

(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
2020 年 9 月 24 日 (24.09.2020)



(10) 国际公布号
WO 2020/186802 A1

(51) 国际专利分类号:
G06F 8/60 (2018.01) **G06F 8/65** (2018.01)

(21) 国际申请号: PCT/CN2019/119957

(22) 国际申请日: 2019 年 11 月 21 日 (21.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910209166.7 2019 年 3 月 19 日 (19.03.2019) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。

(72) 发明人: 陈志辉(CHEN, Zhihui); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518000 (CN)。

(74) 代理人: 深圳众鼎专利商标代理事务所(普通合伙)(SHENZHEN ZHONGDING INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市龙岗区龙城街道中心城清林路 546 号城投商务中心 4 层/B, Guangdong 518172 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) **Title:** VERSION UPDATE PACKAGE RELEASE METHOD AND APPARATUS, COMPUTER DEVICE AND STORAGE MEDIUM

(54) 发明名称: 版本更新包的发布方法、装置、计算机设备及存储介质

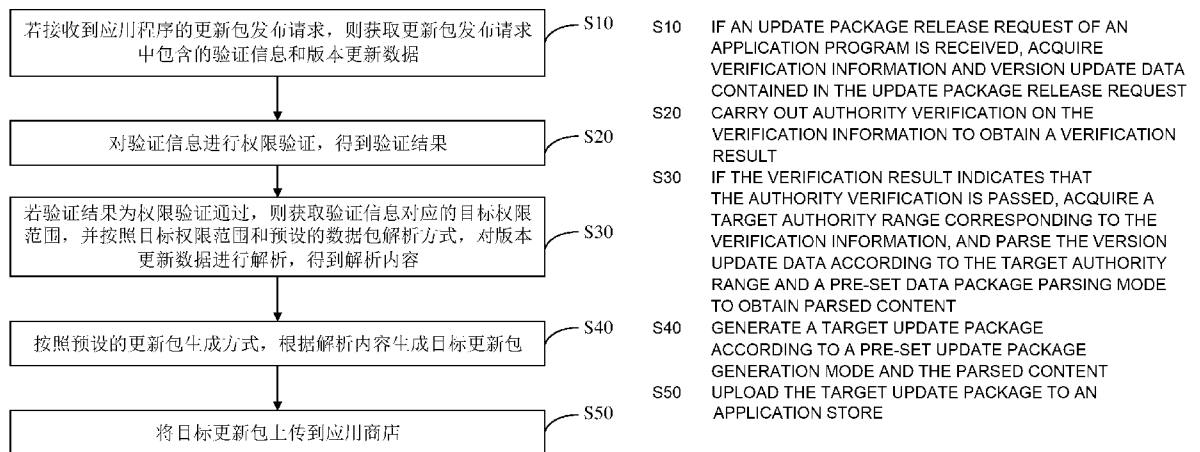


图 2

(57) **Abstract:** A version update package release method and apparatus, a computer device and a storage medium. The method comprises: when an update package release request of an application program is received, acquiring verification information and version update data contained in the update package release request, and carrying out authority verification on the verification information; and when an obtained verification result indicates that the authority verification is passed, parsing version update data to obtain parsed content, so that before an update package is automatically constructed, the authority of a user of a management end sending the update package release request is confirmed, thereby improving the update package release security. Moreover, generating a target update package according to a pre-set update package generation mode and the parsed content, and then uploading the target update package to an application store can realize automatic generation and release of the update package of an application program, thereby improving the update package release efficiency of the application program.

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)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种版本更新包的发布方法、装置、计算机设备及存储介质, 所述方法包括: 通过在接收到应用程序的更新包发布请求时, 获取更新包发布请求中包含的验证信息和版本更新数据, 并对验证信息进行权限验证, 在得到验证结果为权限验证通过时, 对版本更新数据进行解析, 得到解析内容, 使得在自动构建更新包之前, 确认发送更新包发布请求的管理端的用户的权限, 提高了更新包发布的安全性, 同时, 按照预设的更新包生成方式, 根据所述解析内容生成目标更新包, 再将目标更新包上传到应用商店, 实现了应用程序的更新包的自动生成和发布, 提高了应用程序的更新包发布的效率。

版本更新包的发布方法、装置、计算机设备及存储介质

本申请以 2019 年 3 月 19 日提交的申请号为 201910209166.7，名称为“版本更新包的发布方法、装置、计算机设备及存储介质”的中国发明专利申请为基础，并要求其优先权。

技术领域

本申请涉及数据处理领域，尤其涉及一种版本更新包的发布方法、装置、计算机设备及存储介质。

背景技术

随着经济的飞速发展和人们生活质量的日益提高，移动智能设备，尤其是智能手机，与人们的生活越来越密切，人们对移动智能设备上的应用程序（Application，APP）的功能需求，在不同时间会有些变化，同时，移动智能设备的 APP 本身也需要进行一些优化和 BUG 修复，因而，在移动智能设备的 APP 发布到应用商店后，需要定时或不定时地对其进行版本更新操作。

当前，移动智能设备的 APP 开发商在对 APP 进行版本更新操作时，主要是 APP 的研发人员对 APP 的源代码进行更新并测试通过后，由管理用户通过人工的方式，对源代码进行项目构建、签名和加固得到更新包，并设置更新包的相关信息后，进行人工发布，这种人工方式进行更新包构建和发布的过程，由于构建和发布繁琐的流程，容易导致更新包发布效率低，同时，由于发布更新包的管理用户的身份未经过认证，可能存在越权发布或流程不熟悉导致发布出错等一些不规范的情况，导致更新包发布的安全性不高。

发明内容

本申请实施例提供一种版本更新包的发布方法、装置、计算机设备和存储介质，以解决人工方式构建导致的更新包发布效率低和安全性不高的问题。

一种版本更新包的发布方法，包括：

若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

对所述验证信息进行权限验证，得到验证结果；

若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

将所述目标更新包上传到应用商店。

一种版本更新包的发布装置，包括：

请求接收模块，用于若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

权限验证模块，用于对所述验证信息进行权限验证，得到验证结果；

数据解析模块，用于若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

更新包生成模块，用于按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

更新包发布模块，用于将所述目标更新包上传到应用商店。

一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

对所述验证信息进行权限验证，得到验证结果；

若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

将所述目标更新包上传到应用商店。

一个或多个存储有计算机可读指令的可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如下步骤：

若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

对所述验证信息进行权限验证，得到验证结果；

若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

将所述目标更新包上传到应用商店。

本申请的一个或多个实施例的细节在下面的附图和描述中提出，本申请的其他特征和优点将从说明书、附图以及权利要求变得明显。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例的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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例提供的版本更新包的发布方法的应用环境示意图；

图 2 是本申请实施例提供的版本更新包的发布方法的实现流程图；

图 3 是本申请实施例提供的版本更新包的发布方法中步骤 S20 的实现流程图；

图 4 是本申请实施例提供的版本更新包的发布方法中步骤 S40 的实现流程图；

图 5 是本申请实施例提供的版本更新包的发布方法中步骤 S21 的实现流程图；

图 6 是本申请实施例提供的版本更新包的发布方法中语音信号交叠分帧的示例图；

图 7 是本申请实施例提供的版本更新包的发布方法中步骤 S25 的实现流程图；

图 8 是本申请实施例提供的版本更新包的发布装置的示意图；

图 9 是本申请实施例提供的计算机设备的示意图。

具体实施方式

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，都属于本申请保护的范围。

请参阅图 1，图 1 示出本申请实施例提供的版本更新包的发布方法的应用环境。该版本更新包的发布方法应用在应用程序的版本更新包发布场景中。该版本更新包发布场景包

括管理端和服务端，其中，管理端和服务端之间通过网络进行连接，管理端向服务端发送更新包发布请求，服务端接收该更新包发布请求，并获取更新包发布请求中包括的验证信息和版本更新信息，并通过验证信息对发送该更新包发布请求的管理人员进行权限验证，在权限验证通过后，根据版本更新信息，进行智能更新，管理端具体可以但不限于是手机、平板电脑、个人计算机（Personal Computer，PC）等智能终端设备，服务端具体可以用独立的服务器或者多个服务器组成的服务器集群实现。

请参阅图 2，图 2 示出本申请实施例提供的一种版本更新包的发布方法，以该方法应用在图 1 中的服务端为例进行说明，详述如下：

S10：若接收到应用程序的更新包发布请求，则获取更新包发布请求中包含的验证信息和版本更新数据。

具体地，在对应用程序进行更新后，需要对该应用程序对应的代码进行更新包构建，得到应用程序对应的更新包，进而将更新包发布到应用商店，管理用户可以通过管理端向服务端发送应用程序的更新包发布请求，服务端通过网络传输协议接收该更新包发布请求，并获取该更新包发布请求中包含的验证信息和版本更新信息。

其中，验证信息用于服务端对通过管理端发送的更新包发布请求的用户身份进行验证，在本实施例中，为避免误操作或者越权操作，在管理用户通过管理端向服务端发送更新包发布请求之前，需要先提供验证信息，并将验证信息与版本更新信息一起写入到更新包发布请求中发送，该验证信息具体包括但不限于：管理用户的指纹信息、管理用户的语音信息、管理用户的账号密码信息或管理用户的证件信息等，具体可根据实际情况进行设置，此处不做限定。

优选地，本实施例采用带有账号密码信息的管理用户的语音信息来作为验证信息，即管理用户录入一段语音信息，该语音信息中包含管理用户的账号密码信息，将该语音信息作为该管理用户的验证信息。

其中，版本更新信息是指应用程序需要进行更新的信息，包括但不限于：项目标识、版本信息和更新时间等，版本更新信息有固定的格式和分隔符，以便后续可以快速进行解析。

其中，网络传输协议包括但不限于：互联网控制报文协议（Internet Control Message Protocol，ICMP）、地址解析协议（ARP Address Resolution Protocol，ARP）和文件传输协议（File Transfer Protocol，FTP）等。

S20：对验证信息进行权限验证，得到验证结果。

具体地，针对不同职位的管理用户，在服务端预先设置的相应权限不一定相同，服务端在获取到验证信息和版本更新信息后，需要先对验证信息进行权限验证，以确定通过管理端进行发送更新包发布请求的管理用户是否具有更新包发布的权限。

在本实施例中，权限验证可以是但不限于是通过账号密码进行验证或者通过生物特征进行验证等，其中，生物特征包括但不限于：指纹特征、人脸特征、声纹特征和虹膜特征等。

若采用账号密码进行权限验证，则在服务端预先存储有每个管理用户标识对应的账号密码，以及每个管理用户标识对应的权限，在接收到验证信息后，获取该验证信息中的账号密码信息，进而将该账号密码信息与预先存储的每个管理用户标识对应的账号密码进行匹配，将匹配成功的账号密码对应的管理用户标识作为当前管理用户标识，并获取当前管理用户标识对应的权限作为目标权限，进而判断该目标权限是否包括更新包发布的权限，若该目标权限包括更新包发布的权限，则权限验证通过，若该目标权限不包括更新包发布的权限，则权限验证失败，并向管理端发送权限不匹配的提示信息。容易理解地，若验证信息中的账号密码与每个管理用户标识对应的账号密码均匹配失败，则确认权限验证失败，并向管理端发送账号密码有误的提示信息。

若采用生物特征进行权限验证,则在服务端预先存储有每个管理用户标识对应的生物特征,以及每个管理用户标识对应的权限,在接收到验证信息后,获取该验证信息中的生物特征,作为当前生物特征,进而分别计算当前生物特征与预先存储的每个管理用户标识对应的生物特征的相似度值,并将最大的相似度值与预设的相似度阈值进行比较,若最大的相似度值大于或等于预设的相似度阈值,则将最大的相似度值对应的管理用户标识作为目标管理用户标识,并获取目标管理用户标识对应的权限作为目标权限,进而判断该目标权限是否包括更新包发布的权限,若该目标权限包括更新包发布的权限,则权限验证通过,若该目标权限不包括更新包发布的权限,则权限验证失败,并向管理端发布权限不匹配的提示信息。容易理解地,若最大的相似度值小于预设的相似度阈值,则判断生物特征不符合要求,确认权限验证失败,并向管理端发送权限验证失败的提示信息。

值得说明的是,权限验证的方式可以根据实际需要,选择账号密码验证,或者根据实际需要,进行生物特征识别,也可以是其他方式,此处不做具体限制。

优选地,本实施例采用包含账号密码和声纹特征的音频信息来进行权限验证,也即,接收到的验证信息中,需要包括带有账号密码内容的语音信息,验证信息具体可以是一段音频文件,也可以是一段视频文件,可按照实际验证的需要进行设定,此处不做具体限制,通过音频信息进行权限验证,具体过程可参考本实施例中步骤 S21 至步骤 S26 的描述的方法,为避免重复,此处不再赘述。

S30:若验证结果为权限验证通过,则获取验证信息对应的目标权限范围,并按照目标权限范围和预设的数据包解析方式,对版本更新数据进行解析,得到解析内容。

具体地,在对发送更新包发布请求的管理端的管理用户的权限进行确认通过后,即确定该更新包发布请求的合法性后,获取该验证信息对应的目标权限范围,并根据目标权限范围和预设的数据包解析方式,对获取到的版本更新信息进行解析,得到解析内容。

值得说明的是,在本实施例中,不同管理人员具有的发布权限不同,例如,张三具有的发布权限为对第一分支代码、第二分支代码和第三分支代码进行更新发布的权限,李四具有的发布权限为对第四分支代码和第五分支代码进行更新发布的权限,在解析内容中包含的更新内容超出了目标权限范围时,将超出范围的内容作为无权限发布的内容,将忽略该部分内容,并向客户端发送相关提示信息。

进一步地,解析内容可以包括项目标识、版本号和构建脚本。

其中,项目标识用于对应用程序进行唯一标识,根据项目标识可以获取应用程序对应的所有代码,在本实施例中,不同版本号对应不同的分支代码,项目标识具体包括数字、字母、符号、汉字中的至少一种,也可以是多种的组合。

其中,版本号用于区分同一应用程序的不同分支代码。

其中,构建脚本用于将分支代码构建成目标项目。

其中,由于版本更新信息具有固定格式,因而,对获取到的版本更新信息进行解析,预设的数据包解析方式解析包括但不限于:字符分割、正则匹配和关键字匹配等。

优选地,本实施例采用基于正则匹配的方式对版本更新信息进行解析,先获取版本更新信息中的分隔符,使用预设的正则表达式,匹配到每个分隔符的位置,作为分割位置,在每个分割位置对版本更新信息进行分割,再按照预设的版本更新信息的格式,得到版本更新信息中的各项解析内容。

例如,在一具体实施方式中,预设的版本更新信息格式按照次序依次为:项目标识、版本号和指令,预设的分隔符为“;”,获取到的版本更新信息为“平安银行;v3.4.1;开始打包”,通过采用正则表达式,对该版本更新信息中的分隔符“;”进行匹配,得到两个分隔位置,进而按照预设的版本更新信息格式,得到三个解析内容,分别为:项目标识“平安银行”、版本号“v3.4.1”和指令“开始打包”。

S40:按照预设的更新包生成方式,根据解析内容生成目标更新包。

具体地，预设的更新包生成方式为预先设置的生成目标更新包的处理方式，其具体可以是服务端预设的代码库中，获取所述解析内容对应的分支代码，并对该分支代码进行项目构建，得到目标项目后，对该目标项目进行加固和重签名处理，得到目标更新包。

S50：将目标更新包上传到应用商店。

具体地，服务端针对每个应用存储有预设的应用商店地址，通过目标更新包对应的项目标识，获取与该项目标识对应的应用商店地址，并将得到的目标更新包上传到该项目标识对应的应用商店地址。

值得说明的是，预设的应用商店地址可以为一个，也可以为多个，可以根据实际需求进行设置，此处不做具体限定。

在本实施例中，通过在接收到应用程序的更新包发布请求时，获取更新包发布请求中包含的验证信息和版本更新数据，并对验证信息进行权限验证，在得到验证结果为权限验证通过时，对版本更新数据进行解析，得到解析内容，使得在自动构建更新包之前，确认发送更新包发布请求的管理端的用户的权限，提高了更新包发布的安全性，同时，按照预设的更新包生成方式，根据所述解析内容生成目标更新包，再将目标更新包上传到应用商店，实现了应用程序的更新包的自动生成和发布，提高了应用程序的更新包发布的效率。

在图2对应的实施例的基础之上，步骤S10中获取的验证信息为包含当前账号和当前密码的音频信息。该音频信息为管理人员根据预设语音录入的方式，对账号密码进行朗读录入得到。例如，在一具体实施方式中，预设语音录入的方式为先朗读“账号”然后读出账号，再朗读“密码”，然后读出密码，得到音频信息。

进一步地，下面通过一个具体的实施例来对步骤S20中所提及的对验证信息进行权限验证，得到验证结果的具体实现方法进行详细说明。

请参阅图3，图3示出了本申请实施例提供的步骤S20的具体实现流程，详述如下：

S21：对音频信息进行声纹提取，得到目标声纹信息。

具体地，对音频信息进行语音信号解析，得到初始声纹，并初始声纹进行预处理和声纹特征提取，得到目标声纹信息，具体过程也可以参考步骤S211至步骤S215的描述，为避免重复，此处不再赘述。

容易理解地，目标声纹信息为发送更新包发布请求的管理端的管理用户的声纹信息。

S22：将目标声纹信息与每个预设的权限声纹信息进行对比验证，得到声纹验证结果，其中，预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息。

具体地，在服务端，预先存储有每个具有更新包发布权限的管理用户的声纹信息，作为预设的权限声纹信息，通过预设的相似度计算方式，分别计算步骤S21中得到的目标声纹信息与每个预设的权限声纹信息的相似度，得到目标声纹信息与每个预设的权限声纹信息的相似度值，若这些相似度值中，存在大于或等于预设相似度阈值的相似度值，则确定该目标声纹信息为预设的权限声纹信息中的一个，也即，确定发送更新包发布请求的管理端的管理用户，具有更新包发布的权限，此时，确认声纹验证结果为验证通过，若这些相似度值均小于预设相似度阈值的相似度值，则确定该目标声纹信息不属于预设的权限声纹信息中的任意一个，此时，确认声纹验证结果为验证失败。

其中，预设的相似度计算方式包括但不限于：余弦相似性、最近邻(k-NearestNeighbor, kNN)分类算法、曼哈顿距离(Manhattan Distance)、基于SimHash算法的汉明距离等。

S23：采用预设的语音转换文本的方式，对音频信息进行文本转换，得到目标文本。

具体地，通过预设的语音转换文本的方式，对音频信息进行文本转换，得到目标文本。

其中，预设的语音转换文本的方式可以通过语音转换文本算法，也可以是通过第三方工具来实现，还可以是通过调用第三方应用程序编程接口(Application Programming Interface, API)来实现，可依据实际需求进行选择，此处不做限定。

S24: 对目标文本进行解析, 得到当前账号和当前密码。

具体地, 采用预设好的正则表达式对目标文本进行正则匹配, 得到目标文本中包含的当前账号和当前密码。

例如, 在一具体实施方式中, 预设语音录入的方式为先朗读“账号”然后读出账号, 再朗读“密码”, 然后读出密码, 得到音频信息, 根据该音频信息进行语音转换文本, 得到目标文本为“账号 yztfb523 密码 yzt652369”, 通过预设的正则表达式, 匹配出“账号”和“密码”, 并将“账号”和“密码”之间的文本作为当前账号, 将“密码”之后的文本作为当前密码。

S25: 对当前账号和当前密码进行合法性验证, 得到登录信息验证结果。

具体地, 对步骤 S24 中得到的当前账号和当前密码的合法性进行验证, 得到登录信息验证结果, 其中, 登录信息验证结果包括验证通过和验证失败, 在合法性验证通过时, 确认登录信息验证结果为验证通过, 在合法性验证失败时, 确认登录信息验证结果为验证失败。

其中, 合法性验证是用于验证当前账号和当前密码是否为服务端存储的具有更新包发布权限的账号和密码, 若当前账号为服务端存储的具有更新包发布权限的账号, 则继续验证当前密码的正确性。合法性的验证过程可参考步骤 S251 至步骤 S254 的描述, 为避免重复, 此处不再赘述。

需要说明的是, 步骤 S21 至步骤 S22, 与步骤 S23 至步骤 S25 之间, 没有必然的先后执行顺序, 其可以是并列执行的关系, 此处不做限制。

S26: 若声纹验证结果和登录信息验证结果均为验证通过, 则确认验证结果为权限验证通过。

具体地, 在声纹验证结果和登录信息验证结果均为验证通过, 则确认验证结果为权限验证通过。

若声纹验证结果为验证失败, 或者, 登录信息验证结果为验证失败, 或者声纹验证结果和登录信息验证结果均为验证失败, 则确认验证结果为权限验证失败, 此时, 拒绝此次更新包发布请求, 并将该音频信息和验证信息进行记录并保存到预设的异常信息文件中, 以便后续可以通过对该预设的异常信息文件进行分析, 得到异常原因, 并作出相应异常处理。

在本实施例中, 通过对音频信息进行声纹提取, 得到目标声纹信息, 进而将目标声纹信息与每个预设的权限声纹信息进行对比验证, 得到声纹验证结果, 同时, 采用预设的语音转换文本的方式, 对音频信息进行文本转换, 得到目标文本, 并对目标文本进行解析, 得到当前账号和当前密码, 进而对当前账号和当前密码进行合法性验证, 得到登录信息验证结果, 在声纹验证结果和登录信息验证结果均为验证通过, 则确认验证结果为权限验证通过。实现了管理人员根据预设语音录入的方式, 对账号密码进行朗读录入得到音频信息, 同时完成声纹信息验证和登录信息验证, 快捷多重进行身份认证, 提升了身份认证的效率和安全性。

在图 2 或图 3 对应的实施例的基础之上, 步骤 S30 中得到的解析内容包括项目标识、版本号和构建脚本, 其中, 项目标识用于对应用程序进行唯一标识, 根据项目标识可以获取应用程序对应的所有代码, 所有代码中, 不同版本号对应不同的分支代码。版本号用于区分同一应用程序的不同分支代码。

进一步地, 下面通过一个具体的实施例来对步骤 S40 中所提及的按照预设的更新包生成方式, 根据解析内容生成目标更新包的具体实现方法进行详细说明。

请参阅图 4, 图 4 示出了本申请实施例提供的步骤 S40 的具体实现流程, 详述如下:

S41: 根据项目标识, 从预设的代码库中获取所述项目标识对应的代码, 并从代码中获取版本号对应的分支代码, 作为目标代码。

具体地，通过项目标识，从预设的代码库中获取该项目标识对应的代码，并从该代码中获取该版本号对应的分支代码，作为目标代码。

S42：使用构建脚本，对目标代码进行项目构建，得到目标项目。

具体地，使用预设的构建脚本，对目标代码进行项目构建，得到目标项目。

其中，预设的构建脚本可以根据预先设定的项目构建条件进行设置，此处不作具体限定。

S43：对目标项目进行加固处理，并对完成加固处理后的目标项目进行重签名处理，得到目标更新包。

具体地，对得到的目标项目进行加固处理，并对完成加固处理后的目标项目进行重签名处理，得到目标更新包。

其中，加固处理是指对目标更新包进行安全检测和安全防护处理，加固处理包括但不限于：防盗版和破解的加密处理、安全性漏洞检测、分发下载渠道监控和专业场景下的安全解决方案设置等，若应用不做任何安全防护，则应用程序极易被病毒植入、广告替换、支付渠道篡改、钓鱼、信息劫持等，严重侵害开发者的利益，通过对应用程序进行加固方案处理，有效防止应用分发后，被反编译、调试、盗版、破解、二次打包等威胁，保障了应用程序发布的安全性。

其中，重签名是指对得到的更新包进行重新签名操作，为了保证每个应用程序开发商合法 ID，防止部分开放商可能通过使用相同的 Package Name 来混淆替换已经安装的程序，需要在应用程序发布前，对应用程序进行签名，保证每次发布的应用程序版本的唯一性。

在本实施例中，根据项目标识，从预设的代码库中获取项目标识对应的代码，并从代码中获取版本号对应的分支代码，作为目标代码，并使用构建脚本，对目标代码进行项目构建，得到目标项目，进而对目标项目进行加固处理，并对完成加固处理后的目标项目进行重签名处理，得到目标更新包，实现了自动构建目标更新包，提高了更新包构建的效率。

在图 3 对应的实施例的基础之上，下面通过一个具体的实施例来对步骤 S21 中所提及的对音频信息进行声纹提取，得到目标声纹信息的具体实现方法进行详细说明。

请参阅图 5，图 5 示出了本申请实施例提供的步骤 S21 的具体实现流程，详述如下：

S211：对音频信息进行声纹解析，得到初始声纹样本。

具体地，通过语音信号提取的方式，提取音频信息中包含的语音信号，作为初始声纹样本。

S212：对初始声纹样本进行预加重处理，生成具有平坦频谱的加重处理声纹样本。

具体地，由于声门激励和口鼻辐射会对语音信号的平均功率谱产生影响，导致高频在超过 800Hz 时会按 6dB/倍频跌落，所以在计算语音信号频谱时，频率越高相应的成分越小，为此要在预处理中进行预加重（Pre-emphasis）处理，预加重的目的是提高高频部分，使信号的频谱变得平坦，保持在低频到高频的整个频带中，能用同样的信噪比求频谱，以便于频谱分析或者声道参数分析。预加重可在语音信号数字化时在反混叠滤波器之前进行，这样不仅可以进行预加重，而且可以压缩信号的动态范围，有效地提高信噪比。预加重可使用一阶的数字滤波器来实现，例如：有限脉冲响应（Finite Impulse Response, FIR）滤波器。

值得说明的是，利用设备获取的语音信号都是模拟信号，在对这些模拟信号进行预加重处理之前，需要经过采样和量化将模拟信息转化为数字信号，根据语音的频谱范围 200-3400Hz，采样率可设置为 8KHz，量化精度为 16bit。

应理解，此处采样率和量化精度的数值范围，为本申请优选范围，但可以根据实际应用的需要进行设置，此处不做限制。

语音信号在经过预加重后，频谱的高频部分得到提升，信号也变得平坦，生成具有平坦频谱的加重处理声纹样本，有利于后续的声纹特征提取。

S213: 采用分帧和加窗的方式, 对加重处理声纹样本进行分帧处理, 得到初始语音帧。

具体地, 语音信号具有短时平稳的性质, 语音信号在经过预加重处理后, 需要对其进行分帧和加窗处理, 来保持信号的短时平稳性, 通常情况下, 每秒钟包含的帧数在 33~100 帧之间。为了保持帧与帧之间的连续性, 使得相邻两帧都能平滑过渡, 采用交叠分帧的方式, 如图 6 所示, 图 6 示出了交叠分帧的样例, 在图 6 中, 第 k 帧和第 k+1 帧之间的交叠部分即为帧移。

优选地, 帧移与帧长的比值的取值范围为 (0, 0.5)。

例如, 在一具体实施方式中, 预加重后的语音信号为 $s'(n)$, 帧长为 N 个采样点, 帧移为 M 个采样点。当第 l 帧对应的采样点为第 n 个时, 原始语音信号 $x_l(n)$ 与各参数之间的对应关系为:

$$x_l(n) = x[(l-1)M + n]$$

其中, $n = 0, 1, \dots, N-1$, $N = 256$ 。

进一步地, 声纹样本经过分帧之后, 使用相应的窗函数 $w(n)$ 与预加重后的语音信号 $s'(n)$ 相乘, 即得到加窗后的语音信号 S_w , 将该语音信号作为初始语音帧信号。

其中, 窗函数包括但不限于: 矩形窗 (Rectangular)、汉明窗 (Hamming) 和汉宁窗 (Hanning) 等。

矩形窗表达式为:

$$w(n) = \begin{cases} 1 & (0 \leq n \leq N-1) \\ 0 & (n < 0, n > N) \end{cases}$$

汉明窗表达式为:

$$w(n) = \begin{cases} 0.54 - 0.46 \cos(2 * \pi * n / (N-1)) & (0 \leq n \leq N-1) \\ 0 & (n < 0, n > N) \end{cases}$$

汉宁窗表达式为:

$$w(n) = \begin{cases} 0.5(1 - \cos(2 * \pi * n / (N-1))) & (0 \leq n \leq N-1) \\ 0 & (n < 0, n > N) \end{cases}$$

对经过预加重处理的声纹样本进行分帧和加窗处理, 使得声纹样本保持帧与帧之间的连续性, 并剔除掉一些异常的信号点, 提高了声纹样本的鲁棒性。

S214: 对初始语音帧进行静默音分离, 得到目标语音帧。

具体地, 在通话持续期间, 语音信号可分为激活期和静默期两个状态, 静默期不传送任何语音信号, 上、下行链路的激活期和静默期相互独立。在步骤 S211 中, 管理用户进行录音获取音频信息的过程中, 在每次发音前后, 均会有停顿的状态, 这个状态会带来语音信号的停顿, 即静默期, 在进行声纹特征提取的时候, 需要检测出静默期状态, 进而将静默期与激活期进行分离, 以得到持续的激活期, 将保留下来的持续的激活期的语音信号作为目标语音帧。

其中, 检测静默音状态的方式包括但不限于: 语音端点检测、FFMPEG 探测音频静音算法和语音活动检测 (Voice Activity Detection, VAD) 算法等。

S215: 基于目标语音帧, 提取声纹特征, 将得到的声纹特征作为目标声纹信息。

具体地, 在经过预加重处理、分帧和加窗和静默音分离之后, 获取了稳定性强的声纹样本, 使用该样本进行声纹特征的提取, 并将得到的声纹特征作为目标声纹信息。

其中, 声纹特征提取是提取并选择对说话人的声纹具有可分性强、稳定性高等特性的声学或语言特征。

优选地, 本申请选择提取的声纹特征为声学特征中的线性倒谱特征。

在本实施例中, 针对验证信息中的音频信息进行声纹解析, 得到该初始声纹样本, 并对初始声纹样本进行预加重处理, 生成具有平坦频谱的加重处理声纹样本, 采用分帧和加窗的方式, 对加重处理声纹样本进行分帧处理, 得到具有鲁棒性的初始语音帧, 然后对初始语音帧信号进行静默音分离, 过滤掉有干扰的静默音, 得到目标语音帧, 使得声纹样本具有连续性和鲁棒性, 进而从该声纹样本中提取管理用户的声纹特征, 提升了获取目标声纹特征的准确度和鲁棒性, 有利于提高声纹验证的准确率。

在图 3 对应的实施例的基础之上, 下面通过一个具体的实施例来对步骤 S25 中所提及的对当前账号和当前密码进行合法性验证, 得到登录信息验证结果的具体实现方法进行详细说明。

请参阅图 7, 图 7 示出了本申请实施例提供的步骤 S25 的具体实现流程, 详述如下:

S251: 从预设的数据库存储的基础账号中, 查询是否存在与当前账号相同的基础账号, 得到查询结果, 其中, 基础账号为预设的数据库中存储的具有更新包发布权限的账号。

具体地, 在服务端预设的数据库中, 存储有每个管理用户的账号, 并对这些账号按照权限进行分组, 将具有更新包发布权限的管理用户的账号作为基础账号, 在对目标文本进行解析, 得到当前账号和当前密码后, 在预设的数据存储的基础账号中, 查询是否存在与当前账号相同的账号, 得到查询结果。

其中, 查询结果为预设的数据库存储的基础账号中存在与当前账号相同的账号, 或者, 查询结果为不存在与当前账号相同的账号。

容易理解的, 若预设的数据库存储的基础账号中存在与当前账号相同的账号, 则需要继续对当前密码进行验证, 以校验当前密码与该基础账号对应的基础密码是否一致, 若预设的数据库存储的基础账号中不存在与当前账号相同的账号, 则直接确定登录信息验证结果为验证失败。

S252: 若查询结果为存在与当前账号相同的基础账号, 则将与当前账号相同的基础账号作为目标账号, 并获取目标账号对应的基础密码, 作为目标密码。

具体地, 在预设的数据库中, 每个基础密码对应有一个基础密码, 在查询结果为存在与所述当前账号相同的基础账号时, 将与所述当前账号相同的基础账号作为目标账号, 并获取目标账号对应的基础密码, 作为目标密码, 以便后续使用该目标密码与当前密码进行比较。

S253: 对目标密码和当前密码进行一致性校验, 得到校验结果。

具体地, 对目标密码和当前密码进行一致性校验, 具体可以是先分别获取目标密码和当前密码的字符个数, 若目标密码的字符个数和当前密码的字符个数相同, 则使用字符截取函数, 分别截取目标密码和当前密码相同位置的字符进行比较, 或者, 将当前密码和目标密码分别放入两个初始为空的数组中, 进而对这两个数组中相同位置的数组元素进行比较, 若每个位置的字符或者每个位置的数组元素的比较结果均为相同, 则确定校验结果为目标密码与当前密码一致, 若存在比较结果不同的字符或者数组元素, 则确定校验结果为目标密码与当前密码不一致。

其中, 获取目标密码和当前密码的字符个数可以通过字符串长度统计函数, 例如: Strlen、str.Length 和 Sizeof 等。

其中, 字符截取函数指的是编程语言中用来进行字符串处理的函数, 常用的字符截取

函数包括但不限于：InStr, InStrRev, InStrB, Mid, Right 和 Left 等。

应理解，若获取到目标密码的字符个数和当前密码的字符个数不相同，则可直接判定目标密码和当前密码不一致，而无需进行后续的字符比较的过程，即可确定登录信息验证结果为验证失败。

S254: 若校验结果为目标密码与当前密码一致，则确定登录信息验证结果为验证通过。

具体地，在校验结果为目标密码与当前密码一致时，确认登录信息验证结果为验证通过。

若校验结果为目标密码与当前密码不一致，则说明管理人员提供的当前密码错误，确定登录信息验证结果为验证不通过。

在本实施例中，通过从预设的数据库存储的基础账号中，查询是否存在与所述当前账号相同的基础账号，得到查询结果，并在查询结果为存在与当前账号相同的基础账号时，将所述与当前账号相同的基础账号作为目标账号，并获取目标账号对应的基础密码，作为目标密码，进而对目标密码和当前密码进行一致性校验，得到校验结果，在校验结果为目标密码与当前密码一致时，则确定登录信息验证结果为验证通过，实现了通过将目标文本中解析得到的当前账号和当前密码，与预设的数据库中存储的每个基础账号和基础账号对应的基础密码进行一致性校验，在校验通过后，确认登录信息验证结果为验证通过，确保了通过音频信息中解析出的当前账号和当前密码的合法性，有利于提高权限验证的安全性。

应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。

图 8 示出与上述实施例版本更新包的发布方法一一对应的版本更新包的发布装置的原理框图。如图 8 所示，该版本更新包的发布装置包括请求接收模块 10、权限验证模块 20、数据解析模块 30、更新包生成模块 40 和更新包发布模块 50。各功能模块详细说明如下：

请求接收模块 10，用于若接收到应用程序的更新包发布请求，则获取更新包发布请求中包含的验证信息和版本更新数据；

权限验证模块 20，用于对验证信息进行权限验证，得到验证结果；

数据解析模块 30，用于若验证结果为权限验证通过，则获取验证信息对应的目标权限范围，并按照目标权限范围和预设的数据包解析方式，对版本更新数据进行解析，得到解析内容；

更新包生成模块 40，用于按照预设的更新包生成方式，根据解析内容生成目标更新包；

更新包发布模块 50，用于将目标更新包上传到应用商店。

进一步地，权限验证模块 20 包括：

声纹提取单元 21，用于对音频信息进行声纹提取，得到目标声纹信息；

声纹验证单元 22，用于将目标声纹信息与每个预设的权限声纹信息进行对比验证，得到声纹验证结果，其中，预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息；

文本转换单元 23，用于采用预设的语音转换文本的方式，对音频信息进行文本转换，得到目标文本；

文本解析单元 24，用于对目标文本进行解析，得到当前账号和当前密码；

登录验证单元 25，用于对当前账号和当前密码进行合法性验证，得到登录信息验证结果；

结果确定单元 26，用于若声纹验证结果和登录信息验证结果均为验证通过，则确认验证结果为权限验证通过。

进一步地，更新包生成模块 40 包括：

代码获取单元 41，用于根据项目标识，从预设的代码库中获取项目标识对应的代码，并从该代码中获取版本号对应的分支代码，作为目标代码；

项目构建单元 42，用于使用构建脚本，对目标代码进行项目构建，得到目标项目；

加固签名单元 43，用于对目标项目进行加固处理，并对完成加固处理后的目标项目进行重签名处理，得到目标更新包。

进一步地，声纹提取单元 21 包括：

初始样本获取子单元 211，用于对音频信息进行声纹解析，得到初始声纹样本；

预加重处理子单元 212，用于对初始声纹样本进行预加重处理，生成具有平坦频谱的加重处理声纹样本；

分帧加窗子单元 213，用于采用分帧和加窗的方式，对加重处理声纹样本进行分帧处理，得到初始语音帧；

静默音分离子单元 214，用于对初始语音帧进行静默音分离，得到目标语音帧；

声纹特征提取子单元 215，用于基于目标语音帧，提取声纹特征，将得到的声纹特征作为目标声纹信息。

进一步地，登录验证单元 25 包括：

账号查询子单元 251，用于从预设的数据库存储的基础账号中，查询是否存在与当前账号相同的基础账号，得到查询结果，其中，基础账号为预设的数据库中存储的具有更新包发布权限的账号；

密码获取子单元 252，用于若查询结果为存在与当前账号相同的基础账号，则将与当前账号相同的基础账号作为目标账号，并获取目标账号对应的基础密码，作为目标密码；

一致性校验子单元 253，用于对目标密码和当前密码进行一致性校验，得到校验结果；

结果确定子单元 254，用于若校验结果为目标密码与当前密码一致，则确定登录信息验证结果为验证通过。

关于版本更新包的发布装置的具体限定可以参见上文中对于版本更新包的发布方法的限定，在此不再赘述。上述版本更新包的发布装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

图 9 是本申请一实施例提供的计算机设备的示意图。该计算机设备可以是服务端，其内部结构图可以如图 9 所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机可读指令和数据库。该内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的数据库用于存储预设的权限声纹信息、基础账号和基础账号对应的基础密码。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种版本更新包的发布方法。

在一个实施例中，提供了一种计算机设备，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可读指令，处理器执行计算机可读指令时实现上述实施例版本更新包的发布方法的步骤，例如图 2 所示的步骤 S10 至步骤 50。或者，处理器执行计算机可读指令时实现上述实施例版本更新包的发布装置各模块/单元的功能，例如图 8 所示的模块 10 至模块 50 的功能。为避免重复，这里不再赘述。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。

在一实施例中，提供一个或多个存储有计算机可读指令的可读存储介质，所述计算机可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行时实现上述实施例版本更新包的发布方法的步骤，或者，该计算机可读指令被处理器执行时实现上述实施例版本更新包的发布装置中各模块/单元的功能。为避免重复，这里不再赘述。本实施例中的可读存储介质包括非易失性可读存储介质和易失性可读存储介质。

可以理解地，所述计算机可读存储介质可以包括：能够携带所述计算机可读指令代码的任何实体或装置、记录介质、U 盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、电载波信号和电信信号等。

以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权 利 要 求 书

1. 一种版本更新包的发布方法，其特征在于，所述版本更新包的发布方法包括：
若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；
对所述验证信息进行权限验证，得到验证结果；
若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；
按照预设的更新包生成方式，根据所述解析内容生成目标更新包；
将所述目标更新包上传到应用商店。
2. 如权利要求 1 所述的版本更新包的发布方法，其特征在于，所述验证信息为包含当前账号和当前密码的音频信息；所述对所述验证信息进行权限验证，得到验证结果包括：
对所述音频信息进行声纹提取，得到目标声纹信息；
将所述目标声纹信息与每个预设的权限声纹信息进行对比验证，得到声纹验证结果，其中，所述预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息；
采用预设的语音转换文本的方式，对所述音频信息进行文本转换，得到目标文本；
对所述目标文本进行解析，得到所述当前账号和所述当前密码；
对所述当前账号和所述当前密码进行合法性验证，得到登录信息验证结果；
若所述声纹验证结果和所述登录信息验证结果均为验证通过，则确认所述验证结果为权限验证通过。
3. 如权利要求 1 或 2 所述的版本更新包的发布方法，其特征在于，所述解析内容包括项目标识、版本号和构建脚本；所述按照预设的更新包生成方式，根据所述解析内容生成目标更新包包括：
根据所述项目标识，从预设的代码库中获取所述项目标识对应的代码，并从所述代码中获取所述版本号对应的分支代码，作为目标代码；
使用所述构建脚本，对所述目标代码进行项目构建，得到目标项目；
对所述目标项目进行加固处理，并对完成加固处理后的所述目标项目进行重签名处理，得到目标更新包。
4. 如权利要求 2 所述的版本更新包的发布方法，其特征在于，所述对所述音频信息进行声纹提取，得到目标声纹信息包括：
对所述音频信息进行声纹解析，得到初始声纹样本；
对所述初始声纹样本进行预加重处理，生成具有平坦频谱的加重处理声纹样本；
采用分帧和加窗的方式，对所述加重处理声纹样本进行分帧处理，得到初始语音帧；
对所述初始语音帧进行静默音分离，得到目标语音帧；
基于所述目标语音帧，提取声纹特征，将得到的声纹特征作为目标声纹信息。
5. 如权利要求 2 所述的版本更新包的发布方法，其特征在于，所述对所述当前账号和所述当前密码进行合法性验证，得到登录信息验证结果包括：
从预设的数据库存储的基础账号中，查询是否存在与所述当前账号相同的基础账号，得到查询结果，其中，所述基础账号为所述预设的数据库中存储的具有更新包发布权限的账号；
若查询结果为存在与所述当前账号相同的基础账号，则将所述与所述当前账号相同的基础账号作为目标账号，并获取所述目标账号对应的基础密码，作为目标密码；
对所述目标密码和所述当前密码进行一致性校验，得到校验结果；
若所述校验结果为所述目标密码与所述当前密码一致，则确定所述登录信息验证结果

为验证通过。

6. 一种版本更新包的发布装置，其特征在于，所述版本更新包的发布装置包括：

请求接收模块，用于若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

权限验证模块，用于对所述验证信息进行权限验证，得到验证结果；

数据解析模块，用于若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

更新包生成模块，用于按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

更新包发布模块，用于将所述目标更新包上传到应用商店。

7. 如权利要求 6 所述的版本更新包的发布装置，其特征在于，所述验证信息为包含当前账号和当前密码的音频信息；所述权限验证模块包括：

声纹提取单元，用于对所述音频信息进行声纹提取，得到目标声纹信息；

声纹验证单元，用于将所述目标声纹信息与每个预设的权限声纹信息进行对比验证，得到声纹验证结果，其中，所述预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息；

文本转换单元，用于采用预设的语音转换文本的方式，对所述音频信息进行文本转换，得到目标文本；

文本解析单元，用于对所述目标文本进行解析，得到当前账号和当前密码；

登录验证单元，用于对所述当前账号和所述当前密码进行合法性验证，得到登录信息验证结果；

结果确定单元，用于若所述声纹验证结果和所述登录信息验证结果均为验证通过，则确认所述验证结果为权限验证通过。

8. 如权利要求 6 或 7 所述的版本更新包的发布装置，其特征在于，所述解析内容包括项目标识、版本号和构建脚本；所述更新包生成模块包括：

代码获取单元，用于根据所述项目标识从预设的代码库中获取所述项目标识对应的代码，并从所述代码中获取所述版本号对应的分支代码，作为目标代码；

项目构建单元，用于使用所述构建脚本，对所述目标代码进行项目构建，得到目标项目；

加固签名单元，用于对所述目标项目进行加固处理，并对完成加固处理后的所述目标项目进行重签名处理，得到目标更新包。

9. 如权利要求 7 所述的版本更新包的发布装置，其特征在于，所述声纹提取单元包括：

初始样本获取子单元，用于对所述音频信息进行声纹解析，得到初始声纹样本；

预加重处理子单元，用于对所述初始声纹样本进行预加重处理，生成具有平坦频谱的加重处理声纹样本；

分帧加窗子单元，用于采用分帧和加窗的方式，对所述加重处理声纹样本进行分帧处理，得到初始语音帧；

静默音分离子单元，用于对所述初始语音帧进行静默音分离，得到目标语音帧；

声纹特征提取子单元，用于基于所述目标语音帧，提取声纹特征，将得到的声纹特征作为目标声纹信息。

10. 如权利要求 7 所述的版本更新包的发布装置，其特征在于，所述登录验证单元包括：

账号查询子单元，用于从预设的数据库存储的基础账号中，查询是否存在与所述当前账号相同的基础账号，得到查询结果，其中，所述基础账号为所述预设的数据库中存储的

具有更新包发布权限的账号；

密码获取子单元，用于若查询结果为存在与所述当前账号相同的基础账号，则将所述与所述当前账号相同的基础账号作为目标账号，并获取所述目标账号对应的基础密码，作为目标密码；

一致性校验子单元，用于对所述目标密码和所述当前密码进行一致性校验，得到校验结果；

结果确定子单元，用于若所述校验结果为所述目标密码与所述当前密码一致，则确定所述登录信息验证结果为验证通过。

11. 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

若接收到应用程序的更新包发布请求，则获取所述更新包发布请求中包含的验证信息和版本更新数据；

对所述验证信息进行权限验证，得到验证结果；

若所述验证结果为权限验证通过，则获取所述验证信息对应的目标权限范围，并按照所述目标权限范围和预设的数据包解析方式，对所述版本更新数据进行解析，得到解析内容；

按照预设的更新包生成方式，根据所述解析内容生成目标更新包；

将所述目标更新包上传到应用商店。

12. 如权利要求 11 所述的计算机设备，其特征在于，所述验证信息为包含当前账号和当前密码的音频信息；所述对所述验证信息进行权限验证，得到验证结果包括：

对所述音频信息进行声纹提取，得到目标声纹信息；

将所述目标声纹信息与每个预设的权限声纹信息进行对比验证，得到声纹验证结果，其中，所述预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息；

采用预设的语音转换文本的方式，对所述音频信息进行文本转换，得到目标文本；

对所述目标文本进行解析，得到所述当前账号和所述当前密码；

对所述当前账号和所述当前密码进行合法性验证，得到登录信息验证结果；

若所述声纹验证结果和所述登录信息验证结果均为验证通过，则确认所述验证结果为权限验证通过。

13. 如权利要求 11 或 12 所述的计算机设备，其特征在于，所述解析内容包括项目标识、版本号和构建脚本；所述按照预设的更新包生成方式，根据所述解析内容生成目标更新包包括：

根据所述项目标识，从预设的代码库中获取所述项目标识对应的代码，并从所述代码中获取所述版本号对应的分支代码，作为目标代码；

使用所述构建脚本，对所述目标代码进行项目构建，得到目标项目；

对所述目标项目进行加固处理，并对完成加固处理后的所述目标项目进行重签名处理，得到目标更新包。

14. 如权利要求 12 所述的计算机设备，其特征在于，所述对所述音频信息进行声纹提取，得到目标声纹信息包括：

对所述音频信息进行声纹解析，得到初始声纹样本；

对所述初始声纹样本进行预加重处理，生成具有平坦频谱的加重处理声纹样本；

采用分帧和加窗的方式，对所述加重处理声纹样本进行分帧处理，得到初始语音帧；

对所述初始语音帧进行静默音分离，得到目标语音帧；

基于所述目标语音帧，提取声纹特征，将得到的声纹特征作为目标声纹信息。

15. 如权利要求 12 所述的计算机设备，其特征在于，所述对所述当前账号和所述当前

密码进行合法性验证, 得到登录信息验证结果包括:

从预设的数据库存储的基础账号中, 查询是否存在与所述当前账号相同的基础账号, 得到查询结果, 其中, 所述基础账号为所述预设的数据库中存储的具有更新包发布权限的账号;

若查询结果为存在与所述当前账号相同的基础账号, 则将所述与所述当前账号相同的基础账号作为目标账号, 并获取所述目标账号对应的基础密码, 作为目标密码;

对所述目标密码和所述当前密码进行一致性校验, 得到校验结果;

若所述校验结果为所述目标密码与所述当前密码一致, 则确定所述登录信息验证结果为验证通过。

16. 一个或多个存储有计算机可读指令的可读存储介质, 所述计算机可读指令被一个或多个处理器执行时, 使得所述一个或多个处理器执行如下步骤:

若接收到应用程序的更新包发布请求, 则获取所述更新包发布请求中包含的验证信息和版本更新数据;

对所述验证信息进行权限验证, 得到验证结果;

若所述验证结果为权限验证通过, 则获取所述验证信息对应的目标权限范围, 并按照所述目标权限范围和预设的数据包解析方式, 对所述版本更新数据进行解析, 得到解析内容;

按照预设的更新包生成方式, 根据所述解析内容生成目标更新包;

将所述目标更新包上传到应用商店。

17. 如权利要求 16 所述的可读存储介质, 其特征在于, 所述验证信息为包含当前账号和当前密码的音频信息; 所述对所述验证信息进行权限验证, 得到验证结果包括:

对所述音频信息进行声纹提取, 得到目标声纹信息;

将所述目标声纹信息与每个预设的权限声纹信息进行对比验证, 得到声纹验证结果, 其中, 所述预设的权限声纹信息为具有更新包发布权限的管理用户的声纹信息;

采用预设的语音转换文本的方式, 对所述音频信息进行文本转换, 得到目标文本;

对所述目标文本进行解析, 得到所述当前账号和所述当前密码;

对所述当前账号和所述当前密码进行合法性验证, 得到登录信息验证结果;

若所述声纹验证结果和所述登录信息验证结果均为验证通过, 则确认所述验证结果为权限验证通过。

18. 如权利要求 16 或 17 所述的可读存储介质, 其特征在于, 所述解析内容包括项目标识、版本号和构建脚本; 所述按照预设的更新包生成方式, 根据所述解析内容生成目标更新包包括:

根据所述项目标识, 从预设的代码库中获取所述项目标识对应的代码, 并从所述代码中获取所述版本号对应的分支代码, 作为目标代码;

使用所述构建脚本, 对所述目标代码进行项目构建, 得到目标项目;

对所述目标项目进行加固处理, 并对完成加固处理后的所述目标项目进行重签名处理, 得到目标更新包。

19. 如权利要求 17 所述的可读存储介质, 其特征在于, 所述对所述音频信息进行声纹提取, 得到目标声纹信息包括:

对所述音频信息进行声纹解析, 得到初始声纹样本;

对所述初始声纹样本进行预加重处理, 生成具有平坦频谱的加重处理声纹样本;

采用分帧和加窗的方式, 对所述加重处理声纹样本进行分帧处理, 得到初始语音帧;

对所述初始语音帧进行静默音分离, 得到目标语音帧;

基于所述目标语音帧, 提取声纹特征, 将得到的声纹特征作为目标声纹信息。

20. 如权利要求 17 所述的可读存储介质, 其特征在于, 所述对所述当前账号和所述当

前密码进行合法性验证，得到登录信息验证结果包括：

从预设的数据库存储的基础账号中，查询是否存在与所述当前账号相同的基础账号，得到查询结果，其中，所述基础账号为所述预设的数据库中存储的具有更新包发布权限的账号；

若查询结果为存在与所述当前账号相同的基础账号，则将所述与所述当前账号相同的基础账号作为目标账号，并获取所述目标账号对应的基础密码，作为目标密码；

对所述目标密码和所述当前密码进行一致性校验，得到校验结果；

若所述校验结果为所述目标密码与所述当前密码一致，则确定所述登录信息验证结果为验证通过。

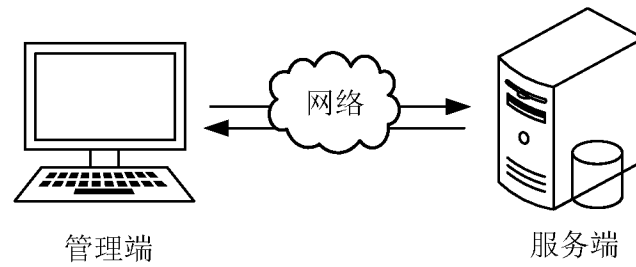


图 1

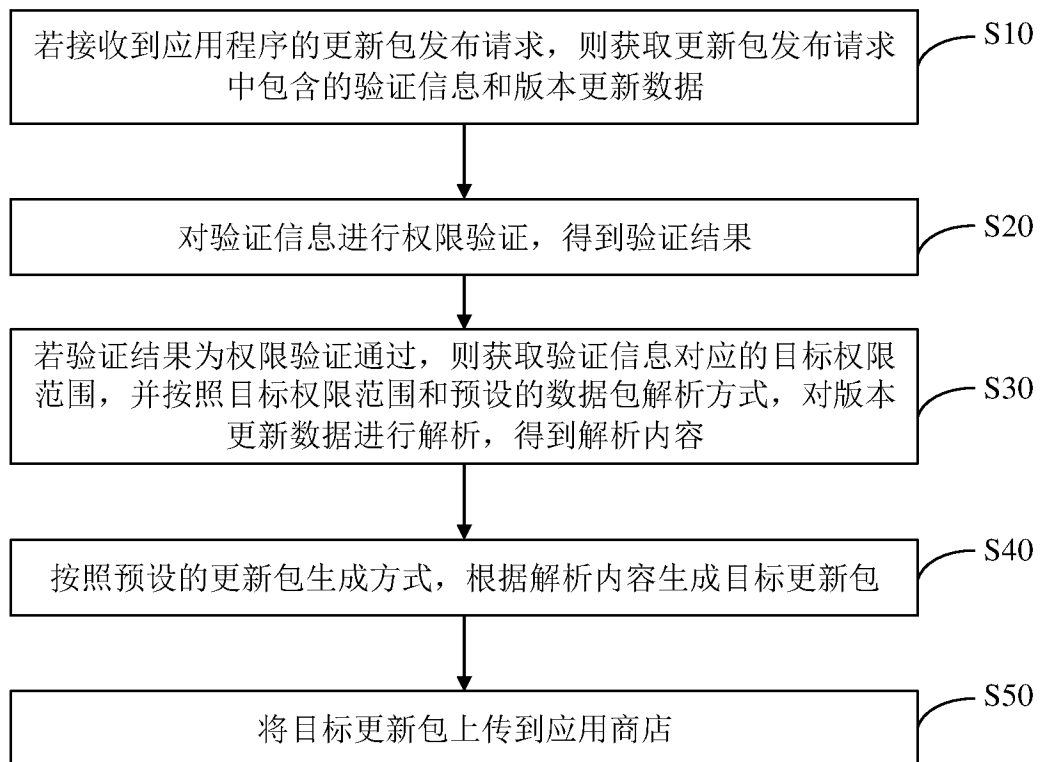
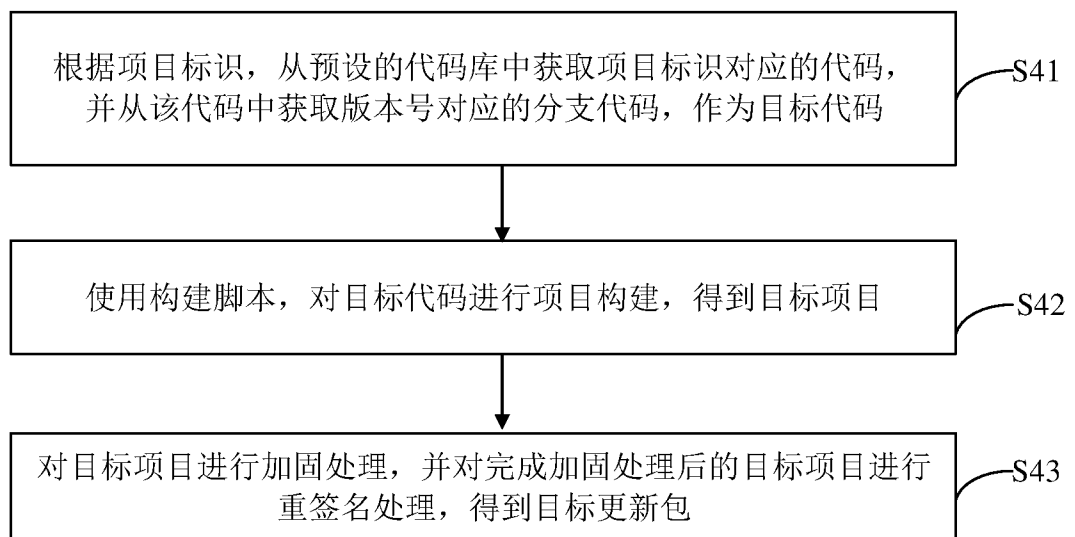
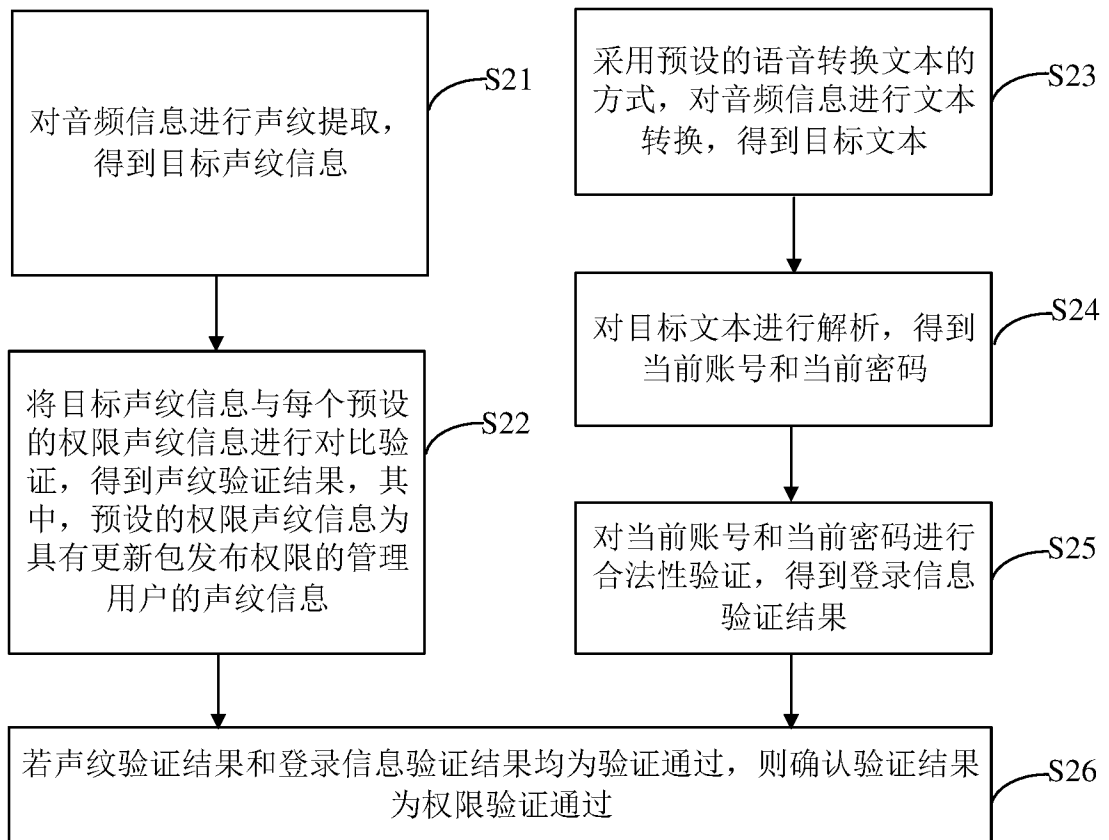


图 2



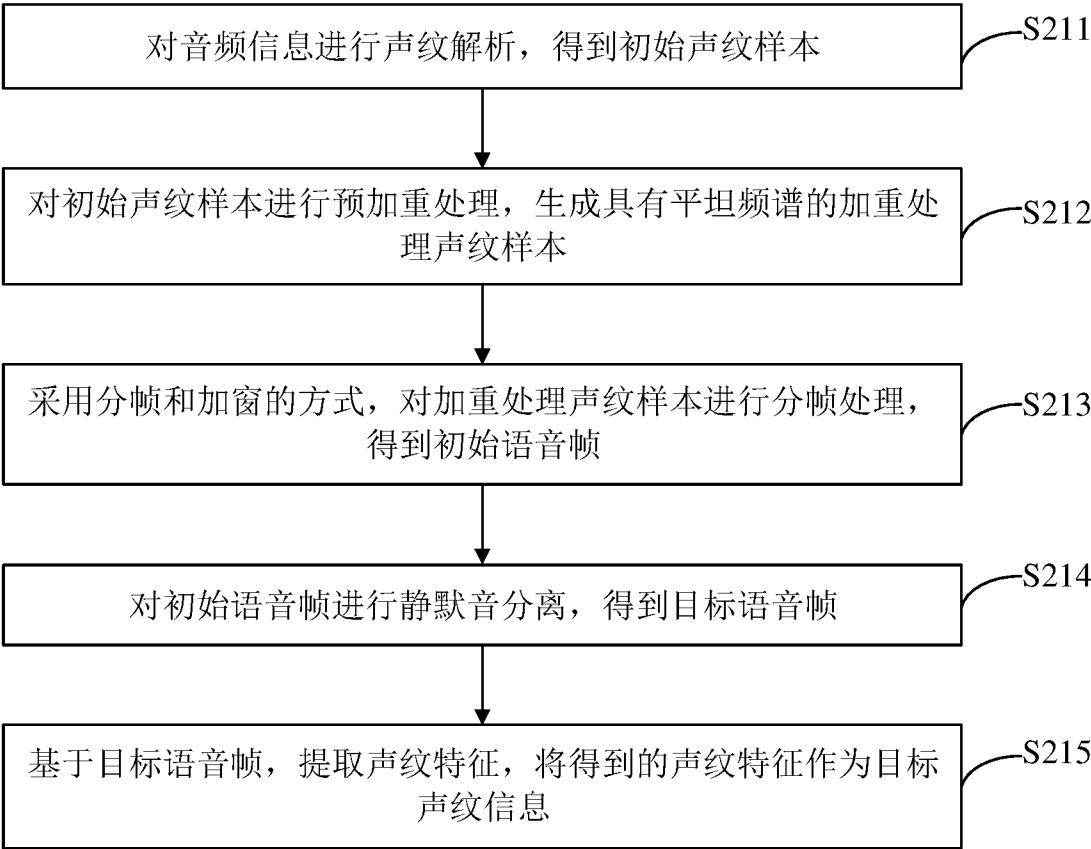


图 5

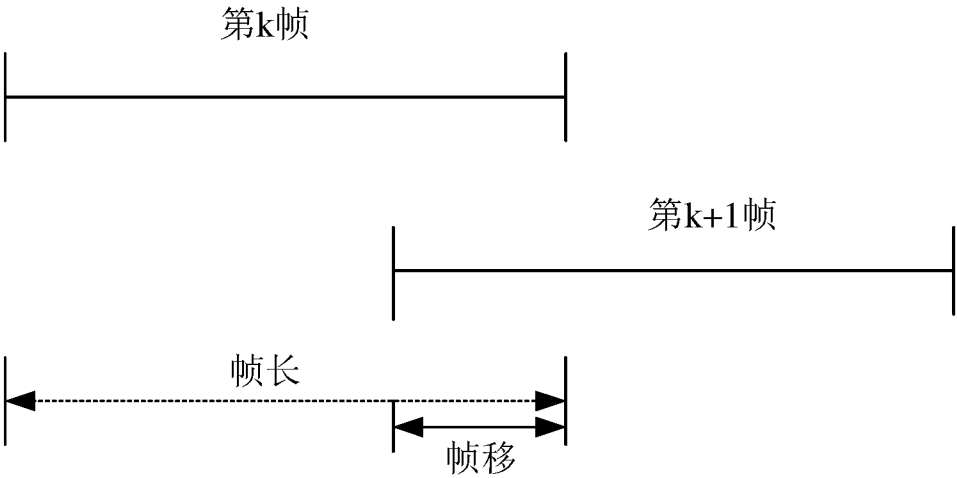


图 6

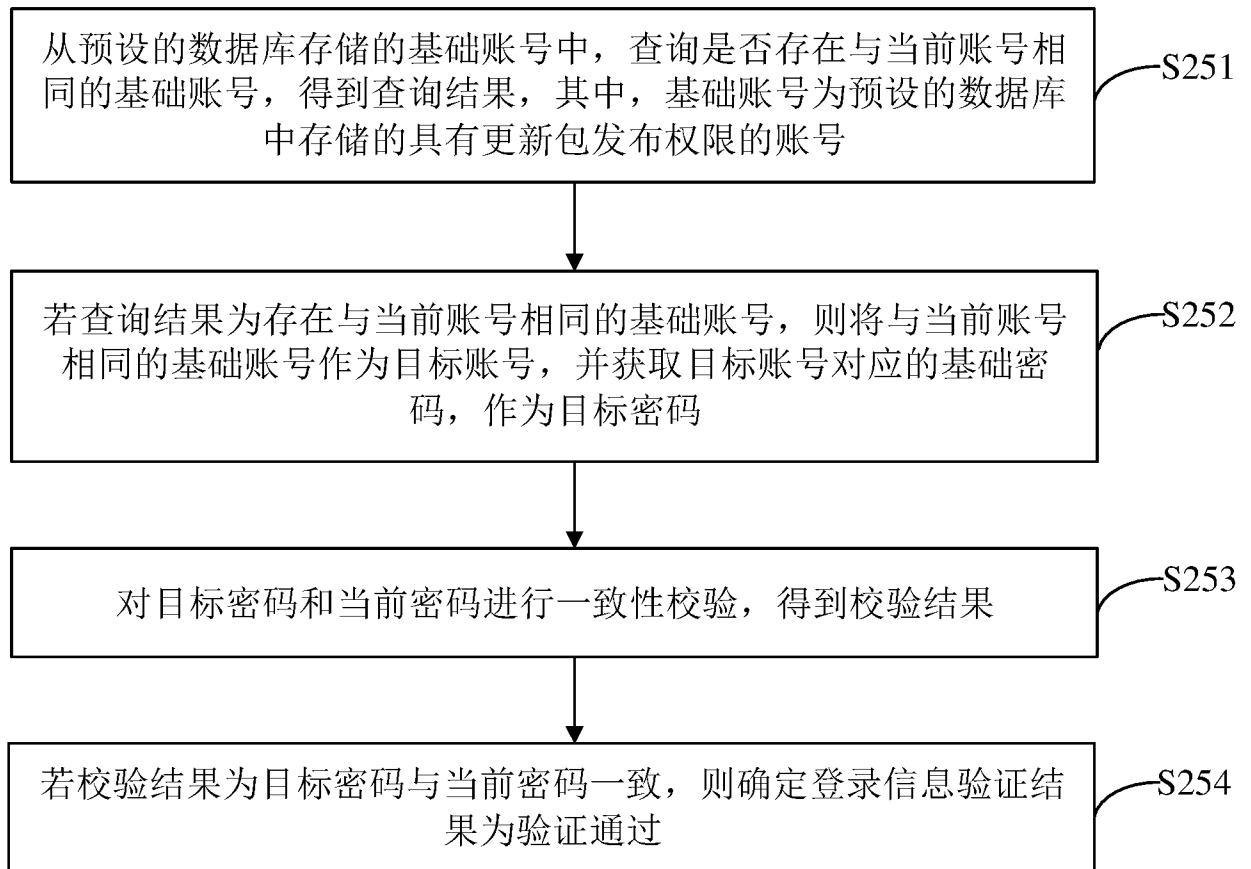


图 7

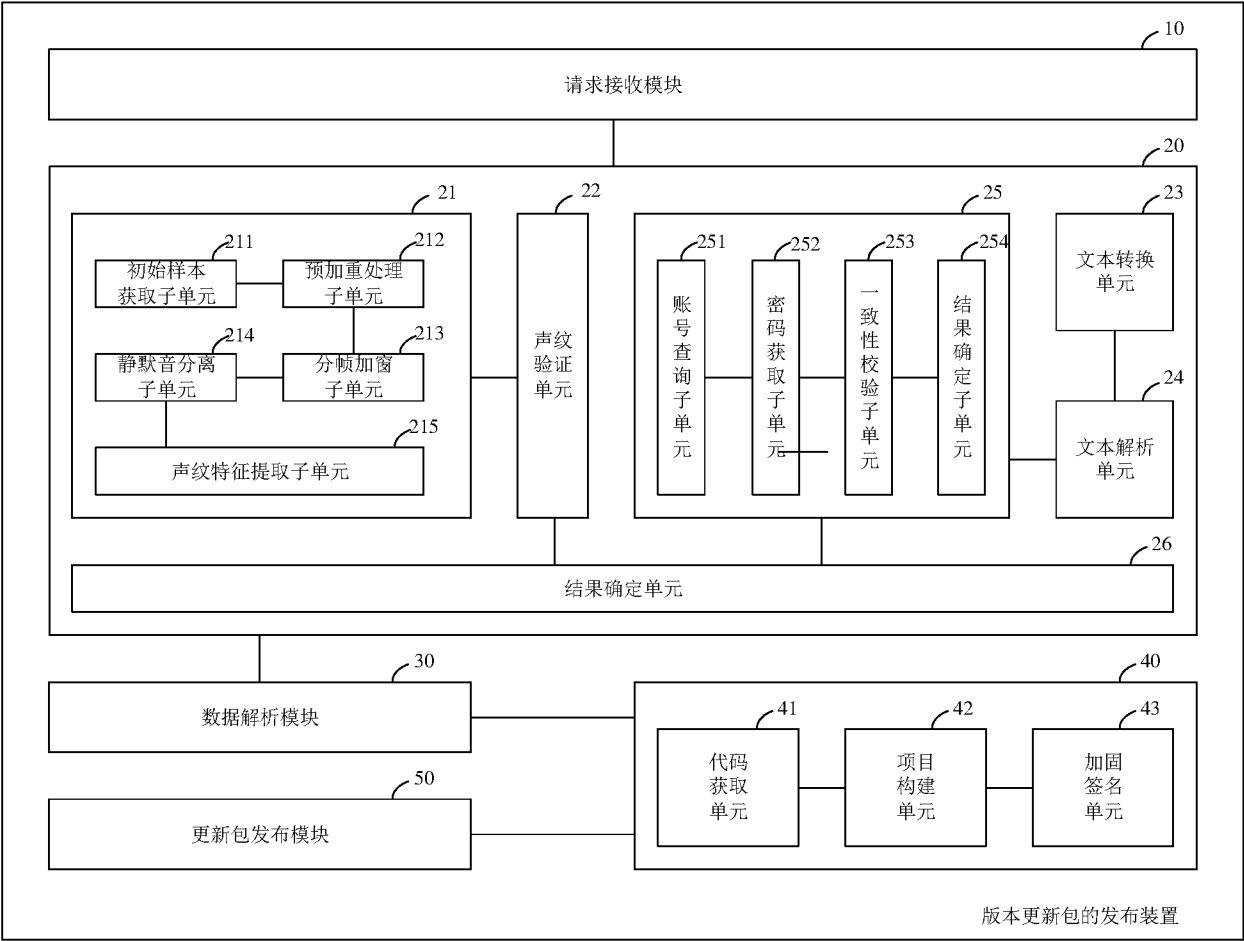


图 8

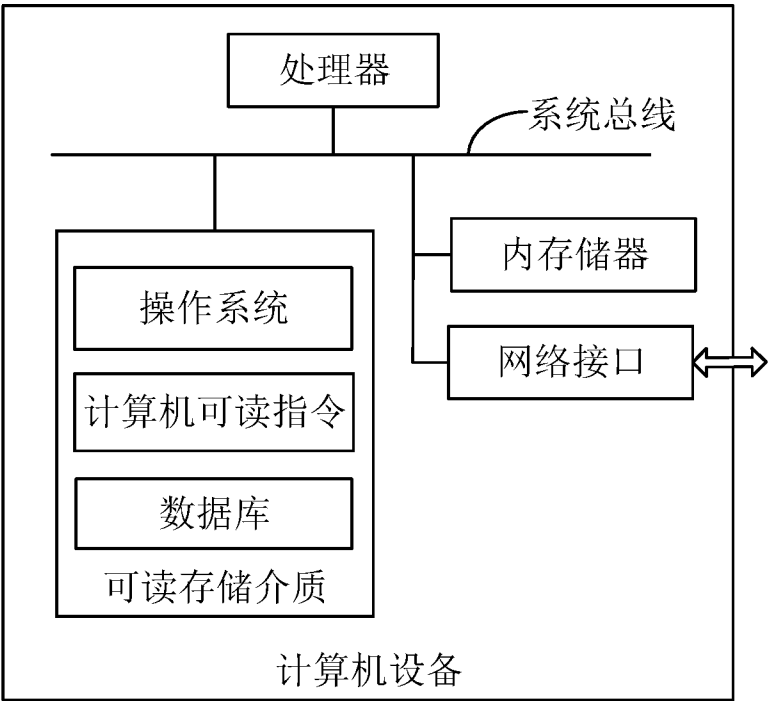


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/119957

A. CLASSIFICATION OF SUBJECT MATTER G06F 8/60(2018.01)i; G06F 8/65(2018.01)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) G06F 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) CNPAT, CNKI, WPI, EPODOC: 版本, 更新, 请求, 验证, 权限, 声纹, version, update, verif+, authority, voiceprint		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110083365 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 02 August 2019 (2019-08-02) claims 1-10, and description, paragraphs 31-181	1-20
Y	CN 108874409 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 23 November 2018 (2018-11-23) description, paragraphs 101-121	1-20
Y	CN 108829439 A (TAIKANG INSURANCE GROUP CO., LTD. et al.) 16 November 2018 (2018-11-16) description, paragraphs 48-139	1-20
Y	CN 109473108 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 15 March 2019 (2019-03-15) description, paragraphs 35-119	2, 4-5, 7, 9-10, 12, 14-15, 17, 19-20
A	CN 108351771 A (MICROSOFT TECHNOLOGY LICENSING LLC) 31 July 2018 (2018-07-31) entire document	1-20
A	CN 109117178 A (PING AN LIFE INSURANCE COMPANY OF CHINA) 01 January 2019 (2019-01-01) entire document	1-20
☒ 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 19 February 2020		Date of mailing of the international search report 26 February 2020
Name and mailing address of the ISA/CN China National Intellectual Property Administration No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088 China Facsimile No. (86-10)62019451		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/119957

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018316508 A1 (INTEL CORPORATION) 01 November 2018 (2018-11-01) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/119957

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110083365	A	02 August 2019	None			
CN	108874409	A	23 November 2018	None			
CN	108829439	A	16 November 2018	None			
CN	109473108	A	15 March 2019	None			
CN	108351771	A	31 July 2018	US	2017134476	A1	11 May 2017
				EP	3371698	A1	12 September 2018
				WO	2017079615	A1	11 May 2017
				US	2019058753	A1	21 February 2019
CN	109117178	A	01 January 2019	None			
US	2018316508	A1	01 November 2018	WO	2017095565	A1	08 June 2017
				US	2017155514	A1	01 June 2017

国际检索报告

国际申请号

PCT/CN2019/119957

A. 主题的分类 G06F 8/60(2018.01)i; G06F 8/65(2018.01)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) G06F 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)) CNPAT, CNKI, WPI, EPDOC: 版本, 更新, 请求, 验证, 权限, 声纹, version, update, verif+, authority, voiceprint		
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
PX	CN 110083365 A (深圳壹账通智能科技有限公司) 2019年 8月 2日 (2019 - 08 - 02) 权利要求1-10, 说明书第31-181段	1-20
Y	CN 108874409 A (腾讯科技深圳有限公司) 2018年 11月 23日 (2018 - 11 - 23) 说明书第101-121段	1-20
Y	CN 108829439 A (泰康保险集团股份有限公司 等) 2018年 11月 16日 (2018 - 11 - 16) 说明书第48-139段	1-20
Y	CN 109473108 A (深圳壹账通智能科技有限公司) 2019年 3月 15日 (2019 - 03 - 15) 说明书第35-119段	2, 4-5, 7, 9-10, 12, 14-15, 17, 19-20
A	CN 108351771 A (微软技术许可有限责任公司) 2018年 7月 31日 (2018 - 07 - 31) 全文	1-20
A	CN 109117178 A (中国平安人寿保险股份有限公司) 2019年 1月 1日 (2019 - 01 - 01) 全文	1-20
A	US 2018316508 A1 (INTEL CORP.) 2018年 11月 1日 (2018 - 11 - 01) 全文	1-20
☐ 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 “E” 在国际申请日的当天或之后公布的在先申请或专利 “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) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “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 “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 “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 “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 “&” 同族专利的文件		
国际检索实际完成的日期 2020年 2月 19日		国际检索报告邮寄日期 2020年 2月 26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 吴黄飞 电话号码 86-(10)-53961430

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/119957

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	110083365	A	2019年 8月 2日	无			
CN	108874409	A	2018年 11月 23日	无			
CN	108829439	A	2018年 11月 16日	无			
CN	109473108	A	2019年 3月 15日	无			
CN	108351771	A	2018年 7月 31日	US	2017134476	A1	2017年 5月 11日
				EP	3371698	A1	2018年 9月 12日
				WO	2017079615	A1	2017年 5月 11日
				US	2019058753	A1	2019年 2月 21日
CN	109117178	A	2019年 1月 1日	无			
US	2018316508	A1	2018年 11月 1日	WO	2017095565	A1	2017年 6月 8日
				US	2017155514	A1	2017年 6月 1日