[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/28
H04L 9/00 G06F 12/14

[12] 发明专利申请公开说明书

[21] 申请号 03150744.1

[43] 公开日 2005 年 3 月 9 日

[11] 公开号 CN 1592194A

[22] 申请日 2003.9.3 [21] 申请号 03150744.1

[71] 申请人 上海乐金广电电子有限公司
地址 201206 上海市浦东新区金桥出口加工区云桥路 600 号
[72] 发明人 金柄辰 金亨善 亚历山大

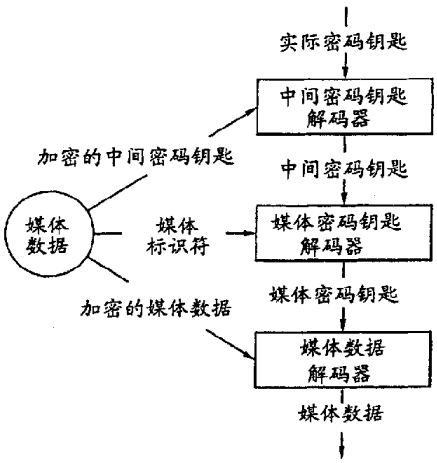
[74] 专利代理机构 上海专利商标事务所
代理人 王月珍

权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称 防止数码媒体复制的方法及系统

[57] 摘要

一种防止数码媒体复制的方法及系统。本发明包括：接收包含可用播放装置的密码钥匙识别符的媒体认证，搜索相当于上述密码钥匙识别符的实际密码钥匙的密码钥匙鉴定器；接收密码化的中间密码钥匙，用上述实际密码钥匙解码上述中间密码钥匙的解码器；把上述解码的中间密码钥匙以媒体识别符解码，得到原来的媒体密码钥匙的媒体密码钥匙解码器；接收密码化的媒体数据组，用上述原来的媒体密码钥匙，解译上述媒体数据组的媒体数据解码器。本发明的方法及系统，可以适用于所有类型的数码媒体数据，没有特定媒体特性。本发明显著减少在非标准装置中非法复制媒体数据的可能性，把媒体数据只限制给数据传送许可的个人。



ISSN1008-4274

1、一种防止数码媒体复制的方法，其特征包括：

a)利用属于原来媒体密码钥匙的运算法，对原来媒体数据组进行加密的步骤；

b)把上述原来的媒体密码钥匙以媒体标识符加密，生成加密的中间密码钥匙的步骤；

c)用可以利用上述中间密码钥匙的播放装置的公开的密码钥匙进行加密的步骤；

d)包含上述加密的媒体数据组和上述加密的中间密码钥匙以及上述播放装置的密码钥匙识别符的媒体认证传达给上述播放装置的步骤；

e)搜索相当于上述密码钥匙识别符的实际密码钥匙的步骤；

f)用上述实际密码钥匙解译上述传达的中间密码钥匙的步骤；

g)用上述媒体认证解译上述解码的中间密码钥匙，得到上述原来的媒体密码钥匙的步骤；

h)用上述得到的媒体密码钥匙，解译上述传达的媒体数据组的步骤。

2、如权利要求 1 所述的防止数码媒体复制的方法，其特征在于所述的实际密码钥匙是，确认保存在上述播放装置的可用密码钥匙，是否相当于上述密码钥匙标识而搜索。

3、如权利要求 2 所述的防止数码媒体复制的方法，其特征在于所述的可用密码钥匙包括，最近密码钥匙和一个以上的以前密码钥匙，上述以前各个密码钥匙通过密码钥匙撤销过程已被撤销。

4、 如权利要求 3 所述的防止数码媒体复制的方法，其特征在于所述的以前密码保存在可重复记录的存储器。

5、如权利要求 4 防止数码媒体复制的方，其特征在于所述的保存在上述存储器的上述以前密码钥匙，加密为上述公开的密码钥匙。

6、一种防止数码媒体复制的系统，其特征包括：

密码钥匙鉴定器，接收包含可用播放装置的密码钥匙识别符的媒体认证，搜

索相当于上述密码钥匙识别符的实际密码钥匙密码钥匙鉴定器；

中间密码钥匙的解码器，接收密码化的中间密码钥匙，用上述实际密码钥匙解码上述中间密码钥匙；

媒体密码钥匙解码器，把上述解码的中间密码钥匙以媒体识别符解码，得到原来的媒体密码钥匙；

媒体数据解码器，接收密码化的媒体数据组，用上述原来的媒体密码钥匙，解译上述媒体数据组。

7、如权利要求 6 所述的防止数码媒体复制的系统，其特征在于所述的上述实际密码钥匙是，确认保存在上述播放装置的每个可用密码钥匙，是否相当于上述密码钥匙标识符而搜索。

8、如权利要求 7 所述的防止数码媒体复制的系统，其特征在于所述的可用密码钥匙包括，最近密码钥匙和一个以上的以前密码钥匙，上述以前各个密码钥匙通过密码钥匙撤销过程已被撤销。

9、如权利要求 8 所述的防止数码媒体复制的系统，其特征在于所述的一个以上的以前密码钥匙，保存在可重复记录的数据存储器。

10、如权利要求 9 所述的防止数码媒体复制的系统，其特征在于所述的保存在上述存储器的上述以前密码钥匙，以上述播放装置的公开的密码钥匙加密。

11、如权利要求 6 所述的防止数码媒体复制的系统，其特征在于所述的加密的中间密码钥匙在开始，以上述播放装置的公开的密码钥匙加密。

12、如权利要求 6 所述的防止数码媒体复制的系统，其特征在于所述的加密的媒体数据组以原来媒体密码钥匙初始加密。

防止数码媒体复制的方法及系统

（1）技术领域

本发明是涉及防止媒体复制的方法及系统，尤其是指利用复杂的密码技术，防止未经数码媒体数据组许可而复制的一种防止数码媒体复制的方法及系统。

（2）背景技术

为了保护电脑网络，远程通信系统及其他系统等通信系统的信息，增加密码的利用。密码的记法大致分为对称的钥匙密码记法和公开的钥匙密码记法。对称的钥匙密码记法中对称的钥匙密码为了数据的加密及解密使用。有对称的钥匙密码记法的几种有效的实例（implementations），但是在这样的实例中，实际密码钥匙运用上经常出现问题。

另外，在公开的钥匙密码记法中的数据加密及解密处理是相互独立完成。即，数据加密处理主要需要以“e”指定的公开的密码钥匙。虽然数据解密处理在数学方面有关联，但是使用的是另一种密码钥匙“d”。因此，有公开的密码钥匙的实体（entity），虽然可以加密基本形式的信息明文（plain text），但是不能解密加密形式的信息加密文（cyper text）。

个人选择公开的密码钥匙并公开该公开的密码钥匙时，谁都可以使用公开的密码钥匙加密上述个人的一个以上消息。这样的话，上述个人保密自己的私有钥匙，保证只有自己解密信息的加密文。目前，公开的密码钥匙记法的实例虽然比对称的密码钥匙记法的实例效率低，但是更安全。

混合密码钥匙记法中，明文以对称的密码钥匙的运算法则加密，对称的密码钥匙以公开的密码钥匙运算法则加密。当接收用公开的密码钥匙加密的对称的密码钥匙和用对称的密码钥匙加密的数据时，接收者先用自己的私有钥匙解译用公开的密码钥匙加密的对称的密码钥匙，然后，接收者使用解译的对称的密码钥匙解译用对称的密码钥匙加密的数据。在混合密码钥匙记法中，得到原始数据的过程一般比公开的密码钥匙密码记法快。另外混合密码钥匙记法可以每次使用对称

密码钥匙，很大程度上提高对称运算法的安全。因为这些理由，混合密码钥匙记法是，把被保护的媒体数据，安全传送给受信者的理想的方法。

（3）发明内容

本发明的目的是要解决原有技术中媒体数据保护的的限界和不便等引起的问题，提出一种防止数码媒体复制的方法及系统。

本发明是利用混合密码技术及媒体认证，提供一种防止未经数码媒体数据组的访问而被复制的控制方法。

本发明的目的是这样实现的：

一种防止数码媒体复制的方法，包括，

a)利用属于原来媒体密码钥匙的运算法，对原来媒体数据组进行加密的步骤；

b)把上述原来的媒体密码钥匙以媒体标识符加密，生成加密的中间密码钥匙的步骤；

c)用可以利用上述中间密码钥匙的播放装置的公开的密码钥匙进行加密的步骤；

d)包含上述加密的媒体数据组和，上述加密的中间密码钥匙和，上述播放装置的密码钥匙识别符的媒体认证传达给上述播放装置的步骤；

e)搜索相当于上述密码钥匙识别符的实际密码钥匙的步骤；

f)用上述实际密码钥匙解译上述传达的中间密码钥匙的步骤；

g)用上述媒体认证解译上述解码的中间密码钥匙，得到上述原来的媒体密码钥匙的步骤；

h)用上述得到的媒体密码钥匙，解译上述传达的媒体数据组的步骤。

一种防止数码媒体复制的系统，包括：

密码钥匙鉴定器，接收包含可用播放装置的密码钥匙识别符的媒体认证，搜索相当于上述密码钥匙识别符的实际密码钥匙密码钥匙鉴定器；

中间密码钥匙的解码器，接收密码化的中间密码钥匙，用上述实际密码钥匙解码上述中间密码钥匙；

媒体密码钥匙解码器，把上述解码的中间密码钥匙以媒体识别符解码，得到

原来的媒体密码钥匙；

媒体数据解码器，接收密码化的媒体数据组，用上述原来的媒体密码钥匙，解译上述媒体数据组。

本发明的效果：

本发明的方法及系统，可以适用于所有类型的数码媒体数据，没有特定媒体特性。本发明显著减少在非标准装置中非法复制媒体数据的可能性，把媒体数据只限制给数据传送许可的个人。

为进一步说明本发明的上述目的、结构特点和效果，以下将结合附图对本发明进行详细的描述。

（4）附图说明

图 1 是关于本发明的媒体数据编码方法及系统的图；

图 2 是使用关于本发明的媒体认证，检出实际密码钥匙的过程；

图 3 是关于本发明的自动密码钥匙更新过程。

（5）具体实施方式

下面参照本发明的实施例的附图，对本发明的防止数码媒体复制的方法及系统的实施方式作详细说明。

图 1 所示的关于本发明的媒体保护方法及系统是，以一般的混合密码原理为基础。首先，媒体数据组加密以相当于原来媒体密码钥匙的对称运算法加密。之后把持有媒体识别附的原来媒体密码钥匙加密，生成中间密码钥匙。接下来，中间密码钥匙对各个可用装置的公开的密码钥匙，独立加密。之后加密的媒体数据组和加密的中间密码钥匙传达到一个以上的目标播放装置。

在可用播放装置中，播放接收一个的媒体数据组时，上述可用播放装置使用自己的密码钥匙（实际密码钥匙），通过中间密码钥匙解码器解译接收的中间密码钥匙。这里接收的中间密码钥匙，事先加密为上述可用播放装置的公开的密码钥匙。上述可用播放装置用媒体识别符，解译被媒体密码钥匙解码器解码的中间密码钥匙，得到原来的媒体密码钥匙。最后，上述可用播放装置用原来的媒体密码钥匙经媒体数据解码器解译上述传达的媒体数据组，得到原来的媒体数据组。这

些过程在图 1 及图 2 有示。选择中间密码钥匙的公开的密码钥匙加密及媒体数据组的媒体加密的密码级别，加密的数据可以抵抗周知的类型攻击，保证安全。

一般，其他组的可用播放装置，各自有不同的密码钥匙。把装置群化的原理，不属于本发明的范围。媒体数据组传达到各自有不同密码钥匙的装置时，数据组需要包含几种媒体密码钥匙的其他样本。其中一个要求是，为各装置的密码钥匙服务。各装置为了得到有效媒体密码钥匙，要求可以识别加密的样本。这点可以以数码媒体格式-特定方式为之。

另外，各装置因密码钥匙撤销处理过程，可以得到多种可利用密码钥匙，即，当前一个密码钥匙和多个撤销的以前密码钥匙。上述以前密码钥匙保存在可重复记录的存储器。被播放装置当前播放的媒体数据组可以成为新的数据组或已播放的已有数据组。在这种情况，为了在可利用的密码钥匙中识别有效的密码钥匙，可以使用包含在媒体数据组的媒体认证。

所有媒体数据组都包括多个媒体认证，其中一个是，给有同一密码钥匙的装置的各组服务的。媒体认证包括装置组的密码钥匙标识符和媒体标识符。密码钥匙标识符是各装置的公开的密码钥匙，把媒体标识符以加密生成。用这样的方式，每个可用装置解译媒体标识符，比较每个上述密码钥匙标识符和保存在播放装置的可用密码钥匙，很容易地识别自己的密码钥匙。

播放装置需要有，保存以前所有加密的密码钥匙的安全的可记录的存储器（密码钥匙数据库）。保存在存储器的所有数据，必须加密为当前公开的密码钥匙。在播放媒体数据组之前，播放装置初始化如图 2 所示的搜索合适密码钥匙的过程。如图所示，包含，最近密码钥匙的保存的所有最近密码钥匙，经密码钥匙选择器得到选择的密码钥匙，接收包含可用播放装置的密码钥匙识别符的媒体认证，搜索相当于上述密码钥匙识别符的实际密码钥匙的密码钥匙鉴定器，一直搜索到发现符合选择的密码钥匙为止，测试为媒体认证。如果没有发现符合的密码钥匙，媒体数据组就当作不能播放。；

对于装置的密码钥匙变更，密码钥匙-更新认证可以与媒体数据组一起传达到装置。媒体数据组的密码钥匙-更新认证的保存不属于本发明的范围。密码钥匙-更新认证包含一对装置的新的公开和密码钥匙，这对公开及密码钥匙以装置的主要公开的密码钥匙加密。装置的主要公开的密码钥匙和相应的主密码钥匙（私用），

保存在装置内部。为了安全，装置的主密码钥匙需要以装置的最近公开的密码钥匙加密。认证包括，以前的密码钥匙到最近的密码钥匙的公开的密码钥匙及决定密码钥匙序列的时间记号。

首先，密码钥匙-更新认证使用装置中主密码钥匙处理，经时间显示分析器中的时间记号被分析出来，如果处理的密码钥匙-更新认证是最近时，抽出的最近的公开的密码钥匙及主密码钥匙（私用钥匙）代替以前的密码钥匙。以前的密码钥匙包含在以前的密码钥匙数据库，整个数据库和主密码钥匙，以新的公开的密码钥匙再加密。这样的过程如图 3 有示。

装置的主密码钥匙变更虽然没有可能性，但是并不意味着不产生变更。装置的主密码钥匙偶然变更时，新的媒体数据组要以和主密码钥匙相关联的密码钥匙-更新认证形成，接收这样的媒体数据组的装置把其主密码钥匙代替为客户服务。

综上所述本发明的防止数码媒体复制的方法，包括，

a)利用属于原来媒体密码钥匙的运算法，对原来媒体数据组进行加密的步骤；b)把上述原来的媒体密码钥匙以媒体标识符加密，生成加密的中间密码钥匙的步骤；c)用可以利用上述中间密码钥匙的播放装置的公开的密码钥匙进行加密的步骤；d)包含上述加密的媒体数据组和，上述加密的中间密码钥匙和，上述播放装置的密码钥匙识别符的媒体认证传达给上述播放装置的步骤；e)搜索相当于上述密码钥匙识别符的实际密码钥匙的步骤；f)用上述实际密码钥匙解译上述传达的中间密码钥匙的步骤；g)用上述媒体认证解译上述解码的中间密码钥匙，得到上述原来的媒体密码钥匙的步骤；h)用上述得到的媒体密码钥匙，解译上述传达的媒体数据组的步骤。

本发明的防止数码媒体复制的系统，包括：

密码钥匙鉴定器，接收包含可用播放装置的密码钥匙识别符的媒体认证，搜索相当于上述密码钥匙识别符的实际密码钥匙密码钥匙鉴定器；中间密码钥匙的解码器，接收密码化的中间密码钥匙，用上述实际密码钥匙解码上述中间密码钥匙；媒体密码钥匙解码器，把上述解码的中间密码钥匙以媒体识别符解码，得到原来的媒体密码钥匙；媒体数据解码器，接收密码化的媒体数据组，用上述原来的媒体密码钥匙，解译上述媒体数据组。

本技术领域中的普通技术人员应当认识到，以上的实施例仅是用来说明本发明，而并非用作为对本发明的限定，只要在本发明的实质精神范围内，对以上所述实施例的变化、变型都将落在本发明权利要求书的范围内。

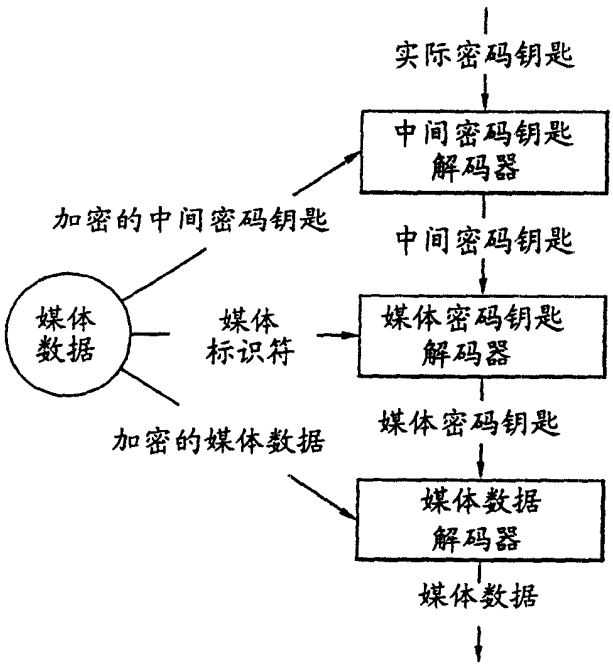

实际密码钥匙
中间密码钥匙解码器
加密的中间密码钥匙
中间密码钥匙
媒体数据
媒体标识符
媒体密码钥匙解码器
媒体密码钥匙
加密的媒体数据
媒体数据解码器
媒体数据

图 1

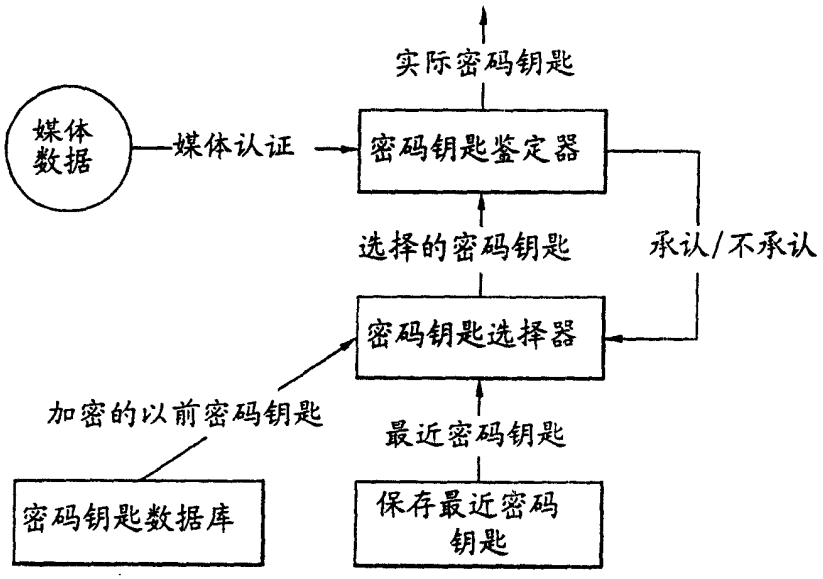

实际密码钥匙
媒体数据
媒体认证
密码钥匙鉴定器
选择的密码钥匙
承认/不承认
密码钥匙选择器
加密的以前密码钥匙
最近密码钥匙
密码钥匙数据库
保存最近密码钥匙

图 2

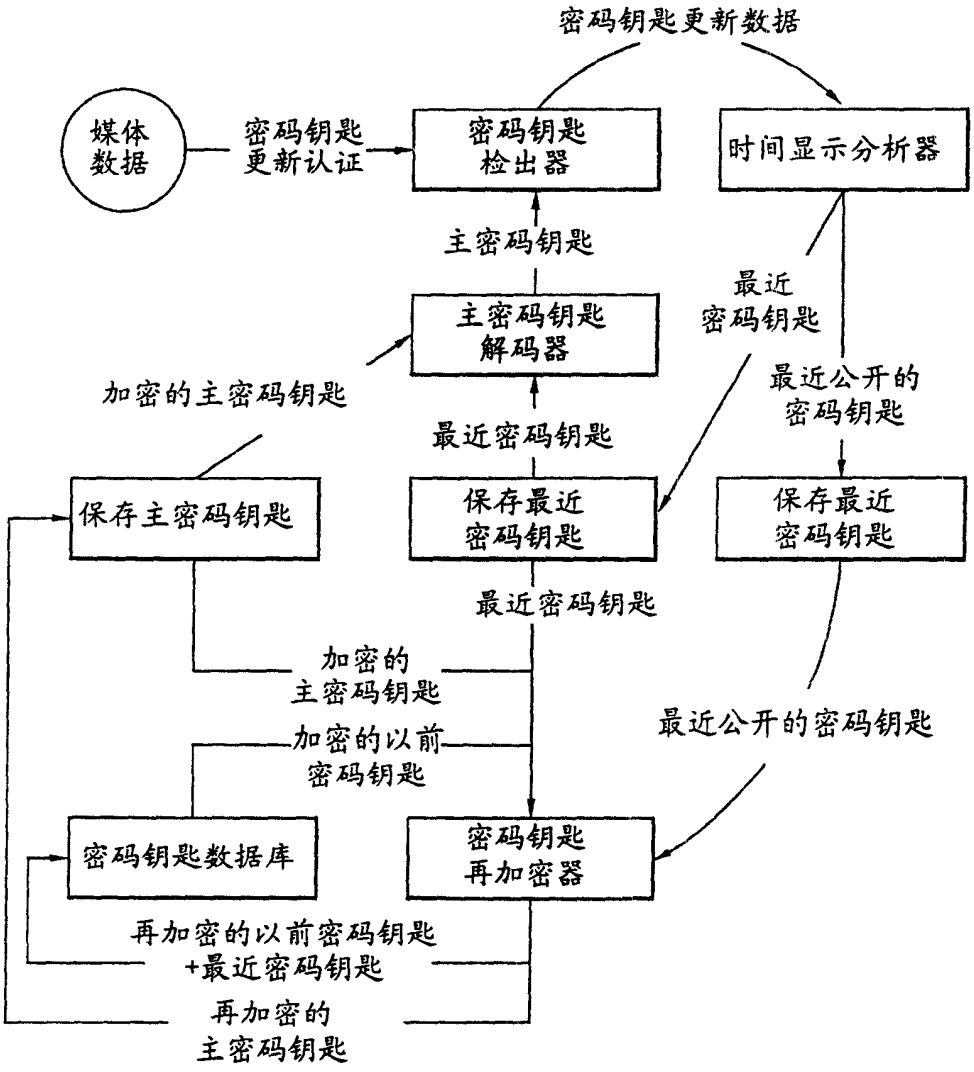

密码钥匙更新数据
媒体数据
密码钥匙更新认证
密码钥匙检出器
时间显示分析器
主密码钥匙
最近密码钥匙
主密码钥匙解码器
加密的主密码钥匙
最近公开的密码钥匙
最近密码钥匙
保存主密码钥匙
保存最近密码钥匙
保存最近密码钥匙
最近密码钥匙
加密的主密码钥匙
加密的以前密码钥匙
最近公开的密码钥匙
密码钥匙数据库
密码钥匙再加密器
再加密的以前密码钥匙+最近密码钥匙
再加密的主密码钥匙

图 3