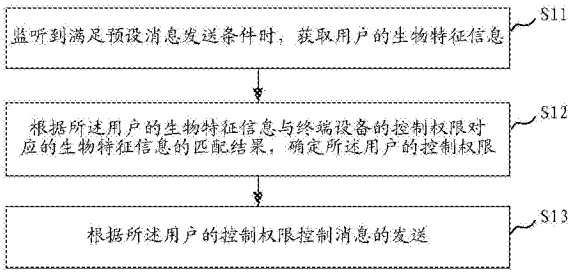
权利要求书2页 说明书9页 附图2页

(54)发明名称

消息发送方法和移动终端

(57)摘要

本发明公开了一种消息发送方法和移动终端，以提高消息发送的安全性。该方法包括：监听到满足预设消息发送条件时，获取用户的生物特征信息；根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；根据所述用户的控制权限控制消息的发送。




CN 107846517 A

1.一种消息发送方法，其特征在于，包括：

监听到满足预设消息发送条件时，获取用户的生物特征信息；

根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；

根据所述用户的控制权限控制消息的发送。

2.如权利要求1所述的方法，其特征在于，根据所述用户的控制权限控制消息的发送，具体包括：

根据所述用户的控制权限允许消息的发送，或，根据所述用户的控制权限拒绝消息的发送。

3.如权利要求2所述的方法，其特征在于，根据所述用户的控制权限允许消息的发送时，所述方法还包括：

在发送的消息中添加与所述用户的生物特征信息相对应的标识信息。

4.如权利要求3所述的方法，其特征在于，所述方法还包括：

设置所述标识信息在发送端的应用界面中为显示或隐藏；和/或，

设置所述标识信息在接收端的应用界面中为显示或隐藏。

5.如权利要求1至4任一项所述的方法，其特征在于，根据所述用户的控制权限控制消息的发送，包括：

当所述用户不具备发送消息的控制权限时，在进入所述终端设备的应用界面后，控制所述应用界面中用于发送消息的按钮的状态为不可用；或，

在进入所述终端设备的应用界面后，当点击所述应用界面中用于发送消息的按钮后，根据所述用户的控制权限，控制是否触发所述按钮的点击事件。

6.如权利要求5所述的方法，其特征在于，所述生物特征信息包括屏幕指纹特征信息，则，根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，具体包括：

将所述用户的屏幕指纹特征信息与终端设备的控制权限对应的屏幕指纹特征信息进行匹配，得到匹配结果；

根据匹配结果，确定所述用户的控制权限。

7.一种移动终端，其特征在于，包括：

获取模块，用于监听到满足预设消息发送条件时，获取用户的生物特征信息；

权限确定模块，用于根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；

消息发送模块，用于根据所述用户的控制权限控制消息的发送。

8.如权利要求7所述的移动终端，其特征在于，所述消息发送模块，具体用于：

根据所述用户的控制权限允许消息的发送，或，根据所述用户的控制权限拒绝消息的发送。

9.如权利要求8所述的移动终端，其特征在于，所述移动终端还包括：

标识信息添加模块，用于在发送的消息中添加与所述用户的生物特征信息相对应的标识信息。

10.如权利要求9所述的移动终端，其特征在于，所述移动终端还包括：

显示模式控制模块，用于设置所述标识信息在发送端的应用界面中为显示或隐藏；和/或，

设置所述标识信息在接收端的应用界面中为显示或隐藏。

11.如权利要求7至10任一项所述的移动终端，其特征在于，所述消息发送模块，根据所述用户的控制权限控制消息的发送，包括：

当所述用户不具备发送消息的控制权限时，在进入所述终端设备的应用界面后，控制所述应用界面中用于发送消息的按钮的状态为不可用；或，

在进入所述终端设备的应用界面后，当点击所述应用界面中用于发送消息的按钮后，根据所述用户的控制权限，控制是否触发所述按钮的点击事件。

12.如权利要求11所述的移动终端，其特征在于，所述生物特征信息包括屏幕指纹特征信息，则，根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，具体包括：

将所述用户的屏幕指纹特征信息与终端设备的控制权限对应的屏幕指纹特征信息进行匹配，得到匹配结果；

根据匹配结果，确定所述用户的控制权限。

13.一种移动终端，其特征在于，包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1至6中任一项所述的方法的步骤。

# 消息发送方法和移动终端

## 技术领域

[0001] 本发明涉及通信领域/终端领域，尤其涉及一种消息发送方法和移动终端。

## 背景技术

[0002] 随着通信技术的发展，用户与用户之间更倾向于利用移动终端通过消息互发实现交流。现有技术中，对于归属于某一用户(机主)的移动终端，得到该移动终端的其他用户也可以使用该移动终端进行消息发送；并且，消息的接收方也不能确定接收到的消息是否来自移动终端的机主，这样，机主之外的用户冒充机主发送虚假信息时，容易致使接收方上当受骗。因此，现有技术中的消息发送方法，其安全性较低。

## 发明内容

[0003] 本发明实施例的目的是提供一种消息发送方法和移动终端，以提高消息发送的安全性。

[0004] 第一方面，提供了一种消息发送方法，该方法包括：监听到满足预设消息发送条件时，获取用户的生物特征信息；根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；根据所述用户的控制权限控制消息的发送。

[0005] 第二方面，提供了一种移动终端，该移动终端包括：获取模块，用于监听到满足预设消息发送条件时，获取用户的生物特征信息；权限确定模块，用于根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；消息发送模块，用于根据所述用户的控制权限控制消息的发送。

[0006] 第三方面，提供了一种移动终端，该移动终端包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如第一方面所述的方法的步骤。

[0007] 第四方面，提供了一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的方法的步骤。

[0008] 在本发明实施例中，首先获取用户的生物特征信息，然后根据与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，最终根据用户的控制权限控制消息的发送，由于在消息发送之前先验证用户的生物特征信息对应的控制权限，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

## 附图说明

[0009] 此处所说明的附图用来提供对本发明的进一步理解，构成本发明的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0010] 图1是本发明的一个实施例提供的消息发送方法流程示意图；

[0011] 图2是本发明的另一个实施例提供的消息发送方法流程示意图；

[0012] 图3是本发明的一个实施例提供的移动终端结构示意图；

[0013] 图4为实现本发明各个实施例的一种移动终端的硬件结构示意图。

## 具体实施方式

[0014] 为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明具体实施例及相应的附图对本发明技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本发明一部分实施例，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他实施例，都属于本发明保护的范围。

[0015] 实施例1

[0016] 本发明实施1例提供一种消息发送方法，用于提高消息发送的安全性。该实施例中的消息发送，具体可以是通过短信业务进行消息发送；也可以是通过即时通信软件如微信、QQ等进行消息发送；还可以是通过电子邮箱进行邮件(也称为是消息)发送等。如图1所示，该实施例1包括如下步骤：

[0017] 步骤S11：监听到满足预设消息发送条件时，获取用户的生物特征信息。

[0018] 该实施例中，监听到满足预设消息发送条件，可以是在监听到用户点击用于发送消息的应用的图标，还可以是监听到用户点击所述应用内用于发送消息的按钮等。该处所称的应用，可以是安装在终端设备上，具体可以是上述提到的短信业务软件、即时通信软件、或电子邮箱等。

[0019] 该实施例中的生物特征信息，具体可以是指纹特征信息、面部特征信息或虹膜特征信息等。步骤S11在获取用户的生物特征信息时，可以利用终端设备上的指纹传感器采集用户的指纹后进行特征提取，得到用户的指纹特征信息；或者是采用摄像头采集用户的面部图像后进行特征提取，得到用户的面部特征信息；又或者是采用摄像头采集用户的虹膜图像后进行特征提取，得到用户的虹膜特征信息。

[0020] 步骤S12：根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限。

[0021] 该实施例中的终端设备，具体可以是手机、平板电脑或个人计算机等。终端设备的控制权限，具体可以是终端设备中的短信业务的使用权限(或称发送消息的控制权限，后续类似)；或者是终端设备中的即时通信软件的使用权限；或者是终端设备中的电子邮箱的使用权限等。又或者，可以具体到是短信业务中发送按钮的使用权限；即时通信软件中发送按钮的使用权限；或电子邮箱中发送按钮的使用权限等。

[0022] 该实施例获取用户的生物特征信息之前，还可以设置终端设备的控制权限和生物特征信息的对应关系。一种控制权限与生物特征信息的对应关系示例如表1所示，表1中的生物特征信息字段存储的为多个用户的生物特征信息，控制权限字段存储的允许使用(即拥有控制权限)的应用。

[0023] 该步骤具体执行时，可以将步骤S11中获取到的生物特征信息，与存储的如表1所示的生物特征信息进行匹配，得到匹配结果，得到的匹配结果可以是与存储的某一生物特征信息匹配成功；也可以是与存储的生物特征信息均匹配失败。

[0024] 表1控制权限与生物特征信息对应表

[0025]

| 生物特征信息 | 控制权限 |
| --- | --- |
| 生物特征信息1 | 短信业务、即时通信软件和电子邮箱 |
| 生物特征信息2 | 短信业务和即时通信软件 |
| 生物特征信息3 | 电子邮箱 |
| 生物特征信息4 | 即时通信软件 |
| …… | …… |

[0026] 根据上述得到的匹配结果，即可确定出所述用户的控制权限，该控制权限包括允许发送消息和拒绝发送消息。例如，得到的匹配结果如果是与存储的某一生物特征信息匹配成功，即可查询得到用户的控制权限；得到的匹配结果是与存储的生物特征信息均匹配失败，则确定用户没有发送消息的权限。

[0027] 步骤S13：根据所述用户的控制权限控制消息的发送。

[0028] 在步骤S12中确定出所述用户的控制权限，包括允许发送消息和拒绝发送消息等，因此，该步骤中控制消息的发送，具体可以是根据所述用户的控制权限允许消息的发送，或，根据所述用户的控制权限拒绝消息的发送。

[0029] 另外，根据所述用户的控制权限控制消息的发送时，当所述用户不具备发送消息的控制权限时，在进入所述终端设备的应用界面后，还可以控制所述应用界面中用于发送消息的按钮的状态为不可用。

[0030] 该步骤根据所述用户的控制权限控制消息的发送，还可以是在进入所述终端设备的应用界面后，当点击所述应用界面中用于发送消息的按钮后，根据所述用户的控制权限，控制是否触发所述按钮的点击事件。

[0031] 通过本发明实施例提供的消息发送方法，首先获取用户的生物特征信息，然后根据与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，最终根据用户的控制权限控制消息的发送，由于在消息发送之前先验证用户的生物特征信息对应的控制权限，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

[0032] 上述提到，在实施例1的步骤S13中根据用户的控制权限控制消息的发送，当根据用户的控制权限允许消息的发送时，还可以在发送的消息中添加与获取到的用户的生物特征信息相对应的标识信息。

[0033] 一个终端设备中，可能有多个用户同时具有发送消息的权限，又或者是，机主设置了任何生物标识信息均具有发送消息的权限，由于该标识信息与上述获取到的用户的生物特征信息相对应，这样，接收方在接收到所述消息时，根据同时接收到的所述标识信息，即可准确地确定出发送方的身份，进一步避免了机主之外的其他用户冒充机主发送虚假信息时，容易致使接收方上当受骗的问题。具体在发送的消息中添加标识信息时，可以在发送的消息内容的头部或者是尾部保留预设字段，该预设字段用于保存上述标识信息。

[0034] 在上述提到在发送消息时，在消息中添加的标识信息与生物特征信息相对应，因此，实施例1在验证发送方的生物特征信息之前，还可以设置生物特征信息和标识信息的对应关系，这样，一个终端设备虽然允许有多个用户使用，但是在进行消息发送时，首先验证

用户的生物特征信息对应的控制权限，并且在待发送的消息中添加与验证通过的生物特征信息相对应的标识信息，保证了用户与发送的消息之间的唯一对应关系。

[0035] 另外，实施例1在验证发送方的生物特征信息之前，还可以预先设置所述标识信息在发送端的显示界面中的显示模式，所述显示模式包括显示和隐藏。当设置的显示模式为隐藏时，该标识信息对发送方不可见，而对接收方可见。这样，即使机主设置了其他任意生物标识信息均具有发送消息的权限，其他任意生物标识信息可以是与标识信息“未知用户”对应，不法分子在冒充机主发送虚假信息时，其并不知情，而接收方根据该标识信息即可准确地确定出并非是机主本人发送的消息，进一步提高了消息发送的安全性。当然，还该实施例可以设置所述标识信息在接收端的应用界面中的显示模式。

[0036] 实施例2

[0037] 由于移动终端(如手机、平板电脑等)多配备有指纹识别功能，大部分移动终端的指纹识别功能需要通过按压移动终端的某个特定区域(如home键、背部按键)实现。随着全屏指纹识别技术的出现，特别是基于超声波的全屏指纹识别技术，使得用户可以通过按压移动终端触摸屏的任何一个部分，即可实现指纹识别操作。因此，为了详细说明本发明提供的消息发送方法，以下将结合一基于全屏指纹的消息方法实施例进行说明，当然，本实施例并不以全屏指纹为限，如图2所示，该实施例包括如下步骤：

[0038] 步骤S21：检测到点击即时通信软件的图标时，获取用户的全屏指纹特征信息。

[0039] 该实施例中的即时通信软件，具体可以是移动终端内安装的应用，可以用来发送消息。该实施例中的全屏指纹信息，即用户触摸移动终端触摸屏的任意位置时，所能够采集到的全屏指纹特征信息。

[0040] 该实施例虽然是在检测到点击即时通信软件的图标的事件时，执行获取用户的全屏指纹特征信息的操作，在其他的实施例中，还可以是在进入即时通信软件后，在检测到点击发送按钮的事件时，再执行获取用户的全屏指纹特征信息的操作，也即，还可以有其他的、与本实施例执行时机不同的实施例，来详细地说明本发明的发明构思。

[0041] 步骤S22：根据所述用户的指纹信息与即时通信软件的消息发送权限对应的全屏指纹特征信息的匹配结果，确定所述用户的消息发送权限。

[0042] 该实施例中，可以预先设定全屏指纹特征信息的与即时通信软件的消息发送权限的对应关系。例如，机主本人，可以设置机主的指纹特征信息为允许发送消息；可以设置预置授权用户(如机主的亲属)的指纹特征信息为允许发送消息；还可以设置其他未录入指纹特征信息的用户的消息发送权限(可以是允许发送消息，也可以是拒绝消息发送)。

[0043] 步骤S23：确定所述用户的具有消息发送权限时，在待发送的消息中添加与所述用户的全屏指纹特征信息相对应的标识信息。当然，如果确定所述用户的不具有消息发送权限时，则拒绝消息的发送。

[0044] 该标识信息具体可以是“发送于XX”，该处的标识信息与所述用户的生物特征信息相对应。例如，标识信息“发送于机主本人”与机主的生物特征信息相对应；标识信息“小孩误发”与机主家庭内小孩的生物特征信息相对应；标识信息“发送于未知用户”与未录入保存的生物特征信息相对应。

[0045] 此外，在该实施例执行之前，还可以设置所述标识信息在应用界面中的显示模式，所述显示模式包括显示和隐藏。这样，即使机主设置了其他任意生物标识信息均具有发送

消息的权限，其他任意生物标识信息可以是与标识信息“发送于未知用户”对应，不法分子在冒充机主发送虚假信息时，其并不知情，而接收方根据该标识信息即可准确地确定出并非是机主本人发送的消息，进一步提高了消息发送的安全性。

[0046] 步骤S24：发送添加标识信息后的所述消息。

[0047] 通过发送添加标识信息后的所述消息，接收方即可在接收到所述消息的同时，接收到标识信息，根据该标识信息，即可确定发送方的身份。

[0048] 通过本发明提供的消息发送方法，首先获取用户的全屏指纹特征信息，然后根据与即时通信软件的消息发送权限对应的全屏指纹特征信息的匹配结果，确定所述用户的消息发送权限，最终根据用户的消息发送权限控制消息的发送，由于在消息发送之前先验证用户的全屏指纹特征信息对应的消息发送权限，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

[0049] 在发送的消息中添加与获取到的用户的全屏指纹特征信息相对应的标识信息。由于该标识信息与上述获取到的用户的全屏指纹特征信息相对应，这样，接收方在接收到所述消息时，根据同时接收到的所述标识信息，即可准确地确定出发送方的身份，进一步避免了机主之外的其他用户冒充机主发送虚假信息时，容易致使接收方上当受骗的问题。

[0050] 该实施例基于移动终端的全屏指纹识别方式获取用户的全屏指纹特征信息，相对于home键或背部按键识别指纹的方法，无需用户特意去执行按压home键或背部按键的操作，对于消息发送方而言，可以在不增添任何额外操作的前提下下采集到用户的全屏指纹特征，并执行实施例2后续的方法步骤，使整个消息发送过程简单、便捷、安全，更有利于提高用户体验。

[0051] 实施例3

[0052] 基于相同的发明构思，本发明还提供一种移动终端实施例，用于提高消息发送的安全性，如图3所示，该移动终端包括：

[0053] 获取模块31，可以用于监听到满足预设消息发送条件时，获取用户的生物特征信息；

[0054] 权限确定模块32，可以用于根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；

[0055] 消息发送模块33，可以用于根据所述用户的控制权限控制消息的发送。

[0056] 通过本发明实施例提供的移动终端，获取模块首先获取用户的生物特征信息，然后权限确定模块根据与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，最终消息发送模块根据用户的控制权限控制消息的发送，由于在消息发送之前先验证用户的生物特征信息对应的控制权限，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

[0057] 上述消息发送模块33，具体可以用于根据所述用户的控制权限允许消息的发送，或，根据所述用户的控制权限拒绝消息的发送。

[0058] 另外，上述移动终端还可以包括标识信息添加模块(未图示)，可以用于在发送的消息中添加与所述用户的生物特征信息相对应的标识信息。

[0059] 另外，上述移动终端还可以包括显示模式控制模块(未图示)，可以用于设置所述标识信息在发送端的应用界面中为显示或隐藏；和/或，设置所述标识信息在接收端的应用

界面中为显示或隐藏。

[0060] 上述消息发送模块33，根据所述用户的控制权限控制消息的发送，包括：当所述用户不具备发送消息的控制权限时，在进入所述终端设备的应用界面后，控制所述应用界面中用于发送消息的按钮的状态为不可用；或，在进入所述终端设备的应用界面后，当点击所述应用界面中用于发送消息的按钮后，根据所述用户的控制权限，控制是否触发所述按钮的点击事件。

[0061] 所述生物特征信息包括屏幕指纹特征信息，则，权限确定模块32根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，具体包括：权限确定模块32将所述用户的屏幕指纹特征信息与终端设备的控制权限对应的指纹特征信息进行匹配，得到匹配结果；根据匹配结果，确定所述用户的控制权限。

[0062] 另外，上述移动终端还可以包括权限信息设置模块(未图示)，可以用于设置终端设备的控制权限和生物特征信息的对应关系。

[0063] 本发明实施例提供的移动终端能够实现图1至图2的方法实施例中移动终端实现的各个过程，为避免重复，这里不再赘述。通过本发明实施例提供的移动终端，首先获取用户的生物特征信息，然后根据与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，最终根据用户的控制权限控制消息的发送，由于在消息发送之前先验证用户的生物特征信息对应的控制权限，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

[0064] 另外，还可以在发送的消息中添加与获取到的用户的生物特征信息相对应的标识信息。由于该标识信息与上述获取到的用户的生物特征信息相对应，这样，接收方在接收到所述消息时，根据同时接收到的所述标识信息，即可确定出发送方的身份，进一步避免了机主之外的其他用户冒充机主发送虚假信息时，容易致使接收方上当受骗的问题。

[0065] 实施例4

[0066] 图4为实现本发明各个实施例的一种移动终端的硬件结构示意图，该移动终端400包括但不限于：射频单元401、网络模块402、音频输出单元403、输入单元404、传感器405、显示单元406、用户输入单元407、接口单元408、存储器409、处理器410、以及电源411等部件。本领域技术人员可以理解，图4中示出的移动终端结构并不构成对移动终端的限定，移动终端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。在本发明实施例中，移动终端包括但不限于手机、平板电脑、笔记本电脑、掌上电脑、车载终端、可穿戴设备、以及计步器等。

[0067] 其中，处理器410，用于在监听到满足预设消息发送条件时，获取用户的生物特征信息；根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限；根据所述用户的控制权限控制消息的发送。

[0068] 通过本发明提供的消息发送方法，首先获取用户的生物特征信息，然后根据与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限，最终根据用户的控制权限控制消息的发送，由于在消息发送之前先验证用户的生物特征信息，避免了机主用户之外的用户冒充机主发送虚假信息，容易致使接收方上当受骗的问题，从而提高了消息发送的安全性。

[0069] 应理解的是，本发明实施例中，射频单元401可用于收发信息或通话过程中，信号的接收和发送，具体的，将来自基站的下行数据接收后，给处理器410处理；另外，将上行的数据发送给基站。通常，射频单元401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、双工器等。此外，射频单元401还可以通过无线通信系统与网络和其他设备通信。

[0070] 移动终端通过网络模块402为用户提供了无线的宽带互联网访问，如帮助用户收发电子邮件、浏览网页和访问流式媒体等。

[0071] 音频输出单元403可以将射频单元401或网络模块402接收的或者在存储器409中存储的音频数据转换成音频信号并且输出为声音。而且，音频输出单元403还可以提供与移动终端400执行的特定功能相关的音频输出(例如，呼叫信号接收声音、消息接收声音等等)。音频输出单元403包括扬声器、蜂鸣器以及受话器等。

[0072] 输入单元404用于接收音频或视频信号。输入单元404可以包括图形处理器(Graphics Processing Unit,GPU)4041和麦克风4042，图形处理器4041对在视频捕获模式或图像捕获模式中由图像捕获装置(如摄像头)获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示单元406上。经图形处理器4041处理后的图像帧可以存储在存储器409(或其它存储介质)中或者经由射频单元401或网络模块402进行发送。麦克风4042可以接收声音，并且能够将这样的声音处理为音频数据。处理后的音频数据可以在电话通话模式的情况下转换为可经由射频单元401发送到移动通信基站的格式输出。

[0073] 移动终端400还包括至少一种传感器405，比如光传感器、运动传感器以及其他传感器。具体地，光传感器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4061的亮度，接近传感器可在移动终端400移动到耳边时，关闭显示面板4061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，可用于识别移动终端姿态(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；传感器405还可以包括指纹传感器、压力传感器、虹膜传感器、分子传感器、陀螺仪、气压计、湿度计、温度计、红外线传感器等，在此不再赘述。

[0074] 显示单元406用于显示由用户输入的信息或提供给用户的信息。显示单元406可包括显示面板4061，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4061。

[0075] 用户输入单元407可用于接收输入的数字或字符信息，以及产生与移动终端的用户设置以及功能控制有关的键信号输入。具体地，用户输入单元407包括触控面板4071以及其他输入设备4072。触控面板4071，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4071上或在触控面板4071附近的操作)。触控面板4071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410，接收处理器410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4071。除了触控面板4071，用户输入单元407还可以包括其他输入设备4072。具体地，其他输入设备4072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,在此不再赘述。

[0076] 进一步的,触控面板4071可覆盖在显示面板4061上,当触控面板4071检测到在其上或附近的触摸操作后,传送给处理器410以确定触摸事件的类型,随后处理器410根据触摸事件的类型在显示面板4061上提供相应的视觉输出。虽然在图4中,触控面板4071与显示面板4061是作为两个独立的部件来实现移动终端的输入和输出功能,但是在某些实施例中,可以将触控面板4071与显示面板4061集成而实现移动终端的输入和输出功能,具体此处不做限定。

[0077] 接口单元408为外部装置与移动终端400连接的接口。例如,外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。接口单元408可以用于接收来自外部装置的输入(例如,数据信息、电力等等)并且将接收到的输入传输到移动终端400内的一个或多个元件或者可以用于在移动终端400和外部装置之间传输数据。

[0078] 存储器409可用于存储软件程序以及各种数据。存储器409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409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、或其他易失性固态存储器件。

[0079] 处理器410是移动终端的控制中心,利用各种接口和线路连接整个移动终端的各个部分,通过运行或执行存储在存储器409内的软件程序和/或模块,以及调用存储在存储器409内的数据,执行移动终端的各种功能和处理数据,从而对移动终端进行整体监控。处理器410可包括一个或多个处理单元;优选的,处理器410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410中。

[0080] 移动终端400还可以包括给各个部件供电的电源411(比如电池),优选的,电源411可以通过电源管理系统与处理器410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。

[0081] 另外,移动终端400包括一些未示出的功能模块,在此不再赘述。

[0082] 优选的,本发明实施例还提供一种移动终端,包括处理器410,存储器409,存储在存储器409上并可在所述处理器410上运行的计算机程序,该计算机程序被处理器410执行时实现上述图1和图2所示的方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0083] 实施例5

[0084] 本发明实施例还提供一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,该计算机程序被处理器执行时实现上述图1和图2所示的方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。其中,所述的计算机可读存储介质,如只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等。

[0085] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排

他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0086] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0087] 上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本发明的保护之内。

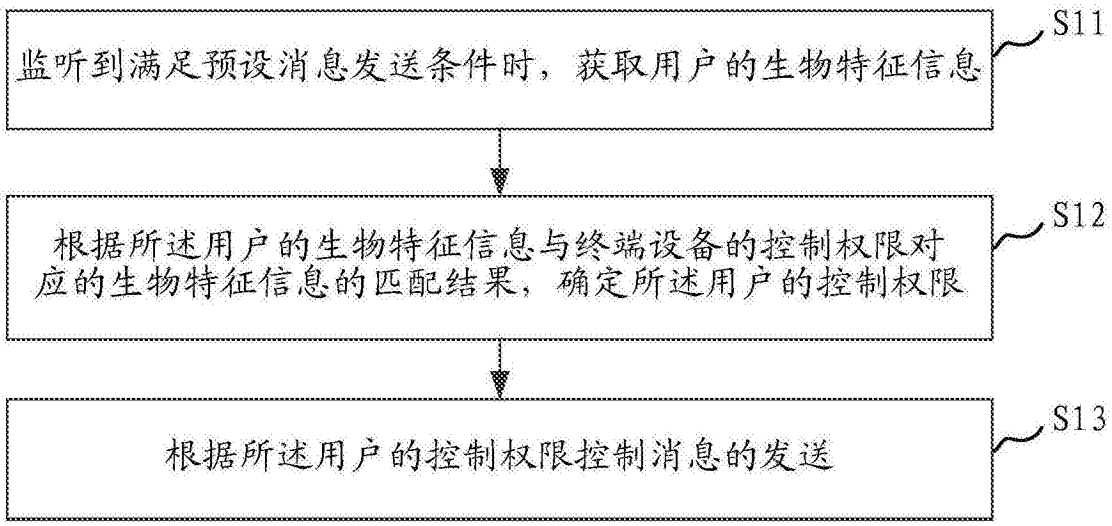

监听到满足预设消息发送条件时，获取用户的生物特征信息
S11
根据所述用户的生物特征信息与终端设备的控制权限对应的生物特征信息的匹配结果，确定所述用户的控制权限
S12
根据所述用户的控制权限控制消息的发送
S13

图1

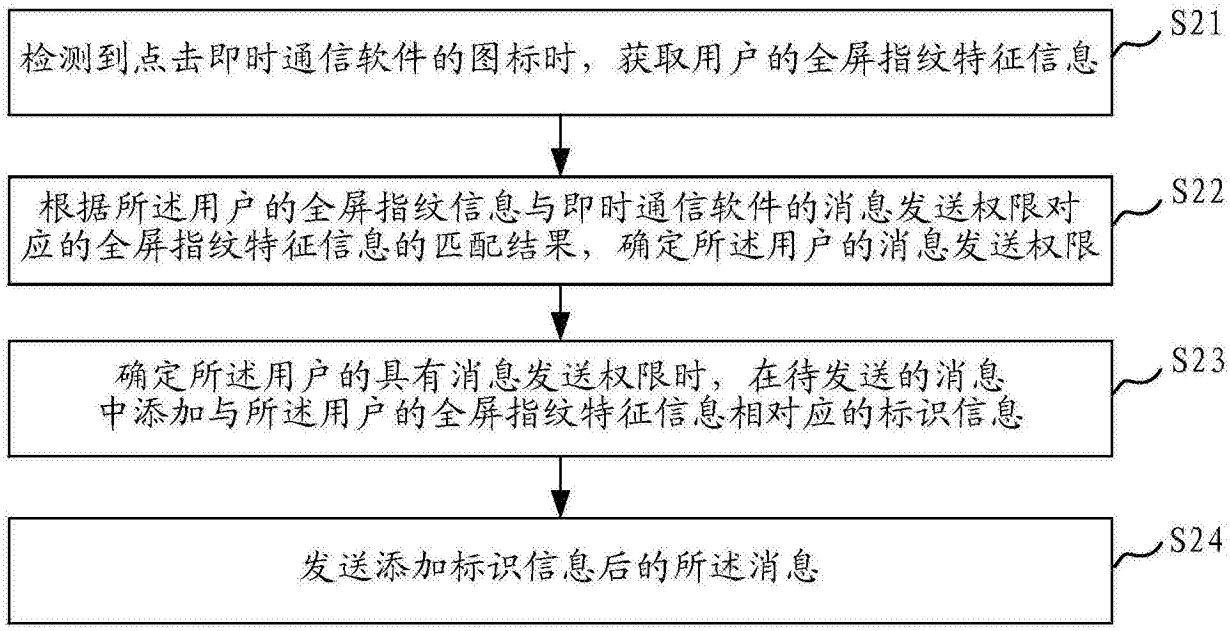

检测到点击即时通信软件的图标时，获取用户的全屏指纹特征信息
S21
根据所述用户的全屏指纹信息与即时通信软件的消息发送权限对应的全屏指纹特征信息的匹配结果，确定所述用户的消息发送权限
S22
确定所述用户的具有消息发送权限时，在待发送的消息中添加与所述用户的全屏指纹特征信息相对应的标识信息
S23
发送添加标识信息后的所述消息
S24

图2

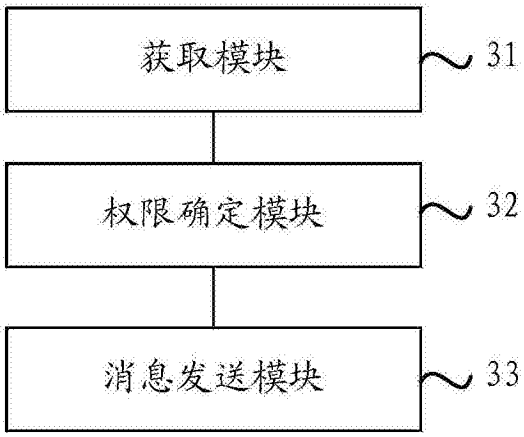

获取模块
31
权限确定模块
32
消息发送模块
33

图3

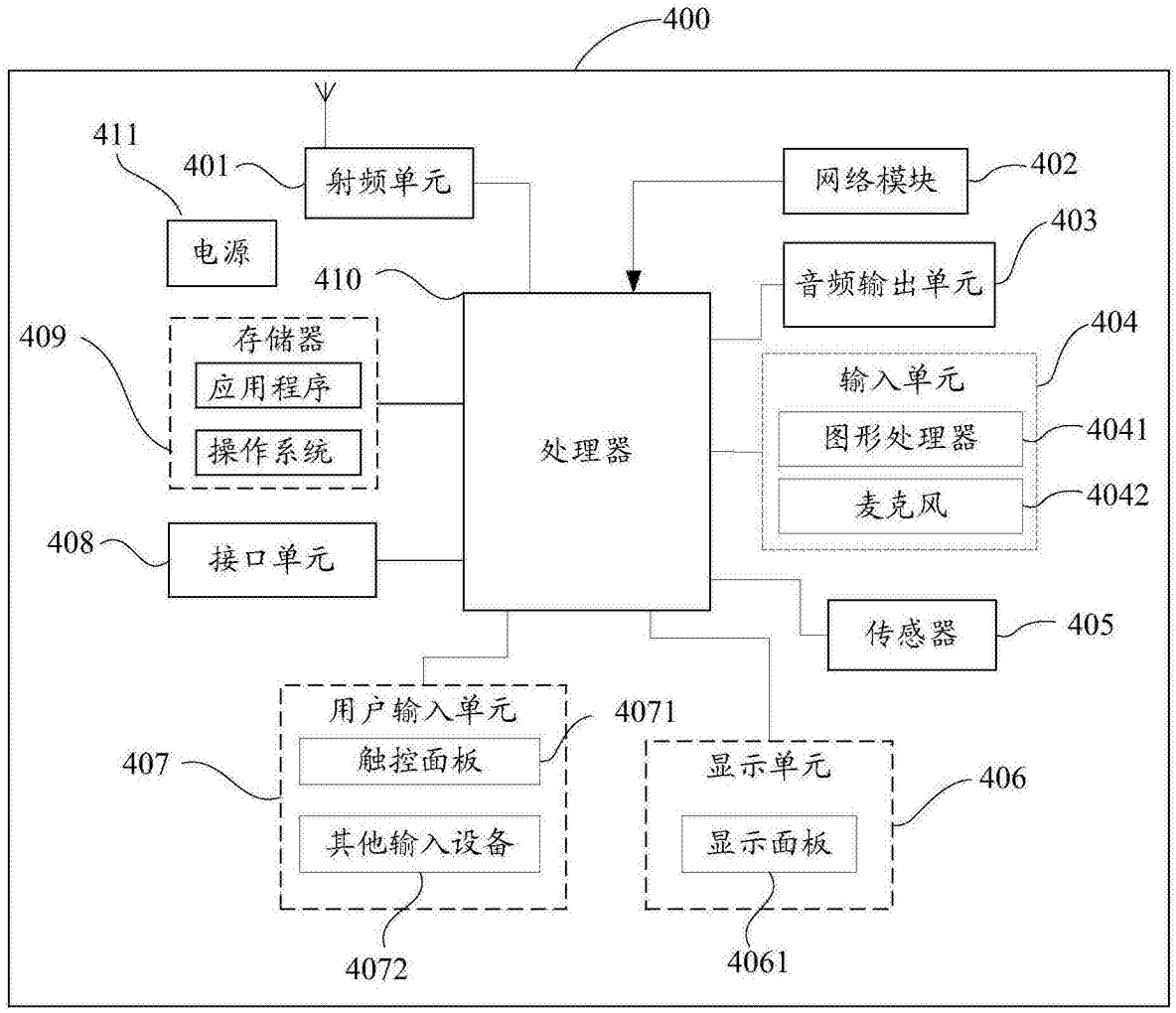

400
411
401
射频单元
网络模块
402
电源
403
音频输出单元
410
404
存储器
409
应用程序
输入单元
操作系统
处理器
4041
图形处理器
4042
麦克风
408
接口单元
传感器
405
用户输入单元
4071
407
触控面板
显示单元
406
其他输入设备
显示面板
4072
4061

图4