(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112287389 B
(45)授权公告日 2024.08.02

(21)申请号 202011122541.3

(22)申请日 2016.03.02

(65)同一申请的已公布的文献号
申请公布号 CN 112287389 A

(43)申请公布日 2021.01.29

(30)优先权数据
62/127,404 2015.03.03 US

(62)分案原申请数据
201680013686.5 2016.03.02

(73)专利权人 旺德海尔斯有限责任公司
地址 美国佐治亚州

(72)发明人 肯尼思·希尔 K·S·希尔

(74)专利代理机构 隆天知识产权代理有限公司 72003
专利代理师 石海霞 金鹏

(51)Int.Cl.
*G06F 21/62*(2013.01)
*G06F 21/36*(2013.01)
*G06K 7/10*(2006.01)
*G16H 10/65*(2018.01)
*G06K 7/14*(2006.01)
*G06K 19/06*(2006.01)
*H04L 9/08*(2006.01)
*H04L 9/14*(2006.01)

(56)对比文件
US 2013191640 A1,2013.07.25
US 2006088166 A1,2006.04.27

审查员 杨珺

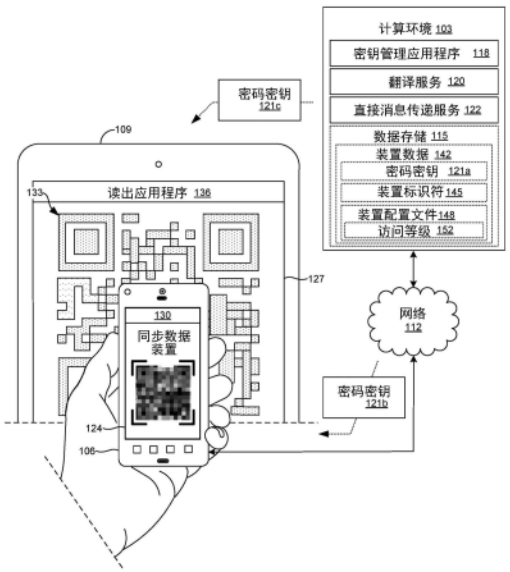
权利要求书3页 说明书25页 附图25页

(54)发明名称

# 机器可读标识符中加密数据的访问控制

(57)摘要

公开了当各个读出装置读取时,用于提供对单个机器可读标识符的底层数据的访问控制的各个实施例。客户端装置可接收与第一装置配置文件相关联的第一密码密钥以及与第二装置配置文件相关联的第二密码密钥。摄取过程提供的数据被格式化成至少第一数据部分和第二数据部分,其中所述第一数据部分旨在用于第一读出装置,所述第二数据部分旨在用于第二读出装置。所述第一数据部分可被所述第一密码密钥加密,所述第二数据部分可被所述第二密码密钥加密。可以使用由加密的所述第一数据部分以及加密的第二数据部分生成机器可读标识符。




CN 112287389 B

1.一种系统,包括:

客户端装置,包括至少一个硬件处理器;

客户端应用程序,能够在所述客户端装置中执行,包括程序指令,该程序指令在被执行时使得所述客户端装置:

响应于所述客户端装置上做出的第一装置配置文件的选择,从至少一个远程计算装置通过网络接收与所述第一装置配置文件相关的第一密码密钥;

响应于所述客户端装置上做出的第二装置配置文件的选择,从所述至少一个远程计算装置通过所述网络接收与所述第二装置配置文件相关的第二密码密钥,其中,所述第二装置配置文件与至少一个第二访问等级相关联,所述至少一个第二访问等级与至少一个第一访问等级不同,所述第一密码密钥与所述第二密码密钥不同;

从所述客户端装置的数据存储中访问输入数据,所述输入数据通过由所述客户端应用程序生成的至少一个用户界面提供;

将所述输入数据格式化成第一数据部分和第二数据部分,所述第一数据部分与所述第二数据部分不同;

使用所述第一密码密钥加密所述第一数据部分,以及使用所述第二密码密钥加密所述第二数据部分,使得所述第一数据部分仅能够由具有所述第一密码密钥的第一读取装置访问,所述第二数据部分仅能够由具有所述第二密码密钥的第二读取装置访问;所述第一读取装置与所述第二读取装置不同;

使用加密的所述第一数据部分和加密的所述第二数据部分生成机器可读标识符,以呈现在所述客户端装置能够访问的显示器中;其中与所述第一装置配置文件相关联的所述第一读取装置具有存储在其上的所述第一密码密钥;与所述第二装置配置文件相关联的所述第二读取装置具有存储在其上的所述第二密码密钥;以及

其中所述第一读取装置被配置为使用所述第一密码密钥根据所述机器可读标识符访问所述第一数据部分,以及所述第二读取装置被配置为使用所述第二密码密钥根据所述机器可读标识符访问所述第二数据部分。

2.根据权利要求1所述的系统,其中,所述机器可读标识符为第一机器可读标识符,并且所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置:

标识由与客户端装置通信的摄像头捕捉的图像中的第二机器可读标识符,所述第二机器可读标识符由不同于所述客户端装置的装置生成;

从所述第二机器可读标识符标识一定量的加密的数据;

使用所述第一密码密钥或所述第二密码密钥解密一定量的加密的数据,以标识解密的数据;以及

将所述解密的数据存储在所述数据存储中,供所述客户端应用程序访问。

3.根据权利要求2所述的系统,其中:将所述解密的数据存储在所述数据存储中进一步包括:

标识存储在所述数据存储中的所述输入数据与所述解密的数据之间是否存在冲突;以及

存储所述解密的数据以替代存储在所述数据存储中的所述输入数据。

4.根据权利要求1所述的系统,其中:

所述客户端应用程序还包括以下程序指令,所述程序指令在被执行时使得所述客户端装置向与所述客户端装置不同的另一客户端装置发送所述机器可读标识符。

5.根据权利要求1所述的系统,其中:

所述第一读取装置包括第一成像装置,所述第二读取装置包括第二成像装置,所述机器可读标识符由所述第一成像装置或所述第二成像装置捕捉。

6.根据权利要求1所述的系统,其中:

根据所述输入数据使用一定量的解密的数据生成所述机器可读标识符。

7.根据权利要求1所述的系统,其中,使用所述第一密码密钥加密所述第一数据部分以及使用所述第二密码密钥加密所述第二数据部分还包括:

标识与所述第一数据部分相关联的所述至少一个第一访问等级;

标识与所述第二数据部分相关联的所述至少一个第二访问等级;

使用所述第一密码密钥至少部分地基于所述至少一个第一访问等级加密所述第一数据部分;以及

使用所述第二密码密钥至少部分地基于所述至少一个第二访问等级加密所述第二数据部分,其中所述至少一个第一访问等级与所述至少一个第二访问等级不同。

8.根据权利要求1所述的系统,其中所述机器可读标识符是快速响应QR码或条形码。

9.一种计算机实现的方法,包括:

响应于客户端装置上做出的第一装置配置文件的选择,由包括至少一个硬件处理器的客户端装置从至少一个远程计算装置通过网络接收与所述第一装置配置文件相关联的第一密码密钥;

响应于所述客户端装置上做出的第二装置配置文件的选择,由所述客户端装置从所述至少一个远程计算装置通过所述网络接收与所述第二装置配置文件相关联的第二密码密钥,其中,所述第二装置配置文件与至少一个第二访问等级相关联,所述至少一个第二访问等级与至少一个第一访问等级不同,所述第一密码密钥是与所述第二密码密钥不同;

由所述客户端装置从所述客户端装置的数据存储中访问输入数据,所述输入数据由至少一个用户界面提供,所述用户界面由能够在所述客户端装置上执行的客户端应用程序生成;

通过所述客户端装置将所述输入数据格式化成至少第一数据部分和第二数据部分,所述第一数据部分与所述第二数据部分不同;

由所述客户端装置使用所述第一密码密钥加密所述第一数据部分以及使用所述第二密码密钥加密所述第二数据部分,使得所述第一数据部分仅能够由具有所述第一密码密钥的第一读取装置访问,所述第二数据部分仅能够由具有所述第二密码密钥的第二读取装置访问;所述第一读取装置与所述第二读取装置不同;

由所述客户端装置使用加密的所述第一数据部分和加密的所述第二数据部分生成机器可读标识符,以呈现在所述客户端装置能够访问的显示器中;

通过所述第一读取装置使用所述第一密码密钥根据所述机器可读标识符访问所述第一数据部分,所述第一读取装置与所述第一装置配置文件相关联且具有存储于其上的第一密码密钥;以及

通过所述第二读取装置使用所述第二密码密钥根据所述机器可读标识符访问所述第二数据部分,所述第二读取装置与所述第二装置配置文件相关联且具有存储于其上的第二密码密钥。

10.根据权利要求9所述的计算机实现的方法,其中,所述机器可读标识符为第一机器可读标识符,所述方法还包括:

通过所述客户端装置标识由与所述客户端装置通信的摄像头捕捉的图像中的第二机器可读标识符,所述第二机器可读标识符由不同于所述客户端装置的装置生成;

通过所述客户端装置根据所述第二机器可读标识符标识一定量的加密的数据;

使用所述第一密码密钥或所述第二密码密钥,通过所述客户端装置解密所述一定量的加密的数据,以标识解密的数据;以及

通过所述客户端装置将所述解密的数据存储在所述数据存储中,供客户端应用程序访问。

11.根据权利要求10所述的计算机实现的方法,其中将所述解密的数据存储在所述数据存储中进一步包括:

通过以下方式进行访问:

通过所述客户端装置标识存储在所述数据存储中的所述输入数据与所述解密的数据之间是否存在冲突;以及

通过所述客户端装置存储所述解密的数据以替代存储在所述数据存储中的所述输入数据。

12.根据权利要求9所述的计算机实现的方法,其中,所述第一读取装置包括第一成像装置,所述第二读取装置包括第二成像装置,由所述第一成像装置或所述第二成像装置捕捉所述机器可读标识符。

# 机器可读标识符中加密数据的访问控制

[0001] 本申请是申请号为2016800136865、发明名称为“机器可读标识符中加密数据的访问控制”、申请日为2016年3月2日的发明专利申请的分案申请。

[0002] 相关申请的交叉引用

[0003] 本申请要求于2015年3月3日提交的、序列号为62/127,404、题目为“用编码的健康信息生成标识符”的共同未决美国临时专利申请的权益和优先权,其内容特此通过引用被整体合并至此。

## 背景技术

[0004] 机器可读标识符可被用于格式化读出装置(诸如条形码或矩阵码扫描器)可识别的介质中的数据。然而,具有合适的读出器的任何人可获得机器可读标识符中体现的数据,除非底层数据被加密。管理哪一装置可以访问机器可读标识符中的加密数据仍存在问题。

## 技术领域

[0005] 本公开涉及密码学、机器可读标识符技术、数据安全,以及在某种程度上涉及计算机视觉。

## 附图说明

[0006] 参考以下附图,可更好地理解本公开的多个方面。附图中的部件并非成比例的,而重点是在于清楚地示出本公开的原理。然而,在附图中,相同的附图标记指示多个视图中相应的部分。

[0007] 图1示出了根据各个实施例的用于向由客户端应用程序收集的信息提供访问控制的网络化环境的一个示例。

[0008] 图2示出了根据各个实施例用于通过加密的机器可读标识符扩增和更新内容数据的网络化环境的另一示例。

[0009] 图3示出了根据各个实施例的用于生成机器可读标识符的数据结构,其部分数据用多个密钥加密。

[0010] 图4包括示出了40-L版本的矩阵编码的容量的表格。

[0011] 图5包括示出了用于编码数据模式的模式指示符二进制数字的表格。

[0012] 图6是示出了根据各个实施例的用于机器可读标识符中加密和编码数据的一个示例的流程图。

[0013] 图7A至图7N示出了根据各个实施例的客户端应用程序生成的用户界面的各个示例。

[0014] 图8是示出了根据各个实施例的用于配置计算装置或客户端装置以生成机器可读标识符的代码一个示例的伪代码。

[0015] 图9示出了根据各个实施例的使用另一装置生成的机器可读标识符在客户端装置上更新或扩增数据的一个示例。

[0016] 图10-图12是示出了根据各个实施例的在客户端装置中执行的客户端应用程序的功能的流程图。

[0017] 图13和图14是示出了根据各个实施例的在计算环境中执行的远程应用程序的功能的流程图。

[0018] 图15至图17是提供根据各个实施例的图1和图2的网络化环境中使用的计算环境、客户端装置以及读出装置的例证的示意方框图。

## 具体实施方式

[0019] 本公开涉及用于机器可读标识符中分段数据的访问控制。机器可读标识符,诸如条形码、矩阵码或其它类似的标识符,可被用于格式化读出装置(诸如条形码或矩阵码扫描器)可识别的介质中的数据。尽管机器可读标识符可被用于将数据从一个装置传递到另一个装置,而不使用有线或无线网络,但是具有合适读出器的任何人可获得体现在机器可读标识符中的数据,除非底层数据被加密。由于底层数据可能是敏感的,所以用户会希望控制哪一部分底层数据能够被各种装置读出。

[0020] 例如,在一些示例中,医疗信息可被编码在机器可读标识符中。人们有时被要求来生成他/她希望保密的敏感数据,诸如,在访问诊所的过程中提供病史。脊椎按摩师、整体医疗提供者、兽医、紧急或急诊医学中心、牙医诊所、保险公司等通常需要病例以及其它个人标识信息。如果人们无法提供这种信息,则家庭成员会承担代表他们的亲属向健康护理提供者提供这种信息的责任。

[0021] 尽管一个人可能会希望向他或她的全科医生提供完整的病历,但这个人可能不希望向另一个提供者(诸如脊椎按摩师或牙医)提供完整的病例。替代地,他们会希望将数据限制为与健康护理专业人士相关。因此,在各个实施例中,单个机器可读标识符可由数据编码,其中不同装置能够读出该数据的不同部分。例如,一个人可以授权他或她的全科医生从矩阵码中获得完整的病例,而脊椎按摩师在使用同样的矩阵码时可仅能够获得病例的一个被用户授权的子集。

[0022] 根据各个实施例,与使用纸和笔填写医疗表格的标准实践相反地,用户可使用他的或她的电子装置(诸如智能手机或平板电脑)来提供医疗摄入信息。由于用户通过电子装置提供的医疗、个人以及其它微妙信息可能是敏感的,因此通过网络发送信息会引起担心。例如,信息可被数据包侦听软件或未授权访问点拦截。此外,存储信息的数据库可被侵入。正因为如此,机器可读标识符(诸如条形码或矩阵码)可被用于在邻近装置之间传递信息,无不使用网络。

[0023] 然而,机器可读标识符通常依赖于开源或透明标准,这使得机器可读标识符中体现的数据的解释易遭到未经授权的访问。例如,如果医疗信息被嵌入到矩阵码中,则任何可商业获得的矩阵码读出器都能够获得该医疗信息。虽然底层数据可被加密,使得仅有权使用合适密钥的装置能够解密该数据,但是,因为人们可能意识到具有密钥的所有装置均能够访问他们的信息,所以在多个装置之间共享该一个密钥会阻止人们提供完整数量的信息。

[0024] 因此,在此处所述实施例中,提供了对机器可读标识符中分段数据的访问控制。在一个实施例中,可在客户端装置上执行的客户端应用程序可被配置为通过网络接收与第一

装置配置文件相关的第一密码密钥(cryptographic key),以及与第二装置配置文件相关的第二密码密钥。客户端应用程序可便于通过摄取过程从用户收集输入数据,该摄取过程可以包括提示用户输入各种数据的一系列用户界面。一旦接收到数据,客户端应用程序会将输入数据分割或以其它方式格式化成至少第一数据部分和第二数据部分。例如,第一数据部分能够被全科医生的读出装置解释,而第二数据部分能够被脊椎按摩师的读出装置解释。

[0025] 客户端应用程序可用第一密码密钥加密第一数据部分,用第二密码密钥加密第二数据部分。远程应用程序,此处称为密钥管理应用程序,可在用户的授权下,在诸如服务器的远程计算装置中执行并监督能够解密数据的密钥的传送和收到。可替代地,在其它实施例中,接收装置可与远程计算环境中的密钥相关联。远程应用程序可向客户端应用程序提供用于接收装置的密钥,使得信息被加密以被接收装置访问。最终,客户端应用程序可使用加密的第一数据部分和加密的第二数据部分生成机器可读标识符,以呈现在客户端装置可访问的显示器中。接收装置可捕捉机器可读标识符的一幅或多幅图像,以使用自动图像分析和计算机视觉访问底层数据。

[0026] 作为非限制性示例,客户端应用程序的用户可将他或她的全科医生与高等级访问相关联,在该等级中,全科医生能够使用他或她的装置访问客户端应用程序的用户提供的所有输入数据。密钥管理应用程序可向全科医生的装置以及用户的装置发送密钥。类似地,密钥管理应用程序可向脊椎按摩师或其它医疗提供者的装置以及用户的装置发送密钥。客户端应用程序可将授权数据编码,以供全科医生使用相应密钥接收,同时将授权数据编码,以供脊椎按摩师使用对于脊椎按摩师不同的的密钥接收。为此,提供了使用单个机器可读标识符,对机器可读标识符的底层数据的访问控制。

[0027] 可以理解的是,因为存在多种拦截通过网络传输的数据的方法,所以存在在装置间传递敏感数据的技术问题,而不使用网络。此外,存在的技术问题是有多种方式可以无授权地获得网络存储数据(存储在网络装置上的数据)。因此,本文所述的实施例通过提出在装置之间传输敏感数据的方式而解决了该技术问题,而不使用网络来传输和接收敏感数据。

[0028] 尽管该公开提供了健康护理数据情况下的多个示例,但此处所附实施例可被应用在许多行业。此外,本公开提供了矩阵码和其它类似的机器可读标识符的情况中的示例。然而,在一些实施例中,视觉图像识别可被用于辨识以不同图像形式编码的数据,诸如被用于RICOH®销售的Clickable PaperTM(可点击纸张)应用程序中。

[0029] 在下文描述中,提供了对系统及其部件的整体说明,然后是对系统及其部件的操作的描述。

[0030] 参考图1,其示出了根据各个实施例的网络化环境100。网络化环境100包括计算环境103、客户端装置106以及读出装置109,它们通过网络112相互数据通信。在各个实施例中,如下文将要描述的,除了密码密钥,客户端装置106和读出装置109通过网络112相互之间可不传达任何信息。网络112包括,例如因特网、内联网、外联网、广域网(WANs)、局域网(LANs)、有线网络、无线网络或其它适合的网络等、或者两个或多个这种网络的任意组合。例如,这种网络可包括卫星网络、电缆网络、以太网以及其它类型的网络。

[0031] 计算环境103可包括例如服务器计算机或提供计算能力的任何其它系统。可替代

地,计算环境103可使用多个计算装置,这些计算装置可例如被布置为一个或多个服务器库、计算机库、或其它布置方式。这种计算装置可被放置在单个安装处,或者可被分布在多个不同的地理位置。例如,计算环境103可包括多个计算装置,这些计算装置一起可包括托管计算资源、网格计算资源和/或任何其它分布式计算配置。在一些情况中,计算环境103可对应于弹性计算资源,其中处理、网络、存储或其它计算相关资源所分配的容量可随时间变化。

[0032] 根据各种实施例,可在计算环境103中执行各种应用程序和/或其它功能。另外,各种数据被存储在数据存储115中,计算环境103可进入该数据存储115。可以理解的是,数据存储115可代表多个数据存储115。例如,数据存储115中存储的数据与下文描述的各种应用程序和/或功能实体的操作相关。

[0033] 例如,计算环境103上执行的部件可包括密钥管理应用程序118、翻译服务120、直接消息传递服务122以及本文未详细描述的其他应用程序、服务、进程、系统、引擎或功能。可以执行密钥管理应用程序118,以监督存储在数据存储115中的各种密码密钥121a...121c的传输和接收,如下文所述。

[0034] 可以执行翻译服务120,以将用户输入从第一语言(诸如西班牙语)翻译成第二语言(诸如英语)。在一些实施例中,翻译服务120可被用于将存储在计算环境103中的、用于摄取过程的问题从第一语言翻译成第二语言。

[0035] 直接消息传递服务122可被用于将加密的直接消息通过网络从一个客户端装置106发送到另一个。在一个实施例中,可在客户端装置106上执行的应用程序对客户端装置106的用户生成的消息加密并将该加密的消息通过网络112发送到直接消息传递服务122,然后该直接消息传递服务122将该加密的消息传输到接收方客户端装置106。在一个示例中,直接消息传递服务122允许患者与他或她的健康提供者直接交流。在其它实施例中,如下文将要描述的,可使用机器可读标识符在客户端装置106之间传递消息。

[0036] 在其它实施例中,计算环境103可包括提供加密信息(诸如加密的健康信息)的基于云存储的应用程序或服务,尽管在其它实施例中,加密信息可不存储在计算环境103中。

[0037] 客户端装置106代表可被耦接到网络112的多个客户端装置。客户端装置106可包括例如基于处理器的系统,诸如计算机系统。这种计算机系统的具体形式可为台式电脑、笔记本电脑、个人数字助理、移动电话、智能手机、机顶盒、音乐播放器、上网平板、平板电脑系统、游戏机、电子图书阅读器、智能手表或具有相似功能的其它装置。客户端装置106可包括客户端装置显示器124,读出装置109可包括读出器装置显示器127。客户端装置显示器124和读出装置127可包括例如一个或多个装置,诸如液晶显示(LCD)显示器、基于气体等离子体的平板显示器、有机发光二极管(OLED)显示器、电泳墨水(E墨水)显示器、LCD投影仪或其它类型的显示装置等。

[0038] 客户端装置106可被配置为执行各种应用程序,诸如客户端应用程序130和/或其它应用程序。可以在客户端装置106中执行客户端应用程序130,例如,以执行摄取过程,从而在客户端装置显示器124中呈现一系列用户界面131a,以提示用户进行用户输入。在一个示例中,一个或多个问题被提供给用户,以获得个人信息、医疗信合或其它适当的信息。一个或多个问题可从计算环境103获得,或被硬编码在客户端应用程序130中。

[0039] 客户端应用程序130可对用户输入进行加密并用加密的用户输入生成机器可读标

识符133。可以理解的是,读出装置109使用读出应用程序136解释机器可读标识符133并访问加密的用户输入。使用一个或多个密码密钥121,读出应用程序136可解密被加密的用户输入,以供读出装置109上的本地存储或远程存储。

[0040] 在一些实施例中,客户端应用程序130和读出应用程序136可包括例如浏览器、专用应用程序等,客户端应用程序130生成的用户界面131a或读出应用程序136生成的用户界面131b可包括网络页面、应用程序屏幕等。客户端装置106可被配置为执行客户端应用程序130以外的应用程序,诸如,例如电子邮件应用程序、社交网络应用程序、文字处理器、电子表格和/或其它应用程序。

[0041] 读出装置109可包括前置成像装置139或后置成像装置(未示出),诸如照相机或能够解释机器可读标识符133的其它装置。可在读出装置109中执行读出应用程序136,以捕捉客户端应用程序130生成的机器可读标识符133的一幅或多幅图像。类似地,客户端装置106可包括一个或多个成像装置,诸如前置或后置照相机。在各个实施例中,读出应用程序136还被执行为解密从机器可读标识符133获得的加密的用户输入,并在读出装置显示器127中呈现健康信息。

[0042] 读出应用程序136可被配置为保留用户提供的多个版本的数据并生成便于特定类型数据或不同版本之间浏览(navigate)的适合界面。尽管客户端应用程序130可被配置为禁止在网络112上传输医疗或其它类型的信息,但在一些实施例中,读出应用程序136可以将数据传达到远程或基于云的服务(诸如符合HIPAA的电子健康档案系统)。尽管客户端应用程序130可以不通过网络112发送健康或其它类型的信息,但计算环境103可在数据存储115中备份或存储各个版本的机器可读标识符133。当用户升级或替换他或她的客户端装置106时,机器可读标识符133可被用于在新的客户端装置106上填充数据。

[0043] 可理解的是,数据存储115中存储的数据可包括装置数据142和其它数据。装置数据142可包括与一个或多个客户端装置106和读出装置109相关联的信息。在一个示例中,每个读出装置109可与唯一的密码密钥121相关联,其中密钥管理应用程序118向客户端应用程序130发送密码密钥121。然后客户端应用程序130可为读出装置109生成包括被密码密钥121加密的用户输入数据的机器可读标识符133。由于读出装置109也保留其密码密钥121的副本,因此其能够解密并解释用户输入数据。

[0044] 在另一个示例中,每个客户端装置106可与一个或多个密码密钥121相关联,其中密钥管理应用程序118根据客户端应用程序130的用户的指令向读出装置109发送密码密钥121。客户端应用程序130可生成包括被一个或多个密码密钥121加密的用户输入数据的机器可读标识符133。例如,密钥管理应用程序118可以根据客户端应用程序130的用户的指令向读出装置109发送密码密钥121,使得其能够解密并解释用户输入数据。

[0045] 装置数据142可包括装置标识符145,其唯一地标识客户端装置106或读出装置109。装置数据142还可包括装置配置文件148,而该装置配置文件148可包括访问等级152。在一些实施例中,客户端应用程序130的用户可将某一读出装置109与特定访问等级152相关联。在一个示例中,一个人可将用于他或她的全科医生的第一读出装置109与第一访问等级相关联,将用于他或她的牙医的第二读出装置109与第二等级相关联。为此,客户端应用程序130的用户可基于访问等级指定哪些数据可以被哪一读出装置109访问。如将要描述的,用户输入可被每个读出装置109可获得的信息分段或划分。为此,读出应用程序136可为

由用户指定的、或由计算环境103预定的信息提供不同的访问等级。

[0046] 密码密钥121可包括用于加密数据的数字、二进制或字母数字字符串。在各个实施例中,密码密钥121可包括对称密码密钥121、非对称密码密钥121或其组合。

[0047] 参考图2,其示出了根据各个实施例的网络化环境100的另一个示例。在一些情形下,可在读出装置109或能够访问解密信息的其它装置上操作客户端应用程序130的用户提供的输入数据。例如,医生可将用户提供的数据修改成包括最新的血压、体重或其它信息。用户可能希望将该信息存储在他或她的客户端装置106上,以保持更完整和精确的病例。

[0048] 为此,在一些实施例中,读出应用程序136可使用其密码密钥121(或客户端装置106可获得的其它密码密钥121),以向客户端装置106提供更新的、修改的、补充的或以其它方式操作的数据。客户端应用程序130可便于捕捉在读出装置109上生成的、并呈现在读出装置显示器127中的机器可读标识符133的一幅或多幅图像。

[0049] 在各个实施例中,使用密码密钥121来加密由读出应用程序136产生的机器可读标识符133的底层数据,仅客户端装置106和读出装置109可获得该密码密钥121。客户端应用程序130可解密底层数据并将数据本地存储在客户端装置106上。如果用户执行了部分摄取过程,则更新后的数据可被提供在用户界面131中的自动填充字段中。通过扫描机器可读标识符133并使适合的密码密钥121访问底层数据,读出应用程序136可本地更新存储的数据,并且可与其他应用程序(诸如调度应用程序、预约管理应用程序、药物重配(refill)应用程序或EHR应用程序)交互,以更新与其相关联的信息。

[0050] 接下来参考图3,示出了数据结构300的一个示例,该数据结构300包括用于生成机器可读标识符133a...133c的图像的数据。可以理解的是,数据结构300可包括例如纠错等级303、字符计数指示符306、模式指示符309、有效载荷312、纠错315和/或其它数据。

[0051] 矩阵码,也被称为快速响应(QR)码,通常使用Reed-Solomon纠错,其被用于基于编码的数据产生纠错代码字(字节)。读出应用程序136a...136b可使用这些纠错等级303来确定数据是否被错误地读出,如果是,则使用纠错代码字纠正数据中的错误。对于矩阵码,有四个等级的纠错等级303,被命名为L、M、Q和H,其纠错能力分别为7%、15%、25%和30%。

[0052] 矩阵码具有不同的尺寸,一个特定尺寸的矩阵码被称为一个版本。可用的版本有四十个,但是其它的版本也是可以的并且被包括在本公开的范围内。例如,版本1是最小版本的矩阵码,尺寸为21像素乘21像素。每个版本比前一版本大4个像素。版本4是最大的版本,其为177像素乘177像素。最大的版本具有最大的字符容量,如图4的表格所示。

[0053] 可根据模式指示符309设置的不同模式来编码有效载荷312。模式指示符309可包括四位字符串,如图5所示。编码的数据可从合适的模式指示符开始,其描述了被用于后续位的模式。最大的版本的矩阵码具有最高的字符容量,如图4的表格所示。字符计数指示符306包括被编码的字符的个数。

[0054] 为了生成机器可读标识符133,客户端应用程序130(或读出应用程序136)可访问摄取过程中接收的用户输入,并用密码密钥121加密该数据。在密码密钥121是非对称的实施例中,可采用RSA或其它适合的加密算法。在密码密钥121是对称的实施例中,可采用高级加密标准(AES)或其它适合的加密算法。可根据模式指示符309来编码被加密的用户输入。例如,假设加密的用户输入为一串字母数字字符,则模式指示符309可被设置为0010。字母数字编码可包括将串分成多个对,并为每个对创建二进制数字。

[0055] 用于第一读出装置109a的数据可被第一读出装置109a可访问的密码密钥121(如图3所示,密码密钥$121_A$)加密并被编码为有效载荷$_A$。类似地,用于第二读出装置109b的数据可被第二读出装置109b可访问的密码密钥121(如图3所示,密码密钥$121_B$)加密并被编码为有效载荷$_B$。当被读出装置109扫描时,仅一部分有效载荷$_{Total}$可被读出装置109解释。

[0056] 接下来参考图6,其所示的流程图示出了输入数据至矩阵码或其它机器可读标识符133的转换。从步骤603开始,用户输入被访问。用户输入可以包括例如健康信息、紧急联系信息或摄取过程中或者从客户端应用程序130呈现的用户界面131获得的其它类型的数据。在图6的示例中,出于解释的目的,一串用户输入包括“Hello world”。

[0057] 在步骤606中,基于读出装置109标识密码密钥121,其中数据被用于该读出装置109。例如,用户可指定他或她的病例的特定部分,以供他或她的全科医生使用。用于全科医生的一个或多个读出装置109的密码密钥121可被标识。在步骤609中,使用步骤606中标识的密码密钥121来加密用户输入。使用AES加密和密钥“exampleencryptionkey”,一串加密数据包括“BBd2iHwO/gy+xnFUg6HeAA==”。

[0058] 接下来,在步骤612中,使用字母数字模式或其它合适的模式(诸如数字、字节、日本汉字或ECI)对加密的数据进行编码。对于加密数据的前两个字符“BB”,使用字母数字编码生成二进制数字,以得到“111111010”。这可以继续进行,直到所有的加密数据被以合适的模式编码。最终,在步骤615,根据矩阵码标准,使用编码数据作为有效载荷生成矩阵码的图像。

[0059] 在各个实施例中,AES-256加密算法可被用于对底层数据加密。初始矢量(IV)或开始变量(SV)可被采用,以供随机化加密并产生不同密文的模式使用,即使相同的明文被加密多次。(AES CBC Pkcs7)。一些模式,诸如电子密码本(ECB)和密码块链接(CBC),可能会要求在加密之前对最后一块进行填充,因此可采用适合的填充。

[0060] 在采用AES-256的实施例中,密码密钥121可包括256比特(32字节),其中IV为128比特(16字节)。对于客户端应用程序130或读出应用程序136执行的每次加密,可随机生成IV,以提供不同的加密结果(与之前的加密不同),即使待加密的数据并未改变。考虑到将来的解密,生成的IV可以与加密的数据一起本地存储在客户端装置106或读出装置109上,如此处所述。

[0061] 在一些实施例中,加密数据被本地存储在与密码、生物数据或PIN码相关联的客户端装置106或读出装置109上。此外,每个用户或为其提供数据的实体(例如,患者、亲戚、宠物)可具有他或她自己的密码密钥121(即,加密密钥)。因此,被加密在特定装置上的任何数据只可在提供了适合的密码、生物数据或PIN码时在该装置上被解密。

[0062] 由于AES加密算法需要密码密钥121和IV以加密或解密数据,因此IV可与加密数据联合存储,从而在将来被成功解密。在一些实施例中,密钥管理服务115管理IV向客户端装置106或读出装置109的存储和传输以及密码密钥121。IV密钥可包括16个字节或其它合适的长度。在一些实施例中,IV密钥可被拆分并存储在沿密码密钥121的预定义位置中。例如,IV密钥的第一数量的字节可被放置在密码密钥121中的第一位置处,而IV密钥的第二数量的字节可被放置在密码密钥121中的第二位置处,等等。在使用密码密钥121之前,可从密码密钥121中移走IV密钥。该特征在加密数据中增加了额外的安全等级。例如,即使密码密钥121被拦截、被蛮力地成功猜中等,而不知道如何从数据中恢复IV,如果有可能解密被加密

的数据的话,也将是很困难的。

[0063] 图7A至图7N示出了用于通过利用各种类型的用户输入提示用户而执行摄取过程的客户端应用程序130的用户界面131的各种示例。可以理解的是,在执行摄取过程之前,要求用户提供用户名、密码、生物计量信息、或适当地鉴定客户端装置106的用户的其它信息。在图7A中,示出了用于客户端应用程序130的示例性主屏幕,其中用户可为个体输入基本信息。这可不包括医疗信息,而包括用于标识目的的信息。这可被用于标识个体(例如,所有者、被抚养人、宠物或其它个体)的名字。

[0064] 接续,客户端应用程序130可提示用户输入基本信息,诸如出生日期、紧急联系信息、初级护理医师联系信息、或其它基本信息。用户界面131还可允许用户改变为其提供信息的个体。例如,用户可将个体从他自己或她自己更改为另一个体,诸如孩子、被抚养人、宠物等。这些二级配置文件也将具有数据字段,以放置关于初级护理医师、紧急联系信息、病历等的信息。

[0065] 图7B示出了符合健康保险携带和责任法案(HIPAA)合规性以及文档用户界面131的实施例。根据该用户界面131,示出与各种法规(诸如HIPPA)相关的信息,其后跟随适合的解释,以获得必要的准许。在各个实施例中,可生成链接或其它用户界面部件,其使得另一应用程序(诸如浏览器应用程序)为那些需要关于合规性细节进一步解释的人显示信息。查阅后,可出现电子签名和日期或时间戳的提示,以核实用户已经查阅该材料并获得必要的准许。

[0066] 现在转而参见图7C,用户界面131示出了专用于获得个体的过往医疗信息的屏幕的一个实施例。图7C的用户界面131使得用户能够提供医学专业人士在过去给他们做出的医疗诊断。在各个实施例中,可包括智能文本、自动填充、下拉式建议和/或其它类似组成,以便于纠正最常见病症和/或疾病的拼写。客户端应用程序130还可获得与给出诊断的日期相关的数据。然后可以基于日期,按数字顺序对这些进行排列。在诊断未被列出的情形下,可获得自由文本选项。可为额外的、可能重要的信息创建额外的文本框。

[0067] 图7D示出了用户界面131,其中通过提示用户提供所有之前的手术经历可获得过往手术信息。如上文所提示的,在各个实施例中,可包括智能文本、自动填充、下拉式建议和/或其它类似组成,以便于纠正大多数普通手术或医疗程序的拼写。如果知晓的话,也可获得这些手术程序的日期和机构。然后以具有手术程序被执行的日期和机构的相关数据字段的时间顺序来排列手术程序。在手术程序未被列出的情况中,可获得自由文本的选项。

[0068] 接续参考图7E,其示出了用户界面131,该用户界面131示出了专用于获得当前和过往药物治疗的屏幕的实施例,其能够使用户提供当前或之前的药物。在各个实施例中,可包括智能文本、自动填充、下拉式建议和/或其它类似组成,以便于纠正大多数普通药物的拼写。可包括所提供药物开始时的日期、用药原因以及服药的剂量和频率。在用户不再服用的旧药的情况下,将包括用于药物停止的日期的字段并具有为何停止服用的原因。在药物未被列出的情况中,可获得自由文本的选项。

[0069] 图7F示出了用户可提供当前和过往过敏、药物治疗、环境触发、动物和其它相关信息的用户界面131。在各个实施例中,可包括智能文本、自动填充、下拉式建议和/或其它类似组成,以便于纠正大多数普通药物和过敏原的拼写。还将包括对过敏原的反应的类型。将以具有对每个过敏原的反应类型的相关字段的数字顺序来放置这些。

[0070] 在图7G的非限制示例中,示出了用户界面131,其使得用户能够提供与她或她的家族病史相关的信息。在一些实施例中,详细的常见临床问题可被呈现给用户,以建议其是否适用于家族病史。合适的数据字段可被用于非常见疾病。此外,可包括智能文本、自动填充、下拉式建议和/或其它类似组成,以便于纠正常见病症和/或疾病的拼写。如果适用,用户还可用年龄和去世年份来描述哪一家族成员具有该诊断。

[0071] 图7H示出了专用于从用户获得社会历史的用户界面131的实施例。例如,一个表格可被呈现给用户,以提供与个人社会历史相关的信息。在一些实施例中,表格包括覆盖吸烟史、饮酒、国外旅行、教育程度等的数据字段。基于根据之前提供的出生日期推算的年龄,这还可包括详细的儿科信息,诸如家庭居住成员、家庭枪支、家庭宠物、铅和结核病接触等。

[0072] 下面参考图7I,用户界面131示出了从用户获得免疫的实施例。可采用智能文本辅助用户正确地拼写免疫。可为出国旅行可能需要的通常不给予的免疫提供开放文本字段。在一些实施例中,提供免疫的日期可以为必填字段。可基于免疫的日期,以年月日次序来排列该信息。

[0073] 图7J示出了用户界面131一个实施例,其使得用户能够提供杂项笔记,该杂项笔记可仅本地保存用于用户访问,或者可被包括在机器可读标识符133中。例如,笔记可包括关于特定医疗经历的提醒。在各个实施例中,这可被限制为100个字符或其它适合的量,这并不是症状列表,而仅仅是特定访问的提醒。与任意其它部分一样,如果无需更新该信息,则该笔记页可保留为空。在一些实施例中,可从机器可读标识符133的数据中排除笔记字段中提供的数据。

[0074] 图7K示出了在客户端装置显示器124中生成用户界面131的客户端装置106的另一附图。在图7K的非限制示例中,所示实施例中为用户提供之前提供给用户的信息。可以理解的是,在获得健康信息的实施例中,可理想地获得关于十一个器官系统中的一个或多个的信息。用户界面131可便于向医生或其它相关人员以用户、管理员预定义的格式或健康护理提供者指定的格式打印或传递信息包。这能够以医生更喜欢的格式来关联信息,且对于所有者和医生都是易读的。在其它示例中,用户界面131可接收与患者的药房、保险或其它相关对象有关的信息。该摄取过程可包括身体系统的核查以及健康筛查。

[0075] 此外,客户端应用程序130可以预定义格式组织在摄取过程中提供的信息。在一个示例中,信息可被以按年月日次序并且按主题(诸如过敏或药物)分类。对于信息为医疗数据的实施例,对健康护理提供者常见的按时间排列的格式提供了一种高效地呈现适用客户端应用程序130获得的数据的方式。其将提供健康护理提供者指定要求的所有健康信息。由于所提供的信息可为完整、准确的,因此其有助于通过正确地标识药物和过敏来限制医疗差错,以及提供被证明为对医生和提供者必要的完整的病例。

[0076] 在被客户端应用程序130加密之前,数据可被格式化和/或压缩,或者读出应用程序136可在被解密和/或解压缩时格式化数据。因此,客户端应用程序130或读出应用程序136均可将数据格式化成预定义格式,诸如临床文档架构(CDA)格式,其包括由Health Level 7International开发的灵活的标记标准。CDA格式包括某些医疗记录的预定义结构,诸如出院小结和病程记录,以在患者和医疗专业人士之间交换信息。CDA格式允许包括文本、图像以及其他类型的多媒体(诸如音频和视频)。在另一实施例中,可由健康护理提供者通过读出应用程序136来指定格式。

[0077] 在各个实施例中,客户端应用程序130可将信息总结导出到Microsoft Word®、PDF®或其它适合的格式,用于用户在健康护理提供者的办公室中或访问之前打印。在一些实施例中,机器可读标识符133可被放置在所生成文档的角落中或另一合适的位置。使用读出装置109,根据具体实践的习惯,健康护理提供者可扫描来自客户端装置显示器124或文档的机器可读标识符133,以将该信息导入到图表或电子健康档案(EHR)。可以理解的是,当客户端应用程序130可被配置为在生成机器可读标识符133之前加密健康信息时,健康护理提供者的读出装置109能够解密机器可读标识符133提供的信息。因此,例如在坐在办公室时,客户端应用程序130的用户可绕开填写医疗摄取表格的漫长过程。由于用户提供的信息可被医疗专业人士更新,因此其有助于通过正确地标识药物和过敏来限制医疗差错,以及提供被证明为对医生必要的完整的病例。

[0078] 客户端应用程序130可包括移动应用程序或通过浏览器应用程序访问的基于网页的应用程序。使用基于网页的应用程序的个体能够为所有者将总结信息转换为Word®或PDF®格式,以在访问之前打印,且当会面结束时可以删除信息。在打印输出的角落,可示出相关的机器可读标识符133。

[0079] 基于健康护理提供者的判定和能力,另一个实施例指定客户端应用程序130生成具有信息和/或机器可读标识符133的附件的电子邮件,以给健康护理提供者、职员或健康系统发送邮件并与其电子分享。所有者在访问之前在家里或当在健康护理提供者的等待室中时可将其完成。信息的格式将是健康护理提供者更喜欢的格式。从这点来看,其能够被打印以被添加到患者的纸质表中、被扫描或手动输入到电子医疗记录中。最后,其可被电链接到EHR或专有的电子医疗记录(EMR)系统。在电子分享该信息之前,可以再次要求所有者审核HIPAA法规以及电子签名和日期/时间戳,以审核该信息。

[0080] 此时转向图7L,示出了具有摄取过程中提供的用户输入的机器可读标识符133。通过将加密图像保存到读出装置109的镜头或照相机,加密的健康信息可被转移,以供读出装置109解释。在一些实施例中,被抚养人可通过捕捉机器可读标识符133的图像而将他或她的信息传递到父母的客户端装置106,反之亦然。当获得必要的准许时,密钥管理应用程序118便于适合的密码密钥121的传递。

[0081] 参考图7M,客户端应用程序130的用户可指定密码密钥121和数据的接收方(诸如读出装置109或不同的客户端装置106的所有者)。在其它实施例中,可由客户端应用程序130或密钥管理应用程序118伪随机地生成密码密钥121。如果由客户端应用程序130生成,则密码密钥121被传送到密钥管理应用程序118,该密钥管理应用程序118转而根据客户端应用程序130的用户的指示将密码密钥121传达给读出装置109或其它客户端装置106。例如,客户端装置106的用户可将传送给一个或多个读出装置109的密码密钥121与“Atlanta Health”提供者相关联。在其它实施例中,基于提供者的选择而使用预定义的密码密钥121。例如,密钥管理应用程序118可为“Atlanta Health”提供者存储一个或多个密码密钥121。当“Atlanta Health”被选择时,客户端应用程序130可使用相关联于“Atlanta Health”提供者而存储的一个或多个密码密钥121,来加密用于机器可读标识符133中的信息。

[0082] 在其它实施例中,密码密钥121可被设置为出生日期、社会保险号码或不会被广泛地或公共地获得的其它常数。然后,可允许获得对于读出和传递以加密的QR图像代表的信

息所必需的软件的任何健康护理提供者电子地、无线地即刻提取用户输入。在一些实施例中,可采用额外的安全层,其中可能要求信息的接收方在信息将被解密之前,输入针对初始用户的另一标识符,诸如出生日期或社会保险号码。

[0083] 可通过将机器可读标识符133保存至健康护理提供者或其它相关人员拥有的读出装置109或另一客户端装置106的照相机镜头来完成提取信息的过程。可以理解的是,这可通过管理部门中的人员在一分钟内或更短时间内完成。然后,所获得的信息可被读出应用程序136或读出装置109上的其它应用程序使用,以被添加到患者的纸质图中或电子医疗记录系统中。此外,读出应用程序136可被配置为自动地填充第三方EMR系统中的字段。

[0084] 下面参考图7N,客户端应用程序130可便于从一个客户端装置106向另一个发送加密的消息。在一个示例中,客户端应用程序130允许患者直接与他或她的健康提供者交流。客户端应用程序130可加密由客户端装置106的用户生成的消息,并通过网络112将该加密的消息发送到直接消息传递服务122。然后,直接消息传递服务122可将加密的信息传送到接收方客户端装置106。在其它实施例中,可使用机器可读标识符133在客户端装置106之间传递消息。客户端应用程序130还可便于机器可读标识符133通过直接消息传递服务122的传输。

[0085] 此时转至图8,其示出了伪代码800,在配置客户端应用程序130、读出应用程序136或用以生成矩阵码或其它类型的机器可读标识符133的其它合适应用程序时,可执行该伪代码800。例如,伪代码的行01中的功能可被以编程的方式调用,以生成矩阵码。行02接收将被包括在机器可读标识符133中的用户输入,诸如在通过呈现图7A至图7K的用户界面131而执行的摄取过程中提供的用户输入。由于用户输入被本地存储在客户端装置106上,因此其可被合适地查询。

[0086] 在行03中,使用合适的函数调用获得密码密钥121。在图8的实施例中,基于为特定读出装置109提供的标识符获得密码密钥121。例如,客户端应用程序130的用户可指定预期的数据接收方。在其它实施例中,用户可指定他或她自己的密码密钥121。在其它实施例中,可使用出生日期、社会保险号码或用户提供的其它信息来伪随机地生成或确定密码密钥121。

[0087] 在行04中,建立模式指示符309。在图8的示例中,模式指示符被设置为“0010”,其指示字母数字模式。在行05中,确定输入数据的字符计数。在行06中,进行函数调用,以实现合适的功能,该功能使用密码密钥121加密用户输入,返回加密字符串或其它合适的变量类型。在行07中,使用合适的函数调用确定Reed-Solomon错误代码。在行08-09中,数据被格式化。在行10中,格式化的数据被提供为可编程函数调用的变量,以生成以图像或其它合适格式的机器可读标识符133。

[0088] 现在转至图9,其示出了从外部来源导入数据的客户端应用程序130的另一个示例。如上文所述,在一些情形中,可在读出装置109或能够访问解密信息的其它装置上操作客户端应用程序130的用户提供的输入数据。例如,医生可将数据更新或修改成包括最新的血压读数、体重测量、血糖水平测量或其它信息。用户可能会希望将该更新后的信息存储在他或她的客户端装置106上,以保持更完整和精确的病例。在一些实施例中,读出应用程序136可生成能够打印的文档900,以插入实体医疗文件中。

[0089] 读出应用程序136可利用其密码密钥121生成具有机器可读标识符133a...133b的

文档900。密钥管理应用程序118可基于读出装置109或生成机器可读标识符133的其它装置为客户端装置106提供合适的密码密钥121。客户端应用程序130可便于捕捉位于文档900上的机器可读标识符133的一幅或多幅图像。一旦机器可读标识符133的图像在客户端装置106上被获得并解密，客户端装置106可更新本地存储的信息和/或在用户界面中自动填充字段以供用户审核。

[0090] 在各个实施例中，使用密码密钥121来加密由读出应用程序136生成的机器可读标识符133的底层数据，仅客户端装置106和读出装置109可获得该密码密钥121。客户端应用程序130可解密底层数据并将数据本地存储在客户端装置106上。如果用户完成了部分摄取过程，则更新后数据可被提供在用户界面131中的自动填充字段中。

[0091] 多个安全机制被构建于代码和客户端应用程序130的执行中。因为潜在的关键信息的广度，在各个实施例中，该信息被本地存储在客户端装置106上。因此，该信息通过“云”的潜在损失可被减少或消除。在各个实施例中，客户端应用程序130可与基于云的系统结合，用于远程输入和更新信息。

[0092] 除了在智能手机或其它类型的客户端装置106上提供的默认密码保护，还需要额外的密码或个人标识符号码(PIN)，以访问客户端应用程序130的特征。连续预定义次数(例如5次)的错误密码会使客户端应用程序的使用失效预定义时间段，诸如24小时。在电子地分享该信息之前，需要表示所有者允许分享该信息的额外标识符。

[0093] 在各个实施例中，被允许从机器可读标识符133撤回信息的健康护理提供者还可被允许更新或扩增信息，并将更新的或扩增的信息以另一种机器可读标识符133的形式提供回所有者。因此，更新的信息可与已经存在于客户端装置106上的信息相协调。以这种方式，所有者将不必输入新的信息，因为这将被客户端应用程序130完成。这还可包括合并移动装置日历的对未来访问的提醒、药物填充的提醒等。在另一示例中，客户端应用程序130可与药房电子地协调药物治疗。

[0094] 客户端应用程序130可体现为多个版本，其中每个版本使用不同的语言，诸如英语、西班牙语、法语或其它语言。如果需要的话，翻译服务120可将用户输入从用户语言翻译到接收方语言。这可发生在对用于机器可读标识符133中的数据编码之前，或者读出应用程序136一解码信息，这就发生。对于当更高级的交流或英语医学术语未知的那些情况，该信息被用于辅助医疗或其它类型的评估。

[0095] 在一个实施例中，机器可读标识符133可被编码在客户端装置106的“锁定屏幕”中，因此，无权访问电话的人可获得重要的标识、健康或联系信息的，而不必解锁客户端装置106。在其它实施例中可在客户端装置106上或读出装置109上定期地(例如，在所用会面结束时)擦除摄取过程中提供的信息。

[0096] 接续参考图10，其示出了一个流程图，该流程图提供了根据各个实施例的客户端应用程序130的一部分的操作的一个示例。可以理解的是，图10的流程图仅提供了可被用于执行如本文所述客户端应用程序130的部分的操作的多个不同类型功能布局中的一个示例。可替代地，图10的流程图可被视为描述根据一个或多个实施例的在客户端装置106中执行的方法的元素的示例。

[0097] 从步骤1003开始，客户端应用程序130被执行为从用户为一个或多个个体(诸如被抚养人、宠物或其它动物等)获得信息，诸如健康信息。这可通过使用用户界面131来完成，

用户界面131接下来被呈现在摄取过程中,在摄取过程中用户在一个或多个会面过程中循环访问用户界面131。然后,在步骤1006中,客户端应用程序130用户是否已经确收HIPPA通知。如果HIPPA通知没有被确收,则HIPAA通知可被描述给用户,步骤可返回1003或继续至结尾。如果用户已经确收HIPAA通知,则步骤行进至1009,其中根据一个或多个预定义加密标准和格式来加密用户提供的基本信息、健康信息或其它信息。

[0098] 在各个实施例中,使用一个或多个密码密钥121来加密数据。在各个实施例中,密码密钥121包括用户提供的信息,诸如出生日期、姓氏、名字、社会保险号码、它们的组合或其它潜在的独特信息。在1012中,加密的信息被用于生成机器可读标识符133,诸如二维码或矩阵码。参照图6和图8描述了用于生成机器可读标识符的步骤。

[0099] 返回至图10,在步骤1015中,可以利用询问用户是否希望在客户端装置显示器124上显示生成的机器可读标识符133的额外通知来提示用户。最后,在步骤1018中,机器可读标识符可被编码在用户界面131中,以呈现在客户端装置显示器124中。此时,用户能够提供机器可读标识符133以用于被读出装置109扫描,或者用户可打印含有信息且并其上具有机器可读标识符133的文档。

[0100] 接续参考图11,其示出了一个流程图,该流程图提供了根据各个实施例的客户端应用程序130的一部分的操作的另一个示例。可以理解的是,图11的流程图仅提供了可被用于执行如本文所述客户端应用程序130的部分的操作的多个不同类型功能布局中的一个示例。可替代地,图11的流程图可被视为描述根据一个或多个实施例的在客户端装置106中执行的方法的元素的示例。

[0101] 从步骤1103开始,可在客户端装置106上执行的客户端应用程序130可被配置为访问与第一装置配置文件148a相关联的第一密码密钥121a。类似地,在步骤1106中,客户端应用程序130可访问通过网络112接收的、与第二装置配置文件148b相关联的第二密码密钥121b。可以理解的是,第一密码密钥121a和第二密码密钥121b可由密钥管理应用程序118或其它类似服务通过网络112发送到客户端装置106。第一密码密钥121a和第二密码密钥121b可响应于某一实体或组织(诸如医疗机构或医疗专业人士)的选择而被提供给客户端应用程序130。在一个示例中,第一密码密钥121a与第一医疗提供者相关联。第一医疗提供者可拥有或操作与第一装置配置文件148a相关联的并且其上存储有第一密码密钥121a的第一读出装置109a。类似地,第二密码密钥121b与第二医疗提供者相关联,由此,第二医疗提供者可拥有或操作与第二装置配置文件148b相关联的并且其上存储有第二密码密钥121b的第二读出装置109b。

[0102] 因为客户端应用程序130便于通过摄取过程从用户收集输入数据,因此在步骤1109中,输入数据可被访问,用于包含在机器可读标识符133中。摄取过程可包括一些列用户界面131,这些用户界面131提示使用者输入各种数据,诸如图7A至图7K中所示的那些。在步骤1112中,客户端应用程序130会将输入数据分割、划分或以其它方式格式化成至少第一数据部分和第二数据部分。例如,第一数据部分能够被全科医生的装置解释,而第二数据部分能够被脊椎按摩师的装置解释。

[0103] 接下来,在步骤1115中,客户端应用程序130可使用第一密码密钥121a加密第一数据部分,同时在步骤1118中,客户端应用程序130可使用第二密码密钥121b加密第二数据部分。在计算环境103中操作的密钥管理应用程序118可监督能够在用户的授权下解密数据的

密码密钥121的传送和接收。可替代地,在其它实施例中,读出装置109可与存储在计算环境103的数据存储115中的预定义密码密钥121相关联。密钥管理应用程序118可为特定读出装置109向客户端应用程序130提供密码密钥121,从而使信息被加密,以供读出装置109或其它客户端装置106访问。

[0104] 在步骤1121中,客户端应用程序130可使用解密的第一数据部分和解密的第二数据部分生成机器可读标识符133,以呈现在客户端装置显示器124中。读出装置109可捕捉机器可读标识符133的一幅或多幅图像,以访问底层数据。

[0105] 在其它实施例中,客户端应用程序的用户可将装置配置文件148(诸如与全科医生有关的一个)与高等级访问相关联,在该等级访问中,全科医生能够使用他或她的装置109,以访问客户端应用程序130的用户提供的所有或大量的输入数据。密钥管理应用程序118可向全科医生的读出装置109以及用户的客户端装置106发送密码密钥121。类似地,密钥管理应用程序118可向脊椎按摩师或其它医疗提供者的读出装置109发送不同的密码密钥121。客户端应用程序130可将授权数据编码,以供使用对应于全科医生的读出装置109的密码密钥121的全科医生接收,同时将授权数据编码,以供使用对于脊椎按摩师的读出装置109的不同密码密钥121的脊椎按摩师接收。为此,使用单个机器可读标识符133,提供了对机器可读标识符133的底层数据的访问控制。其后,程序行至终止。

[0106] 在一些实施例中,可定义与第一数据部分相关联的第一访问等级152a。例如,用户可将所需的低访问等级152与他的个人信息相关联,同时将所需的高访问等级152与他的病例相关联。与高访问等级152相关联的读出装置109既可访问病例也可访问个人信息,而与低访问等级152相关联的读出装置109仅可访问个人信息。在一个示例中,根据运动员或父母的授权,儿童的教练可将低访问等级152授权给一客户端装置106,该客户端装置106用于访问运动员的紧急联系信息。

[0107] 换句话说,访问等级152可被用于确定读出装置109可访问数据的哪一部分。用户还可通过客户端应用程序130定义哪个实体(诸如医疗机构)有权访问与各个访问等级152相关联的数据。为此,与第一数据部分相关联的第一访问等级152a和与第二数据部分相关联的第二访问等级152b可被标识,其中将至少部分地基于第一访问等级152a使用第一密码密钥121a来解密第一数据部分,并且将至少部分地基于第二访问等级152b使用第二密码密钥121b来解密第二数据部分。可以理解的是,第一访问等级152a可以与第二访问等级152b不同。

[0108] 接续参考图12,其示出了一个流程图,该流程图提供了根据各个实施例的客户端应用程序130的一部分的操作的另一个示例。可以理解的是,图12的流程图仅提供了可被用于执行如本文所述客户端应用程序130的部分的操作的多个不同类型功能布局中的一个示例。可替代地,图12的流程图可被视为描述根据一个或多个实施例的在客户端装置106中执行的方法的元素的示例。

[0109] 从步骤1203开始,客户端应用程序130可标识与客户端装置106通信的照相机或其它成像装置捕捉的图像中的机器可读标识符133。例如,机器可读标识符133可以是读出装置109生成的一个机器可读标识符133,以提供更新的、补充的或其它操作数据,该数据最初由客户端应用程序130的用户使用摄取过程完成后生成的初始机器可读标识符133来提供。可以理解的是,可从客户端装置106上生成的初始机器可读标识符133获得被读出装置109

修改的数据。可通过客户端装置106获得机器可读标识符133的图像,以更新其本地存储的数据。可从如图2所示的读出装置显示器127、从另一客户端装置106的显示器或从如图9所示的文档900中捕捉图像。

[0110] 接下来,在步骤1206中,机器可读标识符133被解码,以标识大量的加密数据。在步骤1209中,客户端应用程序130可使用与来自原始装置的装置配置文件148相关联的密码密钥121来解密所述大量的加密数据,从该原始装置获得机器可读标识符133。在一些实施例中,从机器可读标识符133读出的大量数据可为公开的(非加密的),其标识从中获得机器可读标识符133的读出装置109,其中任何装置可解码所述大量的数据。所述大量数据可包括装置标识符145和/或标识被授权访问加密数据的人或客户端装置106的唯一标识符。如果客户端装置106被这样授权,则客户端应用程序130可将装置标识符145传达到计算环境103,以获得密码密钥121。

[0111] 在步骤1212中,从机器可读标识符133获得的解密数据可被用于更新或补充本地存储在客户端装置106上的数据。在一些情形中,解密的数据可能与用户提供的数据冲突。例如,用户通过第一机器可读标识符133向读出装置109提供的部分数据可能已经被改变了。可替代地,可利用医生读取的、之前用户未知的读数来扩增用户提供的数据。

[0112] 因此,在步骤1215中,例如通过摄取过程,客户端应用程序130确定解密数据与用户提供的数据之间是否存在冲突。例如,如果用户使用他或她的客户端装置106提供的数据在任何方面均不同于读出装置106返回的数据,则数据可能冲突。例如,使用读出装置109,医生或护士可更新用户提供的数据,以反映最近的读数或测量。可替代地,使用读出装置109,医生或护士可扩增用户提供的数据。在任一情况中,当两组数据不同时,数据之间的冲突被标识。DIFF功能或类似的功能可被采用,以标识数据中存在冲突的具体部分。

[0113] 如果数据之间的冲突存在,则程序行进至步骤1218,以协调或以其它方式解决数据冲突。在一些实施例中,关于冲突的信息可被呈现给用户,其中用户可选择保留用户提供的原始数据还是用读出装置109提供的数据更新数据。在其它实施例中,读出装置109提供的数据可自动地替换用户提供的数据,或被自动地添加到客户端装置106的存储器中以扩增用户在摄取过程中提供的数据。

[0114] 在一些示例中,数据的一些部分可与不同的访问等级152相关联,不同的访问等级与特定类型的数据相关。例如,如果医疗提供者更新存储在客户端装置106上的医疗数据,因为医疗提供者可被用户(或默认)分配高的访问等级152,所以相对于用户会更顺从医疗提供者。在另一示例中,如果医疗提供者为客户端装置106的用户更新了个人信息(诸如电话号码或地址),则因为用户可能更加熟悉他或她自己的电话号码和地址,所以更顺从用户。换句话说,医疗提供者可对于医疗信息具有高的访问等级152,而对个人信息具有低的访问等级152。

[0115] 可替代地,如果数据冲突不存在,则程序进行至步骤1221,其中在将来的摄取过程中,可用从机器可读标识符133获得的数据自动地填充用户界面131中的字段。其后,程序行至终止。

[0116] 参考图13,其示出了根据各个实施例的密钥管理应用程序118的一部分的操作的示例的流程图。可以理解的是,如本文所述,图13的流程图仅提供了可被用于执行密钥管理应用程序118的部分的操作的多个不同类型功能布局中的一个示例。可替代地,图13的流程

图可被视为描述根据一个或多个实施例的在计算环境103中执行的方法的元素的示例。

[0117] 从步骤1303开始,从客户端装置106接收一个实体(诸如医疗提供者)的选择,其中在客户端应用程序130中做出该选择。例如,用户可指定他或她希望分享摄取过程中提供的输入数据的实体。在一个示例中,用户可在客户端应用程序130生成的用户界面131中选择“Atlanta Health”提供者。“Atlanta Health”可拥有或操作一个或多个读出装置109,该读出装置109与存储在数据存储115中的一个或多个装置配置文件148相关联。

[0118] 在一些示例中,实体或与该实体操作的读出装置109对应的装置配置文件148可具有存储在数据存储115中预定义密码密钥121。然而,在步骤1306中,可为装置配置文件148生成密码密钥121,例如,以创建对于用户-实体关系而言唯一的密码密钥121。可以理解的是,步骤1306是可选的。在一些示例中,使用用户提供的信息或其组合,伪随机地生成密码密钥121。

[0119] 接下来,在步骤1309中,密码密钥121被发送到客户端装置106,从而使客户端应用程序130能够为了与装置配置文件148相关联的读出装置109的接收而编码输入数据。如果读出装置109不具有存储于其上的密码密钥121,则在步骤1312中,密码密钥121可被发送到读出装置109(如果需要的话)。

[0120] 参考图14,其示出了一个流程图,该流程图示出了根据各个实施例的一个密钥管理应用程序118的操作的另一个示例。可以理解的是,如本文所述,图14的流程图仅提供了可被用于执行密钥管理应用程序118的部分的操作的多个不同类型功能布局中的一个示例。可替代地,图14的流程图可被视为描述根据一个或多个实施例的在计算环境103中执行的方法的元素的示例。

[0121] 在一些实施例中,机器可读标识符133可包括非加密数据或可使用全局或分享密码密钥121进行解密的数据。数据可包括用于原始装置的第一装置标识符145a以及用于预期接收方的第二装置标识符145b。例如,客户端应用程序130可生成机器可读标识符133,该机器可读标识符133包括用于生成了机器可读标识符133a的客户端装置106的第一装置标识符145a和用于与特定实体(诸如选定的医疗提供者)相关联的预期接收方的读出装置109的第二装置标识符145b。

[0122] 当读出装置109扫描机器可读标识符133时,其可通过分析第一装置标识符145a或预期接收方的第二装置标识符145b,而确定其是否能够访问底层数据。在其它示例中,读出装置109可为了远程授权,将装置标识符145传达到密钥管理应用程序118。为此,在步骤1403中,密钥管理应用程序118可接收生成了机器可读标识符133的装置的第一装置标识符145a。类似地,在步骤1406中,密钥管理应用程序118可接收预期访问机器可读标识符133的底层数据的装置的第二装置标识符145b。

[0123] 使用第一装置标识符145a和第二装置标识符145b,密钥管理应用程序118可在步骤1409中确定初始用户(例如,客户端应用程序130的用户或医疗提供者)是否授权请求密码密钥121来解密机器可读标识符133的底层数据的装置访问底层数据。如果请求装置被授权访问底层数据,则在步骤1412中,密钥管理应用程序118可向该装置发送密码密钥121,其中密码密钥121能够解密被编码在机器可读标识符133中的数据。其后,程序行至终止。返回参考步骤1409,如果请求装置未被授权访问机器可读标识符133的底层数据,则程序行至终止。

[0124] 本文描述的应用程序,诸如客户端应用程序130、读出应用程序136和密钥管理应用程序118,提供了有效获得、存储和复制重要信息(诸如在初次访问或随后访问健康护理提供者时所需的信息)的能力。特别地,本公开描述了一种客户端应用程序130,其用于以容易使用的方式获得病历并生成机器可读标识符133,该机器可读标识符133包括作为编码和加密数据的所得病历。在各个实施例中,用户通过客户端应用程序130提供的信息可被本地存储在客户端装置106上。存储在客户端装置106上的信息可被加密以供本地存储。此外,在复诊时,对健康史的任何改变都可被容易地标识并被提供给提供者。

[0125] 如今,现有的健康相关应用程序集中在帮助个体提高他们对于他们自己的护理负责的能力、促进健康生活、以及链接到针对提供者或机构的电子病历记录系统以获得检测和实验室结果。这些应用程序包括不同程度的每天、或最好是每周数据点,这些数据点需要被更新,以证明客户端应用程序130的用处。

[0126] 可在iOS®、Blackberry®、 Linux®、Android®、Windows®和/或其它合适的操作系统上执行客户端应用程序130和读出应用程序136。客户端应用程序130获得的信息只需要被用户提供一次,且只更新重大的和相关的改变(例如药物改变、手术程序),这对大部分患者而言仅很少时候是必要的。此外,客户端应用程序130允许用户为被抚养人或该用户对其负有责任的人提供重要信息。可以理解的是,容易地且正确地提供的基本信息的值是巨大的。

[0127] 根据各个实施例,获得了基本医疗信息的专注的、易维护的、专有的账户,健康护理提供者和其他实体需要该账户提供必要的常规护理。该信息通过医生记在心里而由医生生成,但为了系统的易于浏览而被创建。以仅具有基本文字水平的所有个体均可完成浏览的方式来创建工作流程。在各个实施例中,用户所需的信息幅度可围绕对所有的对任意健康护理提供者的最初访问是重要的预定数量(例如,7个问题或其它数量)的问题。在各个实施例中,这些问题可以是特定的并且不是无限多的。

[0128] 客户端应用程序130生成一系列的一个或多个用户界面131,以从用户获得信息。此外,客户端应用程序130将信息关联于对于医生和患者都容易且可阅的形式。这还允许基本医疗信息在各种提供者(诸如普通医生和专家)之间的高效传递。客户端应用程序130便于用于亲属或其它个体(诸如父母、子女、宠物等)的病历或其它信息的关联。例如,在患者由于疼痛、压力、困惑、意识丧失等不能够提供他们自己的病历的情况中、以及父母因紧急情况而心烦意乱的时候,另一个人提供的信息可能是有利的。在这些情况中,该重要信息可被快速、容易且准确地有效传达,由此防止因缺乏准确和完整信息而导致的医疗错误。此外,客户端应用程序130被配置为为了具有沟通障碍的个体(诸如听觉受损的人或哑人)改进健康护理。

[0129] 在各个实施例中,医生办公室或其它健康护理提供者可在客户端摄取过程中指定信息作为必须的或可选的。客户端应用程序130被执行为收集被指定为健康护理提供者需要的数据点。该信息可根据HIPAA和用于经济与临床卫生法案的健康信息技术(“HITECH”)的规定而被加密,且可被用户或特定健康护理提供者使用密钥或密码访问。

[0130] 根据各个实施例,收集的信息可被限制为:过往病历、过往手术史、过敏、药物、家族史、社会史以及免疫,尽管在其它实施例中,可收集额外的信息。客户端应用程序130可辅助用户提供基本医疗术语和药物的正确拼写,以防止可能导致医疗错误的混淆和错误文

档。

[0131] 客户端应用程序130收集的信息可被组织在概要屏幕中,其在用户界面131示出,在填写新的患者信息包时以供参考。在各种实施例中,该信息可被转换成Microsoft Word®或PDF格式,以在访问健康护理提供者之前打印。最后,该信息可被加密,加密的信息可被转换成矩阵码或其它机器可读标识符133,以无纸化和无线地直接向健康护理提供者传递信息。在各个实施例中,机器可读标识符133的扫描使底层信息自动填充到各种电子医疗记录系统的数据库中。

[0132] 除了收集个人信息,客户端应用程序130可被配置为为被抚养者、家庭成员、宠物等获得健康信息。当被扶养人和家庭成员由于年龄、丧失能力等原因不能够自己提供该信息时,这可有助于向健康护理专业人士提供完整、准确的信息。这可帮助健康护理提供者准确地评估患者、合理化护理、避免因不完整病历导致的医疗失误。如上所述,因为宠物的病历对所有者和兽医也是有价值的,所以客户端应用程序130可被配置为获得关于它们的信息。通过能够简单地参考在与客户端应用程序130的用户相同平台中的该信息,该信息可被用于学校、大学、国际旅行、紧急事件或其它情况中。

[0133] 尽管该公开提供了医疗保健数据情况下的多个示例,但本文所附实施例可被应用在许多行业。例如,健康信息可包括关于汽车的信息。修理工可通过扫描呈现在客户端装置106(可包括个人的智能手机或汽车的计算装置)上的机器可读标识符133查阅服务记录。

[0134] 参考图15,其示出了根据本公开实施例的计算环境103的示意性方框图。计算环境103包括一个或多个计算装置1500。每个计算装置1500包括至少一个处理器电路,例如,具有处理器1503和存储器1506,它们都被耦接到本地接口1509。为此,每个计算装置1500可包括例如至少一个服务器计算机或类似装置。可以理解的是,本地接口1509可包括例如具有附带地址/控制总线的数据总线或其它总线结构。

[0135] 处理器1503可执行的数据和若干部件均存储在存储器1506中。特别地,密钥管理应用程序118、翻译服务120、直接消息传递服务122和其它计算环境应用程序存储在存储器1506中并且可被处理器1503执行。是数据存储115和其它数据也可以存储在存储器1506中。此外,操作系统1512可被存储在存储器1506中并可被处理器1503执行。可以理解的是,还可以有其它应用程序存储在存储器1506中且可被处理器1503执行。

[0136] 参考图16,其示出了根据本公开的实施例的客户端装置106的示意性方框图。每个客户端装置106包括至少一个处理器电路,例如,具有处理器1603和存储器1606,它们都被耦接到本地接口1609。为此,每个客户端装置106可包括例如智能手机、平板电脑、个人计算机或其它类似装置。可以理解的是,本地接口1609可包括例如具有附带地址/控制总线的数据总线或其它总线结构。

[0137] 处理器1603可执行的数据和若干部件均存储在存储器1606中。特别地,客户端应用程序130和其他应用程序存储在存储器1606中且可被处理器1603执行。客户端数据存储1612(此处也被称为本地数据存储)和其它数据也可以存储在存储器1606中。此外,客户端操作系统1615可被存储在存储器1606中并可被处理器1603执行。可以理解的是,还可以有其它应用程序存储在存储器1606中且可被处理器1603执行。

[0138] 参考图17,其示出了根据本公开实施例的读出装置109的示意性方框图。每个读出装置109包括至少一个处理器电路,例如,具有处理器1703和存储器1706,它们都被耦接到

本地接口1709。为此,每个读出装置109可包括例如智能手机、平板电脑、个人计算机或其它类似装置。可以理解的是,本地接口1709可包括例如具有附带地址/控制总线的数据总线或其它总线结构。

[0139] 处理器1703可执行的数据和若干部件均存储在存储器1706中。特别地,读出应用程序136和其它应用程序存储在存储器1706中且可被处理器1703执行。读出装置数据存储1712和其它数据也可以存储在存储器1706中。此外,客户端操作系统1715可被存储在存储器1706中并可被处理器1703执行。可以理解的是,还可以有其它应用程序存储在存储器1706中且可被处理器1703执行。

[0140] 当此处描述的任意部件以软件的形式被执行时,可采用多种编程语言中的任一种,诸如C、C++、C#、Objective C、Java®、JavaScript®、Perl、PHP、Visual Basic®、Python®、Ruby、Flash®、Swift®或者其它编程语言。

[0141] 多个软件部件被存储在处理器可执行的存储器中。在这方面,术语"可执行的"指程序文件是以可最终被处理器运行的形式。可执行程序的示例可为,例如,以下编译程序,该编译程序可被转化成以能够被加载到存储器的随机存取部分的形式、且被处理器运行的机器代码;可被以合适的形式表达的源代码(诸如能够被加载到存储器的随机存取部分且被处理器执行的目标代码);以下源代码,该源代码可被另一可执行程序解释,以在存储器的随机存取部分中生成将被处理器执行的指令,等等。可执行的程序可被存储在存储器的任何部分或部件中,存储器例如包括随机存取存储器(RAM)、只读存储器(ROM)、硬盘驱动器、固态驱动器、USB闪存驱动器、存储卡、诸如光盘(CD)或数字通用盘(DVD)的光盘、软盘、磁带或其它存储部件。

[0142] 此处存储器被限定为包括易失和非易失存储器和数据存储部件。当断电时,易失部件不保留数据值。当断电时,非易失部件会保留数据值。因此,存储器可包括例如随机存取存储器(RAM)、只读存储器(ROM)、硬盘驱动器、固态驱动器、USB闪存驱动器、通过存储卡读卡器访问的存储卡、通过相关联的软盘驱动器访问的软盘、通过光盘驱动器访问的光盘、通过适当的磁带驱动器访问的磁带和/或其它存储部件、或这些存储部件中的任意两种或更多种的组合。此外,RAM可包括例如静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)或磁随机存取存储器(MRAM)以及其它这种装置。ROM可包括例如可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)或其它类似存储装置。

[0143] 另外,处理器可表示多个处理器和/或多个处理器内核,存储器可表示多个在平行处理电路中分别操作的多个存储器。在这种情况下,本地接口可为便于多个处理器中任意两个之间、任意处理器与任意存储器之间、或者任意两个存储器之间等通信的合适网络。本地接口可包括被设计为协调通信(例如,执行负载平衡)的额外系统。处理器可以为电的或一些其它可利用的结构。

[0144] 尽管客户端应用程序130、读出应用程序136、密钥管理应用程序118和此处描述的其它各个系统可被具体化为上文所述的可被通用硬件执行的软件或代码,但是可替代地,上述还可被具体化为专用硬件或软件/通用硬件和专用硬件的组合。如果具体化为专用硬件,则每个可被被实施为采用多种技术中任意一种或组合的电路或状态机器。这些技术可

包括但不限于,当应用一个或多个数据信号时,具有用于执行各种逻辑功能的逻辑门的离散逻辑电路、具有合适的逻辑门的专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它部件等。这种技术通常被本领域技术人员所熟知,因此此处不再赘述。

[0145] 图6和图10-图14的流程图示出了客户端应用程序130、读出应用程序136和密钥管理应用程序118的部分的执行的功能和操作。如果具体化为软件,则每个方块可代表包括执行特定逻辑功能的程序指令的模块、片段或一部分代码。程序指令可具体化为源代码的形式,该源代码包括由程序语言或机器代码写成的人可读语句,其中程序语言或机器代码包括可由合适的执行系统(诸如计算机系统或其它系统中的处理器)识别的数字指令。机器代码可从源代码等转化而来。如果具体化为硬件,则每个方块可代表执行特定逻辑功能的电路或多个互联电路。

[0146] 尽管图6和图10-图14的流程图示出了特定执行顺序,但是可以理解的是执行顺序可与所示的不同。例如,两个或更多个方块的执行顺序可相对于所示的顺序被打乱。另外,图6和图10-图14中连续示出的两个或更多方块可同时被执行或部分同时地被执行。此外,在一些实施例中,图6和图10-图14中所示的一个或更多方块可被跳过或省略。此外,任意数量的计数器、状态变量、警告信号或消息可被添加到本文所述的逻辑流程中,用以提高效用、解释、性能测量或提高故障排除帮助等。可以理解的是,所有这种变化都落入本公开的范围。

[0147] 此外,本文所描述的任何逻辑或应用包括客户端应用程序130、读出应用程序136以及密钥管理应用程序118,其含有可体现在任何非暂时性计算机可读介质中以被指令执行系统使用或与指令执行系统(诸如例如计算机系统或其它系统中的处理器)相关的软件或代码。从这个意义上来说,逻辑可包括例如含有指令和声明的语句,其中该指令和声明可从计算机可读介质中取得并可被指令执行系统执行。在本公开的上下文中,“计算机可读介质”可以是可含有、存储或保持本文所述的逻辑或应用程序的、用于或关联于指令执行系统的任何介质。

[0148] 计算机可读介质可包括多个物理介质中的任意一个,诸如例如磁、光或半导体介质。合适的计算机可读介质的更多具体示例可包括但不限于磁带、磁软盘、磁硬盘驱动器、存储卡、固态驱动器、USB闪存驱动器或光盘。计算机可读介质还可为随机存取存储器(RAM),其包括例如静态随机存取存储器(SRAM)和动态随机存取存储器(DRAM)或磁随机存取存储器(MRAM)。此外,计算机可读介质可为只读存储器(ROM)、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、电可擦除可编程只读存储器(EEPROM)或其它类似存储装置。

[0149] 进一步地,可以多种方式来执行和结构化本文所述的任何逻辑或应用程序、客户端应用程序130、读出应用程序136以及密钥管理应用程序118。例如,所描述的一个或多个应用程序可被执行为单个应用程序的模块或部件。进一步地,可在共享的或分离的计算装置中或其组合中执行本文所描述的一个或多个应用程序。例如,此处所描述的多个应用程序可在同样的计算装置1500中或在同样计算环境103中的多个计算装置中执行。此外,可理解的是,诸如“应用程序”、“服务”、“系统”、“引擎”、“模块”等的术语是可互换的,且并非旨在限制。

[0150] 析取语言,诸如短语“X、Y或Z中的至少一个”,除非另外指定,否则根据上下文应被

理解为像通常所使用的表示一项、一个术语等,可为X、Y或Z中的任何一个或它们的任意组合(例如X、Y和/或Z)。因此,这种析取语言通常并不旨在、也不应该意指特定实施例需要X中的至少一个、Y中的至少一个或者Z中的至少一个中的每个都出现。

[0151] 应强调的是,本公开的上述实施例仅仅是为了清楚的理解本公开的原理所描述的执行的可能示例。在基本不背离本公开的精神和原理的情形下,可对上述实施例做出各种变形和修改。

[0152] 条款1.一种系统,包括:客户端装置,包括至少一个硬件处理器;可在所述客户端装置中执行的客户端应用程序,包括以下程序指令,该程序指令在被执行时使得所述客户端装置:通过网络接收与第一装置配置文件相关联的第一密码密钥以及与第二装置配置文件相关联的第二密码密钥;从所述客户端装置的数据存储中访问输入数据,通过由所述客户端应用程序生成的至少一个用户界面提供所述输入数据;将所述输入数据格式化成第一数据部分和第二数据部分;使用所述第一密码密钥加密所述第一数据部分,以及使用所述第二密码密钥加密所述第二数据部分;以及,使用加密的所述第一数据部分和加密的所述第二数据部分生成机器可读标识符,以呈现在所述客户端装置可访问的显示器中。

[0153] 条款2.条款1的系统,其中所述机器可读标识符为第一机器可读标识符,并且所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置:标识由与客户端装置通信的照相机捕捉的图像中的第二机器可读标识符,所述第二机器可读标识符由不同于所述客户端装置的装置生成;根据所述第二机器可读标识符标识大量的加密数据;用所述第一密码密钥或所述第二密码密钥解密大量的加密数据以标识解密的数据;以及将所述解密的数据存储在所述数据存储中,供所述客户端应用程序访问。

[0154] 条款3.条款2的系统,其中将所述解密的数据存储在所述数据存储中还包括:识别存储在所述数据存储中的所述输入数据与所述解密的数据之间是否存在冲突;以及存储所述解密的数据替代存储在所述数据存储中的所述输入数据。

[0155] 条款4.条款1的系统,还包括:与所述第一装置配置文件相关联的其上存储有第一密码密钥的第一读出装置;与所述第二装置配置文件相关联的其上存储有第二密码密钥的第二读出装;以及其中所述第一读出装置被配置为使用所述第一密码密钥根据所述机器可读标识符访问所述第一数据部分,第二读出装置被配置为使用所述第二密码密钥根据所述机器可读标识符访问所述第二数据部分。

[0156] 条款5.条款4的系统,其中所述第一读出装置包括第一成像装置,所述第二读出装置包括第二成像装置,由所述第一成像装置或所述第二成像装置捕捉所述机器可读标识符。

[0157] 条款6.条款1的系统,其中所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置向与所述客户端装置不同的另一客户端装置发送机器可读标识符。

[0158] 条款7.条款1的系统,其中根据所述输入数据使用大量解密的数据生成所述机器可读标识符。

[0159] 条款8.条款1的系统,其中响应于所述客户端装置上做出的所述第一装置配置文件的选择,由所述客户端装置从至少一个远程计算装置通过所述网络接收与所述第一装置配置文件相关联的所述第一密码密钥;以及,其中响应于所述客户端装置上做出的所述第

二装置配置文件的选择,由所述客户端装置从至少一个远程计算装置通过所述网络接收与所述第二装置配置文件相关联的所述第二密码密钥。

[0160] 条款9.条款1的系统,其中使用所述第一密码密钥加密所述第一数据部分以及使用所述第二密码密钥加密所述第二数据部分还包括:标识与所述第一数据部分相关联的第一访问等级;标识与所述第二数据部分相关联的第二访问等级;使用所述第一密码密钥至少部分地基于所述第一访问等级加密所述第一数据部分;以及使用所述第二密码密钥至少部分地基于所述第二访问等级加密所述第二数据部分,其中所述第一访问等级与所述第二访问等级不同。

[0161] 条款10.条款1的系统,其中所述机器可读标识符为快速响应(QR)码或二维码。

[0162] 条款11.一种计算机执行方法,包括:由包括至少一个硬件处理器的客户端装置通过网络接收与第一装置配置文件相关联的第一密码密钥以及与第二装置配置文件相关联的第二密码密钥;由所述客户端装置从所述客户端装置的数据存储中访问输入数据,所述输入数据由至少一个用户界面提供,所述用户界面由可在所述客户端装置上执行的客户端应用程序生成;通过所述客户端装置将所述输入数据格式化成至少第一数据部分和第二数据部分;由所述客户端装置使用所述第一密码密钥加密所述第一数据部分,以及使用所述第二密码密钥加密所述第二数据部分;以及,由所述客户端装置使用加密的所述第一数据部分和加密的所述第二数据部分生成机器可读标识符,以呈现在所述客户端装置可访问的显示器中。

[0163] 条款12.条款11的计算机执行方法,其中所述机器可读标识符为第一机器可读标识符,所述方法还包括:通过所述客户端装置标识由与所述客户端装置通信的照相机捕捉的图像中的第二机器可读标识符,所述第二机器可读标识符由不同于所述客户端装置的装置生成;通过所述客户端装置从所述第二机器可读标识符标识大量的加密数据;使用所述第一密码密钥或所述第二密码密钥,通过所述客户端装置解密所述大量的加密数据,以标识解密的数据;以及,通过所述客户端装置将所述解密的数据存储在所述数据存储中,供客户端应用程序访问。

[0164] 条款13.条款12的计算机执行方法,其中将所述解密的数据存储在所述数据存储中还包括:通过所述客户端装置识别存储在所述数据存储中的所述输入数据与所述解密的数据之间是否存在冲突;以及通过所述客户端装置存储所述解密的数据替代存储在所述数据存储中的所述输入数据。

[0165] 条款14.条款11的计算机执行方法,还包括:通过第一读出装置使用所述第一密码密钥从所述机器可读标识符访问所述第一数据部分,所述第一读出装置与所述第一装置配置文件相关联且具有存储于其上的第一密码密钥;以及通过第二读出装置使用所述第二密码密钥从所述机器可读标识符访问所述第二数据部分,所述第二读出装置与所述第二装置配置文件相关联且具有存储于其上的第二密码密钥。

[0166] 条款15.条款14的计算机执行方法,其中所述第一读出装置包括第一成像装置,所述第二读出装置包括第二成像装置,由所述第一成像装置或所述第二成像装置捕捉所述机器可读标识符。

[0167] 条款16.条款11的计算机执行方法,还包括由所述客户端装置通过所述网络向与所述客户端装置不同的另一客户端装置发送所述机器可读标识符。

[0168] 条款17.条款11的计算机执行方法,其中根据所述输入数据使用大量解密的数据生成所述机器可读标识符。

[0169] 条款18.条款11的计算机执行方法,其中响应于所述客户端装置上做出的所述第一装置配置文件的选择,由所述客户端装置从至少一个远程计算装置通过所述网络接收与所述第一装置配置文件相关联的所述第一密码密钥;以及,其中响应于所述客户端装置上做出的所述第二装置配置文件的选择,由所述客户端装置从至少一个远程计算装置通过所述网络接收与所述第二装置配置文件相关联的所述第二密码密钥。

[0170] 条款19.条款11的计算机执行方法,其中使用所述第一密码密钥加密所述第一数据部分以及使用所述第二密码密钥加密所述第二数据部分还包括:通过所述客户端装置标识与所述第一数据部分相关联的第一访问等级;通过所述客户端装置标识与所述第二数据部分相关联的第二访问等级;通过所述客户端装置,使用所述第一密码密钥至少部分地基于所述第一访问等级加密所述第一数据部分;以及,通过所述客户端装置,使用所述第二密码密钥至少部分地基于所述第二访问等级加密所述第二数据部分,其中所述第一访问等级与所述第二访问等级不同。

[0171] 条款20.条款11的计算机执行方法,其中所述机器可读标识符为快速响应(QR)码或二维码。

[0172] 条款21.一种系统,包括:客户端装置,包括至少一个硬件处理器;可在所述客户端装置中执行的客户端应用程序,包括以下程序指令,该程序指令在被执行时使得所述客户端装置:使用由至少一个密码密钥加密的第一数量数据生成第一机器可读标识符,以呈现在所述客户端装置的显示器中,其中,具有存储于其上的所述至少一个密码密钥的读出装置被配置为解密所述数据;在由所述客户端装置捕捉的至少一幅图像中标识第二机器可读标识符;解码所述第二机器可读标识符,以标识由读出装置使用所述至少一个密码密钥加密的第二数量数据;使用所述至少一个密码密钥解密所述第二数量数据;以及识别所述第一数量数据与所述第二数量数据之间是否存在冲突。

[0173] 条款22.条款21的系统,其中所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置响应于所述第一数量数据与所述第二数量数据之间存在的冲突而执行任务从而解决该冲突。

[0174] 条款23.条款21的系统,其中响应于所述读出装置改变所述第一数量数据以产生所述第二数量数据的而标识所述冲突。

[0175] 条款24.条款22的系统,其中所述任务还包括:在所述客户端应用程序的用户界面中显示与所述冲突相关联的信息;在所述用户界面中接收所述第一数量数据或所述第二数量数据中的选择;以及响应于所述选择,用所选择的所述第一数量数据或所选择的所述第二数量数据更新所述客户端装置的数据存储。

[0176] 条款25.条款22的系统,其中所述任务包括用所述第二数量数据更新所述客户端装置的数据存储。

[0177] 条款26.条款21的系统,其中所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置用所述第二数量数据中的至少一部分填充所述客户端应用程序中的用户界面的至少一个字段。

[0178] 条款27.条款21的系统,其中由至少一个密码密钥加密的所述第一数量数据还包

括摄取过程中获得的第一用户输入部分和第二用户输入部分,由可被所述读出装置访问的第一密码密钥加密所述第一用户输入部分,由所述读出装置不可访问的第二密码密钥加密所述第二用户输入部分。

[0179] 条款28.条款21的系统,其中所述机器可读标识符为快速响应(QR)码或二维码。

[0180] 条款29.条款21的系统,其中所述客户端应用程序还包括以下程序指令,该程序指令在被执行时使得所述客户端装置通过网络从远程计算环境中执行的远程应用程序接收至少一个密码密钥。

[0181] 条款30.条款29的系统,其中在所述远程计算环境中执行的所述远程应用程序被配置为通过网络向所述读出装置发送至少一个密码密钥。

[0182] 条款31.一种计算机执行方法,包括:通过包括至少一个硬件处理器的客户端装置,使用由至少一个密码密钥加密的第一数量数据生成第一机器可读标识符,以呈现在所述客户端装置的显示器中,其中,具有其上存储有所述至少一个加密密钥的读出装置被配置为解密所述数据;通过所述客户端装置,在由所述客户端装置捕捉的至少一幅图像中标识第二机器可读标识符;通过所述客户端装置,解码所述第二机器可读标识符,以标识由读出装置使用所述至少一个密码密钥加密的第二数量数据;通过所述客户端装置,使用所述至少一个密码密钥解密所述第二数量数据;以及,通过所述客户端装置识别所述第一数量数据与所述第二数量数据之间是否存在冲突。

[0183] 条款32.条款31的计算机执行方法,还包括,响应于所述第一数量数据与所述第二数量数据之间存在冲突,所述客户端装置执行任务从而解决该冲突。

[0184] 条款33.条款31的计算机执行方法,其中响应于所述读出装置改变所述第一数量数据以产生所述第二数量数据,而标识所述冲突。

[0185] 条款34.条款32的计算机执行方法,其中所述任务包括:通过所述客户端装置,在所述客户端应用程序的用户界面中显示与所述冲突相关联的信息;通过所述客户端装置,标识在所述用户界面中做出的所述第一数量数据或所述第二数量数据中的选择;以及响应于所述选择被标识的,通过所述客户端装置,使用所选择的所述第一数量数据或所选择的所述第二数量数据更新所述客户端装置的数据存储。

[0186] 条款35.条款32的计算机执行方法,其中所述任务包括,通过客户端装置,使用所述第二数量数据更新所述客户端装置的数据存储。

[0187] 条款36.条款31的计算机执行方法,还包括,通过所述客户端装置,使用所述第二数量数据中的至少一部分填充客户端应用程序中的用户界面的至少一个字段。

[0188] 条款37.条款31的计算机执行方法,其中由至少一个密码密钥加密的所述第一数量数据还包括摄取过程中获得的第一用户输入部分和第二用户输入部分,由可被所述读出装置访问的第一密码密钥加密所述第一用户输入部分,由所述读出装置不可访问的第二密码密钥加密所述第二用户输入部分。

[0189] 条款38.条款31的计算机执行方法,其中所述机器可读标识符为快速响应(QR)码或二维码。

[0190] 条款39.条款31的计算机执行方法,还包括,通过所述客户端装置,通过网络从远程计算环境中执行的远程应用程序接收至少一个密码密钥。

[0191] 条款40.条款39的计算机执行方法,其中在所述远程计算环境中执行的所述远程

应用程序被配置为通过网络向所述读出装置发送至少一个密码密钥。

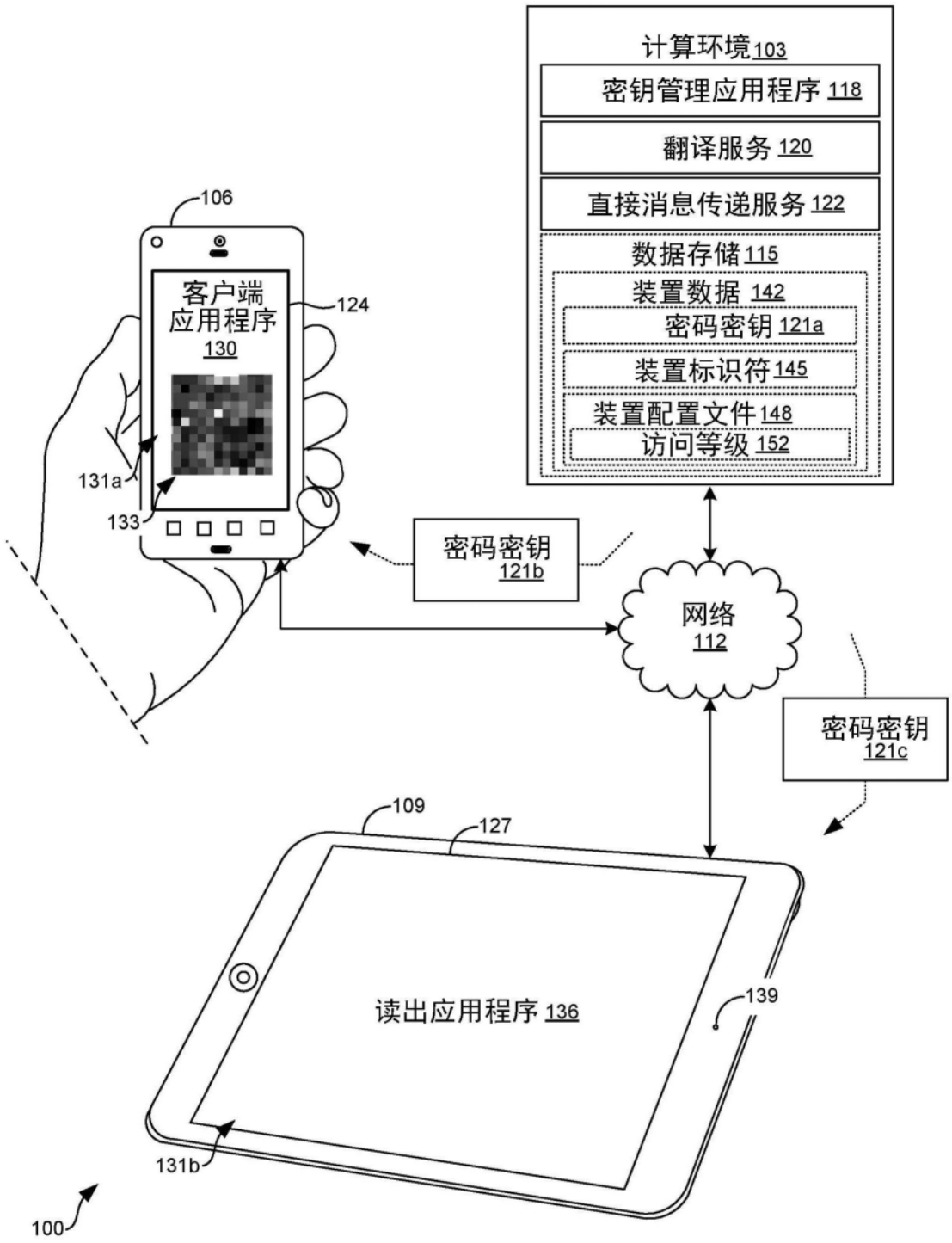

计算环境103
密钥管理应用程序 118
翻译服务 120
直接消息传递服务 122
数据存储 115
装置数据 142
密码密钥 121a
装置标识符 145
装置配置文件 148
访问等级 152
106
客户端
应用程序
130
124
131a
133
密码密钥
121b
网络
112
密码密钥
121c
109
127
读出应用程序 136
139
131b
100

图1

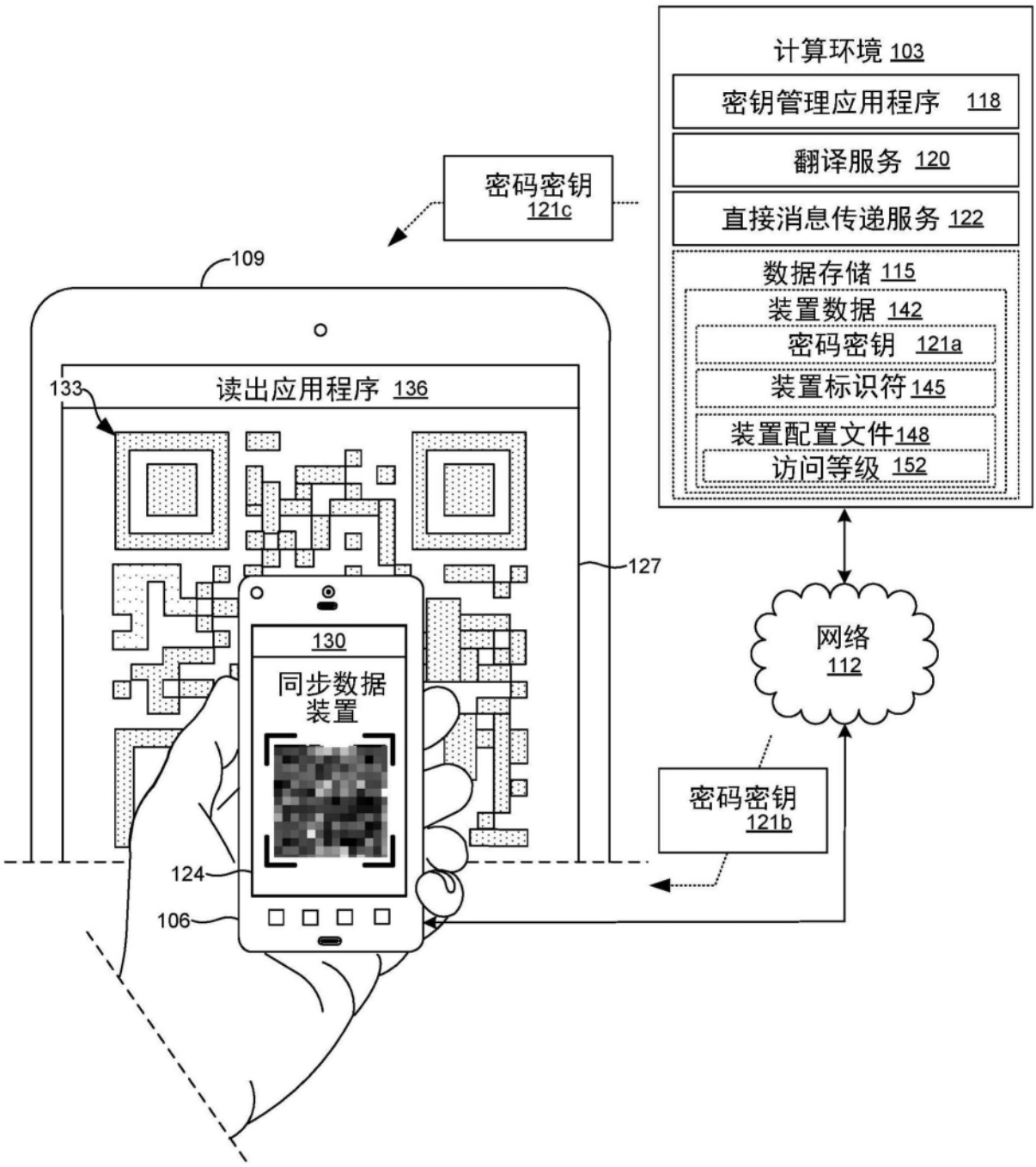

计算环境 103
密钥管理应用程序 118
翻译服务 120
直接消息传递服务 122
数据存储 115
装置数据 142
密码密钥 121a
装置标识符 145
装置配置文件 148
访问等级 152
密码密钥 121c
109
读出应用程序 136
133
127
130
同步数据装置
网络 112
密码密钥 121b
124
106

图2

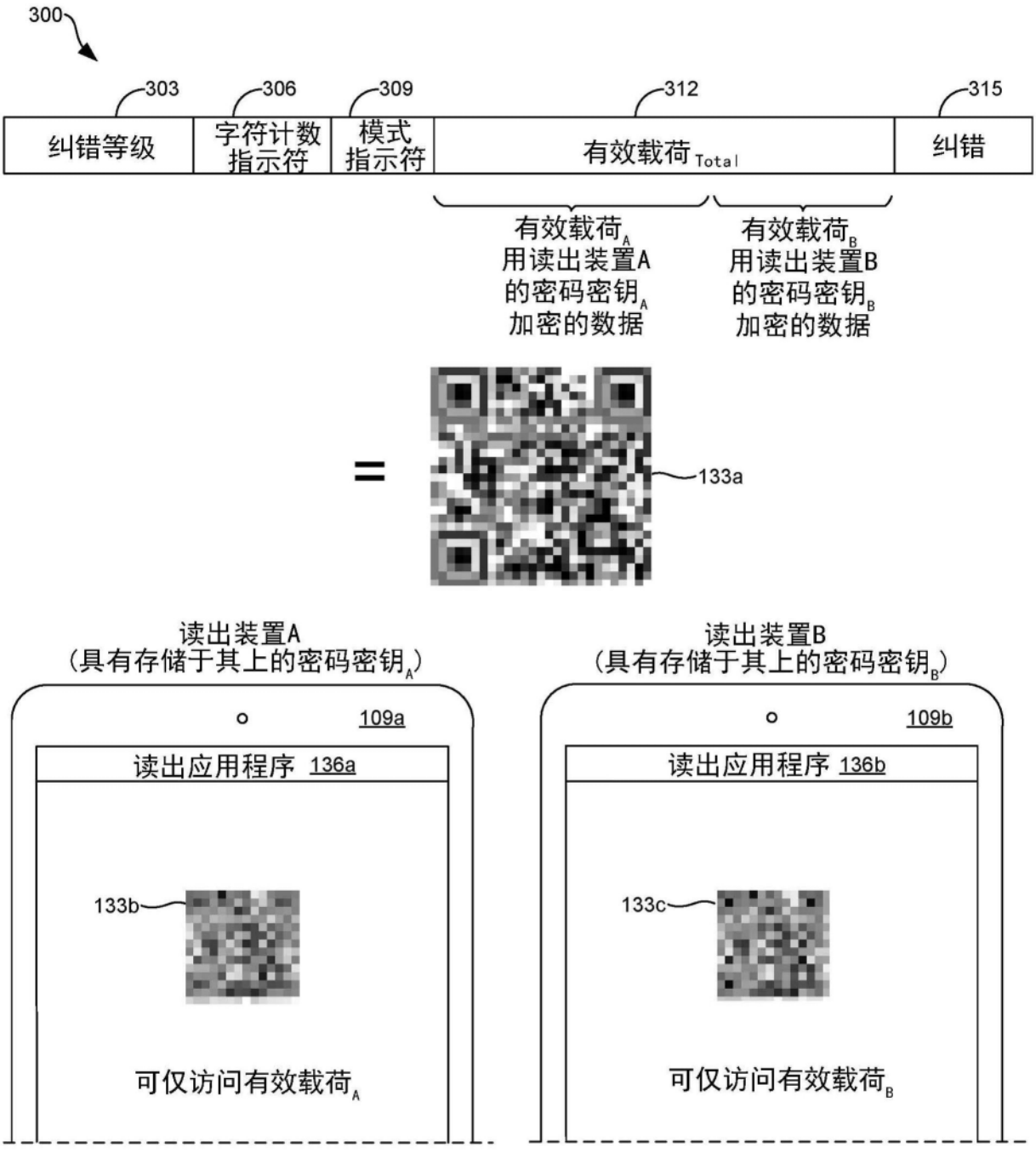

300
303
306
309
312
315
纠错等级
字符计数指示符
模式指示符
有效载荷 Total
纠错
有效载荷A 用读出装置A的密码密钥A加密的数据
有效载荷B 用读出装置B的密码密钥B加密的数据
=
133a
读出装置A（具有存储于其上的密码密钥A）
读出装置B（具有存储于其上的密码密钥B）
109a
109b
读出应用程序 136a
读出应用程序 136b
133b
133c
可仅访问有效载荷A
可仅访问有效载荷B

图3

40-L版本的矩阵码的容量

| 编码模式 | 模式指示符 |
|---|---|
| 数字 | 7089 字符 |
| 字母数字 | 4296 字符 |
| 字节 | 2953 字符 |
| 日本汉字 | 1817 字符 |

图4

| 模式名称 | 模式指示符 |
|---|---|
| 数字 | 0001 |
| 字母数字 | 0010 |
| 字节 | 0100 |
| 日本汉字 | 1000 |
| ECI | 0111 |

图5

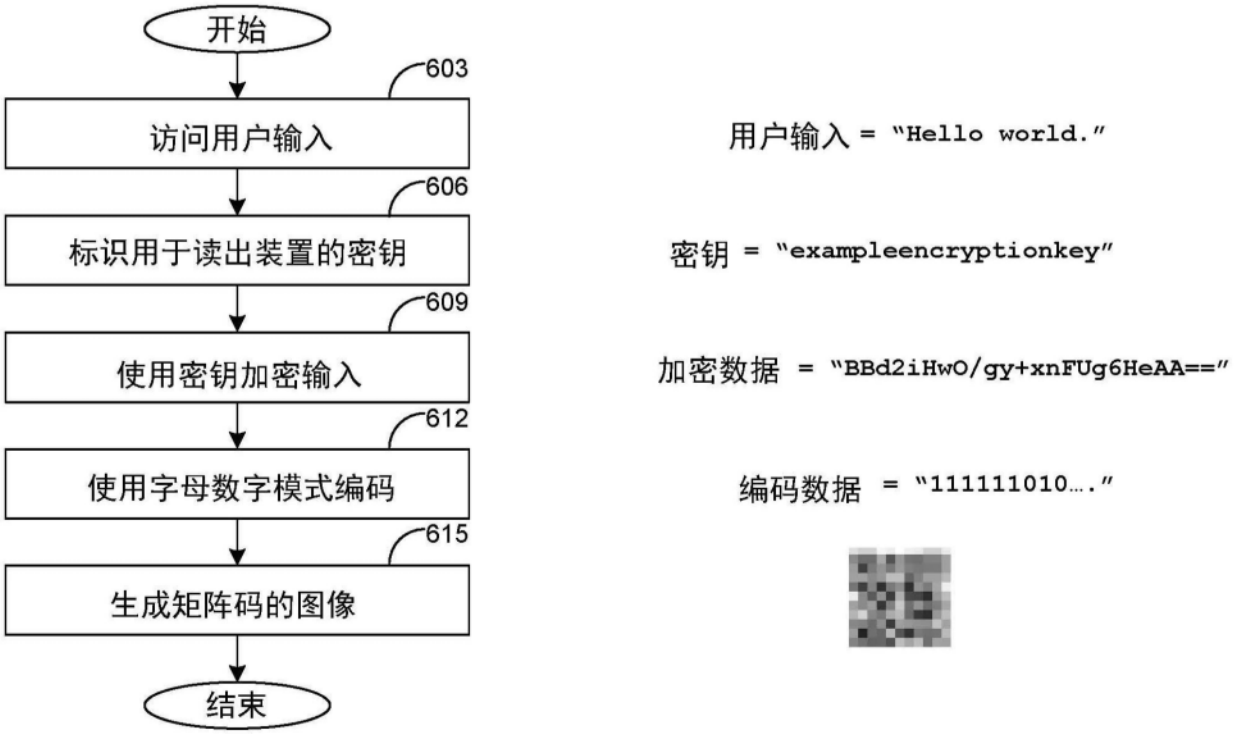



图6

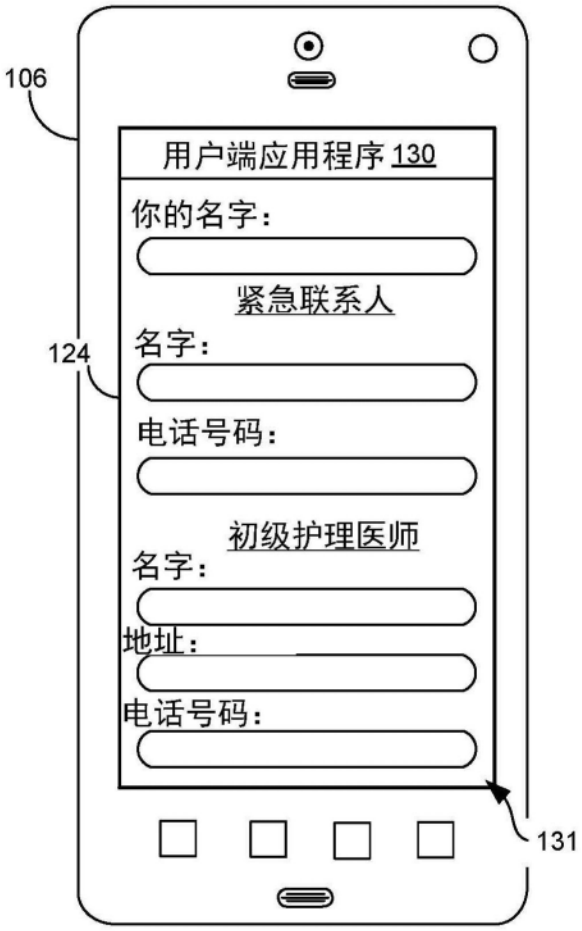



图7A


图7B

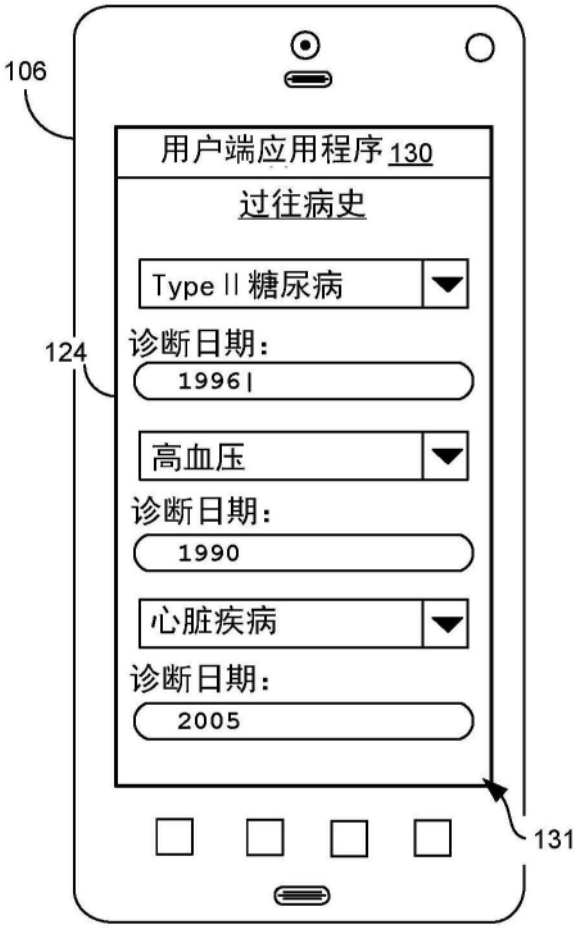

106
用户端应用程序130
过往病史
Type II 糖尿病
124
诊断日期:
1996
高血压
诊断日期:
1990
心脏疾病
诊断日期:
2005
131

图7C

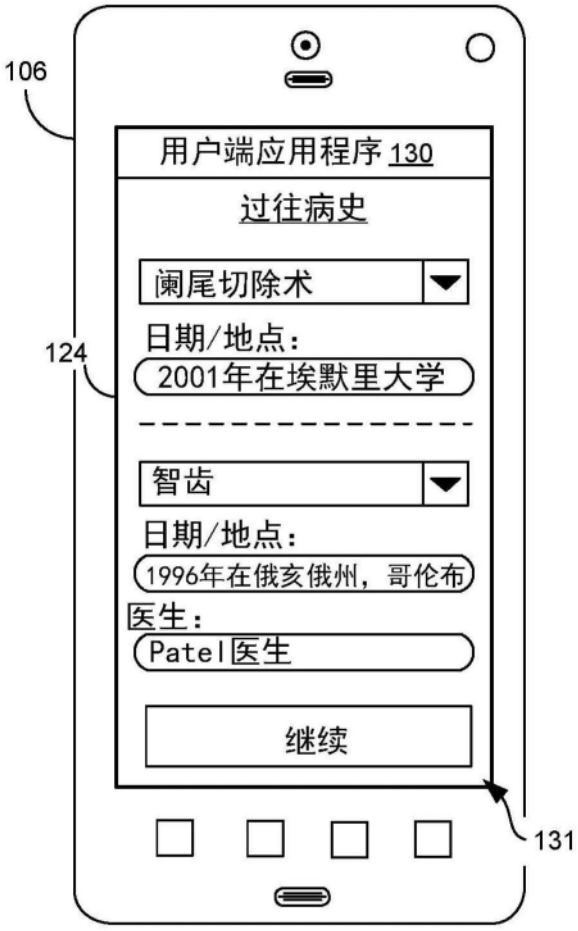

106
用户端应用程序 130
过往病史
阑尾切除术
日期/地点：
124
2001年在埃默里大学
智齿
日期/地点：
1996年在俄亥俄州，哥伦布
医生：
Patel医生
继续
131

图7D

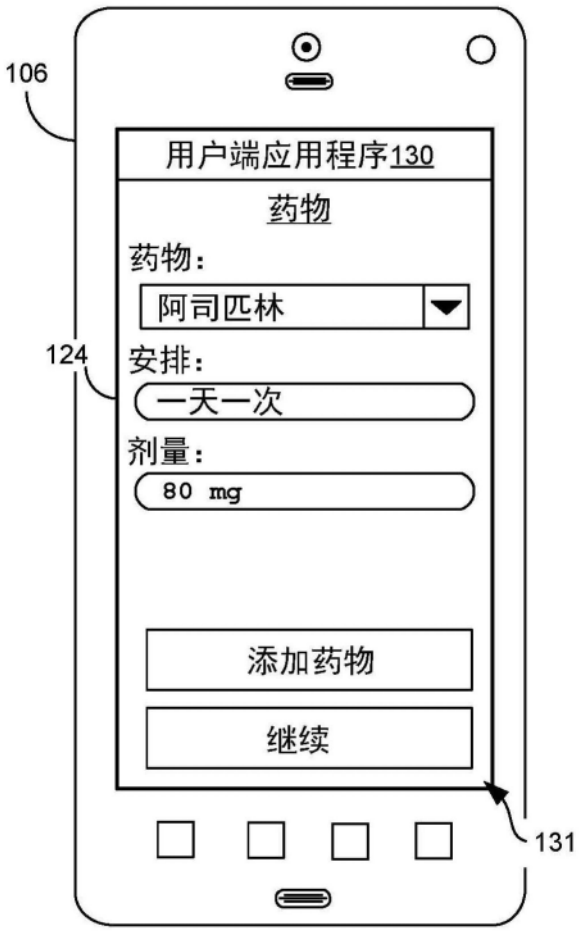



图7E

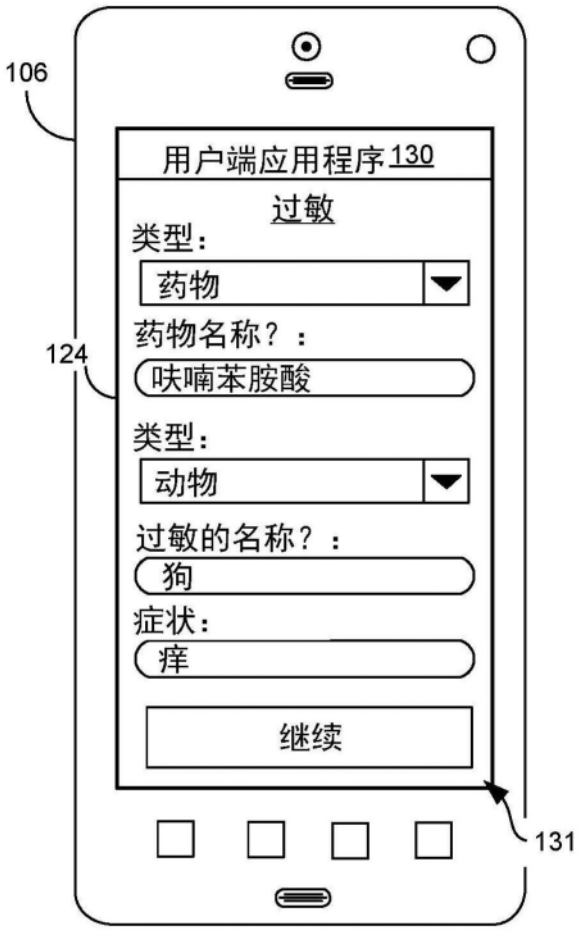



图7F

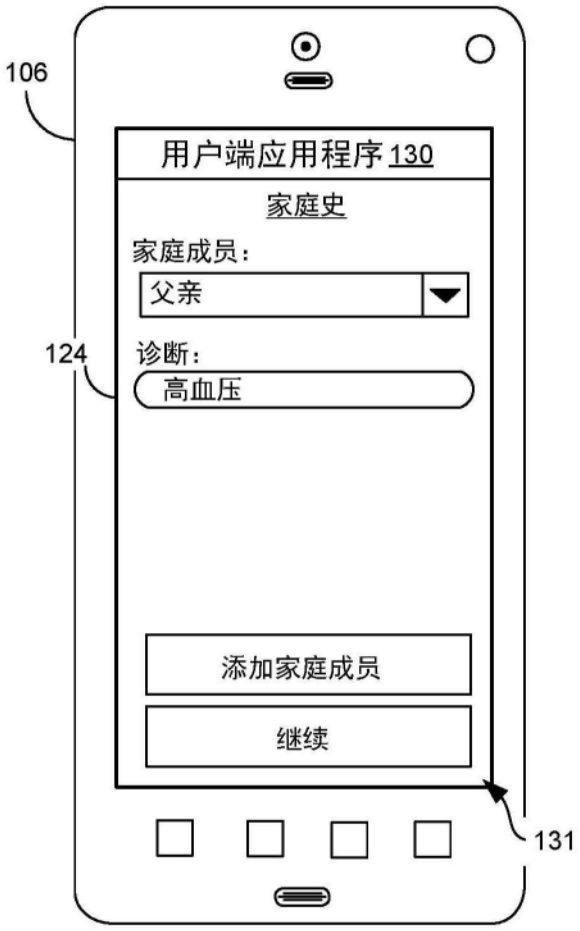



图7G

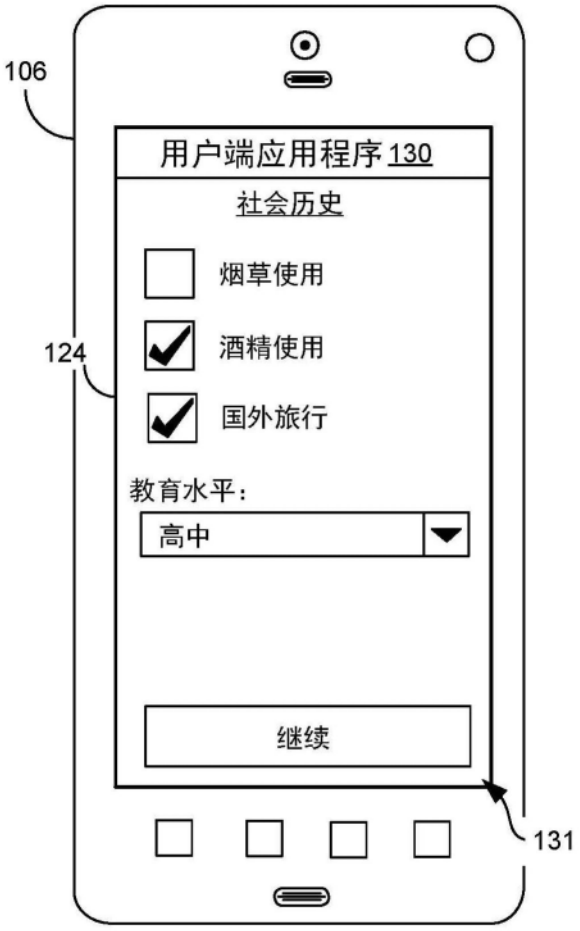



图7H

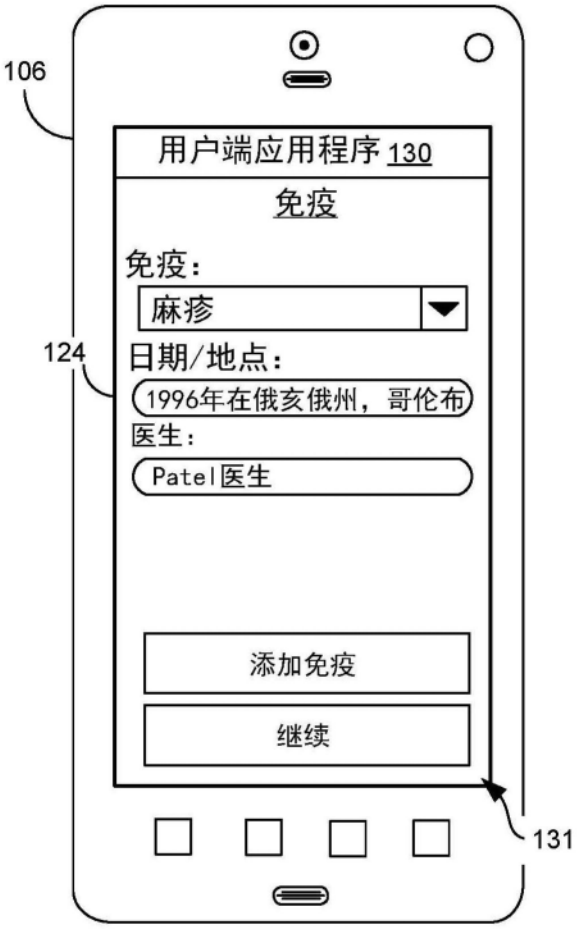

106
用户端应用程序 130
免疫
免疫：
麻疹
124
日期/地点：
1996年在俄亥俄州，哥伦布
医生：
Patel医生
添加免疫
继续
131

图7I

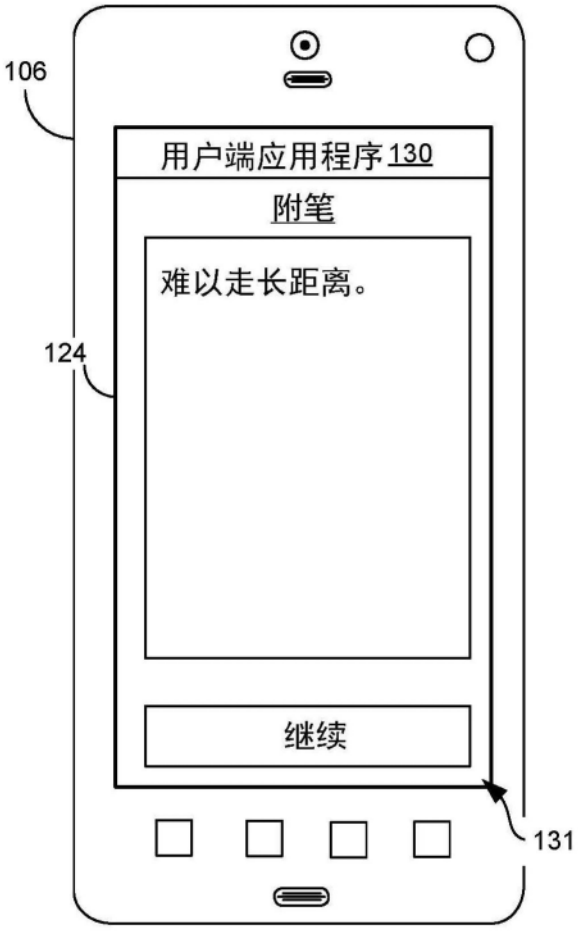



图7J

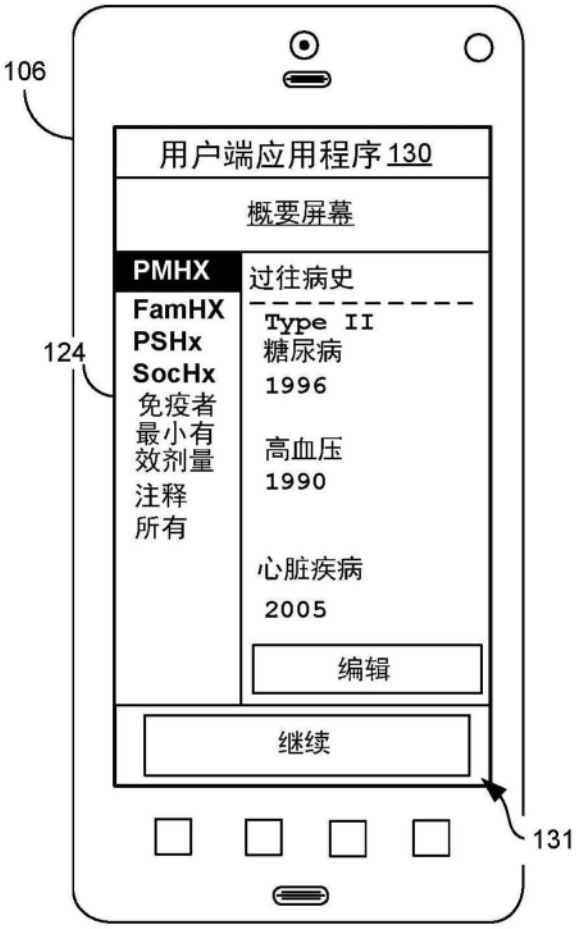

106
用户端应用程序130
概要屏幕
PMHX
FamHX
PSHx
SocHx
免疫者
最小有效剂量
注释
所有
124
过往病史
Type II
糖尿病
1996
高血压
1990
心脏疾病
2005
编辑
继续
131

图7K

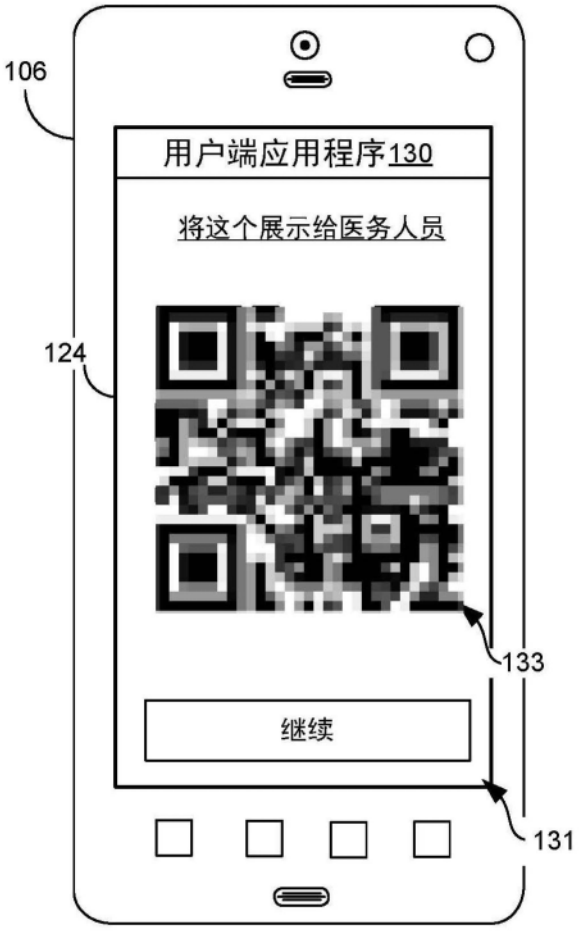



图7L

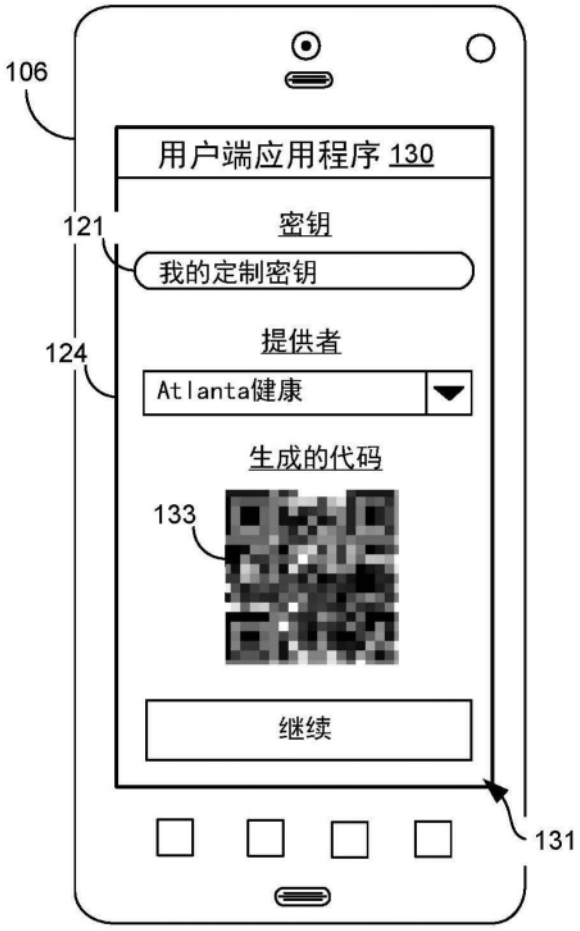

106
用户端应用程序 130
121
密钥
我的定制密钥
124
提供者
Atlanta健康
生成的代码
133
继续
131

图7M

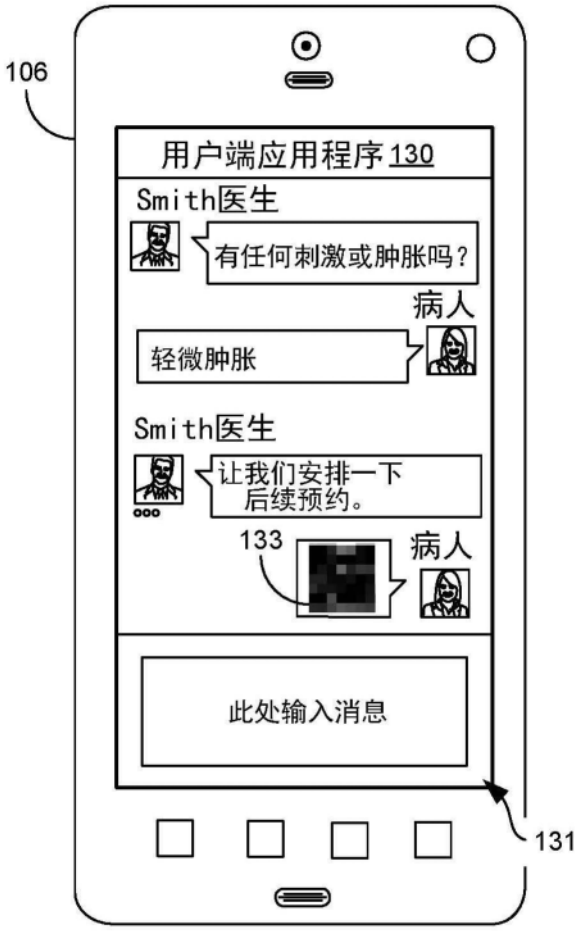



图7N

```
01    func generateMatrixCode() {
02          payloadData = getInputData();          // Get User Input from UI
03          key = getKey(receiverDevice);          // Get Key for Receiver Device
04          modeIndicator = "0010";                // Alphanumeric Mode
05          charCount = sizeOf(payloadData);       // Get Char Size of Payload Data
06          encryptedData = encrypt(payloadData, key); // Encrypt Payload Data
07          error = calculateError(encryptedData);     // Reed Solomon Error Code
08          a = formatData(modeIndicator, charCount,
09                         encryptedData, error);      // Format Data
10          return generateMatrixImage(a);             // Matrix Code Image
11    }
```

800

图8

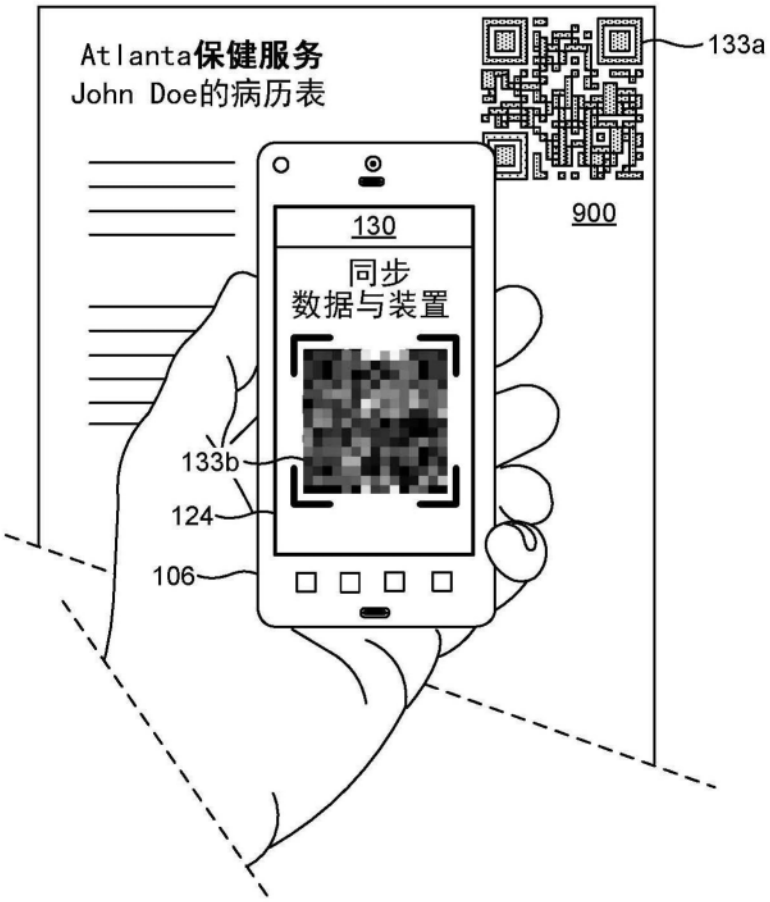



图9

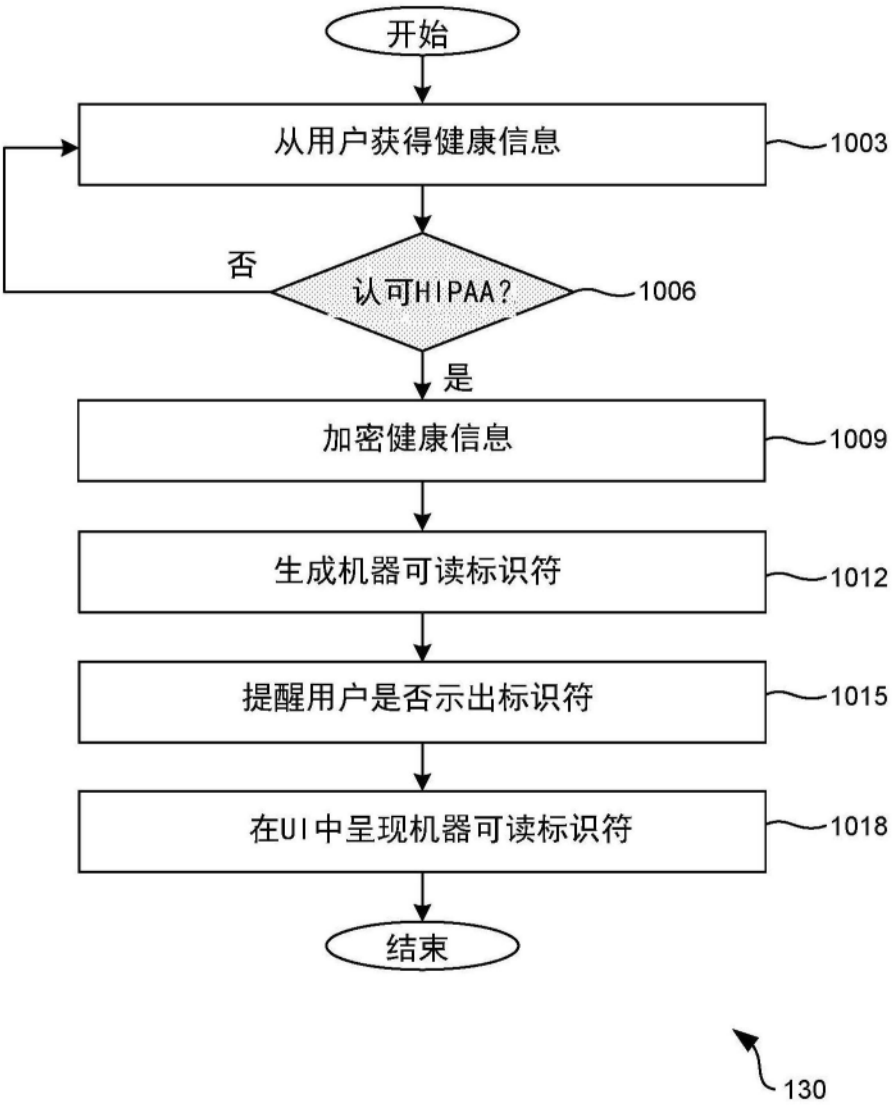

开始
从用户获得健康信息
1003
否
认可HIPAA?
1006
是
加密健康信息
1009
生成机器可读标识符
1012
提醒用户是否示出标识符
1015
在UI中呈现机器可读标识符
1018
结束
130

图10


开始
接收与第一装置配置文件相关联的第一密码密钥
1103
接收与第二装置配置文件相关联的的第二密码密钥
1106
访问来自数据存储的输入数据
1109
将输入数据格式化成第一部分和第二部分
1112
用第一密码密钥加密第一部分
1115
用第二密码密钥加密第二部分
1118
用加密的数据生成机器可读标识符
1121
结束
130

图11

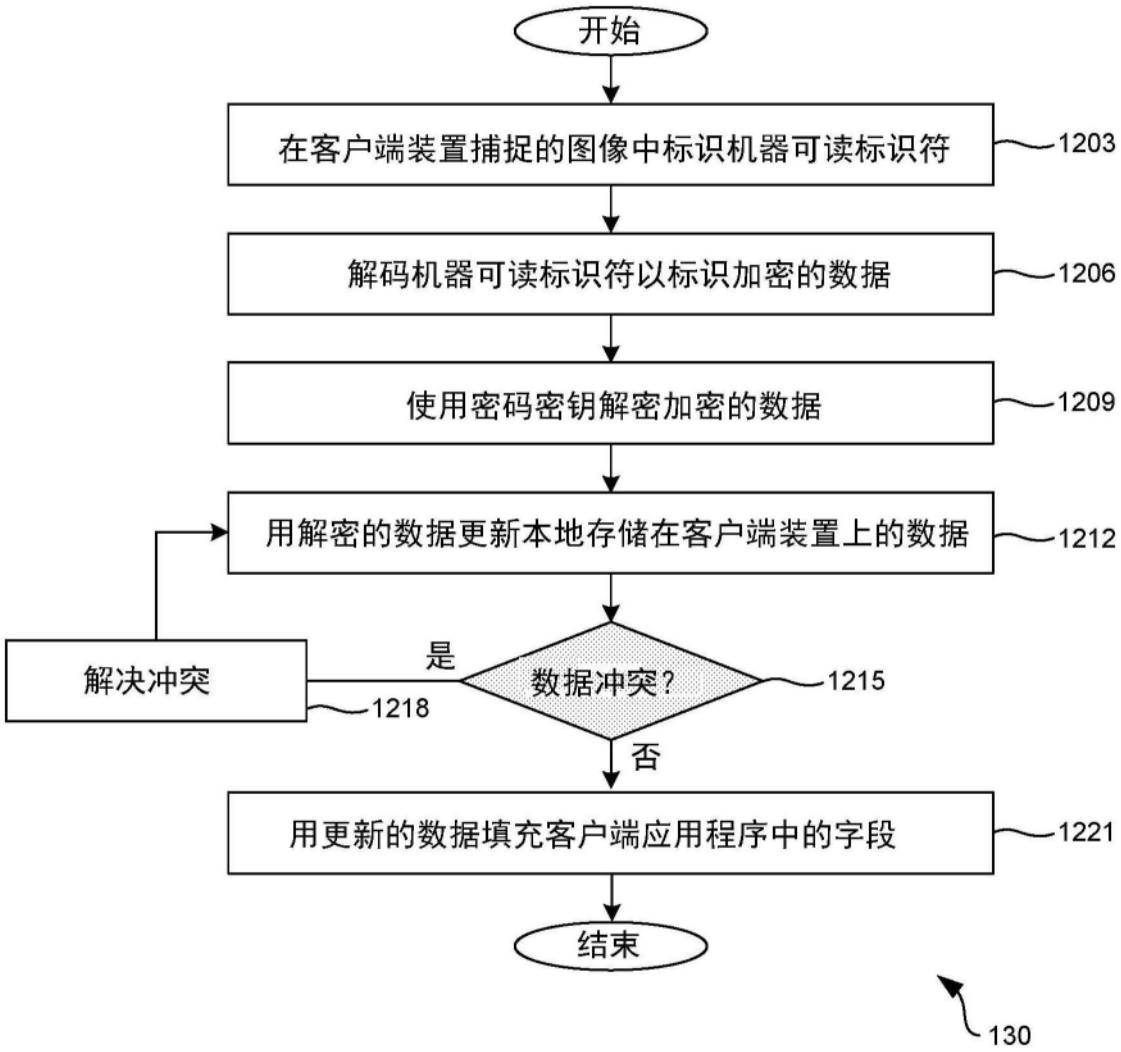

开始
在客户端装置捕捉的图像中标识机器可读标识符
1203
解码机器可读标识符以标识加密的数据
1206
使用密码密钥解密加密的数据
1209
用解密的数据更新本地存储在客户端装置上的数据
1212
数据冲突?
1215
是
解决冲突
1218
否
用更新的数据填充客户端应用程序中的字段
1221
结束
130

图12

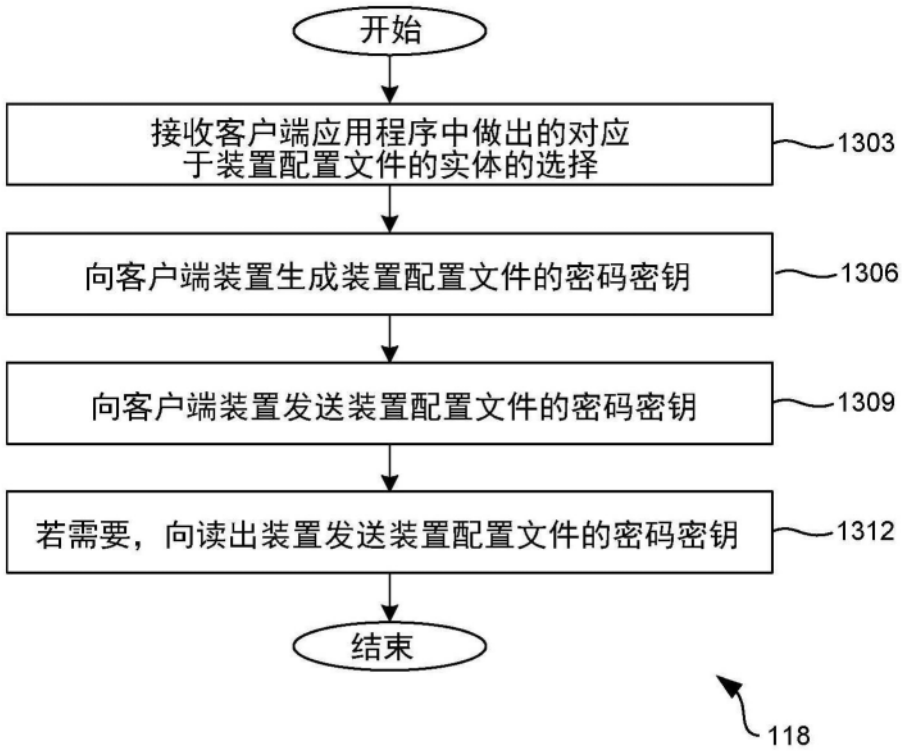

开始
接收客户端应用程序中做出的对应于装置配置文件的实体的选择
1303
向客户端装置生成装置配置文件的密码密钥
1306
向客户端装置发送装置配置文件的密码密钥
1309
若需要，向读出装置发送装置配置文件的密码密钥
1312
结束
118

图13

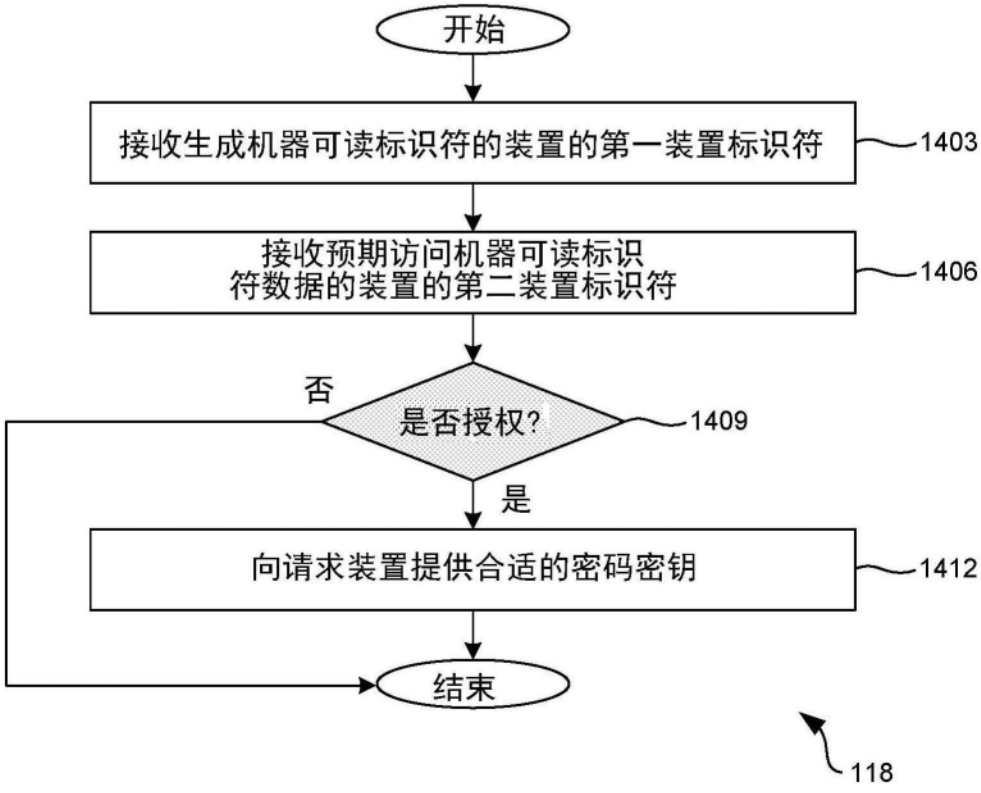

开始
接收生成机器可读标识符的装置的第一装置标识符
1403
接收预期访问机器可读标识符数据的装置的第二装置标识符
1406
否
是否授权?
1409
是
向请求装置提供合适的密码密钥
1412
结束
118

图14

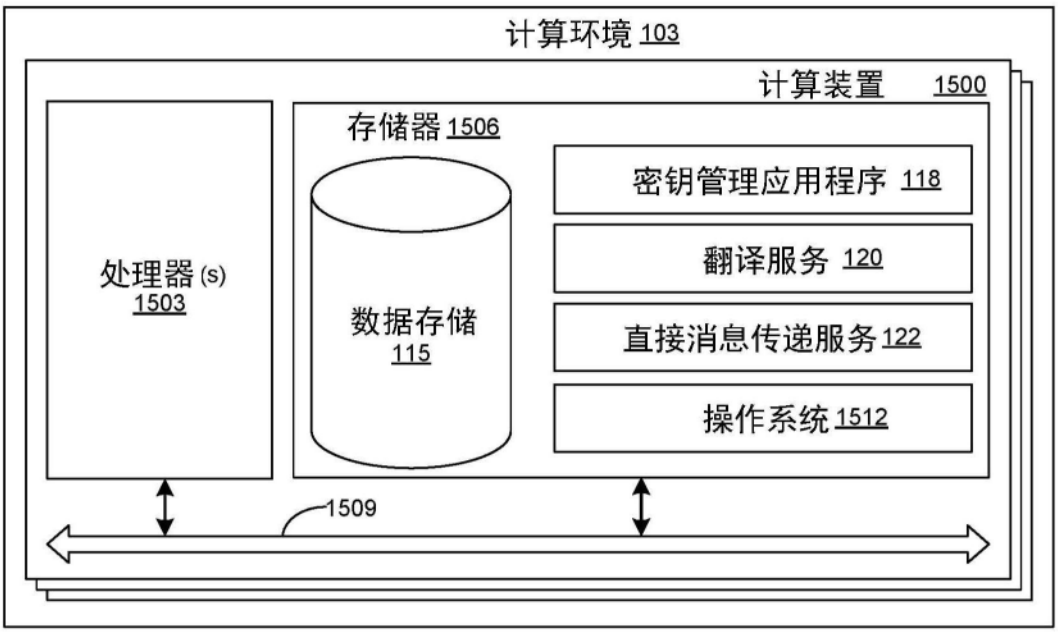

计算环境 103
计算装置 1500
存储器 1506
处理器 (s) 1503
数据存储 115
密钥管理应用程序 118
翻译服务 120
直接消息传递服务 122
操作系统 1512
1509

图15

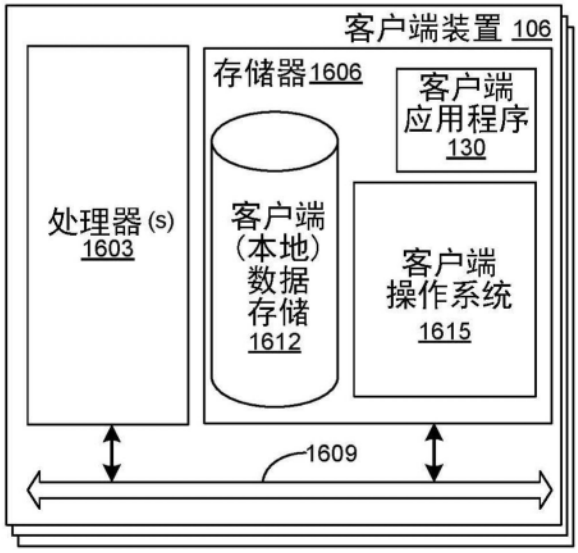

客户端装置 106
存储器 1606
客户端应用程序 130
处理器 (s) 1603
客户端 (本地) 数据存储 1612
客户端操作系统 1615
1609

图16

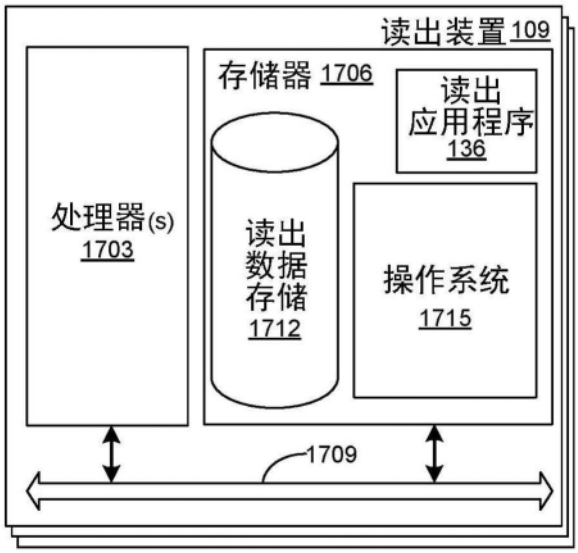

读出装置 109
存储器 1706
读出
应用程序
136
处理器(s)
1703
读出
数据
存储
1712
操作系统
1715
1709

图17