(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 103714274 B
(45)授权公告日 2019.03.22

(21)申请号 201310267941.7

(22)申请日 2013.06.28

(65)同一申请的已公布的文献号
申请公布号 CN 103714274 A

(43)申请公布日 2014.04.09

(30)优先权数据
13/630,137 2012.09.28 US

(73)专利权人 阿瓦亚公司
地址 美国新泽西州

(72)发明人 N·奥康纳 D·基瑞
T·麦科玛克

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李晓芳

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/57(2013.01)

(56)对比文件
CN 101043337 A,2007.09.26,
CN 101043337 A,2007.09.26,
US 7552467 B2,2009.06.23,
WO 2011/117666 A1,2011.09.29,
CN 101427268 A,2009.05.06,
US 2006/0206709 A1,2006.09.14,

审查员 石蒙蒙

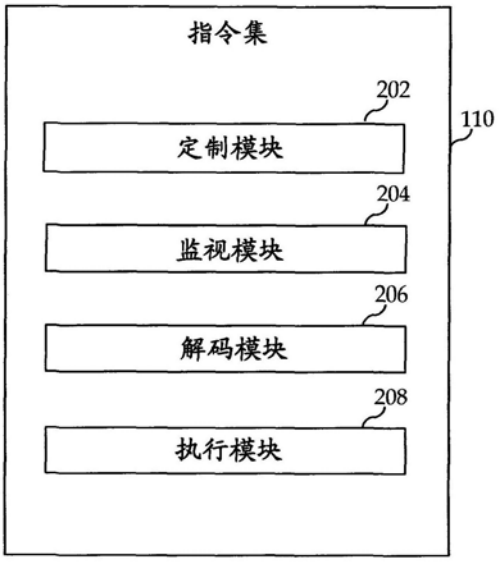
权利要求书3页 说明书12页 附图5页

(54)发明名称

用于增强自助服务安全应用的系统和方法

(57)摘要

本发明涉及用于增强自助服务安全应用的系统和方法。本发明的实施例可以使得电子设备的用户能够在电子设备之内设置可以用作阻止非法的或未经授权的用户的访问的验证平台的基于游戏的环境。通信设备可以包括显示器屏幕、处理器和耦接到处理器的存储器。存储器可以包括数据库和指令集。数据库可以存储可被用于验证过程的预定义的访问模式。此外,指令集可以包括处理器可执行的指令以监视由新用户在基于游戏的环境中做出的输入。此外,处理器可执行的指令可以将新用户的输入与预定义的访问模式匹配以检查新用户的验证。



CN 103714274 B

1.一种用于使得用户能够在电子设备上设置用于限制未经授权的访问的交互式验证环境的验证系统，该验证系统包括：

定制模块，被配置为使得用户能够在电子设备上定制并且设置交互式验证环境；

一个或多个输入装置，用于使得用户能够与交互式验证环境交互以定义多个访问模式，其中，所述多个访问模式中的第一访问模式需要被模拟以对用户进行验证以便得到对应用的访问，并且，在用户被成功验证并由此得到对应用的访问之后，所述多个访问模式中的第二访问模式需要被模拟以对用户进行验证以便进一步得到对所述应用的特征的访问；以及

数据库，存储定义的访问模式。

2.如权利要求1所述的系统，其中该交互式验证环境是基于游戏的环境。

3.如权利要求1所述的系统，其中该交互式验证环境是三维虚拟环境。

4.如权利要求3所述的系统，其中该三维虚拟环境是可导航的虚拟环境。

5.如权利要求1所述的系统，其中该交互式验证环境包括前景、背景和可移动的对象。

6.如权利要求1所述的系统，其中该电子设备能够使得用户能够在得到验证之后经由网络连接到服务。

7.如权利要求6所述的系统，其中该电子设备能够使得用户能够经由IVR系统连接到服务。

8.如权利要求7所述的系统，其中该电子设备能够使得用户能够从IVR系统转移到协助服务系统。

9.如权利要求1所述的系统，其中该输入装置包括电子设备的触敏屏幕。

10.一种用于使得用户能够在电子设备上与交互式验证环境交互以提供用于对用户进行验证以便得到对电子设备的访问的第一输入模式、和在用户被成功验证并由此得到对电子设备的访问之后提供用于对用户进行验证以便进一步得到对存储在所述电子设备中的数据和应用的访问的第二输入模式的验证系统，该验证系统包括：

一个或多个输入装置，使得用户能够通过提供输入序列与交互式验证环境交互；

监视模块，被配置为从由用户向交互式验证环境给出的输入序列监视所述第二输入模式；

解码模块，被配置为通过将所述第二输入模式与一个或多个预定义的访问模式匹配来解码所述第二输入模式中隐藏的指令；和

执行模块，被配置为执行经解码的从用户接收到的所述第二输入模式中隐藏的指令。

11.如权利要求10所述的系统，其中该交互式验证环境是基于游戏的环境。

12.如权利要求10所述的系统，其中该交互式验证环境是三维虚拟环境。

13.如权利要求12所述的系统，其中该三维虚拟环境是可导航的虚拟环境。

14.如权利要求10所述的系统，其中该交互式验证环境包括前景、背景和可移动的对象。

15.如权利要求10所述的系统，其中该电子设备能够使得用户能够在得到验证之后经由网络连接到服务。

16.如权利要求10所述的系统，其中该输入装置包括电子设备的触敏屏幕。

17.一种在电子设备上布置交互式验证环境作为安全性应用的方法，所述安全性应用

用于使得仅仅合法用户能够得到对电子设备的访问并且在得到对电子设备的访问之后进一步得到对存储在所述电子设备中或企业数据库中的数据或应用的访问，所述方法包括：

使得用户能够通过提供第一输入模式与交互式验证环境交互来对用户进行验证以便得到对电子设备的访问，其中，在所述第一输入模式与预定义的访问模式成功匹配后，用户被成功验证并由此得到对所述电子设备的访问；以及

使得用户能够通过提供第二输入模式进一步与交互式验证环境交互来对用户进行验证以便进一步得到对存储在所述电子设备中或企业数据库中的数据或应用的访问，其中，在所述第二输入模式与另一个预定义的访问模式成功匹配后，用户被成功验证并由此得到对存储在所述电子设备中或企业数据库中的数据或应用的访问，

其中所述交互式验证环境是三维虚拟环境。

18.如权利要求17所述的方法，其中使得用户能够与交互式验证环境交互包括：使得用户能够经由电子设备的触敏屏幕与交互式验证环境交互。

19.如权利要求17所述的方法，其中布置交互式验证环境包括在电子设备处定制和安装交互式验证环境。

20.如权利要求19所述的方法，其中安装交互式验证环境包括将交互式验证环境连接到触发事件。

21.如权利要求17所述的方法，其中与从用户接收到的、用于得到对电子设备的访问的所述第一输入模式相比，用于得到对存储在所述电子设备中或企业数据库中的数据或应用的访问的所述第二输入模式具有更少数目的输入。

22.如权利要求17所述的方法，其中存储在电子设备中的应用使得用户能够经由网络连接到一个或多个服务供应商以访问企业系统。

23.如权利要求20所述的方法，其中该触发事件包括与企业的IVR系统对接以访问用户的企业数据。

24.如权利要求23所述的方法，其中在访问IVR系统之后，在第二触发事件之后，将用户转移到企业的协助服务系统。

25.如权利要求24所述的方法，其中该转移步骤包括在协助服务系统内预先使匹配用户的协助需要或状态的代理合格。

26.一种用于使得用户能够在电子设备上设置用于限制未经授权的访问的交互式验证环境的方法，该方法包括：

使得用户能够在电子设备上定制并且设置交互式验证环境，其中所述交互式验证环境是三维虚拟环境；

使得用户能够与交互式验证环境交互以定义多个访问模式，其中，所述多个访问模式中的第一访问模式需要被模拟以对用户进行验证以便得到对所述电子设备的访问，并且，在用户被成功验证并由此得到对所述电子设备的访问之后，所述多个访问模式中的第二访问模式需要被模拟以对用户进行验证以便进一步得到对存储在所述电子设备或与所述电子设备的用户相关联的服务帐户中的数据和应用的访问；以及

将用户定义的访问模式存储在数据库中。

27.如权利要求26所述的方法，其中该交互式验证环境是基于游戏的环境。

28.如权利要求26所述的方法，其中该三维虚拟环境是可导航的虚拟环境。

29.如权利要求26所述的方法，其中该交互式验证环境包括前景、背景和可移动的对象。

30.如权利要求26所述的方法，其中该电子设备能够使得用户能够在得到验证之后经由网络连接到服务。

31.如权利要求30所述的方法，其中该电子设备能够使得用户能够经由IVR系统连接到服务。

32.如权利要求31所述的方法，其中该电子设备能够使得用户能够从IVR系统转移到协助服务系统。

33.如权利要求26所述的方法，其中使得用户能够与交互式验证环境交互包括：使得用户能够经由电子设备的触敏屏幕与交互式验证环境交互。

34.一种电子设备，包括如权利要求1-16中的任何一项所述的系统。

用于增强自助服务安全应用的系统和方法

技术领域

[0001] 本发明的实施例涉及自助服务安全应用。更具体地，本发明的实施例涉及用于经由交互式验证应用创建并随后验证用户的身份的系统和方法。

背景技术

[0002] 一般地，企业具有防止未经授权的使用所需的数据或设备。因此，企业通过使用多级安全系统来保护这样的数据和设备。这样的安全系统的目的是使得任何入侵者不可能访问被保护的数据或设备。但是，这样的安全系统无意间使得合法用户更难以访问被保护的数据或服务。

[0003] 此外，在大多数在线安全系统中，被保护的数据通过传统的用户名和口令保护技术来保证。用户名和口令可以包括数字、字母数字、以及某些特殊字符。基于需要的安全级别，需要增加口令的长度以便使得任何入侵者极其难以预测这样的口令。这样的技术已经证明在对非法用户的保护方面是有效的。但是，这样的技术也使得合法的客户更难以记住这样的口令。

[0004] 此外，在需要高度保护的在线系统的情况下，以多个级别实现口令保护。例如，银行可能需要一次口令来登入在线银行帐户并且可能需要二次口令来进行交易。此外，某些银行帐户甚至需要由银行生成并发送到用户的移动设备银行第三口令。因此，这样的银行的用户一定要记住这样的口令并且在任何交易期间一定要使得他们的移动设备靠近他们。这对于某些用户来说可能是忙乱的和繁重的。此外，对于许多用户来说，可能难以记住与一个服务相关联的长的和多个口令。

[0005] 另一个已知的验证系统是生物统计学验证系统。这些生物统计学系统需要用户使用他们的指纹、眼睛视网膜、脸部结构或语音装置来验证自身是合法用户。但是，这样的验证系统实现起来是昂贵的并且需要高的维护来进行正确的功能。此外，这些验证系统可能被专业入侵者欺骗。

[0006] 另外，所有前述安全或验证系统由它们的相关企业布置。有时，企业开发这样的复杂的安全系统，它们需要训练它们的用户以能够与这样的安全系统交互。因此，不愿意面对这样的访问它们自己的财产的困难的许多人通常使用可能被容易突破的低级别的安全系统，因此将他们自己暴露于不必要的风险之下。

[0007] 因此，需要改进安全系统以使得安全系统足够难被突破，并且同时足够简单以能够被合法用户访问。此外，需要使得安全系统更直观和用户友好。

发明内容

[0008] 根据本发明的实施例提供一种用于使得用户能够在电子设备上设置用于限制未经授权的访问的交互式验证环境的验证系统。此外，该系统可以包括被配置为使得用户能够在电子设备上定制并且设置交互式验证环境以访问服务的定制模块。此外，该系统可以包括一个或多个输入装置，用于使得用户能够与交互式验证环境交互以定义为了得到验证

并且得到对存储在用户的设备或服务帐户中的数据和应用的验证后访问而需要被模拟的一个或多个访问模式。另外，该系统可以包括数据库，用于存储定义的访问模式。

[0009] 优选地，该交互式验证环境是基于游戏的环境。

[0010] 优选地，该交互式验证环境是三维虚拟环境。

[0011] 优选地，该三维虚拟环境是可导航的虚拟环境。

[0012] 优选地，该交互式验证环境包括前景、背景和可移动的对象。

[0013] 优选地，该输入装置包括电子设备的触敏屏幕。

[0014] 在本发明的另一个实施例中，提供一种用于使得用户能够与交互式验证环境交互以用于验证和用于得到对存储在用户的设备或服务帐户中的数据和应用的验证后访问的验证系统。此外，该系统可以包括一个或多个输入装置，使得用户能够通过提供输入序列与交互式验证环境交互。此外，该系统可以包括监视模块，被配置为从由用户向交互式验证环境给出的输入序列监视输入模式。此外，该系统可以包括解码模块，被配置为通过将输入模式与一个或多个预定义的访问模式匹配来解码输入模式中隐藏的指令。另外，该系统可以包括执行模块，被配置为执行从用户接收到的输入模式中隐藏的指令。

[0015] 优选地，电子设备可以使得用户能够在得到验证之后经由网络与服务连接。

[0016] 在本发明的另一个实施例中，提供一种用于使得用户能够在电子设备上设置用于限制未经授权的访问的交互式验证环境的方法。该方法可以包括使得用户能够在电子设备上定制并且设置交互式验证环境以访问服务。此外，该方法可以包括使得用户能够与交互式验证环境交互以定义为了得到验证并且得到对存储在用户的设备或服务帐户中的数据和应用的验证后访问而需要被模拟的一个或多个访问模式。另外，该方法可以包括将定义的访问模式存储在数据库中。

[0017] 在本发明的另一个实施例中，提供一种在电子设备上布置交互式验证环境作为安全性应用的方法，所述安全性应用用于使得仅仅合法用户能够得到用于访问电子设备的验证并且得到对存储存储在用户的设备或服务帐户中的数据和应用的验证后访问。此外，该方法包括使得用户能够通过提供输入模式与交互式验证环境交互来得到对访问的验证。此外，该方法包括在输入模式与预定义的访问模式成功匹配后，验证用户以得到访问。再一次此外，该方法包括使得用户能够通过提供第二输入模式来进一步与交互式验证环境交互以得到验证后数据访问。另外，该方法包括在第二输入模式与另一个预定义的访问模式成功匹配后，验证用户以得到对数据或应用的访问。

[0018] 优选地，使得用户能够与交互式验证环境交互包括使得用户能够经由电子设备的触敏屏幕与交互式验证环境交互。

[0019] 优选地，布置交互式验证环境包括在电子设备处定制和安装交互式验证环境。

[0020] 优选地，安装交互式验证环境包括将交互式验证环境连接到触发事件。

[0021] 优选地，与从用户接收到的、用于得到用于访问的验证的输入模式相比，用于验证后数据访问的第二输入模式具有更少数目的输入。

[0022] 优选地，存储在电子设备中的应用可以使得用户能够经由网络连接到一个或多个服务提供者以访问企业系统。

[0023] 优选地，该触发事件包括与企业的IVR系统对接以访问用户的企业数据。

[0024] 优选地，在访问IVR系统之后，在第二触发事件之后，将用户转移到企业的协助服

务系统。

[0025] 优选地，该转移步骤包括在帮助服务系统之内预先使匹配用户的帮助需要或状态的代理合格。

[0026] 优选地，第二验证步骤包括：如果用户的状态处于预定级别，则向用户显示某些高价值代理。

[0027] 在本发明的另一个实施例中，提供一种电子设备，包括上述验证系统中的一个。

附图说明

[0028] 本发明的上述和更进一步的特征和优点在考虑以下具体实施方式，特别是结合附图之后将变得明显，其中各个图中类似的附图标记被用于指定类似的组件，其中：

[0029] 图1是根据本发明的实施例的用于支持用户定义用于访问服务的验证的个性化模式的系统的示范性框图；

[0030] 图2是根据本发明的实施例的用于验证用户对系统的访问并且用于验证用户的验证后数据或服务访问请求的指令集的示范性框图；

[0031] 图3示出了其中本发明的各个实施例可以运行的示范性环境；

[0032] 图4是根据本发明的实施例的用于使得用户能够利用交互式语音响应(IVR)系统验证和导航的基于游戏的验证环境的例示；

[0033] 图5是根据本发明的实施例的在电子设备上定制和设置基于游戏的验证应用的方法的流程图；和

[0034] 图6是根据本发明的实施例的通过使用基于游戏的验证模块来验证用户的方法的流程图。

[0035] 这里使用标题仅仅是用于组织目的，而不意味着用于限制说明书或权利要求书的范围。贯穿此申请使用的词“可以”在允许的意义上使用(即，意味着有...的潜能)，而不是在强制的意义上使用(即，意味着必须)。类似地，词“包括”意味着包括但是不限于此。为了便于理解，可能时已经使用类似的参考数字，以指定图中共同的类似的元件。图的可选部分可以使用破折号或虚线示出，除非另外指明了使用背景。

具体实施方式

[0036] 现在将在下文中参考附图更完整地描述本发明的说明性的实施例，其中示出了本发明的某些而不是所有实施例。实际上，本发明可以以许多不同的形式实施，并且不应该被理解为限于这里阐述的实施例；相反地，提供这些实施例以使得此公开将满足可申请的法定要求。

[0037] 图1是根据本发明的实施例的用于支持用户定义用于访问服务帐户的验证的个性化模式的系统102的示范性框图。在实施例中，系统可以被实现为可以安装在任何电子设备中的软件/固件。在另一个实施例中，系统可以被实现为通信设备。通信设备的示例可以包括但是不局限于移动电话、智能电话、个人数字助理(PDA)、平板、个人计算机(PC)、膝上计算机、自动柜员机(ATM)等等。

[0038] 通信设备可以用于通过公共交换电话网(PSTN)、蜂窝网络、因特网、以太网等等进行诸如数据之类的通信和语音通信。在本发明的实施例中，通信设备可以包括操作系统

(OS)，诸如但是不限于Windows、Windows Mobile、Apple iOS、Google Android、Symbian、Linux、Unix、Macintosh等等。在另一个实施例中，通信设备可以是仅仅具有固件指令的基本电子设备。

[0039] 系统102包括处理器104和存储器106。存储器106包括数据库108和指令集110。此外，存储器106可以包括用户接口应用(未示出)，其对用户可以是定制的/个性化的。在实施例中，用户接口应用可以被用户定制。此外，系统102可以利用用户接口应用来验证由用户发起的‘访问请求’(用于访问服务帐户或设备的请求)。在实施例中，访问请求可以由用户发起以便访问设备，或可以用于经由该设备访问服务帐户。此外，在实施例中，经由设备可访问的服务帐户可以是设备的一部分或可以通过网络(局域网或企业宽带网)访问。

[0040] 数据库108可以存储与存储在存储器106中的用户接口应用对应的用户定义的数据。在实施例中，可以在用户接口应用的定制/个性化处理期间生成用户定义的数据并且存储在数据库108中。此外，用户定义的数据可以使得系统102能够在验证处理期间识别用户。此外，在验证处理期间，用户可以向运行在设备上的用户接口应用(实现系统102)提供某些输入。系统102然后可以将从用户接收到的输入与存储在数据库108中的用户定义的数据匹配。基于该匹配，系统102可以允许/不允许对设备的用户的访问和/或对服务帐户的访问。

[0041] 此外，数据库108可以包括与系统108的注册用户对应的数据。数据可以包括但是不局限于注册用户的个人详情、专业详情、联系信息和照片。在成功验证之后，数据库可以显示与验证的用户对应的存储的数据。此外，联系信息可以包括联系人的名称、联系人的地址、联系人的电子邮件地址等。

[0042] 如图所示，存储器106包括指令集110。指令集110进一步结合在本发明的图2中描述的实施例详细地说明。广泛地，指令集110可以包括可以由处理器104执行来处理/执行可以从系统102的用户接收到的各种输入的一个或多个指令。从用户接收到的输入可以包括某些模式。模式的目的可以是识别用户。每个模式可以被用户向系统102预先注册并且可以被存储在数据库108中作为用户定义的数据(如前面图1中所述的)。用户输入的模式可以在验证过程中支持用户，其可以允许用户访问系统或由系统102提供的服务帐户或经由网络访问企业系统。此外，用户的随后模式输入可以使得用户能够得到从系统102或企业服务帐户的验证后数据访问。

[0043] 此外，指令集110可以包括可由处理器104执行以使得用户能够产生用户接口(如前所述)的指令，用户接口本身可以用作系统中的验证应用。在本发明的实施例中，用户接口或验证应用可以是需要用户输入的交互式应用。在另一个实施例中，验证应用可以是上面具有用户可移动的对象的图像。用户可以以预定义的方式移动对象或将对象放置在图像上以得到对系统提供的数据或服务的访问。在另一实施例中，验证应用可以是基于游戏的应用，其可以由用户玩以向系统提供输入(作为访问模式)用于验证。

[0044] 其后，用户可以将产生的用户接口安装在系统102中的任何安全检查点处。例如，用户需要将自制的安全检查点安装在他的智能电话机中，该自制的安全检查点可以允许用户通过解锁触摸锁或键区锁或通过智能电话机访问他的服务帐户来访问他的智能电话机，然后系统102可以通过提供必需的工具来支持用户，通过该工具，用户可以产生并且将期望类型的验证应用(用户接口应用)安装在期望类型的安全检查点(诸如智能电话机或服务帐户的键区解锁检查点)处。

[0045] 此外，在将验证应用安装在系统102中之后，存储在指令集110中的指令可以使得用户能够定义访问模式(用户定义的模式)，如果在验证应用中输入访问模式，则可以向用户授权访问系统或该系统提供的服务帐户。访问模式可以被系统102存储在数据库108中。在实施例中，用户可以定义多个访问模式，这些访问模式可以被(用户)使用以验证用户的访问请求或者可以被用作用户的验证后数据访问请求。

[0046] 例如，用户可以具有存储在他的智能电话机中的私人数据，从而可能不愿意允许任何其他人得以访问智能电话机以及得以访问保密数据。因此，用户可以产生期望的验证应用，其可以阻止除了该用户以外的任何人访问智能电话机和存储在它中的私人数据。此外，用户可以在系统中存储访问模式，其可以被提供作为向产生的验证应用的输入。在验证期间，用户可以向安装在系统中的验证应用输入访问模式。系统然后可以将输入模式与存储的访问模式匹配。如果模式匹配，则用户可以获得对设备的访问，否则对设备的访问可以被系统拒绝。

[0047] 此外，在得到对系统的访问之后，用户可以需要向存储在系统102中的验证应用提供另一个输入以得到对存储在系统中的特定数据的访问或得到对系统提供的服务帐户的访问。在实施例中，系统提供的服务帐户可以需要到因特网或内部网的连接。因此，存储在指令集110中的指令可以支持用户预先定义另一个访问模式集，其可以使得用户能够利用系统102提供的验证后服务。

[0048] 例如，在用户成功验证系统之后，用户可以将另一个模式输入到验证应用。系统可以再一次将输入模式与存储的模式匹配。如果输入的模式与存储的模式中的任何一个匹配，则系统可以向用户提供对应的数据或服务。否则，系统可以宣布用户是未被验证的用户或可以允许用户尝试另一个模式集。在实施例中，存储在系统102处的每个模式可以为用户调用系统的不同功能。例如，存储的每个模式可以提供不同的访问级。用户可以将得到访问和访问级所需的那么多的模式预存储到系统102提供的特定数据集或服务帐户。

[0049] 此外，存储在指令集110中的指令的功能详细地通过将存储在指令集110中的各种指令划分成例如某些数目的模块来在本发明的图2中说明。本领域技术人员可以理解，在本发明的图2中定义的模块(和它们的对应功能)的数目不意欲限制本发明的范围。本发明可以通过使用任何数目的模块、其组合或通过完全不使用模块来实现。用在图2中的模块仅仅用于说明本发明的实施例。另外，本领域技术人员可以理解，上面在图1中定义的功能也不意欲作为本发明的限制性的方面；相反地，上面定义的功能意欲更好地说明本发明的范围。此外，上面在图1中使用的示例仅仅用于更好地说明本发明的实施例并且用于满足专利申请的法定要求。

[0050] 图2是根据本发明的实施例的用于验证用户对系统(诸如系统102)的访问和用于验证用户的验证后数据或服务访问请求的指令集(诸如指令集110)的示范性框图。指令集110可以包括用于处理由用户提供的输入以验证用户并且验证用户做出的访问系统102提供的数据或服务的请求的各个模块。

[0051] 如图所示，指令集110包括定制模块202、监视模块204、解码模块206和执行模块208。在实施例中，定制模块202可以使得用户能够导入期望的基于游戏的环境以用于定制。基于游戏的环境可以被用户使用作为验证的媒介。定制模块202可以使得用户能够设置基于游戏的环境作为可以被实现为系统102的任何电子设备中的验证应用。

[0052] 在实施例中，用户可以从任何第三方资源导入基于游戏的环境。在另一个实施例中，定制模块202可以使得用户能够产生期望的基于游戏的环境。此外，基于游戏的环境可以指代需要用户的输入以执行某些功能的任何交互式应用。交互式应用可以是音频或图形或二者的结合。

[0053] 此外，在本发明的示范性实施例中，用户可以创建基于游戏的环境作为用户可以熟悉的虚拟环境。创建用户熟悉的环境的目的是通过向系统的验证过程添加高度的个性化(用户熟悉的环境)来增强系统的安全性。这也可以减轻用户记住任何种类的口令(诸如文本、声音或图形)，因为在这样的用户熟悉的环境下需要的口令将是用户在熟悉的环境中的直观动作。

[0054] 此外，在基于游戏的环境的定制处理期间，用户可以在环境中定义和记录一个或多个活动序列(访问模式)，并且可以在每个用户定义的活动序列的完成之后分配要被系统执行的唯一的功能。因此，系统可以在预先定义的活动序列中的任何一个(由用户存储在系统之内)的完成之后执行分配的活动。另外，定制模块202可以使得用户能够将定制的环境安装/实施在用户想要用户想要防止其他用户或入侵者的任何数据或服务上。

[0055] 例如，如果用户具有安装在他的智能电话机中的因特网银行软件应用并且用户需要保护该应用不被任何未被授权的人使用，则用户可以从第三方源导入基于验证游戏的环境或者可以在智能电话机本身中创建基于验证游戏的环境。基于验证游戏的环境可以包括例如海滨胜地，而没有文本或数字显示在它上。环境可以简单地是可3D导航的世界。

[0056] 此外，在3D世界的定制期间，用户可以通过导航(在虚拟3D世界中)至他最喜爱的海滨别墅，然后访问海滨别墅附近的第三直升机，然后向右转向冰淇淋站，然后通过访问位于码头(附近的)中的红色船完成输入序列，来在3D世界中提供并且记录输入序列。

[0057] 此访问模式可以由用户分配作为在访问安装在智能电话机中的因特网银行软件应用时的验证措施。因此，可以向尝试访问因特网银行应用的任何人闪现前述3D环境以用于验证(通过重复存储的输入模式)。

[0058] 另外，在存储第一输入模式作为应用验证措施之后，用户可以存储进一步坐在红色船中以驱动船通过弯曲的海滩直至他的海角的另一个输入模式。此外，用户可以将此活动作为指令分配给智能电话机以经由文本消息发送(相关银行的)帐户结余(account balance)。类似地，用户可以产生另一个输入模式，在该输入模式中，用户将红色船从码头驱动到灯塔。用户可以将此活动作为指令分配给智能电话机以经由文本消息发送帐户小型声明或可以经由声音输出。这样，用户定制了基于游戏的环境以充当访问因特网银行应用的验证措施。

[0059] 另外，用户定制了基于游戏的环境以充当访问因特网银行应用的各种特征的验证后手段。在实施例中，前述定制处理全部可以由指令集110的定制模块202执行。

[0060] 此外，只有当用户已经通过访问受保护的服务或数据触发了基于游戏的环境(其被实现为访问服务或数据时的验证措施)时，监视模块204才可以工作。在初始化作为验证检查应用的基于游戏的环境之后，监视模块可以开始与基于游戏的环境通信。此外，基于游戏的环境可以跟踪所有输入装置，用户可以通过输入装置向系统提供输入。

[0061] 监视模块从而可以监视基于游戏的环境的状态和用户提供的输入。这可以使得监视模块能够监视用户在基于游戏的环境中执行的活动。在实施例中，用户可以在基于游戏

的环境中执行活动以验证他的/她的身份作为受保护的数据或服务的真正的用户。因此，监视模块204可以监视用户的这样的活动并且可以将记录的数据传递到解码模块206。

[0062] 解码模块206可以解码从监视模块206接收到的监视的数据。在实施例中，解码过程可以包括将从用户接收到的输入(用于在基于游戏的环境中执行活动)解释为由用户给出的指令(隐藏在输入模式中)以验证他的/她的身份或者识别用户给出的指令以执行验证后活动。在实施例中，解码模块206可以通过比较从用户接收到的输入模式与预存储的访问模式比较来执行这样的识别。

[0063] 在实施例中，解码模块可以被配置为通过匹配输入模式与存储在数据库108中的一个或多个预定义的访问模式来解码隐藏在从用户接收到的输入模式中的指令。此外，在实施例中，解码模块206可以被配置为提供比较输入和访问模式方面的某些灵活性。这可以通过将人为误差的范围保持至某一可调节的级别来便利用户。可调节的级别可以由用户在基于游戏的应用的定制处理期间定义。

[0064] 此外，解码模块206可以仅仅由监视模块204激活。因此，监视模块204可以激活解码模块206以解码从用户接收到的输入模式。解码模块206然后可以解码从用户接收到的输入模式以识别用户是否已经提供了与任何预存储的访问模式相似的任何输入模式。在一种情况下，如果解码模块206将任何输入模式解释为访问模式，然后解码模块206可以激活执行模块208以接收解码的指令。

[0065] 执行模块208然后可以分析用户给出的指令是否有效(基于解码的指令)。例如，如果用户已经访问存储在智能电话机中的受保护的因特网银行应用并且已经给出被分配为验证后指令的输入模式，则执行模块208可以不执行解码的指令，因为用户需要首先验证他的/她的身份，然后仅仅该用户可以被使能来提供指令以利用因特网银行应用执行进一步的活动。

[0066] 因此，如果执行模块208分析解码的指令用于验证，则执行模块可以执行解码的指令以用于验证以执行将用户验证为有效的用户所需的任务。其后，执行模块可以等待解码模块提供解码的指令以执行验证后活动，从而执行模块可以执行验证后指令(如果从解码模块接收到)以服务用户。

[0067] 例如，如果新用户已经触发了存储在移动设备中的因特网银行应用，则可以向用户闪现基于游戏的验证环境。其后，监视模块204可以被激活以监视用户的活动。用户然后可以通过从他/她最喜爱的海滨别墅开始以访问第三直升机、然后向右转到冰淇淋站然后在码头中的红色船处完成，来在基于游戏的环境中导航(如在前述示例中所述)。

[0068] 此活动可以由监视模块204监视，并且可以将对应信息传递到解码模块206。解码模块206可以解码该信息以确认用户执行的活动是否与存储在系统102的数据库108中的访问模式中的一个相似。其后，解码模块206可以通知执行模块208执行分配(由用户在定制处理期间预分配)给存储在数据库中的匹配的访问模式的活动。执行模块然后可以确定匹配的访问模式用于验证目的，从而可以开始用户的验证处理。其后，如果用户将红色船驱动到灯塔，则监视模块204可以再一次将信息传递给解码模块206。解码模块可以将活动解释为预存储的类似的活动，然后可以指示执行模块208执行相关的分配的活动，并且执行模块208然后可以将SMS的小型声明发送到用户。

[0069] 图3示出了其中本发明的各个实施例可以运行的示范性环境300。如图所示，用户

的用户设备302经由网络306与服务提供者304通信。通信设备的示例包括但是不局限于移动电话、智能电话、个人数字助理(PDA)、平板、个人计算机(PC)、自动柜员机(ATM)等等。此外，网络306可以包括但是不局限于诸如因特网、PSTN、局域网(LAN)、广域网(WAN)、城域网(MAN)等等之类的通信网络。在实施例中，网络106可以是诸如因特网之类的数据网络。

[0070] 此外，用户设备302可以包括用于向用户设备302提供对未被授权的访问的安全性的诸如系统102之类的系统。系统102可以便利用户设备302的用户通过网络306与服务提供者304通信。此外，在服务器102和用户设备302之间交换的消息可以包括能够传送服务提供者304向用户设备302提供期望的服务所需的信息的任何合适的消息格式和协议。

[0071] 在实施例中，服务提供者可以是用户设备302的用户具有储蓄帐户的银行。此外，用户设备302的用户可以将软件应用安装在用户设备302中，用户经由该软件应用可以访问来执行金钱交易。因此，可以需要用户保护软件应用的任何未经授权的使用。用户可以设置可能难以记住的用于访问软件应用的传统的用户名和口令，或者可以使用系统102安装基于游戏的环境作为用户名和口令保护的替换方式。在本发明的实施例中，基于游戏的环境可以由服务提供者304提供作为可以被认为是有效的基于游戏的验证环境的标准的基于游戏的环境。

[0072] 这里，用户可以使用该系统来以期望的方式定制基于游戏的环境并且可以将定制的环境存储在用户设备302中。其后，用户可以定义可以用于验证和验证后服务的某些访问模式。因为基于游戏的验证环境由服务提供者304识别，因此服务提供者可以不实现用于验证用户的任何安全措施，因为用户将由基于游戏的环境本身验证。

[0073] 在实施例中，基于游戏的环境可以包括在背景中的山脉、云和太阳以及在前景中的草地、池塘、动物的3D视图。此外，用户可以存储从前景挑选特定的动物并且将它放置在背景中的特定的山顶上的验证访问模式。此输入(如果由用户给出)可以将用户验证为有效的用户，并且用户设备302可以经由网络306与服务提供者304连接。其后，可以在3D环境中以某些预定义的对象上的标签显示服务提供者可用的选项。

[0074] 例如，如果服务提供者是银行并且用户被验证并且与银行连接，则可以为3D视图添加某些银行选项的标签，诸如结余检查、帐户声明、转帐和移动再充值等。每个标签可以被显示在3D环境中存在的某些对象上。因此，如果结余检查的标签在太阳上，则用户可以需要使用用户设备302的触摸屏在山脉之前拖放太阳以从银行取回结余。此活动可以被预存储为取回结余的验证后活动，因此也可由系统识别。类似地，用户可以通过重复预存储的访问模式以触发对应的银行功能来执行其他银行选项。

[0075] 在本发明的示范性实施例中，用户可以限制地访问在3D环境上呈现的某些对象。这可以发生在成功验证用户之后和在用户设备302与服务提供者304的连接建立之后。这可以因为验证的用户对他的/她的银行帐户的限制的访问。例如，如果验证的用户没有申请信用卡，则已经显示了信用卡名称的对象可以在3D环境中不可被验证的用户访问。

[0076] 此外，本领域技术人员可以理解，前述示例不是本发明的限制性的方面，并且仅仅用于本发明的更好说明。此外，服务提供者304的范围不仅仅局限于银行。服务提供者可以是任何组织的交互式语音响应(IVR)系统，其可以调用用户设备302以用于只能被给予有效的用户的某些安全的信息。因此，用户设备302的用户可以使用基于游戏的环境来验证他的/她的身份以从IVR系统访问被保护的信息。类似地，其它实施例也是可能的，其中需要高

级别或多级别安全性。

[0077] 图4是根据本发明的实施例的用于使得用户能够利用服务系统(例如,银行或IVR系统)验证和导航的基于游戏的验证环境400的例示。在实施例中,用户可以使用基于游戏的环境400作为在例如IVR调用或任何其他调用期间进行验证的支持。例如,如果用户需要验证他的/她的身分证明,则用户可以使用基于游戏的环境400来提供IVR系统需要的输入。此外,在调用期间,如果用户需要进行得更深到IVR菜单选项中,则用户可以再一次使用基于游戏的环境400来提供IVR系统所需的输入。

[0078] 如图所示,例如,基于游戏的验证环境400是数字化的风景。数字化的风景包括许多数字化的对象,诸如但不局限于云、太阳、房子、灯塔、石头、球、垫子、伞、汽车等等。在实施例中,这些对象可以通过使用触摸屏设备而被触摸(选择为输入)。在另一个实施例中,对象可以是可移动的对象(即,其在风景上的位置可以被改变),因此可以由用户通过使用触敏设备重新排列(以提供输入模式)。在另一实施例中,对象可以被显示有标签号码(如图4所示)。用户可以使用触摸屏来触摸那些对象或对应的标签以向基于游戏的验证环境400提供输入,或可以使用键区(在非触摸设备的情况下)通过按压它的对应键来选择对象。对象和/或号码可以一直被用户看得见,或者可以在开始设置阶段被用户看得见,随后在将来验证和校验会话期间被隐藏。

[0079] 此外,在本发明的示范性实施例中,用户可以调用他的/她的银行的IVR系统。网络服务提供者可以要求用户通过输入个人识别号码(PIN)验证他/她自己。用户然后可以通过选择/触摸嵌入在显示在屏幕上的对象上的对象或号码来输入他的/她的PIN号码。例如,如果用户的PIN是9717,则用户可以按以下顺序选择基于游戏的环境400中的对象:汽车、灯塔、布和灯塔。在实施例中,如上所述,用户可以具有接通或关断嵌入在数字化的对象顶部的号码的显示来用于此目的。用户可以在输入PIN的同时记住用户输入的序列,即首先选择汽车然后选择灯塔然后是布然后再一次是灯塔的序列。因此,用户可以切断嵌入的号码的显示并且可以总是输入记住的序列,该序列将充当银行的有效输入。

[0080] 此外,在验证后,IVR系统可以要求用户按下‘1’以知道帐户结余,按下‘2’以用于小型声明等等。用户然后可以触摸/选择布以知道他的/她的帐户结余。类似地,用户可以通过经由基于游戏的环境400选择期望的选择来导航得更深到IVR系统中。在另一个实施例中,用户可以再一次记住验证后选择并且可以每次输入所有输入以直接导航到期望的服务,以便通过直接输入输入序列:汽车、灯塔、布、灯塔和布,来取回他的帐户结余。

[0081] 在本发明的另一个实施例中,游戏环境400可以不显示嵌入在风景的任何数字化的对象上的任何号码。用户可以需要预先向银行注册以存储用于验证和验证后服务或数据访问的一个或多个访问模式。因此,为了验证,用户可以总是需要按以下序列触摸风景中的对象:汽车、灯塔、布和灯塔。此外,风景的对象的位置可以是随机的,并且每当用户与基于游戏的环境通信时,云、灯塔、太阳、球和布等等的位置可以被改变。但是,银行存储的序列或访问模式将保持相同,并且用户可以需要找到对象在风景中的位置以输入与访问模式相同的序列,即汽车、灯塔、布和灯塔。这可以使得用户能够直观地识别他的/她的口令并且将使得入侵者非常难以破译模式。

[0082] 本领域技术人员将理解,如图所示的环境400仅仅用于更好地说明本发明。本发明的范围不仅仅局限于风景。基于游戏的环境可以包括任何游戏类型,包括二维游戏、三维游

戏、或任何其他交互式环境，诸如谜语、钢琴弹奏等等。例如，用户可以在钢琴上弹奏他或她最喜爱的歌曲，或歌曲的至少几小节，以得到访问并且验证他或她自己。

[0083] 此外，将号码嵌入在数字和可移动的对象上仅仅是本发明的实施例并且不覆盖本发明的全范围。基于游戏的环境可以或可以不包括嵌入可见号码的任意对象。此外，基于游戏的环境可以被随机地显示，并且因此用户可以必须输入他们预存储的序列。

[0084] 在本发明的另一个实施例中，游戏接口此外被用作从自助服务领域到协助服务领域的管道。例如，在已经验证了之后，如果用户接近游戏环境之内的一队人，这可以被推断为请求帮助。“协助服务”可以可选地在自助服务之后，并且是指在与用户交互中涉及人类代理。

[0085] 通过使用视觉特性，其它可见的游戏符号可以通告可以被用户“拜访”的技能，包括通过由用户做出的动作序列组合对象的能力。例如，通过用户访问埃菲尔铁塔然后护士，用户将需要说法语的医嘱。

[0086] 在进一步的实施例中，对于企业高价值的用户，专门扩展玩游戏财产。例如，在仅仅某些用户可访问的某些位置处，可以使得代理组可用或“可见”。

[0087] 本发明的实施例还涉及自助服务交互的背景如何可以用于选择合适地熟练的人类代理。

[0088] 图5是根据本发明的实施例的在电子设备上定制和设置基于游戏的验证应用的方法的流程图。在实施例中，流程图表示定制模块202的功能(由先前在本发明的图2中定义的)。此外，当结合图1、2、3和4阅读与方法对应的描述时，可以更清楚地理解该方法。执行方法的顺序不意欲被理解为限制，并且可以组合任意数目的方法步骤以便实现该方法或可替换方法，而不背离本发明的范围。

[0089] 在步骤502，电子设备的用户可以从第三方源导入基于游戏的验证环境，或可以在设备本身上创建环境。基于游戏的验证环境可以使得用户能够阻止对电子设备的未授权访问或对存储在电子设备中的任何数据或服务选项的未授权访问或对诸如IVR系统之类的服务提供者的企业系统的未授权访问。其后，用户可以将基于游戏的环境安装在电子设备中以用于定制环境。

[0090] 在步骤504，用户可以定制基于游戏的环境以便使环境变得为用户所熟知。环境可以类似用户童年所居住的地方，或可以类似用户的某些想象或梦，或可以类似最喜爱的电影场景或用户的生活事件。这可以向环境增加高级别的个性化，因而增加安全性，因为这样的环境可以不被任何其他用户识别。

[0091] 在步骤506，用户可以记录给予基于游戏的环境的输入序列，其可以以用户期望的方式修改环境的外观和感觉或可以改变环境的状态。用户然后可以将记录的输入序列存储为访问模式，访问模式可以用于验证尝试访问电子设备的用户。此外，用户可以提供要被存储为访问模式的这样的(但是不同的)输入序列中的一个或多个，访问模式可以用于执行电子设备上的某些任务作为验证后活动。

[0092] 在步骤508，用户可以确定用户需要对其激活基于游戏的验证环境以验证发起事件的用户的事件。事件可以是接通电子设备，或可以是访问存储在电子设备中的某些数据，或可以是访问由电子设备或由企业服务提供者提供的服务。因此，如果用户发起实现触发器的任何事件，则发起事件的用户将首先遇到基于游戏的环境，因此在允许用户访问发起

的事件之前，用户的身份可以首先被确认。

[0093] 在步骤510，用户可以对基于游戏的环境做出最终的定制改变，然后可以通过将基于游戏的环境与在步骤508确定的触发事件连接来完成定制的处理。因此，在电子设备的任何事件下基于游戏的验证环境的设置完成并且准备被使用。在实施例中，用户可以通过尝试触发事件并且尝试检查基于游戏的环境是否被激活来测试该设置。这样，用户可以确信对电子设备、它的数据或嵌入在企业服务数据库中的用户的数据的未授权访问的安全性。

[0094] 图6是根据本发明的实施例的通过使用基于游戏的验证模块来验证用户的方法的流程图。当结合图1、2、3、4和5阅读与方法对应的描述时，可以更清楚地理解该方法。执行方法的顺序不意欲被理解为限制，并且可以组合任意数目的方法步骤以便实现该方法或可替换方法，而不背离本发明的范围。

[0095] 在步骤602，用户可以尝试经由IVR系统或相反(共同地“访问点”)激活电子设备或包含在其中的数据或企业服务数据库或用户的帐户。在实施例中，电子设备可以被实现为系统102。在另一个实施例中，系统102可以被实现为电子设备的一部分。在另一实施例中，系统102可以被安装为电子设备的固件/软件。此外，电子设备可以被基于游戏的验证应用保护，基于游戏的验证应用可以直到用户成功地输入与预定义的模式匹配的输入模式才允许用户访问电子设备。

[0096] 因此，在步骤604，在激活电子设备之后，基于游戏的环境可以被加载在电子设备上并且用户可以不得不通过该环境以访问电子设备或上述其它访问点。此外，在步骤606将基于游戏的验证环境加载在电子设备上之后，电子设备可以开始监视电子设备的所有输入装置以记录用户可以使用来与基于游戏的环境交互的用户输入。此步骤(即，步骤606)可以由监视模块204执行(如前面在本发明的图2中描述的)。

[0097] 此外，在步骤608，电子设备可以开始将监视的用户输入(用户的活动)与存储在电子设备中的预定义的模式匹配。如果监视的用户输入与预存储的模式中的任何一个匹配，则该方法可以前进到步骤610，否则该方法可以再一次从步骤606开始，其中电子设备保持监视用户提供的与基于游戏的验证应用交互的输入。在实施例中，此步骤(步骤608)可以由解码模块206执行(如先前在本发明的图2中描述的)。

[0098] 在步骤610，电子设备可以执行可以与识别的访问模式相关联的任务。例如，如果在步骤608确定用户提供的输入模式匹配与用户的验证相关联的访问模式，则在步骤610，用户可以被验证。此外，如果在步骤608确定用户提供的第二输入模式匹配与取回帐户结余的指令相关联的访问模式，则在步骤610可以取回相关银行帐户的帐户结余并且合适地显示给用户。

[0099] 在实施例中，与仅仅为了验证目的而从用户接收到的输入模式相比，第二输入模式(作为验证后数据访问请求接收的)可以包括更少数目的输入/输入序列。这可以在验证后数据访问期间向用户提供便利。因此，在步骤610，有效的用户瞄准的实际任务由电子设备执行。在实施例中，步骤610可以由执行模块208执行(如先前在本发明的图2中描述的)。

[0100] 此外，方法不局限于这里提及的上述信息。在图1-5中说明的各个实施例可以由上面这里说明的方法的每一个使用。此外，本发明不局限于上述实施例和示例，并且许多其它实施例和示例可以根据本发明来实现而不背离本发明的范围。

[0101] 此外，本领域技术人员可以理解，与本发明对应的设备、系统和方法提供用于电子

设备的有效用户的验证的更直观的、用户友好的和一致的手段。此外，本发明提供用于访问由电子设备提供的数据或服务的验证后手段。本发明的这些功能和特征不局限于上述描述。各个实施例(不局限于上述描述)可以根据本发明的范围实现。

[0102] 有利地，本发明提供一种系统、方法和设备作为用户名和口令保护的应用和服务的繁重系统的替换解决方案。本发明可以增强想要保护任何数据或服务免受未授权访问的用户的体验。此外，本发明可以在管理被保护的交易中增加年轻孩子或成人的乐趣。此外，本发明可以使得年长的人免于记住用户名和口令。另外，本发明可以提高验证系统中的安全性级别而不增大合法用户的障碍。

[0103] 此外，本发明描述想要合法地在企业之内访问数据的用户如何可以使用它们自己的偏好和创作的接口来安全地这样做。此外，本发明使得用户能够以高度直观的和灵活的方式与自定义的基于游戏的验证平台交互。再一次此外，本发明使得用户能够以再现身份的方式交互，由于所有分立的步骤/交互涉及的高度个性化，盗窃更困难。

[0104] 本领域技术人员可以理解，本发明不局限于上面这里提及的优点。此外，许多其它优点可以根据上面给出的描述被理解，而不背离本发明的范围。本发明的实施例在上面参考根据本发明的实施例的方法和系统的框图和简图描述。可以理解，图的每个块和图中块的组合可以由计算机程序指令实现。可以将这些计算机程序指令加载到一个或多个通用计算机、专用计算机或其它可编程的数据处理翻译器的处理器上以产生机器，以使得在计算机或其它可编程的数据处理翻译器上运行的指令产生用于实现在块中指定的功能的手段。这样的计算机程序指令也可以被存储在计算机可读存储器中，所述计算机可读存储器可以引导计算机或其它可编程的数据处理装置以特定方式运行，以使得存储在计算机可读存储器中的指令产生包括实现在块中指定的功能的指令装置的制品。

[0105] 尽管已经结合当前被认为是实际的和各种实施例描述了本发明，但是应当理解，本发明不局限于公开的实施例，而是相反地，意图覆盖包括在所附权利要求书的精神而且范围内的各种修改和等效配置。本发明已经在计算设备、电话机和计算机可执行指令(诸如由计算机执行的程序模块)的一般背景下描述。一般地，程序模块包括例程、程序、符号、组件、数据结构等等，执行特定任务或实现特定抽象数据类型。本领域技术人员将理解，本发明可以利用其它计算机系统配置实践，包括手持设备、多处理器系统、基于微处理器或可编程的消费电子设备、网络PC、小型计算机、大型计算机等等。此外，本发明也可以在分布式计算世界中实践，在分布式计算世界中，任务由通过通信网络链接的远程处理设备执行。在分布式计算世界中，程序模块可以位于本地和远程存储器存储设备二者中。

[0106] 撰写的说明书使用示例公开本发明，包括最佳方式，并且还使得任何本领域技术人员能够实践本发明，包括做出和使用任何设备或系统并且执行任何合并的方法。本发明的可取得专利的范围在权利要求书中定义，并且可以包括本领域技术人员想到的其它示例。这样的其它示例预期在权利要求书的范围内，如果它们具有不不同于权利要求书的文字语言的结构元素，或如果它们包括与权利要求书的文字语言无实质差别的等效的结构元素。

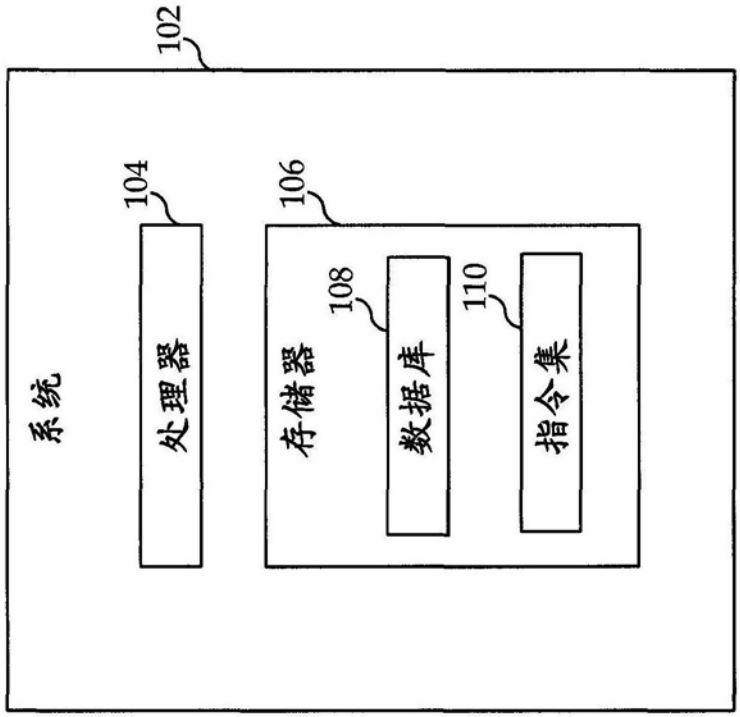

102
系统
104
处理器
106
存储器
108
数据库
110
指令集

图1

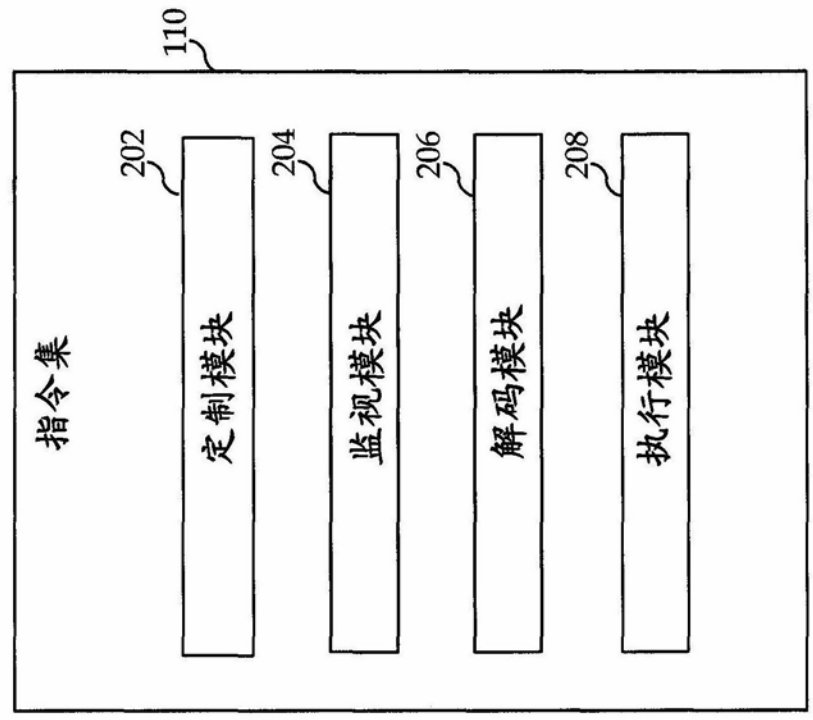

110
指令集
202
定制模块
204
监视模块
206
解码模块
208
执行模块

图2

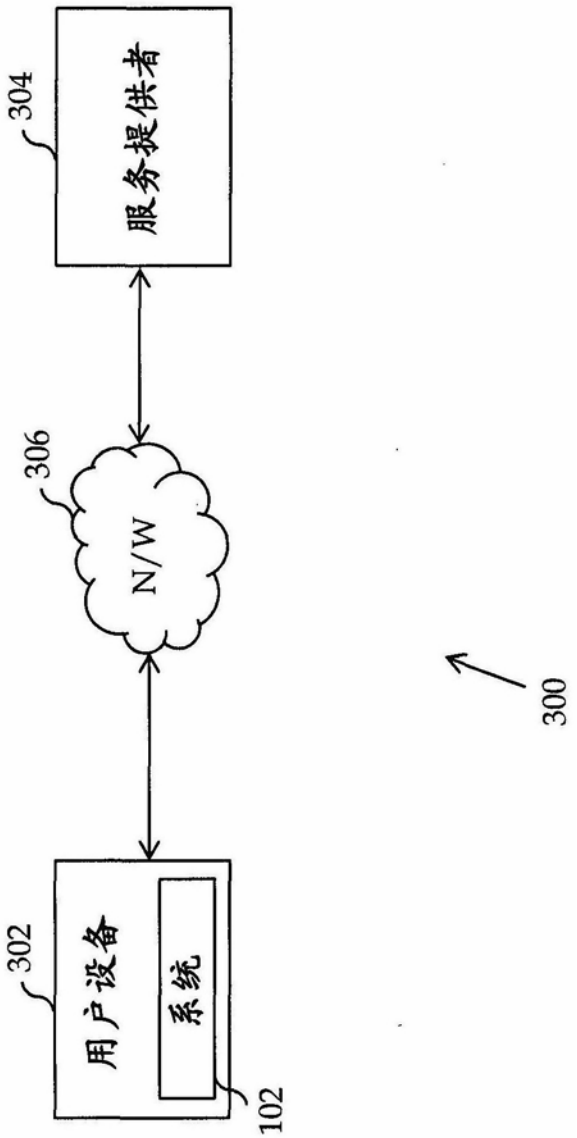


图3

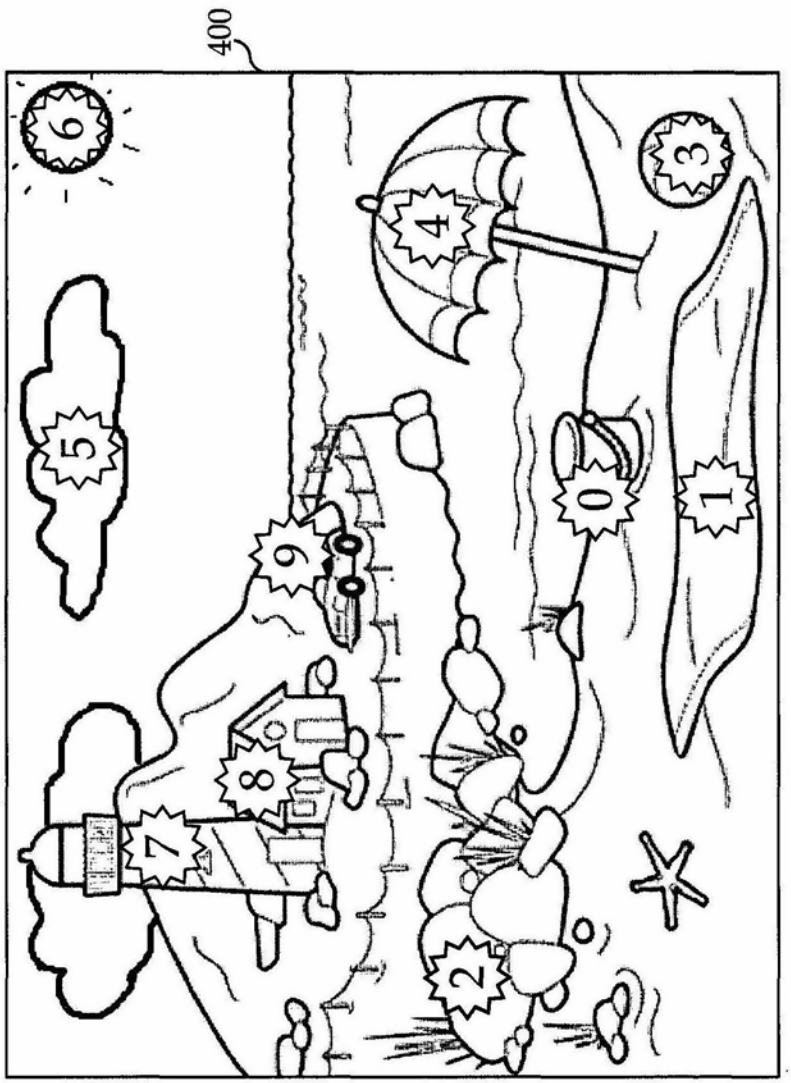


图4

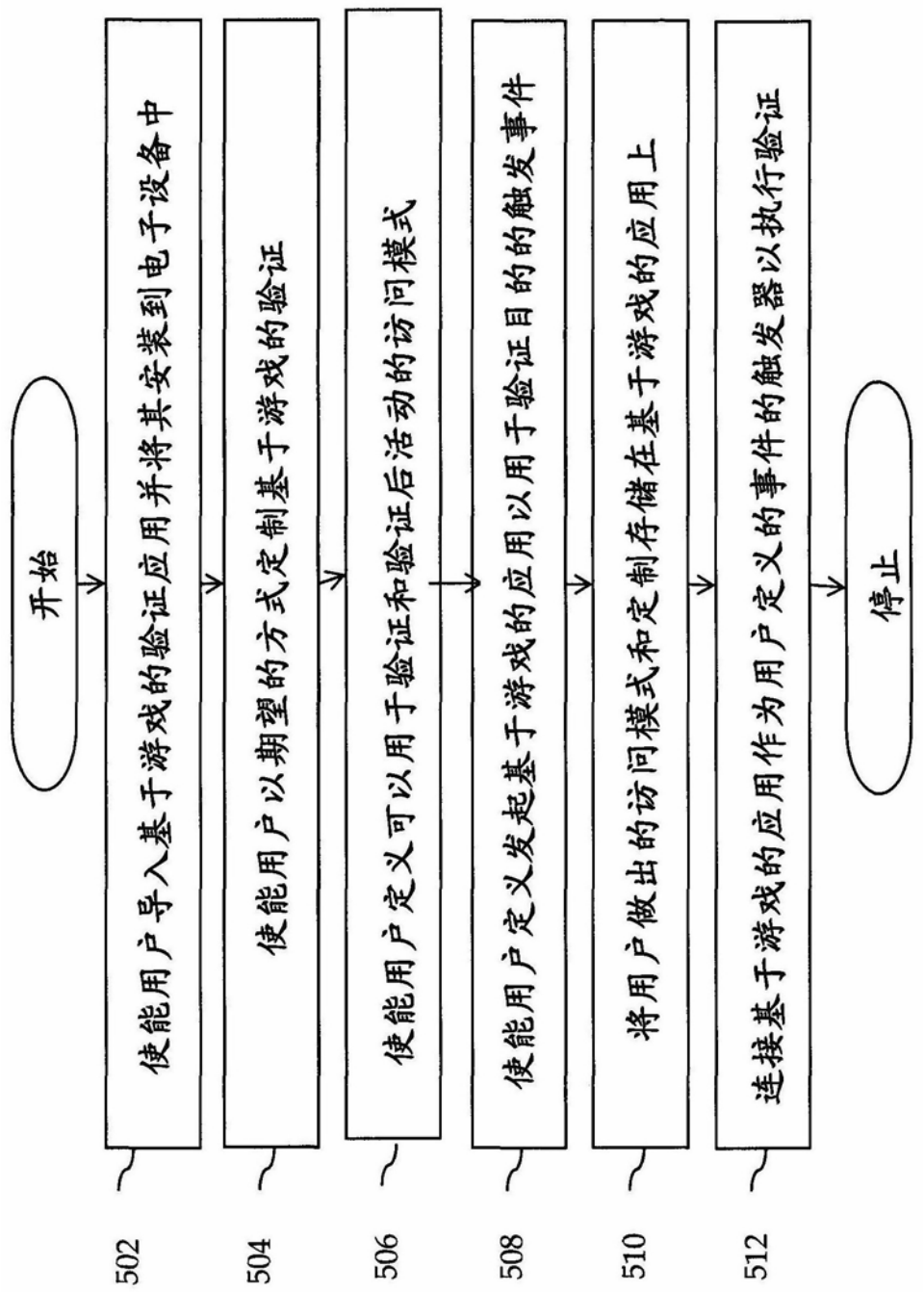

开始
使能用户导入基于游戏的验证应用并将其安装到电子设备中
使能用户以期望的方式定制基于游戏的验证
使能用户定义可以用于验证和验证后活动的访问模式
使能用户定义发起基于游戏的应用以用于验证目的的触发事件
将用户做出的访问模式和定制存储在基于游戏的应用上
连接基于游戏的应用作为用户定义的事件的触发器以执行验证
停止
502
504
506
508
510
512

图5

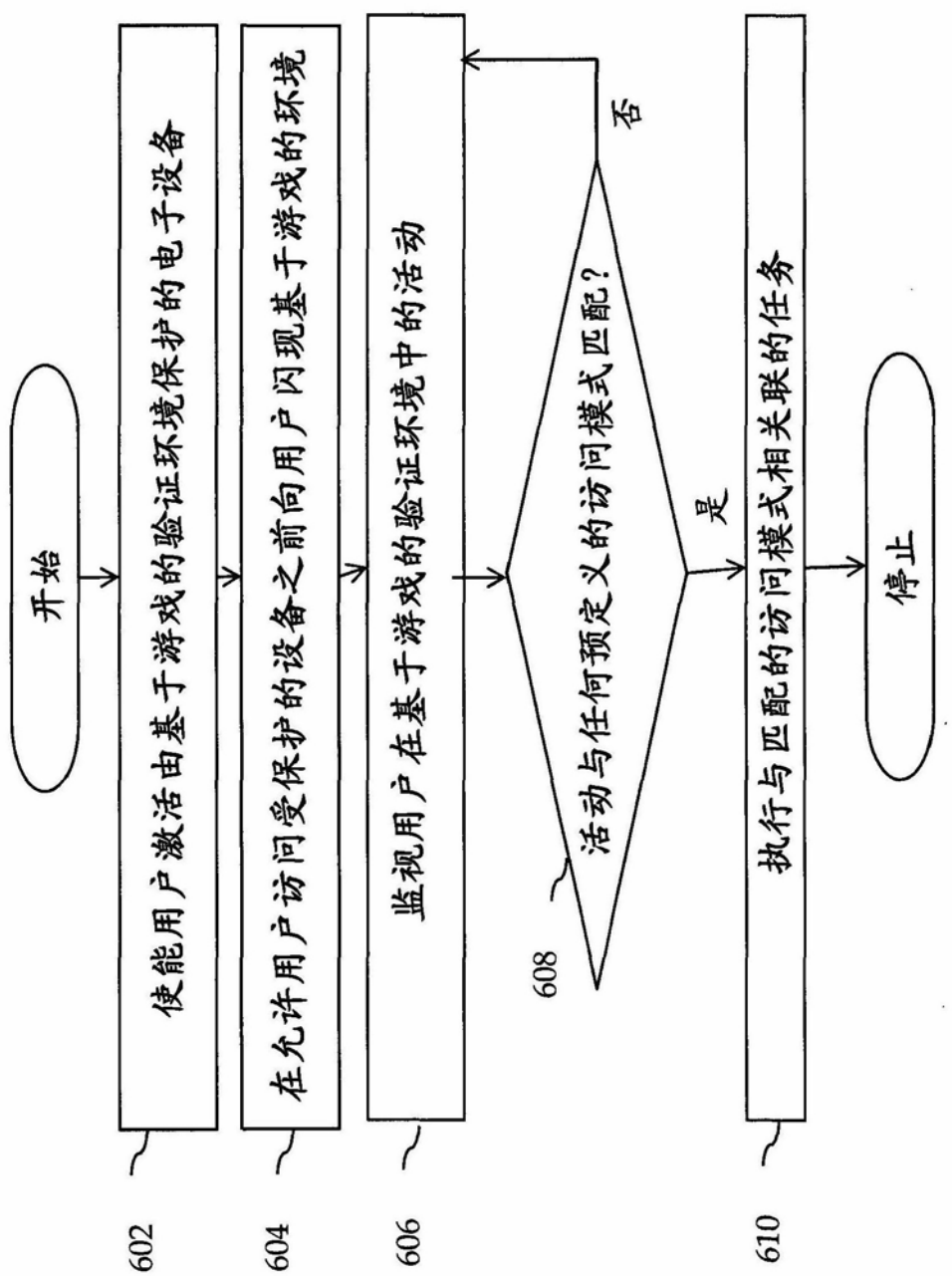

开始
使能用户激活由基于游戏的验证环境保护的电子设备
602
在允许用户访问受保护的设备之前向用户闪现基于游戏的环境
604
监视用户在基于游戏的验证环境中的活动
606
活动与任何预定义的访问模式匹配?
608
否
是
执行与匹配的访问模式相关联的任务
610
停止

图6