(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106295268 B
(45)授权公告日 2020.01.31

(21)申请号 201510325047.X

(22)申请日 2015.06.12

(65)同一申请的已公布的文献号
申请公布号 CN 106295268 A

(43)申请公布日 2017.01.04

(73)专利权人 联想(北京)有限公司
地址 100085 北京市海淀区上地西路6号

(72)发明人 宋建华

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 安之斐

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/51(2013.01)

(56)对比文件
CN 103020509 A,2013.04.03,
CN 103793643 A,2014.05.14,
CN 104217142 A,2014.12.17,
US 2003107600 A1,2003.06.12,

审查员 叶珊

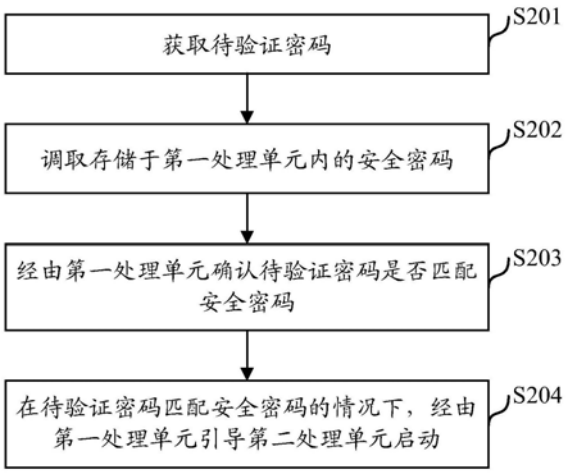
权利要求书2页 说明书6页 附图3页

(54)发明名称

信息处理方法和电子设备

(57)摘要

本发明公开了一种信息处理方法和使用该信息处理方法的电子设备。所述信息处理方法用于处理针对电子设备的操作请求的密码验证,所述信息处理方法包括:获取待验证密码;调取存储于第一处理单元内的安全密码;经由所述第一处理单元确认所述待验证密码是否匹配所述安全密码;在所述待验证密码匹配所述安全密码的情况下,经由所述第一处理单元引导第二处理单元启动。



CN 106295268 B

1.一种信息处理方法,用于处理针对电子设备的操作请求的密码验证,所述信息处理方法包括:

获取待验证密码;

调取存储于第一处理单元内的安全密码;

经由所述第一处理单元确认所述待验证密码是否匹配所述安全密码;

在所述待验证密码匹配所述安全密码的情况下,经由所述第一处理单元引导第二处理单元启动;

所述第二处理单元启动之后,控制显示安全密码设置用户界面,用于接收对于所述安全密码的安全密码设置和修改指令,

所述第一处理单元响应于所述安全密码设置和修改指令,设置是否启用所述安全密码和/或修改所述安全密码,

其中所述获取待验证密码包括:

响应于接收所述电子设备的操作系统的启动或唤醒指令,所述第一处理单元向控制器发送验证用户界面显示指令;

所述控制器基于所述验证用户界面显示指令,显示验证用户界面;

获取经由所述验证用户界面输入的待验证密码,

其中,所述控制器是所述电子设备的显示面板中的时序控制器。

2.如权利要求1所述的信息处理方法,还包括:

在所述待验证密码不匹配所述安全密码的情况下,所述第一处理单元控制关闭所述电子设备。

3.如权利要求1所述的信息处理方法,还包括:

在接收所述电子设备的操作系统的启动或唤醒指令之后,判断是否启用安全密码;

在启用安全密码的情况下,所述第一处理单元向所述控制器发送验证用户界面显示指令;

在不启用安全密码的情况下,所述第一处理单元引导所述第二处理单元启动。

4.如权利要求1所述的信息处理方法,其中所述第一处理单元为协处理器,所述第二处理单元为主处理器。

5.一种电子设备,包括:

第一处理单元,用于处理针对所述电子设备的操作请求的密码验证;

第二处理单元,用于运行所述电子设备的操作系统;

控制器,用于获取待验证密码;

其中,所述第一处理单元还包括第一存储子单元,用于存储安全密码;所述第一处理单元确认所述待验证密码是否匹配所述安全密码,并且在所述待验证密码匹配所述安全密码的情况下,所述第一处理单元引导所述第二处理单元启动,

其中所述第二处理单元启动之后,控制显示安全密码设置用户界面,用于接收对于所述安全密码的安全密码设置和修改指令,

所述第一处理单元响应于所述安全密码设置和修改指令,设置是否启用所述安全密码和/或修改所述安全密码,

其中所述获取待验证密码包括:

响应于接收所述电子设备的操作系统的启动或唤醒指令,所述第一处理单元向控制器发送验证用户界面显示指令;

所述控制器基于所述验证用户界面显示指令,显示验证用户界面;

获取经由所述验证用户界面输入的待验证密码,

其中,所述控制器是所述电子设备的显示面板中的时序控制器;

第一处理单元获取经由所述验证用户界面输入的待验证密码。

6.如权利要求5所述的电子设备,其中在所述待验证密码不匹配所述安全密码的情况下,所述第一处理单元控制关闭所述电子设备。

7.如权利要求5所述的电子设备,其中在接收所述电子设备的操作系统的启动或唤醒指令之后,所述第一处理单元判断是否启用安全密码;

在启用安全密码的情况下,所述第一处理单元向所述控制器发送验证用户界面显示指令;

在不启用安全密码的情况下,所述第一处理单元引导所述第二处理单元启动。

8.如权利要求5所述的电子设备,其中所述第一处理单元为协处理器,所述第二处理单元为主处理器。

信息处理方法和电子设备

技术领域

[0001] 本发明涉及密码信息处理领域，更具体地，本发明涉及一种信息处理方法和使用该信息处理方法的电子设备。

背景技术

[0002] 在现有的诸如笔记本电脑、个人计算机、服务器的电子设备中，不论是在其BIOS下设置的开机密码还是在电子设备的操作系统下设置的密码，都难以起到真正的防盗用功能。因为只要重新刷新BIOS或者重新安装电子设备的操作系统，盗用者就可以重置这些密码。

[0003] 因此，希望提供一种信息处理方法和使用该信息处理方法的电子设备，其通过利用现有硬件进行电子设备的密码信息的存储和验证，在现有硬件中存储的密码信息无法被盗用者通过重新刷新BIOS或者重新安装操作系统来重置，从而保证了电子设备及其内部数据的安全性。

发明内容

[0004] 有鉴于上述情况，本发明提供了一种信息处理方法和使用该信息处理方法的电子设备。

[0005] 根据本发明的一个实施例，提供了一种信息处理方法，用于处理针对电子设备的操作请求的密码验证，所述信息处理方法包括：获取待验证密码；调取存储于第一处理单元内的安全密码；经由所述第一处理单元确认所述待验证密码是否匹配所述安全密码；在所述待验证密码匹配所述安全密码的情况下，经由所述第一处理单元引导第二处理单元启动。

[0006] 此外，根据本发明的一个实施例的信息处理方法，其中所述获取待验证密码包括：响应于接收所述电子设备的操作系统的启动或唤醒指令，所述第一处理单元向控制器发送验证用户界面显示指令；所述控制器基于所述验证用户界面显示指令，显示验证用户界面；获取经由所述验证用户界面输入的待验证密码。

[0007] 此外，根据本发明的一个实施例的信息处理方法，还包括：在所述待验证密码不匹配所述安全密码的情况下，所述第一处理单元控制关闭所述电子设备。

[0008] 此外，根据本发明的一个实施例的信息处理方法，还包括：在接收所述电子设备的操作系统的启动或唤醒指令之后，判断是否启用安全密码；在启用安全密码的情况下，所述第一处理单元向所述控制器发送验证用户界面显示指令；在不启用安全密码的情况下，所述第一处理单元引导所述第二处理单元启动。

[0009] 此外，根据本发明的一个实施例的信息处理方法，还包括：所述第二处理单元启动之后，控制显示安全密码设置用户界面，用于接收对于所述安全密码的安全密码设置和修改指令，所述第一处理单元响应于所述安全密码设置和修改指令，设置是否启用所述安全密码和/或修改所述安全密码。

[0010] 此外，根据本发明的一个实施例的信息处理方法，其中所述第一处理单元为协处理器，所述第二处理单元为主处理器。

[0011] 根据本发明的另一实施例，提供了一种电子设备，包括：第一处理单元，用于处理针对所述电子设备的操作请求的密码验证；第二处理单元，用于运行所述电子设备的操作系统；控制器，用于获取待验证密码；其中，所述第一处理单元还包括第一存储子单元，用于存储安全密码；所述第一处理单元确认所述待验证密码是否匹配所述安全密码，并且在所述待验证密码匹配所述安全密码的情况下，所述第一处理单元引导所述第二处理单元启动。

[0012] 此外，根据本发明的另一实施例的电子设备，其中响应于接收所述电子设备的操作系统的启动或唤醒指令，所述第一处理单元向所述控制器发送验证用户界面显示指令；所述控制器基于所述验证用户界面显示指令，显示验证用户界面；所述第一处理单元获取经由所述验证用户界面输入的待验证密码。

[0013] 此外，根据本发明的另一实施例的电子设备，其中在所述待验证密码不匹配所述安全密码的情况下，所述第一处理单元控制关闭所述电子设备。

[0014] 此外，根据本发明的另一实施例的电子设备，其中在接收所述电子设备的操作系统的启动或唤醒指令之后，所述第一处理单元判断是否启用安全密码；在启用安全密码的情况下，所述第一处理单元向所述控制器发送验证用户界面显示指令；在不启用安全密码的情况下，所述第一处理单元引导所述第二处理单元启动。

[0015] 此外，根据本发明的另一实施例的电子设备，其中所述第二处理单元启动之后，控制显示安全密码设置用户界面，用于接收对于所述安全密码的安全密码设置和修改指令，所述第一处理单元响应于所述安全密码设置和修改指令，设置是否启用所述安全密码和/或修改所述安全密码。

[0016] 此外，根据本发明的另一实施例的电子设备，其中所述第一处理单元为协处理器，所述第二处理单元为主处理器。

[0017] 根据本发明实施例的信息处理方法和使用该信息处理方法的电子设备，其通过利用现有硬件进行电子设备的密码信息的存储和验证，在现有硬件中存储的密码信息无法被盗用者通过重新刷新BIOS或者重新安装操作系统来重置，从而保证了电子设备及其内部数据的安全性。

[0018] 要理解的是，前面的一般描述和下面的详细描述两者都是示例性的，并且意图在于提供要求保护的技术的进一步说明。

附图说明

[0019] 通过结合附图对本发明实施例进行更详细的描述，本发明的上述以及其它目的、特征和优势将变得更加明显。附图用来提供对本发明实施例的进一步理解，并且构成说明书的一部分，与本发明实施例一起用于解释本发明，并不构成对本发明的限制。在附图中，相同的参考标号通常代表相同部件或步骤。

[0020] 图1是图示根据本发明实施例的电子设备的功能框图。

[0021] 图2是图示根据本发明实施例的信息处理方法的流程图。

[0022] 图3是进一步图示根据本发明实施例的电子设备的示意图。

[0023] 图4是进一步图示根据本发明实施例的信息处理方法的详细流程图。

具体实施方式

[0024] 为了使得本发明的目的、技术方案和优点更为明显，下面将参照附图详细描述根据本发明的示例实施例。显然，所描述的实施例仅仅是本发明的一部分实施例，而不是本发明的全部实施例，应理解，本发明不受这里描述的示例实施例的限制。基于本公开中描述的本发明实施例，本领域技术人员在没有付出创造性劳动的情况下所得到的所有其它实施例都应落入本发明的保护范围之内。

[0025] 以下，将参考附图详细描述本发明的优选实施例。

[0026] 图1是图示根据本发明实施例的电子设备的功能框图。所述电子设备1例如是笔记本计算机、桌面型计算机、服务器等。如图1所示，根据本发明实施例的电子设备1具有第一处理单元10、第二处理单元20和控制器30。

[0027] 具体地，所述第一处理单元10用于处理针对所述电子设备1的操作请求的密码验证。在本发明的一个实施例中，所述第一处理单元10可以是所述电子设备1的协处理器(例如，嵌入式处理器EC)。所述第二处理单元20用于运行所述电子设备1的操作系统。在本发明的一个实施例中，所述第二处理单元20可以是所述电子设备1的主处理器(例如，中央处理单元CPU)。所述控制器30用于获取待验证密码。在本发明的一个实施例中，所述控制器30可以是所述电子设备1的显示面板中的时序控制器(例如，T-con)。进一步地，如图1所示，所述第一处理单元10还具有第一子存储单元11，用于存储安全密码，所述安全密码是预先设置并且存储在所述第一子存储单元11中的。在本发明的一个实施例中，所述第一子存储单元11是所述电子设备1的协处理器中的安全闪存区。

[0028] 在本发明的一个实施例中，当所述电子设备1的所述第二处理单元20(主处理单元)处于关机/休眠状态时，所述第一处理单元10(从处理单元)负责从所述电子设备1的用户接收启动/唤醒指令。所述第一处理单元10(从处理单元)响应于接收到对于所述电子设备的操作系统的启动或唤醒指令，向所述控制器30发送验证用户界面显示指令。所述控制器30基于所述验证用户界面显示指令，显示验证用户界面，所述第一处理单元10获取经由所述验证用户界面输入的待验证密码。所述第一处理单元10确认所述待验证密码是否匹配其内部第一子存储单元11中预先存储的所述安全密码，并且在所述待验证密码匹配所述安全密码的情况下，所述第一处理单元10引导所述第二处理单元20启动/唤醒。在所述待验证密码不匹配所述安全密码的情况下，所述第一处理单元10将结束密码验证，并且控制关闭所述电子设备1。

[0029] 因此，在如图1所示的电子设备1的架构中，通过在所述第一处理单元10(从处理单元)的第一子存储单元11(安全闪存区)中存储安全密码，由于该第一子存储单元11(安全闪存区)不能通过刷新BIOS或者重装所述电子设备1的操作系统来重置，从而确保所述电子设备1的密码安全。

[0030] 图2是图示根据本发明实施例的信息处理方法的流程图。如图2所示，根据本发明实施例的信息处理方法包括以下步骤。

[0031] 在步骤S201中，获取待验证密码。如上参照图1所述，所述控制器30用于获取待验证密码。此后，处理进到步骤S202。

[0032] 在步骤S202中，调取存储于第一处理单元内的安全密码。如上参照图1所述，所述第一处理单元10(从处理单元)从第一子存储单元11(安全闪存区调取预先存储的安全密码。此后，处理进到步骤S203。

[0033] 在步骤S203中，经由第一处理单元确认待验证密码是否匹配安全密码。如上参照图1所述，所述第一处理单元10(从处理单元)比对在步骤S201中获取的待验证密码与在步骤S202中调取的安全密码。此后，处理进到步骤S204。

[0034] 在步骤S204中，在待验证密码匹配安全密码的情况下，经由第一处理单元引导第二处理单元启动。如上参照图1所述，如果在步骤S201中获取的待验证密码与在步骤S202中调取的安全密码匹配，则所述第一处理单元10引导所述第二处理单元20启动/唤醒。

[0035] 以上，参照图1和图2概述了根据本发明实施例的电子设备及其信息处理方法。以下，将参照图3和图4进一步详细描述根据本发明实施例的电子设备配置示例和具体密码验证流程。

[0036] 图3是进一步图示根据本发明实施例的电子设备的示意图。如图3所示的电子设备3例如是笔记本计算机。所述电子设备3包括EC 31、显示面板32、CPU 33和键盘34。

[0037] 具体地，所述EC 31对应于图1所示的所述第一处理单元10，所述EC 31中设置的安全闪存301对应于图1所示的第一子存储单元11。所述显示面板32中设置的T-con 302对应于图1所示的所述控制器30。所述CPU 33则对应于图1所示的所述第二处理单元20。

[0038] 例如，用户通过按压电源按钮(或者触摸鼠标或者键盘等)输入操作系统启动/唤醒指令时，所述EC 31向所述显示面板32发送验证用户界面显示指令。所述显示面板32中的T-con 302调用其ROM中预先存储的几帧画面(验证用户界面)，并且在所述显示面板32上显示所述验证用户界面。用户基于显示的所述验证用户界面，通过所述键盘34输入待验证密码。所述EC 31将经由所述键盘34输入待验证密码与其安全闪存301中预先存储的安全密码执行比对验证。当所述输入待验证密码与其安全闪存301中预先存储的安全密码匹配时，所述EC 31将引导所述CPU 33完成操作系统启动/唤醒。相反地，在所述输入待验证密码与其安全闪存301中预先存储的安全密码不匹配时，所述EC 31将结束密码验证，并且控制关闭所述电子设备3。

[0039] 此外，在操作系统启动/唤醒之后，所述CPU 33可以控制所述显示面板32显示安全密码设置用户界面。用户基于显示的所述安全密码设置用户界面，通过所述键盘34(或者鼠标等其他输入输出设备)，对于所述安全密码进行设置和修改。所述EC 31响应于所述安全密码设置和修改，设置是否启用所述安全密码和/或修改所述安全密码。

[0040] 因此，在如图3所示的电子设备3的具体示例中，通过在所述EC 31的所述安全闪存301中存储安全密码，由于该安全闪存301不能通过刷新BIOS或者重装所述电子设备3的操作系统来重置，从而确保所述电子设备3的密码安全。此外，所述电子设备3进一步通过所述显示面板32执行验证用户界面以及安全密码设置用户界面的显示，便于用户进行待验证密码的输入，以及安全密码的设置。

[0041] 图4是进一步图示根据本发明实施例的信息处理方法的详细流程图。如图4所示，根据本发明实施例的信息处理方法包括以下步骤：

[0042] 在步骤S401中，接收电子设备的操作系统的启动或唤醒指令。如上所述，用户通过按压电源按钮(或者触摸鼠标或者键盘等)输入操作系统启动/唤醒指令。此后，处理进到步

骤S402。

[0043] 在步骤S402中，判断是否启用安全密码。例如，用户可以预先通过由所述显示面板32显示的安全密码设置用户界面，进行是否启用安全密码的设置。

[0044] 如果在步骤S402中获得肯定结果，即已经启用安全密码，则处理进到步骤S403。

[0045] 在步骤S403中，控制器基于验证用户界面显示指令，显示验证用户界面。例如，所述显示面板32中的T-con 302调用其ROM中预先存储的几帧画面(验证用户界面)，并且在所述显示面板32上显示所述验证用户界面。此后，处理进到步骤S404。

[0046] 在步骤S404中，获取经由验证用户界面输入的待验证密码。例如，用户基于显示的所述验证用户界面，通过所述键盘34输入待验证密码。此后，处理进到步骤S405。

[0047] 在步骤S405中，调取存储于第一处理单元内的安全密码。例如，所述EC 31调取其安全闪存301中预先存储的安全密码。此后，处理进到步骤S406。

[0048] 在步骤S406中，判断待验证密码是否匹配所述安全密码。例如，所述EC 31将经由所述键盘34输入待验证密码与其安全闪存301中预先存储的安全密码执行比对验证。

[0049] 如果在步骤S406中获得肯定结果，即经由所述键盘34输入待验证密码与安全闪存301中预先存储的安全密码匹配，则处理进到步骤S407。

[0050] 在步骤S407中，第一处理单元引导第二处理单元启动。例如，所述EC31将引导所述CPU 33完成操作系统启动/唤醒。

[0051] 相反地，如果在步骤S406中获得否定结果，即经由所述键盘34输入待验证密码与安全闪存301中预先存储的安全密码不匹配，则处理进到步骤S408。

[0052] 在步骤S408中，第一处理单元控制关闭电子设备。例如，所述EC 31将结束密码验证，并且控制关闭所述电子设备。

[0053] 返回步骤S402，如果在步骤S402中获得否定结果，即没有启用安全密码，则处理直接进到步骤S407，所述EC 31将引导所述CPU 33完成操作系统启动/唤醒。

[0054] 在步骤S407之后，即操作系统启动/唤醒之后，处理可以进到步骤S409。

[0055] 在步骤S409中，控制显示安全密码设置用户界面。例如，所述CPU 33可以控制所述显示面板32显示安全密码设置用户界面。用户基于显示的所述安全密码设置用户界面，通过所述键盘34(或者鼠标等其他输入输出设备)，对于所述安全密码进行设置和修改。所述EC 31响应于所述安全密码设置和修改，设置是否启用所述安全密码和/或修改所述安全密码。

[0056] 以上，参照图1到图4描述了根据本发明实施例的信息处理方法和使用该信息处理方法的电子设备，其通过利用现有硬件进行电子设备的密码信息的存储和验证，在现有硬件中存储的密码信息无法被盗用者通过重新刷新BIOS或者重新安装操作系统来重置，从而保证了电子设备及其内部数据的安全性。

[0057] 需要说明的是，在本说明书中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0058] 最后，还需要说明的是，上述一系列处理不仅包括以这里所述的顺序按时间序列

执行的处理，而且包括并行或分别地、而不是按时间顺序执行的处理。

[0059] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的硬件平台的方式来实现，当然也可以全部通过硬件来实施。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0060] 以上对本发明进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

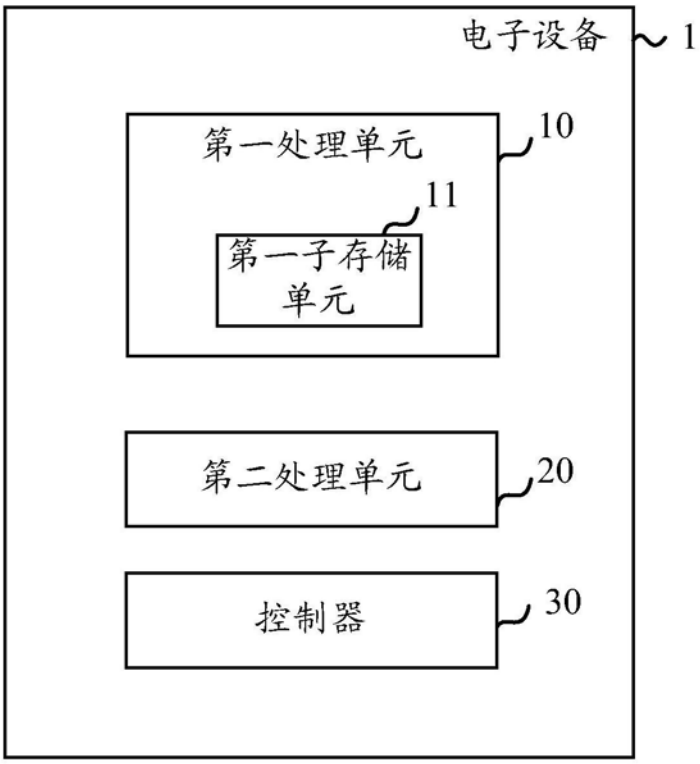

电子设备
1
第一处理单元
10
11
第一子存储单元
第二处理单元
20
控制器
30

图1

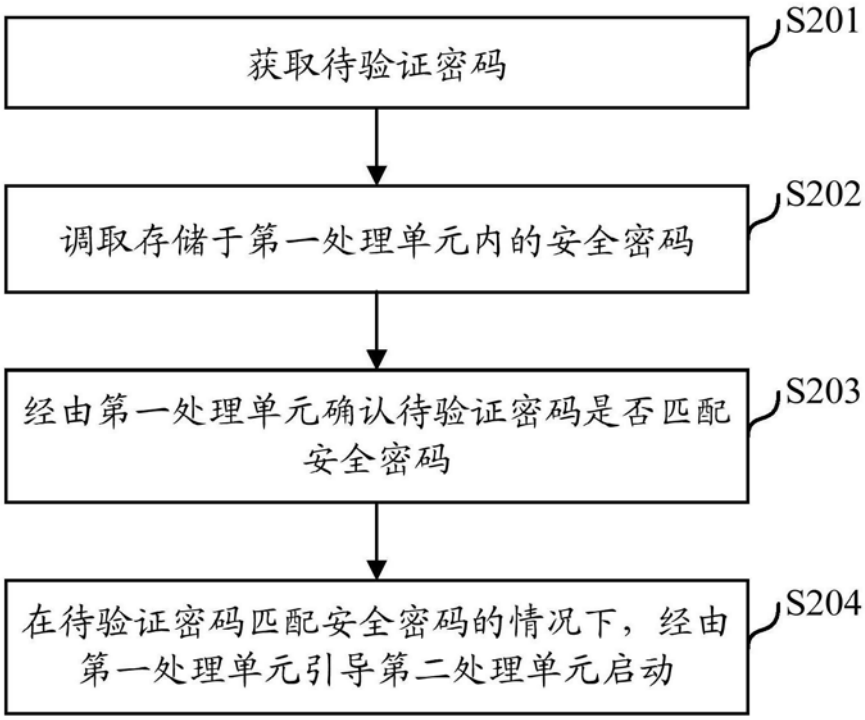

获取待验证密码
S201
调取存储于第一处理单元内的安全密码
S202
经由第一处理单元确认待验证密码是否匹配安全密码
S203
在待验证密码匹配安全密码的情况下，经由第一处理单元引导第二处理单元启动
S204

图2

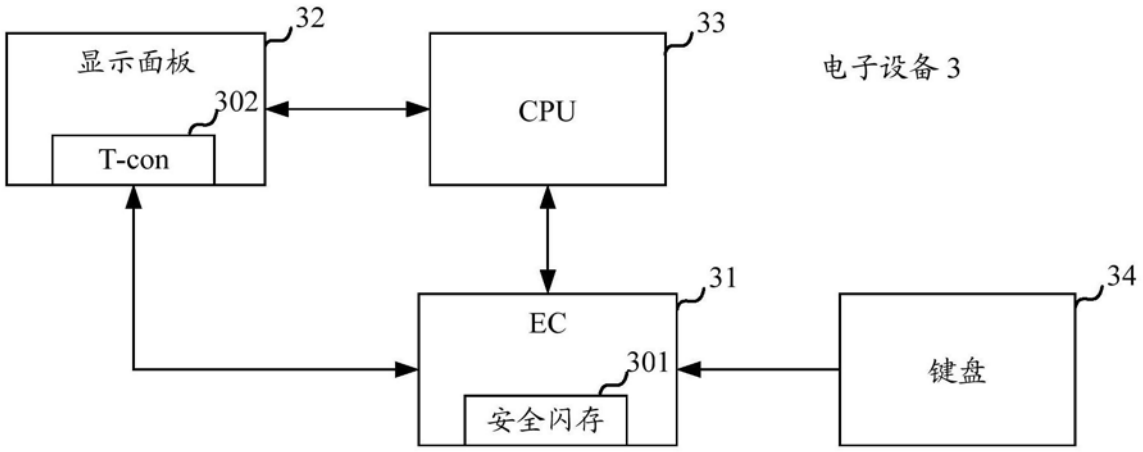


图3

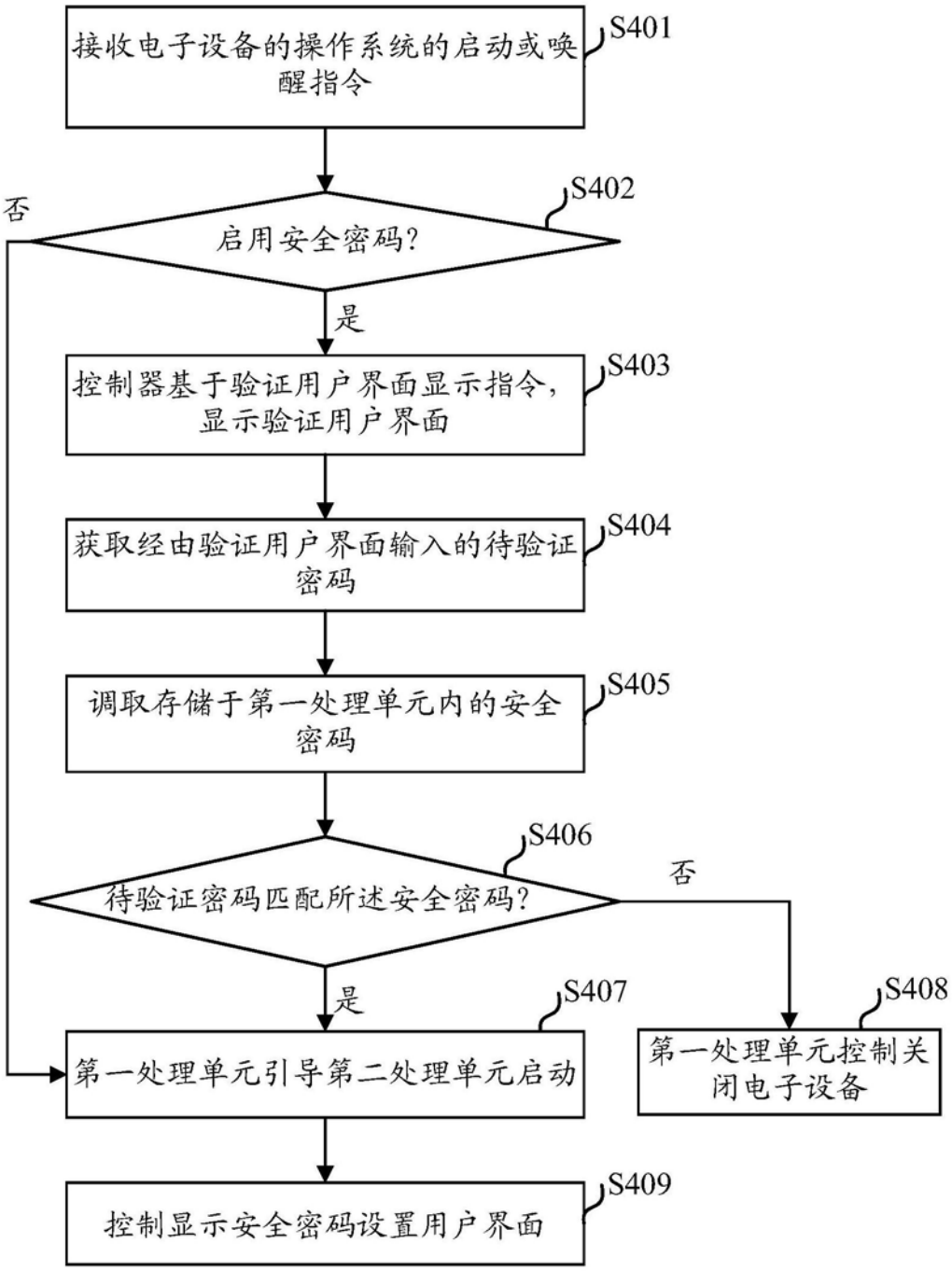

接收电子设备的操作系统的启动或唤醒指令
S401
启用安全密码?
S402
否
是
控制器基于验证用户界面显示指令，显示验证用户界面
S403
获取经由验证用户界面输入的待验证密码
S404
调取存储于第一处理单元内的安全密码
S405
待验证密码匹配所述安全密码?
S406
否
是
第一处理单元引导第二处理单元启动
S407
第一处理单元控制关闭电子设备
S408
控制显示安全密码设置用户界面
S409

图4