(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103917980 B
(45)授权公告日 2018.05.01

(21)申请号 201180074739.1

(22)申请日 2011.11.08

(65)同一申请的已公布的文献号
申请公布号 CN 103917980 A

(43)申请公布日 2014.07.09

(85)PCT国际申请进入国家阶段日
2014.05.08

(86)PCT国际申请的申请数据
PCT/SE2011/051334 2011.11.08

(87)PCT国际申请的公布数据
WO2013/070124 EN 2013.05.16

(73)专利权人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩

(72)发明人 古兰·塞兰德 马茨·内斯隆德

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 赵伟

(51)Int.Cl.
G06F 21/46(2013.01)

(56)对比文件
WO 2007/038924 A1,2007.04.12,
US 6643784 B1,2003.11.04,
US 2011/0187497 A1,2011.08.04,
US 2004/0139331 A1,2004.07.15,
WO 2007/038924 A1,2007.04.12,
WO 2007/038924 A1,2007.04.12,
US 6643784 B1,2003.11.04,

审查员 李莎

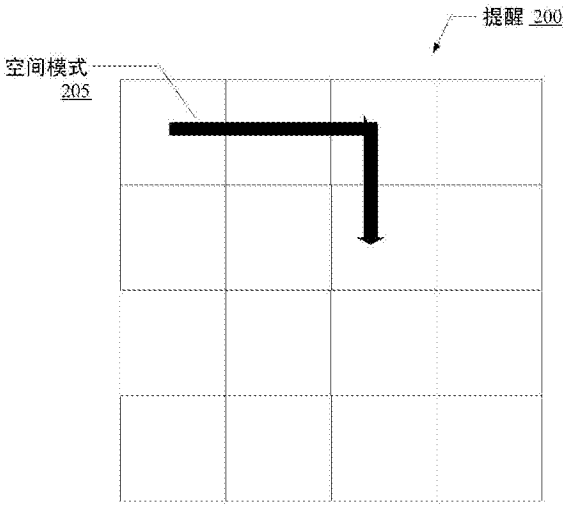
权利要求书2页 说明书15页 附图13页

(54)发明名称

用于获得密码提示的装置和方法

(57)摘要

公开了用于获得密码提示的方法和装置。在一些实施例中，该方法包括：从用户接收空间模式；获得包括多个字符的密码；获得包括字符布置的密码提示，其中，字符布置包括密码的多个字符和额外字符，并且密码的多个字符根据接收的空间模式位于字符布置内。该方法还包括：存储密码提示或者向用户提供密码提示。



CN 103917980 B

1.一种由计算机系统执行以用于获得密码提示的方法,所述方法包括:

从用户接收空间模式;

根据所述空间模式生成包括多个字符的密码;

生成包括字符布置的密码提示;

针对所述用户,在通过通信网络能够访问的存储位置处存储所述密码提示;以及

响应于检测到所述用户对所述密码提示的请求,通过所述通信网络向所述用户提供所述密码提示,而不显露所述空间模式,其中,

所述字符布置包括所述密码的所述多个字符和额外字符,

所述密码的所述多个字符根据所述空间模式位于所述字符布置中,

存储所述密码提示包括使用不同于所述密码对应于的网络服务的第二网络服务来存储所述密码提示,

所述请求是从具有订户标识模块的移动通信设备发送且在所述第二网络服务处接收的,以及

向所述用户提供所述密码提示包括:响应于使用所述订户标识模块验证所述移动通信设备,授予对所存储的密码提示的访问权。

2.根据权利要求1所述的方法,还包括:接收密码要求,其中,所述生成密码的步骤包括:根据所述要求生成所述密码。

3.根据权利要求1或2所述的方法,其中,存储所述密码提示包括:与所述密码对应于的网络服务相关联地或者与所述密码对应于的目标验证系统相关联地存储所述密码提示。

4.根据权利要求1或2所述的方法,还包括:

使用图形图像来向所述用户提醒所述空间模式;

其中,所述密码提示包括所述图形图像。

5.根据权利要求4所述的方法,其中,所述密码提示包括叠加在所述图形图像上的所述字符布置。

6.根据权利要求1或2所述的方法,还包括:响应于检测到正在提醒所述用户输入与所述密码提示相关联的密码,自动地向所述用户提供所述密码提示。

7.根据权利要求1或2所述的方法,还包括:

在接收到所述空间模式之前接收初始空间模式;

确定所述初始空间模式不满足一个或更多个模式要求;以及

响应于确定所述初始空间模式不满足所述一个或更多个模式要求,提醒所述用户输入新空间模式。

8.根据权利要求1所述的方法,其中,生成密码的步骤在生成密码提示的步骤之后发生,并且生成密码的步骤包括:确定所述密码提示的与所述空间模式相对应的字符,以及设置所述密码使得所述密码的字符由所确定的所述密码提示的与所述空间模式相对应的字符构成。

9.一种用于获得密码提示的系统,所述系统包括:

用于从用户接收空间模式的装置;

用于生成包括多个字符的密码的装置;

用于生成包括字符布置的密码提示的装置;

用于针对所述用户在通过通信网络能够访问的存储位置处存储所述密码提示的装置；以及

用于以下操作的装置：响应于检测到所述用户对所述密码提示的请求，通过所述通信网络向所述用户提供所述密码提示，而不显露所述空间模式，其中，

所述字符布置包括所述密码的所述多个字符和额外字符，

所述密码的所述多个字符根据所述空间模式位于所述字符布置中，

存储所述密码提示包括使用不同于所述密码对应于的网络服务的第二网络服务来存储所述密码提示，

所述请求是从具有订户标识模块的移动通信设备发送且在所述第二网络服务处接收的，以及

向所述用户提供所述密码提示包括：响应于使用所述订户标识模块验证所述移动通信设备，授予对所存储的密码提示的访问权。

10.根据权利要求9所述的系统，还包括用于接收密码要求的装置；以及

所述用于生成密码的装置还用于根据所述要求生成所述密码。

11.根据权利要求9所述的系统，其中，

用于存储所述密码提示的装置与所述密码对应于的网络服务相关联地或者与所述密码对应于的目标验证系统相关联地存储所述密码提示，和/或

用于存储所述密码提示的装置在移动设备上的本地存储设备中存储所述密码提示。

12.根据权利要求9所述的系统，还包括：用于使用图形图像向所述用户提醒所述空间模式的装置，其中，所述密码提示包括叠加在所述图形图像上的所述字符布置。

13.根据权利要求9所述的系统，其中，所述系统是移动通信设备或者是移动通信设备的一部分。

用于获得密码提示的装置和方法

技术领域

[0001] 实施例涉及用于提供密码提示的系统和方法。

背景技术

[0002] 对于很多系统而言，用户验证是重要的需求。例如，软件应用可能针对不同用户容纳不同相应账户并且要求用户验证其身份作为给予用户对其账户的访问权限的条件。例如，互联网应用通常由成千上万的不同用户共享，并且通常要求每一个用户(例如，通过提供验证凭证)验证其身份作为获得对用户账户的访问权限的前提。虽然通常使用验证来证实用户的具体身份，但是该过程更一般地被认为是证实用户拥有一个或更多个特权的特定集合。

[0003] 很多验证过程依赖于用户重现密码的能力。例如，很多网络服务(例如，web应用)利用登录过程来验证用户，其中，该登录过程要求用户重现用户名和密码组合。对企业设施和其他设施及服务的访问可能要求用户重现密码和个人标识号(PIN)组合和/或拥有某一物理令牌(例如，公共/私有密钥、访问/支付智能卡、证书等)的证据。存在很多其他变型。

[0004] 基于密码的验证方案容易受到能够猜测用户的密码的攻击者的攻击。例如，如果用户已经选择“弱”密码(例如，具有几个字符的密码)，则蛮力攻击者可能通过重复地猜测密码并且尝试验证来发现密码。

[0005] 为了阻止攻击者，可期望用户选择难以猜测的“强”密码。密码可能较强，这是因为它是由从较大的字符集合中选择的很多字符和/或很多类型的字符构成。这种密码可以被称作“高熵”。较弱的“低熵”密码可以包括可能从较小的字符集合中选择的较少的字符和/或较少类型的字符。

[0006] 为了确保高熵密码，一些系统施加防止用户创建太弱密码的密码要求(即，密码策略)。此类要求可以包括字符的最小数量、重复字符的最大数量、来自多个集合的字符、无字典词、以及其他此类要求。对密码的复杂度的此类最低要求可以在本文中不加区分地称作密码要求或密码策略。

[0007] 虽然从安全性的角度来看高熵密码可能是期望的，但是此类密码难以记住。因此，用户可能选择低熵密码或者针对多个系统选择相同的高熵密码。此外，用户可以将其密码记录在例如纸上或者计算机文件中。不幸的是，所有这些方法通过使得攻击者更容易猜测或盗取用户的密码而危害系统安全性。

发明内容

[0008] 公开了一种密码提示方法和装置。在一些实施例中，系统可以生成(或以其他方式获得)密码(例如，高熵密码)和使用户能够回想起密码的密码提示。例如，在一些实施例中，当用户需要新密码(例如，以与受密码保护的web应用一起使用)时，用户可以调用密码提示系统并且向该系统提供空间模式。然后，该系统可以获得(例如，生成)强密码并且基于空间模式向用户提供密码提示。用户可以存储密码提示并且当他希望回想起密码时取回密码提

示。

[0009] 在一些实施例中，用于获得密码提示的方法可以包括：从用户接收空间模式以及获得包括多个字符的密码。所述方法还可以包括：获得包括字符布置的密码提示，所述字符布置包括所述密码的所述多个字符和额外字符。所述密码的所述多个字符可以根据所接收的空间模式位于所述字符布置中。所述方法还包括：针对所述用户存储或者向所述用户提供所述密码提示。例如，所述方法还可以包括：针对所述用户存储或者向所述用户提供所述字符布置、或者可以根据其生成所述字符布置的提示信息。

[0010] 在一些实施例中，所述方法还包括：接收密码要求，并且所述获得密码的步骤包括：根据所接收的要求生成所述密码。在所述实施例中，所述方法还可以包括以下步骤：接收对所述密码所针对的网络服务的指示；以及向所指示的网络服务请求所述密码要求。

[0011] 在一些实施例中，所述存储所述密码提示的步骤包括：与所述密码对应于的网络服务相关联地或者与所述密码对应于的目标验证系统相关联地存储所述密码提示。

[0012] 在一些实施例中，所述针对所述用户存储或者向所述用户提供所述密码提示的步骤包括存储或提供：(a)所述字符布置、或者(b)可以根据其生成所述字符布置的提示信息。所述字符布置或可以根据其生成所述字符布置的提示信息可以被存储在移动设备的本地存储设备中或者可以使用第二网络服务来存储。如果是后一种情况，则所述方法还可以包括以下步骤：由所述第二网络服务接收指示用户期望访问所存储的密码提示的请求，其中，所述请求是由移动通信设备发送的。响应于接收到所述请求，如果已经使用所述移动通信设备的订户标识模块验证了所述移动通信设备，则所述第二网络服务给予对所存储的密码提示的访问权限。

[0013] 在一些实施例中，所述方法还可以包括：使用图形图像向所述用户提醒所述空间模式，并且所述密码提示包括所述图形图像。在所述实施例中，所述密码提示可以包括叠加在所述图形图像上的所述字符布置。

[0014] 在一些实施例中，所述方法还包括：响应于检测到正在提醒所述用户输入与所述密码提示相关联的密码，自动地向所述用户提供所述密码提示。在一些实施例中，所述方法还包括：响应于获得所述密码，自动地使用所述密码来向与所述密码相关联的网络服务验证所述用户。

[0015] 在一些实施例中，所述方法(或其特定步骤)可以由移动通信设备来执行。

[0016] 在一些实施例中，所述方法还可以包括：接收与该空间模式不同的初始空间模式；确定所述初始空间模式不满足一个或更多个模式要求；以及响应于确定所述初始模式不满足所述一个或更多个模式要求，提醒所述用户输入另一空间模式，其中，接收最初提到的空间模式的步骤在所述提醒所述用户输入另一空间模式的步骤之后发生。

[0017] 在另一方案中，提供了用于获得密码提示的装置。在一些实施例中，所述装置包括：处理器、以及耦合到所述处理器的存储器。所述存储器存储用于执行以下操作的程序指令：获得包括多个字符的密码以及生成包括字符布置的密码提示。所述字符布置包括所述密码的所述多个字符和额外字符，并且所述密码的所述多个字符根据用户选择的空间模式位于所述字符布置中。所述存储器还存储用于执行以下操作的程序指令：针对所述用户存储或者向所述用户提供所述密码提示。

[0018] 下面参照附图来描述上述和其他方案和实施例。

附图说明

[0019] 并入本文并且形成说明书的一部分的附图示出了本发明的各个实施例，并且结合描述进一步用于解释本发明的原则并使相关领域技术人员能够利用和使用本发明。在附图中，相似的附图标记指示相同或功能上相似的元素。

[0020] 图1是示出了根据一些实施例用于实现密码提示系统的环境的高层次视图的框图。

[0021] 图2a示出了根据一些实施例针对空间模式的提醒的示例。

[0022] 图2b示出了根据一些实施例的密码提示的示例。

[0023] 图3是示出了根据一些实施例用于操作密码提示系统的一般方法的流程图。

[0024] 图4是示出了根据一些实施例用于操作密码提示系统的方法的流程图。

[0025] 图5A是示出了根据一些实施例用于生成密码提示的方法的流程图。

[0026] 图5B是示出了用于获得密码的方法的流程图。

[0027] 图6a是示出了根据一些实施例在客户端(即，用户)、密码提示系统和目标验证系统之间的交互的时间轴示意图。

[0028] 图6b是示出了根据一些实施例在客户端(即，用户)、密码提示系统和目标验证系统之间的交互的时间轴示意图。

[0029] 图6c是示出了根据一些实施例在客户端(即，用户)、密码提示系统和目标验证系统之间的交互的时间轴示意图。

[0030] 图7是示出了根据各个实施例的密码提示系统的各个组件的框图。

[0031] 图8是示出了根据一些实施例用于使用密码提示的过程800的流程图。

[0032] 图9是示出了根据一些实施例用于生成并提供密码提示的密码提示装置的框图。

[0033] 图10是示出了根据一些实施例存储计算机可读程序代码(CRPC)的存储介质的框图。

具体实施方式

[0034] 诸如互联网应用等的很多系统要求基于密码的验证。通常期望用户不创建弱(低熵)密码，这是因为此类密码易于使用蛮力攻击或简单猜测策略而解开。因此，一些验证技术尝试通过施加多种密码要求来防止弱密码。

[0035] 不幸的是，强(高熵)密码难以记住，这引起了很多安全性弱点。例如，用户可能在易受攻击的地方记录其强密码，其中，在该易受攻击的地方，这些密码可能被盗取。一些用户可以根据常见短语或根据先前使用的密码来形成密码，这可能容易被猜测或者已经泄露。一些用户可能在多个系统之间重复使用其强密码，使得针对一个系统盗取用户密码的攻击者可以获得对所有其他系统的访问权限。

[0036] 根据各个实施例，密码提示系统可以代表用户生成(或者以其他方式获得)唯一高熵密码，并且向用户提供可存储的密码提示以帮助用户回想起高熵密码。在一些实施例中，当用户需要新密码(以与web应用一起使用)时，用户可以调用密码提示系统并且向其提供空间模式。然后，系统可以获得(例如，生成)强密码并且基于空间模式向用户提供密码提示。用户可以存储密码提示并且当他需要密码时取回密码提示。在一些实施例中，密码提示

系统可以代表用户存储提示并且当请求提示时为用户取回提示。

[0037] 在一些实施例中，当密码提示系统被调用时，它可以通过显示二维单元网格来向用户提醒空间模式。所有单元可以为空，或者一些或全部单元可以包含一个或更多个字符。在该单元中的至少一些单元包含一个或更多个字符的情况下，网格可以变为密码提示。在该单元中的至少一些单元中具有一个或更多个字符的二维网格在本文中可被称作“abagram”。在向用户显示单元网格之后，用户可以通过从网格中选择单元序列来提供空间模式。在单元中的至少一些单元包含一个或更多个字符的实施例中，与空间模式相对应的单元中的字符(如果有的话)变为用户的密码(假设空间模式满足特定要求)。在其他实施例中，在用户提供空间模式之后，系统可以生成强密码(考虑到密码要求和诸如空间模式的长度、交叉点等空间模式的属性)并且获得密码提示(例如，通过在网格的空单元中放置字符使得所生成的密码的字符根据用户提供的空间模式出现并且在不是空间模式的一部分的单元中的至少一些单元中放置其他字符，来生成abagram)。然后，可以将密码提示(即，具有包含密码的字符的单元和包含其他字符的其他单元的网格)提供给用户。例如，如果用户选择网格的第一行，则密码的字符将是出现在第一行的单元(其中一些可能是空的)中的字符并且多个字符将占用其他单元(或者其他单元中的一些单元)。

[0038] 用户可以用多种方式(例如，将其打印出来、将abagram数字地存储在计算机或电话上、将abagram与通过网络提供的服务存储在一起等)来存储密码提示(例如，abagram)。在一些实施例中，密码提示系统可以针对用户存储abagram。因为在没有用户选择的空间模式的额外知识的情况下密码提示不会直接揭露密码，因此无需像密码一样保护密码提示。当用户希望访问密码时，他可以从存储abagram的地方获得abagram，并且通过回想起当创建密码提示时他最初提供的空间模式来重构密码。

[0039] 图1是示出了根据一些实施例用于实现密码提示系统的环境的高层视图的框图。所示的实施例包括多个客户端设备100，例如，移动电话100a、个人计算机100b、和膝上型计算机100c。示出了三种类型的客户端计算设备以仅用于说明的目的，并且应当理解的是，如本文所描述的，用户可以没有限制地使用多种不同的设备来访问密码提示功能。

[0040] 如图1中所示，任何客户端设备100可以被配置为运行如本地应用105等的密码提示系统。例如，移动设备100a可以被配置为运行本地密码提示应用105a以执行本文所描述的各种功能(例如，创建密码、创建密码提示、存储密码提示、取回密码提示等)。例如，个人计算机100b的用户可以调用密码提示应用105b以在受密码保护的本地软件应用上为新用户账户创建新密码。作为响应，密码提示应用105b可以使用二维网格向用户提醒空间模式，获得密码，基于空间模式和获得的密码创建abagram，并且与受密码保护的本地软件应用相关联地针对用户来存储abagram。当用户稍后希望登录本地软件应用时，他可以指示密码提示应用105b显示abagram并且使用所显示的abagram和空间模式来回想起密码。虽然密码提示应用105a-105c在本文中被统称为密码提示应用105，但是应当理解的是，每一个应用都可以被优化或以其他方式改变以在其相应的主机设备100上工作。

[0041] 在各个实施例中，客户端设备可以通过一个或更多个网络(例如，110)连接到受密码保护的网络服务(例如，120)。网络110可以表示一个或更多个网络(例如，无线或有线局域网、广域网(例如，互联网)和/或其他网络)的任意组合。受密码保护的网络服务120可以与任意数量或类型的网络可接入服务或提供网络接入的服务相对应。例如，服务120可以与

受密码保护的网站(例如,商务网站、社交网络网站、电子邮件应用、云计算服务、和/或其他类型的网络服务)相对应。(例如,从公共位置)对互联网或企业内联网的访问是网络服务的其他示例。任意数量的服务120可以实现网站、web应用、web服务、数据库访问服务、数据通信或处理服务、和/或需要基于密码的验证的任何其他网络可接入服务。如本文所使用的,术语"网络服务"是指通过网络提供的或者提供网络接入的任何服务,例如,如关于网络服务120所描述的。

[0042] 在一些实施例中,密码提示系统(例如,密码提示应用105)可以用于为受密码保护的网络服务(例如,120)创建和/或管理密码。例如,密码提示应用105可以被配置为检测到用户正在给定的受密码保护的网络服务120上创建账户(例如,密码提示应用105可以被配置为检测到web浏览器已经接收到请求用户为网络服务创建新密码的web文档(例如,HTML文档)),并且作为响应,从该网络服务取回密码要求,生成满足这些要求的密码,提醒用户选择空间模式,以及生成abagram(或者其他密码提示)以使得密码的字符根据用户选择的空间模式位于abagram中。然后,用户可以通过将生成的密码提供给网络服务来完成创建用户账户。在一些实施例中,密码提示应用105可以被配置为与针对其来创建密码提示的网络服务相关联地存储该密码提示。因此,用户能够通过网络服务浏览存储的密码提示。在一些实施例中,密码提示应用105能够自动地检测网络服务的验证提醒(例如,检测到用户的浏览器正在显示网站的登录屏幕,该登录屏幕包括请求用户在其中输入密码的文本输入框)并且自动地取回和/或显示与网络服务相关联地存储的密码提示。下面更详细地描述该功能。

[0043] 在一些实施例中,除了密码提示应用105之外或取代密码提示应用105,密码提示系统可以包括密码提示服务115。例如,在一些实施例中,密码提示服务115可以执行上文关于密码提示应用105所描述的所有功能(例如,用户可以调用服务115以生成密码提示、存储密码提示、和/或稍后取回密码提示)。在这样的实施例中,可以使用通用工具(例如,web浏览器)来访问密码提示服务115,使得客户端110根本不需要运行本地密码提示应用105。

[0044] 在一些实施例中,可以在密码提示应用105与密码提示服务115之间划分密码提示系统的各个功能。例如,密码提示应用105可以被配置为生成密码和密码提示,但是使用密码提示服务115来存储和稍后取回密码提示。因此,使用一个客户端设备(例如,个人计算机100b)创建密码和提示的用户可以稍后使用另一客户端设备(例如,移动设备100a)取回提示。例如,应用105b可以在计算机100b上为用户创建密码提示,并且在密码提示服务115处存储提示。稍后,同一用户可以通过使用移动设备100a上的密码提示应用105a或膝上型计算机100c上的应用105c来访问存储在服务115上的密码提示。

[0045] 在各个实施例中,对密码提示存储功能的访问(如上文关于密码提示应用105和密码提示服务115所描述的)可能自身需要验证,例如,基于密码的验证、生物验证或者其任意组合。在一些实施例中,验证可以基于与客户端设备100和/或其组件相关联的标识符。例如,在密码提示被存储在密码提示服务115处的实施例中,服务115可以基于移动设备100a正在使用的订户标识模块(即,SIM卡)来对移动设备100a的用户进行验证。

[0046] 图2a示出了根据一些实施例,针对空间模式的提醒200的示例。在各个实施例中,可以由诸如密码提示应用105或密码提示服务115等的密码提示系统来创建和/或显示提醒200。响应于用户输入,或者响应于检测到用户正在尝试创建新验证凭证,密码提示系统可

以自动地创建和/或显示提醒200。

[0047] 根据所示的实施例，提醒200是二维(4 x 4)单元网格，其中，每一个单元都是空的。在其他实施例中，提醒200的一些单元可以包含一个或更多个字符，如图2b中所示。因此，在一些实施例中，提醒200可以是abagram。此外，在其他实施例中，提醒可以是具有不同维度的网格，例如，n x m的网格，其中，n和m是不同的。在一些实施例中，网格的相对侧可以是一致的(identify)使得空间模式可以回绕，例如，从一侧出去并且在相对侧继续。在其他实施例中，提醒可以由多个网格组成。在一些实施例中，提醒可以是具有任意形状的非矩形网格。在其他实施例中，提醒可以根本不是网格。例如，提醒可以是准许用户例如通过在图形中选择区域序列来规定和回想起空间模式的任意图形(例如，照片)，或者提醒可以是诸如立方体等的三维结构或者其他三维结构。在一些实施例中，提醒可以包括子提醒的序列，其中，每一个子提醒可以根据前述实施例之一来形成。然后，每一个子提醒可以与密码的一部分相关联。

[0048] 在所示的实施例中，向其呈现了提醒200的用户可以选择空间模式(例如，空间模式205)，该空间模式包括二维网格的四个单元的有序(ordered)集合。如本文所使用的，术语“空间模式”是指具有任意数量的维度的空间中的任意有序位置序列。例如，空间模式可以是任意数量的维度的一条或多条线的序列。例如，空间模式205包括通过二维空间的两条直线，其中，在提醒200中，该两条线定义四个单元的有序序列。

[0049] 用户可以使用适合于用户正用于访问密码提示系统的客户端设备的无论哪种方式来选择诸如模式205等的空间模式。例如，使用移动设备(例如，100a)的用户可以在定义空间模式205的单元序列上滑动其手指或者按压与空间模式205相对应的按键序列。在台式计算机(例如，100b)上，用户可以利用键盘、鼠标、操纵杆、或者其他定点设备来选择模式。在各个实施例中，空间模式无需是连续的，并且可以与提醒的任意单元/区域序列相对应。在一些情况下，用户可以重复地选择相同模式中的单元/区域。

[0050] 在一些实施例中，当正在选择模式时，所选择的空间模式可以显示在提醒上。例如，在图2a中，当正在定义空间模式205时，空间模式205被显示在提醒200上，如图2a中所示。将理解的是，在用户定义空间模式205之前，空间模式205不会在一开始作为提醒200的一部分被显示。

[0051] 在提醒200具有图2a中所示的形式(即，单元为空)的实施例中，在(例如，使用提醒200)向用户提醒空间模式并且在用户提供空间模式(例如，空间模式205)之后，系统可以使用空间模式和字符集合(例如，字母、数字等)生成密码提示。例如，密码提示可以包括叠加在提醒上的字符布置，使得密码的字符根据用户定义的模式被叠加。在其他实施例中，提示可以仅包括字符布置而没有原始提醒中的任意或全部字符。在提醒200是abagram的实施例中，在用户提供空间模式(例如，空间模式205)之后，系统可以确定空间模式是否满足特定的预定义要求。如果不满足，则用户必须输入新空间模式，否则，系统将获得abagram的与用户选择的空间模式相对应的字符来作为用户的密码。

[0052] 图2b示出了根据一些实施例的密码提示250的示例。在所示的示例中，密码提示250是abagram，其可以与响应于用户使用图2a的提醒200选择空间模式205而创建的密码提示相对应。

[0053] 根据图2b所示的实施例，密码提示250包括覆盖在提醒200上的字符布置，使得网

格中的特定单元包含一个、两个或三个字符。在其他情况下，系统可以在每一个单元中包括任意数量的字符，特定的单元甚至可以根本不具有字符，这是可以取决于目标验证系统的密码要求和/或由用户选择的空间模式所规定的单元数量的决定。例如，如果目标验证系统要求密码具有至少八个字符但是用户已经选择仅覆盖三个单元的空间模式，则提示生成器可以在每一个单元中包括至少三个字符。作为第二示例，如果用户已经选择自相交空间模式，则模式自相交处的网格单元可以为空。

[0054] 如本文所使用的，术语“目标验证系统”是指可以由服务或网络服务使用的任何验证系统。验证系统可以是网络服务的一部分、子组件、或者与它为其提供验证的服务分离的第三方验证系统。给定的验证系统还可以为多个不同的服务或网络服务提供验证功能。

[0055] 密码提示250的字符被布置为使得密码中的字符根据所选的空间模式出现。例如，如果用户选择了图2a的空间模式205，则由密码提示250指示的密码为“i8pBn j4u”。当用户看见密码提示250时，他可以回想起他选择的空间模式，并且使用该记忆结合密码提示250来确定他的密码。

[0056] 图3是示出了根据一些实施例用于操作密码提示系统以生成密码提示从而辅助用户回想起目标服务的密码的一般方法的流程图。图3的方法可以由密码提示应用(例如，图1的105)、密码提示服务(例如，图1的115)或者其任意组合来执行，如上所述。可以通过多种方式(例如，通过用户请求和/或通过自动检测到用户正在尝试创建验证凭证或者已经被提醒创建针对目标服务的验证凭证)来发起该方法。

[0057] 根据所示的实施例，如步骤300所示，密码提示系统可以接收密码要求。密码要求可以与目标服务的验证系统(即，目标验证系统)指定的那些密码要求相对应。例如，受密码保护的网站(例如，网络服务120的受密码保护的网站)通常要求用户的密码符合要求，例如最小长度、至少包括特定类型的字符、包括最小字符多样性、不包括特定词(例如，字典词、用户的名字、和/或其明显变型)、不包括重复字符和/或其他类型的要求等。

[0058] 可以通过不同方式执行300的密码要求收集步骤。例如，在一些实施例中，密码提示系统可以提醒用户识别特定的密码要求。在其他实施例中，系统可以被配置为经由特定接口来请求密码要求。例如，如果目标服务(和/或目标验证系统)被实现为网络服务，则网络服务可以开放(expose)编程接口(API)或者符合通信协议，其中，通过该通信协议，密码提示系统可以以某一机器可读格式向网络服务(和/或向目标验证系统)请求并获得密码要求。

[0059] 在步骤310中，密码提示系统向用户提醒空间模式。例如，系统可以通过显示诸如图2a中的提醒200等的二维网格来提醒用户。如上文所讨论的，提醒可以包括辅助用户定义并选择空间模式的任意图形。

[0060] 在步骤315中，系统从用户接收空间模式。如上所述，用户可以利用适合于他正在使用的计算设备的任何选择方式。例如，用户可以使用其手指在触摸屏上滑动模式，点击键盘或键区上的按键，使用诸如鼠标或操纵杆等的定点设备，和/或利用用于规定模式的任何其他适合的方式。

[0061] 在步骤320中，密码提示系统确定接收到的模式是否满足一个或更多个模式要求(例如，足够复杂、不太复杂等)。320的决定可以取决于多种因素，例如，在300中接收到的密码要求和/或在310中向用户提供的提醒。例如，密码提示系统可以被配置为要求空间模式

包括提醒的最小数量的可分辨区域(例如,从网格中选择的最小数量的单元)、和/或最小数量的连续区域,使得模式难以猜测。决定320还可以或者以其他方式取决于目标验证系统的密码要求。例如,考虑密码提示系统能够使用覆盖在提醒的每一个区域上的最多四个字符来创建提示的实施例。如果目标验证系统需要具有至少10个字符的密码并且用户已经选择仅包括提醒的两个区域的空间模式,则密码提示系统可能不能生成组适当的提示。在该情况下,密码提示系统可以提醒用户选择包括提醒的至少三个区域的更长/更复杂的空间模式。

[0062] 在一些实施例中,在步骤320中,系统可以确定空间模式是否太复杂。例如,在一些系统中,可以禁止用户选择自相交的空间模式。在这种系统中,如果用户选择自相交模式,则决定320可以判定为否定。在步骤320中,系统可以检查各种其他要求。例如,如果提示系统确定给定模式限制了可以使用该模式生成的密码的熵,则提示系统可以在决定320中拒绝这种模式。

[0063] 如320的否定支路所指示的,如果密码提示系统确定所选模式不满足模式要求,则该方法返回310并且密码提示系统再次向用户提醒新空间模式。

[0064] 如320的肯定支路所指示的,如果密码提示系统确定模式满足要求,则在步骤322中,在一些实施例(例如,提醒200具有图2a中所示的形式的实施例)中,密码提示系统获得(例如,生成、选择、接收、取回)满足在步骤300中接收的要求的密码。例如,在一些实施例中,密码提示系统可以通过使用随机数或伪随机数发生器生成满足要求的密码来获得密码。下面更详细地描述用于生成密码的多种方法。如320的肯定支路所指示的,如果密码提示系统确定模式满足要求,则在其他实施例(例如,提醒200是abagram的实施例)中,密码提示系统通过确定abagram的与空间模式相对应的单元的字符来获得密码。

[0065] 在一些实施例中,密码提示系统可以从不同组件、从第三方或者从用户自身接收密码。例如,目标验证系统自身可以开放用于获得满足验证系统的最小复杂度要求的新密码的编程接口。在这样的实施例中,密码提示系统可以在步骤322中从目标验证系统获得有效密码,而无需获得密码要求(如在步骤300中一样)并且执行密码生成。在其他实施例中,在获得满足特定要求的密码时,密码提示系统可以从先前生成的密码集合中选择密码,其中,集合中的每一个密码满足要求。在用户已经知道密码的其他实施例中,在获得密码时,密码提示系统提醒用户输入密码。

[0066] 在一些实施例中,在步骤322中获得的密码可以取决于在步骤315中接收的空间模式。例如,在一些实施例中,所获得的密码可以包含取决于空间模式(例如,针对网格提醒的每一个单元具有一个字符)的多个字符。在另一示例中,如果空间模式是自相交的路径,则可以生成具有重复字符的密码。通常,在各个实施例中,在空间模式与生成的密码长度之间可能存在任意关系。如果没有关系,则可以在接收到空间模式之前或之后生成密码。

[0067] 在步骤325中,密码提示系统获得(例如,生成、选择)包括字符布置的密码提示,其中,密码字符根据空间模式位于布置内。例如,密码提示可以是abagram,例如,图2b的密码提示250。

[0068] 在一些实施例中,提示系统可以生成密码提示使得将难以在给定提示的情况下猜测密码。在这样做时,提示系统可以考虑目标验证系统的密码策略。例如,如果验证系统要求每一个密码包括至少一个数字,则提示系统可以尝试生成在多个位置中包括至少一个数

字的提示，使得很多模式将包括至少一个数字。

[0069] 在一些实施例中，可以在步骤322之前执行步骤325。例如，在一些实施例中，密码提示系统可以维持预先存在的abagram的集合，并且在执行步骤325时，密码提示系统仅选择预先存在的abagram之一。在这样的实施例中，密码提示系统可以通过按照用户所选的空间模式仅从所选的预先存在的abagram中选择字符序列来执行步骤322(即，获得密码)。在其他实施例中，密码提示系统可以迭代地并且可能自适应地根据字符集合的某一概率分布来生成随机密码提示，直到提示和模式引起的字符串满足密码要求为止。

[0070] 在步骤330中，密码提示系统存储密码提示和/或向用户提供密码提示。在一些实施例中，提供密码提示可以包括显示密码提示，提供密码提示文件，打印密码提示，和/或执行使用户能够立即和/或稍后访问密码提示的任何其他功能，例如，存储或请求在可以重构密码提示的算法中使用的输入值。在一些实施例中，针对用户存储或者向用户提供密码提示可以仅包括存储或提供可以根据其生成字符布置的提示信息。例如，在通过使用伪随机数发生器和具有一个或更多个种子值(提示信息)的集合生成包括密码提示的字符来创建密码提示的实施例中，存储或提供密码提示的步骤可以包括(或仅包括)存储或提供提示信息(具有一个或更多个种子的集合)。

[0071] 在一些实施例中，该方法还可以包括向用户提供对在步骤322中获得的密码的访问。在用户期望在创建密码之后立即使用密码的情况下，向用户提供密码可以带来一定程度的方便。例如，在一些实施例中，可以向用户显示密码，该用户然后可以将密码复制到目标网络服务的密码验证字段中。除了显示密码文本之外和/或取代显示密码文本，密码提示系统可以通过以下方式提供新密码：将新密码放置在用户系统的复制/粘贴缓存中、将密码直接写入受密码保护的服务的适当验证字段中、自动地使用密码向目标服务进行验证、和/或更直接地向用户提供密码。

[0072] 如上所述，在一些实施例中，密码提示系统可以通过与图3中所示的顺序不同的顺序来获得密码和/或密码提示。例如，在一些实施例中，密码提示系统可以首先生成密码提示，然后使用密码提示提醒用户选择模式。为了进一步说明此构思，考虑生成abagram提示的提示系统，该abagram提示满足强制字符来自特定字符集合的这种类型的密码要求。这种提示系统可以按如下方式操作：(1)根据字符集合C1生成M个随机字符，其中，M至少具有abagram矩形的列的长度(针对其他策略要求的字符集合应用相同的过程)；(2)将属于特定集合的字符作为列或者其他从上至下的连续模式进行嵌入；(3)添加关于模式必须在左侧与右侧之间包含连续组成部分的模式要求；(4)从字符集合的并集中随机地、均匀地选择或者根据策略以加权的方式选择abagram中的其他(非模式覆盖的)条目。如果符合额外的模式要求，则密码要求也是如此。

[0073] 图4是示出了根据一些实施例用于操作密码提示系统的方法的流程图。图4的方法可以与图3的方法的更具体的实现方式相对应，并且可以由相同的系统并且响应于相同的条件来执行。

[0074] 当密码提示系统从用户输入接收到密码要求时，图4的方法在步骤400中开始。例如，用户可以使用图形用户界面向系统输入密码要求。因此，步骤400可以与图3的步骤300相对应。

[0075] 在步骤410中，密码提示系统通过显示空的NxM网格来向用户提醒空间模式(在一

些实施例中，N可以等于M)。网格可以看起来与图2a中的提醒200类似。因此，步骤410可以与图3的步骤310相对应。

[0076] 在步骤415中，密码提示系统接收用户选择的单元序列。例如，系统可以接收图2a的空间模式205。因此，步骤415可以与图3的步骤315相对应。

[0077] 在步骤420中，与步骤320中一样，密码提示系统确定空间模式是否满足模式要求(例如，足够复杂)。如果否(如来自420的否定支路所指示的)，则密码提示系统向用户提醒另一模式(如至410的反馈回路所指示的)。否则，如果序列是令人满意的(如来自420的肯定支路所指示的)，则系统生成密码，如步骤422所示。

[0078] 在步骤422中，密码提示系统生成满足步骤400中输入的要求的密码。在步骤422中，密码提示系统可以使用用于生成高熵密码的各种已知方法(例如，通过应用伪随机数生成和/或其他统计方法)来生成密码。因此，步骤422可以与图3中的步骤322相对应。在一些实施例中，在步骤422中生成的密码可以取决于在步骤415中接收的空间模式。例如，如果在步骤415中接收的空间模式具有长度为(1)的单元，则在步骤422中生成的密码也可以具有长度为(1)的字符。

[0079] 在步骤425中，密码提示系统获得NxM的abagram，其中，所生成的密码的字符出现在用户所选的单元序列中(即，符合空间模式)。因此，NxM的abagram用作密码提示。因此，步骤425可以与图3的步骤325相对应。

[0080] 在步骤430中，密码提示系统将abagram作为密码提示进行存储。在各个实施例中，系统可以在本地(例如，作为文件、在DB中等)或者在通过网络可访问的远端服务器(例如，图1的密码提示服务115)中存储abagram。

[0081] 在步骤435中，密码提示系统向用户显示abagram。在各个实施例中，密码提示系统可以在存储abagram之前、之后或者同时向用户显示abagram。除了在步骤435中显示abagram之外或者取代在步骤435中显示abagram，密码提示系统可以向用户提供对在步骤422中生成的密码的直接访问，或者以其他方式方便向目标系统进行验证。

[0082] 图5A是示出了根据一些实施例用于生成密码提示的方法的流程图。图5的方法可以与图3的步骤322和325或者图4的步骤422和425相对应。

[0083] 在步骤500中，密码提示系统获得满足目标验证系统可施加的无论什么最低密码要求的密码。获得密码可以涉及生成、取回和/或以其他方式获得来自第三方的密码，如关于图3的步骤322或图4的步骤422所述的。例如，为了生成密码，系统可以伪随机地从所需字符的一个或更多个集合中选择字符，直到密码包含所有所需字符为止，伪随机地选择额外字符，直到密码具有期望长度为止，并且伪随机地改变所选字符的顺序。

[0084] 在步骤505中，密码提示系统根据所接收的空间模式布置密码的字符。例如，如果密码提醒是图2a的网格并且所生成的密码是“i8pBnj4u”，则密码提示系统可以将密码嵌入到网格中(即，将字符“i8”放置在由模式指示的第一单元中，将“pB”放置在由模式指示的第二单元中，以此类推，直到由空间模式指示的四个单元共同包含密码“i8pBnj4u”为止，如密码提示250中所示)。在一些实施例中，密码提示系统无需将字符直接嵌入到提醒(例如，网格)中，而是可以根据空间模式对其进行简单布置。

[0085] 在步骤510中，密码提示系统通过插入来自可能字符集合的多个字符来填满字符布置的剩余部分。密码提示系统可以被配置为经由与用于获得密码要求的机制相同或类似

的机制来确定可能字符集合。在各个实施例中，可以通过均匀方式或加权方式从所有有效字符集合中选择填满提示布置的字符。举非均匀选择的例子，字符的剩余部分可以被选择为使得网格的更大数量的空间布置包含符合密码要求的字符。例如，如果密码要求是每一个密码必须包含(来自集合“0”、“1”、……“9”的)至少一个数字，则可以确保每一行和列包含至少一个这样的数字。这使得已经获得对密码提示的访问权限的第三方难以提取密码。

[0086] 用于创建字符布置提示的各种其他算法是可能的。例如，系统可以首先接收用户的空间模式，然后生成伪随机地和/或通过加权分布从合法字符集合中选择的字符布置，并且最终检查以确定布置和模式是否定义合法密码。如果是，则向用户提供提示。否则，密码提示系统可以重复该过程(可选地，例如通过响应于哪些密码要求未被符合而改变字符的加权分布，以调整布置生成算法)，直到它(考虑到用户的空间模式)产生定义合法密码的密码提示为止。因此，可以在步骤320之后执行步骤322，并且可以在步骤420之后执行步骤422。

[0087] 图5B是示出了用于在获得密码提示之后获得密码的过程的流程图。该过程可以在步骤520中开始，在步骤520中，密码提示系统获得密码提示(例如，生成密码提示或者从预定义的密码提示集合中选择密码提示)。在步骤522中，密码提示系统显示密码提示，从而向用户提醒空间模式。在步骤524中，密码系统接收用户输入的空间模式。在步骤526中，密码提示系统确定空间模式是否满足特定要求。如果否，则过程返回步骤522，使得用户可以输入新空间模式，否则，过程前进至步骤528。在步骤528中，密码提示系统基于用户输入的空间模式来根据密码提示获得密码。例如，密码提示系统确定密码提示的与空间模式相对应的字符。在步骤530中，密码提示系统针对用户存储(和/或向用户提供)密码提示。

[0088] 图6a是示出了根据一些实施例在客户端、密码提示系统和目标验证系统之间的交互的时间轴示意图。客户端100可以与图1的可以由用户操作的客户端系统100中的任意一个相对应。密码提示系统600可以与密码提示应用105、密码提示服务115或者其任意组合相对应。目标验证系统605可以与任何基于密码的验证系统相对应，不论它是在与客户端100和/或密码提示系统600相同的计算机上运行，在相同网络上的不同计算机上运行，还是在互联网或其他广域网上的远端计算机上运行的。例如，验证系统605可以与web应用(例如，web电子邮件应用)的用户名和/或密码登陆相对应。用垂直方向表示时间，其中，稍后事件出现在早前事件的下方。请求描述出现在请求上方并且请求参数出现在下方。

[0089] 根据所示的实施例，客户端100向密码提示系统600发送对密码提示生成的请求610。请求610包括对目标验证系统605的密码策略(即，要求)的描述。客户端可以通过用户输入、通过查询数据库或另一系统(例如，目标验证系统605)或者任何其他方式来获得密码策略。

[0090] 请求610还包括用户定义的空间模式(例如，空间模式205)。在一些实施例中，客户端100可以在首先向密码提示系统600请求并接收到提醒(例如，二维网格)之后向密码提示系统600发送空间模式。在各种这样的实施例中，客户端100可以在请求610中或者在(例如，针对提示提醒的)前一请求中向密码提示系统提交密码策略。

[0091] 在响应615中，密码提示系统600通过向客户端100返回密码提示来对请求610进行响应。密码提示可以是abagram或者任何其他字符布置，其中，目标验证系统的密码的字符根据在610中接收的空间模式位于布置内。提示自身可以具有多种形式，例如，图像文件、标

记描述(例如,HTML、XML)、或者足以表示字符布置的任何其他格式。

[0092] 在各个实施例中,为了方便用户,响应615可以包括密码自身。例如,如果密码提示系统600被实现在远端系统(例如,115)上,则密码提示系统可以返回提示以及客户端100的密码的文本表示以向用户显示,从而为用户节省根据提示导出密码的时间。如果密码提示系统600是与客户端在相同的设备上的本地应用(例如,应用105),则返回密码提示可以包括显示和/或保存提示、显示密码、和/或将密码放置在客户端系统100的复制/粘贴缓存中。

[0093] 在请求620中,客户端100使用密码来创建其登陆凭证和/或向目标验证系统605进行验证。在密码提示系统600将密码放置在客户端100的复制/粘贴缓存中的实施例中,用户可以简单地将密码粘贴到目标验证系统605的密码字段中,并且在请求620中提交密码。

[0094] 图6b是示出了根据一些实施例在客户端、密码提示系统和目标验证系统之间的交互的时间轴示意图。图6b是图6a的时间轴的变型。可以对类似元素进行等同编号,并且可以应用关于图6a对这些元素的描述。

[0095] 在图6b中,客户端100发送针对提示生成的请求612。与图6a中的请求610相比,请求612不直接包括密码要求,而是包括服务标识符(例如,URL),在服务标识符处,密码提示系统600可以获得目标验证系统605的密码策略。在一些实施例中,标识符可以是目标验证系统605或相关系统开放的URL。

[0096] 在请求625中,密码提示系统600向目标验证系统605请求密码策略。在响应630中,目标验证系统605返回关于密码策略的指示。通过使用630中接收的密码策略,密码提示系统600可以生成满足要求的新高熵密码。在一些实施例中,不同于在630中返回密码策略,目标验证系统605可以返回可用的新高熵密码。这种系统可以减少密码提示系统600的复杂度。

[0097] 与图6a中一样,密码提示系统600在响应615中向客户端100返回提示(潜在地还有密码)。在请求620中,客户端100向目标验证系统605呈现其密码和/或其他验证凭证。

[0098] 图6c是示出了根据一些实施例在客户端、密码提示系统与目标验证系统之间的交互的时间轴示意图。图6c是图6a和图6b的时间轴的变型。可以对类似元素进行等同编号,并且可以应用关于图6a和图6b对这些元素的描述。

[0099] 在图6c中,客户端100尝试通过向目标验证系统605发送请求635来创建验证证书。例如,客户端100可以向受验证系统605保护的web应用请求“创建账户”或“重置密码”网页。作为响应,目标验证系统605或相关系统可以向客户端100发送登录/凭证-创建界面以向用户进行显示。

[0100] 响应于检测到客户端100尝试创建新密码(如请求635中所示),目标验证系统605可以调用密码提示系统600。在各个实施例中,验证系统605可以用不同的方式来调用密码提示系统600。例如,在一些实施例中,验证系统605可以向密码提示系统600直接发送请求(例如,请求640),该请求指示密码提示系统600与客户端100进行交互以创建密码和提示。请求640可以包括目标验证系统605的密码策略。

[0101] 在其他实施例中,验证系统600可以向客户端100发送重定向指令,从而指示客户端100使用密码提示系统600建立密码。重定向指令可以包括关于验证系统605的密码策略的指示。重定向指令可以使客户端100例如在弹出窗口、web浏览器的新标签或窗口、网页的新框或者其他界面机制中向用户显示针对密码提示系统600的界面。在一些实施例中,可以

显示针对密码提示系统的界面，使得目标验证系统605的登录/凭证创建界面中的一些或全部仍然被显示。

[0102] 在请求645中，密码提示系统600向客户端100请求空间模式。该请求可以包括提醒，例如，二维网格。响应于接收到请求645，客户端100可以向其用户提醒空间模式并且在应答650中将模式返回密码提示系统600。在一些实施例中，用户可以将客户端100配置为始终使用相同的模式。在这样的系统中，客户端100可以无需每当它接收到诸如645等的请求时便向其用户提醒模式。取而代之地，客户端可以自动地在应答650中发送先前存储的默认模式。

[0103] 响应于在650中接收到空间模式，密码提示系统600在响应615中发送密码提示(可选择地，以及密码)。在请求620中，客户端100的用户使用提示和/或密码来创建其登录凭证和/或登录到验证系统605。

[0104] 在一些实施例中，密码提示系统600可以使用密码在目标验证系统605处自动地设置用户的密码和/或向目标验证系统605验证用户。因此，不同于要求客户端100单独地发送消息620和/或后续验证消息，密码提示系统600可以代表用户自动地发送这样的消息。

[0105] 在一些实施例中，图6c的密码提示系统600可以是身份提供商服务(IdP)的一部分。IdP可以用作用户(例如，客户端100)与各种验证系统(例如，系统605)之间的中间设备。在这样的系统中，除了为客户端100创建密码和密码提示之外，IdP还可以与用户和目标验证系统605相关联地存储提示，并且在后续适合时间将提示提供给用户。例如，当用户稍后(例如，通过到达登录屏幕)占用(engage)目标验证系统605时，目标验证系统可以向用户提供(例如，通过点击按钮)从IdP取回其提示的选项。响应于用户请求，目标验证系统可以从IdP取回密码提示或者(例如，经由重定向或弹出窗口)使客户端取回密码提示。

[0106] 图7是示出了根据各个实施例的密码提示系统的各个组件的框图。密码提示系统700可以与提示应用(例如，图1的105)、提示服务(例如，图1的115)或者其任意组合相对应。在不同的实施例中，图7中所示的组件中的任意一个组件可以被组合或者被进一步分解为执行各个功能。

[0107] 根据所示的实施例，密码提示系统700包括接口模块705。接口模块705可以包括用于调用密码提示系统的API。在各个实施例中，可以通过在相同机器上运行的软件和/或通过经由web服务接口在远端机器上运行的软件来调用API。在一些实施例中，接口模块705可操作以显示图形用户界面和/或与其他系统或组件进行通信。

[0108] 系统700还包括密码要求取回器710。在一些实施例中，要求取回器710可以被配置为查询目标验证系统以得到其密码要求。要求取回器710可操作以例如通过提醒用户进行输入或者查询具有已知要求的数据库来从其他或额外的源取回密码要求。

[0109] 系统700包括密码获得模块715。密码获得模块715可以被配置为生成或者以其他方式获得满足密码策略取回器710取回的密码要求的高熵密码。如本文所描述的，模块715可以通过应用各种随机数或伪随机数生成技术来创建满足给定要求的新高熵密码，以生成密码。在一些实施例中，不同于生成密码自身，模块715可以查询不同系统(例如，目标验证系统)以得到密码。

[0110] 系统700包括空间模式取回器720。如本文所使用的，取回器720可以被配置为创建提醒(例如，二维网格)并向用户发送提醒，并且接收和记录响应于提醒的空间模式。

[0111] 系统700还包括密码提示生成器725。生成器725可以被配置为生成或以其他方式获得包括字符布置的提示，其中，密码的字符根据接收的空间模式位于布置内。如本文所描述的，生成器725可以通过应用各种随机数或伪随机数生成技术来生成提示。例如，在一些实施例中，生成器725可以通过执行图5的方法来生成提示。

[0112] 系统700包括提示存储服务730和提示取回服务735。存储服务730可以用于存储针对不同验证系统(例如，不同网站)的密码提示。存储服务可以位于单个计算机本地或者可以由多个不同客户端通过网络进行调用以存储密码提示。提示取回服务735可以联合存储服务730操作以允许用户取回用户先前存储的提示。

[0113] 如上所述，为了存储和取回为多个不同用户提供服务的服务，服务可能自身需要验证。在一些实施例中，可以通过提供密码、通过确认用户正在使用预先验证的软件或硬件(例如，SIM卡)或者其他方法来准许验证。

[0114] 图8是示出了根据一些实施例用于使用密码提示的过程800的流程图。过程800可以在步骤802开始，在步骤802中，用户使用客户端设备100来向网站的web服务器发送对网页的请求(例如，提醒用户输入用户名和密码以允许用户获得对网站的访问权限的网页)。在步骤810中，客户端设备100接收所请求的网页。在步骤820中，在客户端设备100上运行的密码提示应用105确定所接收的网页是否提醒用户向密码输入字段(例如，文本框，或指示它不仅是文本而且是密码文本的现有或新型字段)输入密码。如果所接收的网页未提醒用户输入密码，则过程前进至步骤860。

[0115] 否则，如果所接收的网页提醒用户输入密码，则过程前进至步骤830。在步骤830中，密码提示应用105响应关注于密码输入字段而自动地显示与网站相关联的密码提示，并且提醒用户输入空间模式。在其他实施例中，在步骤830中，密码提示应用105不自动地显示密码提示，而是可以使可选元件(例如，按钮)显示在密码输入字段的附近，并且显示密码提示并响应于用户选择可选元件来提醒用户输入空间模式。备选地，可以向网页嵌入针对默认或可选密码提示系统的这种可选元件。在任意一种情况下，假设用户先前已经使用密码提示应用105(或密码提示服务115)来获得考虑中的网站的密码提示并且密码提示应用105具有对该密码提示的访问权限。

[0116] 在步骤840中，密码提示应用105接收用户输入的空间模式。在步骤850中，密码提示应用使用来自密码提示的与用户接收的空间模式相对应的字符序列来自动地填充密码输入字段。通过这种方式，如果用户能够记住他/她使用以生成密码提示的空间模式，则用户可以获得对网站的访问权限，即使用户不能记住网站的密码。

[0117] 图9示出了根据一些实施例的密码提示系统105/115的至少一些组件的可能实现方式。如图9中所示，密码提示系统105/115可以包括：数据处理系统902，数据处理系统902可以包括一个或更多个数据处理设备，每一个数据处理设备具有一个或更多个微处理器和/或一个或更多个电路，例如，专用集成电路(ASIC)、现场可编程门阵列(FPGA)等；用于接收消息(例如，从客户端100和/或网络服务120发送的消息)和发送消息的网络接口925；数据存储系统905，数据存储系统905可以包括一个或更多个计算机可读介质，例如，非易失性存储设备和/或易失性存储设备(例如，随机存取存储器(RAM))。如图所示，数据存储系统905可以用于存储密码提示250和密码要求信息911。

[0118] 在数据处理系统902包括微处理器的实施例中，提供了密码提示计算机程序产品，

计算机程序产品包括：计算机可读程序代码943，计算机可读程序代码943执行存储在计算机可读介质942上的计算机程序，计算机可读介质942例如但不限于：磁性介质（例如，硬盘）、光学介质（例如，DVD）、存储设备（例如，随机存取存储器）等。在一些实施例中，计算机可读程序代码943被配置为使得当由数据处理系统902执行代码943时，代码943使处理系统执行上述步骤（例如，上文关于图3、图4或图5所示的流程图所述的步骤）。

[0119] 在其他实施例中，密码提示系统105/115可以被配置为执行上述步骤而无需代码943。例如，数据处理系统902可以仅由专用硬件（例如，一个或更多个专用集成电路（ASIC））构成。因此，本发明的上述特征可以用硬件和/或软件来实现。例如，在一些实施例中，上述密码提示系统的功能组件可以由执行计算机指令943的数据处理系统902、由独立于任何计算机指令943操作的数据处理系统902或者由硬件和/或软件的任何适当组合来实现。

[0120] 图10示出了计算机可读程序代码（CRPC）943的实施例。在所示的实施例中，CRPC 943包括（1）用于接收密码要求的指令集合1005、（2）用于获得密码的指令集合1010、（3）用于向用户提醒空间模式的指令集合1015、（4）用于接收空间模式的指令集合1020、（5）用于确定接收的模式是否满足一个或更多个模式要求的指令集合1025、（6）用于生成密码提示的指令集合1030、以及（7）用于存储密码提示和/或向用户提供密码提示的指令集合1035。

[0121] 虽然已经在上文中描述了本发明的各个实施例，但是应当理解的是，它们仅是通过举例说明而非限制性的方式来呈现的。因此，本发明的宽度和范围不应当受到上述示例性实施例中任意一个的限制。此外，除非在本文中另外指示或者通过上下文明确否定，否则本发明涵盖上述元素以其所有可能的变型的任意组合。

[0122] 此外，虽然上文所描述的且在附图中示出的过程被示出为步骤序列，但是这样实现只是为了便于说明。因此，设想可以添加一些步骤，可以省略一些步骤，可以重新布置步骤的顺序，并且可以并行地执行一些步骤。

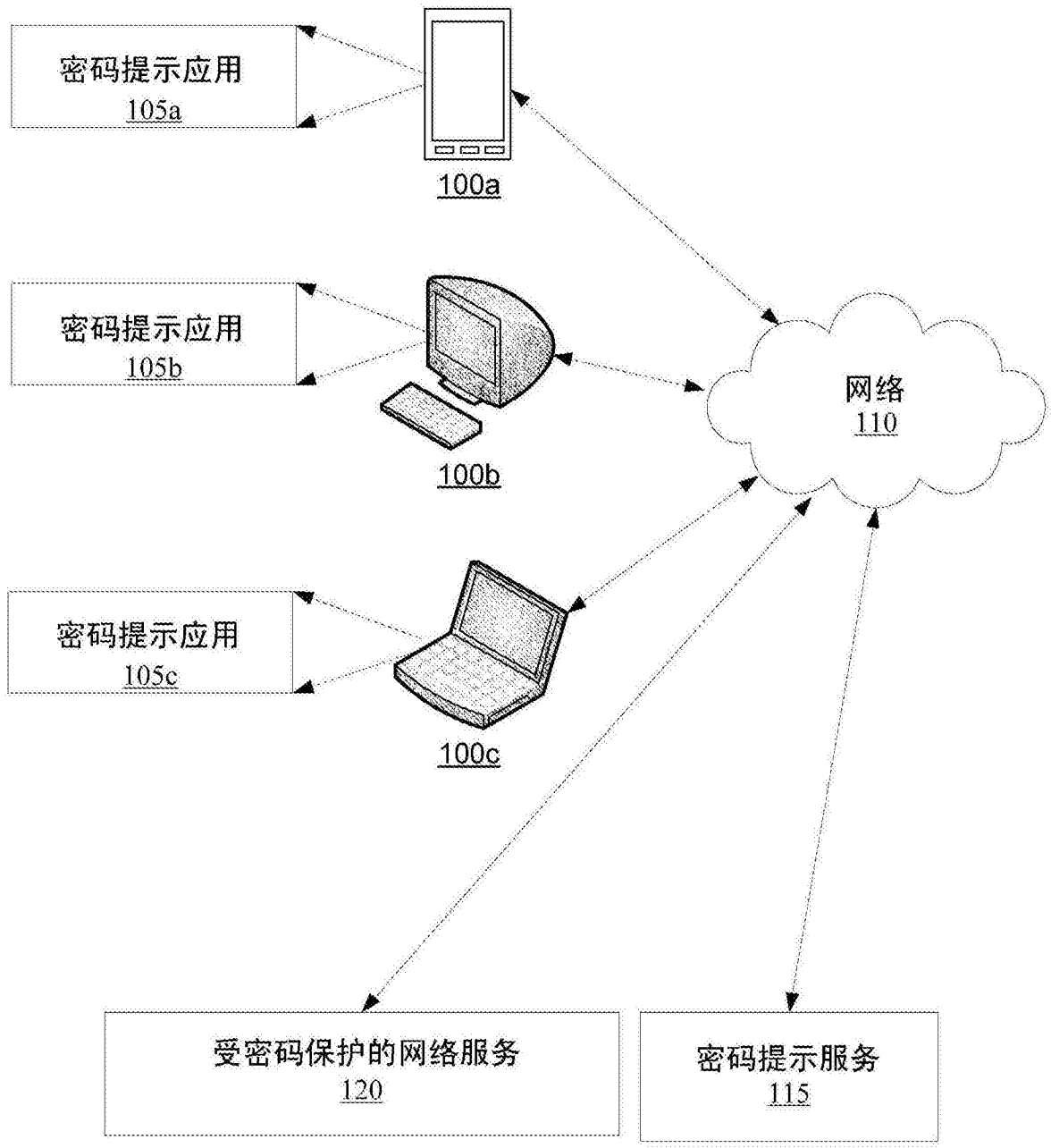

密码提示应用
105a
100a
密码提示应用
105b
100b
网络
110
密码提示应用
105c
100c
受密码保护的网络服务
120
密码提示服务
115

图1

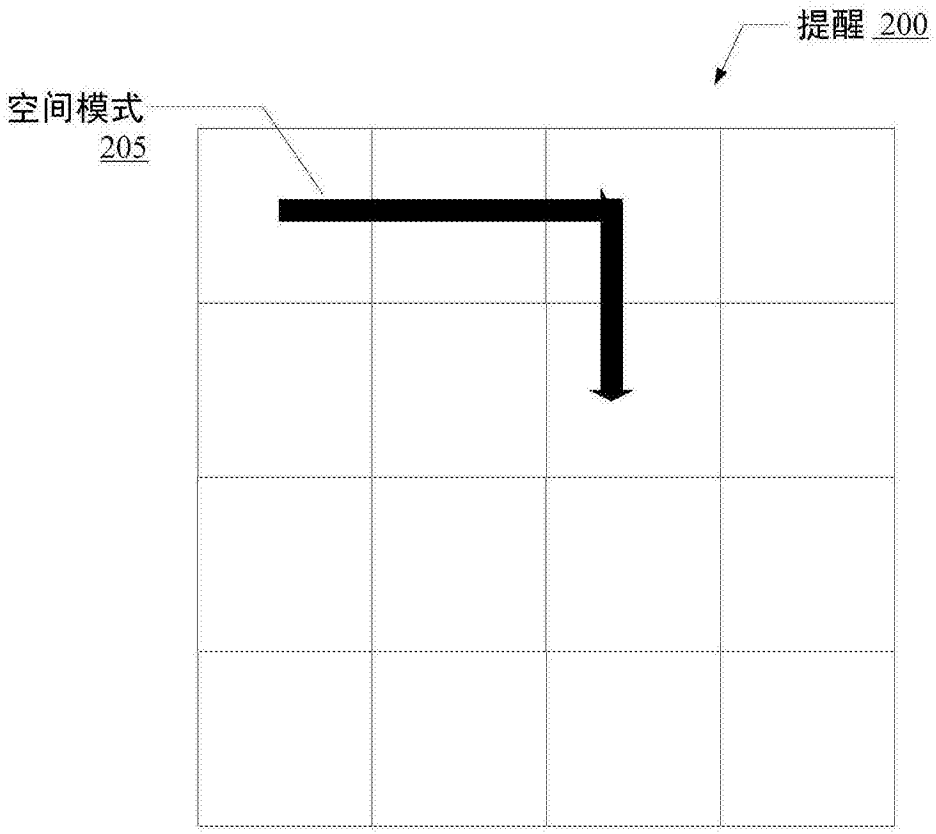
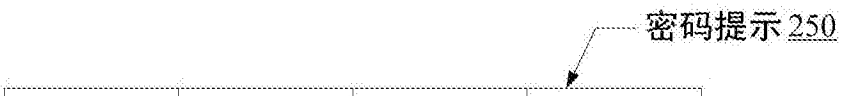


图2a



i8	pB	nj	747
Y!	“>	4u	6
h	k87		,P8
K	hh	56	8&

图2b

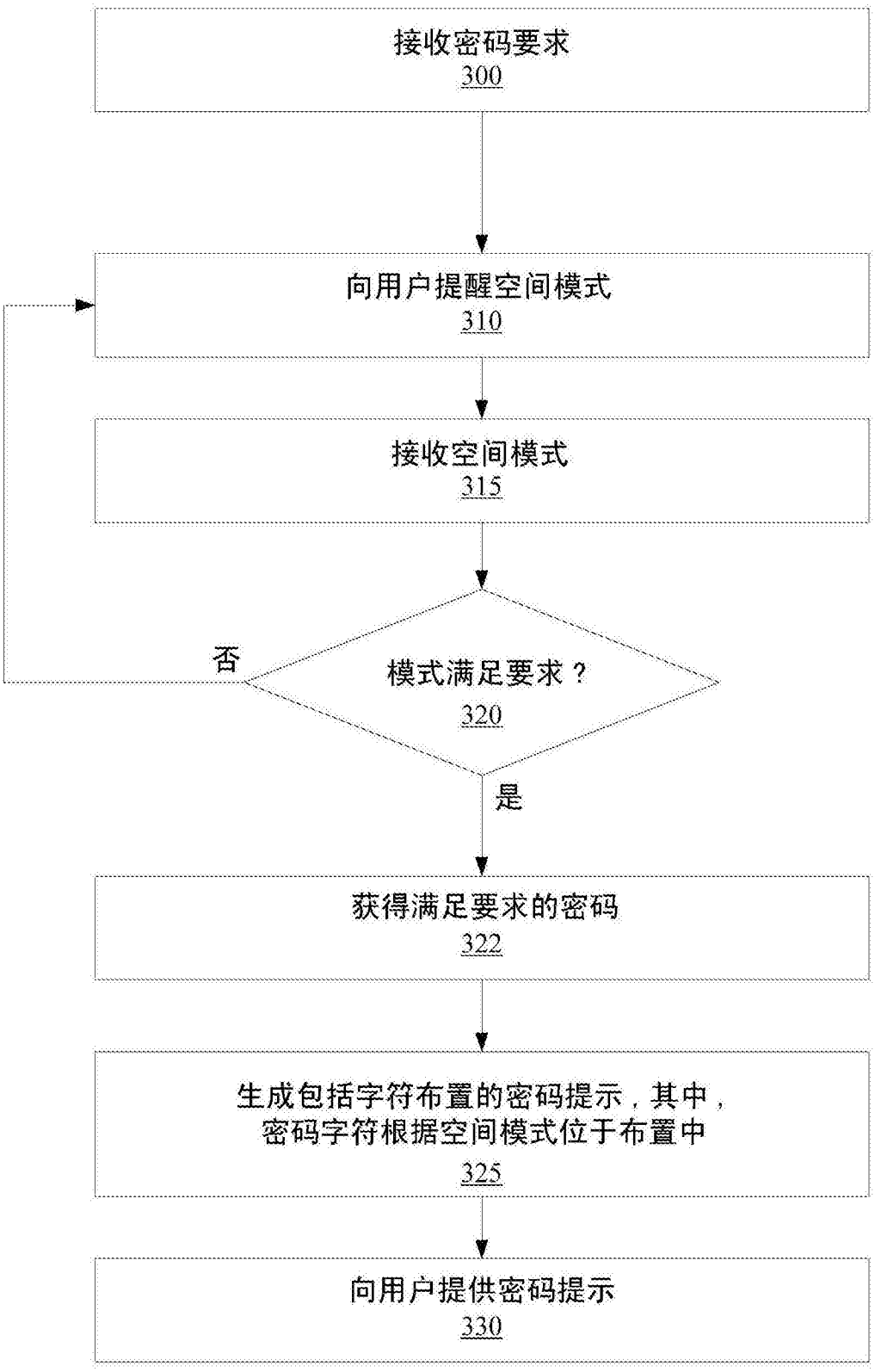

接收密码要求
300
向用户提醒空间模式
310
接收空间模式
315
模式满足要求？
320
否
是
获得满足要求的密码
322
生成包括字符布置的密码提示，其中，
密码字符根据空间模式位于布置中
325
向用户提供密码提示
330

图3

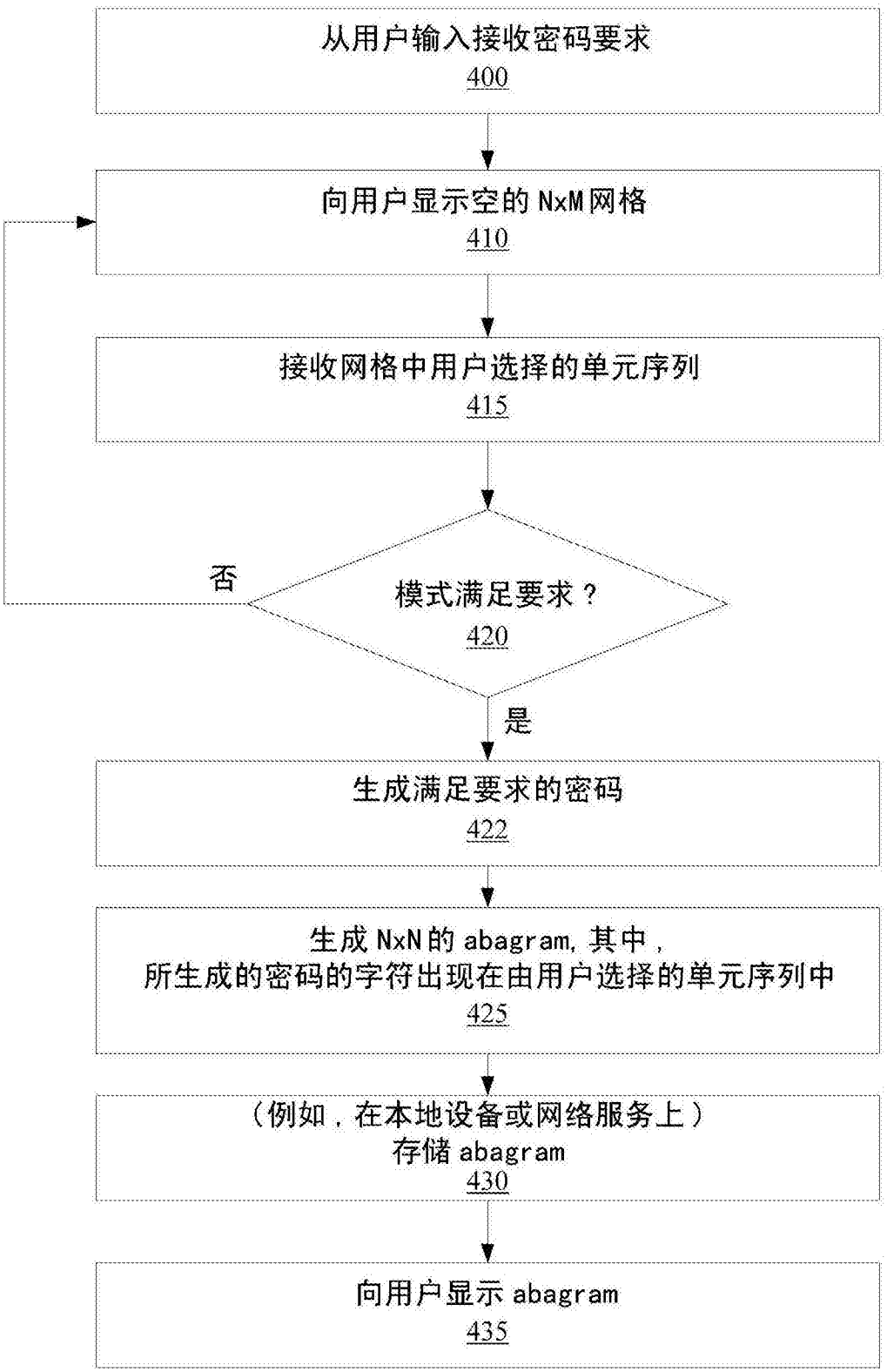

从用户输入接收密码要求
400
向用户显示空的 NxM 网格
410
接收网格中用户选择的单元序列
415
模式满足要求？
420
否
是
生成满足要求的密码
422
生成 NxN 的 abagram，其中，
所生成的密码的字符出现在由用户选择的单元序列中
425
（例如，在本地设备或网络服务上）
存储 abagram
430
向用户显示 abagram
435

图4

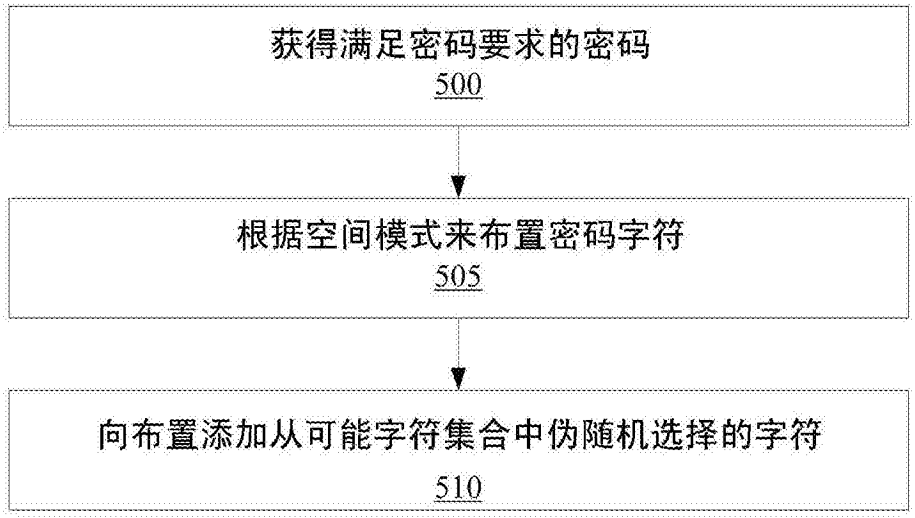

获得满足密码要求的密码
500
根据空间模式来布置密码字符
505
向布置添加从可能字符集合中伪随机选择的字符
510

图5A

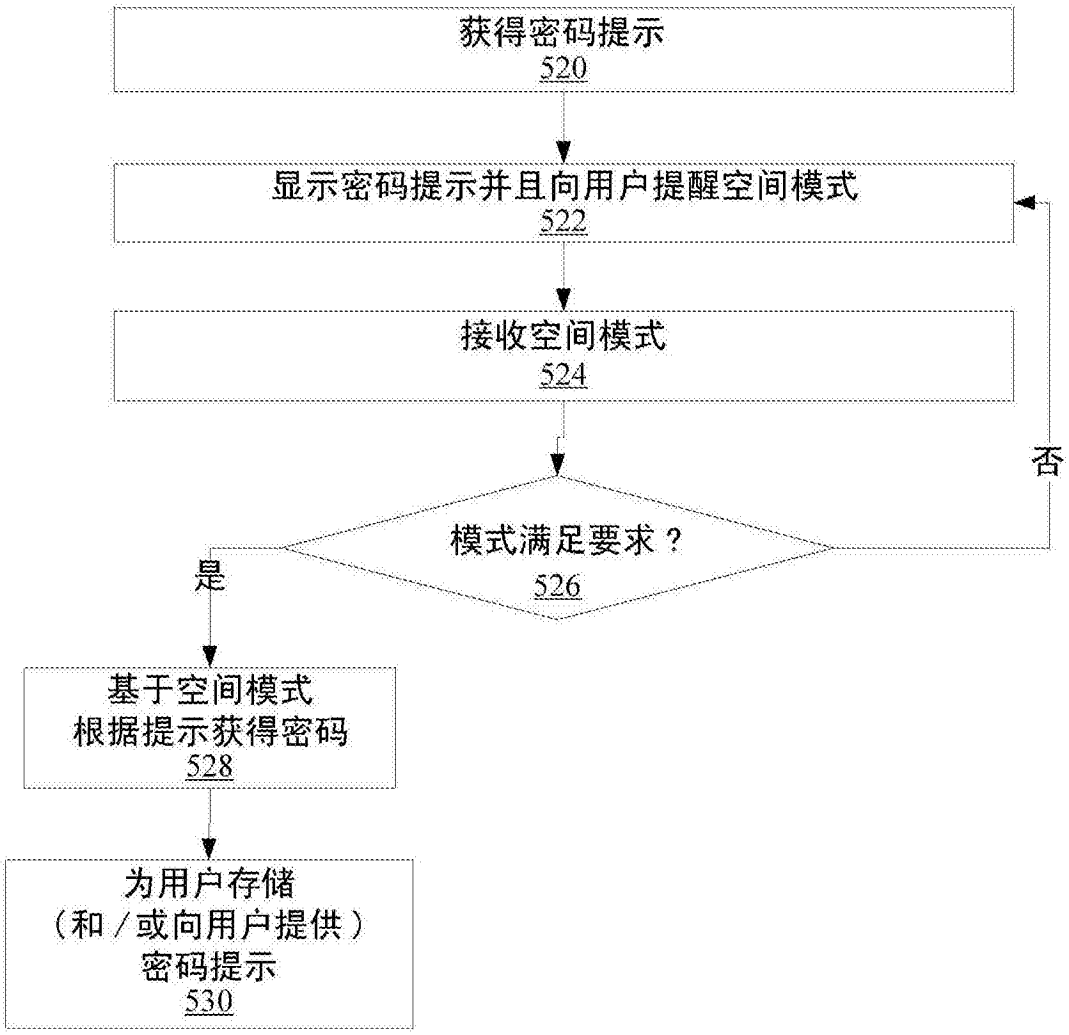

获得密码提示
520
显示密码提示并且向用户提醒空间模式
522
接收空间模式
524
模式满足要求？
526
否
是
基于空间模式
根据提示获得密码
528
为用户存储
（和／或向用户提供）
密码提示
530

图5B

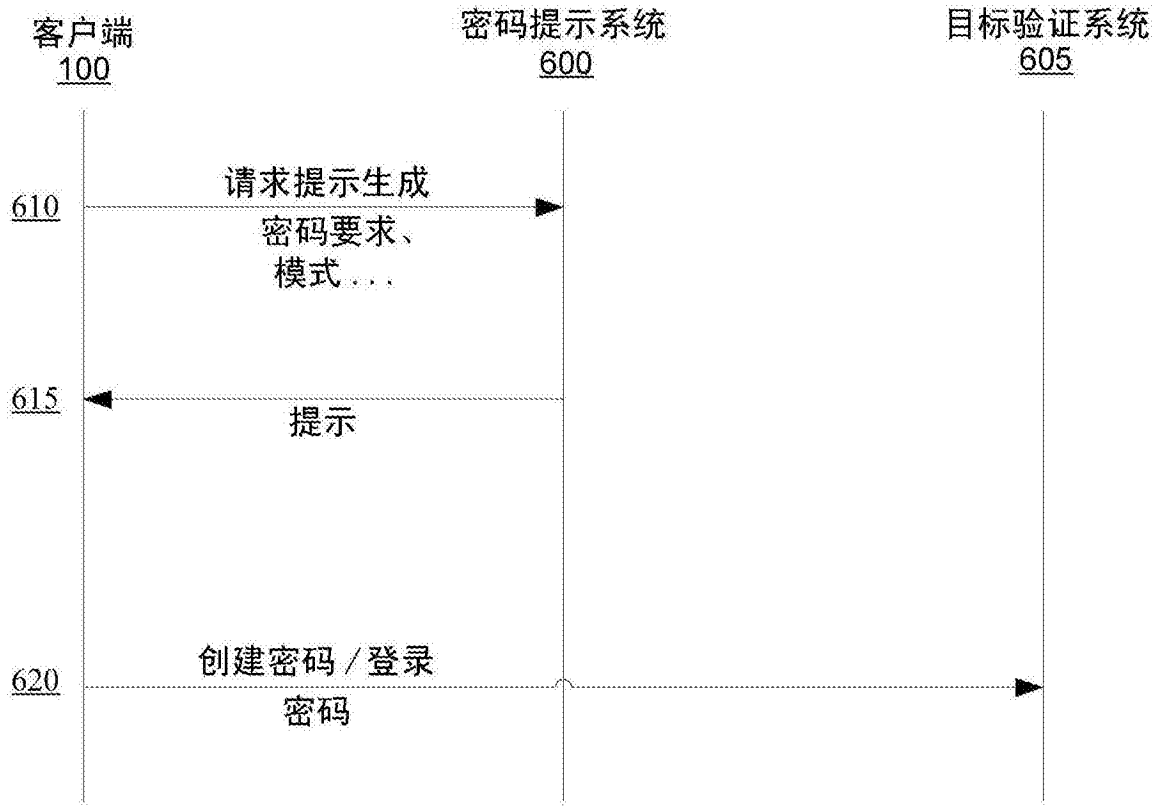

客户端
100
密码提示系统
600
目标验证系统
605
610
请求提示生成
密码要求、
模式 . . .
615
提示
620
创建密码 / 登录
密码

图6a

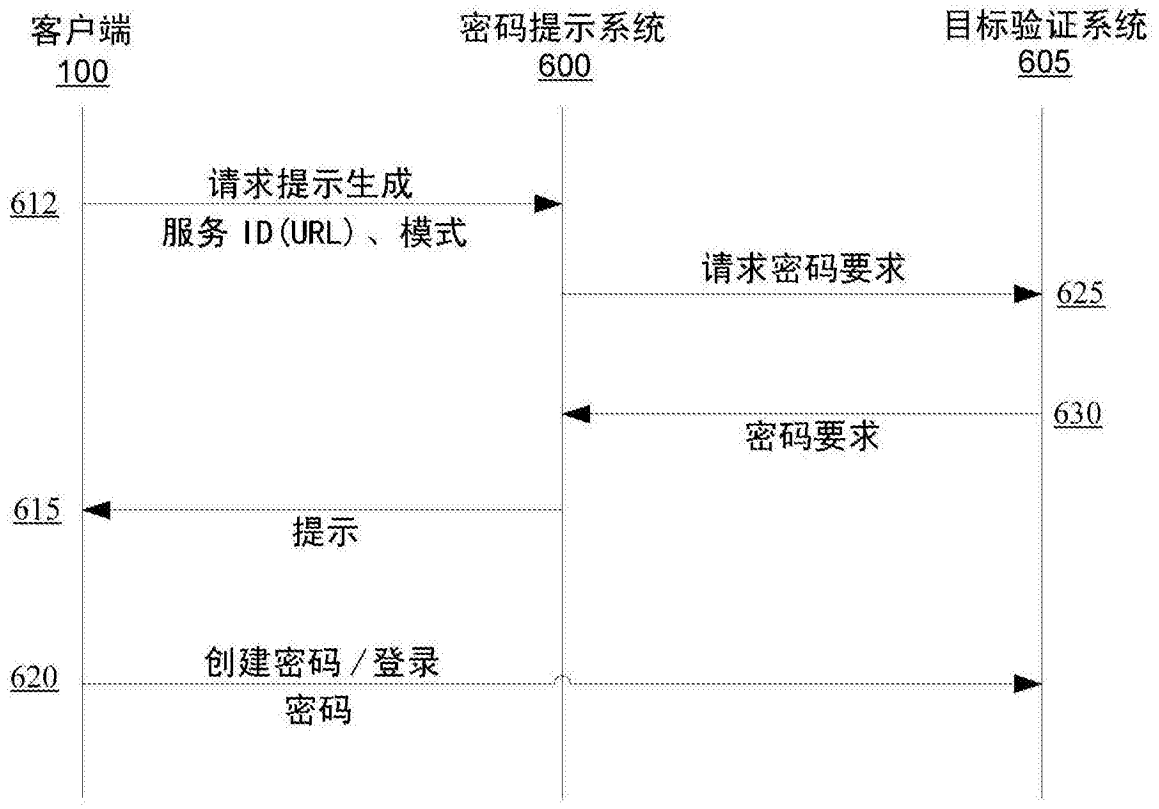

客户端
100
密码提示系统
600
目标验证系统
605
612
请求提示生成
服务 ID(URL)、模式
请求密码要求
625
630
密码要求
615
提示
620
创建密码/登录
密码

图6b

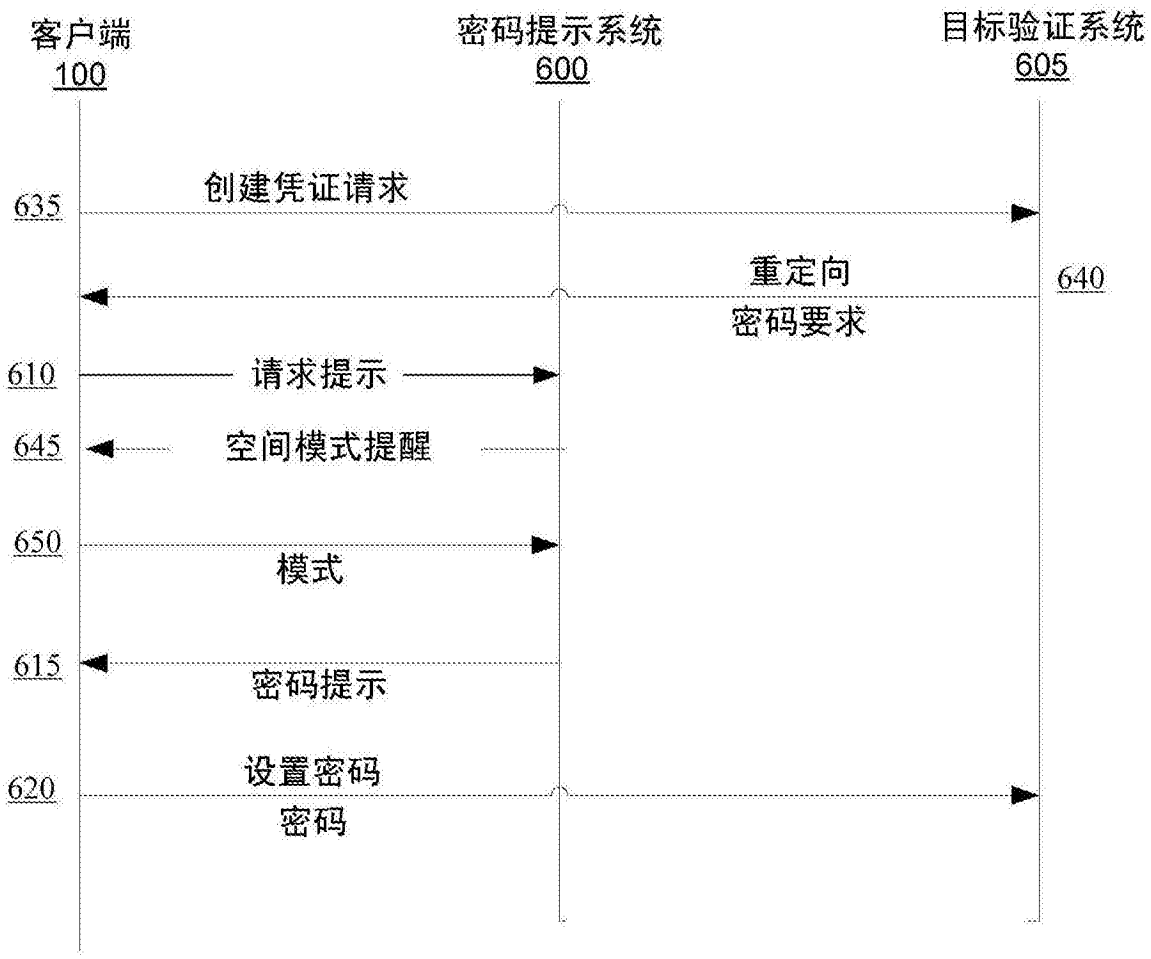

客户端
100
密码提示系统
600
目标验证系统
605
635
创建凭证请求
重定向
密码要求
640
610
请求提示
645
空间模式提醒
650
模式
615
密码提示
620
设置密码
密码

图6c


密码提示系统 700
接口模块
705
密码要求取回器
710
密码获得模块
715
空间模式取回器
720
密码提示生成器
725
提示存储服务
730
提示取回服务
735

图7

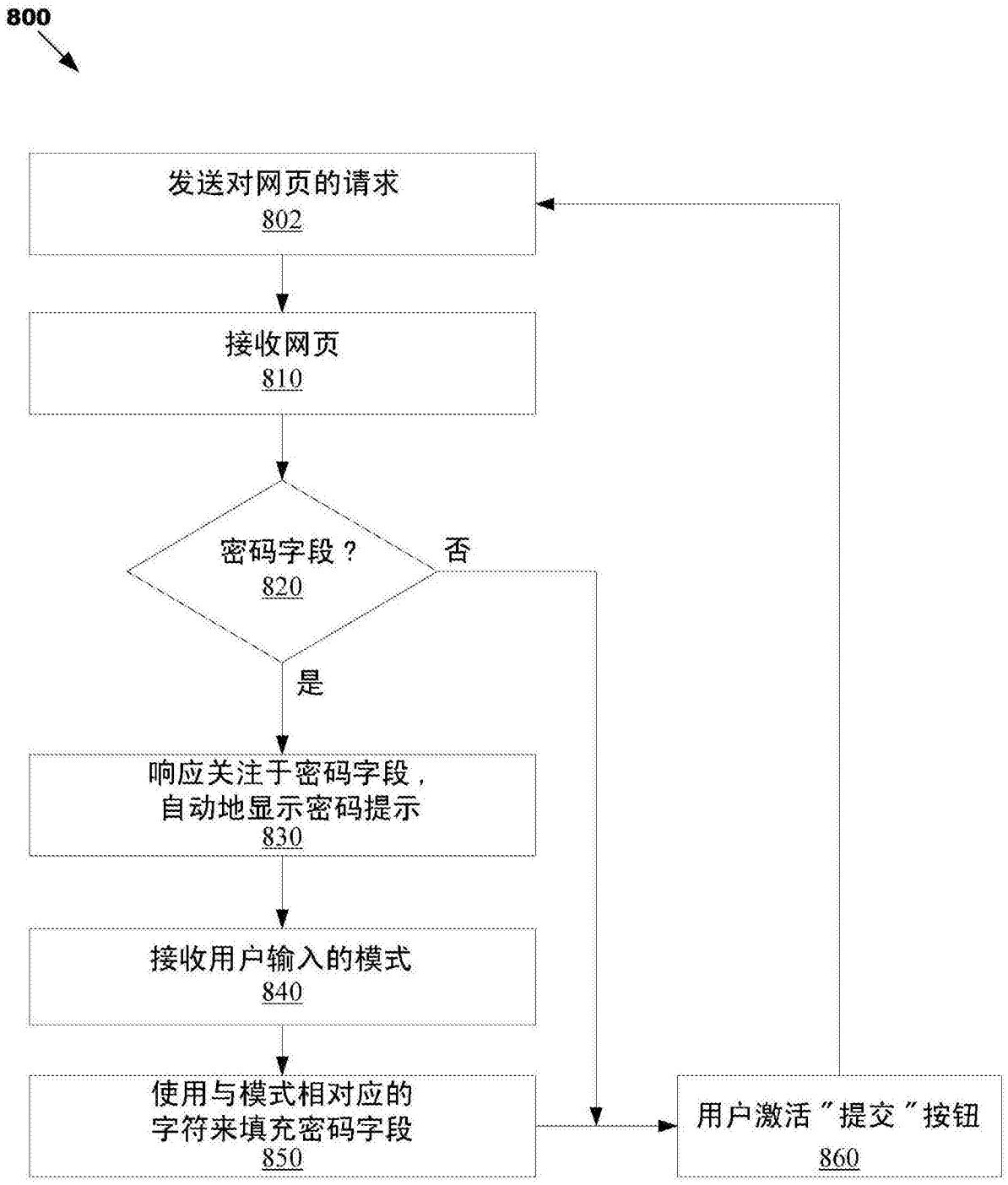

800
发送对网页的请求
802
接收网页
810
密码字段？
820
否
是
响应关注于密码字段，
自动地显示密码提示
830
接收用户输入的模式
840
使用与模式相对应的
字符来填充密码字段
850
用户激活"提交"按钮
860

图8

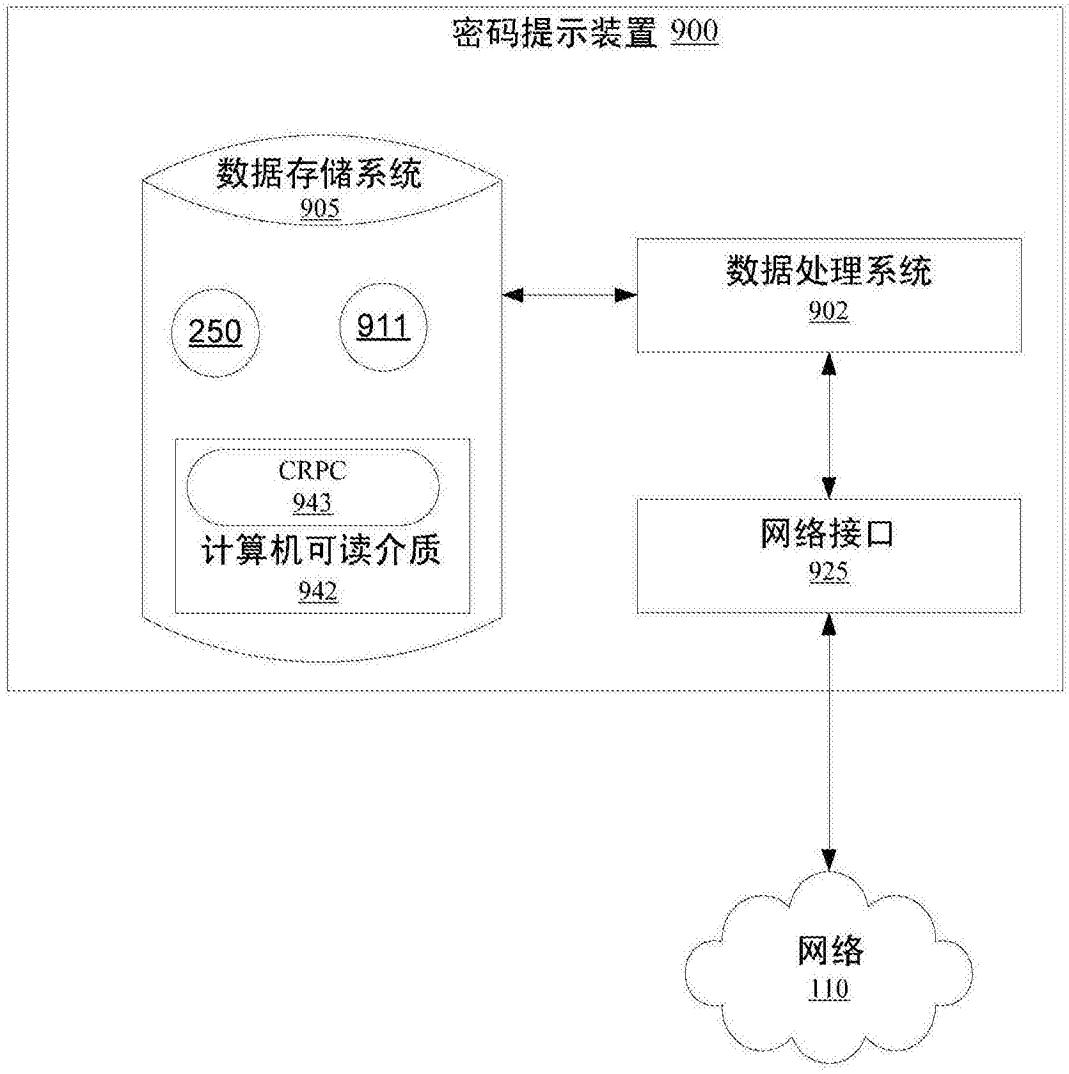

密码提示装置 900
数据存储系统
905
250
911
CRPC
943
计算机可读介质
942
数据处理系统
902
网络接口
925
网络
110

图9


存储介质 943
用于接收密码要求的指令集合
1005
用于获得密码的指令集合
1010
用于向用户提醒空间模式的指令集合
1015
用于接收空间模式的指令集合
1020
用于确定接收的模式是否满足
一个或多个模式要求的指令集合
1025
用于生成密码提示的指令集合
1030
用于向用户提供密码提示的指令集合
1035

图10