



(12) 发明专利

(10) 授权公告号 CN 102682812 B

(45) 授权公告日 2015. 09. 09

(21) 申请号 201210135488. X

G11B 20/00(2006. 01)

(22) 申请日 2006. 10. 30

H04N 5/913(2006. 01)

H04N 5/92(2006. 01)

(30) 优先权数据

2005-371299 2005. 12. 26 JP

(56) 对比文件

CN 1318941 A, 2001. 10. 24, 说明书第 2 页第 1 行至第 10 页第 27 行、附图 1-8.

CN 1182268 A, 1998. 05. 20, 全文.

US 2003/0077074 A1, 2003. 04. 24, 全文.

(62) 分案原申请数据

200610142747. 6 2006. 10. 30

(73) 专利权人 日立麦克赛尔株式会社

地址 日本大阪府

审查员 糜增元

(72) 发明人 野口敬治 柴田晃 小松茂

小川敦史 梅田五郎

(74) 专利代理机构 北京尚诚知识产权代理有限

公司 11322

代理人 龙淳

(51) Int. Cl.

G11B 20/10(2006. 01)

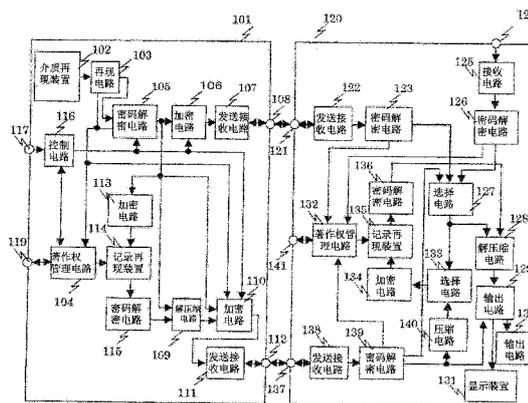
权利要求书2页 说明书7页 附图3页

(54) 发明名称

记录再现装置和记录再现方法、记录装置和记录方法

(57) 摘要

本发明提供一种记录再现装置和记录再现方法、记录装置和记录方法。在采用特定的国家与日美欧标准不同的加密方式的情况,采用不同的加密方式的 AV 信息所记录的介质与再现装置之间无法进行 AV 信息再现。同样采用不同的加密方式的 AV 信息的输出装置与输入装置之间也无法进行 AV 信息的交接。具有不同的 RC 的记录介质与记录介质装置之间也无法进行 AV 信息的再现。本发明提供一种能够连接具有不同的加密方式的机器间的方法和装置,和实现使具有不同的 RC 和密码的记录介质的再现成为可能的机器的新的 RC 方法和装置。也就是说,提供一种如果是著作权人许可的使用条件,与所销售的地域无关的许可的 AV 信息在许可的机器上可以再现的方法与再现装置。



1. 一种图像语音信息记录再现装置, 其对图像语音信息进行记录再现, 该图像语音信息的拷贝利用拷贝管理信息被管理, 该图像语音信息记录再现装置的特征在于, 包括:

再现机构, 其从第一记录介质再现记录于所述第一记录介质的所述图像语音信息;

记录机构, 其将所述再现机构从所述第一记录介质再现的所述图像语音信息记录到第二记录介质; 和

管理机构, 其对将所述再现机构从所述第一记录介质再现的所述图像语音信息向所述记录机构中的所述第二记录介质的记录进行管理, 其中

所述管理机构,

在记录于所述第一记录介质的所述图像语音信息的拷贝根据所述拷贝管理信息被禁止的情况下,

用所述图像语音信息附带的关于管理装置的信息与所述管理装置进行通信, 将所述图像语音信息记录再现装置具有的许可证信息发送到所述管理装置, 向所述管理装置申请所述图像语音信息的拷贝许可,

在从所述管理装置获得了所述图像语音信息的拷贝许可时, 使得能够将所述再现机构从所述第一记录介质再现的所述图像语音信息记录到所述第二记录介质。

2. 如权利要求 1 所述的图像语音信息记录再现装置, 其特征在于:

所述再现机构具有输出机构, 该输出机构输出所述再现机构从所述第一记录介质再现的所述图像语音信息。

3. 一种记录再现方法, 其为对图像语音信息进行记录再现的图像语音信息记录再现装置的记录再现方法, 该图像语音信息的拷贝利用拷贝管理信息被管理, 该记录再现方法的特征在于, 包括:

从第一记录介质再现记录于所述第一记录介质的所述图像语音信息,

在记录于所述第一记录介质的所述图像语音信息的拷贝根据所述拷贝管理信息被禁止的情况下,

用所述图像语音信息附带的关于管理装置的信息与所述管理装置进行通信, 将所述图像语音信息记录再现装置具有的许可证信息发送到所述管理装置, 申请所述图像语音信息的拷贝许可,

在从所述管理装置获得了所述图像语音信息的拷贝许可时, 使得能够将从所述第一记录介质再现的所述图像语音信息记录到第二记录介质。

4. 如权利要求 3 所述的记录再现方法, 其特征在于:

输出从所述第一记录介质再现的所述图像语音信息。

5. 一种图像语音信息记录装置, 其将图像语音信息记录到记录介质, 该图像语音信息的拷贝利用拷贝管理信息被管理, 该图像语音信息记录装置的特征在于, 包括:

接收机构, 其接收所述图像语音信息;

记录机构, 其将所述接收机构接收到的所述图像语音信息记录到所述记录介质; 和

管理机构, 其对将所述接收机构接收到的所述图像语音信息向所述记录机构中的所述记录介质的记录进行管理, 其中

所述管理机构,

在接收到的所述图像语音信息的拷贝根据所述拷贝管理信息被禁止的情况下,

用所述图像语音信息附带的关于管理装置的信息与所述管理装置进行通信,将所述图像语音信息记录装置具有的许可证信息发送到所述管理装置,向所述管理装置申请所述图像语音信息的拷贝许可,

在从所述管理装置获得了接收到的所述图像语音信息的拷贝许可时,使所述记录机构能够将接收到的所述图像语音信息记录到所述记录介质。

6. 一种记录方法,其为将图像语音信息记录到记录介质的图像语音信息记录装置的记录方法,该图像语音信息的拷贝利用拷贝管理信息被管理,该记录方法的特征在于,包括:

接收所述图像语音信息,

在接收到的所述图像语音信息的拷贝根据所述拷贝管理信息被禁止的情况下,

用所述图像语音信息附带的关于管理装置的信息与所述管理装置进行通信,将所述图像语音信息记录装置具有的许可证信息发送到所述管理装置,向所述管理装置申请所述图像语音信息的拷贝许可,

在从所述管理装置获得了接收到的所述图像语音信息的拷贝许可时,使得能够将接收到的所述图像语音信息记录到所述记录介质。

7. 一种图像语音信息记录装置,其将图像语音信息记录到记录介质,该图像语音信息记录装置的特征在于,包括:

接收机构,其接收所述图像语音信息;

记录机构,其将所述接收机构接收到的所述图像语音信息记录到所述记录介质;和

管理机构,其对将所述接收机构接收到的所述图像语音信息向所述记录机构中的所述记录介质的记录进行管理,其中

所述管理机构,

在接收到的所述图像语音信息的记录被禁止的情况下,

用所述图像语音信息附带的关于管理装置的信息与所述管理装置进行通信,将所述图像语音信息记录装置具有的许可证信息发送到所述管理装置,向所述管理装置申请所述图像语音信息的记录许可,

在从所述管理装置获得了接收到的所述图像语音信息的记录许可时,使所述记录机构能够将接收到的所述图像语音信息记录到所述记录介质。

记录再现装置和记录再现方法、记录装置和记录方法

[0001] 本案是申请日为 2006 年 10 月 30 日、申请号为 200610142747.6、发明名称为“信息处理方法和信息处理装置”的专利申请的分案申请。

技术领域

[0002] 本发明涉及记录再现装置和记录再现方法、记录装置和记录方法。

背景技术

[0003] 作为本技术领域的背景技术,有例如非专利文献 1。在本文献中,有记载“(1)内容加密:使用标题密钥、盘密钥、主密钥三层加密密钥加密 MPEG 压缩后的内容。仅受到许可的依据 CSS 的 DVD 机器可以解密、再现。(2)总线认证:进行 PC 系统中的 DVD-ROM 驱动器与 MPEG 解密器模块的相互认证。防止来自 PC 总线的不正当拷贝”。此外,作为其他背景技术,有非专利文献 2~4。

[0004] [非专利文献 1]National Technical Report Vol.43 No.3 Jun.1997(第 339 页—341 页)

[0005] [非专利文献 2]Digital Transmission Content Protection Specification Volume 1 (Informational Version) Revision 1.3, January,2004 published from Digital Transmission Licensing Administrator, LLC. (<http://www.dtcp.com>)

[0006] [非专利文献 3]DTCP Volume 1 Supplement E Mapping DTCP to IP (Informational Version) Revision 1.0, November 24,2003 published from Digital Transmission Licensing Administrator, LLC. (<http://www.dtcp.com>)

[0007] [非专利文献 4]High-Definition Multimedia Interface Specification Version 1.1, May 20,2004 published from HDMI Licensing, LLC, (<http://www.hdmi.org>) High-bandwidth Digital Content Protection System Revision 1.1, June 9,2003 published from Digital Content Protection LLC. (<http://www.digital-cp.com>)

发明内容

[0008] 本发明涉及遵循因国家等各地域而不同的著作权的考虑方式,管理 AV 信息的著作权,以便超越国界在各国欣赏以电影等为代表的由图像与声音构成的 AV 信息的方法和装置。

[0009] 在 1996 年登场的 DVD 中虽然根据电影公司的要求与各国的关于电影的习惯的不同,采用被称为 Regional Coding (区域编码,以下 RC)的著作权管理方法,但是存在其后的市场的变化和电影公司的电影发行战略的变化,现行的 RC 成为问题多的状况。此外,对作为著作权管理的主要技术的加密技术而言,也有像中华人民共和国这样在国务院令第 273 号(1999/10/7)中的“国家认可加密方式”,也可能需要针对每个地域改变加密方式。涉及 AV 信息的著作权管理的加密方式有 DVD-CSS、DVD-CPRM、DTCP、DTCP-IP、HDMT & HDCP、Display Port(显示器端口)、UDI 等,有必要针对各个地域改变这些加密方式的全部或者一

部分。再者,对上述 DVD-CSS、DTCP、DTCP-IP、HDMI & HDCP 而言,希望参考非专利文献。

[0010] 在特定的国家采用与日美欧标准不同的加密方式的情况下,在采用不同的加密方式的 AV 信息所记录的介质与再现装置之间无法再现 AV 信息。同样采用不同的加密方式的 AV 信息的输出装置与输入装置间也无法进行 AV 信息的交换。具有不同的 RC 的记录介质与记录介质再现装置之间也无法再现 AV 信息。

[0011] 本发明提供一种能够连接上述具有不同的加密方式的机器间的方法和装置,和实现使具有不同的 RC 和密码的记录介质的再现成为可能的机器的新的 RC 方法和装置。也就是说在于提供一种如果是著作权人许可的使用条件,与所销售的地域无关的被许可的 AV 信息在被许可的机器上可以再现的方法与再现装置。

[0012] 总之,目的在于提高信息处理装置的使用方便性。

[0013] 上述目的通过权利要求书中所述的发明可以实现。

[0014] 根据本发明,可以提高信息处理的方便性。

附图说明

[0015] 图 1 是连接本发明的介质的再现装置与本发明的电视装置的实施例。

[0016] 图 2 是本发明中使用的密码解密电路 105 的实施例。

[0017] 图 3 是本发明中使用的加密电路 106 的实施例。

[0018] 图 4 是本发明中使用的加密电路 110 的实施例。

[0019] 标号的说明

[0020] 101 :再现装置,102 :介质再现装置,103 :再现电路,104 :著作权管理电路,105 :密码解密电路,106 :加密电路,107 :发送接收电路,108 :外部端子,109 :解压缩电路,110 :加密电路,111 :发送接收电路,112 :外部端子,113 :加密电路,114 :记录再现装置,115 :密码解密电路,116 :控制电路,117 :输入端子,119 :因特网连接端子,120 :电视装置,121 :外部端子,122 :发送接收电路,123 :密码解密电路,124 :天线端子,125 :接收电路,126 :密码解密电路,127 :选择电路,128 :解压缩电路,129 :输出电路,130 :扬声器,131 :显示装置,132 :著作权管理电路,133 :选择电路,134 :加密电路,135 :记录再现装置,136 :密码解密电路,137 :外部端子,138 :发送接收电路,139 :密码解密电路

具体实施方式

[0021] 图 1 是本实施例的 DVD 和 Blu-ray、HD DVD 等 AV 信息所记录的介质的再现装置 101,和显示在该再现装置中被再现的 AV 信息的电视装置 120。

[0022] 102 是 DVD、Blu-ray、HD DVD 的介质再现装置,输出包括被数据压缩的信号、RC 信号、拷贝管理信号 :Copy Generation Management 信号(以下称为 CGM 信号)的信号组数据。该信号组数据由再现电路 103 解码,修正错误,RC 信号与 CGM 信号输入到著作权管理电路 104,数据压缩信号输入到密码解密电路 105。

[0023] 密码解密电路 105 解密 DVD 的 40bit 密钥长密码,Blu-ray 与 HD DVD 中共用的 128bit 密钥长密码这两种密码。密码解密电路 105 将被数据压缩的 AV 信息供给到外部端子 108 用加密电路 106、对被压缩的 AV 信息进行解压缩的解压缩电路 109、以及第二外部端子 112 用加密电路 110。

[0024] 除解压缩电路 109 的输出信号之外,密码解密电路 105 的输出信号与来自再现电路 103 的 RC 信号、CGM 信号被输入到加密电路 110。在加密电路 110 中该三个输入信号时分多路复用后以 40bit 或 56bit 密钥长或者 128bit 密钥长加密,经由发送接收电路 111 从外部端子 112 输出。

[0025] 在介质再现装置 102 再现中国标准的预录介质(prerecorded media)的情况下,从再现电路 103 输出的 CGM 信号中包含“是否对从外部端子 112 输出的信号进行加密的指示信息”,如果该信息指示加密则进行 128bit 密钥长的加密,如果信息未指示加密则不进行加密,而将时分多路复用信号传递到发送接收电路 111。

[0026] 在介质再现装置 102 再现现有的 DVD 介质和 Blu-ray 介质的情况下,加密电路 110 始终进行加密。

[0027] 作为密码解密电路 105 的输出的被压缩的 AV 信息输入到具有规定的保密能力的加密方式固定的加密,例如 56bit 或 128bit 密钥长的加密电路 113,被加密后,记录于 HDD 和非易失性半导体存储器等的内置记录再现装置 114。在记录再现装置 114 再现模式的情况下,记录再现装置 114 的输出信号被密码解密电路 115 解密后,输入到解压缩电路 109,在解压缩电路 109 中该输入信号优先于来自密码解密电路 105 地被解压缩。

[0028] 再现装置 101 具有与采用因使用地域而不同的加密方式的著作权管理系统对应的状况。在再现装置 101 中设置有输入使用地域信息的端子 117,从 117 输入的使用地域信息输入到控制电路 116,控制电路 116 控制与因使用地域而不同的著作权管理系统对应的著作权管理电路 104、密码解密电路 105、加密电路 106、加密电路 110。

[0029] 例如如果发送地为日美欧,则在产品出厂时,外部端子 108 依据 DHCP-IP 标准,加密电路 106 的加密方式设定成 128bit 密钥长的 AES 方式,外部端子 112 依据 HDMI 标准而加密电路 110 的加密方式设定成 40bit 或 56bit 密钥长的 HDCP,介质再现装置 102 依据 DVD 与 Blu-ray 或 HD DVD 标准,密码解密电路 105 的解密方式在 DVD 再现时设定成 40bit 密钥长 CSS 方式,在 Blu-ray 或 HD DVD 再现时设定成 128bit 密钥长 AACS 方式。加密电路 106 的输出信号经由发送接收电路 107 到达外部端子 108。加密电路 110 的输出信号经由发送接收电路 111 到达外部端子 112。

[0030] 而且,由于加密电路 113 与密码解密电路 115 为记录再现装置 114 专有使用,所以可以选择与再现装置 101 的使用地域无关的特定的加密方式。在著作权管理电路 104 中,在产品出厂时设定对应于发送地的 RC。

[0031] 再现装置 101 具有因特网连接端子 119,来自著作权管理网站的著作权控制信息经由因特网发送到著作权管理电路 104。来自再现电路 103 的 RC 信号、CGM 信号也输入到著作权管理电路 104。

[0032] 在将密码解密电路 105 的输出信号记录在记录再现装置 114 中的情况下,从再现电路 103 输出的 CGM 信号输入到著作权管理电路 104,在该 CGM 信号许可“Copy Free(免费拷贝)”、“Copy Once (拷贝一次)”、“Move (移除)”和再现期间限制记录的情况下,著作权管理电路 104 按照该记录条件记录控制记录再现装置 114。即使在该 CGM 信号“Copy Never (不得拷贝)”等禁止拷贝的情况下,如果经由因特网取得来自著作权管理者的拷贝许可则著作权管理电路也记录控制记录再现装置 114。

[0033] 也就是说,如果用户要记录禁止拷贝的 AV 信息,则著作权管理电路 104 自动地经

由因特网按照包含与该 AV 信息对应的 CGM 信号的信息向著作权管理网站传达从再现装置 101 具有的该著作权管理者得到的许可取得信息并且申请拷贝许可。该著作权管理网站将再现装置 101 确认为许可取得产品,赋予内置于该再现装置 101 的记录再现装置 114 正常记录或再现期间限制记录的权利。如果经由因特网从著作权管理网站送出记录许可,则记录再现装置 114 据此开始记录。

[0034] 电视装置 120 中具有由天线端子 124、接收电路 125、密码解密电路 126、解压缩被压缩的 AV 信息恢复到原来的 AV 信号的解压缩电路 128、AV 信号的输出电路 129、扬声器 130、显示装置 131 构成的对应于数字广播的电视功能。

[0035] 电视装置 120 具有依据 DTCP-IP 标准的外部端子 121,输入到外部端子 121 的被压缩的 AV 信号与 CGM 信号经由发送接收电路 122 和密码解密电路 123,输入到选择电路 127。

[0036] 电视装置 120 具有依据 HDMI 标准的外部端子 137,输入到外部端子 137 的被压缩的 AV 信号与非压缩的 AV 信号和 CGM 信号经由 HDMI 的发送接收电路 138 与密码解密电路 139,非压缩 AV 信号输入到 AV 输出电路 129,压缩 AV 信号输入到选择电路 127,CGM 信号输入到著作权管理电路 132。

[0037] 由选择电路 127 选择的压缩 AV 信号之一输入到解压缩电路 128,另一个输入到选择电路 133。压缩密码解密电路 139 的输出信号中的非压缩 AV 信号的压缩电路 140 的输出信号也输入到选择电路 133。

[0038] 电视装置 120 还内置有由加密电路 134、HDD 等记录再现装置 135、密码解密电路 136 构成的记录再现功能。选择电路 133 的输出信号被加密电路 134 加密后记录在记录再现装置 135 中。在记录再现装置 135 的再现模式下,记录再现装置 135 的输出信号被密码解密电路 136 解密,输入到 AV 信号解压缩电路 128,恢复成非压缩信号,经由输出电路 129 到达扬声器 130、显示装置 131。

[0039] 电视装置 120 具有因特网连接端子 141,来自著作权管理者的著作权控制信息经由因特网发送到著作权管理电路 132。来自密码解密电路 123、126、139 的各个 CGM 信号也输入到著作权管理电路 132。

[0040] 在将密码解密电路 123、126、139 的输出信号分别记录在记录再现装置 135 中的情况下,从解密电路 123、126、139 输出的 CGM 信号输入到著作权管理电路 132,该 CGM 信号许可“Copy Free”、“Copy Once”、“Move”和再现期间限制记录的情况下,著作权管理电路 132 按照该记录条件记录控制记录再现装置 135。即使在该 CGM 信号为“Copy Never”等禁止拷贝的情况下,如果经由因特网取得来自著作权管理者的拷贝许可,则著作权管理电路记录控制记录再现装置 135。

[0041] 也就是说,如果用户要记录禁止拷贝的 AV 信息,则著作权管理电路 132 自动地经由因特网按照包含与该 AV 信息对应的 CGM 信号的信息向著作权管理网站传达从再现装置 120 具有的该著作权管理者得到的许可取得信息并且申请拷贝许可。该著作权管理网站将电视装置 120 确认为许可取得产品,赋予内置于该电视装置 120 的记录再现装置 135 正常记录或再现期间限制记录的权利。如果经由因特网从著作权管理网站发出记录许可,则记录再现装置 135 据此开始记录。

[0042] 接下来,对电视装置 120 是面向中国的产品,再现装置 101 是面向日美欧出产的产品,在中国如图 1 所示连接的情况进行说明。电视装置 120 希望选择再现装置 101 的

DTCP-IP 外部端子 108 的输出信号的情况,在再现装置 101 的发送接收电路 107 与电视装置 120 的发送接收电路 122 之间进行通信,由于发送接收电路 122 将电视装置 120 搭载的加密方式为中国标准(128bit 密钥长)的情况传达到发送接收电路 107,所以发送接收电路 107 判别成电视装置采用中国标准的 DTCP-IP 加密方式,将加密电路 106 的加密方式切换到中国标准的加密方式,电视装置 120 以该中国方式加密想要的 AV 信息,从外部端子 108 发送到电视装置 120 的外部端子 121。

[0043] 同样,电视装置 120 希望选择 HDMI 外部端子 112 的输出信号的情况,在再现装置 101 的发送接收电路 111 与电视装置 120 的发送接收电路 138 之间进行通信,通过该通信发送接收电路 111 判别成电视装置采用中国标准的 HDMI 加密方式(128bit 密钥长),将加密电路 110 的加密方式从日美欧标准的 40bit 或 56bit 密钥长切换到中国标准的 128bit 密钥长的加密方式,电视装置 120 以中国方式加密想要的 AV 信息而从外部端子 112 发送到电视装置 120 的外部端子 137。

[0044] 接下来,对面向美国出产的再现装置 101 在中国国内再现在中国国内和美国销售的预录介质的情况进行说明。在中国国内销售的预录介质采用中国标准的加密方式和与中国对应的 RC,在美国销售的预录介质采用日美欧标准的加密方式和与美国对应的 RC。如果由介质再现装置 102 再现在中国销售的预录介质,则从再现电路 103 读出 RC 信号和 CGM 信号,该信号由著作权管理电路 104 分析,判别成 RC 为中国地域和加密方式为中国方式。由于介质与装置的 RC 不同,所以再现装置显示“由于 RC 不同所以无法再现”等,用户通过遥控器等操作模块从输入端子 117 经由控制电路 116 向著作权管理电路 104 发出指令,将再现装置 101 的 RC 从美国切换到中国地区,并且将密码解密电路 105 的方式从依据日美欧标准切换到依据中国标准,由此使再现成为可能。

[0045] 控制电路 116 在著作权管理电路 104 中插入有证明 ID 编号等关于著作权的许可取得的信息,如上所述在中国使用面向美国出产的产品,的情况下,如果将外部端子 119 经由因特网连接到著作权管理网站,进行证明许可取得的信息,和将 RC 从美国变更成中国地域的请求,则也可以是该网站切换 RC 或加密方式或者许可美国与中国双方的 RC 的状况。从著作权管理网站许可美中两国的 RC 后,著作权管理电路 104 可以按照从预录介质再现的 RC,自动地切换再现装置 101 的 RC。

[0046] 对于再现装置 101 的加密电路 106、110 的加密方式的切换也是与 RC 的切换同样按照遥控器等用户操作和著作权管理电路 104 的判别结果,使加密电路 106、110 的加密方式的默认与 RC 和密码解密电路 105 联动而从日美欧方式切换到中国方式。

[0047] 接下来,说明在再现装置 101 的加密电路 110 没有中国标准的加密方式的情况下,电视装置 120 希望选择依据 HDMI 的外部端子 112 的输出信号的情况。如前所述,在 HDMI 发送接收电路 111 与 126 之间进行相互通信,发送接收电路 138 与密码解密电路 139 判别成来自外部端子 112 的输出信号的 HDMI 方式是日美欧方式,将密码解密电路 139 的加密方式选择成 40bit 或 56bit 密钥长方式进行解密。

[0048] 图 2 表示本实施例中使用的密码解密电路 105。来自再现电路 103 已加密的 AV 信号输入到信号处理电路 201,并且从控制电路 116 表示该已加密的 AV 信号的加密方式是 40bit 密钥长的 CSS 还是 128bit 密钥长的 AAC 的信号输入到密码密钥生成电路 202 和信号处理电路 201 以及数据加密电路 203。

[0049] 在来自控制电路 116 的输入信号表示 40bit 密钥长的情况下,信号处理电路 201 以 128bit 单位将信号供给到数据加密电路 203,密码密钥生成电路 202 也将 40bit 的数据密码密钥信号供给到数据加密电路 203,数据加密电路 203 将已解密的 AV 信号供给到加密电路 106、解压缩电路 109、加密电路 113。

[0050] 在来自控制电路 116 的输入信号表示 128bit 密钥长的情况下,信号处理电路 201 以 128bit 单位将信号供给到数据加密电路 203,密码密钥生成电路 202 也将 128bit 的数据密码密钥信号供给到数据加密电路 203,数据加密电路 203 将已解密的 AV 信号供给到加密电路 106、解压缩电路 109、加密电路 113。

[0051] 图 3 表示出本实施例中使用的加密电路 106。来自密码解密电路 105 已解密的 AV 信号输入到信号处理电路 301,并且从控制电路 116 表示再现装置 101 的工作地域如何的信号输入到密码密钥生成电路 302 与数据加密电路 303。

[0052] 由于加密电路 106 具有固定 128bit 密钥长的多个加密方式,所以与来自控制电路 116 的信号无关,信号处理电路 301 始终以 128bit 单位将信号供给到数据加密电路 303。

[0053] 在来自控制电路 116 的输入信号表示日美欧的情况下,密码密钥生成电路 302 和数据加密电路 303 依据 DTCP-IP 标准以 128bit 密钥长进行加密,将 128bit 的数据密码密钥信号供给到数据加密电路 303,数据加密电路 303 将再次加密的 AV 信号供给到发送接收电路 107。

[0054] 在来自控制电路 116 的输入信号表示中国地域的情况下,密码密钥生成电路 302 和数据加密电路 303 依据中国加密标准以 128bit 密钥长进行加密,将 128bit 的数据密码密钥信号供给到数据加密电路 303,数据加密电路 303 将再次加密的 AV 信号供给到发送接收电路 107。

[0055] 图 4 表示出本发明中使用的加密电路 110 的实施例。从解压缩电路 109 解压的 AV 信号与从密码解密电路 105 压缩 AV 信号、RC 和 CGM 信号输入到信号多路复用电路 401,并且从控制电路 116 表示再现装置 101 的工作地域如何的信号输入到信号处理电路 402、数据变换电路 403、密码密钥生成电路 404、数据加密电路 405。

[0056] 信号多路复用电路 401 在解压缩而成为基本频带的图像信号中时分多路复用压缩 AV 信号、RC 信号和 CGM 信号。由于有时解压缩的图像信号与压缩 AV 信号的图像信号相同,有时不同,所以限制两个图像信号的各个 RC 信号和 CGM 信号也同时多路复用。

[0057] 加密电路 110 具有密钥长 40bit 或 56bit 与 128bit 的加密方式,在来自控制电路 116 的信号表示日美欧的情况下,信号处理电路 402 以 24bit 单位将信号供给到数据变换电路 403。数据变换电路 403 除了将该 24bit 单位的信号中的所有 0 或所有 1 相加而变换成 40bit 或 56bit 单位。

[0058] 在来自控制电路 116 的输入信号表示日美欧的情况下,密码密钥生成电路 404 和数据加密电路 405 依据 HDCP 标准以 40bit 或 56bit 密钥长进行加密,将 40bit 或 56bit 的数据密码密钥信号供给到数据加密电路 405,数据加密电路 405 将再次加密的 AV 信号供给到发送接收电路 111。

[0059] 在来自控制电路 116 的输入信号表示中国地域的情况下,信号处理电路 402 以 128bit 单位将信号供给到数据变换电路 403,数据变换电路 403 将 128bit 单位或 24bit 单位的信号中所有 0 或 1 相加变换成 128bit 单位后的信号供给到数据加密电路 405,密码

密钥生成电路 404 与数据加密电路 405 依据中国加密标准以 128bit 密钥长进行加密,将 128bit 的数据密码密钥信号供给到数据加密电路 405,数据加密电路 405 再次加密而将多路复用的信号供给到发送接收电路 111。

[0060] 以上,根据本实施例,在处理 AV 信息的装置中,搭载与采用因装置的使用地域而不同的加密方式的著作权管理系统对应的状况,在 RC 中除现有的限制再现地域的数据以外,追加根据著作权人的许可变更或扩大再现地域的状况,基于附加于该 AV 信息的 RC,或再现地域的变更或扩大的信息,再现装置选择加密方式而再现 AV 信息,传送到电视装置,进行显示,由此可以实现与所销售的地域无关、可以被许可的机器再现被许可的 AV 信息的方法与装置。

[0061] 如上所述,用户可以以单一操作,或者自动地选择可以再现 AV 信息的地域,并且对装置制造者来说可以降低上述能够再现地域选择功能所需的成本。

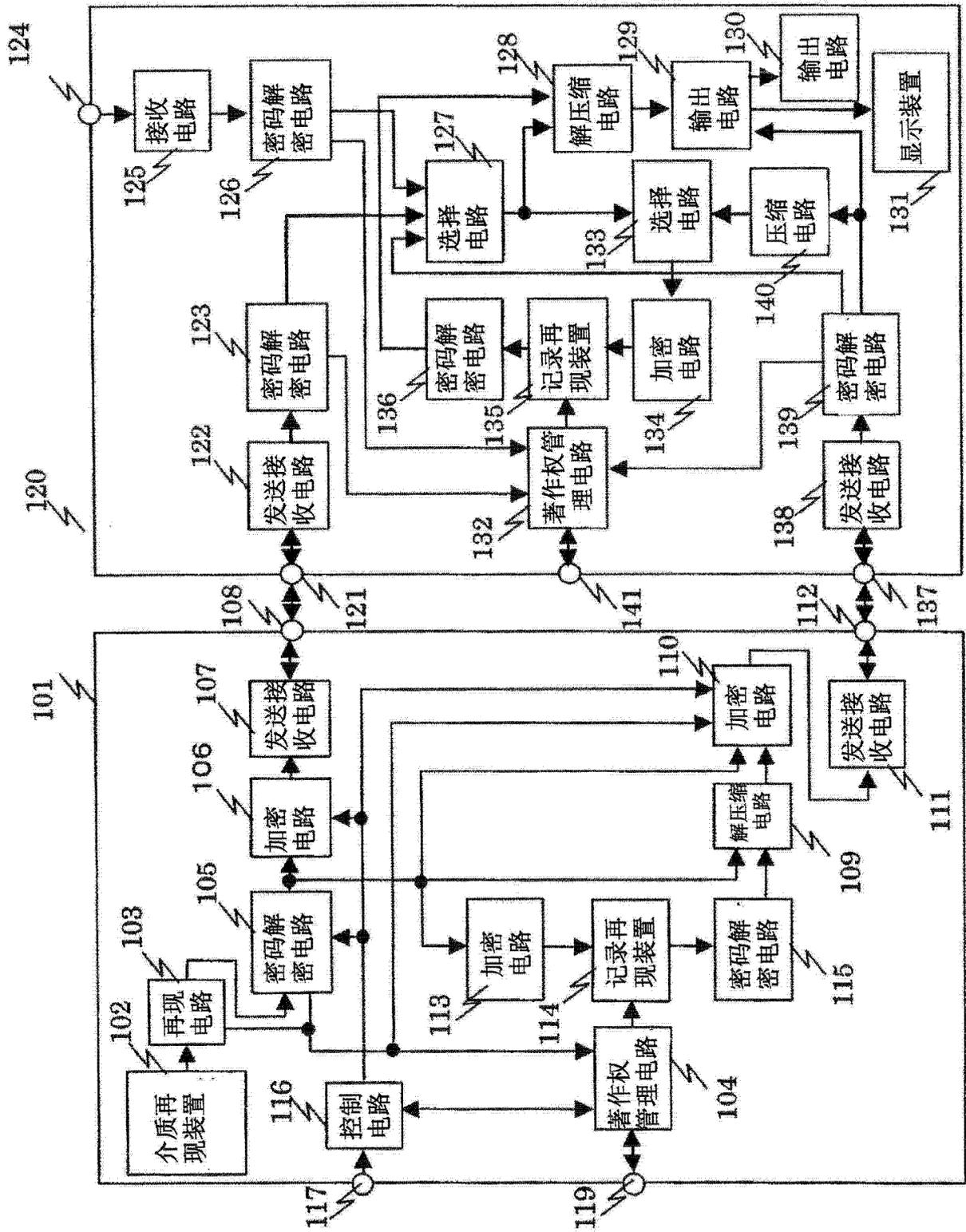


图 1

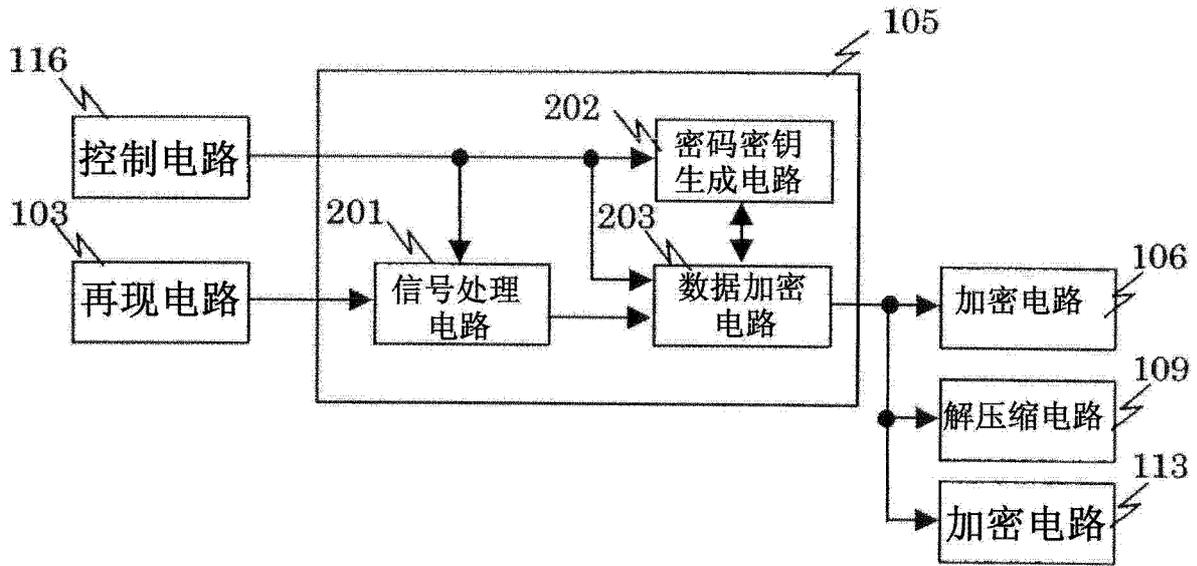


图 2

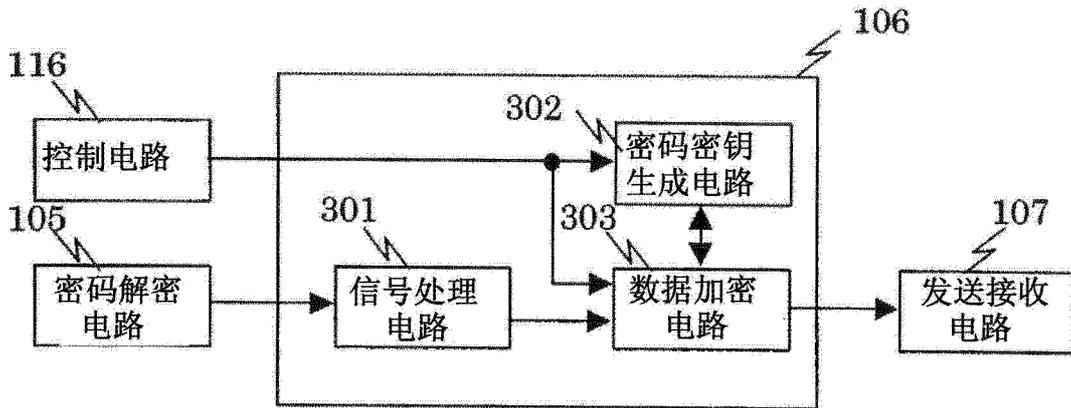


图 3

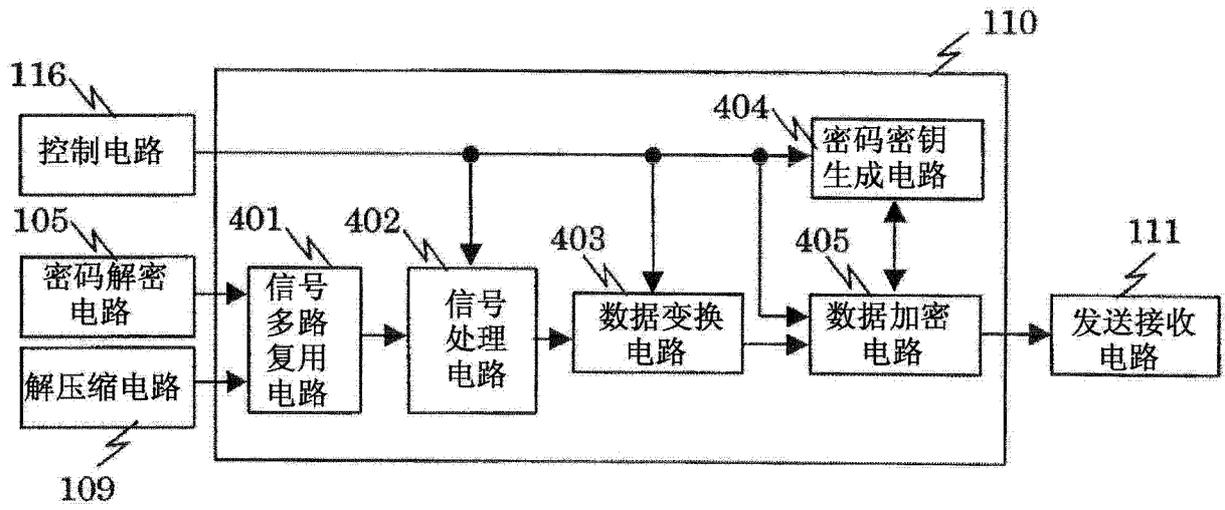


图 4