



[12] 发明专利说明书

[21] ZL 专利号 99811859.1

[45] 授权公告日 2005 年 6 月 8 日

[11] 授权公告号 CN 1205520C

[22] 申请日 1999.10.6 [21] 申请号 99811859.1

[30] 优先权

[32] 1998.10.7 [33] US [31] 09/167,273

[86] 国际申请 PCT/EP1999/007479 1999.10.6

[87] 国际公布 WO2000/020948 英 2000.4.13

[85] 进入国家阶段日期 2001.4.6

[71] 专利权人 因芬尼昂技术股份公司

地址 德国慕尼黑

[72] 发明人 P·瑟尼 J·舍珀斯 D·蔡格

M·斯默拉

审查员 谷 威

[74] 专利代理机构 中国专利代理(香港)有限公司

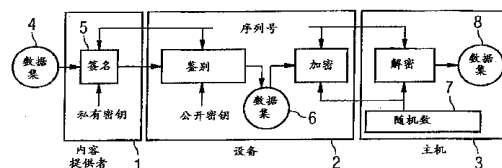
代理人 程天正 张志醒

权利要求书 2 页 说明书 6 页 附图 1 页

[54] 发明名称 拷贝保护系统与方法

[57] 摘要

拷贝保护系统是签名方法和使用可变密钥的编码或加密方法的组合。数据集只被写到预先确定的设备上,且只能在正确授权时才被释放给主机用于读取和解密。由于数据集是用设备的唯一标识符(例如:序列号)签名的,所以拷贝加密的数据集是完全无用的。



1. 一种防止未经授权数据拷贝的方法，包括：
将一个设备的唯一标识传送给内容提供者；
5 将该唯一标识作为鉴别签名添加到数据集中以构成一个已签名数据集；
将已签名数据集连同该唯一标识从内容提供者拷贝到该设备；
在该设备中用该唯一标识对数据集进行编码以构成加密数据；
将该设备的唯一标识传送给一个主机；和
10 用该主机读取并解码加密数据，从而在该主机恢复和使用该数据集。
2. 按照权利要求 1 的方法，其中，还包括在该主机产生一个随机数并将其传送给该设备，并且其中编码步骤包括，使用由唯一标识和该随机数形成的一个动态密钥对数据集进行编码。
- 15 3. 按照权利要求 1 的方法，其中，包括由该唯一标识和提供者的私有密钥构成鉴别签名，并且在拷贝步骤后，将私有密钥与该设备中现有的公开密钥对照以核对签名数据集。
4. 按照权利要求 1 的方法，其中，包括在设备中核对签名数据集，并且如果签名数据集中的鉴别签名与该设备的唯一标识不匹配，则任何到
20 主机的数据集输出将被阻止。
5. 一种拷贝保护系统，包括：
一个具有唯一标识和输入的设备，该输入用于接收由一个数据集和该唯一标识构成的签名数据；
所述设备中的控制器，通过检查，如果所述签名数据集中的授权签名与
25 所述设备的所述唯一标识相匹配，则该控制器用于将所述签名数据鉴别为授权数据，以在所述设备中存储所述数据集，并且用于使用给定的密钥对数据集进行编码以形成加密数据；
连接到该设备的主机，所述主机从所述设备接收所述加密数据、解密所述加密数据并且处理所述数据集。

6. 按照权利要求 5 的系统, 其中, 该主机包括了一个随机数发生器, 并且在所述主机中产生的随机数被包含在给定密钥中。

拷贝保护系统与方法

5 技术领域

本发明涉及防止软件盗版。更具体而言，本发明属于一种保护数字数据防止未经授权拷贝与使用的新方法。

背景技术

10 数字化媒体已经成为各种类型数据信息的流行载体。例如，计算机软件和音频信息广泛地通过光盘（CD）提供。近来，数字录音带（DAT）已经获得共享发行。CD 和 DAT 采用通用的标准进行数据、软件、图象与音频的数字记录。其它的媒体，如多媒体压缩光盘（MCD）、数字视频光盘（DVD）、高密度光盘等正在软件和数据销售市场占有相当大的份额。

15 数字化格式与模拟格式相比具有更高品质，这使得前者实际上更容易遭到未授权的拷贝和盗版。无论数据是压缩的、非压缩的、加密的或非加密的，数字化数据流的拷贝通常不会引起任何数据品质的损失。因此数字化拷贝在多重拷贝方面基本上是无限制的。而相反，模拟数据由于其本身的信噪比，而在多重和大量拷贝方面自然受限制。

20 近来数字化格式的流行同时也使相应的拷贝保护系统和方法应运而生。这些系统和方法通常归为不同类别，如加密、拷贝保护和内容扩展等。

现有技术对于防止未经授权拷贝有版权和有保护价值的数据没有达到很高的保护程度。

25 以数字和模拟格式使用的加密基本上讲是把信息打乱。数据流只有拥有正确的密钥才可用。已经发现加密通常很容易被破解。一旦密钥被盗版者发现，信息就能够被自由复制而无须加密。

在早期的个人计算机中软件拷贝保护被广泛应用。然而，一旦软件制造商发现：一方面，事实上所有的拷贝保护代码都能很快地被黑客破解；以及另一方面，开发新的拷贝保护类型变得异常昂贵，则它们基本上会停止

拷贝保护。并且，未受保护的程序能够很快获得广泛的应用，尽管有许多未经授权的拷贝，但额外的销售能够在很大程度上弥补盗版的损失。

5 一些流行的软件使用了一种系统其中将一个安装密钥与数据载体(如光盘或软盘)中的原始程序包一起分发。在PC机安装程序数据以前，需要输入安装密钥。于是，该密码和CD的数据内容很有可能一起被复制任意次，并因此使任意数量的盗版拷贝被分发与进入流通。

10 另一种已建立的保护机制包括由特殊协议规定支持的防止拷贝。比如，在DAT记录器的音频应用中就已经建立了类似的协议。正如上面所指出的，CD和DAT数据格式基本上是一致的，因此使多重拷贝成为可能。所以，在DAT系统中，被拷贝的CD需要特别的拷贝保护信息，并且如果保护被启动，DAT记录器就不被授权进行拷贝。不过，这种方法的缺陷在于对目标设备必须有很高的要求。特殊的防拷贝电路必须包含在记录器中。这类系统被称为是序列拷贝管理系统(SCMS)。最终用户对这样的方法普遍不感兴趣。已经显示出这样的要求并不总是能够被保证。特别是，用于从数字信号中
15 过滤禁止拷贝指令的黑箱系统能够广泛获得。近来，现代化PC的使用也使得利用上述机制可以变得很容易，从而最终绕过这些保护机制。

20 现有的拷贝保护系统技术在例如德国专利申请DE 196 30 755 A1中已有描述。在该文献中，一个半导体海量存储媒体被分为两个存储区域。其中一个区域配备了一个不可改变的签名，该签名表明数据是需要授权才可以存储在主存储区域中还是可以由任何人存储。这种技术能够将盗版的拷贝和原版区分开来。

发明内容

25 因此本发明的目的是提供一种拷贝保护方法和系统，能够克服目前该通用类型的设备和方法以上所述的缺陷，并且能够安全地防止被保护的数据从一个媒体拷贝到另一个相当的存储媒体，以及防止拷贝的数据能与原有存储媒体上数据同样地使用。这种方法的一个特定目的是在保持已有保护机制以及对解密数据的后续拷贝的同时防止读取信息。这种新颖方法的最后一个特别目的是防止在同类设备(例如多媒体卡等)之间的拷贝，即，

使得目标设备上的数据不可用。

根据前述以及其它考虑目的,本发明提供了一种防止未授权数据拷贝的方法,该方法包括:

将一个设备的唯一标识传送给内容提供者;

5 将该唯一标识作为鉴别签名添加到数据集中以构成一个已签名数据集;

将已签名数据集连同该唯一标识从内容提供者拷贝到该设备;

在该设备中用该唯一标识对数据集进行编码以构成加密数据;

将该设备的唯一标识传送给一个主机; 和

10 用该主机读取并解码该加密数据,从而在该主机恢复和使用该数据集。

依照本发明的一个附加特征,在该主机产生一个随机数并将其传送给设备,其中编码步骤中包括使用由唯一标识和该随机数构成的一个动态密钥对数据集进行编码。

依照本发明的另一个特征,该鉴别签名由该唯一标识和提供者的私有密
15 钥构成,并且在拷贝步骤后,签名数据集通过用该私人密钥对照该设备中现有的公开密钥来进行核对。

依照本发明的另一个特征,签名数据集在该设备中进行核对,并且如果签名数据集中的鉴别签名与该设备的唯一标识不匹配,则任何从该设备到主机的数据集输出将被阻止。

20 根据上述以及其它考虑目的,本发明还提供了一种拷贝保护系统,该系统包括:

一个具有唯一标识和输入的设备,该输入用于接收由一个数据集和该唯一标识构成的签名数据;

25 所述设备中的控制器,通过检查,如果所述签名数据集中的授权签名与所述设备的所述唯一标识相匹配,则该控制器用于将所述签名数据鉴别为授权数据,以在所述设备中存储所述数据集,并且用于使用给定的密钥对数据集进行编码以形成加密数据;

连接到该设备的主机,所述主机从所述设备接收所述加密数据、解密所述加密数据并且处理所述数据集。

依照本发明的伴随的一个特性,主机包括了一个随机数发生器并且在主机中产生的随机数被包含在给定密钥中用于形成动态密钥。

换句话说,本发明描述了一种方法,该方法中要接收数据的设备在将数据释放以便读取之前,以签名的方式监控要被写的数据集的授权。签名核
5 对与数据解密结合起来,所以只有经过鉴别的数据才以加密的形式从该设备交付到使用单元(主机)。

签名的一部分是设备所特有的、不可复制的特性(如,设备的序列号),用于明确地识别每一设备。签名的另一部分是秘密的“私有密钥”,该密钥只有数据集的所有者,即内容提供者才知道。通过单向函数将私有密钥
10 和公开密钥结合在一起。公开密钥出现在设备中,并且它是不可更改的。

设备通过将签名与设备序列号和公共密钥相比较来鉴别数据集。公开/私有密钥对相当于适用于任何设备的主密钥。设备只允许写入那些具有合法签名的数据。数据集的所有者和销售者按照以下步骤确定签名:

将设备的序列号传送给数据集的所有者。

15 数据集的所有者通过单向函数确定签名,其中在自变量中包含以下参数:

私有密钥;

目标设备的序列号; 和

要签名的数据集。

20 用户设备接收数据集并且核对签名。设备只有在核对签名正确后,才发布数据集用于读取。主机只被允许处理来自设备签名部分的数据,该数据通过一个协商一致的算法进行加密。主机无法使用未经加密的数据或者以其他方式加密的数据。未经鉴别的数据不能由设备输出。

对“直接”存贮在设备中的数据集进行加密依赖于:

25 设备的序列号; 和

主机动态产生的随机数。

将编码的数据集从配备保护方法的一个设备拷贝到另一个没有配备(相同)保护方法的设备是可能的。不过由于加密是依赖于设备的,所以该数据集是不能使用的。

总之,本发明基本上是一种签名方法和一种使用可变密钥的加密方法的组合。本发明实现了数据集只能写入预先确定的设备上且只能由主机从该设备读取(解密)的目的。这样拷贝加密后的数据集是毫无意义的,因为数据集采用了设备的序列号加密。结果是得到一个远优于引言中所描述方法的有效的拷贝保护系统。

本发明还包括其他附加的特征。

虽然这里将本发明说明和描述为包含在一个拷贝保护系统和方法中,但是并不是指它局限于展示的细节,而是在不脱离本发明的精神并且在权利要求的等同范围内的情况下,对本发明可以进行修改和结构上的改变。

不过,通过连同附图阅读下面对具体实施方案的描述,会对本发明操作的构建和实施方式,连同附加目的及其优点有更好的了解。

附图说明

图1是内容提供者、设备和主机之间数据流的示意图;和

图2是本发明的一个实施方案的示意图,用于加密数据和明码数据的共同使用。

具体实施方式

现在详细介绍附图,首先并特别地介绍图1,在其中有一个系统框图,图中内容提供者1准备要传送到设备2的数据,主机3将从设备2中读取和处理数据内容。术语“内容提供者”是指拥有数据集版权的合法所有者,比如软件开发商和软件经销商。术语“设备”是指带有控制器的任何存储媒介,比如多媒体卡等。术语“主机”是指能够从设备中读取数据并且能够处理/执行从该设备接收的数据的机械装置,比如计算机、游戏站等。数据在处理器5中根据数据集4(例如,软件程序、音频/视频序列、静态图片等)、私有密钥和设备唯一标识符进行组装。处理器5使用设定的算法将私有密钥和设备标识符绑在一起形成签名数据。该特定算法不是本说明书描述的重点,对它的要求是只要保证设备能找到签名和私有密钥,并能将其从数据集(解码后的)正确分离。那些本领域的技术人员很容易明白

如何在处理器 5 中完成数据组装和如何在设备中完成解码（例如，RSA，DES 等）。

如此封装后的数据，即签名数据随后被传输到设备 2。设备 2 中的控制器通过比较设备标识符（序列号）和公开密钥的增加部分来鉴别签名数据。
5 然后，控制器将数据集写入存储器 6。数据集被从存储器中读取，经过加密后该（加密）信号才能被主机 3 读到。

除使用设备序列号进行加密以外，也引入随机数用于加密密码数据。随机数由主机 3 中随机数发生器 7 输出。随机数同样可用于解密密码数据。数据集 8 经在主机中解密后，准备好被处理或执行。

10 现在讨论图 2，图中展示了组合设备的具体实施方案，该设备既存储签名数据也存储未签名数据。输入到设备 2 的数据，首先被核对签名，如果数据已被是签名则进行鉴别。对未签名数据（“明码数据”）就不做任何改变将其存储在相应的存储位置 9 中。签名数据也存储在相应的存储位置 10 中。只有被识别为合法的签名数据集方被允许在主机中解密和使用。
15 在数据集没有被签名的情况下，数据作为明码数据以没有加密的形式被设备输出。这种方式允许签名数据连同私有数据一起存储在存储媒体上，且从存储媒体中被读取。当加密数据集作为未签名数据集被复制到同一台设备时（未签名），它就不再能被解密，因为主机使用的是动态密钥。

20 存储区域 9 和主机控制器之间（其间有设备控制器）的双箭头例证了动态密钥的有效性，该密钥用于设备和主机间密码数据的交换。如果没有动态密钥，则将签名数据读入主机一次，然后将该数据作为明码数据写回该设备或者相当的设备都是有可能的。这样将允许不受约束的多次拷贝和复制。因此是动态密钥防止了这样的未经授权的多次拷贝。

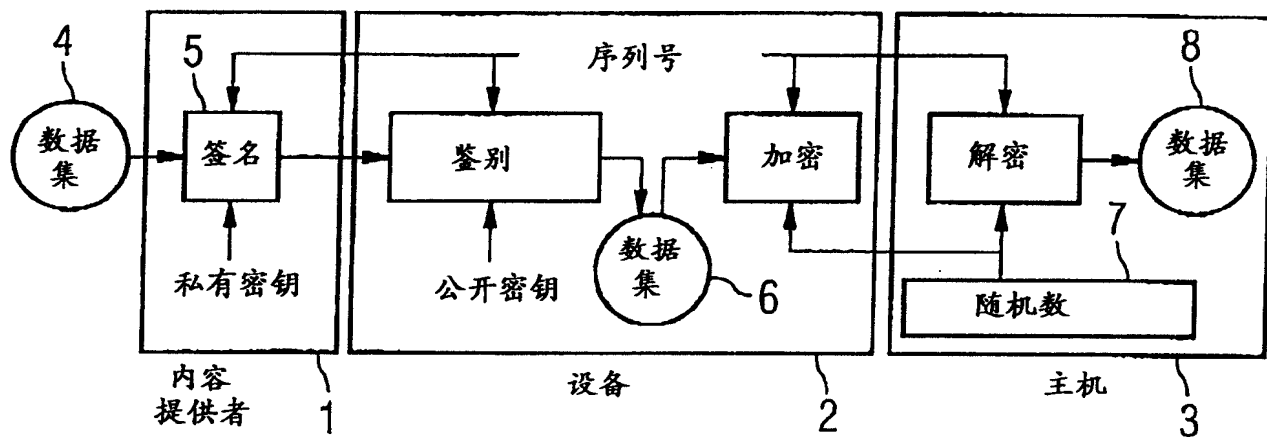


图 1

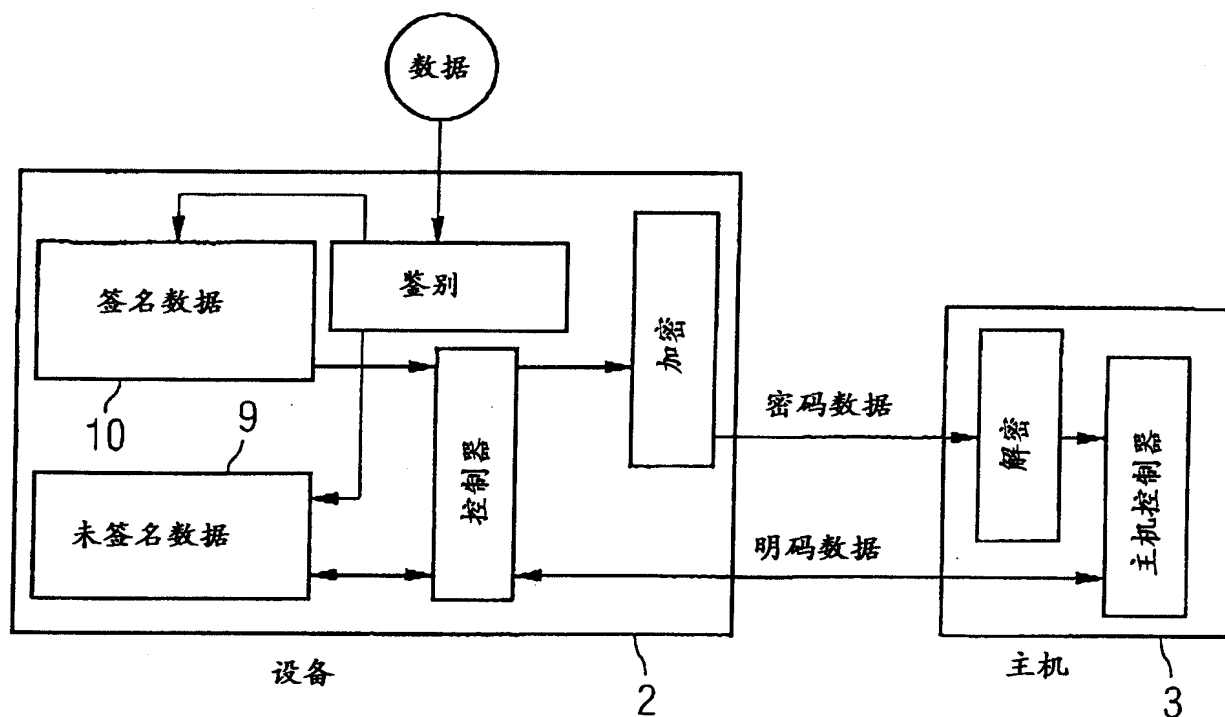


图 2