(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 112005231 A
(43)申请公布日 2020.11.27

(21)申请号 201980027655.9
(22)申请日 2019.04.23
(30)优先权数据
18290038.1 2018.04.23 EP
(85)PCT国际申请进入国家阶段日
2020.10.22
(86)PCT国际申请的申请数据
PCT/EP2019/060273 2019.04.23
(87)PCT国际申请的公布数据
WO2019/206854 EN 2019.10.31
(71)申请人 艾玛迪斯简易股份公司
地址 法国比奥
(72)发明人 C·迈凯尔-莱德伍德 N·拖莱斯 G·G·普莱斯提亚 M-A·马拉福
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 李颖
(51)Int.Cl.
G06F 21/32(2006.01)

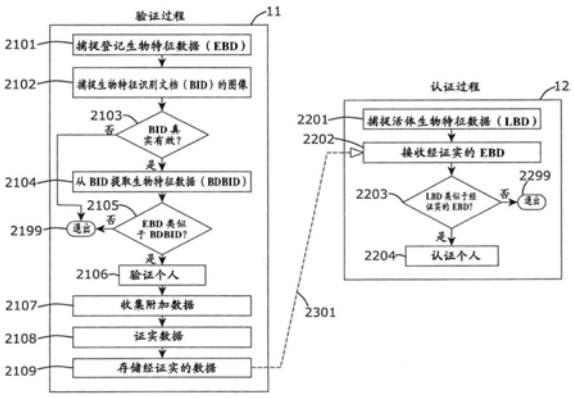
权利要求书3页 说明书18页 附图7页

(54)发明名称

生物特征认证方法、系统和计算机程序

(57)摘要

本公开涉及生物特征认证方法、系统和计算机程序。使用个人的生物特征数据的认证方法和系统。所述方法可以灵活地在多个不同的验证设备和认证设备上使用，包括验证过程和认证过程。由验证设备捕捉第一生物特征数据，并与官方生物特征数据比较。证实并存储捕捉和输入的数据。在需要对所述个人进行认证时，捕捉所述个人的活体生物特征数据，并与第一生物特征数据比较。如果数据相似，那么所述个人被自动认证。



CN 112005231 A

1.一种包括验证过程和认证过程的认证方法,其中所述验证过程和认证过程在至少两个不同的系统上进行,其中所述验证过程的至少一部分在至少一个验证设备上进行,并且所述认证过程的至少一部分在至少一个认证设备上进行,其中所述验证过程包括:

-捕捉个人的第一生物特征数据;

-从生物特征识别文档中提取第二生物特征数据;

-将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较,以获得与第一相似度阈值相当的相似度值;

其中所述认证过程包括:

-捕捉所述个人的活体生物特征数据;

-接收所述个人的所述第一生物特征数据;

-将活体生物特征数据与第一生物特征数据进行比较;和

-响应于活体生物特征数据与所述第一生物特征数据的相似度值超过第二相似度阈值,认证所述个人。

2.按照权利要求1所述的认证方法,其中所述验证过程还包括,响应于第一生物特征数据与第二生物特征数据相比的相似度值超过第一相似度阈值:

-验证所述个人的身份;

-收集附加数据;

-证实所述第一生物特征数据和附加数据;和

-存储经证实的第一生物特征数据和经证实的附加数据。

3.按照权利要求2所述的认证方法,其中所述验证设备中的至少一个是所述个人的移动设备,并且其中在所述验证过程中,存储经证实的第一生物特征数据和经证实的附加数据包括将经证实的数据存储在所述个人的移动设备上,并且其中在所述认证过程中,接收所述个人的第一生物特征数据包括将经证实的第一生物特征数据从所述个人的移动设备传送到所述认证设备。

4.按照权利要求2或3所述的认证方法,其中所述验证设备中的至少一个是自助终端,并且其中在所述自助终端上进行的验证过程还包括:

-获得标识号,其中所述标识号是从所述生物特征识别文档中提取的唯一标识号;

-响应于所述第一生物特征数据与来自所述生物特征识别文档的对应第二生物特征数据的相似度值超过第一相似度阈值:

-使用所述附加数据生成密钥;

-用从所述附加数据生成的密钥,加密所述经证实的第一生物特征数据和经证实的附加数据;和

-将加密的经证实的登记生物特征数据和加密的经证实的附加数据与所述标识号一起存储在中央数据库中;和

其中在所述认证过程中,接收所述个人的第一生物特征数据包括:

-捕捉所述个人的认证生物特征识别文档的图像;

-从所述认证生物特征识别文档中提取认证附加数据;

-从该生物特征文档中提取认证标识号;

-利用所述认证附加数据生成密钥;

-使用所述认证标识号,向中央数据库请求所存储的加密的经证实的第一生物特征数据;和

-用从所述认证附加数据生成的密钥,解密加密的经证实的第一生物特征数据。

5.按照权利要求2-4任意之一所述的认证方法,其中所述验证设备中的至少一个是所述个人的移动设备,并且其中在所述验证过程中,所述经证实的第一生物特征数据和经证实的附加数据被存储在所述个人的移动设备上,并且其中响应于所述个人通告他们在不久的将来需要被认证,所述验证过程还包括:

-获得标识号;和

-将所述经证实的第一生物特征数据和经证实的附加数据连同所述标识号一起存储在中央数据库中。

6.按照权利要求2-5任意之一所述的认证方法,其中所述验证过程还包括:

-从所述验证设备提取所述验证设备特有的数据;

-使用从所述验证设备提取的数据生成密钥;

-用从提取的数据生成的密钥,加密经证实的第一生物特征数据和经证实的附加数据;和

-将加密的经证实的第一生物特征数据和经证实的附加数据存储在中央数据库中;

-响应于所述个人通告他们在不久的将来需要被认证,请求同意使用包括加密的经证实的第一生物特征数据和经证实的附加数据的存储数据;和

-响应于获得所述个人同意使用所述存储数据,用从提取自所述验证设备的数据生成的密钥,解密所述加密的经证实的第一生物特征数据和经证实的附加数据。

7.按照权利要求5或6所述的认证方法,其中所述认证过程还包括:

-使认证设备能从中央数据库得到要认证的人的多个经证实的第一生物特征数据项;和

其中接收所述个人的所述经证实的第一生物特征数据包括将所述多个经证实的第一生物特征数据项与捕捉的所述个人的活体生物特征数据进行比较,以及响应于所述多个经证实的第一生物特征数据之一与所述活体生物特征数据相似,选择相似的经证实的第一生物特征数据作为所述个人的第一生物特征数据。

8.按照权利要求4-7任意之一所述的认证方法,其中所述中央数据库由硬件安全模块保护,和/或存储在所述中央数据库中的数据被加密。

9.按照权利要求1-8任意之一所述的认证方法,其中第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合。

10.按照权利要求2-9任意之一所述的认证方法,其中所述附加数据包括从生物特征文档中提取的数据、手动输入的数据、从第三方取回的数据、或者它们的组合。

11.按照权利要求1-10任意之一所述的认证方法,其中第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合的向量化表示,并且其中用于使数据向量化的算法由所述认证设备的操作者预先定义。

12.按照权利要求1-11任意之一所述的认证方法,其中捕捉所述第一生物特征数据和/

或捕捉所述活体生物特征数据包括拍摄所述个人的至少一部分的照片，和/或其中从所述生物特征识别文档提取第二生物特征数据包括捕捉生物特征识别文档的图像，这包括拍摄生物特征识别文档的照片、扫描生物特征识别文档、或者视觉检查生物特征识别文档。

13.按照权利要求1-12任意之一所述的认证方法，其中当认证的需求结束时，删除任何接收的数据。

14.按照权利要求1-13任意之一所述的认证方法，其中认证所述个人包括准许进入区域、将经证实的附加数据传送到所述认证设备、解密经证实的附加数据、或者它们的组合中的至少一个。

15.按照权利要求1-14任意之一所述的认证方法，其中所述验证过程还包括生成与所述个人的唯一用户ID关联的用户账户，其中所述用户账户由用户名和PIN保护。

16.一种用于认证个人的自动认证系统，包括：

-至少一个验证设备；和

-至少一个认证设备；

其中所述至少一个验证设备远离所述至少一个认证设备；其中所述至少一个验证设备和所述至少一个认证设备被配置成经由网络进行通信；并且其中所述至少一个验证设备被配置成：

-捕捉个人的第一生物特征数据；

-从生物特征识别文档中提取第二生物特征数据；和

-将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较，以获得与第一相似度阈值相当的相似度值；和

其中所述至少一个认证设备被配置成：

-捕捉所述个人的活体生物特征数据；

-接收所述个人的所述第一生物特征数据；

-将活体生物特征数据与第一生物特征数据进行比较；和

-响应于所述活体生物特征数据与所述第一生物特征数据的相似度值超过第二相似度阈值，认证所述个人。

17.按照权利要求16所述的自动认证系统，还包括数据库系统，其中所述数据库系统远离所述至少一个验证设备和所述至少一个认证设备；其中所述数据库系统被配置成经由网络与所述验证设备和所述认证设备通信，并且其中所述数据库系统被配置成：

-从所述至少一个验证设备接收数据；和

-使所述至少一个认证设备能得到数据。

18.按照权利要求16或17所述的自动认证系统，还被配置成执行权利要求2-15任意之一的特征。

19.一种计算机程序，包括用于执行按照权利要求1-15所述的方法的特征的程序代码指令。

生物特征认证方法、系统和计算机程序

技术领域

[0001] 本发明涉及生物特征识别系统，更具体地涉及一种在验证设备上应用验证过程和在认证设备上应用认证过程的人的生物特征认证的方法、系统和计算机程序。

背景技术

[0002] 生物特征识别是一种相关性日益增长的技术，因为它可以应用于对例如在边境、公司、机场或酒店的限制区域的自动进入控制。识别从而主要基于面部照片、指纹图像、手掌静脉图像、虹膜扫描和/或语音记录。

[0003] 现有技术的生物特征识别系统通常需要一个统一的系统，该系统涉及在收集稍后要识别的个人的生物特征数据，并且涉及在识别所述个人时将所收集的生物特征数据与活体生物特征数据进行比较中。如果生物特征识别被用于准许进入公司中的限制区域，那么生物特征数据(例如指纹或虹膜扫描)的收集，以及例如在安全门处，收集的生物特征数据与活体数据的比较可以由同一计算系统处理。然而，如果生物特征识别用于准许进入或多或少的公共空间，例如进入音乐厅、机场中的安全区域、或火车站的站台，那么要被识别的人属于大得多且更广泛的群体。在这种情况下，在单个统一系统中，即使有可能的话，预先收集人们的生物特征数据也似乎是困难的。

[0004] 此外，将生物特征数据存储在数据库中会导致数据安全问题。如果其中存储所收集的生物特征数据的数据库不能被完全封装，例如，如果使用分布式系统收集生物特征数据，并将所收集的生物特征数据与活体生物特征数据进行比较，那么敏感数据可能会被未经授权的人访问。

[0005] 于是，需要一种改进的灵活系统，该系统能够在逻辑上和物理上将一方面的生物特征数据的收集和另一方面的认证和访问控制分开，同时始终关注敏感个人数据的数据安全问题。本发明涉及这样的一种改进的生物特征认证方法、系统和计算机程序。

发明内容

[0006] 按照本发明的第一方面，提出一种包括验证过程和认证过程的认证方法。所述验证过程和认证过程在至少两个不同的系统上进行。所述验证过程的至少一部分在至少一个验证设备上进行，并且所述认证过程的至少一部分在至少一个认证设备上进行。

[0007] 所述验证过程包括捕捉个人的第一生物特征数据，和从生物特征识别文档中提取第二生物特征数据。将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较，以获得与第一相似度阈值相当的相似度值。所述认证过程包括捕捉所述个人的活体生物特征数据，和接收所述个人的所述第一生物特征数据。然后，将活体生物特征数据与第一生物特征数据进行比较。响应于活体生物特征数据和所述第一生物特征数据的相似度值超过第二相似度阈值，认证所述个人。

[0008] 在实施例中，所述验证过程还包括，响应于第一生物特征数据与第二生物特征数据相比的第一相似度值超过第一相似度阈值，验证所述个人的身份。收集另外的附加数据。

证实并存储所述第一生物特征数据和附加数据。在另一个实施例中，验证设备中的至少一个是所述个人的移动设备，并且在验证过程中，存储经证实的第一生物特征数据和经证实的附加数据包括将经证实的数据存储在所述个人的移动设备上。此外，在认证过程中，接收所述个人的所述第一生物特征数据包括将经证实的第一生物特征数据从所述个人的移动设备传送到所述认证设备。

[0009] 在再一个实施例中，所述验证设备中的至少一个是自助终端，并且在所述自助终端上进行的验证过程还包括获得标识号，其中所述标识号是从所述生物特征识别文档中提取的唯一标识号。响应于所述第一生物特征数据与来自所述生物特征识别文档的对应第二生物特征数据的相似度值超过第一相似度阈值，使用所述附加数据生成密钥。所述经证实的第一生物特征数据和经证实的附加数据用从所述附加数据生成的密钥加密，并且与所述标识号一起存储在中央数据库中。此外，在所述认证过程中，接收所述个人的所述第一生物特征数据包括捕捉所述个人的认证生物特征识别文档的图像，并从该生物特征文档中提取认证附加数据和认证标识号。利用所述认证附加数据生成密钥。使用所述认证标识号从中央数据库查询所存储的加密的经证实的第一生物特征数据，并用从所述认证附加数据生成的密钥解密。

[0010] 在又一个实施例中，所述验证设备中的至少一个是所述个人的移动设备，并且在所述验证过程中，所述经证实的第一生物特征数据和经证实的附加数据被存储在所述个人的移动设备上。响应于所述个人通告在不久的将来需要被认证，所述验证过程还包括获得标识号，并将所述经证实的第一生物特征数据和经证实的附加数据连同所述标识号一起存储在中央数据库中。

[0011] 在另一个实施例中，所述验证过程还包括从所述验证设备提取所述验证设备特有的数据，使用从所述验证设备提取的数据生成密钥，用从提取的数据生成的密钥加密经证实的第一生物特征数据和经证实的附加数据，并将加密的经证实的第一生物特征数据和经证实的附加数据存储在中央数据库中。响应于所述个人通告他们在不久的将来需要被认证，所述验证过程还包括请求同意使用包括加密的经证实的第一生物特征数据和经证实的附加数据的存储数据。并且响应于获得所述个人同意使用所述存储数据，所述验证过程还包括用从提取自所述验证设备的数据生成的密钥，解密所述加密的经证实的第一生物特征数据和经证实的附加数据。

[0012] 在另一个实施例中，所述认证过程还包括使认证设备可以从中央数据库得到要认证的个人的多个经证实的第一生物特征数据项，其中接收所述个人的所述经证实的第一生物特征数据包括将所述多个经证实的第一生物特征数据项与捕捉的所述个人的活体生物特征数据进行比较，并且响应所述多个经证实的第一生物特征数据之一与所述活体生物特征数据相似，选择所述相似的经证实的第一生物特征数据作为所述个人的第一生物特征数据。

[0013] 在另一个实施例中，中央数据库由硬件安全模块保护和/或存储在中央数据库中的数据被加密。在又一个实施例中，第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合。在又一个实施例中，所述附加数据包括从生物特征文档中提取的数据、手动输入的数据、从第三方取回的数据、或者它们的组合。

[0014] 在另一个实施例中，第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合的向量化表示，并且其中用于使数据向量化的算法由认证设备的操作者预先定义。在又一个实施例中，捕捉所述第一生物特征数据和/或捕捉所述活体生物特征数据包括拍摄所述个人的至少一部分的照片，和/或从所述生物特征识别文档提取第二生物特征数据包括捕捉生物特征识别文档的图像，这包括拍摄生物特征识别文档的照片、扫描生物特征识别文档、或者视觉检查生物特征识别文档。

[0015] 在另一个实施例中，当认证的需求结束时，删除任何接收的数据。在又一个实施例中，对个人进行认证包括准许进入区域、将经证实的附加数据传送到认证设备、解密经证实的附加数据、或者它们的组合中的至少一个。在又一个实施例中，所述验证过程还包括生成与所述个人的唯一用户ID关联的用户账户，其中所述用户账户由用户名和PIN保护。

[0016] 按照本发明的第二方面，提出一种用于认证个人的自动认证系统，所述系统包括至少一个验证设备和至少一个认证设备。所述至少一个验证设备远离所述至少一个认证设备，并且所述至少一个验证设备和所述至少一个认证设备被配置成经由网络进行通信。

[0017] 所述至少一个验证设备被配置成捕捉个人的第一生物特征数据，从生物特征识别文档中提取第二生物特征数据，并将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较，以获得与第一相似度阈值相当的相似度值。所述至少一个认证设备被配置成捕捉所述个人的活体生物特征数据；接收所述个人的所述第一生物特征数据，将所述活体生物特征数据与所述第一生物特征数据进行比较，和响应于所述活体生物特征数据与所述第一生物特征数据的相似度值超过第二相似度阈值，认证所述个人。在另一个实施例中，所述自动认证系统还包括数据库系统，其中所述数据库系统远离所述至少一个验证设备和所述至少一个认证设备。所述数据库系统被配置成经由网络与所述验证设备和所述认证设备通信。此外，所述数据库系统被配置成从所述至少一个验证设备接收数据，并且使所述至少一个认证设备可以得到所述数据。

[0018] 在另一个实施例中，所述自动认证系统被配置成满足上述方法的所有特征。

[0019] 按照本发明的第三方面，提供一种计算机程序产品，它可以或者是存储有程序代码的机器可读介质的形式，或者是包括程序代码的表现的传播信号的形式，其中在计算机系统上执行的程序代码被安排为执行这里所提出的方法的各个特征。

附图说明

[0020] 实施例的后续描述基于所附的一组附图，其中相同的附图标记指示相同的元件和消息，其中：

[0021] 图1描述可能的操作环境的例子；

[0022] 图2用其主要过程步骤，表示了按照要求保护的方法的验证过程和认证过程的流程图；

[0023] 图3表示按照本发明的实施例的流程图，其中验证设备是个人的移动电话，其中不需要外部数据库，并且其中验证和认证用于准许进入音乐厅；

[0024] 图4表示按照本发明的实施例的流程图，其中验证设备是机场的自助值机终端，其中不需要移动设备作为验证设备，并且其中所使用的生物特征数据是指纹；

[0025] 图5表示按照本发明的实施例的流程图，其中验证设备是平板计算机，其中要认证的个人是需要使用厂房内的机器的员工，并且其中生物特征识别文档是上面具有虹膜扫描数据的员工ID卡；

[0026] 图6表示按照本发明的实施例的流程图，其中验证设备是与网站上的应用连接的任何设备，其中所述方法用于个人想要入境某个国家的情况，并且其中使用生物特征识别特征的组合；

[0027] 图7表示按照本发明的实施例的流程图，其中验证设备是具有相机和通信装置的任何设备，这里是移动电话，并且其中所述方法用于个人希望登机的情况。

具体实施方式

[0028] 图1图解说明例证的操作环境。按照实施例，所述环境可包括一个或多个验证设备1、一个或多个认证设备2和一个数据库系统3。验证设备1、认证设备2和数据库系统3可以通过一个或多个专用或公用网络4，例如因特网或局域网进行通信。数据库系统3包括至少一个数据库。此外，数据库系统3可以由硬件安全模块保护和/或包含以不同方式加密的数据。

[0029] 可以是桌上型计算机、膝上型计算机、平板计算机、移动电话、自助终端、智能相机系统或者任何其他适当设备的各个验证设备1可包括处理器101、存储器102、网络接口103和相机104。此外，它可以包括用户界面控制单元105，用户界面控制单元105控制相机104的使用，以及通过显示器(显示器可以是触摸屏，也可以不是触摸屏)和/或通过字母数字和光标输入设备与用户的交流。

[0030] 可以是门禁系统(access control system)、桌上型计算机、膝上型计算机，平板计算机、移动电话或者任何其他适当设备的各个认证设备2同样可以包括处理器201、存储器202、网络接口203和相机204。此外，它还可以包括用户界面控制单元205，用户界面控制单元205控制相机204的使用，以及通过显示器(显示器可以是触摸屏，也可以不是触摸屏)和/或通过字母数字和光标输入设备与用户的交流。

[0031] 验证设备1和认证设备2被安排为托管具有指令集的计算机程序，以进行如本文中所述的方法的至少一部分。具体体现记载在本文中的任何一个或全部特征的可执行指令集(即软件)完全或至少部分永久地驻留在验证设备1和/或认证设备2的存储器中。当被执行时，对应的过程数据驻留在验证设备1和/或认证设备2的存储器和/或处理器中。在一些实施例中，中央数据库系统3可以完全或部分地托管安排为实现如本文中所述的方法的各个特征的计算机程序。验证设备1和/或认证设备2还可以托管安排为实现剩余的方法特征的计算机程序。

[0032] 各个验证设备1上的计算机程序和所实现的方法步骤可以随验证设备1是何种类型而不同。同样地，在各个认证设备2上，计算机程序和所实现的方法步骤可能不同。例如，在作为验证设备1的移动电话上运行的，实现按照本发明的方法步骤的一部分的计算机程序，即“App”，可被安排为实现与在自助终端(例如在机场的自助值机终端上)运行的按照本发明的计算机程序部分不同的方法步骤。应当注意的是，期望的是提供在同一整体生物特征认证系统中使用不同的验证设备1和/或认证设备2，以及使用按照本发明的方法的可能性。

[0033] 在现在转到图3-6中的具体实施例的详细说明之前，将借助于图2给出关于要求保

护的方法的操作原理的一些概括性解释。要求保护的按照本发明的方法需要至少一个验证设备1和至少一个认证设备2。验证过程11的至少一部分在所述至少一个验证设备1上进行，而认证过程12的至少一部分在所述至少一个认证设备2上进行，其中验证过程在认证过程之前的某个时间发生。

[0034] 想要或者必须在不久的将来通过生物特征被识别和认证的个人，例如因为该个人想要出国旅行或者需要进入公共建筑物的限制区域，可以使用多个所支持的验证设备1中的一个，例如，他/她的移动电话或其他移动设备、在公共建筑物的自助终端、或者其他人的设备来开始验证过程11。

[0035] 在验证过程11的开始，在步骤2101，验证设备1捕捉活体生物特征数据作为第一登记生物特征数据。例如，所述个人拍摄自拍照，即，她/他用她/他的移动电话的内置相机拍摄她/他的面部的照片，或者所述个人将她/他的指尖放在指尖传感器上。所述个人还使用生物特征识别文档。在步骤2102，捕捉生物特征识别的图像，例如，所述个人还用她/他的移动电话拍摄其中存在生物特征数据的她/他的生物特征识别文档的一部分的照片。然后在步骤2103，判定生物特征识别文档是否真实有效。这可以通过向政府数据库查询该生物特征识别文档的唯一ID号，通过验证该生物特征识别文档的安全特征(例如全息图)通过检查有效期，通过这些技术的组合，或者通过任何其他适当的方法来完成。如果生物特征识别文档不真实和/或有效，那么验证过程在步骤2199终止。

[0036] 如果生物特征识别文档真实有效，那么验证过程11前进到步骤2103，在步骤2103，从生物特征识别文档中提取生物特征数据。例如，提取包含在生物特征识别文档中的生物特征面部照片。当然，所述登记生物特征数据和从生物特征识别文档中提取的生物特征数据通常被理解为类型相同，例如，两者都是面部照片、两者都是指纹图像、两者都是虹膜扫描和指纹图像的组合，等等。另一方面，本领域的技术人员可以想象将一个人的指纹与面部图像联系起来的数据库，在这种情况下，作为验证过程的一部分，这样的数据库会被访问。从生物特征识别文档中提取生物特征数据可以用基于具有隐马尔科夫模型和/或支持向量机的机器学习、基于快速傅立叶变换(FFT)或其他适当算法的图像分析算法来完成。

[0037] 在步骤2105，将从生物特征识别文档中提取的生物特征数据与所述登记生物特征数据进行比较。于是，计算相似度值，例如对于不相似为0，对于实质上相同的数据为1，并与相似度阈值(例如0.9)进行比较。如本领域的技术人员所知，存在不同的方式来计算这种相似度值。例如，如果比较两个面部生物特征图像，一个是作为登记生物特征数据捕捉的，一个是从生物特征识别文档中提取的，那么每个图像可以被归一化，并且可以确定特征点(landmark)，比如与人脸的眼睛、鼻子、嘴等相关的特定点。然后通过计算这些特征点之间的距离并将它们写入特征向量，可以生成特征向量。从而，来自同一个人的面部的两个图像应当具有在每个位置具有几乎相等的值的特征向量。于是，可能的相似度值可以是$\frac{1}{1+d}$，其中d是向量之间的距离，例如欧氏距离。

[0038] 如果所述登记生物特征数据和提取的生物特征数据不够相似，例如它们的相似度值没有超过预先定义的相似度阈值，那么验证过程11在步骤2199终止。如果所述登记生物特征数据和来自生物特征识别文档的对应生物特征数据，即它们的相似度值超过相似度阈值，那么在步骤2106，所述个人得到验证。所述个人的验证，即，在所述验证设备前面的个人

与该生物识别文档所属的个人相同的确认可以随在什么地方以及在什么情况下应用该方法而具有另外的效果。例如，如果验证设备是在建筑物入口的自助终端，那么验证所述个人可以导致开门；或者，如果验证设备是想要出国旅行的个人的移动电话，那么验证所述个人可以使该个人能够经由移动应用办理航班登机手续。

[0039] 在验证所述个人之后，在步骤2107有用地收集附加数据，例如姓名、出生日期、性别、常旅客号码或者驾驶证号码。在步骤2108，证实所述登记生物特征数据和附加数据。对于每种类型的数据，可以按不同的方式分别实现证实。例如，如果所述登记生物特征数据与从生物特征识别文档中提取的生物特征数据相似，并且没有发现对数据的篡改，那么可以自动证实所述登记生物特征数据，在将诸如姓名和出生日期之类的附加数据与生物特征文档上的数据进行比较之后，可以证实诸如姓名和出生日期之类的附加数据，而所述个人在旅程中向相关机构出示她/他的驾驶证之后，可以证实诸如常旅客号码之类的附加数据。证实可以在中央公钥基础设施内实现，中央公钥基础设施可以进一步用于实体之间，例如验证设备1和认证设备2之间的安全数据传送。证实的数据带来的优点是由于数据以前已经被批准，因此在认证阶段，所述个人不需要向他人展示任何文档。在验证过程11的最后步骤2109，存储证实的数据，即，已证实的登记生物特征数据和证实的附加数据。数据被存储在哪里和如何存储在很大程度上取决于所使用的特定实施例。

[0040] 验证过程11在认证过程12开始之前完成。认证过程12由要被认证的人的需求触发，例如由于音乐会举行、旅程开始、或者所述个人想要实际进入某个国家。在步骤2201，认证设备2将捕捉活体生物特征数据，即，所述个人的至少一部分的图像，例如，面部图像、指纹图像、虹膜扫描等。为了能够比较活体生物特征数据与所述个人的已证实登记生物特征数据，在步骤2202，认证设备接收存储的已证实登记生物特征数据。

[0041] 虚线2301表示数据传送。取决于方法的实施例，有许多可能的数据传送方式。例如，所述个人的已证实的登记生物特征数据可以与来自数据库的其他人的许多其他已证实的登记生物特征数据一起直接从验证设备传送，或者可以通过使用已知的标识号从数据库中明确地查询。为了增加数据安全性，传送的以及存储的登记生物特征数据还可以被加密和/或采用如用于计算相似度值的原始捕捉图像的向量化表示的形式。可取的是用于加密和/或向量化生物特征数据图像的算法由认证设备的操作者预先定义，以便在认证设备捕捉和接收的数据可以被比较，而不需要传送原始捕捉的生物特征数据。

[0042] 在认证设备2收到证实的登记生物特征数据之后，在步骤2203，将登记生物特征数据与活体生物特征数据进行比较。如果活体生物特征数据和登记生物特征数据不够相似，那么认证过程12在步骤2299终止。否则，在步骤2204认证所述个人。认证，即确认个人的身份，可以包括进一步的动作。例如，门可以打开，准许进入音乐厅或机场的安全区域。或者作为另一个例子，存储的经证实的附加数据也可被传送到认证设备。此外，在认证的需求结束之后，还可以删除任何存储的数据，以满足关于敏感生物特征数据的数据安全性的法律要求。

[0043] 由于要求保护的方法的不同实施例稍微改变了操作原理，因此图3-图6表示了用于不同验证设备和不同应用的实施例。从图3开始，图3表示了其中验证设备1是个人的移动电话，其中不需要外部数据库，并且其中验证和认证用于准许进入音乐厅的实施例。此外，用于验证和认证的生物特征数据是生物特征面部图像。其它生物特征数据也是可能的。在

这种情况下，想要将来去听音乐会的个人在她/他的移动电话上下载应用。然后，她/他可以开始验证过程11。

[0044] 在第一步骤3101，所述个人用移动电话拍摄她/他的面部的自拍照。在步骤3102，她/他还拍摄她/他的护照或者护照的至少一部分的照片。在步骤3103，检查护照是否真实有效。如果否，那么验证过程11在步骤3199终止。如果护照真实有效，那么验证过程11转到步骤3104，从护照中提取生物特征面部照片。然后在步骤3105，将提取的生物特征照片与自拍照进行比较。这里同样地，如果它们不够相似，那么验证过程11在步骤3199终止。否则，在步骤3106，验证所述个人。对于音乐会，可能需要几个数据项。验证过程11从而可以收集诸如姓名、出生日期、入场券号码之类的附加数据。这是在步骤3107完成的。然后在步骤3108证实所述数据，并在步骤3109，将所述数据仅仅本地存储在移动电话上。随即结束验证过程11。

[0045] 在音乐会的当天，例如在音乐厅的入口处，认证过程12开始。认证过程也可以进行一次、两次甚至更多次。例如，可以在音乐厅的入口处时开始一次认证过程12，在音乐厅内的安检处时开始一次认证过程12，在特殊来宾、音乐家和演员的后台区域的入口处开始一次认证过程12。然而，图3聚焦于在音乐厅的入口处的认证过程12。在步骤3201，在进入音乐厅之前，相机204拍摄个人的面部照片。在同一时刻或在此之前或之后不久，存储的经证实的自拍照从移动电话被传送到认证设备2，这示于步骤3202中。数据传送3301可以由移动电话上的应用经由网络，例如蓝牙或Wi-Fi与认证设备的自动连接来触发。

[0046] 之后，在步骤3203，将在入口拍摄的面部照片与经证实的自拍照进行比较。如果它们不够相似，那么认证过程12在步骤3299终止。如果它们足够相似，那么在步骤3204，认证所述个人。认证步骤3204可以触发进一步的动作。然后收集和证实的附加数据可以从移动电话被传送到认证设备2。例如，这可以使认证设备2能够将所述个人的经证实的姓名与特定入场券持有者的姓名进行比较，或者将经证实的入场券号码与该音乐会的所有入场券号码的列表进行比较。在步骤3205最终准许进入音乐厅之前，甚至可以进行其他步骤。

[0047] 现在进入图4的流程图，该流程图描述了其中验证设备1是机场的自助值机终端，所使用的生物特征数据是指纹的实施例。所述个人(这种情况下，乘客)到达机场，并且不需要随身携带移动设备。在自助值机终端，在步骤4101，扫描所述乘客的一个或多个指纹。在步骤4102，也扫描生物特征护照。这里，假定生物特征护照包含所述个人的一个或多个指纹的图像。在步骤4103，检查护照是否真实有效。如果否，那么验证过程11在步骤4199终止。如果护照真实有效，那么验证过程11转到步骤4104，从护照提取指纹数据。此外，在步骤4105，验证过程11提取唯一的护照ID。然后，在步骤4106，比较指纹，即，由自助值机终端扫描的指纹和从护照提取的指纹。如果它们不够相似，那么验证过程11在步骤4199终止。否则，在步骤4107，验证所述乘客。在步骤4108，收集旅行所需的更多数据，例如，姓名、出生日期、访问旅客订座记录(PNR)的订舱号等。该数据例如可以从打印的机票提取，或者由乘客手动输入。在步骤4109，该数据至少部分被证实。

[0048] 为了确保收集的作为敏感个人数据的乘客数据不被滥用，和防止未经授权的访问，在数据被存储在中央数据库之前，对数据进行加密。于是，在步骤4110，通过使用生物特征护照的唯一ID、出生日期和姓名，生成密钥。当然，也可以使用或者改为使用从生物特征护照提取的其他数据。生成这种密钥的方式例如是将姓名附加到出生日期和ID，并散列所

得到的字符串。假设姓名为“John Smith”,出生日期(格式为YYYYMMDD)为“19701020”,并且ID为“123456789ABC”,那么,所得到的字符串将是“JohnSmith19701020123456789ABC”。现在应用预定的散列算法,例如,MD5散列算法,散列将为“f6e398145b4ba7df43af39157d20ab52”。随后在步骤4111,该散列将用作密钥对数据加密。原始字符串也可以在不对其进行散列的情况下用作密钥,或者其他散列算法,比如SHA-3(Keccak)或BLAKE也是适用的。在已经加密了数据之后,在验证过程11的最后步骤4112,加密的数据被存储在中央数据库中。

[0049] 乘客随后步行穿过机场。在不同的位置,比如在安检处、在登机区域、在头等舱休息室的入口、或者在需要认证的其他区域,可以进行认证过程12。图4的流程图聚焦于准许进入飞机的登机区域。在第一步骤4201,扫描想要进入飞机的乘客的指纹。在步骤4202,乘客的护照也被扫描。在步骤4203提取唯一ID号,并在步骤4204,与诸如出生日期和姓名之类的附加数据一起用于生成密钥。应用与在验证过程中使用的相同算法。在步骤4205,从数据库接收加密的经证实的指纹扫描。数据传送4301可以通过向中央数据库查询唯一ID号来触发。然后,在步骤4206,使用生成的密钥解密所述经证实的指纹扫描。

[0050] 现在,在步骤4207,认证过程12比较想要进入飞机的乘客的当前扫描的指纹和来自验证过程11的存储的经证实的指纹。如果它们不够相似,那么认证过程12在步骤4299终止。如果它们足够相似,即,它们的相似度值超过相似度阈值,那么在步骤4208,认证所述个人。在步骤4209准许进入飞机之前,可以另外进行其他步骤。例如,可以将乘客的姓名与乘客名单进行比较,或者可以将来自PNR的数据与护照上的数据进行比较。在整个旅行结束之后,可以删除存储在外部数据库中的所有数据,以克服数据安全问题。

[0051] 图5表示其中验证设备是平板计算机,并且要认证的个人是需要使用厂房内的机器的员工的实施例的流程图。在本实施例中,生物特征识别文档是上面具有虹膜扫描数据的员工ID卡。在步骤5101,知道她/他将来需要使用机器的员工扫描她/他的虹膜中的至少一个。在步骤5102,她/他还扫描她/他的员工ID卡。在步骤5103,检查该ID卡是否真实有效。如果否,那么验证过程11在步骤5199终止。如果该ID卡真实有效,那么验证过程11转到步骤5104,并从员工ID卡提取存储的虹膜扫描。然后,在步骤5105,比较虹膜扫描。如果它们不够相似,那么验证过程11在步骤5199终止。否则,在步骤5106,验证该员工。在步骤5107,所述方法收集附加数据。该附加数据例如可以是员工的年龄,或者一天中的他可以使用机器的时间窗口。在步骤5108,所述数据的至少一部分被证实。在步骤5109,该证实的数据被本地存储在平板计算机上。

[0052] 如果员工计划使用厂房内的机器,从而在不久的将来需要认证,如步骤5110所示,并且在步骤5111,以前本地存储的经证实的数据被传送到中央数据库并存储在其中。通过提供其中验证过程11中的数据开始存储在本地,稍后被传送到中央数据库的这种两阶段存储方法,敏感生物特征数据的数据安全性主要由员工控制。只要数据只存储在本地,数据就只能由她/他访问。只有在不久的将来需要来自验证过程11的经证实的数据时,数据才被传送到中央数据库。可取的是数据库中的数据由硬件安全模块加密和/或保护,硬件安全模块即保护和管理用于强认证的数字密钥并提供进一步的加密功能的加密硬件设备,以避免滥用和保护数据免于未经授权的访问。

[0053] 如果员工随后需要使用所述机器,那么进行认证过程12。从而在本例中,认证设备2与机器紧密关联,甚至包括在机器中。在第一步骤5201,使机器可以得到多个虹膜扫描。可

能有多个员工有权使用所述机器，并且已将他们的数据传送到中央数据库。从而，使机器可以得到所有这些数据，这由多条虚线5301表示。应当广义地理解使其可得到。例如，数据可被传送到机器并存储在机器的存储器的高速缓存中，或者机器可通过网络访问其中存储数据的数据库。在步骤5202，机器扫描要认证的员工的虹膜以便使用它。在本实施例中，机器将一个(所述员工的虹膜扫描)与多个(允被许使用该机器的所有员工的虹膜扫描)进行比较，这示于步骤5203的“对于”循环中。如果找到一个匹配项，那么循环中断，并在步骤5205认证所述员工。然后允许所述员工使用该机器，这示于步骤5206中。如果没有找到匹配项，那么认证过程12在步骤5299终止。

[0054] 在图6的流程图中所示的实施例涉及所述方法在个人想要入境某个国家，并且使用多个生物特征识别特征的情况下的使用。在这种情况下，政府很可能在其托管在服务器上的网站上提供应用。在步骤6101，想要入境的个人将需要创建通常和唯一的用户ID关联的用户账户。在步骤6102，所述个人用她/他的个人计算机或者可与个人计算机连接的任何适当的附件，拍摄她/他的面部的照片，扫描她/他的指纹，以及扫描她/他的虹膜。所述个人还扫描她/他的护照，如步骤6103中所示。在步骤6104，所述方法检查护照是否真实有效。如果否，那么验证过程11在步骤6199终止。如果护照真实有效，那么验证过程11转到步骤6105，从护照提取存储的生物特征数据。假定护照上的生物特征数据包括所述个人的面部照片、指纹的图像和虹膜的图像。然后，在步骤6106，将来自护照的生物特征数据与所述个人借助于个人计算机产生的生物特征数据进行比较。如果它们不够相似，那么验证过程11在步骤6199终止。否则，在步骤6107验证所述个人。

[0055] 在验证所述个人之后，在步骤6108收集附加数据，这种情况下，姓名、出生日期、出生地和入境日期。这可以通过从护照中提取数据自动完成，和/或通过向所述个人请求信息手动完成。在步骤6109，例如通过比较手动输入的数据和政府数据库，证实所述数据。由于生物特征和个人数据是敏感数据，因此应当确保该数据不能被未经授权的人访问和读取。由于该验证过程可以从连接到因特网的任何私人设备，例如个人计算机或移动设备进行，因此必须以某种方式确保从该设备发出的数据被分配给正确的人。从而，应用基于所使用的设备的双因素认证。第一个因素是使用用户名和个人标识号(PIN)创建用户账户。第二个因素是用户账户将与用其进行验证过程的设备相联系。即，从验证设备1的特定数据(例如IP和MAC地址)生成密钥，这示于步骤6110中。在步骤6111，敏感个人数据用该密钥加密，并在步骤6112，存储在中央数据库中。从而，在不使用验证设备1的情况下，任何人都不能访问数据。

[0056] 稍后，在所述个人想要入境所述国家之前不久，进行步骤6113。所述个人然后必须主动确认她/他同意使用存储的数据。如果同意使用所存储的数据，那么所述方法再次从验证设备1提取特定数据。从而，显然必须使用与以前使用的相同的验证设备1。在步骤6114，从验证设备1的该特定数据生成密钥。在步骤6115，所存储的经过加密的经证实数据被解密，以便在认证过程12中使用。然后在步骤6116，经证实的数据随后被存储在数据库中。

[0057] 在入境日，使认证设备2可以从数据库得到多个经证实的生物特征数据集。这示于步骤6201中。在边境管制处用于这种实施例的认证设备2通常可以位于机场、港口或者另外的边界设施。在步骤6202，认证设备2拍摄想要入境的人的活体生物特征照片，扫描指纹和虹膜。对于所述多个经证实的生物特征数据集中的每一个，将活体生物特征数据与之进行

比较，这示于步骤6204中。如果没有找到类似的数据集，那么所述方法在步骤6299终止。否则，如果找到类似的数据集，那么所述个人在步骤6205被认证，并在步骤6206被允许入境所述国家。

[0058] 在另一个实施例中，特别注意存储的敏感数据(比如生物特征图像)只在有限的范围和有限的时间内被存储的事实。所述方法的验证过程11的一部分是在乘客的移动设备(这里特别是移动电话)处应用的。一些数据被传送到中央数据库系统3，并且仅在认证过程12发生的时间内，即，在这种情况下，刚好在旅行认证之前不久和认证时存储该数据。在本实施例中，认证设备2是在登机之前的登机认证站，只有被允许登机的乘客的数据才被传送到所述登机认证站。

[0059] 在图7的流程图中，描述了本实施例的方法步骤。在第一步骤7101，通过使用特定的应用(“App”)，在电话机上创建乘客的用户账户。用户账户通常将和唯一的用户ID相联系，并且与在中央数据库中创建的条目相联系。用户账户可以由用户名和密码保护。中央数据库可以存储唯一的用户ID和对应的移动电话地址的列表。通常在创建用户账户之后，立即完成一次步骤7102-7108。然而，本领域的技术人员将知道，这些步骤中的一些步骤可以更频繁地进行，例如，如果乘客收到新的生物特征文档和必须捕捉新的自拍照。

[0060] 在步骤7102，乘客用她/他的电话机的内置相机拍摄自拍照(即，他们自己的面部照片)。所述个人还用内置相机拍摄她/她的护照的照片，这示于步骤7103。在步骤7104，所述方法检查护照是否真实有效。如果否，那么验证过程11在步骤7199终止。如果护照真实有效，那么验证过程11转到步骤7105，从护照照片中提取存储的生物特征面部照片。然后，在步骤7106，将提取的生物特征照片与自拍照进行比较。如果它们不够相似，那么验证过程11在步骤7199终止。否则，在步骤7107验证所述个人。一旦照片被比较并被确定为匹配，就从护照照片中提取所述个人的数据，以填充移动电话中的应用。个人移动电话从而本地存储自拍照和所述个人的个人数据。

[0061] 同时，中央数据库优选只存储唯一的用户ID和对应的移动电话地址的列表，而不存储人自己的个人详情或照片。

[0062] 对旅行用生物特征认证来说，可能需要几个数据项。在步骤7108，验证过程11收集诸如姓名、出生日期、性别、国籍之类的基本附加数据，并将其本地存储在移动电话上。该数据可以从生物特征护照中提取，以确保不会收到虚假数据。然而，在最终的认证步骤，将只请求该信息的子集，并且以下方法确保只将所请求的信息的子集传递给请求认证的主体。不同的主体需要不同的信息。例如，第一个机场可能只需要护照号码，而第二个机场或特定的航空公司可能需要常旅客号码。

[0063] 验证过程如下继续。

[0064] 在步骤7109，收集更多的附加数据，在该实施例中，旅客订座记录(PNR)。乘客可以通过移动电话中的App输入她/他的PNR号码，所述App可以从旅行专家、运营航空公司等的数据库中查询该PNR的详情。可以提示乘客在预订时将PNR详情添加到他们的应用中。中央数据库还可以至少接收PNR参考号码，从而现在存储每个具有账户并且预订了即将到来的旅程的个人的唯一用户ID、移动电话地址和PNR参考。

[0065] 对于所有收集的数据，验证该数据正确并且未被篡改。例如，如果自拍照和生物特征护照是用同一相机，即，用同一移动电话拍摄的，那么自拍照被证实。对于从生物特征护

照中提取的数据，可以通过稍后确保数据未被篡改来进行证实，例如，如技术人员所知道的那样，使用散列。对于PNR，还可以从数据库传送证书，以确保正确性，和/或可以将PNR的数据的一部分与已在移动电话中证实的数据进行比较。步骤7110中表示了数据的这种证实。在数据的至少所需部分已被证实之后，在步骤7111，证实的数据只被本地存储在移动电话上。应用可以调用分配PNR参考的全球分销系统来确定与PNR关联的旅行的详情，并且这些详情(出发地、目的地等)可以存储在中央数据库中。

[0066] 从而，到目前为止，所有的个人数据都只存储在本地。具体地，到目前为止，电话应用现在可能存储了最少的PNR详情、乘客的照片、护照详情或许还有乘客姓名。

[0067] 下一个步骤发生在旅行之前不久，例如在旅行日期之前两天。扫描中央数据库中具有账户的所有乘客的详情，以便提取将在接下来的两天中旅行的乘客(或者将在两天之后旅行的乘客-如本领域技术人员所理解的，该参数是可修改的)的用户ID。对于提取的每个乘客，根据PNR数据，识别在乘客的旅程期间，将对乘客进行认证的机场(或其他位置)，并确定那些机场或位置(或者，具体地，那些位置的生物特征提供者，或者控制那些位置的管理机构)的个人数据要求(即，认证所需的个人数据的子集)。从而，从全球分销系统或其他安全存储设施只提取该位置所需的个人数据的子集，并将其临时保存在中央数据库中。该数据子集将在认证步骤期间用作用于确认乘客的身份证明的附加数据。

[0068] 同时，如步骤7112中所示，乘客可以主动允许应用将所述数据用于在不久的将来的旅程。如果乘客同意使用所存储的数据，例如，通过点击应用中每个输入的PNR的按钮，并且在不久的将来需要认证，例如旅程的第一个航班是第二天(或两天之后)，那么验证过程11利用由稍后使用的认证设备2的操作者提供的算法来向量化经证实的自拍照。这使得所述方法能够在不同操作者的不同认证设备，即，在不同机场和/或来自不同航空公司的不同认证设备上使用。在自拍照已被变换成向量化表示之后，在步骤7114中，验证过程11将向量化的自拍照和旅程所需的其他数据从移动电话传送到中央数据库系统3。

[0069] 在此阶段，在认证步骤之前，于是在中央数据库系统3中存储有两条数据：乘客的向量化照片和个人信息子集。这两条数据是分开存储的，并且每条数据都是与乘客的唯一用户ID一起存储的。

[0070] 在旅程的时间和日期，进行认证过程12。在第一步骤7201，使至少一个认证设备2，即，在至少一个机场的登机认证站可以得到预订该航班并且对于该航班已值机的乘客的多个经证实的向量化自拍照。应当广义地理解使其可得到。例如，数据可被传送到位于认证设备2可以进入的机场的数据库，存储在每个认证设备2的存储器的高速缓存中或在云存储器上可得到，或者它可以保留在中央数据库系统3上，并且给予认证设备特殊的临时安全访问。选择多个向量化的自拍照，以至少包括认证设备当时负责的航班，并且可以包括当天通过该机场的所有乘客，或者限制误报风险同时确保包括要认证的乘客的任何其他选择。从在验证过程11中存储的数据到认证过程12的该数据传送用虚线7301表示。在步骤7202，登机认证站的相机拍摄想要登机的乘客的面部照片。或者，用户可以用他们的照相机或移动电话拍摄他们自己的照片，并使应用可以得到所述照片。在步骤7113，利用在验证过程11中使用的相同算法变换该面部照片。在本实施例中，登机认证站将一个(面部照片的向量化表示)与多个(经证实的自拍照的向量化表示)进行比较，这示于步骤7205中的“对于”循环7204中。

[0071] 如果没有找到匹配项，那么认证过程12在步骤7299终止。如果找到一个匹配项，那么循环中断，并在步骤7206认证该乘客。登机认证站可以向乘客要求更多的数据，例如姓名、出生日期、常旅客号码等，所述更多的数据随后在步骤7207被传送到认证设备2。在该登机过程结束时，与登机认证站相连的门打开，允许乘客进入飞机，这示于步骤7208中。在步骤7209，认证过程12进一步检查旅程或旅程的相关部分是否已结束。如果是，那么在步骤7210，认证过程12删除中央数据库系统3中的所有存储的数据。

[0072] 以下第一组条款是本公开的一部分：

[0073] 1、第一组条款的认证方法，包括验证过程和认证过程，其中所述验证过程和认证过程在至少两个不同的系统上进行，其中所述验证过程的至少一部分在至少一个验证设备上进行，并且所述认证过程的至少一部分在至少一个认证设备上进行，其中所述验证过程包括：

[0074] -捕捉个人的登记生物特征数据；

[0075] -捕捉所述个人的生物特征识别文档的图像；

[0076] -响应所述生物特征识别文档真实有效：

[0077] -从所述生物特征识别文档中提取对应生物特征数据；

[0078] -将登记生物特征数据与来自所述生物特征识别文档的对应生物特征数据进行比较；和

[0079] -响应于登记生物特征数据与来自所述生物特征识别文档的对应生物特征数据的相似度值超过相似度阈值：

[0080] -验证所述个人；

[0081] -收集附加数据；

[0082] -证实登记生物特征数据和附加数据；和

[0083] -存储经证实的登记生物特征数据和经证实的附加数据；和

[0084] 其中由要被认证的个人的需求触发的认证过程包括：

[0085] -捕捉所述个人的活体生物特征数据；

[0086] -接收存储的所述个人的经证实的登记生物特征数据；

[0087] -将活体生物特征数据与经证实的登记生物特征数据进行比较；和

[0088] -响应于活体生物特征数据与经证实的登记生物特征数据的相似度值超过相似度阈值，认证所述个人。

[0089] 2、第一组条款的条款1的认证方法，其中所述验证设备中的至少一个是所述个人的移动设备，并且其中在所述验证过程中，存储经证实的登记生物特征数据和经证实的附加数据包括将经证实的数据存储在所述个人的移动设备上，其中在所述认证过程中，接收所述个人的经证实的登记数据包括将经证实的登记生物特征数据从所述个人的移动设备传送到所述认证设备。

[0090] 3、第一组条款的条款1或2的认证方法，其中所述验证设备中的至少一个是自助终端，并且其中在所述自助终端上进行的验证过程还包括：

[0091] -获得标识号，其中所述标识号是从所述生物特征识别文档中提取的唯一标识号；

[0092] -响应于登记生物特征数据与来自所述生物特征识别文档的对应生物特征数据的相似度值超过相似度阈值：

[0093] -使用所述附加数据生成密钥；

[0094] -用从所述附加数据生成的密钥，加密经证实的登记生物特征数据和经证实的附加数据；和

[0095] -将加密的经证实的登记生物特征和加密的经证实的附加数据与所述标识号一起存储在中央数据库中；和

[0096] 其中在所述认证过程中，接收所述个人的经证实的登记数据包括：

[0097] -捕捉所述个人的认证生物特征识别文档的图像；

[0098] -从所述认证生物特征识别文档中提取认证附加数据；

[0099] -从该生物特征文档中提取认证标识号，其中认证标识号是从所述认证生物特征识别文档中提取的唯一标识号；

[0100] -利用所述认证附加数据生成密钥；

[0101] -使用所述认证标识号，向中央数据库请求所存储的加密的经证实的登记生物特征；和

[0102] -用从所述认证附加数据生成的密钥，解密所述加密的经证实的登记生物特征数据。

[0103] 4、第一组条款的条款1-3任意之一的认证方法，其中所述验证设备中的至少一个是所述个人的移动设备，并且其中在所述验证过程中，所述经证实的登记生物特征数据和经证实的附加数据被存储在所述个人的移动设备上；并且其中响应于所述个人通告在不久的将来需要被认证，所述验证过程还包括：

[0104] -获得标识号；和

[0105] -将所述经证实的登记生物特征数据和经证实的附加数据连同所述标识号一起存储在中央数据库中。

[0106] 5、第一组条款的条款1-4任意之一的认证方法，其中所述验证过程还包括：

[0107] -从所述验证设备提取所述验证设备特有的数据；

[0108] -使用从所述验证设备提取的数据生成密钥；

[0109] -用从提取的数据生成的密钥，加密经证实的登记生物特征数据和经证实的附加数据；和

[0110] -将加密的经证实的登记生物特征数据和经证实的附加数据存储在中央数据库中；

[0111] -响应于所述个人通告他们在不久的将来需要被认证，请求同意使用包括加密的经证实的登记生物特征数据和经证实的附加数据的存储数据；和

[0112] -响应于获得所述个人同意使用所述存储数据，用从提取自所述验证设备的数据生成的密钥，解密所述加密的经证实的登记生物特征数据和经证实的附加数据。

[0113] 6、第一组条款的条款4或5的认证方法，其中所述认证过程还包括：

[0114] -使认证设备可以从中央数据库得到要认证的个人的多个经证实的登记生物特征数据；和

[0115] 其中接收所述个人的所述经证实的登记生物特征数据包括将所述多个经证实的登记生物特征数据与捕捉的所述个人的活体生物特征数据进行比较，并且响应于所述多个经证实的登记生物特征数据之一与所述活体生物特征数据相似，选择所述相似的经证实的

登记生物特征数据作为所述个人的登记生物特征数据。

[0116] 7、条款3-6任意之一的认证方法，其中所述数据库由硬件安全模块保护，和/或存储在所述数据库中的数据被加密。

[0117] 8、第一组条款的条款1-7任意之一的认证方法，其中登记生物特征数据、来自生物特征识别文档的生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合，和/或其中所述附加数据包括从生物特征文档中提取的数据、手动输入的数据、从第三方取回的数据、或者它们的组合。

[0118] 9、第一组条款的条款1-8任意之一的认证方法，其中登记生物特征数据、来自生物特征识别文档的生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合的向量化表示，并且其中用于向量化数据的算法由所述认证设备的操作者预先定义。

[0119] 10、第一组条款的条款1-9任意之一的认证方法，其中捕捉登记生物特征数据和/或捕捉活体生物特征数据包括拍摄所述个人的至少一部分的照片，和/或其中捕捉生物特征识别文档的图像包括拍摄所述生物特征识别文档的照片，或者扫描所述生物特征识别文档。

[0120] 11、第一组条款的条款1-10任意之一的认证方法，其中响应于认证的需求结束，删除任何数据。

[0121] 12、第一组条款的条款1-11任意之一的认证方法，其中认证所述个人包括准许进入区域、将经证实的附加数据传送到所述认证设备、解密经证实的附加数据、或者它们的组合中的至少一个。

[0122] 13、第一组条款的条款1-12任意之一的认证方法，其中所述验证过程还包括生成与所述个人的唯一用户ID关联的用户账户，其中所述用户账户由用户名和PIN保护。

[0123] 14、第一组条款的用于认证个人的自动认证系统，包括：

[0124] -至少一个验证设备；

[0125] -至少一个认证设备；

[0126] 其中所述至少一个验证设备远离所述至少一个认证设备；其中所述至少一个验证设备和所述至少一个认证设备被配置成经由网络进行通信；和其中所述至少一个验证设备被配置成：

[0127] -捕捉个人的登记生物特征数据；

[0128] -捕捉所述个人的生物特征识别文档的图像；

[0129] -响应于所述生物特征识别文档真实有效：

[0130] -从所述生物特征识别文档中提取对应生物特征数据；

[0131] -将登记生物特征数据与来自所述生物特征识别文档的对应生物特征数据进行比较；和

[0132] -响应于登记生物特征数据与来自所述生物特征识别文档的对应生物特征数据的相似度值超过相似度阈值：

[0133] -验证所述个人；

[0134] -收集附加数据；

[0135] -证实登记生物特征数据和附加数据；和

[0136] -存储经证实的登记生物特征数据和经证实的附加数据;和

[0137] 其中认证设备被配置成:

[0138] -捕捉所述个人的活体生物特征数据;

[0139] -接收存储的所述个人的经证实的登记生物特征数据;

[0140] -将活体生物特征数据与经证实的登记生物特征数据进行比较;和

[0141] -响应于活体生物特征数据与经证实的登记生物特征数据的相似度值超过相似度阈值,认证所述个人。

[0142] 15、第一组条款的条款14的自动认证系统还包括数据库系统,其中所述数据库系统远离所述至少一个验证设备和所述至少一个认证设备;其中所述数据库系统被配置成经由网络与所述验证设备和所述认证设备进行通信;并且其中所述数据库系统被配置成:

[0143] -从所述至少一个验证设备接收数据;和

[0144] -使所述至少一个认证设备可以得到所述数据。

[0145] 16、第一组条款的条款14或15的自动认证系统,还被配置成执行第一组条款的条款2-13任意之一的特征。

[0146] 17、第一组条款所述的计算机程序,包括用于执行按照第一组条款的条款1-13的方法的特征的程序代码指令。

[0147] 以下第二组条款是本公开的一部分:

[0148] 1、第二组条款的认证方法,包括验证过程和认证过程,其中所述验证过程和认证过程在至少两个不同的系统上进行,其中所述验证过程的至少一部分在至少一个验证设备上进行,并且所述认证过程的至少一部分在至少一个认证设备上进行,其中所述认证过程包括:

[0149] -捕捉个人的第一生物特征数据;

[0150] -从生物特征识别文档中提取第二生物特征数据;

[0151] -将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较,以获得与第一相似度阈值相当的相似度,

[0152] 其中所述认证过程包括:

[0153] -捕捉所述个人的活体生物特征数据;

[0154] -接收所述个人的所述第一生物特征数据;

[0155] -将活体生物特征数据与第一生物特征数据进行比较;和

[0156] -响应于活体生物特征数据与所述第一生物特征数据的相似度值超过相似度阈值,认证所述个人。

[0157] 2、第二组条款的条款1的认证方法,其中所述验证过程还包括,响应于第一生物特征数据与第二生物特征数据相比的相似度值超过第一相似度阈值,

[0158] -验证所述个人的身份;

[0159] -收集附加数据;

[0160] -证实所述第一生物特征数据和附加数据;和

[0161] -存储经证实的第一生物特征数据和经证实的附加数据。

[0162] 3、第二组条款的条款2的认证方法,其中所述至少一个验证设备是所述个人的移动设备,并且其中在所述验证过程中,存储第一生物特征数据和经证实的附加数据包括将

经证实的数据存储在所述个人的移动设备上，并且其中在所述认证过程中，接收所述个人的经证实的第一数据包括将经证实的第一生物特征数据从所述个人的移动设备传送到所述认证设备。

[0163] 4、第二组条款的条款2或3的认证方法，其中所述至少一个验证设备是自助终端，并且其中在所述自助终端上进行的验证过程还包括：

[0164] -获得标识号，其中所述标识号是从所述生物特征识别文档中提取的唯一标识号；

[0165] -响应于所述第一生物特征数据与来自所述生物特征识别文档的对应第二生物特征数据的相似度值超过相似度阈值：

[0166] -使用所述附加数据生成密钥；

[0167] -用从所述附加数据生成的密钥，加密所述经证实的第一生物特征数据和经证实的附加数据；和

[0168] -将加密的经证实的登记生物特征和加密的经证实的附加数据与所述标识号一起存储在中央数据库中；和

[0169] 其中在所述认证过程中，接收所述个人的经证实的第一数据包括：

[0170] -捕捉所述个人的认证生物特征识别文档的图像；

[0171] -从所述认证生物特征识别文档中提取认证附加数据；

[0172] -从该生物特征文档中提取认证标识号；

[0173] -利用所述认证附加数据生成密钥；

[0174] -使用所述认证标识号，向中央数据库请求所存储的加密的经证实的第一生物特征数据；和

[0175] -用从所述认证附加数据生成的密钥，解密加密的经证实的第一生物特征数据。

[0176] 5、第二组条款的条款2-4任意之一的认证方法，其中所述至少一个验证设备是所述个人的移动设备，并且其中在所述验证过程中，所述经证实的第一生物特征数据和经证实的附加数据被存储在所述个人的移动设备上，并且其中响应于所述个人通告他们在不久的将来需要被认证，所述验证过程还包括：

[0177] -获得标识号；和

[0178] -将所述经证实的第一生物特征数据和经证实的附加数据连同所述标识号一起存储在中央数据库中。

[0179] 6、第二组条款的条款2-5任意之一的认证方法，其中所述验证过程还包括：

[0180] -使用从所述验证设备提取的数据生成密钥；

[0181] -用从提取的数据生成的密钥，加密经证实的第一生物特征数据和经证实的附加数据；和

[0182] -将加密的经证实的第一生物特征数据和经证实的附加数据存储在中央数据库中；

[0183] -响应于所述个人通告他们在不久的将来需要被认证，请求同意使用包括加密的经证实的第一生物特征数据和经证实的附加数据的存储数据；和

[0184] -响应于获得所述个人同意使用所述存储数据，用从提取自所述验证设备的数据生成的密钥，解密所述加密的经证实的第一生物特征数据和经证实的附加数据。

[0185] 7、第二组条款的条款5或6的认证方法，其中所述认证过程还包括：

[0186] -使认证设备可以从中央数据库得到要认证的个人的多个经证实的第一生物特征数据项;和

[0187] 其中接收所述个人的所述经证实的第一生物特征数据包括将所述多个经证实的第一生物特征数据项与捕捉的所述个人的活体生物特征数据进行比较,并且响应于所述多个经证实的第一生物特征数据之一与所述活体生物特征数据相似,选择所述相似的经证实的第一生物特征数据作为所述个人的第一生物特征数据。

[0188] 8、第二组条款的条款4-7任意之一的认证方法,其中所述中央数据库由硬件安全模块保护,和/或存储在所述中央数据库中的数据被加密。

[0189] 9、第二组条款的条款1-8任意之一的认证方法,其中第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合。

[0190] 10、第二组条款的条款2-9任意之一的认证方法,其中所述附加数据包括从生物特征文档中提取的数据、手动输入的数据、从第三方取回的数据、或者它们的组合。

[0191] 11、第二组条款的条款1-10任意之一的认证方法,其中第一生物特征数据、来自生物特征识别文档的第二生物特征数据和活体生物特征数据包括生物特征面部图像、虹膜扫描、指纹图像、或者它们的组合的向量化表示,并且其中用于使数据向量化的算法由所述认证设备的操作者预先定义。

[0192] 12、第二组条款的条款1-11任意之一的认证方法,其中捕捉所述第一生物特征数据和/或捕捉所述活体生物特征数据包括拍摄所述个人的至少一部分的照片,和/或其中从所述生物特征识别文档提取第二生物特征数据包括捕捉生物特征识别文档的图像,这包括拍摄生物特征识别文档的照片、扫描生物特征识别文档、或者视觉检查生物特征识别文档。

[0193] 13、第二组条款的条款1-12任意之一的认证方法,其中当认证的需求结束时,删除任何接收的数据。

[0194] 14、第二组条款的条款1-13任意之一的认证方法,其中认证所述个人包括准许进入区域、将经证实的附加数据传送到所述认证设备、解密经证实的附加数据、或者它们的组合中的至少一个。

[0195] 15、第二组条款的条款1-14任意之一的认证方法,其中所述验证过程还包括生成与所述个人的唯一用户ID关联的用户账户,其中所述用户账户由用户名和PIN保护。

[0196] 16、第二组条款的用于认证个人的自动认证系统,包括:

[0197] -至少一个验证设备;和

[0198] -至少一个认证设备;

[0199] 其中所述至少一个验证设备远离所述至少一个认证设备;其中所述至少一个验证设备和所述至少一个认证设备被配置成经由网络进行通信;并且其中所述至少一个验证设备被配置成:

[0200] -捕捉个人的第一生物特征数据;

[0201] -从生物特征识别文档中提取第二生物特征数据;和

[0202] -将第一生物特征数据与来自生物特征识别文档的对应第二生物特征数据进行比较;和

[0203] 其中所述至少一个认证设备被配置成:

[0204] -捕捉所述个人的活体生物特征数据；

[0205] -接收所述个人的所述第一生物特征数据；

[0206] -将活体生物特征数据与第一生物特征数据进行比较；和

[0207] -响应于所述活体生物特征数据与所述第一生物特征数据的相似度值超过相似度阈值，认证所述个人。

[0208] 17、第二组条款的条款14的自动认证系统，还包括数据库系统，其中所述数据库系统远离所述至少一个验证设备和所述至少一个认证设备；其中所述数据库系统被配置成经由网络与所述验证设备和所述认证设备通信，并且其中所述数据库系统被配置成：

[0209] -从所述至少一个验证设备接收数据；和

[0210] -使所述至少一个认证设备可以得到所述数据。

[0211] 18、第二组条款的条款16或17的自动认证系统，还被配置成实现第二组条款的条款2-15任意之一的特征。

[0212] 19、第二组条款所述的计算机程序，包括用于实现按照第二组条款的条款1-15的方法的特征的程序代码指令。

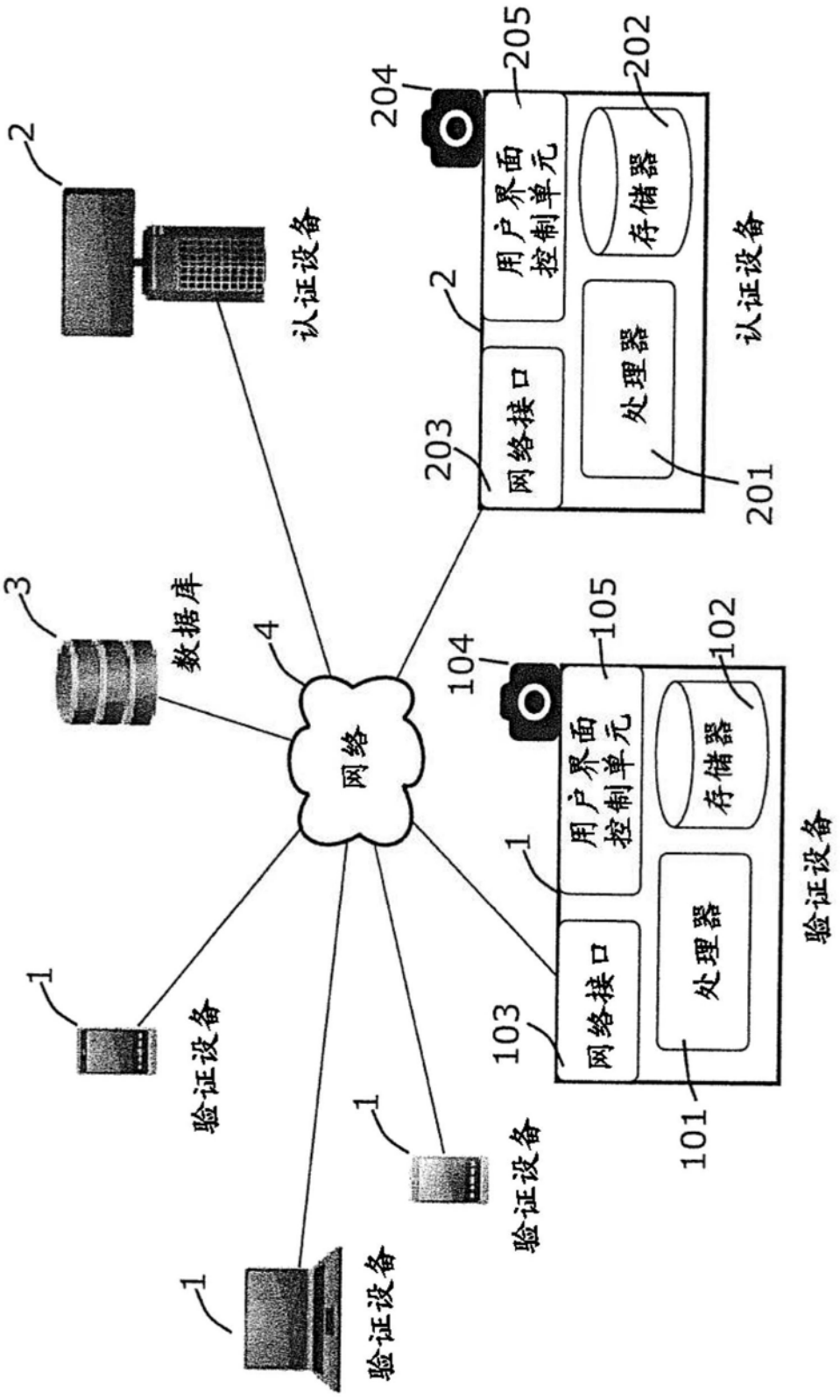

2
认证设备
3
数据库
4
网络
1
验证设备
1
验证设备
1
验证设备
204
205
202
用户界面控制单元
存储器
2
处理器
认证设备
203
网络接口
201
104
105
102
用户界面控制单元
存储器
1
网络接口
处理器
103
101
验证设备

图1

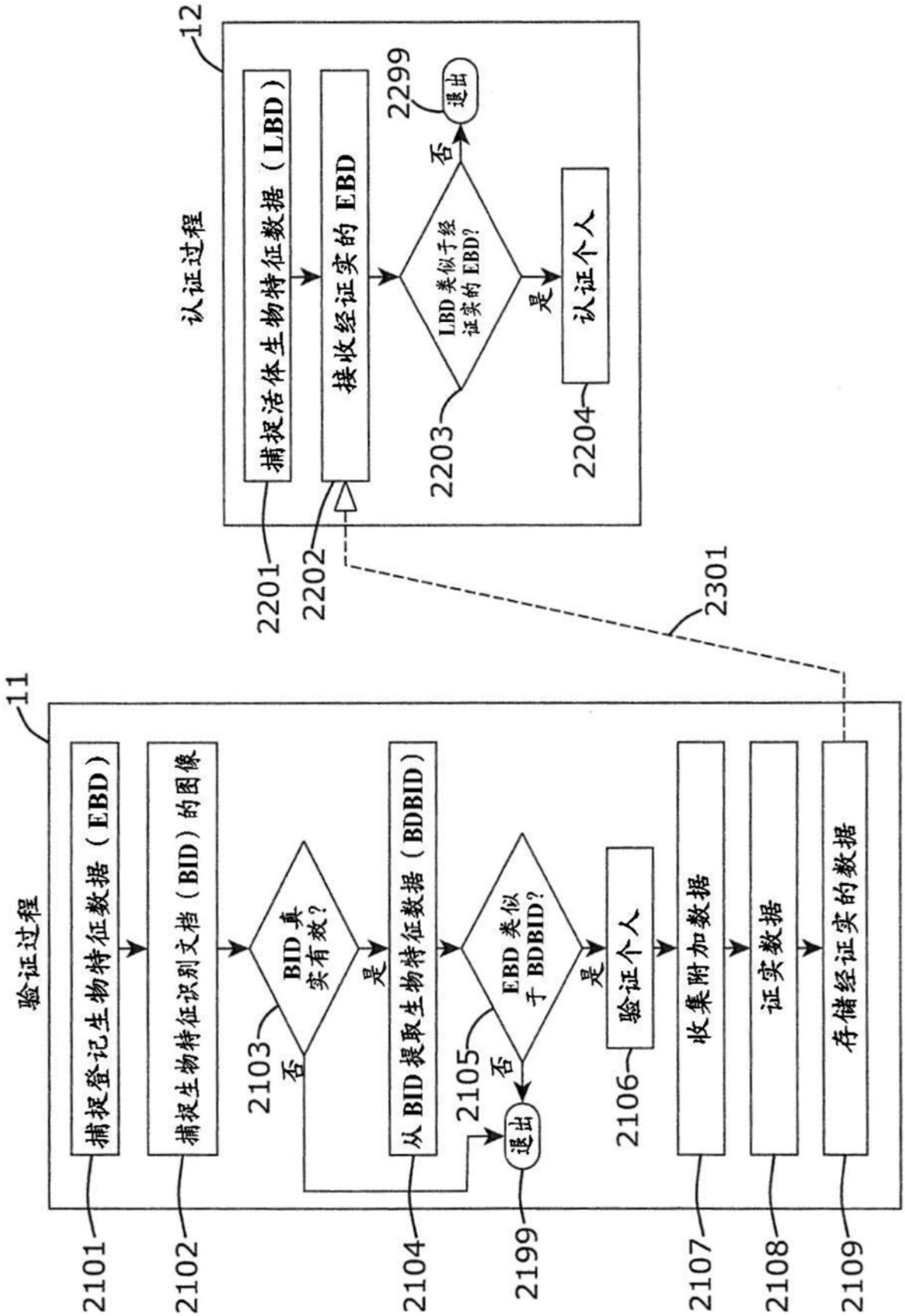

12
认证过程
捕捉活体生物特征数据（LBD）
接收经证实的 EBD
LBD 类似于经证实的 EBD?
否
是
退出
认证个人
2201
2202
2203
2204
2299
2301
11
验证过程
捕捉登记生物特征数据（EBD）
捕捉生物特征识别文档（BID）的图像
BID 真实有效?
否
是
从 BID 提取生物特征数据（BDBID）
EBD 类似于 BDBID?
否
是
退出
验证个人
收集附加数据
证实数据
存储经证实的数据
2101
2102
2103
2104
2105
2106
2107
2108
2109
2199

图2

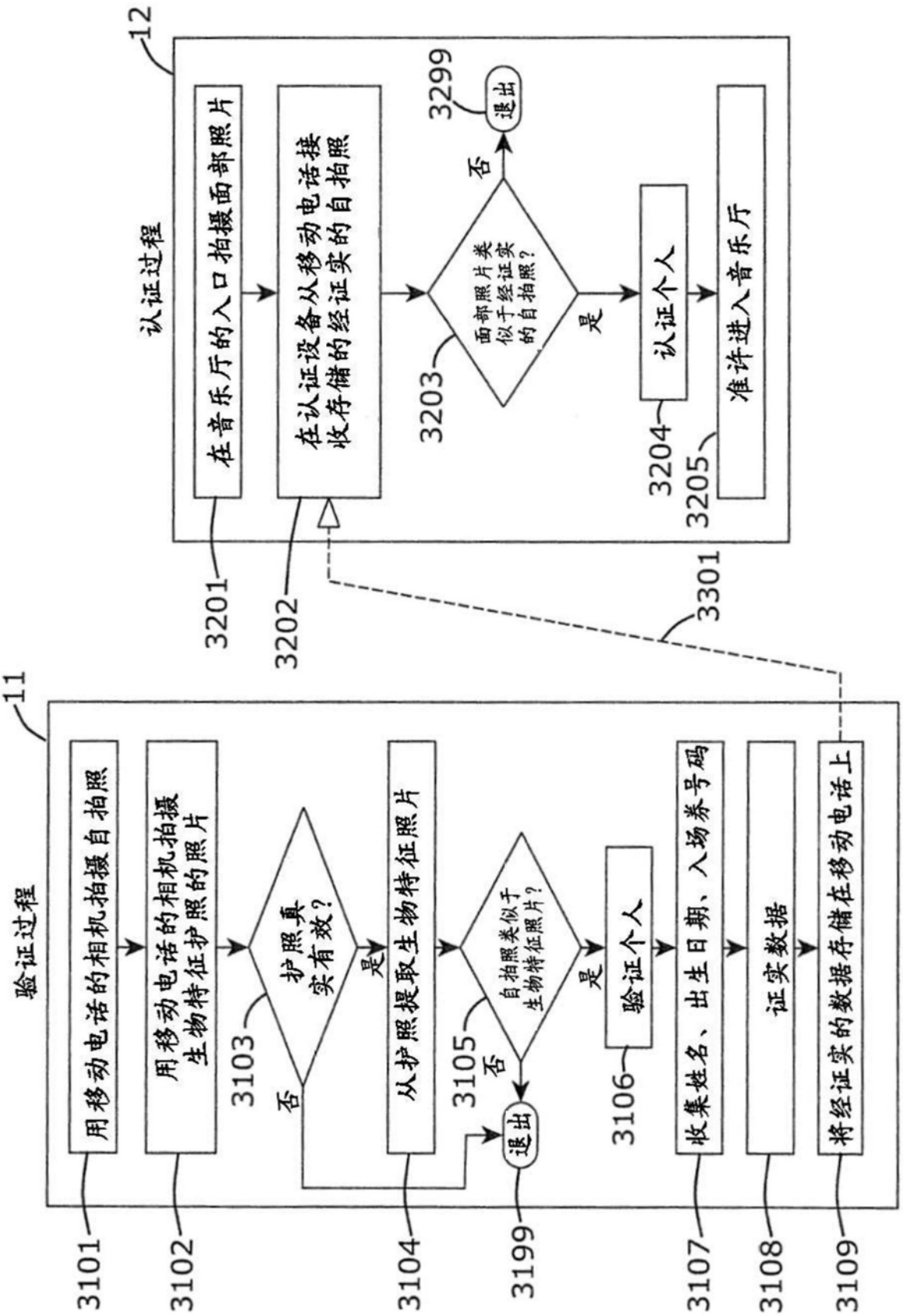

12
认证过程
在音乐厅的入口拍摄面部照片
在认证设备从移动电话接收存储的经证实的自拍照
面部照片类似于经证实的自拍照?
否
是
退出
认证个人
准许进入音乐厅
3201
3202
3203
3204
3205
3299
3301
11
验证过程
用移动电话的相机拍摄自拍照
用移动电话的相机拍摄生物特征护照的照片
护照真实有效?
否
是
从护照提取生物特征照片
自拍照类似于生物特征照片?
否
是
退出
验证个人
收集姓名、出生日期、入场券号码
证实数据
将经证实的数据存储在移动电话上
3101
3102
3103
3104
3105
3106
3107
3108
3109
3199

图3

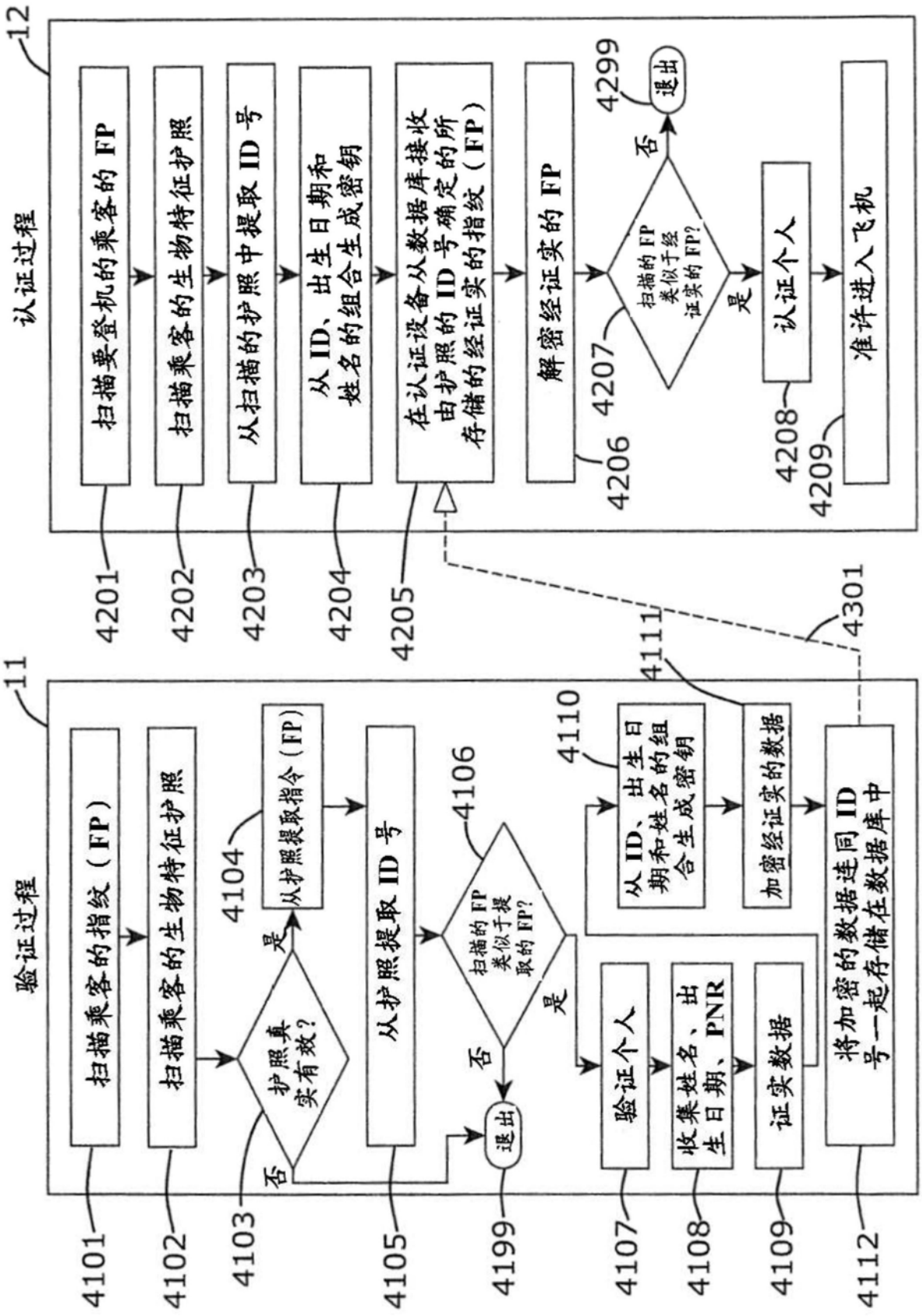

12
认证过程
扫描要登机的乘客的 FP
扫描乘客的生物特征护照
从扫描的护照中提取 ID 号
从 ID、出生日期和姓名的组合生成密钥
在认证设备从数据库接收由护照的 ID 号确定的所存储的经证实的指纹（FP）
解密经证实的 FP
扫描的 FP 类似于经证实的 FP?
否
是
退出
认证个人
准许进入飞机
4201
4202
4203
4204
4205
4206
4207
4208
4209
4299
4301
11
验证过程
扫描乘客的指纹（FP）
扫描乘客的生物特征护照
护照真实有效？
否
是
从护照提取指令（FP）
从护照提取 ID 号
扫描的 FP 类似于提取的 FP?
否
是
退出
从 ID、出生日期和姓名的组合生成密钥
加密经证实的数据
验证个人
收集姓名、出生日期、PNR
证实数据
将加密的数据连同 ID 号一起存储在数据库中
4101
4102
4103
4104
4105
4106
4199
4110
4111
4107
4108
4109
4112

图4

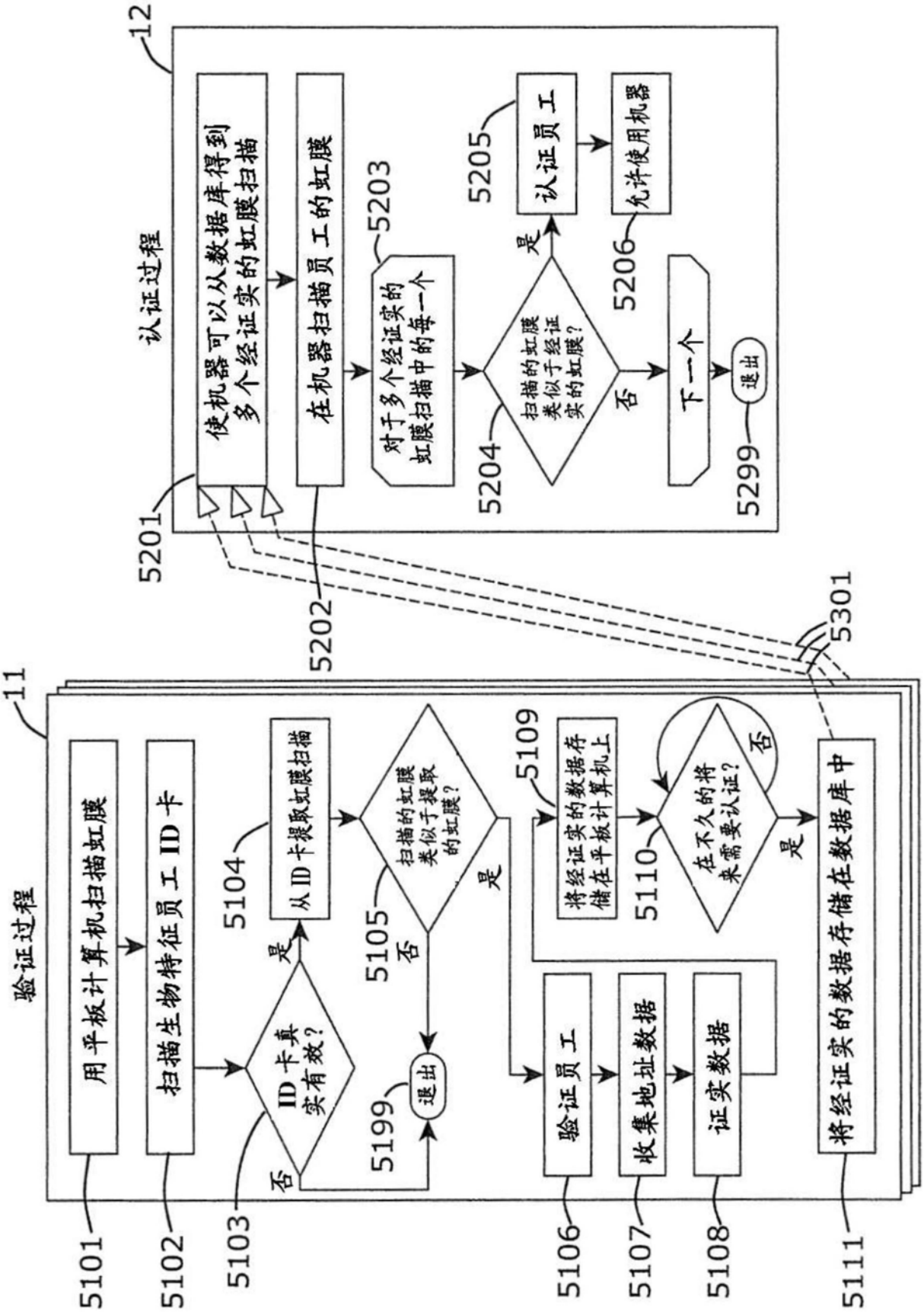

12
认证过程
使机器可以从数据库得到多个经证实的虹膜扫描
在机器扫描员工的虹膜
对于多个经证实的虹膜扫描中的每一个
扫描的虹膜类似于经证实的虹膜?
认证员工
允许使用机器
下一个
退出
5201
5202
5203
5204
5205
5206
5299
是
否
5301
11
验证过程
用平板计算机扫描虹膜
扫描生物特征员工ID卡
ID卡真实有效?
从ID卡提取虹膜扫描
扫描的虹膜类似于提取的虹膜?
退出
将经证实的数据存储在平板计算机上
在不久的将来需要认证?
验证员工
收集地址数据
证实数据
将经证实的数据存储在数据库中
5101
5102
5103
5104
5105
5106
5107
5108
5109
5110
5111
5199
是
否

图5

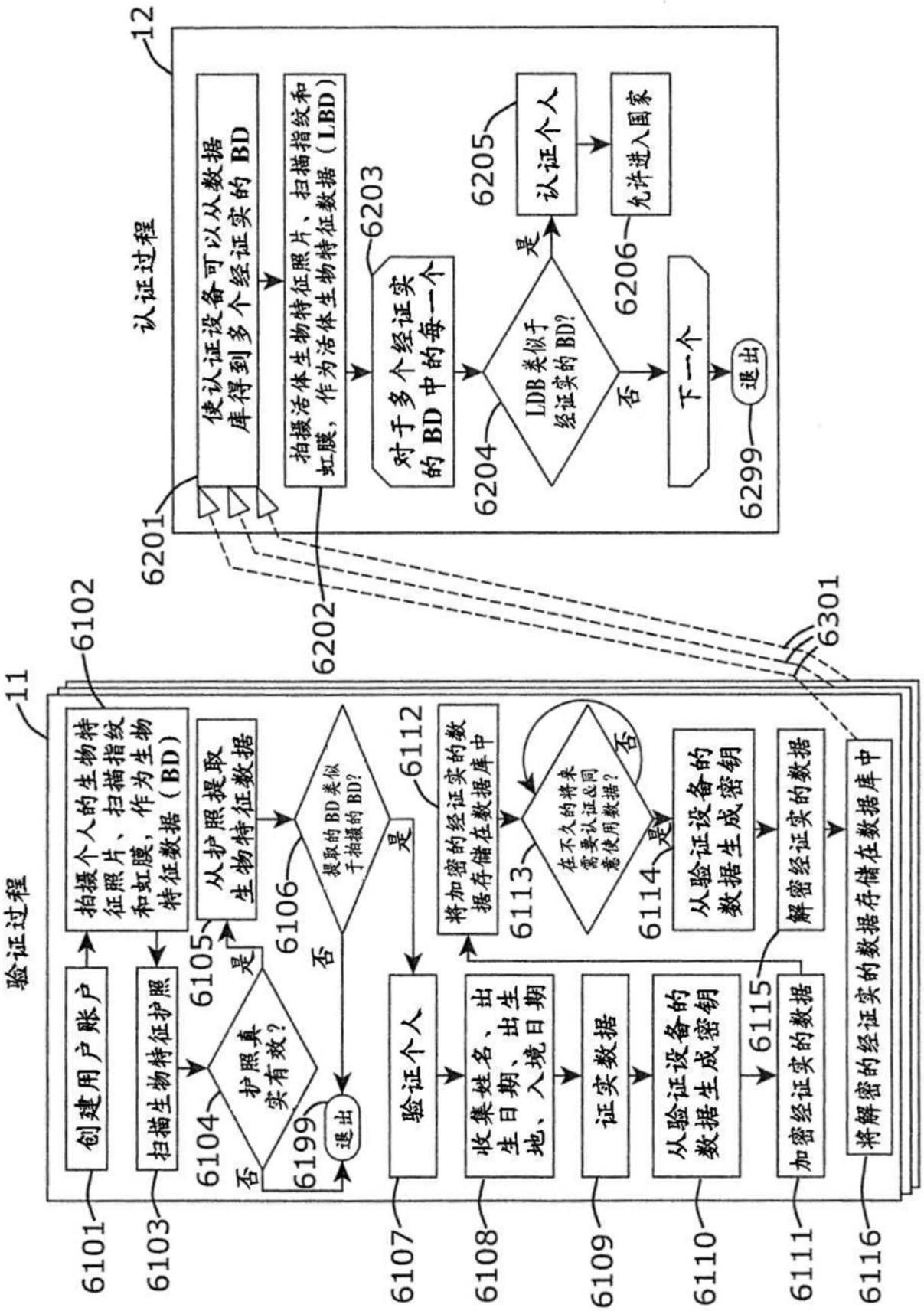

12
认证过程
使认证设备可以从数据库得到多个经证实的 BD
拍摄活体生物特征照片、扫描指纹和虹膜，作为活体生物特征数据（LBD）
对于多个经证实的 BD 中的每一个
LDB 类似于经证实的 BD?
是
否
认证个人
允许进入国家
下一个
退出
6201
6202
6203
6204
6205
6206
6299
6301
11
验证过程
创建用户账户
扫描生物特征护照
拍摄个人的生物特征照片、扫描指纹和虹膜，作为生物特征数据（BD）
护照真实有效?
从护照提取生物特征数据
提取的 BD 类似于拍摄的 BD?
退出
验证个人
收集姓名、出生日期、出生地、入境日期
证实数据
从验证设备的数据生成密钥
加密经证实的数据
将加密的经证实的数据存储在数据库中
在不久的将来需要认证&同意使用数据?
从验证设备的数据生成密钥
解密经证实的数据
将解密的经证实的数据存储在数据库中
6101
6102
6103
6104
6105
6106
6107
6108
6109
6110
6111
6112
6113
6114
6115
6116
6199

图6

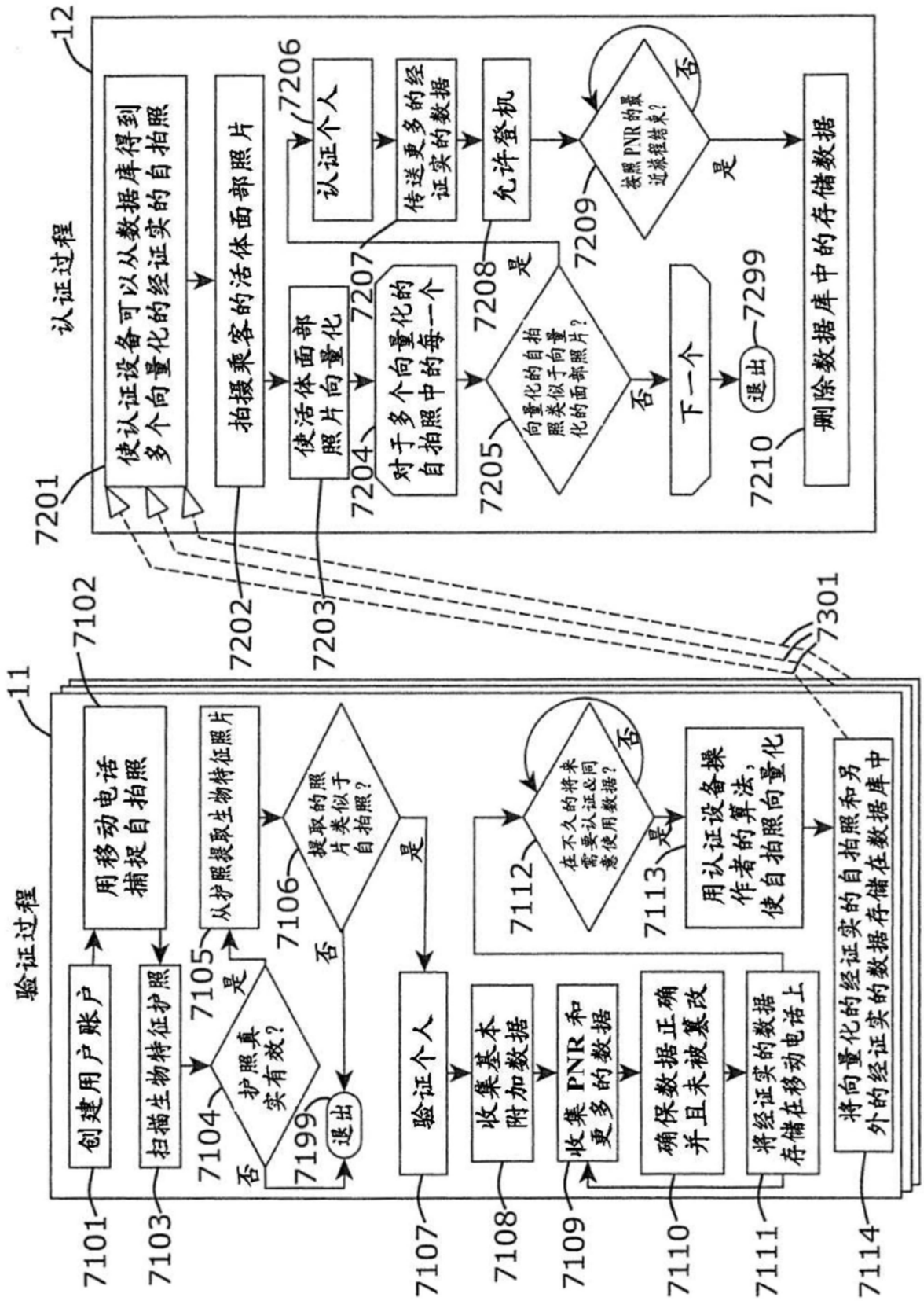

12
认证过程
使认证设备可以从数据库得到多个向量化的经证实的自拍照
拍摄乘客的活体面部照片
使活体面部照片向量化
对于多个向量化的自拍照中的每一个
向量化的自拍照类似于向量化的面部照片?
否
是
下一个
退出
允许登机
传送更多的经证实的数据
认证个人
按照PNR的票证旅程结束?
否
是
删除数据库中的存储数据
7201
7202
7203
7204
7205
7206
7207
7208
7209
7210
7299
7301
11
验证过程
创建用户账户
用移动电话捕捉自拍照
扫描生物特征护照
从护照提取生物特征照片
护照真实有效?
否
是
退出
提取的照片类似于自拍照?
否
是
验证个人
收集基本附加数据
收集PNR和更多的数据
确保数据正确并且未被篡改
将经证实的数据存储在移动电话上
在不久的将来需要认证&同意使用数据?
否
是
用认证设备操作者的算法,使自拍照向量化
将向量化的经证实的自拍照和另外的经证实的数据存储在数据库中
7101
7102
7103
7104
7105
7106
7107
7108
7109
7110
7111
7112
7113
7114
7199

图7