(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
2017 年 12 月 7 日 (07.12.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/206251 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2016/087561

(22) 国际申请日: 2016 年 6 月 29 日 (29.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610373124.3 2016年5月30日 (30.05.2016) CN

(71) 申请人: 宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 吴安峻 (WU, Anjun); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 杨佳佳 (YANG, Jiajia); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 叶瑞权 (YE, Ruiquan); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所（普通合伙）(YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路8号科技财富中心A座506室尚志峰, Beijing 100192 (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,

(54) **Title:** METHOD AND DEVICE FOR FREEZING APPLICATION

(54) **发明名称:** 一种冻结应用方法以及装置

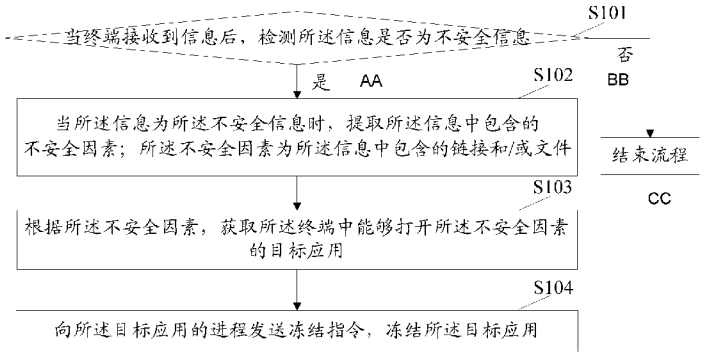


图 1

S101 DETECT, AFTER A TERMINAL RECEIVES INFORMATION, WHETHER THE INFORMATION IS UNSECURE
S102 EXTRACT, IF THE INFORMATION IS UNSECURE, AN UNSECURE FACTOR INCLUDED IN THE INFORMATION, THE UNSECURE FACTOR BEING A LINK AND/OR A FILE INCLUDED IN THE INFORMATION
S103 ACQUIRE, ACCORDING TO THE UNSECURE FACTOR, A TARGET APPLICATION CAPABLE OF OPENING THE UNSECURE FACTOR IN THE TERMINAL
S104 SEND A FREEZING INSTRUCTION TO THE PROCESS OF THE TARGET APPLICATION TO FREEZE THE TARGET APPLICATION
AA YES
BB NO
CC PROCESS ENDS

(57) **Abstract:** A method and a device for freezing an application, the method comprising: detecting, after a terminal receives information, whether the information is unsecure (S101, S201); extracting, if the information is unsecure, an unsecure factor included in the information, the unsecure factor being a link and/or a file included in the information (S102, S202); acquiring, according to the unsecure factor, a target application capable of opening the unsecure factor in the terminal (S103, S204); and sending a freezing instruction to the process of the target application to freeze the target application (S104). The method and device can prevent a user from opening an

WO 2017/206251 A1

[见续页]

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, 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))。

unsecure link or an unsecure file, protecting the user's personal information.

(57) 摘要：一种冻结应用方法以及装置，该方法包括：当终端接收到信息后，检测所述信息是否为不安全信息（S101，S201）；当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件（S102，S202）；根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用（S103，S204）；向所述目标应用的进程发送冻结指令，冻结所述目标应用（S104）。所述方法以及装置能够防止用户打开不安全的链接或不安全文件，保障用户个人信息的安全。

一种冻结应用方法以及装置

技术领域

本发明涉及终端技术领域，特别涉及一种冻结应用方法以及装置。

背景技术

随着终端技术以及信息科技的快速发展，智能终端如智能手机、平板电脑已经广泛应用，短信、QQ、微信等已经成为人们信息交流的重要方式，然而，目前用户在使用智能终端，如智能手机时，常常会收到垃圾信息，例如通过短信、QQ、微信等接收的诈骗信息、推销信息或垃圾软件等，通常这些垃圾信息中可能包含具有安全隐患的不明链接或文件，当用户点击该不明链接或文件时，智能手机会运行相应的应用来打开该不明链接或文件，该不明链接或文件可能会窃取用户的个人信息，从而造成用户个人信息的泄露。

发明内容

本发明实施例公开了一种冻结应用方法以及装置，可以冻结可以打开不安全链接或不安全文件的应用，防止用户打开该不安全的链接或不安全文件，保障用户个人信息的安全。

第一方面，本发明提供了一种冻结应用方法，包括:

当终端接收到信息后，检测所述信息是否为不安全信息;

当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件;

根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用;

向所述目标应用的进程发送冻结指令，冻结所述目标应用。

结合第一方面，在第一方面第一种实现中，所述检测所述信息是否为不安全信息具体包括:

根据预存的信息分类模型，针对接收到的信息执行所述信息分类模型；

获取针对所述信息执行所述信息分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信息。

结合第一方面，在第一方面第二种实现中，所述检测所述信息是否为不安全信息具体包括：

判断所述信息中是否包含预设关键词，当判断结果为是时，所述信息为不安全信息；所述预设关键词是文字、字母、数字或符号中的一种或多种的组合；和/或，

判断所述信息中是否包含链接，如果是，根据所述链接的统一资源定位器地址查看所述链接是否为不安全链接，当查看结果为是时，则所述信息为不安全信息。

结合第一方面，在第一方面第三种实现中，所述根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用具体为：

根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；

遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

结合第一方面，在第一方面第四种实现中，所述当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素之后，所述方法还包括：

提示用户所述信息包含所述不安全因素。

结合第一方面，在第一方面第五种实现中，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述方法还包括：

当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

第二方面，本发明还提供了一种冻结应用装置，包括：

检测单元，用于当终端接收到信息后，检测所述信息是否为不安全信息；

提取单元，用于当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件；

获取单元，用于根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用；

第一执行单元，用于向所述目标应用的进程发送冻结指令，冻结所述目标应用。

结合第二方面，在第二方面第一种实现中，所述检测单元具体用于：

根据预存的分类模型，针对接收到的信息执行所述分类模型；

获取针对所述信息执行所述分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信息。

结合第二方面，在第二方面第二种实现中，所述检测单元具体用于：

判断所述信息中是否包含预设关键词，当判断结果为是时，则所述信息为不安全信息；所述预设关键词是文字、字母、数字或符号中的一种或多种的组合；和/或，

判断所述信息中是否包含链接，如果是，根据所述链接的统一资源定位器地址查看所述链接是否为不安全链接，当查看结果为是时，所述信息为不安全信息。

结合第二方面，在第二方面第三种实现中，，所述获取单元具体用于：

根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；

遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

结合第二方面，在第二方面第四种实现中，所述装置还包括：

提示单元，用于提示用户所述信息包含所述不安全因素。

结合第二方面，在第二方面第五种实现中，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述装置还包括：

第二执行单元，用于当所述目标应用冻结预设时间段后，向所述目标应用

的进程发送解冻指令，解冻所述目标应用。

上述发明，终端通过检测接收到的信息是否为不安全信息，如果是，则提取信息中包含的不安全因素，如不安全链接和/或不安全文件；再根据不安全因素，获取终端中能够打开该不安全因素的目标应用；进而向该目标应用的进程发送冻结指令，冻结可以打开不安全链接或不安全文件的目标应用，防止用户打开该不安全链接或不安全文件，保障用户个人信息的安全。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例提供的冻结应用方法一实施方式的流程示意图；

图 2 是本发明实施例提供的冻结应用方法另一实施方式的流程示意图；

图 3 是本发明实施例提供的冻结应用装置一实施方式的结构示意图；

图 4 为本发明实施例提供的冻结应用装置另一实施方式的结构示意图；

图 5 为本发明实施例提供的终端一实施方式的结构框架图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。

需要说明的是，在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例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。

请参阅图 1，图 1 是本发明实施例提供的冻结应用方法一实施方式的流程示

意图。本发明实施例提供的冻结应用方法可以应用于终端，例如智能手机，平板电脑等，该方法包括:

步骤 S101：当终端接收到信息后，检测所述信息是否为不安全信息。

具体地，终端如智能手机，通常会接收到短信、QQ 信息、微信信息等信息，有些信息中可能包含不安全的链接或不安全的文件，通常可以根据该信息的内容、信息的发送者等检测该信息是否为不安全信息，如果是，则执行步骤 S102；否则，该信息为安全信息，可以结束流程。其中，不安全信息可以是威胁用户财产安全的信息，也可以是包含商业推广的垃圾信息等。

本发明实施例中，检测所述信息是否为不安全信息的方法可以是，根据预存的信息分类模型，针对所述接收到的信息执行所述信息分类模型；获取针对所述信息执行所述信息分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信息。具体地，终端或服务器中可以预存信息分类模型，通过机器学习的方式不断的训练该信息分类模型，使得该信息分类模型更加贴合用户对信息的分类习惯。

可以理解，该信息分类模型可以是 SVM(Support Vector Machine，支持向量机)模型，终端可以针对接收到的信息执行信息抽取模型，进行特征提取，特征选择，进而生成的预测结果。

本发明实施例中，检测所述信息是否为不安全信息的方法还可以是，判断所述信息中是否包含预设关键词，当判断结果为是时，则所述信息为不安全信息；所述预设关键词可以是文字、字母、数字或符号中的一种或多种的组合；和/或，判断所述信息中是否包含链接，如果是，根据所述链接的 URL（Uniform Resoure Locator，统一资源定位器）地址查看所述链接是否为不安全链接，当查看结果为是时，则所述信息为不安全信息。

具体地，终端可以判断信息中是否包含预设关键词，比如“中奖”、“验证码”、“点击领取”、“优惠券”、“欠费”、“请戳”或“点击下载”等中的一种或多种的组合，当判断结果为是时，则该信息为不安全信息；否则，该信息为安全信息。或者，终端也可以判断该信息中是否包含链接，如果是，则进一步分析该链接的 URL 地址，查看该链接是否为垃圾网站的链接，当查看结果为是时，则该信息为不安全信息；否则，该信息为安全信息。或者，终端判断信息中是

否包含预设关键词；以及，判断该信息中是否包含链接，如果是，则进一步分析该链接的 URL 地址，查看该链接是否为垃圾网站的链接。当信息中不包含预设关键词且信息中不存在链接或信息中存在链接，但该链接不为垃圾网站的链接时，认为该信息为安全信息；否则，该信息为不安全信息，可执行步骤 S102。

步骤 S102：当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件；

具体地，当步骤 S101 的检测结果为该信息为不安全信息时，提取该信息中包含的链接和/或文件。

本发明实施例中，步骤 S102 之后，还可以包括，提示用户所述信息包含所述不安全因素。提示的方法可以是弹出提示消息、语音提示、指示灯提示等，本发明不作限制。

可以理解，本发明中文件可以是文档（包括 word、PDF 等）、图片、压缩包、程序、音频文件等，本发明中链接可以指网址、或本地中文件的地址等。

可以理解，提取该信息中包含的链接和/或文件的方法可以是获取在链接和/或文件上输入的打开操作，根据该打开操作生成打开指令，该打开指令用于指示终端打开链接点击的链接和/或文件，此时，终端在执行该打开指令之前，获取点击的链接和/或文件，执行步骤 S103。提取该信息中包含的链接和/或文件的方法还可以通过信息抽取模型，该信息抽取模型可以是基于词典的抽取模型（如，AutoSlog，CRYSTAL，SRV、PALKA 等），基于规则的抽取模型也称为 Wrapper 模型（如，WIEN、WHISK、Wrapper-Up 等），或者基于隐马尔科夫模型的抽取模型等。

步骤 S103：根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用。

具体地，。当终端提取出信息中包含不安全因素后，分析可以打开该不安全因素的应用，比如，可以打开链接的应用可以是浏览器，可以打开 office 文档的应用可以是 office 应用，可以打开视频文件的应用可以是各个视频播放应用等。

本发明实施例中，获取所述终端中能够打开所述不安全因素的目标应用的方法可以是，根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；遍历所述终端中安装的应用，获取所述终端

中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

具体地，终端根据链接与应用的对应关系和/或文件的类别与应用的对应关系，比如，链接与浏览器的对应关系、音频文件与各个音频应用的对应关系、压缩包与各个打开压缩的应用的对应关系等，查找信息中包含的不安全因素对应的应用，比如，信息中包含第一不安全因素和第二不安全因素，第一不安全因素对应的应用包括第一应用和第二应用，第二不安全因素对应的应用包括第三应用、第四应用以及第五应用，则终端获取第一应用、第二应用、第三应用、第四应用以及第五应用；继而，终端遍历该终端中安装的应用，获取终端中与上述获取的应用相匹配的应用，比如上述五个应用中，终端中仅包含其中的第一应用和第二应用，则第一应用和第二应用即为终端中能够打开不安全因素的目标应用，保障用户个人信息的安全。

步骤 S104：向所述目标应用的进程发送冻结指令，冻结所述目标应用。

具体地，终端获取到目标应用后，向该目标应用的进程发送冻结指令，冻结该目标应用，避免使用该目标应用打开不安全链接或不安全文件。

本发明实施例中，终端通过检测接收到的信息是否为不安全信息，如果是，则提取信息中包含的不安全因素，如不安全链接和/或不安全文件；再根据不安全因素，获取终端中能够打开该不安全因素的目标应用；进而向该目标应用的进程发送冻结指令，冻结可以打开不安全链接或不安全文件的目标应用，防止用户打开该不安全链接或不安全文件，保障用户个人信息的安全。

请参阅图 2，图 2 是本发明实施例提供的冻结应用方法另一实施方式的流程示意图。本发明实施例提供的冻结应用方法可以应用于终端，例如智能手机，平板电脑等，该方法包括：

步骤 S201：当终端接收到信息后，检测所述信息是否为不安全信息。

步骤 S202：当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件。

步骤 S203：提示用户所述信息包含所述不安全因素。

步骤 S204：根据所述不安全因素，获取所述终端中能够打开所述不安全因

素的目标应用。

需要说明的是，步骤 S201、步骤 S202、步骤 S203 以及步骤 S204 可参见图 1 描述的实施例相应的步骤，本发明不再赘述。

步骤 S205：向所述目标应用的进程发送冻结指令，冻结所述目标应用，所述冻结指令包括时间权限。

具体地，终端获取到目标应用后，向该目标应用的进程发送冻结指令，冻结该目标应用，避免使用该目标应用打开不安全链接或不安全文件。其中，该时间权限用于指示终端在目标应用冻结预设时间段后发送解冻指令。

步骤 S206：当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

需要说明的是，该预设时间段可以是 1 分钟、2 分钟、5 分钟、30 分钟、1 小时等，本发明不做限制。

本发明实施例中，终端通过检测接收到的信息是否为不安全信息，如果是，则提取信息中包含的不安全因素，如不安全链接和/或不安全文件；提示该不安全因素，再根据不安全因素，获取终端中能够打开该不安全因素的目标应用；进而向该目标应用的进程发送冻结指令，冻结可以打开不安全链接或不安全文件的目标应用，当所述目标应用冻结预设时间段后，自动向所述目标应用的进程发送解冻指令，解冻所述目标应用，既可以防止用户打开该不安全链接或不安全文件，保障用户个人信息的安全，也可以实现冻结预设时间段后自动解冻应用，避免用户进行频繁解冻操作，提高用户体检。

请参阅图 3，图 3 是本发明实施例提供的冻结应用装置一实施方式的结构示意图。本发明实施例提供的冻结应用装置可以应用于终端，例如智能手机，平板电脑等，该冻结应用装置 300 包括：检测单元 301、提取单元 302、获取单元 303 以及第一执行单元 304，其中，

检测单元 301，用于当终端接收到信息后，检测所述信息是否为不安全信息。本发明实施例中，所述检测单元 301 具体用于：根据预存的分类模型，针对接收到的信息执行所述分类模型；获取针对所述信息执行所述分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信

息。

本发明实施例中，所述检测单元具体 301 用于：判断所述信息中是否包含预设关键词，当判断结果为是时，则所述信息为不安全信息，其中，所述预设关键词是文字、字母、数字或符号中的一种或多种的组合；和/或，判断所述信息中是否包含链接，如果是，根据所述链接的URL 地址查看所述链接是否为不安全链接，当查看结果为是时，则所述信息为不安全信息。

提取单元 302，用于当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件；

获取单元 303，用于根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用。

本发明实施例中，所述获取单元 303 具体用于：根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

第一执行单元 304，用于向所述目标应用的进程发送冻结指令，冻结所述目标应用。

需要说明的是，本发明各实施例中的冻结应用装置 300 中检测单元 301、提取单元 302、获取单元 303 以及第一执行单元 304 的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

请参阅图 4，图 4 是本发明实施例提供的冻结应用装置另一实施方式的结构示意图。该冻结应用装置 400 除包括图 3 所示的冻结应用装置 300 中的各个单元外，还可以包括：提示单元 305 以及第二执行单元 306，其中，

本发明实施例中，所述冻结应用装置 300 还包括：提示单元 305，用于提示用户所述信息包含不安全因素。

本发明实施例中，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述冻结应用装置 300

还可以包括：第二执行单元 306，用于当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

需要说明的是，本发明各实施例中的冻结应用装置 400 中检测单元 301、提取单元 302、获取单元 303、第一执行单元 304、提示单元 305 以及第二执行单元 306 的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

请参阅图 5，图 5 是本发明实施例提供的终端一实施方式的结构框架图。该终端用于配合实施上述方案。该终端可以是智能手机，平板电脑等。本发明实施例提供的终端可以用于实施上述图 1 或图 2 所示的本发明各实施例实现的方法，为了便于说明，仅示出了与本发明各实施例相关的部分，具体技术细节未揭示的，请参照图 1 或图 2 所示的本发明各实施例。其中，图 5 所示的终端可以包括：处理器 501 以及通过接口 502 与处理器 501 相连接的输入模块 503、输出模块 504，以及通过总线 505 与处理器 501 相连接的存储器 506。其中，存储器 506 用于存储一组程序代码；处理器 501 用于调用存储器 506 中存储的程序代码，用于执行以下操作：

本发明提供了一种冻结应用方法，包括：

当终端通过输入模块 503 接收到信息后，检测所述信息是否为不安全信息；

当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件；

根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用；

向所述目标应用的进程发送冻结指令，冻结所述目标应用。

本发明实施例中，所述处理器 501 执行所述检测所述信息是否为不安全信息具体包括：

根据预存的信息分类模型，针对接收到的信息执行所述信息分类模型；

获取针对所述信息执行所述信息分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信息。

本发明实施例中，所述处理器 501 执行所述检测所述信息是否为不安全信

息具体包括:

判断所述信息中是否包含预设关键词，当判断结果为是时，则所述信息为不安全信息；所述预设关键词可以是文字、字母、数字或符号中的一种或多种的组合；和/或，

判断所述信息中是否包含链接，如果是，根据所述链接的 URL 地址查看所述链接是否为不安全链接，当查看结果为是时，则所述信息为不安全信息。

本发明实施例中，所述处理器 501 执行所述根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用具体为:

根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

本发明实施例中，所述当所述信息为不安全信息时，所述处理器 501 执行所述提取所述信息中包含的不安全因素之后，所述处理器 501 还用于执行: 通过输出模块 504 提示用户所述信息包含所述不安全因素。

本发明实施例中，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述处理器 501 还用于执行: 当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

综上所述，终端通过检测接收到的信息是否为不安全信息，如果是，则提取信息中包含不安全因素，如不安全链接和/或不安全文件；再根据不安全因素，获取终端中能够打开该不安全因素的目标应用；进而向该目标应用的进程发送冻结指令，冻结可以打开不安全链接或不安全文件的目标应用，防止用户打开该不安全链接或不安全文件，保障用户个人信息的安全。

而且，该方法也可以实现冻结预设时间段后自动解冻应用，避免用户进行频繁解冻操作，提高用户体检。

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流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算

机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所揭露的仅为本发明一种较佳实施例而已，当然不能以此来限定本发明之权利范围，本领域普通技术人员可以理解实现上述实施例的全部或部分流程，并依本发明权利要求所作的等同变化，仍属于发明所涵盖的范围。

权利要求书

1、一种冻结应用方法，其特征在于，包括:

当终端接收到信息后，检测所述信息是否为不安全信息;

当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件;

根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用;

向所述目标应用的进程发送冻结指令，冻结所述目标应用。

2、根据权利要求 1 所述的方法，其特征在于，所述检测所述信息是否为不安全信息具体包括:

根据预存的信息分类模型，针对接收到的信息执行所述信息分类模型;

获取针对所述信息执行所述信息分类模型生成的预测结果，所述预测结果包括：所述信息为不安全信息，或，所述信息为安全信息。

3、根据权利要求 1 所述的方法，其特征在于，所述检测所述信息是否为不安全信息具体包括:

判断所述信息中是否包含预设关键词，当判断结果为是时，所述信息为不安全信息；所述预设关键词是文字、字母、数字或符号中的一种或多种的组合;

和/或，

判断所述信息中是否包含链接，如果是，根据所述链接的统一资源定位器地址查看所述链接是否为不安全链接，当查看结果为是时，所述信息为不安全信息。

4、根据权利要求 1 所述的方法，其特征在于，所述根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用具体为:

根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用;

遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应

用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

5、根据权利要求 1 所述的方法，其特征在于，所述当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素之后，所述方法还包括:

提示用户所述信息包含所述不安全因素。

6、根据权利要求 1 所述的方法，其特征在于，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述方法还包括:

当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

7、一种冻结应用装置，其特征在于，包括:

检测单元，用于当终端接收到信息后，检测所述信息是否为不安全信息;

提取单元，用于当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件;

获取单元，用于根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用;

第一执行单元，用于向所述目标应用的进程发送冻结指令，冻结所述目标应用。

8、根据权利要求 7 所述的装置，其特征在于，所述检测单元具体用于:

根据预存的分类模型，针对接收到的信息执行所述分类模型;

获取针对所述信息执行所述分类模型生成的预测结果，所述预测结果包括:所述信息为不安全信息，或，所述信息为安全信息。

9、根据权利要求 7 所述的装置，其特征在于，所述检测单元具体用于:

判断所述信息中是否包含预设关键词，当判断结果为是时，则所述信息为

不安全信息；所述预设关键词是文字、字母、数字或符号中的一种或多种的组合；和/或，

判断所述信息中是否包含链接，如果是，根据所述链接的统一资源定位器地址查看所述链接是否为不安全链接，当查看结果为是时，所述信息为不安全信息。

10、根据权利要求 7 所述的装置，其特征在于，所述获取单元具体用于：

根据链接与应用的对应关系和/或文件的类别与应用的对应关系，查找所述不安全因素对应的应用；

遍历所述终端中安装的应用，获取所述终端中与所述不安全因素对应的应用相匹配的应用；所述终端中与所述不安全因素对应的应用相匹配的应用即为所述终端中能够打开所述不安全因素的目标应用。

11、根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

提示单元，用于提示用户所述信息包含所述不安全因素。

12、根据权利要求 7 所述的装置，其特征在于，所述冻结指令包括时间权限；所述时间权限用于指示所述终端在所述目标应用冻结预设时间段后发送解冻指令；所述装置还包括：

第二执行单元，用于当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用。

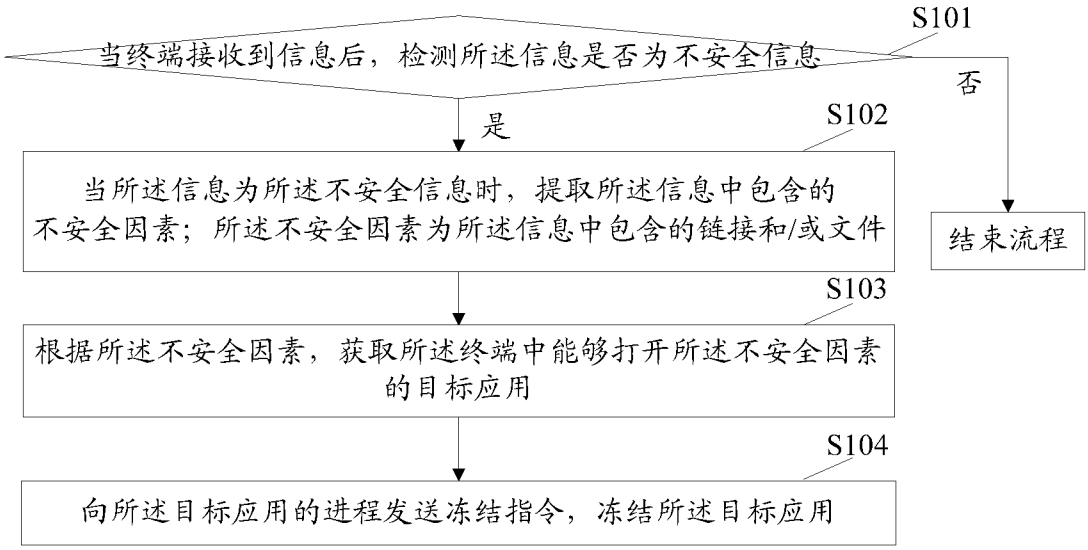

S101
当终端接收到信息后，检测所述信息是否为不安全信息
否
是
S102
当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件
结束流程
S103
根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用
S104
向所述目标应用的进程发送冻结指令，冻结所述目标应用

图 1

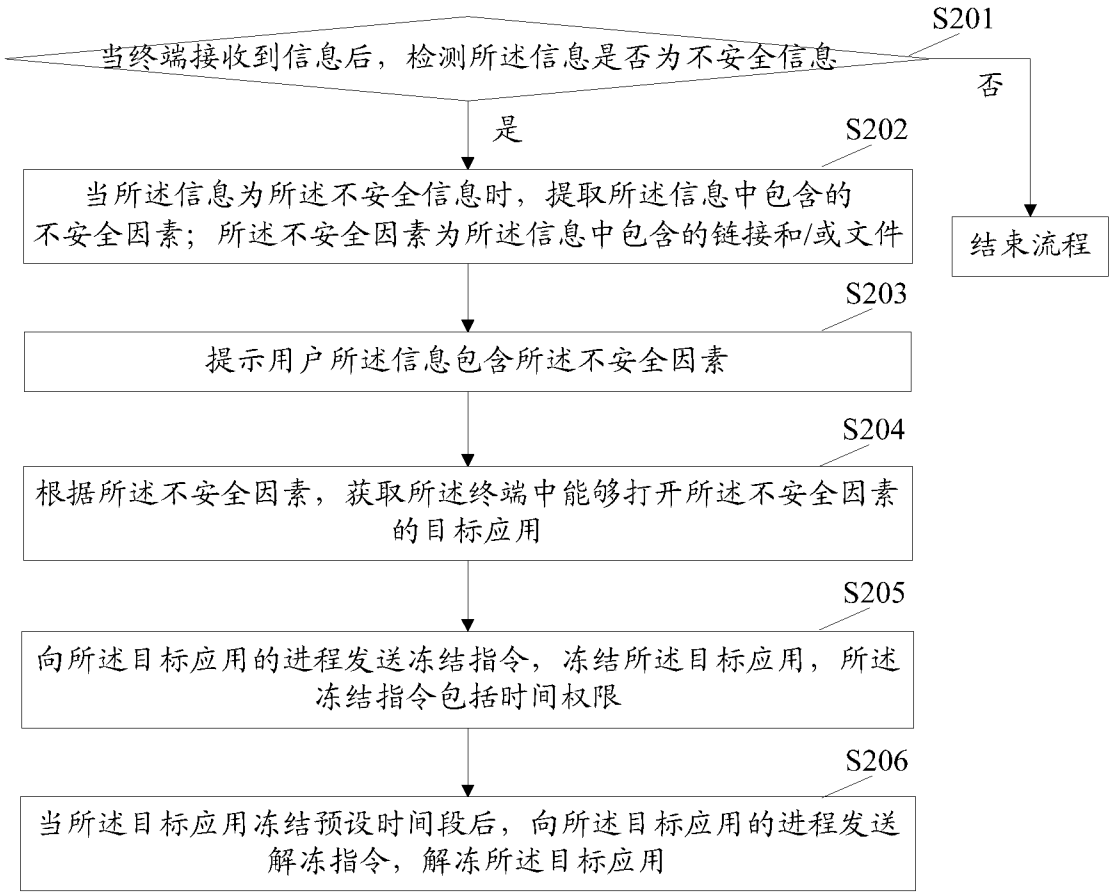

S201
当终端接收到信息后，检测所述信息是否为不安全信息
否
是
结束流程
S202
当所述信息为所述不安全信息时，提取所述信息中包含的不安全因素；所述不安全因素为所述信息中包含的链接和/或文件
S203
提示用户所述信息包含所述不安全因素
S204
根据所述不安全因素，获取所述终端中能够打开所述不安全因素的目标应用
S205
向所述目标应用的进程发送冻结指令，冻结所述目标应用，所述冻结指令包括时间权限
S206
当所述目标应用冻结预设时间段后，向所述目标应用的进程发送解冻指令，解冻所述目标应用

图 2

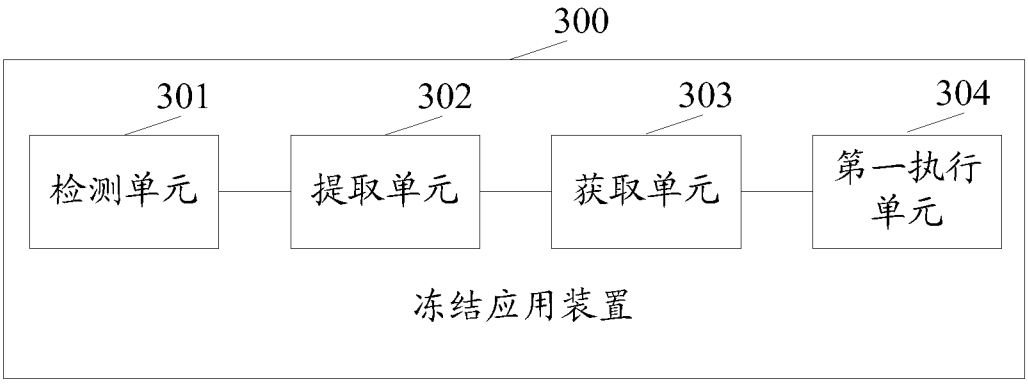

300
301
检测单元
302
提取单元
303
获取单元
304
第一执行单元
冻结应用装置

图 3

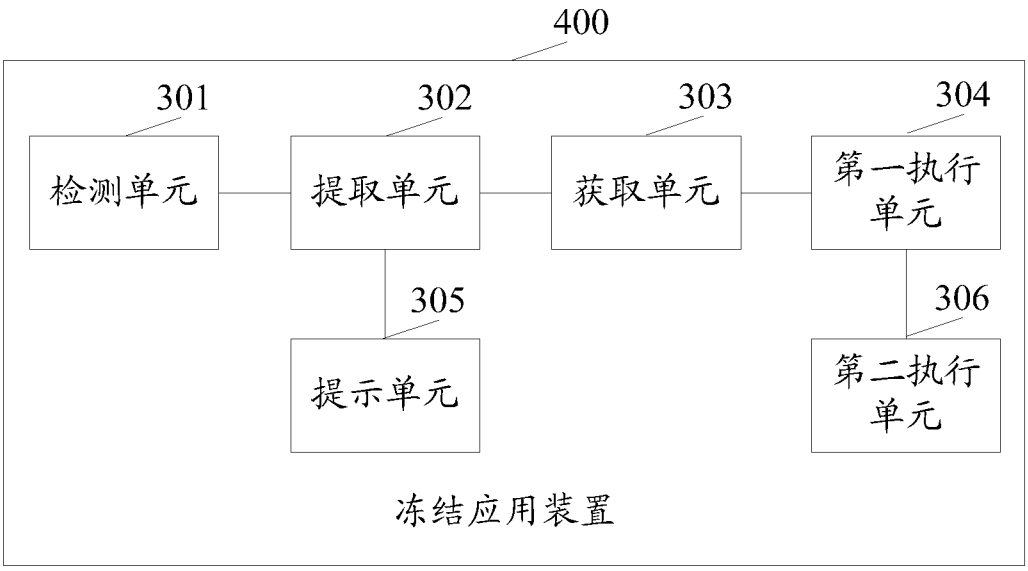

400
301
检测单元
302
提取单元
303
获取单元
304
第一执行单元
305
提示单元
306
第二执行单元
冻结应用装置

图 4

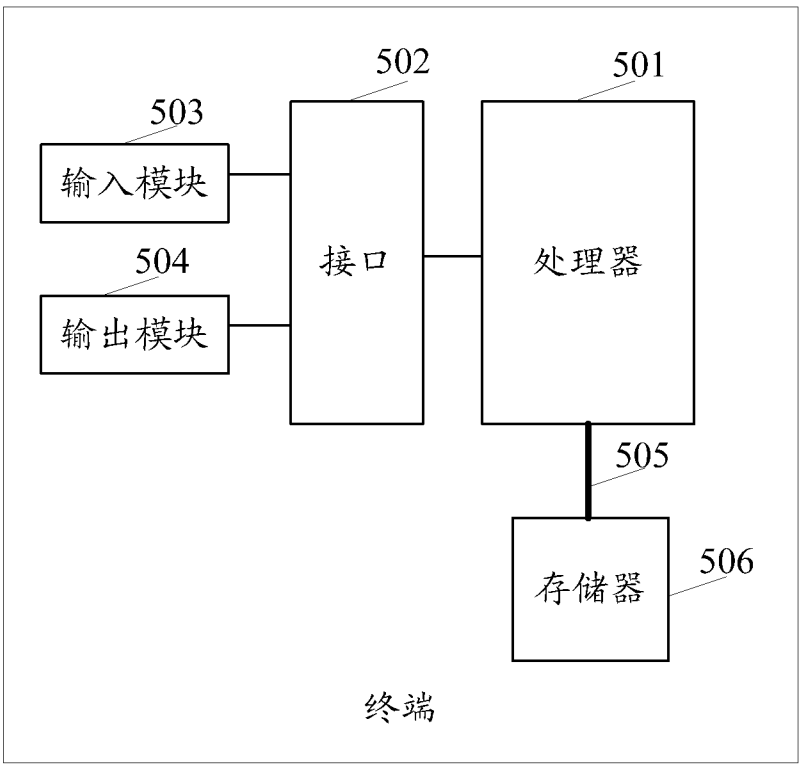

502
501
503
输入模块
504
输出模块
接口
处理器
505
存储器
506
终端

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/087561

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60 (2013.01) 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)

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)

CNPAT, WPI, EPODOC, CNKI: illegal, malicious, application, freezing, terminal, link, unsafe, browser, search, prohibit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102664913 A (QIZHI SOFTWARE (BEIJING) CO., LTD.), 12 September 2012 (12.09.2012), description, paragraphs [0038]-[0045] and [0049]-[0060]	1-12
A	US 2012102545 A1 (MCAFEE, INC.), 26 April 2012 (26.04.2012), the whole document	1-12
A	CN 103544431 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 29 January 2014 (29.01.2014), the whole document	1-12
A	CN 104408368 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 11 March 2015 (11.03.2015), the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2017 (14.02.2017)	**01 March 2017 (01.03.2017)**
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 **MA, Jintao** Telephone No.: (86-10) **62414067**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/087561

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102664913 A	12 September 2012	CN 102664913 B	15 April 2015
US 2012102545 A1	26 April 2012	JP 5973017 B2	17 August 2016
		US 9317680 B2	19 April 2016
		KR 101512253 B1	14 April 2015
		JP 5702470 B2	15 April 2015
		WO 2012054449 A2	26 April 2012
		JP 2013541781 A	14 November 2013
		CN 103221959 A	24 July 2013
		CN 103221959 B	10 August 2016
		JP 2015146188 A	13 August 2015
		KR 20140051102 A	30 April 2014
		EP 2630611 A2	28 August 2013
CN 103544431 A	29 January 2014	CN 103544431 B	06 January 2016
CN 104408368 A	11 March 2015	None	

国际检索报告

国际申请号
PCT/CN2016/087561

A. 主题的分类

G06F 21/60(2013.01)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)

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））

CNPAT, WPI, EPODOC, CNKI: 终端，冻结，禁止，应用，链接，不安全，非法，恶意，浏览器，查找，application, freezing, terminal, link, unsafe, browser, search, prohibit

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
X	CN 102664913 A (奇智软件北京有限公司) 2012年 9月 12日 (2012-09-12) 说明书第[0038]-[0045]、[0049]-[0060]段	1-12
A	US 2012102545 A1 (MCAFEE, INC.) 2012年 4月 26日 (2012-04-26) 全文	1-12
A	CN 103544431 A (腾讯科技深圳有限公司) 2014年 1月 29日 (2014-01-29) 全文	1-12
A	CN 104408368 A (中国联合网络通信集团有限公司) 2015年 3月 11日 (2015-03-11) 全文	1-12

☐ 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	国际检索报告邮寄日期
2017年 2月 14日	2017年 3月 1日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	马晋涛
传真号 (86-10)62019451	电话号码 (86-10)62414067

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/087561

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	102664913	A	2012年 9月 12日	CN	102664913	B	2015年 4月 15日
US	2012102545	A1	2012年 4月 26日	JP	5973017	B2	2016年 8月 17日
				US	9317680	B2	2016年 4月 19日
				KR	101512253	B1	2015年 4月 14日
				JP	5702470	B2	2015年 4月 15日
				WO	2012054449	A2	2012年 4月 26日
				JP	2013541781	A	2013年 11月 14日
				CN	103221959	A	2013年 7月 24日
				CN	103221959	B	2016年 8月 10日
				JP	2015146188	A	2015年 8月 13日
				KR	20140051102	A	2014年 4月 30日
				EP	2630611	A2	2013年 8月 28日
CN	103544431	A	2014年 1月 29日	CN	103544431	B	2016年 1月 6日
CN	104408368	A	2015年 3月 11日		无		