(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 107133552 B
(45)授权公告日 2021.11.16

(21)申请号 201610113246.9
(22)申请日 2016.02.29
(65)同一申请的已公布的文献号
申请公布号 CN 107133552 A
(43)申请公布日 2017.09.05
(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 刘东海 郭德英 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.
G06K 9/00(2006.01)

(56)对比文件
CN 103853965 A,2014.06.11
CN 103778361 A,2014.05.07

审查员 秦涛

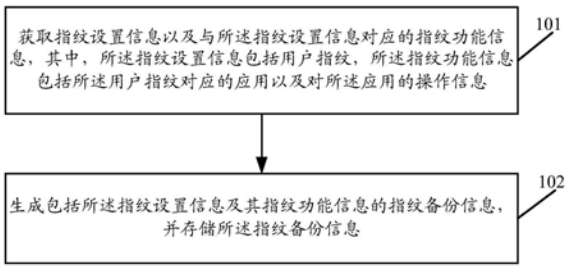
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种指纹信息备份方法及装置

(57)摘要

本发明实施例公开了一种指纹信息备份方法及装置,其中,该方法包括:获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息,其中,所述指纹设置信息包括用户指纹,所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息;生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息,并存储所述指纹备份信息。实施本发明实施例,能够通过对同一指纹下的所有设定信息进行备份来解决因设置的指纹信息被删除或修改而需要重新设置时效率较低的问题。



CN 107133552 B

1.一种指纹信息备份方法,其特征在于,包括:

获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息,其中,所述指纹设置信息包括用户指纹,所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息;

生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息,并存储所述指纹备份信息;

接收基于用户操作触发的指纹信息恢复请求,所述指纹信息恢复请求是在用户设备中的指纹数据被删除或修改后基于用户点击预设的恢复按键触发的;

输出预设的身份验证消息,以提示用户基于所述身份验证消息进行身份验证;

接收用户输入的待验证信息,并判断所述待验证信息是否与预置的身份校验信息相匹配;所述身份校验信息为以下一种或者多种:合法用户的指纹、恢复图案、恢复字符串;

若匹配,则确定对所述用户的身份验证成功,并响应所述指纹信息恢复请求,获取所述指纹备份信息,以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权,以及根据所述指纹备份信息恢复被删除或修改的指纹数据。

2.根据权利要求1所述的方法,其特征在于,所述指纹设置信息还包括所述用户指纹对应的图案或所述用户指纹对应的字符串。

3.根据权利要求1或2所述的方法,其特征在于,所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息,包括:

接收用户输入的指纹设置指令,所述指纹设置指令中携带有指纹设置信息;

响应所述指纹设置指令,获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

4.根据权利要求1或2所述的方法,其特征在于,所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息,包括:

按照预设的时间间隔检测是否存在新的指纹设置信息;

若存在,则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

5.一种指纹信息备份装置,其特征在于,包括:

信息获取模块,用于获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息,其中,所述指纹设置信息包括用户指纹,所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息;

备份模块,用于生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息,并存储所述指纹备份信息;

接收模块,用于接收基于用户操作触发的指纹信息恢复请求,所述指纹信息恢复请求是在用户设备中的指纹数据被删除或修改后基于用户点击预设的恢复按键触发的;

输出模块,用于输出预设的身份验证消息,以提示用户基于所述身份验证消息进行身份验证;

验证模块,用于接收用户输入的待验证信息,判断所述待验证信息是否与预置的身份校验信息相匹配;所述身份校验信息为以下一种或者多种:合法用户的指纹、恢复图案、恢复字符串;并在相匹配时,确定对所述用户的身份验证成功,并触发信息恢复模块响应所述

接收模块接收到的所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权，以及根据所述指纹备份信息恢复被删除或修改的指纹数据。

6.根据权利要求5所述的装置，其特征在于，所述指纹设置信息还包括所述用户指纹对应的图案或所述用户指纹对应的字符串。

7.根据权利要求5或6所述的装置，其特征在于，所述信息获取模块具体用于：

接收用户输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；

响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

8.根据权利要求5或6所述的装置，其特征在于，所述信息获取模块具体用于：

按照预设的时间间隔检测是否存在新的指纹设置信息；

若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

一种指纹信息备份方法及装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种指纹信息备份方法及装置。

背景技术

[0002] 随着终端技术的不断发展，指纹已成为许多手机的标配，用户可方便的进行指纹设置，以通过设置的指纹实现终端的解密，由此方便了用户对终端的使用。此外，在录入指纹时，为了防止因指纹磨损无法识别指纹而导致解密失败，往往会要求用户同步设置解密图案或数字组合作为备用。用户在进行解密时，可输入指纹进行解密，也可输入设置的解密图案或数字组合进行解密。

[0003] 然而，若用户设置的解密图案或数字组合被他人获知，则其他人也可进入指纹设置入口将用户设置的指纹及其图案或数字组合进行删除或重新设置；又或者，设置的指纹可能遇到被用户误删的情况，这就使得用户无法再使用该设置的指纹或解密图案或数字组合进行解密，而需要用户重新设置，操作繁琐，指纹信息重设效率低，给用户带来不便。

发明内容

[0004] 本发明实施例提供了一种指纹信息备份方法及装置，能够通过对同一指纹下的所有设定信息进行备份以使需要时能够及时恢复所有指纹设定，从而解决了设置的指纹数据被删除或修改而需要重新设置时效率较低的问题。

[0005] 本发明实施例公开了一种指纹信息备份方法，包括：

[0006] 获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，其中，所述指纹设置信息包括用户指纹，所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息；

[0007] 生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0008] 可选的，所述指纹设置信息还包括所述用户指纹对应的图案或所述用户指纹对应的字符串；在所述生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息之后，所述方法还包括：

[0009] 接收基于用户操作触发的指纹信息恢复请求；

[0010] 响应所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0011] 可选的，在所述获取所述指纹备份信息之前，所述方法还包括：

[0012] 输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证；

[0013] 接收用户输入的待验证信息，并判断所述待验证信息是否与预置的身份校验信息相匹配；

[0014] 若匹配，则确定对所述用户的身份验证成功，并执行所述获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权的步骤。

[0015] 可选的，所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，包括：

[0016] 接收用户输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；

[0017] 响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0018] 可选的，所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，包括：

[0019] 按照预设的时间间隔检测是否存在新的指纹设置信息；

[0020] 若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

[0021] 相应地，本发明实施例还公开了一种指纹信息备份装置，包括：

[0022] 信息获取模块，用于获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，其中，所述指纹设置信息包括用户指纹，所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息；

[0023] 备份模块，用于生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0024] 可选的，所述指纹设置信息还包括所述用户指纹对应的图案或所述用户指纹对应的字符串；所述装置还包括：

[0025] 接收模块，用于接收基于用户操作触发的指纹信息恢复请求；

[0026] 信息恢复模块，用于响应所述接收模块接收到的所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0027] 可选的，所述装置还包括：

[0028] 输出模块，用于输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证；

[0029] 验证模块，用于接收用户输入的待验证信息，判断所述待验证信息是否与预置的身份校验信息相匹配；并在相匹配时，确定对所述用户的身份验证成功，并通知所述信息恢复模块获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0030] 可选的，所述信息获取模块具体用于：

[0031] 接收用户输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；

[0032] 响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0033] 可选的，所述信息获取模块具体用于：

[0034] 按照预设的时间间隔检测是否存在新的指纹设置信息；

[0035] 若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

[0036] 相应地，本发明实施例还公开了一种用户设备，包括上述的指纹信息备份装置。

[0037] 实施本发明实施例，具有如下有益效果：

[0038] 本发明实施例可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用以及对所述应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时能够及时恢复，且恢复的是指纹下该所有设定信息，由此提升了指纹数据的重设效率。

附图说明

[0039] 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。

[0040] 图1是本发明实施例提供的一种指纹信息备份方法的流程示意图；

[0041] 图2是本发明实施例提供的另一种指纹信息备份方法的流程示意图；

[0042] 图3是本发明实施例提供的一种指纹信息备份装置的结构示意图；

[0043] 图4是本发明实施例提供的另一种指纹信息备份装置的结构示意图；

[0044] 图5是本发明实施例提供的一种用户设备的结构示意图。

具体实施方式

[0045] 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。

[0046] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第三”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0047] 应理解，本发明实施例的技术方案可具体应用于用户设备(User Equipment，简称为“UE”)中，所述用户设备可以包括但不限于智能手机(如Android手机、iOS手机等)、平板电脑、移动互联网设备(Mobile Internet Devices，简称“MID”)、个人数字助理(Personal Digital Assistant，简称“PDA”)等等。在本发明实施例中，用户设备还可称之为终端(Terminal)、移动台(Mobile Station，简称为“MS”)或移动终端(Mobile Terminal)等，本发明实施例不做限定。

[0048] 本发明实施例公开了一种指纹信息备份方法、装置及用户设备，能够通过对同一指纹下的所有设定信息进行备份以使需要时能够及时恢复所有指纹设定，从而解决设置的指纹数据被删除或修改而需要重新设置时效率较低的问题。以下分别详细说明。

[0049] 请参阅图1，图1是本发明实施例提供的一种指纹信息备份方法的流程示意图。具体的，如图1所示，本发明实施例的所述指纹信息备份方法可以包括以下步骤：

[0050] 101、获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，其中，所述指纹设置信息包括用户指纹，所述指纹功能信息包括所述用户指纹对应的应用以及对所

述应用的操作信息。

[0051] 可选的，所述指纹设置信息还可进一步包括该用户指纹对应的图案或该用户指纹对应的字符串等等。

[0052] 具体实施例中，可在检测到用户设置的指纹数据时进行指纹数据备份，如在用户进行指纹设置时立即进行指纹数据备份，或者通过周期性检测指纹设置信息，在检测到新设置的指纹数据时对该指纹数据进行备份，等等，本发明实施例不做限定。

[0053] 具体的，在进行指纹数据备份时，需要获取每一条指纹数据的指纹设置信息及指纹功能信息，包括用户设置的指纹及其对应的应用、对该应用的操作信息等等，即同一指纹下所有的指纹设定信息。

[0054] 102、生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0055] 具体实施例中，在获取得到每一条指纹数据的指纹设置信息及指纹功能信息之后，即可根据该指纹设置信息及指纹功能信息对该指纹数据进行备份，即对该指纹下的所有设定信息进行备份，以便于设置的指纹数据被删除或修改时能够及时地恢复该指纹数据。

[0056] 可选的，该指纹备份信息可存储于用户设备中，或者可存储于云端服务器中，本发明实施例不做限定。

[0057] 进一步的，在所述生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息之后，若接收到用户操作触发的指纹信息恢复请求；还可响应所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。使得能够再次通过该备份信息中的指纹实现对应应用的操作，如对用户设备进行解锁，或打开某一应用，等等。该指纹及其对应应用以及对该应用的操作可预先设置得到，本发明实施例不做限定。

[0058] 在本发明实施例中，可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用以及对所述应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时能够及时恢复，且恢复的是指纹下该所有设定信息，由此提升了指纹数据的重设效率。

[0059] 进一步的，请参阅图2，图2是本发明实施例提供的另一种指纹信息备份方法的流程示意图。具体的，如图2所示，本发明实施例的所述指纹信息备份方法可以包括以下步骤：

[0060] 201、获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0061] 其中，所述指纹设置信息包括用户指纹，还可进一步包括所述用户指纹对应的图案或所述用户指纹对应的字符串(如数字组合)等等。所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息等等，如用户设置的某一指纹对应的应用为安装于用户设备的某一即时应用，其对应的操作为打开该即时应用；又例如，用户设置的另一指纹对应的应用为空，其对应的操作为对用户设备解锁，等等，此处不再赘述。

[0062] 可选的，每一条指纹数据的指纹设置信息及指纹功能信息可存储于预置的数据表中，该数据表中包括用户设置的一条或多条指纹数据，以根据该数据表中的指纹数据对用户设备进行指纹鉴权。例如，该数据表可如下表一所示。

[0063] 表一

[0064]

用户名	指纹命名	鉴权指纹	鉴权图案	鉴权字符串	应用及对应用的操作
用户 A	指纹 1	左手拇指指纹	图案右下角 Z 形状	无	解锁屏幕
用户 A	指纹 2	左手食指指纹	无	9527	打开即时应用 2
用户 B	指纹 3	右手中指指纹	无	1356	打开浏览器 1

[0065] 其中，上述表一中的任一字段(每一列即可表示一个字段，如“用户名”、“指纹命名”可分别表示一个字段)可在进行指纹数据设置时根据用户操作收集得到，如依次提醒用户输入上述字段信息，本发明实施例不做限定。

[0066] 202、生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0067] 可选的，所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，可以具体为：接收用户输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。也就是说，该指纹备份操作可以是在每次检测到用户进行指纹设置(设置完成)时触发进行备份的，即“立即备份”，具体可输出提示消息通知用户手动点击预设的备份按键进行手动备份，或者可设置为自动获取用户设置的指纹数据进行自动备份。

[0068] 可选的，所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，还可以具体为：按照预设的时间间隔检测是否存在新的指纹设置信息；若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。也就是说，该指纹备份操作还可以是按照预设的时间间隔自动同步进行备份的。具体的，可预置一个指纹数据同步功能开关，并设置其对应的检测时间间隔，如每24小时，则可在该指纹数据同步功能开关打开时，每隔24小时检测是否存在新设置的指纹数据，若存在，即可获取该指纹数据的指纹设置信息及指纹功能信息进行备份。

[0069] 203、接收基于用户操作触发的指纹信息恢复请求。

[0070] 具体实施例中，当接收到指纹信息恢复请求，比如在用户设备中的指纹数据被删除或修改时通过点击预设的恢复按键触发的指纹信息恢复请求时，即可根据备份的指纹数据一键恢复所有设定信息，而无需重新手动设置，从而提升了指纹数据重设效率，节省了用户时间。

[0071] 204、响应所述指纹信息恢复请求，输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证。

[0072] 205、接收用户输入的待验证信息，并判断所述待验证信息是否与预置的身份校验信息相匹配。

[0073] 206、确定对所述用户的身份验证成功，并获取所述指纹备份信息，以根据所述指

纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0074] 具体实施例中，在恢复备份的指纹数据即指纹备份信息之前，还可对当前用户进行身份验证，以判断当前用户的身份是否合法。比如可通过预置合法用户的指纹或恢复图案或恢复字符串等等，将该指纹或图案或字符串作为该身份校验信息，使得在接收到用户输入的待验证信息如待验证指纹、待验证图案或待验证字符串时，能够通过两者的匹配比对，并在两者相匹配时确定用户身份合法，即验证成功，则可获取已备份的指纹数据，从而及时地恢复该指纹数据的指纹鉴权功能，即能够根据该指纹备份信息中的指纹设置信息及指纹功能信息进行指纹鉴权，比如对用户设备进行解锁，打开某一即时应用等等。若两者不匹配，则不恢复该指纹数据的指纹鉴权功能，可不做任何处理。

[0075] 在本发明实施例中，可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用及对该应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时，能够根据接收到的指纹信息恢复请求及时地恢复该包括该指纹下所有设定信息的指纹备份信息，从而提升了指纹数据的重设效率，并提高了指纹数据的安全性，增强了用户体验。

[0076] 请参阅图3，图3是本发明实施例提供的一种指纹信息备份装置的结构示意图。具体的，如图3所示，本发明实施例的所述指纹信息备份装置可以包括信息获取模块11以及备份模块12。其中，

[0077] 所述信息获取模块11，用于获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0078] 其中，所述指纹设置信息可包括用户指纹，所述指纹功能信息可包括所述用户指纹对应的应用以及对所述应用的操作信息。可选的，所述指纹设置信息还可进一步包括该用户指纹对应的图案或该用户指纹对应的字符串等等，本发明实施例不做限定。

[0079] 具体的，在进行指纹数据备份时，信息获取模块11需要获取每一条指纹数据的指纹设置信息及指纹功能信息，包括用户设置的指纹及其对应的应用、对该应用的操作信息等等，即信息获取模块11可获取同一指纹下所有的指纹设定信息以进行备份。

[0080] 所述备份模块12，用于生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0081] 具体实施例中，在信息获取模块11获取得到每一条指纹数据的指纹设置信息及指纹功能信息之后，备份模块12即可根据该指纹设置信息及指纹功能信息对该指纹数据进行备份，即对该指纹下的所有设定信息进行备份，以便于设置的指纹数据被删除或修改时能够及时地恢复该指纹数据。

[0082] 可选的，该指纹备份信息可存储于用户设备中，或者可存储于云端服务器中，本发明实施例不做限定。

[0083] 进一步的，所述装置还可包括(图3中未示出)：

[0084] 接收模块13，用于接收基于用户操作触发的指纹信息恢复请求；

[0085] 信息恢复模块14，用于响应所述接收模块13接收到的所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0086] 具体实施例中，在接收模块13接收到指纹信息恢复请求时，信息恢复模块14即可获取存储的指纹备份信息，从而根据该指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权，使得能够再次通过该备份信息中的指纹实现对应应用的操作，如对用户设备进行解锁，或打开某一应用，等等。该指纹及其对应应用以及对该应用的操作可预先设置得到，本发明实施例不做限定。

[0087] 在本发明实施例中，可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用以及对所述应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时能够及时恢复，且恢复的是指纹下该所有设定信息，由此提升了指纹数据的重设效率。

[0088] 进一步的，请参阅图4，图4是本发明实施例提供的另一种指纹信息备份装置的结构示意图。具体的，如图4所示，本发明实施例的所述装置可包括上述图3对应实施例中的指纹信息备份装置的信息获取模块11、备份模块12、接收模块13以及信息恢复模块14，此处不再赘述。进一步的，在本发明实施例中，所述装置还可包括：

[0089] 输出模块15，用于输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证；

[0090] 验证模块16，用于接收用户输入的待验证信息，判断所述待验证信息是否与预置的身份校验信息相匹配；并在相匹配时，确定对所述用户的身份验证成功，并通知所述信息恢复模块14获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0091] 具体实施例中，在信息恢复模块14恢复备份的指纹数据即指纹备份信息之前，还可通过验证模块16对当前用户进行身份验证，以判断当前用户的身份是否合法。比如可预置合法用户的指纹或恢复图案或恢复字符串等等，将该指纹或图案或字符串作为该身份校验信息，使得在验证模块16接收到用户针对输出模块15输出的身份验证消息而输入的待验证信息如待验证指纹、待验证图案或待验证字符串时，能够通过两者的匹配比对，并在两者相匹配时确定用户身份合法，即验证成功。则验证模块16可通知信息恢复模块14获取已备份的指纹数据，从而及时地恢复该指纹数据的指纹鉴权功能，即能够根据该指纹备份信息中的指纹设置信息及指纹功能信息进行指纹鉴权，比如对用户设备进行解锁，打开某一即时应用等等。

[0092] 可选的，在本发明实施例中，所述信息获取模块11可具体用于：

[0093] 接收用户输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；

[0094] 响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0095] 具体的，该指纹备份操作可以是在每次检测到用户进行指纹设置(设置完成)时触发进行备份的，即“立即备份”，信息获取模块11具体可输出提示消息通知用户手动点击预设的备份按键进行手动备份，或者可设置为自动获取用户设置的指纹数据进行自动备份，本发明实施例不做限定。

[0096] 可选的，在本发明实施例中，所述信息获取模块11可具体用于：

[0097] 按照预设的时间间隔检测是否存在新的指纹设置信息；

[0098] 若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

[0099] 具体的，该指纹备份操作还可以是按照预设的时间间隔自动同步进行备份的。具体的，可预置一个指纹数据同步功能开关，并设置其对应的检测时间间隔，如每24小时，则信息获取模块11可在该指纹数据同步功能开关打开时，每隔24小时检测是否存在新设置的指纹数据，若存在，即可获取该指纹数据的指纹设置信息及指纹功能信息进行备份。

[0100] 在本发明实施例中，可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用及对该应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时，能够根据接收到的指纹信息恢复请求及时地恢复该包括该指纹下所有设定信息的指纹备份信息，从而提升了指纹数据的重设效率，增强了用户体验。

[0101] 请参阅图5，图5是本发明实施例提供的一种用户设备的结构示意图。具体的，如图5所示，本发明实施例的所述用户设备可以包括：至少一个处理器100，至少一个输入装置200，至少一个输出装置300，存储器500等组件。其中，这些组件通过一条或多条总线400进行通信连接。本领域技术人员可以理解，图5中示出的用户设备的结构并不构成对本发明实施例的限定，它既可以是总线形结构，也可以是星型结构，还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。其中：

[0102] 处理器100为用户设备的控制中心，利用各种接口和线路连接整个用户设备的各个部分，通过运行或执行存储在存储器500内的程序和/或模块，以及调用存储在存储器500内的数据，以执行用户设备的各种功能和处理数据。处理器100可以由集成电路(Integrated Circuit，简称IC)组成，例如可以由单颗封装的IC所组成，也可以由连接多颗相同功能或不同功能的封装IC而组成。举例来说，处理器100可以仅包括中央处理器(Central Processing Unit，简称CPU)，也可以是CPU、数字信号处理器(digital signal processor，简称DSP)、图形处理器(Graphic Processing Unit，简称GPU)及各种控制芯片的组合。在本发明实施方式中，CPU可以是单运算核心，也可以包括多运算核心。

[0103] 输入装置200可以包括标准的触摸屏、键盘、摄像头等，也可以包括有线接口、无线接口等。

[0104] 输出装置300可以包括显示屏、扬声器等，也可以包括有线接口、无线接口等。

[0105] 存储器500可用于存储软件程序以及模块，处理器100、输入装置200以及输出装置300通过调用存储在存储器500中的软件程序以及模块，从而执行用户设备的各项功能应用以及实现数据处理。存储器500主要包括程序存储区和数据存储区，其中，程序存储区可存储操作系统、至少一个功能所需的应用程序等；数据存储区可存储根据用户设备的使用所创建的数据等。在本发明实施例中，操作系统可以是Android系统、iOS系统或Windows操作系统等等。

[0106] 具体的，所述处理器100调用存储在所述存储器500中的应用程序，用于执行以下步骤：

[0107] 获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，其中，所述指纹设置信息包括用户指纹，所述指纹功能信息包括所述用户指纹对应的应用以及对所述应

用的操作信息；

[0108] 生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息。

[0109] 可选的，所述指纹设置信息还包括所述用户指纹对应的图案或所述用户指纹对应的字符串；所述处理器100调用存储在所述存储器500中的应用程序执行所述生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息之后，还用于执行以下步骤：

[0110] 通过所述输入装置200接收基于用户操作触发的指纹信息恢复请求；

[0111] 响应所述指纹信息恢复请求，获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权。

[0112] 可选的，所述处理器100调用存储在所述存储器500中的应用程序执行所述获取所述指纹备份信息之前，还用于执行以下步骤：

[0113] 通过所述输出装置300输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证；

[0114] 接收用户通过所述输入装置200输入的待验证信息，并判断所述待验证信息是否与预置的身份校验信息相匹配；

[0115] 若匹配，则确定对所述用户的身份验证成功，并执行所述获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权的步骤。

[0116] 可选的，所述处理器100调用存储在所述存储器500中的应用程序执行所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，具体执行以下步骤：

[0117] 接收用户通过所述输入装置200输入的指纹设置指令，所述指纹设置指令中携带有指纹设置信息；

[0118] 响应所述指纹设置指令，获取所述指纹设置信息以及与所述指纹设置信息对应的指纹功能信息。

[0119] 可选的，所述处理器100调用存储在所述存储器500中的应用程序执行所述获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，具体执行以下步骤：

[0120] 按照预设的时间间隔检测是否存在新的指纹设置信息；

[0121] 若存在，则获取所述新的指纹设置信息以及与所述新的指纹设置信息对应的指纹功能信息。

[0122] 在本发明实施例中，可通过获取包括用户指纹的指纹设置信息以及包括所述用户指纹对应的应用以及对所述应用的操作信息的指纹功能信息，并生成包括该指纹设置信息及其指纹功能信息的指纹备份信息进行存储，从而实现了对同一指纹下所有设定信息的备份，使得设置的指纹数据被删除或修改时能够及时恢复，且恢复的是指纹下该所有设定信息，由此提升了指纹数据的重设效率。在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0123] 在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的

相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0124] 所述该作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0125] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0126] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)或处理器(processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0127] 本领域技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0128] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

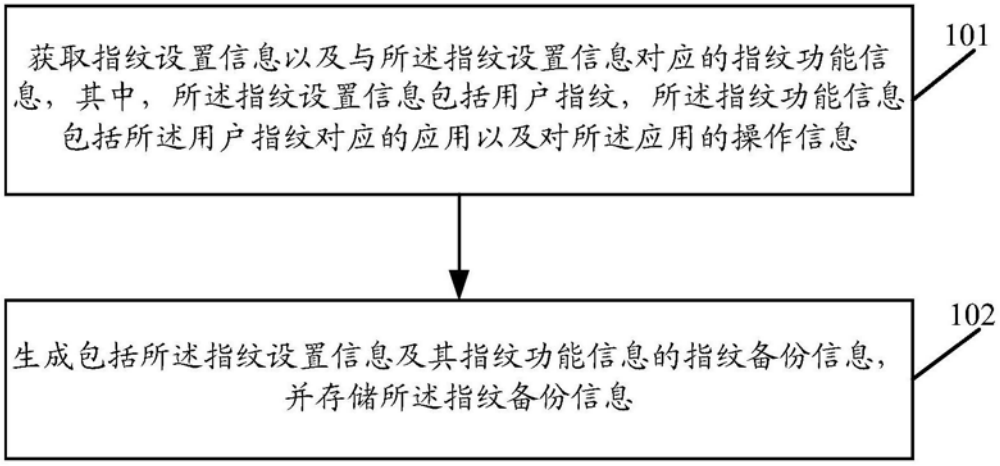

获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息，其中，所述指纹设置信息包括用户指纹，所述指纹功能信息包括所述用户指纹对应的应用以及对所述应用的操作信息
101
生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息
102

图1

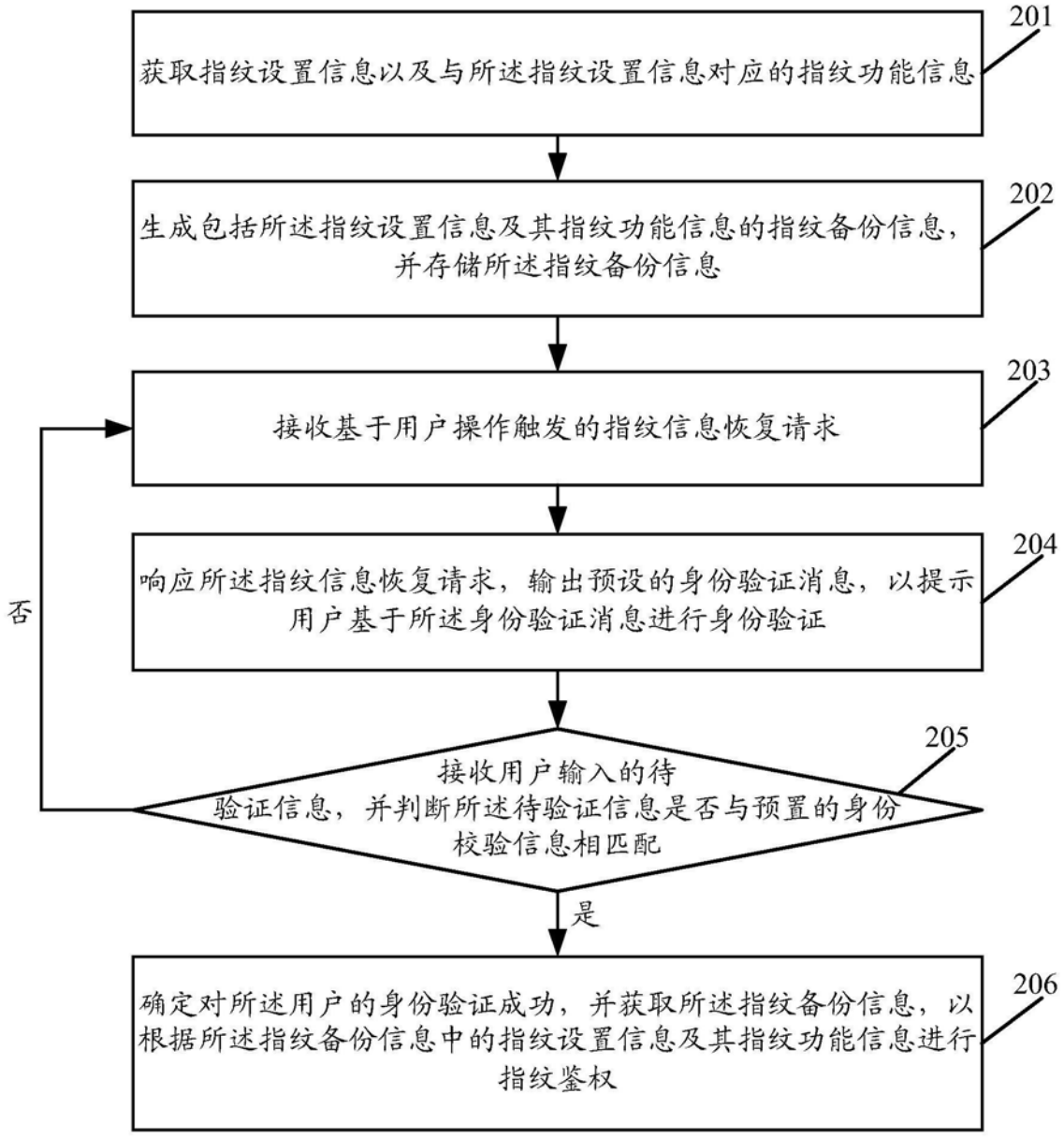

201
获取指纹设置信息以及与所述指纹设置信息对应的指纹功能信息
202
生成包括所述指纹设置信息及其指纹功能信息的指纹备份信息，并存储所述指纹备份信息
203
接收基于用户操作触发的指纹信息恢复请求
204
响应所述指纹信息恢复请求，输出预设的身份验证消息，以提示用户基于所述身份验证消息进行身份验证
205
接收用户输入的待验证信息，并判断所述待验证信息是否与预置的身份校验信息相匹配
否
是
206
确定对所述用户的身份验证成功，并获取所述指纹备份信息，以根据所述指纹备份信息中的指纹设置信息及其指纹功能信息进行指纹鉴权

图2

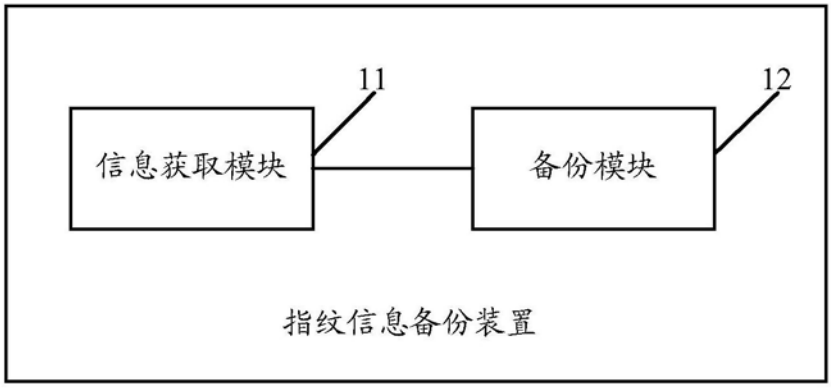

11
12
信息获取模块
备份模块
指纹信息备份装置

图3

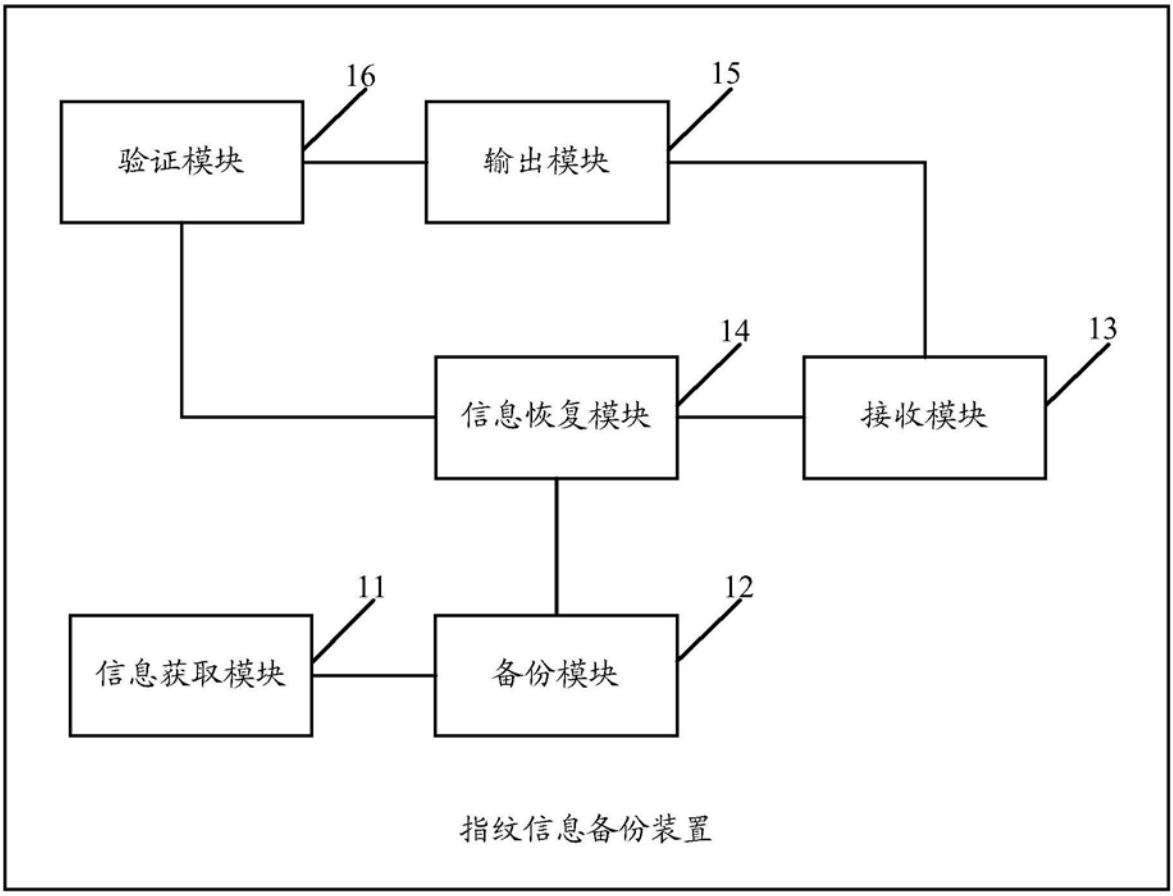

16
15
验证模块
输出模块
14
13
信息恢复模块
接收模块
11
12
信息获取模块
备份模块
指纹信息备份装置

图4

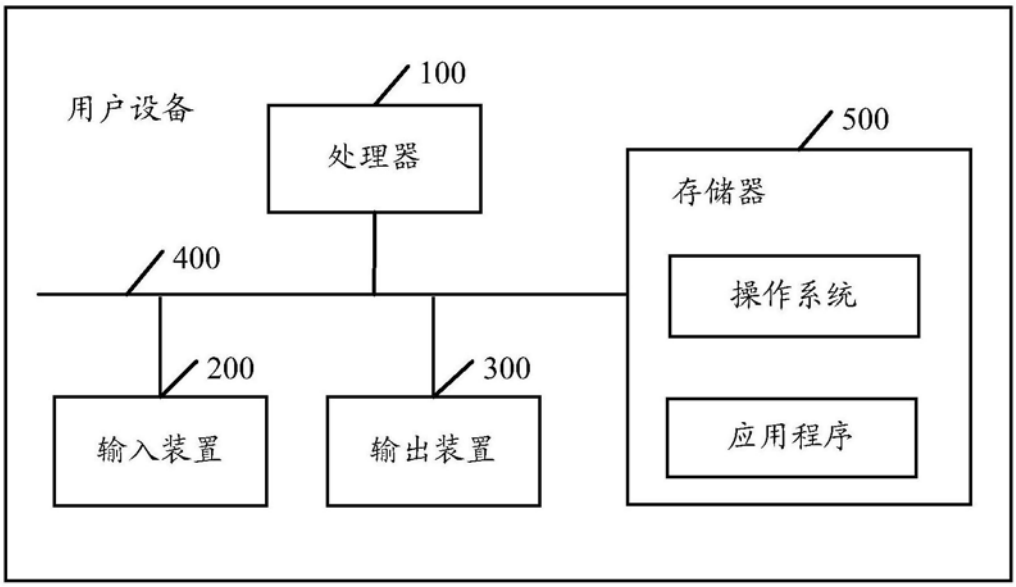


图5