

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



# [12] 发明专利说明书

专利号 ZL 02801720. X

H04N 5/91 (2006.01)  
H04N 7/08 (2006.01)  
G11B 20/10 (2006.01)  
G06F 12/14 (2006.01)  
G06F 12/00 (2006.01)

[45] 授权公告日 2006年7月19日

[11] 授权公告号 CN 1265629C

[22] 申请日 2002.4.9 [21] 申请号 02801720. X

[30] 优先权

[32] 2001. 4. 9 [33] JP [31] 110541/01

[86] 国际申请 PCT/JP2002/003531 2002.4.9

[87] 国际公布 WO2002/085011 日 2002.10.24

[85] 进入国家阶段日期 2003.1.16

[71] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 石坂敏弥 山田诚 石黑隆二

审查员 龚锦玲

[74] 专利代理机构 北京市柳沈律师事务所

代理人 马莹 邵亚丽

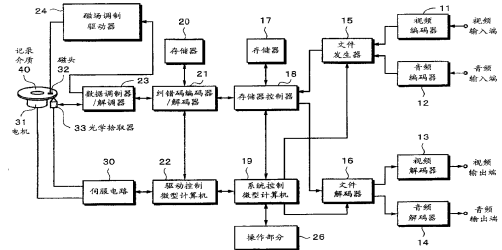
权利要求书 2 页 说明书 17 页 附图 16 页

## [54] 发明名称

记录保护无形财产的信息的记录设备及其记录方法

## [57] 摘要

根据本发明的记录设备包括转换装置 15、18、19、和记录装置 23、24、32、33。转换装置 15、18 和 19 把数据的数据结构转换成可以通过软件来管理的文件结构。记录装置 23、24、32 和 33 把数据记录到记录媒体上。文件结构拥有作为实体数据的第一数据单元、作为数个第一数据单元的集合的第二数据单元、和描述管理数个第一数据单元与第一数据单元的实体数据的属性之间的相互关系的管理信息的数据部分。数据部分包含保护数据的无形财产所需的保护信息。



1. 一种把数据记录到可重写记录媒体上的记录设备, 所述记录设备包括:  
转换装置, 用于把数据的数据结构转换成可以通过软件来管理的文件结  
5 构; 和  
记录装置, 用于把已经转换成文件结构的数据记录到记录媒体上,  
其中, 文件结构拥有作为实体数据的第一数据单元、作为数个第一数据  
单元的集合的第二数据单元、和描述管理数个第一数据单元与第一数据单元  
的实体数据的属性之间的相互关系的管理信息的数据部分, 和  
10 其中, 数据部分包含保护给与第一数据单元的无形财产权的权利所需的  
保护信息。
2. 根据权利要求1所述记录设备,  
其中, 保护信息包含在独立文件中, 而不是包含在数据部分中, 和  
其中, 数据部分包含指定文件的指定信息。
- 15 3. 根据权利要求1所述记录设备,  
其中, 与预定加密方法相对应地加密实体数据, 和  
其中, 保护信息是解密加密实体数据所需的密钥。
4. 根据权利要求3所述记录设备,  
其中, 与预定加密方法相对应地加密密钥, 和  
20 其中, 数据部分还包括解密加密密钥所需的密钥。
5. 根据权利要求3所述记录设备,  
其中, 与预定加密方法相对应地加密密钥, 和  
其中, 记录装置还把包含解密加密密钥所需的密钥的文件记录到记录媒  
体上。
- 25 6. 根据权利要求1所述记录设备,  
其中, 保护信息包含开始使用实体数据的开始时间和停止使用实体数据  
的终止时间的至少一个。
7. 根据权利要求1所述记录设备,  
其中, 保护信息是限制可以再现实体数据的次数的次数限制信息。
- 30 8. 根据权利要求1所述记录设备,  
其中, 保护信息是限制可以复制实体数据的次数的复制限制信息。

9. 根据权利要求1所述记录设备，  
其中，保护信息是标识实体数据是原始实体数据还是复制实体数据的复制标识信息。
10. 根据权利要求1所述记录设备，  
5 其中，数据部分还包含标识保护信息是否已经被篡改的篡改标识信息。
11. 根据权利要求1所述记录设备，其中：  
所述数据是构成运动图像的各个视频数据；  
所述第一数据单元是第一视频数据单元；和  
所述第二数据单元是第二视频数据单元。
- 10 12. 一种把数据记录到可重写记录媒体上的记录方法，所述记录方法包括如下步骤：  
把数据的数据结构转换成可以通过软件来管理的文件结构；和  
把已经转换成文件结构的数据记录到记录媒体上，  
其中，文件结构拥有作为实体数据的第一数据单元、作为数个第一数据  
15 单元的集合的第二数据单元、和描述管理数个第一数据单元与第一数据单元的  
实体数据的属性之间的相互关系的管理信息的数据部分，和  
其中，数据部分包含保护给与第一数据单元的无形财产权所需的保护信息。

## 记录保护无形财产的信息的记录设备及其记录方法

## 5 技术领域

本发明涉及把视频数据和音频数据记录在记录媒体上的记录设备，尤其涉及具有保护无形财产之类已经给与记录在记录媒体上的数据的权利的功能的记录设备。另外，本发明还涉及供这样的记录设备使用的记录方法、记录媒体、和程序。

10

## 背景技术

视频数据、音频数据、或计算机程序的数据在工厂中记录到记录媒体上，然后，分配给用户。或者，通过通信线把它们下载到记录媒体，然后再分配给用户。

15 这样的记录媒体是，例如，诸如 CD (Compact Discs, 激光唱盘) 和 DVD (Digital Versatile Discs or Digital Video Discs, 数字多功能盘或数字视频盘) 之类的光盘、诸如 MD (Mini Discs, 小型盘) 之类的磁光盘、和存储卡。

但是，当把数据分配给用户时，有必要保护诸如版权和专利权之类已经给与数据的无形财产。

20 因此，本发明的一个目的是提供具有保护已经给与数据的无形财产的功能的记录设备。

另外，本发明的另一个目的是提供保护无形财产的记录方法、把数据记录在上面以使无形财产受到保护的记录媒体、和使无形财产能够得到保护的程序。

25

## 发明内容

本发明是把数据记录到可重写记录媒体上的记录设备，它包括：转换装置，用于把数据的数据结构转换成可以通过软件来管理(handle)的文件结构；和记录装置，用于把已经转换成文件结构的数据记录到记录媒体上，其中，  
30 文件结构拥有作为实体数据的第一数据单元、作为数个第一数据单元的集合的第二数据单元、和描述管理数个第一数据单元与第一数据单元的实体数据

的属性之间的相互关系的管理信息的数据部分，并且其中，数据部分包含保护给与第一数据单元的无形财产权所需的保护信息。

根据本发明，在记录设备中，保护信息可以包含在独立文件中，而不是包含在数据部分中。数据部分可以包含指定文件的指定信息。

- 5 根据本发明，在记录设备中，为了安全地保护无形财产权，最好，与预定加密方法相对应地加密实体数据，以及保护信息是解密加密实体数据所需的密钥。另外，最好，与预定加密方法相对应地加密密钥，和数据部分还包括解密加密密钥所需的密钥。

- 10 根据本发明，在记录设备中，为了安全地保护无形财产权，最好，数据部分还包含标识保护信息是否已经被篡改的篡改标识信息。

- 根据本发明，在记录设备中，为了安全地保护无形财产权，最好，保护信息包含开始使用实体数据的开始时间和停止使用实体数据的终止时间的至少一个。另外，最好，保护信息是限制可以再现实体数据的次数的次数限制信息。此外，最好，保护信息是限制可以复制实体数据的次数的复制限制信息。并且，最好，保护信息是标识实体数据是原始实体数据还是复制实体数据的复制标识信息。

- 20 因此，根据本发明，由于相互关联地记录保护无形财产权的保护信息和实体数据，可以安全地保护实体数据免遭侵犯。另外，由于把保护信息加入每个第一数据单元中，可以安全地保护各个实体数据，而不是每个记录媒体免遭侵犯。因此，可以为每个第一数据单元提供各种业务。

#### 附图说明

- 图 1 是显示数字记录和再现设备的结构例子的方块图；
- 图 2 是显示 QuickTime 电影(movie)文件的结构例子的示意图；
- 25 图 3 是显示视频媒体信息原子(atom)的结构例子的示意图；
- 图 4 是显示根据本发明一个的实施例的 QuickTime 电影文件的结构的示意图；
- 图 5 是显示根据本发明实施例的样本描述表的结构示意图；
- 图 6 是显示权利管理数据的结构的示意图；
- 30 图 7 是显示电影数据原子的结构的示意图；
- 图 8 是显示实体数据与媒体原子之间的关系示意图；

- 图 9 是显示在管理加密密钥的情况下样本描述表的结构示意图；  
 图 10 是显示允许(enable)密钥块单元的标志的定义的示意图；  
 图 11 是说明保护信息块是独立文件的情况的示意图；  
 图 12 是显示允许密钥块的数据结构的示意图；  
 5 图 13 是说明权利保护方法与提供的业务之间的第一种关系的示意图；  
 图 14 是说明权利保护方法与提供的业务之间的第二种关系的示意图；和  
 图 15 是说明权利保护方法与提供的业务之间的第三种关系的示意图。

### 具体实施方式

- 10 接着，参照附图，描述本发明的实施例。在附图中，相同的标号表示相同的结构。

图 1 是显示数字记录和再现设备的结构例子的方块图。

- 在图 1 中，数字记录和再现设备包括视频编码器 11、音频编码器 12、视频  
 15 解码器 13、音频解码器 14、文件发生器 15、文件解码器 16、存储器 17 和  
 20、存储器控制器 18、系统控制微型计算机 19、纠错码编码器/解码器 21、  
 驱动控制微型计算机 22、数据调制器/解调器 23、磁场调制驱动器 24、操作  
 部分 26、伺服电路 30、电机 31、磁头 32、和光学拾取器 33。

- 20 视频信号从视频输入端输入。把视频信号供应给视频编码器 11。视频编  
 码器 11 压缩和编码视频信号。音频信号从音频输入端输入。把音频信号供应  
 25 给音频编码器 12。音频编码器 12 压缩和编码音频信号。视频编码器 11 和音  
 频编码器 13 的输出信号被称为基本流。

- 25 根据该实施例，假设数字记录和再现设备是与摄像机合并在一起的设备。  
 视频信号是作为视频摄像机拍摄的画面供应的。光学系统把对物体拍摄的光  
 供应给诸如 CCD（电荷耦合器件）之类的拍摄器件，生成视频信号。提供由  
 30 麦克风收集的声音作为音频信号。

- 30 当压缩和编码过程对应于 MPEG（运动图像专家组）系统时，视频编码  
 器 11 包括模拟/数字转换器（下文简称为 A/D 转换器）、格式转换部分、屏幕  
 重排部分、相减部分、DCT（离散余弦变换）部分、量化部分、可变长度代  
 码编码部分、缓冲存储器、速率控制部分、逆量化部分、逆 DCT 部分、相加  
 35 部分、帧存储器、运动补偿和预测部分、和开关，作为电路线路。

把视频信号供应给视频编码器 11。A/D 转换器数字化视频信号。格式转

换部分把数字化信号转换成用在编码过程中的空间分辨率。屏幕重排部分重排画面的顺序，以便在编码过程中可以适当地处理它们。屏幕重排部分的输出信号通过相减部分输入到 DCT 部分。DCT 部分对屏幕重排部分供应的信号进行 DCT 编码处理。把 DCT 部分的输出信号输入量化部分。量化部分利用预定位数量化 DCT 部分的输出信号。把量化部分的输出信号输入可变长度代码编码部分和逆量化部分。可变长度代码编码部分利用诸如 Huffman (霍夫曼) 码之类的可变长度代码编码量化部分的输出信号。把编码数据输出到缓冲存储器。缓冲存储器以预定速率输出编码数据，作为视频编码器的输出。由于可变长度代码编码部分生成的代码量是可变的，因此，速率控制部分监视缓冲存储器和控制量化部分的量化操作，以便保持预定的位速率。

另一方面，由于 I 画面和 P 画面被运动补偿和预测部分用作参考屏幕，从量化部分输入逆量化部分的信号被逆量化，然后输入逆 DCT 部分。逆 DCT 部分对逆量化信号进行逆 DCT 处理。逆 DCT 部分的输出信号和运动补偿和预测部分的输出信号由相加部分相加。把相加信号输入帧存储器。把帧存储器的输出信号输入运动补偿和预测部分。运动补偿和预测部分对帧存储器的输出信号进行前向预测、反向预测、和双向预测。运动补偿和预测部分的输出信号输出到相加部分和相减部分。逆量化部分、逆 DCT 部分、相加部分、帧部分、和运动补偿和预测部分构成与视频解码器输出相同解码视频信号的局部解码部分。

相减部分从运动补偿和预测部分的输出信号中减去屏幕重排部分的输出信号，获得视频信号与局部解码部分解码的解码视频信号之间的预测误差。当进行帧内编码处理（即，提供 I 画面）时，开关使相减部分不进行对它们的相减处理。换言之，把 I 画面提供给 DCT 部分。

返回到图 1，当使用，例如，MPEG/音频层 1/层 2 (MPEG/Audio layer/layer 2) 时，音频编码器 12 还包括子频带编码部分和自适应量化位指定部分，作为电子线路。音频信号被子频带编码部分划分成 32 个子频带信号。自适应量化位指定部分与心理听觉权重相对应地量化这 32 个子频带信号。输出量化信号作为位流。为了提高编码质量，可以使用 MPEG/音频层 3 (MPEG/Audio layer 3)。

把视频编码器 11 的输出信号和音频编码器 12 的输出信号供应给文件发生器 15。文件发生器 15 把视频基本流和音频基本流转换成无需使用特殊的

硬件结构，同步再现运动图像、声音、和文本的计算机软件程序就可以管理的文件结构。这样的计算机软件程序是，例如，QuickTime（由苹果电脑公司（美国）提供的交叉平台多媒体格式的典型例子）。下文把 QuickTime 缩写成 QT。下面描述使用 QT 的情况。在利用加密密钥加密编码视频数据和编码音频数据之后，文件发生器 15 在系统控制微型计算机 19 的控制下，多路复用加密视频数据和加密音频数据。

由于加密单元是预定单元长度，因此，根据本发明的实施例，最好把块加密系统用作加密算法。例如，如下所述，使用 DES、FEAL、MISTY、MULTI、IDEA、RC5 等。

10 从文件发生器 15 输出的 QuickTime 电影文件通过存储器控制器 18 被连续写入存储器 17 中。当系统控制微型计算机 19 请求存储器控制器 18 把数据写入记录媒体 40 中时，存储器控制器 18 从存储器 17 中读出 QuickTime 电影文件。另外，系统控制微型计算机 19 通过存储器控制器 18 把在执行程序期间出现的各种数据存储存在存储器 17 中。

15 在这种情况下，指定编码 QuickTime 电影文件的传输速率，以便使它低于把数据写入记录媒体 40 中的传输速率（例如，是后者的 1/2）。因此，尽管 QuickTime 电影文件被连续写入存储器 17 中，但是，在系统控制微型计算机的控制下，从存储器 17 中断断续续地读取 QuickTime 电影文件，使得存储器 17 既不会溢出，也不会下溢。

20 从存储器 17 中读出的 QuickTime 电影文件从存储器控制器 18 供应给纠错码编码器/解码器 21。纠错码编码器/解码器 21 把 QuickTime 电影文件临时写入存储器 20 中，以便生成交织数据和纠错码的冗余数据。纠错码编码器/解码器 21 从存储器 20 中读取冗余数据，把冗余数据供应给数据调制器/解调器 23。

25 当把数字数据记录到记录媒体 40 上时，数据调制器/解调器 23 调制数据，以便可以从再现信号中容易地提取时钟脉冲信号，和不会出现码间干扰。例如，可以使用 (1, 7) RLL（游程长度受限）码、Trellis（格子）码等。

30 把数据调制器/解调器 23 的输出信号供应给磁场调制驱动器 24 和光学拾取器 33。磁场调制驱动器 24 与输入信号相对应地驱动磁头 32，以便把磁场施加到记录媒体 40 上。光学拾取器 33 把与输入信号相对应的记录激光束照射在记录媒体 40 上。这样，就可以把数据记录到记录媒体 40 上。记录媒体



40 是可重写光盘（例如，MO：磁光盘）、或相变型盘。

根据该实施例，使用 MO，例如，其直径大约是 4 cm、5 cm、6.5 cm、或 8 cm 的相对小盘。记录媒体 40 以恒定线速率（CLV）、恒定角速度（CAV）、或分区 CLV（ZCLV）随电机 30 而转动。

5 驱动控制微型计算机 22 与来自系统控制微型计算机 19 的请求相对地应地  
把信号输出到伺服电路 30。伺服电路 30 与驱动控制微型计算机 22 的输出信号  
相对地控制电机 31 和光学拾取器 33。结果是，驱动控制微型计算机 22  
控制整个驱动。例如，伺服电路 30 对记录媒体 40 进行径向移动伺服操作、  
跟踪伺服操作、和聚焦伺服操作，并且控制电机 31 的转动。

10 操作部分 26 与系统控制微型计算机 19 相连接。用户可以把预定命令输入  
操作部分 26 中。

在再现模式下，光学拾取器 33 把具有再现输出电平的激光束照射到记录  
媒体 40 上。光学拾取器 33 的光学检测器接收反射光作为再现信号。在这种  
情况下，驱动控制微型计算机 22 从光学拾取器 33 的光学检测器的输出信号  
15 中检测跟踪误差和聚集误差。伺服电路 30 控制光学拾取器 33，以便把读激  
光束聚焦在预定轨道上。另外，驱动控制微型计算机 22 控制光学拾取器沿着  
径向移动，以便再现在记录媒体 40 上的所需位置的信号。与记录模式一样，  
所需位置由系统控制微型计算机 19 按照把预定信号供应给驱动控制微型计  
算机 22 的方式确定。

20 把光学拾取器 33 再现的信号供应给数据调制器/解调器 23。数据调制器/  
解调器 23 解调再现信号。把解调数据供应给纠错码编码器/解码器 21。把再  
现数据临时存储在存储器 20 中。纠错码编码器/解码器 21 对解调数据进行解  
交织处理和纠错处理。通过存储器控制器 18 把已经经过纠错的 QuickTime 电  
影文件存储到存储器 17 中。

25 与来自系统控制微型计算机 19 的请求相对应，把存储在存储器 17 中的  
QuickTime 电影文件输出到文件解码器 16。系统控制微型计算机 19 监视从记  
录媒体 40 再现的和存储在存储器 17 中的再现信号的数据量、和从存储器 17  
中读取的和供应给文件解码器 116 的数据量，并且，控制存储器控制器 18 和  
驱动控制微型计算机 22，以便存储器 17 不会溢出或下溢。这样，系统控制  
30 微型计算机 19 就可以断断续续地从记录媒体 40 中读取数据。

在系统控制微型计算机 19 的控制下，文件解码器 16 把 QuickTime 电影

文件分离成视频基本流和音频基本流。文件解码器 16 在系统控制微型计算机 19 的控制下，与保护信息和加密密钥（如后所述）相对应地解码数据。当保护信息禁止使用数据时，或者，当加密密钥不合适时，不解码数据。把解码视频基本流供应给视频解码器 13。视频解码器 13 解码已经经过压缩和编码的视频基本流。从视频输出端输出解码视频数据。把音频基本流供应给音频解码器 14。音频解码器 14 解码已经经过压缩和编码的音频基本流。从音频输出端输出解码音频数据。文件解码器 16 同步地输出视频基本流和音频基本流。

当视频解码器 13 对应于 MPEG 系统时，视频解码器 13 包括缓冲存储器、可变长度代码解码部分、逆量化部分、逆 DCT 部分、相加部分、帧存储器、运动补偿和预测部分、屏幕重排部分、和数字/模拟转换器（下文缩写为“D/A”），作为电路线路。把视频基本流临时存储在缓冲存储器中。此后，把视频基本流输入可变长度代码编码部分中。可变长度代码编码部分解码宏块编码信息，并且将其分离成预测模式、运动向量、量化信息、和量化 DCT 系数。逆量化部分 73 把量化 DCT 系数去量化成 DCT 系数。逆 DCT 部分把 DCT 系数转换成像素空间数据。相加部分相加逆 DCT 部分的输出信号和运动补偿和预测部分的输出信号。但是，当解码 I 画面时，相加部分不相加这些输出信号。解码屏幕的所有宏块。屏幕重排部分按原来的输入顺序重排解码的宏块。D/A 把重排数据转换成模拟信号。由于在接下来的解码过程中，I 画面和 P 画面用作参考屏幕，因此，把它们存储在存储器中。把 I 画面和 P 画面输出到运动补偿和预测部分。

当使用 MPEG/音频层 1/层 2 时，音频解码器 14 包括位流拆散部分、逆量化部分、和子频带组合滤波器阵列部分，作为电子线路。把输入的音频基本流供应给位流拆散部分。位流拆散部分把输入的音频基本流分离成首标、辅助信息、和量化子频带信号。逆量化部分利用已经指定的预定位数逆量化量化的子频带信号。子频带组合频带滤波器组合逆量化的数据，并且输出组合数据。

当数字记录和再现设备把诸如视频数据、音频数据、文本数据、和计算机程序之类受无形财产权（譬如，版权和专利权）保护的数据记录到记录媒体 40 上时，该设备也把保护无形财产权的数据（下文称这个数据为“保护数据”）记录到记录媒体 40 上。另外，以与视频数据之类要受保护的数据相同

的文件格式生成保护数据，使得数字记录和再现设备可以以相同的方式管理它们。根据本发明的实施例，以，例如，QuickTime 电影文件的格式生成要受保护的数据和保护数据。因此，记录和再现设备可以按照 QT 再现它们。

5 QT 是与时间基(base)一起管理各种类型的数据和具有无需利用特殊的硬件设施就可以同步再现运动图像、声音、文本等的 OS (操作系统) 扩充功能的软件程序。QT 已经公开在，例如，Addison Wesley 著的“Macintosh 内部: QuickTime (日本版)”中 (“Inside Macintosh: QuickTime(Japanese Edition)”, Addison Wesley)。下面与文档相对应地描述 QT。

10 QT 电影资源的基本数据单元被称为原子 (atom)。每个原子除了包含数据之外，还包含信息的长度和类型。在 QT 中，把数据的最小单元当作一个样本来对待。把一个块 (chunk) 定义为一组样本。

图 2 是显示 QuickTime 电影文件的结构例子的示意图。

图 3 是显示视频媒体信息原子的结构例子的示意图。图 3 是显示在轨道是视频信息的情况下，图 2 所示的视频媒体信息原子的详细示意图。

15 在图 2 和 3 中，QuickTime 电影文件主要由两部分组成，它们是电影原子 101 和电影数据原子 102。电影原子 101 是包含再现文件所需的信息和再现实体数据所需的信息的部分。电影数据原子 102 是包含诸如视频数据、音频数据、计算机程序、和文本数据之类的实体数据的部分。

20 电影原子 101 包含电影首标原子 111、电影剪辑原子 112、用户定义数据原子 113、和至少一个轨道原子 114 等。电影首标原子 111 包含与整个电影有关的信息。电影剪辑原子 112 指定剪辑区。

25 轨道原子 114 是为电影的每个轨道定义的。轨道原子 114 包含轨道首标原子 131、轨道剪辑原子 132、轨道遮蔽原子 133、编辑原子 134、和媒体原子 135。轨道原子 114 在原子 131 到 135 中描述与电影数据原子 102 的各段数据有关的信息。图 2 只显示了视频电影的轨道原子 114-1 (省略了其它轨道原子)。

30 媒体原子 135 包含媒体首标原子 144、媒体信息原子 (图 2 和 3 中的视频媒体信息原子 145)、和媒体管理者(handler)参考原子 146。媒体原子 135 在媒体首标原子 144、媒体信息原子、和媒体管理者参考原子 146 中描述用于定义解释电影轨道的数据和媒体数据的部分(component)的信息。

媒体管理者利用媒体信息原子的信息把媒体时间映射成媒体数据。

媒体信息原子 145 包含数据管理者参考原子 161、媒体信息首标原子 162、数据信息原子 163、和样本表原子 164。

5 媒体信息首标原子（图 3 中的视频媒体信息首标原子 162）描述与媒体有关的信息。数据管理者参考原子 161 描述与管理媒体数据有关的信息。数据管理者参考原子 161 包含指定为媒体数据提供存取手段的数据管理者部分的信息。数据信息原子 163 包含数据参考原子。数据参考原子描述与数据有关的信息。

10 样本表原子 164 包含把媒体时间转换成代表样本位置的样本序号所需的信息。样本表原子 164 包括样本长度原子 172、时间-样本原子 173、同步样本原子 174、样本描述原子 175、样本-块原子 176、块偏移原子 177、和阴影同步原子 178。

15 样本长度原子 172 描述样本的长度。时间-样本原子 173 描述样本和时间基之间的关系（已经记录了多少分钟和多少秒钟数据？）。同步样本原子 174 描述与同步有关的信息和指定媒体的关键帧。关键帧是不依赖于前一帧的自包容帧。样本描述原子 175 包含解码媒体的样本所需的信息。媒体可以含有至少一个与用在媒体中的压缩类型相对应的样本描述原子。样本-块原子 176 20 引用包含在样本描述原子 175 中的表格，识别与媒体的每个样本相对应的样本描述。样本-块原子 176 描述样本与块之间的关系。样本-块原子 176 识别与第一块的信息相对应的媒体的样本的位置、每个块的样本数、和样本描述 ID。块偏移原子 177 描述电影数据的块的开始位位置，和定义数据流的每个块的位置。

25 在图 2 中，电影数据原子 102 以由预定个样本组成的块为单元、包含与预定压缩和编码系统相对应地编码的音频数据和与预定压缩和编码系统相对应地编码的视频数据。压缩和编码数据并非总是必要的。取而代之，可以包含线性数据。例如，当管理文本、MIDI（乐器数字接口）等时，电影数据原子 102 包含文本、MIDI 等的实体数据。相应地，电影原子 101 包含文本轨道、MIDI 轨道等。

30 电影原子 101 的每个轨道原子 114 与包含在电影数据原子 102 中的数据（数据流）相关。借助于具有如此特征的结构，无需改变数据实体，就可以安排同步再现操作和可以进行编辑（非破坏性编辑）操作。另外，可以容易地加入和删除轨道。

借助于这样的分层结构，当再现包含在电影数据原子 102 中的数据时，QT 从电影原子 101 开始依次跟踪分层结构，把样本表映射到与包含在样本表原子 164 中的原子 172 到 178 相对应的存储器，和识别每个数据段的解释方法和属性等、以及各个数据段（数据段的位置和长度）之间的关系。QT 再现与数据段之间的关系相对应的数据。

根据本发明的实施例，在使用 QT 的优良特征的同时，扩展了管理要保护的数据所需的功能和格式。结果是，保护了给与数据的无形财产权。下面只描述包含在无形财产权中的版权。但是，应该注意到，本发明可应用于其它无形财产权。通过将作为 QT 的最小存取单元的样本与加密实体数据的最小解密单元（数据块）相关，可以根据 QT 的时间基，利用管理能力进行同步再现操作和编辑操作。与密钥管理相结合，通过更确切地给予权利和指定权利的使用条件，可以以新的方式使用同一内容。

事实上，根据本发明，每个轨道原子的样本描述表具有包含保护数据的扩展格式，以便把解密加密数据的密钥信息和诸如内容的使用条件之类的保护信息保护成独立数据流。结果是，QT 可以管理已经给与无形财产权的多媒体内容。

图 4 是显示根据本发明的一个实施例的 QuickTime 电影文件的结构的示意图。

图 5 是显示根据本发明实施例的样本描述表的结构示意图。

如图 4 所示，保护信息块 191 是接在标准 QT 字段之后的扩展字段。保护信息块 191 位于每个轨道的样本描述表中。如图 5 所示，保护信息块 191 只由权利管理数据（下文缩写为“RMD”）单元组成。可选地，保护信息块 191 由它们是 RMD 单元和其它单元的数个单元组成。这些单元可以以任何次序放置。

单元长度字段包含在每个单元中。单元长度字段代表单元的字节数。单元类型字段是指定单元的类型标记。当当前单元是 RMD 单元时，单元类型字段是 ‘right’。

版本字段代表单元的版本号。标志字段是为单元的标记保留的。

标志字段的后面接着单元的数据实体（单元数据）。当单元是 RMD 单元时，数据实体是一批与保护有关的信息和加密密钥。

当保护系统需要时，重新使用文件格式等，与扩展字段相对应，可以定

义指定标准 QT 字段中的数据类型的数据格式字段的标记。

标准 QT 是根据本发明,其样本描述表不包含保护权利的扩展字段的 QT。

图 6 是显示权利管理数据的结构的示意图。

在图 6 中, RMD 单元包含一批与作为使用条件的版权保护有关的信息,  
5 譬如, 内容加密密钥(下文缩写为“CK”)、C\_MAC、RMF、PPN、回放计数器、开始时间/日期、结束时间/日期、CCF、PCN、复制计数器、和保留区。

CK 字段包含已经用于加密轨道(事实上, 每个轨道分为若干个数据块)的数据流的内容加密密钥。

C\_MAC 字段包含 RMD 篡改防止码。篡改防止码是与, 例如, ISO/IEC  
10 (国际标准化组织/国际电子技术委员会) 9797 MAC (消息认证码) 计算方法相对应, 从 RMD 的所有字段值中唯一地和不可逆地得出的计算值。

RMF (权利管理标志) 字段是代表限制存在与否和它的类型的标志。

PPN (允许回放数) 字段是代表可以进行回放操作的最大次数。

回放计数器字段代表已经进行过回放操作的次数的计数器值。每当进行  
15 回放操作时, 计数器值就减 1。回放计数器字段的初始值与 PPN 字段的初始值相同。

开始时间/日期字段代表当 RMF 字段代表限制存在时的开始时间/日期。

结束时间/日期字段代表当 RMF 字段代表限制存在时的结束时间/日期。

CCF (复制控制标志) 字段是复制控制标志。CCF 字段指定允许/禁止复  
20 制、复制允许生成、和原始数据/复制数据的属性。

PCN 字段代表可以把内容传送/复制到诸如 LCM (Licensed Compliant Module (许可顺应性模块)) 之类的媒体上的次数的最大值。

复制计数器字段代表每当传送/复制内容时其值就减 1 的计数器值。复制计数器的初始值与 PCN 字段的初始值相同。

25 RMF、PPN、回放计数器、开始时间/日期、结束时间/日期、CCF、PCN、和复制计数器指定内容的使用条件。

下面参照图 7 和 8, 描述电影数据原子的结构和实体数据和媒体原子的相关。

图 7 是显示电影数据原子的结构的示意图。

30 图 8 是显示实体数据与媒体原子之间相关的示意图。

在图 7 中, 电影数据是由原子长度、类型和数据组成的原子。在图 7 中,

在长度和类型后面的数据部分是内容的实体数据（数据流）。

与作为美国标准加密系统的 DES（数据加密标准）块加密算法相对应，加密图 7 所示的受保护内容数据。与块加密算法相对应，以块为单位加密数据，和以预定时间段为间隔改变加密密钥。作为首标信息已经用相同密钥加密的和已经把解密加密数据所需的信息加入其中的一块加密数据被称为加密数据块。换句话说，加密数据块是可以利用密钥解密的最小解密单元。加密数据流（由加密数据块 # 1 到加密数据块 # n 组成）是加密数据块序列。

从现在开始，除非另有说明，一个块代表一个加密数据块。加密数据块由 BLK ID、CONNUM、BLK 序号、块种子、和加密数据组成。

10 BLK ID 字段代表标识块开头的代码。

CONNUM 字段是唯一标识内容的标识符 ID。内容的每个块的 CONNUM 字段的值不发生改变。即使内容被编辑，CONNUM 字段的值也不发生改变。每个块的 CONNUM 字段的值是代表每个块构成的内容的信息。

15 BLK 序号字段代表块的块号。内容的第 1 块的 BLK 序号是 0。下一个块的 BLK 序号是 1。以此类推，指定 BLK 序号。

20 块种子字段是用来加密块的密钥的类型。块种子字段的值随每个块而改变。一般说来，由于一个内容只有一个加密解密，用来加密数据的密钥是内容加密密钥和块种子的组合。因此，尽管一个内容只有一个加密密钥，但是一个内容的加密密钥以预定时间段为间隔发生改变。内容加密密钥和块种子的组合和加密密钥发生改变的间隔取决于加密算法和系统。

加密数据字段包含加密数据的实体。一个块等效于诸如运动图像的一个帧或音频数据的一个到几个声音帧之类的一个数据流单元。

25 在图 8 中，作为 QT 上最小存取单元的样本与一个加密数据块相关。因此，当加密数据块对应于运动图像的一个帧时，QT 可以以一个帧为单元存取和再现数据，和与另一个轨道同步可以精确到一个帧。于是，可以保证诸如分割操作、合并操作、和替代操作之类的编辑操作精确到一个帧。在前述样本描述表的结构中，可以为每个样本或每两个或更多个样本指定诸如内容加密密钥之类的使用条件和版权信息。

30 数据可以分数据加密、数据篡改防止、和加密密钥管理三个阶段来保护。通过更多的阶段，可以更安全地保护数据。根据前述实施例，数据加密是利用 DES 完成的，数据篡改防止是利用 C\_MAC 完成的。因此，为了安全地保

护数据，最好，在前述实施例中使用加密密钥管理。下面描述利用管理加密密钥的方法的实施例。

图 9 是显示在管理加密密钥的情况下样本描述表的结构示意图。

在图 9 中，样本描述表包含标准 QT 字段和在它后面的扩展保护信息块。扩展保护信息块包含允许密钥块（下文缩写为“EKB”）单元和 RMD 单元。EKB 单元包含至少一个名为 EKB 的为获取内容的加密密钥所需的密钥、相关属性信息等。

在 EKB 单元中，单元长度字段代表 EKB 单元的总字节数。在 EKB 单元中，单元类型字段是指定单元的类型标记。在本例中，单元类型是“ekbl”。在 EKB 单元中，版本字段代表单元的版本。在 EKB 单元中，标志字段指定单元的数据实体（EKB）的存在与否和对它的参照方法。

在 EKB 字段中，EKB 字段代表 EKB 数据的实体、文件 ID、文件名、诸如 URL（统一资源定位地址）之类的链接信息、或不存在含有标志的状态值的数据（不存在 EKB 字段）。EKB 基本上与数据流成对出现。在这种情况下，在电影原子（资源）中未必包含 EKB 的实体。例如，可以把 EKB 的实体作为独立文件存储在同一记录媒体上。在必要时，可以利用链接信息引用 EKB 的实体。当在数个内容使用同一个 EKB 的情况下，EKB 是冗余的时，借助于作为独立文件的 EKB 的实体，可以提高记录媒体容量的使用率。另外，如果内容提供者愿意，可以只分配不与 EKB 配对的数据流作为内容。其结果是，可以完成只分配数据流和通过利用因特网的 URL 指定 EKB 提供站获取 EKB 的业务。

图 10 是显示 EKB 单元的标志的定义的示意图。

在图 10 中，标志值 0X00 代表 EKB 数据不存在和无效。标志值 0X01 代表 EKB 数据存在和存储在 EKB 单元中。标志值 0X02 代表尽管 EKB 数据不存在于 EKB 单元中，但是，EKB 数据作为独立文件存在于同一记录媒体上和可以利用诸如文件 ID 或文件名之类的参考信息引用。标志值 0X03 代表尽管 EKB 数据不存在于 EKB 单元中，但是，可以利用指定因特网上的适当站点的 URL 信息获取 EKB 数据。其它标志值保留着。

当从外部引用 EKB 时，如图 11 所示，EKB 被构造成独立文件。与 EKB 的实体一起加入诸如代表链接的电影的链接计数器、版本、和类型之类的数据。这样，就可以管理每个内容（轨道）和 EKB 的相关。



除了这样的扩展之外，在必要时，在图 9 所示的标准 QT 字段中重新扩展地定义作为指定表的数据类型的数据格式字段的值的标记。

图 12 是显示 EKB 的数据结构的示意图。

图 12 显示了在前述标志字段指定 EKB 存在和实体包含在单元中的情况下，存储的 EKB 的实体的例子。

在图 12 中，版本字段代表 EKB 的版本值。加密算法字段指定用来加密构成 EKB 的各种类型加密密钥信息的加密算法。当利用密钥  $n$  加密  $A$  时，如果结果用  $E_n(A)$  表示，那么， $E_{\text{root}}(\text{KEK})$  是已经用密钥  $K_{\text{root}}$  加密的密钥加密密钥。KEK 是获取解密数据流所需的加密密钥 (KC) 所需的密钥。换句话说，通常满足关系  $CK = E_{\text{KEK}}(\text{内容 (KC) 的加密密钥})$ 。

签字部分是 EKB 的电子签字。签字部分后面接着用最低分层密钥加密倒数第二低分层密钥，用倒数第二低分层密钥加密倒数第三低分层密钥，以此类推获得的密钥信息序列。最低分层密钥被称为媒体或设备唯一拥有的叶密钥 (用，例如， $K_{\text{leaf}}$  表示)。因此，有效媒体或有效设备可以利用 EKB 检索 KEK。

下面描述通过相应应用程序 QT 再现这样的文件的情况。

当显示电影时，系统控制微型计算机 19 通过文件解码器 16 存取与指定时间相对应的媒体数据。系统控制微型计算机 19 利用样本表原子的信息指定与所请求样本相对应的数据流的位置。类似地，系统控制微型计算机 19 引用解释样本的样本描述表，和利用扩展 EKB 单元的标志字段确定 EKB 数据的属性。当存在 EKB 数据和存储实体时，系统控制微型计算机 19 引用下一个 EKB 字段作为 EKB 数据。当 EKB 数据被表示成独立文件时，系统控制微型计算机 19 利用包含在 EKB 字段中的链接信息指定相关 EKB 文件。当 EKB 字段代表 URL 时，系统控制微型计算机 19 引用通过 URL 指定的 HP (主页) 和从中下载所需 EKB 数据。另一方面，当没有把使用允许赋予内容 (例如，不存在 EKB) 时，系统控制微型计算机 19 进行所需处理 (例如，发出代表不能再现内容的消息或代表应该获取 EKB 的消息)。借助于获取的 EKB 和应用程序唯一拥有的叶密钥，系统控制微型计算机 19 可以为获取内容的加密密钥而获取 KEK。借助于 EKE 和 RMD，系统控制微型计算机 19 获取解密内容的加密密钥。另外，系统控制微型计算机 19 确定各种使用条件的信息。系统控制微型计算机 19 进行与用户条件相对应的处理。借助于获取的内容密钥

和包含在加密数据块中的块种子，系统控制微型计算机 19 让文件解码器 16 解码该块。系统控制微型计算机 19 让相应的编解码器扩充解密的数据流，和让视频解码器显示所得数据。

下面描述权利保护方法和提供的业务之间的关系。

5 图 13 是说明权利保护方法与提供的业务之间的第一种关系的示意图。

在图 13 中，提供了数个轨道。在轨道上记录着质量（分辨率、音质等）不同的同一内容。不同版权信息被加以每个轨道的样本描述表。对各个轨道指定不同费用。把与支付费用相对应的版权保护信息和内容加密密钥提供给用户。其结果是，可以提供具有与支付费用相对应的的质量的内容。

10 例如，轨道 1 包含具有第一分辨率的内容。与具有第一分辨率的内容相对应的版权信息 A 和内容加密密钥 A 包含在样本描述表中。轨道 2 包含具有比第一分辨率高的分辨率的内容。与具有更高分辨率的内容相对应的版权信息 B 和内容加密密钥 B 包含在样本描述表中。在这种情况下，当已经支付了起步费时，把还没有提供给用户的版权信息 A 的 EKB 和内容加密密钥 A 之一或它们二者提供给用户，以便他或她可以再现轨道 1。当用户与起步费一起支付了附加费时，把还没有提供给用户的版权信息 B 的 EKB 和内容加密密钥 B 之一提供给用户或把它们二者提供给用户，以便他或她可以再现轨道 2。

15 或者，指定不同的费用。与支付的费用相对应，把还没有提供给用户的版权信息 A 的 EKB 和内容加密密钥 A 之一提供给用户或把它们二者都提供给用户。或者，与支付的费用相对应，把还没有提供给用户的版权信息 B 的 EKB 和内容加密密钥 B 之一提供给用户或把它们二者都提供给用户。因此，可以提供具有与支付费用相对应的分辨率的内容。这样，就可以提供具有与所付费用相对应的可伸缩性的内容。

20 此外，类似地，当把不同内容，例如，视频内容和音乐内容记录在轨道上时，如果用户为歌曲支付了附加费，或者，他或她通过音乐分配业务购买到，那么，他或她就可以获得各种业务内容，例如，视频内容或卡拉 OK 内容。

图 14 是说明权利保护方法与提供的业务之间的第二种关系的示意图。

25 在图 14 中，一个轨道由加密块和非加密块组成。加密块的样本描述表包含它的版权信息。

其结果是，可以完成如下音乐分配业务。换言之，歌曲由内容提供者指

定的特定部分（例如，特色部分）被构造成非加密部分。因此，用户无需支付费用就可以试听部分歌曲的示范。当用户想要购买歌曲时，他或她就要购买内容密钥（即，获取内容密钥所需的 KEB 数据）。当用户购买了内容密钥时，他或她才可以完全欣赏到整首歌曲。

5 图 15 是说明权利保护方法与提供的业务之间的第三种关系的示意图。

在图 15 中，一个轨道被划分成用不同内容密钥加密的几个块。各个块的样本描述表包含各自的版权信息。

其结果是，可以完成如下的运动图像分配业务。一个内容片断通过按照版权所有者所希望的方式划分的若干段销售。当诸如回放有效期之类的使用条件随同一密钥而改变时，可以在版权所有者所愿望的时间公布诸如一出戏剧之类的内容（可以允许再现内容）。

10 当把前述条件组合在一起时，由于可以把复杂的使用条件指定给一个内容，可以比前面提供更特殊和新颖的内容业务。

传统上，共同管理内容和它的密钥。因此，只把用户想要的内容提供给用户。

15 但是，根据本发明，分开管理内容、与使用内容所需的版权信息有关的 EKB、和内容加密密钥。因此，当把内容分配给用户时，可以事先把数个内容已经记录在上面的记录媒体传送给用户。可选地，可以事先把数个内容分发给用户。换句话说，可以把用户不想要的内容提供给他或她。

20 因此，当提供者只把用户想要的内容的版权信息的 EKB 和加密密钥之一或它们二者提供给用户时，他或她可以使用所需内容。

因此，可以只把诸如版权信息的 EKB 和内容加密密钥之类的最小数据提供给用户。当通过通信线提供最小数据时，通信时间可以变得比把内容和加密密钥二者提供给用户的传统方法短得多。结果是，用户可以低成本地顺利

25 下载内容，不会感到什么压力。  
根据本发明的文件已经记录在上面的记录媒体可以由已经安装了 QT 的计算机读取。如果解密内容所需的加密密钥还没有被记录到记录媒体上，那么，当计算机拥有诸如调制解调器之类可以与通信线连接的通信接口时，可以通过通信线获取加密密钥。因此，可以分开销售实体数据和使用内容数据

30 所需的权利。  
根据本发明，可以安全地保护给与其数据结构已经被转换成可以通过软件来管理的文件结构的实体数据的无形财产权。

---

另外，根据本发明，权利保护单元与构成内容的第一数据单元相匹配。因此，用户可以以数据提供者希望的单元存取数据、再现数据、使数据同步、和编辑数据。

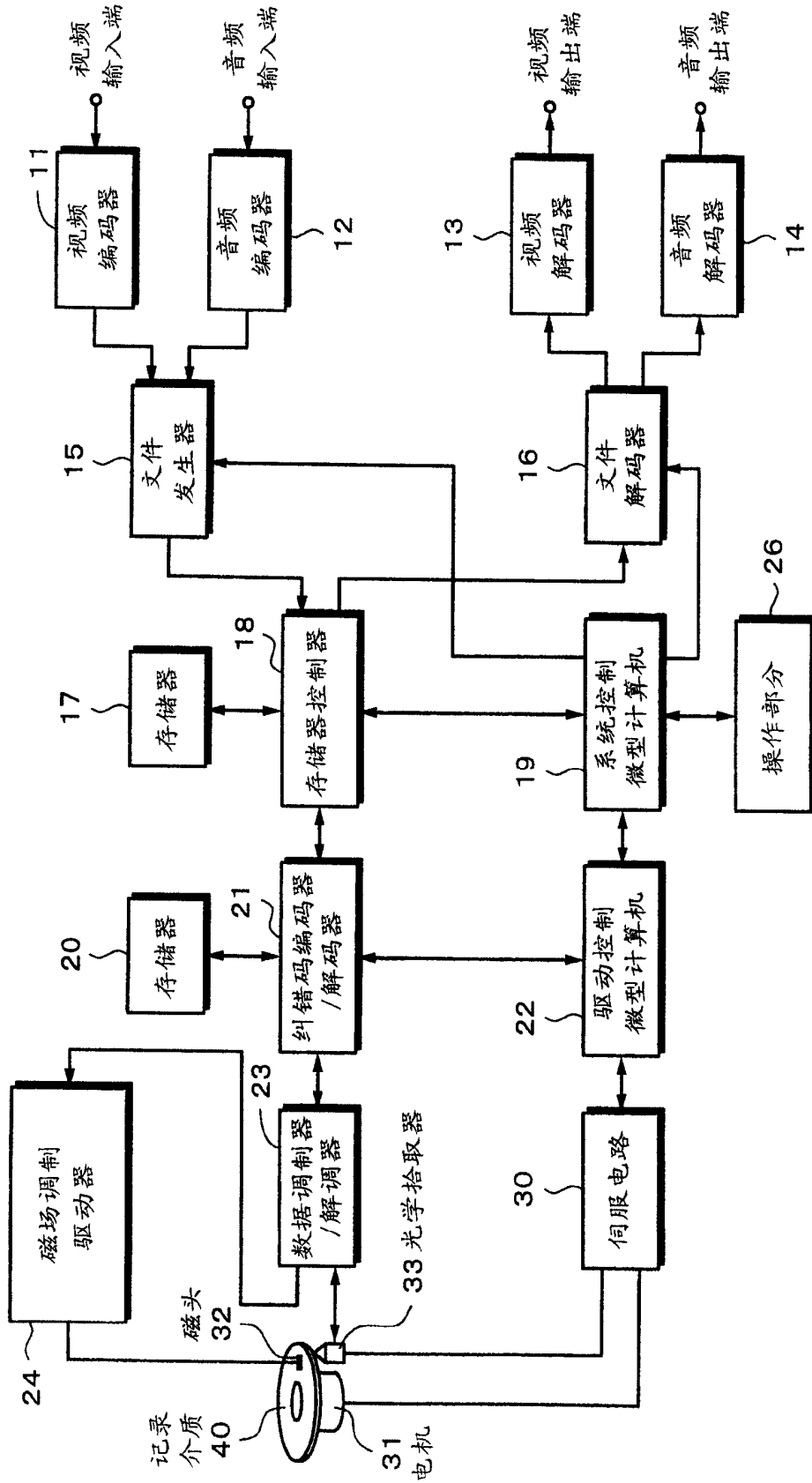


图 1

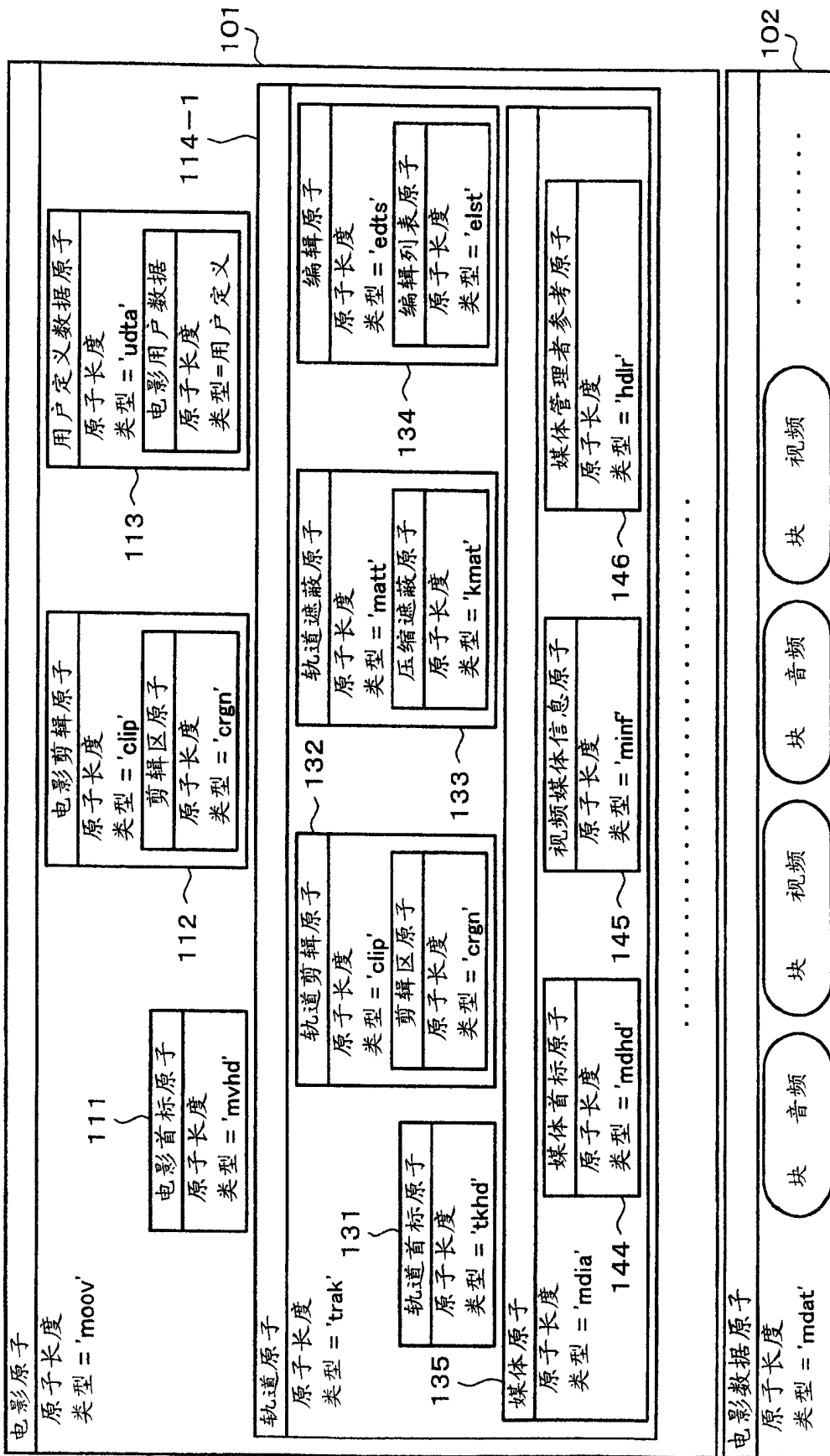


图 2

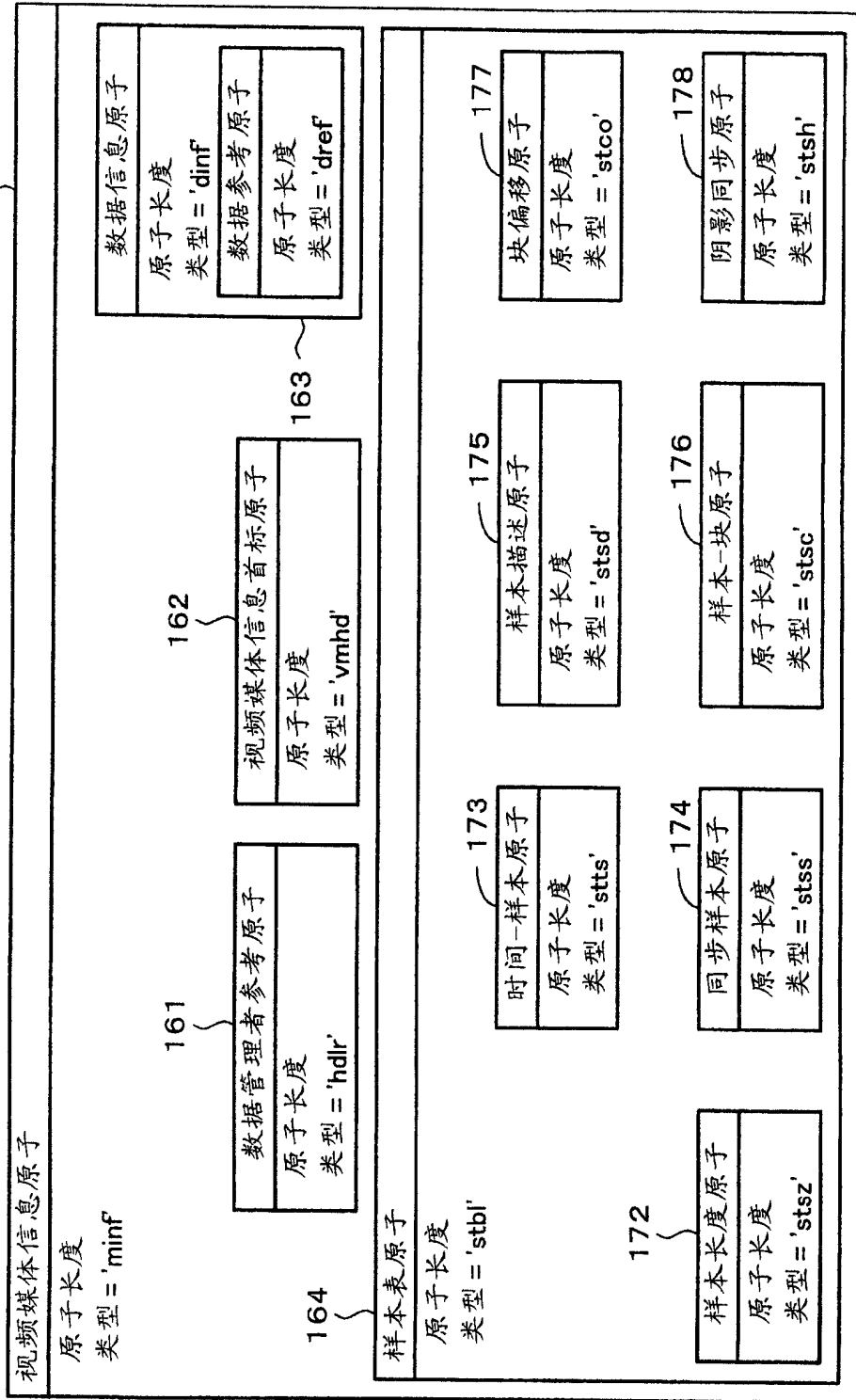


图 3

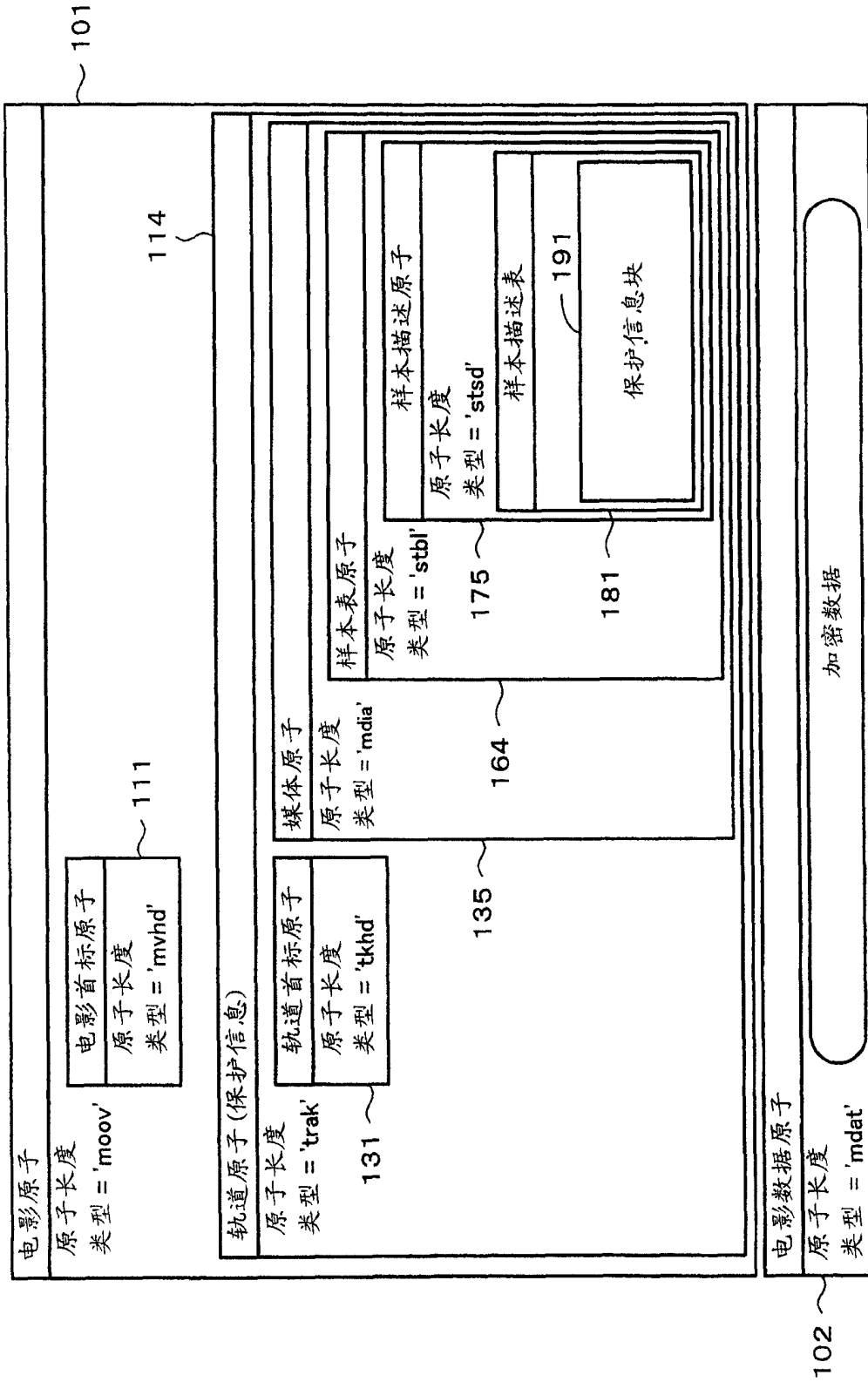


图 4



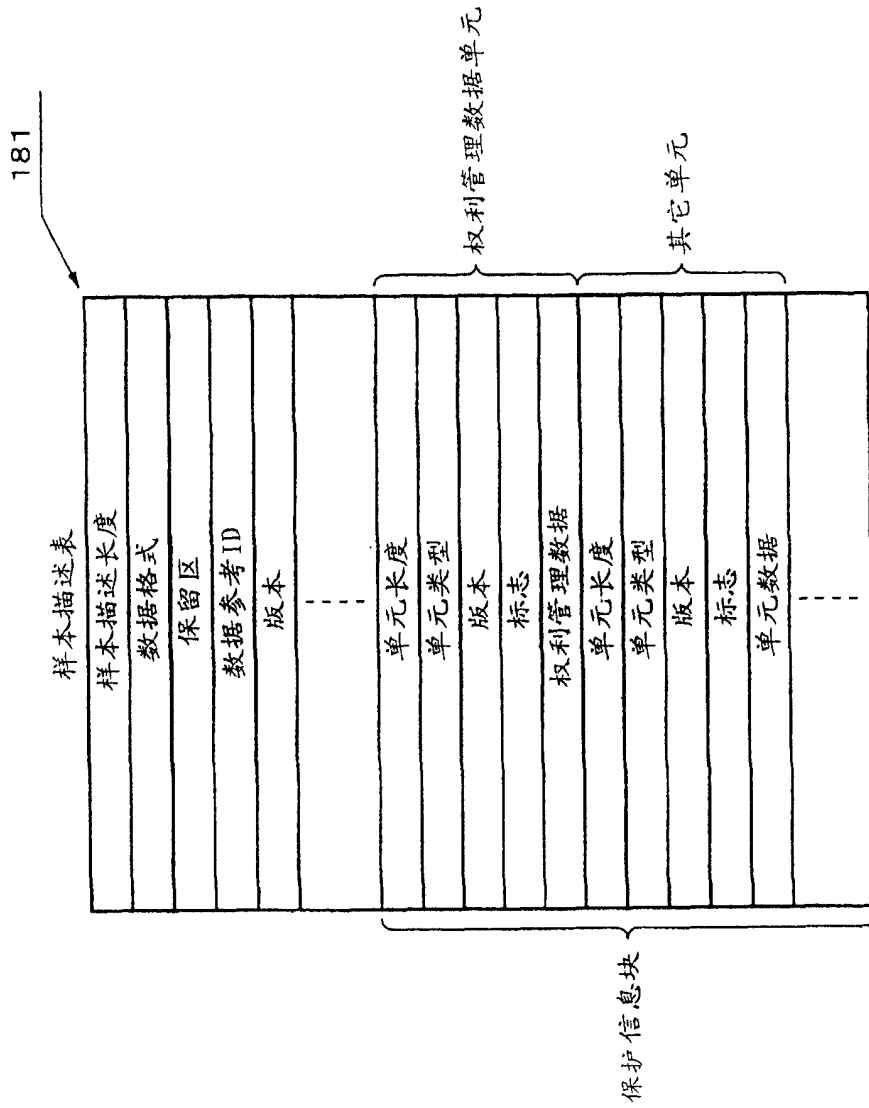


图 5

权利管理数据

加密密钥 (CK)
<b>C_MAC</b>
<b>RMF</b>
<b>PPN</b>
回放计数器
开始时间/日期
结束时间/日期
<b>CCF</b>
<b>PCN</b>
复制计数器
保留区

图 6

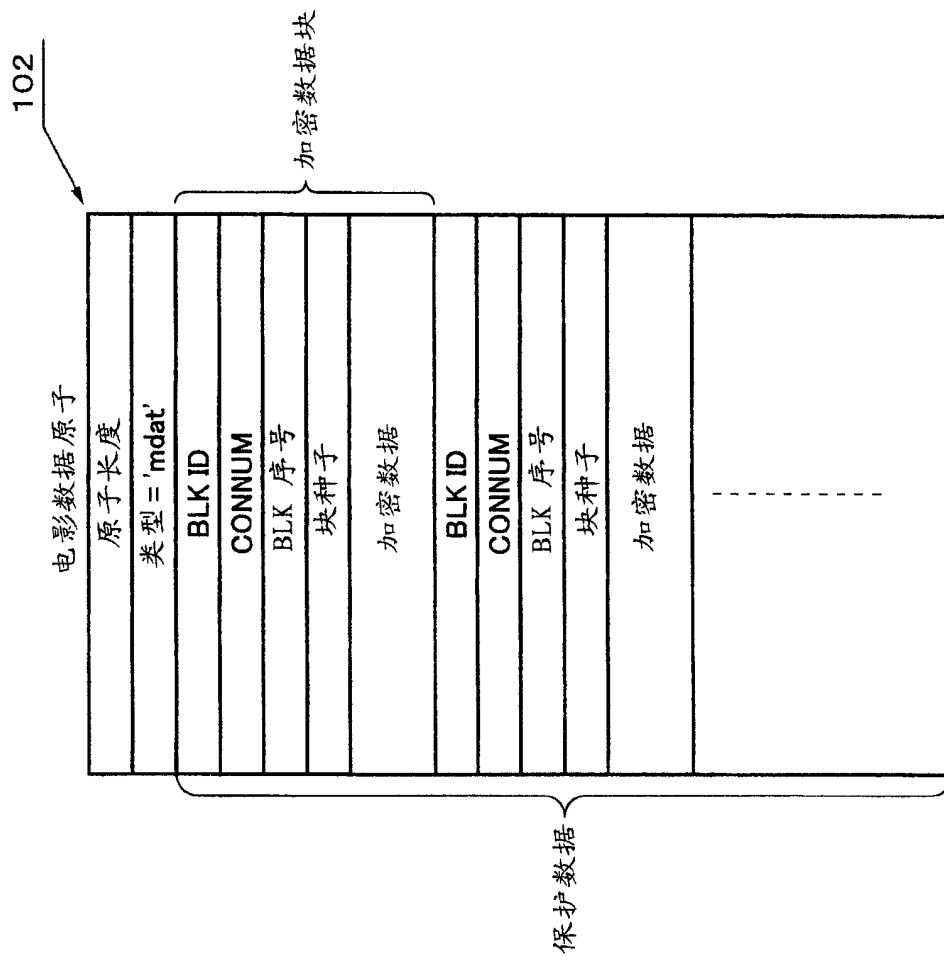


图 7

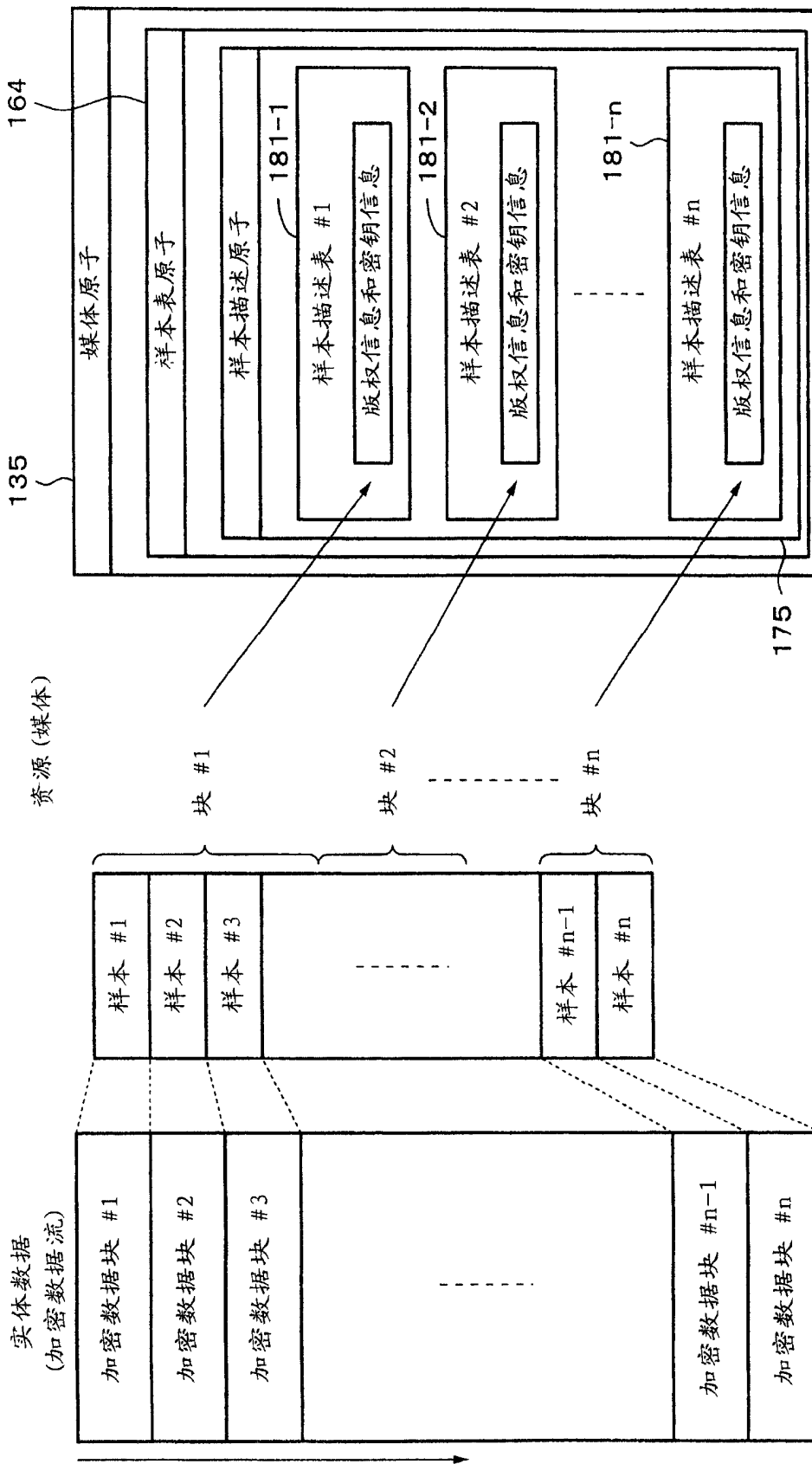


图 8

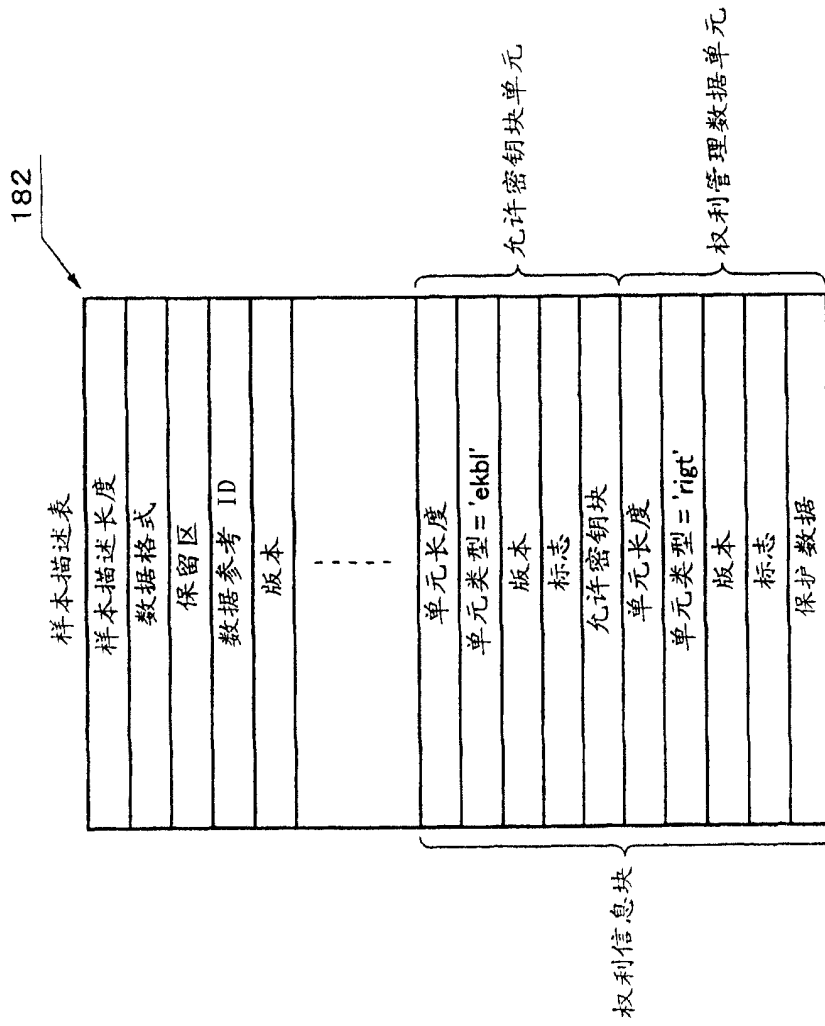


图 9

标志	属性		EKB 字段
	不存在	无效	
0x00	不存在	无效	没有数据
0x01	存在	有效	EKB 数据
0x02	不存在	作为独立文件有效	链接信息(文件ID、文件名等)
0x03	不存在	在因特网上有效	链接信息(URL等)
其它	保留区		

图 10

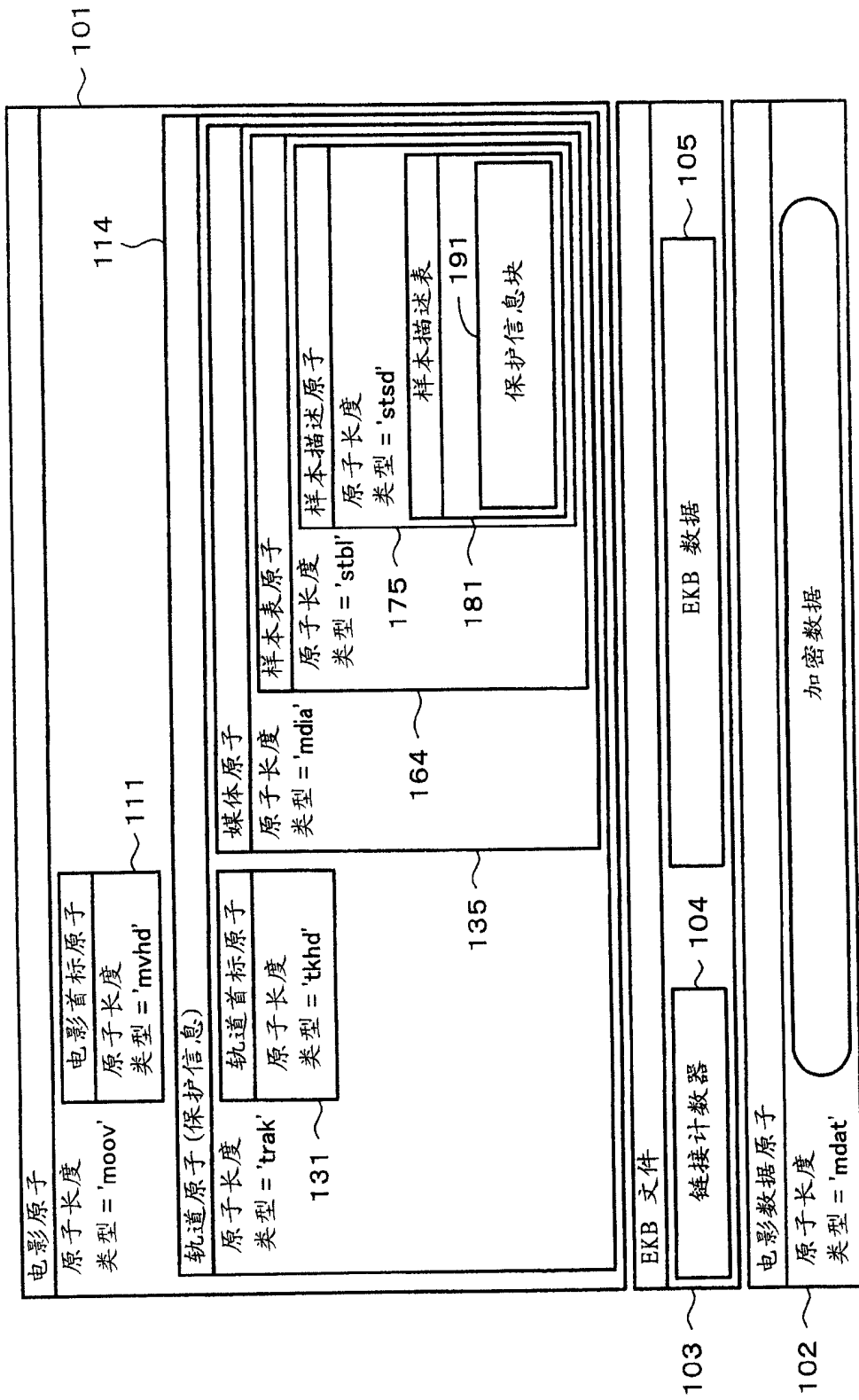


图 11

允许密钥块

版本
加密算法
$E_{kroot}(KEK)$
签字部分
$E_{k0}(Kroot)$
$E_{k1}(K0)$
$E_{k2}(K1)$
⋮
$E_{kn}(Kn-1)$
$E_{kleaf}(Kn)$

图 12



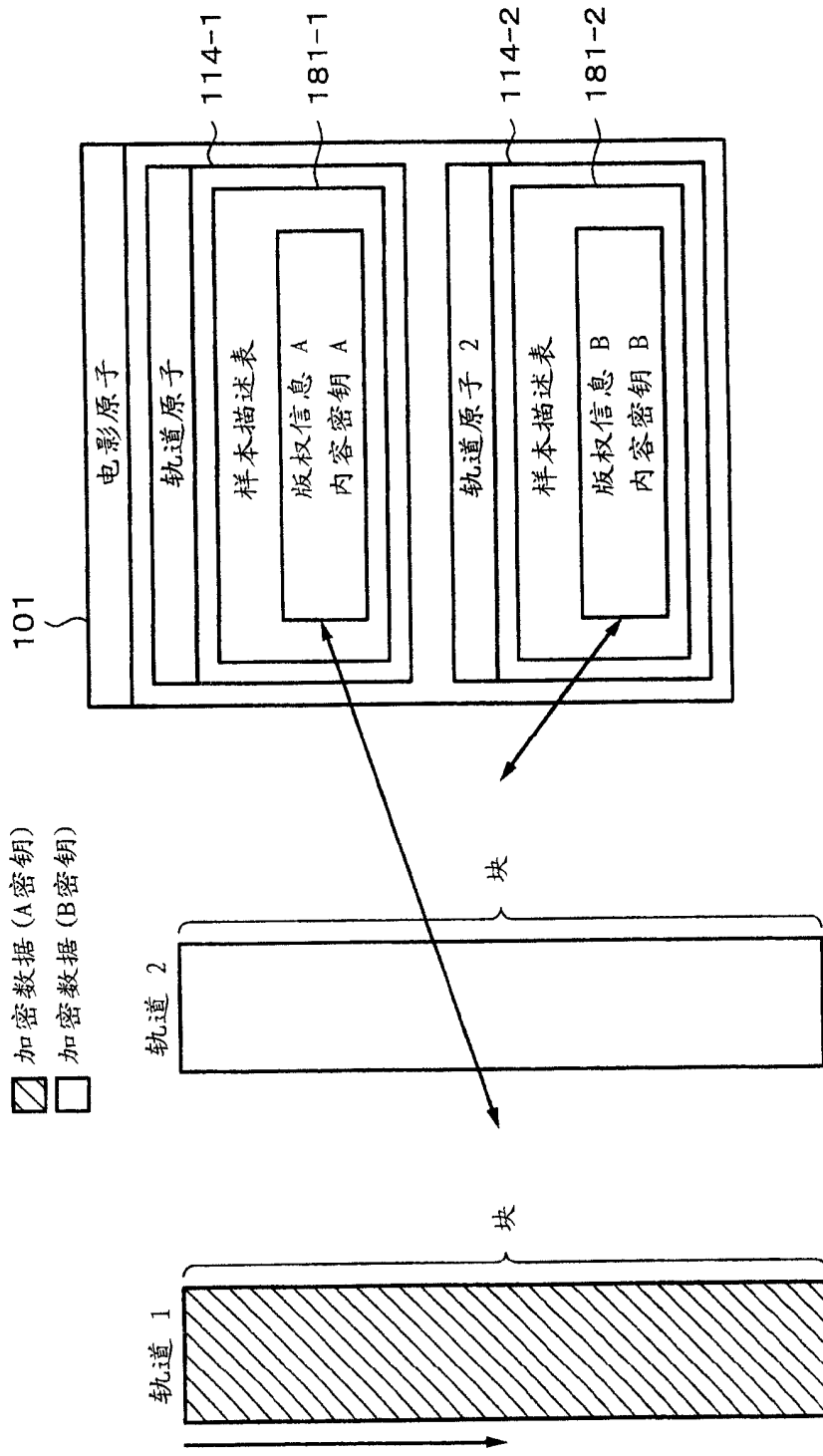


图 13

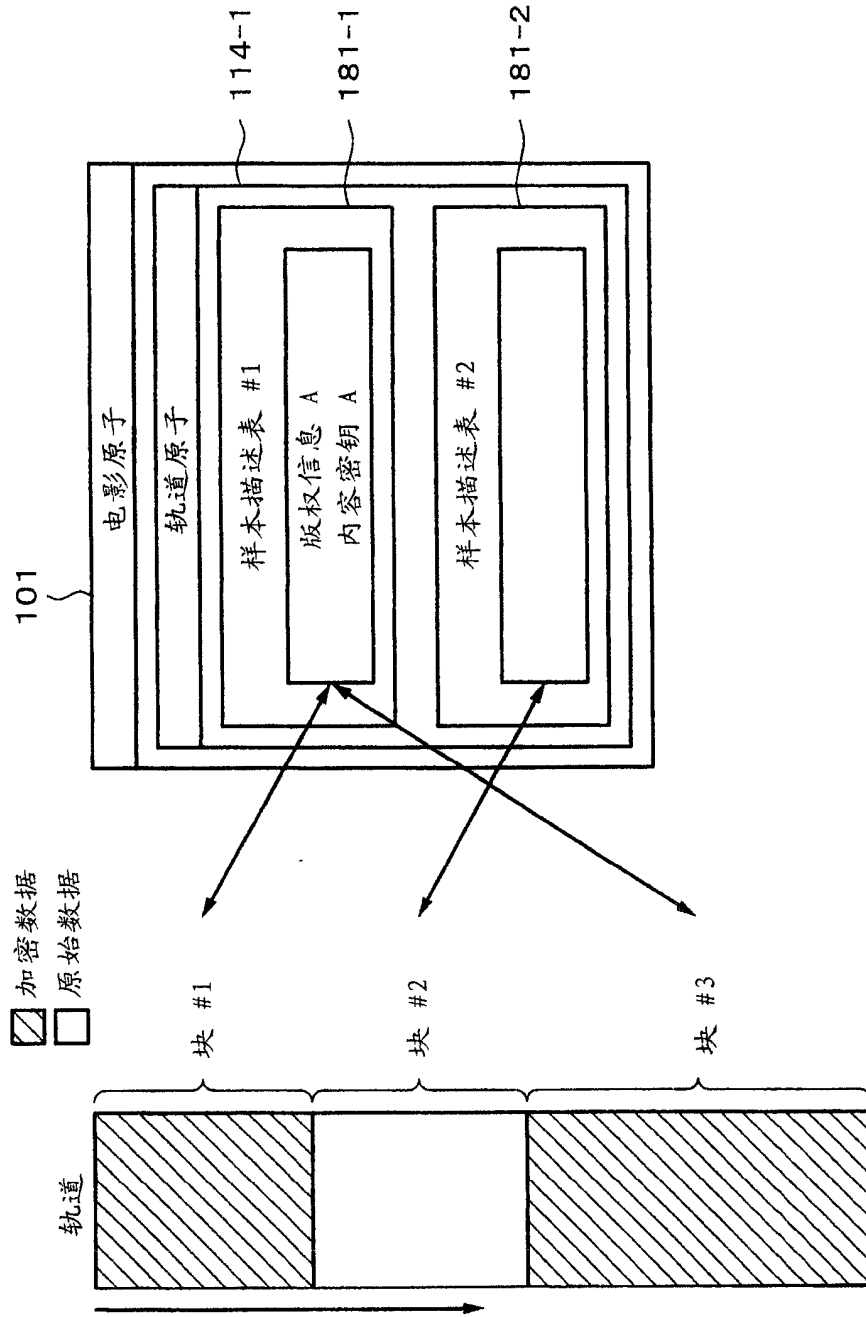


图 14

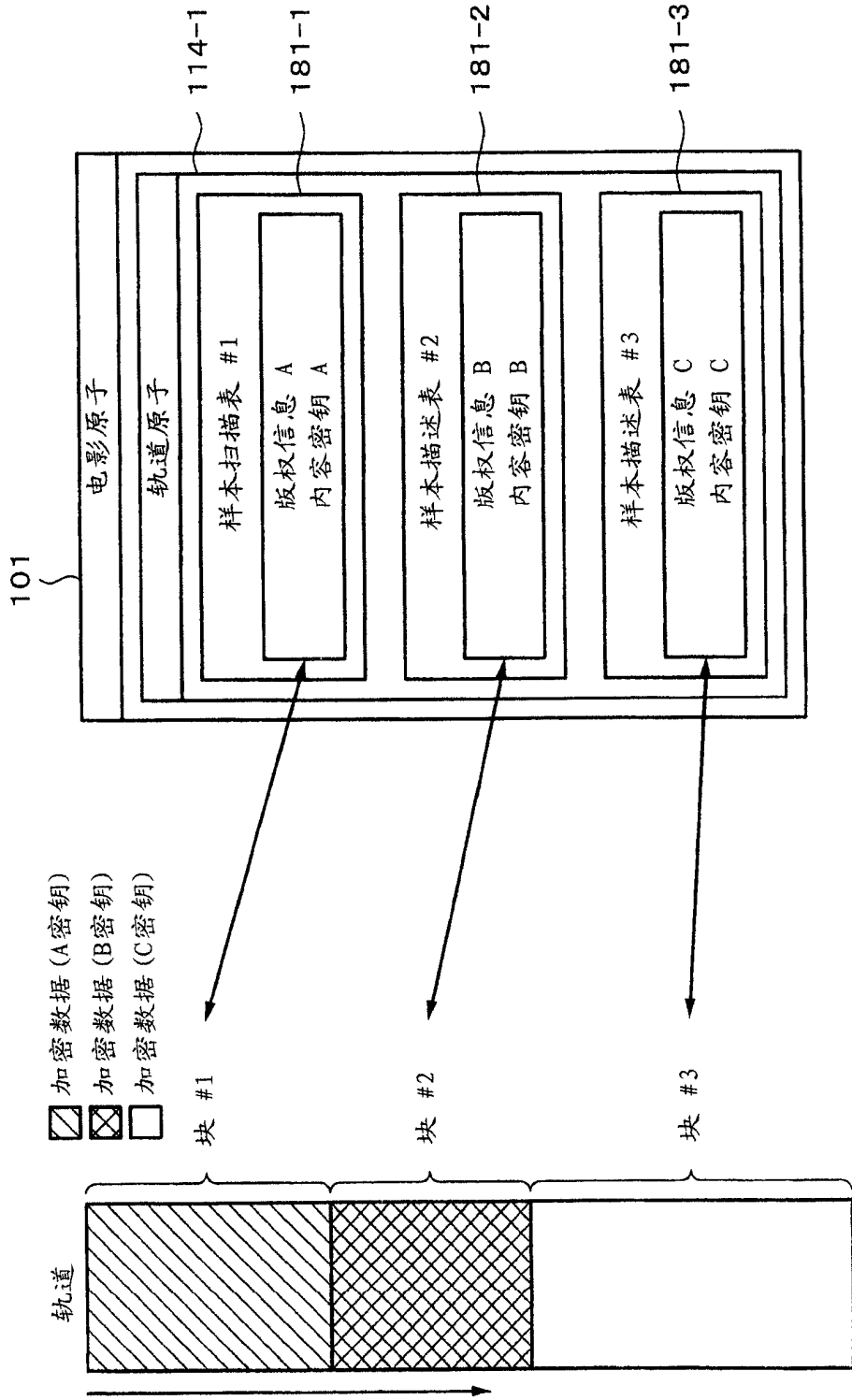


图 15

## 标号说明

11	视频编码器
12	音频编码器
13	视频解码器
14	音频解码器
15	文件发生器
16	文件解码器
17, 20	存储器
18	存储器 控制器
19	系统控制微型计算机
21	纠错码编码器/解码器
23	数据调制器/解调器
24	磁场调制驱动器
26	操作部分
30	伺服电路
31	电机
32	磁头
33	光学拾取器
40	记录媒体
103	EKB文件
104	链接计数器
105	EKB数据
175	样本描述原子
181, 182	样本描述表
191	保护信息块