(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110651268 B
(45)授权公告日 2023.10.17

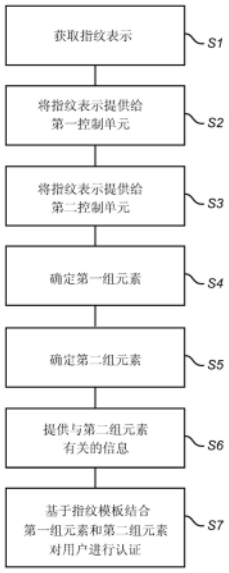
(21)申请号 201880032925.0
(22)申请日 2018.05.23
(65)同一申请的已公布的文献号
申请公布号 CN 110651268 A
(43)申请公布日 2020.01.03
(30)优先权数据
1750644-5 2017.05.23 SE
(85)PCT国际申请进入国家阶段日
2019.11.18
(86)PCT国际申请的申请数据
PCT/SE2018/050521 2018.05.23
(87)PCT国际申请的公布数据
WO2018/217157 EN 2018.11.29
(73)专利权人 指纹卡安娜卡敦知识产权有限公司
地址 瑞典哥德堡
(72)发明人 汉斯·特恩布卢姆
埃里克·塞特贝里
拉尔斯·普高·博吉尔德·克里斯藤森
瑟伦·斯科夫高克里斯滕森
安德斯·O·涅尔森
(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 40/12(2022.01)
(56)对比文件
CN 105138884 A,2015.12.09
CN 105447371 A,2016.03.30
CN 103544599 A,2014.01.29
CN 105900101 A,2016.08.24
US 2013308838 A1,2013.11.21
US 2016048840 A1,2016.02.18
EP 3037998 A1,2016.06.29
US 2014181959 A1,2014.06.26
US 9536131 B1,2017.01.03
CN 105103525 A,2015.11.25
CN 107592933 A,2018.01.16
US 2008212846 A1,2008.09.04
CN 105989490 A,2016.10.05 (续)
审查员 肖倩
权利要求书2页 说明书7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

本公开总体涉及一种使用电子设备认证用户的方法,其中,电子设备包括指纹传感器以及第一控制单元和第二控制单元。优选地,第一控制单元包括适于提供安全处理环境的安全元件和/或安全块。本公开还涉及相应的电子设备和计算机程序产品。



CN 110651268 B

[转续页]

[接上页]

(56)对比文件

CN 101833725 A,2010.09.15

CN 106295285 A,2017.01.04

CN 105354466 A,2016.02.24

CN 106021606 A,2016.10.12

US 2015269409 A1,2015.09.24

芯片安全防护技术助力指纹识别系统安全.中国集成电路.2016,(12),全文.

杨霞 等.基于TrustZone的指纹识别安全技术研究与实现.《计算机科学》.2016,第43卷(第7期),147-152+176.

1.一种使用电子设备认证用户的方法,所述电子设备包括:

-指纹传感器,其被配置成捕获所述用户的手指的指纹图案的指纹表示,

-第一控制单元,其适于提供具有第一安全级别的第一处理环境,其中,所述第一控制单元是安全处理器,所述安全处理器包括安全元件和安全块中的至少一个,以及

-第二控制单元,其适于提供具有第二安全级别的第二处理环境,其中,所述第一安全级别高于所述第二安全级别,其中,与所述第一处理环境相比,所述第二处理环境提供计算量更大的处理环境,

其中,所述方法包括以下步骤:

-使用所述指纹传感器获取指纹表示,

-将所述指纹表示提供给所述第一控制单元,

-将所述指纹表示提供给所述第二控制单元,

-使用所述第一控制单元基于所述指纹表示来确定指示指纹的第一组元素,其中,根据所述指纹表示的子分段确定所述第一组元素,

-在所述第一控制单元处,将所述第一组元素与代表所述用户的所述手指的第一指纹模板进行匹配,

-使用所述第二控制单元基于所述指纹表示来确定指示指纹的第二组元素,

-在所述第二控制单元处,将所述第二组元素与代表所述用户的所述手指的第二指纹模板进行匹配,所述第二指纹模板不同于所述第一指纹模板,

-将来自所述第二控制单元的与所述第二组元素有关的信息提供给所述第一控制单元,

-在所述第一控制单元处,将所述第二控制单元处的匹配结果与所述第一控制单元处的匹配结果进行比较,以及

-在所述第一控制单元处,基于所述第一指纹模板、所述第一组元素以及与所述第二组元素有关的信息来认证所述用户,其中,仅在所述比较的结果表明在所述第一控制单元处的匹配与在所述第二控制单元处的匹配相对应时,认证所述用户。

2.根据权利要求1所述的方法,其中,所述第一控制单元连接到所述指纹传感器,并被配置成控制所述指纹传感器的操作。

3.根据权利要求1所述的方法,其中,所述第二控制单元连接到所述指纹传感器,并被配置成控制所述指纹传感器的操作。

4.根据权利要求1所述的方法,其中,所述方法还包括以下步骤:

-在所述第二控制单元处,基于代表所述用户的所述手指的第二指纹模板以及所述第一组元素和第二组元素来认证所述用户。

5.根据权利要求1所述的方法,其中,将所述指纹表示提供给所述第二控制单元的步骤包括:将所述指纹表示从所述第一控制单元发送到所述第二控制单元。

6.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二控制单元相关联的第二存储元件,其用于存储所述第二指纹模板。

7.根据权利要求5所述的方法,还包括以下步骤:

-在将所述指纹表示发送到所述第二控制单元之前,在所述第一控制单元处对所述指纹表示进行加密,以及

-在所述第二控制单元处，对所加密的指纹表示进行解密。

8.根据权利要求1所述的方法，其中，将在所述第一控制单元处的匹配的结果与在所述第二控制单元处的匹配的结果进行比较的步骤包括：

-将所述第一组元素与所述第二组元素进行比较。

9.根据权利要求1所述的方法，其中，将在所述第一控制单元处的匹配的结果与在所述第二控制单元处的匹配的结果进行比较的步骤包括：

-将所述第一组元素的子部分与所述第二组元素进行比较。

10.一种电子设备，包括：

-指纹传感器，其被配置成捕获用户的手指的指纹图案的指纹表示，

-第一控制单元，其适于提供具有第一安全级别的第一处理环境，其中，所述第一控制单元是安全处理器，所述安全处理器包括安全元件和安全块中的至少一个，以及

-第二控制单元，其适于提供具有第二安全级别的第二处理环境，其中，所述第一安全级别高于所述第二安全级别，其中，与所述第一处理环境相比，所述第二处理环境提供计算量更大的处理环境，

其中，所述电子设备适于：

-使用所述指纹传感器获取指纹表示，

-将所述指纹表示提供给所述第一控制单元，

-将所述指纹表示提供给所述第二控制单元，

-使用所述第一控制单元基于所述指纹表示来确定指示指纹的第一组元素，其中，根据所述指纹表示的子分段确定所述第一组元素，

-在所述第一控制单元处，将所述第一组元素与代表所述用户的所述手指的第一指纹模板进行匹配，

-使用所述第二控制单元基于所述指纹表示来确定指示指纹的第二组元素，

-在所述第二控制单元处，将所述第二组元素与代表所述用户的所述手指的第二指纹模板进行匹配，所述第二指纹模板不同于所述第一指纹模板，

-将来自所述第二控制单元的与所述第二组元素有关的信息提供给所述第一控制单元，

-在所述第一控制单元处，将所述第二控制单元处的匹配结果与所述第一控制单元处的匹配结果进行比较，以及

-在所述第一控制单元处，基于所述第一指纹模板、所述第一组元素以及与所述第二组元素有关的信息来认证所述用户，其中，仅在所述比较的结果表明在所述第一控制单元处的匹配与在所述第二控制单元处的匹配相对应时，认证所述用户。

11.根据权利要求10所述的电子设备，其中，所述电子设备是移动电话、平板计算机、可穿戴电子设备和智能卡中的至少一个。

认证用户的方法和电子设备

技术领域

[0001] 本公开总体上涉及一种使用电子设备认证用户的方法，其中，电子设备包括指纹传感器以及第一控制单元和第二控制单元。优选地，第一控制单元包括适于提供安全处理环境的安全元件和/或安全块。本公开还涉及相应的电子设备和计算机程序产品。

背景技术

[0002] 越来越多地使用生物特征技术来识别和/或认证用户的身份。为此用途而推广的生物特征技术包括语音、指纹、虹膜、静脉图案以及其它扫描。当前，使用指纹传感器来捕获指纹已经显示出是特别有前途的，例如因为其易于与不同类型的电子设备(例如智能电话、手表、平板计算机、或个性化用户交互在其中是有益的任何其它类型的电子设备)集成。此外，已经建议将这种指纹传感器与智能卡系统集成，可能消除用户在进行例如金融交易时输入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“不合适的人手中”和/或遭受例如黑客攻击的风险，黑客攻击的目的是伪造或以其它方式影响生物特征识别和/或认证过程。

[0004] 为了对抗这种企图，继续尝试改进所应用的生物特征识别和/或认证过程。但是，这种尝试通常导致复杂的计算处理，从而增加了为电子设备配备更快、计算能力更强的处理环境的需求。

[0005] 在上述类型的电子设备的一些实现中，需要高安全性和计算能力强的处理环境，建议将计算性能“拆分”为两个部分，第一部分是高性能环境，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，但是安全性较低。相应地，例如包括所谓的安全元件的高安全性环境通常具有较高的安全性，但是计算性能较低。

[0006] 在US9536131中公开了这种实现的示例。US9536131提供了一种有趣的方法，用于在第一处理单元和第二处理单元之间划分执行指纹认证所需的计算资源，第一处理单元提供上述高性能环境，而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在所获取的用户的指纹图像和要认证的用户手指的预先记录的指纹模板之间执行比较处理。

[0007] 遗憾的是，US9536131中提出的解决方案通过如何在第一处理单元和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，本公开的目的是提供一种改进的解决方案，其中降低了根据一些现有技术而引入的风险。特别地，本发明人发现在不安全的处理环境中执行匹配是不合适的，因而提供了仍然在高性能环境和高安全性环境之间以合适的方式平衡计算处理的解决方案。

[0009] 因此，根据本公开的一方面，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:指纹传感器,其被配置成捕获用户的手指的指纹图案的指纹表示;第一控制单元,其适于提供具有第一安全级别的处理环境;以及第二控制单元,其适于提供具有第二安全级别的处理环境;其中,第一安全级别高于第二安全级别;其中,该方法包括以下步骤:使用指纹传感器获取指纹表示;将指纹表示提供给第一控制单元;将指纹表示提供给第二控制单元;使用第一控制单元基于指纹表示来确定指示指纹的第一组元素;使用第二控制单元基于指纹表示来确定指示指纹的第二组元素;将与第二组元素有关的信息提供给第一控制单元;以及在第一控制单元处,基于代表用户手指的第一指纹模板、第一组元素以及与第二组元素有关的信息来认证用户。

[0010] 本公开背后的主要思想在于对指纹认证处理的改进的划分,其中,指纹认证处理的一些部分由第一控制单元执行,指纹认证处理的其它一些部分由第二控制单元执行。根据本公开,第一控制单元适于具有比第二安全控制单元更高的安全级别。因此,在优选实施方式中,第二控制单元适于提供比第一控制单元更高的性能环境。另外,在本公开的可能的实施方式中,第一控制单元是安全处理器,其包括安全元件和/或包括适于提供安全处理环境的安全块。

[0011] 与现有技术相比,本公开允许修改指纹认证处理,其中用于用户手指的主指纹模板(根据本公开的定义的第一指纹模板)永远不会离开由第一控制单元提供的安全处理环境。因此,由于不允许对主/第一指纹模板的外部访问,因此例如第三方将不可能影响所获取的指纹图像与主/第一指纹模板之间的比较。相反,本公开的第一实施方式中的较不安全的第二控制单元仅用于根据所获取的指纹图像确定指示指纹的(第二)组元素。

[0012] 由于在典型实施方式中第二控制单元(如上所述)适于提供比第一控制单元所提供的性能更高的性能环境,因此与根据获取的指纹图像确定第一组元素时第一控制单元可执行的操作相比,可以允许第二组元素的确定相比之下“计算繁重”。

[0013] 根据本公开,因此,由第一控制单元基于第一/主指纹模板,结合根据获取的指纹图像而确定的第一组元素和第二组元素(可能包括第一组元素和第一指纹模板之间的匹配)来执行用户的认证。因此,不仅主/第一指纹模板不被“允许离开”由第一控制单元提供的安全处理环境,而且可以对照使用安全的第一控制单元所确定的第一组元素来“双重检查”使用第二控制单元所确定的第二组元素。在实施方式中,第一存储元件与第一控制单元相关联,其中第一存储元件适于存储第一指纹模板。

[0014] 因此,通过本公开,可以允许实施具有高计算要求的高级认证过程,同时仍确保与现有技术相比,认证过程具有高安全性和较少的黑客攻击成功的风险。除上述内容外,当然应该理解,认证过程的一般划分在电子设备的实现中也可能非常有用,其中,由于成本和/或不动产原因(例如,与智能卡实现有关)而限制了安全处理能力。

[0015] 在本公开的上下文中,应该宽泛地解释表述“用户的手指的指纹图案的表示”或“指纹图像”,并且包括使用手指传感器获取的手指的指纹的常规“可视图像”以及与手指有关的一组测量值。随后可以获取多个指纹表示/图像并将其融合在一起,其中将所得的信息用作用于确定特征组的输入。

[0016] 同样,表述“控制单元”应理解为包括任何类型的计算设备,例如ASIC、微处理器等。还应该理解,这种控制单元的实际实现可在多于一个的元件/设备/电路之间划分,统称为控制单元。优选地,第二控制单元与第一控制单元分开布置。

[0017] 可以使用任何种类的目前或将来的指纹感测原理来实现指纹传感器，包括例如电容、光或热感测技术及其组合。一维传感器和二维传感器都是可能的并且在本公开的范围内。

[0018] 在用户被成功认证的情况下，根据本公开，可以执行至少一个动作。例如，这样的动作可以是电子设备允许用户使用该电子设备执行进一步操作，例如当该电子设备是移动电话或平板计算机时。至少一个动作当然可以是在需要认证手指的情况下适当使用的任何类型的动作，例如在电子设备例如是智能卡的情况下允许进行金融交易。在成功认证的情况下，还可以基于确定的第一组元素和确定的第二组元素中的至少一个来至少更新第一指纹模板。

[0019] 在本公开的一个示例性实施方式中，第一控制单元连接到指纹传感器并被配置成控制指纹传感器的操作。关于电子设备是所提及的移动电话/平板计算机、膝上型计算机等的情况，这样的实现方式可能是有用的。在替选的示例性实施方式中，第二控制单元连接到指纹传感器并被配置成控制指纹传感器的操作。相应地，关于智能卡实现方式等，这样的实现方式可能是有用的。根据所选择的实现方式，指纹表示可以通过适于控制指纹传感器的操作的控制单元“传递”或“传输”。在一些实施方式中，在第一控制单元和第二控制单元之间的任何数据的传输可以包括在发送/接收数据之前/之后对数据进行加密/解密。

[0020] 在本公开的一些实施方式中，可能还可以包括在第二控制单元处，基于代表用户的手指的第二指纹模板以及第一组元素和第二组元素(可能包括第二组元素和第二指纹模板之间的匹配)来认证用户。在一些实现中，这样的实施方式可以允许电子设备的更进一步的安全性。然而，由于与较不安全的第二控制单元相关地提供第二指纹模板，因此希望允许第二指纹模板与主/第一指纹模板完全分离。以如上所述的类似方式，可以包括与第二控制单元相关联的第二存储元件，其中第二存储元件适于存储第二指纹模板。

[0021] 在本公开的可能的实施方式中，该方法包括在第一控制单元处将确定的第一组元素与第一指纹模板进行匹配，以及在第二控制单元处将确定的第二组元素与代表用户手指的第二指纹模板进行匹配，其中，认证用户的步骤还包括：在第一控制单元处比较第二控制单元处的匹配结果和第一控制单元处的匹配结果；以及仅当比较结果指示第一控制单元处的匹配与第二控制单元处的匹配相对应时，才在第一控制单元处认证用户。因此，可以执行两个分开的并且可能不相关的匹配过程；然后比较匹配过程的结果，从而在认证过程中实现附加的安全性。

[0022] 基于第一控制单元与第二控制单元相比在计算角度上稍微“较弱”这一事实，在一些实施方式中根据指纹表示的子分段来确定第一组元素可能是有益的。根据本公开，子分段可以被视为包括例如裁剪、抽取或截短处理，以用于减少将要处理的数据量。因此，减少的信息量被处理以确定第一组元素，从而可以平衡第一控制单元的计算能力。

[0023] 在一个实施方式中，还可以允许在第二控制单元处执行的处理形成/生成要提供给第一控制单元的帮助/协助数据。帮助/协助数据随后可以用于协助第一控制单元进行由第一控制单元执行的处理，例如，包括由第一控制单元执行的匹配处理，使得可以以较少的计算复杂度来执行由第一控制单元执行的处理。帮助/协助数据可以例如包括在第二控制单元处执行的匹配处理期间生成的指纹特征变换信息等。

[0024] 在可能的实施方式中，由第一控制单元选择指纹表示的子分段。与主/第一指纹模

板相比，这样的实现再次不允许任何第三方参与选择进一步使用哪些信息。可能优选的是，允许这种选择至少部分是随机的，或者对于不同的指纹表示至少是不同的(例如对于用户手指的连续认证是不同的)。

[0025] 根据本公开的另一方面，提供一种电子设备，包括：指纹传感器，其被配置成捕获用户的手指的指纹图案的指纹表示；第一控制单元，其适于提供具有第一安全级别的处理环境；以及第二控制单元，其适于提供具有第二安全级别的处理环境，其中，第一安全级别高于第二安全级别；以及电子设备，其适于使用指纹传感器来获取指纹表示；将指纹表示提供给第一控制单元；将指纹表示提供给第二控制单元；使用第一控制单元基于指纹表示来确定指示指纹的第一组元素；使用第二控制单元基于指纹表示来确定指示指纹的第二组元素；将与第二组元素有关的信息提供给第一控制单元；以及在第一控制单元处，基于代表用户手指的第一指纹模板、第一组元素以及与第二组元素有关的信息来认证用户。本公开的这一方面提供了与以上关于本公开的先前方面所讨论的类似优点。

[0026] 根据本公开的另一方面，提供了一种计算机程序产品，其包括计算机可读介质，该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，该电子设备包括：指纹传感器，其被配置成捕获用户的手指的指纹图案的指纹表示；第一控制单元，其适于提供具有第一安全级别的处理环境；第二控制单元，其适于提供具有第二安全级别的处理环境，其中第一安全级别高于第二安全级别；以及计算机程序产品包括：用于使用指纹传感器获取指纹表示的代码；用于将指纹表示提供给第一控制单元的代码；用于将指纹表示提供给第二控制单元的代码；用于使用第一控制单元基于指纹表示来确定指示指纹的第一组元素的代码；用于使用第二控制单元基于指纹表示来确定指示指纹的第二组元素的代码；用于将与第二组元素有关的信息提供给第一控制单元的代码；以及用于在第一控制单元处基于代表用户手指的第一指纹模板、第一组元素以及与第二组元素有关的信息来认证用户的代码。同样，本公开的这个方面提供了与以上关于本公开的先前方面所讨论的类似优点。

[0027] 总之，本公开总体上涉及一种使用电子设备认证用户的方法，其中，电子设备包括指纹传感器以及第一控制单元和第二控制单元。第一控制单元和第二控制单元中的至少一个包括适于提供安全处理环境的安全元件和/或安全块。与现有技术相比，本公开的优点包括允许实现具有高计算要求的高级认证过程，同时仍确保与现有技术相比，认证过程具有高安全性以及较少的黑客攻击成功的风险。

[0028] 当研究所附权利要求和以下描述时，本公开的其它特征和优点将变得明显。本领域技术人员认识到，在不脱离本公开的范围的情况下，可以对本公开的不同特征进行组合以创建不同于以下描述的实施方式。

附图说明

[0029] 从以下详细描述和附图，将容易理解本公开的各个方面，包括其特定的特征和优点，其中：

[0030] 图1A和图1B以包括集成指纹传感器的移动电话和智能卡的形式示意性地示例了根据本公开的不同电子设备。

[0031] 图2示意性地示出了图1的电子设备中包括的指纹传感器阵列。

[0032] 图3A至图3C概念性地示出了根据本公开的当前优选实施方式的电子设备的不同

实现,以及

[0033] 图4是公开了结合图3A和图3B中的任何电子设备通常执行的本公开的示例性步骤的流程图。

具体实施方式

[0034] 现在将在下文中参考附图更全面地描述本公开,在附图中示出了本公开的当前优选实施方式。然而,本公开可以以许多不同的形式来体现,并且不应被解释为限于这里提出的实施方式;相反,提供这些实施方式是为了详尽和完整,并且将本公开的范围完全传达给技术人员。贯穿全文相同的附图标记表示相同的元件。

[0035] 现在转向附图,特别是图1A,以具有集成指纹传感器102的移动电话100和具有触摸屏界面106的显示单元104的形式示意性地示出了根据本公开的电子设备的第一示例。在该实施方式中,指纹传感器102和显示单元104一起布置在移动电话100的前侧。指纹传感器102可以例如用于解锁移动电话100和/或用于授权使用移动电话100执行的业务等。指纹传感器102也可以放置在移动电话100的背侧。

[0036] 优选地且对于本领域技术人员而言明显的是,图1所示的移动电话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、扬声器和电话控制单元。当然,移动电话可能还包含其它硬件元件。还应该注意的是,本公开可以适用于任何其它类型的便携式电子设备,例如膝上型计算机、遥控器、平板计算机或任何其它类型的目前或将来的类似配置的设备。

[0037] 在图1B中,示出了以智能卡100'的形式的根据本公开的电子设备的第二示例,其集成了指纹感测系统,该指纹感测系统例如包括相应的指纹传感器102以及至少一个控制单元装置108,该指纹传感器102包括多个感测元件并且被配置成捕获用户手指的指纹图案的指纹表示,该至少一个控制单元装置108连接到指纹传感器102并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被布置在智能卡100'的前侧。然而,指纹传感器102可以替选地(或者也可以)设置在智能卡100'的背侧。指纹传感器102可以例如在执行支付/交易时用于认证用户,例如,一旦用户手指已经登记就允许智能卡100'与例如POS终端进行交互。此外,智能卡100'可以集成至少电连接到控制单元108的多个触点焊盘110,如果/当智能卡100'插入到设置有POS终端302的卡槽中时,可能允许提供与POS终端的有线连接。

[0038] 另外,在一些实施方式中,智能卡100'还可包括用户接口,例如与智能卡载体100集成在一起并布置成与控制单元108电连接的光源112(例如,发光二极管,LED)。再进一步,智能卡100'优选地包括用于允许与POS终端进行无线交互的装置(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)的装置。因此,在使用无线通信时,用户不需要将智能卡100'插入POS终端的卡槽中。智能卡100'和POS终端之间的NFC连接可以进一步以本领域技术人员已知的方式向智能卡100'提供电力。

[0039] 控制单元装置108优选地被布置成与诸如数据库等的存储器通信,或者包括诸如数据库等的存储器,该存储器例如用于为用户存储一个或多个手指的一个或多个指纹模板。控制单元装置108可以包括微处理器、微控制器、可编程数字信号处理器或其它可编程器件。控制单元装置108还可以或者替代地包括专用集成电路、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。

[0040] 在控制单元装置108包括可编程器件(例如如上所述的微处理器、微控制器或可编程数字信号处理器)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(或通常称为“处理电路”)提供的功能的全部或某些部分可以至少部分地与指纹传感器102集成在一起。关于本公开,由控制单元装置108执行的处理部分地在至少第一控制单元108A和第二控制单元108B之间进行划分,这将在下面关于图3A至图3C进一步详细说明。

[0041] 进一步参考图2,概念性地示出了指纹传感器102的略微放大图。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元件,优选地布置为二维阵列。二维阵列的尺寸可以取决于所规划的实现,并且在一个实施方式中使用160×160像素。当然,其它尺寸也是可能的,并且在本公开的范围内,包括与上述示例相比具有更少像素的二维阵列。单个感测元件(也表示为像素)在图2中由附图标记202指示。但是,如上所示,应当理解本公开还可以适用于其它类型的指纹感测技术,例如光或热感测技术,以及它们的组合。一维和二维传感器都是可能的并且在本公开的范围内。

[0042] 现在转向图3A并结合图4,在概念上示出了根据本公开提供的概念的广义上可能的实现。图3A所示的示例通常能够适用于图1A和图1B所示的电子设备100、100’两个示例,例如能够适用于移动电话和智能卡示例两者。

[0043] 如上所述,与电子设备100、100’一起提供的控制单元装置108包括第一控制单元108A和第二控制单元108B。第一控制单元108A被配置成具有比第二控制单元108B所提供的安全级别更高的安全级别。如上所述,第一控制单元108A优选地是安全处理器,包括安全元件和/或包括适于提供安全处理环境的安全块。还应当理解,在一些实施方式中,第一控制单元108A和第二控制单元108B之间的通信可以被加密。

[0044] 在图3A中提供的示例中,指纹传感器102可通信地耦接至第一控制单元108A以及第二控制单元108B,从而允许通过指纹传感器102来获取S1用户手指的指纹表示,然后将指纹表示提供S2/S3给第一控制单元108A和第二控制单元108B。应当理解,并非总是需要向第一控制单元108A和第二控制单元108B中的每一个提供“完整”指纹表示(例如完整指纹图像)。相反,例如第一控制单元108A和第二控制单元108B中的任何一个可以“负责”操作指纹传感器,由此在一个实施方式中可以在第一控制单元108A处接收指纹表示并且将其“转发”到第二控制单元108B,如上面所举例的,可以以某种调整的形式(例如可以稍有截短或类似地)来进行。

[0045] 一旦已经将指纹表示提供给第一控制单元108A和第二控制单元108B中的每个,控制单元108A/108B中的每一个将基于指纹表示来确定S4/S5指示指纹的相应的第一组元素和第二组元素。接着,第二控制单元108B将与第二组元素有关的信息提供S6给第一控制单元108A。

[0046] 最后,在第一控制单元108A的安全环境内基于第一组元素、与第二组元素有关的信息(例如,基于第二组元素的信息)以及代表用户手指的第一指纹模板对用户进行认证S7。通常可以将指纹模板存储在电子设备100/100’所包括的数据库302内。

[0047] 图3B和图3C概念性地示出了根据本公开的当前优选实施方式的电子设备100/100’的替选实施方式。具体地,在图3B中,第一控制单元108A连接到指纹传感器102并被配

置成控制指纹传感器102的操作，在图3C中，第二控制单元108B连接到指纹传感器102并被配置成控制指纹传感器102的操作。

[0048] 在图3A至图3C所示的所有实施方式中，在第一控制单元108A和第二控制单元108B中的每一个中执行用于形成要用于认证用户的信息的至少一部分处理。然而，在所有实施方式中，是由提供更安全的处理环境的第一控制单元108A来基于在第一控制单元108A和第二控制单元108B中的每一个中形成的信息执行用户认证的最后步骤。因此，可以将用于形成要用于认证用户的信息的算法细分为不同的部分，其中，例如与第一控制单元108A相比，第二控制单元108B通常提供更高的计算性能，因此第二控制单元108B可以适于执行要用于认证用户的信息的形成的更复杂部分。

[0049] 在根据本公开的可能的实施方式中，由第一控制单元108A执行的部分认证过程包括验证在第二控制单元108B处形成的信息。也就是说，与在第二控制单元108B处所确定的相比，第一控制单元108A例如可以适于仅根据所获取的指纹表示的较小部分来确定第一组元素，例如在指纹表示(指纹图像)内可能随机选择的特定位置。因此，在这样的实施方式中，认证步骤包括将第一组元素和第二组元素进行匹配，意图是应该“找到”作为第二组元素的子部分的第一组元素。如果认为第一组元素基本上是在第二组元素内找到的，则第二组元素可以用于与指纹模板进行比较。可替选地，第一控制单元108A和第二控制单元108B都仅检测/确定一些元素。然后那些重叠的元素可以用于与模板进行比较。这些元素可能包括在可能的模板匹配过程中。

[0050] 本公开的控制功能可以使用现有的计算机处理器来实现，或者通过为此目的或其它目的而并入的用于适当系统的专用计算机处理器来实现，或者通过硬连线系统来实现。本公开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可由通用或专用计算机或具有处理器的其它机器访问的任何可用介质。举例来说，此类机器可读介质可以包括RAM、ROM、EPROM、EEPROM、CD-ROM或其它光盘存储器、磁盘存储器或其它磁性存储设备，或任何其它介质，该任何其它介质可以用于承载或存储机器可执行指令或数据结构的形式的所需程序代码，并且可以由通用或专用计算机或其它带有处理器的机器来访问。当信息通过网络或另一通信连接(硬连线、无线、或硬连线或无线的组合)传输或提供给机器时，机器会将该连接适当地视为机器可读介质。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执行某个功能或一组功能的指令和数据。

[0051] 尽管附图可以示出顺序，但是步骤的顺序可以与所描绘的顺序不同。同样，可以同时或部分同时地执行两个或更多步骤。这种变化将取决于所选择的软件和硬件系统以及设计者的选择。所有这些变化都在本公开的范围内。同样，可以使用具有基于规则的逻辑和其它逻辑的标准编程技术来完成软件实现，以完成各种连接步骤、处理步骤、比较步骤和决策步骤。另外，即使已经参照本公开的特定示例性实施方式描述了本公开，但是对于本领域技术人员而言，许多不同的改变、修改等将变得明显。

[0052] 另外，通过研究附图、本公开内容和所附权利要求书，本领域技术人员在实践所要求保护的本公开时可以理解和实现所公开的实施方式的变型。此外，在权利要求中，词语“包括”不排除其它元件或步骤，并且不定冠词“一”或“一个”不排除多个。

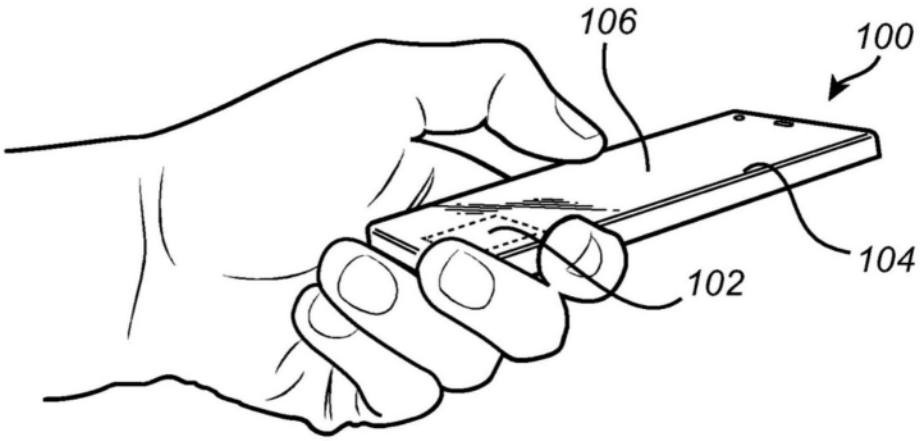


图1A

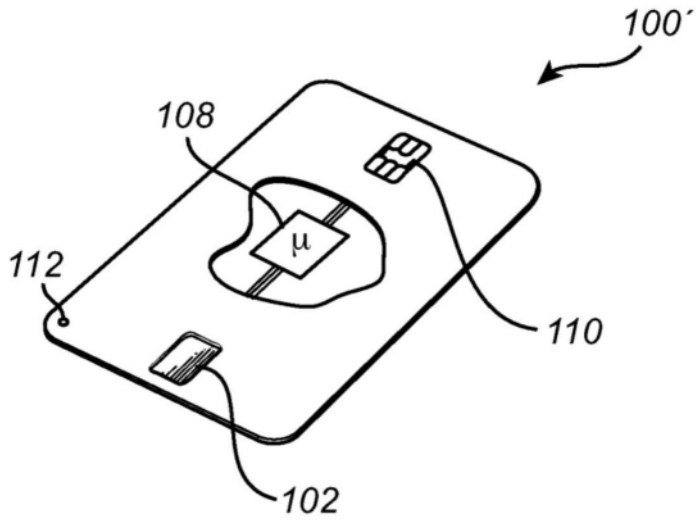


图1B

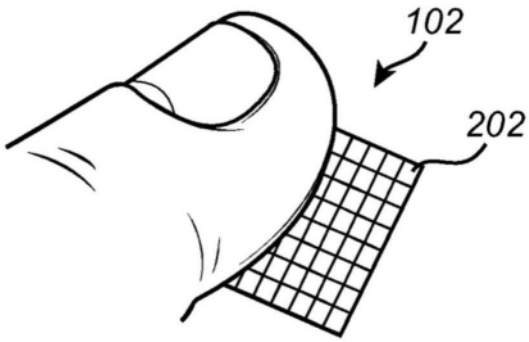


图2

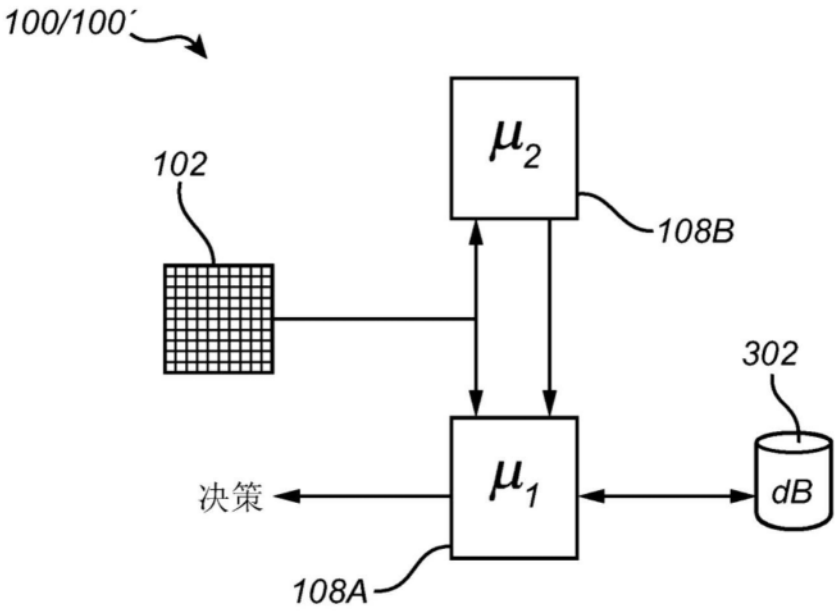

100/100′
102
μ_2
108B
302
μ_1
dB
决策
108A

图3A

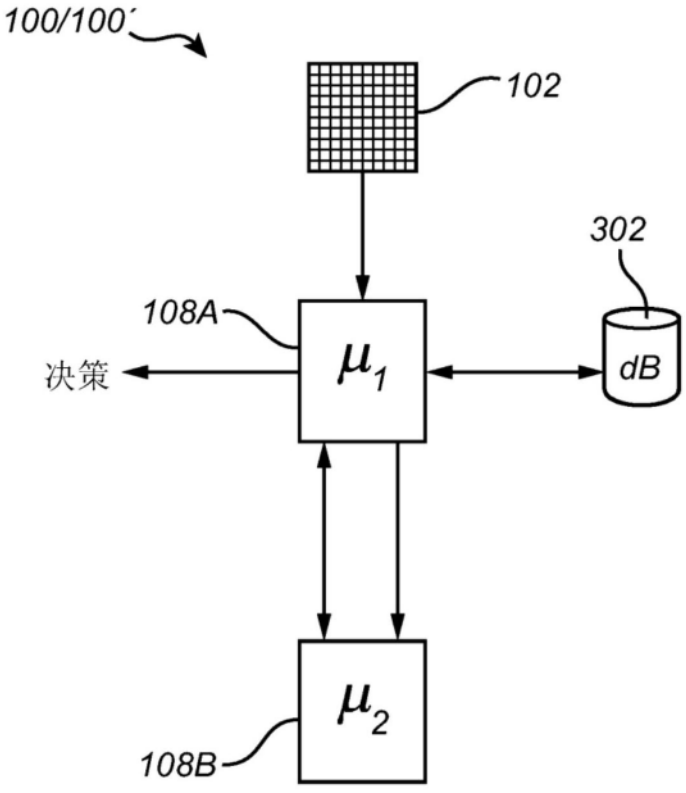

100/100′
102
302
108A
μ_1
dB
决策
μ_2
108B

图3B

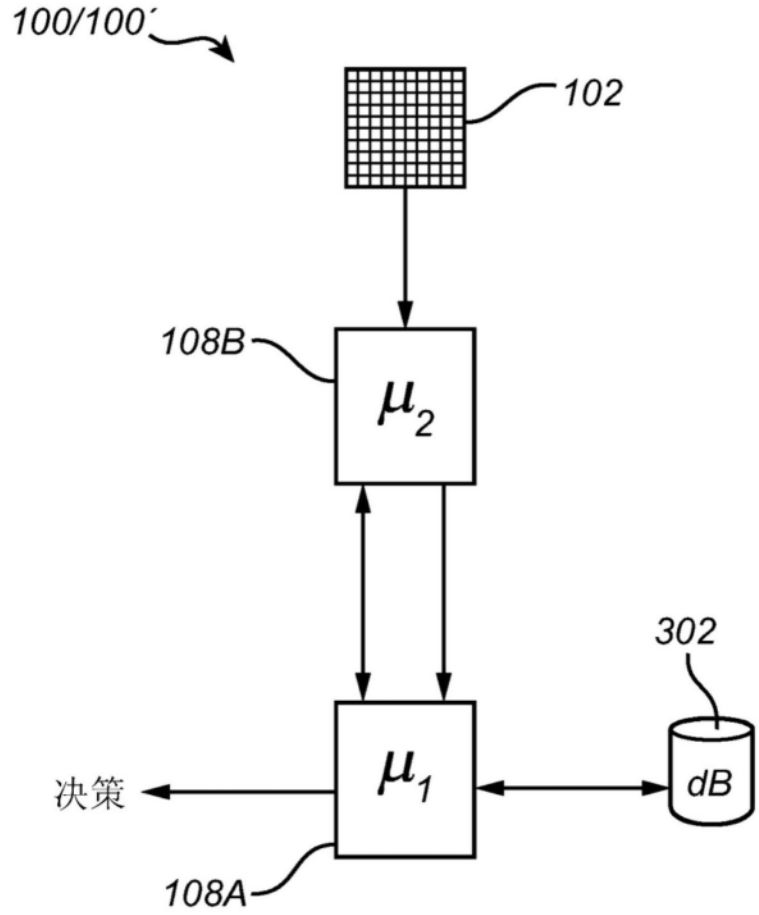


图3C

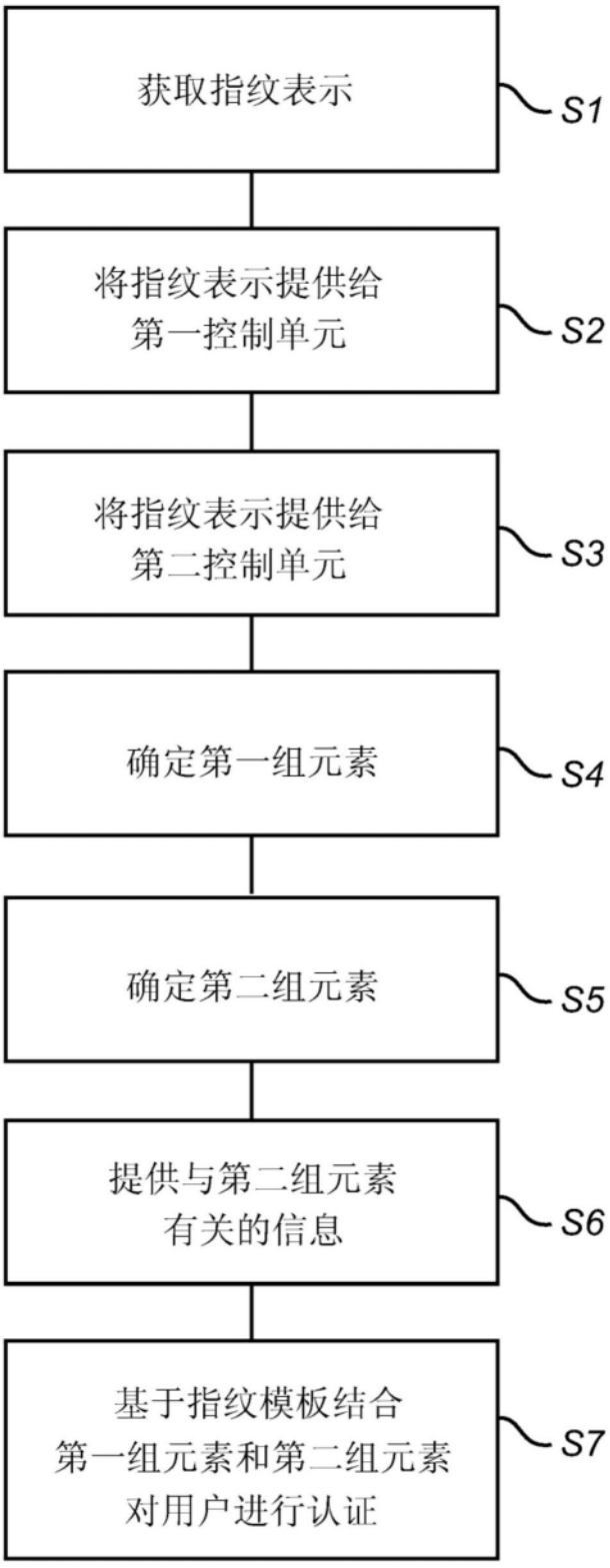

获取指纹表示
S1
将指纹表示提供给
第一控制单元
S2
将指纹表示提供给
第二控制单元
S3
确定第一组元素
S4
确定第二组元素
S5
提供与第二组元素
有关的信息
S6
基于指纹模板结合
第一组元素和第二组元素
对用户进行认证
S7

图4