(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102300093 A
(43)申请公布日 2011.12.28

(21)申请号 201110254025.0

(22)申请日 2011.08.31

(71)申请人 华中科技大学
地址 430074 湖北省武汉市武昌珞喻路 1037 号

(72)发明人 谢长生 黄浩 姚杰 林安 赵学伟 魏明

(74)专利代理机构 武汉帅丞知识产权代理有限公司 42220
代理人 朱必武 李南平

(51)Int.Cl.
H04N 7/26(2006.01)
G06F 21/00(2006.01)
H04L 9/32(2006.01)

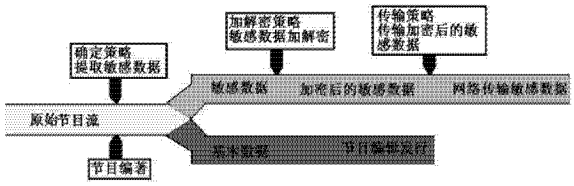
权利要求书 1 页 说明书 4 页 附图 1 页

(54)发明名称

一种用于数据文件分发的加密方法

(57)摘要

本发明提供一种用于数据文件分发的加密方法，其特征在于：将数据文件分割成敏感数据和主体数据，两种数据通过不同的途径传播和分发，在目的地使用时再做数据合成，还原成原始数据文件。本发明加密方法的优点在于，其采用数据分割技术，打破内容完整性，能够更好地保护版权；节省网络带宽，使得版权信息即时可控。



CN 102300093 A

1. 一种用于数据文件分发的加密方法，其特征在于：将数据文件分割成敏感数据和主体数据，两种数据通过不同的途径传播和分发，在目的地使用时再做数据合成，还原成原始数据文件。

2. 根据权利要求 1 所述的用于数据文件分发的加密方法，其特征在于，所述数据文件的分割在文件层进行，以块 / 记录为单位。

3. 根据权利要求 1 所述的用于数据文件分发的加密方法，其特征在于，对于音视频文件，所述数据文件的分割在容器层 / 编码层进行，以包 / 帧为单位。

4. 根据权利要求 1 所述的用于数据文件分发的加密方法，其特征在于，所述敏感数据通过安全的信道传输，该信道包括有线和无线网络，包括模拟信道和数字信道。

5. 根据权利要求 1 所述的用于数据文件分发的加密方法，其特征在于，所述主体数据通过数据存储介质发布，该数据存储介质包括光盘 \ 移动硬盘 \U 盘 \ 存储卡。

6. 根据权利要求 1 至 5 所述的用于数据文件分发的加密方法，其特征在于，敏感数据的传输和主体数据的分发过程可以加密，也可以采用明文。

一种用于数据文件分发的加密方法

技术领域

[0001] 本发明涉及一种加密方法，该方法用于数据文件的发布与分发的加密，特别用于音视频节目的分发放过程中，可以增加节目版权的安全性。

背景技术

[0002] 为了保证分发的音视频节目的安全性，有很多的研究，主要集中在节目载体（光盘和网络）安全和节目内容加密两个方面。

[0003] 在节目载体方面，主要原理是利用光盘母盘上的部分特征信息是不可再现的，当光盘内容被复制时，这些特征信息不能被复制；在网络环境，主要是 DRM 技术。目前的安全技术包括以下几种：

(1) AACS (Advanced Access Content System)

AACS 是一种内容散布和数字版权管理的标准，对新一代光盘进行读取与复制的限制。AACS 是由 AACS LA (AACS Licensing Administrator) 负责制定，使用这种技术进行加密时，首先需要将需要存入光盘的所有信息进行编码处理，而在访问这些经过编码的数据时，又必须对这些数据进行解码，然后才能正确读写这些数据。

[0004] (2) 模拟信号保护系统加密技术

模拟信号保护系统 APS 的主要作用是为了防止从光盘到光盘的复制。他的主要原理是利用 Macrovision 芯片产生的特殊信号，来影响光盘的复制功能，使得光盘的图像产生对比度不均匀、出现横纹等特征。

[0005] (3) 数字版权管理技术 (DRM)

DRM 技术的工作原理是，首先建立数字节目授权中心，编码压缩后的数字节目内容，利用密钥（Key）可以被加密保护（lock），加密的数字节目头部存放着 KeyID 和节目授权中心的 URL。用户在点播时，根据节目头部的 KeyID 和 URL 信息，就可以通过数字节目授权中心的验证授权后送出相关的密钥解密（unlock），节目方可播放。需要保护的节目被加密，即使被用户下载保存，没有得到数字节目授权中心的验证授权也无法播放，从而保护了节目的版权。

[0006] 在节目内容加密方面，针对 MPEG 和 H.264 等不同的编码格式，有很多视频数据加密算法，常见的视频加密算法可以分为如下三类：

(1) 直接加密算法：

在整个加密过程中，视频数据被看做常见的二进制信息来处理，因此加密过程的实现比较简单。加密过程是在压缩编码过程之后进行，所采用的都是传统的加密算法，如 DES，IDEA 等算法。

[0007] (2) 选择性加密算法：

它一般分为两类：部分加密算法和 DCT 系数加密算法，他们的加密过程都是在压缩编码操作之后进行的。在部分加密算法中，由于视频数据有不同的特性，所以加密算法在压缩后的码流中选取小部分敏感数据作为加密的对象，对其余非敏感数据不进行加密操作。DCT

系数加密算法是对经过扫描的到的 DCT 系数，DCT 系数符号之类的信息作为加密对象，以保证视频信息的安全性。

[0008] (3) 具有压缩编码功能的加密算法：

这类算法的主要思想是把视频信息的加密过程和压缩过程结合起来，因此加密算法也就有了压缩编码的功能，在这类实现中，加密过程和压缩过程是同时进行的。

[0009] 虽然有上述多种节目载体安全和节目内容加密技术的支持，分发的音视频节目的数据还是存在安全性问题。由于内容和密钥的无关性，而且加密算法无法频繁更新，在计算机技术飞速发展的今天，很难保证加密算法不被破解，一旦被破解，由于节目载体（如光盘）上节目内容的完整性，将导致版权的丢失，DVD 盗版光盘泛滥就是一个典型例子。

[0010] 现有的数字光盘加密、分发方法，例如专利号为：200610018258.X 的《一种用于光盘存储的数据加扰、解读方法》对用户数据采用原始密码加扰；用户数据解扰需要的原始密码经过多重加密后作为光盘加密密码——模拟密码；将加扰后的用户数据和模拟密码以分离或混合的方式记录在光盘上，解密时也采用同步或异步时序进行；采用专用 IC 序列号管理来协调内容提供商，母盘制造商和芯片制造商之间的关系，该专用 IC 负责将加密后的数字密码转换成模拟密码，每个 IC 都有一个专门的序列号，该序列号强制出现在母盘和光盘上。然而，该加密方法存在的缺点是：尽管采用了多重加密方法，然而由于该光盘上承载了完整的数据信息，所以该光盘仍然存在被破解和盗版的可能。

[0011] 有鉴于此，有必要提供一种用于数据文件分发的加密方法，其采用数据分割技术，打破内容完整性，能够更好地保护版权。

发明内容

[0012] 本发明的目的是：提出一种基于数据分割的安全的数据文件分发技术，把视频文件分割成敏感数据和主体数据两部分，主体数据占总数据量的 90% 以上，其中主体数据加密后通过存储介质（如光盘 / 移动硬盘 /U 盘等）来分发，敏感数据加密后通过网络来传输，从而使光盘内容即使被破解，也无法还原节目内容，从而更好地保护版权。

[0013] 本发明的技术方案是：一种用于数据文件分发的加密方法，其特征在于：将数据文件分割成敏感数据和主体数据，两种数据通过不同的途径传播和分发，在目的地使用时再做数据合成，还原成原始数据文件。

[0014] 如上所述的用于数据文件分发的加密方法，其特征在于，所述数据文件的分割在文件层进行，以块 / 记录为单位。

[0015] 如上所述的用于数据文件分发的加密方法， 其特征在于，对于音视频文件，所述数据文件的分割在容器层 / 编码层进行，以包 / 帧为单位。

[0016] 如上所述的用于数据文件分发的加密方法， 其特征在于，所述敏感数据通过安全的信道传输，该信道包括有线和无线网络，包括模拟信道和数字信道。

[0017] 如上所述的用于数据文件分发的加密方法， 其特征在于，所述主体数据通过数据存储介质发布，该数据存储介质包括光盘 \ 移动硬盘 \U 盘 \ 存储卡。

[0018] 如上所述的用于数据文件分发的加密方法， 其特征在于，敏感数据的传输和主体数据的分发过程可以加密，也可以采用明文。

[0019] 本发明的有益效果是：由于数据文件被分割为两部分：主体数据和敏感数据，分

割的目标在于，用最少的网络带宽来传输数据，来达到加密的效果。这样做的好处在于：

(1) 安全性提高了，即使在最坏的情况下，主体数据被破解了，那么由于缺乏网络传输部分的敏感数据，仅有主体数据，节目播放时无法得到用户满意的效果；

(2) 网络带宽占有量可接受，具有实际价值；

(3) 可以动态调整加密策略，升级加密算法，以应对安全威胁。

[0020]

附图说明

[0021] 图 1 是采用本发明的用于数据文件分发的加密方法实现的节目加密和发行过程的原理图。

[0022] 图 2 是采用本发明的用于数据文件分发的加密方法实现的节目解密和播放过程的原理图。

具体实施方式

[0023] 以下结合附图和实施例对本发明做进一步的说明。

[0024] 本发明的目的是提出一种基于数据分割的安全的节目分发技术。当前，网络带宽发展很快，普通用户普遍可以获得 2M 以上的带宽。因此，我们设想通过把视频文件切割成两部分敏感数据和主体数据。其中，敏感数据是一个比较小的部分，占总数据量的 0.1% 到 10% 不等，主体数据占总数据量的 90% 以上。其中，主体数据加密后通过存储介质（如光盘 / 移动硬盘 /U 盘等）来分发，敏感数据加密后通过网络来传输。分割的目标在于，用最少的网络带宽来传输数据，来达到加密的效果。

[0025] 具体来说，可以采用如下三个层次的基本的数据分割机制，在实际应用中，这三个机制是可以混合使用的。

[0026] (1) 文件层分割

在这个层次下，我们将一个媒体文件当做一个普通的文件来处理。通过调用相应的文件操作接口函数，可以把这个普通文件按照一定比例分成一大一小两个文件。小的部分是该视频信息的敏感数据，一般存放在服务器端，对于经过服务器认证的合法用户，可以通过网络将敏感数据发送给播放机。大的部分视频数据（主体数据）通常被存放在光盘上，通过商业渠道分发给用户。

[0027] (2) 容器层分割

经过压缩编码后得到的音视频帧，会被封装成数据包的形式存放在容器内部。由于视频帧比较大，所以一个数据包中通常只包含一个视频帧。而音频帧和字母帧的数据量比较小，所以一个数据包中通常会含有多个音频帧或者字幕。

[0028] 在容器层的分割过程中，首先需要在服务器端解析整个多媒体文件，得到了数据包序列。根据我们的算法思想，在所有的数据包序列中，按一定的比例提取数据包作为敏感数据，同时将其余部分的数据作为主体数据存放在光盘上。

[0029] 在这种机制下，敏感数据是由一序列的数据包组成，彼此之间具有相当的时间间隔。这样播放机要做的就是把通过网络接口收到的敏感数据包进行拆包，得到音 / 视频或者字母帧，然后进行后续的解密、解码等操作。

[0030] (3) 编码层分割

上面的方法与文件层分割相比较，播放机将相当数量的工作转移到了服务器端(解复用操作)，但是播放机仍然需要自己拆数据包，已得到能够用于解码的音视频或者字母数据帧。可以设想这部分工作也交给服务器端来实现，即就是编码层的分割方式。

[0031] 这种方式的实现方式与前两种方式类似，只是在提取敏感数据时，需要先在服务器端对整个输入文件进行解复用和解包，得到各个轨道的音视频数据帧序列，这时可以有多种选择来提取敏感数据。例如：可以只在视频帧中提取一定量的数据作为敏感数据，而对其他所有轨道不进行操作。这样的话，用户在没有获得敏感数据而播放时，由于缺失一定数量的视频帧，画面会出现马赛克现象，无法满足用户的需求(虽然音频和字幕信息不受影响)。

[0032] 下面举一具体实施例来说明本发明的用于数据文件分发的加密方法的实现过程：

在图一中，原始节目以文件的方式存储，文件大小为 5GB，我们以文件层模式提取敏感数据，比例为 0.2%，这样，敏感数据部分的大小为 10MB，主体数据部分为 4.99GB。

[0033] 敏感数据加密后存放在专门的版权服务器上，等待用户申请，传输给目标用户，主体数据经过编著后做成光盘，分发放给目标用户。

[0034] 在图二中，目标用户使用联网的光盘播放机来观看光盘上的节目。

[0035] 当他开始播放时，播放机会向版权服务器申请节目的敏感数据，只要该用户有合法的权限，他就可以得到敏感数据(经由网络传输，由服务器端下载至播放机)。

[0036] 播放机中的导航软件将敏感数据和光盘中的主体数据解密并合成，这样，该用户就可以合法地欣赏这个节目了。

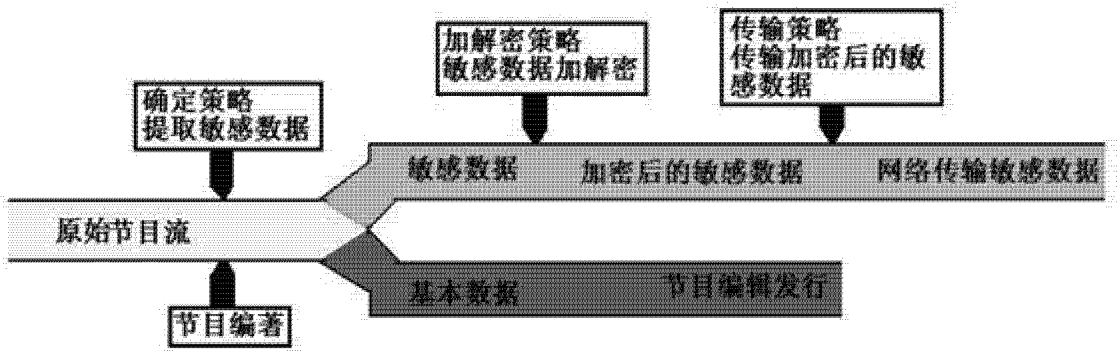

加解密策略
敏感数据加解密
传输策略
传输加密后的敏感数据
确定策略
提取敏感数据
敏感数据
加密后的敏感数据
网络传输敏感数据
原始节目流
基本数据
节目编辑发行
节目编著

图 1

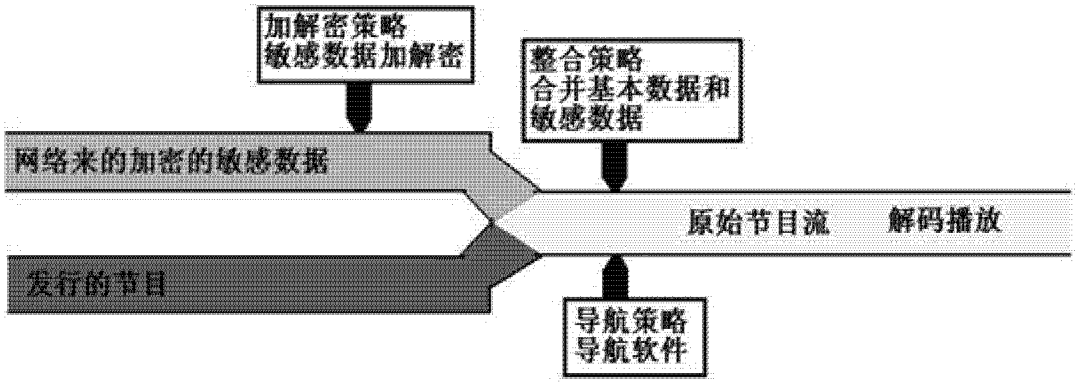

加解密策略
敏感数据加解密
整合策略
合并基本数据和敏感数据
网络来的加密的敏感数据
原始节目流
解码播放
发行的节目
导航策略
导航软件

图 2