



(12)发明专利申请

(10)申请公布号 CN 107678912 A

(43)申请公布日 2018.02.09

(21)申请号 201710817973.8

(22)申请日 2017.09.12

(71)申请人 上海展扬通信技术有限公司

地址 201203 上海市浦东新区自由贸易试
验区盛夏路399弄1号A座922/926室

(72)发明人 陈俊冉

(74)专利代理机构 北京大成律师事务所 11352

代理人 李佳铭 沈汶波

(51)Int.Cl.

G06F 11/30(2006.01)

权利要求书3页 说明书10页 附图6页

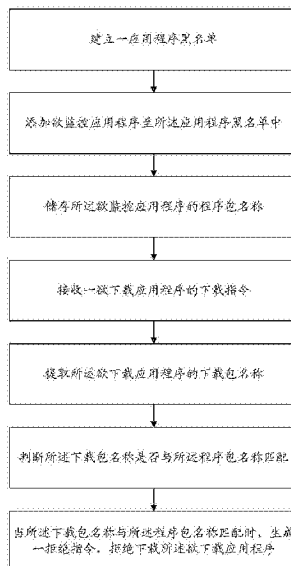
(54)发明名称

一种基于智能终端的应用程序监控方法及监控系统

(57)摘要

本发明提供了一种基于智能终端的应用程序监控方法及监控系统。监控方法具体包括：建立一应用程序黑名单；添加欲监控应用程序至所述应用程序黑名单中；储存所述欲监控应用程序的程序包名称；接收一欲下载应用程序的下载指令；提取所述欲下载应用程序的下载包名称；判断所述下载包名称是否与所述程序包名称匹配；当所述下载包名称与所述程序包名称匹配时，生成一拒绝指令，拒绝下载所述欲下载应用程序。监控系统包括：黑名单模块、添加模块、储存模块、接收模块、提取模块、处理模块和监控模块。采用上述技术方案，可通过对已下载或已安装的应用程序的标记，也可以通过手动输入应用程序名称来实现对应用程序的监控，为用户提供一种更好的使用体验。

CN 107678912 A



1. 一种基于智能终端的应用程序监控方法,其特征在于,所述应用程序监控方法包括如下步骤:
建立一应用程序黑名单;
添加欲监控应用程序至所述应用程序黑名单中;
储存所述欲监控应用程序的程序包名称;
接收一欲下载应用程序的下载指令;
提取所述欲下载应用程序的下载包名称;
判断所述下载包名称是否与所述程序包名称匹配;
当所述下载包名称与所述程序包名称匹配时,生成一拒绝指令,拒绝下载所述欲下载应用程序。
2. 如权利要求1所述的应用程序监控方法,其特征在于,所述应用程序监控方法,进一步包括:
采集包含所述程序包名称的输入信息;
生成与所述输入信息对应的禁用字段;
将所述禁用字段添加到所述应用程序黑名单中;
则,所述应用程序监控方法进一步判断所述下载包字段是否与所述禁用字段匹配;
当所述下载包名称与所述禁用字段匹配时,生成一拒绝指令,拒绝下载所述欲下载应用程序。
3. 如权利要求1所述的应用程序监控方法,其特征在于,储存所述欲监控应用程序的程序包名称的步骤中,进一步包括:
读取所述程序包名称;
根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;
保存所述程序包字段。
4. 如权利要求1所述的应用程序监控方法,其特征在于,判断所述下载包名称是否与所述程序包名称匹配的步骤中,进一步包括:
读取所述下载包名称中所包含的下载包字段及所述程序包中所包含的程序包字段;
计算所述下载包字段与所述程序包字段的匹配程度;
当所述匹配程度大于等于90%时,判断所述下载包字段与所述程序包字段匹配;
当所述匹配程度小于90%时,判断所述下载包字段与所述程序包字段不匹配。
5. 如权利要求1-4任一项所述的应用程序监控方法,其特征在于,所述应用程序监控方法,进一步包括:
将所述欲监控应用程序从所述应用程序黑名单中移除;
移除所述欲监控应用程序后,删除储存的所述程序包名称。
6. 一种基于智能终端的应用程序监控系统,其特征在于,所述应用程序监控系统包括:黑名单模块、添加模块、储存模块、接收模块、提取模块、处理模块和监控模块;
所述黑名单模块,与所述添加模块、处理模块通讯连接,建立一应用程序黑名单;
所述添加模块,与所述黑名单模块、储存模块通讯连接,添加欲监控应用程序至所述应用程序黑名单中;

所述储存模块,与所述添加模块、处理模块通讯连接,储存所述欲监控应用程序的程序包名称,并发送所述程序包名称至所述处理模块;

所述接收模块,与所述提取模块通讯连接,接收一欲下载应用程序的下载指令,并发送所述下载指令至所述提取模块;

所述提取模块,与所述接收模块、处理模块通讯连接,提取所述欲下载应用程序的下载包名称,并发送所述下载包名称至所述处理模块;

所述处理模块,与所述储存模块、提取模块、黑名单模块、监控模块通讯连接,判断所述下载包名称是否与所述程序包名称匹配,并发送匹配结果至所述监控模块;

所述监控模块与所述处理模块通讯连接,当所述下载包名称与所述程序包名称匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。

7. 如权利要求6所述的应用程序监控系统,其特征在于,

所述应用程序监控系统进一步包括:采集模块和生成模块;

所述采集模块,与所述生成模块通讯连接,采集包含所述程序包名称的输入信息,并发送所述输入信息至所述生成模块;

所述生成模块,与所述采集模块、添加模块通讯连接,生成与所述输入信息对应的禁用字段,并发送所述禁用字段至所述黑名单模块;

所述添加模块,与所述生成模块、黑名单模块通讯连接,将所述禁用字段添加到所述应用程序黑名单中;

则,所述处理模块,进一步与所述黑名单模块连接,进一步判断所述下载包字段是否与所述禁用字段匹配;

当所述下载包名称与所述禁用字段匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。

8. 如权利要求6所述的应用程序监控系统,其特征在于,

所述储存模块,进一步包括:

名称读取单元,读取所述程序包名称;

字段生成单元,根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;

保存单元,保存所述程序包字段。

9. 如权利要求6所述的应用程序监控系统,其特征在于,

所述处理模块,进一步包括:

字段读取单元,读取所述下载包名称中所包含的下载包字段及所述程序包中所包含的程序包字段;

计算单元,计算所述下载包字段与所述程序包字段的匹配程度;

当所述匹配程度大于等于90%时,判断单元判断所述下载包字段与所述程序包字段匹配;

当所述匹配程度小于90%时,判断单元判断所述下载包字段与所述程序包字段不匹配。

10. 如权利要求6-9任一项所述的应用程序监控系统,其特征在于,

所述应用程序监控系统,进一步包括:移除模块;

所述移除模块,与所述黑名单模块、储存模块通讯连接;

所述移除模块,将所述欲监控应用程序从所述应用程序黑名单中移除;

移除所述欲监控应用程序后,所述移除模块进一步删除所述储存模块中储存的所述程序包名称。

一种基于智能终端的应用程序监控方法及监控系统

技术领域

[0001] 本发明涉及智能终端技术领域,尤其涉及一种基于智能终端的应用程序监控方法及应用程序监控系统。

背景技术

[0002] 随着手机和平板电脑等智能终端设备的普及越来越广泛,各种基于智能终端设备的应用程序也得到迅速发展,相应地,各种应用程序的广告推广也随之而生。

[0003] 当用户通过智能终端浏览网页时,常常无意间的点击会触发广告应用程序的下载,智能终端自动下载不需要的应用程序,既浪费流量,也浪费智能终端的内存。不仅如此,用户还需进行繁琐的操作、花费额外的时间对已安装的应用程序进行删除。当用户再次无意间触发广告应用程序的下载后,智能终端会再次自动下载,再次对用户产生不必要的烦扰。

[0004] 因此,需要提供一种基于智能终端的应用程序监控方法及监控系统,根据用户标记或手动输入,可以通过应用程序黑名单禁止相应应用程序的初次或再次下载,有效减少数据流量的消耗,避免智能终端内存的过度占用,为用户提供一种更好的使用体验。

发明内容

[0005] 为了克服上述技术缺陷,本发明的目的在于提供一种基于智能终端的应用程序监控方法及监控系统,以通过应用程序黑名单,对应用程序的下载进行管制,能够有效防止用户流量数据的消耗,以及内存空间的占用。

[0006] 本发明提供了一种基于智能终端的应用程序监控方法,所述应用程序监控方法包括如下步骤:

[0007] 建立一应用程序黑名单;

[0008] 添加欲监控应用程序至所述应用程序黑名单中;

[0009] 储存所述欲监控应用程序的程序包名称;

[0010] 接收一欲下载应用程序的下载指令;

[0011] 提取所述欲下载应用程序的下载包名称;

[0012] 判断所述下载包名称是否与所述程序包名称匹配;

[0013] 当所述下载包名称与所述程序包名称匹配时,生成一拒绝指令,拒绝下载所述欲下载应用程序。

[0014] 优选地,所述应用程序监控方法,进一步包括:

[0015] 采集包含所述程序包名称的输入信息;

[0016] 生成与所述输入信息对应的禁用字段;

[0017] 将所述禁用字段添加到所述应用程序黑名单中;

[0018] 则,所述应用程序监控方法进一步判断所述下载包字段是否与所述禁用字段匹配;

- [0019] 当所述下载包名称与所述禁用字段匹配时,生成一拒绝指令,拒绝下载所述欲下载应用程序。
- [0020] 优选地,储存所述欲监控应用程序的程序包名称的步骤中,进一步包括:
- [0021] 读取所述程序包名称;
- [0022] 根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;
- [0023] 保存所述程序包字段。
- [0024] 优选地,判断所述下载包名称是否与所述程序包名称匹配的步骤中,进一步包括:
- [0025] 读取与所述下载包名称对应的下载包字段及与所述程序包对应的程序包字段;
- [0026] 计算所述下载包字段与所述程序包字段的匹配程度;
- [0027] 根据所述匹配程度,判断所述下载包名称是否与所述程序包名称匹配;
- [0028] 当所述匹配程度大于等于90%时,判断所述下载包名称与所述程序包名称匹配;
- [0029] 当所述匹配程度小于90%时,判断所述下载包名称与所述程序包名称不匹配。
- [0030] 优选地,所述应用程序监控方法,进一步包括:
- [0031] 将所述欲监控应用程序从所述应用程序黑名单中移除;
- [0032] 移除所述欲监控应用程序后,删除储存的所述程序包名称。
- [0033] 本发明进一步提供了一种基于智能终端的应用程序监控系统,所述应用程序监控系统包括:黑名单模块、添加模块、储存模块、接收模块、提取模块、处理模块和监控模块。
- [0034] 所述黑名单模块,与所述添加模块、处理模块通讯连接,建立一应用程序黑名单;
- [0035] 所述添加模块,与所述黑名单模块、储存模块、处理模块通讯连接,添加欲监控应用程序至所述应用程序黑名单中;
- [0036] 所述储存模块,与所述添加模块、处理模块通讯连接,储存所述欲监控应用程序的程序包名称,并发送所述程序包名称至所述处理模块;
- [0037] 所述接收模块,与所述提取模块通讯连接,接收一欲下载应用程序的下载指令,并发送所述下载指令至所述提取模块;
- [0038] 所述提取模块,与所述接收模块、处理模块通讯连接,提取所述欲下载应用程序的下载包名称,并发送所述下载包名称至所述处理模块;
- [0039] 所述处理模块,与所述储存模块、提取模块、黑名单模块、监控模块通讯连接,判断所述下载包名称是否与所述程序包名称匹配,并发送匹配结果至所述监控模块;
- [0040] 所述监控模块与所述处理模块通讯连接,当所述下载包名称与所述程序包名称匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。
- [0041] 优选地,所述应用程序监控系统进一步包括:采集模块和生成模块;
- [0042] 所述采集模块,与所述生成模块通讯连接,采集包含所述程序包名称的输入信息,并发送所述输入信息至所述生成模块;
- [0043] 所述生成模块,与所述采集模块、添加模块通讯连接,生成与所述输入信息对应的禁用字段,并发送所述禁用字段至所述黑名单模块;
- [0044] 所述添加模块,与所述生成模块、黑名单模块通讯连接,将所述禁用字段添加到所述应用程序黑名单中;
- [0045] 则,所述处理模块,进一步与所述黑名单模块连接,进一步判断所述下载包字段是否与所述禁用字段匹配;

- [0046] 当所述下载包名称与所述禁用字段匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。
- [0047] 优选地,所述储存模块,进一步包括:
- [0048] 名称读取单元,读取所述程序包名称;
- [0049] 字段生成单元,根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;
- [0050] 保存单元,保存所述程序包字段。
- [0051] 优选地,所述处理模块,进一步包括:
- [0052] 字段读取单元,读取所述下载包名称中所包含的下载包字段及所述程序包中所包含的程序包字段;
- [0053] 计算单元,计算所述下载包字段与所述程序包字段的匹配程度;
- [0054] 当所述匹配程度大于等于90%时,判断单元判断所述下载包字段与所述程序包字段匹配;
- [0055] 当所述匹配程度小于90%时,判断单元判断所述下载包字段与所述程序包字段不匹配。
- [0056] 优选地,所述应用程序监控系统,进一步包括:移除模块;
- [0057] 所述移除模块,与所述黑名单模块、储存模块通讯连接;
- [0058] 所述移除模块,将所述欲监控应用程序从所述应用程序黑名单中移除;
- [0059] 移除所述欲监控应用程序后,所述移除模块进一步删除所述储存模块中储存的所述程序包名称。
- [0060] 采用了上述技术方案后,与现有技术相比,具有以下有益效果:
- [0061] 1.添加应用程序黑名单的方式多样化,可通过对已下载或已安装的应用程序的标记,也可以通过手动输入应用程序名称来实现;
- [0062] 2.可以通过应用程序黑名单禁止相应应用程序的初次或再次下载;
- [0063] 3.能够有效减少数据流量的消耗,避免智能终端内存的过度占用;
- [0064] 4.为用户提供一种更好的使用体验。

附图说明

- [0065] 图1为符合本发明实施例中的一种基于智能终端的应用程序监控方法的流程图;
- [0066] 图2为符合本发明另一实施例中的一种基于智能终端的应用程序监控方法的流程图;
- [0067] 图3为符合本发明另一实施例中的一种基于智能终端的应用程序监控方法的流程图;
- [0068] 图4为符合本发明另一实施例中的一种基于智能终端的应用程序监控方法的流程图;
- [0069] 图5为符合本发明实施例中的一种基于智能终端的应用程序监控系统的结构示意图;
- [0070] 图6为符合本发明另一实施例中的一种基于智能终端的应用程序监控系统的结构

示意图；

[0071] 图7为符合本发明另一实施例中的一种基于智能终端的应用程序监控系统的结构示意图；

[0072] 图8为符合本发明另一实施例中的一种基于智能终端的应用程序监控系统的结构示意图；

具体实施方式

[0073] 以下结合附图与具体实施例进一步阐述本发明的优点。

[0074] 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。

[0075] 在本发明的描述中，除非另有规定和限定，对于本领域的普通技术人员而言，可以根据具体情况理解术语的具体含义。

[0076] 在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本发明的说明，其本身并没有特定的意义，仅表示系统的一部分。因此，“模块”与“部件”可以混合地使用。

[0077] 智能终端可以以各种形式来实施。例如，本发明中描述的终端可以包括诸如移动电话、智能电话、笔记本电脑、PDA(个人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、导航装置等等的移动终端以及诸如数字TV、台式计算机等等的固定终端。

[0078] 参阅图1，为符合本发明实施例中的一种基于智能终端的应用程序监控方法的流程图示意图。于本实施例中，应用程序监控方法包括如下步骤：

[0079] 建立一应用程序黑名单；

[0080] 应用程序黑名单，一般用于防止执行不良程序的网络管理实践。加入应用程序黑名单中的应用程序往往包括已知的安全威胁、漏洞以及被认为不适用于特定组织的应用程序。目前，应用程序黑名单是大部分杀毒程序、入侵保护/检测系统和垃圾邮件过滤器使用的方法。本实施例中，通过在智能终端内通过调用函数，建立一个应用程序黑名单，将需要拉黑的应用程序添加入该黑名单中，以实现对被拉黑的应用程序的监控，以防智能终端对该类应用程序的自动下载。

[0081] 添加欲监控应用程序至所述应用程序黑名单中；

[0082] 欲监控应用程序可以为用户不同意下载的应用程序，具体包括两种：未下载的应用程序以及已下载的应用程序。未下载的应用程序为智能终端未从FTP服务器拷贝到内存中的应用程序，例如，用户从未通过智能终端下载的应用程序。已下载的应用程序可以为用户通过第三方平台自行选择下载并安装于智能终端中的应用程序，但之后又被用户从智能终端中删除。例如，用户从第三方平台自行选择下载并安装了一游戏应用程序，但之后为防止沉迷于游戏，又将该游戏应用程序从智能终端中删除。已下载的应用程序也可以为第三方平台未经用户同意自行选择下载的应用程序。例如，当用户浏览网页时，不经意的情况下触发了广告推广应用程序的下载。上述两种应用程序皆可作为欲监控应用程序，均可作为用户添加至应用程序黑名单，并对其实施监控的对象。

[0083] 储存所述欲监控应用程序的程序包名称；

[0084] 当用户将欲监控应用程序添加到应用程序黑名单之后，智能终端进一步提取该欲监控应用程序的安装程序包所包含的程序包名称。提取该程序包名称后，进一步将该程序包名称转化为程序包字段，并将该程序包字段保存，以作为应用程序黑名单对应用程序下载监控的判断依据。

[0085] 接收下载一欲下载应用程序的下载指令；

[0086] 下载指令包括用户无意触发下载广告应用程序而产生的下载指令，也包括用户自行通过第三方应用平台下载应用程序而产生的下载指令。当用户触发下载广告应用程序的下载或点击第三方应用平台上的应用程序的下载按钮后，智能终端会接收到一下载欲下载应用程序的下载指令，该下载指令控制智能终端通过下载链接从FTP服务器拷贝应用程序到智能终端中。

[0087] 提取所述欲下载应用程序的下载包名称；

[0088] 当接收到下载欲下载应用程序的下载指令后，进一步地，根据下载指令所获得的下载链接提取欲下载应用程序的下载包名称，并根据该下载包名称生成下载包字段，以作为后续判断该欲下载应用程序是否为应用程序黑名单中的欲监控应用程序的判断依据。

[0089] 判断所述下载包名称是否与所述程序包名称匹配；

[0090] 智能终端根据储存于智能终端内存中的程序包名称与提取所得的欲下载应用程序的下载包名称对应的程序包字段与下载包名称对应的下载包字段进行匹配，并根据匹配结果判断下载包字段对应的欲下载应用程序是否为应用程序黑名单中所添加的欲监控应用程序。

[0091] 当所述下载包名称与所述程序包名称匹配时，生成一拒绝指令，拒绝下载所述欲下载应用程序。

[0092] 当智能终端对程序包名称对应的程序包字段与下载包名称对应的下载包字段进行匹配，并判断二者相匹配时，即，智能终端根据该匹配结果判断该欲下载应用程序为应用程序黑名单中所添加的欲监控应用程序，则智能终端根据这一匹配结果自动生成一拒绝指令，拒绝智能终端根据下载指令下载该欲下载应用程序。

[0093] 参阅图2，为符合本发明另一优选实施例的一种基于智能终端的应用程序监控方法流程示意图。在本实施例中，所述应用程序监控方法，进一步包括：

[0094] 采集包含所述程序包名称的输入信息；

[0095] 本实施例中的欲监控应用程序也可以包括用户未通过智能终端下载的应用程序。对于这一类的应用程序，用户若是希望预防智能终端通过网络广告链接自动下载或是防止自己下载诸如一些带有赌博性质的游戏程序，用户也可以进一步通过键盘在智能终端中手动输入包含该类欲监控应用程序的程序包名称，以此，可以进一步拓宽智能终端对应用程序的监控范围。

[0096] 生成与所述输入信息对应的禁用字段；

[0097] 待用户通过智能终端键盘手动输入包含欲监控应用程序程序包名称的输入信息后，智能终端接收到该输入信息，根据该输入信息自动生成与之对应的禁用字段，作为智能终端识别欲监控应用程序的判断依据。

[0098] 将所述禁用字段添加到所述应用程序黑名单中；

[0099] 生成与输入信息对应的禁用字段后,智能终端进一步将禁用字段保存于应用程序黑名单中,以此作为智能终端后续判断欲下载应用程序是否属于应用程序黑名单中的欲监控应用程序的依据。

[0100] 则,所述应用程序监控方法进一步判断所述下载包字段是否与所述禁用字段匹配;

[0101] 则,智能终端收到下载一欲下载应用程序的下载指令后,进一步将该欲下载应用程序的下载包字段与用户预先输入的禁用字段进行匹配,以此进一步判断该欲下载应用程序是否为欲监控应用程序。

[0102] 当所述下载包名称与所述禁用字段匹配时,生成一拒绝指令,拒绝下载所述欲下载应用程序。

[0103] 当判断下载包名称与禁用字段匹配时,则,该欲下载应用程序为欲监控应用程序,智能终端根据该匹配结果,进一步生成一拒绝指令,拒绝智能终端执行对该欲下载应用程序的下载操作,从而实现对欲监控应用程序的监管。

[0104] 参阅图3,为符合本发明实施例中的一种基于智能终端的应用程序监控方法的流程示意图。本实施例中,储存所述欲监控应用程序的程序包名称的步骤中,进一步包括:

[0105] 读取所述程序包名称;

[0106] 根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;

[0107] 保存所述程序包字段。当欲监控应用程序为一智能终端已下载的应用程序时,待被标记添加至应用程序黑名单之后,进一步地,智能终端向该欲监控应用程序的程序包发出一读取权限请求,获得读取权限请求后,读取该欲监控应用程序的程序包名称。例如,读取一欲监控应用程序B的程序包名称“应用程序B”,读取完成后,进一步生成一与该“应用程序B”对应的字段,即为程序包字段,作为后续智能终端判断欲下载应用程序是否为欲监控应用程序的依据。

[0108] 参阅图4,为符合本发明实施例中的一种基于智能终端的应用程序监控方法的流程示意图。本实施例中,判断所述下载包名称是否与所述程序包名称匹配的步骤中,进一步包括:

[0109] 读取所述下载包名称中所包含的下载包字段及所述程序包中所包含的程序包字段;

[0110] 计算所述下载包字段与所述程序包字段的匹配程度;

[0111] 当所述匹配程度大于等于90%时,判断所述下载包字段与所述程序包字段匹配;

[0112] 当所述匹配程度小于90%时,判断所述下载包字段与所述程序包字段不匹配。

[0113] 智能终端基于字段的匹配程度来判断下载包名称是否与应用程序黑名单中的程序包名称匹配。完成对下载包字段和程序包字段的读取后,进一步调用函数,计算读取所得的下载包字段和程序包字段的匹配程度。当计算所得的匹配程度大于等于90%时,则判断下载包字段与程序包字段匹配,即下载包字段对应的欲下载应用程序为应用程序黑名单中添加的欲监控应用程序。相反,若计算所得的匹配程度小于90%,则判断下载包字段与程序包字段不匹配,即下载包字段对应的欲下载应用程序不是应用程序黑名单中所添加的欲监控应用程序。

[0114] 在一优选实施例中,所述应用程序监控方法,进一步包括:

[0115] 将所述欲监控应用程序从所述应用程序黑名单中移除；

[0116] 移除所述欲监控应用程序后，删除储存的所述程序包名称。

[0117] 若用户无需再对已添加至应用程序黑名单中的欲监控应用程序作监控，本实施例中的一种基于智能终端的应用程序监控方法进一步包括将应用程序黑名单中的欲监控应用程序移除操作。例如，用户原本通过应用程序黑名单监控一游戏应用程序的下载，防止沉迷于游戏，浪费过多时间，但之后用户又想再次下载并安装该游戏应用程序，需要首先将该游戏应用程序从应用黑名单的监控列表中移除，以此，应用程序黑名单终止对该游戏应用程序的监控。移除该游戏应用程序后，基于应用程序黑名单无需再对该应用程序的下载进行监控，故，智能终端会进一步删除储存的该应用程序的程序包名称。

[0118] 参阅图5，为符合本发明实施例中的一种基于智能终端的应用程序监控系统的结构示意图。于本实施例中，应用程序监控系统包括：黑名单模块、添加模块、储存模块、接收模块、提取模块、处理模块和监控模块。

[0119] 所述黑名单模块，与所述添加模块通讯连接，建立一应用程序黑名单；黑名单模块，与添加模块通讯连接。于黑名单模块中建立一应用程序黑名单，添加模块通过通讯连接可以于黑名单模块中的应用程序黑名单中添加欲监控应用程序（需要被拉黑的应用程序）。应用程序黑名单，一般用于防止执行不良程序的网络管理实践。加入应用程序黑名单中的应用程序往往包括已知的安全威胁、漏洞以及被认为不适用于特定组织的应用程序。

[0120] 目前，应用程序黑名单是大部分杀毒程序、入侵保护/检测系统和垃圾邮件过滤器使用的方法。本实施例中，通过在黑名单模块内通过调用函数，建立一个应用程序黑名单，将需要拉黑的应用程序添加入该应用程序黑名单中，以实现对被拉黑的应用程序的监控，以防智能终端对该类应用程序的自动下载。

[0121] 所述添加模块，与所述黑名单模块、储存模块通讯连接，添加欲监控应用程序至所述应用程序黑名单中；添加模块，通过通讯连接将欲监控应用程序添加至黑名单模块中的应用程序黑名单中。欲监控应用程序可以为用户不同意下载的应用程序，具体包括两种：未下载的应用程序以及已下载的应用程序。未下载的应用程序为智能终端未从FTP服务器拷贝到内存中的应用程序，例如，用户从未通过智能终端下载的应用程序。已下载的应用程序可以为用户通过第三方平台自行选择下载并安装于智能终端中的应用程序，但之后又被用户从智能终端中删除。例如，用户从第三方平台自行选择下载并安装了一游戏应用程序，但之后为防止沉迷于游戏，又将该游戏应用程序从智能终端中删除。已下载的应用程序也可以为第三方平台未经用户同意自行选择下载的应用程序。例如，当用户浏览网页时，不经意的情况下触发了广告推广应用程序的下载。上述两种应用程序皆可作为欲监控应用程序，均可作为用户添加至应用程序黑名单，并对其实施监控的对象。添加模块通过通讯连接将该欲监控应用程序添加到黑名单模块中后，进一步通过通讯连接将该欲监控应用程序的程序包名称发送到储存模块中储存。

[0122] 所述储存模块，与所述添加模块、处理模块通讯连接，储存所述欲监控应用程序的程序包名称，并发送所述程序包名称至所述处理模块；通过添加模块将欲监控应用程序添加到黑名单模块中的应用程序黑名单之后，添加模块进一步通过通讯连接发送欲监控应用程序的安装包至储存模块中，储存模块提取该欲监控应用程序的安装程序包所包含的程序包名称。提取该程序包名称后，进一步将该程序包名称转化为程序包字段，并将该程序包字

段保存,以作为处理模块对应用程序下载监控的判断依据。

[0123] 所述接收模块,与所述提取模块通讯连接,接收一欲下载应用程序的下载指令,并发送所述下载指令至所述提取模块;接收模块接收到一由用户触发的下载指令,该下载指令包括用户无意触发下载广告应用程序而产生的下载指令,也包括用户自行通过第三方应用平台下载应用程序而产生的下载指令。当用户触发下载广告应用程序的下载或点击第三方应用平台上的应用程序的下载按钮后,接收模块会接收到一下载欲下载应用程序的下载指令,该下载指令控制智能终端通过下载链接从FTP服务器将欲下载应用程序拷贝到智能终端中。接收模块接收到下载指令后,进一步通过通讯连接将下载指令发送到提取模块中。

[0124] 所述提取模块,与所述接收模块、处理模块通讯连接,提取所述欲下载应用程序的下载包名称,并发送所述下载包名称至所述处理模块;当提取模块通过通讯连接接收到下载欲下载应用程序的下载指令后,进一步地,根据下载指令所获得的下载链接提取到欲下载应用程序的下载包名称,并根据该下载包名称生成下载包字段。提取完成后,提取模块进一步通过通讯连接将提取所得的下载包字段发送至处理模块中,以作为后续处理模块判断该欲下载应用程序是否为黑名单模块中的欲监控应用程序的判断依据。

[0125] 所述处理模块,与所述储存模块、提取模块、黑名单模块、监控模块通讯连接,判断所述下载包名称是否与所述程序包名称匹配,并发送匹配结果至所述监控模块;

[0126] 处理模块根据储存模块的程序包名称与提取模块提取所得的欲下载应用程序的下载包名称对应的程序包字段与下载包字段进行匹配,并根据匹配结果输出下载包字段对应的欲下载应用程序是否为黑名单模块中的应用程序黑名单中所添加的欲监控应用程序。匹配完成后,处理模块进一步通过通讯连接,将匹配结果发送至监控模块中。

[0127] 所述监控模块与所述处理模块通讯连接,当所述下载包名称与所述程序包名称匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。监控模块与处理模块通讯连接,根据处理模块发送的匹配结果判断是否执行下载指令下载欲下载应用程序。当处理模块对程序包名称对应的程序包字段与下载包名称对应的下载包字段进行匹配,并判断二者相匹配时,即,监控模块根据该匹配结果判断该欲下载应用程序为应用程序黑名单中所添加的欲监控应用程序,则监控模块根据这一匹配结果自动生成一拒绝指令,拒绝执行下载指令对该欲下载应用程序的下载操作。

[0128] 参阅图6,为符合本发明另一优选实施例的一种基于智能终端的应用程序监控系统的结构示意图。在本实施例中,应用程序监控系统进一步包括:采集模块和生成模块。

[0129] 所述采集模块,与所述生成模块通讯连接,采集包含所述程序包名称的输入信息,并发送所述输入信息至所述生成模块;

[0130] 本实施例中的欲监控应用程序也可以包括用户未通过智能终端下载的应用程序。对于这一类的应用程序,用户若是希望预防智能终端通过网络广告链接自动下载或是防止自己下载诸如一些带有赌博性质的游戏程序,用户也可以进一步通过键盘在中手动输入包含该类欲监控应用程序的程序包名称,以此,可以进一步拓宽智能终端对应用程序的监控范围。用户输入完成后,采集模块进一步将采集所得的输入信息通过通讯连接发送到生成模块中。

[0131] 所述生成模块,与所述采集模块、添加模块通讯连接,生成与所述输入信息对应的禁用字段,并发送所述禁用字段至所述黑名单模块;

[0132] 待采集模块采集到用户通过智能终端键盘手动输入包含欲监控应用程序程序包名称的输入信息后,进一步通过通讯连接发送该输入信息至生成模块,生成模块根据该输入信息自动生成与之对应的禁用字段,并通过通讯连接发送至添加模块,通过添加模块实现在应用程序黑名单中添加禁用字段作为判断欲监控应用程序依据的操作。

[0133] 所述添加模块,与所述生成模块、黑名单模块通讯连接,将所述禁用字段添加到所述应用程序黑名单中;

[0134] 生成模块生成与输入信息对应的禁用字段后,添加模块进一步将禁用字段添加至应用程序黑名单中,以此作为智能终端后续判断欲下载应用程序是否属于应用程序黑名单中的欲监控应用程序的依据。

[0135] 则,所述处理模块,进一步与所述黑名单模块连接,进一步判断所述下载包字段是否与所述禁用字段匹配;

[0136] 则,处理模块待接收模块收到下载一欲下载应用程序的下载指令后,进一步与黑名单模块通讯连接,将该欲下载应用程序的下载包字段与用户预先输入的禁用字段进行匹配,以此进一步判断该欲下载应用程序是否为欲监控应用程序。

[0137] 当所述下载包名称与所述禁用字段匹配时,所述监控模块生成一拒绝指令,拒绝下载所述欲下载应用程序。

[0138] 当处理模块判断下载包名称与禁用字段匹配时,则,判断该欲下载应用程序为欲监控应用程序,监控模块根据该匹配结果,进一步生成一拒绝指令,拒绝执行对该欲下载应用程序的下载操作,从而实现对欲监控应用程序的监管。

[0139] 参阅图7,为符合本发明实施例中的一种基于智能终端的应用程序监控系统的结构示意图。本实施例中,优选地,所述储存模块,进一步包括:

[0140] 名称读取单元,读取所述程序包名称;

[0141] 字段生成单元,根据所述程序包名称,生成一与所述程序包名称对应的程序包字段;

[0142] 保存单元,保存所述程序包字段。

[0143] 本实施例中的欲监控应用程序为已下载的应用程序时,待通过添加模块通过标记将欲监控应用程序添加至黑名单模块中后,进一步地,储存模块向该欲监控应用程序的程序包发出一读取权限请求,获得读取权限请求后,储存模块中的读取单元读取该欲监控应用程序的程序包名称,进一步地,字段生成单元根据读取单元读取所得的程序包名称,生成一与该程序包名称对应的程序包字段,并保存于保存单元中,以作为后续处理模块判断欲下载程序是否为欲监管程序的依据。例如,一欲监控应用程序的程序包名称为“应用程序B”,则名称读取单元读取该欲监控应用程序的程序包名称,名称生成单元进一步根据该读取所得名称生成与之相应的程序包字段,并保存于储存单元中。

[0144] 参阅图8,为符合本发明实施例中的一种基于智能终端的应用程序监控系统的结构示意图。本实施例中,所述处理模块,进一步包括:

[0145] 字段读取单元,读取所述下载包名称中所包含的下载包字段及所述程序包中所包含的程序包字段;

[0146] 计算单元,计算所述下载包字段与所述程序包字段的匹配程度;

[0147] 当所述匹配程度大于等于90%时,判断单元判断所述下载包字段与所述程序包字

段匹配；

[0148] 当所述匹配程度小于90%时，判断单元判断所述下载包字段与所述程序包字段不匹配。

[0149] 处理模块基于字段的匹配程度来判断下载包名称是否与储存模块中的程序包名称匹配。处理模块中的字段读取单元对储存模块中的下载包字段和程序包字段的读取后，计算单元进一步调用函数，计算读取所得的下载包字段和程序包字段的匹配程度。当计算单元计算所得的匹配程度大于等于90%时，判断单元判断下载包字段与程序包字段匹配，即下载包字段对应的欲下载应用程序为应用程序黑名单中添加的欲监控应用程序。相反，若计算单元计算所得的匹配程度小于90%，则判断单元判断下载包字段与程序包字段不匹配，即下载包字段对应的欲下载应用程序不是应用程序黑名单中所添加的欲监控应用程序。

[0150] 在一优选实施例中，所述应用程序监控系统，进一步包括：移除模块；

[0151] 所述移除模块，与所述黑名单模块、储存模块通讯连接；

[0152] 所述移除模块，将所述欲监控应用程序从所述应用程序黑名单中移除；

[0153] 移除所述欲监控应用程序后，所述移除模块进一步删除所述储存模块中储存的所述程序包名称。

[0154] 若用户无需再对已添加至应用程序黑名单中的欲监控应用程序作监控，本实施例中的一种基于智能终端的应用程序监控系统进一步包括一移除模块，与黑名单模块、储存模块通讯连接，将应用程序黑名单中的欲监控应用程序移除操作。例如，用户原本通过黑名单模块中的应用程序黑名单监控一游戏应用程序的下载，防止沉迷于游戏，浪费过多时间，但之后用户又想再次下载并安装该游戏应用程序，需要首先通过移除模块将该游戏应用程序从应用黑名单的监控列表中移除，以此，黑名单模块终止对该游戏应用程序的监控。移除模块移除该游戏应用程序后，基于监控模块无需再对该应用程序的下载进行监控，故，移除模块会进一步删除储存的该应用程序的程序包名称。

[0155] 采用本发明提供的应用程序监控方法和监控系统，可通过对已下载或已安装的应用程序的标记，和手动输入应用程序名称来实现对应用程序的监控；此外，可以通过本发明中的应用程序黑名单能够有效禁止相应应用程序的初次或再次下载，既能有效减少数据流量的消耗，避免智能终端内存的过度占用，为用户提供一种更好的使用体验。

[0156] 应当注意的是，本发明的实施例有较佳的实施性，且并非对本发明作任何形式的限制，任何熟悉该领域的技术人员可能利用上述揭示的技术内容变更或修饰为等同的有效实施例，但凡未脱离本发明技术方案的内容，依据本发明的技术实质对以上实施例所作的任何修改或等同变化及修饰，均仍属于本发明技术方案的范围。

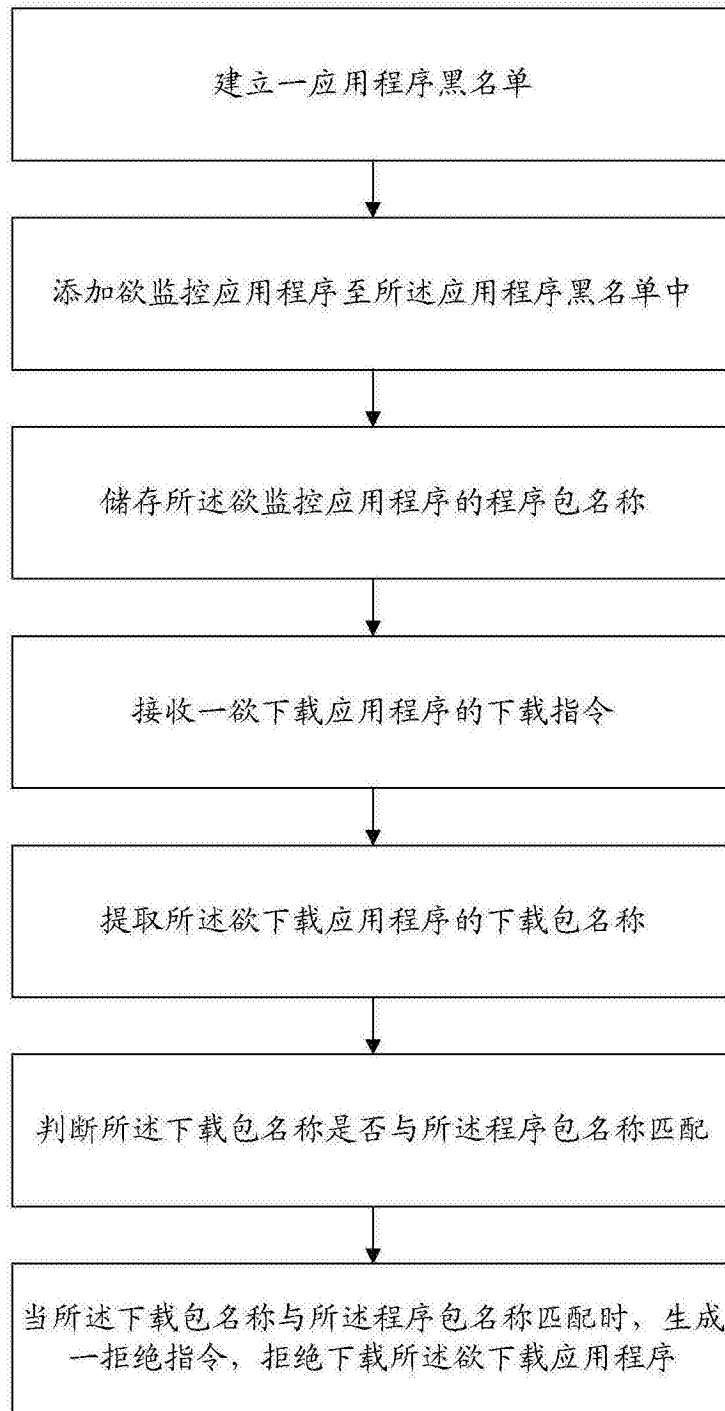


图1

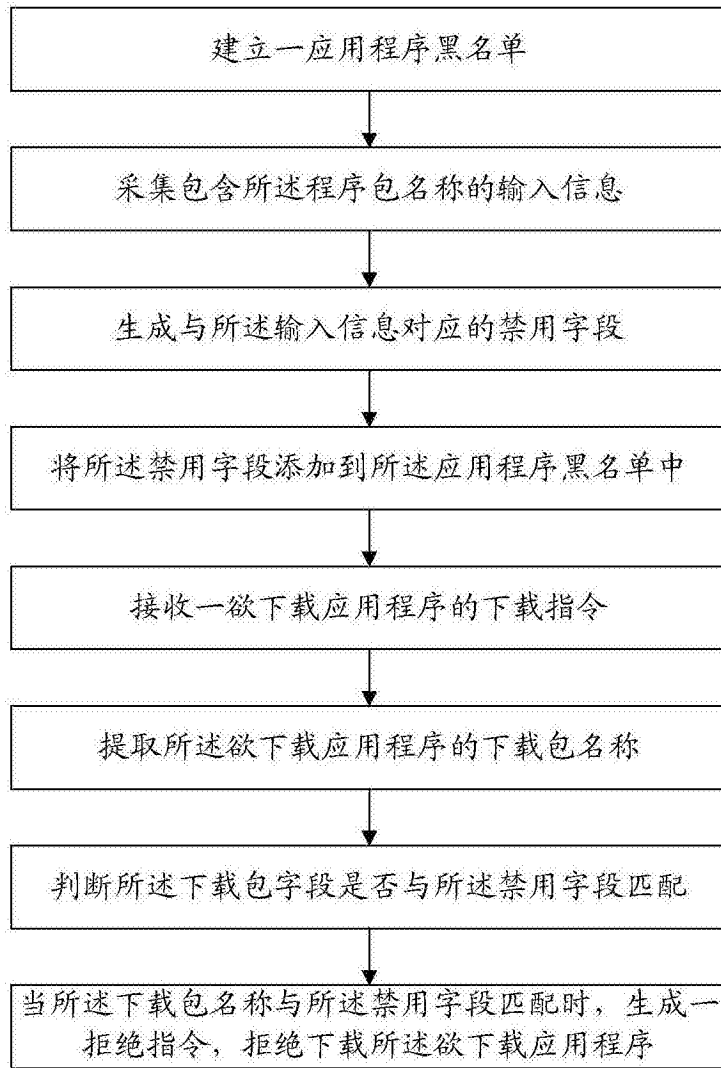


图2

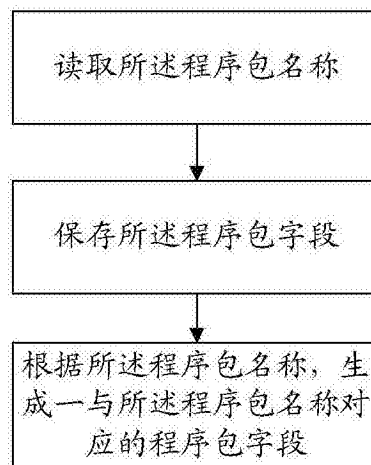


图3

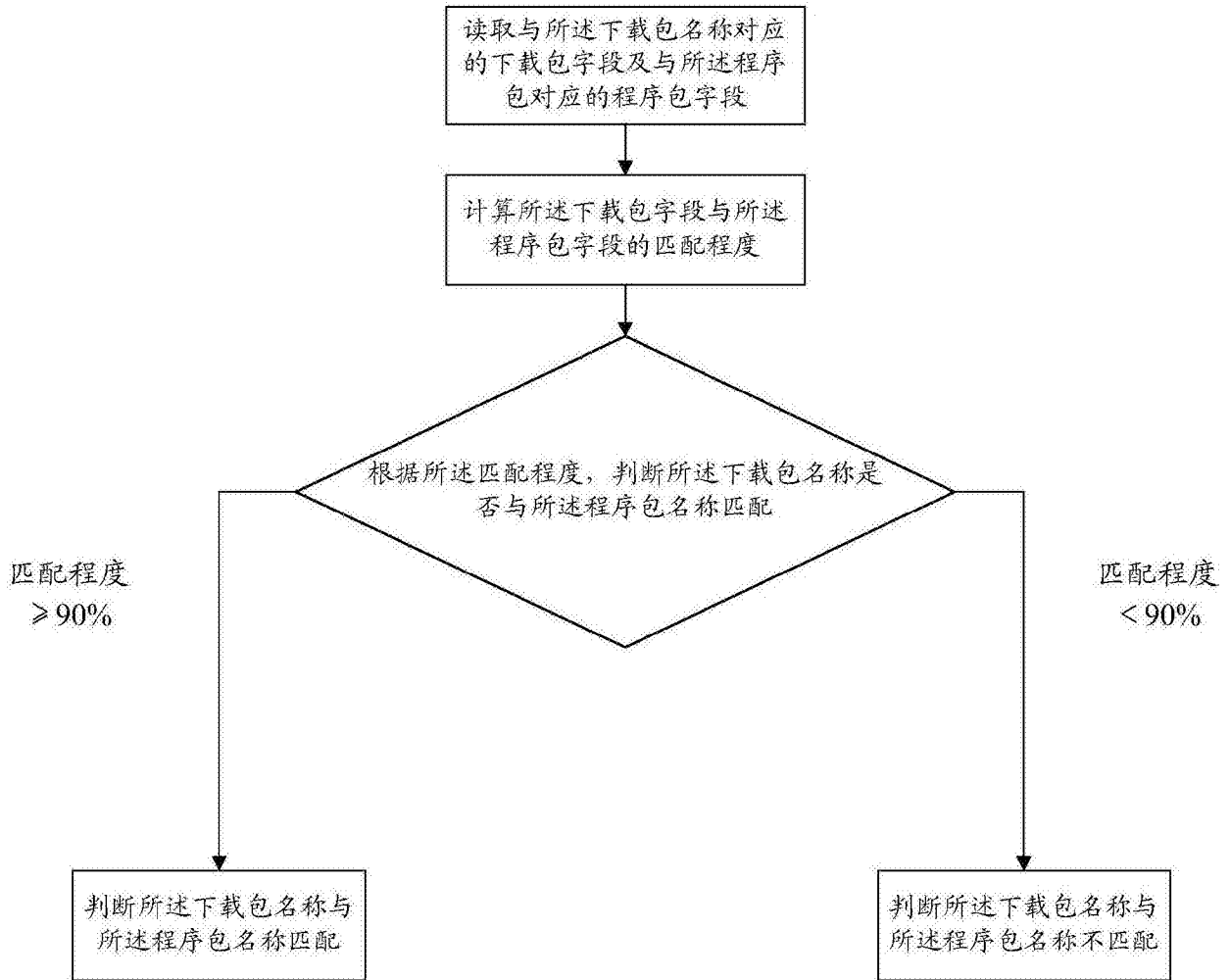


图4

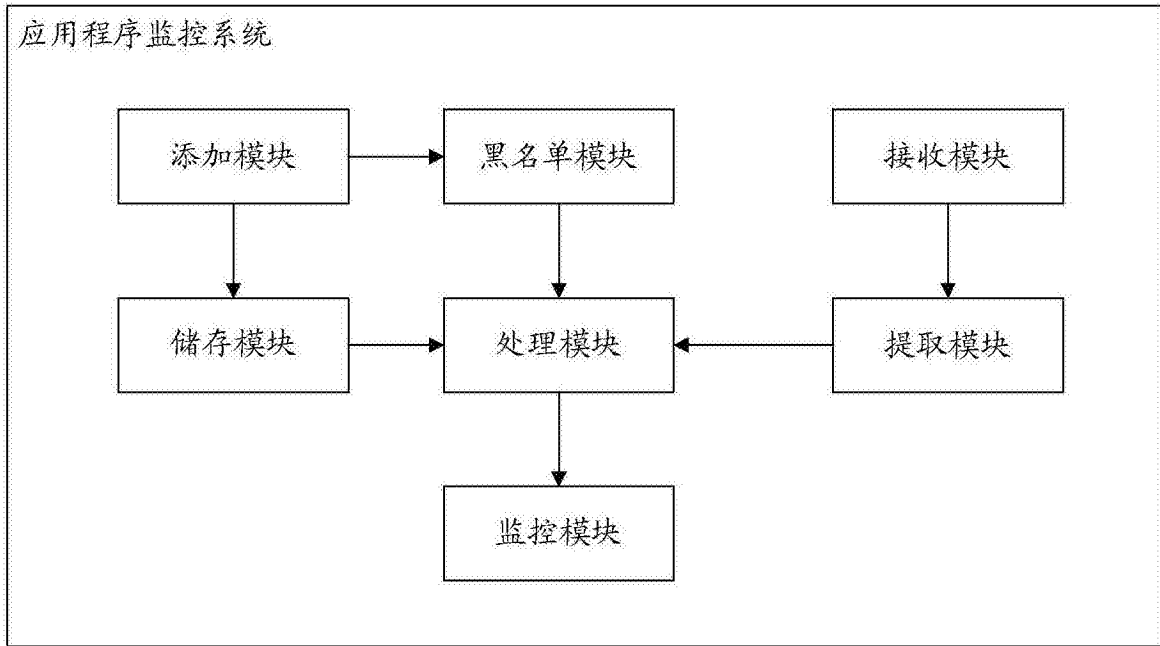


图5

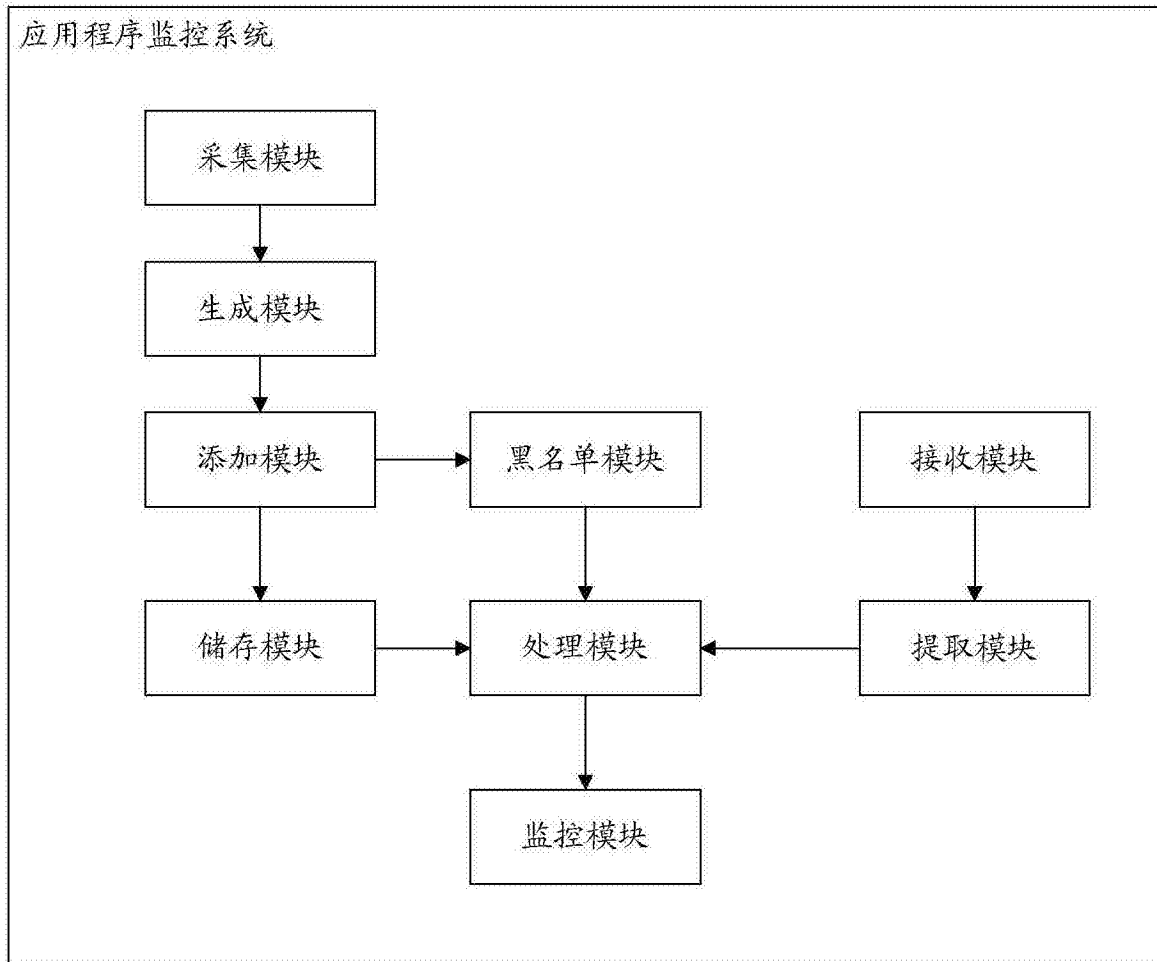


图6

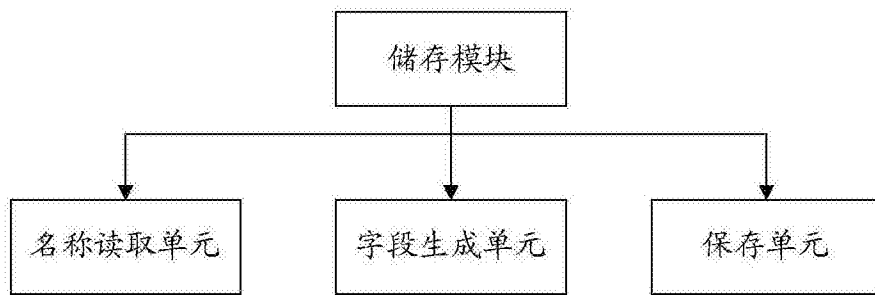


图7

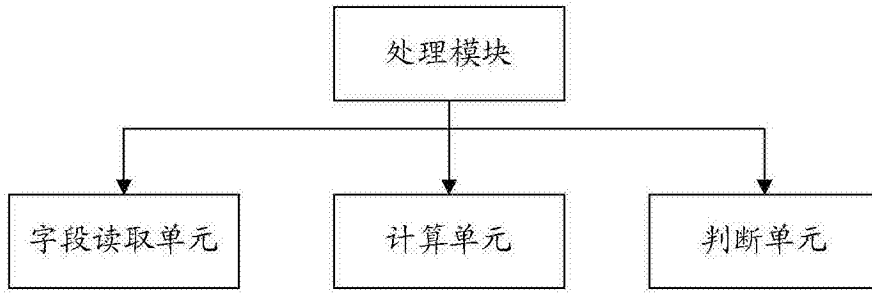


图8