

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2015 年 11 月 12 日 (12.11.2015)



WIPO | PCT



(10) 国际公布号
WO 2015/169158 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2015/077527
- (22) 国际申请日: 2015 年 4 月 27 日 (27.04.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410195546.7 2014 年 5 月 9 日 (09.05.2014) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 邱慧 (QIU, Hui); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。钟明

(ZHONG, Ming); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。张华涛 (ZHANG, Huatao); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) Title: INFORMATION PROTECTION METHOD AND SYSTEM

(54) 发明名称: 信息保护的方法和系统

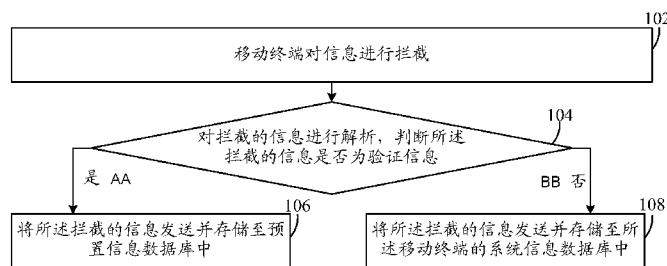


图 1 / FIG. 1

102 INTERCEPTING INFORMATION BY A MOBILE TERMINAL
104 PARSING THE INTERCEPTED INFORMATION, AND JUDGING WHETHER THE INTERCEPTED INFORMATION IS VERIFICATION INFORMATION
106 SENDING THE INTERCEPTED INFORMATION AND STORING SAME IN A PRE-SET INFORMATION DATABASE
108 SENDING THE INTERCEPTED INFORMATION AND STORING SAME IN A SYSTEM INFORMATION DATABASE OF THE MOBILE TERMINAL
AA YES
BB NO

(57) Abstract: Provided are an information protection method and system. The method comprises: intercepting information by a mobile terminal; and parsing the intercepted information, and judging whether the intercepted information is verification information; if the intercepted information is verification information, sending the intercepted information and storing same in a pre-set information database; otherwise, sending the intercepted information and storing same in a system information database of the mobile terminal. The present invention solves the problem of how to protect information in a mobile terminal to ensure the security and reliability of information in an application in the mobile terminal, especially a payment application.

(57) 摘要: 本发明提供了一种信息保护的方法和系统, 其中, 所述方法包括: 移动终端对信息进行拦截; 并, 对拦截的信息进行解析, 判断所述拦截的信息是否为验证信息; 若所述拦截的信息是验证信息, 则将所述拦截的信息发送并存储至预置信息数据库中; 否则, 将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。本发明解决了如何对移动终端中的信息进行保护, 以确保移动终端中的应用尤其是支付应用中, 信息的安全性和可靠性的问题。

WO 2015/169158 A1



RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,

CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

信息保护的方法和系统

技术领域

本发明涉及通信技术领域，具体涉及一种移动终端的信息保护的方法和系统。

5 背景技术

随着移动终端技术的发展，日益繁多的第三方应用在移动终端上被使用。其中，一些恶意软件肆意读取用户在移动终端上存储的信息，并对移动终端上存储的信息进行恶意拦截、篡改，严重影响了移动终端上存储的信息的安全性和可靠性，用户的隐私和安全受到威胁。

10 以移动支付为例，移动支付是指通过终端密码或者分发短信验证码的方式来完成支付过程，确保支付安全的一种技术。如，在银行网银支付时，银行会向用户的手机发送短信验证码，用户除了要输入支付密码外还要输入短信中的验证码，才能完成支付过程。

在传统的移动支付中，用户是在 PC（Personal Computer，个人计算机）
15 端登陆支付页面，在移动终端（如，手机）获取验证码短信，根据移动终端接收到验证码短信中的验证码完成支付过程。由于 PC 端和移动终端具有不同信道、不同通讯方式，保证了数据的独立性，进而保证了移动支付过程的安全性。

然而，随着移动通信技术的发展，越来越多的支付过程是通过安装在移动终端上的第三方应用发出的，使得支付应用和系统短信应用均使用移动终端这同一载体，数据不再具有独立性。系统短信应用中的验证码短信内容可以轻易地被一些恶意第三方应用读取、截获甚至篡改。因此，验证码短信内容中的验证信息不再安全可靠，验证码短信失去了验证的意义，进一步导致支付过程存在严重的安全隐患，甚至给用户带来经济损失。

25 因此，目前本领域技术人员要解决的问题是：如何对移动终端中的信息进行保护，以确保移动终端中的应用尤其是支付应用中，信息的安全性和可靠性。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种信息保护的方法和相应的一种信息保护的系统。

依据本发明的一个方面，提供了一种信息保护的方法，包括：移动终端
5 对信息进行拦截；并，

对拦截的信息进行解析，判断所述拦截的信息是否为验证信息；其中，所述验证信息中至少包括：关键字和字符串；

若所述拦截的信息是验证信息，则将所述拦截的信息发送并存储至预置信息数据库中；其中，所述预置信息数据库根据白名单列表，向所述白名单
10 列表中的第三方应用提供所述预置信息数据库中存储的验证信息；

否则，将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中；其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

根据本发明的另一方面，提供了一种信息保护的系统，包括：

第一拦截模块，配置为对信息进行拦截；

15 第一判断模块，配置为对拦截的信息进行解析，判断所述拦截的信息是否为验证信息；其中，所述验证信息中至少包括：关键字和字符串；

第一发送模块，配置为在所述拦截的信息是验证信息时，将所述拦截的信息发送并存储至预置信息数据库中；其中，所述预置信息数据库根据白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储
20 的验证信息；

第二发送模块，配置为在所述拦截的信息不是验证信息时，将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中；其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

根据本发明的又一方面，提供了一种计算机程序，包括计算机可读代码，
25 当所述计算机可读代码在移动终端上运行时，导致所述移动终端执行权利要求书中的任一个所述的信息保护的方法。

根据本发明的再一方面，提供了一种计算机可读介质，其中存储了权利要求书中要求保护的所述计算机程序。

本发明的有益效果为：

本发明提供了一种移动终端的信息保护方法和系统，移动终端对信息进行拦截判断，将满足验证信息标准的信息发送并存储在预置信息数据库中，以替代原有的直接将获取的信息发送并保存在系统信息数据库中的过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息，拒绝其它第三方应用的访问，从而阻止了恶意第三方应用截取到服务器侧发送的信息，进而避免了信息内容被读取、访问和篡改等，保证了信息的安全性和可靠性。

附图说明

10 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 是本发明第一实施例中一种信息保护的方法的流程图；

15 图 2 是本发明第二实施例中一种信息保护的方法的流程图；

图 3 是本发明第三实施例中一种短信保护的方法的流程图；

图 4 是本发明第三实施例中一种判断短信是否为验证短信的方法流程图；

图 5 是本发明第四实施例中一种信息保护的系统的结构框图；

20 图 6 是本发明第五实施例中一种信息保护的系统的结构框图；

图 7 示意性地示出了用于执行根据本发明的信息保护方法的移动终端的结构框图；以及

图 8 示意性地示出了用于保持或者携带实现根据本发明的信息保护方法的程序代码的存储单元。

具体实施方式

25 下面将参照附图更详细地描述本发明公开的示例性实施例。虽然附图中显示了本发明公开的示例性实施例，然而应当理解，可以以各种形式实现本

公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本发明公开的范围完整的传达给本领域的技术人员。

实施例一

5 参照图 1，示出了本发明第一实施例中一种信息保护的方法的流程图。

在本实施例中，所述信息保护的方法，包括：

步骤 102，移动终端对信息进行拦截。

在本实施例中，移动终端在接收到服务器侧发送的信息时，先对所述信息进行拦截，以阻止所述信息直接被系统中的应用读取。

10 步骤 104，对拦截的信息进行解析，判断所述拦截的信息是否为验证信息。

在本实施例中，所述验证信息中至少包括：关键字和字符串。可以通过所述关键字和所述字符串来判断所述拦截的信息是否为验证信息。其中，验证信息可以是在账号登录时用于进行身份验证的信息；或者是在交易支付时用于确认支付的口令信息；或者是在修改个人信息时用于确认修改的凭证信息，或是与此类似的信息等等。

在本实施例中，若所述步骤 104 的判断结果为：所述拦截的信息是验证信息，则执行步骤 106；否则，执行步骤 108。

步骤 106，将所述拦截的信息发送并存储至预置信息数据库中。

20 在本实施例中，所述预置信息数据库可以设置有一接口，所述接口用于接收所述拦截的信息，所述预置信息数据库根据白名单列表，通过所述接口向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证信息。其中，所述白名单列表可以内置于所述预置信息数据库中。

较佳地，所述接口只向设定的第三方应用发送验证信息，即，只有设定的
25 的第三方应用可以从所述预置信息数据库中读取信息。一般地，所述设定的第三方应用是指所述预置信息数据库内置的白名单列表下的应用。且，所述设定的第三方应用与所述预置信息数据库建立信任关系，以使所述设定的第三方应用可以和所述预置信息数据库通过所述接口进行信息交互。

步骤 108, 将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。

一般地, 由于安装在移动终端上第三方应用, 在应用安装时均获得了用户授权, 因此, 所述移动终端的系统信息数据库中的数据信息可以被所有安装在所述移动终端上的第三方应用读取。也就是说, 系统信息数据库可以用于向所有第三方应用提供存储的信息。

综上所述, 本实施例提供了一种移动终端的信息保护的方法, 移动终端可以对信息进行拦截判断, 并将满足验证信息标准的信息发送并存储在预置信息数据库中, 以替代原有的直接将获取的信息发送并保存在系统信息数据库中的过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息, 拒绝其它第三方应用的访问, 因此, 能够阻止恶意第三方应用截取到服务器侧发送的信息, 进而避免了信息内容被读取、访问和篡改等, 保证了信息的安全性和可靠性。

实施例二

参照图 2, 示出了本发明第二实施例中一种信息保护的方法的流程图。在本实施例中, 所述信息保护的方法, 包括:

步骤 202, 移动终端对信息进行拦截。

在本实施例中, 在所述移动终端对信息进行拦截的步骤之前, 可以先使用安全检测软件对信息的安全性进行检测。其中, 所述安全检测软件可以是安装在移动终端上的 360 安全卫士, 本实施例对此不作限制。

首先, 移动终端接收服务器侧发送的信息, 判断所述服务器侧发送的信息是否为骚扰信息、或诈骗信息、或伪基站信息。如, 可以通过 360 安全卫士检测所述服务器侧发送的信息是否是骚扰信息、或诈骗信息、或伪基站信息。

其次, 若所述移动终端通过 360 安全卫士确定服务器侧发送的信息是骚扰信息、或诈骗信息、或伪基站信息, 则拦截所述服务器侧发送的信息。否则, 确定所述服务器侧发送的信息是安全信息。

上述采用安全检测软件对信息的安全性检测属于第一次拦截过程, 拦截

了不安全和骚扰信息，只有通过了安全性检测的信息才可以在移动终端中继续传递。即，在确定所述服务器侧发送的信息是安全信息后，执行上述步骤 202，移动终端对信息进行拦截。其中，步骤 202，移动终端对信息进行拦截属于第二次拦截，多重拦截过程确保了后续用户读取到的信息、或第三方应用接收到的信息、或系统应用接收到的信息的安全性及可靠性。

较佳地，所述移动终端对信息进行拦截包括：所述移动终端按照用于拦截所述信息的应用的级别高于所述系统信息数据库的级别的规则，对所述信息进行拦截。

例如，以使用安卓操作系统的移动终端为例，在使用安卓操作系统的移动终端中，一般地，系统信息数据库的级别高于用户安装的第三方应用的级别，因此，由服务器侧发送的信息直接被发送并存储至所述系统信息数据库中。在本实施例中，则将所述用于拦截所述信息的应用级别设置为高于所述系统信息数据库的级别；故所述用于拦截信息的应用可以先于所述系统信息数据库获取到由服务器侧发送的信息，对信息进行拦截。优选地，可以将用于拦截所述信息的应用的级别设置为最高级别，以确保拦截的有效性。

步骤 204，移动终端对拦截的信息进行解析，判断所述拦截的信息是否为验证信息。

在本实施例中，所述验证信息中至少包括：关键字和字符串。其中，所述关键字可以是设定的关键字，如，“校验码”或“验证码”；所述字符串可以是满足设定标准的字符串，如：连续数字，且所述连续数字的长度大于等于设定长度标准。

这里需要说明的是，所述设定关键字可以根据实际应用情况进行设置，如：所述设定关键字可以是“支付口令”或“短信口令”等。同理，所述满足设定标准的字符串也可以根据实际情况进行设置，如：可以根据实际情况设置所述设定长度标准为 4 个数字长度或者 8 个数字长度；或者所述满足设定标准的字符串也可以是连续的英文字母组合。本实施例对此不作限制。

较佳地，所述步骤 204 可以包括以下子步骤：

子步骤 2042，移动终端对所述拦截的信息进行解析，当确定所述拦截的

信息为非空信息时，获取所述拦截的信息的信息内容。

子步骤 2044，移动终端根据设定拆分规则对信息内容进行拆分，得到多个字符串。

子步骤 2046，移动终端依次提取所述多个字符串进行判断，确定所述拦截的信息是否是验证信息。当任一字符串中包括所述设定关键字和所述满足设定标准的字符串时，确定所述拦截的信息为验证信息。

在本实施例中，若所述步骤 204 的判断结果为：所述拦截的信息是验证信息，则执行步骤 206；否则，执行步骤 220。

步骤 206，移动终端将所述拦截的信息发送并存储至预置信息数据库中。

10 在本实施例中，所述预置信息数据库设置有一接口，且白名单列表设置于所述预置信息数据库内。所述接口用于接收所述拦截的信息，并根据所述预置信息数据库内置的白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证信息。所述接口可以是对传统向外提供访问功能的数据接口进行修改和限制后的接口，也可以是专门设置的、仅用于
15 实现本发明实施例中相关功能的接口。

其中，所述移动终端可以获取通过安全检测的第三方应用的信息，并将所述通过安全检测的第三方应用的信息添加至所述白名单列表中。和/或，所述移动终端从云端获取确定为安全的第三方应用的信息，并将所述确定为安全的第三方应用的信息添加至所述白名单列表中。进而，完成所述预置信息
20 数据库内置的白名单列表的更新。较佳地，所述通过安全检测的第三方应用可以通过安装在移动终端上的安全检测软件检测的应用。

较佳地，在所述步骤 206 之后，执行步骤 208。

步骤 208，移动终端接收第三方应用发送的验证码获取请求。

其中，所述验证码获取请求包括：身份验证信息。所述身份验证信息可
25 以是第三方应用的签名信息。

步骤 210，移动终端根据所述验证码获取请求中的身份验证信息，判断所述第三方应用是否是可信赖应用。

在本实施例中，移动终端根据所述身份验证信息判断所述身份验证信息

指示的第三方应用是否属于所述白名单列表中的第三方应用。当确定所述身份验证信息指示的第三方应用属于所述白名单列表中的第三方应用时，确定所述身份验证信息指示的第三方应用是可信赖应用；并执行步骤 212。否则，执行步骤 214。

- 5 步骤 212，移动终端根据所述验证码获取请求，将所述字符串通过所述接口发送至所述可信赖应用。

可信赖应用可以通过所述预置信息数据库设置的接口对所述预置信息数据库进行访问。其中，可信赖应用在访问所述预置信息数据库时，移动终端要对访问者身份进行验证，只有当可信赖应用通过身份验证后才可以接受
10 到所述由预置信息数据库发送的字符串。

移动终端在向所述可信赖应用发送所述字符串时，先从所述验证信息中提取出所述字符串，然后将所述字符串发送给第三方应用，并将所述字符串填写至所述第三方应用对应的验证位置处。

- 15 在本实施例中，所述移动终端自动完成所述字符串的发送填写流程，避免了人工手动操作中可能出现的输入错误，确保了验证的准确性，提高了验证效率。

移动终端在向所述可信赖应用发送所述字符串时，先从所述验证信息中提取出所述字符串，然后将所述字符串发送给第三方应用，并将所述字符串填写至所述第三方应用对应的验证位置处。

- 20 步骤 214，移动终端不对所述验证码获取请求进行响应。即，移动终端不向第三方应用发送所述字符串。

另一较佳的方案为，在所述步骤 206 之后，执行步骤 216。

步骤 216，移动终端将所述字符串自动添加至系统剪贴板中。

- 25 步骤 218，移动终端接收用户的粘贴请求，将所述字符串添加至对应的第三方应用。

这里需要说明的是，在本实施例中，所述预置信息数据库中可以存储服务器侧发送的确定是安全信息、且确定是验证信息的所有信息。设置在所述预置信息数据库的白名单列表中可以包括所有验证信息对应的第三方应用。

或者，

5 设置在所述预置信息数据库的白名单列表中只包括部分验证信息对应的第三方应用。即，首先确定所有验证信息对应的所有第三方应用，在确定的所有第三方应用的基础上进一步进行筛选，选择支持与所述预置信息数据库进行数据交互的第三方应用。根据经过再次筛选的、支持与所述预置信息数据库进行数据交互的第三方应用，建立所述白名单列表。如，两条验证信息分别对应支付宝应用和京东支付应用；其中，已经确定的是：所述支付宝应用与所述预置信息数据库可以进行数据交互，而所述京东支付应用不支持与所述预置信息数据库进行数据交互。故，所述白名单中只保存支付宝应用而不保存京东支付应用。

当所述预置信息数据库内置的白名单列表的第三方应用与所述预置信息数据库中存储的验证信息对应的第三方应用相匹配时，可以通过上述步骤 208 至步骤 212，通过所述接口自动完成所述字符串的获取。也可以，通过所述步骤 216 和步骤 218，通过手动的粘贴操作完成所述字符串的获取。

15 当所述预置信息数据库内置的白名单列表的第三方应用与所述预置信息数据库中存储的验证信息对应的第三方应用不匹配（即，所述预置信息数据库中存储的验证信息对应的第三方应用与所述预置信息数据库之间没有建立信任关系）时，则通过所述步骤 216 和步骤 218，通过手动的粘贴操作完成所述字符串的获取。

20 步骤 220，移动终端将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

综上所述，本实施例提供了一种移动终端的信息保护的方法，移动终端对信息进行拦截判断，并将满足验证信息标准的信息发送并存储在预置信息数据库中，以替代原有的直接将获取的信息发送并保存在系统信息数据库中的过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息，拒绝其它第三方应用的访问，因此，能够阻止恶意第三方应用截取到服务器侧发送的信息，进而避免了信息内容被读取、访问和篡改等，保证了信

息的安全性和可靠性。

进一步地，本实施例提供的所述信息保护的方法，在移动终端对信息进行拦截之前，先对由服务器侧发送的信息进行第一次拦截，以确保短信不是恶意和骚扰信息。通过多重拦截判断过程，能够提高信息保护的可靠性。

5 同时，在本实施例中，所述字符串可以自动完成发送填写流程，避免了人工手动操作中可能出现的输入错误，确保了信息的准确性，提高了验证效率。也可以自动将所述字符串复制到系统剪贴板上，以使用户快速复制，提高了用户体验，也避免了手动输入发生人为错误的可能。

实施例三

10 结合上述实施例，下面以短信为例来说明所述信息保护的方法的实现流程。在现有的移动支付过程中，除了验证固定的账号的支付密码外，通常还使用动态密码来确保支付过程的安全性，如，以短信形式进行验证码分发，确保支付过程的安全。这里仅是以短信为例来进行说明，需要说明的是，本实施例不仅限于对短信的保护，也可以用于对其它类似信息的保护，如对微
15 信支付信息进行保护。

参照图 3，示出了本发明第三实施例中一种短信保护的方法的流程图。在本实施例中，移动终端中可以安装一个用于实现所述短信保护的方法的短信 APP 应用，该 APP 应用可能是对用户可见，由用户选择使用的应用，也可能是对用户透明的 APP 应用。其中，所述短信 APP 应用可以是一个用于
20 实现所述信息保护方法的独立的 APP 应用，安装在移动终端上；也可以设置在上述安装在移动终端上的安全检测软件中的一个功能应用。

所述短信保护的方法，包括：

步骤 302，短信 APP 应用对短信进行拦截。

25 较佳地，以安卓移动操作系统的动终端为例，可以将所述短信 APP 应用的级别设置为最高级别，故，所述短信 APP 应用可以最先获取到服务器侧发送的短信。

步骤 304，短信 APP 应用对拦截的短信进行解析，判断所述拦截的短信是否为验证短信。

参照图 4，是本实施例中一种判断短信是否为验证短信的方法流程图。
具体判断过程如下：

S41、判断短信内容是否为空。

若为空，则直接结束判断流程，并确定所述拦截的短信不是验证短信。

5 若不为空，则执行 S42。

S42、将短信内容分割成若干个字符串 `strsplit[i]`。

其中，`i` 从 0 开始计数。

较佳地，可以根据句末分割符（如：“，”、“；”、“。”，以及相应的半角符号“，”、“；”、“。”）对短信内容进行分割。

10 S43、判断第 `i` 个字符串 `strsplit[i]` 是否为空。

若为空，则取第 `i++` 个字符串，判断第 `i++` 个字符串是否为空；直至最后一个字符串为止。若不为空，则执行 S44。

S44、判断第 `i` 个字符串是否包含设定关键字。

15 其中，所述设定关键字包括：“校验码”或“验证码”。若包含设定关键字则执行 S45；否则，返回执行 S43。

S45、判断所述第 `i` 个字符串中是否包含满足设定长度的连续数字。

若包含所述满足设定长度的连续数字，则执行 S46；否则，返回执行 S43。

S46、提取 `str` 中第一次出现、且满足设定长度的连续数字。

20 在本实施例中，当确定第 `i` 个字符串中包含设定关键字、且包含满足设定长度的连续数字时，则可以确定所述拦截的短信是验证短信。

较佳地，若所述拦截的短信是验证短信，则执行步骤 306；否则，执行步骤 320。

步骤 306，短信 APP 应用获取所述拦截的短信的发送方信息。

25 步骤 308，短信 APP 应用根据所述发送方信息，判断所述拦截的短信对应的第三方应用是否属于白名单列表中的应用。这里需要说明的是，上述步骤 306 和步骤 308 也可以在步骤 304 之前执行。

较佳地，短信 APP 应用对所述拦截的短信进行分析，获取到发送所述拦截的短信的号码。当所述发送方信息（即，发送所述拦截的短信的号码）

指示的第三方应用属于所述白名单列表中的第三方应用时，执行步骤 310；否则，执行步骤 320。

步骤 310，短信 APP 应用将所述拦截的短信发送并存储至所述预置信息数据库中。

5 其中，所述预置信息数据库设置有接口，所述接口用于接收所述拦截的短信，并根据所述预置信息数据库内置的白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证短信。

10 在本实施例中，只有当所述发送方信息指示的第三方应用属于所述预置信息数据库内置白名单中的第三方应用时；才将所述发送方信息对应发送的短信存储在所述预置信息数据库中，确保了所述预置信息数据库中存储的验证短信对应的第三方应用一定是与所述预置信息数据库建立了信任关系的应用。因此，所述预置信息数据库中的所有验证短信都可以被第三方应用通过所述预置信息数据库中的接口直接获取。

15 如，被拦截的两条短信（如，短信 A 和短信 B）在经过判断之后，确定均是验证短信；进一步获取所述短信 A 和短信 B 的发送方信息，经过分析确定所述短信 A 对应的是支付宝应用，所述短信 B 对应的是京东支付应用。而，所述支付宝应用属于所述预置信息数据库内置白名单数据库中的应用，所述京东支付应用不属于所述白名单数据库中的应用。较佳地，可以将所述短信 A 发送并存储至所述预置信息数据库中，将所述短信 B 发送并存储至系统信息数据库中。

20 这里需要说明的是，在本实施例中，所述支付宝应用属于所述预置信息数据库内置白名单数据库中的应用，故，所述短信 APP 可以直接将所述短信 A 推送给支付宝应用。或者，也可以在接收到支付宝应用发送的验证码获取请求之后，将所述短信 A 发送给支付宝应用；具体流程如下述步骤 312。

25 步骤 312，短信 APP 应用接收第三方应用发送的验证码获取请求。

其中，所述验证码获取请求包括：身份验证信息。

步骤 314，短信 APP 应用根据所述验证码获取请求中的身份验证信息，判断所述第三方应用是否是可信赖应用。

在本实施例中，当短信 APP 应用根据所述身份验证信息确定所述身份验证信息指示的第三方应用属于所述白名单列表中的第三方应用时，确定所述第三方应用是否是可信赖应用，执行步骤 316；否则，执行步骤 318。

5 步骤 316，短信 APP 应用根据所述验证码获取请求，将所述字符串通过所述接口发送至所述可信赖应用。

例如，短信运行商向用户的移动终端发送短信，短信内容为：“校验码 360360，您正在使用支付宝，需要进行校验，【请勿向任何人提供您收到的短信校验码】【支付宝】【95188】。”

10 首先，所述移动终端上的安全检测应用对所述短信进行检测，判断所述短信是否是伪基站短信、或骚扰短信、或诈骗短信。如果是，则直接拦截所述短信并向用户发送提醒通知。

如果不是，短信 APP 应用对所述短信的内容进行分析，较佳地，可以使用句末分隔符将所述短信的内容分割为如下字符串：“校验码 360360”、“您正在使用支付宝，需要进行校验”和“【请勿向任何人提供您收到的短信校验码】【支付宝】【95188】”。由于在第一个字符串“校验码 360360”中包含
15 设定关键字“校验码”，且，包含满足设定长度（设定长度为 4）的连续数字。故，确定所述短信为支付短信。

然后，短信 APP 应用将所述短信保存在所述预置信息数据库中。在短信预览中高亮显示 360360，并添加相应的时间，同时，将 360360 复制到系
20 统剪贴板中。这里需要说明的是，在本实施例中，所述短信中还包括客服号码 95188，还可以提取出所述 95188，并经过识别确定 95188 为支付宝客服电话，故，对 95188 也进行高亮显示，当用户点击高亮部分时，可以直接拨打号码 95188。

最后，短信 APP 应用根据发送所述短信的号码确定所述短信对应的是
25 支付宝应用，且所述支付宝应用是所述预置信息数据库内置白名单列表中的第三方应用。所述支付宝应用将签名信息通过所述预置信息数据库中设置的接口发送至所述预置信息数据库，所述预置信息数据库根据所述签名信息对所述支付宝应用进行验证，当验证通过之后，通过所述接口将保存在所述预

置信息数据库中的短信发送给所述支付宝应用。

步骤 318, 短信 APP 应用不对所述验证码获取请求进行响应。

即, 所述短信 APP 应用不向第三方应用发送所述字符串。

5 步骤 320, 短信 APP 应用将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。

其中, 所述系统信息数据库用于向所有第三方应用提供存储的信息。

综上所述, 本实施例提供了一种移动终端的信息保护的方法, 移动终端对信息进行拦截判断, 并将满足验证信息标准的信息发送并存储在预置信息数据库中, 以替代原有的直接将获取的信息发送并保存在系统信息数据库中的
10 过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息, 拒绝其它第三方应用的访问, 因此, 能够阻止恶意第三方应用截取到服务器侧发送的信息, 进而避免了信息内容被读取、访问和篡改等, 保证了信息的安全性和可靠性。

进一步地, 本实施例所述的方法有效避免手机木马、病毒等恶意软件或
15 恶意第三方应用读取支付验证码短信, 在用户不知情的情况下完成支付, 给用户带来经济损失。

需要说明的是, 对于前述的方法实施例, 为了简单描述, 故将其都表述为一系列的动作组合, 但是本领域技术人员应该知悉, 本发明并不受所描述的动作顺序的限制, 因为依据本发明, 某些步骤可以采用其他顺序或者同时
20 进行。其次, 本领域技术人员也应该知悉, 说明书中所描述的实施例均属于优选实施例, 所涉及的动作并不一定是本发明所必需的。

实施例四

基于与信息保护的方法同一发明构思, 参照图 5, 示出了本发明第四实施例中一种信息保护的系统的结构框图。在本实施例中, 所述信息保护的系
25 统包括:

第一拦截模块 502, 配置为对信息进行拦截。

第一判断模块 504, 配置为对拦截的信息进行解析, 判断所述拦截的信息是否为验证信息。

其中，所述验证信息中至少包括：关键字和字符串。

第一发送模块 506，配置为在所述拦截的信息是验证信息时，将所述拦截的信息发送并存储至预置信息数据库中。

其中，所述预置信息数据库根据白名单列表，向所述白名单列表中的第
5 三方应用提供所述预置信息数据库中存储的验证信息。

第二发送模块 508，配置为在所述拦截的信息不是验证信息时，将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。

其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

综上所述，本实施例提供了一种信息保护的系统，移动终端使用该系对
10 信息进行拦截判断，并将满足验证信息标准的信息发送并存储在预置信息数据库
中，以替代原有的直接将获取的信息发送并保存在系统信息数据库中的过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息，拒绝其它第三方应用的访问，因此，能够阻止恶意第三方应用截取到服务器侧发送的信息，进而避免了信息内容被读取、访问和篡改等，保证了信
15 息的安全性和可靠性。

实施例五

参照图 6，示出了本发明第五实施例中一种信息保护的系统的结构框图。
在本实施例中，所述信息保护的系统包括：

安全判断模块 602，配置为接收服务器侧发送的信息，并判断所述服务
20 器侧发送的信息是否为骚扰信息、或诈骗信息、或伪基站信息。

在本实施例中，当确定所述服务器侧发送的信息是骚扰信息、或诈骗信息、或伪基站信息时，则执行第三拦截模块 604；否则，执行第一拦截模块 606。

第三拦截模块 604，配置为拦截所述服务器侧发送的信息。

25 第一拦截模块 606，配置为对信息进行拦截。

较佳地，所述第一拦截模块 606，具体配置为按照用于拦截所述信息的应用的级别高于所述系统信息数据库的级别的规则，对所述信息进行拦截。
优选地，拦截所述信息的应用的级别可以设置为整个系统中的最高级别。

第一判断模块 608，配置为对拦截的信息进行解析，判断所述拦截的信息是否为验证信息。其中，所述验证信息中至少包括：关键字和字符串。

较佳地，所述第一判断模块 608，包括：

内容获取模块 6082，配置为对所述拦截的信息进行解析，在确定所述拦截的信息为非空信息时，获取所述拦截的信息的信息内容。

拆分模块 6084，配置为根据设定拆分规则对信息内容进行拆分，得到多个字符串。

验证信息确定模块 6086，配置为依次提取所述多个字符串进行判断，在任一字符串中包括设定关键字和满足设定标准的字符串时，确定所述拦截的信息为验证信息。其中，所述设定关键字包括：“校验码”或“验证码”；所述满足设定标准的字符串为连续数字，且所述连续数字的长度大于等于设定长度标准。

在本实施例中，在所述第一判断模块 608 判断确定所述拦截的信息是验证信息时，执行获取模块 610；否则，执行第二发送模块 626。

获取模块 610，配置为获取所述拦截的信息的发送方信息。

在所述发送方信息指示的第三方应用属于所述白名单列表中的第三方应用时，执行第一发送模块 612；否则，执行所述第二发送模块 626。

第一发送模块 612，配置为将所述拦截的信息发送并存储至预置信息数据库中。其中，所述预置信息数据库设置有接口，所述接口用于接收所述拦截的信息，并根据所述预置信息数据库内置的白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证信息。

较佳地，在所述第一发送模块 612 之后，执行接收模块 614。

接收模块 614，配置为接收第三方应用发送的验证码获取请求。

其中，所述验证码获取请求包括：身份验证信息；所述身份验证信息包括：第三方应用的签名信息。

第二判断模块 616，配置为根据所述验证码获取请求中的身份验证信息，判断所述身份验证信息指示的第三方应用是否是可信应用。

在本实施例中，当所述预置信息数据库根据所述身份验证信息确定所述

身份验证信息指示的第三方应用属于所述白名单列表中的第三方应用时，确定所述身份验证信息指示的第三方应用是可信赖应用，并执行第三发送模块 618；否则执行第二拦截模块 620。

5 第三发送模块 618，根据所述验证码获取请求，将所述满足设定标准的字符串通过所述接口发送至所述可信赖应用。

第二拦截模块 620，配置为不对所述验证码获取请求进行响应。

又一较佳地，在所述第一发送模块 612 之后，执行第一添加模块 622。

第一添加模块 622，配置为将所述满足设定标准的字符串自动添加至系统剪贴板中。

10 第二添加模块 624，配置为接收用户的粘贴请求，将所述满足设定标准的字符串添加至对应的第三方应用。

第二发送模块 626，配置为将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中。其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

15 在本实施例中，还可以通过如下模块对所述预置信息数据库中的白名单列表进行更新：

第一应用添加模块 628，配置为获取通过安全检测的第三方应用的信息，并将所述通过安全检测的第三方应用的信息添加至所述白名单列表中。

20 第二应用添加模块 630，配置为从云端获取确定为安全的第三方应用的信息，并将所述确定为安全的第三方应用的信息添加至所述白名单列表中。

较佳地，所述通过安全检测的第三方应用可以是通过安装在移动终端上的安全检测软件检测的应用。

综上所述，本实施例提供了一种信息保护的系统，移动终端使用该系统对信息进行拦截判断，并将满足验证信息标准的信息发送并存储在预置信息数据库中，以替代原有的直接将获取的信息发送并保存在系统信息数据库中的过程。由于预置信息数据库只向白名单列表中的第三方应用提供存储的信息，拒绝其它第三方应用的访问，因此，能够阻止恶意第三方应用截取到服务器侧发送的信息，进而避免了信息内容被读取、访问和篡改等，保证了信

25

息的安全性和可靠性。

进一步地，本实施例所述信息保护的系统，在移动终端对信息进行拦截之前，先对由服务器侧发送的信息进行第一次拦截，以确保短信不是恶性和骚扰信息。多重拦截判断过程，提高了信息保护的可靠性。

5 同时，在本实施例中，所述满足设定标准的字符串可以自动完成发送填写流程，避免了人工手动操作中可能出现的输入错误，确保了信息的准确性，提高了验证效率。也可以自动将所述满足设定标准的字符串复制到系统剪贴板上，以使用户快速复制，提高了用户体验，也避免了手动输入发生人为错误的可能。

10 对于上述一种信息保护的系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，
15 构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未
20 详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的信息保护的设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 7 示出了可以实现根据本发明的信息保护方法的移动终端。该移动终端传统上包括处理器 710 和以存储器 720 形式的计算机程序产品或者计算机可读介质。存储器 720 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 720 具有用于执行上述方法中的任何方法步骤的程序代码 731 的存储空间 730。例

如，用于程序代码的存储空间 730 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 731。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。

- 5 这样的计算机程序产品通常为如参考图 8 所述的便携式或者固定存储单元。该存储单元可以具有与图 7 的移动终端中的存储器 720 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 731'，即可以由例如诸如 710 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器执行上面所描述的方法中的各个步骤。
- 10

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

- 15 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

- 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换
- 20 实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个
- 25 硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

权 利 要 求 书

1、一种信息保护的方法，包括：

移动终端对信息进行拦截；并，

对拦截的信息进行解析，判断所述拦截的信息是否为验证信息；其中，所述验证信息中至少包括：关键字和字符串；

5 若所述拦截的信息是验证信息，则将所述拦截的信息发送并存储至预置信息数据库中；其中，所述预置信息数据库根据白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证信息；

否则，将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中；其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

10 2、如权利要求 1 所述的方法，其中，在将所述拦截的信息发送并存储至预置信息数据库中的步骤之后，所述方法还包括：

接收第三方应用发送的验证码获取请求；其中，所述验证码获取请求包括：身份验证信息；

15 根据所述验证码获取请求中的身份验证信息，判断所述第三方应用是否是可信赖应用；

当所述预置信息数据库根据所述身份验证信息确定所述身份验证信息指示的第三方应用属于所述白名单列表中的第三方应用时，确定所述身份验证信息指示的第三方应用是可信赖应用；并且，根据所述验证码获取请求，将所述字符串通过接口发送至所述可信赖应用；其中，所述接口设置在所述预置信息数据库上，所述接口用于接收所述拦截的信息并向所述可信赖应用发送所述字符串；

20

否则，不对所述验证码获取请求进行响应。

3、如权利要求 1 或 2 所述的方法，其中，在将所述拦截的信息发送至预置信息数据库中的步骤之前，所述方法还包括：

25 获取所述拦截的信息的发送方信息；

当所述发送方信息指示的第三方应用属于所述白名单列表中的第三方应用时，执行所述将所述拦截的信息发送至预置信息数据库中的步骤；

否则，执行所述拦截的信息发送并存储至所述移动终端的系统信息数据

库中的步骤。

4、如权利要求 1 所述的方法，其中，所述移动终端对信息进行拦截，包括：

所述移动终端按照用于拦截所述信息的应用的级别高于所述系统信息数据库的级别的规则，对所述信息进行拦截。

5、如权利要求 1 所述的方法，其中，所述对拦截的信息进行解析，判断所述拦截的信息是否为验证信息，包括：

对所述拦截的信息进行解析，当确定所述拦截的信息为非空信息时，获取所述拦截的信息的信息内容；

10 根据设定拆分规则对信息内容进行拆分，得到多个字符串；

依次提取所述多个字符串进行判断，当任一字符串中包括设定关键字和满足设定标准的字符串时，确定所述拦截的信息为验证信息；

其中，所述设定关键字包括：“校验码”或“验证码”；所述满足设定标准的字符串为连续数字，且所述连续数字的长度大于等于设定长度标准。

15 6、如权利要求 1 所述的方法，其中，在所述将所述拦截的信息发送至预置信息数据库中的步骤之后，所述方法还包括：

将所述字符串自动添加至系统剪贴板中；

接收用户的粘贴请求，将所述字符串添加至对应的第三方应用。

7、如权利要求 1 所述的方法，其中，所述方法还包括：

20 获取通过安全检测的第三方应用的信息，并将所述通过安全检测的第三方应用的信息添加至所述白名单列表中；和/或，

从云端获取确定为安全的第三方应用的信息，并将所述确定为安全的第三方应用的信息添加至所述白名单列表中。

25 8、如权利要求 1 所述的方法，其中，在所述移动终端对信息进行拦截的步骤之前，所述方法还包括：

接收服务器侧发送的信息，并判断所述服务器侧发送的信息是否为骚扰信息、或诈骗信息、或伪基站信息；

当所述服务器侧发送的信息是骚扰信息、或诈骗信息、或伪基站信息时，

拦截所述服务器侧发送的信息；

否则，确定所述服务器侧发送的信息是安全信息，并执行所述移动终端对信息进行拦截的步骤。

9、如权利要求 2 所述的方法，其中，所述身份验证信息包括：第三方
5 应用的签名信息。

10、一种信息保护的系统，包括：

第一拦截模块，配置为对信息进行拦截；

10 第一判断模块，配置为对拦截的信息进行解析，判断所述拦截的信息是否
否为验证信息；其中，所述验证信息中至少包括：关键字和字符串；

第一发送模块，配置为在所述拦截的信息是验证信息时，将所述拦截的信息发送并存储至预置信息数据库中；其中，所述预置信息数据库根据白名单列表，向所述白名单列表中的第三方应用提供所述预置信息数据库中存储的验证信息；

15 第二发送模块，配置为在所述拦截的信息不是验证信息时，将所述拦截的信息发送并存储至所述移动终端的系统信息数据库中；其中，所述系统信息数据库用于向所有第三方应用提供存储的信息。

11、如权利要求 10 所述的系统，其中，所述系统还包括：

20 接收模块，配置为在所述第一发送模块将所述拦截的信息发送并存储至预置信息数据库之后，接收第三方应用发送的验证码获取请求；其中，所述验证码获取请求包括：身份验证信息；

第二判断模块，配置为根据所述验证码获取请求中的身份验证信息，判断所述身份验证信息指示的第三方应用是否是可信应用；

25 第三发送模块，配置为在所述预置信息数据库根据所述身份验证信息确定所述身份验证信息指示的第三方应用属于所述白名单列表中的第三方应用时，确定所述身份验证信息指示的第三方应用是可信应用；并且，根据所述验证码获取请求，将所述字符串通过接口发送至所述可信应用；其中，所述接口设置在所述预置信息数据库上，所述接口用于接收所述拦截的信息

并向所述可信应用发送所述字符串；

第二拦截模块，配置为在所述预置信息数据库根据所述身份验证信息确定所述身份验证信息指示的第三方应用不属于所述白名单列表中的第三方应用时，不对所述验证码获取请求进行响应。

5 12、如权利要求 10 或 11 所述的系统，其中，所述系统还包括：

获取模块，配置为在所述第一发送模块将所述拦截的信息发送至预置信息数据库之前，获取所述拦截的信息的发送方信息；以及，

在所述发送方信息指示的第三方应用属于所述白名单列表中的第三方应用时，执行所述第一发送模块；否则，执行所述第二发送模块。

10 13、如权利要求 10 所述的系统，其中，所述第一拦截模块，具体配置为按照用于拦截所信息的应用的级别高于所述系统信息数据库的级别的规则，对所述信息进行拦截。

14、如权利要求 10 所述的系统，其中，所述判断模块，包括：

15 内容获取模块，配置为对所述拦截的信息进行解析，在确定所述拦截的信息为非空信息时，获取所述拦截的信息的信息内容；

拆分模块，配置为根据设定拆分规则对信息内容进行拆分，得到多个字符串；

20 验证信息确定模块，配置为依次提取所述多个字符串进行判断，在任一字符串中包括设定关键字和满足设定标准的字符串时，确定所述拦截的信息为验证信息；

其中，所述设定关键字包括：“校验码”或“验证码”；所述满足设定标准的字符串为连续数字，且所述连续数字的长度大于等于设定长度标准。

15、如权利要求 10 所述的系统，其中，所述系统还包括：

25 第一添加模块，配置为在所述第一发送模块将所述拦截的信息发送至预置信息数据库之后，将所述字符串自动添加至系统剪贴板中；

第二添加模块，配置为接收用户的粘贴请求，将所述字符串添加至对应的第三方应用。

16、如权利要求 10 所述的系统，其中，所述系统还包括：

第一应用添加模块，配置为获取通过安全检测的第三方应用的信息，并将所述通过安全检测的第三方应用的信息添加至所述白名单列表中；

和/或，

5 第二应用添加模块，配置为从云端获取确定为安全的第三方应用的信息，并将所述确定为安全的第三方应用的信息添加至所述白名单列表中。

17、如权利要求 10 所述的系统，其中，所述系统还包括：

安全判断模块，配置为在所述第一拦截模块对信息进行拦截之前，接收服务器侧发送的信息，并判断所述服务器侧发送的信息是否为骚扰信息、或诈骗信息、或伪基站信息；

10 第三拦截模块，配置为在所述服务器侧发送的信息是骚扰信息、或诈骗信息、或伪基站信息时，拦截所述服务器侧发送的信息；

安全确定模块，配置为在所述服务器侧发送的信息不是骚扰信息、和诈骗信息、和伪基站信息时，确定所述服务器侧发送的信息是所述安全信息，并执行所述第一拦截模块。

15 18、如权利要求 11 所述的系统，其中，所述身份验证信息包括：第三方应用的签名信息。

20 19、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在移动终端上运行时，导致所述移动终端执行根据权利要求 1-9 中的任一个所述的信息保护的方法。

20 20、一种计算机可读介质，其中存储了如权利要求 19 所述的计算机程序。

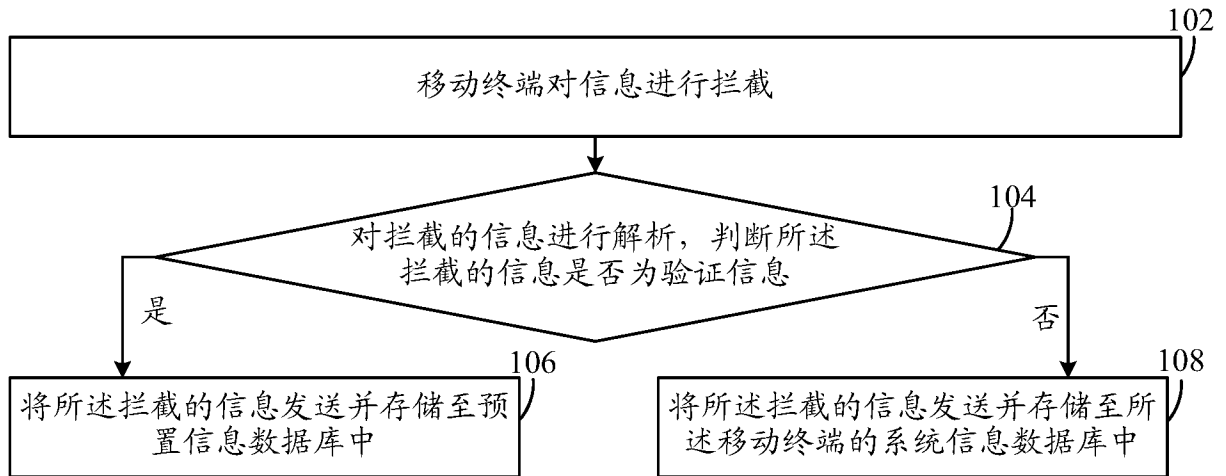


图 1

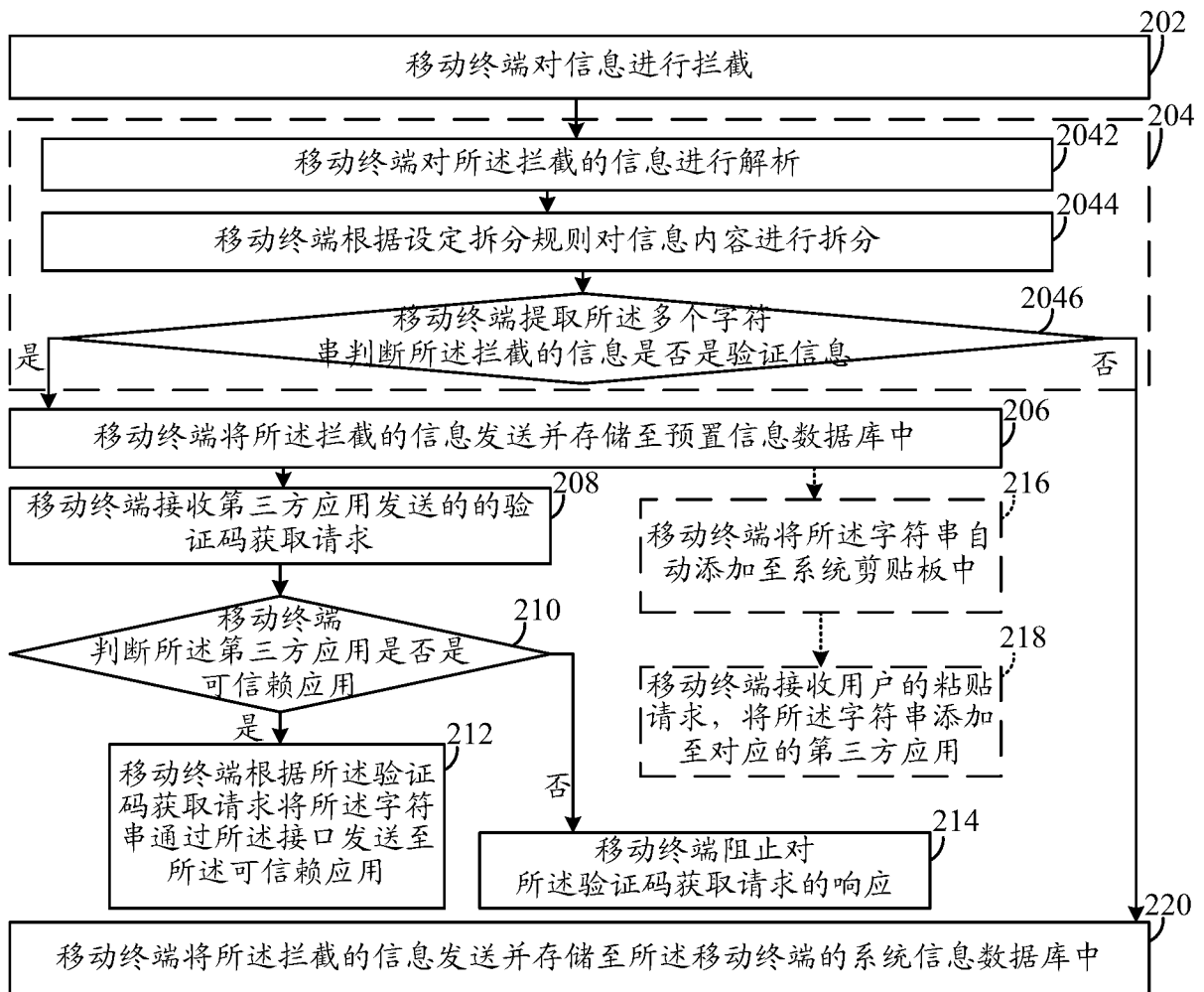


图 2

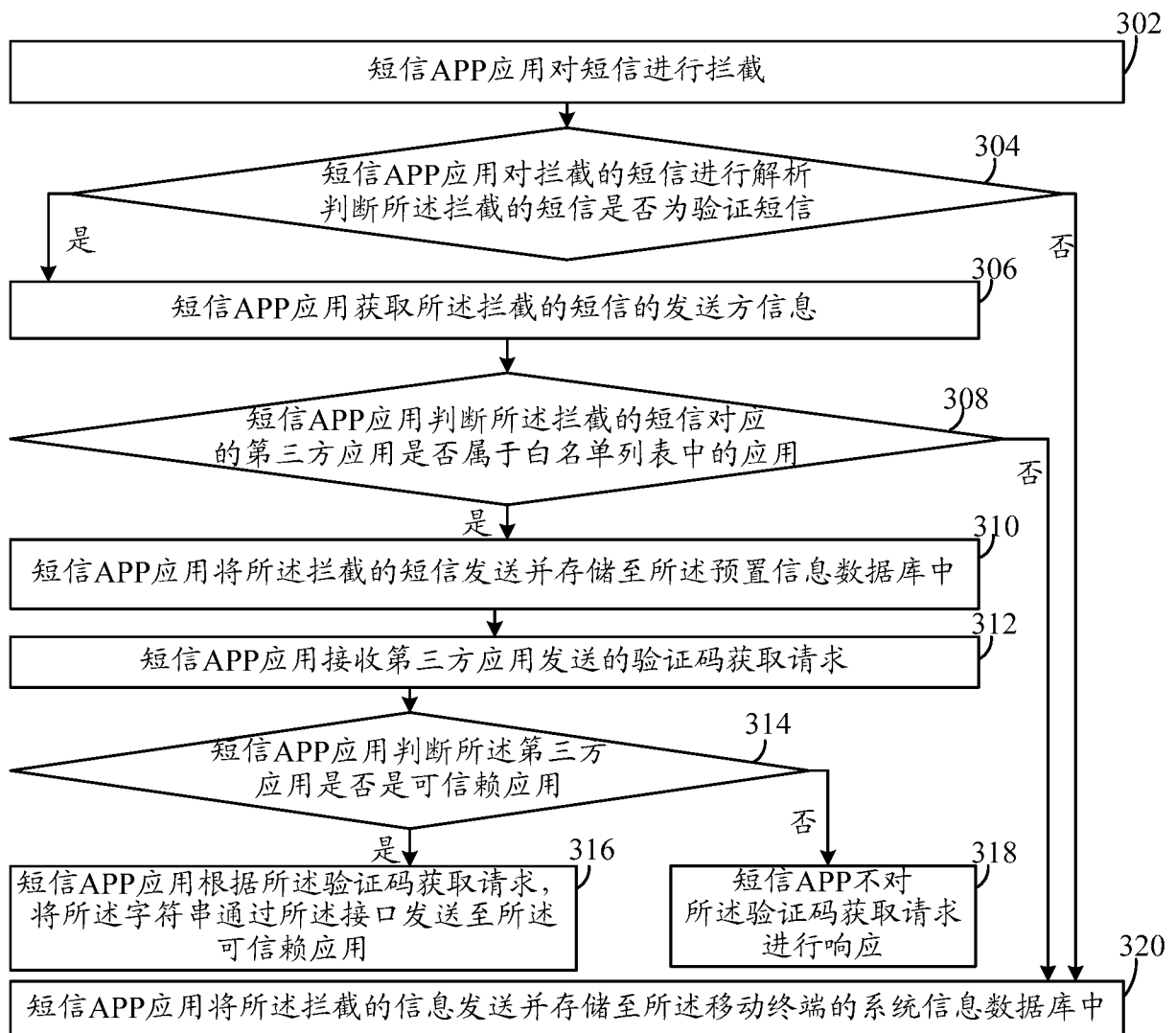


图 3

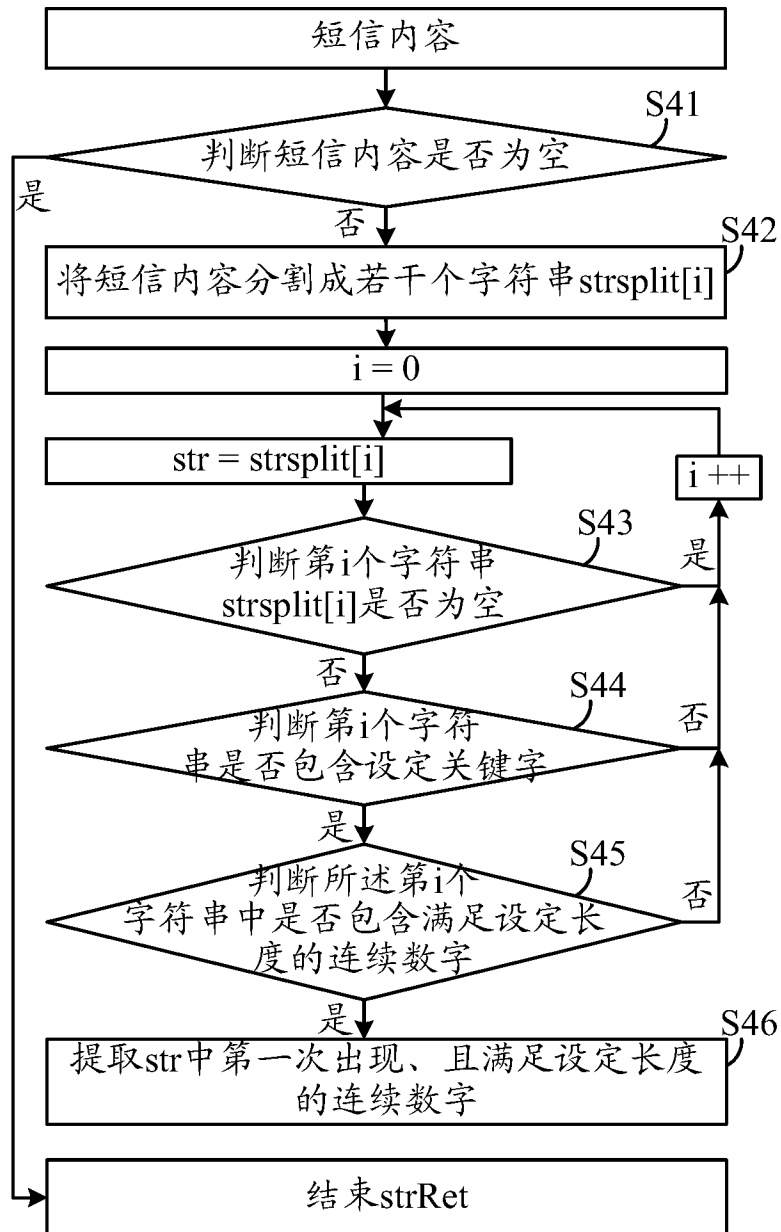


图 4

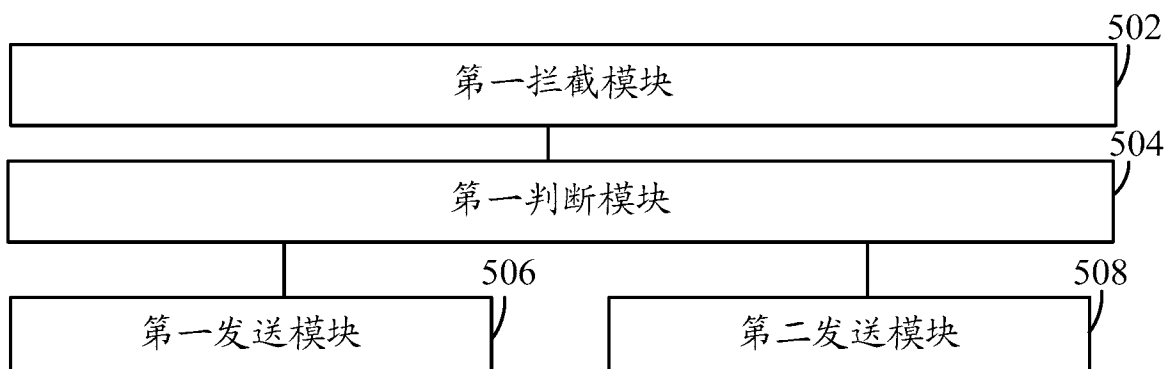


图 5

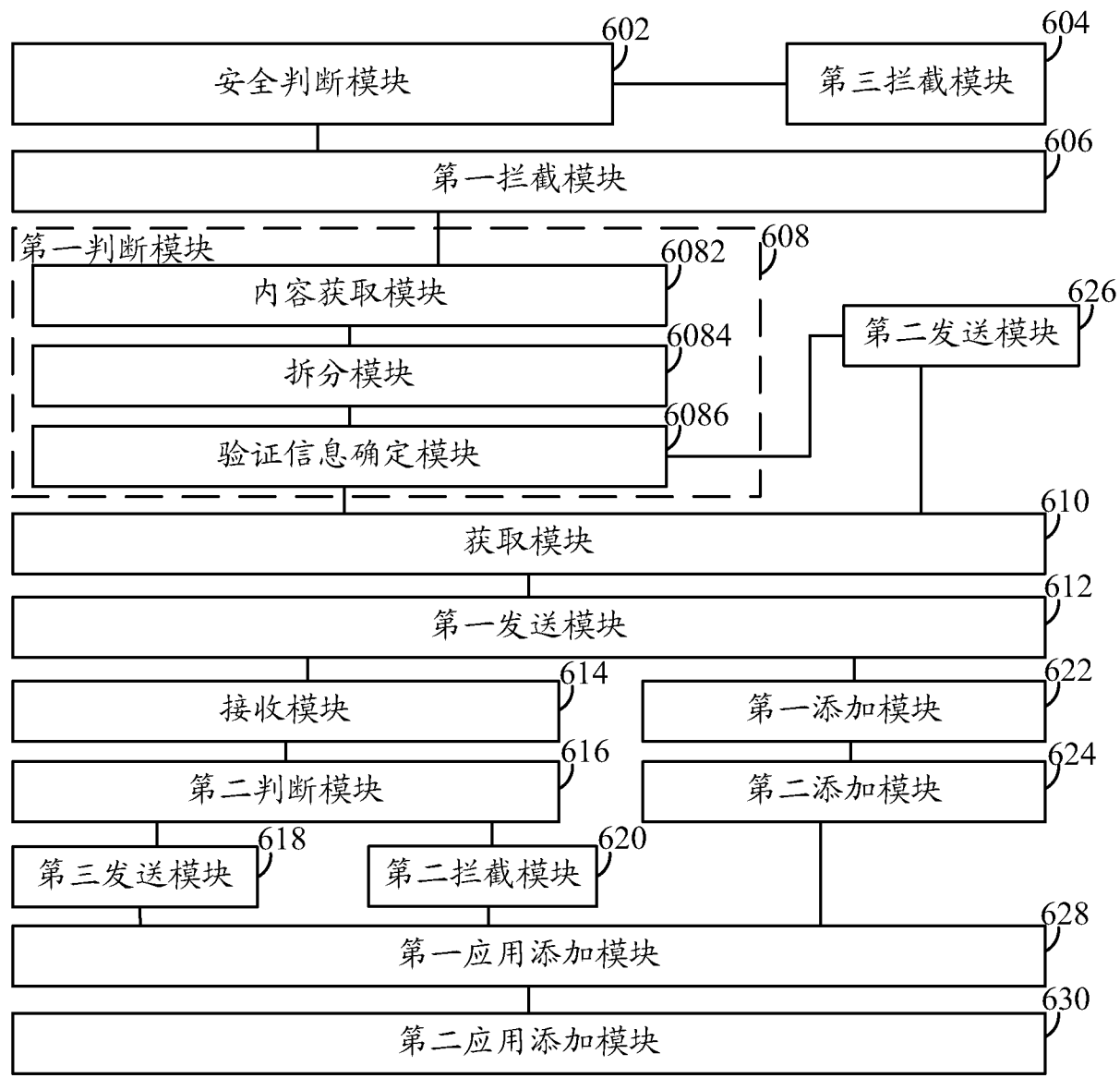


图 6

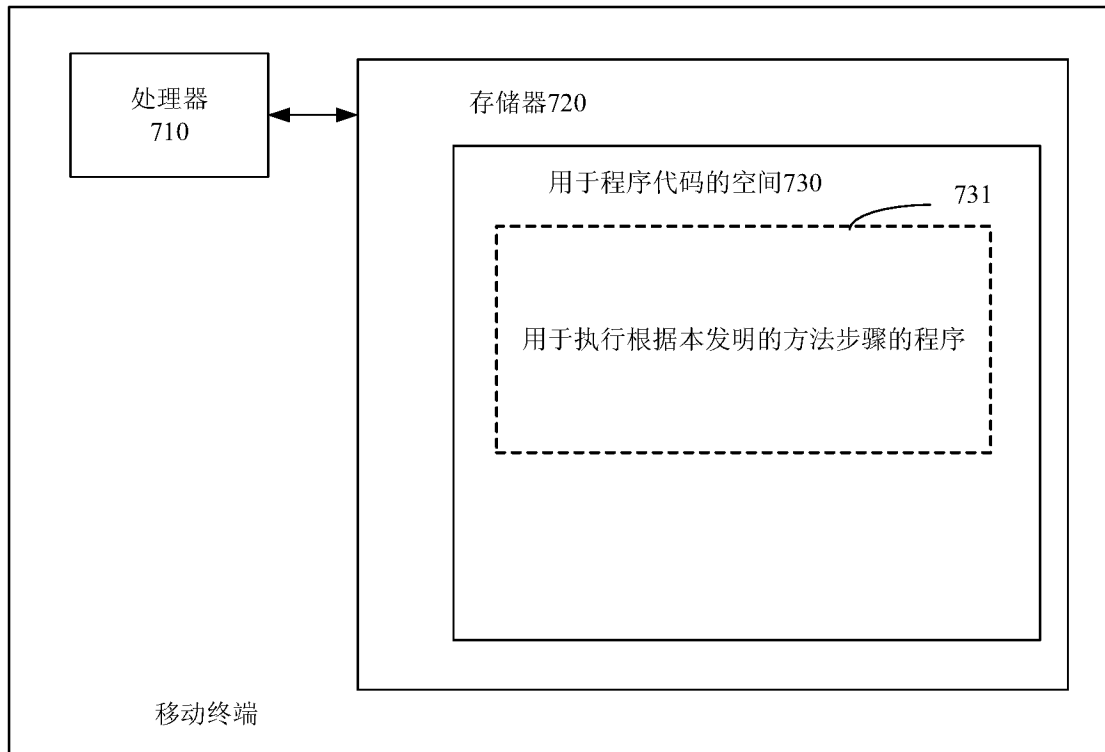


图 7

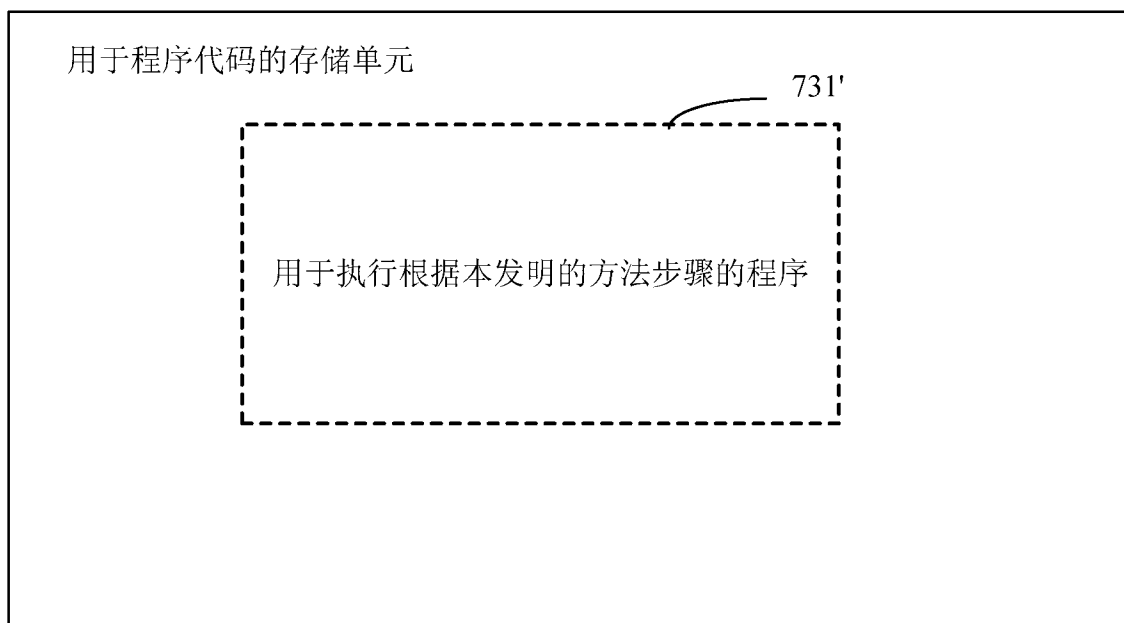


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/077527

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, H04W, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; CNKI; VEN: VERIFY, VERIFICATION, SENSITIVE, IMPORTANT, SECRET, PRIVACY, SAFE, PROTECT, SAVE, WHITE LIST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104009977 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 27 August 2014 (27.08.2014), claims 1-10	1-20
X	CN 1617492 A (FRANCE TELECOM), 18 May 2005 (18.05.2005), description, page 5, lines 7-15 and page 9, line 7 to page 10, line 3, and figure 7	1, 3-8, 10, 12-17, 19, 20
Y	CN 1617492 A (FRANCE TELECOM), 18 May 2005 (18.05.2005), the same as above	2, 9, 11, 18
Y	CN 101212301 A (FEITIAN TECHNOLOGIES CO., LTD.), 02 July 2008 (02.07.2008), description, paragraphs [0038]-[0044]	2, 9, 11, 18
A	CN 103281403 A (ZHEJIANG GONGSHANG UNIVERSITY), 04 September 2013 (04.09.2013), the whole document	1-20
A	CN 102495986 A (SHANGHAI ZHONGBIAO LINGQIAO SOFTWARE TECHNOLOGY CO., LTD.), 13 June 2012 (13.06.2012), the whole document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
18 July 2015 (18.07.2015)

Date of mailing of the international search report
30 July 2015 (30.07.2015)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
WANG, Xiaoling
Telephone No.: (86-10) **62089464**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/077527

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104009977 A	27 August 2014	None	
CN 1617492 A	18 May 2005	DE 60306648 D1	17 August 2006
		EP 1513113 A1	09 March 2005
		US 2005086479 A1	21 April 2005
		DE 60306648 T2	21 June 2007
		US 7587599 B2	08 September 2009
		ES 2268296 T3	16 March 2007
		EP 1513113 B2	23 February 2011
		AT 332549 T	15 July 2006
		EP 1513113 B1	05 July 2006
		JP 2005080315 A	24 March 2005
CN 101212301 A	02 July 2008	CN 101212301 B	14 July 2010
CN 103281403 A	04 September 2013	None	
CN 102495986 A	13 June 2012	None	

国际检索报告

国际申请号

PCT/CN2015/077527

A. 主题的分类

H04L 29/06 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L, H04W, G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CPRSABS; CNTXT; CNKI; VEN: 验证, 敏感, 关键, 重要, 秘密, 安全, 保护, 存储, 保存, 白名单; VERIFY, VERIFICATION, SENSITIVE, IMPORTANT, SECRET, PRIVACY, SAFE, PROTECT, SAVE, WHITE LIST

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 104009977 A (北京奇虎科技有限公司 等) 2014年 8月 27日 (2014 - 08 - 27) 权利要求1-10	1-20
X	CN 1617492 A (法国电信公司) 2005年 5月 18日 (2005 - 05 - 18) 说明书第5页第7-15行、第9页第7行-第10页第3行, 图7	1, 3-8, 10, 12-17, 19, 20
Y	CN 1617492 A (法国电信公司) 2005年 5月 18日 (2005 - 05 - 18) 同上	2, 9, 11, 18
Y	CN 101212301 A (北京飞天诚信科技有限公司) 2008年 7月 2日 (2008 - 07 - 02) 说明书第[0038]-[0044]段	2, 9, 11, 18
A	CN 103281403 A (浙江工商大学) 2013年 9月 4日 (2013 - 09 - 04) 全文	1-20
A	CN 102495986 A (上海中标凌巧软件科技有限公司) 2012年 6月 13日 (2012 - 06 - 13) 全文	1-20

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2015年 7月 18日

国际检索报告邮寄日期

2015年 7月 30日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

授权官员

王晓玲

传真号 (86-10) 62019451

电话号码 (86-10) 62089464

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/077527

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104009977	A	2014年 8月 27日	无			
CN	1617492	A	2005年 5月 18日	DE	60306648	D1	2006年 8月 17日
				EP	1513113	A1	2005年 3月 9日
				US	2005086479	A1	2005年 4月 21日
				DE	60306648	T2	2007年 6月 21日
				US	7587599	B2	2009年 9月 8日
				ES	2268296	T3	2007年 3月 16日
				EP	1513113	B2	2011年 2月 23日
				AT	332549	T	2006年 7月 15日
				EP	1513113	B1	2006年 7月 5日
				JP	2005080315	A	2005年 3月 24日
CN	101212301	A	2008年 7月 2日	CN	101212301	B	2010年 7月 14日
CN	103281403	A	2013年 9月 4日	无			
CN	102495986	A	2012年 6月 13日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)