



(12) 发明专利

(10) 授权公告号 CN 110245482 B

(45) 授权公告日 2022.08.30

(21) 申请号 201910409131.8

(22) 申请日 2016.05.27

(65) 同一申请的已公布的文献号  
申请公布号 CN 110245482 A

(43) 申请公布日 2019.09.17

(30) 优先权数据  
1509031.9 2015.05.27 GB  
1509030.1 2015.05.27 GB  
1520760.8 2015.11.24 GB  
1520741.8 2015.11.24 GB

(62) 分案原申请数据  
201680039224.0 2016.05.27

(73) 专利权人 利森提亚集团有限公司  
地址 英国南格拉摩根  
专利权人 麦品帕德有限公司

(72) 发明人 贾斯汀·派克

(74) 专利代理机构 上海君立衡知识产权代理事务  
所(特殊普通合伙) 31389  
专利代理师 黄庆

(51) Int.Cl.  
G06F 21/32 (2013.01)  
G06F 21/36 (2013.01)  
G06Q 20/10 (2012.01)  
G06Q 20/20 (2012.01)  
G06Q 20/32 (2012.01)  
G06Q 20/40 (2012.01)  
G07F 7/10 (2006.01)

(56) 对比文件  
CN 104584086 A, 2015.04.29  
US 2010259561 A1, 2010.10.14  
US 2010109920 A1, 2010.05.06  
WO 2014111689 A1, 2014.07.24  
US 8176324 B1, 2012.05.08  
JP 2012138011 A, 2012.07.19 (续)

审查员 周杨

权利要求书2页 说明书11页 附图4页

(54) 发明名称  
认证方法和系统

(57) 摘要

本发明提供了一种认证方法和系统。其特别适用于在允许访问受控资源之前验证个人的身份。这可能是或不是金融资源。本发明使用与用户有关的生物特征数据来编码和解码与用户相关联的标识符。因此用户的生物特征数据成为编码标识符和随后解码标识符的密钥。在一个实施方式中,生物特征数据被用于生成小键盘配置。小键盘配置指定多个小键盘按键的顺序和/或位置。然后使用该配置生成可操作的小键盘和/或小键盘的图像。因此,个人的生物特征数据可以被用来生成定制的小键盘和/或图像,然后可以使用该定制的小键盘和/或图像来对与用户相关联的标识符进行编码或解码。根据生物特征数据生成的小键盘或图像可以用于生成不同小键盘

配置之间的映射。



CN 110245482 B

[接上页]

(56) 对比文件

CN 2195777 Y, 1995.04.26

CN 104021322 A, 2014.09.03

US 2014020074 A1, 2014.01.16

CN 102867159 A, 2013.01.09

CN 104007837 A, 2014.08.27

CN 101287051 A, 2008.10.15

1. 一种使用可操作的小键盘和/或小键盘图像中的按键的乱序配置编码和/或解码标识符的认证方法,包括以下步骤:

通过使用与用户有关的生物特征数据来提供值的一个或更多个串、数组或序列来使用所述生物特征数据提供标识符的编码版本和解码版本,所述值的一个或更多个串、数组或序列各自对应于用于创建小键盘或小键盘图像的小键盘配置;以及

使用所述值的一个或更多个串、数组或序列作为子例程调用的输入,

其中,子例程包括用于生成所述可操作的小键盘和/或所述小键盘图像的指令;以及所述生物特征数据确定或用于提供所述可操作的小键盘中的按键的乱序配置和/或所述小键盘图像中描绘的按键的乱序配置。

2. 根据权利要求1所述的方法,还包括以下步骤:

在电子设备处或在电子设备上生成所述生物特征数据。

3. 根据权利要求2所述的方法,其中,所述电子设备是手持式、便携式或移动计算设备。

4. 根据权利要求1、2或3所述的方法,包括以下步骤:

使用所述生物特征数据对所述标识符进行编码,使得所述生物特征数据成为对所述标识符进行解码的密钥。

5. 根据前述权利要求1到3中任一项所述的方法,其中:

所述子例程形成小键盘生成组件的一部分,所述小键盘生成组件被布置为在由所述用户操作的电子设备上或电子设备处生成至少一个小键盘和/或小键盘图像。

6. 根据前述权利要求1到3中任一项所述的方法,还包括以下步骤:

存储所述标识符的编码版本。

7. 根据权利要求6所述的方法,其中,使用由所述生物特征数据指定的小键盘配置来生成所述编码版本;和/或

所述标识符的所述编码版本被存储在服务器上。

8. 根据前述权利要求1到3中任一项所述的方法,包括以下步骤:

生成至少一个可操作的小键盘和至少一个小键盘图像,其中:

所述可操作的小键盘中的按键的配置相对于所述小键盘图像中描绘的按键的配置是不同的。

9. 根据前述权利要求1到3中任一项所述的方法,包括以下步骤:

使用所述生物特征数据来计算编码的标识符的解码版本,

其中,所述解码步骤作为当所述用户希望获得对受控资源或服务的访问或者执行交易时发起的认证会话的一部分来执行。

10. 根据前述权利要求1到3中任一项所述的方法,还包括以下步骤:

通过将所述标识符与先前存储的版本进行比较来验证所述标识符。

11. 根据前述权利要求1到3中任一项所述的方法,还包括以下步骤:

将所述生物特征数据或从所述生物特征数据导出的数据从由所述用户操作的电子设备发送到远程计算资源。

12. 根据权利要求11所述的方法,其中:

所述生物特征数据被发送到所述远程计算资源,以使所述标识符的编码版本能够使用所述生物特征数据或从所述生物特征数据导出的数据进行解码。

13. 根据前述权利要求1到3中任一项所述的方法,其中:

在所述可操作的小键盘中的按键的乱序配置中和/或在所述小键盘图像中描绘的按键的乱序配置中的按键的顺序相对于默认或参考小键盘配置是乱序的。

14. 一种使用可操作的小键盘和/或小键盘图像中的按键的乱序配置编码和/或解码标识符的认证系统,包括:

由用户操作的电子设备;以及

远程计算资源;

其中,所述系统被布置和配置为通过以下步骤使用与用户有关的生物特征数据来提供标识符的编码版本或解码版本:

使用所述生物特征数据来提供值的一个或更多个串、数组或序列,所述值的一个或更多个串、数组或序列各自对应于用于创建小键盘或小键盘图像的小键盘配置;以及

使用所述值的一个或更多个串、数组或序列作为子例程调用的输入,

其中,子例程包括用于生成可操作的小键盘和/或所述小键盘图像的指令;使得所述生物特征数据确定或用于提供所述可操作的小键盘中的按键的乱序配置和/或所述小键盘图像中描绘的按键的乱序配置。

15. 根据权利要求14所述的系统,其中:

在所述电子设备处或在所述电子设备上生成或捕获所述生物特征数据。

16. 根据权利要求15所述的系统,其中,所述电子设备是手持式、便携式或移动计算设备。

17. 根据权利要求14、15或16所述的系统,其中,所述系统被布置成:

使用所述生物特征数据对所述标识符进行编码,使得所述生物特征数据成为对所述标识符进行解码的密钥。

18. 根据权利要求14至16中任一项所述的系统,其中,所述系统被布置和配置为执行根据权利要求1至13中任一项所述的方法。

## 认证方法和系统

[0001] 本申请是申请日为2016年05月27日,申请号为201680039224.0,发明名称为“认证方法和系统”的申请的分案申请。

[0002] 本发明总体上涉及在允许访问受控资源或服务之前对个人的认证(验证),并且更具体地涉及生物特征认证。本发明特别适合于但不限于在执行金融交易之前验证个人身份方面的使用。

[0003] 认证方法和技术是众所周知的。这样的技术包括使用与用户相关联地存储的诸如PIN或代码的标识符。在被授权访问受控资源(例如银行账户)或服务之前,用户需要提供正确的PIN。PIN的使用已经在银行业得到广泛的接受,并且客户对他们的使用熟悉并感到舒适。

[0004] 生物特征数据也已经被研究用于认证解决方案。生物特征数据涉及个人的身体或行为特征,并且因此可以用来唯一地识别该个人。生物特征数据可能涉及到虹膜、语音、指纹识别等等。

[0005] 存在用于捕获这种生物特征数据的技术。例如,智能电话已经适于包括指纹扫描仪。然而,对于例如银行业对安全有强烈需求的高度敏感的应用而言,生物特征认证的使用还未被广泛采用。其中一个原因是,目前的银行系统及其所有基础设施都面向使用基于PIN的认证。向生物特征认证转换需要投入大量的时间、精力和资金来改变或代替现有的硬件和软件平台。另一个原因是生物特征数据可能会被破解。例如,有些情况下指纹已被第三方“提取(lifted)”和复制。这造成了严重的安全风险,并且虽然可以改变破解的PIN,但个人不能改变他们的指纹、声音或虹膜图案。

[0006] 因此,希望提供一种将生物特征认证提供的使用便利性与基于PIN的认证的安全性和逻辑优势相结合的解决方案。

[0007] 这样的改进的解决方案现在已经被构思。

[0008] 因此,根据本发明,提供了如在所附权利要求中定义的认证解决方案。

[0009] 本申请提供了以下内容:

[0010] 1) 一种认证方法,包括以下步骤:

[0011] 使用与用户有关的生物特征数据来提供标识符的编码版本或解码版本。

[0012] 2) 根据1)所述的方法,以及还包括以下步骤:

[0013] 在电子设备处或在电子设备上生成所述生物特征数据,优选地,其中所述电子设备是手持式、便携式或移动计算设备。

[0014] 3) 根据1)或2)所述的方法,以及包括以下步骤:

[0015] 使用所述生物特征数据对所述标识符进行编码,使得所述生物特征数据成为对所述标识符进行解码的密钥。

[0016] 4) 根据1)至3)所述的方法,以及包括以下步骤:

[0017] 其中,所述生物特征数据包括或被处理以提供值的一个或多个串、数组或序列。

[0018] 5) 根据前述1)至4)中任一项所述的方法,其中:

[0019] i) 所述生物特征数据被用于指定可操作的小键盘和/或小键盘图像中的按键的顺

序或位置;和/或

[0020] ii) 所述生物特征数据被用作或用于指定小键盘配置。

[0021] 6) 根据前述1) 至5) 中任一项所述的方法,以及包括以下步骤:

[0022] 使用所述生物特征数据来生成至少一个可操作的小键盘和/或至少一个小键盘图像。

[0023] 7) 根据6) 所述的方法,以及包括以下步骤:

[0024] 生成在5) 中的所述可操作的小键盘或所述小键盘图像与另一可操作的小键盘和/或图像之间的映射;

[0025] 优选地,其中,所述方法还包括使用所述映射对所述标识符进行编码或解码的步骤。

[0026] 8) 根据前述1) 至7) 中任一项所述的方法,以及还包括以下步骤:

[0027] 存储所述标识符的编码版本;优选地,其中:

[0028] 使用由所述生物特征数据指定的小键盘配置来生成所述编码版本;和/或

[0029] 所述标识符的编码版本被存储在服务器上。

[0030] 9) 根据前述1) 至8) 中任一项所述的方法,以及还包括以下步骤:

[0031] 使用所述生物特征数据的至少一部分作为子例程调用的输入,其中,所述子例程包括用于生成可操作的小键盘或小键盘图像的指令。

[0032] 10) 根据前述1) 至9) 中任一项所述的方法,以及还包括以下步骤:

[0033] 通过将所述标识符与先前存储的版本进行比较来验证所述标识符。

[0034] 11) 根据前述1) 至10) 中任一项所述的方法,以及还包括以下步骤:

[0035] 将所述生物特征数据或从所述生物特征数据导出的数据从由所述用户操作的电子设备发送到远程计算资源,优选地,以使得所述标识符的编码版本能够使用所述生物特征数据或由所述生物特征数据导出的数据进行解码。

[0036] 12) 一种认证系统,包括:

[0037] 由用户操作的电子设备;和

[0038] 远程计算资源;

[0039] 其中,所述系统被布置和配置为使用与用户有关的生物特征数据来提供标识符的编码版本或解码版本。

[0040] 13) 根据12) 所述的系统,其中:

[0041] 在所述电子设备处或在所述电子设备上生成或捕获所述生物特征数据;

[0042] 优选地,其中,所述电子设备是手持式、便携式或移动计算设备。

[0043] 14) 根据12) 或13) 所述的系统,其中,所述系统被布置成:

[0044] i) 使用所述生物特征数据作为或指定小键盘配置;和/或

[0045] ii) 使用所述生物特征数据对所述标识符进行编码,使得所述生物特征数据成为对所述标识符进行解码的密钥。

[0046] 15) 根据12) 至15) 所述的系统,其中,所述系统被布置和配置为执行根据1) 至11) 中任一项所述的方法。

[0047] 16) 一种认证方法,包括以下步骤:

[0048] 捕获与用户有关的生物特征数据;

[0049] 使用所述生物特征数据作为软件实现组件的输入,所述软件实现组件被布置和配置成使用所述生物特征数据来编码与所述用户相关联的标识符,使得需要所述生物特征数据来解码所述标识符。

[0050] 本发明可以提供一种认证方法,包括以下步骤:

[0051] 使用与(电子设备的)用户有关的生物特征数据来提供标识符的编码或解码版本。

[0052] 另外地或可选地,该方法包括以下步骤:

[0053] 捕获与用户有关的生物特征数据;

[0054] 使用生物特征数据作为软件实现组件的输入,该软件实现组件被布置和配置成使用生物特征数据来编码与用户相关联的标识符,使得需要生物特征数据来解码标识符。

[0055] 用户的生物特征数据可以被用作或作为用于编码用户的标识符的密钥。另外或可选地,它可以被用作或者作为解码用户的标识符的密钥。

[0056] 标识符可以与用户相关联,和/或与用户相关联的资源相关联。该资源可以是例如诸如借记卡或信用卡之类的支付卡或支付账户。本发明不限于与标识符有关的资源的类型。资源可以是物理资源或电子、数字或虚拟资源。

[0057] 标识符可以包括任何类型、长度或格式的标识符。例如,它可以包括数字、字母、图片等或其任何组合。优选地,标识符被预先选择(即,在认证过程之前被确定)并被存储在服务器上的存储器中。服务器可以位于金融机构,由金融机构操作或者代表金融机构操作。

[0058] 生物特征数据可以是与用户的物理和/或行为属性有关的任何类型的数据。它可以包括与用户的指纹、虹膜图案、声音、书写、静脉或任何其他生物特征来源有关的数据。在该文件中,短语“生物特征数据”可以用于表示从用户直接捕获的数据(即,诸如可以由传感器捕获的“原始”生物特征数据)。另外或可替代地,它也可能意味着从生物特征捕获过程中获得的生物特征数据。例如,其可以是在生物特征认证过程之后获得或导出的处理数据。这可以是在生物特征认证过程或者涉及捕获用户的生物特征数据的注册过程期间已经生成的加密密钥。

[0059] 优选地,生物特征数据在由用户操作的电子设备处或其上生成。电子设备可被称为“本地”设备。优选地,电子设备是手持式、便携式或移动电子设备。例如,它可以是智能电话、笔记本电脑或平板电脑。它可以包括用于通过本地网络、近距离协议或广域电信网络传输数据的无线通信能力。

[0060] 优选地,电子设备包括能够捕获和生成生物特征数据的硬件和/或软件功能,或者与这样的生物特征数据捕获设备例如指纹扫描仪、相机、语音识别软件等进行物理或无线通信。例如,电子设备可以是具有内置的相机和语音识别软件或指纹扫描仪的智能电话。另外地或可选地,其可以包括允许电话连接到例如扫描仪的接口。

[0061] 生物特征数据可以包括或可以被处理以提供值的一个或多个串、数组或序列。值的一个或多个串、数组或序列可以用作小键盘配置或可以被处理以提供小键盘配置。小键盘配置可以是乱序或随机化的小键盘配置。配置中按键的顺序可以相对于默认或参考小键盘配置(例如本地设备的默认配置)是乱序的。

[0062] 因此,生物特征数据捕获设备可以产生或包括一系列值,或者可以处理生物特征设备的输出以提供一系列值。这些值可以用作分配给小键盘或小键盘图像中的按键的标签。因此,生物特征数据可被用作或指定小键盘配置。此后,一系列值可以简单地称为数组。

该数组可以是生物特征数据的一部分或子串。本发明不限于生物特征数据或从生物特征数据生成的数组的数据类型、长度或格式。

[0063] 生物特征数据可被提供给小键盘生成组件(KGC)。KGC可以是本地设备上提供的或与本地设备通信的组件。它可能是软件应用程序。小键盘生成组件可以被布置成生成Pin键入设备(PED)。

[0064] 生物特征数据可以用作到在由用户操作的手持式设备上或者在诸如服务器的远程计算资源上提供的软件组件的输入。软件组件可以被布置成使用生物特征数据来对标识符进行编码,或者将其用作被布置为生成小键盘配置和/或PED的算法的种子。软件组件可以被布置成执行加密和/或随机化处理。

[0065] 另外地或可选地,可以使用一些其他形式的数据作为小键盘配置算法的输入。这个数据可以从用户的生物特征数据中导出或以某种方式与用户的生物特征数据相关。例如,它可以是加密密钥。加密密钥可以被用来生成种子。密钥可以是与用户和/或与用户相关联的数字钱包相关联的私有加密密钥或公共加密密钥。钱包可以存储在电子设备上。加密密钥可能在生物特征认证过程期间或涉及捕获用户的生物特征数据的注册过程期间已经被生成。

[0066] 优选地,虽然可以使用被更改的或随机化的小键盘配置来执行编码和/或解码过程,但是可以使用取决于生物特征数据的任何合适的编码/解码方法。

[0067] 在一个或多个实施方式中,该方法还可以包括使用生物特征数据来生成至少一个可操作的小键盘和/或至少一个小键盘图像的步骤。可以使用生物特征数据或其一部分来确定至少一个可操作的小键盘和/或至少一个小键盘图像的布局。因此,生物特征数据可以作为或用作提供用于可操作的小键盘和/或图像的小键盘配置。小键盘/图像生成步骤可以由KGC执行,该KGC可以被布置和配置为接收生物特征数据并且对其进行处理以提供一个或多个可操作的小键盘和/或一个或多个小键盘图像。

[0068] 优选地,可操作的小键盘中的按键的布置或配置相对于小键盘图像中描绘的按键的布置或配置是不同的。可操作的小键盘是包括多个按键的功能小键盘,在创建小键盘时,每个按键具有与其相关联的值或符号,使得当选择按键时,其相关联的值被放置到存储器中。小键盘可以是电子生成的对象。它可以提供机械小键盘的模型或表示。小键盘对象可以使用子例程(过程、功能或方法)调用来生成。子例程可以使用参数来确定小键盘中按键的布置(顺序,位置)。在执行该过程或方法时,小键盘对象可以驻留在易失性存储器中,直到其被丢弃。可操作的小键盘可以是或者包括事件处理程序(或者在一些替代编程术语中是“事件监听程序”)。事件可以是小键盘事件、触摸屏事件或其他与输入有关的事件。

[0069] 相比之下,小键盘图像可以是小键盘的表示并且本身没有功能。因此,在没有可操作的小键盘的情况下,用户不能通过选择图像中描绘的“按键”将任何值输入到存储器中。在一个或多个实施例中,可以对图像中描绘的一个或多个按键进行颜色编码、加水印或以其他方式进行标记,以向用户提供视觉保证:图像已经由合法来源提供。

[0070] 由于可操作的小键盘中的按键的布置优选相对于小键盘图像中所绘制的按键的布置不同,可操作的按键的类型、顺序和/或位置不完全对应于图像中描绘的按键的类型、顺序和/或位置。可操作的小键盘或小键盘图像中的按键可以相对于参考小键盘是乱序的。由于可操作的小键盘中的按键的顺序优选地不同于图像中描绘的按键的顺序,因此可以在

可操作的小键盘和图像之间生成映射。该映射可以用于对标识符进行编码和/或解码。

[0071] 优选地,所述至少一个可操作的小键盘和/或至少一个小键盘图像被提供在用于捕获或生成生物特征数据的电子设备的显示区域内。显示区域可以包括触摸屏的一部分。有利的是,它们被提供在相同的显示区域内,使得小键盘图像叠加或遮蔽位于图像下面的可操作的小键盘。因此,小键盘和/或图像可以通过过程调用来生成;图像可以呈现为使得其至少部分但优选完全地从用户的视角看阻挡或遮挡小键盘。因此,用户可以看到他们认为是小键盘的东西,并且可以例如通过触摸他们认为是具有给定值的可操作的按键来进行选择,而实际上他们仅仅触摸图像的部分。然而,通过“选择”图像的部分,用户可以使小键盘的可操作的按键起作用,并且因此由可操作的小键盘放置到存储器中的值可能不对应于用户打算输入的值。因此,由于小键盘中的按键与图像中描绘的按键之间的映射,可以生成用户标识符的编码版本。这样做的好处是用户的“真实”标识符永远不会被放置在本地设备的存储器中。因此,已经设法破解本地设备的未经授权的第三方无法访问该“真实”标识符。

[0072] 本发明的这个编码方面可以基本上如WO 2014/013252中所述,其公开了认证解决方案,其中乱序的小键盘的图像叠加在可操作的小键盘上方以提供标识符的编码版本。然而,根据本发明,小键盘和/或图像可以使用生物特征数据在本地设备上或在本地设备处生成。

[0073] 因此,使用用户的生物特征数据生成的至少一个可操作的小键盘和/或至少一个小键盘图像可被用于提供用户标识符的编码版本。标识符的编码版本可以从本地设备传输到标识符的编码版本可以被存储的远程设备(例如服务器)。它可存储在安全的存储器中。它可以无线传输。

[0074] 小键盘图像可以被生成以使得图像中描绘的一个或多个按键被颜色编码、标记或以其他方式被标记(除了与按键相关联的值之外)。由于生物特征数据确保每次都可以生成相同的数组封装并且因此生成相同的图像,所以标记的按键可以向用户提供视觉上的保证,即他们正在观看的图像是合法的而不是在本地设备上未经授权的活动的结果。例如,用户可期望图像的左上角的按键被着色为黄色,并且小键盘图像的底行的中间按键被着色为红色。如果情况并非如此,则用户可能怀疑图像是由未授权方提供的。

[0075] 标识符可以被编码为注册过程的一部分,其中用户注册以使用本发明的实施方式。对于相同的标识符,编码可以只执行一次。注册过程可以包括捕获与用户有关的非生物特征数据,和/或涉及与用户相关的资源的数据,例如信用卡号码。在用户改变标识符的预存储版本(例如,经由他们的金融机构)的情况下,用户的新标识符的编码版本可以使用上述过程来提供,并且可以被存储以代替先前编码的版本。

[0076] 生物特征数据可以用于确定可操作的小键盘中的按键的配置和/或小键盘图像中描绘的按键的配置。这可以通过使用生物特征数据作为过程、功能或方法调用的输入来实现,该过程、功能或方法调用用于生成至少一个可操作的小键盘和/或至少一个小键盘图像。过程或方法调用可以形成小键盘生成组件的一部分。小键盘配置组件可以在本地设备上或在本地设备处生成小键盘和图像。生物特征数据可被用于提供一个或多个的值的数组,每个数组对应于用于创建小键盘或图像的小键盘配置。生物特征数据可被处理以提供一个或多个数组。

[0077] 可以由小键盘生成组件生成多个可操作的小键盘。另外或可选地,可以生成多个

小键盘图像。每个小键盘或图像中的按键的配置可以与相应多个小键盘或图像中的其他按键不同。一个小键盘和/或图像可以在任何给定时间被指定为“活动”小键盘或图像。例如，可以在认证会话期间使用一个小键盘图像，同时可以从用户接收的每个击键使用不同的在下面的小键盘。在一些实施方式中，可以使用一个可变小键盘，并且可以更改小键盘的状态，以便提供按键的不同配置。另外地或替代地，在小键盘图像可能改变的同时，在认证过程期间，下面的可操作的小键盘可保持不变。

[0078] 在最低限度情况下，在本地设备上使用生物特征数据以确定其配置来生成一个可操作的小键盘或一个小键盘图像。额外的配置数据和/或图像可以从服务器发送到本地设备。例如，可以使用生物特征数据来在本地设备处生成可操作的小键盘，然后将小键盘与从服务器接收的小键盘图像叠加。可选地，当在本地设备上使用本地捕获的生物特征数据生成图像时，可以在本地设备处接收来自服务器的小键盘配置数据。然而，在优选实施方式中，(一个或更多个)图像和小键盘可以全部在本地设备处生成。这是有利的，因为它消除了传输到本地设备期间配置数据被截取的风险，并且因为它将处理负担从服务器转移到本地设备。

[0079] 由于个人的生物特征数据不会改变，所以每当给定的用户使用本发明时，将生成相同的标识符的编码版本和/或小键盘配置。另一个优点是，由于用户的生物特征数据可以被用来确定可操作的小键盘中的按键与小键盘图像中描绘的按键之间的映射，所以用户的生物特征数据变成用于解码用户标识符的编码版本的“密钥”。另一个优点是，由于用户的生物特征数据总是可以被捕获或重新生成，所以不需要被存储。因此，一旦已经创建并存储了标识符的编码版本，就可以在提供用户的生物特征数据时始终对其进行解码。这避免了用户携带任何额外的认证设备(例如硬件令牌)或记住任何进一步的信息以解码标识符的需要。用户总是携带密钥来解锁标识符。因此，本发明提供了一种需要生物特征数据(用户是谁)和标识符(用户知道的东西)的多重认证解决方案。当标识符涉及例如用户的支付卡的资源(用户拥有的东西)时，这提供了三重认证解决方案。

[0080] 该方法还可以包括使用与用户有关的生物特征数据来计算编码的标识符的解码版本的步骤。可以在上述注册过程之后执行该解码步骤，在该注册过程期间可以生成并存储用户标识符的编码版本。解码步骤可以作为当用户希望获得对受控资源或服务的访问或者执行交易时发起的认证会话的一部分来执行。解码步骤也可以在注册过程中被执行，以验证用户输入的标识符是正确的，即匹配预先存储的标识符版本。

[0081] 用于对编码的标识符进行解码的生物特征数据可以与用于产生编码的版本的生物特征数据分开地并在其之后被捕获。计算解码版本可涉及使用从与用户有关的生物特征数据中生成的值的一个或更多个串、数组或序列。解码可以由服务器执行或在服务器处执行。解码可以在与服务器相关联的HSM内执行。

[0082] 标识符的解码版本可以关于先前存储的标识符的版本来验证。先前存储的版本可以由与支付卡相关联的机构或与支付卡相关方进行存储。验证可以通过向金融机构发送支付消息或余额查询来执行。如果标识符的解码版本与先前存储的版本相匹配，则标识符的验证可能是成功的，而如果不匹配则验证可能不成功。

[0083] 有利的是，仅需要用户的生物特征数据来解码该标识符。不需要重新输入用户的标识符。也不再需要图像或可操作的小键盘的生成。优选地，在编码版本已经在诸如服务器

的远程设备上被存储(并且可选地被验证)之后,用户可仅需要重新输入他们的生物特征数据,例如,轻扫手指,使得数组可以被重新生成并被传输到服务器用于解码标识符。这些数组可以使得服务器能够知道参考小键盘和使用生物特征数据生成的小键盘和/或图像的配置之间的映射。还有利的是,生物特征数据和由其生成的数组不需要被存储。这提供了更安全的解决方案,因为解码标识符的密钥因此不能从存储器被访问到。

[0084] 还根据本发明,提供了一种认证系统,其被布置和配置为实现上述方法的任何实施方式。这样的系统可以包括被布置和配置为使用与设备的用户有关的生物特征数据来对标识符进行编码的电子设备。

[0085] 生物特征数据可以在电子设备处或在其上生成。电子设备可以是手持式、便携式或移动计算设备。该设备可以被布置和配置为从生物特征数据生成值的一个或更多个串、数组或序列。

[0086] 该设备可以被布置成实现上述的编码处理或者使用生物特征数据作为密钥的任何其他编码处理。设备可以布置成使用生物特征数据来生成或指定小键盘配置。小键盘配置可以用于生成至少一个可操作的小键盘和/或至少一个小键盘图像。可操作的小键盘中的按键的配置可以相对于小键盘图像中描绘的按键的配置是不同的;和/或至少一个可操作的小键盘和/或至少一个小键盘图像可以被设置在用于捕获或生成生物特征数据的电子设备的显示区域内。

[0087] 生物特征数据可以用于确定至少一个可操作的小键盘中的按键的配置和/或至少一个小键盘图像中描绘的按键的配置。该至少一个可操作的小键盘和/或至少一个小键盘图像可以用于提供标识符的编码版本。该系统可以包括用于存储标识符的编码版本的存储器;优选地,其中,该存储器设置在服务器上或设置在服务器处。

[0088] 该至少一个小键盘和/或至少一个小键盘图像可以使用至少一部分生物特征数据作为方法或过程调用中的输入来生成。该至少一个可操作的小键盘可以从用户的视野看至少部分地被该至少一个小键盘图像遮蔽或遮挡。

[0089] 该系统可以包括被布置成使用与用户有关的生物特征数据来计算编码的标识符的解码版本的另外的设备。计算解码版本可涉及使用从与用户有关的生物特征数据中生成的值的一个或更多个串、数组或序列。系统可以被布置成相对于先前存储的标识符版本来验证用户标识符的解码版本。

[0090] 本发明可以提供一种认证方法,包括以下步骤:

[0091] 不止一次地生成可操作的小键盘或小键盘图像,其中,小键盘或图像中的按键的配置相对于按键的参考配置而更改;和

[0092] 颜色编码或以其他方式更改小键盘或图像中的一个或更多个预先选择的按键,使得每次小键盘或图像被生成时,相同的按键或按键位置总是以相同的方式被更改。如上所述,这个方面可以向用户提供小键盘和/或图像已经由合法来源生成的保证。

[0093] 应该注意的是,上面关于本发明的一个方面或实施方式描述的任何特征也可以用于与任何或所有其他方面或实施方式相关的优点。例如,关于本发明的方法描述的特征也可以适用于根据本发明的系统或装置,反之亦然。

[0094] 本发明的这些和其它方面根据本文描述的实施方式将是明显的并参考本文描述的实施方式进行说明。

## 附图说明

[0095] 现在将通过示例的方式并参考附图来描述本发明的实施方式,其中:

[0096] 图1是示出根据本发明的使用生物特征数据生成捕获用户的击键的图像和多个小键盘的过程的流程图。

[0097] 图2示出根据本发明的实施方式的注册过程的部分。

[0098] 图3示出根据本发明的实施方式的注册后过程的部分。

[0099] 图4示出根据本发明的实施方式可以使用的至少一些步骤的概览。

[0100] 现在将针对银行业提供本发明的说明性实施方式。它还使用编码过程,其涉及使用至少部分地使用生物特征数据生成的随机化的小键盘和/或小键盘图像。然而,应该注意的是,本发明不限于这些方面。

[0101] 根据本发明的一个实施方式的方法包括两步骤过程。第一步骤包括用于生成和存储用户标识符的编码版本的注册过程。标识符可以是与用户相关联的任何类型的代码或密码。用户的生物特征数据被用来生成编码版本。在注册之后,每当用户希望对服务或系统进行认证时,用户的生物特征数据被用于对标识符的编码版本进行解码。因此,用户的生物特征成为解锁标识符的编码版本的密钥。用户的生物特征数据不需要存储,但可以根据需要在需要时捕获。这提供了更安全但方便的认证布置,其不需要更改现有的基础设施。

[0102] 图4示出了本发明的至少部分过程的概览。如所示出的,用户的生物特征数据(例如指纹)由捕获设备捕获19。这被存储在用户设备上的安全存储元件中20。生物特征数据和/或用户的私有密钥被用来生成种子21。该种子被用作生成可用于生成PED的多个数组的算法的输入22。因此,PED生成取决于用户的唯一生物特征数据。

[0103] 注册过程

[0104] 首次使用前用户需要向系统注册。注册过程的部分在图1中示出。在注册期间,用户可能需要提供诸如与名字、地址和一个或多个支付卡有关的数据的数据。这些数据可以存储在远程设备(如服务器)上或用户(本地)设备上。本地设备可以是任何类型的计算设备,例如智能电话、笔记本电脑、PC、平板电脑。注册数据可以存储在本地设备上提供的数字钱包中。如本领域中已知的,钱包可以包括密码私有/公共密钥对或与之相关联。密钥对可能在使用生物特征捕获过程设置或注册钱包的过程中已经被生成。

[0105] 本地设备包括生物特征捕获设备或与生物特征捕获设备通信。现有技术中已知各种类型的捕获设备,并且本发明不限于捕获的数据的类型或用于捕获它的设备的类型。以下示例涉及指纹数据和指纹扫描仪,但是可选地或另外地,也可以使用其他类型的生物数据及其相应的捕获设备。

[0106] 指纹扫描仪用于捕获用户的生物特征数据1。然后将其馈送到本地设备上提供的小键盘生成组件(KGC)中。KGC可以从诸如基于云的服务器的远程源下载到本地设备以用于安装的软件应用。生物特征数据作为输入串提供给KGC。该串可用于提供值的一个或多个数组2,每个数组(或其部分/元素)能够作为过程调用的输入。该数组可以从生物特征捕获步骤1产生的串的子串。在优选实施方式中,KGC处理生物特征输入串以生成N+1个数组的封装,其中N是用户的标识符中的数字的数量3。附加数组可用于生成小键盘图像。每个数组指定图像或小键盘中按键的顺序(即配置)。这些数组可以存储在安全的临时存储器中。

[0107] 在步骤3中,KGC采用输入串并用它进行多个过程调用。第一个过程调用是图像生

成过程,它采用一个数组(即输入串的一部分)并生成小键盘图像。因此,生物特征数据被用作过程调用的参数。这些参数决定了图像中描述的按键的配置。术语“配置”可以涉及“按键”的位置、顺序和/或布置。然后图像被显示在与本地设备相关联的屏幕的显示区域内。在这个示例中,本地设备是具有触摸屏的智能电话,但是可以使用PC、监视器和鼠标来实现相同的效果。

[0108] 图像被创建成使得其类似于与本地设备相关联的(默认)小键盘的样式。然而,在一个实施方式中,图像中描绘的按键相对于设备的默认小键盘是乱序的。在其他实施方式中,图像可以描绘非乱序的小键盘。

[0109] 在一个或更多个实施方式中,小键盘图像被布置为使得一个或更多个按键被颜色编码或以其他方式被加标签、标记或标识(除了与按键相关联的值之外)。这使得能够生成对用户而言在视觉上独特的图像。例如,某些按键可以被赋予背景颜色。这可以用作对用户的如下视觉保证:用户看到的图像来自合法来源,而不是已经破解本地设备的未经授权的用户呈现的某些东西。

[0110] KGC还使用生物特征数据的一个或更多个其他部分作为输入来进行对小键盘生成过程的一个或更多个调用。在优选实施方式中,生成多个可操作的小键盘,用户标识符中的每个值或数字用一个小键盘。

[0111] 通过该过程生成可操作的小键盘,并将其设置在屏幕的与图像相同的部分内。优选地,图像完全覆盖小键盘,使得用户由于叠加它的图像而不能看见可操作的小键盘4。可操作的小键盘中按键的配置与图像中描绘的按键的配置不同。至少一个按键位于不同的位置,尽管优选多于一个或全部位置不同。因此,可操作的小键盘中的按键与图像中描绘的按键之间存在映射。这种映射是由生物特征输入决定的或者至少是受到其影响的,因此编码和随后的解码取决于生物特征输入。

[0112] 在一个实施方式中,图像可描绘非乱序的小键盘,而下面的可操作的小键盘的按键是乱序的。在另一个实施方式中,图像可以描绘乱序的小键盘,而下面的可操作的小键盘的按键不是乱序的。在又一个实施方式中,图像中描绘的按键和可操作的小键盘的按键都是位置乱序的。

[0113] 用户通过在屏幕上“选择”第一位数字,输入与其正在注册的支付卡相关联的标识符的第一位数字5。然而,由于图像自身并不包括小键盘功能,并且由于图像遮蔽正在监测屏幕的输入的可操作的小键盘,因此用户使隐藏小键盘的按键操作。与所操作的按键相关联的值被放置在本地设备上的存储器中5。因此,由小键盘实际存储的值可能不对应于用户在图像中“选择”的值。输入的编码版本已经生成,并且只有在小键盘和图像配置之间的映射已知时才能被解码。

[0114] 对用户标识符中的每个数字重复该输入过程(步骤5),使得可以通过将每个输入连接到先前的输入来在存储器中构建完整的编码的标识符6。在一个实施方式中,只有一个可变小键盘被生成,但是按键的配置在该过程期间被更改。从生物特征输入导出的数组被用于更改小键盘的状态。在另一个实施方式中,为每个击键替换下面的小键盘,因此对于每个输入使用具有不同配置的新小键盘。因此,可以不止一次地调用小键盘生成过程,每次调用使用从生物特征数据导出的值的(不同的)数组。在一些实施方式中,图像可以在输入过程中被替换。在一些实施方式中,生物特征数据可以被用于仅指定可操作的小键盘的乱序

配置,或者仅指定图像。在其他实施方式中,其可以用于使显示的图像和隐藏小键盘的配置都乱序。

[0115] 由于相同的用户将总是提供相同的生物特征数据,所以总是会生成相同的串以及因此生成相同的图像和/或小键盘配置。

[0116] 转到图2,当已经构建了用户的完整标识符的编码版本6时,将其与用于创建它的N+1个数组一起存储在用户设备上的安全存储器中。编码的标识符和数组的副本被发送到服务器7并被传递到硬件安全模块(HSM)8。HSM被定位成远离本地设备,位于服务器处。在标识符与诸如信用卡或借记卡之类的卡相关联的情况下,有必要检查由用户键入的标识符对于卡是正确的。因此,其必须由发卡机构进行验证。

[0117] 为了执行验证,使用用于创建编码的标识符的数组封装对编码的标识符进行解码8。这种解码是可能的,因为数组封装提供了图像和小键盘配置之间的映射。标识符的未编码版本然后被存储在HSM中,并被用于生成PIN块。PIN块用于将支付消息发送到收单机构,然后收单机构将其中继到卡的发行机构9。

[0118] 如果标识符不正确12(即,与发行机构存储的与该卡相关联的标识符不匹配),发行机构将用指示此的消息进行响应。然后可以要求用户重新键入他的标识符,并重复上述过程。如果输入了三个不正确的标识符,注册过程可能会中止13。

[0119] 然而,如果发行机构指示标识符是正确的10,则标识符的编码版本从临时存储器移动到安全存储器11。临时存储器然后被擦除。

[0120] 应该注意的是,标识符可以以各种方式进行验证。在一个实施方式中,余额查询可以在服务器处生成并通过ATM网络发送给发行机构。

[0121] 当注册完成时,给定卡的用户标识符的编码版本已被生成并被安全地存储。由于使用从用户的生物特征数据生成的映射来执行编码,所以生物特征数据是解锁或解码标识符所需的密钥。数组封装不需要存储在任何地方,既不需要在本地设备上也不需要服务器上,因为它可以根据需要通过重新捕获用户的生物特征数据来生成。类似地,由于编码版本已经被安全地存储在服务器上,用户不需要在随后的认证会话期间重新键入标识符。因此,在随后的认证期间只需要生成数组封装,并将其发送到服务器,使得先前存储的编码的标识符可以被解码。这提供了安全和方便的认证解决方案。

[0122] 注册后的认证

[0123] 如图3所示,在注册之后,当用户希望使用注册的支付卡进行交易时,从本地设备上的数字钱包中选择该卡。他扫描他的指纹14。如上所述,根据生物特征捕获而生成的串作为输入被馈送到KGC。生成N+1个数组并将其发送到服务器15,在那里将它们放置在临时存储器中。先前验证的编码的标识符从安全存储器中被检索16。编码的标识符和数组被放入HSM中16,其中数组用于解码标识符17。标识符和卡细节(从钱包中检索或者在需要时由用户键入)与交易额一起作为支付消息发送给收单机构例如银行18。然后收单机构将该消息中继给发行银行,如果标识符正确,则处理该交易,或者如果标识符不正确,则拒绝该交易。

[0124] 因此,解码过程不需要来自用户的除了生物特征数据之外的任何输入。标识符不需要重新键入,并且小键盘/图像不需要被重新生成。

[0125] 在一个或更多个实施方式中,编码过程可以由与解码过程不同的一方执行。标识符可以使用生物特征数据被编码,然后被提供给另一方,并以编码形式被存储在另外的系

统或设备上。另一方则只需要用户的生物特征数据,该生物特征数据可以根据需要捕获和提供,以解锁标识符。

[0126] 应注意,上面提到的实现说明而不是限制本发明,以及本领域中的技术人员将能够设计很多可选的实施例而不偏离由所附权利要求限定的本发明的范围。在权利要求中,放置在括号中的任何参考符号不应被解释为限制权利要求。词“comprising (包括)”和“comprises (包括)”等并不排除除了作为整体在任何权利要求或说明书中列出的元素或步骤以外的元素或步骤的存在。在本说明书中,“包括 (comprises)”意指“包含或含有”,以及“包括 (comprising)”意指“包含或含有”。元素的单数引用并不排除这样的元素的复数引用,反之亦然。可借助于包括几个不同的元素的硬件和借助于适当编程的计算机来实现本发明。在列举几个工具的设备权利要求中,这些工具中的几个工具可由硬件的一个且同一项目体现。某些措施在相互不同的从属权利要求中引用的不争事实并不指示这些措施的组合不能有利地被使用。

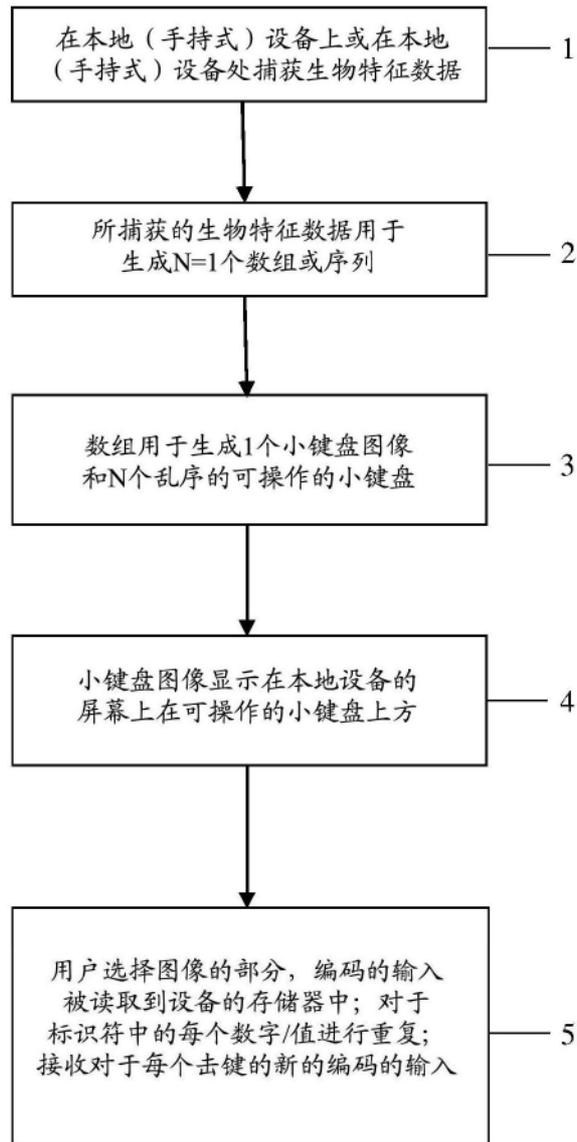


图1

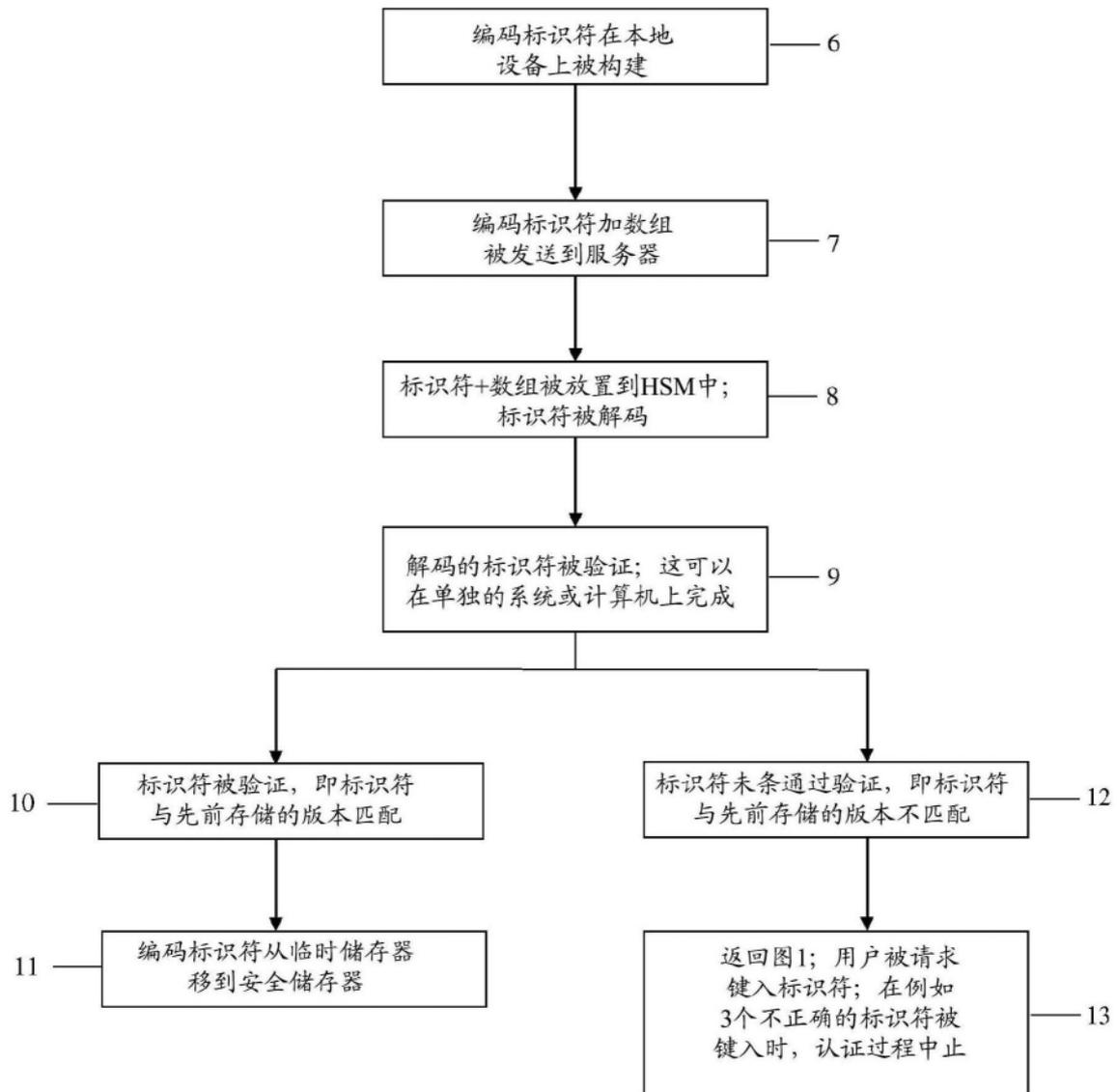


图2

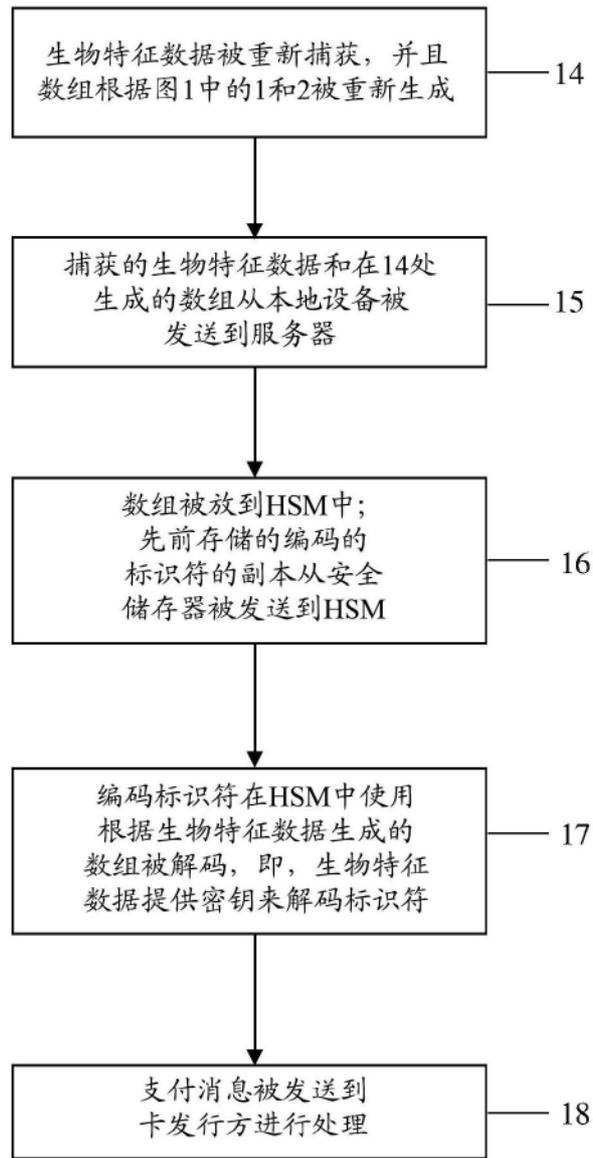


图3

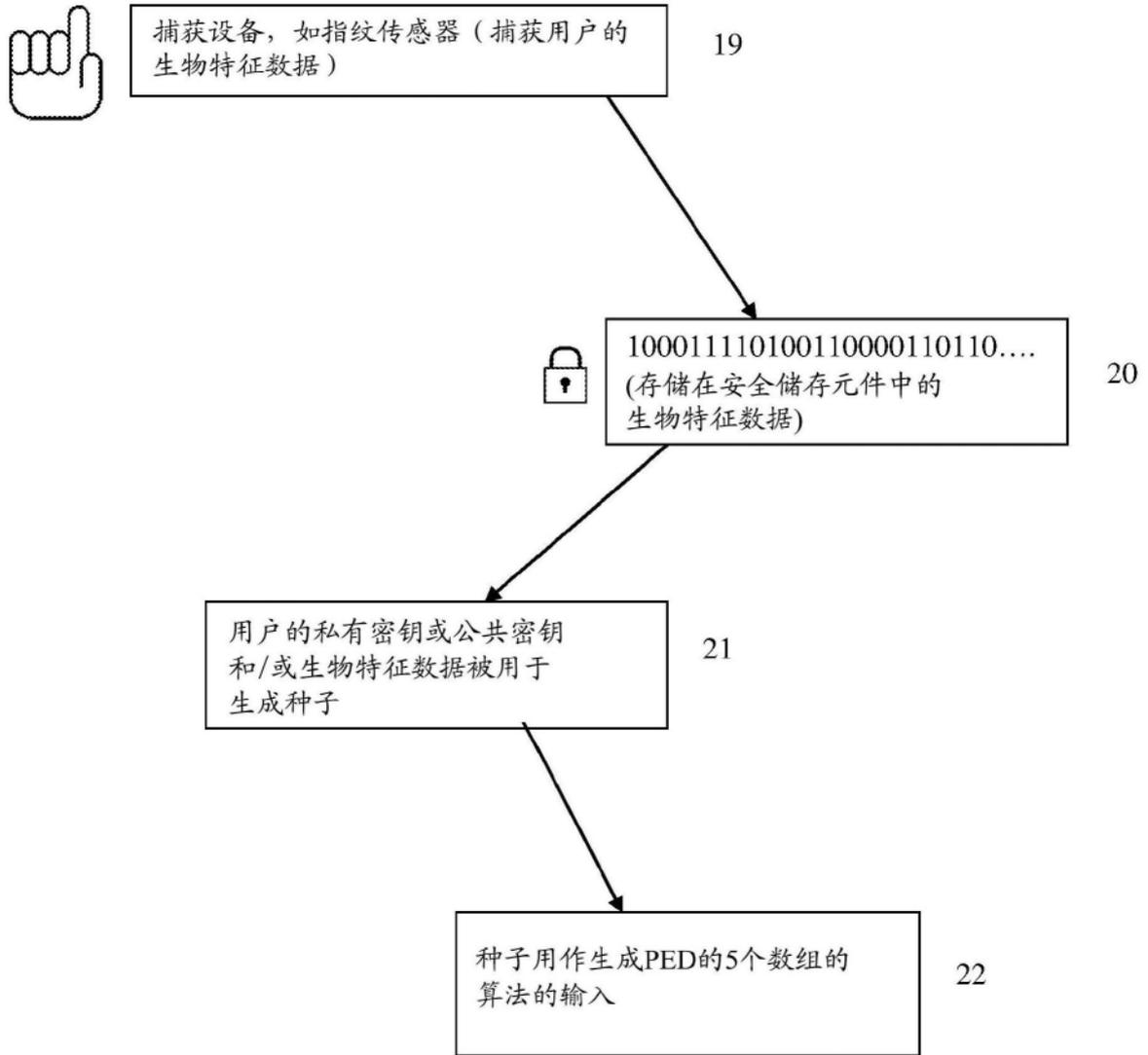


图4