(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 105938526 A
(43)申请公布日 2016.09.14

(21)申请号 201610127887.X

(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.
G06F 21/31(2013.01)
G06F 21/32(2013.01)
G06F 21/34(2013.01)

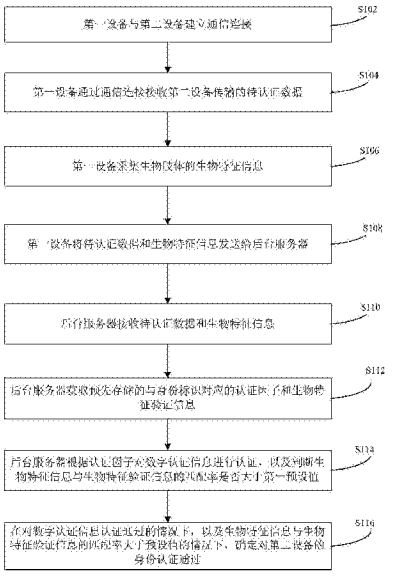
权利要求书2页 说明书12页 附图2页

(54)发明名称

一种身份认证方法及系统

(57)摘要

本发明提供了一种身份认证方法及系统。该方法包括：第一设备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认证数据；第一设备采集生物特征信息；第一设备将待认证数据和生物特征信息发送给后台服务器；后台服务器接收待认证数据和生物特征信息；后台服务器获取预先存储的与身份标识对应的认证因子和生物特征验证信息；后台服务器根据认证因子对数字认证信息进行认证，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第一预设值；在对数字认证信息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第一预设值的情况下，确定对第二设备的身份认证通过。



CN 105938526 A

1.一种身份认证方法,其特征在于,包括:

第一设备与所述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认证数据,其中,所述待认证数据包括:数字认证信息和身份标识;

所述第一设备采集生物特征信息;

所述第一设备将所述待认证数据和所述生物特征信息发送给后台服务器;

所述后台服务器接收所述待认证数据和所述生物特征信息;

所述后台服务器获取预先存储的与所述身份标识对应的认证因子和生物特征验证信息;

所述后台服务器根据所述认证因子对所述数字认证信息进行认证,以及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第一预设值;

在对所述数字认证信息认证通过的情况下,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所述第一预设值的情况下,确定对所述第二设备的身份认证通过。

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:在生物肢体与所述第一设备接触的情况下,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,所述第一设备通过所述通信连接接收所述第二设备传输的待认证数据,包括:

所述第一设备通过所述通信连接接收所述第二设备广播的所述待认证数据;或者

所述第一设备通过所述通信连接向所述第二设备发送认证请求;所述第一设备通过所述通信连接接收所述第二设备响应所述认证请求发送的所述待认证数据。

4.根据权利要求1至3任一项所述的方法,其特征在于,

所述数字认证信息包括:使用签名私钥对待签名数据进行数字签名得到的签名信息;所述认证因子包括:所述签名私钥对应的签名公钥;所述后台服务器根据所述认证因子对所述数字认证信息进行认证,包括:所述后台服务器利用所述签名公钥和所述待签名数据对所述数字认证信息进行验签;或者

所述数字认证信息包括:利用对称密钥对待加密信息进行加密得到的加密信息;所述认证因子包括:所述对称密钥;所述后台服务器根据所述认证因子对所述数字认证信息进行认证,包括:所述后台服务器利用所述对称密钥和所述待加密信息对所述加密信息进行认证;或者,

所述数字认证信息包括:动态口令;所述认证因子包括:对所述动态口令进行验证的种子密钥;所述后台服务器根据所述认证因子对所述数字认证信息进行认证,包括:所述后台服务器至少利用所述种子密钥对所述动态口令进行认证。

5.根据权利要求1至4任一项所述的方法,其特征在于,所述第一预设值小于第二预设值,其中,所述第二预设值用于指示两个生物特征信息为同一个生物特征信息的匹配率。

6.根据权利要求1至5任一项所述的方法,其特征在于,第一设备与所述第二设备建立通信连接,包括:

所述第一设备通过所述生物肢体与所述第二设备建立通信连接。

7.一种身份认证系统，其特征在于，包括：第一设备和后台服务器，其中，

所述第一设备，用于：

通过生物肢体与第二设备建立通信连接；

通过所述通信连接接收所述第二设备传输的待认证数据，其中，所述待认证数据包括：数字认证信息和身份标识；

采集所述生物肢体的生物特征信息；

所述第一设备将所述待认证数据和所述生物特征信息发送给所述后台服务器；

所述后台服务器，用于：

接收所述待认证数据和所述生物特征信息；

获取预先存储的与所述身份标识对应的认证因子和生物特征验证信息；

根据所述认证因子对所述数字认证信息进行认证，以及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；

在对所述数字认证信息认证通过的情况下，以及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所述预设值的情况下，确定对所述第二设备的身份认证通过。

8.根据权利要求7所述的系统，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；

所述第一设备通过以下方式采集所述生物肢体的生物特征信息：在所述生物肢体与所述第一设备接触的情况下，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。

9.根据权利要求7或8所述的系统，其特征在于，所述第一设备通过以下方式接收所述第二设备传输的待认证数据：

所述第一设备通过所述通信连接接收所述第二设备广播的所述待认证数据；或者，

所述第一设备通过所述通信连接向所述第二设备发送认证请求，通过所述通信连接接收所述第二设备响应所述认证请求发送的所述待认证数据。

10.根据权利要求7至9任一项所述的系统，其特征在于，

所述数字认证信息包括：使用签名私钥对待签名数据进行数字签名得到的签名信息；所述认证因子包括：所述签名私钥对应的签名公钥；所述后台服务器通过以下方式对所述数字认证信息进行认证：所述后台服务器利用所述签名公钥和所述待签名数据对所述数字认证信息进行验签；或者，

所述数字认证信息包括：利用对称密钥对待加密信息进行加密得到的加密信息；所述认证因子包括：所述对称密钥；所述后台服务器通过以下方式对所述数字认证信息进行认证：所述后台服务器利用所述对称密钥和所述待加密信息对所述加密信息进行认证；或者，

所述数字认证信息包括：动态口令；所述认证因子包括：对所述动态口令进行验证的种子密钥；所述后台服务器通过以下方式对所述数字认证信息进行认证：所述后台服务器至少利用所述种子密钥对所述动态口令进行认证。

11.根据权利要求7至10任一项所述的系统，其特征在于，第一设备通过以下方式与所述第二设备建立通信连接：

所述第一设备通过所述生物肢体与所述第二设备建立通信连接。

一种身份认证方法及系统

技术领域

[0001] 本发明涉及一种电子技术领域，尤其涉及一种身份认证方法及系统。

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)、个人物品(汽车、保险柜等)、危险物品(如枪支弹药等)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。

[0003] 另外，在现有技术中，由于不同的人某些生物特征相同的概率非常小，例如，指纹，因此，生物特征通常被用着用户的密码。在这种应用中，为了保护用户的安全，在验证生物特征信息时，将匹配率设置得比较高，以避免用户的账户被非法使用，但这种情况下，由于用户的生物特征在不同状态下采集出来的信息可能会有细微差别，例如，用户的指纹在指头干燥和湿润的情况下，同一指纹采集得到的指纹数据很可能不相同，从而可能出现即使是同一用户，在需要输入密码时，将真实的指纹认为是假指纹，从而拒绝用户的请求，需要用户再次输入，有的情况下，可能会导致用户需要无数次的输入，即真实合法的用户被识别失败的概率很高，降低了用户体验，在相关技术中，解决该问题的技术方案主要是优化指纹匹配算法，但这些方案的前提是采集的指纹数据完整、准确，对于采集的指纹数据与存储是采集的指纹数据不同情况，并不能起到很好的效果。

发明内容

[0004] 本发明旨在解决上述问题之一。

[0005] 本发明的主要目的在于提供一种身份认证方法。

[0006] 本发明的另一目的在于提供一种身份认证系统。

[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身份认证方法，包括：第一设备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认证数据，其中，待认证数据包括：数字认证信息和身份标识；第一设备采集生物特征信息；第一设备将待认证数据和生物特征信息发送给后台服务器；后台服务器接收待认证数据和生物特征信息；后台服务器获取预先存储的与身份标识对应的认证因子和生物特征验证信息；后台服务器根据认证因子对数字认证信息进行认证，以及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第一预设值；在对数字认证信息认证通过的情况下，且生物特征信息与生物特征验证信息的匹配率大于第一预设值的情况下，确定对第二设备的身份认证通过。

[0009] 可选地，生物特征信息包括：指纹信息和/或静脉信息；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，采集生物肢体与第一设备的接触部位的生物特征信息。

[0010] 可选地，第一设备通过通信连接接收第二设备传输的待认证数据，包括：第一设备通过通信连接接收第二设备广播的待认证数据；或者第一设备通过通信连接向第二设备发送认证请求；第一设备通过通信连接接收第二设备响应认证请求发送的待认证数据。

[0011] 可选地，数字认证信息包括：使用签名私钥对待签名数据进行数字签名得到的签名信息；认证因子包括：签名私钥对应的签名公钥；后台服务器根据认证因子对数字认证信息进行认证，包括：后台服务器利用签名公钥和待签名数据对数字认证信息进行验签；或者数字认证信息包括：利用对称密钥对待加密信息进行加密得到的加密信息；认证因子包括：对称密钥；后台服务器根据认证因子对数字认证信息进行认证，包括：后台服务器利用对称密钥和待加密信息对加密信息进行认证；或者，数字认证信息包括：动态口令；认证因子包括：对动态口令进行验证的种子密钥；后台服务器根据认证因子对数字认证信息进行认证，包括：后台服务器至少利用种子密钥对动态口令进行认证。

[0012] 可选地，第一预设值小于第二预设值，其中，第二预设值用于指示两个生物特征信息为同一个生物特征信息的匹配率。

[0013] 可选地，第一设备与第二设备建立通信连接，包括：第一设备通过生物肢体与第二设备建立通信连接。

[0014] 本发明另一方面提供了一种身份认证系统，包括：第一设备和后台服务器，其中，第一设备，用于：通过生物肢体与第二设备建立通信连接；通过通信连接接收第二设备传输的待认证数据，其中，待认证数据包括：数字认证信息和身份标识；采集生物肢体的生物特征信息；第一设备将待认证数据和生物特征信息发送给后台服务器；后台服务器，用于：接收待认证数据和生物特征信息；获取预先存储的与身份标识对应的认证因子和生物特征验证信息；根据认证因子对数字认证信息进行认证，以及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；在对数字认证信息认证通过的情况下，以及生物特征信息与生物特征验证信息的匹配率大于预设值的情况下，确定对第二设备的身份认证通过。

[0015] 可选地，生物特征信息包括：指纹信息和/或静脉信息；第一设备通过以下方式采集生物肢体的生物特征信息：在生物肢体与第一设备接触的情况下，采集生物肢体与第一设备的接触部位的生物特征信息。

[0016] 可选地，第一设备通过以下方式接收第二设备传输的待认证数据：第一设备通过通信连接接收第二设备广播的待认证数据；或者，第一设备通过通信连接向第二设备发送认证请求，通过通信连接接收第二设备响应认证请求发送的待认证数据。

[0017] 可选地，数字认证信息包括：使用签名私钥对待签名数据进行数字签名得到的签名信息；认证因子包括：签名私钥对应的签名公钥；后台服务器通过以下方式对数字认证信息进行认证：后台服务器利用签名公钥和待签名数据对数字认证信息进行验签；或者，数字认证信息包括：利用对称密钥对待加密信息进行加密得到的加密信息；认证因子包括：对称密钥；后台服务器通过以下方式对数字认证信息进行认证：后台服务器利用对称密钥和待加密信息对加密信息进行认证；或者，数字认证信息包括：动态口令；认证因子包括：对动态口令进行验证的种子密钥；后台服务器通过以下方式对数字认证信息进行认证：后台服务器至少利用种子密钥对动态口令进行认证。

[0018] 可选地，第一设备通过以下方式与第二设备建立通信连接：第一设备通过生物肢体与第二设备建立通信连接。

[0019] 由上述本发明提供的技术方案可以看出，本发明提供的身份认证方法中，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，并通过该通信连接发送的待认证数据，并且，在生物肢体进入第一设备的预设范围的持续时间内采集生物肢体的生物特征信息，对待认证数据和生物特征信息进行认证。通过本发明提供的技术方案，用户只需要将生物肢体接近第一设备一次，第一设备即可获得第二设备发送的待认证数据，以及用户的生物特征信息，简化了用户的操作，提高了用户体验。并且，在本发明提供的技术方案中，第一设备同时采用用户的生物特征信息作为认证信息，从而使得即使用户不小心将第二设备遗失，其他人也无法使用该用户的电子设备获得认证，进而保证了用户的财产及信息的安全，而且通过后台服务器对数字认证信息和生物特征信息的双重认证，可以降低真实合法的用户被识别失败的概率，提高了用户体验。

附图说明

[0020] 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。

[0021] 图1为本发明实施例1提供的身份认证方法的流程图；

[0022] 图2为本发明实施例2提供的身份认证系统的架构示意图。

具体实施方式

[0023] 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。

[0024] 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。

[0025] 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。

[0026] 下面将结合附图对本发明实施例作进一步地详细描述。

[0027] 实施例1

[0028] 本实施例提供了一种身份认证方法。

[0029] 图1是本实施例提供的身份认证方法的流程图，如图1所示，该方法主要包括以下

步骤S102至步骤S116。

[0030] 步骤S102,第一设备与第二设备建立通信连接。

[0031] 在本实施例中,第一设备可以通过无线或有线的方式连接,例如,NFC、蓝牙等。

[0032] 在本发明实施例的一个可选实施方案中,第一设备可以通过无线或有线的方式连接通过生物肢体与第二设备建立通信连接,即第一设备与第二设备通过人体通信(intra-body communication,IBC)建立通过链接,其中,生物肢体包括但不限于人体。例如,第一设备可以为POS机、支付宝应用等扫码终端、移动终端、PDA、台式机、笔记本、门禁等终端,第二设备可以为植入人体内或者佩戴在人体身上的装置,植入人体内的装置例如可以为植入人体内的血流传感器、脉搏传感器、体温传感器等传感器,佩戴在人体身上的装置例如可以是手环、腕表、项链、戒指、腰带等可穿戴在用户身上的电子设备。

[0033] 在本发明实施例的一个可选实施方案中,第一设备通过生物肢体与第一设备建立通信连接可以是第一设备检测到距第二设备的距离在预设范围内的生物肢体与第一设备接触,通过该生物肢体与第二设备建立通信连接。例如,检测到戴有手环的人体的手指触摸到第一设备,从而通过人体与手环建立通信连接。

[0034] 在本实施例中,第二设备可以穿戴用户的身体上或置入用户的体内上,或者装载在用户穿戴的衣物或配饰中,从而与第二设备通信连接,例如,戴在用户的手腕上,或者装在用户穿戴的衣服兜里,当用户需要登录网络、打开门禁、以及支付等需要进行身份认证的操作时,用户可以通过自己的肢体(例如手臂、脸)接近第一设备(即验证设备),当肢体接近第一设备一定距离(例如,几毫米)时,第一设备通过用户的肢体与第二设备建立通信连接。由于人体通信有一定的范围,比如3～5米,只有在人体进入第一设备的这个预设范围内,才能建立人体通信连接。

[0035] 作为本实施例中的一种可选实施方式,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,例如,第一设备与第二设备至少可以通过以下两种方式之一实现:

[0036] 有线方式:

[0037] 第一设备与第二设备均设有电极,在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(人体)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,即所谓的有线方式的通信连接。在该方式中,第一设备需要与佩戴有第二设备的人体接触。

[0038] 无线方式:

[0039] 在无线方式中,第一设备和第二设备(如POS机和腕表)均可以检测周围的电场是否发生变化,如果对方进入人体通信允许的范围内,就能检测到场强发生变化,与对方建立通信连接。具体地,以第二设备为例,第二设备佩戴或内置在人体内,利用第二设备的发射器的振荡让人体产生电场,当第二设备与第一设备的距离处于人体通信允许的范围内时,第一设备的接收器检测到电场的变化,与第二设备建立通信连接。在该方式中,第一设备不需要与佩戴有第二设备的人体接触。

[0040] 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。

[0041] 步骤S104，第一设备通过通信连接接收第二设备传输的待认证数据，其中，待认证数据包括：数字认证信息和身份标识。

[0042] 本实施例中，数字认证信息可以包括以下至少之一：签名信息、加密信息和动态口令。

[0043] 电子签名信息可以利用签名私钥(可以是第二设备的签名私钥，也可以是与第二设备连接的安全设备(例如，KEY)的私钥)对待签名数据进行数字签名得到的签名信息，在对该签名信息进行认证时，获取与上述签名私钥对应的签名公钥，利用该签名公钥对电子签名信息进行验签，如果验签通过，则认证通过。其中，待签名数据可以是上述的身份标识，也可以是第二设备或与第二设备连接的安全设备产生的随机数，在这种情况下，待认证数据中还可以包括第二设备产生的随机数，另外，待签名数据还可以为第一设备产生的随机数，在这种情况下，第一设备可以在与第二设备建立通信连接后，先向第二设备发送一个验证请求，该请求中携带第一设备产生的随机数，第二设备接收到该随机数后，再利用签名私钥对该随机数进行签名，得到上述签名信息，采用随机数作为待签名数据，可以预防重放攻击。在该可选实施方式中，数字认证信息为签名信息，从而使得在认证时可以确保第二设备的用户的身份。

[0044] 加密信息可以为第二设备利用与第一设备协商的对称密钥对待加密数据计算得到的MAC值，在对该加密信息进行认证时，同样利用该对称密钥对待加密数据计算得到验证MAC值，比较密文信息与验证MAC值，如果一致，则认证通过；或者，加密信息也可以为第二设备利用与第一设备协商的对称密钥对待加密数据得到的密文数据，在对该加密信息进行认证时，利用该对称密钥对密文数据进行解密，比较解密得到的信息与待加密数据是否一致，如果一致，则认证通过。

[0045] 动态口令可以为基于种子密钥生成的动态口令，在对该动态口令进行认证时，同样利用该种子密钥计算得到验证值，比较动态口令与验证值，如果一致，则认证通过，其中，动态口令可以是基于时间的，也可以是基于事件，还可以为动态挑战码，具体本实施例不作限定。

[0046] 在本实施例中，可以通过上述任一种实现对数字认证信息的认证，以保证第二设备的合法性。

[0047] 在上述实施方式中，第二设备可以自己计算上述数字认证信息，也可以与另一设备(例如，具有签名功能、加密功能、或动态口令功能的电子设备)进行交互以得到上述数据认证信息，具体本实施例不作限定。

[0048] 在本实施例一种可选的实施方式中，身份标识可以为第二设备的设备标识、用户ID等可以唯一标识用户身份的信息，通过身份标识可以唯一关联到第二用户用于认证数字认证信息的认证因子以及生物特征验证信息，以便对数字认证信息以及生物特征信息进行双重认证，由此，在双重认证通过后就可以确定生物特征信息以及数字认证信息都来自于同一用户，保证用户的合法性。

[0049] 在本实施例的一种可选实施方式中，第二设备可以在通信连接建立后，主动向第一设备发送上述的待认证数据，例如，可以在第二设备上设置一个开关，用户打开该开关之

后，第二设备开始广播上述待认证数据，在第一设备与第二设备建立通信连接后，第一设备接收第二设备广播的待认证数据，或者，第二设备也可以主动检测是否与第一设备建立通信连接，如果是，则主动向第一设备发送上述待认证数据。采用这种实施方式，可以简化流程，提高认证速度。

[0050] 在本发明实施例的另一个可选实施方式中，第二设备也可以是在接收到第一设备的请求后，发送上述待认证数据。在该可选实施方式中，第一设备可以在与第二设备建立通信连接之后，向第二设备发送认证请求，第二设备接收到该认证请求后，响应该认证请求，向第二设备发送该待认证数据。例如，在支付过程中，第一设备可以将交易信息携带在认证请求中发送给第二设备，第二设备接收到该认证请求后，响应该认证请求，向第一设备发送待认证数据，其中，第二设备可以在接收到交易信息后，从中提取关键信息，并显示该关键信息，在接收到用户确认之后，才向第一设备发送待认证请求，以保证交易的安全。另外，在该可选实施方式中，认证请求中还可以携带第一设备确定的待计算信息，例如，随机数等，第二设备在接收该认证请求后，可以对该待计算信息进行签名、加密或生成动态口令。

[0051] 步骤S106，第一设备采集生物肢体的生物特征信息。

[0052] 其中，生物特征信息包括以下至少之一：指纹信息、虹膜信息、人脸信息和静脉信息。本实施例中，第一设备在与第二设备近距离接触的生物肢体接近时，采集该生物肢体的生物特征信息，例如，在用户手指触摸POS机的触摸部件的短暂的时间内(如3秒)，，POS机的触摸部件采集指纹信息。又例如，在用户的腕表与支付宝支付终端(该支付终端具有拍照功能，可以用于采集人脸信息)建立人体通信连接的期间，通过支付终端采集人脸信息。

[0053] 在本步骤中，特别地，在生物特征信息包括：指纹信息和/或静脉信息的情况下，需要生物肢体与第一设备接触才能采集到生物特征信息，作为一种可选的实施方式，采集生物肢体的生物特征信息可以包括：在生物肢体与第一设备接触的情况下，采集生物肢体与第一设备的接触部位的生物特征信息。例如，用户的手指接触第一设备的指纹采集部，或用户的手腕接触第一设备的静脉信息采集部。通过该可选实施方式，由于用户的肢体需要与第一设备接触才能采集到生物特征信息，因此，可以保持本次认证是用户许可的，进而避免由于第一设备和第二设备不经意间接近而触发认证流程的情况。

[0054] 步骤S108，第一设备将待认证数据和生物特征信息发送给后台服务器。

[0055] 步骤S110，后台服务器接收待认证数据和生物特征信息。

[0056] 步骤S112，后台服务器获取预先存储的与身份标识对应的认证因子和生物特征验证信息。

[0057] 在本实施例中，后台服务器预先按照身份标识(可以是第二设备的，也可以是第二设备的用户的，还可以是与第二设备连接的安全设备(例如，KEY、动态口令牌等))存储该用户的认证因子和生物特征验证信息，例如，在第二设备或第二设备连接的安全设备注册时、或在将第二设备或第二设备连接的安全设备分配给用户时，具体本实施例不作限定。

[0058] 步骤S114，后台服务器根据认证因子对数字认证信息进行认证，以及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第一预设值。

[0059] 本实施例中，后台服务器根据认证标识信息获取认证因子和生物特征验证信息，并利用认证因子和生物特征验证信息对数字认证信息以及生物特征信息进行认证的认证结果。该认证因子和生物特征验证信息与认证标识信息唯一关联，因此根据认证标识信息

可以唯一查询到该用户对应的认证因子和生物特征验证信息，以便利用数字认证信息以及生物特征信息的双重认证通过后，可以保证用户的合法性。

[0060] 本步骤中，后台服务器利用认证因子对数字认证信息的认证的方式与根据数字认证信息的具体形式相关。例如，如果数字认证信息为使用签名私钥(可以是第二设备的私钥，也可以是与第二设备连接的安全设备(例如，KEY)的私钥)对待签名数据进行签名得到的签名信息，则认证因子为签名私钥对应的签名公钥，在认证数字认证信息时，利用签名公钥对待签名数据进行计算，得到验签值，将该验签值与接收到的签名信息进行比对，如果一致，则认证通过，否则，认证不通过。如果数字认证信息为利用对称密钥对待加密信息进行加密得到的加密信息，则认证因子为对称密钥，在对数字认证信息进行认证时，使用对称密钥对待加密信息进行加密，将加密得到的加密验证信息与接收到的加密信息进行比较，如果一致，则认证通过，否则认证不通过；或者，也可以利用对称密钥对接收到的加密信息进行解密，将解密得到的明文信息与待加密信息进行比较，如果一致，则认证通过，否则认证不通过。在数字认证信息为动态口令的情况下，认证因子为对动态口令进行验证的种子密钥，在对数字认证信息进行认证时，使用种子密钥生成动态口令，将生成的动态口令与接收到的动态口令进行比较，如果一致，则认证通过，否则，认证不通过。

[0061] 在本实施例中，衡量生物特征信息与生物特征验证信息的匹配率的第一预设值比实际应用中用于衡量两个生物特征信息是否为同一生物特征信息的匹配率(即第二预设值)。例如，假设在实际应用中，当两个指纹信息的匹配率达到99％(即两个指纹信息相同的比例)时，认为两个指纹信息为同一个指纹的指纹信息(即第二预设值为99％)，否则，认为两个指纹信息不是同一个指纹的指纹信息，而本实施例中的第一预设值可能为80％，即在本实施例中判断接收到的生物特征信息与生物特征验证信息的匹配率是否达到80％而不是99％。

[0062] 步骤S116，在对数字认证信息认证通过的情况下，以及生物特征信息与生物特征验证信息的匹配率大于预设值的情况下，确定对第二设备的身份认证通过。

[0063] 在本发明实施例的一个可选实施方案中，后台服务器还可以将认证结果返回给第一设备。另外，后台服务器也可以在对第二设备的身份认证通过后，执行后续的操作，例如，给予第二设备授权，打开门禁等，或者，在支付流程中，也可以执行支付流程，具体本实施例不作限定。

[0064] 在现有技术的生物特征信息认证技术中存在真实合法的用户被识别失败的概率和非法的用户被识别成功的概率，以指纹识别为例，很多时候，用户的指纹是真实的，但是后台系统识别错误，误将该用户的指纹识别为假指纹，从而不能通过认证，无法实现支付交易；而有的时候，非法用户的指纹明明是假的，但后台也认证通过了，给合法用户造成了经济上的损失，这些情况发生的概率都是很高的。而本实施例通过对数字认证信息和生物特征信息的双重认证可以规避“非法的用户被识别成功”的情况，而且可以降低真实合法的用户被识别失败发生的情况。首先，通过上述3种对数字认证信息的认证，可以确定该用户为合法用户，如果是非法用户则无法通过该数字认证，那么就不会出现对假指纹认证的操作，从而规避了“非法的用户被识别成功”的情况；其次，在保证用户为合法用户的情况下，后台可以将两个生物特征信息匹配的相似度降低，以降低真实合法的用户被识别失败的概率，例如，理论上两个生物特征信息要完全匹配，其相似度至少要达到99％(第二预设值)，而如

果后台发现其相似度仅为90%时，就会识别为不匹配，认证不通过，而出现将真的指纹识别为假指纹的情况，在本发明中，由于数字认证已经保证用户为合法用户，所以，可以将完全匹配的相似度降低为80%（第一预设值），也就是说，只要相似度达到80%（第一预设值）就认为匹配，因此，当两个生物特征信息的相似度为90%时，也可以通过认证，由此，就不会真实合法的用户被识别失败的情况了，从而降低了生物特征信息认证技术中真实合法的用户被识别失败的概率。

[0065] 通过本发明实施例提供的身份认证方法，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，并通过该通信连接发送的待认证数据，并且，在生物肢体进入第一设备的预设范围的持续时间内采集生物肢体的生物特征信息，将待认证数据和生物特征信息发送给后台服务器进行双重认证。通过本发明提供的技术方案，用户只需要将生物肢体接近第一设备一次，第一设备即可获得第二设备发送的待认证数据，以及用户的生物特征信息，简化了用户的操作，提高了用户体验。并且，在本发明提供的技术方案中，第一设备同时采用用户的生物特征信息作为认证信息，从而使得即使用户不小心将第二设备遗失，其他人也无法使用该用户的电子设备获得认证，进而保证了用户的财产及信息的安全，而且通过后台服务器对数字认证信息和生物特征信息的双重认证，可以降低真实合法的用户被识别失败的概率，提高了用户体验。

[0066] 实施例2

[0067] 本实施例提供了一种身份认证系统，该系统可以用于实现实施例1的方法。

[0068] 图2为本实施例提供的身份认证系统的架构示意图，如图2所示，该系统主要包括：第一设备100和后台服务器200。

[0069] 在本实施例中，第一设备100，用于：与第二设备建立通信连接；通过通信连接接收第二设备传输的待认证数据，其中，待认证数据包括：数字认证信息和身份标识；在生物肢体进入第一设备100的预设范围内，采集生物肢体的生物特征信息；第一设备100将待认证数据和生物特征信息发送给后台服务器200；

[0070] 后台服务器200，用于：接收待认证数据和生物特征信息；获取预先存储的与身份标识对应的认证因子和生物特征验证信息；根据认证因子对数字认证信息进行认证，以及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第一预设值；在对数字认证信息认证通过的情况下，以及生物特征信息与生物特征验证信息的匹配率大于预设值的情况下，确定对第二设备的身份认证通过。

[0071] 在本发明实施例的一个可选实施方案中，第一设备100可以通过生物肢体与第二设备建立通信连接，例如，第一设备100可以为POS机、支付宝应用等扫码终端、移动终端、PDA、台式机、笔记本、门禁等终端，第二设备可以为植入人体内或者佩戴在人体身上的装置，植入人体内的装置例如可以为植入人体内的血流传感器、脉搏传感器、体温传感器等传感器，佩戴在人体身上的装置例如可以是手环、腕表、项链、戒指、腰带等可穿戴在用户身上的电子设备。

[0072] 在本发明实施例的一个可选实施方案中，第一设备100通过生物肢体与第一设备100建立通信连接可以是第一设备100检测到距第二设备的距离在预设范围内的生物肢体与第一设备100接触，通过该生物肢体与第二设备建立通信连接。例如，检测到戴有手环的人体的手指触摸到第一设备100，从而通过人体与手环建立通信连接。

[0073] 在本实施例中，第二设备可以穿戴用户的身体上或置入用户的体内上，或者装载在用户穿戴的衣物或配饰中，从而与第二设备通信连接，例如，戴在用户的手腕上，或者装在用户穿戴的衣服兜里，当用户需要登录网络、打开门禁、以及支付等需要进行身份认证的操作时，用户可以通过自己的肢体(例如手臂、脸)接近第一设备100(即验证设备)，当肢体接近第一设备100一定距离(例如，几毫米)时，第一设备100通过用户的肢体与第二设备建立通信连接。由于人体通信有一定的范围，比如3～5米，只有在人体进入第一设备100的这个预设范围内，才能建立人体通信连接。

[0074] 作为本实施例中的一种可选实施方式，第一设备100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，例如，第一设备100与第二设备至少可以通过以下两种方式之一实现：

[0075] 有线方式：

[0076] 第一设备100与第二设备均设有电极，在第一设备100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(人体)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，即所谓的有线方式的通信连接。在该方式中，第一设备100需要与佩戴有第二设备的人体接触。

[0077] 无线方式：

[0078] 在无线方式中，第一设备100和第二设备(如POS机和腕表)均可以检测周围的电场是否发生变化，如果对方进入人体通信允许的范围内，就能检测到场强发生变化，与对方建立通信连接。具体地，以第二设备为例，第二设备佩戴或内置在人体内，利用第二设备的发射器的振荡让人体产生电场，当第二设备与第一设备100的距离处于人体通信允许的范围内时，第一设备100的接收器检测到电场的变化，与第二设备建立通信连接。在该方式中，第一设备100不需要与佩戴有第二设备的人体接触。

[0079] 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。

[0080] 在本实施例一种可选的实施方式中，身份标识可以为第二设备的设备标识、用户ID等可以唯一标识用户身份的信息，通过身份标识可以唯一关联到第二用户用于认证数字认证信息的认证因子以及生物特征验证信息，以便对数字认证信息以及生物特征信息进行双重认证，由此，在双重认证通过后就可以确定生物特征信息以及数字认证信息都来自于同一用户，保证用户的合法性。

[0081] 在本实施例的一种可选实施方式中，第二设备可以在通信连接建立后，主动向第一设备100发送上述的待认证数据，在该可选实施方式中，第一设备100通过以下方式接收第二设备传输的待认证数据：第一设备100通过通信连接接收第二设备广播的待认证数据。例如，可以在第二设备上设置一个开关，用户打开该开关之后，第二设备开始广播上述待认证数据，在第一设备100与第二设备建立通信连接后，第一设备100接收第二设备广播的待认证数据，或者，第二设备也可以主动检测是否与第一设备100建立通信连接，如果是，则主动向第一设备100发送上述待认证数据。采用这种实施方式，可以简化流程，提高认证速度。

[0082] 在本发明实施例的另一个可选实施方式中，第二设备也可以是在接收到第一设备100的请求后，发送上述待认证数据。在该可选实施方式中，第一设备100通过以下方式接收第二设备传输的待认证数据：第一设备100通过通信连接向第二设备发送认证请求，通过通信连接接收第二设备响应认证请求发送的待认证数据。例如，在支付过程中，第一设备100可以将交易信息携带在认证请求中发送给第二设备，第二设备接收到该认证请求后，响应该认证请求，向第一设备100发送待认证数据，其中，第二设备可以在接收到交易信息后，从中提取关键信息，并显示该关键信息，在接收到用户确认之后，才向第一设备100发送待认证请求，以保证交易的安全。另外，在该可选实施方式中，认证请求中还可以携带第一设备100确定的待计算信息，例如，随机数等，第二设备在接收该认证请求后，可以对该待计算信息进行签名、加密或生成动态口令。

[0083] 其中，生物特征信息包括以下至少之一：指纹信息、虹膜信息、人脸信息和静脉信息。本实施例中，第一设备100在与第二设备近距离接触的生物肢体接近时，采集该生物肢体的生物特征信息，例如，在用户手指触摸POS机的触摸部件的短暂的时间内(如3秒)，该触摸时间内，POS机的触摸部件采集指纹信息。又例如，在用户的腕表与支付宝支付终端(该支付终端具有拍照功能，可以用于采集人脸信息)接近一定距离时，通过支付终端采集人脸信息。

[0084] 在本发明实施例的一个可选实施方案中，生物特征信息包括：指纹信息和/或静脉信息；在该可选实施方案中，第一设备100通过以下方式采集生物肢体的生物特征信息：在生物肢体与第一设备100接触的情况下，采集生物肢体与第一设备100的接触部位的生物特征信息。例如，用户的手指接触第一设备100的指纹采集部，或用户的手腕接触第一设备100的静脉信息采集部。通过该可选实施方式，由于用户的肢体需要与第一设备100接触才能采集到生物特征信息，因此，可以保持本次认证是用户许可的，进而避免由于第一设备100和第二设备不经意间接近而触发认证流程的情况。

[0085] 在本实施例中，后台服务器200预先按照身份标识(可以是第二设备的，也可以是第二设备的用户的，还可以是与第二设备连接的安全设备(例如，KEY、动态口令牌等))存储该用户的认证因子和生物特征验证信息，例如，在第二设备或第二设备连接的安全设备注册时、或在将第二设备或第二设备连接的安全设备分配给用户时，具体本实施例不作限定。

[0086] 本实施例中，后台服务器200根据认证标识信息获取认证因子和生物特征验证信息，并利用认证因子和生物特征验证信息对数字认证信息以及生物特征信息进行认证的认证结果。该认证因子和生物特征验证信息与认证标识信息唯一关联，因此根据认证标识信息可以唯一查询到该用户对应的认证因子和生物特征验证信息，以便利用数字认证信息以及生物特征信息的双重认证通过后，可以保证用户的合法性。

[0087] 在本发明实施例的一个可选实施方案中，数字认证信息包括：使用签名私钥对待签名数据进行数字签名得到的签名信息；认证因子包括：签名私钥对应的签名公钥；后台服务器200通过以下方式对数字认证信息进行认证：后台服务器200利用签名公钥和待签名数据对数字认证信息进行验签；即在认证数字认证信息时，后台服务器200利用签名公钥对待签名数据进行计算，得到验签值，将该验签值与接收到的签名信息进行比对，如果一致，则认证通过，否则，认证不通过。

[0088] 在本发明实施例的另一个可选实施方案中，数字认证信息包括：利用对称密钥对

待加密信息进行加密得到的加密信息；认证因子包括：对称密钥；后台服务器200通过以下方式对数字认证信息进行认证：后台服务器200利用对称密钥和待加密信息对加密信息进行认证；即后台服务器200在对数字认证信息进行认证时，使用对称密钥对待加密信息进行加密，将加密得到的加密验证信息与接收到的加密信息进行比较，如果一致，则认证通过，否则认证不通过；或者，也可以利用对称密钥对接收到的加密信息进行解密，将解密得到的明文信息与待加密信息进行比较，如果一致，则认证通过，否则认证不通过

[0089] 在本发明实施例的又一个可选实施方案中，数字认证信息包括：动态口令；认证因子包括：对动态口令进行验证的种子密钥；后台服务器200通过以下方式对数字认证信息进行认证：后台服务器200至少利用种子密钥对动态口令进行认证。即后台服务器200在对数字认证信息进行认证时，使用种子密钥生成动态口令，将生成的动态口令与接收到的动态口令进行比较，如果一致，则认证通过，否则，认证不通过。

[0090] 在本实施例中，衡量生物特征信息与生物特征验证信息的匹配率的第一预设值比实际应用中用于衡量两个生物特征信息是否为同一生物特征信息的匹配率(即第二预设值)。例如，假设在实际应用中，当两个指纹信息的匹配率达到99％(即两个指纹信息相同的比例)时，认为两个指纹信息为同一个指纹的指纹信息(即第二预设值为99％)，否则，认为两个指纹信息不是同一个指纹的指纹信息，而本实施例中的第一预设值可能为80％，即在本实施例中判断接收到的生物特征信息与生物特征验证信息的匹配率是否达到80％而不是99％。

[0091] 在现有技术的生物特征信息认证技术中存在真实合法的用户被识别失败的概率和非法的用户被识别成功的概率，以指纹识别为例，很多时候，用户的指纹是真实的，但是后台系统识别错误，误将该用户的指纹识别为假指纹，从而不能通过认证，无法实现支付交易；而有的时候，非法用户的指纹明明是假的，但后台也认证通过了，给合法用户造成了经济上的损失，这些情况发生的概率都是很高的。而本实施例通过对数字认证信息和生物特征信息的双重认证可以规避“非法的用户被识别成功”的情况，而且可以降低真实合法的用户被识别失败发生的情况。首先，通过上述对数字认证信息的认证，可以确定该用户为合法用户，如果是非法用户则无法通过该数字认证，那么就不会出现对假指纹认证的操作，从而规避了“非法的用户被识别成功”的情况；其次，在保证用户为合法用户的情况下，后台可以将两个生物特征信息匹配的相似度降低，以降低真实合法的用户被识别失败的概率，例如，理论上两个生物特征信息要完全匹配，其相似度至少要达到99％(第二预设值)，而如果后台发现其相似度仅为90％时，就会识别为不匹配，认证不通过，而出现将真的指纹识别为假指纹的情况，在本发明中，由于数字认证已经保证用户为合法用户，所以，可以将完全匹配的相似度降低为80％(第一预设值)，也就是说，只要相似度达到80％(第一预设值)就认为匹配，因此，当两个生物特征信息的相似度为90％时，也可以通过认证，由此，就不会真实合法的用户被识别失败的情况了，从而降低了生物特征信息认证技术中真实合法的用户被识别失败的概率。

[0092] 通过本发明实施例提供的身份认证系统，在生物肢体进入第一设备100的预设范围后，第一设备100通过生物肢体与第二设备建立通信连接，并通过该通信连接发送的待认证数据，并且，在生物肢体进入第一设备100的预设范围的持续时间内采集生物肢体的生物特征信息，将待认证数据和生物特征信息发送给后台服务器200进行双重认证。通过本发明

提供的技术方案，用户只需要将生物肢体接近第一设备100一次，第一设备100即可获得第二设备发送的待认证数据，以及用户的生物特征信息，简化了用户的操作，提高了用户体验。并且，在本发明提供的技术方案中，第一设备100同时采用用户的生物特征信息作为认证信息，从而使得即使用户不小心将第二设备遗失，其他人也无法使用该用户的电子设备获得认证，进而保证了用户的财产及信息的安全，而且通过后台服务器200对数字认证信息和生物特征信息的双重认证，可以降低真实合法的用户被识别失败的概率，提高了用户体验。

[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。

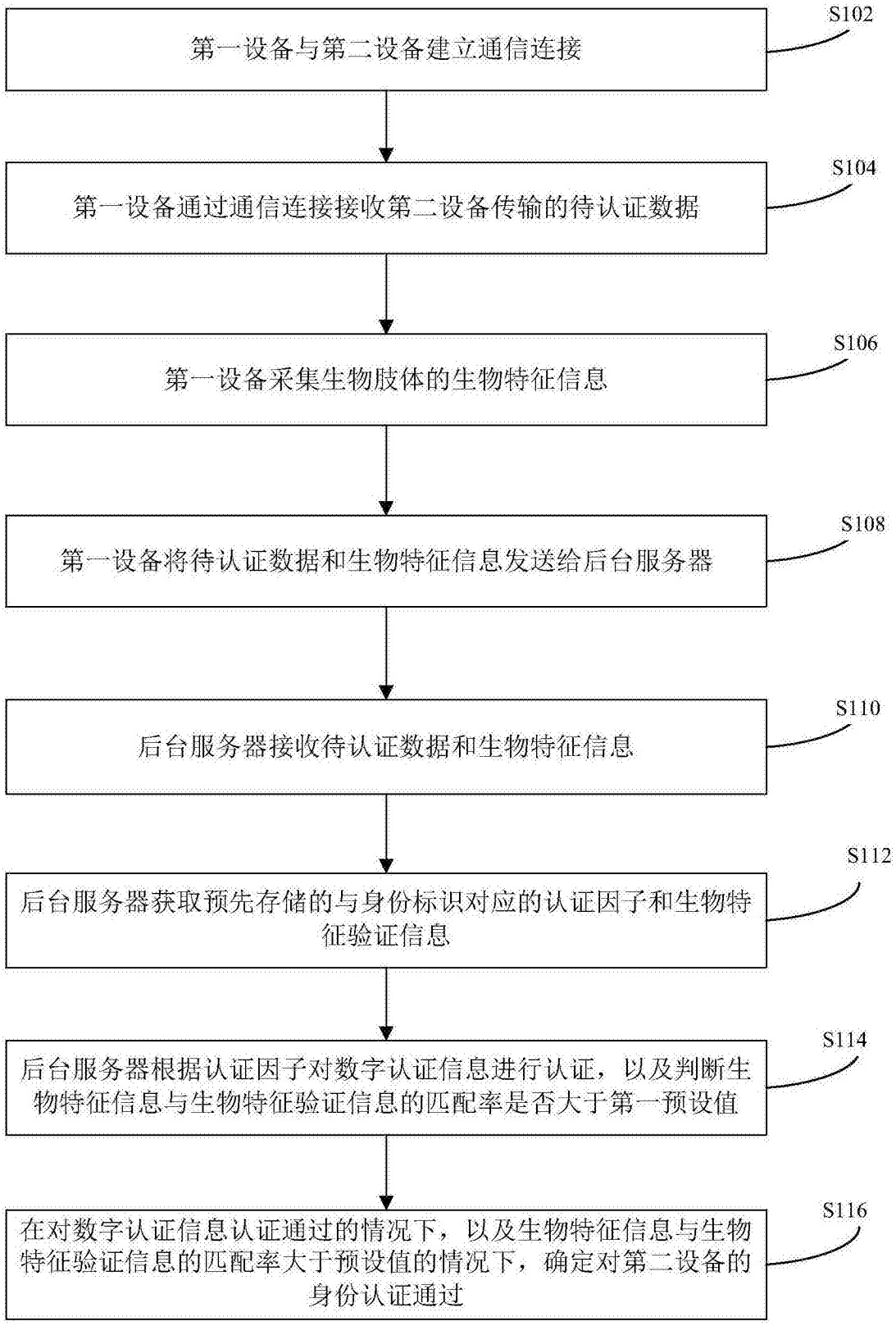

S102
第一设备与第二设备建立通信连接
S104
第一设备通过通信连接接收第二设备传输的待认证数据
S106
第一设备采集生物肢体的生物特征信息
S108
第一设备将待认证数据和生物特征信息发送给后台服务器
S110
后台服务器接收待认证数据和生物特征信息
S112
后台服务器获取预先存储的与身份标识对应的认证因子和生物特征验证信息
S114
后台服务器根据认证因子对数字认证信息进行认证，以及判断生物特征信息与生物特征验证信息的匹配率是否大于第一预设值
S116
在对数字认证信息认证通过的情况下，以及生物特征信息与生物特征验证信息的匹配率大于预设值的情况下，确定对第二设备的身份认证通过

图1

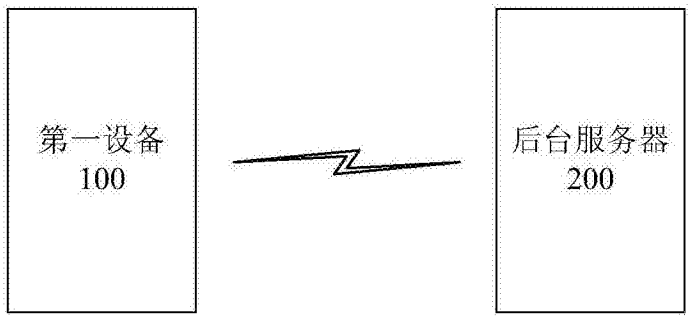


图2