



(12) 发明专利申请

(10) 申请公布号 CN 112470152 A

(43) 申请公布日 2021. 03. 09

(21) 申请号 201980048229.3

(22) 申请日 2019.07.23

(30) 优先权数据

10-2018-0085619 2018.07.23 KR

(85) PCT国际申请进入国家阶段日

2021.01.19

(86) PCT国际申请的申请数据

PCT/KR2019/009068 2019.07.23

(87) PCT国际申请的公布数据

W02020/022737 EN 2020.01.30

(71) 申请人 三星电子株式会社

地址 韩国京畿道水原市灵通区三星路129号

(72) 发明人 赵原峻 金震晟

(74) 专利代理机构 北京英赛嘉华知识产权代理有限公司 11204

代理人 王达佐 杨莘

(51) Int.Cl.

G06F 21/31 (2006.01)

G06F 21/46 (2006.01)

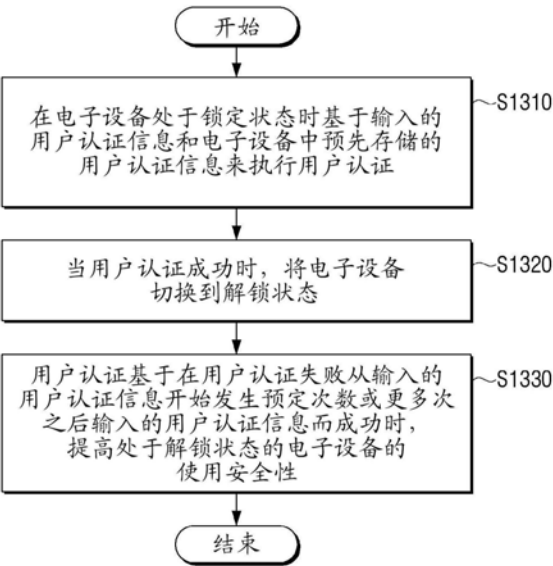
权利要求书2页 说明书19页 附图19页

(54) 发明名称

电子设备及其控制方法

(57) 摘要

提供了一种用于执行用户认证的电子设备。所述电子设备包括输入器和至少一个处理器,所述至少一个处理器被配置为在所述电子设备处于锁定状态时基于通过所述输入器输入的用户认证信息和预先存储在所述电子设备中的用户认证信息来执行用户认证,当所述用户认证成功时将所述电子设备切换到解锁状态,以及当所述用户认证基于用户认证失败从输入用户认证信息输入开始发生预定次数或更多次数之后输入的用户认证信息而成功时,提高处于所述解锁状态下的所述电子设备的使用安全性。



1. 一种电子设备,包括:

输入器;以及

至少一个处理器,其被配置为:

当所述电子设备处于锁定状态时,基于通过所述输入器输入的用户认证信息和预先存储在所述电子设备中的用户认证信息执行用户认证,

当所述用户认证成功时,将所述电子设备切换到解锁状态,以及

当所述用户认证基于用户认证失败从输入用户认证信息输入开始发生预定次数或更多次数之后输入的用户认证信息而成功时,提高处于所述解锁状态下的所述电子设备的使用安全性。

2. 如权利要求1所述的电子设备,其中,所述至少一个处理器还被配置为:当所述用户认证基于所述用户认证失败从输入用户认证信息开始发生所述预定次数或更多次数之后输入的用户认证信息而成功时,执行基于通过所述输入器输入的用户生物信息的用户重新认证。

3. 如权利要求2所述的电子设备,

其中,所述用户认证信息包括预定的图案或密码,以及

其中,所述用户生物信息包括用户指纹或用户虹膜。

4. 如权利要求2所述的电子设备,其中,所述至少一个处理器还被配置为:在所述用户重新认证失败发生的情况下将所述电子设备切换回处于所述锁定状态。

5. 如权利要求2所述的电子设备,其中,所述至少一个处理器还被配置为:在所述电子设备处于所述解锁状态的情况下,当执行预定的应用程序时,执行所述用户重新认证。

6. 如权利要求5所述的电子设备,其中,所述预定的应用程序包括提供需要用户登录的服务的应用程序中的以下应用程序中的至少一个:被设置为执行自动用户登录的应用程序或者存储用户个人信息的应用程序。

7. 如权利要求1所述的电子设备,其中,所述至少一个处理器还被配置为:在所述用户认证失败发生所述预定次数或更多次的情况下,提高在所述锁定状态下的所述电子设备的锁定安全性。

8. 如权利要求7所述的电子设备,其中,所述至少一个处理器还被配置为:

通过所述输入器获取所述用户生物信息,以及

在所述用户认证失败发生所述预定次数或更多次的情况下,在所述用户输入所述用户认证信息以将所述电子设备切换到所述解锁状态的同时,基于输入的所述用户生物信息执行所述用户重新认证。

9. 如权利要求8所述的电子设备,其中,所述至少一个处理器还被配置为:在所述用户重新认证失败发生的情况下保持所述电子设备处于所述锁定状态。

10. 一种电子设备的控制方法,包括:

当所述电子设备处于锁定状态时,基于输入的用户认证信息和预先存储在所述电子设备中的用户认证信息执行用户认证;

当所述用户认证成功时,将所述电子设备切换到解锁状态;以及

当所述用户认证基于用户认证失败从输入用户认证信息输入开始发生预定次数或更多次数之后输入的用户认证信息而成功时,提高处于所述解锁状态下的所述电子设备的使用安全性。

用安全性。

11. 如权利要求10所述的控制方法, 其中, 在提高所述电子设备的使用安全性的过程中, 当所述用户认证基于所述用户认证失败从输入用户认证信息开始发生所述预定次数或更多次数之后输入的用户认证信息而成功时, 执行基于输入的用户生物信息的用户重新认证。

12. 如权利要求11所述的控制方法,

其中, 所述用户认证信息包括预定的图案或密码, 以及

其中, 所述用户生物信息包括用户指纹或用户虹膜。

13. 如权利要求11所述的控制方法, 其中, 在提高所述电子设备的使用安全性的过程中, 当发生用户重新认证失败时, 将所述电子设备切换回所述锁定状态。

14. 如权利要求11所述的控制方法, 其中, 在提高所述电子设备的使用安全性的过程中, 在所述电子设备处于所述解锁状态的情况下, 当执行预定的应用程序时, 执行所述用户重新认证。

15. 如权利要求14所述的控制方法, 其中, 所述预定的应用程序包括提供需要用户登录的服务的应用程序中的以下应用程序中的至少一个: 被设置为执行自动用户登录的应用程序或者存储用户个人信息的应用程序。

电子设备及其控制方法

技术领域

[0001] 本公开涉及一种执行用户认证的电子设备。更具体地，本公开涉及一种电子设备，其中即使用户认证成功，也基于输入的用户认证信息和用户认证失败的数目来执行用户生物认证。

背景技术

[0002] 为了电子设备的安全性，现有技术将电子设备保持在锁定状态，从而防止电子设备执行其功能或执行存储在其中的应用程序。此外，现有技术利用这样一种机制，其中只有在输入特定用户认证时，电子设备才被切换到解锁状态。

[0003] 对于用户认证，通常使用诸如密码输入或图案输入的认证，并且最近，诸如用户指纹认证、虹膜认证、语音认证和面部认证的用户生物认证被更频繁地使用。

[0004] 然而，密码输入或图案输入可以由电子设备的用户以外的人相对容易地解决的认证类型。而用户生物认证对于其他人来说不容易解决，但是认证过程麻烦且耗时。因此，有必要以及时的方式使用这些各种类型的认证。

[0005] 上述信息仅作为背景信息来呈现，以帮助理解本公开。没有作出任何确定，并且没有作出关于上述中的任何一个是否可以作为关于本公开的现有技术适用的断言。

发明内容

[0006] 技术问题

[0007] 本公开的一方面是至少解决上述问题和/或缺点，并至少提供下述优点。因此，本公开的一个方面是提供一种电子设备及其控制方法，其中执行用户认证以仅基于诸如密码输入或图案输入的简单信息输入将电子设备切换到解锁状态。然而，还根据用户认证失败的次数来执行用户生物认证，从而减轻了用户生物认证的不便，并且增强了电子设备的安全性。

[0008] 另外的方面将部分地在随后的描述中阐述，并且部分地将从描述中显而易见，或者可以通过所呈现的实施例的实践来获知。

[0009] 问题的解决方案

[0010] 根据本发明的一个方面，提供了一种电子设备。电子设备包括输入器和至少一个处理器，至少一个处理器被配置为在电子设备处于锁定状态时基于通过输入器输入的用户认证信息和预先存储在电子设备中的用户认证信息来执行用户认证，当用户认证成功时将电子设备切换到解锁状态，以及当用户认证基于用户认证失败从输入用户认证信息输入开始发生预定次数或更多次数之后输入的用户认证信息而成功时，提高处于解锁状态下的电子设备的使用安全性。

[0011] 这里，至少一个处理器还可以被配置为当用户认证基于用户认证失败从输入用户认证信息开始发生预定次数或更多次数之后输入的用户认证信息而成功时，执行基于通过输入器输入的用户生物信息的用户重新认证。

[0012] 在这种情况下,用户认证信息可以包括预定的图案或密码,并且用户生物信息可以包括用户指纹或用户虹膜。

[0013] 此外,至少一个处理器还可配置为在用户重新认证失败发生的情况下将电子设备切换回处于锁定状态。

[0014] 同时,至少一个处理器还可配置为:在电子设备处于解锁状态的情况下,当执行预定的应用程序时,执行用户重新认证。

[0015] 这里,预定的应用程序可以包括提供需要用户登录的服务的应用程序中的以下应用程序中的至少一个:被设置为执行自动用户登录的应用程序或者存储用户个人信息的应用程序。

[0016] 同时,至少一个处理器还可配置为:在用户认证失败发生预定次数或更多次的情况下,提高在锁定状态下的电子设备的锁定安全性。

[0017] 在这种情况下,至少一个处理器还可配置为:通过输入器获取用户生物信息,以及在用户认证失败发生预定次数或更多次的情况下,在用户输入用户认证信息以将电子设备切换到解锁状态的同时,基于输入的用户生物信息执行用户重新认证。

[0018] 这里,至少一个处理器还可配置为:在用户重新认证失败发生的情况下保持电子设备处于锁定状态。

[0019] 根据本公开的另一方面,提供了一种电子设备的控制方法。电子设备的控制方法包括:当电子设备处于锁定状态时,基于输入的用户认证信息和预先存储在电子设备中的用户认证信息执行用户认证;当用户认证成功时,将电子设备切换到解锁状态;以及当用户认证基于用户认证失败从输入用户认证信息开始发生预定次数或更多次数之后输入的用户认证信息而成功时,提高处于解锁状态下的电子设备的使用安全性。

[0020] 在这种情况下,在提高电子设备的使用安全性的过程中,当用户认证基于用户认证失败从输入用户认证信息开始发生预定次数或更多次数之后输入的用户认证信息而成功时,执行基于输入的用户生物信息的用户重新认证。

[0021] 这里,用户认证信息可以包括预定的图案或密码,并且用户生物信息可以包括用户指纹或用户虹膜。

[0022] 此外,在提高电子设备的使用安全性的过程中,当发生用户重新认证失败时,将电子设备切换回锁定状态。

[0023] 同时,在提高电子设备的使用安全性的过程中,在电子设备处于解锁状态的情况下,当执行预定的应用程序时,执行用户重新认证。

[0024] 这里,预定的应用程序包括提供需要用户登录的服务的应用程序中的以下应用程序中的至少一个:被设置为执行自动用户登录的应用程序或者存储用户个人信息的应用程序。

[0025] 同时,控制方法还可以包括在用户认证失败发生预定次数或更多次的情况下提高处于锁定状态下的电子设备的锁定安全性。

[0026] 这里,在提高电子设备的锁定安全性的过程中,可以获得用户生物信息,并且在用户认证失败发生预定次数或更多次的情况下,在用户输入用户认证信息以将电子设备切换到解锁状态的同时,基于输入的用户生物信息执行用户重新认证。

[0027] 在这种情况下,在提高电子设备的锁定的安全性时,当用户重新认证失败时,电子

设备可以保持在锁定状态。

[0028] 通过下面结合附图的详细描述,本公开的其它方面、优点和显著特征对于本领域技术人员将变得显而易见,所述详细描述公开了本公开的多种实施例。

附图说明

[0029] 本公开的某些实施例的上述和/或其它方面、特征和优点将从以下结合附图的描述中变得更加明显,其中:

[0030] 图1a、图1b和图1c是各自示出根据本公开的多个实施例的电子设备的操作的示意性过程的图;

[0031] 图2是示出根据本公开的实施例的电子设备的配置的框图;

[0032] 图3a、图3b和图3c是分别用于解释根据本公开的多个实施例的电子设备基于输入的用户认证信息执行用户认证的示例的图;

[0033] 图4a、图4b和4c是分别用于解释根据本公开的各种实施例的电子设备基于输入的用户认证信息执行用户认证的示例的图;

[0034] 图5a和图5b是分别用于解释其中根据本公开的各种实施例的电子设备隐式地执行用户重新认证的示例的图;

[0035] 图6是用于解释其中根据本公开的实施例的电子设备显式地执行用户重新认证的示例的图;

[0036] 图7a和图7b是分别用于解释根据本公开的各种实施例的电子设备显式地执行用户重新认证的示例的图;

[0037] 图8是用于解释其中根据本公开的实施例的电子设备显式地执行用户重新认证的示例的图;

[0038] 图9a、图9b、图9c和图9d是分别用于解释在用户认证失败发生预定次数或更多次时输入用户认证信息的同时,根据本公开的各种实施例的电子设备隐式或显式地执行用户重新认证的示例的图;

[0039] 图10a和图10b是分别用于解释在用户认证失败发生预定次数或更多次时输入用户认证信息的同时,根据本公开的各个实施例的电子设备隐式或显式地执行用户重新认证的示例的图;

[0040] 图11是用于解释在用户认证失败发生预定次数或更多次时输入用户认证信息的同时,根据本公开的实施例的电子设备隐式或显式地执行用户重新认证的示例的图;

[0041] 图12是示出根据本公开的实施例的电子设备的详细配置的框图;

[0042] 图13是用于解释根据本公开的实施例的电子设备的控制方法的流程图;

[0043] 图14是用于解释根据本公开的实施例的电子设备的控制方法的算法;

[0044] 图15是用于解释根据本公开的实施例的电子设备的控制方法的算法;

[0045] 图16是用于解释根据本公开的实施例的电子设备的控制方法的算法;以及

[0046] 图17是用于解释根据本公开的实施例的电子设备的控制方法的算法。

[0047] 在所有附图中,相同的附图标记将被理解为表示相同的部分、部件和结构。

具体实施方式

[0048] 提供以下参考附图的描述以帮助全面理解如由权利要求书及其等同限定的本发明的各种实施例。它包括各种具体细节以帮助理解,但是这些仅被认为是示例性的。因此,本领域的普通技术人员将认识到,在不脱离本公开的范围和精神的情况下,可以对本文描述的各种实施例进行各种改变和修改。此外,为了清楚和简洁起见,可以省略对众所周知的功能和结构的描述。

[0049] 在以下描述和权利要求中使用的术语和词不限于字面含义,而是仅由发明人使用以使得能够清楚和一致地理解本公开。因此,本领域的技术人员应当清楚,提供本公开的各种实施例的以下描述仅仅是为了说明的目的,而不是为了限制由所附权利要求及其等同限定的本公开。

[0050] 在详细描述本公开之前,描述对说明书和附图进行描述的方法。

[0051] 首先,在本说明书和权利要求书中使用基于其在本公开的各种实施例中的功能的通用术语。然而,这些术语可以根据本领域技术人员的意图、法律或技术解释或新技术的出现而不同地使用。此外,一些术语由申请人任意选择。除非另有说明,否则这些术语可以以本文所定义的含义来解释,并且可以基于说明书的整个内容和本领域的普通技术知识来解释。

[0052] 此外,在整个说明书的附图中,相同的附图标记表示执行基本相同功能的部分或部件。为了便于解释和理解,使用相同的附图标记或符号来描述不同的实施例。换句话说,即使在多个附图中示出了所有具有相同附图标记的元件,但是多个附图可以不涉及相同的实施例。

[0053] 在说明书和权利要求书中,包括诸如“第一”、“第二”等序数的术语可仅用于将相同或类似的组件彼此区分开来,因此,每个组件不受序数的限制。这些术语用于将一个部件与另一个部件区分开。例如,与这样的序号相关联的任何组件在使用顺序、放置等方面不受限制。必要时,每个序数可以互换使用。

[0054] 在本说明书中,单数形式包括复数形式,除非上下文另外清楚地指出。还应理解,在说明书中使用的术语“包括”或“由……形成”规定了在说明书中提及的特征、数字、步骤、操作、组件、部件或其组合的存在,但不排除一个或多个其它特征、数字、步骤、操作、组件、部件或其组合的存在或添加。

[0055] 在本公开的实施例中,诸如“模块”、“单元”或“部分”的术语用于指示执行至少一个功能或操作的组件,并能够用硬件、软件或硬件和软件的组合来实现。此外,除了“模块”、“单元”或“部分”必须用特定硬件单独实现的情况,多个“模块”、“单元”、“部分”等可以集成到至少一个模块或芯片中,并用至少一个处理器(未示出)实现。

[0056] 此外,在本说明书中,应当理解,当一个部件被称为“连接到”另一个部件时,它可以直接连接到另一个部件,或者间接连接到另一个部件且第三部件插入在它们之间。除非另外明确描述,否则“包括”任何部件应理解为隐含地包括其它部件,而不排除任何其它部件。

[0057] 图1a、图1b和图1c是各自示出根据本公开的各种实施例的电子设备的操作的示意性过程的图。

[0058] 图1a假定用户用用户手指10触摸电子设备100的屏幕以输入用于解锁电子设备

100的图案。

[0059] 参照图1a,当用户输入图案与预先存储在电子设备100中的图案不匹配时,发生用户认证失败,这导致电子设备100在其前部显示诸如“图案失配”和“保持锁定”的文本。也就是说,当用户输入的图案与预先存储的图案不匹配时,电子设备100可以保持在锁定状态。

[0060] 参照图1b,其示出了在数个如图1a所示地发生的用户认证失败之后,用户输入与预先存储在电子设备100中的图案相同的图案,从而用户认证成功的情况。

[0061] 参照图1c,当用户认证成功时,电子设备100被切换到解锁状态,使得用户可以执行存储在电子设备100中的应用程序之中的呼叫应用程序。

[0062] 这里,用户可以用用户手指10触摸显示在电子设备100上并对应于呼叫应用程序的呼叫图标101,以执行呼叫应用程序。

[0063] 然而,在这里,电子设备100可以提高处于解锁状态下的电子设备的使用安全性。例如,电子设备100可以识别用户用用户手指10触摸的点的用户指纹10',或者当用户使用电子设备100时通过拍摄用户眼睛来识别用户虹膜20'。

[0064] 在这种情况下,电子设备100可以或者可以不通知用户用户指纹10'或者用户虹膜20'被电子设备识别。

[0065] 这样,由于通过图案输入使用户认证成功,电子设备100被切换到解锁状态,因此用户可以无限制地使用存储在电子设备100中的呼叫应用。然而,如图1a所示的用户认证失败发生几次,直到用户认证成功,从而提高了电子设备100的使用安全性。因此,即使当用户使用存储在电子设备100中的应用程序时,也可以基于用户指纹10'或用户虹膜20'来进一步执行用户重新认证。

[0066] 当用户重新认证失败发生时,电子设备100可以切换回锁定状态。

[0067] 图1a、图1b和图1c各自示出了根据本公开的电子设备100的示意性操作的示例;以及图2和图12各自基于每一组件和每一组件的操作来说明根据本发明的电子设备100的详细实施例。

[0068] 图2是说明根据本发明实施例的电子设备的配置的框图。

[0069] 电子设备100可以被实现为诸如移动电话或智能电话的无线通信设备或终端设备。电子设备100可以被实现为电视(TV)、台式个人计算机(PC)、膝上型PC、平板PC、可佩戴设备、机顶盒、服务器等,或者可以被实现为电子操作的各种电子设备中的一种。此外,电子设备100可以以包括一个或多个电子设备的系统的形式来实现(未示出)。

[0070] 参照图2,电子设备100可以包括:输入器110;以及处理器120。

[0071] 输入器110可以获得与电子设备100相关的各种输入。

[0072] 输入器110可以接收用户以各种方式输入到电子设备100的命令或信息。例如,输入器110可以获得以信号、语音、触摸或按钮操作的形式输入到电子设备100的命令或信息。

[0073] 输入器110可以获得输入到电子设备100以执行用户认证的用户认证信息。在这种情况下,输入器110可以基于按钮操作、触摸、语音等获得数字和/或字符的组合。

[0074] 此外,输入器110可以基于按钮操作、触摸、语音等获得关于特定图案或顺序的信息。

[0075] 输入器110还可以获得输入到电子设备100的用户生物信息。在这种情况下,用户生物信息可以是用户指纹、虹膜、脸部、声音、体温、脉搏、心率等;输入器110可以包括光学

传感器、相机、麦克风、温度测量传感器等。图12示出了输入器110的配置的示例。

[0076] 处理器120可以整体地控制电子设备100的配置。

[0077] 处理器120不仅可以控制输入器110,而且还可以通过基于通过输入器110输入的命令或信息来控制电子设备100的配置来执行各种操作。

[0078] 例如,处理器120可以基于通过输入器110输入的信息执行用户认证,以将电子设备100的状态从锁定状态切换到解锁状态或从解锁状态切换到锁定状态。

[0079] 当电子设备100处于锁定状态时,电子设备100可能不能执行电子设备100可以执行的一些功能。详细地,当电子设备100处于锁定状态时,可以不执行存储在电子设备100中并且可由电子设备100执行的一个或多个应用。

[0080] 这里,输入器110可以仅获得特定形式的信息输入。例如,即使输入器110可以获得诸如信号、语音、触摸、按钮操作等的各种形式的命令或信息,输入器110也能够获得仅以用户触摸的形式输入的信息。

[0081] 此外,当电子设备100处于锁定状态时,处理器120可以仅执行预定的操作。例如,处理器120可以不执行预先存储在电子设备100中的应用程序,而是可以仅基于仅通过输入器110获得的命令或信息来执行用户认证。

[0082] 处理器120可以基于通过输入器110输入的用户认证信息执行用户认证,并且基于用户认证将电子设备100切换到解锁状态。

[0083] 详细地,当电子设备100处于锁定状态时,处理器120可以基于通过输入器110输入的用户认证信息和预先存储在电子设备100中的用户认证信息来执行用户认证。这里,只有当通过输入器110输入的用户认证信息匹配,即与预先存储在电子设备100中的用户认证信息相同时,用户认证才可以成功。

[0084] 当输入的用户认证信息与预先存储的用户认证信息不匹配时,发生用户认证失败,并且处理器120可以将电子设备100保持在锁定状态。相反,当用户认证成功时,处理器120可以将电子设备切换到解锁状态。

[0085] 这里,用户认证信息可以指预定图案、数字和/或字符的组合、特定单词等。在这种情况下,图案可以指电子设备100上的触摸图案,包括在电子设备100中的一个或多个按钮(未示出)的操作图案等。

[0086] 例如,在关于特定触摸图案的信息被存储在电子设备100中的情况下,当用户在电子设备100上绘制与上述特定触摸图案相同的触摸图案时,处理器120可以将电子设备100切换到解锁状态。

[0087] 图3a、图3b和图3c是分别用于解释其中根据本公开的各种实施例的电子设备基于预先存储的触摸图案执行用户认证的示例的图。

[0088] 参照图3a,电子设备100可以显示用户界面(UI),该用户界面(UI)包括通过绘制预先存储的解锁图案来解锁的请求,并且还可以显示要在其上绘制解锁图案的多个点(九个点)。

[0089] 参照图3b,当用户所绘制的触摸图案与预先存储的解锁图案不匹配时,电子设备100可以在显示输入错误图案的消息的同时保持在锁定状态。

[0090] 参考图3c,相反,当用户所绘制的触摸图案与预存的解锁图案精确匹配时,电子设备100被切换到解锁状态,电子设备100可以被切换到电子设备100可以执行诸如呼叫、消息

或相机的应用程序的状态。

[0091] 作为另一个例子,在关于特定密码的信息被存储在电子设备100中的情况下,当用户向电子设备100输入与上述特定密码相同的字符串时,处理器120可以将电子设备100切换到解锁状态。

[0092] 图4a、图4b和图4c各自示出了基于预先存储的密码执行用户认证的示例。

[0093] 参照图4a,电子设备100可以显示包括输入个人识别码(PIN)的请求的UI,以将电子设备100切换到解锁状态,同时显示输入PIN的键盘。

[0094] 参照图4b,当用户通过键盘输入的字符与预先存储的PIN不匹配时,电子设备100可以显示输入错误PIN的消息,并且可以保持在锁定状态。

[0095] 相反,当用户正确地输入预先存储的PIN时,电子设备100可以被切换到解锁状态,使得电子设备100可以被切换到电子设备100可以执行诸如呼叫、消息或相机的应用的状态。

[0096] 即使在执行了用户认证并且电子设备100被切换到处于解锁状态之后,处理器120也可以提高电子设备100的使用安全性。详细地,处理器120可以甚至在执行用户认证之后执行用户重新认证。

[0097] 同时,当用户认证不成功时,处理器120可以执行用户重新认证。例如,在用户认证失败发生一次或多次并且用户认证尚未成功的状态下,处理器120可以执行用户重新认证以提高电子设备100的锁定的安全性。这种性能可以提高将电子设备100切换到解锁状态的要求。也就是说,处理器120可以仅在基于用户生物信息执行用户重新认证时才将电子设备100切换到解锁状态,而不是基于用户认证立即解锁。

[0098] 处理器120可获得用户生物信息并基于所获得的用户生物信息执行用户重新认证。在这种情况下,用户生物信息可以是用户指纹、虹膜、脸部、声音、体温和心率中的至少一个。

[0099] 例如,处理器120可以获得通过输入器110输入的用户生物信息,并通过将输入的用户生物信息与预先存储在电子设备100中的用户生物信息彼此进行比较来执行用户重新认证。详细地,处理器120可以通过将通过输入器110识别的用户指纹或虹膜与以数据形式预先存储在电子设备100中的用户指纹或虹膜进行比较来执行用户重新认证。

[0100] 这里,处理器120可以仅当输入的用户生物信息与预先存储在电子设备100中的用户生物信息匹配时,即以某一比率或更大比率匹配时,执行用户重新认证。当输入的用户生物信息与预先存储的用户生物信息不匹配时,发生用户重新认证失败。

[0101] 在电子设备100基于输入的用户认证信息处于解锁状态的情况下,处理器120可以在用户重新认证失败发生的情况下将电子设备100切换回锁定状态。

[0102] 如图4c所示,处理器120可以隐式地或显式地执行用户重新认证。

[0103] 例如,当隐式地执行用户重新认证时,处理器120可以在用户触摸电子设备100时自动识别用户指纹,而不向用户提供输入用户指纹信息或用户虹膜信息的通知。或者,处理器120可以在用户向电子设备100输入特定命令或信息时从电子设备100所捕获的正面图像中识别用户虹膜。

[0104] 图5a和图5b是分别用于解释其中根据本公开的各种实施例的电子设备隐式地执行用户重新认证的示例的图。

[0105] 参照图5a,其示出了一种情况,其中,为了执行与当前显示在电子设备100的屏幕底部的六个应用图标中位于右下方的应用图标相对应的应用程序,用户用用户手指10触摸位于右下方的应用图标。

[0106] 在这种情况下,当用户触摸电子设备100的屏幕时,电子设备100可以识别用户手指10的用户指纹10'。这里,电子设备100可以不向用户通知电子设备100当前识别了用户指纹10'的事实。

[0107] 在这种情况下,电子设备100可以通过将识别的用户指纹10'与预先存储的用户指纹彼此进行比较来执行用户重新认证。

[0108] 类似于图5a,图5b还示出了用户用用户手指10触摸位于六个应用图标中右下方的应用图标的情况。

[0109] 在这种情况下,当用户触摸电子设备100的屏幕时,电子设备100可以使用包括在电子设备100中的相机115来识别用户虹膜20'。这里,电子设备100可以不通知用户电子设备100当前使用相机115捕获正面图像并且识别用户虹膜20'的事实。

[0110] 在这种情况下,电子设备100可以通过将识别的用户虹膜20'与预先存储的用户虹膜彼此进行比较来执行用户重新认证。

[0111] 例如,当显式地执行用户重新认证时,处理器120可以通过向用户提供用于输入用户生物信息的通知或UI来执行用户重新认证。在这种情况下,被提供通知或UI的用户可以将诸如用户指纹或虹膜的用户生物信息输入到电子设备100。然后,基于输入的用户生物信息,处理器120可以执行用户重新认证。

[0112] 图6、图7a、图7b和图8是各自用于解释根据本公开的各种实施例的电子设备显式地执行用户重新认证的示例的图。

[0113] 执行用户重新认证的过程本身对应于如图7a、图7b和图8等所示的过程。然而,电子设备100可以显示UI,该UI请求用户输入用户生物认证和/或请求用户在如图7a、图7b和图8等所述的过程之前选择用户生物认证方法。

[0114] 例如,图6示出了电子设备100显示请求用户输入用户生物认证的UI 601和请求用户选择用户生物认证方法的用户界面(UI) 602的情况。

[0115] 参照图6,用户可以认识到以下事实:当用户不通过请求用户输入用户生物认证的UI 601执行用户生物认证时,处于解锁状态的电子设备100被切换回锁定状态。

[0116] 此外,通过请求用户选择用户生物认证方法的UI 602,用户可以选择用户喜欢的用户生物认证方法。在图6的情况下,用户可以在电子设备100的屏幕上选择(触摸)包括用户指纹认证、虹膜认证、语音认证或面部认证中的一个的区域,以执行对应于所选区域的用户认证。同时,图6仅示出了用户指纹认证、虹膜认证、语音认证和面部认证;然而,可以由用户选择的用户生物认证方法不一定限于此。

[0117] 当显式地执行用户重新认证时,电子设备100可以立即执行用户指纹认证。或者,当用户通过如图6所示的相同过程选择用户指纹认证时,电子装置100可以执行用户指纹认证。

[0118] 图7a和图7b示出了当执行用户指纹认证时电子设备100显示请求用户指纹认证并指示用户指纹认证方法的UI的示例。图7a和图7b假设在电子设备100的前屏幕上提供用户指纹认证。

[0119] 参照图7a,电子设备100可以显示请求用户指纹识别的UI,并且电子设备100可以显示请求用户指纹认证并指示用户指纹认证方法的UI(“将您的右手拇指指纹输入到下面的正方形中”)。

[0120] 参照图7b,电子设备100可以通过扬声器152请求用户指纹识别,并且可以通过语音输出指示用户指纹识别方法的UI(“将您的右手拇指指纹输入到下面的正方形中”)。

[0121] 当用户手指10被输入到如图7a或7b所示的正方形中并且因此用户指纹被识别时,电子设备100可以基于所识别的用户指纹来执行用户重新认证。

[0122] 同时,尽管是图7a和图7b假设指纹传感器(未示出)被实现在电子设备100的前面;然而,指纹传感器(未示出)可以在电子设备100的背部的部分或全部上实现。

[0123] 图8示出了根据本公开的实施例的、当电子设备100执行用户虹膜认证时显示UI以请求用户虹膜认证并指示用户虹膜认证方法的示例。

[0124] 参照图8,电子设备100可以显示指示用户虹膜识别的完成百分比(“28%”)的消息,该消息指示用户虹膜识别方法(“睁大您的眼睛并看屏幕”、“远离”或“靠近”)等。

[0125] 参照图8,电子设备100还可以显示表示由相机115捕获的用户的图像,使得用户准确地将用户虹膜定位在相机115上。

[0126] 在处理器120试图隐式地执行用户重新认证的情况下,当用户重新认证失败发生预定次数或更多次或预定时间段或更多次时,处理器120可以显式地执行用户重新认证。

[0127] 当执行用户认证时,处理器120可以根据用户认证失败的数量来提高电子设备100的使用安全性。这里,处理器120可以执行用户重新认证。在这种情况下,用户认证失败可以指因为输入的用户认证信息与预先存储的用户认证信息不匹配而发生用户认证失败。

[0128] 例如,当输入与预存的用户认证信息不匹配的用户认证信息时,发生用户认证失败;此后,再次输入与预先存储的用户认证信息不匹配的用户认证信息(与先前输入的用户认证信息相同或不同),从而发生用户认证失败,用户认证失败的数目被计数为2。

[0129] 在用户认证失败发生的次数“小于”预定次数的情况下,当输入的用户认证信息与预先存储的用户认证信息匹配时,处理器120可以确定用户认证成功,并将电子设备100切换到解锁状态。这里,当电子设备100处于解锁状态时,用户在使用电子设备100时可没有任何限制。例如,处理器120可以不执行单独的用户重新认证。

[0130] 在这种情况下,除非发生将电子设备100切换到锁定状态的预定事件(用户没有向电子设备100输入比预定时间长的任何东西、用户按下电子设备100上的按钮以将电子设备100切换到锁定状态等),处理器120可以将电子设备100保持在解锁状态。

[0131] 相反,在用户认证失败发生预定次数或更多次之后,当用户认证信息输入与预先存储的用户认证信息相匹配时,处理器120可以确定用户认证成功,并且将电子设备100切换到解锁状态。然而,与用户认证失败发生的次数少于预定次数的情况不同,处理器120可以提高电子设备100的使用安全性。例如,处理器120可以执行用户重新认证。

[0132] 在这种情况下,当用户重新认证成功时,处理器120不将电子设备100切换到锁定状态;然而,当用户重新认证失败发生时,处理器120可以将电子设备100切换回锁定状态。

[0133] 原因在于,随着用户认证失败的数量增加,尝试电子设备100的用户认证的用户更可能是外人而不是预注册的用户。

[0134] 例如,在用户认证失败发生两次或更少的情况下,当此后的用户认证至多在用户

认证信息输入的第三次尝试时成功时,处理器120不执行用户重新认证。然而,在用户认证失败发生三次或更多次的情况下,并且此后,当此后用户认证在用户认证信息输入的第四次或更多次试用时,处理器120可以执行用户重新认证。

[0135] 例如,参考图9a、图9b、图9c和图9d,在用户认证失败发生三次或更多次的情况下,如图9a、图9b和图9c所示,当用户认证此后在第四次试验中成功并且因此电子设备100被切换到如图9d所示的解锁状态时,电子设备100可以隐式地或显式地执行用户重新认证。

[0136] 这里,在处理器120试图隐式地执行用户重新认证的情况下,当用户重新认证失败发生预定次数或更多次、或者预定时间段或更长时,处理器120可以显式地执行用户重新认证。

[0137] 或者,处理器120可在执行预定应用程序的条件下隐式和/或显式地执行用户重新认证。

[0138] 详细地,在用户认证基于用户认证失败从输入用户认证信息开始发生预定次数或更多次后输入的用户认证信息而成功并且电子设备100处于解锁状态的情况下,当预定的应用程序被执行时,处理器120可以通过输入器110获得用户生物信息,并且基于输入的用户生物信息执行用户重新认证。

[0139] 这里,预定的应用程序可以包括提供需要用户登录的服务的应用程序中的、被设置为执行自动用户登录的应用程序或存储用户个人信息的应用程序中的至少一个。

[0140] 被配置成执行自动用户登录的应用程序是指这样的应用程序,其中当通过电子设备100执行应用程序时,基于预先存储在电子设备100中的用户信息自动执行对应用程序的登录,而无需任何输入用户信息以登录到应用程序的单独处理。

[0141] 预定应用程序需要具有相对较高的安全力,并且可以是具有支付和/或汇款功能的应用程序或电子设备100的管理器应用程序。

[0142] 同时,处理器120可以在用户认证失败发生预定次数或更多次的情况下提高电子设备100的锁定的安全性。例如,在用户认证失败发生预定次数或更多次的情况下,当此后用户认证仍旧成功时,处理器120可以隐式地和/或显式地执行用户重新认证,而不管用户认证是否成功。

[0143] 详细地,当用户输入用户认证信息以将电子设备100切换到解锁状态时,处理器120可以基于通过输入器110输入的用户生物信息来执行用户重新认证。这里,处理器120可以通过输入器110获得用户生物信息,同时执行用户操作(触摸,按钮操作等)以输入用户认证信息。

[0144] 例如,在用户认证失败发生三次的情况下,处理器120之后可以隐式地执行用户重新认证,同时用户第四次或更多次地输入用户认证信息。这里,当以用户触摸电子设备100的方式执行用户认证信息的输入时,处理器120可以基于用于输入用户认证信息的用户触摸通过输入器110获得用户指纹,并且可以将所获得的用户指纹用于用户重新认证。或者,处理器120可在用户输入用户认证信息时使用从电子设备100所拍摄的正面图像获得的用户虹膜信息进行用户重新认证。

[0145] 图10a和图10b假定电子设备100执行用户指纹或虹膜识别,而用户输入图案作为用户认证信息。

[0146] 参照图10a,当用户用用户手指10在电子设备100的屏幕上绘制触摸图案时(当用

户输入用户认证信息时),电子设备100可以识别用户手指10的指纹10'。

[0147] 这里,电子设备100可以不通知用户执行了用户指纹识别,并且可以基于所识别的用户指纹10'执行用户重新认证。

[0148] 参照图10b,当用户用用户手指10在电子设备100的屏幕上绘制图案时(当用户输入用户认证信息时),电子设备100可以通过相机115识别用户虹膜20'。

[0149] 这里,电子设备100可以不通知用户执行了用户虹膜识别,并且可以基于所识别的用户虹膜20'执行用户重新认证。

[0150] 此外,处理器120可以不将电子设备100切换到解锁状态,并且在用户重新认证失败的情况下将电子设备100保持在锁定状态。

[0151] 相反,当用户重新认证基于用户生物信息而成功时,即使用户认证不成功,处理器120也可以将电子设备100切换到解锁状态。

[0152] 如图10a和图10b所示,在处理器120隐式地执行用户重新认证(用户生物认证)的情况下,当用户重新认证失败发生预定次数或更多次或预定时间段或更长时,处理器120可以显式地执行用户重新认证。

[0153] 在这种情况下,即使基于输入的用户认证信息的用户认证成功,处理器120也可以不立即将电子设备100切换为解锁状态,并且可以显式地执行用户重新认证。

[0154] 在这种情况下,如图11所示,电子设备100可以显示请求用户输入用户生物认证的UI 1101和请求用户选择用户生物认证方法的UI1102中的至少一个。此外,电子设备100可以使用与图7a、图7b和图8所示相同的方法来执行用户生物认证。

[0155] 这里,当用户重新认证成功时,处理器120可以将电子设备100切换到解锁状态;然而,当用户重新认证失败发生时,处理器120可以保持电子设备100处于锁定状态。

[0156] 上述实施例中的处理器120根据用户认证失败的数量执行用户重新认证的每个实施例可以与实施例中的一些或全部结合执行。

[0157] 例如,在用户认证失败发生少于预定的第一次数(第一次)的情况下,当此后用户认证成功(解锁)时,处理器120可不执行用户重新认证。处理器120可以隐式地和/或显式地执行用户重新认证,即使在用户认证失败发生预定的第一次数或更多且少于预定的第二次数之后用户认证成功(解锁)。这里,当用户重新认证失败发生时,处理器120可以将电子设备100切换到锁定状态。当用户认证失败发生预定的第二次或更多次时,处理器120可以基于用户输入用户认证信息时输入的用户生物信息来执行用户重新认证。然后,只有当用户重新认证成功时,处理器120才可以将电子设备100切换到解锁状态,并且不限于此。

[0158] 处理器120可以根据用户认证失败的次数以不同的周期执行用户重新认证。

[0159] 例如,在用户认证失败发生少于预定次数的情况下,当此后用户认证成功(解锁)时,处理器120可不执行用户重新认证。在用户认证失败发生预定次数或更多次的情况下,处理器120可以基于预定周期隐式地和/或显式地执行用户重新认证,即使在用户认证成功之后(解锁)。

[0160] 作为另一个例子,在用户认证失败发生少于预定的第一次数(第一次)的情况下,当此后用户认证成功(解锁)时,处理器120可以基于第一周期隐式地执行用户重新认证。在用户认证失败发生预定的第一次数或更多且少于预定的第二次数的情况下,当此后用户认证成功(解锁)时,处理器120可以基于小于第一周期的第二周期隐式地执行用户重新认证。当用户

认证失败发生预定的第二次或更多次时,处理器120可以显式地执行用户重新认证。

[0161] 图12是说明根据本发明的各种实施例中的一者的电子装置的详细配置的框图。

[0162] 除了输入器110和处理器120之外,电子设备100还可以包括存储器130、通信器140(例如,收发器)、输出器150和输入/输出端口160中的至少一个。

[0163] 输入器110可以包括用于获得用户命令或信息的触摸传感器111、按钮输入器112、麦克风113、指纹传感器114、相机115等。

[0164] 触摸传感器111被配置为感测用户触摸点,并且可以在电子设备100的至少部分表面上实现。触摸传感器111可以被实现为压敏或电容式触摸传感器。

[0165] 触摸传感器111可以被实现为联接到电子设备100的显示器151的触摸面板,或者与包括在按钮输入器112中的至少一个按钮相结合。

[0166] 用户可以触摸电子设备100的特定点,该特定点包括触摸传感器111以将用户命令或信息输入到电子设备100中。

[0167] 用户可以触摸显示在显示器151上的特定对象,以将用户命令或对应于该特定对象的信息输入到电子设备100。用户还可以通过触摸传感器111输入用户认证信息。

[0168] 按钮输入器112可以包括在电子设备100的一部分上提供的至少一个按钮。用户可以按下特定按钮或触摸包括触摸传感器111的按钮以向电子设备100输入用户命令或信息。此外,用户可以通过按钮输入器112输入用户认证信息。

[0169] 麦克风113被配置为获得语音形式的用户命令或信息。麦克风113可以包括将模拟信号转换为数字信号的模数转换器。

[0170] 通过麦克风113获得语音,用户可以使用用户语音将用户命令或信息输入到电子设备中。这里,通过麦克风113输入的用户语音被具体地识别,并且对应于用户语音的文本因此可以被用作用户认证信息。或者,通过麦克风113输入的用户语音被识别,因此用户语音的信号特征值可以被用作用户生物信息。

[0171] 指纹传感器114被配置为识别用户指纹。指纹传感器114可以被实现为联接到显示器151,并且可以在电子设备100的特定表面上被实现为不联接到显示器151。

[0172] 处理器120可以基于通过指纹传感器114识别的用户指纹与预先存储的用户指纹之间的比较结果来执行用户重新认证。

[0173] 相机115被配置为拍摄图片或拍摄视频。当电子设备100是移动电话或智能电话时,电子设备100可以仅包括一个相机115,或者可以分别包括位于电子设备100的前面和后面中的一个或多个上的相机。

[0174] 电子设备100可以通过相机115识别用户虹膜或脸部。或者,即使在图12中未示出,除了相机之外,单独的用户虹膜识别传感器(未示出)还可以包括在电子设备100中。

[0175] 处理器120可以基于通过相机115或单独的用户虹膜识别传感器(未示出)识别的用户虹膜信息来执行用户重新认证。

[0176] 处理器120可以包括随机存取存储器(RAM,未示出)、只读存储器(ROM,未示出)、中央处理单元(CPU,未示出)、图形处理单元(GPU,未示出)、系统总线(未示出)等,并且可以执行与包括在电子设备100中的其它组件的控制相关的操作或数据处理。

[0177] 存储器130被配置为存储与控制电子设备100的组件的整体操作和电子设备100的组件的操作系统(OS)有关的命令或数据。

[0178] 为此,存储器130可被实现为非易失性存储器(例如,硬盘、固态驱动器(SSD)、闪存)、易失性存储器等。

[0179] 存储器130可以存储电子设备100的用户信息。详细地,处理器120可以预先从用户获得用于用户认证的用户认证信息和用于用户重新认证的用户生物信息,并且可以将该信息存储在存储器130中。

[0180] 此后,处理器120可以分别基于从用户输入的用户认证信息和/或用户生物信息与所存储的用户认证信息和/或所存储的用户生物信息之间的比较结果来执行用户认证和/或用户重新认证信息。

[0181] 存储器130还可以包括关于显式地执行用户生物认证所需的用户生物认证通知或UI的信息。

[0182] 通信器140被配置成使电子设备100能够根据各种类型的通信方式来执行与各种类型的外部设备的通信。通信器140可以包括WiFi芯片(未示出)、蓝牙芯片(未示出)等。通信器140可以以无线或有线方式执行与各种外部设备的数据通信。

[0183] 当以无线通信方式执行与外部设备(未示出)的数据通信时,通信器140可以包括WiFi直连通信模块、蓝牙模块、红外数据关联(IrDA)模块、近场通信(NFC)模块、Zigbee模块、蜂窝通信模块、第三代(3G)移动通信模块、第四代(4G)移动通信模块和第四代长期演进(LTE)通信模块中的至少一个。

[0184] 在如图2所示的先前实施例中,处理器120基于通过输入器110输入的用户认证信息来执行用户认证。然而,处理器120还可以通过通信器140从外部设备(未示出)获得外部设备(未示出)中的输入用户认证信息,并且可以基于所获得的用户认证信息来执行用户认证。

[0185] 此外,处理器120可以通过通信器140在外部设备(未示出)中获得输入的用户生物信息,并且基于所获得的用户生物信息执行用户重新认证。

[0186] 即使在图12中未示出,通信器140可以包括位置传感器(未示出),例如全球定位系统(GPS)传感器。位置传感器(未示出)是估计电子设备100的当前位置的设备。

[0187] 这里,处理器120可以从位置传感器(未示出)获得电子设备100的位置信息。

[0188] 在这种情况下,处理器120可以从位置传感器(未示出)获得电子设备100的位置信息,并且在电子设备100处于使用中时将该信息预先存储在存储器130中。例如,处理器120可以仅在电子设备100处于解锁状态时从位置传感器(未示出)获得位置信息,并将该信息预先存储在存储器130中。

[0189] 此后,在用户输入用户认证信息并且处理器120执行用户认证的情况下,处理器120可以从位置传感器(未示出)获得电子设备100的位置信息,将该信息与预先存储的位置信息彼此进行比较,并且基于比较结果执行用户重新认证。

[0190] 详细地,处理器120可以在以下情况下执行用户重新认证,其中:所获得的位置信息完全不匹配预先存储的位置信息;获取的位置信息与预先存储的位置信息中最接近的位置信息相比相差预定距离或更多;获取的位置信息对应的国家与预先存储的位置信息对应的一个或多个国家不匹配。

[0191] 输出器150被配置为在视觉或听觉上向用户提供存储在电子设备100中的信息。

[0192] 输出器150可以包括显示器151、扬声器152等,并且可以包括振动马达(未示出)。

振动马达(未示出)被配置为基于从处理器120或通信器140发送的命令或信号振动。

[0193] 显示器151被配置成在处理器120的控制下显示图像。为此,显示器151可以实现为液晶显示器(LCD)、等离子体显示面板(PDP)、有机发光二极管(OLED)、透明OLED(TOLED)等。当实现为LCD时,显示器151可一起包括驱动电路(未示出)、背光单元(未示出)等,其可以实现为a-si薄膜晶体管(TFT)、低温多晶硅(LTPS)、薄膜晶体管(TFT)、有机TFT(OTFT)等的形式。

[0194] 显示器151可以在处理器120的控制下显示指示用户认证和/或用户重新认证的过程或结果的文本和图像;并且当显式地执行用户生物认证时,显示器151还可以显示相关的通知或UI。

[0195] 此外,显示器151可以显示包括在通过电子设备100的广播获得器(未示出)获得的广播信号中的图像、包括在通过通信器140获得的信号中的图像、通过输入器110输入的图像、包括在存储在存储器130中的图像文件中的图像、包括在通过输入/输出端口160从外部获得的信号中的图像等。

[0196] 扬声器152被配置成在处理器120的控制下输出特定的语音。

[0197] 扬声器152可以在处理器120的控制下以语音的形式提供指示用户认证和/或用户重新认证的过程或结果的UI;并且当显式地执行用户生物认证时,扬声器152还可以提供相关的听觉通知或UI。

[0198] 此外,扬声器152可以输出包括在通过电子设备100的广播获得器(未示出)获得的广播信号中的语音、包括在通过通信器140获得的信号中的语音、通过麦克风113输入的语音、包括在存储在存储器130中的音频文件中的语音、包括在通过输入/输出端口160从外部获得的信号中的语音等。

[0199] 电子设备100可以通过输入/输出端口160从外部获得并向外部发送图像和/或语音的信号。此外,电子设备100可以通过输入/输出端口160从外部获得或向外部提供电力。

[0200] 为此,输入/输出端口160可以被实现为有线端口,例如高清晰度多媒体接口(HDMI)端口、显示端口、红绿蓝(RGB)端口、数字视觉接口(DVI)端口、雷电、部件端口等。或者,输入/输出端口160可被实现为用于无线通信(例如WiFi或蓝牙通信)的端口。

[0201] 输入/输出端口160可以包括耳机或头戴式耳机连接端子。在这种情况下,电子设备100可以将包括存储在存储器130中的语音文件中所包括的语音、通过电子设备100的广播获得器或通信器140获得的信号中所包括的语音等的信号发送到所连接的耳机或头戴式耳机。

[0202] 此外,电子设备100可以向所连接的耳机或头戴式耳机发送信号,该信号包括与用户认证和/或用户重新认证的过程或结果所指示的UI相对应的语音、与显式地执行用户生物认证时的相关通知或UI相对应的语音等。

[0203] 即使在图12中未示出,电子设备100还可以包括广播获得器(未示出)、电源供应器(未示出)等。

[0204] 广播获得器(未示出)可以被实现为包括诸如调谐器(未示出)、解调器(未示出)、均衡器(未示出)等组件,以获得从广播站发送的广播内容。

[0205] 电源供应器(未图示)可经配置以将电力供应到电子设备100的组件。电源供应器(未示出)可以使用通过输入/输出端口160从外部供应的电力向电子设备100的部件供应电

力。此外,电源供应器(未示出)可以包括电池,并且可以将外部供应的电力存储在电池中,并且将电力供应到电子设备100的部件。

[0206] 在下文中,描述了根据本公开的电子设备的控制方法。

[0207] 图13是用于解释根据本公开的实施例的电子设备的控制方法的流程图。

[0208] 参照图13,当电子设备处于锁定状态时,控制方法可以基于输入的用户认证信息和电子设备中预先存储的用户认证信息来执行用户认证(S1310)。

[0209] 当用户认证成功时,该方法可以包括将电子设备100切换到解锁状态(S1320)。例如,当输入的用户认证信息与预先存储的用户认证信息匹配时,电子设备可以被切换到解锁状态。

[0210] 这里,该方法可以包括:当在从输入的用户认证信息开始用户认证失败发生预定次数或更多次之后,用户认证基于输入的用户认证信息而成功时,提高处于解锁状态下的电子设备的使用安全性(S1330)。详细地,在提高电子设备的使用安全性的过程中,可以根据由于输入的用户认证信息与预先存储的用户认证信息不匹配而发生的用户认证失败的数量来执行用户重新认证。在这种情况下,用户认证失败可以指用户认证失败因输入的用户认证信息与预先存储的用户认证信息不匹配而发生。

[0211] 用户认证信息可以包括预定图案或密码,并且用户生物信息可以包括用户指纹或用户虹膜。

[0212] 为了执行用户重新认证,可以获得用户生物信息,并且可以基于输入的用户生物信息来执行用户重新认证。这里,当输入的用户生物信息与预先存储的用户生物信息匹配时,用户重新认证可以是成功的。

[0213] 例如,在用户认证失败发生预定次数或更多次的情况下,当基于此后输入的用户认证信息用户认证成功并且因此电子设备被切换到解锁状态时,即使在电子设备被切换到解锁状态之后也可以执行用户重新认证。

[0214] 详细地,在输入的用户认证信息与预先存储的用户认证信息相匹配并且因此电子设备被切换到解锁状态的情况下,即使在电子设备被切换到解锁状态之后,当用户认证失败(其中输入了不正确的用户认证信息)发生预定次数或更多次,直到用户输入与预先存储的用户认证信息相匹配的用户认证信息时,也可以执行用户重新认证。这里,当用户重新认证成功时,可以将电子设备保持在解锁状态;然而,当用户重新认证失败发生时,电子设备可以被切换回处于锁定状态。

[0215] 在提高电子设备的使用安全性的过程中,可以在电子设备切换到解锁状态之后执行预定应用的条件下执行用户重新认证。例如,当在电子设备处于解锁状态的情况下执行预定应用程序时,可以执行用户重新认证。

[0216] 这里,预定应用程序可以包括提供需要用户登录的服务的应用程序中的、被设置为执行自动用户登录的应用程序或存储用户个人信息的应用程序中的至少一个。

[0217] 同时,在用户认证失败发生的次数少于预定次数的情况下,当用户认证成功并因此电子设备切换到解锁状态时,与上述相反,可不提高电子设备的使用安全性。

[0218] 详细地说,在输入的用户认证信息与预先存储的用户认证信息匹配以将电子设备切换到解锁状态之前,在用户认证失败发生一次或多次但少于预定次数的情况下,在电子设备切换到解锁状态之后,不执行用户重新认证。

[0219] 同时,控制方法还可以包括在用户认证失败发生预定次数或更多次的情况下提高电子设备在锁定状态下的锁定安全性。也就是说,电子设备可以被切换到解锁状态,但不是每当用户认证基于用户认证信息成功时,而是仅当用户重新认证基于用户生物信息成功时才被切换到解锁状态。

[0220] 详细地,在用户认证失败发生预定次数或更多次数的情况下,可以在用户输入用户认证信息以将电子设备切换到解锁状态的同时获得用户生物信息,并且可以基于输入的用户生物信息执行用户重新认证。

[0221] 在这种情况下,用户认证失败发生预定次数或更多次的情况下,用户生物信息本身可以在用户输入用户认证信息以成功进行用户认证时获得。例如,在需要输入触摸图案以执行用户认证的情况下,可以在用户触摸电子设备以输入触摸图案的同时识别用户指纹。

[0222] 或者,当用户通过触摸操作输入用户认证信息时,可以在电子设备拍摄图像时获得正面图像,并且可以从所获得的图像中识别用户虹膜或面部。

[0223] 当用户重认证成功时,不管用户认证是否成功,电子设备都可以切换到解锁状态;并且当用户重新认证失败时,无论用户认证是否成功,都可以将电子设备保持在锁定状态。

[0224] 根据用户认证失败的数目执行用户重新认证的上述实施例可以被组合到在各种实施例中要导出的一些或全部实施例中。

[0225] 图14到图17是算法,其每一者用于解释根据本发明的各种实施例中的一者的电子装置的控制方法。

[0226] 参照图14,在电子设备处于锁定状态的情况下(S1405-Y),可以基于输入的用户认证信息来执行用户认证(S1410)。

[0227] 这里,可以识别由于用户认证信息与预先存储的用户认证信息不匹配而发生的用户认证失败的数目(S1415),以确定用户认证失败是否发生少于预定次数。参照图14,确定用户认证失败是否发生三次或更少(S1420)。这里,三次是一个示例,而不限于此。

[0228] 在用户认证失败发生三次或更少次的情况下(S1420-Y),识别用户认证是否成功(S1425)。这里,当用户认证成功时(S1425-Y),电子设备可以切换到解锁状态(S1430)。

[0229] 在用户认证失败连续发生(S1425-N)并且因此用户认证失败发生多于三次(S1420-N)的情况下,可以识别用户认证失败是否发生六次或更少(S1435)。这里,六次是一个示例,而不限于此。

[0230] 在用户认证失败发生六次或更少次的情况下(S1435-Y),识别用户认证是否成功(S1440)。这里,当用户认证成功时(S1440-Y),电子设备可以切换到解锁状态(S1445)。然而,即使在电子设备被切换到解锁状态之后,也可以执行用户重新认证,即用户生物认证(S1450)。这里,发生用户生物认证失败,电子设备可以切换回锁定状态。

[0231] 在用户认证失败连续发生(S1440-N)并且因此用户认证失败发生多于六次的情况下(S1435-N),可以立即执行用户生物认证(S1455)。这里,当用户认证成功时(S1460-Y),电子设备可以切换到解锁状态(S1465)。

[0232] 上述图14的算法可以概括如下。在用户认证失败发生三次或更少并且此后用户认证成功的情况下,电子设备被切换到处于解锁状态并且用户生物认证不被进一步执行。在用户认证失败发生多于三次和六次或更少并且此后用户认证成功的情况下,将电子设备切

换到解锁状态并且进一步执行用户生物认证 (S1500)。在用户认证失败发生7次或更多次的情况下,只有当用户生物认证成功时,电子设备才被切换到解锁状态,而不管用户认证是否成功 (S1700)。

[0233] 这样,在电子设备被切换到处于解锁状态之后是否执行用户生物认证可以取决于用户认证失败的次数。

[0234] 此外,根据用户认证失败的次数,可以提高将电子设备切换到解锁状态的条件。详细地,可以基于输入的用户认证信息将解锁的条件从用户认证改变为基于用户生物信息的用户生物认证。

[0235] 图15是用于解释特定过程的示例的算法,在该特定过程中,用户认证失败发生的次数多于预定的第一次数(图14中的三次)和预定的第二次数或更少(图14中的六次),并且此后用户认证成功,在电子设备切换到解锁状态之后执行用户生物认证 (S1500)。

[0236] 参照图15,在用户认证失败发生的次数多于预定的第一次数和预定的第二次数或更少的情况下,当用户认证之后成功并且因此电子设备被切换到解锁状态时 (S1445),可以根据是否执行预定应用程序来执行用户生物认证。这里,预定应用程序可以是被设置为执行自动用户登录的应用程序、存储用户个人信息等的应用程序以及提供需要用户登录的服务的应用程序。

[0237] 在电子设备被切换到处于解锁状态并且此后执行预定应用程序的情况下 (S1510-Y),可以隐式地执行用户生物认证 (S1520)。也就是说,可以在没有指示执行用户生物认证的单独通知或UI的情况下执行用户生物认证。

[0238] 在这种情况下,当用户生物认证成功时 (S1530-Y),电子设备可以保持在解锁状态。

[0239] 相反,当隐式地执行用户生物认证并因此发生用户生物认证失败时 (S1530-N),可以将电子设备切换回处于锁定状态 (S1540),然后可以显式地执行用户生物认证。

[0240] 详细地,当提供用户生物认证UI (S1550)并且用户基于UI输入用户生物信息时,用户生物认证可以随后基于输入的用户生物信息执行 (S1560)。这里,用户生物认证UI可以是请求用户输入用户生物信息和/或通知用户如何输入用户生物信息的UI。

[0241] 当用户生物认证成功时 (S1570-Y),电子设备可以切换到解锁状态 (S1580);当用户生物认证失败时 (S1570-N),电子设备可以保持在锁定状态。

[0242] 图16示出了另一个实施例,其中可以根据用户认证失败的次数来执行用户重新认证,即用户生物认证。

[0243] 参照图16,大多数操作与图14中所示的操作相同。然而,操作S1635和S1655与图14所示的不同。

[0244] 也就是说,根据图16中的实施例,即使用户认证成功,并且因此电子设备被切换到解锁状态,也可以执行用户生物认证。这里,根据直到用户认证成功之前发生的用户认证失败的数目,可以不同的周期执行用户生物认证。

[0245] 详细地说,随着用户认证失败的次数增加,直到用户认证成功,用户生物认证可以更频繁地执行。也就是说,在图16中,S1655中的第二周期可以比S1635中的第一周期短。如上所述,操作S1605-S1630、S1640-S1650和S1660-S1670类似于图14所示的操作S-1405-S1430、S1435-S1445和S1455-S1465,因此将省略其描述。

[0246] 图17是用于解释实施例的算法,其中在用户认证失败发生的次数多于预定次数的情况下,立即执行用户生物认证(S1700)。

[0247] 参照图17,在用户认证失败发生多于预定次数的情况下,可以隐式地执行用户生物认证(S1710)。详细地说,在用户认证失败发生的次数多于预定次数并且用户认证尚未成功的情况下,可以隐式地执行用户生物认证。

[0248] 在这种情况下,可以在用户进一步输入用户认证信息以执行用户认证的同时隐式地执行用户生物认证。例如,作为用户生物信息的用户指纹可以基于用户的手指触摸来输入用户认证信息而被识别;或者,当用户注视电子设备以输入用户认证信息时,可以通过拍摄用户的眼睛来识别作为用户生物信息的用户虹膜。此后,可以基于所识别的用户指纹或虹膜来执行用户生物认证。

[0249] 在隐式执行用户生物认证并因此用户生物认证成功(S1720-Y)的情况下,电子设备被切换到解锁状态(S1760)。这里,不管用户认证是否成功,都将电子设备切换到解锁状态。

[0250] 相反,在隐式地执行用户生物认证的情况下,并且因此发生用户生物认证失败(S1720-N),则可以显式地执行用户生物认证。

[0251] 详细地,当可以提供用户生物认证UI(S1730)并且用户在所提供的UI之后输入用户生物信息时,可以执行用户生物认证(S1740)。

[0252] 在显式地执行用户生物认证并且因此用户生物认证成功的情况下(S1750-Y),电子设备被切换到处于解锁状态。相反,在用户生物认证失败的情况下(S1750-N),电子设备保持在锁定状态,而不管用户认证是否成功。

[0253] 如图13至图17中具体描述的根据本公开的控制方法的实施例可以由图2或图12所示或所解释的电子设备100来执行。

[0254] 此外,根据本公开的控制方法的实施例可以在特定软件中实现并由电子设备100的处理器120执行,并且因此电子设备100可以执行与控制方法相对应的操作。

[0255] 此外,根据本公开的控制方法的实施例可以由包括电子设备100和一个或多个外部设备(未示出)的系统(未示出)来实现。

[0256] 同时,上述公开中的各种实施例可以在使用软件、硬件或软件和硬件的组合的计算机或计算机可读记录介质中实现。

[0257] 根据硬件实施方案,可使用用于执行其它功能的专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器和电子单元中的至少一者来实施本发明中所描述的实施例。

[0258] 在一些情况下,本公开中描述的实施例可以实现为处理器120本身。根据软件实现,诸如在本公开中描述的过程和功能的实施例可以被实现为单独的软件模块。软件模块中的每一者可执行本发明中所描述的一个或一个以上功能和操作。

[0259] 同时,用于执行根据上述公开中的各种实施例的电子设备100的处理操作的计算机指令可以存储在非暂时性计算机可读介质中。存储在非暂时性计算机可读介质中的计算机指令在由特定设备的处理器执行时允许特定设备执行根据上述各种实施例的电子设备100的处理操作。

[0260] 非暂时性计算机可读介质不是指临时存储数据的介质(诸如寄存器、高速缓存、存储器等),而是指半永久性地存储数据并可由装置读取的介质。详细地说,可以在将上述各种应用或程序存储在诸如光盘(CD)、数字多功能盘(DVD)、硬盘、蓝光盘、通用串行总线(USB)、存储卡、只读存储器(ROM)等非暂时性计算机可读介质中的同时提供上述各种应用或程序。

[0261] 虽然已经参考本公开的各种实施例示出和描述了本公开,但是本领域技术人员将理解,在不脱离由所附权利要求及其等同限定的本发明的精神和范围的情况下,可以在形式和细节上进行各种改变。

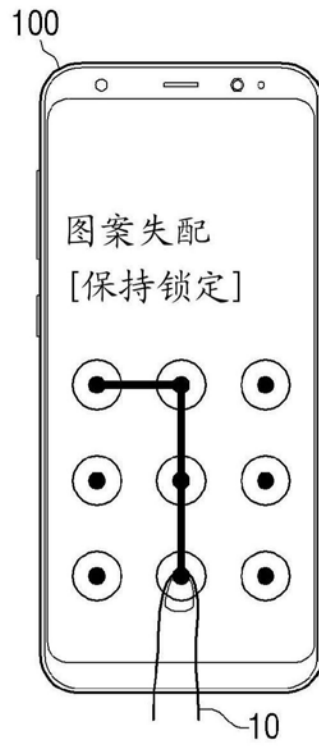


图1a

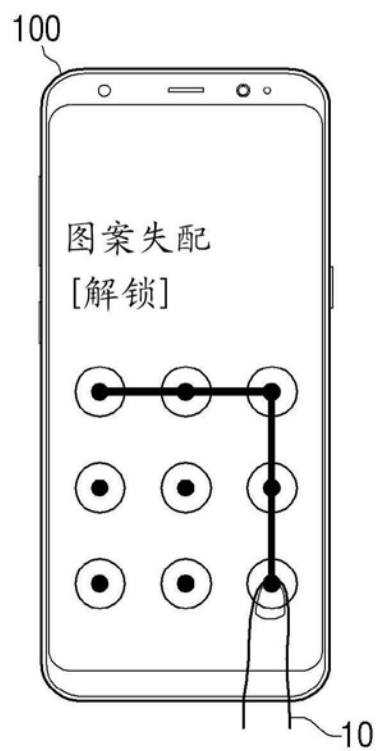


图1b

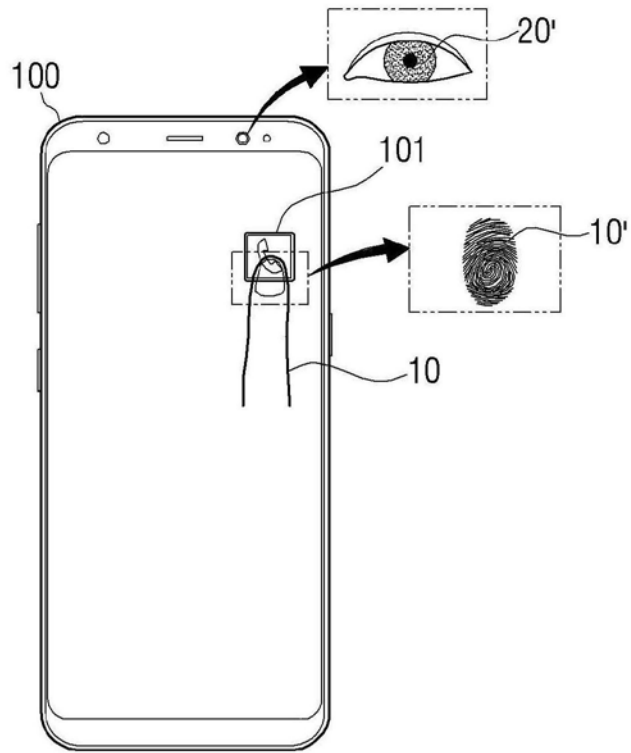


图1c

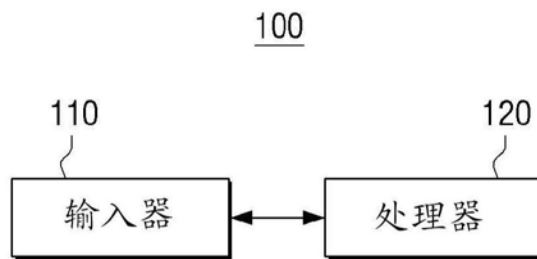


图2

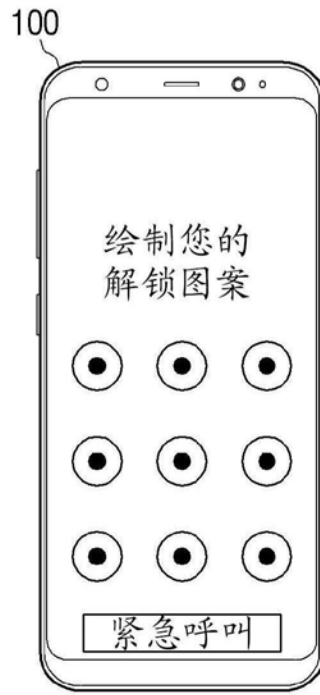


图3a

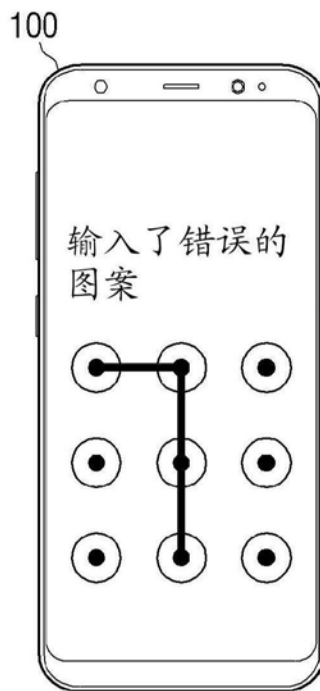


图3b



图3c



图4a

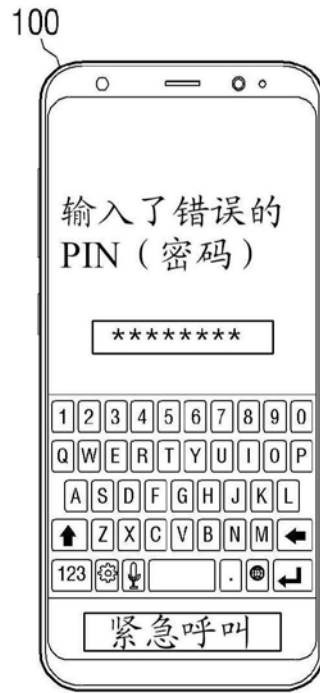


图4b



图4c



图5a

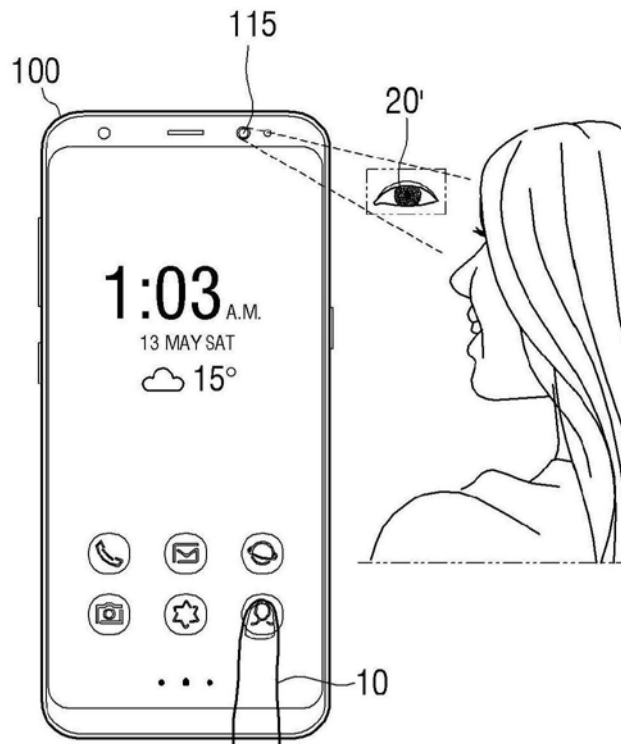


图5b

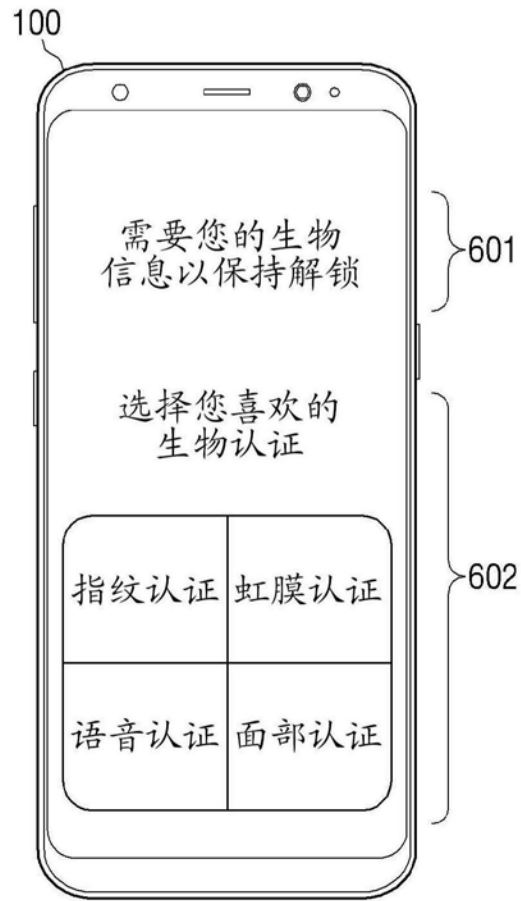


图6

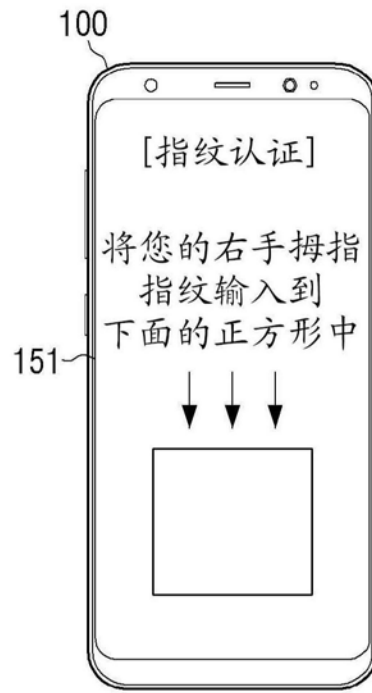


图7a

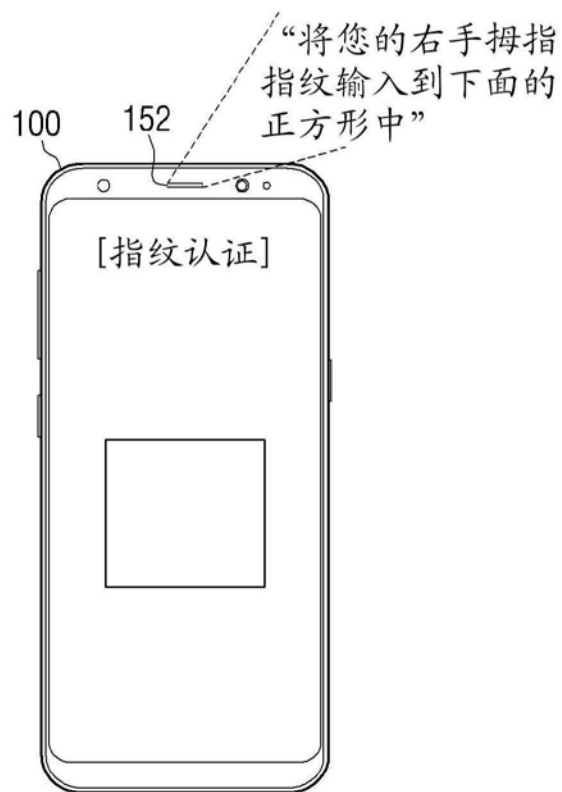


图7b

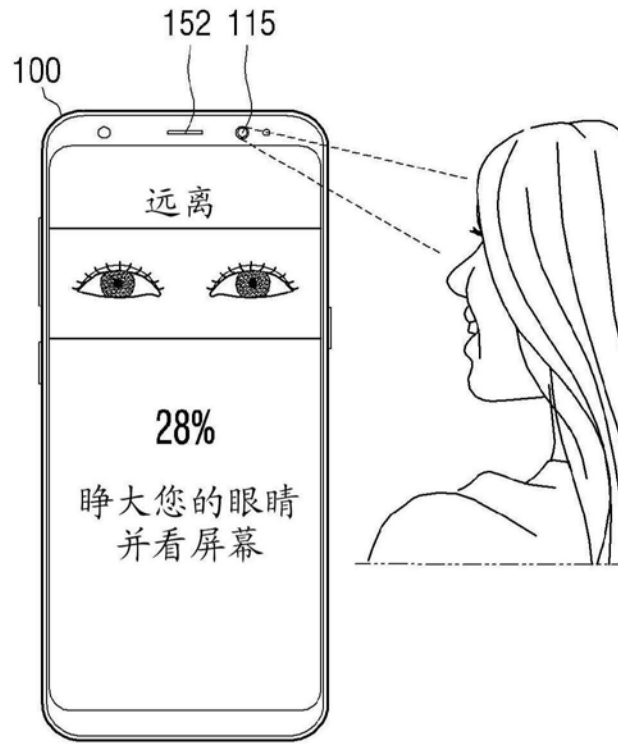


图8

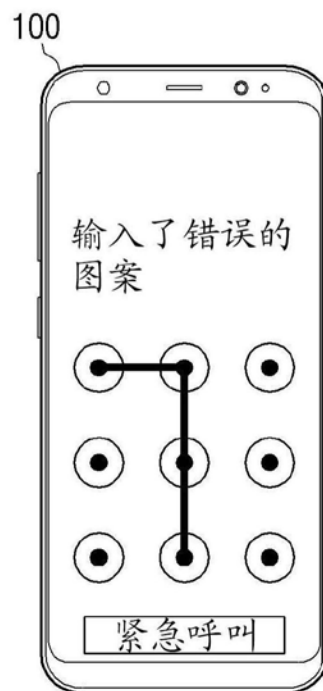


图9a

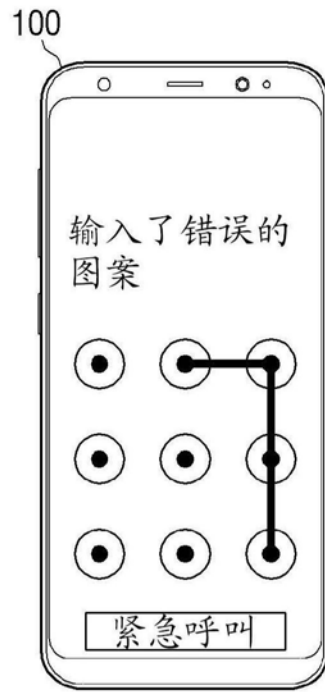


图9b

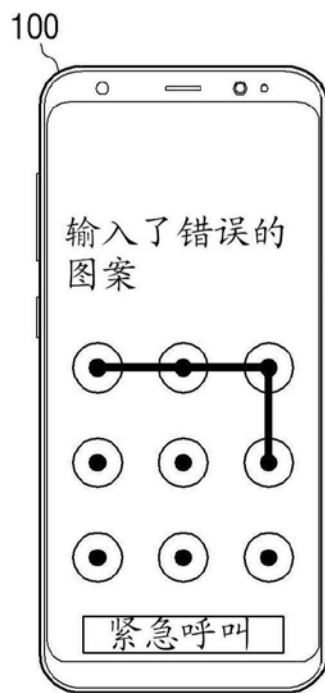


图9c



图9d

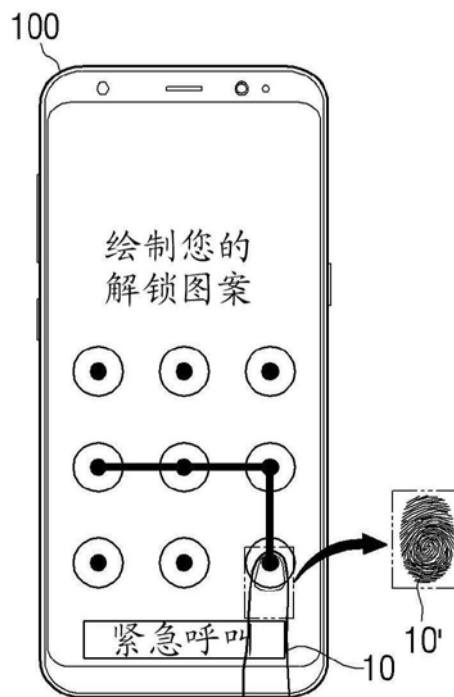


图10a

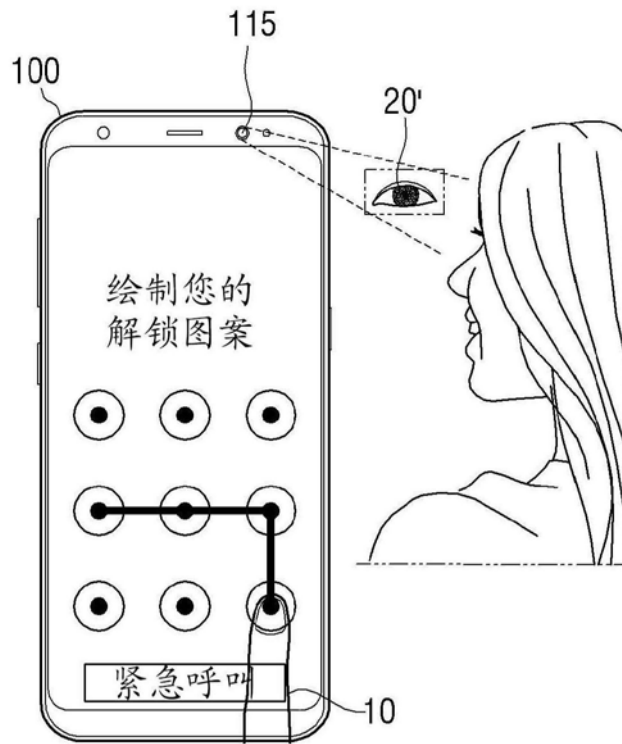


图10b

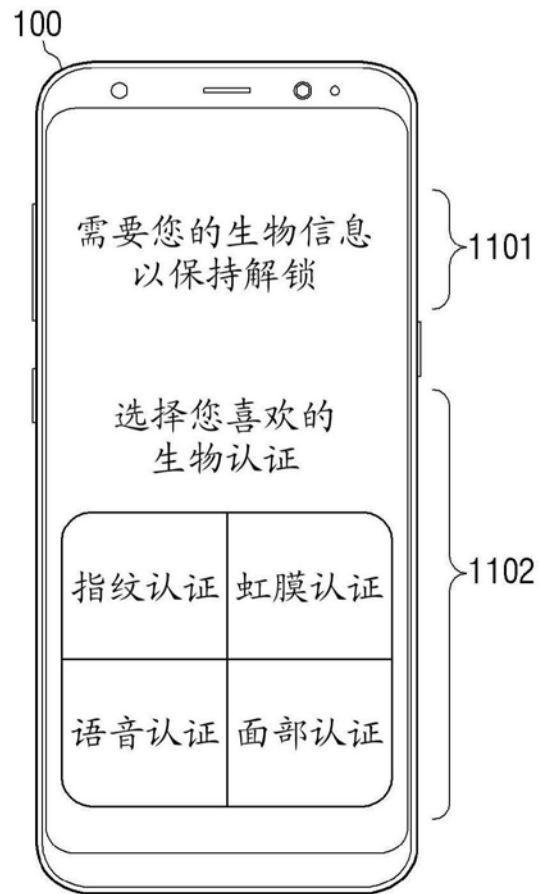


图11

100

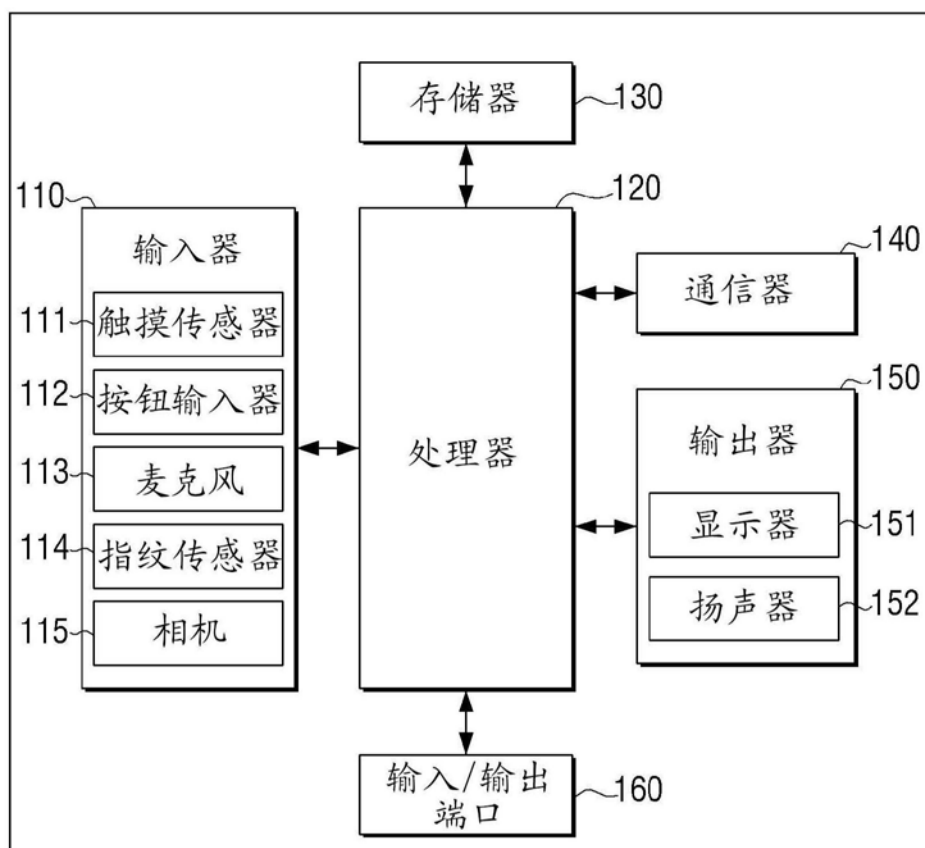


图12

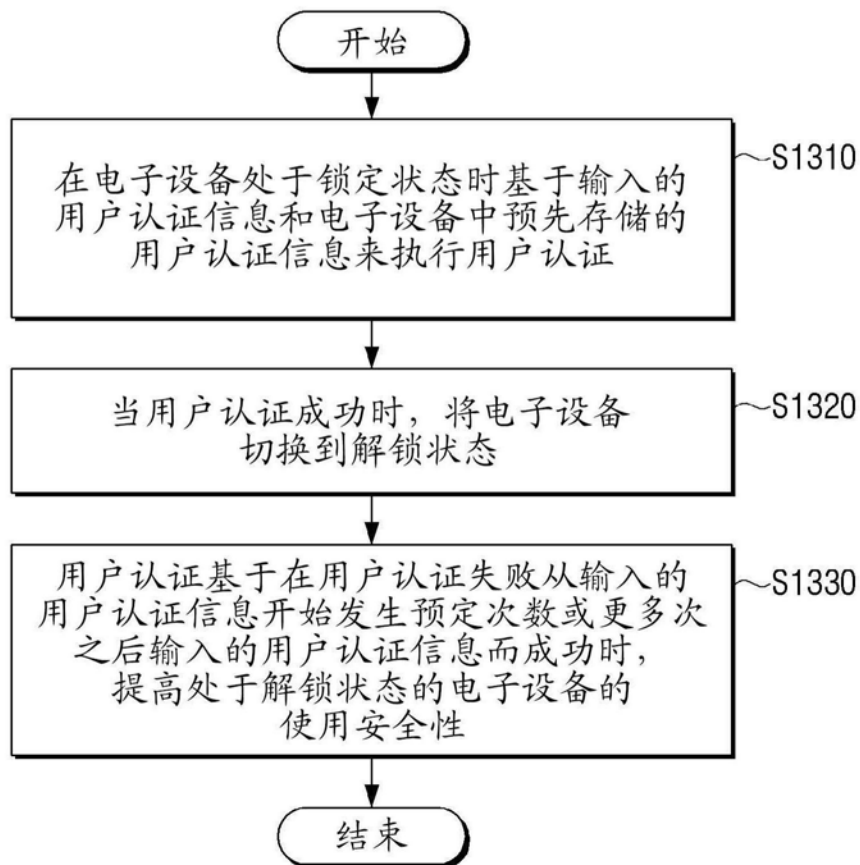


图13

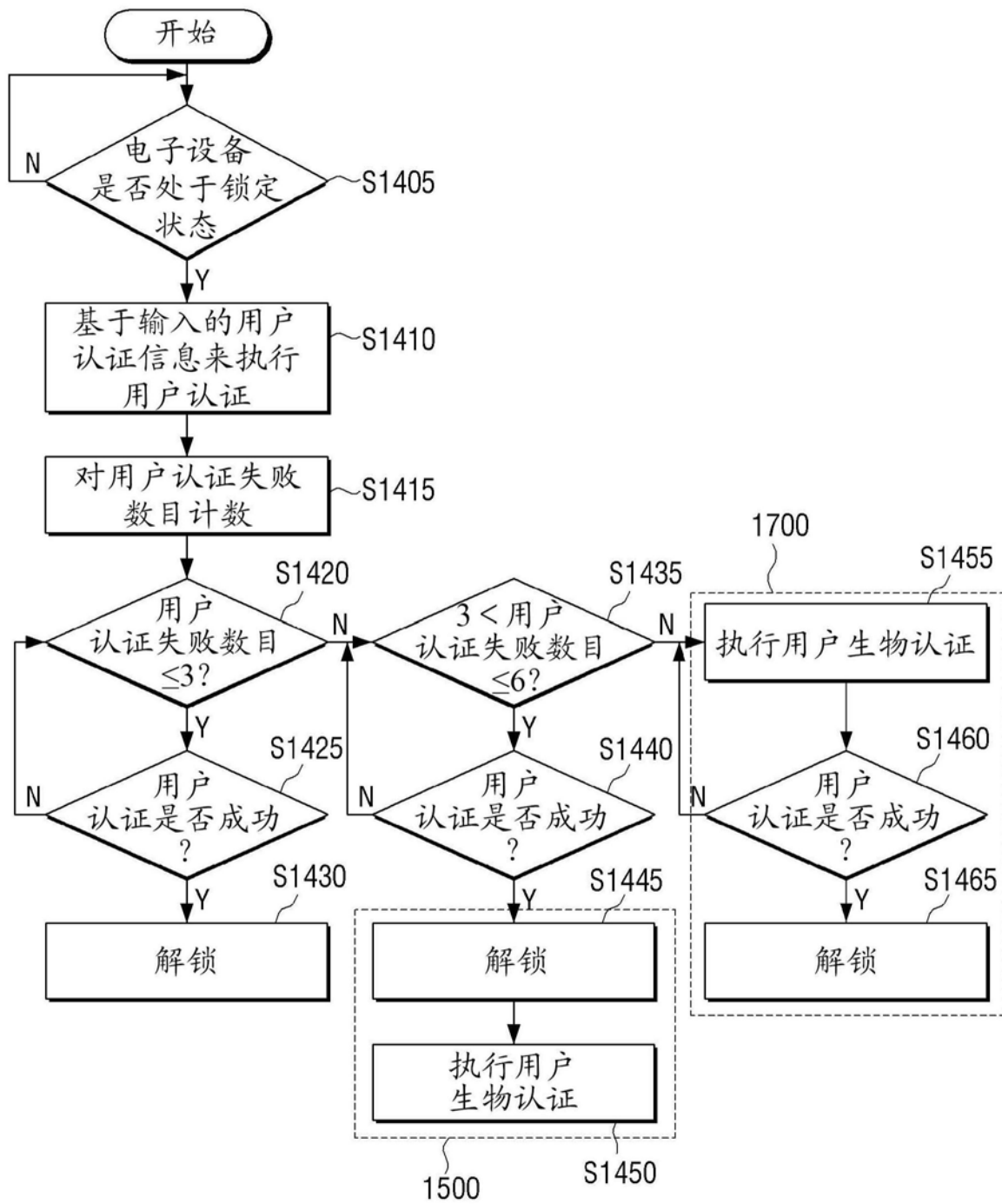


图14

1500

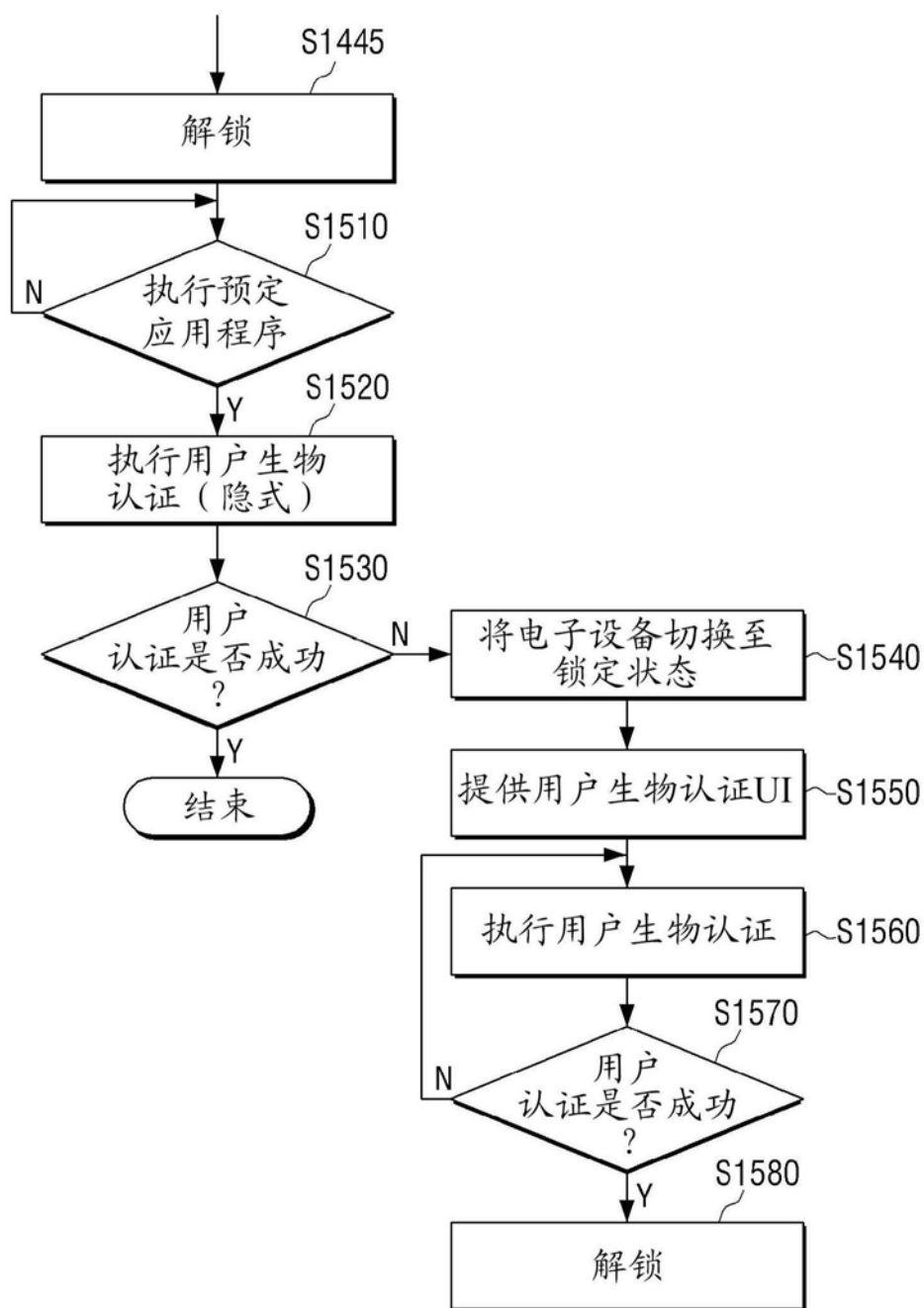


图15

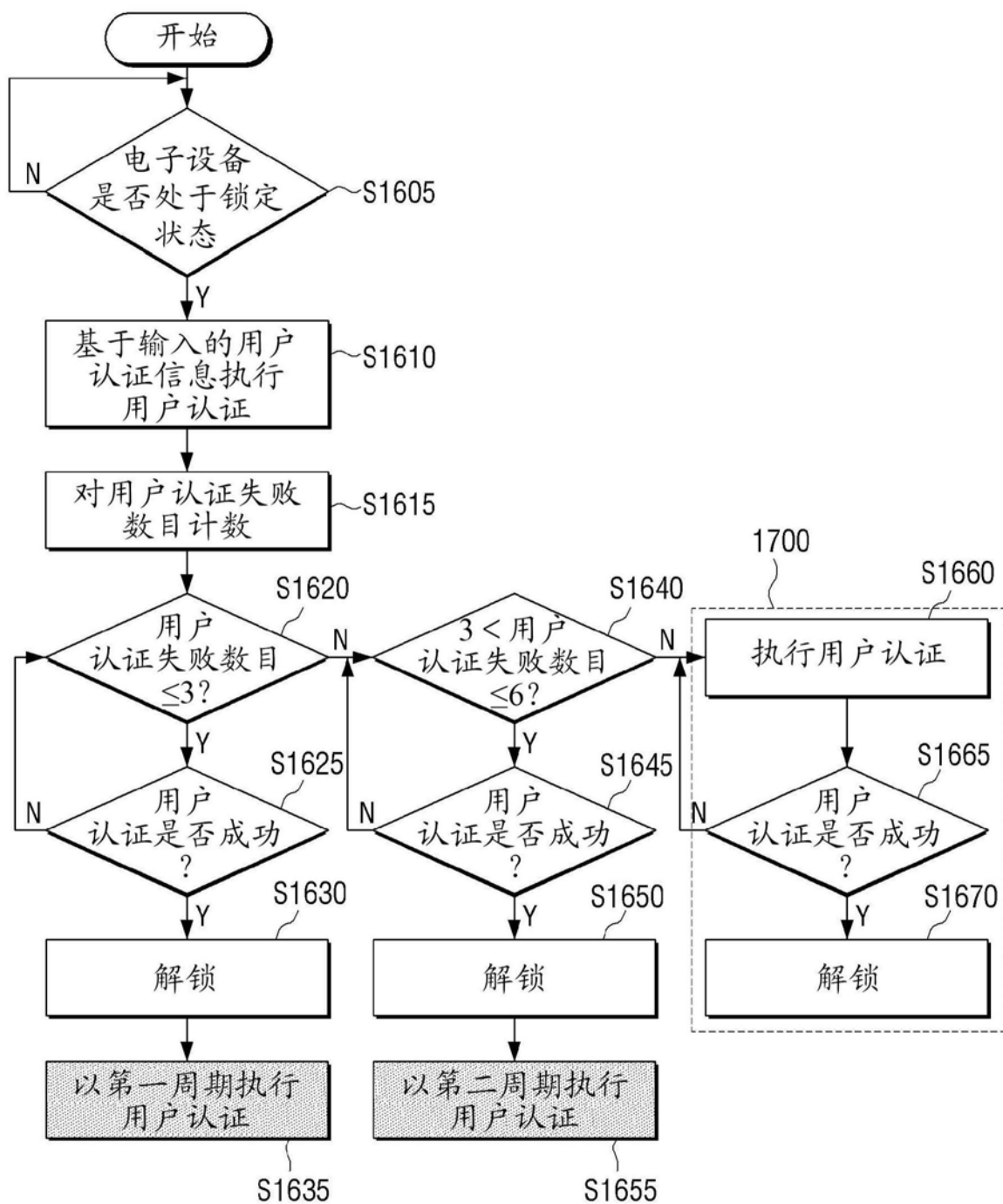


图16

1700

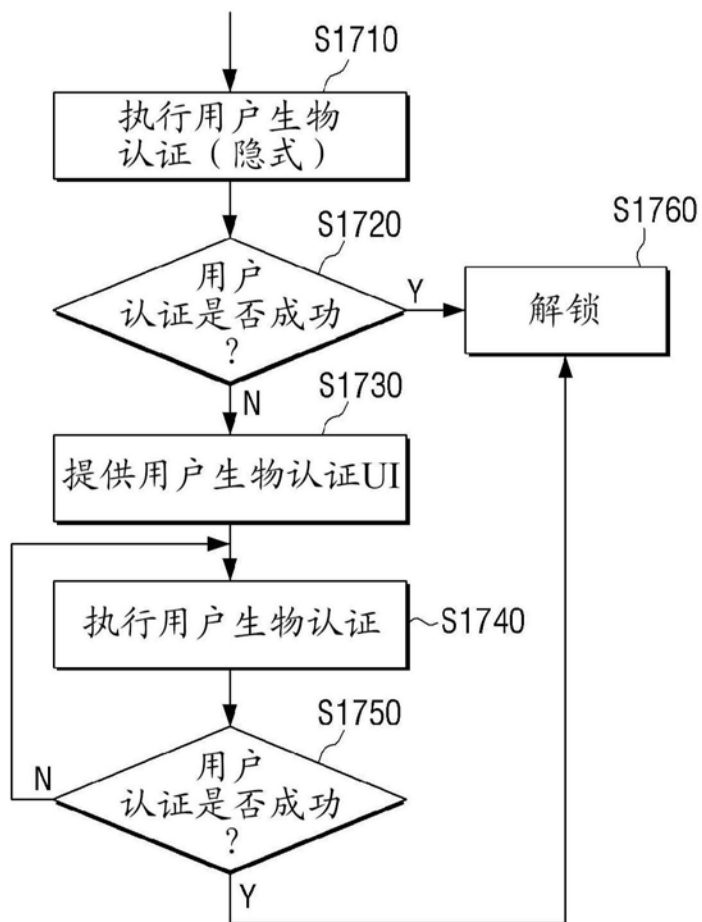


图17