



(12) 发明专利

(10) 授权公告号 CN 1801708 B

(45) 授权公告日 2011. 05. 11

(21) 申请号 200510076385. 0

(22) 申请日 2005. 06. 10

(30) 优先权数据

2005-000122 2005. 01. 04 JP

(73) 专利权人 富士通株式会社

地址 日本神奈川县

(72) 发明人 青山进 中岛佑子 高桥知彦

(74) 专利代理机构 隆天国际知识产权代理有限公司
72003

代理人 张龙哺 郑特强

(51) Int. Cl.

H04L 9/32 (2006. 01)

G06K 9/00 (2006. 01)

(56) 对比文件

US 5699514 A, 1997. 12. 16, 全文.

US 2004/0250074 A1, 2004. 12. 09, 说明书第 23 段.

US 2003/0005336 A1, 说明书第 53-59 段, 图 10.

CN 1299113 A, 2001. 06. 13, 全文.

审查员 高静

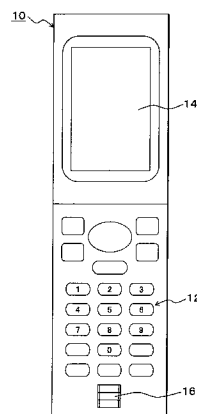
权利要求书 1 页 说明书 7 页 附图 10 页

(54) 发明名称

安全管理方法和信息设备

(57) 摘要

本发明提供安全管理方法、程序和信息设备。在设置指纹认证模式的状态中, 指纹认证单元按照输入指令鉴别指纹输入, 如果认证成功则进行解锁, 如果认证失败就指示另一指纹输入, 并且如果指纹认证连续失败预定次数则确定为未授权使用并将模式切换到 PIN 码认证模式。在 PIN 码认证模式的状态中, PIN 码认证单元按照输入指令鉴别 PIN 码输入, 如果认证成功则进行解锁, 如果认证失败就指示另一 PIN 码输入, 并且如果认证连续失败预定次数就确定为未授权使用并关闭电源。而且, 当 PIN 码认证单元已经关闭电源之后再次开启电源时, 指纹认证单元设置设定了指纹认证模式的状态, 即使指纹认证连续失败预定次数, 也保持指纹认证模式。



1. 一种信息设备安全管理方法,其能通过使用指纹认证限制对特定信息的访问,该安全管理方法包括:

指纹认证步骤,进行指纹认证,并且如果指纹认证失败了预定次数,则启动 PIN 码认证;以及

在该指纹认证步骤被切换到 PIN 码认证之后的 PIN 码认证步骤,进行 PIN 码认证,并且如果 PIN 码认证失败了预定次数,则启动认证失败标志从而仅能够执行指纹认证方式的认证,当随后的指纹认证成功时,所述认证失败标志被清除。

2. 如权利要求 1 所述的方法,其中,在所述 PIN 码认证步骤中,该 PIN 码认证的失败次数被存储于非易失性物质中,并且如果在该 PIN 码认证次数达到预定次数之前关闭电源然后再次开启电源,则以所存储的失败次数作为初始值来对该 PIN 码认证的失败次数进行计数。

3. 如权利要求 1 所述的方法,其中,

在所述指纹认证步骤中,当切换到 PIN 码认证时,该指纹认证的失败次数被清除。

4. 一种信息设备安全管理设备,其能通过使用指纹认证限制对特定信息的访问,该安全管理设备包括:

指纹认证单元,进行指纹认证,并且如果指纹认证失败了预定次数,则启动 PIN 码认证;以及

PIN 码认证单元,在该指纹认证单元切换到 PIN 码认证之后,进行 PIN 码认证,并且如果 PIN 码认证失败了预定次数,则启动认证失败标志从而仅能够执行指纹认证方式的认证,当随后的指纹认证成功时,所述认证失败标志被清除。

5. 如权利要求 4 所述的设备,其中,在所述 PIN 码认证单元中,该 PIN 码认证的失败次数被存储于非易失性物质中,并且如果在该 PIN 码认证次数达到预定次数之前关闭电源然后再次开启电源,则以所存储的失败次数作为初始值来对该 PIN 码认证的失败次数进行计数。

6. 如权利要求 4 所述的设备,其中,

所述指纹认证单元在切换到 PIN 码认证时,清除该指纹认证的失败次数。

安全管理方法和信息设备

[0001] 本申请要求 2005 年 1 月 4 日在日本提交的在先申请号 JP2005-122 的优先权。

技术领域

[0002] 本发明涉及一种含有指纹认证功能的安全管理方法、程序和例如便携式电话设备的信息设备,特别地,本发明涉及一种含有仅指纹认证功能的安全管理方法、程序和信息设备。

背景技术

[0003] 传统地,指纹认证功能已经在便携式终端设备,例如便携式电话和 PDA 的安全管理中,并且结合 PIN 码认证功能来使用传统的指纹认证功能。

[0004] 在结合 PIN 码使用的指纹认证功能中,为了弥补指纹认证的失败,例如当指纹认证连续出现十次失败时,就切换为 PIN 码认证。因此,即使例如由于指纹传感器上的污点而导致指纹认证连续失败时,由于自动切换为 PIN 码认证,用户也能够通过输入 PIN 码来进行解锁,从而启动例如应用程序等。而且,为了防止通过未经授权的使用而进行的解锁,当由于指纹认证失败而切换到 PIN 码认证,并且当 PIN 码认证连续出现例如五次失败时,电源即被强制关闭,从而使得该设备不会再被使用。

[0005] 然而,在通过指纹认证方式的这种传统安全管理方法中,尽管电源在组合使用的指纹认证和 PIN 码认证出现失败时被强制关闭,但是当电源被再次开启时,指纹认证和 PIN 码认证就会被重复并且连续执行,直到达到所设定的失败次数。如果已经设定四位 PIN 码用于组合使用,即使提供有指纹认证功能,安全性能也与 PIN 码认证属于相同级别。因此,存在不能充分利用指纹认证所带来的高安全性能的问题。

发明内容

[0006] 基于本发明,提供一种安全管理方法、程序和信息设备,用于加强指纹认证的安全性能。

[0007] 本发明提供一种信息设备安全管理方法。在通过使用指纹认证来限制对特定信息的访问的安全管理方法中,本发明包括:

[0008] 指纹认证步骤,其执行指纹认证,并且如果指纹认证失败预定次数,则启动 PIN 码认证;以及

[0009] 在将指纹认证步骤切换为 PIN 码认证之后的 PIN 码认证步骤,其执行 PIN 码认证,并且如果 PIN 码认证失败预定次数,则启动认证失败标志,从而只能执行通过指纹认证方式的认证,当随后的指纹认证成功时,所述认证失败标志被清除。

[0010] 这里,在 PIN 码认证步骤中, PIN 码认证的失败次数存储在非易失性物质中,并且如果电源在 PIN 码认证次数达到预定次数之前被关闭,然后电源被再次开启,则以存储的失败次数作为初始值来对 PIN 码认证的失败次数进行计数。在指纹认证步骤中,当切换为 PIN 码认证时,指纹认证的失败次数被清除。

[0011] 在本发明的信息设备安全管理方法中,用于确定未授权使用的 PIN 码认证的失败次数被设定为小于用于确定未授权使用的指纹授权的失败次数。

[0012] 本发明提供一种由信息设备的计算机执行的程序。本发明的程序使得信息设备的计算机执行:

[0013] 指纹认证步骤,其执行指纹认证,并且如果指纹认证失败预定次数,则启动 PIN 码认证;以及

[0014] 在将指纹认证步骤切换为 PIN 码认证之后的 PIN 码认证步骤,其执行 PIN 码认证,并且如果 PIN 码认证失败预定次数,则启动认证失败标志,从而只能执行通过指纹认证方式的认证。

[0015] 本发明提供一种安全管理设备,能够通过使用指纹认证来限制对特定信息的访问。本发明的安全管理设备包括:

[0016] 指纹认证单元,其执行指纹认证,并且如果指纹认证失败预定次数,则启动 PIN 码认证;以及

[0017] 在将指纹认证单元切换为 PIN 码认证之后,PIN 码认证单元执行 PIN 码认证,并且如果 PIN 码认证失败预定次数,则启动认证失败标志,从而只能执行通过指纹认证方式的认证,当随后的指纹认证成功时,所述认证失败标志被清除。

[0018] 请注意,本发明的程序和安全设备的细节与本发明的安全管理方法的细节基本相同。

[0019] 基于本发明,通过仅利用指纹来实现认证,能够充分利用指纹认证所带来的高安全性能。而且,在指纹认证由于例如传感器等上的污点或故障而导致不能正常工作的情况下提供 PIN 码认证作为备份,由此有助于在指纹认证不能工作的情况下进行恢复。依靠通过提供指纹认证和作为备份的 PIN 码认证而实现的安全的加强,当由于未授权使用而导致指纹认证失败预定次数并且切换为 PIN 码认证,并且 PIN 码认证也失败预定次数时,在非易失性物质中开启认证失败标志。随后,仅以指纹认证模式进行认证。结果,能够消除通过进一步的 PIN 码输入而带来的未授权使用的机会。而且,当由于未授权使用而导致 PIN 码重复输入多次,并且在已经从指纹认证切换为 PIN 码认证的状态中 PIN 码认证失败时,PIN 码认证的失败次数被存储在非易失性物质中,以便处理在它到达预定次数之前再次开启电源时的未授权使用。因此,当再次开启电源后,在指纹认证失败预定次数之后切换为 PIN 码认证时,以存储在非易失性物质中的前一次的失败次数作为初始值来对失败次数进行计数。因此,即使电源被再次开启,PIN 码的失败次数也总是限制在预先设定的预定次数,此时认证仅固定于指纹认证。因此,即使提供 PIN 码作为备份,也能充分加强安全性。从参照附图的下述具体描述中,本发明的上述和其他目的、特征和优点将变得明显。

[0020] 附图说明

[0021] 图 1 是本发明所应用到的作为便携式终端设备的便携式电话的说明图;

[0022] 图 2 是具有本发明的功能配置的便携式终端设备的框图;

[0023] 图 3 是在图 2 的认证处理单元中的操作模式设置处理的流程图;

[0024] 图 4A 和 4B 是对应于图 3 的操作模式设置处理的屏幕说明图;

[0025] 图 4C 是图 4A 和 4B 之后的屏幕说明图;

[0026] 图 5A 和 5B 是在“仅使用指纹”被设置为操作模式时,基于本发明的指纹认证处理

的流程图；

[0027] 图 6A 和 6B 是当“与 PIN 码结合使用”被设置为操作模式时，组合认证处理的流程图；以及

[0028] 图 7 是当“不使用”被设置为操作模式时，PIN 码认证处理的流程图。

具体实施方式

[0029] 图 1 是本发明所应用到的便携式终端设备的说明图，其中以便携式电话作为一个实例。在图 1 中，本发明的便携式终端设备 10 是例如便携式电话，并且具有输入操作单元 12 和液晶显示器 14，其中在输入操作单元 12 下方提供指纹传感器 16。

[0030] 图 2 是具有本发明的功能配置的便携式终端设备的框图，其中采用对应于图 1 的便携式电话的功能配置作为一个实例。在图 2 中，在便携式终端设备 10 中提供基带处理单元 18。从基带处理单元 18 输出的音频信号在扬声器放大器 20 处被放大，并且提供给扬声器 22。同时，来自麦克风 24 的音频信号在麦克风放大器 26 处被放大，然后输入到基带处理单元 18。

[0031] 在便携式终端设备 10 中提供认证处理单元 28，并且来自为指纹传感器 16 提供的传感器控制单元 30 的输出信号被输入到认证处理单元 28。经由总线 32 为认证处理单元 28 提供基带处理单元 18、无线发射和接收单元 34、LED 显示单元 38、液晶显示器 14、输入操作单元 12、RAM40 以及采用闪存的非易失性存储器 42。在无线发射和接收单元 34 提供天线 36，其按照 W-CDMA 方法的移动通信来执行发射和接收处理。

[0032] 通过执行由 MPU 运行的认证处理程序的处理，而实现认证处理单元 28 的功能。认证处理单元 28 具有操作模式设置单元 44、第一指纹认证单元 46、第二指纹认证单元 48、以及 PIN 码认证单元 50 的功能。操作模式设置单元 44 实现指纹认证所需的指纹登记，以及操作模式的选择和设置。可由操作模式设置单元 44 设置的操作模式包括下述三种模式：

[0033] (1) 仅使用指纹的认证模式

[0034] (2) 结合 PIN 码使用指纹的认证模式

[0035] (3) 通过 PIN 码而不使用指纹的认证模式

[0036] 这些认证操作模式通过在用户初始登记指纹时执行的操作而被选择，并且在选择上述 (1) 的“仅使用指纹的认证模式”时，本发明的指纹认证处理被实现为第一指纹认证单元 46、第二指纹认证单元 48 以及 PIN 码认证单元 50 的功能。另一方面，上述 (2) 的“结合 PIN 码使用指纹的认证模式”和 (3) 的“通过 PIN 码而不使用指纹的认证模式”与传统的认证操作模式相同。

[0037] 在本发明提供的“仅使用指纹的认证模式”中，指纹认证单元 46 和 PIN 码认证单元 50 具有下述处理功能。

[0038] 首先，在指纹认证模式的状态中，指纹认证单元 46 通过按照使用液晶显示器 14 的屏幕的输入指令而从指纹传感器 16 进行指纹输入，并与先前登记的指纹比较核对，从而执行认证。如果认证成功，则会解锁需要认证处理的适当的应用程序，例如 Felica 芯片的应用程序；以及如果认证失败，则会指示再输入一次指纹，并且如果指纹认证连续失败预定次数，例如连续失败十次，则切换到 PIN 码认证模式。这里，指纹认证限制对特定信息的访问，并且作为对象的信息是需要安全性的适当信息，比如地址簿、个人信息、电子货币和电子价

格。在已经从指纹认证模式切换到 PIN 码认证模式的状态中, PIN 码认证单元 50 通过按照使用液晶显示器 14 的屏幕显示器的输入指令而从输入操作单元 12 进行 PIN 码的输入, 并与先前登记的 PIN 码比较核对, 从而执行认证; 以及如果认证成功则进行解锁, 而如果认证失败则指示再次输入 PIN 码。如果认证连续失败预定次数, 例如连续失败五次, PIN 码认证单元确定这是未授权的使用, 开启认证失败标志 45 并且将其存入非易失性存储器 42, 然后, 强制关闭便携式终端设备 10 的电源。

[0039] 而且, 在每次失败时, PIN 码认证单元 50 都会将 PIN 码认证的失败次数存入非易失性存储器 42 作为 PIN 码失败次数 72, 并且, 当要开始对 PIN 码认证的失败次数计数时, 总是使用非易失性存储器 42 中的 PIN 码失败次数 72 作为初始值来进行计数。而且, 当 PIN 码认证单元 50 已经确定未授权使用并且强制关闭电源之后再次开启电源时, 指纹认证单元 46 再次设置指纹认证模式, 在这种情况下, 不管对应于指纹输入的指纹认证失败了多少次, 都保持指纹认证模式。更具体地, 当电源再次开启时, 指纹认证单元 46 检查已经存储于非易失性存储器 42 中的认证失败标志 45, 并且, 由于在这种情况下认证失败标志 45 已经设置为开启, 则指纹认证单元 46 会得知它处于电源被强制关闭以防止未授权使用的防卫状态, 并且一直保持指纹认证模式, 不管指纹认证失败了多少次。

[0040] 如上所述, 在由于指纹认证连续失败十次然后 PIN 码认证连续失败五次而强制关闭电源之后, 再次开启电源时, 不管对应于指纹输入的认证失败了多少次, 指纹认证单元 46 都不再将模式切换到作为指纹认证的备份的 PIN 码认证模式, 而是保持其中仅执行指纹认证的操作模式。

[0041] 结果, 当要对便携式终端设备 10 进行未授权使用时, 十次指纹认证失败和连续五次 PIN 码认证失败会使得电源强制关闭, 并且当电源被再次开启时, 模式被固定于仅指纹认证模式, 其中如果指纹属于未授权用户的, 则认证必然失败, 并且还保持指纹认证的操作模式, 而不管指纹认证失败了多少次。因此, 未授权用户不能通过使用 PIN 码进行解锁, 并且除了放弃经由未授权使用的解锁之外再没有其他选择, 因此, 能够极大地改进通过指纹认证方式的安全性。

[0042] 由于 PIN 码认证单元 50 在非易失性存储器 42 中存储未授权使用中的 PIN 码失败次数 72, 则即使通过在 PIN 码认证的失败次数达到五次之前再次开启电源来从头再次开始 PIN 码的未授权输入时, 存储于非易失性存储器 42 的前一次的 PIN 码失败次数 72 也会被读取为初始值, 以便对失败次数进行计数。因此, 即使在电源被再次开启时, PIN 码的未授权输入也至多会被执行五次。然后, 模式被固定于指纹认证模式, 因此, 未授权的用户不能通过使用 PIN 码来进行解锁, 并且除了放弃经由未授权使用的解锁之外再没有其他选择, 由此也极大地改进了涉及 PIN 码认证的安全性。

[0043] 图 3 是图 2 的认证处理单元 28 中的操作模式设置单元 44 的处理操作流程图。在图 3 中, 操作模式设置单元 44 在步骤 S1 中执行指纹登记处理。在指纹登记处理中, 例如如图 4A 的指纹认证登记屏幕 52 中所示, “第三手指”被指定为用于进行指纹登记的手指; 在上述屏幕显示的状态中、第三手指的指尖被放置于图 1 所示的便携式终端设备 10 的指纹传感器 16 上并被滑动拖动时, 执行指纹的读取操作; 在图 2 的传感器控制单元 30 产生由根据手指移动而分段扫描的图像合成的指纹图像; 并且, 通过从指纹图像提取指纹的特征, 比如分支和端点来产生指纹认证数据, 由此在例如非易失性存储器 42 的登记区域中登记指纹。

当完成该指纹登记时,显示图 4A 的登记完成消息 54。

[0044] 随后,在图 3 的步骤 S2 中,显示操作模式选择菜单屏幕,例如,如图 4B 的指纹认证登记屏幕 52 中所示。在指纹认证登记屏幕 52 中,显示“你使用登记了的认证指纹么?”的消息,并且在其下方显示含有选择框 58、60 和 62 的操作模式选择菜单 56。

[0045] 其中,当选择在选择框 58 中所示的“仅使用指纹”时设置基于本发明的指纹认证处理。除此之外,也可选择选择框 60 的“结合 PIN 码使用”。选择框 60 和 62 的操作模式与传统操作模式相同。

[0046] 随后,在图 3 的步骤 S3 中,检查是否选择了“仅使用指纹”,并且在确定其选择时,在步骤 S4 中设置仅指纹认证模式。同时,在步骤 S5 中,当确定为选择了“结合 PIN 码使用”时,在步骤 S6 中设置组合认证模式。当在步骤 S7 中选择“不使用”时,在步骤 S8 中设置 PIN 码认证模式。

[0047] 当设置结束时,屏幕切换到图 4C 的指纹认证登记屏幕 52,其中显示“设置结束”作为设置完成消息 64,并且还显示表明“第三手指”的指纹登记的图标 66。

[0048] 图 5A 和 5B 是在将“仅使用指纹”设置为操作模式时,本发明的指纹认证处理的流程图。在图 5A 和 5B 中,在基于本发明的指纹认证处理中,在步骤 S1 检查是否已经输入了指纹,其中如果已经输入了指纹,则处理进行到步骤 S2,在该步骤中进行对先前输入指纹的指纹认证。

[0049] 当在步骤 S3 中该指纹认证结果被确定为成功认证时,处理进行到步骤 S15 并且进行解锁。当在步骤 S3 确定为认证失败时,处理进行到步骤 S4,其中对认证失败次数 A 进行计数。认证失败次数 A 在初始状态是 $A = 0$,并且在每次认证失败之后都加 1。随后,在步骤 S5 中,检查认证失败次数 A 是否到达十次,并且当它到达了十次时,处理返回到步骤 S1,其中通过重复指纹输入的方式进行指纹认证。当认证失败次数 A 在步骤 S5 中已经到达十次时,处理进行到步骤 S6,其中检查认证失败标志是否开启。请注意,认证失败标志 45 是存储在图 2 的非易失性存储器 42 中。

[0050] 这里,由于认证失败标志在初始状态是关闭的,处理进行到步骤 S7,其中认证失败次数 A 被清除,使得 $A = 0$ 。然后,处理进行到步骤 S8 的处理。在步骤 S8 中,在液晶显示器 14 上显示提示 PIN 码输入的消息,并且当按照该消息输入 PIN 码时,确定该输入;以及在步骤 S9 中,进行 PIN 码认证处理,用于将输入的 PIN 码与先前登记的 PIN 码核对。当在步骤 S10 中该认证结果被检测为成功认证时,处理进行到步骤 S16,在该步骤中进行解锁。

[0051] 当认证失败时,处理进行到步骤 S11,其中对认证失败次数 B 进行计数。认证失败次数 B 在初始状态是 $B = 0$,然后在每次失败时都加 1。在每次失败时,认证失败次数 B 都被存储于非易失性存储器 42 中以作为 PIN 码失败次数 72,并且即使在电源被关闭时也能被保持。

[0052] 然后,在步骤 S12 中,检查认证次数 B 是否已经到达五次。当少于五次时,处理返回到步骤 S8,并且重复 PIN 码输入方式的认证。当认证失败次数 B 在步骤 S12 中已经到达五次时,则确定为未授权使用,并且处理进行到步骤 S13,在该步骤中认证失败标志被开启并存储到非易失性存储器 42 中。然后,在步骤 S14 中,电源被强制关闭。

[0053] 当在步骤 S14 中按照确定的未授权使用结果而已经强制关闭电源之后再次开启电源时,启动从步骤 S1 的处理。更具体地,在步骤 S1 中在液晶显示器 14 上显示提示指纹

输入的消息；当按照该消息输入指纹时，在步骤 S2 进行指纹认证，用于将其与先前输入的指纹核对；由于在这种情况下是未授权使用，则在步骤 S3 确定为认证失败；并且在步骤 S4 中，从 $A = 0$ 的状态再次对认证失败次数 A 进行计数。

[0054] 然后，一直到步骤 S5 中的认证次数 A 达到十次，从步骤 S1 重复指纹输入方式的认证。当失败次数到达十次时，处理进行到步骤 S6，其中检查认证失败标记是否开启。在这种情况下，在先前的指纹认证处理的步骤 S13 的处理中，认证失败标志已经设置为开启。因此，处理不会进行到使用 PIN 码的认证处理（其被设置为从步骤 S7 启动，作为指纹认证失败的恢复处理），而是从步骤 S1 重复指纹认证处理。

[0055] 在未授权使用中，在电源被再次开启，以便在步骤 S8 至 S12 的 PIN 码认证处理期间的失败次数是例如 4 次的状态中启动处理的情况下，此时的 PIN 码失败次数 B 被存储于非易失性存储器 42 中。因此，当指纹认证失败十次之后，电源被再次开启并且处理进行到 PIN 码认证处理时，在第一次 PIN 码认证失败的情况下，由于以非易失性存储器 42 中存储的先前失败次数 4 作为初始值来进行计数，所以认证失败次数 B 在步骤 S12 中变为 $B = 5$ ，在步骤 S13 中在非易失性存储器 42 里存储认证失败标志，并且在步骤 S14 电源被强制关闭。随后，由于认证失败标志已经开启，则处理仅固定于指纹方式的步骤 S1 至 S6 的认证。

[0056] 请注意，当随后的指纹认证成功时，非易失性存储器 42 中存储的 PIN 码失败次数 B 和认证失败标志被清除。

[0057] 尽管当 PIN 码认证失败次数到达五次时，在图 5A 的步骤 S14 中电源被强制关闭，但是在另一实施例中，可以不关闭电源而保持认证锁定状态。当然，在这种情况下，当电源被再次开启时，在开启的认证失败标志和 PIN 码失败次数被存储于非易失性存储器 42 中的状态下恢复从步骤 S1 的处理。

[0058] 图 6A 和 6B 是设置“结合 PIN 码使用”作为操作模式的情况下的组合认证处理流程图，并且这里的处理流程基本上与传统设备中的相同。在图 6A 和 6B 的组合认证处理中，在步骤 S1 检查是否已经输入指纹，其中如果已经输入指纹，则处理进行到步骤 S2，在该步骤中进行指纹认证。当在步骤 S3 指纹认证成功时，在步骤 S13 进行解锁。当在步骤 S3 确定指纹认证失败时，在步骤 S4 将认证失败次数 A 加 1。然后，在步骤 S5 中，检查认证失败次数 A 是否已经到达十次，并且重复从步骤 S1 的处理，直到认证失败次数到达十次为止。这时，处理与基于本发明的图 5A 和 5B 的指纹认证处理的步骤 S1 至 S5 相同。

[0059] 随后，在步骤 S6 中认证失败次数 A 被清除使得 $A = 0$ 之后，处理进行到从步骤 S7 开始的 PIN 码方式的认证处理。在这种情况下的 PIN 码方式的认证处理不是指纹认证的恢复处理，而是在指纹认证不能被执行时执行的 PIN 码认证处理。在 PIN 码认证处理中，当步骤 S7 中确定 PIN 码输入时，处理进行到步骤 S8，其中执行 PIN 码认证，用于根据先前登记的 PIN 码来认证输入的 PIN 码。当步骤 S9 中确定成功认证时，在步骤 S14 进行解锁。当确定认证失败时，处理进行到步骤 S10，其中认证失败次数 B 被加 1。然后，重复从步骤 S7 的处理，直到认证失败次数 B 在步骤 S11 中到达五次。当认证失败次数 B 到达五次时，处理从步骤 S11 进行到步骤 S12，在步骤 S12 中电源被强制关闭。

[0060] 作为步骤 S12 中的电源关闭的结果，认证失败次数 B 随着电源关闭而被清除。当在步骤 S12 中强制电源关闭之后再次开启电源时，再次重复步骤 S1 至 S5 的指纹认证处理，并且当指纹认证失败十次时，在步骤 S6 中清除认证失败次数。然后，处理进行到步骤 S7 至

S11 的 PIN 码认证处理,其中当 PIN 码认证处理失败五次时,在步骤 S12 中电源被强制关闭。随后,在每次电源又被开启时重复该处理。

[0061] 图 6A 和 6B 的步骤 S10 的认证失败次数 B 也可存储于非易失性存储器 42 中,从而它能够在下一次开启电源时被作为认证失败的初始值被计数。

[0062] 图 7 是当“不使用指纹认证”设置为操作模式时的 PIN 码认证处理流程图。在步骤 S1 的 PIN 码认证处理中,当按照液晶显示器 14 中的提示输入 PIN 码的消息来输入 PIN 码时,在步骤 S2 进行 PIN 码认证处理,并且当步骤 S3 中认证成功时,处理进行到步骤 S7,在该步骤中进行解锁。

[0063] 当步骤 S3 中认证失败时,在步骤 S4 中对认证失败次数 B 累加计数。然后,重复从步骤 S1 的处理,直到步骤 S5 中认证失败次数 B 到达五次。当步骤 S5 中认证失败次数到达五次时,在步骤 S6 中关闭电源。按照该关闭,认证失败次数 B 被清除使得 $B = 0$,并且当电源被再次开启时,重复从步骤 S1 的处理。这里,图 7 的步骤 S5 的认证失败次数 B 也存储于非易失性存储器 42 中,使得它在下一次开启电源时能作为认证失败的初始值被计数。

[0064] 此外,本发明提供信息设备的计算机执行的安全管理程序,并且该程序包括具有基于图 5A 和 5B 的指纹认证处理流程图的流程的程序流程。

[0065] 在上述实施例中,除了选择“仅使用指纹”用于设置本发明的指纹认证处理的操作模式之外,作为实例,还可采用选择作为常规指纹认证操作模式的“结合 PIN 码使用”或者“不使用”的情况。然而,只要通过选择“仅使用指纹”作为本发明的操作模式来提供图 5A 和 5B 的指纹认证处理的流程图的处理功能,其它操作模式是否存在都不会对本发明施加限制。

[0066] 而且,尽管作为实例,上述实施例采用了指纹认证处理的失败次数是十次,并且作为随后恢复处理而执行的 PIN 码认证处理的失败次数是五次的情况,但是指纹认证处理和 PIN 码认证处理中的各失败次数可随需要采取任意次数。

[0067] 而且,尽管在上述实施例中,用于确定未授权使用(或输入错误)的指纹认证处理的失败次数是十次,并且用作随后恢复处理的 PIN 码认证处理的失败次数是少于上述次数的五次,从而使得可恢复的指纹认证次数增加以便对应于未授权使用之外的指纹认证错误,但是用于确定未授权使用的认证失败次数可以是相同次数,或者 PIN 码认证处理的失败次数可以大于指纹认证处理的失败次数。

[0068] 而且,尽管作为实例,上述实施例采用了便携式终端设备比如便携式电话,但是本发明并不限于此,并且可不加修改地应用于含有指纹传感器的任何信息设备,比如 PDA 或个人计算机。

[0069] 而且,本发明包含不损害其目的和优点的任何修改,并且不限于上述实施例中描述的数值。

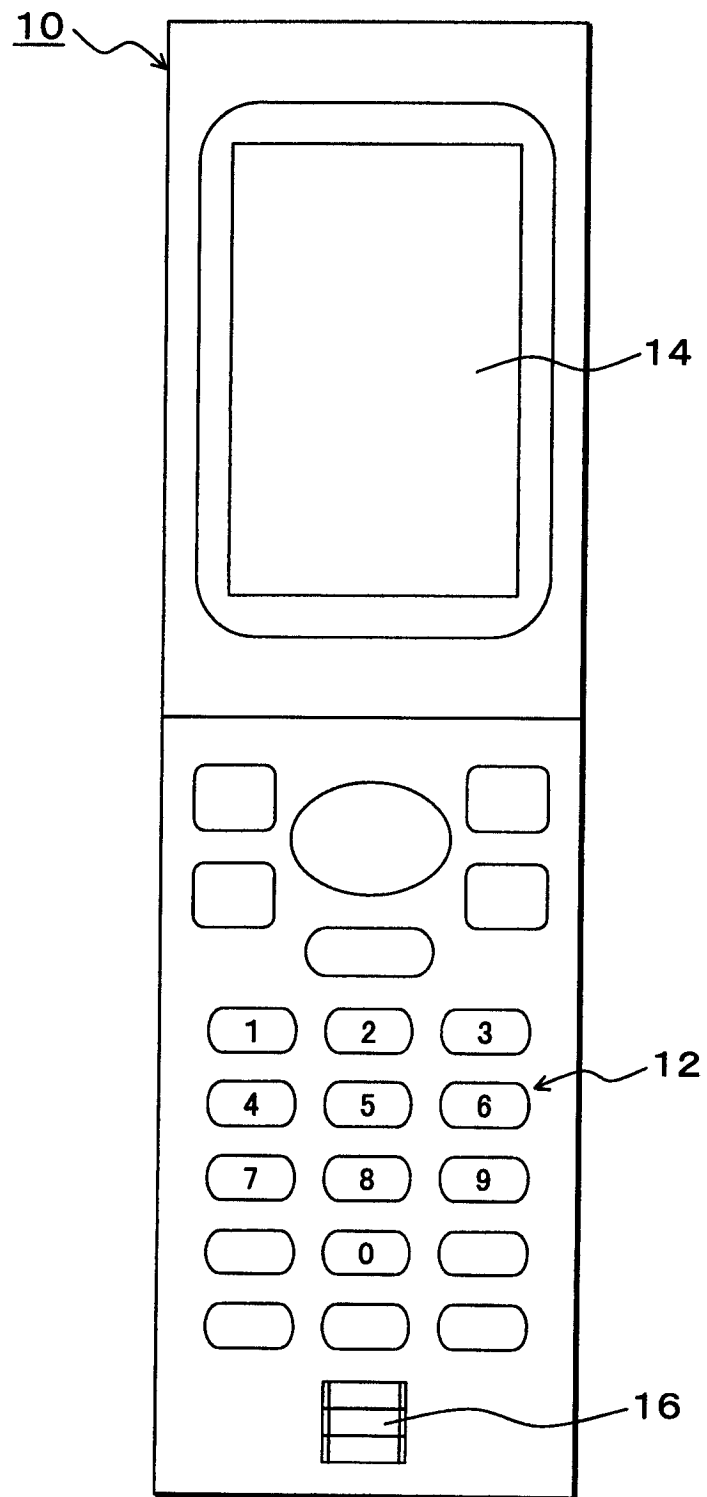


图 1

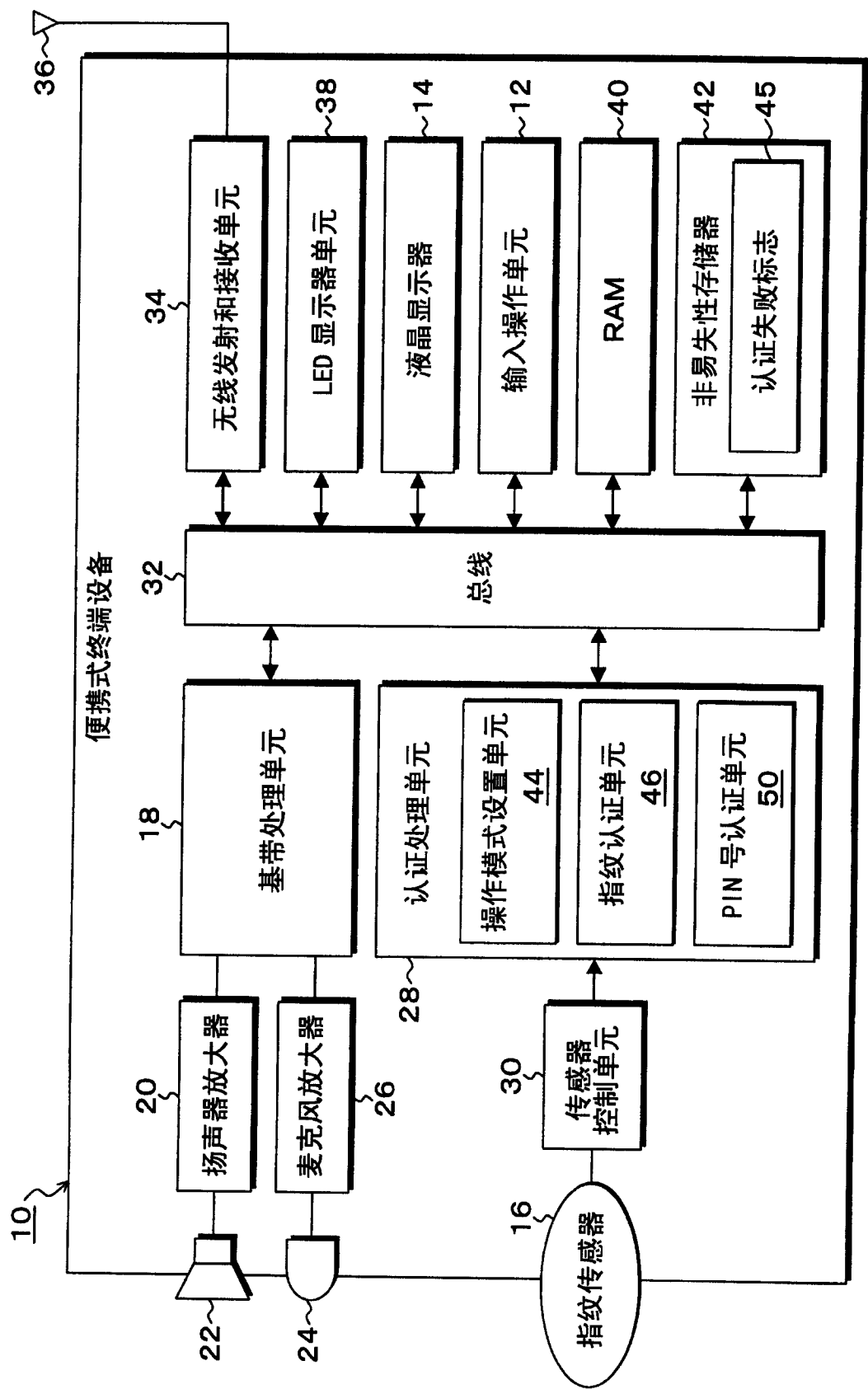


图 2

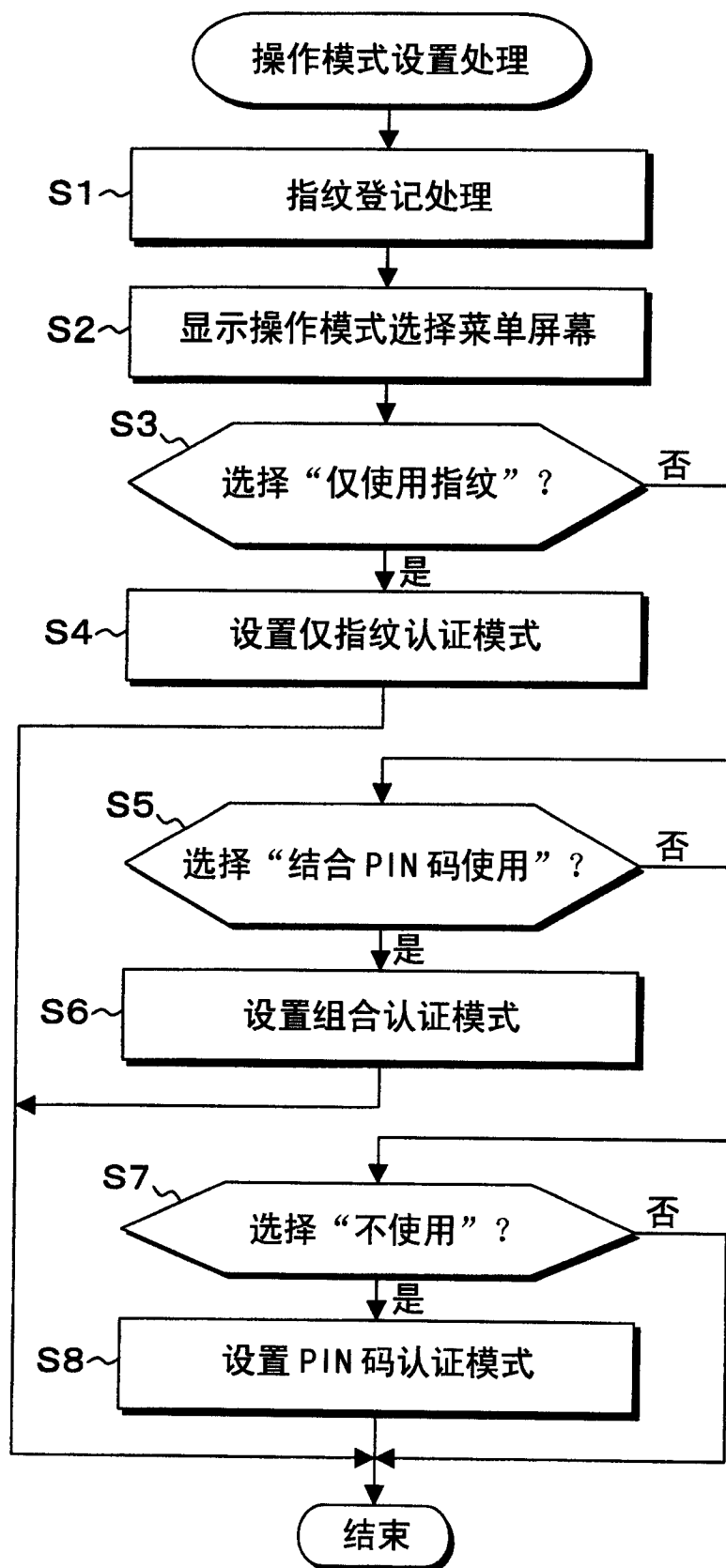


图 3

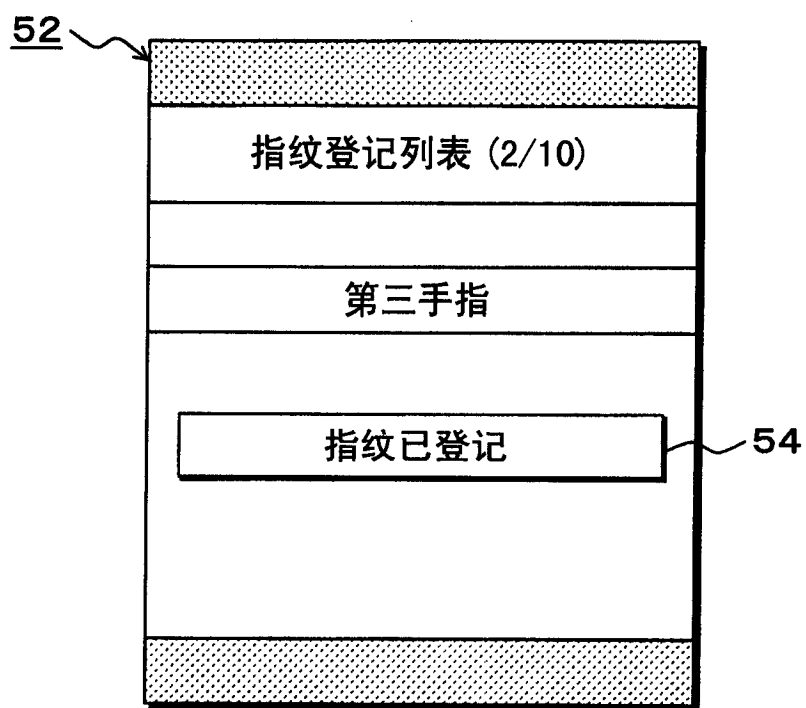


图 4A

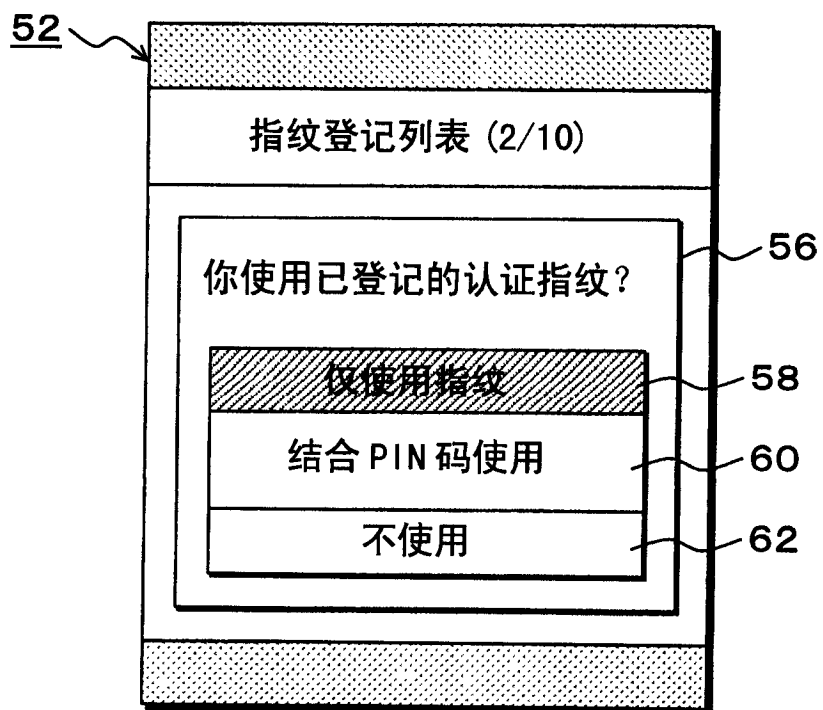


图 4B

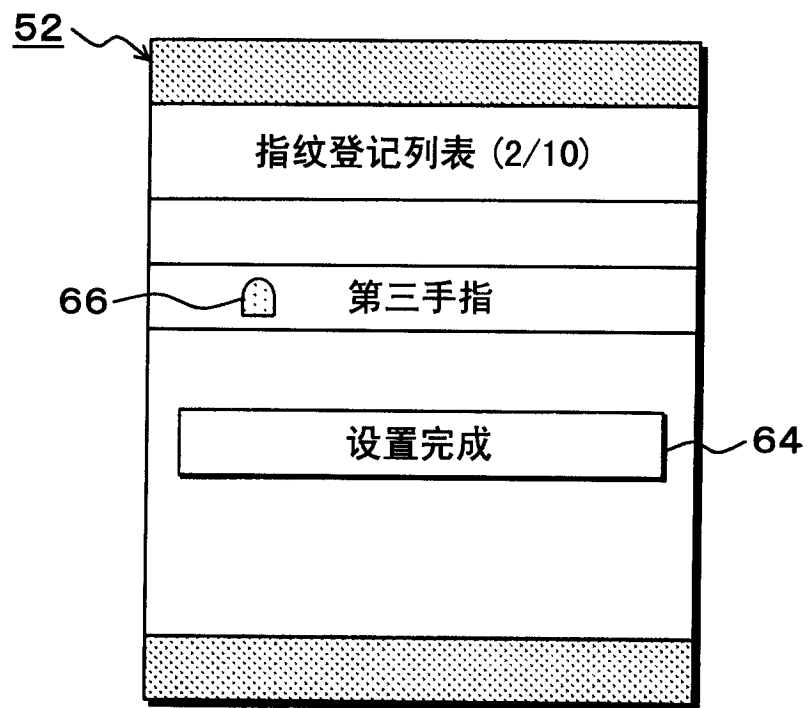


图 4C

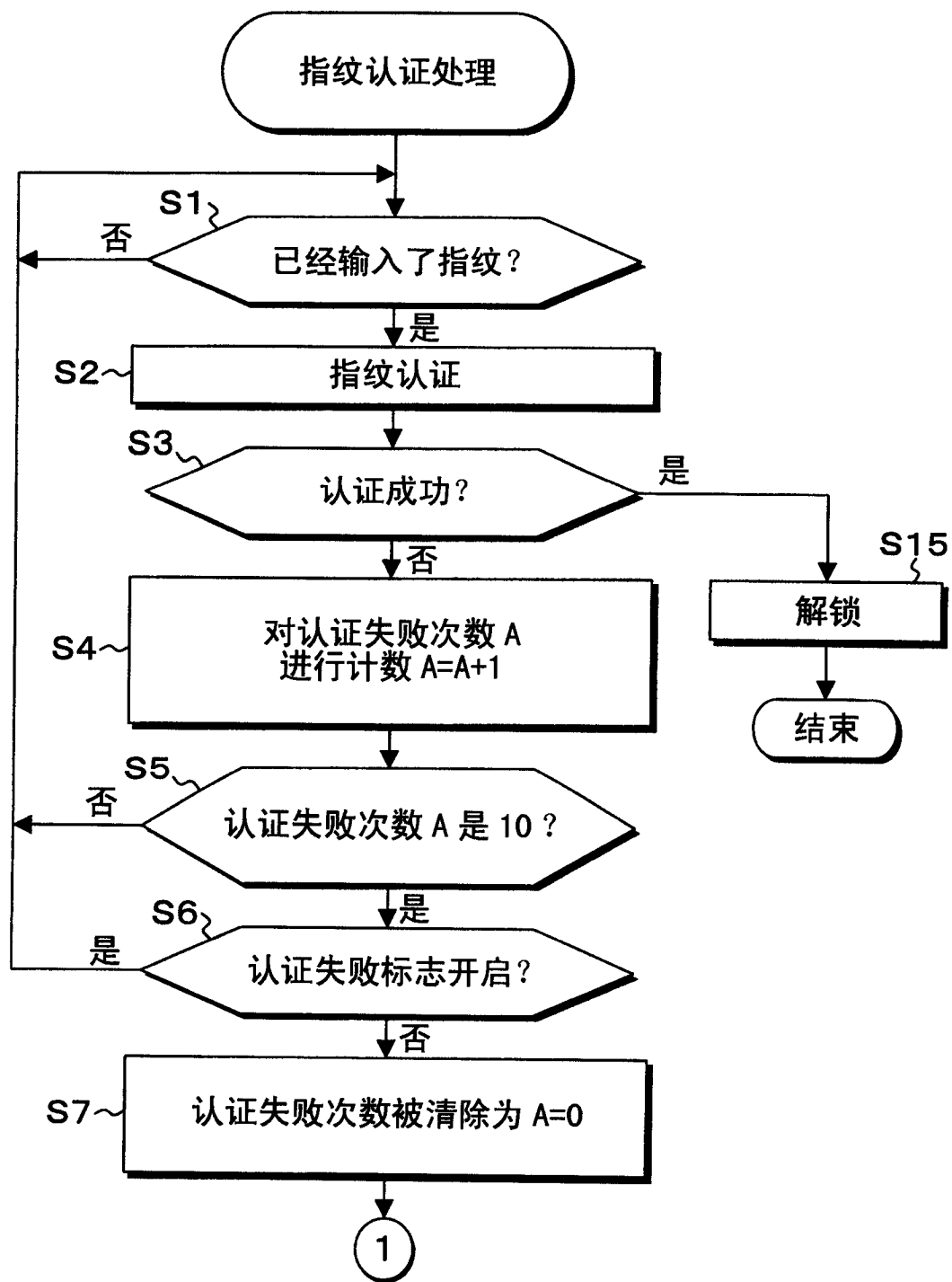


图 5A

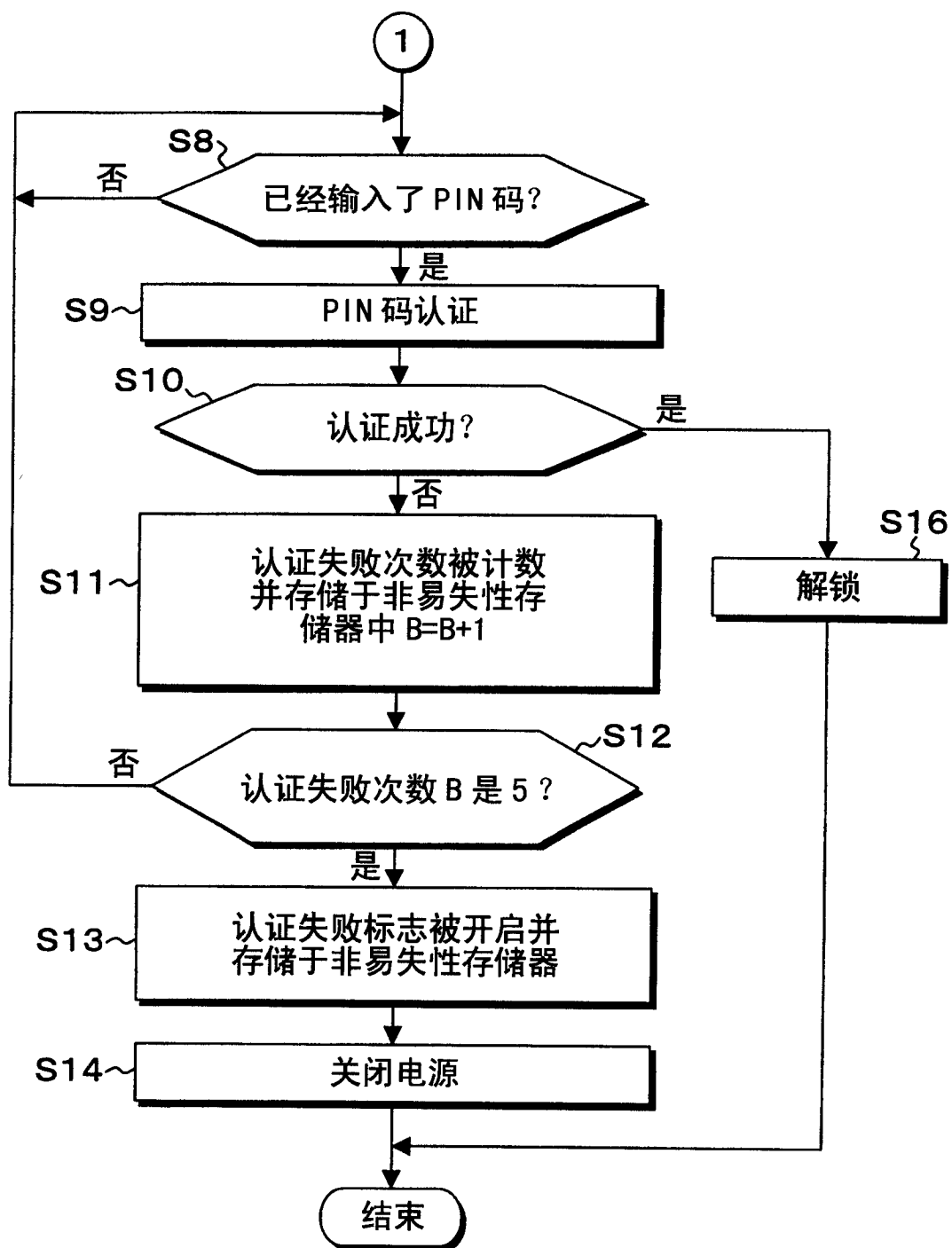


图 5B

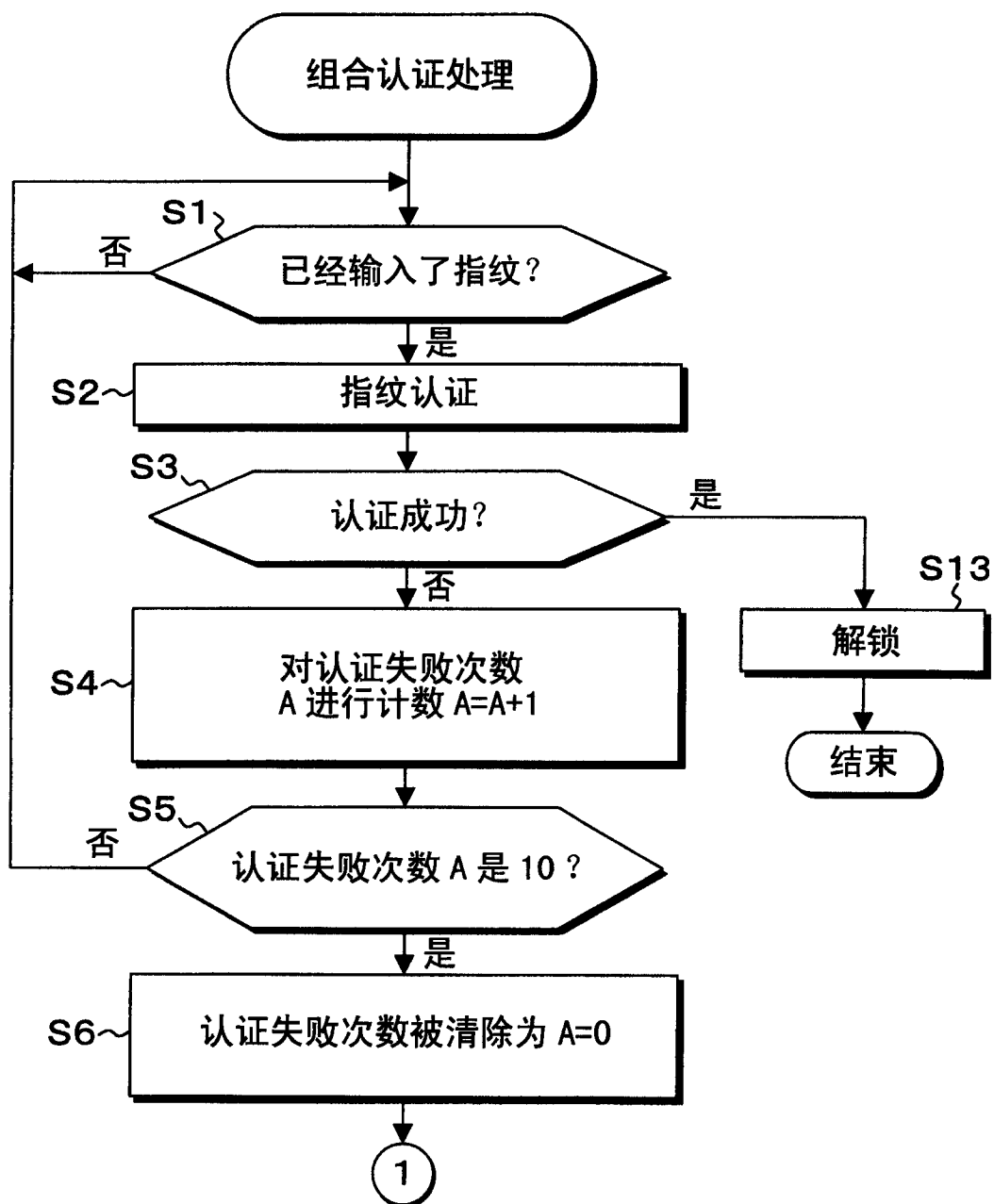


图 6A

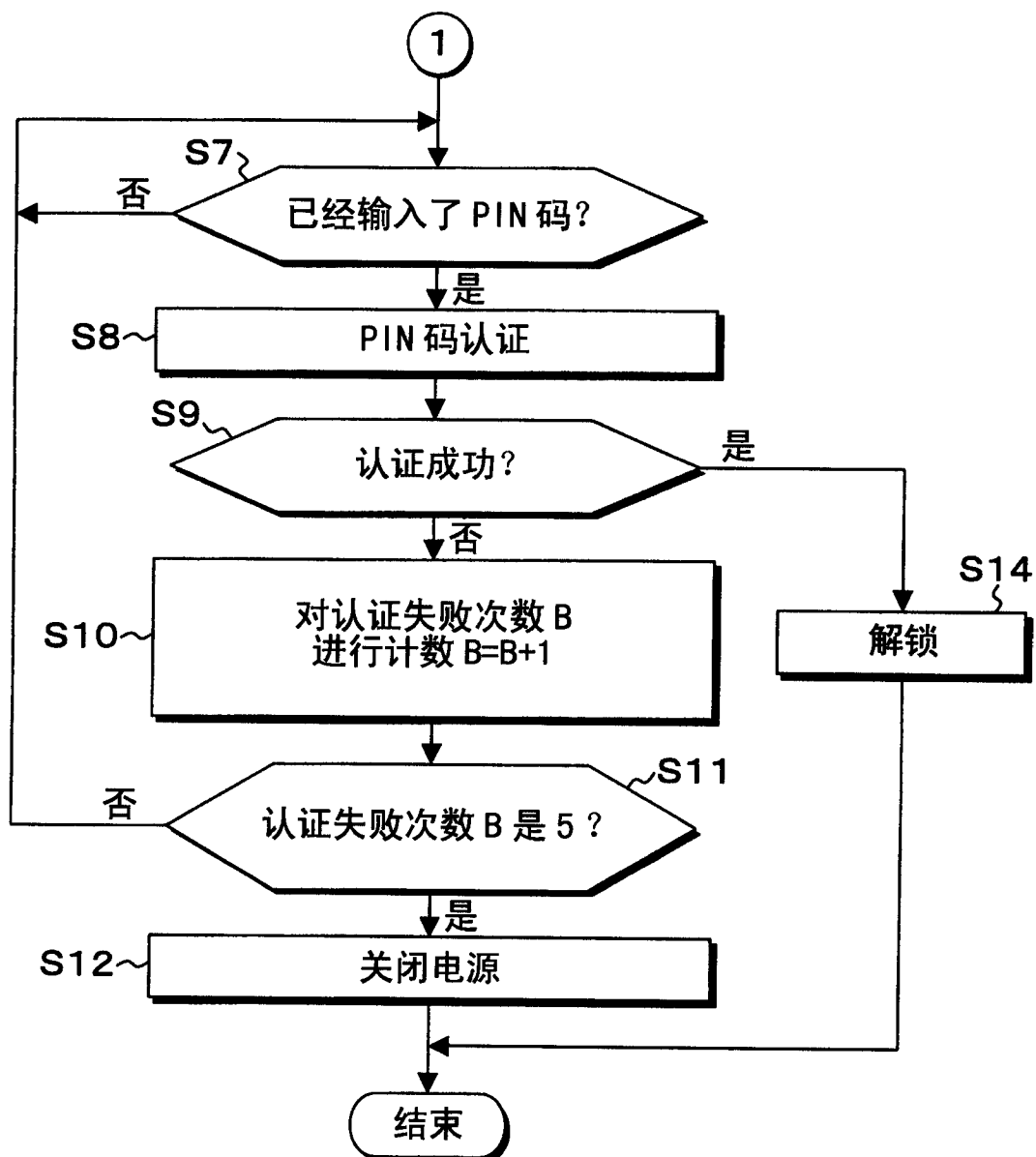


图 6B

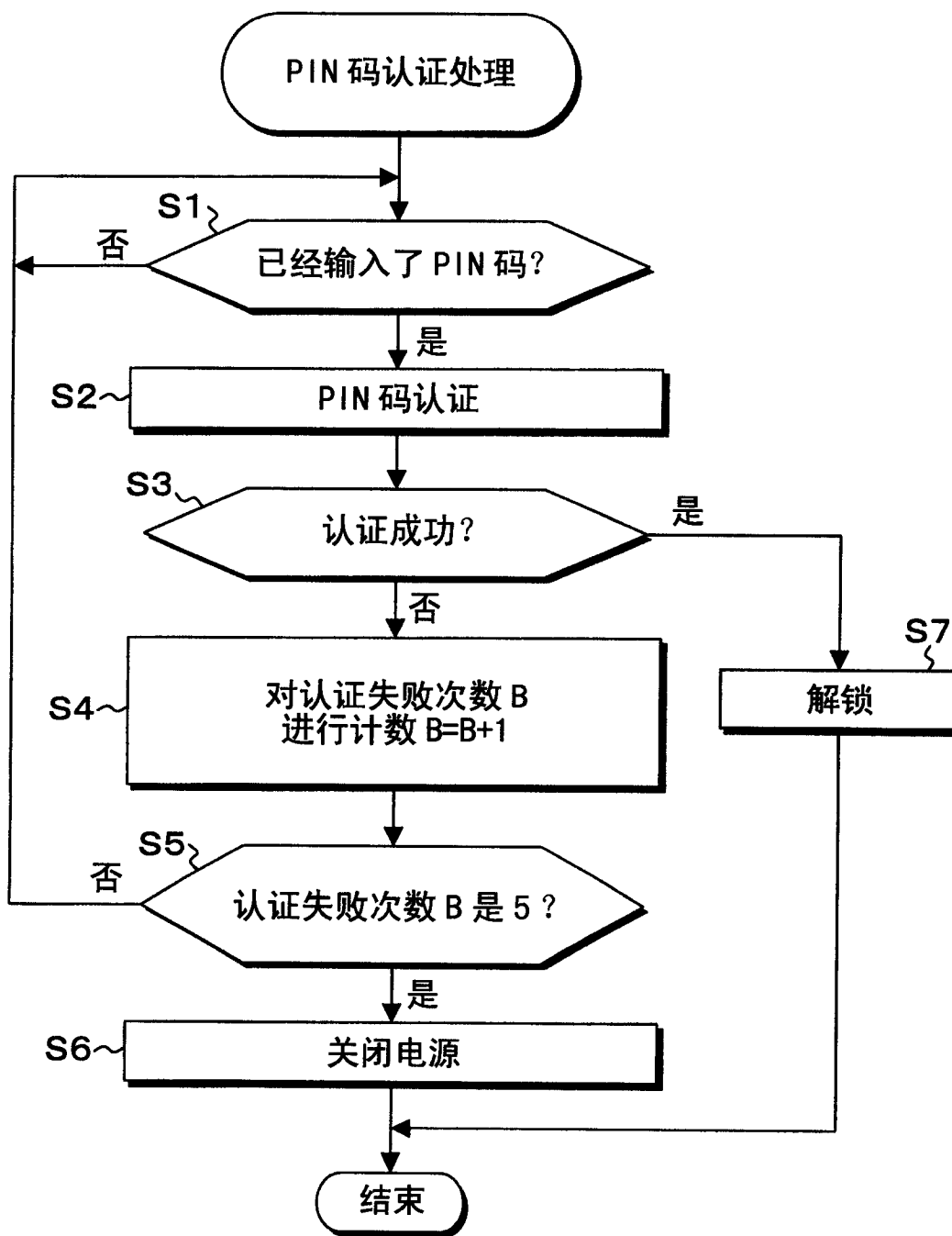


图 7