(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 102760214 B
(45)授权公告日 2015.11.18

(21)申请号 201210195346.2

(22)申请日 2012.06.13

(73)专利权人 北大方正集团有限公司
地址 100871 北京市海淀区成府路 298 号方正大厦 5 层
专利权人 方正信息产业控股有限公司
上海方正数字出版技术有限公司

(72)发明人 孙伟丰 赵伟 郑程光 罗正海 李泉 李浩 李书淦 程仁波

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐

(51)Int.Cl.
G06F 21/12(2013.01)

(56)对比文件
CN 101149775 A,2008.03.26,
CN 101447009 A,2009.06.03,
CN 101609495 A,2009.12.23,
CN 102110199 A,2011.06.29,
CN 102289630 A,2011.12.21,
US 2006/0064488 A1,2006.03.23,
US 5199066 A,1993.03.30,
黄俊等．基于 RSA 算法的注册码软件加密保护．《计算机应用》.2005, 第 25 卷（第 9 期）, 第 2080-2082、2085 页．
王春来．基于计算机硬件序列号进行软件加密的技术．《辽宁科技学院学报》.2008, 第 10 卷（第 2 期）, 第 21-22 页．

审查员 吴琼

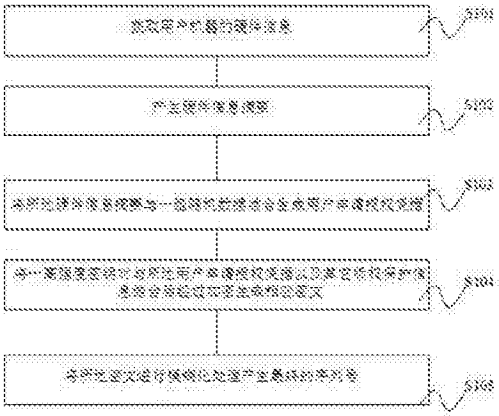
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种新型的软件版权保护方法及装置

(57)摘要

本发明提供一种新型的软件版权保护方法和装置。本发明的技术方案主要利用了用户机器的硬件信息，本发明的关键点在于收集用户运行环境的硬件信息并进行摘要化处理，利用此信息既能有效防止用户随意分发序列号，又与随机数据组合作为密钥加强了序列号的破解难度，从而达到了保护序列号不能被随意分发的目的。本发明结合了序列号方案的便利性以及硬件保护方案的高强度的信息保护方法以及利用硬件本身信息，从而最终用户能使用简单的方法使用软件，而且软件企业的软件副本也得到有效保护，不会被随意分发和使用。



CN 102760214 B

1.一种新型的软件版权保护方法，其特征在于，包括：

获取用户机器的硬件信息；

产生硬件信息摘要，所述硬件信息摘要为使用摘要算法对所述硬件信息计算出的信息摘要，其中，所述摘要算法为对任意长度的数据进行哈希杂凑计算得到固定长度的数据的算法；

将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；

将所述密文进行模糊化处理产生最终的序列号。

2.如权利要求1所述的一种新型的软件版权保护方法，其特征在于，所述的用户机器的硬件信息包括CPU序列号，内存序列号，IP地址，网卡MAC地址，主板编号。

3.如权利要求1所述的一种新型的软件版权保护方法，其特征在于，所述的产生硬件信息摘要具体为使用MD5或者SHAI摘要算法计算出所述硬件信息摘要。

4.如权利要求1所述的一种新型的软件版权保护方法，其特征在于，所述的将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成密文具体为：所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥，采用RSA加密算法将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成RSA密文，并产生密文摘要；采用DES加密算法将所述的其它版权保护信息与所述第二组随机高强度密钥结合产生DES密文。

5.一种新型的软件版权保护装置，其特征在于，包括：

硬件信息获取单元，用于获取用户机器的硬件信息；

信息摘要计算单元，用于根据所述用户机器的硬件信息计算出硬件信息摘要，所述硬件信息摘要为使用摘要算法对所述硬件信息计算出的信息摘要，其中，所述摘要算法为对任意长度的数据进行哈希杂凑计算得到固定长度的数据的算法；

授权凭据生成单元，用于将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

加密单元，用于将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；

序列号生成单元，用于将所述密文经过模糊化处理后产生最终的序列号。

6.如权利要求5所述的一种新型的软件版权保护装置，其特征在于，所述的硬件信息获取单元获取的用户机器的硬件信息包括CPU序列号，内存序列号，IP地址，网卡MAC地址，主板编号。

7.如权利要求5所述的一种新型的软件版权保护装置，其特征在于，所述的信息摘要计算单元采用MD5或者SHAI摘要算法计算产生所述硬件信息摘要。

8.如权利要求5所述的一种新型的软件版权保护装置，其特征在于，所述加密单元进一步包括：所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥；

第一加密单元，用于将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成RSA密文，并产生密文摘要；

第二加密单元，用于将所述的其它版权保护信息与所述第二组随机高强度密钥结合加

密生成密文。

一种新型的软件版权保护方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种新型的软件版权保护方法及装置。

背景技术

[0002] 计算机软件具有易于复制，易于修改的特点，软件侵权问题一直是困扰现代软件企业的一个难题。当前中国软件行业盗版现象猖獗，为保护软件开发者或软件开发企业的利益，软件公司提出了许多的软件版权保护技术，如序列号，版权文件，版权声明，网络验证，硬件保护等，这些技术都对防盗版技术起到一定的作用。

[0003] 现有的版权保护技术方案主要包括以下三种：

[0004] 一种是序列号方案，也即通过一定的算法生成一系列数字或者字符串，软件企业通过将序列号分发给客户，授权用户将得到一个有效的序列号。比如微软的系列产品就采用此技术，序列号中包含产品型号、版本型号、哈希值、序列值等信息，通过这些信息的组合和加密生成对应的序列号，而在用户端则根据序列号生成对应的信息来验证哈希值、序列值是否一致，假若一致，则认定软件已被授权。序列号方法使用起来简单，软件企业和开发者能以最低的代价来判断软件是否在授权状态下运行，同样缺点也非常明显。序列号方法不能有效的防止序列号本身被分发。同一个序列号在不同的机器上，不同用户手中都是能有效使软件进入授权状态。

[0005] 一种是序列号加网络在线激活方案：通过在 internet 网上设立一公开的授权服务器，发布的软件将通过服务器来检测软件使用者的序列号是否有效。同时也对软件激活次数进行限定，防止用户分发有效序列号进行无限次激活。序列号加在线激活方法，对于防止用户随意扩散序列号起到了很好的保护作用，不同的序列号激活次数有限，用户为保护自身权益而会注意保护自己的序列号。使用此种技术方案最大的缺点是部署成本较高，而且使用不方便。软件企业必须在因特网上公开一组授权服务器，同时软件使用者也必须能够连上因特网，这就为软件使用的网络安全埋下的隐患。

[0006] 一种是硬件保护方案：软件企业或者软件开发者使用特定的硬件装置来保护软件不被滥用。其中软件的有效信息等被放在特定的硬件：比如 u 盘、并口卡中。这些信息在软件发行之前交给硬件公司固化在硬件当中，因此破解难度很大，能有效防止软件在未授权状态下使用。该种方法破解难度最高，软件开发企业的权益将得到最高程度的保护。但是，缺点是软件使用者必须为额外的硬件付费且必须将特定的硬件做好保护工作。一旦硬件丢失，就意味着一个有效软件将被浪费或者被别人占用。

[0007] 如何让最用软件使用者很方便的使用授权软件而又同时达到最大程度保护软件开发企业的利益，防止授权信息被泄露和随意分发，已经成为一个急需解决的课题。

发明内容

[0008] 为解决上述问题，本发明技术方案一种新型的软件版权保护方法，包括：

[0009] 获取用户机器的硬件信息；

[0010] 产生硬件信息摘要，所述硬件信息摘要为使用摘要算法对所述硬件信息计算出的信息摘要，其中，所述摘要算法为对任意长度的数据进行哈希杂凑计算得到固定长度的数据的算法；

[0011] 将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

[0012] 将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；

[0013] 将所述密文进行模糊化处理产生最终的序列号。

[0014] 可选地，所述的用户机器的硬件信息包括 CPU 序列号，内存序列号，IP 地址，网卡 MAC 地址，主板编号。

[0015] 可选地，所述的产生硬件信息摘要具体为使用 MD5 或者 SHAI 摘要算法计算出所述硬件信息摘要。

[0016] 可选地，所述的将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成密文具体为：所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥，采用 RSA 加密算法将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成 RSA 密文，并产生密文摘要；采用 DES 加密算法将所述的其它版权保护信息与所述第二组随机高强度密钥结合产生 DES 密文。

[0017] 本发明还提供了一种新型的软件版权保护装置，包括：

[0018] 硬件信息获取单元，用于获取用户机器的硬件信息；

[0019] 信息摘要计算单元，用于根据所述用户机器的硬件信息计算出硬件信息摘要，所述硬件信息摘要为使用摘要算法对所述硬件信息计算出的信息摘要，其中，所述摘要算法为对任意长度的数据进行哈希杂凑计算得到固定长度的数据的算法；

[0020] 授权凭据生成单元，用于将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

[0021] 加密单元，用于将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；

[0022] 序列号生成单元，用于将所述密文经过模糊化处理后产生最终的序列号。

[0023] 可选地，所述的硬件信息获取单元获取的用户机器的硬件信息包括 CPU 序列号，内存序列号，IP 地址，网卡 MAC 地址，主板编号。

[0024] 可选地，所述的信息摘要计算单元采用 MD5 或者 SHAI 摘要算法计算产生所述硬件信息摘要。

[0025] 可选地，所述加密单元进一步包括：所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥；

[0026] 第一加密单元，用于将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成 RSA 密文，并产生密文摘要；

[0027] 第二加密单元，用于将所述的其它版权保护信息与所述第二组随机高强度密钥结合加密生成密文。

[0028] 与现有技术相比，上述技术方案具有下优点：

[0029] 本发明的技术方案主要利用了用户机器的硬件信息，本发明的关键点在于收集用户运行环境的硬件信息并进行摘要化处理，利用此信息既能有效防止用户随意分发序列

号，又与随机数据组合作为密钥加强了序列号的破解难度，从而达到了保护序列号不能被随意分发的目的。本发明结合了序列号方案的便利性以及硬件保护方案的高强度的信息保护方法以及利用硬件本身信息，从而最终用户能使用简单的方法使用软件，而且软件企业的软件副本也得到有效保护，不会被随意分发和使用。

附图说明

[0030] 图 1 是本发明实施方式的新型的软件版权保护方法的流程图；

[0031] 图 2 是本发明实施方式的新型的软件版权保护装置的组成结构框架示意图。

具体实施方式

[0032] 为使本发明的上述目的、特征和优点能够更为明显易懂，下面结合附图对本发明的具体实施方式做详细的说明。在以下描述中阐述了具体细节以便于充分理解本发明。但是本发明能够以多种不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本发明内涵的情况下做类似推广。因此本发明不受下面公开的具体实施方式的限制。

[0033] 为解决现有技术中的问题，本发明的发明人经过研究，提出了一种新型的软件版权保护方法。参阅图 1，图 1 是本发明实施方式的新型的软件版权保护方法的流程图。本发明实施方式的新型的软件版权保护方法，包括：

[0034] 获取用户机器的硬件信息；

[0035] 产生硬件信息摘要；

[0036] 将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

[0037] 将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；

[0038] 将所述密文进行模糊化处理产生最终的序列号。

[0039] 下面结合说明书附图和具体实施方式来对本发明的一种新型的软件版权保护方法和装置做进一步详细的说明。

[0040] 本发明提供的一种新型的软件版权保护方法，包括：

[0041] 步骤 101：获取用户机器的硬件信息；

[0042] 其中，所获取的用户的硬件信息包括：CPU 序列号，内存序列号，IP 地址，网卡 MAC 地址、主板编号，但是不限于上述的计算机硬件信息。由于这些机器的硬件的信息唯一标识了一台机器，因此，对于防止软件版权的保护方面起到了关键的作用。

[0043] 步骤 102：产生硬件信息摘要；

[0044] 其中，本发明中使用摘要算法对前一步骤获取的用户机器的硬件信息计算出信息摘要，其中的摘要算法是指对于任意长度的数据进行哈希 (HASH) 杂凑计算，从而得到一个固定长度的计算结果。随着数据的改变，采用相同哈希算法计算出的摘要也将随之改变。常用的摘要算法有 MD5 或者 SHAI 摘要算法。

[0045] 步骤 103：将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

[0046] 其中，本步骤中一组随机数据是随机产生的一组数据，其与所述的硬件信息摘要进行结合后产生所述用户申请授权凭据。

[0047] 步骤 104：将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结

合后经过加密生成相应密文；

[0048] 其中，本步骤中的所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥，采用 RSA 加密算法将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成RSA密文，并产生密文摘要；采用DES加密算法将所述的其它版权保护信息与所述第二组随机高强度密钥结合产生 DES 密文。

[0049] 步骤 105：将所述密文进行模糊化处理产生最终的序列号。

[0050] 其中，将步骤 104 中产生的密文摘要与 DES 密文进行结合并经过模糊化处理后产生最终的序列号。

[0051] 参阅图 2，图 2 为本发明实施方式的新型的软件版权保护装置的组成框架示意图。本发明实施方式的磁盘管理装置，包括：

[0052] 硬件信息获取单元 110，用于获取用户机器的硬件信息；其中，所述的硬件信息获取单元 110 获取的用户机器的硬件信息包括 CPU 序列号，内存序列号，IP 地址，网卡 MAC 地址、主板编号。

[0053] 信息摘要计算单元 120，用于根据所述用户机器的硬件信息计算出所述硬件信息摘要；其中，所述的信息摘要计算单元 120 采用 MD5 或者 SHAI 摘要算法计算产生所述硬件信息摘要。

[0054] 授权凭据生成单元 130，用于将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据；

[0055] 加密单元 140，用于将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文；其中，所述加密单元 140 进一步包括：所述的高强度密钥对包括第一组随机高强度密钥和第二组随机高强度密钥；第一加密单元 140a，用于将所述的第一组随机高强度密钥与所述用户申请授权凭据结合加密生成 RSA 密文，并产生密文摘要；第二加密单元 140b，用于将所述的其它版权保护信息与所述第二组随机高强度密钥结合加密生成密文。

[0056] 序列号生成单元 150，用于将所述密文经过模糊化处理后产生最终的序列号。

[0057] 综上所述，本发明技术方案具有下优点：

[0058] 本发明的技术方案主要利用了用户机器的硬件信息，本发明的关键点在于收集用户运行环境的硬件信息并进行摘要化处理，利用此信息既能有效防止用户随意分发序列号，又与随机数据组合作为密钥加强了序列号的破解难度，从而达到了保护序列号不能被随意分发的目的。本发明结合了序列号方案的便利性以及硬件保护方案的高强度的信息保护方法以及利用硬件本身信息，从而最终用户能使用简单的方法使用软件，而且软件企业的软件副本也得到有效保护，不会被随意分发和使用。

[0059] 应当理解的是这里所描述的方法和系统可以以各种形式的硬件、软件、固件、专用处理机或者它们的组合实现。尤其是，至少本发明的一部分包括程序指令的应用程序优选实现。这些程序指令被确实地包括在一个或者多个程序存储设备（包括但不限于硬盘，磁性软盘，RAM，ROM，CD，ROM 等）里，并且可由任何包括适当结构的设备或者机器，例如一种具有处理器、内存和输入 / 输出接口的通用数字计算机执行。还应当理解由于附图中描述的一些系统的组成部件和处理步骤优选地以软件实现，所以，系统模块（或者方法步骤的逻辑流程）之间的连接可能不同，这取决于本发明的编程方式。根据这里给出的指导，相关领

域的普通技术人员将能够设计出本发明的这些以及类似的实施方式。

[0060] 以上公开了本发明的多个方面和实施方式，本领域的技术人员会明白本发明的其它方面和实施方式。本发明中公开的多个方面和实施方式只是用于举例说明，并非是对本发明的限定，本发明的真正保护范围和精神应当以权利要求书为准。

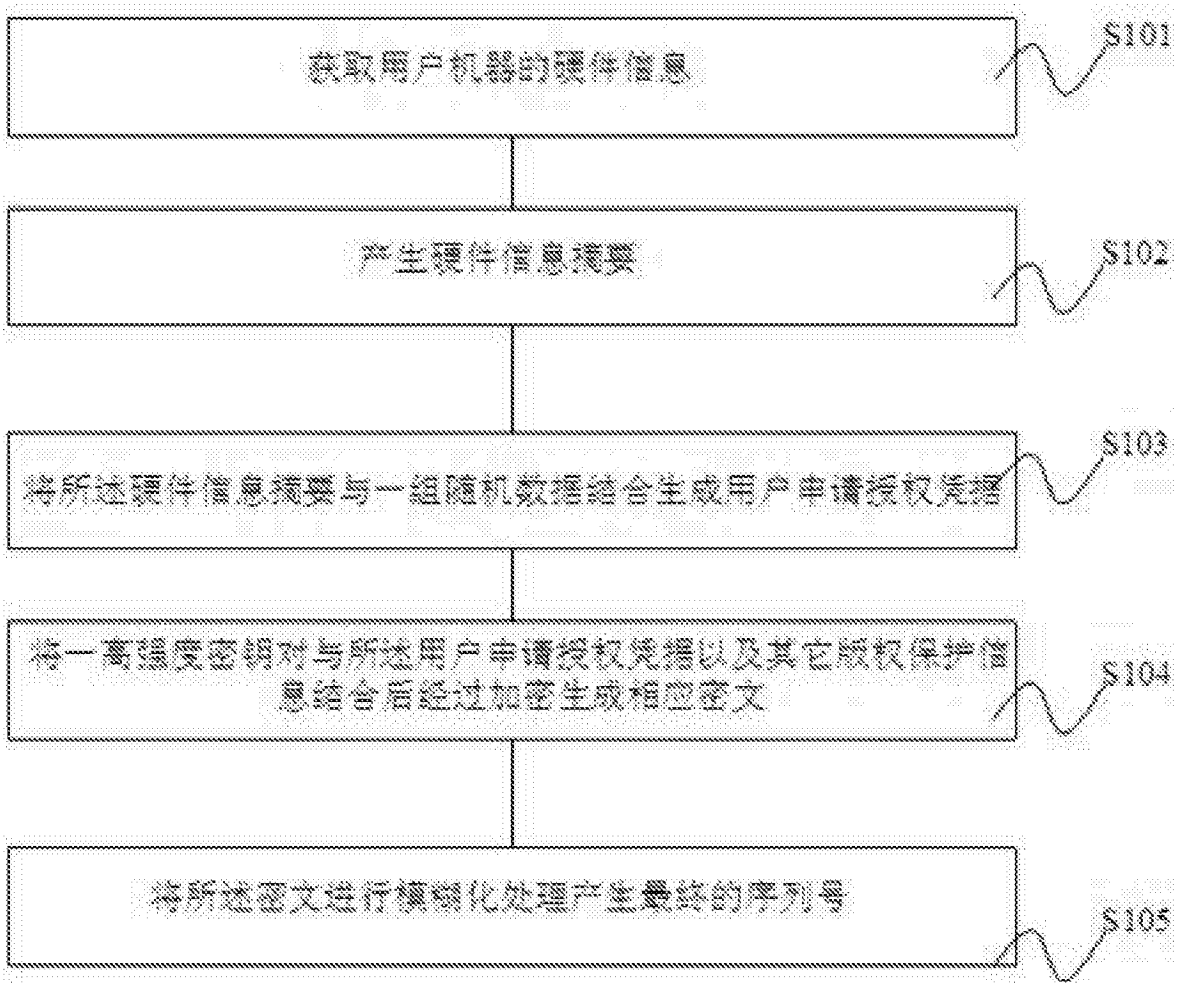

获取用户机器的硬件信息
S101
产生硬件信息摘要
S102
将所述硬件信息摘要与一组随机数据结合生成用户申请授权凭据
S103
将一高强度密钥对与所述用户申请授权凭据以及其它版权保护信息结合后经过加密生成相应密文
S104
将所述密文进行模糊化处理产生最终的序列号
S105

图 1

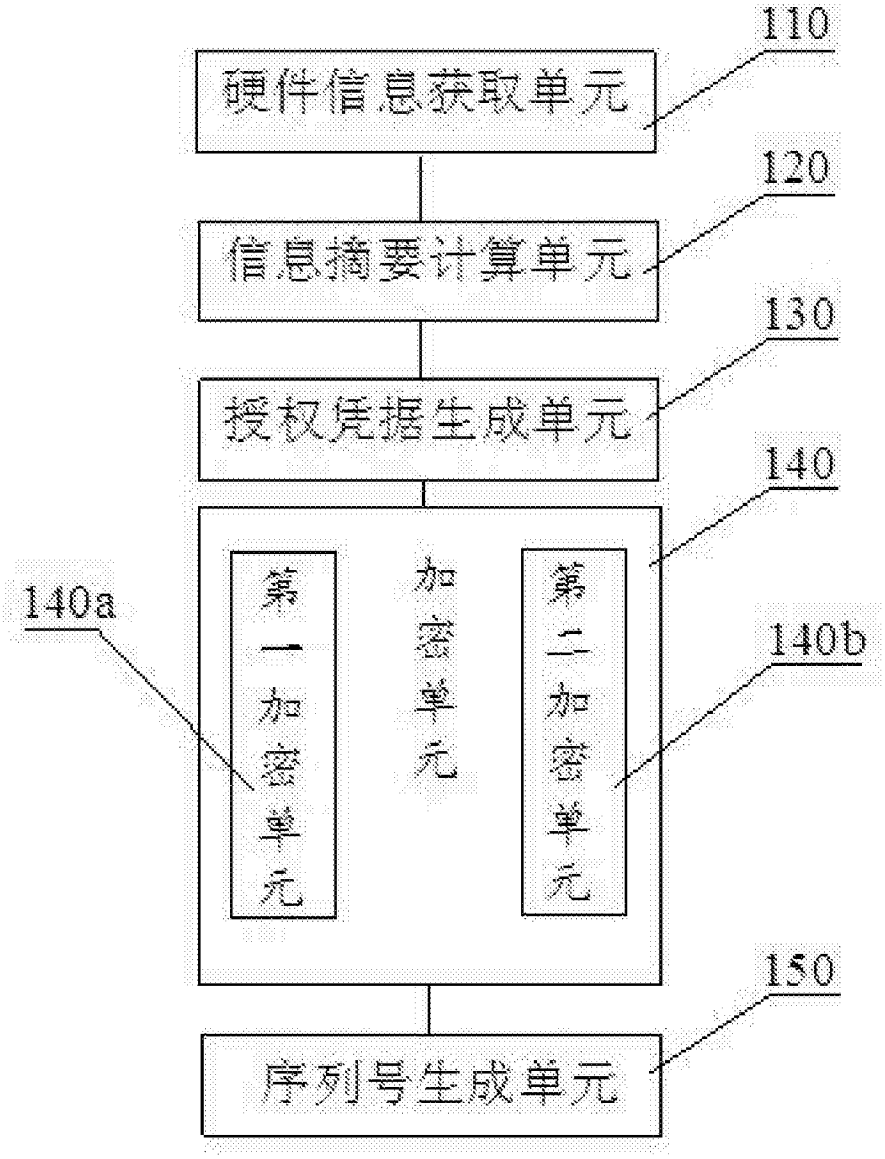

110
硬件信息获取单元
120
信息摘要计算单元
130
授权凭据生成单元
140
140a
第一加密单元
加密单元
第二加密单元
140b
150
序列号生成单元

图 2