



(12) 发明专利申请

(10) 申请公布号 CN 104811304 A

(43) 申请公布日 2015.07.29

(21) 申请号 201410039940.1

(22) 申请日 2014.01.27

(71) 申请人 腾讯科技(深圳)有限公司

地址 518044 广东省深圳市福田区振兴路赛
格科技园 2 栋东 403 室

(72) 发明人 陆莉 刘杰

(74) 专利代理机构 上海波拓知识产权代理有限
公司 31264

代理人 吕静

(51) Int. Cl.

H04L 9/32(2006.01)

H04L 29/06(2006.01)

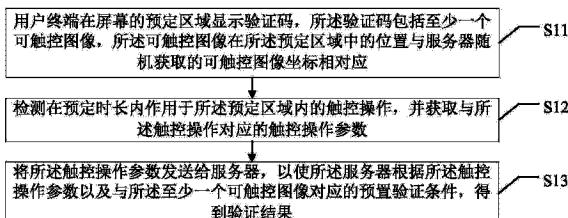
权利要求书5页 说明书14页 附图11页

(54) 发明名称

身份验证方法及装置

(57) 摘要

本发明提出一种成本较低且抗破解能力强、安全性高的身份验证方法及装置。该方法包括：用户终端在屏幕的预定区域显示验证码，所述验证码包括至少一个可触控图像，所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应；检测在预定时长内作用于所述预定区域内的触控操作，并获取与所述触控操作对应的触控操作参数；以及将所述触控操作参数发送给服务器，以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件，得到验证结果。



1. 一种身份验证方法,其特征在于,所述方法包括:

用户终端在屏幕的预定区域显示验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应;

检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数;以及

将所述触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

2. 如权利要求1所述的方法,其特征在于,所述用户终端在屏幕的预定区域显示验证码的步骤之前,还包括:

所述用户终端向服务器发送验证码生成请求;以及

接收服务器返回的第一验证码生成参数,所述第一验证码生成参数包括至少一个所述可触控图像坐标;

所述用户终端在屏幕的预定区域显示验证码的步骤包括:

所述用户终端根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

3. 如权利要求2所述的方法,其特征在于,所述用户终端接收服务器返回的第一验证码生成参数的同时,还接收所述服务器返回的与所述至少一个可触控图像坐标对应的可触控图像,

所述用户终端在屏幕的预定区域显示验证码的步骤包括:

所述用户终端根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像。

4. 如权利要求2或3所述的方法,其特征在于,所述将所述触控操作参数发送给服务器的步骤之后,还包括:

当所述服务器判定验证结果为不通过或者验证的次数未达到预定次数时,接收所述服务器根据预置的验证码下发规则返回的第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标;

根据所述第二验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像;

返回所述检测在预定时长内作用于所述预定区域内的触控操作的步骤。

5. 如权利要求4所述的方法,其特征在于,所述预置的验证码下发规则包括:

如果所述服务器判定验证结果为不通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级;或者

如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级。

6. 如权利要求4所述的方法,其特征在于,当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时,

所述第二验证码生成参数中的可触控图像坐标的个数大于所述第一验证码生成参数中的可触控图像坐标的个数;或者

所述第二验证码生成参数中的多个可触控图像坐标之间的间隔大于所述第一验证码生成参数中的可触控图像坐标之间的间隔 ;或者

所述第二验证码生成参数中的可触控图像的显示时长小于所述第一验证码生成参数中的可触控图像的显示时长。

7. 如权利要求 1 所述的方法,其特征在于,所述至少一个可触控图像显示在所述屏幕的时长小于所述预定时长。

8. 如权利要求 1 所述的方法,其特征在于,当获取到与所述触控操作对应的触控操作参数后,隐藏所述可触控图像。

9. 如权利要求 1 所述的方法,其特征在于,所述用户终端还向用户展示验证提示信息,用以提示用户触控所述验证码中的至少一个可触控图像以进行身份验证。

10. 一种身份验证方法,其特征在于,所述方法包括 :

服务器接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数,所述预定范围内显示有验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与所述服务器下发的可触控图像坐标相对应 ;以及

根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

11. 如权利要求 10 所述的方法,其特征在于,所述服务器接收用户终端返回的触控操作参数的步骤之前,还包括 :

接收所述用户终端发送的验证码生成请求 ;以及

根据所述验证码生成请求随机获取第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标 ;以及

将所述第一验证码生成参数返回所述用户终端。

12. 如权利要求 11 所述的方法,其特征在于,所述服务器将所述第一验证码生成参数返回所述用户终端的同时,还向所述用户终端返回与所述至少一个可触控图像坐标对应的可触控图像。

13. 如权利要求 10 所述的方法,其特征在于,每个所述可触控图像坐标对应一个标准触控操作参数,与所述至少一个可触控图像坐标对应的预置验证条件包括 :所获取的触控操作参数与对应的标准触控操作参数之间的差值小于预定阈值,如果满足所述预置验证条件则验证结果为通过,如果不满足所述预置验证条件,则验证结果为不通过。

14. 如权利要求 11 或 12 所述的方法,其特征在于,所述方法还包括 :

根据所述验证结果或者验证的次数,判断是否需要向所述用户终端返回第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标,如果所述服务器判定验证结果为不通过或者验证的次数未达到预定次数,则根据预置的验证码下发规则,向所述用户终端返回第二验证码生成参数。

15. 如权利要求 14 所述的方法,其特征在于,所述预置的验证码下发规则包括 :

如果所述服务器判定验证结果为不通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级 ;或者

如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过,

则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级。

16. 如权利要求 15 所述的方法,其特征在于,当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时,

所述第二验证码生成参数中的可触控图像坐标的个数大于所述第一验证码生成参数中的可触控图像坐标的个数;或者

所述第二验证码生成参数中的多个可触控图像坐标之间的间隔大于所述第一验证码生成参数中的可触控图像坐标之间的间隔;或者

所述第二验证码生成参数中的可触控图像的显示时长小于所述第一验证码生成参数中的可触控图像的显示时长。

17. 一种身份验证装置,运行于用户终端,所述用户终端具有触控屏幕,其特征在于,所述装置包括:

显示模块,用于在屏幕的预定区域显示验证码,所述验证码包括至少一个可触控图像;

检测模块,用于检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数;以及

第一发送模块,用于将所述触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

18. 如权利要求 17 所述的装置,其特征在于,所述装置还包括:

第二发送模块,用于向所述服务器发送验证码生成请求;以及

第一接收模块,用于接收服务器返回的第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标;

所述显示模块还用于根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

19. 如权利要求 17 所述的装置,其特征在于,所述显示模块显示所述至少一个可触控图像在所述屏幕的时长小于所述预定时长。

20. 如权利要求 17 所述的装置,其特征在于,当所述检测模块获取到与所述触控操作对应的触控操作参数后,所述显示模块隐藏所述可触控图像。

21. 如权利要求 18 所述的装置,其特征在于,所述第一接收模块接收服务器返回的第一验证码生成参数的同时,还接收所述服务器返回的与所述至少一个可触控图像坐标对应的可触控图像,

所述显示模块还用于根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像。

22. 如权利要求 18 或 21 所述的装置,其特征在于,所述装置还包括:

第二接收模块,当所述服务器判定验证结果为不通过或者验证的次数未达到预定次数时,用于接收所述服务器根据预置的验证码下发规则返回的第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标;

所述显示模块还用于根据所述第二验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像。

23. 如权利要求 22 所述的装置，其特征在于，所述预置的验证码下发规则包括：

如果所述服务器判定验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级；或者

如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级。

24. 如权利要求 23 所述的装置，其特征在于，当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时，所述第二验证码生成参数中的可触控图像坐标的个数大于所述第一验证码生成参数中的可触控图像坐标的个数；或者所述第二验证码生成参数中的多个可触控图像坐标之间的间隔大于所述第一验证码生成参数中的可触控图像坐标之间的间隔；或者所述第二验证码生成参数中的可触控图像的显示时长小于所述第一验证码生成参数中的可触控图像的显示时长。

25. 如权利要求 17 所述的装置，其特征在于，所述显示模块还向用户展示验证提示信息，用以提示用户触控所述验证码中的至少一个可触控图像以进行身份验证。

26. 一种身份验证装置，运行于服务器，其特征在于，所述装置包括：

第一接收模块，用于接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数，所述预定范围内显示有验证码，所述验证码包括至少一个可触控图像，所述可触控图像在所述预定区域中的位置与所述服务器下发的可触控图像坐标相对应；以及

验证模块，用于根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件，得到验证结果。

27. 如权利要求 26 所述的装置，其特征在于，所述装置还包括：

第二接收模块，用于接收所述用户终端发送的验证码生成请求；以及

参数生成模块，用于根据所述验证码生成请求随机获取第一验证码生成参数，所述第一验证码生成参数包括至少一个可触控图像坐标；以及

第一发送模块，用于将所述第一验证码生成参数返回所述用户终端。

28. 如权利要求 27 所述的装置，其特征在于，所述第一发送模块将所述第一验证码生成参数返回所述用户终端的同时，还向所述用户终端返回与所述至少一个可触控图像坐标对应的可触控图像。

29. 如权利要求 26 所述的装置，其特征在于，每个所述可触控图像坐标对应一个标准触控操作参数，与所述至少一个可触控图像坐标对应的预置验证条件包括：所获取的触控操作参数与对应的标准触控操作参数之间的差值小于预定阈值，如果满足所述预置验证条件则所述验证模块判定验证结果为通过，如果不满足所述预置验证条件，则所述验证模块判定验证结果为不通过。

30. 如权利要求 27 或 28 所述的装置，其特征在于，所述装置还包括：

判断模块，用于根据所述验证结果或者验证的次数，判断是否需要向所述用户终端返回第二验证码生成参数，所述第二验证码生成参数包括至少一个可触控图像坐标；

第二发送模块，如果所述服务器判定验证结果为不通过或者验证的次数未达到预定次数，用于根据预置的验证码下发规则，向所述用户终端返回所述第二验证码生成参数。

31. 如权利要求 30 所述的装置，其特征在于，所述预置的验证码下发规则包括：

如果所述服务器判定验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级；或者

如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级。

32. 如权利要求 30 所述的装置，其特征在于，当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时，所述第二验证码生成参数中的可触控图像坐标的个数大于所述第一验证码生成参数中的可触控图像坐标的个数；或者所述第二验证码生成参数中的多个可触控图像坐标之间的间隔大于所述第一验证码生成参数中的可触控图像坐标之间的间隔；或者所述第二验证码生成参数中的可触控图像的显示时长小于所述第一验证码生成参数中的可触控图像的显示时长。

身份验证方法及装置

技术领域

[0001] 本发明涉及计算机网络技术领域，特别是涉及一种身份验证方法及装置。

背景技术

[0002] 随着计算机和计算机网络的日益普及，互联网已经深入到人们工作、学习和生活的各个领域。网络的发展在为人们提供便利的同时也带来各种挑战。一些人会利用机器人程序大量地不当使用网络资源，例如群发垃圾邮件等，使服务器效能大为降低。也有人利用程序不断发出服务请求回应，进行“饱和攻击”以达到使服务器瘫痪的目的。甚至还有人尝试利用暴力破解等手段进行恶意破解密码等行为。为避免上述恶意行为，设计一套能够让计算机自动分辨信息是来自合理用户或是非正当使用的机器人程序的工具，就显得非常重要。

[0003] 使用图像验证码是现在比较通行的方式，图像验证码的主要目的是分辨网络服务用户是程序还是人类。图像验证码是含有字符串的图片，在验证时要求用户输入字符串的内容。字符串通常由大小写字母和数字组成，部分验证码包含汉字或数学公式，字符串的长度可以是随机或固定的。为了避免被机器自动识别，通常会对图片的背景进行改进，例如增加各种纹理图案等，从而对机器自动识别进行干扰。

[0004] 然而，只要收集足够的样本，使用字符识别技术进行机器学习和训练，就可以开发出机器程序来解码图像验证码。即使是改进的图像验证码，如果它的背景库不够庞大，依然能够被机器识别。传统的图像验证码无法避免这个问题，以字符图像验证码为例，如果是大小写字符和数字，最多只有 62 个。因此，现有的图像验证码抗破解能力差、安全性不够高。而且这种方式在手机等移动终端使用时，用户输入不太方便，容易出错、效率较低。

[0005] 为了提高验证码的抗破解能力以及适应触控型移动终端的发展趋势，研发人员开发了点选验证码，点选验证码在使用时通常会向用户展示包含多个包含自然物体的图片以及与这些图片内容相关的提示信息，由用户根据提示信息对这些图片进行选择，根据用户的选择来对用户的身份进行验证，由于机器在对提示信息的理解以及对对象的分类这两方面都存在很大的困难，因此可以大大增加机器破解验证码的难度。

[0006] 但是，点选验证码在使用时，图片资源要求很高，而且需要人工筛选分类入库，成本较高。

发明内容

[0007] 本发明实施例的目的在于，提供一种成本较低且抗破解能力强、安全性高的身份验证方法及装置。

[0008] 为了解决上述问题，本发明实施例提供一种身份验证方法，所述方法包括：用户终端在屏幕的预定区域显示验证码，所述验证码包括至少一个可触控图像，所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应；检测在预定时长内作用于所述预定区域内的触控操作，并获取与所述触控操作对应的触控操作参数；以及将所述

触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0009] 本发明实施例还提供一种身份验证方法,所述方法包括:服务器接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数,所述预定范围内显示有验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应;以及根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0010] 相应的,本发明实施例还提供一种身份验证装置,所述装置可以运行于用户终端,所述装置可以包括:显示模块,用于在屏幕的预定区域显示验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应;检测模块,用于检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数;以及第一发送模块,用于将所述触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0011] 相应的,本发明实施例还提供一种身份验证装置,可以运行于服务器,所述装置可以包括:第一接收模块,用于接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数,所述预定范围内显示有验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与所述服务器下发的可触控图像坐标相对应;以及验证模块,用于根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0012] 相对于现有技术,本发明实施例中,验证码由一个或多个可触控图像组成,可触控图像的具体内容可以很简单,例如可以是一个圆点或者是一个方块等,可以降低成本;可触控图像在屏幕区域中的位置与服务器下发的随机的可触控图像坐标相对应,可以增加人工收集验证码作为破解题库的难度;充分利用了人类对位置判断的先天优势,用户可以通过触摸显示在屏幕上的可触控图像进行身份验证,用户终端将采集到的触控操作参数发送给服务器,由服务器根据触控操作参数以及与每个可触控图像对应的预置验证条件来得到验证结果,只有触控操作参数满足对应的预置验证条件时,才判定身份验证通过,大大增加了机器破解验证码的难度,安全性高;相对于点选验证码来说,不需要用户根据问题对图片进行类别辨识,只要用户触摸验证码中的所有可触控图像即可,降低了用户的使用门槛。也就是说本发明在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性。

[0013] 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其他目的、特征和优点能够更明显易懂,以下特举较佳实施例,并配合附图,详细说明如下。

附图说明

[0014] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其它

的附图。

- [0015] 图 1 是本发明实施例的应用环境图。
- [0016] 图 2 是一种可应用于本发明实施例的用户终端的结构框图。
- [0017] 图 3 是一种可应用于本发明实施例的服务器的结构框图。
- [0018] 图 4 是本发明第一实施例提供的一种身份验证方法的流程图。
- [0019] 图 5 是本发明第一实施例提供的一种身份验证方法的部分流程图。
- [0020] 图 6 是本发明实施例中验证码的一种具体示例的示意图。
- [0021] 图 7 是本发明实施例中验证码的另一种具体示例的示意图。
- [0022] 图 8 是本发明第二实施例提供的一种身份验证方法的流程图。
- [0023] 图 9 是本发明第三实施例提供的一种身份验证方法的流程图。
- [0024] 图 10 是本发明第三实施例提供的一种身份验证方法的部分流程图。
- [0025] 图 11 是本发明第四实施例提供的一种身份验证方法的流程图。
- [0026] 图 12 是本发明第五实施例提供的一种身份验证方法的流程图。
- [0027] 图 13 是本发明第六实施例提供的一种身份验证装置的结构框图。
- [0028] 图 14 是本发明第六实施例提供的一种身份验证装置的部分结构框图。
- [0029] 图 15 是本发明第七实施例提供的一种身份验证装置的结构框图。
- [0030] 图 16 是本发明第八实施例提供的一种身份验证装置的结构框图。
- [0031] 图 17 是本发明第八实施例提供的一种身份验证装置的部分结构框图。
- [0032] 图 18 是本发明第九实施例提供的一种身份验证装置的结构框图。
- [0033] 图 19 为本发明实施例中的身份验证系统的结构框图。

具体实施方式

[0034] 为更进一步阐述本发明为达成预定发明目的所采取的技术手段及功效，以下结合附图及较佳实施例，对依据本发明提出的身份验证方法及身份验证装置的具体实施方式、方法、步骤、结构、特征及其功效，详细说明如下。

[0035] 有关本发明的前述及其他技术内容、特点及功效，在以下配合参考图式的较佳实施例的详细说明中将可清楚呈现。通过具体实施方式的说明，当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解，然而所附图式仅是提供参考与说明之用，并非用来对本发明加以限制。

[0036] 请参阅图 1，所示为本发明实施例提供的身份验证方法的应用环境图。如图 1 所示，用户终端 100 以及服务器 200 位于无线或有线网络 300 中，通过该无线或有线网络 300，用户终端 100 以及服务器 200 相互通信。

[0037] 用户终端 100 具体可以包括智能手机、平板电脑、电子书阅读器、MP3 播放器 (Moving Picture Experts Group Audio Layer III, 动态影像专家压缩标准音频层面 3)、MP4 (Moving Picture Experts Group Audio Layer IV, 动态影像专家压缩标准音频层面 4) 播放器、膝上型便携计算机、车载终端等等。

[0038] 图 2 示出了一种可应用于本发明实施例中的用户终端的结构框图。如图 2 所示，用户终端 100 包括存储器 102、存储控制器 104，一个或多个(图中仅示出一个)处理器 106、外设接口 108、射频模块 110、定位模块 112、图像采集模块 114、音频模块 116、触控屏幕 118

以及按键模块 120。这些组件通过一条或多条通讯总线 / 信号线 122 相互通讯。

[0039] 可以理解,图 2 所示的结构仅为示意,用户终端 100 还可包括比图 2 中所示更多或者更少的组件,或者具有与图 2 所示不同的配置。图 2 中所示的各组件可以采用硬件、软件或其组合实现。

[0040] 存储器 102 可用于存储软件程序以及模块,如本发明实施例中的身份验证方法及装置对应的程序指令 / 模块,处理器 106 通过运行存储在存储器 102 内的软件程序以及模块,从而执行各种功能应用以及数据处理,如本发明实施例提供的身份验证方法。

[0041] 存储器 102 可包括高速随机存储器,还可包括非易失性存储器,如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中,存储器 102 可进一步包括相对于处理器 106 远程设置的存储器,这些远程存储器可以通过网络连接至用户终端 100。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。处理器 106 以及其他可能的组件对存储器 102 的访问可在存储控制器 104 的控制下进行。

[0042] 外设接口 108 将各种输入 / 输入装置耦合至 CPU 以及存储器 102。处理器 106 运行存储器 102 内的各种软件、指令以执行用户终端 100 的各种功能以及进行数据处理。

[0043] 在一些实施例中,外设接口 108,处理器 106 以及存储控制器 104 可以在单个芯片中实现。在其他一些实例中,他们可以分别由独立的芯片实现。

[0044] 射频模块 110 用于接收以及发送电磁波,实现电磁波与电信号的相互转换,从而与通讯网络或者其他设备进行通讯。射频模块 110 可包括各种现有的用于执行这些功能的电路元件,例如,天线、射频收发器、数字信号处理器、加密 / 解密芯片、用户身份模块(SIM)卡、存储器等等。射频模块 110 可与各种网络如互联网、企业内部网、无线网络进行通讯或者通过无线网络与其他设备进行通讯。上述的无线网络可包括蜂窝式电话网、无线局域网或者城域网。上述的无线网络可以使用各种通信标准、协议及技术,包括但不限于全球移动通信系统(Global System for Mobile Communication, GSM)、增强型移动通信技术(Enhanced Data GSM Environment, EDGE),宽带码分多址技术(wideband code division multiple access, W-CDMA),码分多址技术(Code division access, CDMA)、时分多址技术(time division multiple access, TDMA),蓝牙,无线保真技术(Wireless, Fidelity, WiFi)(如美国电气和电子工程师协会标准 IEEE802.11a, IEEE802.11b, IEEE802.11g 和 / 或 IEEE802.11n)、网络电话(Voice over internet protocol, VoIP)、全球微波互联接入(Worldwide Interoperability for Microwave Access, Wi-Max)、其他用于邮件、即时通讯及短消息的协议,以及任何其他合适的通讯协议,甚至可包括那些当前仍未被开发出来的协议。

[0045] 定位模块 112 用于获取用户终端 100 的当前位置。定位模块 112 的实例包括但不限于全球卫星定位系统(GPS)、基于无线局域网或者移动通信网的定位技术。

[0046] 图像采集模块 114 用于拍摄照片或者视频。拍摄的照片或者视频可以存储至存储器 102 内,并通过射频模块 110 发送。

[0047] 音频模块 116 向用户提供音频接口,其可包括一个或多个麦克风、一个或者多个扬声器以及音频电路。音频电路从外设接口 108 处接收声音数据,将声音数据转换为电信号,将电信号传输至扬声器。扬声器将电信号转换为人耳能听到的声波。音频电路还从麦克风处接收电信号,将电信号转换为声音数据,并将声音数据传输至外设接口 108 中以进

行进一步的处理。音频数据可以从存储器 102 处或者通过射频模块 110 获取。此外，音频数据也可以存储至存储器 102 中或者通过射频模块 110 进行发送。在一些实例中，音频模块 116 还可包括一个耳机播孔，用于向耳机或者其他设备提供音频接口。

[0048] 触控屏幕 118 在用户终端 100 与用户之间同时提供一个输出及输入界面。具体地，触控屏幕 118 向用户显示视频输出，这些视频输出的内容可包括文字、图形、视频、及其任意组合。一些输出结果是对应于一些用户界面对象。触控屏幕 118 还接收用户的输入，例如用户的点击、滑动等手势操作，以便用户界面对象对这些用户的输入做出响应。检测用户输入的技术可以是基于电阻式、电容式或者其他任意可能的触控检测技术。通过检测用户输入的技术可以获取用户输入的时间、用户输入的位置、用户手势的轨迹、力度等。触控屏幕 118 显示单元的具体实例包括但并不限于液晶显示器或发光聚合物显示器。

[0049] 按键模块 120 同样提供用户向用户终端 100 进行输入的接口，用户可以通过按下不同的按键以使用户终端 100 执行不同的功能。

[0050] 图 3 为一种可应用于本发明实施例中的服务器的结构框图。如图 3 所示，服务器 200 包括：存储器 201、处理器 202 以及网络模块 203。可以理解，图 3 所示的结构仅为示意，其并不对本发明实施例中的服务器的结构造成限定。例如，本发明实施例中的服务器还可包括比图 3 中所示更多或者更少的组件，或者具有与图 3 所示不同的配置。另外，本发明实施例中的服务器还可以包括多个具体不同功能的服务器。

[0051] 存储器 201 可用于存储软件程序以及模块，如本发明实施例中的身份验证方法及装置对应的程序指令 / 模块，处理器 202 通过运行存储在存储器 201 内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现本发明实施例中的身份验证方法。存储器 201 可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器 201 可进一步包括相对于处理器 202 远程设置的存储器，这些远程存储器可以通过网络连接至服务器 200。

[0052] 网络模块 203 用于接收以及发送网络信号。上述网络信号可包括无线信号或者有线信号。在一个实例中，上述网络信号为有线网络信号。此时，网络模块 203 可包括处理器、随机存储器、转换器、晶体振荡器等元件。

[0053] 上述的软件程序以及模块还包括操作系统，例如可为 LINUX, UNIX, WINDOWS，其可包括各种用于管理系统任务(例如内存管理、存储设备控制、电源管理等)的软件组件和 / 或驱动，并可与各种硬件或软件组件相互通讯，从而提供其他软件组件的运行环境。

[0054] 下面将结合附图，对本发明实施例提供的身份验证方法、装置进行详细的介绍。

[0055] 第一实施例

[0056] 请参阅图 4，所示为本发明第一实施例提供的一种身份验证方法的流程图。结合图 1，本实施例描述的是用户终端的处理流程，本实施例提供的身份验证方法包括以下步骤：

[0057] 步骤 S11，用户终端在屏幕的预定区域显示验证码，所述验证码包括至少一个可触控图像，所述可触控图像在所述预定区域中的位置与服务器下发的可触控图像坐标相对应。

[0058] 请参照图 5，在一种具体实施方式中，步骤 S11 前可以进一步包括：

[0059] 步骤 S101，所述用户终端向服务器发送验证码生成请求；以及

[0060] 步骤 S102，接收服务器返回的第一验证码生成参数，所述第一验证码生成参数包

括至少一个所述可触控图像坐标。

[0061] 当用户使用用户终端进行发起交易、帐号注册、帐号登录、论坛发帖、微博发言等需要验证身份的敏感操作、或者用户在某时间段内登录某应用次数过多、或者用户异地登录某应用、或者用户登录某应用密码输入错误次数过多等情况发生时，用户终端都可以向服务器发送验证码生成请求。

[0062] 服务器根据验证码生成请求，随机的选取一个或多个可触控图像坐标作为第一验证码生成参数返回给用户终端。可触控图像坐标可以是事先生成的，且每个可触控图像坐标对应一个标准触控操作参数以及预置的验证条件。

[0063] 标准触控操作参数指的是正常用户触控根据该可触控图像坐标生成的可触控图像时用户终端所采集的触控操作参数，也就是说标准触控操作参数是根据经验获得的，并且是可以根据正常用户的历史行为不断修正的，正常用户验证成功后，服务器根据所采集到的触控操作参数生成用户特有的属性，并据此对标准触控操作参数进行修正。标准触控操作参数可以包括：触控操作的位置、所述触控操作的时长、所述触控操作的力度、以及所述触控操作的轨迹中的一种或几种。

[0064] 所述用户终端接收到服务器下发的第一验证码生成参数后，根据所述第一验证码生成参数中的可触控图像坐标，在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0065] 请参照图 6 及图 7，可触控图像可以是内容非常简单的位图或矢量图，以降低生成图像的成本。可触控图像例如可以是如图 6 所示的一个原点或者如图 7 所示的方块等，为了方便用户识别，原点或方块中可以填充有区别于当前页面的填充色，例如黑色等。

[0066] 在另一种具体实施方式中，所述用户终端接收服务器返回的第一验证码生成参数的同时，还接收所述服务器返回的与所述至少一个可触控图像坐标对应的可触控图像。也就是服务器下发第一验证码生成参数的同时也可以下发对应的可触控图像，用户终端只要根据所述第一验证码生成参数中的可触控图像坐标，在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像即可，不需要再生成可触控图像。

[0067] 需要说明的是，如果验证码中包括多个可触控图像，也就是服务器下发了多个可触控图像坐标，用户终端可以将该多个可触控图像显示在屏幕上，也可以根据预定的时间间隔顺序显示。

[0068] 进一步的，第一验证码生成参数还可以包括可触控图像的显示时长，用于指示用户终端将可触控图像显示在所述屏幕的时长。优选的显示时长小于用户终端检测用户触控操作的预定时长。也就是说如果在预定时长内，不管用户终端有没有检测到触控操作，可触控图像都会消失，用户将无法再触摸触控图像，从而可以增加人工恶意破解的难度。

[0069] 进一步的，所述用户终端还可以向用户展示验证提示信息，用以提示用户触控所述验证码中的至少一个可触控图像以进行身份验证。具体的，如果验证码中包括多个可触控图像，验证提示信息可以提示用户同时触控验证码中的多个可触控图像，并提示用户正确的触控手势，例如点击、触摸并持续一定时间、或者围绕可触控图像画圈等。

[0070] 步骤 S12，检测在预定时长内作用于所述预定区域内的触控操作，并获取与所述触控操作对应的触控操作参数。

[0071] 与所述触控操作对应的触控操作参数可以包括：所述触控操作的位置、所述触控

操作的时长、所述触控操作的力度、以及所述触控操作的轨迹中的一种或几种。

[0072] 进一步的，当用户终端获取到与所述触控操作对应的触控操作参数后，可以隐藏所述可触控图像。例如，在图 6 中，当用户触摸图中的黑色圆点并维持一定时间后，用户终端就可以获取到对应的触控操作参数，然后图中的黑色圆点就会消失，这样一方面可以提醒用户哪些可触控图像已经触摸过，另一方面用户无法再对隐藏后的可触控图像进行重新操作，可以提高检测的准确性，并增加人工恶意破解的难度。

[0073] 步骤 S13，将所述触控操作参数发送给服务器，以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证规则，得到验证结果。

[0074] 与所述至少一个可触控图像坐标对应的预置验证条件，例如可以包括：所获取的触控操作参数与对应的标准触控操作参数之间的差值小于第一预定阈值，如果满足所述预置验证条件则验证结果为通过，如果不满足所述预置验证条件，则验证结果为不通过。

[0075] 服务器还可以将验证结果返回用户终端展示给用户。

[0076] 本发明实施例中，验证码由一个或多个可触控图像组成，可触控图像的具体内容可以很简单，例如可以是一个圆点或者是一个方块等，可以降低成本，可触控图像在屏幕区域中的位置与服务器下发的可触控图像坐标相对应，可以增加人工收集验证码作为破解题库的难度；充分利用了人类对位置判断的先天优势，用户可以通过触摸显示在屏幕上的可触控图像进行身份验证，用户终端将采集到的触控操作参数发送给服务器，由服务器根据触控操作参数以及与每个可触控图像对应的预置验证条件来得到验证结果，只有触控操作参数满足对应的预置验证条件时，才判定身份验证通过，大大增加了机器破解验证码的难度，安全性高；相对于点选验证码来说，不需要用户根据问题对图片进行类别辨识，只要用户触摸验证码中的所有可触控图像即可，降低了用户的使用门槛。也就是说本发明在不影响用户体验的前提下可以大大提高验证码的抗破解力，有效的提高了用户验证的安全性。

[0077] 第二实施例

[0078] 图 8 为本发明第二实施例中的一种身份验证方法的流程示意图。请结合图 1，该实施例描述的是用户终端的处理流程，本实施例中的身份验证方法包括：

[0079] 步骤 S21，用户终端向服务器发送验证码生成请求。

[0080] 步骤 S22，接收服务器返回的第一验证码生成参数，所述第一验证码生成参数包括至少一个可触控图像坐标。

[0081] 步骤 S23，根据所述第一验证码生成参数中的可触控图像坐标，在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0082] 步骤 S24，检测在预定时长内作用于所述预定区域内的触控操作，并获取与所述触控操作对应的触控操作参数。

[0083] 步骤 S25，将所述触控操作参数发送给服务器，以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件，得到验证结果。

[0084] 步骤 S26，当所述服务器判定验证结果为不通过或者验证的次数未达到预定次数时，接收所述服务器根据预置的验证码下发规则返回的第二验证码生成参数，所述第二验证码生成参数包括至少一个可触控图像坐标。

[0085] 在一种具体实施方式中，如果验证结果为失败，服务器可以根据预置的验证码下发规则向用户终端返回第二验证码生成参数，直到验证结果为通过为止。在另一种具体实

施方式中,不管结果是否为通过,只要验证的次数未达到预定的次数(例如三次),服务器都可以根据预置的验证码下发规则向用户终端返回第二验证码生成参数,直到验证的次数达到预定的次数为止。

[0086] 步骤S27,根据所述第二验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0087] 重复步骤S24至步骤S25,直到验证结果为通过或者验证的次数达到预定的次数,也就是可以进行多轮验证。

[0088] 具体的,所述预置的验证码下发规则可以包括:如果所述服务器判定验证结果为不通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级;或者如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级;或者如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为通过,则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级不受限制。

[0089] 进一步的,可以通过调整可触控图像坐标的个数、位置关系、显示时长等将第二轮验证码的难度等级提高。具体的,当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时,所述第二验证码生成参数中的可触控图像坐标的个数可以大于所述第一验证码生成参数中的可触控图像坐标的个数;或者所述第二验证码生成参数中的多个可触控图像坐标之间的间隔可以大于所述第一验证码生成参数中的可触控图像坐标之间的间隔;或者所述第二验证码生成参数中的可触控图像的显示时长可以小于所述第一验证码生成参数中的可触控图像的显示时长。或者同时调整可触控图像坐标的个数、位置关系以及显示时长以增加验证难度。

[0090] 优选的,验证次数不超过三次,也就是说,如果第三轮验证结果还是失败,就不再进行验证,相应的,服务器也不会处理用户所请求的相关业务。

[0091] 与前述实施例相同,本实施例中的验证码,在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性,另外,本实施例中服务器可以在判定验证不通过的情况下,下发新的验证码生成参数,生成难度等级更高的验证码,也就是说对用户进行多轮验证,一方面可以给用户再一次进行验证的机会,另一方面通过多轮验证可以增加码工破解的成本,进一步提高安全性。

[0092] 第三实施例

[0093] 图9为本发明第三实施例中的一种身份验证方法的流程示意图。请结合图1,该实施例描述的是服务器的处理流程,本实施例中的身份验证方法包括:

[0094] 步骤S31,服务器接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数,所述预定范围内显示有验证码,所述验证码包括至少一个可触控图像,所述可触控图像在所述预定区域中的位置与所述服务器下发的可触控图像坐标相对应。

[0095] 步骤S32,根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0096] 请参照图10,在一种具体实施方式中,步骤S31之前,还包括:

- [0097] 步骤 S301,接收所述用户终端发送的验证码生成请求;以及
[0098] 步骤 S302,根据所述验证码生成请求随机获取第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标;以及
[0099] 步骤 S303,将所述第一验证码生成参数返回所述用户终端。

[0100] 在另一种具体实施方式中,所述服务器将所述第一验证码生成参数返回所述用户终端的同时,还向所述用户终端返回与所述至少一个可触控图像坐标对应的可触控图像。
[0101] 与前述实施例相同,本实施例中的验证码,在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性。

[0102] 第四实施例

[0103] 图 11 为本发明第四实施例中的一种身份验证方法的流程示意图。请结合图 1,该实施例描述的是服务器的处理流程,本实施例中的身份验证方法包括:

[0104] 步骤 S41,服务器接收用户终端发送的验证码生成请求;

[0105] 步骤 S42,根据所述验证码生成请求随机获取第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标;

[0106] 步骤 S43,将所述第一验证码生成参数返回所述用户终端,以使用户终端根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的可触控图像;

[0107] 步骤 S44,接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数;

[0108] 步骤 S45,根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0109] 步骤 S46,根据所述验证结果或者验证的次数,判断是否需要向所述用户终端返回第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标。

[0110] 在一种具体实施方式中,如果验证结果为失败,服务器可以向用户终端返回第二验证码生成参数,直到验证结果为通过为止。在另一种具体实施方式中,不管结果是否为通过,只要验证的次数未达到预定的次数(例如三次),服务器都可以向用户终端返回第二验证码生成参数,直到验证的次数达到预定的次数为止。如果验证的次数达到预定的次数,服务器可以根据每次的验证结果得到总的验证结果,例如三次验证结果均为通过,总的验证结果也为通过,如果三次验证结果均为不通过,总的验证结果也为不通过,如果两次通过、一次失败,总的验证结果可以为通过,等等。具体实施时,可以根据实际情况来指定具体的判断规则,本发明并不以此为限。

[0111] 步骤 S47,如果所述服务器判定验证结果为不通过或者验证的次数未达到预定次数,则根据预置的验证码下发规则向所述用户终端返回第二验证码生成参数。

[0112] 重复步骤 S44 至 S45,直到验证结果为通过或者验证的次数达到预定的次数。

[0113] 预置的验证码下发规则可以参照第二实施例中的相关内容,这里不再赘述。

[0114] 与前述实施例相同,本实施例中的验证码,在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性,另外,本实施例中服务器可以在判定验证不通过的情况下,下发新的验证码生成参数,生成难度等级更高的验证码,也就是说对用户进行多轮验证,一方面可以给用户再一次进行验证的机会,另一方面通过多轮验

证可以增加码工破解的成本,进一步提高安全性。

[0115] 第五实施例

[0116] 请参阅图 12,所示为本发明第五实施例提供的一种身份验证方法的流程图。结合图 1,该实施例描述的是用户终端与服务器之间的交互处理流程。本实施例中的身份验证方法可以包括:

[0117] 步骤 S501,用户终端向服务器发送验证码生成请求。

[0118] 步骤 S502,服务器根据所述验证码生成请求随机获取第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标。

[0119] 步骤 S503,服务器将第一验证码生成参数返回给用户终端。

[0120] 步骤 S504,用户终端根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0121] 步骤 S505,用户终端检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数。

[0122] 步骤 S506,用户终端将所述触控操作参数发送给服务器。

[0123] 步骤 S507,服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0124] 步骤 S508,服务器根据所述验证结果或者验证的次数,判断是否需要向所述用户终端返回第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标。

[0125] 步骤 S509,如果所述服务器判定验证结果为不通过或者验证的次数未达到预定次数,服务器则根据预置的验证码下发规则向所述用户终端返回第二验证码生成参数。

[0126] 步骤 S510,用户终端根据所述第二验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0127] 与前述实施例相同,本实施例中的验证码,在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性,另外,本实施例中服务器可以在判定验证不通过的情况下,下发新的验证码生成参数,生成难度等级更高的验证码,也就是说对用户进行多轮验证,一方面可以给用户再一次进行验证的机会,另一方面通过多轮验证可以增加码工破解的成本,进一步提高安全性。

[0128] 第六实施例

[0129] 图 13 为本发明第六实施例提供的一种身份验证装置的结构示意图。请参照图 13,本实施例提出的装置可运行于用户终端,用于实现上述实施例提出的身份验证方法,所述用户终端具有触控屏幕,本实施例中的装置 60 可以包括:

[0130] 显示模块 61,用于在屏幕的预定区域显示验证码,所述验证码包括至少一个可触控图像;

[0131] 检测模块 62,用于检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数;以及

[0132] 第一发送模块 63,用于将所述触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0133] 进一步的,请参照图 14,于一种具体实施方式中,所述装置 60 还可以包括:

[0134] 第二发送模块 64,用于向所述服务器发送验证码生成请求;以及

[0135] 第一接收模块 65,用于接收服务器返回的第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标。

[0136] 所述显示模块 61 还用于根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0137] 于另一种具体实施方式中,所述第一接收模块 65 接收服务器返回的第一验证码生成参数的同时,还接收所述服务器返回的与所述至少一个可触控图像坐标对应的可触控图像,所述显示模块 61 还用于根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0138] 进一步的,所述显示模块 61 显示所述至少一个可触控图像在所述屏幕的时长可以小于所述检测模块 62 检测触控操作时所依据的预定时长。进一步的,当所述检测模块 62 获取到与所述触控操作对应的触控操作参数后,所述显示模块 61 隐藏所述可触控图像。具体的,触控操作参数可以包括:所述触控操作的位置、所述触控操作的时长、所述触控操作的力度、以及所述触控操作的轨迹中的一种或几种。

[0139] 以上各模块可以是由软件代码实现,此时,上述的各模块可存储于用户终端的存储器内。以上各模块同样可以由硬件例如集成电路芯片实现。

[0140] 需要说明的是,本发明实施例的用户终端的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,在此不赘述。

[0141] 本实施例中的身份验证装置在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性。

[0142] 第七实施例

[0143] 图 15 为本发明第七实施例提供的一种身份验证装置的结构示意图。请参照图 15,本实施例提出的装置可运行于用户终端,用于实现上述实施例提出的身份验证方法,所述用户终端具有触控屏幕,本实施例中的装置 70 可以包括:

[0144] 第二发送模块 71,用于向所述服务器发送验证码生成请求;

[0145] 第一接收模块 72,用于接收服务器返回的第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标。

[0146] 显示模块 73,用于根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0147] 检测模块 74,用于检测在预定时长内作用于所述预定区域内的触控操作,并获取与所述触控操作对应的触控操作参数;以及

[0148] 第一发送模块 75,用于将所述触控操作参数发送给服务器,以使所述服务器根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。

[0149] 第二接收模块 76,当所述服务器判定验证结果为不通过或者验证的次数未达到预定次数时,用于接收所述服务器根据预置的验证码下发规则返回的第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标。

[0150] 显示模块 73 还用于根据所述第二验证码生成参数中的可触控图像坐标,在屏幕

的预定区域生成并显示与至少一个所述可触控图像坐标对应的所述可触控图像。

[0151] 所述预置的验证码下发规则可以包括：

[0152] 如果所述服务器判定验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级；或者

[0153] 如果验证的次数未达到预定次数、且所述服务器判定当前轮次的验证结果为不通过，则所述服务器向所述用户终端返回的第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级。

[0154] 当所述第二验证码生成参数所对应的难度等级高于所述第一验证码生成参数所对应的难度等级时，所述第二验证码生成参数中的可触控图像坐标的个数大于所述第一验证码生成参数中的可触控图像坐标的个数；或者所述第二验证码生成参数中的多个可触控图像坐标之间的间隔大于所述第一验证码生成参数中的可触控图像坐标之间的间隔。

[0155] 以上各模块可以是由软件代码实现，此时，上述的各模块可存储于用户终端的存储器内。以上各模块同样可以由硬件例如集成电路芯片实现。

[0156] 需要说明的是，本发明实施例的用户终端的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，在此不赘述。

[0157] 与前述实施例相同，本实施例中的验证码，在不影响用户体验的前提下可以大大提高验证码的抗破解力，有效的提高了用户验证的安全性，另外，本实施例中服务器可以在判定验证不通过的情况下，下发新的验证码生成参数，生成难度等级更高的验证码，也就是说对用户进行多轮验证，一方面可以给用户再一次进行验证的机会，另一方面通过多轮验证可以增加码工破解的成本，进一步提高安全性。

[0158] 第八实施例

[0159] 图 16 为本发明第八实施例提供的一种身份验证装置的结构示意图。请参照图 16，本实施例提出的装置可运行于服务器，可以用于实现上述实施例提出的身份验证方法，包括：所述装置 80 包括：

[0160] 第一接收模块 81，用于接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数，所述预定范围内显示有验证码，所述验证码包括至少一个可触控图像；以及

[0161] 验证模块 82，用于根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件，得到验证结果。

[0162] 具体的，每个所述可触控图像坐标对应一个标准触控操作参数，与所述至少一个可触控图像坐标对应的预置验证条件包括：所获取的触控操作参数与对应的标准触控操作参数之间的差值小于预定阈值，如果满足所述预置验证条件则所述验证模块判定验证结果为通过，如果不满足所述预置验证条件，则所述验证模块判定验证结果为不通过。

[0163] 请参照图 17，所述装置 80 还可以包括：

[0164] 第二接收模块 83，用于接收所述用户终端发送的验证码生成请求；以及

[0165] 参数生成模块 84，用于根据所述验证码生成请求随机获取第一验证码生成参数，所述第一验证码生成参数包括至少一个可触控图像坐标；以及

- [0166] 第一发送模块 85,用于将所述第一验证码生成参数返回所述用户终端。
- [0167] 于本发明的另一种具体实施方式中,所述第一发送模块 85 将所述第一验证码生成参数返回所述用户终端的同时,还向所述用户终端返回与所述至少一个可触控图像坐标对应的可触控图像。
- [0168] 以上各模块可以是由软件代码实现,此时,上述的各模块可存储于服务器的存储器内。以上各模块同样可以由硬件例如集成电路芯片实现。
- [0169] 需要说明的是,本发明实施例的服务器的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,在此不赘述。
- [0170] 与前述实施例相同,本实施例中的身份验证装置在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性。
- [0171] 第九实施例
- [0172] 图 18 为本发明第九实施例提供的一种身份验证装置的结构示意图。请参照图 18,本实施例提出的装置可运行于服务器,可以用于实现上述实施例提出的身份验证方法,包括 :所述装置 90 包括 :
- [0173] 第二接收模块 91,用于接收所述用户终端发送的验证码生成请求;
- [0174] 参数生成模块 92,用于根据所述验证码生成请求随机获取第一验证码生成参数,所述第一验证码生成参数包括至少一个可触控图像坐标;
- [0175] 第一发送模块 93,用于将所述第一验证码生成参数返回所述用户终端,以使用户终端根据所述第一验证码生成参数中的可触控图像坐标,在屏幕的预定区域显示与至少一个所述可触控图像坐标对应的可触控图像;
- [0176] 第一接收模块 94,用于接收用户终端返回的、在预定时长内检测到的作用于所述用户终端屏幕预定区域内的触控操作所对应的触控操作参数;
- [0177] 验证模块 95,用于根据所述触控操作参数以及与所述至少一个可触控图像坐标对应的预置验证条件,得到验证结果。
- [0178] 判断模块 96,用于根据所述验证结果或者验证的次数,判断是否需要向所述用户终端返回第二验证码生成参数,所述第二验证码生成参数包括至少一个可触控图像坐标。
- [0179] 第二发送模块 97,如果所述服务器判定验证结果为不通过或者验证的次数未达到预定次数,则所述第二发送模块 97 根据预置的验证码下发规则向所述用户终端返回第二验证码生成参数。
- [0180] 以上各模块可以是由软件代码实现,此时,上述的各模块可存储于服务器的存储器内。以上各模块同样可以由硬件例如集成电路芯片实现。
- [0181] 需要说明的是,本发明实施例的服务器的各功能模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,在此不赘述。
- [0182] 与前述实施例相同,本实施例中的验证码,在不影响用户体验的前提下可以大大提高验证码的抗破解力,有效的提高了用户验证的安全性,另外,本实施例中服务器可以在判定验证不通过的情况下,下发新的验证码生成参数,生成难度等级更高的验证码,也就是说对用户进行多轮验证,一方面可以给用户再一次进行验证的机会,另一方面通过多轮验证可以增加码工破解的成本,进一步提高安全性。
- [0183] 第十实施例

[0184] 图 19 为本发明第十实施例中的身份验证系统的结构框图。请参照图 19, 本实施例提出的身份验证系统 10 可以用于实现上述实施例提出的身份验证方法, 本实施例中的身份验证系统 10 可以包括: 用户终端 11 以及服务器 12, 用户终端 11 可以是第六或第七实施例中的用户终端, 服务器 12 可以是第八或第九实施例中的服务器。

[0185] 需要说明的是, 本说明书中的各个实施例均采用递进的方式描述, 每个实施例重点说明的都是与其他实施例的不同之处, 各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言, 由于其与方法实施例基本相似, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。

[0186] 需要说明的是, 在本文中, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含, 从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下, 由语句“包括一个……”限定的要素, 并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0187] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成, 也可以通过程序来指令相关的硬件完成, 该的程序可以存储于一种计算机可读存储介质中, 上述提到的存储介质可以是只读存储器, 磁盘或光盘等。

[0188] 以上所述, 仅是本发明的较佳实施例而已, 并非对本发明作任何形式上的限制, 虽然本发明已以较佳实施例揭露如上, 然而并非用以限定本发明, 任何熟悉本专业的技术人员, 在不脱离本发明技术方案范围内, 当可利用上述揭示的技术内容做出些许更动或修饰为等同变化的等效实施例, 但凡是未脱离本发明技术方案内容, 依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰, 均仍属于本发明技术方案的范围内。

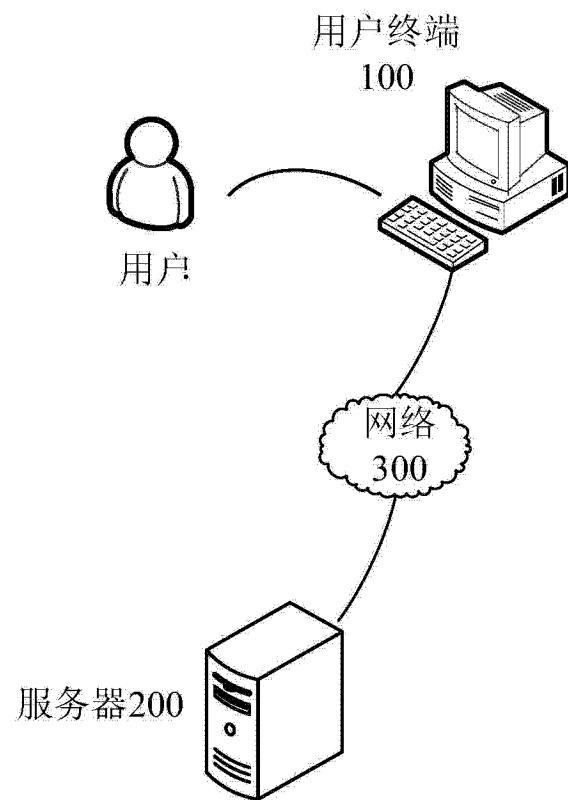


图 1

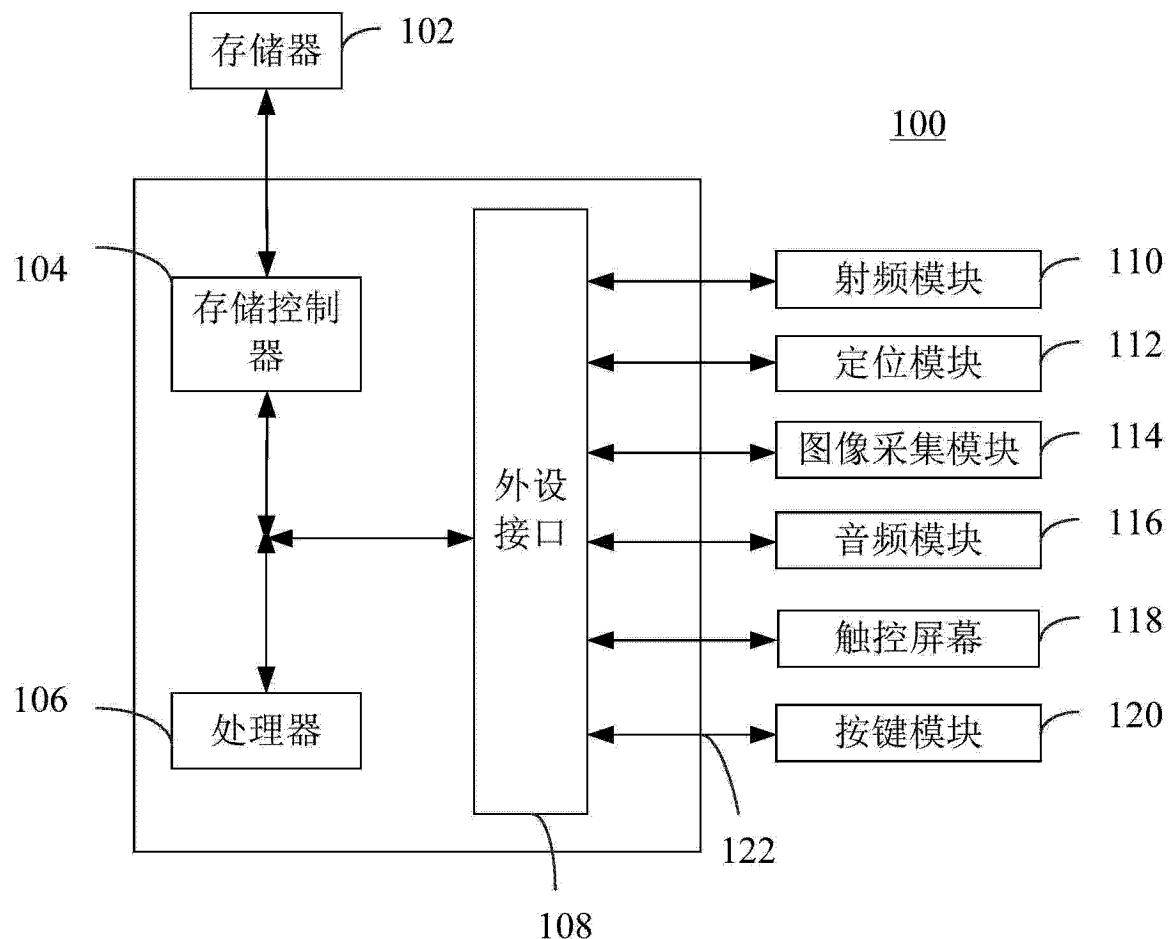


图 2

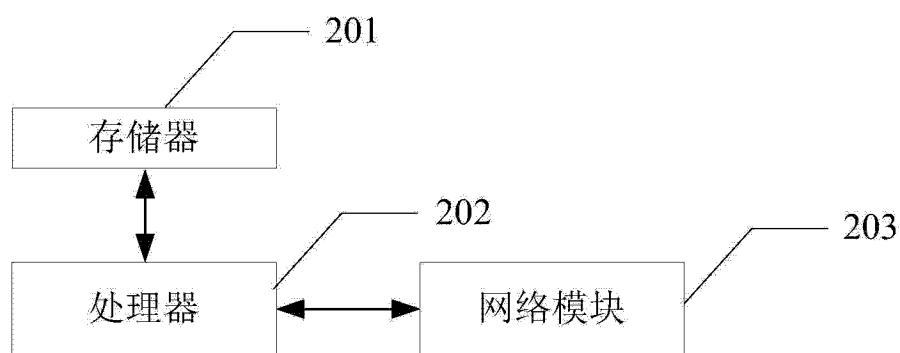
200

图 3

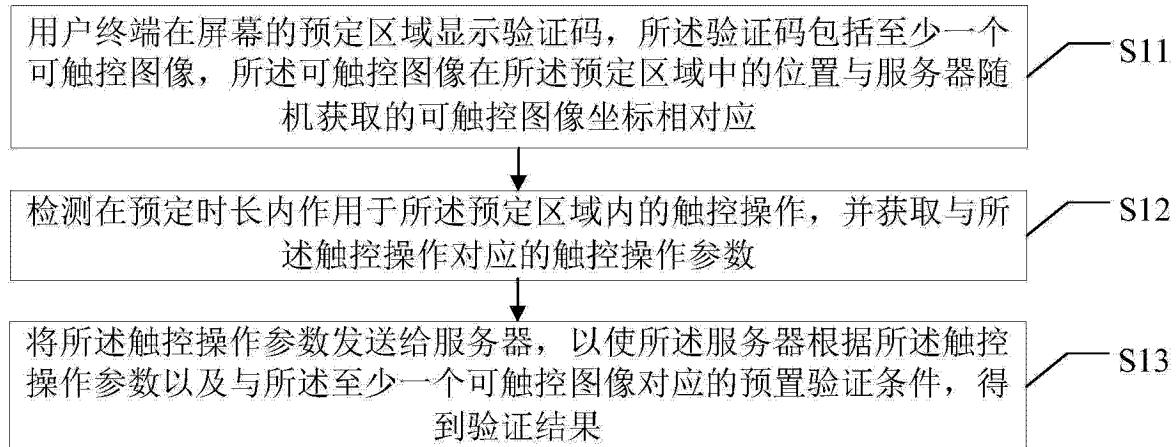


图 4

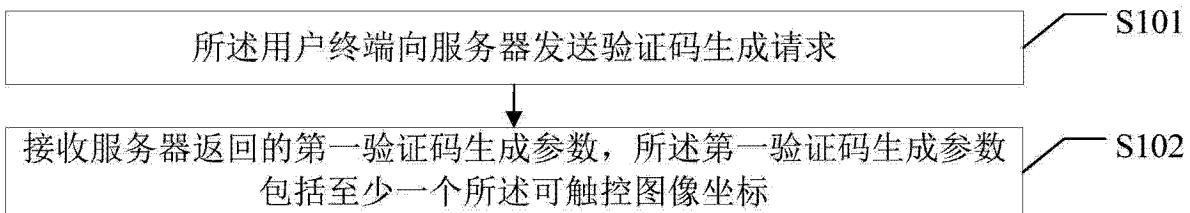


图 5

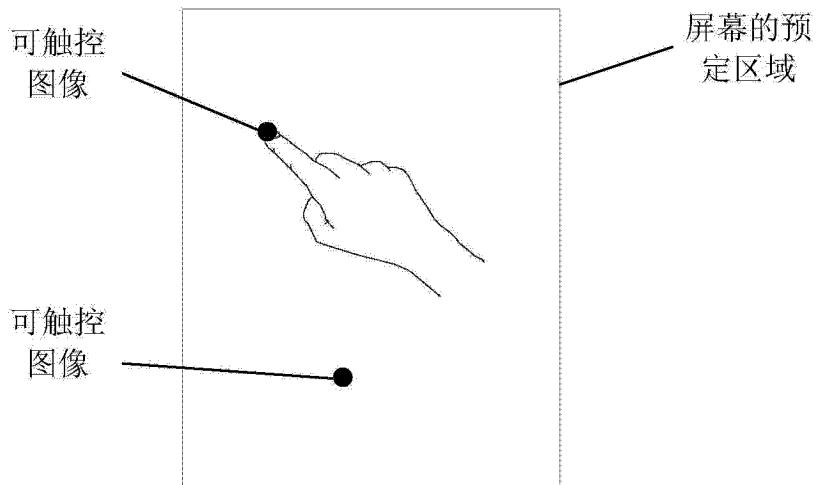


图 6

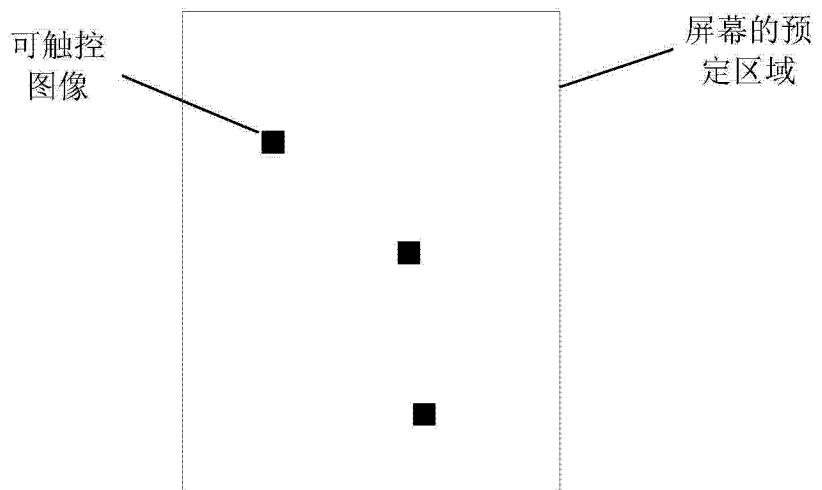


图 7

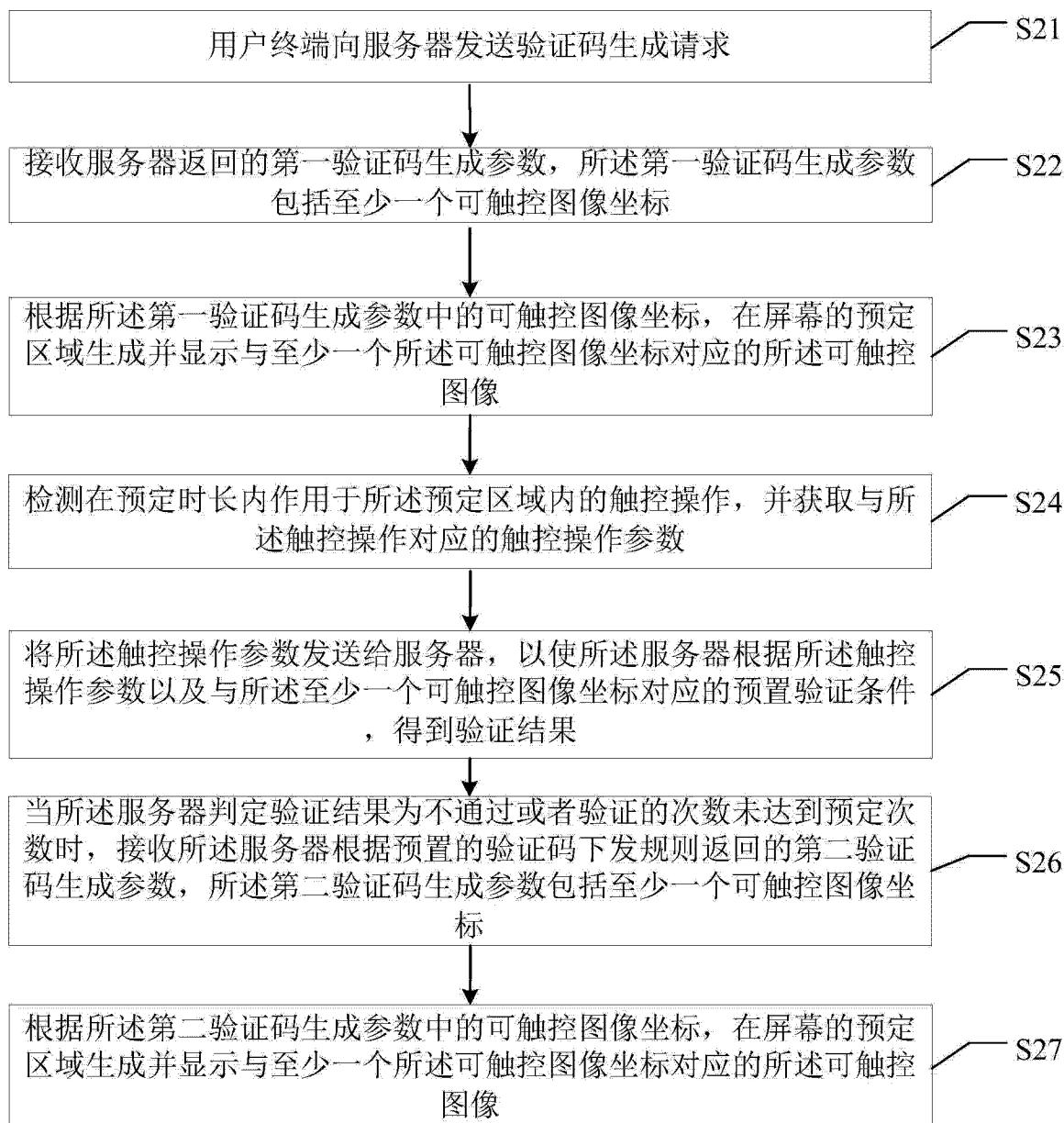


图 8

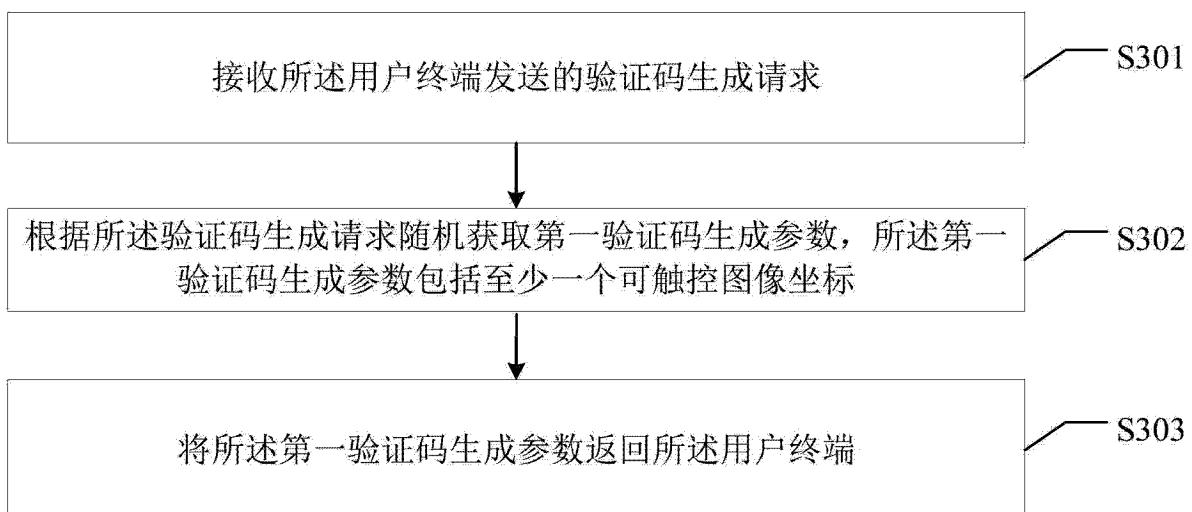
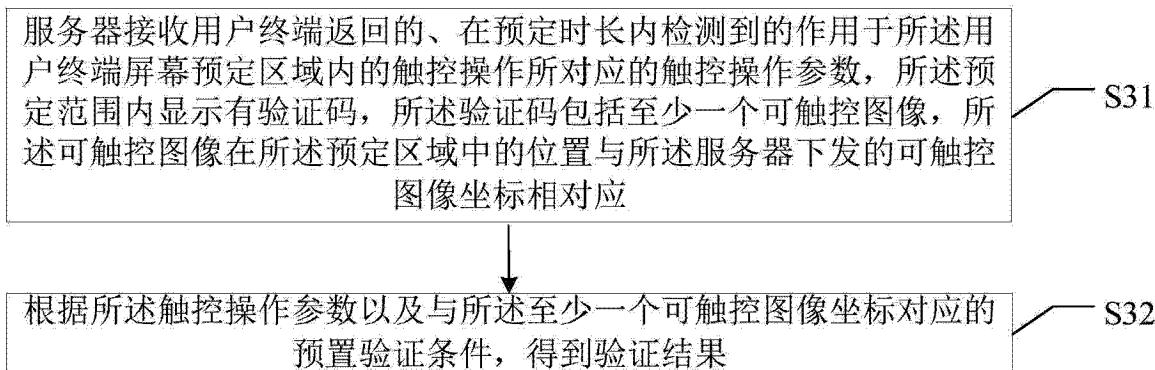




图 11

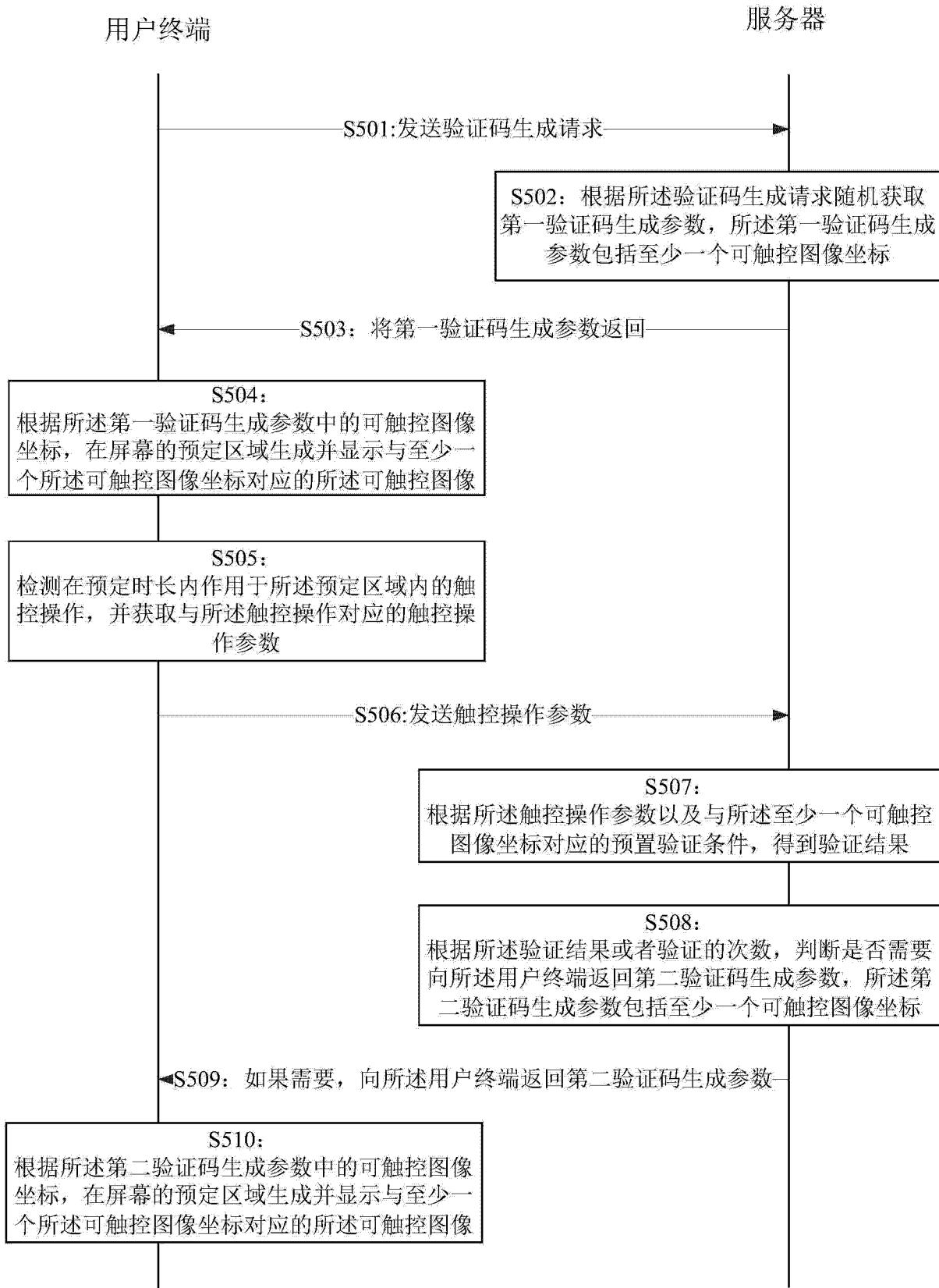


图 12

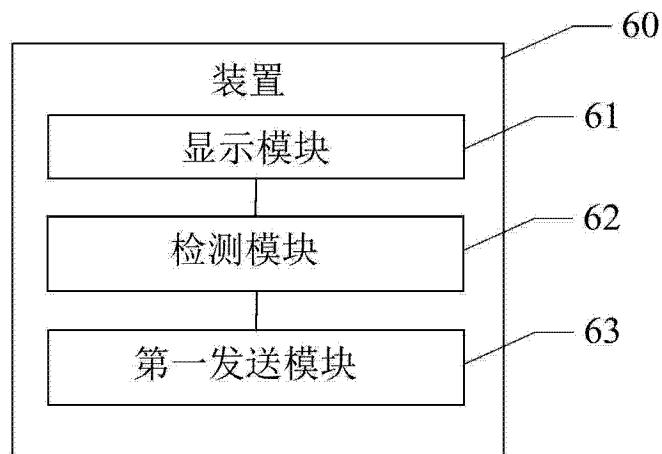


图 13

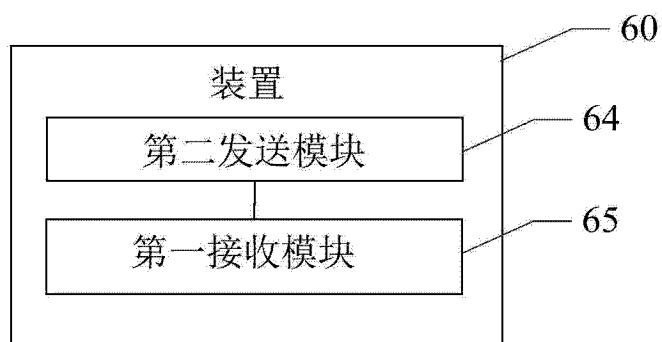


图 14

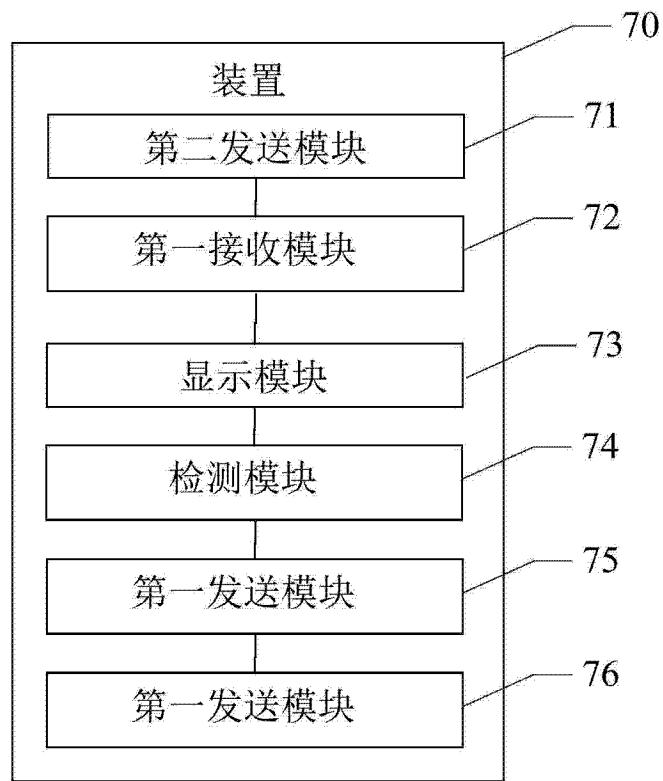


图 15

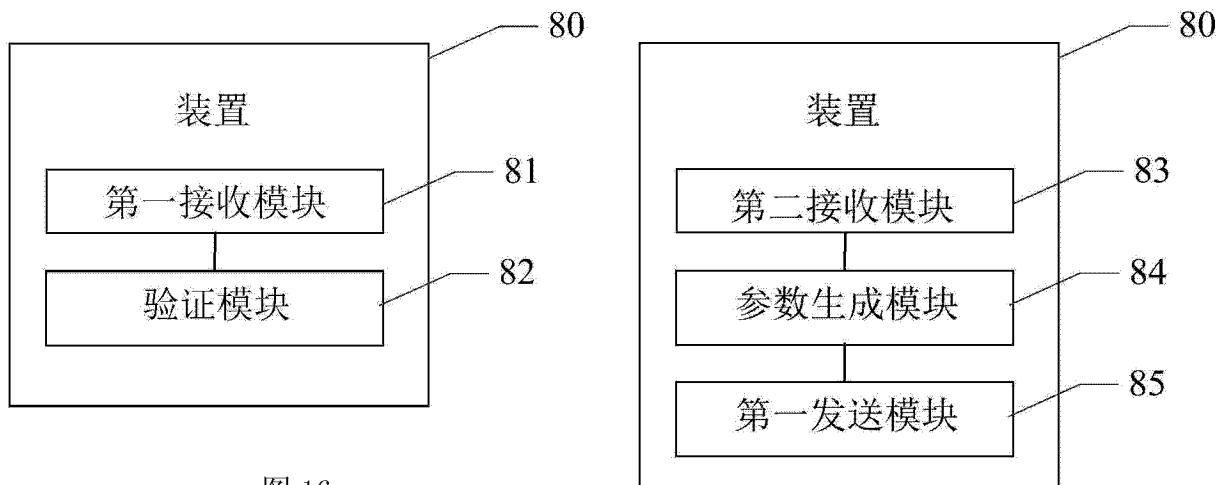


图 16

图 17

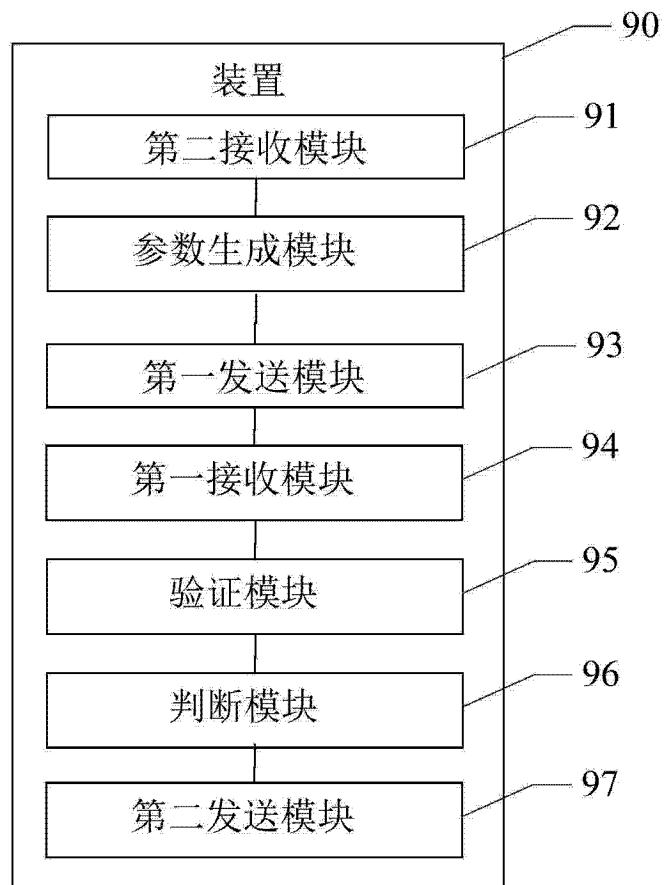


图 18

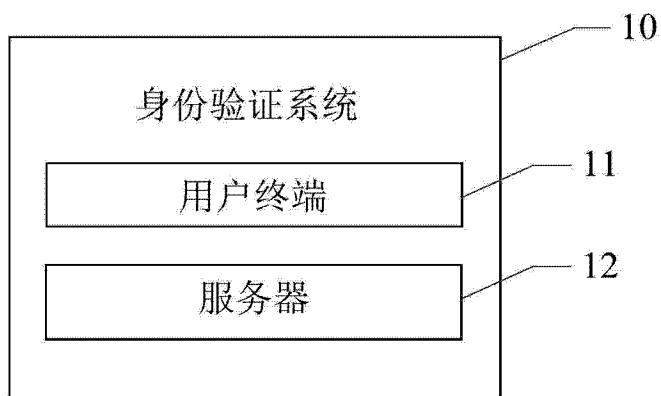


图 19