



(12)发明专利

(10)授权公告号 CN 104166565 B

(45)授权公告日 2017.10.17

(21)申请号 201410393291.5

H04L 9/32(2006.01)

(22)申请日 2014.08.11

(56)对比文件

(65)同一申请的已公布的文献号

申请公布号 CN 104166565 A

CN 101567962 A, 2009.10.28,

CN 101567962 A, 2009.10.28,

CN 101557308 A, 2009.10.14,

CN 101483870 A, 2009.07.15,

CN 103327403 A, 2013.09.25,

CN 101221511 A, 2008.07.16,

KR 1020060029482 A, 2006.04.06,

CN 101826026 A, 2010.09.08,

US 2006/0031664 A1, 2006.02.09,

(43)申请公布日 2014.11.26

审查员 崔鑫彤

(73)专利权人 成都瑞博慧窗信息技术有限公司

地址 610000 四川省成都市高新区天府大道北段1480号1栋3层

(72)发明人 高冬

(74)专利代理机构 北京天奇智新知识产权代理有限公司 11340

代理人 杨春

(51)Int.Cl.

G06F 9/445(2006.01)

G06F 21/51(2013.01)

权利要求书2页 说明书5页 附图1页

(54)发明名称

一种智能显示终端固件升级方法

(57)摘要

本发明提供了一种智能显示终端固件升级方法，该方法包括：设置两个加载程序，根据终端当前状态利用不同的加载程序进行引导和启动；对升级文件进行完整性校验；对升级文件添加数字签名；选择通过自动升级或手动升级之一来完成更新。本发明降低了智能显示终端故障率，保证了升级文件的正确性和升级的安全性。

设置两个加载程序，根据终端当前状态利用不同的加载程序进行引导和启动

对固件升级文件进行完整性校验并添加数字签名

选择通过自动升级或手动升级之一来完成固件更新

1. 一种智能显示终端固件升级方法,其特征在于,包括:

设置两个加载程序,根据终端当前状态利用不同的加载程序进行引导和启动;对固件升级文件进行完整性校验并对固件升级文件添加数字签名;选择通过自动升级或手动升级之一来完成固件更新,所述设置两个加载程序,包括设置主加载程序和备份加载程序,除了与开机引导程序、应用程序同在系统应用分区中的主加载程序外,SD卡分区中还存储了备份加载程序安装包,在所述终端重启后引导程序检测主加载程序损坏时,调用安装SD卡分区的备份加载程序安装包进行同步过程,即安装SD卡中的备份加载程序替换损坏的主加载程序,并在加载程序完成自身升级后,利用新升级的加载程序安装包替换原来的备份加载程序安装包,以使备份加载程序随着主加载程序的更新而更新;

固件升级数据包是由一个或多个PES包组合而成,在每个PES包中均包括MD5校验码,并且所述完整性校验还包括:

对固件升级文件进行双重MD5校验,以确保固件升级文件完整;

将经过MD5算法处理后的固件升级文件发送到终端,终端加载程序模块下载时首先对每个PES包进行校验,对校验通过的PES包保存有效载荷区,并舍弃未通过的PES包,重复上述过程直至所有升级文件下载完成;

在下载完成后,再对缓存区的待升级文件进行MD5校验,若校验通过,则继续固件升级过程,否则停止升级过程;

所述数字签名采用基于签名的权限检查机制,结合信息摘要算法与数字签名对升级数据包进行加解密处理,并且该方法进一步包括:

对于大数据文件,结合信息摘要算法对其信息摘要进行加密,然后将加密的摘要与待升级的原文件一起发送到终端,终端加载程序模块接收完升级包后,首先利用固化在智能显示终端中的运营商公钥对加密的提供商私钥进行解密,然后用解密后的私钥解密发送方加密的摘要文件,得到发送方升级文件的摘要,最后将下载的升级文件通过散列算法生成接收方摘要,若接收方摘要和发送方摘要相同,则继续升级过程,否则停止升级过程;

所述自动升级包括,由运营商前端统一播发升级数据流,通过网络信息表NIT中的描述符中相关内容的变化触发升级,根据NIT表检索机制,当智能显示终端主程序检测到智能显示终端序列号在NIT表规定的范围内,且两者硬件版本相同,描述符中软件版本高于智能显示终端中版本时,先将前端升级码流的下载频率、符号率、解调参数与状态变量存储后,再引导终端重启进入加载程序,加载程序根据存储的升级参数下载升级数据包进行升级过程,升级完成后,若是加载程序自身的升级,则更新SD卡分区中备份加载程序安装包,当自动升级失败次数超过预定义次数时,利用手动升级来实现软件的更新;

所述手动升级包括,用户在智能显示终端开启时通过手动操作强制进入加载程序升级过程,由用户手动设置升级参数,若用户设置下载方式为主动下载,则加载程序根据用户设置的参数下载升级数据包进行升级过程;否则检测NIT表,并根据NIT表中信道参数下载升级文件进行升级过程;

所述方法利用安全更新协议来保证显示终端远程更新的安全性,所述安全更新协议使显示终端对更新信息的来源进行合法性验证,防止攻击者冒充服务器发起更新;并且服务器对终端进行认证,对传输的更新信息利用密码算法进行完整性保护,在检测数据的误码或篡改时拒绝更新;

在初始状态下,每台显示终端在生产时均保存自身的唯一编码,内含伪随机数产生器和散列运算函数,终端编码至少为32字节长度,编码规则采用随机序列,服务器存储所有终端的编号以及部署位置;

更新协议按照消息传递的顺序的步骤如下:

步骤1:服务器生成一个伪随机数Rg,向显示终端发送认证请求,同时将随机数Rg发送给显示终端;

步骤2:显示终端生成一个伪随机数Rd,计算 $Res = h(h(No) \oplus Rg \oplus Rd)$ ,其中h为散列函数,其中No为终端的唯一编码,显示终端将Res发送到服务器;服务器接收到Res后,在相应的后台数据库中查找是否存在某个终端编码Noj( $1 \leq j \leq n$ ),使得 $h(h(Noj) \oplus Rg \oplus Rd) = h(h(No) \oplus Rg \oplus Rd)$ 成立;若找到这样的Noj,则通过对该终端的认证,并计算 $Rep = h(h(No) \oplus Rd)$ ,发送给终端;若找不到这样的Noj,则认证过程终止;

步骤3:服务器将 $Rep = h(h(No) \oplus Rd)$ 发送给终端后,终端验证 $h(h(Noj) \oplus Rd) = h(h(No) \oplus Rd)$ 是否成立;若两式相等,则终端对服务器的认证通过,准备接收新版本固件,否则返回拒绝更新的消息;

步骤4:根据新版本固件和终端唯一编码计算新版本固件散列值SW,将固件升级包和该散列值SW一并发送给终端;终端收到后验证 $h(SW || h(No) || Rd) = h(SW || h(Noj) || Rd)$ 是否成立;若相等,则表明固件未经过篡改和误码,开始擦除原有固件,写入新固件;否则拒绝更新发送告警信息;

所述显示终端远程更新进一步包括:

加载程序负责应用程序的启动和更新,应用程序实现监控功能;当CPU复位时,加载程序开始运行,在对寄存器和外围设备初始化后,向服务器询问是否有升级程序,若有则开始升级处理,若没有则跳转到应用程序执行;在应用程序执行时,若接收到服务器的升级命令,停止监控处理,软复位终端,由加载程序进行升级,加载程序的地址空间分配为0-0x4000,共16K,应用程序的地址空间分配为0x4000-0xffff,共48K,分别编译链接,终端出厂时加载程序通过ISP方式烧写到SD卡中的相应地址,应用程序由加载程序烧写到相应地址,应用程序分包发送,终端将接收到的固件暂时保存到外部RAM中,全部接收并校验通过后进行SD卡的擦除和烧写;

其中所述伪随机数使用线性叠加方法产生,计算公式为:种子=A×种子+C,此公式在几何图中表示一条直线,而且新种子由旧种子反复相加得来,设备采用定时器输出和A/D转换器输出相异或的值作为随机数的第一个种子,所述散列函数为SHA-256算法散列函数。

## 一种智能显示终端固件升级方法

### 技术领域

[0001] 本发明涉及程序升级,特别涉及一种智能显示终端的更新方法。

### 背景技术

[0002] 随着智能系统的广泛应用,数字电视技术的日新月异,基于智能系统的数字电视智能显示终端应运而生。作为一种新兴的智能终端设备,固件在其中扮演了非常重要的角色。由于智能显示终端的功能不断拓展,内部的固件及加载程序本身的不断更新,智能显示终端能够进行固件升级的需求也变得日益迫切。目前,智能显示终端加载程序模块多基于Linux平台,基于智能平台的较少,而且还存在很大的弊端。当加载程序出现BUG或与前端设备不匹配时,必须通过加载程序模块的自身升级进行修复,然而加载程序在进行自身升级时,一旦发生意外将导致安装失败,加载程序便不能正常运行,用户便无法固件升级。

[0003] 因此,针对相关技术中所存在的上述问题,目前尚未提出有效的解决方案。

### 发明内容

[0004] 为解决上述现有技术所存在的问题,本发明提出了一种智能显示终端固件升级方法,基于智能平台,有效完成应用程序以及固件自身升级加载,包括:

[0005] 设置两个加载程序,根据终端当前状态利用不同的加载程序进行引导和启动;对升级文件进行完整性校验;对升级文件添加数字签名;选择通过自动升级或手动升级之一来完成更新。

[0006] 优选地,所述设置两个加载程序,包括设置主加载程序和备份加载程序,除了与开机引导程序、应用程序同在系统应用分区中的主加载程序外,SD卡分区中还存储了备份加载程序安装包,在所述终端重启后引导程序检测主加载程序损坏时,调用安装SD卡分区的备份加载程序安装包进行同步过程,即安装SD卡中的备份加载程序替换损坏的主加载程序,并在加载程序完成自身升级后,利用新升级的加载程序安装包替换原来的备份加载程序安装包,以使备份加载程序随着主加载程序的更新而更新;

[0007] 所述升级数据包是由一个或多个PES包组合而成,在每个PES包中均包括MD5校验码,并且所述完整性校验还包括:

[0008] 对升级文件进行双重MD5校验,以确保升级文件完整;

[0009] 将经过MD5算法处理后的升级文件发送到终端,终端加载程序模块下载时首先对每个PES包进行校验,对校验通过的PES包保存有效载荷区,并舍弃未通过的PES包,重复上述过程直至所有升级文件下载完成;

[0010] 在下载完成后,再对缓存区的待升级文件进行MD5校验,若校验通过,则继续升级过程,否则 停止升级过程。

[0011] 优选地,所述方法利用安全更新协议来保证显示终端远程更新的安全性,所述安全更新协议使显示终端对更新信息的来源进行合法性验证,防止攻击者冒充服务器发起更新;并且服务器对终端进行认证,对传输的更新信息利用密码算法进行完整性保护,在检测

数据的误码或篡改时拒绝更新；

[0012] 在初始状态下，每台显示终端在生产时均保存自身的唯一编码，内含伪随机数产生器和散列运算函数，终端编码至少为32字节长度，编码规则采用随机序列，服务器存储所有终端的编号以及部署位置；

[0013] 更新协议按照消息传递的顺序的步骤如下：

[0014] 步骤1：服务器生成一个伪随机数Rg，向显示终端发送认证请求，同时将随机数Rg发送给显示终端；

[0015] 步骤2：显示终端生成一个伪随机数Rd，计算 $Res = h(h(No) \oplus Rg \oplus Rd)$ ，其中h为散列函数，其中No为终端的唯一编码，显示终端将Res发送到服务器；服务器接收到Res后，在相应的后台数据库中查找是否存在某个终端编码No j ( $1 \leq j \leq n$ )，使得 $h(h(Noj) \oplus Rg \oplus Rd) = h(h(No) \oplus Rg \oplus Rd)$ 成立；若找到这样的No j，则通过对该终端的认证，并计算Rep= $h(h(No) \oplus Rd)$ ，发送给终端；若找不到这样的No j，则认证过程终止；

[0016] 步骤3：服务器将Rep= $h(h(No) \oplus Rd)$ 发送给终端后，终端验证 $h(h(Noj) \oplus Rd) = h(h(No) \oplus Rd)$ 是否成立；若两式相等，则终端对服务器的认证通过，准备接收新版本固件，否则返回拒绝更新的消息；

[0017] 步骤4：根据新版本固件和终端唯一编码计算新版本固件散列值SW，将升级包和该散列值SW一并发送给终端；终端收到后验证 $h(SW || h(No) || Rd) = h(SW || h(Noj) || Rd)$ 是否成立；若相等，则表明固件未经过篡改和误码，开始擦除原有固件，写入新固件；否则拒绝更新发送告警信息。

[0018] 优选地，所述程序更新进一步包括：

[0019] 加载程序负责应用程序的启动和更新，应用程序实现监控功能；当CPU复位时，加载程序开始运行，在对寄存器和外围设备初始化后，向服务器询问是否有升级程序，若有则开始升级处理，若没有则跳转到应用程序执行；在应用程序执行时，若接收到服务器的升级命令，停止监控处理，软复位终端，由加载程序进行升级，加载程序的地址空间分配为0-0x4000，共16K，应用程序的地址空间分配为0x4000-0xffff，共48K，分别编译链接，终端出厂时加载程序通过ISP方式烧写到SD卡中的相应地址，应用程序由加载程序烧写到相应地址，应用程序分包发送，终端将接收到的固件暂时保存到外部RAM中，全部接收并校验通过后进行SD卡的擦除和烧写。

[0020] 本发明相比现有技术，具有以下优点：

[0021] 本发明的程序升级方法降低了智能显示终端故障率，保证了升级文件的正确性和升级的安全性，也实现了生产商和运营商对固件升级的管控，确保升级固件的合法性和双方相互认证以及完整性保护。

## 附图说明

[0022] 图1是根据本发明实施例的智能显示终端固件升级方法的流程图。

## 具体实施方式

[0023] 下文与图示本发明原理的附图一起提供对本发明一个或者多个实施例的详细描

述。结合这样的实施例描述本发明，但是本发明不限于任何实施例。本发明的范围仅由权利要求书限定，并且本发明涵盖诸多替代、修改和等同物。在下文描述中阐述诸多具体细节以便提供对本发明的透彻理解。出于示例的目的而提供这些细节，并且无这些具体细节中的一些或者所有细节也可以根据权利要求书实现本发明。

[0024] 本发明的一方面提供了一种智能显示终端固件升级方法。图1是根据本发明实施例的智能显示终端固件升级方法流程图。

[0025] 加载程序是智能显示终端固件升级的功能模块，也是其核心模块，加载程序模块对于智能显示终端的正常工作和后续固件的升级起着至关重要的作用。本发明设计的加载程序在运行模式上，采用两个加载程序运行模式；在升级文件完整性校验上，采用MD5算法校验；而在安全性上，结合信息摘要算法与RSA算法，对升级文件添加数字签名。

[0026] 为了确保加载程序的可用性，保证用户能及时地进行固件更新，本发明引入两个加载程序运行模式，即除了与开机引导程序、应用程序同在系统应用分区中的主加载程序外，SD卡分区中也存储了一份备份加载程序安装包。若因意外导致升级失败或加载程序损坏，智能显示终端重启后，引导程序检测到主加载程序损坏便调用安装SD卡分区的备份加载程序安装包进行同步过程，即安装SD卡中的备份加载程序替换损坏的主加载程序，使智能显示终端能重新具有升级功能。而在加载程序完成自身升级后，要用新升级的加载程序安装包替换原来的备份加载程序安装包，以保证备份加载程序随着主加载程序的更新而更新。

[0027] 升级数据包是由一个或多个PES包组合而成，由于数据的完整性十分重要，运营商在前端发送升级数据包时在每个PES包中均增加了MD5校验码。然而，单一的MD5校验并不能完全可靠地验证数据的完整性，升级文件在传输的过程可能会出现部分丢失或损坏的现象，造成文件传输不完整，因此，为了增加校验的可靠性，本发明在原有的基础上再增加了一次MD5校验，即对升级文件进行双重MD5校验，以确保升级文件完整。

[0028] MD5校验，是数据通信领域中的一种差错校验码，实现简单，检错能力强，运行时间短。经过MD5算法处理后的升级文件发送到用户终端，用户终端加载程序模块下载时首先对每个PES包进行校验，校验通过的PES包保存有效载荷区，未通过的舍弃，重复上述过程，直至所有升级文件下载完成为止。下载完成后再对缓存区的待升级文件进行MD5校验，若校验通过，则继续升级过程，反之则停止升级过程。

[0029] 为了让本品牌的显示终端只下载属于自身型号对应的固件，拒绝非法固件的安装，本发明采用基于签名的权限检查机制，结合信息摘要算法(散列算法)与数字签名技术对升级数据包进行加解密处理，让智能显示终端以更安全的方式进行固件更新。

[0030] RSA加密算法适合处理小数据量的信息。对于大数据文件，本发明结合信息摘要算法只对其信息摘要进行加密，然后将加密的摘要与待升级的原文件一起发送到用户终端。用户终端加载程序模块接收完升级包后，首先利用固化在智能显示终端中的运营商公钥(OPK)对加密的提供商私钥(PSK)进行解密，然后用解密后的私钥(PSK)解密发送方加密的摘要文件，得到发送方升级文件的摘要，最后将下载的升级文件通过散列算法生成接收方摘要，由于接收方摘要和发送方摘要是由相同的方法得到的，若两者相同，则继续升级过程，否则停止升级过程。

[0031] 智能操作系统拥有开放的开发平台，可帮助运营商便捷地完成系统的修改和二次

开发,当某一程序经过完善再次投入使用时需要通过智能显示终端加载程序模块进行固件更新。固件更新通过自动升级或手动强制升级来完成。

[0032] 其中,自动升级是指由运营商前端统一播发升级数据流,通过网络信息表(NIT)中的描述符中相关内容的变化触发升级。根据NIT表检索机制,当智能显示终端主程序检测到智能显示终端序列号在NIT表规定的范围内时,且两者硬件版本相等,描述符中固件版本高于智能显示终端中版本时,先将前端升级码流的信道参数(下载频率、符号率、解调参数等)与一些状态变量存储后,再引导智能显示终端重启进入加载程序。加载程序根据存储的升级参数下载升级数据包进行升级过程。升级完成后,若是加载程序自身的升级,则需更新SD卡分区中备份加载程序安装包。当自动升级失败次数超过2次,需手动升级来实现固件的更新。

[0033] 另一方面,手动升级是指用户在智能显示终端开启时通过手动操作强制进入加载程序更新协议。此时,升级参数是由用户手动设置而非前端码流中的参数。若用户设置下载方式为主动下载,则加载程序根据用户设置的参数下载升级数据包进行更新协议;反之,则需要检测NIT表,并根据NIT表中信道参数下载升级文件进行更新协议。

[0034] 根据本发明的另一方面,网络的开放性使得更新过程容易遭到各种安全攻击。例如,在更新信息的传输过程中,攻击者可截获并篡改固件信息,重新计算校验和,并将篡改后的更新信息发送至显示终端,或者直接伪造更新信息发送至显示终端,而显示终端通过更新接口接收到篡改或伪造的升级信息后,不进行任何合法性认证即直接对其内部固件进行升级,从而使得该设备被攻击者利用或破坏。

[0035] 为保证显示终端远程更新的安全性,安全更新协议设计要满足相互可认证性,显示终端要能对更新信息的来源进行合法性验证,防止攻击者冒充服务器发起更新;服务器要能对设备进行认证,在设备已被控制的情况下告知服务器更新成功。并满足完整性保护:对传输的更新信息利用密码算法进行完整性保护,在数据遭到误码或篡改时能够检测到,并拒绝更新。

[0036] 在初始状态下,每台显示终端在生产时均保存自身的唯一编码,内含伪随机数产生器和散列运算函数。设备编码应至少32字节长度,编码规则采用随机序列。服务器存储着所有设备的编号以及部署位置等相关信息,能够进行复杂的运算。

[0037] 按照消息传递的顺序,更新协议的主要步骤如下:

[0038] 步骤1:服务器生成一个伪随机数Rg,向显示终端发送认证请求,同时将随机数Rg发送给显示终端。

[0039] 步骤2:显示终端生成一个伪随机数Rd,计算 $Res=h(h(No) \oplus Rg \oplus Rd)$ ,其中h为散列函数,其中No为终端的唯一编码,显示终端将Res发送到服务器,( $\oplus$ 为异或运算符)。服务器接收到Res后,在相应的后台数据库中查找是否存在某个设备编码Noj( $1 \leq j \leq n$ ),使得 $h(h(Noj) \oplus Rg \oplus Rd)=h(h(No) \oplus Rg \oplus Rd)$ 成立。若找到这样的Noj,则通过对该终端的认证,并计算 $Rep=h(h(No) \oplus Rd)$ ,发送给设备;若找不到这样的Noj,则认证过程终止。

[0040] 步骤3:服务器将 $Rep=h(h(No) \oplus Rd)$ 发送给设备后,设备验证 $h(h(Noj) \oplus Rd)=h(h(No) \oplus Rd)$ 是否成立。若两式相等,则设备对服务器的认证通过,准备接收新版本固件,否则返回拒绝更新的消息。

[0041] 步骤4:根据新版本固件和设备唯一编码计算新版本固件散列值SW,将升级包和该散列值SW一并发送给终端。设备收到后验证 $h(SW || h(No) || Rd) = h(SW || h(No.j) || Rd)$ 是否成立。若相等,则表明固件未经过篡改和误码,开始擦除原有固件,写入新固件;否则拒绝更新发送告警信息。

[0042] 以下是与安全更新过程相关的部分的体系结构的实现。包括:

[0043] CPU中程序分为两部分:加载程序和应用程序,加载程序负责应用程序的启动和更新,应用程序实现监控功能,本发明的安全协议在加载程序中实现。当CPU复位时,加载程序开始运行,在对寄存器和外围设备初始化后,向服务器询问是否有升级程序,若有则开始升级处理,若没有则跳转到应用程序执行。在应用程序执行时,若接收到服务器的升级命令时,停止监控处理,软复位设备,由加载程序进行升级。加载程序的地址空间分配为0-0x4000,共16K,应用程序的地址空间分配为0x4000-0xffff,共48K,分别编译链接。设备出厂时加载程序通过ISP方式烧写到SD卡中的相应地址,应用程序由加载程序烧写到相应地址。

[0044] 本发明选用线性叠加伪随机数的产生方法,该方法的计算公式为:种子=A×种子+C,此公式在几何图中表示一条直线,而且新种子由旧种子反复相加得来。在常数的选择上,A选择1634529,C选择1,可以获得较好的随机性。该设备采用了定时器输出和A/D转换器输出相异或的值作为随机数的第一个种子。

[0045] 本发明选用SHA-256算法作为散列函数,该算法有常见的C语言版本,移植较为容易。

[0046] 该设备完全按照上文的安全协议实现。需要注意的是,在安全性更新的第4步,由于嵌入式协议栈不能缓存较多数据,应用程序要分包发送,设备需要将接收到的固件暂时保存到外部RAM中,全部接收并校验通过后才可进行SD卡擦除和烧写。

[0047] 综上所述,本发明提出的更新方法降低了智能显示终端故障率,双重加密技术的采用保证了升级文件的正确性和升级的安全性,也实现了生产商和运营商对固件升级的管控,确保升级固件的合法性和双方相互认证以及完整性保护,为智能显示终端生产商和运营商提供了一种优良的固件升级方案。

[0048] 显然,本领域的技术人员应该理解,上述的本发明的各模块或各步骤可以用通用的计算系统来实现,它们可以集中在单个的计算系统上,或者分布在多个计算系统所组成的网络上,可选地,它们可以用计算系统可执行的程序代码来实现,从而,可以将它们存储在存储系统中由计算系统来执行。这样,本发明不限制于任何特定的硬件和固件结合。

[0049] 应当理解的是,本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理,而不构成对本发明的限制。因此,在不偏离本发明的精神和范围的情况下所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。此外,本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或者这种范围和边界的等同形式内的全部变化和修改例。

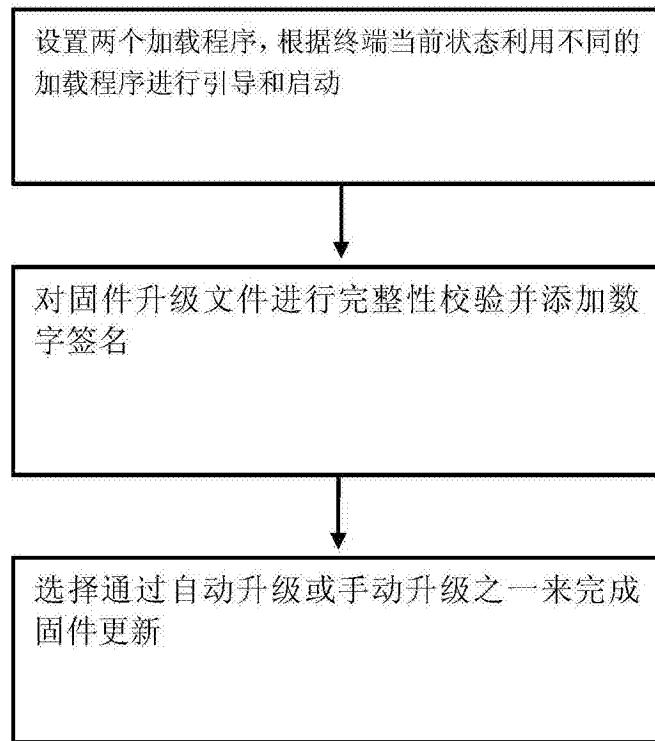


图1