(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 111935709 B
(45)授权公告日 2021.02.05

(21)申请号 202011005942.0

(22)申请日 2020.09.23

(65)同一申请的已公布的文献号
申请公布号 CN 111935709 A

(43)申请公布日 2020.11.13

(73)专利权人 广州市玄武无线科技股份有限公司
地址 510000 广东省广州市天河区体育西路103号之一维多利广场B栋32层01单元房

(72)发明人 吴景行 杨梦飞 卢超 李海荣 陈永辉

(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 陈志明

(51)Int.Cl.
H04W 12/033(2021.01)
H04W 12/37(2021.01)
H04W 12/42(2021.01)
H04W 12/02(2009.01)

(56)对比文件
CN 103124269 A,2013.05.29
CN 103124269 A,2013.05.29
CN 108616360 A,2018.10.02
CN 109787991 A,2019.05.21
CN 110719590 A,2020.01.21
CN 105791262 A,2016.07.20
CN 111083694 A,2020.04.28
CN 110753033 A,2020.02.04
US 9356924 B1,2016.05.31

审查员 杨志忠

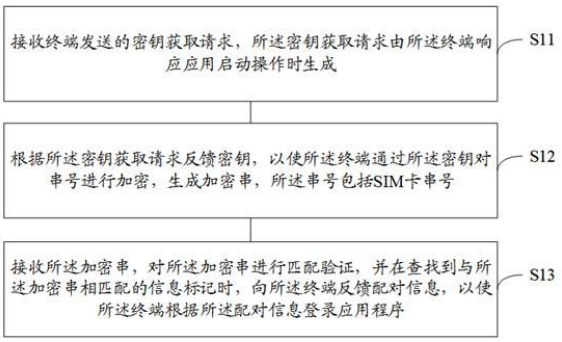
权利要求书2页 说明书11页 附图6页

(54)发明名称

终端的应用程序登录方法、装置及电子设备

(57)摘要

本申请公开了一种终端的应用程序登录方法、装置及电子设备，所述方法包括：接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成；根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号；接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，以使所述终端根据所述配对信息登录应用程序。本申请可以对SIM卡串号和密钥进行拼接加密，从而实现用户信息保密的效果，在出现攻击或数据入侵时，也可以避免用户的信息丢失，减少信息泄漏的风险。



CN 111935709 B

1.一种终端的应用程序登录方法,其特征在于,包括:

接收终端发送的密钥获取请求,所述密钥获取请求由所述终端响应应用启动操作时生成;

根据所述密钥获取请求反馈密钥,以使所述终端通过所述密钥对串号进行加密,生成加密串,所述串号包括SIM卡串号和终端串号;

接收所述加密串,对所述加密串进行匹配验证,并在查找到与所述加密串相匹配的信息标记时,向所述终端反馈配对信息,以使所述终端根据所述配对信息登录应用程序;其中,所述配对信息包括界面配置信息;所述向所述终端反馈配对信息,包括根据所述终端串号,获取所述终端信息;根据所述终端信息,查找对应的所述界面配置信息后,将所述界面配置信息反馈至所述终端,以使所述终端根据所述界面配置信息渲染所述终端的用户登录界面。

2.根据权利要求1所述的终端的应用程序登录方法,其特征在于,接收所述加密串,对所述加密串进行匹配验证,并在查找到与所述加密串相匹配的信息标记时,向所述终端反馈配对信息,包括:

接收所述加密串和所述终端当前连接的运营商信息;

根据所述运营商信息,从对应的运营商服务端获取信息标记集对所述加密串进行匹配验证,并当从所述信息标记集中查找到与所述加密串相匹配的信息标记时,向所述终端反馈配对信息。

3.根据权利要求1或2所述的终端的应用程序登录方法,其特征在于,所述配对信息包括配对码,所述向所述终端反馈配对信息,包括:

获取当前时间戳;

将所述当前时间戳与所述加密串进行字符串拼接,获取拼接串;

根据所述拼接串生成所述配对码后,向所述终端反馈所述配对码。

4.根据权利要求3所述的终端的应用程序登录方法,其特征在于,所述根据所述拼接串生成所述配对码,包括:

对所述拼接串进行加密压缩,生成带有压缩密码的所述配对码。

5.根据权利要求1或2所述的终端的应用程序登录方法,其特征在于,还包括:

在未查找到与所述加密串相匹配的信息标记时,向所述终端反馈生物识别请求;

在接收到所述终端根据所述生物识别请求发送的生物信息时,对所述生物信息进行匹配验证,并在查找到与所述生物信息相匹配的生物图像时,向所述终端反馈对应的登录信息,以使所述终端根据所述登录信息登录应用程序。

6.一种终端的应用程序登录装置,其特征在于,包括:

请求接收模块,用于接收终端发送的密钥获取请求,所述密钥获取请求由所述终端响应应用启动操作时生成;

信息加密模块,用于根据所述密钥获取请求反馈密钥,以使所述终端通过所述密钥对串号进行加密,生成加密串,所述串号包括SIM卡串号和终端串号;

信息验证模块,用于接收所述加密串,对所述加密串进行匹配验证,并在查找到与所述加密串相匹配的信息标记时,向所述终端反馈配对信息,以使所述终端根据所述配对信息登录应用程序;其中,所述配对信息包括界面配置信息;所述信息验证模块具体用于,根据

所述终端串号，获取所述终端信息；根据所述终端信息，查找对应的所述界面配置信息后，将所述界面配置信息反馈至所述终端，以使所述终端根据所述界面配置信息渲染所述终端的用户登录界面。

7.根据权利要求6所述终端的应用程序登录装置，其特征在于，所述信息验证模块具体用于：

接收所述加密串和所述终端当前连接的运营商信息；

根据所述运营商信息，从对应的运营商服务端获取信息标记集对所述加密串进行匹配验证，并当从所述信息标记集中查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息。

8.一种电子设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1至5中任一项所述的终端的应用程序登录方法。

终端的应用程序登录方法、装置及电子设备

技术领域

[0001] 本申请涉及通讯技术领域，尤其涉及一种终端的应用程序登录方法、装置及电子设备。

背景技术

[0002] 随着互联网技术的飞速发展，各种不同类型、不同功能的应用程序(Application，App)已经成为了大众日常生活中不可或缺的一部分。用户在首次登录这些应用程序时，通常需要利用手机号获取验证码进行登录。而由于手机号是用户的私人账号，一旦终端或应用程序被恶意攻击或入侵时，容易泄露用户信息。为了避免用户信息泄露，现有的登录方式是，服务器预先采用用户的身份信息生成对应的登录编码，在登录时终端根据登录编码进行登录。

[0003] 但在采用现有技术进行登录时，发现由于生成登录编码的过程中需提取用户的身份信息，若上述过程出现攻击或入侵时，依然会存在用户信息的丢失或泄漏的情况，留下了信息安全的隐患，增加了信息泄漏的风险。

发明内容

[0004] 本申请实施例所要解决的技术问题在于，解决在生成登录编码时需提取用户的身份信息，容易出现用户信息丢失和泄漏的问题，提高用户登录时的安全性。

[0005] 为解决上述问题，本申请实施例提供一种终端的应用程序登录方法，适于在计算装置中执行，至少包括如下步骤：接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成；

[0006] 根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号；

[0007] 接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，以使所述终端根据所述配对信息登录应用程序。

[0008] 进一步的，接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，包括：

[0009] 接收所述加密串和所述终端当前连接的运营商信息；

[0010] 根据所述运营商信息，从对应的运营商服务端获取信息标记集对所述加密串进行匹配验证，并当从所述信息标记集中查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息。

[0011] 进一步的，所述配对信息包括配对码，所述向所述终端反馈配对信息，包括：

[0012] 获取当前时间戳；

[0013] 将所述当前时间戳与所述加密串进行字符串拼接，获取拼接串；

[0014] 根据所述拼接串生成所述配对码后，向所述终端反馈所述配对码。

[0015] 进一步的，所述根据所述拼接串生成所述配对码，包括：

[0016] 对所述拼接串进行加密压缩，生成带有压缩密码的所述配对码。

[0017] 进一步的，所述串号还包括终端串号。

[0018] 进一步的，所述配对信息包括界面配置信息；

[0019] 所述向所述终端反馈配对信息，包括：

[0020] 根据所述终端串号，获取所述终端信息；

[0021] 根据所述终端信息，查找对应的所述界面配置信息后，将所述界面配置信息反馈至所述终端，以使所述终端根据所述界面配置信息渲染所述终端的用户登录界面。

[0022] 进一步的，所述方法还包括：

[0023] 在未查找到与所述加密串相匹配的信息标记时，向所述终端反馈生物识别请求；

[0024] 在接收到所述终端根据所述生物识别请求发送的生物信息时，对所述生物信息进行匹配验证，并在查找到与所述生物信息相匹配的生物图像时，向所述终端反馈对应的登录信息，以使所述终端根据所述登录信息登录应用程序。

[0025] 进一步的，本申请实施例还提供了一种终端的应用程序登录装置，包括：

[0026] 请求接收模块，用于接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成；

[0027] 信息加密模块，用于根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号；

[0028] 信息验证模块，用于接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，以使所述终端根据所述配对信息登录应用程序。

[0029] 进一步的，所述信息验证模块具体用于：

[0030] 接收所述加密串和所述终端当前连接的运营商信息；

[0031] 根据所述运营商信息，从对应的运营商服务端获取信息标记集对所述加密串进行匹配验证，并当从所述信息标记集中查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息。

[0032] 进一步的，所述配对信息包括配对码，所述信息验证模块具体用于：

[0033] 获取当前时间戳；

[0034] 将所述当前时间戳与所述加密串进行字符串拼接，获取拼接串；

[0035] 根据所述拼接串生成所述配对码后，向所述终端反馈所述配对码。

[0036] 进一步的，所述信息验证模块具体用于：

[0037] 对所述拼接串进行加密压缩，生成带有压缩密码的所述配对码。

[0038] 进一步的，所述串号还包括终端串号。

[0039] 进一步的，所述配对信息包括界面配置信息；

[0040] 所述信息验证模块具体用于：

[0041] 根据所述终端串号，获取所述终端信息；

[0042] 根据所述终端信息，查找对应的所述界面配置信息后，将所述界面配置信息反馈至所述终端，以使所述终端根据所述界面配置信息渲染所述终端的用户登录界面。

[0043] 进一步的，所述装置还包括：

[0044] 生物识别请求模块，用于在未查找到与所述加密串相匹配的信息标记时，向所述

终端反馈生物识别请求；

[0045] 生物信息验证模块，用于在接收到所述终端根据所述生物识别请求发送的生物信息时，对所述生物信息进行匹配验证，并在查找到与所述生物信息相匹配的生物图像时，向所述终端反馈对应的登录信息，以使所述终端根据所述登录信息登录应用程序。

[0046] 进一步的，本申请实施例提供一种电子设备，包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如上述实施例所述的终端的应用程序登录方法。

[0047] 进一步的，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行如上述实施例所述的终端的应用程序登录方法。

[0048] 与现有技术相比，本实施例通过服务器在终端响应用户的启动操作后向终端发送密钥，使得终端可以通过密钥对串号进行加密生成加密串，接着服务器可以对加密串进行匹配验证，并在查找到与加密串匹配的信息标记时，向终端反馈配对信息，使得终端可以根据配对信息登录应用程序。由终端对SIM卡串号和密钥进行拼接加密，可以实现用户信息保密的效果，即使出现攻击或数据入侵，也可以避免用户的信息丢失，减少信息泄漏的风险；同时服务器可以对加密串作匹配认证，并在认证通过后向终端反馈配对信息，使终端可以根据配对信息登录应用程序，实现应用程序的快速登录。

附图说明

[0049] 图1是一个实施例中终端的应用程序登录方法的应用环境图；

[0050] 图2是一个实施例中终端的应用程序登录方法的流程示意图；

[0051] 图3是一个实施例中终端的应用程序登录方法的流程示意图；

[0052] 图4是一个实施例中终端的应用程序登录方法的流程示意图；

[0053] 图5是一个实施例中终端的应用程序登录方法的流程示意图；

[0054] 图6是一个实施例中终端的应用程序登录方法的流程示意图；

[0055] 图7是一个实施例中终端的应用程序登录方法的流程示意图；

[0056] 图8是一个实施例中终端的应用程序登录装置的结构框图；

[0057] 图9是一个实施例中终端的应用程序登录装置的结构框图。

具体实施方式

[0058] 下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

[0059] 现有的应用程序登录通常需要利用手机号获取验证码。但由于手机号是用户的私人账号，一旦终端或应用程序被恶意攻击或入侵时，容易泄露用户信息。为了避免用户信息泄露，现有的登录方式是，服务器预先采用用户的身份信息生成对应的登录编码，在登录时终端根据登录编码进行登录。但在采用现有技术进行登录时，发现由于生成登录编码的过程中需提取用户的身份信息，若上述过程出现攻击或入侵时，依然会存在用户信息的丢失

或泄漏的情况，留下了信息安全的隐患，增加了信息泄漏的风险。

[0060] 为解决上述问题，下面将通过以下几个具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0061] 如图1所示，是一个实施例中终端的应用程序登录方法的应用环境图，参照图1，该终端的应用程序登录方法涉及终端110和服务器120。其中第一终端110与服务器120可以通过网络连接。第一终端110具体可以是台式终端或移动终端，移动终端具体可以手机、平板电脑、笔记本电脑等中的至少一种。服务器120可以用独立的服务器120，或者是多个服务器120组成的服务器120集群来实现。

[0062] 如图2所示，在一个实施例中，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0063] 参照图2，该终端的应用程序登录方法具体包括如下步骤：

[0064] S11、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0065] 在本申请实施例中，当用户需要使用终端的应用程序时，用户可以点击或扫动终端的屏幕时，可以触发终端启动应用程序。终端在启动应用程序的同时可以触发生成密钥获取请求，并将密钥获取请求发送至服务器中。

[0066] S12、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0067] 在本申请实施例中，服务器在接收密钥获取请求时，可以响应密钥获取请求生成密钥。该密钥可以是一种参数，可以在明文转换为密文或将密文转换为明文的算法中输入的参数。在可选的实施例中，该密钥可以是对称密钥也可以是非对称密钥。服务器在生成密钥时，可以对密钥进行加密，也可以对密钥不加密。该SIM卡串号可以是用户的手机号。

[0068] 当终端接收到服务器发送的密钥时，终端可以获取用户的SIM卡串号以及SIM卡串号对应的运营商信息，该运营商信息可以是SIM卡账号所在的运营商的通信编号，也可以SIM卡账号所在的运营商对应的网络识别号或运营商代码等等。接着终端可以将SIM卡串号、运营商信息与密钥进行拼接，生成加密串。通过密钥与SIM卡串号和运营商信息进行拼接，实现对SIM卡串号的加密。从而避免了在服务器与终端在通信过程中，因数据入侵或黑客攻击而导致用户信息泄漏的情况。

[0069] 在一可选的实施例中，拼接的方式可以使SIM卡串号+运营商信息+密钥，或者密钥+SIM卡串号+运营商信息，或者运营商信息+SIM卡串号+密钥，或者密钥号+运营商信息+SIM卡串等等，拼接的具体方式可以根据实际需要进行调整，在本申请实施例中对拼接的具体方式不作具体限定。

[0070] 在本实施例中，终端通过获取服务器发送的密钥对SIM卡串号进行加密，可以提高用户信息的隐私度，减少信息被盗取的风险。

[0071] S13、接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，向终端反馈配对信息，以使终端根据配对信息登录应用程序。

[0072] 在本申请实施例中，该信息标记可以是用户在先注册时，服务器生成并存储的与用户账号对应的标记，该配对信息可以是用户登录应用程序所需的配对码、验证码和用户在应用程序中所配置的各种信息，该配对信息可以与信息标记对应，从而可以通过信息标

记与用户SIM卡串号对应。用户在注册时，服务器可以在接收用户的SIM卡串号后生成对应的信息标记，并将信息标记存储在预置数据库中。当终端发送加密串时，服务器可以从预置的数据库中提取信息标记。

[0073] 终端在生成加密串后，可以发送至服务器，服务器可以对加密串进行匹配验证。通过匹配验证可以确定该终端对应的SIM卡串号是否已经在服务器中注册，实现快速登录认证。

[0074] 在本实施例中，服务器可以向终端发送的密钥，由终端对SIM卡串号和密钥进行拼接加密，并在加密后发送至服务器，实现用户信息保密的效果，即使在传输过程中出现攻击或数据入侵，也可以避免用户的信息丢失，从而减少了信息泄漏的风险，确保用户信息安全；同时服务器可以对加密串作匹配认证，在认证通过后向终端反馈配对信息，使终端可以根据配对信息登录应用程序，实现应用程序的快速登录。

[0075] 在现有技术中，由于用户使用的SIM卡账号不同，SIM卡账号对应的运营商也不同，当服务器需要对不同运营商的用户SIM卡账号进行验证时，难以快速确定SIM卡所属运营商，服务器需遍历运营商服务端进行验证，使得验证时间长，验证效率差。

[0076] 为了解决上述问题，下面将通过以下具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0077] 如图3所示，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0078] 参照图3，该终端的应用程序登录方法具体包括如下步骤：

[0079] S21、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0080] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0081] S22、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0082] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0083] S23、接收加密串和终端当前连接的运营商信息。

[0084] 在本实施例中，运营商信息可以是SIM卡账号所在的运营商的通信编号，或SIM卡账号所在的运营商对应的网络识别号或运营商代码等等。终端在获取SIM卡串号的同时可以获取运营商信息。可选地，终端可以在对SIM卡串号进行加密生成加密串后，再同时将得到加密串和运营商信息发送至服务器；也可以先发送加密串，再发送运营商信息，或者先发送运营商信息，再发送加密串。具体可以根据实际需要进行选择。

[0085] S24、根据运营商信息，从对应的运营商服务端获取信息标记集对加密串进行匹配验证，并当从信息标记集中查找到与加密串相匹配的信息标记时，向终端反馈配对信息，以使终端根据配对信息登录应用程序。

[0086] 在本实施例中，信息标记集可以是运营商对应的SIM卡串号的集合，例如可以是133开头的手机号码集合，或者是189开头的手机串号的集合。该配对信息可以是用户登录应用程序所需的配对码、验证码和用户在应用程序中所配置的各种信息。该信息标记可以

是信息标记集中与SIM卡串号相同的串号。

[0087] 服务器在接收终端发送的运营商信息后，可以根据运营商信息进行识别，确定加密串中的SIM卡串号所对应的运营商，从而可以向对应的运营商服务端发送获取信息标记集的请求。运营商服务器可以响应该获取信息标记集的请求向服务器发送信息标记集。服务器可以从加密串中获取对应的SIM卡串号，从信息标记集中查找与SIM卡串号对应的信息标记。当查找到信息标记时，服务器可以向终端发送配对信息，终端可以采用配对信息登录应用程序。

[0088] 在本实施例中，终端可以向服务器发送运营商信息，使得服务器可以通过运营商信息快速查找到与终端的SIM卡串号对应的运营商，从而无需让服务器从多个不同的运营商中进行验证操作，缩短了服务器的验证时间，提高了验证效率。

[0089] 在现有技术中，若遭受入侵或攻击，终端采用的密钥还是会有被破解可能性，若密钥被破解，加密串中的SIM卡串号也会有机会泄漏，存在信息泄漏的风险。而且设置配对信息的可用时长需重新发送配对信息至终端，可能造成设置的时长与发送的配对信息不对应的情况。

[0090] 下面将通过以下具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0091] 如图4所示，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0092] 参照图4，该终端的应用程序登录方法具体包括如下步骤：

[0093] S31、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0094] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0095] S32、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0096] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0097] S33、接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，获取当前时间戳。

[0098] 该当前时间戳可以是一份能够表示一份数据在一个特定时间点已经存在的完整的可验证的数据。服务器可以使用预设的数字签名技术产生当前时间戳，当前时间戳可以包括原始文件信息、签名参数、签名时间等信息。

[0099] S34、将当前时间戳与加密串进行字符串拼接，获取拼接串。

[0100] 在获取当前时间戳后，服务器可以将当前时间戳与终端发送的加密串进行字符串拼接，生成新的拼接串。通过将当前时间戳与加密串进行字符串拼接，可以进一步对加密串进行加密，减少信息泄漏的风险，增加信息的安全隐秘性。

[0101] 在一实施例中，该配对信息包括配对码，该配对码可以是数字密码，也可以图像密码。

[0102] S35、根据拼接串生成配对码后，向终端反馈配对码，以使终端根据配对信息登录

应用程序。

[0103] 在本实施例中，服务器在生成拼接串后，可以按照用户预设的数据转换格式将拼接串转换生成配对码。例如，可以按照用户预设的图像转换格式将拼接串转换生成二维码图像的配对码；也可以按照用户预设的数字转换格式将拼接串转换生成一个或多个的一连串的数字码。

[0104] 而终端可以根据配对码登录应用程序，例如，配对码为二维码图像，终端可以通过扫描二维码图像，登录应用程序。例如，配对码为数字码，终端可以分别将数字码添加至登录页面完成登录。

[0105] 在本实施例中，服务器可以获取当前时间戳，利用当前时间戳对加密串进行二次加密，可以有效增加配对码的安全性，可以避免因密钥被破解而导致加密串中的SIM卡串号泄漏的情况，降低了信息泄漏的风险。而且每次配对时都由服务器获取当前时间戳，可以对配对信息的产生时间进行认证，从而可以避免配对信息被篡改。

[0106] 在现有技术中，若配对码的字符串过长，会增加服务器与终端之间的传输时间，降低传输效率，而且配对码的字符串过长，用户需要填写登录至应用程序时，也不方便用户记忆。

[0107] 为了解决上述问题，下面将通过以下具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0108] 如图5所示，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0109] 参照图5，该终端的应用程序登录方法具体包括如下步骤：

[0110] S41、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0111] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0112] S42、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0113] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0114] S43、接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，获取当前时间戳。

[0115] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0116] S44、将当前时间戳与加密串进行字符串拼接，获取拼接串。

[0117] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0118] S45、对拼接串进行加密压缩，生成带有压缩密码的配对码，向终端反馈配对码，以使终端根据配对信息登录应用程序。

[0119] 在本实施例中，服务器可以使用用户预设的算法(例如zip算法)压缩拼接串，在压缩的同时设置压缩密码，最后生成压缩串，以压缩串为配对码。

[0120] 在本实施例中，通过设置压缩密码压缩拼接串生成的配对码，即隐含了加密串和配对码的有效时间，又利用压缩算法压缩了长度；同时，设置压缩密码又避免他人直接通过压缩算法解压，从而避免了修改有效时间的情况。

[0121] 由于终端的型号越来越多，不同的终端可能运行不同的操作系统，而不同的操作系统在登录相同的应用程序时会有不同的变化，但在现有技术中，现有的登录界面面对不同的用户群体均是相同的，无法满足不同用户的登录界面需求。

[0122] 为了解决上述问题，下面将通过以下具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0123] 如图6所示，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0124] 参照图6，该终端的应用程序登录方法具体包括如下步骤：

[0125] S51、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0126] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0127] S52、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0128] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0129] S53、接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，根据终端串号，获取终端信息。

[0130] 在一实施例中，串号还可以包括终端串号。该终端串号可以是终端的型号，或终端的操作版本信号，或终端的制造商型号等等。例如，终端是华为荣耀10x，该终端串号可以是10x。又例如，终端为iPhone 6splus，该终端串号可以是6sp。又例如该终端是三星Galaxy Note20 / 20 Ultra 5G，采用安卓10.0系统，该终端串号可以是10.0等等。该终端信息可以是用户在应用程序中的配置信息、用户在应用程序中绑定的对象信息，例如绑定了企业或应用程序中不同的账号，而不同的企业和不同的账号可以对应不同的登录界面。

[0131] 终端在生成加密串时，可以采用密钥与SIM卡串号和终端串号一起拼接加密生成加密串。当服务器通过信息标记集合中查找到与加密串匹配的信息标记时，服务器可以从加密串中获取终端串号，并从终端串号中获取对应的终端信息。

[0132] S54、根据终端信息，查找对应的界面配置信息后，将界面配置信息反馈至终端，以使终端根据界面配置信息渲染终端的用户登录界面和登录应用程序。

[0133] 在一实施例中，该配对信息可以包括界面配置信息，该界面配置信息可以使应用程序登录页面的配置信息，可以包括登录所需的渲染颜色、图案、图片、动态图画、界面和标记等等。

[0134] 服务器可以通过终端信息查找用户在应用程序中的配置信息和用户在应用程序中绑定的对象信息等等，通过用户在应用程序中的配置信息和用户在应用程序中绑定的对象信息可以查找到登录所需的渲染颜色、图案、图片、动态图画、界面和标记。服务器可以将登录所需的渲染颜色、图案、图片、动态图画、界面和标记等打包成界面配置信息，再将界面

配置信息发送至终端，终端可以根据界面配置信息在屏幕中显示中对应的渲染颜色、图案、图片、动态图画、界面和标记等。同时服务器也可以将登陆所需的配对信息与界面配置信息一并发送至终端，终端可以根据配对信息登录应用程序。

[0135] 在本实施例中，服务器可以通过终端串号确定终端信息，进而可以根据终端信息确定当前使用终端的用户在登录时所需要的界面配置信息，从而可以向不同的用户显示不同登录页面或登录颜色等，也可以根据不同的终端信号或操作系统版本好显示不同的登录界面，以满足不同用户的登录界面需求。

[0136] 由于现有的SIM卡运营商越来越多，不同的运营商会有不同的SIM卡认证方式，若将不同的运营商的认证方式存储在服务器上，再由服务器执行认证，会加大服务器的操作负担，而且若要对非三大运营商的用户进行SIM卡认证时，需要额外设置工具包或软件包进行认证，一旦有一个需要升级或修改，就需要整个工具包或软件包进行修改，大大增加了操作难度，难以满足不同用户的登录需求。

[0137] 为了解决上述问题，下面将通过以下具体的实施例对本申请实施例提供的终端的应用程序登录方法进行详细介绍和说明。

[0138] 如图7所示，提供了一种终端的应用程序登录方法，本实施例主要以该方法应用于服务器来举例说明。该服务器具体可以是上述图1中的服务器120。

[0139] 参照图7，该终端的应用程序登录方法具体包括如下步骤：

[0140] S61、接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成。

[0141] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0142] S62、根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号。

[0143] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0144] S63、接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，向终端反馈配对信息，以使终端根据配对信息登录应用程序。

[0145] 此步骤与上述实施例相同，具体解析可以参照上述实施例，为了避免重复，在此不再赘述。

[0146] S64、在未查找到与加密串相匹配的信息标记时，向终端反馈生物识别请求。

[0147] 在本实施例中，服务器可以分别存储三大运营商的运营商标记，将三大运营商的运营商标记集合生成信息标记集合，在接收终端发送的加密串时，服务器可以从信息标记集合中查找与加密串对应的信息标记。当服务器无法从信息标记集合中查找与加密串对应的信息标记时，可以确定加密串对应的SIM卡账号并不是三大运营商的账号。服务器可以生成生物识别请求，并将生物识别请求发送至终端。

[0148] 终端可以在获取生物识别请求后，获取当前使用终端的用户的生物信息。该生物信息可以是当前用户的图像信息或指纹信息。

[0149] 具体地，终端可以在屏幕中显示获取操作提示，提示用户按照指示执行对应的操作。例如，终端可以开启摄像头拍摄当前用户的脸部图像。又例如终端可以记录当前用户的

指纹图像。

[0150] S65、在接收到终端根据生物识别请求发送的生物信息时，对生物信息进行匹配验证，并在查找到与生物信息相匹配的生物图像时，向终端反馈对应的登录信息，以使终端根据登录信息登录应用程序。

[0151] 在本实施例中，当用户SIM卡账号未非三大运营商的账号时，在用户注册时，终端可以获取用户的生物信息并发送至服务器，服务器可以记录用户注册时的生物信息。当用户需要登录时，服务器可以在接收终端发送的终端当前使用用户的生物信息后，从终端当前使用用户的生物信息提取生物特征，然后将生物特征与存储的多个用户注册时上传的生物信息作匹配验证，当服务器可以根据生物特征从多个用户注册时上传的生物信息中匹配到对应的生物图像时，服务器可以确定该终端的当前使用用户已注册，并将终端的当前使用用户对应的登录信息，从而让终端可以根据登录信息登录应用程序。

[0152] 本实施例通过服务器在用户注册时预先存储用户的生物信息，即使用户使用的SIM卡账号非三大运营商账号或非特定运营商账号，服务器也可以通过生物信息进行验证判断，从而可以简化服务器的验证操作，提高验证效率，而且由于服务器可以对不同运营商的用户进行验证，也可以吸纳不同运营商的用户使用该应用程序，从而拓宽应用程序的使用群体，进一步提高了实用性。

[0153] 在一个实施例中，如图8所示，提供了一种终端的应用程序登录装置，包括：

[0154] 请求接收模块801，用于接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成；

[0155] 信息加密模块802，用于根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号；

[0156] 信息验证模块803，用于接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，以使所述终端根据所述配对信息登录应用程序。

[0157] 在一实施例中，所述信息验证模块具体用于：接收所述加密串和所述终端当前连接的运营商信息；根据所述运营商信息，从对应的运营商服务端获取信息标记集对所述加密串进行匹配验证，并当从所述信息标记集中查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息。

[0158] 在一实施例中，所述配对信息包括配对码，所述信息验证模块具体用于：获取当前时间戳；将所述当前时间戳与所述加密串进行字符串拼接，获取拼接串；根据所述拼接串生成所述配对码后，向所述终端反馈所述配对码。

[0159] 在一实施例中，所述信息验证模块具体用于：对所述拼接串进行加密压缩，生成带有压缩密码的所述配对码。

[0160] 在一实施例中，所述串号还包括终端串号；所述配对信息包括界面配置信息；所述信息验证模块具体用于：根据所述终端串号，获取所述终端信息；

[0161] 根据所述终端信息，查找对应的所述界面配置信息后，将所述界面配置信息反馈至所述终端，以使所述终端根据所述界面配置信息渲染所述终端的用户登录界面。

[0162] 在一个实施例中，如图9所示，提供了一种终端的应用程序登录装置，包括：

[0163] 请求接收模块901，用于接收终端发送的密钥获取请求，所述密钥获取请求由所述

终端响应应用启动操作时生成。

[0164] 信息加密模块902,用于根据所述密钥获取请求反馈密钥,以使所述终端通过所述密钥对串号进行加密,生成加密串,所述串号包括SIM卡串号。

[0165] 信息验证模块903,用于接收所述加密串,对所述加密串进行匹配验证,并在查找到与所述加密串相匹配的信息标记时,向所述终端反馈配对信息,以使所述终端根据所述配对信息登录应用程序。

[0166] 生物识别请求模块904,用于在未查找到与所述加密串相匹配的信息标记时,向所述终端反馈生物识别请求。

[0167] 生物信息验证模块905,用于在接收到所述终端根据所述生物识别请求发送的生物信息时,对所述生物信息进行匹配验证,并在查找到与所述生物信息相匹配的生物图像时,向所述终端反馈对应的登录信息,以使所述终端根据所述登录信息登录应用程序。

[0168] 在一个实施例中,提供了一种电子设备,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时执行上述终端的应用程序登录方法的步骤。此处终端的应用程序登录方法的步骤可以是上述各个实施例的终端的应用程序登录方法中的步骤。

[0169] 在一个实施例中,提供了一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可执行指令,所述计算机可执行指令用于使计算机执行上述终端的应用程序登录方法的步骤。此处终端的应用程序登录方法的步骤可以是上述各个实施例的终端的应用程序登录方法中的步骤。

[0170] 以上所述是本申请的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本申请原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也视为本申请的保护范围。

[0171] 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。

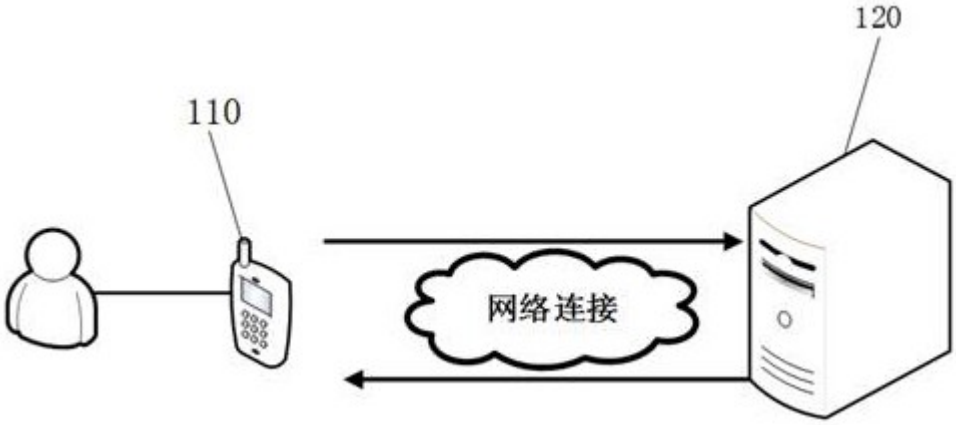

120
110
网络连接

图1

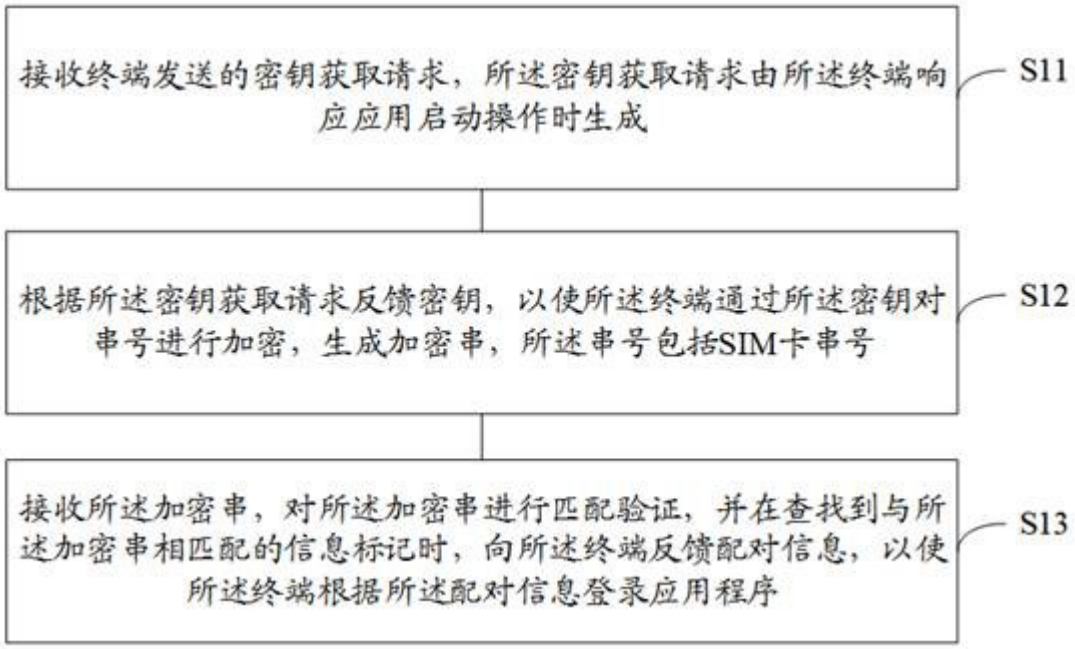

接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成
S11
根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号
S12
接收所述加密串，对所述加密串进行匹配验证，并在查找到与所述加密串相匹配的信息标记时，向所述终端反馈配对信息，以使所述终端根据所述配对信息登录应用程序
S13

图2

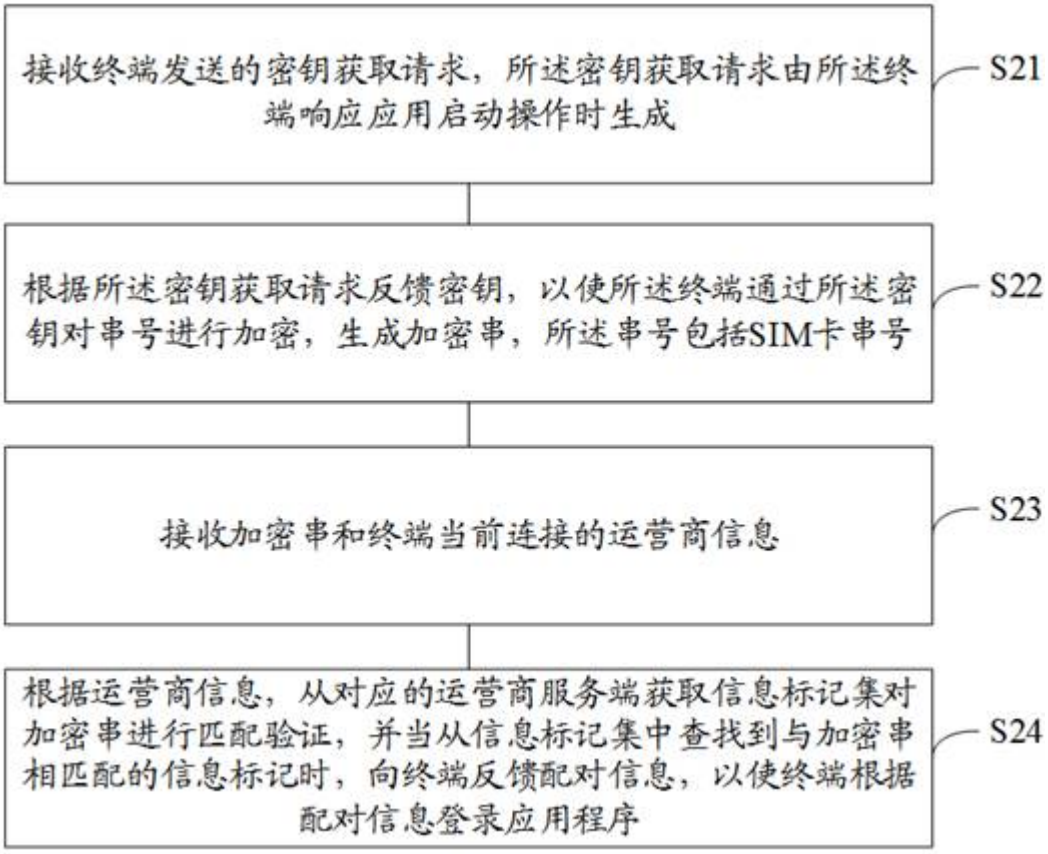

接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成
S21
根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号
S22
接收加密串和终端当前连接的运营商信息
S23
根据运营商信息，从对应的运营商服务端获取信息标记集对加密串进行匹配验证，并当从信息标记集中查找到与加密串相匹配的信息标记时，向终端反馈配对信息，以使终端根据配对信息登录应用程序
S24

图3

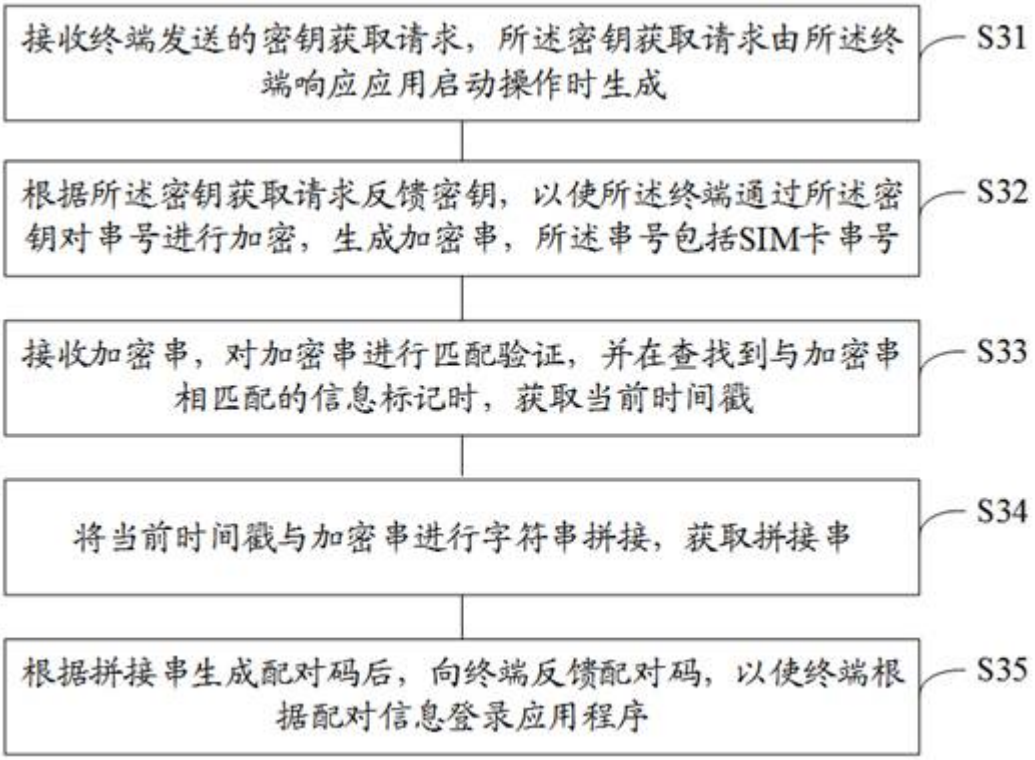

接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成
S31
根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号
S32
接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，获取当前时间戳
S33
将当前时间戳与加密串进行字符串拼接，获取拼接串
S34
根据拼接串生成配对码后，向终端反馈配对码，以使终端根据配对信息登录应用程序
S35

图4

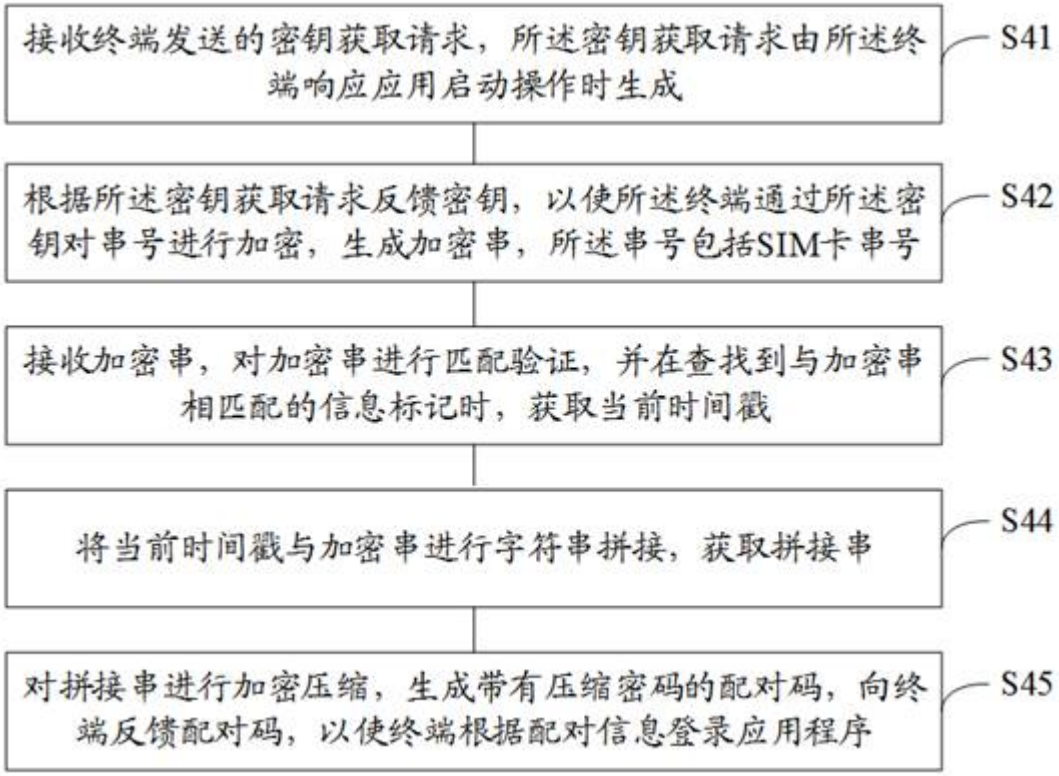

接收终端发送的密钥获取请求，所述密钥获取请求由所述终端响应应用启动操作时生成
S41
根据所述密钥获取请求反馈密钥，以使所述终端通过所述密钥对串号进行加密，生成加密串，所述串号包括SIM卡串号
S42
接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，获取当前时间戳
S43
将当前时间戳与加密串进行字符串拼接，获取拼接串
S44
对拼接串进行加密压缩，生成带有压缩密码的配对码，向终端反馈配对码，以使终端根据配对信息登录应用程序
S45

图5

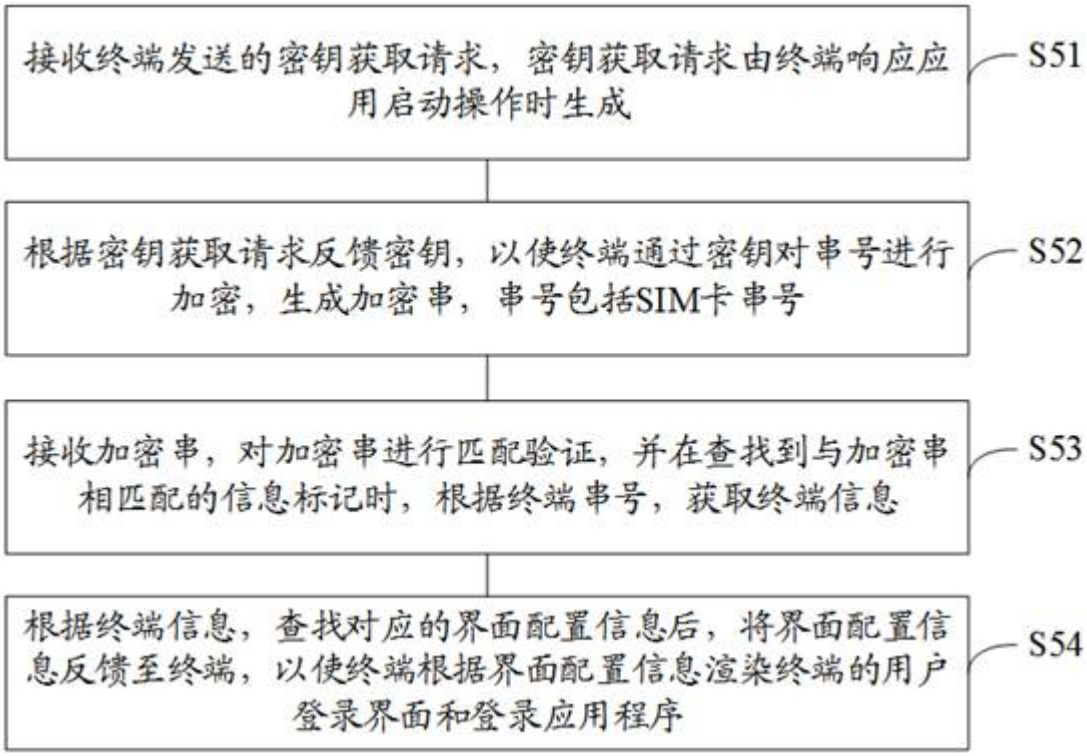

接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成
S51
根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号
S52
接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，根据终端串号，获取终端信息
S53
根据终端信息，查找对应的界面配置信息后，将界面配置信息反馈至终端，以使终端根据界面配置信息渲染终端的用户登录界面和登录应用程序
S54

图6

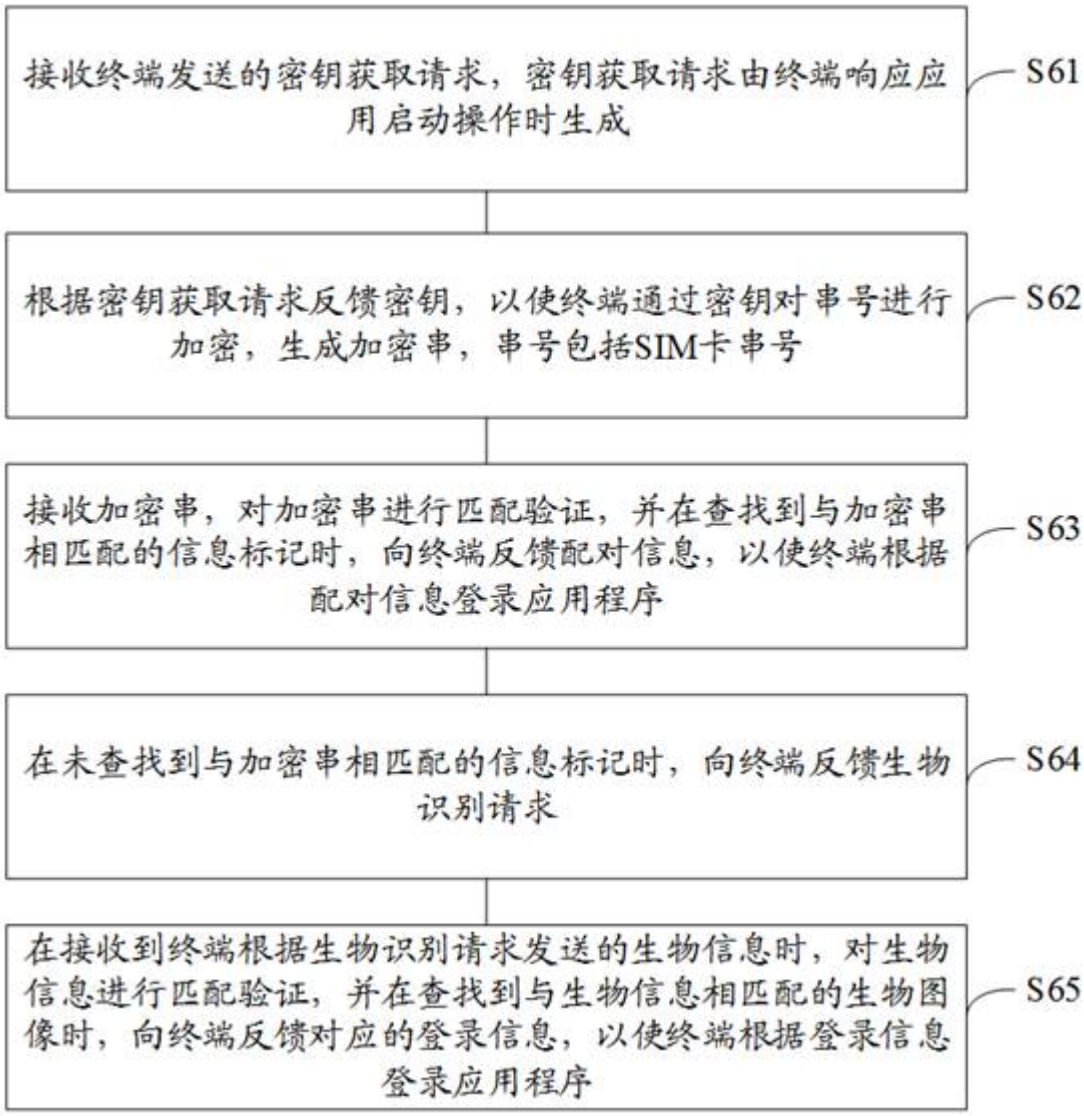

接收终端发送的密钥获取请求，密钥获取请求由终端响应应用启动操作时生成
S61
根据密钥获取请求反馈密钥，以使终端通过密钥对串号进行加密，生成加密串，串号包括SIM卡串号
S62
接收加密串，对加密串进行匹配验证，并在查找到与加密串相匹配的信息标记时，向终端反馈配对信息，以使终端根据配对信息登录应用程序
S63
在未查找到与加密串相匹配的信息标记时，向终端反馈生物识别请求
S64
在接收到终端根据生物识别请求发送的生物信息时，对生物信息进行匹配验证，并在查找到与生物信息相匹配的生物图像时，向终端反馈对应的登录信息，以使终端根据登录信息登录应用程序
S65

图7

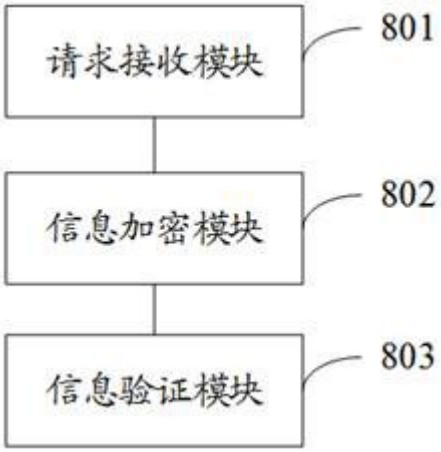

请求接收模块
801
信息加密模块
802
信息验证模块
803

图8

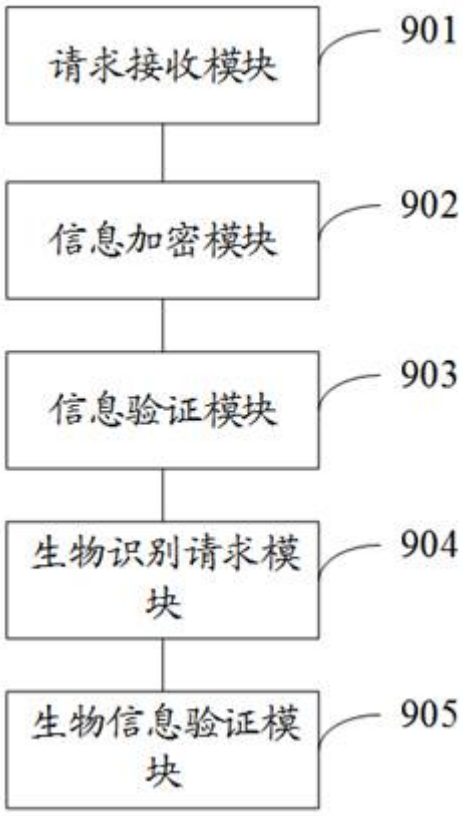


图9