[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/167 (2006.01)

[12] 发明专利说明书

专利号 ZL 02147994.1

[45] 授权公告日 2006 年 4 月 19 日

[11] 授权公告号 CN 1253001C

[22] 申请日 2002.11.1 [21] 申请号 02147994.1

[30] 优先权

[32] 2001.11.2 [33] JP [31] 338363/2001

[32] 2002.8.20 [33] JP [31] 239775/2002

[71] 专利权人 佳能株式会社

地址 日本东京

[72] 发明人 田头信博 岩村惠市

审查员 陈荣华

[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 李德山

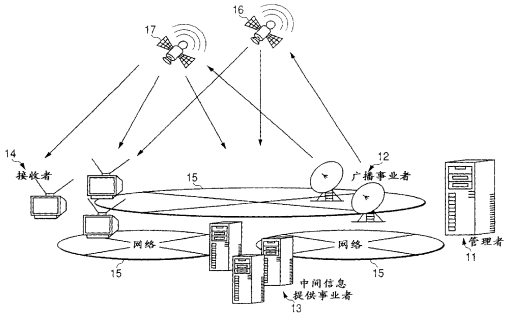
权利要求书 3 页 说明书 14 页 附图 9 页

[54] 发明名称

数字内容处理装置及处理方法、数字内容处理系统

[57] 摘要

提供一种数字内容处理装置及处理方法、数字内容处理系统。为了保护经过网络流通的数字内容的著作权，根据有关数字内容的中间信息的可靠性，控制能否进行对于数字内容的基于上述中间信息的编辑以及编辑程度。



1.一种数字内容处理装置，该数字内容处理装置处理数字内容和有关上述数字内容的中间信息，其特征在于包括:

接收上述数字内容及加密了的上述中间信息的接收装置，其中由上述接收装置接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的;

使用密钥对所接收的上述中间信息进行解密的解密装置;

根据在上述解密装置中使用的密钥的属性信息，决定上述数字内容的再生或编辑的级别的决定装置; 以及

根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

2.根据权利要求 1 所述的数字内容处理装置，其特征在于:

还包括存储多个密钥的存储装置; 以及从存储在上述存储装置中的多个密钥中选择一个密钥的选择装置，

其中，上述解密装置使用由上述选择装置所选择的密钥。

3.根据权利要求 1 所述的数字内容处理装置，其特征在于:

上述决定装置根据由上述解密装置解密了的中间信息是否是预定的格式而决定上述再生或编辑的级别。

4.根据权利要求 1 所述的数字内容处理装置，其特征在于:

上述接收装置接收与上述数字内容有关的契约信息，

上述控制装置具有根据所接收的契约信息而判定可否再生上述数字内容的判定装置，根据上述判定装置的判定，控制上述数字内容的再生。

5.根据权利要求 1 所述的数字内容处理装置，其特征在于:

由第 1 密钥对上述数字内容进行加密，且由第 2 密钥对上述第 1 密钥进行加密，

上述接收装置还接收用第 1 密钥加密了的上述数字内容和用上述第 2 密钥加密了的上述第 1 密钥，

上述解密装置用上述第 2 密钥对上述第 1 密钥进行解密，用解密了的第 1 密钥对上述数字内容进行解密。

6.一种数字内容处理装置，该数字内容处理装置处理数字内容和有关上述数字内容的中间信息，其特征在于包括:

接收上述数字内容及上述中间信息的接收装置，其中由上述接收装置接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的;

根据在所接收的上述中间信息的署名检验中所使用的密钥的证明书，决定上述数字内容的再生或编辑的级别的决定装置；以及

根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

7.根据权利要求 6 所述的数字内容处理装置，其特征在于:

由上述接收装置接收了的中间信息具有上述中间信息的数字署名，

上述决定装置具有对上述数字署名进行检验的检验装置，

根据上述检验的结果和上述证明书决定上述再生或编辑的级别。

8.一种数字内容处理系统，该数字内容处理系统包括处理有关数字内容的中间信息的第 1 信息处理装置以及第 2 信息处理装置，其特征在于:

上述第 1 信息处理装置具有: 对上述中间信息进行加密的加密装置；以及把由上述加密装置加密了的中间信息发送到上述第 2 信息处理装置的发送装置，

上述第 2 信息处理装置具有: 从上述第 1 信息处理装置接收加密了的中间信息、从与上述第 1 信息处理装置不同的第 3 信息处理装置接收上述数字内容的接收装置；使用密钥对所接收的上述中间信息进行解密的解密装置；根据在上述解密装置中使用的密钥的属性信息，决定上述数字内容的再生或编辑的级别的决定装置；以及根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

9. 一种数字内容处理方法，该数字内容处理方法处理数字内容

和有关上述数字内容的中间信息，其特征在于包括:

接收上述数字内容及加密了的上述中间信息的接收步骤，其中由上述接收步骤接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的;

使用密钥对所接收的上述中间信息进行解密的解密步骤;

根据在上述解密步骤中使用的密钥的属性信息，决定数字内容的再生或编辑的级别的决定步骤; 以及

根据由上述决定步骤决定了的级别，控制上述数字内容的再生或编辑的控制步骤。

10. 根据权利要求 **9** 所述的数字内容处理方法，其特征在于:

由上述接收步骤接收了的中间信息具有上述中间信息的数字署名，

上述决定步骤包括对上述数字署名进行检验的检验步骤，

根据上述检验的结果和上述证明书决定上述再生或编辑的级别。

11.一种数字内容处理方法，该数字内容处理方法处理数字内容和有关上述数字内容的中间信息，其特征在于包括:

接收上述数字内容及上述中间信息的接收步骤，其中由上述接收步骤接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的;

根据在所接收的上述中间信息的署名检验中所使用的密钥的证明书，决定上述数字内容的再生或编辑的级别的决定步骤; 以及

根据由上述决定步骤决定了的级别，控制上述数字内容的再生或编辑的控制步骤。

数字内容处理装置及处理方法、数字内容处理系统

技术领域

本发明涉及有关对于各种内容的中间信息，能够检验中间信息的可靠性或者有效性的系统。特别是，在广播等中，检验中间信息的可靠性或者有效性，根据其检验结果和中间信息能够控制改变节目内容的系统中所使用的系统。

背景技术

伴随着至今为止的数字化的潮流，在各个领域中正在发展数字化。在广播领域也正在开展数字化，其中一部分正在实行数字化广播。在数字化广播中由于能够与广播节目一起，发送记载了其节目内容的中间信息等，因此提出了具有大容量存储功能（以下称为存储）的接收机灵活运用这些中间信息，自动地存储广播节目，提供画面检索或者摘要视听等新的服务。

另外，伴随着至今为止的硬盘的大容量化，已经在市场上销售记录了数字广播的内容的硬盘记录器等，正在具备实现这种服务的环境。另外，在数字广播中，作为所必须的工作，还要有防止非法复制以便保护广播节目的对策。

另外，具有大容量存储功能的接收机还期待与互联网或者其它信息家电的连接功能等作为家用服务器的功能，因此，称为「服务器型接收机」，另外，面向服务器型接收机的广播称为「服务器型广播」。

另一方面，以往收费广播方式广泛地研究了适用于电视广播或者高清晰度电视广播（以下，称为高清晰度电视广播）的限定接收方式。一般用收费方式广播的图像信号或者声音信号用某些方法实施扰频（干扰），使得不能够由允许接收者以外的人员接收，向允许接收者

发送用于把该扰频了的信号复原的信号，控制接收。

作为用于控制该接收的信号传送的信息由称为关联信息的用于复原扰频了的信号的密钥（扰频密钥 Ks）的信息，用于判定广播节目是否进入到接收者的契约范围的信息以及播放台用于把特定的接收机强制地打开·关闭的信息等构成。

在用卫星广播进行收费方式的电视广播或者高清晰度电视广播的情况下，关联信息通过数据通道以数据包的形式传送。这种情况下，扰频密钥或者有关广播节目的信息（称为节目内容）被加密成使得不能够由第三者了解或者篡改。

用于把扰频密钥或者节目内容加密了的密钥称为工作密钥 Kw，与表示各接收者契约内容的契约信息一起发送给接收者。这些信息称为单独信息，通过广播波或者 IC 卡，磁卡等物理媒体以及电话线等传送。在需要把单独信息加密的情况下，使用主密钥 Km。原则上每个接收者的主密钥 Km 互不相同。

图 8 示出实施扰频的方式的结构例。图 8 中，801～808 位于播放台一侧装置中，801 是扰频单元，802 是复用单元，803 是扰频密钥（Ks），804 是工作密钥（Kw），805 是契约信息，806 以及 807 是加密单元，808 是主密钥（Km）。

另外，809～815 位于接收一侧装置中，809 是分离单元，810 是去扰频单元，811、812 是解码单元，813 是视听判定单元，814 是契约信息，815 是主密钥（Km）。

在服务器型广播中，中间信息的提供并不仅限定于广播事业者，还能够设想经过互联网等通信媒体从各种事业者或者使用者分配。

另外，在中间信息中，并不仅是节目标题那样的单纯的中间信息，还能够设想生成节目的摘要这样的变更节目结构的中间信息等具有各种功能的信息。

而且，变更节目结构的中间信息由于在节目的改变中利用，因此必须考虑著作权法。

但是，以往完全没有考虑检验分配中间信息的从业者或者中间信

息的可靠性或可靠性的结构。

发明内容

在本发明的一实施例中，第1个目的在于使得能够检验对应于节目内容的中间信息的可靠性或者有效性。

另外，第2个目的在于提供能够根据中间信息的可靠性或者有效性，控制节目内容的再生或者编辑的系统。

本发明提供一种数字内容处理装置，该数字内容处理装置处理数字内容和有关上述数字内容的中间信息，其特征在于包括：接收上述数字内容及加密了的上述中间信息的接收装置，其中由上述接收装置接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的；使用密钥对所接收的上述中间信息进行解密的解密装置；根据在上述解密装置中使用的密钥的属性信息，决定上述数字内容的再生或编辑的级别的决定装置；以及根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

本发明提供一种数字内容处理装置，该数字内容处理装置处理数字内容和有关上述数字内容的中间信息，其特征在于包括：接收上述数字内容及上述中间信息的接收装置，其中由上述接收装置接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的；根据在所接收的上述中间信息的署名检验中所使用的密钥的证明书，决定上述数字内容的再生或编辑的级别的决定装置；以及根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

本发明提供一种数字内容处理系统，该数字内容处理系统包括处理有关数字内容的中间信息的第1信息处理装置以及第2信息处理装置，其特征在于：上述第1信息处理装置具有：对上述中间信息进行加密的加密装置；以及把由上述加密装置加密了的中间信息发送到上述第2信息处理装置的发送装置，上述第2信息处理装置具有：从上述第1信息处理装置接收加密了的中间信息、从与上述第1信息处理装置不同的第3信息处理装置接收上述数字内容的接收装置；使用密

钥对所接收的上述中间信息进行解密的解密装置；根据在上述解密装置中使用的密钥的属性信息，决定上述数字内容的再生或编辑的级别的决定装置；以及根据由上述决定装置决定了的级别，控制上述数字内容的再生或编辑的控制装置。

本发明提供一种数字内容处理方法，该数字内容处理方法处理数字内容和有关上述数字内容的中间信息，其特征在于包括：接收上述数字内容及加密了的上述中间信息的接收步骤，其中由上述接收步骤接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的；使用密钥对所接收的上述中间信息进行解密的解密步骤；根据在上述解密步骤中使用的密钥的属性信息，决定数字内容的再生或编辑的级别的决定步骤；以及根据由上述决定步骤决定了的级别，控制上述数字内容的再生或编辑的控制步骤。

本发明提供一种数字内容处理方法，该数字内容处理方法处理数字内容和有关上述数字内容的中间信息，其特征在于包括：接收上述数字内容及上述中间信息的接收步骤，其中由上述接收步骤接收的上述数字内容和上述中间信息是分别从不同的发送源传送来的；根据在所接收的上述中间信息的署名检验中所使用的密钥的证明书，决定上述数字内容的再生或编辑的级别的决定步骤；以及根据由上述决定步骤决定了的级别，控制上述数字内容的再生或编辑的控制步骤。

本发明的其它特征和优点将从以下与附图一起进行的叙述中明确，其中，相同的参考符号在所有的附图中表示相同或者相当的部分。

附图说明

图 1 是示出了本发明中的系统的概要的结构图。

图 2 是示出了本发明中的系统的概要的结构图。

图 3 是示出了本发明中的系统的概要的结构图。

图 4 是示出了本发明中的验证机构的构造的结构图。

图 5 是示出了本发明中的系统的概要的结构图。

图 6 是示出了本发明中的系统的概要的结构图。

图 7 示出对应于本发明中的中间信息的可靠性的分类信息的一例。

图 8 是示出以往的实现接收者限定广播的系统的结构例的结构图。

图 9 是示出了本发明中的系统的结构的结构图。

具体实施方式

下面，参照附图，说明本发明的数字内容处理装置，数字内容处理系统，数字广播系统，数字内容处理方法，计算机可读取的存储媒体以及计算机程序的实施形态。

图 1 示出本发明的第 1 实施形态中的系统的结构例。第 1 实施形态由单个或多个管理者，单个或多个广播事业者，单个或多个中间信息提供事业者以及多个接收者构成。他们分别用各种通信媒体相互连接。

管理者一侧装置 11 管理系统总体的运行。即，管理在系统中使用的密钥的发行等。

广播事业者一侧装置 12 是通过广播提供节目内容的实体，一般相当于播放台。但是本实施形态并不是特别地限定于图像的广播，还既能够适用在无线广播等音乐广播中，也能够适用在数字广播等一般内容的广播中。在本实施形态中，把这些广播内容总称为节目内容。

中间信息提供事业者一侧装置 13 是提供对应于节目内容的中间信息的实体。

在服务器型广播中，在存储装置中保持节目内容，同样还保持中间信息。另外，接收者一侧装置 14 的服务器型接收机具有与网络 15 的连接功能。服务器型接收机经由网络 15，通信卫星 16、17 等，接收节目内容和中间信息。另外，服务器型接收机也能够与节目内容分开，独立地接收中间信息。

由此，能够由提供中间信息的广播事业者一侧装置 12 以外的实体提供中间信息。

接收者一侧装置 14 是接收节目内容，并且再生节目内容或者根据中间信息编辑节目内容的实体。

以下，说明广播事业者一侧装置 12 与其它的实体之间使用称为电波广播的通信媒体进行通信的情况。另外，也能够用光纤等其它的通信媒体进行通信。另外，接收者一侧装置 14 与中间信息提供事业者一侧装置 13 之间不仅能够通过经由广播事业者一侧装置 12 的称为电波广播的单向通信媒体，还能够通过电话线路网或者移动电话网，有线电视网等各种双向通信媒体进行通信。还有，广播事业者一侧装置 12 还可以收容中间信息提供者提供事业者一侧装置 13。另外，广播事业者一侧装置 12 还可以收容管理者一侧装置 11。

图 2 示出中间信息提供事业者一侧装置 13 与接收者一侧装置 14 的结构的一例。如图 2 所示，中间信息提供事业者一侧装置 13 与接收者一侧装置 14 之间用通信媒体连接。中间信息提供事业者一侧装置 13 保持从管理者一侧装置 11 分配的第 1 密钥 131。另外，中间信息提供事业者一侧装置 13 具有加密单元 132。

加密单元 132 用第 1 密钥 131 把中间信息加密，并且输出加密中间信息。该加密的加密算法没有特别限定。

接收者一侧装置 14 保持从管理者一侧装置 11 分配的多个密钥 14a、14b、14c，密钥可靠性列表 141。在多个密钥 14a～14c 中，包括管理者一侧装置 11 对于中间信息提供事业者一侧装置 13 分配的密钥。

另外，密钥可靠性列表 141 是表示由管理者一侧装置 11 决定的各密钥 14a～14c 的可靠性的数据。密钥的可靠性例如根据保持密钥的中间信息提供事业者一侧装置 13 的可靠性决定。例如，如图 2 所示，在中间信息提供者一侧装置 13 与广播事业者一侧装置 12 不同的情况下可靠性低，另一方面，在中间信息提供者一侧装置 13 被收容在广播事业者一侧装置 12 中的情况下，较高地决定可靠性信息。

另外，接收者一侧装置 14 具有解码单元 142，密钥选择单元 143，检验单元 144。

解码单元142使用从密钥选择单元143输出的密钥信息把加密中间信息进行解码。解码算法与中间信息提供事业者一侧装置13的加密单元132使用的加密算法相对应。另外，从密钥选择单元143输出的密钥信息与加密单元132在中间信息的加密时使用的密钥相对应。

密钥选择单元143从多个密钥14a～14c中选择解码单元142使用的密钥。选择方法可以考虑顺序地选择所有的密钥14a～14c的方法，或者根据输入到解码单元142中的加密中间信息的标题部分中添加的密钥的识别信息进行选择的方法等。

在本实施形态中，通过中间信息提供事业者一侧装置13和接收者一侧装置14共用密钥，实现加密通信。另外，由于中间信息不是二进制数据，而是具有某些格式，因此通过检查解码单元142解码了的信息是否遵从特定的格式，能够检验中间信息的正当性。

检验单元144根据解码单元142的解码结果，解码中使用的密钥和密钥可靠性列表141，输出可靠性信息。

例如，假设密钥选择单元143选择密钥14a，解码单元142能够使用密钥14a把加密中间信息解码，则检验单元144从密钥可靠性列表141参照密钥14a的可靠性输出可靠性信息。

如以上那样，在能够确认中间信息的正当性的情况下，通过参照密钥可靠性列表141，能够检查与所使用的密钥相对应的可靠性，能够决定保持密钥的中间信息提供事业者一侧装置13或者中间信息的可靠性。

在不能够确认中间信息的正当性的情况下，也可以使中间信息的可靠性成为最低级。例如，如上述那样，在把密钥可靠性列表141作为保有密钥的中间信息提供事业者一侧装置13的可靠性的情况下，中间信息的可靠性信息成为生成中间信息的中间信息提供事业者一侧装置13的可靠性。

其次，图3中示出把本实施形态适用于接收者限定广播时的结构例。

图3由广播事业者一侧装置120，中间信息提供事业者一侧装置

130 和接收者一侧装置 140 构成，广播事业者一侧装置 120 对于接收者一侧装置 140 提供接收者限定广播。

在接收者限定广播中播放的节目内容以某种方法施加了扰频使得不能够在未被允许的接收者一侧装置 140 中再生。向被允许的接收者一侧装置 140 送出用于把该扰频了的节目内容复原的信号，使其能够进行再生。

图 3 中，广播事业者一侧装置 120 保持从管理者一侧装置 11 分配的第 1 密钥 128，由扰频单元 121，复用单元 124，第 1 加密单元 123，第 2 加密单元 127 构成。

扰频单元 121 使用扰频密钥 Ks122，把节目内容进行扰频。第 1 加密单元 123 使用工作密钥 Kw125，把扰频密钥 Ks122 加密。

第 2 加密单元 127 使用第 1 密钥 128，把工作密钥 Kw125 和契约信息 126 加密。复用单元 124 把从扰频单元 121 输出的加密节目内容，从第 1 加密单元 123 输出的加密扰频密钥 Ks122 以及从第 2 加密单元 127 输出的加密信息复用。其中，从第 2 加密单元 127 输出的加密工作密钥 Kw125 和加密契约信息 126 也可以不进行复用。

通过把从第 1 加密单元 123 和第 2 加密单元 127 输出的信息复用，能够控制是否再生节目内容，能够减少控制是否再生所需要的工作密钥 Kw125 以及契约信息 126 等的数据量。

图 3 中，中间信息提供事业者一侧装置 130 保持从管理者一侧装置 11 分配的第 2 密钥 133，具有第 3 加密单元 135。第 3 加密单元 135 用第 2 密钥 133 把中间信息提供事业者一侧装置 130 生成的中间信息 134 加密，把加密中间信息输出到网络 160。

图 3 中，接收者一侧装置 140 保持从管理者一侧装置 11 分配的多个密钥 150 和密钥信息可靠性列表 148，由分离单元 141，去扰频单元 143，第 1 解码单元 142，第 2 解码单元 144，密钥选择单元 146，检验单元 147，视听判定单元 145，视听控制单元 149 构成。

分离单元 141 分离从广播事业者一侧装置 120 接收的复用信息。而且，分离了的加密节目内容输出到去扰频单元 143，加密扰频密钥

Ks 输出到第 1 解码单元 142，加密信息输出到第 2 解码单元 144。

密钥选择单元 146 从多个密钥 150 选择解码处理使用的密钥。第 2 解码单元 144 使用从密钥选择单元 146 输出的密钥，把加密工作密钥 Kw125 和加密契约信息 126 解码。另外，第 2 解码单元 144 使用从密钥选择单元 146 输出的密钥，把经过网络 160 从第 3 加密单元 135 输出的加密中间信息解码。

第 1 解码单元 142 使用从第 2 解码单元 144 输入的工作密钥 Kw125 把加密扰频密钥 Ks 解码。

视听判定单元 145 根据从第 2 解码单元 144 输入的契约信息 126，从第 1 解码单元 142 得到扰频密钥 Ks，输入到去扰频单元 140。

去扰频单元 140 使用从视听判定单元 145 输入的扰频密钥 Ks，把从分离单元 141 输入的加密节目内容去扰频。

另外，如果密钥选择单元 146 不从多个密钥中选择特定的密钥，则不能够用与其相对应的工作密钥 Kw，把用加密了的扰频密钥 Ks 加密了的节目内容复原。另外，如果密钥选择单元 146 从多个密钥中仅选择特定的密钥，则仅能够用与其相对应的工作密钥 Kw，把用加密了的扰频密钥 Ks 加密了的节目内容复原。即，通过控制用密钥选择单元 146 选择的密钥，能够仅在特定的期间，使接收者一侧装置 140 再生节目内容。

检验单元 147 根据解码中使用的密钥 150 和密钥可靠性列表 148，输出中间信息的可靠性信息。

视听控制单元 149 输入中间信息和中间信息的可靠性信息，根据中间信息的可靠性，控制能否编辑基于中间信息的节目内容。控制成使得如果是可靠性高的中间信息，则能够对于节目内容进行编辑，如果是可靠性低的中间信息，则不能够对于节目内容进行编辑。

另外，图 9 中示出在本实施形态中，根据中间信息的可靠性控制对于节目内容的基于中间信息的编辑时的接收者一侧装置 140 的结构。

图 9 中的接收者一侧装置 140 除去上述图 3 中的结构以外，由编

辑控制单元 171，编辑单元 170 构成。

编辑控制单元171根据中间信息和可靠性信息控制能否由编辑单元 170 进行对于节目内容的编辑。

另外，编辑控制单元 171 还可以根据中间信息和可靠性信息，控制编辑单元 170 对于节目内容的编辑程度。例如，如果中间信息的可靠性高，则能够进行对于节目内容的大编辑，另一方面，如果中间信息的可靠性低，则只能够进行对于节目内容的小编辑。所谓大编辑，例如，是节目内容的情节展开等改变结构的编辑，可以举出从多个节目内容剪切出特定演员的剪辑，生成演员的剪辑集这样的编辑。另外，所谓小编辑，例如是维持节目内容的编辑，可以举出生成节目内容的摘要或者在开头加入节目内容的标题这样的编辑。另外，编辑的式样还可以考虑多种，本发明并没有限定特别的编辑。

另外，在对于 1 个节目内容具有多个中间信息时，为了决定在节目内容中发生作用的中间信息的优先顺序，可以利用可靠性。

第 2 实施形态

以下，说明本发明中的第 2 实施形态。

在利用了在加密和解码中使用不同密钥的公开密钥加密方式的系统中，大多利用以使用了验证机构（称为 CA），证明书，证明书失效列表（称为 CRL）的公开密钥底层结构（称为 PKI）为基础的系统。

通过共同使用由验证机构 CA 生成的对于利用者的公开密钥的证明书和公开密钥，保证公开密钥的正当性。另外，在证明书的检验过程中，通过参照证明书失效列表 CRL，能够检查是否没有取消其证明书。

另外，如图 4 的结构说明图所示那样，根据下位的验证机构 CA1 从上位的根验证机构 CA 得到验证的构造，能够分层地构成验证机构 CA。把其称为管理者署名连锁。

另外，在通常进行的证明书发行服务中，在证明书的发行时，有时还定义对应于本人确认的严格性的证明书的类别。但是，在本实施

形态中，证明书的类别不是定义与发行证明书时本人确认的严格性，而是与中间信息的可靠性相对应的多个类别。

例如，如图 7 所示，对于「能够进行节目内容的完全视听控制的类别」，「不允许节目内容的视听控制的类别」，「能够再生节目内容的摘要的类别」等各种视听控制，定义各个证明书的类别。另外，关于证明书失效列表 CRL，能够利用为排除分配不正当的中间信息的信息提供事业者，或者能够利用为排除不正当的中间信息类别。

第 2 实施形态的系统结构例与第 1 实施形态相同。其中，管理者具有验证机构 CA 的功能。图 5 中示出第 2 实施形态的基本结构例。第 2 实施形态的基本结构如图 5 所示，由中间信息提供事业者 510 和接收者 520 构成。

中间信息提供事业者 510 生成公开密钥加密方式中的公开密钥和秘密密钥，从管理者 530 得到对于公开密钥的证明书，并且保持这些密钥和证明书。另外中间信息提供事业者 510 由第 1 密钥管理单元 512 和数字署名单元 511 构成。

第 1 密钥管理单元 512 保持并管理秘密密钥和证明书。另外，根据需要，把秘密密钥输出到数字署名单元 511。数字署名单元 511 使用从第 1 密钥管理单元 512 输入的秘密密钥，在中间信息中生成数字署名。

接收者 520 从管理者 530 得到中间信息提供事业者 510 等的证明书，并且保持该证明书。进而，还管理从管理者 530 得到的证明书失效列表 CRL。另外，接收者 520 由数字署名检验单元 521，第 2 密钥管理单元 522，检验单元 523 构成。

第 2 密钥管理单元 522 得到并管理中间信息提供事业者 510 等的证明书。作为管理方法，有在登录时预先登录从管理者 530 得到的证明书的方法，或者根据需要从管理者 530 得到证明书的方法。进而，还管理从管理者 530 得到的证明书失效列表 CRL。另外，还根据需要输出证明书。

数字署名检验单元 521 使用从第 2 密钥管理单元 522 输入的证明

书，检验中间信息的数字署名。检验单元 523 从数字署名检验单元 521 的检验结果和在检验中使用的证明书得到可靠性信息。可靠性信息从能够检验数字署名的正当性的证明书的类别和对于证明书的管理者 530 的署名连锁决定可靠性信息。

例如，在对于中间信息的署名是广播事业者署名时的证明书的类别为最上级时，是最上级的可靠性信息，在对于中间信息署名是作为第三者的中间信息提供事业者 512 的署名时的证明书的类别为最下级时，是最下级的可靠性信息。

第 2 实施形态以公开密钥底层结构 PKI 为基础，检验中间信息，从中间信息的数字署名的检验结果和检验中使用的证明书得到可靠性信息。与第 1 实施形态不同，通过以公开密钥底层结构 PKI 为基础，能够不保持多个秘密密钥而进行中间信息的验证。另外，根据证明书的水平或者对于证明书的管理者 530 的署名连锁，能够容易地决定有关证明书的上下关系或者优劣。

图 6 中示出把图 5 的基本结构适用于已经存在的接收者限定广播时的结构图。

图 6 中，广播事业者 610 由扰频单元 611，复用单元 618，加密单元 615，第 1 加密／署名单元 616，第 1 密钥管理单元 617 构成。扰频单元 611，复用单元 618，加密单元 615 是与第 1 实施形态相同的结构。

第 1 加密／署名单元 616 输入工作密钥 613 和契约信息 614，使用从第 1 密钥管理单元 617 输入的密钥进行加密，生成数字署名。

第 1 密钥管理单元 617 管理广播事业者 610 的秘密密钥和证明书，根据需要，还管理从管理者 640 得到的证明书失效列表 CRL。进而，根据需要，或者生成共用的密钥，或者输出在数字署名处理中使用的秘密密钥。

图 6 中，中间信息提供事业者 620 与基本结构相同，生成公开密钥加密方式中的公开密钥和秘密密钥，从管理者 640 得到对于公开密钥的证明书，并且保持这些密钥和证明书。另外，中间信息提供事业

者 620 由第 2 加密／署名单元 622，第 2 密钥管理单元 623 构成，在中间信息 621 中生成数字署名。 第 2 密钥管理单元 623 保持并管理秘密密钥和证明书。另外根据需要，把秘密密钥输出到第 2 加密／署名单元 622。第 2 加密／署名单元 622 使用从第 2 密钥管理单元 623 输入的秘密密钥，在中间信息 621 中生成数字署名。

图 6 中，接收者 630 由分离单元 631，去扰频单元 638，解码单元 632，视听判定单元 636，视听控制单元 637，解码／检验单元 633，检验单元 635，第 3 密钥管理单元 634 构成。分离单元 631，去扰频单元 638，解码单元 632，视听控制单元 636 的结构与上述第 1 实施形态相同。

解码／检验单元 633 输入从分离单元 631 或者网络 650 输入的加密信息，使用从第 3 密钥管理单元 634 输入的密钥进行解码，检验数字署名。

第 3 密钥管理单元 634 保持并管理广播事业者 610 的证明书。另外，根据需要，或者从管理者 640 得到新的证明书，或者得到并且管理证明书失效列表 CRL。另外，根据需要，输出在数字署名的检验中所需要的公开密钥。这些证明书管理实现各种密钥管理，各种密钥管理与第 1 实施例相同，能够使用在服务器型广播中特定化了的接收者限定广播方式。

检验单元 635 检查来自解码／检验单元 633 的中间信息的检验结果，以及在解码／检验单元 633 中使用的证明书的类别或者对于证明书的管理者的数字署名连锁，作为可靠性信息。

如上述那样，在该第 2 实施形态中，检验中间信息，从中间信息的数字署名的检验结果和在检验中使用的证明书得到可靠性信息。

本发明的其它实施形态

另外，以上述说明的本实施形态的数字内容处理装置由计算机的 CPU 或者 MPU，RAM，ROM 等构成，能够通过存储在 RAM 或者 ROM 中的程序进行动作而实现。

从而，通过把使计算机起到上述功能那样进行动作的程序记录在

例如 CD—ROM 那样的记录媒体中，能够通过使计算机读入而实现。作为记录上述程序的记录媒体，除去 CD—ROM 以外，还能够使用软盘，硬盘，磁盘，光磁盘，非易失性存储卡等。

另外，不仅通过计算机执行所供给的程序实现上述实施形态的功能，该程序与在计算机中工作的 OS（操作系统）或者其它应用软件等一起实现上述实施形态的功能的情况，或者通过计算机的功能扩展板或功能扩展单元进行所供给的程序的全部处理或者一部分处理实现上述实施形态的功能的情况等这样的程序也包含在本发明的实施形态中。

另外，还可以由要在网络环境下利用本发明的其它计算机执行全部或者一部分程序。例如，画面输入处理可以由远端计算机进行，各种判断、对数记录等可以由其它的中心计算机等进行。

图1

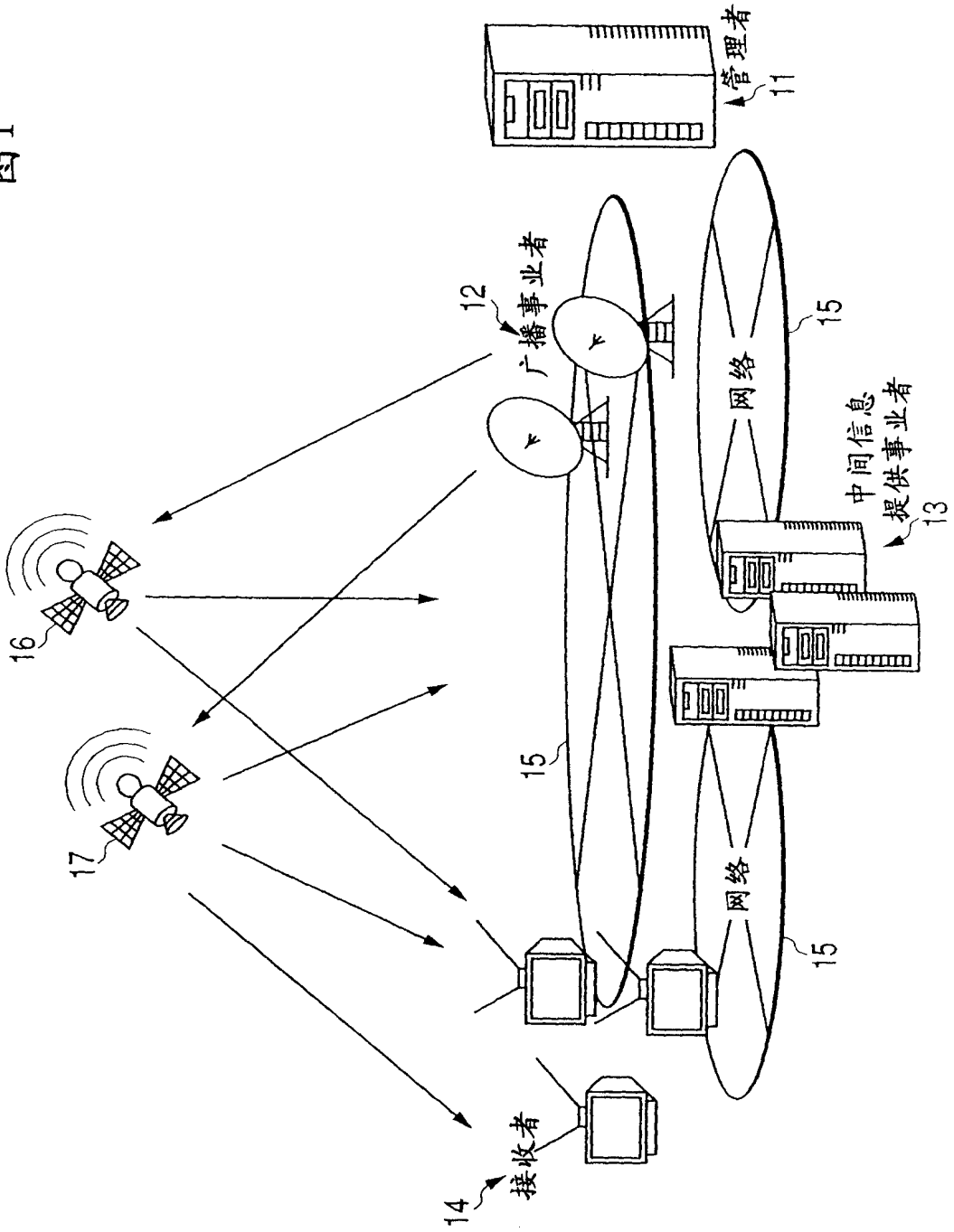


图2

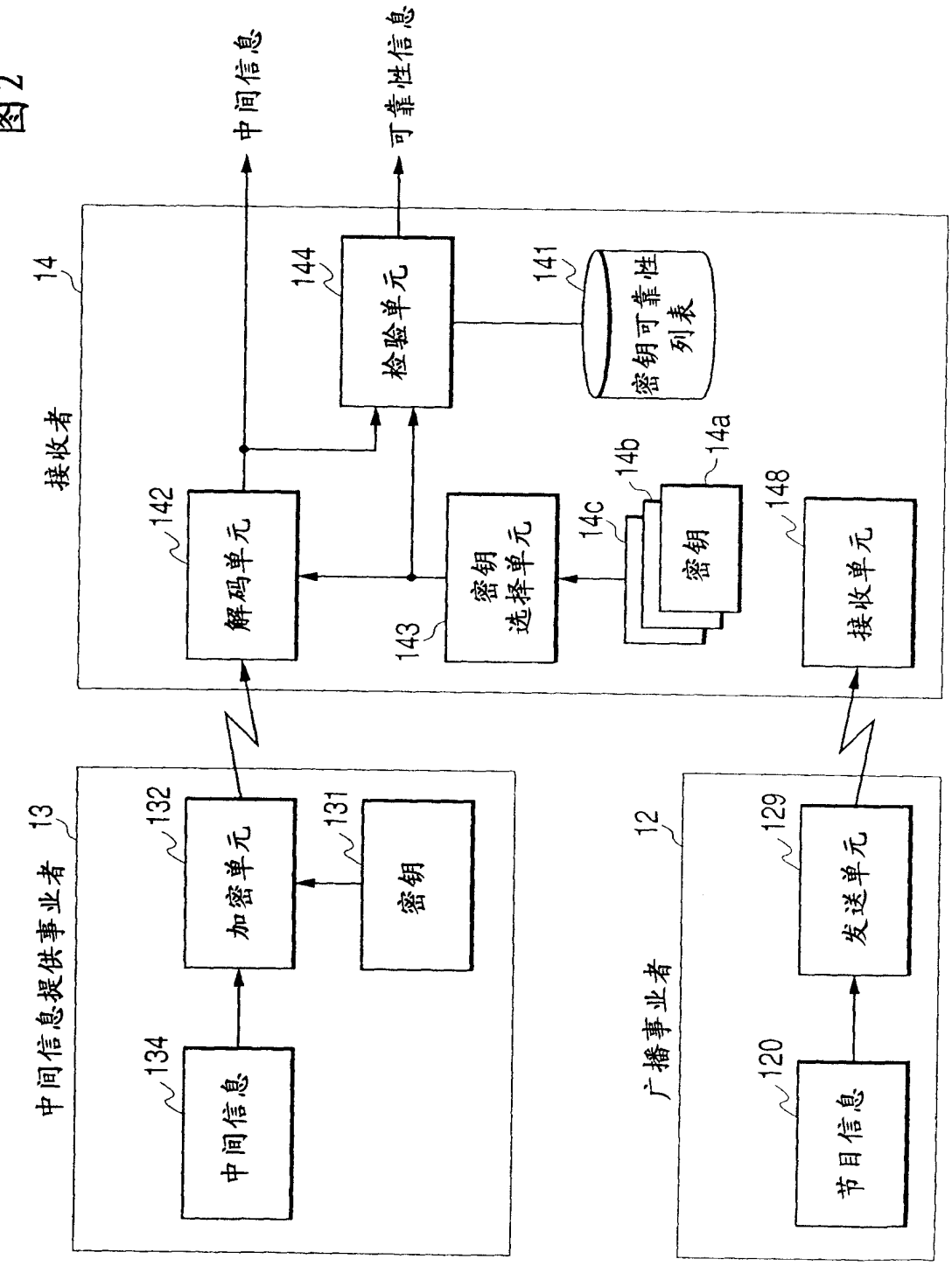

中间信息
可靠性信息
14
接收者
144
检验单元
141
密钥可靠性列表
142
解码单元
143
密钥选择单元
14c
14b
密钥
14a
148
接收单元
中间信息提供事业者
13
132
加密单元
131
密钥
134
中间信息
广播事业者
12
129
发送单元
120
节目信息

图 3

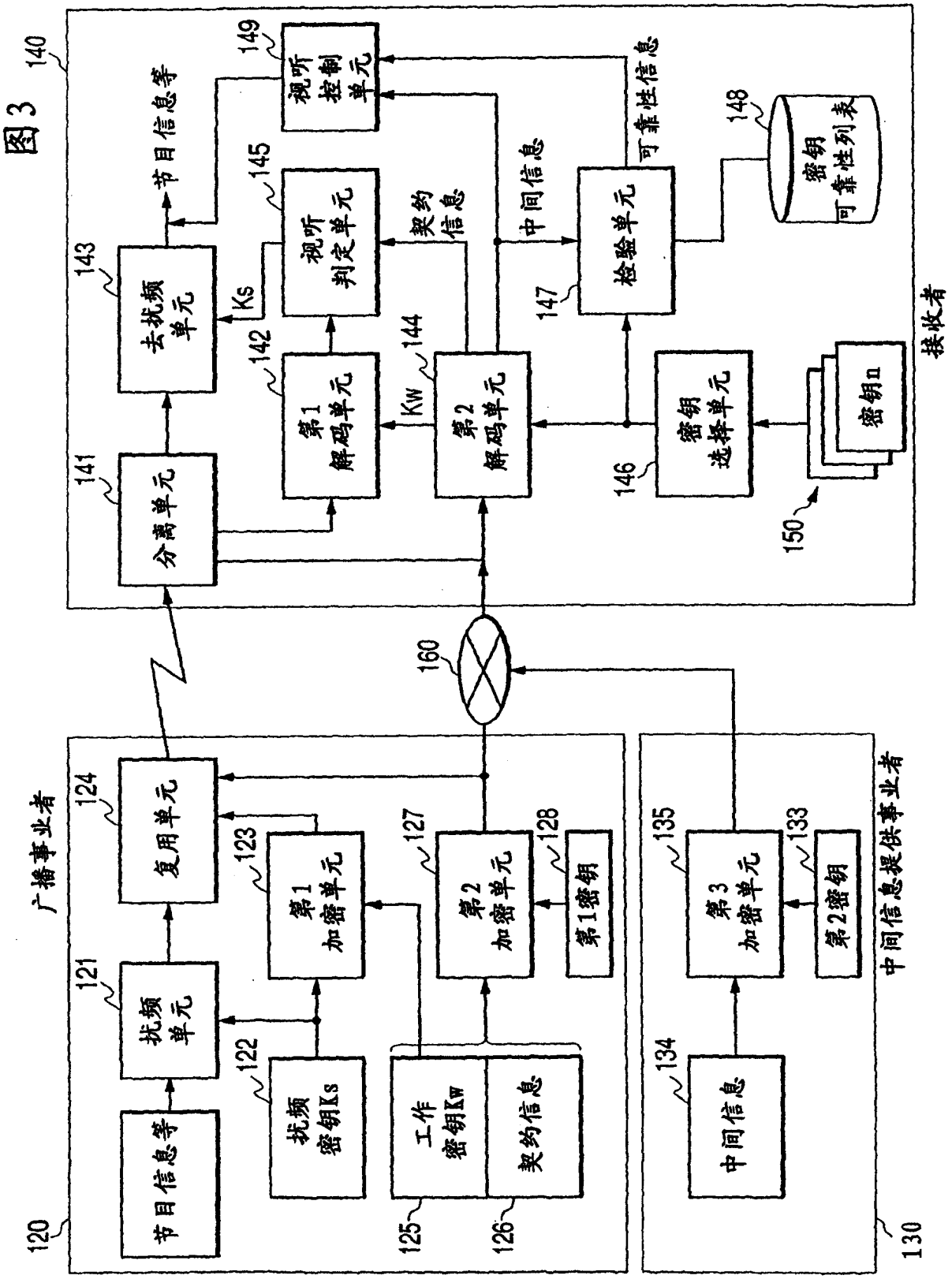

广播事业者
120
节目信息等
扰频单元
121
扰频密钥Ks
122
第1加密单元
123
复用单元
124
工作密钥Kw
125
契约信息
126
第2加密单元
127
第1密钥
128
中间信息提供事业者
130
中间信息
134
第3加密单元
135
第2密钥
133
160
接收者
140
分离单元
141
去扰频单元
143
节目信息等
第1解码单元
142
Kw
第2解码单元
144
Ks
视听判定单元
145
契约信息
视听控制单元
149
中间信息
检验单元
147
可靠性信息
密钥选择单元
146
密钥n
150
密钥可靠性列表
148

图 4

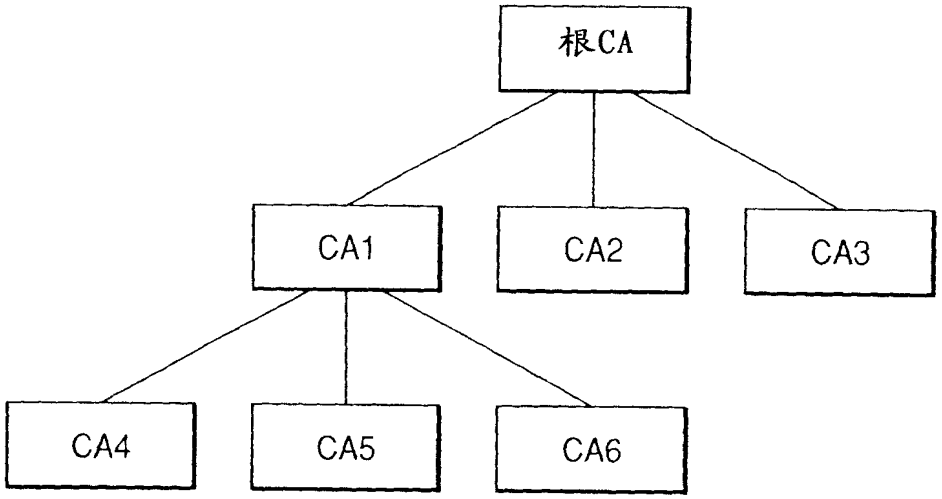


图5

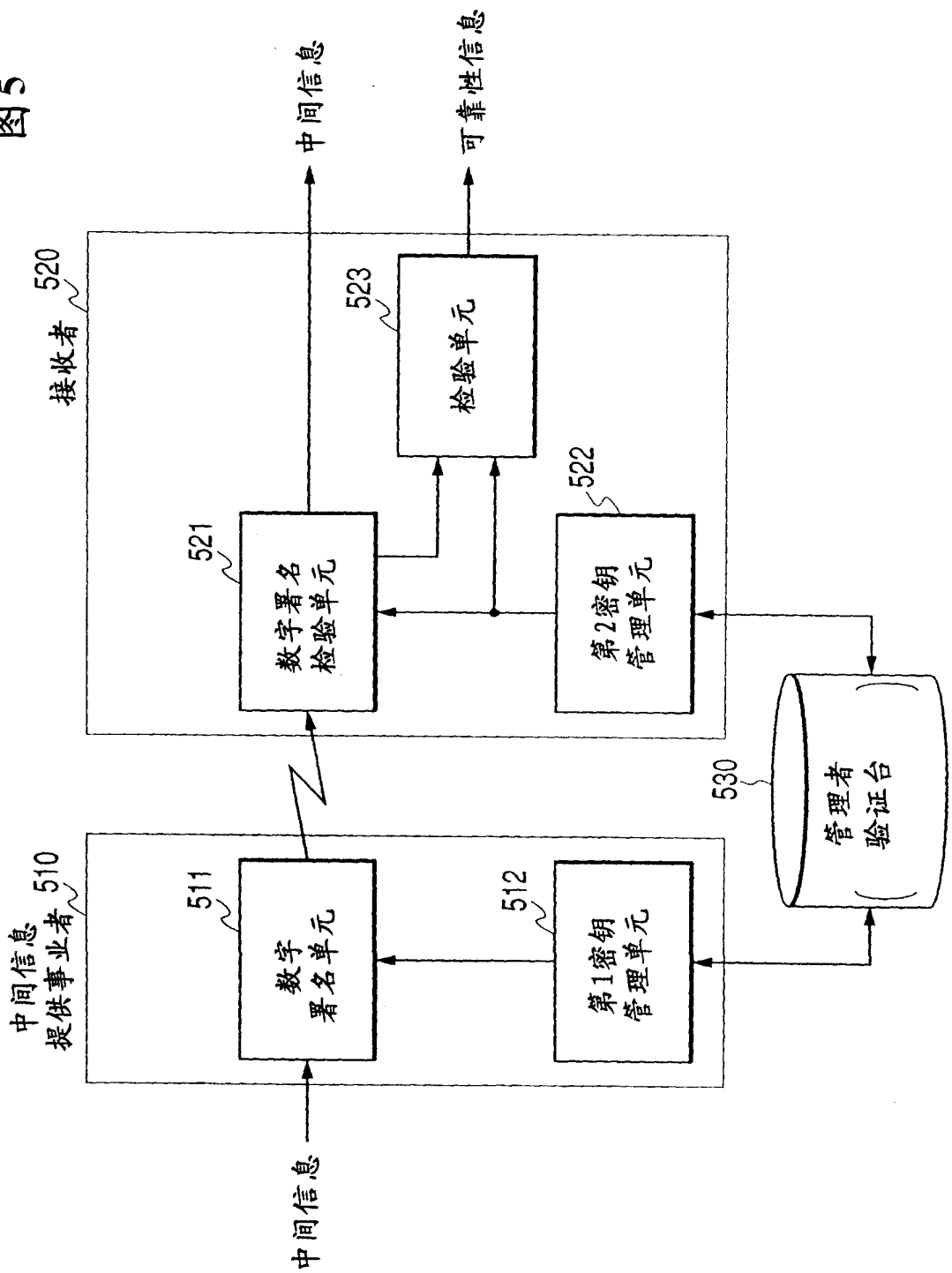

中间信息
可靠性信息
520
接收者
523
检验单元
521
数字署名
检验单元
522
第2密钥
管理单元
530
管理者
验证台
中间信息
提供事业者
510
511
数字
署名单元
512
第1密钥
管理单元
中间信息

图 6

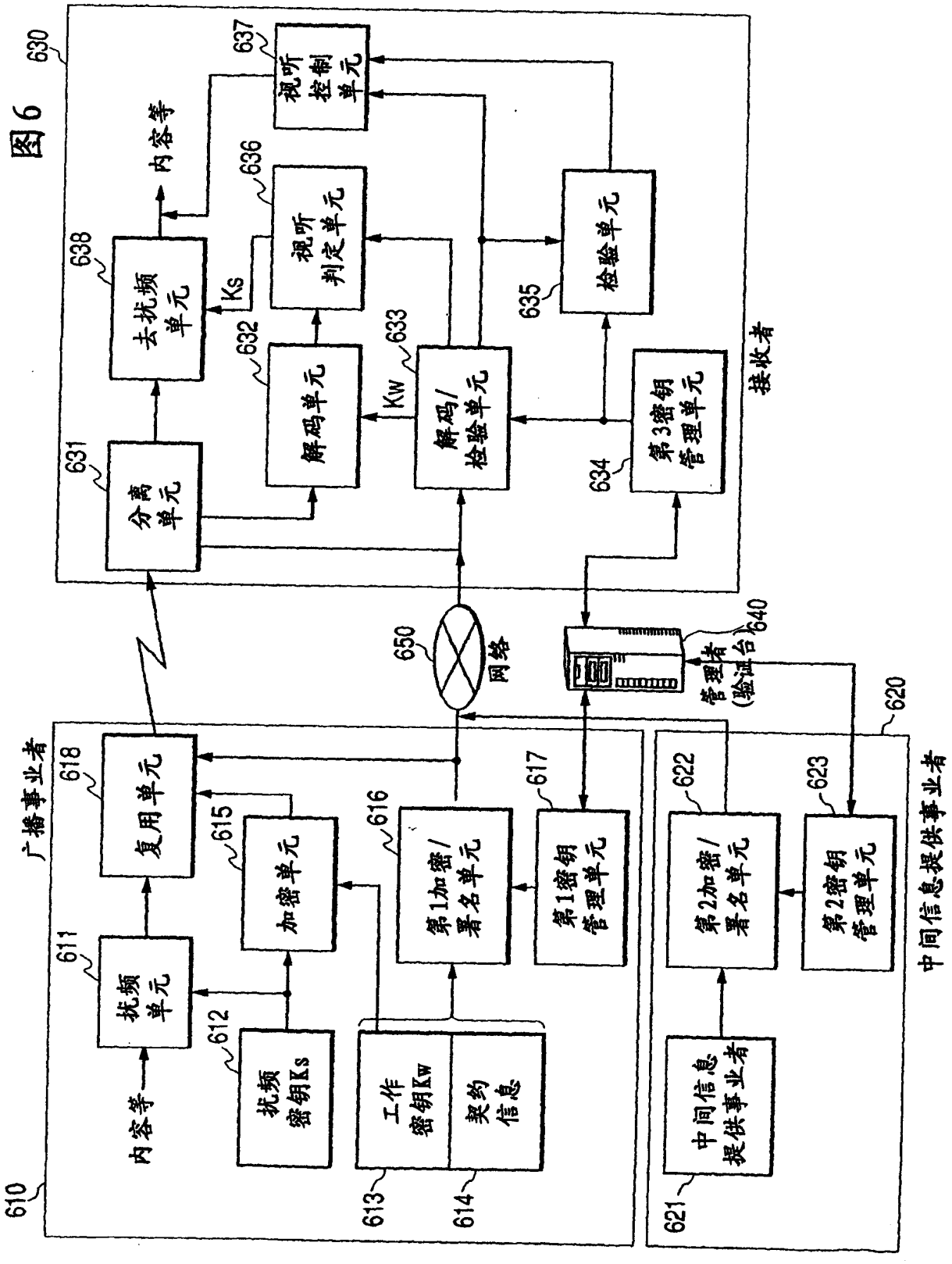

630
637
视听控制单元
内容等
636
视听判定单元
638
去扰频单元
Ks
632
解码单元
633
Kw
解码/检验单元
635
检验单元
631
分离单元
634
第3密钥管理单元
接收者
650
网络
640
管理者(验证台)
620
广播事业者
618
复用单元
615
加密单元
616
第1加密/署名单元
617
第1密钥管理单元
622
第2加密/署名单元
623
第2密钥管理单元
中间信息提供事业者
611
扰频单元
内容等
612
扰频密钥Ks
工作密钥Kw
契约信息
613
614
610
中间信息提供事业者
621

图7

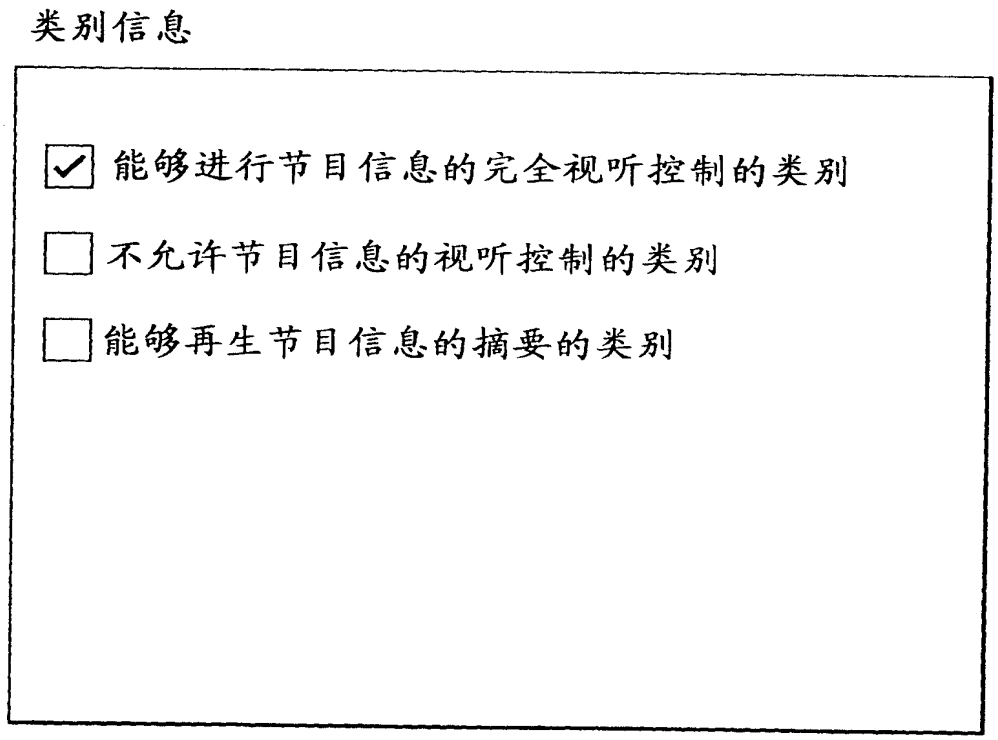

类别信息
能够进行节目信息的完全视听控制的类别
不允许节目信息的视听控制的类别
能够再生节目信息的摘要的类别

图8

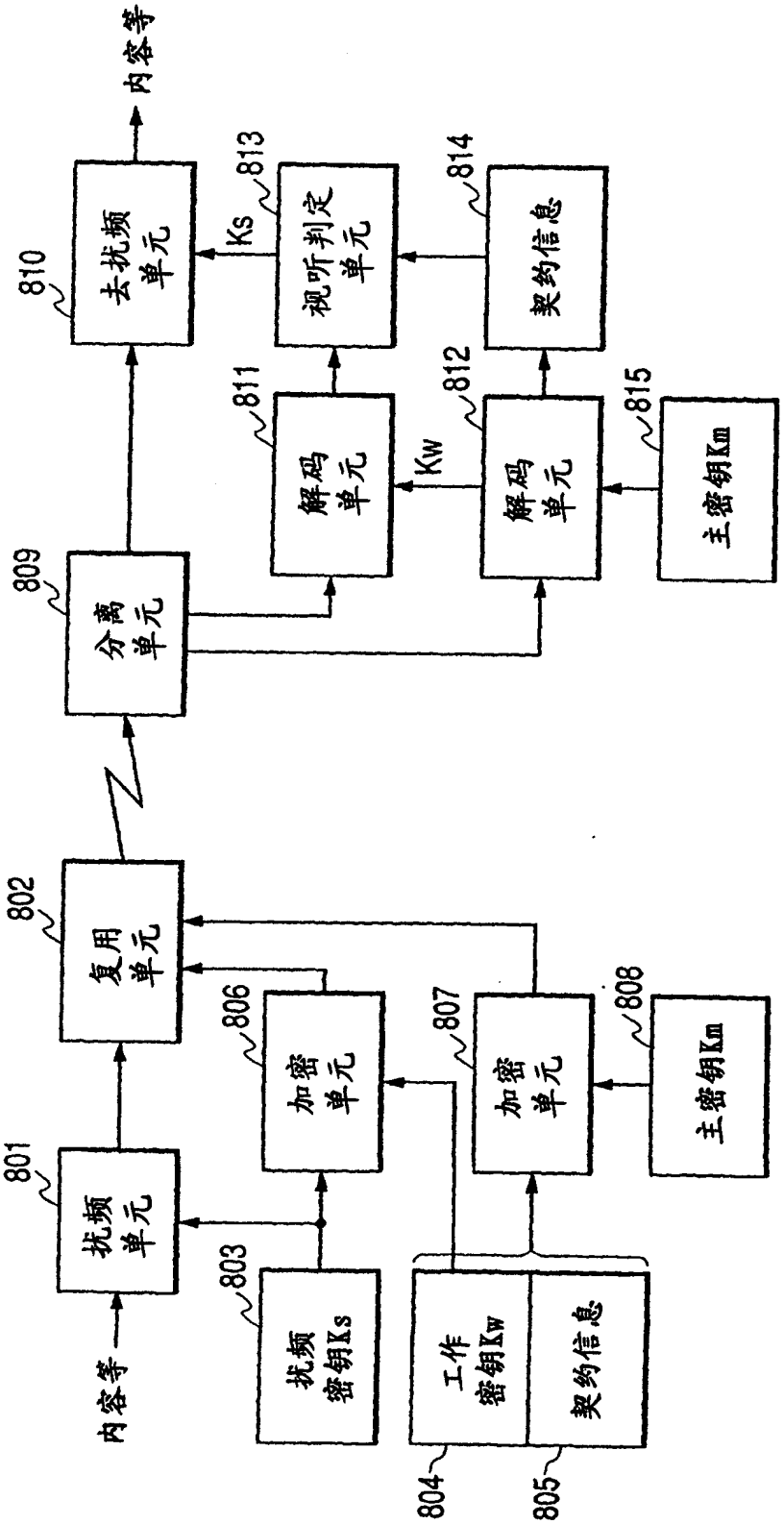
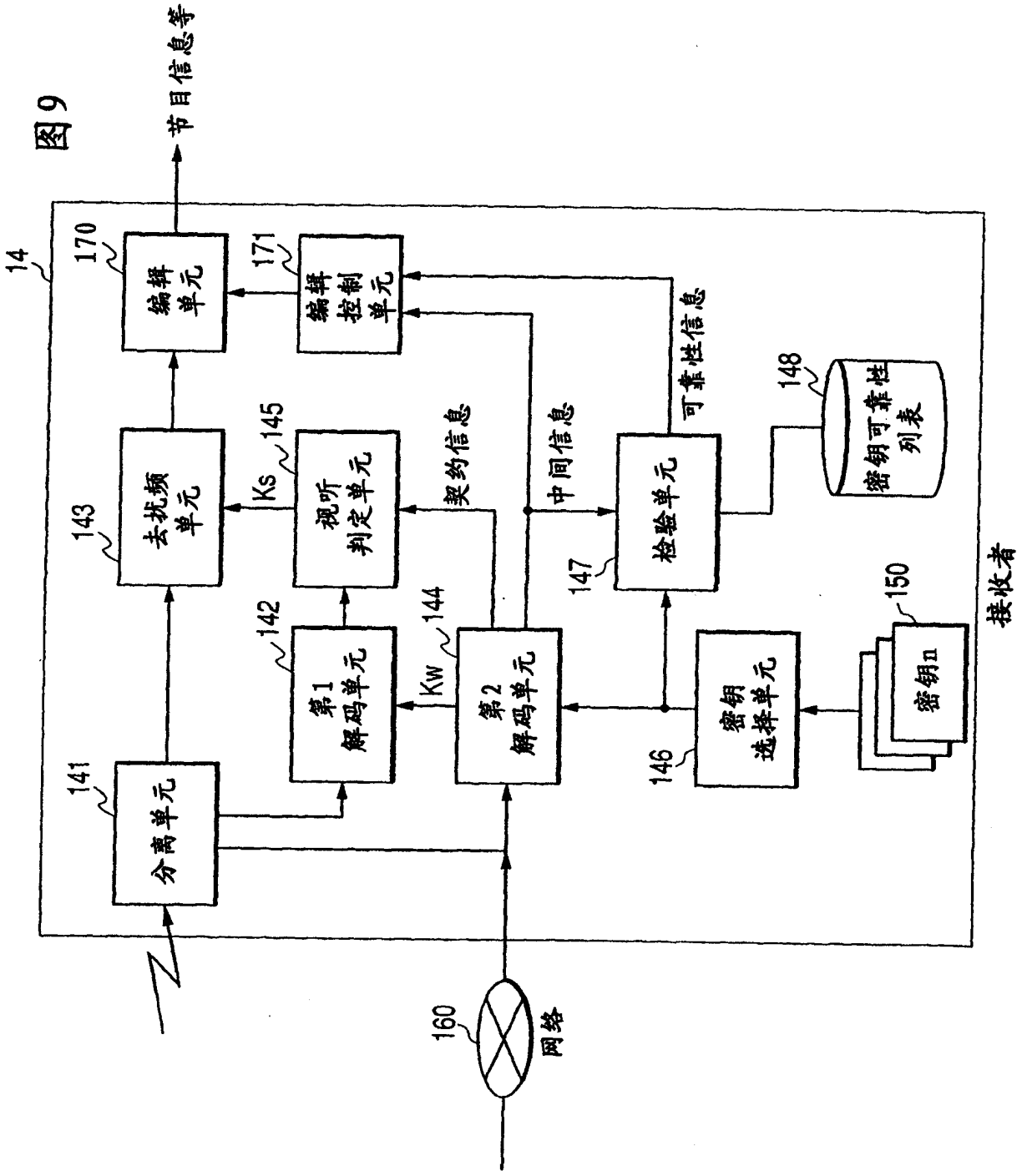

内容等
801
扰频单元
803
扰频密钥Ks
802
复用单元
806
加密单元
807
加密单元
808
主密钥Km
804
工作密钥Kw
805
契约信息
809
分离单元
811
解码单元
Kw
812
解码单元
815
主密钥Km
810
去扰频单元
Ks
813
视听判定单元
814
契约信息
内容等

图 9


节目信息等
14
170
编辑单元
171
编辑控制单元
143
去扰频单元
Ks
145
视听判定单元
契约信息
中间信息
可靠性信息
148
密钥可靠性列表
147
检验单元
142
第1解码单元
Kw
144
第2解码单元
150
密钥n
密钥选择单元
146
141
分离单元
160
网络
接收者