[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 7/16
H04N 5/913 H04N 5/00

[12] 发明专利说明书

[21] ZL 专利号 01808216.5

[45] 授权公告日 2005 年 3 月 23 日

[11] 授权公告号 CN 1194548C

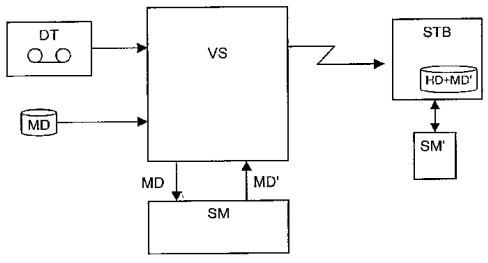
[22] 申请日 2001.4.11 [21] 申请号 01808216.5
[30] 优先权
[32] 2000. 4.17 [33] EP [31] 00810331.9
[32] 2000. 6.15 [33] CH [31] 1179/2000
[86] 国际申请 PCT/IB2001/000604 2001.4.11
[87] 国际公布 WO2001/080563 法 2001.10.25
[85] 进入国家阶段日期 2002.10.17
[71] 专利权人 纳格拉影像股份有限公司
地址 瑞士洛桑
[72] 发明人 菲利普·史特兰斯基
审查员 刘琳琦
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 王永刚

权利要求书 2 页 说明书 6 页 附图 1 页

[54] 发明名称 安全数据系统和方法

[57] 摘要

本发明是有关一种声频/视频数据的传送和存储的系统和方法，该数据为加密形式，在一分发中心和至少一个开发组件之间。 替代传送信息，允许解密与该数据并行，这些信息被重新集合在解密数据文档中，而该文档同等地包括定义该声频/视频信号的访问条件的数据。 此文档被存储，与该数据无关，并且可以被立即使用或者延缓使用。



ISSN1008-4274

1. 一种声频/视频数据的安全传输系统，该声频/视频数据被至少一个控制字加密，所述声频/视频数据相伴于被加密的、被称为解密信息文件的文件，该文件包括控制字和由所述声频/视频数据的供应商确定的被加密声频/视频数据的第一使用条件，其特征在于，此系统包括解密此文件的工具，核实第一使用条件是否完成的工具，并且如果完成，通过将所述文件与由分发商定义的第二使用条件相联系，来重新加密该文件的工具。

2. 根据权利要求 1 的系统，其特征在于，第二使用条件包括确定被加密的声频/视频数据的立即使用的权利的访问信息，和确定被加密的声频/视频数据的延缓使用的权利的访问信息。

3. 根据权利要求 2 的系统，其特征在于，确定延缓使用的权利的访问信息包括使用时间限制或最大使用数目。

4. 根据权利要求 1 到 3 中任一项的系统，其特征在于，此系统属于一个视频服务器，该视频服务器被提供了一个负责确定一种数据的安全组件，该数据确定对于该声频/视频数据的访问条件。

5. 一种用于声频/视频数据的安全传输的方法，该声频/视频数据被至少一个控制字加密，所述方法包括以下步骤：

为声频/视频数据加密，以控制字为解密钥匙，该解密钥匙在对应所述声频/视频数据的供应商的第一位置内随时间变化；

加密由解密钥匙和由供应商确定的该声频/视频数据的第一访问条件形成的文件；

不依赖于此文件地传送和存储该声频/视频数据；

当这些声频/视频数据被一个分发商使用时，将此文件传送给一个安全组件，后者负责解密所述文件并且核实第一访问条件，

用第二访问条件重新加密该文件，该第二访问条件对应由分发商确定的条件。

6. 根据权利要求5的方法，其特征在于，它包含通过确定被加密声频/视频数据的立即使用权的信息和确定所述被加密声频/视频数据的延缓使用权的信息来确定该第二访问条件。

安全数据系统和方法

技术领域

本发明涉及数据保密的领域，特别是在传输过程中的数据保密。

背景技术

根据一个典型的分配方案，数据发生器，或者是声频/视频信息或者是一个电脑程序，将它们传送给负责分发它们以付款的分发商。

根据一个已知的方案，数据就没有被扰码地存储在分发商处，当数据被传送到最终的消费者时，分发商具有加密的方法。

数据通常通过一种途径如电缆链接，或者通过发送一数据载体如磁带，从供应商处传送给分发商。

已经证明该传送存在一种非法复制的重要危险，全部资料很容易被复制。

面对这种情况，供应商和分发商只有在加密该数据后才同意这些数据的传送。

从这些数据传送过程中的非法偏差的观点看来，这种解决方法是令人满意的。一旦数据安全的到达，他们就被存储在用于批发它们的视频服务器上。

尽管如此，一旦数据被传送到分发商，供应商就失去了对他/她的数据的控制，并且恶意的人会从视频服务器中进行违法的复制。

当分发商就这些加密的数据传送给最终的消费者时，相同的问题就出现了，这些消费者拥有将它们解密的手段，并且因此可以得到未扰码的数据，未经授权的复制就从消费者那里发生了。

而且，数据传送领域的加密模式的启用由加在其上的所用算法限制安全可能性。

发明内容

本发明的目的在于确保在所有不同的中介媒体中的数据分发，该中介媒体确保控制这些数据的使用者的数目。

这样，负责解密声频/视频数据的单元将根据条件访问信息决定使用者是否具有必要的权利。

当以一种规范施加的时候，第二类加密的使用允许在已知系统的基础上加强加密。

本发明提供一种声频/视频数据的安全传输系统，该声频/视频数据被至少一个控制字加密，所述声频/视频数据相伴于被加密的、被称为解密信息文件的文件，该文件包括控制字和由所述声频/视频数据的供应商确定的被加密声频/视频数据的第一使用条件，其特征在于，此系统包括解密此文件的工具，核实第一使用条件是否完成的工具，并且如果完成，通过将所述文件与由分发商定义的第二使用条件相联系，来重新加密该文件的工具。

根据本发明的上述系统，其特征在于，第二使用条件包括确定被加密的声频/视频数据的立即使用的权利的访问信息，和确定被加密的声频/视频数据的延缓使用的权利的访问信息。

根据本发明的上述系统，其特征在于，确定延缓使用的权利的访问信息包括使用时间限制或最大使用数目。

根据本发明的上述系统，其特征在于，此系统属于一个视频服务器，该视频服务器被提供了一个负责确定一种数据的安全组件，该数据确定对于该声频/视频数据的访问条件。

本发明还提供一种用于声频/视频数据的安全传输的方法，该声频/视频数据被至少一个控制字加密，所述方法包括以下步骤：为声频/视频数据加密，以控制字为解密钥匙，该解密钥匙在对应所述声频/视频数据的供应商的第一位置内随时间变化；加密由解密钥匙和由供应商确定的该声频/视频数据的第一访问条件形成的文件；不依赖于此文件地传送和存储该声频/视频数据；当这些声频/视频数据被一个分

发商使用时，将此文件传送给一个安全组件，后者负责解密所述文件并且核实第一访问条件，用第二访问条件重新加密该文件，该第二访问条件对应由分发商确定的条件。

根据本发明的上述方法，其特征在于，它包含通过确定被加密声频/视频数据的立即使用权的信息和确定所述被加密声频/视频数据的延缓使用权的信息来确定该第二访问条件。

用户层次的系统

为了使数据传送不被侵犯，被传输的流包括由控制字 CW 所加密的数据，以及包含在一个名为 MD(元数据)的文档中的加密信息。控制字作为随时间变化的解密匙。元数据的文档一方面包含用作控制字 CW 的解密匙，另一方面包含用于解密的必要权利的定义，用以直接与此传送连接的定购或者账单的支付。此文档通过 IDEA（国际数据加密算法）型算法加密，而该算法的安全性优于用控制字（CW）加密的算法。

在定购者的一方有一安全组件，通常是包括用户权利（尤其是他/她的信用）的智能卡的形式，并且将这些权利与传送所需要的那些权利比较。如果权利允许它，则安全组件将元数据的文档解码，并且送回数据解密所必需的控制字 CW。

越来越多的用户装置包括诸如硬盘那样的信息存储单元。这允许再次观看场景，以实行慢动作观看，而不会在再次观看过程中丢失任何分发的信息。

这些单元能够存储整部的电影，从而将电影提供给用户购买。在一天的流量较小的期间完成这样的下载，如果用户接受了购买交易，那么每当他/它想要时，他/她都能观看。

此过程表现出具有数字支持的不便利，而数字支持是很容易被复制的信息，其控制是必要的。在软件的传送过程中，这同样有效。实际上，用户装置可以是一台电脑，一保密组件连接在此电脑上，并且

下载可以表现为例如一个游戏程序。

根据本发明，数据可以以具有第一类加密的加密方式来传送，伴随着由根据第二类方式加密的分发密钥加密的控制消息文档。在这种文档中，同等地包括条件访问信息，用以定义立即使用的权利和与延缓使用有关的权利。

数据流以一种加密的方式存储在用户单元中，这避免了任何滥用的使用。数据的每一个的后续使用需要安全组件的存在。安全组件就控制了延缓使用的权利，例如，及时限制它，甚至仅授权它一定数目的次数。

在被授权一定数目的使用的情况下，控制消息包括传送的识别符，使用的最大数目以及最终一持久指示器。在第一次使用中，安全组件将初始化它自身用于传送的计数器，该计数器将会随着安全组件的每一次解密而增加。当达到最大值时，解密就会被禁止。

持久性指示器允许安全组件知道：用什么延时传送的计数器将能够被清除。为了不让该信息填满安全组件的存储器，当超过指示器的日期时，存储器被分配给该操作的部分能够再度被使用。有利地是从第一次使用开始标示天数（1 到 250 天）。

分发商层次的系统

分发商拥有巨大的存储单元，重新集合所有即将被分发的传送。这通常被称作视频服务器。某些传送将被分发一次，如电视信息，而其它的传送则将在几天的期间被循环分发，从而将它提供给要购买的用户。

这些传送以加密方式到达，伴随着有供应商的第一密匙加密的控制消息。这些数据以加密的方式被存储在存储单元里，避免任何漏洞或非法复制。

当使用这些数据时，视频服务器传送用于分发的加密数据。这些数据伴随着具有由视频服务器传送到安全单元的解密信息的文档。

此单元进行此文档的解密，以便提取控制字 CW，并核实使用权

利。一旦结束该操作，安全组件将新的使用权利加进这些控制字以将它们编码，这些新的权利由分发商来定义，并且能够包括用于订购的条件，或者能够将此应用与此传送的购买相链接，在此阶段定义使用或者观看的次数。

解密信息的新的文档于是与加密数据流一起被传送。

附图说明

通过以下的详细说明，其被参考提供作为非限制的实例的附图，本发明将会被更好的了解，其中：图 1 和图 2 表示本发明的两个实施例。

具体实施方式

根据我们的实例，视频服务器 VS 接收到磁带形式的数据 DT，但是该数据能够以任何已知的途径传送。解密信息文档 MD 被均等地供应给视频服务器。此文档一般被同时供应，就是说，它有利地在同一磁带上作为加密数据。不过，如果我们希望加强安全，可能通过其他途径传送 MD 文档。

一旦这两个文档在视频服务器 VS 中，该系统就作好了分发的准备。

此时，MD 文档被传送给安全组件 SM，以加进我们为此传送定义的权利。此组件给 MD 文档解码，然后加进与观看的必要权利相关的信息，并且将此由传输密钥加密的新 MD 文档送回服务器 VS。

数据 DT 以及此新文档被分发给不同的用户组件 STB。

因为没有 MD'文档就不能够完成数据 DT 的解码，所以 MD'文档一般被先送。

到达解码器 STB 的数据或者马上被处理，或者被存储在 HD 单元中供以后使用。在第二种情况下，很明显，如图 1 所示，MD'文档必须被均等地存储在 HD 单元中。

为了获得未扰码的数据，此 MD'文档存在于用户的安全组件 SM'，

因此其能够将所述文档解码，并且提取控制字 CW。

根据如图 2 所示的实施例，MD'文档仅被存储在用户的安全组件 SM'中。这样，任何寻找数据内容与 MD'文档间相互关系的企图都必定会失败。

在本发明的框架内，我们提出了一种预加密组件，该组件被指定产生加密形式的数据 DT。此组件接收未扰码的数据，并且产生配对的加密数据 DT 和 MD 文件。

根据所选择的安全结构，根据第一加密模式来加密 DT 文档，控制字 CW 作为解密钥匙。由于处理所需要的速度，最好是对称模式。这些控制字 CW 也根据第二种加密模式（例如 DES（数据加密标准））被加密。

当全部的控制字被集合在 MD 文档中时，此文档的加密是第三类的高级加密级别，例如 IDEA。实际上，对文档成功攻击的结果将比对控制字成功攻击更严重。

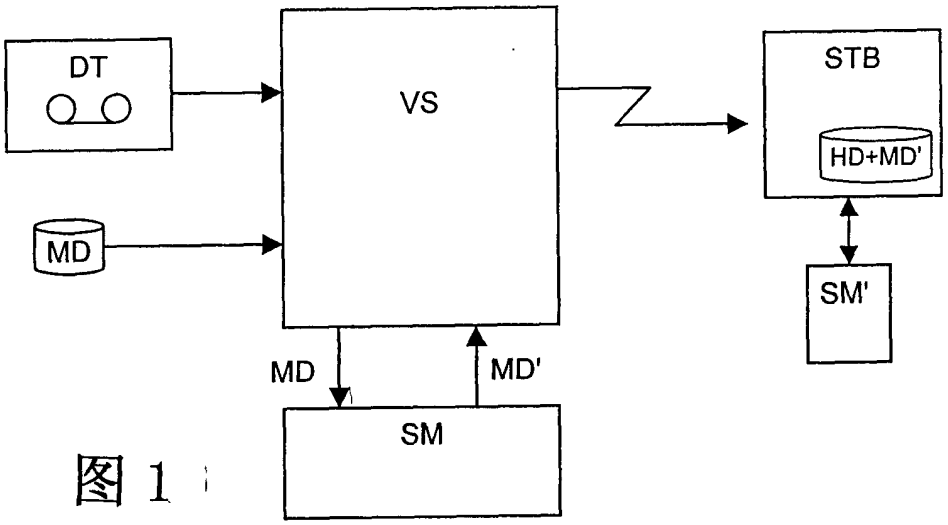


图 1

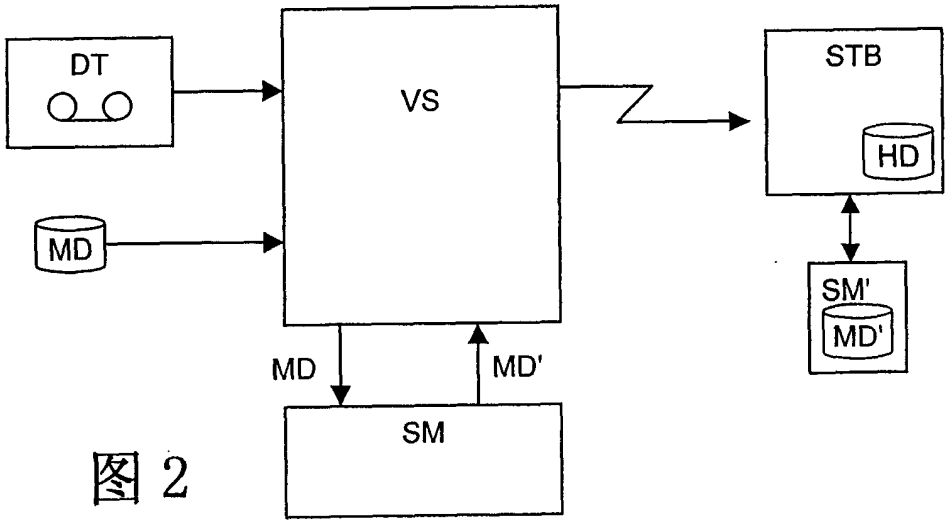


图 2