

(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
2018 年 3 月 8 日 (08.03.2018)



(10) 国际公布号
WO 2018/040944 A1

(51) 国际专利分类号:
G06Q 30/06 (2012.01)

(21) 国际申请号: PCT/CN2017/097953

(22) 国际申请日: 2017 年 8 月 18 日 (18.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610797563.7 2016 年 8 月 31 日 (31.08.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛
大开曼资本大厦一座四层 847 号 邮箱,
Grand Cayman (KY)。

(72) 发明人: 肖 谦 (XIAO, Qian); 中国浙江省杭州市
余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团
法务部, Zhejiang 311121 (CN)。 赵争超 (ZHAO,
Zhengchao); 中国浙江省杭州市余杭区文一西路
969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang
311121 (CN)。 林君 (LIN, Jun); 中国浙江省杭州
市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集
团法务部, Zhejiang 311121 (CN)。 潘林林 (PAN,
Linlin); 中国浙江省杭州市余杭区文一西路 969 号
3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121
(CN)。 张一昌 (ZHANG, Yichang); 中国浙江省
杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴
巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北 京 三 友 知 识 产 权 代 理
有 限 公 司 (BEIJING SANYOU INTELLECTUAL
PROPERTY AGENCY LTD.); 中 国 北 京 市 金

(54) Title: SYSTEM, METHOD, AND DEVICE FOR IDENTIFYING MALICIOUS ADDRESS/MALICIOUS PURCHASE ORDER

(54) 发明名称: 恶意地址/恶意订单的识别系统、方法及装置

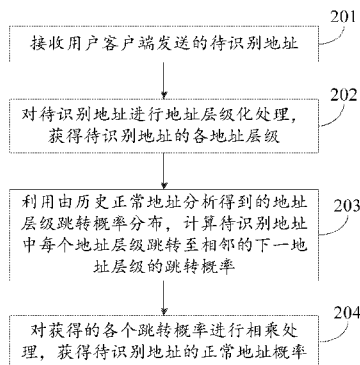


图 3

- 201 Receive an address to be identified and sent by a client end
202 Process the address to be identified to obtain address levels, and acquire all address levels of the address to be identified
203 Calculate, by employing an address level jump probability distribution obtained by analyzing past normal addresses, for each of the address levels, a jump probability of jumping from said address level in the address to be identified to the next adjacent address level
204 Multiply all acquired jump probabilities to acquire a probability of the address to be identified being a normal address

(57) Abstract: The present invention relates to the technical field of the Internet, and discloses a system, method, and device for identifying a malicious address/malicious purchase order, solving the problem of a poor identification rate of malicious addresses/malicious purchase orders in the prior art. The method of the present invention primarily comprises: receiving an address to be identified and sent by a client end; processing the address to be identified to obtain address levels, and acquiring all address levels of the address to be identified; calculating, by employing an address level jump probability distribution obtained by analyzing past normal addresses, for

融街 35 号国际企业大厦 A 座 16 层,
Beijing 100033 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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))。

each of the address levels, a jump probability of jumping from said address level in the address to be identified to the next adjacent address level, the address level jump probability distribution comprising jump probabilities of jumping from an arbitrary address level to another address level; and multiplying all acquired jump probabilities to acquire a probability of the address to be identified being a normal address.

(57) 摘要: 本发明公开一种恶意地址/恶意订单的识别系统、方法及装置, 涉及互联网技术领域, 能够解决现有技术中识别恶意地址/恶意订单准确率较低的问题。本发明的方法主要包括: 接收用户客户端发送的待识别地址; 对所述待识别地址进行地址层级化处理, 获得所述待识别地址的各地址层级; 利用由历史正常地址分析得到的地址层级跳转概率分布, 计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率, 所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率; 对获得的各个跳转概率进行相乘处理, 获得所述待识别地址的正常地址概率。

恶意地址/恶意订单的识别系统、方法及装置

本申请要求 2016 年 08 月 31 日递交的申请号为 201610797563.7、发明名称为“恶意地址/恶意订单的识别系统、方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及互联网技术领域，特别是涉及一种恶意地址/恶意订单的识别系统、方法及装置。

10 背景技术

随着互联网技术的发展，人们通过网络不仅可以实现观看视频、浏览网页、聊天等操作，还可以进行购物，并且实现购物的操作过程也十分方便。

然而，在实际应用中，却常常发生某些买家通过故意填写不完整的收货地址、错误的收货地址等恶意行为使商品无法送达，由此给商家带来经济损失、信誉损失的现象，

15 因此，如何识别恶意地址对商家是极其重要的。现有识别恶意地址的方式主要有三种：

（1）通过将待识别地址与预设恶意关键词进行匹配，来确定待识别地址是否为恶意地址；（2）通过将待识别地址与黑白名单中的地址分别进行匹配，来确定待识别地址是否为恶意地址；（3）通过对待识别地址进行层级结构化划分，然后与预设地址层级结构进行匹配，来确定待识别地址是否为恶意地址。

20 虽然上述三种方式均可以在一定程度上识别出部分恶意地址，但是无法识别出一些隐藏的恶意地址，或者可能会将正常的地址误判为恶意地址。例如，对于同一个关键词，在一个地址中可能为恶意关键词，但在另一个地址中可能为正常关键词，因此若将该关键词作为预设恶意地址进行识别，则可能出现将正常地址误判为恶意地址的现象。又如，由于黑白名单是根据商家发货后的实际反馈进行的人工维护的名单，所以利用黑白名单
25 进行识别的方式不仅需要消耗人力，还不能及时识别出新的恶意地址。再如，对于一些地址层级结构完整但在现实生活中不存在的地址，如果利用预设地址层级结构进行识别，会将其误判为正常地址。因此，现有技术中识别恶意地址的准确率较低，从而使得识别恶意订单的准确率也较低。

30 发明内容

有鉴于此，本发明提供一种恶意地址/恶意订单的识别系统、方法及装置，能够解决现有技术中识别恶意地址/恶意订单准确率较低的问题。

第一方面，本发明提供了一种恶意地址的识别系统，所述系统包括用户客户端、服务器和商家客户端；其中，

5 所述用户客户端用于接收输入的待识别地址，并将所述待识别地址发送给所述服务器；

所述服务器用于接收所述用户客户端发送的所述待识别地址，并对所述待识别地址进行地址层级化处理，获得所述待识别地址的各地址层级；利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得所述待识别地址的正常地址概率，并将基于所述正常地址概率进行恶意地址识别的识别结果发送给所述商家客户端；

10

所述商家客户端用于接收并输出所述服务器发送的所述识别结果。

15 第二方面，本发明提供了一种恶意地址的识别方法，所述方法包括：

接收用户客户端发送的待识别地址；

对所述待识别地址进行地址层级化处理，获得所述待识别地址的各地址层级；

利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

20

对获得的各个跳转概率进行相乘处理，获得所述待识别地址的正常地址概率。

第三方面，本发明提供了一种恶意地址的识别装置，所述装置包括：

接收单元，用于接收用户客户端发送的待识别地址；

第一处理单元，用于对所述待识别地址进行地址层级化处理，获得所述待识别地址的各地址层级；

25

计算单元，用于利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

第二处理单元，用于对所述计算单元获得的各个跳转概率进行相乘处理，获得所述待识别地址的正常地址概率。

30

第四方面，本发明提供了一种恶意订单的识别系统，所述系统包括用户客户端、服务器和商家客户端；其中，

所述用户客户端用于接收输入的待识别订单，并将所述待识别订单发送给所述服务器；

5 所述服务器用于接收所述用户客户端发送的所述待识别订单，并基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得所述地址的正常地址概率；根据所述正常地址概率判断所述待识别订单是否为恶意订单，并将
10 判断结果发送给所述商家客户端；

所述商家客户端用于接收并显示所述服务器发送的所述判断结果。

第五方面，本发明提供了一种恶意订单的识别方法，所述方法包括：

接收用户客户端发送的待识别订单；

15 基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

对获得的各个跳转概率进行相乘处理，获得所述地址的正常地址概率；

根据所述正常地址概率判断所述待识别订单是否为恶意订单。

第六方面，本发明提供了一种恶意订单的识别装置，所述装置包括：

20 接收单元，用于接收用户客户端发送的待识别订单；

计算单元，用于基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

25 处理单元，用于对获得的各个跳转概率进行相乘处理，获得所述地址的正常地址概率；

判断单元，用于根据所述正常地址概率判断所述待识别订单是否为恶意订单。

借由上述技术方案，本发明提供的恶意地址/恶意订单的识别系统、方法及装置，能够在服务器获取待识别地址以及由历史正常地址分析得到的地址层级跳转概率分布后，先对该待识别地址进行地址层级化处理，获得该待识别地址的各地址层级，然后利用
30 用获取的地址层级跳转概率分布，计算该待识别地址中每个地址层级跳转至相邻的下一

地址层级的跳转概率，并对各个跳转概率进行相乘处理，获得该待识别地址属于正常地址的概率，以便根据该概率判断待识别地址是否为恶意地址，或者根据该概率判断包括该待识别地址的订单是否为恶意订单。由此可知，与现有技术中粗滤地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史

5 正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构

10 不完整的地址的正常地址概率，并可以根据该正常地址概率来确定待识别地址是否为恶意地址，从而根据是否为恶意地址来确定待识别订单是否为恶意订单，进而提高了恶意地址/恶意订单识别的准确率。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够

15 更明显易懂，以下特举本发明的具体实施方式。

附图说明

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

20 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 示出了本发明实施例提供的一种恶意地址的识别系统示意图；

图 2 示出了本发明实施例提供的一种商家客户端侧选择界面示意图；

图 3 示出了本发明实施例提供的一种恶意地址的识别方法的流程图；

图 4 示出了本发明实施例提供的另一种恶意地址的识别方法的流程图；

25 图 5 示出了本发明实施例提供的恶意地址识别过程中服务器与客户端的交互图；

图 6 示出了本发明实施例提供的一种恶意地址的识别装置的组成框图；

图 7 示出了本发明实施例提供的另一种恶意地址的识别装置的组成框图；

图 8 示出了本发明实施例提供的一种恶意订单的识别方法的流程图；

图 9 示出了本发明实施例提供的一种恶意订单的识别装置的组成框图；

30 图 10 示出了本发明实施例提供的另一种恶意订单的识别装置的组成框图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本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，并且能够将本公开的范围完整的传达给本领域的技术人员。

为了提高识别恶意地址的准确率，本发明实施例提供了一种恶意地址的识别系统，如图 1 所示，系统包括用户客户端 11、服务器 12 和商家客户端 13；其中，

用户客户端 11 用于接收输入的待识别地址，并将待识别地址发送给服务器 12；

10 服务器 12 用于接收用户客户端 11 发送的待识别地址，并对待识别地址进行地址层级化处理，获得待识别地址的各地址层级；利用由历史正常地址分析得到的地址层级跳转概率分布，计算待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得待识别地址的正常地址概率，并将基于正常地址
15 概率进行恶意地址识别的识别结果发送给商家客户端 13；

商家客户端 13 用于接收并输出服务器 12 发送的识别结果。

本发明实施例提供的恶意地址的识别系统，能够在服务器接收到用户客户端发送的待识别地址后，先对该待识别地址进行地址层级化处理，获得该待识别地址的各地址层级，然后利用地址层级跳转概率分布，计算该待识别地址中每个地址层级跳转至相邻的
20 下一地址层级的跳转概率，并对各个跳转概率进行相乘处理，获得该待识别地址属于正常地址的概率，以便根据该概率判断待识别地址是否为恶意地址。由此可知，与现有技术中粗略地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地
25 址属于正常地址的概率，从而不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构不完整的地址的正常地址概率，并可以根据该正常地址概率来确定待识别地址是否为恶意地址，从而提高了恶意地址识别的准确率。

30 进一步的，服务器 12 用于当识别结果是待识别地址为恶意地址时，向商家客户端

13 发送预警提示信息；

商家客户端 13 用于接收并输出服务器 12 发送的预警提示信息。

进一步的，商家客户端 13 用于在接收到预警提示信息后，输出用于选择对待识别地址进行二次识别的识别结果的选择界面，并接收基于选择界面输入的、二次识别的识别结果，将二次识别的识别结果返回给服务器 12。

示例性的，如图 2 所示，当商家客户端接收到预警提示信息后，不仅会在界面显示该预警提示信息，还会显示一个供商家选择二次识别结果的选择界面，如该选择界面上可以有一个文本内容“请联系买家再次确认地址***是否为恶意地址”，以及两个选择按钮“是”和“否”，供用户选择。

10 需要说明的是，预警提示信息可以位于选择界面，也可以位于另一个界面。

进一步的，商家客户端 13 用于在未接收到预警提示信息的情况下，输出用于选择对待识别地址进行二次识别的识别结果的选择界面，并接收基于选择界面输入的、用于描述待识别地址为恶意地址的识别结果，并将携带恶意标识的待识别地址返回给服务器 12。

15 进一步的，依据上述系统实施例，本发明的另一个实施例还提供了一种恶意地址的识别方法，如图 3 所示，该方法主要包括：

201、接收用户客户端发送的待识别地址。

当用户下单成功后，用户客户端（即买家客户端）可以将订单上传给服务器，服务器接收到该订单后，能够对该订单进行恶意地址识别操作，并将订单以及订单的识别结果发送给商家客户端，以便商家根据识别结果对该订单进行相应处理。由于服务器接收到的待识别订单中往往会存在一些没有意义的数据，所以为了防止这些数据干扰待识别地址的识别，在获得待识别订单后，服务器需要对该待识别订单先进行预处理，然后再从预处理后的待识别订单中提取待识别地址。

25 因此，获取待识别地址的具体实现过程可以为：获取待识别订单；对待识别订单进行冗余处理以及格式化处理；从处理后的待识别订单中获取待识别地址。

其中，对待识别订单进行冗余处理以及格式化处理具体包括：

（1）对待识别订单的待识别地址中满足预设过滤条件的文字进行过滤。

30 由于用户可能会在地址中填写一些表情符号、无意义的英文字母以及其他一些无意义的数据，所以可以检测待识别地址中是否含有这些信息，若含有则将这些信息进行过滤。

(2) 对待识别订单中的脏数据进行过滤。

由于服务器在保存待识别订单时，可能会保存一些包含 HTML (HyperText Markup Language, 超文本标记语言) 文本、JSON (JavaScript Object Notation) 字符串等异常信息的脏数据，所以服务器可以将这些脏数据进行过滤。

5 (3) 根据预设格式化处理规则，对过滤后的待识别订单进行格式化处理。

由于用户在填写地址、电话等信息时，可能会添加空格、使用繁体字、使用拼音等，所以为了便于后续能够准确识别待识别地址，在对待识别订单进行过滤后，还需要进行去除空格、全角半角转换、繁简体转换、拼音转汉字等格式化操作，从而使得获得的地址具有统一的格式。

10 需要说明的是，在对历史正常地址以及历史恶意地址进行分析时，同样也需要进行上述预处理操作。

202、对待识别地址进行地址层级化处理，获得待识别地址的各地址层级。

因为地址的每一层级仅与邻近的上一层级有关，而与其他层级无关，所以地址层级结构符合马尔科夫性，从而可以利用条件随机场模型进行地址层级化处理。其中，对待
15 识别地址进行地址层级化处理的具体实现方式为：在获得待识别地址后，服务器可以通过条件随机场模型对待识别地址进行分词、地址层级标注，从而获得待识别地址的各个地址层级。例如，待识别地址为四川省成都市青羊区苏坡街道**家园 5 号楼 1 单元，则各地址层级分别为：“省：四川省、市：成都市、区县：青羊区、道路：苏坡街道、小区：**家园、楼号：5 号楼、单元号：1 单元”。

20 203、利用由历史正常地址分析得到的地址层级跳转概率分布，计算待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率。

其中，地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率。由于历史正常地址为商家送货成功的地址，所以服务器在获得大量的历史正常地址后，可以对历史正常地址的地址层级跳转情况进行统计与分析，从中获得地址层级跳
25 转概率分布，以便通过地址层级跳转概率分布确定待识别地址的各地址层级之间的跳转情况。

当获得待识别地址的各地址层级后，服务器可以利用地址层级跳转概率分布计算出待识别地址中相邻地址层级的跳转概率，即第 N 层级跳转至第 N+1 层级的概率。例如，在获得待识别地址的各地址层级“省：四川省、市：成都市、区县：青羊区、道路：苏
30 坡街道、小区：**家园、楼号：5 号楼、单元号：1 单元”后，可以利用地址层级跳转

概率分布，获得“四川省跳转至成都市的概率、成都市跳转至青羊区的概率、青羊区跳转至苏坡街道的概率、苏坡街道跳转至**家园的概率、**家园跳转至5号楼的概率、以及5号楼跳转至1单元的概率”。

204、对获得的各个跳转概率进行相乘处理，获得待识别地址的正常地址概率。

- 5 在对历史正常地址的地址层级跳转概率进行训练时，可以利用全国范围内大量地址进行训练，并在获得待识别地址各地址层级的跳转概率后，可以将这些跳转概率相乘，获得待识别地址属于正常地址的概率。

在实际应用中，有的恶意地址可能是由多个省内的不同地方顺序拼凑而成，例如，上海市闸北区龙岗区龙岗镇龙岗街道高科技工业园区内深圳***有限公司，其中，“上海市闸北区”属于上海市地址，“龙岗区龙岗镇龙岗街道高科技工业园区内深圳***有限公司”属于广东省地址。因此，当利用全国范围大量正常地址进行训练时，只有在闸北区到龙岗区这个地址层级间的跳转是异常的，而其他都是正常跳转，从而获得的整个地址属于正常地址的概率较大，进而将其误判为正常地址；而若单独利用上海市内海量历史正常地址进行训练，则整个地址只有上海市到闸北区的跳转是正常的，而其他地址层级间的跳转都是异常的，从而获得整个地址属于恶意地址的概率较大，进而将其确定为恶意地址。因此，在增加省份这一变量后，恶意地址识别的准确率得到提高。

10

15

在实际应用中，在增加省份这一变量后，计算待识别地址属于正常地址的概率计算公式可以为：

$$P(S/C) = P(w_1 w_2 \dots w_n / C) = P(w_1 / C) \prod_{i=1}^{i=n-1} P(w_{i+1} / w_i, C), \text{ 其中, } S \text{ 表示待识别地址,}$$

20 w_i 表示待识别地址中的第 i 地址层级, C 表示待识别地址所属省份。

本发明实施例提供的恶意地址的识别方法，能够在获取待识别地址后，先对该待识别地址进行地址层级化处理，获得该待识别地址的各地址层级，然后利用地址层级跳转概率分布，计算该待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，并对各个跳转概率进行相乘处理，获得该待识别地址属于正常地址的概率，以便根据该概率判断待识别地址是否为恶意地址。由此可知，与现有技术中粗略地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而

25

不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构不完整的地址的正常地址概率，并可以根据该正常地址概率来确定待识别地址是否为恶意地址，从而提高了恶意地址识别的准确率。

进一步的，在获得待识别地址属于正常地址的概率后，可以根据预设识别规则以及待识别地址的正常地址概率，判断待识别地址是否为恶意地址。

具体的，在获得待识别地址的正常地址概率后，可以直接利用正常地址概率判断待识别地址是否为恶意地址，也可以对待识别地址对应的其他特征进行分析，然后根据正常地址概率以及其他特征综合判断待识别地址是否为恶意地址（如下述步骤 305 至 307 所述）。其中，直接利用正常地址概率判断待识别地址是否为恶意地址的具体实现方式为：判断待识别地址的正常地址概率是否大于预设概率阈值；若待识别地址的正常地址概率大于预设概率阈值，则确定待识别地址为正常地址；若待识别地址的正常地址概率小于或等于预设概率阈值，则确定待识别地址为恶意地址。

此外，当服务器获得识别结果后，可以将该识别结果发送给商家客户端，以便商家客户端接收并显示识别结果，供商家根据识别结果确定是否发货。

进一步的，依据上述实施例，本发明的另一个实施例还提供了一种恶意地址的识别方法，如图 4 所示，该方法主要包括：

301、接收用户客户端发送的待识别地址。

302、对待识别地址进行地址层级化处理，获得待识别地址的各地址层级。

303、利用由历史正常地址分析得到的地址层级跳转概率分布，计算待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率。

304、对获得的各个跳转概率进行相乘处理，获得待识别地址的正常地址概率。

305、从待识别地址对应的待识别订单和/或待识别订单对应的历史订单中提取用于识别待识别地址是否为恶意地址的预设识别特征。

具体的，预设识别特征包括以下任意一项或者任意几项的组合：地址文本信息特征、历史购物行为特征、订单特征以及交叉特征。

相应的，本步骤可以具体细化为下述步骤 a-d：

(a) 从待识别地址中提取对应的地址文本信息特征。

其中，地址文本信息特征包括：是否包括预设长度的数字、是否包括预设敏感词以

及是否包括广告信息等。其中，预设长度包括手机号长度、座机号长度、QQ号长度等。

由于用户可能会为了辱骂商家或者为自己、自己的商品打广告而在地址中填写一些辱骂信息、手机号、广告信息等，并且填写这些内容的用户可能会填写一个恶意地址，所以可以从待识别地址中提取地址文本信息特征，以便从该维度分析待识别地址是否为

5 恶意地址。

(b) 从待识别订单对应的历史订单中提取历史购物行为特征。

由于用户的历史购物行为能够反映其是否可能会填写一个恶意地址，例如经常与商家发生纠纷、经常无故退款、交易成功率较低的用户填写恶意地址的可能性较大，而从未与商家发生纠纷、从未退过款、交易成功率较高的用户填写恶意地址的可能性较小，

10 所以可以从待识别订单对应的历史订单中提取历史购物行为特征，并将该特征作为判断待识别地址是否为恶意地址的一个维度。

此外，在实际应用中，历史购物行为特征主要包括：预设时间段内支付订单数、预设时间段内支付总额、预设时间段内的退款发起总量、预设时间段内交易成功率、预设时间段内纠纷商家数、预设时间段内投诉发起率、预设时间段内退款纠纷占比等。其中，

15 各个历史购物行为特征的预设时间段可以相同，也可以不同。

(c) 从待识别订单中提取对应的订单特征。

具体的，订单特征包括：待识别订单中的电话号码是否正常、待识别地址的使用次数是否大于预设使用阈值、待识别订单对应的店铺的相关状态以及待识别订单到对应的商品的相关状态。其中，店铺的相关状态包括：店铺的开店时间、最近时间段内店铺评分的波动、店铺被恶意攻击的次数等；商品的相关状态包括：商品的销量、商品的价格、商品是否热门等。

20

由于用户在填写地址时，可能会故意填写错误的电话号码，或者填写不曾使用过的新地址，并且恶意行为往往集中在大商家或者热门商品上，所以服务器可以从待识别订单提取这些订单特征，并通过订单特征这一维度来分析待识别地址是否为恶意地址。

25 (d) 根据地址文本信息特征、历史购物行为特征、订单特征以及待识别地址的正常地址概率中至少两项的组合，获取待识别地址对应的交叉特征。

在实际应用中，将地址文本信息特征、历史购物行为特征、订单特征以及待识别地址的正常地址概率这些基本特征进行交叉组合，可以产生更抽象的特征描述，例如将地址文本信息特征与订单特征进行交叉组合，可以获得待识别地址中不仅没有包含无意义的文本描述（即地址中没有携带电话号码、QQ号、预设敏感词、广告信息等信息），且

30

该地址为用户的常用地址。因此，可以将待识别地址对应的交叉特征作为识别恶意地址的又一个维度。

306、获取通过历史订单训练的预设识别模型。

5 具体的，服务器训练预设识别模型的实现方式可以为：先获取历史订单；然后根据地址层级跳转概率分布，获得历史订单中携带的历史地址的正常地址概率；再从历史订单中提取预设识别特征；最后通过各个历史地址的正常地址概率以及对应的预设识别特征训练预设识别模型。

其中，历史订单中包括预设比例的历史正常订单和历史恶意订单，且当历史正常订单与历史恶意订单的比例大约为 4: 1 时，恶意地址识别的准确率相对较高。

10 需要说明的是，在实际应用中，本步骤需要训练的预设识别模型可以为 GBDT (Gradient Boosting Decision Tree, 梯度提升决策树) 模型，也可以为其他模型，例如 SVM (Support Vector Machine, 支持向量机) 模型、LR (Logistic Regression, 逻辑回归) 模型、神经网络模型等。

15 307、根据待识别地址的正常地址概率、预设识别特征以及预设识别模型，判断待识别地址是否为恶意地址。

在获得待识别地址的正常地址概率以及预设识别特征之后，服务器可以将这些特征输入到预设识别模型中进行识别，以便预设识别模型可以对这些特征进行综合分析，获得待识别地址最终属于正常地址的概率或者恶意地址的概率，并根据预设正常概率阈值或者预设恶意地址概率阈值来确定该待识别地址是否为恶意地址。

20 308、若判断待识别地址为恶意地址，则向商家客户端发送预警提示信息，以便商家客户端接收并输出预警提示信息。

当服务器判断待识别地址为恶意地址后，为了避免商家因恶意地址而造成经济、信誉等损失，服务器在向商家客户端发送待识别订单的同时，可以向其发送用于指示地址可能为恶意地址的预警提示信息，商家接收到该预警提示信息后，可以根据订单中的电
25 话与买家进行联系，从而判断该地址是否确实为恶意地址；若商家确定该地址为恶意地址，则可以拒绝发货，若商家确定该地址为正常地址，而非恶意地址，则可以放心发货。

此外，若服务器判断该待识别地址为正常地址，则可以仅向商家客户端发送待识别订单，而无需发送预警提示信息；当商家发现接收到的订单没有预警提示信息时，会直接根据订单中的地址进行发货。然而，服务器可能会将恶意地址误判为正常地址，因此，
30 当商家在实际发货过程中发现地址无法送达时，商家可以在商家客户端中选择地址为恶

意地址的按钮，以便商家客户端将携带恶意标识的待识别地址发送给服务器，并在服务器接收到携带恶意标识的待识别地址后，对历史正常地址库、历史恶意地址库进行更新，以及对预设识别模型进行重新训练。

309、接收商家客户端发送的、基于预警提示信息对待识别地址进行二次识别的识别结果。

在实际应用中，当商家确定待识别地址为恶意地址时，可以在预警工具的页面（或者上述系统实施例中提及的选择界面）中选择用于指示确定为恶意地址的按钮，以便商家客户端将携带恶意标识的待识别地址发送给服务器；当商家确定待识别地址是正常地址而非恶意地址时，可以在预警工具的页面中选择用于指示确定为正常地址的按钮，以便商家客户端将携带正常标识的待识别地址发送给服务器。

310、若识别结果是待识别地址为正常地址，则更新历史正常地址库、历史恶意地址库以及预设识别模型。

当商家客户端发送的二次识别的识别结果是待识别地址为正常地址，则服务器确定其判断错误，并立即更新历史正常地址库、历史恶意地址库，然后对地址层级跳转概率分布进行重新分析，对预设识别模型进行重新训练。

此外，以 GBDT 模型为例，本发明实施例中服务器与客户端之间的交互过程可以如图 5 所示，且通过上述实施例可知，本发明实施例不仅能够基于地址层级跳转概率分布初步获得待识别地址属于正常地址的概率，还能够从历史订单以及待识别订单中获得地址文本信息特征、历史购物行为特征、订单特征以及交叉特征等其他预设识别特征，并将待识别地址的正常地址概率以及这些预设识别特征输入至 GBDT 模型（或者其他识别模型）中进行综合分析，判断待识别地址是否为恶意地址，从而进一步提高了恶意地址识别的准确率。此外，当服务器最终确定该待识别地址为恶意地址时，还能够向商家客户端发送预警提示信息，从而使得商家能够通过与买家联系核实该地址是否为恶意地址，来决定是否发货，进而避免产生损失。进一步的，在商家根据实际情况确定地址是否为恶意地址后，还能够在商家客户端上选择对应的确定按钮，以便商家客户端将实际确定结果反馈给服务器，从而服务器可以根据商家客户端的反馈来确定其是否发生误判，若发生误判，则可以及时对 GBDT 模型进行重新训练，使 GBDT 模型更加完善，并由此提高了后续恶意地址识别的准确率。

进一步的，依据上述方法实施例，本发明的另一个实施例还提供了一种恶意地址的识别装置，如图 6 所示，该装置主要包括：接收单元 41、第一处理单元 42、计算单元

43、第二处理单元 44。其中，

接收单元 41，用于接收用户客户端发送的待识别地址；

第一处理单元 42，用于对待识别地址进行地址层级化处理，获得待识别地址的各地
址层级；

5 计算单元 43，用于利用由历史正常地址分析得到的地址层级跳转概率分布，计算待
识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，地址层级跳转概率分
布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

第二处理单元 44，用于对计算单元 43 获得的各个跳转概率进行相乘处理，获得待
识别地址的正常地址概率。

10 本发明实施例提供的恶意地址的识别装置，能够在获取待识别地址后，先对该待识
别地址进行地址层级化处理，获得该待识别地址的各地址层级，然后利用地址层级跳转
概率分布，计算该待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，
并对各个跳转概率进行相乘处理，获得该待识别地址属于正常地址的概率，以便根据该
15 概率判断待识别地址是否为恶意地址。由此可知，与现有技术中粗滤地通过恶意关键词、
黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史
正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址
各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而
不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常
20 地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词
的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构
不完整的地址的正常地址概率，并可以根据该正常地址概率来确定待识别地址是否为恶
意地址，从而提高了恶意地址识别的准确率。

进一步的，如图 7 所示，该装置还包括：

判断单元 45，用于在获得所述待识别地址的正常地址概率之后，根据预设识别规则
25 以及待识别地址的正常地址概率，判断待识别地址是否为恶意地址。

进一步的，如图 7 所示，判断单元 45 包括：

提取模块 451，用于从待识别地址对应的待识别订单和/或待识别订单对应的历史订
单中提取用于识别待识别地址是否为恶意地址的预设识别特征；

获取模块 452，用于获取通过历史订单训练的预设识别模型；

30 第一判断模块 453，用于根据待识别地址的正常地址概率、预设识别特征以及预设

识别模型，判断待识别地址是否为恶意地址。

进一步的，如图 7 所示，提取模块 451 包括：

第一提取子模块 4511，用于从待识别地址中提取对应的地址文本信息特征；

第二提取子模块 4512，用于从待识别订单对应的历史订单中提取历史购物行为特

5 征；

第三提取子模块 4513，用于从待识别订单中提取对应的订单特征。

进一步的，如图 7 所示，提取模块 451 还包括：

获取子模块 4514，用于根据地址文本信息特征、历史购物行为特征、订单特征以及待识别地址的正常地址概率中至少两项的组合，获取待识别地址对应的交叉特征。

10 进一步的，第一提取子模块 4511 提取的地址文本信息特征包括：是否包括预设长度的数字、是否包括预设敏感词以及是否包括广告信息；

第三提取子模块 4513 提取的订单特征包括：待识别订单中的电话号码是否正常、待识别地址的使用次数是否大于预设使用阈值、待识别订单对应的店铺的相关状态以及待识别订单到对应的商品的相关状态。

15 进一步的，获取模块 452 还用于获取历史订单，历史订单中包括预设比例的历史正常订单和历史恶意订单；

获取模块 452 还用于根据条件随机场模型以及地址层级跳转概率分布，获得历史订单中携带的历史地址的正常地址概率；

提取模块 451 还用于从历史订单中提取预设识别特征；

20 如图 7 所示，判断单元 45 还包括：

训练模块 454，用于通过各个历史地址的正常地址概率以及对应的预设识别特征训练预设识别模型。

进一步的，如图 7 所示，判断单元 45 包括：

第二判断模块 455，用于判断待识别地址的正常地址概率是否大于预设概率阈值；

25 确定模块 456，用于当第二判断模块的判断结果为待识别地址的正常地址概率大于预设概率阈值时，确定待识别地址为正常地址，当第二判断模块的判断结果为待识别地址的正常地址概率小于或等于预设概率阈值时，确定待识别地址为恶意地址。

进一步的，如图 7 所示，该装置还包括：

30 第一发送单元 46，用于将判断待识别地址是否为恶意地址的识别结果发送给商家客户端，以便商家客户端接收并输出识别结果。

进一步的，如图 7 所示，该装置还包括：

第二发送单元 47，用于当判断单元 45 判断待识别地址为恶意地址时，向商家客户端发送预警提示信息，以便所述商家客户端接收并输出所述预警提示信息；

接收单元 41，用于接收商家客户端发送的、基于预警提示信息对待识别地址进行二次识别的识别结果；

第一更新单元 48，用于当第一接收单元 48 接收的识别结果是待识别地址为正常地址时，更新历史正常地址库、历史恶意地址库以及预设识别模型。

进一步的，接收单元 41，用于接收商家客户端发送的携带恶意标识的待识别地址；如图 7 所示，该装置还包括：

第二更新单元 49，用于更新历史正常地址库、历史恶意地址库以及预设识别模型。

进一步的，待识别地址为在第一处理单元 42 对待识别订单进行冗余处理以及格式化处理后获得的地址。

进一步的，如图 7 所示，第一处理单元 42 包括：

过滤模块 421，用于对待识别订单的待识别地址中满足预设过滤条件的文字进行过滤；

过滤模块 421 还用于对待识别订单中的脏数据进行过滤；

处理模块 422，用于根据预设格式化处理规则，对过滤模块 421 过滤后的待识别订单进行格式化处理。

本发明实施例提供的恶意地址的识别装置，不仅能够基于地址层级跳转概率分布初步获得待识别地址属于正常地址的概率，还能够从历史订单以及待识别订单中获得地址文本信息特征、历史购物行为特征、订单特征以及交叉特征等其他预设识别特征，并将待识别地址的正常地址概率以及这些预设识别特征输入至预设识别模型中进行综合分析，判断待识别地址是否为恶意地址，从而进一步提高了恶意地址识别的准确率。此外，当服务器最终确定该待识别地址为恶意地址时，还能够向商家客户端发送预警提示信息，从而使得商家能够通过与买家联系核实该地址是否为恶意地址，来决定是否发货，进而避免产生损失。进一步的，在商家根据实际情况确定地址是否为恶意地址后，还能够商家客户端上选择对应的确定按钮，以便商家客户端将实际确定结果反馈给服务器，从而服务器可以根据商家客户端的反馈来确定其是否发生误判，若发生误判，则可以及时对预设识别模型进行重新训练，使预设识别模型更加完善，并由此提高了后续恶意地址识别的准确率。

进一步的，为了提高识别恶意订单的准确率，本发明的另一个实施例提供了一种恶意订单的识别系统，该系统包括用户客户端、服务器和商家客户端；其中，

用户客户端用于接收输入的待识别订单，并将待识别订单发送给服务器；

服务器用于接收用户客户端发送的待识别订单，并基于由历史正常地址分析得到的地址层级跳转概率分布，计算待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得地址的正常地址概率；根据正常地址概率判断待识别订单是否为恶意订单，并将判断结果发送给商家客户端；

商家客户端用于接收并显示服务器发送的判断结果。

10 本发明实施例提供的恶意订单的识别系统，在服务器接收到用户客户端发送的待识别订单后，先利用地址层级跳转概率分布，计算该待识别订单中的地址属于正常地址的概率，然后再利用该概率判断该待识别订单是否为恶意订单。由此可知，与现有技术中粗滤地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史正常地址中各地址层级之间相关性进行统计与分析，并利
15 用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构不完整的地址的正常地址概率，并根据正常地址概率确定地址
20 是否为恶意地址，从而提高了识别恶意地址的准确率，进而提高了识别恶意订单的准确率。

进一步的，依据上述实施例中提及的恶意订单的识别系统，本发明的另一个实施例提供了一种恶意订单的识别方法，如图 8 所示，该方法主要包括：

501、接收用户客户端发送的待识别订单。

25 当用户下单成功后，用户客户端可以将订单上传给服务器，服务器接收到该订单后，能够对该订单进行恶意地址识别操作。

502、基于由历史正常地址分析得到的地址层级跳转概率分布，计算待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率。

其中，地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转
30 概率。

具体的，服务器可以先对待识别订单的地址进行地址层级化处理，获得地址的各地地址层级（详见上述步骤 202）；然后基于地址层级跳转概率分布，计算每个地址层级跳转至相邻的下一地址层级的跳转概率（详见上述步骤 203）。

503、对获得的各个跳转概率进行相乘处理，获得地址的正常地址概率。

5 本步骤的具体实现方式与上述步骤 204 相同，在此不再赘述。

504、根据正常地址概率判断待识别订单是否为恶意订单。

具体的，服务器可以先根据正常地址概率判断待识别订单的地址是否为恶意地址；若待识别订单的地址为恶意地址，则确定待识别订单为恶意订单；若待识别订单的地址为正常地址，则确定待识别订单为正常订单。

10 其中，根据正常地址概率判断待识别订单的地址是否为恶意地址的具体实现方式与上述“恶意地址的识别方法”的实施例中的具体实现方式相同，在此不再赘述。

进一步的，由于在实际应用中，恶意用户除了通过添加恶意地址的方式给商家带来困扰外，往往还通过其他方式困扰商家，例如填写错误的电话号码，使得商家无法与其进行联系，所以当判断待识别订单的地址为正常地址时，还需要再判断待识别订单中的电话号码是否正常。若电话号码异常，则确定待识别订单为恶意订单；若电话号码正常，则确定待识别订单为正常订单。

15

其中，判断电话号码是否异常的方法可以为：构建一个正常电话号码库，将待识别电话号码与正常电话号码库进行匹配，若匹配失败，则确定待识别电话号码异常，若匹配成功，则确定待识别电话号码正常。

20 本发明实施例提供的恶意订单的识别方法，在服务器接收到用户客户端发送的待识别订单后，先利用地址层级跳转概率分布，计算该待识别订单中的地址属于正常地址的概率，然后再利用该概率判断该待识别订单是否为恶意订单。由此可知，与现有技术中粗略地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地址概率以及地址层级结构不完整的地址的正常地址概率，并根据正常地址概率确定地址

25

30 是否为恶意地址，从而提高了识别恶意地址的准确率，进而提高了识别恶意订单的准确

率。

进一步的，依据图 8 所示的方法，本发明的另一个实施例提供了一种恶意订单的识别装置，如图 9 所示，该装置主要包括：

接收单元 61，用于接收用户客户端发送的待识别订单；

5 计算单元 62，用于基于由历史正常地址分析得到的地址层级跳转概率分布，计算待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

处理单元 63，用于对获得的各个跳转概率进行相乘处理，获得地址的正常地址概率；

判断单元 64，用于根据正常地址概率判断待识别订单是否为恶意订单。

10 进一步的，如图 10 所示，判断单元 64 包括：

判断模块 641，用于根据正常地址概率判断待识别订单的地址是否为恶意地址；

确定模块 642，用于当待识别订单的地址为恶意地址时，确定待识别订单为恶意订单。

进一步的，判断模块 641 还用于当待识别订单的地址为正常地址时，判断待识别订
15 单中的电话号码是否正常；

确定模块 642 还用于当电话号码异常时，确定待识别订单为恶意订单。

进一步的，如图 10 所示，计算单元 62 包括：

处理模块 621，用于对待识别订单的地址进行地址层级化处理，获得地址的各地址
层级；

20 计算模块 622，用于基于地址层级跳转概率分布，计算每个地址层级跳转至相邻的下一地址层级的跳转概率。

本发明实施例提供的恶意订单的识别装置，在服务器接收到用户客户端发送的待识别订单后，先利用地址层级跳转概率分布，计算该待识别订单中的地址属于正常地址的概率，然后再利用该概率判断该待识别订单是否为恶意订单。由此可知，与现有技术中
25 粗滤地通过恶意关键词、黑白名单或者地址层级结构来判断待识别地址是否为恶意地址相比，本发明通过对历史正常地址中各地址层级之间相关性进行统计与分析，并利用分析结果来判断待识别地址各地址层级的跳转概率，再由跳转概率获得整个待识别地址属于正常地址的概率，从而不仅能够获得包含恶意关键词的地址的正常地址概率、包含在黑白名单中的地址的正常地址概率以及地址层级结构完整的地址的正常地址概率，还能
30 够获得不包含恶意关键词的地址的正常地址概率、不包含在黑白名单中的地址的正常地

址概率以及地址层级结构不完整的地址的正常地址概率，并根据正常地址概率确定地址是否为恶意地址，从而提高了识别恶意地址的准确率，进而提高了识别恶意订单的准确率。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中沒有详述的部分，
5 可以参见其他实施例的相关描述。

可以理解的是，上述方法、装置及系统中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

10 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，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。

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。

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
20 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。

25 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地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，以及此外可以把它們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
30 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
5 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恶意地址/恶意订单
10 的识别系统、方法及装置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载得到，或者
在载体信号上提供，或者以任何其他形式提供。

15 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
20 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. 一种恶意地址的识别系统，其特征在于，所述系统包括用户客户端、服务器和商家客户端；其中，

所述用户客户端用于接收输入的待识别地址，并将所述待识别地址发送给所述服务器；

所述服务器用于接收所述用户客户端发送的所述待识别地址，并对所述待识别地址进行地址层级化处理，获得所述待识别地址的各地址层级；利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得所述待识别地址的正常地址概率，并将基于所述正常地址概率进行恶意地址识别的识别结果发送给所述商家客户端；

所述商家客户端用于接收并输出所述服务器发送的所述识别结果。

2. 根据权利要求 1 所述的系统，其特征在于，所述服务器用于当所述识别结果是所述待识别地址为恶意地址时，向所述商家客户端发送预警提示信息；

所述商家客户端用于接收并输出所述服务器发送的所述预警提示信息。

3. 根据权利要求 2 所述的系统，其特征在于，所述商家客户端用于在接收到所述预警提示信息后，输出用于选择对所述待识别地址进行二次识别的识别结果的选择界面，并接收基于所述选择界面输入的、二次识别的识别结果，将所述二次识别的识别结果返回给所述服务器。

4. 根据权利要求 2 或 3 所述的系统，其特征在于，所述商家客户端用于在未接收到所述预警提示信息的情况下，输出用于选择对所述待识别地址进行二次识别的识别结果的选择界面，并接收基于所述选择界面输入的、用于描述所述待识别地址为恶意地址的识别结果，并将携带恶意标识的所述待识别地址返回给所述服务器。

5. 一种恶意地址的识别方法，其特征在于，所述方法包括：

接收用户客户端发送的待识别地址；

对所述待识别地址进行地址层级化处理，获得所述待识别地址的各地址层级；

利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

对获得的各个跳转概率进行相乘处理，获得所述待识别地址的正常地址概率。

6. 根据权利要求 5 所述的方法，其特征在于，在获得所述待识别地址的正常地址概率之后，所述方法还包括：

5 根据预设识别规则以及所述待识别地址的正常地址概率，判断所述待识别地址是否为恶意地址。

7. 根据权利要求 6 所述的方法，其特征在于，根据预设识别规则以及所述待识别地址的正常地址概率，判断所述待识别地址是否为恶意地址包括：

从所述待识别地址对应的待识别订单和/或所述待识别订单对应的历史订单中提取用于识别所述待识别地址是否为恶意地址的预设识别特征；

10 获取通过历史订单训练的预设识别模型；

根据所述待识别地址的正常地址概率、所述预设识别特征以及所述预设识别模型，判断所述待识别地址是否为恶意地址。

8. 根据权利要求 7 所述的方法，其特征在于，从所述待识别地址对应的待识别订单和/或所述待识别订单对应的历史订单中提取用于识别所述待识别地址是否为恶意地址的预设识别特征包括：

从所述待识别地址中提取对应的地址文本信息特征；

和/或，从所述待识别订单对应的历史订单中提取历史购物行为特征；

和/或，从所述待识别订单中提取对应的订单特征。

9. 根据权利要求 8 所述的方法，其特征在于，从所述待识别地址对应的待识别订单和/或所述待识别订单对应的历史订单中提取用于识别所述待识别地址是否为恶意地址的预设识别特征还包括：

根据所述地址文本信息特征、所述历史购物行为特征、所述订单特征以及所述待识别地址的正常地址概率中至少两项的组合，获取所述待识别地址对应的交叉特征。

10. 根据权利要求 8 所述的方法，其特征在于，所述地址文本信息特征包括：是否
25 包括预设长度的数字、是否包括预设敏感词以及是否包括广告信息；

所述订单特征包括：所述待识别订单中的电话号码是否正常、所述待识别地址的使用次数是否大于预设使用阈值、所述待识别订单对应的店铺的相关状态以及所述待识别订单到对应的商品的相关状态。

11. 根据权利要求 7 所述的方法，其特征在于，在获取通过历史订单训练的预设识别模型之前，所述方法还包括：

获取历史订单，所述历史订单中包括预设比例的历史正常订单和历史恶意订单；

根据所述地址层级跳转概率分布，获得所述历史订单中携带的历史地址的正常地址概率；

从所述历史订单中提取预设识别特征；

- 5 通过各个历史地址的正常地址概率以及对应的预设识别特征训练所述预设识别模型。

12. 根据权利要求 6 所述的方法，其特征在于，根据预设识别规则以及所述待识别地址的正常地址概率，判断所述待识别地址是否为恶意地址包括：

判断所述待识别地址的正常地址概率是否大于预设概率阈值；

- 10 若所述待识别地址的正常地址概率大于所述预设概率阈值，则确定所述待识别地址为正常地址；

若所述待识别地址的正常地址概率小于或等于所述预设概率阈值，则确定所述待识别地址为恶意地址。

13. 根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

- 15 将判断所述待识别地址是否为恶意地址的识别结果发送给商家客户端，以便所述商家客户端接收并输出所述识别结果。

14. 根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

若判断所述待识别地址为恶意地址，则向商家客户端发送预警提示信息，以便所述商家客户端接收并输出所述预警提示信息；

- 20 接收所述商家客户端发送的、基于所述预警提示信息对所述待识别地址进行二次识别的识别结果；

若所述识别结果是所述待识别地址为正常地址，则更新历史正常地址库、历史恶意地址库以及所述预设识别模型。

15. 根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

- 25 接收商家客户端发送的携带恶意标识的所述待识别地址；
更新历史正常地址库、历史恶意地址库以及所述预设识别模型。

16. 根据权利要求 5 所述的方法，其特征在于，所述待识别地址为在对待识别订单进行冗余处理以及格式化处理后获得的地址。

- 30 17. 根据权利要求 16 所述的方法，其特征在于，对待识别订单进行冗余处理以及格式化处理包括：

对所述待识别订单的待识别地址中满足预设过滤条件的文字进行过滤；

对所述待识别订单中的脏数据进行过滤；

根据预设格式化处理规则，对过滤后的待识别订单进行格式化处理。

18. 根据权利要求 5 至 17 中任一项所述的方法，其特征在于，对所述待识别地址
5 进行地址层级化处理包括：

基于条件随机场模型，对所述待识别地址进行地址层级化处理。

19. 一种恶意地址的识别装置，其特征在于，所述装置包括：

接收单元，用于接收用户客户端发送的待识别地址；

第一处理单元，用于对所述待识别地址进行地址层级化处理，获得所述待识别地址
10 的各地址层级；

计算单元，用于利用由历史正常地址分析得到的地址层级跳转概率分布，计算所述
待识别地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转
概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

第二处理单元，用于对所述计算单元获得的各个跳转概率进行相乘处理，获得所述
15 待识别地址的正常地址概率。

20. 一种恶意订单的识别系统，其特征在于，所述系统包括用户客户端、服务器和
商家客户端；其中，

所述用户客户端用于接收输入的待识别订单，并将所述待识别订单发送给所述服务
器；

20 所述服务器用于接收所述用户客户端发送的所述待识别订单，并基于由历史正常地
址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转
至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级
跳转至另一个地址层级的跳转概率；对获得的各个跳转概率进行相乘处理，获得所述地
址的正常地址概率；根据所述正常地址概率判断所述待识别订单是否为恶意订单，并将
25 判断结果发送给所述商家客户端；

所述商家客户端用于接收并显示所述服务器发送的所述判断结果。

21. 一种恶意订单的识别方法，其特征在于，所述方法包括：

接收用户客户端发送的待识别订单；

基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地
30 址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布

包括任意一个地址层级跳转至另一个地址层级的跳转概率；

对获得的各个跳转概率进行相乘处理，获得所述地址的正常地址概率；

根据所述正常地址概率判断所述待识别订单是否为恶意订单。

22. 根据权利要求 21 所述的方法，其特征在于，根据所述正常地址概率判断所述

5 待识别订单是否为恶意订单包括：

根据所述正常地址概率判断所述待识别订单的地址是否为恶意地址；

若所述待识别订单的地址为恶意地址，则确定所述待识别订单为恶意订单。

23. 根据权利要求 22 所述的方法，其特征在于，若所述待识别订单的地址为正常地址，则所述方法还包括：

10 判断所述待识别订单中的电话号码是否正常；

若所述电话号码异常，则确定所述待识别订单为恶意订单。

24. 根据权利要求 21 至 23 中任一项所述的方法，其特征在于，基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率包括：

15 对所述待识别订单的地址进行地址层级化处理，获得所述地址的各地址层级；

基于所述地址层级跳转概率分布，计算每个地址层级跳转至相邻的下一地址层级的跳转概率。

25. 一种恶意订单的识别装置，其特征在于，所述装置包括：

接收单元，用于接收用户客户端发送的待识别订单；

20 计算单元，用于基于由历史正常地址分析得到的地址层级跳转概率分布，计算所述待识别订单的地址中每个地址层级跳转至相邻的下一地址层级的跳转概率，所述地址层级跳转概率分布包括任意一个地址层级跳转至另一个地址层级的跳转概率；

处理单元，用于对获得的各个跳转概率进行相乘处理，获得所述地址的正常地址概率；

25 判断单元，用于根据所述正常地址概率判断所述待识别订单是否为恶意订单。

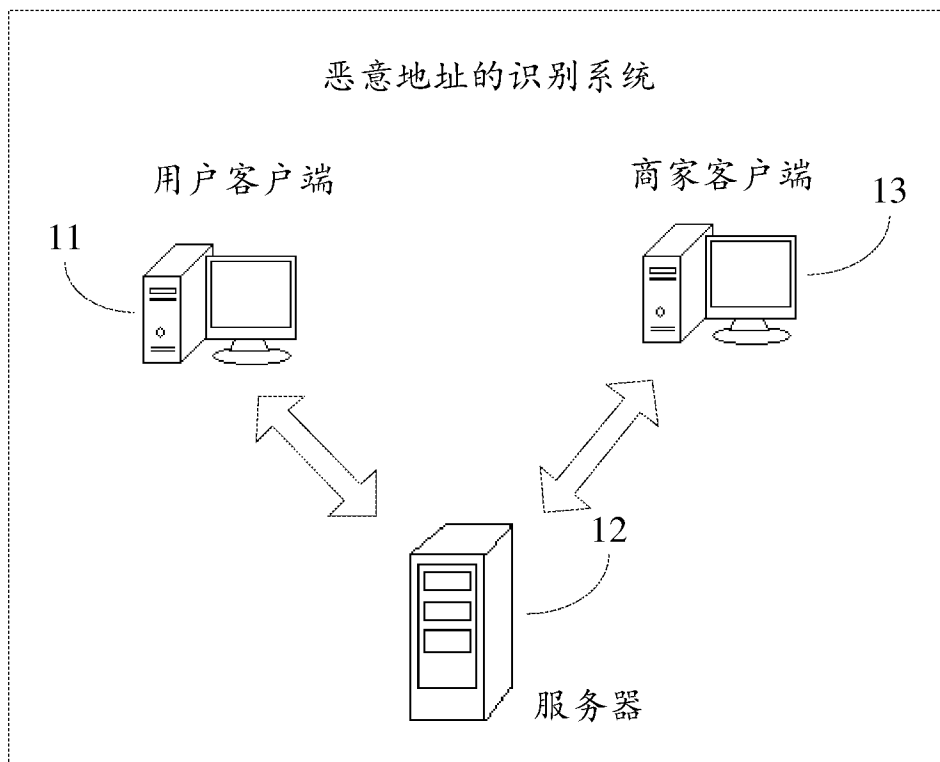


图 1

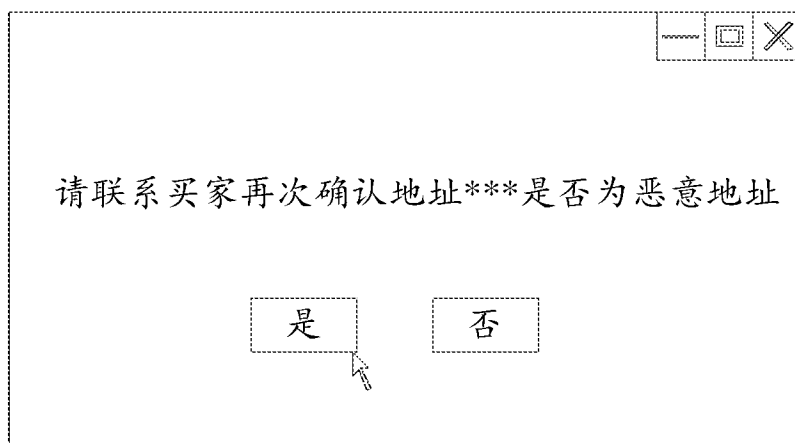


图 2

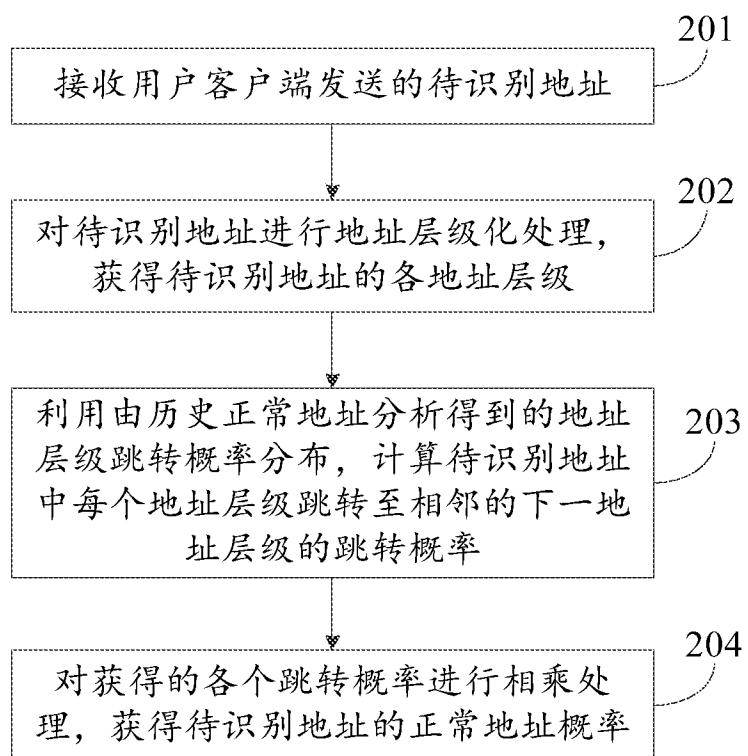


图 3

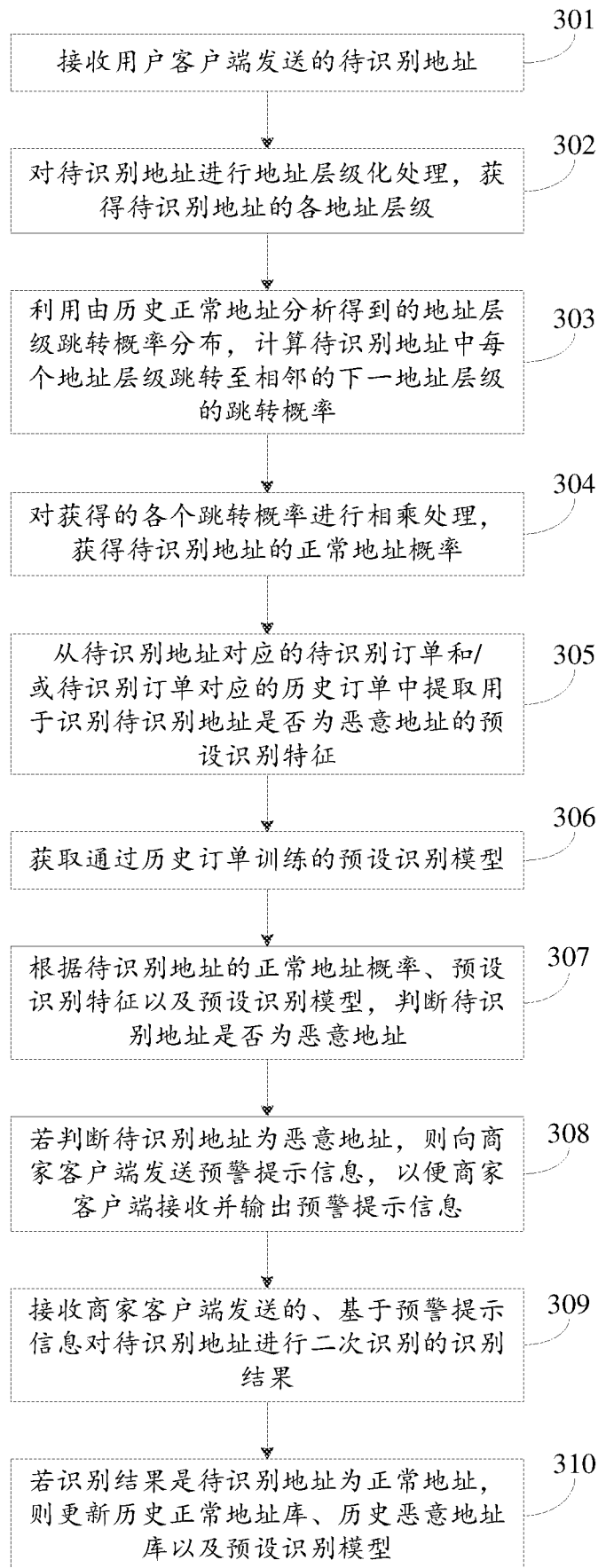


图 4

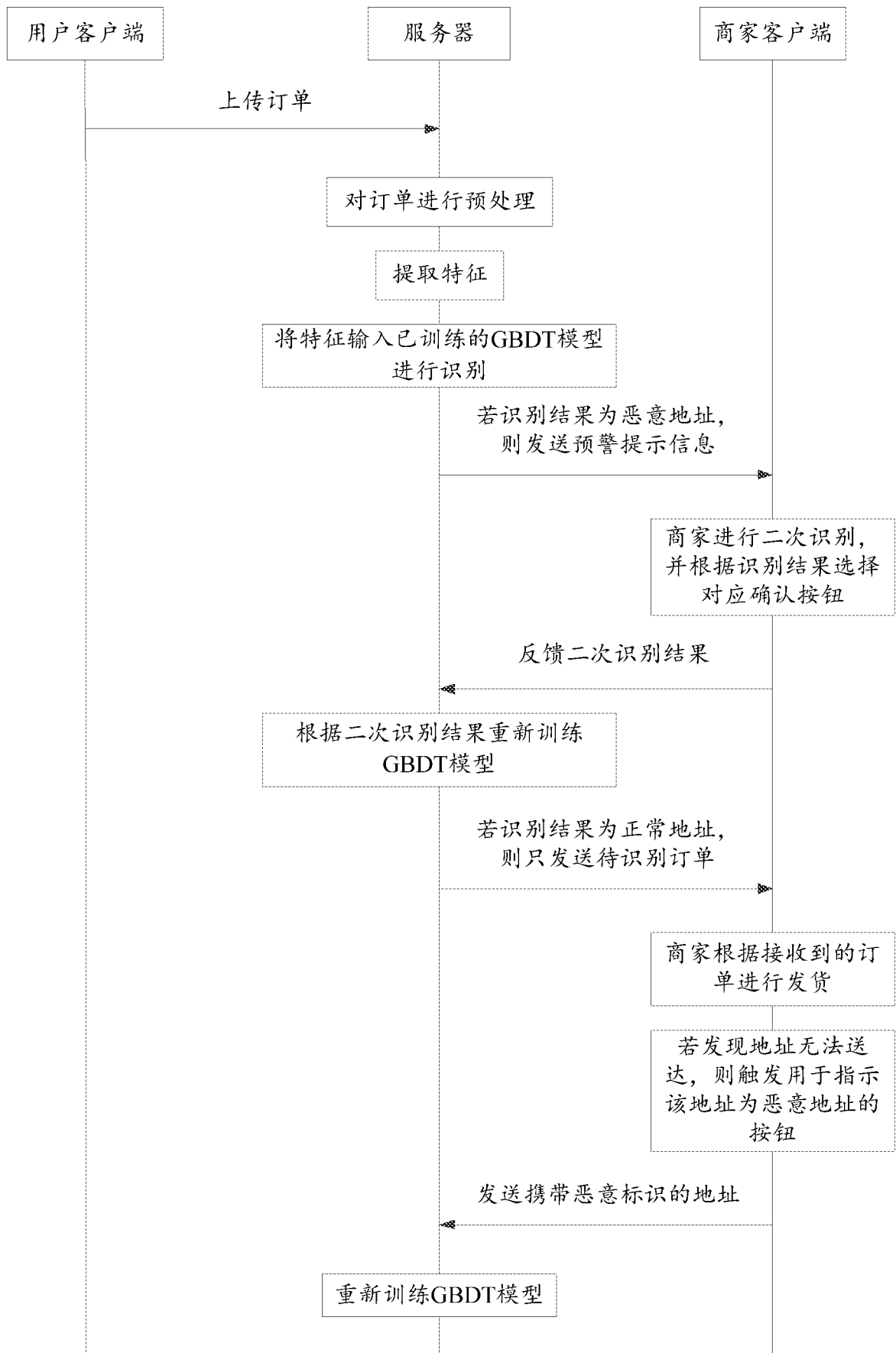


图 5

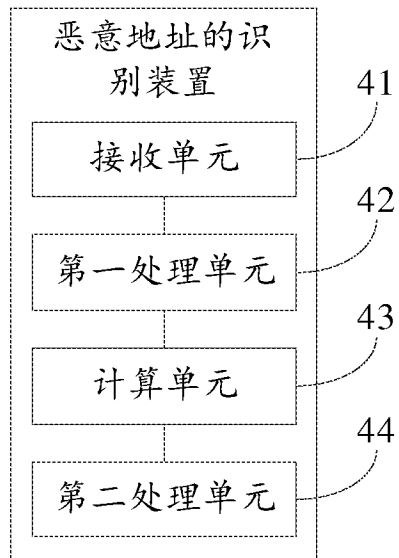


图 6

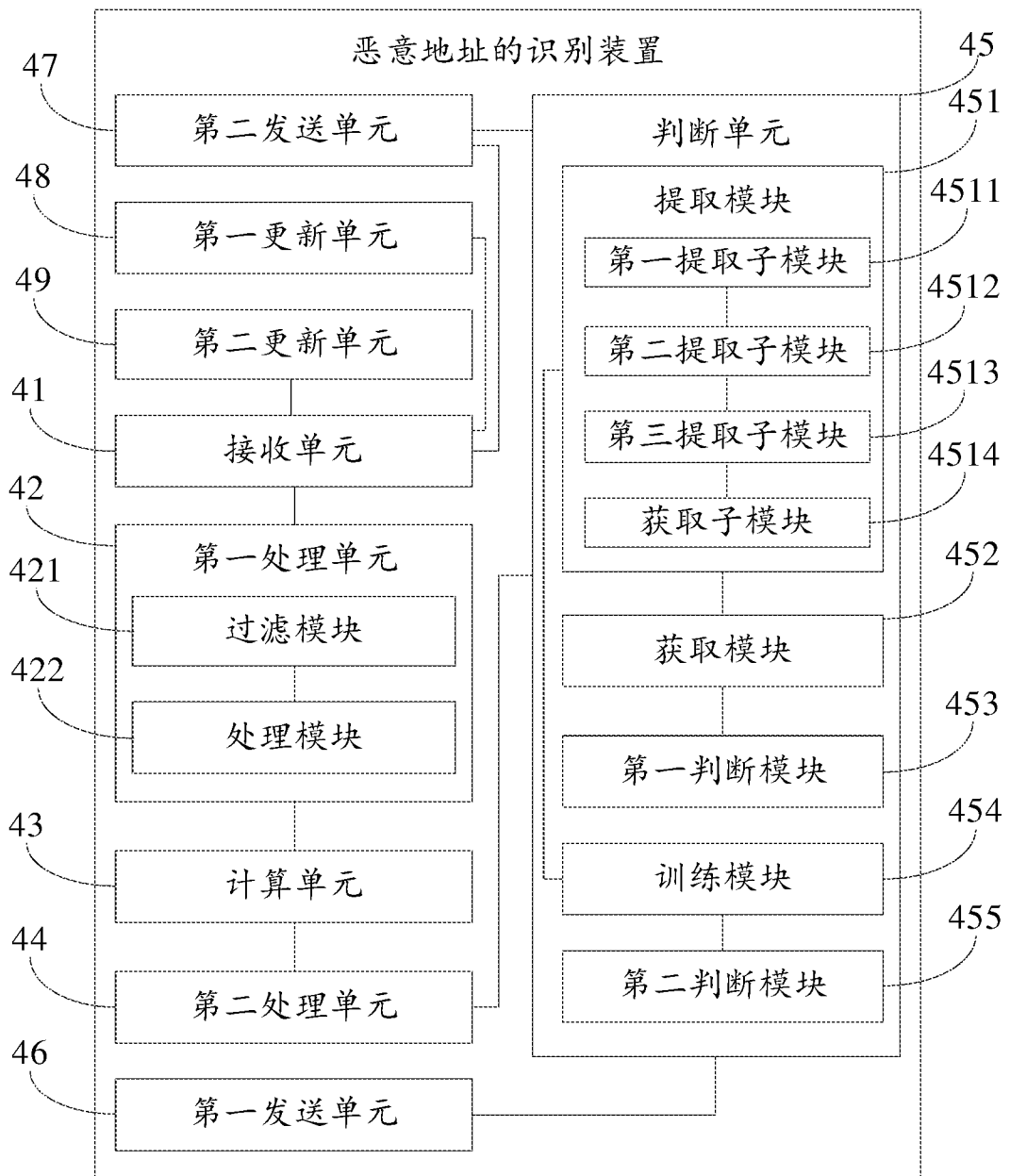


图 7

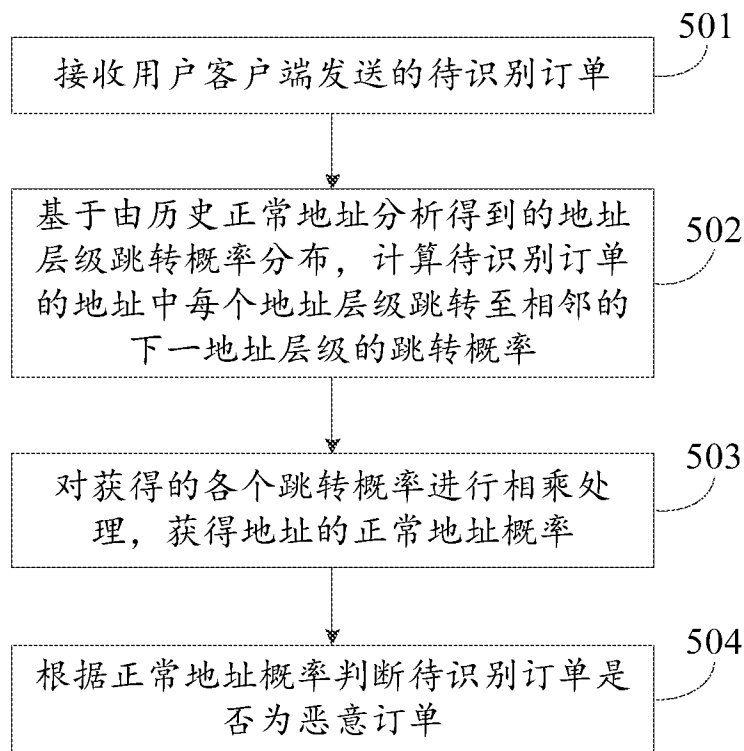


图 8

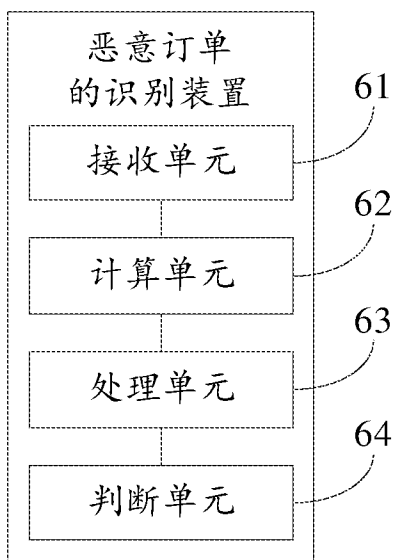


图 9

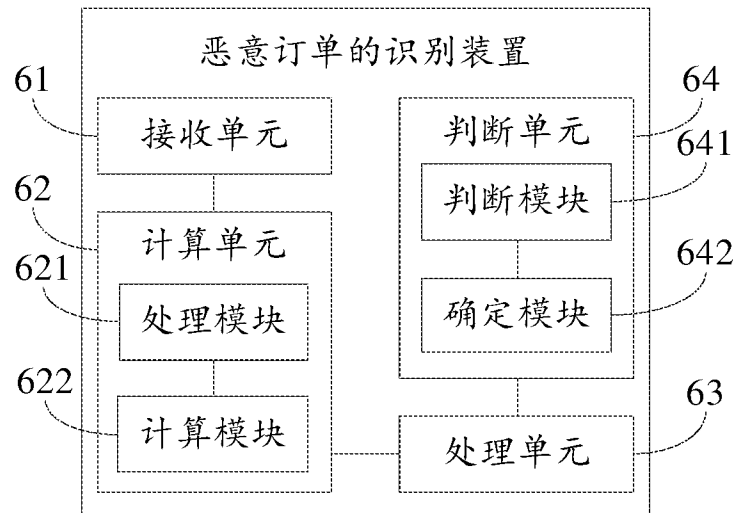


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/097953

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 30/06 (2012.01) 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)

G06Q; G06F; H04L

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, CNKI, WPI, EPODOC: 恶意, 虚假, 地址, 识别, 跳转, 概率, 分布, 订单, 正常, baleful, illusive, address, distinguish, jumping, probability, distributing, order, normal+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105389722 A (XIAOMI TECHNOLOGY CO., LTD.) 09 March 2016 (09.03.2016), description, paragraphs [0069]-[0082]	1-25
A	CN 103095711 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 08 May 2013 (08.05.2013), entire document	1-25
A	CN 105468742 A (XIAOMI TECHNOLOGY CO., LTD.) 06 April 2016 (06.04.2016), entire document	1-25
A	CN 104462059 A (UNIONPAY SMART INFORMATION SERVICES (SHANGHAI) CO., LTD.) 25 March 2015 (25.03.2015), entire document	1-25
A	WO 2008038017 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 03 April 2008 (03.04.2008), entire document	1-25

☐ 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 25 October 2017	Date of mailing of the international search report 21 November 2017
--	--

Name and mailing address of the ISA
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
GUO, Jing
Telephone No. (86-10) 62413415

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/097953

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105389722 A	09 March 2016	None	
CN 103095711 A	08 May 2013	None	
CN 105468742 A	06 April 2016	None	
CN 104462059 A	25 March 2015	None	
WO 2008038017 A1	03 April 2008	EP 2067097 A1	10 June 2009
		CN 101535954 A	16 September 2009
		EP 1923783 A1	21 May 2008

国际检索报告

国际申请号

PCT/CN2017/097953

A. 主题的分类 G06Q 30/06 (2012.01) 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) G06Q; G06F; H04L 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, CNKI, WPI, EPODOC; 恶意, 虚假, 地址, 识别, 跳转, 概率, 分布, 订单, 正常, baleful, illusive, address, distinguish, jumping, probability, distributing, order, normal+																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 105389722 A (小米科技有限责任公司) 2016年 3月 9日 (2016 - 03 - 09) 说明书第69-82段</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>CN 103095711 A (重庆邮电大学) 2013年 5月 8日 (2013 - 05 - 08) 全文</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>CN 105468742 A (小米科技有限责任公司) 2016年 4月 6日 (2016 - 04 - 06) 全文</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>CN 104462059 A (银联智惠信息服务上海有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文</td> <td>1-25</td> </tr> <tr> <td>A</td> <td>WO 2008038017 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 2008年 4月 3日 (2008 - 04 - 03) 全文</td> <td>1-25</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 105389722 A (小米科技有限责任公司) 2016年 3月 9日 (2016 - 03 - 09) 说明书第69-82段	1-25	A	CN 103095711 A (重庆邮电大学) 2013年 5月 8日 (2013 - 05 - 08) 全文	1-25	A	CN 105468742 A (小米科技有限责任公司) 2016年 4月 6日 (2016 - 04 - 06) 全文	1-25	A	CN 104462059 A (银联智惠信息服务上海有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文	1-25	A	WO 2008038017 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 2008年 4月 3日 (2008 - 04 - 03) 全文	1-25
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
A	CN 105389722 A (小米科技有限责任公司) 2016年 3月 9日 (2016 - 03 - 09) 说明书第69-82段	1-25																		
A	CN 103095711 A (重庆邮电大学) 2013年 5月 8日 (2013 - 05 - 08) 全文	1-25																		
A	CN 105468742 A (小米科技有限责任公司) 2016年 4月 6日 (2016 - 04 - 06) 全文	1-25																		
A	CN 104462059 A (银联智惠信息服务上海有限公司) 2015年 3月 25日 (2015 - 03 - 25) 全文	1-25																		
A	WO 2008038017 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 2008年 4月 3日 (2008 - 04 - 03) 全文	1-25																		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																
* 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 10月 25日		2017年 11月 21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 传真号 (86-10)62019451		郭婧																		
		电话号码 (86-10)62413415																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/097953

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	105389722	A	2016年 3月 9日	无			
CN	103095711	A	2013年 5月 8日	无			
CN	105468742	A	2016年 4月 6日	无			
CN	104462059	A	2015年 3月 25日	无			
WO	2008038017	A1	2008年 4月 3日	EP	2067097	A1	2009年 6月 10日
				CN	101535954	A	2009年 9月 16日
				EP	1923783	A1	2008年 5月 21日