



(12) 发明专利

(10) 授权公告号 CN 101896914 B

(45) 授权公告日 2014. 10. 29

(21) 申请号 200880120599. 5

(51) Int. Cl.

(22) 申请日 2008. 11. 07

G06F 21/78 (2013. 01)

(30) 优先权数据

11/936, 471 2007. 11. 07 US

(56) 对比文件

(85) PCT国际申请进入国家阶段日

2010. 06. 12

US 2002/0162011 A1, 2002. 10. 31,
US 2005/0138390 A1, 2005. 06. 23,
US 4593384, 1986. 06. 03,
US 2005/0198525 A1, 2005. 09. 08,

(86) PCT国际申请的申请数据

PCT/US2008/082878 2008. 11. 07

审查员 徐春

(87) PCT国际申请的公布数据

W02009/062092 EN 2009. 05. 14

(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 柯克·S·泰勒

吉列尔梅·路易斯·卡纳斯·赫费尔

杰克·斯藤斯特拉 陈立仁

卢奇安·舒塔 张扬

(74) 专利代理机构 北京律盟知识产权代理有限

责任公司 11287

代理人 刘国伟

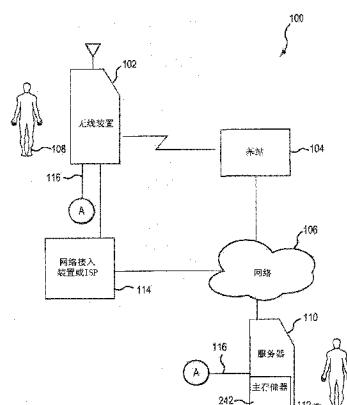
权利要求书2页 说明书8页 附图8页

(54) 发明名称

用于擦除无线装置上的存储器的系统、方法和设备

(57) 摘要

提供一种具有存储器的无线装置。如果多个传感器指示存在对所述装置的威胁，那么所述存储器或所述存储器的受保护部分经受所述存储器的硬擦除（对照所述存储器的软擦除）。所述威胁可由多个传感器检测，所述传感器例如是定时器、连接性传感器、位置传感器或越界报警、破坏传感器、验证程序等。



1. 一种用于基于威胁确定而自动硬擦除无线装置上的数据以制止对数据的未授权存取的由所述无线装置执行的方法, 所述方法包括 :

在所述无线装置的存储器空间内存储个人和 / 或敏感性数据 ;

监视所述无线装置上的验证码的输入 ;

基于所述监视, 确定所述所输入的验证码是否正确、评估所述所输入的验证码与正确的码的接近性、及其确定所述所输入的验证码是否超过阈值尝试数目 ;

监视所述无线装置中的传感器, 所述传感器提供与所述无线装置的状态有关的信息, 所述监视传感器包括 :

监视所述无线装置的外壳看是否被破坏 ;

监视所述无线装置的不活动期 ;

监视定位传感器以确定所述无线装置是否已离开地理边界 ; 以及

监视连接性传感器以确定所述无线装置是否已离开网络覆盖区域 ;

基于来自所述传感器的与所述无线装置的所述状态有关的所述信息, 自动确定是否存在对所述无线装置中所含有的数据的威胁 ;

响应于下述四种情况中的任一种情况 : 所述所输入的验证码错误、所述所输入的验证码与所述正确的验证码不充分接近、所述所输入的验证码超过所述阈值尝试数目、或确定存在对包括在所述无线装置内的数据的威胁, 向用户提示需要硬擦除中断码, 以中断数据的硬擦除 ;

确定是否已在预定的时间帧内输入硬擦除中断码 ;

若确定已在所述预定的时间帧内正确地输入所述硬擦除中断码, 则终止或推迟数据的硬擦除 ; 以及

若确定未在所述预定的时间帧内正确地输入所述硬擦除中断码, 则通过使用新数据替换所述存储器空间内的所述个人和 / 或敏感性数据, 来硬擦除包括在所述无线装置上的所述数据。

2. 根据权利要求 1 所述的方法, 其进一步包括 :

检测选自由 MP3 播放器、音频 / 视频装置和电子医疗装置所组成的群组中的插入式模块何时从所述无线装置的串行数据端口去除 ; 以及

将与所去除的插入式模块相关联的数据从所述无线装置的所述存储器中硬擦除。

3. 根据权利要求 1 所述的方法, 其进一步包括 :

所述无线装置检测与另一装置上的主存储器的数据同步 ; 以及

所述无线装置将所述经同步的数据从所述无线装置的所述存储器中硬擦除。

4. 根据权利要求 1 所述的方法, 其中在硬擦除所述个人和 / 或敏感性数据之前, 将所述个人和 / 或敏感性数据上载到主存储器。

5. 一种用于基于威胁确定而自动硬擦除无线装置上的数据以制止对数据的未授权存取的由所述无线装置执行的装置, 所述装置包括 :

用于在所述无线装置的存储器空间内存储个人和 / 或敏感性数据的装置 ;

用于监视所述无线装置上的验证码的输入的装置 ;

用于基于所述监视, 确定所述验证码是否正确、评估所述所输入的验证码与正确的码的接近性、及其确定所述所输入的验证码是否超过阈值尝试数目的装置 ;

用于监视所述无线装置中的传感器的装置,所述传感器提供与所述无线装置的状态有关的信息,所述用于监视所述传感器的装置包括:

用于监视所述无线装置的外壳看是否被破坏的装置;

用于监视所述无线装置的不活动期的装置;

用于监视定位传感器以确定所述无线装置是否已离开地理边界的装置;以及

用于监视连接性传感器以确定所述无线装置是否已离开网络覆盖区域的装置;

用于基于来自所述传感器的与所述无线装置的所述状态有关的所述信息,自动确定是否存在对所述无线装置中所含有的数据的威胁的装置;

用于响应于所述所输入的验证码错误、所述所输入的验证码与正确的码不充分接近、所述所输入的验证码超过阈值尝试数目、或确定存在对包括在所述无线装置内的数据的威胁四种情况中的任一种情况,向用户提示需要硬擦除中断码,以中断数据的硬擦除的装置;

用于确定是否已在预定的时间帧内输入硬擦除中断码的装置;

用于若确定已在所述预定的时间帧内正确地输入所述硬擦除中断码,则终止或推迟数据的硬擦除的装置;以及

用于若确定未在所述预定的时间帧内正确地输入所述硬擦除中断码,则通过使用新数据替换所述存储器空间内的所述个人和 / 或敏感性数据,来硬擦除包括在所述无线装置上的所述数据的装置。

6. 根据权利要求 5 所述的装置,其进一步包括:

用于检测选自由 MP3 播放器、音频 / 视频装置和电子医疗装置所组成的群组中的插入式模块何时从所述无线装置的串行数据端口去除的装置;以及

用于将与所去除的插入式模块相关联的数据从所述无线装置的所述存储器中硬擦除的装置。

7. 根据权利要求 5 所述的装置,其进一步包括:

用于检测与另一装置上的主存储器的数据同步的装置;以及

用于将所述经同步的数据从所述无线装置的所述存储器中硬擦除的装置。

8. 根据权利要求 5 所述的装置,其进一步包括:

用于在硬擦除所述个人和 / 或敏感性数据之前,将所述个人和 / 或敏感性数据上载到主存储器的装置。

用于擦除无线装置上的存储器的系统、方法和设备

技术领域

[0001] 本申请案的技术大体上涉及为无线装置擦除存储器，且更具体地说，涉及用于在威胁或不当存取或试图存取是可能的时硬擦除无线装置上的存储器的系统、方法和设备。

背景技术

[0002] 无线装置且特别是蜂窝式电话如今是普遍存在的。蜂窝式电话（例如）不再仅仅是提供个人之间的语音通信的装置，而现在是强大的处理装置。蜂窝式电话（例如）可用于存储和处理数据。在本文中，蜂窝式电话或手机可与无线装置互换使用，但无线装置不限于蜂窝式电话，且可包含其它无线装置，例如桌上型计算机、膝上型计算机、手持式计算机、电子游戏、便携式数字助理、MP3 播放器、DVD 播放器等。

[0003] 随着蜂窝式电话的处理和存储能力的增加，人们已开始将个人、敏感性和有时令人困窘的信息存储在其蜂窝式电话或无线装置上。所述信息可包含（例如）银行业务信息、个人健康信息、图片、视频剪辑、联系人名单、信用卡信息等。

[0004] 虽然将个人和敏感性信息保存在蜂窝式电话上是方便的，但这导致一些问题。一些蜂窝式电话丢失或被盗。此外，蜂窝式电话经常在二手市场上出售。因此，删除个人、敏感性且令人困窘的信息是必要的。

[0005] 使用常规技术来从存储器擦除信息涉及向处理器指示存储器空间能够自由用以接收来自写入（或读取 / 写入）模块的新信息。然而，在写入模块将新信息写入到存储器空间之前，数据仍存储在存储器中。因此，换句话说，只是指向数据的指针被擦除了，且数据仍存储在存储器中。为了方便，删除指针而不是数据被称为“软擦除”。一些公司已开始通过允许蜂窝式电话的拥有者或用户对电话进行“硬擦除”来解决此问题。在本申请案中，硬擦除表示向处理器指示存储器空间可用，以及积极地用新数据来代替存储器空间中的数据。新数据可为预定义的数据系列或随机数据。

[0006] 目前，一些蜂窝式电话提供用于起始硬擦除协议的机制。举例来说，一种机制要求在装置上输入密码。通过输入密码，所述装置起始硬擦除协议。密码可从蜂窝式电话直接输入，或使用常规的无线数据协议从单独的位置传输到电话。其它蜂窝式装置通过键击或其它预定义协议来实现硬擦除。

[0007] 尽管用于存储在蜂窝式电话存储器中的数据的硬擦除的一些机制是可用的，但将希望提供用于硬擦除蜂窝式和其它无线装置中的存储器的经改进的系统、方法和设备。

发明内容

[0008] 本文所揭示的实施例通过提供用以在检测到威胁时硬擦除无线装置的存储器的威胁检测器和硬擦除模块来解决上文所陈述的需要。所述威胁可为对装置的实际物理威胁，或指示无线装置已经丢失、被盗或以其它方式被损害的可能性的其它指示。

[0009] 在一个方面中，提供一种用于基于威胁确定而自动硬擦除无线装置上的数据以制止对数据的未授权存取的方法。所述方法包括：监视无线装置中的至少一个传感器，其提供

与无线装置的状态有关的信息。使用所感测到的关于状态的信息来作出关于是否存在对数据的威胁的确定,以及基于所述威胁确定而硬擦除存储在无线装置上的数据。

[0010] 在另一方面中,提供一种存储器管理方法。存储器管理去除被确定为无线装置不需要的数据。

[0011] 在又一方面中,提供一种无线装置。所述无线装置包含:控制处理器控制器处理器,用于控制无线装置的功能;以及存储器,其存储可由控制处理器用来执行无线装置的功能的可执行代码以及数据。所述无线装置包含发射和接收电路,其用以提供对天线与控制处理器之间的通信信号的调制和解调。威胁检测器监视无线装置,以确定对存储在存储器中的数据的威胁,且硬擦除模块用以根据来自威胁检测器的威胁指示而硬擦除所述存储器的至少一部分以去除数据。

[0012] 从以下对如附图中所说明的本发明的实施例的更具体描述中将明白所述装置和系统的前述和其它特征、效用和优点。

附图说明

- [0013] 图 1 是本发明的示范性实施例的无线通信系统的框图说明;
- [0014] 图 2 是本发明的示范性实施例的无线装置的框图说明;
- [0015] 图 3 是说明用于操作示范性实施例的无线装置的操作步骤的流程图;
- [0016] 图 4 是说明用于操作示范性实施例的无线装置的操作步骤的流程图;
- [0017] 图 5 是说明示范性实施例的威胁检测器的操作步骤的流程图;
- [0018] 图 6 是说明示范性实施例的手动硬擦除的操作步骤的流程图;
- [0019] 图 7 是说明示范性实施例的存储器管理的操作步骤的流程图;
- [0020] 图 8 是说明示范性实施例的存储器管理的操作步骤的流程图;以及
- [0021] 图 9 是说明示范性实施例的在硬擦除存储器之前加载存储器的操作步骤的流程图。

具体实施方式

[0022] 现在将参考图式来描述本申请案的技术。虽然具体参考蜂窝式电话来描述所述技术,但所属领域的技术人员在阅读本发明之后将认识到,所描述的技术适用于其它无线装置,例如手持式计算机、膝上型计算机、桌上型计算机等。无线装置与蜂窝式电话在本文中可互换使用。此外,参考具体的示范性实施例来描述本申请案的技术。词“示范性”在本文中用于表示“充当实例、例子或说明”。本文描述为“示范性”的任何实施例不一定被解释为比其它实施例优选或有利。此外,本文所描述的所有实施例应被视为示范性的,除非另有陈述。

[0023] 词“网络”在本文中用于表示使用适当的网络数据传输协议的一个或一个以上常规或专有网络。这些网络的实例包含:PSTN、LAN、WAN、WiFi、WiMax、因特网、万维网、以太网、其它无线网络等。

[0024] 短语“无线装置”在本文中用于表示使用射频传输技术的一个或一个以上常规或专有装置。这些无线装置的实例包含蜂窝式电话、桌上型计算机、膝上型计算机、手持式计算机、电子游戏、便携式数字助理、MP3 播放器、DVD 播放器等。

[0025] 短语“软擦除”在本文中用于表示指示存储器的一部分可用于接受新数据。可通过删除数据查找表或类似物中的信息来指示可用性。

[0026] 短语“硬擦除”在本文中用于表示指示存储器的一部分可用于接受新数据，且用预定的数据串或随机数据盖写存储器字段。

[0027] 图 1 说明示范性实施例的无线通信网络 100。在此实施例中，无线通信网络 100 包含无线装置 102，其可由个人或用户 108 使用，通过无线通信链路连接到与网络 106 互连的基站 104，网络 106 可为单个网络或不同网络的组合，例如公共交换电话网 (PSTN) 或因特网，仅以两个可能网络为例。此实施例中还包含服务器 110，其与网络 106 互连。服务器 110 可由网络管理员 112 接入而接入。虽然将无线装置 102 展示为经由基站 104 连接到网络 106，但有可能无线装置 102 可经由有线网络接入装置 114 或所提供的因特网服务直接连接到网络 106。无线装置 102 可使用有线连接（例如通用串行总线）或无线连接（例如蓝牙连接）等连接到网络接入装置 114。无线装置 102 还可经由直接常规连接 116（例如 USB 缆线、其它数据端口连接、蓝牙连接或另一局部无线连接）而直接连接到服务器 110。

[0028] 现在参看图 2，更详细地展示无线装置 102 的示范性实施例。无线装置包含包括控制处理器 202 的若干组件。控制处理器 202 控制无线装置 102 的主要功能，包含提供计算功能性以处理无线装置 102 的操作所需的输入和 / 或数据。发射 / 接收电路 204 连接到控制处理器 202 和天线 206。发射 / 接收电路 204 可为一个或一个以上实际电路，且可在各种协议和波长上起作用。发射 / 接收电路 204 像无线通信中所使用的组件那样典型地起作用，例如调制从控制处理器 202 接收到的将从天线 206 发射的信号，以及解调在天线 206 处接收到的信号。将经调制的信号提供给控制处理器 202。无线装置 102 还提供用户接口 208。用户接口 208 可包括对蜂窝式电话来说典型的或对无线装置来说典型的用户接口，例如键盘、字母数字盘、鼠标、跟踪球、触摸屏、语音识别、麦克风、扬声器、数据端口、输入端口、视频输入（相机或类似物）等。无线装置的用户经由用户接口 208 存取、接收和发射信息。无线装置 102 包含连接到控制处理器 202 的存储器 210。存储器 210 可存储对无线装置 102 的操作来说必要或方便的数据和处理指令。存储器 210 可包含任何合适媒体上的易失性和 / 或非易失性存储器。存储器 210 可包括多个存储器，但提供单个存储器。存储器 210 还存储由用户输入的信息。此信息可（例如）包含经由用户接口 208 输入的信息（包含图片、文本信息、视频等），以及从远程处理器接收到的信息。远程处理器可为（例如）上文所描述的服务器 110，其可经由网络 106 或直接连接 116 连接到无线装置 102。此信息还可包含由无线装置 102 经由其它机制接收到的信息，例如驻存在无线装置 102 上的应用程序可接收或产生信息，且将此信息存储在存储器 210 中。此信息的一个实例包含将信息下载到无线装置 102 的电子医疗装置 212，无线装置可存储所述信息以最终发射或下载给护理者、医务人员等。电子医疗装置 212 可集成到无线装置 102 中，或与无线装置 102 分开（如图所示）。如果分开，那么可使用任何连接着的连接（例如到达串行数据端口 216 的有线连接 214、到达蓝牙天线 220 的无线连接 218 等）来将信息从电子医疗装置 212 发射到无线装置 102。虽然将关于用户的医疗信息来描述本申请案的技术，但所属领域的技术人员现在将认识到其它类型的个人信息可受益于本发明。其它类型的个人信息包含图片、音频剪辑、视频剪辑、音频 / 视频剪辑、金融信息、购买信息、位置信息、密码、客户名单等。

[0029] 存储器 210 的一些部分（受保护存储器 210p）仅在对存取受保护存储器 210p 的

许可被验证之后才可存取。对受保护存储器 210p 的存取权可由控制处理器 202 使用已知的保护技术（包含密码保护、生物保护（语音印迹、指纹、眼睛扫描等）、加密等）来授予。

[0030] 无线装置 102 还包含威胁检测器 222 和硬擦除模块 224。威胁检测器 222 如下文所阐释监视无线装置 102 的状态，且使用监视到的状态来确定对无线装置 102 上的数据的未授权或不当存取是可能的。威胁检测器 222 使用监视到的信息作为用于指示无线装置 102 已被盗、丢失或正被不当使用的代表。威胁检测器 222 和硬擦除模块 224 可根据设计选择而为独立的装置（如图所示）、组合成单个装置、并入控制处理器 202 或无线装置 102 的其它部分中。威胁检测器 222 和硬擦除模块 224 可直接连接或经由控制处理器 202 连接。如下文将进一步阐释，威胁检测器 222 监视无线装置 102，看是否有存取存储器 210 或受保护存储器 210p 的不当请求。在检测到威胁后，威胁检测器 222 将向硬擦除模块 224 提供威胁警告或硬擦除请求，以硬擦除存储器 210、受保护存储器 210p、存储器 210 或 210p 的指定部分或其组合。威胁检测器 222 可根据设计选择而并入服务器 110 而不是无线装置 102 中。在一些情况下，可能优选使威胁检测器 222 并入无线装置 102 中，且在一些情况下，可能优选使威胁检测器 222 并入服务器 110 或无线装置 102 与服务器 110 两者的组合中。

[0031] 威胁检测器 222 可包含传感器阵列 226。传感器阵列 226 可监视无线装置 102，看是否有不当活动，包含（例如）传感器阵列 226 可提供围绕无线装置 102 的周边的电子电路 228。如果个人不当地试图打开无线装置 102，电子电路 228 将从闭路转换为开路。开路检测将向威胁检测器 222 指示将触发硬擦除模块 224 以执行存储器的硬擦除的潜在威胁。其它传感器阵列将类似地监视对无线装置 102 的不当物理活动，且类似地向威胁检测器 222 提供触发存储器的硬擦除的警告等。

[0032] 如果存储器 210 具有仅在适当验证之后才可存取的受保护部分 210p，那么威胁检测器 222 将监视验证程序以确定是否存在威胁。如果（例如）输入不正确的密码超过预定次数（例如 5 次），那么威胁检测可发生。对于生物测量，如果生物测量是不正确的，那么威胁检测可发生。

[0033] 威胁检测器 222 可并入有评估模块 230。评估模块 230 可在确定是否存在威胁之前作出关于验证的接近性的确定。举例来说，威胁检测器 222 可经编程以在密码被不正确地输入 5 次的情况下触发硬擦除模块 224 的硬擦除，不管不正确的密码有多么接近正确的密码。然而，如果单次不正确的输入与正确的密码相差甚远，那么评估模块 230 可在所述输入之后评估威胁。如果密码（例如）为 12345，且输入为 12354，那么评估模块 230 可将换位识别为充分接近，而不发送威胁警告。然而，如果所提供的输入为 94870，那么评估模块 230 将识别与实际密码无相似性，且在单次密码尝试之后发送威胁警告。或者，评估模块 230 可并入控制处理器 202 中、作为独立单元等。

[0034] 此外，评估模块 230 可具备对无线装置 102 的状态的不同敏感性。如上文和下文所阐释，无线装置 102 可与同（例如）服务器 110 相关联的主（且通常是远程）存储器同步。如果存储器 210、受保护的存储器 210p、存储器 210 与受保护的存储器 210p 的组合等已与主存储器同步，那么评估模块 230 可经设置以用于更主动的威胁检测，因为存储器损失的成本因同步化而降低。然而，随着无线装置 102 增加未同步数据的量，评估模块 230 可被设置（手动或自动）为在威胁检测中的主动性较小，这归因于与通过硬擦除程序不可挽回地删除存储器和数据相关联的相对较高的成本。因此，评估模块可提供可调整标度（手

动或自动),以平衡丢失有价值的信息或数据的风险与信息泄漏的风险。此可调整标度可基于大量因素,包含(例如)存储到装置的数据的量,以及未上载到主存储器的数据的量等。

[0035] 如下文进一步阐释,在触发存储器 210 的硬擦除之前,威胁检测器 222 可致使控制处理器 202 尝试将适当的存储器 210 上载到服务器 110,以保存用户的数据。

[0036] 威胁检测器 222 还应能够接收来自控制处理器 202 的硬擦除请求。在此情况下,无线装置 102 的用户可使用用户接口 208 来输入请求。或者,无线装置 102 的用户还可发射来自服务器 110 或所连接的单独装置(其可与无线装置 102 通信)的导致硬擦除的请求。

[0037] 威胁检测器 222 还可连接其它传感器 226。举例来说,威胁检测器 222 可包含定时器 232。定时器 232 可与控制处理器 202、威胁检测器 222 等成一体式,或可为单独的单元,如图所示。定时器 232 可在无线装置在使用中时、在密码被输入时或在到达网络 106 的连接被建立时或类似时间复位。在预定的时期(其将可能为相对较长的时间,但可为若干分钟、小时、天、月、周等)之后,定时器 232 将向威胁检测器 222 提供不活动装置指示。威胁检测器 222 将不活动装置指示视为威胁,因为不活动将是已丢失或被盗无线装置的代表,且导致硬擦除。在起始硬擦除之前,任选地,威胁检测器 222 可请求来自用户的密码。如果密码被不正确地输入,或在某一时期内未接收到响应,那么硬擦除可触发。

[0038] 威胁检测器 222 还可包含定位传感器 234。定位传感器 234 可与控制处理器 202 或威胁检测器 222 集成,或为单独的单元(如图所示)。定位传感器 234 能够确定无线装置 102 的位置。定位传感器 234 将向威胁检测器 222 提供定位信息(例如从全球定位卫星系统),且如果无线装置 102 在预定位置边界之外,那么威胁检测器 222 可确定存在威胁。

[0039] 威胁检测器 222 还可包含连接性传感器 236。连接性传感器 236 可与控制处理器 202 或威胁检测器 222 集成,或为单独的单元(如图所示)。连接性传感器 236 监视与网络 106 的连接性。如果连接性传感器 236 确定在预定时期内尚未建立连接性,那么可向威胁检测器 222 提供连接性信号的缺乏,其将触发硬擦除。

[0040] 无线装置还可包含存储器管理模块 240。存储器管理模块 240 可与控制处理器 202 或威胁检测器 222 集成,或为单独的单元,如图所示。存储器管理模块 240 用于使存储器 210、受保护存储器 210p 或其组合中的个人信息减到最少。因此,存储器管理模块 240 将监视与主存储器 242(图 1)(例如与服务器 110 相关联的主存储器 242)的同步。主存储器 242 可与单独的处理器 118(图 1 中以阴影展示)相关联。单独的处理器 118 可为用户的个人计算机或任何常规装置。一旦与主存储器 242 的同步完成,存储器管理模块 240 就将向硬擦除模块 224 发送硬擦除信号,以致使经同步的数据从无线装置 102 的存储器 210、受保护存储器 210p 或其组合去除。

[0041] 一些无线装置 102 具备插入式模块 120,其以可装卸方式附接到无线装置 102。这些模块 120 可包含(例如)MP3 播放器、音频/视频装备、电子医疗装置等。这些可装卸模块 120 产生可存储在无线装置 102 中的存储器 210、受保护存储器 210p 或其组合中的数据。威胁检测器 222、存储器管理模块 240 等(例如作为传感器阵列 226 的一部分的单独的插入式装置监视器)可检测可装卸模块 120 何时从无线装置 102 去除,且致使硬擦除模块 224 对相关联的存储器进行硬擦除。

[0042] 威胁检测器 222 可向硬擦除模块 224 提供连续的“无威胁”信号。在此情况下,代替向硬擦除模块 224 提供触发信号以触发存储器的硬擦除,无威胁信号的不存在可触发

硬擦除功能。

[0043] 现在参看图3到图9,现在针对示范性实施例描述用于导致与无线装置102相关联的存储器硬擦除的操作步骤。起先,应注意,示范性实施例中的任一者中所描述的操作步骤被描述以提供实例和论述。所描述的操作可以不同于所说明序列的大量不同序列执行。另外,单个操作步骤中所描述的操作实际上可在许多不同步骤中执行。另外,示范性实施例中所论述的一个或一个以上操作步骤可组合。此外,被描述为在一个处理器处发生操作步骤可在其它处理器处执行。因此,将理解,流程图和图式中所说明的操作步骤可经受大量不同修改,如所属领域的技术人员在阅读本发明后将容易明白。此外,以下说明规定威胁检测器222与无线装置102位于同一地点。然而,威胁检测器222可根据所属领域的技术人员现在将认识到的设计选择而远程定位。

[0044] 首先参看图3,提供示范性实施例的通电操作300。首先,在步骤302处,对无线装置102供电。任选地,可提示用户108输入验证码(步骤304)。验证码可为使用用户接口208来输入密码、生物统计等。威胁检测器将评估密码输入,以确定其是否正确(步骤306)。如果验证码是正确的,那么无线装置102被启用以进行操作(步骤308)。如果验证码不正确,那么(任选地)进一步确定所输入的验证码是否充分地接近于正确的码以致成为错误(步骤310)。如果确定验证码并不充分地接近且/或任选步骤310未被执行,那么硬擦除模块224硬擦除存储器210或其指定部分(步骤312)。如果任选地确定验证码充分地接近,那么接下来确定是否已进行了预定数目的输入验证码输入尝试(步骤314)。如果确定尚未超过预定数目,那么在控制返回到步骤304时提示用户重新输入验证码。如果已超过预定数目,那么硬擦除模块224硬擦除存储器210或其指定部分(步骤312)。任选地,在硬擦除步骤312之前,无线装置102可向用户提示需要硬擦除中断码(步骤312a)。通常,将需要在预定的时间帧内输入中断码,否则擦除将继续。硬擦除中断码可不同于验证码。正输入的中断码可中断存储器的擦除,但将锁定无线装置的特征或那些特征的部分,直到适当的验证码被输入为止。虽然被描述为通电或上电说明性操作,但所属领域的技术人员在阅读本发明之后现在将认识到,操作300可适用于在预定的不活动期之后、在装置已被锁定的情况下、或在请求存取特定功能性或存储器的情况下存取无线装置102。

[0045] 接下来参看图4,提供示范性实施例的威胁监视操作400。在正常操作期间,威胁检测器222监视关于无线装置102的信息(下文将进一步阐释)看是否有威胁指示(步骤402)。如果检测到威胁,那么威胁检测器222致使硬擦除模块224擦除存储器210或其部分(步骤404)。任选地,在步骤403处,可向用户提示需要擦除中断码,以在硬擦除被不适当的情况下由用户中断硬擦除操作。通常,将需要在预定义的时间量内输入中断,以中断擦除。

[0046] 现在参看图5,提供威胁检测器222的示范性操作500。威胁检测器222从充当对存储器210的不适当存取的代理的多个传感器接收一系列输入(步骤502)。虽然被描述为多个传感器,但所属领域的技术人员在阅读本发明之后现在将认识到,在本文所描述的技术的范围和精神内,更多、更少或不同的输入是可能的。所述多个传感器可包含(例如)物理篡改传感器或外壳破坏传感器,例如电路228、定时器232、位置传感器234、连接性传感器236等,如上文所述。基于这些输入,威胁检测器222作出关于对无线装置102的威胁的各种确定。举例来说,基于来自电路228的输入,威胁检测器222确定用于无线装置102

的外壳是否正被破坏（步骤 504）。如果传感器指示外壳正被破坏，那么威胁检测器 222 致使硬擦除模块 224 擦除存储器 210 或其部分（步骤 506）。基于来自定时器 232 的输入，威胁检测器确定无线装置 102 是否已在预定量的时间内不活动（步骤 508）。如果确定装置已在预定量的时间内不活动，那么威胁检测器 222 推断所述装置被盗或丢失，且致使硬擦除模块 224 擦除存储器 210 或其部分（步骤 506）。基于来自位置传感器 234 的输入，威胁检测器确定无线装置 102 是否已离开预定义的边界或地理区域（步骤 510）。如果确定无线装置 102 已离开预定义的边界，那么威胁检测器 222 致使硬擦除模块 224 擦除存储器 210 或其部分（步骤 506）。基于来自连接性传感器 236 的输入，威胁检测器确定无线装置 102 是否已离开覆盖区域（步骤 512）。如果确定无线装置 102 已离开覆盖区域，那么威胁检测器 222 致使硬擦除模块 224 擦除存储器 210 或其部分（步骤 506）。如所提及，威胁检测器可触发比上文所述的传感器更多、更少或不同于上文所述的传感器的传感器。另外，威胁检测器可触发其组合，例如，如果威胁检测只可在位置传感器 234 确定装置在地理边界之外且装置已在所述边界之外历时定时器 232 所确定的预定时间时发生。任选地，在步骤 505a 和 505b 处，根据威胁检测器 222 的威胁指示，无线装置 102 可提示用户输入硬擦除中断码（步骤 505a）。如果输入中断码，那么硬擦除被终止或推迟（步骤 505b）。

[0047] 现在参看图 6，提供无线装置 102 的示范性操作 600，其中用户积极地发信号通知擦除存储器 210 或其部分。此操作通过提供硬擦除信号来向用户 108 提供远程硬擦除存储器 210 的能力。在此实例中，用户 108 将确定擦除存储器 210 或其部分的需要（步骤 602）。用户将直接或远程地存取服务器 110（步骤 604），且致使服务器 110 将擦除信号广播到无线装置 102（步骤 606）。擦除信号将致使威胁检测器 222 或控制处理器 202 触发硬擦除模块 224 擦除存储器 210（步骤 608）。任选地，在步骤 607 处，无线装置 102 可在擦除存储器之前，请求来自用户 108 的验证码。远程擦除可由用户 108 或管理员 112 导致。

[0048] 如可了解，以上操作是为了防止对存储器 210 中的个人、敏感性且可能令人困窘的信息的不当存取被第三方存取。上述内容还提供用于在特定条件下擦除信息的措施。然而，有可能使用存储器管理模块 240 来减少存储器 210 中的个人、敏感性且可能令人困窘的信息的量。现在参看图 7，提供存储器管理模块 240 的示范性操作 700。首先，存储器管理模块 240（或与无线装置相关联的某一其它组件）监视无线装置 102，看是否有插入式模块（步骤 702）。接下来，存储器管理模块 240 确定正监视的插入式模块是否从无线装置 102 拔去，例如电子媒体装置 212 是否从串行数据端口 216 去除（步骤 704）。如果确定装置被拔出，那么存储器管理模块 240 识别存储器 210 的与被拔去的模块相关联的部分（步骤 706）。最后，存储器管理模块 240 致使硬擦除模块 224 擦除存储器 210 的与被拔去的模块相关联的部分（步骤 708）。一旦不再需要信息，此举就将所述信息从存储器删除。

[0049] 参看图 8，提供存储器管理模块 240 的另一示范性操作 800。在此情况下，存储器管理模块监视无线装置 102，看是否有上载或与主存储器 242 的同步（步骤 802）。当检测到存储器 210 与主存储器 242 之间的存储器上载或同步时，存储器管理模块导致相关联的经上载存储器的硬擦除（步骤 804）。因此，当信息存储在较持久且安全的位置（即主存储器 242）中时，可将信息从较不安全的无线装置 102 中擦除。

[0050] 如上文所提及，且参看图 9，在任何硬擦除程序之前，可能希望尝试将信息从无线装置 102 上载到主存储器 242。如示范性操作 900 中所示，硬擦除模块 224 首先从威胁检测

器 222、存储器管理模块 240 或用户 108 中的任一者接收硬擦除请求（步骤 902）。接下来，硬擦除模块 224 确定是否存在到达主存储器 242 的链接（步骤 904）。如果确定存在链接，那么硬擦除模块 224 致使存储器 210 或其部分上载到主存储器 242（步骤 906）。一旦上载完成，或如果确定不存在链接，那么硬擦除模块 224 擦除存储器 210 或其部分（步骤 908）。

[0051] 所属领域的技术人员将理解，可使用多种不同技术和技法中的任一者来表示信息和信号。举例来说，可贯穿以上描述内容而参考的数据、指令、命令、信息、信号、位、符号和码片可由电压、电流、电磁波、磁场或磁微粒、光场或光学微粒或其组合来表示。

[0052] 所属领域的技术人员将进一步了解，结合本文所揭示的实施例而描述的各种说明性逻辑块、模块、电路和算法步骤可实施为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件与软件的这种可互换性，上文已大体上根据各种说明性组件、块、模块、电路和步骤的功能性而描述了各种说明性组件、块、模块、电路和步骤。将此功能性实施为硬件还是软件取决于特定应用和强加于整个系统的设计限制。熟练的技术人员可针对每个特定应用以不同的方式来实施所描述的功能性，但此类实施决策不应被解释为导致偏离本发明的范围。

[0053] 结合本文所揭示的实施例而描述的各种说明性逻辑块、模块和电路可用以下各项来实施或执行：通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其经设计以执行本文所描述的功能的任一组合。通用处理器可以是微处理器，但在替代方案中，所述处理器可以是任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算机装置的组合，例如 DSP 与微处理器的组合、多个微处理器、一个或一个以上微处理器结合 DSP 核心，或任何其它此类配置。

[0054] 结合本文所揭示的实施例而描述的方法或算法的步骤可直接以硬件、以由处理器执行的软件模块或以上述两者的组合的形式体现。软件模块可驻存在随机存取存储器（RAM）、快闪存储器、只读存储器（ROM）、电可编程 ROM（EPROM）、电可擦除可编程 ROM（EEPROM）、寄存器、硬盘、可装卸盘、CD-ROM 或此项技术中已知的任何其它形式的存储媒体中。示范性存储媒体耦合到处理器，使得处理器可从存储媒体读取信息和将信息写入到存储媒体。在替代方案中，存储媒体可与处理器成一体式。

[0055] 提供对所揭示实施例的先前描述，以使所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易明白对这些实施例的各种修改，且本文所界定的一般原理可在不脱离本发明的精神或范围的情况下应用于其它实施例。因此，本发明无意限于本文所示的实施例，而是应被赋予与本文所揭示的原理和新颖特征一致的最宽范围。

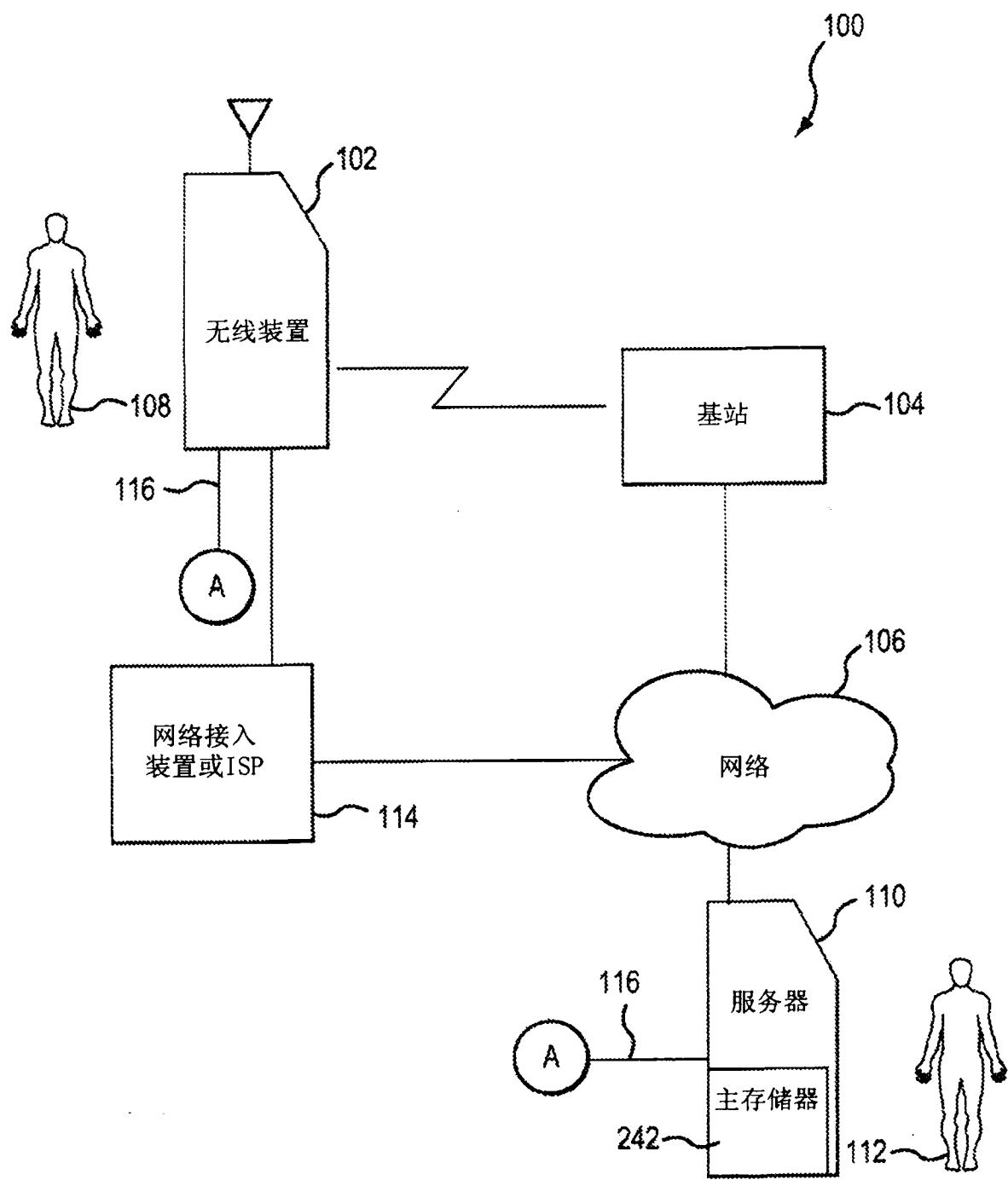


图 1

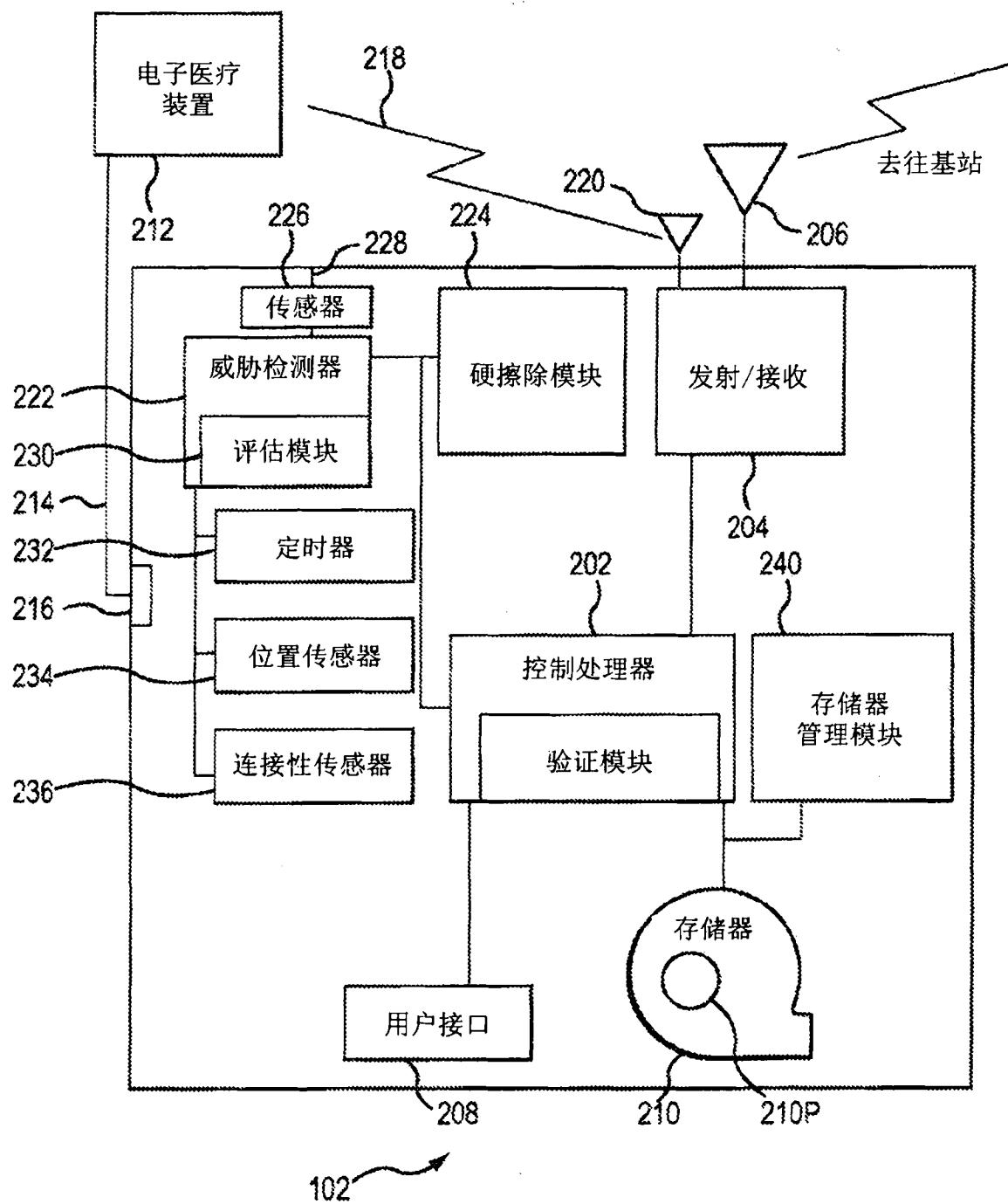


图 2

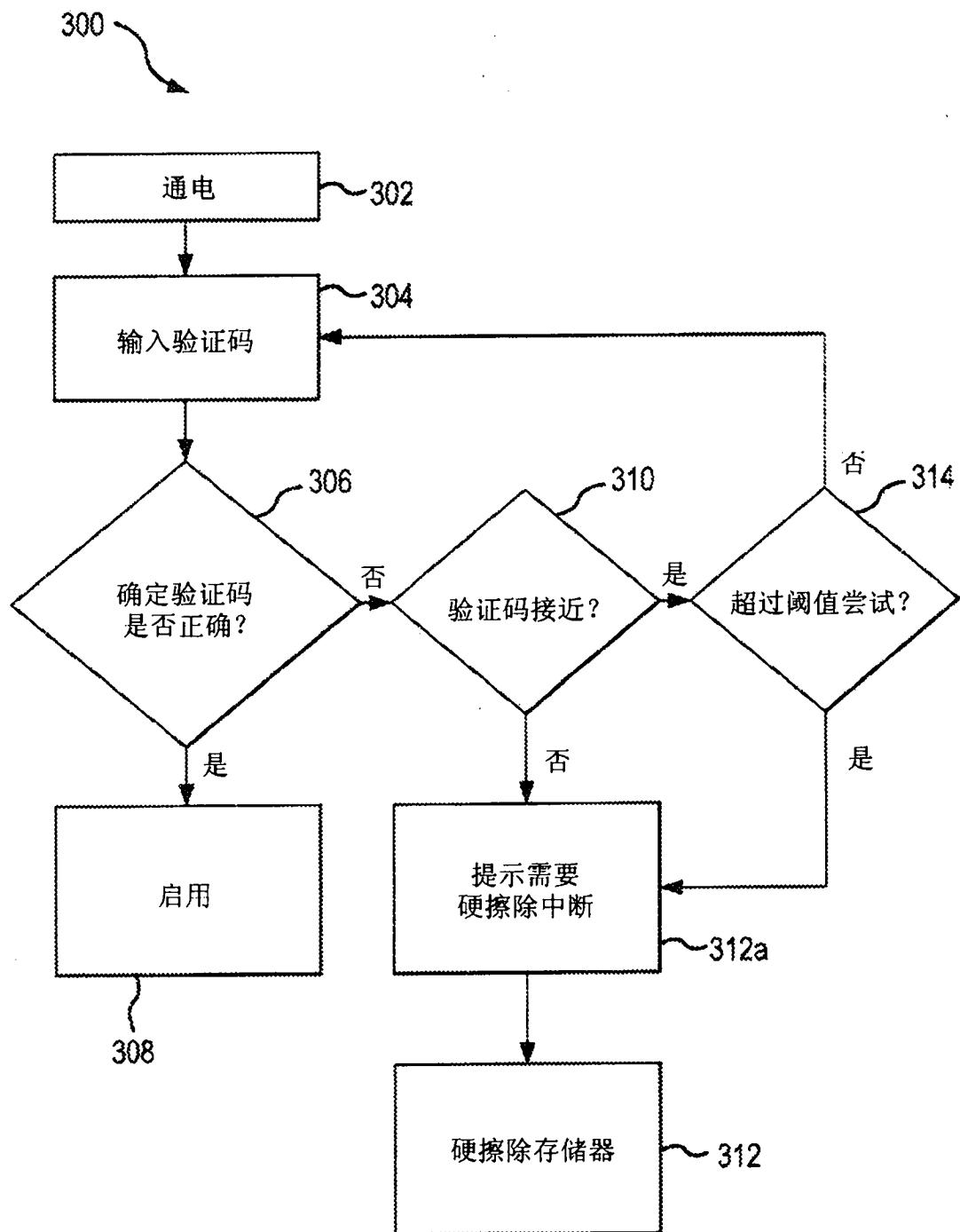


图 3

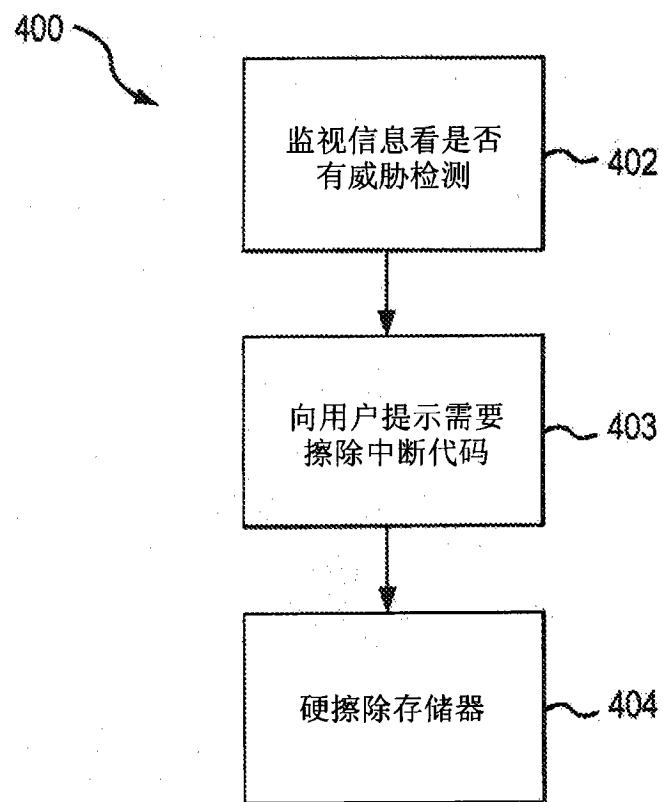


图 4

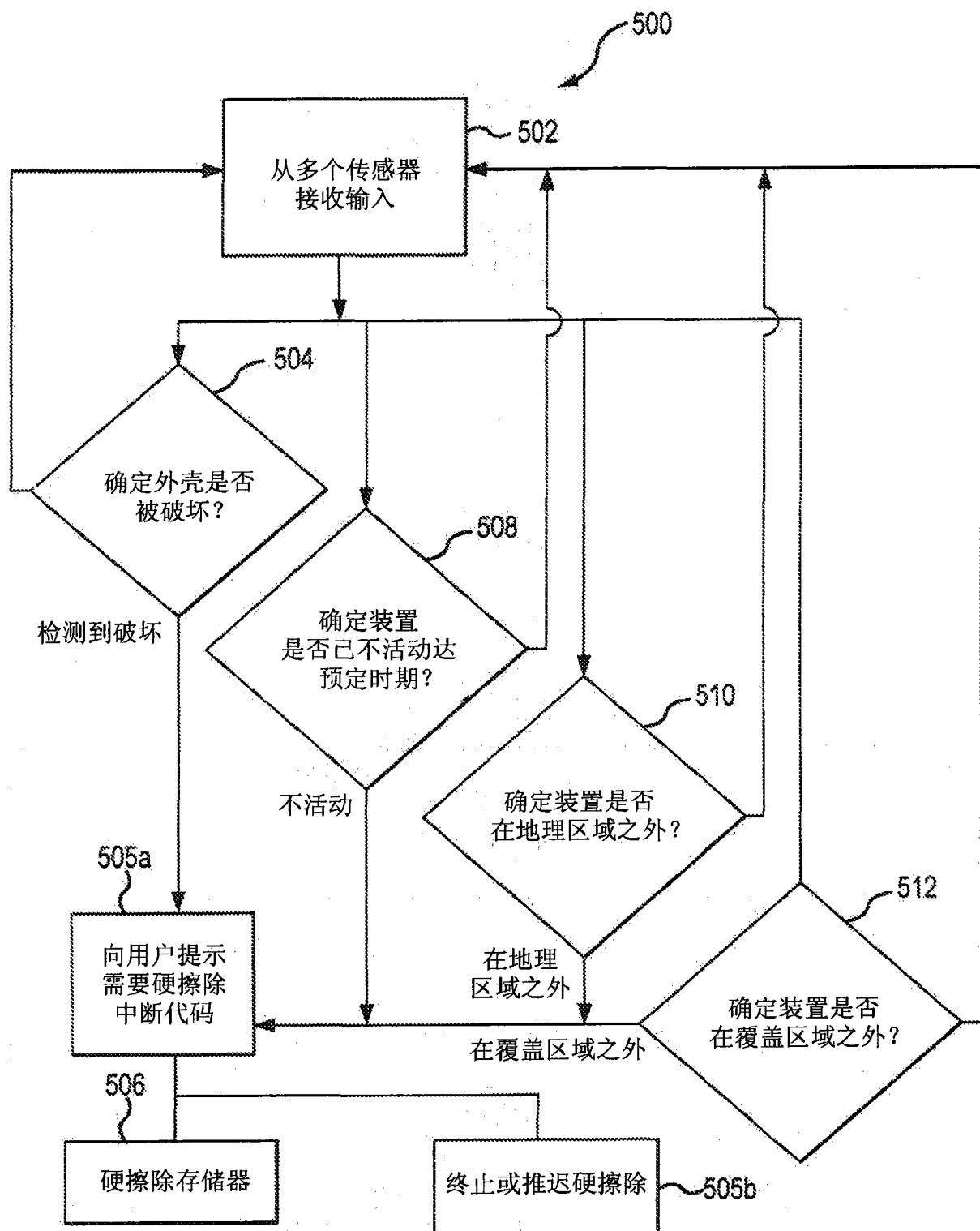


图 5

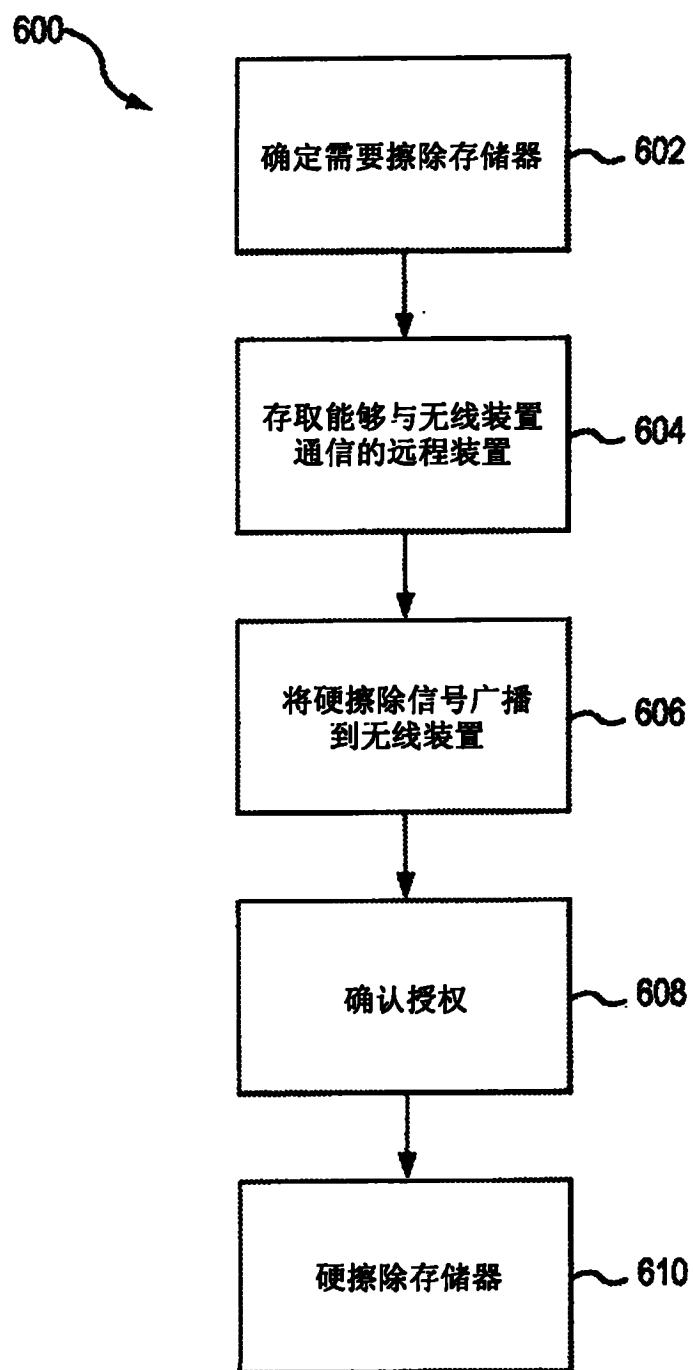


图 6

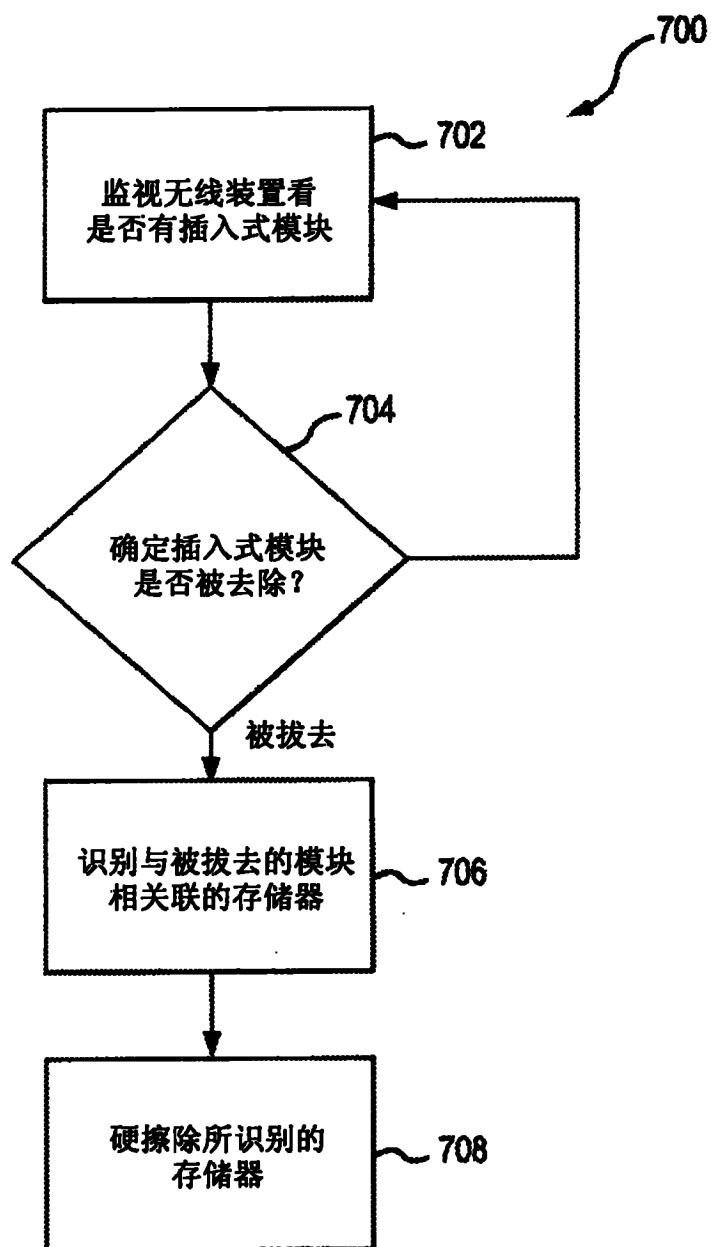


图 7

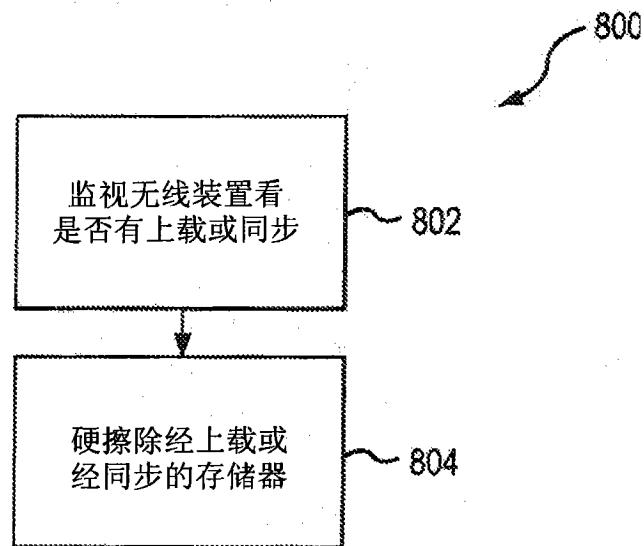


图 8

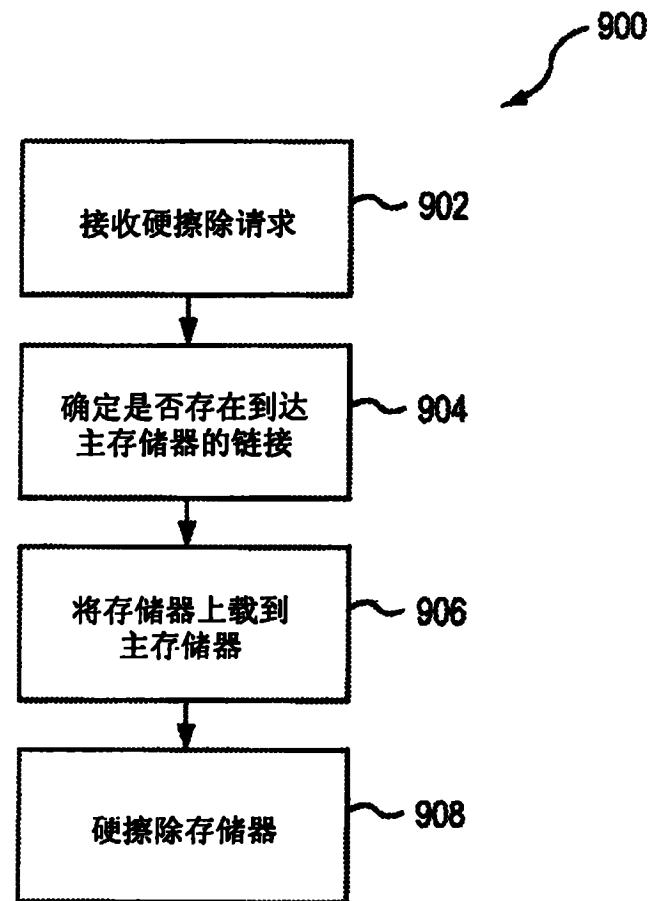


图 9