(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 107798224 A
(43)申请公布日 2018.03.13

(21)申请号 201610812287.7

(22)申请日 2016.09.07

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦

(72)发明人 胡楠

(74)专利代理机构 深圳鼎合诚知识产权代理有限公司 44281
代理人 江婷 李发兵

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/44(2013.01)
G06F 21/45(2013.01)
G06F 21/85(2013.01)

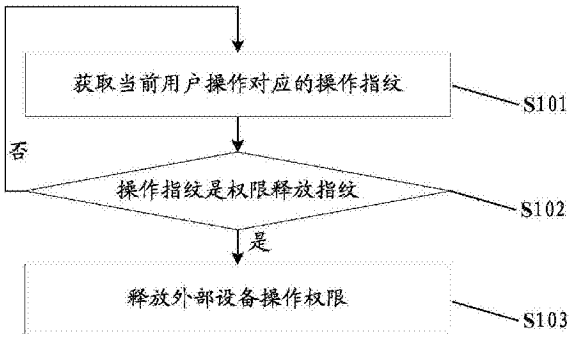
权利要求书2页 说明书6页 附图4页

(54)发明名称

一种终端控制方法及装置、用户终端

(57)摘要

本发明实施例提供了一种终端控制方法及装置、用户终端；该方法包括：获取当前用户操作对应的操作指纹；判断操作指纹是否是权限释放指纹；若是权限释放指纹，则释放外部设备操作权限。本发明通过设置用于开启USB调试等释放外部设备操作权限的权限释放指纹，在后续工作时，只要检测到用户使用权限释放指纹，就将终端从正常模式切换到处于释放外部设备操作权限的状态，供用户通过电脑PC等获取手机里面的用户数据，解决了现有当手机由于显示屏损坏等故障导致用户无法进入到指定页面开启USB调试功能的问题，增强了用户的使用体验。



CN 107798224 A

1.一种终端控制方法,包括:

获取当前用户操作对应的操作指纹;

判断所述操作指纹是否是权限释放指纹;

若是所述权限释放指纹,则释放外部设备操作权限。

2.如权利要求1所述的终端控制方法,其特征在于,在获取当前用户操作对应的操作指纹之前,还包括:

开启所述权限释放指纹的设置界面;

在所述设置界面接收用户进行设置操作时的按压指纹;

加密存储所述按压指纹,作为所述权限释放指纹。

3.如权利要求1所述的终端控制方法,其特征在于,在释放外部设备操作权限之后,还包括:

判断在预设时间内是否接收到来自外部设备的操作指令;

若否,则关闭所述外部设备操作权限。

4.如权利要求1所述的终端控制方法,其特征在于,在释放外部设备操作权限之后,还包括:

判断是否完成来自外部设备的操作指令;

若是,则关闭所述外部设备操作权限。

5.如权利要求1至4任一项所述的终端控制方法,其特征在于,所述释放外部设备操作权限包括:

将预设指定数据备份,将设备端口映射成U盘模式;

或者,

开启设备映射成调试模式。

6.一种终端控制装置,其特征在于,包括:采集模块、控制模块及权限模块,其中,

所述采集模块用于获取当前用户操作对应的操作指纹;

所述控制模块用于判断所述操作指纹是否是权限释放指纹,若是所述权限释放指纹,则控制所述权限模块释放外部设备操作权限;

所述权限模块用于在所述控制模块的控制下工作。

7.如权利要求6所述的终端控制装置,其特征在于,还包括存储模块,所述控制模块用于通过所述采集模块开启所述权限释放指纹的设置界面,在所述设置界面接收用户进行设置操作时的按压指纹,并将所述按压指纹作为所述权限释放指纹加密存储在所述存储模块。

8.如权利要求6所述的终端控制装置,其特征在于,所述权限模块在释放外部设备操作权限之后,还用于判断在预设时间内是否接收到来自外部设备的操作指令;若否,则关闭所述外部设备操作权限,和/或判断是否完成来自外部设备的操作指令;若是,则关闭所述外部设备操作权限。

9.如权利要求6至8任一项所述的终端控制装置,其特征在于,所述权限模块用于将预设指定数据备份,将设备端口映射成U盘模式;或者,开启设备映射成调试模式。

10.一种用户终端,其特征在于,包括:存储器、控制器、采集器及通信接口,其中,

所述采集器用于采用用户进行操作时的操作指纹;

所述存储器用于存储用户数据及权限释放指纹；

所述控制器用于在所述操作指纹为权限释放指纹时，开启外部设备操作权限，使得外部设备可以通过所述通信接口访问所述存储器内的用户数据。

11.如权利要求10所述的用户终端，其特征在于，所述控制器用于通过显示屏开启所述权限释放指纹的设置界面，通过所述采集器在所述设置界面接收用户进行设置操作时的按压指纹，并将所述按压指纹作为所述权限释放指纹加密存储在所述存储器。

12.如权利要求10所述的用户终端，其特征在于，还包括：设置在安全区域的指纹传递应用和设置在非安全区域的指纹识别应用，所述指纹传递应用用于在传递所述权限释放指纹时，使用终端私钥对所述权限释放指纹标识及时间戳进行加密生成加密信息，上传至所述指纹识别应用，所述指纹识别应用用于使用终端公钥对所述加密信息解密，判断所述权限释放指纹标识及时间戳是否均有效，并输出识别结果至所述控制器，供其判断所述操作指纹是否为权限释放指纹，或者将所述权限释放指纹存储到所述存储器。

一种终端控制方法及装置、用户终端

技术领域

[0001] 本发明涉及终端应用领域，尤其涉及一种终端控制方法及装置、用户终端。

背景技术

[0002] 为了便于用户调试手机等用户终端，现有技术提供了开发者调试模式，具体的是电脑PC侧应用通过USB连接手机，下发特定的指令，操控手机，把相应的资料信息提取出来。开发者调试模式必须保证手机USB功能一直处于开发者调试模式，即需要保证：手机USB必须要处于非充电模式，即手机USB可以接收电脑下发的控制指令；手机必须提前使能USB调试功能，例如通过在“设置”->“开发者选项”->“USB调试”内开启。

[0003] 在实际应用中，因为开发者调试模式会给予PC侧USB更大的权限，让其可以操控更多的手机资源，因此若其一直处于开启状态，就好存在较大的安全隐患，因为只要和USB一连接，PC软件就可以获取手机几乎全部的信息资源，毫无安全可言。

[0004] 为了解决上述问题，现有手机的USB调试功能默认是处于关闭状态，当用户需要通过USB接口发送数据到电脑时，手动到指定页面开启。这种方式在一定程度上保证了用户数据的安全，但也存在下面的问题：

[0005] 当手机由于显示屏损坏等故障，导致用户无法进入到指定页面开启USB调试功能，进而导致用户无法通过电脑获取手机里面的用户数据。

发明内容

[0006] 本发明实施例提供了一种终端控制方法及装置、用户终端，以解决现有当手机由于显示屏损坏等故障导致用户无法进入到指定页面开启USB调试功能的问题。

[0007] 一方面，提供了一种终端控制方法，包括：

[0008] 获取当前用户操作对应的操作指纹；

[0009] 判断操作指纹是否是权限释放指纹；

[0010] 若是权限释放指纹，则释放外部设备操作权限。

[0011] 一方面，提供了一种终端控制装置，包括：采集模块、控制模块及权限模块，其中，

[0012] 采集模块用于获取当前用户操作对应的操作指纹；

[0013] 控制模块用于判断操作指纹是否是权限释放指纹，若是权限释放指纹，则控制权限模块释放外部设备操作权限；

[0014] 权限模块用于在控制模块的控制下工作。

[0015] 一方面，提供了一种用户终端，包括：存储器、控制器、采集器及通信接口，其中，

[0016] 采集器用于采用用户进行操作时的操作指纹；

[0017] 存储器用于存储用户数据及权限释放指纹；

[0018] 控制器用于在操作指纹为权限释放指纹时，开启外部设备操作权限，使得外部设备可以通过通信接口访问存储器内的用户数据。

[0019] 另一方面，提供了一种计算机存储介质，计算机存储介质中存储有计算机可执行

指令，计算机可执行指令用于执行前述的终端控制方法。

[0020] 本发明实施例的有益效果：

[0021] 本发明实施例提供了一种终端控制方法，该方法通过设置用于开启USB调试等释放外部设备操作权限的权限释放指纹，在后续工作时，只要检测到用户使用权限释放指纹，就将终端从正常模式切换到处于释放外部设备操作权限的状态，供用户通过电脑PC等获取手机里面的用户数据，解决了现有当手机由于显示屏损坏等故障导致用户无法进入到指定页面开启USB调试功能的问题，增强了用户的使用体验。

附图说明

[0022] 图1为本发明第一实施例提供的终端控制方法的流程图；

[0023] 图2为本发明第二实施例提供的终端控制装置的结构示意图；

[0024] 图3为本发明第三实施例涉及的设置特殊指纹的流程图；

[0025] 图4是本发明第三实施例涉及的判断特征指纹的流程图；

[0026] 图5是本发明第三实施例涉及的手机模式切换方法的流程图。

具体实施方式

[0027] 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，所描述的实施例只是本发明中一部分实施例，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。

[0028] 现通过具体实施方式结合附图的方式对本发明做出进一步的诠释说明。

[0029] 第一实施例：

[0030] 图1为本发明第一实施例提供的终端控制方法的流程图，由图1可知，本实施例提供的终端控制方法包括：

[0031] S101：获取当前用户操作对应的操作指纹；

[0032] 在实际应用中，步骤S101可以是用户终端一直运行的后台程序，如指纹检测程序等，那么，这样本实施例就可以实现：手机等用户终端没有故障时，根据用户预先设置的权限释放指纹，如用户不常用的无名指等特殊指纹，快速切换工作模式的效果；手机等用户终端发生显示故障时，根据用户预先设置的权限释放指纹，如用户不常用的小拇指等特殊指纹，直接切换工作模式的效果。

[0033] 在实际应用中，步骤S101可以是用户终端检测到设备故障，如显示屏故障，数据连接线坏断等时，开启指纹检测功能，那么，这样本实施例就可以实现：手机等用户终端发生显示故障时，根据用户预先设置的权限释放指纹，如用户不常用的小拇指等特殊指纹，直接切换工作模式的效果。

[0034] 在实际应用中，获取当前用户操作对应的操作指纹的步骤可以由手机上的指纹采集器来采集，如屏幕正前方的主按钮，设置在手机背部的指纹采集单元，或者具备压力感应功能的显示屏等采集设备来采集用户指纹。

[0035] S102：判断操作指纹是否是权限释放指纹；

[0036] 在实际应用中，用户可以根据需要设置一个或者多个权限释放指纹，具体的，可以

参照如图3所示的方法，设置步骤简单的包括：

[0037] 开启权限释放指纹的设置界面；

[0038] 在设置界面接收用户进行设置操作时的按压指纹；

[0039] 加密存储按压指纹，作为权限释放指纹。

[0040] S103：若是权限释放指纹，则释放外部设备操作权限；若否，则返回S101继续获取当前用户操作对应的操作指纹。

[0041] 在实际应用中，释放外部设备操作权限可以通过将预设指定数据备份，将设备端口映射成U盘模式；或者，开启设备映射成调试模式等，可以实现开启手机USB调试模式等方式实现。

[0042] 在实际应用中，为了避免手机等终端一直处于开启手机USB调试模式等释放外部设备操作权限的状态，在释放外部设备操作权限之后，还包括：

[0043] 判断在预设时间内是否接收到来自外部设备的操作指令；若否，则关闭外部设备操作权限；若是，则执行接收到的来自外部设备的操作指令；

[0044] 或者，

[0045] 判断是否完成来自外部设备的操作指令；若是，则关闭外部设备操作权限，若否，则继续执行接收到的来自外部设备的操作指令。

[0046] 第二实施例：

[0047] 图2为本发明第二实施例提供的终端控制装置的结构示意图，由图2可知，本实施例提供的终端控制装置包括：采集模块21、控制模块22及权限模块23，其中，

[0048] 采集模块21用于获取当前用户操作对应的操作指纹；

[0049] 控制模块22用于判断操作指纹是否是权限释放指纹，若是权限释放指纹，则控制权限模块释放外部设备操作权限；

[0050] 权限模块23用于在控制模块的控制下工作。

[0051] 在一些实施例中，上述实施例中的终端控制装置还包括存储模块，控制模块22用于通过采集模块开启权限释放指纹的设置界面，在设置界面接收用户进行设置操作时的按压指纹，并将按压指纹作为权限释放指纹加密存储在存储模块。

[0052] 在一些实施例中，上述实施例中的权限模块23在释放外部设备操作权限之后，还用于判断在预设时间内是否接收到来自外部设备的操作指令；若否，则关闭外部设备操作权限，和/或判断是否完成来自外部设备的操作指令；若是，则关闭外部设备操作权限。

[0053] 在一些实施例中，上述实施例中的权限模块23用于将预设指定数据备份，将设备端口映射成U盘模式；或者，开启设备映射成调试模式。

[0054] 在实际应用中，图2所示实施例中的所有功能模块，都可以采用处理器、编辑逻辑器件等方式实现。

[0055] 对应的，本发明在一些实施例中，也提供了一种用户终端，包括：存储器、控制器、采集器及通信接口，其中，

[0056] 采集器用于采用用户进行操作时的操作指纹；

[0057] 存储器用于存储用户数据及权限释放指纹；

[0058] 控制器用于在操作指纹为权限释放指纹时，开启外部设备操作权限，使得外部设备可以通过通信接口访问存储器内的用户数据。

[0059] 在一些实施例中，上述实施例中的控制器用于通过显示屏开启权限释放指纹的设置界面，通过采集器在设置界面接收用户进行设置操作时的按压指纹，并将按压指纹作为权限释放指纹加密存储在存储器。

[0060] 在一些实施例中，上述实施例中的用户终端，还包括设置在安全区域的指纹传递应用和设置在非安全区域的指纹识别应用，指纹传递应用用于在传递权限释放指纹时，使用终端私钥对权限释放指纹标识及时间戳进行加密生成加密信息，上传至指纹识别应用，指纹识别应用用于使用终端公钥对加密信息解密，判断权限释放指纹标识及时间戳是否均有效，并输出识别结果至控制器，供其判断操作指纹是否为权限释放指纹，或者将权限释放指纹存储到存储器。

[0061] 第三实施例：

[0062] 现结合具体应用场景对本发明做进一步的诠释说明。

[0063] 本实施例利用指纹识别的安全便捷性，让PC软件在安全环境下操控手机资源，完成备份、删除等操作。本发明不增加硬件成本的基础，可以在保证用户在足够安全的环境下通过PC操控手机，具有安全、便捷的特点；就是让指纹识别成为手机USB模式切换的一种触发条件，保证PC要想通过USB获取手机资料和控制权限时必须是在用户许可的情况下。本实施例通过将不常用的手指录入为特殊指纹模板，当此指纹被识别后，手机自动切换到USB可控模式，可以通过PC软件把数据拷贝到电脑侧，以及删除手机里个人信息(恢复出厂设置)等操作。

[0064] 本实施例主要分为指纹录入/识别、手机模式转换两个步骤。工作原理如下：

[0065] 第一步指纹录入/识别：将特殊手指的指纹录入到手机里面，一般选择不常用的手指。该指纹可以不参与屏幕解锁、支付等常规操作，专门用于后续手机模式切换。当指纹识别出是这根特殊的手指，手机进入模式切换。为了保证手机信息不被泄漏，所以此步骤必须采用特殊加密方式。

[0066] 第二步手机模式切换：当检测到特殊指纹，手机会自动切换到USB通讯模式。这种模式可以有很多方式来实现，比如a、手机将自身重要信息资源备份(包括通信录、照片、常用软件等)，将USB端口映射成U盘模式，方便用户拷贝；b、手机将USB映射成调试模式，给PC侧软件更多的资源控制权限，让PC侧软件从手机内存中读取/删除相应的数据，并可以对手机进行各种其他操作(比如发短信、打电话，共享数据流量等)。手机重启、等待超时或断开USB后恢复到正常模式，关闭USB相关功能，保护用户信息安全。

[0067] 由于每个人的手指指纹具有唯一性，一部手机只有用户的一个指纹有此权限，这样特殊指纹的录入和识别就保证了用户信息的安全性；由于指纹只用按一次就可以实现手机模式的切换，保证USB端口和PC侧通讯的正常，具有良好的便捷性。当用户需要PC侧连接手机时，只用轻轻进行一次指纹识别，USB自动完成切换，相关的资源信息也已经备份或者可以被PC访问；其他时间，手机处于PC无法连接状态，防止非法侵入到用户手机。这样就保证了操作的便捷性以及用户信息的安全性。

[0068] 在实际应用中，特殊指纹的录入和识别，如果被破解就可能导致手机信息的泄漏，所以对应操作必须加入特定的加密操作。所以其同普通的指纹处理方式是不一样的。此指纹的识别并不是为了屏幕解锁、支付等常规操作，而是为了将手机切到USB通讯模式，让PC软件能够获取手机里的数据资源以及其操作权。选取指纹最好是不常用手指的，比如小拇

指，这样可以防止误触发。

[0069] 在手机生产过程中，要产生一对密匙(私匙和公匙，其中私匙用于加密，公匙用于解密)。将私匙存放到手机Trustzone区域(安全区域，普通应用无法访问，恢复出厂设置也无法擦除。例如高通平台的RPMB，the Replay Protected Memory Block)；将公匙存放到指纹解锁应用中。Trustzone区域到设置在Non-Trustzone非安全区域的应用之间传输指纹数据，可能存在数据泄漏或者伪造数据，所以必须进行加密传输。

[0070] 如图3所示，指纹录制分为两块：在Trustzone区域进行指纹录制、模板保存以及指纹id的生成和传输；在Non-Trustzone区域进行指纹id的获取和保存。一般讲Trustzone区域进行的所有操作都是安全可靠的。但特殊指纹id如果在Non-Trustzone区域传输时泄漏，可能会被他人仿冒，导致手机将操作权误开放给PC侧，引起信息和资源的泄漏。所以要在步骤205中对指纹和时间戳用私匙进行加密，在步骤206、207、208中对加密后的信息用公匙进行解密，并进行判断处理。这里之所以要加入时间戳，是为了防止他人用旧的指纹id加密信息仿冒新的指纹id信息。如果应用判断时间戳超过一定范围，就认为是仿冒数据，加以丢弃。

[0071] 如图4所示，指纹识别与指纹录入是一致的。在Trustzone区域传输指纹id的时候，对id和时间戳进行加密；在应用测对加密信息进行解密，判断指纹id和时间戳进行判断，根据判断条件进行处理。

[0072] 在实际应用中，如果要删除特殊指纹，由于不涉及信息的泄漏风险，可以同普通指纹删除一致。

[0073] 这样操作可以保证用户信息和资料的安全，而且操作便捷。在代码中略加修改就可以实现。

[0074] 如图5所示，本实施例提供的手机模式切换方法包括：

[0075] S501：在设备故障时，识别到特殊指纹。

[0076] 本步骤可以由图4所示的方法来实现特殊指纹的识别。

[0077] S502：终端切换到USB调试模式。

[0078] S503-S507：手机进行用户数据的处理。

[0079] 本实施例是在指纹识别后手机自身进行的模式切换，包括数据备份、USB接口的转换以及配合PC侧指令进行相应操作。主要实现目的就是让PC软件能够通过USB从手机提取相关的数据，并对手机进行一定的操作。这种具体实现方式可以有很多种，比如a、手机将自身重要信息资源备份(包括通信录、照片、常用软件等)，将USB端口映射成U盘模式，方便用户拷贝；b、手机将USB映射成调试模式，给PC侧软件更多的资源控制权限，让PC侧软件从手机内存中读取相应的数据，运行PC对手机进行各种其他操作(比如发短信、打电话、删除数据和恢复出厂设置等)。手机重启、等待超时或拔出USB后恢复到正常模式，关闭USB相关功能，保护用户信息安全。图5具体的给出了b方案的实现方式。

[0080] 本实施例通过指纹识别来触发手机USB不同的工作模式，从而保证要想让PC通过USB获取手机的控制权，必须是在用户允许的范围内进行的。通过这种方式，既保证了用户操作的安全性，也不需要用户设置繁琐的USB权限。即使屏幕损坏，我们依旧可以把手机当成数据卡来用，而且不用担心数据的泄漏，具有安全、便捷的特性。

[0081] 综上可知，通过本发明实施例的实施，至少存在以下有益效果：

[0082] 本发明实施例提供了一种终端控制方法，该方法通过设置用于开启USB调试等释放外部设备操作权限的权限释放指纹，在后续工作时，只要检测到用户使用权限释放指纹，就将终端从正常模式切换到处于释放外部设备操作权限的状态，供用户通过电脑PC等获取手机里面的用户数据，解决了现有当手机由于显示屏损坏等故障导致用户无法进入到指定页面开启USB调试功能的问题，增强了用户的使用体验。

[0083] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0084] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0085] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0086] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0087] 以上仅是本发明的具体实施方式而已，并非对本发明做任何形式上的限制，凡是依据本发明的技术实质对以上实施方式所做的任意简单修改、等同变化、结合或修饰，均仍属于本发明技术方案的保护范围。

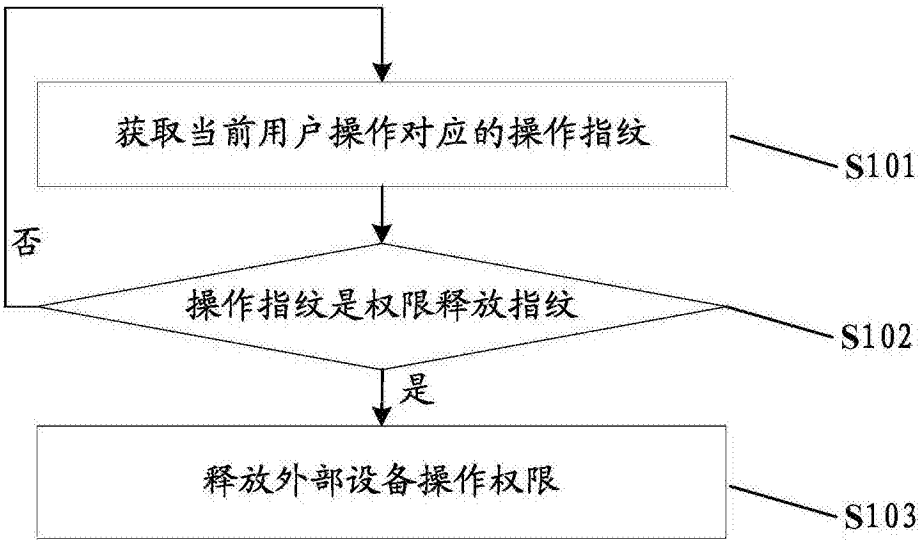

获取当前用户操作对应的操作指纹
S101
否
操作指纹是权限释放指纹
S102
是
释放外部设备操作权限
S103

图1

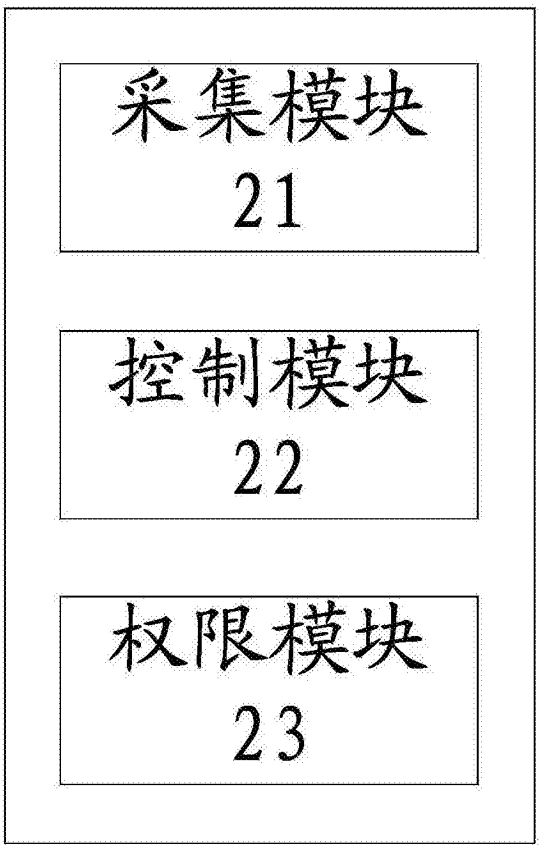

采集模块
21
控制模块
22
权限模块
23

图2

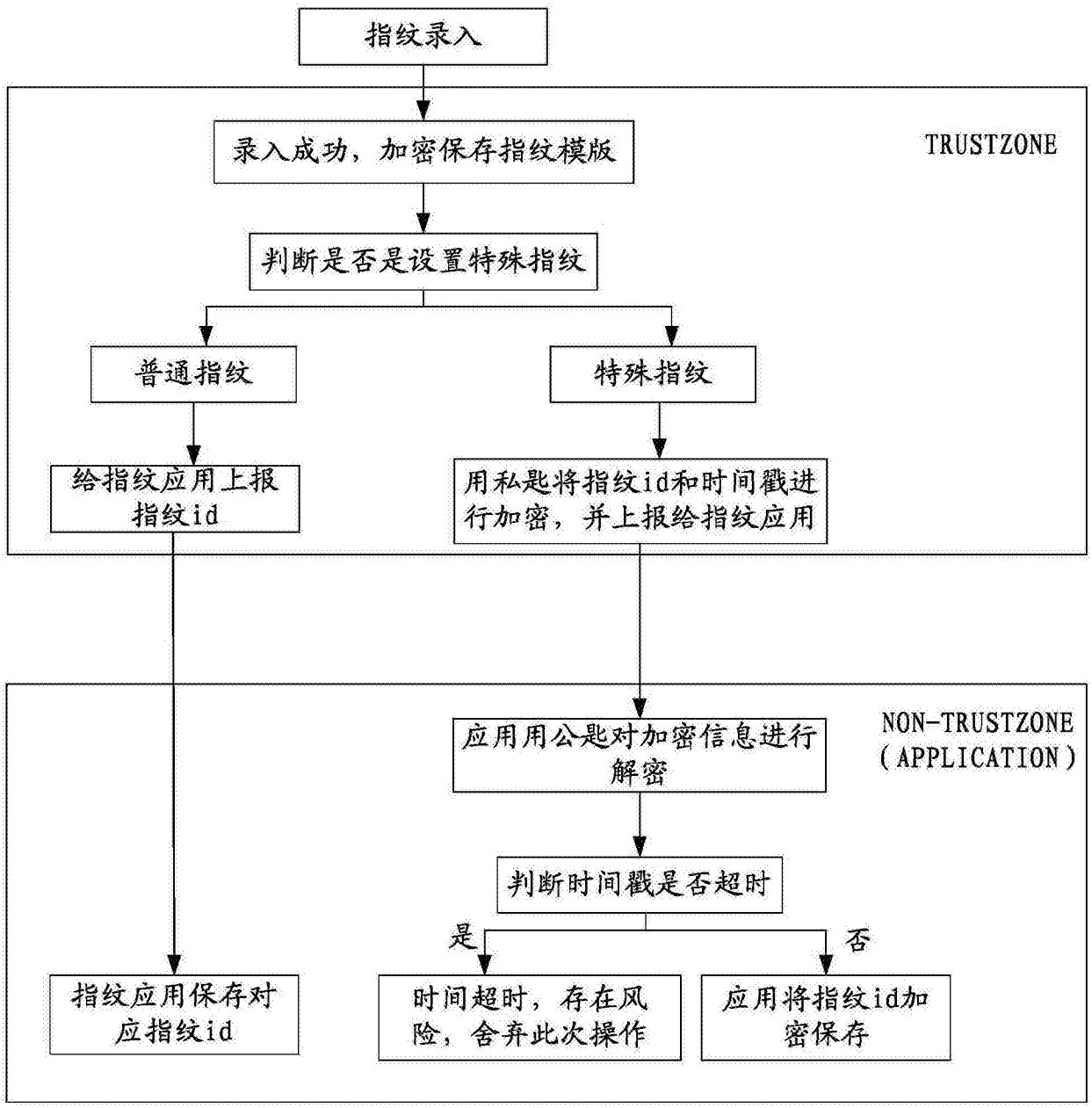

指纹录入
TRUSTZONE
录入成功，加密保存指纹模版
判断是否是设置特殊指纹
普通指纹
特殊指纹
给指纹应用上报指纹id
用私匙将指纹id和时间戳进行加密，并上报给指纹应用
NON-TRUSTZONE
(APPLICATION)
应用用公匙对加密信息进行解密
判断时间戳是否超时
是
否
指纹应用保存对应指纹id
时间超时，存在风险，舍弃此次操作
应用将指纹id加密保存

图3

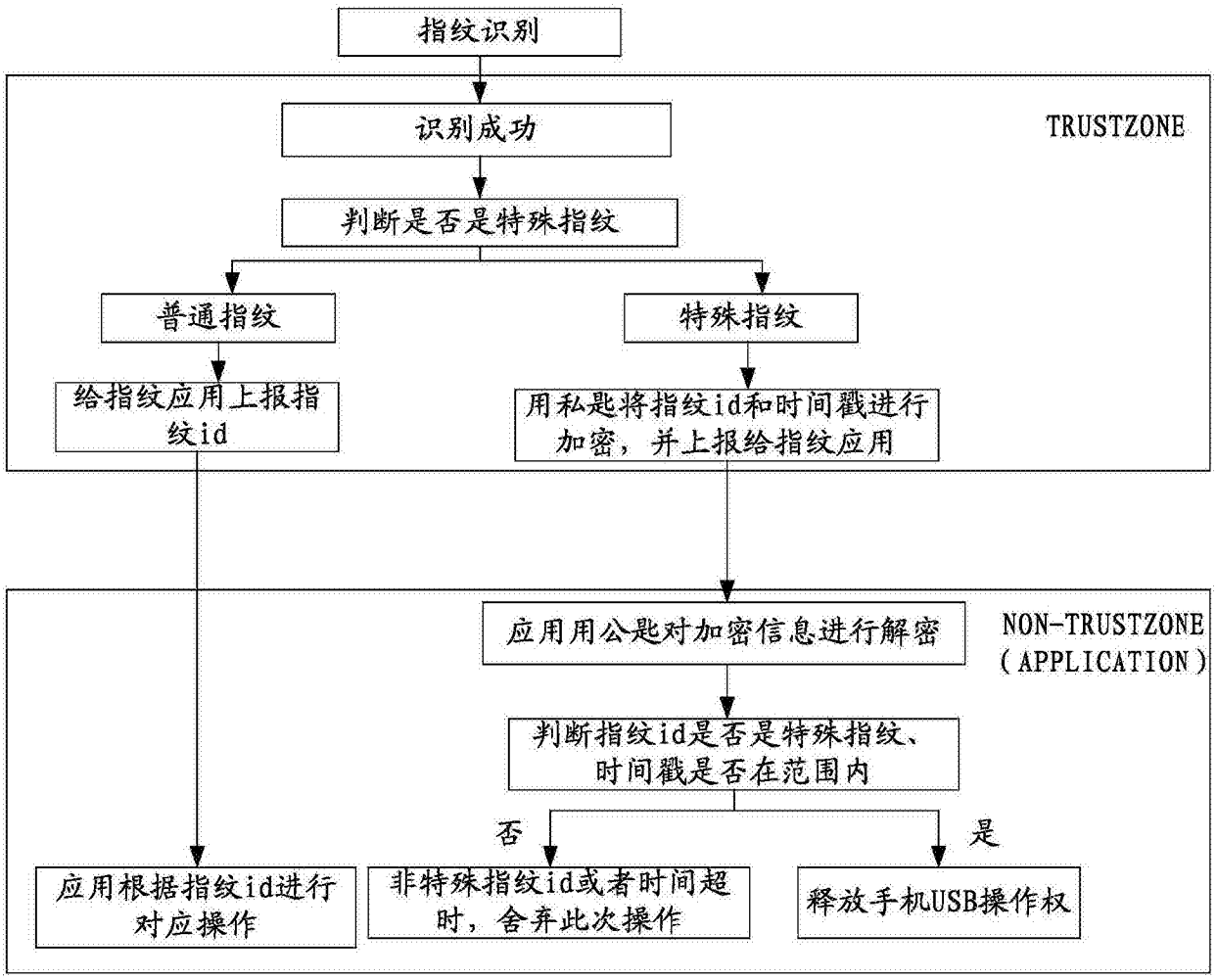

指纹识别
识别成功
TRUSTZONE
判断是否是特殊指纹
普通指纹
特殊指纹
给指纹应用上报指纹id
用私匙将指纹id和时间戳进行加密，并上报给指纹应用
应用用公匙对加密信息进行解密
NON-TRUSTZONE
(APPLICATION)
判断指纹id是否是特殊指纹、时间戳是否在范围内
否
是
应用根据指纹id进行对应操作
非特殊指纹id或者时间超时，舍弃此次操作
释放手机USB操作权

图4

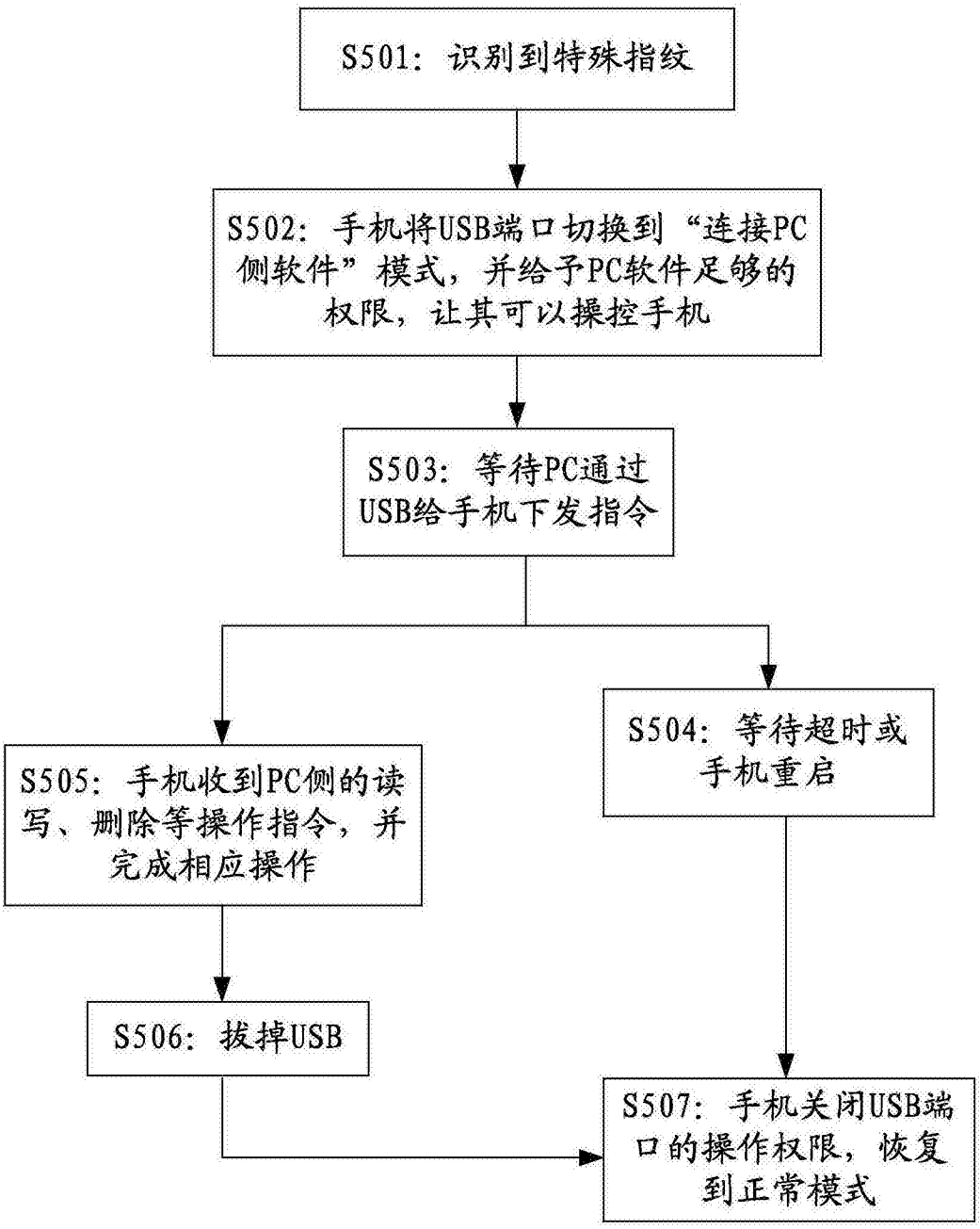

S501：识别到特殊指纹
S502：手机将USB端口切换到“连接PC侧软件”模式，并给予PC软件足够的权限，让其可以操控手机
S503：等待PC通过USB给手机下发指令
S504：等待超时或手机重启
S505：手机收到PC侧的读写、删除等操作指令，并完成相应操作
S506：拔掉USB
S507：手机关闭USB端口的操作权限，恢复到正常模式

图5