

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G07F 19/00

G07F 7/10 H04M 1/66



[12] 发明专利申请公开说明书

[21] 申请号 01811823.2

[43] 公开日 2004 年 3 月 31 日

[11] 公开号 CN 1486476A

[22] 申请日 2001.6.1 [21] 申请号 01811823.2

[30] 优先权

[32] 2000.6.26 [33] US [31] 09/603,169

[86] 国际申请 PCT/US01/17704 2001.6.1

[87] 国际公布 WO02/01516 英 2002.1.3

[85] 进入国家阶段日期 2002.12.26

[71] 申请人 英特尔公司

地址 美国加利福尼亚

[72] 发明人 戴维·奥克西斯 小罗伯特·沙利文

[74] 专利代理机构 永新专利商标代理有限公司

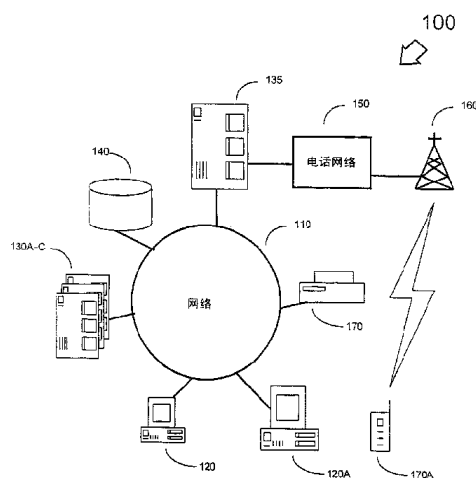
代理人 夏青

权利要求书 3 页 说明书 8 页 附图 5 页

[54] 发明名称 使用蜂窝电话作为鉴定装置的方法和
设备

[57] 摘要

一种用于鉴定电子交易的参与者的方法和设备。利用一呼叫者数据库预先登记参与者，参与者的无线电话号码对特定用户是唯一的。当将交易通知一鉴定服务器时，它为交易参与者产生交易 PIN，并经网络将该交易 PIN 传送给参与者。参与者经无线电话呼叫该鉴定服务器。该鉴定服务器识别该无线电话号码，并为交易 PIN 提示该呼叫者。当与一已知交易 PIN 和一特定的无线电话号码组合时，无线电话用户可被鉴定为在线交易的合法参与者。



1、一种设备，包括：

第一网络接口，连接一计算机网络，被构成以接收交易通知，该交易通知包含用户标识，该用户标识识别电子交易的参与者；

处理器，连接该第一网络接口，被构成以将该用户标识与一呼叫者数据库中的用户电话号码匹配，并产生一个交易 PIN，该第一网络接口将该交易 PIN 传送给该参与者；以及

第二网络接口，连接至该处理器和一个电话网络，被构成以接收具有一呼叫者电话号码的呼叫者发出的电话呼叫，其中，该处理器为呼叫者 PIN 提示该呼叫者，该处理器识别该呼叫者电话号码，当该呼叫者电话号码和用户电话号码匹配以及该交易 PIN 和该呼叫者 PIN 匹配时，该处理器鉴定该参与者。

2、如权利要求 1 的设备，该处理器还包括：

交易处理器，将用户电话号码与用户标识匹配，产生交易 PIN，当该呼叫者电话号码和用户电话号码匹配以及该交易 PIN 和该呼叫者 PIN 匹配时、鉴定参与者。

3、如权利要求 2 的设备，该处理器还包括：

呼叫者 ID 处理器，连接该交易处理器，被构成以识别该呼叫者电话号码。

4、如权利要求 3 的设备，该处理器还包括：

一个呼叫者验证器，连接该交易处理器，被构成以使该用户标识与该呼叫者数据库中的用户电话号码匹配。

5、一种方法，包括：

经一第一网络接口接收交易通知，该交易通知包含识别电子交易参与者的用户标识；

将一用户电话号码与该用户标识匹配；

产生交易 PIN;

将该交易 PIN 传送给参与者;

经第二网络接口接收具有呼叫者电话号码的呼叫者发出的电话呼叫;

为呼叫者 PIN 提示该呼叫者;

当该呼叫者电话号码和用户电话号码匹配时, 验证该呼叫者是用户; 以及

当该交易 PIN 和该呼叫者 PIN 匹配时, 验证该呼叫者是电子交易的参与者。

6、如权利要求 5 的方法, 还包括:

当该呼叫者被验证为用户时, 以及当该呼叫者被验证为电子交易的参与者时, 鉴定电子交易的用户。

7、如权利要求 6 的方法, 还包括:

通知交易服务器是否电子交易的用户被鉴定。

8、如权利要求 7 的方法, 还包括:

当电子交易的用户未被鉴定时取消该电子交易。

9、如权利要求 8 的方法, 还包括:

将用户鉴定的结果记录在一交易日志中。

10、如权利要求 9 的方法, 其中, 产生交易 PIN 是通过产生数字和字母的伪随机组合来完成的。

11、如权利要求 9 的方法, 其中, 产生交易 PIN 是通过从字典中产生一个或多个单词的伪随机选择来完成的。

12、一种编码有数据和指令的计算机可读介质, 这些数据和指令使一设备执行这些指令以实现:

经一第一网络接口接收交易通知, 该交易通知包含识别电子交易参与者的用户标识;

将一用户电话号码与该用户标识匹配;

产生交易 PIN;

将该交易 PIN 传送给参与者;

经第二网络接口接收具有呼叫者电话号码的呼叫者发出的电话呼叫;

为呼叫者 PIN 提示该呼叫者;

当该呼叫者电话号码和用户电话号码匹配时, 验证该呼叫者是用户; 以及

当该交易 PIN 和该呼叫者 PIN 匹配时, 验证该呼叫者是电子交易的参与者。

13、如权利要求 12 的计算机可读介质, 还编码有数据和指令, 这些数据和指令使一设备执行这些指令以实现:

当该呼叫者被验证为用户时, 以及当该呼叫者被验证为电子交易的参与者时, 鉴定电子交易的用户。

14、如权利要求 13 的计算机可读介质, 还编码有数据和指令, 这些数据和指令使一设备执行这些指令以实现:

通知交易服务器是否电子交易的用户被鉴定。

15、如权利要求 14 的计算机可读介质, 还编码有数据和指令, 这些数据和指令使一设备执行这些指令以实现:

当电子交易的用户未被鉴定时取消该电子交易。

16、如权利要求 15 的计算机可读介质, 还编码有数据和指令, 这些数据和指令使一设备执行这些指令以实现:

将用户鉴定的结果记录在一交易日志中。

17、如权利要求 16 的计算机可读介质, 其中, 产生交易 PIN 是通过产生数字和字母的伪随机组合来完成的。

18、如权利要求 16 的计算机可读介质, 其中, 产生交易 PIN 是通过从字典中产生一个或多个单词的伪随机选择来完成的。

使用蜂窝电话作为鉴定装置的方法和设备

背景技术

发明领域

本发明总体上涉及对用户的鉴定，具体地说是涉及对电子交易中的用户进行查证的方法和系统。

相关技术的描述

对人的身份进行鉴定的问题已存在数百年了。在普通的交易中，可以用多种方式完成鉴定。例如，可以采用一种普遍接受形式的身份证明文件来查证一个人的身份，例如图片标识（“图片 ID”）。

然而，随着因特网的出现，电子交易（电子商务）的数量不断增加。利用电子交易，参与交易的各当事人不能看见其它当事人，往往从不会与其它各方相遇或认识。

而且，在电子交易中验证身份的常规方法通常包括传送只有正当的人应该知道的个人信息。示例包括采用信用卡号、社会安全号、地址及其它个人信息。由于个人信息激增，保密专家和公众有理由担心这些数据的扩散。更糟的是，由于个人信息的激增，信息变得“受污染”以及太大众化，用作个人身份的有效鉴定。

因此，鉴定交易参与者身份的问题是不简单的和困难的。

因而人们需要一种安全鉴定电子交易中的用户的方法。

附图简述

图 1 示出一种在电子交易中鉴定用户的系统的实施例。

图 2 是在电子交易中鉴定用户的设备的方框图。

图 3 是在电子交易中鉴定用户的实施例的方框图。

图 4 是在电子交易中请求鉴定用户的方法之流程图。

图 5a 和图 5b 是在电子交易中鉴定用户的方法之流程图。

详细说明

图 1 描述根据本发明的实施例构成及运行的系统 100 的功能方框简图。系统 100 被构成以在电子交易中鉴定用户。电子交易是在计算机网络上发生的任何交易（即“在线”交易）。这种交易的示例包括但不限于商品和服务的任何销售或购买，或是涉及当事人之电子鉴定的任何操作。前者的一个示例是通过万维网（“WWW”或“Web”）因特网浏览器购买书籍、光盘、或任何其它商品或服务。后者交易的示例是医生同意由电子药房填写的医药处方。

该方法依赖的事实是，利用一个呼叫者数据库使用户预先注册，用户的无线电话号码对一个特定的用户是唯一的。当与一个已知的交易代码（例如个人识别号码 PIN）组合时（其被送给用户作为部分在线/网络交易），无线电话用户可被鉴定为该在线交易的参与者。

在系统 100 中，计算机 120 和鉴定服务器 135 连接通信网络 110。网络 110 也可包括本技术领域公知的其它可联网装置，如其它计算机 120、服务器 130、打印机 125 和存储介质 140。本技术领域易于理解的是，任何数量或种类的计算机可联网装置或部件可被连接至网络 110，而无需创造性的能力。其它装置的示例包括但不限于服务器、计算机、工作站、终端、输入装置、输出装置、打印机、绘图仪、路由器、网桥、摄像机、传感器或在本领域公知的任何其它这类的装置。计算机 120 能在网络 110 上进行通信，它可以是本领域公知的任何类型。服务器 130A-C 可以是本领域已知的任何服务器，包括 web、数据库、打印或应用服务器。更重要的是，服务

器 130A—C 可以产生、发起或参与要求进行用户鉴定的电子交易。参与电子交易的服务器被称为“交易服务器” 130。

网络 110 可以是本领域公知的任何通信网络，包括因特网、局域网 (LAN)、广域网 (WAN) 或任何将计算机链接至鉴定服务器 135 的系统。此外，网络 110 可以根据本领域已知的任何布局构成，包括星形、环形、总线形或它们的任何组合。

鉴定服务器 135 连接一个电话网络 150，该网络支持呼叫号码传送 (CND)，也被称为呼叫者 ID (CID)。电话网络 150 可被构成为分组交换电话网络、通常电话业务 (POTS)、综合业务数字网络 (ISDN) 或支持呼叫者 ID 的任何其它本领域公知电话网络 150。而电话网络 150 连接也支持呼叫者 ID 的无线电话系统 160。

系统 100 中的每个用户具有无线电话 170。鉴定服务器 135 掌握每个用户的无线电话号码，并将无线电话号码存储在呼叫者数据库中。在一些实施例中，要求进行用户鉴定的交易服务器 130 也可能是与鉴定服务器 135 相同的设备，并没有任何功能损失。

以下将参照图 2 的示例性鉴定服务器 135 的功能框图描述实施例。鉴定服务器 135 运行多任务操作系统，并包括至少一个中央处理单元 (CPU) 102。CPU 102 可以是本领域公知的任何微处理器或微控制器。例如，CPU 102 可以是微处理器，如由英特公司制造的奔腾 III 处理器。用于编程 CPU 的软件可以在计算机可读存储介质 140 上得到，或者另一方式是来自通过网络 110 的另一位置。CPU 102 连接计算机存储器 118。鉴定服务器 135 受控于在计算机存储器 118 中执行的操作系统 (OS)。

CPU 102 连通多个外围设备，包括计算机网络接口 116 和电话网络接口 112。附加的外围设备包括显示器 104、人工输入装置 106、存储介质 140、话筒 108 和数据输入端口 114。显示器 104 可以是可视显示器，如阴极射线管 (CRT) 监视器、液晶显示 (LCD) 屏、

触摸屏、或本领域公知的任何其它监视器，用于向用户在视觉上显示图像和文字。人工输入装置 106 可以是常规的键盘、小键盘、鼠标、跟踪球、或本领域公知的其它输入装置，用于人工输入数据。存储介质 140 可以是常规的读写存储器，如磁盘驱动器、软盘驱动器、光盘只读存储器（CD-ROM）驱动器、基于晶体管的存储器或本领域所公知的其它计算机可读存储装置，用于存储和取出数据。值得注意的是，存储介质 140 可以位于远离 CPU 的位置，并经网络 110（如局域网、广域网或因特网）连接 CPU 102。

话筒 108 可以是本领域公知的任何合适的话筒，用于向 CPU 102 提供音频信号。另外，可以连接扬声器（未示出），用于从 CPU 102 再现音频信号。应该理解的是，话筒 108 和扬声器可包括适当的数模转换电路和适当的模数转换电路。

数据输入端口 114 可以是本领域公知的任何数据端口，用于连接外部辅助设备，其采用的数据协议如 RS-232、通用串行总线（USB）和电气与电子工程师学会（IEEE）标准第 1394 号（“火线”）。

网络接口 116 可以是本领域公知的任何接口，用于在计算机网络上进行文件的通信和传输，这样的网络之示例包括传输控制协议/因特网协议（TCP/IP）、以太网、光纤分布式数据接口（FDDI）、权标总线、或权标总线网。另外，在一些系统中，网络接口 116 可包含连接数据输入端口 114 的一个调制解调器。同样，电话网络接口 112 提供与鉴定服务器 135 的连接，以与电话网络 150 进行通信。因此，电话网络接口 112 允许鉴定服务器 135 通信并处理来自电话线的输入。

图 3 是 CPU 102 和存储介质 140 的扩展功能方框图。本领域技术人员易于理解的是，图 3 的功能部件可以采用硬件、固件的形式实现，或者被实现为计算机可读存储介质 140 上编码的软件指令和数据。如图 3 所示，中央处理单元 102 在功能上包括数据处理器 202、

应用接口 204、交易处理器 206 和呼叫处理器 210。数据处理器 202 连接显示器 104、人工输入装置 106、存储介质 140、话筒 108、数据输入端口 114、因特网接口 116 和电话网络接口 112。数据处理器 202 使 CPU 102 能够将数据安排在这些部件上、从这些部件中读取数据以及将数据写入这些部件。

应用接口 204 使 CPU 102 能够根据独立的软件应用或实体 (entity) 进行一些处理。例如, 应用接口 204 可采用开窗用户接口的形式, 如本领域所公知的那样。

交易处理器 206 处理电子商务交易。交易处理器 206 根据由呼叫处理器 210 对用户的验证批准或不批准交易。交易处理器 206 的结果可以被记录在存储介质 140 上, 作为交易日志 242。呼叫处理器 210 可进一步包括呼叫者 ID 处理器 212 和呼叫者验证器 214。呼叫处理器 210 的这些部件与一个已知的呼叫者数据库 244 进行交互, 根据图 4、5a 及 5b 的流程图可以更好地理解, 如下所述。

图 4 是描述了根据本发明实施例构成及操作的过程 300 的流程图。如在方框 302 中所示, 过程 300 开始确定是否交易服务器 130 参加需要做用户鉴定的电子交易。该确定可以通过采用本领域中任何公知的手段来完成, 包括对需要用户鉴定的电子交易的清单进行查表, 或者可以被嵌入在由交易服务器 130 执行的程序中。在鉴定用户的期间, 在方框 304, 过程 300 可暂停交易。

在方框 306 中, 过程 300 启动交易服务器 130 以传送鉴定请求 (也称为“交易通知”) 至鉴定服务器 135。该鉴定请求可包括用户标识和交易标识。该用户标识可以是识别用户为交易当事人的任何信息, 包括姓名、社会安全号或任何其它类似的标识。该交易标识鉴别需要鉴定的交易。另外, 在有些实施例中, 用户的电子邮件地址也可以被编码在鉴定请求中。该通知经网络 110 被传送给鉴定服务器 135。在组合鉴定服务器 135 与交易服务器 130 的实施例中,

该通知可以在装置本身内被内部发送。

在方框 310 中, 过程 300 等待鉴定服务器 135 以响应鉴定请求。一旦接收到来自鉴定服务器 135 的响应, 过程 300 确定是否所接收的响应指示用户被鉴定。当用户被鉴定服务器 135 鉴定时, 交易被批准。否则, 在方框 314 中, 交易被禁止。

图 5a 和图 5b 分别是描述过程 400 和 450 的流程图。过程 400 和 450 描述从鉴定服务器 135 的观点来看的鉴定顺序。在方框 401, 鉴定服务器 135 接收来自交易服务器 130 的鉴定请求或交易通知。交易处理器 206 对用户标识和交易标识进行译码。在方框 403, 交易处理器 206 产生一个交易 PIN, 该交易 PIN 包括介于 0 和 9 之间之数字的序列。该序列与用户的无线电话号码结合使用, 以鉴定用户参与交易。应注意的是在一些实施例中, 交易 PIN 可包含字母数字的字符, 其中也包括符号 “*” 和 “#”、单词或可通过电话键盘输入的字母序列。

产生数字交易 PIN 的实施例可通过本领域已知的任何手段产生伪随机数。采用字母的实施例可产生伪随机系列字母和数字, 或可采用字典产生交易 PIN。有些实施例在呼叫者数据库 244 中查找用户的条目, 并添加或存储该交易标识和交易 PIN 作为呼叫者数据库 244 中的字段, 或作为交易日志 242 的一部分。

在方框 405, 过程 400 向用户发送交易 PIN。该交易处理器 206 通过网络接口 116 和网络 110 将该交易 PIN 发送给用户。在所有实施例中, 用户被提供一个电话号码, 它们被要求呼叫以鉴定它们自身为交易中的合法用户。该被提供的电话号码经电话网络 150 被连接到鉴定服务器 135。在有些实施例中, 该电话号码的传送是通过在一个呼叫者数据库 244 中查找用户的电子邮件地址, 然后向用户发电子邮件来传送该电话号码。其它实施例包括利用被编码在鉴定请求中的电子邮件地址。还有另外的实施例通过万维网页在用户之

前显示交易 PIN。

图 5b 的过程 450 鉴定用户，是通过使用该用户之呼叫者识别的无线电话号码与由图 5a 中的过程 400 提供的交易 PIN 相匹配。该用户呼叫所提供的电话号码，到达鉴定服务器 135。在方框 402，鉴定服务器 135 接收来自该用户的呼叫。在方框 404，鉴定服务器 135 通过使用该用户匹配为经呼叫者 ID 来自某一无线电话号码的呼叫者，对用户进行鉴定。鉴定服务器 135 经其电话网络接口 112 接收到该呼叫。然后该呼叫被送到呼叫处理器 210。在一些实施例中，该呼叫者 ID 信号被传送为第一和第二环形周期之间的 V.23 调制解调信号。在实施例中，被连接至 ISDN 线路，按照 ITU-T 规范 Q.81.3，在呼叫设置的初始发动时，在 D（信令）信道上传送呼叫者 ID。呼叫者 ID 处理器 212 导出用户的电话号码，而与呼叫者 ID 的实现无关。呼叫者验证器 214 取该电话号码并在呼叫者数据库 244 中查找该呼叫者身份。

如果不能确定电话号码，或者该呼叫者不是该系统的已知用户（如由呼叫者数据库 244 所确定），在方框 408，不理睬该电话呼叫，鉴定服务器 135 挂断。

否则，如果该呼叫者被识别为呼叫者数据库 244 中的已知用户，在方框 410，提示该呼叫者输入交易 PIN。

如果呼叫者输入的交易 PIN 与通过过程 400 发送给用户的交易 PIN 匹配，如由交易处理器 206 所确定的，则该用户被鉴定，在方框 414，通过因特网接口 116 将该鉴定通知交易服务器 130。

如果呼叫者输入的交易 PIN 与发送给用户的交易 PIN 不匹配，如由交易处理器 206 所确定的，鉴定失败，通过因特网接口 116 将该鉴定失败通知交易服务器 130。在有些实施例中，可让用户有机会再次输入交易 PIN，见方框 416。

鉴定的结果可被记录在交易日志 242 中。

以上提供的实施例的描述使本领域任何技术人员可以实现该方法。本领域技术人员将很容易确定对这些实施例的各种变型，在此定义的一般原理可以适用于其它实施例，而无需利用创造性才能。因此，本发明并非是要限制于这里所述的实施例，而应该被给予与以上所述原理和新颖特征一致的最宽范围。

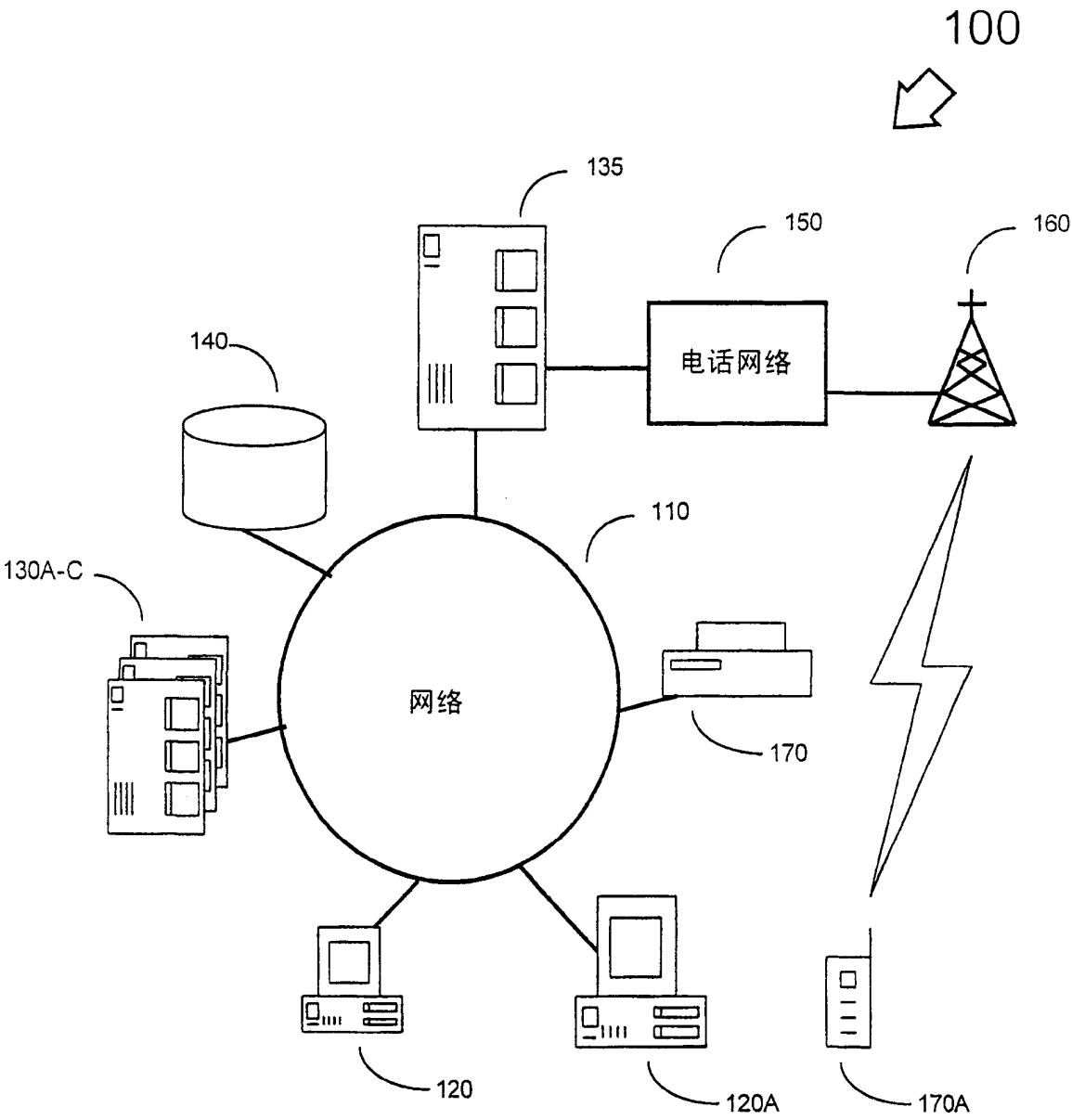


图1

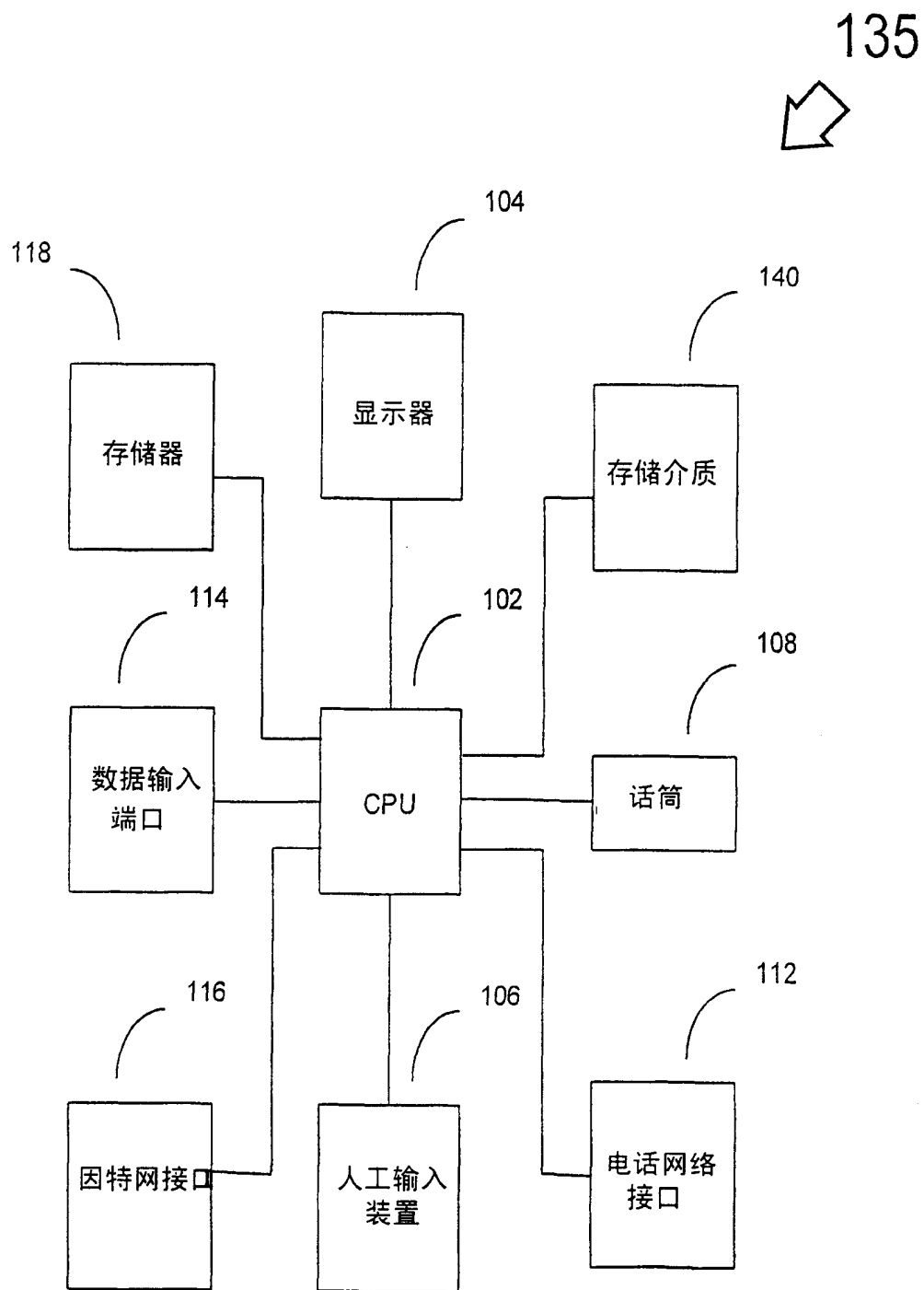


图2

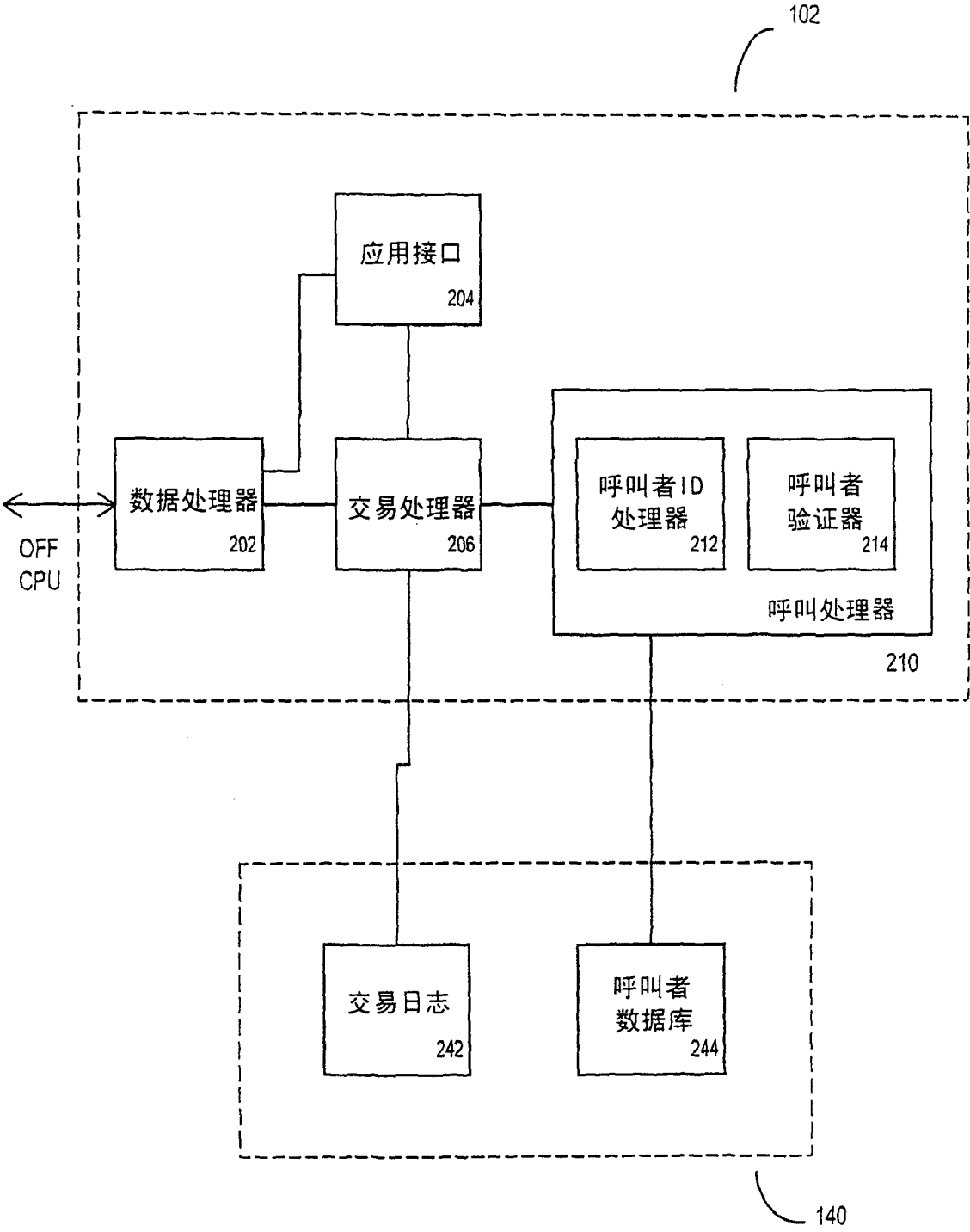
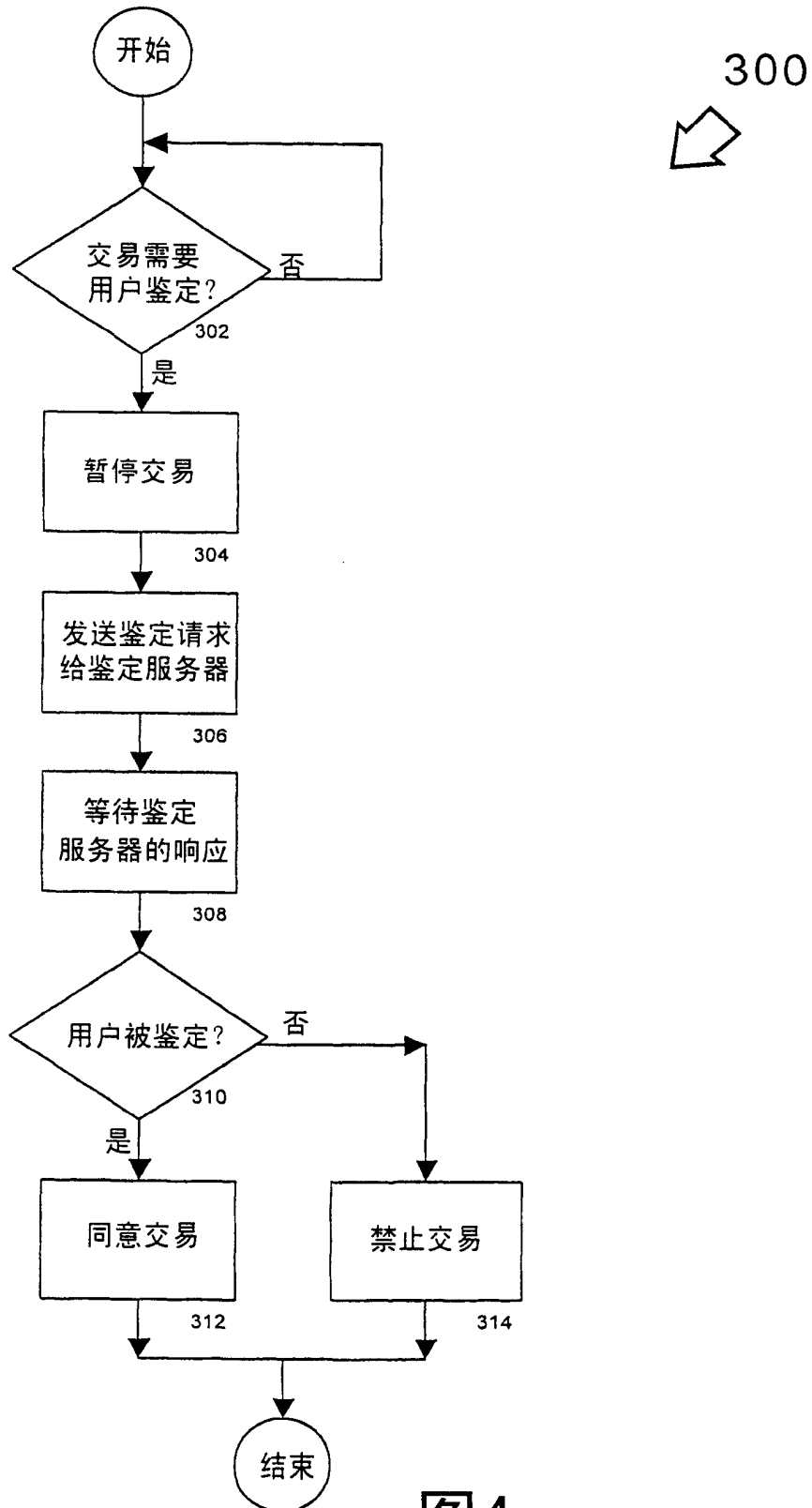


图3



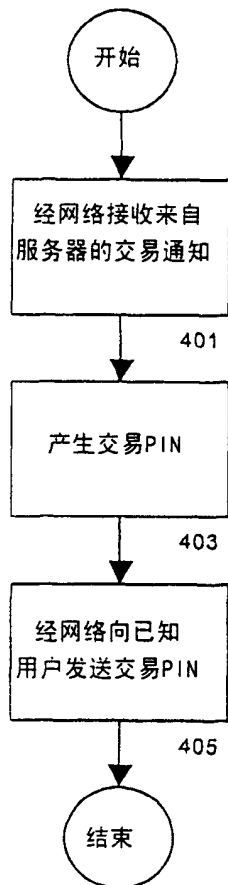


图5a

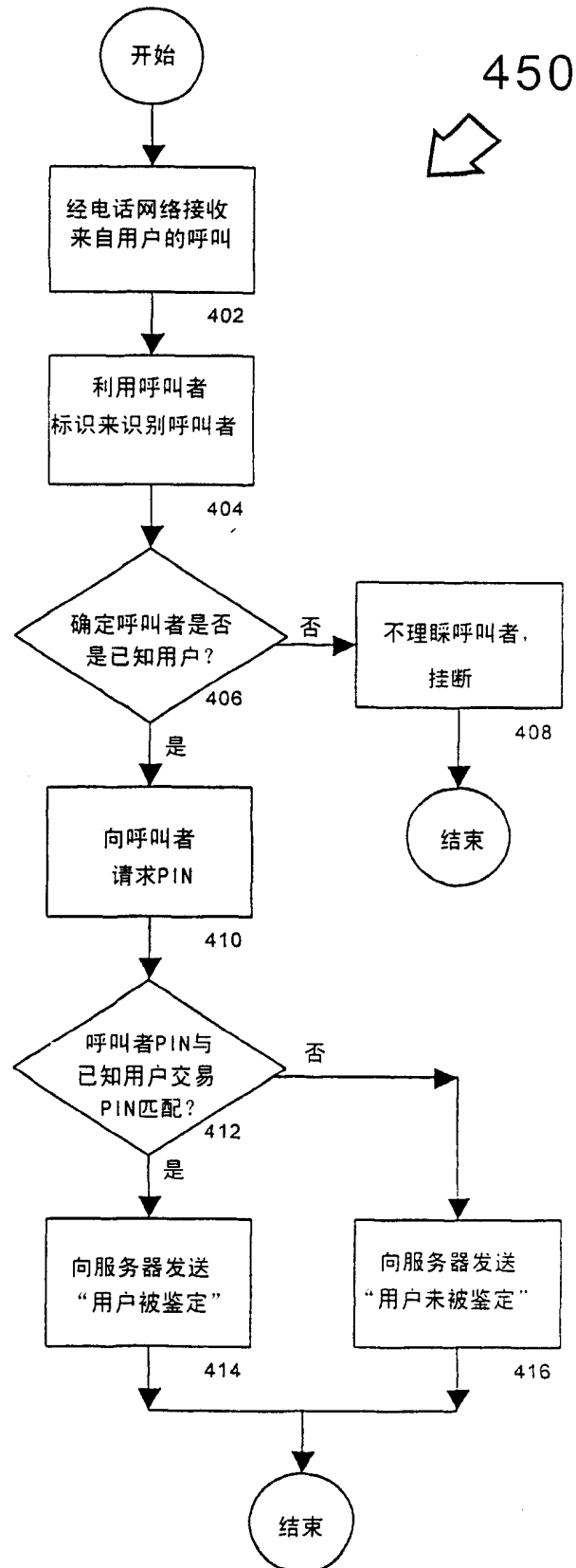


图5b