(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 106407779 A
(43)申请公布日 2017.02.15

(21)申请号 201610806164.2

(22)申请日 2016.09.05

(71)申请人 广东欧珀移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 彭凡

(74)专利代理机构 深圳翼盛智成知识产权事务所(普通合伙) 44300
代理人 黄威

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

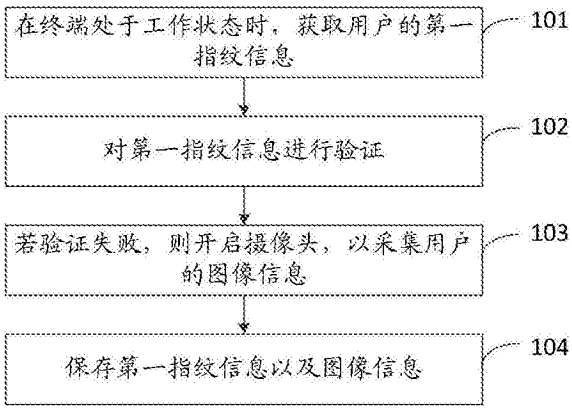
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种信息获取方法、装置和终端

(57)摘要

本发明实施例公开了一种信息获取方法、装置和终端;该信息获取方法采用在终端处于工作状态时,获取用户的第一指纹信息,然后,对第一指纹信息进行验证,若验证失败,则开启摄像头,以采集用户的图像信息,最后,保存第一指纹信息以及图像信息;该方案可以在指纹验证失败时采集并保存当前操作者的指纹信息和图像信息,相对于现有技术而言,提高了终端中信息的安全性。



CN 106407779 A

1.一种信息获取方法，其特征在于，包括：

在终端处于工作状态时，获取用户的第一指纹信息；

对所述第一指纹信息进行验证；

若验证失败，则开启摄像头，以采集所述用户的图像信息；

保存所述第一指纹信息以及所述图像信息。

2.如权利要求1所述的信息获取方法，其特征在于，所述获取用户的第一指纹信息的步骤，具体包括：

获取用户通过指纹键所触发的操作指令；

判断所述操作指令是否满足预设条件；

若满足，通过所述指纹键获取用户的第一指纹信息。

3.如权利要求1所述的信息获取方法，其特征在于，在对所述第一指纹信息验证失败之后，开启摄像头之前，所述方法还包括：

获取当前指纹信息验证失败的累计次数；

判断所述累计次数是否大于预设阈值；

若大于，则执行开启摄像头的步骤。

4.如权利要求1所述的信息获取方法，其特征在于，在保存所述第一指纹信息以及所述图像信息之后，所述方法还包括：

判断在预设时间段内是否获取到第二指纹信息；

若是，则对所述第二指纹信息进行验证；

若验证成功，则删除保存的所述第一指纹信息以及所述图像信息。

5.如权利要求1所述的信息获取方法，其特征在于，所述对所述第一指纹信息进行验证的步骤，具体包括：

判断在样本集合中是否存在与所述第一指纹信息匹配的样本指纹信息；

若存在，则判定对所述第一指纹信息验证成功；

若不存在，则判定对所述第一指纹信息验证失败。

6.一种信息获取装置，其特征在于，包括：

指纹获取模块，用于在终端处于工作状态时，获取用户的第一指纹信息；

验证模块，用于对所述第一指纹信息进行验证；

开启模块，用于在对所述第一指纹信息验证失败时，开启摄像头，以采集所述用户的图像信息；

保存模块，用于保存所述第一指纹信息以及所述图像信息。

7.如权利要求1所述的信息获取装置，其特征在于，所述指纹获取模块，具体用于：

获取用户通过指纹键所触发的操作指令；

判断所述操作指令是否满足预设条件；

若满足，通过所述指纹键获取用户的第一指纹信息。

8.如权利要求1所述的信息获取装置，其特征在于，所述装置还包括：

次数获取模块，用于在对所述第一指纹信息验证失败之后，开启摄像头之前，获取当前指纹信息验证失败的累计次数；

第一判断模块，用于判断所述累计次数是否大于预设阈值；

所述开启模块，具体用于在所述第一判断模块判定为是时，开启摄像头。

9.如权利要求1所述的信息获取装置，其特征在于，所述装置还包括：

第二判断模块，用于在保存所述第一指纹信息以及所述图像信息之后，判断在预设时间段内是否获取到第二指纹信息；

所述验证模块，具体用于在所述第二判断模块判定为是时，对所述第二指纹信息进行验证；

删除模块，用于在对所述第二指纹信息验证成功时，删除保存的所述第一指纹信息以及所述图像信息。

10.如权利要求1所述的信息获取装置，其特征在于，所述验证模块，具体用于：

判断在样本集合中是否存在与所述第一指纹信息匹配的样本指纹信息；

若存在，则判定对所述第一指纹信息验证成功；

若不存在，则判定对所述第一指纹信息验证失败。

11.一种终端，其特征在于，所述终端包括：

摄像头；

触摸显示屏；

一个或多个处理器；

存储器；以及

一个或多个程序，其中所述一个或多个程序被存储于所述存储器中，并配置为由所述一个或多个处理器执行，所述一个或多个程序包括用于实现如权利要求1-5任一项所述的信息获取方法的指令。

一种信息获取方法、装置和终端

技术领域

[0001] 本发明涉及终端技术领域，尤其涉及一种信息获取方法、装置和终端。

背景技术

[0002] 随着互联网的发展和移动通信网络的发展，同时也伴随着终端的处理能力和存储能力的迅猛发展，海量的应用程序得到了迅速传播和使用；常用的应用程序在方便用户工作和生活的同时，不乏新开发的应用程序也进入到用户的日常生活，提高了用户的生活质量、使用终端的频率以及使用中的娱乐感。

[0003] 目前，市面上的终端逐步具有指纹识别功能，利用指纹识别进行设备解锁，能够很好的提高手机的安全性。但是整体安全性还是存在一定安全风险。比如，开启指纹解锁时还保留了原有的手势密码解锁、数字密码解锁等，这样一旦手势密码、数字密码等被非授权用户知道，非授权用户可以轻易绕过指纹解锁，在用户毫无察觉的情况下打开用户终端，侵犯用户隐私。

[0004] 可知，终端中存在信息安全性较差的技术问题。

发明内容

[0005] 本发明实施例提供一种信息获取方法、装置和终端，可以解决终端中存在信息安全性较差的技术问题。

[0006] 本发明实施例提供一种信息获取方法，包括：

[0007] 在终端处于工作状态时，获取用户的第一指纹信息；

[0008] 对所述第一指纹信息进行验证；

[0009] 若验证失败，则开启摄像头，以采集所述用户的图像信息；

[0010] 保存所述第一指纹信息以及所述图像信息。

[0011] 相应地，本发明实施例提供了一种信息获取装置，包括：

[0012] 指纹获取模块，用于在终端处于工作状态时，获取用户的第一指纹信息；

[0013] 验证模块，用于对所述第一指纹信息进行验证；

[0014] 开启模块，用于在对所述第一指纹信息验证失败时，开启摄像头，以采集所述用户的图像信息；

[0015] 保存模块，用于保存所述第一指纹信息以及所述图像信息。

[0016] 相应地，本发明实施例还提供一种终端，所述终端包括摄像头；

[0017] 触摸显示屏；

[0018] 一个或多个处理器；

[0019] 存储器；以及

[0020] 一个或多个程序，其中所述一个或多个程序被存储于所述存储器中，并配置为由所述一个或多个处理器执行，所述一个或多个程序包括用于实现上述信息获取方法的指令。

[0021] 本发明实施例采用在终端处于工作状态时，获取用户的第一指纹信息，然后，对第一指纹信息进行验证，若验证失败，则开启摄像头，以采集用户的图像信息，最后，保存第一指纹信息以及图像信息；该方案可以在指纹验证失败时采集并保存当前操作者的指纹信息和图像信息，相对于现有技术而言，提高了终端中信息的安全性。

附图说明

[0022] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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。

[0023] 图1是本发明实施例一提供的信息获取方法的流程示意图；

[0024] 图2是本发明实施例二提供的信息获取方法的流程示意图；

[0025] 图3是本发明实施例三提供的第一种信息获取装置的结构示意图；

[0026] 图4是本发明实施例三提供的第二种信息获取装置的结构示意图；

[0027] 图5是本发明实施例三提供的第三种信息获取装置的结构示意图；

[0028] 图6是本发明实施例四提供的终端的结构示意图。

具体实施方式

[0029] 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，本领域技术人员在没有作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。

[0030] 本发明实施例提供一种信息获取方法、装置和终端。以下将分别进行详细说明。

[0031] 实施例一、

[0032] 本实施例将从信息获取装置的角度进行描述，该信息获取装置具体可以集成在终端中，该终端可以为智能手机、平板电脑等设备。

[0033] 一种信息获取方法，包括：在终端处于工作状态时，获取用户的第一指纹信息；对第一指纹信息进行验证；若验证失败，则开启摄像头，以采集用户的图像信息；保存第一指纹信息以及图像信息。

[0034] 如图1所示，信息获取方法，具体流程可以如下：

[0035] 101、在终端处于工作状态时，获取用户的第一指纹信息。

[0036] 具体地，工作状态指非锁屏状态，此时，终端已解除屏幕锁定而进入操作界面。可以在该终端内设置指纹识别模组，当检测到有指纹输入操作时，可以触发获取该指纹识别模组识别到的指纹信息。

[0037] 本实施例中，为了监控非授权用户私自使用机主的设备，可以在操作者未察觉的情况下获取其指纹等相关信息。而获取第一指纹信息的方式可以有多种，比如，操作者在使用终端的过程中难免会用到home键执行回归主屏幕、返回上一页、查看后台等操作，有鉴于此，可以在操作者触发这些操作指令的同时采集用户指纹，以避免操作者察觉；也即，步骤“获取用户的第一指纹信息”具体流程可以如下：

[0038] 获取用户通过指纹键所触发的操作指令；

[0039] 判断操作指令是否满足预设条件；

[0040] 若满足，通过该指纹键获取用户的第一指纹信息。

[0041] 具体地，指纹键指具有指纹识别模组(如指纹传感器)的物理键或者虚拟键，比如，该指纹键可以是具有指纹识别模组的主屏键(即home键)，其可以是嵌入显示屏内的虚拟键，也可以为位于显示屏外的物理按键。而预设条件可以根据终端的结构、功能等特性，由本领域技术人员或者设备生产商进行设定。比如，该预设条件可以设为：指示界面跳转或切换；也即，步骤“判断操作指令是否满足预设条件”的步骤，具体可以为：

[0042] 判断该操作指令是否为预设类型的操作指令；

[0043] 若是，则判定该操作指令满足预设条件；

[0044] 若否，则判定该操作指令不满足预设条件。

[0045] 在具体实施过程中，该预设类型的操作指令可以设为通过按压或触控指纹键的方式触发的界面切换指令，如返回主界面、返回上一页等等。无论判定结果如何，终端都可以正常执行用户通过指纹键所触发的操作指令，不受判定结果的影响。

[0046] 102、对第一指纹信息进行验证。

[0047] 具体地，可以通过指纹验证确定操作者是否为非授权用户。其中，验证指纹信息的方式可以有多种，比如，可以将操作者输入的指纹信息与预先设定的指纹信息库做比对；也即，步骤“对第一指纹信息进行验证”具体可以包括：

[0048] 判断在样本集合中是否存在与第一指纹信息匹配的样本指纹信息；

[0049] 若存在，则判定对第一指纹信息验证成功；

[0050] 若不存在，则判定对第一指纹信息验证失败。

[0051] 其中，样本集合中包括有至少一个样本指纹信息。若判定验证成功，则可以确定操作者为已授权用户，若验证失败，则在一定程度上可以确定操作者为非授权用户。

[0052] 在具体实施过程中，为了保证用户体验，同时也为了避免操作者察觉终端的监控操作，无论验证结果如何，终端都可以正常执行上述用户通过指纹键所触发的操作指令，而不受验证结果的影响。

[0053] 103、若验证失败，则开启摄像头，以采集用户的图像信息。

[0054] 具体地，若验证失败，则可以认为是非授权用户私自使用机主的设备，此时可以开启摄像头采集操作者的图像信息，以记录当前操作者信息。其中，摄像头可以优选为前置摄像头，当然，还可以开启后置摄像头。采集到的图像信息具体可以为人体信息，如人脸信息、肢体信息、服装信息等。

[0055] 在具体实施过程中，可能由于外界因素干扰(如水滴)、指纹识别模组不够灵敏等，导致指纹识别模组获取操作者的指纹信息不完整，而造成指纹验证失败，使得终端判断。为了避免这种误判断的情况，可以多次对指纹信息进行验证，若多次验证失败，则可以认为是非授权用户私自使用机主的设备。也即，在对第一指纹信息验证失败之后，开启摄像头之前，该方法还可以包括：

[0056] 获取当前指纹信息验证失败的累计次数；

[0057] 判断累计次数是否大于预设阈值；

[0058] 若大于，则执行开启摄像头的步骤。

[0059] 其中，预设阈值可以基于设备的硬件结构、设备性能等，由本领域技术人员或者设备生产商进行设置，当然，也可以根据终端中软件的安装情况，由用户自行设置。比如，该预设阈值可以设置为2次、3次等。

[0060] 104、保存第一指纹信息以及图像信息。

[0061] 具体地，在对第一指纹信息验证失败之后，将获取到的第一指纹信息和操作者的图像信息保存在终端的存储区内，以供授权用户后期查看。待下次授权用户使用终端时，可以到指定文件夹中，阅读安全报告，查看是否有非授权用户入侵手机，若有异常可以查阅照片和指纹，以确定非授权用户信息。

[0062] 本实施例中，保存第一指纹信息的操作与开启摄像头的操作并无时间先后顺序上的要求。也即，步骤103可以在保存第一指纹信息之后，保存图像信息之前执行，也可以在对第一指纹信息进行验证之后，保存第一指纹信息之前执行。

[0063] 在具体实施时，对第一指纹信息验证失败之后，还可以记录当前操作者的操作记录，如查看了哪些文件，发送、拷贝了哪些文件等，一并保存在安全报告中。

[0064] 在实际应用中，为了避免因外界因素干扰、指纹识别模组不够灵敏等造成终端误判断，导致误获取、误保存指纹信息和图像信息，占据不必要的存储空间，可以将误保存的信息删除；也即，在保存第一指纹信息以及图像信息之后，该方法还可以包括：

[0065] 判断在预设时间段内是否获取到第二指纹信息；

[0066] 若是，则对第二指纹信息进行验证；

[0067] 若验证成功，则删除保存的第一指纹信息以及图像信息。

[0068] 其中，预设时间段可以由本领域技术人员或者生产商进行设定，比如，该预设时间段可以设定为10s、1min等等。

[0069] 具体地，考虑到终端机型普遍为指纹识别与home键复用机型，操作者在使用终端的过程中会不断地用到home键的功能。因此，只要把预设时间段设置的合理，则可以认为在预设时间段内获取到的指纹信息，也即同一操作者通过指纹键(即home键)输入的指纹信息，并再次对指纹信息进行验证。若验证成功，则认为之前的验证失败为终端误判断。此时，可以删除保存的第一指纹信息以及图像信息，以扩大存储空间。

[0070] 由上可知，本发明实施例提供了一种信息获取方法，采用在终端处于工作状态时，获取用户的第一指纹信息，然后，对第一指纹信息进行验证，若验证失败，则开启摄像头，以采集用户的图像信息，最后，保存第一指纹信息以及图像信息；该方案可以在指纹验证失败时采集并保存当前操作者的指纹信息和图像信息，相对于现有技术而言，提高了终端中信息的安全性。

[0071] 实施例二、

[0072] 根据实施例一所描述的方法，以下将举例作进一步详细说明。

[0073] 在本实施例中，将以该信息获取装置具体集成在移动终端中，将指纹键与主屏键(home键)复用，并以物理键的形式集成在移动终端为例进行详细描述。

[0074] 如图2所示，一种信息获取方法，具体流程可以如下：

[0075] 201、移动终端获取用户输入的鉴权信息，其中，该鉴权信息用于解除屏幕锁定。

[0076] 本实施例中，移动终端需要开启屏幕锁，成功解锁才可进入操作界面。该鉴权信息具体可以是手势信息(如图案密码)、生物特征信息(如指纹密码)、文字信息(如数字密码)

等，用于解除屏幕锁定。

[0077] 202、移动终端判断鉴权信息是否与预设鉴权信息相同；若是，执行步骤203，若否，执行步骤205。

[0078] 具体地，移动终端在获取到用户输入的鉴权信息后，可以调用数据库中存储的预设鉴权信息，基于该预设鉴权信息对获取的鉴权信息进行验证，判断是否验证成功。

[0079] 203、移动终端解除屏幕锁定，并通过按压home键获取用户的指纹信息。

[0080] 具体地，在判定鉴权信息与预设鉴权信息相同时，也即对获取的鉴权信息验证成功，此时，可以调用相关程序解除屏幕锁定，以使移动终端进入工作状态。其中，home键为具有指纹识别模组(如指纹传感器)的物理按键。当检测到有指纹输入操作时，可以触发获取该指纹识别模组识别到的指纹信息。

[0081] 本实施例中，为了监控非授权用户私自使用机主的设备，可以在操作者未察觉的情况下获取其指纹等信息。而获取指纹信息的方式可以有多种，比如，操作者在使用移动终端的过程中难免会用到home键执行回归主屏幕、返回上一页、查看后台等操作，有鉴于此，可以在操作者触发这些操作指令的同时采集用户指纹，以避免操作者察觉；也即，步骤“通过按压home键获取用户的指纹信息”具体流程可以如下：

[0082] 获取用户通过home键所触发的操作指令；

[0083] 判断操作指令是否满足预设条件；

[0084] 若满足，则通过该指纹键获取用户的指纹信息。

[0085] 比如，该预设条件可以设为：指示界面跳转或切换；也即，步骤“判断操作指令是否满足预设条件”的步骤，具体可以为：

[0086] 判断该操作指令是否为预设类型的操作指令；

[0087] 若是，则判定该操作指令满足预设条件；

[0088] 若否，则判定该操作指令不满足预设条件。

[0089] 在具体实施过程中，该预设类型的操作指令可以设为界面切换指令，如返回主界面、返回上一页等等。无论判定结果如何，移动终端都可以正常执行用户通过指纹键所触发的操作指令，不受判定结果的影响。

[0090] 204、移动终端判断对指纹信息是否验证成功；若是，执行步骤203；若否，执行步骤205。

[0091] 具体地，可以通过指纹验证确定操作者是否为非授权用户。其中，验证指纹信息的方式可以有多种，比如，可以将操作者输入的指纹信息与预先设定的指纹信息库做比对；也即，步骤“判断对指纹信息是否验证成功”具体可以包括：

[0092] 判断在样本集合中是否存在与指纹信息匹配的样本指纹信息；

[0093] 若存在，则判定对指纹信息验证成功；

[0094] 若不存在，则判定对指纹信息验证失败。

[0095] 其中，样本集合中包括有至少一个样本指纹信息。若判定验证成功，则可以确定操作者为已授权用户，此时可以继续执行步骤203中检测、获取指纹信息的操作；若验证失败，则在一定程度上可以确定操作者为非授权用户。

[0096] 在具体实施过程中，为了保证用户体验，同时也为了避免操作者察觉移动终端的监控操作，无论验证结果如何，移动终端都可以正常执行上述通过home键触发操作指令，而

不受验证结果的影响。

[0097] 205、移动终端开启摄像头，以采集用户的图像信息。

[0098] 具体地，若验证失败，则可以认为是非授权用户私自使用机主的设备，此时可以开启摄像头采集操作者的图像信息，如人脸信息、肢体信息、服装信息等，以记录当前操作者信息。

[0099] 在具体实施过程中，可能由于外界因素干扰(如水滴)、指纹识别模组不够灵敏等，导致指纹识别模组获取操作者的指纹信息不完整，而造成指纹验证失败，使得移动终端判断。为了避免这种误判断的情况，可以多次对指纹信息进行验证，若多次验证失败，则可以认为是非授权用户私自使用机主的设备。也即，在对指纹信息验证失败之后，开启摄像头之前，该方法还可以包括：

[0100] 获取当前指纹信息验证失败的累计次数；

[0101] 判断累计次数是否大于预设阈值；

[0102] 若大于，则执行开启摄像头的步骤。

[0103] 其中，预设阈值可以基于设备的硬件结构、设备性能等，由本领域技术人员或者设备生产商进行设置，当然，也可以根据移动终端中软件的安装情况，由用户自行设置。比如，该预设阈值可以设置为2次、3次等。

[0104] 206、移动终端保存指纹信息以及图像信息。

[0105] 具体地，在获取到指纹信息和图像信息之后，将其保存在移动终端的存储区内，以供授权用户后期查看。待下次授权用户使用移动终端时，可以到指定文件夹中，阅读安全报告，查看是否有非授权用户入侵手机，若有异常可以查阅照片和指纹，以确定非授权用户信息。

[0106] 在具体实施时，对第一指纹信息验证失败之后，还可以记录当前操作者的操作记录，如查看了哪些文件，发送、拷贝了哪些文件等，一并保存在安全报告中。

[0107] 在实际应用中，为了避免因外界因素干扰、指纹识别模组不够灵敏等造成移动终端误判断，导致误获取、误保存指纹信息和图像信息，占据不必要的存储空间，可以将误保存的信息删除；也即，在保存指纹信息以及图像信息之后，该方法还可以包括：

[0108] 判断在预设时间段内是否对通过home键获取的指纹信息验证成功；

[0109] 若验证成功，则删除保存的指纹信息以及图像信息。

[0110] 其中，预设时间段可以由本领域技术人员或者生产商进行设定，比如，该预设时间段可以设定为10s、1min等等。

[0111] 具体地，考虑到移动终端指纹识别与home键复用机型，操作者在使用移动终端的过程中会不断地用到home键的功能。因此，只要把预设时间段设置的合理，则可以认为在预设时间段内获取到的指纹信息，也即同一操作者通过指纹键(即home键)输入的指纹信息，并再次对指纹信息进行验证。若验证成功，则认为之前的验证失败为移动终端误判断。此时，可以删除最近一次保存的指纹信息以及图像信息，以扩大存储空间。

[0112] 由上可知，本发明实施例提供了一种信息获取方法，采用移动终端对用户输入的鉴权信息进行验证，若验证失败，则开启摄像头采集操作者图像信息；若验证成功，则解除屏幕锁定，在通过home键检测到用户的指纹信息时，对指纹信息进行验证，若验证失败，则开启摄像头采集操作者图像信息，并保存指纹信息以及采集到的图像信息；该方案可以在

指纹验证失败时采集并保存当前操作者的指纹信息和图像信息，相对于现有技术而言，提高了终端中信息的安全性。

[0113] 实施例三、

[0114] 为了更好地实施以上方法，本发明实施例还提供一种信息获取装置，该信息获取装置可以集成在终端中，该终端具体可以包括手机、平板电脑、笔记本电脑等设备。如图3所示，该信息获取装置可以包括指纹获取模块301、验证模块302、开启模块303和保存模块304，如下：

[0115] 指纹获取模块301，用于在终端处于工作状态时，获取用户的第一指纹信息；

[0116] 验证模块302，用于对第一指纹信息进行验证；

[0117] 开启模块303，用于在对第一指纹信息验证失败时，开启摄像头，以采集用户的图像信息；

[0118] 保存模块304，用于保存第一指纹信息以及图像信息。

[0119] 在某些实施方式中，该指纹获取模块301，具体可以用于：

[0120] 获取用户通过指纹键所触发的操作指令；

[0121] 判断该操作指令是否满足预设条件；

[0122] 若满足，则通过该指纹键获取用户的第一指纹信息

[0123] 在某些实施方式中，如图4所示，该装置还可以包括：次数获取模块305和第一判断模块306；

[0124] 次数获取模块305，用于在对第一指纹信息验证失败之后，开启摄像头之前，获取当前指纹信息验证失败的累计次数；

[0125] 第一判断模块306，用于判断累计次数是否大于预设阈值；

[0126] 开启模块303，具体用于在第一判断模块306判定为是时，开启摄像头。

[0127] 在某些实施方式中，如图5所示，该装置还可以包括：第二判断模块307和删除模块308；

[0128] 第二判断模块307，用于在保存第一指纹信息以及所述图像信息之后，判断在预设时间段内是否获取到第二指纹信息；

[0129] 该验证模块302，具体用于在第二判断模块307判定为是时，对第二指纹信息进行验证；

[0130] 删除模块308，用于在对第二指纹信息验证成功时，删除保存的第一指纹信息以及图像信息。

[0131] 在某些实施方式中，验证模块302，具体可以用于：

[0132] 判断在样本集合中是否存在与第一指纹信息匹配的样本指纹信息；

[0133] 若存在，则判定对第一指纹信息验证成功；

[0134] 若不存在，则判定对第一指纹信息验证失败。

[0135] 由上可知，本发明实施例提供了一种信息获取装置，采用指纹获取模块301在终端处于工作状态时，获取用户的第一指纹信息，由验证模块302对第一指纹信息进行验证，若验证失败，则由开启模块303开启摄像头，以采集用户的图像信息，由保存模块304保存第一指纹信息以及图像信息；该方案可以在指纹验证失败时采集并保存当前操作者的指纹信息和图像信息，相对于现有技术而言，提高了终端中信息的安全性。

[0136] 实施例四、

[0137] 本实施例提供一种终端，该终端可以包括摄像头；

[0138] 触摸显示屏；

[0139] 一个或多个处理器；

[0140] 存储器；以及

[0141] 一个或多个程序，其中一个或多个程序被存储于所述存储器中，并配置为由一个或多个处理器执行，一个或多个程序包括用于实现如上述任一个信息获取方法的指令。

[0142] 比如，请参考图6，该终端400可以包括射频(RF，Radio Frequency)电路401、包括有一个或一个以上计算机可读存储介质的存储器402、输入单元403、显示单元404、传感器405、音频电路406、无线保真(WiFi，Wireless Fidelity)模块407、包括有一个或者一个以上处理核心的处理器408、电源409、以及摄像头410等部件。本领域技术人员可以理解，图6中示出的终端结构并不构成对终端的限定，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。

[0143] 射频电路401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，交由一个或者一个以上处理器408处理；另外，将涉及上行的数据发送给基站。通常，射频电路401包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM，SubscriberIdentity Module)卡、收发信机、耦合器、低噪声放大器(LNA，LowNoiseAmplifier)、双工器等。此外，射频电路401还可以通过无线通信与网络和其他设备通信。该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(GSM，Global System ofMobile communication)、通用分组无线服务(GPRS，General Packet Radio Service)、码分多址(CDMA，Code Division Multiple Access)、宽带码分多址(WCDMA，Wideband Code Division MultipleAccess)、长期演进(LTE，Long Term Evolution)、电子邮件、短消息服务(SMS，Short Messaging Service)等。

[0144] 存储器402可用于存储软件程序以及模块。处理器408通过运行存储在存储器402的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器402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终端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402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。相应地，存储器402还可以包括存储器控制器，以提供处理器408和输入单元403对存储器402的访问。

[0145] 输入单元403可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地，在一个具体的实施例中，输入单元403可包括触敏表面以及其他输入设备。触敏表面，也称为触摸显示屏或者触控板，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敏表面上或在触敏表面附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触敏表面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408，并能接收处理

器408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敏表面。除了触敏表面，输入单元403还可以包括其他输入设备。具体地，其他输入设备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、指纹识别模组等中的一种或多种。

[0146] 显示单元404可用于显示由用户输入的信息或提供给用户的信息以及终端的各种图形用户接口，这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元404可包括显示面板，可选的，可以采用液晶显示器(LCD，Liquid Crystal Display)、有机发光二极管(OLED，Organic Light-Emitting Diode)等形式来配置显示面板。进一步的，触敏表面可覆盖显示面板，当触敏表面检测到在其上或附近的触摸操作后，传送给处理器408以确定触摸事件的类型，随后处理器408根据触摸事件的类型在显示面板上提供相应的视觉输出。虽然在图6中，触敏表面与显示面板是作为两个独立的部件来实现输入和输入功能，但是在某些实施例中，可以将触敏表面与显示面板集成而实现输入和输出功能。

[0147] 终端还可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的亮度，接近传感器可在终端移动到耳边时，关闭显示面板和/或背光。作为运动传感器的一种，重力加速度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；至于终端还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0148] 音频电路406可通过扬声器、传声器提供用户与终端之间的音频接口。音频电路406可将接收到的音频数据转换成电信号，传输到扬声器，由扬声器转换为声音信号输出；另一方面，传声器将收集的声音信号转换为电信号，由音频电路406接收后转换为音频数据，再将音频数据输出处理器408处理后，经射频电路401以发送给比如另一终端，或者将音频数据输出至存储器402以便进一步处理。音频电路406还可能包括耳塞插孔，以提供外设耳机与终端的通信。

[0149] 无线保真(WiFi)属于短距离无线传输技术，终端通过无线保真模块407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6示出了无线保真模块407，但是可以理解的是，其并不属于终端的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0150] 处理器408是终端的控制中心，利用各种接口和线路连接整个终端的各个部分，通过运行或执行存储在存储器402内的软件程序和/或模块，以及调用存储在存储器402内的数据，执行终端的各种功能和处理数据，从而对终端进行整体监控。可选的，处理器408可包括一个或多个处理核心；优选的，处理器408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408中。

[0151] 终端还包括给各个部件供电的电源409(比如电池)。优选的，电源可以通过电源管理系统与处理器408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。电源409还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0152] 终端还包括具备拍摄功能的摄像头410(比如可以包括前置摄像头、后置摄像头等)。优选的,摄像头可以通过视频处理系统、摄像头驱动等与处理器408逻辑相连,从而通过视频处理系统、摄像头驱动实现拍照、摄像等功能。

[0153] 尽管未示出,终端还可以包蓝牙模块等,在此不再赘述。

[0154] 具体在本实施例中,终端中的处理器408会按照如下的指令,将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器402中,并由处理器408来运行存储在存储器402中的应用程序,从而实现各种功能:

[0155] 在终端处于工作状态时,获取用户的第一指纹信息,然后,对第一指纹信息进行验证,若验证失败,则开启摄像头,以采集用户的图像信息,最后,保存第一指纹信息以及图像信息。

[0156] 由上可知,本发明实施例提供了一种终端,该终端采用在其处于工作状态时,获取用户的第一指纹信息,然后,对第一指纹信息进行验证,若验证失败,则开启摄像头,以采集所述用户的图像信息,最后,保存第一指纹信息以及图像信息;该方案可以在指纹验证失败时采集并保存当前操作者的指纹信息和图像信息,相对于现有技术而言,提高了终端中信息的安全性。

[0157] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质可以包括:只读存储器(ROM,Read Only Memory)、随机存取记忆体(RAM,Random Access Memory)、磁盘或光盘等。

[0158] 以上对本发明实施例所提供的一种信息获取方法、装置和终端进行了详细介绍,本文中应用程序了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的技术人员,依据本发明的思想,在具体实施方式及应用程序范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

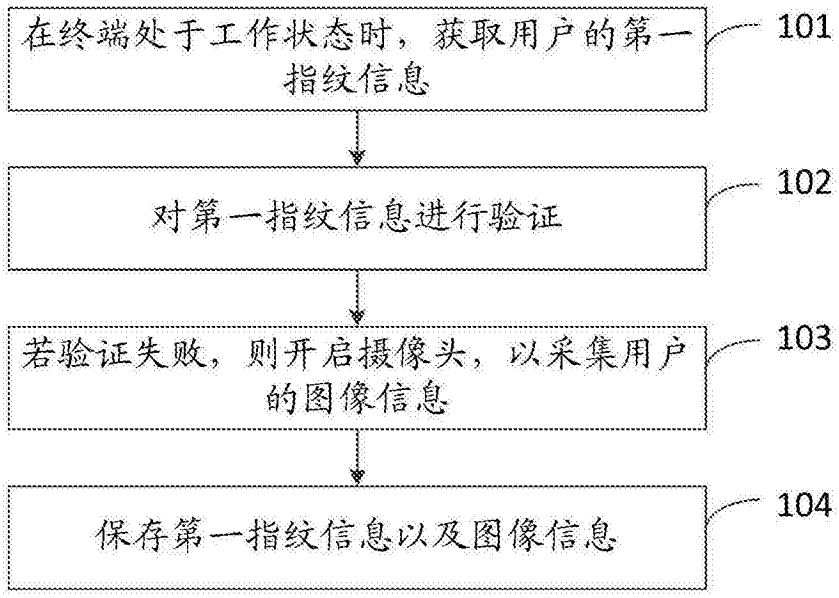

在终端处于工作状态时，获取用户的第一指纹信息
101
对第一指纹信息进行验证
102
若验证失败，则开启摄像头，以采集用户的图像信息
103
保存第一指纹信息以及图像信息
104

图1

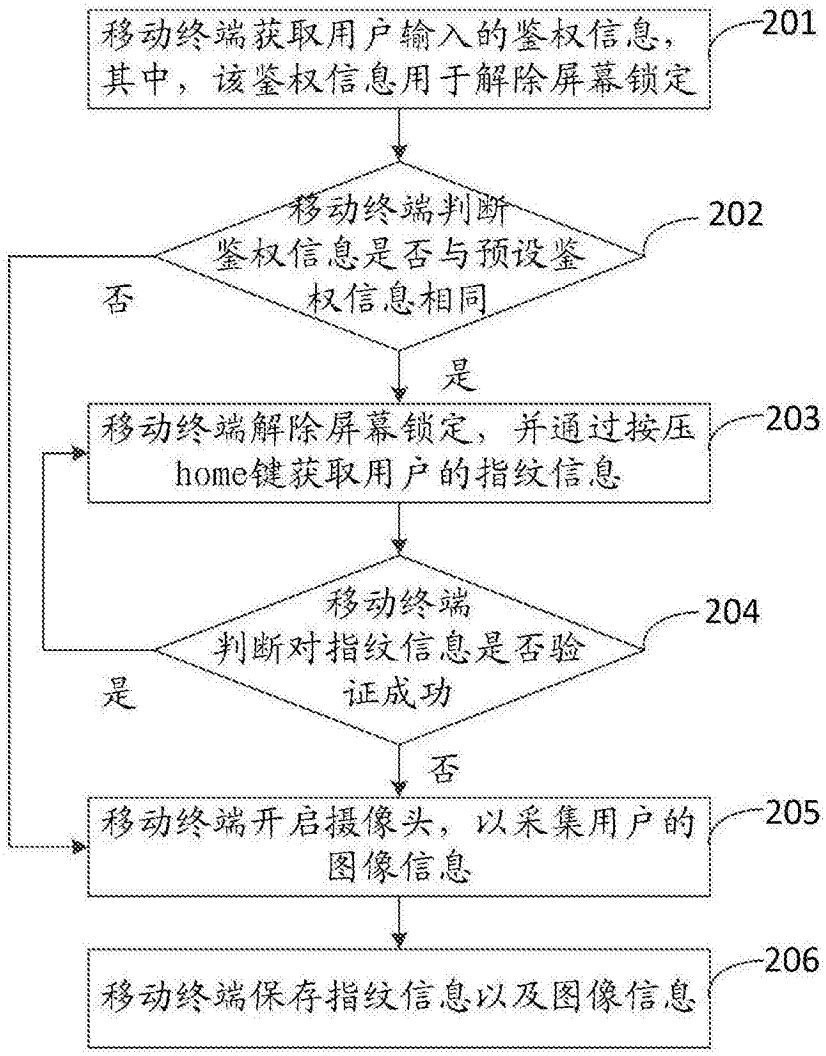

移动终端获取用户输入的鉴权信息，其中，该鉴权信息用于解除屏幕锁定
201
移动终端判断鉴权信息是否与预设鉴权信息相同
202
否
是
移动终端解除屏幕锁定，并通过按压home键获取用户的指纹信息
203
移动终端判断对指纹信息是否验证成功
204
是
否
移动终端开启摄像头，以采集用户的图像信息
205
移动终端保存指纹信息以及图像信息
206

图2

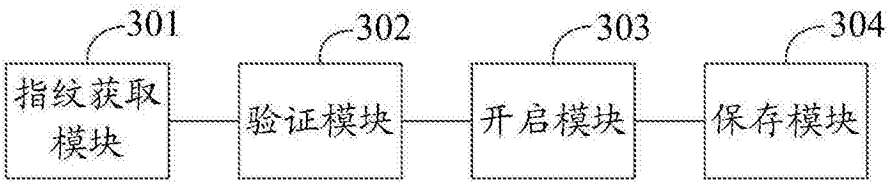

301
指纹获取模块
302
验证模块
303
开启模块
304
保存模块

图3

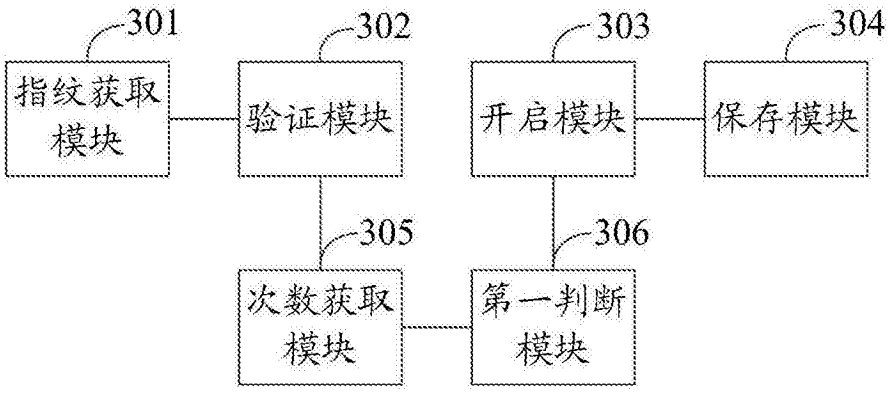

301
指纹获取模块
302
验证模块
303
开启模块
304
保存模块
305
次数获取模块
306
第一判断模块

图4

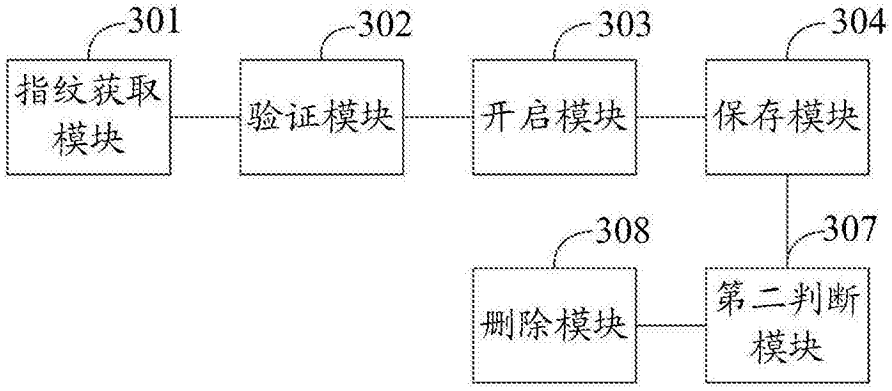

301
指纹获取模块
302
验证模块
303
开启模块
304
保存模块
308
删除模块
307
第二判断模块

图5

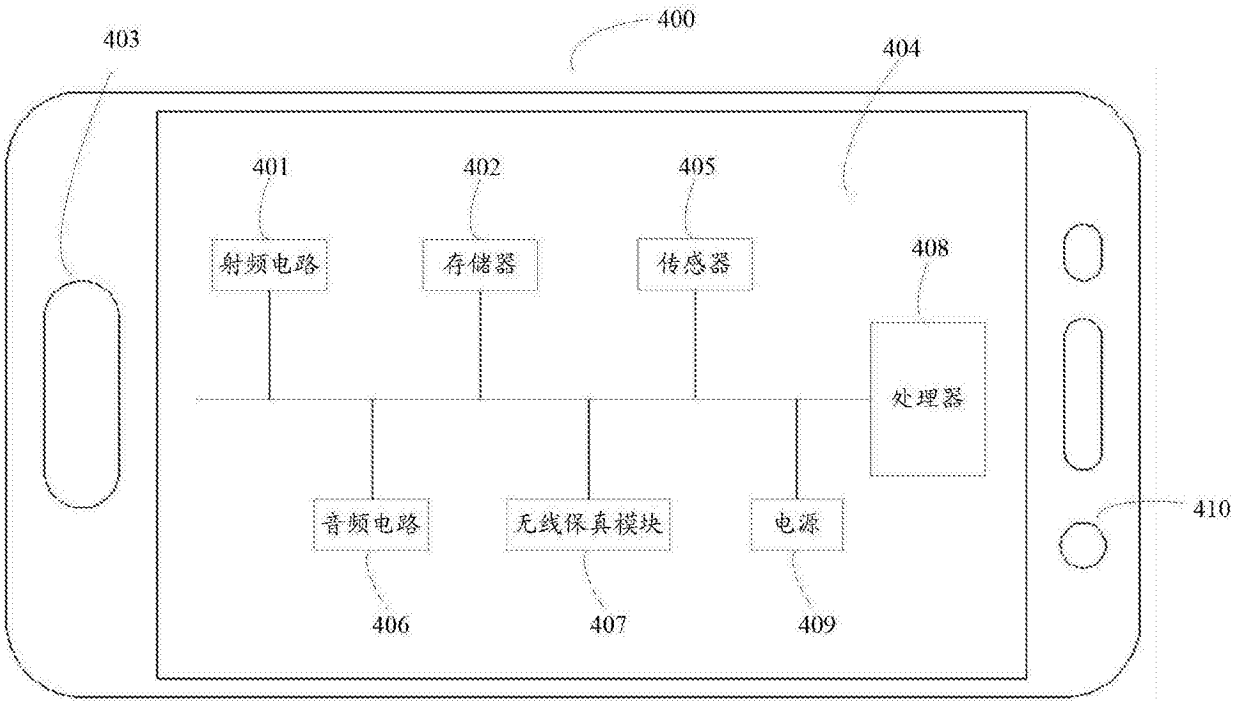

400
403
404
401
402
405
408
射频电路
存储器
传感器
处理器
音频电路
无线保真模块
电源
410
406
407
409

图6