



(12) 发明专利

(10) 授权公告号 CN 112334897 B

(45) 授权公告日 2025. 01. 07

(21) 申请号 201980039812.8

(22) 申请日 2019.06.18

(65) 同一申请的已公布的文献号
申请公布号 CN 112334897 A

(43) 申请公布日 2021.02.05

(30) 优先权数据
1850741-8 2018.06.19 SE

(85) PCT国际申请进入国家阶段日
2020.12.14

(86) PCT国际申请的申请数据
PCT/SE2019/050577 2019.06.18

(87) PCT国际申请的公布数据
W02019/245437 EN 2019.12.26

(73) 专利权人 指纹卡安娜卡敦知识产权有限公
司
地址 瑞典哥德堡

(72) 发明人 马茨·图内尔德

克里斯蒂安·格尔曼

埃里克·塞特贝里

(74) 专利代理机构 北京集佳知识产权代理有限
公司 11227

专利代理师 杜诚 刘敏

(51) Int.Cl.
G06F 21/32 (2013.01)
G06V 40/10 (2022.01)
G06V 40/12 (2022.01)
G06V 40/50 (2022.01)
G06F 21/83 (2013.01)
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(56) 对比文件
US 2017330021 A1,2017.11.16
GB 2546459 A,2017.07.19

审查员 赵婷

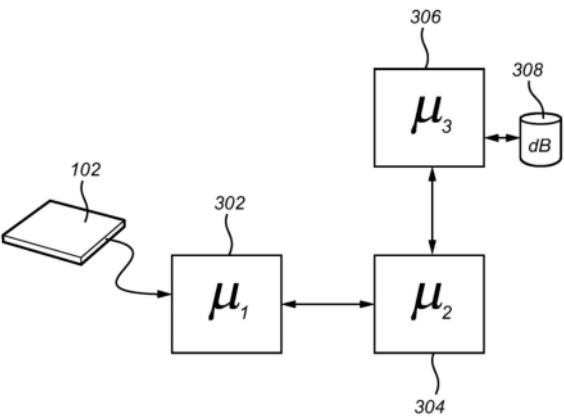
权利要求书4页 说明书9页 附图4页

(54) 发明名称

认证用户的方法和电子设备

(57) 摘要

本公开内容总体上涉及使用电子设备来认证用户的方法,其中,该电子设备包括生物计量感测系统以及第一、第二和第三控制单元。本公开内容还涉及相应的电子设备和计算机程序产品。



1. 一种使用电子设备认证用户的方法,所述电子设备包括:

- 生物计量感测系统,其被配置用于捕获所述用户的生物计量表示,
- 第一控制单元,其连接至所述生物计量感测系统,并且适于提供具有第一安全水平的处理环境,
- 第二控制单元,其被布置成与所述第一控制单元通信,并且适于提供具有第二安全水平的处理环境,以及
- 第三控制单元,其被布置成与所述第二控制单元通信,并且适于提供具有第三安全水平的处理环境,

其中,所述第二安全水平低于所述第一安全水平和所述第三安全水平,并且所述方法包括以下步骤:

- 使用所述生物计量感测系统和所述第一控制单元获取生物计量表示,
- 使用所述第一控制单元确定指示所述生物计量表示的第一特征集,
- 使用所述第一控制单元形成所述第一特征集的受保护表示,
- 将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元,
- 使用所述第二控制单元确定指示所述生物计量表示的第二特征集,其中,与对所述第二特征集的确定相比,根据相比之下的低分辨率生物计量表示来确定所述第一特征集,
- 将所述第一特征集的受保护表示和所述第二特征集提供给所述第三控制单元,
- 在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示,以及
- 在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集的组合来认证所述用户,其中利用与所述第三控制单元相关联的存储元件存储所述生物计量模板布置,并且所述生物计量模板布置表示所述用户的生物计量表示。

2. 根据权利要求1所述的方法,其中,提取所述第一特征集的受保护表示的步骤包括:从所述第三控制单元向所述第一控制单元提供质询。

3. 根据权利要求2所述的方法,其中,通过所述第二控制单元中继所述质询。

4. 根据权利要求1所述的方法,其中,形成所述第一特征集的受保护表示的步骤包括:使所述第一特征集的受保护表示包括时间戳。

5. 根据权利要求4所述的方法,其中,认证所述用户的步骤还取决于所述时间戳。

6. 根据权利要求1所述的方法,其中,所述第一控制单元和所述第三控制单元适于提供安全处理环境。

7. 根据权利要求1所述的方法,其中,所述第一控制单元被配置成控制指纹感测系统的操作。

8. 根据权利要求1所述的方法,其中,所述第二控制单元是用于所述电子设备的通用控制单元,还适于至少部分地控制所述电子设备所包括的显示屏。

9. 根据权利要求1所述的方法,其中,所述生物计量模板布置包括第一生物计量模板部分(T_{vl})和第二生物计量模板部分(T_{vh})。

10. 根据权利要求9所述的方法,其中:

- 所述第一生物计量模板部分(T_{vl})对应于所述第一特征集的提取表示的结构,并且
- 所述第二生物计量模板部分(T_{vh})对应于所述第二特征集的结构。

11. 根据权利要求9和10中任一项所述的方法,其中,基于所述第一特征集的提取表示与所述第一生物计量模板部分之间的第一比较以及所述第二特征集与所述第二生物计量模板部分之间的第二比较来认证所述用户。

12. 根据权利要求11所述的方法,其中,如果所述第一比较和所述第二比较两者都被指示为成功,则所述用户被认证。

13. 根据权利要求1所述的方法,还包括以下步骤:

- 使用所述第二控制单元形成所述第二特征集的受保护表示,以及
- 在所述第三控制单元处从所述第二特征集的受保护表示提取所述第二特征集,从而形成所述第二特征集的提取表示。

14. 根据权利要求13所述的方法,其中,使用密钥来形成所述第二特征集的受保护表示,所述密钥与用于形成所述第一特征集的受保护表示的密钥不同。

15. 根据权利要求1所述的方法,其中,与所述第二特征集相比,所述第一特征集包括较少的信息。

16. 根据权利要求1所述的方法,其中,根据所述生物计量表示的子部分来确定所述第一特征集。

17. 根据权利要求16所述的方法,其中,由所述第一控制单元选择所述生物计量表示的所述子部分。

18. 根据权利要求1所述的方法,其中,所述第二控制单元被布置为与所述第一控制单元和所述第三控制单元分开。

19. 根据权利要求1所述的方法,其中,所述第三控制单元被布置为与所述第一控制单元和所述第二控制单元分开。

20. 根据权利要求1所述的方法,其中,所述电子设备还包括与所述第三控制单元相关联的所述存储元件,所述存储元件用于存储指纹模板布置。

21. 根据权利要求1所述的方法,其中,所述第一控制单元和所述第三控制单元共享对称完整性保护密钥(K),所述对称完整性保护密钥(K)用于对所述第一特征集的保护和提取。

22. 根据权利要求1所述的方法,其中,所述第一控制单元和所述第三控制单元适于应用基于非对称密码学的方案,以用于对所述第一特征集和所述第二特征集中的至少一个的完整性保护。

23. 根据权利要求1所述的方法,其中,所述生物计量感测系统被配置用于捕获所述用户的手指的指纹图案的指纹表示。

24. 根据权利要求1所述的方法,其中,所述生物计量感测系统被配置用于捕获所述用户的图像和所述用户的虹膜表示中的至少一者。

25. 一种电子设备,包括:

- 生物计量感测系统,其被配置用于捕获用户的生物计量表示,
- 第一控制单元,其连接至所述生物计量感测系统,并且适于提供具有第一安全水平的处理环境,以及
- 第二控制单元,其被布置成与所述第一控制单元通信,并且适于提供具有第二安全水平的处理环境,

其中,所述电子设备适于进行以下操作:

- 使用所述生物计量感测系统和所述第一控制单元获取生物计量表示,
- 使用所述第一控制单元确定指示所述生物计量表示的第一特征集,
- 使用所述第一控制单元形成所述第一特征集的受保护表示,
- 将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元,
- 使用所述第二控制单元确定指示所述生物计量表示的第二特征集,其中,与对所述第二特征集的确定相比,根据相比之下的低分辨率生物计量表示来确定所述第一特征集,
- 将所述第一特征集的受保护表示和所述第二特征集提供给第三控制单元,其中,所述第三控制单元被布置成与所述第二控制单元通信并且适于提供具有第三安全水平的处理环境,所述第二安全水平低于所述第一安全水平和所述第三安全水平,
- 在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示,以及
- 在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集的组合来认证所述用户,其中利用与所述第三控制单元相关联的存储元件存储所述生物计量模板布置,并且所述生物计量模板布置表示所述用户的生物计量表示。

26. 根据权利要求25所述的电子设备,还包括所述第三控制单元。

27. 根据权利要求25所述的电子设备,其中,所述第三控制单元被布置成远离所述电子设备。

28. 根据权利要求25所述的电子设备,其中,所述电子设备是移动电话、平板电脑、可穿戴电子设备和智能卡中的至少一者。

29. 根据权利要求25所述的电子设备,其中,所述生物计量感测系统包括采用光学感测技术、热感测技术和超声感测技术中的至少一种的指纹感测装置。

30. 根据权利要求25所述的电子设备,其中,所述生物计量感测系统包括用于获取所述用户的图像和所述用户的虹膜表示中的至少一者的装置。

31. 一种包括非暂态计算机可读介质的计算机程序产品,所述非暂态计算机可读介质上存储有用于操作电子设备的计算机程序装置,所述电子设备包括:

- 生物计量感测系统,其被配置用于捕获用户的生物计量表示,
- 第一控制单元,其连接至所述生物计量感测系统,并且适于提供具有第一安全水平的处理环境,
- 第二控制单元,其被布置成与所述第一控制单元通信,并且适于提供具有第二安全水平的处理环境,以及
- 第三控制单元,被布置成与所述第二控制单元通信,并且适于提供具有第三安全水平的处理环境,

其中,所述第二安全水平低于所述第一安全水平和所述第三安全水平,并且所述计算机程序产品包括:

- 用于使用所述生物计量感测系统和所述第一控制单元获取生物计量表示的代码,
- 用于使用所述第一控制单元确定指示所述生物计量表示的第一特征集的代码,
- 用于使用所述第一控制单元形成所述第一特征集的受保护表示的代码,
- 用于将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元

的代码,

- 用于使用所述第二控制单元确定指示所述生物计量表示的第二特征集的代码,其中,与对所述第二特征集的确定相比,根据相比之下的低分辨率生物计量表示来确定所述第一特征集,

- 用于将所述第一特征集的受保护表示和所述第二特征集提供给所述第三控制单元的代码,

- 用于在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示的代码,以及

- 用于在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集的组合来认证所述用户的代码,其中利用与所述第三控制单元相关联的存储元件存储所述生物计量模板布置,并且所述生物计量模板布置表示所述用户的生物计量表示。

认证用户的方法和电子设备

技术领域

[0001] 本公开内容总体上涉及使用电子设备来认证用户的方法,其中,该电子设备包括生物计量感测系统,以及第一、第二和第三控制单元。本公开内容还涉及相应的电子设备和计算机程序产品。

背景技术

[0002] 正在越来越多地使用生物计量技术来识别和/或认证用户的身份。为了这种用途而推广的生物计量技术包括语音、指纹、虹膜、静脉图案和其他扫描。目前,使用指纹传感器以捕获指纹已经例如由于其易于与不同类型的电子设备集成而显示出了特别的前景,所述电子设备例如是智能手机、手表、平板电脑或任何其它类型的电子设备,在所述它类型的电子设备中个性化用户交互是有益的。还提出将这样的指纹传感器与智能卡系统集成,可能消除在执行例如财务交易时用户输入PIN码的需要。

[0003] 然而,由于上述电子设备的移动性,总是存在电子设备落入“坏人之手”并且/或者面临例如黑客攻击的风险,该黑客攻击的目的是篡改或以其他方式影响生物计量识别和/或认证过程。

[0004] 为了抵制这样的尝试,继续尝试改进所应用的生物计量识别和/或认证过程。然而,这样的尝试通常导致复杂的计算处理,从而增加为电子设备配备更快和计算上更强大的处理环境的需求。

[0005] 在期望高安全性和计算上强大的处理环境的上述类型的电子设备的一些实现方式中,已经提出将计算性能“分割”为两部分,第一部分是高性能环境,而第二部分是高安全性环境。高性能环境通常具有较高的计算性能但安全性较低。相应地,高安全性环境,例如包括所谓的安全元件,通常具有较高的安全性但计算性能较低。

[0006] 在US9536131中公开了这样的实现方式的示例。US9536131提供了一种有趣的方法以划分执行生物计量认证所需的计算资源,特别是关于第一处理单元与第二处理单元之间的指纹认证,第一处理单元提供上述高性能环境,第二处理单元提供上述高安全性环境。根据US9536131,高性能第一处理单元用于执行所获取的用户的指纹图像与待认证用户的手指的预先记录的指纹模板之间的比较过程。

[0007] 遗憾的是,US9536131中提出的解决方案借助于如何在第一处理单元与第二处理单元之间划分计算处理而引入了一些可能的安全风险。

发明内容

[0008] 鉴于现有技术的上述问题,本公开内容的目的是提供一种针对使用电子设备的用户的生物计量认证,在维持高安全性的同时有效地划分计算资源的进一步均衡的解决方案。

[0009] 根据本公开内容的一个方面,因此提供了一种使用电子设备认证用户的方法,该电子设备包括:生物计量感测系统,其被配置用于捕获所述用户的生物计量表示;第一控制

单元,其连接至所述生物计量感测系统并且适于提供具有第一安全水平的处理环境,第二控制单元,其被布置成与所述第一控制单元通信并且适于提供具有第二安全水平的处理环境;以及第三控制单元,其被布置成与所述第二控制单元通信并且适于提供具有第三安全水平的处理环境,其中,所述第二安全水平低于所述第一安全水平和所述第三安全水平,并且所述方法包括以下步骤:使用所述生物计量感测系统和所述第一控制单元获取生物计量表示;使用所述第一控制单元来确定指示所述生物计量表示的第一特征集;使用所述第一控制单元形成所述第一特征集的受保护表示;将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元;使用所述第二控制单元来确定指示所述生物计量表示的第二特征集;将所述第一特征集的受保护表示和所述第二特征集提供给所述第三控制单元;在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示;以及在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集来认证所述用户,其中所述生物计量模板布置表示所述用户的生物计量表示。

[0010] 本公开内容背后的主要构思在于对生物计量认证过程的改进的分割,其中,生物计量认证过程的一些部分由第一控制单元执行,而生物计量认证过程的一些其他部分由第二控制单元执行。根据本公开内容,与先前为用户形成的生物计量模板相关地,第三控制单元进而被用于第一特征集和第二特征集的“双重匹配”。

[0011] 因此,在优选实施方式中,第二控制单元适于提供与第一控制单元所提供的性能环境相比更高的性能环境。此外,在本公开内容的可能实施方式中,第一控制单元和第三控制单元提供安全处理环境。

[0012] 与现有技术相比,本公开内容允许生物计量认证过程的适配(adaptation),其中,两个单独的特征提取过程由两个不同的控制单元(即,第一控制单元和第二控制单元)执行,并且其中,第三控制单元被布置成执行双重匹配过程,其中,将两个特征提取过程的结果与在第三控制单元处布置的生物计量模板进行比较。

[0013] 根据本公开内容,第一控制单元和第三控制单元被表示为具有比第二控制单元更高的安全水平。表述“更高的安全水平”应当被理解为涉及以下处理环境:其中,对个人数据的可信处理成为可能,例如用于执行指示生物计量表示的第一特征集的确定以及用于执行用户的最终认证。这种处理环境(例如,使用所谓的安全元件使其成为可能)将提供信任根(root of trust),使得在至少第一控制单元和第三控制单元上运行的处理在受控且可信的环境中执行。除了常规的密码或加密保护之外,可以基于例如嵌入式安全元件从软件级别和硬件级别两者引入替选的安全特征。

[0014] 为了确保在第一控制单元处提取的特征不被例如第三方“触及”,第一控制单元形成第一特征集的受保护版本。在一个实施方式中,对第一特征集的保护包括以第三控制单元稍后可以验证第一特征集的完整性的方式来确保第一特征集的完整性。

[0015] 然而,在优选的实施方式中,对第一特征集的保护还包括确保第一特征集的机密性(例如,借助于加密)和完整性。因此,与这样的实施方式一致,可以优选地确保在第一控制单元和第三控制单元之间以及在第二控制单元和第三控制单元之间的第一特征集和/或第二特征集的传输包括提供以下质询:从第三控制单元到第一控制单元的质询,以及从第三控制单元到第二控制单元的质询。这种“质询-响应(challenge-response)”处理的实现

可以例如与已知处理一致地进行。

[0016] 作为备选(或者此外),可以允许时间戳被包括在受保护的第一特征集中,其中,时间戳可以用于确保从第一控制单元提供给第三控制单元的第一数据集的“新鲜度”。即,例如,可以将时间戳与“时间阈值”进行比较,其中,如果第一特征集例如“太旧”,则可能丢弃该第一特征集。在这种情况下,因为在涉及第一生物计量模板的匹配过程中没有第一特征集“可用”,所以双重匹配将不会成功。

[0017] 在本公开内容的实施方式中,生物计量模板布置包括第一生物计量模板部分(T_{vl})和第二生物计量模板部分(T_{vh})。因此,认证过程可以涉及将第一特征集与第一生物计量模板部分进行比较/匹配,以及将第二特征集与第二生物计量模板部分进行比较/匹配。因此,在一个实施方式中,第一模板部分的“结构”与第一生物计量模板部分的“结构”相匹配(对于第二特征集和第二生物计量模板部分而言类似地),例如,出于确保在其之间高效比较/匹配的目的。

[0018] 在本公开内容的优选实施方式中,基于第一特征集的提取表示与第一生物计量模板部分之间的第一比较以及第二特征集与第二生物计量模板部分之间的第二比较来认证用户。因此,只有当第一比较和第二比较都被指示为成功时,用户才被认证。

[0019] 与本公开内容一致,与第二控制单元实现的特征提取过程相比,可以允许第一控制单元实现的特征提取过程“在计算方面更轻量”,因为在典型实施方式中第二控制单元(如上所述)适于提供与第一控制单元所提供的性能环境相比更高的性能环境。

[0020] 因此,借助于本公开内容,可以使得能够实现具有高计算要求的高级认证过程,同时与现有技术相比,仍然确认证过程具有较高的安全性和较低的黑客成功攻击的风险。除了上述之外,当然应当理解,认证过程的一般分割在以下电子设备的实现中(例如与智能卡实现相关)也可能是非常有用的:在该电子设备的实现中,由于成本和/或基板面(real estate)原因,安全过程的能力受到限制。

[0021] 在本公开内容的上下文中,表述“控制单元”应当被理解为包括任何类型的计算设备,例如ASIC、微处理器等。还应当理解,这种控制单元的实际实现可以在多个元件/设备/电路之间划分,仍然统称为控制单元。优选地,第二控制单元被布置成与第一控制单元分开。

[0022] 在用户被成功认证的情况下,根据本公开内容,可以执行至少一个动作。这样的动作可以例如针对电子设备,以允许用户使用电子设备执行进一步的操作,例如当电子设备是移动电话或平板电脑时。当然,所述至少一个动作可以是当需要认证用户时(例如允许进行财务交易)适当使用的任何类型的动作。在成功认证的情况下,还可以基于第一特征集和第二特征集中的至少一个来更新第一生物计量模板。

[0023] 在本公开内容的一个示例性实施方式中,第一控制单元连接至生物计量感测系统,并且被配置成控制生物计量感测系统的操作。这种实现方式例如关于以下情况可能是有用的:电子设备是所提及的移动电话/平板电脑、膝上型计算机等。

[0024] 基于从计算角度来看第一控制单元比第二控制单元稍微“更弱”的事实,在一些实施方式中,根据生物计量表示的子部分来确定第一特征集可能是有利的。根据本公开内容,子部分可以被视为包括例如用于减少待处理数据量的剪切、抽取或截断处理。因此,减少的信息量被处理以确定第一特征集,从而可能平衡第一控制单元的计算能力。

[0025] 在可能的实施方式中,生物计量表示的子部分由第一控制单元选择。与主要/第一生物计量模板相比,这种实现方式再次不允许任何第三方参与选择进一步使用哪些信息。优选地,允许该选择是至少部分地随机的,或者至少针对不同的生物计量表示是不同的(例如针对用户的生物计量表示的连续认证是不同的)。

[0026] 为了进一步确保认证过程的足够安全性,在一些实施方式中,可以安排共享对称完整性保护密钥(K),该对称完整性保护密钥(K)被用于保护和提取第一特征集。相应地,关于在第二控制单元和第三控制单元之间的第二特征集的传输,出于相同的目的,可以使用另一不同的对称完整性保护密钥。

[0027] 应当理解,作为备选,关于与以上讨论一致的第一特征集和第二特征集中的至少一个,可以使用基于非对称密码学的方案以用于实现适当的完整性保护。

[0028] 在本公开内容的优选实施方式中,生物计量感测系统被配置用于捕获用户手指的指纹图案的指纹表示。与这样的实施方式一致,表述“用户手指的指纹图案的表示”或“指纹图像”应当被广义地解释,并且包括手指的指纹的常规“视觉图像”以及在使用指纹传感器获取时与手指有关的一组测量结果。随后可以获取多个指纹表示/图像并将其融合在一起,其中,所得到的信息被用作为用于确定特征集的输入。

[0029] 可以使用任何种类的当前或将来的指纹感测原理来实现所提及的指纹传感器,所述指纹感测原理包括例如电容式感测技术、光学感测技术、或热感测技术及其组合。一维传感器和二维传感器两者都是可能的,并且在本公开内容的范围内。

[0030] 在本公开内容的另一可能实施方式中,生物计量感测系统被配置用于捕获用户的图像和用户的虹膜表示中的至少一者。同样,例如,可以使用摄像装置或其他装置来捕获例如用户的图像或用户的虹膜。其他实现方式对于获取例如用户的虹膜表示是可能的。

[0031] 根据本公开内容的另一方面,提供了一种电子设备,包括:生物计量感测系统,其被配置用于捕获用户的生物计量表示;第一控制单元,其连接至所述生物计量感测系统,并且适于提供具有第一安全水平的处理环境;以及第二控制单元,其被布置成与所述第一控制单元通信,并且适于提供具有第二安全水平的处理环境,其中,所述电子设备适于进行以下操作:使用所述生物计量感测系统和所述第一控制单元获取生物计量表示;使用所述第一控制单元来确定指示所述生物计量表示的第一特征集;使用所述第一控制单元形成所述第一特征集的受保护表示;将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元;使用所述第二控制单元来确定指示所述生物计量表示的第二特征集;将所述第一特征集的受保护表示和所述第二特征集提供给第三控制单元,其中,所述第三控制单元被布置成与所述第二控制单元通信,并且适于提供具有第三安全水平的处理环境,所述第二安全水平低于所述第一安全水平和所述第三安全水平;在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示;以及在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集来认证所述用户,其中所述生物计量模板布置表示所述用户的生物计量表示。本公开内容的该方面提供了与以上关于本公开内容的先前方面所讨论的优点类似的优点。

[0032] 在一个实施方式中,电子设备还包括第三控制单元。作为备选,第三控制单元可以被布置成远离电子设备。

[0033] 根据本公开内容的另一方面,提供了一种包括计算机可读介质的计算机程序产品,所述计算机可读介质上存储有用于控制电子设备的计算机程序装置,所述电子设备包括:生物计量感测系统,其被配置用于捕获所述用户的生物计量表示;第一控制单元,其连接至所述生物计量感测系统并且适于提供具有第一安全水平的处理环境;第二控制单元,其被布置成与所述第一控制单元通信并且适于提供具有第二安全水平的处理环境;以及第三控制单元,被布置成与所述第二控制单元通信并且适于提供具有第三安全水平的处理环境,其中,所述第二安全水平低于所述第一安全水平和所述第三安全水平,并且所述计算机程序产品包括:用于使用所述生物计量感测系统和所述第一控制单元获取生物计量表示的代码;用于使用所述第一控制单元确定指示所述生物计量表示的第一特征集的代码;用于使用所述第一控制单元形成所述第一特征集的受保护表示的代码;用于将所述生物计量表示和所述第一特征集的受保护表示提供给所述第二控制单元的代码;用于使用所述第二控制单元确定指示所述生物计量表示的第二特征集的代码;用于将所述第一特征集的受保护表示和所述第二特征集提供给所述第三控制单元的代码;用于在所述第三控制单元处从所述第一特征集的受保护表示提取所述第一特征集,从而形成所述第一特征集的提取表示的代码;以及用于在所述第三控制单元处基于生物计量模板布置、所述第一特征集的提取表示和所述第二特征集来认证所述用户的代码,其中所述生物计量模板布置表示所述用户的生物计量表示。同样,本公开内容的该方面提供了与以上关于本公开内容的先前方面所讨论的优点类似的优点。

[0034] 当研究所附权利要求和以下描述时,本公开内容的进一步特征和优点将变得明显。本领域技术人员认识到,在不脱离本公开内容的范围的情况下,可以组合本公开内容的不同特征以创建除了以下描述的实施方式之外的实施方式。

附图说明

[0035] 根据以下具体实施方式和附图将容易地理解本公开内容的各个方面,包括本公开内容的特定特征和优点,在附图中:

[0036] 图1A和图1B示出了根据本公开内容的当前优选实施方式的不同电子设备的示例实现方式,

[0037] 图2示意性地示出了包括在例如图1A和1B所示的电子设备中的指纹传感器阵列的示例,

[0038] 图3A概念性地示出了在图1A和图1B所示的电子设备处实现的并且与本公开内容一致的架构块结构,并且图3B示出了与本公开内容一致的备选分布式架构,

[0039] 图4呈现了描述认证过程的实施方式的详细消息图,以及

[0040] 图5是公开了本公开内容的示例性步骤的流程图。

具体实施方式

[0041] 现在将在下文中参照附图更全面地描述本公开内容,在附图中示出了本公开内容的当前优选实施方式。然而,本公开内容可以以许多不同的形式来实施,并且不应被解释为限于本文中阐述的实施方式。而是说,提供这些实施方式是为了彻底性和完整性,并且向技术人员全面地传达本公开内容的范围。相同的附图标记始终指代相同的特征。

[0042] 现在转到附图,特别是图1A,示意性地示出了根据本公开内容的电子设备的第一示例,其形式为移动电话100,移动电话100具有集成生物计量感测系统和带有触摸屏界面106的显示单元104。在该实施方式中,生物计量感测系统被例示为指纹传感器布置在移动电话100的前侧。指纹传感器102可以例如用于解锁移动电话100以及/或者用于授权使用移动电话100执行的交易等。作为替选,生物计量感测系统例如可以被布置成包括摄像装置(或类似物),该摄像装置(或类似物)被布置成捕获例如用户的面部或虹膜的图像,以用于认证用户。

[0043] 优选地,并且对技术人员而言明显的是,图1A中示出的移动电话100还包括:用于WLAN/Wi-Fi通信的第一天线、用于电信通信的第二天线、麦克风、扬声器以及电话控制单元。当然,移动电话可以包括另外的硬件特征。此外,应当注意,本公开内容可以与任何其他类型的便携式电子设备相关地应用,例如膝上型计算机、遥控器、平板计算机,或者任何其他类型的当前或将来类似配置的设备。

[0044] 在图1B中,示出了根据本公开内容的电子设备的第二示例,其形式为智能卡100',集成了生物计量感测系统,该生物计量感测系统包括指纹传感器102以及控制单元装置108,该指纹传感器102包括多个感测特征并且被配置用于捕获用户手指的指纹图案的指纹表示,该控制单元装置108连接至指纹传感器102并且被配置成控制指纹传感器102的操作。在该实施方式中,指纹传感器102布置在智能卡100'的前侧。然而,指纹传感器102可以替选地(或者此外也)设置在智能卡100'的后侧。指纹传感器102可以例如用于在执行支付/交易时认证用户,例如,一旦用户的手指已经被登记,就允许智能卡100'与例如POS终端进行交互。此外,智能卡100'可以集成多个接触板110,该多个接触板110至少电连接到控制单元108,如果/当智能卡100'被插入到POS终端中设置的卡槽中时,可以允许提供与POS终端的有线连接。

[0045] 另外,在一些实施方式中,智能卡100'还可以包括用户界面,例如与智能卡集成并被布置成与控制单元装置108电连接的光源112(例如,发光二极管、LED)。更进一步,智能卡100'优选地包括用于允许与POS终端的无线交互的装置(未示出),例如适于允许智能卡100'与POS终端之间的近场通信(NFC)。因此,在使用无线通信时,用户不需要将智能卡100'插入到POS终端的卡槽中。智能卡100'与POS终端之间的NFC连接还可以以技术人员已知的方式向智能卡100'提供电力。

[0046] 控制单元装置108优选地被布置成与诸如数据库的存储器通信或者包括存储器,例如用于存储针对用户的一个或多个手指的一个或多个指纹模板。控制单元装置108可以包括一个或多个微处理器、微控制器、可编程数字信号处理器或其他可编程器件。控制单元装置108还可以或者替选地包括一个或多个专用集成电路、可编程门阵列或可编程阵列逻辑、可编程逻辑器件或数字信号处理器。

[0047] 在控制单元装置108包括如上所述的诸如微处理器、微控制器或可编程数字信号处理器的可编程器件的情况下,处理器还可以包括控制可编程器件的操作的计算机可执行代码。应当理解,借助于控制单元装置108而提供的功能中的全部或一些部分可以至少部分地与指纹传感器102集成。关于本公开内容,在第一控制单元302、第二控制单元304和第三控制单元306之间部分地划分由控制单元装置108执行的处理,将在下面关于图3进一步详尽阐述。

[0048] 进一步参照图2,概念性地示出了指纹传感器102的稍微放大的视图。在采用电容式感测技术的情况下,指纹传感器102被配置成包括大量的感测特征,优选地被布置为二维阵列。二维阵列的尺寸可以取决于所计划的实现方式,并且在实施方式中使用 160×160 像素。其他尺寸当然是可能的,并且在本公开内容的范围内,包括与上述示例相比具有更少像素的二维阵列。在图2中通过附图标记202指出单个感测元件(也表示为像素)。然而,如上所示,应当理解,本公开内容还可以应用于其他类型的指纹感测技术,例如光学感测技术、或热感测技术、以及其组合。一维传感器和二维传感器两者都是可能的,并且在本公开内容的范围内。

[0049] 现在转到图3A并结合图4和图5,概念性地示出了根据本公开内容所提供的概念的概括化的可能实现。图3A所示的示例通常可以应用于如图1A和图1B所示的电子设备100、100'的示例两者,例如可应用于移动电话和智能卡示例两者。

[0050] 如上所示,电子设备100、100'所提供的控制单元装置108分别包括第一控制单元302、第二控制单元304和第三控制单元306。根据本公开内容,第一控制单元302被布置成与指纹传感器102通信。第一控制单元302和第三控制单元306中的至少一个可以包括安全元件。

[0051] 根据本公开内容,第二控制单元304被布置成与第一控制单元302和第三控制单元306通信。根据本公开内容,第一控制单元302被布置成提供至少与第二控制单元304相比具有更高安全水平的处理环境。同样,在典型实施方式中,第三控制单元被布置成至少与第二控制单元304相比具有更高的安全水平。第三控制单元306进而被布置成与存储元件308通信或包括存储元件308,例如包括适于存储(待认证的)用户手指的先前登记的表示(或指纹模板)的数据库。根据本公开内容,期望的是仅允许使用第三控制单元306访问存储元件308。

[0052] 在电子设备100、100'的操作期间,并且与图3中提供的图示一致地,第一控制单元302被布置成在与指纹传感器102协作的情况下,一旦用户的手指被布置在指纹传感器102附近或与指纹传感器接触,则获取用户手指的指纹图像。

[0053] 基于指纹图像,第一控制单元302确定指示用户的指纹图案的第一特性特征集存在于所获取的指纹图像内。用于提取特性指纹特征的不同技术是可能的,并且在本公开内容的范围内。

[0054] 第一控制单元302随后形成第一特征集的受保护表示。借助于形成第一特征集的受保护表示,可以确保第一特征集的完整性。第一特征集的这种完整性还可以包括确保第一特征集的新鲜度,这意味着第一特征集的(相比较而言)“旧”版本实际中不能用于认证用户。也就是说,在例如黑客打算利用第一特征集的旧版本的情况下,他不会成功,因为第一特征集(借助于完整性保护)可以适于例如包括时间戳(或类似物),可以在认证步骤中验证该时间戳(或类似物)(如下面将进一步讨论的)。

[0055] 如图4所示,例如可以使用质询-响应过程来确保完整性。在这种实施方式中,假设在控制单元302、304、306之间的实际数据传输之前已经进行了预配置。例如,预先共享的对称密钥K可以安全地存储在传感器/第一控制单元302中和第三控制单元306处。另外,在这样的实施方式中,第三控制单元306优选地适于将用户的至少一对注册模板安全地存储在相关的存储元件308中,即: T_{vh} 、 T_{vl} 。

[0056] 关于图4,使用下列符号:

[0057] 终端用户高分辨率生物计量图像: I_h

[0058] 终端用户低分辨率生物计量图像: I_l

[0059] 生物计量高分辨率验证模板: T_{vh}

[0060] 生物计量低分辨率验证模板: T_{vl}

[0061] 生物计量高分辨率识别模板: T_{IDh}

[0062] 生物计量低分辨率识别模板: T_{IDl}

[0063] (在传感器与高度受保护的系统之间) 共享的对称完整性保护密钥: K

[0064] 消息认证,以对称密钥 K 和消息 m 为输入: $a = \text{MAC}(K, m)$, 以及

[0065] 两个二进制参数的级联: $||$

[0066] 然后,第一特征集的受保护表示和指纹图像将被提供给第二控制单元304。在本公开内容的实施方式中,第二控制单元304可以例如由电子设备100、100' 所包括的“通用”控制单元来表明,例如用于移动电话100的总体处理和控制(例如处理呼叫、显示器等)的公共处理器。

[0067] 然后,第二控制单元304确定表示指纹图像的第二特征集。与第一特征集相比,第二特征集通常包括“更多信息”。即,由于第一控制单元302与第二控制单元304相比通常具有较少的计算能力,因此根据本公开内容期望的是,例如,调整特征确定过程以便与第二控制单元304相比对于第一控制单元302是不同的。因此,在本公开内容的实施方式中,第一控制单元302可以例如适于仅处理指纹图像的子部分,以用于确定第一特征集。相反地,第二控制单元304然后可以适于基于(基本上)所有获取的指纹图像来形成第二特征集。

[0068] 第二控制单元304然后向第三控制单元306提供第一特征集的受保护表示和第二特征集。第三控制单元306随后从第一特征集的受保护表示中提取第一特征集,从而形成第一特征集的提取表示。因此,第一控制单元302和第三控制单元306可以例如采用对称或非对称密码学方案中的至少一个,以确保第一特征集的完整性。因此,一旦在第三控制单元306处提取,所选的密码学方案就可以用于确保第一特征集是“新鲜的”(例如,基于所提及的时间戳或类似物),并且确保在从第一控制单元302中继到第三控制单元306(即,“经过”第二控制单元304)时第一特征集是“未触及的”。

[0069] 然后,第三控制单元306认证用户。与本公开内容一致地,该认证优选地被实现为“双重匹配”,这意味着仅在第一特征集和第二特征集两者都与存储在存储元件308处的先前登记的指纹模板正确匹配的情况下,用户才被认证。在本公开内容的实施方式中,例如,可以允许存储元件308存储与第一特征集的提取表示的结构相对应的第一指纹模板部分(T_{vl})以及与第二特征集的结构相对应的第二生物计量模板部分(T_{vh})两者。这样,可以执行两个单独的匹配过程,其中,只有在两个匹配过程都成功的情况下用户才被认证。另外,与上述新鲜度一致地,时间戳信息可以附加地用作认证过程的组件。

[0070] 在存在“双重匹配”的情况下,第三控制单元306可以输出认证信号。认证信号随后可以用于例如解锁移动电话100或智能卡100'。

[0071] 在本公开内容的范围内,应当理解,第三控制单元306不一定必须被布置为与电子设备集成的部件。相反,如图3B中所例示的,第三控制单元306可以与电子设备306分开地(例如,远程地)布置。例如,在一个实施方式中,第三控制单元306可以是布置成(例如使

用网络通信310)与第二控制单元304通信的服务器。在这样的实施方式中,图4中例示的消息图也可以适应于与这样的实现方式对应。

[0072] 本公开内容的控制功能可以使用现有的计算机处理器来实现,或由针对此目的或其它目的而结合的适当系统的专用计算机处理器来实现,或由硬线系统来实现。在本公开内容的范围内的实施方式包括程序产品,该程序产品包括机器可读介质,该机器可读介质用于承载或在其上存储机器可执行指令或数据结构。这样的机器可读介质可以是能够被通用或专用计算机或具有处理器的其他机器访问的任何可用的介质。例如,这样的机器可读介质可以包括RAM、ROM、EPROM、EEPROM、CD-ROM或其他光盘存储器、磁盘存储器或其他磁存储设备、或者任何其他介质,该任何其他介质可以用于承载或者存储以机器可执行指令或者数据结构的形式的期望的程序代码并且能够被通用计算机或专用计算机或者具有处理器的其他机器访问。当信息通过网络或其他通信连接(硬线、无线、或者硬线或无线的组合)被传送或提供给机器时,机器适当地将该连接视为机器可读介质。因此,任何这样的连接被适当地称为机器可读介质。以上的组合也包括在机器可读介质的范围内。机器可执行指令包括例如使通用计算机、专用计算机或专用处理机器来执行特定功能或功能组的指令和数据。

[0073] 尽管附图可能示出了顺序,但是步骤的顺序可以与所描绘的顺序不同。同样,两个或更多个步骤可以同时执行,也可以部分并发执行。这样的变型将取决于选取的软件系统和硬件系统以及设计者的选择。所有这样的变型都在本公开内容的范围内。同样,软件实现可以通过标准编程技术来实现,该标准编程技术具有基于规则的逻辑及其他逻辑,以实现各种连接步骤、处理步骤、比较步骤及决定步骤。附加地,即使已经参照本公开内容的具体示例性实施方式描述了本公开内容,但是对于本领域技术人员而言,许多不同的变更、修改等将变得明显。

[0074] 另外,根据附图、公开内容和所附权利要求书的研究,本领域技术人员在实践所要求保护的本公开内容时可以理解并实现对所公开的实施方式的变型。此外,在权利要求书中,词语“包括”不排除其他元件或步骤,并且不定冠词“一”或“一个”不排除多个。

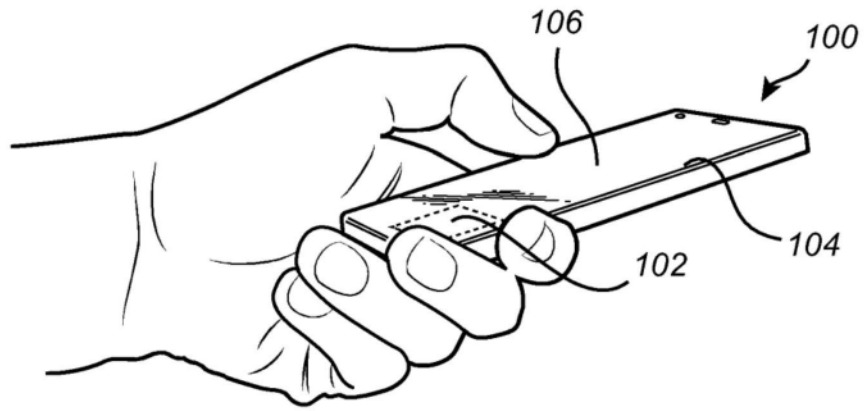


图1A

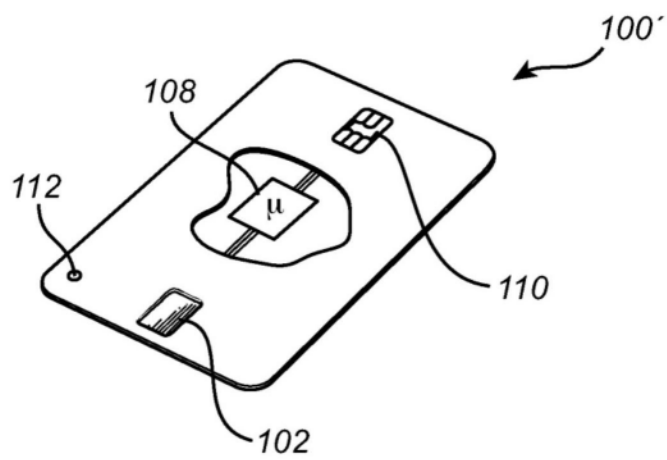


图1B

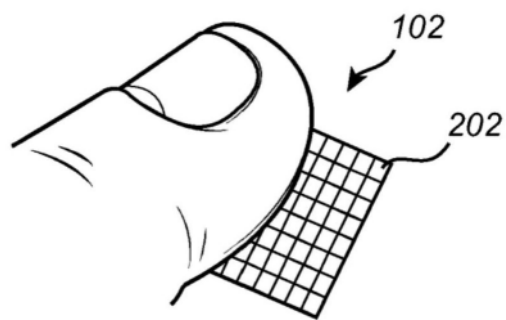


图2

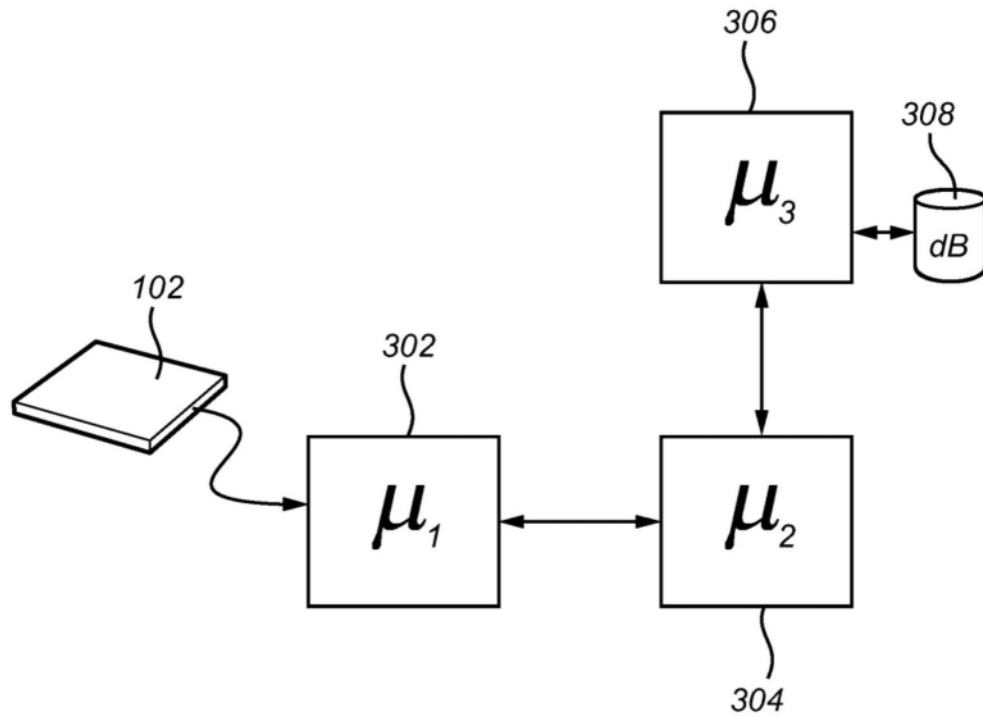


图3A

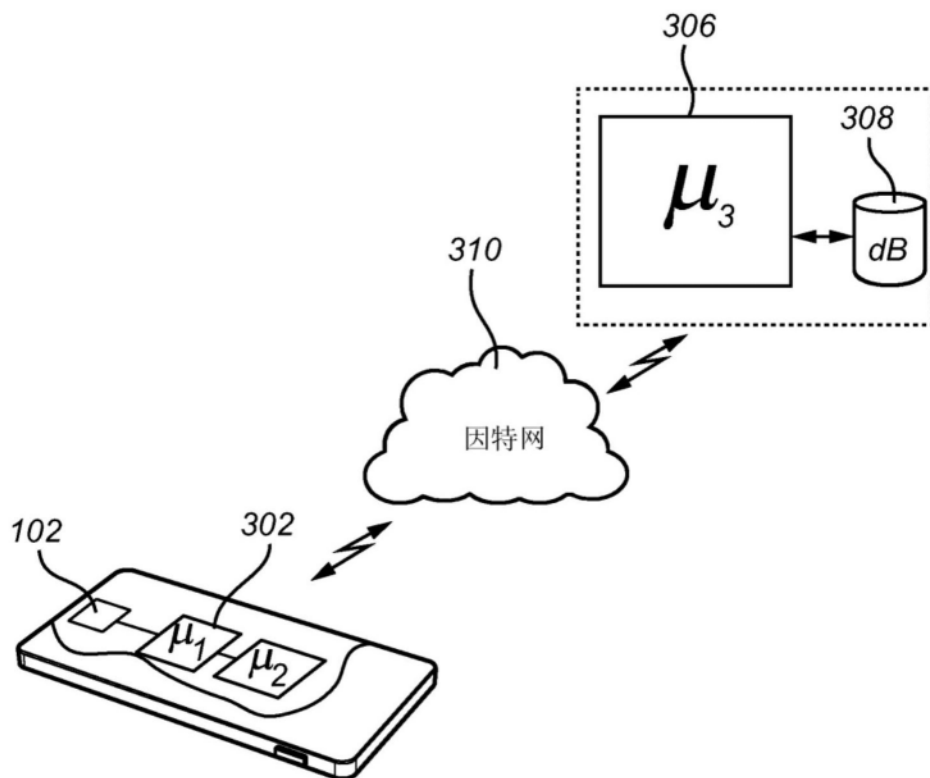


图3B

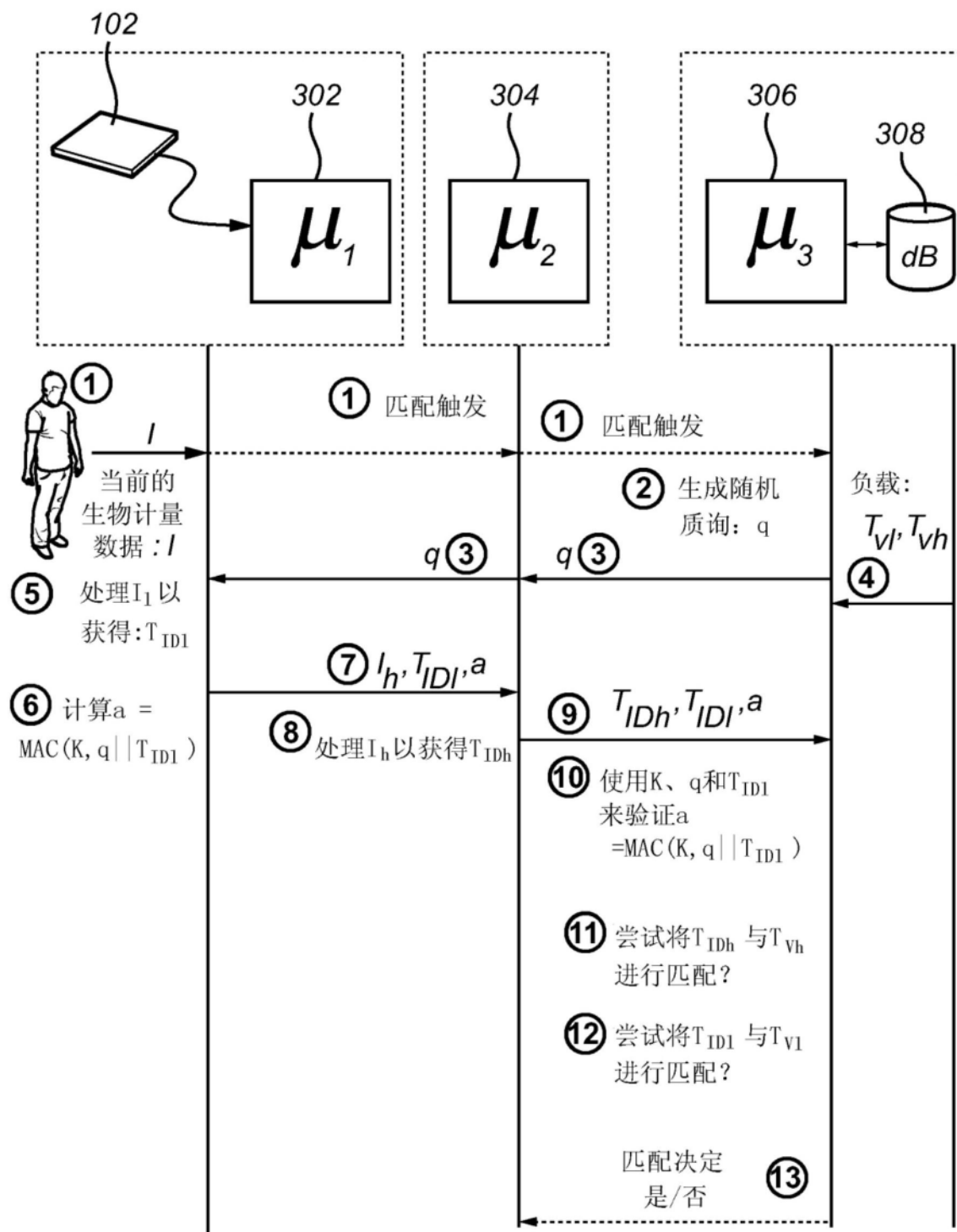


图4

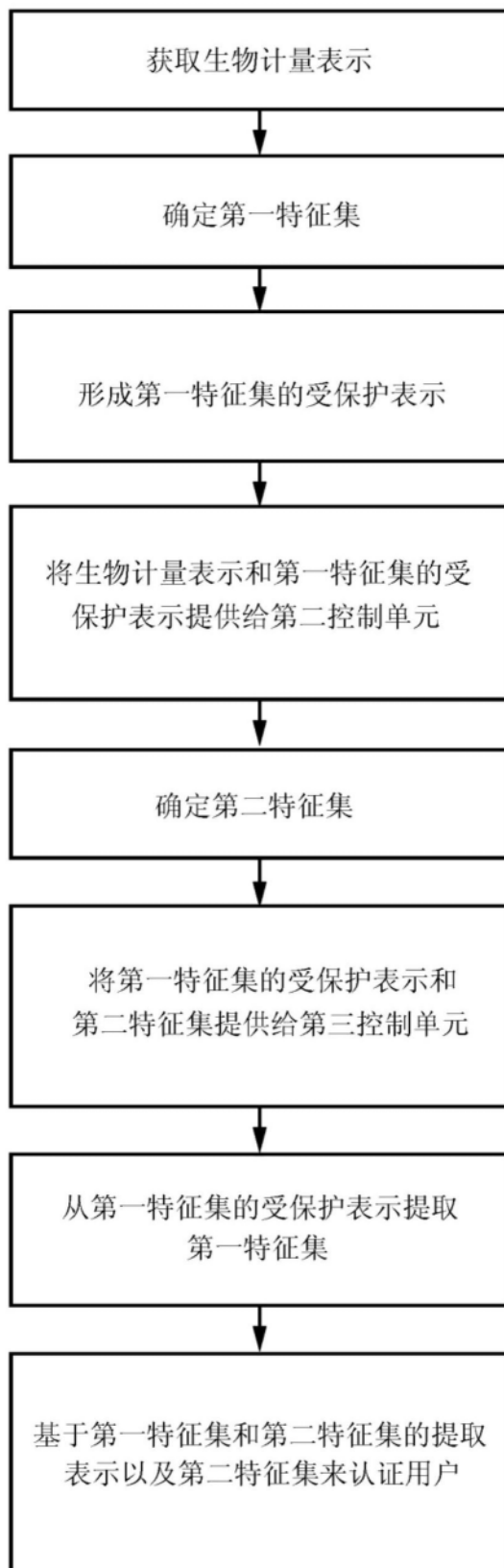


图5