

(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
2020 年 3 月 19 日 (19.03.2020)



(10) 国际公布号
WO 2020/052371 A1

(51) 国际专利分类号:
G06Q 20/18 (2012.01)

(21) 国际申请号: PCT/CN2019/098999

(22) 国际申请日: 2019 年 8 月 2 日 (02.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811066827.7 2018 年 9 月 13 日 (13.09.2018) 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: 齐元子 (**QI, Yuanzi**); 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: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市
海淀区上地三街 9 号嘉华大厦 B 座 409,
Beijing 100085 (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,

(54) **Title:** CONTROL METHOD, APPARATUS, AND SYSTEM EMPLOYING CODE SCANNING

(54) 发明名称: 一种扫码控制方法、装置及系统

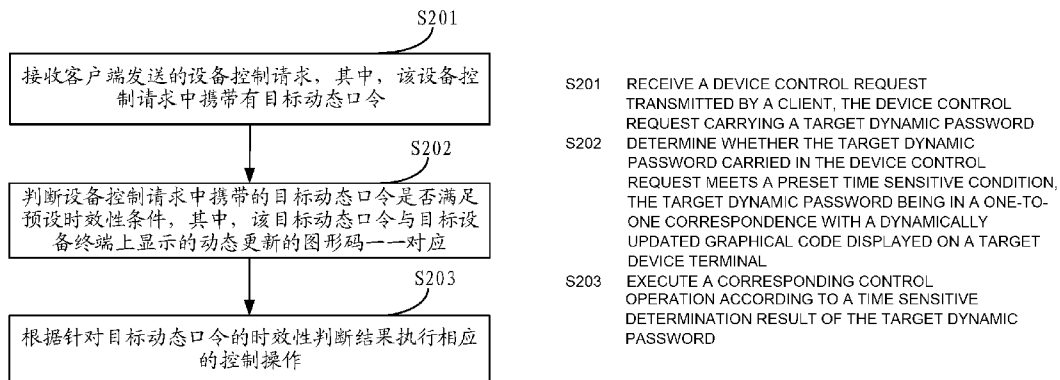


图 2

(57) **Abstract:** One or more embodiments of the present specification provide a control method, apparatus, and system employing code scanning. The method comprises: receiving a device control request transmitted by a client; determining whether a target dynamic password carried in the device control request meets a preset time sensitive condition, wherein the target dynamic password is in a one-to-one correspondence with a dynamically updated graphical code displayed on a target device terminal; and executing a corresponding control operation according to a time sensitive determination result. In one or more embodiments of the present specification, a graphical code displayed on a terminal device is dynamically changed, such that a dynamic password uploaded by a client has a certain degree of time sensitivity, so as to identify, by means of the time sensitivity of the dynamic password, whether the client has been attacked, and to perform effective control in a timely manner if it is identified that the client is illegally attacked by a malicious user, thereby avoiding unnecessary losses incurred by ordinary users.

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))。

(57) 摘要: 本说明书一个或多个实施例提供了一种扫码控制方法、装置及系统, 其中, 该方法包括: 接收客户端发送的设备控制请求; 判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件, 其中, 该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应; 根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中, 由于设备终端上显示的图形码是动态变化的, 以使客户端上传的动态口令应具有一定时效性, 这样能够借助动态口令的时效性识别客户端是否被攻击, 针对识别出客户端被恶意用户非法攻击的情况, 及时进行有效控制, 避免给正常用户带来不必要的损失。

一种扫码控制方法、装置及系统

技术领域

[01] 本说明书一个或多个涉及互联网技术领域，尤其涉及一种扫码控制方法、装置及系统。

5 背景技术

[02] 目前，随着互联网技术的快速发展，智能设备终端的应用越来越广泛，例如自取式商品售卖柜，用户通过使用移动终端（如智能手机）扫描商品售卖柜上的图形码，能够向后台服务端发送设备控制请求，以实现对商品售卖柜的智能控制，具体的，后台服务端自动控制商品售卖柜执行开门操作，这样用户能够从商品售卖柜内取出自身所需购买的商品，商品售卖柜向后台服务端发送用户所购买商品信息，以使后台服务端进行支付结算。

[03] 其中，针对智能设备终端的广泛应用，给人们的日常生活带来便利性的同时，在扫码控制的过程中存在一定的安全隐患，给恶意用户提供了攻击正常用户的机会，从而将给正常用户带来一定的经济损失。具体的，针对消费类的智能设备终端，如自取式商品售卖柜、共享租赁商品等。

[04] 当前，由于现有的智能设备终端上设置的用于提供用户扫描的图形码均为静态图形码，只要恶意用户一次性获取到该静态图形码对应的 URL 地址和设备标识后，恶意用户可以通过非法手段触发正常用户所用的客户端向后台服务端发送携带该 URL 地址和设备标识的设备控制请求，后台服务端直接基于该控制请求控制与该设备标识对应的智能设备终端执行目标操作，例如，控制商品售卖柜执行开门操作，并对发出该控制请求的正常用户进行支付扣款，使得恶意用户能够实现在不需要支付费用的情况下，从商品售卖柜中取出所需的商品，而是直接从正常用户的资金账号上扣款。

[05] 由此可知，需要提供一种防攻击且安全性高的扫码控制设备终端的方法。

发明内容

[06] 本说明书一个或多个实施例的目的是提供一种扫码控制方法、装置及系统，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，

这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[07]为解决上述技术问题，本说明书一个或多个实施例是这样实现的：

[08]本说明书一个或多个实施例提供了一种扫码控制方法，包括：

5 [09]接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[10]判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

[11]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[12]本说明书一个或多个实施例提供了一种扫码控制方法，包括：

10 [13]接收客户端发送的针对扫码售卖设备的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[14]判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应；

[15]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

15 [16]本说明书一个或多个实施例提供了一种扫码控制装置，包括：

[17]请求接收模块，用于接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[18]口令识别模块，用于判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

20 [19]控制模块，用于根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[20]本说明书一个或多个实施例提供了一种扫码控制装置，包括：

[21]请求接收模块，用于接收客户端发送的针对扫码售卖设备的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[22]口令识别模块，用于判断所述目标动态口令是否满足预设时效性条件，其中，所述

25 目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应；

[23]控制模块，用于根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[24]本说明书一个或多个实施例提供了一种扫码控制设备,包括:处理器;以及

[25]被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器:

[26]接收客户端发送的设备控制请求,其中,所述设备控制请求中携带有目标动态口令;

5 [27]判断所述目标动态口令是否满足预设时效性条件,其中,所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应;

[28]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[29]本说明书一个或多个实施例提供了一种扫码控制设备,包括:处理器;以及

10 [30]被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器:

[31]接收客户端发送的针对扫码售卖设备的设备控制请求,其中,所述设备控制请求中携带有目标动态口令;

[32]判断所述目标动态口令是否满足预设时效性条件,其中,所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应;

15 [33]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[34]本说明书一个或多个实施例提供了一种存储介质,用于存储计算机可执行指令,所述可执行指令在被执行时实现以下流程:

[35]接收客户端发送的设备控制请求,其中,所述设备控制请求中携带有目标动态口令;

20 [36]判断所述目标动态口令是否满足预设时效性条件,其中,所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应;

[37]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[38]本说明书一个或多个实施例提供了一种存储介质,用于存储计算机可执行指令,所述可执行指令在被执行时实现以下流程:

25 [39]接收客户端发送的针对扫码售卖设备的设备控制请求,其中,所述设备控制请求中携带有目标动态口令;

[40]判断所述目标动态口令是否满足预设时效性条件,其中,所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应;

[41]根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[42]本说明书一个或多个实施例中的扫码控制方法、装置及系统，接收客户端发送的设备控制请求；判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件，其中，该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

附图说明

10 [43]为了更清楚地说明本说明书一个或多个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说明书一个或多个中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[44]图 1 为本说明书一个或多个实施例提供的扫码控制系统的应用场景示意图；

15 [45]图 2 为本说明书一个或多个实施例提供的应用于后台服务端的扫码控制方法的第一种流程示意图；

[46]图 3 为本说明书一个或多个实施例提供的应用于后台服务端的扫码控制方法的第二种流程示意图；

20 [47]图 4 为本说明书一个或多个实施例提供的应用于后台服务端的扫码控制方法的第三种流程示意图；

[48]图 5 为本说明书一个或多个实施例提供的应用于后台服务端的扫码控制方法的第四种流程示意图；

[49]图 6 为本说明书一个或多个实施例提供的应用于后台服务端的扫码控制方法的第五种流程示意图；

25 [50]图 7a 为本说明书一个或多个实施例提供的扫码控制方法的第一种信息交互示意图；

[51]图 7b 为本说明书一个或多个实施例提供的扫码控制方法的第二种信息交互示意图；

[52]图 8 为本说明书一个或多个实施例提供的应用于客户端的扫码控制方法的流程示意图

图；

[53]图 9 为本说明书一个或多个实施例提供的应用于设备终端的扫码控制方法的流程图；

5 [54]图 10 为本说明书一个或多个实施例提供的针对扫码售卖设备的扫码控制方法的流程图示意图；

[55]图 11 为本说明书一个或多个实施例提供的设置于后台服务端的扫码控制装置的模块组成示意图；

[56]图 12 为本说明书一个或多个实施例提供的设备终端的模块组成示意图；

[57]图 13 为本说明书一个或多个实施例提供的扫码控制系统的结构组成示意图；

10 [58]图 14 为本说明书一个或多个实施例提供的扫码控制设备的结构示意图。

具体实施方式

[59]为了使本技术领域的人员更好地理解本说明书一个或多个中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个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说明书一个或多个一部分实施例，
15 而不是全部的实施例。基于本说明书一个或多个中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书一个或多个保护的范围。

[60]本说明书一个或多个实施例提供了一种扫码控制方法、装置及系统，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。
20

[61]图 1 为本说明书一个或多个实施例提供的扫码控制系统的应用场景示意图，如图 1 所示，该控制系统包括：后台服务端、客户端和设备终端，其中，该客户端可以是智能手机、平板电脑等移动终端，该后台服务端可以是用于对设备终端进行管理控制且具有 saas 服务的后台服务器，该设备终端可以是扫码售卖设备、扫码租赁产品等等，其中，
25 扫码控制的具体过程为：

[62]首先，客户端向后台服务端发送设备控制请求，其中，该设备控制请求中携带有目

标动态口令;

[63]具体的, 客户端可以是基于主动对设备终端上的图形码进行扫码操作而发出的设备控制请求, 即属于正常主动请求控制设备终端; 客户端还可以是在恶意用户通过非法手段触发下而发出的设备控制请求, 即被攻击后被动请求控制设备终端;

5 [64]然后, 后台服务端接收到上述设备控制请求后, 判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件;

[65]具体的, 针对客户端基于对设备终端上的图形码进行扫码操作而发出的设备控制请求的情况, 设备控制请求中携带的目标动态口令是有效的; 由于设备终端上显示的图形码对应的动态口令是动态更新的, 恶意用户从获取动态口令再到触发正常用户向后台服
10 务端发出携带该动态口令的设备控制请求的过程需要一定时间, 因此, 针对客户端在恶意用户通过非法手段触发下而发出的设备控制请求的情况, 设备控制请求中携带的目标动态口令是无效的;

[66]最后, 后台服务端根据针对目标动态口令的时效性判断结果执行相应的控制操作;

[67]具体的, 当确定出目标动态口令有效时, 说明客户端属于正常主动向后台服务端请求控制设备终端, 此时, 后台服务端需要正常响应该设备控制请求, 控制设备终端执行相应的控制动作; 当确定出目标动态口令无效时, 说明客户端属于被攻击而向后台服务端请求控制设备终端, 此时, 后台服务端需要向客户端返回提示信息, 从而实现对恶意用户的非法攻击行为进行有效控制, 避免给正常用户带来不必要的损失。

[68]图 2 为本说明书一个或多个实施例提供的扫码控制方法的第一种流程示意图, 图 2
20 中的方法能够由图 1 中的后台服务端执行, 如图 2 所示, 该方法至少包括以下步骤:

[69]S201, 接收客户端发送的设备控制请求, 其中, 该设备控制请求中携带有目标动态口令;

[70]具体的, 后台服务端接收到的设备控制请求可以是客户端基于主动对设备终端上的图形码进行扫码操作而发出的, 即属于客户端正常主动请求控制设备终端; 还可以是客户端在恶意用户通过非法手段触发下而发出的, 即属于客户端被攻击后被动请求控制设备终端;

[71]S202, 判断设备控制请求中携带的目标动态口令是否满足预设时效性条件, 其中, 该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应, 即在扫描图形码验证阶段, 确定目标动态口令的时效性, 以识别是否存在用户被攻击的情形, 针对设备

终端为扫码售卖设备的情况，该扫描图形码验证阶段即为用户使用客户端扫描图形码请求打开开门页面的过程；

[72]具体的，针对客户端基于对设备终端上的图形码进行扫码操作而发出的设备控制请求的情况，设备控制请求中携带的目标动态口令是满足预设时效性条件的，即目标动态口令对应的图形码未失效，此时设备终端上显示的图形码对应的动态口令即为该目标动态口令；

[73]针对客户端在恶意用户通过非法手段触发下而发出的设备控制请求的情况，设备控制请求中携带的目标动态口令是不满足预设时效性条件的，即目标动态口令对应的图形码已失效，此时设备终端上显示的图形码对应的动态口令不是该目标动态口令；

[74]S203，根据针对目标动态口令的时效性判断结果执行相应的控制操作，其中，该判断结果可以是目标动态口令满足预设时效性条件，还可以是目标动态口令不满足预设时效性条件；

[75]具体的，若目标动态口令满足预设时效性条件，说明客户端属于正常主动向后台服务端请求控制设备终端，此时，后台服务端需要正常响应该设备控制请求，控制设备终端执行相应的控制动作；若目标动态口令不满足预设时效性条件，说明客户端属于被攻击而向后台服务端请求控制设备终端，此时，后台服务端需要向客户端返回提示信息，例如，触发客户端展示报错页面。

[76]本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[77]其中，如图3所示，上述S203根据针对目标动态口令的时效性判断结果执行相应的控制操作，具体包括：

[78]若判断结果为是，则执行S2031，向客户端返回业务页面，以使该客户端基于该业务页面向后台服务端请求控制目标设备终端；

[79]具体的，针对判断结果为是的情况，即目标动态口令满足预设时效性条件，说明客户端属于正常主动向后台服务端请求控制设备终端，此时，后台服务端需要正常响应该设备控制请求，即后台服务端可以直接向设备终端发送控制指令，例如，下发开门指令；为了进一步提高设备控制的准确度，还可以先向客户端返回用于渲染业务页面的业务数

据，以使用户基于客户端展示的业务页面向客户端发送确认控制信息，对应的，后台服务端接收到该确认控制信息后，控制设备终端执行相应的控制动作；

[80]若判断结果为否，则执行 S2032，向客户端返回第一提示信息，以使该客户端基于该第一提示信息进行提示；

- 5 [81]具体的，针对判断结果为否的情况，即目标动态口令不满足预设时效性条件，说明客户端属于被攻击而向后台服务端请求控制设备终端，此时，后台服务端需要向客户端返回第一提示信息，以提示用户当前存在被攻击的可能性，另外，还可以在客户端显示的第一提示信息的展示页面上，提供确认提交设备控制请求的选项，例如，提供手动提交开门请求的选项，以防止因客户端扫码延时而出现上传的目标动态口令失效的情况下
- 10 导致无法交易的问题。

[82]进一步的，为了进一步提高设备控制的准确度，还可以先向客户端返回用于渲染业务页面的业务数据，以使用户基于客户端展示的业务页面向客户端发送确认控制信息，基于此，如图 4 所示，在上述 S2031 向客户端返回业务页面之后，还包括：

- [83]S2033，接收客户端针对展示的业务页面发送的控制确认信息，其中，针对设备终端为扫码售卖设备的情况，该业务页面可以是开门确认页面，当客户端检测到用户在开门确认页面上点击开门选项后，向后台服务端发送确认开门信息，针对设备终端为扫码租赁产品的情况，该业务页面还可以是开锁确认页面，当客户端检测到用户在开锁确认页面上点击开锁选项后，向后台服务端发送确认开锁信息；
- 15

- [84]S2034，基于接收到的控制确认信息向目标设备终端发送控制指令，以使该目标设备终端执行相应的控制动作，其中，该控制指令可以是开门指令，还可以是开锁指令，对应的，该目标设备终端执行的控制动作可以是开门操作，还可以是开锁操作等等。
- 20

- [85]其中，后台服务端需要按照预设规则生成包含动态口令的图形码信息，并将该图形码信息下发给对应的设备终端，以使设备终端显示于该图形码信息对应的图形码，这样能够保证设备终端上显示的用于提供客户端扫描的图形码是动态更新的，从而保证客户端上传的设备控制请求中携带的目标动态口令是动态变化的，以便后续基于对目标动态口令的时效性判断来确定执行何种控制操作，具体的，如图 5 所示，在上述 S201 接收客户端发送的设备控制请求之前，还包括：
- 25

[86]S204，根据目标设备终端的设备标识、与该设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令，其中，该设备标识可以是预先为每个设备终端分配的

唯一性标识, 该标识密钥可以是按照预设方式基于设备标识确定的, 该时间戳信息可以是确定动态口令时的当前时间戳, 具体的, 可以将该动态口令存储于 key-value 数据库 (即 redis) 中;

5 [87]S205, 根据确定出的动态口令, 生成图形码信息, 其中, 该图形码信息可以是预设 URL 地址与动态口令拼接得到的, 即可以将动态口令添加至 URL 地址的尾端, 例如, 该 URL 地址可以是 <https://alipay.com/detail.htm>;

10 [88]S206, 将生成的图形码信息下发给目标设备终端, 以使该目标设备终端基于该图形码信息显示相应的图形码, 其中, 由于每次生成的动态口令各不相同, 因此, 图形码信息各不相同, 以使设备终端展示的图形码是动态更新的, 该图形码可以是二维码, 还可以是条形码;

[89]具体的, 为了降低设备终端的制造成本, 可以以电子墨水标签屏幕作为图形码显示屏, 例如, 设备终端上设置的用于显示图形码的显示屏可复用。

15 [90]其中, 客户端在扫描目标设备终端上显示的图形码时, 能够解析出该图形码对应的目标动态口令, 再基于该目标动态口令生成设备控制请求, 以及向后台服务端发送该设备控制请求, 以使该后台服务端基于该设备控制请求对目标设备终端进行控制。

[91]进一步的, 为了提高目标动态口令的时效性的判断效率和判断准确度, 可以将失效的动态口令自动删除, 进而在接收到设备控制请求后, 判断是否存在该设备控制请求中携带的目标动态口令, 从而确定该目标动态口令是否满足预设时效性条件, 基于此, 如图 6 所示, 在上述 S206 将生成的图形码信息下发给目标设备终端之后, 还包括:

20 [92]S207, 将确定出的动态口令添加至动态口令集合中, 以及当任一动态口令满足预设销毁条件时, 将该动态口令从动态口令集合中移除, 其中, 该预设销毁条件包括: 动态口令达到预设存活时间和/或动态口令已使用, 具体的, 动态口令达到预设存活时间是指动态口令的存活时间大于预设时效阈值, 即动态口令过期销毁, 动态口令已使用是指已针对该动态口令进行设备终端控制, 即动态口令已使用销毁, 其中, 该动态口令集合包
25 括至少一个有效的动态口令, 该动态口令集合设置于 key-value 数据库 (即 redis) 中;

[93]对应的, 上述 S202 判断设备控制请求中携带的目标动态口令是否满足预设时效性条件, 具体包括:

[94]S2021, 判断动态口令集合中是否存在设备控制请求中携带的目标动态口令;

[95]若判断结果为是, 则确定目标动态口令₉满足预设时效性条件, 并执行上述 S2031 向

客户端返回业务页面，以使该客户端基于该业务页面向后台服务端请求控制目标设备终端；

[96]若判断结果为否，则确定目标动态口令不满足预设时效性条件，并执行上述 S2032 向客户端返回第一提示信息，以使该客户端基于该第一提示信息进行提示。

- 5 [97]具体的，当将某一动态口令从动态口令集合中移除后，说明该动态口令对应的图形码变为失效，需要更新对应的设备终端上显示的图像码，基于此，上述 S207 将该动态口令从动态口令集合中移除之后，还包括：

[98]生成新的动态口令，基于该新的动态口令更新对应的目标设备终端上显示的图形码；

- 10 [99]具体的，生成新的动态口令的过程，参见上述步骤 S204，其中，生成新的动态口令后，根据该动态口令，生成图形码信息，将该图形码信息下发给对应的目标设备终端，以更新该目标设备终端上显示的图形码。

[100] 其中，上述 S204 根据目标设备终端的设备标识、与该设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令，具体包括：

- 15 [101] 利用消息摘要算法根据目标设备终端的设备标识、与该设备标识对应的标识密钥以及时间戳信息的至少两个，确定动态口令，其中，该消息摘要算法可以是 md5 加密算法，具体的，利用 md5 加密算法对设备 id、与该设备 id 对应的唯一 key 以及时间戳信息中至少两个进行 md5 加密，生成 sign 字段。

[102] 其中，上述 S2034 基于接收到的控制确认信息向目标设备终端发送控制指令，具体包括：

- 20 [103] 在动态口令集合中，查找是否存在与接收到的控制确认信息对应的动态口令，具体的，在接收到客户端针对业务页面发送的控制确认信息后，再次判断动态集合中是否存在对应的动态口令；

[104] 若是，则将该动态口令从上述动态口令集合中移除，以及向目标设备终端发送控制指令；

- 25 [105] 具体的，在接收到客户端针对业务页面发送的控制确认信息后，说明后台服务端需要对设备终端执行相应的控制操作，对应的，该动态口令满足预设销毁条件，销毁该动态口令后，针对展示包含该动态口令的图形码的目标设备终端，生成新的动态口令，基于该新的动态口令更新该目标设备终端上显示的图形码；

[106] 若否，则向目标设备终端发送控制指令，或者向客户端返回第二提示信息，以提示用户是否重新向后台服务端发送设备控制请求；

[107] 具体的，由于在扫描图形码验证阶段验证通过后，即设备控制请求中携带的目标动态口令满足预设时效性条件，如果客户端在预设时间内针对业务页面向后台服务端发送的控制确认信息，本次设备控制请求对应的目标动态口令应该是有效的，即在动态口令集合中存在目标动态口令，若在动态口令集合中不存在目标动态口令，则说明客户端未在预设时间内针对业务页面向后台服务端发送的控制确认信息。

[108] 在一个具体实施例中，上述扫码控制方法主要包括：图形码信息下发过程和基于图形码时效性进行设备控制的过程，如图 7a 所示，给出了扫码控制方法中图形码信息下发过程的信息交互示意图，具体为：

[109] S701，后台服务端获取目标设备终端的设备标识；

[110] S702，后台服务端根据目标设备终端的设备标识、与该设备标识对应的标识密钥以及时间戳信息，生成动态口令，其中，可以是在确定目标设备终端上显示的图形码过期后，生成新的动态口令，以更新目标设备终端上显示的图形码，还可以是在确定客户端已基于图形码对于的动态口令发出设备控制请求后，生成新的动态口令，以更新目标设备终端上显示的图形码；

[111] S703，后台服务端根据生成的动态口令和预设 URL 地址，生成图形码信息；

[112] S704，后台服务端向目标设备终端发送图形码信息；

[113] S705，目标设备终端在接收到图形码信息后，在显示屏上基于该图形码信息展示图形码；

[114] S706，后台服务端在 key-value 数据库中存储生成的动态口令，其中。针对存储于 key-value 数据库中的动态口令，若该动态口令满足预设销毁条件，则删除该动态口令；

[115] 如图 7b 所示，给出了扫码控制方法中基于图形码时效性进行设备控制过程的信息交互示意图，针对设备终端为扫码售卖设备的情况，具体为：

[116] S707，客户端向后台服务端发送携带有目标动态口令的设备控制请求，其中，该设备控制请求可以是客户端基于主动对目标设备终端上的图形码进行扫码操作而发出的，还可以是客户端在恶意用户通过非法手段触发下而发出的；

[117] S708, 后台服务端在接收到设备控制请求后, 触发 key-value 数据库查询是否存在设备控制请求中携带的目标动态口令;

[118] S709, key-value 数据库向后台服务端返回动态口令的查询结果, 其中, 该查询结果可以是存在目标动态口令, 还可以是不存在目标动态口令;

5 [119] S710, 后台服务端在接收到的查询结果为不存在时, 向客户端发送报错提示页面;

[120] S711, 后台服务端在接收到的确定查询结果为存在时, 则向客户端发送用于渲染开门页面的业务数据;

10 [121] S712, 客户端渲染并展示开门页面, 其中, 该开门页面用于触发用户进行开门请求确认;

[122] S713, 客户端若监测到用户点击确认开门选项后, 向后台服务端发送确认开门请求;

[123] S714, 后台服务端在接收到确认开门请求后, 触发 key-value 数据库查询是否存在与该确认开门请求对应的目标动态口令;

15 [124] S715, key-value 数据库若确定查询结果为存在, 则销毁目标动态口令;

[125] S716, key-value 数据库向后台服务端返回动态口令存在的查询结果;

[126] S717, 后台服务端在接收到动态口令存在的查询结果后, 向设备终端下发开门指令; 以及,

20 [127] S718, 后台服务端重新执行图形码信息下发步骤, 以更新设备终端上显示的图形码, 从而实现控制设备终端上显示的图形码动态更新。

[128] 本说明书一个或多个实施例中的扫码控制方法, 接收客户端发送的设备控制请求; 判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件, 其中, 该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应; 根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中, 由于设备终端上显示的图形码是动态变化的, 以使客户端上传的动态口令应具有一定时效性, 这样能够借助动态口令的时效性识别客户端是否被攻击, 针对识别出客户端被恶意用户非法攻击的情况, 及时进行有效控制, 避免给正常用户带来不必要的损失。

25

[129] 对应上述图 2 至图 6 描述的扫码控制方法, 基于相同的技术构思, 本说明书一

个或多个实施例还提供了一种扫码控制方法，图 8 为本说明书一个或多个实施例提供的扫码控制方法的流程示意图，图 8 中的方法能够由图 1 中的客户端执行，如图 8 所示，该方法至少包括以下步骤：

5 [130] S801，向后台服务端发送携带有目标动态口令的设备控制请求，以使后台服务端判断该目标动态口令是否满足预设时效性条件；

[131] S802，接收后台服务端发送的反馈信息，其中，该反馈信息是后台服务端针对目标动态口令的时效性判断结果生成的。

10 [132] 本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[133] 其中，上述 S802 接收后台服务端发送的反馈信息，具体包括：

15 [134] 接收后台服务端确定目标动态口令满足预设时效性条件时所发送的业务页面，并基于该业务页面向后台服务端请求控制目标设备终端；

[135] 接收后台服务端确定目标动态口令不满足预设时效性条件时所发送的提示信息，并基于该提示信息进行提示。

20 [136] 本说明书一个或多个实施例中的扫码控制方法，向后台服务端发送携带有目标动态口令的设备控制请求，以使后台服务端判断该目标动态口令是否满足预设时效性条件；以及接收后台服务端发送的反馈信息，其中，该反馈信息是后台服务端针对目标动态口令的时效性判断结果生成的。本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免
25 给正常用户带来不必要的损失。

[137] 需要说明的是，本说明书中该实施例与本说明书中上一实施例基于同一发明构思，因此该实施例的具体实施可以参见前述扫码控制方法的实施，重复之处不再赘述。

[138] 对应上述图 2 至图 6 描述的扫码控制方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种扫码控制方法，图 9 为本说明书一个或多个实施例提供的

扫码控制方法的流程示意图,图 9 中的方法能够由图 1 中的设备终端执行,如图 9 所示,该方法至少包括以下步骤:

[139] S901, 基于后台服务端下发的图形码信息展示相应的图形码, 其中, 该图形码是在后台服务端控制下动态更新的, 每个图形码对应于一个唯一的动态口令;

5 [140] S902, 接收后台服务端发送的控制指令, 其中, 该控制指令是后台服务端针对接收到的设备控制请求中携带的目标动态口令的时效性判断结果生成的。

[141] 本说明书一个或多个实施例中, 通过后台服务端控制设备终端上显示的图形码动态更新, 由于设备终端上显示的图形码是动态变化的, 以使客户端上传的动态口令应具有一定时效性, 这样能够借助动态口令的时效性识别客户端是否被攻击, 针对识别出
10 客户端被恶意用户非法攻击的情况, 及时进行有效控制, 避免给正常用户带来不必要的损失。

[142] 其中, 上述 S902 接收后台服务端发送的控制指令, 具体包括:

[143] 接收后台服务端确定目标动态口令满足预设时效性条件时所发送的控制指令, 以及基于该控制指令执行相应的控制动作, 其中, 针对扫码售卖设备而言, 该控制指令
15 为开门指令, 扫码售卖设备接收到该开门指令后, 执行开门操作。

[144] 本说明书一个或多个实施例中的扫码控制方法, 基于后台服务端下发的图形码信息展示相应的图形码, 其中, 该图形码是在后台服务端控制下动态更新的, 每个图形码对应于一个唯一的动态口令; 以及接收后台服务端发送的控制指令, 其中, 该控制指令是后台服务端针对接收到的设备控制请求中携带的目标动态口令的时效性判断结果
20 生成的。本说明书一个或多个实施例中, 通过后台服务端控制设备终端上显示的图形码动态更新, 由于设备终端上显示的图形码是动态变化的, 以使客户端上传的动态口令应具有一定时效性, 这样能够借助动态口令的时效性识别客户端是否被攻击, 针对识别出客户端被恶意用户非法攻击的情况, 及时进行有效控制, 避免给正常用户带来不必要的损失。

25 [145] 需要说明的是, 本说明书中该实施例与本说明书中上一实施例基于同一发明构思, 因此该实施例的具体实施可以参见前述扫码控制方法的实施, 重复之处不再赘述。

[146] 对应上述图 2 至图 6 描述的扫码控制方法, 基于相同的技术构思, 本说明书一个或多个实施例还提供了一种扫码控制方法, 图 10 为本说明书一个或多个实施例提供的扫码控制方法的流程示意图, 图 10 中的方法能够由图 1 中的后台服务端执行, 如图

10 所示, 针对设备终端为扫码售卖设备的情况, 该方法至少包括以下步骤:

[147] S1001, 接收客户端发送的针对扫码售卖设备的设备控制请求, 其中, 该设备控制请求中携带有目标动态口令, 该扫码售卖设备可以是智能扫码开门自取式货柜; 其中, 步骤 S1001 的具体实施方式参见步骤 S201, 这里不再赘述。

5 [148] S1002, 判断设备控制请求中携带的目标动态口令是否满足预设时效性条件, 其中, 该目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应; 其中, 步骤 S1002 的具体实施方式参见步骤 S202, 这里不再赘述。

[149] S1003, 根据针对目标动态口令的时效性判断结果执行相应的控制操作; 其中, 步骤 S1003 的具体实施方式参见步骤 S203, 这里不再赘述。

10 [150] 本说明书一个或多个实施例中, 通过后台服务端控制设备终端上显示的图形码动态更新, 由于设备终端上显示的图形码是动态变化的, 以使客户端上传的动态口令应具有一定时效性, 这样能够借助动态口令的时效性识别客户端是否被攻击, 针对识别出客户端被恶意用户非法攻击的情况, 及时进行有效控制, 避免给正常用户带来不必要的损失。

15 [151] 其中, 在 S1001 接收客户端发送的针对扫码售卖设备的设备控制请求之前, 还包括:

[152] 步骤一, 根据目标扫码售卖设备的设备标识、与该设备标识对应的标识密钥以及时间戳信息中的至少两个, 确定动态口令;

[153] 步骤二, 根据确定出的动态口令, 生成图形码信息;

20 [154] 步骤三, 将生成的图形码信息下发给目标扫码售卖设备, 以使该目标扫码售卖设备基于该图形码信息显示图形码。

[155] 其中, 上述步骤一根据目标扫码售卖设备的设备标识、与该设备标识对应的标识密钥以及时间戳信息中的至少两个, 确定动态口令之后, 还包括:

25 [156] 将确定出的动态口令添加至动态口令集合, 以及当任一动态口令满足预设销毁条件时, 将该动态口令从动态口令集合中移除, 其中, 该预设销毁条件包括: 动态口令达到预设存活时间和/或动态口令已使用;

[157] 对应的, 上述 S1002 判断设备控制请求中携带的目标动态口令是否满足预设时效性条件, 具体包括:

[158] 若动态口令集合中存在目标动态口令，则确定该目标动态口令满足预设时效性条件；

[159] 若动态口令集合中不存在目标动态口令，则确定该目标动态口令不满足预设时效性条件。

5 [160] 其中，上述将动态口令从动态口令集合中移除之后，还包括：

[161] 生成新的动态口令，基于该新的动态口令更新目标扫码售卖设备上显示的图形码。

[162] 本说明书一个或多个实施例中的扫码控制方法，接收客户端发送的设备控制请求；判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件，其中，该目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应；根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

10

15

[163] 需要说明的是，本说明书中该实施例与本说明书中上一实施例基于同一发明构思，因此该实施例的具体实施可以参见前述扫码控制方法的实施，重复之处不再赘述。

[164] 对应上述图 2 至图 6 描述的扫码控制方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种扫码控制装置，图 11 为本说明书一个或多个实施例提供的扫码控制装置的模块组成示意图，该装置用于执行图 2 至图 6 描述的扫码控制方法，如图 11 所示，该装置包括：

20

[165] 请求接收模块 1101，用于接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[166] 口令识别模块 1102，用于判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

25

[167] 控制模块 1103，用于根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[168] 可选地，上述控制模块 1103，具体用于：

[169] 若判断结果为是，则向所述客户端返回业务页面，以使所述客户端基于所述业务页面向后台服务端请求控制所述目标设备终端；

[170] 若判断结果为否，则向所述客户端返回提示信息，以使所述客户端基于所述提示信息进行提示。

5 [171] 可选地，上述装置还包括控制指令下发模块，其中，该控制指令下发模块，用于：

[172] 在向所述客户端返回业务页面之后，接收所述客户端针对所述业务页面发送的控制确认信息；

10 [173] 基于所述控制确认信息向所述目标设备终端发送控制指令，以使所述目标设备终端执行相应的控制动作。

[174] 可选地，上述装置还包括图形码更新模块，其中，该图形码更新模块，用于：

[175] 在接收客户端发送的设备控制请求之前，根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令；

[176] 根据确定出的所述动态口令，生成图形码信息；

15 [177] 将所述图形码信息下发给所述目标设备终端，以使所述目标设备终端基于所述图形码信息显示图形码。

[178] 可选地，上述装置还包括动态口令增删模块，其中，该动态口令增删模块，用于：

20 [179] 在确定动态口令之后，将所述动态口令添加至动态口令集合，以及当所述动态口令满足预设销毁条件时，将所述动态口令从所述动态口令集合中移除，其中，所述预设销毁条件包括：动态口令达到预设存活时间和/或动态口令已使用；

[180] 对应的，上述口令识别模块 1102，具体用于：

[181] 若所述动态口令集合中存在所述目标动态口令，则确定所述目标动态口令满足预设时效性条件；

25 [182] 若所述动态口令集合中不存在所述目标动态口令，则确定所述目标动态口令不满足预设时效性条件。

[183] 可选地，上述图形码更新模块，还用于：

[184] 将所述动态口令从所述动态口令集合中移除之后，生成新的动态口令，基于所述新的动态口令更新所述目标设备终端上显示的图形码。

[185] 可选地，上述图形码更新模块，具体用于：

[186] 利用消息摘要算法根据目标设备终端的设备标识、与所述设备标识对应的标识
5 密钥以及时间戳信息中的至少两个，确定动态口令。

[187] 可选地，上述控制指令下发模块，具体用于：

[188] 在动态口令集合中，查找是否存在与所述控制确认信息对应的动态口令；

[189] 若是，则触发动态口令增删模块将所述动态口令从所述动态口令集合中移除，以及向目标设备终端发送控制指令。

10 [190] 本说明书一个或多个实施例中的扫码控制装置，接收客户端发送的设备控制请求；判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件，其中，该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中，由于设备终端上显示的图形码是
15 动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[191] 对应上述图 2 至图 6 描述的扫码控制方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种设备终端，其中，该终端设备可以是扫码售卖设备，图 12
20 为本说明书一个或多个实施例提供的设备终端的模块组成示意图，该装置用于执行图 9 描述的扫码控制方法，如图 12 所示，该设备终端包括：

[192] 图形码展示模块 1201，用于基于后台服务端下发的图形码信息展示相应的图形码，其中，该图形码是在后台服务端控制下动态更新的，每个图形码对应于一个唯一的动态口令；

[193] 控制指令接收模块 1202，用于接收后台服务端发送的控制指令，其中，该控制
25 指令是后台服务端针对接收到的设备控制请求中携带的目标动态口令的时效性判断结果生成的。

[194] 本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应

具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[195] 其中，上述控制指令接收模块 1202，具体用于：

- 5 [196] 接收后台服务端确定目标动态口令满足预设时效性条件时所发送的控制指令，以及基于该控制指令执行相应的控制动作，其中，针对扫码售卖设备而言，该控制指令为开门指令，扫码售卖设备接收到该开门指令后，执行开门操作。

- [197] 本说明书一个或多个实施例中的设备终端，基于后台服务端下发的图形码信息展示相应的图形码，其中，该图形码是在后台服务端控制下动态更新的，每个图形码对
10 应于一个唯一的动态口令；以及接收后台服务端发送的控制指令，其中，该控制指令是后台服务端针对接收到的设备控制请求中携带的目标动态口令的时效性判断结果生成的。本说明书一个或多个实施例中，通过后台服务端控制设备终端上显示的图形码动态更新，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客
15 户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[198] 需要说明的是，本说明书中该实施例与本说明书中上一实施例基于同一发明构思，因此该实施例的具体实施可以参见前述扫码控制方法的实施，重复之处不再赘述。

- [199] 对应上述图 2 至图 6 描述的扫码控制方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种扫码控制系统，图 13 为本说明书一个或多个实施例提供
20 的设备终端的模块组成示意图，该装置用于执行图 2 至图 6 描述的扫码控制方法，如图 13 所示，该设备终端包括：后台服务端 20、客户端 10 和设备终端 30；

[200] 其中，上述后台服务端 20，用于接收客户端发送的设备控制请求；判断所述设备控制请求中携带的目标动态口令是否满足预设时效性条件；根据针对所述目标动态口令的时效性判断结果执行相应的控制操作；

- 25 [201] 上述客户端 10，用于向后台服务端发送设备控制请求；以及接收所述后台服务端针对所述目标动态口令的时效性判断结果发送的反馈信息；

[202] 上述设备终端 30，用于基于后台服务端下发的图形码信息展示相应的图形码，其中，所述图形码是动态更新的，每个所述图形码对应于一个唯一的动态口令；以及接收所述后台服务端针对所述目标动态口令的时效性判断结果发送的控制指令。

[203] 本说明书一个或多个实施例中的扫码控制方法，接收客户端发送的设备控制请求；判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件，其中，该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[204] 进一步地，对应上述图 2 至图 6 所示的方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种扫码控制设备，该设备用于执行上述的扫码控制方法，如图 14 所示。

[205] 扫码控制设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上的处理器 1401 和存储器 1402，存储器 1402 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 1402 可以是短暂存储或持久存储。存储在存储器 1402 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括对扫码控制设备中的一系列计算机可执行指令。更进一步地，处理器 1401 可以设置为与存储器 1402 通信，在扫码控制设备上执行存储器 1402 中的一系列计算机可执行指令。扫码控制设备还可以包括一个或一个以上电源 1403，一个或一个以上有线或无线网络接口 1404，一个或一个以上输入输出接口 1405，一个或一个以上键盘 1406 等。

[206] 在一个具体的实施例中，扫码控制设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对扫码控制设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：

[207] 接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[208] 判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

[209] 根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[210] 可选地，计算机可执行指令在被执行时，所述根据针对所述目标动态口令的时

效性判断结果执行相应的控制操作，包括：

[211] 若判断结果为是，则向所述客户端返回业务页面，以使所述客户端基于所述业务页面向后台服务端请求控制所述目标设备终端；

5 [212] 若判断结果为否，则向所述客户端返回提示信息，以使所述客户端基于所述提示信息进行提示。

[213] 可选地，计算机可执行指令在被执行时，还包含用于进行以下计算机可执行指令：

[214] 在向所述客户端返回业务页面之后，还包括：

[215] 接收所述客户端针对所述业务页面发送的控制确认信息；

10 [216] 基于所述控制确认信息向所述目标设备终端发送控制指令，以使所述目标设备终端执行相应的控制动作。

[217] 可选地，计算机可执行指令在被执行时，还包含用于进行以下计算机可执行指令：

[218] 在接收客户端发送的设备控制请求之前，还包括：

15 [219] 根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令；

[220] 根据确定出的所述动态口令，生成图形码信息；

[221] 将所述图形码信息下发给所述目标设备终端，以使所述目标设备终端基于所述图形码信息显示图形码。

20 [222] 可选地，计算机可执行指令在被执行时，还包含用于进行以下计算机可执行指令：

[223] 在确定动态口令之后，还包括：

[224] 将所述动态口令添加至动态口令集合，以及当所述动态口令满足预设销毁条件时，将所述动态口令从所述动态口令集合中移除，其中，所述预设销毁条件包括：动态
25 口令达到预设存活时间和/或动态口令已使用；

[225] 所述判断所述目标动态口令是否满足预设时效性条件，包括：

[226] 若所述动态口令集合中存在所述目标动态口令，则确定所述目标动态口令满足

预设时效性条件；

[227] 若所述动态口令集合中不存在所述目标动态口令，则确定所述目标动态口令不满足预设时效性条件。

[228] 可选地，计算机可执行指令在被执行时，还包含用于进行以下计算机可执行指令：

[229] 所述将所述动态口令从所述动态口令集合中移除之后，还包括：

[230] 生成新的动态口令，基于所述新的动态口令更新所述目标设备终端上显示的图形码。

[231] 可选地，计算机可执行指令在被执行时，所述根据目标设备终端的设备标识、与

[232] 利用消息摘要算法根据目标设备终端的设备标识、与

[233] 可选地，计算机可执行指令在被执行时，所述基于所述控制确认信息向所述目标设备终端发送控制指令，包括：

[234] 在动态口令集合中，查找是否存在与

[235] 若是，则将所述动态口令从所述动态口令集合中移除，以及向目标设备终端发送控制指令。

[236] 本说明书一个或多个实施例中的扫码控制设备，接收客户端发送的设备控制请求；判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件，其中，该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施例中，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[237] 进一步地，对应上述图 2 至图 6 所示的方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种存储介质，用于存储计算机可执行指令，一种具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令在被处理器执行时，能实现以下流程：

[238] 接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

[239] 判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

5 [240] 根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

[241] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述根据针对所述目标动态口令的时效性判断结果执行相应的控制操作，包括：

[242] 若判断结果为是，则向所述客户端返回业务页面，以使所述客户端基于所述业务页面向后台服务端请求控制所述目标设备终端；

10 [243] 若判断结果为否，则向所述客户端返回提示信息，以使所述客户端基于所述提示信息进行提示。

[244] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，还实现以下流程：

[245] 在向所述客户端返回业务页面之后，还包括：

15 [246] 接收所述客户端针对所述业务页面发送的控制确认信息；

[247] 基于所述控制确认信息向所述目标设备终端发送控制指令，以使所述目标设备终端执行相应的控制动作。

[248] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，还实现以下流程：

20 [249] 在接收客户端发送的设备控制请求之前，还包括：

[250] 根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令；

[251] 根据确定出的所述动态口令，生成图形码信息；

[252] 将所述图形码信息下发给所述目标设备终端，以使所述目标设备终端基于所述

25 图形码信息显示图形码。

[253] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，还实现以下流程：

[254] 在确定动态口令之后, 还包括:

[255] 将所述动态口令添加至动态口令集合, 以及当所述动态口令满足预设销毁条件时, 将所述动态口令从所述动态口令集合中移除, 其中, 所述预设销毁条件包括: 动态口令达到预设存活时间和/或动态口令已使用;

5 [256] 所述判断所述目标动态口令是否满足预设时效性条件, 包括:

[257] 若所述动态口令集合中存在所述目标动态口令, 则确定所述目标动态口令满足预设时效性条件;

[258] 若所述动态口令集合中不存在所述目标动态口令, 则确定所述目标动态口令不满足预设时效性条件。

10 [259] 可选地, 该存储介质存储的计算机可执行指令在被处理器执行时, 还实现以下流程:

[260] 所述将所述动态口令从所述动态口令集合中移除之后, 还包括:

[261] 生成新的动态口令, 基于所述新的动态口令更新所述目标设备终端上显示的图形码。

15 [262] 可选地, 该存储介质存储的计算机可执行指令在被处理器执行时, 所述根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个, 确定动态口令, 包括:

[263] 利用消息摘要算法根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个, 确定动态口令。

20 [264] 可选地, 该存储介质存储的计算机可执行指令在被处理器执行时, 所述基于所述控制确认信息向所述目标设备终端发送控制指令, 包括:

[265] 在动态口令集合中, 查找是否存在与所述控制确认信息对应的动态口令;

[266] 若是, 则将所述动态口令从所述动态口令集合中移除, 以及向目标设备终端发送控制指令。

25 [267] 本说明书一个或多个实施例中的存储介质存储的计算机可执行指令在被处理器执行时, 接收客户端发送的设备控制请求; 判断该设备控制请求中携带的目标动态口令是否满足预设时效性条件, 其中, 该目标动态口令与目标设备终端上显示的动态更新的图形码一一对应; 根据时效性判断结果执行相应的控制操作。本说明书一个或多个实施

例中，由于设备终端上显示的图形码是动态变化的，以使客户端上传的动态口令应具有一定时效性，这样能够借助动态口令的时效性识别客户端是否被攻击，针对识别出客户端被恶意用户非法攻击的情况，及时进行有效控制，避免给正常用户带来不必要的损失。

[268] 在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HD Cal、JHDL（Java Hardware Description Language）、Lava、Lola、My HDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[269] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而

对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[270] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[271] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[272] 本领域内的技术人员应明白，本说明书一个或多个的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[273] 本说明书一个或多个是参照根据本说明书一个或多个实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[274] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[275] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或

方框图一个方框或多个方框中指定的功能的步骤。

[276] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[277] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）

5 和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[278] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存

10 储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑
15 可读媒体（transitory media），如调制的数据信号和载波。

[279] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在
20 包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[280] 本领域技术人员应明白，本说明书一个或多个的实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、
25 CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[281] 本说明书一个或多个可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行

任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[282] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，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。

[283] 以上所述仅为本说明书一个或多个的实施例而已，并不用于限制本说明书一个或多个。对于本领域技术人员来说，本说明书一个或多个可以有各种更改和变化。凡在本说明书一个或多个的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书一个或多个的权利要求范围之内。

权利要求书

1、一种扫码控制方法，其特征在于，包括：

接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标

5 设备终端上显示的动态更新的图形码一一对应；

根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

2、根据权利要求 1 所述的方法，其特征在于，所述根据针对所述目标动态口令的时效性判断结果执行相应的控制操作，包括：

若判断结果为是，则向所述客户端返回业务页面，以使所述客户端基于所述业务页
10 面向后台服务端请求控制所述目标设备终端；

若判断结果为否，则向所述客户端返回提示信息，以使所述客户端基于所述提示信息
15 进行提示。

3、根据权利要求 2 所述的方法，其特征在于，在向所述客户端返回业务页面之后，
还包括：

15 接收所述客户端针对所述业务页面发送的控制确认信息；

基于所述控制确认信息向所述目标设备终端发送控制指令，以使所述目标设备终端
20 执行相应的控制动作。

4、根据权利要求 1 所述的方法，其特征在于，在接收客户端发送的设备控制请求
之前，还包括：

20 根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令；

根据确定出的所述动态口令，生成图形码信息；

将所述图形码信息下发给所述目标设备终端，以使所述目标设备终端基于所述图形
25 码信息显示图形码。

5、根据权利要求 4 所述的方法，其特征在于，在确定动态口令之后，还包括：

将所述动态口令添加至动态口令集合，以及当所述动态口令满足预设销毁条件时，
将所述动态口令从所述动态口令集合中移除，其中，所述预设销毁条件包括：动态口令
30 达到预设存活时间和/或动态口令已使用；

所述判断所述目标动态口令是否满足预设时效性条件，包括：

30 若所述动态口令集合中存在所述目标动态口令，则确定所述目标动态口令满足预设
时效性条件；

若所述动态口令集合中不存在所述目标动态口令，则确定所述目标动态口令不满足预设时效性条件。

6、根据权利要求 5 所述的方法，其特征在于，所述将所述动态口令从所述动态口令集合中移除之后，还包括：

5 生成新的动态口令，基于所述新的动态口令更新所述目标设备终端上显示的图形码。

7、根据权利要求 4 所述的方法，其特征在于，所述根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令，包括：

利用消息摘要算法根据目标设备终端的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令。

10 8、根据权利要求 3 所述的方法，其特征在于，所述基于所述控制确认信息向所述目标设备终端发送控制指令，包括：

在动态口令集合中，查找是否存在与所述控制确认信息对应的动态口令；

若是，则将所述动态口令从所述动态口令集合中移除，以及向目标设备终端发送控制指令。

15 9、一种扫码控制方法，其特征在于，包括：

向后台服务端发送携带有目标动态口令的设备控制请求，以使所述后台服务端判断所述目标动态口令是否满足预设时效性条件；

接收所述后台服务端发送的反馈信息，其中，所述反馈信息是所述后台服务端针对所述目标动态口令的时效性判断结果生成的。

20 10、根据权利要求 9 所述的方法，其特征在于，所述接收所述后台服务端发送的反馈信息，包括：

接收所述后台服务端确定所述目标动态口令满足预设时效性条件时所发送的业务页面，并基于所述业务页面向所述后台服务端请求控制目标设备终端；

25 接收所述后台服务端确定所述目标动态口令不满足预设时效性条件时所发送的提示信息，并基于所述提示信息进行提示。

11、一种扫码控制方法，其特征在于，包括：

基于后台服务端下发的图形码信息展示相应的图形码，其中，所述图形码是动态更新的，每个所述图形码对应于一个唯一的动态口令；

30 接收所述后台服务端发送的控制指令，其中，所述控制指令是所述后台服务端针对接收到的设备控制请求中携带的目标动态口令的时效性判断结果生成的。

12、根据权利要求 11 所述的方法，其特征在于，所述接收所述后台服务端发送的控制指令，包括：

接收所述后台服务端确定所述目标动态口令满足预设时效性条件时所发送的控制指令，以及基于所述控制指令执行相应的控制动作。

5 13、一种扫码控制方法，其特征在于，包括：

接收客户端发送的针对扫码售卖设备的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应；

10 根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

14、根据权利要求 13 所述的方法，其特征在于，在接收客户端发送的针对扫码售卖设备的设备控制请求之前，还包括：

根据目标扫码售卖设备的设备标识、与所述设备标识对应的标识密钥以及时间戳信息中的至少两个，确定动态口令；

15 根据确定出的所述动态口令，生成图形码信息；

将所述图形码信息下发给所述目标扫码售卖设备，以使所述目标扫码售卖设备基于所述图形码信息显示图形码。

15、根据权利要求 14 所述的方法，其特征在于，在确定动态口令之后，还包括：

20 将所述动态口令添加至动态口令集合，以及当所述动态口令满足预设销毁条件时，将所述动态口令从所述动态口令集合中移除，其中，所述预设销毁条件包括：动态口令达到预设存活时间和/或动态口令已使用；

所述判断所述目标动态口令是否满足预设时效性条件，包括：

若所述动态口令集合中存在所述目标动态口令，则确定所述目标动态口令满足预设时效性条件；

25 若所述动态口令集合中不存在所述目标动态口令，则确定所述目标动态口令不满足预设时效性条件。

16、根据权利要求 15 所述的方法，其特征在于，所述将所述动态口令从所述动态口令集合中移除之后，还包括：

30 生成新的动态口令，基于所述新的动态口令更新所述目标扫码售卖设备上显示的图形码。

17、一种扫码控制装置，其特征在于，包括：

请求接收模块，用于接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

口令识别模块，用于判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

5 控制模块，用于根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

18、一种扫码控制装置，其特征在于，包括：

请求接收模块，用于接收客户端发送的针对扫码售卖设备的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；

10 口令识别模块，用于判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应；

控制模块，用于根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

19、一种扫码控制系统，其特征在于，包括：后台服务端、客户端和设备终端；

其中，所述后台服务端，用于接收客户端发送的设备控制请求；判断所述设备控制请求中携带的目标动态口令是否满足预设时效性条件；根据针对所述目标动态口令的时效性判断结果执行相应的控制操作；

所述客户端，用于向后台服务端发送设备控制请求；以及接收所述后台服务端针对所述目标动态口令的时效性判断结果发送的反馈信息；

20 所述设备终端，用于基于后台服务端下发的图形码信息展示相应的图形码，其中，所述图形码是动态更新的，每个所述图形码对应于一个唯一的动态口令；以及接收所述后台服务端针对所述目标动态口令的时效性判断结果发送的控制指令。

20、一种扫码控制设备，其特征在于，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

25 接收客户端发送的设备控制请求，其中，所述设备控制请求中携带有目标动态口令；判断所述目标动态口令是否满足预设时效性条件，其中，所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应；

根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

21、一种扫码控制设备，其特征在于，包括：

30 处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理

器:

接收客户端发送的针对扫码售卖设备的设备控制请求, 其中, 所述设备控制请求中携带有目标动态口令;

5 判断所述目标动态口令是否满足预设时效性条件, 其中, 所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应;

根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

22、一种存储介质, 用于存储计算机可执行指令, 其特征在于, 所述可执行指令在被执行时实现以下流程:

接收客户端发送的设备控制请求, 其中, 所述设备控制请求中携带有目标动态口令;

10 判断所述目标动态口令是否满足预设时效性条件, 其中, 所述目标动态口令与目标设备终端上显示的动态更新的图形码一一对应;

根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

23、一种存储介质, 用于存储计算机可执行指令, 其特征在于, 所述可执行指令在被执行时实现以下流程:

15 接收客户端发送的针对扫码售卖设备的设备控制请求, 其中, 所述设备控制请求中携带有目标动态口令;

判断所述目标动态口令是否满足预设时效性条件, 其中, 所述目标动态口令与目标扫码售卖设备上显示的动态更新的图形码一一对应;

根据针对所述目标动态口令的时效性判断结果执行相应的控制操作。

20

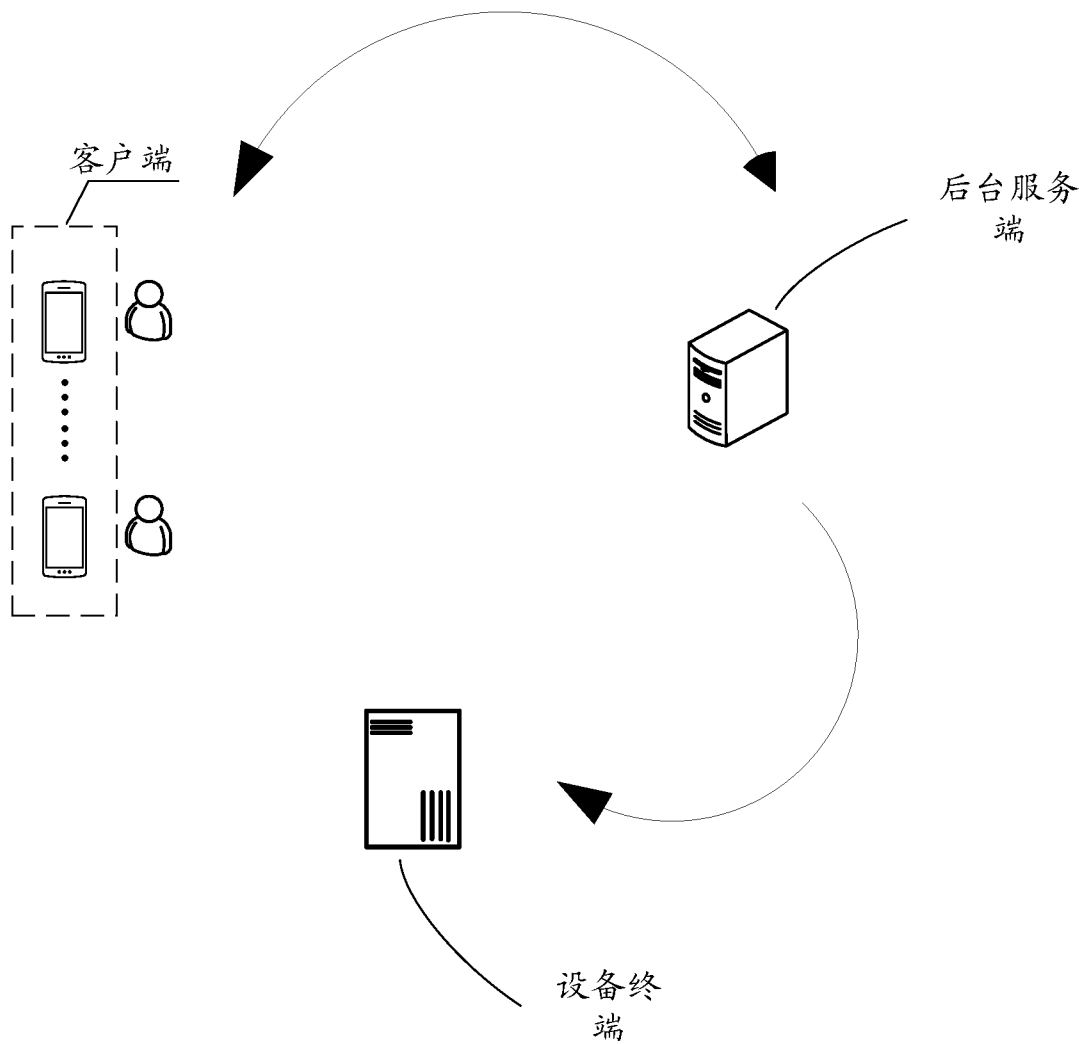


图 1

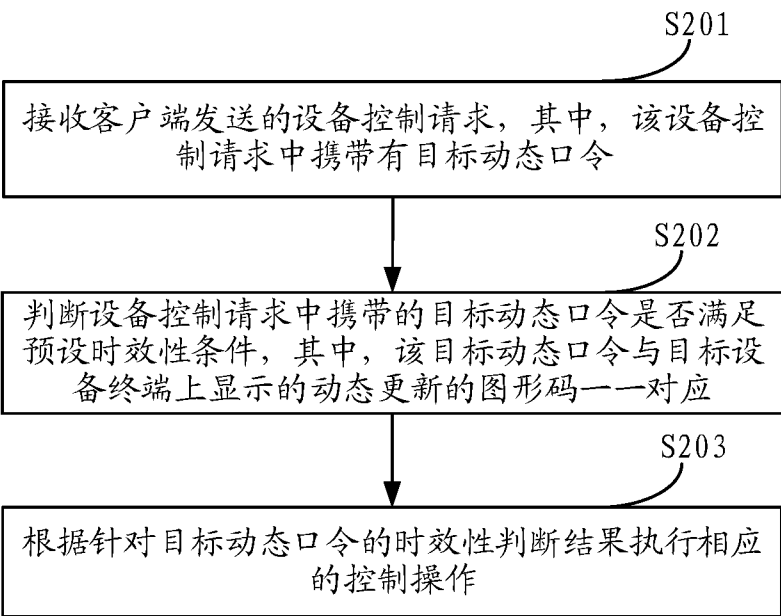


图 2

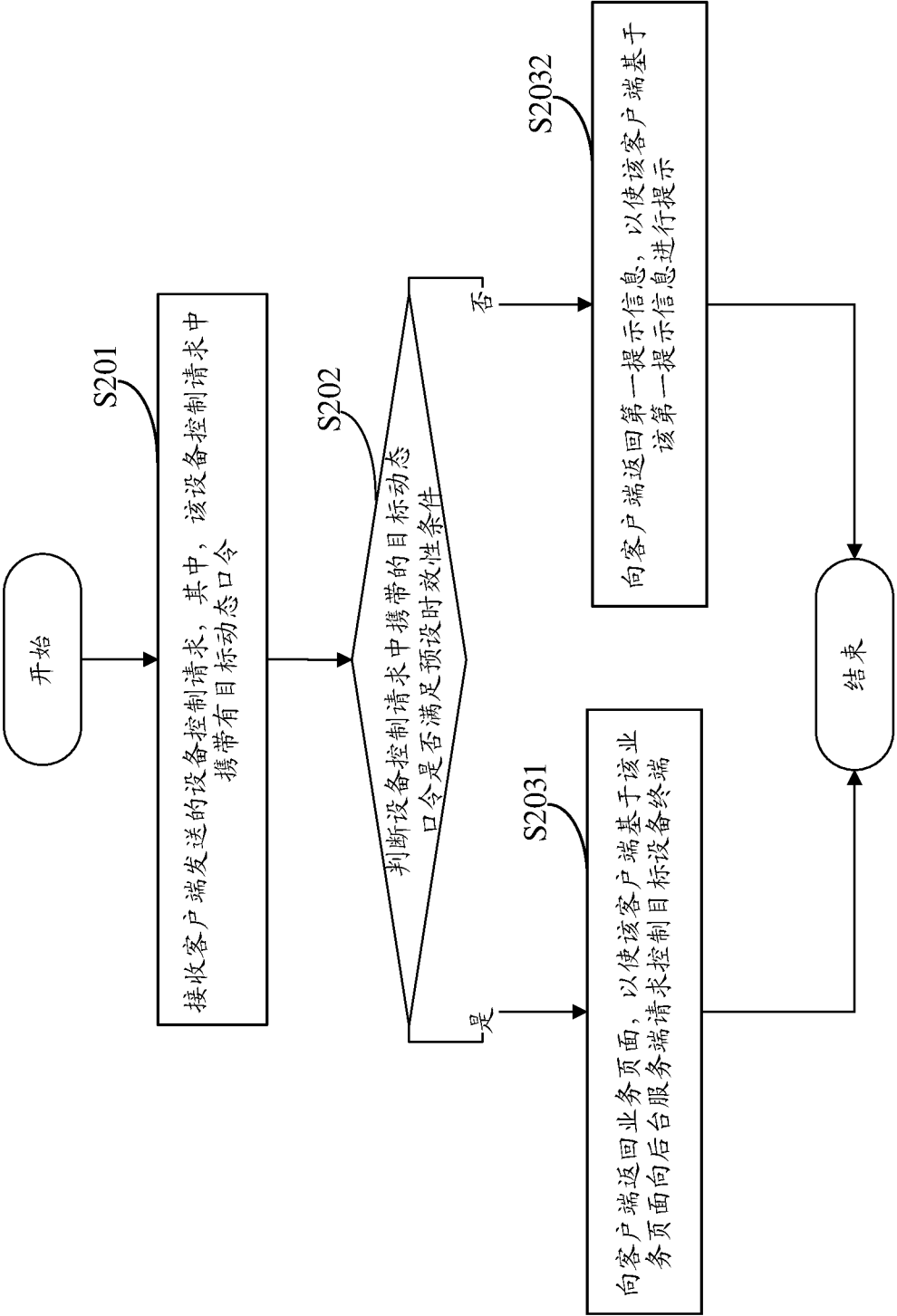


图 3

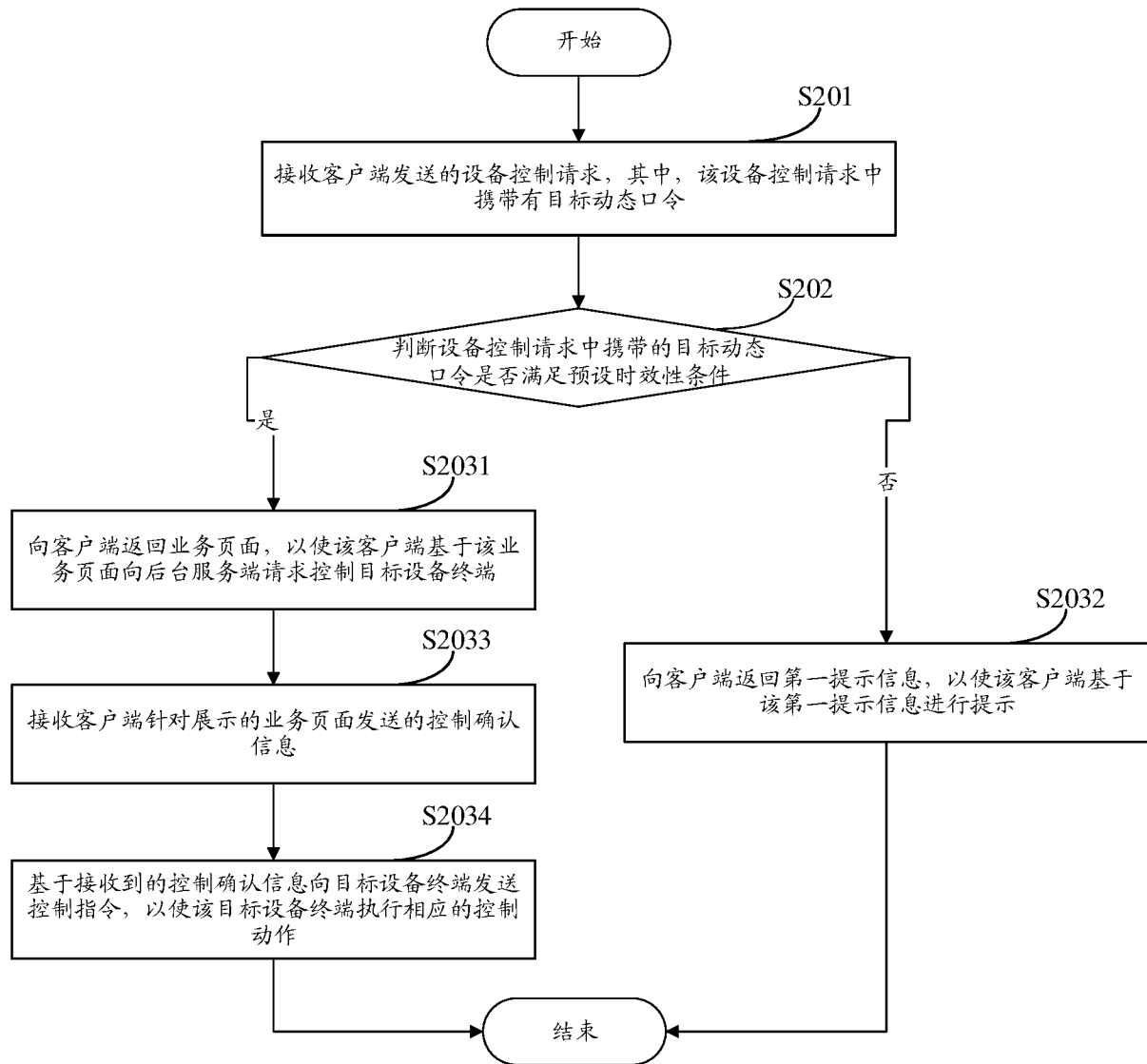


图 4

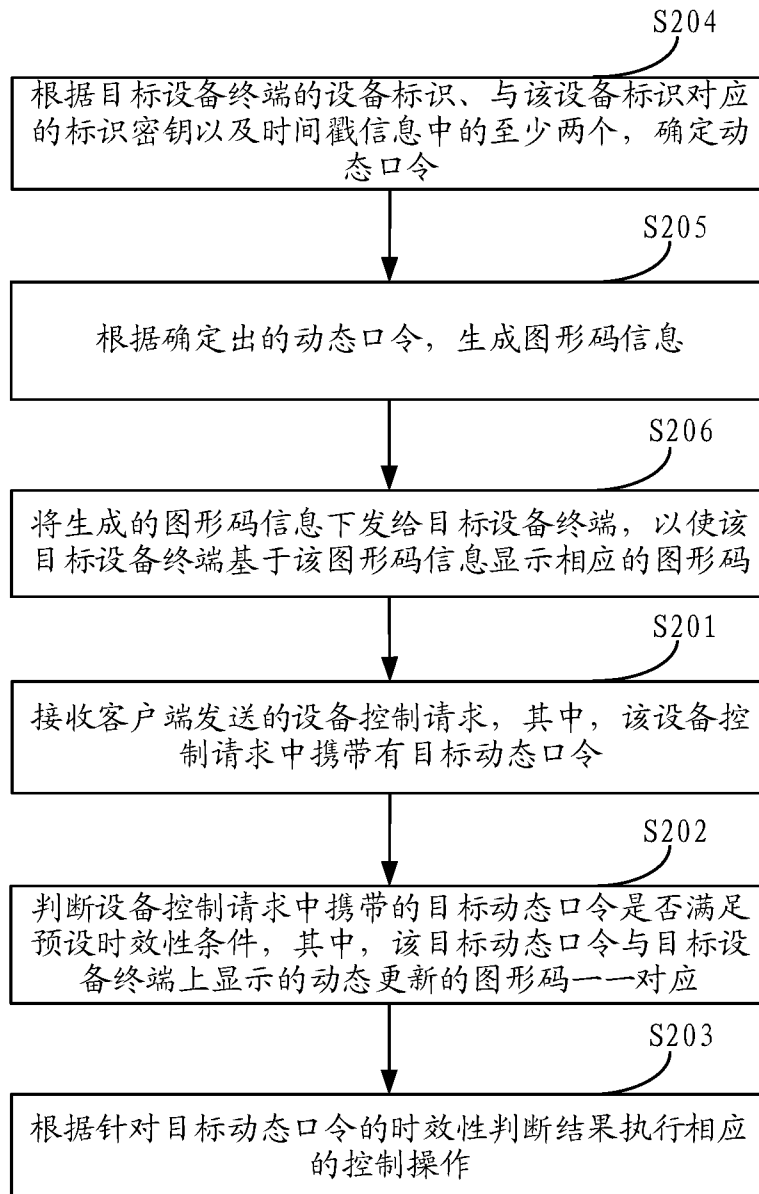


图 5

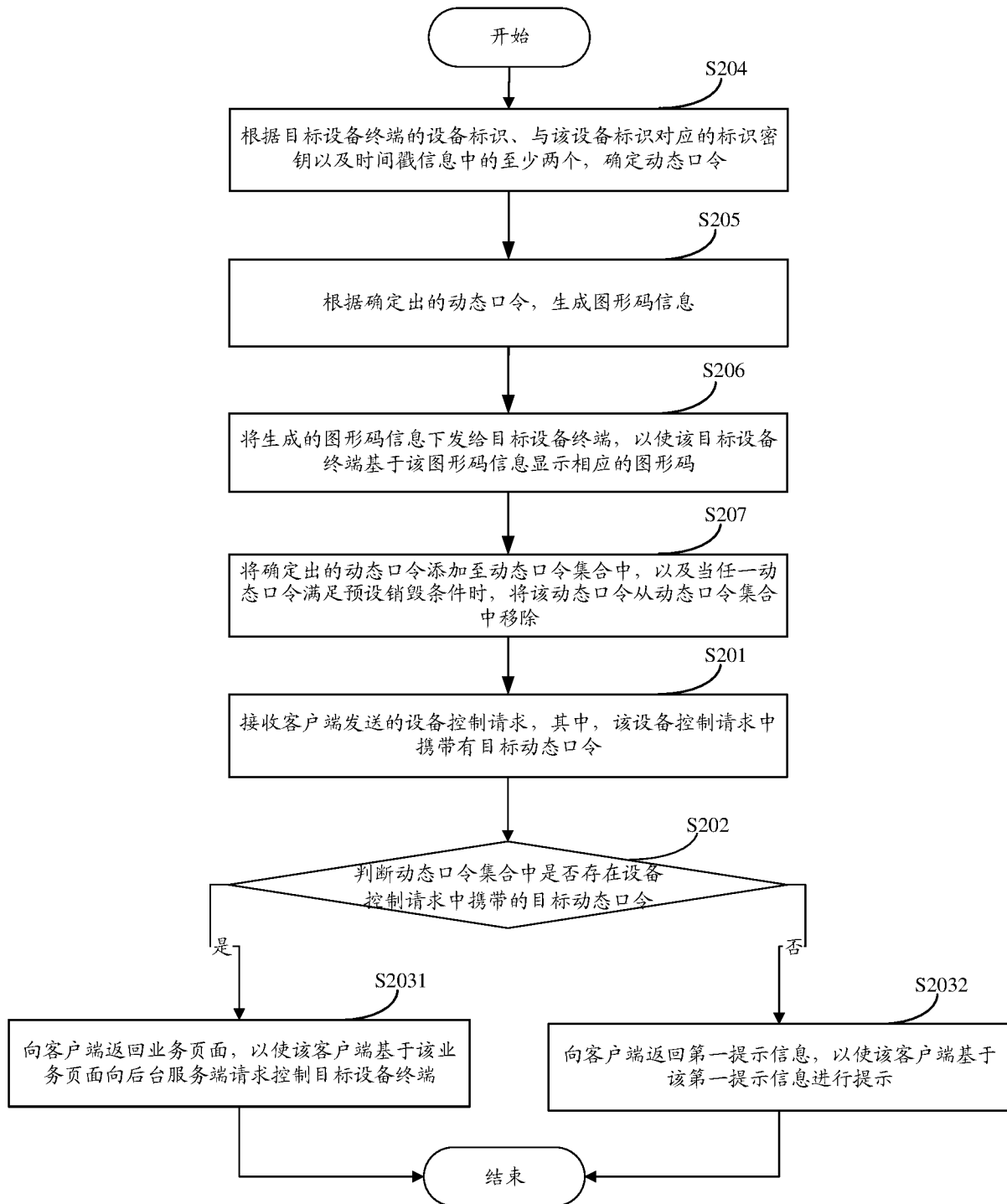


图 6

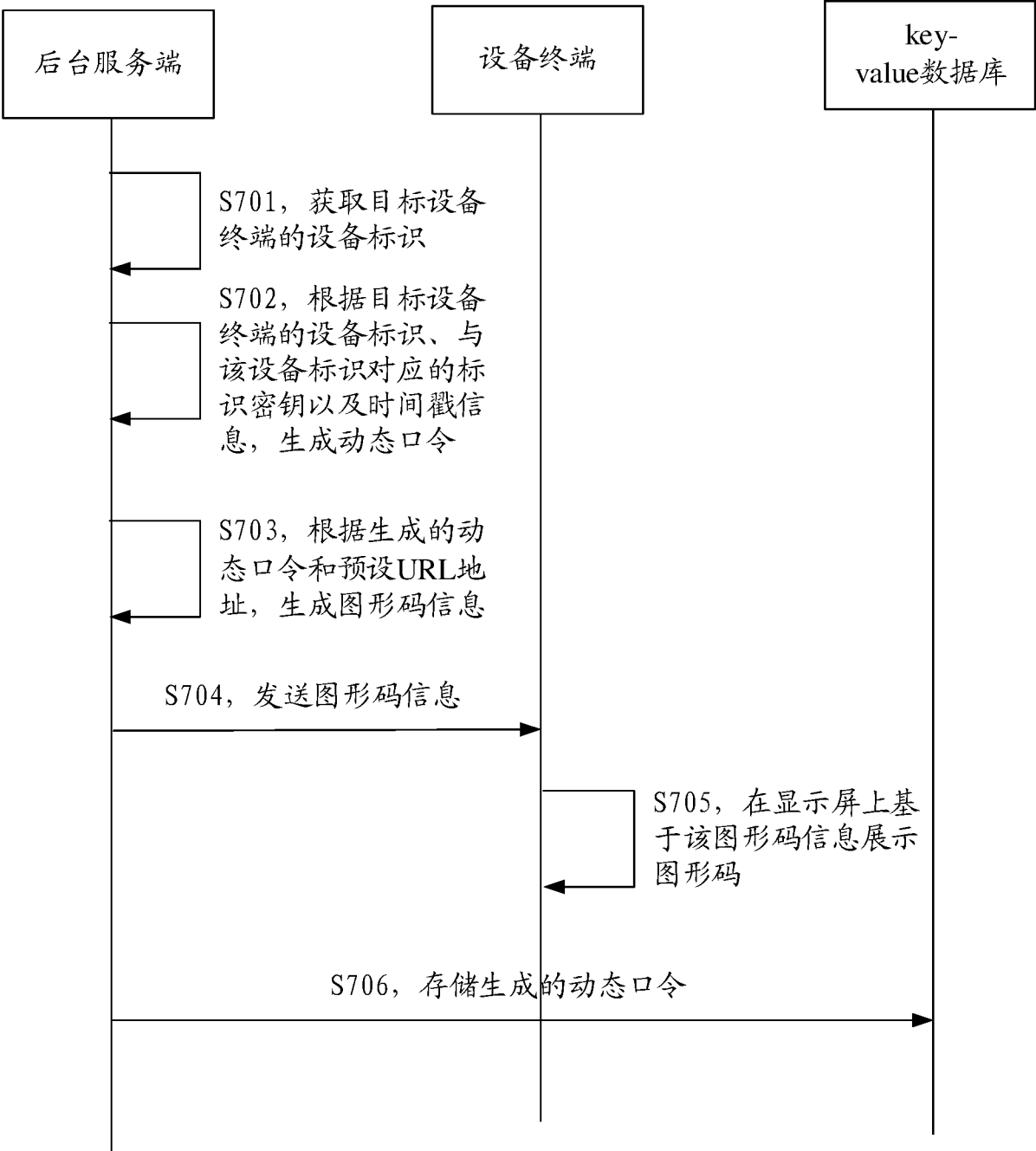


图 7a

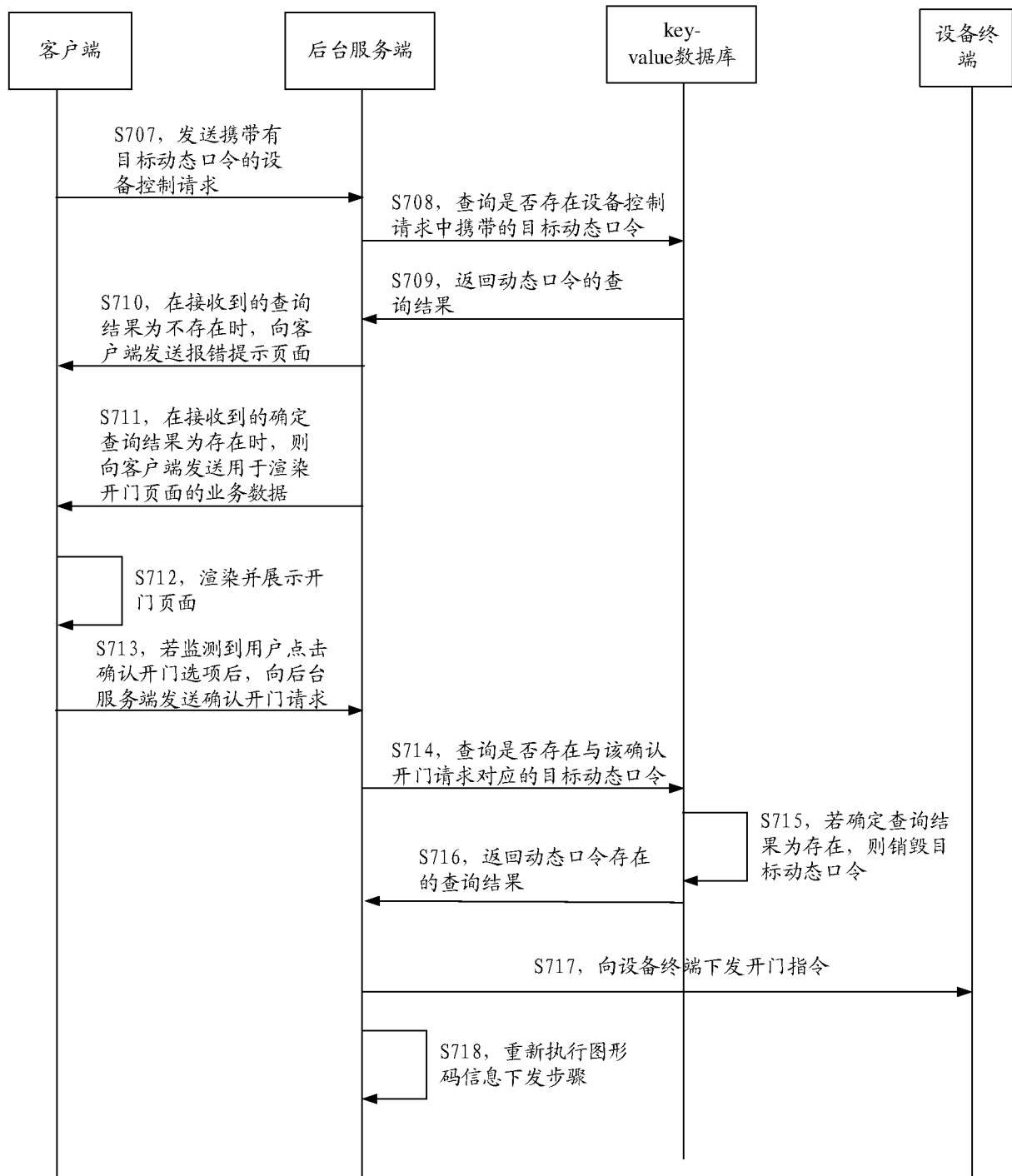


图 7b

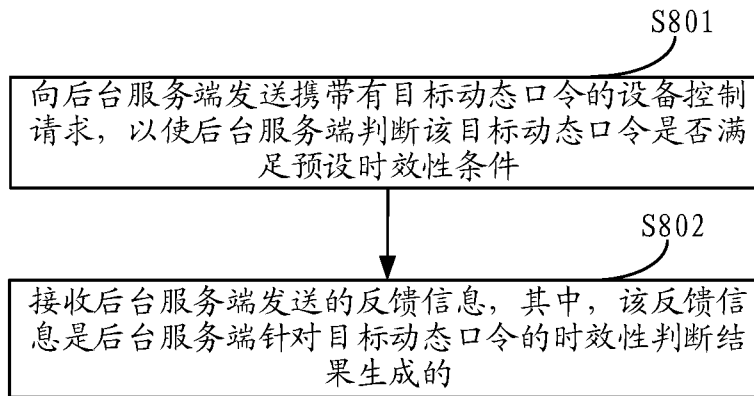


图 8

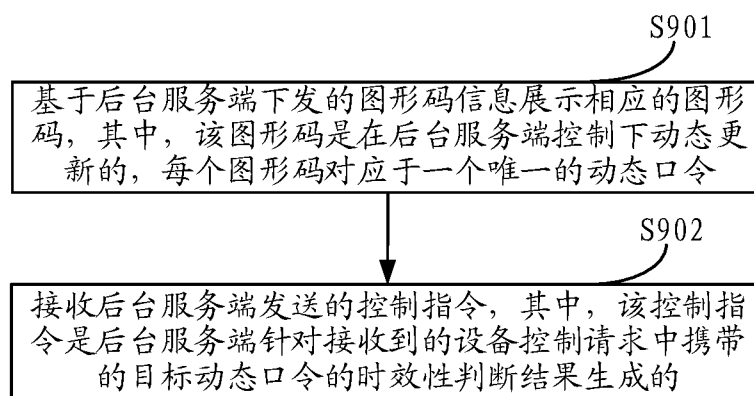


图 9

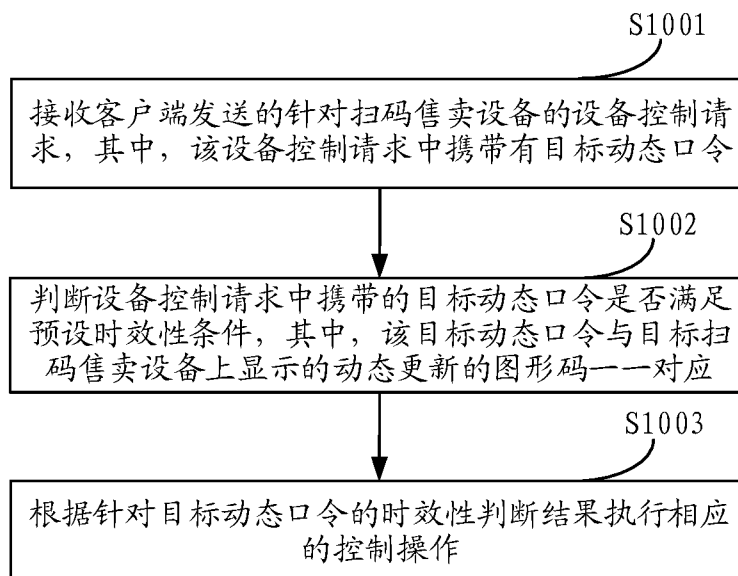


图 10

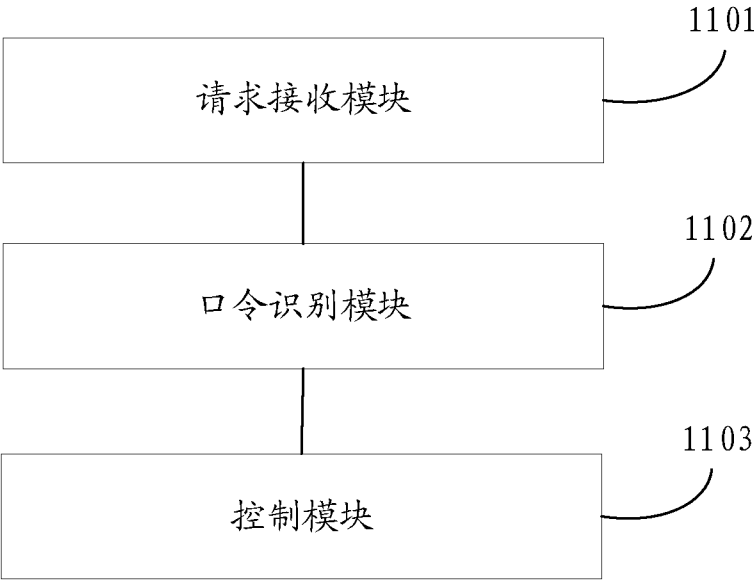


图 11

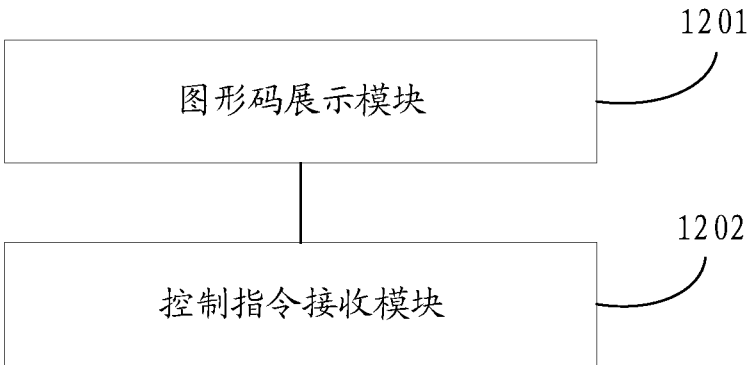


图 12

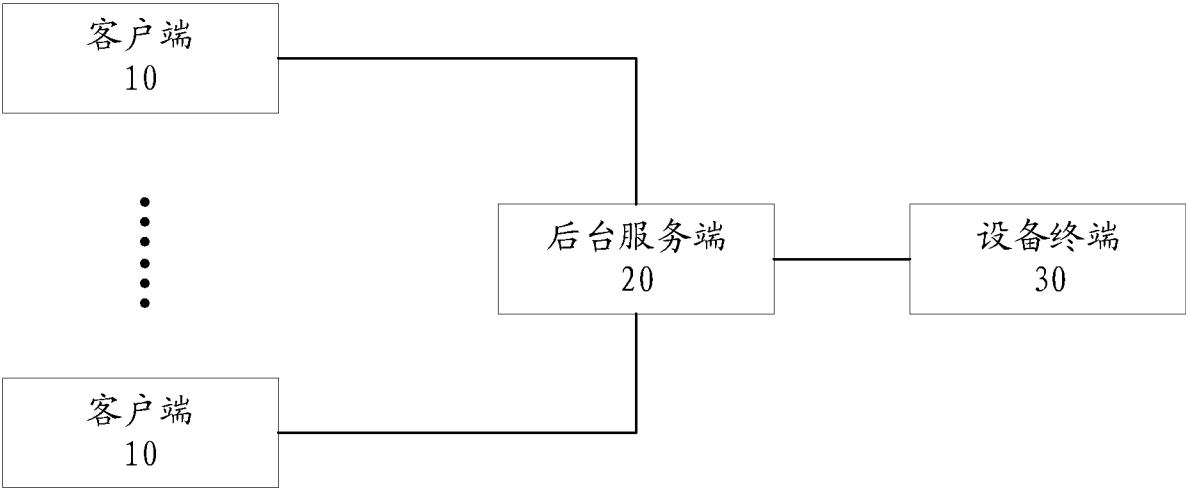


图 13

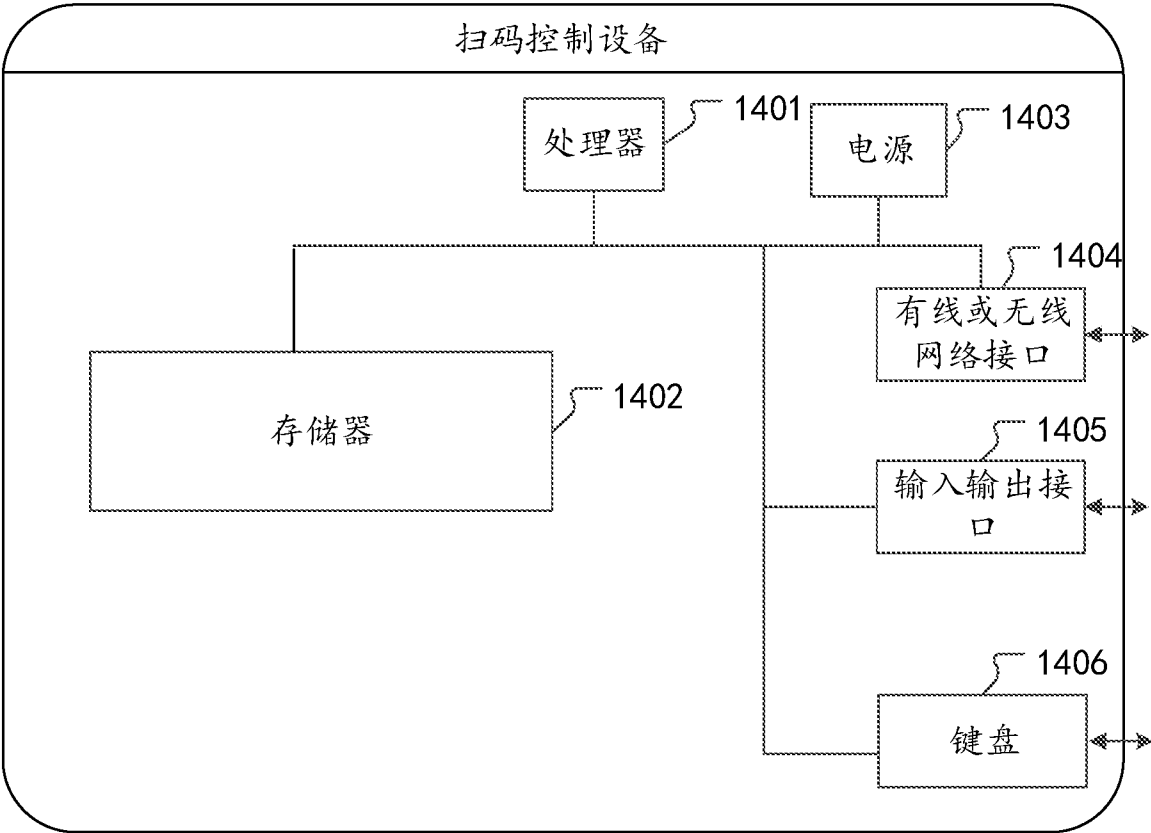


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/098999

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/18(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

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; IEEE: 二维码, 条形码, 动态, 静态, 控制, 门禁, 售货机, 扫描, 验证, 时效, 时间戳, 攻击, 复制, two dimensional code, barcode, dynamic, static, control, door access lock, vending machine, scan, verify, timeliness, time, attack, copy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109389386 A (ALIBABA GROUP HOLDING LIMITED) 26 February 2019 (2019-02-26) description, paragraphs 0006-0042, and claims 1-23	1-23
X	CN 106204864 A (BEIJING UPVALUE INTELLECTUAL PROPERTY CONSULTANT CO., LTD.) 07 December 2016 (2016-12-07) description, paragraphs 0005-0032 and 0067-0090, and figure 1	1-23
A	CN 107256584 A (LI, ZHIYING) 17 October 2017 (2017-10-17) entire document	1-23
A	US 2010125509 A1 (KRANZLEY, A. D. ET AL.) 20 May 2010 (2010-05-20) entire document	1-23



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

29 September 2019

Date of mailing of the international search report

30 October 2019

Name and mailing address of the ISA/CN

**China National Intellectual Property Administration (ISA/
CN)**
**No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088**
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/098999

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109389386	A	26 February 2019	None			
CN	106204864	A	07 December 2016	None			
CN	107256584	A	17 October 2017	None			
US	2010125509	A1	20 May 2010	US	2018114213	A1	26 April 2018
				US	2010125516	A1	20 May 2010

国际检索报告

国际申请号

PCT/CN2019/098999

A. 主题的分类

G06Q 20/18(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

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;EPDOC;IEEE: 二维码,条形码,动态,静态,控制,门禁,售货机,扫描,验证,时效,时间戳,攻击,复制, two dimensional code, barcode, dynamic, static, control, door access lock, vending machine, scan, verify, timeliness, time, attack, copy

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 109389386 A (阿里巴巴集团控股有限公司) 2019年 2月 26日 (2019 - 02 - 26) 说明书第0006-0042段, 权利要求第1-23项	1-23
X	CN 106204864 A (北京厚文知识产权顾问有限公司) 2016年 12月 7日 (2016 - 12 - 07) 说明书第0005-0032、0067-0090段、附图1	1-23
A	CN 107256584 A (黎志瀛) 2017年 10月 17日 (2017 - 10 - 17) 全文	1-23
A	US 2010125509 A1 (KRANZLEY, ARTHUR D. 等) 2010年 5月 20日 (2010 - 05 - 20) 全文	1-23

☐ 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

2019年 9月 29日

国际检索报告邮寄日期

2019年 10月 30日

ISA/CN的名称和邮寄地址

中国国家知识产权局(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

授权官员

刘静微

电话号码 86-10-53961592

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/098999

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	109389386	A	2019年 2月 26日	无			
CN	106204864	A	2016年 12月 7日	无			
CN	107256584	A	2017年 10月 17日	无			
US	2010125509	A1	2010年 5月 20日	US	2018114213	A1	2018年 4月 26日
				US	2010125516	A1	2010年 5月 20日