(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 104050402 A
(43)申请公布日 2014.09.17

(21)申请号 201410262255.5

(22)申请日 2014.06.12

(71)申请人 深圳市汇顶科技股份有限公司
地址 518000 广东省深圳市福田保税区腾飞工业大厦B座2、13层

(72)发明人 毛金勇 邓耿淳 阙滨城 唐成

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张大威

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 3/01(2006.01)
G06F 3/0488(2013.01)

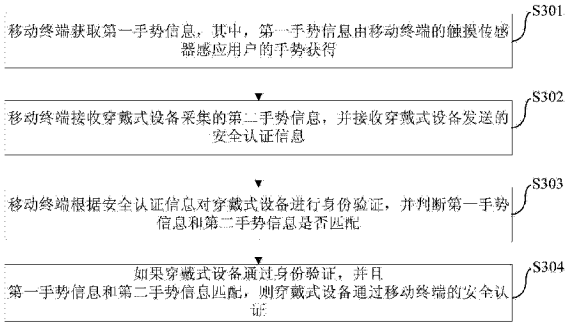
权利要求书3页 说明书11页 附图4页

(54)发明名称

移动终端安全认证的方法、系统与移动终端

(57)摘要

本发明提出一种移动终端安全认证的方法、系统和移动终端，其中，该方法包括：移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息；移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息；以及如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证。本发明实施例的移动终端安全认证的方法，保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。



CN 104050402 A

1. 一种移动终端安全认证的方法，其特征在于，包括：

移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息；

所述移动终端根据所述安全认证信息对所述穿戴式设备进行身份验证，并验证所述第一手势信息；

如果所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

2. 如权利要求 1 所述的方法，其特征在于，所述移动终端根据所述安全认证信息对所述穿戴式设备进行身份验证，具体包括：

所述移动终端根据所述安全认证信息计算所述移动终端与所述穿戴式设备之间的距离，并判断所述移动终端与所述穿戴式设备之间的距离是否小于预设阈值，若小于所述预设阈值，则所述穿戴式设备通过身份验证。

3. 如权利要求 1 所述的方法，其特征在于，所述移动终端根据所述安全认证信息对所述穿戴式设备进行身份验证，具体包括：

所述移动终端从所述安全认证信息中获取密码信息；以及

所述移动终端将获取的密码信息和预存的密码信息进行比对，若二者一致，则所述穿戴式设备通过身份验证。

4. 如权利要求 1 所述的方法，其特征在于，所述移动终端根据所述安全认证信息对所述穿戴式设备进行身份验证，具体包括：

所述移动终端从所述安全认证信息中获取生物特征信息；以及

所述移动终端将获取的生物特征信息和预存的生物特征信息进行比对，若二者一致，则所述穿戴式设备通过身份验证。

5. 如权利要求 4 所述的方法，其特征在于，所述生物特征信息包括静脉特征信息、气味特征信息、皮肤特征信息、血管纹理特征信息、手掌特征信息、眼睛特征信息、脸型特征信息中的一种或者多种。

6. 如权利要求 1 所述的方法，其特征在于，所述第一手势信息由所述穿戴式设备采集，并发送至所述移动终端。

7. 如权利要求 1 所述的方法，其特征在于，所述第一手势信息由所述移动终端的触摸传感器感应所述用户的手势获得。

8. 如权利要求 7 所述的方法，其特征在于，所述方法还包括：

所述移动终端接收所述穿戴式设备采集的第二手势信息；

所述验证所述第一手势信息，具体包括：

判断所述第一手势信息和所述第二手势信息是否匹配，若二者一致，则所述第一手势信息通过验证。

9. 如权利要求 1-8 任一项所述的方法，其特征在于，所述穿戴式设备通过所述移动终端的安全认证之后，所述方法还包括：

所述移动终端接收用户触发的操作请求，并根据所述操作请求完成相应的操作。

10. 如权利要求 9 所述的方法，其特征在于，所述接收用户触发的操作请求，并根据所述操作请求完成相应的操作，具体包括：

所述移动终端接收用户触发的不同级别的操作请求，并从所述安全认证信息中获取级

别信息，执行对应级别的操作，并进入相关的应用。

11. 如权利要求 1-10 任一项所述的方法，其特征在于，所述穿戴式设备包括手环、手表、手套、眼镜、戒指、衣服、腰带、鞋子、袜子、帽子中的一种或者多种。

12. 一种移动终端，其特征在于，包括：

获取模块，用于获取第一手势信息，并接收穿戴式设备发送的安全认证信息；

身份验证模块，用于根据所述安全认证信息对所述穿戴式设备进行身份验证；

手势信息验证模块，用于验证所述第一手势信息，如果所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

13. 如权利要求 12 所述的移动终端，其特征在于，所述身份验证模块具体用于：

根据所述安全认证信息计算所述移动终端与所述穿戴式设备之间的距离，并判断所述移动终端与所述穿戴式设备之间的距离是否小于预设阈值，若小于所述预设阈值，则所述穿戴式设备通过身份验证。

14. 如权利要求 12 所述的移动终端，其特征在于，所述身份验证模块具体用于：

从所述安全认证信息中获取密码信息，以及将获取的密码信息和预存的密码信息进行比对，若二者一致，则所述穿戴式设备通过身份验证。

15. 如权利要求 12 所述的移动终端，其特征在于，所述身份验证模块具体用于：

从所述安全认证信息中获取生物特征信息，以及将获取的生物特征信息和预存的生物特征信息进行比对，若二者一致，则所述穿戴式设备通过身份验证。

16. 如权利要求 15 所述的移动终端，其特征在于，所述生物特征信息包括静脉特征信息、气味特征信息、皮肤特征信息、血管纹理特征信息、手掌特征信息、眼睛特征信息、脸型特征信息中的一种或者多种。

17. 如权利要求 12 所述的移动终端，其特征在于，所述第一手势信息由所述穿戴式设备采集，并发送至所述移动终端。

18. 如权利要求 12 所述的移动终端，其特征在于，所述第一手势信息由所述移动终端的触摸传感器感应所述用户的手势获得。

19. 如权利要求 18 所述的移动终端，其特征在于，所述移动终端还包括：

接收模块，用于接收所述穿戴式设备采集的第二手势信息；

所述手势信息验证模块具体用于判断所述第一手势信息和所述第二手势信息是否匹配，若二者一致，则所述第一手势信息通过验证。

20. 如权利要求 12-19 任一项所述的移动终端，其特征在于，还包括：

操作模块，用于接收用户触发的操作请求，并根据所述操作请求完成相应的操作。

21. 如权利要求 20 所述的移动终端，其特征在于，所述操作模块具体包括：

接收单元，用于接收用户触发的不同级别的操作请求，并从所述安全认证信息中获取级别信息；

执行单元，用于执行对应级别的操作，并进入相关的应用。

22. 一种移动终端安全认证的系统，其特征在于，包括：移动终端和穿戴式设备，其中，

所述穿戴式设备用于将安全认证信息发送至所述移动终端；

所述移动终端用于获取第一手势信息，并接收穿戴式设备发送的安全认证信息，以及根据所述安全认证信息对所述穿戴式设备进行身份验证，并验证所述第一手势信息，如果

所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

23. 如权利要求 22 所述的系统，其特征在于，所述移动终端具体用于：

根据所述安全认证信息计算所述移动终端与所述穿戴式设备之间的距离，并判断所述移动终端与所述穿戴式设备之间的距离是否小于预设阈值，若小于所述预设阈值，则所述穿戴式设备通过身份验证；或者

从所述安全认证信息中获取密码信息，以及将获取的密码信息和预存的密码信息进行比对，若二者一致，则所述穿戴式设备通过身份验证；或者

从所述安全认证信息中获取生物特征信息，以及将获取的生物特征信息和预存的生物特征信息进行比对，若二者一致，则所述穿戴式设备通过身份验证。

24. 如权利要求 23 所述的系统，其特征在于，所述生物特征信息包括静脉特征信息、气味特征信息、皮肤特征信息、血管纹理特征信息、手掌特征信息、眼睛特征信息、脸型特征信息中的一种或者多种。

25. 如权利要求 22 所述的系统，其特征在于，所述第一手势信息由所述穿戴式设备采集，并发送至所述移动终端。

26. 如权利要求 22 所述的系统，其特征在于，所述第一手势信息由所述移动终端的触摸传感器感应所述用户的手势获得。

27. 如权利要求 26 所述的系统，其特征在于，所述移动终端还用于：

接收所述穿戴式设备采集的第二手势信息，判断所述第一手势信息和所述第二手势信息是否匹配，若二者一致，则所述第一手势信息通过验证。

28. 如权利要求 22-27 任一项所述的系统，其特征在于，所述穿戴式设备包括手环、手表、手套、眼镜、戒指、衣服、腰带、鞋子、袜子、帽子中的一种或者多种。

移动终端安全认证的方法、系统与移动终端

技术领域

[0001] 本发明涉及移动终端技术领域，尤其涉及一种移动终端安全认证的方法、系统与移动终端。

背景技术

[0002] 随着移动终端的使用越来越普及，用户在移动终端中存储的信息越来越多样化。目前，当移动终端处于锁定状态时，用户可通过点击组合的按键输入密码对屏幕进行解锁；或者对触摸屏的手机而言，在触摸屏上按照固定的轨迹进行触摸操作，以对屏幕进行安全认证，进而访问移动终端的重要应用。

[0003] 然而发明人在实现本发明的过程中，发现现有的对移动终端屏幕解锁后进入移动终端的方法不安全、用户体验不佳，如果用户解锁屏幕的密码和手势被其它人知道后，其它人也可以根据该密码或者手势对移动终端屏幕进行解锁，进入应用，造成移动终端的数据不安全，导致用户的隐私泄露。

发明内容

[0004] 本发明旨在至少解决上述技术问题之一。

[0005] 为此，本发明的第一个目的在于提出一种移动终端安全认证的方法。该方法不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私泄露，改善用户体验。

[0006] 本发明的第二个目的在于提出一种移动终端。

[0007] 本发明的第三个目的在于提出一种移动终端安全认证的系统。

[0008] 为了实现上述目的，本发明第一方面实施例的移动终端安全认证的方法，包括：移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息；所述移动终端根据所述安全认证信息对所述穿戴式设备进行身份验证，并验证所述第一手势信息；以及如果所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

[0009] 为了实现上述目的，本发明第二方面实施例的移动终端，包括：获取模块，用于获取第一手势信息，并接收穿戴式设备发送的安全认证信息；身份验证模块，用于根据所述安全认证信息对所述穿戴式设备进行身份验证；手势信息验证模块，用于验证所述第一手势信息，如果所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

[0010] 为了实现上述目的，本发明第三方面实施例的移动终端安全认证的系统，包括：移动终端和穿戴式设备，其中，所述穿戴式设备用于将所述安全认证信息发送至所述移动终端；所述移动终端用于获取第一手势信息，并接收穿戴式设备发送的安全认证信息，以及根据所述安全认证信息对所述穿戴式设备进行身份验证，并验证所述第一手势信息，如果所述穿戴式设备通过身份验证和所述第一手势信息通过验证，则所述穿戴式设备通过所述移

动终端的安全认证。

[0011] 本发明通过穿戴式设备将携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，二者均通过验证则为通过移动终端的安全认证，由此，不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0012] 本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0013] 本发明上述的和 / 或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中，

[0014] 图 1 是根据本发明第一个实施例的移动终端安全认证的方法的流程图；

[0015] 图 2 是根据本发明第二个实施例的移动终端安全认证的方法的流程图；

[0016] 图 3 是根据本发明第三个实施例的移动终端安全认证的方法的流程图；

[0017] 图 4(a) 和 (b) 是根据本发明一个实施例的移动终端安全认证的方法适用的应用场景；

[0018] 图 5 是根据本发明第四个实施例的移动终端安全认证的方法的流程图；

[0019] 图 6 是根据本发明第五个实施例的移动终端的结构示意图；

[0020] 图 7 是根据本发明第六个实施例的移动终端的结构示意图；

[0021] 图 8 是根据本发明第七个实施例的移动终端的结构示意图；以及

[0022] 图 9 是根据本发明第八个实施例的移动终端安全认证的系统的示意图。

具体实施方式

[0023] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

[0024] 在本发明的描述中，需要理解的是，术语“第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0025] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0026] 下面参考附图描述根据本发明实施例的移动终端安全认证的方法、系统和移动终端。

[0027] 目前，通过用户输入手势进行解锁然后访问移动终端的方法并不安全，如果在移动终端通过手势解锁的基础上，增加携带安全认证信息的可穿戴式设备，移动终端对可穿戴式设备的安全认证信息进行安全认证这样，不仅操作简单方便，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露。为此，本发明提出了一种移动终端安全认证的方法。

[0028] 图 1 是根据本发明第一个实施例的移动终端安全认证的方法的流程图。如图 1 所示，该移动终端安全认证的方法包括：

[0029] S101，移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息。

[0030] 在本发明的实施例中，穿戴式设备包括但不限于手环、手表、手套、眼镜、戒指、衣服、腰带、鞋子、袜子、帽子等中的一种或者多种。穿戴式设备可佩戴在用户的手上或者头上，并且穿戴式设备和移动终端进行绑定，其中，穿戴式设备可通过无线通信的方式，例如，蓝牙、红外、WIFI 等，与移动终端进行数据通信。

[0031] 具体地，移动终端可实时对屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，移动终端在监测到屏幕上有手势操作时，可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。同时，移动终端向穿戴式设备发送唤醒指令，以使穿戴式设备根据唤醒指令从睡眠模式切换至工作模式。穿戴式设备在进入工作模式之后，可将存储的安全认证信息通过无线通信的方式发送至移动终端。其中，安全认证信息可以是预先获取并存储在穿戴式设备的存储器中的，且安全认证信息用于移动终端对穿戴式设备的身份验证。

[0032] S102，移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息。

[0033] 在本发明的实施例中，移动终端根据安全认证信息计算移动终端与穿戴式设备之间的距离，并判断移动终端与穿戴式设备之间的距离是否小于预设阈值，若小于预设阈值，则穿戴式设备通过身份验证。具体地，安全认证信息中可包括穿戴式设备和移动终端之间的距离信息，也就是说，穿戴式设备可通过检测移动终端发射的无线信号的信号强度指示(RSSI，Received Signal Strength Indication)值，或者通过穿戴式设备上的例如距离传感器等，确定穿戴式设备和移动终端之间的距离，并将该距离作为安全认证信息发送至移动终端。如果移动终端判断移动终端与穿戴式设备之间的距离小于预设阈值，则说明穿戴式设备在移动终端可操控的范围内，也就是说，佩戴穿戴式设备的用户在移动终端附近，由此，可以确定是合法用户希望对移动终端进行操作，即穿戴式设备通过身份验证。

[0034] 在本发明的实施例中，移动终端从安全认证信息中获取密码信息，并从本地提取出预存的密码信息，以及将获取的密码信息和提取的密码信息进行比对，若二者一致，则确定穿戴式设备通过身份验证。具体而言，安全认证信息中可包括密码信息，也就是说，穿戴式设备和移动终端中可预先存储约定的密码信息，通过二者的比对，确定合法用户对移动终端进行操作。其中，穿戴式设备向移动终端发送安全认证信息时可进行加密处理，例如，穿戴式设备用存储的公钥对密码信息进行加密，然后将加密后的密码信息发送至移动终端。移动终端接收到加密后的密码信息之后，可使用存储的私钥对密码信息进行解密，然后

判断解密后的密码信息和移动终端中预存的密码信息是否匹配，从而确定是否通过对穿戴式设备的身份验证。

[0035] 在本发明的实施例中，在上述两种通过安全认证信息对穿戴式设备进行身份验证的方式的基础上，还可以结合对用户的生物特征信息进行验证的方式。换言之，移动终端可先对穿戴式设备进行身份验证，然后再对佩戴穿戴式设备的用户进行身份验证，即先确定穿戴式设备是授权设备，再确定用户是授权用户，从而进一步提高身份验证的准确性。具体地，移动终端从安全认证信息中获取用户的生物特征信息，并从本地提取出预存的生物特征信息，以及将获取的生物特征信息和提取的生物特征信息进行比对，若二者一致，则确定穿戴式设备通过身份验证。其中，移动终端本地中预存的生物特征信息可由穿戴式设备获取的，并由穿戴式设备发送至移动终端的，以使移动终端将用户的生物特征信息保存在本地中。其中，生物特征信息可包括但不限于用户的静脉特征信息、气味特征信息、皮肤特征信息、血管纹理特征信息、手掌特征信息、眼睛特征信息、脸型特征信息中的一种或者多种。

[0036] 进一步而言，移动终端判断第一手势信息和移动终端中预存的手势信息是否匹配。

[0037] 需要说明的是，对穿戴式设备的身份验证和对第一手势信息的验证的顺序可任意调整，在此不做限定。

[0038] S103，如果穿戴式设备通过身份验证和第一手势信息通过验证，则所述穿戴式设备通过所述移动终端的安全认证。

[0039] 当对穿戴式设备的身份验证和对第一手势信息的验证均通过时，才认为穿戴式设备通过移动终端的安全认证。

[0040] 在本发明的实施例中，在穿戴式设备通过移动终端的安全认证之后，移动终端向穿戴式设备发送睡眠指令，以使穿戴式设备根据睡眠指令从工作模式切换至睡眠模式，由此，可以节约穿戴式设备的电量。

[0041] 本发明实施例的移动终端安全认证的方法，通过穿戴式设备将携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在二者均通过验证才认为通过移动终端的安全验证，由此，不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0042] 图 2 是根据本发明第二个实施例的移动终端安全认证的方法的流程图。如图 2 所示，该移动终端安全认证的方法包括：

[0043] S201，移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息，其中，第一手势信息由穿戴式设备采集，并发送至移动终端。

[0044] 在本发明的实施例中，移动终端可实时对移动终端的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端可从其它工作状态下转换到待解锁状态，并初始化相关的设置。同时，移动终端向穿戴式设备发送唤醒指令，以使穿戴式设备根据唤醒指令从睡眠模式切换至工作模式。穿戴式设备在进入工作模式之后，可通过穿戴式设备中的传感器采集用户的手势操作，例如，通过内置的陀螺仪传感器、加速度传感器、方向传感器等采集用户的手势操作的数据，并根据采集到的数据计算出第一手势信息。然后，穿戴式设备将第一手势信息和存储的安全认证信息通过无线通信的方式发送至移动终端。

[0045] S202，移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息。

[0046] 移动终端对穿戴式设备进行身份验证，并且移动终端判断第一手势信息和移动终端中预存的手势信息是否匹配。

[0047] S203，如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证。

[0048] 本发明实施例的移动终端安全认证的方法，通过穿戴式设备将采集的手势信息和携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在二者均通过验证才认为通过移动终端的安全验证，由此，不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0049] 图 3 是根据本发明第三个实施例的移动终端安全认证的方法的流程图。如图 3 所示，该移动终端安全认证的方法包括：

[0050] S301，移动终端获取第一手势信息，其中，第一手势信息由移动终端的触摸传感器感应用户的手势获得。

[0051] 具体地，移动终端可实时对移动终端的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，移动终端在监测到屏幕上有手势操作时，可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。同时，移动终端向穿戴式设备发送唤醒指令，以使穿戴式设备根据唤醒指令从睡眠模式切换至工作模式。

[0052] S302，移动终端接收穿戴式设备采集的第二手势信息，并接收穿戴式设备发送的安全认证信息。

[0053] 在本发明的实施例中，穿戴式设备在进入工作模式之后，可通过穿戴式设备中的传感器采集用户的手势操作，例如，通过内置的陀螺仪传感器、加速度传感器、方向传感器等采集用户的手势操作的数据，并根据采集到的数据计算出第二手势信息。然后，穿戴式设备将第二手势信息和存储的安全认证信息通过无线通信的方式发送至移动终端。

[0054] S303，移动终端根据安全认证信息对穿戴式设备进行身份验证，并判断第一手势信息和第二手势信息是否匹配。

[0055] 移动终端对穿戴式设备进行身份验证，并且移动终端判断第一手势信息和从穿戴式设备接收到的第二手势信息是否匹配。

[0056] S304，如果穿戴式设备通过身份验证，并且第一手势信息和第二手势信息匹配，则穿戴式设备通过移动终端的安全认证。

[0057] 本发明实施例的移动终端安全认证的方法，通过穿戴式设备将采集的手势信息和携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在穿戴式设备身份验证通过后以及确定穿戴式设备采集的手势信息和移动终端识别的手势信息一致时，认为通过移动终端的安全验证，由此，不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0058] 下面结合实际场景详细说明本发明第三个实施例的移动终端安全认证的方法。图

4(a) 和 (b) 是根据本发明一个实施例的移动终端安全认证的方法适用的应用场景。

[0059] 如图 4(a) 和 (b) 所示，移动终端 10 包括触摸屏 11、处理器 12、触控管理模块 13、无线模块 14 和存储器 15。触摸屏 11 是移动终端 10 的输入设备，例如，可为电容式触摸屏。处理器 20 具有主控芯片，是移动终端 10 的核心部分，用于协调处理相关事务。触控管理模块 13 具有触控芯片，是触摸屏 11 的管理模块，主要用于处理用户手指触摸的传感解析。无线模块 14 是移动终端 10 与穿戴式设备 20 之间进行通信的模块。存储器 15 用于处理器 12 的数据存储、程序存储以及相关运算处理等。

[0060] 穿戴式设备 20 包括传感器 21、无线模块 22、处理器 23、安全模块 24 和存储器 25。传感器 21 可为例如陀螺仪传感器、加速度传感器等，用于辨别用户手势动作的传感。无线模块 22 用于与移动终端 10 进行信息的交互。处理器 23 用于运算传感器 21 采集到的手势，控制整个穿戴式设备的系统。安全模块 24 用于存储核心的安全认证信息，对安全认证信息的加密解密操作通过硬件的运算完成。存储器 25 用于存储数据、存储程序以及存储处理器 23 当前运行程序的指令和数据，并与处理器 23 交换信息。

[0061] 穿戴式设备 20，例如，手表，可佩戴在用户 30 的手腕上，处于低功耗的睡眠模式。用户 30 在移动终端 10 的触摸屏 11 上画出手势后，移动终端 10 的触控管理模块 13 持续检测手势，计算触摸坐标已获得此时间段内的手势信息，并且移动终端 10 通过无线模块 14 唤醒穿戴式设备 20，穿戴式设备 20 从低功耗的睡眠模式转入工作模式。穿戴式设备 20 启动传感器 21，通过传感器 21 采集用户的手势，并通过处理器 23 计算出传感器 21 采集的手势对应的手势信息。穿戴式设备 20 将手势信息和安全模块 24 中存储的安全认证信息通过硬件加密运算后，通过无线通信模块 22 传输至移动终端 10，其中，手势信息和安全认证信息可分开传输。移动终端 10 的处理器 12 在验证身份信息后，对比穿戴式设备 20 传感器 21 采集的手势信息和触控管理模块 13 计算的手势信息是否一致，如果二者一致，则通过安全认证。

[0062] 图 5 是根据本发明第四个实施例的移动终端安全认证的方法的流程图。如图 5 所示，该移动终端安全认证的方法包括 ：

[0063] S501，移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息。

[0064] S502，移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息。

[0065] S503，如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证。

[0066] S504，移动终端接收用户触发的操作请求，并根据操作请求完成相应的操作。

[0067] 在本发明的实施例中，移动终端接收用户触发的不同级别的操作请求，并从安全认证信息中获取级别信息，执行对应级别的操作，并进入相关的应用。具体地，移动终端可对不同的用户设置不同的级别，例如，移动终端可基于用户的通讯记录生成对应的级别信息，对联系频繁的用户授予较高级别，对偶尔联系的用户授予较低级别，对非联系的用户不授予级别。此外，移动终端可对移动终端的所有者定义为系统内人员，授予可以进入移动终端系统的权限，对系统信息进行修改等操作。移动终端将用户对应的级别信息发送至穿戴式设备，以使穿戴式设备保存该级别信息。在用户佩戴穿戴式设备进行操作时，可根据用户的级别信息确定用户可进入系统的等级，从而授权用户进行相应的操作，进入相关的应用。

[0068] 本发明实施例的移动终端安全认证的方法，在通过移动终端的安全认证后，通过接收不同级别的用户触发的操作请求，在用户具有对应的级别时才执行相应的应用，由此，可以进一步提高移动终端中存储的用户数据的安全性，避免了用户隐私被泄露。

[0069] 为了实现上述实施例，本发明还提出一种移动终端。

[0070] 图 6 是根据本发明第五个实施例的移动终端的结构示意图。如图 6 所示，该移动终端包括：获取模块 110、身份验证模块 120、手势信息验证模块 130。

[0071] 具体地，获取模块 110 用于获取第一手势信息，并接收穿戴式设备发送的安全认证信息。具体而言，移动终端可实时对移动终端的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，移动终端在监测到屏幕上有手势操作时，获取模块 110 可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。

[0072] 身份验证模块 120 用于根据安全认证信息对穿戴式设备进行身份验证。

[0073] 手势信息验证模块 130 用于验证第一手势信息，如果第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证。

[0074] 本发明实施例的移动终端，通过穿戴式设备将携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在二者均通过验证后，认为通过移动终端的安全认证，由此，不仅无需增加用户额外的操作，还可以提高移动终端屏幕解锁的安全性，保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0075] 图 7 是根据本发明第六个实施例的移动终端的结构示意图。如图 7 所示，该移动终端包括：获取模块 110、身份验证模块 120、手势信息验证模块 130、解锁模块 140、发送模块 150 和接收模块 160。

[0076] 获取模块 110、身份验证模块 120 和手势信息验证模块 130 的描述与上述实施例相同。

[0077] 进一步地，移动终端还包括解锁模块 140，发送模块 150 和接收模块 160。解锁模块 140 用于如果第一手势信息通过验证，对屏幕进行解锁。在解锁模块对屏幕解锁之后，发送模块 150 向穿戴式设备发送睡眠指令，以使穿戴式设备根据睡眠指令从工作模式切换至睡眠模式，由此，可以节约穿戴式设备的电量。接收模块 160 用于接收穿戴式设备采集的第二手势信息，其中，第二手势信息由穿戴式设备识别用户的动作获得。具体地，穿戴式设备在进入工作模式之后，可通过穿戴式设备中的传感器采集用户的手势操作，例如，通过内置的陀螺仪传感器、加速度传感器、方向传感器等采集用户的手势操作的数据，并根据采集到的数据计算出第二手势信息。然后，穿戴式设备将第二手势信息和存储的安全认证信息通过无线通信的方式发送至接收模块 160。

[0078] 手势信息验证模块 130 还用于判断第一手势信息和第二手势信息是否匹配。具体地，移动终端可实时对屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，获取模块 110 在监测到屏幕上有手势操作时，可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。进一步而言，如果身份验证模块 120 通过对穿戴式设备的身份验证，则手势信息验证模块 130 继续判断第一手势信息和从穿戴式设备接收到的第二手势信息是否匹配。

[0079] 本发明实施例的移动终端，通过穿戴式设备将采集的手势信息和携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在穿戴式设备身份验证通过后以及确定穿戴式设备采集的手势信息和移动终端识别的手势信息一致时，认为通过移动终端的安全认证，由此，不仅无需增加用户额外的操作，还保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0080] 图 8 是根据本发明第七个实施例的移动终端的结构示意图。如图 8 所示，该移动终端包括：获取模块 110、身份验证模块 120、手势信息验证模块 130、解锁模块 140、发送模块 150、接收模块 160 和操作模块 170，其中，操作模块 170 具体包括接收单元 171 和执行单元 172。

[0081] 获取模块 110、身份验证模块 120、手势信息验证模块 130、解锁模块 140、发送模块 150 和接收模块 160 与上述实施例相同。

[0082] 具体地，操作模块 170 用于接收用户触发的操作请求，并根据操作请求完成相应的操作。

[0083] 在本发明的实施例中，操作模块 170 具体包括接收单元 171 和执行单元 172。其中，接收单元 171 用于接收用户触发的不同级别的操作请求，并从安全认证信息中获取级别信息。执行单元 172 用于当用户具有级别信息对应的级别时，执行对应级别的操作，并进入相关的应用。具体而言，操作模块 170 可对不同的用户设置不同的级别，例如，操作模块 170 可基于用户的通讯记录生成对应的级别信息，对联系频繁的用户授予较高级别，对偶尔联系的用户授予较低级别，对非联系的用户不授予级别。此外，操作模块 170 可对移动终端的所有者定义为系统内人员，授予可以进入移动终端系统的权限，对系统信息进行修改等操作。操作模块 170 将用户对应的级别信息发送至穿戴式设备，以使穿戴式设备保存该级别信息。在用户佩戴穿戴式设备进行操作时，接收单元 171 接收用户触发的不同级别的操作请求，然后执行单元 172 可根据用户的级别信息确定用户可进入系统的等级，从而授权用户进行相应的操作，进入相关的应用。

[0084] 本发明实施例的移动终端，在移动终端对屏幕解锁后，通过接收不同级别的用户触发的操作请求，在用户具有对应的级别时才执行相应的应用，由此，可以进一步提高移动终端中存储的用户数据的安全性，避免了用户隐私被泄露。

[0085] 为了实现上述实施例，本发明还提出一种移动终端安全认证的系统。

[0086] 图 9 是根据本发明第八个实施例的移动终端安全认证的系统的示意图。如图 9 所示，该移动终端安全认证的系统包括：移动终端 10 和穿戴式设备 20，其中，

[0087] 移动终端 10 用于获取第一手势信息，并接收穿戴式设备 20 发送的安全认证信息，以及根据安全认证信息对穿戴式设备 20 进行身份验证，并验证第一手势信息，如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证。

[0088] 在本发明的实施例中，穿戴式设备 20 包括但不限于手环、手表、手套、眼镜、戒指、衣服、腰带、鞋子、袜子、帽子等中的一种或者多种。穿戴式设备 20 可佩戴在用户的手上或者头上，并且穿戴式设备 20 和移动终端 10 进行绑定，其中，穿戴式设备 20 可通过无线通信的方式，例如，蓝牙、红外、WIFI 等，与移动终端 10 进行数据通信。具体地，移动终端 10 可实时对移动终端 10 的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端 10 可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，移动终端 10 在监测

到屏幕上有手势操作时，可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。同时，移动终端 10 向穿戴式设备 20 发送唤醒指令，以使穿戴式设备 20 根据唤醒指令从睡眠模式切换至工作模式。穿戴式设备 20 在进入工作模式之后，可将存储的安全认证信息通过无线通信的方式发送至移动终端 10。其中，安全认证信息可以是穿戴式设备 20 预先获取并存储在穿戴式设备 20 的存储器中的，且安全认证信息用于移动终端 10 对穿戴式设备 20 的身份安全认证。

[0089] 在本发明的实施例中，移动终端 10 还用于从安全认证信息中获取移动终端 10 与穿戴式设备 20 之间的距离，并判断移动终端 10 与穿戴式设备 20 之间的距离是否小于预设阈值，若小于预设阈值，则确定穿戴式设备 20 通过身份验证。具体地，安全认证信息中可包括穿戴式设备 20 和移动终端 10 之间的距离信息，也就是说，穿戴式设备 20 可通过检测移动终端 10 发射的无线信号的信号强度指示 (RSSI，Received Signal Strength Indication) 值，或者通过穿戴式设备 20 上的例如距离传感器等，确定穿戴式设备 20 和移动终端 10 之间的距离，并将该距离作为安全认证信息发送至移动终端 10。如果移动终端 10 判断移动终端 10 与穿戴式设备 20 之间的距离小于预设阈值，则说明穿戴式设备 20 在移动终端 10 可操控的范围内，也就是说，佩戴穿戴式设备 20 的用户在移动终端 10 附近，由此，可以确定是合法用户希望对移动终端 10 进行操作，即移动终端 10 通过对穿戴式设备 20 的身份验证。

[0090] 在本发明的实施例中，移动终端 10 还用于从安全认证信息中获取密码信息，并从本地提取出预存的密码信息，以及将获取的密码信息和提取的密码信息进行比对，若二者一致，则确定穿戴式设备 20 通过身份验证。具体而言，安全认证信息中可包括密码信息，也就是说，穿戴式设备 20 和移动终端 10 中可预先存储约定的密码信息，通过二者的比对，确定合法用户对移动终端 10 进行操作。其中，穿戴式设备 20 向移动终端 10 发送安全认证信息时可进行加密处理，例如，穿戴式设备 20 用存储的公钥对密码信息进行加密，然后将加密后的密码信息发送至移动终端 10。移动终端 10 接收到加密后的密码信息之后，可使用存储的私钥对密码信息进行解密，然后判断解密后的密码信息和移动终端 10 中预存的密码信息是否匹配，从而确定是否通过对穿戴式设备 20 的身份验证。

[0091] 在本发明的实施例中，在上述两种通过安全认证信息对穿戴式设备 20 进行身份验证的方式的基础上，移动终端 10 还可以结合对用户的身份特征信息进行验证的方式。换言之，移动终端 10 可先对穿戴式设备 20 进行身份验证，然后再对佩戴穿戴式设备 20 的用户进行身份验证，即先确定穿戴式设备 20 是授权设备，再确定用户是授权用户，从而进一步提高身份验证的准确性。具体地，移动终端 10 从安全认证信息中获取用户的生物特征信息，并从本地提取出预存的生物特征信息，以及将获取的生物特征信息和提取的生物特征信息进行比对，若二者一致，则确定穿戴式设备 20 通过身份验证。其中，移动终端 10 本地中预存的生物特征信息可由穿戴式设备 20 获取的，并由穿戴式设备 20 发送至移动终端 10 的，以使移动终端 10 将用户的生物特征信息保存在本地中。其中，生物特征信息可包括但不限于用户的静脉特征信息、气味特征信息、皮肤特征信息、血管纹理特征信息、手掌特征信息、眼睛特征信息、脸型特征信息中的一种或者多种。

[0092] 移动终端 10 对穿戴式设备 20 进行身份验证，并且移动终端 10 判断第一手势信息和移动终端中预存的手势信息是否匹配。如果穿戴式设备 20 通过身份验证，并且移动终端 10 判断第一手势信息和预设的手势信息匹配，则对屏幕进行解锁。

[0093] 在本发明的实施例中，在移动终端 10 对屏幕解锁之后，移动终端 10 向穿戴式设备 20 发送睡眠指令，以使穿戴式设备 20 根据睡眠指令从工作模式切换至睡眠模式，由此，可以节约穿戴式设备的电量。

[0094] 本发明实施例的移动终端安全认证的系统，通过穿戴式设备将携带的安全认证信息发送至移动终端，移动终端在通过结合对穿戴式设备的身份验证以及对手势信息的验证，在二者均通过验证后对屏幕进行解锁，由此，不仅无需增加用户额外的操作，还可以提高移动终端屏幕解锁的安全性，保证了移动终端中存储的用户数据的安全性，避免了用户隐私被泄露，改善了用户体验。

[0095] 在本发明的实施例中，第一手势信息通过穿戴式设备 20 获得，并发送至移动终端 10。具体而言，移动终端 10 可实时对移动终端 10 的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端 10 可从其它工作状态下转换到待解锁状态，并初始化相关的设置。同时，移动终端 10 向穿戴式设备 20 发送唤醒指令，以使穿戴式设备 20 根据唤醒指令从睡眠模式切换至工作模式。穿戴式设备 20 在进入工作模式之后，可通过穿戴式设备 20 中的传感器采集用户的手势操作，例如，通过内置的陀螺仪传感器、加速度传感器、方向传感器等采集用户的手势操作的数据，并根据采集到的数据计算出第一手势信息。然后，穿戴式设备 20 将第一手势信息和存储的安全认证信息通过无线通信的方式发送至移动终端 10。

[0096] 在本发明的实施例中，第一手势信息由移动终端 10 识别用户的动作获得，移动终端 10 还用于接收穿戴式设备 20 采集的第二手势信息，并根据第二手势信息对第一手势信息进行匹配验证，其中，第二手势信息由穿戴式设备 20 识别用户的动作获得。具体地，移动终端 10 可实时对移动终端的屏幕进行监测，当监测到用户在屏幕上进行手势操作时，移动终端 10 可从其它工作状态下转换到待解锁状态，并初始化相关的设置，由此，移动终端 10 在监测到屏幕上有手势操作时，可通过计算该手势操作的坐标，以获得用户在屏幕上输入的第一手势信息。同时，移动终端 10 向穿戴式设备 20 发送唤醒指令，以使穿戴式设备 20 根据唤醒指令从睡眠模式切换至工作模式。穿戴式设备 20 在进入工作模式之后，可通过穿戴式设备 20 中的传感器采集用户的手势操作，例如，通过内置的陀螺仪传感器、加速度传感器、方向传感器等采集用户的手势操作的数据，并根据采集到的数据计算出第二手势信息。然后，穿戴式设备 20 将第二手势信息和存储的安全认证信息通过无线通信的方式发送至移动终端 10。如果移动终端 10 通过对穿戴式设备 20 的身份验证，则移动终端 10 继续判断第一手势信息和从穿戴式设备 20 接收到的第二手势信息是否匹配。

[0097] 在本发明的实施例中，移动终端 10 接收用户触发的操作请求，并根据操作请求完成相应的操作。其中，移动终端 10 接收用户触发的不同级别的操作请求，并从安全认证信息中获取级别信息，当用户具有级别信息对应的级别时，执行对应级别的操作，并进入相关的应用。具体地，移动终端 10 可对不同的用户设置不同的级别，例如，移动终端 10 可基于用户的通讯记录生成对应的级别信息，对联系频繁的用户授予较高级别，对偶尔联系的用户授予较低级别，对非联系的用户不授予级别。此外，移动终端 10 可对移动终端 10 的所有者定义为系统内人员，授予可以进入移动终端系统的权限，对系统信息进行修改等操作。移动终端 10 将用户对应的级别信息发送至穿戴式设备 20，以使穿戴式设备 20 保存该级别信息。在用户佩戴穿戴式设备 20 进行操作时，可根据用户的级别信息确定用户可进入系统的等级，从而授权用户进行相应的操作，进入相关的应用。由此，在移动终端 10 对屏幕解锁

后，通过接收不同级别的用户触发的操作请求，在用户具有对应的级别时才执行相应的应用，可以进一步提高移动终端 10 中存储的用户数据的安全性，避免了用户隐私被泄露。

[0098] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列 (PGA)，现场可编程门阵列 (FPGA) 等。

[0099] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0100] 尽管已经示出和描述了本发明的实施例，本领域的普通技术人员可以理解：在不脱离本发明的原理和宗旨的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由权利要求及其等同物限定。

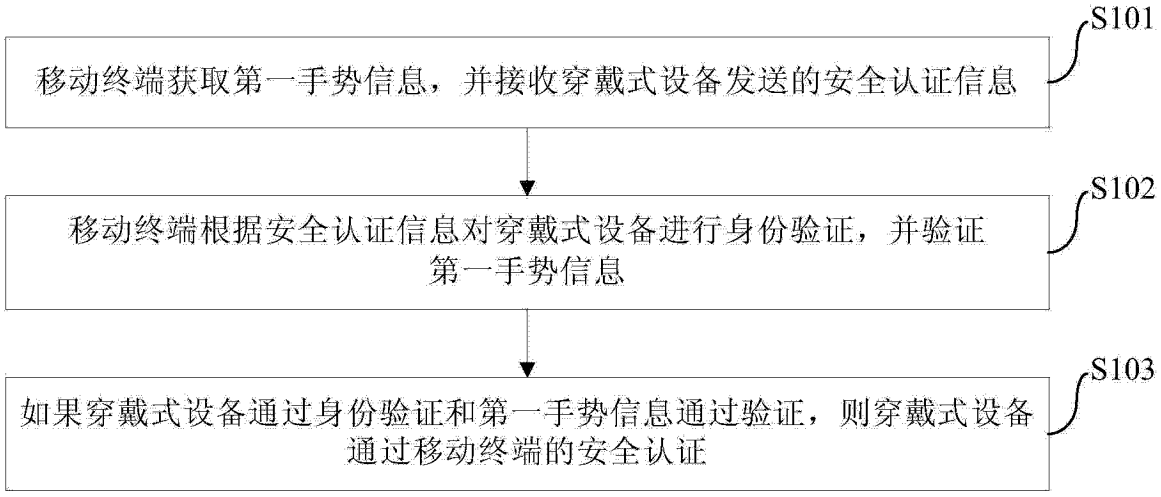

S101
移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息
S102
移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息
S103
如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证

图 1

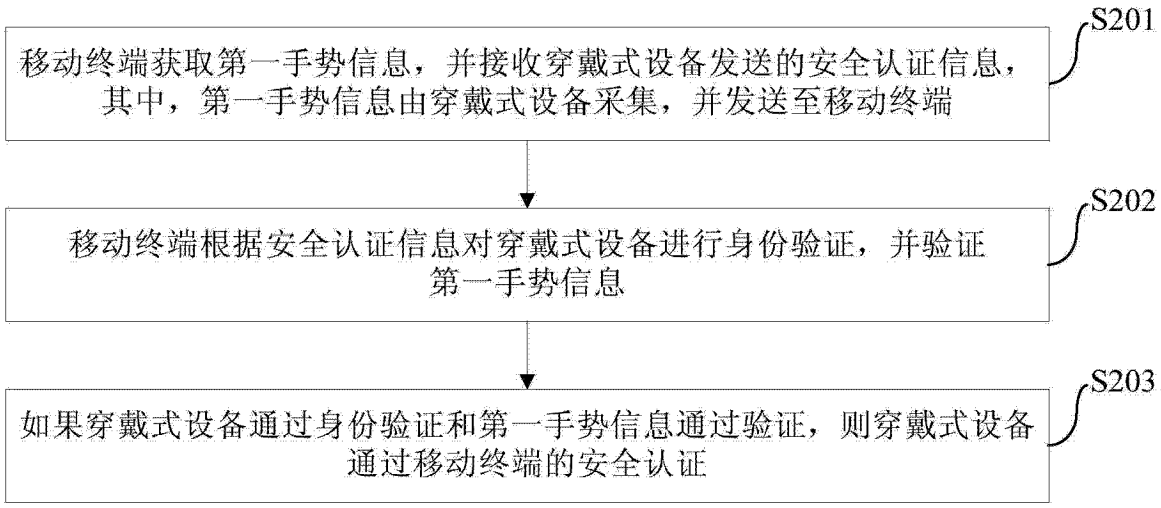

S201
移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息，其中，第一手势信息由穿戴式设备采集，并发送至移动终端
S202
移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息
S203
如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证

图 2

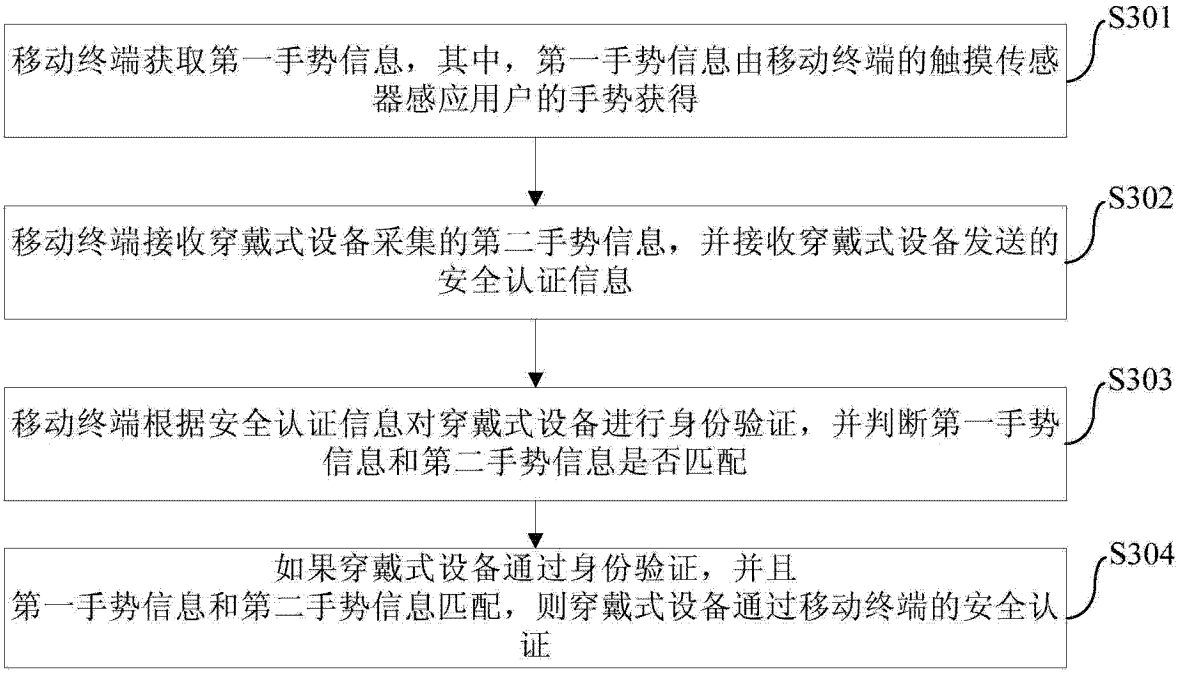

移动终端获取第一手势信息，其中，第一手势信息由移动终端的触摸传感器感应用户的手势获得
S301
移动终端接收穿戴式设备采集的第二手势信息，并接收穿戴式设备发送的安全认证信息
S302
移动终端根据安全认证信息对穿戴式设备进行身份验证，并判断第一手势信息和第二手势信息是否匹配
S303
如果穿戴式设备通过身份验证，并且
第一手势信息和第二手势信息匹配，则穿戴式设备通过移动终端的安全认证
S304

图 3

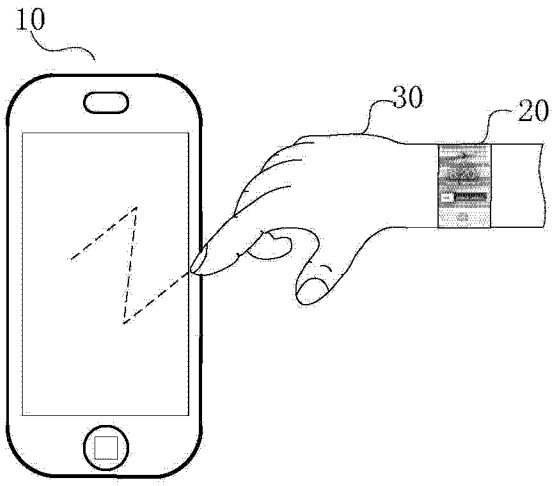

10
30
20

图 4(a)

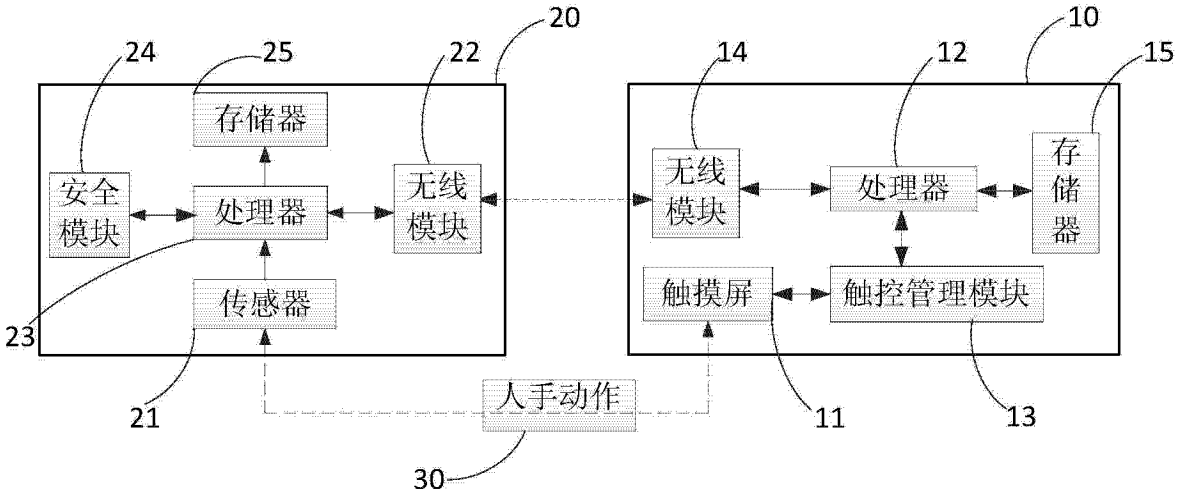

20
24
25
22
14
12
10
15
存储器
安全模块
处理器
无线模块
无线模块
处理器
存储器
传感器
触摸屏
触控管理模块
23
21
人手动作
11
13
30

图 4(b)

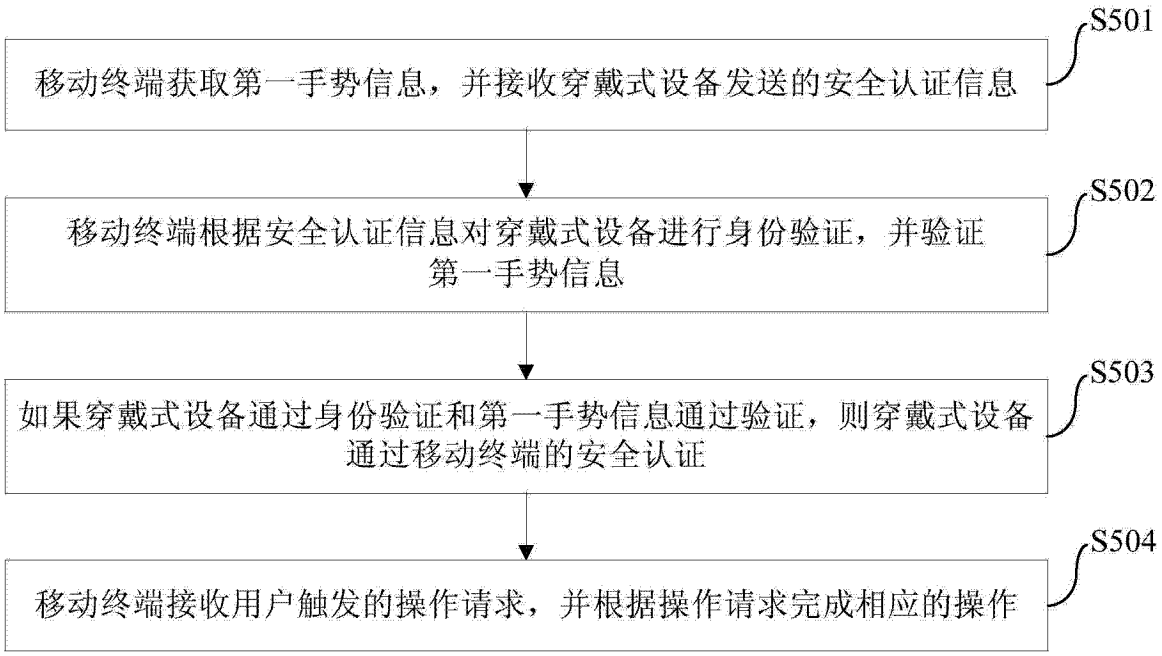

S501
移动终端获取第一手势信息，并接收穿戴式设备发送的安全认证信息
S502
移动终端根据安全认证信息对穿戴式设备进行身份验证，并验证第一手势信息
S503
如果穿戴式设备通过身份验证和第一手势信息通过验证，则穿戴式设备通过移动终端的安全认证
S504
移动终端接收用户触发的操作请求，并根据操作请求完成相应的操作

图 5

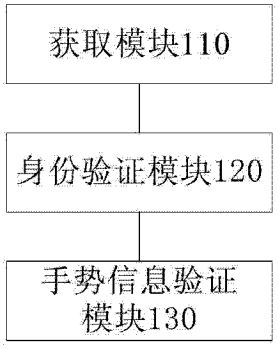

获取模块110
身份验证模块120
手势信息验证模块130

图 6

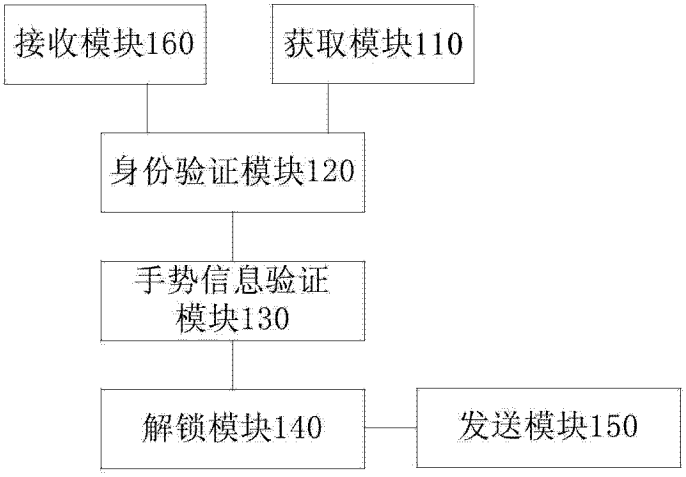

接收模块160
获取模块110
身份验证模块120
手势信息验证模块130
解锁模块140
发送模块150

图 7

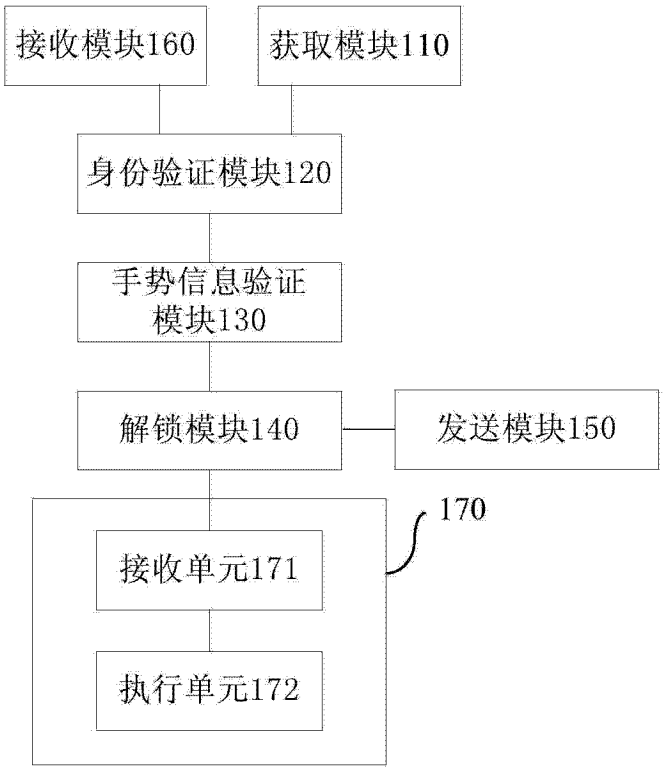

接收模块160
获取模块110
身份验证模块120
手势信息验证模块130
解锁模块140
发送模块150
170
接收单元171
执行单元172

图 8

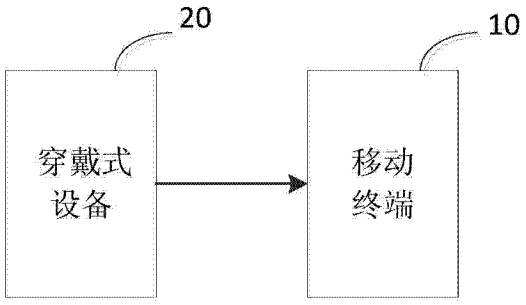

20
10
穿戴式设备
移动终端

图 9