

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日

2015年10月22日 (22.10.2015)

WIPO | PCT

(10) 国际公布号

WO 2015/158148 A1

(51) 国际专利分类号:

H04L 9/32 (2006.01)

(21) 国际申请号:

PCT/CN2014/093910

(22) 国际申请日:

2014年12月16日 (16.12.2014)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201410153707.6 2014年4月17日 (17.04.2014) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 翟征德 (Zhai, Zhengde); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司
(LONGSUN LEAD IP LTD.); 中国北京市海淀区丹棱街16号海兴大厦C座1108, Beijing 100080 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国国际公布:

— 包括国际检索报告(条约第21条(3))。

(54) Title: USER AUTHENTICATION METHOD AND DEVICE AND TERMINAL

(54) 发明名称: 用户认证方法、认证装置和终端

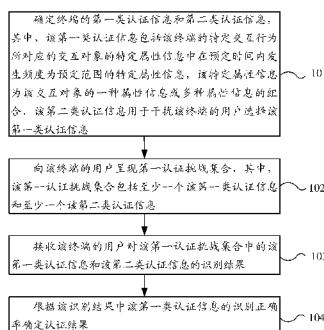


图1 / FIG. 1

101 DETERMINE CLASS 1 AUTHENTICATION INFORMATION AND CLASS 2 AUTHENTICATION INFORMATION. WHEREIN THE CLASS 1 AUTHENTICATION INFORMATION COMPRISSES SPECIFIC ATTRIBUTE INFORMATION, AMONG SPECIFIC ATTRIBUTE INFORMATION OF AN INTERACTION OBJECT CORRESPONDING TO A SPECIFIC INTERACTION BEHAVIOR, THERE IS AT LEAST ONE PIECE OF OCCURRENCE FREQUENCY WITHIN A PREDETERMINED RANGE IN A PREDETERMINED TIME. THE SPECIFIC ATTRIBUTE INFORMATION IS ONE TYPE OF ATTRIBUTE INFORMATION OR A COMBINATION OF MULTIPLE TYPES OF ATTRIBUTE INFORMATION OF THE INTERACTION OBJECT. AND THE CLASS 2 AUTHENTICATION INFORMATION IS USED FOR INTERFERING A USER OF THE TERMINAL IN SELECTING THE CLASS 1 AUTHENTICATION INFORMATION.

102 PRESENT A FIRST AUTHENTICATION CHALLENGE SET TO THE TERMINAL. WHEREIN THE FIRST AUTHENTICATION CHALLENGE SET COMPRISSES AT LEAST ONE PIECE OF THE CLASS 1 AUTHENTICATION INFORMATION AND AT LEAST ONE PIECE OF THE CLASS 2 AUTHENTICATION INFORMATION.

103 RECEIVE A RECOGNITION RESULT OF THE USER OF THE TERMINAL ON THE AUTHENTICATION CHALLENGE SET AND THE CLASS 2 AUTHENTICATION INFORMATION IN THE FIRST AUTHENTICATION CHALLENGE SET.

104 DETERMINE AN AUTHENTICATION RESULT ACCORDING TO A CORRECT RECOGNITION RATE OF THE CLASS 1 AUTHENTICATION INFORMATION IN THE RECOGNITION RESULT.

(57) Abstract: Embodiments of the present invention provide a user authentication method and device and a terminal. The method comprises: determining class 1 authentication information and class 2 authentication information of a terminal, wherein the class 1 authentication information comprises specific attribute information, among specific attribute information of an interaction object corresponding to a specific interaction behavior of the terminal, having an occurrence frequency within a predetermined range in predetermined time, and the class 2 authentication information is used for interfering a user of the terminal in selecting the class 1 authentication information; presenting an authentication challenge set to the user of the terminal; receiving a recognition result of the user of the terminal on the authentication challenge set; and determining an authentication result according to a correct recognition rate of the class 1 authentication information in the recognition result. By means of the user authentication method and device and the terminal in the embodiments of the present invention, authentication information is dynamically generated by using information of an interaction object having a predetermined occurrence frequency in predetermined time in the terminal to authenticate a user, so that a certain anti-peeping capability is provided while reducing the memory cost of the user on authentication information.

(57) 摘要:

[见续页]



本发明实施例提供了一种用户认证方法、认证装置和终端，该方法包括：确定终端的第一类认证信息和第二类认证信息，其中，第一类认证信息包括终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，第二类认证信息用于干扰终端的用户选择第一类认证信息；向终端的用户呈现认证挑战集合；接收终端的用户对认证挑战集合的识别结果；根据识别结果中第一类认证信息的识别正确率确定认证结果。本发明实施例的用户认证方法、认证装置和终端，通过利用终端中预定时间内预定发生频率的交互对象的信息动态地生成认证信息以对用户进行认证，在减少用户对认证信息的记忆代价的同时，还具备一定的抗偷窥能力。

用户认证方法、认证装置和终端

本申请要求于 2014 年 4 月 17 日提交中国专利局、申请号为 201410153707.6、发明名称为“用户认证方法、认证装置和终端”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明实施例涉及终端领域，并且更具体地，涉及一种用户认证方法、认证装置和终端。

10 背景技术

用户设备或应用程序需要频繁地认证用户以确定当前用户的身份。认证是允许用户访问终端中的数据和应用之前最主要的安全屏障。

15 用户认证机制的最关键因素之一是尽量低的用户的记忆代价，提高易用性。另外用户设备总是被用户随身携带，在各种场合和环境中使用，认证过程易被偷看，所以要求认证机制有一定的抗偷窥能力。

发明内容

本发明实施例提供一种用户认证方法、认证装置和终端，能够在降低用户记忆代价的同时具备一定的抗偷窥能力。

20 第一方面，提供了一种用户认证的方法，该方法包括：确定终端的第一类认证信息和第二类认证信息，其中，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类认证信息用于干扰该终端的用户选择该第一类认证信息；向该终端的用户呈现第一认证挑战集合，其中，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息；接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果；根据该识别结果中该第一类认证信息的识别正确率确定认证结果。

25

30 结合第一方面，在第一种可能的实现方式中，具体实现为该第二类认证信息包括以下至少一种：该终端的特定交互行为所对应的交互对象的特定属

性信息中在预定时间内发生频度为预定范围以外的特定属性信息；不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

结合第一方面或第一方面的第一种可能的实现方式，在第二种可能的实现方式中，具体实现为：该第一类认证信息还包括该终端的用户在该终端中
5 所指定的交互对象的特定属性信息，以便减少该终端的用户对该第一类认证信息的记忆代价。

结合第一方面或第一方面的第一种可能的实现方式或第一方面的第二种可能的实现方式，在第三种可能的实现方式中，在接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果
10 之前，该方法还包括：如果该终端的特定交互行为所对应的交互对象发生变化，或者该终端产生新的该特定交互行为，则重新确定该终端的第一类认证信息和第二类认证信息，并向该终端的用户呈现第二认证挑战集合，其中，该第二认证挑战集合基于重新确定后的第一类认证信息和第二类认证信息生成。

15 结合第一方面的第三种可能的实现方式，在第四种可能的实现方式中，具体实现为该终端的特定交互行为所对应的交互对象发生变化包括：增加该终端的特定交互行为所对应的交互对象，或者删除该终端的特定交互行为所对应的交互对象，或者修改该终端的特定交互行为所对应的交互对象。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第四种可能的实现方式中任一种可能的实现方式，在第五种可能的实现方式中，具体实现为：该终端的特定交互行为包括该终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为联系人的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性信息；或者，该终端的特定交互行为包括该终端访问网站的行为，该第一类认证信息和该第二类认证信息为网站的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，该终端

的特定交互行为包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第五种可能的实现方式中任一种可能的实现方式，在第六种可能的实现方式中，在确定终端的第一类认证信息和至少一个第二类认证信息之前，该方法还包括：配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数N。该根据该识别结果中该第一类认证信息的识别正确率确定认证结果具体实现为：如果该识别结果中该终端的用户识别的该第一类认证信息的条数不小于N条，则确定对该终端的用户的认证通过；或者，如果该识别结果中该终端的用户识别的该第一类认证信息的条数小于N条，则确定对该终端的用户的认证不通过。

结合第一方面的第六种可能的实现方式，在第七种可能的实现方式中，如果该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对该终端的用户的认证的安全强度越大；如果对该终端的用户进行认证所需要识别的第一类认证信息的条数N越大，则通过对该终端的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对该终端的用户的认证的安全强度越大。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第七种可能的实现方式中任一种可能的实现方式，在第八种可能的实现方式中，具体实现为：该预定范围为该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第八种可能的实现方式中任一种可能的实现方式，在第九种可能的实现方式中，在确定终端的第一类认证信息之前，该方法还包括：配置该终端的排除认证信息集合，其中该排除认证信息集合中的认证信息不允许作为该第一类认证

信息。此时，确定终端的第一类认证信息具体实现为：确定该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围且不属于该排除认证集合的特定属性信息为该第一类认证信息。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第九
5 种可能的实现方式中任一种可能的实现方式，在第十种可能的实现方式中，在向该终端的用户呈现第一认证挑战集合之前，该方法还包括：根据该终端的该第一类认证信息和该第二类认证信息生成该第一认证挑战集合，以便向该终端的用户呈现该第一认证挑战集合。

结合第一方面或第一方面的第一种可能的实现方式至第一方面的第十
10 种可能的实现方式中任一种可能的实现方式，在第十一种可能的实现方式中，该终端包括智能手机、平板电脑、个人计算机、服务器或工作站。

第二方面，提供了一种认证装置，该装置包括：确认单元，用于确定所述装置所在的终端的第一类认证信息和第二类认证信息，其中，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类认证信息用于干扰该终端的用户选择该第一类认证信息；认证呈现单元，用于向该终端的用户呈现第一认证挑战集合，其中，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息；接收单元，用于接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果；认证单元，用于根据该识别结果中该第一类认证信息的识别正确率确定认证结果。

结合第二方面，在第一种可能的实现方式中，具体实现为该第二类认证信息包括以下至少一种：该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。
25

结合第二方面或第二方面的第一种可能的实现方式，在第二种可能的实现方式中，具体实现为：该第一类认证信息还包括该终端的用户在该终端中所指定的交互对象的特定属性信息，以便减少该终端的用户对该第一类认证信息的记忆代价。
30

结合第二方面或第二方面的第一种可能的实现方式或第二方面的第二

种可能的实现方式，在第三种可能的实现方式中，在接收单元接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果之前，如果该终端的特定交互行为所对应的交互对象发生变化，或者该终端产生新的该特定交互行为，则该确认单元还用于重新确定该终端的第一类认证信息和第二类认证信息，以便该认证呈现单元向该终端的用户呈现第二认证挑战集合，其中，该第二认证挑战结合基于该确定单元重新确定后的第一类认证信息和第二类认证信息生成。

结合第二方面的第三种可能的实现方式，在第四种可能的实现方式中，具体实现为该终端的特定交互行为所对应的交互对象发生变化包括：增加该终端的特定交互行为所对应的交互对象，或者删除该终端的特定交互行为所对应的交互对象，或者修改该终端的特定交互行为所对应的交互对象。

结合第二方面或第二方面的第一种可能的实现方式至第二方面的第四种可能的实现方式中任一种可能的实现方式，在第五种可能的实现方式中，具体实现为：该终端的特定交互行为包括该终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为联系人的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性信息；或者，该终端的特定交互行为包括该终端访问网站的行为，该第一类认证信息和该第二类认证信息为网站的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，该终端的特定交互行为包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。

结合第二方面或第二方面的第一种可能的实现方式至第二方面的第五种可能的实现方式中任一种可能的实现方式，在第六种可能的实现方式中，该装置还包括第一配置单元，该第一配置单元用于：配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数

N。该认证单元具体用于：如果该识别结果中该终端的用户识别的该第一类认证信息的条数不小于 N 条，或者，如果该识别结果中该终端的用户识别的该第一类认证信息的条数小于 N 条，则确定对该终端的用户的认证不通过。

结合第二方面的第六种可能的实现方式，在第七种可能的实现方式中，
5 该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对该终端的用户的认证的安全强度越大；对该终端的用户进行认证所需要识别的第一类认证信息的条数越大，则通过对该终端的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对该终端的用户的认证的安全强度越大。

10 结合第二方面或第二方面的第一种可能的实现方式至第二方面的第七种可能的实现方式中任一种可能的实现方式，在第八种可能的实现方式中，具体实现为：该预定范围为该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在
15 总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间
间内发生次数排名在预定比例以内的范围。

结合第二方面或第二方面的第一种可能的实现方式至第二方面的第八种可能的实现方式中任一种可能的实现方式，在第九种可能的实现方式中，
20 该装置还包括第二配置单元，该第二配置单元用于配置该终端的排除认证信息集合，其中该排除认证信息集合中的认证信息不允许作为该第一类认证信息。在用于确定该终端的第一类认证信息的过程中，该确定单元具体用于确定该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间
25 内发生频度为预定范围且不属于该排除认证集合的特定属性信息为该第一类认证信息。

结合第二方面或第二方面的第一种可能的实现方式至第二方面的第九种可能的实现方式中任一种可能的实现方式，在第十种可能的实现方式中，
30 该装置还包括生成单元，该生成单元用于：根据该终端的该第一类认证信息和该第二类认证信息生成该第一认证挑战集合，以便向该终端的用户呈现该第一认证挑战集合。

结合第二方面或第二方面的第一种可能的实现方式至第二方面的第十种可能的实现方式中任一种可能的实现方式，在第十一种可能的实现方式中，该终端包括智能手机、平板电脑、个人计算机、服务器或工作站。

第三方面，提供了一种终端，该终端包括：包括处理器、存储器、通信接口、显示设备和输入设备，该处理器与该存储器相连，且通过该通信接口连接到该显示设备和该输入设备，该存储器中存储一组程序代码，且该处理器用于调用该存储器中存储的程序代码，用于执行以下操作：确定该终端的第一类认证信息和第二类认证信息，并通过该通信接口在该显示设备上向该终端的用户呈现第一认证挑战集合，其中，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类认证信息用于干扰该终端的用户选择该第一类认证信息，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息；通过该通信接口从该输入设备中接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果，并根据该识别结果中该第一类认证信息的识别正确率确定认证结果。该显示设备，用于向该终端的用户呈现该第一认证挑战集合。该输入设备，用于输入该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果。

结合第三方面，在第一种可能的实现方式中，具体实现为该第二类认证信息包括以下至少一种：该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

结合第三方面或第三方面的第一种可能的实现方式，在第二种可能的实现方式中，具体实现为：该第一类认证信息还包括该终端的用户在该终端中所指定的交互对象的特定属性信息，以便减少该终端的用户对该第一类认证信息的记忆代价。

结合第三方面或第三方面的第一种可能的实现方式或第三方面的第二种可能的实现方式，在第三种可能的实现方式中，在该处理器通过该通信接口从该输入设备中接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果之前，如果该终端的特定交互行为

所对应的交互对象发生变化，或者该终端产生新的该特定交互行为，则该处理器还用于重新确定该终端的第一类认证信息和第二类认证信息，以便通过该通信接口在该显示设备中向该终端的用户呈现第二认证挑战集合，该第二认证挑战集合基于该确定单元重新确定后的第一类认证信息和第二类认证
5 信息生成。

结合第三方面的第三种可能的实现方式，在第四种可能的实现方式中，具体实现为该终端的特定交互行为所对应的交互对象发生变化包括：增加该终端的特定交互行为所对应的交互对象，或者删除该终端的特定交互行为所对应的交互对象，或者修改该终端的特定交互行为所对应的交互对象。

结合第三方面或第三方面的第一种可能的实现方式至第三方面的第四种可能的实现方式中任一种可能的实现方式，在第五种可能的实现方式中，具体实现为：该终端的特定交互行为包括该终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为联系人的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性信息；或者，该终端的特定交互行为包括该终端访问网站的行为，该第一类认证信息和该第二类认证信息为网站的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，该终端的特定交互行为包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，该终端的特定交互行为包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。
10
15
20
25

结合第三方面或第三方面的第一种可能的实现方式至第三方面的第五种可能的实现方式中任一种可能的实现方式，在第六种可能的实现方式中，该处理器还用于配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数 N。在用于根据该识别结果中该第一类
30 认证信息的识别正确率确定认证结果的过程中，该处理器具体用于：如果该识别结果中该终端的用户识别的该第一类认证信息的条数不小于 N 条，则确

定对该终端的用户的认证通过，或者，如果该识别结果中该终端的用户识别的该第一类认证信息的条数小于 N 条，则确定对该终端的用户的认证不通过。

结合第三方面的第六种可能的实现方式，在第七种可能的实现方式中，
5 该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对该终端的用户的认证的安全强度越大；对该终端的用户进行认证所需要识别的第一类认证信息的条数越大，则通过对该终端的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对该终端的用户的认证的安全强度越大。

10 结合第三方面或第三方面的第一种可能的实现方式至第三方面的第七种可能的实现方式中任一种可能的实现方式，在第八种可能的实现方式中，具体实现为：该预定范围为该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在
15 总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间
间内发生次数排名在预定比例以内的范围。

结合第三方面或第三方面的第一种可能的实现方式至第三方面的第八种可能的实现方式中任一种可能的实现方式，在第九种可能的实现方式中，
20 该处理器还用于配置该终端的排除认证信息集合，其中该排除认证信息集合中的认证信息不允许作为该第一类认证信息。在用于确定该终端的第一类认证信息的过程中，该处理器具体用于确定该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围且不属于该排除认证集合的特定属性信息为该第一类认证信息。
25

结合第三方面或第三方面的第一种可能的实现方式至第三方面的第九种可能的实现方式中任一种可能的实现方式，在第十种可能的实现方式中，该处理器还用于：根据该终端的该第一类认证信息和该第二类认证信息生成该第一认证挑战集合，以便向该终端的用户呈现该第一认证挑战集合。

30 结合第三方面或第三方面的第一种可能的实现方式至第三方面的第十种可能的实现方式中任一种可能的实现方式，在第十一种可能的实现方式

中，该终端包括智能手机、平板电脑、个人计算机、服务器或工作站。

结合第三方面或第三方面的第一种可能的实现方式至第三方面的第十一种可能的实现方式中任一种可能的实现方式，在第十二种可能的实现方式中，该显示设备和该输入设备为该终端中同时具备显示和输入功能的同一设备；或者，该显示设备和该输入设备为该终端中不同的设备。
5

基于以上技术方案，本发明实施例的用户认证方法、认证装置和终端，通过根据用户最近最频繁使用的特定交互对象的特定属性信息进行身份认证。由于最近最频繁使用的特定交互对象的特定属性信息属于用户记忆期内的信息，可以降低用户记忆的代价，同时每次出现的认证信息都不固定，又
10 可以避免因为不慎被偷窥而导致认证信息被窃取，从而能够在降低用户记忆代价的同时具备一定的抗偷窥能力。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术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他的附图。
15

图 1 是本发明实施例用户认证的方法流程图。

图 2 是本发明实施例以联系人信息进行用户认证的流程示意图。

20 图 3 是本发明实施例以播放的音乐作品信息进行用户认证的流程示意图。

图 4 是本发明实施例以访问网站的网站信息进行用户认证的流程示意图。

图 5 是本发明实施例以阅读的电子书信息进行用户认证的流程示意图。

25 图 6 是本发明实施例以使用的 APP 进行用户认证的流程示意图。

图 7 是本发明实施例认证装置的结构示意图。

图 8 是本发明实施例终端的结构示意图。

具体实施方式

30 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是

全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

图 1 是本发明实施例用户认证的方法流程图。图 1 的方法由认证装置执行。该认证装置可以是终端内的系统的一个认证模块，或者是终端内的一个实现认证功能的芯片，本发明实施例在此不作限制。
5 实现认证功能的芯片，本发明实施例在此不作限制。

101，确定终端的第一类认证信息和第二类认证信息。

其中，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类
10 交互对象信息用于干扰该终端的用户选择该第一类认证信息。

应理解，特定交互行为，是指认证过程中用于判定发生频度的交互行为。特定交互行为所对应的交互对象，是指采集第一类认证信息的来源，该交互对象的特定属性信息可用于构成第一类认证信息。

应理解，该特定属性信息为该交互对象的一种属性信息或多种属性信息
15 的组合，可例如唯一标识、名称、图片，或者名称+图片，等等。

应理解，不同交互对象的特定属性信息可能相同。例如，同一个专辑的音频文件中，其专辑名称相同。又例如，几本不同电子书的作者，可能为同一个作者，等等。在确认第一类认证信息时，是以特定交互行为所对应的交互对象的特定属性信息的发生频率来确定的。
20

应理解，该第二类认证信息可包括以下至少一种：该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。
25

可选地，该终端的特定交互行为是认证过程中指定的交互行为。该终端的特定交互行为可以有多种表现形式，相应的，该第一类认证信息和该第二类认证信息也可以有多种表现形式。例如，该终端的特定交互行为可包括该终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为联系人的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性
30

信息；或者，该终端的特定交互行为可包括该终端访问网站的行为，该第一类认证信息和该第二类认证信息为网站的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，该终端的特定交互行为可包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。本发明实施例的一种具体实现方式，当第一类认证信息为联系人的特定属性信息时，该联系人信息具体可以是联系人的照片、联系人的姓名、联系人的联系电话，或者联系人的姓名+图片等等。本发明实施例的另一种具体实现方式，当第一类认证信息为音频文件信息时，该音频文件信息可以是音频文件的名称、音频文件的专辑名称或者是音频文件的演奏者，等等。

可选地，该终端可以有多种具体实现形式，例如，智能手机、平板电脑、个人计算机、服务器或工作站。当然，该终端还可以是其它具备认证功能的设备，本发明实施例在此不作限制。

应理解，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，其中发生频度为预定范围，该范围可以是一个绝对频度范围，也可以是一个相对频度范围，例如该预定范围为该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。例如，该第一类认证信息可以是3天内通话次数在5次以上的联系人的姓名，或者是2天内电子书阅读次数占两天内总阅读10%以上的电子书名称，或者是5天内播放排名前3位的音乐专辑，或者是12小时内访问网站频率在前5%的网站，等等。

应理解，该预定时间、预定范围都是可配置的。例如，可将该预定时间配置为12小时，1天，2天，3天乃至1月，等等，本发明实施例对此不作

限制。又例如，可将该预定范围配置为发生频度在 1 次以上，5 次以上，或者是所有发生频度的前 5 名，前 5%，等等。

可选地，该第一类认证信息还包括该终端的用户在该终端中所指定的交互对象的特定属性信息，以便减少该终端的用户对该第一类认证信息的记忆
5 代价。

可选地，在步骤 101 之前，该方法还可包括：配置该终端的排除认证信息集合，其中，该排除认证信息集合中的认证信息不允许作为该第一类认证信息。此时，步骤 101 中，确定该终端的第一类认证信息具体可实现为：确定该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间
10 内发生频度为预定范围且不属于该排除认证集合的特定属性信息为该第一类认证信息。

102，向该终端的用户呈现第一认证挑战集合。

其中，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息。

15 103，接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果。

104，根据该识别结果中该第一类认证信息的识别正确率确定认证结果。

本发明实施例中，通过使用终端中预定时间内预定发生频率的交互对象的特定属性信息动态地生成认证信息以对用户进行认证，由于最近最频繁使用的特定交互对象的信息属于用户记忆期内的信息，可以降低用户记忆的代价，同时每次出现的认证信息都不固定，又可以避免因为不慎被偷窥而导致
20 认证信息被窃取，因此本发明实施例的认证方法在减少用户对认证信息的记忆代价的同时，还具备一定的抗偷窥能力。

另外，本发明实施例的方法，由于可以基于访问频率动态地生成认证信息以对用户进行认证，还可以提高用户的使用体验。
25

可选地，在步骤 103 之前，该方法还可包括：如果该终端的特定交互行为所对应的交互对象发生变化，或者该终端产生新的该特定交互行为，则重新确定该终端的第一类认证信息和第二类认证信息，并向该终端的用户呈现第一认证挑战集合，其中该第二认证挑战集合基于重新确定后的第一类认证信息和第二类认证信息生成。在具体的应用中，该终端的特定交互行为所对应的交互对象发生变化包括：增加该终端的特定交互行为所对应的交互对
30

象，或者删除该终端的特定交互行为所对应的交互对象，或者修改该终端的特定交互行为所对应的交互对象。应理解，导致第一类认证信息和第二类认证信息发生变化的行为并不限于上述列举的情况，导致交互对象发生变化的情况也不限于上述列举的情况。

5 可选地，在步骤 101 之前，该方法还可包括：配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数 N。应理解，对该终端的用户进行认证所需要识别的第一类认证信息的条数为该终端的用户在用户认证过程中需要从该第一认证挑战集合中识别出来的第一类认证信息的条数。此时，步骤 104 具体实现为：如果该识别结果中该终端的用户识别出的第一类认证信息不小于 N 条，则确定对该终端的用户的认证通过；或者如果该识别结果中该终端的用户识别出的第一类认证信息小于 N 条，则确定对该终端的用户的认证不通过。其中，N 取值为正整数。

10 具体地，该配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数可包括：通过配置该预定时间、该预定范围以及该对该终端的用户进行认证所需要识别的第一类认证信息的条数调整对该终端的用户的认证的安全强度。其中，如果该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对该终端的用户的认证的安全强度越大；如果对该终端的用户进行认证所需要识别的第一类认证信息的条数越大，则通过对该终端的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对该终端的用户的认证的安全强度越大。

15 可选地，在步骤 102 之前，该方法还包括：根据该终端的该第一类认证信息和该第二类认证信息生成该第一认证挑战集合，以便向该终端的用户呈现第一认证挑战集合。

20 下面将结合具体的实施例，对本发明实施例的方法做进一步的描述。

25 图 2 是本发明实施例以联系人信息进行用户认证的流程示意图。本发明实施例中，认证信息为联系人的特定属性信息。此时，联系人的特定属性信息的发生频度等于终端的用户访问联系人的访问频度，认证装置根据终端中最近频繁访问的联系人的特定属性信息进行用户认证。本发明实施例中的联系人，可以是终端中电话通讯录中的联系人、邮件的联系人或者其它社交软件的联系人；联系人的特定属性信息，可以是联系人的姓名，联系人的姓名+照片，等等，本发明实施例在此不作限制。为方便描述，下文提到的联系

人信息即指代联系人的特定属性信息。

第一类认证信息，包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内访问频度为预定范围的特定属性信息。本发明实施例中，第一类认证信息为该终端的联系人信息中预定时间内访问频度为预定范围的联系人信息，即最近频繁联系人信息，该联系人信息可以是联系人姓名、联系人姓名+照片等。第二类认证信息，用于干扰终端的用户对第一类认证信息的判断。该第二类认证信息可以是该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内访问频度为预定范围以外的特定属性信息，或者是不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。在本发明实施例中，该第二类认证信息可以是预定时间内访问频度在预定范围外的联系人信息，或者是不属于该终端的联系人信息。

应理解，本发明实施例中，不同联系人的联系人信息一般不相同。也就是说，确定联系人可以等价于确定联系人信息。

如图 2 所示，本发明实施例初始认证过程的详细步骤具体如下：

210，认证参数配置。

用户可对认证装置的工作方式进行配置，配置的参数可保存在认证装置的配置数据库中。

用户可进行以下配置：

(1) 排除联系人(可记为 NP)，即排除交互对象。其中集合 NP 的元素不出现在第一类联系人中。当然，为了避免混淆，集合 NP 的元素也不会出现在第二类联系人中。

(2) 第一类联系人选择方法参数，可包括有效的访问联系人记录的时间要求(记为 T，例如 3 天、5 天、10 小时等)，联系人访问频度要求(记为 X，表示预定次数，例如 5 次，或表示预定名次，例如前 3 名，或表示预定比例，例如 3% 等)。基于 T 和 X 确定的第一类联系人可记为 L。当然，用户也可不进行配置，认证装置可对第一类联系人选择方法参数设置一个默认设置。另外，用户也可指定一个或多个联系人作为固定的第一类联系人，而不是通过上述 T 和 X 临时计算获得。用户指定的第一类联系人可记为 D。

(3) 第二类联系人参数，可包括构造认证信息时混淆项数目(记为 f)和/或构造认证信息时的干扰项的数目(记为 i)。其中，混淆项是指系统随

机生成的虚假联系人，或者说终端中不存在的联系人，干扰项是指用户最近没有与之联系的联系人。

(4) 认证选择参数，可包括每次认证必须同时正确选择的第一类联系人的个数(记为 c，例如，必须要同时正确选择 3 个才算通过认证)。认证装置还可引入一个安全强度调整功能，通过调整上述 f、i 和 c 的值来调整身份认证的安全强度，显然这三个数值越大，安全强度越高。具体地，认证装置可设定不同的难度级别，每个级别对应不同的值，其实现可通过安全强度拖动条或难度选择框等实现；或者，认证装置可提供一个数值调整功能，分别调整上述三个值。

10 配置完毕后，认证装置在启动认证时会自动加载对应的配置参数。

应理解，本发明实施例中，第一类联系人的信息即为第一类认证信息，第二类联系人的信息即为第二类认证信息。

220，读取终端的联系人。

15 认证装置可读取终端中维护的通讯录放入集合 M。对于终端的电话通讯录，认证装置可以通过系统的 API 获取联系人信息；对于邮件或其它社交程序，认证装置可以通过软件程序的插件或者系统 API Hook 获取联系人信息。

230，确定第一类联系人的集合。

20 如果用户指定了使用集合 D 或终端中尚且没有足够的联系记录，则认证装置直接将 D 中所有元素加入集合 L 中；否则通过系统 API 读取终端设备电话程序、邮件程序或其它社交软件维护的时间 T 之内的联系记录 N，去除在联系人在 NP 集合中或者不在终端的通讯录中的联系记录，计算每个联系人的出现频率并且排序，取得联系频率满足要求的一组联系人，放入集合 L。在计算联系频率时可以有多种方法，例如可以只包含终端属主动对外发起的联系记录，而忽略联系人对终端属主发起的联系记录，或者同时包含两者。

25 此时构建的集合 L 为第一类联系人的集合。

另外，在通过 T 和 X 确定第一类联系人时，可以根据 X 所表示的内容来确定第一类联系人的范围。本发明实施例的第一种具体实现方式，X 表示预定访问次数，此时可确定预定时间内访问频度在预定次数以上的联系人为第一类联系人，例如，3 天内访问频度为 5 次以上的联系人为第一类联系人。
30 本发明实施例的第二种具体实现方式，X 表示总访问次数的第一预定比例，此时可确定预定时间内访问频度在总访问次数的第一预定比例以上的联系

人为第一类联系人，其中该总访问次数为预定时间内对联系人的总访问次数，例如 5 天内访问频度在总访问次数的 3%以上的联系人。本发明实施例的第三种具体实现方式，X 表示访问频度的预定名次，此时可确定预定时间内访问频度排名在预定名次以内的联系人，例如 10 小时内访问频度排名前 3 5 名的联系人。本发明实施例的第四种具体实现方式，X 表示访问频度排名的第二预定比例，此时可确定预定时间内访问频度排名在第二预定比例以上的联系人为第一类联系人，例如 5 天内访问频度排名前 3%的联系人。

当然，还可能存在其它确定第一类联系人的算法，本发明实施例在此不作限制。

10 240，确定参与认证的第一类联系人及第二类联系人中的干扰项。

本发明实施例中，干扰项是指用户最近没有访问过的联系人的信息。

认证装置根据配置信息从集合 M 中选取一个大小为 i 的子集 R，要求用户最近没有与集合 R 中的联系人联系过，且集合 R 中元素都不在 L 中，然后从集合 L 中取一个大小为 c 的子集 V，作为本次认证中要求用户的识别出 15 来的第一类联系人。

如果集合 L 包含了系统中所有的联系人，则集合 R 为空，此时方案退化为要求用户从包含虚假联系人的联系人集合中识别出真实存在的联系人。

另外，为了降低记忆的难度，还可以增加 V 中元素的个数，也就是说，V 中元素的个数可以多于 c 个。

20 250，确定第二类联系人中的混淆项。

本发明实施例中，混淆项是指系统随机生成的虚假联系人，或者说终端中不存在的联系人。

认证装置生成一组虚假联系人，个数为 f，记为集合 F。虚假联系人可以按照系统中初始配置好的常见姓氏和常见名字以及相关信息（如头像等） 25 随机组合而成，也可以通过连接远端网络服务获取。集合 F 中的元素不能在集合 L 或 D 中出现。严格地说，集合 F 中的元素也不能在集合 R 中出现。

当然，也可不生成混淆项，此时 f 为 0，集合 F 为空集。

260，生成认证挑战集合。

认证装置将集合 V、R 和 F 中的元素打乱混合，形成认证挑战集合 A， 30 即 $A=V+R+F$ （其中符号“+”代表集合加）。

270，呈现认证挑战集合，确认认证结果。

认证装置将认证挑战集合 A 呈现给用户，以供用户进行识别。

根据用户的认证识别结果，认证装置可确定认证的结果。如果用户能够从中选择出 c 个 V 中的元素，则认证成功；否则认证失败。

例如，可向用户呈现 24 条联系人信息，如果用户能够从中选择出 3 条正确的联系人信息，则认证成功，否则认证失败。

本发明实施例中，在计算第一类联系人时，可以按照联系行为产生时间到当前的时间长度进行赋权计算，用户也可以直接指定一组固定的联系人作为永久的第一类联系人，此时相当于对这组固定的联系人都赋予了最大的权。通过在构建最终显示在屏幕上的联系人集合 A 的过程中引入虚假联系人集合 F，可以提高选择空间的大小，起到混淆的作用，另外还可以保护集合 R 和 V 中的信息，避免攻击者直接推断出终端中真实存在的联系人。另外，通过引入集合 R 可以进一步提高选择的难度，避免一个熟悉当前终端属主的攻击根据其关于该终端属主可能常用联系人的背景知识直接猜测出第一类联系人。

如图 2 所示，本发明实施例的方法可支持多种运行模式。当开机首次进行运行或者认证参数配置发生变化时，需要执行初始认证模式。初始认证模式需要执行前述步骤 210 至步骤 270。如图 2 的箭头 272 指向所示，在认证结束后，如果认证参数配置发生变化，初始认证模式直接跳转到步骤 210，执行步骤 210 至步骤 270。当用户发生新的联系行为之后，此时用户的第一类联系人可能已经发生变化，认证装置需要执行联系认证模式。理论情况下，认证装置可在步骤 270 之前，步骤 230 之后的任一个步骤执行联系认证模式，但是，实际情况下，在认证过程中通常不会产生认证以外的交互行为，只有在认证结束后才可能产生别的交互行为。如图 2 的箭头 273 指向所示，此时，联系认证模式需要跳转到步骤 230，执行步骤 230 到步骤 270。重选认证主要在用户希望提供最强的抗偷窥能力，或当用户认证错误次数太多时使用，要求在集合 L 不变的前提下每次重新计算的子集 V 都不同，最多可以重选 $C_{L,V}$ (组合计算) 次。与联系认证模式类似，重选认证模式需要在上一次认证完毕后执行。如图 2 的箭头 274 指向所示，此时，重选认证模式需要跳转到步骤 240，重选认证模式需要执行步骤 240 到步骤 270，不变认证模式中集合 A 完全不变，基于同样的秘密和干扰信息对用户进行认证。如图 2 的箭头 271 指向所示，此时不变认证模式只需要重新执行步骤 270。

在不变认证模式下，如果当前用户认证错误，下次认证仍然基于同样的干扰和秘密进行。随着通过逐步试错，排除的联系人组合逐渐增多，攻击者猜中可能性增大，但是下降速度非常缓慢。例如假设集合 A 中包含 24 个元素，认证时要求识别出 3 个第一类联系人（集合 V 大小为 3），则攻击者 5 开始猜中的概率是 $1/2024$ （3 个联系人的组合数为 $24*23*22/6=2024$ ），攻击者尝试 m 次之后，其猜中的概率变为 $1/2014-m$ ，由此可以看出该方案在常见的参数尺寸下抵抗数千次的猜测攻击。通过在用户连续认证错误的情况，延时一段时间再进行认证（例如 30 秒），该方案可以长时间抵抗猜测攻击。为了进一步提高抗猜测能力，在连续认证错误一定次数之后，系统执行 10 一次重选认证，可以重新计算挑战集合 A，然后重新进入不变认证模式。

现有各种的认证方案，如口令，由于秘密是固定的，所以一旦认证时被偷窥，攻击者就能够掌握所有认证秘密，完全突破认证机制。本方案的认证秘密是基于第一类联系人这一不断动态变化的信息的。假设攻击者偷窥到了 15 用户上次认证的秘密（当时的一组第一类联系人），并且他有条件能够拿到用户的终端，则他可以基于以前获得的秘密尝试认证。在很多情况下，终端的真实用户已经发生过几次新的通讯行为，此时第一类联系人已经发生变化，则上次的认证秘密失效，本方案具有完全的抗偷窥能力。在极少的情况下即使用户没有发生过任何新的通讯行为，如果用户对于抗偷窥特别关心，可以设置系统每次都执行重选认证，使得每次都基于不同的秘密认证用户， 20 结合认证错误时延，可以提供较好的抗偷窥能力。例如用户有 8 个符合条件的第一类联系人 ($|L|=8$)，如果每次要求选中 3 个频繁联系人 ($|v|=3$)，则在执行 56 次重选认证之前，每次认证的秘密都不相同。

本发明实施例的方法通过虚假联系人集合 F 保护终端中真实存在的联系人信息，避免隐私信息的泄露。如果攻击者没有当前终端属主的可能的联系人的背景知识，则他将难以通过终端屏幕上的显示信息把终端中部分的真实的联系人从虚假联系人中区分开来，所以此时本方案不会引起额外的信息泄露。如果攻击者 M 同时拥有当前终端属主 N 和 N 的联系人 O 的背景知识，且拿到了 N 的终端，则此时 M 从 N 的终端上能够获得最大信息的是：N 和 O 相互认识。此时这种隐私泄露量是极为微量的。 25

图 3 是本发明实施例以播放的音乐作品信息进行用户认证的流程示意图。本发明实施例中，认证信息为音频文件的特定属性信息，例如音频文件 30

名称、音频文件的专辑名称、音频文件中音乐的演奏者，音频文件中音乐的演唱歌手、演奏乐队或乐团等。本发明实施实例通过让用户回忆和选择其最近频繁播放收听的音乐作品或者音乐作品演奏者来实现对终端属主（即用户）的识别。为方便描述，下文提到的音乐作品信息即音频文件的特定属性
5 信息。

本发明实施例中，认证装置可通过各种方式获取音频文件的音乐作品信息。例如，认证装置可能包括一个音频文件监控模块，用于监控终端的系统中音频文件及其打开的情况。

本发明实施例中，第一类认证信息为预定时间内发生频度在预定范围的
10 音乐作品信息。应理解，一个音乐作品信息可能可以对应于多个音频文件。例如，当音乐作品信息为专辑名称时，属于同一专辑的所有音频文件的音乐作品信息相同，在计算发生频率时，应将属于同一专辑的所有音频文件的音乐作品信息合在一起计算。第二类认证信息为用于干扰用户判断的音乐作品信息。
15

如图 3 所示，本发明实施例初始认证过程的详细步骤具体如下：

310，认证参数配置。

用户可对认证装置的工作方式进行配置，配置的参数可保存在认证装置的配置数据库中。

用户可进行以下配置：

20 (1) 排除音乐作品信息(可记为 NP)，此部分指定的音乐作品信息(例如，专辑、演奏者、演唱歌手、乐队等)将不参与认证信息的生成过程，从而允许用户可以直接排除一些敏感的音乐曲目或终端所有者的被众所周知的偏爱艺人。换句话说，集合 NP 的元素不出现在第一类音乐作品信息中。当然，为了避免混淆，集合 NP 的元素也不会出现在第二类音乐作品信息中。
25

(2) 第一类音乐作品信息选择方法参数，可包括有效的播放音乐作品的时间要求(记为 T，例如 3 天、5 天、10 小时等)，音乐作品信息发生频度要求(记为 X，表示预定次数，例如 5 次，或表示预定名次，例如前 3 名，或表示预定比例，例如 3% 等)。基于 T 和 X 确定的第一类音乐作品信息可记为 L。当然，用户也可不进行配置，认证装置可对第一类音乐作品信息选择方法参数设置一个默认设置。另外，用户也可指定一个或多个音乐作品信息作为固定的第一类音乐作品信息，而不是通过上述 T 和 X 临时计算获得。
30

用户指定的第一类音乐作品信息可记为 D。

(3) 第二类音乐作品信息参数，可包括构造认证信息时混淆项数目（记为 f）和/或构造认证信息时的干扰项的数目（记为 i）。其中，混淆项是指系统随机生成的虚假音乐作品信息，或者说终端中不存在的音乐作品信息，
5 干扰项是指没有出现在用户最近播放过音乐作品中的音乐作品信息。

(4) 认证选择参数，可包括每次认证必须同时正确选择的第一类音乐作品信息的个数（记为 c，例如，必须要同时正确选择 3 个才算通过认证）。认证装置还可引入一个安全强度调整功能，通过调整上述 f、i 和 c 的值来调整身份认证的安全强度，显然这三个数值越大，安全强度越高。具体地，
10 认证装置可设定不同的难度级别，每个级别对应不同的值，其实现可通过安全强度拖动条或难度选择框等实现；或者，认证装置可提供一个数值调整功能，分别调整上述三个值。

配置完毕后，认证装置在启动认证时会自动加载对应的配置参数。

应理解，本发明实施例中，第一类音乐作品信息即为第一类认证信息，
15 第二类音乐作品信息即为第二类认证信息。

320，读取终端的音乐作品信息。

认证装置可包括音频文件监控模块，用于监控音频文件的播放情况。认证装置可通过音频文件监控模块读取终端存储的所有音频文件及其演奏者的列表（记为 L1）、最近音频文件播放列表（记为 L2）。如果音频文件监控
20 开关打开，则可以通过 Hook 系统文件打开函数等方式监控终端系统中对音频文件的打开操作，并且对数据库记录的信息进行持续更新。当然认证装置也可通过类似音频文件监控模块的功能模块实现上述功能，本发明实施例在此不作限制。

330，确定第一类音乐作品信息的集合。

如果用户指定了集合 D 或者终端中尚且没有足够的音乐播放记录，则把
25 D 中的元素都放入集合 L 中；否则模块根据 L2 计算音乐和演奏者的播放频度，取出一组最近频繁播放的音乐或作品演奏者放入集合 L。如果 L 的元素个数小于 c，则可以把所有音频文件列表或所有音频文件对应的演奏者放入集合 L 中。

30 通过 T 和 X 确定第一类音乐作品信息的集合的具体实现方式与步骤 230 中确定第一类联系人的方式类似，本发明实施例在此不再赘述。

此时构建的集合 L 为第一类音乐作品信息的集合。

340，确定参与认证的第一类音乐作品信息及第二类音乐作品信息中的干扰项。

本发明实施例中，干扰项是指没有出现在用户最近播放过音乐作品中的
5 音乐作品信息。

认证装置根据配置信息从集合 L1 中选取一个大小为 i 的子集 R，要求 R 中元素都没有在集合 L2 中出现（这些音乐作品信息近期未出现过），且集合 R 中元素都不在 L 中，然后从集合 L 中取一个大小为 c 的子集 V，作为本次
10 认证中要求用户的识别出来的第一类音乐作品信息。如果 L 包含了终端上的所有音频文件，则 R 为空而没有干扰项，此时方案退化为要求用户从包含虚假音乐作品信息集合中识别出终端上真实存在的音乐作品信息。

另外，为了降低记忆的难度，还可以增加 V 中元素的个数，也就是说，
V 中元素的个数可以多于 c 个。

350，获取第二类音乐作品信息中的混淆项。

15 本发明实施例中，混淆项是指系统随机生成的音乐作品信息，或者说终端中不存在的音乐作品信息。

认证装置生成一组虚假音乐作品信息（虚假的音乐、音乐专辑或者演奏者等），个数为 f，记为集合 F。虚假音乐作品信息可以按照系统中初始配置好的音乐库或者演奏者库而成；也可以通过连接远端网络服务获取。集合 F
20 中的元素不能在集合 L 或 D 中出现。

当然，也可不生成混淆项，此时 f 为 0，集合 F 为空集。

360，生成认证挑战集合。

认证装置将集合 V、R 和 F 中的元素打乱混合，形成认证挑战集合 A，即
A=V+R+F（其中符号“+”代表集合加）。

25 370，呈现认证挑战集合，确认认证结果。

认证装置将认证挑战集合 A 呈现给用户，以供用户进行识别。

根据用户的认证识别结果，认证装置可确定认证的结果。如果用户能够从中选择出 c 个 V 中的元素，则认证成功；否则认证失败。

本发明实施例中，在计算第一类音乐作品信息时，可以按照播放行为产生时间到当前的时间长度进行赋权计算，用户也可以直接指定一组固定的音乐作品信息作为第一类音乐作品信息，此时相当于对这组固定的实体都赋予
30

了最大的权。通过在构建最终显示在屏幕上的集合 A 的过程中引入虚假认证信息集合 F，提高选择空间的大小，起到混淆的作用，以提高对用户的区分度，另外还可以保护集合 R 和 V 中的信息。本方法引入集合 R 的目的是进一步提高选择的难度，避免一个知道终端中存在的音乐作品信息的攻击者直接猜测出第一类音乐作品信息。

如图 3 所示，本发明实施例的方法可支持多种运行模式。当开机首次进行运行或者认证参数配置发生变化时，需要执行初始认证模式。初始认证模式需要执行前述步骤 310 至步骤 370。如图 3 的箭头 372 指向所示，在认证结束后，如果认证参数配置发生变化，初始认证模式直接跳转到步骤 310，
10 执行步骤 310 至步骤 370。当用户发生新的播放行为之后，此时用户的第一类音乐作品信息可能已经发生变化，认证装置需要执行播放认证模式。理论情况下，认证装置可在步骤 370 之前，步骤 330 之后的任一个步骤执行播放认证模式，但是，实际情况下，在认证过程中通常不会产生认证以外的交互行为，只有在认证结束后才可能产生别的交互行为。如图 3 的箭头 373 指向
15 所示，此时，播放认证模式需要跳转到步骤 330，执行步骤 330 到步骤 370。重选认证主要在用户希望提供最强的抗偷窥能力，或当用户认证错误次数太多时使用，要求在集合 L 不变的前提下每次重新计算的子集 V 都不同，最多可以重选 $C_{|L|}^{IV}$ (组合计算) 次。与播放认证模式类似，重选认证模式需要在上一次认证完毕后执行。如图 3 的箭头 374 指向所示此时，重选认证模式
20 需要跳转到步骤 340，重选认证模式需要执行步骤 340 到步骤 370，不变认证模式中集合 A 完全不变，基于同样的秘密和干扰信息对用户进行认证。如图 3 的箭头 371 指向所示，此时不变认证模式只需要重新执行步骤 370。

在不变认证模式下，如果当前用户认证错误，下次认证仍然基于同样的干扰和秘密进行。随着通过逐步试错，排除的音乐作品信息组合逐渐增多，
25 攻击者猜中可能性增大，但是下降速度非常缓慢。例如假设集合 A 中包含 24 个元素，认证时要求识别出 3 个第一类音乐作品信息(集合 V 大小为 3)，则攻击者一开始猜中的概率是 $1/2024$ (3 个音乐作品信息的组合数为 $24*23*22/6=2024$)，攻击者尝试 m 次之后，其猜中的概率变为 $1/2014-m$ ，由此可以看出该方案在常见的参数尺寸下抵抗数千次的猜测攻击。通过在用
30 户连续认证错误的情况下，延时一段时间再进行认证(例如 30 秒)，该方案可以长时间抵抗猜测攻击。为了进一步提高抗猜测能力，在连续认证错误一定

次数之后，系统执行一次重选认证，可以重新计算挑战集合 A，然后重新进入不变认证模式。

现有各种的认证方案，如口令，由于秘密是固定的，所以一旦认证时被偷窥，攻击者就能够掌握所有认证秘密，完全突破认证机制。本方案的认证
5 秘密是基于第一类音乐作品信息这一不断动态变化的信息的。假设攻击者偷
窥到了用户上次认证的秘密（当时的一组第一类音乐作品信息），并且他有
条件能够拿到用户的终端，则他可以基于以前获得的秘密尝试认证。在很多
情况下，终端的真实用户已经发生过几次新的播放行为，此时第一类音乐作品
10 信息已经发生变化，则上次的认证秘密失效，本方案具有完全的抗偷窥能
力。在极少的情况下即使用户没有发生过任何新的播放行为，如果用户对于
抗偷窥特别关心，可以设置系统每次都执行重选认证，使得每次都基于不同的
秘密认证用户，结合认证错误时延，可以提供较好的抗偷窥能力。例如用
户有 8 个符合条件的第一类音乐作品信息 ($|L|=8$)，如果每次要求选中 3 个
15 第一类音乐作品信息 ($|l|=3$)，则在执行 56 次重选认证之前，每次认证的秘
密都不相同。

图 4 是本发明实施例以访问网站的网站信息进行用户认证的流程示意图。本发明实施例中，认证信息为访问网站的特定属性信息，例如网址、网
站名、网站图标、域名等作为用户识别的网站标识。为方便描述，下文提到
的网站信息即指代访问网站的特定属性信息。

20 本发明实施例中，认证装置可通过各种方式获取网站信息。例如，认证
装置可能包括一个网址输入监控模块，负责监控并记录用户在浏览器中的网
址输入，实现形式可以是嵌入到现有浏览器中的 BHO (浏览器辅助对象)
对象或者手机设备制造商自主开发的、支持网址访问记录的浏览器。网址输
入监控模块可一直监控和记录用户通过浏览器地址栏或者收藏夹输入的网
25 站地址，浏览器自动打开窗口自动进行的网址访问不进行记录。

本发明实施例中，第一类认证信息为预定时间内访问频度在预定范围的
网站信息。第二类认证信息为用于干扰用户判断的网站信息。

如图 4 所示，本发明实施例初始认证过程的详细步骤具体如下：

410，认证参数配置。

30 用户可对认证装置的工作方式进行配置，配置的参数可保存在认证装置
的配置数据库中。

用户可进行以下配置：

(1) 排除网站信息(可记为NP)，此部分指定网站信息将不参与认证信息的生成过程，从而允许用户可以直接排除一些用户感到敏感而不想使用的网址和一些用户几乎每天都固定会访问的网站。换句话说，集合NP的元素不出现在第一类网站信息中。当然，为了避免混淆，集合NP的元素也不会出现在第二类网站信息中。

(2) 第一类网站信息选择方法参数，可包括有效的网站信息的时间要求(记为T，例如3天、5天、10小时等)，网站信息发生频度要求(记为X，表示预定次数，例如5次，或表示预定名次，例如前3名，或表示预定比例，例如3%等)。基于T和X确定的第一类网站信息可记为L。当然，用户也可不进行配置，认证装置可对第一类网站信息选择方法参数设置一个默认设置。另外，用户也可指定一个或多个网站信息作为固定的第一类网站信息，而不是通过上述T和X临时计算获得。用户指定的第一类网站信息可记为D。

(3) 第二类网站信息参数，可包括构造认证信息时混淆项数目(记为f)和/或构造认证信息时的干扰项的数目(记为i)。其中，混淆项是指系统随机生成的虚假网站信息，即用户从未访问过的网站的网站信息，干扰项是指用户之前访问过但最近没有访问过的网站的网站信息。

(4) 认证选择参数，可包括每次认证必须同时正确选择的第一类网站信息的个数(记为c，例如，必须要同时正确选择3个才算通过认证)。认证装置还可引入一个安全强度调整功能，通过调整上述f、i和c的值来调整身份认证的安全强度，显然这三个数值越大，安全强度越高。具体地，认证装置可设定不同的难度级别，每个级别对应不同的值，其实现可通过安全强度拖动条或难度选择框等实现；或者，认证装置可提供一个数值调整功能，分别调整上述三个值。

配置完毕后，认证装置在启动认证时会自动加载对应的配置参数。

应理解，本发明实施例中，第一类网站信息即为第一类认证信息，第二类网站信息即为第二类认证信息。

420，读取终端的网站信息。

认证装置可包括网址输入监控模块，用于监控访问的网站。认证装置可通过网址输入监控模块读取终端存储的用户网址访问记录(记为列表List)，如果监控开关打开，则可以通过网址输入监控模块监控用户网址输入并更新

列表 List。对于集合 NP 或集合 D 中的网站信息，可不予以记录。当然认证装置也可通过类似网址输入监控模块的功能模块，实现上述功能，本发明实施例在此不作限制。

430，确定第一类网站信息的集合。

5 初始启动或列表 List 更新后，模块按照预先配置的筛选条件选择一组最近频繁访问的网站放入集合 L。如果用户指定了集合 D 或者终端中尚且没有足够的网址记录，则把 D 中的元素都放入集合 L 中。从集合 L 中取一个大小为 c 的子集 V，作为本次认证中要求用户的识别出来的网站信息。如果 L 的大小小于 c，则可以把所有网址放入集合 L 中。

10 此时构建的集合 L 为第一类网站信息的集合。

440，确定参与认证的第一类网站信息及第二类网站信息中的干扰项。

本发明实施例中，干扰项是用户之前访问过但最近没有访问过的访问网站的网站信息。

15 认证装置根据配置信息从列表 List 中选取一个大小为 i 的子集 R，要求 R 中元素都不在 L 中，然后从集合 L 中取一个大小为 c 的子集 V，作为本次认证中要求用户的识别出来的第一类网站信息。如果 L 包含了终端上的所有访问网站的网站信息记录，则 R 为空而没有干扰项，此时方案退化为要求用户从包含虚假网站信息的集合中识别出终端上真实存在的访问网站的网站信息。

20 另外，为了降低记忆的难度，还可以增加 V 中元素的个数，也就是说，V 中元素的个数可以多于 c 个。

450，确定第二类网站信息中的混淆项。

本发明实施例中，混淆项是指系统随机生成的网站信息，或者说终端从未访问过的网站的网站信息。

25 认证装置生成一组虚假网站信息，个数为 f，记为集合 F。虚假网站信息可以按照系统中初始配置好的网站信息库筛选而生；也可以通过连接远端网络服务检索获取。集合 F 中的元素不能在集合 L 或 D 中出现。

当然，也可不生成混淆项，此时 f 为 0，集合 F 为空集。

460，生成认证挑战集合。

30 认证装置将集合 V、R 和 F 中的元素打乱混合，形成认证挑战集合 A，即 $A = V + R + F$ （其中符号“+”代表集合加）。

470，呈现认证挑战集合，确认认证结果。

认证装置将认证挑战集合 A 呈现给用户，以供用户进行识别。

根据用户的认证识别结果，认证装置可确定认证的结果。如果用户能够从中选择出 c 个 V 中的元素，则认证成功；否则认证失败。

5 本发明实施例中，在计算第一类网站信息时，可以按照访问行为产生时间到当前的时间长度进行赋权计算，用户也可以直接指定一组固定的网站信息作为第一类网站信息，此时相当于对这组固定的实体都赋予了最大的权。通过在构建最终显示在屏幕上的集合 A 的过程中引入虚假认证信息集合 F，提高选择空间的大小，起到混淆的作用，以提高对用户的区分度，另外还可以保护集合 R 和 V 中的信息。本方法引入集合 R 的目的是进一步提高选择的难度，避免一个知道终端中存在的网站信息的攻击者直接猜测出第一类网站信息。

如图 4 所示，本发明实施例的方法可支持多种运行模式。当开机首次进行运行或者认证参数配置发生变化时，需要执行初始认证模式。初始认证模式需要执行前述步骤 410 至步骤 470。如图 4 的箭头 472 指向所示，在认证结束后，如果认证参数配置发生变化，初始认证模式直接跳转到步骤 410，执行步骤 410 至步骤 470。当用户发生新的访问网站行为之后，此时用户的最近频繁访问网站可能已经发生变化，认证装置需要执行访问认证模式。理论情况下，认证装置可在步骤 470 之前，步骤 430 之后的任一个步骤执行访问认证模式，但是，实际情况下，在认证过程中通常不会产生认证以外的交互行为，只有在认证结束后才可能产生别的交互行为。如图 4 的箭头 473 指向所示，此时，访问认证模式需要跳转到步骤 430，执行步骤 430 到步骤 470。重选认证主要在用户希望提供最强的抗偷窥能力，或当用户认证错误次数太多时使用，要求在集合 L 不变的前提下每次重新计算的子集 V 都不同，最多可以重选 $C_{L,V}$ (组合计算) 次。与访问认证模式类似，重选认证模式需要在上一次认证完毕后执行。如图 4 的箭头 474 指向所示此时，重选认证模式需要跳转到步骤 440，重选认证模式需要执行步骤 440 到步骤 470，不变认证模式中集合 A 完全不变，基于同样的秘密和干扰信息对用户进行认证。如图 4 的箭头 471 指向所示，此时不变认证模式只需要重新执行步骤 470。

30 在不变认证模式下，如果当前用户认证错误，下次认证仍然基于同样的干扰和秘密进行。随着通过逐步试错，排除的网站信息组合逐渐增多，攻击

者猜中可能性增大，但是下降速度非常缓慢。例如假设集合 A 中包含 24 个元素，认证时要求识别出 3 个第一类网站信息（集合 V 大小为 3），则攻击者一开始猜中的概率是 $1/2024$ (3 个访问网站的组合数为 $24*23*22/6=2024$)，
5 攻击者尝试 m 次之后，其猜中的概率变为为 $1/2014-m$ ，由此可以看出该方案在常见的参数尺寸下抵抗数千次的猜测攻击。通过在用户连续认证错误的情况，延时一段时间再进行认证（例如 30 秒），该方案可以长时间抵抗猜测攻击。为了进一步提高抗猜测能力，在连续认证错误一定次数之后，系统执行一次重选认证，可以重新计算挑战集合 A，然后重新进入不变认证模式。

现有各种的认证方案，如口令，由于秘密是固定的，所以一旦认证时被
10 偷窥，攻击者就能够掌握所有认证秘密，完全突破认证机制。本方案的认证秘密是基于第一类网站信息这一不断动态变化的信息的。假设攻击者偷窥到了用户上次认证的秘密（当时的一组第一类网站信息），并且他有条件能够拿到用户的终端，则他可以基于以前获得的秘密尝试认证。在很多情况下，
15 终端的真实用户已经发生过几次新的访问行为，此时第一类网站信息已经发生变化，则上次的认证秘密失效，本方案具有完全的抗偷窥能力。在极少的情况下即使用户没有发生过任何新的访问行为，如果用户对于抗偷窥特别关心，可以设置系统每次都执行重选认证，使得每次都基于不同的秘密认证用户，结合认证错误时延，可以提供较好的抗偷窥能力。例如用户有 8 个符合
20 条件的第一类网站信息 ($|V|=8$)，如果每次要求选中 3 个第一类网站信息 ($|v|=3$)，则在执行 56 次重选认证之前，每次认证的秘密都不相同。

图 5 是本发明实施例以阅读的电子书信息进行用户认证的流程示意图。
本发明实施例中，认证信息为为阅读的电子书的特定属性信息，例如，电子书的书名，电子书的作者，电子书的封面，或者电子书的书名和封面的组合，等等。本发明实施例通过让用户回忆和识别他/她最近的频繁阅读的电子书实现身份验证。为方便描述，下文提到的电子书信息即指电子书的特定属性信息。
25

如图 5 所示，本发明实施例初始认证过程的详细步骤具体如下：

510，认证参数配置。

30 用户可对认证装置的工作方式进行配置，配置的参数可保存在认证装置的配置数据库中。

用户可进行以下配置：

(1) 排除电子书信息(可记为 NP)，此部分指定电子书信息将不参与认证信息的生成过程，从而允许用户可以直接排除一些用户认为敏感的电子书信息。换句话说，集合 NP 的元素不出现在第一类电子书信息。当然，为了避免混淆，集合 NP 的元素也不会出现在第二类电子书信息中。

(2) 第一类电子书信息选择方法参数，可包括有效的阅读的电子书的时间要求(记为 T，例如 3 天、5 天、10 小时等)，阅读的电子书信息发生频度要求(记为 X，表示预定次数，例如 5 次，或表示预定名次，例如前 3 名，或表示预定比例，例如 3% 等)。基于 T 和 X 确定的第一类电子书信息可记为 L。当然，用户也可不进行配置，认证装置可对第一类电子书信息选择方法参数设置一个默认设置。另外，用户也可指定一个或多个阅读的电子书作为固定的第一类电子书信息，而不是通过上述 T 和 X 临时计算获得。用户指定的第一类电子书信息可记为 D。(3) 第二类电子书信息参数，可包括构造认证信息时混淆项数目(记为 f) 和/或构造认证信息时的干扰项的数目(记为 i)。其中，混淆项是指系统随机生成的虚假电子书信息，或者说终端中不存在的电子书信息，干扰项是指用户最近没有阅读过的电子书信息。(4) 认证选择参数，可包括每次认证必须同时正确选择的第一类电子书信息的个数(记为 c，例如，必须要同时正确选择 3 个才算通过认证)。认证装置还可引入一个安全强度调整功能，通过调整上述 f、i 和 c 的值来调整身份认证的安全强度，显然这三个数值越大，安全强度越高。具体地，认证装置可设定不同的难度级别，每个级别对应不同的值，其实现可通过安全强度拖动条或难度选择框等实现；或者，认证装置可提供一个数值调整功能，分别调整上述三个值。

配置完毕后，认证装置在启动认证时会自动加载对应的配置参数。

25 520，读取终端的电子书阅读记录。

认证装置可通过类似电子书监控模块的功能模块，读取终端存储的中所有电子书的记录(记为 L1)及用户的电子书打开记录(记为 L2)。如果电子书监控开关是打开的，根据主要的电子书类型(如 PDF 等)跟踪这些类型的文件的创建、打开和关闭行为，并据此更新 L1 和 L2。对于集合 NP 或集合 D 中的电子书，可不进行监控。

30 530，确定第一类电子书信息的集合。

如果用户指定了集合 D 或者终端中尚且没有足够的电子书打开记录，则认证装置可以把 D 中的元素放入集合 L 中；否则认证装置可获取 L2 和 L1，依据 L2 结合权重配置计算各个电子书的阅读频率，取出频度最高的一组电子书放入集合 L。

5 此时构建的集合 L 为第一类电子书信息的集合。

540，确定参与认证的第一类电子书信息及第二类电子书信息中的干扰项。

本发明实施例中，干扰项是用户最近没有阅读过的阅读的电子书。

认证装置从 L1 中选取一个子集 R，要求 R 中元素都没有在集合 L2 和 L
10 中出现，然后从集合 L 中取一个大小为 c 的子集 V，作为本次认证中要求用户识别出来的第一类电子书信息。如果 L 包含了系统所有的电子书的信息，则 R 为空，此时方案退化为要求用户从包含虚假信息的全部电子书中识别出终端中真实存在的电子书的信息。

另外，为了降低记忆的难度，还可以增加 V 中元素的个数，也就是说，
15 V 中元素的个数可以多于 c 个。

550，确定第二类电子书信息中的混淆项。

本发明实施例中，混淆项是指系统随机生成的阅读的电子书，或者说终端中不存在的电子书。

认证装置生成一组虚假的电子书，个数为 f，记为集合 F。虚假阅读的
20 电子书可以按照系统中初始配置好的电子书库筛选而生；也可以通过连接远端网络服务检索获取。集合 F 中的元素不能在集合 L 或 D 中出现。

当然，也可不生成混淆项，此时 f 为 0，集合 F 为空集。

560，生成认证挑战集合。

认证装置将集合 V、R 和 F 中的元素打乱混合，形成认证挑战集合 A，
25 即 $A = V + R + F$ （其中符号 “+” 代表集合加）。

570，呈现认证挑战集合，确认认证结果。

认证装置将认证挑战集合 A 呈现给用户，以供用户进行识别。

根据用户的认证识别结果，认证装置可确定认证的结果。如果用户能够从中选择出 c 个 V 中的元素，则认证成功；否则认证失败。

30 本发明实施例中，在计算第一类电子书信息时，可以按照阅读行为产生时间到当前的时间长度进行赋权计算，用户也可以直接指定一组固定的电子

书作为第一类电子书信息，此时相当于对这组固定的实体都赋予了最大的权。通过在构建最终显示在屏幕上的集合 A 的过程中引入虚假认证信息集合 F，提高选择空间的大小，起到混淆的作用，以提高对用户的区分度，另外还可以保护集合 R 和 V 中的信息。本方法引入集合 R 的目的是进一步提高
5 选择的难度，避免一个知道终端中存在的电子书信息的攻击者直接猜测出第一类电子书信息。

如图 5 所示，本发明实施例的方法可支持多种运行模式。当开机首次进行运行或者认证参数配置发生变化时，需要执行初始认证模式。初始认证模式需要执行前述步骤 510 至步骤 570。如图 5 的箭头 572 指向所示，在认证
10 结束后，如果认证参数配置发生变化，初始认证模式直接跳转到步骤 510，执行步骤 510 至步骤 570。当用户发生新的阅读的电子书行为之后，此时用户的第一类电子书信息可能已经发生变化，认证装置需要执行阅读认证模式。理论情况下，认证装置可在步骤 570 之前，步骤 530 之后的任一个步骤执行阅读认证模式，但是，实际情况下，在认证过程中通常不会产生认证以外的交互行为，只有在认证结束后才可能产生别的交互行为。如图 5 的箭头
15 573 指向所示，此时，阅读认证模式需要跳转到步骤 530，执行步骤 530 到步骤 570。重选认证主要在用户希望提供最强的抗偷窥能力，或当用户认证错误次数太多时使用，要求在集合 L 不变的前提下每次重新计算的子集 V 都不同，最多可以重选 $C_{|L|}^{|\mathcal{V}|}$ (组合计算) 次。与阅读认证模式类似，重选认证模式需要在上一次认证完毕后执行。如图 5 的箭头 574 指向所示此时，重
20 选认证模式需要跳转到步骤 540，重选认证模式需要执行步骤 540 到步骤 570，不变认证模式中集合 A 完全不变，基于同样的秘密和干扰信息对用户进行认证。如图 5 的箭头 571 指向所示，此时不变认证模式只需要重新执行步骤 570。
25

在不变认证模式下，如果当前用户认证错误，下次认证仍然基于同样的干扰和秘密进行。随着通过逐步试错，排除的电子书信息组合逐渐增多，攻击者猜中可能性增大，但是下降速度非常缓慢。例如假设集合 A 中包含 24 个元素，认证时要求识别出 3 个第一类电子书信息 (集合 V 大小为 3)，则攻击者一开始猜中的概率是 $1/2024$ (3 个阅读的电子书的组合数为 $24*23*22/6=2024$)，攻击者尝试 m 次之后，其猜中的概率变为 $1/2014-m$ ，由此可以看出该方案在常见的参数尺寸下抵抗数千次的猜测攻击。通过在用
30

户连续认证错误的情况，延时一段时间再进行认证（例如 30 秒），该方案可以长时间抵抗猜测攻击。为了进一步提高抗猜测能力，在连续认证错误一定次数之后，系统执行一次重选认证，可以重新计算挑战集合 A，然后重新进入不变认证模式。

现有各种的认证方案，如口令，由于秘密是固定的，所以一旦认证时被偷窥，攻击者就能够掌握所有认证秘密，完全突破认证机制。本方案的认证秘密是基于第一类电子书信息这一不断动态变化的信息的。假设攻击者偷窥到了用户上次认证的秘密（当时的一组第一类电子书信息），并且他有条件能够拿到用户的终端，则他可以基于以前获得的秘密尝试认证。在很多情况下，终端的真实用户已经发生过几次新的阅读行为，此时第一类电子书信息已经发生变化，则上次的认证秘密失效，本方案具有完全的抗偷窥能力。在极少的情况下即使用户没有发生过任何新的阅读行为，如果用户对于抗偷窥特别关心，可以设置系统每次都执行重选认证，使得每次都基于不同的秘密认证用户，结合认证错误时延，可以提供较好的抗偷窥能力。例如用户有 8 个符合条件的第一类电子书信息 ($|L|=8$)，如果每次要求选中 3 个第一类电子书信息 ($|v|=3$)，则在执行 56 次重选认证之前，每次认证的秘密都不相同。

图 6 是本发明实施例以使用的应用（Application，APP）信息进行用户认证的流程示意图。本发明实施例中，认证信息为使用的 APP 的特定属性信息，例如 APP 的名称，APP 的开发公司，APP 的应用图标，或者 APP 的名称和图标的组合，等等。本发明实施例通过让用户回忆和识别他/她最近的频繁使用的 APP 实现身份验证。为方便描述，下文提到的 APP 信息即指 APP 的特定属性信息。

如图 6 所示，本发明实施例初始认证过程的详细步骤具体如下：

610，认证参数配置。

25 用户可对认证装置的工作方式进行配置，配置的参数可保存在认证装置的配置数据库中。

用户可进行以下配置：

(1) 排除 APP 信息（可记为 NP），此部分指定 APP 信息将不参与认证信息的生成过程，从而允许用户可以直接排除一些众所周知的 APP 信息或者用户异常敏感的 APP 信息。换句话说，集合 NP 的元素不出现在第一类 APP 信息中。当然，为了避免混淆，集合 NP 的元素也不会出现在第二类

APP 信息中。

(2) 第一类 APP 信息选择方法参数，可包括有效的使用的 APP 的时间要求（记为 T，例如 3 天、5 天、10 小时等），使用的 APP 发生频度要求（记为 X，表示预定次数，例如 5 次，或表示预定名次，例如前 3 名，或表示预定比例，例如 3% 等）。基于 T 和 X 确定的第一类 APP 信息可记为 L。当然，用户也可不进行配置，认证装置可对第一类 APP 信息选择方法参数设置一个默认设置。另外，用户也可指定一个或多个 APP 信息作为固定的第一类 APP 信息，而不是通过上述 T 和 X 临时计算获得。用户指定的第一类 APP 信息可记为 D。

(3) 第二类 APP 信息参数，可包括构造认证信息时混淆项数目（记为 f）和/或构造认证信息时的干扰项的数目（记为 i）。其中，混淆项是指系统随机生成的虚假 APP 信息，或者说终端中不存在的 APP 信息，干扰项是指用户最近没有使用过的 APP 的信息。（4）认证选择参数，可包括每次认证必须同时正确选择的第一类 APP 信息的个数（记为 c，例如，必须要同时正确选择 3 个才算通过认证）。认证装置还可引入一个安全强度调整功能，通过调整上述 f、i 和 c 的值来调整身份认证的安全强度，显然这三个数值越大，安全强度越高。具体地，认证装置可设定不同的难度级别，每个级别对应不同的值，其实现可通过安全强度拖动条或难度选择框等实现；或者，认证装置可提供一个数值调整功能，分别调整上述三个值。

配置完毕后，认证装置在启动认证时会自动加载对应的配置参数。

620，读取终端的 APP 的安装使用行为记录。

认证装置可包括 APP 使用跟踪模块，用于读取 APP 安装和使用行为记录。认证装置通过 APP 使用跟踪模块，读取 APP 安装和使用行为记录（记为 H）。如果 APP 追踪开关是打开的，开始跟踪系统中的 APP 安装和使用行为，并更新 H。对于集合 NP 或集合 D 中的 APP，其安装和打开行为可不予以记录。

630，获取第一类 APP 信息的集合。

如果用户指定了使用集合 D 或用户终端中尚且没有足够的 APP 使用记录，则认证信息计算模块直接将 D 中元素加入到 L 中；否则获取集合 H，结合权重参数计算各个 APP 的使用频度并且排序，取频度满足要求的一组 APP 放入集合 L。

此时构建的集合 L 为第一类 APP 信息的集合。

640，获取参与认证的第一类 APP 信息及第二类 APP 信息中的干扰项。

本发明实施例中，干扰项是用户最近没有使用过的 APP 的信息。

认证装置查询并获取一组已经安装的 APP 放入集合 R 中，要求 R 中的

5 APP 用户最近没有使用过且不在 L 中出现，然后从集合 L 中取一个大小为 c 的子集 V，作为本次认证中要求用户的识别出来的第一类 APP 信息。如果 L 包含了系统通讯录中所有的联系人信息，则 R 为空，此时方案退化为要求用户从混入混淆项的 APP 集合中识别出终端上真实存在的 APP 信息。

另外，为了降低记忆的难度，还可以增加 V 中元素的个数，也就是说，

10 V 中元素的个数可以多于 c 个。

650，确定第二类 APP 信息中的混淆项。

本发明实施例中，混淆项是指系统随机生成的 APP 信息，或者说终端中不存在的 APP 信息。

认证装置生成一组虚假 APP 信息，个数为 f，记为集合 F。虚假 APP 信息可以按照系统中初始配置好虚假 APP 数据库获得；也可以通过连接远端网络服务获取。集合 F 中的元素不能在集合 L 或 D 中出现。

当然，也可不生成混淆项，此时 f 为 0，集合 F 为空集。

660，生成认证挑战集合。

认证装置将集合 V、R 和 F 中的元素打乱混合，形成认证挑战集合 A，

20 即 $A = V + R + F$ （其中符号“+”代表集合加）。

670，呈现认证挑战集合，确认认证结果。

认证装置将认证挑战集合 A 呈现给用户，以供用户进行识别。

根据用户的认证识别结果，认证装置可确定认证的结果。如果用户能够从中选择出 c 个 V 中的元素，则认证成功；否则认证失败。

25 本发明实施例中，在计算第一类 APP 信息时，可以按照使用行为产生时间到当前的时间长度进行赋权计算，用户也可以直接指定一组固定的 APP 信息作为第一类 APP 信息，此时相当于对这组固定的实体都赋予了最大的权。通过在构建最终显示在屏幕上的集合 A 的过程中引入虚假认证信息集合 F，提高选择空间的大小，起到混淆的作用，以提高对用户的区分度，另外

30 还可以保护集合 R 和 V 中的信息。本方法引入集合 R 的目的是进一步提高选择的难度，避免一个知道终端中存在的使用的 APP 的攻击者直接猜测出

第一类 APP 信息。

如图 6 所示，本发明实施例的方法可支持多种运行模式。当开机首次进行运行或者认证参数配置发生变化时，需要执行初始认证模式。初始认证模式需要执行前述步骤 610 至步骤 670。如图 6 的箭头 672 指向所示，在认证 5 结束后，如果认证参数配置发生变化，初始认证模式直接跳转到步骤 610，执行步骤 610 至步骤 670。当用户发生新的使用的 APP 行为之后，此时用户的第一类 APP 信息可能已经发生变化，认证装置需要执行使用认证模式。理论情况下，认证装置可在步骤 670 之前，步骤 630 之后的任一个步骤执行 10 使用认证模式，但是，实际情况下，在认证过程中通常不会产生认证以外的交互行为，只有在认证结束后才可能产生别的交互行为。如图 6 的箭头 673 指向所示，此时，使用认证模式需要跳转到步骤 630，执行步骤 630 到步骤 670。重选认证主要在用户希望提供最强的抗偷窥能力，或当用户认证错误次数太多时使用，要求在集合 L 不变的前提下每次重新计算的子集 V 都不同，最多可以重选 $C_{|L|}^{|V|}$ (组合计算) 次。与使用认证模式类似，重选认证模 15 式需要在上一次认证完毕后执行。如图 6 的箭头 674 指向所示此时，重选认证模式需要跳转到步骤 640，重选认证模式需要执行步骤 640 到步骤 670，不变认证模式中集合 A 完全不变，基于同样的秘密和干扰信息对用户进行认 20 证。如图 6 的箭头 671 指向所示，此时不变认证模式只需要重新执行步骤 670。

在不变认证模式下，如果当前用户认证错误，下次认证仍然基于同样的干扰和秘密进行。随着通过逐步试错，排除的使用的 APP 组合逐渐增多，攻击者猜中可能性增大，但是下降速度非常缓慢。例如假设集合 A 中包含 24 个元素，认证时要求识别出 3 个第一类 APP 信息 (集合 V 大小为 3)，则攻击者一开始猜中的概率是 $1/2024$ (3 个使用的 APP 的组合数为 $24*23*22/6=2024$)，攻击者尝试 m 次之后，其猜中的概率变为 $1/2014-m$ ， 25 由此可以看出该方案在常见的参数尺寸下抵抗数千次的猜测攻击。通过在用户连续认证错误的情况下，延时一段时间再进行认证 (例如 30 秒)，该方案可以长时间抵抗猜测攻击。为了进一步提高抗猜测能力，在连续认证错误一定次数之后，系统执行一次重选认证，可以重新计算挑战集合 A，然后重新进入不变认证模式。

30 现有各种的认证方案，如口令，由于秘密是固定的，所以一旦认证时被偷窥，攻击者就能够掌握所有认证秘密，完全突破认证机制。本方案的认证

秘密是基于第一类 APP 信息这一不断动态变化的信息的。假设攻击者偷窥到了用户上次认证的秘密（当时的一组第一类 APP 信息），并且他有条件能够拿到用户的终端，则他可以基于以前获得的秘密尝试认证。在很多情况下，终端的真实用户已经发生过几次新的使用行为，此时第一类 APP 信息已经 5 发生变化，则上次的认证秘密失效，本方案具有完全的抗偷窥能力。在极少的情况下即使用户没有发生过任何新的使用行为，如果用户对于抗偷窥特别关心，可以设置系统每次都执行重选认证，使得每次都基于不同的秘密认证用户，结合认证错误时延，可以提供较好的抗偷窥能力。例如用户有 8 个符合 10 条件的第一类 APP 信息 ($|L|=8$)，如果每次要求选中 3 个第一类 APP 信息 ($|v|=3$)，则在执行 56 次重选认证之前，每次认证的秘密都不相同。

上述几个实施例只是介绍了几种可以用作身份认证的交互对象的信息，例如联系人信息、使用的 APP 信息、音乐作品的标识或演奏者信息、访问网站信息和阅读电子书信息。当然，本发明实施例的方法还可以使用多种认证信息，例如，视频文件的导演、名称、终端所到过的地理区域信息（通过 15 终端上的终端用户在移动网络的位置记录获得）或者终端内浏览的图片信息，等等，具体实现的方法可以参考上述实施例。

图 7 是本发明实施例认证装置 700 的结构示意图。认证装置 700 可包括确认单元 701、认证呈现单元 702、接收单元 703 和认证单元 704。

确认单元 701 用于确定认证装置 700 所在的终端的第一类认证信息和第 20 二类认证信息。

其中，该第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类认证信息用于干扰该终端的用户选择该第一类认证信息。

应理解，特定交互行为，是指认证过程中用于判定发生频度的交互行为。特定交互行为所对应的交互对象，是指采集第一类认证信息的来源，该交互对象的特定属性信息可用于构成第一类认证信息。

应理解，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，可例如唯一标识、名称、图片，或者名称+图片，等等。

应理解，不同交互对象的特定属性信息可能相同。例如，同一个专辑的音频文件中，其专辑名称相同。又例如，几本不同电子书的作者，可能为同

一个作者，等等。在确认第一类认证信息时，是以特定交互行为所对应的交互对象的特定属性信息的发生频率来确定的。

应理解，该第二类认证信息可包括以下至少一种：该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围
5 以外的特定属性信息；不属于该终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

可选地，该终端的特定交互行为是认证过程中指定的交互行为。该终端的特定交互行为可以有多种表现形式，相应的，该第一类认证信息和该第二类认证信息也可以有多种表现形式。例如，该终端的特定交互行为可包括该
10 终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为联系人的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性信息；或者，该终端的特定交互行为可包括该终端访问网站的行为，该第一
15 类认证信息和该第二类认证信息为网站的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，该终端的特定交互行为可包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，该终端的特定交互行为可包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。本发明实施例的一种具体实现方式，当第一类认证信息为联系人的特定属性信息时，该联系人信息具体可以是联系人的照片、联系人的姓名、联系人的联系电话，或者联系人的姓名+图片等等。本发明实施例的另一种具体实现方式，当第一类认证信息为音频文件信息时，该音频文件信息可以是音频文件的名称、音频文件的专辑名称或者是音频文件的演奏者，等等。
20
25

可选地，该终端可以有多种具体实现形式，例如，智能手机、平板电脑、个人计算机、服务器或工作站。当然，该终端还可以是其它具备认证功能的设备，本发明实施例在此不作限制。
30

应理解，该第一类认证信息包括该终端的特定交互行为所对应的交互对

象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，其中发生频度为预定范围，该范围可以是一个绝对频度范围，也可以是一个相对频度范围，例如该预定范围为该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者该终端
5 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。例如，该第一类认证信息可以是 3 天内通话次数在 5 次以上的联系人的姓名，或者是 2 天内电子书阅读次数占两天内总阅读 10% 以上的电子书名称，或者是 5 天内播放排名前 3 位的音乐专辑，或者是 12 小时内访问网站频率在前 5% 的网站，等等。
10

应理解，该预定时间、预定范围都是可配置的。例如，可将该预定时间配置为 12 小时，1 天，2 天，3 天乃至 1 月，等等，本发明实施例对此不作限制。又例如，可将该预定范围配置为发生频度在 1 次以上，5 次以上，或者
15 是所有发生频度的前 5 名，前 5%，等等。

可选地，该第一类认证信息还包括该终端的用户在该终端中所指定的交互对象的特定属性信息，以便减少该终端的用户对该第一类认证信息的记忆代价。

20 认证呈现单元 702，用于向该终端的用户呈现第一认证挑战集合。

其中，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息。

接收单元 703，用于接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果。

25 认证单元 704，用于根据该识别结果中该第一类认证信息的识别正确率确定认证结果。

本发明实施例中，认证装置 700 通过所在终端中预定时间内预定发生频率的交互对象的特定属性信息动态地生成认证信息以对用户进行认证，由于最近最频繁使用的特定交互对象的信息属于用户记忆期内的信息，可以降低
30 用户记忆的代价，同时每次出现的认证信息都不固定，又可以避免因为不慎被偷窥而导致认证信息被窃取，因而认证装置 700 在减少用户对认证信息的

记忆代价的同时，还具备一定的抗偷窥能力。

另外，由于认证装置 700 可以基于访问频率动态地生成认证信息以对用户进行认证，还可以提高用户的使用体验。

可选地，在接收单元 703 接收该终端的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果之前，如果该终端的特定交互行为所对应的交互对象发生变化，或者该终端产生新的该特定交互行为，则确定单元 701 还用于重新确定该终端的第一类认证信息和第二类认证信息，以便认证呈现单元 702 向该终端的用户呈现第二认证挑战集合，其中该第二认证挑战集合基于确定单元 701 重新确定后的第一类认证信息和第二类认证信息生成。在具体的应用中，该终端的特定交互行为所对应的交互对象发生变化可包括：增加该终端的特定交互行为所对应的交互对象，或者删除该终端的特定交互行为所对应的交互对象，或者修改该终端的特定交互行为所对应的交互对象，等等。

可选地，认证装置 700 还可包括第一配置单元 705。第一配置单元 705 用于配置该预定时间、该预定范围以及对该终端的用户进行认证所需要识别的第一类认证信息的条数 N。此时，认证单元 704 具体用于：如果该识别结果中该终端的用户识别的该第一类认证信息的条数不小于 N 条，则确定对该终端的用户的认证通过，或者，如果该识别结果中该终端的用户识别的该第一类认证信息的条数小于 N 条，则确定对该终端的用户的认证不通过。

具体地，第一配置单元 705 可用于通过配置该预定时间、该预定范围以及该对该终端的用户进行认证所需要识别的第一类认证信息的条数调整对该终端的用户的认证的安全强度。其中，如果该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对该终端的用户的认证的安全强度越大；如果对该终端的用户进行认证所需要识别的第一类认证信息的条数越大，则通过对该终端的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对该终端的用户的认证的安全强度越大。

可选地，认证装置 700 还可包括第二配置单元 706。第二配置单元 706 用于配置该终端的排除认证信息集合，其中该排除认证信息集合中的认证信息不允许作为该第一类认证信息。在用于确定该终端的至少一个第一类认证信息的过程中，确定单元 701 具体用于确定该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围且不属于该

排除认证集合的特定属性信息为该第一类认证信息。

可选地，认证装置 700 还可包括生成单元 707。生成单元 707 用于根据该终端的该第一类认证信息和该第二类认证信息生成该认证集合，以便向该终端的用户呈现该认证集合。

5 具体的，在实际的应用中，认证装置的各个组成单元中，可以是几个单元合成一个实现模块，也可以是一个单元由几个实现模块一起实现。例如，确认单元 701 可包括监控跟踪模块、交互对象计算模块和虚假交互对象生成模块。其中，监控跟踪模块用于监控与交互对象之间的交互行为，交互对象计算模块用于计算出第一类交互对象，以及第二类交互对象中的干扰项，虚
10 假交互对象生成模块用于生成第二类交互对象中的混淆项。认证呈现单元 702、接收单元 703 和认证单元 704 可以由一个认证交互模块实现，或者认证呈现单元 702 和接收单元 703 可以由一个输入输出模块实现，比如触摸屏。第一配置单元 705 和第二配置单元 706，可由一个配置模块实现。当然，认证装置还可能存在其它的具体实现方式，本发明实施例在此不作限制。

15 另外，认证装置 700 还可执行图 1 的方法，并实现认证装置在图 1 至图 6 所示实施例的功能，具体可参考图 1 至图 6 所示的实施例，本发明在此不再赘述。

图 8 是本发明实施例终端 800 的结构示意图。终端 800 可包括通信接口 801，处理器 802 和存储器 803。

20 通信接口 801、处理器 802 和存储器 803 通过总线 803 系统相互连接。总线 804 可以是 ISA 总线、PCI 总线或 EISA 总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

25 存储器 803，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器 803 可以包括只读存储器和随机存取存储器，并向处理器 802 提供指令和数据。存储器 803 可能包含高速 RAM 存储器，也可能还包括非易失性存储器 (non-volatile memory)，例如至少一个磁盘存储器。

30 处理器 802，用于调用存储器 803 所存放的程序，并具体用于执行以下操作：

确定终端 800 的至少一个第一类认证信息和至少一个第二类认证信息，

并通过通信接口 801 在显示设备 805 中向终端 800 的用户呈现第一认证挑战集合，其中，该第一类认证信息包括终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，该第二类认证信息用于干扰终端 800 的用户选择该第一类认证信息，该第一认证挑战集合包括至少一个该第一类认证信息和至少一个该第二类认证信息；

通过通信接口 801 从输入设备 806 中接收终端 800 的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果，并根据该识别结果中该第一类认证信息的识别正确率确定认证结果。

应理解，特定交互行为，是指认证过程中用于判定发生频度的交互行为。特定交互行为所对应的交互对象，是指采集第一类认证信息的来源，该交互对象的特定属性信息可用于构成第一类认证信息。

通信接口 801，用于实现处理器 802 与显示设备 805、输入设备 806 之间的数据通信。

显示设备 805，用于向终端 800 的用户呈现该第一认证挑战集合。

所述输入设备，用于输入终端 800 的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果。

应理解，该特定属性信息为该交互对象的一种属性信息或多种属性信息的组合，可例如唯一标识、名称、图片，或者名称+图片，等等。

应理解，不同交互对象的特定属性信息可能相同。例如，同一个专辑的音频文件中，其专辑名称相同。又例如，几本不同电子书的作者，可能为同一个作者，等等。在确认第一类认证信息时，是以特定交互行为所对应的交互对象的特定属性信息的发生频率来确定的。

应理解，该第二类认证信息可包括以下至少一种：终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；不属于终端 800 的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

可选地，终端的特定交互行为是终端在认证过程中指定的交互行为。终端的特定交互行为可以有多种表现形式，相应的，该第一类认证信息和该第二类认证信息也可以有多种表现形式。例如，终端的特定交互行为可包括该终端访问该终端的联系人的行为，该第一类认证信息和该第二类认证信息为

联系人的特定属性信息；或者，终端的特定交互行为可包括该终端访问该终端的音视频文件的行为，该第一类认证信息和该第二类认证信息为音视频文件的特定属性信息；或者，终端的特定交互行为可包括该终端访问该终端的应用的行为，该第一类认证信息和该第二类认证信息为应用的特定属性信息；或者，终端的特定交互行为可包括该终端访问网站的行为，该第一类认证信息和该第二类认证信息为网站的特定属性信息；或者，终端的特定交互行为可包括该终端访问该终端的图片的行为，该第一类认证信息和该第二类认证信息为图片的特定属性信息；或者，终端的特定交互行为可包括该终端访问该终端的电子书的行为，该第一类认证信息和该第二类认证信息为电子书的特定属性信息；或者，终端的特定交互行为可包括该终端与该终端外设备通信的行为，该第一类认证信息和该第二类认证信息为该终端与该终端外设备通信时所处的地理区域的信息。本发明实施例的一种具体实现方式，当第一类认证信息为联系人的特定属性信息时，该联系人信息具体可以是联系人的照片、联系人的姓名、联系人的联系电话，或者联系人的姓名+图片等等。本发明实施例的另一种具体实现方式，当第一类认证信息为音频文件信息时，该音频文件信息可以是音频文件的名称、音频文件的专辑名称或者是音频文件的演奏者，等等。

可选地，终端 800 可以有多种具体实现形式，例如，智能手机、平板电脑、个人计算机、服务器或工作站。当然，终端 800 还可以是其它具备认证功能的设备，本发明实施例在此不作限制。

可选地，显示设备 805 和输入设备 806 在终端 800 中可以合成一个设备，例如，触摸屏等。

或者，可选地，显示设备 805 和输入设备 806 在终端 800 为不同的设备，显示设备 805 为显示器、显示屏等显示设备，输入设备 806 为鼠标，键盘等输入设备。

应理解，该第一类认证信息包括终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，其中发生频度为预定范围，该范围可以是一个绝对频度范围，也可以是一个相对频度范围，例如该预定范围为终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发

生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。例如，该第一类认证
5 信息可以是 3 天内通话次数在 5 次以上的联系人的姓名，或者是 2 天内电子书阅读次数占两天内总阅读 10% 以上的电子书名称，或者是 5 天内播放排名前 3 位的音乐专辑，或者是 12 小时内访问网站频率在前 5% 的网站，等等。

应理解，该预定时间、预定范围都是可配置的。例如，可将该预定时间配置为 12 小时，1 天，2 天，3 天乃至 1 月，等等，本发明实施例对此不作
10 限制。又例如，可将该预定范围配置为发生频度在 1 次以上，5 次以上，或者是所有发生频度的前 5 名，前 5%，等等。

可选地，该第一类认证信息还包括终端 800 的用户在终端 800 中所指定的交互对象的特定属性信息，以便减少终端 800 的用户对该第一类认证信息的记忆代价。

15 上述如本发明图 1 至图 6 任一实施例揭示的认证装置执行的方法可以应用于处理器 802 中，或者由处理器 802 实现。处理器 802 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器 802 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 802 可以是通用处理器，包括中央处理器（Central Processing Unit，简称
20 CPU）、网络处理器（Network Processor，简称 NP）等；还可以是数字信号处理器（DSP）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 803，处理器 802 读取存储器 803 中的信息，结合其硬件完成上述方法的步骤。
25

30 本发明实施例中，终端 800 通过使用终端中预定时间内预定发生频率的交互对象的信息动态地生成认证信息以对用户进行认证，由于最近最频繁使

用的特定交互对象的信息属于用户记忆期内的信息，可以降低用户记忆的代价，同时每次出现的认证信息都不固定，又可以避免因为不慎被偷窥而导致认证信息被窃取，因而终端 800 在减少用户对认证信息的记忆代价的同时，还具备一定的抗偷窥能力。

5 另外，由于终端 800 可以基于访问频率动态地生成认证信息以对用户进行认证，还可以提高用户的使用体验。

可选地，在处理器 802 通过通信接口 801 从输入设备 806 中接收终端 800 的用户对该第一认证挑战集合中的该第一类认证信息和该第二类认证信息的识别结果之前，如果终端 800 的特定交互行为所对应的交互对象发生变化，
10 或者终端 800 产生新的该特定交互行为，则处理器 802 还用于重新确定终端 800 的第一类认证信息和第二类认证信息，以便通过通信接口 801 在显示设备 805 中向终端 800 的用户呈现第二认证挑战集合，其中该第二认证挑战集合基于处理器 802 重新确定后的第一类认证信息和第二类认证信息生成。在具体的应用中，终端 800 的特定交互行为所对应的交互对象发生变化可包括：
15 增加终端 800 的特定交互行为所对应的交互对象，或者删除终端 800 的特定交互行为所对应的交互对象，或者修改终端 800 的特定交互行为所对应的交互对象，等等。

可选地，处理器 802 还可用于配置该预定时间、该预定范围以及对终端 800 的用户进行认证所需要识别的第一类认证信息的条数 N。此时，在用于
20 根据该识别结果中该第一类认证信息的识别正确率确定认证结果的过程中，处理器 802 具体可用于：如果该识别结果中终端 800 的用户识别的该第一类认证信息的条数不小于 N 条，则确定对终端 800 的用户的认证通过，或者，如果该识别结果中终端 800 的用户识别的该第一类认证信息的条数小于 N 条，则确定对终端 800 的用户的认证不通过。

25 具体地，处理器 800 可通过配置该预定时间、该预定范围以及该对终端 800 的用户进行认证所需要识别的第一类认证信息的条数调整对终端 800 的用户的认证的安全强度。其中，如果该预定时间和该预定范围越大，则该第一类认证信息的集合越大，对终端 800 的用户的认证的安全强度越大；如果对终端 800 的用户进行认证所需要识别的第一类认证信息的条数 N 越大，则
30 通过对终端 800 的用户的认证时所需要的该识别结果中该第一类认证信息的识别正确率越大，对终端 800 的用户的认证的安全强度越大。

可选地，处理器 802 还可用于配置终端 800 的排除认证信息集合，其中该排除认证信息集合中的认证信息不允许作为该第一类认证信息。在用于确定终端 800 的第一类认证信息的过程中，处理器 802 具体用于确定终端 800 的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频率为预定范围且不属于该排除认证集合的特定属性信息为该第一类认证信息。

可选地，处理器 802 还可用于根据该终端 800 的该第一类交互对象的信息和该第二类交互对象的信息生成该认证集合。

另外，终端 800 还可执行图 1 的方法，并实现认证装置在图 1 至图 6 所示实施例的功能，具体可参考图 1 至图 6 所示的实施例，本发明在此不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

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

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元

中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器(ROM, Read-Only Memory)、
10 随机存取存储器 (RAM, Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。
15

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于
此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护
范围应所述以权利要求的保护范围为准。

权利要求

1、一种用户认证方法，其特征在于，包括：

5 确定终端的第一类认证信息和第二类认证信息，其中，所述第一类认证信息包括该终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，所述特定属性信息为所述交互对象的一种属性信息或多种属性信息的组合，所述第二类认证信息用于干扰所述终端的用户选择所述第一类认证信息；

10 向所述终端的用户呈现第一认证挑战集合，其中，所述第一认证挑战集合包括至少一个所述第一类认证信息和至少一个所述第二类认证信息；

接收所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果；

根据所述识别结果中所述第一类认证信息的识别正确率确定认证结果。

15 2、如权利要求 1 所述的方法，其特征在于，所述第二类认证信息包括以下至少一种：

所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；

不属于所述终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

20 3、如权利要求 1 或 2 所述的方法，其特征在于，所述第一类认证信息还包括所述终端的用户在所述终端中所指定的交互对象的特定属性信息，以便减少所述终端的用户对所述第一类认证信息的记忆代价。

25 4、如权利要求 1 至 3 任一项所述的方法，其特征在于，在所述接收所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果之前，还包括：

如果所述终端的特定交互行为所对应的交互对象发生变化，或者所述终端产生新的所述特定交互行为，则重新确定所述终端的第一类认证信息和第二类认证信息，并向所述终端的用户呈现第二认证挑战集合，其中所述第二认证挑战集合基于重新确定后的第一类认证信息和第二类认证信息生成。

30 5、如权利要求 4 所述的方法，其特征在于，所述终端的特定交互行为所对应的交互对象发生变化包括：增加所述终端的特定交互行为所对应的交

互对象，或者删除所述终端的特定交互行为所对应的交互对象，或者修改所述终端的特定交互行为所对应的交互对象。

6、如权利要求 1 至 5 任一项所述的方法，其特征在于，

所述终端的特定交互行为包括所述终端访问所述终端的联系人的行为，

5 所述第一类认证信息和所述第二类认证信息为联系人的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的音视频文件的行为，所述第一类认证信息和所述第二类认证信息为音视频文件的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的应用的行为，所

10 述第一类认证信息和所述第二类认证信息为应用的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问网站的行为，所述第一类认证信息和所述第二类认证信息为网站的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的图片的行为，所述第一类认证信息和所述第二类认证信息为图片的特定属性信息；或者

15 所述终端的特定交互行为包括所述终端访问所述终端的电子书的行为，所述第一类认证信息和所述第二类认证信息为电子书的特定属性信息；或者

所述终端的特定交互行为包括所述终端与所述终端外设备通信的行为，所述第一类认证信息和所述第二类认证信息为所述终端与所述终端外设备通信时所处的地理区域的信息。

7、如权利要求 1 至 6 任一项所述的方法，其特征在于，

在所述确定终端的第一类认证信息和第二类认证信息之前，还包括：

配置所述预定时间、所述预定范围以及对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N；

所述根据所述识别结果中所述第一类认证信息的识别正确率确定认证结果包括：

如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数不小于 N 条，则确定对所述终端的用户的认证通过；或者

如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数小于 N 条，则确定对所述终端的用户的认证不通过。

8、如权利要求 7 所述的方法，其特征在于，

所述预定时间和所述预定范围越大，则所述第一类认证信息的集合越

大，所述对所述终端的用户的认证的安全强度越大；

所述对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N 越大，则通过对所述终端的用户的认证时所需要的所述识别结果中所述第一类认证信息的识别正确率越大，所述对所述终端的用户的认证的安全强度
5 越大。

9、如权利要求 1 至 8 任一项所述的方法，其特征在于，

所述预定范围为所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在
10 总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。

10、如权利要求 1 至 9 任一项所述的方法，其特征在于，在所述确定终
15 端的第一类认证信息之前，还包括：配置所述终端的排除认证信息集合，其中所述排除认证信息集合中的认证信息不允许作为所述第一类认证信息；

所述确定所述终端的第一类认证信息包括：确定所述终端的特定交互行
为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围且不属
于所述排除认证集合的特定属性信息为所述第一类认证信息。

20 11、如权利要求 1 至 10 任一项所述的方法，其特征在于，在向所述终
端的用户呈现第一认证挑战集合之前，还包括：

根据所述终端的所述第一类认证信息和所述第二类认证信息生成所述
第一认证挑战集合，以便向所述终端的用户呈现所述认证挑战集合。

25 12、如权利要求 1 至 11 任一项所述的方法，其特征在于，所述终端包
括智能手机、平板电脑、个人计算机、服务器或工作站。

13、一种认证装置，其特征在于，包括：

确认单元，用于确定所述装置所在的终端的第一类认证信息和第二类认
证信息，其中，所述第一类认证信息包括该终端的特定交互行为所对应的交
互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信
息，所述特定属性信息为所述交互对象的一种属性信息或多种属性信息的组
合，所述第二类认证信息用于干扰所述终端的用户选择所述第一类认证信
30 信。

息；

认证呈现单元，用于向所述终端的用户呈现第一认证挑战集合，其中，所述第一认证挑战集合包括至少一个所述第一类认证信息和至少一个所述第二类认证信息；

5 接收单元，用于接收所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果；

认证单元，用于根据所述识别结果中所述第一类认证信息的识别正确率确定认证结果。

14、如权利要求 13 所述的装置，其特征在于，所述第二类认证信息包
10 括以下至少一种：

所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；

不属于所述终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

15 15、如权利要求 13 或 14 所述的装置，其特征在于，所述第一类认证信息还包括所述终端的用户在所述终端中所指定的交互对象的特定属性信息，以便减少所述终端的用户对所述第一类认证信息的记忆代价。

16、如权利要求 13 至 15 任一项所述的装置，其特征在于，

20 在所述接收单元接收所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果之前，如果所述终端的特定交互行为所对应的交互对象发生变化，或者所述终端产生新的所述特定交互行为，则

25 所述确认单元还用于重新确定所述终端的第一类认证信息和第二类认证信息，以便所述认证呈现单元向所述终端的用户呈现第二认证挑战集合，所述第二认证挑战集合基于所述确定单元重新确定后的第一类认证信息和第二类认证信息生成。

30 17、如权利要求 16 所述的装置，其特征在于，所述终端的特定交互行为所对应的交互对象发生变化包括：增加所述终端的特定交互行为所对应的交互对象，或者删除所述终端的特定交互行为所对应的交互对象，或者修改所述终端的特定交互行为所对应的交互对象。

18、如权利要求 13 至 17 任一项所述的装置，其特征在于，

所述终端的特定交互行为包括所述终端访问所述终端的联系人的行为，所述第一类认证信息和所述第二类认证信息为联系人的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的音视频文件的行为，所述第一类认证信息和所述第二类认证信息为音视频文件的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的应用的行为，所述第一类认证信息和所述第二类认证信息为应用的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问网站的行为，所述第一类认证信息和所述第二类认证信息为网站的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的图片的行为，所述第一类认证信息和所述第二类认证信息为图片的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的电子书的行为，所述第一类认证信息和所述第二类认证信息为电子书的特定属性信息；或者

所述终端的特定交互行为包括所述终端与所述终端外设备通信的行为，所述第一类认证信息和所述第二类认证信息为所述终端与所述终端外设备通信时所处的地理区域的信息。

19、如权利要求 13 至 18 任一项所述的装置，其特征在于，

所述装置还包括第一配置单元，所述第一配置单元用于：配置所述预定时间、所述预定范围以及对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N；

所述认证单元具体用于：如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数不小于 N 条，则确定对所述终端的用户的认证通过，或者，如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数小于 N 条，则确定对所述终端的用户的认证不通过。

20、如权利要求 19 所述的装置，其特征在于，

所述预定时间和所述预定范围越大，则所述第一类认证信息的集合越大，所述对所述终端的用户的认证的安全强度越大；

所述对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N 越大，则通过对所述终端的用户的认证时所需要的所述识别结果中所述第一类认证信息的识别正确率越大，所述对所述终端的用户的认证的安全强度越大。

21、如权利要求 13 至 20 任一项所述的装置，其特征在于，所述预定范围为所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。
5

22、如权利要求 13 至 21 任一项所述的装置，其特征在于，所述装置还包括第二配置单元，所述第二配置单元用于配置所述终端的排除认证信息集合，其中所述排除认证信息集合中的认证信息不允许作为所述第一类认证信息；
10

在用于确定所述终端的第一类认证信息的过程中，所述确定单元具体用于确定所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围且不属于所述排除认证集合的特定属性信息为所述第一类认证信息。
15

23、如权利要求 13 至 22 任一项所述的装置，其特征在于，所述装置还包括生成单元，所述生成单元用于：根据所述终端的所述第一类认证信息和所述第二类认证信息生成所述第一认证挑战集合，以便向所述终端的用户呈现所述第一认证挑战集合。
20

24、如权利要求 13 至 23 任一项所述的装置，其特征在于，所述终端包括智能手机、平板电脑、个人计算机、服务器或工作站。

25、一种终端，其特征在于，包括处理器、存储器、通信接口、显示设备和输入设备，所述处理器与所述存储器相连，且通过所述通信接口连接到所述显示设备和所述输入设备，所述存储器中存储一组程序代码，且所述处理器用于调用所述存储器中存储的程序代码，用于执行以下操作：
25

确定所述终端的第一类认证信息和第二类认证信息，并通过所述通信接口在所述显示设备上向所述终端的用户呈现第一认证挑战集合，其中，所述第一类认证信息包括所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围的特定属性信息，所述特定属性信息为所述交互对象的一种属性信息或多种属性信息的组合，所述第二类认
30

证信息用于干扰所述终端的用户选择所述第一类认证信息，所述第一认证挑战集合包括至少一个所述第一类认证信息和至少一个所述第二类认证信息；

通过所述通信接口从所述输入设备中接收所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果，

5 并根据所述识别结果中所述第一类认证信息的识别正确率确定认证结果；

所述显示设备，用于向所述终端的用户呈现所述第一认证挑战集合；

所述输入设备，用于输入所述终端的用户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信息的识别结果。

26、如权利要求 25 所述的终端，其特征在于，所述第二类认证信息包

10 括以下至少一种：

所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生频度为预定范围以外的特定属性信息；

不属于所述终端的特定交互行为所对应的交互对象的特定属性信息中的特定属性信息。

15 27、如权利要求 25 或 26 所述的终端，其特征在于，所述第一类认证信息还包括所述终端的用户在所述终端中所指定的交互对象的特定属性信息，以便减少所述终端的用户对所述第一类认证信息的记忆代价。

28、如权利要求 25 至 27 任一项所述的终端，其特征在于，

在所述处理器通过所述通信接口从所述输入设备中接收所述终端的用
20 户对所述第一认证挑战集合中的所述第一类认证信息和所述第二类认证信
息的识别结果之前，如果所述终端的特定交互行为所对应的交互对象发生变
化，或者所述终端产生新的所述特定交互行为，则

所述处理器还用于重新确定所述终端的第一类认证信息和第二类认证信
25 息，以便通过所述通信接口在所述显示设备中向所述终端的用户呈现第二
类认证挑战集合，所述第二类认证挑战集合基于所述确定单元重新确定后的第
一类认证信息和第二类认证信息生成。

29、如权利要求 28 所述的终端，其特征在于，所述终端的特定交互行
为所对应的交互对象发生变化包括：增加所述终端的特定交互行为所对应的
交互对象，或者删除所述终端的特定交互行为所对应的交互对象，或者修改
30 所述终端的特定交互行为所对应的交互对象。

30、如权利要求 25 至 29 任一项所述的终端，其特征在于，

所述终端的特定交互行为包括所述终端访问所述终端的联系人的行为，所述第一类认证信息和所述第二类认证信息为联系人的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的音视频文件的行为，所述第一类认证信息和所述第二类认证信息为音视频文件的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的应用的行为，所述第一类认证信息和所述第二类认证信息为应用的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问网站的行为，所述第一类认证信息和所述第二类认证信息为网站的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的图片的行为，所述第一类认证信息和所述第二类认证信息为图片的特定属性信息；或者

所述终端的特定交互行为包括所述终端访问所述终端的电子书的行为，所述第一类认证信息和所述第二类认证信息为电子书的特定属性信息；或者

所述终端的特定交互行为包括所述终端与所述终端外设备通信的行为，所述第一类认证信息和所述第二类认证信息为所述终端与所述终端外设备通信时所处的地理区域的信息。

31、如权利要求 25 至 30 任一项所述的终端，其特征在于，

所述处理器还用于配置所述预定时间、所述预定范围以及对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N；

在用于根据所述识别结果中所述第一类认证信息的识别正确率确定认证结果的过程中，所述处理器具体用于：如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数不小于 N 条，则确定对所述终端的用户的认证通过，或者，如果所述识别结果中所述终端的用户识别的所述第一类认证信息的条数小于 N 条，则确定对所述终端的用户的认证不通过。

32、如权利要求 31 所述的终端，其特征在于，

所述预定时间和所述预定范围越大，则所述第一类认证信息的集合越大，所述对所述终端的用户的认证的安全强度越大；

所述对所述终端的用户进行认证所需要识别的第一类认证信息的条数 N 越大，则通过对所述终端的用户的认证时所需要的所述识别结果中所述第一类认证信息的识别正确率越大，所述对所述终端的用户的认证的安全强度越大。

33、如权利要求 25 至 32 任一项所述的终端，其特征在于，所述预定范围为所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在预定次数以上的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数在总发生次数的预定比例以上的范围，或者终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定名次以内的范围，或者所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定时间内发生次数排名在预定比例以内的范围。
5

34、如权利要求 25 至 33 任一项所述的终端，其特征在于，所述处理器
10 还用于配置所述终端的排除认证信息集合，其中所述排除认证信息集合中的
认证信息不允许作为所述第一类认证信息；

在用于确定所述终端的第一类认证信息的过程中，所述处理器具体用于
确定所述终端的特定交互行为所对应的交互对象的特定属性信息中在预定
时间 15 内发生频度为预定范围且不属于所述排除认证集合的特定属性信息为
所述第一类认证信息。

35、如权利要求 25 至 34 任一项所述的终端，其特征在于，所述处理器
还用于根据所述终端的所述第一类认证信息和所述第二类认证信息生成所
述第一认证挑战集合，以便向所述终端的用户呈现所述第一认证挑战集合。
15

36、如权利要求 25 至 35 任一项所述的终端，其特征在于，所述终端包
括智能手机、平板电脑、个人计算机、服务器或工作站。
20

37、如权利要求 25 至 36 任一项所述的终端，其特征在于，

所述显示设备和所述输入设备为所述终端中同时具备显示和输入功能
的同一设备；或者

所述显示设备和所述输入设备为所述终端中不同的设备。
25

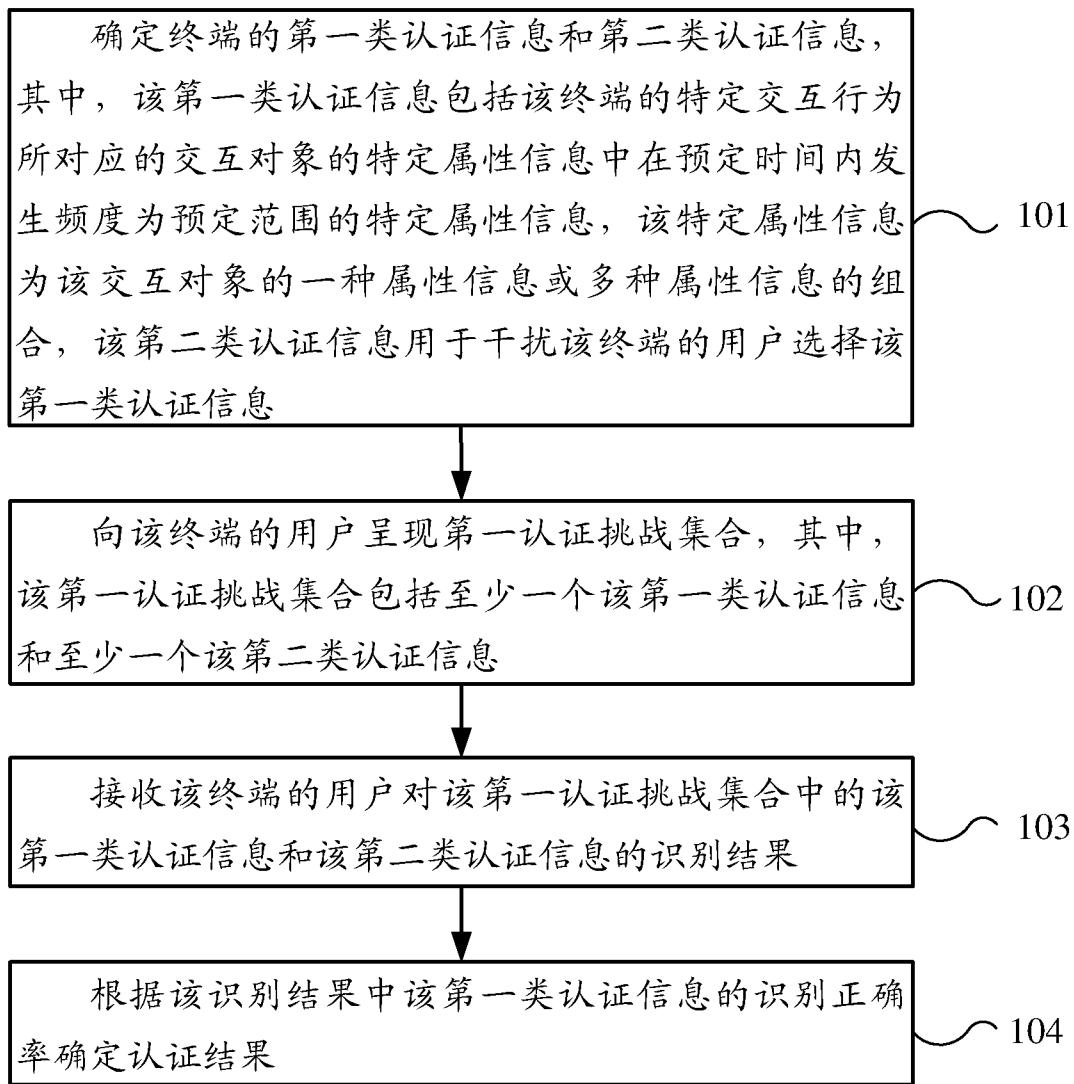


图1

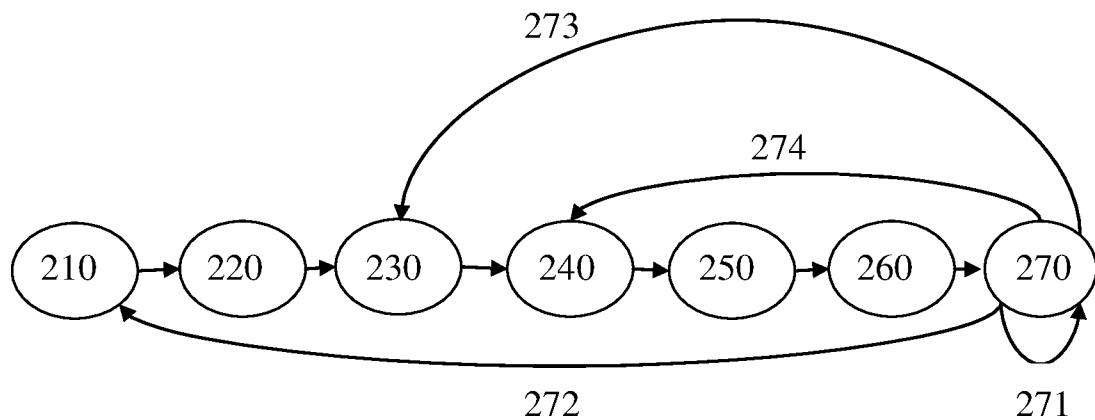


图2

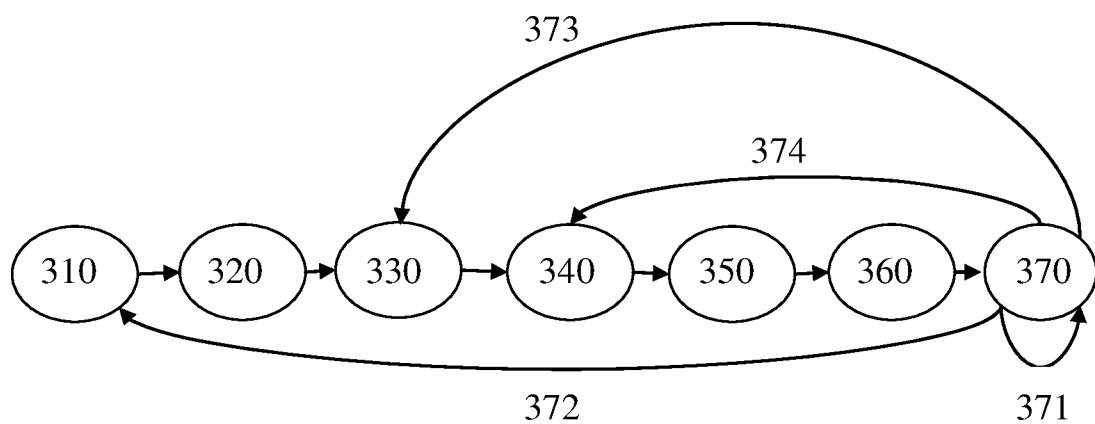


图3

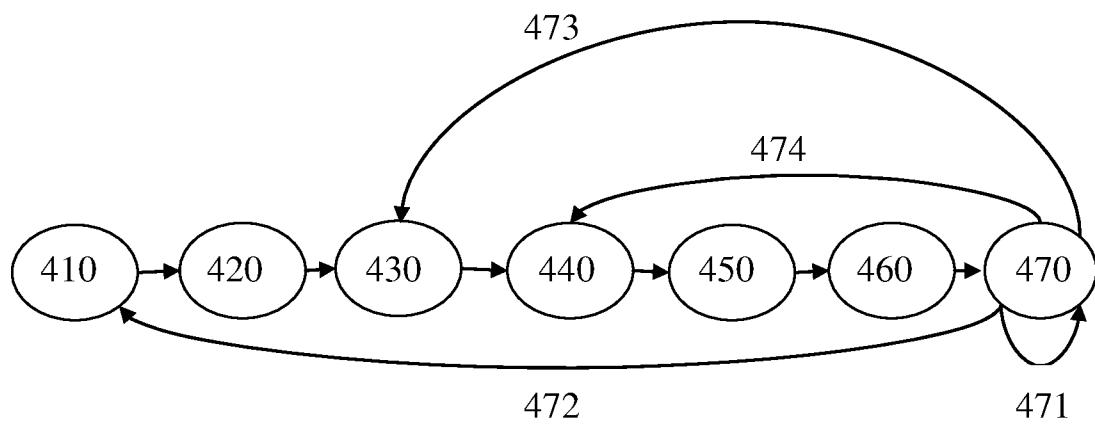


图4

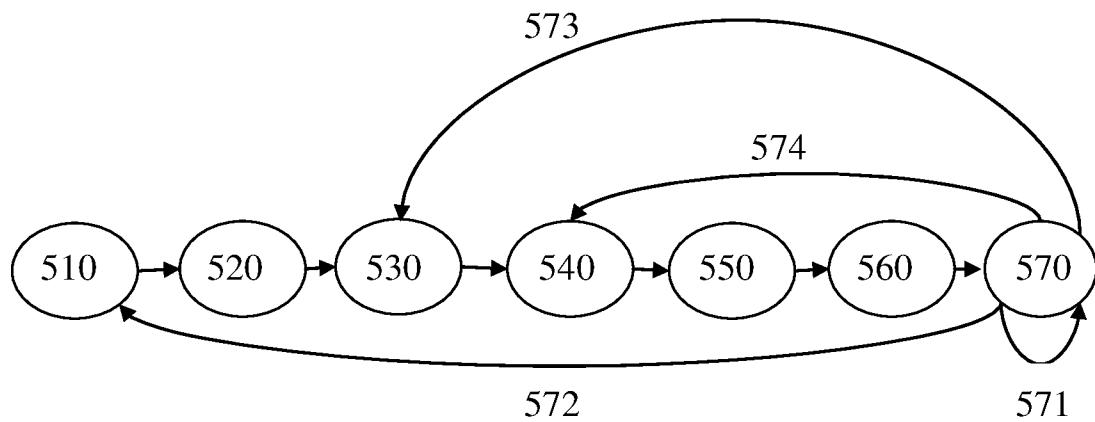


图5

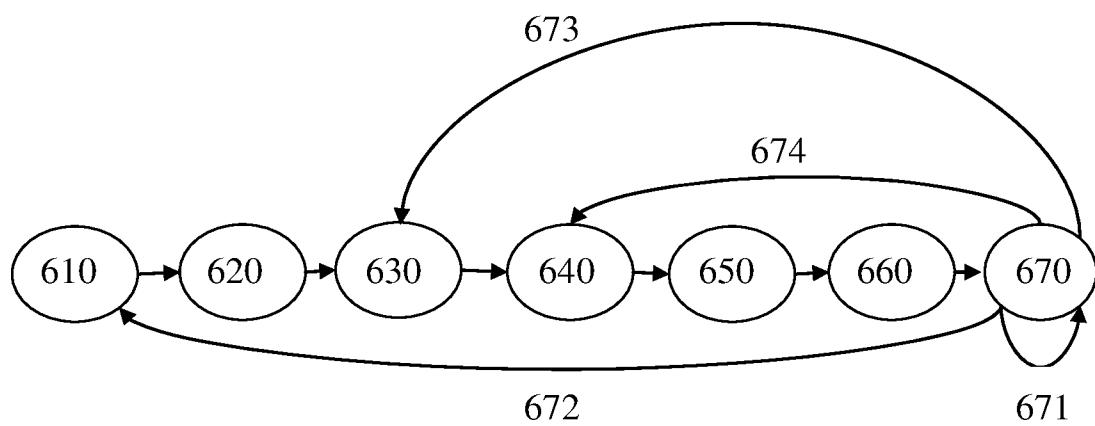


图6

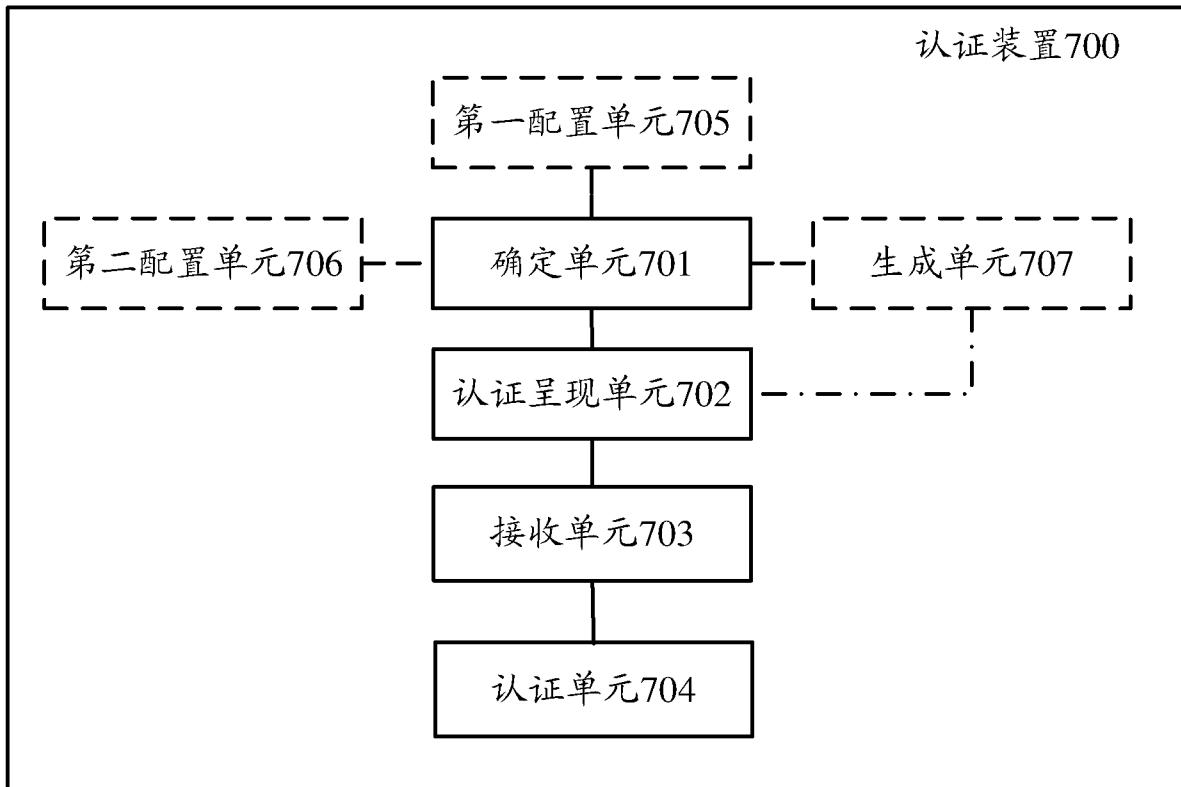


图7

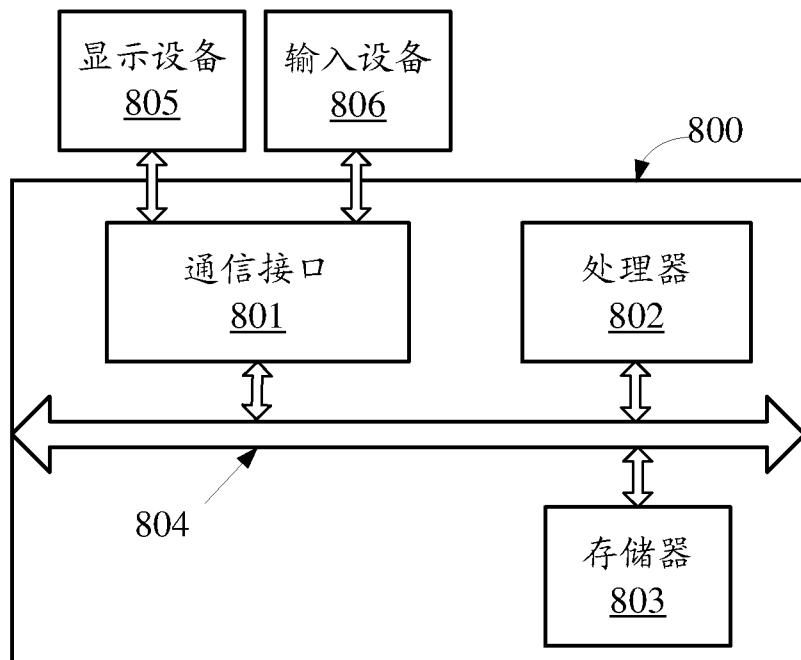


图8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/093910

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; CNABS; VEN; CNKI: recognise, authentication, legitimacy, confuse, disturb, number of times, dynamic, TENCENT, device, terminal, user, identity, examin+, check+, verif+, log+, question?, friend?, contact?, interfer+, frequency, often,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103455965 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 18 December 2013 (18.12.2013), the whole document	1-37
A	CN 101110667 A (HUAWEI TECHNOLOGIES CO., LTD.), 23 January 2008 (23.01.2008), the whole document	1-37
A	US 2013091559 A1 (SAP AG), 11 April 2013 (11.04.2013), the whole document	1-37

Further documents are listed in the continuation of Box C.

See patent family annex.

- * Special categories of cited documents:
- “A” document defining the general state of the art which is not considered to be of particular relevance
- “E” earlier application or patent but published on or after the international filing date
- “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- “O” document referring to an oral disclosure, use, exhibition or other means
- “P” document published prior to the international filing date but later than the priority date claimed

- “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- “&” document member of the same patent family

Date of the actual completion of the international search
07 March 2015 (07.03.2015)

Date of mailing of the international search report
27 March 2015 (27.03.2015)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
ZHU, Xiuling
Telephone No.: (86-10) 62412012

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2014/093910

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103455965 A	18 December 2013	None	
CN 101110667 A	23 January 2008	CN 101110667 B	23 May 2012
US 2013091559 A1	11 April 2013	US 8635684 B2	21 January 2014
		US 2014123263 A1	01 May 2014

国际检索报告

国际申请号

PCT/CN2014/093910

A. 主题的分类

H04L 9/32 (2006. 01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS; CNTXT; CNABS; VEN; CNKI: 设备, 终端, 用户, 身份, 识别, 验证, 校验, 认证, 登陆, 登录, 合法性, 问题, 提问, 好友, 联系人, 干扰, 混淆, 扰乱, 频率, 次数, 动态, 腾讯, device, terminal, user, identity, examin+, check+, verif+, log+, question?, friend?, contact?, interfer+, frequency, often, frequent

C. 相关文件

类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 103455965 A (北京小米科技有限责任公司) 2013年 12月 18日 (2013 - 12 - 18) 全文	1-37
A	CN 101110667 A (华为技术有限公司) 2008年 1月 23日 (2008 - 01 - 23) 全文	1-37
A	US 2013091559 A1 (SAP AG) 2013年 4月 11日 (2013 - 04 - 11) 全文	1-37

 其余文件在C栏的续页中列出。 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“&” 同族专利的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

国际检索实际完成的日期

2015年 3月 7日

国际检索报告邮寄日期

2015年 3月 27日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)

北京市海淀区蓟门桥西土城路6号

100088 中国

传真号 (86-10) 62019451

受权官员

朱秀玲

电话号码 (86-10) 62412012

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/093910

检索报告引用的专利文件		公布日 (年/月/日)		同族专利		公布日 (年/月/日)	
CN	103455965	A	2013年 12月 18日		无		
CN	101110667	A	2008年 1月 23日	CN	101110667	B	2012年 5月 23日
US	2013091559	A1	2013年 4月 11日	US	8635684	B2	2014年 1月 21日
				US	2014123263	A1	2014年 5月 1日

表 PCT/ISA/210 (同族专利附件) (2009年7月)