(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108574658 B
(45)授权公告日 2022.04.22

(21)申请号 201710132482.X
(22)申请日 2017.03.07
(65)同一申请的已公布的文献号
申请公布号 CN 108574658 A
(43)申请公布日 2018.09.25
(73)专利权人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层
(72)发明人 李冠耀 柳锋 唐松
(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强
(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 105306610 A,2016.02.03
CN 101557590 A,2009.10.14
CN 105024986 A,2015.11.04
CN 103248657 A,2013.08.14
CN 104954350 A,2015.09.30
CN 104980400 A,2015.10.14
US 2013205370 A1,2013.08.08

审查员 程杰

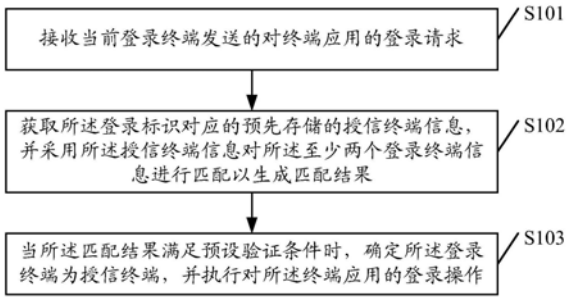
权利要求书3页 说明书15页 附图6页

(54)发明名称

一种应用登录方法及其设备

(57)摘要

本发明实施例公开一种,其中方法包括如下步骤:接收当前登录终端发送的对终端应用的登录请求,所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息;获取所述登录标识对应的预先存储的授信终端信息,并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果;当所述匹配结果满足预设验证条件时,确定所述登录终端为授信终端,并执行对所述终端应用的登录操作。采用本发明,可以保证在登录操作过程中的终端识别的准确性,进一步提升终端应用的登录效率。



CN 108574658 B

1.一种应用登录方法,其特征在于,包括:

接收当前登录终端发送的对终端应用的登录请求,所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息;

获取所述登录标识对应的预先存储的授信终端信息,并采用所述授信终端信息对按照信息被修改由难到易的排列顺序进行排列、加密处理后的所述至少两个登录终端信息进行匹配以生成匹配结果,所述授信终端信息为所述授信终端的至少两个授信终端信息,所述授信终端信息是根据所述授信终端的终端标识获取的,所述终端标识是所述至少两个授信终端信息按照信息被修改由难到易的排列顺序进行排列、加密和封装处理得到的;

当所述匹配结果满足预设验证条件时,确定所述登录终端为授信终端,并执行对所述终端应用的登录操作,所述预设验证条件包括所述匹配结果存在的不匹配的终端信息的权重值小于预设权重阈值,所述预设权重阈值为根据终端信息被修改的难易程度确定的值,所述终端信息越难被修改对应的权重值越大。

2.根据权利要求1所述的方法,其特征在于,所述接收当前登录终端发送的对终端应用的登录请求之前,还包括:

获取在授信终端中对终端应用进行登录操作的登录标识,并获取所述授信终端的授信终端信息;

对所述登录标识和所述授信终端信息进行存储。

3.根据权利要求2所述的方法,其特征在于,所述对所述登录标识和所述授信终端信息进行存储,包括:

获取所述至少两个授信终端信息中各授信终端信息的信息类型;

基于所述各授信终端信息的信息类型,并按照预设排列顺序对所述各授信终端信息进行排列处理;

采用预设加密算法分别对排列处理后的所述各授信终端信息进行加密处理,以生成加密后的所述各授信终端信息;

对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识,并对所述登录标识和所述终端标识进行存储。

4.根据权利要求3所述的方法,其特征在于,所述获取所述登录标识对应的预先存储的授信终端信息,并采用所述授信终端信息对按照信息被修改由难到易的排列顺序进行排列、加密处理后的所述至少两个登录终端信息进行匹配以生成匹配结果,包括:

获取所述登录标识对应的预先存储的授信终端信息,并获取所述至少两个登录终端信息中各登录终端信息的信息类型;

基于所述各登录终端信息的信息类型,按照信息被修改由难到易的排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理;

采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理,以生成加密后的所述各登录终端信息;

采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果。

5.根据权利要求4所述的方法,其特征在于,所述当所述匹配结果满足预设验证条件时,确定所述登录终端为授信终端,并执行对所述终端应用的登录操作,包括:

当所述匹配结果为加密后的所述各登录终端信息中存在至多一个与加密后的所述各授信终端信息不匹配的终端信息时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

6.根据权利要求4所述的方法，其特征在于，所述当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作，包括：

当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

7.根据权利要求4所述的方法，其特征在于，还包括：

当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求，以使所述登录终端获取针对所述登录验证请求所输入的验证信息；

接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作。

8.根据权利要求7所述的方法，其特征在于，还包括：

对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储。

9.一种应用登录设备，其特征在于，包括：

请求接收单元，用于接收当前登录终端发送的对终端应用的登录请求，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息；

结果生成单元，用于获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对按照信息被修改由难到易的排列顺序进行排列、加密处理后的所述至少两个登录终端信息进行匹配以生成匹配结果，所述授信终端信息为所述授信终端的至少两个授信终端信息，所述授信终端信息是根据所述授信终端的终端标识获取的，所述终端标识是所述至少两个授信终端信息按照信息被修改由难到易的排列顺序进行排列、加密和封装处理得到的；

登录操作执行单元，用于当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作，所述预设验证条件包括所述匹配结果存在的不匹配的终端信息的权重值小于预设权重阈值，所述预设权重阈值为根据终端信息被修改的难易程度确定的值，所述终端信息越难被修改对应的权重值越大。

10.根据权利要求9所述的设备，其特征在于，还包括：

信息获取单元，用于获取在授信终端中对终端应用进行登录操作的登录标识，并获取所述授信终端的授信终端信息；

信息存储单元，用于对所述登录标识和所述授信终端信息进行存储。

11.根据权利要求10所述的设备，其特征在于，所述信息存储单元包括：

第一类型获取子单元，用于获取所述至少两个授信终端信息中各授信终端信息的信息类型；

第一信息排列子单元，用于基于所述各授信终端信息的信息类型，并按照预设排列顺序对所述各授信终端信息进行排列处理；

第一信息加密子单元，用于采用预设加密算法分别对排列处理后的所述各授信终端信

息进行加密处理，以生成加密后的所述各授信终端信息；

标识存储子单元，用于对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识，并对所述登录标识和所述终端标识进行存储。

12.根据权利要求11所述的设备，其特征在于，所述结果生成单元包括：

第二类型获取子单元，用于获取所述登录标识对应的预先存储的授信终端信息，并获取所述至少两个登录终端信息中各登录终端信息的信息类型；

第二信息排列子单元，用于基于所述各登录终端信息的信息类型，按照信息被修改由难到易的排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理；

第二信息加密子单元，用于采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理，以生成加密后的所述各登录终端信息；

结果生成子单元，用于采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果。

13.根据权利要求12所述的设备，其特征在于，所述登录操作执行单元具体用于当所述匹配结果为加密后的所述各登录终端信息中存在至多一个与加密后的所述各授信终端信息不匹配的终端信息时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

14.根据权利要求12所述的设备，其特征在于，所述登录操作执行单元具体用于当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

15.根据权利要求12所述的设备，其特征在于，还包括：

请求发送单元，用于当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求，以使所述登录终端获取针对所述登录验证请求所输入的验证信息；

所述登录操作执行单元，还用于接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作。

16.根据权利要求15所述的设备，其特征在于，还包括：

标识存储单元，用于对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储。

17.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有多条指令，所述指令适于由处理器加载并执行如权利要求1-8任一项所述的方法。

一种应用登录方法及其设备

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种应用登录方法及其设备。

背景技术

[0002] 随着计算机技术不断的开发和完善，手机和平板电脑等终端已经成为了人们生活中不可或缺的一个部分，通过终端中的终端应用可以满足用户的不同需求，例如：即时通信、多媒体浏览等。通过使用在对终端应用进行注册时分配的应用账号、密码等登录标识，可以实现对终端应用的应用登录操作，基于登录标识，可以对用户提供个性化的服务，例如：存储用户的个人数据、与用户的好友进行通信等。

[0003] 在现有的登录操作过程中，已对终端应用进行用户身份验证的常用终端称为授信终端，往往会将授信终端单一的授信终端信息与登录标识进行关联存储，在后续使用授信终端进行终端应用的登录操作时，可以无需重复进行用户身份验证，然而由于单一的授信终端信息存在修改、伪造等可能性，例如：系统版本升级导致系统版本号的修改，或者黑客程序入侵导致国际移动设备识别码(International Mobile Equipment Identity，IMEI)的伪造等，在登录操作过程中容易因终端识别失败而无法进行登录操作，或者需要再次进行用户身份验证等，影响了终端识别的准确性，进而影响了终端应用的登录效率。

发明内容

[0004] 本发明实施例提供一种应用登录方法及其设备，可以保证在登录操作过程中的终端识别的准确性，进一步提升终端应用的登录效率。

[0005] 本发明实施例第一方面提供了一种应用登录方法，可包括：

[0006] 接收当前登录终端发送的对终端应用的登录请求，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息；

[0007] 获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果；

[0008] 当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0009] 本发明实施例第二方面提供了一种应用登录设备，可包括：

[0010] 请求接收单元，用于接收当前登录终端发送的对终端应用的登录请求，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息；

[0011] 结果生成单元，用于获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果；

[0012] 登录操作执行单元，用于当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0013] 在本发明实施例中，在接收到当前的登录终端发送的对终端应用的登录请求时，可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息，并采用预先存储的

授权终端信息对至少两个登录终端信息进行匹配，最终在匹配结果满足预设验证条件时，确定登录终端为授信终端，对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率。

附图说明

[0014] 为了更清楚地说明本发明实施例或现有技术中的技术方案，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。

[0015] 图1是本发明实施例提供的一种应用登录方法的流程示意图；

[0016] 图2是本发明实施例提供的另一种应用登录方法的流程示意图；

[0017] 图3是本发明实施例提供的一种应用登录设备的结构示意图；

[0018] 图4是本发明实施例提供的另一种应用登录设备的结构示意图；

[0019] 图5是本发明实施例提供的信息存储单元的结构示意图；

[0020] 图6是本发明实施例提供的结果生成单元的结构示意图；

[0021] 图7是本发明实施例提供的又一种应用登录设备的结构示意图。

具体实施方式

[0022] 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，所描述的实施例仅仅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做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。

[0023] 本发明实施例提供的应用登录方法可以应用于终端应用登录时，确定登录终端为授信终端并在登录终端上登录的场景，例如：应用登录设备接收当前登录终端发送的对终端应用的登录请求，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息，所述应用登录设备获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果，当所述匹配结果满足预设验证条件时，所述应用登录设备确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率。

[0024] 本发明实施例涉及的应用登录设备可以为终端应用的后台服务设备，具体可以用于管理终端应用的应用数据以及登录标识等；所述登录终端和授信终端均可以包括：平板电脑、智能手机、掌上电脑以及移动互联网设备(MID)等具备对终端应用进行使用的终端设备，所述登录终端具体可以为当前所使用的对终端应用进行登录操作的终端，所述授信终端具体可以为已对终端应用进行用户身份验证的常用终端；所述终端应用可以包括云存储

应用、即时通信应用等需要进行登录操作的应用。

[0025] 下面将结合附图1和附图2,对本发明实施例提供的应用登录方法进行详细介绍。

[0026] 请参见图1,为本发明实施例提供了一种应用登录方法的流程示意图。如图1所示,本发明实施例的所述方法可以包括以下步骤S101-步骤S103。

[0027] S101,接收当前登录终端发送的对终端应用的登录请求;

[0028] 具体的,应用登录设备可以接收当前登录终端发送的对终端应用的登录请求,可以理解的是,所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息,所述登录标识可以是用户登录终端应用时的登录账户(例如:账户昵称或者由数字和字母组成的登录账号),所述至少两个登录终端信息,可以是识别所述当前登录终端身份的识别信息,可以包括软件可识别信息和硬件可识别信息,例如:可以是当前登录终端的网卡(Media Access Control,MAC)、国际移动设备识别码IMEI、Vendor标识符(Identifier For Vendor,IDFV)、广告标识符(Identifier For Identifier,IDFA)、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0029] S102,获取所述登录标识对应的预先存储的授信终端信息,并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果;

[0030] 具体的,所述应用登录设备可以获取所述登录标识对应的预先存储的授信终端信息,可以理解的是,所述授信终端信息可以是识别授信终端身份的识别信息,例如:可以是授信终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0031] 进一步的,所述应用登录设备可以采用所述授信终端信息对所述至少两个登录终端信息进匹配以生成匹配结果,可以理解的是,所述授信终端信息可以为至少两个,所述匹配结果可以是所述至少两个登录终端信息中与所述授信终端信息不匹配的登录终端信息的个数。

[0032] S103,当所述匹配结果满足预设验证条件时,确定所述登录终端为授信终端,并执行对所述终端应用的登录操作;

[0033] 具体的,当所述匹配结果满足预设验证条件时,所述应用登录设备可以确定所述登录终端为授信终端,并可以执行对所述终端应用的登录操作。例如,当所述匹配结果为所述至少两个登录终端信息中存在至多一个与所述授信终端信息不匹配的终端信息时,所述应用登录设备可以确定所述登录终端为授信终端,并可以根据所述登录标识执行对所述终端应用的登录操作。

[0034] 在本发明实施例中,在接收到当前的登录终端发送的对终端应用的登录请求时,可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息,并采用预先存储的授权终端信息对至少两个登录终端信息进行匹配,最终在匹配结果满足预设验证条件时,确定登录终端为授信终端,对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断,避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况,保证了在登录操作过程中的终端识别的准确性,进一步提升了终端应用的登录效率。

[0035] 请参见图2,为本发明实施例提供了另一种应用登录方法的流程示意图。如图2所示,本发明实施例的所述方法可以包括以下步骤S201-步骤S211。

[0036] S201,获取在授信终端中对终端应用进行登录操作的登录标识,并获取所述授信终端的授信终端信息;

[0037] 具体的,所述应用登录设备可以获取在授信终端中对终端应用进行登录操作的登录标识,可以理解的是,所述登录标识可以是用户登录终端应用时的登录账户,例如:账户昵称或者由数字和字母组成的登录账号等。

[0038] 进一步的,所述应用登录设备可以获取所述授信终端的授信终端信息,可以理解的是,所述授信终端信息可以是识别授信终端身份的识别信息,可以包括软件可识别信息和硬件可识别信息,例如:可以是授信终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0039] S202,对所述登录标识和所述授信终端信息进行存储;

[0040] 具体的,所述应用登录设备可以对获取到的所述登录标识和所述授信终端信息进行存储。可以理解的是,当再次在所述授信终端上登录所述登录标识对应的终端应用时,所述应用登录设备可以直接执行登录该终端应用的登录操作,无需对用户身份进行验证。

[0041] 优选的,所述授信终端信息可以为至少两个授信终端信息,则所述应用登录设备对所述登录标识和所述授信终端信息进行存储的过程可以是:

[0042] 所述应用登录设备可以获取所述至少两个授信终端信息中各授信终端信息的信息类型,可以理解的是,所述各授信终端信息的信息类型可以是按照信息本身所属的软硬件进行界定的类型(例如:软件信息类型和硬件信息类型),也可以按照信息能够被修改的难易程度进行界定的类型(例如:易修改信息类型和难修改信息类型),也可以是按其他划分信息类型的方式进行界定所述各授信终端信息的信息类型。

[0043] 进一步的,所述应用登录设备可以基于所述各授信终端信息的信息类型,并可以按照预设排列顺序对所述各授信终端信息进行排列处理,例如,按照所述各授信终端信息可以被修改的难易程度,从难被修改的信息到易被修改的信息依次排列(例如,按照信息可以被修改的难易程度(由难到易)得到的各授信终端信息的排列为:网卡MAC、国际移动设备识别码IMEI、广告标识符IDFA、Vendor标识符IDFV、设备厂商标识、设备型号标识、操作系统版本号和设备名称标识)。

[0044] 进一步的,所述应用登录设备可以采用预设加密算法分别对排列处理后的所述各授信终端信息进行加密处理,以生成加密后的所述各授信终端信息,可以理解的是,所述预设加密算法可以是对排列处理后的所述各授信终端信息进行变换操作,变换后的所述各授信终端信息不能被恢复。

[0045] 优选的,所述应用登录设备可以采用不可逆的散列函数(例如:SHA256算法)对排列处理后的所述各授信终端信息进行加密处理,具体加密过程可以是:

[0046] F1=SHA256(MAC+SALT1)

[0047] F2=SHA256(IEMI+SALT2)

[0048] F3=SHA256(IDFA+SALT3)

[0049] F4=SHA256(IDFV+SALT4)

[0050] F5=SHA256(设备厂商标识+SALT5)

[0051] F6=SHA256(设备型号标识+SALT6)

[0052] F7=SHA256(操作系统版本号+SALT7)

[0053] F8＝SHA256(设备名称标识+SALT8)

[0054] 可以理解的是,为避免其他数据库泄露造成的数据碰撞,在对上述各授信终端信息进行散列变换时分别加入SALT1-SALT8的盐值,其中,FI-F8为采用SHA256算法进行加密处理后的各授信终端信息。

[0055] 进一步的,所述应用登录设备可以对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识,例如,所述应用登录设备可以对加密后的所述各授信终端信息FI-F8,进行封装生成所述授信终端的终端标识GUID,可以理解的是,GUID＝F1+F2+...+F8。进一步的,所述应用登录设备可以对所述登录标识和所述终端标识进行存储,可以理解的是,所述终端标识可以是GUID。

[0056] S203,接收当前登录终端发送的对终端应用的登录请求;

[0057] 具体的,所述应用登录设备可以接收当前登录终端发送的对终端应用的登录请求,可以理解的是,所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息,所述至少两个登录终端信息,可以是识别所述当前登录终端身份的识别信息,例如:可以是当前登录终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0058] S204,获取所述登录标识对应的预先存储的授信终端信息,并获取所述至少两个登录终端信息中各登录终端信息的信息类型;

[0059] 具体的,所述应用登录设备可以获取所述登录标识对应的预先存储的授信终端信息,并可以获取所述至少两个登录终端信息中各登录终端信息的信息类型,可以理解的是,所述各登录终端信息的信息类型的划分方法可以与所述各授信终端信息的信息类型的划分方法一致,例如,按信息所属的软硬件进行界定或按信息可被修改的难易程度进行界定。

[0060] S205,基于所述各登录终端信息的信息类型,按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理;

[0061] 具体的,所述应用登录设备可以基于所述各登录终端信息的信息类型,并按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理,例如,按照所述各登录终端信息可以被修改的难易程度,从难被修改的信息到易被修改的信息依次排列(例如,按照信息可以被修改的难易程度(由难到易)得到的各登录终端信息的排列为:网卡MAC、国际移动设备识别码IMEI、广告标识符IDFA、Vendor标识符IDFV、设备厂商标识、设备型号标识、操作系统版本号和设备名称标识)。

[0062] S206,采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理,以生成加密后的所述各登录终端信息;

[0063] 具体的,所述应用登录设备可以采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理,以生成加密后的所述各登录终端信息,可以理解的是,所述预设加密算法可以是对排列处理后的所述各登录终端信息进行变换操作,变换后的所述各登录终端信息不能被恢复。

[0064] 优选的,所述应用登录设备可以采用不可逆的散列函数(例如:SHA256算法)对排列处理后的所述各登录终端信息进行加密处理,加密过程与步骤S202中对各授信终端信息的加密过程一致,可以用$F1^1$,$F2^2$……代表采用SHA256算法进行加密处理后的所述至少两个登录终端信息中的各登录终端信息,具体的加密过程此处不再赘述。

[0065] S207，采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果；

[0066] 具体的，所述应用登录设备可以采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果，可以理解的是，由于对所述各授信终端信息和所述各登录终端信息采用的加密算法一致，若加密二者能匹配，则加密后也可以匹配，可以理解的是，所述匹配结果可以是所述各登录终端信息中与所述各授信终端信息不匹配的登录终端信息的个数或登录终端信息的权重值。

[0067] 在本发明实施例中，通过对所述各授信终端信息和所述各登录终端信息进行排列、加密和封装处理得到相应的终端标识，降低了终端标识被修改的可能性。

[0068] S208，当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作；

[0069] 具体的，当所述匹配结果满足预设验证条件时，所述应用登录设备可以确定所述登录终端为授信终端，并可以执行对所述终端应用的登录操作

[0070] 可选的，当所述匹配结果为加密后的所述各登录终端信息中存在至多一个与加密后的所述各授信终端信息不匹配的终端信息时，所述应用登录设备可以确定所述登录终端为授信终端，并可以执行对所述终端应用的登录操作。

[0071] 可选的，当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，所述应用登录设备可以确定所述登录终端为授信终端，并可以执行对所述终端应用的登录操作。可以理解的是，所述预设权重阈值可以是根据所述各登录终端信息能够被修改的难以程度确定的值。在本发明实施例中，可以将所述各登录终端信息中容易被修改的登录终端信息的权重值设置为小于难以被修改的登录终端信息的权重值，即登录终端信息越难被修改对应的权重值越大。可以理解的是，当加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，所述不匹配的终端信息为易被修改的终端信息，可以认为该终端信息不影响所述应用登录设备确定所述当前登录终端为授信终端的结果。

[0072] 在本发明实施例中，通过对终端信息添加相应的权重值，并忽略权重值小于预设权重阈值的与授信终端信息不匹配的登录终端信息对判断登录终端是否为授信终端的影响，提高了判断登录终端是否为授信终端的判断效率。

[0073] S209，当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求；

[0074] 具体的，当所述匹配结果不满足预设验证条件时，所述应用登录设备可以向所述登录终端发送与所述终端应用相关联的登录验证请求，以使所述登录终端获取针对所述登录验证请求所输入的验证信息。

[0075] 可选的，当所述匹配结果为加密后的所述各登录终端信息中存在至少两个与加密后的所述各授信终端信息不匹配的终端信息时，所述应用登录设备可以向所述登录终端发送与所述终端应用相关联的登录验证请求。可以理解的是，所述登录验证请求可以是与所述终端应用相关联，用于验证用户身份的验证问题或者提示输入身份验证信息的请求(例如，提示输入指纹验证信息)。

[0076] 可选的，当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值大于或等于预设权重阈值时，所述应用登录设备可以向所述登录终端发送与所述终端应用相关联的登录验证请求。可以理解的是，当不匹配的终端信息的权重值大于或等于预设权重阈值时，代表较难被修改的终端信息可能被修改了，所述应用登录设备需要向所述登录终端发送与所述终端应用相关联的登录验证请求，以验证所述登录终端是否为用户信任的终端设备。

[0077] 进一步的，当所述登录终端接收到所述登录验证请求后，可以获取用户针对所述登录验证请求所输入的验证信息。

[0078] 在本发明的具体实施方式中，一个登录标识可以在多个授信终端上登录，因此同一个登录标识可以被关联多个授信终端的终端标识GUID。当所述登录终端信息与所述登录标识相关联的多个授信终端的终端标识GUID中的任一个相匹配时，所述应用登录设备都可以确定所述登录终端信息对应的登录终端为授信终端，并可以执行对所述登录标识对应的终端应用的登录操作。

[0079] 在本发明的具体实施方式中，若一个授信终端的终端标识GUID与多个登录标识相关联，则所述多个登录标识之间具有一定的关联性。当所述多个登录标识中存在重度登录标识(例如，可以是关联了终端应用会员的登录标识)时，所述应用登录设备可以获取所述重度登录标识对应的所有授信终端的终端标识GUID，当所述多个登录标识中的非重度登录标识对应的登录终端标识为上述所有授信终端标识GUID中的任一个，且所述非重度登录标识对应的授信终端标识与所述登录终端标识不匹配时，所述应用登录设备可以向所述登录终端发送简单的验证请求，也可以不发送验证请求，即简化非重度登录标识的登录验证过程。

[0080] S210，接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作；

[0081] 具体的，所述应用登录设备可以接收所述登录终端发送的所述验证信息，可以理解的是，所述验证信息可以是验证所述登录验证请求的信息，例如：所述登录验证请求为“身份验证问题”，则所述验证信息是“问题对应的答案”。

[0082] 进一步的，在验证处理通过后，所述应用登录设备可以执行对所述终端应用的登录操作。

[0083] S211，对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储；

[0084] 具体的，所述应用登录设备可以对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并可以对所述登录标识和所述终端标识进行存储。例如，经SHA256算法处理加密后的各登录终端信息为$F1^1$，$F2^2$……，则所述应用登录设备可以对$F1^1$，$F2^2$……进行封装生成所述登录终端的终端标识$GUID^1$，可以理解的是$GUID^1=F1^1+F2^2+...$。进一步的，所述应用登录设备可以对所述登录标识和所述终端标识进行存储，可以理解的是，所述终端标识可以是$GUID^1$。

[0085] 在本发明实施例中，在接收到当前的登录终端发送的对终端应用的登录请求时，可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息，并采用预先存储的授权终端信息对至少两个登录终端信息进行匹配，最终在匹配结果满足预设验证条件时，

确定登录终端为授信终端，对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率；通过对各授信终端信息和各登录终端信息进行排列、加密和封装处理得到相应的终端标识，降低了终端标识被修改的可能性；通过对终端信息添加相应的权重值，提高了判断登录终端是否为授信终端的判断效率。

[0086] 下面将结合附图3-附图6，对本发明实施例提供的应用登录设备进行详细介绍。需要说明的是，附图3-附图6所示的应用登录设备，用于执行本发明图1和图2所示实施例的方法，为了便于说明，仅示出了与本发明实施例相关的部分，具体技术细节未揭示的，请参照本发明图1和图2所示的实施例。

[0087] 请参见图3，为本发明实施例提供了一种应用登录设备的结构示意图。如图3所示，本发明实施例的所述应用登录设备1可以包括：请求接收单元11、结果生成单元12和登录操作执行单元13。

[0088] 请求接收单元11，用于接收当前登录终端发送的对终端应用的登录请求；

[0089] 具体实现中，所述请求接收单元11可以接收当前登录终端发送的对终端应用的登录请求，可以理解的是，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息，所述登录标识可以是用户登录终端应用时的登录账户(例如：账户昵称或者由数字和字母组成的登录账号)，所述至少两个登录终端信息，可以是识别所述当前登录终端身份的识别信息，可以包括软件可识别信息和硬件可识别信息，例如：可以是当前登录终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0090] 结果生成单元12，用于获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果；

[0091] 具体实现中，所述结果生成单元12可以获取所述登录标识对应的预先存储的授信终端信息，可以理解的是，所述授信终端信息可以是识别授信终端身份的识别信息，例如：可以是授信终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0092] 进一步的，所述结果生成单元12可以采用所述授信终端信息对所述至少两个登录终端信息进匹配以生成匹配结果，可以理解的是，所述授信终端信息可以为至少两个，所述匹配结果可以是所述至少两个登录终端信息中与所述授信终端信息不匹配的登录终端信息的个数。

[0093] 登录操作执行单元13，用于当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作；

[0094] 具体实现中，当所述匹配结果满足预设验证条件时，所述登录操作执行单元13可以确定所述登录终端为授信终端，并可以执行对所述终端应用的登录操作。例如，当所述匹配结果为所述至少两个登录终端信息中存在至多一个与所述授信终端信息不匹配的终端信息时，所述登录操作执行单元13可以确定所述登录终端为授信终端，并可以根据所述登录标识执行对所述终端应用的登录操作。

[0095] 在本发明实施例中，在接收到当前的登录终端发送的对终端应用的登录请求时，

可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息，并采用预先存储的授权终端信息对至少两个登录终端信息进行匹配，最终在匹配结果满足预设验证条件时，确定登录终端为授信终端，对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率。

[0096] 请参见图4，为本发明实施例提供了另一种应用登录设备的结构示意图。如图4所示，本发明实施例的所述应用登录设备1可以包括：请求接收单元11、结果生成单元12、登录操作执行单元13、信息获取单元14、信息存储单元15、请求发送单元16和标识存储单元17。

[0097] 信息获取单元14，用于获取在授信终端中对终端应用进行登录操作的登录标识，并获取所述授信终端的授信终端信息；

[0098] 具体实现中，所述信息获取单元14可以获取在授信终端中对终端应用进行登录操作的登录标识，可以理解的是，所述登录标识可以是用户登录终端应用时的登录账户，例如：账户昵称或者由数字和字母组成的登录账号等。

[0099] 进一步的，所述信息获取单元14可以获取所述授信终端的授信终端信息，可以理解的是，所述授信终端信息可以是识别授信终端身份的识别信息，可以包括软件可识别信息和硬件可识别信息，例如：可以是授信终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0100] 信息存储单元15，用于对所述登录标识和所述授信终端信息进行存储；

[0101] 具体实现中，所述信息存储单元15可以对获取到的所述登录标识和所述授信终端信息进行存储。可以理解的是，当再次在所述授信终端上登录所述登录标识对应的终端应用时，所述应用登录设备1可以直接执行登录该终端应用的登录操作，无需对用户身份进行验证。

[0102] 具体的，请一并参见图5，为本发明实施例提供了信息存储单元的结构示意图。如图5所示，所述信息存储单元15可以包括：

[0103] 第一类型获取子单元151，用于获取所述至少两个授信终端信息中各授信终端信息的信息类型；

[0104] 具体实现中，所述第一类型获取子单元151可以获取所述至少两个授信终端信息中各授信终端信息的信息类型，可以理解的是，所述各授信终端信息的信息类型可以是按照信息本身所属的软硬件进行界定的类型(例如：软件信息类型和硬件信息类型)，也可以按照信息能够被修改的难易程度进行界定的类型(例如：易修改信息类型和难修改信息类型)，也可以是按其他划分信息类型的方式进行界定所述各授信终端信息的信息类型。

[0105] 第一信息排列子单元152，用于基于所述各授信终端信息的信息类型，并按照预设排列顺序对所述各授信终端信息进行排列处理；

[0106] 具体实现中，所述第一信息排列子单元152可以基于所述各授信终端信息的信息类型，并可以按照预设排列顺序对所述各授信终端信息进行排列处理，例如，按照所述各授信终端信息可以被修改的难易程度，从难被修改的信息到易被修改的信息依次排列(例如，按照信息可以被修改的难易程度(由难到易)得到的各授信终端信息的排列为：网卡MAC、国际移动设备识别码IMEI、广告标识符IDFA、Vendor标识符IDFV、设备厂商标识、设备型号标

识、操作系统版本号和设备名称标识)。

[0107] 第一信息加密子单元153,用于采用预设加密算法分别对排列处理后的所述各授信终端信息进行加密处理,以生成加密后的所述各授信终端信息;

[0108] 具体实现中,所述第一信息加密子单元153可以采用预设加密算法分别对排列处理后的所述各授信终端信息进行加密处理,以生成加密后的所述各授信终端信息,可以理解的是,所述预设加密算法可以是对排列处理后的所述各授信终端信息进行变换操作,变换后的所述各授信终端信息不能被恢复。

[0109] 优选的,所述应用登录设备可以采用不可逆的散列函数(例如:SHA256算法)对排列处理后的所述各授信终端信息进行加密处理,具体加密过程可以参照上述方法实施例的相关描述,此处不再赘述。

[0110] 标识存储子单元154,用于对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识,并对所述登录标识和所述终端标识进行存储;

[0111] 具体实现中,所述标识存储子单元154可以对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识,例如,所述标识存储子单元154可以对加密后的所述各授信终端信息FI-F8,进行封装生成所述授信终端的终端标识GUID,可以理解的是GUID=F1+F2+...+F8。进一步的,所述标识存储子单元154可以对所述登录标识和所述终端标识进行存储,可以理解的是,所述终端标识可以是GUID。

[0112] 请求接收单元11,用于接收当前登录终端发送的对终端应用的登录请求;

[0113] 具体实现中,所述请求接收单元11可以接收当前登录终端发送的对终端应用的登录请求,可以理解的是,所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息,所述至少两个登录终端信息,可以是识别所述当前登录终端身份的识别信息,例如:可以是当前登录终端的网卡MAC、国际移动设备识别码IMEI、Vendor标识符IDFV、广告标识符IDFA、设备厂商、设备型号、操作系统版本或设备名称等信息。

[0114] 结果生成单元12,用于获取所述登录标识对应的预先存储的授信终端信息,并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果;

[0115] 具体实现中,所述结果生成单元12可以获取所述登录标识对应的预先存储的授信终端信息,并可以采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果。

[0116] 具体的,请一并参见图6,为本发明实施例提供了结果生成单元的结构示意图。如图6所示,所述结果生成单元12可以包括:

[0117] 第二类型获取子单元121,用于获取所述登录标识对应的预先存储的授信终端信息,并获取所述至少两个登录终端信息中各登录终端信息的信息类型;

[0118] 具体实现中,所述第二类型获取子单元121可以获取所述登录标识对应的预先存储的授信终端信息,并可以获取所述至少两个登录终端信息中各登录终端信息的信息类型,可以理解的是,所述各登录终端信息的信息类型的划分方法可以与所述各授信终端信息的信息类型的划分方法一致,例如,按信息所属的软硬件进行界定或按信息可被修改的难易程度进行界定。

[0119] 第二信息排列子单元122,用于基于所述各登录终端信息的信息类型,按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理;

[0120] 具体实现中，所述第二信息排列子单元122可以基于所述各登录终端信息的信息类型，并按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理，例如，按照所述各登录终端信息可以被修改的难易程度，从难被修改的信息到易被修改的信息依次排列(例如，按照信息可以被修改的难易程度(由难到易)得到的各登录终端信息的排列为：网卡MAC、国际移动设备识别码IMEI、广告标识符IDFA、Vendor标识符IDFV、设备厂商标识、设备型号标识、操作系统版本号和设备名称标识)。

[0121] 第二信息加密子单元123，用于采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理，以生成加密后的所述各登录终端信息；

[0122] 具体实现中，所述第二信息加密子单元123可以采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理，以生成加密后的所述各登录终端信息，可以理解的是，所述预设加密算法可以是对排列处理后的所述各登录终端信息进行变换操作，变换后的所述各登录终端信息不能被恢复。

[0123] 优选的，所述第二信息加密子单元123可以采用不可逆的散列函数(例如：SHA256算法)对排列处理后的所述各登录终端信息进行加密处理，加密过程与各授信终端信息的加密过程一致，可以用$F1^1$，$F2^2$……代表采用SHA256算法进行加密处理后的所述至少两个登录终端信息中的各登录终端信息，具体的加密过程可以参加上述方法实施例的相关描述，此处不再赘述。

[0124] 结果生成子单元124，用于采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果；

[0125] 具体实现中，所述结果生成子单元124可以采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果，可以理解的是，由于对所述各授信终端信息和所述各登录终端信息采用的加密算法一致，若加密二者能匹配，则加密后也可以匹配，可以理解的是，所述匹配结果可以是所述各登录终端信息中与所述各授信终端信息不匹配的登录终端信息的个数或登录终端信息的权重值。

[0126] 在本发明实施例中，通过对所述各授信终端信息和所述各登录终端信息进行排列、加密和封装处理得到相应的终端标识，降低了终端标识被修改的可能性。

[0127] 登录操作执行单元13，用于当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作；

[0128] 具体实现中，所述登录操作执行单元13具体用于，当所述匹配结果为加密后的所述各登录终端信息中存在至多一个与加密后的所述各授信终端信息不匹配的终端信息时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0129] 所述登录操作执行单元13还用于，当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。可以理解的是，所述预设权重阈值可以是根据所述各登录终端信息能够被修改的难以程度确定的值。在本发明实施例中，可以将所述各登录终端信息中容易被修改的登录终端信息的权重值设置为小于难以被修改的登录终端信息的权重值，即登录终端信息越难被修改对应的权重值越大。可以理解的是，当加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，所述不匹配的终端信息为易被

修改的终端信息，可以认为该终端信息不影响所述应用登录设备确定所述当前登录终端为授信终端的结果。

[0130] 在本发明实施例中，通过对终端信息添加相应的权重值，并忽略权重值小于预设权重阈值的与授信终端信息不匹配的登录终端信息对判断登录终端是否为授信终端的影响，提高了判断登录终端是否为授信终端的判断效率。

[0131] 请求发送单元16，用于当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求；

[0132] 具体实现中，当所述匹配结果不满足预设验证条件时，所述请求发送单元16可以向所述登录终端发送与所述终端应用相关联的登录验证请求，以使所述登录终端获取针对所述登录验证请求所输入的验证信息。

[0133] 可选的，当所述匹配结果为加密后的所述各登录终端信息中存在至少两个与加密后的所述各授信终端信息不匹配的终端信息时，所述请求发送单元16可以向所述登录终端发送与所述终端应用相关联的登录验证请求。可以理解的是，所述登录验证请求可以是与所述终端应用相关联，用于验证用户身份的验证问题或者提示输入身份验证信息的请求(例如，提示输入指纹验证信息)。

[0134] 可选的，当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值大于或等于预设权重阈值时，所述请求发送单元16可以向所述登录终端发送与所述终端应用相关联的登录验证请求。可以理解的是，当不匹配的终端信息的权重值大于或等于预设权重阈值时，代表较难被修改的终端信息可能被修改了，所述应用登录设备需要向所述登录终端发送与所述终端应用相关联的登录验证请求，以验证所述登录终端是否为用户信任的终端设备。

[0135] 进一步的，当所述登录终端接收到所述登录验证请求后，可以获取用户针对所述登录验证请求所输入的验证信息。

[0136] 在本发明的具体实施方式中，一个登录标识可以在多个授信终端上登录，因此同一个登录标识可以被关联多个授信终端的终端标识GUID。当所述登录终端信息与所述登录标识相关联的多个授信终端的终端标识GUID中的任一个相匹配时，所述应用登录设备都可以确定所述登录终端信息对应的登录终端为授信终端，并可以执行对所述登录标识对应的终端应用的登录操作。

[0137] 在本发明的具体实施方式中，若一个授信终端的终端标识GUID与多个登录标识相关联，则所述多个登录标识之间具有一定的关联性。当所述多个登录标识中存在重度登录标识(例如，可以是关联了相关终端应用会员的登录标识)时，所述应用登录设备可以获取所述重度登录标识对应的所有授信终端的终端标识GUID，当所述多个登录标识中的非重度登录标识对应的登录终端标识为上述所有授信终端标识GUID中的任一个，且所述非重度登录标识对应的授信终端标识与所述登录终端标识不匹配时，所述应用登录设备可以向所述登录终端发送简单的验证请求，也可以不发送验证请求，即简化非重度登录标识的登录验证过程。

[0138] 所述登录操作执行单元13，还用于接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作；

[0139] 具体实现中，所述登录操作执行单元13可以接收所述登录终端发送的所述验证信

息，可以理解的是，所述验证信息可以是验证所述登录验证请求的信息，例如：所述登录验证请求为“身份验证问题”，则所述验证信息是“问题对应的答案”。

[0140] 进一步的，在验证处理通过后，所述登录操作执行单元13可以执行对所述终端应用的登录操作。

[0141] 标识存储单元17，用于对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储；

[0142] 具体实现中，所述标识存储单元17可以对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并可以对所述登录标识和所述终端标识进行存储。例如，经SHA256算法处理加密后的各登录终端信息为$F1^1$，$F2^2$……，则所述标识存储单元17可以对$F1^1$，$F2^2$……进行封装生成所述登录终端的终端标识$GUID^1$，可以理解的是$GUID^1=F1^1+F2^2+...$。进一步的，所述标识存储单元17可以对所述登录标识和所述终端标识进行存储，可以理解的是，所述终端标识可以是$GUID^1$。

[0143] 在本发明实施例中，在接收到当前的登录终端发送的对终端应用的登录请求时，可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息，并采用预先存储的授权终端信息对至少两个登录终端信息进行匹配，最终在匹配结果满足预设验证条件时，确定登录终端为授信终端，对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率；通过对各授信终端信息和各登录终端信息进行排列、加密和封装处理得到相应的终端标识，降低了终端标识被修改的可能性；通过对终端信息添加相应的权重值，提高了判断登录终端是否为授信终端的判断效率。

[0144] 请参见图7，为本发明实施例提供了又一种应用登录设备的结构示意图。如图7所示，所述应用登录设备1000可以包括：至少一个处理器1001，例如CPU，至少一个网络接口1004，用户接口1003，存储器1005，至少一个通信总线1002。其中，通信总线1002用于实现这些组件之间的连接通信。其中，用户接口1003可以包括显示屏(Display)、键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器。存储器1005可选的还可以是至少一个位于远离前述处理器1001的存储装置。如图7所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及应用登录应用程序。

[0145] 在图7所示的人流分布处理设备1000中，用户接口1003主要用于为用户提供输入的接口，获取用户输入的数据；网络接口1004用于与登录终端和/或授信终端进行数据通信；而处理器1001可以用于调用存储器1005中存储的应用登录应用程序，并具体执行以下操作：

[0146] 接收当前登录终端发送的对终端应用的登录请求，所述登录请求包含所述终端应用对应的登录标识和所述登录终端的至少两个登录终端信息；

[0147] 获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果；

[0148] 当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0149] 在一个实施例中，所述处理器1001在执行接收当前登录终端发送的对终端应用的登录请求之前，还执行以下操作：

[0150] 获取在授信终端中对终端应用进行登录操作的登录标识，并获取所述授信终端的授信终端信息；

[0151] 对所述登录标识和所述授信终端信息进行存储。

[0152] 在一个实施例中，所述授信终端信息为所述授信终端的至少两个授信终端信息，所述处理器1001在执行对所述登录标识和所述授信终端信息进行存储时，具体执行以下操作：

[0153] 获取所述至少两个授信终端信息中各授信终端信息的信息类型；

[0154] 基于所述各授信终端信息的信息类型，并按照预设排列顺序对所述各授信终端信息进行排列处理；

[0155] 采用预设加密算法分别对排列处理后的所述各授信终端信息进行加密处理，以生成加密后的所述各授信终端信息；

[0156] 对加密后的所述各授信终端信息进行封装以生成所述授信终端的终端标识，并对所述登录标识和所述终端标识进行存储。

[0157] 在一个实施例中，所述处理器1001在执行获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果时，具体执行以下操作：

[0158] 获取所述登录标识对应的预先存储的授信终端信息，并获取所述至少两个登录终端信息中各登录终端信息的信息类型；

[0159] 基于所述各登录终端信息的信息类型，按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理；

[0160] 采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理，以生成加密后的所述各登录终端信息；

[0161] 采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果。

[0162] 在一个实施例中，所述处理器1001在执行当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作时，具体执行以下操作：

[0163] 当所述匹配结果为加密后的所述各登录终端信息中存在至多一个与加密后的所述各授信终端信息不匹配的终端信息时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0164] 在一个实施例中，所述处理器1001在执行当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作时，具体执行以下操作：

[0165] 当所述匹配结果为加密后的所述各登录终端信息中与加密后的所述各授信终端信息中存在的不匹配的终端信息的权重值小于预设权重阈值时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作。

[0166] 在一个实施例中，所述处理器1001还用于执行以下操作：

[0167] 当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求，以使所述登录终端获取针对所述登录验证请求所输入的验证信息；

[0168] 接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作。

[0169] 在一个实施例中，所述处理器1001还用于执行以下操作：

[0170] 对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储。

[0171] 在本发明实施例中，在接收到当前的登录终端发送的对终端应用的登录请求时，可以获取终端应用的登录标识以及登录终端的至少两个登录终端信息，并采用预先存储的授权终端信息对至少两个登录终端信息进行匹配，最终在匹配结果满足预设验证条件时，确定登录终端为授信终端，对终端应用进行登录操作。通过采用至少两个登录终端信息对登录终端是否为授信终端进行判断，避免了单一信息被修改或伪造时无法登录终端应用或需要进行用户身份验证的情况，保证了在登录操作过程中的终端识别的准确性，进一步提升了终端应用的登录效率；通过对各授信终端信息和各登录终端信息进行排列、加密和封装处理得到相应的终端标识，降低了终端标识被修改的可能性；通过对终端信息添加相应的权重值，提高了判断登录终端是否为授信终端的判断效率。

[0172] 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流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0173] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

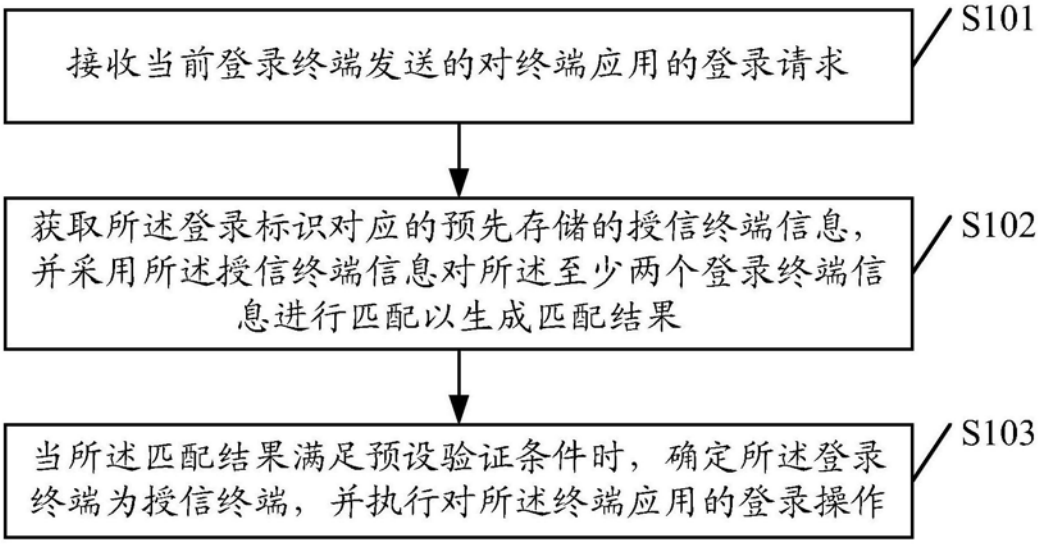

接收当前登录终端发送的对终端应用的登录请求
S101
获取所述登录标识对应的预先存储的授信终端信息，并采用所述授信终端信息对所述至少两个登录终端信息进行匹配以生成匹配结果
S102
当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作
S103

图1

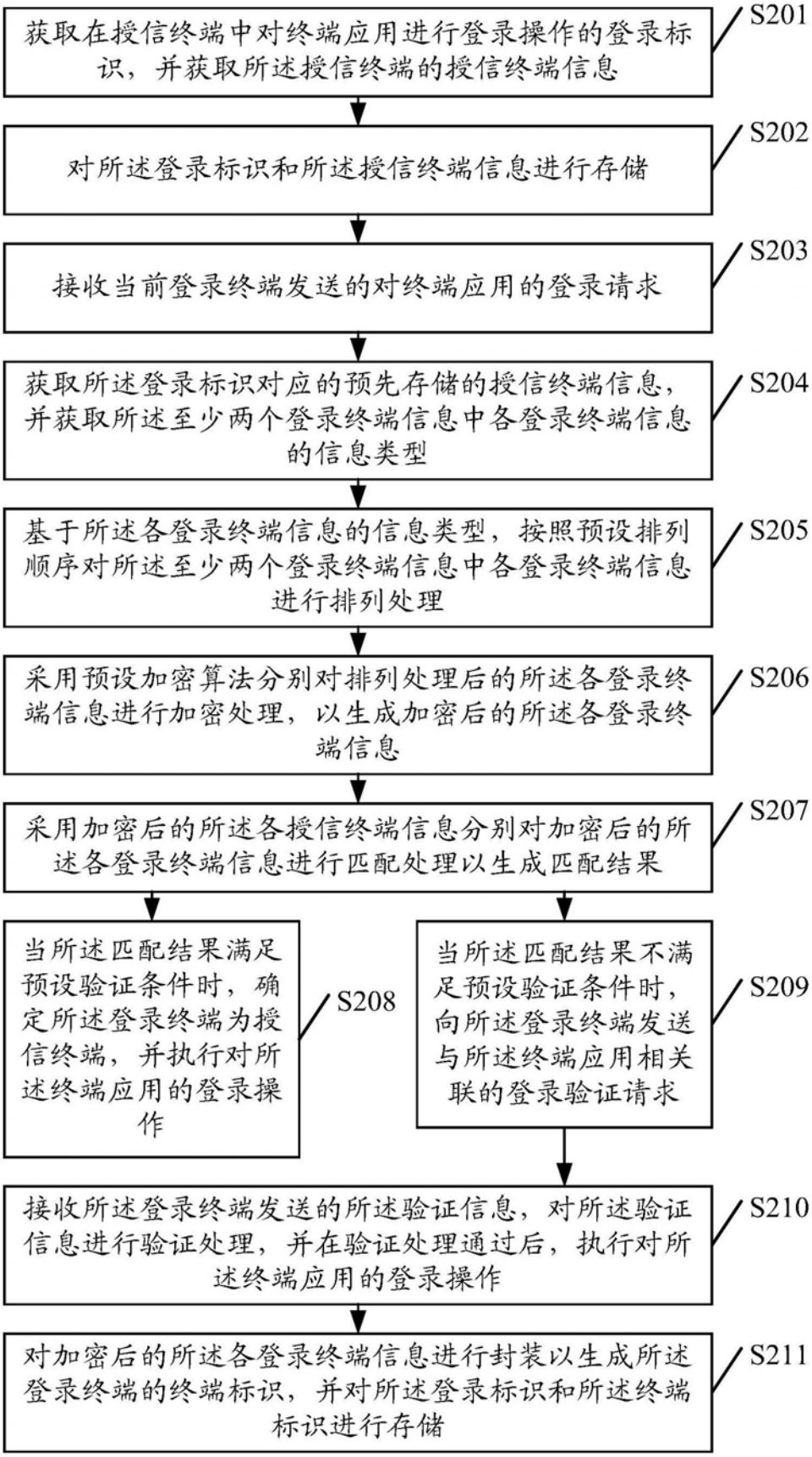

获取在授信终端中对终端应用进行登录操作的登录标识，并获取所述授信终端的授信终端信息
S201
对所述登录标识和所述授信终端信息进行存储
S202
接收当前登录终端发送的对终端应用的登录请求
S203
获取所述登录标识对应的预先存储的授信终端信息，并获取所述至少两个登录终端信息中各登录终端信息的信息类型
S204
基于所述各登录终端信息的信息类型，按照预设排列顺序对所述至少两个登录终端信息中各登录终端信息进行排列处理
S205
采用预设加密算法分别对排列处理后的所述各登录终端信息进行加密处理，以生成加密后的所述各登录终端信息
S206
采用加密后的所述各授信终端信息分别对加密后的所述各登录终端信息进行匹配处理以生成匹配结果
S207
当所述匹配结果满足预设验证条件时，确定所述登录终端为授信终端，并执行对所述终端应用的登录操作
S208
当所述匹配结果不满足预设验证条件时，向所述登录终端发送与所述终端应用相关联的登录验证请求
S209
接收所述登录终端发送的所述验证信息，对所述验证信息进行验证处理，并在验证处理通过后，执行对所述终端应用的登录操作
S210
对加密后的所述各登录终端信息进行封装以生成所述登录终端的终端标识，并对所述登录标识和所述终端标识进行存储
S211

图2

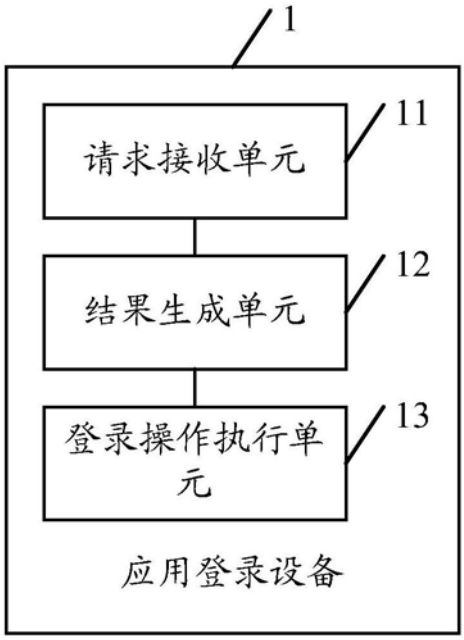


图3

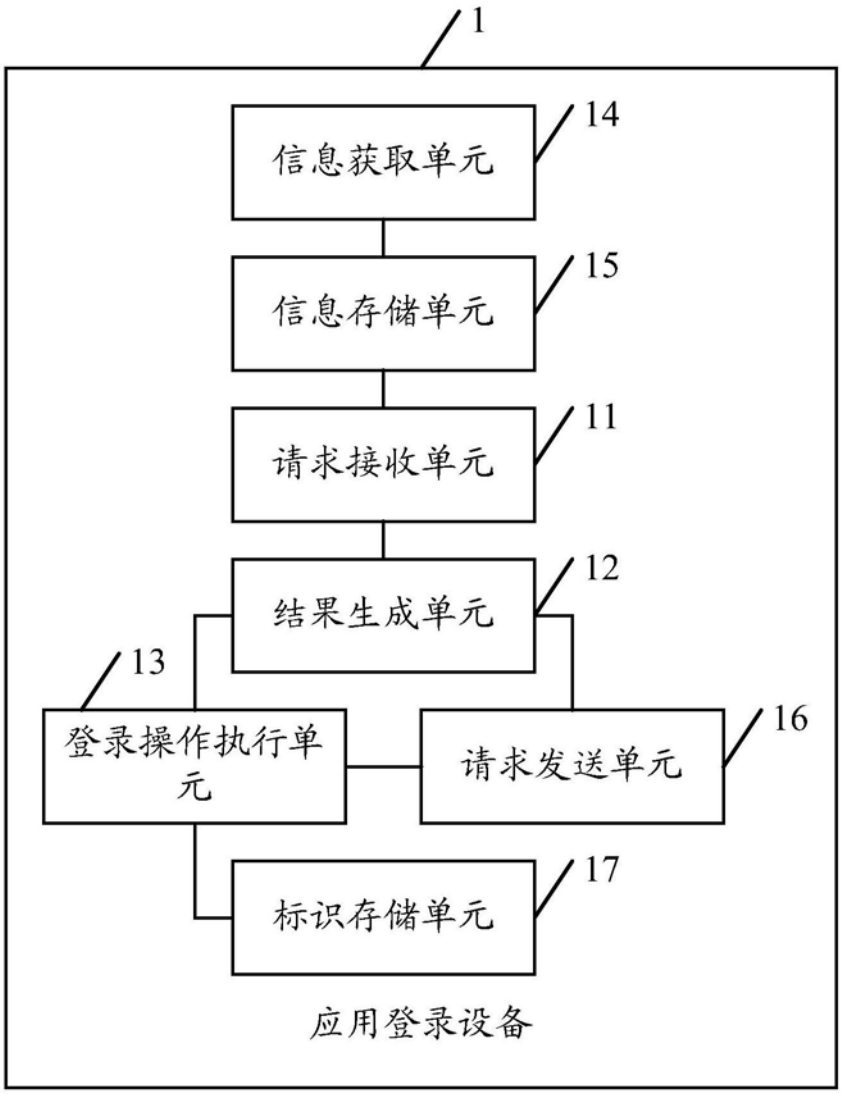

1
信息获取单元
14
信息存储单元
15
请求接收单元
11
结果生成单元
12
13
登录操作执行单元
请求发送单元
16
标识存储单元
17
应用登录设备

图4

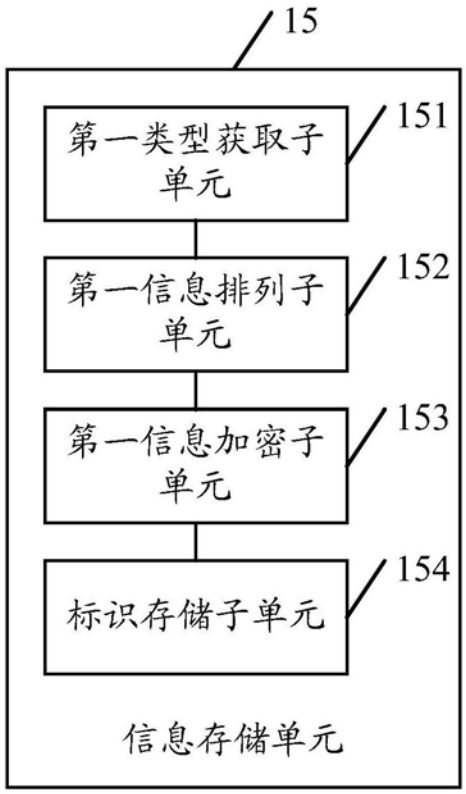

15
第一类型获取子单元
151
第一信息排列子单元
152
第一信息加密子单元
153
标识存储子单元
154
信息存储单元

图5

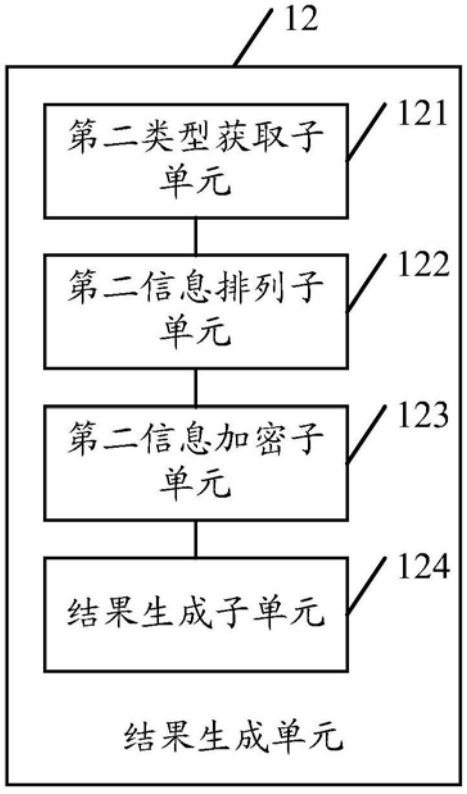

12
第二类型获取子单元
121
第二信息排列子单元
122
第二信息加密子单元
123
结果生成子单元
124
结果生成单元

图6

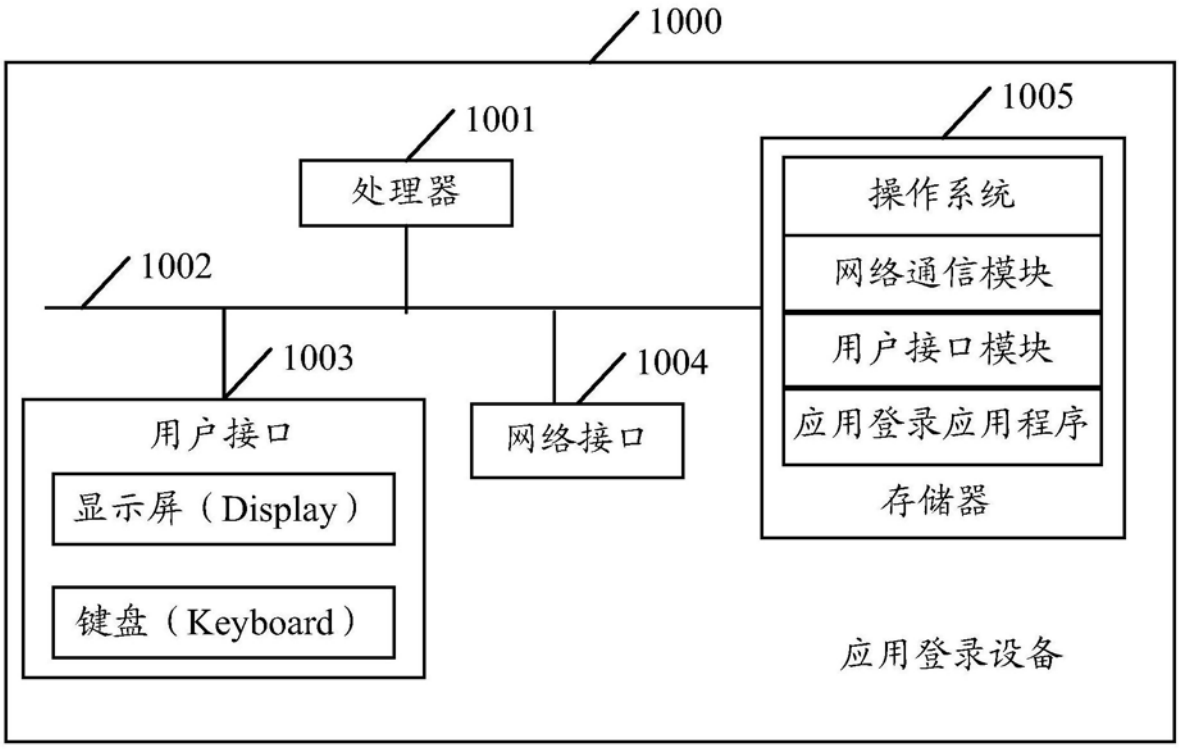

1000
1001
处理器
1002
1003
用户接口
显示屏（Display）
键盘（Keyboard）
1004
网络接口
1005
操作系统
网络通信模块
用户接口模块
应用登录应用程序
存储器
应用登录设备

图7