(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 105991654 A
(43)申请公布日 2016.10.05

(21)申请号 201610127235.6

(22)申请日 2016.03.07

(71)申请人 李明
地址 100086 北京市海淀区太月园12号楼603室

(72)发明人 李明

(51)Int.Cl.
H04L 29/06(2006.01)

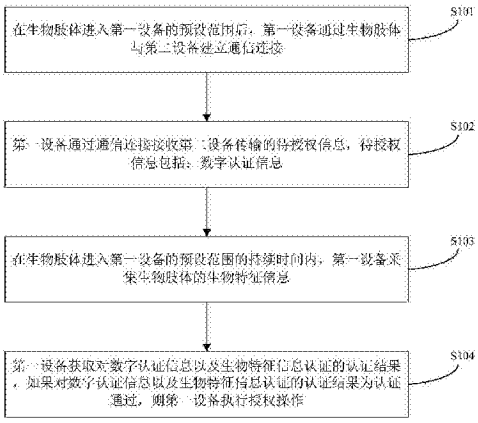
权利要求书3页 说明书11页 附图2页

(54)发明名称

一种授权认证方法、装置和系统

(57)摘要

本发明提供一种授权认证方法、装置和系统，该授权认证方法包括：在生物肢体进入第一设备的预设范围后，第一设备通过生物肢体与第二设备建立通信连接；第一设备通过通信连接接收第二设备传输的待授权信息，待授权信息包括：数字认证信息；在生物肢体进入第一设备的预设范围的持续时间内，第一设备采集生物肢体的生物特征信息；第一设备获取对数字认证信息以及生物特征信息认证的认证结果，如果对数字认证信息以及生物特征信息认证的认证结果为认证通过，则第一设备执行授权操作。通过该授权认证方法可以防止他人利用腕表等电子设备冒充用户通过授权，保证了信息和财产的安全。



CN 105991654 A

1.一种授权认证方法,其特征在于,包括:

在生物肢体进入第一设备的预设范围后,所述第一设备通过所述生物肢体与第二设备建立通信连接;

所述第一设备通过所述通信连接接收所述第二设备传输的待授权信息,所述待授权信息包括:数字认证信息;

在所述生物肢体进入第一设备的预设范围的持续时间内,所述第一设备采集所述生物肢体的生物特征信息;

所述第一设备获取对所述数字认证信息以及所述生物特征信息认证的认证结果,如果对所述数字认证信息以及所述生物特征信息认证的认证结果为认证通过,则所述第一设备执行授权操作。

2.根据权利要求1所述的方法,其特征在于,

所述生物特征信息包括:指纹信息和/或静脉信息;

所述第一设备采集所述生物肢体的生物特征信息包括:

在所述生物肢体与所述第一设备接触的情况下,第一设备采集所述生物肢体与所述第一设备的接触部位的所述生物特征信息。

3.根据权利要求1或2所述的方法,其特征在于,所述第一设备获取对所述数字认证信息以及所述生物特征信息认证的认证结果包括:

所述第一设备对所述数字认证信息以及所述生物特征信息进行认证,获得所述认证结果。

4.根据权利要求1或2所述的方法,其特征在于,所述第一设备获取对所述数字认证信息以及所述生物特征信息的认证结果包括:

所述第一设备向后台发送所述生物特征信息以及所述数字认证信息;

所述第一设备接收所述后台发送的所述认证结果,其中:所述认证结果为所述后台对所述数字认证信息以及所述生物特征信息进行认证,获得的认证结果。

5.根据权利要求3或4所述的方法,其特征在于,所述待授权信息还包括:标识信息;

所述对所述数字认证信息以及所述生物特征信息认证包括:

根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证。

6.根据权利要求5所述的方法,其特征在于,根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证包括:

获取所述标识信息对应的认证因子和生物特征验证信息,并利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率,其中,所述认证结果为认证通过包括:在利用所述认证因子对所述数字认证信息进行数字认证通过且所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时,所述认证结果为认证通过。

7.根据权利要求6所述的方法,其特征在于,所述利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率包括:

利用所述认证因子对所述数字认证信息进行认证,当对所述数字认证信息认证通过时,判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值;或

判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值,当判断出

所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，利用所述认证因子对所述数字认证信息进行认证。

8.根据权利要求6或7所述的方法，其特征在于，

所述数字认证信息包括利用私钥签名后获得的电子签名信息，所述认证因子包括对所述电子签名信息进行验签的公钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述公钥对所述电子签名信息进行验签；和/或

所述数字认证信息包括利用对称密钥计算得到的MAC值，所述认证因子包括计算所述MAC值的对称密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述对称密钥计算MAC校验值，验证所述MAC值和MAC校验值；和/或

所述数字认证信息包括利用种子密钥生成的动态口令，所述认证因子包括所述验证所述动态口令的种子密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述种子密钥对所述动态口令进行验证。

9.一种授权认证装置，其特征在于，包括：

连接单元，在生物肢体进入授权认证装置的预设范围后，用于通过所述生物肢体与身份识别装置建立通信连接；

接收单元，用于通过所述通信连接接收所述身份识别装置传输的待授权信息，所述待授权信息包括：数字认证信息；

采集单元，在所述生物肢体进入授权认证装置的预设范围的持续时间内，用于采集所述生物肢体的生物特征信息；

执行单元，用于获取对所述数字认证信息以及所述生物特征信息认证的认证结果，如果对所述数字认证信息以及所述生物特征信息认证的认证结果为认证通过，则执行授权操作。

10.根据权利要求9所述的装置，其特征在于，所述生物特征信息包括：指纹信息和/或静脉信息；

所述采集单元，在所述生物肢体与所述授权认证装置接触的情况下，用于采集所述生物肢体与所述授权认证装置的接触部位的所述生物特征信息。

11.根据权利要求9或10所述的装置，其特征在于，

所述执行单元，具体用于对所述数字认证信息以及所述生物特征信息进行认证，获得所述认证结果。

12.根据权利要求9或10所述的装置，其特征在于，

所述执行单元，具体用于向后台发送所述生物特征信息以及所述数字认证信息，并接收所述后台发送的所述认证结果，其中：所述认证结果为所述后台对所述数字认证信息以及所述生物特征信息进行认证，获得的认证结果。

13.根据权利要求11或12所述的装置，其特征在于，所述待授权信息还包括：标识信息；

所述对所述数字认证信息以及所述生物特征信息认证包括：

根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证。

14.根据权利要求13所述的装置，其特征在于，根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证包括：

获取所述标识信息对应的认证因子和生物特征验证信息，并利用所述认证因子对所述

数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率，其中，所述认证结果为认证通过包括：在利用所述认证因子对所述数字认证信息进行数字认证通过且所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，所述认证结果为认证通过。

15.根据权利要求14所述的装置，其特征在于，所述利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率包括：

利用所述认证因子对所述数字认证信息进行认证，当对所述数字认证信息认证通过时，判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值；或

判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值，当判断出所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，利用所述认证因子对所述数字认证信息进行认证。

16.根据权利要求14或15所述的装置，其特征在于，

所述数字认证信息包括利用私钥签名后获得的电子签名信息，所述认证因子包括对所述电子签名信息进行验签的公钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述公钥对所述电子签名信息进行验签；和/或

所述数字认证信息包括利用对称密钥计算得到的MAC值，所述认证因子包括计算所述MAC值的对称密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述对称密钥计算MAC校验值，验证所述MAC值和MAC校验值；和/或

所述数字认证信息包括利用种子密钥生成的动态口令，所述认证因子包括所述验证所述动态口令的种子密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述种子密钥对所述动态口令进行验证。

17.一种授权认证系统，其特征在于，包括：身份识别装置以及如权利要求9-16所述的授权认证装置；

所述身份识别装置，用于通过所述通信连接向所述授权认证装置发送所述待授权信息。

18.根据权利要求17所述的系统，其特征在于，所述系统还包括：

后台，用于接收所述授权认证装置发送的所述生物特征信息以及所述数字认证信息，对所述数字认证信息以及所述生物特征信息进行认证，获得认证结果，并将所述认证结果发送至所述授权认证装置。

一种授权认证方法、装置和系统

技术领域

[0001] 本发明涉及一种电子技术领域，尤其涉及一种授权认证方法、装置和系统。

背景技术

[0002] 在用户使用电子设备获取某些特定场所(例如，办公区域、保密区域等)、网站登录、个人物品(汽车、保险柜等)、危险物品等的授权时，电子设备与设置在这些场所、个人物品或危险物品上的电子系统建立通信连接，然后将存储的密钥发送给电子系统，电子系统对密钥进行认证。由此可见，现有技术中的这种授权方式，其它人可以使用别人的电子设备进而获得授权，进而执行非法操作，造成用户的财产、信息等损失。

发明内容

[0003] 本发明旨在解决上述问题之一。

[0004] 本发明的主要目的在于提供一种授权认证方法。

[0005] 本发明的另一目的在于提供一种授权认证装置。

[0006] 本发明的又一目的在于提供一种授权认证系统。

[0007] 为达到上述目的，本发明的技术方案具体是这样实现的：

[0008] 本发明一方面提供了一种授权认证方法，包括：在生物肢体进入第一设备的预设范围后，所述第一设备通过所述生物肢体与第二设备建立通信连接；所述第一设备通过所述通信连接接收所述第二设备传输的待授权信息，所述待授权信息包括：数字认证信息；在所述生物肢体进入第一设备的预设范围的持续时间内，所述第一设备采集所述生物肢体的生物特征信息；所述第一设备获取对所述数字认证信息以及所述生物特征信息认证的认证结果，如果对所述数字认证信息以及所述生物特征信息认证的认证结果为认证通过，则所述第一设备执行授权操作。

[0009] 此外，所述生物特征信息包括：指纹信息和/或静脉信息；所述第一设备采集所述生物肢体的生物特征信息包括：在所述生物肢体与所述第一设备接触的情况下，第一设备采集所述生物肢体与所述第一设备的接触部位的所述生物特征信息。

[0010] 此外，所述第一设备获取对所述数字认证信息以及所述生物特征信息认证的认证结果包括：所述第一设备对所述数字认证信息以及所述生物特征信息进行认证，获得所述认证结果。

[0011] 此外，所述第一设备获取对所述数字认证信息以及所述生物特征信息的认证结果包括：所述第一设备向后台发送所述生物特征信息以及所述数字认证信息；所述第一设备接收所述后台发送的所述认证结果，其中：所述认证结果为所述后台对所述数字认证信息以及所述生物特征信息进行认证，获得的认证结果。

[0012] 此外，所述待授权信息还包括：标识信息；所述对所述数字认证信息以及所述生物特征信息认证包括：根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证。

[0013] 此外，根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证包括：获取所述标识信息对应的认证因子和生物特征验证信息，并利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率，其中，所述认证结果为认证通过包括：在利用所述认证因子对所述数字认证信息进行数字认证通过且所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，所述认证结果为认证通过。

[0014] 此外，所述利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率包括：

[0015] 利用所述认证因子对所述数字认证信息进行认证，当对所述数字认证信息认证通过时，判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值；或

[0016] 判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值，当判断出所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，利用所述认证因子对所述数字认证信息进行认证。

[0017] 此外，所述数字认证信息包括利用私钥签名后获得的电子签名信息，所述认证因子包括对所述电子签名信息进行验签的公钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述公钥对所述电子签名信息进行验签；和/或所述数字认证信息包括利用对称密钥计算得到的MAC值，所述认证因子包括计算所述MAC值的对称密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述对称密钥计算MAC校验值，验证所述MAC值和MAC校验值；和/或所述数字认证信息包括利用种子密钥生成的动态口令，所述认证因子包括所述验证所述动态口令的种子密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述种子密钥对所述动态口令进行验证。

[0018] 本发明另一方面还一种授权认证装置，包括：连接单元，在生物肢体进入授权认证装置的预设范围后，用于通过所述生物肢体与所述身份识别装置建立通信连接；接收单元，用于通过所述通信连接接收所述身份识别装置传输的待授权信息，所述待授权信息包括：数字认证信息；采集单元，在所述生物肢体进入授权认证装置的预设范围的持续时间内，用于采集所述生物肢体的生物特征信息；执行单元，用于获取对所述数字认证信息以及所述生物特征信息认证的认证结果，如果对所述数字认证信息以及所述生物特征信息认证的认证结果为认证通过，则执行授权操作。

[0019] 此外，所述生物特征信息包括：指纹信息和/或静脉信息；所述采集单元，在所述生物肢体与所述授权认证装置接触的情况下，用于采集所述生物肢体与所述授权认证装置的接触部位的所述生物特征信息。

[0020] 此外，所述执行单元，具体用于对所述数字认证信息以及所述生物特征信息进行认证，获得所述认证结果。

[0021] 此外，所述执行单元，具体用于向后台发送所述生物特征信息以及所述数字认证信息，并接收所述后台发送的所述认证结果，其中：所述认证结果为所述后台对所述数字认证信息以及所述生物特征信息进行认证，获得的认证结果。

[0022] 此外，所述待授权信息还包括：标识信息；所述对所述数字认证信息以及所述生物特征信息认证包括：根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证。

[0023] 此外，根据所述标识信息对所述数字认证信息以及所述生物特征信息进行认证包括：获取所述标识信息对应的认证因子和生物特征验证信息，并利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率，其中，所述认证结果为认证通过包括：在利用所述认证因子对所述数字认证信息进行数字认证通过且所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，所述认证结果为认证通过。

[0024] 此外，所述利用所述认证因子对所述数字认证信息进行数字认证以及检测所述生物特征验证信息与所述生物特征信息的匹配率包括：利用所述认证因子对所述数字认证信息进行认证，当对所述数字认证信息认证通过时，判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值；或判断所述生物特征信息与所述生物特征验证信息的匹配率是否大于预设值，当判断出所述生物特征信息与所述生物特征验证信息的匹配率大于预设值时，利用所述认证因子对所述数字认证信息进行认证。

[0025] 此外，所述数字认证信息包括利用私钥签名后获得的电子签名信息，所述认证因子包括对所述电子签名信息进行验签的公钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述公钥对所述电子签名信息进行验签；和/或所述数字认证信息包括利用对称密钥计算得到的MAC值，所述认证因子包括计算所述MAC值的对称密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述对称密钥计算MAC校验值，验证所述MAC值和MAC校验值；和/或所述数字认证信息包括利用种子密钥生成的动态口令，所述认证因子包括所述验证所述动态口令的种子密钥；所述利用所述认证因子对所述数字认证信息进行认证包括：利用所述种子密钥对所述动态口令进行验证。

[0026] 本发明又一方面还提供一种授权认证系统，包括：身份识别装置以及如权利要求9-16所述的授权认证装置；所述身份识别装置，用于通过所述通信连接向所述授权认证装置发送所述待授权信息。

[0027] 此外，所述系统还包括：后台，用于接收所述授权认证装置发送的所述生物特征信息以及所述数字认证信息，对所述数字认证信息以及所述生物特征信息进行认证，获得认证结果，并将所述认证结果发送至所述授权认证装置。

[0028] 由上述本发明提供的技术方案可以看出，本发明提供了一种授权认证方法、装置及系统，通过该授权认证方法可以验证腕表等电子设备的数字认证信息和人体的生物特征信息，保证了所验证的数字认证信息和生物特征信息的关联性和统一性，在本发明的授权认证方法中，对数字认证信息的验证和对人体生物特征信息的验证在一次连续的操作中完成，一旦分开两次进行则会导致验证的不成功，从而能够防止他人利用腕表等电子设备冒充用户通过授权，保证了信息和财产的安全。此外，本发明通过人体活体当作传输导体，可以有效地防止非法分子利用他人的电子设备和生物特征信息来通过授权。此外，使用本发明的授权认证方法，可以将用户需要使用的多种数字认证密钥信息均存储在腕表等随身携带的电子设备，电子设备自动将数字认证信息发送给认证端，用户只需采集生物特征信息即可完成被授权操作，方便快捷安全。

附图说明

[0029] 为了更清楚地说明本发明实施例的技术方案，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，对于本领域的普通技术人员来讲，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附图。

[0030] 图1为本发明实施例1提供的授权认证方法的流程图；

[0031] 图2为本发明实施例1提供的授权认证装置的结构示意图；

[0032] 图3为本发明实施例1提供的授权认证系统的结构示意图。

具体实施方式

[0033] 下面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，都属于本发明的保护范围。

[0034] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

[0035] 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“安装”、“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，可以是两个元件内部的连通。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。

[0036] 下面将结合附图对本发明实施例作进一步地详细描述。

[0037] 在本发明中利用生物肢体来进行通信，即利用生物肢体将通信的双方设备纳入到体域网范围内。所谓体域网(Body Area Network，简称BAN)就是以人体为中心，由和人体相关的网络元素(包括个人终端，分布在人身体上、衣物上、人体周围一定距离范围如3～5米内、甚至人身体内部的传感器、组网设备)等组成的通信网络，因此，只有和人体相关的网络元素进入通信设备的这个预设范围内，才能建立体域网的人体通信连接。

[0038] 实施例1

[0039] 本发明提供一种授权认证方法，如图1所示，包括：

[0040] 步骤S101，在生物肢体进入第一设备的预设范围后，第一设备通过生物肢体与第二设备建立通信连接。

[0041] 具体的实施方式中，第一设备具备生物特征采集功能，且能够与第二设备通过生物肢体进行通信的。第一设备可以用于对场所(办公区域、保密区域)、网站登录、个人物品(汽车、保险柜等)、危险物品等的进入或使用权限进行管理，第一设备也可以用于执行交易，例如可以是门禁读卡器、智能汽车锁、保险柜锁、危险物品管理器、带有生物识别功能的计算机、ATM机和POS机等。

[0042] 第二设备放置于活体(包括人体、动物体等)外部(佩戴在活体或者携带在活体周

边)或植入活体体内,例如,第二设备可以是可穿戴设备(智能腕表、智能眼镜等)、智能手机、植入活体内的传感设备等。当第二设备与生物肢体处于可通信范围内(例如佩戴在手腕、颈脖)时,第二设备与活体建立人体通信信道,生物肢体可以相当于第二设备的扩展天线,当检测方检测到生物肢体时,即相当于检测到该第二设备。

[0043] 第一设备在利用人体信道进行通信时,其具有预设的通信范围,当携带有第二设备的生物肢体进入到其通信范围时,第一设备可以检测到生物肢体,第二设备通过该生物肢体扩展的天线,也可以检测到第一设备。当然,上述第一设备和第二设备可以还支持其他的有线或者无线通信方式。

[0044] 在具体的实施方式中,第一设备与第二设备通过生物肢体建立体域网(Body Area Network,BAN),利用生物肢体建立活体通信信道,从而实现通过生物肢体来传输第一设备和第二设备之间的数据,实现利用活体进行通信。第一设备通过生物肢体与第二设备建立通信连接可以通过有线方式和无线方式,具体地,至少可以通过以下两种方式之一实现:

[0045] 有线方式:第一设备和第二设备均设有电极,第一设备与植入人体内或者佩戴在人体身上的第二设备的生物肢体接触(例如,佩戴有腕表的用户将手指接触POS机)时,将人体作为导体,双方的电极连通形成人体内的通路,该人体内的通路可以是简单线路方式,也可以电流耦合方式,从而实现有线方式的通信。此时第一设备需要与佩戴有第二设备的生物肢体接触,通过电平变化或者波导来传输信号,从而完成通信。

[0046] 无线方式:在无线方式中,第一设备和第二设备均可以检测周围的电场是否发送变化,如果通信对方进入到人体通信允许的范围内,就能检测到场强变化,与对方建立通信连接。

[0047] 此外,在通信的发起方面,可以由第一设备实时检测第二设备,在检测到第二设备后主动发起通信;也可以由第二设备来主动检测第一设备,从而主动发起通信。

[0048] 上述方式利用人体作为电信号的传输介质,实现体表、体内及人体周围(3～5米)的设备的信息交互。与传统的蓝牙、WIFI、射频和红外等无线通信技术相比,人体通信过程中信号经过人体传输,因而电磁噪声对其影响很小,具有低功耗、高保密性以及更低的人体损害等优点。此外由于不存在多人通信时效率降低的问题,也可免除有线通讯方式冗余的连线困扰。

[0049] 步骤S102,第一设备通过通信连接接收第二设备传输的待授权信息,待授权信息包括:数字认证信息。

[0050] 具体的实施方式中,第二设备可以是自己生成待传输的待授权信息后发送给第一设备,也可以由第二设备接收待授权信息生成装置发来的待授权信息后发送给第一设备。该待授权信息中包括有用于进行数字认证的信息,例如,该数字认证信息可以是利用私钥签名后获得的电子签名信息(当该电子签名信息由待授权信息生成装置生成时,此时该待授权信息生成装置可以是电子签名设备、USBkey等装置);该数字认证信息可以是利用对称密钥计算得到的MAC值(当该MAC值由待授权信息生成装置生成时,此时该待授权信息生成装置可以是密码机等装置);该数字认证信息可以是种子密钥生成的动态口令(当该动态口令由待授权信息生成装置生成时,此时该待授权信息生成装置可以是OTP等装置)。

[0051] 该待授权信息还可以包括代表第二设备的信息(如产品序列号等)、持有者身份信息、用户帐号等信息。

[0052] 当然，第二设备可以通过广播方式发送该待授权信息，也可以在接收到第一设备的授权请求信息后再向第二设备发送待授权信息。

[0053] 步骤S103，在生物肢体进入第一设备的预设范围的持续时间内，第一设备采集生物肢体的生物特征信息；具体的实施方式中，生物特征信息包括指纹信息、虹膜信息、人脸信息和静脉信息等信息。该第一设备设置有用于采集生物特征信息的模块，例如，指纹采集模块，用于在人体的手指进入到第一设备的预设通信范围内并且接触到第一设备的指纹采集模块时，采集该手指的指纹，又如，静脉采集模块，用于在人体的手腕进入到第一设备的预设通信范围内并且接触到静脉采集模块时，采集该手腕中的静脉信息，还比如，虹膜采集模块，用于在人眼进入到第一设备的预设通信范围内并且位于虹膜采集区域时，采集该人眼的虹膜信息，还比如，人脸识别模块，用于在人脸进入到第一设备的预设通信范围内并且位于人脸采集区域时，采集该人脸的人脸信息。

[0054] 在本发明的一个实施方式中，当生物特征信息为指纹信息和/或静脉信息时；第一设备采集生物肢体的生物特征信息包括：在生物肢体与第一设备接触的情况下，第一设备采集生物肢体与第一设备的接触部位的生物特征信息。

[0055] 具体来说，当生物特征信息为指纹信息或静脉信息时，第一设备需要接触用户的生物肢体才能采集到相应的生物特征信息，用户通过主动接触第一设备采集指纹或者静脉信息，避免了在人多拥挤场合其他用户不经意通过时造成的误通信，保证了通信的唯一性和安全性，同时表达了用户的真实意图和真实身份。

[0056] 第一设备采集生物肢体的生物特征信息这一动作可以在第一设备与第二设备建立通信的持续过程中完成，也可以在在第一设备和第二设备建立通信之前完成。只要保证采集生物肢体的生物特征信息与授权通信是在一次连续的操作中完成即可，从而保证发送的待授权信息和生物特征信息的一致性。

[0057] 需要注意的是，步骤103与步骤101和步骤102的执行不存在先后顺序，步骤103可以在步骤101之后步骤102之前执行，也可以与步骤102同时执行，还可以在步骤102之后执行。

[0058] 步骤S104，第一设备获取对数字认证信息以及生物特征信息认证的认证结果，如果对数字认证信息以及生物特征信息认证的认证结果为认证通过，则第一设备执行授权操作。具体的，当第一设备可以利用自身预存的信息对数字认证信息以及生物特征信息进行认证，也可以将数字认证信息以及生物特征信息发送给与之连接的后台，利用后台对数字认证信息以及生物特征信息进行认证。当获得认证通过的结果时，则第一设备执行相应的授权操作，如授权登录网站、授权打开门禁、授权打开某些设备(汽车、枪支等)。

[0059] 在本发明的具体实施方式中，第一设备获取对数字认证信息以及生物特征信息认证的认证结果可以通过但不限于以下方式完成：

[0060] 方式一、第一设备对数字认证信息以及生物特征信息进行认证，获得认证结果。具体来说，第一设备可以存储有与数字认证和生物特征相关的密钥以及其他信息，同时具备对数字认证信息以及生物特征信息进行认证的功能模块，可以自行完成整个认证过程，从而可以提高授权的效率，且由于第一设备可以独立完成授权，保证了授权的安全性。例如，当该第一设备是门禁卡读卡器、保险柜锁等设备时，由门禁卡读卡器、保险柜锁等自行完成认证功能，可以让持有有效授权信息的用户快速、安全、便捷地打开这些设备。

[0061] 方式二、第一设备向后台发送生物特征信息以及数字认证信息；第一设备接收后台发送的认证结果，其中：认证结果为后台对数字认证信息以及生物特征信息进行认证，获得的认证结果。具体来说，第一设备可以仅完成对生物特征信息的采集以及与第二设备的通信，而将认证的过程交由后台完成，后台具备更快的运算速度，可以快速完成复杂的运算。此外，将采集部分和认证部分分开放置，也可以保证系统的安全性。

[0062] 通过本发明的授权认证方法，可以验证腕表等电子设备的数字认证信息和人体的生物特征信息，保证了所验证的数字认证信息和生物特征信息的关联性和统一性，在本发明的授权认证方法中，对数字认证信息的验证和对人体生物特征信息的验证在一次连续的操作中完成，一旦分开两次进行则会导致验证的不成功，从而能够防止他人利用腕表等电子设备冒充用户通过授权，保证了信息和财产的安全。此外，本发明通过人体活体当作传输导体，可以有效地防止非法分子利用他人的电子设备和生物特征信息来通过授权。此外，使用本发明的授权认证方法，可以将用户需要使用的多种数字认证密钥信息均存储在腕表等随身携带的电子设备，电子设备自动将数字认证信息发送给认证端，用户只需采集生物特征信息即可完成被授权操作，方便快捷安全。

[0063] 在本发明的一个实施方式中，待授权信息还包括：标识信息；对数字认证信息以及生物特征信息认证包括：根据标识信息对数字认证信息以及生物特征信息进行认证。具体来说，第一设备在获取到第二设备发送来的待授权信息时，该待授权信息中还包括了用于指示获取对数字认证信息和生物特征信息进行认证的关键信息的标识信息，标识信息可以是序列号、名称、索引号等方式。通过标识信息可以快速获取到用于数字认证信息和生物特征信息认证的关键信息，提高认证的速度和效率。

[0064] 在本发明的一个实施方式中，根据标识信息对数字认证信息以及生物特征信息进行认证包括：获取标识信息对应的认证因子和生物特征验证信息，并利用认证因子对数字认证信息进行数字认证以及检测生物特征验证信息与生物特征信息的匹配率，其中，认证结果为认证通过包括：在利用认证因子对数字认证信息进行数字认证通过且生物特征信息与生物特征验证信息的匹配率大于预设值时，认证结果为认证通过。具体的，根据标识信息可以索引或者查快速地找出与数字认证信息对应的认证因子以及与生物特征信息对应的生物特征验证信息，例如，当数字认证信息为一个电子签名信息时，该标识信息可以是指示找到对应的用于验证签名的公钥，该公钥可以直接存放或者存放在数字证书中，该标识信息可以标识该公钥的编号或者数字证书的编号，从而使得要进行验证的设备可以从数据库中快速找到对应的公钥；当获取到的生物特征信息是指纹信息时，该标识信息可以是该指纹信息的编号或者持有该指纹信息的用户的编号，从而可以通过标识信息迅速准确地获取到对应的认证因子和生物特征验证信息。当对数字认证信息和生物特征信息进行认证的过程中，可以先对数字认证信息进行认证，也可以先对生物特征信息进行认证，也可以同时进行认证，只有当对两者的认证结果均为通过时，才确定认证结果为认证通过。

[0065] 目前对生物特征信息的验证方式主要是通过设定匹配率，判断采集到的生物特征信息与生物特征验证信息进行比对，当匹配率大于一定值时，则判断为验证通过。而由于现在生物识别技术的限制，设置高匹配率虽然可以确保结果的真实性，但是高匹配率往往经常会使得误将真实的用户判定为错误用户或识别失败从而拒绝授权，造成用户的操作不便。例如，现有技术中，检测生物特征验证信息与接收到的生物特征信息的匹配率大于特定

门限值(例如,99%、90%等)时,则认为对生物认证信息认证通过。为避免出现非法用户也通过认证的情况,现有技术中该特定门限值通常设置较高,此时容易出现合法用户无法识别而导致认证失败的问题。本申请为了降低合法用户认证失败的概率,所采取的预设值小于现有技术中的特定门限值,当检测所述生物特征验证信息与所述生物特征信息的匹配率大于预设值(例如,匹配率大于预设值但小于现有技术中的特定门限值)时,通过结合上述利用所述数字认证因子对所述待认证信息进行数字认证的结果来确定最终的认证结果。利用本发明的生物特征信息和数字认证信息双重验证,由于数字认证的强认证作用,可以将对生物特征认证的匹配率设置得比一般设备的生物特征认证匹配率低,从而降低了携带有真实生物特征的用户被误判为错误用户或识别失败的概率。

[0066] 在本发明的一个实施方式中,利用认证因子对数字认证信息进行数字认证以及检测生物特征验证信息与生物特征信息的匹配率包括:利用认证因子对数字认证信息进行认证,当对数字认证信息认证通过时,判断生物特征信息与生物特征验证信息的匹配率是否大于预设值;或判断生物特征信息与生物特征验证信息的匹配率是否大于预设值,当判断出生物特征信息与生物特征验证信息的匹配率大于预设值时,利用认证因子对数字认证信息进行认证。具体的,在对数字认证信息和生物特征信息进行认证的过程中,先对数字认证信息进行认证,可以通过强认证作用的数字认证的保证,来降低了真实合法的用户被识别失败的概率,且当数字认证没有通过时,无需再对生物特征信息进行验证,简化了流程;而当先对生物认证信息进行认证时,通过对生物特征信息验证,可以识别出假冒者,从而无需再进行后续的数字认证流程,简化了流程。

[0067] 在本发明的具体实施方式中,对数字认证信息的认证可以包括但不限于以下的一种或几种方式:

[0068] 方式一、数字认证信息包括利用私钥签名后获得的电子签名信息,认证因子包括对电子签名信息进行验签的公钥;利用认证因子对数字认证信息进行认证包括:利用公钥对电子签名信息进行验签;具体的,该方式中数字认证为电子签名认证,电子签名信息的生成方式可以采用私钥对预设值(如随机数等)进行签名,得到签名值,将签名值和预设值作为电子签名信息。通过电子签名认证可以确保该数字认证经过了用户的真实授权,且具有防止用户对执行过的操作反悔和抵赖的功能。

[0069] 方式二、数字认证信息包括利用对称密钥计算得到的MAC值,认证因子包括计算MAC值的对称密钥;利用认证因子对数字认证信息进行认证包括:利用对称密钥计算MAC校验值,验证MAC值和MAC校验值;具体的,该方式中数字认证为利用对称密钥对信息进行加密后,由验证方利用对称密钥对信息进行解密,例如采用对称算法(例如MAC计算)利用对称密钥对预设值进行加密得到密文值(例如MAC值),将密文值和预设值作为密文信息,通过该方式可以保证数据传输的安全性,提高通信的安全,同时还能通过双方预存的对称密钥来验证用户的身份。

[0070] 方式三、数字认证信息包括利用种子密钥生成的动态口令,认证因子包括验证动态口令的种子密钥;利用认证因子对数字认证信息进行认证包括:利用种子密钥对动态口令进行验证。具体的,该方式中利用动态口令来验证身份,可以基于时间或者基于挑战值生成的动态口令,通过该动态口令可以验证用户的真实身份,保证授权的安全性。

[0071] 本实施例还提供一种授权认证装置20,如图2所示。该授权认证装置20是授权认证

方法对应的装置，该授权认证装置20相当于授权认证方法中的第一设备，而身份识别装置30相当于授权认证方法中的第二设备。在此仅对该授权认证装置20的结构进行简单说明，其余未尽之处参照对授权认证方法的描述。该授权认证装置20包括：

[0072] 连接单元201，在生物肢体进入授权认证装置20的预设范围后，用于通过生物肢体与身份识别装置30建立通信连接；

[0073] 接收单元202，用于通过通信连接接收身份识别装置30传输的待授权信息，待授权信息包括：数字认证信息；

[0074] 采集单元203，在生物肢体进入授权认证装置20的预设范围的持续时间内，用于采集生物肢体的生物特征信息；

[0075] 执行单元204，用于获取对数字认证信息以及生物特征信息认证的认证结果，如果对数字认证信息以及生物特征信息认证的认证结果为认证通过，则执行授权操作。

[0076] 在本发明的一个实施方式中，生物特征信息包括：指纹信息和/或静脉信息；

[0077] 采集单元203，在生物肢体与授权认证装置20接触的情况下，用于采集生物肢体与授权认证装置20的接触部位的生物特征信息。

[0078] 在本发明的一个实施方式中，执行单元204获取对数字认证信息以及生物特征信息认证的认证结果可以通过但不限于以下两种方式完成：

[0079] 方式一、执行单元204，具体用于对数字认证信息以及生物特征信息进行认证，获得认证结果。

[0080] 方式二、执行单元204，具体用于向后台40发送生物特征信息以及数字认证信息，并接收后台发送的认证结果，其中：认证结果为后台40对数字认证信息以及生物特征信息进行认证，获得的认证结果。

[0081] 在本发明的一个实施方式中，待授权信息还包括：标识信息；对数字认证信息以及生物特征信息认证包括：根据标识信息对数字认证信息以及生物特征信息进行认证。

[0082] 在本发明的一个实施方式中，根据标识信息对数字认证信息以及生物特征信息进行认证包括：获取标识信息对应的认证因子和生物特征验证信息，并利用认证因子对数字认证信息进行数字认证以及检测生物特征验证信息与生物特征信息的匹配率，其中，认证结果为认证通过包括：在利用认证因子对数字认证信息进行数字认证通过且生物特征信息与生物特征验证信息的匹配率大于预设值时，认证结果为认证通过。

[0083] 在本发明的一个实施方式中，利用认证因子对数字认证信息进行数字认证以及检测生物特征验证信息与生物特征信息的匹配率包括：

[0084] 利用认证因子对数字认证信息进行认证，当对数字认证信息认证通过时，判断生物特征信息与生物特征验证信息的匹配率是否大于预设值；或

[0085] 判断生物特征信息与生物特征验证信息的匹配率是否大于预设值，当判断出生物特征信息与生物特征验证信息的匹配率大于预设值时，利用认证因子对数字认证信息进行认证。

[0086] 在本发明的一个实施方式中，对数字认证信息进行认证可以通过但不限于以下方式完成：

[0087] 方式一、数字认证信息包括利用私钥签名后获得的电子签名信息，认证因子包括对电子签名信息进行验签的公钥；利用认证因子对数字认证信息进行认证包括：利用公钥

对电子签名信息进行验签;和/或

[0088] 方式二、数字认证信息包括利用对称密钥计算得到的MAC值,认证因子包括计算MAC值的对称密钥;利用认证因子对数字认证信息进行认证包括:利用对称密钥计算MAC校验值,验证MAC值和MAC校验值;和/或

[0089] 方式三、数字认证信息包括利用种子密钥生成的动态口令,认证因子包括验证动态口令的种子密钥;利用认证因子对数字认证信息进行认证包括:利用种子密钥对动态口令进行验证。

[0090] 本实施例还提供一种授权认证系统,如图3所示,该授权认证系统包括前述的身份识别装置30以及前述的授权认证装置20;

[0091] 身份识别装置30,用于通过通信连接向授权认证装置20发送待授权信息。

[0092] 在本发明的一个实施方式中,授权认证系统还包括:后台40,用于接收授权认证装置20发送的生物特征信息以及数字认证信息,对数字认证信息以及生物特征信息进行认证,获得认证结果,并将认证结果发送至授权认证装置20。

[0093] 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。

[0094] 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。

[0095] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中,该程序在执行时,包括方法实施例的步骤之一或其组合。

[0096] 此外,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模块中,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模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。

[0097] 上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0098] 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。

[0099] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例

性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

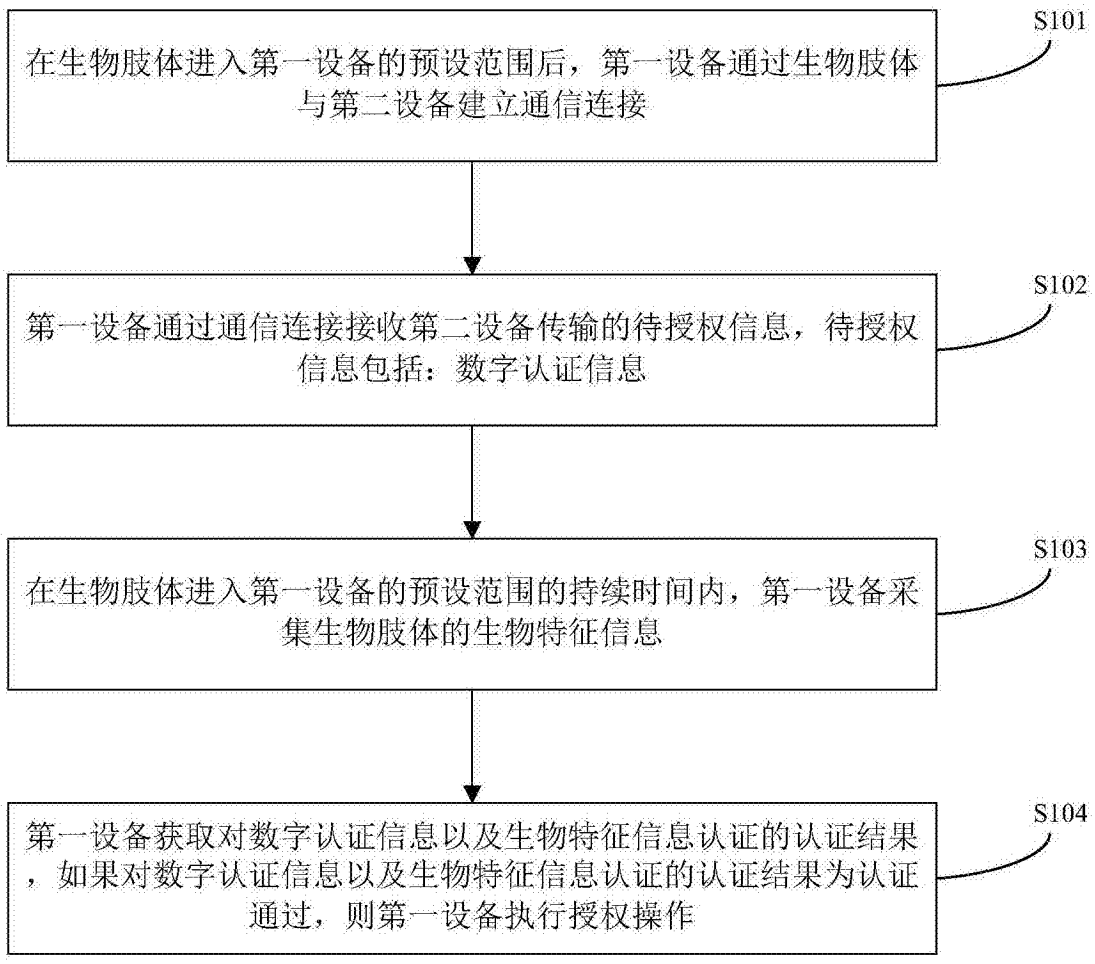

在生物肢体进入第一设备的预设范围后，第一设备通过生物肢体与第二设备建立通信连接
S101
第一设备通过通信连接接收第二设备传输的待授权信息，待授权信息包括：数字认证信息
S102
在生物肢体进入第一设备的预设范围的持续时间内，第一设备采集生物肢体的生物特征信息
S103
第一设备获取对数字认证信息以及生物特征信息认证的认证结果，如果对数字认证信息以及生物特征信息认证的认证结果为认证通过，则第一设备执行授权操作
S104

图1

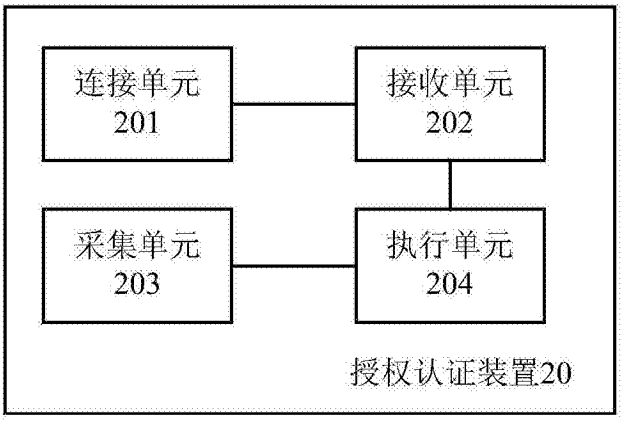

连接单元
201
接收单元
202
采集单元
203
执行单元
204
授权认证装置20

图2

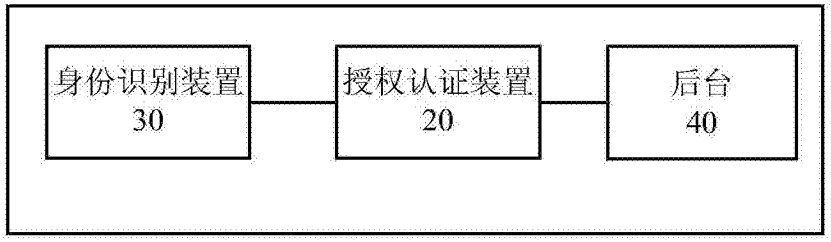


图3