



[12] 发明专利申请公开说明书

[21] 申请号 02800507.4

[43] 公开日 2003 年 11 月 19 日

[11] 公开号 CN 1457600A

[22] 申请日 2002.2.26 [21] 申请号 02800507.4

[30] 优先权

[32] 2001.3.2 [33] JP [31] 58236/2001

[32] 2001.12.14 [33] JP [31] 381406/2001

[86] 国际申请 PCT/JP02/01698 2002.2.26

[87] 国际公布 WO02/071752 日 2002.9.12

[85] 进入国家阶段日期 2002.11.4

[71] 申请人 松下电器产业株式会社

地址 日本大阪府

[72] 发明人 申省梅 吉 明 妹尾孝宪

小暮拓世

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 汪惠民

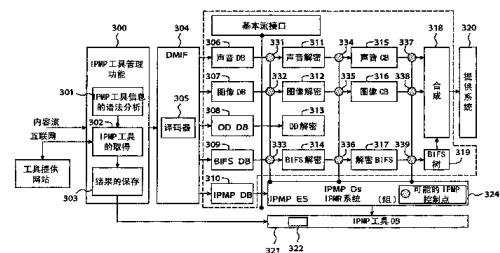
权利要求书 3 页 说明书 15 页 附图 7 页

[54] 发明名称 内容的传递及保护的方法及装置

[57] 摘要

一种内容的传递及保护的进行方法及装置。

通过导入位于内容数据流的先头的 IPMP 工具信息和作为事前处理模块的位置于内容解码器前方的 IPMP 工具管理功能部，根据 IPMP 工具信息取得 IPMP 工具，可确切地定义适用于 MPEG - n IPMP (知识产权管理及保护) 系统的可实现的标准。为了对于不同的 IPMP 系统提高其安全性及终端的兼容性，在提出 2 层构造的同时，定义用户认证输出。通过在 IPMP 工具的取得中对不同的特性进行定义，简化了终端中的复杂程度。



1. 一种从提供者传递内容的传递方法，其特征在于包括：
 - 5 对内容进行编码并转换成内容数据流的步骤；
使用数据加密工具对所述编码化的内容数据流进行加密的步骤；
生成对应所述内容的内容 ID 的步骤；
生成包含为了解读通过所述数据加密工具加密的内容数据流所需要的必要信息的 IPMP（知识产权管理保护）工具信息的步骤；
10 生成表示存在 IPMP 工具信息的 IPMP 工具信息标志的步骤；
通过所述 IPMP 工具信息标志和与其相连的所述 IPMP 工具信息、所述内容 ID、及被加密的内容数据流构成数据流的步骤。
 2. 根据权利要求 1 所述的方法，其特征在于：所述数据加密工具根据内容单位的不同而不同。
15 3. 根据权利要求 1 所述的方法，其特征在于：所述数据加密工具通过加密的密钥进行加密。
4. 根据权利要求 3 所述的方法，其特征在于：对所述加密密钥通过许可证密钥进行进一步的加密。
5. 根据权利要求 1 所述的方法，其特征在于：所述 IPMP 工具信息
20 的生成步骤包括：
对在各个内容分配特定所使用的加密工具的 IPMP 工具 ID 的步骤；
分配表示所述加密工具所存在的位置的种类的位置类型 ID 的步骤；
分配所述加密工具所存在的具体位置的具体位置信息的步骤。
6. 根据权利要求 1 所述的方法，其特征在于：还包括向所述内容嵌
25 入电子水印信息的步骤。
7. 根据权利要求 6 所述的方法，其特征在于：在 IPMP 工具信息中
包含为了读出嵌入在所述内容内的电子水印信息所需要的必要信息。
8. 根据权利要求 1 所述的方法，其特征在于：还包括在其他提供者
传递相同内容的情况下，生成对由其他提供者用其他的数据加密工具对内
30 容数据流进行加密，及解读该加密所需要的必要信息的其他 IPMP 工具信

息的步骤，在数据流中包含所述 IPMP 工具信息和该其他的 IPMP 工具信息。

9. 一种通过接收从提供者传递来的包含内容的数据流的终端读出内容的方法，其特征在于：包括对数据流进行语法分析的步骤；

5 检测出 IPMP 工具信息标志、内容 ID 及 IPMP 工具信息的步骤；
根据检测出的 IPMP 工具信息取得 IPMP 工具的步骤。

10. 根据权利要求 9 所述的方法，其特征在于：所述 IPMP 工具是用于解读内容的暗号的工具。

11. 根据权利要求 10 所述的方法，其特征在于：所述暗号解读工具
10 根据内容单位的不同而不同。

12. 根据权利要求 10 所述的方法，其特征在于：所述暗号解密工具通过加密密钥进行加密。

13. 根据权利要求 12 所述的方法，其特征在于：所述用于解读加密密钥的解读密钥进一步通过许可证密钥进行加密。

15 14. 根据权利要求 9 所述的方法，其特征在于：取得 IPMP 工具的步骤包括：从 IPMP 工具 ID 中特定用于解读在内容中所使用的暗号的工具的步骤；

从位置类型 ID 中检测出所述暗号解读工具所存在的位置的类型的步骤；

20 从具体位置信息中特定所述暗号解读工具所存在的具体位置并进行存取的步骤。

15. 根据权利要求 14 所述的方法，其特征在于：所述取得 IPMP 工具的步骤中利用包括多个 IPMP 工具 ID 和特定对应于各个 IPMP 工具的暗号解读工具的信息的信息表。

25 16. 根据权利要求 15 所述的方法，其特征在于：所述信息表由提供者和终端的双方保持。

17. 根据权利要求 9 所述的方法，其特征在于：取得所述 IPMP 工具的步骤包括对预先被保持在终端中的 IPMP 工具进行编码的步骤。

30 18. 根据权利要求 9 所述的方法，其特征在于：取得所述 IPMP 工具的步骤包括从规定的工具供给源进行在线下载的步骤。

-
19. 根据权利要求 9 所述的方法，其特征在于：还包括读出嵌入在所述内容内的电子水印信息的步骤。
20. 根据权利要求 19 所述的方法，其特征在于：所述 IPMP 工具是用于解读电子水印信息的工具。
- 5 21. 根据权利要求 9 所述的方法，其特征在于：用于所述 IPMP 工具的通信接口与在终端被要求的接口相匹配。
22. 根据权利要求 1 所述的方法，其特征在于：所述加密步骤对内容数据流进行部分的加密。
23. 一种从提供者传递内容的传递装置，其特征在于：包括对内容
10 进行编码并转换成内容数据流的装置；
使用数据加密工具对所述编码化的内容数据流进行加密的装置；
生成对应所述内容的内容 ID 的装置；
生成包含为了解读通过所述数据加密工具加密的内容数据流所需要的必要信息的 IPMP（知识产权管理保护）工具信息的装置；
15 生成表示存在 IPMP 工具信息的 IPMP 工具信息标志的装置；
通过所述 IPMP 工具信息标志和与其相连的所述 IPMP 工具信息、所述内容 ID、及被加密的内容数据流构成数据流的装置。
24. 一种接收从提供者传递的包含内容的数据流并读出内容的终端装置，其特征在于：包括对数据流进行语法分析的装置；
20 检测出 IPMP 工具信息标志、内容 ID 及 IPMP 工具信息的装置；和根据检测出的 IPMP 工具信息取得 IPMP 工具的装置。

内容的传递及保护的方法及装置

5

技术领域

本发明涉及内容的传递及保护，特别是关于被保护的内容可被不同的 IPMP 系统利用、而且同一内容可被不同的 IPMP 系统保护的应用程序。

10

背景技术

随着通信技术的进步，使人们能够在任意方便的时间把多媒体数据或内容传递到任意所希望的地点，并且对内容传递的要求越来越高。使用户在满足于其便利性和灵活性的同时，可简单且高效率地享受该内容的信息。而另一方面，虽然内容的所有者也希望满足顾客的要求，然而同时又担心自己的所有物被非法使用。因此，必须要解决好这 2 方面的矛盾。

现在，已开发出数据加密、电子水印、密码等的多种用于保护内容的保护技术。可以把这些安装在大多数的内容传递应用程序中。为了使内容在受到保护的状态下进行传递，可以使不同的系统采用不同种类的机制和保护技术。在这种情况下，全部的终端和内容的使用装置只能再生或利用由同一内容提供者所提供的内容。即，如果更换了终端或装置则不能再生不同的内容。

在 MPEG 标准化组织中，正在进行包含终端的 IPMP 系统的标准化工作。全部的终端无论使用什么样的 IPMP 工具，都可再生被按照同一 IPMP 标准加密及保护的被保护的内容。这样的终端由进行声音和图像解码的内容解码器构成，并且，在能够对内容进行加密及再生之前，终端能够解除处于被保护状态的内容的保护。因此，需要获知保护信息，即 IPMP 工具信息，并能够在终端中加以利用。

30 另一方面，为了具有使销售商能够选择适合自己的 IPMP 系统的工

具的灵活性，不能在事前把 IPMP 工具固定在特定的工具中。这样，为了同时提高灵活性和安全性，必须要定义出某种标准的方法和接口。

根据以往技术的用户认证和 IPMP 工具的取得，例如，如 MPEG-2 或 MPEG-4 那样，无论是否使用相同的解码，其工具的安装对应每个不同的销售商具有很大的差别。在这种情况下，对于由不同的内容提供者所提供的不同的内容很难在同一终端中实现再生。换言之，被保护的同一内容不能在不同的 IPMP 系统下实现再生。

发明内容

10 (本发明要解决的技术问题)

本发明为了能够在不同的 IPMP 系统中利用被保护的同一内容，定义具有相同结构的 IPMP 系统。提供一种使安装 IPMP 系统的用户能够牢固地构成从编码到通道传递、最后到终端的整体系统的标准方法。

(解决方案)

15 首先，把 IPMP 工具信息置于内容 ID 以外的实际的内容数据流的先头位置，定义为包含以下项目的 1 个特定数据包。

- 为了保护内容而使用的 IPMP 工具的类型。
- IPMP 工具的位置类型。
- 能够取得 IPMP 工具的位置。

20 把 IPMP 工具信息标志作为标题配置在所述数据包的先头位置。IPMP 工具管理功能位于内容解码器的前方，被设计成为能够对通过内容数据流输送来的 IPMP 工具信息进行语法分析、并且取得解除内容数据流的保护的 IPMP 工具的 1 个模块。

25 为了提高安全性及终端的兼容性并且为了对任意不同的用户认证方法确定输出要件，导入了 2 层安全构造。

IPMP 工具 ID 由规定的信息表进行定义，该信息表可在事前进行编码或者被下载到终端内。为了对同一 IPMP 工具使用同一 IPMP 工具 ID，必须使内容的提供者侧和终端侧参照同一信息表。

30 终端能够通过被认为是标准 IPMP 工具的某种现存的 IPMP 工具进行事前的编码，而且在终端中，在其能力允许的情况下，根据由内容数

据流传送来的 IPMP 工具信息，能够下载被许可登录的 IPMP 工具。加密密钥在 2 层安全构造的基础上进一步被加密，并能够被插入到 IPMP 数据字段内，与内容数据流一同传递到终端。在内容提供者一侧，内容通过使用 MPEG-2 或 MPEG-4 等的现有的编码技术被进行编码，通过使用 DES 或 AES 等的现有的 IPMP 工具被加密。也可以在编码之前在内容中嵌入电子水印。

同时，内容 ID 是根据内容著作权信息、内容作成信息等而生成。IPMP 工具信息是根据为了保护内容而使用的 IPMP 工具信息而生成。IPMP 工具信息包含 IPMP 工具 ID、位置类型及 IPMP 工具的位置。IPMP 工具信息标志被置于前头位置，在其后连接 IPMP 工具信息、内容 ID 及内容。

虽然任何终端都能够取得内容或者访问内容，但是在没有正当的使用许可和与其对应的或者是 IPMP 工具的情况下不能进行再生。在终端侧，内容数据流是经过 IPMP 工具管理功能模块被传送过来，在进行了 IPMP 工具的验证之后在本地或远程取得 IPMP 工具。被取得的 IPMP 工具在此时可以在终端中进行使用。

内容数据流通过内容解码器，然后 IPMP 数据解码模块启动用户认证模块，通过提供用户的终端 ID、内容 ID 及 IPMP 工具 ID，向内容提供者传递请求。在首尾完好地进行完用户认证后，向终端传递许可证。最后，解读被加密的密钥，并解读被加密的内容，使内容被解密，从而能够在终端中进行再生。

（相对以往技术的有益效果）

通过导入把 IPMP 工具信息包配置在内容数据流的前头，而且对 IPMP 工具信息进行语法分析，取得 IPMP 工具的 IPMP 工具管理功能模块，实现了把被保护的同一内容在不同种类的 IPMP 系统中的再生。

2 层构造不仅提高了安全性，而且固定了不同用户认证方法的输出构造，提高了终端之间的兼容性。在这样的构造中，用户认证可以根据面向不同的提供者以不同的方法进行安装，增加了相互的使用性。通过针对用于获得 IPMP 工具的终端的复杂程度和灵活性而定义不同的特性，从而可使不同的终端能够利用同一标准，扩大了利用范围。

附图说明

图 1 是表示与本发明相关的进行内容传递及保护的以往的 IPMP 系统的图。

图 2 是表示置于内容数据流前端部的 IPMP 工具信息包的图。

图 3 是表示 IPMP 工具管理功能配合 MPEG-4 IPMP 系统进行工作的状态的图。

图 4 是表示 IPMP 工具管理功能配合 MPEG-2 系统进行工作的状态的图。

图 5 是表示用户认证模块配合 MPEG-4 IPMP 系统及 IPMP 工具管理功能模块进行工作的状态的图。

图 6 是表示用户认证模块配合 MPEG-2 系统及 IPMP 工具管理功能模块进行工作的状态的图。

图 7 是表示以 8 个方框构成的内容 ID 格式的构成图。

图 8 是表示认证结果的格式构成图。

15

具体实施方式

图 1 表示涉及本发明的 IPMP 系统。单元 10 的内容所有者通过单元 11、15 及 19 的不同的内容提供者 A、B、及 C 提供内容。3 组 IPMP 系统分别为不同的 IPMP 系统。关于 IPMP 工具的取得、验证，是使用从共用的 IPMP 工具表中选择出的共用的或不同的用户认证工具等进行。单元 12、16 及 110 可以是不同的用户认证方法，也可以是相同的用户认证方法。把 IPMP 工具的取得方法在单元 13、17 及 111 中表示，这些是使用从共用的 IPMP 工具表中选择出来 IPMP 工具。

25

因此，即使内容的编码或内容利用终端如单元 14、18 及 112 所示的那样相互不同，也可以从共用的表中取得 IPMP 工具。即使内容提供者 B 传递的是被保护的内容，在终端 A 中，也可以从共用的表中取得内容提供者 B 所使用的 IPMP 工具，并可通过取得的 IPMP 工具进行再生。在本实施例中，所谓工具是指解读被加密的内容和读出预先嵌入在内容中的电子水印信息的工具，但也可以包括认证读取工具和收费设定工具等。即以往的技术是，由内容提供者 B 传递的被保护的内容只能够在与

内容提供者 B 签约的终端 B 上进行再生，而在未与内容提供者 B 签约的终端 A、C 中则不能进行再生。但是，在本发明中，由内容提供者 B 传递的被保护的内容不仅能够在与内容提供者 B 签约的终端 B 上，而且还能在未与内容提供者 B 签约的终端 A、C 上进行再生。

5 为了提供这样的系统，必须要使用如下的从提供者传递内容的装置。

即：把内容通过编码转换为内容数据流的装置；

使用数据加密工具对编码化的内容数据流进行加密的装置；

生成与内容对应的内容 ID 的装置；

10 生成包含在使用数据加密工具对加密的内容数据流进行解密时所必要的信息的 IPMP（知识产权保护）工具信息的装置；

生成表示存在 IPMP 工具信息的 IPMP 工具信息标志的装置；

通过 IPMP 工具信息标志和与其连接的 IPMP 工具信息、内容 ID 及被加密的内容数据流构筑数据流的装置。

另外，为了接收从提供者传递的包含内容的数据流、并读出内容，
15 需要具有如下构成的终端装置：

数据流的语法分析装置；

检测出 IPMP 工具信息标志、内容 ID 及 IPMP 工具信息的装置；

根据检测出的 IPMP 工具信息取得 IPMP 工具的装置。

下面，对这些装置进行说明。

20 图 2 中的上边部分表示通过图 1 中的 P 点的数据流的构成，表示由提供者 A 所准备的数据流。首先，有信息数据的包标题 201，其后连接 IPMP 工具信息包 202。还有内容的包标题 203，其后连接内容包 204。在包标题 201 或 IPMP 工具信息包 202 中，包含 IPMP 工具信息标志，用于表示存在 IPMP 工具信息。也可以把 IPMP 工具信息标志包含在数据流内的其他位置中。例如，也可以包含在方框 203 或 204 的任意位置中。在 IPMP 工具信息包 202 中，内容 ID 与内容 ID 用 IPMP 工具信息形成信息对，并存在一个或多个信息对。在这里，表示有 2 个信息对。在第 1 个信息对中包含内容 ID1 205 和内容 ID1 用 IPMP 工具信息 206，在第 2 信息对中包含内容 ID2 207 和内容 ID2 用 IPMP 工具信息 208。内容包 204 的内
25 容 1 包含对应第 1 信息对中的内容 ID1 的内容（例如，音乐 1），内容 2

包含对应第 2 信息对中的内容 ID2 的内容（例如，音乐 2）。对于内容 1 和内容 2 也可以使用不同的数据加密工具。

图 2 中的中间部分表示详细的内容 ID1 用的 IPMP 信息 206。在这里包含多个提供者的 IPMP 工具的信息。在此所示的例中，包含内容 5 提供者 A 的 IPMP 工具信息 211 和内容提供者 B 的 IPMP 工具信息 212。不言而喻，也能够包含内容提供者 C、内容提供者 D 的 IPMP 工具信息。作为内容提供者 A 的 IPMP 工具信息，包含有 IPMP 工具 ID 213、IPMP 工具名 214、IPMP 工具位置识别因子 215。IPMP 工具 ID 213 例如是用于解读被加密的数据的工具，即被特定为解密工具。IPMP 工具名 214 用于表示解密工具的名称。IPMP 工具位置识别因子 215 表示能够取得解密 10 工具的位置（例如是互联网的主页）。也可以省略 IPMP 工具名 214。由于在终端用户的各个终端中，预先记录有将在后面说明的表 1，所以，只要知道了 IPMP 工具 ID 213，便可从表 1 中取得 IPMP 工具名 214。

IPMP 工具 ID 213，如表 1 中所示，用 8 位构成的 ID 进行特定，并 15 且在全部的终端机中通用。作为 IPMP 工具位置识别因子 215，如同下面说明的那样，例如写入有主页的地址。

图 2 中的下边部分表示 IPMP 工具位置识别因子 215 的具体内容。在 IPMP 工具位置识别因子 215 中包含可获得由 IPMP 工具名 214 特定的工具程序的信息，具体的是，包含位置类型 219 和详细位置 220。作 20 为位置类型 219，例如表示为互联网，作为具体位置 220，例如表示为主页的地址。

图 3 表示终端 A 的构成。终端 A 具有接收外部输入信号的 IPMP 工具管理功能部 300。在 IPMP 工具管理功能部 300 中，包括 IPMP 工具信息语法分析部 301、IPMP 工具取得部 302 和结果保存部 303。结果保存部 25 303 与 IPMP 工具数据库 321 连接。在 IPMP 工具数据库 321 中存储有表 1 的数据和取得的 IPMP 工具软件。另外，在 IPMP 工具数据库 321 中还包含用于解读密钥的模块 322。IPMP 工具管理功能部 300 与译码器接口 304 连接。在译码器接口 304 中包括译码器 305。

在译码器接口 304 之后包括声音解码缓冲器 306、图像解码缓冲器 307、目标描述符解码缓冲器 308、场景的二进制数据 (binary data for

scene) (BIFS) 解码缓冲器 309 和 IPMP 解码缓冲器 310。场景的二进制数据包含表示被分段化的场景的配置位置的数据。306、307、309 的输出的声音信号、图像信号和 BIFS 信号还保持着被加密的状态。

声音解码缓冲器 306 通过控制点 331 与声音解密器连接，图像解码缓冲器 307 通过控制点 332 与图像解密器 312 连接，目标描述符解码缓冲器 308 直接与目标描述符解密器 313 连接，场景二进制数据(binary data for scene) (BIFS) 解码缓冲器 309 通过控制点 333 与 BIFS 解密器 314 连接。另外，IPMP 解码缓冲器 310 与 IPMP 系统 324 连接。在图中，由包括多点的圆圈所表示的控制点 331~339 为 IPMP 控制点，对于通过控制点的数据，使用 IPMP 系统 324 中的工具施加必要的处理（伪随机序列译码、电子水印的检测、复制防护等）。

在本实施例中，在控制点 331、332、333 进行伪随机序列译码。进行伪随机序列译码所必要的工具（软件）是从 IPMP 系统 324（包含 IPMP 工具数据库 321）中取得。

声音解密器 311 通过控制点 334 与声音合成缓冲器 315 连接，图像解密器 312 通过控制点 335 与图像合成缓冲器 316 连接，BIFS 解密器 314 通过控制点 336 与解密器 BIFS317 连接。

在本实施例中，在控制点 334、335、336 进行电子水印的检测。进行电子水印检测所必要的工具（软件）是从 IPMP 系统 324（包含 IPMP 工具数据库 321）中取得。

声音解合成缓冲器 315 通过控制点 337 与合成器 318 连接，图像合成缓冲器 316 通过控制点 338 与合成器 318 连接，BIFS 解密器 317 通过控制点 339 和 BIFS 树 319 与合成器 318 连接。合成器 318 进一步与作为输出的租赁系统 320 连接。

在本实施例中，在控制点 337、338、339 还进行其他的电子水印的检测和复制防护的处理。进行电子水印检测和复制防护处理所必要的工具（软件）是从 IPMP 系统 324（包含 IPMP 工具数据库 321）中取得。

图 2 中所示的内容数据流，例如是 MPEG4 的数据流，被输入到 IPMP 工具管理功能部 300 中，通过检测包标题 201 而检测出内容数据包 202，然后把其送到 IPMP 工具信息语法分析部 301。另外，通过包标题 203 而

检测出的内容数据包 204 被送到下一段的译码器接口 304。被检测出的 IPMP 工具信息包 202 通过 IPMP 信息语法分析部 301 被解读，从而确定出作为该数据流传递源的提供者。

在 IPMP 工具取得部 302 中，如果提供者为提供者 A，则读出提供者 A 所使用的 IPMP 工具 A 的信息 211。如果提供者为提供者 B，则读出提供者 B 所使用的 IPMP 工具 B 的信息 212。被读出的结果被暂时保存在结果保存部 303，并且被保存到 IPMP 工具数据库 321 中。

另外，被传递到译码器接口 304 的内容数据包 204 被译码成声音信号、图像信号、OD 信号、BIFS 信号，并且被送到各自的处理电路。然后进行上述的处理。

下面，把本发明分成 4 个部分，对各部分进行详细的说明。

IPMP 工具信息和 IPMP 工具管理功能

下面，对 IPMP 工具信息和 IPMP 工具管理功能进行说明。对 IPMP 工具信息和 IPMP 工具管理功能的定义如下：关于 IPMP 的概念，是把 IPMP 信息定义为“为了使规定的 IPMP 工具对被保护的规定的内容进行正确处理所必要的信息”。把 IPMP 工具定义为“所谓 IPMP 工具，是指以规定的方法执行认证、加密、电子水印等的 IPMP 功能操作的模块。IPMP 工具能够执行 1 个以上的 IPMP 功能操作。也可以作为调整其他 IPMP 工具的 IPMP 工具。”。

在本发明中提出了导入 IPMP 工具信息的定义的方案。即，“所谓 IPMP 工具信息，是指由 IPMP 工具管理功能对 IPMP 工具进行识别、并取得 IPMP 工具所必要的信息。其包括 IPMP 工具的唯一识别因子、IPMP 工具的位置识别因子及 IPMP 工具与内容 ID 之间的相关信息。IPMP 工具应存在于内容数据流全体的最初的数据包内。”。

另外，提出了 IPMP 工具管理功能的方案。即，“所谓 IPMP 工具管理功能，是指仅以通过对 IPMP 工具信息进行处理，而取得对内容数据流全体的利用所必要的 IPMP 工具为目的的信息体。IPMP 工具管理功能部应置于内容解码器之前。”。

IPMP 信息

如在 IPMP 工具信息中被定义的那样，应把其作为内容数据流全体

的最初的数据包配置位置。该数据包的具体构造在图 2 中给出了最简明的图示。IPMP 工具信息包应包括对别保护的内容进行利用所必要的全部的 IPMP 工具信息。当内容中包含多种的内容时，例如在内容的第 1 部分是由内容提供者 A 提供的、第 2 部分是由内容提供者 B 提供来的情况下，与不同的 IPMP 工具建立相关关系的信息应依照各自的内容 ID 形成编组化。

把内容 ID 的格式 (cIDf) 定义为如图 7 所示那样的由 8 个方框部分构成的内容 ID 格式。在图 7 中，例如“内容属性”方框包含作者和内容的信息，在“著作权属性”方框中包含谁、保有形式等的有关著作权背景的具体事项。内容的各个 ID 应当把例如内容所有者 ID、内容著作权保有者 ID 及记录装置 ID 分别分配在所指定的属性方框中。在作为工作而进行的内容记录的情况下，能够使摄影者对这样复杂的内容 ID 编码体系进行合理地组合和使用。

因此，各个内容 ID 用的 IPMP 工具的信息应由各个 IPMP 工具信息构成，而各个 IPMP 工具信息的顺序并不重要。

各个 IPMP 工具信息还应由 2 个主要部，即 IPMP 工具 ID 和 IPMP 工具位置识别因子构成。IPMP 工具 ID 能够以明确的方法进行工具的识别，并且能够在终端中进行定义或进行事前的保存或下载到终端中。在表 1 中表示一例作成的信息表，序列地表示出可利用的 IPMP 工具 ID。

表 1 可利用的 IPMP 工具 ID

工具功能	IPMP 工具 ID	IPMP 工具名	备注
解读工具	000 00000	DESDecrypt	用 5 位能够表示 32 个不同的工具
	000 00001	AESDecrypt	
	000 00010	SC2000Decrypt	
	000 00011	CamelliaDecrypt	
	000 00100	Xxxx	
	000 00101	Xxxx	
	000 00110	Xxxx	
	000 00111	Xxxx	
	000 01000	Xxxx	
	000 0xxxx	Xxxx	
	000 0xxxx	Xxxx	
电子水印的嵌入处 理	000 10000	预约	作为将来追加预 定许可登录完成 工具的备用
	000 10001	预约	
	001 00000	空间区域	对卓越的工具进 行必要的集中分 类
	001 00001	频率区域	
	001 00010	Xxxxx	
	001 00011	Xxxxx	
	001 00100	Xxxxx	
	001 0xxxx		作为将来追加预 定许可登录完成 工具的备用

5 另外，前面的 3 位可用于表示加密和电子水印等的 IPMP 工具的分类。

IPMP 工具名是为了由 IPMP 工具管理功能部保存所 IPMP 工具而使用的名称，可从载入的表中取得。位置识别因子表示传递信息体，相对 1 个 IPMP 工具可以有 1 个以上的位置识别因子。IPMP 工具管理功能部使用各个识别因子来取得工具。如果能够清楚地识别 IPMP 工具 A 的最初的位置识别因子的首尾，则跳过下一个位置识别因子。如果不能，则接下来识别第 2 个位置识别因子。

实例：

本地：终端系统的内部或周边。

外部：被指定的终端系统的外部（http:，ftp:）

IPMP 工具识别因子由位置类型和具体位置这 2 个部分构成。位置类型为以下的任意一种。位置类型与具体位置的对应关系由以下的表 2 表示。

表 2 位置的类型及具体位置

位置类型	具体位置
本地	N/A
周边	N/A
能够进行远程下载	网站（http、ftp...）
不能进行远程下载	Java servlet 的远程位置等
内容内数据流	在此部分中包含 IPMP 工具本身
...	...

15

其中，例如本地是表示位于接收终端内。周边是表示在包括接收终端的在主网络中的某个机器内。能够进行远程下载是表示能够从网站上下载解读软件。不能进行远程下载是表示分散处理，例如是表示把被加密的数据传递到特定的网站，在那里进行解密处理，然后返回解读数据。

20 内容内的数据流是表示解读数据存在于数据流内。

IPMP 工具管理功能

IPMP 工具管理功能应优先于系统解码执行。该功能对输入内容数据流的最初的数据包中的 IPMP 工具信息进行语法分析，进行在本章节中

详细叙述的必要的动作。在图 3 中, 表示适合于 MPEG4-IPMP 系统的 IPMP 工具管理功能的情形。图 3 所示的 IPMP 工具 DB 是保存了全部的 IPMP 工具取得结果的数据库。

IPMP 工具管理功能进行以下 4 种动作。

5 步骤 1: 对存在于内容数据流的最初数据包中的 IPMP 工具信息进行语法分析。

步骤 2: 取得由 IPMP 工具信息所指定的必要的 IPMP 工具。

步骤 3: 把取得结果保存在 IPMP 系统在以后进行参照的 IPMP 工具 DB 中。

10 步骤 4: 使输入数据包只过度到 Demux (译码器) 层。(透过性地)

IPMP 工具管理功能当接收到内容数据流后, 立即在全部内容数据流中查找出作为唯一的数据包标题的 IPMP 工具信息包标志, 找出最初的内容数据流。在未找到 IPMP 工具信息包的标志的情况下, 跳至步骤 4, 使全部的数据只过度到 DeMux 层, 在不是未找到的情况下, 执行步骤 2。

15 在第 2 步骤中, IPMP 工具管理功能参照位置类型识别因子和具体位置识别因子进行各个 IPMP 工具的获取。在具有多个与 1 个 IPMP 工具相关联的位置识别因子的情况下, 应首先使用位置识别因子 1 取得 IPMP 工具, 在最初的取得失败时, 再使用位置识别因子 2 进行获取。在每次取得成功时, 必须将取得结果保存在 IPMP 工具 DB 中 (步骤 3),
20 当全部的 IPMP 工具被首尾完好地取得后, 返回到步骤 2。

在位置识别因子类型为“本地”的情况下, IPMP 工具管理功能部根据被指定的 IPMP 工具名或 IPMP 工具 ID 在当前的终端内进行检索, 如果检索到, 则将结果保存到 IPMP 工具 DB 中。在位置识别因子类型为“周边机器”的情况下, IPMP 工具管理功能部根据被指定的 IPMP 工具名或 IPMP 工具 ID 对全部的周边机器进行检索, 如果检索到, 则将结果保存到 IPMP 工具 DB 中。在位置识别因子类型为“能够进行远程下载”的情况下, IPMP 工具管理功能连接到指定的远程地址, 根据指定的 IPMP 工具名或 IPMP 工具 ID 下载 IPMP 工具, 如果下载成功, 则将结果保存在 IPMP 工具 DB 中。

30 在位置识别因子类型为“不能进行远程下载”的情况下, IPMP 工

具管理功能只把远程地址保存在 IPMP 工具 DB 中。在位置识别因子类型为“内部内容数据流”的情况下，IPMP 工具管理功能保存二进制数据流（例如，保存在文件中），并对被保存的信息体分配 IPMP 工具名。在步骤 3 中，取得的结果被保存在 IPMP 工具 DB 中。在 IPMP 工具 DB 中存在 4 个信息体，用表 3 表示其实例。

表 3 IPMP 工具 DB 的 4 个信息体

内容 ID	IPMP 工具 ID	IPMP 工具名	IPMP 工具位置
0000000011000100	00101001	DESDecrypt.dll	C:\ipmptools\DesDecrypt.dll
0000000011000100	00100110	硬密钥	LPT1
0000000011000100	00100010	JAVA servlet1	10.2.3.1/servlet1

IPMP 系统（组）在以后需要生成特定的 IPMP 工具的情况下，参照该 IPMP 工具 DB，使用工具 ID、工具名或当前的内容 ID，查找特定的 IPMP 工具的位置（有必要）。包括 IPMP 工具管理功能和 IPMP 工具 DB 的本结构可适用于任意的 MPEG 系统，下面参照如图 4，对适用在 MPEG2-IPMP 系统中的 IPMP 工具管理功能情形进行说明。在图 4 中，被虚线所包围的部分与图 3 中的被虚线包围的部分相对应，进行了简略图示。

用户认证的必要的输出

虽然还不能推出用户认证方法的标准化，但有必要构成认证结果的标准化。为了公开正当地利用被保护的内容，认证结果必须要通过 MPEG-nIPMP 系统。因此，提出了应对认证结果设定基准，如图 8 所示，必须至少由 3 个字段构成。

正当性（合法性）表示用户（终端）是否是正规的用户，其结果用真或伪表示。利用规则应包括关于用户的内容访问权（例如是只许可 1 次再生还是许可多次再生）的具体信息。下面对许可证进行说明。内容被搅乱，如在 IPMP 数据中所示的那样，搅乱密钥被传送到内容数据流内（例如，MPEG4-IPMP 的 IPMP ES）的技术是公知技术。为了提高安全性，通过对搅乱密钥进行进一步加密可实现双层的安全性。把为了

解读被搅乱的内容用的搅乱密钥而使用的第 2 层的密钥称为“许可证”。

“许可证”是为了利用被保护的内容的最低条件。许可证应在进行非标准用户认证处理当中通过安全的通道从许可证服务器取得。

双层安全的本提案是基于在 La Baule 会议上“关于 IPMP 系统的更新可能性的提案”所提出的以前的 M6473 号提案，其中，为了提高安全性，对于用户认证，在该双层构造的上部进一步导入了 1 个信号层。无论 IPMP 终端使用任何种类的用户认证方法，上述的认证结果必须在用户认证的期间被确定并且通知。如图 5 所示，与 MPEG-4 IPMP 系统配合动作的用户认证模块在进行了用户认证之后，向内容代理提出向用户发行许可证的要求。如图 6 所示，可实现适用于 MPEG-nIPMP 的由同一双层安全构成的解决手段。

在图 5 中，解读软件是通过互联网由 IPMP 工具取得部 302 取得，并且在暂时保存在结果保存部 303 中之后，被记录在 IPMP 工具数据库 321 中。解读软件不能直接用于执行，为了打开解读软件必须要有解读密钥。该用于打开解读软件的解读密钥在加密的状态下，由 IPMP 工具信息语法分析部 301 从内容数据流中检测出来。被加密的解读密钥通过译码器 304、IPMP 解码缓冲器 310 被送到 IPMP 系统 324 中。另一方面，许可证密钥通过互联网从许可证服务器 501 被送来。许可证密钥在非标准用户认证部 502 进行完用户认证后，被送至 IPMP 系统 324。在 IPMP 系统 324 中设有 IPMP 解码模块 503。IPMP 解码模块 503 使用许可证密钥对加密的解读密钥进行解读，并生成解读密钥。使用该解读密钥可执行上述的解读软件。

IPMP 系统能够实现的特性

由于应用程序、终端或提供方的不同，对 IPMP 系统的要求也不同，所以难于对其全部用 1 个标准统一。这个问题基本上是由于 IPMP 工具已装入或是能够被下载所致。关于硬件的实际安装，虽然主机一般能够下载特定的工具，但大多数的工具还是被预装，或者是被嵌入到内部。关于移动或便携终端，为了简化安装，也需要完成编码的 IPMP 工具。PC 应用程序具有非常好的兼容性，所以可使用能够下载的或完成编码的工具。

如表 4 所示，只要能够指定兼容以复杂程度低的便携形终端、复杂程度高的主机终端及灵活性好的 PC 终端这 3 种为代表的终端的 3 种概要，则在安装任意的 IPMP 系统的终端中，IPMP 工具都可得到最适合的利用。

5

表 4 不同终端用的 3 种概要

IPMP 工具的取得手段	便携形终端	主机终端	PC 终端
	<u>简单 概要</u>	<u>中级 概要</u>	<u>高级 概要</u>
完成编码	Yes	Yes	Yes
能够下载	No (在一般情况下)	Yes (在某些情况下)	Yes

当工具在终端内已完成编码的情况下，为了使制造者能够在终端中进行安装，必须要定义作为 IPMP 工具的标准而推荐/固定的种类。在本 10 发明中，导入这样的项目具有以下所述的利点。即，IPMP 工具信息的定义明确地表示出了应把位置识别因子等的 IPMP 工具相关信息保存在何处、如何保存的信息。

通过导入 IPMP 工具管理功能及 IPMP 工具信息，解决了在使用内容的过程中，在需要取得新的 IPMP 工具的情况下，发生不可预测的延迟的问题。如图 3 及图 5 所示，在当前或是在内容数据流全体所必要的各种 IPMP 工具被进行译码处理之前被取得并被正确地保存。而且，通过进行这些处理，能够系统地且简单地进行 IPMP 的安装。通过导入 IPMP 工具管理功能及 IPMP 工具信息，还能够满足 IPMP 的要求，而且还能够如图 4 所示地实现适用于 MPEG-n 的功能。

20 用于用户认证的方法即使是原来的非标准的方法，在本发明中也可以对认证结果进行明确的定义。并且为了提高安全性还提出了 IPMP 用的 2 层安全保护的解决方案。如图 6 所示，所提出的解决方案可适用于 MPEG-n IPMP 系统中。而且通过定义 3 种可能的终端类型用的 3 种特性，可对 IPMP 终端进行明确的分类，从而可确信为 IPMP 的扩张标准化铺 25 平了道路。

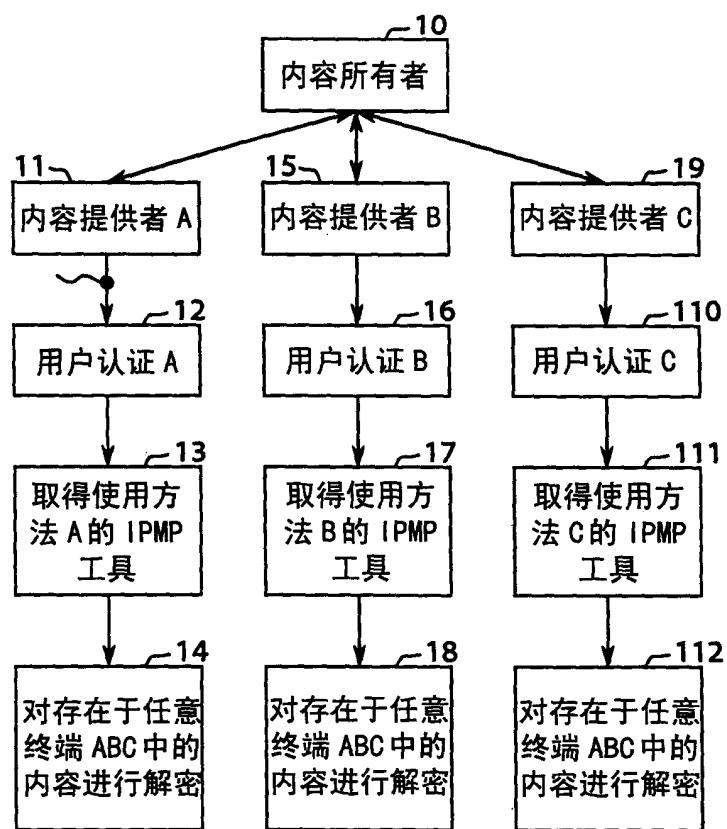


图 1

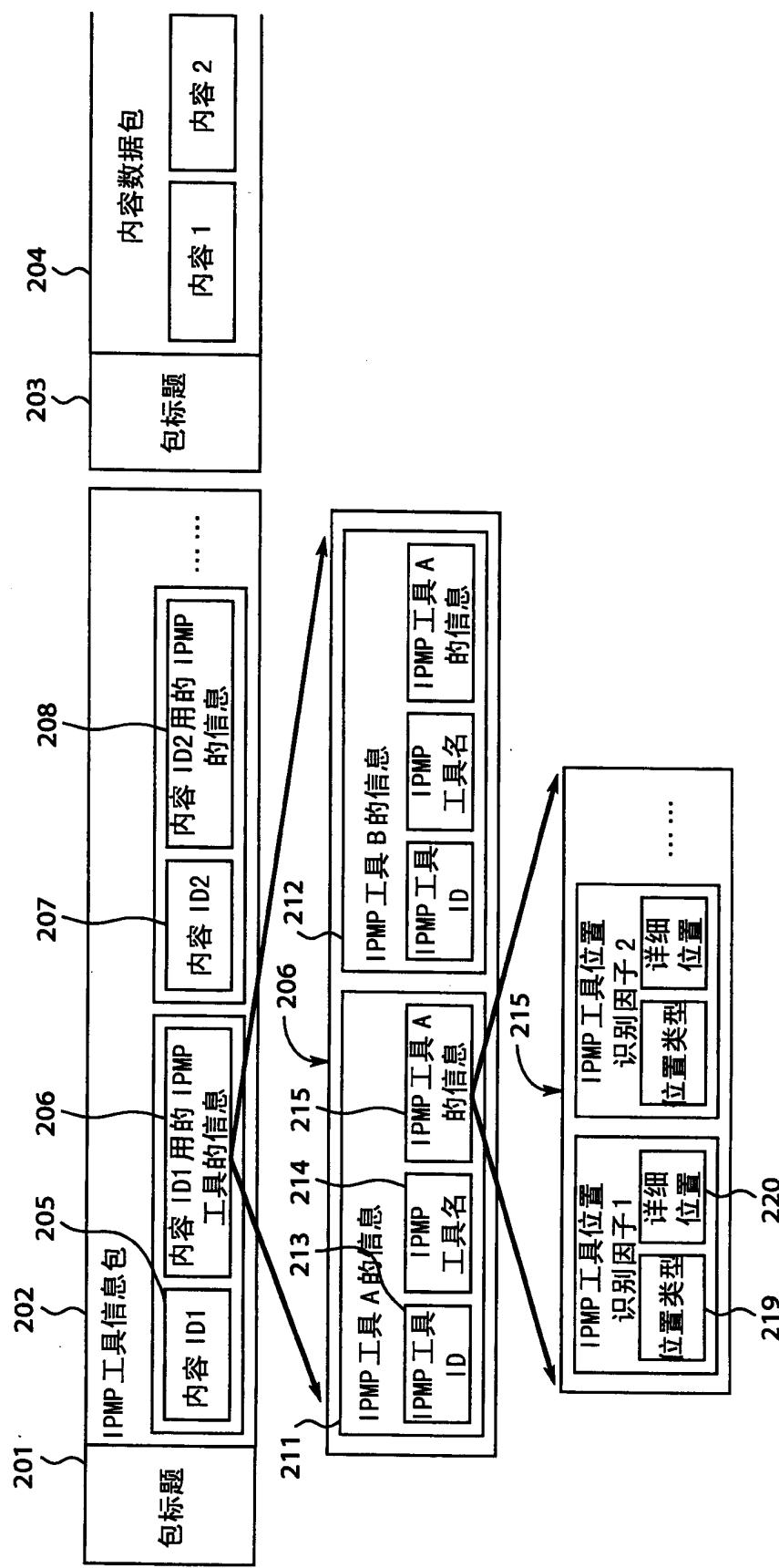


图 2

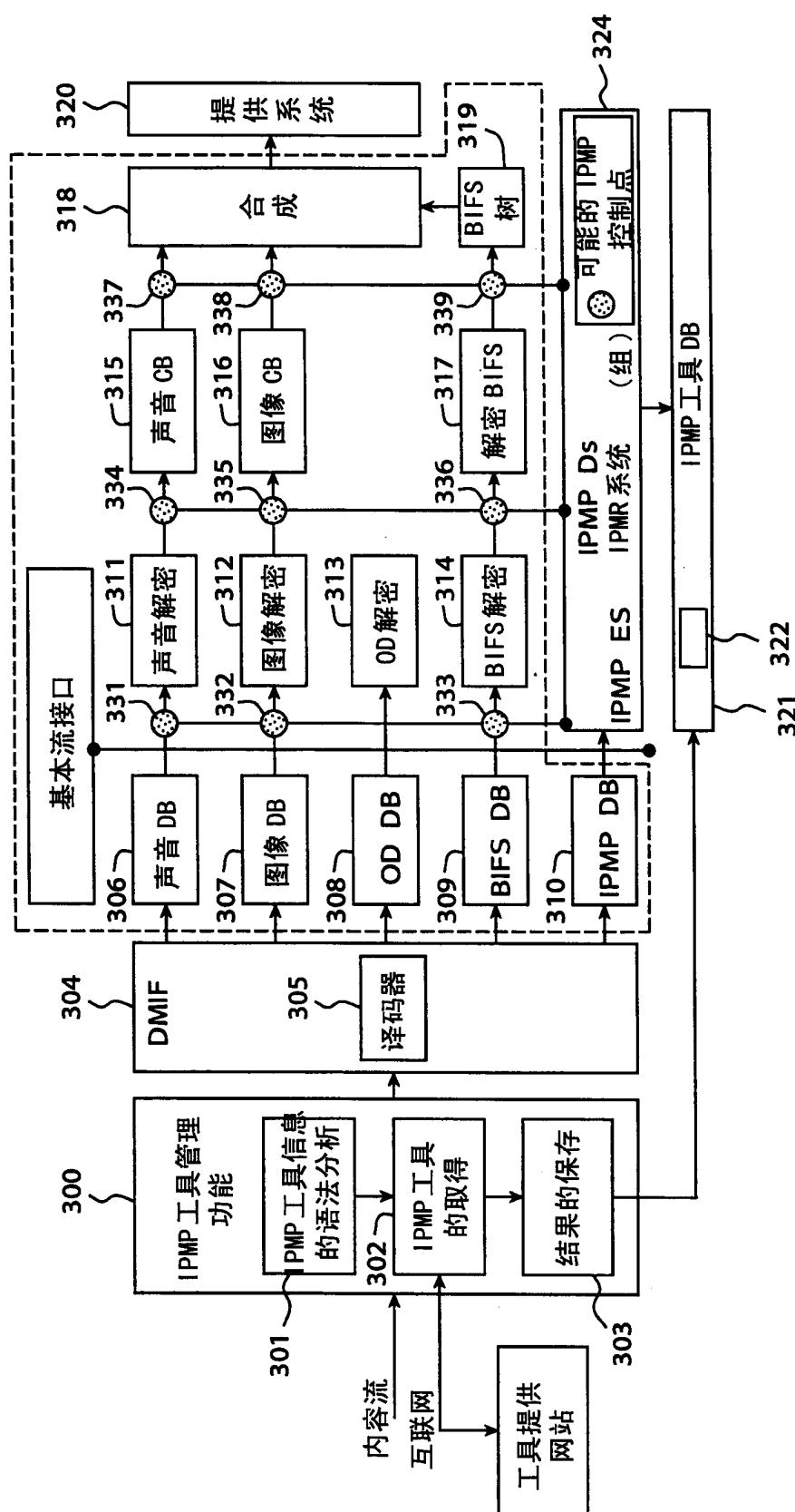


图 3

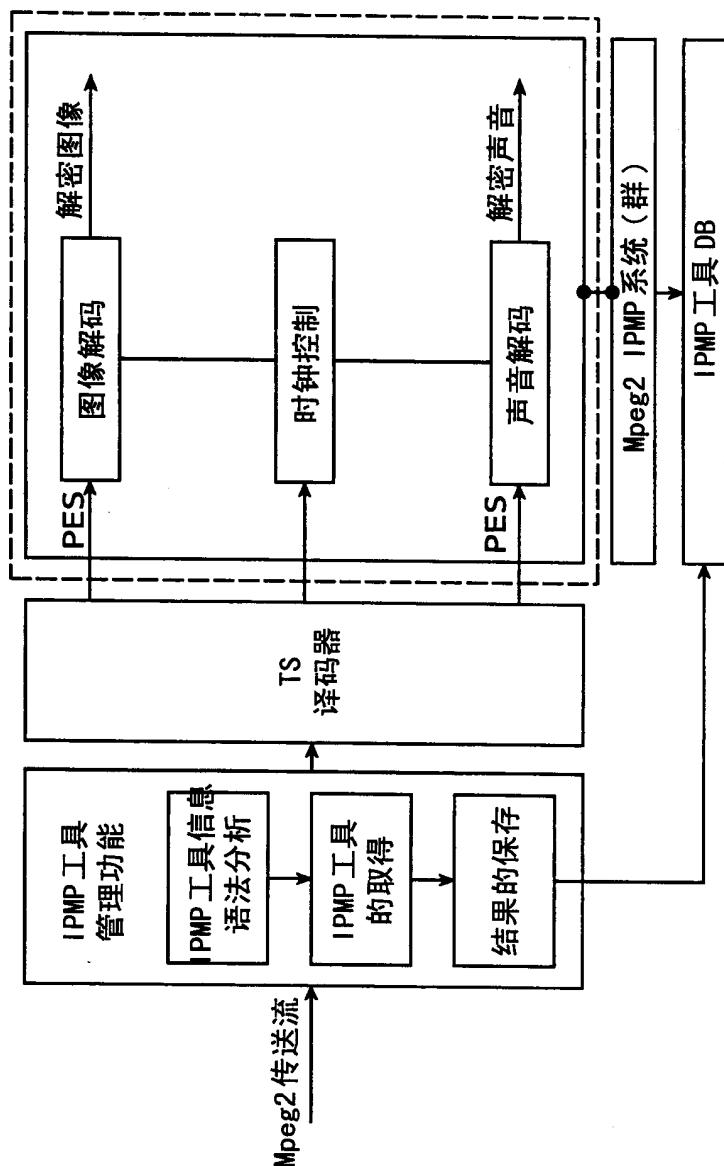


图 4

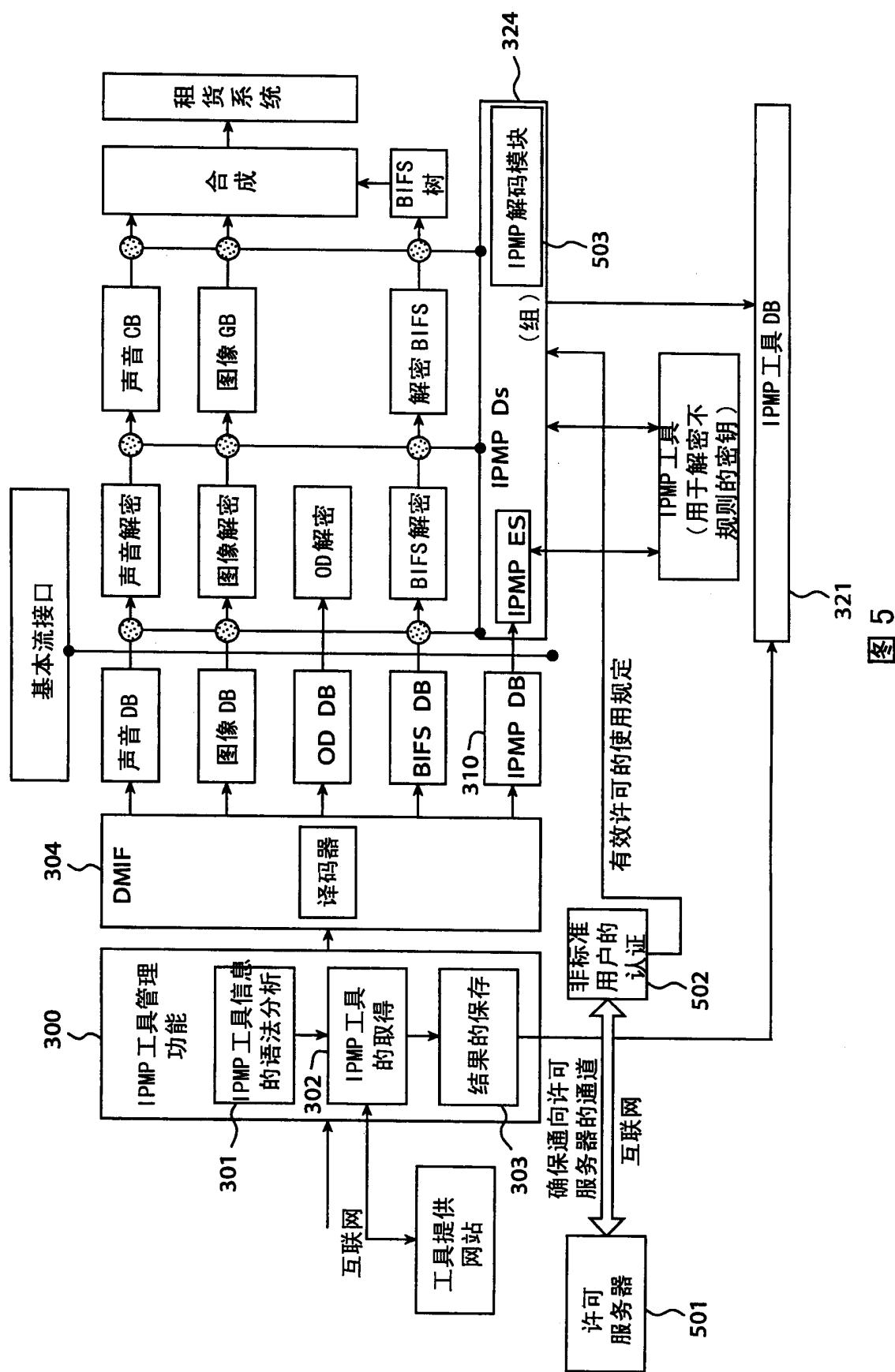


图 5

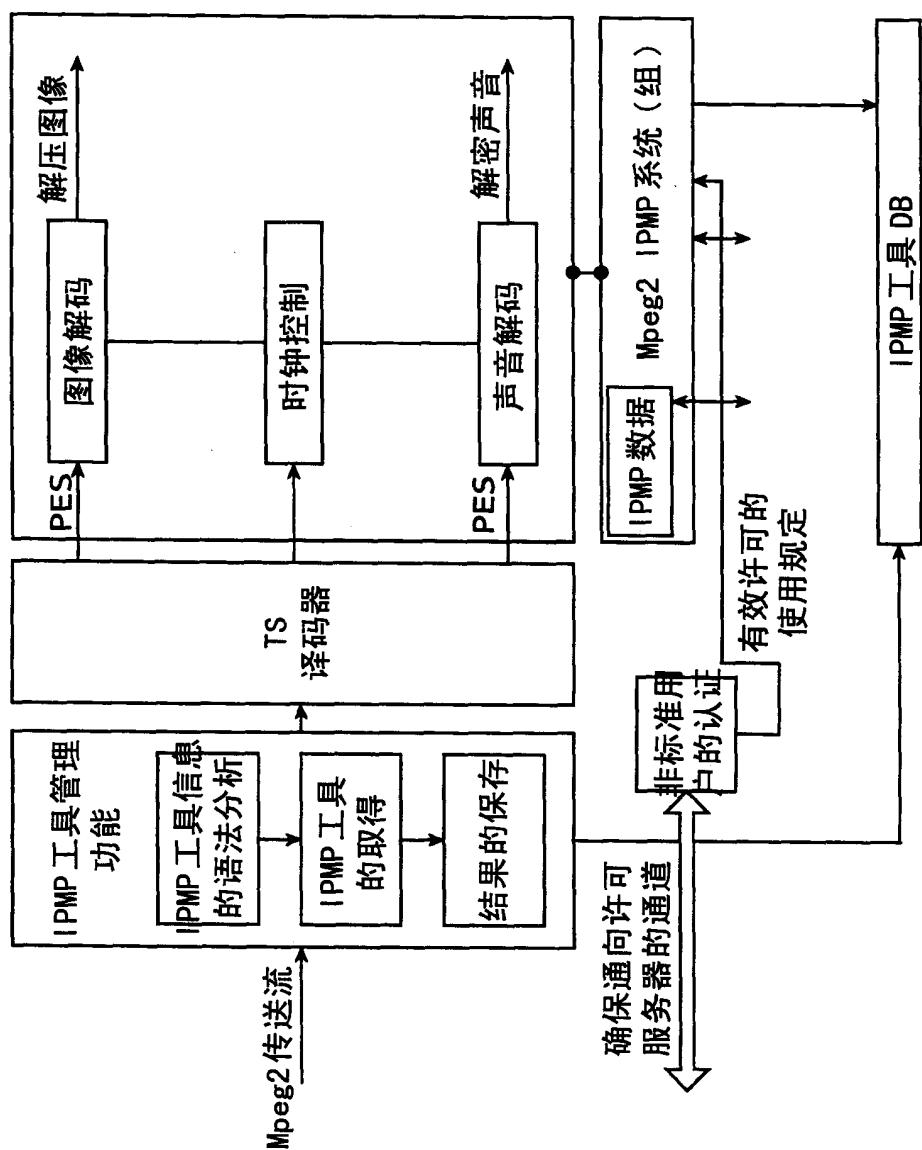


图 6



图 7

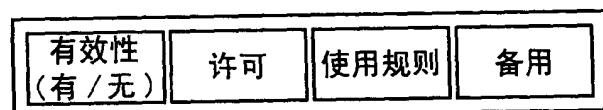


图 8