(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 110870283 A
(43)申请公布日 2020.03.06

(21)申请号 201880046172.9

(22)申请日 2018.04.25

(30)优先权数据
1707471.7 2017.05.10 GB

(85)PCT国际申请进入国家阶段日
2020.01.10

(86)PCT国际申请的申请数据
PCT/GB2018/051088 2018.04.25

(87)PCT国际申请的公布数据
WO2018/206912 EN 2018.11.15

(71)申请人 PQ解决方案有限公司
地址 英国伦敦

(72)发明人 马丁·汤姆林森 郑毓辉 蔡增荣

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 杨贝贝 臧建明

(51)Int.Cl.
H04L 29/06(2006.01)
G09C 1/00(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

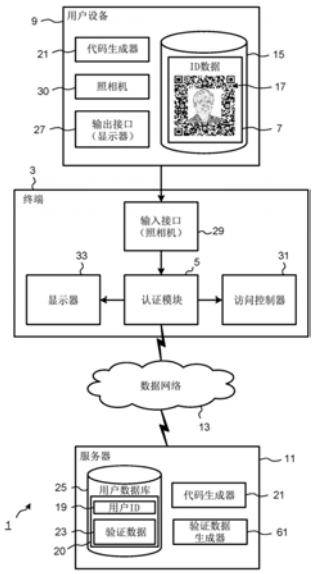
权利要求书3页 说明书14页 附图13页

(54)发明名称

数据验证

(57)摘要

描述了用于用户身份和交易认证的系统和方法。在一个实施例中，通过配置为处理二维代码的图像数据以解码密钥信息的终端对用户进行认证，该二维代码包括用户凭证与存储在安全服务器上的数据库用户信息的加密绑定，该用户凭证包括用户面部的低分辨率图像以及可选地，用户生物特征数据。二维代码的哈希被设置为与存储在安全服务器上的用户信息的哈希具有共同的数个数位。通过计算和比较哈希值，将从安全服务器获取的用户面部的高分辨率图像与用户以及嵌入在二维代码中的低分辨率图像进行比较，以进行认证。在其它实施例中，该二维代码是在用户设备上生成的，作为交易的证明，并且可以随后用作入场券或商业合同的输出。



CN 110870283 A

1.一种数据验证方法,包括由一个或多个计算设备执行的以下步骤:

接收定义二维代码的代码数据,所述二维代码包括表示可用于标识用户的数据的图像的图形元素;

检索与所述用户相关联的验证数据;

至少根据接收到的代码数据中的所述图像的所述图形元素计算第一密码哈希值;

根据所述验证数据计算第二密码哈希值;以及

基于所述第一密码哈希值与所述第二密码哈希值的比较,验证所述接收的代码数据的可靠性。

2.根据权利要求1所述的方法,其中,所述二维代码还包括来自纠错码的奇偶校验符号和/或与所述图像相关联的辅助数据。

3.根据权利要求1或2所述的方法,其中,所述代码数据是从标识所述用户的源数据生成的,并且其中,所述验证数据包括源数据的操作版本,由此,所述计算的第一和第二密码哈希值满足定义的对应关系。

4.根据权利要求3所述的方法,其中,所述代码数据定义二维代码,所述二维代码包括表示用户的一个或多个可见、独特和可测量特征的图像的图形元素。

5.根据权利要求4所述的方法,其中,所述源用户标识数据包括所述二维代码中的所述图像的高分辨率版本,并且其中,表示所述用户的可见特征的所述图像的所述图形元素是根据所述源数据中所述图像的高分辨率版本获得的。

6.根据权利要求4或5所述的方法,其中,所述操作版本是通过以隐写方式改变所述图像数据直到所述计算的第一和第二密码哈希值满足所述定义的对应关系生成的。

7.根据权利要求3所述的方法,其中,所述源数据包括用户提供的信息或与所述用户相关联的生物特征数据。

8.根据权利要求3所述的方法,其中,所述源数据包括与所述用户相关联的交易数据。

9.根据权利要求3-8中任一项所述的方法,其中,所述对应关系定义所述计算的第一和第二密码哈希值之间的共同数位。

10.根据权利要求3-8中任一项所述的方法,其中,所述对应关系定义所述计算的第一和第二密码哈希值的数位之间的数学关系。

11.根据权利要求9或10所述的方法,还包括:比较所述密码哈希值以定位和验证所述共同数位。

12.根据前述权利要求中任一项所述的方法,还包括:确定所接收的代码数据的区域,所述接收的代码数据包括表示所述用户的标识特征的图像的图形元素,其中,所述第一密码哈希值是根据所确定的区域中的数据值计算的。

13.根据前述权利要求中任一项所述的方法,其中,所述接收的代码数据包括从照相机捕获的图像数据。

14.根据前述权利要求中任一项所述的方法,还包括:处理所述接收的代码数据以对用户信息进行解码。

15.根据权利要求14所述的方法,其中,所述验证数据是基于所述解码的用户信息从远程数据库检索的。

16.根据权利要求15所述的方法,还包括:基于所述解码的用户信息确定解密密钥。

17.根据权利要求15所述的方法，其中，所述解码的用户信息包括所述解密密钥。

18.根据权利要求16或17所述的方法，其中，所述验证数据包括所述用户的标识特征的加密图像数据，并且其中，所述方法还包括：使用所述解密密钥对所述检索到的加密图像数据进行解密。

19.根据前述权利要求中任一项所述的方法，其中，所述二维代码包括表示所述用户的低分辨率图像的图形元素，所述方法还包括：执行图像处理以根据所述二维代码中的低分辨率图像和所述检索到的验证数据中的对应的高分辨率图像验证所述用户的标识数据的至少一个特征。

20.根据权利要求19所述的方法，其中，所述存储的数据还包括与所述用户相关联的简档数据，并且其中，所述方法还包括：相对于所述存储的简档数据验证所述至少一个特征。

21.根据前述权利要求中任一项所述的方法，还包括根据用户提供的信息或与所述用户相关联的生物特征数据计算第三密码哈希值，其中，基于所述第一、第二和第三密码哈希值的比较验证所述代码数据。

22.一种生成二维代码数据的方法，所述二维代码数据以密码方式绑定到相关联的用户的验证数据，所述方法包括：

将源数据编码为二维代码，所述二维代码包括表示可用于标识用户的数据的图像的图形元素；

至少根据接收到的代码数据中表示所述图像的图形元素计算第一密码哈希值；

根据所述用户的验证数据计算第二密码哈希值；

迭代地改变所述验证数据，并根据改变的验证数据重新计算所述第二密码哈希值，直到所述计算出的第一和第二密码哈希值满足定义的对应关系为止。

23.根据权利要求22所述的方法，还包括将来自纠错码的奇偶校验符号和/或与所述图像相关联的辅助数据添加到所述二维代码。

24.根据权利要求22或23所述的方法，还包括生成包含所述二维代码的可验证数据工具。

25.根据权利要求24所述的方法，其中，所述可验证数据工具与所述用户的电子交易相关联，并且其中，在所述交易时，由照相机捕获所述用户的标识数据的高分辨率图像。

26.根据权利要求22-25中的任一项所述的方法，其中，迭代地改变所述验证数据包括：操作标识所述用户的源数据，由此，所述计算的第一和第二密码哈希值满足定义的对应关系。

27.根据权利要求26所述的方法，其中，所述源数据是由所述二维代码的图形元素表示的所述图像的高分辨率版本，并且其中，迭代地改变所述验证数据包括：以隐写的方式改变所述高分辨率图像数据，直到所述计算的第一和第二密码哈希值满足所述定义的对应关系。

28.根据权利要求22-26中任一项所述的方法，其中，所述对应关系定义所述第一和第二密码哈希值之间的共同数位。

29.根据权利要求22-26中任一项所述的方法，其中，所述对应关系定义所述第一和第二密码哈希值的数位之间的数学关系。

30.根据权利要求22-29中任一项所述的方法，其中，所述验证数据包括所述用户的生

物特征数据。

31.根据权利要求22-29中任一项所述的方法,其中,所述源数据包括交易数据和所述用户的面部的数字图像。

32.根据权利要求31所述的方法,其中,所述源数据还包括标识所述用户的生物特征信息。

33.根据权利要求31或32所述的方法,其中,所述源数据还包括仅所述用户知晓的信息。

34.根据权利要求22-33中任一项所述的方法,其中,所述二维代码数据与所述相关联的用户的验证数据的绑定是基于权利要求1-21中任一项所述的方法验证的。

35.根据权利要求1或22所述的方法,其中,所述二维代码包括表示另一二维代码的图像的图形元素,所述另一二维代码编码可用于识别所述用户的数据。

36.一种验证二维代码的计算机实现的方法,所述方法包括至少一个计算设备:

接收捕获的表示二维代码的图像数据;

处理所述二维代码以对标识相关联的实体的数据进行解码;

检索与所标识的实体相关联的验证数据;

至少根据所述接收的图像数据的部分计算第一密码哈希值;

根据所述检索的验证数据计算第二密码哈希值;以及

基于确定所述第一密码哈希值与所述第二密码哈希值满足定义的对应关系,验证所述二维代码。

37.一种系统,包括用于执行根据权利要求1-36中任一项所述的方法的装置。

38.一种存储介质,包括存储在其上的机器可读指令,所述机器可读指令用于使计算机系统执行根据权利要求1-36中任一项所述的方法。

数据验证

技术领域

[0001] 本发明总体上涉及数据处理，并且更具体地，涉及用于生成和验证标识数据的方法和系统，所述标识数据被绑定到所述标识数据的被授权的所有者的身份。

背景技术

[0002] 安全的访问控制系统是众所周知的，在其中向用户发出特定于系统的永久或临时身份(identification,ID)通行证。发出的通行证通常由希望越过控制点的所有者出示，并在用户被允许进入关联的安全区域、建筑物、设施等之前进行检查。一种常规的访问控制形式依赖于静态的标识形式例如在通行证上打印诸如个人姓名和/或用户面部照片。但是，这种形式的标识容易受到欺诈性生产和复制的影响。访问控制的另一种传统形式依赖于对编码的标识符数据的机器验证。例如，标识符数据可以被编码在打印在通行证上的条形码中，例如一维(1D,one-dimensional)条形码或二维(2D,two-dimensional)条形码，通常被称为QR码。作为另一示例，标识符数据可以嵌入在电子标签中，例如近场通信(NFC,near field communication)标签标识符或射频标识符(RFID,Radio Frequency Identifier)标签。但是，这样的机器验证系统不验证出示访问通行证的人的身份。

[0003] 因此，本领域仍然需要技术改进。

发明内容

[0004] 根据一个方面，本发明提供了一种数据验证方法，包括：接收定义二维代码的代码数据，该二维代码包括表示用户的图像或与该用户相关联的其它形式的可见特征的图形元素；检索与该用户相关联的验证数据；至少根据接收到的代码数据中表示该图像的所述图形元素计算第一密码哈希值；根据验证数据计算第二密码哈希值，并基于第一密码哈希值和第二密码哈希值的比较来验证代码数据。

[0005] 根据另一方面，本发明提供了一种生成二维代码数据的方法，所述二维代码数据以密码方式绑定到相关联的用户的验证数据，该方法包括：将源数据编码为二维代码，该二维代码包括表示用户的图像或与该用户相关联的其它形式的可见特征的图形元素；至少根据接收的代码数据中代表该图像的图形元素计算第一密码哈希值；根据用户的验证数据计算第二密码哈希值；迭代地改变验证数据，并根据改变的验证数据重新计算第二密码哈希值，直到计算的第一和第二密码哈希值满足定义的对应关系为止。

[0006] 根据再一方面，本发明提供了一种计算机实现的验证二维代码的方法，该方法包括：接收捕获的表示二维代码的图像数据，处理该二维代码以对标识相关联的实体的数据进行解码，检索与所标识的实体相关联的验证数据，至少根据接收的图像数据的部分计算第一密码哈希值，根据检索到的验证数据计算第二密码哈希值，并基于确定第一密码哈希值与第二密码哈希值满足定义的对应关系验证二维代码。

[0007] 根据另一方面，提供了一种在终端处认证用户的方法，该方法包括：处理二维代码的图像数据以解码密钥信息，该二维代码包括表示用户的面部或其它可见用户特征的低分

辨率图像的图形元素;检索与该用户相关联的加密标识数据,该加密标识数据包括该用户的面部或其它可见特征的高分辨率图像;以及基于解码的密钥信息解密检索到的加密标识数据;其中该二维代码提供编码的密钥信息与该用户的面部或特征的至少一个可识别特征的不可撤销的绑定,并且其中该用户是通过根据二维代码中的低分辨率图像和加密标识数据中的高分辨率图像验证所述用户面部或特征的至少一个特征而被授权的。

[0008] 在又一方面中,本发明提供一种验证二维代码的方法,该方法包括:处理二维代码的图像数据以确定表示用户的面部或其它可见特征的低分辨率图像的图形元素,根据该二维代码中的低分辨率图像数据计算第一密码哈希值,从数据库中检索该用户的面部或特征的高分辨率图像,根据检索到的高分辨率图像数据计算第二密码哈希值,并基于对第一和第二密码哈希值的比较验证二维代码。

[0009] 在其它方面,提供了被配置为执行如上所述的方法的装置和系统。在另一方面,提供了一种计算机程序,该计算机程序包括机器可读指令,该机器可读指令被设置为使可编程设备执行如上所述的任何一种方法。

附图说明

[0010] 下面仅通过示例的方式,参照以下示出的附图,对本发明的实施例进行详细描述。

[0011] 图1是示出根据本发明的一个实施例的访问控制系统的主要组件的示意性方框流程图。

[0012] 图2是示意性示出根据本发明的一个实施例的如图1中所示的代码生成器的主要组件的方框流程图。

[0013] 图3包括图3A-图3C,示出了由图2中所示的代码生成器生成的2D代码的一个示例。

[0014] 图4是示意性地示出根据本发明的一个实施例的图1中所示的认证模块的主要组件的方框流程图。

[0015] 图5是示出根据一个实施例的由图1所示的系统组件执行的主要处理步骤的流程图。

[0016] 图6是示出根据本发明另一实施例的如图1中所示的用户设备中的代码生成器的主要组件和服务器中提供的验证数据的示意性方框流程图。

[0017] 图7是示意性地示出根据本发明一个实施例的用于验证由图6中所示的代码生成器生成的2D代码的认证模块的主要组件的方框流程图。

[0018] 图8是根据本发明一个实施例的,使用图7中所示的认证模块在终端上对用户进行认证的计算机实现的过程的流程图。

[0019] 图9是示出根据本发明另一实施例的交易数据处理系统的主要组件的示意性方框流程图。

[0020] 图10是示出根据本发明另一实施例的交易数据处理系统的主要组件的示意性方框流程图。

[0021] 图11是示意性地示出由图10的系统生成的示例数据结构的框图。

[0022] 图12是示出根据本发明另一实施例的电子标签生成和验证系统的主要组件的示意性方框流程图。

[0023] 图13是可以在其上实现实施例的一个或多个功能的计算机系统的示例的图。

具体实施方式

[0024] 图1示出了根据一个实施例的访问控制系统1的主要组件，包括例如位于安全限制区域的控制点处的终端3。在该示例性实施例中，在终端3处提供的认证模块5被配置为验证由终端3例如从用户的计算设备9接收的标识数据7的可靠性。在其它实施例中，可以在远程服务器11处提供认证模块5。终端3和用户设备9可以被配置为经由数据网络13与服务器11进行数据通信。在该实施例中采用电子通行证形式的标识数据7存储在用户的计算设备9的存储器15中，并且包括定义二维(2D)条形码17的数据。如本领域所公知的，2D代码17是由图形元素组成的机器可读的光学标签，通常是在正方形网格中排列的像素/图案。图形元素对源信息进行编码，诸如与最初向其发行电子通行证的用户相关联的用户标识符19，该用户可能是也可能不是向终端3出示相关联的标识数据7的同一用户。

[0025] 如图1所示，本实施例中的2D代码17包含了表示用户面部的低分辨率图像的图形元素。设置在用户设备9和/或远程服务器11处的代码生成器21被配置为从源数据生成2D代码17，该2D代码17包含了表示可以从图像数据的高分辨率版本获得的用户面部的低分辨率图像的像素数据。高分辨率图像可以作为验证数据23存储在服务器11的安全用户数据库25中，例如，如将在下面更详细描述的，作为与用户标识符19相关联的用户数据20存储，以供认证模块5随后进行检索以验证标识数据7的可靠性。在一些实施例中，例如在使用相关联的用户的密码密钥由验证数据生成器61加密高分辨率图像数据之后，高分辨率图像数据23以加密形式存储。验证数据可以附加地或可替代地包括简档数据，诸如与用户相关联的生物特征数据(例如指纹、声纹、视网膜/虹膜扫描等)和/或可见特征数据(例如面部特征)和/或任何其它识别数据(例如密码、PIN等)。作为又一替代，验证数据生成器61可以配置为生成输入数据的修改或改变的版本，例如高分辨率图像数据23和/或简档数据等，其在各个字符串或数据值数组内的定义位置处编码或嵌入定义的与2D代码17的图像数据的对应关系，诸如具有共同值，或具有阈值数量的匹配值。

[0026] 用户设备9可以被配置为经由诸如显示器的输出接口27输出标识数据7，由此用户将2D条形码17出示给终端3的照相机输入接口29。或者，用户设备9可以被配置为经由用于数据通信的输出接口27向终端3发送标识数据7，例如使用无线或非接触式数据通信协议。可以理解的是，附加地或替代地，标识数据7可以被打印在物理通行证上并发给用户，以在终端3处出示给照相机29。作为又一替代方式，用户设备9可以是存储生成的ID数据7的电子密钥卡或安全令牌，被配置为经由数据通信输出接口27向终端3的对应的数据通信输入接口29发送ID数据7。

[0027] 响应于肯定验证，认证模块5随后可以向终端3的访问控制器31输出控制信号，以使得被授权的用户能够通过控制点。认证模块5还可以向显示器33输出所检索到的用户图像的版本，以促进对用户身份的附加人工验证。应当理解，系统1可以包括计算系统/设备中常见的其它组件、子组件、模块和设备，为了描述的清楚在图1中未示出。

[0028] 在图2的方框流程图中示意性地示出了用于生成2D代码17的代码生成器21-1的一个示例实施例。在该示例性实施例中，代码生成器21-1接收用户面部的图像数据23，例如，作为要合并到2D代码17中的图像的高分辨率版本。用户面部的高分辨率图像数据23可以由用户设备9的照相机(未示出)捕获。在该示例中，图像数据处理器35处理所接收的高分辨率图像数据23以生成所接收的图像数据23的低分辨率版本37。

[0029] 应当理解，低分辨率的图像使得各个像素尺寸更大，从而降低了随后使用扫描仪或照相机捕获二维代码的图像时图像数据捕获错误的可能性。替代地，低分辨率的图像可以通过纠错码保护，其中相关联的奇偶校验/纠错符号例如作为编码数据包括在二维代码本身中，和/或作为附加/补充图像数据存在，例如作为低分辨率图像或二维代码本身之后的一行或多行像素值。诸如图像支持数据之类的辅助数据也可以存在于图像像素之后的一行或多行像素值中。在随后捕获低分辨率图像之后的任何错误可以通过纠错码使用解码/捕获的奇偶校验/纠错符号来纠正。使用纠错码的纠错技术本身是公知的，因此无需进一步描述。

[0030] 代码生成器21-1包括编码器39，该编码器39执行用于从输入源数据41生成2D代码元素的任何已知算法。可以生成2D代码17以包括一种或多种类型的源数据，例如用户标识符19、与交易相关联的数据、代表计算的密码哈希值的数据、认证令牌、密码密钥、数字签名等。如本领域中已知的，通常在2D代码中提供冗余，从而尽管扫描/捕获的2D代码数据损坏，仍然能够恢复原始数据。例如，使用级别为H的Reed-Solomon代码集定义了可以恢复的相应最大数据损坏/丢失量，例如30％。在该示例性实施例中，编码器39被配置为确定并插入损坏的2D代码区域，该区域随后被所生成的低分辨率图像37占据。可替换地，已知其它用于直接从输入源数据41和原始的，例如高分辨率的用户面部图像数据生成2D代码元素的算法，从而源数据至少部分编码为所得2D代码17中表示用户面部图像的图形元素。

[0031] 所生成的2D代码17被传递到用户设备9的ID生成器32-1，以生成定义标识数据7的数据，该数据包括所生成的2D代码17数据。应当理解，可以在远程服务器11处提供代码生成器21-1和/或ID生成器32-1的部分或全部功能。标识数据7可以存储在用户设备9的存储器15中，用于随后的检索和输出，例如在用户设备9的显示器27上输出以由终端3的照相机29捕获。

[0032] 包括图3A-图3C的图3示出了由代码生成器21-1生成的2D代码17的一个示例。首先，如图3A所示，将具有对应于或小于最大可恢复数据丢失量的面积的空白矩形插入2D代码17-1中。如图3B所示，由图像数据处理器35例如通过缩放和灰度量化来获得高分辨率用户图像23的低分辨率版本37。将低分辨率图像37插入或放置在图3A的空白矩形中，以产生图3C所示的输出结果数据。优选地，诸如白色像素的边界之类的标记或标界也被插入到2D代码17-1中，以便于随后的图像处理以从捕获的2D代码数据中提取低分辨率图像数据37。代码生成器21-1可以检查所生成的2D代码17是否能够由2D代码读取器正确地读取，并且解码和恢复的原始数据是否没有错误。

[0033] 应当理解，存在将图像插入2D代码中的许多已知的替代方法，例如，如Chu等人在“Half Tone QR Codes(半色调二维码)”(ACM图形学报，第32卷第6期，文章217，2013年11月)中所述。还应理解，本发明的实现方式通常将是封闭的专有系统，其中2D代码图像在系统内生成并读取。在这种情况下，使用定制的QR码格式是有利的，由此QR码数据被限制在区域内或以其它方式进行了编码，从而不会受到来自低分辨率图像数据的干扰。生成的QR码将无法由标准QR码识读器读取，但这在封闭系统中没有任何影响，并且可以成为一个优势。

[0034] 图4是示出根据示例性实施例的认证模块5-1的主要数据处理组件和流程的方框流程图。认证模块5-1包括解码器45，该解码器45接收定义2D代码17的数据，例如由终端3的照相机29从用户设备9的显示器27捕获的2D代码图像数据。在该实施例中，2D代码17对包括

用户ID 19和与用户相关联的密码密钥47的源数据进行编码。解码器45处理接收到的2D代码17数据以解码标识密码密钥47和用户标识符19的数据。如果标识数据7是可靠的，则解码的用户标识符19’将对应于存储在用户数据库25中的注册用户数据20。所存储的用户数据20还包括用户面部的高分辨率图像数据23a的加密版本，其使用用户的密码密钥47加密。高分辨率图像数据也可以被数字签名，例如使用RSA或DSA密钥，以证明可靠性并防止对手部署的任何伪造或替代图像。用户数据20还可以包括数据库25中每个注册用户的简档数据24，例如包括定义用户面部的一个或多个可识别的可见特征的生物特征简档数据。数据库25可以是关系数据库；然而，可以使用任何其它类型的数据组织结构。

[0035] 解码的用户标识符19’被传递到数据库接口49，其从用户数据库25检索相应用户数据20的加密图像数据23a。数据库25可以设置在终端3的本地存储器中，或作为远程服务器11上的安全数据库，其可以由数据库接口49通过数据网络13进行访问。例如，诸如TLS或SSL的安全通信协议可以由数据库接口49实施以从安全数据库25将加密形式的图像数据检索到数据解密器51。数据解密器51使用解码的密码密钥47处理检索到的加密图像数据23’，以解密用户面部的高分辨率图像23。数据验证器53-1接收捕获的包括用户面部的低分辨率图像37’的2D代码17的图像数据，并且还从数据解密器51接收解密的用户面部的高分辨率图像数据23。数据验证器53-1处理接收的捕获图像数据，以定位和提取与低分辨率用户图像37’相对应的像素，例如，通过确定插入2D代码17的标记或标界。例如，如果在捕获的图像数据和/或解码的数据中存在奇偶校验符号，可以使用纠错码来纠正任何像素错误。

[0036] 在本示例性实施例中，数据验证器53-1还执行数据处理，以验证接收的低分辨率图像数据37’对应于检索和解密的用户面部的高分辨率图像数据23。例如，数据验证器53-1可以在两个图像上执行面部识别处理，以验证所识别的特征/特点与从用户数据库25中检索出的用户的简档数据24相匹配。2D代码17中存在的用户面部的低分辨率图像还使用户或其他人能够在将其出示给验证系统1之前人工检查他们是否具有正确的通行证。数据验证器53-1还可接收将标识数据7出示给终端3的用户的面部的图像数据，例如从终端3的另一个照相机(未示出)，并且对接收到的图像数据执行图像处理，以检测和验证低分辨率、高分辨率和/或捕获的图像数据中的用户面部的可识别可见特征。数据验证器53-1还可以在终端3的显示器33上输出低分辨率和高分辨率图像数据，以进一步人工验证出示身份通行证7的用户是被授权的所有者。在数据验证器53-1对接收的2D代码17的肯定验证之后，可以生成认证令牌55并将其输出到例如终端3的访问控制器31。作为响应，访问控制器31可以生成并输出一个或多个控制信号，从而控制被认证/验证的用户访问相关联的安全限制区域。

[0037] 图5是根据示例性实施例的在终端处对用户进行认证的计算机实现的过程的流程图。如图5所示，该过程开始于步骤S5-1，其中，照相机29例如从用户的身份通行证捕获出示给终端3的2D代码17的图像数据。在该实施例中，2D代码17包括编码密码密钥47和与用户相关联的用户ID 19的图形代码元素。至少部分图形代码元素代表用户面部的低分辨率图像。在步骤S5-3，解码器45处理捕获的2D代码17的图像数据，以解码用户的密码密钥47和ID 19’。

[0038] 在步骤S5-5，数据库接口49例如基于解码的用户ID 19’，从存储在用户数据库25中的用户数据20中检索对应的用户的加密图像数据23a。在步骤S5-7，数据解密器51处理从用户数据库25检索的数据以解密用户面部的高分辨率图像数据23。数据验证器53-1然后可

以处理解密的高分辨率图像数据23和从捕获的2D代码11的图像数据中提取的用户面部的低分辨率图像，以根据存储在用户数据库25中的用户简档数据20验证低分辨率和高分辨率图像中的用户面部的可见特征。例如，如步骤S5-9所示，数据验证器53-1处理捕获的2D代码17的图像数据，以确定并提取代表用户面部低分辨率图像的图形元素。数据验证器53-1可以被配置为定位标记或标界，诸如插入到2D代码17-1中的白色像素的边界，以确定包含低分辨率用户图像37'的像素数据的区域。

[0039] 在该示例中，在步骤S5-11中，数据验证器53-1对提取的低分辨率图像数据执行面部识别处理，以识别用户面部的一个或多个可识别特征。类似地，在步骤S5-13，数据验证器53-1对解密的高分辨率图像数据23执行面部识别处理，以识别用户面部的一个或多个可识别特征。合适的特征识别算法本身是已知的，并且不需要进一步描述。在步骤S5-15，数据验证器53-1根据从用户数据库25检索的用户简档数据24验证所识别的特征。替代地或附加地，终端3上的操作者可以目视检查个体本身是否与终端3的显示器33上所输出的高分辨率图像23和2D代码图像17都相对应，这是因为个体和低分辨率2D代码图像本身之间的对应关系可能不是无可辩驳的。

[0040] 在步骤S5-17，数据验证器53-1可以例如向终端3的访问控制器31生成输出信号，以授权已验证用户访问。这样，系统1有利地提供了一个在低分辨率用户图像37'和高分辨率解密用户图像23之间的不可辩驳的绑定，并因此对声称是出示给终端3的相关联的标识数据7的所有者的个人提供了不可辩驳的绑定。还应理解，由于存储的高分辨率图像以加密形式安全地存储在数据库25中，图像数据不是欺诈者能够容易访问的。即使欺诈者可以学习密码密钥或认证过程以欺诈地访问安全系统1，在下面描述的其它实施例中，再现必要的对应哈希值也是另一个障碍。

[0041] 图6是示出了根据另一实施例的，用于生成2D代码17的用户设备9和远程服务器11的主要组件的方框流程图，其中在适当的情况下使用与前述附图相对应的附图标记来表示对应的元素。如以上参考图2所讨论的，代码生成器21被设置在用户设备9处，并且生成包括对接收的源数据41进行编码的2D代码元素的2D代码数据17，以及从例如由用户设备9的照相机30捕获的相应的高分辨率图像数据23计算出的低分辨率图像37。

[0042] 如图6所示，在该示例性实施例中，高分辨率版本的用户图像23和2D代码数据17由用户设备9例如通过数据网络13向远程服务器11的验证数据生成器61发送。验证数据生成器61被配置为执行迭代数据处理，以获得所接收的高分辨率图像数据23b的操作版本，其具有关联的计算出的密码哈希值，该密码哈希值与根据至少部分2D代码数据17(诸如，提取的对应于低分辨率用户图像37的2D代码17的像素值)计算得到的密码哈希值具有共同的对应值。例如，哈希对应性确定器61可以反复调用数据操作器65以通过隐写方式改变或更改高分辨率图像数据，然后调用加密哈希计算器63计算相应的哈希值，直到数据的两种版本的哈希值满足定义的对应关系，例如具有所需的共同值，或在各个数据值字符串内的定义位置处具有阈值数量的匹配值。加密哈希计算器63可以实现一个或多个已知的加密哈希函数，例如SHA-3加密哈希函数，这是由美国国家标准技术研究院(National Institute of Standards and Technology,NIST)发布的标准。然后，所获得的高分辨率图像数据23b的操作版本作为用户数据20存储在用户数据库25中，以便在相应的用户验证过程中进行后续检索。将理解的是，替代实施例可以计算用户设备9内的部分2D代码数据的哈希值，并且将所

述哈希值而不是2D代码数据17发送到服务器11。

[0043] 图7是根据另一示例性实施例的认证模块5-2的方框流程图，其对应于图6中所示的代码生成器21，并且在合适的情况下使用与前述附图相对应的附图标记来表示对应的元件。该实施例中的认证模块5-2还包括解码器45，该解码器45接收定义2D代码17的数据，该2D代码17对包括与用户相关联的用户ID 19的源数据进行编码。如以上实施例中所讨论的，可以由终端3的照相机29从用户设备9的显示器27通过无线通信或者从其上打印有2D代码的物理通行证捕获2D代码图像数据。解码器17处理接收的2D代码17数据，以对标识用户标识符19的数据进行解码，该数据对应于存储在用户数据库25中的包括用户验证数据的操作版本23c的注册用户数据20，例如上面参考图6讨论的由数据操作器65输出的改变后的用户面部的高分辨率图像数据23b。

[0044] 解码的用户标识符19’被传递到数据库接口49，该数据库接口49从用户数据库25检索相应用户数据20的操作验证数据23c。包括用户面部的低分辨率图像数据37的2D代码数据17和相应的检索到的操作验证数据23c被传递到认证模块5的加密哈希计算器63，该加密哈希计算器63对应于图6所示的验证数据生成器61的加密哈希计算器63。认证模块5-2使用加密哈希计算器63根据2D代码数据17的定义的部分或整体，诸如上面参考相应的代码生成器21所讨论的提取的表示低分辨率用户图像37’的像素值，计算哈希值67。可以理解，低分辨率用户图像37’的特定图像分辨率将确定输入给加密哈希计算器63的像素值的数量。优选地，尽管不是必须的，低分辨率用户图像37’的图像分辨率可以不大于常规QR码扫描设备的捕获分辨率。认证模块5-2还使用加密哈希计算器63以根据检索到的操作验证数据23c计算哈希值69。数据验证器53-2接收所计算的第一和第二哈希值67、69，并且执行数据处理，以识别和验证例如在所计算的哈希值的每个字符串内的定义位置中各个哈希值具有共同的对应值，如上面参考相应的代码生成器21所讨论的。这样，当确定各个计算出的哈希值包括嵌入的对应关系时，示例性实施例的数据验证器53-2验证所接收的低分辨率图像数据37’对应于检索到用户面部的高分辨率图像数据23b。

[0045] 图8是根据另一示例性实施例的，使用图7所示的认证模块5-2在终端上对用户进行认证的计算机实现的过程的流程图。如图8所示，该过程开始于步骤S8-1，在步骤S8-1中，照相机29例如从用户的身份通行证捕获出示给终端3的2D代码17的图像数据，该2D代码17包括编码与该用户相关联的用户ID 19的图形代码元素。如上述实施例所述，至少一些图形代码元素以低图像分辨率表示用户面部的图像。在步骤S8-3，解码器45处理捕获的2D代码17的图像数据，以解码用户的ID 19’。在步骤S8-5，数据库接口49例如基于解码的用户ID 19’，从存储在用户数据库25中的用户数据20中检索用户图像的操作版本23b。如上面参考图6所示的相应的验证数据生成器61所讨论的，操作图像数据23b以比2D代码17中的低分辨率图像37’更高的图像分辨率来表示用户的图像。

[0046] 在该示例性实施例中，认证模块5-2被配置为验证根据所接收的图像数据和所检索到的服务器数据计算出的各个密码哈希值之间的对应关系。因此，在步骤S8-7，加密哈希计算器63可以处理捕获的2D代码17的图像数据，以确定并提取表示用户面部的低分辨率图像的图形元素。与上述数据验证器53-1类似，加密哈希计算器63可配置为定位标记或标界，例如插入2D代码17的白色像素的边界，以确定包含低分辨率用户图像37’的像素数据的区域。在步骤8-11中，根据确定的2D代码数据17的区域的像素值，计算第一加密哈希，以表示

用户面部。可替代地，可以根据整个2D代码图像数据17的像素值或其组合计算哈希。现在将给出一个样例，其中使用的哈希函数是SHA-3加密哈希函数，具有256位(32字节)输出。在本样例中，低分辨率图像数据的256位哈希可以用十六进制格式表示为：

[0047] 74a76ed7a52cb5a4b3524c4f0ff5ad5efa89a356e21ec70e16a37a75462496aa。

[0048] 在步骤S8-11，加密哈希计算器63根据检索到的高分辨率图像数据23b计算第二密码哈希值69。在该示例性实施例中，由数据操作器65对用户面部的原始高分辨率图像23进行隐写信号处理，使得因此计算出的操作高分辨率图像数据23b的哈希值69与根据2D代码数据17计算出的哈希值67例如在字符串中定义数量的位置中具有共同特征。可以通过使用图像处理而根据高分辨率图像23获得2D代码17中的低分辨率图像37，但这不是必需的。从本样例之后，可以以十六进制格式将以隐写方式改变的高分辨率图像23b的哈希值表示为：

[0049] 75b6978d787ef28daea0610f1d5856705340397aff571b52efc57a75462496aa

[0050] 其中，第二哈希值69的最后十二个数位对应于根据相应的用户面部低分辨率图像37'获得的第一哈希值67的最后十二个数位。用于改变像素值而不将图像降级为无法识别的形式的合适的隐写算法本身是已知的，例如，如F.Marino和G.Mastronardi在论文“关于数字图像中的隐写术效果”中所讨论的，无需进一步描述。应当理解，由于对原始图像的改变是以隐写方式改变，所以图像本身将呈现为与个体面部相同的高分辨率图像，因此适合于自动和/或人工验证可识别的可见特征。

[0051] 在步骤S8-13，数据验证器53-2接收并比较第一和第二密码哈希值67、69，以验证共同的数位。参照本样例，数据验证器53-2可以比较两个哈希值以确定对应的定义位置中的字符是相同的。在步骤S8-15，数据验证器53-2可以生成认证令牌并将其输出到例如访问控制器31，以授权经验证用户访问。

[0052] 设想了用于验证两个获得的哈希值之间的对应关系的许多替代实施方式。例如，哈希值可以配置为在不同的位置一致，而不是如上面提供的示例中仅是在字符串的末尾。对应位置可以在字符串内的可变位置中，例如在由代码查找表定义的位置中，和/或可以根据从2D代码17获得的哈希值的至少部分来确定。

[0053] 作为另一种选择，高分辨率图像不需要以隐写方式修改以实现所定义的对应关系。而是可以将伪随机值附加到高分辨率图像数据，使得计算出的整个数据(即，高分辨率图像数据和附加值)的哈希值具有所需的共同数位。

[0054] 作为另一种选择，可以通过密钥/数据输入级联，使用秘密密钥或从2D代码获得的密钥(例如，通过使用固定或秘密的AES密钥对2D代码图像数据17进行AES加密而获得的)，通过诸如HMAC(keyed-hash message authentication code，密钥哈希消息认证码)之类的密钥哈希函数或SHA-3来确定哈希值。

[0055] 作为另一种选择，所讨论的哈希数位不需要具有确切的对应关系或一致，而是可以被定义为彼此具有数学关系，例如纯粹是模2和，或者具有预定义信息元素的模和，预定义信息元素例如用户的姓名、电话号码、URL和/或诸如指纹、虹膜扫描等的用户生物特征数据。

[0056] 在又一替代实施例中，可以组合参考图2描述的代码生成器21-1和参考图6描述的验证数据生成器61的各方面，从而根据2D代码图像数据17获得的哈希值可以直接使用或将其用作密钥伪随机函数的输入，以产生密码密钥47，以对存储在数据库25中并从数据库25

中检索出的个体的加密高分辨率图像23a进行解密。可理解，在该替代方式中，该系统被有利地配置为通过避免直接暴露加密密钥来提供增强的安全策略，因为解码的密钥信息用于计算或以其它方式从安全存储器或数据库中检索关联的加密密钥，并且哈希值不用作认证工具，以使得能够访问由安全系统1存储的加密高分辨率图像。可替代地，系统1可以包括其它安全功能，例如多因素认证，要求个体额外输入PIN、指纹或其它生物特征输入。

[0057] 现在将参考图9，针对具有认证服务器93的系统91，描述本发明的另一实施例，在合适的情况下，使用与先前附图相对应的附图标记表示对应元件，其中，该认证服务器93被配置为验证经由用户设备9a上的用户应用程序95a发起、生成交易或以其它方式参与交易的用户的身份。在该实施例中，用户应用程序95a被配置为例如经由应用服务器99的应用程序模块97来处理与用户设备9a处的用户应用程序95a和接收方设备9b处的对应用户应用程序95b之间的交易有关的数据。应当理解，在其它实现环境中，交易可以在用户应用程序95a与应用服务器99本身之间进行。

[0058] 纯粹通过示例的方式，用户应用程序95可以提供在各个用户之间执行数据传输交易、电子数据消息传递、点对点(peer-to-peer，P2P)支付交易(可能不需要中间应用服务器)或从客户设备到商户和/或银行计算实体的支付交易的功能。

[0059] 在该示例性实施例中，用户应用程序95a包括配置为根据特定用户应用程序实现环境生成交易数据的交易数据生成器101。所生成的交易数据作为源数据41被提供给用户应用程序95a的代码生成器21，代码生成器21还例如在交易数据生成时或之后响应于来自用户应用程序95a的提示，接收由用户设备9a的照相机30捕获的用户面部的图像数据23。如以上参考图6所讨论的，代码生成器21生成2D代码数据17，该2D代码数据17包括对所生成的交易数据进行编码的2D代码元素，以及根据对应的高分辨率图像数据23计算出的低分辨率图像37。用户图像的高分辨率版本23和2D代码数据17也由用户应用程序95a例如经由应用服务器99发送到远程服务器11的验证数据生成器61。用户应用程序95a还可以将一些或全部生成的交易数据发送给验证数据生成器61。同样如上面参考图6所述，验证数据生成器61执行迭代数据处理，以获得高分辨率图像数据23b的操作版本以及从用户应用程序95a接收的任何交易数据，操作的验证数据23具有关联的计算出的密码哈希值，其与根据至少一部分2D代码数据17计算得出的密码哈希值具有共同的对应值。

[0060] 在该实施例中，将生成的2D代码17传递到用户应用程序95a的交易令牌生成器32-2，其生成包括2D代码数据17的交易令牌7’，从而建立交易的电子收据，其将发起交易或与交易相关联的用户与交易本身的被编码的详细信息无可辩驳地绑定在一起。认证服务器93还用于随后对交易进行认证，该认证是通过例如基于认证服务器93处的认证模块5对来自交易令牌7’的2D代码17的处理来验证声称与该交易相关联的用户的身份，如上面参考图7所讨论的。

[0061] 如图所示，用户应用程序95与应用服务器99的相应应用程序模块97经由各自的应用服务器和客户端接口103a、b例如通过数据网络13通信。应用程序模块97也与认证服务器93经由各自的接口105a、b通过数据网络13进行通信。应当理解，接口103、105可以包括用于各个应用的计算机可执行指令，以在它们之间的传输路径上建立和传输数据。

[0062] 用户设备9a与系统91的注册用户相关联，认证服务器93将标识每个注册用户的用户数据20存储在例如一个或多个数据库25中。用户和接收方设备9各自可以是一种本身已

知的类型，例如台式计算机、膝上型计算机、平板计算机、智能手机(基于iOS®、Blackberry®或Android®的智能手机)、“功能”电话、个人数字助理(personal digital assistant,PDA)，或任何具有适当输入和显示装置的处理器供电的设备。应当理解，多个用户设备9可在系统91内同时操作。

[0063] 图10是根据另一实施例的系统1001的框图，在合适的情况下使用与先前附图的附图标记相对应的附图标记表示对应元件。在该示例性实施例中，认证服务器107还被配置为验证经由用户设备9a上的用户应用程序95a’发起、生成交易或以其它方式参与交易的用户的身份。然而，并非如上面参考图9所讨论的那样生成交易令牌，本实施例中的用户应用程序95a’包括数据包装器生成器108，其被配置为基于所捕获的2D代码17的图像数据和由交易数据生成器101输出的交易数据生成2D代码包装器数据实体111。图12是示意性地说明由数据包装器生成器107生成的示例包装器数据结构111的框图。如图所示，数据包装器生成器107将接收到的包含嵌入的用户的低分辨率照片的2D代码图像数据17插入到QR包装器数据结构111的核心层113-1中。可选地，其它用户数据(未示出)，例如密码或PIN和/或诸如指纹或虹膜扫描之类的用户生物特征数据可以包括在2D代码17中。

[0064] 数据包装器生成器107根据核心层113-1中的数据计算第一哈希值115-1，该数据包括2D代码17的图像数据和任何附带的附加用户数据。核心层113-1、核心哈希值115-1以及从交易数据生成器101接收的交易数据117一起形成包装器数据结构111的第二层，称为第一包装器层113-2或“包装器1”。数据包装器生成器107根据第一包装器层113-2的数据计算第二哈希值115-2。计算的包装器1哈希值115-2和第一包装器层113-2本身的数据一起形成包装器数据结构111的第三层，称为第二包装器层113-3或“包装器2”。然后，数据包装器生成器107可以例如使用RSA或DSA密钥对第二包装器层113-3进行数字签名。

[0065] 在该示例性实施例中，包装器数据实体111被发送到应用服务器99的应用程序模块97，其中应用程序模块97的相应数据包装器验证器109对接收到的包装器数据实体111进行数据处理以首先通过根据计算的所接收的包装器1数据本身的哈希值检查接收到的包装器1哈希值115-1，以检查包装器2数据层113-3是否完整。然后，数据包装器验证器109通过根据计算的所接收的2D代码图像数据17本身的哈希值检查接收到的核心层哈希值115-1以及任何附带的附加用户数据(如果存在于核心层113-1中)，来执行数据处理以检查包装器1数据层113-2是否完整。数据包装器验证器109还根据特定实现环境提取交易数据117以用于后续处理。数据包装验证器109可以将核心数据层113-1发送到接收方设备9b的用户应用程序95b，以在显示器33’上输出，由此可以由接收方用户对嵌入的低分辨率图像进行附加的视觉检查。

[0066] 在该实施例中，数据包装器验证器109还将接收到的核心数据层113-1的2D代码图像数据17发送到认证服务器107，以由认证模块5进行处理。认证模块5进行的2D代码和用户身份验证处理类似于以上实施例中参照图4或图7描述的处理。在认证模块5的肯定验证之后，可以将输出认证令牌55返回到应用服务器99的应用程序模块97。替代地或附加地，认证服务器107还可以将检索/解密的高分辨率图像23b返回给应用服务器99，例如，将其转发给接收方设备9b，以在显示器33’上输出，作为进一步的人工视觉验证。

[0067] 以这种方式，身份验证过程涉及由应用服务器99发起的对包装器1和包装器2数据层113-2、113-3的检查，并且涉及随后由认证服务器107对核心数据层113-1的检查，以验证

包含在2D代码17中的低分辨率图像不会被篡改或欺诈性产生。响应于从认证服务器107接收到认证令牌55,应用程序模块97可以根据用户应用实现环境来执行进一步的处理步骤以完成验证的交易。

[0068] 现在将参考图12,针对系统1201描述本发明的另一实施例,在合适的情况下使用与先前附图相同的附图标记表示相应元件,系统1201被配置为生成和验证经认证的电子标签形式的2D图像代码,该2D图像代码例如表示入场券或即将到来的事件(诸如音乐会、酒店预订、VIP会议等)的邀请。在该实施例中,通常通过在用户的移动计算设备9a(例如智能手机)上使用应用程序1203来启动该过程。用户应用程序1203的代码生成器21接收用户面部的图像数据,该图像数据例如由用户设备9a的照相机30捕获为高分辨率数字照片。代码生成器21还接收由用户应用程序1203的源数据生成器41a生成的源数据41,例如与电子标签相关联的事件的交易数据,诸如,用户ID和其它凭证、事件日期、地点和场所等,具体取决于实施环境。

[0069] 如上面参考图2所述,代码生成器21根据接收的源数据41和捕获的图像数据23生成2D代码17,所生成的2D代码17包含表示根据接收的高分辨率图像数据23获得的用户面部的低分辨率图像37的像素数据。原始高分辨率图像23作为验证数据23存储在远程认证服务器93的安全用户数据库25中,例如作为与用户标识符19相关联的用户数据20存储,以便随后由认证模块5检索以验证电子标签7的可靠性。在一些实施例中,使用相关联的用户的密码密钥以加密形式存储高分辨率图像数据23。在其它实施例中,验证数据可以附加地或替代地包括简档数据,诸如与用户相关联的生物特征数据,例如,指纹、声纹、视网膜/虹膜扫描等,和/或可见特征数据,例如,面部特征,和/或任何其它识别数据,例如密码、PIN等,可以通过用户设备9a的合适的输入接口(未示出)从用户接收。

[0070] 所生成的2D代码17被传递到用户应用程序1203的标签生成器32-3,以生成定义电子标签7的数据,包括所生成的2D代码17数据。因此,2D代码17嵌入将用户绑定到与电子标签7相关联的事件的数据。应当理解,可以在相应的应用服务器99和/或认证服务器93处提供部分或全部代码生成器21和/或标签生成器32-3功能。

[0071] 在该示例性实施例中,认证服务器93还包括验证数据生成器61,如上面参考图6所讨论的,该验证数据生成器61被配置为迭代地改变用户的原始验证数据,直到根据改变的验证数据计算出的密码哈希值和根据2D代码数据17计算出的密码哈希值满足定义的对应关系为止。例如,如以上实施例中所讨论的,可以由在认证服务器93处提供的验证数据生成器61执行迭代图像处理,以生成接收的图像数据23的操作版本,其体现对应的计算出的哈希值的可验证特征,其中该对应的计算出的哈希值与根据生成的2D代码17或电子标签7的图像数据计算出的哈希值具有定义数量或阈值数量的共同数位。替代地或附加地,验证数据生成器61可以被配置为获得与原始用户或实体相关联的原始验证数据的其它形式的操作版本。

[0072] 为了提高安全性,2D代码17可以包括用户发布的PIN或用户输入的信息。2D代码17还可包括诸如指纹的用户生物特征输入。在这样的替代方案中,可以将2D代码17的哈希安排为与存储在用户数据库25中的高分辨率图像的哈希加上任何用户数据/生物特征数据的哈希具有共同的数位。这提供了防止欺诈的进一步优点,例如,如果用户的设备被盗,而2D代码图像17在准入场景中由相貌相似的人出示。另外,被传送到认证服务器93的捕获的高

分辨率图像23可以由认证服务器5处理，以将接收到的图像数据23与数据库25中存储的用户的其它高分辨率图像进行比较，以进行额外的用户验证。

[0073] 如以上实施例中所讨论的，电子标签7数据可以存储在用户设备9a的存储器15中，以用于随后的检索和输出，例如在用户设备9a的显示器(未示出)上输出，以由终端的相机29捕获。如图12所示，在本实施例中，例如，电子标签7由用户应用程序1203从存储器15中检索，并由标签发送器1205a发送至终端3'的相应接收器接口1205b和/或应用服务器99。标签发送器1205a和接收器1205b可以被配置为例如使用诸如Mobile、Bluetooth®或WiFi®之类的无线电或通过近场通信(near field communication,NFC)在数据网络13上和/或在数据通信链路上传送数据。带有2D代码图像11的电子标签7由终端3'处理，在本实施例中，终端3'将2D代码11的数据传送到认证服务器93，以由认证模块5进行验证，如以上实施例中所讨论的。

[0074] 一旦电子标签7由终端3'确认，例如包括由认证模块5验证来自电子标签7的2D代码17和存储在用户数据库25中的诸如高分辨率用户图像的对应验证数据23之间的共同哈希值，终端3'可以在显示器29上将确认消息与高分辨率用户图像一起输出，以用于例如由准入场景的代理者进行的附加人工验证。用户验证的其它步骤可以包括代理者要求从用户输入的PIN或生物特征数据，可以将其进行哈希处理并与2D代码17的哈希组合，以便与存储在用户数据库25中的验证数据23的哈希进行比较。

[0075] 示例计算机系统实现

[0076] 本发明的各个方面可以通过软件、固件、硬件或其组合来实现。图13示出了示例计算机系统1300，其中本发明或其部分可以被实现为计算机可读代码。例如，图5和8的流程图所示的方法可以在系统1300中实现。图1、2、4、6、7、9、10、11和12所示的系统的组件架构和系统组件可以分别在系统1300中实现。根据该示例计算机系统1300描述了本发明的各种实施例。在阅读了该描述之后，对于相关领域的技术人员来说，如何使用其它计算机系统和/或计算机体系结构来实现本发明将变得显而易见。

[0077] 计算机系统1300包括一个或多个处理器，诸如处理器1304。处理器1304可以是专用或通用处理器。处理器1304连接到通信基础架构1306(例如，总线或网络)。

[0078] 计算机系统1300还包括主存储器1308，优选地是随机存取存储器(random access memory,RAM)，并且还可以包括辅助存储器1310。辅助存储器1310可以包括例如硬盘驱动器1312、可移动存储驱动器1314、闪存、记忆棒和/或任何类似的非易失性存储机制。可移动存储驱动器1314可以包括软盘驱动器、磁带驱动器、光盘驱动器、闪存等。可移动存储驱动器1314以公知的方式从可移动存储单元1318读取和/或向可移动存储单元1318写入。可移动存储单元1318可以包括由可移动存储驱动器1314读取和写入的软盘、磁带、光盘等。相关领域的技术人员将理解，可移动存储单元1318包括非暂时性计算机可用存储介质，其中存储了计算机软件和/或数据。

[0079] 在替代实施方式中，辅助存储器1310可以包括用于使得计算机程序或其它指令能够加载到计算机系统1300中的其它类似装置。该装置可以包括例如可移动存储单元1322和接口1320。该装置的示例可以包括程序盒式存储器和盒接口(例如在视频游戏设备中发现的接口)、可移动存储芯片(例如EPROM或PROM)和相关的插槽，以及其它能够使软件和数据从可移动存储单元1322传输到计算机系统1300的可移动存储单元1322和接口1320。

[0080] 计算机系统1300还可包括通信接口1324。通信接口1324使得软件和数据能够在计算机系统1300和外部设备之间传送。通信接口1324可以包括调制解调器、网络接口(诸如以太网卡)、通信端口、PCMCIA插槽和卡或无线通信。

[0081] 计算机系统1300可以另外包括计算机显示器1309。根据一个实施例,计算机显示器1309结合显示接口1307,可以用于显示例如在图1、6、7、9、10和12中描绘的终端、用户设备和/或用户应用程序的接口。

[0082] 在本文中,术语“计算机程序介质”、“非暂时性计算机可读介质”和“计算机可用介质”通常用于指代诸如可移动存储单元1318、可移动存储单元1322和安装在硬盘驱动器1312中的硬盘的介质。计算机程序介质、计算机可读存储介质和计算机可用介质也可以指代诸如主存储器1308和辅助存储器1310的存储器,其可以是存储器半导体(例如DRAM等)。这些计算机程序产品是用于向计算机系统1300提供软件的装置。

[0083] 计算机程序(也称为计算机控制逻辑)存储在主存储器1308和/或辅助存储器1310中。计算机程序也可以经由通信接口1324接收。这样的计算机程序在被执行时使计算机系统1300能够实现如本文所述的本发明。特别地,计算机程序在被执行时使处理器1304能够实现本发明的处理,诸如上述图5和图8的流程图所示的方法中的步骤以及图1、2、4、6、7、9、10和12的系统组件架构。因此,这样的计算机程序代表计算机系统1300的控制器。在使用软件来实现本发明的情况下,可以将软件存储在计算机程序产品中并使用可移动存储驱动器1314、接口1320、硬盘驱动器1312或通信接口1324加载到计算机系统1300中。

[0084] 本发明还针对包括存储在任何计算机可用介质上的软件的计算机程序产品。当在一个或多个数据处理设备中执行时,这样的软件使数据处理设备如本文所述进行操作。本发明的实施例采用现在已知或未来的任何计算机可用或可读介质。计算机可用介质的示例包括但不限于主存储设备(例如,任何类型的随机存取存储器)、辅助存储设备(例如,硬盘驱动器、USB记忆棒、软盘、CD ROM、ZIP磁盘、磁带、磁存储设备、光存储设备、MEMS、纳米技术存储设备等)和通信介质(例如,有线和无线通信网络、局域网、广域网、内联网、基于云的服务等)。

[0085] 其它替代和修改

[0086] 将理解的是,本文中仅通过举例的方式描述了本发明的实施方式,并且在不脱离本发明的范围的情况下可以进行各种改变和修改。

[0087] 例如,在上述实施例中,在上述实施例中,二维代码包括表示用户面部的低分辨率图像的图形元素,并且该二维代码与对应的存储在例如远程服务器的安全数据库中的用户面部的高分辨率图像相关联。如本领域技术人员将理解的,二维代码可以包括表示用户的面部图像的图形元素和/或可用于识别用户的任何其它形式的数据,例如用户的其它可见、独特和可测量的特征,代表与用户相关联的独特特征的数据等。

[0088] 作为另一替代,代码生成器可以替代地或附加地被配置为生成包括表示第二2D条形码的图形元素的二维代码,该第二2D条形码编码可以由相应的认证模块用于身份验证的信息。例如,可以将基于表示低分辨率用户图像的像素值计算出的哈希值编码到第二2D条形码中,以供数据验证器随后根据检索的数据的计算出的哈希值进行验证。此外,第二2D条码可以包括用于另外的用户身份验证的其它编码信息,诸如,用户简档数据、关联交易的详细信息、会议、约会等。

[0089] 作为另一个示例，在上述实施例中，2D代码对包括与身份通行证的被授权的所有者相关联的用户标识符和密码密钥的密钥信息进行编码。如本领域技术人员将理解的，编码的密钥信息可以不包括密码密钥本身。相反，解码的密钥信息可用于例如基于解码的用户标识符从安全数据库中识别和检索相关联的用户的密码。

[0090] 作为另一示例，在上述实施例中，终端包括照相机，该照相机从出示给终端的身份通行证捕获2D条形码的图像数据，并且所捕获的图像数据由解码器处理以对其中编码的密钥信息进行解码。如本领域技术人员将理解的，终端可以替代地包括捕获和解码编码数据的2D条形码扫描器模块。作为另一种选择，可以将定义2D条形码的数据存储在电子通行证的存储器中，并通过通信接口(诸如，无线或RFID或NFC接口)将其传送给终端。

[0091] 将理解，尽管将各个过程和相关联的处理模块描述为单独的实施例，但是所描述的实施例的各方面可以组合以形成其它实施例。例如，替代实施例可以包括以上实施例中描述的认证模块和QR包装器数据结构方面中的一个或多个。

[0092] 作为另一替代，可以将认证模块或认证服务器模块设置为经由数据网络与其它系统组件通信的远程服务器上的一个或多个分布式计算模块或处理服务。另外，如本领域技术人员将理解的，认证模块功能可以作为用户设备或终端上执行的应用程序可访问的一个或多个应用程序接口(application programming interface,API)或作为插件模块、扩展、嵌入式代码等来提供，被配置为与应用程序进行通信。

[0093] 在本说明书中对“一个实施例”的引用不一定全部指的是同一实施例，也不是与其它实施例互斥的单独的或替代的实施例。特别地，将认识到，上述实施例的各方面可以组合以形成其它实施例。类似地，描述了可以由一些实施例而不是其它实施例展现的各种特征。可以设想另外的替代实施例，其仍然落入所附权利要求的范围内。

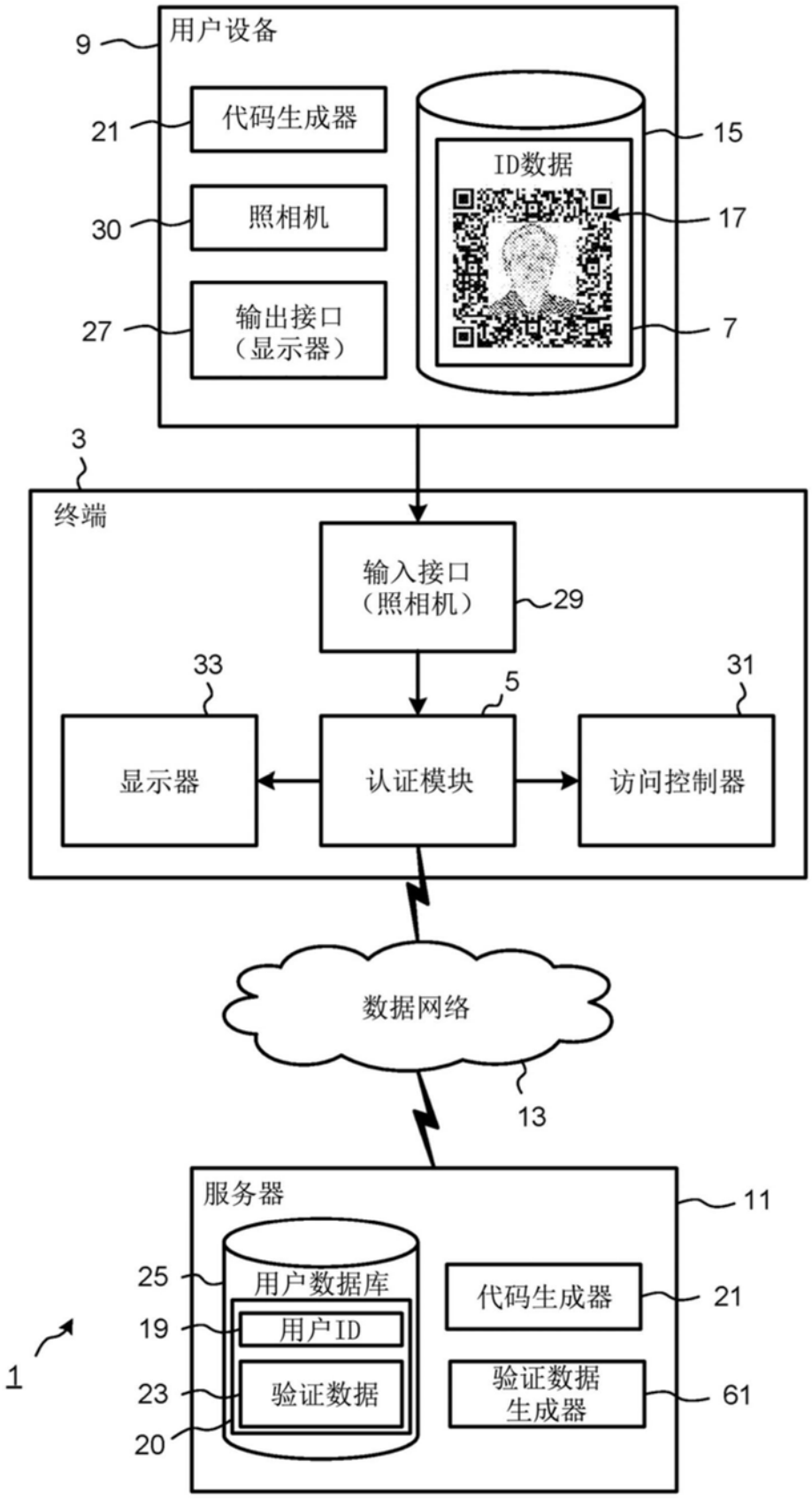

9
用户设备
21
代码生成器
30
照相机
27
输出接口
（显示器）
15
ID数据
17
7
3
终端
输入接口
（照相机）
29
33
5
31
显示器
认证模块
访问控制器
数据网络
13
服务器
11
25
用户数据库
19
用户ID
23
验证数据
20
代码生成器
21
验证数据
生成器
61
1

图1

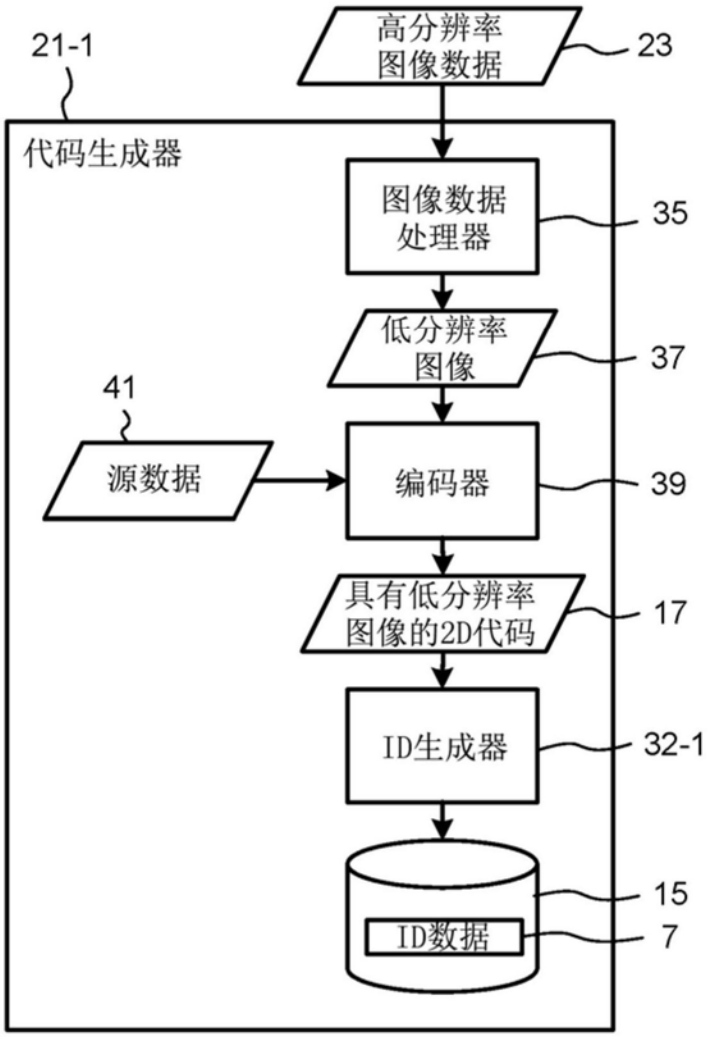

21-1
高分辨率
图像数据
23
代码生成器
图像数据
处理器
35
低分辨率
图像
37
41
源数据
编码器
39
具有低分辨率
图像的2D代码
17
ID生成器
32-1
15
ID数据
7

图2

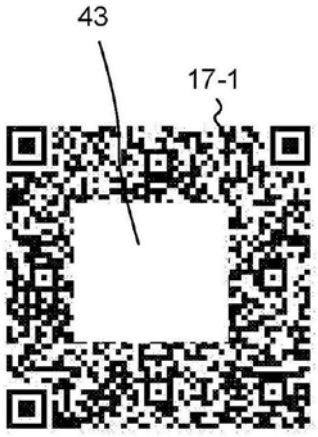

43
17-1

图3A

图3B

图3C

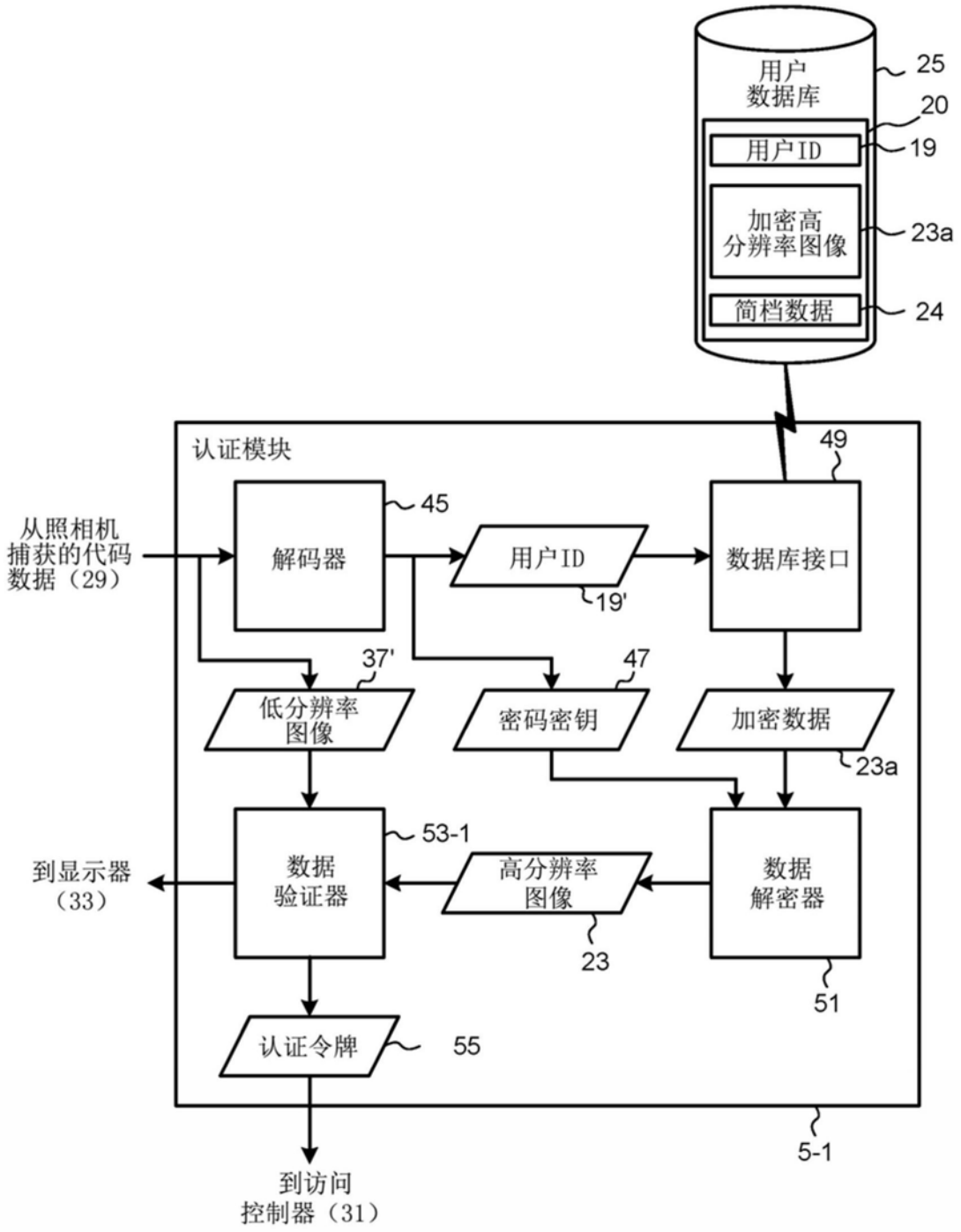

用户
数据库
25
20
用户ID
19
加密高
分辨率图像
23a
简档数据
24
认证模块
49
从照相机
捕获的代码
数据（29）
解码器
45
用户ID
19'
数据库接口
37'
47
低分辨率
图像
密码密钥
加密数据
23a
53-1
到显示器
（33）
数据
验证器
高分辨率
图像
23
数据
解密器
51
认证令牌
55
5-1
到访问
控制器（31）

图4

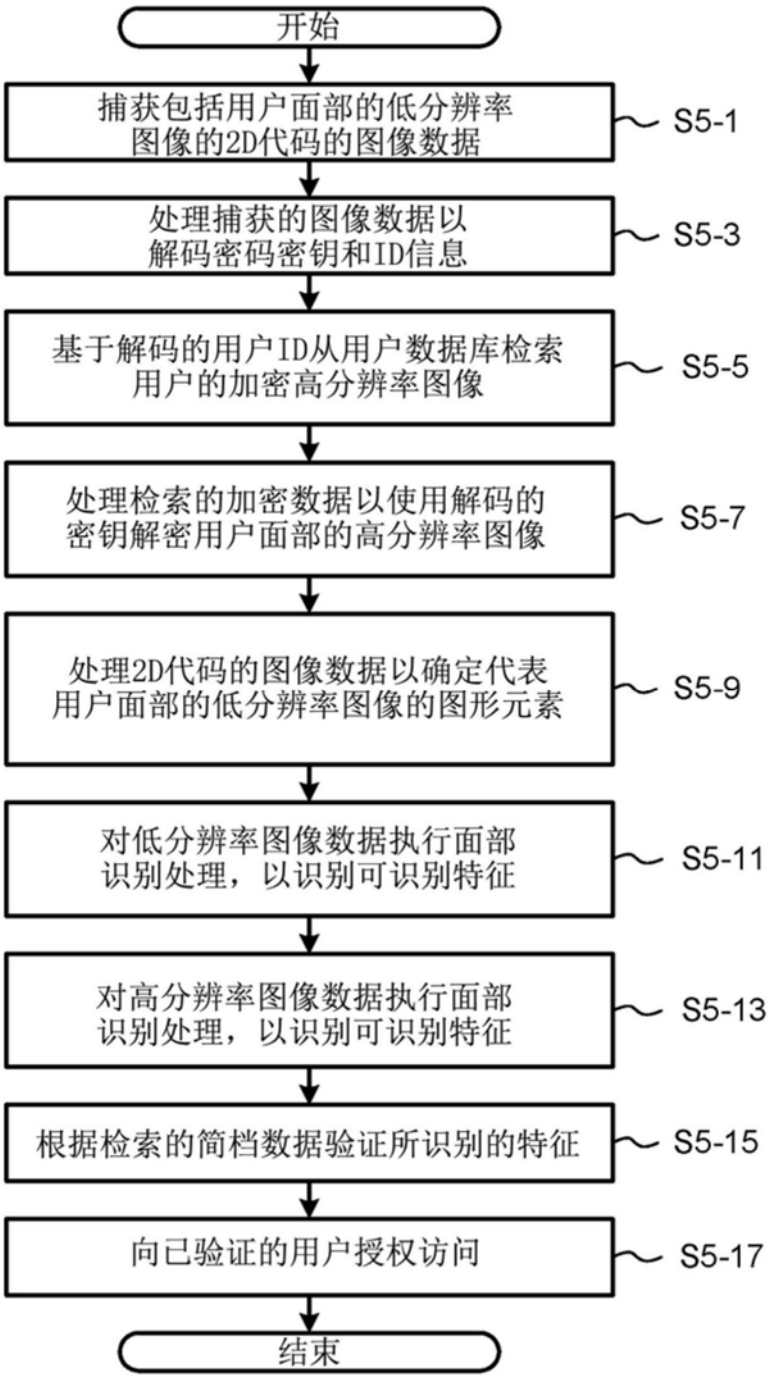

开始
捕获包括用户面部的低分辨率图像的2D代码的图像数据
S5-1
处理捕获的图像数据以解码密码密钥和ID信息
S5-3
基于解码的用户ID从用户数据库检索用户的加密高分辨率图像
S5-5
处理检索的加密数据以使用解码的密钥解密用户面部的高分辨率图像
S5-7
处理2D代码的图像数据以确定代表用户面部的低分辨率图像的图形元素
S5-9
对低分辨率图像数据执行面部识别处理，以识别可识别特征
S5-11
对高分辨率图像数据执行面部识别处理，以识别可识别特征
S5-13
根据检索的简档数据验证所识别的特征
S5-15
向已验证的用户授权访问
S5-17
结束

图5

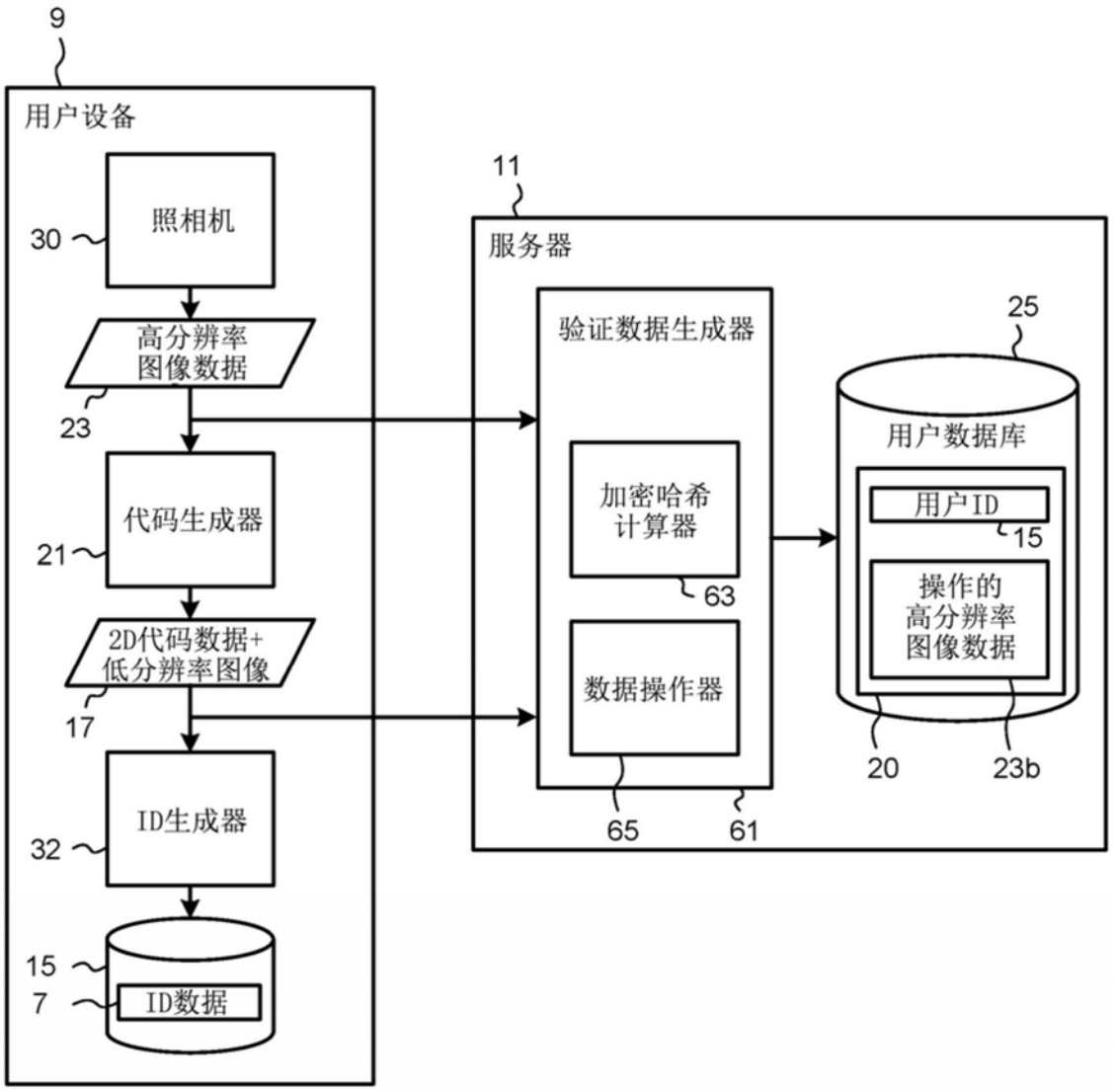

9
用户设备
照相机
30
高分辨率
图像数据
23
代码生成器
21
2D代码数据+
低分辨率图像
17
ID生成器
32
15
7
ID数据
11
服务器
验证数据生成器
加密哈希
计算器
63
数据操作器
65
61
25
用户数据库
用户ID
15
操作的
高分辨率
图像数据
20
23b

图6

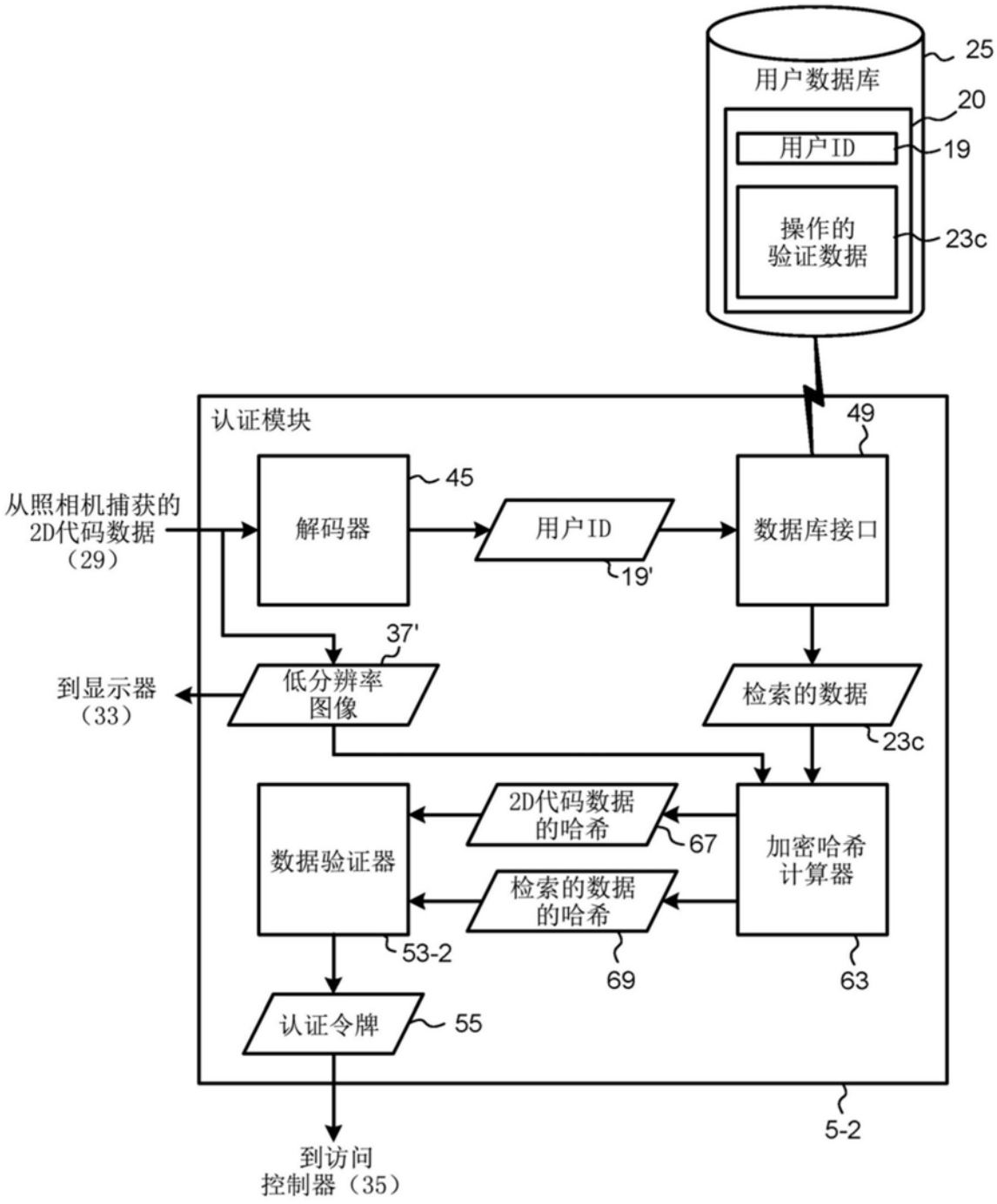

用户数据库
25
20
用户ID
19
操作的
验证数据
23c
认证模块
49
从照相机捕获的
2D代码数据
（29）
解码器
45
用户ID
19'
数据库接口
37'
到显示器
（33）
低分辨率
图像
检索的数据
23c
2D代码数据
的哈希
67
数据验证器
检索的数据
的哈希
加密哈希
计算器
53-2
69
63
认证令牌
55
5-2
到访问
控制器（35）

图7

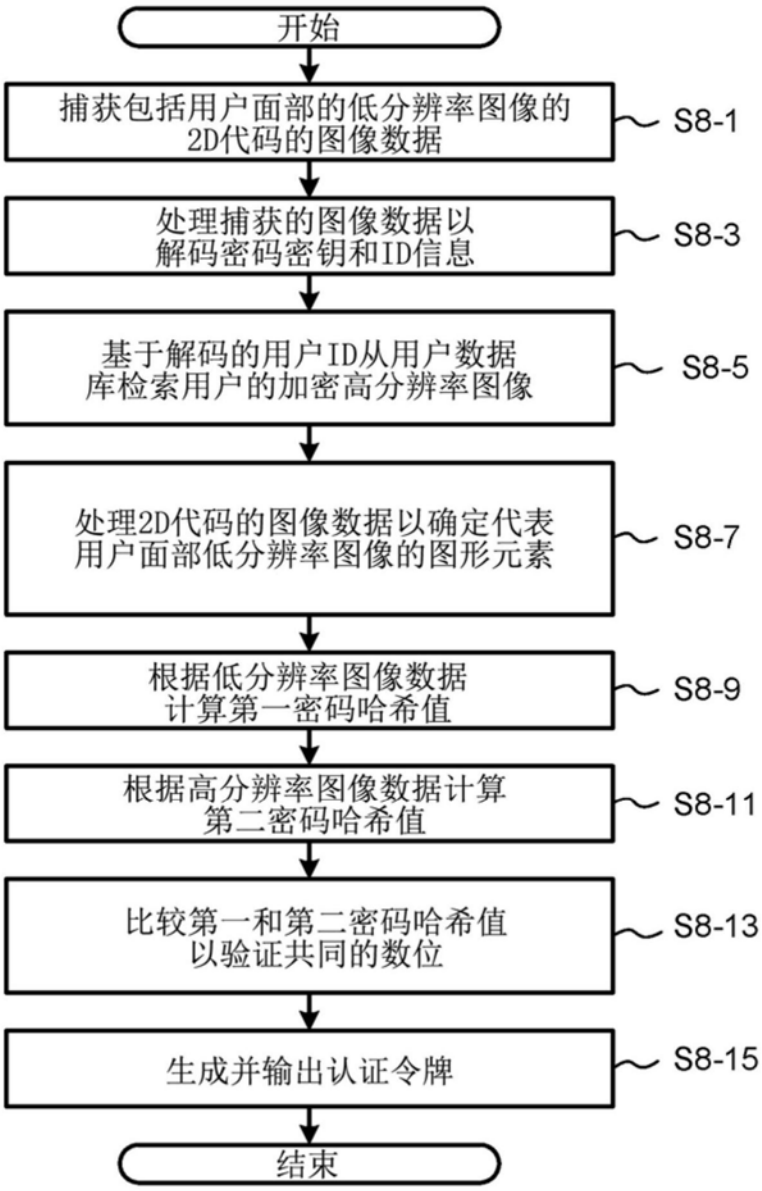

开始
捕获包括用户面部的低分辨率图像的2D代码的图像数据
S8-1
处理捕获的图像数据以解码密码密钥和ID信息
S8-3
基于解码的用户ID从用户数据库检索用户的加密高分辨率图像
S8-5
处理2D代码的图像数据以确定代表用户面部低分辨率图像的图形元素
S8-7
根据低分辨率图像数据计算第一密码哈希值
S8-9
根据高分辨率图像数据计算第二密码哈希值
S8-11
比较第一和第二密码哈希值以验证共同的数位
S8-13
生成并输出认证令牌
S8-15
结束

图8

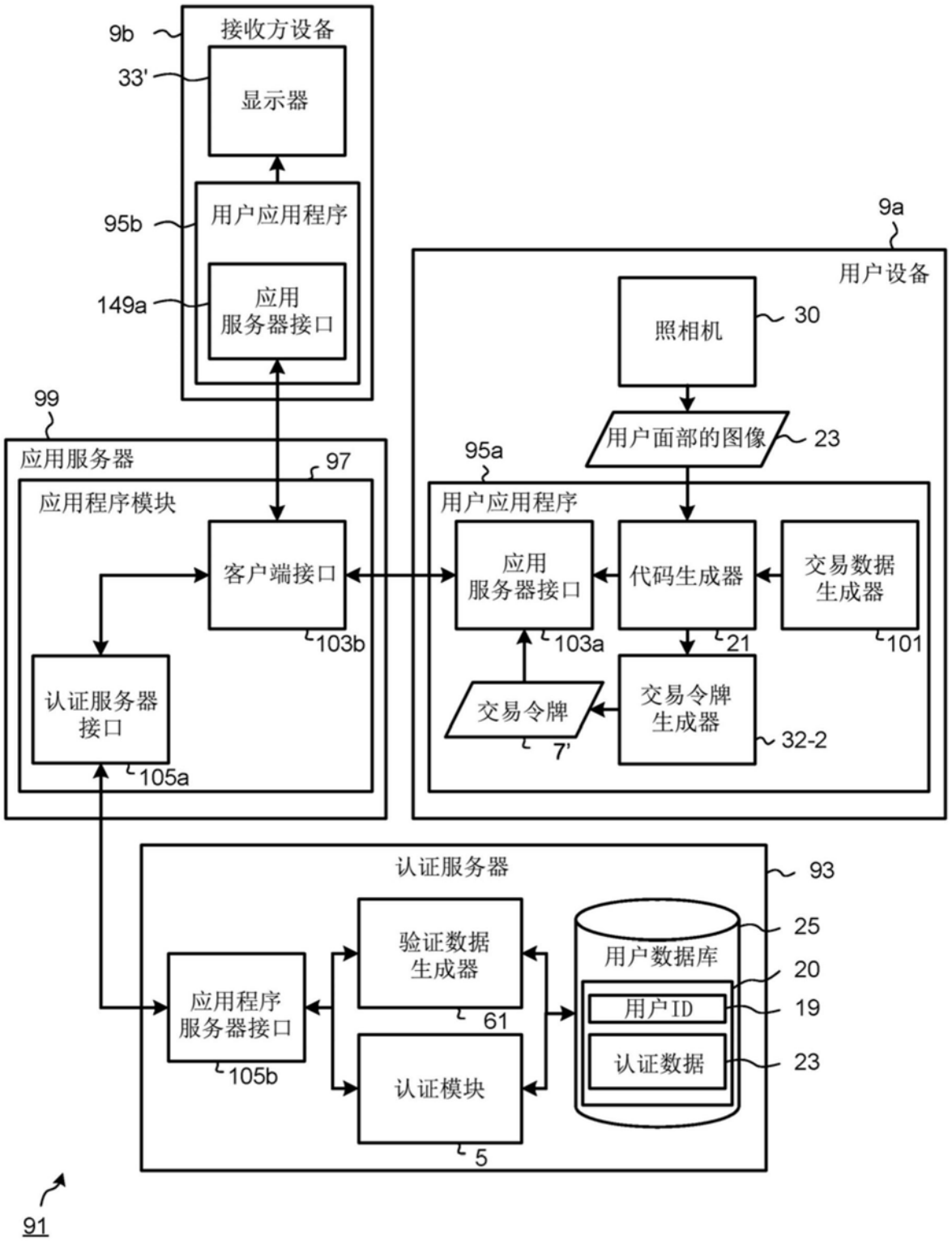

9b
接收方设备
33'
显示器
95b
用户应用程序
149a
应用
服务器接口
9a
用户设备
照相机
30
99
用户面部的图像
23
应用服务器
97
95a
应用程序模块
用户应用程序
客户端接口
应用
服务器接口
代码生成器
交易数据
生成器
103b
103a
21
101
认证服务器
接口
交易令牌
交易令牌
生成器
7'
32-2
105a
认证服务器
93
验证数据
生成器
25
用户数据库
20
应用程序
服务器接口
用户ID
19
61
认证数据
23
认证模块
105b
5
91

图9

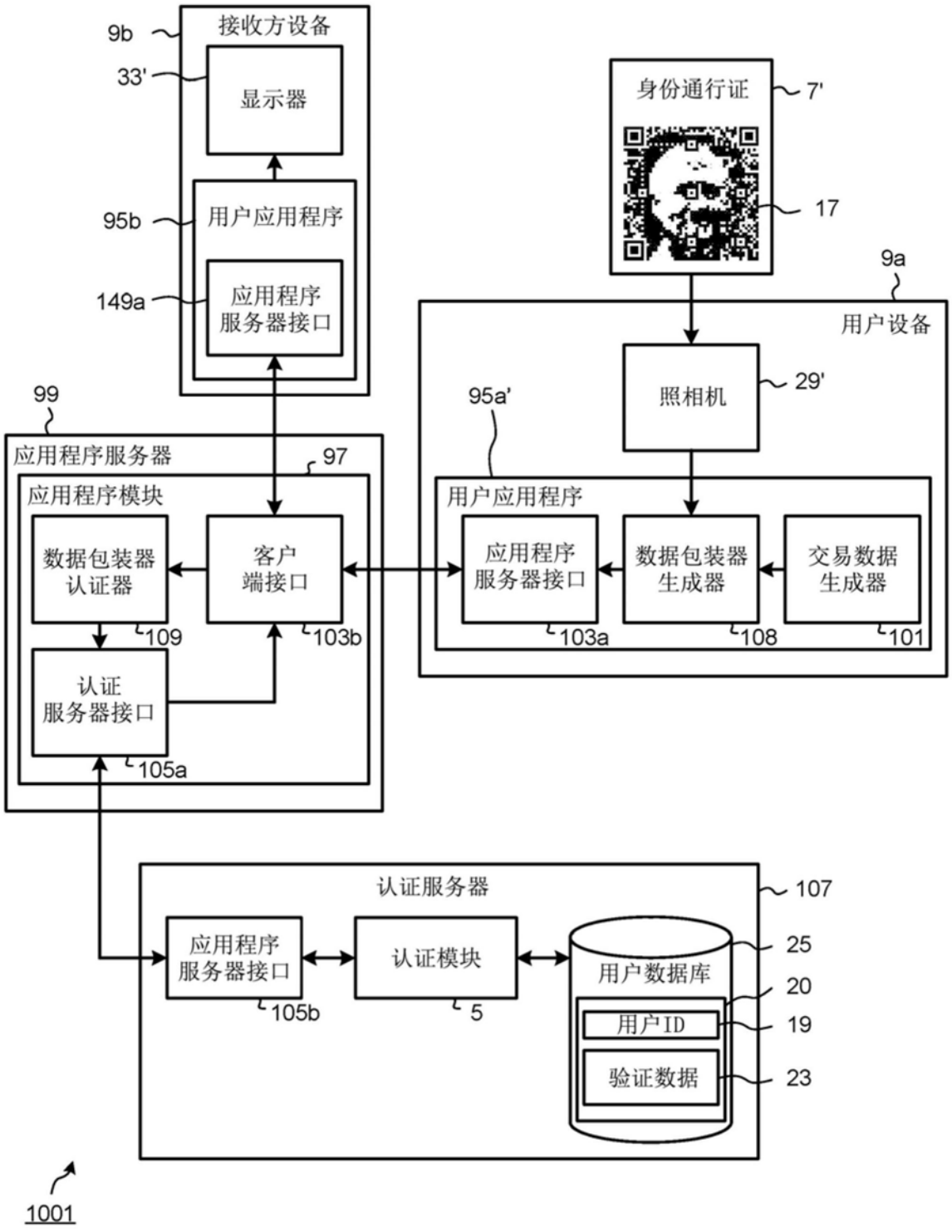

9b
接收方设备
33'
显示器
95b
用户应用程序
149a
应用程序
服务器接口
身份通行证
7'
17
9a
用户设备
照相机
29'
95a'
99
应用程序服务器
97
应用程序模块
用户应用程序
数据包装器
认证器
客户
端接口
应用程序
服务器接口
数据包装器
生成器
交易数据
生成器
109
103b
103a
108
101
认证
服务器接口
105a
认证服务器
107
应用程序
服务器接口
105b
认证模块
5
用户数据库
25
20
用户ID
19
验证数据
23
1001

图10

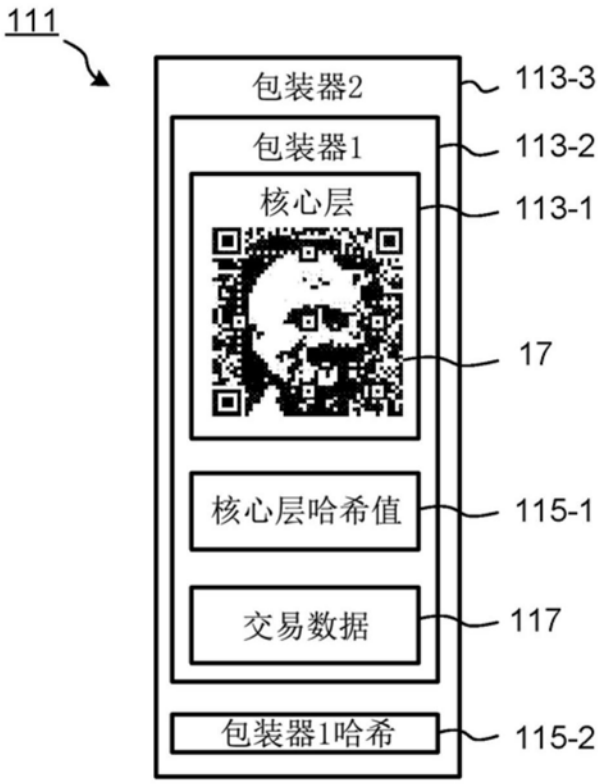

111
包装器2
113-3
包装器1
113-2
核心层
113-1
17
核心层哈希值
115-1
交易数据
117
包装器1哈希
115-2

图11

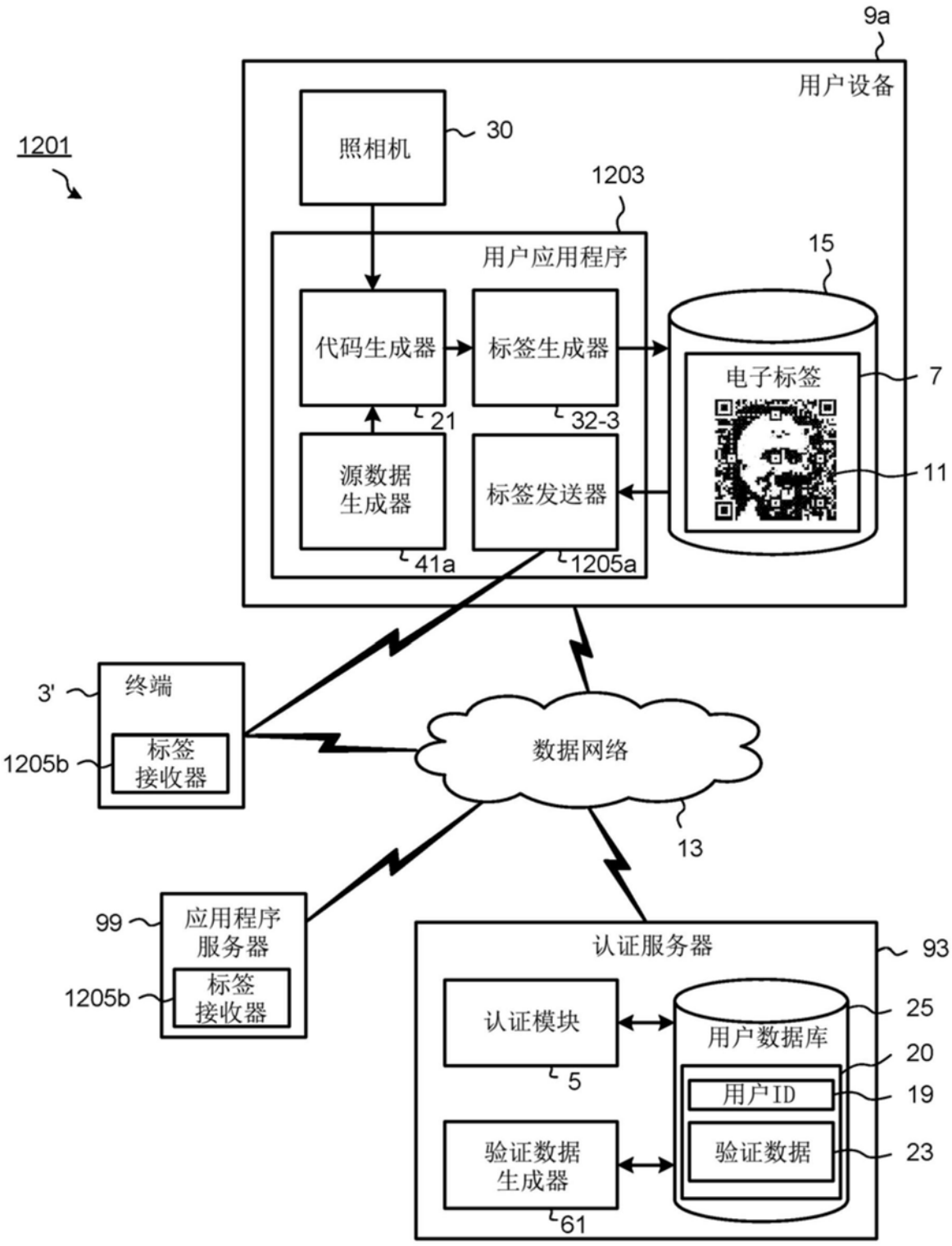

9a
用户设备
1201
照相机
30
1203
用户应用程序
15
代码生成器
标签生成器
电子标签
7
21
32-3
源数据
生成器
标签发送器
11
41a
1205a
3'
终端
1205b
标签
接收器
数据网络
13
99
应用程序
服务器
1205b
标签
接收器
认证服务器
93
认证模块
用户数据库
25
20
5
用户ID
19
验证数据
生成器
验证数据
23
61

图12

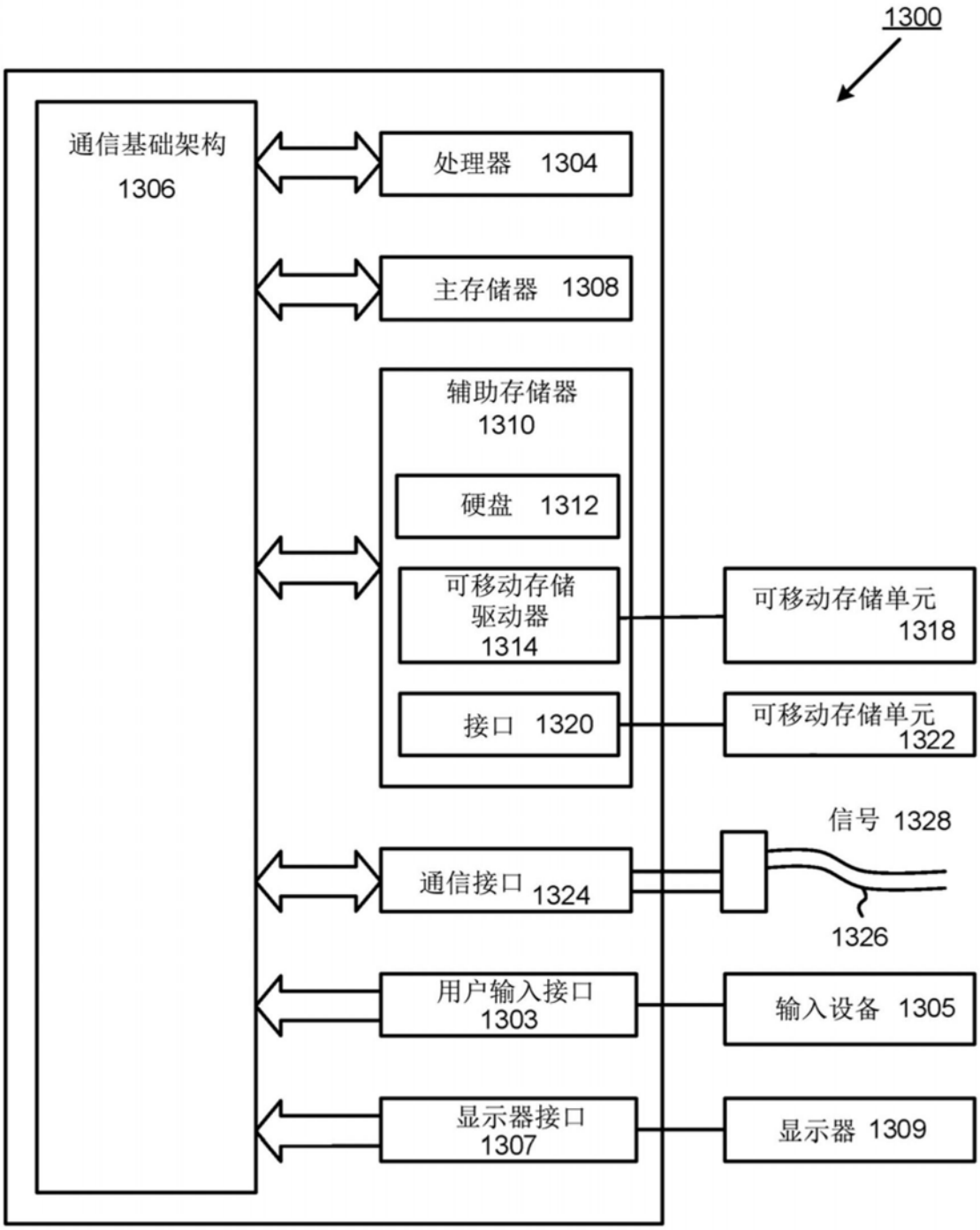

1300
通信基础架构
1306
处理器 1304
主存储器 1308
辅助存储器
1310
硬盘 1312
可移动存储
驱动器
1314
接口 1320
可移动存储单元
1318
可移动存储单元
1322
信号 1328
通信接口 1324
1326
用户输入接口
1303
输入设备 1305
显示器接口
1307
显示器 1309

图13