



(12) 实用新型专利

(10) 授权公告号 CN 202679426 U

(45) 授权公告日 2013. 01. 16

(21) 申请号 201220365428. 2

(22) 申请日 2012. 07. 26

(73) 专利权人 深圳市赛格导航科技股份有限公司

地址 518019 广东省深圳市南山区高新区市
高新技术工业村 T2 栋 B6 厂房

(72) 发明人 洪军 黄冠明

(74) 专利代理机构 深圳市顺天达专利商标代理
有限公司 44217

代理人 郭伟刚

(51) Int. Cl.

H04L 29/08 (2006. 01)

H04M 1/725 (2006. 01)

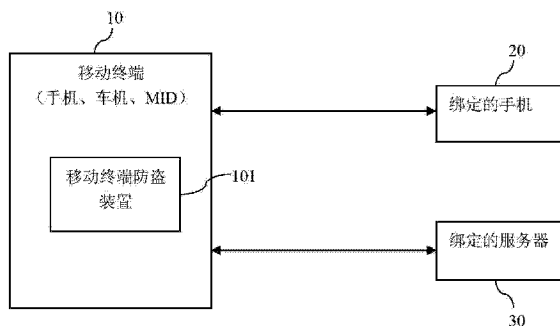
权利要求书 1 页 说明书 3 页 附图 1 页

(54) 实用新型名称

一种移动终端防盗装置

(57) 摘要

本实用新型公开了一种移动终端防盗装置。当移动终端防盗装置(101)检测到移动终端(10)更换了SIM卡时,自动定时发送被盗移动终端(10)的位置信息至绑定的手机(20)或服务器(30),用户可在绑定的手机(20)或服务器(30)上发送远程控制指令到该移动终端(10)以实现对该移动终端(10)的远程控制。本实用新型通过多种指令实现对被盗移动终端(10)的远程控制,可更好地保护用户的私人信息以及更快地找到被盗的终端。此外,本实用新型还可通过与SIM卡号无关的无线网络连接,以此为基础,结合现有的移动终端的功能以及无线技术和无线服务,在服务器上实现对被盗终端的远程控制,具有较强的通用性和实用性。



1. 一种移动终端防盗装置,其特征在于,所述装置包括核心处理器(1011),与核心处理器分别连接的 GPS 定位单元(1012)、设置单元(1014)、检测单元(1015)、分析处理单元(1016)和远程控制单元(1017);其中,

设置单元(1014)用于读取当前使用的 SIM 卡的特征码并将其存储在移动终端(10)的 FlashROM 中,以及设置绑定的手机号码或服务器 IP 地址;当检测单元(1015)检测到新换的 SIM 卡的特征码与前次存储的特征码不符时,分析处理单元(1016)定时调用 GPS 定位单元(1012)获得移动终端(10)的当前位置,并将该位置信息自动发送至绑定的手机(20)或服务器(30);绑定的手机(20)或服务器(30)可发送远程控制指令到远程控制单元(1017)以实现移动终端(10)的远程控制,所述远程控制包括锁定移动终端(10)、发送或销毁短信和电话本、发送移动终端(10)被盗后的通话记录信息、拍照并发送照片、录音并发送音频。

2. 根据权利要求 1 所述的移动终端防盗装置,所述装置还包括与核心处理器(1011)连接的密码验证单元(1013),用于移动终端(10)在设置防盗追踪功能之前或重新开机时,进入密码验证界面验证密码。

3. 根据权利要求 1 或 2 所述的移动终端防盗装置,其特征在于,所述移动终端(10)为手机、车机和 MID。

4. 根据权利要求 1 所述的移动终端防盗装置,其特征在于,当检测单元(1015)检测到新换的 SIM 卡的特征码与前次存储的特征码不符时,在所述移动终端(10)的屏幕上自动弹出预先设定的信息。

5. 根据权利要求 1 所述的移动终端防盗装置,其特征在于,当检测单元检测(1015)到新换的 SIM 卡的特征码与前次存储的特征码不符时,所述移动终端(10)自动将预先录制好的声音信息播放出来;所述播放的时机包括:定时、有电话拨入时、有电话拨出时、收到短信时、发出短信时。

一种移动终端防盗装置

技术领域

[0001] 本实用新型涉及一种移动终端防盗装置。

背景技术

[0002] 随着信息化、智能化、网络化的发展,手机、车机、MID 等移动终端的应用程度大大提高。此类移动终端中一般不具有识别的方法或记号(如指纹识别等)来证明使用者的身份,并且,无法知道丢失的终端的具体位置进而找到,同时终端中的一些私人或商务信息也可能会泄漏,因此,一旦遭到偷窃或是丢失,将会用户造成很大的困扰。

实用新型内容

[0003] 本实用新型的目的在于提供一种移动终端防盗装置,可以通过 GPS 单元获得被盗移动终端的地理位置,并在绑定的手机或服务器上实现对被盗移动终端的多种指令的远程控制,从而可保护用户的私人信息以及帮助找到该被盗终端。

[0004] 为了实现上述目的,本实用新型主要采用以下技术方案:

[0005] 一种移动终端防盗装置,所述装置包括核心处理器,与核心处理器分别连接的 GPS 定位单元、设置单元、检测单元、分析处理单元和远程控制单元;其中,

[0006] 设置单元用于读取当前使用的 SIM 卡的特征码并将其存储在移动终端的 FlashROM 中,以及设置绑定的手机号码或服务器 IP 地址;当检测单元检测到新换的 SIM 卡的特征码与前次存储的特征码不符时,分析处理单元定时调用 GPS 定位单元获得移动终端的当前位置,并将该位置信息自动发送至绑定的手机或服务器;绑定的手机或服务器可发送远程控制指令到远程控制单元以实现对移动终端的远程控制,所述远程控制包括锁定移动终端、发送或销毁短信和电话本、发送移动终端被盗后的通话记录信息、拍照并发送照片、录音并发送音频。

[0007] 所述移动终端防盗装置还包括与核心处理器连接的密码验证单元,用于移动终端在设置防盗追踪功能之前或重新开机时,进入密码验证界面验证密码。

[0008] 进一步,所述移动终端为手机、车机和 MID。

[0009] 进一步,当检测单元检测到新换的 SIM 卡的特征码与前次存储的特征码不符时,在所述移动终端的屏幕上自动弹出预先设定的信息。

[0010] 进一步,当检测单元检测到新换的 SIM 卡的特征码与前次存储的特征码不符时,所述移动终端自动将预先录制好的声音信息播放出来;所述播放的时机包括:定时、有电话拨入时、有电话拨出时、收到短信时、发出短信时。

[0011] 本实用新型的优点在于,可通过多种指令实现对被盗移动终端的远程控制,以便更好地保护用户的私人信息以及更快地找到被盗的终端。此外,本实用新型还可通过与 SIM 卡号无关的无线网络连接,以此为基础,结合现有的移动终端的功能以及无线技术和无线服务,在服务器上实现对被盗终端的远程控制,具有较强的通用性和实用性。

附图说明

[0012] 图 1 是本实用新型的原理图；

[0013] 图 2 是本实用新型的装置的模块框图。

具体实施方式

[0014] 为了使本实用新型的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本实用新型做进一步的详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本实用新型，并不用于限定本实用新型。

[0015] 图 1 是本实用新型的原理图。移动终端 10（例如，手机、车机和 MID）被盗后，盗取者必然会使用新的 SIM 卡，当移动终端防盗装置 101 检测到移动终端 10 更换了 SIM 卡时，自动定时发送丢失的移动终端的位置信息至绑定的手机 20 或服务器 30，用户可在绑定的手机 20 或服务器 30 上发送远程控制指令到该移动终端 10 以实现对该移动终端 10 的远程控制，从而保护用户的私人信息，以及帮助用户更方便地找到被盗手机。

[0016] 图 2 是本实用新型的装置的模块框图。移动终端防盗装置 101 包括核心处理器 1011，与核心处理器 1011 分别连接的 GPS 定位单元 1012、密码验证单元 1013、设置单元 1014、检测单元 1015、分析处理单元 1016 和远程控制单元 1017。

[0017] GPS 定位单元 1012，用于接收卫星的定位信号，获取移动终端的地理位置；

[0018] 密码验证单元 1013，用于用于移动终端 10 在设置防盗追踪功能之前或重新开机时，进入密码验证界面验证密码；

[0019] 设置单元 1014，用于开启防盗追踪功能，读取当前使用的 SIM 卡的特征码并将其存储在移动终端 10 的 FlashROM（闪速存储器）中，并设置绑定的手机号码或绑定的服务器的 IP 地址，绑定的手机号码或绑定的服务器的 IP 地址可以为若干个，例如，可以为公安机关的相关号码；

[0020] 检测单元 1015，用于在每次开机时，将当前 SIM 卡的特征码与前次存储的特征码进行比较；

[0021] 分析处理单元 1016，用于当检测单元 1015 检测到新换的 SIM 卡的特征码与前次存储的特征码不符时，定时调用 GPS 定位单元 1012 获得移动终端 10 的当前位置后，将该位置自动信息发送至绑定的手机 20 或服务器 30。此外，分析处理单元 1016 可使被盗移动终端 10 的屏幕上自动弹出预先设定的信息（例如，请与失主联系，号码 XXXXXX）。再者，分析处理单元 1016 还可使被盗移动终端 10 自动将预先录制好的声音信息播放出来；所述播放的时机包括：定时、有电话拨入时、有电话拨出时、收到短信时、发出短信时，上述声音信息可以由机主录制，当移动终端 10 被检测为非法时，自动把来电、来短信的铃音改为该录音，且在主动拨号和发短信时也自动播放，这样可使盗机者难以将被盗移动终端 10 出卖；

[0022] 远程控制单元 1017，用于在绑定的手机 20 或服务器 30 上发送远程控制指令到被盗移动终端 10，以进行远程控制，该指令为可扩展的指令集，可以随着无线网络的应用的普及和无线网络应用的丰富而进行扩展，所述远程控制包括但不限于：锁定移动终端、发送或销毁短信和电话本、发送该移动终端被盗后的通话记录信息。由于现今的移动终端，例如智能手机上，大都具有摄像头和录音模块，因此，还可远程控制被盗移动终端对偷盗者或周围环境进行拍照和录音，并将照片和音频文件发送至绑定的手机或服务器。需要指出的是，上

述远程控制动作中的销毁原有机主的短信及电话本可以保护原机主的私人信息或商业信息不外泄,在销毁前将其发送至绑定的手机可以帮助原机主重新获得重要的联系人或相关信息;发送移动终端被盗后的通话记录信息至绑定的手机或服务器,可以使得原机主或公安机关更加方便地找到盗机者。

[0023] 以上是对实用新型所提供的一种移动终端防盗装置进行了详细的介绍,本文中应用了具体个例对本实用新型的结构原理及实施方式进行了阐述,以上实施例指示用于帮助理解本实用新型的方法及核心思想;同时,对于本领域的一般技术人员,依据本实用新型的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本使用新型的限制。

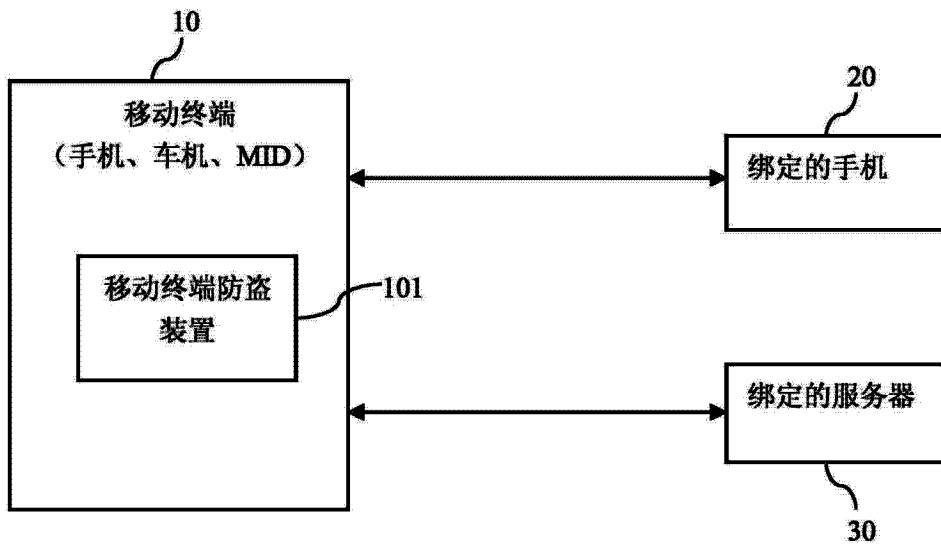


图 1

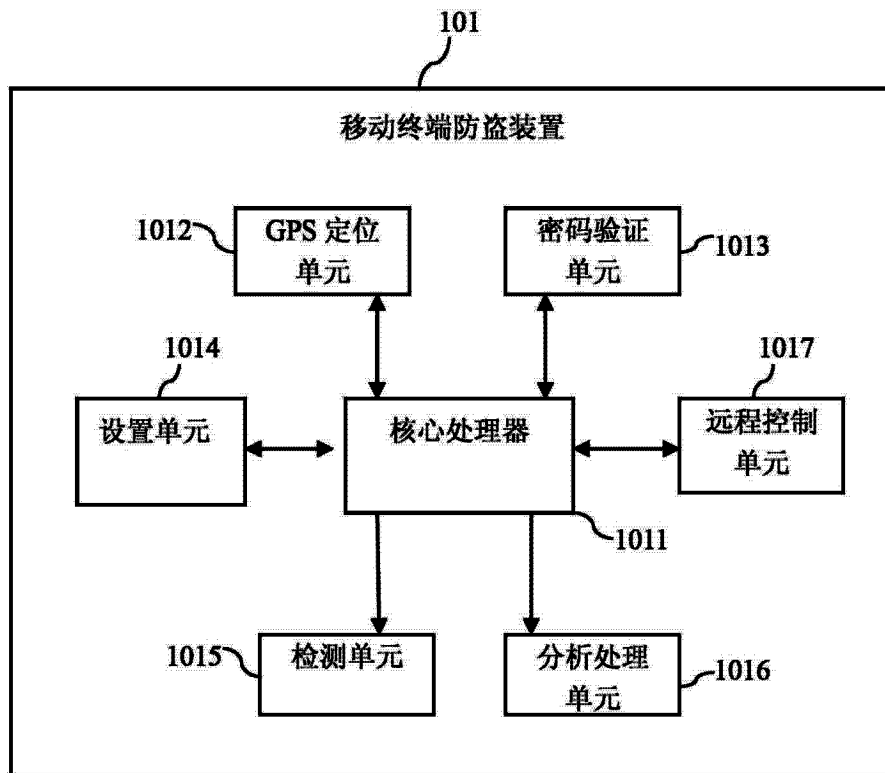


图 2