(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 1901067 B
(45)授权公告日 2011.10.12

(21)申请号 200610099666.2
(22)申请日 2002.08.08
(30)优先权数据
240778/2001 2001.08.08 JP
260932/2001 2001.08.30 JP
(62)分案原申请数据
02127686.2 2002.08.08
(73)专利权人 松下电器产业株式会社
地址 日本大阪府
(72)发明人 中野稔久 原田俊治 松崎枣
館林诚
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 浦柏明 刘宗杰
(51)Int.Cl.
G11B 20/10(2006.01)
H04N 5/91(2006.01)

(56)对比文件
JP 2001076425 A,2001.03.23, 全文.
EP 1098311 A,2001.05.09, 全文.
US 5555304 A,1996.09.10, 全文.
EP 0878796 A,1998.11.18, 全文.

审查员 孙蓉蓉

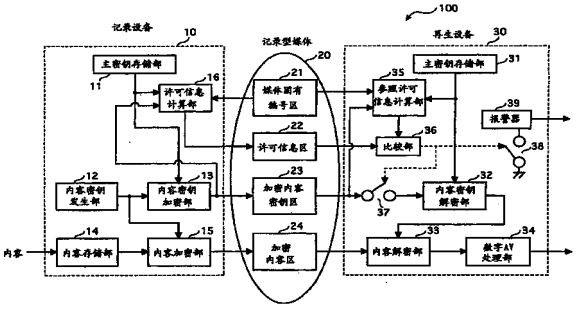
权利要求书 3 页 说明书 16 页 附图 10 页

(54)发明名称

著作权保护系统、记录设备及解密设备

(57)摘要

在记录型媒体中，媒体固有的媒体固有编号以不可改写状态被记录。记录设备把加密内容、用于对加密内容解密的加密内容密钥、利用加密内容密钥及媒体固有编号双方所生成的反映双方的值的许可信息写入记录型媒体内。再生设备获取被记录在记录型媒体内的媒体固有编号和加密内容密钥及许可信息，对该许可信息是否反映出该媒体固有编号及该加密内容密钥双方进行判定，只有在反映出双方的场合下，才对被记录在记录型媒体内的加密内容密钥解密，利用被解密的内容密钥对加密内容解密。通过上述构成，著作权保护系统只再生原始的内容，不再生复制的内容。



CN 1901067 B

1. 一种用于再生记录在记录媒体上的加密内容的再生设备，该记录媒体具有记录了该记录媒体固有的媒体编号的不能改写区，其中通过记录设备将加密内容、加密内容密钥以及许可信息记录在记录媒体上，该内容密钥用于解密加密内容，

其中记录在记录媒体上的加密内容密钥是由记录设备基于指定给该记录设备的第一主密钥来加密的内容密钥，并且记录在记录媒体上的许可信息基于媒体编号和内容密钥，

再生设备包括：

第二主密钥存储单元，可用于存储指定给该再生设备的第二主密钥；

计算单元，可用于从记录媒体获得媒体编号和加密内容密钥，并且基于该媒体编号和加密内容密钥生成参照许可信息；

比较单元，可用于从记录媒体获得许可信息以及从所述计算单元获得参照许可信息，并且将该许可信息和该参照许可信息进行比较，以确定该许可信息和该参照许可信息是否彼此匹配；

解密单元，可用于从记录媒体获得加密内容和加密内容密钥，获得存储在所述第二主密钥存储单元中的第二主密钥，利用该第二主密钥解密加密内容密钥，以及利用该内容密钥解密加密内容，以生成解密内容；

再生单元，可用于再生该解密内容；以及

制止单元，可用于在所述比较单元确定许可信息与参照许可信息不匹配时制止解密内容的再生。

2. 根据权利要求 1 所述的再生设备

其中，所述记录设备包括：

第一主密钥存储单元，可用于存储该第一主密钥；

内容密钥加密单元，可用于基于所述第一主密钥存储单元中存储的第一主密钥，加密内容密钥；

生成单元，可用于从记录媒体获得媒体编号并且基于该媒体编号和内容密钥生成许可信息；以及

记录单元，可用于将许可信息、加密内容密钥和加密内容记录在记录媒体上。

3. 根据权利要求 2 所述的再生设备，其中：

所述生成单元可用于为多组加密内容中的每一组生成一组许可信息，这通过基于媒体编号以及与该组加密内容对应的一组内容密钥生成许可信息来实现；

所述记录单元可用于将多组加密内容、与多组加密内容一一对应的多组内容密钥、以及由所述生成单元生成并与多组加密内容一一对应的多组许可信息，组合地记录在记录媒体上；并且

所述比较单元和所述解密单元分别对记录在记录媒体上的每个组合进行比较和解密。

4. 根据权利要求 2 所述的再生设备，其中，

所述生成单元可用于为多组加密内容生成一组许可信息，这通过基于媒体编号以及与该多组加密内容一一对应的多组内容密钥生成许可信息来实现。

5. 根据权利要求 2 所述的再生设备，其中存储在所述第一主密钥存储单元中的第一主密钥与存储在所述第二主密钥存储单元中的第二主密钥相同。

6. 根据权利要求 2 所述的再生设备，其中所述比较单元可用于：在由用于生成许可信

息的所述生成单元获得的媒体编号不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的媒体编号时，确定许可信息与参照许可信息不匹配。

7. 根据权利要求 2 所述的再生设备，其中所述生成单元可用于基于媒体编号和加密内容密钥来生成许可信息。

8. 根据权利要求 7 所述的再生设备，其中所述比较单元可用于在如下情况中的至少一种下，确定许可信息与参照许可信息不匹配：

(a) 由用于生成许可信息的所述生成单元获得的媒体编号不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的媒体编号，以及

(b) 由用于生成许可信息的所述生成单元获得的加密内容密钥不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的加密内容密钥。

9. 根据权利要求 1 所述的再生设备，其中：

所述记录设备为多组加密内容中的每一组生成一组许可信息，这通过基于媒体编号以及与该组加密内容对应的一组内容密钥生成许可信息来实现；

所述记录设备将多组加密内容、与多组加密内容一一对应的多组内容密钥、以及由所述生成单元生成并与多组加密内容一一对应的多组许可信息，组合地记录在记录媒体上；并且

所述比较单元和所述解密单元分别对记录在记录媒体上的每个组合进行比较和解密。

10. 根据权利要求 1 所述的再生设备，其中

存储在所述记录设备中的第一主密钥与存储在所述第二主密钥存储单元中的第二主密钥相同。

11. 根据权利要求 1 所述的再生设备，其中

所述比较单元可用于：在由用于生成许可信息的所述记录设备获得的媒体编号不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的媒体编号时，确定许可信息与参照许可信息不匹配。

12. 根据权利要求 1 所述的再生设备，其中

所述比较单元可用于在如下情况中的至少一种下，确定许可信息与参照许可信息不匹配：

(a) 由用于生成许可信息的所述记录设备获得的媒体编号不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的媒体编号，以及

(b) 由用于生成许可信息的所述记录设备获得的加密内容密钥不同于由用于生成参照许可信息的所述计算单元从记录媒体获得的加密内容密钥。

13. 一种用于在再生设备中再生记录在记录媒体上的加密内容的再生方法，该记录媒体具有记录了该记录媒体固有的媒体编号的不能改写区，

其中通过记录设备将加密内容、加密内容密钥以及许可信息记录在记录媒体上，所述内容密钥用于解密该加密内容，

其中记录在记录媒体上的加密内容密钥是由记录设备基于指定给该记录设备的第一主密钥而加密的内容密钥，并且记录在记录媒体上的许可信息基于媒体编号和内容密钥，以及所述再生方法包括：

存储指定给所述再生设备的第二主密钥；

从记录媒体获得媒体编号和加密内容密钥，并且基于该媒体编号和该加密内容密钥生成参照许可信息；

从记录媒体获得许可信息，并将该许可信息与该参照许可信息进行比较，以确定该许可信息与该参照许可信息是否彼此匹配；

从记录媒体获得加密内容和加密内容密钥，利用第二主密钥解密该加密内容密钥，以及利用该内容密钥解密该加密内容，以生成解密内容；

再生该解密内容；以及

当所述比较中确定许可信息与参照许可信息不匹配时制止解密内容的所述再生。

14. 根据权利要求 13 所述的再生方法，还包括：

在该记录设备中使用的记录方法包括：

存储该第一主密钥；

基于存储在该记录设备中的该第一主密钥来加密内容密钥，该内容密钥用于解密加密内容；

从记录媒体获得媒体编号，以及基于该媒体编号和内容密钥生成许可信息；以及

将该许可信息、加密内容密钥以及加密内容记录在记录媒体上。

著作权保护系统、记录设备及解密设备

[0001] 本申请是下述申请的分案申请：

[0002] 发明名称：著作权保护系统、记录设备及解密设备

[0003] 申请号：200410064416.6

技术领域

[0004] 本发明涉及利用记录了媒体固有编号的可写入记录型媒体，保护被记录在记录型媒体上的内容著作权的技术。

背景技术

[0005] 近年来，采用接收通过数字广播被广播的电影等内容，在光盘等记录媒体上记录并再生的设备的内容利用形式正在普及。另一方面，利用个人计算机等把通过这样的设备被记录到记录媒体上的内容非法复制到其它记录媒体上的情况也在增多。

[0006] 作为使这种被非法复制的内容不能再生的技术，以往所知的有图 1 所示的著作权保护系统。

[0007] 同图中的著作权保护系统由对内容加密，并记录到记录型媒体 2000 内的记录设备 1000、对被记录到记录型媒体 2000 内的加密内容解密，并使之再生的再生设备 3000 构成。

[0008] 记录型媒体 2000 是一种光盘等记录媒体，配有记录了媒体固有编号的媒体固有编号区 2001。媒体固有编号是各记录型媒体各自固有的识别符，在记录型媒体制造时被记录。媒体固有编号区 2001 被实施在制造时的记录以后不能再改写该媒体固有编号的保护。

[0009] 记录设备 1000 从外部获取内容，并存储到内容存储部 1004 内。

[0010] 在记录型媒体 2000 被连接到记录设备 1000 内后，内容加密部 1005 读出被存储在内容存储部 1004 内的内容，利用内容密钥加密，并记录到记录型媒体 2000 的加密内容区 2003 内。内容密钥是在内容密钥发生部 1002 内发生的随机数。内容密钥加密部 1003 利用内容密钥加密密钥对内容密钥加密，并记录到记录型媒体 2000 的加密内容密钥区 2002 内。内容密钥加密密钥是通过密钥加密密钥计算部 1001 计算出来的密钥。密钥加密密钥计算部 1001 利用被记录在媒体固有编号区 2001 内的媒体固有编号及主密钥，通过散列函数计算出内容密钥加密密钥。这里的所谓主密钥是记录设备 1000 与再生设备 3000 预先配有的对第三者保密的密钥。

[0011] 图 2 表示密钥加密密钥计算部 1001 的内部运算机构。

[0012] 媒体固有编号被从 A 点输入，在 DES 加密部 4000 中，利用被保存在主密钥存储部 4001 内的主密钥，通过 DES(Data EncryptionStandard) 被加密。被加密后的媒体固有编号在“异”电路 4002 中被实施与媒体固有编号的“异或”计算，其结果通过 B 被输出。该 B 输出是内容密钥加密密钥。

[0013] 在再生设备 3000 内连接记录型媒体 2000 后，密钥解密密钥计算部 3001 从记录型媒体 2000 的媒体固有编号区 2001 内获取媒体固有编号，通过与记录设备 1000 的密钥加密

密钥计算部 1001 相同的运算，计算出内容密钥解密密钥。如果密钥加密密钥计算部 1001 与密钥解密密钥计算部 3001 各自采用相同数值的主密钥及媒体固有编号，内容密钥加密密钥与内容密钥解密密钥将具有相同的数值。

[0014] 内容密钥解密部 3002 从加密内容密钥区 2002 读出加密内容密钥，通过内容密钥解密密钥对其进行解密，获取内容密钥。该内容密钥被暂时存储在内容密钥暂时存储部 3003 内。

[0015] 内容解密部 3004 从加密内容区 2003 读出加密内容，通过内容密钥对其进行解密，获取内容。

[0016] 数字 AV 处理部 3005 把被解密的内容转换成模拟音响图像数据，向外部的扬声器及显示器等输出。

[0017] 通过上述构成，再生设备 3000 只有在采用与在加密时被采用的媒体固有编号相同的媒体固有编号的场合下，才能对内容密钥正确解密。

[0018] 换言之，再生设备 3000 在采用与在加密时被采用的媒体固有编号不同的媒体固有编号的场合下，不能对内容密钥正确解密。

[0019] 更具体地说，在把被记录在记录型媒体 2000 内的加密内容密钥及加密内容复制到其它记录型媒体内，通过再生设备 3000 对该其它记录型媒体实施再生的场合下，由于记录型媒体 2000 与该其它记录型媒体的媒体固有编号不同，因而再生设备 3000 不能利用被记录在其它记录型媒体内的加密内容密钥对正确的内容密钥解密。

[0020] 这样，现有的著作权保护系统通过只有由记录设备 1000 记录的原始内容才能由再生设备 3000 对内容密钥正确解密，而对复制的内容，再生设备 3000 则不能实施正确解密的方式使非法复制无效。

[0021] 然而，再生设备 3000 不能识别某内容是原始内容还是复制内容，对复制内容也实施解密。在使复制内容再生的场合下，由于不能正确解密，因而所输出的是完全不同于原内容的杂乱的图像和声音。

[0022] 这样，由于不知道是被复制的内容，因而欲利用该内容的利用者不知道产生再生异常的原因是复制所致，有时误把它当作设备故障。此外有时由于异常的再生也可能造成设备损坏。

发明内容

[0023] 有鉴于此，本发明的目的是提供一种设有检查记录型媒体的内容是原始内容还是复制内容的机构，根据该检查结果只再生原始内容，不再生复制内容的著作权保护系统。

[0024] 为达到上述目的，本发明涉及的著作权保护系统由对具有记录了随各记录媒体而异的媒体固有编号的不能改写区的可写入记录媒体记录作为被加密过的内容的加密内容的记录设备、从被记录了加密内容的该记录媒体中读出加密内容并进行解密的解密设备组成，其中，上述记录设备配有通过实施采用了记录在记录媒体中的媒体固有编号和上述加密内容解密所需要的解密信息双方的特定运算，生成反映出该媒体固有编号及该解密信息双方的许可信息的生成单元；把上述许可信息、上述解密信息和上述加密内容记录到上述记录媒体的记录单元，上述解密设备，配有通过采用被记录到记录媒体内的媒体固有编号、解密信息和许可信息的全部，来判定该许可信息是否是由采用该媒体固有编号及该解密信

息双方进行的上述特定运算而导出的信息的判定单元；只有在由上述判定单元作出了肯定判定的场合下，才利用上述解密信息对被记录到上述记录媒体内的加密内容进行解密的解密单元。

[0025] 根据这种构成，生成单元利用被记录在该记录媒体内的媒体固有编号和用于对加密内容解密的解密信息来生成反映该双方的值的许可信息。更具体地说，许可信息是把媒体固有编号与解密信息结合后的值作为输入数据使用，由散列函数生成的散列值。由于散列函数包括不可逆单向函数，因而不能根据许可信息求出媒体固有编号与解密信息。而且难以产生生成相同许可信息的不同的输入数据。根据该散列函数的性质，许可信息只有在采用用于生成该许可信息的媒体固有编号及解密信息的场合下才能生成。因此，如果记录媒体的内容是原始内容，而不是复制内容，则被记录到该记录媒体内的许可信息应当反映出被记录到该记录媒体内的媒体固有编号及解密信息。这样，判定单元通过判定是否反映出来判定记录媒体内的记录内容是原始内容还是复制内容。更具体地说，判定单元利用媒体固有编号与解密信息，利用与生成单元所采用的生成方法相同的方法来生成参照许可信息，对参照许可信息与被记录在记录媒体内的参照许可信息进行比较，根据双方的值是否一致来进行判定。而且解密单元只对原始记录媒体进行内容解密，不对复制的记录媒体内容解密。这样，可以阻止内容被非法复制到其它记录媒体而被利用。

[0026] 此外，可构成为：上述解密信息是通过利用上述解密信息进行规定的运算，可以获取用于对上述加密内容解密的解密密钥的信息，上述解密单元配有对上述解密信息实施上述规定的运算，获取解密密钥的解密密钥运算单元，在加密内容的解密中，利用上述解密密钥从上述加密内容解密内容。

[0027] 此外，可构成为：上述记录设备还配有通过从外部获取或者通过预先存储而拥有秘密密钥的记录设备侧拥有单元；利用上述秘密密钥通过秘密密钥加密方式对上述解密密钥加密，并生成上述解密信息的解密密钥加密单元，上述解密设备，还配有通过从外部获取或者通过预先存储而拥有与上述记录设备所拥有的秘密密钥相同的秘密密钥的解密设备侧拥有单元，上述解密密钥运算单元，利用上述秘密密钥通过秘密密钥加密方式对上述解密信息解密，获取解密密钥。

[0028] 此外，可构成为：上述记录设备的上述生成单元，在上述特定的运算中，除了上述媒体固有编号及上述解密信息之外，还采用上述秘密密钥，上述解密设备的上述判定单元，除了上述媒体固有编号及上述解密信息之外，还采用上述解密设备侧拥有单元所用有的秘密密钥，判定上述许可信息是否是由上述特定的运算导出的信息。

[0029] 此外，可构成为：上述记录媒体，还在上述不能改写区内记录有只有在采用了特定装置密钥的场合下才能对上述秘密密钥正确解密的秘密密钥信息，上述记录设备侧拥有单元及上述解密设备侧拥有单元，配有预先存储设备固有的装置密钥的装置密钥存储单元；利用被存储在上述装置密钥存储单元内的装置密钥对上述记录媒体的秘密密钥信息解密的秘密密钥解密单元；通过只在可由上述秘密密钥解密单元正确解密了上述秘密密钥的场合下才存储上述秘密密钥而拥有秘密密钥的秘密密钥存储单元，上述记录设备及解密设备，还配有在由上述秘密密钥解密单元未能正确解密上述秘密密钥的场合下，中止以后的各单元处理的中止单元。

[0030] 此外，可构成为：在上述解密设备中，上述判定单元配有通过采用被记录在记录媒

体内的媒体固有编号及解密信息，实施与上述生成单元中的上述特定的运算相同的运算，来生成作为运算结果的参照许可信息的生成部；对上述参照许可信息与上述媒体固有编号进行比较，在二者一致的场合下作出肯定判定，在二者不一致的场合下作出否定判定的比较判定部。

[0031] 此外，可构成为：在上述记录设备中，上述生成单元，按被记录在上述记录媒体内的每个加密内容，利用媒体固有编号及针对该加密内容的解密信息来生成许可信息，上述记录单元，将由加密内容、解密信息和许可信息组成的各组相关联，记录到上述记录媒体，在上述解密设备中，上述判定单元及上述解密单元，对被记录在上述记录媒体内的上述各组分别实施处理。

[0032] 此外，可构成为：在上述记录设备中，上述生成单元，利用被记录在上述记录媒体内的各加密内容所对应的所有解密信息及媒体固有编号生成一个许可信息。

[0033] 本发明的记录设备是一种对具有被记录了记录媒体固有的媒体固有编号的不能改写区的可写入记录媒体、记录作为被加密的内容的加密内容的记录设备，其配有通过实施采用了记录在记录媒体中的媒体固有编号和上述加密内容解密所需要的解密信息双方的特定运算，生成反映出该媒体固有编号及该解密信息双方的许可信息的生成单元；把上述许可信息、上述解密信息和上述加密内容记录到上述记录媒体的记录单元。

[0034] 本发明的解密设备是一种从具有被记录了记录媒体固有的媒体固有编号的不能改写区、并被记录了加密内容及用于该加密内容解密的解密信息及用于判定是否允许该加密内容解密的许可信息的记录媒体中读出加密内容并予以解密的解密设备，其配有通过采用被记录到记录媒体内的媒体固有编号、解密信息和许可信息的全部，来判定该许可信息是否是由采用该媒体固有编号及该解密信息双方进行的特定运算而导出的信息的判定单元；只有在由上述判定单元作出了肯定判定的场合下，才利用上述解密信息对被记录到上述记录媒体内的加密内容进行解密的解密单元。

附图说明

[0035] 图 1 是表示现有的著作权保护系统构成的方框图。

[0036] 图 2 表示密钥加密密钥计算部 1001 的内部运算机构。

[0037] 图 3 是表示第 1 实施方式的著作权保护系统 100 的构成方框图。

[0038] 图 4 是表示记录设备 10 的处理步骤的流程图。

[0039] 图 5 是表示再生设备 30 的处理步骤的流程图。

[0040] 图 6 是表示第 2 实施方式的著作权保护系统 200 的构成方框图。

[0041] 图 7 表示被记录在媒体密钥数据区 25 内的媒体密钥数据一例。

[0042] 图 8 是表示第 3 实施方式的著作权保护系统 300 的构成方框图。

[0043] 图 9 是表示第 4 实施方式的著作权保护系统 400 的构成方框图。

[0044] 图 10 表示记录型媒体的构成例。

[0045] 图 11 表示记录型媒体的构成例。

具体实施方式

[0046] 以下结合附图对本发明的实施方式作以说明。

[0047] < 第 1 实施方式 >

[0048] 以下通过附图对本发明的第 1 实施方式作以说明。

[0049] < 构成 >

[0050] 图 3 是表示第 1 实施方式的著作权保护系统 100 的构成方框图。

[0051] 同图中的著作权保护系统 100 由用于在记录型媒体 20 内记录加密内容的记录设备 10 与对被记录在记录型媒体 20 内的加密内容解密并使之再生的再生设备 30 构成。以下首先对记录型媒体 20 作以说明，然后对记录设备 10 的构成及再生设备 30 的构成作以说明。

[0052] < 记录型媒体 20>

[0053] 记录型媒体 20 是一种光盘，配有被记录了媒体固有编号的不可改写的媒体固有编号区 21 和可以记录的记录区。

[0054] 媒体固有编号是各记录型媒体的固有的 64 位识别符，在记录型媒体制造时被写入媒体固有编号区 21 内。媒体固有编号区 21 被施加在制造时的写入之后不能再改写该媒体固有编号的保护。

[0055] 在记录区内，通过记录设备 10 确保许可信息区 22、加密内容密钥区 23、加密内容区 24，通过记录设备 10 记录各种数据。

[0056] 在加密内容区 24 内，通过记录设备 10 记录加密内容。

[0057] 在加密内容密钥区 23 内，通过记录设备 10 记录加密内容密钥。

[0058] 加密内容密钥是一种在再生设备 30 对加密内容实施解密时的所必需的信息，是一种已对内容密钥加密的信息。内容密钥是一种通用于内容的加密及解密的秘密密钥加密方式的秘密密钥。

[0059] 在许可信息区 22 内通过记录设备 10 记录许可信息。

[0060] 许可信息是用于证明被记录在记录型媒体 20 内的数据是由记录设备 10 初始记录的数据的信息。所谓初始记录系指记录型媒体的原始记录，而不是由其它记录媒体等复制后的数据。再生设备 30 通过对该许可信息的确认，可以判定是记录型媒体的原始记录还是复制品。对于许可信息将在后文中详细说明。

[0061] < 记录设备 10 的构成 >

[0062] 以下对记录设备 10 的构成作以说明。

[0063] 记录设备 10 配有主密钥存储部 11、内容密钥发生部 12、内容密钥加密部 13、内容存储部 14、内容加密部 15、许可信息计算部 16。

[0064] 主密钥存储部 11 是用于预先存储 56 位主密钥的存储器。主密钥是由记录设备 10 及再生设备 30 共同拥有的对外部保密的密钥。

[0065] 内容密钥发生部 12 是一种发生作为内容密钥的随机数的随机数发生器。内容密钥发生部 12 在接收到由记录设备 10 的控制电路（未图示）输出的起动信号后，生成一个 56 位的随机数据，把它作为内容密钥输出。

[0066] 内容密钥加密部 13 用于通过主密钥对内容密钥加密，并记录到记录型媒体 20 内。采用比如 DES 作为加密算法。内容密钥加密部 13 获取由内容密钥发生部 12 发生的内容密钥及被存储在主密钥存储部 11 内的主密钥，通过主密钥对内容密钥加密，获得 64 位加密内容密钥。从而在记录型媒体 20 的记录区内确保加密内容密钥区 23，在该区域内记录加密内

容密钥。

[0067] 内容存储部 14 是一种硬盘类存储装置，用于对由外部输入的内容进行记录和存储。外部输入状况包括比如由卫星广播接收装置接收通过数字卫星广播所广播的数字电影内容，并把该内容存入内容存储部 14 内的状况。

[0068] 内容加密部 15 用于通过内容密钥对内容加密，并记录到记录型媒体 20 内。采用比如 DES 作为加密算法。内容加密部 15 获取由内容密钥发生部 12 发生的内容密钥及被记录在内容存储部 14 内的内容，把内容分割成各为 64 位的内容块，通过内容密钥对各内容块加密。从而在记录型媒体 20 的记录区内确保加密内容区 24，在该区域内记录作为被加密的内容块的集合的加密内容。

[0069] 许可信息计算部 16 是用于生成许可信息的运算机构。许可信息计算部 16 首先获取被记录在媒体固有编号区 21 内的媒体固有编号、作为由内容密钥加密部 13 加密后的结果的加密内容密钥、被存储在主密钥存储部 11 内的主密钥。然后把媒体固有编号、主密钥及加密内容密钥连接起来，形成一个位串，在输入该位串时，可通过 SHA-1(SecureHash algorithm 1) 等散列函数的运算实施。其结果是，获取 160 位散列值，把该散列值作为许可信息。最后，在记录型媒体 20 的记录区内确保许可信息区 22，在该区域内记录许可信息。

[0070] 在此对散列函数 SHA-1 作以说明。

[0071] 散列函数 SHA-1 是用于认证及数字署名等的散列函数中的一种。该函数可生成从 2 乘以 64 以下的数据至 160 位的散列值。由于散列函数 SHA-1 包括不可逆的单向函数，因而不能根据散列值再现原始数据。此外，极难以生成能生成相同散列值的其它数据。利用这一性质，传送侧把数据及根据数据所生成的散列值传送给接收侧，接收侧根据所接收的数据生成散列值，通过将所生成的散列值与所接收的散列值的比较，可以检测出在通信途中数据是否被改写等。

[0072] 根据散列函数 SHA-1 的性质，许可信息难以通过在许可信息生成中所采用的媒体固有编号、加密内容密钥及主密钥以外的其它值生成。即许可信息将全部反映出在生成许可信息时所采用的媒体固有编号、加密内容密钥及主密钥。

[0073] 因此许可信息，通过许可信息中所反映出的媒体固有编号、加密内容密钥及主密钥分别与被记录在媒体固有编号区 21 内的媒体固有编号、被记录在加密内容密钥区 23 内的加密内容密钥、记录设备 10 所拥有的主密钥相同，来证明媒体固有编号、加密内容密钥及主密钥的合法性。

[0074] < 再生设备 30 的构成 >

[0075] 以下对再生设备 30 的构成作以说明。

[0076] 再生设备 30 配有主密钥存储部 31、内容密钥解密部 32、内容解密部 33、数字 AV 处理部 34、参照许可信息计算部 35、比较部 36、第 1 开关 37、第 2 开关 38、报警器 39。

[0077] 主密钥存储部 31 是用于预先存储 56 位主密钥的存储器。该主密钥与被存储在记录设备 10 的主密钥存储部 11 内的主密钥具有相同值。

[0078] 内容密钥解密部 32 用于利用主密钥对被记录在记录型媒体 20 内的加密内容密钥解密。内容密钥解密部 32 用于获取被记录在加密内容密钥区 23 内的加密内容密钥及被存储在主密钥存储部 31 内的主密钥，通过主密钥对加密内容密钥解密，获得内容密钥。

[0079] 内容解密部 33 通过内容密钥对被记录在记录型媒体 20 内的加密内容解密，并向

数字 AV 处理部 34 输出。内容解密部 33 用于获取通过内容解密部 32 解密的内容密钥及被记录在加密内容区 24 内的加密内容，把加密内容分割成各为 64 位的内容块，通过内容密钥在各内容块内解密。然后把作为解密后的内容块的集合的内容向数字 AV 处理部 34 输出。

[0080] 数字 AV 处理部 34 从内容解密部 33 获取内容，把内容转换成模拟音响图像数据，向外部的扬声器及显示器等输出。

[0081] 第 1 开关 37 根据来自比较部 36 的控制开闭，当第 1 开关 37 关闭时，从加密内容密钥区 23 向内容密钥解密部 32 读出加密内容密钥，当第 1 开关 7 打开时，加密内容密钥的读出被制止。

[0082] 第 2 开关 38 根据来自比较部 36 的控制开闭，当第 2 开关 38 关闭时，向报警器 39 提供电源，打开后不提供电源。

[0083] 报警器 39 是在电源接通时动作，并发出警告声音的电路。

[0084] 参照许可信息计算部 35 是实施与许可信息计算部 16 相同运算的并生成参照许可信息的运算机构。参照许可信息计算部 35 用于获取被记录在媒体固有编号区 21 内的媒体固有编号、被记录在加密内容密钥区 23 内的加密内容密钥、被存储在主密钥存储部 31 内的主密钥。接下来，参照许可信息计算部 35 把媒体固有编号、主密钥、加密内容密钥连接成一个位串。这里的各数据的连接顺序与许可信息计算部 16 中的连接顺序相同。因此参照许可信息计算部 35 根据 SHA-1 等散列函数进行作为输入该位串的运算。其结果是，获取 160 位散列值，把该散列值作为参照许可信息。

[0085] 比较部 36 用于获取被记录在许可信息区 22 内的许可信息及由参照许可信息计算部 35 生成的参照许可信息，并对这 2 个数值进行比较，只有在一致的场合下，才实施对加密内容解密的控制，在不一致的场合下，实施制止对加密内容的解密，并使报警器 39 发出警告音的控制。

[0086] 更详细地说，在比较结果、许可信息与参照许可信息一致的场合下，第 1 开关 37 关闭，加密内容密钥区 23 的加密内容密钥被向内容密钥解密部 32 读出。这样，内容密钥被解密，内容被解密及再生。

[0087] 作为比较结果，如果许可信息与参照许可信息不一致，则第 1 开关 37 打开，第 2 开关 38 关闭。通过第 1 开关 37 的打开，由于加密内容密钥区 23 的加密内容密钥不向内容密钥解密部 32 读出，因而内容密钥不被解密，内容也不被解密及再生。通过第 2 开关 38 的关闭，向报警器 39 提供电源，报警器 39 动作。

[0088] 参照许可信息计算部 35 及比较部 36 对被记录在媒体固有编号区 21 内的媒体固有编号、被记录在加密内容密钥区 23 内的加密内容密钥、被存储在主密钥存储部 31 内的主密钥是否在被记录在许可信息区 22 内的许可信息中都被反映出来进行检查，只有在被反映出来的场合下，才按照加密内容被解密的方式对各部进行控制，在未被反映出来的场合下，则实施制止加密内容的解密，并发出警告音的控制。

[0089] 只有在用于生成参照许可信息的媒体固有编号、加密内容密钥、主密钥与用于生成许可信息的媒体固有编号、加密内容密钥、主密钥的任意一个分别具有相同值的场合下，许可信息与参照许可信息才具有相同的值。反过来说，如果用于生成参照许可信息的媒体固有编号、加密内容密钥、主密钥与用于生成许可信息的媒体固有编号、加密内容密钥、主密钥的任意一个有不同，则许可信息与参照许可信息将具有不同的值。

[0090] <动作>

[0091] 以下对具有上述构成的记录设备 10 及再生设备 30 的各自的动作作以说明。

[0092] 图 4 是表示记录设备 10 的处理步骤的流程图。

[0093] 首先，内容密钥发生部 12 生成内容密钥（步骤 S201）。

[0094] 其次，内容密钥加密部 13 从主密钥存储部 11 内读出主密钥（步骤 S202）。

[0095] 接下来，内容密钥加密部 13 利用主密钥对所生成的内容密钥加密，其结果是，获取加密内容密钥（步骤 S203）。

[0096] 内容密钥加密部 13 在记录型媒体 20 的记录区内确保加密内容密钥区 23，在该区域内记录加密内容密钥（步骤 S204）。

[0097] 内容加密部 15 读出被存储在内容存储部 14 内的内容，把该内容分割成 64 位的内容块，利用内容密钥对每个内容块加密，生成加密内容（步骤 S205）。

[0098] 接下来，内容加密部 15 在记录型媒体 20 内确保加密内容区 24，在该区域内记录所生成的加密内容（步骤 S206）。

[0099] 许可信息计算部 16 从记录型媒体 20 的媒体固有编号区 21 中读出媒体固有编号（步骤 S207）。

[0100] 接下来，许可信息计算部 16 利用所读出的媒体固有编号、主密钥存储部 11 的主密钥、内容密钥加密部 13 的加密内客密钥，通过散列函数生成许可信息（步骤 S208）。

[0101] 最后，许可信息计算部 16 在记录型媒体 20 的记录区内确保许可信息区 22，在该区域内记录所生成的许可信息（步骤 S209）。

[0102] 图 5 是表示再生设备 30 的处理步骤的流程图。

[0103] 参照许可信息计算部 35 从记录型媒体 20 的媒体固有编号区 21 内读出媒体固有编号，从加密内容密钥区 23 中读出加密内容密钥。此外比较部 36 从许可信息区 22 中读出许可信息（步骤 S301）。

[0104] 其次，参照许可信息计算部 35 从主密钥存储部 31 中读出主密钥（步骤 S302）。

[0105] 接下来，参照许可信息计算部 35 利用媒体固有编号、加密内容密钥、主密钥，通过散列函数生成参照许可信息。该生成的运算顺序与步骤 S208 相同（步骤 S303）。

[0106] 比较部 36 把从记录型媒体 20 读出的许可信息与由参照许可信息计算部 35 生成的参照许可信息进行比较（步骤 S304）。

[0107] 作为比较结果，在许可信息与参照许可信息一致的场合下，比较部 36 实施步骤 S306、S307、S308 的处理，在许可信息与参照许可信息不一致的场合下，实施步骤 S309 的处理。

[0108] 作为步骤 S305 的比较结果，在许可信息与参照许可信息一致的场合下，比较部 36 使第 1 开关 37 关闭。这样，内容密钥解密部 32 从加密内容密钥区 23 读出加密内容密钥，通过被存储在主密钥存储部 31 内的主密钥对加密内容密钥解密，获取内容密钥（步骤 S306）。

[0109] 接下来，内容解密部 33 从加密内容区 24 内读出加密内容，通过由内容密钥解密部 32 解密的内容密钥对加密内容解密，获取内容（步骤 S307）。

[0110] 数字 AV 处理部 34 对解密后的内容以音响及视频信号形式再生，向扬声器、显示器等输出（步骤 S308）。

[0111] 作为步骤 S305 的比较结果，在许可信息与参照许可信息不一致的场合下，比较部

36 使第 1 开关 37 打开，使第 2 开关 38 关闭。这样，内容密钥解密部 32 不实施加密内容密钥的解密。因此加密内容不被解密及再生。另一方面，向报警器 39 提供电源，，报警器 39 发出警告音，向扬声器等输出（步骤 S309）。

[0112] ＜效果＞

[0113] 通过按上述方式构成著作权保护系统 100，再生设备 30 在下列场合下不实施记录型媒体的再生。

[0114] (1) 用于被记录在记录型媒体中的许可信息生成的媒体固有编号与用于参照许可信息生成的媒体固有编号不同的场合下。

[0115] 这种场合比如包括，由记录设备 10 记录的记录型媒体 20 的许可信息、加密内容密钥及加密内容在其它的记录型媒体上被复制，然后通过再生设备 30 对该其它记录型媒体实施再生的场合。这是因为其它记录型媒体的媒体固有编号与记录型媒体 20 的媒体固有编号不同。

[0116] (2) 用于被记录在记录型媒体内的许可信息的生成的加密内容密钥与用于参照许可信息的生成的加密内容密钥不同的场合。

[0117] 这种场合比如包括，其它记录型媒体的加密内容密钥及加密内容分别在记录型媒体 20 的加密内容密钥区 23 及加密内容区 24 内被标名复制，然后通过再生设备 30 对该记录型媒体 20 实施再生的场合。这是因为被记录在其它记录型媒体内的加密内容密钥极少能与最初被记录在记录型媒体 20 内的加密内容密钥具有相同值，几乎都是不相同的值。

[0118] (3) 用于被记录在记录型媒体内的许可信息的再生的主密钥与用于参照许可信息的生成的主密钥不同的场合。

[0119] 这种场合比如包括，通过再生设备 30 使由不具有记录设备 10 及再生设备 30 所拥有的主密钥的其它记录设备记录的记录型媒体再生的场合。由于主密钥相对著作权保护系统 100 以外的其它设备是保密的，因而只要主密钥没有失窃，著作权保护系统 100 的设备以外的其它设备便不能制作出旨在在再生设备 30 上再生的记录型媒体。

[0120] 由于上述的再生设备 30 不能使通过非法复制等被记录的记录型媒体再生，只能使通过记录设备 10 被记录的原始记录型媒体再生，因而著作权保护系统 100 可以阻止通过非法复制等渠道的内客流通。

[0121] ＜第 2 实施方式＞

[0122] 接下来，对本发明的第 2 实施方式作以说明。

[0123] 在上述第 1 实施方式中，记录设备 10 及再生设备 30 采用一种把内容加密及解密所必需的主密钥预先储存在设备内部的构成。在记录设备 10 及再生设备 30 有多台的场合下，各设备都采用储存相同主密钥的构成。但在这种构成下，如果一台设备遭到物理性攻击，即一台设备的内部被解析，主密钥暴露，则主密钥变得不能使用，不仅该设备，拥有相同主密钥的所有设备都将面临失效的危险。

[0124] 为此第 2 实施方式下的著作权保护系统对第 1 实施方式下的著作权保护系统 100 作了改进，即使在一台记录设备或再生设备遭到物理性攻击的场合下，也不会使其它设备因此而失效。

[0125] 主要的改进点如下。

[0126] (1) 分别为每台记录设备及再生设备分配不同值的装置密钥，分别被储存到各自

的设备内。

[0127] (2) 在记录型媒体内，在制造时，加工被称为媒体密钥的密钥并予以记录。所谓媒体密钥系指内容密钥及内容加密及解密所必需的密钥。所谓加工在后文中有详述，系指只在采用特定的装置密钥的场合下，才能从被加工的媒体密钥中取出媒体密钥，在采用其它的装置密钥的场合下，不能从被加工的媒体密钥中取出媒体密钥的加工方式。所谓特定的装置密钥系指被保存在记录型媒体制造时未报告受到物理性攻击的设备内的装置密钥，所谓其它的装置密钥系指被储存在已报告受到了物理性攻击的设备内的装置密钥。

[0128] (3) 记录设备利用所储存的装置密钥，试探性获取被记录在记录型媒体内的媒体密钥。记录设备只有在获取媒体密钥的场合下，才能利用该媒体密钥，实施内容密钥及内容的加密，在未获取的场合下，不实施加密。

[0129] (4) 与记录设备相同，再生设备利用所储存的装置密钥，试探性获取被记录在记录型媒体内的媒体密钥。再生设备只有在获取媒体密钥的场合下，才能利用该媒体密钥，对被记录在记录型媒体内的加密内容密钥及加密内容解密，在未获取的场合下，不实施解密。

[0130] 以下，对该改进后的著作权保护系统的构成及动作作以说明。

[0131] < 构成 >

[0132] 图 6 是表示第 2 实施方式下的著作权保护系统 200 的构成方框图。

[0133] 同图中的著作权保护系统 200 由在记录型媒体 70 内记录加密内容的记录设备 60 和对被记录在记录型媒体 70 内的加密内容进行解密并再生的再生设备 80 构成。

[0134] 同图中，与图 3 中相同符号的构成要素是相同的部件。以下以与图 3 中不同的部分为中心作说明。

[0135] < 记录型媒体 70>

[0136] 记录型媒体 70 是与记录型媒体 20 相同的光盘，除了具有与记录型媒体 20 相同的构成外，还配有媒体密钥数据区 25。

[0137] 媒体密钥数据区 25 是一种只能读取不能写入的区域，在记录型媒体 70 制造时记录媒体密钥数据。

[0138] 媒体密钥数据是上述改进点 (2) 中说明的对媒体密钥加工后的数据。

[0139] 图 7 表示被记录在媒体密钥数据区 25 内的媒体密钥数据一例。在同图的示例中，媒体密钥数据由其长度各为 8 字节的 128 个记录内容构成。各记录内容是以 E(Kdi,Km) 或 E(Kdi,0)(i 为从 1 至 128 的整数) 符号表示的加密数据。

[0140] Km 表示媒体密钥。媒体密钥是把多个记录型媒体 70 分成 1 个或多个组，各组被固有分配 1 个的 56 位随机值。为与 E(Kdi,0) 中的 0 区别，媒体密钥取 0 以外的值。

[0141] Kdi(i 为从 1 至 128 的整数) 表示 56 位装置密钥。装置密钥有 Kd1,Kd2,.....,Kd128 共 128 种，分别被储存在装置编号为 1,2,.....,128 的记录设备 60 或再生设备 80 内。装置编号是分别被预先分配到 128 台记录设备 60 及再生设备 80 内的从 1 至 128 的编号。第 1 记录内容～第 128 记录内容分别与装置密钥 Kd1 ～ Kd128 对应，与装置编号为 1 ～ 128 的记录设备 60 及再生设备 80 对应。

[0142] E( ) 表示加密算法，比如 DES。即 E(Kdi, Km) 表示采用 DES，使媒体密钥 Km 明码化，以 56 位的装置密钥 Kdi 作为加密密钥，利用装置密钥 Kdi 对媒体密钥 Km 加密的结果。比如第 2 记录内容的 E(Kd2, Km) 表示利用装置密钥 Kd2 对媒体密钥 Km 加密的结果。另一

方面，E(Kdi,0) 表示利用装置密钥 Kdi 对 0 值加密的结果。比如第 3 记录内容的 E(Kd3,0) 表示利用装置密钥 Kd3 对 0 加密的结果。

[0143] 反之，如果 E(Kdi,Km) 通过装置密钥 Kdi 解密，则解密结果将成为媒体密钥 Km。比如如果第 2 记录内容的 E(Kd2,Km) 通过装置密钥 Kd2 解密，则解密结果将成为媒体密钥 Km。另一方面，如果 E(Kdi,0) 通过装置密钥 Kdi 解密，解密结果将成为 0。比如如果第 3 记录内容的 E(Kd3,0) 通过装置密钥 Kd3 解密，则解密结果将成为 0。

[0144] 通过是把与上述 128 种装置密钥对应的各记录内容设为 E(Kdi, Km)，还是设为 E(Kdi,0)，可以把装置密钥的种类分为能获取媒体密钥的装置密钥和不能获取媒体密钥的装置密钥。

[0145] 记录型媒体 70 的制造者在制造该媒体时，获取曾经受到了物理性攻击的设备的信息，根据该信息把各装置密钥类型分为能获取媒体密钥的装置密钥和不能获取媒体密钥的装置密钥，生成把能获取媒体密钥的装置密钥所对应的记录内容设为 E(Kdi,Km)，把不能获取媒体密钥的装置密钥所对应的记录内容设为 E(Kdi,0) 的媒体密钥数据，并把它记录到媒体密钥数据区 25 内。这样，只有在采用特定媒体密钥的场合下，才能取出媒体密钥，在采用其它的装置密钥的场合下，不能取出媒体密钥。

[0146] < 记录设备 60 的构成 >

[0147] 记录设备 60 与记录设备 10 的构成的不同点是没有主密钥存储部 11，而是设置了装置密钥存储部 17、媒体密钥计算部 18 及媒体密钥暂时存储部 19。

[0148] 装置密钥存储部 17 是用于预先存储对记录设备 60 分配的装置密钥的存储器。记录设备 60 配有对外保密的装置密钥。

[0149] 媒体密钥计算部 18 从装置密钥存储部 17 中读出装置密钥，并从媒体密钥数据区 25 的与该记录设备 60 的装置编号对应的记录内容中读出加密数据。这样，媒体密钥计算部 18 利用装置密钥对加密数据解密。由于加密数据是 E(Kdi,Km) 或 E(Kdi,0)，因而通过装置密钥 Kdi 解密后，可以得到媒体密钥 Km 或 0。媒体密钥计算部 18 对所得到的值是否为 0 进行判定，在为 0 的场合下，中止记录设备 60 以后的处理。即中止内容密钥及内容的加密等处理。

[0150] 另一方面，媒体密钥计算部 18 在所得到的值是媒体密钥 Km 的场合下，把媒体密钥 Km 暂时存储到媒体密钥暂时存储部 19 内。所谓暂时存储意味着在从媒体密钥 Km 被存储时至媒体密钥 Km 被用于内容密钥加密等之后不需要时的期间内，把媒体密钥 Km 存储到媒体密钥暂时存储部 19 内，这一期间结束后，对媒体密钥暂时存储部 19 进行初始化处理，删除媒体密钥 Km 的值。通过这种必要时以外的删除处理，可以把记录设备 60 受到物理性攻击后的被害程度降到最低。

[0151] 媒体密钥暂时存储部 19 是一种用于对由媒体密钥计算部 18 解密后的媒体密钥 Km 进行暂时存储的存储器。

[0152] 许可信息计算部 16 及内容密钥加密部 13 各自的机构虽然与第 1 实施方式相同，但与第 1 实施方式的不同点是，没有主密钥，而是采用被存储在媒体密钥暂时存储部 19 内的媒体密钥 Km。

[0153] < 再生设备 80 的构成 >

[0154] 再生设备 80 与再生设备 30 的构成相比，不同点是没有主密钥存储部 31，而是设置

了装置密钥存储部 40、媒体密钥计算部 41、媒体密钥暂时存储部 42。

[0155] 装置密钥存储部 40 是用于预先存储对再生设备 80 分配的装置密钥的存储器。再生设备 80 配有对外保密的装置密钥。

[0156] 媒体密钥计算部 41 从装置密钥存储部 40 内读出装置密钥，并从媒体密钥数据区 25 的与该再生设备 80 的装置编号对应的记录内容中读出加密数据。这样，媒体密钥计算部 41 利用装置密钥对加密数据解密。由于加密数据是 E(Kdi,Km) 或 E(Kdi,0)，因而通过装置密钥 Kdi 解密后，得到媒体密钥 Km 或 0。媒体密钥计算部 41 对所得到的值是否为 0 进行判定，在为 0 的场合下，中止再生设备 80 以后的处理。即中止内容密钥及内容的解密等处理。

[0157] 另一方面，媒体密钥计算部 41 在所得到的值是媒体密钥 Km 的场合下，把媒体密钥 Km 暂时存储到媒体密钥暂时存储部 42 内。所谓暂时存储意味着在从媒体密钥 Km 被存储时至媒体密钥 Km 被用于加密内容密钥解密后不需要时的期间内，把媒体密钥 Km 存储到媒体密钥暂时存储部 42 内，这一期间结束后，对媒体密钥暂时存储部 42 实施初始化处理，删除媒体密钥 Km 的值。通过这种必要时以外的删除处理，可以把再生设备 80 受到物理性攻击后的被害程度降到最低。

[0158] 媒体密钥暂时存储部 42 是一种用于对由媒体密钥计算部 41 解密后的媒体密钥 Km 进行暂时存储的存储器。

[0159] 参照许可信息计算部 35 及内容密钥解密部 32 各自的机构虽然与第 1 实施方式相同，但与第 1 实施方式的不同点是，没有主密钥，而是采用被存储在媒体密钥暂时存储部 42 内的媒体密钥 Km。

[0160] < 动作 >

[0161] 以下对上述构成的记录设备 60 及再生设备 80 各自的动作作以说明。

[0162] 首先说明记录设备 60 的动作。

[0163] (1) 记录设备 60 中的媒体密钥计算部 18 从装置密钥存储部 17 中获取装置密钥，从媒体密钥数据区 25 获取记录设备 60 所对应的记录内容的加密数据。

[0164] (2) 其次，媒体密钥计算部 18 利用装置密钥对加密数据解密，对其结果是否为 0 进行判定。

[0165] (3) 在解密结果为 0 的场合下，记录设备 60 中止以后的加密处理。

[0166] (4) 在解密结果不为 0 的场合下，媒体密钥计算部 18 在媒体密钥暂时存储部 19 内存储作为解密结果的媒体密钥。

[0167] (5) 接下来，记录设备 60 实施与图 4 的流程图相同的处理。但在图 4 及其说明中的主密钥存储部 11 更换为媒体密钥暂时存储部 19，主密钥更换为媒体密钥。

[0168] (6) 最后，记录设备 60 对媒体密钥暂时存储部 19 进行初始化处理，删除媒体密钥的值。

[0169] 接下来对再生设备 80 的动作作以说明。

[0170] (1) 再生设备 80 中，媒体密钥计算部 41 从装置密钥存储部 40 中获取装置密钥，从媒体密钥数据区 25 获取再生设备 80 所对应的记录内容的加密数据。

[0171] (2) 接下来，媒体密钥计算部 41 利用装置密钥对加密数据解密，对其结果是否为 0 进行判定。

[0172] (3) 在解密结果为 0 的场合下，再生设备 80 中止其后的解密处理。

[0173] (4) 在解密结果不为 0 的场合下，媒体密钥计算部 41 把作为解密结果的媒体密钥存储到媒体密钥暂时存储部 42 内。

[0174] (5) 接下来，再生设备 80 实施与图 5 的流程图相同的处理。但在图 5 及其说明中的主密钥存储部 31 更换为媒体密钥暂时存储部 42，主密钥更换为媒体密钥。

[0175] (6) 最后，再生设备 80 对媒体密钥暂时存储部 42 进行初始化处理，删除媒体密钥的值。

[0176] < 效果 >

[0177] 通过上述构成，在著作权保护系统 200 中，通过是把媒体密钥数据的各记录内容的加密数据设为 E(Kdi, Km)，还是设为 E(Kdi,0)，只利用特定的装置密钥便可使媒体密钥解密，采用除此之外的其它装置密钥则不能对媒体密钥解密。

[0178] 这样，比如如果一台设备受到第三者的物理性攻击，装置密钥暴露，记录型媒体 70 的制造者便可以生成把该设备所对应的记录内容的加密数据设为 E(Kdi,0) 的媒体密钥数据，并把它记录到记录型媒体 70 内。这样，即使第三者试图利用已暴露的装置密钥非法获取媒体密钥也是徒劳的。这样，由于第三者不能得到媒体密钥，因而不能使通过该媒体密钥被加密的加密内容密钥及加密内容解密，从而可以防止第三者非法利用内容。

[0179] 此外著作权保护系统 200 通过是把媒体密钥数据的各记录内容的加密数据设为 E(Kdi, Km)，还是设为 E(Kdi,0)，对是否发挥各设备的加密或解密功能进行控制。

[0180] 比如，如果一台设备的装置密钥被暴露，通过把该设备所对应的记录内容的加密数据设为 E(Kdi,0)，便可以使该设备无法使用。

[0181] 此外由于在著作权保护系统 200 中，只要加密数据不为 E(Kdi,0)，便可以在具有不同的装置密钥的记录设备、再生设备之间利用通用的记录型媒体，因而具有不影响记录型媒体的可移动性的效果。

[0182] 此外虽然记录设备 60 及再生设备 80 具有在通过装置密钥对加密数据解密后的解密结果是 0 的场合下，中止内容的加密或解密处理的构成，但也可以采用不中止处理，以 0 作为密钥使用，实施加密或解密的构成。以 0 作为密钥被加密的加密内容密钥及加密内容不能利用媒体密钥 Km 解密。此外反之，利用媒体密钥 Km 加密的加密内容密钥及加密内容不能以 0 作为密钥解密。这样，可以防止通过受到物理性攻击的设备非法利用内容。

[0183] 虽然装置密钥为各设备固有，但也可以为由多台设备组成的各组固有。在该场合下，当一台设备受到物理性攻击时，通过把该设备所对应的加密数据设为 E(Kdi,0)，虽然该设备所属组内的所有设备都不能使用，但除此之外的其它组的设备还可以使用。

[0184] < 第 3 实施方式 >

[0185] 以下对本发明的第 3 实施方式作以说明。

[0186] 在上述第 1 及第 2 实施方式中，记录设备配有内容密钥加密部，再生设备配有内容密钥解密部，因而记录设备与再生设备具有不同的构成要素。这对于设备的制造成本方面是不利的。因此在第 3 实施方式中，记录设备与再生设备配有相同的内容密钥生成部，以降低成本。

[0187] 图 8 是表示第 3 实施方式的著作权保护系统 300 的构成方框图。

[0188] 该图中，著作权保护系统由用于在记录型媒体 120 内记录加密内容的记录设备 110、对被记录在记录型媒体 120 内的加密内容进行解密及再生的再生设备 130 构成。

[0189] 该图中，与图 3 具有相同符号的构成要素是相同的部件。以下以不同的部分为中心作说明。

[0190] 记录型媒体 120 没有加密内容密钥区 23，而配有随机数区 121，这一点与记录型媒体 20 不同，其它部分与记录型媒体 20 相同。

[0191] 随机数区 121 由记录设备 110 在记录型媒体 120 的记录区内确保，用于记录随机数。该随机数是内容密钥的源数。

[0192] 记录设备 110 与记录设备 10 相比，不同点是，没有配备内容密钥发生部 12 及内容密钥加密部 13，而配备了随机数发生部 111 及内容密钥生成部 112。其它的构成要素与记录设备 10 相同。

[0193] 随机数发生部 111 用于发生随机数，并向许可信息计算部 16 及内容密钥生成部 112 输出，此外在记录型媒体 120 的记录区内确保随机数区 121，对该随机数进行记录。

[0194] 内容密钥生成部 112 利用由随机数发生部 111 提供的随机数及被存储在主密钥存储部 11 内的主密钥，实施比如散列函数 SHA-1 等的运算，生成内容密钥。

[0195] 内容加密部 15 利用由内容密钥生成部 112 生成的内容密钥对内容加密，并记录到加密内容区 24 内。

[0196] 许可信息计算部 16 获取媒体固有编号、主密钥、随机数发生部 111 的随机数，将它们连接成一个位串，实施作为输入该位串的散列函数 SHA-1 等的运算。把该运算结果的散列值作为许可信息记录到许可信息区 22 内。

[0197] 再生设备 130 与再生设备 30 相比，不同点是没有内容密钥解密部 32，而设置了内容密钥生成部 131。其它构成要素与再生设备 30 相同。

[0198] 内容密钥生成部 131 与内容密钥生成部 112 相同，利用被记录在随机数区 121 内的随机数与被存储在主密钥存储部 31 内的主密钥，实施与内容密钥生成部 112 相同的运算，生成内容密钥。

[0199] 内容解密部 33 利用由内容密钥生成部 131 所生成的内容密钥对内容解密。

[0200] 参照许可信息计算部 35 获取媒体固有编号与主密钥及随机数区 121 的随机数，实施与记录设备 110 的许可信息计算部 16 相同的运算，生成参照许可信息。

[0201] 通过上述构成，与在著作权保护系统 100 的制造中，需要制造内容密钥加密部与内容密钥解密部相比，在著作权保护系统 300 的制造中，不制造上述二种单元，而是制造二个内容密钥生成部，著作权保护系统 300 与著作权保护系统 100 相比可以抑制制造成本。

[0202] < 第 4 实施方式 >

[0203] 接下来对本发明的第 4 实施方式作以说明。

[0204] 本实施方式下的著作权保护系统是一种分别将著作权保护系统 300 及著作权保护系统 200 的特征部分组合起来的构成。

[0205] 图 9 是表示第 4 实施方式下的著作权保护系统 400 的构成方框图。

[0206] 同图中的著作权保护系统 400 由用于在记录型媒体 170 内记录加密内容的记录设备 160 与对被记录在记录型媒体 170 内的加密内容解密并再生的再生设备 180 构成。

[0207] 在同图中，与图 6 及图 8 相同符号的构成要素是相同的部件。

[0208] 记录型媒体 170 是一种在记录型媒体 120 中增加了记录型媒体 70 的媒体密钥数据区 25 的构成。

[0209] 在记录设备 160 的构成中，把记录设备 110 的主密钥存储部 11 更换为记录设备 60 的装置密钥存储部 17、媒体密钥计算部 18 及媒体密钥暂时存储部 19。

[0210] 在再生设备 180 的构成中，把再生设备 130 的主密钥存储部 31 更换为再生设备 80 的装置密钥存储部 40、媒体密钥计算部 41 及媒体密钥暂时存储部 42。

[0211] 通过上述构成，著作权保护系统 400 同时具备著作权保护系统 200 与著作权保护系统 300 双方的优点。

[0212] < 其它实施方式 >

[0213] 以上虽然对实施方式 1 ～ 4 作了说明，但不言而喻本发明并不局限于上述实施方式。即，

[0214] (1) 实施方式 1 是一种记录设备 10 在记录型媒体 20 内分别各记录一个许可信息、加密内容密钥及加密内容的构成。但没有必要局限于各记录一个。比如记录设备也可以如图 10 所示的记录型媒体 800 那样，采用记录多个许可信息、加密内容密钥及加密内容的构成。

[0215] 更详细地说，记录设备利用内容密钥 A、B、C 分别对多个内容 A、B、C 加密，把加密内容 A、B、C 记录到加密内容区 840 中。此外利用主密钥分别对内容密钥 A、B、C 加密，将加密内容密钥 A、B、C 记录到加密内容密钥区 830 内。此外全部利用媒体固有编号、主密钥及加密内容密钥 A 生成许可信息 A，并记录到许可信息区 820 内。对于许可信息 B、C，也可以按照与许可信息 A 场合下相同的顺序生成，并记录到许可信息区 820 内。

[0216] 再生设备利用媒体固有编号、主密钥及加密内容密钥区 830 的加密内容密钥 A 生成参照许可信息 A，把它与许可信息区 820 的许可信息 A 进行比较，只有在一致的场合下，才能利用主密钥对加密内容密钥区 830 的加密内容密钥 A 解密，利用解密后的内容密钥 A 对加密内容区 840 的加密内容 A 解密，使解密后的内容 A 再生。对于加密内容 B、C，按照与加密内容 A 场合下相同的顺序解密、再生。

[0217] (2) 此外记录设备也可以按图 11 所示的记录型媒体 900 的方式记录。

[0218] 更详细地说，记录设备按照与上述 (1) 中相同的方法生成加密内容 A、B、C 及加密内容密钥 A、B、C，把它们记录到加密内容区 940 及加密内容密钥区 930 内。以此全部利用媒体固有编号、主密钥、加密内容密钥 A、B、C 生成许可信息，并记录到许可信息区 920 内。

[0219] 再生设备全部利用媒体固有编号、主密钥、加密内容密钥 A、B、C 生成参照许可信息，把它与许可信息区 920 的许可信息进行比较，只有在一致的场合下，才能利用主密钥对加密内容密钥 A、B、C 解密，利用内容密钥 A、B、C 对加密内容 A、B、C 解密、再生。

[0220] (3) 记录型媒体 20 并不局限于光盘，也可以是在不能在磁盘、光磁盘、存储卡等其它记录媒体内改写媒体固有编号的状态下附加的媒体。

[0221] (4) 媒体固有编号在不能改写的状态下，而且在可以由读出机构读出的状态下，也可以被记录到不能改写的区域以外的其它位置上。

[0222] (5) 虽然在各实施方式下，在各种运算中采用散列函数 SHA-1、DES 等，但没有必要局限于此。也可以采用其它种类的散列函数和其它种类的运算。而且没有必要将各值的位数限定于 56 位或 64 位。

[0223] (6) 许可信息及参照许可信息也可以是不采用主密钥的按照能反映媒体固有编号及与解密有关的信息这二者的方式生成的信息。

[0224] (7) 比较部 36 虽然采用根据第 1 开关 37 与第 2 开关 38 的开闭对各构成要素进行控制的构成，但没有必要局限于该构成。原则是，应采用只有在许可信息与参照许可信息一致的场合下，数字 AV 处理部 34 才能使加密内容再生，在不一致的场合下不能再生的构成。

[0225] (9) 报警器 39 也可采用不发出警告音，而向显示器输出显示警告信息的数据的构成。

[0226] (10) 也可以把上述实施方式 1 ～ 4 及图 10、11 的记录型媒体所对应的各著作权保护系统的动作顺序作为一种方法。

[0227] (11) 也可以把上述实施方式 1 ～ 4 的各著作权保护系统的各构成要素的动作顺序设为程序，通过计算机运行该程序。此外也可以把该程序记录到记录媒体内，或者利用各种通信线路等使其流通。这种记录媒体包括 IC 卡、光盘、软盘、ROM 等。

[0228] (12) 再生设备也可以配备在某种记录型媒体的加密内容的再生中，检测警报器的动作是否超出规定次数的机构、在检测时在记录型媒体的该加密内容中记录该超规标记的机构、检查有无标记，在有标记的场合下，不对该加密内容解密的机构。此外再生设备也可以被设计成在判定出记录型媒体的许可信息与参照许可信息不一致的场合下，把该记录型媒体的记录内容加工成不可利用的状态的构成。该加工方法包括比如 (i) 再生设备删除该记录型媒体的记录内容，(ii) 把该记录型媒体的媒体固有编号存储到存储器内，在与再生设备连接的记录型媒体的媒体固有编号与存储器的内容一致的场合下，不实施记录内容读出等。

[0229] (13) 也可以把上述实施方式 1 ～ 4 及上述 (1) ～ (12) 组合起来实施。

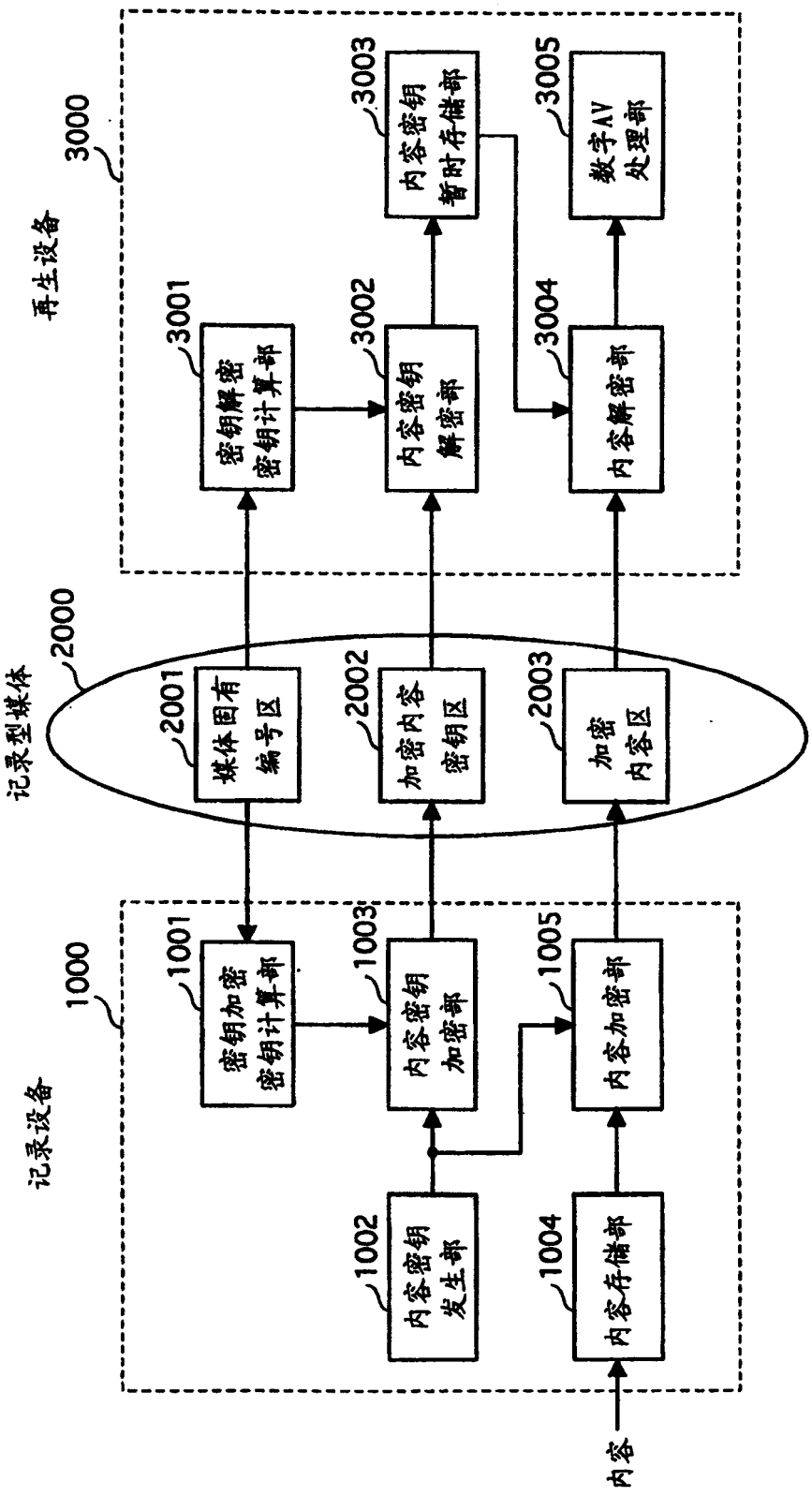

再生设备
3000
3001
密钥解密
密钥计算部
3002
内容密钥
解密部
3003
内容密钥
暂时存储部
3004
内容解密部
3005
数字AV
处理部
记录型媒体
2000
2001
媒体固有
编号区
2002
加密内容
密钥区
2003
加密
内容区
记录设备
1000
1001
密钥加密
密钥计算部
1002
内容密钥
发生部
1003
内容密钥
加密部
1004
内容存储部
1005
内容加密部
内容

图 1

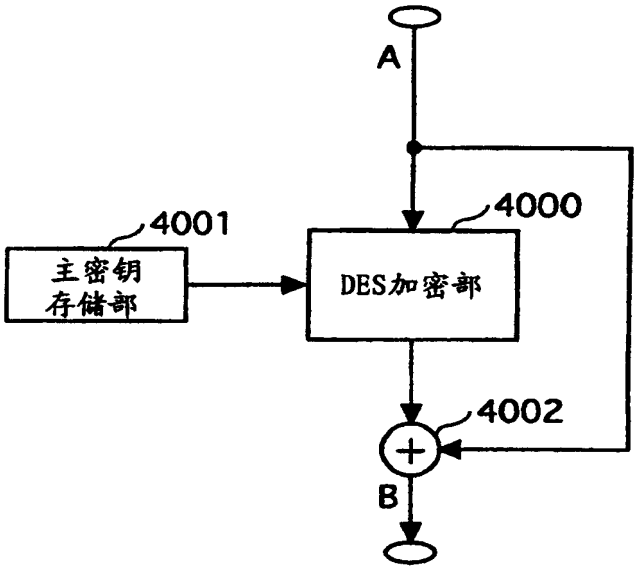


图 2

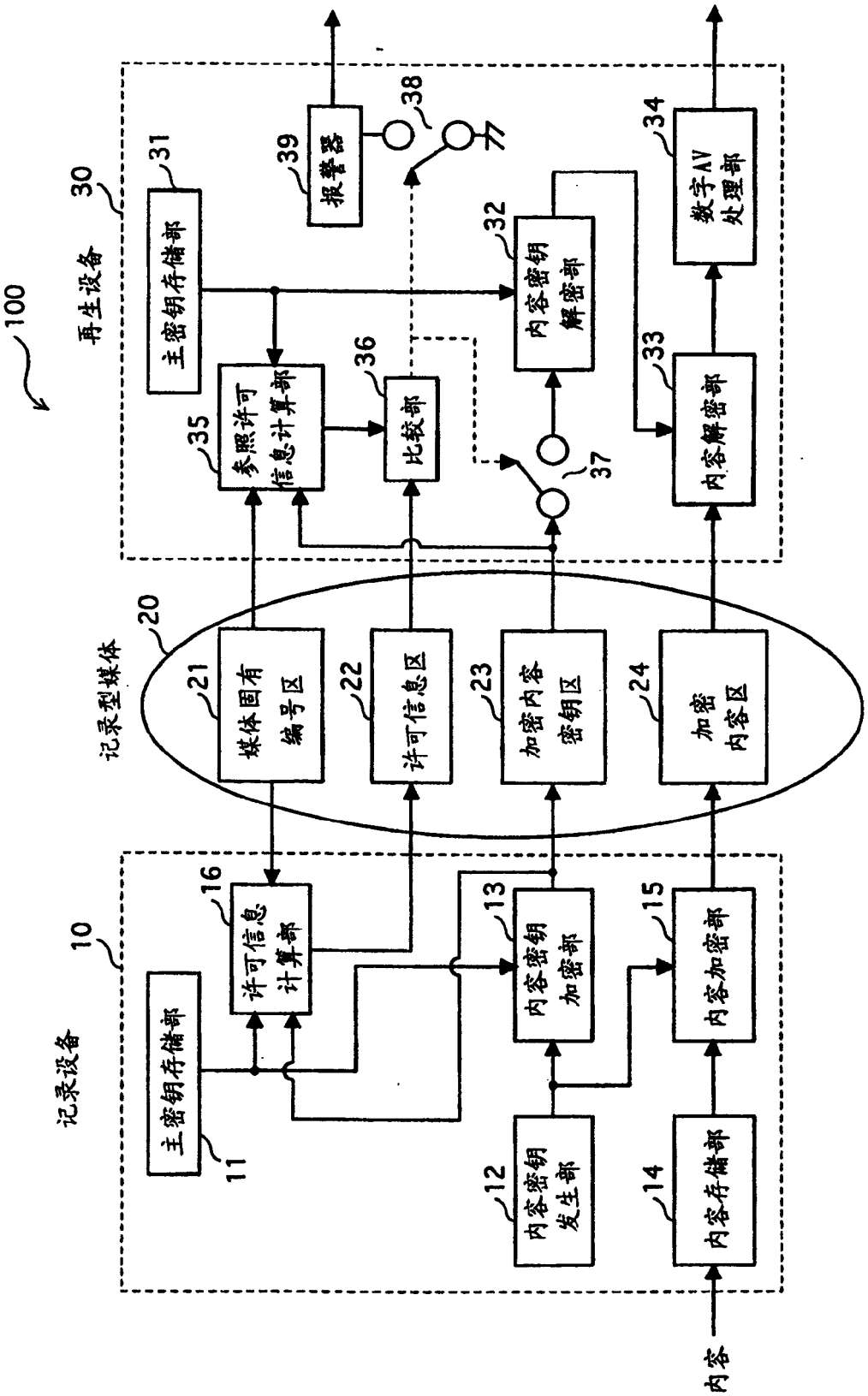

100
再生设备
30
主密钥存储部
31
参照许可信息计算部
35
比较部
36
报警器
39
38
77
内容密钥解密部
32
37
内容解密部
33
数字AV处理部
34
记录型媒体
20
媒体固有编号区
21
许可信息区
22
加密内容密钥区
23
加密内容区
24
记录设备
10
主密钥存储部
11
许可信息计算部
16
内容密钥加密部
13
内容加密部
15
内容密钥发生部
12
内容存储部
14
内容

图 3

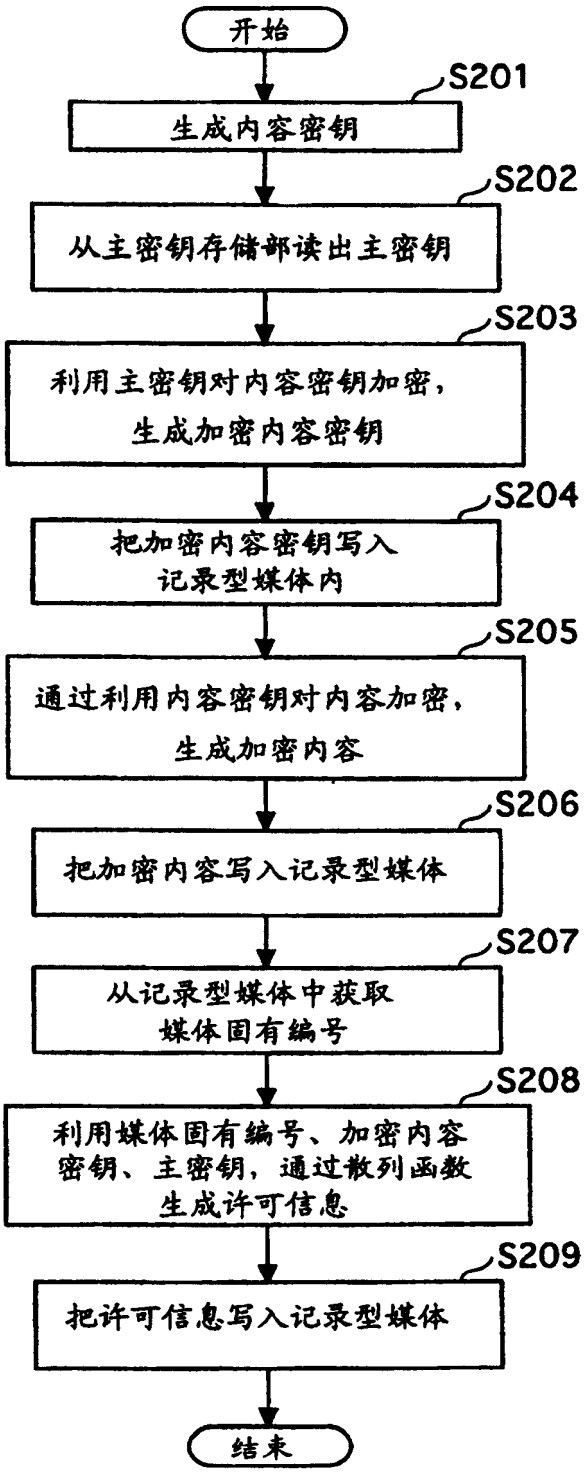

开始
S201
生成内容密钥
S202
从主密钥存储部读出主密钥
S203
利用主密钥对内容密钥加密，
生成加密内容密钥
S204
把加密内容密钥写入
记录型媒体内
S205
通过利用内容密钥对内容加密，
生成加密内容
S206
把加密内容写入记录型媒体
S207
从记录型媒体中获取
媒体固有编号
S208
利用媒体固有编号、加密内容
密钥、主密钥，通过散列函数
生成许可信息
S209
把许可信息写入记录型媒体
结束

图 4

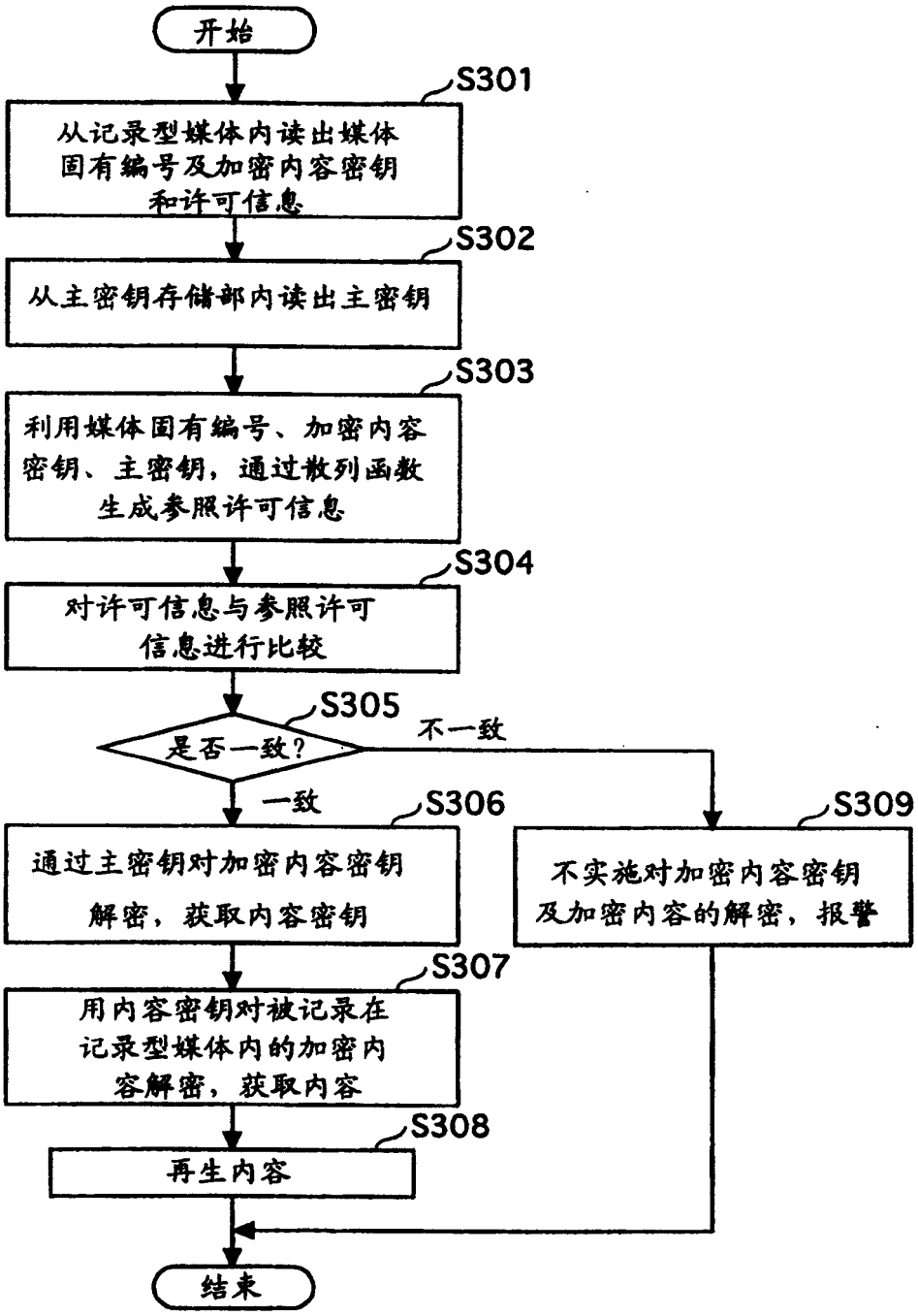

开始
S301
从记录型媒体内读出媒体固有编号及加密内容密钥和许可信息
S302
从主密钥存储部内读出主密钥
S303
利用媒体固有编号、加密内容密钥、主密钥，通过散列函数生成参照许可信息
S304
对许可信息与参照许可信息进行比较
S305
是否一致?
不一致
一致
S306
通过主密钥对加密内容密钥解密，获取内容密钥
S309
不实施对加密内容密钥及加密内容的解密，报警
S307
用内容密钥对被记录在记录型媒体内的加密内容解密，获取内容
S308
再生内容
结束

图 5

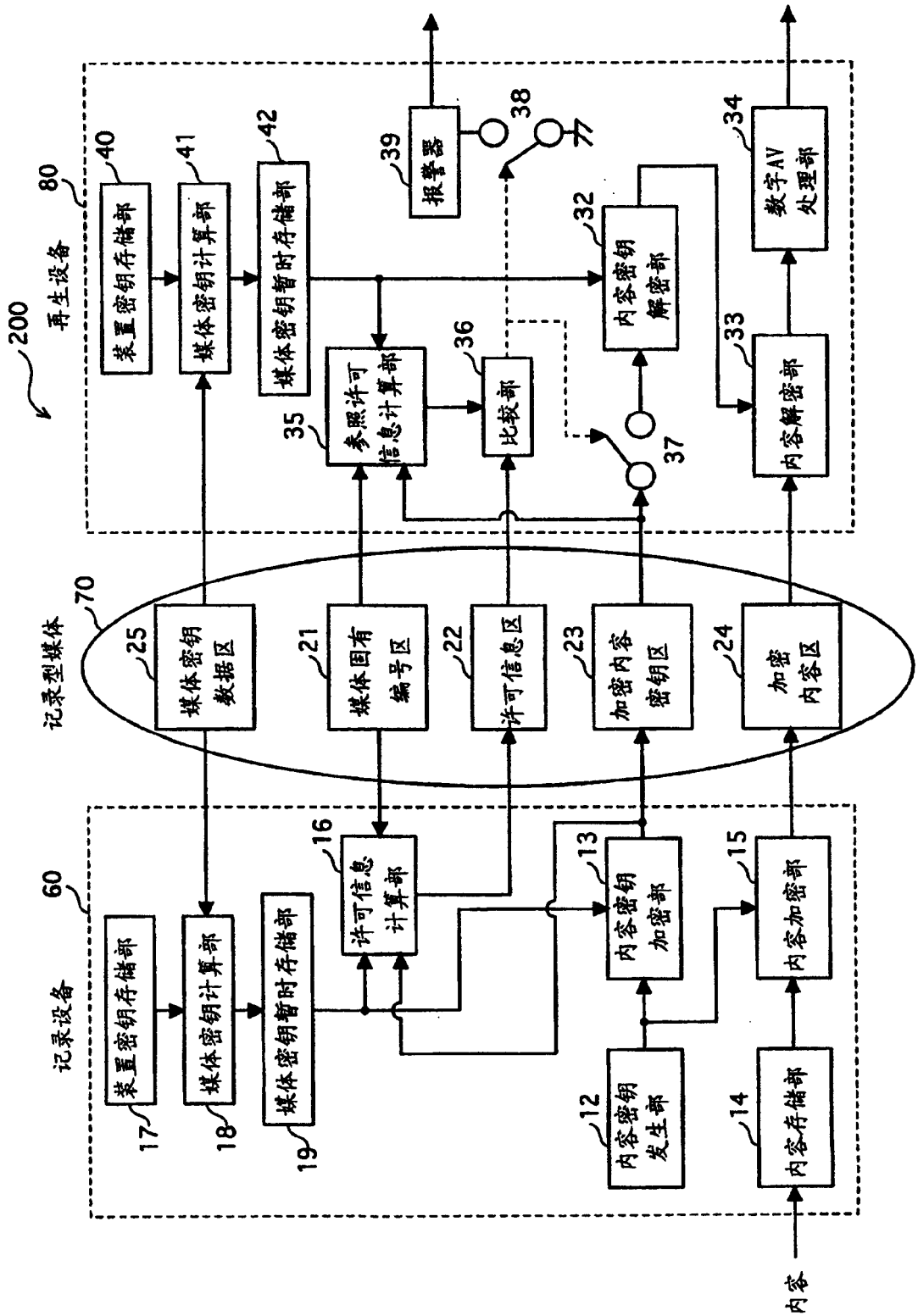

200
再生设备
80
装置密钥存储部
40
媒体密钥计算部
41
媒体密钥暂时存储部
42
报警器
39
38
77
数字AV处理部
34
内容密钥解密部
32
参照许可信息计算部
35
比较部
36
内容解密部
33
37
记录型媒体
70
媒体密钥数据区
25
媒体固有编号区
21
许可信息区
22
加密内容密钥区
23
加密内容区
24
记录设备
60
装置密钥存储部
17
媒体密钥计算部
18
媒体密钥暂时存储部
19
许可信息计算部
16
内容密钥加密部
13
内容加密部
15
内容密钥发生部
12
内容存储部
14
内容

图 6

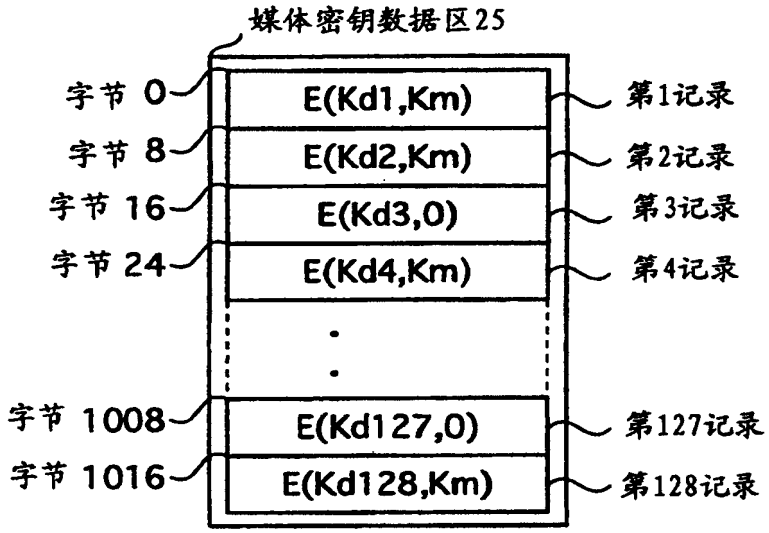

媒体密钥数据区25
字节 0
字节 8
字节 16
字节 24
字节 1008
字节 1016
E(Kd1,Km)
E(Kd2,Km)
E(Kd3,0)
E(Kd4,Km)
E(Kd127,0)
E(Kd128,Km)
第1记录
第2记录
第3记录
第4记录
第127记录
第128记录

图 7

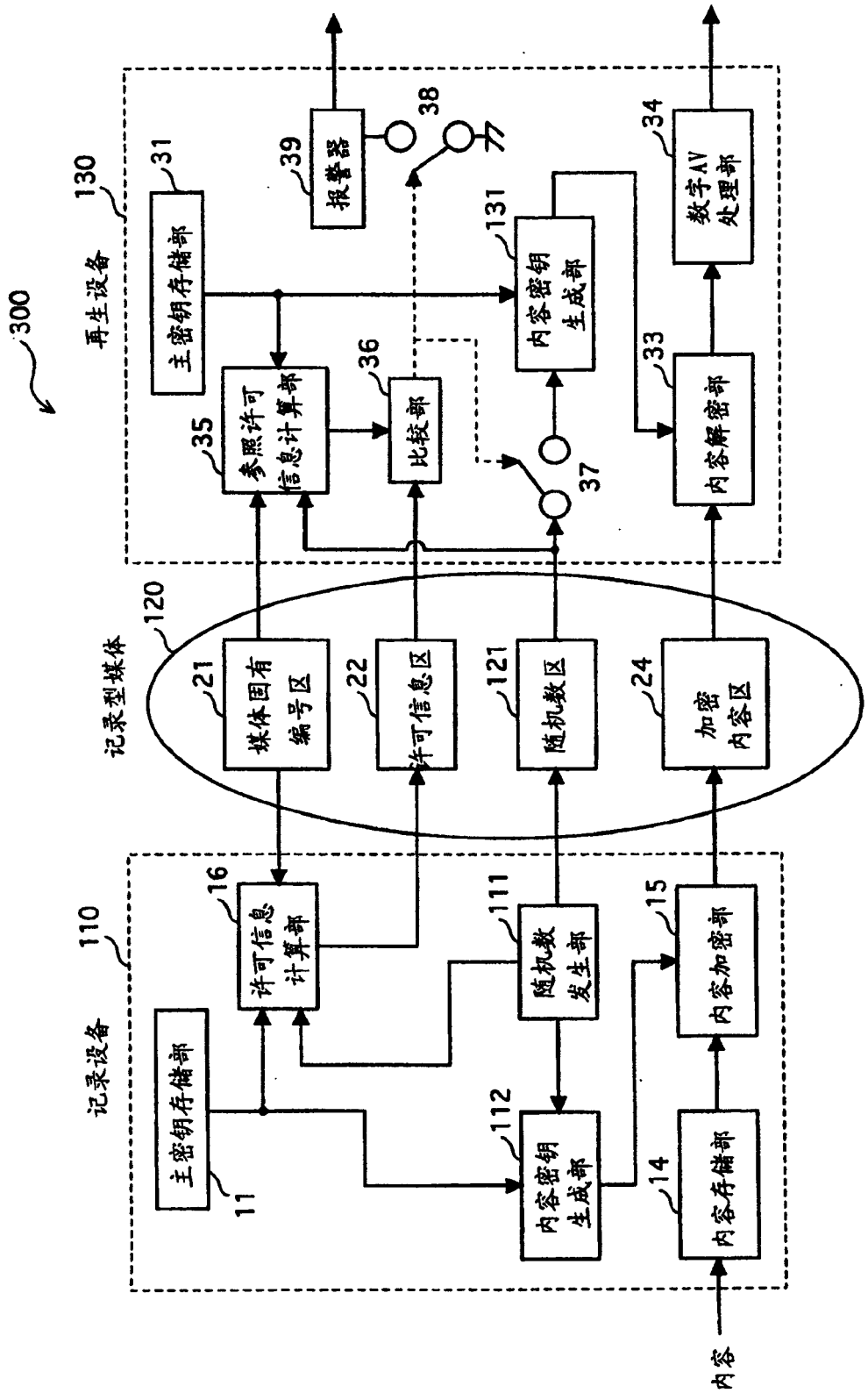

300
再生设备
130
主密钥存储部
31
参照许可信息计算部
35
比较部
36
报警器
39
38
37
内容密钥生成部
131
数字AV处理部
34
内容解密部
33
记录型媒体
120
媒体固有编号区
21
许可信息区
22
随机数区
121
加密内容区
24
记录设备
110
主密钥存储部
11
许可信息计算部
16
随机数发生部
111
内容密钥生成部
112
内容加密部
15
内容存储部
14
内容

图 8

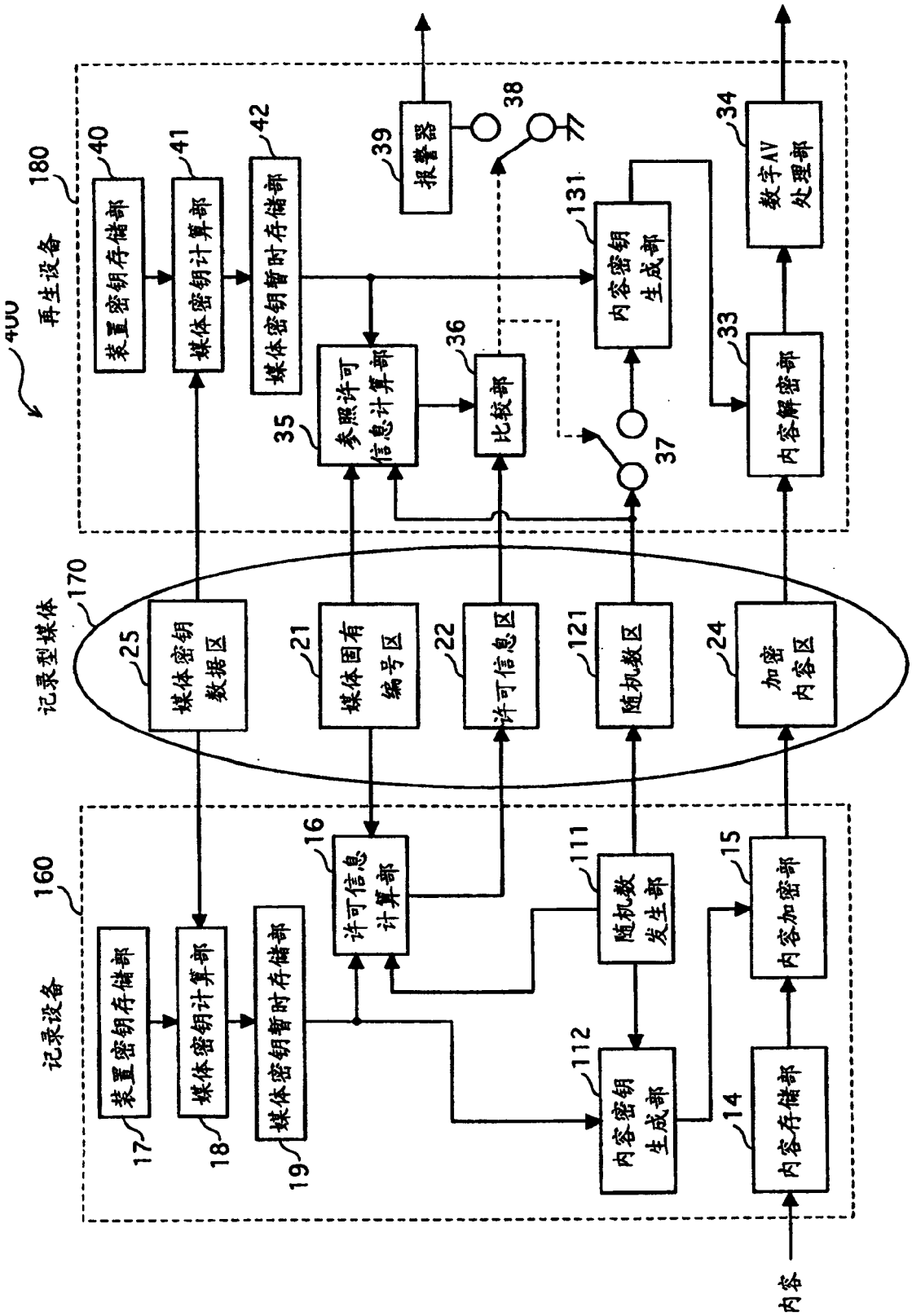

400
再生设备
180
装置密钥存储部
40
媒体密钥计算部
41
媒体密钥暂时存储部
42
报警器
39
38
77
数字AV处理部
34
内容密钥生成部
131
参照许可信息计算部
35
比较部
36
37
内容解密部
33
记录型媒体
170
媒体密钥数据区
25
媒体固有编号区
21
许可信息区
22
随机数区
121
加密内容区
24
记录设备
160
装置密钥存储部
17
媒体密钥计算部
18
媒体密钥暂时存储部
19
许可信息计算部
16
随机数发生部
111
内容密钥生成部
112
内容加密部
15
内容存储部
14
内容

图 9

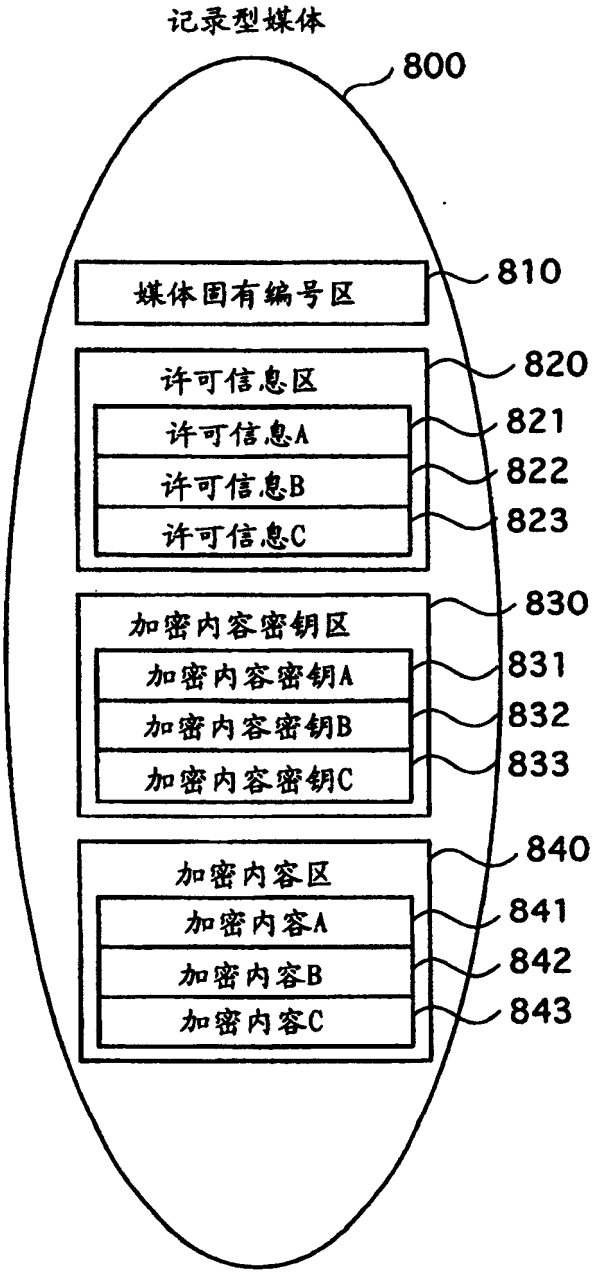

记录型媒体
800
媒体固有编号区
810
许可信息区
820
许可信息A
821
许可信息B
822
许可信息C
823
加密内容密钥区
830
加密内容密钥A
831
加密内容密钥B
832
加密内容密钥C
833
加密内容区
840
加密内容A
841
加密内容B
842
加密内容C
843

图 10

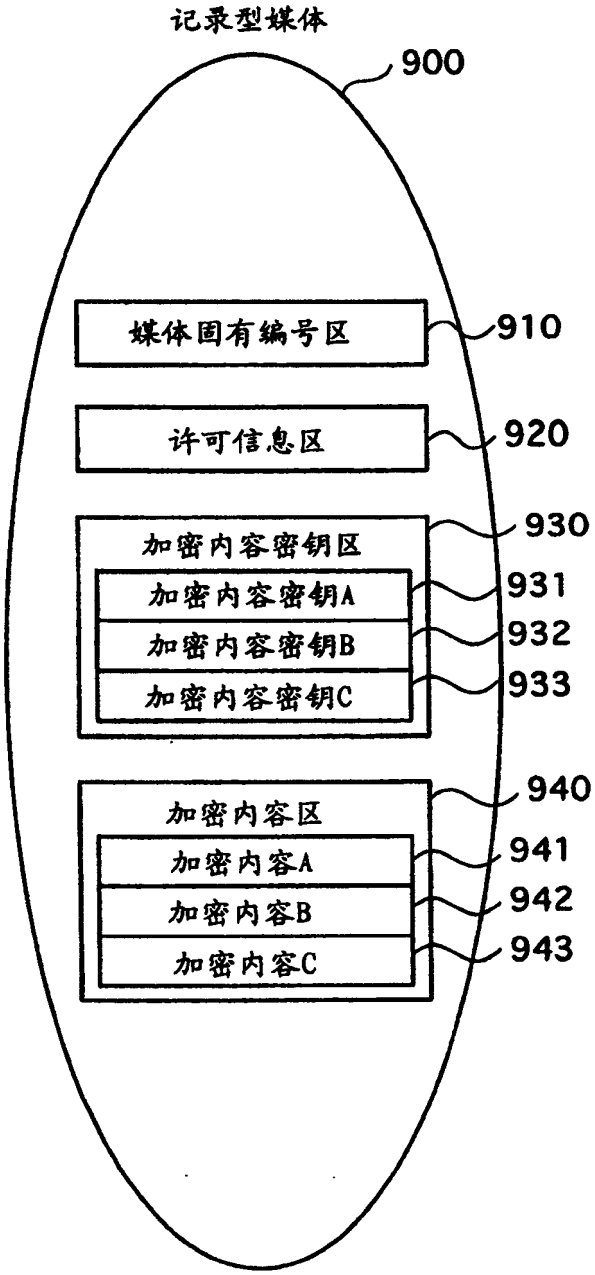

记录型媒体
900
媒体固有编号区
910
许可信息区
920
加密内容密钥区
930
加密内容密钥A
931
加密内容密钥B
932
加密内容密钥C
933
加密内容区
940
加密内容A
941
加密内容B
942
加密内容C
943

图 11