

(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 4 月 26 日 (26.04.2018)



(10) 国际公布号
WO 2018/072403 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/079616

(22) 国际申请日: 2017 年 4 月 6 日 (06.04.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610916303.7 2016 年 10 月 20 日 (20.10.2016) CN

(71) 申请人: 武汉斗鱼网络科技有限公司
(**WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.**) [CN/CN]; 中国湖北省武汉市东湖开发区软件园东路 1 号软件产业 4.1 期 B1 栋 11 楼, Hubei 430000 (CN)。

(72) 发明人: 郝梦茹 (**HAO, Mengru**); 中国湖北省武汉市东湖开发区软件园东路 1 号软件产

业 4.1 期 B1 栋 11 楼, Hubei 430000 (CN)。周志刚 (**ZHOU, Zhigang**); 中国湖北省武汉市东湖开发区软件园东路 1 号软件产业 4.1 期 B1 栋 11 楼, Hubei 430000 (CN)。

(74) 代理人: 北京超凡志成知识产权代理事务所 (普通合伙) (**CHOFN INTELLECTUAL PROPERTY**); 中国北京市海淀区北四环西路 68 号左岸工社 12 层 1215-1218 室, Beijing 100080 (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, 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,

(54) **Title:** PASSWORD RESET METHOD, APPARATUS, TERMINAL DEVICE AND SERVER, AND COMPUTER-READABLE MEDIUM

(54) 发明名称: 密码重设方法、装置、终端设备及服务器、计算机可读介质

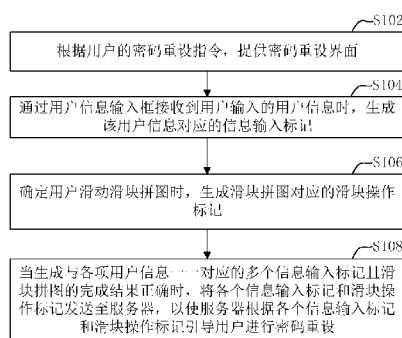


图 2

- S102 Providing a password reset interface according to a password reset instruction of a user
- S104 Generating an information input mark corresponding to user information when receiving the user information input by the user by means of the user information input boxes
- S106 Generating a slide block operation mark corresponding to a slide block puzzle when determining that the user slides the slide block puzzle
- S108 Sending each information input mark and the slide block operation marks to a server when the plurality of the information input marks that are in one-to-one correspondence with the various user information are generated and a completion result of the slide block puzzle is correct, so that the server instructs the user to reset a password according to each information input mark and the slide block operation marks

(57) **Abstract:** Provided by the present application are a password reset method, an apparatus, a processing device and server, and a computer-readable medium, the method comprising: providing a password reset interface according to a password reset instruction of a user, the password reset interface comprising a plurality of user information input boxes and slide block puzzles that are in one-to-one correspondence with various user information; generating an information input mark corresponding to the user information when receiving the user information input by the user by means of the user information input boxes; generating a slide block operation mark corresponding to a slide block puzzle when determining that the user slides the slide block puzzle; and sending each information input mark and the slide block operation marks to a server when the plurality of the information input marks that are in one-to-one correspondence with the various user information are generated and a completion result of the slide block puzzle is correct, so that the server instructs the user to reset a password according to each information input mark and the slide block operation marks. By means of the password reset method, apparatus, processing device and server of the present application, the difficulty in cracking a communication protocol between a terminal device and a server may be increased, and the risk of a user password being stolen may be reduced.

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: 本申请提供了一种密码重设方法、装置、处理设备及服务器、计算机可读介质, 该方法包括: 根据用户的密码重设指令提供密码重设界面, 密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图; 通过用户信息输入框接收到用户输入的用户信息时, 生成用户信息对应的信息输入标记; 确定用户滑动所述滑块拼图时, 生成滑块拼图对应的滑块操作标记; 当生成与各项用户信息一一对应的多个所述信息输入标记且滑块拼图的完成结果正确时, 将各个信息输入标记和滑块操作标记发送至服务器, 以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。通过本申请中的密码重设方法、装置、处理设备及服务器能够提高终端设备与服务器之间的通信协议的破解难度, 降低用户密码被盗的风险。

密码重设方法、装置、终端设备及服务器、计算机可读介质

本申请要求于 2016 年 10 月 20 日提交中国专利局、申请号为 CN201610916303.7、发明名称为“密码重设方法及装置”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。

技术领域

本申请涉及互联网技术领域，具体而言，涉及一种密码重设方法、装置、终端设备及服务器、计算机可读介质。

背景技术

目前，各个网站均提供账号密码登录功能，用户需要在网站中输入有效的账号和密码，网站对账号和密码进行校验，校验通过后用户登录成功，否则登录失败。

当用户忘记密码时，能够通过网站提供的密码重设功能重设密码。相关技术中的密码重设流程大致如下：用户在终端设备提供的网页面上输入用户信息，如昵称和手机号码，终端设备将用户信息发送至服务器，服务器校验该用户信息是否正确，如果正确，则通过终端设备引导用户重新设置密码，如果不正确，则通过终端设备提示上述用户信息错误。

相关技术中的密码重设流程，终端设备将用户信息发送至服务器，服务器在校验获取到的用户信息正确后引导用户重设密码。然而，相关技术中终端设备与服务器之间的通信协议很容易被黑客破解，黑客破解终端设备与服务器之间的通信协议后，能够拦截终端设备与服务器之间的通信数据，或者绕开终端设备直接与服务器通信，从而冒充用户重设密码，导致用户密码被盗。

可见，相关技术中终端设备与服务器之间的通信协议破解难度低，用户密码被盗的风险大。

发明内容

有鉴于此，本申请的目的在于提供一种密码重设方法、装置、终端设备及服务器、计算机可读介质，以提高终端设备与服务器之间的通信协议的破解难度，降低用户密码被盗的风险。

第一方面，本申请实施例提供了一种密码重设方法，包括：根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

结合第一方面，本申请实施例提供了第一方面第一种可能的实施方式，其中，所述生成所述用户信息对应的信息输入标记，包括：利用第一预设算法对第一预设参数进行运算，生成所述用户信息对应的信息输入标记，其中，所述第一预设参数包括当前日期或者所述用户信息的全部或部分内容。

结合第一方面，本申请实施例提供了第一方面第二种可能的实施方式，其中，所述生成所

述滑块拼图对应的滑块操作标记，包括：利用第二预设算法对第二预设参数进行运算，生成所述滑块拼图对应的滑块操作标记，其中，所述第二预设参数包括当前日期。

结合第一方面，本申请实施例提供了第一方面第三种可能的实施方式，其中，对应用户信息输入框设置信息参数，所述生成所述用户信息对应的信息输入标记，包括：将所述信息参数赋值为第一预设协议值，生成用户信息对应的信息输入标记。

结合第一方面，本申请实施例提供了第一方面第四种可能的实施方式，其中，对应滑块操作设置滑块参数，所述生成所述滑块拼图对应的滑块操作标记，包括：将滑块参数赋值为第二预设协议值，生成滑块拼图对应的滑块操作标记。结合第一方面，本申请实施例提供了第一方面第五种可能的实施方式，其中，在所述通过所述用户信息输入框接收到用户输入的用户信息后，所述方法还包括：将所述用户信息发送至所述服务器，以使所述服务器校验所述用户信息是否正确；在接收到所述服务器发送的各项所述用户信息均校验正确的指令后，将所述滑块拼图变为可滑动状态。

结合第一方面上述的实施方式，本申请实施例提供了第一方面第六种可能的实施方式，其中，所述将各个所述信息输入标记和所述滑块操作标记发送至服务器，包括：对各个所述信息输入标记和所述滑块操作标记进行加密，将各个所述信息输入标记和所述滑块操作标记的密文发送至所述服务器。

第二方面，本申请实施例提供了一种密码重设方法，包括：在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；若各个所述信息输入标记和所述滑块操作标记均符合所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

结合第二方面，本申请实施例提供了第二方面第一种可能的实施方式，其中，所述校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则，包括：通过第一预设算法解析所述信息输入标记，校验解析结果是否为第一预设参数，若是，则确定所述信息输入标记符合所述预设规则，所述第一预设参数包括当前日期或者所述信息输入标记对应的用户信息的全部或部分内容。

结合第二方面，本申请实施例提供了第二方面第二种可能的实施方式，其中，校验所述滑块操作标记是否符合预设规则包括：通过第二预设算法解析所述滑块操作标记，校验解析结果是否为第二预设参数，若是，则确定所述滑块操作标记符合所述预设规则，所述第二预设参数

包括当前日期。

结合第二方面，本申请实施例提供了第二方面第三种可能的实施方式，其中，所述信息输入标记中包括信息参数，所述校验各个所述信息输入标记是否均符合预设规则，包括：校验信息输入标记中信息参数的值是否为第一预设协议值，若是，则确定信息输入标记符合预设规则。

结合第二方面，本申请实施例提供了第二方面第四种可能的实施方式，其中，所述滑块操作标记中包括滑块参数，校验所述滑块操作标记是否符合预设规则包括：校验滑块操作标记中滑块参数的值是否为第二预设协议值，若是，则确定滑块操作标记符合预设规则。

结合第二方面，本申请实施例提供了第二方面第五种可能的实施方式，其中，在判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记之前，所述方法还包括：接收所述终端设备发送的所述用户信息，校验所述用户信息是否正确；当校验所述用户信息正确时，向所述终端设备发送所述用户信息校验正确的指令。

结合第二方面上述的实施方式，本申请实施例提供了第二方面第六种可能的实施方式，其中，各个所述信息输入标记和所述滑块操作标记均为密文形式，所述校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则，包括：对各个所述信息输入标记和所述滑块操作标记进行解密，得到各个所述信息输入标记和所述滑块操作标记的明文；校验各个所述信息输入标记和所述滑块操作标记的明文是否均符合所述预设规则。

第三方面，本申请实施例提供了一种密码重设装置，包括：界面提供模块，用于根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；第一标记生成模块，用于通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；第二标记生成模块，用于确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；标记发送模块，用于当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

第四方面，本申请实施例提供了一种密码重设装置，包括：标记判断模块，用于在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；标记校验模块，用于若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；指令发送模块，用于若各个所述信息输入标记和

所述滑块操作标记均符合所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

第五方面，本申请实施例提供了一种终端设备，包括：存储器，被配置为存储程序，处理器，被配置为通过调用所述存储器中存储的程序，执行包括以下步骤的方法：根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

第六方面，本申请实施例提供了一种服务器，所述服务器包括：存储器，被配置为存储程序，处理器，被配置为通过调用所述存储器中存储的程序，执行包括以下步骤的方法：在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；若各个所述信息输入标记和所述滑块操作标记均符合所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

根据本发明再一方面，提供一种具有处理器可执行的非易失的程序代码的计算机可读介质，所述程序代码使所述处理器执行上述方法。

本申请实施例中的方法、装置、终端设备及服务器、计算机可读介质，根据用户的密码重设指令，提供密码重设界面，该密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图；通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记；确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记；当生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。与相关技术相比，通过本实施例中的方法、装置、终端设备及服务器、计算机可读介质，终端设备与服务器之间在进行通信时，通信内容中增加了多个信息输入标记和滑块操作标记，也即改变了原有的通信格式和通信内容，使得通信内容更多，从而提高了终端设备与服务器之间的通信协议的破解难度，降低了用户密码被盗的风险。

为使本申请的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

图 1 为本申请较佳实施例提供的服务器与终端设备进行交互的示意图；

图 2 示出了本申请实施例提供的密码重设方法的终端设备侧的流程示意图；

图 3 示出了本申请实施例提供的密码重设界面的示意图；

图 4 示出了本申请实施例提供的密码重设方法的服务器侧的流程示意图；

图 5 示出了本申请实施例所提供的位于终端设备侧的密码重设装置的模块组成示意图；

图 6 示出了本申请实施例所提供的位于服务器侧的密码重设装置的模块组成示意图；

图 7 是本申请的实施例所提供的一种电子设备的示意性方框图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中附图，对本申请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申请一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本申请的实施例的详细描述并非旨在限制要求保护的本申请的范围，而是仅仅表示本申请的选定实施例。基于本申请的实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本申请保护的范围。

如图 1 所示，是本发明较佳实施例提供的服务器与终端设备进行交互的示意图。所述服务器通过网络与一个或多个终端设备进行通信连接，以进行数据通信或交互。所述服务器可以是网络服务器、数据库服务器等。所述终端设备可以是个人电脑（personal computer，PC）、平板电脑、智能手机、个人数字助理（personal digital assistant，PDA）等。

考虑到相关技术中终端设备与服务器之间的通信协议破解难度低，用户密码被盗的风险大的问题，本申请实施例提供了一种密码重设方法、装置、终端设备及服务器、计算机可读介质，以提高终端设备与服务器之间的通信协议的破解难度，降低用户密码被盗的风险，下面结合实施例进行具体描述。

图 2 示出了本申请实施例提供的密码重设方法的终端设备侧的流程示意图，该方法由终端设备执行，如图 2 所示，该方法包括以下步骤：

步骤 S102，根据用户的密码重设指令，提供密码重设界面，该密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项。

本实施例中，终端设备内安装有特定的应用程序，如网站 APP，或者运行有特定的应用平台，如通过浏览器运行的网页，当用户通过该应用程序或者该应用平台输入密码重设指令时，如在该应用程序或者该应用平台提供的登录界面上点击“忘记密码”控件时，该应用程序或者该应用平台接收用户输入的密码重设指令，向用户提供密码重设界面。

图 3 示出了本申请实施例提供的密码重设界面的示意图。如图 3 所示，密码重设界面包括多个用户信息输入框，每个用户信息输入框与一项用户信息相对应，用户信息至少包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，其中指定问题可以是用户注册时预留的密保问题。图 3 中，用户信息包括用户账号和用户手机号，用户信息输入框包括两个，一个用于输入用户账号，另一个用于输入用户手机号。如图 3 所示，该密码重设界面还包括滑块拼图，当用户拖动滑块到正确位置时，该应用程序或者该应用平台确定滑块拼图完成结果正确。

本实施例中，滑块拼图的实现方式有多种，具体可以是如图 3 所示的拖动滑块的同时拼图随之移动，当用户沿着滑块移动指示方向拖动滑块至指定位置时，拼图成功。

步骤 S104，通过用户信息输入框接收到用户输入的用户信息时，生成该用户信息对应的信息输入标记。

本实施例中，用户信息包括多项信息，每项用户信息均对应有一个用户信息输入框，当终端设备通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记，信息输入标记用于表示用户通过用户信息输入框输入用户信息的行为动作的发生。

具体地，当用户点击用户信息输入框时，用户信息输入框被激活，当用户在用户信息输入框内输入字符信息时，终端设备接收用户输入的字符信息，将该字符信息作为用户信息。

用户通过用户信息输入框输入的每项用户信息都对应有一个信息输入标记，终端设备生成用户信息对应的信息输入标记的具体过程可以是：利用第一预设算法对第一预设参数进行运算，生成用户信息对应的信息输入标记，其中，第一预设参数包括当前日期或者用户信息的全部或部分内容，第一预设算法可以是对称加密算法，或者是非对称加密算法。

具体地，终端设备以当前日期，如年-月-日中的“日”作为第一预设参数，利用第一预设算法对第一预设参数进行对称加密，将得到的结果作为用户信息对应的信息输入标记。由于第一预设参数为当前日期时，各项用户信息对应的信息输入标记均一致，为了进一步提高信息输入标记的灵活性，还可以设置第一预设参数为用户信息的全部或者部分内容，利用第一预设算法对第一预设参数进行对称加密，将得到的结果作为用户信息对应的信息输入标记，由于每项用户信息的具体内容均不相同，因此将用户信息的全部或者部分内容作为第一预设参数，能够使得各个信息输入标记的内容均不相同，从而提高信息输入标记的灵活性。

一种具体的实施例中，第一预设参数为当前日期，如 20 日，对字符“20”进行对称加密，得到信息输入标记。另一种具体的实施例中，用户信息为用户账号，将用户账号的全部字符作为第一预设参数，对用户账号的全部字符进行非对称加密，得到用户账号对应的信息输入标记；

用户信息为用户手机号，将手机号后四位作为第一预设参数，对手机号后四位进行对称加密，得到用户手机号对应的信息输入标记。

当然，在本实施例中，终端设备生成用户信息对应的信息输入标记的具体过程也可以是：对应用户信息输入框设置信息参数，通过用户信息输入框接收到用户输入的用户信息时，将信息参数赋值为第一预设协议值，生成用户信息对应的信息输入标记。

例如，用户账号为用户昵称，设置信息参数 `nicknameflag`，用户通过用户账号对应的信息输入框输入用户昵称时，将该信息参数 `nicknameflag` 赋值为第一预设协议值 1，得到表明用户发生了昵称输入动作的用户昵称对应的信息输入标记。若用户信息还包括用户手机号，设置信息参数 `phoneflag`，用户通过用户手机号对应的信息输入框输入用户信息时，将该信息参数 `nicknameflag` 赋值为第一预设协议值 1，得到表明用户发生了手机号输入动作的用户手机号对应的信息输入标记。可以理解的，第一预设协议值的具体值并不作为限定，并且，不同的用户信息输入框，其对应的第一预设协议值也可以不同。

本实施例中，当终端设备通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记，从而标记用户在页面上输入该项用户信息的行为动作的发生，达到记录用户页面操作的目的。

步骤 S106，确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记。

当终端设备确定用户滑动密码重设界面上的滑块拼图时，生成滑块拼图对应的滑块操作标记。

具体地，当终端设备监听到用户点击密码重设界面上的滑块并且拖动该滑块时，无论用户的滑动拼图的完成结果是否正确，终端设备均生成滑块拼图对应的滑块操作标记，从而标记用户在密码生成界面上滑动滑块的行为的发生，记录用户的页面操作。

终端设备生成滑块拼图对应的滑块操作标记的具体过程可以是：利用第二预设算法对第二预设参数进行运算，生成滑块拼图对应的滑块操作标记，其中，第二预设参数包括当前日期，第二预设算法可以是对称加密算法，或者是非对称加密算法。

具体地，终端设备以当前日期，如年-月-日中的“日”作为第二预设参数，利用第二预设算法对第二预设参数进行对称加密，将得到的结果作为滑块拼图对应的滑块操作标记。一种具体的实施例中，第一预设参数为当前日期，如 25 日，对字符“25”进行对称加密，得到滑块拼图对应的滑块操作标记。

另外，在本实施例中，生成滑块拼图对应的滑块操作标记的具体过程也可以是：对应滑块操作设置滑块参数，确定用户滑动滑块拼图时，将滑块参数赋值为第二预设协议值，生成滑块拼图对应的滑块操作标记。该第二预设协议值的具体数值并不作为限定，并且，第二预设协议值可以和第一预设协议值相同，也可以和第一预设协议值不同，可以根据实际需求设定。

例如，设置滑块参数 `slideflag`，用户滑动所述滑块拼图时，将该滑块参数 `slideflag` 赋值为第二预设协议值 1，得到表明用户发生了滑块滑动的滑块操作标记。

本实施例中，当终端设备确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记，

从而标记用户在页面上滑动滑块的行为动作的发生，达到记录用户页面操作的目的。

步骤 S108，当生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。

本实施例中，用户信息包括多项信息，每项用户信息均对应有一个用户信息输入框，当终端设备通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记，因此当用户通过所有用户信息输入框输入完所有用户信息时，终端设备生成与用户信息（用户信息输入框）的数量相等的多项信息输入标记。

在用户滑动完成滑块拼图时，终端设备校验滑块拼图的完成结果是否正确，当终端设备生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，终端设备将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。

本申请实施例中的方法，根据用户的密码重设指令，提供密码重设界面，该密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图；通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记；确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记；当生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。与相关技术相比，通过本实施例中的方法，终端设备与服务器之间在进行通信时，通信内容中增加了多个信息输入标记和滑块操作标记，也即改变了原有的通信格式和通信内容，使得通信内容更多，从而提高了终端设备与服务器之间的通信协议的破解难度，降低了用户密码被盗的风险。

另一方面来说，本实施例中的方法，终端设备通过生成多个信息输入标记和滑块操作标记记录用户的页面操作，表示用户在网站页面上进行过输入信息、滑动滑块等实际操作行为。由于黑客盗取用户密码时通常不在网站页面进行操作，而是绕过终端设备直接与服务器进行信息交互，因此黑客向服务器发送的信息必定不包括多个信息输入标记和滑块操作标记，或者包括错误的信息输入标记和滑块操作标记，因此通过本实施例中的方法，还能够帮助服务器辨别接收到的信息是来自正常用户还是来自黑客，从而防止黑客盗取用户密码，提高密码的安全性。

考虑到终端设备接收到的用户输入的用户信息存在错误的情况，本实施例中的方法，在通过用户信息输入框接收到用户输入的用户信息后，还包括：

- (1) 将用户信息发送至服务器，以使服务器校验用户信息是否正确；
- (2) 在接收到服务器发送的各项用户信息均校验正确的指令后，将滑块拼图变为可滑动状态。

具体地，终端设备可以采用两种方式接收用户信息并发送至服务器，一种方式是，终端设备控制界面上的第一个用户信息输入框为可输入状态，第一个用户信息输入框为用户账号输入框，其余的用户信息输入框均为不可输入状态，滑块拼图也为不可用状态。当终端设备接收到

用户输入的第一项用户信息时，终端设备将该项用户信息发送至服务器，当接收到服务器发送的该项用户信息校验正确的指令后，将界面上的下一个用户信息输入框变为可输入状态，从而使用户输入下一项用户信息，当终端设备接收到用户输入的下一项用户信息时，将该下一项用户信息发送至服务器，在服务器校验该下一项用户信息正确时，终端设备将界面上的再下一个用户信息输入框变为可输入状态，如此重复，直至用户所有的用户信息均输入正确，在此过程中，当有一项用户信息错误且错误次数超过预设值时，终端设备都结束该密码重设流程。当终端设备接收到服务器发送的最后一项用户信息校验正确的指令后，将滑块拼图变为可滑动状态，从而使用户进行拼图验证。

另一种方式是，终端设备控制界面上所有的用户信息输入框均为可输入状态，滑块拼图为不可用状态。终端设备通过各个用户信息输入框接收用户输入的用户信息，当接收到所有用户信息后，终端设备将所有用户信息发送至服务器，当终端设备接收到服务器发送的所有用户信息均正确的指令后，将滑块拼图变为可滑动状态，从而使用户进行拼图验证，当终端设备接收到服务器发送的某项用户信息错误的指令后，显示该项用户信息错误的提示信息，当存在用户信息错误且错误次数超过预设值时，终端设备都结束该密码重设流程。

当用户信息为用户账号时，服务器校验该用户账号是否存在，当用户信息为用户手机号时，服务器校验该用户手机号是否存在以及与用户账号是否匹配，当用户信息为用户对指定问题的回答时，服务器校验该回答是否正确以及该回答是否与该用户账号匹配。

本实施例中，通过将用户信息发送至服务器进行校验，能够保证在各项用户信息均正确的情况下引导用户重设密码，进一步保证密码重设的安全性。

在本申请的一个具体实施例中，用户信息包括用户账号和用户手机号，终端设备首先通过用户信息输入框接收用户输入的用户账号，并发送至服务器校验该用户账号是否存在，如果账号不存在，则密码重设失败，如果账号存在，则终端设备生成用户账号对应的信息输入标记，并将用户手机号输入框变为可输入状态，通过用户手机号输入框接收用户手机号，并发送至服务器校验该手机号与用户账号是否匹配，如果不匹配，密码重设失败，如果匹配，则终端设备生成用户手机号对应的信息输入标记，并将滑块拼图变为可滑动状态，当终端设备监测到用户滑动滑块时，生成滑块拼图对应的滑块操作标记，当终端设备校验用户的滑块拼图完成结果错误时，密码重设失败，当终端设备校验用户的滑块拼图完成结果正确时，将上述两个信息输入标记和一个滑块操作标记发送至服务器，以使服务器根据上述两个信息输入标记和一个滑块操作标记引导用户重设密码。当服务器接收到的数据中不存在上述两个信息输入标记和一个滑块操作标记或者存在的标记内容错误时，服务器认为该信息来自于黑客，结束密码重设流程，当服务器接收到的数据中存在上述两个信息输入标记和一个滑块操作标记且标记内容正确时，引导用户重设密码。

其中，当终端设备接收到不为空的用戶信息时，确认用户存在点击用户信息输入框和输入信息的动作，生成信息输入标记以记录用户的页面操作，当终端设备确定用户滑动滑块拼图时，确定用户存在页面操作，生成滑块操作标记以记录用户的页面操作。

该具体的实施例中，账号和手机号码可以验证是哪个用户丢失了密码，加入滑动拼图、信息输入标记和滑块操作标记是为了防止黑客破解终端设备与服务器之间的协议，绕过网站页面直接与服务器进行交换，伪造真实用户协议。对于正常用户而言，其会对页面的用户信息输入框有点击操作，并且有信息输入操作，滑块拼图也会有用户点击滑动条移动的操作，黑客在绕过终端设备直接与服务器通信时，不会在网站页面进行操作，终端设备不会生成信息输入标记和滑块操作标记，因此本实施例中将这些用户操作记录下来作为判断是否为正常用户重设密码的依据，通过逐步验证用户身份信息和记录页面操作的方式极大的加强了密码重设功能的安全性及可靠性。

考虑到终端设备与服务器之间数据传输的安全性，图 2 中，将各个信息输入标记和滑块操作标记加密后发送至服务器，具体实现为：对各个信息输入标记和滑块操作标记进行加密，将各个信息输入标记和滑块操作标记的密文发送至服务器，从而通过加密通信的方式提高数据传输的安全性。

具体地，加密算法优选为 DES 加密算法，DES 全称为 Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法。DES 加密算法需要一个 key 值做为加密的参数。本实施例的 key 值通过服务器随机生成后下发到终端设备，各个用户之间的 key 值均不同，从而保证各个标记通过同样的 DES 算法加密后，各个用户的加密结果互不相同，进一步提高终端设备与服务器之间通信协议的安全性。对应地，本实施例中，终端设备根据服务器下发的当前用户对应的加密参数（key 值）对各个信息输入标记和滑块操作标记进行加密，将各个信息输入标记和滑块操作标记的密文发送至服务器。

DES 加密算法的具体加密过程为：

$\text{flagencryptdata} = \text{DES.encrypt}(\text{flagdata}, \text{key})$ ；

其中，flagencryptdata 是所有标记加密后的结果，直接发送到服务器，DES.encrypt 是 DES 加密算法的加密接口，flagdata 是 DES 加密的数据，是上述所有标记组合成的一个数据，key 是服务器下发的 DES 加密算法的 key 值。

服务器收到加密数据后具体解密过程如下：

$\text{Flagdecryptdata} = \text{DES.decrypt}(\text{flagencryptdata}, \text{key})$ ；

其中，Flagdecryptdata 是最终解密得到数据，DES.decrypt 是 DES 算法的解密接口，flagencryptdata 是终端设备上报的加密数据，key 是服务器下发到终端设备的加密 key。

本实施例中，通过对各个信息输入标记和滑块操作标记进行加密，尤其是根据服务器针对不同用户生成的互不相同的 key 值采用 DES 加密算法进行加密，能够保证标记的安全性，防止黑客伪造数据。

服务器接收到终端设备发送的加密数据后，对数据进行解密，并判断解密得到的数据是否为上述终端设备生成的各个标记，如果是，则确定是正常用户，引导进行密码重设，如果不是，则终止密码重设流程。需要说明的是，终端设备生成各个标记的方式与服务器事先约定好，因此服务器能够判断解密得到的数据是否为终端设备生成的各个标记，另外，如果服务器没有接

收到加密数据，也终止密码重设流程（这是由于黑客无法破解加密数据，导致黑客向服务器发送的数据中不存在加密数据的情况）。

对应图 2 中的终端设备执行的密码重设方法，如图 4 所示，本申请实施例还提供了一种由服务器执行的密码重设方法，该方法包括以下步骤：

步骤 S302，在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；

其中，用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，信息输入标记为终端设备在通过用户信息输入框接收到用户输入的用户信息时生成，用户信息输入框为多个，与各项用户信息一一对应，滑块操作标记为终端设备在确定用户滑动滑块拼图时生成，用户信息输入框和滑块拼图从属于密码重设界面，密码重设界面为终端设备根据用户的密码重设指令所提供。

本实施例中，各项用户信息、各个用户信息输入框、各个信息输入标记之间一一对应。在用户申请密码重设过程中，服务器判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记。其中滑块拼图的实现方式有多种，具体可以是如图 3 所示的拖动滑块的同时拼图随之移动，当用户沿着滑块移动指示方向拖动滑块至指定位置时，拼图成功。

步骤 S304，若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个信息输入标记和滑块操作标记是否均符合预设规则。

本实施例中，终端设备生成各个标记的方式与服务器事先约定好，如：

（1）终端设备利用第一预设算法对第一预设参数进行运算，生成某项用户信息对应的信息输入标记，其中，第一预设参数包括当前日期或者该项用户信息的全部或部分内容，第一预设算法为对称加密算法或者非对称加密算法；

（2）终端设备利用第二预设算法对第二预设参数进行运算，生成滑块拼图对应的滑块操作标记，其中，第二预设参数包括当前日期，第二预设算法为对称加密算法或者非对称加密算法。

对应地，预设规则指的是生成各个标记时所使用的参数和算法，服务器校验各个信息输入标记和滑块操作标记是否均符合预设规则具体可以为：

（1）通过第一预设算法解析信息输入标记，校验解析结果是否为第一预设参数，若是，则确定信息输入标记符合预设规则，第一预设参数包括当前日期或者信息输入标记对应的用户信息的全部或部分内容；

（2）通过第二预设算法解析滑块操作标记，校验解析结果是否为第二预设参数，若是，则确定滑块操作标记符合预设规则，第二预设参数包括当前日期。

过程（1）中，服务器通过第一预设算法解析信息输入标记，其中第一预设算法与终端设备生成信息输入标记时所使用的的第一预设算法相同。服务器判断解析结果是否为第一预设参数，其中第一预设参数与终端设备生成信息输入标记时所使用的的第一预设参数相同，若为第一预设参数，则确定信息输入标记符合预设规则。

一种具体的实施方式可以为：用户信息为用户手机号，第一预设算法为对称加密算法，第一预设信息为用户手机号的后四位，终端设备对用户手机号后四位进行对称加密，得到用户手机号对应的信息输入标记。服务器在收到用户手机号对应的信息输入标记时，利用相同的对称加密算法解析信息输入标记，判断解析结果是否为用户手机号后四位，如果是，则确定信息输入标记符合预设规则。

过程(2)中，服务器通过第二预设算法解析滑块操作标记，其中第二预设算法与终端设备生成滑块操作标记时所使用的第二预设算法相同。服务器判断解析结果是否为第二预设参数，其中第二预设参数与终端设备生成滑块操作标记时所使用的第二预设参数相同，若为第二预设参数，则确定滑块操作标记符合预设规则。

一种具体的实施方式可以为：终端设备为当前日期，如年-月-日中的“日”作为第二预设参数，利用第二预设算法对第二预设参数进行对称加密，将得到的结果作为滑块拼图对应的滑块操作标记。服务器在收到滑块操作标记时，利用相同的对称加密算法解析滑块操作标记，判断解析结果是否为当前日期中的“日”，如果是，则确定滑块操作标记符合预设规则。

另外，若终端设备与服务器事先约定好的生成各个标记的方式为：对应用户信息输入框设置信息参数，将信息参数赋值为第一预设协议值，生成用户信息对应的信息输入标记；对应滑块操作设置滑块参数，确定用户滑动滑块拼图时，将滑块参数赋值为第二预设协议值，生成滑块拼图对应的滑块操作标记。

则服务器校验信息输入标记是否均符合预设规则具体可以为，校验信息输入标记中信息参数的值是否为第一预设协议值，若是，则确定信息输入标记符合预设规则。校验滑块操作标记中滑块参数的值是否为第二预设协议值，若是，则确定滑块操作标记符合预设规则。

需要说明的是，本实施例中，可以校验各个标记的顺序不做具体限定，可以基于实际情况决定。

步骤 S306，若各个信息输入标记和滑块操作标记均符合预设规则，向终端设备发送密码重设指令，以引导用户进行密码重设。

若服务器校验各个信息输入标记和滑块操作标记通过，则向终端设备发送密码重设指令，以引导用户进行密码重设。

考虑到黑客在绕开终端设备直接与服务器进行通信时，一种情况是无法破解通信协议中的各个标记，从而黑客向服务器发送的数据中不包括完整的各个标记，另一种情况是协议破解错误，导致黑客向服务器发送的数据中包括错误的各个标记，因此当服务器没有接收到与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记时，或者服务器接收到的各个标记中存在不符合预设规则的标记时，确认数据来自异常用户，结束密码重设流程。

本申请实施例中的方法，服务器在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，若接收到，则校验各个信息输入标记和滑块操作标记是否均符合预设规则；若各个信息输入标记和滑块操作标记均符合预设规则，向终端设备发送密码重设指令，以引导用户进行密码重设。与相关技

术相比，通过本实施例中的方法，终端设备与服务器之间在进行通信时，通信内容中增加了多个信息输入标记和滑块操作标记，也即改变了原有的通信格式和通信内容，使得通信内容更多，从而提高了终端设备与服务器之间的通信协议的破解难度，降低了用户密码被盗的风险。

另一方面来说，本实施例中的方法，终端设备通过生成多个信息输入标记和滑块操作标记记录用户的页面操作，表示用户在网站页面上进行过输入信息、滑动滑块等实际操作行为。由于黑客盗取用户密码时通常不在网站页面进行操作，而是绕过终端设备直接与服务器进行信息交互，因此黑客向服务器发送的信息必定不包括多个信息输入标记和滑块操作标记，或者包括错误的信息输入标记和滑块操作标记，因此通过本实施例中的方法，还能够帮助服务器辨别接收到的信息是来自正常用户还是来自黑客，从而防止黑客盗取用户密码，提高密码的安全性。

对应上述的终端设备的方法流程，本实施例中的服务器还能够对终端设备发送的用户信息进行校验，具体地，在判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记之前，本实施例中的方法还包括：

- (1) 接收终端设备发送的用户信息，校验用户信息是否正确；
- (2) 当校验用户信息正确时，向终端设备发送用户信息校验正确的指令。

对应上述的终端设备的方法流程，本实施例中服务器能够采用两种方式校验用户信息是否正确。一种方式是在终端设备逐个发送用户信息的情况下，服务器接收终端设备发送的第一项用户信息，校验第一项用户信息是否正确，如账户名称是否存在，如果校验通过，则向终端设备发送校验正确指令，服务器接收终端设备发送的第二项用户信息，如手机号码，校验手机号码与账户名称是否匹配，如果匹配，则向终端设备发送校验正确指令，如此循环，直至校验最后一项用户信息是否正确，以及向终端设备发送校验结果。另一种方式是在终端设备将多项用户信息同时发送的情况下，服务器接收所有用户信息，对所有用户信息进行校验，并将校验结果发送至终端设备。

本实施例中，对各项用户信息进行校验，能够保证在各项用户信息均正确的情况下引导用户重设密码，进一步保证密码重设的安全性。

对应上述的终端设备的方法流程，本实施例中的服务器还能够对加密的标记进行解析，具体地，各个信息输入标记和滑块操作标记均为密文形式，校验各个信息输入标记和滑块操作标记是否均符合上述预设规则具体可以是：

- (1) 对各个信息输入标记和滑块操作标记进行解密，得到各个信息输入标记和滑块操作标记的明文；
- (2) 校验各个信息输入标记和滑块操作标记的明文是否均符合上述预设规则。

对应上述的终端设备的方法流程，本实施例中，根据预先下发至终端设备的 key 值对各个信息输入标记和滑块操作标记进行解密，得到各个信息输入标记和滑块操作标记的明文，并校验各个信息输入标记和滑块操作标记的明文是否均符合上述预设规则。具体解密过程可以参考上述终端设备侧的描述，这里不再赘述。

由于服务器随机生成与各个用户对应的 key 值，从而使得各个用户的标记加密结果互不相

同，能够进一步保证标记的安全性，防止黑客伪造数据。

综上，通过本申请实施例中的密码重设方法，结合终端设备与服务器侧的相互配合，能够提高通信协议的破解难度，降低用户密码被盗的风险，并有助于服务器辨别接收到的信息是来自正常用户还是来自黑客，从而防止黑客盗取用户密码，提高密码的安全性。

对应上述的终端设备的方法流程，如图 5 所示，本申请实施例还提供了一种密码重设装置，该装置位于终端设备侧，可以位于终端设备内部，也可以位于终端设备外部，包括：

界面提供模块 41，用于根据用户的密码重设指令，提供密码重设界面，密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；

第一标记生成模块 42，用于通过用户信息输入框接收到用户输入的用户信息时，生成用户信息对应的信息输入标记；

第二标记生成模块 43，用于确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记；

标记发送模块 44，用于当生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。

其中，第一标记生成模块 42 具体用于：利用第一预设算法对第一预设参数进行运算，生成用户信息对应的信息输入标记，其中，第一预设参数包括当前日期或者用户信息的全部或部分信息。第二标记生成模块 43 具体用于：利用第二预设算法对第二预设参数进行运算，生成滑块拼图对应的滑块操作标记，其中，第二预设参数包括当前日期。

本申请实施例中的装置，根据用户的密码重设指令，提供密码重设界面，该密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图；通过一个用户信息输入框接收到用户输入的一项用户信息时，生成该项用户信息对应的信息输入标记；确定用户滑动滑块拼图时，生成滑块拼图对应的滑块操作标记；当生成与各项用户信息一一对应的多个信息输入标记且滑块拼图的完成结果正确时，将各个信息输入标记和滑块操作标记发送至服务器，以使服务器根据各个信息输入标记和滑块操作标记引导用户进行密码重设。与相关技术相比，通过本实施例中的装置，终端设备与服务器之间在进行通信时，通信内容中增加了多个信息输入标记和滑块操作标记，也即改变了原有的通信格式和通信内容，使得通信内容更多，从而提高了终端设备与服务器之间的通信协议的破解难度，降低了用户密码被盗的风险。

考虑到终端设备接收到的用户输入的用户信息存在错误的情况，本实施例中的装置还包括：信息发送模块，用于在通过用户信息输入框接收到用户输入的用户信息后，将用户信息发送至服务器，以使服务器校验用户信息是否正确；状态转变模块，用于在接收到服务器发送的各项用户信息均校验正确的指令后，将滑块拼图变为可滑动状态。

本实施例中，通过将用户信息发送至服务器进行校验，能够保证在各项用户信息均正确的情况下引导用户重设密码，进一步保证密码重设的安全性。

考虑到终端设备与服务器之间数据传输的安全性，上述标记发送模块 44 具体用于：对各个

信息输入标记和滑块操作标记进行加密，将各个信息输入标记和滑块操作标记的密文发送至服务器。

对应上述的服务器的方法流程，如图 6 所示，本申请实施例还提供了一种密码重设装置，该装置位于服务器侧，可以位于服务器内部，也可以位于服务器外部，包括：

标记判断模块 51，用于在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；

其中，用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，信息输入标记为终端设备在通过用户信息输入框接收到用户输入的用户信息时生成，用户信息输入框为多个，与各项用户信息一一对应，滑块操作标记为终端设备在确定用户滑动滑块拼图时生成，用户信息输入框和滑块拼图从属于密码重设界面，密码重设界面为终端设备根据用户的密码重设指令所提供；

标记校验模块 52，用于若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个信息输入标记和滑块操作标记是否均符合预设规则；

指令发送模块 53，用于若各个信息输入标记和滑块操作标记均符合预设规则，向终端设备发送密码重设指令，以引导用户进行密码重设。

其中，标记校验模块 52 包括：第一校验子模块，用于通过第一预设算法解析信息输入标记，校验解析结果是否为第一预设参数，若是，则确定信息输入标记符合预设规则，第一预设参数包括当前日期或者信息输入标记对应的用户信息的全部或部分内容；第二校验子模块，用于通过第二预设算法解析滑块操作标记，校验解析结果是否为第二预设参数，若是，则确定滑块操作标记符合预设规则，第二预设参数包括当前日期。

本申请实施例中的装置，服务器在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，若接收到，则校验各个信息输入标记和滑块操作标记是否均符合预设规则；若各个信息输入标记和滑块操作标记均符合预设规则，向终端设备发送密码重设指令，以引导用户进行密码重设。与相关技术相比，通过本实施例中的装置，终端设备与服务器之间在进行通信时，通信内容中增加了多个信息输入标记和滑块操作标记，也即改变了原有的通信格式和通信内容，使得通信内容更多，从而提高了终端设备与服务器之间的通信协议的破解难度，降低了用户密码被盗的风险。

本实施例中的服务器还能够对终端设备发送的用户信息进行校验，具体地，该装置还包括：信息校验模块，用于在判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记之前，接收终端设备发送的用户信息，校验用户信息是否正确；结果发送模块，用于当校验用户信息正确时，向终端设备发送用户信息校验正确的指令。

本实施例中，对各项用户信息进行校验，能够保证在各项用户信息均正确的情况下引导用户重设密码，进一步保证密码重设的安全性。

本实施例中的服务器还能够对加密的标记进行解析，具体地，各个信息输入标记和滑块操作标记均为密文形式，标记校验模块 52，包括：解密子模块，用于对各个信息输入标记和滑块操作标记进行解密，得到各个信息输入标记和滑块操作标记的明文；明文校验子模块，用于校验各个信息输入标记和滑块操作标记的明文是否均符合预设规则。

由于服务器随机生成与各个用户对应的 key 值，从而使得各个用户的标记加密结果互不相同，能够进一步保证标记的安全性，防止黑客伪造数据。

综上，通过本申请实施例中的密码重设装置，结合终端设备与服务器侧的相互配合，能够提高通信协议的破解难度，降低用户密码被盗的风险，并有助于服务器辨别接收到的信息是来自正常用户还是来自黑客，从而防止黑客盗取用户密码，提高密码的安全性。

进一步的，本申请实施例还提供了一种电子设备。

图 7 是本申请一个实施例的一种电子设备 60 的示意性方框图。

如图 7 所示，本申请实施例提供的电子设备 60 包括：存储器 61 和处理器 62。

存储器 61，用于存储程序。

处理器 62，用于通过调用所述存储器 61 中存储的程序并执行。

具体的，该电子设备 60 可以是上述的终端设备或者服务器。当该电子设备 60 是终端设备，处理器 62 调用所述存储器 61 中存储的程序，执行包括以下步骤的方法：

根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

当该电子设备 60 是服务器，处理器 62 调用所述存储器 61 中存储的程序，执行包括以下步骤的方法：

在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；若各个所述信息输入标记和所述滑块操作标记均符合

所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

需说明的是，关于上述方法的进一步描述具体参见前面方法流程中的详细描述，此处不再赘述。

在本实施例中，处理器 62 通过运行存储在存储器 61 中的上述程序，从而执行各种功能应用以及数据处理。存储器 61 可以包括但不限于随机存取存储器(Random Access Memory, RAM)，只读存储器(Read Only Memory, ROM)，可编程只读存储器(Programmable Read-Only Memory, PROM)，可擦除只读存储器(Erasable Programmable Read-Only Memory, EPROM)，电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory, EEPROM)等。其中，所述处理器 62 可以在接收到执行指令后，执行所述存储器 61 中存储的上述程序，相应地实现前述本申请实施例任一实施例揭示的流程所定义的方法。

处理器 62 可以是一种集成电路芯片，具有信号处理能力。上述处理器可以是通用处理器，包括中央处理器(Central Processing Unit，简称 CPU)、网络处理器(Network Processor，简称 NP)等；还可以是数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。其可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

可以理解的，图 7 所示的结构仅为示意，电子设备 60 还可以包括比图 7 中所示更多或者更少的组件，或者具有与图 7 所示不同的配置。图 7 中所示的各组件可以采用硬件、软件或其组合实现。

前述实施例中的装置各模块和单元可以由软件代码实现，此时，上述的各模块和单元可存储于电子设备 60 的存储器 601 内。以上各模块和单元同样可以由硬件例如集成电路芯片实现。

本申请实施例所提供的密码重设装置可以为设备上的特定硬件或者安装于设备上的软件或固件等。本申请实施例所提供的装置，其实现原理及产生的技术效果和前述方法实施例相同，为简要描述，装置实施例部分未提及之处，可参考前述方法实施例中相应内容。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，前述描述的系统、装置和单元的具体工作过程，均可以参考上述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。

可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请提供的实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对相关技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释，此外，术语“第一”、“第二”、“第三”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

最后应说明的是：以上所述实施例，仅为本申请的具体实施方式，用以说明本申请的技术方案，而非对其限制，本申请的保护范围并不局限于此，尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质的脱离本申请实施例技术方案的精神和范围。都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

权利要求书

1、一种密码重设方法，其特征在于，包括：

根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；

通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；

确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；

当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

2、根据权利要求1所述的方法，其特征在于，所述生成所述用户信息对应的信息输入标记，包括：

利用第一预设算法对第一预设参数进行运算，生成所述用户信息对应的信息输入标记，其中，所述第一预设参数包括当前日期或者所述用户信息的全部或部分内容。

3、根据权利要求1至2任一项所述的方法，其特征在于，所述生成所述滑块拼图对应的滑块操作标记，包括：

利用第二预设算法对第二预设参数进行运算，生成所述滑块拼图对应的滑块操作标记，其中，所述第二预设参数包括当前日期。

4、根据权利要求1至3任一项所述的方法，其特征在于，对应用户信息输入框设置信息参数，所述生成所述用户信息对应的信息输入标记，包括：

将所述信息参数赋值为第一预设协议值，生成用户信息对应的信息输入标记。

5、根据权利要求1至4任一项所述的方法，其特征在于，对应滑块操作设置滑块参数，所述生成所述滑块拼图对应的滑块操作标记，包括：

将滑块参数赋值为第二预设协议值，生成滑块拼图对应的滑块操作标记。

6、根据权利要求1至5任一项所述的方法，其特征在于，在所述通过所述用户信息输入框接收到用户输入的用户信息后，所述方法还包括：

将所述用户信息发送至所述服务器，以使所述服务器校验所述用户信息是否正确；

在接收到所述服务器发送的各项所述用户信息均校验正确的指令后，将所述滑块拼图变为可滑动状态。

7、根据权利要求1至6任一项所述的方法，其特征在于，所述将各个所述信息输入标记和所述滑块操作标记发送至服务器，包括：

对各个所述信息输入标记和所述滑块操作标记进行加密，将各个所述信息输入标记和所述滑块操作标记的密文发送至所述服务器。

8、一种密码重设方法，其特征在于，包括：

在用户申请密码重设过程中,判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记;

其中,所述用户信息包括用户账号,还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项,所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成,所述用户信息输入框为多个,与各项所述用户信息一一对应,所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成,所述用户信息输入框和所述滑块拼图从属于密码重设界面,所述密码重设界面为所述终端设备根据用户的密码重设指令所提供;

若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记,则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则;

若各个所述信息输入标记和所述滑块操作标记均符合所述预设规则,向所述终端设备发送密码重设指令,以引导所述用户进行密码重设。

9、根据权利要求 8 所述的方法,其特征在于,所述校验各个所述信息输入标记是否均符合预设规则,包括:

通过第一预设算法解析所述信息输入标记,校验解析结果是否为第一预设参数,若是,则确定所述信息输入标记符合所述预设规则,所述第一预设参数包括当前日期或者所述信息输入标记对应的用户信息的全部或部分内容。

10、根据权利要求 8 至 9 任一项所述的方法,其特征在于,校验所述滑块操作标记是否符合预设规则包括:

通过第二预设算法解析所述滑块操作标记,校验解析结果是否为第二预设参数,若是,则确定所述滑块操作标记符合所述预设规则,所述第二预设参数包括当前日期。

11、根据权利要求 8 至 10 任一项所述的方法,其特征在于,所述信息输入标记中包括信息参数,所述校验各个所述信息输入标记是否均符合预设规则,包括:

校验信息输入标记中信息参数的值是否为第一预设协议值,若是,则确定信息输入标记符合预设规则。

12、根据权利要求 8 至 11 任一项所述的方法,其特征在于,所述滑块操作标记中包括滑块参数,校验所述滑块操作标记是否符合预设规则包括:

校验滑块操作标记中滑块参数的值是否为第二预设协议值,若是,则确定滑块操作标记符合预设规则。

13、根据权利要求 8 至 12 任一项所述的方法,其特征在于,在判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记之前,所述方法还包括:

接收所述终端设备发送的所述用户信息,校验所述用户信息是否正确;

当校验所述用户信息正确时,向所述终端设备发送所述用户信息校验正确的指令。

14、根据权利要求 8 至 13 任一项所述的方法,其特征在于,各个所述信息输入标记和所述滑块操作标记均为密文形式,所述校验各个所述信息输入标记和所述滑块操作标记是否均符

合预设规则，包括：

对各个所述信息输入标记和所述滑块操作标记进行解密，得到各个所述信息输入标记和所述滑块操作标记的明文；

校验各个所述信息输入标记和所述滑块操作标记的明文是否均符合所述预设规则。

15、一种密码重设装置，其特征在于，包括：

界面提供模块，配置成根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；

第一标记生成模块，配置成通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；

第二标记生成模块，配置成确定所述用户滑动所述滑块拼图时，生成所述滑块拼图对应的滑块操作标记；

标记发送模块，配置成当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

16、一种密码重设装置，其特征在于，包括：

标记判断模块，配置成在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；

其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；

标记校验模块，配置成若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；

指令发送模块，配置成若各个所述信息输入标记和所述滑块操作标记均符合所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

17、一种终端设备，其特征在于，包括：

存储器，被配置为存储程序，

处理器，被配置为通过调用所述存储器中存储的程序，执行包括以下步骤的方法：

根据用户的密码重设指令，提供密码重设界面，所述密码重设界面包括与各项用户信息一一对应的多个用户信息输入框和滑块拼图，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项；通过所述用户信息输入框接收到用户输入的用户信息时，生成所述用户信息对应的信息输入标记；确定所述用户滑动所述滑块拼图时，

生成所述滑块拼图对应的滑块操作标记；当生成与各项所述用户信息一一对应的多个所述信息输入标记且所述滑块拼图的完成结果正确时，将各个所述信息输入标记和所述滑块操作标记发送至服务器，以使所述服务器根据各个所述信息输入标记和所述滑块操作标记引导所述用户进行密码重设。

18、一种服务器，其特征在于，所述服务器包括：

存储器，被配置为存储程序，

处理器，被配置为通过调用所述存储器中存储的程序，执行包括以下步骤的方法：

在用户申请密码重设过程中，判断是否接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记；其中，所述用户信息包括用户账号，还包括用户姓名、用户手机号、用户对指定问题的回答中的一项或多项，所述信息输入标记为所述终端设备在通过用户信息输入框接收到用户输入的所述用户信息时生成，所述用户信息输入框为多个，与各项所述用户信息一一对应，所述滑块操作标记为所述终端设备在确定用户滑动滑块拼图时生成，所述用户信息输入框和所述滑块拼图从属于密码重设界面，所述密码重设界面为所述终端设备根据用户的密码重设指令所提供；若接收到来自终端设备的与各项用户信息一一对应的多个信息输入标记和对应滑块拼图的滑块操作标记，则校验各个所述信息输入标记和所述滑块操作标记是否均符合预设规则；若各个所述信息输入标记和所述滑块操作标记均符合所述预设规则，向所述终端设备发送密码重设指令，以引导所述用户进行密码重设。

19. 一种具有处理器可执行的非易失的程序代码的计算机可读介质，其特征在于，所述程序代码使所述处理器执行所述权利要求 1-14 任一项所述方法。

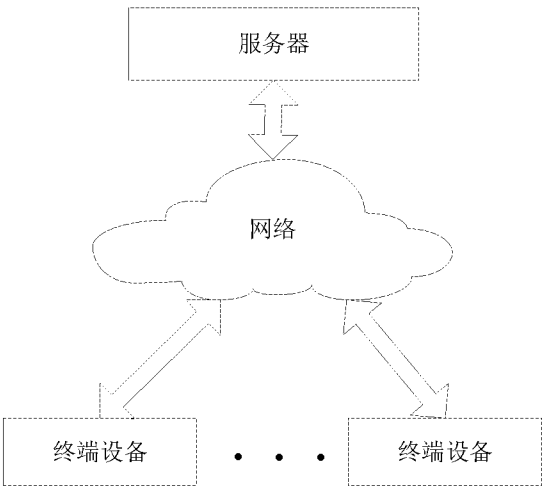


图 1

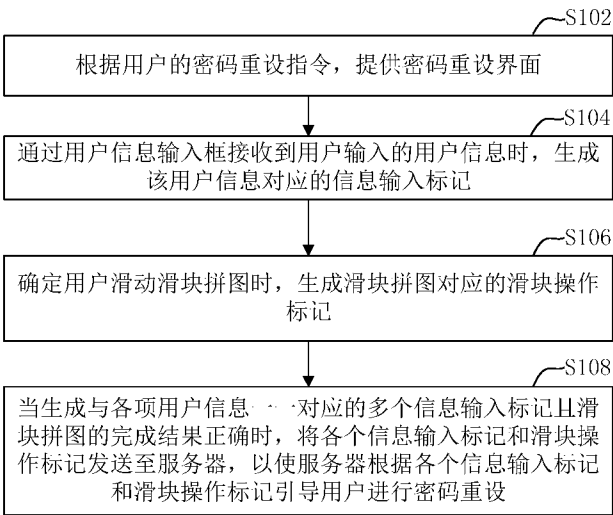


图 2

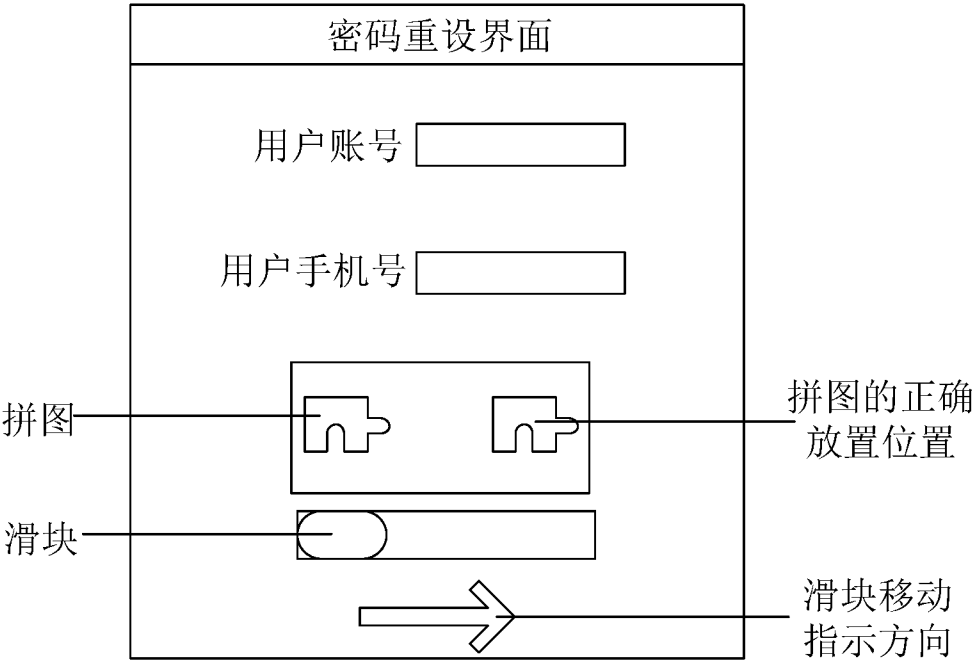


图 3

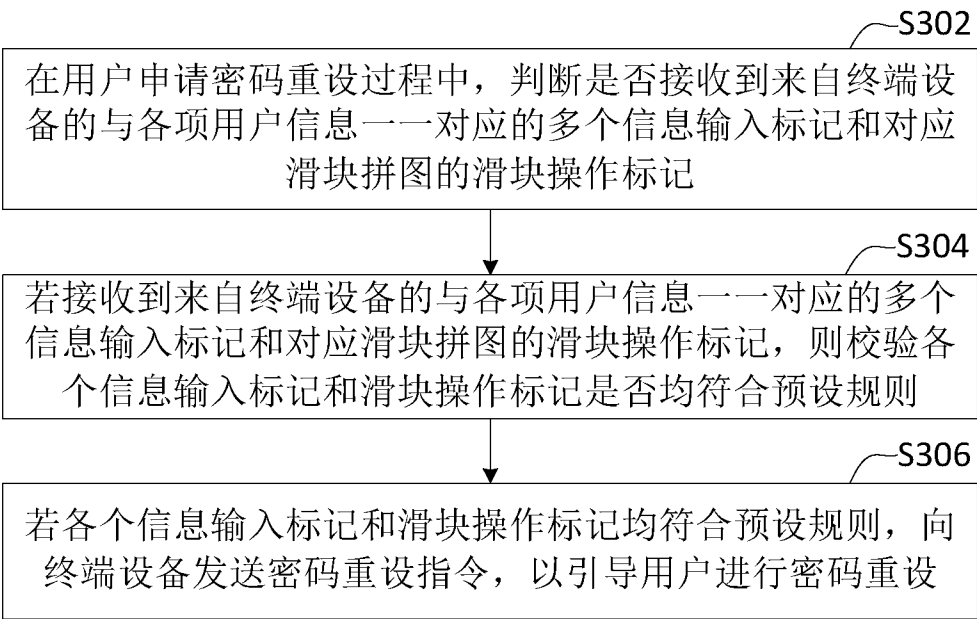


图 4

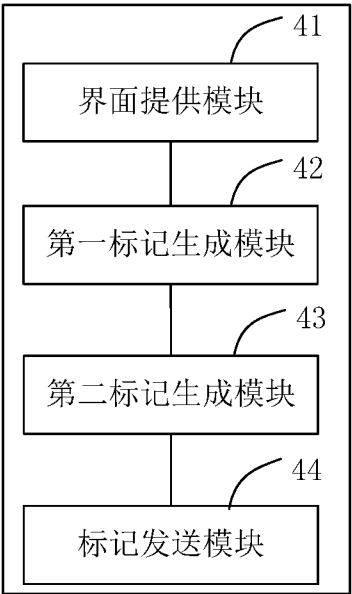


图 5

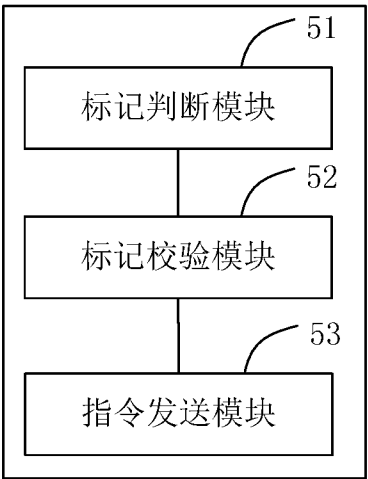


图 6

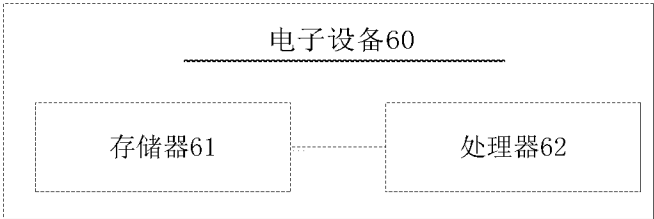


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/079616

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W, H04B, 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: 密码, 口令, 密钥, 账户, 帐号, 拼图, 拖, 拽, 滑, 验证, 校验, 附加, 重设, 设置, 找回, 取回, password, key, account, user w name, withdraw, draw, drag, picture, slide

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106330437 A (WUHAN DOUYU NETWORK TECHNOLOGY CO., LTD.), 11 January 2017 (11.01.2017), claims 1-10	1-19
X	CN 104917720 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 16 September 2015 (16.09.2015), description, paragraphs [0003] and [0025]-[0051], and figures 1 and 2	1-19
A	CN 105323065 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 10 February 2016 (10.02.2016), entire document	1-19
A	CN 104580104 A (TENCENT INC.), 29 April 2015 (29.04.2015), entire document	1-19
A	CN 104796428 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 22 July 2015 (22.07.2015), entire document	1-19
A	CN 104378343 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 25 February 2015 (25.02.2015), entire document	1-19
A	US 2016226853 A1 (INTERACTIVE INTELLIGENCE INC.), 04 August 2016 (04.08.2016), entire document	1-19

☐ 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 19 May 2017	Date of mailing of the international search report 31 May 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 SUN, Lili Telephone No. (86-10) 62413850

International application No.
PCT/CN2017/079616

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																										
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04W, H04B, 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: 密码, 口令, 密钥, 账户, 帐号, 拼图, 拖, 拽, 滑, 验证, 校验, 附加, 重设, 设置, 找回, 取回, password, key, account, user w name, withdraw, draw, drag, picture, slide																										
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>PX</td> <td>CN 106330437 A (武汉斗鱼网络科技有限公司) 2017年 1月 11日 (2017 - 01 - 11) 权利要求1-10</td> <td>1-19</td> </tr> <tr> <td>X</td> <td>CN 104917720 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16) 说明书第[0003]、[0025]-[0051]段, 附图1、2</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 105323065 A (腾讯科技深圳有限公司) 2016年 2月 10日 (2016 - 02 - 10) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 104580104 A (深圳市腾讯计算机系统有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 104796428 A (中国联合网络通信集团有限公司) 2015年 7月 22日 (2015 - 07 - 22) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>CN 104378343 A (腾讯科技深圳有限公司) 2015年 2月 25日 (2015 - 02 - 25) 全文</td> <td>1-19</td> </tr> <tr> <td>A</td> <td>US 2016226853 A1 (INTERACTIVE INTELLIGENCE INC.) 2016年 8月 4日 (2016 - 08 - 04) 全文</td> <td>1-19</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	PX	CN 106330437 A (武汉斗鱼网络科技有限公司) 2017年 1月 11日 (2017 - 01 - 11) 权利要求1-10	1-19	X	CN 104917720 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16) 说明书第[0003]、[0025]-[0051]段, 附图1、2	1-19	A	CN 105323065 A (腾讯科技深圳有限公司) 2016年 2月 10日 (2016 - 02 - 10) 全文	1-19	A	CN 104580104 A (深圳市腾讯计算机系统有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-19	A	CN 104796428 A (中国联合网络通信集团有限公司) 2015年 7月 22日 (2015 - 07 - 22) 全文	1-19	A	CN 104378343 A (腾讯科技深圳有限公司) 2015年 2月 25日 (2015 - 02 - 25) 全文	1-19	A	US 2016226853 A1 (INTERACTIVE INTELLIGENCE INC.) 2016年 8月 4日 (2016 - 08 - 04) 全文	1-19
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
PX	CN 106330437 A (武汉斗鱼网络科技有限公司) 2017年 1月 11日 (2017 - 01 - 11) 权利要求1-10	1-19																								
X	CN 104917720 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16) 说明书第[0003]、[0025]-[0051]段, 附图1、2	1-19																								
A	CN 105323065 A (腾讯科技深圳有限公司) 2016年 2月 10日 (2016 - 02 - 10) 全文	1-19																								
A	CN 104580104 A (深圳市腾讯计算机系统有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-19																								
A	CN 104796428 A (中国联合网络通信集团有限公司) 2015年 7月 22日 (2015 - 07 - 22) 全文	1-19																								
A	CN 104378343 A (腾讯科技深圳有限公司) 2015年 2月 25日 (2015 - 02 - 25) 全文	1-19																								
A	US 2016226853 A1 (INTERACTIVE INTELLIGENCE INC.) 2016年 8月 4日 (2016 - 08 - 04) 全文	1-19																								
☐ 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 2017年 5月 19日		国际检索报告邮寄日期 2017年 5月 31日																								
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 孙丽丽 电话号码 (86-10) 62413850																								

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/079616

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	106330437	A	2017年 1月 11日	无	
CN	104917720	A	2015年 9月 16日	无	
CN	105323065	A	2016年 2月 10日	无	
CN	104580104	A	2015年 4月 29日	无	
CN	104796428	A	2015年 7月 22日	无	
CN	104378343	A	2015年 2月 25日	无	
US	2016226853	A1	2016年 8月 4日	无	