



# (12)发明专利申请

(10)申请公布号 CN 105989496 A

(43)申请公布日 2016. 10. 05

(21)申请号 201610127266.1

(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.

G06Q 20/40(2012.01)

G06Q 20/38(2012.01)

G06Q 20/20(2012.01)

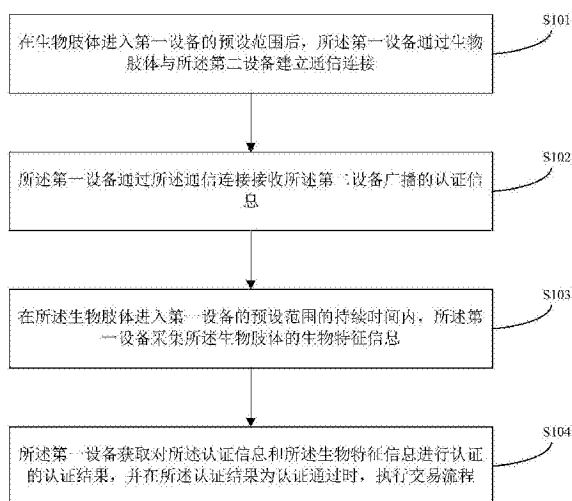
权利要求书1页 说明书6页 附图1页

## (54)发明名称

一种交易方法及设备

## (57)摘要

本发明提供一种交易方法及设备,该方法包括: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广播的认证信息;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;第一设备获取对认证信息和生物特征信息进行认证的认证结果,并在认证结果为认证通过时,执行交易流程。



1. 一种交易方法,其特征在于,包括:

在生物肢体进入第一设备的预设范围后,所述第一设备通过生物肢体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广播的认证信息;

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认证信息和所述生物特征信息进行认证的认证结果,并在所述认证结果为认证通过时,执行交易流程。

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:在通过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所述的方法,其特征在于,

所述认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

4. 一种交易设备,其特征在于,包括:

第一通信模块,用于在生物肢体进入第一设备的预设范围后,所述第一设备通过生物肢体与所述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广播的认证信息;

采集模块,用于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;

第二通信模块,用于获取对所述认证信息和所述生物特征信息进行认证的认证结果,并在所述认证结果为认证通过时,执行交易流程。

5. 根据权利要求4所述的交易设备,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;

所述采集模块,具体用于在通过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。

6. 根据权利要求4所述的交易设备,其特征在于,所述认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

## 一种交易方法及设备

### 技术领域

[0001] 本发明涉及一种支付领域,尤其涉及一种交易方法及设备。

### 背景技术

[0002] 电子支付相比现金支付,具有安全、快捷、可靠等优势。POS机作为一种支付终端,被广泛地运用于电子支付中。现有的POS机有的是通过读卡器读取银行卡的持卡人磁条信息,由POS机操作人员输入交易金额,持卡人在POS机上刷银行卡,然后再输入密码,POS机把这些信息上传给银行后台,完成联机交易。由此可见,在现有的电子支付流程中,用户需要执行两次操作,第一次将银行卡放到POS机上与POS机建立连接,第二次用户需要输入密码,操作流程复杂。

### 发明内容

[0003] 本发明旨在解决上述问题。

[0004] 本发明的主要目的在于提供一种交易方法;

[0005] 本发明的另一目的在于提供一种交易设备。

[0006] 为达到上述目的,本发明的技术方案具体是这样实现的:

[0007] 本发明一方面提供了一种交易方法,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广播的认证信息;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;第一设备获取对认证信息和生物特征信息进行认证的认证结果,并在认证结果为认证通过时,执行交易流程。

[0008] 其中,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:在通过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。

[0009] 其中,认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

[0010] 本发明另一方面提供了一种交易设备,包括:第一通信模块,用于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;通过通信连接接收第二设备广播的认证信息;采集模块,用于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;第二通信模块,用于获取对认证信息和生物特征信息进行认证的认证结果,并在认证结果为认证通过时,执行交易流程。

[0011] 其中,生物特征信息包括:指纹信息和/或静脉信息;采集模块,具体用于在通过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。

[0012] 其中,认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

[0013] 由上述本发明提供的技术方案可以看出,在生物肢体进入第一设备的预设范围

后,例如,生物肢体为用户的手部时,用户通过一次操作(该操作可以是接触第一设备或者靠近第一设备),第一设备可以获取第二设备的认证信息和采集到生物特征信息,简化操作次数,降低了方案实现的复杂度。

### 附图说明

[0014] 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。

[0015] 图1为本发明实施例1提供的交易方法的流程图;

[0016] 图2为本发明实施例1提供的交易设备结构示意图。

### 具体实施方式

[0017] 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。

[0018] 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。

[0019] 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,可以根据具体情况理解上述术语在本发明中的具体含义。

[0020] 下面将结合附图对本发明实施例作进一步地详细描述。

[0021] 实施例1

[0022] 本实施例提供一种交易方法,如图1所示,该方法包括:

[0023] 101、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。

[0024] 生物肢体,例如可以为人体上的肢体,例如手部、手腕、眼部、面部等;

[0025] 第一设备,例如可以是支付设备,包括POS机、ATM等;

[0026] 第二设备,例如可以是智能腕表、智能眼镜、智能手环等可穿戴设备,可以佩戴(可以紧贴生物表皮或者与生物表皮未贴合)在生物肢体上,或者可植入生物体内。

[0027] 第一设备的预设范围是指第一设备的有效通信范围,生物肢体进入第一设备的预设范围后可以被第一设备检测到。

[0028] 第一设备采用BAN(体域网)技术通过生物肢体与第二设备建立通信连接的实现方式如下:例如,佩戴有第二设备的生物肢体进入第一设备的预设范围,并接触第一设备,使得第一设备通过生物肢体与第二设备之间形成通信通路,从而实现建立通信连接,此时生物肢体相当于有线导体。或者又如,佩戴有第二设备的生物肢体进入第一设备的预设范围,靠近第一设备,第一设备检测到第二设备通过生物肢体产生的电场变化时,实现建立通信连接,当然,也可以是第二设备通过生物肢体检测到第一设备的电场变化时,实现建立通信连接,此时生物肢体相当于第二设备的外接天线。

[0029] 本实施例中,利用生物肢体作为数据信号的传输介质,可以实现两个设备通过生物肢体(例如人体)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,外界噪声对其影响很小,功耗低、保密性较高等优点。

[0030] 102、第一设备通过通信连接接收第二设备广播的认证信息;

[0031] 第二设备按照预设周期产生广播信号,,或者第二设备检测到第一设备的电场变化后,该广播信号携带有认证信息,基于BAN技术该广播信号可以耦合进入生物肢体,通过生物肢体对外进行广播。当第一设备和第二设备通过生物肢体建立通信连接后,第一设备可以接收到第二设备通过生物肢体广播的认证信息。

[0032] 其中,认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

[0033] 认证信息可以是第二设备自身生成的,例如电子签名信息的生成方式例如由第二设备采用第二设备的私钥对预设值进行签名,得到签名值,将签名值和预设值作为电子签名信息;密文信息的生成方式例如由第二设备采用对称算法(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;动态口令的生成方式例如是第二设备基于时间或者基于挑战值生成的动态口令。

[0034] 或者,认证信息还可以是第二设备从认证设备接收到的,例如与第二设备关联的认证工具(例如KEY)生成认证信息,并通过有线方式(usb或者音频接头)或者无线网络(例如WIFI、蓝牙、红外、NFC)将认证信息发送给第二设备。与第二设备关联的电子签名工具生成认证信息方式可以和第二设备生成认证信息方式相同,在此不再赘述。

[0035] 103、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;

[0036] 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。

[0037] 该第一设备设置有用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范围内并且位于人脸采集区域时,采集该人脸的人脸信息。

[0038] 其中,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的实现如下:在通过生物肢体与第二设备建立通信连接的持续期间且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。

[0039] 上述步骤101-102和步骤103的实现是通过用户一次接触第一设备或者一次靠近第一设备触发完成。例如,佩戴有第二设备(例如腕表)的用户手部接触到第一设备的采集生物特征信息的模块时,或者进入但未接触到第一设备的采集生物特征信息的模块的采集区域时,第一设备通过生物肢体(用户手部)接收第二设备广播的认证信息,并同时采集到生物肢体的生物特征信息。

[0040] 本实施例中通过用户的一次接触操作或者靠近操作就可以同时获取第二设备的认证信息和生物特征信息,可以简化用户操作,降低方案实现的复杂度。

[0041] 步骤101-102和步骤103在执行时没有前后次序之分,例如,步骤101和102可以在步骤103之前,或者也可以在步骤103之后,或者同时进行。

[0042] 104、第一设备获取对认证信息和生物特征信息进行认证的认证结果,并在认证结果为认证通过时,执行交易流程。

[0043] 第一设备获取到认证结果后,如果认证结果为认证通过,说明第二设备是合法的且该生物特征信息所属用户是第二设备的合法拥有者,也就是该生物特征信息所属用户使用的第二设备是自己拥有的合法设备,则执行交易流程。例如,在小额免密支付时,佩戴有腕表(第二设备)的用户手部通过一次触摸POS机(第一设备),POS机通过用户手部与腕表建立通信连接,POS机接收到腕表发送的认证信息且POS机采集到用户手部的指纹或者静脉信息,POS机获取对认证信息和用户手部的指纹或者静脉信息的认证结果。通过对认证信息进行验证确定第二设备为合法设备,通过对用户手部的指纹或者静脉信息进行验证确定该用户为第二设备的合法拥有者,认证结果通过,也就是说,可以验证得出该用户使用的是自己拥有的合法设备,之后执行交易流程,例如,小额支付操作,转账操作等。

[0044] 对认证信息和生物特征信息进行认证的操作可以是第一设备执行,或者由第一设备将认证信息和生物特征信息发送给后台,由后台对认证信息和生物特征信息进行认证。

[0045] 本实施例中,在生物肢体进入第一设备的预设范围后,例如,生物肢体为用户的手部时,用户通过一次操作(该操作可以是接触第一设备或者靠近第一设备),第一设备可以获取第二设备的认证信息和采集到生物特征信息,简化操作次数,降低了方案实现的复杂度。

[0046] 另外,通过获取对认证信息进行验证且对生物特征信息进行验证的认证结果,可以确定使用第二设备的用户真实合法性以及第二设备的真实合法性。如果对认证信息进行验证通过说明第二设备为合法设备,如果对生物特征信息进行验证通过说明该生物特征信息所属用户为第二设备的合法拥有者,此时可以验证得出该用户使用的是自己拥有的合法设备,提高认证的准确性,并在获取认证结果为认证通过后,第一设备执行交易流程,进而提高了交易的安全性。

[0047] 实施例2

[0048] 本发明实施例提供一种交易设备,该设备采用上述交易方法实现交易,如图2所示,该设备包括:第一通信模块11、采集模块12和第二通信模块13。

[0049] 第一通信模块11,用于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;通过通信连接接收第二设备广播的认证信息;

[0050] 采集模块12,用于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;

[0051] 第二通信模块13,用于获取对认证信息和生物特征信息进行认证的认证结果,并在认证结果为认证通过时,执行交易流程。

[0052] 其中,该第一通信模块为人体通信模块,可以采用人体通信技术通过生物肢体与第二设备建立通信连接。第二通信模块例如为有线通信模块或者无线通信模块。

[0053] 其中,生物特征信息包括:指纹信息和/或静脉信息;

[0054] 采集模块,具体用于在通过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。

[0055] 其中,认证信息至少包括以下信息之一:利用私钥进行签名得到电子签名信息,利用对称密钥进行加密得到的密文信息或动态口令。

[0056] 该设备执行本实施例1的交易方法,该设备实现的功能可以参见实施例1中交易方法中第一设备的相关描述,第二设备实现的功能可以参见实施例1中交易方法中第二设备的相关描述。

[0057] 本实施例中,在生物肢体进入第一设备的预设范围后,例如,生物肢体为用户的手部时,用户通过一次操作(该操作可以是接触第一设备或者靠近第一设备),第一设备可以获取第二设备的认证信息和采集到生物特征信息,简化操作次数,降低了方案实现的复杂度。

[0058] 另外,通过获取对认证信息进行验证且对生物特征信息进行验证的认证结果,可以确定使用第二设备的用户真实合法性以及第二设备的真实合法性。如果对认证信息进行验证通过说明第二设备为合法设备,如果对生物特征信息进行验证通过说明该生物特征信息所属用户为第二设备的合法拥有者,此时可以验证得出该用户使用的是自己拥有的合法设备,提高认证的准确性,并在获取认证结果为认证通过后,第一设备执行交易流程,进而提高了交易的安全性。

[0059] 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。

[0060] 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。

[0061] 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。

[0062] 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，也可以存储在一个计算机可读取存储介质中。

[0063] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0064] 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。

[0065] 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。



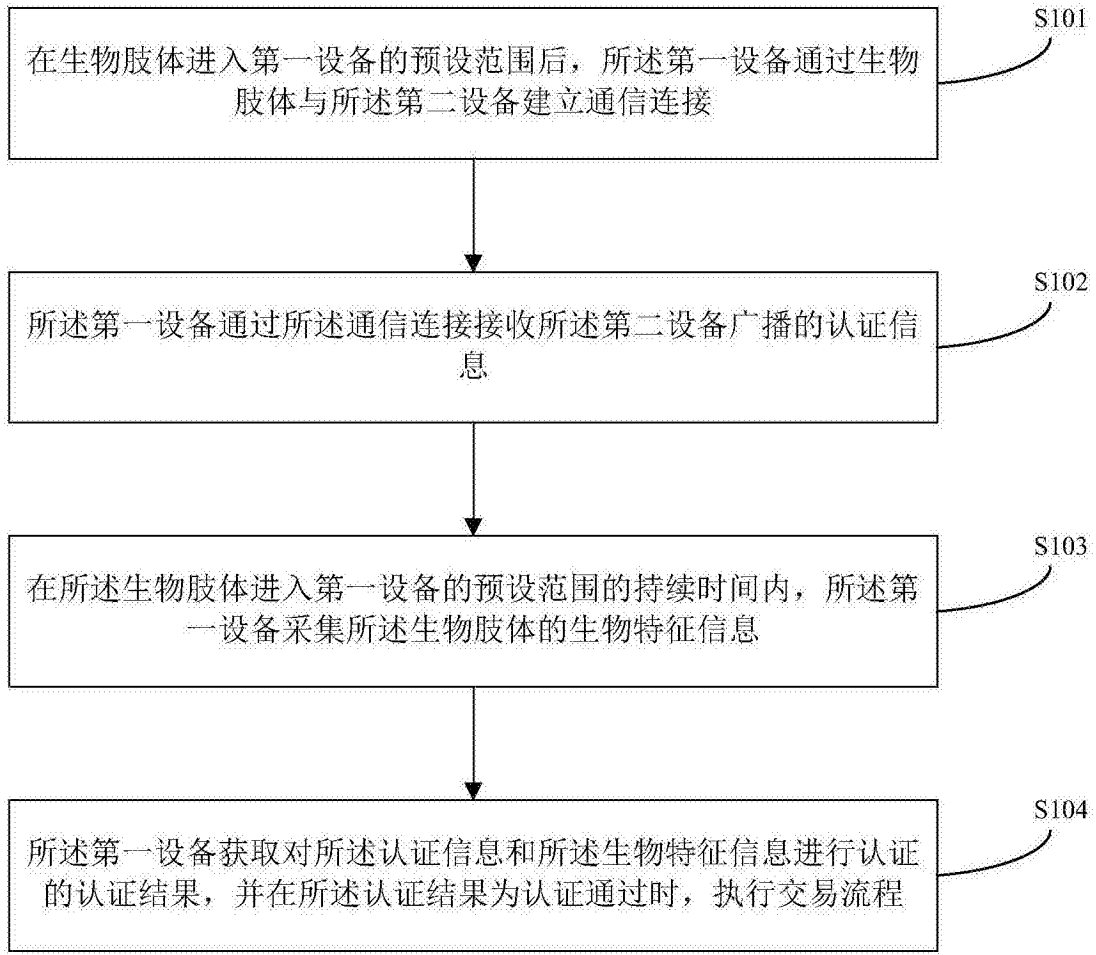


图1

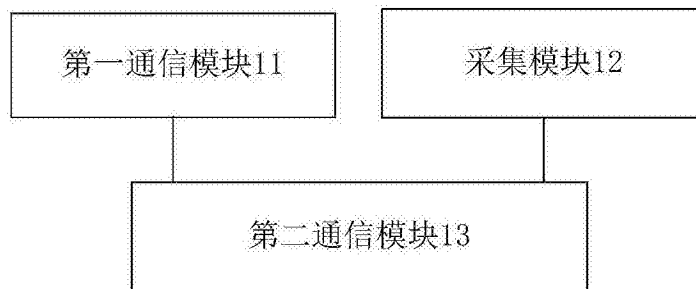


图2