



(12) 发明专利

(10) 授权公告号 CN 101159715 B

(45) 授权公告日 2010. 11. 10

(21) 申请号 200710188308. 3

US 6253328 B1, 2001. 06. 26, 全文 .

(22) 申请日 2007. 11. 16

CN 1937500 A, 2007. 03. 28, 全文 .

(73) 专利权人 腾讯科技 (深圳) 有限公司

审查员 文娟

地址 518044 广东省深圳市福田区振兴路赛格科技园 2 栋东 410 室

(72) 发明人 陈坚 蔡耿平

(74) 专利代理机构 北京德琦知识产权代理有限公司 11018

代理人 谢安昆 宋志强

(51) Int. Cl.

H04L 12/58 (2006. 01)

H04L 9/00 (2006. 01)

H04L 29/06 (2006. 01)

G06F 17/30 (2006. 01)

(56) 对比文件

WO 2007/089356 A2, 2007. 08. 09, 全文 .

CN 1365055 A, 2002. 08. 21, 全文 .

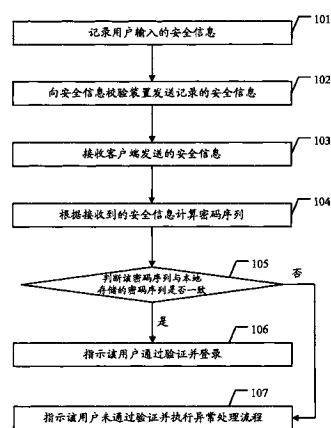
权利要求书 2 页 说明书 9 页 附图 4 页

(54) 发明名称

一种安全信息校验方法及安全信息校验装置以及客户端

(57) 摘要

本发明公开了一种安全信息校验方法及安全信息校验装置以及客户端,用于提高用户信息的安全性,同时提高用户体验。本发明方法包括:接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息;判断所述安全信息是否合法,若合法,则指示所述用户通过验证。本发明还提供一种安全信息校验装置以及客户端。本发明可以有效地提高用户信息的安全性,同时提高用户体验。



1. 一种安全信息校验方法,其特征在于,包括:

接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息,所述轨迹校验点信息为用户通过轨迹输入设备在校验点矩阵中输入的轨迹所经过的校验点的坐标,所述校验点触发信息为用户通过轨迹输入设备在校验点矩阵中点击的校验点的标识以及点击次数;

根据所述轨迹校验点信息和/或校验点触发信息计算密码序列;

判断所述密码序列与本地存储的密码序列是否一致,若一致,则指示所述用户通过验证。

2. 根据权利要求1所述的方法,其特征在于,所述接收客户端发送的安全信息的步骤之前包括:

记录用户输入的轨迹校验点信息和/或校验点触发信息,所述轨迹校验点信息和/或校验点触发信息为用户根据本地预置的登录信息,通过轨迹输入设备输入的;

发送包含所述轨迹校验点信息和/或校验点触发信息的安全信息。

3. 根据权利要求2所述的方法,其特征在于,所述记录用户输入的轨迹校验点信息和/或校验点触发信息的步骤之前包括:

获取本地预置的登录信息的属性;

判断所述属性中的有效期是否超过预置期限,若超过,则发起登录信息更新请求,并接收预置网元反馈的登录信息;

用所述接收到的登录信息替换本地保存的登录信息。

4. 根据权利要求2或3所述的方法,其特征在于,所述轨迹输入设备为鼠标,或手柄,或触摸板;

所述记录用户输入的轨迹校验点信息和/或校验点触发信息的步骤包括:

根据所述登录信息生成包含若干个校验点的矩阵;

记录用户通过鼠标,或手柄,或触摸板在所述矩阵中输入的轨迹所经过的校验点,将所述校验点的坐标作为所述轨迹校验点信息;

并记录用户通过鼠标,或手柄,或触摸板在所述矩阵中点击的校验点的标识以及点击次数,将所述校验点的标识以及点击次数作为校验点触发信息。

5. 根据权利要求4所述的方法,其特征在于,所述根据登录信息生成包含若干个校验点的矩阵的步骤包括:

获取登录信息中的矩阵维数信息以及间距生成参数;

根据矩阵维数信息确定矩阵的行数和列数;

按照所述行数和列数分配校验点;

根据所述间距生成参数调整所述矩阵中相邻校验点之间的距离以生成包含若干个校验点的矩阵。

6. 一种安全信息校验装置,其特征在于,包括:

安全信息接收单元,用于接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息,所述轨迹校验点信息为用户通过轨迹输入设备在校验点矩阵中输入的轨迹所经过的校验点的坐标,所述校验点触发信息为用户通过轨迹输入设备在校验点矩阵中点击的校验点的标识以及点击次数;

安全信息校验单元,用于判断所述安全信息是否合法,若合法,则指示所述用户通过验证;

所述安全信息校验单元包括:

密码序列计算单元,用于根据所述轨迹校验点信息和 / 或校验点触发信息计算密码序列;

密码序列判断单元,用于判断所述密码序列与本地存储的密码序列是否一致;

校验指示单元,当密码序列与本地存储的密码序列一致时,指示所述用户通过验证,当密码序列与本地存储的密码序列不一致时,指示所述用户未通过验证。

7. 根据权利要求 6 所述的安全信息校验装置,其特征在于,所述安全信息校验装置还包括:

登录信息反馈单元,用于接收客户端发起的登录信息更新请求,向所述客户端反馈本地的登录信息。

8. 一种客户端,其特征在于,包括:

安全信息记录单元,用于记录用户输入的轨迹校验点信息和 / 或校验点触发信息,所述轨迹校验点信息和 / 或校验点触发信息为用户根据本地预置的登录信息,通过轨迹输入设备输入的;

安全信息发送单元,用于向安全信息校验装置发送包含所述轨迹校验点信息和 / 或校验点触发信息的安全信息;

所述安全信息记录单元包括:

矩阵生成单元,用于根据本地存储的登录信息生成包含若干个校验点的矩阵;

轨迹记录单元,用于记录用户通过鼠标,或手柄,或触摸板在所述矩阵中输入的轨迹所经过的校验点,将所述校验点的坐标作为所述轨迹校验点信息;

触发记录单元,用于记录用户通过鼠标,或手柄,或触摸板在所述矩阵中点击的校验点的标识以及点击次数,将所述校验点的标识以及点击次数作为校验点触发信息。

9. 根据权利要求 8 所述的客户端,其特征在于,所述客户端还包括:

登录信息校验单元,用于获取本地预置的登录信息的属性,判断所述属性中的有效期是否超过预置期限;

登录信息更新单元,用于当所述属性中的有效期超过预置期限时,向安全信息校验装置发送登录信息更新请求,并接收安全信息校验装置反馈的登录信息,利用接收到的登录信息替换本地保存的登录信息。

一种安全信息校验方法及安全信息校验装置以及客户端

技术领域

[0001] 本发明涉及信息安全领域,尤其涉及一种安全信息校验方法及安全信息校验装置以及客户端。

背景技术

[0002] 随着网络技术的发展,网络即时通讯(IM, Instant Message)工具逐渐被大多数用户所接受,已经成为用户必不可少的软件工具。因此用户对IM软件的易用性,稳定性,安全性等方面提出了较高的要求。

[0003] 在IM软件中,每个用户都会关联一个用户账号,用户账号信息保存着用户很多基本属性和重要信息。用户登录进行身份验证是使用IM软件的必要条件,只有经过身份验证才能正常使用IM软件的功能,才能维护用户的账号信息。

[0004] 现有技术中一种安全信息校验方法为:用户登录进行身份验证时都是基于键盘密码输入的方式,从键盘输入各种字符,服务器端将用户输入的字符与本地存储的正确密码进行比较,若一致,则校验通过,允许用户登录,若不一致,则拒绝用户登录。

[0005] 但是现有技术中,由于采用字符作为密码,所以用户为了提高密码的安全性,往往会设置比较长的字符串,同时为了方便记忆,用户很有可能会使用一些容易记忆的单词或信息作为字符串的一部分,由于字符数量的限制(即字符的总数量是有限的),再加上用户可能采用容易记忆的单词或信息作为字符串的一部分,因此增加了密码被暴力破解的可能,进而降低了用户信息的安全性。

[0006] 现有技术中一种安全信息校验方法为:用户登录进行身份验证时,不仅需要从键盘输入密码,同时也需要输入由服务器端随机分配的一个验证码,该验证码采用明码显示,用户需要按照该验证码,在特定的文本框内填入相同的内容才能够完成登录,所以在一定程度上避免了密码被暴力破解的可能。

[0007] 但是,在上述现有技术中,服务器端为了避免明码显示的验证码被非法的截图程序从登录界面直接截取分析出验证码,所以会在验证码处加入很多干扰因素,例如将验证码变成扭曲的字符,或者是加入杂乱无章的颜色作为验证码的底色,这样就可能会使得用户在某些情况下自己都无法清楚的识别验证码,从而降低了用户体验。

发明内容

[0008] 本发明实施例要解决的技术问题是提供一种安全信息校验方法及安全信息校验装置以及客户端,能够提高用户信息的安全性,同时提高用户体验。

[0009] 本发明实施例提供的安全信息校验方法,包括:接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息;判断所述安全信息是否合法,若合法,则指示所述用户通过验证。

[0010] 可选地,所述接收客户端发送的安全信息的步骤之前包括:

[0011] 记录用户输入的轨迹校验点信息和/或校验点触发信息,所述轨迹校验点信息和

/ 或校验点触发信息为用户根据本地预置的登录信息,通过轨迹输入设备输入的;发送包含所述轨迹校验点信息和 / 或校验点触发信息的安全信息。

[0012] 可选地,所述记录用户输入的轨迹校验点信息和 / 或校验点触发信息的步骤之前包括:获取本地预置的登录信息的属性;判断所述属性中的有效期是否超过预置期限,若超过,则发起登录信息更新请求,并接收预置网元反馈的登录信息;用所述接收到的登录信息替换本地保存的登录信息。

[0013] 可选地,所述轨迹输入设备为鼠标,或手柄,或触摸板;

[0014] 所述记录用户输入的轨迹校验点信息和 / 或校验点触发信息的步骤包括:根据所述登录信息生成包含若干个校验点的矩阵;记录用户通过鼠标,或手柄,或触摸板在所述矩阵中输入的轨迹所经过的校验点,将所述校验点的坐标作为所述轨迹校验点信息;并记录用户通过鼠标,或手柄,或触摸板在所述矩阵中点击的校验点的标识以及点击次数,将所述校验点的标识以及点击次数作为校验点触发信息。

[0015] 可选地,所述根据登录信息生成包含若干个校验点的矩阵的步骤包括:获取登录信息中的矩阵维数信息以及间距生成参数;根据矩阵维数信息确定矩阵的行数和列数;按照所述行数和列数分配校验点;根据所述间距生成参数调整所述矩阵中相邻校验点之间的距离以生成包含若干个校验点的矩阵。

[0016] 可选地,所述判断所述安全信息是否合法的步骤包括:

[0017] 根据所述轨迹校验点信息和 / 或校验点触发信息计算密码序列;判断所述密码序列与本地存储的密码序列是否一致,若一致,则确定所述安全信息合法。本发明实施例提供的的安全信息校验装置,包括:安全信息接收单元,用于接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和 / 或校验点触发信息;安全信息校验单元,用于判断所述安全信息是否合法,若合法,则指示所述用户通过验证。

[0018] 可选地,所述安全信息校验装置还包括:

[0019] 登录信息反馈单元,用于接收客户端发起的登录信息更新请求,向所述客户端反馈本地的登录信息。

[0020] 可选地,所述安全信息校验单元包括:

[0021] 密码序列计算单元,用于根据所述轨迹校验点信息和 / 或校验点触发信息计算密码序列;密码序列判断单元,用于判断所述密码序列与本地存储的密码序列是否一致;校验指示单元,当密码序列与本地存储的密码序列一致时,指示所述用户通过验证,当密码序列与本地存储的密码序列不一致时,指示所述用户未通过验证。

[0022] 本发明实施例提供的客户端,包括:安全信息记录单元,用于记录用户输入的轨迹校验点信息和 / 或校验点触发信息,所述轨迹校验点信息和 / 或校验点触发信息为用户根据本地预置的登录信息,通过轨迹输入设备输入的;安全信息发送单元,用于向安全信息校验装置发送包含所述轨迹校验点信息和 / 或校验点触发信息的安全信息。

[0023] 可选地,所述安全信息记录单元包括:

[0024] 矩阵生成单元,用于根据本地存储的登录信息生成包含若干个校验点的矩阵;轨迹记录单元,用于记录用户通过鼠标,或手柄,或触摸板在所述矩阵中输入的轨迹所经过的校验点,将所述校验点的坐标作为所述轨迹校验点信息;触发记录单元,用于记录用户通过鼠标,或手柄,或触摸板在所述矩阵中点击的校验点的标识以及点击次数,将所述校验点的

标识以及点击次数作为校验点触发信息。

[0025] 可选地,所述客户端还包括:

[0026] 登录信息校验单元,用于获取本地预置的登录信息的属性,判断所述属性中的有效期是否超过预置期限;登录信息更新单元,用于当所述属性中的有效期超过预置期限时,向安全信息校验装置发送登录信息更新请求,并接收安全信息校验装置反馈的登录信息,利用接收到的登录信息替换本地保存的登录信息。

[0027] 从以上技术方案可以看出,本发明实施例具有以下优点:

[0028] 本发明实施例中由于从客户端接收到的安全信息中包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息,即用户输入的安全信息并不是采用键盘方式输入的字符信息,所以降低了安全信息被暴力破解的可能性,从而提高了用户信息的安全性;

[0029] 此外,由于本发明实施例中,用户可以使用轨迹输入设备输入安全信息,所以输入的内容从用户角度来看是一种图形或图像,由于用户对图形或图像的识别能力以及理解能力一般都优于对字符的识别能力以及理解能力,因此更有利于用户牢记安全信息,同时由于降低了安全信息被暴力破解的可能性,所以用户不需要输入验证码,简化了用户操作,进而提高了用户体验。

附图说明

[0030] 图1为本发明实施例中安全信息校验方法实施例流程图;

[0031] 图2为本发明实施例中安全信息记录过程示意图;

[0032] 图3为本发明实施例中安全信息校验装置实施例示意图;

[0033] 图4为本发明实施例中客户端实施例示意图;

[0034] 图5为本发明实施例中第一矩阵示意图;

[0035] 图6为本发明实施例中第二矩阵示意图。

具体实施方式

[0036] 本发明实施例提供了一种安全信息校验方法及安全信息校验装置以及客户端,用于提高用户信息的安全性,同时提高用户体验,本发明实施例的主要思路是通过记录用户某特定矩阵中轨迹输入设备移动的轨迹以及点击次数作为密码输入来验证用户身份。

[0037] 本发明实施例中由于从客户端接收到的安全信息中包括用户通过轨迹输入设备输入的轨迹校验点信息和/或校验点触发信息,即用户输入的安全信息并不是采用键盘方式输入的字符信息,所以降低了安全信息被暴力破解的可能性,从而提高了用户信息的安全性;

[0038] 此外,由于本发明实施例中,用户可以使用轨迹输入设备输入安全信息,所以输入的内容从用户角度来看是一种图形或图像,由于用户对图形或图像的识别能力以及理解能力一般都优于对字符的识别能力以及理解能力,因此更有利于用户牢记安全信息,同时由于降低了安全信息被暴力破解的可能性,所以用户不需要输入验证码,简化了用户操作,进而提高了用户体验。

[0039] 下面的各实施例中以鼠标作为轨迹输入设备的例子进行说明,可以理解的是,在

具体应用中,还可以是其他类型的轨迹输入设备,例如手柄,触摸板等,具体流程与鼠标的处理流程类似,本发明实施例中不作限定。

[0040] 下面首先介绍本发明实施例中的安全信息校验方法:

[0041] 请参阅图 1,本发明实施例中安全信息校验方法实施例包括:

[0042] 101、记录用户输入的安全信息;

[0043] 该步骤为本发明实施例中的关键步骤,将在后续实施例中进行详细说明,本实施例仅作简要描述。

[0044] 本实施例中,当用户请求登录时,需要验证用户名以及安全信息,则用户需要输入用户名以及通过鼠标输入安全信息,可以理解的是,若所有用户的安全信息均不相同,即安全信息与用户之间具有一一对应的关系,则用户可以不输入用户名。

[0045] 客户端记录用户通过鼠标输入的安全信息,该安全信息中包含轨迹校验点信息,或者是包含校验点触发信息,或者是两者均包含,本实施例中轨迹校验点信息是指用户使用鼠标在客户端生成的矩阵中移动的轨迹所经过的校验点的坐标,校验点触发信息是指用户使用鼠标在客户端生成的矩阵中点击的校验点的标识以及点击次数。

[0046] 102、向安全信息校验装置发送记录的安全信息;

[0047] 客户端记录了用户通过鼠标输入的安全信息之后,向安全信息校验装置发送该安全信息。

[0048] 103、接收客户端发送的安全信息;

[0049] 安全信息校验装置接收客户端发送的安全信息。

[0050] 104、根据接收到的安全信息计算密码序列;

[0051] 本实施例中,安全信息校验装置接收到客户端发送的安全信息之后,为便于进行比较判断,需要首先根据安全信息计算出密码序列,具体的计算方法将在后续的实施例中详细描述。

[0052] 105、判断该密码序列与本地存储的密码序列是否一致,若一致,则执行步骤 106,若不一致,则执行步骤 107;

[0053] 安全信息校验装置计算得到密码序列后,根据该用户的用户标识查询该用户预先在安全信息校验装置中存储的密码序列,判断计算得到的密码序列是否与存储的密码序列一致。

[0054] 本实施例中,当用户需要输入用户名时,会将用户名与安全信息一同发送至安全信息校验装置,则安全信息校验装置可以根据该用户名查询对应的密码序列,可以理解的是,若用户不需要输入用户名,则安全信息校验装置可以根据该用户发送的安全信息中所携带的该用户的互联网协议(IP, InternetProtocol)地址或其他可以标识用户身份的信息查询对应的密码序列。

[0055] 106、指示该用户通过验证并登录;

[0056] 当计算得到的密码序列与该用户预先存储的密码序列一致时,则判断该用户为合法用户,可以正常登录。

[0057] 107、指示该用户未通过验证并执行异常处理流程。

[0058] 当计算得到的密码序列与该用户预先存储的密码序列不一致时,则判断该用户为非法用户,可以提示用户“密码错误”,并请求用户重新输入密码。

[0059] 本实施例中由于从客户端接收到的安全信息中包括用户通过轨迹输入设备输入的轨迹校验点信息和 / 或校验点触发信息,即用户输入的安全信息并不是采用键盘方式输入的字符信息,所以降低了安全信息被暴力破解的可能性,从而提高了用户信息的安全性。

[0060] 下面介绍本发明实施例中有关记录用户通过鼠标输入的安全信息的过程,请参阅图 2,本发明实施例中安全信息记录流程包括:

[0061] 201、获取本地预置的登录信息的属性;

[0062] 本实施例中,在客户端会预置有登录信息,其中包含用于生成矩阵的相关信息,例如矩阵维数信息以及间距生成参数等信息。

[0063] 登录信息包含一些常规属性,例如创建时间,有效期,使用者等等。

[0064] 202、判断该登录信息是否过期,若是,则执行步骤 203,若否,则执行步骤 204;

[0065] 获取登录信息的创建时间属性以及有效期属性,根据这两个属性判断该登录信息是否过期,例如某登录信息的创建时间为 2007 年 1 月 1 日,有效期为 30 天,则假设当前为 2007 年 3 月 1 日,则该登录信息过期。可以理解的是,有效期同样可以是一个具体的日期,例如有效期为 2007 年 2 月 1 日,则表示该登录信息在 2007 年 2 月 1 日之前(包括当日)有效,这种情况下,只需要判断有效期即可获知登录信息是否过期。

[0066] 203、更新登录信息,并跳转至步骤 204;

[0067] 当登录信息过期时,客户端需要对登录信息进行更新才能够正确地生成矩阵,则此时客户端向安全信息校验装置发送登录信息更新请求,当安全信息校验装置接收到该请求后,会查询本地存储的最新的登录信息,并将该登录信息携带于登录信息更新响应中,下发至客户端,客户端接收到最新的登录信息后,用该登录信息替换原先本地存储的登录信息以完成登录信息的更新。

[0068] 204、根据登录信息生成包含若干个校验点的矩阵,并跳转至步骤 205 以及步骤 206;

[0069] 若客户端本地存储的登录信息没有过期,或者是客户端已经对本地存储的登录信息进行了更新,则需要根据本地存储的登录信息生成包含若干个校验点的矩阵,具体的生成过程可以为:

[0070] 首先,获取登录信息中的矩阵维数信息以及间距生成参数;

[0071] 其次,根据矩阵维数信息确定矩阵的行数和列数,即矩阵维数信息中会指示生成的矩阵应该具有多少行,多少列;

[0072] 再次,按照该行数和列数分配校验点,即在每行列交点处设置一个校验点;

[0073] 最后,根据间距生成参数调整矩阵中相邻校验点之间的距离以生成包含若干个校验点的矩阵。

[0074] 205、记录用户通过鼠标在矩阵中输入的轨迹所经过的校验点;

[0075] 当用户通过鼠标输入安全信息时,记录鼠标指针在矩阵中的移动轨迹所经过的校验点,即记录这些校验点的坐标。

[0076] 206、记录用户通过鼠标在矩阵中点击的校验点以及点击次数。

[0077] 当用户通过鼠标输入安全信息时,记录鼠标指针在矩阵中所点击的校验点的标识以及点击的次数,可以理解的是,校验点的标识可以为该校验点的坐标。

[0078] 上述实施例中描述的是客户端记录安全信息的过程,上述流程中,步骤 205 与步

骤 206 可以同时执行,或者根据实际情况只执行其中一个步骤。

[0079] 下面介绍本发明实施例中安全信息校验装置实施例,请参阅图 3,一并参阅图 4,本发明实施例中安全信息校验装置实施例包括:

[0080] 安全信息接收单元 302,用于接收客户端中的安全信息发送单元 402 发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和 / 或校验点触发信息,并将接收到的安全信息发送至安全信息校验单元 303 进行校验;

[0081] 安全信息校验单元 303,用于判断所述安全信息是否合法,若合法,则指示所述用户通过验证。

[0082] 本实施例中,安全信息校验装置还包括:

[0083] 登录信息反馈单元 301,用于接收客户端中的登录信息更新单元 404 发起的登录信息更新请求,向客户端中的登录信息更新单元 404 反馈本地的登录信息。

[0084] 本实施例中,安全信息校验单元 303 包括:

[0085] 密码序列计算单元 3031,用于根据安全信息接收单元 302 发送的轨迹校验点信息和 / 或校验点触发信息计算密码序列,并将密码序列发送至密码序列判断单元 3032;

[0086] 密码序列判断单元 3032,用于判断密码序列与本地存储的密码序列是否一致,并将判断结果发送至校验指示单元 3033;

[0087] 校验指示单元 3033,当密码序列与本地存储的密码序列一致时,指示用户通过验证,当密码序列与本地存储的密码序列不一致时,指示用户未通过验证。

[0088] 请参阅图 4,一并参阅图 3,本发明实施例中客户端实施例包括:

[0089] 安全信息记录单元 401,用于记录用户输入的轨迹校验点信息和 / 或校验点触发信息,所述轨迹校验点信息和 / 或校验点触发信息为用户根据本地预置的登录信息,通过轨迹输入设备输入的;

[0090] 安全信息发送单元 402,用于向安全信息校验装置中的安全信息接收单元 302 发送包含轨迹校验点信息和 / 或校验点触发信息的安全信息。

[0091] 本实施例中,安全信息记录单元 401 包括:

[0092] 矩阵生成单元 4011,用于根据本地存储的登录信息生成包含若干个校验点的矩阵;

[0093] 轨迹记录单元 4012,用于记录用户通过鼠标在所述矩阵中输入的轨迹所经过的校验点,将校验点的坐标作为轨迹校验点信息;

[0094] 触发记录单元 4013,用于记录用户通过鼠标在所述矩阵中点击的校验点的标识以及点击次数,将校验点的标识以及点击次数作为校验点触发信息。

[0095] 本实施例中,客户端还包括:

[0096] 登录信息校验单元 403,用于获取本地预置的登录信息的属性,判断属性中的有效期是否超过预置期限;

[0097] 登录信息更新单元 404,用于当属性中的有效期超过预置期限时,向安全信息校验装置中的登录信息反馈单元 301 发送登录信息更新请求,并接收登录信息反馈单元 301 反馈的登录信息,利用接收到的登录信息替换本地保存的登录信息。

[0098] 为便于理解,下面以一个具体实例说明本发明实施例:

[0099] 客户端获取到本地的登录信息后,判断该登录信息未过期,则从该登录信息中提

取出生成矩阵的相关信息,假设矩阵维数信息为 4 乘 4,则表示该矩阵一共有 16 个校验点,分成 4 行 4 列,如图 5 所示,间距生成参数为 1,则表示该矩阵中,每一个校验点与自身周围行相邻,或者是列相邻的校验点之间的距离为 1 毫米,如图 5 中,校验点 B2(B,2) 与其周围的校验点 A2(A,2),B1(B,1),B3(B,3) 以及 C2(C,2) 之间的距离均为 1 毫米。

[0100] 如图 5 所示,假设用户通过鼠标输入的轨迹为从校验点 A1 至校验点 A3 的折线,并在鼠标移动过程中点击校验点 A3 两次,则客户端记录此次用户通过鼠标输入的轨迹经过的校验点为 A1(A,1),B2(B,2),C2(C,2),D3(D,3),C4(C,4),A3(A,3),记录此次用户通过鼠标在矩阵中点击的校验点为 A3,次数为 2 次,则将记录的信息包含于安全信息中发送至安全信息校验装置;

[0101] 安全信息校验装置接收到这些信息后,首先将这些信息计算转换为密码序列,具体的转换方法此处不作限定,仅举例说明:假设计算算法的规则为“第一校验点行列坐标乘积”+“第二校验点行列坐标乘积”+.....+“&”+“点击校验点坐标乘积”* 点击次数。则计算出的密码序列为“1A2B2C3D4C3A&3A3A”,得到密码序列后,可以根据用户输入的用户名,或在安全信息中携带的用户的 IP 地址等标识查询该用户预先在安全信息校验装置中存储的正确密码序列,假设该正确密码序列与计算得到的序列一致,则指示用户通过验证。

[0102] 上述例子在生成矩阵的过程中采用的间距生成参数为 1,即一个固定值,则在该矩阵中,每一个校验点与自身周围行相邻,或者是列相邻的校验点之间的距离为 1 毫米,可以理解的是,该间距生成参数同样可以设置为一个动态值,可以以函数变量作为间距,例如设置该间距生成参数为 x+1,则表示第一行校验点与第二行校验点之间的间距为 1,第二行校验点与第三行校验点之间的间距为 1+1,第三行校验点与第四行校验点之间的间距为 1+1+1,依次类推,在列方向类似,具体的间距生成参数可以根据用户的需求进行确定,此处不作限定。

[0103] 可以理解的是,在实际应用中,为了能够进一步提高用户信息的安全性,可以为上述矩阵设置更加复杂的校验点,例如可以设置不固定的校验点间距或校验点形状,此外,为了防止非法用户破解鼠标轨迹,还可以在矩阵中加入干扰图形,下面以一个具体实例进行说明:

[0104] 请参阅图 6,假设矩阵维数信息为 6 乘 5,则表示该矩阵一共有 30 个校验点,分成 6 行 5 列显示,如图 6 所示,间距生成参数为 X+1,则表示该矩阵中,每两行之间的间距都比前两行之间的间距多 1,即 B 行与 C 行之间的间距比 A 行与 B 行之间的间距多 1,列方向同理,此外,在本矩阵中,校验点信息中还包括一项“形状信息”,用于指示该校验点为何种形状,可以理解的是,校验点信息中还可以包括一项“颜色信息”,用于指示该校验点为何种颜色。

[0105] 需要说明的是,在客户端与服务端中均在系统初始化时协商设置有一个对应关系,用于保存校验点形状信息与该校验点形状之间的对应关系,以及保存校验点颜色信息与该校验点颜色之间的对应关系,结合本实施例,具体可如下表所示:

[0106] 表 1

[0107]

校验点形状	形状信息
圆形	T1

校验点形状	形状信息
正六边形	T2
正方形	T3
三角形	T4
五角星形	T5

[0108] 表 2

[0109]

校验点颜色	颜色信息
黑色	C1
绿色	C2
蓝色	C3
红色	C4
紫色	C5

[0110] 如图 6 所示,图中的虚线标识干扰图形,在实际应用中可以增加或减少虚线的数目,或者改用其他形状作为干扰图形,此处不作限定,假设用户通过鼠标输入的轨迹为从校验点 A1 至校验点 F3 的折线,并在鼠标移动过程中点击校验点 D3 一次,F3 两次,本实施例中的轨迹经过的校验点的信息由一个六元组构成,具体为(行坐标,列坐标,形状信息,颜色信息,是否被点击,被点击次数),则客户端记录此次用户通过鼠标输入的轨迹经过的校验点为 A1(A,1,T1,C4,N,0),B2(B,2,T3,C1,N,0),D3(D,3,T2,C3,Y,1),D4(D,4,T3,N,0),E5(E,5,T2,C2,N,0),E4(E,4,T1,C5,N,0),F3(F,3,T4,C2,Y,2),则将记录的信息包含于安全信息中发送至安全信息校验装置;

[0111] 安全信息校验装置接收到这些信息后,首先将这些信息计算转换为密码序列,具体的转换方法此处不作限定,仅举例说明:假设计算算法的规则为“(第一校验点六元组信息)”+“(第二校验点六元组信息)”+.....+“&”+“(被点击校验点六元组信息)”。则计算出的密码序列为“(A,1,T1,C4,N,0)(B,2,T3,C1,N,0)(D,3,T2,C3,Y,1)(D,4,T3,N,0)(E,5,T2,C2,N,0)(E,4,T1,C5,N,0)(F,3,T4,C2,Y,2)&(D,3,T2,C3,Y,1)(F,3,T4,C2,Y,2)”,得到密码序列后,可以根据用户输入的用户名,或在安全信息中携带的用户的 IP 地址等标识查询该用户预先在安全信息校验装置中存储的正确密码序列,假设该正确密码序列与计算得到的序列一致,则指示用户通过验证。

[0112] 上述实施例中描述的是用户通过鼠标一次性输入一个连续轨迹的情况,可以理解的是,用户同样可以通过鼠标输入多段连续轨迹,具体方式与上述实施例中类似,此处不再赘述。

[0113] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中,该程序在执行时,包括如下步骤:

[0114] 接收客户端发送的安全信息,所述安全信息包括用户通过轨迹输入设备输入的轨迹校验点信息和 / 或校验点触发信息;

[0115] 判断所述安全信息是否合法,若合法,则指示所述用户通过验证。

[0116] 上述提到的存储介质可以是只读存储器,磁盘或光盘等。

[0117] 以上对本发明所提供的一种安全信息校验方法及安全信息校验装置以及客户端进行了详细介绍,对于本领域的一般技术人员,依据本发明实施例的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

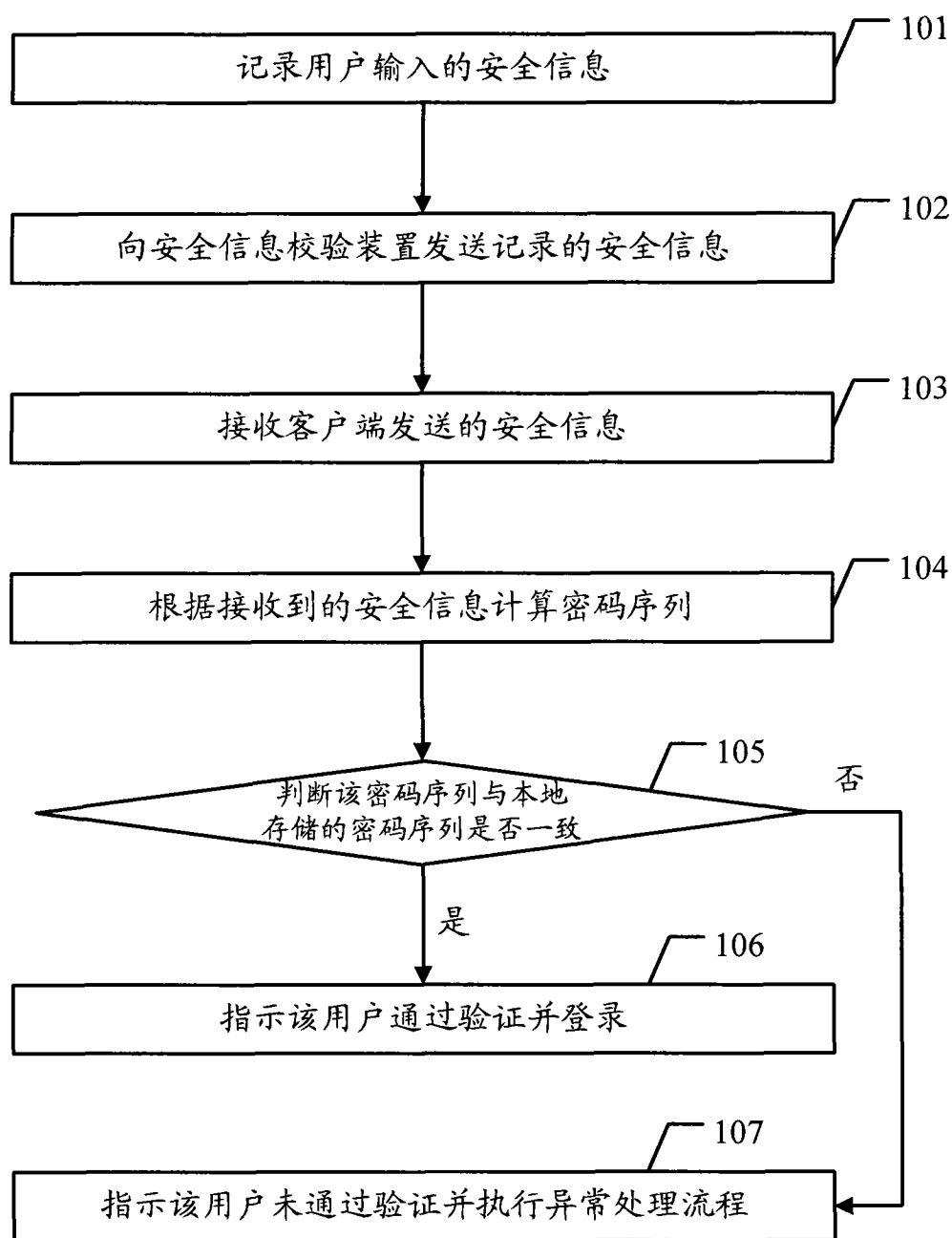


图 1

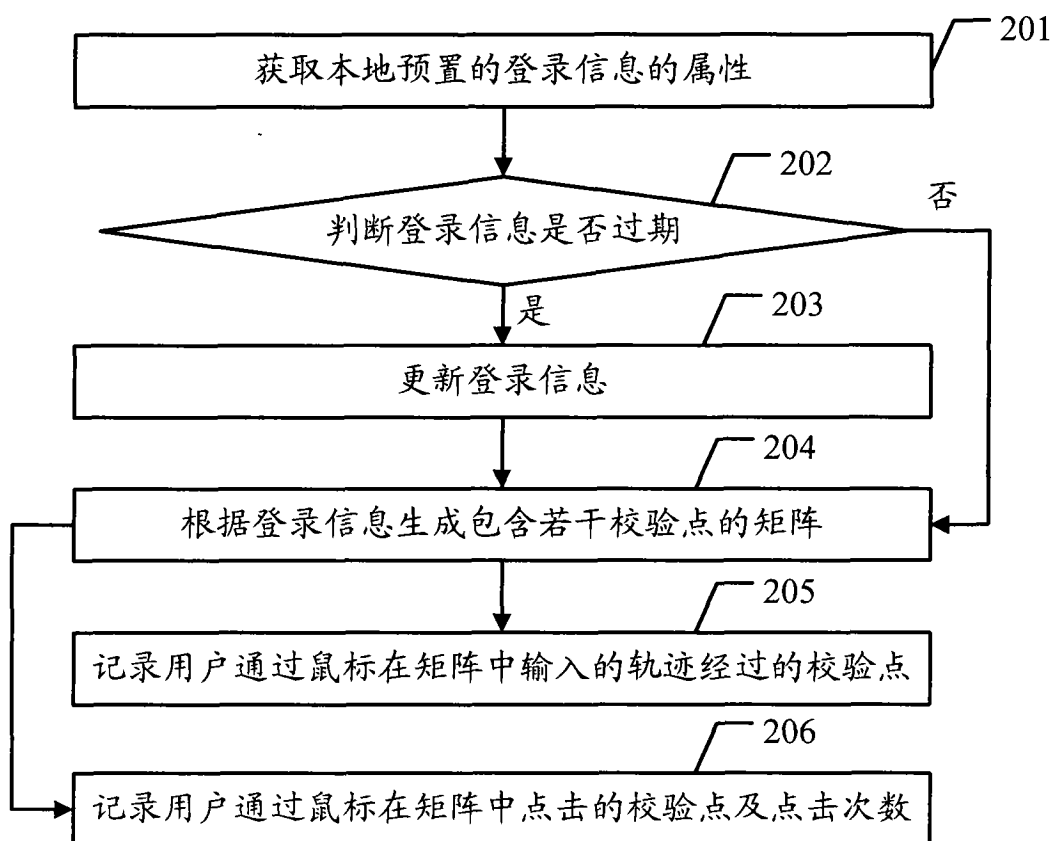


图 2

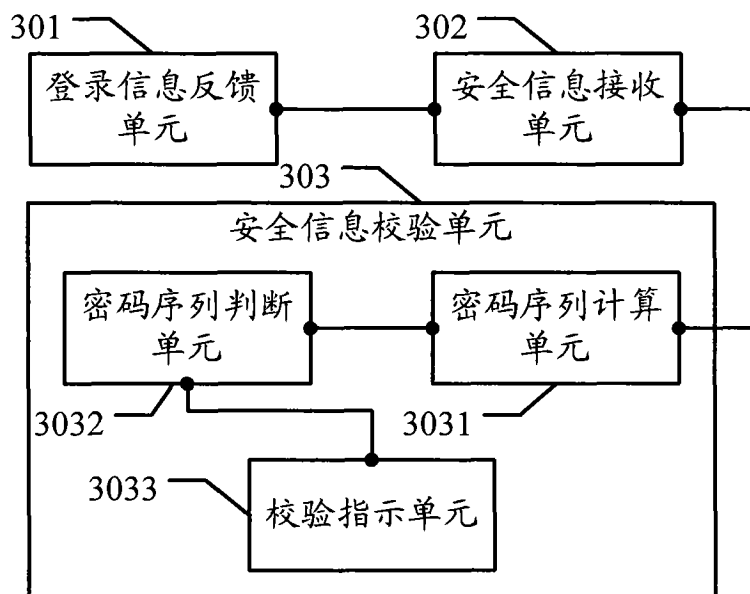


图 3

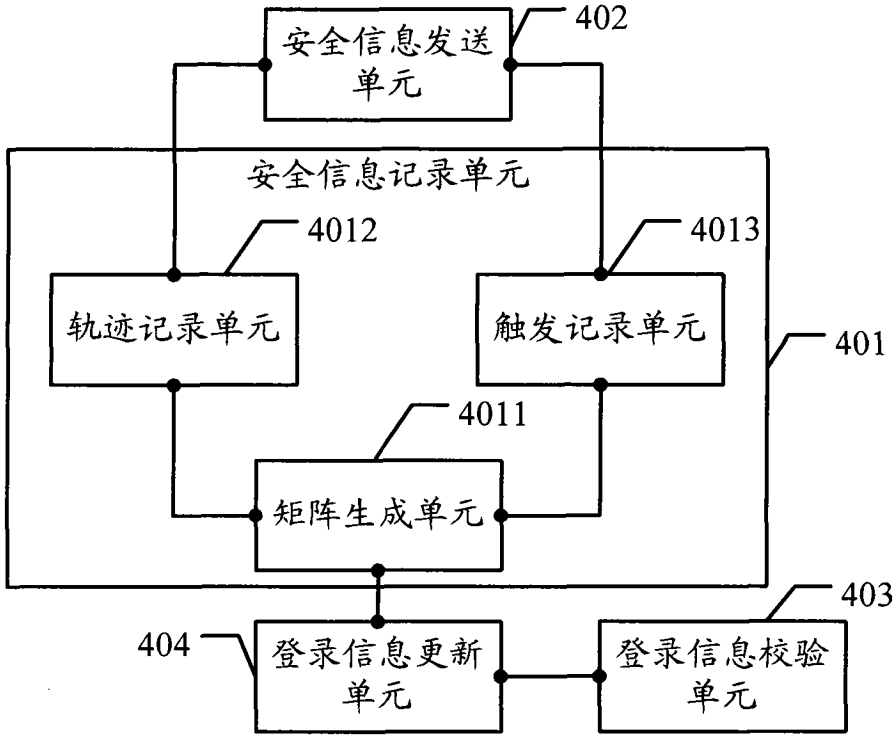


图 4

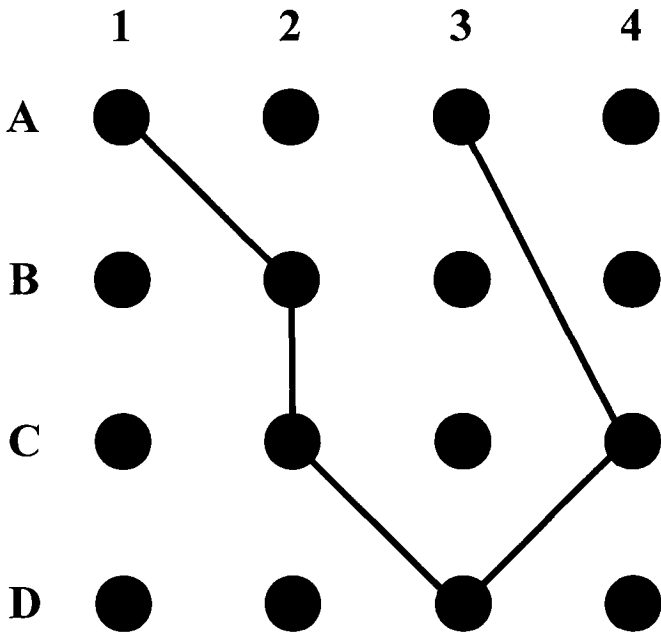


图 5

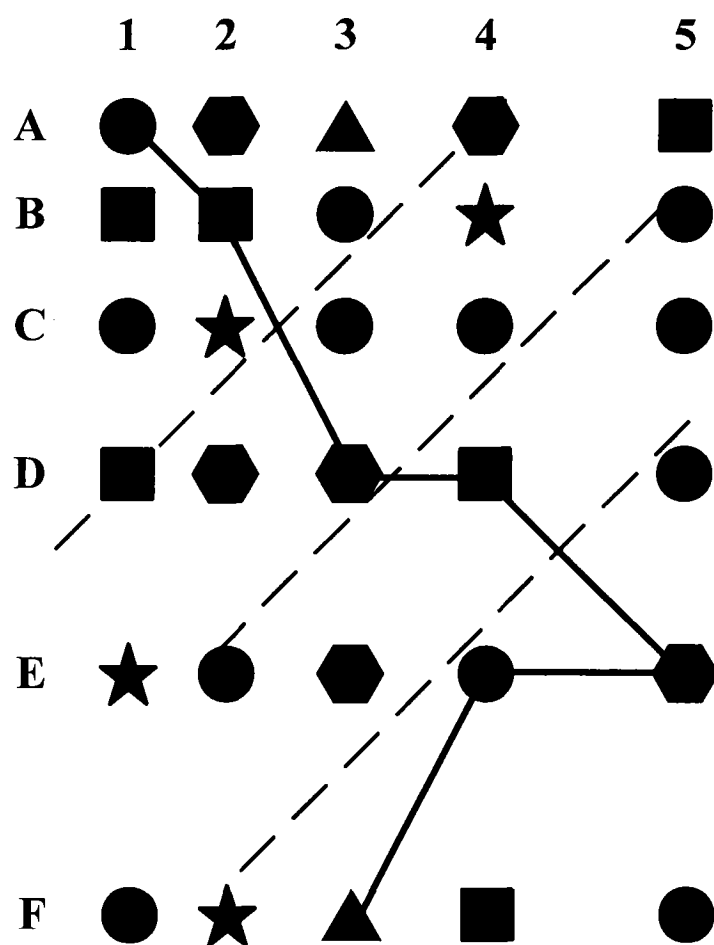


图 6