(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 105678226 B
(45)授权公告日 2019.06.11

(21)申请号 201511019709.7

(22)申请日 2015.12.30

(65)同一申请的已公布的文献号
申请公布号 CN 105678226 A

(43)申请公布日 2016.06.15

(73)专利权人 宇龙计算机通信科技(深圳)有限公司
地址 518040 广东省深圳市车公庙天安数码城创新科技广场B座8楼

(72)发明人 刘东海 汪智勇

(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏

(51)Int.Cl.
G06K 9/00(2006.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

(56)对比文件
CN 105138132 A,2015.12.09,
CN 105022570 A,2015.11.04,
WO 2015119326 A1,2015.08.13,
CN 104182275 A,2014.12.03,

审查员 朱俊

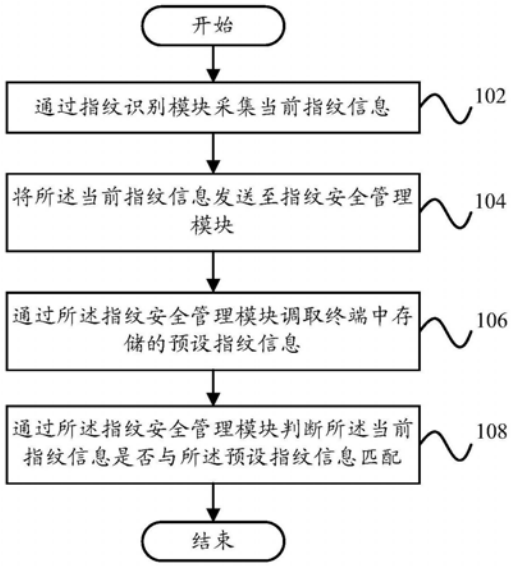
权利要求书1页 说明书9页 附图3页

(54)发明名称

指纹识别的安全管理方法及装置、终端

(57)摘要

本发明提供了一种指纹识别的安全管理方法、一种指纹识别的安全管理装置和一种终端，其中所述指纹识别的安全管理方法包括：通过指纹识别模块采集当前指纹信息；将所述当前指纹信息发送至指纹安全管理模块；通过所述指纹安全管理模块调取终端中存储的预设指纹信息；通过所述指纹安全管理模块判断所述当前指纹信息是否与所述预设指纹信息匹配。通过本发明的技术方案，可以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。



CN 105678226 B

1.一种指纹识别的安全管理方法,其特征在于,包括:

通过指纹识别模块采集当前指纹信息;

将所述当前指纹信息发送至指纹安全管理模块;

通过所述指纹安全管理模块调取终端中存储的预设指纹信息;

通过所述指纹安全管理模块判断所述当前指纹信息是否与所述预设指纹信息匹配;

当通过所述指纹安全管理模块判定所述当前指纹信息与所述预设指纹信息匹配时,

根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序,以访问所述目标应用程序;

检测对所述目标应用程序的访问是否结束;

在检测到访问结束时,锁定所述指纹识别模块采集指纹信息的操作,以清除所述指纹识别模块上的所述当前指纹信息。

2.根据权利要求1所述的指纹识别的安全管理方法,其特征在于,

当检测到对所述指纹识别模块上的所述当前指纹信息的清除操作完成时,解锁所述指纹识别模块采集指纹信息的操作。

3.根据权利要求1或2所述的指纹识别的安全管理方法,其特征在于,

所述指纹识别模块上涂有预设清除涂层,以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

4.一种指纹识别的安全管理装置,其特征在于,包括:

指纹识别模块,用于采集当前指纹信息;

发送模块,用于将所述指纹识别模块采集到的所述当前指纹信息发送至指纹安全管理模块;

所述指纹安全管理模块,用于调取终端中存储的预设指纹信息,并判断所述指纹识别模块采集到的所述当前指纹信息是否与所述预设指纹信息匹配;

获取模块,用于当所述指纹安全管理模块判定所述指纹识别模块采集到的所述当前指纹信息与所述预设指纹信息匹配时,根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序,以访问所述获取模块获取到的所述目标应用程序;

检测模块,用于检测对所述获取模块获取到的所述目标应用程序的访问是否结束;

处理模块,用于在所述检测模块检测到访问结束时,锁定所述指纹识别模块采集指纹信息的操作,以清除所述指纹识别模块上的所述当前指纹信息。

5.根据权利要求4所述的指纹识别的安全管理装置,其特征在于,所述处理模块还用于:

当检测到对所述指纹识别模块上的所述当前指纹信息的清除操作完成时,解锁所述指纹识别模块采集指纹信息的操作。

6.根据权利要求4或5所述的指纹识别的安全管理装置,其特征在于,

所述指纹识别模块上涂有预设清除涂层,以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

7.一种终端,其特征在于,包括如权利要求4至6中任一项所述的指纹识别的安全管理装置。

指纹识别的安全管理方法及装置、终端

技术领域

[0001] 本发明涉及终端技术领域，具体而言，涉及一种指纹识别的安全管理方法、一种指纹识别的安全管理装置和一种终端。

背景技术

[0002] 目前，据科技网站ZDNet报道，指纹可能不像人们想象的那样安全。已有相关内容披露了通过攻击Android(基于Linux(操作系统)的自由及开放源代码的操作系统)设备可以远程大规模获取用户指纹的方法，具体地，主要局限于配置有指纹传感器的Android设备，由于厂商没有完全锁死指纹传感器，即指纹传感器处于可以实时获取指纹的工作状态，从而使黑客可以从受影响的设备中秘密获取用户的指纹图像，而雪上加霜的是，只需“system(系统)”权限而不是“root(根)”权限，即可访问部分设备上的指纹传感器，使黑客更加容易得手，而一旦攻击得手，黑客能继续悄悄获取使用该指纹传感器的任何用户的指纹。

[0003] 综上，现有的指纹识别方案至少存在以下缺陷：一方面，由于厂商没有完全锁死指纹传感器，黑客可以从受影响的设备中秘密获取用户的指纹图像，而且只需要“system”权限而不是“root”权限，即可访问部分设备上的指纹传感器，黑客利用收集的指纹数据进行移动支付和解锁设备等活动，从而威胁用户的账户、设备和数据安全；另外一方面，用户使用指纹传感器后，很容易在指纹传感器上留下指纹，一些不法分子会复制指纹传感器上遗留的指纹信息，从而收集用户的指纹数据。

[0004] 因此，如何有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验成为亟待解决的技术问题。

发明内容

[0005] 本发明正是基于上述技术问题，提出了一种新的技术方案，可以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0006] 有鉴于此，本发明的第一方面，提出了一种指纹识别的安全管理方法，包括：通过指纹识别模块采集当前指纹信息；将所述当前指纹信息发送至指纹安全管理模块；通过所述指纹安全管理模块调取终端中存储的预设指纹信息；通过所述指纹安全管理模块判断所述当前指纹信息是否与所述预设指纹信息匹配。

[0007] 在该技术方案中，通过将指纹识别模块采集到的当前指纹信息发送到在终端中独立设置的指纹安全管理模块中，并通过该指纹安全管理模块调取存储在终端中的预设指纹信息，以在该指纹安全管理模块中进行判断识别采集到的当前指纹信息是否与预设指纹信息匹配，从而确定当前用户是否为终端的合法用户，如此，通过设置一个独立的指纹安全管理模块并由其统一调取访问预设指纹信息，以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0008] 在上述技术方案中，优选地，还包括：当通过所述指纹安全管理模块判定所述当前指纹信息与所述预设指纹信息匹配时，根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序，以访问所述目标应用程序。

[0009] 在该技术方案中，当通过指纹安全管理模块判定指纹识别模块采集到的当前指纹信息与终端中存储的预设指纹信息匹配时，则可以进一步根据预先建立的用户的指纹信息与终端中的应用程序的关联关系获取与采集到的当前指纹信息匹配的预设指纹信息对应的目标应用程序，比如左中指的指纹信息对应打开短信应用，进而可以开启并访问该目标应用程序，以实现对终端中的应用程序的安全访问，提高用户数据、账户的安全性，从而提升用户的使用体验。

[0010] 在上述任一技术方案中，优选地，还包括：检测对所述目标应用程序的访问是否结束；在检测到访问结束时，锁定所述指纹识别模块采集指纹信息的操作，以清除所述指纹识别模块上的所述当前指纹信息。

[0011] 在该技术方案中，当对与指纹识别模块采集到的当前指纹信息对应的目标应用程序访问结束时，则锁定指纹识别模块采集指纹信息的操作，即不再允许指纹识别模块采集、识别新的指纹信息，以在锁定后对指纹识别模块上已经采集到的当前指纹信息进行清除操作，去除在指纹信息采集过程中保留在指纹识别模块上的痕迹，即采集一次、使用一次、清除一次，以避免通过攻击终端设备而非法获取到用户保留在指纹识别模块(比如指纹传感器)上的指纹信息，从而确保用户指纹信息的安全性。

[0012] 在上述任一技术方案中，优选地，当检测到对所述指纹识别模块上的所述当前指纹信息的清除操作完成时，解锁所述指纹识别模块采集指纹信息的操作。

[0013] 在该技术方案中，只有在确保将指纹识别模块上的当前指纹信息清除完毕时才解锁指纹识别模块采集指纹信息的操作，允许指纹识别模块进行新的一次指纹采集、识别以及访问相应的应用程序，进一步可以通过设置的指纹安全管理模块再次匹配当前指纹信息和预设指纹信息的结果确定是否指纹清除操作已经完成，比如，在连续数次匹配失败时可以确定清除完毕，进一步确保用户指纹信息的安全性。

[0014] 在上述任一技术方案中，优选地，所述指纹识别模块上涂有预设清除涂层，以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

[0015] 在该技术方案中，可以在指纹识别模块上涂设可以在预设条件下自动清除痕迹的清除涂层，比如能够在较高温度下恢复原状的涂层材料，以避免保留在指纹识别模块上的指纹信息被非法获取，从而确保用户指纹信息的安全性。

[0016] 在上述任一技术方案中，优选地，当通过所述指纹安全管理模块判定所述当前指纹信息与所述预设指纹信息不匹配时，还包括：提示指纹匹配失败。

[0017] 在该技术方案中，当通过指纹安全管理模块判定采集到的当前指纹信息与终端中存储的预设指纹信息不匹配时，则提示指纹匹配失败，以禁止对终端进行任何操作，确保用户数据、账户和设备的安全性；同时，可以进一步在一定时间内禁止继续获取指纹信息，以进一步确保用户数据、账户和设备的安全性，从而提升用户的使用体验。

[0018] 根据本发明的第二方面，提出了一种指纹识别的安全管理装置，包括：指纹识别模块，用于采集当前指纹信息；发送模块，用于将所述指纹识别模块采集到的所述当前指纹信息发送至指纹安全管理模块；所述指纹安全管理模块，用于调取终端中存储的预设指纹信

息，并判断所述指纹识别模块采集到的所述当前指纹信息是否与所述预设指纹信息匹配。

[0019] 在该技术方案中，将指纹识别模块采集到的当前指纹信息通过发送模块发送到在终端中独立设置的指纹安全管理模块中，并通过该指纹安全管理模块调取存储在终端中的预设指纹信息，以在该指纹安全管理模块中进行判断识别采集到的当前指纹信息是否与预设指纹信息匹配，从而确定当前用户是否为终端的合法用户，如此，通过设置一个独立的指纹安全管理模块并由其统一调取访问预设指纹信息，以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0020] 在上述技术方案中，优选地，还包括：获取模块，用于当所述指纹安全管理模块判定所述指纹识别模块采集到的所述当前指纹信息与所述预设指纹信息匹配时，根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序，以访问所述获取模块获取到的所述目标应用程序。

[0021] 在该技术方案中，当通过指纹安全管理模块判定指纹识别模块采集到的当前指纹信息与终端中存储的预设指纹信息匹配时，则可以进一步通过获取模块根据预先建立的用户的指纹信息与终端中的应用程序的关联关系获取与指纹识别模块采集到的当前指纹信息匹配的预设指纹信息对应的目标应用程序，比如左中指的指纹信息对应打开短信应用，进而可以开启并访问该目标应用程序，以实现对终端中的应用程序的安全访问，提高用户数据、账户的安全性，从而提升用户的使用体验。

[0022] 在上述任一技术方案中，优选地，还包括：检测模块，用于检测对所述获取模块获取到的所述目标应用程序的访问是否结束；处理模块，用于在所述检测模块检测到访问结束时，锁定所述指纹识别模块采集指纹信息的操作，以清除所述指纹识别模块上的所述当前指纹信息。

[0023] 在该技术方案中，当通过检测模块检测到对与指纹识别模块采集到的当前指纹信息对应的目标应用程序访问结束时，则通过处理模块锁定指纹识别模块采集指纹信息的操作，即不再允许指纹识别模块采集、识别新的指纹信息，以在锁定后对指纹识别模块上已经采集到的当前指纹信息进行清除操作，去除在指纹信息采集过程中保留在指纹识别模块上的痕迹，即采集一次、使用一次、清除一次，以避免通过攻击终端设备而非法获取到用户保留在指纹识别模块(比如指纹传感器)上的指纹信息，从而确保用户指纹信息的安全性。

[0024] 在上述任一技术方案中，优选地，所述处理模块还用于：当检测到对所述指纹识别模块上的所述当前指纹信息的清除操作完成时，解锁所述指纹识别模块采集指纹信息的操作。

[0025] 在该技术方案中，只有在确保将指纹识别模块上的当前指纹信息清除完毕时才通过处理模块解锁指纹识别模块采集指纹信息的操作，允许指纹识别模块进行新的一次指纹采集、识别以及访问相应的应用程序，进一步可以通过设置的指纹安全管理模块再次匹配当前指纹信息和预设指纹信息的结果确定是否指纹清除操作已经完成，比如，在连续数次匹配失败时可以确定清除完毕，进一步确保用户指纹信息的安全性。

[0026] 在上述任一技术方案中，优选地，所述指纹识别模块上涂有预设清除涂层，以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

[0027] 在该技术方案中，可以在指纹识别模块上涂设可以在预设条件下自动清除痕迹的清除涂层，比如能够在较高温度下恢复原状的涂层材料，以避免保留在指纹识别模块上的

指纹信息被非法获取，从而确保用户指纹信息的安全性。

[0028] 在上述任一技术方案中，优选地，还包括：提示模块，用于当所述指纹安全管理模块判定所述指纹识别模块采集到的所述当前指纹信息与所述预设指纹信息不匹配时，提示指纹匹配失败。

[0029] 在该技术方案中，当通过指纹安全管理模块判定采集模块采集到的当前指纹信息与终端中存储的预设指纹信息不匹配时，则通过提示模块提示指纹匹配失败，以禁止对终端进行任何操作，确保用户数据、账户和设备的安全性；同时，可以进一步在一定时间内禁止继续获取指纹信息，以进一步确保用户数据、账户和设备的安全性，从而提升用户的使用体验。

[0030] 本发明的第三方面，提出了一种终端，包括上述技术方案中任一项所述的指纹识别的安全管理装置，因此，该终端具有和上述技术方案中任一项所述的指纹识别的安全管理装置相同的技术效果，在此不再赘述。

[0031] 通过以上技术方案，可以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

附图说明

[0032] 图1示出了根据本发明的一个实施例的指纹识别的安全管理方法的流程示意图；

[0033] 图2示出了根据本发明的一个实施例的指纹识别的安全管理装置的框图；

[0034] 图3示出了根据本发明的一个实施例的终端的框图；

[0035] 图4示出了根据本发明的另一个实施例的指纹识别的安全管理装置的框图；

[0036] 图5示出了图4中所示的指纹管理模块在终端中的设置位置示意图；

[0037] 图6示出了图4所示的指纹识别的安全管理装置的工作流程示意图。

具体实施方式

[0038] 为了能够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。

[0039] 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其他方式来实施，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。

[0040] 图1示出了根据本发明的一个实施例的指纹识别的安全管理方法的流程示意图。

[0041] 如图1所示，根据本发明的一个实施例的指纹识别的安全管理方法，包括：步骤102，通过指纹识别模块采集当前指纹信息；步骤104，将所述当前指纹信息发送至指纹安全管理模块；步骤106，通过所述指纹安全管理模块调取终端中存储的预设指纹信息；步骤108，通过所述指纹安全管理模块判断所述当前指纹信息是否与所述预设指纹信息匹配。

[0042] 在该技术方案中，通过将指纹识别模块采集到的当前指纹信息发送到在终端中独立设置的指纹安全管理模块中，并通过该指纹安全管理模块调取存储在终端中的预设指纹信息，以在该指纹安全管理模块中进行判断识别采集到的当前指纹信息是否与预设指纹信息匹配，从而确定当前用户是否为终端的合法用户，如此，通过设置一个独立的指纹安全管

理模块并由其统一调取访问预设指纹信息，以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0043] 在上述技术方案中，优选地，还包括：当通过所述指纹安全管理模块判定所述当前指纹信息与所述预设指纹信息匹配时，根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序，以访问所述目标应用程序。

[0044] 在该技术方案中，当通过指纹安全管理模块判定指纹识别模块采集到的当前指纹信息与终端中存储的预设指纹信息匹配时，则可以进一步根据预先建立的用户的指纹信息与终端中的应用程序的关联关系获取与采集到的当前指纹信息匹配的预设指纹信息对应的目标应用程序，比如左中指的指纹信息对应打开短信应用，进而可以开启并访问该目标应用程序，以实现对终端中的应用程序的安全访问，提高用户数据、账户的安全性，从而提升用户的使用体验。

[0045] 在上述任一技术方案中，优选地，还包括：检测对所述目标应用程序的访问是否结束；在检测到访问结束时，锁定所述指纹识别模块采集指纹信息的操作，以清除所述指纹识别模块上的所述当前指纹信息。

[0046] 在该技术方案中，当对与指纹识别模块采集到的当前指纹信息对应的目标应用程序访问结束时，则锁定指纹识别模块采集指纹信息的操作，即不再允许指纹识别模块采集、识别新的指纹信息，以在锁定后对指纹识别模块上已经采集到的当前指纹信息进行清除操作，去除在指纹信息采集过程中保留在指纹识别模块上的痕迹，即采集一次、使用一次、清除一次，以避免通过攻击终端设备而非法获取到用户保留在指纹识别模块(比如指纹传感器)上的指纹信息，从而确保用户指纹信息的安全性。

[0047] 在上述任一技术方案中，优选地，当检测到对所述指纹识别模块上的所述当前指纹信息的清除操作完成时，解锁所述指纹识别模块采集指纹信息的操作。

[0048] 在该技术方案中，只有在确保将指纹识别模块上的当前指纹信息清除完毕时才解锁指纹识别模块采集指纹信息的操作，允许指纹识别模块进行新的一次指纹采集、识别以及访问相应的应用程序，进一步可以通过设置的指纹安全管理模块再次匹配当前指纹信息和预设指纹信息的结果确定是否指纹清除操作已经完成，比如，在连续数次匹配失败时可以确定清除完毕，进一步确保用户指纹信息的安全性。

[0049] 在上述任一技术方案中，优选地，所述指纹识别模块上涂有预设清除涂层，以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

[0050] 在该技术方案中，可以在指纹识别模块上涂设可以在预设条件下自动清除痕迹的清除涂层，比如能够在较高温度下恢复原状的涂层材料，以避免保留在指纹识别模块上的指纹信息被非法获取，从而确保用户指纹信息的安全性。

[0051] 在上述任一技术方案中，优选地，当通过所述指纹安全管理模块判定所述当前指纹信息与所述预设指纹信息不匹配时，还包括：提示指纹匹配失败。

[0052] 在该技术方案中，当通过指纹安全管理模块判定采集到的当前指纹信息与终端中存储的预设指纹信息不匹配时，则提示指纹匹配失败，以禁止对终端进行任何操作，确保用户数据、账户和设备的安全性；同时，可以进一步在一定时间内禁止继续获取指纹信息，以进一步确保用户数据、账户和设备的安全性，从而提升用户的使用体验。

[0053] 图2示出了根据本发明的一个实施例的指纹识别的安全管理装置的框图。

[0054] 如图2所示，根据本发明的一个实施例的指纹识别的安全管理装置200，包括：指纹识别模块202、发送模块204、指纹安全管理模块206。

[0055] 其中，指纹识别模块202，用于采集当前指纹信息；发送模块204，用于将所述指纹识别模块202采集到的所述当前指纹信息发送至指纹安全管理模块206；所述指纹安全管理模块206，用于调取终端中存储的预设指纹信息，并判断所述指纹识别模块202采集到的所述当前指纹信息是否与所述预设指纹信息匹配。

[0056] 在该技术方案中，将指纹识别模块202采集到的当前指纹信息通过发送模块204发送到在终端中独立设置的指纹安全管理模块206中，并通过该指纹安全管理模块206调取存储在终端中的预设指纹信息，以在该指纹安全管理模块206中进行判断识别采集到的当前指纹信息是否与预设指纹信息匹配，从而确定当前用户是否为终端的合法用户，如此，通过设置一个独立的指纹安全管理模块206并由其统一调取访问预设指纹信息，以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0057] 在上述技术方案中，优选地，还包括：获取模块208，用于当所述指纹安全管理模块206判定所述指纹识别模块202采集到的所述当前指纹信息与所述预设指纹信息匹配时，根据指纹信息与终端应用的关联关系获取与所述预设指纹信息对应的目标应用程序，以访问所述获取模块208获取到的所述目标应用程序。

[0058] 在该技术方案中，当通过指纹安全管理模块206判定指纹识别模块202采集到的当前指纹信息与终端中存储的预设指纹信息匹配时，则可以进一步通过获取模块208根据预先建立的用户的指纹信息与终端中的应用程序的关联关系获取与指纹识别模块202采集到的当前指纹信息匹配的预设指纹信息对应的目标应用程序，比如左中指的指纹信息对应打开短信应用，进而可以开启并访问该目标应用程序，以实现对终端中的应用程序的安全访问，提高用户数据、账户的安全性，从而提升用户的使用体验。

[0059] 在上述任一技术方案中，优选地，还包括：检测模块210，用于检测对所述获取模块208获取到的所述目标应用程序的访问是否结束；处理模块212，用于在所述检测模块210检测到访问结束时，锁定所述指纹识别模块202采集指纹信息的操作，以清除所述指纹识别模块202上的所述当前指纹信息。

[0060] 在该技术方案中，当通过检测模块210检测到对与指纹识别模块202采集到的当前指纹信息对应的目标应用程序访问结束时，则通过处理模块212锁定指纹识别模块202采集指纹信息的操作，即不再允许指纹识别模块202采集、识别新的指纹信息，以在锁定后对指纹识别模块202上已经采集到的当前指纹信息进行清除操作，去除在指纹信息采集过程中保留在指纹识别模块202上的痕迹，即采集一次、使用一次、清除一次，以避免通过攻击终端设备而非法获取到用户保留在指纹识别模块(比如指纹传感器)上的指纹信息，从而确保用户指纹信息的安全性。

[0061] 在上述任一技术方案中，优选地，所述处理模块212还用于：当检测到对所述指纹识别模块202上的所述当前指纹信息的清除操作完成时，解锁所述指纹识别模块202采集指纹信息的操作。

[0062] 在该技术方案中，只有在确保将指纹识别模块202上的当前指纹信息清除完毕时才通过处理模块212解锁指纹识别模块202采集指纹信息的操作，允许指纹识别模块202进

行新的一次指纹采集、识别以及访问相应的应用程序，进一步可以通过设置的指纹安全管理模块206再次匹配当前指纹信息和预设指纹信息的结果确定是否指纹清除操作已经完成，比如，在连续数次匹配失败时可以确定清除完毕，进一步确保用户指纹信息的安全性。

[0063] 在上述任一技术方案中，优选地，所述指纹识别模块202上涂有预设清除涂层，以通过所述预设清除涂层在预设条件下清除所述当前指纹信息。

[0064] 在该技术方案中，可以在指纹识别模块202上涂设可以在预设条件下自动清除痕迹的清除涂层，比如能够在较高温度下恢复原状的涂层材料，以避免保留在指纹识别模块202上的指纹信息被非法获取，从而确保用户指纹信息的安全性。

[0065] 在上述任一技术方案中，优选地，还包括：提示模块，用于当所述指纹安全管理模块206判定所述指纹识别模块202采集到的所述当前指纹信息与所述预设指纹信息不匹配时，提示指纹匹配失败。

[0066] 在该技术方案中，当通过指纹安全管理模块206判定采集模块采集到的当前指纹信息与终端中存储的预设指纹信息不匹配时，则通过提示模块(此模块在图中未示出)提示指纹匹配失败，以禁止对终端进行任何操作，确保用户数据、账户和设备的安全性；同时，可以进一步在一定时间内禁止继续获取指纹信息，以进一步确保用户数据、账户和设备的安全性，从而提升用户的使用体验。

[0067] 图3示出了根据本发明的一个实施例的终端的框图。

[0068] 如图3所示，根据本发明的一个实施例的终端300，包括上述技术方案中任一项所述的指纹识别的安全管理装置200，因此，该终端300具有和上述技术方案中任一项所述的指纹识别的安全管理装置200相同的技术效果，在此不再赘述。

[0069] 下面结合图4至图6对本发明的技术方案进行详细说明。

[0070] 图4示出了根据本发明的另一个实施例的指纹识别的安全管理装置的框图；

[0071] 图5示出了图4中所示的指纹管理模块在终端中的设置位置示意图；

[0072] 图6示出了图4所示的指纹识别的安全管理装置的工作流程示意图。

[0073] 如图4所示，根据本发明的另一个实施例的指纹识别的安全管理装置400，主要由两个模块组成：指纹管理模块(即指纹安全管理模块)402和指纹数据模块404。

[0074] 其中，指纹管理模块402，主要负责管控和调度不同指纹对不同空间里的不同应用的操作，其具体设置位置如图5所示，也就是说，通过设置一个独立的指纹管理模块402，在各个空间调用指纹传感器(指纹识别模块)和TrustZone指纹存储模块获取相应数据时，都通过这个指纹管理模块402来统一调取访问。

[0075] 指纹数据模块404，主要存储多空间选择信息、用户指纹信息和指纹对应的不同空间中的功能操作信息，即预存用户的指纹和对不同空间的不同应用的对应关系。这些信息会维护在指纹数据模块中的数据配置信息列表中，如下表1所示。

[0076] 表1

[0077]

用户	多空间	手指指纹信息	功能操作
用户 A	空间 1	左中指	打开安全域私密短信应用
		……	……
	空间 2	左食指	打开游戏域中某个游戏应用
		……	……
	空间 3	右食指	解锁，进入普通域
		……	……
用户 B	空间 1	右中指	进入安全域
		……	……
	空间 3	左大拇指	代替支付域中支付宝的密码
		……	……
用户 C	空间 2	右大拇指	打开运营商域中的某个运营商应用
		……	……
……			

[0078] 另外，本发明的指纹管理模块在终端中的设置400的工作流程如图6所示，具体包括以下步骤：

[0079] 步骤602，接收指纹传感器传来的指令，通过指纹管理模块管控指纹指令，即采集当前指纹信息并发送至指纹管理模块。

[0080] 步骤604，将指纹传感器的指令与底层存储的指纹(预设指纹信息)进行比对，若指纹有登记，则执行步骤606，若指纹未登记，则执行步骤612。

[0081] 步骤606，根据指纹数据模块中的配置表访问某个空间的相应应用，如安全空间、支付空间、普通空间、运营商空间等不同空间中的某个应用。

[0082] 步骤608，通过应用进程判断应用访问是否完成，若已经完成，则执行步骤610，否则继续访问应用。

[0083] 步骤610，通过加密等技术锁死指纹传感器，并自动清除残留在指纹传感器上的指纹，指纹清除后，即可解开指纹传感器。

[0084] 步骤612，提示“指纹不匹配”。

[0085] 综上，本发明通过设置一个独立的指纹管理模块，在各个空间调用指纹传感器获取相应数据时，都通过这个指纹管理模块来统一调取访问，并且在应用访问完成之后，自动清除残留在指纹传感器上的指纹(可通过在指纹传感器上涂一层特殊材料等实现方式，功能类似于Nissan公司就与油漆公司共同研发了一种叫做Scratch Shield的保护漆，这个就是所谓的“刮痕自动修复烤漆”，汽车喷涂上这种油漆之后，就可以通过一段时间自动修复细小的刮痕，原理是通过改变汽车车漆最外层的保护漆分子结构，让它能够在具备坚硬防

护的功能外，也具备更高的柔韧性、类似塑料的“弹性”，只要保护漆没有受到严重的穿透性破坏(就是说没伤到汽车油漆)，那么这个特殊的保护漆就能够在较高温度的改变下展现出“弹性”，并且自动修补先前所产生的刮伤，而且温度越高，自动修复的速度就越快)，并且锁死指纹传感器，以防非法空间/应用来获取相应数据，或者给非法访问请求传输加密错误指纹数据等。如此，可以有效保护用户的指纹信息，从而保证用户数据、账户和设备的安全。用户使用带有指纹终端的设备时，当应用访问完成后，本提案会锁死指纹传感器，并自动清除残留在指纹传感器上的指纹。

[0086] 以上结合附图详细说明了本发明的技术方案，可以有效地确保用户指纹信息的安全性，避免被非法获取，从而提高用户数据、账户和设备的安全性，提升用户的使用体验。

[0087] 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。

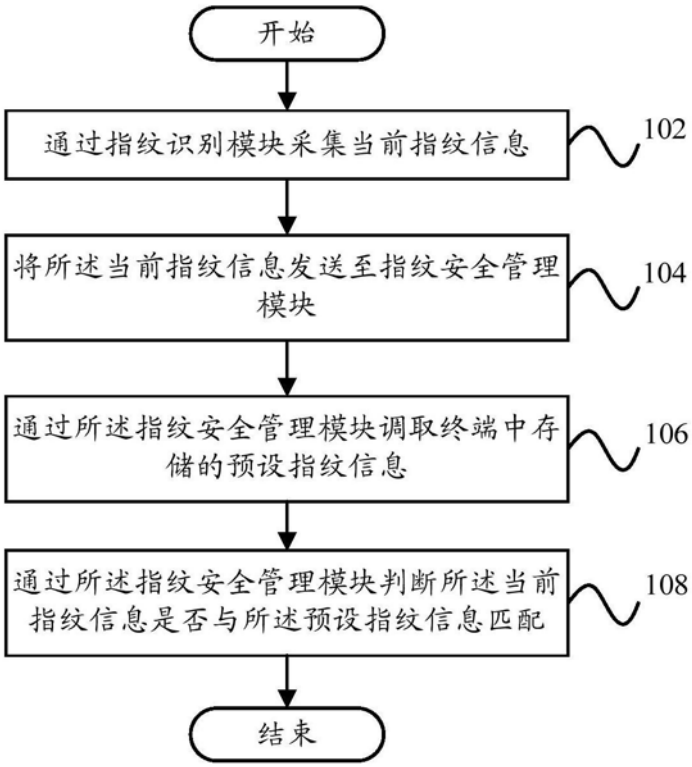

开始
通过指纹识别模块采集当前指纹信息
102
将所述当前指纹信息发送至指纹安全管理模块
104
通过所述指纹安全管理模块调取终端中存储的预设指纹信息
106
通过所述指纹安全管理模块判断所述当前指纹信息是否与所述预设指纹信息匹配
108
结束

图1


指纹识别模块202
获取模块208
发送模块204
检测模块210
指纹安全管理模块206
处理模块212
指纹识别的安全管理装置200

图2


指纹识别的安全管理装置200
终端300

图3

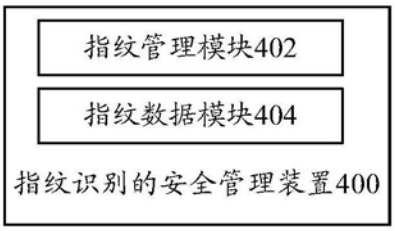

指纹管理模块402
指纹数据模块404
指纹识别的安全管理装置400

图4

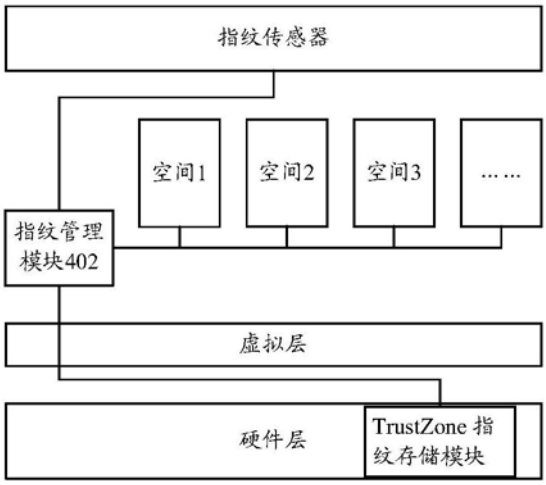

指纹传感器
空间1
空间2
空间3
……
指纹管理模块402
虚拟层
硬件层
TrustZone 指纹存储模块

图5

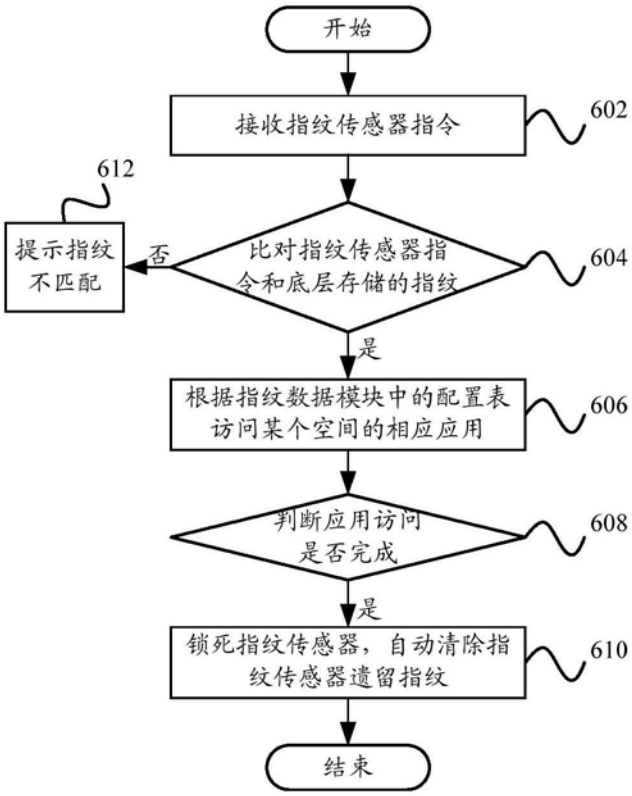

开始
接收指纹传感器指令
602
612
提示指纹不匹配
否
比对指纹传感器指令和底层存储的指纹
604
是
根据指纹数据模块中的配置表访问某个空间的相应应用
606
判断应用访问是否完成
608
是
锁死指纹传感器，自动清除指纹传感器遗留指纹
610
结束

图6