(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 106295279 B
(45)授权公告日 2019.05.10

(21)申请号 201610657863.5

(22)申请日 2016.08.11

(65)同一申请的已公布的文献号
申请公布号 CN 106295279 A

(43)申请公布日 2017.01.04

(73)专利权人 北京小米移动软件有限公司
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9层01房间

(72)发明人 卢镇洲 陈巧卓 杨飘

(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 林锦澜

(51)Int.Cl.
*G06F 21/31*(2013.01)
*G06F 21/32*(2013.01)
*G06F 21/36*(2013.01)

(56)对比文件
CN 103677551 A,2014.03.26,
CN 104820564 A,2015.08.05,
KR 10-2015-0010258 A,2015.01.28,
CN 104915582 A,2015.09.16,

审查员 王慧敏

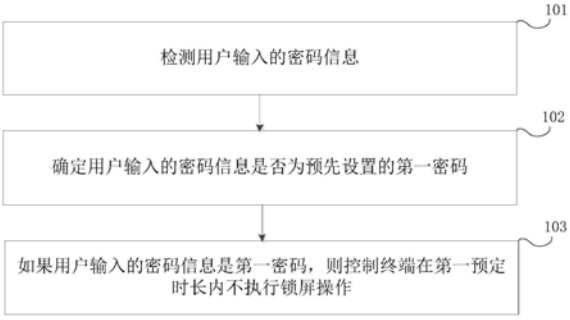
权利要求书2页 说明书10页 附图6页

(54)发明名称

终端控制的方法及装置

(57)摘要

本公开关于一种终端控制的方法及装置，属于计算机技术领域。该方法包括：检测用户输入的密码信息；确定所述密码信息是否为预先设置的第一密码；如果所述密码信息是第一密码，则控制终端在第一预定时长内不执行锁屏操作。通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。




CN 106295279 B

1.一种终端控制方法,其特征在于,所述方法包括:

检测用户输入的密码信息;

确定所述密码信息是否为预先设置的第一密码;

如果所述密码信息是所述第一密码,则控制终端在第一预定时长内不执行锁屏操作;

所述第一密码用于在被第二密码加密的终端检测到用户输入的所述第一密码时,对被所述第二密码加密的终端进行解密操作,所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密,或接收到用户发出的锁屏操作指令时对终端进行加密。

2.根据权利要求1所述的方法,其特征在于,所述控制终端在第一预定时长内不执行锁屏操作包括:

控制终端在无用户操作的第一预定时长内不执行锁屏操作。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

确定终端中是否设置有第二密码。

4.根据权利要求3所述的方法,其特征在于,如果终端中设置有所述第二密码,所述控制终端在第一预定时长内不执行锁屏操作,包括:

控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。

5.根据权利要求3所述的方法,其特征在于,如果终端中设置有所述第二密码,所述方法还包括:

如果所述密码信息不是所述第一密码,则确定所述密码信息是否为所述第二密码;

如果所述密码信息是所述第二密码,用所述第二密码对所述终端进行解密。

6.根据权利要求3所述的方法,其特征在于,如果终端中设置有所述第二密码,所述方法还包括:

控制终端在无用户操作的第一预定时长后,执行锁屏操作并采用所述第二密码对所述终端进行加密。

7.根据权利要求1至6任一项所述的方法,其特征在于,所述检测用户输入的密码信息包括:

在锁屏状态,检测用户输入的密码信息。

8.根据权利要求3所述的方法,其特征在于,所述第一预定时长大于所述第二预定时长。

9.一种终端控制装置,其特征在于,所述装置包括:

信息检测模块,被配置为检测用户输入的密码信息;

第一确定模块,被配置为确定所述密码信息是否为预先设置的第一密码;

控制模块,被配置为如果所述密码信息是所述第一密码,则控制终端在第一预定时长内不执行锁屏操作;

所述第一密码用于在被第二密码加密的终端检测到用户输入的所述第一密码时,对被所述第二密码加密的终端进行解密操作,所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密,或接收到用户发出的锁屏操作指令时对终端进行加密。

10.根据权利要求9所述的装置,其特征在于,所述控制模块,被配置为控制终端在无用

户操作的第一预定时长内不执行锁屏操作。

11.根据权利要求9所述的装置，其特征在于，所述装置还包括：

第二确定模块，被配置为确定终端中是否设置有第二密码。

12.根据权利要求11所述的装置，其特征在于，所述控制模块，被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。

13.根据权利要求11所述的装置，其特征在于，所述装置还包括：

第三确定模块，被配置为如果终端中设置有所述第二密码，如果所述密码信息不是所述第一密码，则确定所述密码信息是否为所述第二密码；

解密模块，被配置为如果所述密码信息是所述第二密码，用所述第二密码对所述终端进行解密。

14.根据权利要求11所述的装置，其特征在于，所述装置还包括：

加密模块，被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密。

15.根据权利要求9至14任一项所述的装置，其特征在于，所述信息检测模块，被配置为在锁屏状态，检测用户输入的密码信息。

16.根据权利要求11所述的装置，其特征在于，所述第一预定时长大于所述第二预定时长。

17.一种终端控制装置，其特征在于，所述装置包括：

处理器；

用于存储所述处理器的可执行指令的存储器；

其中，所述处理器被配置为：

检测用户输入的密码信息；

确定所述密码信息是否为预先设置的第一密码；

如果所述密码信息是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作；

所述第一密码用于在被第二密码加密的终端检测到用户输入的所述第一密码时，对被所述第二密码加密的终端进行解密操作，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行加密。

# 终端控制的方法及装置

## 技术领域

[0001] 本公开涉及计算机技术领域，特别涉及一种终端控制的方法及装置。

## 背景技术

[0002] 随着终端技术的快速发展，终端中应用程序的种类越来越繁多，功能也越来越丰富。用户的终端中安装应用程序的数量在不断的增长，用户每天都会使用手机进行信息的搜索与浏览，甚至于使用手机进行信息的编辑及存储，如便签、图库等。为了保证手机上内容的安全，现在的方式是对手机进行加密。

[0003] 现有的手机加密方式大多是：当手机中无用户操作一段时间后就执行加密并锁屏的操作。这样导致的一个问题就是：用户只是在浏览一个内容，虽然在这段时间内没有执行任何操作，但用户确实是在使用手机的，但是按照现在的手机保护模式，依然在这种情况下对手机进行加密锁屏，用户就不得不输入密码进行解锁，造成了不必要的操作。

## 发明内容

[0004] 本公开实施例提供了一种终端控制方法及装置。所述技术方案如下：

[0005] 根据本公开实施例的第一方面，提供了一种终端控制方法，所述方法包括：

[0006] 检测用户输入的密码信息；

[0007] 确定所述密码信息是否为预先设置的第一密码；

[0008] 如果所述密码信息是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作。

[0009] 可选的，所述控制终端在第一预定时长内不执行锁屏操作包括：

[0010] 控制终端在无用户操作的第一预定时长内不执行锁屏操作。

[0011] 本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0012] 可选的，所述方法还包括：

[0013] 确定终端中是否设置有第二密码，其中，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行加密。

[0014] 可选的，如果终端中设置有所述第二密码，所述控制终端在第一预定时长内不执行锁屏操作，包括：

[0015] 控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。

[0016] 可选的，如果终端中设置有所述第二密码，所述方法还包括：

[0017] 如果所述密码信息不是所述第一密码，则确定所述密码信息是否为所述第二密码；

[0018] 如果所述密码信息是所述第二密码，用所述第二密码对所述终端进行解密。

[0019] 可选的，如果终端中设置有所述第二密码，所述方法还包括：

[0020] 控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密。

[0021] 可选的，所述检测用户输入的密码信息包括：

[0022] 在锁屏状态，检测用户输入的密码信息。

[0023] 可选的，所述第一预定时长大于所述第二预定时长。

[0024] 本公开实施例可以通过第一密码的设置，来控制终端在无用户操作的第一预定时长内不执行锁屏及被第二密码加密的操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现加密锁屏，需反复输入密码来解密终端才能查看信息的情况出现。

[0025] 根据本公开实施例的第二方面，提供了一种终端控制装置，所述装置包括：

[0026] 信息检测模块，被配置为检测用户输入的密码信息；

[0027] 第一确定模块，被配置为确定所述密码信息是否为预先设置的第一密码；

[0028] 控制模块，被配置为如果所述密码信息是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作。

[0029] 可选的，所述控制模块被配置为控制终端在无用户操作的第一预定时长内不执行锁屏操作。

[0030] 本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0031] 可选的，所述装置还包括：

[0032] 第二确定模块，被配置为确定终端中是否设置有第二密码，其中，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行加密。

[0033] 可选的，所述控制模块，被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。

[0034] 可选的，所述装置还包括：

[0035] 第三确定模块，被配置为如果终端中设置有所述第二密码，如果所述密码信息不是所述第一密码，则确定所述密码信息是否为所述第二密码；

[0036] 解密模块，被配置为如果所述密码信息是所述第二密码，用所述第二密码对所述终端进行解密。

[0037] 可选的，所述装置还包括：

[0038] 加密模块，被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密。

[0039] 可选的，所述信息检测模块，被配置为在锁屏状态，检测用户输入的密码信息。

[0040] 可选的，所述第一预定时长大于所述第二预定时长。

[0041] 本公开实施例可以通过第一密码的设置，来控制终端在无用户操作的第一预定时

长内不执行锁屏及被第二密码加密的操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现加密锁屏，需反复输入密码来解密终端才能查看信息的情况出现。

[0042] 根据本公开实施例的第三方面，提供一种终端控制装置，所述装置包括：

[0043] 处理器；

[0044] 用于存储所述处理器的可执行指令的存储器；

[0045] 其中，所述处理器被配置为：

[0046] 检测用户输入的密码信息；

[0047] 确定所述密码信息是否为预先设置的第一密码；

[0048] 如果所述密码信息是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作。

[0049] 本公开实施例提供的技术方案可以包括以下有益效果：

[0050] 本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0051] 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。

## 附图说明

[0052] 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。

[0053] 图1是根据一示例性实施例示出的一种终端控制方法的流程图；

[0054] 图2是根据另一示例性实施例示出的一种终端控制方法的流程图；

[0055] 图3是根据另一示例性实施例示出的一种终端控制方法的流程图；

[0056] 图4是根据一示例性实施例示出的一种终端控制装置的框图；

[0057] 图5是根据另一示例性实施例示出的一种终端控制装置的框图；

[0058] 图6是根据另一示例性实施例示出的一种终端控制装置的框图；

[0059] 图7是根据另一示例性实施例示出的一种终端控制装置的框图；

[0060] 图8是根据另一示例性实施例示出的一种终端控制装置的框图。

[0061] 通过上述附图，已示出本公开明确的实施例，后文中将有更详细的描述。这些附图和文字描述并不是为了通过任何方式限制本公开构思的范围，而是通过参考特定实施例为本领域技术人员说明本公开的概念。

## 具体实施方式

[0062] 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。

[0063] 在本公开使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本公开。在本公开和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0064] 应当理解，尽管在本公开可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本公开范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0065] 本公开实施例提供的技术方案应用于终端，该终端可以是各种能够通过触摸屏进行触摸操作的智能终端，例如，智能手机、平板电脑、个人数字助理(Personal Digital Assistant，PDA)等，但不限于此。本领域的技术人员容易理解，本发明实施例还可应用于任何具有处理器和显示输出装置的移动终端中。另外，本公开实施例提供的技术方案还适用于具有指纹识别模块、声纹识别模块或/和人脸识别模块等生物识别模块的终端中。

[0066] 本公开实施例提供了一种在上述终端上应用的终端控制方法，可以为：检测用户输入的密码信息，并确定用户输入的密码信息是否为预先设置的第一密码，如果用户输入的密码是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作。本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏的情况，需反复的解锁终端才能查看信息的情况出现。

[0067] 参见图1，图1是根据一示例性实施例示出的一种终端控制的方法，该方法可用于上述移动终端中，包括以下步骤：

[0068] 在步骤101中，检测用户输入的密码信息；

[0069] 本公开实施例中，在终端屏幕被点亮，处于锁屏的状态下，检测用户输入的密码信息。这里，用户输入的密码信息可以是数字信息、指纹、头像或者声音等生物识别特征信息或者是手势信息，本公开实施例对该密码信息的类型不做特定的限制。

[0070] 在步骤102中，确定用户输入的密码信息是否为预先设置的第一密码；

[0071] 本公开实施例中，用户可以通过终端的功能设置项来预先设置第一密码并保存。这里，第一密码被设置对应的功能是：对终端进行解密操作并控制终端在第一预定时长内不会被锁屏。这里，可以将用户输入的密码信息与预先存储的第一密码信息进行对比，以确定用户输入的密码信息是否为预先设置的第一密码。

[0072] 本公开实施例中，第一密码被设置对应的功能：对终端进行解密操作，指：即使终端被设置的其他密码(如预先设置的第二密码)进行加密，在检测到用户输入的第一密码时，依然可以对被第二密码加密的终端进行解密操作。

[0073] 在步骤103中，如果用户输入的密码信息是第一密码，则控制终端在第一预定时长内不执行锁屏操作。

[0074] 本公开实施例中，第一预定时长可以由用户根据需求预先设定。

[0075] 在本公开实施例中，如果用户输入的密码信息是第一密码，控制终端在无用户操作的第一预定时长内不执行锁屏操作。

[0076] 本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0077] 本公开实施例中，该终端控制的方法还可以包括：

[0078] 确定终端中是否设置有第二密码，其中，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行加密并锁屏。

[0079] 这里，用户可以通过终端的功能设置项来设置上述第二密码并保存。确定终端中是否设置有第二密码就可以通过功能设置项来查询得知用户是否设置有第二密码。

[0080] 其中，第二预定时长可以由用户根据个人的需要而预先设置并保存使用。

[0081] 本公开实施例中，一般情况下，第一预定时长被设置为长于第二预定时长。如第一预定时长为10分钟，第二预定时长为1分钟，本公开实施例对此并不做过多限定。

[0082] 本公开实施例中，如果终端中设置有所述第二密码，那么，控制终端在第一预定时长内不执行锁屏操作，就可以包括：

[0083] 控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。这样，就可以通过第一密码的设置，来控制终端在无用户操作的第一预定时长内不执行锁屏及被第二密码加密的操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现加密锁屏，需反复输入密码来解密终端才能查看信息的情况出现。

[0084] 在本公开实施例中，如果终端中设置有所述第二密码，该终端控制的方法还可以包括以下操作：

[0085] 如果所述密码信息不是所述第一密码，则确定所述密码信息是否为所述第二密码；

[0086] 如果所述密码信息是所述第二密码，用所述第二密码对所述终端进行解密。

[0087] 在本公开实施例中，如果终端中设置有所述第二密码，该终端控制的方法还可以包括以下操作：

[0088] 控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密。

[0089] 综上所述，本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0090] 参见图2，图2是根据一示例性实施例示出的一种终端控制的方法，该方法用于终端，可以包括以下步骤：

[0091] 在步骤201中，预操作，记录用户设置的第二密码；

[0092] 这里，用户可以通过终端的功能设置项来设置第二密码，并终端记录存储该第二密码。

[0093] 其中，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终

端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行锁屏并加密。

[0094] 这样，在用户设置了第二密码且开启了密码保护的情况下，如果检测到终端在第二预定时长内无用户操作，则终端会执行锁屏并使用第二密码进行加密的操作。或者，在接收到用户发送的锁屏指令时，执行锁屏操作并使用第二密码进行加密的操作。

[0095] 其中，第二预定时长可以由用户根据个人的需要而预先设置并保存使用。

[0096] 在步骤202中，在终端为锁屏的状态下，检测用户输入的密码信息；

[0097] 本公开实施例中，在终端屏幕被点亮，处于锁屏的状态下，检测用户输入的密码信息。这里，用户输入的密码信息可以是数字信息、指纹、头像或者声音等生物识别特征信息或者是手势信息，本公开实施例对该密码信息的类型不做特定的限制。

[0098] 在步骤203中，确定用户输入的密码信息是否为预先设置的第一密码；

[0099] 本公开实施例中，用户可以通过终端的功能设置项来预先设置第一密码并保存。其中，第一密码被设置对应的功能是：对终端进行解密操作并控制终端在第一预定时长内不会被锁屏。这里，可以将用户输入的密码信息与预先存储的第一密码信息进行对比，以确定用户输入的密码信息是否为预先设置的第一密码。

[0100] 本公开实施例中，第一密码被设置对应的功能：对终端进行解密操作，指：即使终端被设置的其他密码(如预先设置的第二密码)进行加密，在检测到用户输入的第一密码时，依然可以对被第二密码加密的终端进行解密操作。

[0101] 本公开实施例中，第一预定时长可以由用户根据个人的需要而预先设置并保存使用，一般情况下，第一预定时长被设置为长于第二预定时长。如第一预定时长为10分钟，第二预定时长为1分钟，本公开实施例对此并不做过多限定。

[0102] 当确定用户输入的密码信息为预先设置的第一密码时，执行步骤204；

[0103] 当确定用户输入的密码信息不是预先设置的第一密码时，执行步骤207；

[0104] 在步骤204中，控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作；

[0105] 在步骤205中，检测是否达到第一预定时长；

[0106] 如果达到第一预定时长，则执行步骤206；

[0107] 如果未达到第一预定时长，则继续执行步骤204；

[0108] 在步骤206中，控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密

[0109] 在步骤207中，确定用户输入的密码信息是否为第二密码；

[0110] 这里，对用户输入的密码信息进行识别，并将识别出的用户输入的密码信息与预先存储的第二密码信息进行对比，以确定用户输入的密码信息是否为预先设置的第二密码。当用户输入的密码信息为第二密码时，执行步骤208；当用户输入的密码信息不是第二密码时，执行步骤209。

[0111] 在步骤208中，用用户输入的第二密码对所述终端进行解密。

[0112] 在步骤209中，提示用户输入的密码有误，并返回执行步骤202。

[0113] 本公开实施例所公开的技术方案，可以通过第一密码的设置，来控制终端在无用户操作的第一预定时长内不执行锁屏及被第二密码加密的操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现加密锁

屏，需反复输入密码来解密终端才能查看信息的情况出现。

[0114] 参见图3，图3是根据一示例性实施例示出的一种终端控制的方法，该方法用于终端，可以包括以下步骤：

[0115] 在步骤301中，预操作，记录用户设置的终端锁屏时间；

[0116] 这里，用户可以通过终端的功能设置项来设置终端的锁屏时间，如第三预定时长。

[0117] 其中，设置的终端锁屏时间被配置为的功能是：当检测到终端在第三预定时长内无用户操作，则执行锁屏操作。

[0118] 这样，在用户设置了终端锁屏时间的情况下，如果检测到终端在第三预定时长内无用户操作，则会执行锁屏操作。

[0119] 在步骤302中，在终端为锁屏的状态下，检测用户输入的密码信息；

[0120] 本公开实施例中，在终端屏幕被点亮，处于锁屏的状态下，检测用户输入的密码信息。这里，用户输入的密码信息可以是数字信息、指纹、头像或者声音等生物识别特征信息或者是手势信息，本公开实施例对该密码信息的类型不做特定的限制。

[0121] 在步骤303中，确定用户输入的密码信息是否为预先设置的第一密码；

[0122] 本公开实施例中，用户可以通过终端的功能设置项来预先设置第一密码并保存。其中，第一密码被设置对应的功能是：对终端进行解密操作并控制终端在第一预定时长内不会被锁屏；或者，控制终端在第一预定时长内不会被锁屏。这里，可以将用户输入的密码信息与预先存储的第一密码信息进行对比，以确定用户输入的密码信息是否为预先设置的第一密码。

[0123] 本公开实施例中，第一密码被设置对应的功能：对终端进行解密操作，指：即使终端被设置的其他密码(如预先设置的第二密码)进行加密，在检测到用户输入的第一密码时，依然可以对被第二密码加密的终端进行解密操作。

[0124] 本公开实施例中，第一预定时长可以由用户根据个人的需要而预先设置并保存使用，一般情况下，第一预定时长被设置为长于第三预定时长。如第一预定时长为8分钟，第三预定时长为2分钟，本公开实施例对此并不做过多限定。

[0125] 当确定用户输入的密码信息为预先设置的第一密码时，执行步骤304；

[0126] 当确定用户输入的密码信息不是预先设置的第一密码时，执行步骤307；

[0127] 在步骤304中，控制终端在无用户操作的第一预定时长内不执行锁屏操作；

[0128] 在步骤305中，检测是否达到第一预定时长；

[0129] 当达到第一预定时长时，执行步骤306；

[0130] 当未达到第一预定时长时，继续执行步骤304。

[0131] 在步骤306中，控制终端执行锁屏操作。

[0132] 在步骤307中，提示用户输入的密码有误，并返回执行步骤302。

[0133] 本公开实施例所公开的技术方案，可以通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0134] 下述为本公开装置实施例，可以用于执行本公开方法实施例。对于本公开装置实施例中未披露的细节，请参照本公开方法实施例。

[0135] 图4是根据一示例性实施例示出的一种终端控制装置400的框图，该终端控制装置400可以通过软件、硬件或者两者的结合实现成为终端的部分或者全部，该终端可以是手机或者平板电脑等电子显示设备。该终端控制装置400可以包括：

[0136] 信息检测模块401，可以被配置为检测用户输入的密码信息；

[0137] 第一确定模块402，可以被配置为确定所述密码信息是否为预先设置的第一密码；

[0138] 控制模块403，可以被配置为如果所述密码信息是所述第一密码，则控制终端在第一预定时长内不执行锁屏操作。

[0139] 在一个实施例中，控制模块403，可以被具体配置为控制终端在无用户操作的第一预定时长内不执行锁屏操作。

[0140] 本公开实施例通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0141] 参见图5，如图4所示的终端控制装置400还可以包括：

[0142] 第二确定模块404，可以被配置为确定终端中是否设置有第二密码，其中，所述第二密码用于在检测到终端在第二预定时长内无用户操作时对所述终端进行锁屏并加密，或接收到用户发出的锁屏操作指令时对终端进行加密。

[0143] 在一个实施例中，控制模块403，可以被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作。

[0144] 参见图6，如图5所示的终端控制装置400还可以包括：

[0145] 第三确定模块405，被配置为如果终端中设置有所述第二密码，如果所述密码信息不是所述第一密码，则确定所述密码信息是否为所述第二密码；

[0146] 解密模块406，可以被配置为如果所述密码信息是所述第二密码，用所述第二密码对所述终端进行解密。

[0147] 参见图7，如图4所示的终端控制装置400还可以包括：

[0148] 加密模块407，可以被配置为如果终端中设置有所述第二密码，控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密。

[0149] 在一个实施例中，信息检测模块401，可以被配置为在锁屏状态，检测用户输入的密码信息。

[0150] 本公开实施例中，所述第一预定时长大于所述第二预定时长。

[0151] 本公开实施例所公开的技术方案，可以通过第一密码的设置，来控制终端在无用户操作的第一预定时长内不执行锁屏及被第二密码加密的操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现加密锁屏，需反复输入密码来解密终端才能查看信息的情况出现。

[0152] 综上所述，本公开实施例所公开的技术方案，可以通过预先设置的第一密码，可以控制终端在无用户操作的第一预定时长内不执行锁屏操作，方便用户在第一预定时长内查看终端中的某些内容，而避免因为可能在第一预定时长内因用户无操作而出现锁屏，需反复解锁终端才能查看信息的情况出现。

[0153] 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。

[0154] 请参考图8，其示出了一示例性实施例示出的一种用于终端控制装置500的框图。例如，装置500可以是手机或者平板电脑等电子显示设备。

[0155] 参照图8，装置500可以包括以下一个或多个组件：处理组件502，存储器504，电源组件506，多媒体组件508，音频组件510，输入/输出(I/O)接口512，传感器组件514，以及通信组件516。

[0156] 处理组件502通常控制装置500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。处理组件502可以包括一个或多个处理器320来执行指令，以完成上述终端控制方法的全部或部分步骤。此外，处理组件502可以包括一个或多个模块，便于处理组件502和其他组件之间的交互。例如，处理组件502可以包括多媒体模块，以方便多媒体组件508和处理组件502之间的交互。

[0157] 存储器504被配置为存储各种类型的数据以支持在装置500上的操作。这些数据的示例包括用于在装置500上操作的任何应用或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器504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。

[0158] 电源组件506为装置500的各种组件提供电力。电源组件506可以包括电源管理系统，一个或多个电源，及其他与为装置500生成、管理和分配电力相关联的组件。

[0159] 多媒体组件508包括在装置500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。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508包括一个前置摄像头和/或后置摄像头。当装置500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。

[0160] 音频组件510被配置为输出和/或输入音频信号。例如，音频组件510包括一个麦克风(MIC)，当装置500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504或经由通信组件516发送。在一些实施例中，音频组件510还包括一个扬声器，用于输出音频信号。

[0161] I/O接口512为处理组件502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。

[0162] 传感器组件514包括一个或多个传感器，用于为装置500提供各个方面的状态评估。例如，传感器组件514可以检测到装置500的打开/关闭状态，组件的相对定位，例如组件为装置500的显示器和小键盘，传感器组件514还可以检测装置500或装置500一个组件的位置改变，用户与装置500接触的存在或不存在，装置500方位或加速/减速和装置500的温度变化。传感器组件514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514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514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。

[0163] 通信组件516被配置为便于装置500和其他设备之间有线或无线方式的通信。装置500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，通信组件516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，通信组件516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。

[0164] 在示例性实施例中，装置500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，用于执行上述显示界面切换的方法。

[0165] 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504，上述指令可由装置500的处理器420执行以完成上述终端控制方法。例如，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。

[0166] 一种非临时性计算机可读存储介质，当存储介质中的指令由装置500的处理器执行时，使得装置500能够执行上述终端控制方法。

[0167] 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。

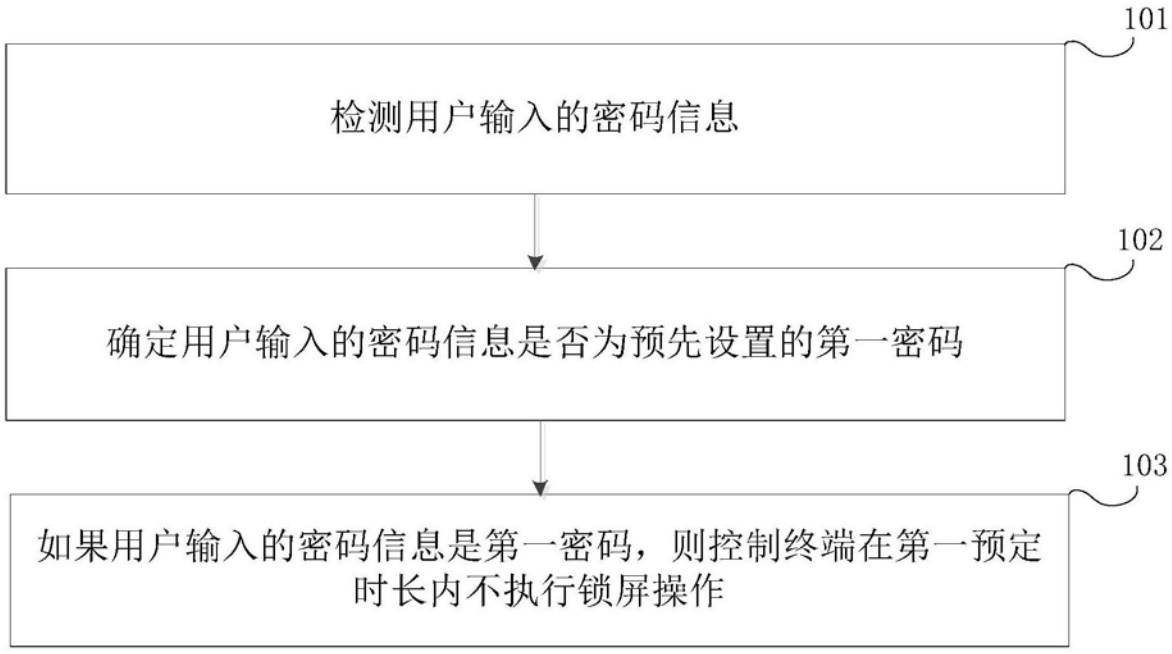

101
检测用户输入的密码信息
102
确定用户输入的密码信息是否为预先设置的第一密码
103
如果用户输入的密码信息是第一密码，则控制终端在第一预定时长内不执行锁屏操作

图1

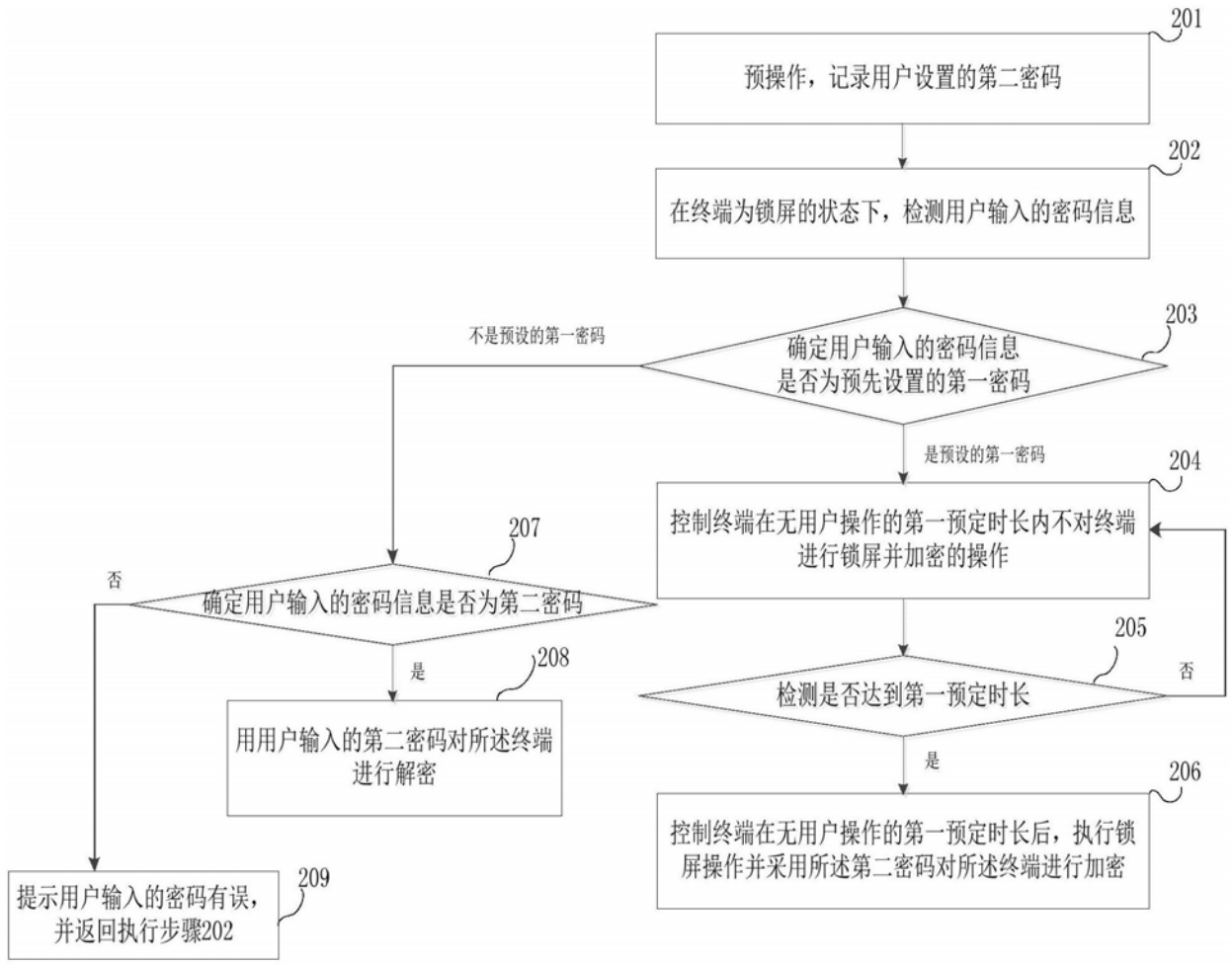

201
预操作，记录用户设置的第二密码
202
在终端为锁屏的状态下，检测用户输入的密码信息
203
确定用户输入的密码信息是否为预先设置的第一密码
不是预设的第一密码
是预设的第一密码
204
控制终端在无用户操作的第一预定时长内不对终端进行锁屏并加密的操作
205
检测是否达到第一预定时长
否
是
206
控制终端在无用户操作的第一预定时长后，执行锁屏操作并采用所述第二密码对所述终端进行加密
207
确定用户输入的密码信息是否为第二密码
否
是
208
用用户输入的第二密码对所述终端进行解密
209
提示用户输入的密码有误，并返回执行步骤202

图2

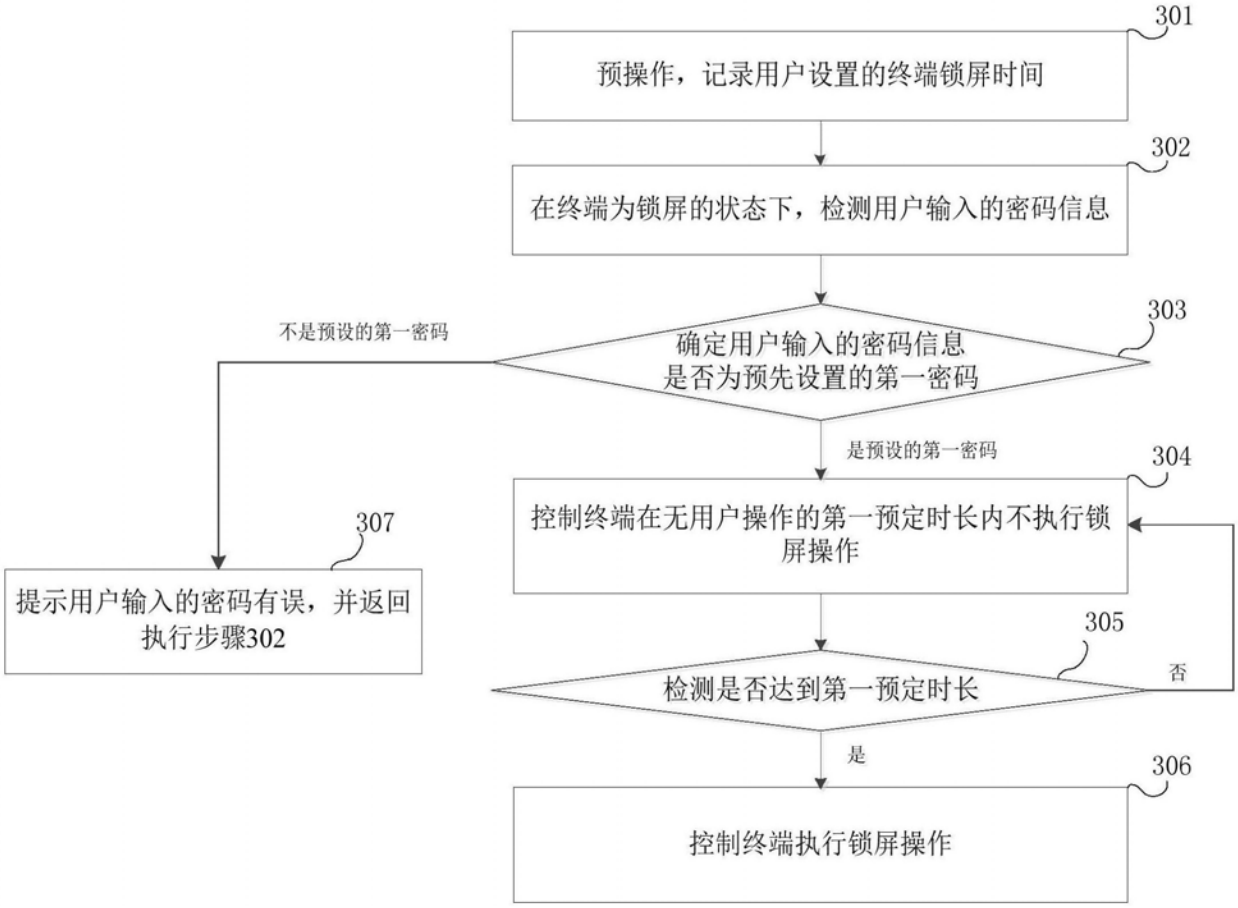

301
预操作，记录用户设置的终端锁屏时间
302
在终端为锁屏的状态下，检测用户输入的密码信息
303
确定用户输入的密码信息
是否为预先设置的第一密码
不是预设的第一密码
是预设的第一密码
304
控制终端在无用户操作的第一预定时长内不执行锁屏操作
307
提示用户输入的密码有误，并返回执行步骤302
305
检测是否达到第一预定时长
否
是
306
控制终端执行锁屏操作

图3

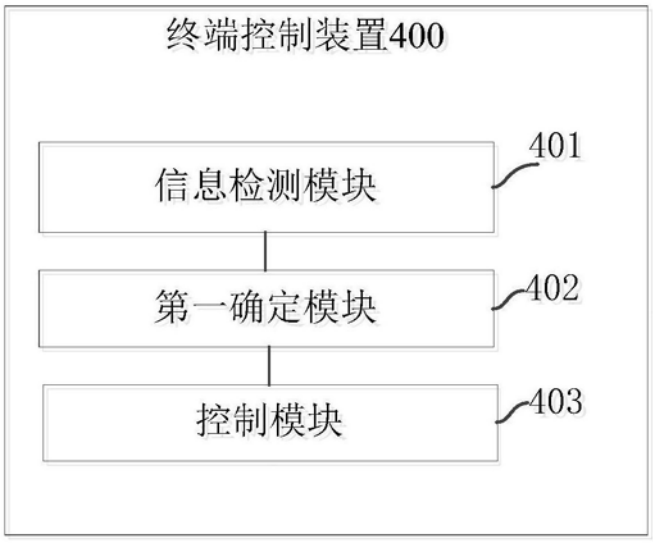

终端控制装置400
401
信息检测模块
402
第一确定模块
403
控制模块

图4

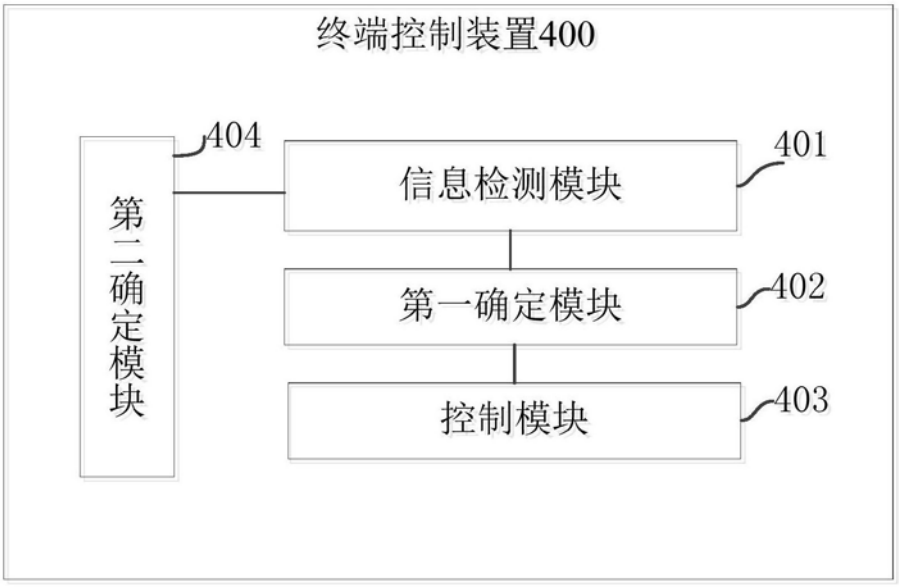

终端控制装置400
404
第二确定模块
信息检测模块
401
第一确定模块
402
控制模块
403

图5

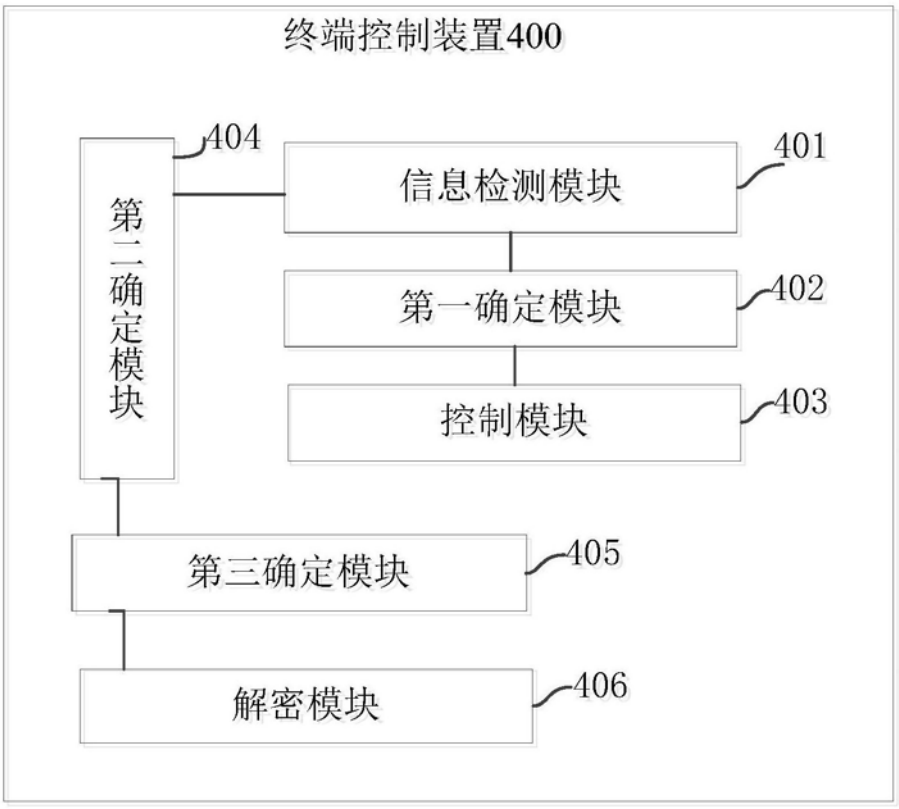

终端控制装置400
404
第二确定模块
信息检测模块
401
第一确定模块
402
控制模块
403
第三确定模块
405
解密模块
406

图6

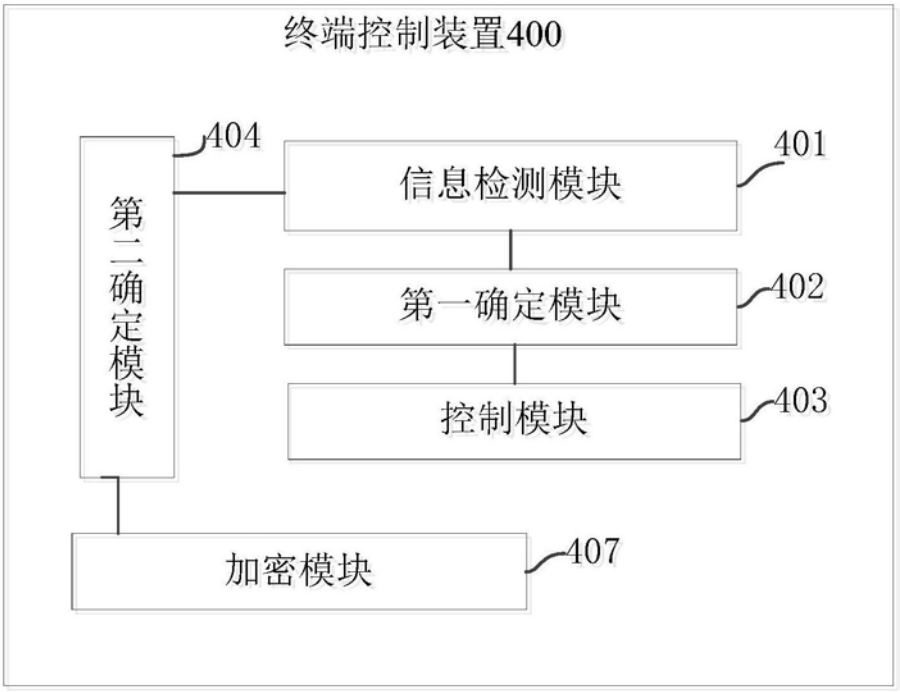

终端控制装置400
404
第二确定模块
信息检测模块
401
第一确定模块
402
控制模块
403
加密模块
407

图7

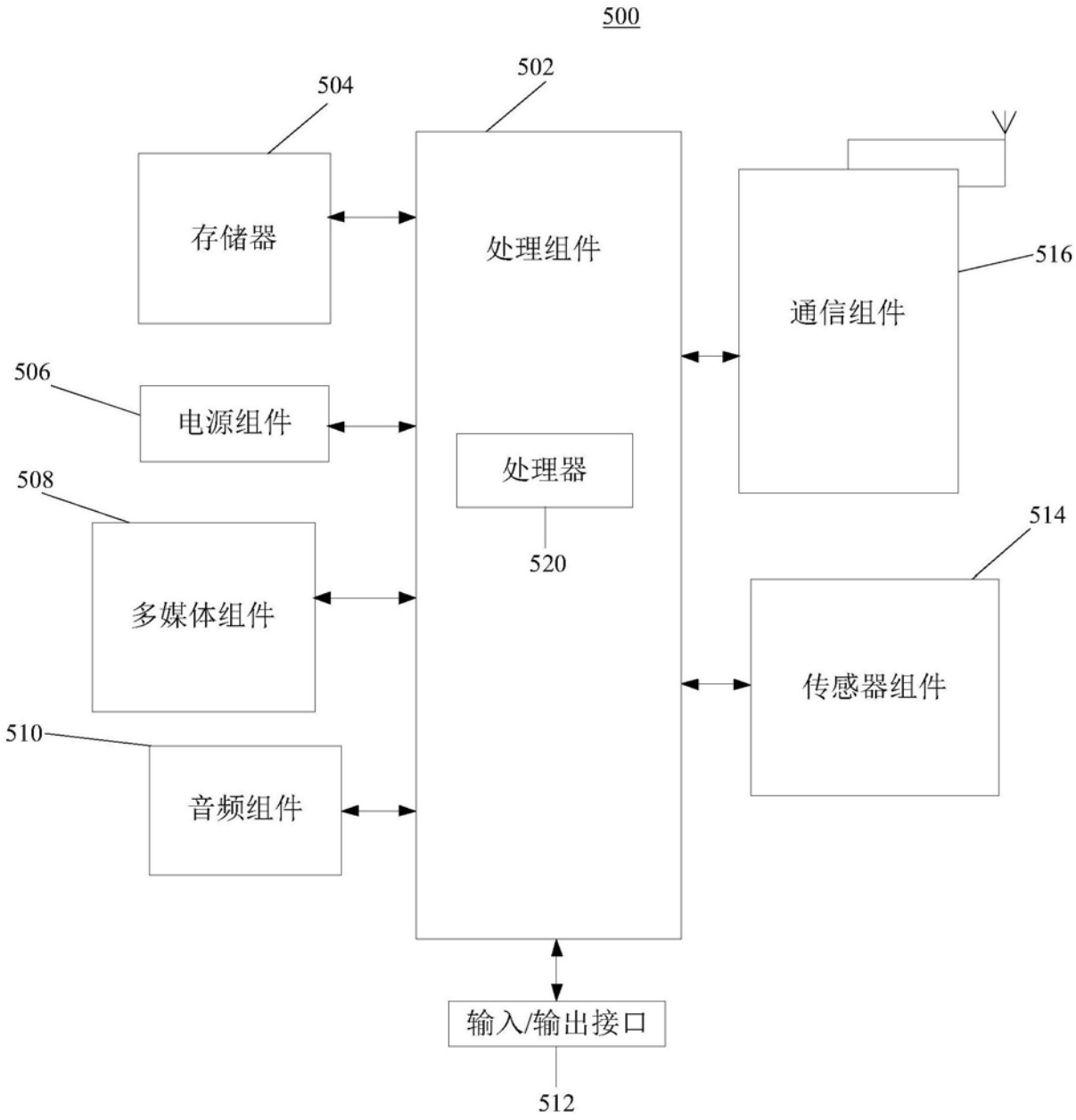

500
502
504
存储器
处理组件
通信组件
516
506
电源组件
处理器
520
508
多媒体组件
514
传感器组件
510
音频组件
输入/输出接口
512

图8