

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
G06F 17/00 (2006.01)



## [12] 发明专利申请公布说明书

[21] 申请号 200480036369.2

[43] 公开日 2007 年 2 月 21 日

[11] 公开号 CN 1918561A

[22] 申请日 2004. 12. 8

[21] 申请号 200480036369.2

[30] 优先权

[32] 2003. 12. 8 [33] KR [31] 10-2003-0088795

[86] 国际申请 PCT/KR2004/003213 2004. 12. 8

[87] 国际公布 WO2005/055075 英 2005. 6. 16

[85] 进入国家阶段日期 2006. 6. 7

[71] 申请人 学校法人大洋学园

地址 韩国首尔市

共同申请人 三星电子株式会社

[72] 发明人 慎东揆 金濬一 申东日 金龙彬  
崔珣容

[74] 专利代理机构 北京市柳沈律师事务所  
代理人 邸万奎 黄小临

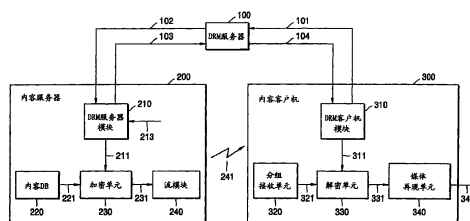
权利要求书 4 页 说明书 9 页 附图 11 页

### [54] 发明名称

运动画面文件加密方法及其数字权限管理方法

### [57] 摘要

一种加密运动画面文件的方法、以及使用该方法的数字权限管理的方法，其中加密方法包括：从运动画面文件的元数据中提取有关至少一个作为实时流单位的视频样本的位置的信息；基于位置信息提取视频样本；基于预定加密信息，对除了每个所提取的视频样本的视频样本首标内的起始码之外所提取的视频样本加密；以及通过重新组合加密的视频样本，产生加密的运动画面文件。由于以视频对象平面(VOP)为单位对文件加密、同时维持 MPEG-4 文件格式，所以可将加密方法容易地应用于完整的文件格式，并还可能实现流服务。



- 1、一种对包括多个视频样本的运动画面文件加密的方法，该方法包括：  
提取至少一个视频样本的位置信息；  
基于已提取的位置信息提取视频样本；  
根据加密信息，对除了标识所提取的视频样本的视频样本标识信息之外的所提取的视频样本的一部分加密；以及  
通过将加密的视频样本重新插入到运动画面文件中，生成加密的运动画面文件。
- 2、如权利要求 1 所述的方法，其中，加密信息包括加密密钥以及加密类型。
- 3、如权利要求 2 所述的方法，其中，使用数字权限管理服务传送加密密钥。
- 4、如权利要求 2 所述的方法，其中，执行加密，使得加密之前的消息字具有与加密之后的对应码字相同数目的位。
- 5、如权利要求 4 所述的方法，其中，加密方法是数据加密标准（DES）或标准韩国语加密算法（SEED）中的一个。
- 6、如权利要求 1 所述的方法，其中，运动画面文件是 MPEG 文件。
- 7、如权利要求 1 所述的方法，其中，运动画面文件是 MPEG 文件，并且，每个视频样本是示出流单位、且被包括在块中的视频对象平面（VOP）。
- 8、如权利要求 7 所述的方法，其中，提取至少一个视频样本的位置信息包括：  
从保存了 VOP 的元数据的 moov 原子内的较低级原子之中的样本表原子内的元数据中，提取块大小、块偏移、以及样本大小；以及  
基于块大小、块偏移、以及样本大小，计算每个 VOP 的位置信息。
- 9、如权利要求 8 所述的方法，其中，加密信息还包括加密模式，其是仅对 VOP 之中的 I-VOP 加密的第一模式、仅对 VOP 之中的 B-VOP 和 P-VOP 加密的第二模式、以及对所有 VOP 加密的第三模式中的一个。
- 10、如权利要求 9 所述的方法，其中，加密信息还包括：用来标识要被加密的 VOP 的 VOP ID。
- 11、如权利要求 10 所述的方法，其中，moov 原子包括数字权限管理原

子, 并且, 数字权限管理原子包括作为元数据的加密信息。

12、如权利要求 11 所述的方法, 其中, 保存数字权限管理原子, 作为 moov 原子的顶部较低级原子。

13、如权利要求 11 所述的方法, 其中, 数字权限管理原子包括加密标志和条目表, 并且, 加密包括: 当将加密标志设置为第一类型时, 对所有 VOP 加密, 而当将加密标志设置为第二类型时, 仅对与包括在条目表内的 VOP ID 相关的 VOP 加密。

14、一种基于加密信息对以视频样本为单位而被选择性加密的运动画面文件解密的方法, 该解密方法包括:

在运动画面文件中检查标识每个视频样本的起始的视频样本标识信息;

基于视频样本标识信息而提取每个视频样本;

基于加密信息, 在已提取的视频样本之中提取加密的视频样本, 其中, 仅对除了视频样本标识信息之外的加密的视频样本的一部分加密;

基于与加密信息相对应的解密信息, 对加密的视频样本解密; 以及

通过在运动画面文件中重新插入解密的视频样本, 生成解密的运动画面文件。

15、如权利要求 14 所述的方法, 其中, 加密信息包括加密密钥以及加密类型。

16、如权利要求 14 所述的方法, 其中, 使用数字权限管理服务传送解密信息。

17、如权利要求 15 所述的方法, 其中, 执行加密, 使得加密之前的消息字具有与加密之后的对应码字相同数目的位。

18、如权利要求 17 所述的方法, 其中, 加密方法是数据加密标准 (DES) 或标准韩国语加密算法 (SEED) 中的一个。

19、如权利要求 15 所述的方法, 其中, 运动画面文件是 MPEG 文件, 每个视频样本是视频对象平面 (VOP), 并且, 加密信息还包括加密模式, 其是仅对 VOP 之中的 I-VOP 加密的第一模式、仅对 VOP 之中的 B-VOP 和 P-VOP 加密的第二模式、以及对所有 VOP 加密的第三模式中的一个。

20、如权利要求 15 所述的方法, 其中, 加密信息还包括用来标识要被加密的 VOP 的 VOP ID。

21、一种使用内容服务器和内容客户机的数字权限管理 (DRM) 的方法,

该方法包括:

对预定运动画面文件执行用户验证过程,其中,内容服务器和内容客户机分别接收加密和解密信息;

在内容服务器上,基于加密信息而以视频样本为单位对运动画面文件加密;

将已被加密的运动画面文件通过流服务器从内容服务器传送到内容客户机;

在内容客户机上,从运动画面文件中提取加密的视频样本;

在内容客户机上,使用解密信息,仅对除了标识视频样本的视频样本标识信息之外的加密视频样本的一部分解密;以及

在内容客户机上,通过在运动画面文件中重新插入解密的视频样本,实时再现解密的运动画面文件。

22、如权利要求 21 所述的方法,其中,接收加密和解密信息包括:

将有关运动画面文件的用户验证请求从内容客户机传送到 DRM 服务器;

在 DRM 服务器上执行用户验证过程,并将包括有关用户验证的信息的 DRM 验证信息从 DRM 服务器传送到内容服务器;

基于 DRM 验证信息而在内容服务器上生成加密密钥,并基于加密密钥和用户输入的可选加密信息而生成加密信息;以及

将加密信息从内容服务器传送到 DRM 服务器,

其中,DRM 服务器将与加密信息对应的解密信息传送到内容客户机。

23、如权利要求 22 所述的方法,其中,运动画面文件是 MPEG 文件。

24、如权利要求 22 所述的方法,其中,运动画面文件是 MPEG 文件,并且,视频样本是作为流单位、且被包括在块中的视频对象平面(VOP),并且,以视频样本为单位加密运动画面文件包括:

通过解析 MPEG 文件的 moov 原子,生成有关每个 VOP 的位置的信息;

基于有关每个 VOP 的位置的信息,提取 MPEG 文件的媒体数据原子内的每个 VOP;

基于加密信息仅对除了 VOP 首标内的起始码之外的每个提取的 VOP 的一部分加密;以及

通过在 MPEG 文件中重新插入已被加密的 VOP,生成加密的 MPEG 文

件。

25、如权利要求 24 所述的方法，其中，生成有关每个 VOP 的位置的信息包括：

从 moov 原子内的较低级原子之中的样本表中，提取块大小、块偏移、以及样本大小；以及

基于块大小、块偏移、以及样本大小，计算有关每个 VOP 的位置的信息。

26、如权利要求 21 所述的方法，其中，加密信息包括加密密钥以及加密类型。

27、如权利要求 26 所述的方法，其中，执行加密，使得加密之前的消息字具有与加密之后的对应码字相同数目的位。

28、如权利要求 27 所述的方法，其中，加密方法是数据加密标准 (DES) 或标准韩国语加密算法 (SEED) 中的一个。

29、如权利要求 21 所述的方法，其中，视频样本是作为流单位、且被包括在块中的视频对象平面 (VOP)，并且，提取加密的视频样本包括：

通过对传送分组的传送协议首标去封装，仅提取分组的数据部分；

通过重新组合分组的数据部分，产生组合的数据流；

检查标识组合的数据流内的每个 VOP 的 VOP 标识信息；

基于 VOP 标识信息提取每个 VOP；以及

基于加密信息提取所提取的 VOP 之中的加密的 VOP。

## 运动画面文件加密方法及其数字权限管理方法

### 技术领域

本发明涉及对运动画面文件加密的方法、以及使用该方法来管理数字权限的方法，并且，更具体地涉及对运动画面文件加密、同时保持运动画面文件的格式以便有可能实现在数字权限管理下的流服务的方法，以及使用该加密方法的数字权限管理方法。

### 背景技术

当前，服务提供方以下载服务或流服务的形式向用户提供多媒体数据。下载服务允许将整个多媒体文件从服务提供方的计算机下载到用户的计算机，并随后再现该文件。流服务是在服务提供方将文件分割为实时可刷新片段、并将所述片段传送到实时再现所述片段的用户时的服务。

无论服务提供方提供哪个服务，用户均必须在能够再现文件之前完成获取相关多媒体数据的合法权限的过程。应阻止尝试在未获取合法权限的情况下访问文件的用户。为帮助这样的选择性规定、以及访问的拒绝，对多媒体文件加密。

数字权限管理（DRM）是用于仅允许具有合法权限的用户访问加密文件的所有种类的系统的解决方案。通常，DRM 系统包括内容提供方、用户、DRM 服务器等，并可包括电子支付过程、用户验证过程、以及公共密钥基础结构（infrastructure）（PKI）。

最基本的 DRM 方法是：对运动画面专家组（MPEG）文件加密、将加密的文件传送到用户，并且，随后，如果通过用户验证过程而确认用户具有合法权限，则将可对加密的文件解密的密钥提供给用户。用户验证过程可包括电子支付过程，并且，PKI 可用于传送密钥。

然而，因为解密仅在下载整个文件之后才可能实现，所以，加密方法不能用于流服务。也就是说，即使从 DRM 服务器传送了用户密钥，也不可能再现对应的文件，直到下载了整个加密的文件为止。

另一个加密方法涉及：在运动画面文件编码过程期间，对离散余弦变换

系数 - 例如 AC 或 DC 值 - 加密。

然而, 此方法不对完整的运动画面文件加密, 而是向运动画面文件编码过程添加附加的加密过程。结果, 不能将此方法容易地应用于完整的运动画面文件。另外, 如果内容提供方必须在运动画面文件产生过程中应用专为内容提供方指定的加密算法, 则内容提供方具有必需依赖于运动画面文件提供方来提供服务的缺点。这阻碍了在线内容产业的成长和发展。

### 发明内容

本发明提供了一种加密方法以及使用该加密方法的数字权限管理方法。该加密算法可被应用于流服务, 并且同时, 其可被容易地应用于完整的运动画面文件, 而不参与运动画面文件产生过程。

因为在维持 MPEG-4 文件格式的同时以 VOP 为单位来加密文件, 所以, 根据本发明的 MPEG-4 文件加密方法和使用其的数字权限管理方法可容易被应用于文件格式的完整形式, 并且有可能实现流服务。

另外, 因为可在不参与 MPEG-4 文件产生过程的情况下加密文件, 所以, 有可能实现内容提供方的独立加密, 这将帮助推进内容提供产业。

### 附图说明

通过参照附图来详细描述本发明的示范实施例, 本发明的各方面将变得更加清楚, 附图中:

图 1 是运动画面文件格式的图;

图 2 是根据本发明的示范实施例的数字权限管理系统的示意图;

图 3 是根据本发明的示范实施例的 MPEG-4 文件加密方法的流程图;

图 4 是 MPEG-4 文件的媒体数据原子 (atom) 的结构图;

图 5A 是 MPEG-4 文件的 moov 原子的结构图;

图 5B 是块大小原子、样本数目原子、以及样本大小原子的内部结构的图;

图 6A、6B、及 6C 是以各种方式加密的 MPEG 文件的再现图像;

图 7 是通过流模块而分组化的传送分组的内部结构的图;

图 8 是在接收到传送分组之后播放 MPEG-4 文件的内容客户机的方法的流程图;

图 9 是所传送的视频对象平面 (video object plane, VOP) 的内部结构的图;

图 10 是根据本发明的示范实施例的数字权限管理原子的内部结构图；和图 11 是产生原子的应用程序接口代码的例子的图。

### 具体实施方式

根据本发明的一方面，提供了对包括媒体数据区和元数据区的运动画面文件加密的方法，该方法包括：从运动画面文件的元数据中提取与至少一个作为实时流单位的视频样本的位置有关的信息；基于位置信息提取至少一个视频样本；基于预定的加密信息，除了每个所提取的视频样本的视频样本首标内的起始码之外，对所提取的视频样本加密；以及通过组合所加密视频样本产生加密的运动画面文件。

提取至少一个视频样本的位置信息可包括：检查在 moov 原子的较低级原子之中是否存在视频媒体信息原子；当存在视频媒体信息原子时，从块偏移原子和样本大小原子中提取块大小、块偏移、以及样本大小；以及基于所提取的块大小、块偏移、以及样本大小，计算每个视频对象平面（VOP）的偏移。

根据本发明的另一方面，提供了基于预定信息而对以 VOP 为单位加密的 MPEG-4 文件解密的方法，该解密方法包括：检测 MPEG-4 文件内的每个 VOP 的起始码；基于起始码提取每个 VOP；基于加密信息在所提取的 VOP 中提取加密的 VOP；基于与加密信息相对应的解密信息对加密的 VOP 解密；以及通过组合解密的 VOP 而再现解密的 MPEG-4 文件。

加密信息可包括解密密钥、加密类型、加密模式、以及 VOP ID。

根据本发明的另一方面，提供了数字权限管理的方法，其包括：内容服务器和内容客户机通过 DRM 服务器对预定的 MPEG-4 文件进行用户验证过程，来接收加密和解密信息；内容服务器基于加密信息而以 VOP 为单位对相关的 MPEG-4 文件加密；将包括加密的 MPEG-4 文件的 VOP 的分组通过流服务器传送到内容客户机；内容客户机从该分组中提取加密的 VOP；使用解密信息对所提取的 VOP 解密；以及通过组合解密的 VOP 而实时再现解密的 MPEG-4 文件。

现在，将通过参照附图而更完全地描述本发明，在附图中示出了本发明的示范实施例。

图 1 是运动画面文件格式的图。

运动画面文件包括 MPEG-1、MPEG-2、以及 MPEG-4 文件格式。将每个运动画面文件划分为包括用户数据的媒体数据区、以及存储再现文件所需的元数据 - 如用户数据的位置和大小 - 的元数据区。下面, 将描述应用于 MPEG-4 文件格式的本发明的示范实施例。

MPEG-4 文件 10 包括多个原子 20、21、22、30、31、以及 32。每个原子 20、21、22、30、31、以及 32 具有较低级别原子, 由此形成分层结构。这里, 将较高的原子称为容器原子, 而较低的原子称为叶 (leaf) 原子。两个顶级原子为 moov 原子 20 和媒体数据原子 mdat 30。将被保存在 MPEG 文件内的用户媒体数据 - 即音频或视频数据 - 保存在媒体数据原子 30 中。将有关媒体数据的信息 - 即元数据 - 保存在 moov 原子 20 中。媒体数据原子 30 包括多个视频对象平面 VOP 31 和 32 等、以及音频数据 33 和 34。

图 2 是用于解释根据本发明的数字权限管理系统的示意图。

用于数字权限管理 (DRM) 的系统包括内容服务器 200、以及内容客户机 300。内容服务器 200 向用户提供媒体数据, 并包括 DRM 服务器模块 210、内容数据库 220、加密单元 230、以及流模块 240。内容客户机 300 从内容服务器 200 接收内容、并再现该内容, 且包括 DRM 客户机模块 310、分组接收单元 320、解密单元 330、以及媒体再现单元 340。

DRM 服务器 100 进行用户验证、以及内容服务器 200 和内容客户机 300 之间的密钥的传送。当内容客户机 300 内的 DRM 客户机模块 310 将用于用户验证的请求 101 发送到 DRM 服务器 100 时, DRM 服务器 100 使用电子支付系统 (未示出) 进行用户验证过程。在完成了用户验证之后, DRM 服务器 100 使用例如已用来执行用户验证的用户信息, 产生 DRM 验证信息 102。随后, 将所产生的 DRM 验证信息 102 传送到内容服务器 200。

内容服务器 200 内的 DRM 服务器模块 210 根据从内容客户机 300 传送的 DRM 验证信息 102 产生加密密钥, 并将加密密钥和用户输入的可选加密信息 213 发送到加密单元 230, 作为加密信息 211。可选加密信息 213 包括加密方法的类型、作为加密的对象的 VOP ID、加密模式等。

内容服务器 200 内的 DRM 服务器模块 210 和内容客户机 300 内的 DRM 客户机模块 310 与 DRM 服务器 100 进行用户验证。DRM 服务器模块 210 从 DRM 服务器 100 接收 DRM 验证信息 102, 并使用 DRM 验证信息 102 来产生加密密钥。并且, DRM 服务器模块 210 将包括加密密钥和用户输入的可选

加密信息 213 的加密信息 211 发送到加密单元 230。另外，DRM 服务器模块 210 使用加密信息 211 和 DRM 服务所需的其它信息产生 DRM 加密信息 103，并将 DRM 加密信息 103 发送到 DRM 服务器 100。

DRM 服务器 100 执行用户验证过程，并通过将从用户验证过程接收的各种信息添加到从 DRM 服务器模块 210 接收的 DRM 加密信息 103，产生 DRM 解密信息 104，并将 DRM 解密信息 104 发送到 DRM 客户机模块 310。如果 DRM 服务使用对称密钥结构，那么，包括在 DRM 加密信息 103 中的加密密钥与包括在 DRM 解密信息 104 中的解密密钥相同。然而，如果 DRM 服务使用非对称密钥结构，那么，加密密钥与解密密钥不同。结果，DRM 加密信息 103 和 DRM 解密信息 104 不同。

客户机模块 310 从 DRM 服务器 100 接收 DRM 解密信息 104，并从 DRM 解密信息 104 中提取解密信息 311。解密单元 330 使用解密信息 311 对运动画面文件解密。

在图 2 中，内容服务器 200 内的加密单元 230 通过从内容数据库 220 接收内容 221、并对内容 221 加密，而产生加密内容 231。根据本发明的示范实施例，内容 221 和加密内容 231 具有图 1 中图解的相同的 MPEG-4 文件格式。

图 3 是根据本发明的示范实施例的 MPEG-4 文件加密方法的流程图。

根据本发明的示范实施例，以 VOP 为单位加密 MPEG-4 文件，而不是作为整体来加密 MPEG-4 文件。可通过可选加密信息 213 选择要被加密的 VOP。加密方法是块加密方法，如数据加密标准 (DES) 或 128 位类型标准韩国语 (Korean) 加密算法 (SEED)。由于加密方法是块加密方法，所以，它不改变原始 MPEG-4 文件的大小和形式。换句话说，在加密之前和之后的 MPEG-4 文件的大小和格式是相同的。因此，可在无任何修改的情况下使用原始 MPEG-4 文件的再现算法。并且，尽管以 VOP 为单位进行加密，但是，因为每个 VOP 的最先 4 个字节是用来在内容客户机 300 上提取 VOP 的起始码，所以，不对每个 VOP 的最先 4 个字节加密。

在从内容数据库接收的 MPEG-4 文件的 moov 原子中提取每个 VOP 的偏移 (操作 301)。VOP 的偏移表示 MPEG-4 文件内的 VOP 的位置信息。利用每个 VOP 的偏移作为基础，提取由可选加密信息 213 选择的 VOP (操作 302)。使用 DES 或 SEED 对所提取的 VOP 加密 (操作 303)。通过将加密的 VOP 和非加密的 VOP 组合，产生加密的 MPEG-4 文件 (操作 304)。

下面,参照图 4 至 6 描述用于 MPEG-4 文件的每个 VOP 的偏移提取过程。

图 4 是 MPEG-4 文件的媒体数据原子的结构图。

取决于 MPEG-4 文件格式,媒体数据原子包括存在实际媒体数据的块(chunk)、以及不存在媒体数据的未使用部分。块包括视频块和音频块,并将每个块划分为很多样本。当包括在块中的媒体数据为视频数据时,样本为 VOP。

图 5A 是 MPEG-4 文件的 moov 原子的结构图。

moov 原子 510 包括很多轨道原子(轨道 1) 520,并且,每个轨道原子(轨道 1) 520 包括作为较低级原子的媒体原子 530,媒体原子 530 包括作为较低级原子的媒体信息原子 540,并且,媒体信息原子 540 包括作为较低级原子的样本表原子 550。

每个原子的最先 4 字节具有与原子的大小有关的信息,接下来的 4 个字节具有与原子的类型有关的信息,而该区的余下部分具有原子示出的媒体数据信息。媒体信息原子 540 还具有作为较低级原子的视频信息原子 541。视频信息原子 541 示出:对应的媒体数据为视频数据。样本表原子 550 具有作为较低级原子的块大小原子 551、样本数目原子 552、以及样本大小原子 553。

图 5B 是块大小原子 551、样本数目原子 552、以及样本大小原子 553 的内部结构的图。

在图 5B 的第一个图中,与每个块中的样本数目有关的信息被包括在块大小原子 551 的元数据区中。此图示出了第一和第四块 611 和 612 各自具有 14 个视频样本,并且,第十块 613 具有 13 个视频样本。在图 5B 的第二个图中,与每个块的位置有关的信息被包括在样本数目原子 552 的元数据区中。此图示出了:从 40 位起示出第一块 614,而从 607848 位起示出第十块 615。在图 5B 的第三个图中,样本大小原子 553 示出了与每个样本的大小有关的信息。此图示出了第一样本 617 具有 12604 位的大小。

通过解析元数据而进行提取 MPEG-4 文件内的每个 VOP 的偏移的过程。首先,通过确认对应的媒体数据是视频数据,确定视频媒体信息原子 541 是否存在于媒体信息原子 540 内。如果媒体数据是视频数据,则将媒体数据解析到作为下一个较低级原子的样本表原子 550,以提取元数据。

可根据在上述三个原子中保存的信息的组合,提取样本-即 VOP-的偏移信息。在图 5B 的第一个图中,第一块的大小-即包括在第一块中的样本的

数目 - 为 14。在图 5B 的第二个图中, 第一块的偏移为 40 位。在图 5B 的第三个图中, 第一块的大小为 12604 位。因此, 第二块的偏移为  $40+12604=12644$  位。可使用相同的方法提取所有样本 (VOP) 的偏移。

图 6A 至 6C 是以各种方式加密的加密 MPEG 文件的再现图像。

可通过可选加密信息 (213) 选择要加密的 VOP。可选加密信息 (213) 被用户输入到 DRM 服务器模块 (210), 与加密密钥一起被传送到加密单元 (230), 并用于加密。

可选加密信息包括加密模式、或加密标识 ID。将加密模式划分为对所有 I-VOP 加密的第一模式、对所有 B-VOP 和 P-VOP 加密的第二模式、以及对所有 I-VOP、B-VOP 和 P-VOP 加密的第三模式。如果选择了加密 ID, 则仅对与作为可选加密信息而输入的加密号相对应的 VOP 加密。在不考虑 VOP 的类型的情况下选择被加密的 VOP。

在图 6A 中, 左边的图像是加密前的图像, 而右边的图像是使用第一模式加密后的 MPEG 图像。由于 I-VOP 是帧内编码的 VOP, 所以, 有关图示图像的所有信息被包括在宏块内。由此, 可以看出, 完全丢失了帧内块信息。另外, 因为 I-VOP、P-VOP 和 B-VOP 的参考位置改变, 所以, 再现了完全不同的图像。

在图 6B 中, 左边的图像是加密前的原始图像, 而右边的图像是使用第二模式加密的 MPEG 图像。有关帧内编码的宏块的信息和运动向量共存于 B-VOP 和 P-VOP 中。因此, 以第二模式加密的 MPEG 图像比第一模式更相似于原始图像。对 P-VOP 中的运动向量加密, 但是, 由于 I-VOP 中的帧内块的影响, 偶尔会示出连续帧之间的整个帧。可以看出, 因为对运动向量加密, 仅每个对象的运动路径变得不规则。

在图 6C 中, 左边的图像是加密前的原始图像, 而右边的图像是使用第三模式加密的 MPEG 图像。因为第三模式加密所有 VOP, 所以, 第三模式产生最完整的加密运动画面。随着被加密的 VOP 的数目的增加, 加密性能增加, 但解密需要更多资源。

在加密之后, 通过重新组合加密的 VOP, 产生了新的加密的 MPEG-4 文件。通过流模块 240 将所产生的加密 MPEG-4 文件流式发送到内容客户机 300。为了流式发送 MPEG-4 文件, 需要将它分组化。

图 7 是通过流模块而分组化的传送分组的内部结构的图。

回来参照图 2, 流模块 240 通过对所接收的加密 MPEG-4 文件分组化, 产生传送分组 241。图 7 示出了以时间次序传送的四个传送分组。每个传送分组 710、720、730 和 740 包括: 传送协议首标 711、712、721、722、731、732、741 和 742; 和传送数据 713、723、724、733、743 和 744。传送协议首标根据传送路径而不同, 并且通常使用用户数据程序协议和实时传送协议。

第一传送分组 710 包括作为传送数据 713 的第一 VOP (VOP1) 的一部分, 而第二传送分组 720 包括作为传送数据 723 的第一 VOP (VOP1) 的余下部分、以及作为传送数据 724 的第二 VOP (VOP2) 的一部分。第三传送分组 730 包括作为传送数据 733 的第二 VOP (VOP2) 的另一部分, 而第四传送分组 740 包括作为传送数据 743 的第二 VOP (VOP2) 的余下部分、以及作为传送数据 744 的第三 VOP (VOP3) 的一部分。每个传送分组具有作为传送数据的 VOP 的一部分的原因在于: VOP 的大小不同, 并且, 传送分组的长度和传送的 VOP 的大小不匹配。在图 7 中, 传送数据 724、733 和 743 的阴影线部分示出了加密的 VOP。

可将流模块 240 构造为独立服务器, 且与内容服务器 200 分离。在此情况下, 在例如因特网的通信网络上进行从加密单元 230 到流服务器 (未示出) 的 MPEG-4 文件的传送。

图 8 是内容客户机 300 在接收到传送分组 241 之后播放 MPEG-4 文件的方法的流程图。

内容客户机 300 内的分组接收单元 320 接收传送分组 241, 并提取 VOP。通过监控在分组接收单元 320 内输入缓冲器的分组, 进行 VOP 提取过程。首先, 分组接收单元 320 通过从所接收的传送分组 241 中移除传送协议首标 711、712、721、722、731、732、741 和 742, 执行去封装 (decapsulization) (操作 801)。

接下来, 检查是否接收到每个 VOP 中的 VOP 首标内的起始码 (操作 802)。

图 9 是所传送的 VOP 900 的内部结构的图。每个 VOP 910、920、930 等包括 VOP 首标 911 和 VOP 数据 912, 并具有起始码 913, 其是每个 VOP 首标 911 的最先 4 个字节。

起始码是每个 VOP 的最先 4 个字节, 并具有预定值。当检测到下一 VOP 的起始码时, 提取当前 VOP, 并将其发送到解密单元 330 (操作 803)。

使用通过 DRM 服务器 100 而从内容服务器 200 接收的 DRM 解密信息

311, 解密单元 330 对相关的 VOP 解密 (操作 804)。DRM 加密信息 311 包括加密类型、加密的 VOP ID、有关加密模式的信息、以及加密密钥, 并分别通过 DRM 服务器模块 210、DRM 服务器 100、以及 DRM 客户机模块 310 而被发送到解密单元 330。

在从解密单元 330 接收到解密的 VOP、并重新组合解密的 VOP 之后, 媒体再现单元 340 创建并再现解密的 MPEG-4 文件 (操作 805)。

图 10 是根据本发明的示范实施例的数字权限管理原子的内部结构的图。

在本发明的另一个示范实施例中, 包括新的原子, 其是传统的 MPEG-4 文件的元数据。在图 2 中, 加密信息 211 被包括在 DRM 加密信息 103 中, 并被发送到 DRM 服务器 100, 但是在本示范实施例中, 加密信息 211 被包括在 DRM 原子 1000 中。加密信息 211 可包括加密密钥、加密类型、加密模式、以及加密的 VOP ID。

图 10 中图解的 DRM 原子 1000 包括原子大小 1010、原子类型 1020、加密模式 1030、加密标志 1040、条目的数目 1050、以及条目表 1060。

当将加密标志 1040 设为 1 时, 其意味着对所有 VOP 加密, 而当将加密标志 1040 设为 0 时, 其意味着仅对一部分 VOP 加密。将被加密的一部分 VOP 的 VOP ID 保存在条目表 1060 中, 并将加密的 VOP 的数目保存在条目数目 1050 中。

为了不改变传统的 MPEG-4 文件格式, 将 DRM 原子 1000 定位为 moov 原子内的顶级原子。如果 DRM 原子 1000 被定位在 moov 原子内的较低级, 则将必须改变所有较高级 DRM 原子的大小。

本示范实施例具有减少对内容客户机 300 管理与加密信息 211 相对应的解密信息 311 上的分离文件系统的需要, 这是因为, 连同 MPEG-4 文件一起传送加密信息 211。

图 11 是产生原子的应用程序接口 (API) 代码的例子的图。苹果公司提供了 QuickTime, 作为用来产生 MPEG-4 文件格式原子的 API。图 11 是使用 QuickTime 的原子产生的例子。根据图 11, 可以看出, 将原子命名为 'drma', 并且, 将其大小设为 '1000'。

尽管已参照本发明的示范实施例具体地示出并描述了本发明, 但本领域的技术人员将理解, 可在其中作出形式和细节上的各种改变, 而不背离如由所附权利要求及其等价物定义的本发明的精神和范围。

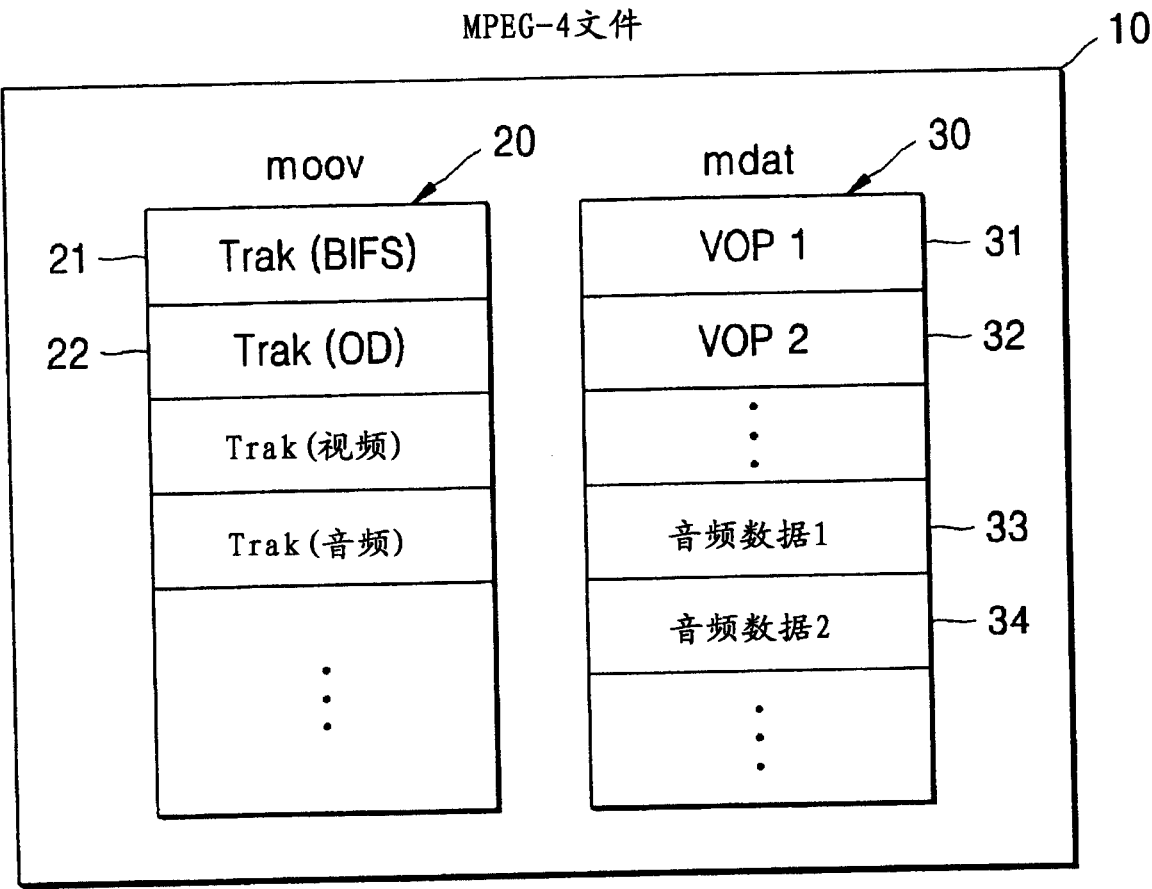


图 1

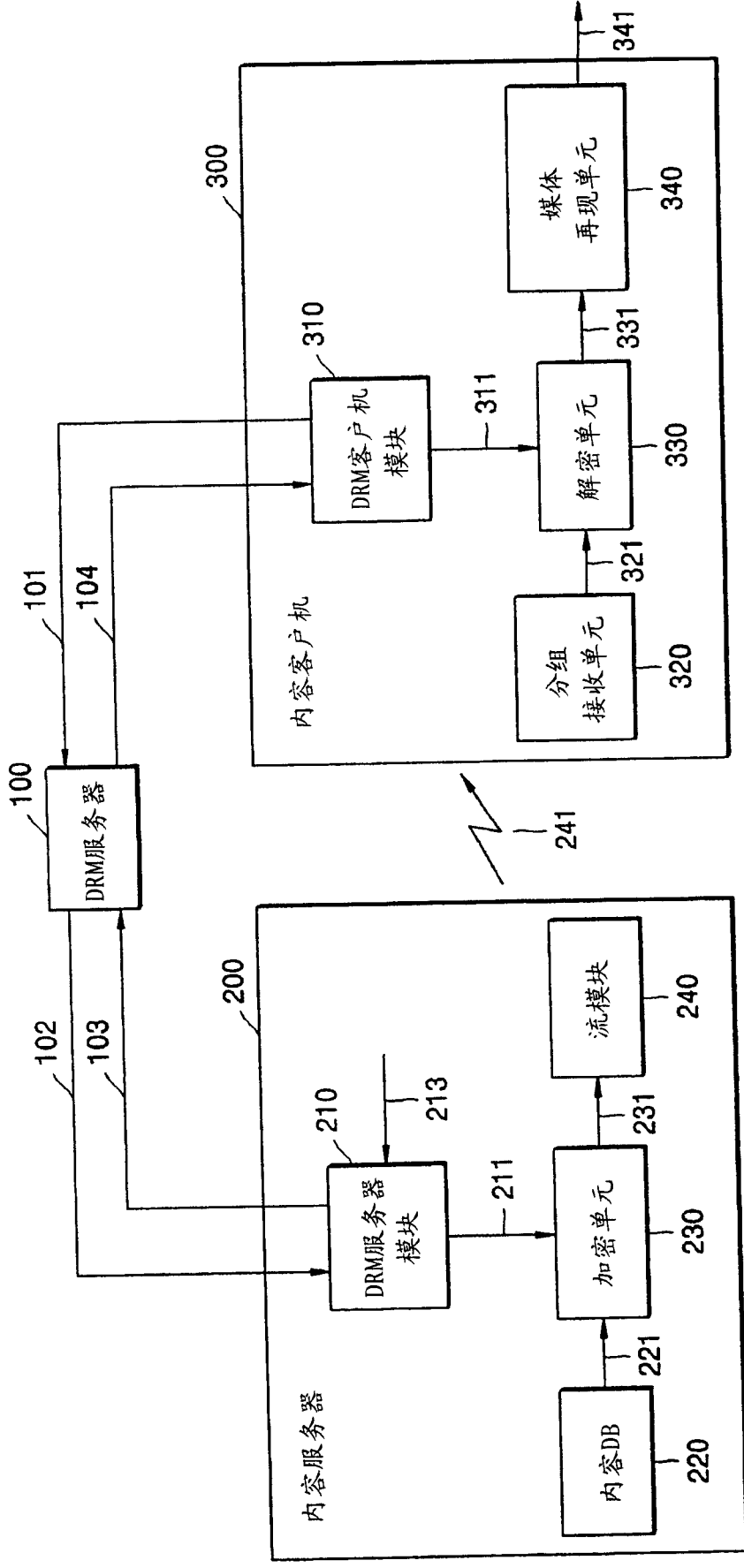


图 2

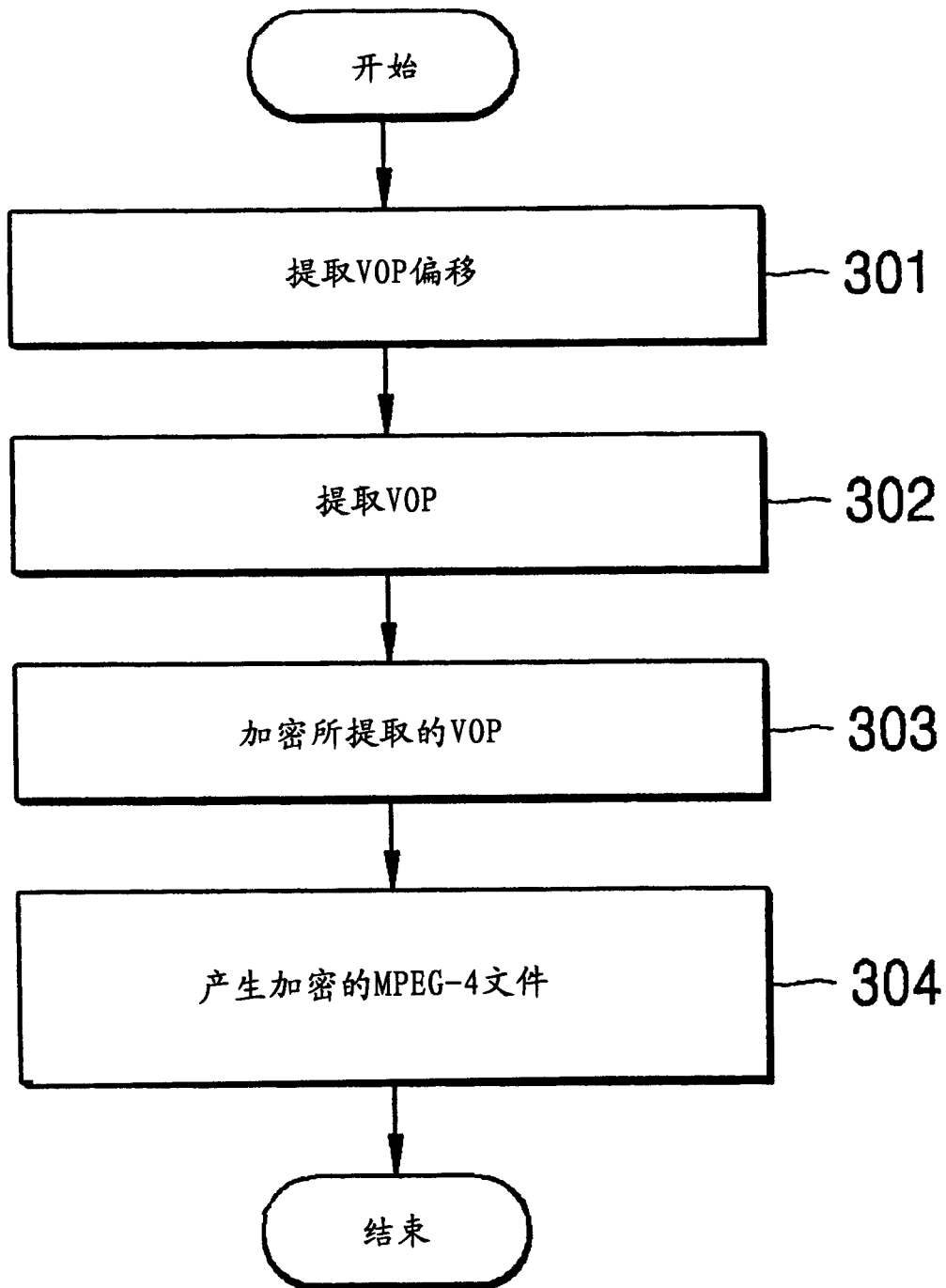


图 3

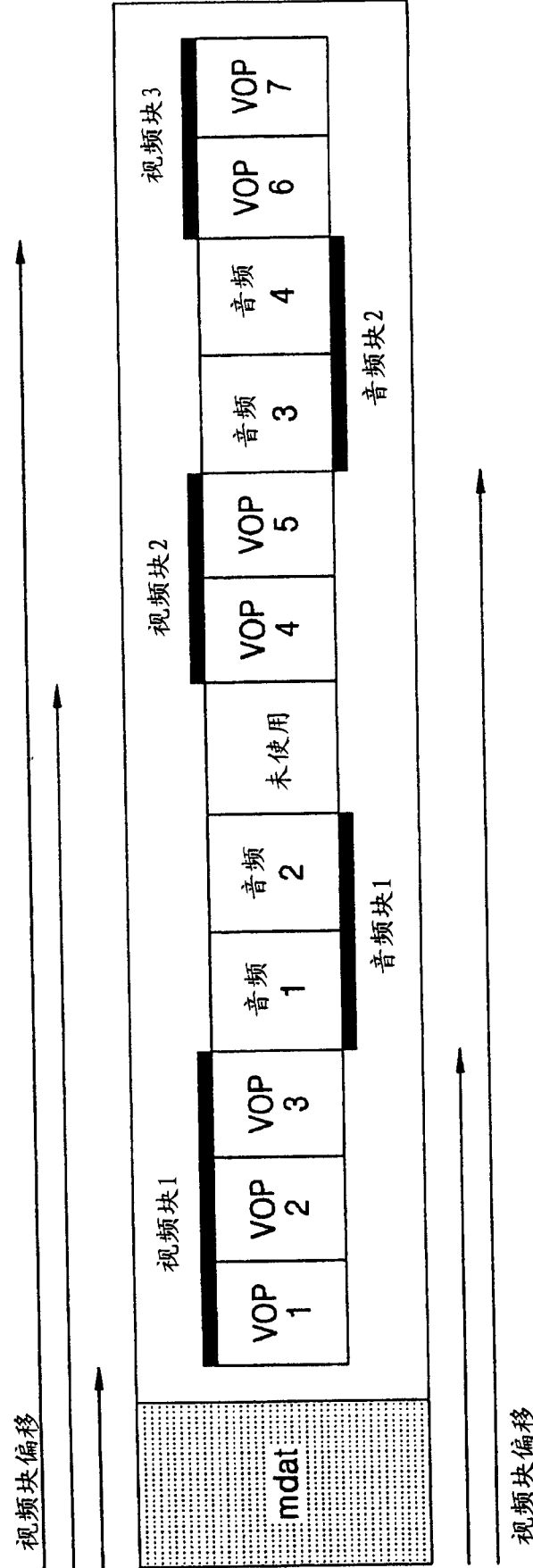


图 4

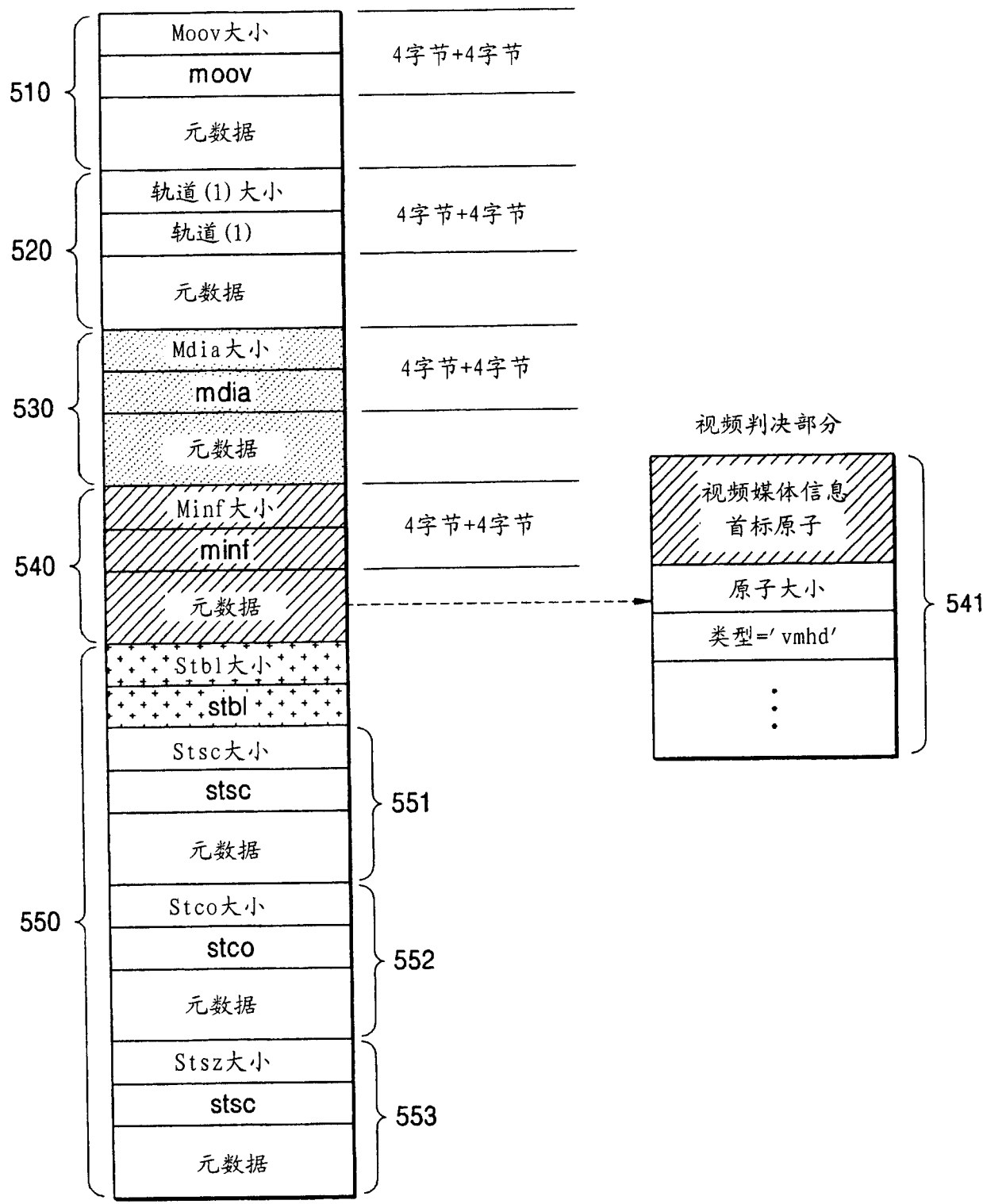


图 5A

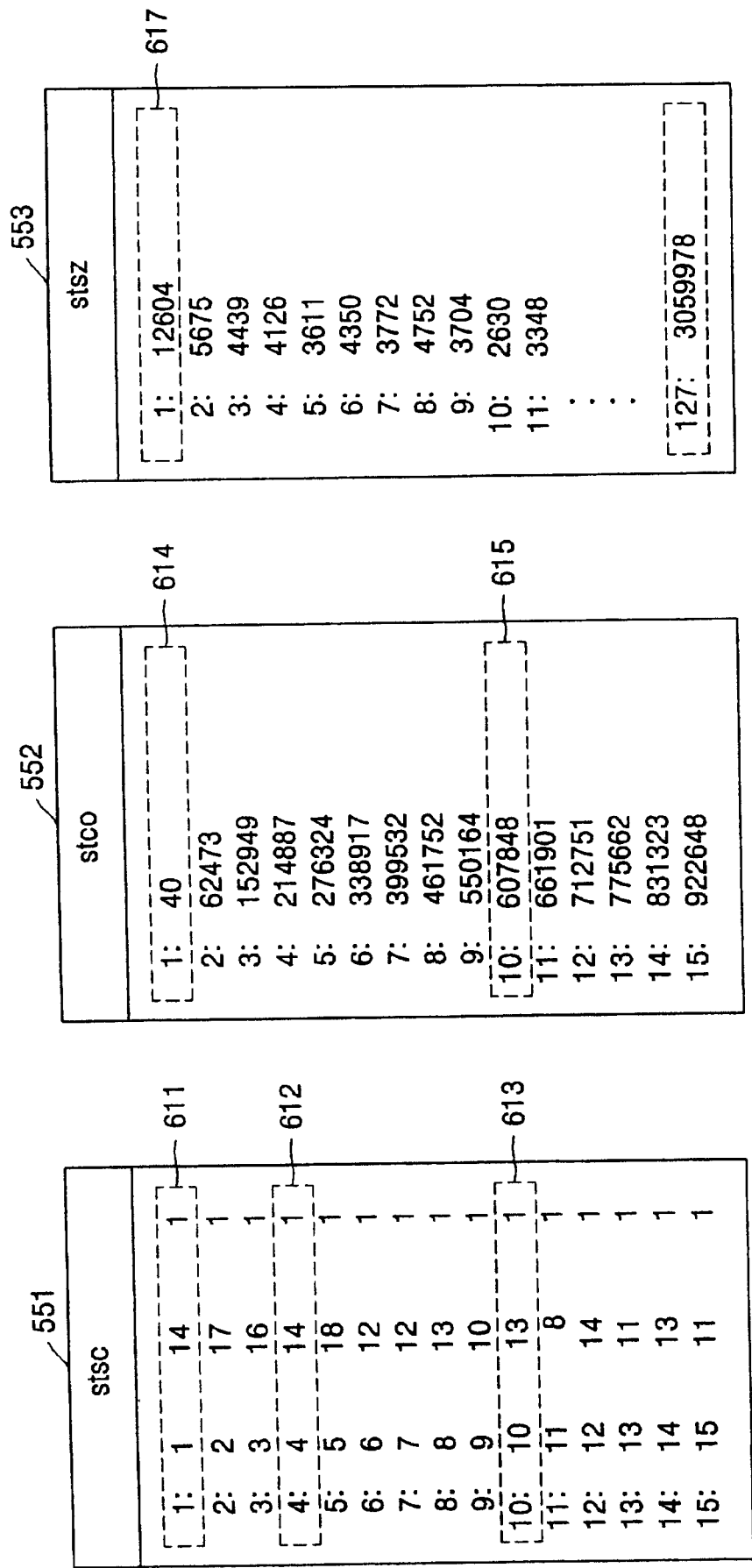


图 5B

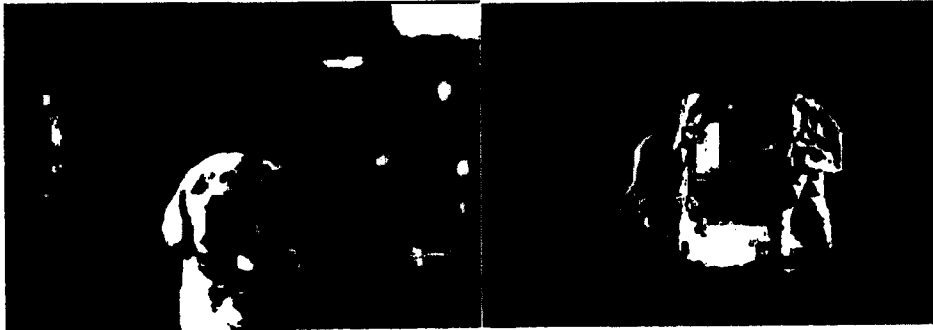


图 6A

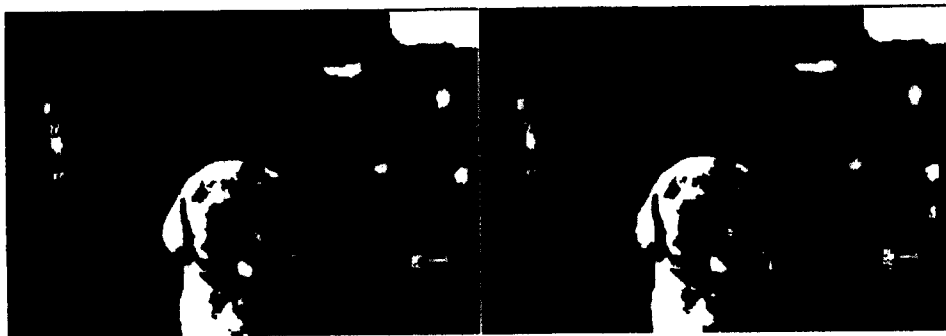


图 6B

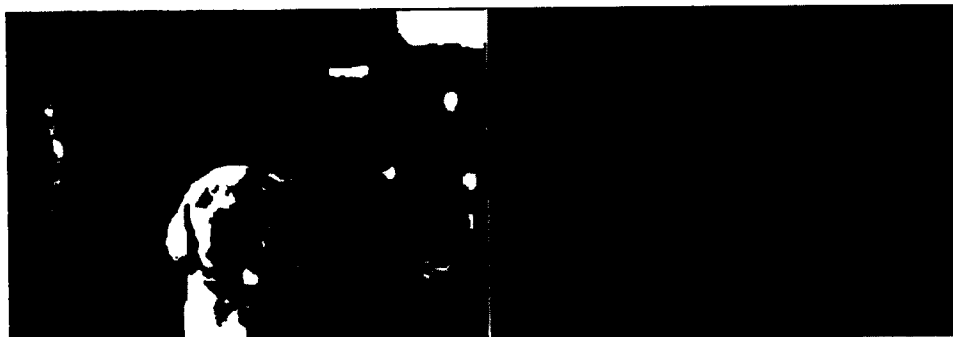


图 6C

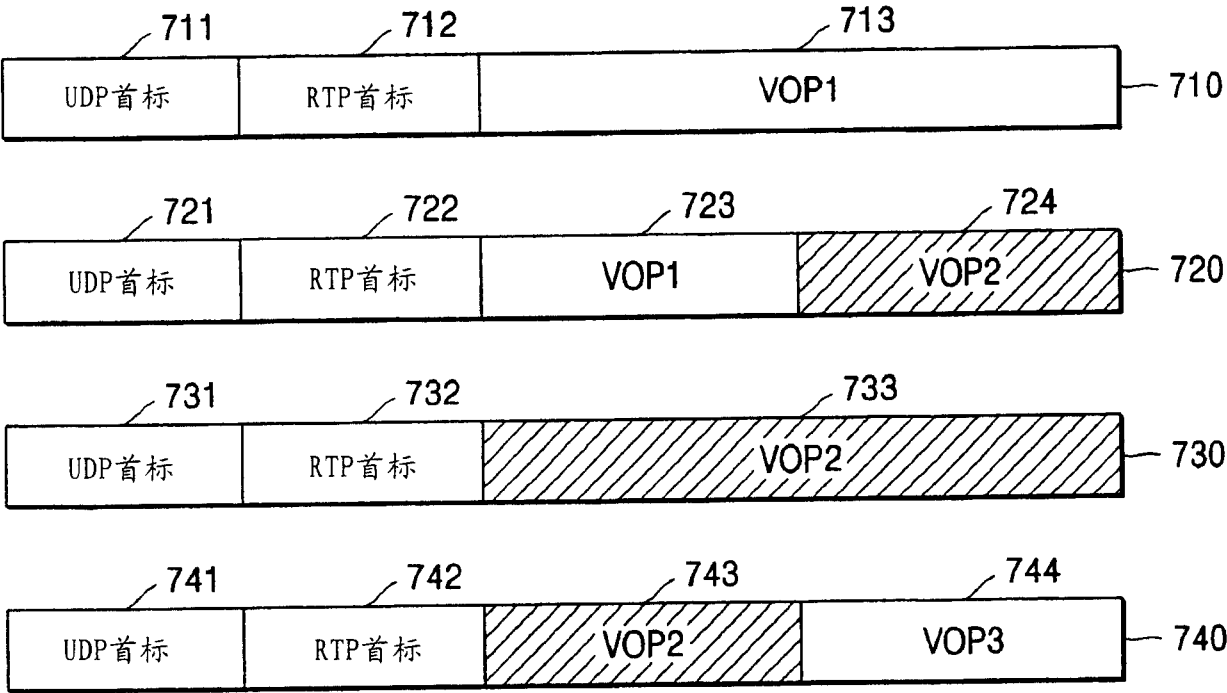


图 7

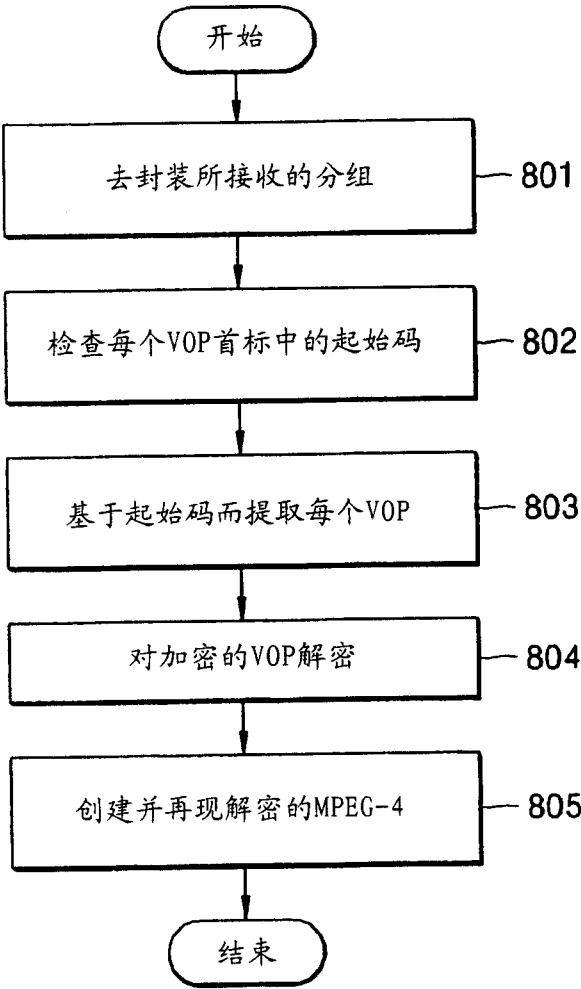


图 8

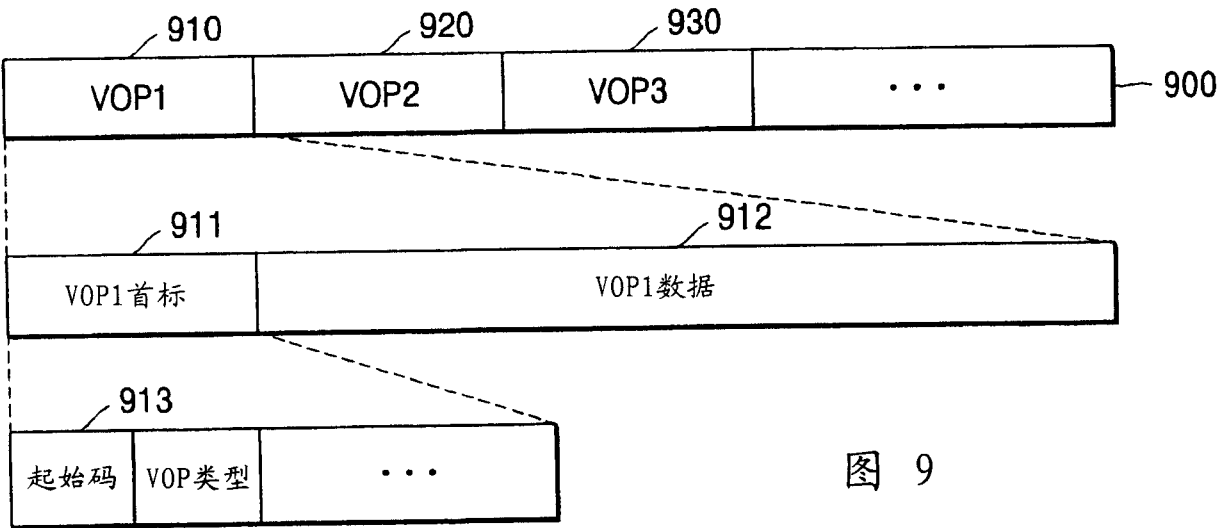


图 9

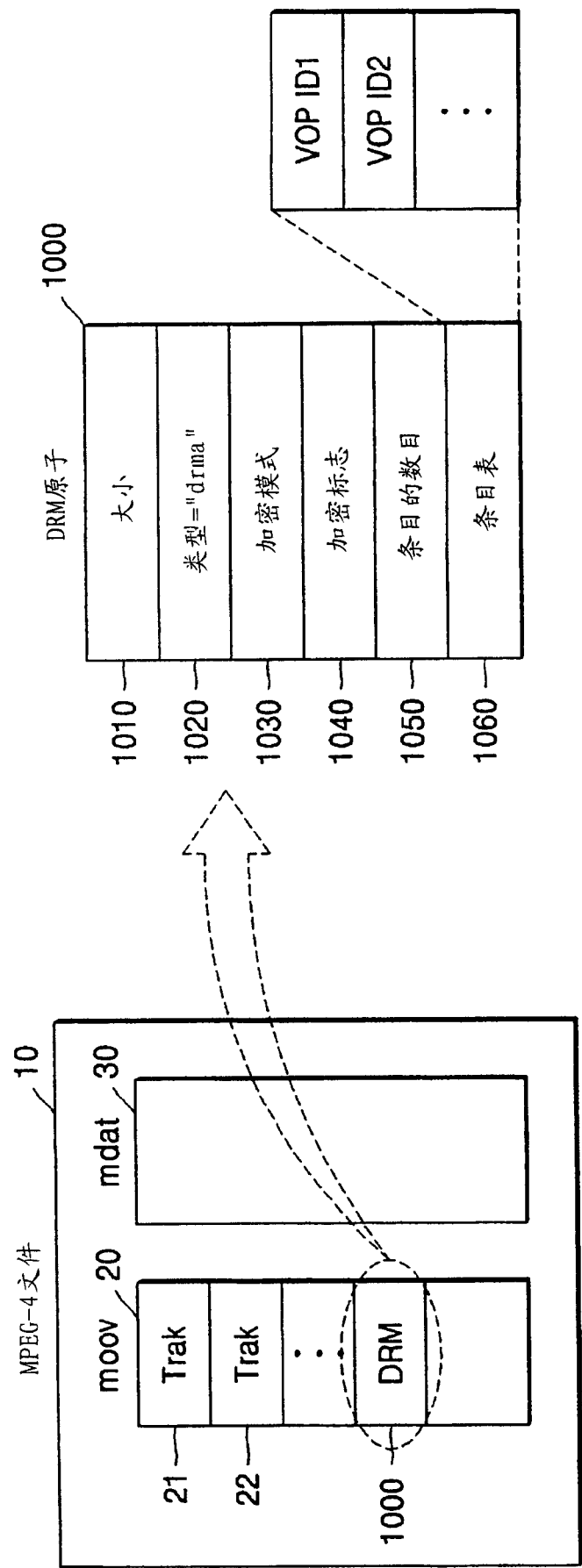


图 10

```
QTAtom firstAtom;  
QTAtomContainer container;  
OSError err;  
err = QTNewAtomContainer (&container);  
if(!err)  
err = QTInsertChild (container, kParentAtomIsContainer,  
                    drma', 1000, 1, 0, nil, &firstAtom);
```

图 11