(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105069344 A
(43)申请公布日 2015.11.18

(21)申请号 201510438507.X

(22)申请日 2015.07.23

(71)申请人 小米科技有限责任公司
地址 100085 北京市海淀区清河中街68号华润五彩城购物中心二期13层

(72)发明人 王舒捷 万钰臻 李明浩

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 祝亚男

(51)Int.Cl.
G06F 21/34(2013.01)

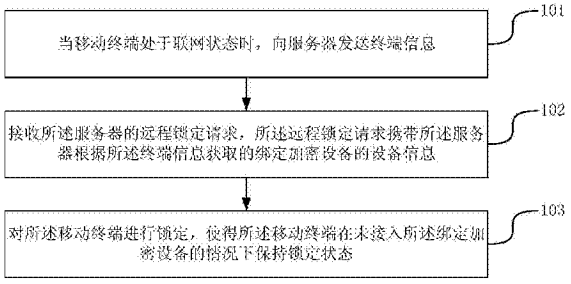
权利要求书3页 说明书9页 附图4页

(54)发明名称

移动终端锁定方法及装置

(57)摘要

本公开提供了一种移动终端锁定方法及装置，属于移动终端技术领域。所述方法包括：当移动终端处于联网状态时，向服务器发送终端信息；接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。本公开通过与移动终端绑定的加密设备，提供了对远程锁定后的移动终端的唯一解锁途径，非合法用户的任何其他用户在没有获取与该移动终端绑定的加密设备的情况下，都无法解锁该移动终端，提高了移动终端的安全性。



CN 105069344 A

1. 一种移动终端锁定方法，其特征在于，所述方法包括：

当移动终端处于联网状态时，向服务器发送终端信息；

接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

2. 根据权利要求 1 所述的方法，其特征在于，当移动终端处于联网状态时，向服务器发送终端信息之前，所述方法还包括：

所述移动终端获取所述绑定加密设备的设备信息；

将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和所述终端信息进行对应存储。

3. 根据权利要求 2 所述的方法，其特征在于，所述移动终端获取所述绑定加密设备的设备信息之前，还包括：

在加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述加密设备，使得所述加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

4. 根据权利要求 1 所述的方法，其特征在于，对所述移动终端进行锁定包括：

在所述锁定状态下，禁止所述移动终端的指定功能。

5. 根据权利要求 1 所述的方法，其特征在于，对所述移动终端进行锁定之后，所述方法还包括：

当所述移动终端有设备接入时，获取接入设备的设备信息；

当确定所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

6. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括：

在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；

当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

7. 根据权利要求 5 所述的方法，其特征在于，所述方法还包括：

在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；

当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

8. 根据权利要求 1 所述的方法，其特征在于，所述绑定加密设备与所述移动终端通过所述移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

9. 根据权利要求 1 所述的方法，其特征在于，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的媒体访问控制 MAC 地址。

10. 根据权利要求 1 所述的方法，其特征在于，所述绑定加密设备的设备信息为硬件序列号。

11. 一种移动终端锁定装置，其特征在于，所述装置包括：

发送模块，用于当移动终端处于联网状态时，向服务器发送终端信息；

接收模块，用于接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

锁定模块，用于对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

12. 根据权利要求 11 所述的装置，其特征在于，所述装置还包括：

获取模块，用于获取所述绑定加密设备的设备信息；

所述发送模块还用于将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和所述终端信息进行对应存储。

13. 根据权利要求 12 所述的装置，其特征在于，所述装置还包括：

写入模块，用于在加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述加密设备，使得所述加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

14. 根据权利要求 11 所述的装置，其特征在于，所述锁定模块用于在所述锁定状态下，禁止所述移动终端的指定功能。

15. 根据权利要求 11 所述的装置，其特征在于，所述装置包括：

所述获取模块还用于当所述移动终端有设备接入时，获取接入设备的设备信息；

确定模块，用于确定当所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

16. 根据权利要求 15 所述的装置，其特征在于，所述获取模块还用于在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；

所述锁定模块还用于当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

17. 根据权利要求 15 所述的装置，其特征在于，所述装置还包括：

显示模块，用于在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；

所述锁定模块还用于当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

18. 根据权利要求 11 所述的装置，其特征在于，所述绑定加密设备与所述移动终端通过所述移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

19. 根据权利要求 11 所述的装置，其特征在于，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的媒体访问控制 MAC 地址。

20. 根据权利要求 11 所述的装置，其特征在于，所述绑定加密设备的设备信息为硬件序列号。

21. 一种移动终端锁定装置，其特征在于，包括：

处理器；

用于存储处理器可执行的指令；

其中，所述处理器被配置为：

当移动终端处于联网状态时，向服务器发送终端信息；

接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

移动终端锁定方法及装置

技术领域

[0001] 本公开涉及移动终端技术领域，尤其涉及一种移动终端锁定方法及装置。

背景技术

[0002] 随着移动通信技术的不断发展，如今的移动终端不仅具有基本的通信功能，还具有存储用户信息、进行社交和金融类活动的功能，其所面临的安全威胁也越来越多，为了保证移动终端的合法用户的个人隐私和财产安全，移动终端提供了安全防护措施，如软件防护方法和硬件防护方法。

[0003] 目前，移动终端的软件防护方法可以是密码保护，也即是，当移动终端处于锁定状态，一旦需要对移动终端进行操作，需要在移动终端所提供的解锁页面上输入密码，从而实现解锁。移动终端的硬件防护方法包括指纹识别等硬件加密技术，指纹识别技术通过获取当前用户的指纹，并将其与预存的指纹进行比对，若比对结果一致，则对移动终端进行解锁，若比对结果不一致，则不响应当前用户对移动终端的操作。

发明内容

[0004] 为克服相关技术中存在的问题，本公开提供一种移动终端锁定方法及装置，所述技术方案如下：

[0005] 根据本公开实施例的第一方面，提供一种移动终端锁定方法，包括：

[0006] 当移动终端处于联网状态时，向服务器发送终端信息；

[0007] 接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

[0008] 对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0009] 在本公开的第一方面的第一种可能实现方式中，当移动终端处于联网状态时，向服务器发送终端信息之前，所述方法还包括：

[0010] 所述移动终端获取所述绑定加密设备的设备信息；

[0011] 将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和终端信息进行对应存储。

[0012] 在本公开的第一方面的第二种可能实现方式中，所述移动终端获取所述绑定加密设备的设备信息之前，还包括：在所述绑定加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述绑定加密设备，使得所述绑定加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

[0013] 在本公开的第一方面的第三种可能实现方式中，对所述移动终端进行锁定包括：在所述锁定状态下，禁止所述移动终端的指定功能。

[0014] 在本公开的第一方面的第四种可能实现方式中，对所述移动终端进行锁定之后，所述方法还包括：

[0015] 当所述移动终端有设备接入时，获取接入设备的设备信息；

[0016] 当确定所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

[0017] 在本公开的第一方面的第五种可能实现方式中，在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

[0018] 在本公开的第一方面的第六种可能实现方式中，在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

[0019] 在本公开的第一方面的第七种可能实现方式中，所述绑定加密设备与所述移动终端通过移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

[0020] 在本公开的第一方面的第八种可能实现方式中，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的物理地址 MAC 地址。

[0021] 在本公开的第一方面的第九种可能实现方式中，所述绑定加密设备的设备信息为硬件序列号。

[0022] 根据本公开实施例的第二方面，提供一种移动终端锁定装置，包括：

[0023] 发送模块，用于当移动终端处于联网状态时，向服务器发送终端信息；

[0024] 接收模块，用于接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

[0025] 锁定模块，用于对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0026] 在本公开的第二方面的第一种可能实现方式中，所述装置还包括：

[0027] 获取模块，用于获取所述绑定加密设备的设备信息；

[0028] 所述发送模块还用于将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和所述终端信息进行对应存储。

[0029] 在本公开的第二方面的第二种可能实现方式中，所属装置还包括：

[0030] 写入模块，用于在加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述加密设备，使得所述加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

[0031] 在本公开的第二方面的第三种可能实现方式中，所述锁定模块用于在所述锁定状态下，禁止所述移动终端的指定功能。

[0032] 在本公开的第二方面的第四种可能实现方式中，所述获取模块还用于当所述移动终端有设备接入时，获取接入设备的设备信息；所述装置还包括确定模块，用于确定当所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

[0033] 在本公开的第二方面的第五种可能实现方式中，所述获取模块还用于在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；所述锁定模块还用于当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

[0034] 在本公开的第二方面的第六种可能实现方式中，所述装置还包括显示模块，用于

在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；所述锁定模块还用于当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

[0035] 在本公开的第二方面的第七种可能实现方式中，所述绑定加密设备与所述移动终端通过所述移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

[0036] 在本公开的第二方面的第八种可能实现方式中，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的媒体访问控制 MAC 地址。

[0037] 在本公开的第二方面的第九种可能实现方式中，所述绑定加密设备的设备信息为硬件序列号。

[0038] 第三方面，还提供了一种移动终端锁定装置，包括：

[0039] 处理器；

[0040] 用于存储处理器可执行的指令的存储器；

[0041] 其中，所述处理器被配置为：

[0042] 当移动终端处于联网状态时，向服务器发送终端信息；

[0043] 接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

[0044] 对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0045] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

[0046] 本公开实施例提供的技术方案带来的有益效果是：

[0047] 通过与移动终端绑定的加密设备，提供了对远程锁定后的移动终端的唯一解锁途径，非合法用户的任何其他用户在没有获取与该移动终端绑定的加密设备的情况下，都无法解锁该移动终端，提高了移动终端的安全性。

附图说明

[0048] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0049] 图 1 是根据一示例性实施例示出的一种移动终端锁定方法的流程图。

[0050] 图 2 是根据一示例性实施例示出的一种移动终端锁定方法的流程图。

[0051] 图 3 是根据一示例性实施例示出的一种移动终端锁定装置的框图。

[0052] 图 4 是根据一示例性实施例示出的一种移动终端锁定装置 400 的框图。

具体实施方式

[0053] 为使本公开的目的、技术方案和优点更加清楚，下面将结合附图对本公开实施方式作进一步地详细描述。

[0054] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附

权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0055] 图 1 是根据一示例性实施例示出的一种移动终端锁定方法的流程图，如图 1 所示，该方法用于移动终端中，包括以下步骤。

[0056] 在步骤 101 中，当移动终端处于联网状态时，向服务器发送终端信息。

[0057] 在步骤 102 中，接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息。

[0058] 在步骤 103 中，对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0059] 在本公开的第一种可能实现方式中，当移动终端处于联网状态时，向服务器发送终端信息之前，所述方法还包括：

[0060] 所述移动终端获取所述绑定加密设备的设备信息；

[0061] 将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和终端信息进行对应存储。

[0062] 在本公开的第二种可能实现方式中，所述移动终端获取所述绑定加密设备的设备信息之前，在加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述加密设备，使得所述绑定加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

[0063] 在本公开的第三种可能实现方式中，对所述移动终端进行锁定包括：在所述锁定状态下，禁止所述移动终端的指定功能。

[0064] 在本公开的第四种可能实现方式中，对所述移动终端进行锁定之后，所述方法还包括：

[0065] 当所述移动终端有设备接入时，获取接入设备的设备信息；

[0066] 当确定所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

[0067] 在本公开的第五种可能实现方式中，在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

[0068] 在本公开的第六种可能实现方式中，在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

[0069] 在本公开的第七种可能实现方式中，所述绑定加密设备与所述移动终端通过移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

[0070] 在本公开的第八种可能实现方式中，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的物理地址 MAC 地址。

[0071] 在本公开的第九种可能实现方式中，所述绑定加密设备的设备信息为硬件序列号。

[0072] 上述所有可选技术方案，可以采用任意结合形成本公开的可选实施例，在此不再一一赘述。

[0073] 图 2 是根据一示例性实施例示出的一种移动终端锁定方法的流程图。参照图 2，该

实施例具体包括：

[0074] 在步骤 201 中，在加密设备首次接入所述移动终端时，将移动终端的终端信息写入该加密设备，使得该加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

[0075] 该加密设备可以为移动存储设备，如 U 盘、移动硬盘等，该移动存储设备可以通过移动终端的通用串行总线 USB 接口或移动终端的耳机孔与该移动终端相连。

[0076] 移动终端的终端信息可以为：移动终端的 IMEI(International Mobile Equipment Identity，移动设备国际身份码）；和 / 或，该移动终端的 MAC(Media Access Control，媒体访问控制）地址。每个移动终端都只有对应的一个固定的 IMEI 和 MAC 地址，使得在发生如移动终端丢失等特殊情况时，即使非法用户拥有同款加密设备，只要不是之前与该丢失移动终端建立绑定关系的加密设备，都无法对该丢失移动终端执行解锁操作。

[0077] 该加密设备变更为只读状态的方式可以有两种：一种是在写入数据后自动变更为只读状态；另一种是手动变更为只读状态，也即是，用户自行选择将该加密设备变更为只读状态，当需要更换与该加密设备绑定的移动终端时，可先格式化该加密设备，清除该加密设备中原先存储的终端信息，以重新写入新的与该加密设备相连的移动终端的终端信息，从而实现加密设备的循环使用。

[0078] 对于第一种自动变更为只读状态的情况，当该加密设备中写入某一个移动终端的终端信息后，就自动封锁该加密设备的写入通道，将该加密设备变更为只读状态，当该加密设备再与其他移动终端相连时，其他移动终端无法再向该加密设备中写入终端信息，从而实现加密设备与移动终端的一对一的不可逆绑定，使得之后只有与该移动终端绑定的加密设备才能对该移动终端执行解锁操作，从而提高移动终端的安全性。

[0079] 对于手动变更为只读状态的情况，以加密设备上设置有不同功能的三个按键为例进行说明，如该三个按键分别为：只读、可读写、格式化。当该加密设备中写入某一个移动终端的终端信息后，用户可以按下加密设备上的只读按键，将该加密设备设置为只读状态，当该加密设备再与其他移动终端相连时，其他移动终端无法再向该加密设备中写入终端信息；当用户更换移动终端时，可以先按下加密设备上的格式化按键，清除之前存储在加密设备中的终端信息，再按下加密设备上的可读写按键，接入新的移动终端，重新写入该新的移动终端的终端信息。这种能够被手动变更状态的加密设备可以实现循环利用，减少资源浪费。当然，加密设备还可以是其他硬件形式，如加密设备上具有硬件开关，通过该硬件开关来控制只读或可读状态的切换，本发明实施例对此不作具体限定。

[0080] 移动终端将终端信息写入与该移动终端相连的加密设备的过程可以包括以下步骤：当该移动终端检测到该加密设备时，该移动终端的屏幕上显示信息写入界面，所述信息写入界面至少包括是否向该加密设备写入该移动终端身份信息的选项，当检测到对该选项的确定操作时，该移动终端将其终端信息写入加密设备中。

[0081] 在步骤 202 中，该移动终端获取该绑定加密设备的设备信息。

[0082] 该绑定加密设备的设备信息可以为该绑定加密设备的硬件序列号。

[0083] 在步骤 203 中，该移动终端将该设备信息与该移动终端的终端信息发送至服务器，使得服务器对该设备信息和该终端信息进行对应存储。

[0084] 该服务器为向该移动终端提供服务的信息服务平台，该信息服务平台可以实现对

移动终端的终端信息和绑定加密设备的设备信息的对应存储。

[0085] 在步骤 204 中，当移动终端处于联网状态时，该移动终端向服务器发送终端信息。

[0086] 移动终端合法用户可以向服务器申请一个用户名，并设置密码，当移动终端遗失时，该合法用户可以使用对应该遗失移动终端的用户名和密码登录服务器，更改该遗失移动终端在服务器上的状态，服务器根据该状态对该遗失移动终端做相应标记。当该遗失移动终端处于联网状态时，该遗失移动终端向服务器发送终端信息，使服务器得知该移动终端已处于联网状态。

[0087] 在步骤 205 中，当服务器接收到终端信息时，如果确定该移动终端已被标记，向该移动终端发送远程锁定请求，该远程锁定请求携带该服务器根据该终端信息获取的绑定加密设备的设备信息。

[0088] 由于移动终端合法用户在服务器上对移动终端进行了标记，服务器一旦接收到该已被标记的移动终端所发送的终端信息时，可以确定当前移动终端已处于联网状态，则自动向移动终端发送远程锁定请求。

[0089] 在步骤 206 中，移动终端接收该服务器的远程锁定请求，该远程锁定请求携带该服务器根据该终端信息获取的绑定加密设备的设备信息。

[0090] 在步骤 207 中，对该移动终端进行锁定，使得该移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0091] 在上述步骤 206 和 207 中，该移动终端接收到远程锁定请求后，内嵌在该移动终端操作系统中的程序锁定该移动终端。

[0092] 该锁定状态可以为完全锁定状态，也可以为部分锁定状态。当移动终端处于完全锁定状态时，不响应对该移动终端执行的任何操作。当移动终端处于部分锁定状态时，禁止移动终端的指定功能，该指定功能可以包括：涉及该移动终端合法用户隐私的功能，以及可能对该合法用户的财产安全造成威胁的功能。上述两种锁定状态可以由移动终端的合法用户在登录服务器后自行选择，也可以先执行部分锁定，再执行完全锁定。

[0093] 在步骤 205 中，该远程锁定请求还可以携带锁定类型标识，该锁定类型标识可以为部分锁定标识，还可以为完全锁定标识，其具体类型可以根据用户在服务器上对锁定类型的指定确定。其中，移动终端在部分锁定状态下，可以建立通话连接。基于此，用户在发现移动终端遗失时，可以通过登录服务器触发携带部分锁定标识的远程锁定请求，以对该遗失移动终端先执行部分锁定操作，然后呼叫该遗失移动终端，若有人接听，可以进行沟通让对方归还该遗失移动终端；若无人接听或对方不愿意归还，则可通过服务器触发携带完全锁定标识的远程锁定请求，以对已经进行了部分锁定的移动终端进行完全锁定操作。

[0094] 在步骤 208 中，当该移动终端有设备接入时，获取接入设备的设备信息。

[0095] 在移动终端有设备接入时，移动终端均会通过与接入设备建立的初步连接，获取该接入设备的设备信息。

[0096] 在步骤 209 中，当确定该接入设备的设备信息和绑定加密设备的设备信息相同时，对该移动终端进行解锁。

[0097] 如果接入设备的设备信息和远程锁定请求所携带的设备信息相同，可以确定该接入设备是合法用户所持有的绑定加密设备，则此时可以对移动终端进行解锁，以保证合法用户能够对移动终端进行操作。

[0098] 为了进一步提高移动终端的安全性，当确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，该移动终端还可以获取所述绑定加密设备中存储的终端信息，将该信息与该移动终端的终端信息进行对比。相同，直接解锁。

[0099] 为了增加移动终端操作的灵活性，还可以增加移动终端的锁定状态解除选项，用于控制是否对锁定状态进行解锁处理。若所述绑定加密设备中存储的终端信息与该移动终端的终端信息相同，则在该移动终端的屏幕上显示锁定状态解除选项，当检测到对该锁定状态解除选项的确认操作时，对该移动终端执行解锁操作，使得该移动终端的各项功能恢复正常。若所述绑定加密设备中存储的终端信息与该移动终端的终端信息不同，则该移动终端无响应。

[0100] 本公开实施例提供的方法，通过与移动终端绑定的加密设备，提供了对远程锁定后的移动终端的唯一解锁途径，非合法用户的任何其他用户在没有获取与该移动终端绑定的加密设备的情况下，都无法解锁该移动终端，提高了移动终端的安全性。

[0101] 图 3 是根据一示例性实施例示出的一种移动终端锁定装置的框图。参照图 3，该装置包括发送模块 301，接收模块 302 和锁定模块 303。

[0102] 发送模块 301，用于当移动终端处于联网状态时，向服务器发送终端信息；

[0103] 接收模块 302，用于接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息；

[0104] 锁定模块 303，用于对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态。

[0105] 在本公开提供的第一种可能实现方式中，所述装置还包括：

[0106] 获取模块，用于获取所述绑定加密设备的设备信息；

[0107] 所述发送模块还用于将所述绑定加密设备的设备信息和所述移动终端的终端信息发送至服务器，使得服务器对所述设备信息和所述终端信息进行对应存储。

[0108] 在本公开提供的第二种可能实现方式中，所述装置还包括：

[0109] 写入模块，用于在加密设备首次接入所述移动终端时，将所述移动终端的终端信息写入所述加密设备，使得所述加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备。

[0110] 在本公开提供的第三种可能实现方式中，所述锁定模块用于在所述锁定状态下，禁止所述移动终端的指定功能。

[0111] 在本公开提供的第四种可能实现方式中，所述装置包括：

[0112] 所述获取模块还用于当所述移动终端有设备接入时，获取接入设备的设备信息；

[0113] 确定模块，用于确定当所述接入设备的设备信息和绑定加密设备的设备信息相同时，对所述移动终端进行解锁。

[0114] 在本公开提供的第五种可能实现方式中，所述获取模块还用于在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，获取所述绑定加密设备中存储的终端信息；

[0115] 所述锁定模块还用于当所述存储的终端信息和所述移动终端的终端信息相同时，执行对所述移动终端进行解锁的步骤。

[0116] 在本公开提供的第六种可能实现方式中，所述装置还包括：

[0117] 显示模块，用于在确定所述接入设备的设备信息和绑定加密设备的设备信息相同后，显示锁定状态解除选项；

[0118] 所述锁定模块还用于当检测到对所述锁定状态解除选项的确认操作时，执行对所述移动终端进行解锁的步骤。

[0119] 在本公开提供的第七种可能实现方式中，所述绑定加密设备与所述移动终端通过所述移动终端的通用串行总线 USB 接口或所述移动终端的耳机孔相连。

[0120] 在本公开提供的第八种可能实现方式中，所述移动终端的终端信息为所述移动终端的移动设备国际身份码 IMEI；和 / 或，所述移动终端的媒体访问控制 MAC 地址。

[0121] 在本公开提供的第九种可能实现方式中，所述绑定加密设备的设备信息为硬件序列号。

[0122] 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0123] 图 4 是根据一示例性实施例示出的一种移动终端锁定装置 400 的框图。例如，装置 400 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

[0124] 参照图 4，装置 400 可以包括以下一个或多个组件：处理组件 402，存储器 404，电源组件 406，多媒体组件 404，音频组件 410，输入 / 输出 (I/O) 的接口 412，传感器组件 414，以及通信组件 416。

[0125] 处理组件 402 通常控制装置 400 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理元件 402 可以包括一个或多个处理器 420 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 402 可以包括一个或多个模块，便于处理组件 402 和其他组件之间的交互。例如，处理部件 402 可以包括多媒体模块，以方便多媒体组件 408 和处理组件 402 之间的交互。

[0126] 存储器 404 被配置为存储各种类型的数据以支持在设备 400 的操作。这些数据的示例包括用于在装置 400 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 404 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器 (SRAM)，电可擦除可编程只读存储器 (EEPROM)，可擦除可编程只读存储器 (EPROM)，可编程只读存储器 (PROM)，只读存储器 (ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0127] 电力组件 406 为装置 400 的各种组件提供电力。电力组件 406 可以包括电源管理系统，一个或多个电源，及其他与为装置 400 生成、管理和分配电力相关联的组件。

[0128] 多媒体组件 408 包括在所述装置 400 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器 (LCD) 和触摸面板 (TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 408 包括一个前置摄像头和 / 或后置摄像头。当设备 400 处于操作模式，如拍摄模式或视频模式时，前置摄像头和 / 或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0129] 音频组件 410 被配置为输出和 / 或输入音频信号。例如，音频组件 410 包括一个麦克风 (MIC)，当装置 400 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 404 或经由通信组件 416 发送。在一些实施例中，音频组件 410 还包括一个扬声器，用于输出音频信号。

[0130] I/O 接口 412 为处理组件 402 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于 :主页按钮、音量按钮、启动按钮和锁定按钮。

[0131] 传感器组件 414 包括一个或多个传感器，用于为装置 400 提供各个方面的状态评估。例如，传感器组件 414 可以检测到设备 400 的打开 / 关闭状态，组件的相对定位，例如所述组件为装置 400 的显示器和小键盘，传感器组件 414 还可以检测装置 400 或装置 400 一个组件的位置改变，用户与装置 400 接触的存在或不存在，装置 400 方位或加速 / 减速和装置 400 的温度变化。传感器组件 414 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 414 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 414 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

[0132] 通信组件 416 被配置为便于装置 400 和其他设备之间有线或无线方式的通信。装置 400 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信部件 416 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信部件 416 还包括近场通信 (NFC) 模块，以促进短程通信。例如，在 NFC 模块可基于射频识别 (RFID) 技术，红外数据协会 (IrDA) 技术，超宽带 (UWB) 技术，蓝牙 (BT) 技术和其他技术来实现。

[0133] 在示例性实施例中，装置 400 可以被一个或多个应用专用集成电路 (ASIC)、数字信号处理器 (DSP)、数字信号处理设备 (DSPD)、可编程逻辑器件 (PLD)、现场可编程门阵列 (FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述移动终端锁定方法。

[0134] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 404，上述指令可由装置 400 的处理器 420 执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器 (RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0135] 在示例性实施例中，还提供了一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行上述移动终端锁定方法。

[0136] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

[0137] 应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

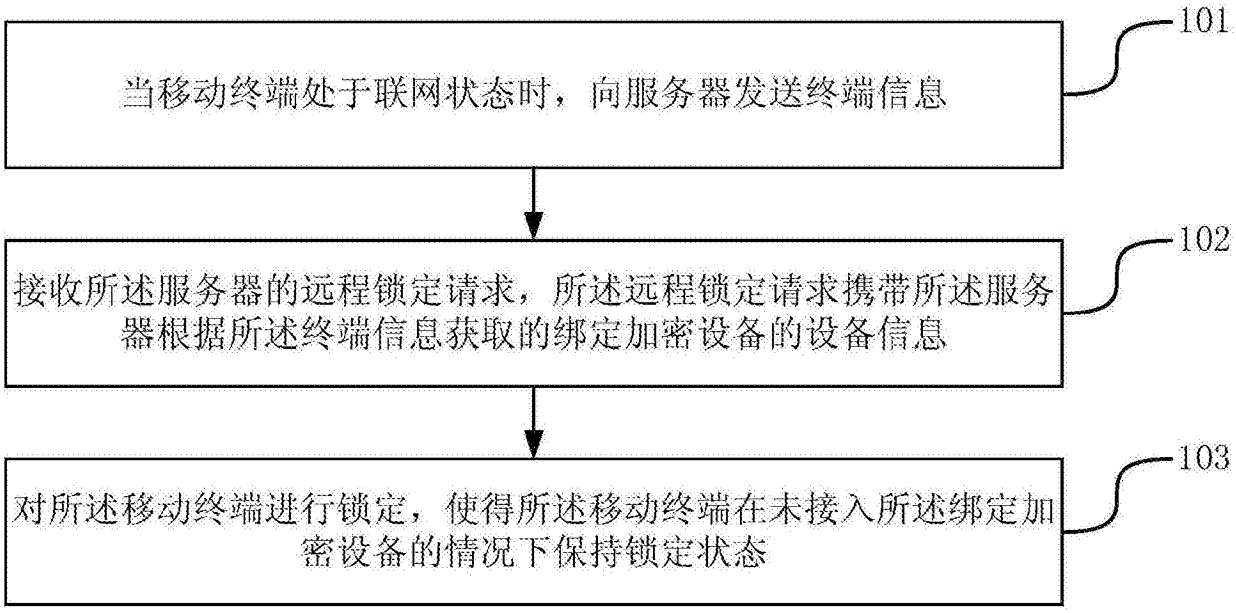

101
当移动终端处于联网状态时，向服务器发送终端信息
102
接收所述服务器的远程锁定请求，所述远程锁定请求携带所述服务器根据所述终端信息获取的绑定加密设备的设备信息
103
对所述移动终端进行锁定，使得所述移动终端在未接入所述绑定加密设备的情况下保持锁定状态

图 1

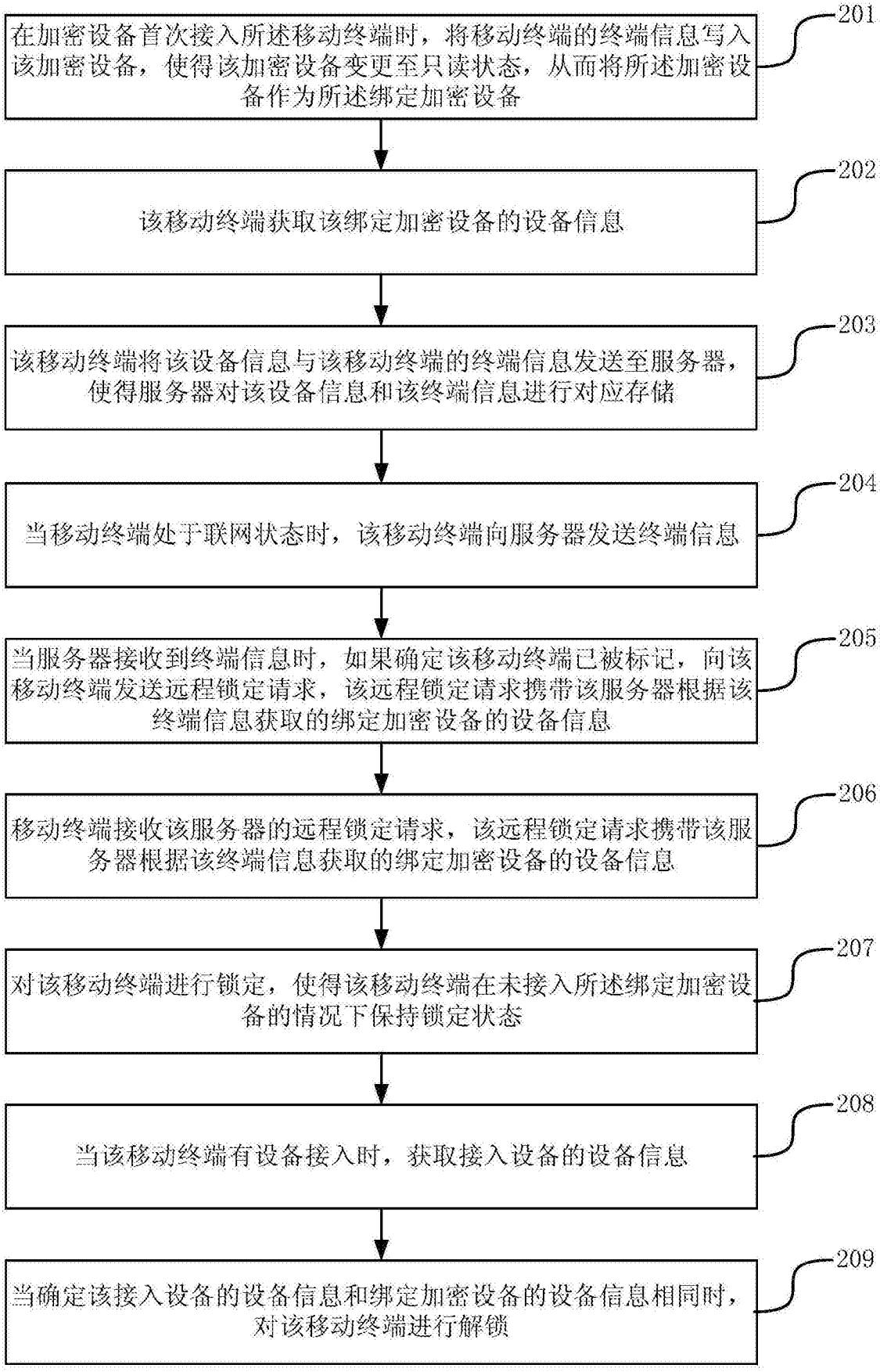

在加密设备首次接入所述移动终端时，将移动终端的终端信息写入该加密设备，使得该加密设备变更至只读状态，从而将所述加密设备作为所述绑定加密设备
201
该移动终端获取该绑定加密设备的设备信息
202
该移动终端将该设备信息与该移动终端的终端信息发送至服务器，使得服务器对该设备信息和该终端信息进行对应存储
203
当移动终端处于联网状态时，该移动终端向服务器发送终端信息
204
当服务器接收到终端信息时，如果确定该移动终端已被标记，向该移动终端发送远程锁定请求，该远程锁定请求携带该服务器根据该终端信息获取的绑定加密设备的设备信息
205
移动终端接收该服务器的远程锁定请求，该远程锁定请求携带该服务器根据该终端信息获取的绑定加密设备的设备信息
206
对该移动终端进行锁定，使得该移动终端在未接入所述绑定加密设备的情况下保持锁定状态
207
当该移动终端有设备接入时，获取接入设备的设备信息
208
当确定该接入设备的设备信息和绑定加密设备的设备信息相同时，对该移动终端进行解锁
209

图 2

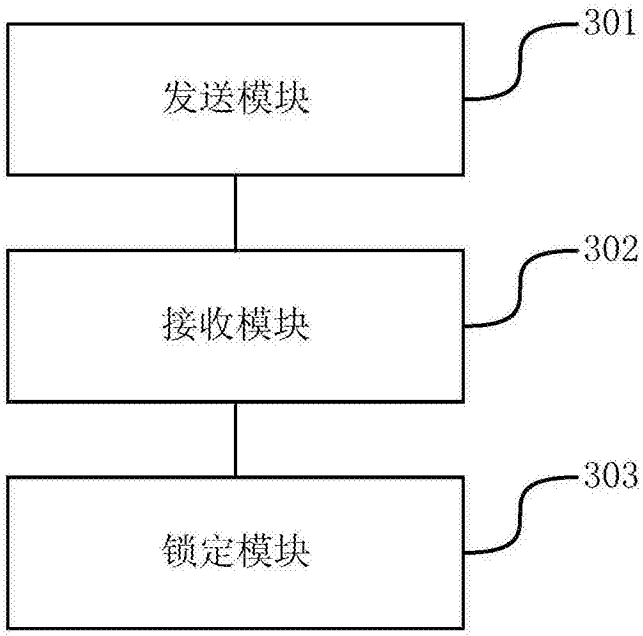


图 3

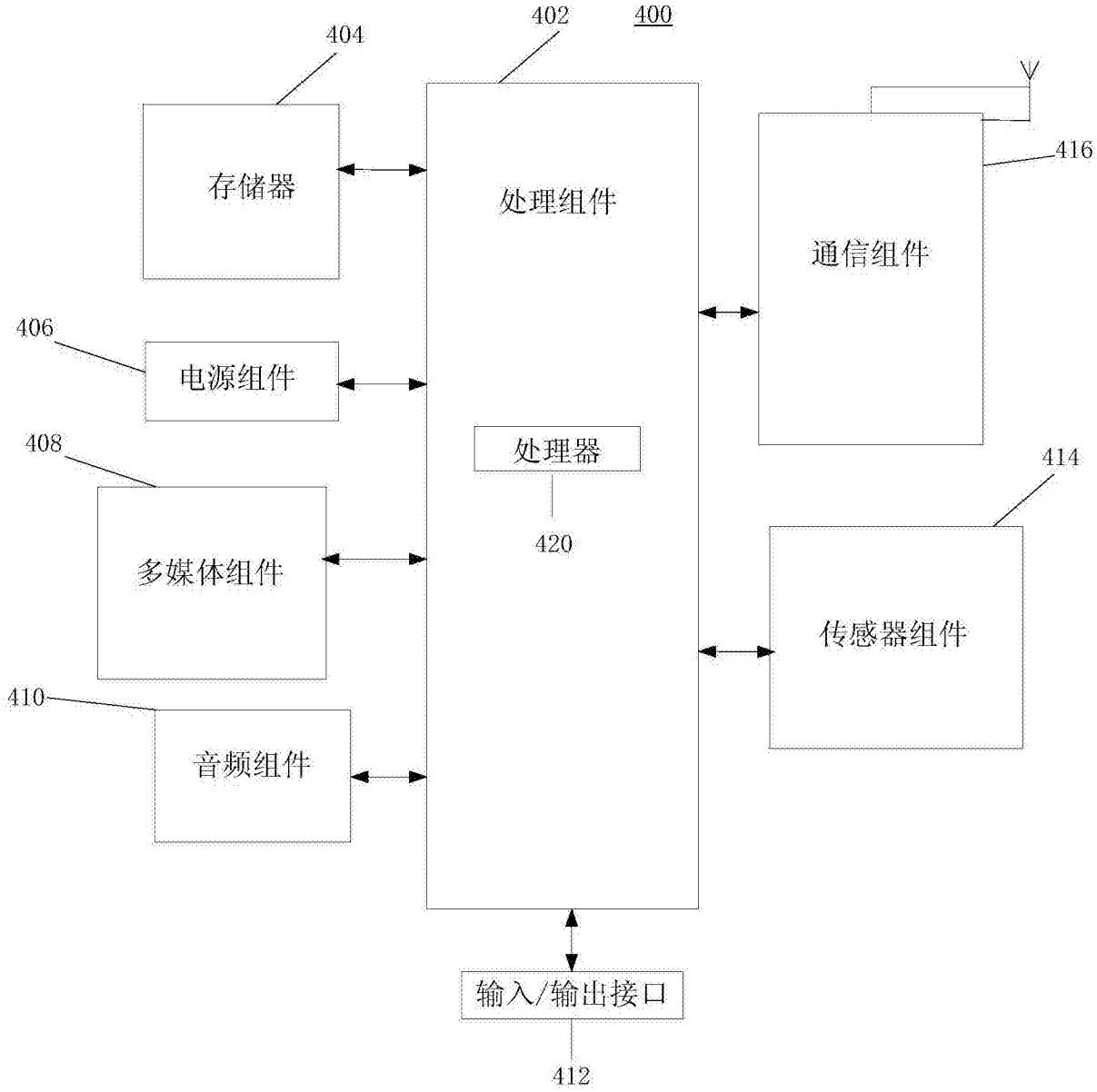

402
400
404
存储器
处理组件
通信组件
416
406
电源组件
处理器
420
408
多媒体组件
414
传感器组件
410
音频组件
输入/输出接口
412

图 4