(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105550552 B
(45)授权公告日 2019.01.15

(21)申请号 201510374639.0

(22)申请日 2015.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 105550552 A

(43)申请公布日 2016.05.04

(73)专利权人 宇龙计算机通信科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新技术产业园(北区)梦溪道2号

(72)发明人 许行 许奕波 张碧君

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
G06F 21/32(2013.01)

(56)对比文件
CN 103118174 A,2013.05.22,说明书第[0005]-[0035]段,附图1-3.
US 2014/0335862 A1,2014.11.13,全文.
CN 104484970 A,2015.04.01,全文.
CN 103745148 A,2014.04.23,说明书第[0004]-[0022]段,附图1-2.

审查员 胡学岭

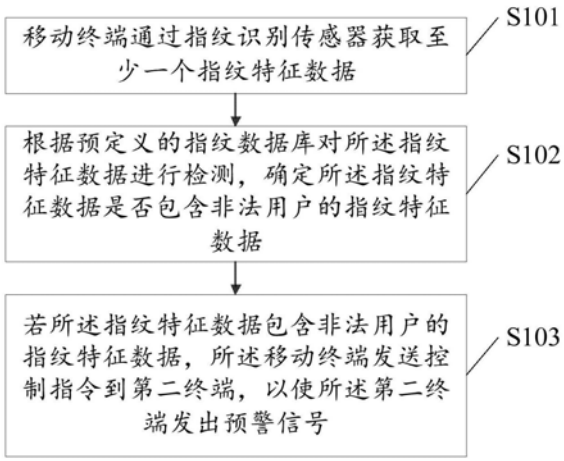
权利要求书2页 说明书9页 附图6页

(54)发明名称

一种移动终端的保护方法及装置

(57)摘要

本发明实施例公开了一种移动终端的保护方法及装置,其中该方法包括:移动终端通过指纹识别传感器获取至少一个指纹特征数据;根据预定义的指纹数据库对所述指纹特征数据进行检测,确定所述指纹特征数据是否包含非法用户的指纹特征数据;若所述指纹特征数据包含非法用户的指纹特征数据,所述移动终端发送控制指令到第二终端,以使所述第二终端发出预警信号。实施本发明实施例,当检测到接近或触碰移动终端的用户的身份非法时,在第二终端上发出预警信号,提升了移动终端的安全性。



CN 105550552 B

1.一种移动终端的保护方法,其特征在于,所述方法包括:

移动终端通过指纹识别传感器获取至少一个指纹特征数据,其中,所述指纹特征数据是通过对用户的指纹图像进行去噪处理后所提取得到的,所述用户的指纹图像是通过超声波指纹识别传感器获取的二维指纹图像和三维指纹图像;

根据预定义的指纹数据库对所述指纹特征数据进行检测,确定所述指纹特征数据是否包含非法用户的指纹特征数据;

若所述指纹特征数据包含非法用户的指纹特征数据,所述移动终端发送控制指令到第二终端,包括:若在所述指纹特征数据中检测到非法用户的指纹特征数据,且在所述指纹特征数据中检测到至少一个的合法用户的指纹特征数据,控制在所述第二终端上产生第一强度的预警信号;若在指纹特征数据中检测到非法用户的指纹特征数据,且未检测到至少一个的合法用户的指纹特征数据,则控制在所述第二终端上产生第二强度的预警信号,所述第一强度小于所述第二强度。

2.如权利要求1所述的方法,其特征在于,所述移动终端通过指纹识别传感器获取至少一个指纹特征数据,包括:

所述移动终端通过指纹识别传感器获取用户的指纹图像;

根据所述用户的指纹图像获得用户的至少一个指纹特征数据,所述指纹特征数据用于用户的身份鉴定。

3.如权利要求2所述的方法,其特征在于,所述移动终端通过指纹识别传感器获取用户的指纹图像,包括:

所述移动终端通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像,所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像;或

所述移动终端通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像。

4.如权利要求1-3任一项所述的方法,其特征在于,

所述预定义的指纹数据库包括合法用户的指纹特征数据;

所述根据预定义的指纹数据库对所述指纹特征数据进行检测,确定所述指纹特征数据是否包含非法用户的指纹特征数据,包括:

计算所述合法用户的指纹特征数据与所述指纹特征数据的匹配相似度;

若所述匹配相似度不大于预设阈值,确定所述指纹特征数据包含非法用户的指纹特征数据。

5.如权利要求1-3任一项所述的方法,其特征在于,

所述预定义的指纹数据库包括非法用户的指纹特征数据;

所述根据预定义的指纹数据库对所述指纹特征数据进行检测,确定所述指纹特征数据是否包含非法用户的指纹特征数据,包括:

计算所述非法用户的指纹特征数据与所述指纹特征数据的匹配相似度;

若所述匹配相似度大于预设阈值,确定所述指纹特征数据包含非法用户的指纹特征数据。

6.一种移动终端的保护装置,其特征在于,所述装置包括:

获取模块,用于在移动终端上通过指纹识别传感器获取至少一个指纹特征数据,其中,

所述指纹特征数据是通过对用户的指纹图像进行去噪处理后所提取得到的，所述用户的指纹图像是通过超声波指纹识别传感器获取的二维指纹图像和三维指纹图像；

检测模块，用于根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据；

预警模块，用于若所述指纹特征数据包含非法用户的指纹特征数据，从所述移动终端发送控制指令到第二终端，包括：若在所述指纹特征数据中检测到非法用户的指纹特征数据，且在所述指纹特征数据中检测到至少一个的合法用户的指纹特征数据，控制在所述第二终端上产生第一强度的预警信号；若在指纹特征数据中检测到非法用户的指纹特征数据，且未检测到至少一个的合法用户的指纹特征数据，则控制在所述第二终端上产生第二强度的预警信号，所述第一强度小于所述第二强度。

7.如权利要求6所述的装置，其特征在于，所述获取模块包括：

图像获取单元，用于在所述移动终端上通过指纹识别传感器获取用户的指纹图像；

特征提取单元，用于根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定。

8.如权利要求7所述的装置，其特征在于，所述图像获取单元包括：

超声获取子单元，用于在所述移动终端上通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像，所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像；

按压获取子单元，用于在所述移动终端上通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像。

9.如权利要求6-8任一项所述的装置，其特征在于，

所述预定义的指纹数据库包括合法用户的指纹特征数据；

所述检测模块包括：

第一匹配单元，用于计算所述合法用户的指纹特征数据与所述指纹特征数据的匹配相似度；

第一确定单元，用于若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

10.如权利要求6-8任一项所述的装置，其特征在于，

所述预定义的指纹数据库包括非法用户的指纹特征数据；

所述检测模块包括：

第二匹配单元，用于计算所述非法用户的指纹特征数据与所述指纹特征数据的匹配相似度；

第二确定单元，用于若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

一种移动终端的保护方法及装置

技术领域

[0001] 本发明涉及移动通信领域，尤其涉及一种移动终端的保护方法及装置。

背景技术

[0002] 现实生活中，以智能手机为代表的移动终端的失窃现象屡见不鲜。伴随着移动互联网与人们生活的深度结合，智能手机已成为用户重要的个人物品。加强对智能手机等移动终端的保护成为一个热点话题。

[0003] 目前的移动终端主要是通过远程控制的方法来达到防盗保护及找回的目的，比如苹果手机可以通过“查找iPhone”应用获取苹果的终端设备的地理位置信息、远程控制苹果的终端设备发出铃声、远程格式化内存数据等，安装了“腾讯手机管家”应用的移动终端在开启了“手机防盗”功能选项后，一旦移动终端丢失或者被盗了，只要该移动终端有更换SIM(Subscriber Identity Module，用户身份识别模块)卡，会将更换后的号码通过短信的方式发送给用户设置的紧急联系人，也会发邮件到预设邮箱，提醒用户手机可能被盗，可登陆应用的官方网站来远程控制该移动终端。但是，以上的保护方法都是在移动终端丢失后的补救措施，不能防止移动终端被盗走。

发明内容

[0004] 本发明实施例提供一种移动终端的保护方法及装置，当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0005] 本发明一方面提供了一种移动终端的保护方法，包括：

[0006] 移动终端通过指纹识别传感器获取至少一个指纹特征数据；

[0007] 根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据；

[0008] 若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0009] 本发明另一方面还提供了一种移动终端的保护装置，包括：

[0010] 获取模块，用于在移动终端上通过指纹识别传感器获取至少一个指纹特征数据；

[0011] 检测模块，用于根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据；

[0012] 预警模块，用于若所述指纹特征数据包含非法用户的指纹特征数据，从所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0013] 实施本发明实施例，具有如下有益效果：

[0014] 本发明实施例通过移动终端通过指纹识别传感器获取至少一个指纹特征数据，根据预定义的指纹数据库对该指纹特征数据进行检测，确定该指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端

的保护。本发明实施例中，当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

附图说明

[0015] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要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他的附图。

[0016] 图1为本发明实施例提供的一种移动终端的保护方法的流程图；

[0017] 图2为本发明实施例提供的超声波指纹识别传感器的工作原理图；

[0018] 图3为本发明实施例提供的另一种移动终端的保护方法的流程图；

[0019] 图4为本发明实施例提供的又一种移动终端的保护方法的流程图；

[0020] 图5为本发明实施例提供的又一种移动终端的保护方法的流程图；

[0021] 图6为本发明实施例提供的又一种移动终端的保护方法的流程图；

[0022] 图7为本发明实施例提供的一种移动终端的保护装置的结构示意图；

[0023] 图8为本发明实施例提供的获取模块的一个实施例的结构示意图；

[0024] 图9为本发明实施例提供的图像获取单元的一个实施例的结构示意图；

[0025] 图10为本发明实施例提供的检测模块的一个实施例的结构示意图。

具体实施方式

[0026] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅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。

[0027] 本发明实施例中，移动终端可以是智能手机、平板电脑、PC(Personal Computer，个人计算机)、电子阅读器等设备中的任一种，第二终端可以是智能手机、平板电脑、智能眼镜、智能手环、智能手表等设备中的任一种，优选的，将可穿戴智能设备作为第二终端。

[0028] 下面将结合附图1-附图6，对本发明实施例提供的移动终端的保护方法进行详细说明。

[0029] 请参见图1，为本发明实施例提供的一种移动终端的保护方法的流程图，该方法可包括步骤S101-S103。

[0030] S101，移动终端通过指纹识别传感器获取至少一个指纹特征数据。

[0031] 作为一种可选的实施方式，移动终端具有指纹识别功能，移动终端通过内置的指纹识别传感器获取指纹特征数据。进一步可选的，指纹识别传感器可独立于移动终端而存在，移动终端与指纹识别传感器之间通过无线网络相连接，移动终端接收由指纹识别传感器采集并发送的指纹特征数据。

[0032] 作为一种可选的实施方式，移动终端的机身内置了一个或多个的超声波指纹识别传感器，该传感器可置于终端屏幕内层，也可以内嵌于构成机身的塑料或金属外壳里，本发明实施例对此不做限定。如图2所示，为超声波指纹识别传感器的工作原理图，超声波指纹

识别传感器向周边空间发射一定频率的超声波，检测超声探测范围内的物体，若被探测物体是人体手指，超声波在遇到人体手指后会产生反射波，人体手指表面凹凸不平的指纹纹路导致不同位置上的反射波的延迟时间各不相同，通过分析接收到的反射波可以得到该手指的指纹图像，该指纹图像既可以是二维的，也可以是三维的，能够准确地捕捉指纹上的纹路。基于超声波指纹识别传感器的指纹图像获取方式，即便用户手指上沾有水、灰尘、油脂等杂物，也不会影响所获取的指纹图像的准确性；同时，超声波指纹识别传感器能检测超声探测范围内的所有物体，这意味着不需要被探测物体与移动终端存在直接接触。超声波指纹识别传感器获得一个或多个手指的指纹图像，从中可提取出至少一个指纹特征数据，用于鉴定用户的身份。

[0033] 作为一种可选的实施方式，移动终端的机身内置了按压式指纹识别传感器，该按压式指纹识别传感器可处于机框沿、机身背面、机身正面的屏幕上，以便在用户握持移动终端时采集用户的指纹。移动终端通过按压式指纹识别传感器获得包括一个或多个手指指纹的指纹图像，并从所述指纹图像中提取出至少一个指纹特征数据，用于鉴定用户的身份。

[0034] S102，根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据。

[0035] 作为一种可选的实施方式，移动终端上存储了预定义的指纹数据库，该指纹数据库用于对获得的用户的指纹特征数据进行检测，判断用户身份的合法性。预定义的指纹数据库可存储于内存或ROM中，通常是由该移动终端的管理员用户设置的。在对指纹特征数据进行检测之前，管理员用户获取移动终端的控制权限，进入预定义的指纹数据库的初始化步骤，将至少一个手指的指纹录入到移动终端中。

[0036] 作为一种可选的实施方式，预定义的指纹数据库包括合法用户的指纹特征数据，根据预定义的指纹数据库对获得的指纹特征数据进行检测，确定指纹特征数据是否包含非法用户的指纹特征数据。首先遍历计算合法用户的指纹特征数据与每一个指纹特征数据的匹配相似度，若当前参与匹配相似度计算的指纹特征数据与任意一个合法用户的指纹特征数据的匹配相似度都不大于预设阈值，确定当前参与匹配相似度计算的指纹特征数据不属于合法用户的指纹特征数据，即步骤S101中获得的指纹特征数据包含非法用户的指纹特征数据。

[0037] 作为一种可选的实施方式，预定义的指纹数据库包括非法用户的指纹特征数据，根据预定义的指纹数据库对获得的指纹特征数据进行检测，确定指纹特征数据是否包含非法用户的指纹特征数据。首先遍历计算非法用户的指纹特征数据与每一个指纹特征数据的匹配相似度，若当前参与匹配相似度计算的指纹特征数据与其中一个非法用户的指纹特征数据的匹配相似度大于预设阈值，确定步骤S101中获得的指纹特征数据包含非法用户的指纹特征数据。

[0038] S103，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0039] 作为一种可选的实施方式，在确定指纹特征数据包含非法用户的指纹特征数据时，认定当前场景下该移动终端存在非善意的触碰或接近，面临一定程度的失窃风险，移动终端生成并发送控制指令到第二终端，所述控制指令用于在第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。优选的，可将用户的可穿戴智能设备作为第二终端，比

如智能手表、智能手环、智能眼镜等。第二终端与移动终端之间存在包括近场通信(Near Field Communication,NFC)、蓝牙、Wi-Fi的无线连接。通过在第二终端上产生LED灯闪烁、终端振动、播放铃声等预警信号,使用户能及时地去查看移动终端的状态,加强对移动终端的保护。例如当第二终端与移动终端之间存在NFC的连接时,移动终端通过近场通信单元将控制指令发送到第二终端上,以使第二终端产生预警信号。

[0040] 进一步可选的,第二终端在接收到控制指令后,根据预存的配置表生成预警信号。该配置表维护了第二终端的类型与优选的预警信号之间的映射关系。比如当第二终端为智能手表时,在接收到控制指令后,根据预存的配置表中的映射关系产生响铃、振动等形式的预警信号;当第二终端为智能手环时,则产生LED灯闪烁、振动等形式的预警信号;当第二终端为智能眼镜时,则在镜片上显示预设的提示信息等。

[0041] 进一步可选的,若在指纹特征数据中只检测到非法用户的指纹特征数据,同时没检测到至少一个的合法用户的指纹特征数据,则认为移动终端面临较高的失窃风险,可控制在第二终端上产生的更明显的预警信号,比如更高频率的LED灯闪烁、更强烈的终端振动、播放更急促的铃声等。

[0042] 本发明实施例中,移动终端通过指纹识别传感器获取至少一个指纹特征数据,根据预定义的指纹数据库对所述指纹特征数据进行检测,确定所述指纹特征数据是否包含非法用户的指纹特征数据,若所述指纹特征数据包含非法用户的指纹特征数据,所述移动终端发送控制指令到第二终端,在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时,在第二终端上发出预警信号,提升了移动终端的安全性。

[0043] 请参见图3,为本发明实施例提供的另一种移动终端的保护方法的流程图,该方法可包括步骤S301-S305。

[0044] S301,所述移动终端通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像,所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像。

[0045] 作为一种可选的实施方式,移动终端的机身内置了一个或多个的超声波指纹识别传感器,该传感器可置于终端屏幕内层,也可以内嵌于构成机身的塑料或金属外壳里,本发明实施例对此不做限定。超声波指纹识别传感器向周边空间发射的超声波在遇到人体手指后会产生反射波,人体手指表面凹凸不平的指纹纹路导致不同位置上的反射波的延迟时间各不相同,通过分析接收到的反射波可以得到该手指的指纹图像,该指纹图像既可以是二维的,也可以是三维的,能够准确地捕捉指纹上的纹路。基于超声波指纹识别传感器的指纹图像获取方式,即便用户手指上沾有水、灰尘、油脂等杂物,也不会影响所获取的指纹图像的准确性;同时,超声波指纹识别传感器能检测超声探测范围内的所有物体,这意味着不需要被探测物体与移动终端存在直接接触。假设此处移动终端的超声波指纹识别传感器的超声探测距离为15cm,若在距离移动终端机身10cm处有手指靠近,则可获得手指的指纹图像。

[0046] S302,根据所述用户的指纹图像获得用户的至少一个指纹特征数据,所述指纹特征数据用于用户的身份鉴定。

[0047] 作为一种可选的实施方式,对步骤S301中获得的用户的指纹图像执行图像去噪等预处理操作后,在该指纹图像上运行指纹特征提取算法。对特征信息不足的指纹特征数据

予以舍弃，得到至少一个指纹特征数据。假设这里得到了两个指纹特征数据，分别为Pm1和Pm2。

[0048] S303，计算包括合法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度。

[0049] 作为一种可选的实施方式，移动终端预先录入并保存了一个预定义的指纹数据库，具有管理员权限的用户在该移动终端上预先录入了一个或多个的合法用户的指纹特征数据作为预定义的指纹数据库。遍历计算S302中得到的每一个指纹特征数据与预定义的指纹数据库的匹配相似度。假设这里的合法用户的指纹特征数据为Pm3和Pm4，一共需计算Pm1与Pm3、Pm1与Pm4、Pm2与Pm3、Pm2与Pm4这四对数据的匹配相似度。

[0050] S304，若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0051] 作为一种可选的实施方式，若在步骤S303中的匹配相似度计算中，某一个指纹特征数据与任意一个合法用户的指纹特征数据的匹配相似度都不大于预设阈值，确定该指纹特征数据不属于合法用户的指纹特征数据，即步骤S302中获得的指纹特征数据包含非法用户的指纹特征数据。例如预设阈值为0.99，Pm1与Pm3、Pm1与Pm4、Pm2与Pm3、Pm2与Pm4这四对数据的匹配相似度分别为0.57、0.45、0.55、0.997，可确定Pm2属于合法用户的指纹特征数据，Pm1不属于合法用户的指纹特征数据，Pm1和Pm2中包含非法用户的指纹特征数据。

[0052] S305，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0053] 作为一种可选的实施方式，在确定指纹特征数据包含非法用户的指纹特征数据时，认定当前场景下该移动终端存在非善意的触碰或接近，面临一定程度的失窃风险，移动终端生成并发送控制指令到第二终端，所述控制指令用于在第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。优选的，可将用户的可穿戴智能设备作为第二终端，比如智能手表、智能手环、智能眼镜等。第二终端与移动终端之间存在包括近场通信(Near Field Communication，NFC)、蓝牙、Wi-Fi的无线连接。通过在第二终端上产生LED灯闪烁、终端振动、播放铃声等预警信号，使用户能及时地去查看移动终端的状态，加强对移动终端的保护。例如当第二终端与移动终端之间存在NFC的连接时，移动终端通过近场通信单元将控制指令发送到第二终端上，以使第二终端产生预警信号。

[0054] 进一步可选的，第二终端在接收到控制指令后，根据预存的配置表生成预警信号。该配置表维护了第二终端的类型与优选的预警信号之间的映射关系。比如当第二终端为智能手表时，在接收到控制指令后，根据预存的配置表中的映射关系产生响铃、振动等形式的预警信号；当第二终端为智能手环时，则产生LED灯闪烁、振动等形式的预警信号；当第二终端为智能眼镜时，则在镜片上显示预设的提示信息等。

[0055] 进一步可选的，若在指纹特征数据中只检测到非法用户的指纹特征数据，同时没检测到至少一个的合法用户的指纹特征数据，则认为移动终端面临较高的失窃风险，可控制在第二终端上产生的更明显的预警信号，比如更高频率的LED灯闪烁、更强烈的终端振动、播放更急促的铃声等。

[0056] 本发明实施例中，移动终端通过超声波指纹识别传感器获取至少一个指纹特征数据，根据包括合法用户的指纹特征数据的预定义的指纹数据库对所述指纹特征数据进行检

测，确定所述指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0057] 请参见图4，为本发明实施例提供的又一种移动终端的保护方法的流程图，该方法可包括步骤S401-S405。

[0058] S401，所述移动终端通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像，所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像。

[0059] S402，根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定。

[0060] S403，计算包括非法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度。

[0061] 作为一种可选的实施方式，预定义的指纹数据库包括非法用户的指纹特征数据，根据预定义的指纹数据库对获得的指纹特征数据进行检测，确定指纹特征数据是否包含非法用户的指纹特征数据。具有管理员权限的用户在该移动终端上预先录入了一个或多个的非法用户的指纹特征数据作为预定义的指纹数据库。遍历计算获取到的每一个指纹特征数据与预定义的指纹数据库的匹配相似度。假设这里的非法用户的指纹特征数据为Pm5和Pm6，获取到的指纹特征数据为Pm7和Pm8，一共需计算Pm7与Pm5、Pm7与Pm6、Pm8与Pm5、Pm8与Pm6这四对数据的匹配相似度。

[0062] S404，若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0063] 若在步骤S403中的匹配相似度计算中，某一个指纹特征数据与任意一个非法用户的指纹特征数据的匹配相似度大于预设阈值，确定该指纹特征数据是非法用户的指纹特征数据，即步骤S402中获得的指纹特征数据包含非法用户的指纹特征数据。例如预设阈值为0.99，Pm7与Pm5、Pm7与Pm6、Pm8与Pm5、Pm8与Pm6这四对数据的匹配相似度分别为0.998、0.45、0.55、0.37，可确定Pm7是非法用户的指纹特征数据，Pm7和Pm8中包含非法用户的指纹特征数据。

[0064] S405，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0065] 本发明实施例中的步骤S401～S402、步骤S405的具体功能可分别参见图3所示的方法的步骤S301～S302、步骤S305，在此不赘述。

[0066] 本发明实施例中，移动终端通过超声波指纹识别传感器获取至少一个指纹特征数据，根据包括非法用户的指纹特征数据的预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0067] 请参见图5，为本发明实施例提供的又一种移动终端的保护方法的流程图，该方法

可包括步骤S501-S505。

[0068] S501，所述移动终端通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像。

[0069] 作为一种可选的实施方式，移动终端的机身内置了按压式指纹识别传感器，该按压式指纹识别传感器可处于机框沿、机身背面、机身正面的屏幕上，以便在用户握持移动终端时采集用户的指纹。当检测到有用户的手指碰触到移动终端时，该移动终端通过按压式指纹识别传感器获得包括一个或多个手指指纹的指纹图像。

[0070] S502，根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定。

[0071] S503，计算包括合法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度。

[0072] S504，若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0073] S505，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0074] 本发明实施例中的步骤S502～S505的具体功能可参见图3所示的方法的步骤S302～S305，在此不赘述。

[0075] 本发明实施例中，移动终端通过按压式指纹识别传感器获取至少一个指纹特征数据，根据包括合法用户的指纹特征数据的预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0076] 请参见图6，为本发明实施例提供的又一种移动终端的保护方法的流程图，该方法可包括步骤S601-S605。

[0077] S601，所述移动终端通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像。

[0078] S602，根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定。

[0079] S603，计算包括非法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度。

[0080] S604，若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0081] S605，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0082] 本发明实施例中的步骤S601、S602～S605的具体功能可分别参见图5所示的方法的步骤S501、图4所示的方法的步骤S402～S405，在此不赘述。

[0083] 本发明实施例中，移动终端通过按压式指纹识别传感器获取至少一个指纹特征数据，根据包括非法用户的指纹特征数据的预定义的指纹数据库对所述指纹特征数据进行检

测，确定所述指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0084] 下面将结合附图7-附图10，对本发明实施例提供的移动终端的保护装置进行详细介绍。

[0085] 请参见图7，为本发明实施例提供的一种移动终端的保护装置的结构示意图，该装置包括：获取模块701、检测模块702、预警模块703。

[0086] 获取模块701，用于在移动终端上通过指纹识别传感器获取至少一个指纹特征数据。

[0087] 检测模块702，用于根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据。

[0088] 预警模块703，用于若所述指纹特征数据包含非法用户的指纹特征数据，从所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号。

[0089] 本发明实施例中的获取模块701～预警模块703的具体功能可参见图1所示的方法的步骤S101～S103，在此不赘述。

[0090] 请参见图8，为本发明实施例提供的获取模块701的一个实施例的结构示意图，获取模块701可包括：图像获取单元7011、特征提取单元7012。

[0091] 图像获取单元7011，用于在所述移动终端上通过指纹识别传感器获取用户的指纹图像。

[0092] 特征提取单元7012，用于根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定。

[0093] 本发明实施例中的特征提取单元7012的具体功能可参见图3所示的方法的步骤S302，在此不赘述。

[0094] 作为一种可选的实施方式，本发明实施例中的图像获取单元7011的一个实施例的结构示意图可参见图9，图像获取单元7011可包括：超声获取子单元70111、按压获取子单元70112。

[0095] 超声获取子单元70111，用于在所述移动终端上通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像，所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像。

[0096] 按压获取子单元70112，用于在所述移动终端上通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像。

[0097] 超声获取子单元70111、按压获取子单元70112的具体功能可分别参见图3所示的方法的步骤S301、图5所示的方法的步骤S501，在此不赘述。包含超声获取子单元70111的图像获取单元7011可应用于图3及图4所示的方法，包含按压获取子单元70112的图像获取单元7011可应用于图5及图6所示的方法。

[0098] 请参见图10，为本发明实施例提供的检测模块702的一个实施例的结构示意图，检测模块702可包括：第一匹配单元70211、第一确定单元70212、第二匹配单元70221、第二确定单元70222。

[0099] 若所述预定义的指纹数据库包括合法用户的指纹特征数据，所述检测模块702包括：

[0100] 第一匹配单元70211，用于计算所述合法用户的指纹特征数据与所述指纹特征数据的匹配相似度。

[0101] 第一确定单元70212，用于若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0102] 若所述预定义的指纹数据库包括非法用户的指纹特征数据，所述检测模块702包括：

[0103] 第二匹配单元70221，用于计算所述非法用户的指纹特征数据与所述指纹特征数据的匹配相似度。

[0104] 第二确定单元70222，用于若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据。

[0105] 本发明实施例中的第一匹配单元70211、第一确定单元70212的具体功能可参见图3所示的方法的步骤S303、S304，第二匹配单元70221、第二确定单元70222的具体功能可参见图4所示的方法的步骤S403、S404，在此不赘述。包含第一匹配单元70211和第一确定单元70212的检测模块702可应用于图3及图5所示的方法，包含第二匹配单元70221和第二确定单元70222的检测模块702可应用于图4及图6所示的方法。

[0106] 本发明实施例中，移动终端通过指纹识别传感器获取至少一个指纹特征数据，根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据，若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，在所述第二终端上产生预警信号以提醒用户加强对所述移动终端的保护。本发明实施例当检测到接近或触碰移动终端的用户的身份非法时，在第二终端上发出预警信号，提升了移动终端的安全性。

[0107] 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流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0108] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

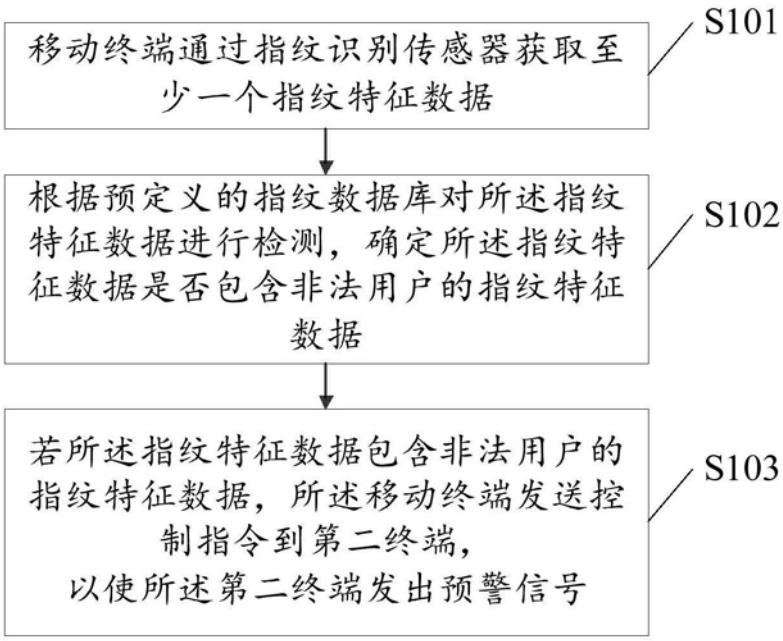

移动终端通过指纹识别传感器获取至少一个指纹特征数据
S101
根据预定义的指纹数据库对所述指纹特征数据进行检测，确定所述指纹特征数据是否包含非法用户的指纹特征数据
S102
若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，
以使所述第二终端发出预警信号
S103

图1


移动终端屏幕

图2

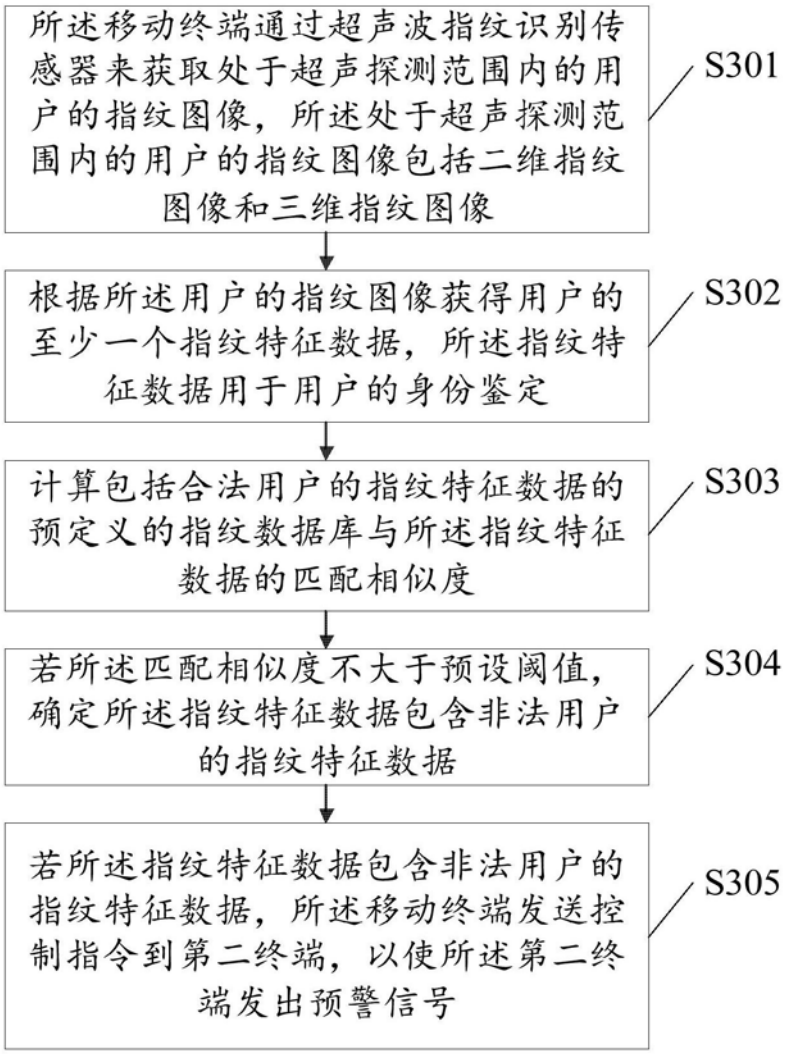

所述移动终端通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像，所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像
S301
根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定
S302
计算包括合法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度
S303
若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据
S304
若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号
S305

图3

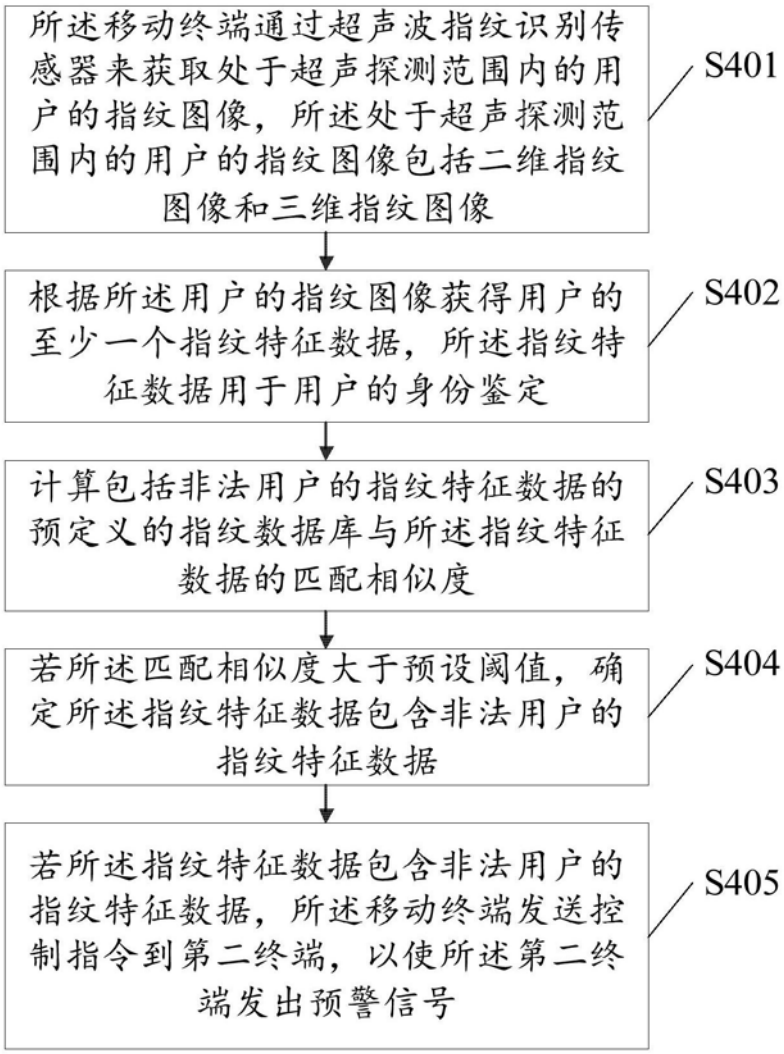

所述移动终端通过超声波指纹识别传感器来获取处于超声探测范围内的用户的指纹图像，所述处于超声探测范围内的用户的指纹图像包括二维指纹图像和三维指纹图像
S401
根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定
S402
计算包括非法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度
S403
若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据
S404
若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号
S405

图4

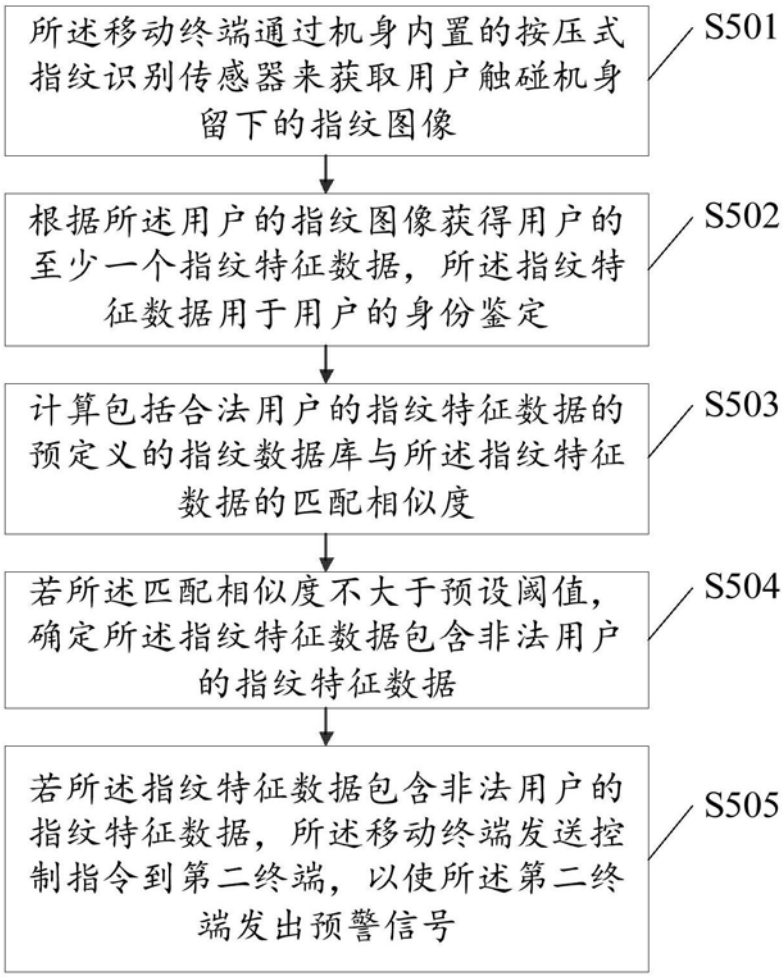

所述移动终端通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像
S501
根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定
S502
计算包括合法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度
S503
若所述匹配相似度不大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据
S504
若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号
S505

图5

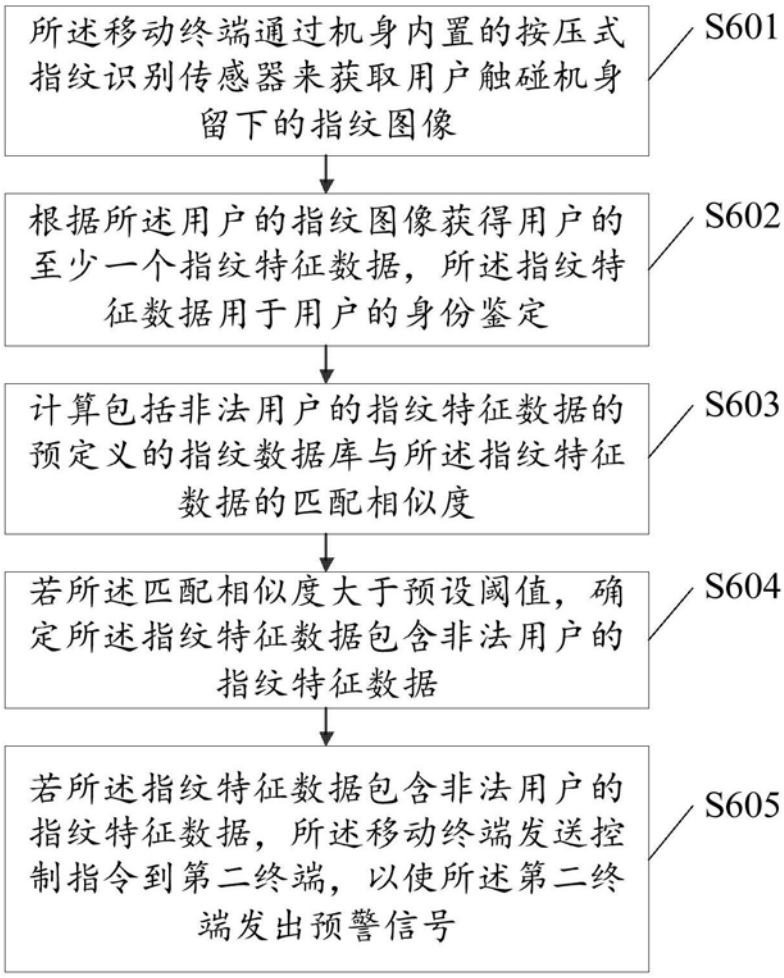

所述移动终端通过机身内置的按压式指纹识别传感器来获取用户触碰机身留下的指纹图像
S601
根据所述用户的指纹图像获得用户的至少一个指纹特征数据，所述指纹特征数据用于用户的身份鉴定
S602
计算包括非法用户的指纹特征数据的预定义的指纹数据库与所述指纹特征数据的匹配相似度
S603
若所述匹配相似度大于预设阈值，确定所述指纹特征数据包含非法用户的指纹特征数据
S604
若所述指纹特征数据包含非法用户的指纹特征数据，所述移动终端发送控制指令到第二终端，以使所述第二终端发出预警信号
S605

图6


移动终端的保护装置
获取模块
701
检测模块
702
预警模块
703

图7

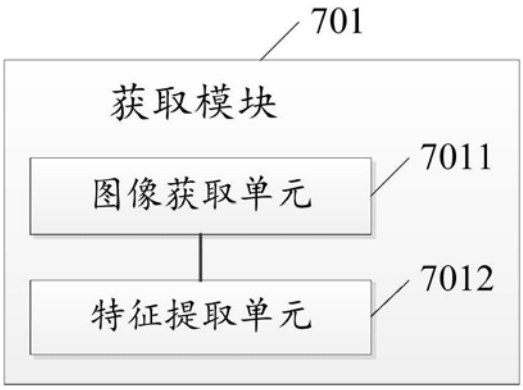

701
获取模块
7011
图像获取单元
7012
特征提取单元

图8

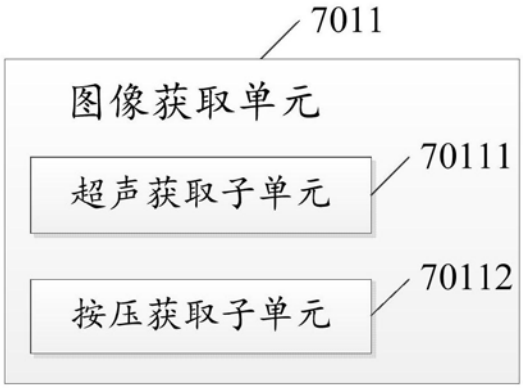

7011
图像获取单元
70111
超声获取子单元
70112
按压获取子单元

图9

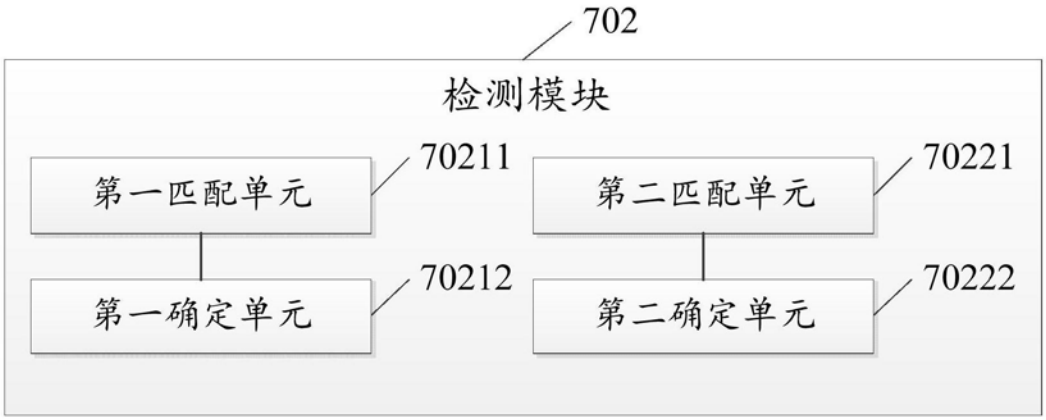

702
检测模块
70211
第一匹配单元
70212
第一确定单元
70221
第二匹配单元
70222
第二确定单元

图10