



(12) 发明专利

(10) 授权公告号 CN 102006597 B

(45) 授权公告日 2014. 02. 05

(21) 申请号 201010508310. 6

CN 101068441 A, 2007. 11. 07,

(22) 申请日 2010. 10. 14

审查员 薛永旭

(73) 专利权人 宇龙计算机通信科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新技术产业园(北区) 梦溪道 2 号酷派信息港(1 号楼)

(72) 发明人 陈历伟 黄家练

(74) 专利代理机构 深圳中一专利商标事务所 44237

代理人 张全文

(51) Int. Cl.

H04W 12/06 (2009. 01)

H04W 12/12 (2009. 01)

(56) 对比文件

CN 101203000 A, 2008. 06. 18,

CN 101316167 A, 2008. 12. 03,

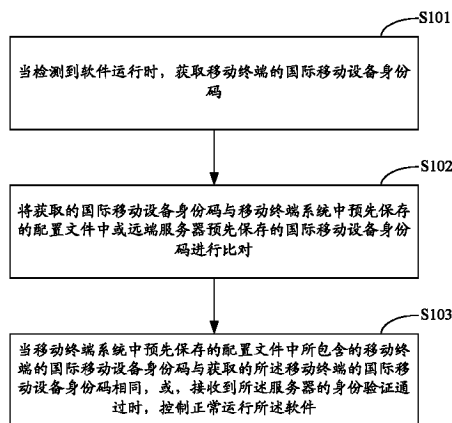
权利要求书2页 说明书8页 附图3页

(54) 发明名称

一种软件使用权的控制方法、系统及移动终端

(57) 摘要

本发明适用于通信技术领域,提供了一种软件使用权的控制方法、系统及移动终端,所述方法包括:当检测到软件运行时,获取移动终端的国际移动设备身份码;将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件中或远端服务器预先保存的国际移动设备身份码进行比对验证;当配置文件中所包含的国际移动设备身份码与获取的国际移动设备身份码相同,或,接收到服务器的身份验证通过时,控制正常运行软件,实现对软件使用的有效控制和保护。



1. 一种软件使用权的控制方法,其特征在于,所述方法包括下述步骤:

当检测到软件运行时,获取移动终端的国际移动设备身份码;

将获取的国际移动设备身份码与移动终端中预先保存的配置文件中或远端服务器预先保存的国际移动设备身份码进行比对验证;

当移动终端中预先保存的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件;

其中,所述将获取的国际移动设备身份码与移动终端中预先保存的配置文件中或远端服务器预先保存的国际移动设备身份码进行比对验证的步骤具体包括:

判断移动终端中是否存在预先保存的与所述软件相关的配置文件;

当移动终端中存在预先保存的与所述软件相关的配置文件时,判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同;

当移动终端中不存在预先保存的与所述软件相关的配置文件时,将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证;

在所述远端服务器反馈身份验证不通过的情况下,移动终端显示屏输出一包含用户注册成为合法用户的提示信息;

接收注册成为合法用户的注册信息,并转发给所述远端服务器,所述注册信息包含移动终端的国际移动设备身份码以及移动终端的系统版本信息,以使所述远端服务器生成配置文件,并注册所述移动终端用户;

在所述当检测到软件运行时,获取移动终端的国际移动设备身份码的步骤之前还包括下述步骤:

预先保存与所述软件相关的配置文件,所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息,所述配置文件包括移动终端的国际移动设备身份码和当前系统版本信息,存放于移动终端根目录。

2. 如权利要求1所述的方法,其特征在于,当移动终端中存在预先保存的与所述软件相关的配置文件时,所述判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同的步骤之前还包括下述步骤:

对预先保存的与所述软件相关的配置文件进行解密操作。

3. 如权利要求1所述的方法,其特征在于,当移动终端中不存在预先保存的与所述软件相关的配置文件时,所述将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证的步骤之前还包括下述步骤:

判断移动终端建立的网络连接是否成功;

当移动终端建立的网络连接成功时,执行所述将获取的移动终端的国际移动设备身份码发送远端的服务器的步骤;

当移动终端建立的网络连接不成功时,执行控制结束所述软件的运行的步骤。

4. 一种软件使用权的控制系统,其特征在于,所述系统包括:

获取模块,用于当检测到软件运行时,获取移动终端的国际移动设备身份码;

比对验证模块,用于将获取的国际移动设备身份码与移动终端中预先保存的配置文件
中或远端服务器预先保存的国际移动设备身份码进行比对验证;以及

软件正常运行控制模块,用于当所述比对验证模块比对得到预先保存的与所述软件相
关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际
移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件;

其中,所述比对验证模块具体包括:

第一判断模块,用于判断移动终端中是否存在预先保存的与所述软件相关的配置文
件;

第二判断模块,用于当所述第一判断模块判断移动终端中存在预先保存的与所述软件
相关的配置文件时,判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端
的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同;以及

身份验证请求模块,用于当所述第一判断模块判断移动终端中不存在预先保存的与所
述软件相关的配置文件时,将获取的移动终端的国际移动设备身份码发送远端的服务器,
请求服务器进行身份验证,在所述远端服务器反馈身份验证不通过的情况下,移动终端显
示屏输出一包含用户注册成为合法用户的提示信息,接收注册成为合法用户的注册信息,
并转发给所述远端服务器,所述注册信息包含移动终端的国际移动设备身份码以及移动终
端的系统版本信息,以使所述远端服务器生成配置文件,并注册所述移动终端用户;

预先保存模块,用于预先保存与所述软件相关的配置文件,所述配置文件为在移动终
端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息,所述配置文件包括
移动终端的国际移动设备身份码和当前系统版本信息,存放于移动终端根目录。

5. 如权利要求 4 所述的系统,其特征在于,当移动终端中存在预先保存的与所述软件
相关的配置文件时,所述系统还包括:

解密模块,用于对所述预先保存的与所述软件相关的配置文件进行解密操作。

6. 如权利要求 4 所述的系统,其特征在于,当移动终端中不存在预先保存的与所述软
件相关的配置文件时,所述系统还包括:第三判断模块、软件结束运行控制模块;

第三判断模块,用于判断移动终端建立的网络连接是否成功;

当所述第三判断模块判断所述移动终端建立的网络连接成功时,执行所述身份验证请
求模块将获取的移动终端的国际移动设备身份码发送远端的服务器的步骤;

当移动终端建立的网络连接不成功时,执行所述软件结束运行控制模块控制结束所述
软件的运行。

7. 一种包括权利要求 4 至 6 任一项所述的软件使用权的控制系统的移动终端。

一种软件使用权的控制方法、系统及移动终端

技术领域

[0001] 本发明属于通信技术领域,尤其涉及一种软件使用权的控制方法、系统及移动终端。

背景技术

[0002] 现有技术中,很多终端软件仅仅是在安装或者使用时,提示用户输入一注册码即可安装或者使用该软件。对于一些非授权用户,只要有该注册码即可在离线的情况下正常安装或使用该软件;很多软件都是在联网的情况下进行用户合法性的检测,即便在联网的情况下,只要用户不主动更新软件的最新版本,对用户使用该软件不会造成太大的问题。

[0003] 因此,现有技术不能有效的控制该终端软件的使用权限,不能有效禁止非法用户的恶意使用。

发明内容

[0004] 本发明实施例的目的在于提供一种软件使用权的控制方法,旨在解决现有技术提供的控制方案不能有效的控制软件的使用权限,不能有效禁止非法用户的恶意使用的问题。

[0005] 本发明实施例是这样实现的,一种软件使用权的控制方法,所述方法包括下述步骤:

[0006] 当检测到软件运行时,获取移动终端的国际移动设备身份码;

[0007] 将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件中或远端服务器预先保存的国际移动设备身份码进行比对验证;

[0008] 当预先保存的与该软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件;

[0009] 其中,所述将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件中或远端服务器预先保存的国际移动设备身份码进行比对验证的步骤具体包括:

[0010] 判断移动终端系统中是否存在预先保存的与该软件相关的配置文件;

[0011] 当移动终端系统中存在预先保存的与该软件相关的配置文件时,判断所述预先保存的与该软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同;

[0012] 当移动终端系统中不存在预先保存的与该软件相关的配置文件时,将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证;

[0013] 在所述远端服务器反馈身份验证不通过的情况下,移动终端显示屏输出一包含用户注册成为合法用户的提示信息;

[0014] 接收注册成为合法用户的注册信息,并转发给所述远端服务器,所述注册信息包含移动终端的国际移动设备身份码以及移动终端的系统版本信息,以使所述远端服务器生

成配置文件,并注册所述移动终端用户;

[0015] 在所述当检测到软件运行时,获取移动终端的国际移动设备身份码的步骤之前还包括下述步骤:

[0016] 预先保存与所述软件相关的配置文件,所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息,所述配置文件包括移动终端的国际移动设备身份码和当前系统版本信息,存放于移动终端系统根目录。

[0017] 本发明实施例的另一目的在于提供一种软件使用权的控制系统,所述系统包括:

[0018] 获取模块,用于当检测到软件运行时,获取移动终端的国际移动设备身份码;

[0019] 比对验证模块,用于将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对验证;以及

[0020] 软件正常运行控制模块,用于当所述比对验证模块比对得到预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件;

[0021] 其中,所述比对验证模块具体包括:

[0022] 第一判断模块,用于判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件;

[0023] 第二判断模块,用于当所述第一判断模块判断移动终端系统中存在预先保存的与所述软件相关的配置文件时,判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同;以及

[0024] 身份验证请求模块,用于当所述第一判断模块判断移动终端系统中不存在预先保存的与所述软件相关的配置文件时,将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证,在所述远端服务器反馈身份验证不通过的情况下,移动终端显示屏输出一包含用户注册成为合法用户的提示信息,接收注册成为合法用户的注册信息,并转发给所述远端服务器,所述注册信息包含移动终端的国际移动设备身份码以及移动终端的系统版本信息,以使所述远端服务器生成配置文件,并注册所述移动终端用户;

[0025] 预先保存模块,用于预先保存与所述软件相关的配置文件,所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息,所述配置文件包括移动终端的国际移动设备身份码和当前系统版本信息,存放于移动终端系统根目录。

[0026] 本发明实施例的另一目的在于提供一种包括软件使用权的控制系统移动终端。

[0027] 在本发明实施例中,当检测到软件运行时,获取移动终端的国际移动设备身份码;将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对验证;当预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件,实现对软件使用的有效控制和保护。

附图说明

- [0028] 图 1 是本发明第一实施例提供的软件使用权的控制方法的实现流程图；
[0029] 图 2 是本发明第二实施例提供的软件使用权的控制方法的实现流程图；
[0030] 图 3 是本发明第一实施例提供的软件使用权的控制系统的结构框图；
[0031] 图 4 是本发明第二实施例提供的软件使用权的控制系统的结构框图。

具体实施方式

[0032] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0033] 在本发明实施例中，当用户运行终端软件时，通过对终端中是否预先保存软件的配置文件和网络服务器的验证匹配的方式对软件的使用权进行验证，从而有效控制软件的使用权。

[0034] 本发明实施例的目的在于提供一种软件使用权的控制方法，所述方法包括下述步骤：

[0035] 当检测到软件运行时，获取移动终端的国际移动设备身份码；

[0036] 将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对；

[0037] 当预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同，或，接收到所述服务器的身份验证通过时，控制正常运行所述软件；

[0038] 其中，所述将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对验证的步骤具体包括：

[0039] 判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件；

[0040] 当移动终端系统中存在预先保存的与所述软件相关的配置文件时，判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同；

[0041] 当移动终端系统中不存在预先保存的与所述软件相关的配置文件时，将获取的移动终端的国际移动设备身份码发送远端的服务器，请求服务器进行身份验证；

[0042] 在所述远端服务器反馈身份验证不通过的情况下，移动终端显示屏输出一包含用户注册成为合法用户的提示信息；

[0043] 接收注册成为合法用户的注册信息，并转发给所述远端服务器，所述注册信息包含移动终端的国际移动设备身份码以及移动终端的系统版本信息，以使所述远端服务器生成配置文件，并注册所述移动终端用户；

[0044] 在所述当检测到软件运行时，获取移动终端的国际移动设备身份码的步骤之前还包括下述步骤：

[0045] 预先保存与所述软件相关的配置文件，所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息，所述配置文件包括移动终端的国际移动设备身份码和当前系统版本信息，存放于移动终端系统根目录。

[0046] 本发明实施例的另一目的在于提供一种软件使用权的控制系统,所述系统包括:

[0047] 获取模块,用于当检测到软件运行时,获取移动终端的国际移动设备身份码;

[0048] 比对验证模块,用于将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对;以及

[0049] 软件正常运行控制模块,用于当所述比对验证模块比对得到预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件;

[0050] 其中,所述比对验证模块具体包括:

[0051] 第一判断模块,用于判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件;

[0052] 第二判断模块,用于当所述第一判断模块判断移动终端系统中存在预先保存的与所述软件相关的配置文件时,判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同;以及

[0053] 身份验证请求模块,用于当所述第一判断模块判断移动终端系统中不存在预先保存的与所述软件相关的配置文件时,将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证,在所述远端服务器反馈身份验证不通过的情况下,移动终端显示屏输出一包含用户注册成为合法用户的提示信息,接收注册成为合法用户的注册信息,并转发给所述远端服务器,所述注册信息包含移动终端的国际移动设备身份码以及移动终端的系统版本信息,以使所述远端服务器生成配置文件,并注册所述移动终端用户;

[0054] 预先保存模块,用于预先保存与所述软件相关的配置文件,所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息,所述配置文件包括移动终端的国际移动设备身份码和当前系统版本信息,存放于移动终端系统根目录。

[0055] 本发明实施例的另一目的在于提供一种包括软件使用权的控制系统的移动终端。

[0056] 图1示出了本发明第一实施例提供的软件使用权的控制方法的实现流程,其具体的步骤如下所述:

[0057] 在步骤S101中,当检测到软件运行时,获取移动终端的国际移动设备身份码。

[0058] 在步骤S102中,将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对。

[0059] 在步骤S103中,当移动终端系统中预先保存的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同,或,接收到所述服务器的身份验证通过时,控制正常运行所述软件。

[0060] 在本发明实施例中,当获取到移动终端的国际移动设备身份码后,即可将该国际移动设备身份码与移动终端预先存储的配置文件中所包含的国际移动设备身份码进行比对,或者请求远端服务器的验证,当比对成功或验证通过时,控制软件的正常运行。

[0061] 图2示出了本发明第二实施例提供的软件使用权的控制方法的实现流程,其具体的步骤如下所述:

- [0062] 在步骤 S201 中,当检测到软件运行时,获取移动终端的国际移动设备身份码。
- [0063] 在本发明实施例中,移动终端的该国际移动设备身份码用以唯一标识该移动终端。
- [0064] 在步骤 S202 中,判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件,是则执行步骤 S203,否则执行步骤 S207。
- [0065] 在本发明实施例中,该与软件相关的配置文件为预先保存在移动终端系统中的文件,其具体的信息下述有一实施例进行说明,在此不再赘述。
- [0066] 在步骤 S203 中,读取移动终端系统中预先保存的与所述软件相关的配置文件,并解密,得到该配置文件中所包含的移动终端的国际移动设备身份码。
- [0067] 在本发明实施例中,该对配置文件的解析的过程即可以理解为对配置文件的解密过程,其解密的密钥可以通过远端的服务器获取的。
- [0068] 在步骤 S204 中,判断获取移动终端的国际移动设备身份码与解密得到的配置文件中所包含的移动终端的国际移动设备身份码是否相同,是则执行步骤 S205,否则执行步骤 S206。
- [0069] 在步骤 S205 中,控制正常运行该软件。
- [0070] 在本发明实施例中,当获取移动终端的国际移动设备身份码与解析得到的配置文件中所包含的移动终端的国际移动设备身份码相同时,表示该移动终端为合法用户,则可以正常使用该软件。
- [0071] 在步骤 S206 中,控制结束该软件的运行。
- [0072] 在本发明实施例中,当获取移动终端的国际移动设备身份码与解析得到的配置文件中所包含的移动终端的国际移动设备身份码不相同时,表示该移动终端为非法用户,则可以正常使用该软件。
- [0073] 在步骤 S207 中,判断移动终端建立的网络连接是否成功,是则执行步骤 S208,否则执行步骤 S206。
- [0074] 在本发明实施例中,当移动终端系统中没有存在预先保存的与所述软件相关的配置文件时,将移动终端与网络建立连接,该网络连接方式可以现有的网络连接,在此不用以限制本发明。
- [0075] 在步骤 S208 中,将获取的移动终端的国际移动设备身份码发送远端的服务器,请求服务器进行身份验证。
- [0076] 在步骤 S209 中,接收远端服务器反馈的身份验证结果。
- [0077] 在本发明实施例中,该身份验证结果包括验证通过和验证不通过两种情况;
- [0078] 当验证通过时,则执行上述步骤 S105,正常运行该软件;
- [0079] 当验证不通过时,则执行上述步骤 S106,控制结束该软件的运行。
- [0080] 在本发明实施例中,上述仅为本发明的一个实施例。
- [0081] 作为本发明的一个具体实施例,当移动终端在建立网络连接,远端服务器反馈身份验证不通过的情况下,可以在移动终端输出一提示信息,该提示信息可以是“注册成为合法用户”的功能选项按钮或者菜单,用户可以选择注册成为合法用户,以便使用运行该软件,其具体的实现流程为:
- [0082] 1、移动终端显示屏输出一提示信息,提示信息包含用户注册成为合法用户的信

息。

[0083] 2、接收注册成为合法用户的注册信息，并转发给远端服务器，所述信息还包含移动终端的国际移动设备身份码以及移动终端的系统版本信息，使所述服务器生成配置文件，注册所述移动终端用户。

[0084] 作为本发明的另一个实施例，对于保存在移动终端中的配置文件，可以在软件预装时生成的，也可以是服务器端生成推送给移动终端存储的，下述给出具体的说明：

[0085] 1、软件预装时生成配置文件

[0086] 在本发明实施例中，对于预装的软件，首先使用加密算法为当前移动终端生成一个与国际移动设备身份码相关的配置文件，其中，该加密算法包括但不限于 DES 算法，该配置文件包括移动终端的国际移动设备身份码和当前移动终端系统版本信息，并存放于移动终端的系统根目录中。

[0087] 2、服务器端生成配置文件

[0088] 当服务器对到用户发送的身份验证请求验证不通过时，接收注册成为合法用户的信息，所述信息还包含移动终端的国际移动设备身份码以及移动终端的系统版本信息，根据相应的加密算法（DES 加密算法）将移动终端的国际移动设备身份码以及移动终端的系统版本信息生成配置文件，并将配置文件推送给移动终端，移动终端保存在系统根目录。同时，服务器将该移动终端的国际移动设备身份码保存到服务器数据库，防止移动终端加密文件丢失或者损坏时，保证合法用户的正常访问。

[0089] 在本发明实施例中，当移动终端与网络建立连接时，向服务器发送身份验证请求，服务器根据保存在数据库中的合法用户的移动终端的国际移动设备身份码，对移动终端的身份进行验证，该验证过程与现有技术中的用户身份验证过程相似，在此不再赘述，但不用以限制本发明。

[0090] 图 3 示出了本发明第一实施例提供的软件使用权的控制系统的结构框图，为了便于说明，图中仅给出了与本发明实施例相关的部分，其中，软件使用权的控制系统可以内置于移动终端的软件单元、硬件单元或软硬件结合单元。

[0091] 获取模块 11 当检测到软件运行时，获取移动终端的国际移动设备身份码；比对验证模块 12 将获取的国际移动设备身份码与移动终端系统中预先保存的配置文件或远端服务器预先保存的国际移动设备身份码进行比对；当所述比对验证模块 12 比对得到预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同，或，接收到所述服务器的身份验证通过时，软件正常运行控制模块 13 控制正常运行所述软件。

[0092] 上述仅为本发明的一个系统实施例，其各模块的功能如上述方法实施例所述，在此不再赘述。

[0093] 图 4 示出了本发明第二实施例提供的软件使用权的控制系统的结构框图，为了便于说明，图中仅给出了与本发明实施例相关的部分，其中，软件使用权的控制系统可以内置于移动终端的软件单元、硬件单元或软硬件结合单元。

[0094] 获取模块 11 当检测到软件运行时，获取移动终端的国际移动设备身份码；第一判断模块 121 判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件；当所述第一判断模块 121 判断移动终端系统中存在预先保存的与所述软件相关的配置文件时，第

二判断模块 122 判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同；当所述第一判断模块 122 判断移动终端系统中不存在预先保存的与所述软件相关的配置文件时，身份验证请求模块 123 将获取的移动终端的国际移动设备身份码发送远端的服务器，请求服务器进行身份验证；当所述第二判断模块 122 判断预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同，或，接收到所述服务器的身份验证通过时，软件正常运行控制模块 13 控制正常运行所述软件；当所述第二判断模块 122 判断预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码不相同，或，接收到所述服务器的身份验证不通过时，软件结束运行控制模块 14 控制结束所述软件的运行。

[0095] 在本发明实施例中，预先保存模块 15 预先保存与所述软件相关的配置文件，所述配置文件为在移动终端生成或所述服务器生成并推送给所述移动终端的加密后的文件信息。

[0096] 作为本发明的一个实施例，当第一判断模块 121 移动终端系统中存在预先保存的与所述软件相关的配置文件时，解密模块 16 对所述预先保存的与所述软件相关的配置文件进行解密操作，然后第二判断模块 122 执行判断所述预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同的步骤。

[0097] 当第一判断模块 121 判断移动终端系统中不存在预先保存的与所述软件相关的配置文件时，第三判断模块 17 判断移动终端建立的网络连接是否成功；当所述第三判断模块 17 判断所述移动终端建立的网络连接成功时，执行所述身份验证请求模块 1123 将获取的移动终端的国际移动设备身份码发送远端的服务器的步骤；当移动终端建立的网络连接不成功时，执行所述软件结束运行控制模块 14 控制结束所述软件的运行的步骤。

[0098] 在本发明实施例中，当检测到软件运行时，获取移动终端的国际移动设备身份码；判断移动终端系统中是否存在预先保存的与所述软件相关的配置文件；当移动终端系统中存在预先保存的与软件相关的配置文件时，判断预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码是否相同；当移动终端系统中不存在预先保存的与所述软件相关的配置文件时，将获取的移动终端的国际移动设备身份码发送远端的服务器，请求服务器进行身份验证；当判断预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码相同，或，接收到所述服务器的身份验证通过时，控制正常运行所述软件；当判断预先保存的与所述软件相关的配置文件中所包含的移动终端的国际移动设备身份码与获取的所述移动终端的国际移动设备身份码不相同，或，接收到所述服务器的身份验证不通过时，控制结束所述软件的运行，实现对软件使用的有效控制和保护。

[0099] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成，所述的程序可以在存储于一计算机可读取存储介质中，所述的存储介质，如 ROM/RAM、磁盘、光盘等。

[0100] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

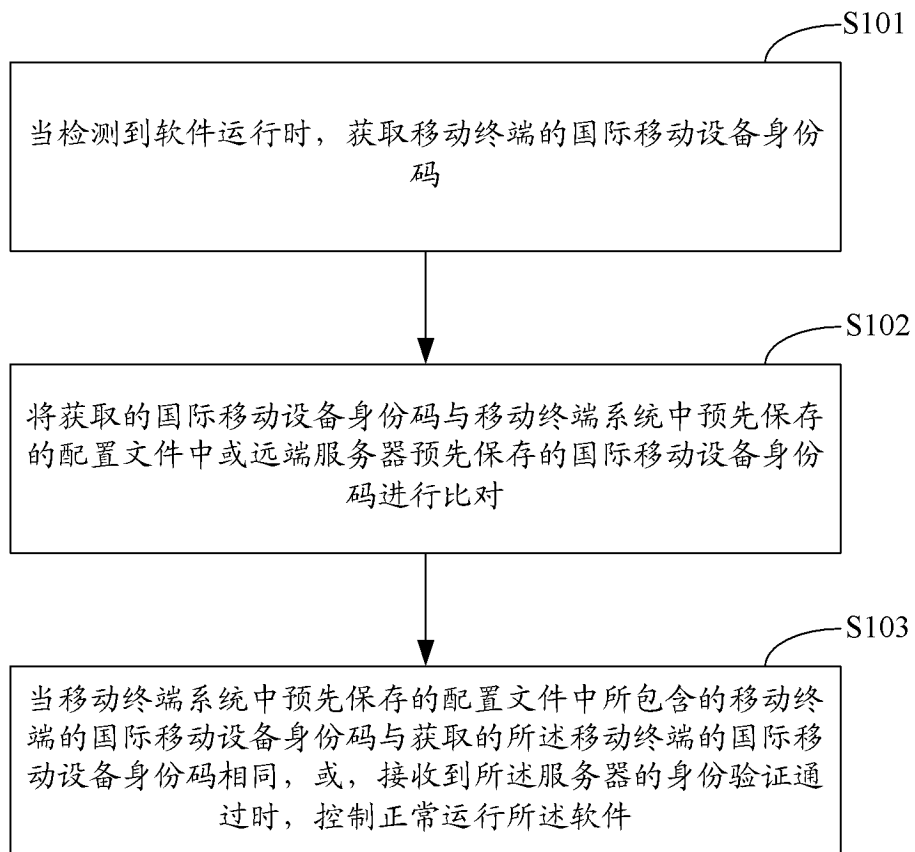


图 1

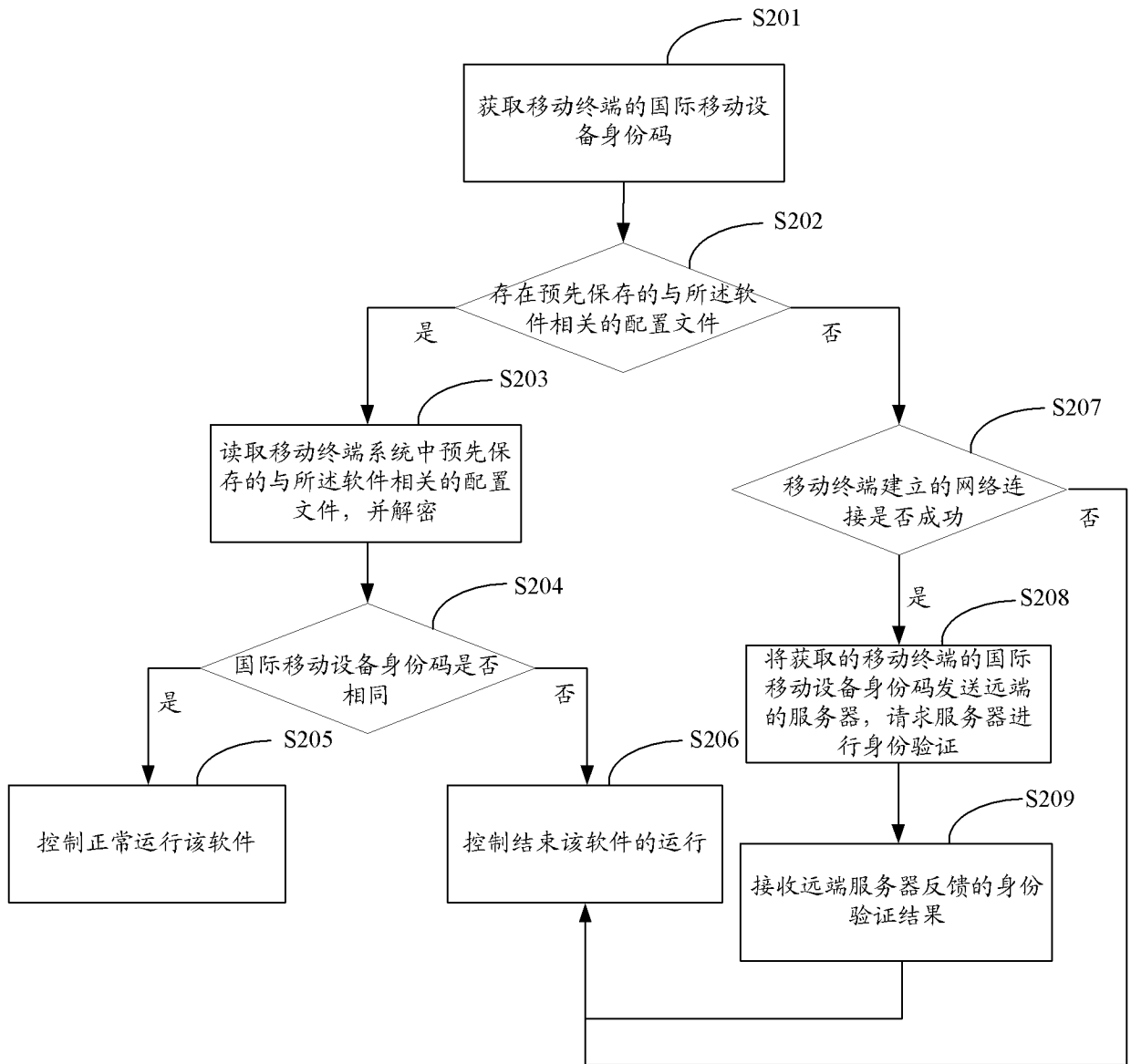


图 2

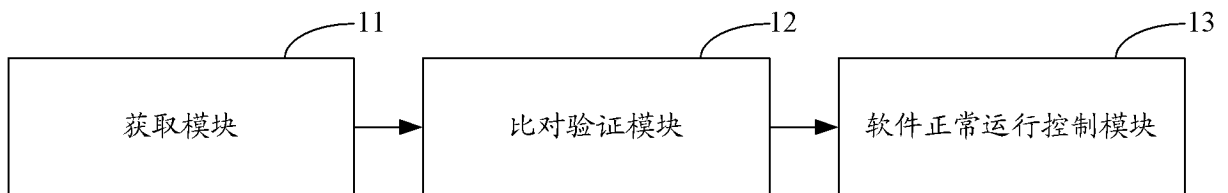


图 3

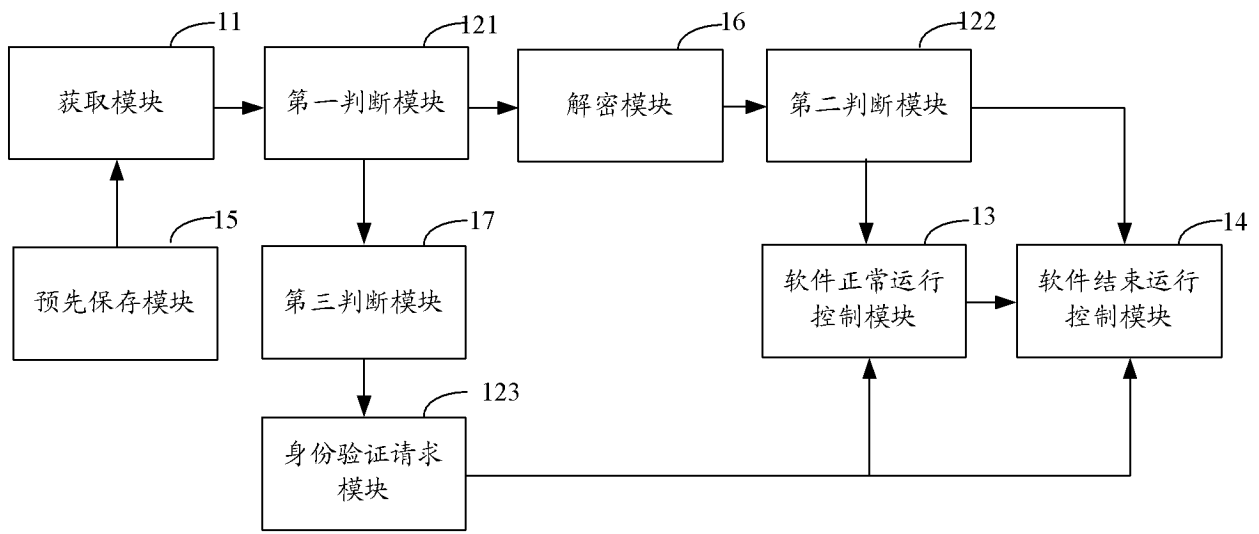


图 4