(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 105391838 B
(45)授权公告日 2019.01.01

(21)申请号 201510669902.9

(22)申请日 2012.07.13

(65)同一申请的已公布的文献号
申请公布号 CN 105391838 A

(43)申请公布日 2016.03.09

(30)优先权数据
13/183,311 2011.07.14 US

(62)分案原申请数据
201280043451.2 2012.07.13

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 L·蔡 J·R·梅尼德斯
R·B·西尔弗斯坦
R·帕拉玛什沃兰

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 袁逸

(51)Int.Cl.
H04M 1/66(2006.01)
H04M 1/725(2006.01)
H04W 52/02(2009.01)

(56)对比文件
CN 1980428 A,2007.06.13,
US 2009253410 A1,2009.10.08,
CN 101969493 A,2011.02.09,
CN 101990196 A,2011.03.23,
WO 2010020883 A3,2010.06.17,

审查员 何丹霞

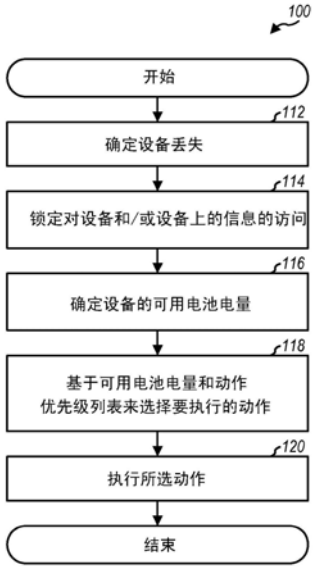
权利要求书1页 说明书11页 附图5页

(54)发明名称

用于检测和处理丢失的电子设备的方法和装置

(57)摘要

公开了用于检测和处理丢失的电子设备的方法和装置。在一种设计中,设备可自主确定它是否丢失。响应于确定它丢失,该设备可破坏至少一个组件以使得它无法操作并且可执行其它动作。在另一设计中,设备在确定它丢失时可确定该设备的可用电池电量,基于可用电池电量选择可能动作列表中的至少一个动作,并执行所选动作。在又一设计中,在确定它丢失时,设备可基于副安全密钥来阻止对该设备上的信息的访问,该副安全密钥在正常操作期间不被用于加密信息。在又一设计中,在确定它丢失时,设备可通知至少一个联系人,并可执行至少一个附加动作。



CN 105391838 B

1.一种用于电子设备的方法,包括:

基于主安全密钥来对设备上的信息加密以保护所述信息;

确定所述设备丢失;以及

基于副安全密钥来阻止对所述设备上的所述信息的访问,所述副安全密钥在所述设备的正常操作期间不被用于加密所述信息,其中阻止对所述信息的访问包括在确定所述设备丢失之后基于所述副安全密钥对所述已加密信息再次加密。

2.如权利要求1所述的方法,其特征在于,阻止对所述信息的访问包括除非所述设备接收到所述副安全密钥,否则阻止对所述信息的访问。

3.如权利要求1所述的方法,其特征在于,所述副安全密钥是所述设备的所有者不可取得的,且是所述设备的可信实体可取得的。

4.一种用于电子设备的装备,包括:

用于基于主安全密钥来对设备上的信息加密以保护所述信息的装置;

用于确定所述设备丢失的装置;以及

用于基于副安全密钥来阻止对所述设备上的所述信息的访问的装置,所述副安全密钥在所述设备的正常操作期间不被用于加密所述信息,其中所述用于阻止对所述信息的访问的装置包括用于在确定所述设备丢失之后基于所述副安全密钥对所述已加密信息再次加密的装置。

5.如权利要求4所述的装备,其特征在于,所述用于阻止对所述信息的访问的装置包括用于除非所述设备接收到所述副安全密钥,否则阻止对所述信息的访问的装置。

6.一种用于电子设备的装置,包括:

至少一个处理器,其被配置成基于主安全密钥来对设备上的信息加密以保护所述信息,确定设备丢失并基于副安全密钥对所述已加密信息再次加密来阻止对所述设备上的所述信息的访问,所述副安全密钥在所述设备的正常操作期间不被用于加密所述信息。

7.如权利要求6所述的装置,其特征在于,所述至少一个处理器被配置成除非所述设备接收到所述副安全密钥,否则阻止对所述信息的访问。

8.一种其上存储有代码非瞬态计算机可读介质,所述代码可由至少一个处理器执行以使得所述至少一个处理器:

基于主安全密钥来对设备上的信息加密以保护所述信息;

确定所述设备丢失,以及

基于副安全密钥来阻止对所述设备上的信息的访问,所述副安全密钥在所述设备的正常操作期间不被用于加密所述信息,其中阻止对所述信息的访问包括在确定所述设备丢失之后基于所述副安全密钥对所述已加密信息再次加密。

9.如权利要求8所述的非瞬态计算机可读介质,其特征在于,所述代码可由所述至少一个处理器执行以使得所述至少一个处理器:

除非所述设备接收到所述副安全密钥,否则阻止对所述信息的访问的代码。

用于检测和处理丢失的电子设备的方法和装置

[0001] 本分案申请是PCT国际申请日为2012年7月13日、国家申请号为201280043451.2、题为“用于检测和处理丢失的电子设备的方法和装置”的PCT国家阶段专利申请的分案申请。

[0002] 背景

[0003] I.领域

[0004] 本公开一般涉及电子器件,尤其涉及用于处理丢失的电子设备的技术。

[0005] II.背景

[0006] 电子设备(诸如蜂窝电话和智能电话)被广泛用于各种目的和应用。这些设备通常存储用户的敏感信息(例如,个人信息)。设备可支持基于口令的屏幕锁,除非正确的口令被输入,否则屏幕锁可阻止对设备的使用(且因此阻止对敏感信息的未经授权的访问)。然而,这种基于口令的屏幕锁特征不是所有设备都支持的。而且,这种基于口令的屏幕锁特征可能在确实支持这种特征的设备上未被用户利用。如果基于口令的屏幕锁不被一设备支持,或者被支持但未被利用,则接触到该设备的任何人都能够利用该设备并访问敏感信息。这种情况可能是不期望的,尤其是当设备丢失的时候。

[0007] 概述

[0008] 本文描述了用于检测和处理丢失的电子设备的技术。在一种设计中,设备可自主确定它是否丢失。这可基于设备的位置、设备上的传感器等来达成。设备可响应于确定它丢失而破坏该设备的至少一个组件以使该设备无法操作。设备还可响应于确定它丢失而执行其它动作。

[0009] 在另一设计中,例如响应于确定设备丢失,该设备可确定该设备的可用电池电量。设备可基于该设备的可用电池电量和可能还有可能动作列表中的每一动作的优先级来选择该列表中的至少一个动作。该设备可执行至少一个所选动作。在一种设计中,可能动作列表可包括阻止对设备的访问和/或对设备上的信息的访问的动作、当设备丢失时通知联系人列表的动作、备份设备上的信息的动作、擦除设备上的信息的动作、对设备上的信息加密的动作、自销毁该设备的动作等。可对设备上的一些信息或所有信息执行动作。

[0010] 在又一设计中,设备可确定它丢失并可基于副安全密钥来阻止对该设备上的信息的访问,该副安全密钥在该设备的正常操作期间不被用于加密该信息。在一种设计中,在确定设备丢失之前,该设备可基于主安全密钥来加密信息以保护信息。在确定设备丢失之后,该设备可基于副安全密钥来对已加密信息再次加密。

[0011] 在又一设计中,设备可获得它丢失的指示。设备可响应于获得该指示而执行通知至少一个联系人的第一动作。设备还可响应于获得该指示而执行动作列表中的至少一个附加动作。在一种设计中,设备可存储万一该设备丢失则要通知的联系人列表以及联系信息。在确定设备丢失时,该设备可向联系人列表中的每一联系人通知该设备丢失,并还可提供相关信息(诸如该设备的位置)。

[0012] 以下更加详细地描述本公开的各种方面和特征。

[0013] 附图简要说明

[0014] 图1示出了用于检测和处理丢失的设备的过程。

[0015] 图2示出了用于自主确定设备丢失并执行一个或多个动作的过程。

[0016] 图3示出了用于基于设备的可用电池电量来执行动作的过程。

[0017] 图4示出了用于基于安全密钥来锁定信息的过程。

[0018] 图5示出了用于通知联系人和执行其它动作的过程。

[0019] 图6示出了设备的框图。

[0020] 详细描述

[0021] 本文描述了用于检测和处理丢失的电子设备的技术。这些技术可用于各种类型的设备，诸如蜂窝电话、智能电话、个人数字助理(PDA)、膝上型计算机、平板设备、上网本、智能本等。这些技术可用于支持无线和/或有线通信的设备(例如，蜂窝电话、智能电话、膝上型计算机等)以及不支持通信的设备。

[0022] 设备可用于各种目的，且可为该设备的所有者/用户存储敏感信息以及其它信息。敏感信息可包括个人信息、商业信息等。敏感信息可被有意或无意地存储在设备上的缓冲器、非易失性存储器(诸如闪存或静态随机存取存储器(SRAM))、易失性存储器(诸如随机存取存储器(RAM))、虚拟存储器、临时文件中等等。

[0023] 所有者可能丢失设备并担心存储在该设备上的敏感信息。然而，所有者可能具有该设备上的相关信息的近期备份副本，该副本可能被存储在指定的服务器、备份存储设备上等。因此，所有者可能不担心当设备丢失时将信息从该设备复制到新设备上。设备可支持远程擦除特征，且能够响应于来自所有者的远程擦除命令而破坏该设备上的敏感信息和/或其它信息。当所有者意识到设备丢失并想要破坏该设备上的信息时，所有者可向该设备发送这一远程擦除命令。所有者可经由该设备支持的通信网络从远程位置发送远程擦除命令。

[0024] 远程擦除命令由于若干原因可能不能保证丢失的设备上的信息的销毁。首先，该设备可能不能被远程访问，例如因为该设备未连接到通信网络，或者电源从该设备被移除等等。其次，该设备可能被欺骗而给出虚假响应。例如，设备可能从通信网络断开，且设备上的信息可能被复制。该设备之后可连接到通信网络，接收远程擦除命令，擦除该设备上的信息，并发送指示信息已被破坏的响应。然而，由于信息已在接收到远程擦除命令之前或之后被复制，这一响应将实际上是虚假的。

[0025] 在一方面，设备可自主确定它已丢失。该设备然后可响应于确定它丢失而自主执行一个或多个动作。该设备因此可具有可触发锁定、备份、擦除和/或自销毁的整个过程的失知开关(dead-man switch)。

[0026] 一般而言，如果设备的所有者不知道设备的下落和/或设备不在所有者的控制之中，则该设备可被认为丢失。例如，如果设备被所有者遗失、被从所有者偷走等，则该设备可能丢失。该设备可按照各种方式来确定该设备丢失。这种确定可能不是完全准确的，且存在当设备确定它丢失时该设备判断错误的可能性。

[0027] 在一种设计中，如果设备已掉落但未被拾起，则该设备可确定它丢失。设备可包括加速计，加速计可感测下落的加速度、然后是当该设备撞击地面时的突然停止、之后没有移动。设备还可包括可感测由掉落的冲击导致的振动、该设备的外表面因掉落而导致的变形等的其它传感器。设备还可基于其它传感器和/或按照其它方式检测到它已掉落。设备可在

检测到它已掉落时启动定时器。设备然后可基于其传感器或该设备上按下的键等确定它是否已被拾起。如果该设备在定时器期满之前未被拾起，则该设备可断言它丢失。该定时器可基于正确确定该设备丢失的可能性、可以多快地检测到丢失等之间的折衷来被设为合适的值。

[0028] 在另一设计中，如果设备在预定的持续时间内未被移动，则该设备可确定它丢失。这可意味着该设备已被丢失、遗忘或遗弃。设备可基于该设备上的传感器、或检测到无线网络中的同一蜂窝小区或同一组蜂窝小区等来确定它未被移动。

[0029] 在又一设计中，如果设备在不熟悉的环境中，则该设备可确定它丢失。设备可使用该设备上的各种传感器时不时地确定其环境。设备可存储先前被确定为安全的环境的日志。设备可时不时地将其当前环境与该日志进行比较，并且如果当前环境偏离先前确定的安全环境，则可断言它丢失。

[0030] 设备的环境可基于该设备上的各种传感器来确定。设备的环境还可基于以下准则中的一个或多个来确定：

[0031] • 设备的位置，这可基于定位方法(诸如全球定位系统(GPS)、增强蜂窝小区身份(ID)等)来确定，

[0032] • 设备是否关于蓝牙、Wi-Fi、广域网(WAN)等感测到熟悉的设备、基站、网络等，

[0033] • 设备是否以其通常的取向(使用罗盘和加速计)或底座、适配器、电压、电流等被插入，

[0034] • 设备是否在其通常位置被插入，

[0035] • 设备是否检测到熟悉的磁场，这可使用内部罗盘或采用其它手段来感测，

[0036] • 设备是否检测到熟悉的背景噪声，诸如环境噪声、语音、音乐等，

[0037] • 设备是否感测到熟悉的环境光(例如，缺乏光线可意味着设备卡在沙发或汽车后座等里面)，

[0038] • 设备是否感测到熟悉的加速度(例如，所有者/用户的步伐对比卡在汽车后座中的加速度)，

[0039] • 设备是否检测到熟悉的物体(例如，家具、墙壁颜色、天花板图案、脸等)，

[0040] • 在设备上运行的应用是否是常用的，

[0041] • 在设备上正在访问的数据是否是常访问、使用、消费、下载、共享的等等，

[0042] • 设备正拍摄的照片是否是熟悉的区域、位置、地标等的照片，

[0043] • 设备是否检测到熟悉的触摸(例如，每分钟字数、左手持握对比右手持握、手的取向、手的大小、指尖大小等)，

[0044] • 设备是否检测到其所有者或可信次要用户(例如，家庭成员、同事、朋友等)的语音，以及

[0045] • 其它准则。

[0046] 设备的环境可基于以上列出的准则中的任何一个或任何组合来确定。设备的环境也可基于其它准则来确定。

[0047] 在一种设计中，设备可时不时地确定其环境，并可查明其环境是否安全。例如，设备可要求所有者/用户确认它未丢失，且可在接收到来自所有者的确认时确定当前环境是安全的。在另一设计中，每当设备参与到被认为有效的任务中时，该设备即可确定其环境。

有效的任务可以是对存储在该设备上的号码的电话呼叫、涉及有效安全密钥或口令的功能等等。有效任务期间的环境可被认为是安全的。设备还可以用其它方式确定安全环境。设备可存储安全环境的日志以用于检测该设备是否丢失。

[0048] 图1示出由设备执行的过程100的设计。设备可确定它丢失(框112)。如上所述,这种确定可基于各种准则来作出,且可能具有该确定并不正确的某种可能性。设备可在确定其丢失时执行各种动作。在一种设计中,设备可锁定对该设备和/或该设备上的信息的访问(框114)。设备可确定该设备的可用电池电量(框116)。该设备可基于可用电池电量和动作优先级列表来选择要执行的动作(框118)。一般而言,设备可取决于可用电池电量和/或其它准则来选择零个、一个或多个动作。该设备可执行所选动作(若有)(框120)。

[0049] 在一种设计中,优先级列表可包括以下动作中的一个或多个:

[0050] 1.向联系人列表告知该设备丢失,

[0051] 2.备份该设备上的信息,

[0052] 3.擦除该设备上的信息,以及

[0053] 4.自销毁该设备。

[0054] 在以上设计中,这些动作按照从最不重要到最重要的次序列出。因此,告知联系人列表是该列表中最不重要的动作,而自销毁是该列表中最重要的动作。优先级列表可包括更少、更多和/或不同的动作。动作还可按照与以上示出的次序不同的次序来区分优先级。

[0055] 在一种设计中,可向所有者提供当确定设备丢失时可由该设备执行的动作列表。所有者可选择哪些动作供该设备执行,并有可能选择每一所选动作的优先级。这种设计可允许所有者基于所有者的要求和偏好来定制万一该设备丢失则要执行哪些动作。例如,所有者可偏好数据安全性超过设备和数据可恢复性,于是可选择当确定设备丢失时擦除设备上的信息和/或自销毁设备。作为另一示例,所有者可偏好设备和数据可恢复性超过数据安全性,于是可选择当确定设备丢失时保护该设备和存储在该设备上的信息而不擦除该设备上的信息且不使该设备自销毁。在另一设计中,动作优先级列表可由可信实体配置,可信实体可以是网络运营商、企业信息技术(IT)部门、可信个人等。优先级列表中的动作可从可能动作列表中选择。

[0056] 在图1的框114中,设备可在确定它丢失时锁定并阻止对存储在该设备上的信息的访问。这种锁定可用各种方式来达成。在一种设计中,该设备可基于副安全密钥来锁定对信息的访问,副安全密钥在正常操作期间不被用于对该信息加密。设备可基于主密钥来对该设备上的敏感信息以及可能的其它信息加密来保护该信息,并可将已加密信息存储在该设备上。在锁定信息的一种设计中,设备可在确定它丢失时基于副安全密钥对已加密信息再次加密。在这种设计中,当设备确定它丢失时,信息可使用两个安全密钥被加密。在锁定信息的另一设计中,当设备确定它丢失时,该设备可仅用副安全密钥来对该设备上的信息加密。在锁定信息的又一设计中,除非提供副安全密钥,否则该设备可阻止对信息的访问,而不基于副安全密钥来对信息加密。在这种设计中,副安全密钥可按照类似于口令的方式被使用以访问信息。设备还可按照其它方式锁定对存储在该设备上的信息的访问。

[0057] 在一种设计中,主安全密钥可由设备的所有者在正常操作中在有规律的基础上使用以访问该设备上的信息。主安全密钥可例如当设备被激活时或当需要安全密钥时在该设备上被配置。在一种设计中,副安全密钥可能为可信实体所知但不为设备的所有者所知。该

可信实体可以是网络运营商、企业IT部门、可信个人等。在这种设计中，如果设备被找到，则该设备可被带到该可信实体以解锁。在另一设计中，副安全密钥可为所有者所知，且如果设备被找到，则该设备可由所有者解锁。

[0058] 替换地或另外地，在框114，设备在确定它丢失时可锁定对该设备的访问。在一种设计中，设备可锁定该设备的用户界面。例如，响应于确定它丢失，设备可激活屏幕锁。在另一设计中，设备可禁用该设备的某些功能。在又一设计中，设备可禁用该设备上的某些电路以使该设备无法操作。该设备可由所有者、或可信实体、或某个其它实体解锁。

[0059] 在图1的框116中，设备在确定它丢失时可确定可用电池电量。这可用无线设备上通常可用的电池电量检测器来达成。该设备可基于可用电池电量来确定要执行的一个或多个动作。

[0060] 一般而言，设备在确定它丢失时可执行的动作的数目可受到该设备的可用电池电量的限制。如果可用的电池电量越多，则设备可以能够执行越多动作，反之亦然。为了确保较重要的动作在较不重要的动作之前被执行，可由设备执行的动作可区分优先级并放置在列表中。设备然后可基于可用电池电量来从优先级列表中选择要执行的一个或多个动作。

[0061] 在一种设计中，设备可存储动作优先级列表，且可存储或确定每一动作所需的电池电量。一动作所需的电池电量可以是固定的，或可以是可变的且取决于一个或多个因素。例如，告知联系人列表所需的电池电量可取决于信道状况。擦除或备份信息所需的电池电量可取决于要擦除或备份的信息量。在任何情形中，设备可知道优先级列表中每一动作的所需电池电量。设备可向下遍历该列表，从最重要的动作开始。设备可一次考虑一个动作，且可基于该设备的可用电池电量和该动作的所需电池电量来确定是否要执行该动作。每当一动作被选择，设备就可更新可用电池电量。要选择的动作的数目以及选择哪些动作可取决于设备的可用电池电量和每一动作的所需电池电量。

[0062] 对以上给出的四个动作的示例性优先级列表，设备可首先确定是否有足够的电池电量来自销毁该设备。如果答案为是，则设备可选择这个动作并可从该设备的当前可用电池电量中减去该动作的所需电池电量。接下来，设备可确定是否有足够的电池电量来擦除该设备上的信息。如果答案为是，则该设备可选择这个动作并可通过减去该动作的所需电池电量来更新该设备的当前可用电池电量。接下来，设备可确定是否有足够的电池电量来备份该设备上的信息。如果答案为是，则该设备可选择这个动作并可通过减去该动作的所需电池电量来更新该设备的当前可用电池电量。接下来，设备可确定是否有足够的电池电量来通知联系人列表。如果答案为是，则设备可选择这个动作。

[0063] 设备也可基于其它准则来选择要执行的动作。在一种设计中，设备可考虑完成动作所需的时间量。例如，特定动作(例如，擦除)可能要花较长时间(例如，数小时)来完成，即使有足够的电源。所有者可能担心安全性(例如，担心在该动作完成之前电源会从该设备被移除)。所有者然后可配置该设备跳过将花太长时间的动作，或者可设置在移动到或跳到下一步骤之前完成这些动作的最大时间限制。设备也可基于不同和/或其它准则来选择要执行的动作。

[0064] 设备可获得要执行的动作列表，例如如上所述。一般而言，设备可按照任何次序执行该列表中的动作。动作被执行的次序可取决于每一动作的严重性以及给定动作是否影响其它动作。例如，设备可最后执行自销毁动作，因为这个动作可能损害执行其它动作的能

力。设备还可在擦除信息之前备份信息。

[0065] 在一种设计中，对以上给出的四个动作的优先级列表，设备可按照重要性的倒序来执行动作。例如，如果有足够的电池电量来执行全部四个动作，则设备可首先通知联系人列表。设备然后可备份该设备上的信息。设备然后可擦除该设备上的信息。设备然后可自销毁。设备可如下所述地执行每一动作。

[0066] 在一种设计中，设备可存储联系人列表，以便当该设备丢失时进行可能的通知。联系人列表可包括该设备的所有者和/或其他指定的人或实体。联系人列表还可包括或可关联于相关信息的数据库。例如，联系人的相关信息可包括电话号码、电子邮件地址和/或可用于向联系人通知该设备丢失的其它信息。联系人列表可由所有者在任何时间配置并可按照安全方式来配置。

[0067] 在一种设计中，如果有足够的电池电量，则设备可向联系人列表告知该设备丢失。设备可经由短消息服务(SMS)、电子邮件、语音呼叫、寻呼等来告知联系人。设备可在通知联系人列表时提供相关信息。在一种设计中，设备可提供与该设备的位置有关的信息，诸如其当前地理位置、或Wi-Fi位置等。地理位置可基于GPS或某种其它定位方法来确定。Wi-Fi位置可基于由该设备检测到的无线局域网(WLAN)中的一个或多个接入点来确定。在另一设计中，设备可提供与其环境相关的信息。环境相关信息可包括该设备上的相机拍摄的一张或多张照片、相机所捕捉的视频、经由该设备上的话筒录制的声音剪辑、对该设备是静止还是运动的指示、和/或该设备上的其它传感器所捕捉的其它信息。

[0068] 联系人列表中的联系人可接收设备丢失的通知。联系人还可接收由设备随该通知发送的相关信息。该信息可能能够给该联系人提供信息和/或可由该联系人用来作出关于该设备的决策。在一种设计中，可给予联系人中止将要由该设备执行的后续动作的选择。如果联系人决定中止后续动作并在特定时间窗口内提供合适的响应，则该设备可跳过后续动作。

[0069] 在一种设计中，如果存在足够的电池电量，设备可备份该设备上的信息。设备可定期安全地连接至指定服务器以备份该设备上的信息。在一种设计中，当确定设备丢失时，该设备可仅备份自从上次备份或同步以来已改变的信息。这种设计可减少当确定设备丢失时要备份信息的信息量。在另一设计中，设备可备份所有指定的信息(例如，所有敏感信息以及可能其它信息)。对这两种设计，设备均可按照安全方式备份信息。设备可建立与可备份信息的指定服务器的安全连接。安全连接可使用加密、或虚拟专用网络(VPN)、或通过各种代理服务器的回弹式数据流、或其它手段、或其组合来达成。设备然后可经由安全连接发送信息以便备份在指定服务器上。

[0070] 在一种设计中，如果存在足够的电池电量，设备可擦除/删除该设备上的信息。要擦除的信息可以匹配或可以不匹配要备份的信息。例如，设备可仅备份该设备上的相关信息但是可擦除该设备上的全部信息。要擦除的信息可驻留在外部存储器、内部存储器、SIM卡中等等。所有者可事先配置万一设备丢失则要擦除哪些信息、哪个存储器和/或哪个存储器的哪些部分。设备可使用合适的擦除算法或某种其它手段来永久地擦除信息。例如，设备可使用可反复地覆写每个位以便使信息不可恢复的军事级别擦除算法(例如，由www.dban.org提供的算法)。

[0071] 在一种设计中，所有者可事先配置存储器的哪些部分和/或哪些信息不应被擦除。

例如，存储器中存储归还信息以便能够将设备归还给所有者的部分可不被擦除。归还信息可包括设备的发现者可用来与所有者通信以便归还该设备的1-800号码、电子邮件地址、或者网站。

[0072] 在一种设计中，如果存在足够的电池电量，设备可禁用自身并自销毁。在一种设计中，设备可永久地破坏某些组件(例如，除了某些豁免区域之外的所有存储器)以便使该设备无法操作且在物理上不能起作用，并使得该设备上的信息是任何人都不能恢复的。组件可经由短路、电磁脉冲、烧断熔丝、篡改电池以导致爆炸和/或其它手段来破坏。设备还可破坏该设备上具有商业价值的组件，诸如显示器、中央处理单元(CPU)、图形处理单元(GPU)等。这可使得该设备无法操作，并且还可阻止窃取该设备来转售整个设备或其部件。

[0073] 设备的自销毁的严重性可取决于各种因素，诸如设备类型、期望的销毁程度等。例如，对军事设备可允许暴力自销毁，而对消费者设备可能需要不会伤害握持该设备的任何人的自销毁。作为另一示例，一些所有者可能期望其设备的完全自销毁，且在其设备丢失的情况下对找回其设备没有兴趣。相反，其他所有者可期望在其设备丢失的情况下其设备中仅某些关键组件的自销毁，抱有找回并可能重用其设备的希望。

[0074] 设备可确定其丢失但是电池电量太低而不能执行优先级列表中的任何动作或全部动作。设备然后可监视其电池电量以确定它是否已被再充电。设备可按照各种方式检测它已被再充电并可解释这一事件。在一种设计中，设备可将电池再充电解释为意味着该设备实际上没有丢失且之前关于丢失的检测是错误的。该设备然后可移出“丢失”状态。在另一设计中，设备可将电池再充电解释为意味着之前关于丢失的检测中可能出错。该设备然后可在移出丢失状态之前认证用户。例如，设备可要求用户输入主安全密钥、口令或某种其它认证信息以便移出丢失状态。如果用户不能得到认证(例如，如果主安全密钥、口令或某种其它认证信息未被提供)，则该设备可继续图1中的框116和118。在又一设计中，设备甚至在检测到电池再充电之后也可维持其关于该设备丢失的确定。该设备然后可确定可用电池电量(图1中的框116)并执行优先级列表中的一个或多个动作(图1中的框118)。

[0075] 在一种设计中，设备可包括备用电源，例如备用电池。备用电源可具有足够的电量来使得该设备在确定其丢失时能够执行一个或多个动作。例如，备用电源可提供足够的电量来自销毁存储器以及可能的其它组件(例如，CPU、GPU、显示器等)使其不能恢复。

[0076] 如上所述，设备可在确定其丢失时例如基于可用电池电量和每一动作的优先级来选择要执行的动作。在一种设计中，设备可立即执行全部所选动作。在另一设计中，设备可按照交错的方式执行所选动作。例如，设备在确定其丢失时可立即锁定对该设备和/或该设备上的信息的访问。设备还可立即或在此后不久通知联系人列表并备份该设备上的信息。设备然后可在擦除该设备上的信息之前等待某个时间量。设备然后可等待某个额外的时间量，然后执行自销毁。设备可立即执行不会破坏信息或该设备的动作。针对越来越具破坏性的动作，设备可等待越来越长的时间。或者，所有者可将设备配置成立即自销毁。

[0077] 在一种设计中，设备可纳入能感测并阻止侵入式篡改和/或非侵入式篡改的防篡改安全硬件。侵入式篡改可包括打开壳体、移除电源、在壳体中钻小孔以进入内部等。非侵入式篡改可包括超快速冷却以阻止感测到电源的移除、高频观测以检查位状态等等。对设备的篡改还可基于其它准则来检测，诸如访问敏感信息的反复尝试、设备上某些组件的故障等等。设备还可按照其它方式来检测它是否已经由侵入式或非侵入式的方式被篡改。

[0078] 在一种设计中，设备可例如在确定它丢失之前或之后确定它是否已被篡改。设备可在检测到它已被篡改时采取纠正动作。在一种设计中，设备在确定它已被篡改时可立即擦除该设备上的信息。在另一设计中，设备在确定其已被篡改时可立即锁定对该设备和/或该设备上的信息的访问。设备还可在检测到篡改时立即执行其它动作(例如，优先级列表中的任何动作)。

[0079] 图1示出了检测并处理丢失的设备的示例性设计。一般而言，上述特征中的一个或多个特征可被实现以处理丢失的设备。而且，上述特征可用于除丢失设备以外的其它情况。

[0080] 图2示出由设备执行的过程200的设计。设备可自主确定它丢失(框212)。响应于确定设备丢失，该设备可破坏该设备的至少一个组件以使该设备无法操作(框214)。例如，设备可破坏该设备上的存储器、CPU、GPU、显示器和/或其它某个组件。

[0081] 在一种设计中，当检测到设备已被掉落且在预定时间段内未被拾起时，该设备可确定它丢失。在另一设计中，当检测到设备在预定持续时间内未被移动时，该设备可确定它丢失。在又一设计中，设备可基于该设备的当前环境确定它丢失。设备可基于该设备的位置、该设备上的一个或多个传感器所感测到的结果、在该设备上运行的一个或多个应用、在该设备上访问的信息和/或其它准则来确定其当前环境。在一个设计中，设备可存储已知对该设备安全的环境的日志。设备可基于该设备的当前环境以及已知安全的环境的日志来确定它丢失。

[0082] 在一种设计中，设备可检测到它被篡改。设备可响应于检测到它被篡改而执行至少一个动作。这至少一个动作可包括阻止对该设备上的信息的访问、擦除该设备上的信息、阻止对该设备的访问等。

[0083] 图3示出由设备执行的过程300的设计。设备可响应于确定它丢失而确定该设备的可用电池电量(框312)。设备可基于该设备的可用电池电量来选择可能动作列表中的至少一个动作(框314)。可能动作列表可被区分优先级，且该设备可进一步基于可能动作列表中每一动作的优先级来选择该至少一个动作。该设备可执行该至少一个动作(框316)。

[0084] 设备可自主确定它丢失，或者可(例如由所有者经由通信链路)被通知它丢失。响应于确定设备丢失，该设备然后可在框312确定可用电池电量，在框314选择至少一个动作，并在框316执行该至少一个动作。响应于确定设备丢失，该设备可阻止对该设备的访问和/或对该设备上的信息的访问。

[0085] 在一种设计中，可能动作列表可包括当设备丢失时告知联系人列表的第一动作、备份该设备上的信息的第二动作、擦除该设备上的信息的第三动作、自销毁该设备的第四动作、某个其它动作、或其组合。可能动作列表可例如由该设备的所有者或该设备的可信实体为该设备专门配置。

[0086] 设备可检测该设备电池电量的再充电。在一种设计中，设备可响应于电池再充电而断言它未丢失。在另一设计中，设备可执行认证来确定该设备实际上是否丢失。在又一设计中，即使电池电量被再充电，设备也可继续认为它丢失。

[0087] 图4示出由设备执行的过程400的设计。设备可确定它丢失(框412)。设备可自主确定它丢失，或者可(例如由所有者经由通信链路)被通知它丢失。设备可基于副安全密钥来阻止对该设备上的信息的访问，该副安全密钥在该设备的正常操作期间不被用于对信息加密(框414)。

[0088] 在一种设计中，设备可在确定该设备丢失之前基于主安全密钥来加密信息以保护信息。设备可在确定该设备丢失之后基于副安全密钥来对已加密信息再次加密。在这种设计中，信息可基于两个安全密钥被加密。在另一设计中，设备可在确定该设备丢失之后仅基于副安全密钥来加密信息以保护信息。在又一设计中，设备可阻止对信息的访问，除非该设备(例如经由该设备上的用户接口或远程经由通信链路)接收到副安全密钥。在这种设计中，副安全密钥可按照类似于口令的方式被使用，且信息可不被加密。

[0089] 在一种设计中，副安全密钥可以是设备的所有者不可取得的，而是该设备的可信实体可取得的。在这种设计中，该所有者可通过将该设备带到该可信实体来恢复信息。在另一设计中，副安全密钥可以是设备的所有者可取得的，设备的所有者可以能够恢复信息。

[0090] 图5示出由设备执行的过程500的设计。设备可获得它丢失的指示(框512)。设备可响应于获得该指示而执行通知至少一个联系人的第一动作(框514)。设备可响应于获得该指示而执行动作列表中的至少一个附加动作(框516)。动作列表可包括备份该设备上的信息的第二动作、擦除该设备上的信息的第三动作、自销毁该设备的至少一部分的第四动作、某个其它动作、或其组合。

[0091] 设备可存储万一该设备丢失则要通知的联系人列表以及该列表中的联系人的联系信息。在一种设计中，设备可向至少一个联系人中的每一者通知该设备丢失。设备还可提供相关信息，诸如与该设备的位置相关的信息、与该设备的环境相关的信息、某种其它信息、或其组合。设备可从该设备通知到的至少一个联系人之中的一联系人接收响应。基于来自该联系人的响应，该设备可跳过该至少一个附加动作。

[0092] 图6示出设备600的设计的框图，该设备可以能够执行本文所述的技术。设备600可以是蜂窝电话、智能电话、PDA、膝上型计算机、平板设备、上网本、智能本、终端、手持机等。设备600可支持经由一个或多个无线通信网络的通信，无线通信网络可包括码分多址(CDMA)网络、全球移动通信系统(GSM)网络、长期演进(LTE)网络、WLAN等。

[0093] 设备600可支持经由接收路径和发射路径的双向通信。在接收路径中，由基站和/或其它设备发射的信号可由天线612接收并被提供给接收机(RCVR)614。接收机614可调理并数字化收到的信号并向数字段620提供输入采样以供进一步处理。在发射路径中，发射机(TMTR)616可从数字段620接收要传送的数据。发射机616可处理并且调理该数据并且可生成经调制信号，该经调制信号可经由天线612向基站和/或其它设备发射。

[0094] 数字段620可包括各种处理、接口和存储器组件，诸如举例而言CPU 622、控制器/处理器624、安全模块626、内部存储器628、GPU 632、电池电量检测器634、丢失设备检测器636、输入/输出(I/O)接口模块638、和位置确定模块640，所有这些可经由总线630通信。CPU 622可执行用于数据传送和接收的处理，例如编码、调制、解调、解码等。CPU 622还可为各种应用(诸如举例而言语音呼叫、web浏览、多媒体、游戏、用户接口、定位等)执行处理。GPU 632可执行对文本、图形和视频的处理，并可将其输出提供给显示器642。控制器/处理器624可指导数字段620内的各个处理和接口模块的操作。控制器/处理器624、CPU 622、和/或设备600中的其它模块可执行或指导图1中的过程100、图2中的过程200、图3中的过程300、图4中的过程400、图5中的过程500、和/或本文描述的技术的其它过程。

[0095] 安全模块626可安全地存储敏感信息、安全密钥、和/或用于设备600的其它信息。存储器628可为设备600存储信息和/或其它数据，且可包括RAM、SRAM等。电池电量检测器

634可确定电池644的可用电量。尽管未在图6中示出，设备600可包括备用电源(例如，备用电池)，当设备600被确定为丢失时，备用电源可确保有足够的电池电量来执行一个或多个动作。丢失设备检测器636可接收一个或多个传感器646的输出、确定设备600的环境、确定设备600是否丢失等。I/O接口模块638可促成数字段620与外部存储器648之间的数据传递。存储器648可包括RAM、SRAM、动态RAM(DRAM)、同步DRAM(SDRAM)、闪存等。模块640可基于卫星、基站和/或其它发射机站的测量来确定设备600的位置。

[0096] 数字段620可用一个或多个数字信号处理器(DSP)、微处理器、精简指令集计算机(RISC)等来实现。数字段620还可在一个或多个专用集成电路(ASIC)或某种其它类型的集成电路(IC)上实现。

[0097] 本文中所描述的技术可以提供各种优点。设备可自主地确定它是否丢失。设备可以能够自己这样做而不必连接到通信网络且不必由所有者或某个其它实体来告知。设备还可自己自主地执行一个或多个动作，而几乎或完全不需要来自所有者或某个其它实体的输入。设备可保护自己和存储在该设备上的信息不被访问、将信息备份到指定服务器上、破坏该设备上的信息、和/或执行其它动作。设备可基于动作的优先级和该设备的可用电池电量来选择要执行哪些动作，以使得当没有足够的电池电量来执行全部动作时较为重要的动作可被执行。

[0098] 本文所述的技术可提供比远程擦除请求更好的安全性，远程擦除请求可在所有者确定设备丢失时由该所有者向该设备发送。本技术不需要对通信网络的连接就能保护和/破坏设备上的信息。本技术还可为不想要处理用口令解锁其设备的持久麻烦的用户提供安全性措施。本技术可尤其适用于便携式电子设备，诸如智能电话、平板设备等。这些便携式电子设备可具有类似计算机的能力，但与计算机相比更易于携带并易于在各个位置丢失。

[0099] 本领域技术人员将理解，可使用各种各样的不同技术和技艺中的任何技术和技艺来表示信息和信号。例如，以上描述通篇可能引述的数据、指令、命令、信息、信号、位(比特)、码元、和码片可由电压、电流、电磁波、磁场或磁粒子、光场或光学粒子、或其任何组合来表示。

[0100] 技术人员将进一步领会，结合本文公开所描述的各种解说性逻辑块、模块、电路、和算法步骤可被实现为电子硬件、计算机软件、或两者的组合。为清楚地解说硬件与软件的这一可互换性，各种解说性组件、框、模块、电路、和步骤在上面是以其功能性的形式作一般化描述的。此类功能性是被实现为硬件还是软件取决于具体应用和施加于整体系统的设计约束。技术人员可针对每种特定应用以不同方式来实现所描述的功能性，但此类实现决策不应被解读为致使脱离本公开的范围。

[0101] 结合本文公开描述的各种解说性逻辑块、模块、以及电路可用设计成执行本文中描述的功能的通用处理器、DSP、ASIC、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合来实现或执行。通用处理器可以是微处理器，但替换地，处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可以被实现为计算设备的组合，例如DSP与微处理器的组合、多个微处理器、与DSP核心协同的一个或多个微处理器、或任何其它此类配置。

[0102] 结合本文的公开所描述的方法或算法的步骤可直接在硬件中、在由处理器执行的软件模块中、或在这两者的组合中实施。软件模块可驻留在RAM存储器、闪存、ROM存储器、

EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动盘、CD-ROM、或本领域内已知的任何其它形式的存储介质中。示例性存储介质耦合到处理器以使得该处理器能从该存储介质读取信息以及向该存储介质写入信息。替换地，存储介质可以被整合到处理器。处理器和存储介质可驻留在ASIC中。ASIC可驻留在用户终端中。替换地，处理器和存储介质可作为分立组件驻留在用户终端中。

[0103] 在一个或多个示例性设计中，所描述的功能可以在硬件、软件、固件、或其任何组合中实现。如果在软件中实现，则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。计算机可读介质包括计算机存储介质和通信介质两者，包括促成计算机程序从一地向另一地转移的任何介质。存储介质可以是能被通用或专用计算机访问的任何可用介质。作为示例而非限定，此类计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储、磁盘存储或其它磁存储设备、或能被用来携带或存储指令或数据结构形式的期望程序代码手段且能被通用或专用计算机、或者通用或专用处理器访问的任何其它介质。任何连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)、或诸如红外、无线电、以及微波之类的无线技术从web网站、服务器、或其它远程源传送而来，则该同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之中。如本文中所使用的盘(disk)和碟(disc)包括压缩碟(CD)、激光碟、光碟、数字多用碟(DVD)、软盘和蓝光碟，其中盘(disk)往往以磁的方式再现数据，而碟(disc)用激光以光学方式再现数据。上述的组合也应被包括在计算机可读介质的范围内。

[0104] 提供对本公开的先前描述是为了使得本领域任何技术人员皆能够制作或使用本公开。对本公开的各种修改对本领域技术人员来说都将是显而易见的，且本文中所定义的普适原理可被应用到其它变体而不会脱离本公开的精神或范围。由此，本公开并非旨在被限定于本文中所描述的示例和设计，而是应被授予与本文中所公开的原理和新颖性特征相一致的最广范围。

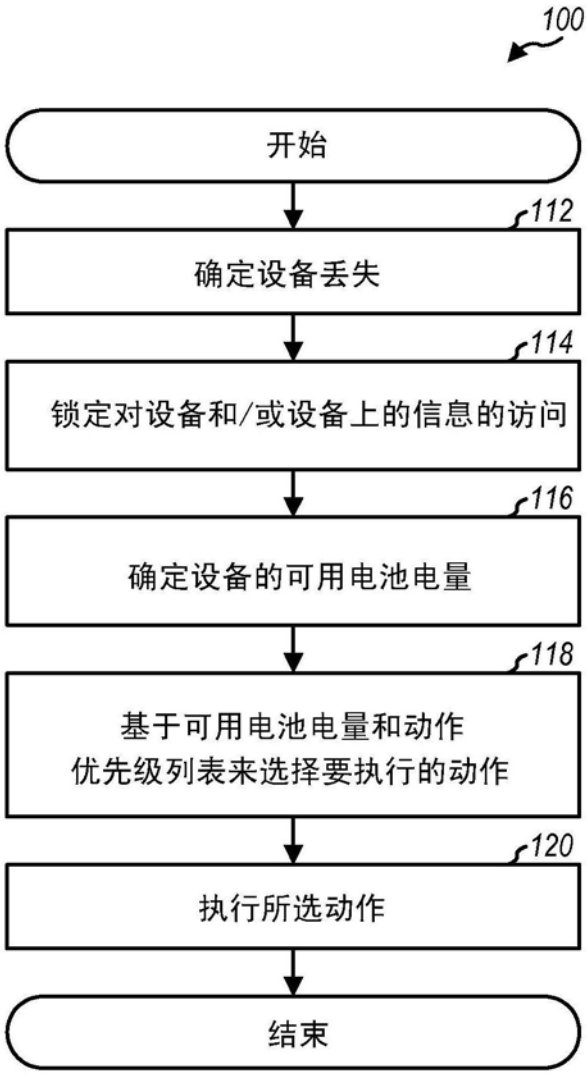

100
开始
112
确定设备丢失
114
锁定对设备和/或设备上的信息的访问
116
确定设备的可用电池电量
118
基于可用电池电量和动作
优先级列表来选择要执行的动作
120
执行所选动作
结束

图1

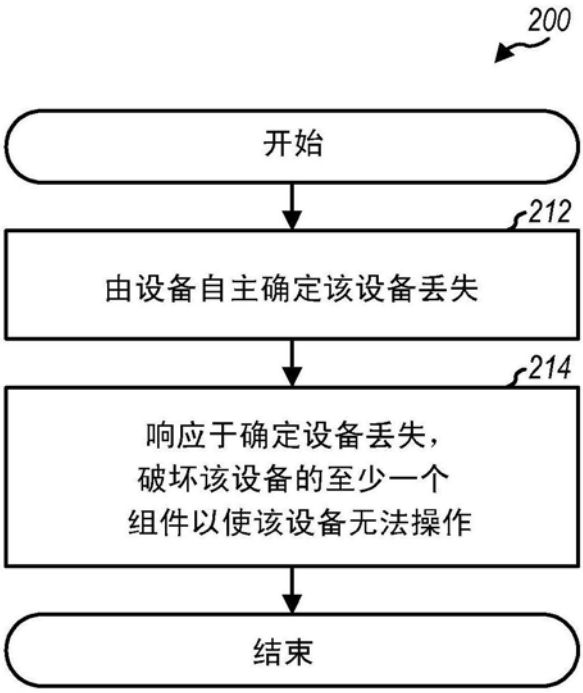

200
开始
212
由设备自主确定该设备丢失
214
响应于确定设备丢失，
破坏该设备的至少一个
组件以使该设备无法操作
结束

图2

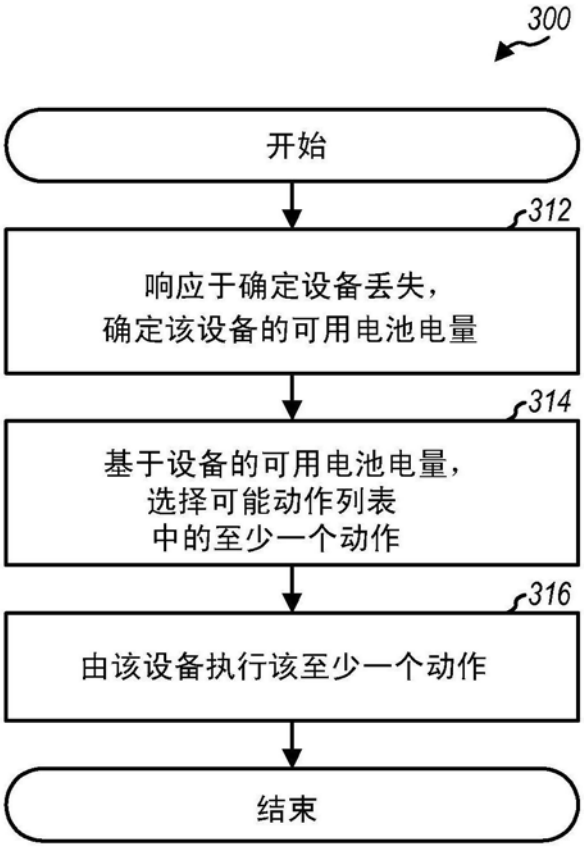

300
开始
312
响应于确定设备丢失，
确定该设备的可用电池电量
314
基于设备的可用电池电量，
选择可能动作列表
中的至少一个动作
316
由该设备执行该至少一个动作
结束

图3

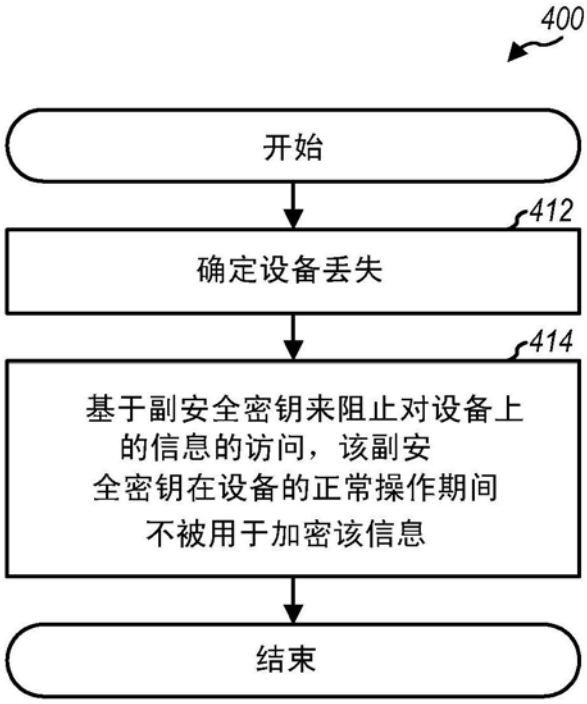

400
开始
412
确定设备丢失
414
基于副安全密钥来阻止对设备上的信息的访问，该副安全密钥在设备的正常操作期间不被用于加密该信息
结束

图4

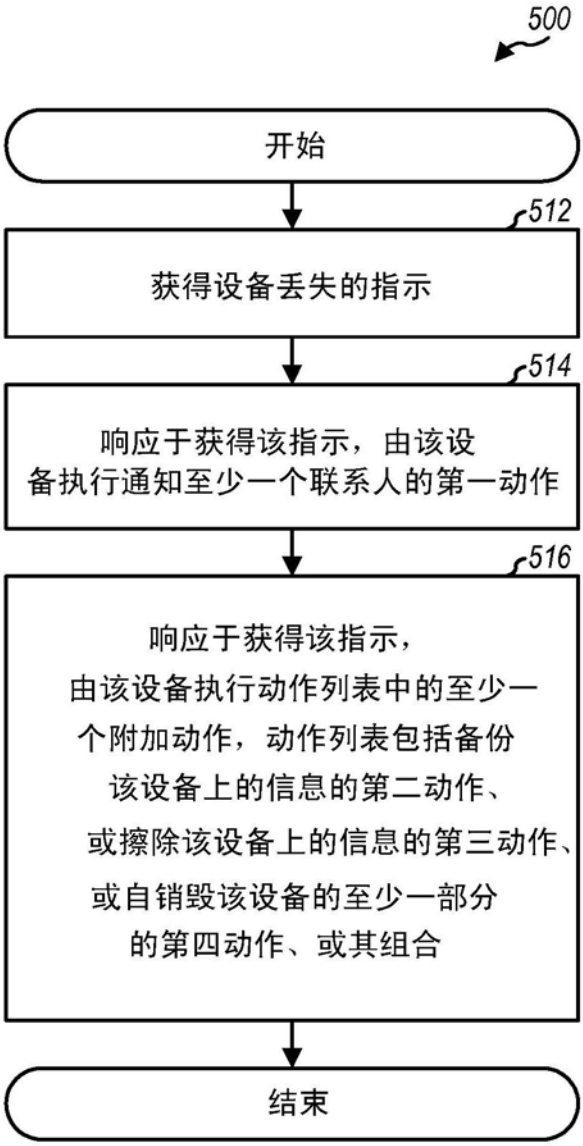

500
开始
512
获得设备丢失的指示
514
响应于获得该指示，由该设备执行通知至少一个联系人的第一动作
516
响应于获得该指示，由该设备执行动作列表中的至少一个附加动作，动作列表包括备份该设备上的信息的第二动作、或擦除该设备上的信息的第三动作、或自销毁该设备的至少一部分的第四动作、或其组合
结束

图5

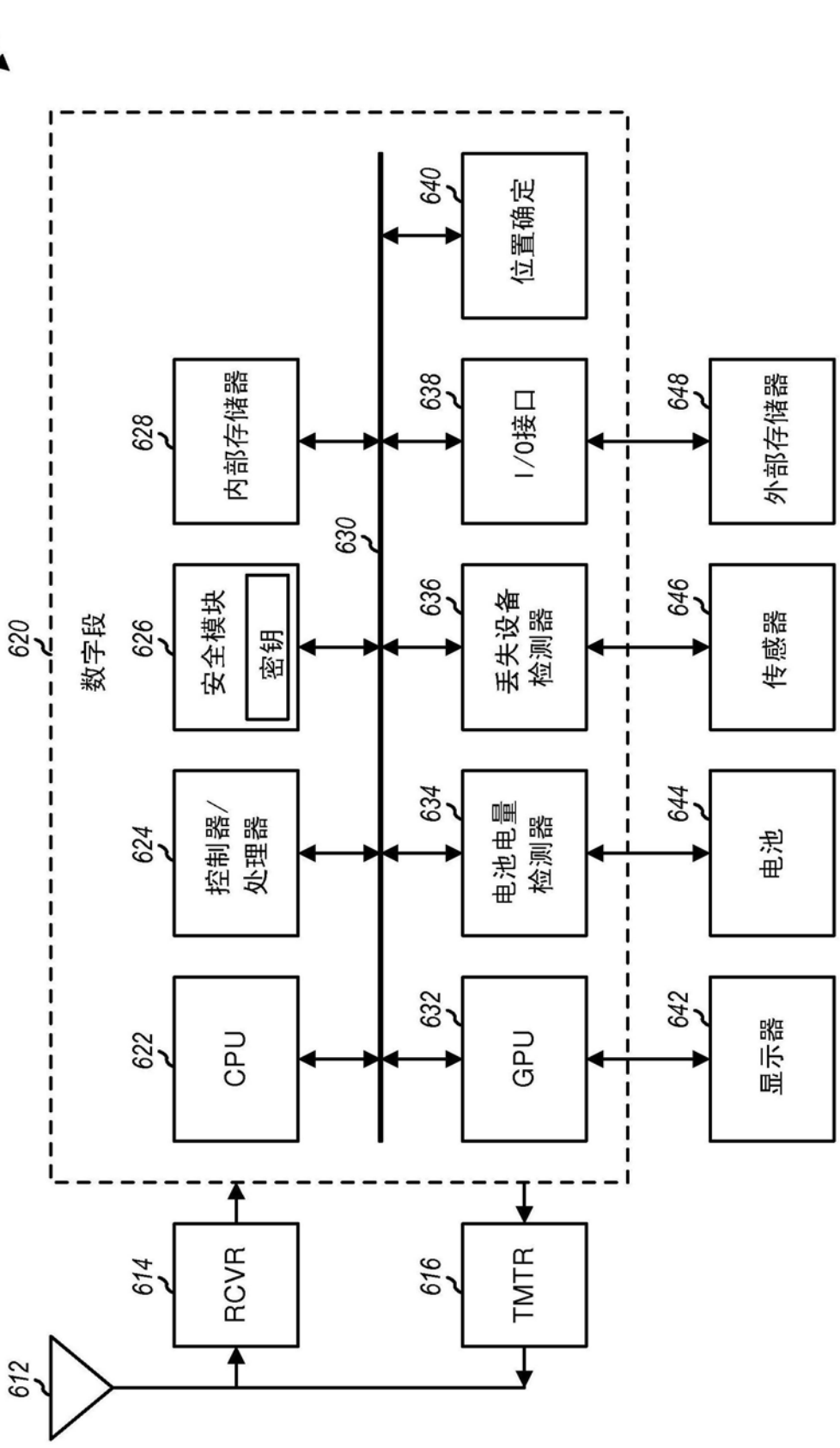

600
620
数字段
622
CPU
624
控制器/处理器
626
安全模块
密钥
628
内部存储器
630
632
GPU
634
电池电量检测器
636
丢失设备检测器
638
I/O接口
640
位置确定
642
显示器
644
电池
646
传感器
648
外部存储器
612
614
RCVR
616
TMTR

图6