(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101309391 B
(45)授权公告日 2012.07.04

(21)申请号 200810094882.7

(22)申请日 2008.04.25

(30)优先权数据
2007-118253 2007.04.27 JP

(73)专利权人 巴比禄股份有限公司
地址 日本国爱知县名古屋市南区柴田本通四丁目15番地

(72)发明人 山岸良和 高桥良辅 高木义行

(74)专利代理机构 上海市华诚律师事务所 31210
代理人 徐申民

(51)Int.Cl.
H04N 21/4143(2011.01)
H04N 21/426(2011.01)
H04N 21/4367(2011.01)
H04N 5/913(2006.01)

(56)对比文件
CN 2809715 Y,2006.08.23,
CN 2653787 Y,2004.11.03,
CN 1578460 A,2005.02.09,
US 2003/0126455 A1,2003.07.03,
CN 1863305 A,2006.11.15,

审查员 张伟

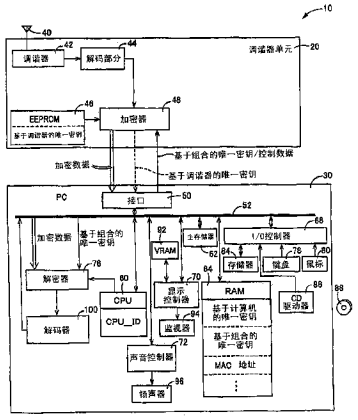
权利要求书 4 页 说明书 15 页 附图 4 页

(54)发明名称

使用加密和解密技术播放广播节目内容的方法

(57)摘要

一种用于播放广播节目内容的方法，包括：(a)产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；以及(b)响应于来自使用者的实时播放指令或者记录视频回放指令的发送，在广播节目内容从调谐器单元传送到计算机单元后实时播放该广播节目内容，或者在从数据存储器取回记录数据后播放记录数据。在说明性实施例中，产生的基于组合的唯一密钥被输出到调谐器单元的加密器用于加密，加密后的数字数据被输入到计算机单元。计算机单元的解密器使用产生的基于组合的唯一密钥解密加密的数字数据。



CN 101309391 B

1. 一种由计算机单元实施的方法，用于在计算机单元允许使用通过接口与计算机单元可拆卸地连接的调谐器单元来观看和／或收听广播节目内容的环境中，播放广播节目内容，

其中，调谐器单元被构成为包括：

无线或有线接收器，被配置为接收代表广播节目内容的广播信号；

加密器，被配置为根据基于指定密钥的算法对接收器接收到的广播信号进行加密，并将加密后的广播信号作为加密数据输出；

密钥存储器，被配置为存储基于调谐器的唯一密钥，该密钥是对调谐器单元唯一的加密密钥，以及

其中，计算机单元被构成为包括：

解密器，被配置为根据基于指定密钥的算法对加密数据进行解密；

数据存储器，被配置为存储数据；以及

播放装置，被配置为播放数据，

该方法包括以下步骤：

产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；以及

响应于使用者发出的实时播放指令，在广播节目内容从调谐器单元传输到计算机单元后，实时播放该广播节目内容，

其中，产生步骤包括：

通过接口从调谐器单元获取基于调谐器的唯一密钥；

获得对于计算机单元是唯一的基于计算机的唯一密钥；以及

从基于调谐器的唯一密钥和基于计算机的唯一密钥产生基于组合的唯一密钥，

播放步骤包括：

响应于实时播放指令的发出，实施产生步骤；

通过接口向加密器输出基于组合的唯一密钥，该密钥由产生步骤的实施而生成；

响应于基于组合的唯一密钥向加密器的输出，通过接口输入已经从加密器输出的加密数字数据；

利用产生的基于组合的唯一密钥，使得解密器试图解密输入的加密数字数据；以及

向播放装置输出由解密器的成功解密而产生的数字数据的解密版本。

2. 一种由计算机单元实施的方法，用于在计算机单元允许使用通过接口与计算机单元可拆卸地连接的调谐器单元来观看和／或收听广播节目内容的情况下，播放广播节目内容，

其中调谐器单元被构成为包括：

无线或有线接收器，被配置为接收代表广播节目内容的广播信号；

加密器，被配置为根据基于指定密钥的算法对接收器接收到的广播信号进行加密，并将加密后的广播信号作为加密数据输出；

密钥存储器，被配置为存储基于调谐器的唯一密钥，该密钥是对调谐器单元唯一的加密密钥，以及

其中，计算机单元被构成为包括：

解密器，被配置为根据基于指定密钥的算法对加密数据进行解密；

数据存储器，被配置为存储数据；以及

播放装置，被配置为播放数据，

该方法包括以下步骤：

产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；

响应于使用者发出的记录指令，将已经从调谐器单元输入的数字数据作为记录数据存储在数据存储器中；以及

响应于使用者发出的记录视频回放指令，在从数据存储器中取回记录数据后，回放记录数据，

其中，产生步骤包括：

通过接口从调谐器单元获取基于调谐器的唯一密钥；

获得对于计算机单元是唯一的基于计算机的唯一密钥；以及

从基于调谐器的唯一密钥和基于计算机的唯一密钥产生基于组合的唯一密钥，

存储步骤包括：

响应于记录指令的发出，实施产生步骤；

通过接口向加密器输出基于组合的唯一密钥，该密钥由产生步骤的实施而生成；

响应于基于组合的唯一密钥向加密器的输出，通过接口输入已经从加密器输出的加密数字数据；

将输入的数字数据作为记录数据存储在数据存储器中，

其中播放步骤包括：

响应于记录视频回放指令的发出，从数据存储器中取回记录数据，并实施产生步骤；

利用作为实施产生步骤的结果产生的基于组合的唯一密钥，使得解密器试图解密输入的取回的记录数据，

向播放装置输出由解密器的成功解密而产生的数字数据的解密版本。

3. 如权利要求 1 所述的方法，其特征在于，所述播放步骤包括：只在与使用者发出的单个实时播放指令相对应的实时播放期间的长度的初始部分的期间，实施产生步骤的步骤，以及保存作为实施产生步骤的结果而产生的基于组合的唯一密钥直到实时播放期间结束的步骤。

4. 如权利要求 1 所述的方法，其特征在于，所述播放步骤包括：只在与使用者发出的单个实时播放指令相对应的实时播放期间的长度的初始部分的期间，周期性地实施产生步骤，从而周期性地产生基于组合的唯一密钥的步骤。

5. 如权利要求 2 所述的方法，其特征在于，所述播放步骤包括：只在与使用者发出的单个记录视频回放指令相对应的记录视频回放期间的长度的初始部分的期间，实施产生步骤的步骤，以及保存作为实施产生步骤的结果而产生的基于组合的唯一密钥直到记录视频回放期间结束的步骤。

6. 如权利要求 2 所述的方法，其特征在于，所述播放步骤包括：只在与使用者发出的单个记录视频回放指令相对应的记录视频回放期间的长度的初始部分的期间，周期性地实施产生步骤，从而周期性地产生基于组合的唯一密钥的步骤。

7. 如权利要求 1 所述的方法，其特征在于，所述计算机单元被构成为具有中央处理单元 CPU 和媒体存取控制器 MAC，

CPU 已经被分配了对于 CPU 是唯一的基于 CPU 的唯一 ID ;

MAC 已经被分配了对于 MAC 是唯一的 MAC 地址 ;

产生步骤包括从基于 CPU 的唯一 ID 和 MAC 地址中的至少一个产生基于计算机的唯一密钥的步骤。

8. 如权利要求 2 所述的方法,其特征在于,所述计算机单元被构成为具有中央处理单元 CPU 和媒体存取控制器 MAC,

CPU 已经被分配了对于 CPU 是唯一的基于 CPU 的唯一 ID ;

MAC 已经被分配了对于 MAC 是唯一的 MAC 地址 ;

产生步骤包括从基于 CPU 的唯一 ID 和 MAC 地址中的至少一个产生基于计算机的唯一密钥的步骤。

9. 如权利要求 1 所述的方法,其特征在于,配制所述广播信号,从而内容信息信号被嵌入广播信号中,该广播信号代表与由广播信号定义的广播节目内容相关的内容信息,

该方法进一步包括确定是否有需要在广播信号从调谐器单元传送到计算机单元之前使加密器加密广播信号的步骤,

该确定步骤包括 :

从广播信号中提取内容信息信号 ;以及

基于提取的内容信息信号确定是否有该需要。

10. 如权利要求 9 所述的方法,其特征在于,所述内容信息信号被配制成包括已经被嵌入到广播信号中的复制管理信息信号,该复制管理信息信号表示关于是否使用者被授权复制广播节目内容的状态,或者使用者被授权复制广播节目内容的次数。

11. 如权利要求 10 所述的方法,其特征在于,所述内容信息信号被配制成包括传输流,并且复制管理信息信号被配制成包括先前已经被嵌入传输流中的复制控制信息 CCI 信号。

12. 如权利要求 9 所述的方法,其特征在于,所述播放步骤包括 :一旦确定不存在该需要时,以非加密格式输入从调谐器单元通过接口输出的数字数据,并将已输入的数字数据输出到播放装置,而不实施产生步骤。

13. 如权利要求 2 所述的方法,其特征在于,配制所述广播信号,从而内容信息信号被嵌入广播信号中,该内容信息信号代表与由广播信号定义的广播节目内容相关的内容信息,

该方法进一步包括确定是否有需要在广播信号从调谐器单元传送到计算机单元之前使加密器加密广播信号的步骤,

该确定步骤包括 :

从广播信号中提取内容信息信号 ;以及

基于提取的内容信息信号确定是否有该需要。

14. 如权利要求 13 所述的方法,其特征在于,所述内容信息信号被配制成包括已经被嵌入到广播信号中的复制管理信息信号,该复制管理信息信号表示关于是否使用者被授权复制广播节目内容的状态,或者使用者被授权复制广播节目内容的次数。

15. 如权利要求 14 所述的方法,其特征在于,所述内容信息信号被配制成包括传输流,并且复制管理信息信号被配制以包括先前已经被嵌入传输流中的复制控制信息 CCI 信号。

16. 如权利要求 15 所述的方法,其特征在于,所述播放步骤包括 :一旦确定不存在该需

要时，以非加密格式输入从调谐器单元通过接口输出的数字数据，并将已输入的数字数据输出到播放装置，而不实施产生步骤。

17. 如权利要求 2 所述的方法，其特征在于，播放步骤包括确定已经存储在数据存储器中的记录数据是否已经被加密，并且，一旦确定记录数据未被加密时，从数据存储器中取回记录数据，并将取回的记录数据输出到播放装置，而不实施产生步骤或使解密器解密记录数据的步骤。

使用加密和解密技术播放广播节目内容的方法

[0001] 相关申请的交叉引用

[0002] 本申请基于并要求享有 2007 年 4 月 27 日提交的在先日本专利申请 2007-118253 号的优先权，其完整内容通过引用结合于本申请中。

[0002] 技术领域

[0003] 本发明主要涉及一种以增强的安全性播放广播节目内容的技术，尤其涉及在计算机单元允许使用通过接口可拆卸地与计算机单元连接的调谐器单元观看和 / 或收听广播节目内容的环境中，播放广播节目内容的改进技术。

[0004] 背景技术

[0004] 近年来，由于卫星或地面广播，数字广播已经变得越来越流行。例如，由卫星广播等发送的数字广播节目以下述方式被观看和 / 或被收听 ：

[0005] 首先，无线电波通过天线被接收，接收到的无线电波通过变频器进行频率变换。其次，在调谐器进行频道选择后，经频率变换的信号被解码。

[0006] 然后，从被解码的信号中提取传输流（下面被称为“MPEG2-TS”），其形式是与 MPEG-2 标准符合的编码比特流。提取的 MPEG2-TS 被格式化以包含多种内容，诸如图像，或者静止图像或者动画，声音或者节目指南。

[0007] 被解码后，MPEG2-TS 进一步被转换成模拟信号，这样允许观看者通过诸如电视监视器或者 LCD（液晶显示器）监视器的图像输出装置和 / 或诸如扬声器的声音输出装置观看和 / 或收听节目内容。

[0008] 另外，近来在个人电脑（下文缩写为“PC”）以可拆卸的方式增加用于接收电视广播的调谐器已普遍起来，从而允许广播节目内容被显示在 PC 的 LCD 显示器上观看，并且允许广播节目内容被记录在诸如 HDD（硬盘驱动器）的存储装置中，该存储装置以内置或者外设的方式与 PC 连接。

[0009] 在数字广播工业中，广播节目内容以数字格式被发送，在信号传播过程中图片和 / 或声音质量没有任何重大衰减。这样更容易完全复制这样的广播节目内容，但是存在版权侵犯的风险。

[0010] 另外，一般对于 PC 来说通过连接比较容易容纳多种外部设备，但存在非法复制 PC 已经接收的广播节目内容的风险。另外，当调谐器和 PC 可拆卸地互相连接时，表示广播节目内容的数据在从调谐器传送到 PC 的过程中，存在通过 PC 的接口被中途截取或窃听的风险。

[0011] 在 PC 从与其可拆卸地连接的调谐器接收广播节目内容之前，已经有将广播节目内容加密以提供版权保护。

[0012] 这种方法借助加密可以防止非法观看和复制广播节目内容，即使在广播节目内容从调谐器传送到 PC 的过程中，表示广播节目内容的数据从具有调谐器的 PC 的接口被窃听。日本专利申请公开号为 2004-173027 的专利揭示了加密广播节目内容的示例性传统技术。

发明内容

[0013] 根据本发明一些方面，提供一种播放广播节目内容的方法，包括：(a) 产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；(b) 响应于使用者发出的实时播放指令或者记录视频回放指令，在广播节目内容从调谐器单元传输到计算机单元后，实时播放该广播节目内容，或者在从数据存储器取回其后回放记录的数据。

[0014] 在说明性实施例中，在示例性的第一步骤，从调谐器单元获得基于调谐器的唯一密钥，其中，基于调谐器的唯一密钥对于调谐器是唯一的，获得基于计算机的唯一密钥，该密钥对于计算机单元是唯一的，从基于调谐器的唯一密钥和基于计算机的唯一密钥产生基于组合的唯一密钥。

[0015] 在示例性的第二步骤，产生的基于组合的唯一密钥被输出到调谐器单元的加密器用于加密，加密的数字数据被输入到计算机单元。加密的数字数据是响应基于组合的唯一密钥输出到加密器而从加密器已经输出的数据。然后，计算机单元的解密器试图使用产生的基于组合的唯一密钥解密输入的加密的数字数据。

[0016] 这里要注意的是，如在说明书中使用的单数形式“一个”和“这个”包括复数的引用，除非上下文明确表示其它含义。还要注意的是术语“包括”，“包含”和“具有”可以互换使用。

附图说明

[0017] 前述的发明内容以及下面本发明较佳实施例的具体描述，当结合附图阅读时将被更好地理解。为了图解本发明的目的，示出了当前较佳的实施例附图。但是，应该理解本发明并不限于示出的准确的配置和手段。在图中：

[0018] 图 1 是概念性图解可适合地实施根据本发明示意性实施例的播放广播节目内容的方法的数字广播接收系统的框图；

[0019] 图 2 是概念性图解传输流 (TS) 的数据结构的立体图；

[0020] 图 3 是概念性地图解图 1 描述的个人电脑 (PC) 执行的广播信号处理程序的流程图；以及

[0021] 图 4 是图解监视器上显示的在图 1 中描述的数字广播接收系统中播放广播节目内容的示例性图像的主视图。

具体实施方式

[0022] 总体概括

[0023] 根据本发明的第一方面，提供由计算机单元实施的方法，用于在计算机单元允许使用通过接口与计算机单元可拆卸地连接的调谐器单元观看和 / 或收听广播节目内容的环境中，播放广播节目内容，

[0024] 其中，调谐器单元被构成为包括：

[0025] 无线或有线接收器，被配置为接收代表广播节目内容的广播信号；

[0026] 加密器，被配置为根据基于指定密钥的算法对接收器接收到的广播信号进行加密，并将加密的广播信号作为加密数据输出；

[0027] 密钥存储器，被配置为存储基于调谐器的唯一密钥，该密钥是对调谐器单元唯一的加密密钥，以及

[0028] 其中，计算机单元被构成为包括：

[0029] 解密器，被配置为根据基于指定密钥的算法对加密数据进行解密；

[0030] 数据存储器，被配置为存储数据；以及

[0031] 播放装置，被配置为播放数据，

[0032] 该方法包括以下步骤：

[0033] 产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；以及

[0034] 响应于使用者发出的实时播放指令，在广播节目内容从调谐器单元传输到计算机单元后实时播放该广播节目内容，

[0035] 其中，产生步骤包括：

[0036] 通过接口从调谐器单元获取基于调谐器的唯一密钥；

[0037] 获得对于计算机单元唯一的基于计算机的唯一密钥；以及

[0038] 从基于调谐器的唯一密钥和基于计算机的唯一密钥产生基于组合的唯一密钥，

[0039] 播放步骤包括：

[0040] 响应于实时播放指令的发出，实施产生步骤；

[0041] 通过接口向加密器输出基于组合的唯一密钥，该密钥由产生步骤的实施而生成；

[0042] 响应于基于组合的唯一密钥向加密器的输出，通过接口输入已经从加密器输出的加密数字数据；

[0043] 利用产生的基于组合的唯一密钥，使得解密器试图解密输入的加密数字数据；以及

[0044] 向播放装置输出由解密器的成功解密而产生的数字数据的解密版本。

[0045] 例如，为了提供具有增强的版权保护的广播节目内容，在广播节目内容通过与计算机单元可拆卸地连接的调谐器被观看的情况下，期望增强从调谐器单元传送到计算机单元的数据的安全性，以允许计算机单元通过调谐器单元接收广播信号的硬件环境或者配置保持不被改变。例如，硬件环境指用于接收广播信号的计算机单元和调谐器单元的硬件组合（即组合的硬件）。

[0046] 进一步地，作为其研究结果，本发明的发明者已经获得这样的发现，为了防止表示广播节目内容的数据从计算机单元的接口被中途截取或窃听，利用与以前产生记录数据相同的调谐器单元和计算机单元的组合，回放以前记录的广播节目内容数据是更有利的。

[0047] 基于上述发现，根据本发明的第一方面的方法用于，在用与计算机单元可拆卸地连接的调谐器单元观看和／或收听广播节目内容的情况下，增强从调谐器单元传送到计算机单元的数据的安全性，和／或用于允许计算机单元通过调谐器单元接收广播信号的硬件环境或者配置保持不被改变。

[0048] 实行根据本发明的第一方面的方法时，调谐器单元这样操作，从而表示广播节目内容的数字数据使用唯一地分配给在那时存在的调谐器单元和计算机单元的组合的加密密钥进行加密，加密的数字数据从调谐器单元被传送到计算机单元。

[0049] 另外，实行本方法时，计算机单元这样操作，从而正要被实时播放的广播节目内容

的加密版本（即将要实时播放的播放中的（on-the-air）节目）使用唯一地分配给在那时存在的调谐器单元和计算机单元的组合的加密密钥进行解密，只要该加密密钥和调谐器单元加密相同的广播节目内容用过的加密密钥是相同的。

[0050] 结果，该方法防止数字数据的加密版本被解密和实时播放，除非发现用于加密数字数据的加密密钥（该密钥被产生以响应于数字数据接收期间调谐器单元和计算机单元的组合）和将被用于试图解密已加密的数字数据的加密密钥（该密钥被产生以响应于实时播放数字数据期间存在的调谐器单元和计算机单元的组合）是相同的。

[0051] 因此，该方法允许调谐器单元和计算机单元的组合，也就是说，计算机单元通过调谐器单元接收广播节目内容和实时播放接收到的内容的硬件环境保持不变。

[0052] 换句话说，该方法保持与用于接收和实时播放广播节目内容的调谐器单元和计算机单元其中之一一起使用的相似装置的特性。

[0053] 结果，该方法使得在接收和实时播放广播节目内容时调谐器单元和计算机单元互相连接是必要的，并允许和调谐器单元与计算机单元其中之一一起使用的相似装置被唯一地确定，而不管调谐器单元和计算机单元已经被设计成允许它们物理上分离的事实。

[0054] 因此，该方法使得增强从调谐器单元传送到计算机单元的数据的安全性更容易，并且，保持计算机单元通过调谐器单元接收广播信号并实时播放接收到的广播信号的硬件环境的特性为同一程度，好像调谐器单元和计算机单元被设计为总是物理上不可分离的，即组合的调谐器／计算机单元。

[0055] 这里使用的术语“计算机单元”可以被解释为例如台式计算机（如个人计算机），便携式计算机（如 PDA（个人数字助理），便携式电话）等，除非这里定义为其他的含义。

[0056] 术语“计算机单元”也可以被解释为例如为不同目的使用计算机作为引擎的多用途装置，为特定目的使用计算机作为引擎的特定用途装置等，除非这里定义为其他的含义。

[0057] 这里使用的术语“广播节目”可以被解释为例如电视广播节目，无线电广播节目等，除非这里定义为其他的含义。

[0058] 根据本发明的第二方面，一种由计算机单元实施的方法，在计算机单元允许使用通过接口与计算机单元可拆卸地连接的调谐器单元观看和／或收听广播节目内容的情况下，播放广播节目内容，

[0059] 其中调谐器单元被构成为包括：

[0060] 无线或有线接收器，被配置为接收代表广播节目内容的广播信号；

[0061] 加密器，被配置为根据基于指定密钥的算法对接收器接收到的广播信号进行加密，并将加密的广播信号作为加密数据输出；

[0062] 密钥存储器，被配置为存储基于调谐器的唯一密钥，该密钥是对调谐器单元唯一的加密密钥，以及

[0063] 其中，计算机单元被构成为包括：

[0064] 解密器，被配置为根据基于指定密钥的算法对加密数据进行解密；

[0065] 数据存储器，被配置为存储数据；以及

[0066] 播放装置，被配置为播放数据，

[0067] 该方法包括以下步骤：

[0068] 产生基于组合的唯一密钥，该密钥对调谐器单元和计算机单元的组合是唯一的；

[0069] 响应于使用者发出的记录指令，将已经从调谐器单元输入的数字数据作为记录数据存储在数据存储器中；以及

[0070] 响应于使用者发出的记录视频回放指令，在从数据存储器中取回记录数据后，回放该记录数据，

[0071] 其中，产生步骤包括：

[0072] 通过接口从调谐器单元获取基于调谐器的唯一密钥；

[0073] 获得对于计算机单元唯一的基于计算机的唯一密钥；以及

[0074] 从基于调谐器的唯一密钥和基于计算机的唯一密钥产生基于组合的唯一密钥，

[0075] 存储步骤包括：

[0076] 响应于记录指令的发出，实施产生步骤；

[0077] 通过接口向加密器输出基于组合的唯一密钥，该密钥由产生步骤的实施而生成；

[0078] 响应于基于组合的唯一密钥向加密器的输出，通过接口输入已经从加密器输出的加密数字数据；

[0079] 将输入的数字数据作为记录数据存储在数据存储器中，

[0080] 其中播放步骤包括：

[0081] 响应于记录视频回放指令的发出，从数据存储器中取回记录的数据，并实施产生步骤；

[0082] 利用作为实施产生步骤的结果产生的基于组合的唯一密钥，使得解密器试图解密输入的取回的记录数据，

[0083] 向播放装置输出由解密器的成功解密而产生的数字数据的解密版本。

[0084] 实行根据本发明的第二方面的方法时，调谐器单元这样操作，从而表示广播节目内容的数字数据使用唯一地分配给在那时存在的调谐器单元和计算机单元的组合的加密密钥进行加密，加密的数字数据从调谐器单元被传送到计算机单元，然后作为记录视频数据被存储到计算机单元中。

[0085] 另外，实行本方法时，计算机单元这样操作，从而以前已经被存储并正要被播放的广播节目内容的加密版本使用唯一地分配给在那时存在的调谐器单元和计算机单元的组合的加密密钥进行解密，只要该加密密钥和调谐器单元加密相同的广播节目内容用过的加密密钥是相同的。

[0086] 结果，该方法防止以前记录的数字数据的加密版本被解密和用于回放记录数据，除非发现用于加密数字数据的加密密钥（该密钥被产生以响应于数字数据记录或存储期间调谐器单元和计算机单元的组合）和将被用于试图解密已加密的数字数据的加密密钥（该密钥被产生以响应于回放记录的数字数据期间调谐器单元和计算机单元的组合）是相同的。

[0087] 因此，该方法允许调谐器单元和计算机单元的组合，也就是说，计算机单元通过调谐器单元接收广播节目内容和记录接收到的广播节目内容以及记录的广播节目内容被回放的硬件环境保持不变。

[0088] 换句话说，该方法保持与用于接收和记录广播节目内容和回放记录的广播节目内容的调谐器单元和计算机单元其中之一一起使用的相似装置的特性。

[0089] 结果，与根据前述发明的第一方面的方法相似，该方法使得在接收和记录广播节

目内容并回放记录的广播节目内容时调谐器单元和计算机单元互相连接是必要的，并允许和调谐器单元与计算机单元其中之一一起使用的相似装置被唯一地确定，而不管调谐器单元和计算机单元已经被设计成允许它们物理上分离的事实。

[0090] 因此，与根据前述发明的第一方面的方法相似，该方法使得增强从调谐器单元传送到计算机单元的数据的安全性更容易，并且，保持计算机单元通过调谐器单元接收和记录广播节目内容并回放记录的广播节目内容的硬件环境的特性为同一程度，好像调谐器单元和计算机单元被设计为总是物理上不可分离的，即组合的调谐器 / 计算机单元。

[0091] 这里使用的术语“记录视频回放”可以被解释为狭义 (narrow sense) 或广义 (broadsense) 的记录视频回放，除非这里定义为其他的含义。

[0092] 术语“狭义 (narrow sense) 的记录视频回放”也可以被解释为例如结束播放中的 (on-the-air) 或实时广播时用记录数据全部回放特定节目的模式，除非这里定义为其他的含义。

[0093] 相反，这里使用的术语“广义 (broad sense) 的记录视频回放”可以被解释为例如所谓的时光平移回放 (time-shift playback)，它是一种这样的模式，即在播放中的 (on-the-air) 广播期间特定节目的播放被临时暂停，然后仅在暂停期间节目被顺序记录，并只有节目的中间部分（例如在暂停期间已经被记录的节目的部分）利用记录的数据被回放。

[0094] 说明性实施例

[0095] 根据本发明，提供下面的模式作为本发明的说明性实施例。

[0096] 根据前述的本发明的第一方面的方法的第一模式，提供一种方法，其中播放步骤包括：只在与使用者发出的单个实时播放指令相对应的实时播放期间的长度的初始部分的期间实施产生步骤，并保存作为实施产生步骤的结果产生的基于组合的唯一密钥直到实时播放期间结束。

[0097] 该方法允许基于组合的唯一密钥只在实时播放期间的长度的初始部分产生，并被保存直到实时播放期间结束。

[0098] 结果，该方法消除或降低了在一系列实时播放期间基于组合的唯一密钥的循环频繁产生的需要。

[0099] 根据前述的本发明的第一方面的方法的第二模式，提供一种方法，其中播放步骤包括：只在与使用者发出的单个实时播放指令相对应的实时播放期间的长度的初始部分的期间周期性地实施产生步骤，从而周期性地产生基于组合的唯一密钥。

[0100] 该方法允许基于组合的唯一密钥在一系列实时播放期间周期性地产生。

[0101] 结果，该方法允许检测不期望的事件，如在一系列实时播放期间已经开始后，调谐器单元和计算机单元物理上互相分离，或者如在一系列实时播放期间已经开始后，实际使用的调谐器单元和计算机单元的组合的特性已经被改变。

[0102] 这个方法可以以示例性的方式实行，一旦这种不期望的事件被检测到，实时播放的当前循环就被终止。

[0103] 根据前述的本发明的第二方面的方法的第三模式，提供一种方法，其中播放步骤包括：只在与使用者发出的单个记录视频回放指令相对应的记录视频回放期间的长度的初始部分的期间实施产生步骤，并保存作为实施产生步骤的结果产生的基于组合的唯一密钥

直到记录视频回放期间结束。

[0104] 该方法允许基于组合的唯一密钥只在记录视频回放期间的长度的初始部分产生，并被保存直到记录视频回放期间结束。

[0105] 结果，该方法消除或降低了在一系列记录视频回放期间基于组合的唯一密钥的循环频繁产生的需要。

[0106] 根据前述的本发明的第二方面的方法的第四模式，提供一种方法，其中播放步骤包括：只在与使用者发出的单个记录视频回放指令相对应的记录视频回放期间的长度的初始部分的期间周期性地实施产生步骤，从而周期性地产生基于组合的唯一密钥。

[0107] 该方法允许基于组合的唯一密钥在一系列实时播放期间周期性地产生。

[0108] 结果，该方法允许检测不期望的事件，如在一系列记录视频回放期间已经开始后，调谐器单元和计算机单元物理上互相分离，或者如在一系列记录视频回放期间已经开始后，实际使用的调谐器单元和计算机单元的组合的特性已经被改变。

[0109] 这个方法可以以示例性的方式实行，一旦这种不期望的事件被检测到，记录视频回放的当前循环就被终止。

[0110] 根据前述的本发明的第一或第二方面的方法的第五模式，或者前述第一到第四模式中的任何一个模式，提供一种方法，其中计算机单元被构成为具有 CPU（中央处理单元）和 MAC（媒体存取控制器），

[0111] CPU 已经被分配了对于 CPU 来说是唯一的基于 CPU 的唯一 ID；

[0112] MAC 已经被分配了对于 MAC 来说是唯一的 MAC 地址；

[0113] 产生步骤包括从基于 CPU 的唯一 ID 和 MAC 地址中的至少一个产生基于计算机的唯一密钥的步骤。

[0114] 该方法允许利用以前已经被分配给计算机单元的基于 CPU 的唯一 ID 和 MAC 地址中的至少一个产生基于计算机的唯一密钥，该密钥代表计算机单元的特性。

[0115] 利用基于 CPU 的唯一 ID 和 MAC 地址产生基于计算机的唯一密钥，将使得定义计算机的特性更容易，比仅利用基于 CPU 的唯一 ID 和 MAC 地址中的一个产生基于计算机的唯一密钥更精确。利用基于 CPU 的唯一 ID 和 MAC 地址产生基于计算机的唯一密钥，将使得用更强的确定性保持播放广播节目内容（例如在彼此电连接中使用的调谐器单元和计算机单元的组合）的硬件环境的特性。

[0116] 根据前述的本发明的第一或第二方面的方法的第六模式，或者前述第一到第五模式中的任何一个模式，提供一种方法，其中，配制广播信号，从而内容信息信号被嵌入广播信号中，该内容信息信号代表与由广播信号定义的广播节目内容相关的内容信息，

[0117] 该方法进一步包括确定是否有需要在广播信号从调谐器单元传送到计算机单元之前使加密器加密广播信号的步骤，

[0118] 该确定步骤包括：

[0119] 从广播信号中提取内容信息信号；以及

[0120] 基于提取的内容信息信号确定是否有该需要。

[0121] 根据第六模式的方法的第七模式，提供一种方法，其中内容信息信号被配制以包括已经被嵌入到广播信号中的复制管理信息信号，该复制管理信息信号表示关于是否使用者被授权复制广播节目内容的状态，或者使用者被授权复制广播节目内容的数量和次数。

[0122] 根据第七模式的方法的第八模式，提供一种方法，其中广播信号被配制以包括传输流，并且复制管理信息信号被配制以包括先前已经被嵌入传输流中的 CCI（复制控制信息）信号。

[0123] 根据第六到第八模式中的任何一个的方法的第九模式，提供一种方法，其中播放步骤包括：一旦确定不存在该需要时，以非加密格式输入从调谐器单元通过接口输出的数字数据，并将已输入的数字数据输出到播放装置，而不实施产生步骤。

[0124] 根据本发明第二方面，第三模式或者第四模式的方法的第十模式，提供一种方法，其中，回放步骤包括确定已经存储在数据存储器中的记录数据是否已经被加密，并且，当确定记录数据已经被加密时，从数据存储器中取回记录数据，并输出取回的记录数据到播放装置，而不实施产生步骤或使解密器解密记录数据的步骤。

[0125] 根据本发明的第十一模式，提供一种计算机可执行程序，当由计算机执行时，实现根据第一和第二方面以及第一到第十模式的任何一个的方法。

[0126] 当由计算机执行时，该程序根据与第一和第二方面以及第一到第十模式的任何一个的方法基本相同的原则，提供基本相同的功能和效果。

[0127] 术语“程序”可以被解释为不仅包括计算机执行的以完成程序的功能的一组指令，而且包括根据指令要被处理的相关文件，数据等。

[0128] 另外，术语“程序”可以被解释为例如，由计算机独自执行获得目的用途的程序，或者由计算机执行和另一个程序或其它程序一起获得目的用途的程序。在后一种情况下，术语“程序”可以主要被构建为数据。

[0129] 根据本发明的第十二模式，提供一种计算机可读介质，其中存储了计算机可执行程序，当由计算机执行时，实施根据本发明的第十一模式的方法。

[0130] 已经存储在该介质中的程序，当由计算机执行时，根据与第一和第二方面以及第一到第十模式的任何一个的方法基本相同的原则，提供基本相同的功能和效果。

[0131] 说明书中表述的“计算机可读介质”可以以多种类型的任何一种实现，包括例如软盘的磁记录介质，例如 CD 和 CD-ROM 的光记录介质，例如 MO 的光磁记录介质，例如 ROM 的不可擦除存储器。

[0132] 根据本发明的第十三模式，提供与调谐器可拆卸地连接的，通过接口允许广播节目内容被观看和 / 或被收听的计算机单元，

[0133] 其中，调谐器单元被构成为包括：

[0134] 无线或有线接收器，被配置为接收代表广播节目内容的广播信号；

[0135] 加密器，被配置为根据基于指定密钥的算法对接收器接收到的广播信号进行加密，并作为加密数据输出加密的广播信号；

[0136] 密钥存储器，被配置为存储基于调谐器的唯一密钥，其是对调谐器单元唯一的加密密钥，以及

[0137] 其中，计算机单元被构成为包括：

[0138] 解密器，被配置为根据基于指定密钥的算法对加密数据进行解密；

[0139] 数据存储器，被配置为存储数据；

[0140] 播放装置，被配置为播放数据；

[0141] 密钥产生器，被配置为产生基于组合的唯一密钥，该密钥是对调谐器单元和计算

机单元的组合唯一的；以及

[0142] 实时播放处理器，响应于使用者发出的实时播放指令，被配置为在广播节目内容从调谐器单元传送到计算机单元后实时播放该广播节目内容，

[0143] 其中，密钥产生器被配置为实施：

[0144] 通过接口从调谐器单元获取基于调谐器的唯一密钥；

[0145] 获得对于计算机单元唯一的基于计算机的唯一密钥；以及

[0146] 从基于调谐器的唯一密钥和基于计算机的唯一密钥，产生基于组合的唯一密钥，

[0147] 实时播放处理器被配置为实施：

[0148] 响应于实时播放指令的发出，激活密钥产生器；

[0149] 通过接口向加密器输出由密钥产生器产生的基于组合的唯一密钥；

[0150] 响应于基于组合的唯一密钥向加密器的输出，通过接口输入已经从加密器输出的加密数字数据；

[0151] 利用产生的基于组合的唯一密钥，使解密器试图解密输入的加密数字数据；以及

[0152] 向播放装置输出由解密器成功解密产生的数字数据的解密版本。

[0153] 本发明的当前较佳实施例中的一个将参考附图被详细描述，其中相同的数字始终用于表示相似的元件。

[0154] 图 1 是根据本发明的一个说明性实施例构造的数字广播接收系统（下文简称为“接收系统”）10 的框图。

[0155] 接收系统 10 被构成为包括调谐器单元 20 和个人计算机（下文简称为“PC”）30。在这点上，PC 30 构成计算机单元的例子。

[0156] 调谐器单元 20 和 PC 30 被设计成电气上互相连接并一起使用。在例子中，调谐器单元 20 被与 PC 30 分开购买并可拆卸地加载到 PC 30 上。更具体地，调谐器单元 20 的 USB（通用串行总线）连接器（未图示）被可拆卸地插入 PC 30 的 USB（通用串行总线）端口中。

[0157] 调谐器单元 20 和 PC 30 被期望在使用中（例如播放或者记录）保持互相连接，这样，组合的特性可以被保持不变，用于提供例如具有充分版权保护的广播节目内容。

[0158] 但是，调谐器单元 20 和 PC 30 在物理上互相分开。这样，在本实施例中，调谐器单元 20 和 PC 30 被设计为执行特殊信号处理，以防止使用者在播放电视节目或者视频文件期间有意地分开调谐器单元 20 和 PC 30，以及在播放电视节目或者视频文件期间有意地丢失组合的特性。

[0159] 结果，在播放电视节目或者先前记录的视频文件期间，调谐器单元 20 和 PC 30 被处理，好像调谐器单元 20 和 PC 30 被整体形成或者被形成为一个单元。

[0160] 调谐器单元 20 适合于无线接收代表数字广播节目内容的广播信号。因此，如图 1 所示，调谐器单元 20 被构成为包括天线 40，调谐器 42 以及解码器 44，如公知的。

[0161] 天线 40 适用于接收从用于数字广播的广播站或者广播卫星发射的无线电波，并将接收到的无线电波的信号发射到调谐器 42。

[0162] 调谐器单元 42 适用于通过天线 42 接收数字广播信号然后调谐到期望的频道。更具体地，调谐器 42 调谐到运载并广播代表使用者期望的节目的数字广播信号其中之一的频道，并将该接收到的信号传送给解码器 44。

[0163] 解码器 44 适用于对已经从调谐器 42 传送的并且先前已经以预定方式被调制的信号执行 A/D 转换，然后数字地解码转换好的信号。解码器 44 进一步适用于纠正传送路径中发生的误码等，并产生（如果需要，进一步解码）符合运动图像专家组 2(MPEG-2) 标准的传输流（下文简称“TS”）。该标准和“TS”在美国专利号 7,095,945 中已经被公布，其通过引用被全文结合在此。

[0164] “TS”和视频信息，音频信息，诸如节目指南信息等的附加信息由用于提供数字广播节目的广播站产生，其中每个信息都被压缩成数字信息，并按照 MPEG-2 标准被多路传输。

[0165] 图 2 概念地说明“TS”的数据结构。“TS”是多个包排列的数据序列的形式，每个包称为传输流包（下文简称“TS 包”），具有 188 字节的固定长度。

[0166] 以多个 TS 包的形式的“TS”构成为包括打包基本流 (PES, Packetized ElementaryStream) 包和称为“节 (section)”的包。

[0167] 在每个 PES 包中，存储了表示诸如视频信息（视频），音频信息（音频）或数据的节目内容的编码流。另外，在每个节 (section) 中存储有标识内容类型（例如关于是音频还是视频的类型）的信息，电子节目指南 (EPG)，鉴别广播公司的信息，复制控制信息 (CCI) 信号等。

[0168] CCI 信号是用于限制使用者（如电视观众）被授权复制每个广播内容的次数的信息。更具体地，CCI 信号被格式化以包括关于广播公司是否授权使用者复制节目内容的信息，以及另外包括关于在广播公司授权使用者复制广播内容的情况下使用者被授权复制广播内容的次数的信息。

[0169] 如图 1 所示，调谐器单元 20 被构成为另外包括 EEPROM（电可擦除只读存储器）46，以及加密器 48。

[0170] 在本实施例中，EEPROM 46，作为非易失性存储器的例子，其中已经存储了基于调谐器的唯一密钥，该密钥对于调谐器单元 20 是唯一的。基于调谐器的唯一密钥由制造调谐器单元 20 的制造商在调谐器单元 20 售出前存储。

[0171] 众所周知，加密器 48 根据基于指定的加密密钥（在本实施例中，如后文更详细地描述，加密密钥由 PC 30 指定）的算法，加密从解码器 44 输入的“TS”（以数字数据形式），并将加密的数据传输给 PC 30。

[0172] 更详细地，在加密之前，加密器 48 从解码器 44 输入的“TS”中提取 CCI 信号。然后，加密器 48 确定提取的 CCI 信号表示使用者未被授权还是仅被授权一次复制当前广播节目内容，从而确定是否需要加密代表当前广播节目内容的数字数据。仅当加密器 48 确定需要加密时，加密器 48 加密数字数据并将代表广播节目内容的加密的数字数据传输到 PC 30。

[0173] 更详细地，如图 1 所示，加密器 48 响应来自 PC 30 的请求的发送，从 EEPROM46 中取回基于调谐器的唯一密钥，并将取回的基于调谐器的唯一密钥传输到 PC 30。进一步地，加密器 48 从 PC 30 接收基于组合的唯一密钥及控制数据。基于组合的唯一密钥和控制数据将在下文详细描述。

[0174] 另外，加密器 48 利用基于组合的唯一密钥完整作为保护密钥，或者利用唯一地分配给基于组合的唯一密钥的密钥作为保护密钥，加密从解码器 44 输入的“TS”（数字数据），

然后将加密密钥输出到 PC 30。

[0175] 如图 1 所示，PC 30 被构成为包括接口（例如符合 USB 2.0 标准）50 和总线 52，如公知的。

[0176] 前述的加密数据和基于调谐器的唯一密钥从调谐器单元 20 通过接口 50 被传输到 PC 30。加密防止使用者未被授权地观看和收听以及复制数据，即使接口 50 中的数据（表示广播节目内容的数字数据）被窃取。前述基于组合的唯一密钥和控制数据通过接口 50 从 PC 30 传输到调谐器单元 20。

[0177] 如图 1 所示，PC 30 被构成为包括：作为处理器的 CPU（中央处理单元）60；存储操作程序或者应用程序的非易失性存储器（例如硬盘驱动存储器）62；易失性 RAM（随机存取存储器）64；I/O 控制器 68；显示控制器 70；声音控制器 72；和解密器 76，前述部件都和总线 52 连接。

[0178] 如图 1 所示，CPU 60 之前已经存储了 CPU_ID。CPU_ID 作为对于各个 CPU 60 唯一的密钥。在主存储器 62 中，存储了多种程序，以图 3 中的流程图中概念性所示的广播信号处理程序为首。

[0179] 在 RAM 64 中，存储了基于计算机的唯一密钥，其对于各个 PC 30 是唯一的密钥，前述的基于组合的唯一密钥，以及 MAC（媒体存取控制器）地址。基于组合的唯一密钥，如前所述，是对于各个调谐器 20 和各个 PC 30 的组合唯一的密钥，各 PC 30 已与各调谐器 20 电气连接。

[0180] I/O 控制器 68 连接有：键盘 78 和鼠标 80，各自作为输入装置；用于存储记录视频等的存储器 84；以及 CD 驱动器 86。例如，CD 驱动器 86 被用于从之前已经存储了广播信号处理程序的 CD-ROM 88 读取前述广播信号处理程序并在 PC 30 中安装读取的广播信号处理程序。

[0181] 显示控制器 70 连接有：用于暂时存储视频信息（视频数据）的 VRAM（视频随机存取存储器）92，以及监视器（如 LCD）94。视频信息（视频数据）通过监视器 94 被呈现给使用者。图 4 示出显示在监视器 94 上的显示屏的例子，以允许使用者通过监视器 94 输入来观看电视节目。

[0182] 如图 1 所示，声音控制器 72 连接有扬声器 96，通过扬声器 96 音频信息（音频数据）被呈现给使用者。

[0183] 使解密器 76 试图利用作为加密密钥的指定的基于组合的唯一密钥，解密代表广播节目内容的数字数据的加密版本。

[0184] 只有在曾用于加密代表广播节目内容的数字数据的加密密钥和将用于解密相同的数字数据的当前基于组合的唯一密钥一致时，解密器 76 适用于进行成功地解密代表广播节目内容的数字数据的加密版本。代表广播节目内容的数字数据的解密版本被格式化以包括视频数据、音频数据和电子节目指南信息，所有这些如前所述。

[0185] 另外，在曾用于加密代表广播节目内容的数字数据的加密密钥和将用于解密相同的数字数据的当前基于组合的唯一密钥不一致时，进一步地，解密器 76 不适用于进行成功地解密代表广播节目内容的数字数据的加密版本。

[0186] 如图 1 所示，在 PC 30 中，解码器 100 连接到总线 52 和解密器 76。解码器 100 从解密器 76 接收数字数据。解码器 100 被构成为允许解密器 76 提供的数字数据以视频数据

和音频数据的原始形式存储。存储的视频数据通过总线 52 被传输到显示控制器 70，而存储的音频数据通过总线 52 被传输到音频控制器 72。

[0187] 接着参考图 3，前述的广播信号处理程序将被更详细地描述。在描述之前，将参考图 4 描述用于播放电视节目的显示屏幕 110，其中显示屏幕 110 响应于 PC 30 中的广播信号处理程序的激活被显示在监视器 94 上。

[0188] 如图 4 所示，用于播放电视节目的显示屏幕 110 被构成为包括视频显示区 112 和设置面板区 114。

[0189] 在视频显示区 112 中，显示有使用者实时观看的电视节目的图像，和 / 或先前记录的视频文件的图像。

[0190] 另外，设置面板区 114 允许使用者设置系统或者改变设置。在设置面板区 114 中，显示有“设置”按钮 120 和“频道设置”按钮 122。

[0191] “设置”按钮 120 被使用者按下（例如选择使用鼠标 80 或者键盘 78 上的光标键）以显示允许使用者输入用于播放电视节目的期望设置的屏幕或者画面。另外，“频道设置”按钮 122 被使用者操作以显示允许使用者设置或者选择传送使用者期望的电视节目的频道的屏幕或画面。

[0192] 如图 4 所示，在设置面板区 114 中，另外显示有“频道改变”按钮 124，“记录”按钮 126，“时光平移 (time-shift)”按钮 128，“回放”按钮 130 和“停止”按钮 132。

[0193] “频道改变”按钮 124 由使用者按下，用于允许使用者改变用户期望的电视节目的频道。“记录”按钮 126 由使用者按下，用于允许使用者开始记录用户期望的电视节目。

[0194] “时光平移”按钮 128 由使用者按下，用于开始以缩短的时间记录当前观看的电视节目的部分，从而执行时光平移回放（即改变时间回放）。一旦时光平移回放模式开始，实况转播的或者播放中的 (on-the-air) 电视节目被暂停，同时被连续地记录，然后从暂停点回放相同的电视节目。该时光平移回放模式被公开在美国专利号 7,095,945 中，其通过引用被全文结合在此。

[0195] “回放”按钮 130 由使用者按下，用于开始回放先前记录的视频文件的模式，其中该模式被定义为包括记录的视频回放（其表示通常用于狭义的先前记录的视频回放）和前述的时光平移回放。

[0196] “停止”按钮 132 由使用者按下，用于停止当前选择的实时播放（即实时播放和观看播放中的 (on-the-air) 电视节目的模式），记录视频回放和时光平移回放中的一个。

[0197] 如图 4 所示，在设置面板区 114 中，“电视”按钮 134 和“视频”按钮 136 被另外显示。

[0198] “电视”按钮 134 由使用者按下，用于执行实时播放以实时观看选择的播放中的 (on-the-air) 电视节目，或记录选择的播放中的 (on-the-air) 电视节目。另外，“视频”按钮 136 由使用者按下，用于回放先前记录的视频文件（包括在时光平移回放期间产生的视频文件），这就是说，用于执行选择的记录视频回放和时光平移回放中的一个。

[0199] 接下来，再参考图 3，前述的广播信号处理程序将被描述。

[0200] 广播信号处理程序，其响应于使用者的动作而被激活，从步骤 S1 开始从 CPU 60 获得 CPU_ID，以及从 RAM 64 获得 MAC 地址。MAC 地址在 PC 30 通电后获得并随后存储在 RAM 64 中。

[0201] 接下来，在步骤 S2，基于计算机的唯一密钥被产生，该密钥对于获得的 CPU_ID 和 MAC 地址的组合是唯一的。在一个例子中，基于计算机的唯一密钥通过用表示 CPU_ID 的数字串和表示 MAC 地址的数字串产生。该产生的基于计算机的唯一密钥被存储在 RAM64 中。

[0202] 然后，在步骤 S3，基于调谐器的唯一密钥从调谐器单元 20 被获得，PC 30 和调谐器单元 20 连接。

[0203] 接着，在步骤 S4，基于组合的唯一密钥被产生，该密钥对于当前基于计算机的唯一密钥和当前基于调谐器的唯一密钥的组合是唯一的。在一个例子中，基于组合的唯一密钥通过用表示基于计算机的唯一密钥的数字串和表示基于调谐器的唯一密钥的数字串产生。该产生的基于组合的唯一密钥被存储在 RAM 64 中，直到执行广播信号处理程序的当前循环结束。

[0204] 然后，在步骤 S5，对关于是否使用者选择的模式等于用于实时观看的实时播放模式或者用于以后观看的记录模式作出判断。如果是，那么步骤 S6 接着通过设置面板区 114 输入使用者已经定义的设置和当前模式。在一个例子中，设置包括使用者期望的电视节目的频道。

[0205] 随后，在步骤 S7 中，前述控制数据被产生用于传输到调谐器 20。控制数据被产生以包括指示调谐器单元 20 开始接收表示播放中的 (on-the-air) 电视节目的广播信号的指令，以及指定调谐器单元 20 选择的频道号码的命令。产生的控制数据被传输到调谐器单元 20。

[0206] 然后，在步骤 S8，对于选择的频道，PC 30 从调谐器单元 20 接收对于所选频道已经被调谐器单元 20 接收的表示广播节目内容的数字数据作为“TS”。

[0207] 随后，在步骤 S9，PC 30 从调谐器单元 20 获得当前 CCI 信号。然后，在步骤 S10，对关于获得的 CCI 信号表示当前广播节目内容根本未被授权复制还是表示当前广播节目内容仅被授权复制一次作出判断，从而确定是否需要用调谐器单元 20 对表示当前广播节目内容的数字数据加密。

[0208] 如果需要用调谐器单元 20 进行加密，那么在期望的加密之前，步骤 S10 接着从 RAM 64 取回基于组合的唯一密钥并将它传送到调谐器单元 20。然后，在步骤 S12，PC 30 从调谐器单元 20 接收已经由调谐器单元 20 使用基于组合的唯一密钥加密的数字数据。

[0209] 然后，在步骤 S13，对关于当前模式是否等于记录模式作出判断。如果是的话，那么步骤 S14 接着将接收到的加密数据存储在存储器 84 中。接着是步骤 S17。

[0210] 相反，如果当前模式不等于记录模式，那么步骤 S15 接着将当前基于组合的唯一密钥输出到解密器 76，另外输出信号到解密器 76，用于指示解密器 76 试图用输出的基于组合的唯一密钥对表示当前广播节目内容的加密的数字数据进行解密。

[0211] 接着，在步骤 S16，解码器 100 接收解密器 76 的输出信号（例如，不要求解密的信号，已经成功解密的信号，或者未能成功解密的信号）。

[0212] 在上述两种情况的任何一种情况下，步骤 S17 接着判断用户是否按下了“停止”按钮 132 或者“频道改变”按钮 124。如果是的话，那么执行该广播信号处理程序的一个循环结束；然而，如果不是的话，那么接着进行步骤 S5。

[0213] 虽然上文已经描述了该广播信号处理程序在需要由调谐器单元 20 进行加密时执行的操作，但是当不需要由调谐器单元 20 加密时，该广播信号处理程序也被执行，这样步

骤 S18 被实施以判断是否当前模式等于记录模式。如果是的话，随后进行步骤 S14，但是如果否的话，那么步骤 S16 接着将调谐器单元 20 已经输出的信号（即，未被加密的数字数据）传输到解码器 100。

[0214] 如前述的操作中，解码器 100 将表示广播节目内容的数字数据复原 (restore) 到视频数据和音频数据的原始格式。复原的视频数据通过总线 52 被传输到显示控制器 70，而复原的音频数据通过总线 52 被传输到声音控制器 72。

[0215] 虽然上文已经描述了该广播信号处理程序在当前模式等于实时播放模式或者记录模式时执行的操作，但是在当前模式不等于实时播放模式或者记录模式时，该广播信号处理程序也被执行，这样步骤 S19 被实施以判断当前模式是否等于记录视频回放模式。

[0216] 如果当前模式等于记录视频回放模式，那么步骤 S20 接着从存储器 84 取回数字数据（即先前的记录视频文件）作为记录视频数据。接着，在步骤 S21，通过参考取回的记录视频数据，判断记录视频数据是否是加密数据。

[0217] 如果取回的记录视频数据是加密数据，那么接着步骤 S22 从 RAM 64 获取基于组合的唯一密钥，以向解密器 76 输出获得的基于组合的唯一密钥作为加密密钥，并指示解密器 76 试图解密取回的记录视频数据。

[0218] 随后，步骤 S16 接着将解密器 76 的输出信号传送到解码器 100。

[0219] 但是，如果取回的记录视频数据不是加密数据，那么跳过步骤 S22，进入到步骤 S16。

[0220] 虽然上文已经描述了该广播信号处理程序在当前模式等于记录视频回放模式时执行的操作，但是在当前模式不等于记录视频回放模式时，该广播信号处理程序也被执行，这样，步骤 S23 被实施以判断是否使用者按下了用于进行时光平移回放的“时光平移”按钮 128。

[0221] 如果是的话，那么接着步骤 S24 执行时光平移回放的子程序（未显示）。更具体地，如果使用者按下“时光平移”按钮 128，那么与步骤 S6-S16 相等同的步骤以与选择记录模式时相似的方式被实施。

[0222] 广播节目内被顺序地存储在进行时光平移回放所用的存储器（例如高速缓冲存储器，虽然未显示）中，直到使用者后来按下“回放”按钮 130。该存储器与用于记录模式的存储器是分开的。

[0223] 最后，如果使用者按下“回放”按钮 130，那么与步骤 S20-S22 等同的步骤依次以与选择记录视频回放模式时使用的方式相似的方式被实施。但是，在等同于 S20 的步骤中，所期望的广播节目内容被从上述用于时光平移回放的存储器取回。

[0224] 如果步骤 S24 的实施结束，那么随后进行步骤 S17。

[0225] 从前述解释很显然的是，对于本实施例，可以认为为了说明的目的，PC 30 构成本发明的第一和第二方面的每一个中的“计算机单元”的例子，调谐器 42 构成本发明的第一和第二方面的每一个中的“接收器”的例子，加密器 48 构成本发明的第一和第二方面的每一个中的“加密器”的例子，存储器 84 构成本发明的第一和第二方面的每一个中的“数据存储器”的例子，监视器 94 和扬声器 96 构成本发明的第一和第二方面的每一个中的“播放装置”的例子。

[0226] 进一步地，对于本实施例，可以认为为了说明的目的，步骤 S1-S12 和步骤 S14-S17

构成本发明的第一方面中的“实时播放广播节目内容的步骤”的例子，步骤 S1-S4 构成本发明的第一方面中的“产生基于组合的唯一密钥的步骤”的例子。

[0227] 进一步地，对于本实施例，可以认为为了说明的目的，步骤 S1-S18 构成本发明的第二方面的“回放步骤”的例子，步骤 S1-S4 构成本发明的第二方面的“产生基于组合的唯一密钥的步骤”的例子。

[0228] 进一步地，对于本实施例，可以认为为了说明的目的，图 3 所示的广播信号处理程序构成根据本发明前述第十一模式的“程序”的例子，CD-ROM 88 构成根据前述第十二模式的“介质”的例子。

[0229] 在不脱离本发明概念的情况下，本领域的技术人员可以对前述实施例作各种改变。因此，可以理解本发明并不被限于公布的具体实施例，而可以覆盖后附的权利要求定义的在本发明的精神和范围内的任何变型。

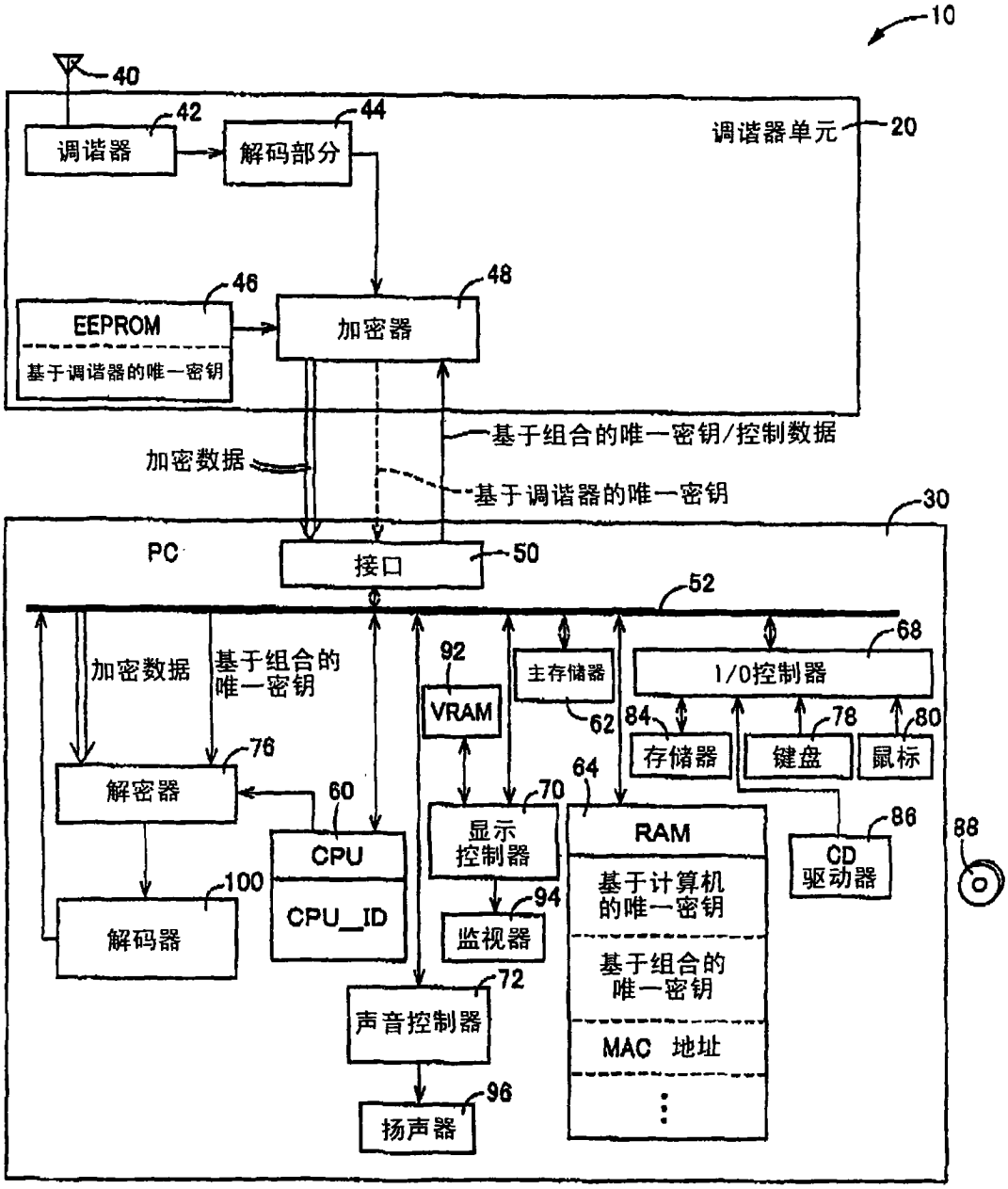

10
40
42
调谐器
44
解码部分
调谐器单元
20
46
EEPROM
基于调谐器的唯一密钥
48
加密器
基于组合的唯一密钥/控制数据
加密数据
基于调谐器的唯一密钥
30
PC
接口
50
52
加密数据
基于组合的唯一密钥
92
VRAM
主存储器
62
I/O控制器
68
84
存储器
78
键盘
80
鼠标
76
解密器
60
CPU
CPU_ID
64
显示控制器
70
RAM
基于计算机的唯一密钥
基于组合的唯一密钥
MAC 地址
86
CD驱动器
88
100
解码器
94
监视器
72
声音控制器
96
扬声器

图 1

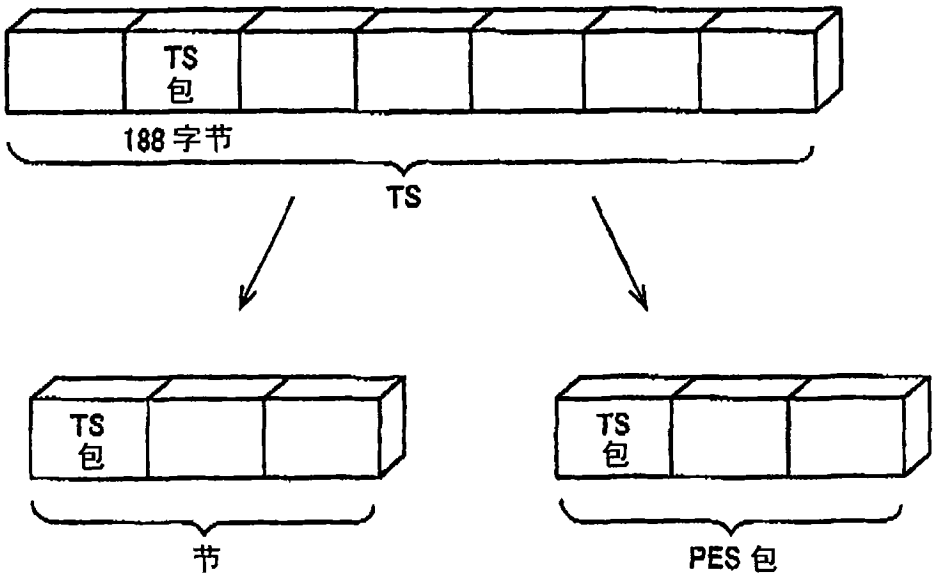


图 2

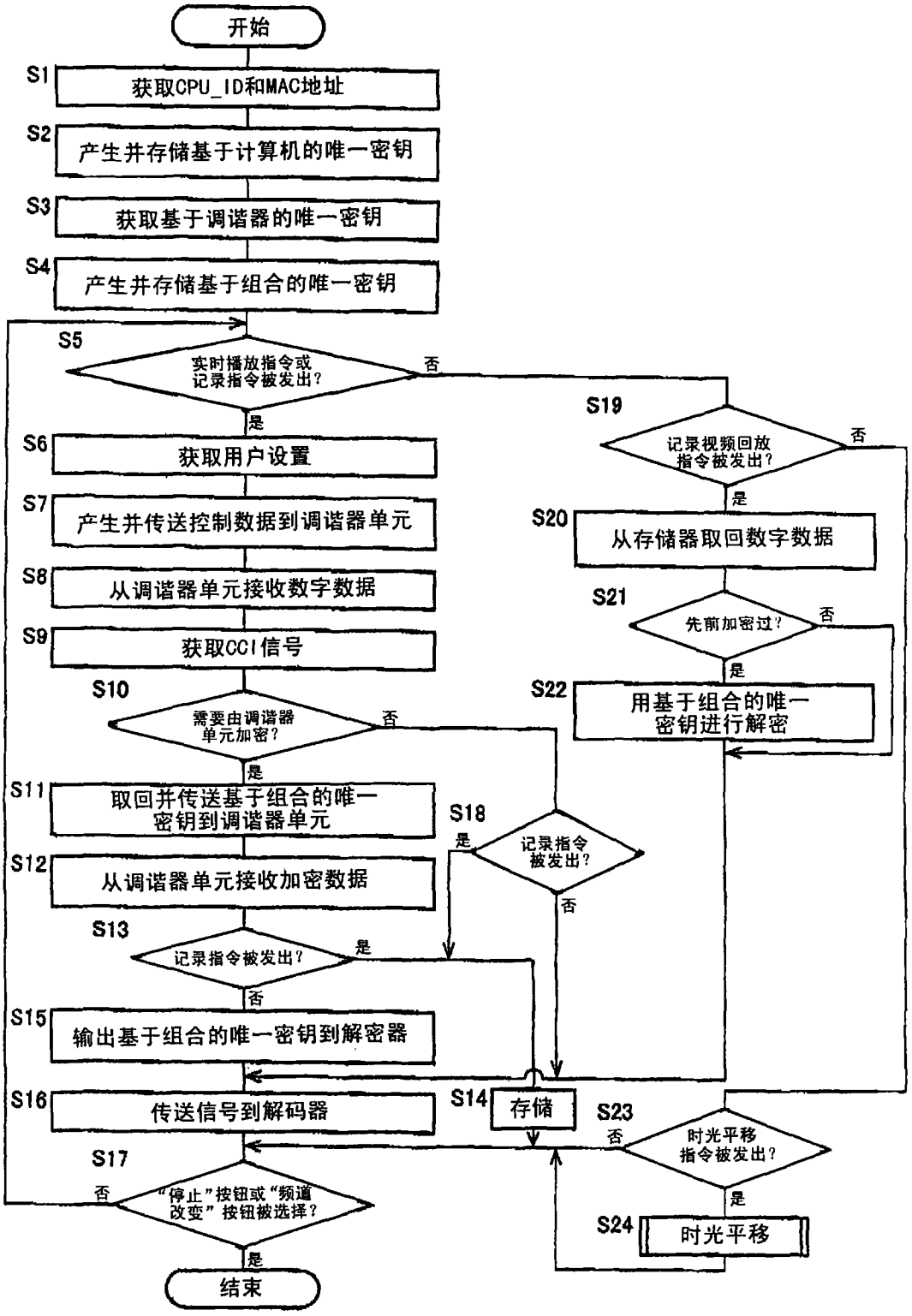

开始
S1
获取CPU_ID和MAC地址
S2
产生并存储基于计算机的唯一密钥
S3
获取基于调谐器的唯一密钥
S4
产生并存储基于组合的唯一密钥
S5
实时播放指令或记录指令被发出?
否
是
S6
获取用户设置
S7
产生并传送控制数据到调谐器单元
S8
从调谐器单元接收数字数据
S9
获取CCI信号
S10
需要由调谐器单元加密?
否
是
S11
取回并传送基于组合的唯一密钥到调谐器单元
S12
从调谐器单元接收加密数据
S13
记录指令被发出?
是
否
S15
输出基于组合的唯一密钥到解密器
S16
传送信号到解码器
S17
"停止"按钮或"频道改变"按钮被选择?
否
是
结束
S18
记录指令被发出?
是
否
S14
存储
S19
记录视频回放指令被发出?
否
是
S20
从存储器取回数字数据
S21
先前加密过?
否
是
S22
用基于组合的唯一密钥进行解密
S23
时光平移指令被发出?
否
是
S24
时光平移

图 3

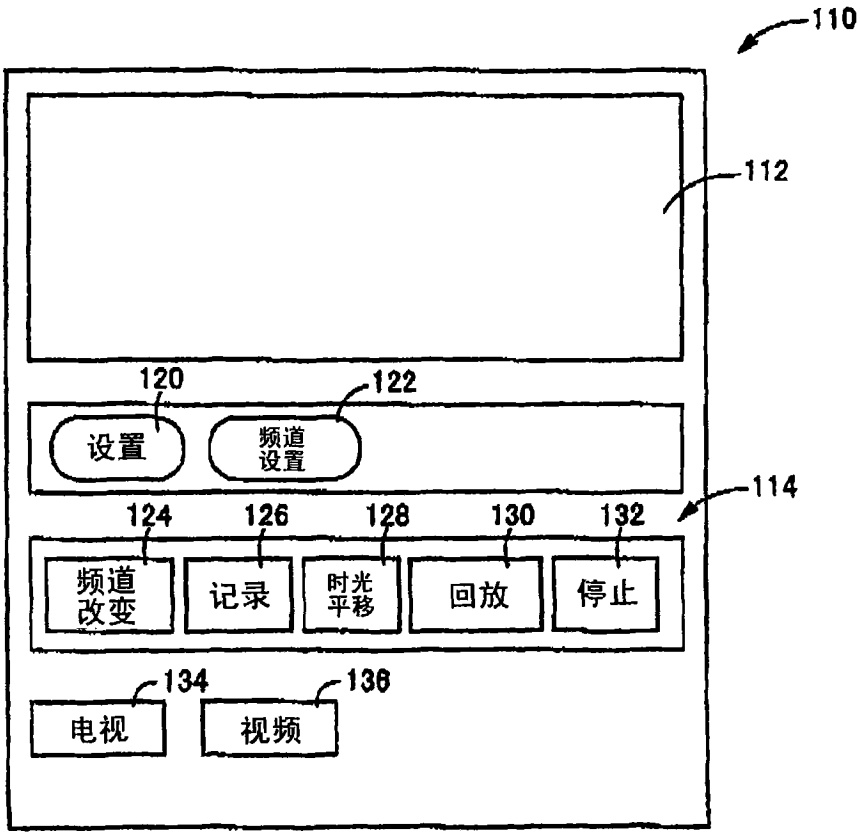

110
112
120
122
设置
频道
设置
114
124
126
128
130
132
频道
改变
记录
时光
平移
回放
停止
134
136
电视
视频

图 4