(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
2018 年 4 月 19 日 (19.04.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/068633 A1

(51) 国际专利分类号:
G06F 21/14 (2013.01)

(21) 国际申请号: PCT/CN2017/103403

(22) 国际申请日: 2017 年 9 月 26 日 (26.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610887188.5 2016年10月11日 (11.10.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司(ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层847号邮箱, Grand Cayman (KY)。

(72) 发明人; 及

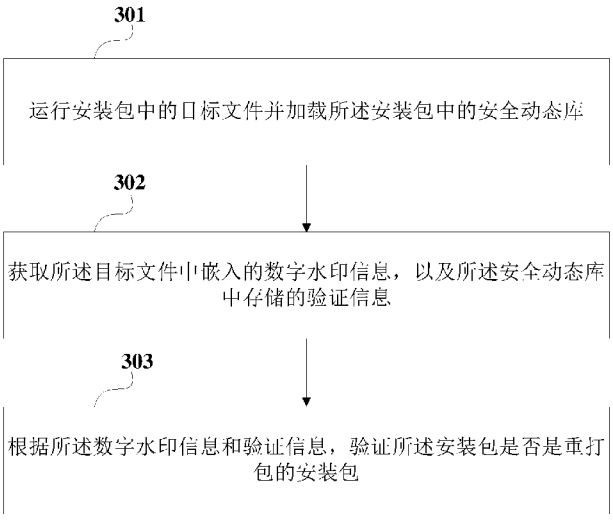
(71) 申请人 (仅对*US*): 陈耀光(CHEN, Yaoguang) [CN/CN]; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 王加水(WANG, Jiashui) [CN/CN]; 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司(CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲2号渔阳置业大厦B座605, Beijing 100029 (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, 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。

(54) **Title:** SOFTWARE REPACKAGING PREVENTION METHOD AND DEVICE

(54) **发明名称**: 一种防重打包的方法及其装置



301 Operate a target file in an installation package, and load a security dynamic library in the installation package

302 Execute codes in the target file to perform the following step: acquiring digital watermark information embedded in the target file, and verification information stored in the security dynamic library

303 Verify, according to the digital watermark information and the verification information, whether the installation package is a repackaged installation package

图 3

(57) **Abstract:** A software repackaging prevention method and device. The method comprises: operating a target file in an installation package, and loading a security dynamic library in the installation package (301); executing codes in the target file to perform the following step: acquiring digital watermark information embedded in the target file, and verification information stored in the security dynamic library (302); and verifying, according to the digital watermark information and the verification information, whether the installation package is a repackaged installation package (303). The method resolves problems of low verification efficiency, and being unable to effectively verify whether an installation package is repackaged.

WO 2018/068633 A1

[见续页]

(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：一种防重打包的方法及其装置，所述方法包括：运行安装包中的目标文件并加载安装包中的安全动态库（301）；根据目标文件中的代码执行下述步骤：获取目标文件中嵌入的数字水印信息，以及安全动态库中存储的验证信息（302）；根据数字水印信息和验证信息，验证安装包是否是重打包的安装包（303）。所述方法解决了无法有效地验证安装包是否被重打包、以及验证效率低的问题。

一种防重打包的方法及其装置

技术领域

本申请涉及计算机技术领域，尤其涉及一种防重打包的方法及其装置。

背景技术

目前，许多恶意应用软件通过重打包的方式修改原始的安装包，在原始的安装包中嵌入广告、自动下载恶意软件以及实现 root 等程序。

重打包的过程如图 1 所示：首先，对原始安装包进行反编译，获得该原始安装包的源代码，然后，用户对该源代码进行修改，例如，添加其他代码，添加的代码可以是广告，也可以是自动下载恶意软件的程序，等等，最后，对修改后的文件进行重打包，获得重打包的安装包。

由于上述重打包的过程中对源代码进行了修改，因此，重打包的安装包的自签名，不再是原始安装包的自签名。因此，现有技术中，防重打包的方法就可以通过校验安装包的自签名，从而判断该安装包是否是被重打包，具体验证过程如图 2 所示：

当某安装包被安装时，该安装包中的目标文件就会被运行，同时，在该安装包中的安全动态库也会被加载，通常，为了保证信息的安全性，会将一些验证信息存储在安全动态库中，该验证信息包括：该安装包对应的原始安装包的自签名。由于操作系统提供了验证安装包自签名的接口，因此，操作系统从该目标文件中获取该安装包的自签名，以及从该安全动态库中获取原始安装包的自签名后，验证该安装包的自签名与该原始安装包的自签名是否一致，若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

现有技术中，防重打包的方法还可以是：操作系统计算本次安装的安装包的哈希（hash）值，并对该哈希值进行校验，具体地，将该哈希值与原始安装包的哈希值进行对比，若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

上述两种现有技术中的防重打包方法，必须建立在完全信任的操作系统下，才能有效的防止重打包的情形，但由于目前很多操作系统具有开源性，因此，用户可以对原有的操作系统进行改造，使操作系统不进行校验安装包自签名的过程，以及不进行校验安装包哈希值的过程，这样，无论用户下载的安装包是否是经过重打包的安装包，操作系统都会默认该安装包是原始安装包。

另外，上述第二种防重打包的方法中，有时待安装的安装包占用的内存会很大，这样，操作系统在计算该安装包的哈希值时，会影响操作系统的验证效率。

发明内容

鉴于上述问题，本申请提供了一种防重打包的方法及其装置，用于解决现有技术中在系统通过校验安装包自签名，有时无法有效地验证该安装包是否被重打包的问题，以及解决现有技术中系统通过计算安装包的哈希值来校验安装包是否被重打包时，有时由于安装包占用内存较大，导致验证效率较低的问题。

本申请提供了一种防重打包的方法，该方法包括：

运行安装包中的目标文件并加载所述安装包中的安全动态库；

根据所述目标文件中的代码执行下述步骤：

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息；

根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

相应地，本申请还提供了一种防重打包的装置，该装置包括：

运行单元和执行单元，其中：

所述运行单元，运行安装包中的目标文件并加载所述安装包中的安全动态库；

所述执行单元，根据所述目标文件中的代码执行下述步骤：

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息；

根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

本申请提供防重打包的方法中，安装包本身包含有验证代码，当该安装包被安装时，操作系统就会根据该代码，获取该目标文件中嵌入的数字水印信息，以及获取该安装包中的安全动态库中的验证信息，并根据该数字水印信息和该验证信息，验证该安装包是否是重打包的安装包。采用本申请提供的防重打包的方法，获得的有益效果如下：

1、由于本申请中安装包本身包含有用于验证该安装包是否被重打包的代码，因此，无论对操作系统如何改造，也无法避开验证安装包的过程，解决了现有技术通过系统校验安装包自签名来验证安装包是否被重打包时，由于系统有时会绕过验证安装自签名的过程，导致无法有效地验证该安装包是否被重打包的问题。

2、由于本申请是根据数字水印信息和验证信息，验证该安装包是否被重打包，因此，相比于现有技术通过计算安装包哈希值来验证安装包是否被重打包的方法，本申请验证安装包是否被重打包的效率更高。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为现有技术提供的一种重打包的方法的流程示意图；

图 2 为现有技术提供的一种防重打包的方法的流程示意图；

图 3 为本申请实施例提供的一种防重打包的方法的流程示意图；

图 4 为本申请实施例提供的在目标文件中嵌入数字水印信息的流程示意

图；

图 5 为本申请实施例提供的另一种防重打包的方法的流程示意图；

图 6 为本申请实施例提供的查找数字水印信息的方法的流程示意图；

图 7 为本申请实施例提供的再一种防重打包的方法的流程示意图；

图 8 为本申请实施例提供的又一种防重打包的方法的流程示意图；

图 9 为本申请实施例提供的一种防重打包的装置的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例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。

以下结合附图，详细说明本申请各实施例提供的技术方案。

本申请提供了一种防重打包的方法，用于解决现有技术中在系统通过校验安装包自签名，有时无法有效地验证该安装包是否被重打包的问题，以及解决现有技术中系统通过计算安装包的哈希值来校验安装包是否被重打包时，有时由于安装包占用内存较大，导致验证效率较低的问题。该方法的具体流程如图 3 所示，具体包括以下步骤：

步骤 301：运行安装包中的目标文件并加载所述安装包中的安全动态库。

在本步骤中，当用户下载了某个安装包，并对该安装包进行安装时，操作系统就会运行该安装包中的目标文件，并同时加载该安装包中的安全动态库。该目标文件是根据预设的代码编译后得到的目标文件，且在编译后的目标文件中嵌入了数字水印信息。该数字水印信息可以是字符串，还可以是指令，等等，该安全动态库中存储有关该安装包的验证信息，该验证信息用于验证该安装包是否是重打包的安装包。

上述在目标文件中嵌入数字水印信息的方式，可以是在目标文件的末尾嵌入该数字水印信息，或者是在目标文件的其他的位置上嵌入该数字水印信息。

上述操作系统可以是安卓系统，则目标文件可以是 dex 文件，该 dex 文件具体为安卓系统下可执行文件的类型，采用 java 代码编写而成，安全动态库可以是 so 库，采用 c/c++编写而成，通常 so 库里保存有一些安全信息，例如，验证信息，当可执行的文件加载或运行时，由操作系统加载 so 库；或者，该操作系统可以是 windows，则目标文件可以是 exe 文件，安全动态库为 dll 库，等等，这里不对该操作系统、目标文件以及动态安全库进行限定。

如图 4 所示，如果该目标文件是 dex 文件，在该目标文件中嵌入数字水印信息时，为了保证该目标文件数据的完整性和准确性，会根据该数字水印信息，重新计算该目标文件头部的校验总和（checksum）、签名（signature）、文件大小（filesize）等对应的值。

需要说明的是：如果该安装包是重打包的安装包，用户在对原始安装包进行重打包时，虽然用户可以修改原始安装包中原始文件的代码，但该原始安装包的安全动态库中的验证信息却不容易被修改，因此，该安装包的安全动态库中仍会保存有原始安装包的验证信息。假设该原始安装包中也嵌入了数字水印信息，则存储在安全动态库中的验证信息可以是嵌入该原始文件中的数字水印信息，具体原因如图 5 所示：

当对原始安装包重打包时，需要先将该原始安装包进行反编译，获得该原始安装包对应的源代码文件，由于数字水印信息是在根据预设代码编译成原始文件后，才嵌入到该原始文件中的，因此，在对原始安装包反编译的过程中，该数字水印信息 A 将会丢失，然后，用户对源代码文件进行修改，如图 5 所示，可以是添加其他代码，同时，用户为了伪装该安装包重打包的身份，还会在源代码文件中嵌入数字水印信息 B，最后，对该源代码文件进行重打包，重打包后的安装包的安全动态库中仍存储有验证信息 A。因此，可以将数字水印信息 A 可以作为原始安装包的标识，用于验证该安装包是否被重打包。

为了清楚地说明本申请实施例，下面就以在目标文件的末尾嵌入数字水印信息为例，说明本申请实施例中的各个步骤。

步骤 302：根据所述目标文件中的代码执行下述步骤：

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息，并根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

在本步骤中，操作系统根据目标文件中的代码，获取目标文件的数字水印信息的方法如图 6 所示：根据目标文件的原始长度，确定数字水印信息在该目标文件中的起始地址，并根据该起始地址，从该目标文件中获取该数字水印信息，这里的目标文件的原始长度为在嵌入数字水印信息前该目标文件的长度。

当操作系统获得该数字水印信息，以及从安全动态库中获取验证信息后，根据该数字水印信息和验证信息，验证该安装包是否是重打包的安装包，具体的验证方法可以由数字水印信息的类型来决定，如表 1 所示：

数字水印信息的类型	验证方法
固定长度的字符串	直接验证该字符串是否与验证信息一致
	验证水印值是否与验证信息一致
随机长度的字符串	先计算随机字符串的长度，再验证该字符串是否与验证信息一致
指令	验证该指令与验证信息是否一致
	验证操作结果与验证信息是否一致
	验证操作结果与验证信息中的操作结果是否一致，以及验证指令与验证信息中的指令是否一致
……	

表 1

当数字水印信息为字符串时，验证该数字水印信息与验证信息是否一致，

若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

在实际应用中，如果数字水印信息为字符串，该字符串可能是固定长度的字符串，也可能是随机长度的字符串。当数字水印信息为固定长度的字符串时，直接验证该字符串与安全动态库中的验证信息是否一致；或者计算当前下载安装包对应的水印值与安全动态库中的验证信息是否一致，如图 7 所示为 dex 文件中通过计算水印值来验证安装包是否被重打包的方法，具体如下：

Dex 文件包括 dex header 和 dex body，其中，dex header 中包含 data size 和 data off，dex body 中包含 data，且 data size 表示该 data 的大小，data off 表示该 data 的偏移。假设在原始 dex 文件中嵌入了数字水印信息，当对该原始 dex 文件进行重打包时，具体是将 dex body 中 data 部分对应的代码进行修改，修改后，不仅嵌入在原始 dex 文件中的数字水印信息将会丢失，而且 data 的大小将会发生改变，则 dex header 中 data size 对应的值会发生变化；对该原始 dex 文件进行重打包，还可以是对 dex body 中除了 data 以外其它部分对应的代码进行修改，修改后，同样嵌入在原始 dex 文件中的数字水印信息将会丢失，而且 dex body 中 data 的位置会发生偏移（如图 7 所示），则 dex header 中 data off 对应的值会发生变化。

假设原始安装包对应水印值的计算方法为“data size +data off”，即水印值为 data size 对应的值加 data off 对应的值。当用户对该原始安装包重打包时，data off 或 data size 对应的值就会发生改变，则重打包的安装包对应的水印值也会发生变化，这时，操作系统只要验证重打包的安装包对应的水印值与安全动态库中的验证信息是否一致，就可以确定出该安装包是否是被重打包。这里水印值的计算方法只是示例性的说明，在实际应用中，可以根据实际情况进行设定水印值的计算方法，例如，可以是“data size-data off”，或者是“data size/data off”，等等。

利用上述方法验证当前下载安装包是否被重打包时，即使是在重打包的安

装包中嵌入原始安装包中的数字水印信息，该安装包对应的水印值也会发生变化，因此，操作系统根据该安装包的水印值可以准确地判断出该安装包是否被重打包。

当数字水印信息为随机长度的字符串时，可以先计算该字符串的长度，然后，验证该字符串的长度是否与安全动态库中的验证信息的长度一致，若不一致，则直接确定该安装包是重打包的安装包，若一致，再验证该字符串与安全动态库中的验证信息是否一致，若仍一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

当数字水印信息为指令时，验证安全包的方法有很多种，下面示例性的说明三种验证方法:

第一种方法，与上述数字水印信息为字符串时验证安装包的方法类似，即:操作系统验证该指令与安全动态库中的验证信息是否一致，若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

第二种方法，操作系统根据该指令执行相应操作，获得操作结果，然后，验证该操作结果与验证信息是否一致，若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

例如，该指令可以是“查询 XX 地址中内容，是否与安全动态库中的验证信息一致”，操作系统根据该指令，从目标文件中的 XX 地址中，查询该地址对应的内容（操作结果），并验证该内容是否与安全动态库中的验证信息一致，若一致，则确定该安装包是原始安装包，若不一致，则确定该安装包是重打包的安装包。

第三种方法，操作系统根据该指令执行相应操作，获得操作结果，验证该操作结果与该验证信息中的操作结果是否一致，以及验证该指令与该验证信息中的指令是否一致，若两次验证的结果均为“一致”，则确定该安装包是原始安装包，若两次验证中任一次验证的结果为“不一致”，或者是两次验证的结果均为“不一致”，则确定该安装包是重打包的安装包。

为了清楚地说明该验证方法，这里通过一个简单的例子来说明该验证方法，假设安全动态库中验证信息中的操作结果为“2”，操作指令为“1+1”，而目标文件中的数字水印信息对应的指令为“3-1”，操作系统根据该指令执行操作后，获得的操作结果也为“2”，如果操作系统只验证该操作结果与验证信息中的操作结果是否一致，就会误认为该装包是原始安装包，但如果操作系统还验证指令与验证信息中的指令是否一致，就会准确地判断出该安装包是否被重打包。

上述目标文件中数字水印信息对应的指令可以是简单的“返回”指令，或者是其他实现与操作系统之间交互的指令，例如，该指令可以是“让操作系统验证目标文件自签名与安全动态库中的验证信息是否一致”，再例如，该指令还可以是“让操作系统验证嵌入数字水印信息前目标文件的长度，与安全动态库中的保存的验证信息是否一致”，等等，可以根据用户的需求进行设定指令。

另外，如果该安装包是重打包的安装包，还可能存在这样一种情形：该安装包对应的原始文件中嵌入了数字水印信息，由前述内容可知，在对该原始安装包重打包的过程中，将会丢失原始安装包中的数字水印信息，如果用户在对该原始文件的代码修改后，没有相应地加入数字水印信息，这时，操作系统只要根据该安装包中的代码，查询该安装包中的目标文件中是否具有该数字水印信息即可。

上述验证安装包的方法只是示例性的说明，在实际应用中，数字水印信息的类型有很多种，对应的验证方法也会有很多种，这里不作具体限定。

本申请提供防重打包的方法中，安装包本身包含有验证代码，当该安装包被安装时，如图 8 所示，操作系统就会根据该代码，获取该安装包中的安全动态库中的验证信息，以及获取该目标文件中嵌入的数字水印信息，并根据该数字水印信息和该验证信息，验证该安装包是否是重打包的安装包。采用本申请提供的防重打包的方法，获得的有益效果如下：

1、由于本申请中安装包本身包含有用于验证该安装包是否被重打包的代

码，因此，无论对操作系统如何改造，也无法避开验证安装包的过程，解决了现有技术通过系统校验安装包自签名来验证安装包是否被重打包时，由于系统有时会绕过验证安装自签名的过程，导致无法有效地验证该安装包是否被重打包的问题。

2、由于本申请是根据数字水印信息和验证信息，验证该安装包是否被重打包，因此，相比于现有技术通过计算安装包哈希值来验证安装包是否被重打包的方法，本申请验证安装包是否被重打包的效率更高。

相应地，本申请还提供了一种防重打包的装置，同样用于解决现有技术中在系统通过校验安装包自签名，有时无法有效地验证该安装包是否被重打包的问题，以及解决现有技术中系统通过计算安装包的哈希值来校验安装包是否被重打包时，有时由于安装包占用内存较大，导致验证效率较低的问题。该装置的具体结构如图 9 所示，具体包括以下单元:

运行单元 901 和执行单元 902，其中:

所述运行单元 901，运行安装包中的目标文件并加载所述安装包中的安全动态库;

所述执行单元 902，根据所述目标文件中的代码执行下述步骤:

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息;

根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

本装置实施例的工作流程是: 首先，运行单元 901 运行安装包中的目标文件，并加载该安装包中的安全动态库，其次，执行单元 902，根据该目标文件中的代码执行下述步骤: 获取该目标文件中嵌入的数字水印信息，以及该安全动态库中存储的验证信息，根据该数字水印信息和验证信息，验证该安装包是否是重打包的安装包。

本装置实施例实现防重打包的方式有很多种，例如，在第一种实施方式中，

所述目标文件是将预设的代码进行编译后得到的目标文件；所述数字水印信息是在编译后得到的目标文件中的末尾嵌入的。

在第二种实施方式中，获取所述目标文件中嵌入的数字水印信息，具体包括：

根据所述目标文件的原始长度，确定所述数字水印信息在所述目标文件中的起始地址，其中，所述原始长度为嵌入所述数字水印信息前所述目标文件的长度；

根据所述起始地址，从所述目标文件中获取所述数字水印信息。

在第三种实施方式中，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括：

验证所述数字水印信息与验证信息是否一致；

若一致，则确定所述安装包是原始安装包；

若不一致，则确定所述安装包是重打包的安装包。

在第四种实施方式中，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括：

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果；

验证所述操作结果与验证信息是否一致；

若一致，则确定所述安装包是原始安装包；

若不一致，则确定所述安装包是重打包的安装包。

在第五种实施方式中，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括：

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果；

验证所述操作结果与所述验证信息中的操作结果是否一致，以及验证所述指令与所述验证信息中的指令是否一致；

若均一致，则确定所述安装包是原始安装包；

否则，则确定所述安装包是重打包的安装包。

应用本装置实施例获得的有益效果与前述方法实施例获得的有益效果相同或类似，为避免重复，这里不再赘述。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。

内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种防重打包的方法，其特征在于，该方法包括:

运行安装包中的目标文件并加载所述安装包中的安全动态库;

根据所述目标文件中的代码执行下述步骤:

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息;

根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

2、根据权利要求 1 所述的方法，其特征在于，所述目标文件是将预设的代码进行编译后得到的目标文件;

所述数字水印信息是在编译后得到的目标文件中的末尾嵌入的。

3、根据权利要求 2 所述的方法，其特征在于，获取所述目标文件中嵌入的数字水印信息，具体包括:

根据所述目标文件的原始长度，确定所述数字水印信息在所述目标文件中的起始地址，其中，所述原始长度为嵌入所述数字水印信息前所述目标文件的长度;

根据所述起始地址，从所述目标文件中获取所述数字水印信息。

4、根据权利要求 1 所述的方法，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

验证所述数字水印信息与验证信息是否一致;

若一致，则确定所述安装包是原始安装包;

若不一致，则确定所述安装包是重打包的安装包。

5、根据权利要求 1 所述的方法，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果;

验证所述操作结果与验证信息是否一致;

若一致，则确定所述安装包是原始安装包;

若不一致，则确定所述安装包是重打包的安装包。

6、根据权利要求 1 所述的方法，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果;

验证所述操作结果与所述验证信息中的操作结果是否一致，以及验证所述指令与所述验证信息中的指令是否一致;

若均一致，则确定所述安装包是原始安装包;

否则，则确定所述安装包是重打包的安装包。

7、根据权利要求 1-6 任一所述的方法，其特征在于，所述方法应用于安卓操作系统中;

所述目标文件为 dex 文件;

所述安全动态库为 so 库。

8、一种防重打包的装置，其特征在于，该装置包括:

运行单元和执行单元，其中:

所述运行单元，运行安装包中的目标文件并加载所述安装包中的安全动态库;

所述执行单元，根据所述目标文件中的代码执行下述步骤:

获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息;

根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包。

9、根据权利要求 8 所述的装置，其特征在于，所述目标文件是将预设的代码进行编译后得到的目标文件;

所述数字水印信息是在编译后得到的目标文件中的末尾嵌入的。

10、根据权利要求 9 所述的装置，其特征在于，获取所述目标文件中嵌入的数字水印信息，具体包括:

根据所述目标文件的原始长度，确定所述数字水印信息在所述目标文件中的起始地址，其中，所述原始长度为嵌入所述数字水印信息前所述目标文件的长度;

根据所述起始地址，从所述目标文件中获取所述数字水印信息。

11、根据权利要求 8 所述的装置，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

验证所述数字水印信息与验证信息是否一致;

若一致，则确定所述安装包是原始安装包;

若不一致，则确定所述安装包是重打包的安装包。

12、根据权利要求 8 所述的装置，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果;

验证所述操作结果与验证信息是否一致;

若一致，则确定所述安装包是原始安装包;

若不一致，则确定所述安装包是重打包的安装包。

13、根据权利要求 8 所述的装置，其特征在于，根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包，具体包括:

当所述数字水印信息为指令时，根据所述指令执行操作，获得操作结果;

验证所述操作结果与所述验证信息中的操作结果是否一致，以及验证所述指令与所述验证信息中的指令是否一致;

若均一致，则确定所述安装包是原始安装包;

否则，则确定所述安装包是重打包的安装包。

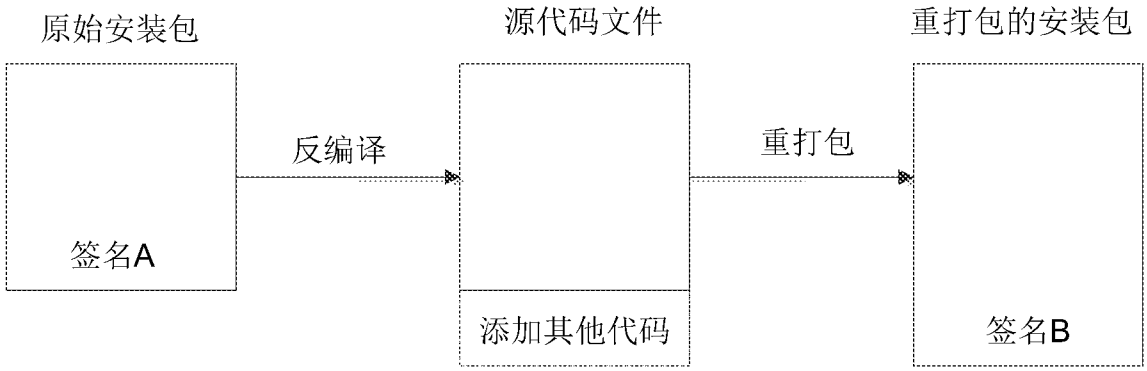

原始安装包
源代码文件
重打包的安装包
反编译
重打包
签名A
添加其他代码
签名B

图 1

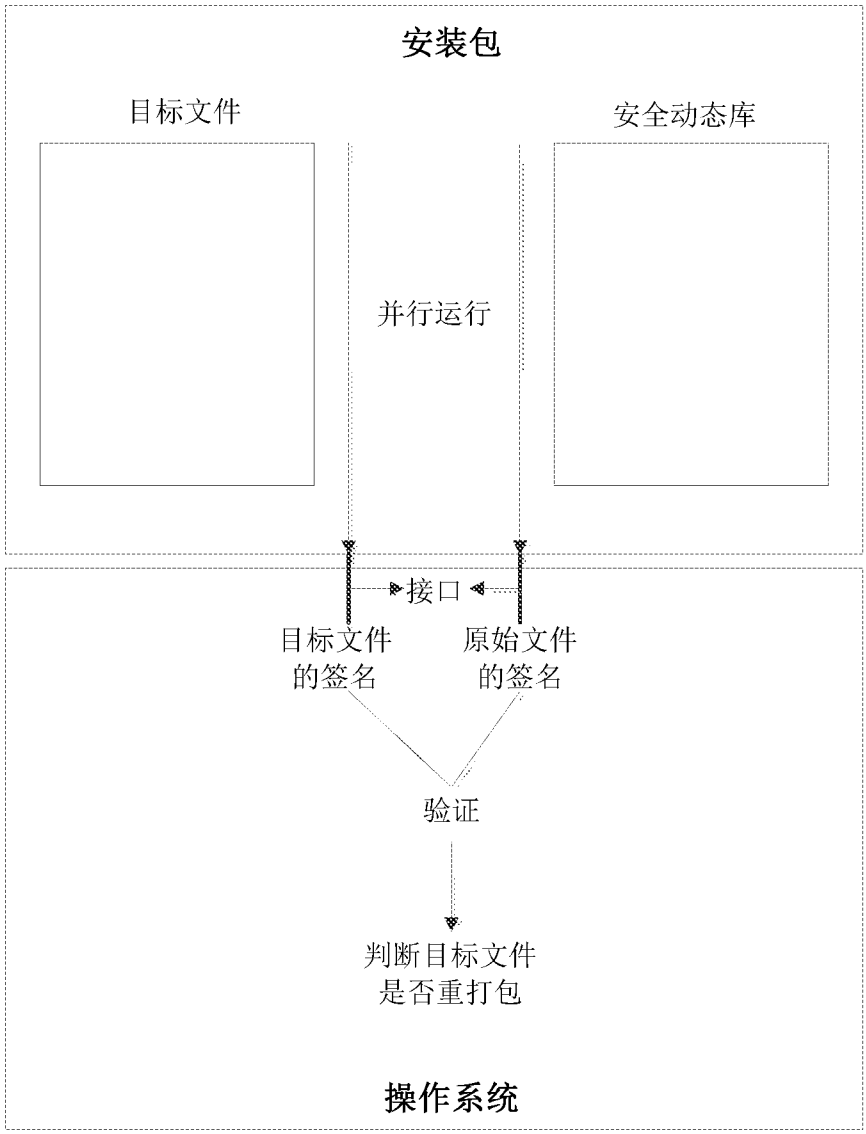

安装包
目标文件
安全动态库
并行运行
接口
目标文件
的签名
原始文件
的签名
验证
判断目标文件
是否重打包
操作系统

图 2

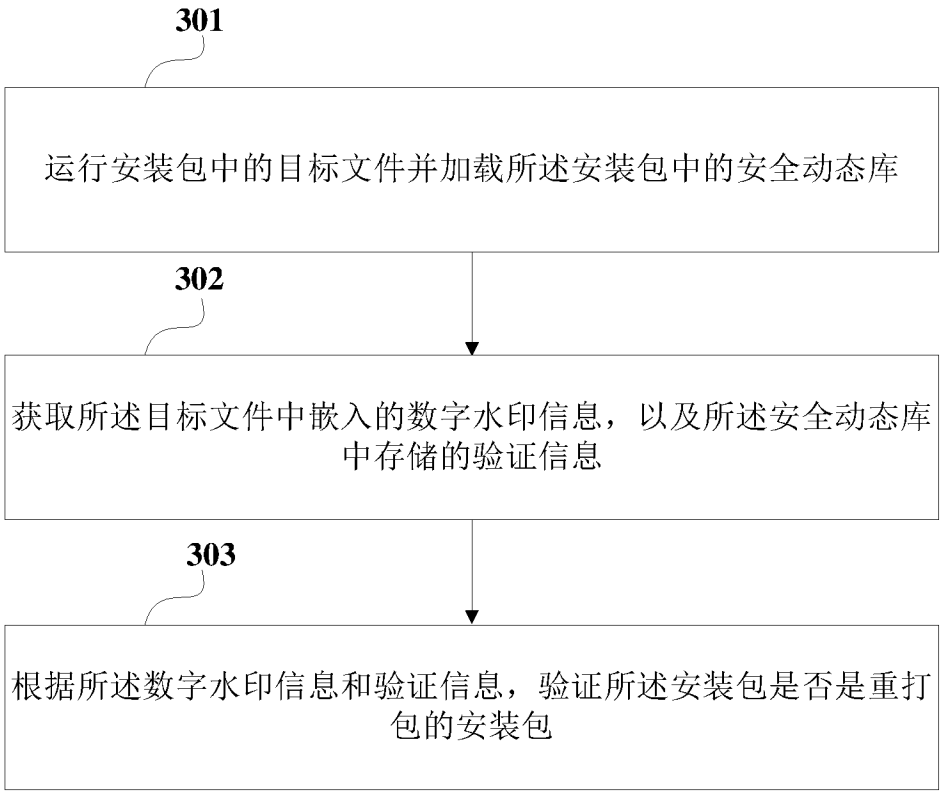

301
运行安装包中的目标文件并加载所述安装包中的安全动态库
302
获取所述目标文件中嵌入的数字水印信息，以及所述安全动态库中存储的验证信息
303
根据所述数字水印信息和验证信息，验证所述安装包是否是重打包的安装包

图 3

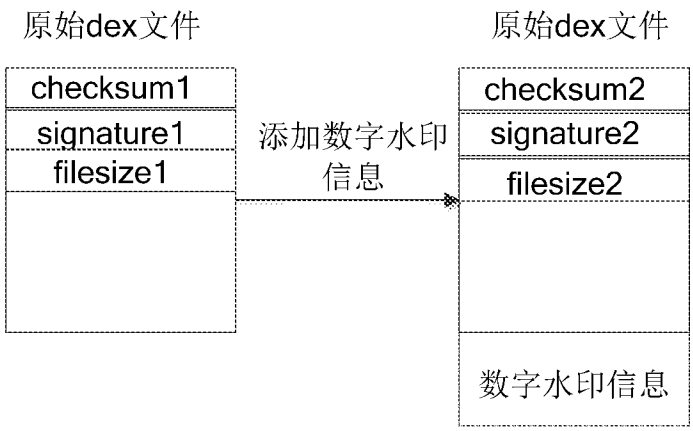

原始dex文件
checksum1
signature1
filesize1
添加数字水印信息
原始dex文件
checksum2
signature2
filesize2
数字水印信息

图 4

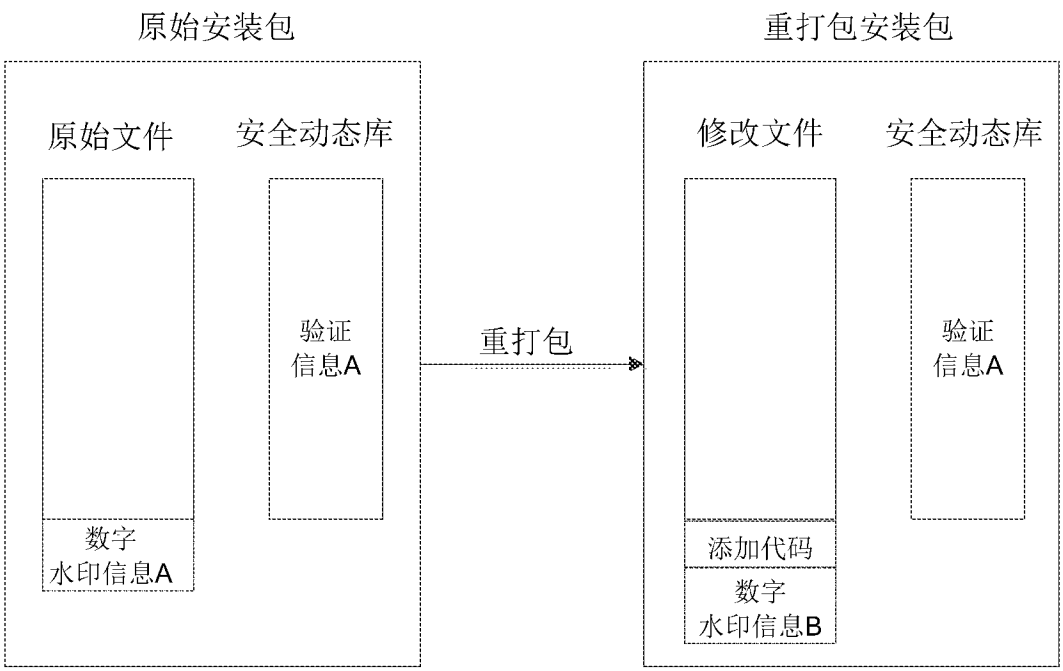

原始安装包
重打包安装包
原始文件
安全动态库
修改文件
安全动态库
验证
信息A
重打包
验证
信息A
数字
水印信息A
添加代码
数字
水印信息B

图 5

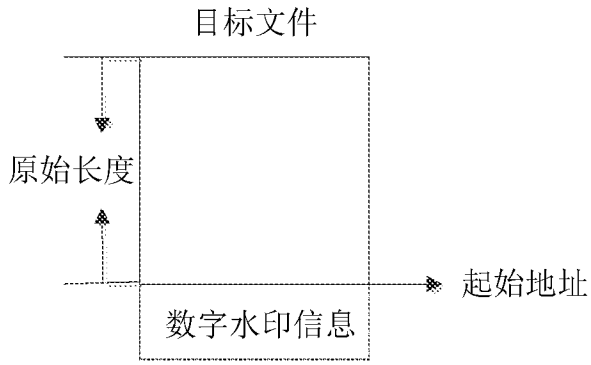

目标文件
原始长度
起始地址
数字水印信息

图 6

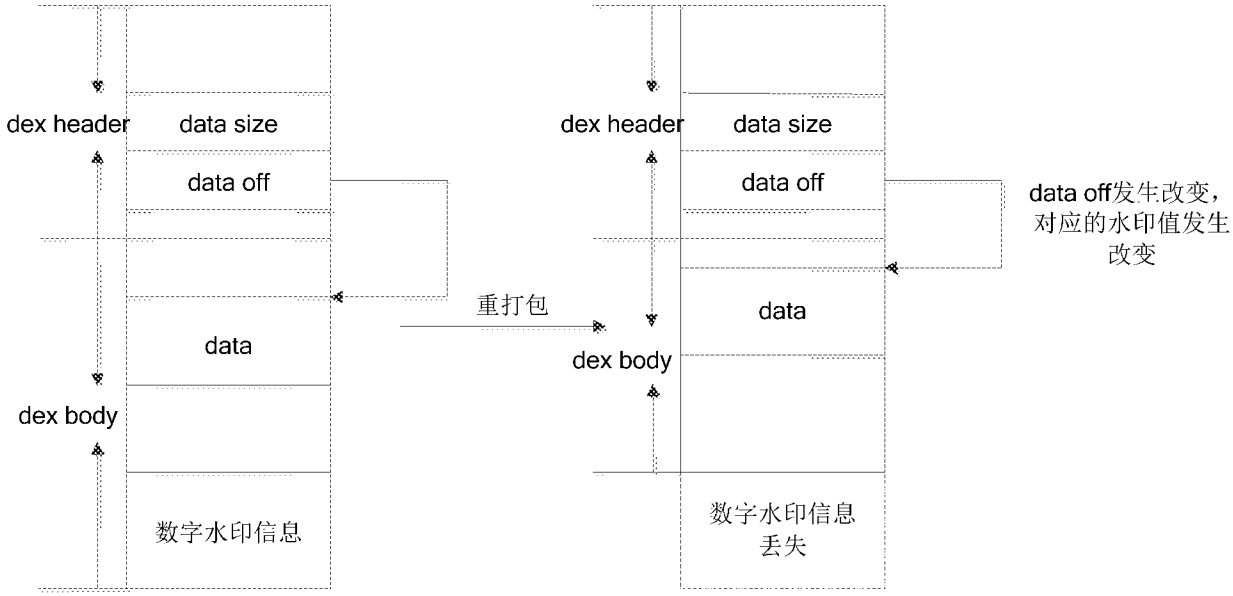

dex header
data size
data off
data
dex body
数字水印信息
重打包
dex header
data size
data off
data
dex body
数字水印信息
丢失
data off发生改变，
对应的水印值发生
改变

图 7

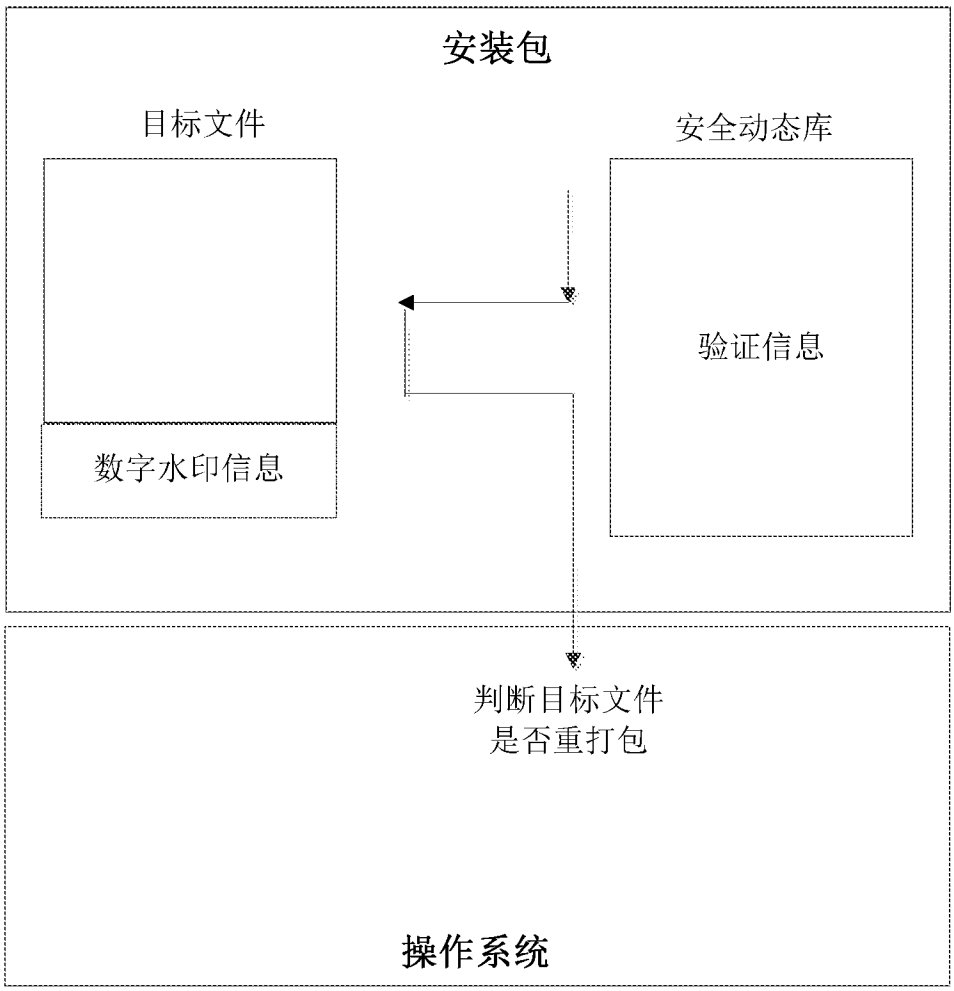

安装包
目标文件
数字水印信息
安全动态库
验证信息
判断目标文件
是否重打包
操作系统

图 8

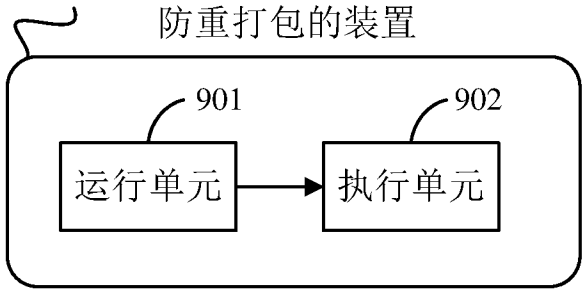


图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/103403

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/14 (2013.01) 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, WPI, EPODOC, IEEE, CNKI: 安装, 执 line, 打包, 文件, 安全库, 动态库, 水印, 嵌入, 插入, 验证, 调用, install, setup, file, package, dynamic, library, watermark, bed, embed, insert, validate, transfer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106971098 A (ALIBABA GROUP HOLDING LIMITED), 21 July 2017 (21.07.2017), claims 1-13	1-13
X	CN 104932902 A (MEIZU SCIENCE & TECHNOLOGY (CHINA) CO., LTD.), 23 September 2015 (23.09.2015), description, paragraphs [0004], [0055]-[0067] and [0094]	1-13
A	CN 104239757 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 24 December 2014 (24.12.2014), entire document	1-13
A	US 2013232540 A1 (SAIDI, H. et al.), 05 September 2013 (05.09.2013), entire document	1-13

☐ 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	Date of mailing of the international search report
02 November 2017	28 December 2017
Name and mailing address of the ISA 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 REN, Xingchao Telephone No. (86-10) 62413667

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/103403

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106971098 A	21 July 2017	None	
CN 104932902 A	23 September 2015	None	
CN 104239757 A	24 December 2014	None	
US 2013232540 A1	05 September 2013	US 2014380414 A1	25 December 2014
		US 2013232573 A1	05 September 2013

国际检索报告

国际申请号
PCT/CN2017/103403

A. 主题的分类

G06F 21/14(2013.01)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, WPI, EPODOC, IEEE, CNKI: 安装, 执行, 打包, 文件, 安全库, 动态库, 水印, 嵌入, 插入, 验证, 调用, install, setup, file, package, dynamic, library, watermark, bed, embed, insert, validate, transfer

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 106971098 A (阿里巴巴集团控股有限公司) 2017年 7月 21日 (2017-07-21) 权利要求1-13	1-13
X	CN 104932902 A (魅族科技中国有限公司) 2015年 9月 23日 (2015-09-23) 说明书第[0004]段, 第[0055]-[0067]段, 第[0094]段	1-13
A	CN 104239757 A (北京奇虎科技有限公司 等) 2014年 12月 24日 (2014-12-24) 全文	1-13
A	US 2013232540 A1 (SAIDI, HASSEN 等) 2013年 9月 5日 (2013-09-05) 全文	1-13

☐ 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	国际检索报告邮寄日期
2017年 11月 2日	2017年 12月 28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) 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 任兴超 电话号码 (86-10)62413667

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/103403

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	106971098	A	2017年 7月 21日	无			
CN	104932902	A	2015年 9月 23日	无			
CN	104239757	A	2014年 12月 24日	无			
US	2013232540	A1	2013年 9月 5日	US	2014380414	A1	2014年 12月 25日
				US	2013232573	A1	2013年 9月 5日