

[19] 中华人民共和国国家知识产权局

[51] Int. Cl'

G11B 20/10

G11B 20/12 G06F 17/60

G06F 3/06 H04N 5/91

H04L 9/00



[12] 发明专利申请公开说明书

[21] 申请号 00819187.5

[43] 公开日 2003 年 8 月 20 日

[11] 公开号 CN 1437749A

[22] 申请日 2000.12.26 [21] 申请号 00819187.5

[30] 优先权

[32] 1999.12.28 [33] JP [31] 375777/1999

[32] 2000.8.17 [33] JP [31] 247688/2000

[86] 国际申请 PCT/JP00/09260 2000.12.26

[87] 国际公布 WO01/48755 日 2001.7.5

[85] 进入国家阶段日期 2002.8.26

[71] 申请人 松下电器产业株式会社

地址 日本国大阪府门真市

[72] 发明人 吉田修一 冈田孝文 久野良树

米野润一 神门俊和 清水亮辅

久保德章

[74] 专利代理机构 上海专利商标事务所

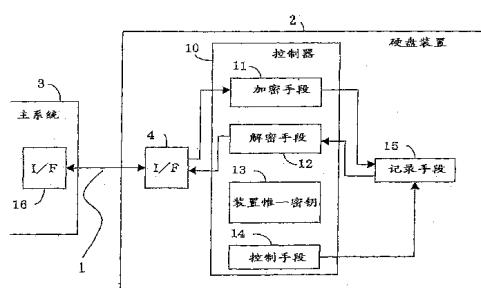
代理人 孙敬国

权利要求书 14 页 说明书 72 页 附图 39 页

[54] 发明名称 记录装置、重放装置、数据处理装置、记录重放装置、数据发送装置

[57] 摘要

在将 AV 等数据记录到记录装置的情况下以及/或者由重放装置重放数据的情况下，没有保护著作权的具体构成环节。具备：将从接口 4 传送来的 AV 数据进行加密的加密手段 11；进行控制以记录加密后的 AV 数据的控制手段 14；以及由控制手段 14 控制并将加密后的 AV 数据记录到磁盘上的记录手段 15，控制手段 14 进行控制以使得重放所记录的数据，记录手段 15 由控制手段 14 控制并且重放记录到盘片上的数据，解密手段 12 将重放后的数据解密并发送到接口。



1. 一种记录装置，其特征在于，具备

将从接口传送来的数据加密的加密手段；

进行控制以使得记录所述加密后的数据的控制手段；

由所述控制手段控制并将所述加密后的数据记录到盘片上的记录手段。

2. 如权利要求 1 所述的记录装置，其特征在于，

所述加密手段采用分配给记录装置本身的固有数值以及/或者记号即装置惟一密钥将所述数据加密。

3. 如权利要求 1 或 2 所述的记录装置，其特征在于，

所述加密手段采用与所述控制手段连续访问所述记录手段的最小单位即记录单元对应的记录块所固有的编号以及/或者记号的记录单元信息，将所述数据加密。

4. 如权利要求 3 所述的记录装置，其特征在于，

采用所述记录单元信息将所述数据加密是，以根据所述记录单元信息所获得的密钥将所述数据加密。

5. 如权利要求 3 或 4 所述的记录装置，其特征在于，

至少记录在所述记录块中的、所述加密后的数据以及附加在所述加密后的数据中的附加信息的所有部分都被加密并记录在所述记录手段。

6. 如权利要求 3~5 中任意一项所述的记录装置，其特征在于，

在所述数据中附加复制许可信息，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述复制许可信息，

所述加密手段生成第 1 信息，所述第 1 信息包含所述装置惟一密钥与所述复制许可信息中的至少一个，

采用所述记录单元信息，所述加密手段生成将所述第 1 信息加密后的信息即内容密钥，

所述加密手段采用所述内容密钥将所述数据加密，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的数据。

7. 如权利要求 2 所述的记录装置，其特征在于，

对于所述数据，分配所述数据所固有的数值以及/或者记号即标题密钥，所述加密手段采用所述装置惟一密钥将所述标题密钥加密，所述控制手段控制所述记录手段，以使得将所述加密后的标题密钥记录到所述记录手段。

8. 如权利要求 7 所述的记录装置，其特征在于，

所述加密手段采用所述标题密钥将所述数据加密。

9. 如权利要求 8 所述的记录装置，其特征在于，

所述加密手段采用所述装置惟一密钥将所述标题密钥加密，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的标题密钥，

所述加密手段生成包含所述标题密钥的第 3 信息，

所述加密手段采用记录单元信息生成将所述第 3 信息加密后的信息即内容密钥，所述记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，

所述加密手段采用所述内容密钥将所述数据加密，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的数据。

10. 如权利要求 8 所述的记录装置，其特征在于，

在所述数据中附加有复制许可信息，

所述加密手段也采用所述复制许可信息将所述数据加密。

11. 如权利要求 10 所述的记录装置，其特征在于，

所述加密手段采用所述装置惟一密钥将所述标题密钥加密，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的标题密钥，所述控制手段控制所述记录手段以使得所述记录手段记录所述复制许可信息，

所述加密手段生成第 2 信息，所述第 2 信息包含所述标题密钥与所述复制许可信息中的至少一个，

所述加密手段采用记录单元信息生成将所述第 2 信息加密后的信息即内容密钥，所述记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，

所述加密手段采用所述内容密钥将所述数据加密，

所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的数据。

12. 如权利要求 1 所述的记录装置，其特征在于，

所述加密手段采用所述复制许可信息将附加有复制许可信息的、从接口传送来的数据加密，

所述控制手段控制所述记录手段，以使得所述记录手段在记录所述数据之前以及/或者记录所述数据之后记录所述复制许可信息。

13. 如权利要求 12 所述的记录装置，其特征在于，

所述控制手段控制所述记录手段，以使得至少所述记录手段在记录所述数据之前记录所述复制许可信息。

14. 如权利要求 12 所述的记录装置，其特征在于，

所述控制手段控制所述记录手段，以使得所述记录手段仅在记录了所述数据之后记录所述复制许可信息。

15. 一种记录装置，其特征在于，具备

进行控制以使得记录从接口传送来的加密后的数据的控制手段；以及由所述控制手段控制且将所述加密后的数据记录到盘片上的记录手段。

16. 一种重放装置，其特征在于，具备

控制手段，进行控制以使得重放由权利要求 1 所述的记录装置记录到盘片上的加密后的数据；

由所述控制手段控制、重放所述数据的重放手段；以及

将所述重放后的数据解密并传送到接口的解密手段。

17. 一种重放装置，其特征在于，

具备：控制手段，进行控制以使得重放由权利要求 2 所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，

所述解密手段采用所述装置惟一密钥将所述重放后的数据解密。

18. 一种重放装置，其特征在于，

具备：控制手段，进行控制以使得重放由权利要求 3 所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，

所述解密手段采用所述记录单元信息将所述重放后的数据解密。

19. 一种重放装置，其特征在于，

具备：控制手段，进行控制以使得重放由权利要求 4 所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，

所述解密手段以根据所述记录单元信息所获得的密钥将所述重放后的数据解密。

20. 一种重放装置，其特征在于，

具备：控制装置，进行控制以使得重放由权利要求 14 所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，

在记录所述数据时，当不能够正常地将所述复制许可信息记录到所述记录手段中时，所述解密手段假设所述复制许可信息取各种值并试着对所述加密后的数据的全部或一部分进行解密，

在所述试着解密的结果为能够正常将所述重放后的数据解密时，采用所述复制许可信息的值，将所述重放后的数据解密。

21. 一种重放装置，其特征在于，

具备：控制装置，进行控制以使得重放由权利要求 15 所述的记录装置记录到盘片上的加密后的数据；以及由所述控制手段控制、重放所述数据的重放手段，

将所述重放后的数据传送到接口。

22. 如权利要求 1~14 任意一项所述的记录装置，其特征在于，

将所述接口、所述加密手段以及所述控制手段一体化设置在同一印刷基板上。

23. 如权利要求 22 所述的记录装置，其特征在于，

使得所述接口、所述加密手段以及所述控制手段为一片芯片。

24. 如权利要求 16~20 任意一项所述的重放手段，其特征在于，

将所述接口、所述解密手段以及所述控制手段一体化地设置在同一印刷基板上。

25. 如权利要求 24 所述的记录装置，其特征在于，

将所述接口、所述解密手段以及所述控制手段作成一片芯片。

26. 如权利要求 22 所述的记录装置，其特征在于，

从所述印刷基板上的端子检测出的信号完全被加密以及/或者以非公开的格式描述记载，所述印刷基板上的端子输出由第3者能够作为数据重放的信息。

27. 如权利要求24所述的记录装置，其特征在于，

从所述印刷基板上的端子检测出的信号完全被加密以及/或者以非公开的格式描述，所述印刷基板上的端子输出由第3者能够作为数据重放的信息。

28. 如权利要求22所述的记录装置，其特征在于，

所述印刷基板上的端子的性质是以非公开的格式确定的，所述印刷基板上的端子输出由第3者能够作为数据重放的信号。

29. 如权利要求24所述的记录装置，其特征在于，

所述印刷基板上的端子的性质是以非公开的格式确定的，所述印刷基板上的端子输出由第3者能够作为数据重放的信号。

30. 如权利要求2~11任意一项所述的记录装置，其特征在于，

所述装置惟一密钥不能够由外部设备进行访问。

31. 如权利要求6、10、11、12、13、14中的任意一项所述的记录装置，其特征在于，

将所述复制许可信息记录在由所述记录手段的用户不能够直接访问的系统区域。

32. 如权利要求1~15、22、23、26、28、30、31任意一项所述的记录装置，其特征在于，

在从所述接口传送来的数据中，附加有复制许可信息，

所述控制手段在规定条件下，即使在所述数据的所述复制许可信息表示复制禁止(copy never)的情况下，也能够进行控制，以使得所述记录手段记录所述数据。

33. 如权利要求32所述的记录装置，其特征在于，

所述规定条件是指，记录下来的所述数据在规定时间后不能够重放的情况。

34. 如权利要求32所述的记录装置，其特征在于，

所述规定条件是指，记录下来的所述数据由于收费条件不能够重放的情况。

35. 如权利要求16~21、24、25、27、29中的任意一项所述的重放装置，其特征在于，

在从所述接口传送来的数据中，附加有复制许可信息，

所述控制手段在规定条件下，即使在所述数据的所述复制许可信息表示复制禁止(copy never)的情况下，也能够进行控制，以使得所述重放手段至少重放一次所述数据。

36. 如权利要求 35 所述的重放装置，其特征在于，

所述规定条件是指，记录下来的数据在规定时间后不能够重放的情况。

37. 如权利要求 35 所述的重放录装置，其特征在于，

所述规定条件是指，记录下来的数据由于收费条件不能够重放的情况。

38. 如权利要求 16~21、24、25、27、29 任意一项所述的重放装置，其特征在于，

在所述记录的加密后的数据中，附加有复制许可信息，

所述控制手段在规定条件下，在所述数据的所述复制许可信息表示仅许可复制一次的情况下，使得由所述记录手段复制一次后的所述数据的所述复制信息为表示仅许可再复制一次的情况，并且进行控制以使得所述重放手段仅能够复制输出一次所述数据。

39. 如权利要求 38 所述的记录重放装置，其特征在于，

所述规定条件是指，在所述重放手段复制输出所述数据的规定时间之后，删去所述数据或者所述数据加密中所采用的密钥。

40. 如权利要求 38 所述的重放装置，其特征在于，

所述规定条件是指，仅被复制输出一次的所述数据的记录对象是记录所述数据作为备份用的装置的情况。

41. 如权利要求 40 所述的重放装置，其特征在于，

在所述记录目的地作为备份记录下来的所述数据，在所述记录目的地不能够重放。

42. 如权利要求 40 所述的重放装置，其特征在于，

在所述记录目的地作为备份记录下来的所述数据，除非返回原来的重放装置，否则不能够重放。

43. 如权利要求 1~14、22、23、26、30~34 中的任意一项所述的记录装置，其特征在于，

所述加密手段与从所述接口传送来的数据的复制许可信息的值无关，将所述数据加密。

44. 如权利要求 1~14、22、23、26、30~34 中的任意一项所述的记录装置，其特征在于，

所述加密手段在从所述接口传送来的数据的复制许可信息表示可自由复制(Copy free)的情况下，不对所述数据加密，

所述控制手段进行控制，以使得所述记录手段记录所述没有加密的数据。

45. 一种数据处理装置，至少具备将记录在记录数据的记录媒体中的数据移动到其他记录装置的移动手段，其特征在于，

在所述移动手段要移动的数据为禁止复制的复制禁止数据的情况下，该复制禁止数据至少在从所述数据处理装置输出时，以所述数据处理装置固有的加密密钥被加密。

46. 一种数据处理装置，至少具备将记录在记录数据的记录媒体中的数据复制到其他记录装置的复制手段，其特征在于，

当所述复制手段要复制的数据为被禁止复制的复制禁止数据时，该复制禁止数据至少在从所述数据处理装置输出时，以所述数据处理装置固有的加密密钥被加密。

47. 如权利要求 45 或 46 所述的数据处理装置，其特征在于，

还具备以所述加密密钥将所述复制禁止数据加密的加密手段。

48. 如权利要求 45~47 任意一项所述的数据处理装置，其特征在于，

还具备重放手段，所述重放手段采用所述加密密钥解读以所述加密密钥被加密的所述复制禁止数据并且重放所述复制禁止数据。

49. 如权利要求 48 所述的数据处理装置，其特征在于，

所述重放手段是在用户进行收视时以必要的速度重放所述复制禁止数据的手段，

还具备存放手段，所述存放手段在从所述其他记录装置以比所述用户收视时所需要的速度更快的速度发送来以所述加密密钥加密的所述复制禁止数据的情况下，以比所述用户收视时需要的速度更快的速度存放发送来的所述复制禁止数据，

所述重放手段在所述存放手段存放从所述其他记录装置发送来的所述复制禁止数据时，能够重放存放在所述存放手段中的所述复制禁止数据或者预先存放在所述存放手段中的数据。

50. 如权利要求 45~49 任意一项所述的数据处理装置，其特征在于，

所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，
还具备判断所述第 2 记录媒体是否为与所述数据处理装置对应的记录媒体
的判断手段，

所述移动手段或者所述复制手段在由所述判断手段判断为所述第 2 记录媒体
是与所述数据处理装置对应的记录媒体时，将所述复制禁止数据移动或者复
制。

51. 如权利要求 45~49 任意一项所述的数据处理装置。

所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，
还具备判断所述其他记录装置是否为与所述数据处理装置对应的装置的
判断手段，

所述移动手段或者所述复制手段在由所述判断手段判断为所述其他记录
装置是对应于所述数据处理装置对应的装置时，将所述复制禁止数据移动或者
复制。

52. 如权利要求 45~51 任意一项所述的数据处理装置，其特征在于，

所述移动手段或者所述复制手段在移动或者复制所述复制禁止数据时，将
该复制禁止数据作为仅可复制一次的数据输出。

53. 一种记录重放装置，其特征在于，具备

将从权利要求 45~47 任意一项所述的数据处理装置输出的、以所述加密
密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段。

54. 一种记录重放装置，其特征在于，具备

将从权利要求 48 所述的数据处理装置输出的、以所述加密密钥加密的所
述复制禁止数据记录到第 2 记录媒体中的记录手段；

将记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数
据在保护所述加密密钥加密的状态下发送到所述数据处理装置的发送手段。

55. 一种记录重放装置，其特征在于，具备

将从权利要求 50 或 51 所述的数据处理装置输出的、以所述加密密钥加密
的所述复制禁止数据记录到第 2 记录媒体中的记录手段；

将记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数
据在保持所述加密密钥加密的状态下发送到所述数据处理装置的发送手段。

56. 一种记录重放装置，其特征在于，具备

将从权利要求 45、46、47、50、51 任意一项所述的数据处理装置输出的、

以所述加密密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段；

用所述加密密钥解读记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数据并且重放所述复制禁止数据的解读重放手段。

57. 如权利要求 56 所述的记录重放装置，其特征在于，

还具备：重放记录了所述加密密钥的加密密钥记录媒体的密钥重放手段；存储所述密钥重放手段重放的所述加密密钥的密钥存储手段，

所述解读重放手段利用所述密钥存储手段存储的所述加密密钥来重放所述复制禁止数据。

58. 如权利要求 56 所述的记录重放装置，其特征在于，

还具备：接收从所述数据处理装置发送来的所述加密密钥的接收手段，

所述解读重放手段利用由所述接收手段接收到的所述加密密钥来重放所述复制禁止数据。

59. 一种数据处理装置，其特征在于，

至少具备移动手段，所述移动手段将记录在记录数据的记录媒体中的数据作为在其他记录装置可解读形式的数据，移动到其他记录装置，

所述移动手段要移动的数据是禁止复制的复制禁止数据。

60. 一种数据处理装置，其特征在于，

至少具备复制手段，所述复制手段将记录在记录数据的记录媒体中的数据作为在其他记录装置可解读形式的数据，复制到其他记录装置，

所述复制手段要复制的数据是禁止复制的复制禁止数据。

61. 如权利要求 59 或 60 所述的数据处理装置，其特征在于，

在所述其他记录装置可解读形式的数据是，未加密的数据、或者以所述其他记录装置固有的密钥加密的数据、或者以附加在所述其他记录装置的第 2 记录媒体中的密钥加密的数据。

62. 如权利要求 61 所述的数据处理装置，其特征在于，

在所述其他记录装置可解读形式的数据也可以是所述其他记录装置所采用的格式的数据。

63. 如权利要求 59~62 所述的数据处理装置，其特征在于，

所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，

还具备判断所述第 2 记录媒体是否为与所述数据处理装置对应的记录媒体的判断手段，

所述移动手段或者所述复制手段在由所述判断手段判断为所述第 2 记录媒体是与所述数据处理装置对应的记录媒体时，将所述复制禁止数据移动或者复制。

64. 如权利要求 63 所述的数据处理装置，其特征在于，

当在所述第 2 记录媒体中附有表示所述第 2 记录媒体是与所述数据处理装置对应的记录媒体的密钥时，所述判断手段采用所述密钥进行所述判断，

还具备：当由所述判断手段判断所述第 2 记录媒体是与所述数据处理装置对应的记录媒体时，采用所述密钥将所述复制禁止数据加密的加密手段，

所述移动手段或所述复制手段将所述加密后的所述复制禁止数据移动或者复制。

65. 如权利要求 59～62 任意一项所述的数据处理装置，其特征在于，

所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，

还具备判断所述其他记录装置是否为与所述数据处理装置的装置对应的判断手段，

所述移动手段或者所述复制手段当由所述判断手段判断为所述其他记录装置是与所述数据处理装置对应的装置时，将所述复制禁止数据移动或者复制。

66. 如权利要求 65 所述的数据处理装置，其特征在于，

当在所述其他记录装置具有表示其与所述数据处理装置对应的装置的密钥时，所述判断手段采用所述密钥进行所述判断，

还具备：当由所述判断手段判断所述其他记录装置是与所述数据处理装置对应的装置时，采用所述密钥将所述复制禁止数据加密的加密手段，

所述移动手段或所述复制手段将所述加密后的所述复制禁止数据移动或者复制。

67. 如权利要求 59～66 所述的数据处理装置，其特征在于，

所述移动手段或者所述复制手段在将所述复制禁止数据移动或者复制时，将该复制禁止数据作为仅可一次复制的数据输出。

68. 一种记录重放装置，其特征在于，

是将来自权利要求 59 或 60 所述的数据处理装置的所述复制禁止数据记录到第 2 记录媒体中并进行重放的记录重放装置，

所述复制禁止数据为未加密的数据，

具备：采用附加在所述第 2 记录媒体中的加密密钥或者所述记录重放装置固有的加密密钥将所述复制禁止数据加密的加密手段；将由所述加密手段加密后的所述复制禁止数据记录到所述第 2 记录媒体的记录手段；利用所述密钥解读记录在所述第 2 记录媒体中的、所述加密后的所述复制禁止数据并进行重放的重放手段。

69. 一种记录重放装置，其特征在于，

是将来自权利要求 59 或 60 所述的数据处理装置的所述复制禁止数据记录到第 2 记录媒体中并进行重放的记录重放装置，

所述复制禁止数据为以所述记录重放装置固有的密钥加密的数据或以附加在所述第 2 记录媒体中的密钥加密的数据，

具备：将所述加密后的所述复制禁止数据记录到所述第 2 记录媒体的记录手段；利用所述密钥解读记录在所述第 2 记录媒体中的、所述加密后的所述复制禁止数据并进行重放的重放手段。

70. 如权利要求 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 中的任意一项所述的数据处理装置，其特征在于，

还具备收费信息发送手段，所述收费信息发送手段在所述移动手段移动所述数据时或者在所述复制手段复制所述数据时，将所述数据的移动或复制所相应的收费信息发送到管理所述数据处理装置的管理装置。

71. 如权利要求 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 中的任意一项所述的数据处理装置，其特征在于，

当确认在连接所述数据处理装置与所述其他记录装置的接口上连接有至少对于所述复制禁止数据的移动或复制具有收费能力的管理装置时，所述移动手段或者所述复制手段将所述复制禁止数据移动或复制到所述其他记录装置。

72. 一种加密数据解密记录装置系统，其特征在于，

具备：将相同内容的、禁止复制的复制禁止数据加密并分别进行记录的多个记录装置；以及具有解密手段与记录手段的解密记录装置，

所述解密手段将从上述多个记录装置输出的所述加密后的所述复制禁止数据解密，所述记录手段记录与所述复制禁止数据相同内容的、加密后或者未加密的复制禁止数据。

73. 一种解密记录装置，其特征在于，具备

解密手段，对将相同内容的、禁止复制的复制禁止数据加密并分别记录的

多个记录装置输出的所述加密后的复制禁止数据解密；

记录与所述复制禁止数据相同内容的、加密或者未加密的复制禁止数据的记录手段。

74. 一种记录装置，其特征在于，

该记录装置是将相同内容的、禁止复制的复制禁止数据加密并且分别记录的多个记录装置中的一个记录装置，

具备：记录所述加密后的所述复制禁止数据的记录手段；输出记录在该记录手段中的所述加密后的复制禁止数据的输出手段，

从该输出手段输出的所述加密后的复制禁止数据是，仅在至少具有对该加密后的复制禁止数据进行解密的解密手段的解密记录装置中被解密的数据。

75. 一种数据发送装置，其特征在于，

具备发送由多个数据构成的数据流的发送手段，

所述数据流或者构成所述数据流的各块内的多个所述数据分别是，若不重放该数据的时间上前一个数据则不能够重放的数据，

所述发送手段以所述数据流的或者构成所述数据流的各块内的、所述多个数据在时间上从最末尾到最前面的顺序发送所述各数据。

76. 一种记录装置，其特征在于，

该记录装置是能够将设定为禁止或限制复制的数据所构成的复制限制内容进行转录重放用的记录装置，

具备：能够记录规定容量部分的所述复制限制内容的记录媒体；将数据记录到所述记录媒体的记录手段，

所述记录手段在将所述复制限制内容记录到所述记录媒体的同时，从开始记录所述复制限制内容起，经过规定时间之后，使得记录在所述记录媒体中的所述复制限制内容的数据为不能够收视的状态。

77. 如权利要求 76 所述的记录装置，其特征在于，

通过删去所述复制限制内容的数据来实现所述不能够收视的状态。

78. 如权利要求 76 所述的记录装置，其特征在于，

通过不删去所述复制限制内容的数据来实现所述不能够收视的状态。

79. 如权利要求 76 所述的记录装置，其特征在于，

通过使所述复制限制内容的数据不能够重放来实现所述不能够收视的状态。

80. 如权利要求 79 所述的记录装置，其特征在于，
通过将重放后的所述复制限制内容的数据加密来实现不能够收视的状态。

81. 如权利要求 76~80 任意一项所述的记录装置，其特征在于，
通过参照所述复制限制内容所相关的判别信息，确定所述记录手段开始记
录所述复制限制内容的时刻。

82. 如权利要求 81 所述的记录装置，其特征在于，
所述记录手段采用判别信息分别记录所述复制限制内容与其他内容。

83. 如权利要求 81 所述的记录装置，其特征在于，
所述判别信息是包含在所述复制限制内容的数据串中的著作权信息。

84. 如权利要求 76~82 任意一项所述的记录装置，其特征在于，
根据来自外部的输入，确定所述记录手段开始记录所述复制限制内容的时
刻。

85. 如权利要求 76~80 任意一项所述的记录装置，其特征在于，
所述记录媒体具有用于暂时记录所述复制限制内容的记录缓冲器。

86. 如权利要求 85 所述的记录装置，其特征在于，
所述记录用缓冲器是通过反复在同一区域上进行重写记录而能够记录一
定量数据的环形缓冲器。

87. 一种记录重放装置，其特征在于，
具备：权利要求 76~85 任意一项所述的记录装置；重放记录在所述记录
媒体中的数据的重放手段，

所述重放手段从开始记录所述复制限制内容的时刻起经过规定待机时间
之后，重放记录的所述复制限制内容。

88. 一种记录重放装置，其特征在于，
具备：权利要求 86 所述的记录装置；重放记录在所述记录媒体中的数据
的重放手段，

所述重放手段从开始记录所述复制限制内容的时刻起经过规定待机时间
之后，重放记录的所述复制限制内容。

89. 如权利要求 88 所述的记录重放装置，其特征在于，
在向所述环形缓冲器进行重写记录的状态下，所述重放手段进行重放动作
时，在所述环形缓冲器上，从记录最早的数据的位置开始进行该数据的重放。

90. 如权利要求 89 所述的记录重放装置，其特征在于，

在向所述环形缓冲器进行重写记录的状态下，所述重放手段进行重放动作时，从所述环形缓冲器上的记录开始位置起进行该数据的重放。

91. 如权利要求 87 或 88 所述的记录重放装置，其特征在于，

所述记录装置当在所述规定待机时间内没有重放记录在所述记录媒体中的复制限制内容时，停止该复制限制内容的记录动作。

92. 如权利要求 87 或 88 所述的记录重放装置，其特征在于，

还具备根据所述规定时间或所述规定的待机时间中的任一个量预先告知所述记录装置或者重放手段的动作内容的告知手段。

93. 如权利要求 76 的记录装置，其特征在于，

所述记录手段能够测量包含所述规定时间的时间信息。

94. 如权利要求 76 的记录装置，其特征在于，

所述复制限制内容包含时间信息，该时间信息包含所述规定时间。

95. 如权利要求 76 的记录装置，其特征在于，

与所述复制限制内容相独立地，从外部取得包含所述规定时间的时间信息。

记录装置、重放装置、数据处理装置、
记录重放装置、数据发送装置

技术领域

本发明涉及记录数据的记录装置、重放数据的重放装置、将记录在记录媒体上的数据移向其他装置或进行复制的数据处理装置、记录并重放上述这样移动后的数据的记录重放装置、发送由多个数据构成的数据流的数据发送装置、用于进行将由电视广播等所广播的内容延迟规定时间后再收视的进行转录重放的记录装置与记录重放装置。

背景技术

当处理新播出的电影、收费广播的电视节目及音乐等必须保护著作权的数据时，必须要保护著作权。作为保护著作权的有效方法，有一种方法是将必须保护著作权的数据进行加密以限制数据使用。

例如，在传送视频音频数据(以下，记作 AV 数据)时，当必须对 AV 数据进行著作权保护时，将该 AV 数据加密后传送。作为这样的示例，以 IEEE1394—DTCP(Digital Transmission Protection，数字传输保护)方式为标准。

IEEE 1394 利用进行串行传输的高速总线系统，由于能够同步传送数据，故能够进行 AV 数据等的实时传送。这样的 IEEE1394 作为外部用接口安装在家庭用数字 AV 设备等多种数字视频音频设备上。

根据 IEEE1394—DTCP 方式，在以 IEEE1394 总线进行数据传送时，具备认证功能与密钥无效功能，将 AV 数据等的需要保护著作权的数据进行加密后传送，由此，能够实现著作权的保护。

另外，随着个人计算机的普及及发展，作为外部存储装置，由于其大容量、高速，经常采用硬盘装置等记录装置及重放装置。再者，最近的硬盘装置不仅能够用于计算机，而且通过数字技术，也用于记录重放视频、音频的数字 AV 设备等中，发挥其高速性、大容量的特点。

这样，一直以来，电影的创作者等就常常考虑不想让第三者随意复制自己制作的数据。这里，为了保护著作权，存在两种数据，一种是禁止复制到其他

记录媒体的数据，另一种是允许复制一次的数据。

对于这样的数据，若例如复制并存储到 HDD 的情况下，则仅在该 HDD 中重放。

又，作为电视广播的收视方法之一，是先将广播的节目暂时存储到 VTR 等记录装置，之后再重放所记录的数据，由此，可以在与原来广播时刻不同的时刻收视节目，以往经常采用这样的方法。

特别是对于记录装置，在采用硬盘等随机可存取且能够同时进行记录重放的记录媒体时，相对于以往的采用磁带媒体的 VTR，能够实现狭义的转录重放，即在节目广播时间内即使仅延迟一点点时间之后，也不会遗漏该节目的内容并能够连续地进行收视。

图 43 是表示以往技术中用于实现转录重放的记录重放装置的构造图。如图所示，记录重放手段 2120 是用于记录并重放来自外部的广播的手段，记录媒体 2130 是通过硬盘等来实现的、存储广播数据的手段，切换手段 2160 是接受从记录重放手段 2120 的输入及来自外部的广播输入并选择任意之一输出到外部的显示器等的手段。

以下，说明具有上述构造的以往技术的记录重放装置的一示例。

首先，收视者在实时收视节目时，切换手段 2160 进行设定，使得将来自外部的广播照原样输出到显示器，另一方面，记录重放手段 2120 将相同的节目内容记录到记录媒体 2130。

然后，收视者在暂时离开显示器前面之后，再次返回到显示器前面而重新开始收视节目时，记录重放手段 2120 从收视者离开显示器前面的时刻起，重放记录的数据，切换手段 2160 进行设定，使得来自记录重放手段 2120 的输入对显示器输出。此后，收视者收视来自记录重放手段 2120 的重放输出作为收视的节目。

在上述动作中，记录重放手段 2120 在进行数据重放的同时，也同时对来自外部的广播进行录象。即，记录重放手段 2120 同时进行数据的重放与记录。

由此，收视者在收视实时广播的节目时，即使在必不得已暂时中断收视的情况下，能够仅延迟收视中断的时间，而不会断开节目的内容继续收视。

然而，与传送 AV 数据的情况相同，当将必须保护著作权的 AV 数据记录到硬盘装置等记录媒体的情况下以及/或者进行重放的情况下，必须要有保护著作权的构成环节。然而，向记录装置以及/或者由重放装置记录以及/或者重放

需要保护著作权的 AV 数据时，并没有具体确定如何进行著作权保护。

又，不限于 AV 数据，对于从因特网等传送到文件数据或游戏软件等计算机程序，有时也与 AV 数据相同需要进行著作权保护。然而，对于向记录装置以及/或者由重放装置记录/或者重放需要保护著作权的上述数据的情况，并没有具体确定如何保护著作权。

即，存在这样的问题，在将 AV 数据、文件数据、计算机程序等的数据记录到记录装置以及/或者通过重放装置重放这些数据的情况下，并没有保护著作权的具体构成环节。

又，当上述 HDD 的数据记录剩余容量减少时，必须在已记录在 HDD 的数据上再写入新的数据或者删去已记录在 HDD 的一部分数据以增加剩余容量。然而，当 HDD 的用户不希望在已经记录在 HDD 的数据上写入数据或者删去数据时，有时会考虑将记录在 HDD 上的数据复制到其他记录媒体上。

另一方面，如上所述，忽略著作权而对记录在 HDD 上的数据进行复制，这对于著作权者来说是很头痛的。

即，当将需要保护著作权的数据记录到 HDD 等记录装置时，存在用户不能将该数据复制到其他记录媒体的问题。

又，利用有线电视以及 CS 广播等各种广播形式及信号数字化等进行广播的节目，也存在著作权上的问题，通过在信号中包含复制保护，能够实现播映的节目已预先设定不能够进行用于复制的记录。

然而，在以往的记录重放装置中，对于考虑到上述著作权的节目，为了实现转录重放，而将节目记录到记录媒体 2130，对此，存在有可能引起侵害节目著作权的问题。

即，对于必须保护著作权的节目，若实现转录重放，则存在有可能引起侵害节目著作权的问题。

作为避免该问题的措施可以考虑下述的一些方法。即，(1)限制可进行转录的时间。(2)防止广播的内容完整保存。

发明内容

本发明鉴于上述问题，目的在于提供一种在记录必须保护著作权的数据时以及/或者重放必须保护著作权时能够保护著作权的记录装置以及重放装置。

又，本发明鉴于上述问题，目的在于提供一种在保护著作权的同时能够将

被禁止复制的数据移动到其他记录媒体或者进行复制的数据处理装置、将来自该数据处理装置的数据记录到记录媒体或者在记录的同时进行重放的记录重放装置、保护著作权并预先将数据备份的加密数据解密记录装置系统以及构成该系统的解密记录装置、记录装置与保护著作权并发送数据的数据发送装置。

又，本发明鉴于上述问题，目的在于提供一种在比原来的广播时间晚进行收视的转录重放中能够避免侵害著作权的记录装置以及记录重放装置。

为了解决上述问题，第 1 方面(与权利要求 1 对应)是一种记录装置，其特征在于，具备：将从接口传送来的数据加密的加密手段；进行控制以使得记录所述加密后的数据的控制手段；以及由所述控制手段控制并将所述加密后的数据记录到盘片上的记录手段。

又，第 2 方面(与权利要求 2 对应)是在第 1 方面所述的记录装置中，其特征在于，所述加密手段采用分配给记录装置本身的固有的数值以及/或者记号即装置惟一密钥将所述数据加密。

又，第 3 方面(与权利要求 3 对应)是在第 1 或第 2 方面所述的记录装置中，其特征在于，所述加密手段采用与所述控制手段连续访问所述记录手段的最小单位即记录单元对应的记录块采用所固有的编号以及/或者记号的记录单元信息，将所述数据加密。

又，第 4 方面(与权利要求 4 对应)是在第 3 方面所述的记录装置中，其特征在于，采用所述记录单元信息将所述数据加密是指，以根据所述记录单元信息所获得的密钥将所述数据加密。

又，第 5 方面(与权利要求 5 对应)是在第 3 或 4 方面所述的记录装置中，其特征在于，至少记录在所述记录块中的、所述加密后的数据以及附加在所述加密后的数据中的附加信息的所有部分都被加密并记录在所述记录手段。

又，第 6 方面(与权利要求 6 对应)是在第 3~5 任意一方面所述的记录装置中，其特征在于，在所述数据中附加复制许可信息，所述控制手段控制所述记录手段以使得所述记录手段记录所述复制许可信息，所述加密手段生成第 1 信息，所述第 1 信息包含所述装置惟一密钥与所述复制许可信息中的至少一个，采用所述记录单元信息，所述加密手段生成将所述第 1 信息加密后的信息即内容密钥，所述加密手段采用所述内容密钥将所述数据加密，所述控制手段控制所述记录手段以使得所述记录手段记录所述加密后的数据。

又，第 7 方面(与权利要求 7 对应)是在第 2 方面所述的记录装置中，其特

征在于，对于所述数据，分配所述数据所固有的数值以及/或者记号即标题密钥，所述加密手段采用所述装置惟一密钥将所述标题密钥加密，所述控制手段控制所述记录手段，以使得将所述加密后的标题密钥记录到所述记录手段。

又，第 8 方面(与权利要求 8 对应)是在第 7 方面所述的记录装置中，其特征在于，所述加密手段采用所述标题密钥将所述数据加密。

又，第 9 方面(与权利要求 9 对应)是在第 8 方面所述的记录装置中，其特征在于，所述加密手段采用所述装置惟一密钥将所述标题密钥加密，所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的标题密钥，所述加密手段生成包含所述标题密钥的第 3 信息，所述加密手段采用记录单元信息生成将所述第 3 信息加密后的信息即内容密钥，所述记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述加密手段采用所述内容密钥将所述数据加密，所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的数据。

又，第 10 方面(与权利要求 10 对应)是在第 8 方面所述的记录装置中，其特征在于，在所述数据中附加有复制许可信息，所述加密手段也采用所述复制许可信息将所述数据加密。

又，第 11 方面(与权利要求 11 对应)是在第 10 方面所述的记录装置中，其特征在于，所述加密手段采用所述装置惟一密钥将所述标题密钥加密，所述控制手段控制所述记录手段，以使得所述记录手段所述加密后的标题密钥，所述控制手段控制所述记录手段，以使得所述记录手段记录所述复制许可信息，所述加密手段生成第 2 信息，所述第 2 信息包含所述标题密钥与所述复制许可信息中的至少一个，所述加密手段采用记录单元信息生成将所述第 2 信息加密后的信息即内容密钥，所述记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述加密手段采用所述内容密钥将所述数据加密，所述控制手段控制所述记录手段，以使得所述记录手段记录所述加密后的数据。

又，第 12 方面(与权利要求 12 对应)是在第 1 方面所述的记录装置中，其特征在于，所述加密手段采用所述复制许可信息将附加有复制许可信息的、从接口传送来的数据加密，所述控制手段控制所述记录手段，以使得所述记录手段在记录所述数据之前以及/或者记录所述数据之后记录所述复制许可信息。

又，第 13 方面(与权利要求 13 对应)是在第 12 方面所述的记录装置中，其特征在于，所述控制手段控制所述记录手段，以使得至少所述记录手段在记录所述数据之前记录所述复制许可信息。

又，第 14 方面(与权利要求 14 对应)是在第 12 方面所述的记录装置中，其特征在于，所述控制手段控制所述记录手段，以使得所述记录手段仅在记录了所述数据之后记录所述复制许可信息。

又，第 15 方面(与权利要求 15 对应)是一种记录装置，其特征在于，具备：进行控制以使得记录从接口传送来的加密后的数据的控制手段；以及由所述控制手段控制且将所述加密后的数据记录到盘片上的记录手段。

又，第 16 方面(与权利要求 16 对应)是一种重放装置，其特征在于，具备：控制手段，进行控制以使得重放由第 1 方面所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及

将所述重放后的数据解密并传送到接口的解密手段。

又，第 17 方面(与权利要求 17 对应)是一种重放装置，其特征在于，具备：控制手段，进行控制以使得重放由第 2 方面所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，所述解密手段采用所述装置惟一密钥将所述重放后的数据解密。

又，第 18 方面(与权利要求 18 对应)是一种重放装置，其特征在于，具备：控制手段，进行控制以使得重放由第 3 方面所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，所述解密手段采用所述记录单元信息将所述重放后的数据解密。

又，第 19 方面(与权利要求 19 对应)是一种重放装置，其特征在于，具备：控制手段，进行控制以使得重放由第 4 方面所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述重放后的数据解密并传送到接口的解密手段，所述解密手段以根据所述记录单元信息所获得的密钥将所述重放后的数据解密。

又，第 20 方面(与权利要求 20 对应)是一种重放装置，其特征在于，具备：控制装置，进行控制以使得重放由第 14 方面所述的记录装置记录到盘片上的加密后的数据；由所述控制手段控制、重放所述数据的重放手段；以及将所述

重放后的数据解密并传送到接口的解密手段，在记录所述数据时，当不能够正常地将所述复制许可信息记录到所述记录手段中时，所述解密手段假设所述复制许可信息取各种值并试着对所述加密后的数据的全部或一部分进行解密，在所述试着解密的结果为能够正常将所述重放后的数据解密时，采用所述复制许可信息的值，将所述重放后的数据解密。

又，第 21 方面(与权利要求 21 对应)是一种重放装置，其特征在于，具备：控制装置，进行控制以使得重放由第 15 方面所述的记录装置记录到盘片上的加密后的数据；以及由所述控制手段控制、重放所述数据的重放手段，将所述重放后的数据传送到接口。

又，第 22 方面(与权利要求 22 对应)是在第 1~14 任意一方面所述的记录装置中，其特征在于，将所述接口、所述加密手段以及所述控制手段一体化设置在同一印刷基板上。

又，第 23 方面(与权利要求 23 对应)是在第 22 方面所述的记录装置中，其特征在于，使得所述接口、所述加密手段以及所述控制手段为一片芯片。

又，第 24 方面(与权利要求 24 对应)是在第 16~20 任意一方面所述的重放装置中，其特征在于，将所述接口、所述解密手段以及所述控制手段一体化设置在同一印刷基板上。

又，第 25 方面(与权利要求 25 对应)是在第 24 方面所述的重放装置中，其特征在于，使得所述接口、所述解密手段以及所述控制手段为一片芯片。

又，第 26 方面(与权利要求 26 对应)是在第 22 方面所述的记录装置中，其特征在于，从所述印刷基板上的端子检测出的信号完全被加密以及/或者以非公开的格式描述，所述印刷基板上的端子输出能够作出数据重放的信息。

又，第 27 方面(与权利要求 27 对应)是在第 24 方面所述的重放装置中，其特征在于，从所述印刷基板上的端子检测出的信号完全被加密以及/或者以非公开的格式描述，所述印刷基板上的端子输出由第 3 者能够作为数据重放的信息。

又，第 28 方面(与权利要求 28 对应)是在第 22 方面所述的记录装置中，其特征在于，所述印刷基板上的端子的性质是以非公开的格式确定的，所述印刷基板上的端子输出由第 3 者能够作为数据重放的信号。

又，第 29 方面(与权利要求 29 对应)是在第 24 方面所述的重放装置中，其特征在于，所述印刷基板上的端子的性质是以非公开的格式确定的，所述印

刷基板作为数据输出由第 3 者能够重放的信号。

又，第 30 方面(与权利要求 30 对应)是在第 2~11 任意一方面所述的记录装置中，其特征在于，所述装置惟一密钥不能够由外部设备进行访问。

又，第 31 方面(与权利要求 31 对应)是在第 6、10、11、12、13、14 方面中的任意一方面所述的记录装置中，其特征在于，将所述复制许可信息记录在由所述记录手段的用户不能够直接访问的系统区域。

又，第 32 方面(与权利要求 32 对应)是在第 1~15、22、23、26、28、30、31 任意一方面所述的记录装置中，其特征在于，在从所述接口传送来的数据中，附加有复制许可信息，所述控制手段在规定条件下，即使在所述数据的所述复制许可信息表示复制禁止(copy never)的情况下，也能够进行控制，以使得所述记录手段记录所述数据。

又，第 33 方面(与权利要求 33 对应)是在第 32 方面所述的记录装置中，其特征在于，所述规定条件是指，记录下来的所述数据在规定时间后不能够重放的情况。

又，第 34 方面(与权利要求 34 对应)是在第 32 方面所述的记录装置中，其特征在于，所述规定条件是指，记录下来的所述数据由于收费条件不能够重放的情况。

又，第 35 方面(与权利要求 35 对应)是在第 16~21、24、25、27、29 中的任意一方面所述的重放装置中，其特征在于，在所述记录的加密后的数据中，附加有复制许可信息，所述控制手段在规定条件下，即使在所述数据的所述复制许可信息表示复制禁止(copy never)的情况下，也能够进行控制，以使得所述重放手段至少重放一次所述数据。

又，第 36 方面(与权利要求 36 对应)是在第 35 方面所述的重放装置中，其特征在于，所述规定条件是指，记录下来的所述数据在规定时间后不能够重放的情况。

又，第 37 方面(与权利要求 37 对应)是在第 35 方面所述的重放装置中，其特征在于，所述规定条件是指，记录下来的数据由于收费条件不能够重放的情况。

又，第 38 方面(与权利要求 38 对应)是在第 16~21、24、25、27、29 任意一方面所述的重放装置中，其特征在于，在所述记录的加密后的数据中，附加有复制许可信息，所述控制手段在规定条件下，在所述数据的所述复制许可

信息表示仅许可复制一次的情况下，使得由所述记录手段复制一次后的所述数据的所述复制信息为表示仅许可再复制一次的情况，并且进行控制以使得所述重放手段仅能够复制输出一次所述数据。

又，第 39 方面(与权利要求 39 对应)是在第 38 方面所述的重放装置中，其特征在于，所述规定条件是指，在所述重放手段复制输出所述数据的规定时间之后，删去所述数据或者所述数据加密中所采用的密钥。

又，第 40 方面(与权利要求 40 对应)是在第 38 方面所述的重放装置中，其特征在于，所述规定条件是指，仅被复制输出一次的所述数据的记录对象是记录所述数据作为备份用的装置的情况。

又，第 41 方面(与权利要求 41 对应)是在第 40 方面所述的重放装置中，其特征在于，在所述记录目的地作为备份记录下来的所述数据，在所述记录目的地不能够重放。

又，第 42 方面(与权利要求 42 对应)是在第 40 方面所述的重放装置中，其特征在于，在所述记录目的地作为备份记录下来的所述数据，除非返回原来的重放装置，否则不能够重放。

又，第 43 方面(与权利要求 43 对应)是在第 1~14、22、23、26、30~34 任意一方面所述的记录装置中，其特征在于，所述加密手段与从所述接口传送来的数据的复制许可信息的值无关，将所述数据加密。

又，第 44 方面(与权利要求 44 对应)是在第 1~14、22、23、26、30~34 任意一方面所述的记录装置中，其特征在于，所述加密手段在从所述接口传送来的数据的复制许可信息表示可自由复制(Copy free)的情况下，不对所述数据加密，所述控制手段进行控制，以使得所述记录手段记录所述没有加密的数据。

又，第 45 方面(与权利要求 45 对应)是一种数据处理装置，至少具备将记录在记录数据的记录媒体中的数据移动到其他记录装置的移动手段，其特征在于，在所述移动手段要移动的数据为禁止复制的复制禁止数据的情况下，该复制禁止数据至少在从所述数据处理装置输出时，以所述数据处理装置固有的加密密钥被加密。

又，第 46 方面(与权利要求 46 对应)是一种数据处理装置，至少具备将记录在记录数据的记录媒体中的数据复制到其他记录装置的复制手段，其特征在于，当所述复制手段要复制的数据为被禁止复制的复制禁止数据时，该复制禁

止数据至少在从所述数据处理装置输出时，以所述数据处理装置固有的加密密钥被加密。

又，第 47 方面(与权利要求 47 对应)是在第 45 或 46 方面所述的数据处理装置中，其特征在于，还具备以所述加密密钥将所述复制禁止数据加密的加密手段。

又，第 48 方面(与权利要求 48 对应)是在第 45~47 任意一方面所述的数据处理装置中，其特征在于，还具备重放手段，所述重放手段采用所述加密密钥解读以所述加密密钥被加密的所述复制禁止数据并且重放所述复制禁止数据。

又，第 49 方面(与权利要求 49 对应)是在第 48 方面所述的数据处理装置中，其特征在于，所述重放手段是在用户进行收视时以必要的速度重放所述复制禁止数据的手段，还具备存放手段，所述存放手段在从所述其他记录装置以比所述用户收视时所需要的速度更快的速度发送来以所述加密密钥加密的所述复制禁止数据的情况下，以比所述用户收视时需要的速度更快的速度存放发送来的所述复制禁止数据，所述重放手段在所述存放手段存放从所述其他记录装置发送来的所述复制禁止数据时，能够重放存放在所述存放手段中的所述复制禁止数据或者预先存放在所述存放手段中的数据。

又，第 50 方面(与权利要求 50 对应)是在第 45~49 任意一方面所述的数据处理装置中，其特征在于，所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，还具备判断所述第 2 记录媒体是否为与所述数据处理装置对应的记录媒体的判断手段，所述移动手段或者所述复制手段在由所述判断手段判断为所述第 2 记录媒体是与所述数据处理装置对应的记录媒体时，将所述复制禁止数据。

又，第 51 方面(与权利要求 51 对应)是在第 45~49 任意一方面所述的数据处理装置中，其特征在于，所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，还具备判断所述其他记录装置是否为与所述数据处理装置对应的装置的判断手段，所述移动手段或者所述复制手段当由所述判断手段判断为所述其他记录装置是与所述数据处理装置对应的装置时，将所述复制禁止数据移动或者复制。

又，第 52 方面(与权利要求 52 对应)是在第 45~51 任意一方面所述的数据处理装置中，其特征在于，所述移动手段或者所述复制手段在移动或者复制

所述复制禁止数据时，将该复制禁止数据作为仅可复制一次的数据输出。

又，第 53 方面(与权利要求 53 对应)是一种记录重放装置，其特征在于，具备：将从第 45~47 任意一方面所述的数据处理装置输出的、以所述加密密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段。

又，第 54 方面(与权利要求 54 对应)是一种记录重放装置，其特征在于，具备：将从第 48 方面所述的数据处理装置输出的、以所述加密密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段；将记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数据在保持所述加密密钥加密的状态下发送到所述数据处理装置的发送手段。

又，第 55 方面(与权利要求 55 对应)是一种记录重放装置，其特征在于，具备：将从第 50 或 51 方面所述的数据处理装置输出的、以所述加密密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段；将记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数据在保持所述加密密钥加密的状态下发送到所述数据处理装置的发送手段。

又，第 56 方面(与权利要求 56 对应)是一种记录重放装置，其特征在于，具备：将从第 45、46、47、50、51 任意一方面所述的数据处理装置输出的、以所述加密密钥加密的所述复制禁止数据记录到第 2 记录媒体中的记录手段；以及用所述加密密钥解读记录在所述第 2 记录媒体中的、以所述加密密钥加密的所述复制禁止数据并且重放所述复制禁止数据的解读重放手段。

又，第 57 方面(与权利要求 57 对应)是在第 56 方面所述的记录重放装置中，其特征在于，还具备：重放记录了所述加密密钥的加密密钥记录媒体的密钥重放手段；存储所述密钥重放手段重放的所述加密密钥的密钥存储手段，所述解读重放手段利用所述密钥存储手段存储的所述加密密钥来重放所述复制禁止数据。

又，第 58 方面(与权利要求 58 对应)是在第 56 方面所述的记录重放装置中，其特征在于，还具备：接收从所述数据处理装置发送来的所述加密密钥的接收手段，所述解读重放手段利用由所述接收手段接收到的所述加密密钥来重放所述复制禁止数据。

又，第 59 方面(与权利要求 59 对应)是一种数据处理装置，其特征在于，至少具备移动手段，所述移动手段将记录在记录数据的记录媒体中的数据作为在其他记录装置可解读形式的数据，移动到其他记录装置，所述移动手段要移

动的数据是禁止复制的复制禁止数据。

又，第 60 方面(与权利要求 60 对应)是一种数据处理装置，其特征在于，至少具备复制手段，所述复制手段将记录在记录数据的记录媒体中的数据作为在其他记录装置可解读形式的数据，复制到其他记录装置，所述复制手段要复制的数据是禁止复制的复制禁止数据。

又，第 61 方面(与权利要求 61 对应)是在第 59 或 60 方面所述的数据处理装置中，其特征在于，在所述其他记录装置可解读形式的数据是指，未加密的数据、或者以所述其他记录装置固有的密钥加密的数据、或者以附加在所述其他记录装置的第 2 记录媒体中的密钥加密的数据。

又，第 62 方面(与权利要求 62 对应)是在第 61 方面所述的数据处理装置中，其特征在于，在所述其他记录装置可解读形式的数据还指，所述其他记录装置所采用的格式的数据。

又，第 63 方面(与权利要求 63 对应)是在第 59~62 方面所述的数据处理装置中，其特征在于，所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，还具备判断所述第 2 记录媒体是否为与所述数据处理装置对应的记录媒体的判断手段，所述移动手段或者所述复制手段在由所述判断手段判断为所述第 2 记录媒体是与所述数据处理装置对应的记录媒体时，将所述复制禁止数据移动或者复制。

又，第 64 方面(与权利要求 64 对应)是在第 63 方面所述的数据处理装置中，其特征在于，当在所述第 2 记录媒体中附有表示所述第 2 记录媒体是与所述数据处理装置对应的记录媒体的密钥时，所述判断手段采用所述密钥进行所述判断，还具备：当由所述判断手段判断所述第 2 记录媒体是与所述数据处理装置对应的记录媒体时，采用所述密钥将所述复制禁止数据加密的加密手段，所述移动手段或所述复制手段将所述加密后的所述复制禁止数据移动或者复制。

又，第 65 方面(与权利要求 65 对应)是第 59~62 任意一方面所述的数据处理装置中，其特征在于，所述其他记录装置是能够将数据记录到第 2 记录媒体的装置，还具备判断所述其他记录装置是否为与所述数据处理装置对应的装置的判断手段，所述移动手段或者所述复制手段当由所述判断手段判断为所述其他记录装置是与所述数据处理装置对应的装置时，将所述复制禁止数据移动或者复制。

又，第 66 方面(与权利要求 66 对应)是在第 65 方面所述的数据处理装置中，其特征在于，当在所述其他记录装置具有表示其是与所述数据处理装置的装置对应的密钥时，所述判断手段采用所述密钥进行所述判断，还具备：当由所述判断手段判断所述其他记录装置是与所述数据处理装置对应的装置时，采用所述密钥将所述复制禁止数据加密的加密手段，所述移动手段或所述复制手段将所述加密后的所述复制禁止数据移动或者复制。

又，第 67 方面(与权利要求 67 对应)是在第 59~66 所述的数据处理装置中，其特征在于，所述移动手段或者所述复制手段在将所述复制禁止数据移动或者复制时，将该复制禁止数据作为仅可一次复制的数据输出。

又，第 68 方面(与权利要求 68 对应)是一种记录重放装置，其特征在于，是将来自第 59 或 60 方面所述的数据处理装置的所述复制禁止数据记录到第 2 记录媒体中并进行重放的记录重放装置，所述复制禁止数据为未加密的数据，具备：采用附加在所述第 2 记录媒体中的加密密钥或者所述记录重放装置固有的加密密钥将所述复制禁止数据加密的加密手段；将由所述加密手段加密后的所述复制禁止数据记录到所述第 2 记录媒体的记录手段；利用所述密钥解读记录在所述第 2 记录媒体中的、所述加密后的所述复制禁止数据并进行重放的重放手段。

又，第 69 方面(与权利要求 69 对应)是一种记录重放装置，其特征在于，是将来自第 59 或 60 方面所述的数据处理装置的所述复制禁止数据记录到第 2 记录媒体中并进行重放的记录重放装置，所述复制禁止数据为以所述记录重放装置固有的密钥加密的数据或以附加在所述第 2 记录媒体中的密钥加密的数据，具备：将所述加密后的所述复制禁止数据记录到所述第 2 记录媒体的记录手段；利用所述密钥解读记录在所述第 2 记录媒体中的、所述加密后的所述复制禁止数据并进行重放的重放手段。

又，第 70 方面(与权利要求 70 对应)是在第 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 任意一方面所述的数据处理装置中，其特征在于，还具备收费信息发送手段，所述收费信息发送手段在所述移动手段移动所述数据时或者在所述复制手段复制所述数据时，将所述数据的移动或复制所相应的收费信息发送到管理所述数据处理装置的管理装置。

又，第 71 方面(与权利要求 71 对应)是在第 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 任意一方面所述的数据处理装置中，

其特征在于，当确认在连接所述数据处理装置与所述其他记录装置的接口上连接有至少对于所述复制禁止数据的移动或复制具有收费能力的管理装置时，所述移动手段或者所述复制手段将所述复制禁止数据移动或复制到所述其他记录装置。

又，第 72 方面(与权利要求 72 对应)是一种加密数据解密记录装置系统，其特征在于，具备：将相同内容的、禁止复制的复制禁止数据加密并分别进行记录的多个记录装置；以及具有解密手段与记录手段的解密记录装置，所述解密手段将从上述多个记录装置输出的所述加密后的所述复制禁止数据解密，所述记录手段记录与所述复制禁止数据相同内容的、加密后或者未加密的复制禁止数据。

又，第 73 方面(与权利要求 73 对应)是一种解密记录装置，其特征在于，具备：解密手段，对将相同内容的、禁止复制的复制禁止数据加密并分别记录的多个记录装置输出的所述加密后的复制禁止数据解密；记录与所述复制禁止数据相同内容的、加密或者未加密的复制禁止数据的记录手段。

又，第 74 方面(与权利要求 74 对应)是一种记录装置，其特征在于，它是将相同内容的、禁止复制的复制禁止数据加密并且分别记录的多个记录装置中的一个记录装置，具备：记录所述加密后的所述复制禁止数据的记录手段；输出记录在该记录手段中的所述加密后的复制禁止数据的输出手段，从该输出手段输出的所述加密后的复制禁止数据是，仅在至少具有对该加密后的复制禁止数据进行解密的解密手段的解密记录装置中被解密的数据。

又，第 75 方面(与权利要求 75 对应)是一种数据发送装置，其特征在于，具备发送由多个数据构成的数据流的发送手段，所述数据流或者构成所述数据流的各块内的多个所述数据分别是，若不重放该数据的时间上前一个数据则不能够重放的数据，所述发送手段以所述数据流的或者构成所述数据流的各块内的、所述多个数据在时间上从最末尾到最前面的顺序发送所述各数据。

又，第 76 方面(与权利要求 76 对应)是一种记录装置，其特征在于，它是能够将设定为禁止或限制复制的数据所构成的复制限制内容进行转录重放的记录装置，具备：能够记录规定容量部分的所述复制限制内容的记录媒体；将数据记录到所述记录媒体的记录手段，所述记录手段在将所述复制限制内容记录到所述记录媒体的同时，从开始记录所述复制限制内容起，经过规定时间之后，使得记录在所述记录媒体中的所述复制限制内容的数据为不能够收视的状态。

态。

又，第 77 方面(与权利要求 77 对应)是在第 76 方面所述的记录装置中，其特征在于，通过删去所述复制限制内容的数据来实现所述不能够收视的状态。

又，第 78 方面(与权利要求 78 对应)是在第 76 方面所述的记录装置中，其特征在于，通过不删去所述复制限制内容的数据来实现所述不能够收视的状态。

又，第 79 方面(与权利要求 79 对应)是在第 76 方面所述的记录装置中，其特征在于，通过使所述复制限制内容的数据不能够重放来实现所述不能够收视的状态。

又，第 80 方面(与权利要求 80 对应)是在第 79 方面所述的记录装置中，其特征在于，通过将重放后的所述复制限制内容的数据加密来实现不能够收视的状态。

又，第 81 方面(与权利要求 81 对应)是在第 76~80 任意一方面所述的记录装置中，其特征在于，通过参照所述复制限制内容所相关的判别信息，确定所述记录手段开始记录所述复制限制内容的时刻。

又，第 82 方面(与权利要求 82 对应)是在第 81 方面所述的记录装置中，其特征在于，所述记录手段采用判别信息分别记录所述复制限制内容与其他内容。

又，第 83 方面(与权利要求 83 对应)是在第 81 方面所述的记录装置中，其特征在于，所述判别信息是包含在所述复制限制内容的数据串中的著作权信息。

又，第 84 方面(与权利要求 84 对应)是在第 76~82 任意一方面所述的记录装置中，其特征在于，根据来自外部的输入，确定所述记录手段开始记录所述复制限制内容的时刻。

又，第 85 方面(与权利要求 85 对应)是在第 76~80 任意一方面所述的记录装置中，其特征在于，所述记录媒体具有用于暂时记录所述复制限制内容的记录缓冲器。

又，第 86 方面(与权利要求 86 对应)是在第 85 方面所述的记录装置中，其特征在于，所述记录用缓冲器是通过反复在同一区域上进行重写记录而能够记录一定量数据的环形缓冲器。

又，第 87 方面(与权利要求 87 对应)是一种记录重放装置，其特征在于，具备：第 76~85 任意一方面所述的记录装置；重放记录在所述记录媒体中的数据的重放手段，所述重放手段从开始记录所述复制限制内容的时刻起经过规定待机时间之后，重放记录的所述复制限制内容。

又，第 88 方面(与权利要求 88 对应)是一种记录重放装置，其特征在于，具备：第 86 方面所述的记录装置；重放记录在所述记录媒体中的数据的重放手段，所述重放手段从开始记录所述复制限制内容的时刻起经过规定待机时间之后，重放记录的所述复制限制内容。

又，第 89 方面(与权利要求 89 对应)是在第 88 方面所述的记录重放装置中，其特征在于，在向所述环形缓冲器进行重写记录的状态下，所述重放手段进行重放动作时，在所述环形缓冲器上，从记录最早的数据的位置开始进行该数据的重放。

又，第 90 方面(与权利要求 90 对应)是在第 89 方面所述的记录重放装置中，其特征在于，在向所述环形缓冲器进行重写记录的状态下，所述重放手段进行重放动作时，从所述环形缓冲器上的记录开始位置起进行该数据的重放。

又，第 91 方面(与权利要求 91 对应)是在第 87 或 88 方面所述的记录重放装置中，其特征在于，所述记录装置当在所述规定待机时间内没有重放记录在所述记录媒体中的复制限制内容时，停止该复制限制内容的记录动作。

又，第 92 方面(与权利要求 92 对应)是在第 87 或 88 方面所述的记录重放装置中，其特征在于，还具备根据所述规定时间或所述规定的待机时间中的任一个量预先告知所述记录装置或者重放手段的动作内容的告知手段。

又，第 93 方面(与权利要求 93 对应)是在第 76 方面所述的记录装置中，其特征在于，所述记录手段能够测量包含所述规定时间的时间信息。

又，第 94 方面(与权利要求 94 对应)是在第 76 方面所述的记录装置中，其特征在于，所述复制限制内容包含时间信息，该时间信息包含所述规定时间。

又，第 95 方面(与权利要求 95 对应)是在第 76 方面所述的记录装置中，其特征在于，与所述复制限制内容相独立，从外部取得包含所述规定时间的时间信息。

又，第 96 方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第 6 方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并

送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述复制许可信息，所述解密手段生成包含所述装置惟一密钥与所述复制许可信息中的至少一个的第1信息，所述解密手段采用所述记录单元信息生成将所述第1信息解密后的信息即内容密钥，所述解密手段采用所述内容密钥将所述数据解密。

又，第97方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第7方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述加密后的标题密钥解密。

又，第98方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第8方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述解密手段采用所述标题密钥将所述数据解密。

又，第99方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第9方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述重放后的标题密钥解密，所述解密手段生成包含所述标题密钥的第3信息，所述解密手段采用记录单元信息生成将所述第3信息解密后的信息即内容密钥，该记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述解密手段采用所述内容密钥将所述数据解密。

又，第100方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第10方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述解密手段采用所述复制许可信息将所述数据解密。

又，第101方面是一种重放装置，其特征在于，具备：进行控制以使得重

放由第 11 方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述重放后的标题密钥解密，所述控制手段控制所述记录手段以使得所述记录手段重放所述复制许可信息，所述解密手段生成包含所述标题密钥与所述复制许可信息中的至少一个的第 2 信息，所述解密手段采用记录单元信息生成将所述第 2 信息解密后的信息即内容密钥，该记录单元信息是将所述控制手段连续存取所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述解密手段采用内容密钥将所述数据解密。

又，第 102 方面是一种重放装置，其特征在于，具备：进行控制以使得重放由第 12 或 13 方面所述的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得重放所述复制许可信息，所述解密手段采用所述重放后的复制许可信息将所述数据解密。

又，第 103 方面是一种媒体，是装有通过计算机实现第 1~102 任意一方面的全部或一部分手段的全部或一部分功能用的程序以及/或者数据的媒体，其特征在于，它是由计算机能进行处理的媒体。

又，第 104 方面是一种信息集合体，其特征在于，它是利用计算机实现第 1~102 任意一方面所述的全部或部分手段的全部或一部分功能的程序以及/或者数据。

附图说明

图 1 是表示本发明第 1、2、4~6 实施形态中的硬盘装置的结构框图。

图 2 是说明本发明第 1 实施形态中的硬盘装置的主要功能图。

图 3 是表示本发明第 1 实施形态中的硬盘装置的加密手段结构框图。

图 4 是表示本发明第 1 实施形态中的硬盘装置的解密手段结构框图。

图 5(a) 是表示本发明第 1 实施形态中的硬盘装置在记录时的工作流程图。

(b) 是表示本发明第 1 实施形态中的硬盘装置在记录时的动作相关性的模式图。

图 6(a)是表示本发明第 1 实施形态中的硬盘装置在重放时的动作流程图。

(b)是表示本发明第 1 实施形态中的硬盘装置在重放时的动作相关性的模式图。

图 7(a)是说明采用本发明第 1 实施形态的硬盘装置的记录格式。

(b)表示与上述(a)的格式不同格式的示例。

图 8 是说明 CCI 的值及其含义。

图 9 是说明本发明第 1 实施形态中的硬盘装置进行记录重放的磁盘格式。

图 10 是表示本发明第 3 实施形态中的硬盘装置的结构框图。

图 11 是表示本发明第 4 实施形态中的硬盘装置的加密手段结构框图。

图 12 是表示本发明第 4 实施形态中的硬盘装置的解密手段结构框图。

图 13 是表示本发明第 5 实施形态中的硬盘装置的加密手段结构框图。

图 14 是表示本发明第 5 实施形态中的硬盘装置的解密手段结构框图。

图 15 是表示本发明第 6 实施形态中的硬盘装置的加密手段结构框图。

图 16 是表示本发明第 6 实施形态中的硬盘装置的解密手段结构框图。

图 17(a)是表示本发明实施形态中的硬盘装置的加密手段结构框图。

(b)是表示本发明实施形态中的硬盘装置的解密手段结构框图。

图 18(a)是表示本发明实施形态中的硬盘装置的加密手段结构框图。

(b)是表示本发明实施形态中的硬盘装置的解密手段结构框图。

图 19(a)是表示本发明实施形态的硬盘装置的加密手段的结构框图。

(b)是表示本发明实施形态中的硬盘装置的解密手段的结构框图。

图 20 是表示本发明第 7 实施形态中的硬盘装置的结构框图。

图 21 是本发明实施形态 1 的 AVHDD1 以及存档设备 2 的框图。

图 22 是本发明实施形态 1 的 AVHDD12 以及存档设备 13 的框图。

图 23 是本发明实施形态 1 的存档设备 16 的框图。

图 24 是本发明实施形态 1 的 AVHDD19 以及存档设备 2 的框图。

图 25 是本发明实施形态 2 的 AVHDD22 以及存档设备 23 的框图。

图 26 是本发明实施形态 4 的 AVHDD32 以及 DVD 装置 33 的框图。

图 27 是本发明实施形态 4 的数据流的结构图。

图 28 是本发明实施形态 1 的具备复制手段 80 的 AVHDD81 的框图。

图 29 是本发明实施形态 2 的具备复制手段 90 的 AVHDD91 的框图。

图 30 是本发明实施形态 3 的加密数据解密记录系统的框图。

图 31 是本发明实施形态 3 的记录装置 100 的框图。

图 32 是本发明实施形态 3 的解密记录装置 101 的框图。

图 33 是本发明实施形态 1 的记录重放装置的结构图。

图 34 是用于说明本发明实施形态 1 的记录重放装置动作的时序图。

图 35 是用于说明本发明实施形态 1 的记录重放装置动作的时序图。

图 36 是本发明实施形态 2 的记录重放装置的结构图。

图 37 是用于说明本发明实施形态 2 的记录重放装置动作的时序图。

图 38 是用于说明本发明实施形态 2 的记录重放装置动作的时序图。

图 39 是用于说明本发明实施形态 3 的记录重放装置动作的时序图。

图 40 是本发明实施形态 4 的记录重放装置的结构图。

图 41 是本发明实施形态 5 的记录重放装置的结构图。

图 42 是本发明实施形态 5 的记录重放装置动作的说明图。

图 43 是以往技术中进行转录重放的记录重放装置的结构图。

符号说明

1 IEEE1394 总线

2 硬盘装置

3 主系统

4 I/F

10 控制器

11 加密手段

12 解密手段

13 装置惟一密钥

14 控制手段

15 记录手段

16 I/F

17 加密后的内容

18 加密区域

19 加密器

22 加法器

23 标题密钥

24 CCI

-
- 25 记录单元号
 - 26 内容
 - 27 CCI
 - 28 加密后的标题密钥
 - 29 磁盘媒体
 - 31 解密器
 - 32 解密器
 - 33 解密器
 - 34 加法器
 - 35 标题密钥
 - 36 CCI
 - 37 解密后的内容
 - 39 记录单元
 - 41 格式
 - 47 硬盘装置
 - 51 控制器
 - 1001、1012、1019、1022、1032 AVHDD
 - 1002、1013、1016、1023 存档设备
 - 1003 STB
 - 1004、1028 加密手段
 - 1005 第 1 记录手段
 - 1006、1025、1034 存储手段
 - 1007、1027 移动手段
 - 1008、1031、1038 重放手段
 - 1009 第 2 记录手段
 - 1010、1021 第 2 记录媒体
 - 1011、1035 发送手段
 - 1014 缓冲器
 - 1015 高速发送手段
 - 1017 解读重放手段
 - 1018 IC 卡

1020 判断手段
1024 第 3 记录手段
1026 未加密数据化手段
1029 第 4 记录手段
1030 第 3 记录媒体
1033 DVD 装置
1036 第 5 记录手段
1037 DVD
2010 判别信息检测手段
2011 时间信息取得手段
2012 记录重放手段
2013 记录媒体
2014 记录缓冲器
2015 控制输入 I/F
2016 切换手段
具体实施方式

以下，参照附图对于本发明的实施形态进行说明。

(第 1 实施形态)

首先，对于第 1 实施形态进行说明。

图 1 是表示作为本发明的记录装置以及重放装置一实施形态的硬盘装置 2 的结构。

硬盘装置 2 与 IEEE1394 总线 1 连接，而且 IEEE1394 总线 1 与主系统 3 连接。

IEEE1394 总线是将 AV 数据的传输或命令的交换进行中继的 IEEE1394—1995 中所述的 IEEE 标准的高性能串行总线 (high performance serial bus)。

主系统 3 具备作为 IEEE1394 接口的 I/F16，它将要记录到硬盘装置 2 的必须保护著作权的数据传送给 IEEE1394 总线 1，或者通过 IEEE1394 总线 1 接收来自硬盘装置 2 的必须保护著作权的数据并进行重放，例如可以是 STB (set up box, 机顶盒) 等。

硬盘装置 2 是能够通过 IEEE1394 总线 1 与主系统 3 进行 AV 数据的交换并同时能够保护著作权且将 AV 数据记录到磁盘媒体或者从磁盘媒体重放 AV 数据

的装置。

即，硬盘装置 2 是这样的装置，即如图 2 所示，将必须保护著作权的 AV 数据加密后的内容 17 那样在加密后加以记录或者重放加密后的内容 17。

硬盘装置 2 由 I/F4、控制器 10、记录手段 15 构成。

又，控制器 10 由加密手段 11、解密手段 12、装置惟一密钥 13、控制手段 14 构成。

I/F4 是 IEEE1394—DTCP(Digital Transmission Content Protection, 数字传输内容保护)方式的接口，它是能够进行下述动作的接口，即通过 IEEE1394 总线 1 与主系统 3 等外部设备进行命令及 AV 数据交换，而且，将 AV 数据加密，进行与其他设备的认证，根据认证是否成功来使得解读密码的密钥无效等，由此，来保护通过 IEEE1394 总线 1 传送的 AV 数据的著作权。

构成控制器 10 的加密手段 11 是对从 I/F4 传送来的 AV 数据以及附加在 AV 数据上的数据进行加密的手段。

解密手段 12 是对记录手段 15 读出的 AV 数据以及附加 AV 数据上的数据进行解密的手段。

加密手段 11 与解密手段 12 的构造将在下文叙述。

装置惟一密钥 13 是固有分配给每一台硬盘装置的编号以及/或者记号，将其记录在不能由硬盘装置 2 以及/或者从控制器 10 的外部进行访问的区域中。

记录手段 15 由记录数据的磁盘媒体、对磁盘媒体进行信息记录重放的磁头、在前端安装磁头并且在磁盘媒体的任意的半径位置上进行定位动作的驱动臂、及使得磁盘媒体旋转的主轴电动机等构成，记录手段 15 是将数据记录到磁盘媒体或者从磁盘媒体读出数据的手段。在记录手段 15 中，读取数据的磁盘媒体安装在硬盘装置 2 内，对于硬盘装置 2 不能够自由脱卸。

控制手段 14 是进行控制的手段，它指定 LBA 并使得该 LBA 与记录手段 15 的磁盘媒体的磁头、扇区相对应，控制驱动臂、主轴电动机，将磁头定位并从磁头对磁盘媒体写入或读出数据。

另外，如上所述，在图 3 表示加密手段 11 的结构。

加密手段 11 由加密器 19、加密器 20、加密器 21 及加法器 22 构成。

又，在图 3 中，装置惟一密钥 13 如上所述是分配给硬盘装置 2 的硬盘装置 2 固有的数值以及/或者记号。即，将不同的装置惟一密钥 13 分配给每一台硬盘装置 2。又，将装置惟一密钥 13 存储在设置于硬盘装置 2 的控制器 10 内

的秘密区域 18。该秘密区域 18 是外部设备既不能写入也不能读出的受保护的区域，并且它是仅控制器 10 能够读出存储在秘密区域 18 中的信息的区域。具体来说，该秘密区域 18 是利用印刷基板上的 ROM 来实现的。即，将装置惟一密钥 13 记录在印刷基板上的 ROM 中。也就是说，不能够从硬盘装置 2 以及/或者控制器 10 的外部对该 ROM 进行访问。

标题密钥 23 是固有分配给每个 AV 数据的数值以及/或者记号。

CCI(Copy control information，复制控制信息)24 附加在 AV 数据中，它是表示复制许可信息的 2 位的数值，CCI24 是附加在同步数据包的同步首部的 sy 区域进行发送的。

图 8 表示 CCI 所获得的值及其含义。CCI 为 11 时，表示不许可复制。即，虽然能够收视附加了该值的 CCI 的 AV 数据，但禁止生成将该 AV 数据记录到硬盘装置 2 等形成的复制品。

当 CCI 为 10 时，表示能够复制一次。即，能够收视附加有该值的 CCI 的 AV 数据，并且还能够生成记录到硬盘装置 2 等形成的第 1 代 AV 数据复制品。

当 CCI 为 01 时，表示不可再进行复制。即，将 CCI 为仅复制一次的 AV 数据经过复制后的 AV 数据不可再进行复制。这表示禁止在此之上再进行复制。即，在记录可复制一次的内容之后，为了使得重放时不再进行复制，必须为不可再进行复制。

当 CCI 为 00 时，表示许可复制。即，能够自由地收视附加有该 CCI 值的 AV 数据并且还能够自由地进行复制。

记录单元号 25 是具有记录单元大小的记录块中固有的编号以及/或者记号，所述记录单元是控制手段 14 连续地对记录手段 15 进行访问的最小单位。即，对于上述不同的记录块分配不同的记录单元号 25。如此，记录单元号 25 是用户以及外部设备所不能够看到的秘密信息。关于记录单元号 25 与记录单元会在后文叙述。

又，本实施形态的记录单元号 25 是本发明的记录单元信息的示例。

内容 26 是构成电影、音乐、电视剧等节目的 AV 数据。

又，磁盘媒体 29 是由记录手段 15 能够读写数据的磁盘。

加密器 19 是读取存储在秘密区域 18 中的装置惟一密钥 13、将标题密钥 23 加密并输出加密后的标题密钥 28 的手段。

加法器 22 是生成接着标题密钥 23 的低位附加 CCI24 的密钥生成用信息的

手段。

又，本实施形态的密钥生成用信息是本发明第2信息的示例。

加密器20是采用记录单元号25将密钥生成用信息进行加密、生成内容密钥的手段。

加密器21是采用内容密钥将内容26进行加密的手段。

又，图4表示解密手段12的结构。

解密手段12由解密器31、解密器32、解密器33、加法器34构成。

又，在图4中表示了装置惟一密钥13、标题密钥35、CCI36、记录单元号25、解密后的内容37，而它们分别对应于图3所示的装置惟一密钥13、标题密钥23、CCI24、记录单元号25、内容26。

又，磁盘媒体29是由记录手段15读写数据的磁盘，与图3所示磁盘媒体相同。

解密器31是读取存储在秘密区域18中的装置惟一密钥13、采用装置惟一密钥13将加密后的标题密钥28解密并输出标题密钥35的手段。

加法器34是生成接着标题密钥35的低位附加CCI27的密钥生成用信息的手段。

解密器32是采用记录单元号25将密钥生成用信息解密并且生成内容密钥的手段。

解密器33是采用内容密钥将加密后的内容17解密并输出解密后的内容37的手段。

在图7(a)中表示记录手段15的磁盘媒体29的记录格式。磁盘媒体29的区域被分为记录单元大小的多个记录块即记录单元39。控制手段14不能够对比记录单元39更小的区域进行访问，而且必须要从记录单元39等的记录块的首部开始访问。即，控制手段14必须对记录单元39的每一记录块读出或写入数据。

又，在本实施形态中，将一个记录单元39分成首部38与数据区域40，这样来记录AV数据。

数据40是记录传输数据包的区域。又，在首部38中记录加密后的标题密钥35。记录在记录单元39的首部38区域中的信息以及记录在数据40区域中的信息都被加密。

即，图7(b)表示在记录媒体的记录块中记录AV数据的其他示例。将记录

块 150 分为首部 151 与数据 152 进行记录，这一点与本实施形态的记录格式是相同的。然而，在图 7(b) 中，首部 151 的部分是非加密 154 的部分，数据 155 的部分是加密 155 的部分。即仅仅数据 152 部分进行加密。因此，在 IEEE1394 总线 1 等中进行传送时，加密后被传送的密钥 153 并没有加密而记录在首部 151 的部分。因此，当外部设备不正当地对首部 151 的部分进行访问时，由于外部设备能够获得密钥 153，故会解读 AV 数据的密码而不能够保护其著作权。

与此相反，本实施形态的记录格式如图 7(a) 所示，由于将记录在记录单元 39 中的所有数据都进行加密，与图 7(b) 所示的记录格式相比，能够更可靠地保护著作权。

如此，本实施形态的记录格式是制造硬盘装置的制造厂所固有的。因此，采用标准格式的外部设备很难读取这样的以制造厂所固有的格式记录的数据。因此，通过采用本实施形态的记录格式，能够保护记录在磁盘媒体 29 上的 AV 数据的著作权。而且，还能够自由地设计本实施形态的记录格式的扇区大小以及记录单元的大小。

作为记录单元的具体示例，例如有磁盘媒体 29 的扇区。即，能够将 1 个扇区、连续的 62 个扇区、连续的 128 个扇区、…连续的 2048 个扇区等连续的规定个数的扇区作为记录单元 39。

又，作为上述的记录单元号 25 的具体示例，例如能够将扇区 LBA(logical block address，逻辑块地址)作为记录单元号 25。即，能够记录单元 39 的首个扇区的 LBA、从记录单元 39 首个扇区起第 2 个扇区的 LBA、从记录单元 39 首个扇区起第 N 个(N 为小于构成记录单元的扇区总数的整数)的任意一个作为记录单元号 25。

或者，也能够采用惟一确定记录单元 39 用的编号。即，能够将从磁盘媒体 29 的内周向外周顺序点数记录单元 39 时的编号作为记录单元号 25。

或者，也能够使用管理记录单元所用的内部管理用的地址。

或者，也能够采用根据一定规则组合上述那样多个示例后输出的数值或记号。

总之，作为记录单元号 25，是用户不能够看到的信息，只要是不重复地、惟一确定磁盘媒体 29 的所有记录单元 39 的信息即可。

又，本实施形态的硬盘装置 2 是本发明的记录装置的示例，本实施例的硬盘装置 2 也是本发明的重放装置的示例，本实施形态的记录手段兼作为本发明

的重放手段的示例。

再者，本实施形态的 I/F4 是本发明的接口的示例，本实施形态的磁盘媒体 29 是本发明的盘片的示例。

又，将包含加密手段 11、解密手段 12 以及装置惟一密钥 13 的控制器 13 与 I/F4 一体化设置在一块印刷基板上。又，将加密手段 11、解密手段 12、控制手段 14、I/F4 分别作为单片 LSI(大规模集成电路)进行安装。对于这些芯片端子上的信号，实施以不公开的格式进行位的交叉排列等的加密。因此，即使外部设备从这些端子作为 AV 数据取出能够重放的信号，由于不能解开生成信号的格式，故很难对 AV 数据进行重放。

其次，对于这样的本实施形态的动作进行说明。

首先，对于硬盘装置 2 记录必须保护著作权的 AV 数据时的动作进行说明。

又，在本实施形态中，以 MPEG2 传输流形式传送 AV 数据。

在图 5(a) 中，以流程图表示主系统 3、硬盘装置 2 的主要的动作。以下，根据该流程图进行说明。又，在图 5(b) 中，采用模式图来表示主系统 3、硬盘装置 2 的动作的相关性。

主系统 3 将必须保护著作权的 AV 数据进行加密并且作为同步数据包传递到 IEEE1394 总线 1。

I/F16 对 MPEG2 传输流形式的 AV 数据进行加密。再者，在加密后的 MPEG2 传输流的传输数据包上附加源数据包首部，生成源数据包。然后，在将源数据包分割或结合后的数据块中附加 CIP 首部，生成 CIP。再者，在 CIP 中附加同步首部，生成同步数据包并传递到 IEEE1394 总线 1。

又，在生成同步数据包时，将图 3 的 CCI24 附加到同步数据包的 sy 区域。

主系统 3 向硬盘装置 2 发出开始记录 AV 数据的命令。

该命令作为异步数据包从 I/F16 经 IEEE1394 总线 1 传递至 I/F4。

当 I/F4 接收到指示记录开始的命令时，向 I/F16 请求认证。

接收该请求后，I/F16 与 I/F4 进行认证动作(S1)。图 5(b) 中以认证 85 表示该认证动作。

为了由硬盘装置 2 记录 AV 数据，而由 I/F16 判断是正当的设备还是不正当的设备。若为正当设备，则认证成功，若为不正当的设备，则认证失败(S2)。

硬盘装置 2 在没有记录 AV 数据的资格的情况下，认证失败(S3)。此时，硬盘装置 2 不能够记录 AV 数据。

硬盘装置 2 若为能够记录 AV 数据的正当设备，则认证成功。

当认证成功时，I/F4 识别该同步信道并且接收主系统 3 传送的同步数据包。

然后，I/F4 从接收到的同步数据包的同步首部中分离出 CCI。

接着，根据 CCI 的值进行以下的动作。

即，在图 8 中，CCI 为 11 时，即在禁止复制的情况下，由于不允许记录 AV 数据，故 I/F4 通知主系统 3 不进行记录处理，并不向控制器 10 指示要开始记录处理。

当 CCI 为 10 时，即在许可复制一次的情况下，I/F4 通知主系统 3 开始记录处理并且还向控制器 10 指示要开始记录处理。

当 CCI 为 01 时，即在不再许可复制的情况下，I/F4 与禁止复制时进行相同动作。

当 CCI 为 00 时，即在允许复制的情况下，通知主系统 3 开始记录处理并且还向控制器 10 指示要开始记录处理。

因此，当 CCI 为 10 时，I/F4 以进行认证动作时从主系统 3 获得的密钥对加密的 AV 数据进行解密。然后，将解密后的 AV 数据在传用时间标记所指示的时刻对于每一传输数据包进行输出，该传用时间标记对于每一传送数据包附加在源数据包首部。当 CCI 为 00 时，由于没有加密而传送 AV 数据，故不进行解密处理，在传用时间标记所指示的时刻，对于每一传输数据包进行输出。

如此，从 I/F4 输出的 AV 数据被解密，成为未加密的数据，但由于输出的是以硬盘装置 2 独自的格式所记述的信号，故第 3 者即使从 I/F4 的芯片端子获得信号，第 3 者也很难恢复成能够利用的 AV 数据。

加密手段 11 输入从 I/F4 传送来的 MPEG2 传输数据包。

首先，加密器 19 读取存储在秘密区域 18 中的装置惟一密钥 13(S4)。

加密手段 11 检测出从 I/F4 传送来的 AV 数据上所附加的标题密钥 23。然后，加密器 19 通过装置惟一密钥 13 将检测出的标题密钥 23 进行加密(S5)。

然后，根据控制手段 14 的控制，如加密后的标题密钥 28 那样，将加密器 19 加密后的标题密钥 23 记录到记录手段 5 的磁盘媒体 29 上。图 5(b)中也表示了该加密后的标题密钥 28。

再者，加密手段 11 检测出附加在 AV 数据中并传送来的 CCI24。根据控制手段 14 的控制，将检测出的 CCI24 作为 CCI27 记录到记录手段 15 的磁盘媒体 29 上。

加法器 22 生成接着标题密钥 23 低位附加了 CCI24 的信息即密钥生成用信息。

另一方面，从控制手段 14，还传送来在哪个记录单元中记录 AV 数据的信息作为 AV 数据的附加信息。加密手段 11 求得进行记录的记录单元的记录单元号 25。

加密器 20 采用要记录 AV 数据的记录单元的记录单元号 25，将加法器所生成的密钥生成用信息进行加密。将该加密后的信息称作为内容密钥。内容密钥由于是以记录单元号 25 进行加密，对每个记录单元都不同。

其次，加密器 21 以内容密钥对从此开始记录的 AV 数据即内容 26 进行加密(S7)。

根据控制手段 14 的控制，将加密后的 AV 数据作为加密后的内容 17，记录到记录手段 15 的磁盘媒体 29 的应记录的记录单元(S8)。在图 5(b)中也表示加密后的内容 17。

以下，同样重复上述动作，即，对于每一记录单元以记录单元号 25 将密钥生成用信息进行加密，生成内容密钥，以生成的内容密钥将内容 26 进行加密(S7)，将加密后的内容 17 记录到磁盘媒体 29(S8)。

如此，硬盘媒体 29 能够将必须保护著作权的 AV 数据记录到磁盘媒体 29 上。

其次，对于硬盘装置 2 重放必须保护著作权的 AV 数据时的动作进行说明。

图 6(a)以流程图表示主系统 3、硬盘装置 2 重放时的主要动作。以下，根据该流程图进行说明。又，在图 6(b)中表示说明主系统 3、硬盘装置 2 重放时的主要动作的相关性的模式图。

主系统 3 向硬盘装置 2 发出指示开始重放的命令。

该命令作为异步数据包从 I/F16 经由 IEEE1394 总线 1 传送至 I/F4。

再者，I/F16 对 I/F4 进行认证请求。

接收该请求后，I/F16 与 I/F4 进行认证动作(S9)。在图 6 的(b)中，该认证动作表示为认证 86。

为了主系统 3 利用 AV 数据，I/F4 判断中正当设备还是不正当设备。若为正当设备，则认证成功，若为不正当设备，则认证失败(S10)。

当主系统 3 没有利用 AV 数据的资格时，认证失败(S11)。此时，主系统 3 不能够记录 AV 数据。

主系统 3 若为能够记录 AV 数据的正当设备时，则认证成功。

当认证成功时，I/F4 向控制器 10 通知已传送来重放 AV 数据的命令。

解密手段 12 当接收该通知时，首先，解密器 31 读取存储在秘密区域 18 中的装置惟一密钥 13(S12)。

然后，根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 中读出加密后的标题密钥 28(S13)。图 6(b)页表示了加密后的标题密钥 28。

解密器 31 根据装置惟一密钥 13 将加密后的标题密钥 28 解密(S14)。然后，解密手段 12 将解密后的标题密钥 35 传送至 I/F4。

根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 读出 CCI27。

解密手段 12 将 CCI27 传送至 I/F4。

加法器 34 生成密钥生成信息，该密钥生成信息是接着解密后的标题密钥 35 的低位附加了所读出的 CCI27 的信息。

控制手段 14 指定要读取的记录单元 39，并且进行控制以使得记录手段 15 读取存储在记录单元 39 中的信息即加密后的内容 17。

解密手段 12 求得记录单元 39 的记录单元号 25。

解密器 32 利用要进行读出数据的记录单元 39 的记录单元号 25，将加法器生成的密钥生成用信息进行解密。将该解密后的信息称作为内容密钥。由于内容密码是以记录单元号 25 进行解密的，故对于每个记录单元都不同。

其次，根据控制手段 14 的控制，记录手段 15 读出磁盘媒体 29 要读出的记录单元中记录的信息即加密后的内容 17(S15)。图 6(b)也表示加密后的内容 17。

其次，解密器 33 通过内容密钥将记录手段 15 读出的加密后的内容 17 进行解密(S16)。

解密手段 12 将解密后的内容传送至 I/F4。

以下，同样重复上述动作，即，对于每一记录单元以记录单元号 25 将密钥生成用信息解密，生成内容密钥，读出加密后的内容 17(S15)，通过内容密钥将加密后的内容 17 解密(S16)，将解密后的内容 27 作为 MPEG2 传输流传送至 I/F4。

又，虽然从解密手段 12 输出的 AV 数据被解密，但由于是以硬盘装置 2 独自的格式所记述的信息，故第 3 者即使从解密手段 12 的芯片端子取出信号，第 3 者也很难将其复原成能够利用的 AV 数据。

I/F4 将从控制器 10 传送来的 AV 数据进行加密。然后，作为同步数据包传送到 IEEE1394 总线 1。

主系统 3 的 I/F16 识别同步信道并且接收同步数据包，将加密的 AV 数据进行解密。

I/F16 将接收到的 AV 数据作为 MPEG2 传输流输出。

输出的 AV 数据被主系统 3 所具有的未图示的传输流解码器分离。然后，未图示的 AV 解码器进行 AV 解密并且变换为模拟信号而显示在显示器上。

如此，硬盘媒体 29 从磁盘媒体 29 重放必须保护著作权的 AV 数据。

本实施形态的硬盘装置 2 在记录 AV 数据时、重放 AV 数据时以及对记录手段 15 完成 AV 数据记录的任何一种情况下，都能够保护必须保护著作权的 AV 数据的著作权。

又，在本实施形态中，是以磁盘 29 不能够从硬盘装置 2 脱卸的情况为示例进行了说明，但不仅限于此，也可以能够为自由脱卸的结构。

再者，在本实施形态中，是以将装置惟一密钥 13 存储到硬盘装置 2 的印刷基板上作为秘密区域 18 的 ROM 为示例进行了说明，但并不仅限于此。在磁盘媒体 29 中也可以设置秘密区域 18。即，也可以将装置惟一密钥 13 存储到磁盘 29 中的用户不能够访问的区域中。

再者，在本实施形态中，是对于将加密后的标题密钥 28 记录到磁盘 29 的用户能够访问的用户区域的情况进行了说明，但不仅限于此。也可以记录到磁盘媒体 29 的用户不能够访问的系统区域中。又，也可以记录到设置在硬盘装置 2 的印刷基板上的 RAM 中。

再者，在本实施形态中，是对于本发明的记录装置以及重放装置作为硬盘装置 2 而一体化的情况进行了说明，但并不仅限于此。本发明的记录装置可以由 I/F4、加密手段 11、控制手段 14、记录手段 15 构成，它是记录 AV 数据的装置，又，本发明的重放装置可以由 I/F4、解密手段 12、记录手段 15 构成，总之，只要本发明的记录装置具备加密手段、控制手段、记录手段即可。又，只要本发明的重放装置具备解密手段、控制手段即可。

再者，对于本实施形态的硬盘装置 2 的 I/F4、加密手段 11、解密手段 12、控制手段 14 是分别由单片 LSI 构成的情况进行了说明，但并不仅限于此。I/F4、加密手段、解密手段 12、控制手段 14 也可以分别由多个芯片 LSI 构成。又，是对于在芯片的端子上 AV 数据以非公开格式记述的情况进行了说明，但并不

仅限于此，为了在端子间进行传送，也可以进行加密。又，芯片端子的性质也可以由非公开的格式来决定。又，这里芯片端子的性质是表示，哪个端子输出哪种信号、哪个端子与哪个端子组合后输出哪种信号、或各端子用于哪种用途等性质。由于这样的芯片端子的性质由非公开的格式决定，例如，用户不能够获知各端子用于何种用途等等。总之，在设置 I/F4、控制器 10 的印刷基板上的端子以及芯片端子中，输出第 3 者能够作为 AV 数据重放的信号的端子所检测出的信号，只要都被加密或者/以及以非公开的格式进行记述或者以非公开的格式决定这些端子的性质即可。

再者，本实施形态的硬盘装置 2 的 I/F4、加密手段 11、解密手段 12、控制手段 14 也可以由单片 LSI 构成。若如此，更能够可靠地保证 AV 数据的著作权。

再者，在本实施形态中，是采用 CCI 对 AV 数据进行加密的情况作为了说明，但并不仅限于此。也可以不用 CCI 对 AV 数据进行加密。即，取代加法器 22 根据 CCI 与标题密钥 23 生成密钥生成用信息，也可以不采用加法器 22，将标题密钥 23 直接作为密钥生成用信息，通过记录单元号将该密钥生成用信息进行加密，生成内容密钥。又，此时的标题密钥 23 是本发明的第 3 信息的示例。如此，在不采用 CCI 而对 AV 数据进行加密的情况下，也可以如本实施形态那样将 CCI 记录到磁盘媒体 29，或者也可以不将 CCI 记录到磁盘媒体 29。

再者，在本实施形态中，对对于下述情况进行了说明，即硬盘装置 2 当附加在 AV 数据上的 CCI 的值为禁止复制的情况下，不记录该 AV 数据，当 CCI 的值为复制一次的情况下，将该 AV 数据加密之后进行记录，当 CCI 的值为不允许再复制的情况下，不记录该 AV 数据，在 CCI 的值为允许复制的情况下，将该 AV 数据加密之后进行记录，但并不仅限于此。即使在获得了附加在 AV 数据上的 CCI 的值为任意值的情况下，也可以将 AV 数据加密后加以记录。或者，当附加在 AV 数据上的 CCI 的值为允许复制的情况下，也可以不将该 AV 数据加密而直接记录未加密的数据。

再者，在本实施形态中，对于密钥生成用信息是接着解密后的标题密钥其低位附加所读出的 CCI 的信息的情况作了说明，但并不仅限于此，作为密钥生成用信息，也可以是在标题密钥的高位前附加所读出的 CCI 的信息。再者，密钥生成用信息也可以仅包含标题密钥与 CCI 的信息，也可以包含标题密钥与 CCI 并且还包含其他信息。另外，也可以是包含标题密钥及 CCI 的任何一个的信息。

管理信息写入系统 FAT42，将系统 FAT42 更新为最新的信息。

最后，控制手段 14 将重新写入了 AV 数据的记录单元的 CCI 的值写入到文件管理信息。

如此，在记录 AV 数据时，首先，将 AV 数据记录到磁盘媒体 29 上，在完成记录 AV 数据之后，将管理信息记录到磁盘媒体 29，最后将 CCI 写入系统 FAT42。

然而，假设在记录 AV 数据的过程中，用户错将硬盘装置 2 的电源插头拔掉，而切断了硬盘装置 2 的电源。此时，已经正在记录中的 AV 数据的已经记录下来部分的文件管理信息与 CCI 消失。

本实施形态的硬盘装置 2 如下述这样重放如此中断记录的 AV 数据。

控制手段 14 根据一定的规则决定写入磁盘媒体 29 的空记录单元的顺序。

中断了记录的 AV 数据是根据该规则进行记录，控制手段 14 根据更新前的文件管理信息进行重放。然后，加密手段 11 根据 CCI 的 2 位的值的组合，试着进行解密。

然后，以解密成功的 CCI 的值，从最初开始将 AV 数据解密。

如此，本实施形态的硬盘装置 2 能够对记录中断了的 AV 数据进行正常的解密。

进一步，AV 数据的终端根据附加在传输数据包中的 PCR 的值的连贯性进行检测。

即，PCR 以最长为 100ms 的间隔附加在传输数据包中，PCR 的值是以 27MHz 的频率计数为高位 33 位、低位 9 位的计数值。因此可见，若 PCR 的值变成相当于 100ms 以上的值时，则超过 AV 数据的终端而重放其他 AV 数据。因此，加密手段 11 仅将 PCR 的值为连续的范围中的 AV 数据传送给 I/F4。

又，在本实施形态的硬盘装置 2 中，是对于与第 1 实施形态相同进行加密以及解密的情况进行了说明，但并不局限于此。也可以进行与第 1 实施形态不同的加密。总之，只要是采用 CCI 进行加密的硬盘装置即可。

再者，在本实施形态的硬盘装置 2 中，是对假定 CCI 的值并试着进行解码的情况进行了说明，但并不局限于此。也可以在记录 AV 数据之前将 CCI 记录到磁盘 29，即使中断 AV 数据记录，CCI 也一定记录在记录手段 15 中。

再者，在本实施形态中，对于本发明的记录装置以及重放装置是作为硬盘装置 2 形成一体化的情况进行了说明，但并不局限于此。本发明的记录装置可

总之，本实施形态的密钥生成用信息只要是包含标题密钥与 CCI 中的至少一个的信息即可。

(第 2 实施形态)

其次，对于第 2 实施形态进行说明。

在本实施形态中，以 CCI 的处理为中心进行说明。

图 1 中表示作为本发明记录装置以及重放装置一实施形态的硬盘装置 2 的结构。

本实施形态的硬盘装置 2 的结构与第 1 实施形态相同。

图 9 表示记录手段 15 的磁盘媒体 29 的格式 41。纸面左侧是磁盘媒体 29 的磁盘内周 45，纸面右侧与磁盘外周 46 相对应。磁盘内周 45 侧的区域是系统 FAT42，磁盘外周 46 侧是数据 43。

系统 FAT42 是用户不能够访问的系统区域，它是文件管理信息等、控制手段 14 控制系统所使用的区域。

另一方面，对于数据 43，是用户能够访问区域，记录 AV 数据。即，如图 3、图 4 所示那样，记录加密后的内容 17、加密后的标题密钥 28 等。

然后，将 CCI 如 CCI 数据 44 所示那样，记录到系统 FAT42 中每一构成数据 43 的记录单元。即，将 CCI 的值分配给每一记录单元。

又，作为文件管理信息，例如由 FAT(File allocation Table，文件分配表)与称为目录的信息构成。

FAT 是成对表示记录单元的地址与下一记录单元的地址的表，它表示将文件的数据以何种顺序存放到哪个记录单元中。

又，目录是分级管理文件的表，它是成对表示文件名及存放于文件中的数据存放的首部其记录单元的地址、与表示文件为只读或可进行重写等属性的信息的表。

若采用 FAT 与目录，则能够管理文件的生成、编辑、删去等的处理。

其次，对于本实施形态的动作进行说明。

与第 1 实施形态相同，硬盘装置 2 记录 AV 数据。此时，与第 1 实施形态相同，AV 数据一个接一个地记录到每个记录单元。每当向新的记录单元完成记录 AV 数据，则由控制手段 14 生成、更新表示将 AV 数据记录在哪个记录单元的文件管理信息。然后，将该文件管理信息存储在自身的存储器中。

接着，在完成记录所有的 AV 数据的时刻，控制手段将生成、更新的文件

以由 I/F4、加密手段 11、控制手段 14、记录手段 15 构成，它是记录 AV 数据的装置，又，本发明的重放装置可以由 I/F4、解密手段 12、控制手段 14、记录手段 15 构成，总之，本发明的记录装置只要具备加密手段、控制手段、记录手段即可。又，本发明的重放装置只要具备解密手段、控制手段即可。

再者，在本发明的实施形态中，对于文件管理信息由 FAT 与目录形成的情况进行了说明，但并不局限于此。也可以采用 OS/2 中的 HPFS (high performance file system, 高性能文件系统)、Mac OS 的文件系统、UNIX 中的 i 节点、Windows 95 中的 VFAT (virtual FAT, 虚拟 FAT)，Windows NT 的 NTFS (new technology file system, 新技术文件系统) 等的文件管理信息。然而，此时，必须要使得第 1 实施形态中所说明的记录单元与这些文件管理信息的记录块相一致。总之，也可以采用对于硬盘能够进行记录重放的 OS 中的文件管理信息。

(第 3 实施形态)

其次，对于第 3 实施形态进行说明。

图 10 是表示本发明的记录装置以及重放装置的一实施形态的硬盘装置 47 的结构。

本实施形态的硬盘装置 47 具备 I/F48 以替代第 1 实施形态的 I/F4。又，本实施形态的控制器 51 不具有加密手段 11、解密手段 12、装置惟一密钥 13。

I/F48 的接口是不将从 IEEE1394 总线 1 传送来的加密后的 AV 数据解密而传送到控制器 51，并且将从控制器 51 传送来的加密后的 AV 数据原样地传送到 IEEE1394 总线 1。除此之外，与第 1 实施形态的 I/F4 相同。

其次，以与第 1 实施形态的不同点为中心，对于本实施形态的硬盘装置 47 的动作进行说明。

首先，对于记录 AV 数据时的动作进行说明。

与第 1 实施形态相同，I/F16 与 I/F48 进行认证动作，并假设认证成功。这样，I/F48 识别同步信道并且接收从主系统 3 传送来的同步数据包。

然后，从同步数据包中复原出 MPEG2 传输流。接着，将传输数据包依次传送到控制器 15。

控制手段 14 进行控制，以使得记录手段将加密的 AV 数据记录到磁盘 29。

除此之外，与第 1 实施形态相同。

如此，本实施形态的硬盘装置 47 原样地记录加密的 AV 数据。

其次，对于重放加密的 AV 数据时的动作进行说明。

与第 1 实施形态相同，I/F16 与 I/F48 进行认证动作，并假设认证成功。这样，控制手段 14 进行控制，以使得记录手段 15 读出加密的 AV 数据，然后，控制器 51 将读出的 AV 数据作为 MPEG2 传输流传送到 I/F48。

I/F48 将加密的 MPEG2 传输流作为同步数据包传送到 IEEE1394 总线 1。

除此之外，与第 1 实施形态相同。

如此，本实施形态的硬盘装置 47 照原样地记录以及重放传送给而加密的 AV 数据，通过这样的简单结构能够保护 AV 数据的著作权。

(第 4 实施形态)

其次，对于第 4 实施形态进行说明。

图 1 是表示作为本发明的记录装置以及重放装置的一实施形态的硬盘装置 2。本实施形态的硬盘装置 2 将第 1 实施形态中所说明的硬盘装置 2 的加密手段 11 与解密手段 12 替换成其他的加密手段与解密手段。

图 11 表示本实施形态的硬盘装置 2 的加密手段 60。又，图 12 表示本实施形态的解密手段 61。

在本实施形态中，以作为与第 1 实施形态的不同点的加密手段 60 与解密手段 61 为中心进行说明。

在图 11 中，加密手段 60 由加密器 19、加密器 52、加密器 21 形成。即，加密手段 60 与第 1 实施形态的加密手段 11 不同，没有采用 CCI 进行加密。

即，加密器 19 是读取存储在秘密区域 18 中的装置惟一密钥 13 并将标题密钥 23 加密而输出加密后的标题密钥 28 的手段。

又，本实施形态的标题密钥 23 是本发明第 1 信息的示例。

加密器 52 是采用记录单元号 25 将标题密钥 23 加密即生成内容密钥的手段。

加密器 21 是采用内容密钥将内容 26 加密的手段。

图 12 表示本实施形态的硬盘装置 2 的解密手段 61。

在图 12 中，解密手段 61 由解密器 31、解密器 53、解密器 33 构成。解密手段 61 与第 1 实施形态不同，它在解密中没有采用 CCI。

即，解密器 31 是读取存储在秘密区域 18 中的装置惟一密钥 13 并采用装置惟一密钥 13 将加密的标题密钥 28 解密而输出标题密钥 35 的手段。

又，本实施形态的标题密钥 28 是本发明的第 2 信息的示例。

解密器 53 是采用记录单元号 25 将标题密钥 35 进行解密并生成内容密钥

的手段。

解密器 33 是采用内容密钥将加密后的内容 17 解密并且输出解密后的内容 37 的手段。

其次，以作为与第 1 实施形态不同点的加密手段 60 与解密手段 61 的动作为中心进行说明本实施形态的动作。

首先，说明加密手段 60 的动作。

加密器 19 读取存储在秘密区域 18 中的装置惟一密钥 13。

加密手段 60 检测出从 I/F4 传送给的附加在 AV 数据中的标题密钥 23。然后，加密器 19 通过装置惟一密钥 13 将检测出的标题密钥 23 进行加密。

然后，由加密器 19 加密后的标题密钥 23，根据控制手段 14 的控制，如加密后的标题密钥 28 那样，记录到记录手段 15 的磁盘媒体 29 中。

再者，加密手段 60 检测出附加在 AV 数据中而传送给的 CCI24。根据控制手段 14 的控制，将检测出的 CCI24 作为 CCI27 记录到记录手段 15 的磁盘媒体 29 上。

加密手段 60 求得进行记录的记录单元的记录单元号 25。

加密器 52 采用要进行 AV 数据记录的记录单元的记录单元号 25 将标题密钥 23 加密。将该加密后的信息称为内容密钥。内容密钥由于以记录单元号 25 进行加密，故对于每个记录单元都不同。

其次，加密器 21 将从此要开始记录的 AV 数据即内容 26 通过内容密钥进行加密。

根据控制手段 14 的控制，将加密后的 AV 数据作为加密后的内容 17 记录到记录手段 15 的磁盘媒体 29 的要进行记录的记录单元。

以下，同样反复进行上述动作，即对于每个记录单元，将标题密钥 23 以记录单元号 25 进行加密并输出内容密钥，以生成的内容密钥将内容 26 加密，将加密后的内容 17 记录到磁盘媒体 29。

如此，硬盘媒体 29 将必须保护著作权的 AV 数据记录到磁盘媒体 29。

其次，对于解密手段 61 的动作进行说明。

解密器 31 读取存储在秘密区域 18 中的装置惟一密钥 13。

再者，根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 中读出加密后的标题密钥 28。

解密器 31 根据装置惟一密钥 13 将加密后的标题密钥 28 解密。然后，解

密手段 61 将解密后的标题密钥 35 传送到 I/F4。

根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 读出 CCI27。

解密手段 12 将 CCI27 传送到 I/F4。

控制手段 14 指定要读取的记录单元 39 并且进行控制，以使得记录手段 15 读取存储在记录单元 39 中的信息即加密后的内容 17。

解密手段 61 求得记录单元 39 的记录单元号 25。

解密器 53 采用要读出数据的记录单元 39 的记录单元号 25 将标题密钥 35 解密。将该解密后的信息称为内容密钥。内容密钥由于通过记录单元号 25 解密，故对于每个记录单元都不同。

然后，根据控制手段 14 的控制，记录手段 15 读出存储在磁盘媒体 29 的要读出的记录单元中的信息即加密后的内容 17。

然后，解密器 33 通过内容密钥将记录手段 15 读出的加密后的内容 17 解密。

解密手段 61 将解密后的内容 37 传送到 I/F4。

以下，同样重复上述动作，即对于每个记录单元，通过记录单元号 25 将标题密钥 35 解密并生成内容密钥，读出加密后的内容 17，通过内容密钥将加密后的内容 17 解密，将解密后的内容 27 作为 MPEG2 传输流传送到 I/F4。

通过将本实施形态中所说明的加密手段 60 与解密手段 61 用于硬盘装置 2，能够获得与第 1 实施形态相同的效果。

又，当然，也能够将加密手段 60 与解密手段 61 适用于第 1 实施形态中所说明的各种变形例。

(第 5 实施形态)

其次，对于第 5 实施形态进行说明。

图 1 是表示作为本发明的记录装置以及重放装置的一实施形态的硬盘装置 2。本实施形态的硬盘装置 2 将第 1 实施形态中所说明的硬盘装置 2 的加密手段 11 与解密手段 12 替换成其他的加密手段与解密手段。

图 13 表示本实施形态的硬盘装置 2 的加密手段 62。又，图 14 表示本实施形态的解密手段 63。

在本实施形态中，以作为与第 1 实施形态的不同点的加密手段 62 与解密手段 63 为中心进行说明。

在图 13 中，加密手段 62 由加法器 54、加密器 55、加密器 21 构成。本实

施形态的加密手段 62 与加密手段 11 不同，在 AV 数据的加密中并没有采用标题密钥。

即，加法器是 54 是生成接着装置惟一密钥 13 的低位附加了 CCI24 的密钥生成用信息的手段。

又，本实施形态的密钥生成用信息是本发明第 1 信息的示例。

加密器 55 是采用记录单元号 25 将密钥生成用信息加密即生成内容密钥的手段。

加密器 21 是采用内容密钥将内容 26 加密的手段。

图 14 中表示本实施形态的硬盘装置 2 的解密手段 63。

在图 14 中，解密手段 13 由加法器 56、解密器 57、解密器 33 构成。

加法器 56 是读取存储在秘密区域 18 中的装置惟一密钥 13 并且生成接着装置惟一密钥 13 的低位附加了 CCI36 的密钥生成用信息的手段。

解密器 57 是采用记录单元号 25 将密钥生成用信息解密并生成内容密钥的手段。

解密器 33 是采用内容密钥将加密后的内容 17 解密并输出解密后的内容 37 的手段。

其次，以作为与第 1 实施形态的不同点的加密手段 62 与解密手段 63 的动作为中心，对于这样的本实施形态的动作进行说明。

首先，说明加密手段 62 的动作。

加法器 54 读取存储在秘密区域 18 中的装置惟一密钥 13。然后，生成在装置惟一密钥 13 的低位附加 CCI24 的密钥生成用信息。

再者，加密手段 62 检测出附加在 AV 数据中而传送来的 CCI24。根据控制手段 14 的控制，将检测出的 CCI24 作为 CCI27 记录到记录手段 15 的磁盘媒体 29 上。

然后，加法器 54 生成接着装置惟一密钥 13 的低位附加 CCI24 的密钥生成用信息。

加密手段 62 求得要记录的记录单元的记录单元号 25。

加密器 55 采用要记录 AV 数据的记录单元的记录单元号 25 将密钥生成用信息加密。将该加密后的信息称为内容密钥。内容密钥由于是通过记录单元号 25 而加密，故对于每个记录单元都不同。

其次，加密器 21 通过内容密钥将就此开始记录的 AV 数据即内容 26 加密。

根据控制手段 14 的控制，将加密后的 AV 数据作为加密后的内容 17 记录到记录手段 15 的磁盘媒体 29 的要进行记录的记录单元中。

以下，同样重复上述动作，即对于每个记录单元，以记录单元号 25 将密钥生成用信息加密并生成内容密钥，以生成的内容密钥将内容 26 加密，将加密后的内容 17 记录到磁盘媒体 29。

如此，硬盘媒体 29 将必须保护著作权的 AV 数据记录到磁盘媒体 29 上。

其次，对于解密手段 63 的动作进行说明。

加法器 56 读出存储在秘密区域 18 中的装置惟一密钥 13。

根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 中读出 CCI27。

解密手段 63 将 CCI27 传送到 I/F4。

加法器 56 生成接着装置惟一密钥 13 的低位附加了 CCI27 的密钥生成用信息。

控制手段 14 指定要读取的记录单元 39 并且进行控制，以使得记录手段 15 读出存储在记录单元 39 中的信息即加密后的内容 17。

解密手段 63 求得记录单元 39 的记录单元号 25。

解密器 57 采用要读出数据的记录单元 39 的记录单元号 25 将密钥生成用信息解密。将该解密后的信息称为内容密钥。内容密钥由于通过记录单元号 25 解密，故对于每个记录单元都不同。

然后，根据控制手段 14 的控制，记录手段 15 读出存储在磁盘媒体 29 的要读出的记录单元中的信息即加密后的内容 17。

然后，解密器 33 通过内容密钥将记录手段 15 读出的加密的内容 17 解密。

解密手段 63 将解密后的内容 37 传送到 I/F4。

以下，同样重复上述动作，即对于每个记录单元，以记录单元号 25 将密钥生成用信息解密并生成内容密钥，读出加密后的内容 17，通过内容密钥将加密后的内容 17 解密，并将解密后的内容 27 作为 MPEG2 传输流传送到 I/F4。

通过将本实施形态中所说明的加密手段 62 与解密手段 63 用于硬盘装置 2，能够获得与第 1 实施形态相同的效果。

又，当然，加密手段 62 与解密手段 63 也能够适合第 1 实施形态中所说明的各种变形例。

(第 6 实施形态)

其次，对于第 6 实施形态进行说明。

图 1 中表示作为本发明的记录装置以及重放装置的一实施形态的硬盘装置 2。本实施形态的硬盘装置 2 将第 1 实施形态中所说明的硬盘装置 2 的加密手段 11 与解密手段 12 替换成其他加密手段与解密手段。

图 15 表示本实施形态的硬盘装置 2 的加密手段 64。又，图 16 表示本实施形态的解密手段 65。

在本实施形态中，以作为与第 1 实施形态的不同点的加密手段 64 与解密手段 65 为中心进行说明。

在图 15 中，加密手段 64 由加密器 58、加密器 21 构成。本实施形态的加密手段 64 与加密手段 11 不同，在 AV 数据的加密中并没有采用标题密钥及 CCI。

即，加密器是 58 是采用记录单元号 25 将装置惟一密钥 13 加密即生成内容密钥的手段。

又，本实施形态的装置惟一密钥 13 是本发明第 1 信息的示例。

加密器 21 是采用内容密钥将内容 26 加密的手段。

图 16 中表示本实施形态的硬盘装置 2 的解密手段 65。

在图 16 中，解密手段 65 由解密器 59、解密器 33 构成。

解密器 59 是采用记录单元号 25 将装置惟一密钥 13 解密并生成内容密钥的手段。

解密器 33 是采用内容密钥将加密后的内容 17 解密并输出解密后的内容 37 的手段。

其次，以作为与第 1 实施形态的不同点的加密手段 64 与解密手段 65 的动作作为中心，对于这样的本实施形态的动作进行说明。

首先，说明加密手段 64 的动作。

加密手段 64 检测出附加在 AV 数据中而传送来的 CCI24。根据控制手段 14 的控制，将检测出的 CCI24 作为 CCI27 记录到记录手段 15 的磁盘媒体 29 上。

加密器 58 从秘密区域 18 读取装置惟一密钥 13。

加密手段 64 求得要记录的记录单元的记录单元号 25。

加密器 58 采用要记录 AV 数据的记录单元的记录单元号 25 将装置惟一密钥 13 加密。将该加密后的信息称为内容密钥。内容密钥由于是通过记录单元号 25 而加密，故对于每个记录单元都不同。

其次，加密器 21 通过内容密钥将就此开始记录的 AV 数据即内容 26 加密。

根据控制手段 14 的控制，将加密后的 AV 数据作为加密后的内容 17 记录

到记录手段 15 的磁盘媒体 29 的要进行记录的记录单元中。

以下，同样重复上述动作，即对于每个记录单元，以记录单元号 25 将装置惟一密钥 13 加密并生成内容密钥，以生成的内容密钥将内容 26 加密，将加密后的内容 17 记录到磁盘媒体 29。

如此，磁盘媒体 29 上记录有必须保护著作权的 AV 数据。

其次，对于解密手段 63 的动作进行说明。

解密器 59 读取存储在秘密区域 18 中的装置惟一密钥 13。

根据控制手段 14 的控制，记录手段 15 从磁盘媒体 29 中读出 CCI27。

解密手段 65 将 CCI27 传送到 I/F4。

控制手段 14 指定要读取的记录单元 39 并且进行控制，以使得记录手段 15 读出存储在记录单元 39 中的信息即加密后的内容 17。

解密手段 63 求得记录单元 39 的记录单元号 25。

解密器 59 采用要读出数据的记录单元 39 的记录单元号 25 将装置惟一密钥解密。将该解密后的信息称为内容密钥。内容密钥由于通过记录单元号 25 解密，故对于每个记录单元都不同。

然后，根据控制手段 14 的控制，记录手段 15 读出存储在磁盘媒体 29 的要读出的记录单元中的信息即加密后的内容 17。

然后，解密器 33 通过内容密钥将记录手段 15 读出的加密后的内容 17 解密。

解密手段 63 将解密后的内容 37 传送到 I/F4。

以下，同样重复上述动作，即对于每个记录单元，以记录单元号 25 将装置惟一密钥解密并生成内容密钥，读出加密后的内容 17，通过内容密钥将加密后的内容 17 解密，并将解密后的内容 27 作为 MPEG2 传输流传送到 I/F4。

如此，解密手段 65 将加密后的内容 17 解密。

通过将本实施形态中所说明的加密手段 64 与解密手段 65 用于硬盘装置 2，能够获得与第 1 实施形态相同的效果。

又，当然，加密手段 64 与解密手段 65 也能够适合第 1 实施形态中所说明的各种变形例。

又，在第 4~6 实施形态中说明了各种加密手段与解密手段，但不局限于此，例如，也能够采用图 17、图 18、图 19 所示手段，替代硬盘装置 2 的加密手段 11 以及解密手段 12。

在图 17(a) 中表示加密手段 73。加密手段 73 采用装置惟一密钥 13，由加密器 67 将内容 26 加密。

又，在图 17(b) 中表示解密手段 74。解密手段 74 利用装置惟一密钥 13 将由加密手段 73 加密后的内容 17 解密，并且输出解密后的内容 37。

在图 18(a) 中表示加密手段 75。加密手段 75 采用记录单元号 25，由加密器 69 将内容 26 加密。

又，在图 18(b) 中表示解密手段 76。解密手段 76 由解密器 70 利用记录单元号 25 将由加密手段 75 加密后的内容 17 解密，并且输出解密后的内容 37。

在图 19(a) 中表示加密手段 77。加密手段 77 采用装置惟一密钥 13 与记录单元号 25，由加密器 71 将内容 26 加密。另外，也可以这样构成，即对加密手段 77 追加加法器，加法器将装置惟一密钥 13 与记录单元号 25 结合，加密器 71 采用该信息将内容 26 加密。

又，在图 19(b) 中表示解密手段 78。解密手段 78 利用装置惟一密钥 13 与记录单元号 25 由解密器 72 将由加密手段 77 加密后的内容 17 解密。

又，也可以在解密手段 78 中追加加法器，加法器将装置惟一密钥与记录单元号 25 结合，利用该信号解密器 72 将加密后的内容 17 解密。

(第 7 实施形态)

其次，对于第 7 实施形态进行说明。

图 20 是表示作为本发明记录装置以及重放装置的一实施形态的硬盘装置 83 的结构。

硬盘装置 83 除了具备第 1 实施形态的硬盘装置 2 之外，还具备 CCI 判定手段 79、重放信息管理手段 80。又，取代第 1 实施形态中的 I/F 而具有 I/F81、取代第 1 实施形态的控制手段 14 而具备控制手段 82。

I/F81 与第 1 实施形态的 I/F4 的不同点在于，即使当从 IEEE1394 总线 1 获得的 AV 数据的 CCI 为禁止复制的情况下，也向控制器 10 通知开始记录处理，控制器 10 根据来自 I/F81 的通知，即使在 AV 数据的 CCI 为禁止复制的情况下，也在规定的条件下能够记录 AV 数据。

又，CCI 判定手段 79 是判定重放后的 AV 数据的 CCI 值并且决定重放后的 CCI 值的手段。

重放信息管理手段 80 是管理重放信息的手段，重放信息是表示对于每个记录单元重放了一次记录在记录手段 15 中的 AV 数据或者一次都没有进行重放

的信息。

又，重放管理手段 80 也是对于每个记录单元在记录手段 15 中记录的 AV 数据被其他设备复制了还是一次也没有复制的信息进行管理的手段。

若根据重放信息，能够获知已经重放了一次记录在记录单元中的 AV 数据或者一次也没有进行重放，例如，重放信息能够由 1 位的标记来表示。

又，若参照复制信息，能够获知已经复制了一次记录在记录单元中的 AV 数据或者一次也没有被复制。

控制手段 82 除了进行第 1 实施形态的控制手段 14 的动作以外，还进行下述控制动作，即将重放中的 AV 数据的 CCI 提供给 CCI 判定手段 79，根据重放中的 AV 数据的 CCI 与由重放信息管理手段 80 生成并更新的重放信息，控制记录手段 15 是否进行 AV 数据的重放，又，将复制到其他设备过程中的 AV 数据的 CCI 提供给 CCI 判定手段 79，根据复制中的 AV 数据的 CCI 与重放信息管理手段 80 生成并更新的复制信息，控制记录手段 15 是否进行 AV 数据的复制。

又，本实施形态的 CCI 判定手段 79、控制手段 82、重放信息管理手段 80 是本发明的控制手段的示例，本实施形态的 I/F81 是本发明的接口的示例。

其次，以与第 1 实施形态的不同点为中心，对于上述本实施形态的动作进行说明。

首先，说明记录时的动作。

从主系统传送来 AV 数据。

I/F81 即使当该 AV 数据的 CCI 为禁止复制的情况下也通知控制器 84 以使得开始记录。

加密手段 11 将 AV 数据加密。

根据控制手段 82 的控制，记录手段 15 将加密后的 AV 数据记录到磁盘 29 中。此时，与第 1 实施形态相同，也记录 CCI。

然而，控制手段 82 当 CCI 即使为禁止复制的情况下，也记录该 AV 数据。而记录在记录手段 15 中的 CCI 是禁止复制的 AV 数据在被记录后的规定时间之后不能够重放。如何使得在规定时间后不能够重放，将下文叙述。

又，控制手段 82 为了复制 CCI 为允许复制一次的 AV 数据虽然将数据输出，但从被复制输出之后的规定时间之后不能够重放。对此，也将在下文中叙述。

重放信息管理手段 80 当对于每个记录单元将 AV 数据记录到记录手段 15 时，如下述这样生成重放信息与复制信息。

即，当从新记录 AV 数据时，对于每个记录单元将重放信息设定为未重放、将复制信息设定为未复制。再者，将记录 AV 数据的时刻进行记录。

其次，对于重放这样记录下来的 AV 数据时的动作进行说明。

重放信息管理手段 80 参照由此开始重放的记录单元的 AV 数据的重放信息并且通知控制手段 82。

再者，CCI 判定手段 79 判定由此开始重放的 AV 数据的 CCI 的值，确定被重放输出时的 CCI 的值。

即，被重放的 AV 数据的 CCI 为禁止复制时，将从 I/F81 输出时的 CCI 作为禁止复制。又，被重放的 AV 数据的 CCI 为允许复制一次时，将从 I/F81 输出时的 CCI 变成不再许可复制。又，当 CCI 为允许自由复制时，使得从 I/F81 输出时的 CCI 为自由复制。又，由于没有记录 CCI 的值为不再许可复制的 AV 数据，故 CCI 不会为不再许可复制。

根据控制手段 82 的控制，记录手段重放 AV 数据。

重放信息管理手段 80 如下述这样更新重放管理信息。

即，当重放记录单元部分的 AV 数据时，向控制手段 82 通知该重放信息。又，当重放记录单元部分的 AV 数据时，将该部分的重放信息设定为重放完成。

重放信息管理手段 80 当当前重放中的 AV 数据的重放信息为已经重放完成时，通知控制手段 82。

又，重放信息管理手段 80 将当前重放中的 AV 数据的时刻信息通知控制手段 82。

控制手段 82 根据由 CCI 判定手段 79 改变前的 CCI 的值，进行以下动作。

即，若为 CCI 是禁止复制的 AV 数据时，则进行控制以使得中止重放信息的重放完成部分的重放。又，当从重放信息管理手段 80 发出通知、从与该 AV 数据相关的时刻信息所表示的时刻起当前的时刻已经经过规定时间例如 240 小时(10 天)以上的情况下，进行控制以使得不重放该 AV 数据。

又，当为 CCI 是允许复制一次的 AC 数据的情况下，进行控制，以使得与重放信息的值无关，继续重放。

又，当为 CCI 是许可自由复制的 AV 数据时，进行控制以使得继续重放。

如此被重放的 AV 数据由解密手段 12 解密。

然后，在 I/F81 为了传送而被加密，并且作为同步数据包输出到 IEEE1394 总线 1。此时在同步首部中，如上述那样附加了由 CCI 判定手段 79 决定的 CCI。

其次，对于复制上述这样记录下来的 AV 数据时的工作进行说明。

重放信息管理手段 80 参照从此开始复制的记录单元的 AV 数据的复制信息并通知控制手段 82。

再有，CCI 判定手段 79 判定从此开始复制的 AV 数据的 CCI 的值并且决定被重放输出时的 CCI 的值。

即，被重放的 AV 数据的 CCI 为禁止复制时，没有设定 I/F81 输出时的 CCI 或者使其为禁止复制。又，当被重放的 AV 数据的 CCI 为复制一次时，使得从 I/F81 输出时的 CCI 保持原样为复制一次且没有改变成不再许可复制。又，当 CCI 为许可复制时，使得从 I/F81 输出时的 CCI 为许可复制。又，由于没有记录 CCI 的值为不再许可复制的 AV 数据，因此 CCI 不会为不再许可复制。

根据控制手段 82 的控制，记录手段重放被复制的 AV 数据。

重放信息管理手段 80 如下述这样更新复制管理信息。

即，当复制记录单元部分的 AV 数据时，将该复制信息通知控制手段 82。又，当复制记录单元部分的 AV 数据时，将该部分的复制信息设定为复制完成。

重放信息管理手段 80 当当前复制中的 AV 数据的 复制信息为已经复制完成时，通知控制手段 82。

控制手段 82 根据由 CCI 判定手段 79 改变前的 CCI 的值，进行下述动作。

即，若是 CCI 为禁止复制的 AV 数据，则进行控制以使得不进行复制。

又，当是 CCI 为许可复制一次的 AV 数据时，进行控制以使得不进行复制信息为复制完成的部分的复制，当复制信息为未复制时，限于将该部分 AV 数据加以记录的装置是作为备份用而记录所述数据的装置的情况，进行控制以使得继续复制。

又，当 CCI 为许可复制的 AV 数据的情况下，继续控制以使得继续复制。

为了这样进行复制，由解密手段 12 将重放后的 AV 数据解密。

然后，在 I/F81 为了进行传送而加密，并作为同步数据包输出到 IEEE1394 总线 1。此时，在同步首部中，如上述那样附加 CCI 判定手段 79 决定的 CCI。通过 IEEE1394 总线 1 由其他设备接收并记录。

又，被复制的 AV 数据的 CCI 为许可复制一次的情况下，在作为备份用而记录的记录装置，不能够重放该 AV 数据，若不返回原来的硬盘 83，则不能够进行重放。

即，本实施形态的硬盘装置 83 记录禁止复制的 AV 数据并且能够仅重放一

次。

由于不允许记录 CCI 为禁止复制的 AV 数据，故仅在广播时间段能够进行收视。

然而，若采用本实施形态的硬盘装置 83，则维持著作权者的本意的情况下，在与广播 AV 数据的时间段不同的其他时间段能够进行收视。

又，允许仅复制一次 CCI 为许可复制一次的 AV 数据。即，一旦记录了许可复制一次的 AV 数据时，仅能够从记录下该数据的装置重放该 AV 数据。

但是，若采用本实施形态的硬盘装置 83，由于能够将许可复制一次的 AV 数据按照许可复制一次的 CCI 那样仅复制一次，故能够在维护著作权的本意的基础上，将该 AV 数据移动到其他记录重放装置中。

又，在本实施形态中说明的情况是，重放信息管理手段 80 当重放记录单元部分的 AV 数据时，将该重放信息通知控制手段 82，当重放记录单元部分的 AV 数据时，将该部分的重放信息设定为重放完成，通过这样对于本实施形态的硬盘装置 83 能够仅重放一次 CCI 为禁止复制的 AV 数据，但并不局限于此。重放信息管理手段 80 也可以如下述这样构成更新重放信息的方法。

即，重放信息管理手段 80 也可以对于重放了几次记录单元部分的 AV 数据进行计数，直到重放规定次数例如 5 次起将该记录单元部分的 AV 数据的重放信息设定为重放完成。如此，硬盘装置 83 能够将 CCI 为复制禁止的数据仅重放规定次数。

又，重放信息管理手段 80 也可以对于一个 AV 数据中的记录在各记录单元中的部分进行重放的次数进行计数，在一个 AV 数据所有的记录单元中所记录的部分都被重放的时刻，重放信息管理手段 80 将该一个 AV 数据所有的记录单元中所记录的部分的重放管理信息设定为重放完成。如此，硬盘装置 83 能够无数次重放 CCI 为复制禁止的 AV 数据的一部分，在重放了全部该 AV 数据的时刻开始就不能够进行重放。

再有，在本实施形态中，是对于从记录了 CCI 为禁止复制的 AV 数据开始经过规定时间后不能够进行重放的情况作了说明，但并不局限于此，也可以根据收费条件，CCI 为禁止复制的 AV 数据为禁止复制。作为这样的收费条件，在记录了 CCI 为禁止复制的 AV 数据时，若支付了规定的费用时，则能够进行重放，若没有付费则不能进行重放。

再者，在本实施形态中说明的情况是，对于 CCI 为许可复制一次的 AV 数

据，当复制信息为未复制时，限于将该部分 AV 数据加以记录的装置是作为备份用记录所述数据的装置的情况，进行控制以使得继续复制，但并不局限于此，也可以从记录 CCI 为许可复制一次的 AV 数据开始经过规定时间后，删去该记录的 AV 数据或者记录该数据时的加密用的密钥。

如此，本实施形态的硬盘装置 83 由于记录 CCI 为禁止复制的 AV 数据，或者将 CCI 为许可复制一次的 AV 数据按照许可复制一次的 CCI 那样仅进行一次重放，因此，可以说能够保护著作权者的本意，能够抵制侵犯著作权的情况。即，这是由于当 CCI 为禁止复制的情况下，表示绝对不可以复制。然而，现在正在研究，使用将这样的 CCI 的含义的扩展 CCI。在扩展 CCI 中，将禁止复制以及许可复制一次的含义加以扩展解释。本实施形态的硬盘装置 83 也能够替代以往的 CCI 而采用扩展 CCI 进行上述动作。如此，若本实施形态的硬盘装置 83 采用扩展 CCI 进行上述动作时，也不会侵犯著作权。

如此，若采用本实施形态的硬盘装置 83，对于不允许记录的 AV 数据，能够在广播时间段以外的任意时间进行收视。又，由于能够将仅允许复制 1 次的 AV 数据移动到其他的记录装置，故能够用作为备份装置。

又，关于对不允许记录的 AV 数据，能够在广播时间段以外的任意时间段进行收视或者进行备份，这在下述的实施形态中还将进一步详细说明。

又，对于本实施形态的硬盘装置 83，当然也能够进行第 1 实施形态中所说明的种种变形。

再者，对于本实施形态的硬盘装置 83，是就具备加密手段 11、解密手段 12 的情况作了说明，而也可以采用第 1 实施形态以后所说明的加密手段、解密手段。

再者，本发明的数据并不局限于本实施形态的 AV 数据。也可以是通过因特网等传送来的文本数据及图像数据、通过因特网等传送来的游戏软件及文本生成软件等计算机程序。总之，本发明的数据只要是能够记录在本发明的盘片并且能够从本发明的盘片中重放出来并加以利用的数据即可。

再者，本发明的接口不局限于本实施形态中的 IEEE1394 接口，也可以采用 USB 接口。

再者，本发明的盘片不限于本实施形态的磁盘媒体，也可以是光盘媒体或光磁盘媒体等。总之，本发明的盘片只要是能够在记录时以及/或者重放时随机对数据进行存取的记录媒体即可。

再者，本发明的复制许可信息不限于本实施形态中的 CCI 以及扩展 CCI 等，总之只要是表示关于复制数据是否许可的信息即可。

又，在上述的实施形态中，作为附加在 AV 数据中的 CCI 的值，是对于其为禁止复制、许可复制一次、禁止再复制、许可自由复制的情况作了说明，而在以下说明的第 8~11 实施形态中，将 CCI 的值为禁止复制、许可复制一次以及禁止再复制中的任意之一的 AV 数据一概作为复制禁止数据进行处理。又，关于复制禁止数据的 CCI 与上述的禁止复制、许可复制一次以及禁止再复制中的哪一个对应，将在第 8~第 11 实施形态中个别进行说明。

(第 8 实施形态)

其次，对于本发明第 8 实施形态的 AVHDD1001 以及存档设备 1002 的结构进行描述。

在图 21 中，表示本发明第 8 实施形态的 AVHDD1001 以及存档设备 1002 的框图。又，在图 21 中，为了说明方便，也画出 STB(机顶盒)1003。

本发明第 8 实施形态的 AVHDD1001 如图 21 所示，由将来自 STB1003 的数据通过 AVHDD1001 固有加密密钥进行加密的加密手段 1004、将由加密手段 1004 加密后的数据记录到存储手段 1006 内的记录媒体的第 1 记录手段 1005、存储数据的存储手段 1006、将存储在存储手段 1006 中的数据移动到存档设备 1002 中的移动手段 1007、解读来自存档设备 1002 的数据即通过 AVHDD1001 固有加密密钥加密的数据并进行重放的重放手段 8 构成。又，存储手段 1006 具有记录数据的第 1 记录媒体，将数据记录在该第 1 记录媒体中。

又，在“发明的实施形态”中，将 AVHDD 用作表示采用硬盘驱动器(HDD)对音频(Audio)以及视频(Video)以及其他数据进行记录重放的装置的单词。

其次，如图 21 所示，本发明第 8 实施形态的存档设备 1002 由将来自 AVHDD1001 的数据记录到第 2 记录媒体 1010 中的第 2 记录手段 1009、第 2 记录媒体 1010、读出记录在第 2 记录媒体 1010 中的数据并且发送至 AVHDD1001 的发送手段 1011 构成。又，作为存档设备 1002，例如相当于 DVD 装置。D-VHS 装置、在本实施形态中，作为存档设备 1002 的一示例是采用 DVD 装置进行说明的。因此，作为第 2 记录媒体 1010 的一示例，相当于 DVD。

又，STB1003 是例如接收来自广播台的数据并且将该数据输出到 AVHDD1001 且同时重放来自 AVHDD101 的数据的手段，被重放的数据若为视频数据，则显示在与 STB1003 连接的显示器上，若为音频数据，则从与 STB1003 连接的扬声

器输出。又，在图中没有表示显示器以及扬声器。

又，在第 8 实施形态中，作为本发明的数据处理装置的一示例采用 AVHDD1001、作为记录重放装置的一示例采用存档设备 1002。

又，AVHDD1001 的存储手段 1006 内的第 1 记录媒体也可以是可移动的记录媒体，也可以是固定设置型的记录媒体。同样，存档设备 1002 内的第 2 记录媒体 1010 也可以是可移动的记录媒体、也可以是固定设置型的记录媒体。

又，AVHDD1001 与存档设备 1002 的连接可以通过 IEEE1394 标准的接口进行，也可以通过 IDE 标准的接口进行。又，也可以通过其他接口进行。对于 AVHDD1001 与 STB1003 的连接，也可以通过任意的接口进行。

其次，对于本发明第 8 实施形态的 AVHDD1001 以及存档设备 1002 的动作进行叙述。

以下，为了说明方便起见，将 AVHDD1001 的存储手段 1006 内的第 1 记录媒体的可记录容量作为到达界限，必须要重写或删去任一数据，才能够存储来自 STB1003 的新的数据，用户将使得存储手段 1006 内的数据移动到存档设备 1002 内的第 2 记录媒体 1010 用的指示提供到 AVHDD1001 以及存档设备 1002。

又，所谓数据的移动，表示例如将记录在第 1 记录媒体中的数据移动到其他的第 2 记录媒体中，并且移动后在第 1 记录媒体内不保留已经移动的数据。

又，为了以下的说明方便起见，假设从 AVHDD1001 移动到存档设备 1002 的数据由加密手段 1004 以 ACHDD1001 固有的加密密钥加密并且由第 1 记录手段 1005 记录到存储手段 1006 内的第 1 记录媒体。又，为了进行著作权保护，使得上述移动对象的数据为允许移动到其他记录装置而禁止复制的复制禁止数据。

此时，移动手段 1007 从存储手段 1006 内的第 1 记录媒体中读出以 AVHDD1001 固有的加密密钥加密的复制禁止数据并且发送到存档设备 1002。如此，在移动手段 1007 发送复制禁止数据时(移动时)，该移动手段 1007 将复制禁止数据作为仅可复制一次的数据输出。

然后，在存档设备 1002 中，第 2 记录手段 1009 将来自 AVHDD1001 的复制禁止数据记录到第 2 记录媒体 1010 中。又，由移动手段 1007 移动到存档设备 1002 的数据在 AVHDD1001 内并没有被解密而在保持加密的状态下移动到存档设备 1002。因此，由第 2 记录手段 1009 记录到第 2 记录媒体 1010 中的数据成为以 AVHDD1001 固有的加密密钥加密的复制禁止数据。

其次，对于重放记录在第 2 记录媒体 1010 中的、被加密的复制禁止数据的情况进行说明。如图 21 所示，在存档设备 1002 中，由于没有设置解读被加密的复制禁止数据并进行重放的手段，故必须再次将数据移动到能够解读复制禁止数据并进行重放的 AVHDD1001 的重放手段 1008。

这里，在重放记录在第 2 记录媒体 1010 中的、被加密的复制禁止数据时，发送手段 1011 读出记录在第 2 记录媒体 1010 中的数据并发送给 AVHDD1001，在 AVHDD1001 中，重放手段 1008 解读被加密的复制禁止数据并进行重放。

将该解读重放后的数据输出到 STB1003，若为视频数据，则显示在与 STB1003 连接的显示器上，若为音频数据，则从与 STB1003 连接的显示器输出。

如此，例如，即使在 ACHDD1001 的存储手段 1006 内的第 1 记录媒体的可记录容量达到界限的情况下，由于也可以不因重写存储手段 1006 内的数据等而删去，能够将数据移动到其他记录媒体，因此，具有能够重放移动后的数据的优点。

又，即使由于不正当行为，在大量复制与存档设备 1002 对应的且与第 2 记录媒体 1010 同样的媒体并进行分发的情况下，但记录在该媒体中的数据是由 AVHDD1001 的加密手段 1004 以 AVHDD1001 固有的加密密钥进行了加密后的数据，故能够重放该数据的也仅是 AVHDD1001，能够对著作权保护对象数据即复制禁止数据保护其著作权，移动到其他装置即存档设备 1002。因此，能够实现数据的安全移动。另外，生产的许多 AVHDD1001 的固有加密密钥各不相同。

又，在上述的实施形态中，复制禁止数据是由 AVHDD1001 的加密手段 1004 以 AVHDD1001 固有加密密钥进行了加密，但复制禁止数据并不局限于由加密手段 1004 来加密。例如，也可以在 AVHDD1001 的制造阶段，将以 AVHDD1001 固有加密密钥加密后的复制禁止数据记录到存储手段 1006 内的第 1 记录媒体。

又，在上述实施形态中，复制禁止数据是在由加密手段 1004 加密后记录在存储手段 1006 内的第 1 记录媒体，但也可以将加密手段 1004 设置在存储手段 1006 与移动手段 1007 之间，在复制禁止数据和用移动手段 1007 移动时，利用 HVHDD1001 固的加密密钥进行加密。总之，移动手段 1007 想要移动的复制禁止数据，只要至少在从 AVHDD1001 输出时利用该 AVHDD1001 固有的加密密钥进行加密即可。

又，在本实施形态中，是将复制禁止数据作为允许移动到其他的记录装置而禁止复制的数据，而在“发明实施形态”中的“复制禁止数据”中，也包含

以 2 位表示为“01”的“此后禁止复制”的数据以及以 2 位表示为“11”的“绝对禁止复制”的数据。

又，采用图 21 所说明的上述实施形态的发送手段 1011 也可以置换成如图 23 所示的将记录在第 2 记录媒体 1010 中的数据以通常的 N 倍速 (N 为超过 1 的正数) 发送到 AVHDD1001 的高速发送手段 1015。此时，将图 21 的 AVHDD1001 置换成还设有作为数据存放手段的缓冲器 1014 的 AVHDD1012，能够将来自高速发送手段 1015 中的数据暂时存放到缓冲器 1014 中，再由重放手段 1008 重放该暂时存放的数据。

于是它带来的优点是从存档设备 1013 向 AVHDD1012 能够以 N 倍速 (高速) 传送数据，同时在 AVHDD1012 能够按通常情况重放数据。又，缓冲器 1014 也可以设置在存储手段 1006 内。又，“通常的 N 倍速”是指，比在重放手段 1008 重放数据时、用户收视时所必要的数据重放速度更快的速度。

又，在采用图 23 进行说明的示例中，是在存档设备 1013 中设置高速发送手段 1015，并且使得从存档设备 1013 向 AVHDD1012 以 N 倍速 (高速) 传送数据，但也可以将 AVHDD1007 置换成使得数据以 N 倍速 (N 为超过 1 的正数) 高速移动到存档设备的高速移动手段。此时，在存档设备中最好设置暂时存放数据的缓冲器。如此，当在 AVHDD 中设有高速移动手段时，具有能够在短时间将数据从 AVHDD 移动到存档设备的优点。又，在后述的实施形态 2 的 AVHDD 中，若也替代移动手段设置高速移动手段，则也具有能够在短时间移动数据的效果。

又，在上述实施形态中，在存档设备 1002 中并没有设置解读以 AVHDD1001 固有的加密密钥被加密的数据并进行重放的手段，但也可以如图 23 所示，将存档设备 1002 置换成具备能够解读并重放以 AVHDD1001 固有的加密密钥被加密的数据的解读重放手段 1017 的存档设备 1016，就不需要向 AVHDD1001 发送数据，在存档设备 1016 中，解读并重放以 AVHDD1001 固有的加密密钥被加密的数据。

如此，在存档设备 1016 中，当能够解读并重放以 AVHDD1001 固有的加密密钥被加密的数据时，则解决了仅为了重放数据而必须连接存档设备 1002 与 AVHDD1001 的问题。

又，为了存档设备 1016 的解读重放手段 1017 解读并重放被加密的数据，必须要 AVHDD1001 固有的加密密钥，而也可以预先在存档设备 1016 中设置 IC 卡槽，如图 23 所示，当将记录有 AVHDD1001 固有的加密密钥的 IC 卡 1018 插

入到 IC 卡槽时，解读重放手段 1017 从 IC 卡 1018 取得 AVHDD1001 固有的加密密钥，并采用该加密密钥解读加密的数据并进行重放。

又，当采用 IC 卡 1018 时，除了解读重放手段 1017 之外，也可以在存档设备 1016 中设置重放 IC 卡 1018 的密钥重放手段。又，也可以在存档设备 1016 中设置存储来自 IC 卡 1018 的 AVHDD1001 固有的加密密钥的密钥存储手段。如此，若在存档设备 1016 中设置密钥存储手段，则当解读并重放记录在第 2 记录媒体 1010 中的、以 AVHDD1001 固有的加密密钥被加密的数据时，能够避免每次必须将 IC 卡 1018 插入 IC 卡槽中的问题。又，作为记录在 IC 卡 1018 中的密钥，为了防止密钥的泄漏，可以将秘密密钥与公开密钥组合起来。

又，在上述记载中，是解读重放手段 1017 直接或间接地从 IC 卡 1018 中取得 AVHDD1001 固有的加密密钥，但也可以替代 IC 卡 1018，解读重放手段 1017 从记录或者埋入了 AVHDD1001 固有的加密密钥的密钥盘片以及密钥盒中取得加密密钥。又，也可以在第 2 记录媒体 1010 中记录 AVHDD1001 固有的加密密钥。此时，则不必要 IC 卡 1018、密钥盘片、密钥盒。

又，也可以不采用 IC 卡 1018、密钥盘片或者密钥盒，而在 AVHDD1001 中设置发送 AVHDD1001 固有的加密密钥的手段，同时在存档设备 1016 中设置接收来自 AVHDD1001 的加密密钥的手段，则解读重放手段 1017 采用发送来的加密密钥将加密的数据解密并重放。

又，在上述实施形态中，如图 21 所示，是使得 AVHDD1001 无条件地 将加密的数据移动到存档设备 1002，但也可以如图 24 所示，将图 21 的存档设备 2 的第 2 记录媒体 1010 置换成记录认证信息的第 2 记录媒体 1021，所述认证信息表示是与 AVHDD1019 对应的记录媒体的情况，与此同时将 AVHDD1001 置换成具备判断手段 1020 的 AVHDD1019，该判断手段 1020 判断第 2 记录媒体 1021 是否为与 AVHDD1019 对应的记录媒体，仅当由判断手段 1020 判断第 2 记录媒体 1021 为与 AVHDD1019 对应的记录媒体时，移动手段 1007 从 AVHDD1019 向存档设备 1002 移动数据。

又，若在第 2 记录媒体 1021 记录认证信息，则判断手段 1020 判断第 2 记录媒体 1021 是与 AVHDD1019 相对应的记录媒体，若没有记录认证信息，则判断手段 1020 判断第 2 记录媒体 1021 与 AVHDD1019 并不对应。

然而，记录认证信息的第 2 记录媒体 1021 为了与没有记录认证信息的记录媒体进行区别，可以使盘片表面具有与未记录认证信息的记录媒体表面颜色

不同的颜色，又，由于为著作权保护用的记录媒体，故也可以比没有记录认证信息的记录媒体贵一定的程度。这样，与没有记录认证信息的记录媒体的价格差额的全部或一部分也可以返回著作权者或者著作权团体。

又，也可以在第 2 记录媒体 1021 是与 AVHDD1019 对应的记录媒体时，不使得数据从 AVHDD1019 移动到存档设备 1002，在存档设备 1002 是与 AVHDD1019 对应的装置时，使得数据从 AVHDD1019 移动到存档设备 1002。此时，在 AVHDD1019 中，设置判断存档设备 1002 是否为与 AVHDD1019 对应的装置的判断手段。

又，当确认在连接 AVHDD1001 与存档设备 2 的接口上连接有能够至少对复制禁止数据的移动进行收费的管理装置时，AVHDD1001 的移动手段 1007 也可以使得该复制禁止数据移动到存档设备 2 中。又，作为管理装置的一示例，可以举出有了 STB。

又，在上述实施形态中，使得复制禁止数据从 AVHDD 移动到存档设备。即，在使得复制禁止数据移动到存档设备之后，从 AVHDD 中删去复制禁止数据。然而，有时由于认为在存档设备中不能够处理复制禁止数据，故最好将复制禁止数据作为备份保留在 AVHDD 中。

此时，若将上述实施形态中的各 AVHDD 的移动手段 1007 置换成将复制禁止数据复制到存档设备的复制手段，则在向存档设备发送复制禁止数据的同时，能够在 AVHDD 内备份存储复制禁止数据，它的优点是，即使在存档设备中不能够处理复制禁止数据的情况下，也能够利用备份存储在 AVHDD 中的复制禁止数据。

这里，作为具备复制手段的 AVHDD 结构的一示例，是将图 21 所示的具备移动手段 1007 的 AVHDD1001 置换成替代移动手段 1007 而具备复制手段 1080 的 AVHDD1081，作为示例将其示于图 28 中。

(第 9 实施形态)

其次，对于本发明第 9 实施形态的 AVHDD1022 以及存档设备 1023 的结构进行叙述。

在图 25 中表示本发明第 9 实施形态的 AVHDD1022 以及存档设备 1023 的框图。又，与上述第 8 实施形态的图 21 相同，为了说明方便起见，在图 25 中也画出 STB1003。

另外，本发明的第 9 实施形态的 AVHDD1022 如图 25 所示，由将来自 STB1003

的数据记录到存储手段 1025 内的记录媒体的第 3 记录手段 1024、存储数据的存储手段 1025、将存储在存储手段 1025 中的数据变成未加密的数据的未加密数据化手段 1026、将由未加密数据化手段 1026 未加密数据化后的存储在存储手段 1025 中的数据移动到存档设备 1023 的移动手段 1027 构成。

本发明第 9 实施形态的存档设备 1023 如图 25 所示，由采用存档设备 1023 固有的加密密钥对来自 AVHDD1022 的数据进行加密的加密手段 1028、将由加密手段 1028 加密后的数据记录到第 3 记录媒体 1030 的第 4 记录手段 1029、第 3 记录媒体 1030、采用存档设备 1023 固有的加密密钥将记录在第 3 就媒体 1030 中的数据解密并重放的重放手段 1031 构成。又，作为存档设备 1023，例如相当于 DVD 装置、D-VHS 装置。本实施形态中，作为存档设备 1023 的一示例采用 DVD 装置，作为第 3 记录媒体 1030 的一示例采用 DVD。

又，在第 9 实施形态中，作为本发明的数据处理装置的一示例采用 AVHDD1022、作为本发明的记录重放装置的一示例采用存档设备 1023。

又，AVHDD1022 的存储手段 1025 内的记录媒体可以是可移动的记录媒体，也可以是固定设置型的记录媒体。同样，存档设备 1023 中内的第 3 记录媒体可以是可移动的记录媒体、也可以是固定设置型的记录媒体。

又，AVHDD1022 与存档设备 1023 的连接，与采用图 21 所说明的第 8 实施形态相同，可以通过任意一种接口进行连接。

其次，对于本发明第 9 实施形态的 AVHDD22 以及存档设备 23 的动作进行叙述。

由用户对 AVHDD1022 以及存档设备 1023 发出使得存储手段 1025 内的数据移动到存档设备 1023 内的第 3 记录媒体 1030 的指示。又，所谓数据的移动与第 8 实施形态所述的相同，表示例如将记录在第 1 记录媒体上的数据移动到另一第 2 记录媒体并且在移动之后在第 1 记录媒体内不保留移动了的数据。

又，为了说明方便起见，移动对象数据是为了著作权保护而允许移动到其他记录装置且禁止复制的复制禁止数据，是由第 3 记录手段 1024 记录在存储手段 1025 内的记录媒体中的数据。

另外，此时未加密数据化手段 1026 将存储在存储手段 1025 中的数据生成未加密数据，移动手段 1027 从存储手段 1025 内的记录媒体中读出未加密数据的复制禁止数据并且发送给存档设备 1023。如此，在移动手段 1027 发送复制禁止数据时(移动时)，该移动手段 1027 将复制禁止数据作为仅可复制一次的

数据输出。

然后，在存档设备 1023 中，加密手段 1028 采用存档设备 1023 固有的加密密钥将来自 AVHDD1022 的数据加密，第 4 记录手段 1029 将由加密手段 1028 加密的数据记录到第 3 记录手段 1030。又，将数据输入存档设备 1023 时或者记录到第 3 记录媒体 1030 时，将其作为复制禁止数据处理。

又，在从 AVHDD1022 到存档设备 1023 的数据传送路径上，例如也可以通过 DTCP 保护传送数据。

其次，对于重放在第 3 记录媒体 1030 中记录的、以存档设备 1023 固有的加密密钥被加密的复制禁止数据的情况进行说明。此时，重放手段 1031 采用存档设备 1023 固有的加密密钥来重放记录在第 3 记录媒体 1030 中的复制禁止数据。

如此，在存档设备 1023 中，由于以存档设备 1023 固有的加密密钥加密数据并加以记录，故具有的优点是，在存档设备 1023 内能够重放记录的数据。

又，在上述实施形态中，存档设备 1023 的加密手段 1028 是采用存档设备 1023 固有的加密密钥对来自 AVHDD1022 的复制禁止数据进行加密，而当在第 3 记录媒体 1030 中记录加密密钥时，加密手段 1028 也可以采用记录在第 3 记录媒体 1030 中的加密密钥对来自 AVHDD1022 的复制禁止数据加密。此时，重放手段 1031 采用记录在第 3 记录媒体 1030 中的加密密钥来重放复制禁止数据。

又，在上述实施形态中，从 AVHDD1022 移动到存档设备 1023 的数据为未加密数据，而移动数据也可以为以存档设备 1023 固有的加密密钥加密后的数据，当将加密密钥记录在第 3 记录媒体 1030 时，移动数据也可以为以记录在该第 3 记录媒体 1030 中的加密密钥加密后的数据。

此时，在 AVHDD1022 中设置加密手段，该加密手段采用存档设备 1023 固有的加密密钥或者记录在第 3 记录媒体 1030 中的加密密钥，对复制禁止数据进行加密。又，在 AVHDD1022 中设置从存档设备 1023 取得存档设备 1023 固有的加密密钥的手段或从存档设备 1023 中取得记录在第 3 记录媒体 1030 中的加密密钥的手段。又，存档设备 1023 中不需要设置加密手段 28。

又，从 AVHDD1022 移动到存档设备 1023 的数据也可以是存档设备 1023 中所采用的格式的数据。此时，在 AVHDD1022 中可以设置格式变换手段，该格式变换手段将移动来的数据转换成存档设备 1023 所用格式的数据。又，在 AVHDD1022 中，当向存储手段 1025 内记录数据时，也可以以存档设备 1023 所

使用的格式记录该数据。

又，也可以如第 8 实施形态中采用图 24 进行的说明那样，在 AVHDD1022 中设置判断第 3 记录媒体 1030 是否为与 AVHDD1022 相对应的记录媒体的判断手段，当由该判断手段判断第 3 记录媒体 1030 是与 AVHDD1022 对应的记录媒体时，移动手段 1027 将未加密数据的或加密后的复制禁止数据移动到存档设备 1023 中。

又，当在第 3 记录媒体 1030 中，附加表示该第 3 记录媒体 1030 是否为与 AVHDD1022 对应的记录媒体的密钥时，设置在 AVHDD1022 中的判断手段也可以利用附加在第 3 记录媒体 1030 中的密钥，判断第 3 记录媒体 1030 是否为与 AVHDD1022 对应的记录媒体。

又，也可以不判断第 3 记录媒体 1030 是否为与 AVHDD1022 对应的记录媒体后移动数据，而判断存档设备 1023 是否为与 AVHDD1022 对应的装置后移动数据。此时，在 AVHDD1022 中，设置判断存档设备 1023 是否为与 AVHDD1022 对应的装置的判断手段，当由该判断手段判断存档设备 1023 是与 AVHDD1022 对应的装置时，移动手段 1027 也可以将未加密数据的或加密后的复制禁止数据移动到存档设备 1023。

又，当存档设备 1023 具有表示是否为与 AVHDD1022 对应的装置的密钥时，设置在 AVHDD1022 的判断手段也可以利用存档设备 1023 所具有的密钥，判断存档设备 1023 是否为与 AVHDD1022 对应的装置。

又，当确认在连接 AVHDD1022 与存档设备 1023 的接口上具有能够至少对复制禁止数据的移动进行收费的管理装置时，AVHDD1022 的移动手段 1027 也可以将该复制禁止数据移动到存档设备 1023。又，作为管理装置的一示例，可以举出有 STB。

又，在第 8 实施形态以及 2 的各 AVHDD 中，也可以设置在进行数据移动时将该数据移动的收费信息发送到管理各 AVHDD 的管理装置的手段。又，作为管理装置的一示例，可以采用加入进行收费的手段的 STB1003。

又，在上述的实施形态中，是从 AVHDD 向存档设备移动复制禁止数据。即，在将复制禁止数据移动到存档设备之后，从 AVHDD 中删去复制禁止数据。然而，由于考虑到在存档设备中不能够处理复制禁止数据，故有的情况下最好将复制禁止数据作为备份保留在 AVHDD 中。

此时，若将上述实施形态的 AVHDD 的移动手段 1027 置换成将复制禁止数

据复制到存档设备的复制手段，则在向存档设备发送复制禁止数据的同时，在 AVHDD 内能够备份存储复制禁止数据，它的优点是，即使在存档设备中不能够处理复制禁止数据的情况下，也能够利用备份存储在 AVHDD 中的复制禁止数据。

这里，作为具备复制手段的 AVHDD 结构的一示例，是将图 24 所示的具备移动手段 1007 的 AVHDD1022 置换成替代移动手段 1027 而具备复制手段 1090 的 AVHDD1091，作为示例将其示于图 29 中。

(第 10 实施形态)

其次，对于本发明的第 10 实施形态的加密数据解密记录系统进行说明。

图 30 表示该第 10 实施形态的加密数据解密记录系统的结构。如图 30 所示，该第 10 实施形态的加密数据解密记录系统由 5 个记录装置 1100a～1100e、解密记录装置 1101 构成。

图 31 表示该第 10 实施形态中各记录装置 1100 的结构。如图 31 所示，各记录装置 1100 具有记录手段 1102、输出记录在该记录手段 1102 中的数据的输出手段 1103。这里，记录在记录手段 1102 中的数据是将禁止复制的复制禁止数据加密后的数据，在各记录装置 1100 的记录手段 1102 中记录有相同内容的加密后的复制禁止数据。

其次，图 32 中表示第 10 实施形态中解密记录装置 1101 的结构。如图 32 所示，解密记录装置 1101 具有解密手段 1104、记录手段 1105。这里，解密手段 1104 是将从记录装置 1100 输出的加密后的复制禁止数据解密的手段，记录手段 1105 是记录与记录在记录装置 1100 中的复制禁止数据相同内容的数据即加密后的复制禁止数据或未加密的复制禁止数据的手段。

然而，在上述本第 10 实施形态的加密数据解密记录系统中，相同内容的数据分别记录在 5 个记录装置 1100a～1100e 以及解密记录装置 1101 中，而加密后的复制禁止数据只能由解密记录装置 1101 的解密手段 1104 来解密。

因此，当采用该第 10 实施形态的加密数据解密记录系统时，它呈现的效果是在保护著作权的同时，能够将要保护著作权的数据进行备份。

又，上述实施形态的加密数据解密记录系统是具备记录装置 1100a～1100e，而记录装置 1100 的个数并不限定于 5 个。总之，也可以存在多个。

(第 11 实施形态)

其次，对于本发明第 11 实施形态的 AVHDD1032 进行说明。又，在第 11 实施形态中，将对来自 AVHDD1032 的数据的发送情况进行叙述，而使得发送来的

数据记录在 DVD 装置 1033 的 DVD1037 中。

在图 26 中表示本发明第 11 实施形态的 AVHDD1032 以及 DVD 装置 1033 的框图。

另外，本发明的第 11 实施形态的 AVHDD1032 如图 26 所示，由存储数据的存储手段 1034、将存储在存储手段 1034 中的数据发送到 DVD 装置 1033 的发送手段 1035 构成。

本发明第 11 实施形态的 DVD 装置 1033 如图 26 所示，由将来自 AVHDD1032 的数据记录到 DVD1037 的第 5 记录手段 1036、重放记录在第 5 记录手段 1036 中的数据的重放手段 1038 构成。

又，在第 11 实施形态中，作为本发明的数据发送装置的一示例，采用 AVHDD1032。

又，AVHDD1032 与 DVD 装置 1033 的连接也可以通过任何接口进行连接。

其次，对于本发明第 11 实施形态的 AVHDD1032 以及 DVD 装置 1033 的动作进行叙述。

这里，将 AVHDD1032 发送的数据作为由数个数据包构成的数据流。在图 27 中表示该数据流的一部分的结构。数据流是由多个如图 27 所示的由 D0、D1、D2、D3、D4 这 5 个数据包所构成的块构成的数据流，D0、D1、D2、D3、D4 分别是以数字逐渐变大的顺序时间上连续的数据包，即若时间上的前一数据没有重放就不能够重放的连锁加密的数据。

因此，当取出数据包 D0、D1、D2 时，数据包 D0 时间上后续的是数据包 D1，其次接着的是数据包 D2，若没有重放数据包 D0，就不能够重放数据包 D1，若没有重放数据包 D1，就不能够重放数据包 D2。

这样的数据流是与由 AVHDD1032 发送到 DVD 装置 1033 时的动作有关，而 AVHDD1032 的发送手段 1035 将存储在存储手段 1034 中的数据流发送到 DVD 装置 1033 时，将构成数据流的各块的数据包以 D4、D3、D2、D1、D0 的顺序进行发送。

在 DVD 装置 1033 中，第 5 记录手段 1036 将来自 AVHDD1032 的数据记录到 DVD1037。

当重放记录在 DVD1037 中的数据时，重放手段 1038 对于构成数据流的各块，以 D0、D1、D2、D3、D4 的顺序不断重放数据包，这样重放整个数据流。

如此，由于从 AVHDD1032 发送到 DVD 装置 1033 的数据包以 D4、D3、D2、

D1、D0 的顺序被发送，故即使在数据发送的途中因停电等而电源切断的情况下，由于若没有发送 D4、D3、D2、D1、D0，则不重放由 D4、D3、D2、D1、D0 构成的块，故即使当发送数据泄漏到其它装置的情况下，也能够避免在其他装置中解读该发送数据的情况。

又，在上述实施形态中，对于数据包 D0、D1、D2、D3、D4 的连锁加密并没有进行详细叙述，这里可以将连锁加密的数据包 D0、D1、D2、D3、D4 存储到 AVHDD1032 的存储手段 1034 中，也可以在 AVHDD1032 中设置进行连锁加密的手段，在 AVHDD1032 的发送手段 1035 要发送数据流时，分别对于各块的数据包进行连锁加密。

又，在上述实施形态中，数据流是由多个由 D0、D1、D2、D3、D4 这 5 个数据包构成的块构成，但构成各块的数据包的个数并不限定于 5 个。又，数据流也并不局限于由多个块构成。数据流可以不由多个块构成而由多个数据包构成。此时，发送手段 1035 将构成数据流的数据包从最末尾到最前面依次进行发送。

又，在上述实施形态中，是对于数据流的发送进行了说明，而移动数据流的情况下，若来看数据包 D0、D1、D2、D3、D4，出可以在数据包 D4、D3、D2、D1 传送结束之后，从移动前的记录媒体中删去数据包 D1~D4，在完成删去之后，传送数据包 D0，再从移动前的记录媒体中删去数据包 D0。

又，在以上第 8~第 11 实施形态中，是将 CCI 的值为禁止复制、许可复制一次、禁止再次复制的任意一种 AV 数据都统一称为复制禁止数据，而在以下第 12~第 16 实施形态中，将 CCI 为复制禁止的 AV 数据等被禁止进行复制的内容称为复制禁止内容。

(第 12 实施形态)

图 33 是表示本发明第 12 实施形态的记录重放装置的结构图。如图所示，判别信息检测手段 2010 是从外部的广播信号中检测出与复制限制相关的判别信息用的手段，时间信息取得手段 2011 是从外部的广播信号中取得与时间相关的时间信号用的手段，记录重放手段 2010 是记录重放来自外部的广播信号用的手段，记录媒体 2013 是通过硬盘等实现的、能够同时进行记录重放并且随机可存取的、存储广播数据用的手段，控制输入接口(以下称为控制输入 I/F)2015 是接收来自用户的控制的手段，切换手段 2016 是接收来自记录重放手段 2012 的输入与来自外部的广播输入并且选择其中之一输出到外部的显

示器等的手段。又，在记录媒体 2013 中，记录缓冲器 2014 是记录复制受到限制的数据所专用的区域。又，在本实施形态中所涉及的广播是采用 MPEG 传输流或者 MPEG 程序流(以下总称为 MPEG 数据流)的数字广播，省略有关解码处理的手段等。以下，各实施形态也都相同。又，判别信息检测手段 2010、时间信息取得手段 2011、记录重放手段 2012 是本发明的记录手段的一示例。

以下，对于具有上述结构的本发明第 12 实施形态的记录重放装置的动作进行说明。

首先，判别信息检测手段 2010 从外部接收 MPEG 数据流的输入，参照首部或者构成数据串的各数据包，检测出复制保护或者 CCI(Copy Control Information，复制控制信息)等有关著作权的信息，判断输入的内容是否为复制禁止或者复制受限制的内容。这里，设仅输入复制禁止的复制禁止内容的情况。

其次，当判断输入的 MPEG 数据流为复制禁止内容时，判别信息检测手段 2010 向记录重放手段 2012 输出检测信息。作为检测信息的示例，有包含在 MPEG 数据流中的著作权信息、复制保护等。记录重放手段 2012 当接收检测信息时，根据该信息，准备将 MPEG 数据流记录到记录媒体 2013 内的记录缓冲器 2014。

当从外部通过判别信息检测手段 2010 输入 MPEG 数据流时，记录重放手段 2012 将其记录到记录缓冲器 2014。

其次，对于记录重放手段 2012 向记录缓冲器 2014 的记录动作的进行详细说明。图 34 是用于说明本第 12 实施形态的记录重放装置动作的时序图。如图所示，作为本实施形态的动作示例，是采用对于记录缓冲器 2014 暂时记录相当于广播时间 90 分钟的数据量的本实施形态的记录重放装置，对于实况广播期间 2020 所广播的广播时间 120 分钟的复制禁止内容，在从广播开始时刻起经过 90 分钟后通过转录重放进行收视。

首先，当到达广播开始时刻，记录重放手段 2012 开始向记录缓冲器 2014 记录构成复制静止内容的数据。在广播开始时刻以后，记录重放手段 2012 向记录缓冲器 2014 连续地逐次记录数据，而不进行重放。

另一方面，时间信息取得手段从 MPEG 数据流中取得 PCR 数据包以及时间标记等时间信息，从记录重放手段 2012 将复制禁止内容开始记录到记录缓冲器 2014 的时刻起，开始测量记录时间。

其次，从广播开始时刻起，根据时间信息取得手段 2011 的测量，经过记

录期间 2021(90 分钟)时, 记录重放手段 2012 继续逐次记录从外部输入的 MPEG 数据流, 同时, 从记录缓冲器 2014 上开始删去广播开始时刻以后记录的数据。然而, 在本次动作示例中, 从广播开始时刻起经过记录期间 2021 的时刻, 由于为利用转录重放的收视期间 2024 开始的收视开始时刻, 故记录重放手段 2012 在删去所记录的数据之前进行重放, 并通过切换手段 2016 输出到外部监视器。

即, 在记录期间 2021 中所记录的数据中, 相当于最初 30 分钟的部分 2022a 的数据(实况广播期间 2020a 中广播的内容)在从广播开始时刻起经过 90 分钟之后, 与利用转录重放的收视开始时刻同时进行重放(利用转录重放的收视期间 2024a 中所收视的内容), 此后立即删去。

其次, 从利用转录重放的收视开始时刻起, 当经过记录重放期间 2022a 时, 记录重放手段 2012 作为记录重放期间 2022b, 直到广播结束时刻继续进行数据的逐次记录, 同时继续连续地从数据部分 2022a 重放已经存储在记录缓冲器 2014 内的数据。

其次, 当到达广播结束时刻, 记录重放手段 2012 停止逐次记录数据, 重放记录在缓冲器 2014 中的数据(重放期间 2023), 直到收视结束时刻为止。

又, 对于上述动作, 也可以在记录重放期间 2022b 以及重放期间 2023 中, 将重放的数据暂时保存在记录缓冲器 2014 中, 在经过收视结束时刻之后一并删去, 但在由于事故而切断记录重放装置电源等的情况下, 为了防止数据保存在记录媒体 2013 上的情况, 最好能够在重放后立即删去。

又, 在即使经过收视开始时刻也没有进行转录重放时, 记录重放手段 2012 将记录在记录缓冲器 2014 中的所有数据删去。由此, 能够防止以转录以外的形式重放复制禁止内容。

又, 在上述说明中, 是对于当判别信息检测手段 2010 检测出包含在复制禁止内容的数据中的判别信息时, 记录重放手段 2012 自动地开始转录重放用的记录动作的情况作了说明, 而记录重放手段 2012 的记录动作也可以不根据判别信息而开始, 而是根据通过控制输入 I/F2015 来自外部(用户)侧的控制进行。

又, 在以上的说明中, 是将记录期间 2021 的结束与利用转录重放所进行的收视开始时刻设定为相同时刻, 并且使得复制禁止内容的转录重放动作与构成该复制禁止内容的数据的删去动作连动地进行, 但并不局限于此, 也可以如图 35 所示那样, 只要收视开始时刻在记录期间 2021 内(能够将转录重放设定

为任意时刻的期间 2024c)，就根据来自控制输入 I/F2015 的控制设定为任意的时刻，也可以不设定时刻而根据提供给记录重放手段 2012 的直接命令进行。此时，在记录期间 2021 内若没有对记录重放手段 2012 提供转录重放的直接命令时，记录重放手段 2012 最好使其停止记录动作(图 35 中的期间 2021a)。又，同时，即使再次执行转录重放的直接命令时，最好设定为不接收该命令的状态。

又，在以上的动作中，说明的是当经过记录期间 2021 时，记录重放手段 2012 继续逐次记录从外部输入的 MPEG 数据流，同时，从记录缓冲器 2014 中删去在广播开始时刻以后记录的数据，但也可以在不能够重放的状态下，在重写该数据之后，将数据保存在记录缓冲器 2014 上。

(第 13 实施形态)

本发明第 13 实施形态的记录重放装置是采用环形缓冲器作为记录复制禁止内容用的记录缓冲器。

图 36 是表示本发明第 13 实施形态的记录重放装置的结构图。在该图中，对于与图 33 相同的或相当的部分采用同样的符号并省略说明。又，环形缓冲器 2044 是通过在同一区域中反复进行重写记录而暂时记录一定量数据的手段。

对于具有上述结构的本发明第 13 实施形态的记录重放装置，以下，对其动作进行说明。

首先，关于判别信息检测手段 2010 参照外部的 MPEG 程序流，记录重放手段 2012 将复制禁止内容记录到环形缓冲器 2044 的动作，与第 12 实施形态相同地进行。

其次，对于利用记录重放手段 2012 向环形缓冲器 2044 的记录动作进行详细说明。如上所述，环形缓冲器 2044 是记录媒体 2013 上的特定区域，当记录一定量的数据时，则返回记录开始位置并进行重写。此时，可以预先设定环形缓冲器 2044 的大小，也可以根据从判别信息检测手段 2010 取得的检测信息进行设定，但不管哪一种情况下，都是将环形缓冲器 2044 的大小设定为不能够完全记录成为记录对象的复制禁止内容。例如，若设复制禁止内容的广播时间为 120 分钟，则将环形缓冲器 2044 设定为相当于 90 分钟的容量。

对于上述这样设定的环形缓冲器 2044，记录重放手段 2012 开始记录复制禁止内容。

这里，图 37 是用于说明该第 13 实施形态中的记录重放装置动作的时序图。以下，参照图 37，对于该第 13 实施形态的记录重放手段 2012 与环形缓冲器

2044 的动作进行详细说明。且，如图所示那样，本实施形态的动作示例的各时刻、各时间的设定，与图 34 所示的第 12 实施形态的情况相同。

首先，当达到广播开始时刻时，记录重放手段 2012 向环形缓冲器 2044 开始记录构成复制禁止内容的数据。在广播开始时刻之后，记录重放手段 2012 向环形缓冲器 2044 继续逐次记录数据，直到设定的容量满了为止，而不进行重放（记录期间 2051）。

其次，从广播开始时刻起经过记录期间 2051，当环形缓冲器 2044 所设定的容量满了，则记录重放手段 2012 在环形缓冲器 2044 上，使得记录头（环形缓冲器指针）从记录期间 2051 时刻的记录位置返回记录开始位置，并且进行新的数据的重写记录。

又，在本次动作示例中，由于记录期间 2051 的结束是与通过转录重放的收视期间 2054 的开始时间相同，故记录重放手段 2012 在对从外部输入的 MPEG 数据流进行重写记录的同时，开始重放从广播开始时刻起记录的、就要重写之前的数据。即，在记录期间 2051 已经记录的数据中的、相当于最初 30 分钟部分 2052a 的数据（在实况广播期间 2050a 广播的内容）从广播开始时刻起经过 90 分钟后，与利用转录重放的收视开始时刻同时进行重放，并且通过重写记录而删去。

接着，记录重放手段 2012 继续进行数据的逐次记录直到广播结束时刻，并同时继续进行数据的重放（记录重放期间 2052b）。

其次，当达到广播结束时刻，记录重放手段 2012 停止数据的重写记录，并对记录在环形缓冲器 2044 中的数据进行重放（重放期间 2053），直到收视结束时刻为止。

又，在上述动作中，从环形缓冲器 2044 重放的数据也可以暂时保存在环形缓冲器 2044 中，在收视结束时刻经过之后一并删去，但为了防止因事故而切断记录重放装置电源等原因使数据保存到记录媒体 2013 上的情况，最好在重放之后立即删去。

又，在即使经过收视开始时刻也没有进行转录重放时，记录重放手段 2012 删去记录在环形缓冲器 2044 中的所有的数据。由此，能够防止以转录以外的形式重放复制禁止内容。

又，在以上的动作中，说明的是将记录期间 2051 的结束与利用转录重放的收视开始时刻设定为相同时刻，并且使得复制禁止内容的转录重放动作与构

成该复制禁止内容的数据的重写记录动作连动，但并不局限于此，也可以如图 38 所示，收视开始时刻只要在记录期间 2061 内（能够将转录重放设定为任意时刻的期间 2064c），则根据来自控制输入 I/F2015 的控制，设定为任意的时刻，也可以不设定时刻而根据对于记录重放手段 2012 的直接命令执行。此时，在记录期间 2061 内，当没有对记录重放手段 2012 提供转录重放的直接命令时，最好使得记录重放手段 2012 停止记录动作（图中的期间 2061a）。又，同时，最好设定为，即使再次发出转录重放的直接命令也不接收的状态。

又，在上述动作中，说明的是当经过记录期间 2061 时，记录重放手段 2012 继续逐次记录从外部输入的 MPEG 数据流并且同时从记录缓冲器 2014 上删去在广播开始时刻以后记录的数据，但也可以在不能够重放的状态下重写该数据并且将数据保持在记录缓冲器 2014 上。

又，在本实施形态的转录重放中，对于重放数据时的环形缓冲器上的记录位置，(1)使得在环形缓冲器 2044 上没有进行重写记录状态下的重放位置与环形缓冲器 2044 上开始记录的位置相同，(2)使得进行重写记录的状态下的重放位置在环形缓冲器 2044 上处于在进行重放动作控制时刻的位置（最后进行重写记录的位置）之后。即，在上述(1)、(2)的任何一种情况下，使得转录重放是从记录在环形缓冲器 2044 中的最早的数据开始依次读出。在图 38 所示的示例中，上述(1)是相当于在期间 2064d（广播开始时刻之后 30 分钟）内进行转录重放的情况，重放开始位置通常惟一决定为图中点 A。上述(2)相当于在期间 2064e（广播开始时刻 30 分钟经过之后 60 分钟为止）内进行转录重放的情况，重放开始位置相当于期间 2064e 上的环形缓冲器的记录头（缓冲器指针）的当前位置。

（第 14 实施形态）

本发明第 14 实施形态的记录重放装置是在接收混合了复制禁止内容与可复制内容的广播时，使其能够选择性地仅对复制禁止内容进行转录重放。

由于本实施形态的结构与第 12 实施形态相同，故在说明中参照图 33。又，图 39 是用于说明本实施形态的记录重放装置的动作。并且，在本实施形态中，将能够转录的时间设定为 120 分钟而并非为上述实施形态的 90 分钟。以下，参照图 39 对于本发明的实施形态的动作进行说明。

从外部输入的 MPEG 数据流 2070 混合了禁止复制的复制禁止内容 2070a 以及 2070c、与能够复制的通常的内容 2070b 以及 2070d，按时间序列顺序，以

复制禁止内容 2070a、内容 2070b、复制禁止内容 2070c、内容 2070d 的顺序输入记录重放装置。判别信息检测手段 2010 获得包含在各内容的判别信息并输出到记录重放手段 2012，时间信息取得手段将每个内容的时间信息输出给记录重放手段 2012。取得了判别信息以及时间信息的记录重放手段 2012，根据这些信息，在每经过各内容的广播时间，将复制禁止内容暂时记录到记录缓冲器 2014 并且将通常的内容记录到记录媒体 2013 内的记录缓冲器之外的记录区域。

此时，由于内容的输入为时间序列顺序，故如图 39 所示，在记录缓冲器 2014 中，首先记录复制禁止内容 2070a，接着记录复制禁止内容 2070c，在记录媒体 2013 中，首先记录内容 2070b，接着记录内容 2070d。

与第 12 实施形态相同，依次转录重放记录在记录缓冲器 2014 内的复制禁止内容 2070a 以及 2070c。在转录重放结束之后，从记录缓冲器 2014 中删去数据或者使其成为不能够进行重放的状态，而能够使得记录在记录媒体 2013 内的内容 2070b 以及 2070d 长久地保持下来。

又，在上述说明中，本实施形态是对于由具有第 12 实施形态结构的记录重放装置来实现的情况作了说明，而在为第 13 实施形态的结构的情况下，也能够同样地进行。

(第 15 实施形态)

本发明第 15 实施形态的记录重放装置是将暂时记录的复制禁止内容的数据加密并且使其成为不能够收视的状态。

图 40 是表示本发明第 15 实施形态的记录重放装置中所使用的数据加密手段 2080 的结构图。如图所示，记录缓冲器 2014 是与第 12 实施形态的记录缓冲器相同的手段，加密手段 2081 是通过时变密钥将从记录重放手段 2012 输入的数据加密的手段，解码手段 2082 是将从记录缓冲器 2014 输出的加密后的数据解密的手段，时变密钥生成手段 2083 生成加密手段 2081 以及解密手段 2082 中所使用的时变密钥的手段，密钥缓冲器 2084 是暂时存储时变密钥的手段。

以下，对于具有上述构造的本实施形态的动作进行说明。当从记录重放手段 2012 向加密手段 2081 输入数据时，加密手段 2081 根据时变密钥生成手段 2083 生成的时变密钥将原数据加密。将加密后的数据记录到记录缓冲器 2014 中。

另一方面，时变密钥生成手段 2083 将与加密手段 2081 取得的相同的时变密钥输出到密钥缓冲器 2084，将其存放在密钥缓冲器 2084 中。

其次，在记录重放手段 2012 进行转录重放，从记录缓冲器将加密后的数据输出到解密手段 2082 时，解密手段从密钥缓冲器 2084 获得数据解密所必须的数据，对该数据进行解密。

在上述动作中，使得暂时存放时变密钥的密钥缓冲器，当超过与记录缓冲器 2014 数据容量的时间部分相同的时间部分时消失。由此，没有进行转录重放的数据在加密的状态下原样地保持在记录缓冲器 2014 内，即使能够重放，也不能够进行收视。

为了删去时变密钥，例如，可以使得密钥缓冲器 2084 为环形缓冲器结构，通常通过新的密钥来重写存储在密钥缓冲器中的密钥。作为环形缓冲器的容量，例如，若为图 34 所示的第 12 实施形态的动作示例，则使得与记录期间 2021 相同。

又，也可以另外设置计时器进行计时，当经过规定时刻时，从密钥缓冲器 2084 逐次删去设定时刻以后的密钥。

又，当由易失性存储器构成密钥缓冲器 2084 时，当切断记录重放装置的电源时，删去密钥缓冲器内的所有密钥，由此，也能够确保保密性。

(第 16 实施形态)

本发明第 16 实施形态的记录重放装置是使得能够向用户告知转录重放的时刻。

图 41 是本发明第 16 实施形态的记录重放装置的结构图。在该图中，对于与图 33 相同的部分或者相当的部分，采用同一符号并省略说明。又，告知手段 2091 是通过声音、图像或者文字信息告知该记录重放装置的动作状态的手段。

又，图 42 是用于说明本实施形态的记录重放装置的动作。对于具有上述结构的本发明第 16 实施形态的记录重放装置，以下对其动作进行说明。并且，使得记录缓冲器 2014 中设定的容量与第 12 实施形态相同，即相当于广播时间 90 分钟的容量，关于其他与第 12 实施形态重复的动作则省略说明，仅对不同点作叙述。

首先，用户通过实况广播收视从广播台广播的复制禁止内容，下面研究在时刻 t 由于某种原因而暂时中断收视的情况。此时，用户从控制输入 I/F2015 进行输入，并使得记录重放手段 2012 起动。记录重放手段 2012 从接收来自控制输入 I/F2015 的输入的时刻起(与时刻 t_1 相同)，开始向记录缓冲器 2014 记

录该复制禁止内容。另一方面，在此之间，记录重放装置为“暂停”状态。

在记录缓冲器 2014 中，与第 12 实施形态的动作相同，不断记录复制禁止内容的数据，而当为时刻 t_2 时，对用户发出报警声并督促用户注意对记录重放装置的控制。在本实施形态中，对于时刻 t_2 ，设定为从时刻 t_1 起记录重放手段 2012 记录在记录缓冲器 2014 的数据之中的、到达设定容量为止的剩余量（广播时间单位），在本实施形态中使该时刻 t_2 为（以广播时间单位）5 分钟。因此，时刻 t_2 具体为（记录开始（暂停开始）时刻 +85 分钟（暂时记录到记录缓冲器的复制禁止内容的数据量 -5 分钟））。

通过来自告知手段 2091 的通报，用户从控制输入 I/F2015 进行输入并解除暂停，重新开始复制禁止内容的收视。与暂停前不同点在于，用户收视的复制禁止内容不是来自广播台的实况广播而是从记录缓冲器 2014 被转录重放的内容。

此时，由于从时刻 t_2 到时刻 t_1 之间为暂停，用户收视节目结束时刻 t_6 ，比实际的广播结束时刻 t_4 延迟该 (t_2-t_1) 的时间。

又，若在该动作中从时刻 t_2 起进行转录重放，则在从广播台广播节目的期间，虽然暂时记录在记录缓冲器 2014 中的内容结束了重放，而从该重放结束时刻 t_7 起到节目收视结束时刻 t_6 为止，在记录缓冲器 2014 中，进行数据的记录重放，同时，重放后的节目数据以不能够收视的状态保存或者删去。

另一方面，即使经过时刻 t_2 也没有从用户向控制输入 I/F2015 进行输入的情况下，对于记录缓冲器 2014，在完全记录了设定时间部分的数据的时刻 t_3 ，停止向记录缓冲器 2014 进行暂时记录的动作，同时，强制开始转录重放。在本实施形态中，从告知手段 2091 进行了告知的时刻 t_2 起经过 5 分钟后的时刻 t_3 相当于该时刻。在该动作中，从时刻 t_3 起，仅延迟开始暂停的时刻 t_1 的差，节目就进行转录重放，用户结束节目收视的时刻 t_5 比实际的广播结束时刻 t_4 仅延迟上述的 (t_3-t_1) 的部分。又，该 (t_3-t_1) 的部分，与开始对记录缓冲器 2014 设定的复制禁止内容的记录时间相同。再者，时刻 t_3 之后的广播不再记录到记录缓冲器 2014 中。因此，从强制转录重放的结束时刻 t_8 起到节目收视结束时刻 t_5 为止的期间，用户收视已经结束广播节目之后广播的其他节目，或者转录重放的结束时刻 t_8 依旧为用户的收视时刻。

即，若经过时刻 t_2 从用户也没有输入转录重放，而一旦暂时强制地开始转录重放，则用户在暂停解除后不能够完整地收视从暂停前开始收视的节目。

如上所述，根据本实施形态，用户能够设定在所要求的时间对复制禁止内容进行转录重放，同时为了保护复制禁止内容的著作权，能够督促用户进行完整的转录重放，直到经过规定时间为止。

又，在上述实施形态中，是对于采用记录缓冲器 2014 的示例进行了说明，而替代记录缓冲器 2014，采用第 13 实施形态的环形缓冲器 2044 也可以获得相同的效果。采用环形缓冲器 2044 时的动作如图 42 的点划线所示，在从时刻 t_4 到 t_3 为止的期间，在环形缓冲器即记录缓冲器中，继续进行数据的重写记录，并且同时进行重放，由此，能够进行缓冲器所设定的时间部分的转录重放。这里，设定使得在时刻 t_3 禁止重写动作时的动作，与上述通常的记录缓冲器强制实行转录重放时的动作相同。

又，本实施形态的结构也可以采用与上述第 14 实施形态相组合的结构。

再者，在上述各实施形态中，是对于将本发明的记录装置与重放手段一体化的记录重放手段向记录缓冲器进行记录以及重放的情况作了说明，但本发明的结构并不局限于此，也可以仅具备进行记录的记录手段，将从记录缓冲器 2014 或者环形缓冲器 2044 重放数据的手段作为外部设备而另外设置。

再者，在上述各实施形态中，复制禁止内容的记录期间等是作为时间信息，通过对内容的 MPEG 数据流内中 PCR 数据包进行计数来进行测量，但时间信息并不局限于此，作为其他的时间信息也可以采用 EPG，并参照取得的 EPG 根据另外设置的计时器进行绝对时间的测定，由此进行测量。

再者，也可以由记录媒体 2013 测量该时间信息。

再者，该时间信息也可以在向本发明实施形态的记录重放装置输入 MPEG 数据流的 STB 等的设备内进行测量，与 MPEG 数据流同时输入。再者，这些时间信息也可以包含作为暂时记录对象的内容其广播开始时刻等。

再者，在上述各实施形态中，是对于将复制禁止内容作为由一次都不允许复制的数据所构成的内容作了说明，但本发明的复制限制内容并不局限于此，也可以将由仅许可复制一次的数据所形成的内容作为对象。总之，对于附加有复制禁止或规定限制的数据，本发明都可以采用。

又，在本发明的说明书中，还记载关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手

段，以使得所述记录手段重放所述复制许可信息，所述解密手段生成包含所述装置惟一密钥与所述复制许可信息中的至少一个的第1信息，所述解密手段采用所述记录单元信息生成将所述第1信息解密后的信息即内容密钥，所述解密手段采用所述内容密钥将所述数据解密。

又，在本发明说明书中，还记载了关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述加密后的标题密钥解密。

又，在本发明的说明书中，还记载了关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述解密手段采用所述标题密钥将所述数据解密。

又，在本发明的说明书中，还记载了关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述重放后的标题密钥解密，所述解密手段生成包含所述标题密钥的第3信息，所述解密手段采用记录单元信息生成将所述第3信息解密后的信息即内容密钥，该记录单元信息是将所述控制手段连续访问所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述解密手段采用所述内容密钥将所述数据解密。

又，在本发明的说明书中，还记载了关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述解密手段采用所述复制许可信息将所述数据解密。

又，在本发明的说明书中，还记载了关于一种重放装置的发明，其特征在

于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述加密后的标题密钥，所述解密手段采用所述装置惟一密钥将所述重放后的标题密钥解密，所述控制手段控制所述记录手段以使得所述记录手段重放所述复制许可信息，所述解密手段生成包含所述标题密钥与所述复制许可信息中的至少一个的第2信息，所述解密手段采用记录单元信息生成将所述第2信息解密后的信息即内容密钥，该记录单元信息是将所述控制手段连续访问所述记录手段的最小单位即记录单元为前提的记录块所固有的编号以及/或者记号，所述解密手段采用内容密钥将所述数据解密。

又，在本发明的说明书中，还记载了关于一种重放装置的发明，其特征在于，具备：进行控制以使得重放由上述本发明的记录装置记录在盘片上的加密后的数据的控制手段；由所述控制手段控制并重放所述数据的重放手段；以及将所述重放后的数据解密并送至接口的解密手段，所述控制手段控制所述记录手段，以使得所述记录手段重放所述复制许可信息，所述解密手段采用所述重放后的复制许可信息将所述数据解密。

又，在本说明书中，还记载了关于一种媒体的发明，它是装有通过计算机实现上述本发明的全部或一部分手段的全部或一部分功能用的程序以及/或者数据的媒体，由计算机可读取并且读取的所述程序以及/或者数据能够与所述计算机连动地实行所述功能。

又，在本说明书中，记载了关于一种信息集合体的发明，它是利用计算机实现上述本发明的全部或部分手段的全部或一部分功能的程序以及/或者数据，由计算机可读取并且读取的所述程序以及/或者数据能够与所述计算机一起执行所述功能。

再者，所谓数据包含数据结构、数据格式、数据的种类等。

再者，所谓媒体包含 ROM 等记录媒体、网络等传送媒体、光·电波·声波等传送媒体。

再者，所谓进行存储的媒体包含例如记录了程序以及/或者数据的记录媒体、以及传送程序以及/或者数据的传送媒体等。

再者，所谓由计算机可处理是包含下述情况，例如若为 ROM 等记录媒体的情况下，是由计算机可读取，若为传送媒体的情况下，是由计算机可获得作为

传送结果的作为传送对象的程序以及/或者数据。

再者， 所谓信息集合体是指例如包含了程序以及/或者数据等的软件的集合体。

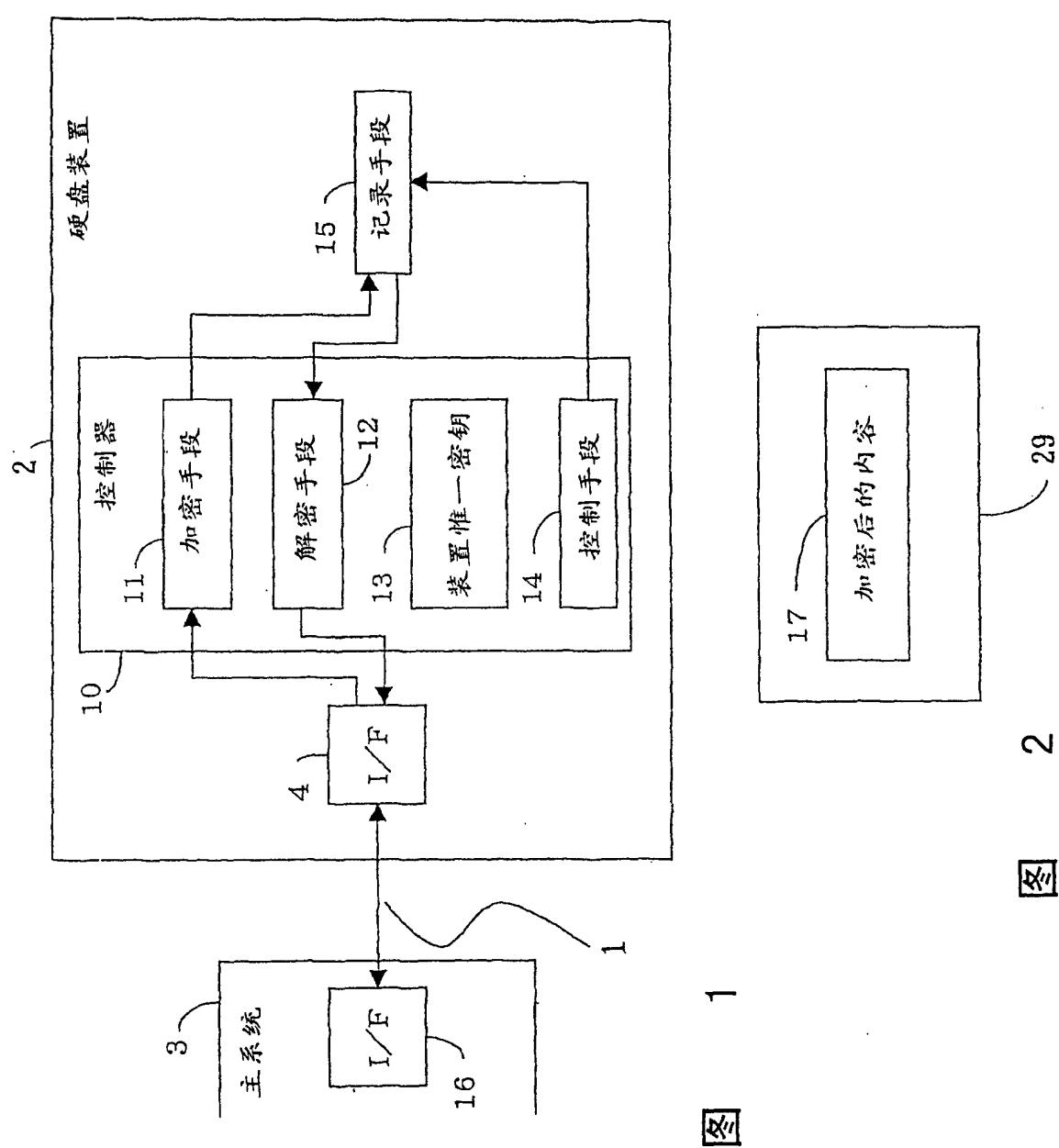
再者， 如上所述， 本发明的结构可以由软件实现， 也可以由硬件实现。

工业利用性

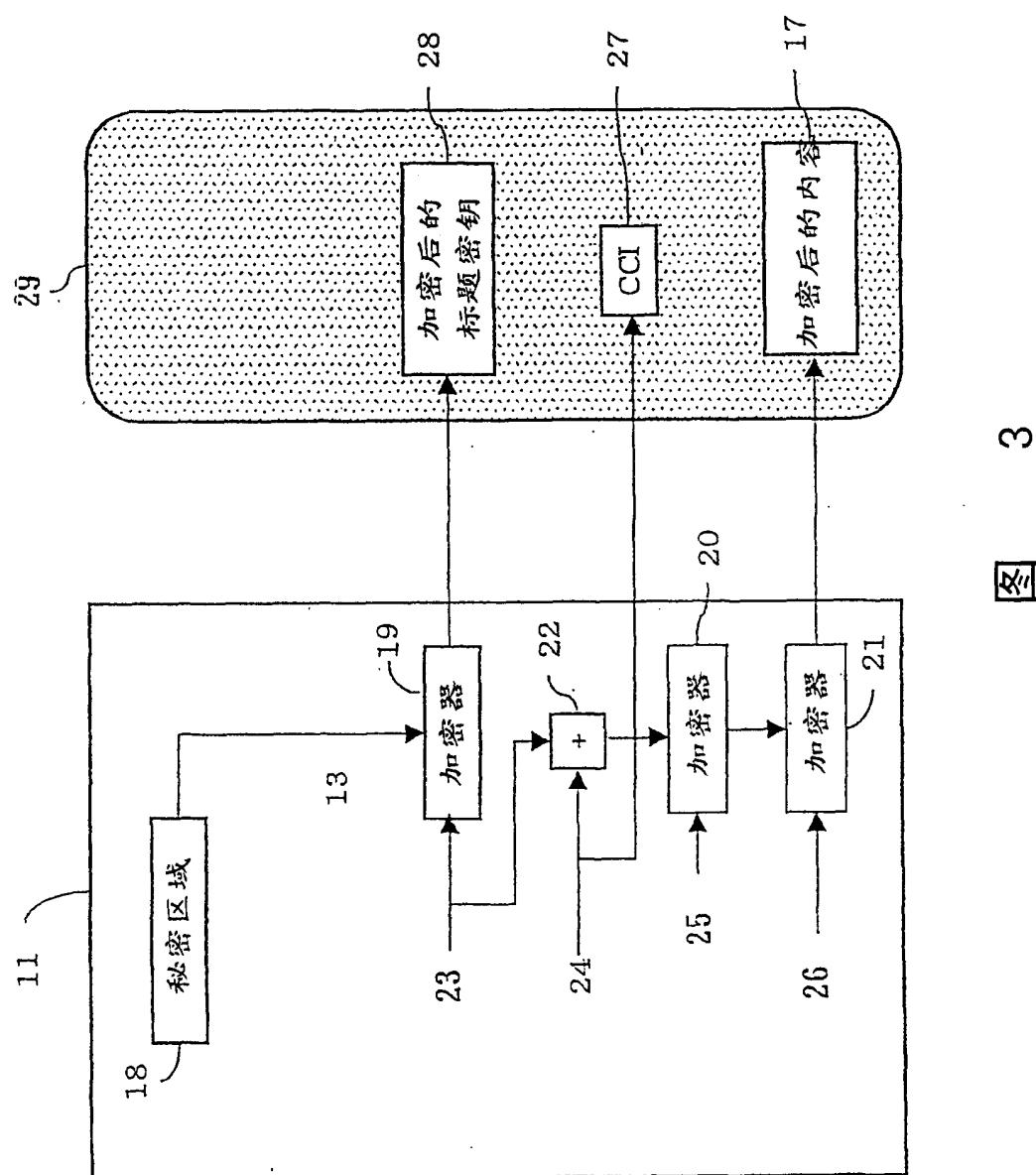
如上述说明可知， 本发明能够提供一种在记录必须保护著作权的数据时以及/或者重放必须保护著作权的数据时能够保护著作权的记录装置以及重放装置。

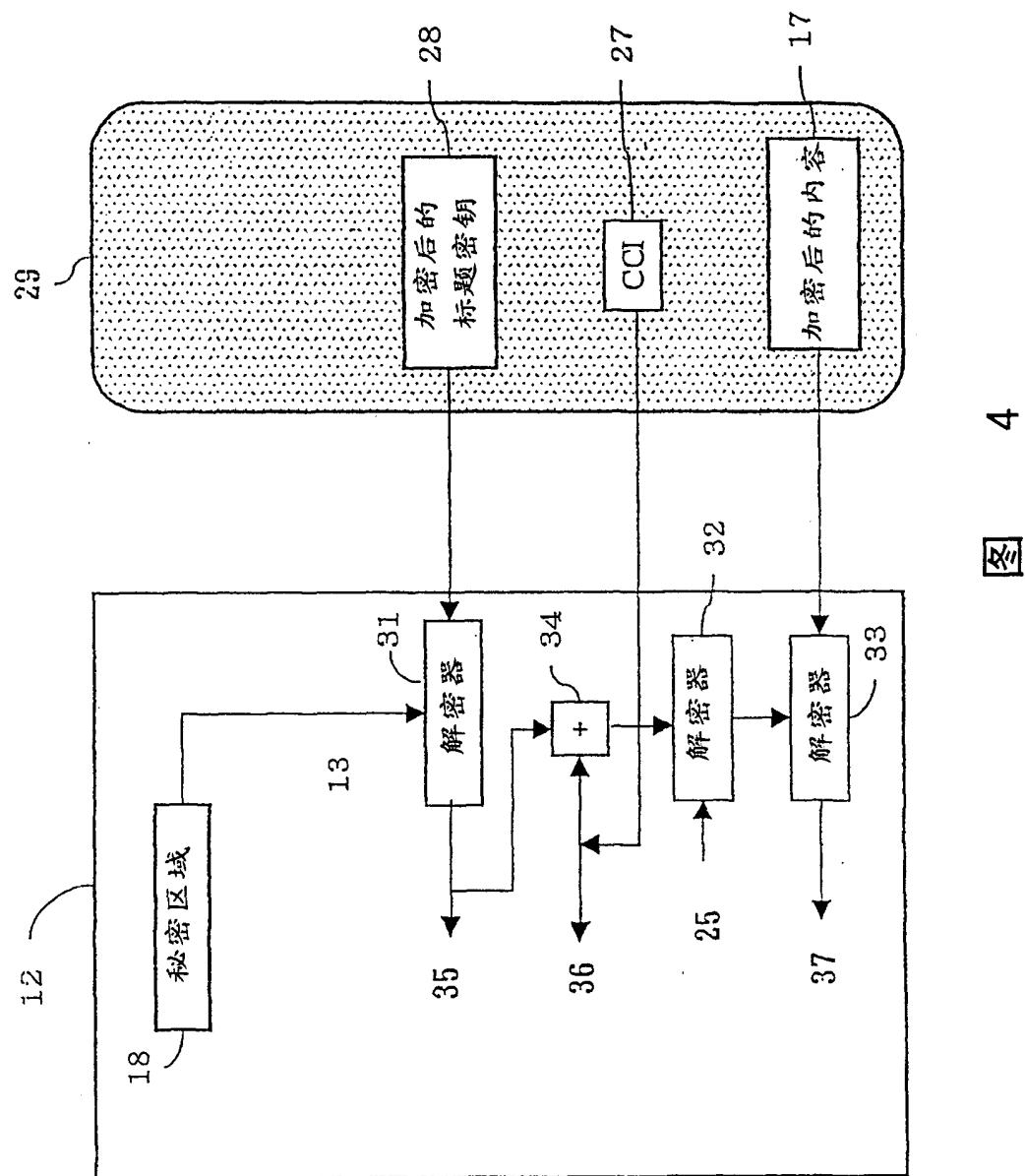
又， 本发明能够提供一种在保护著作权的同时能够将禁止复制的数据移动或复制到其他记录媒体上的数据处理装置、 将来自其他数据处理装置的数据记录到记录媒体或者记录的同时进行重放的记录重放装置、 保护著作权并且将数据预先备份的加密数据解密记录装置系统以及构成该系统的解密记录装置、 记录装置、 保护著作权并发送数据的数据发送装置。

又， 本发明能够提供一种使得被禁止复制的广播节目能避免著作权侵害而进行转录重放的记录装置以及记录重放装置。



1
冬





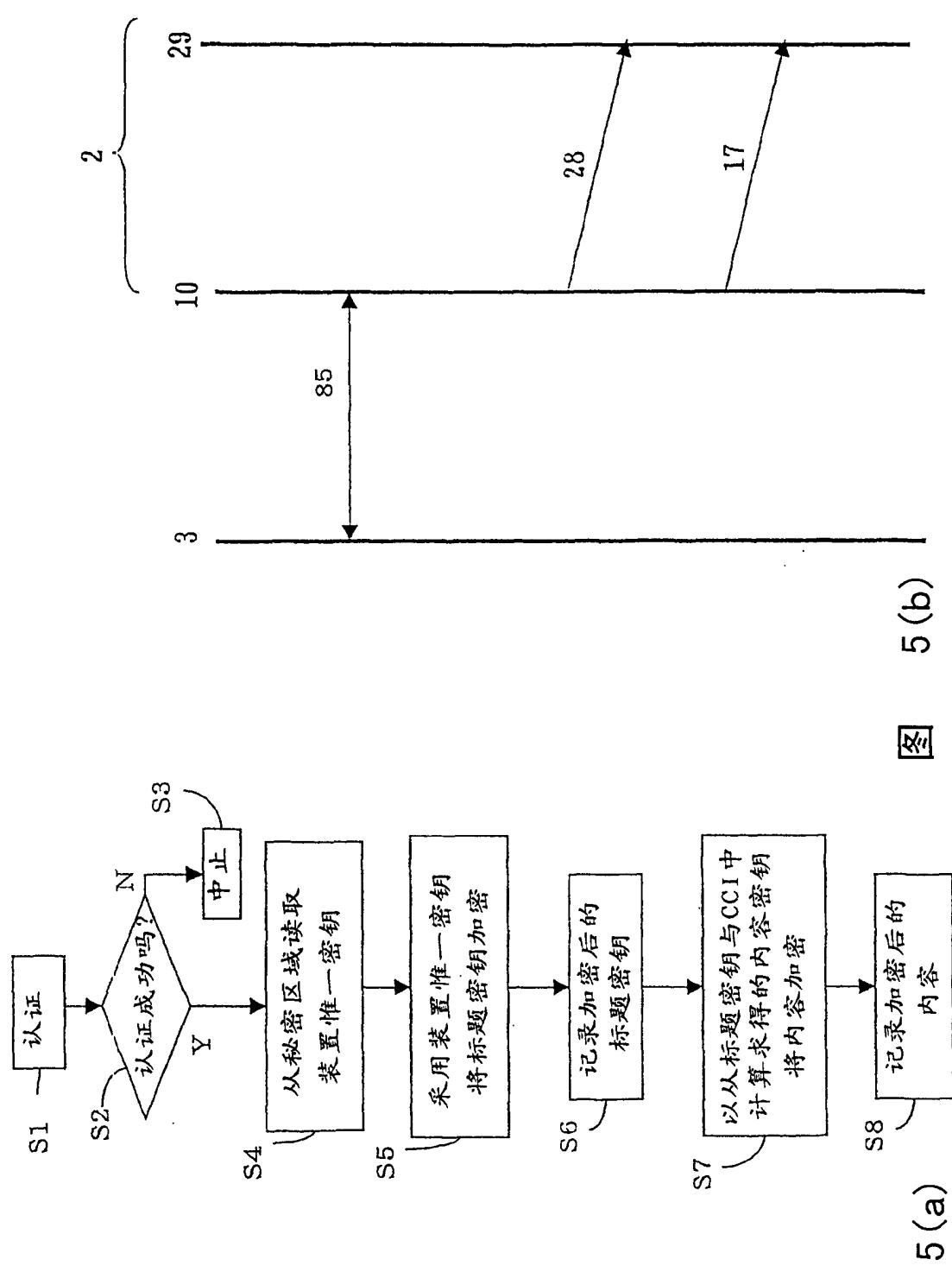
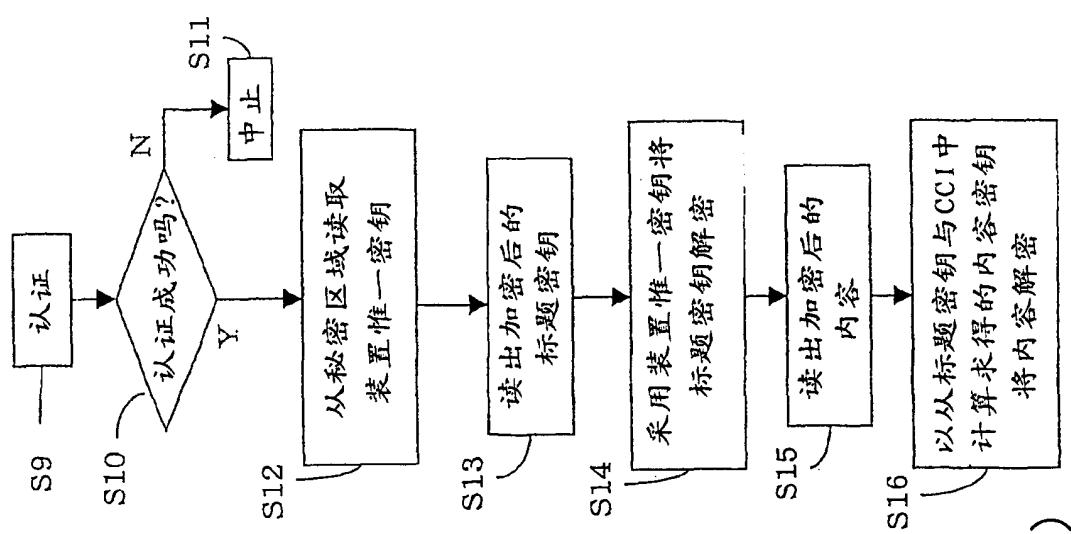
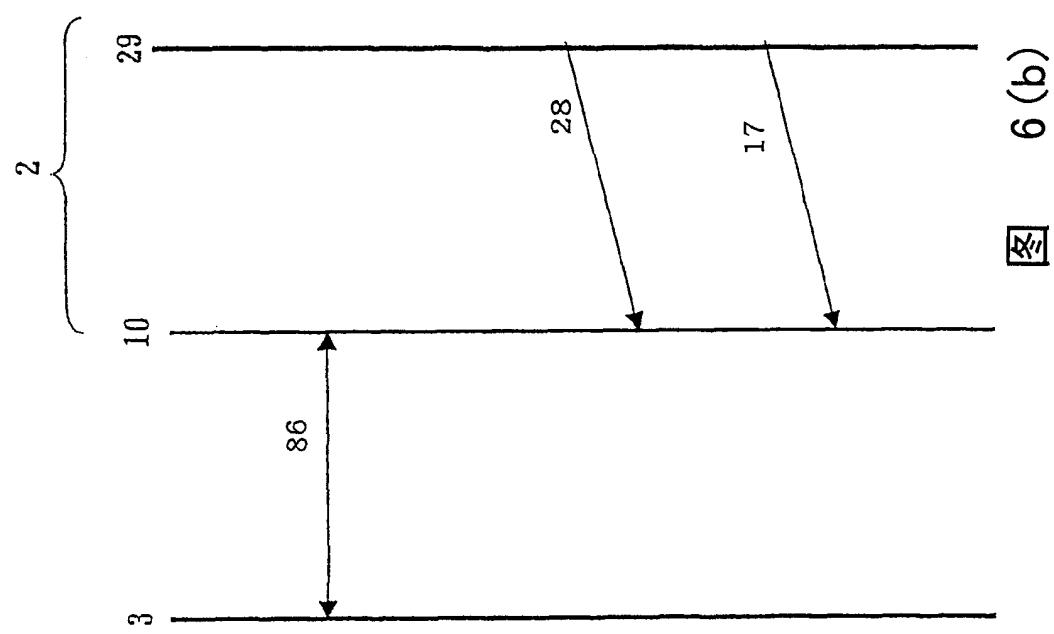


图 5 (a)
图 5 (b)



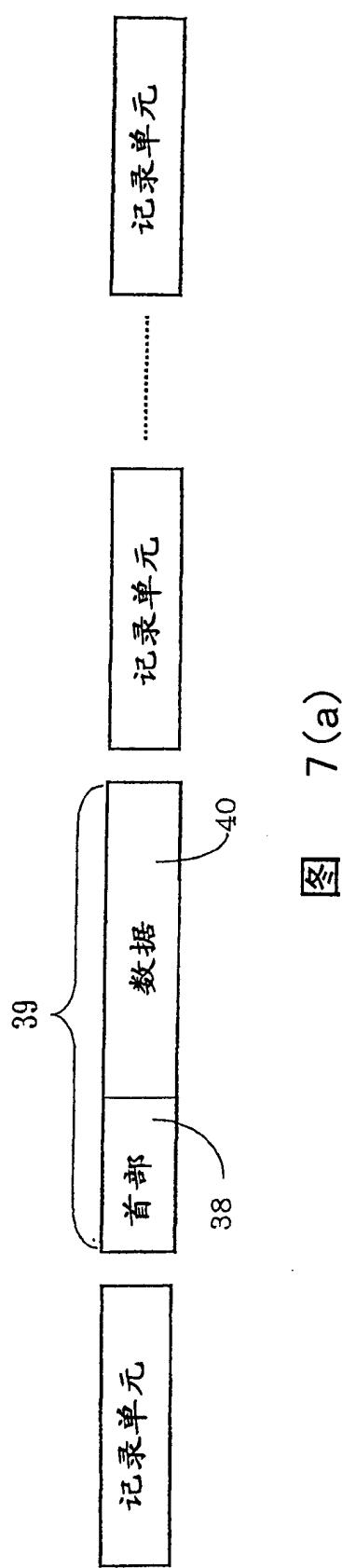


图 7(a)

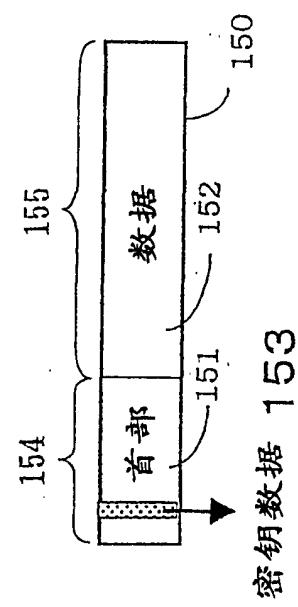


图 7(b)

CCI的值	含义
11	禁止复制
10	允许复制一次
01	禁止再次复制
00	允许自由复制

图 8

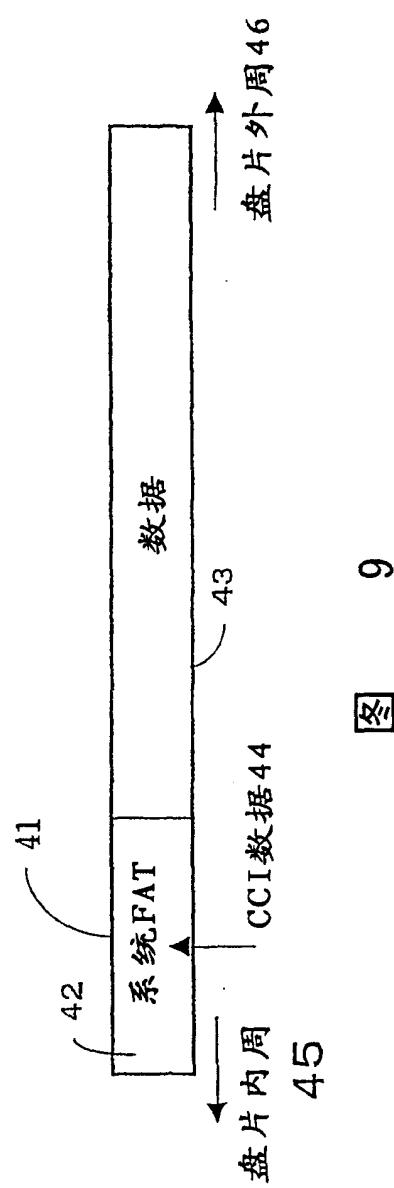
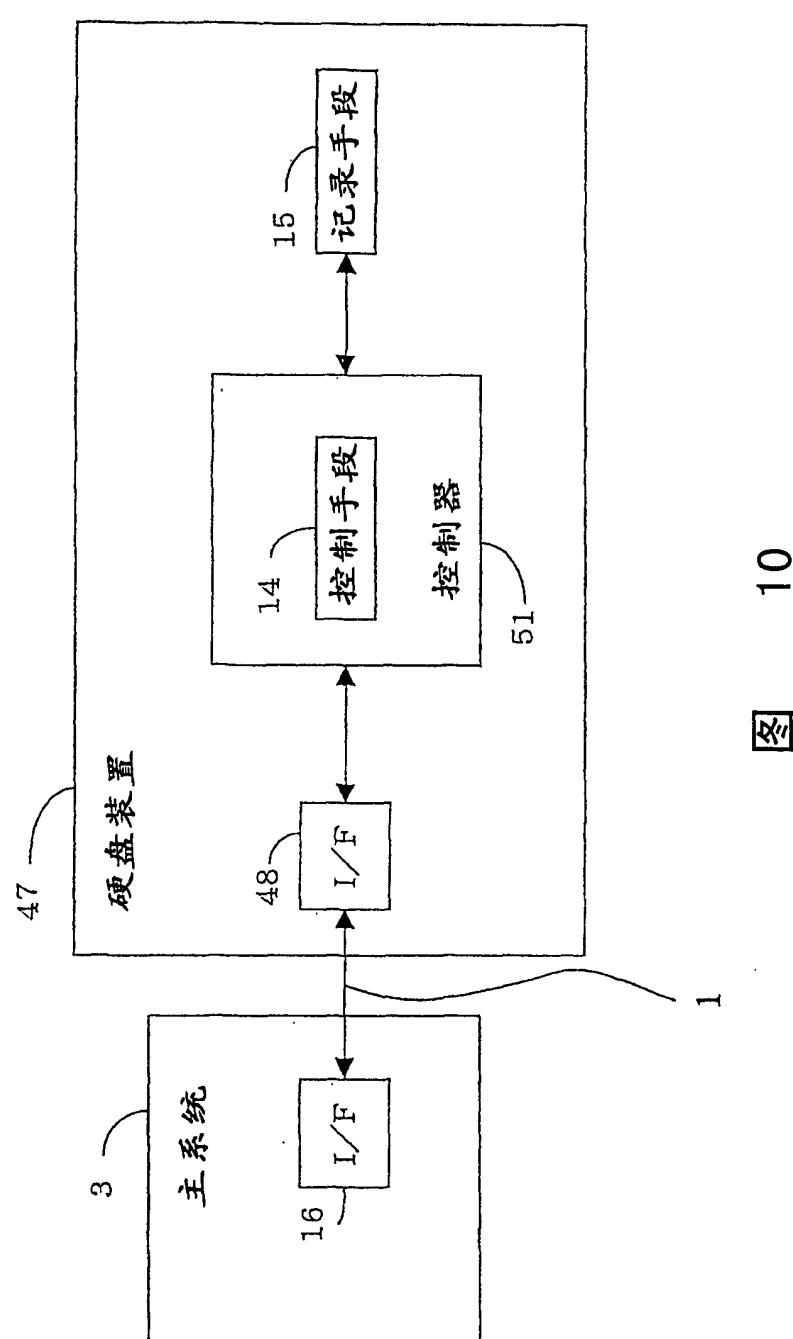
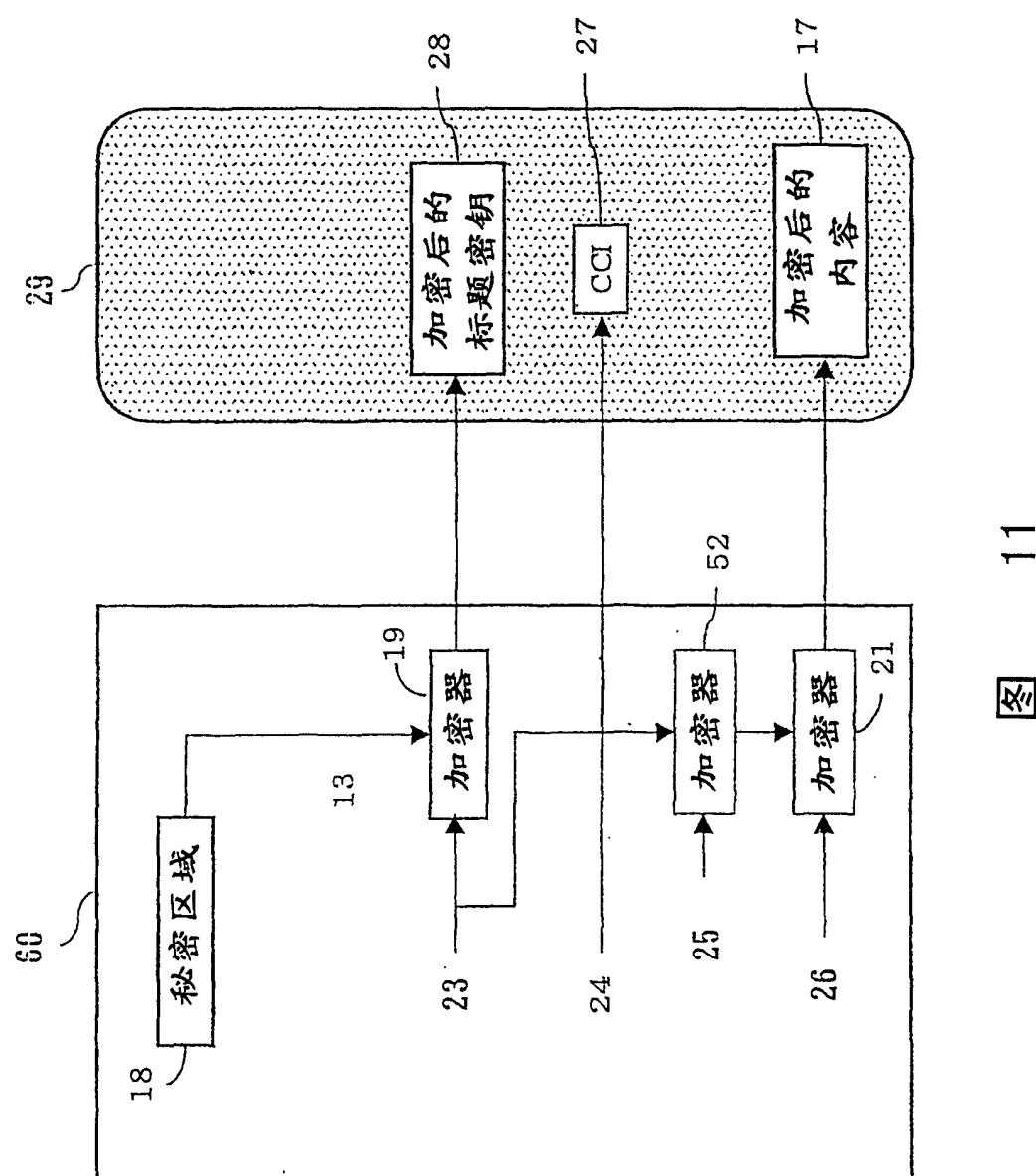
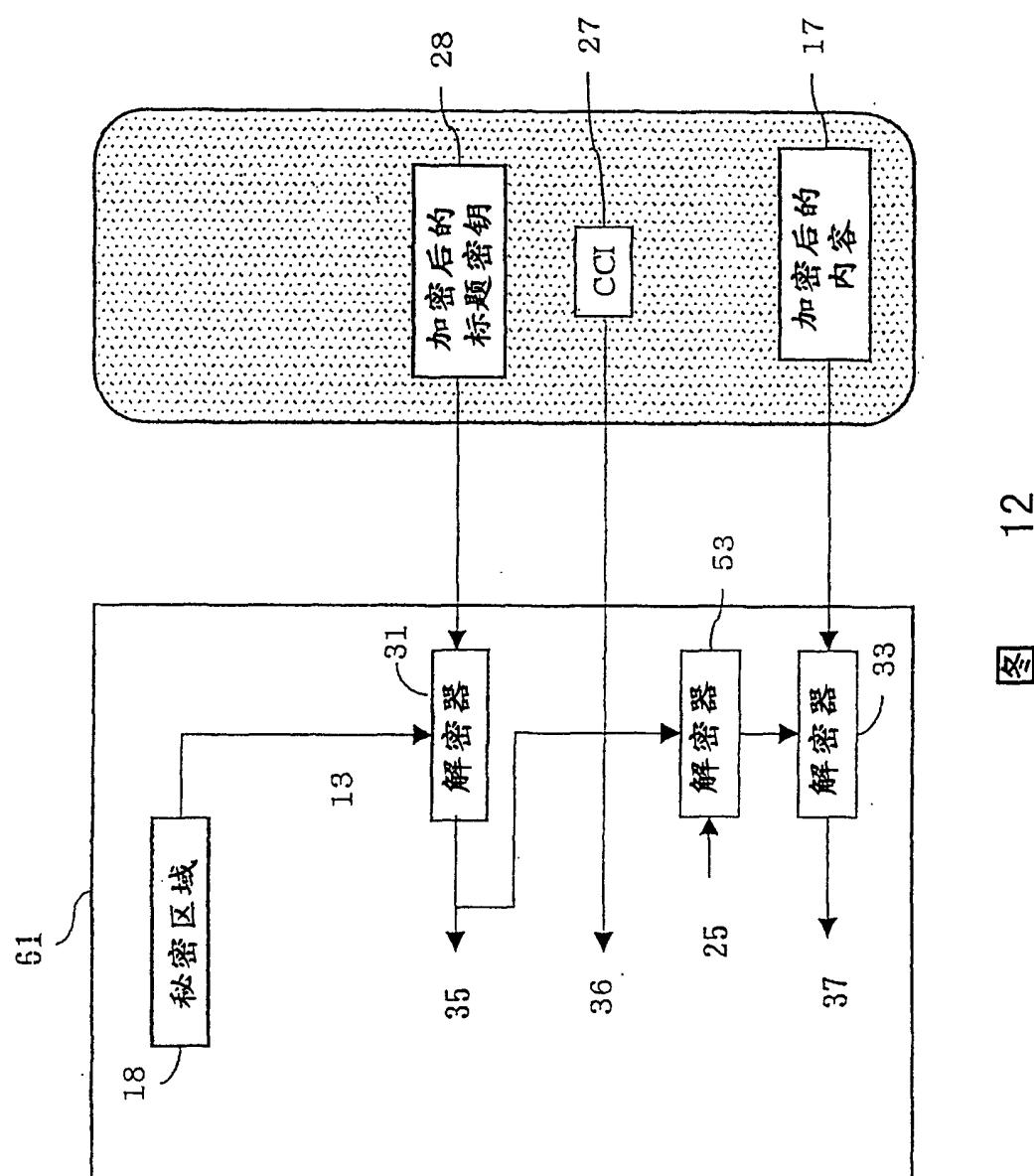
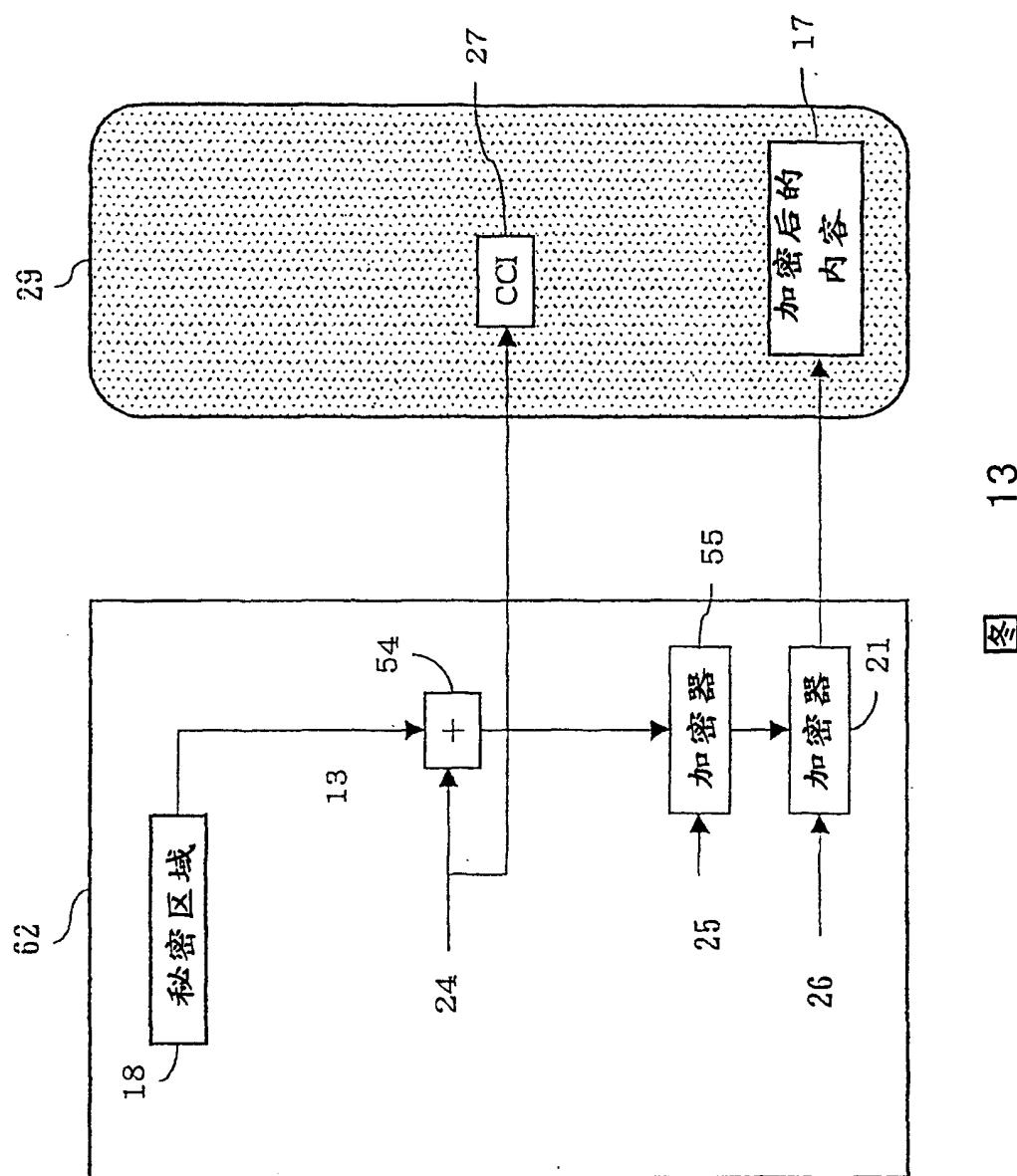


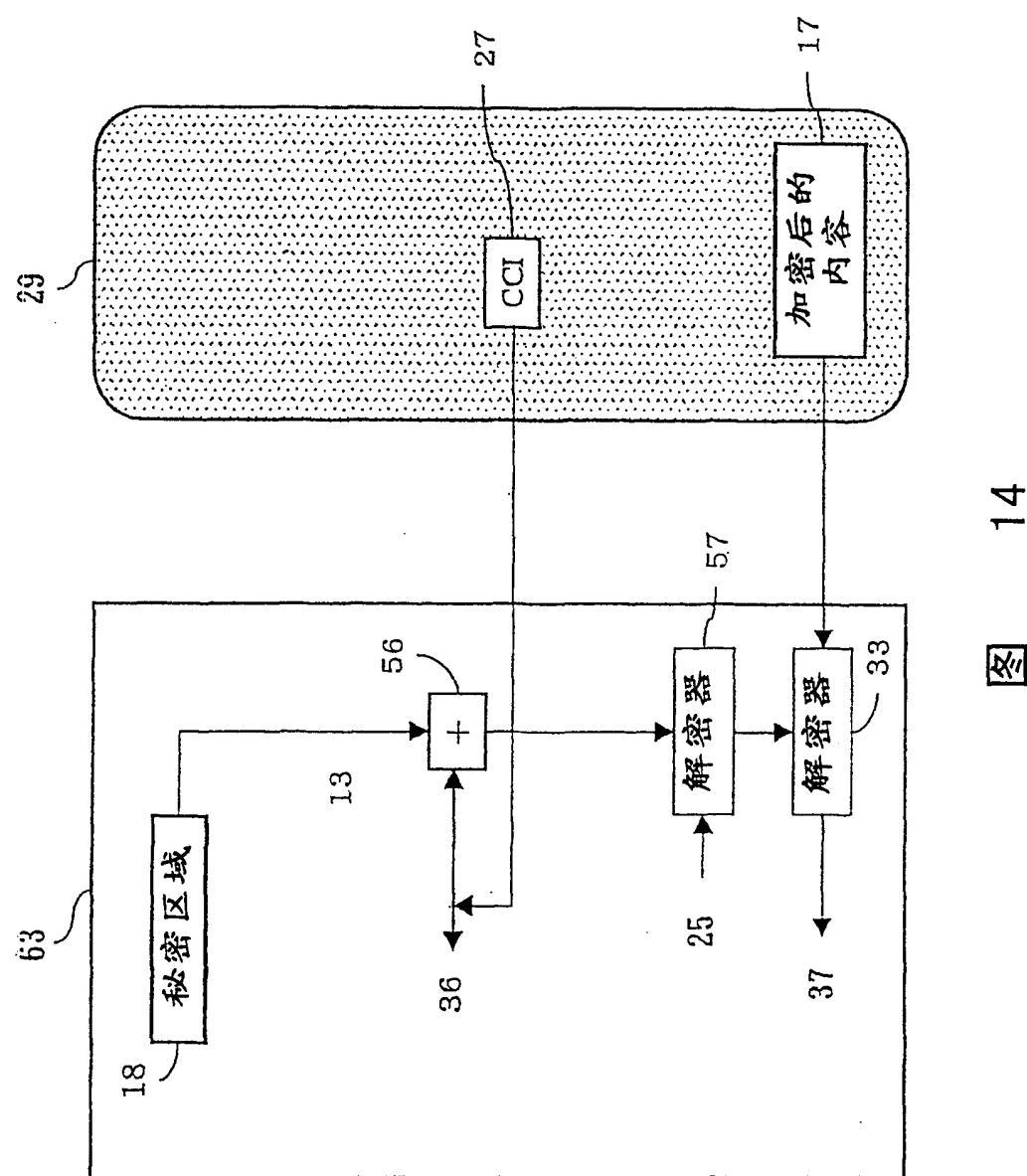
图 9

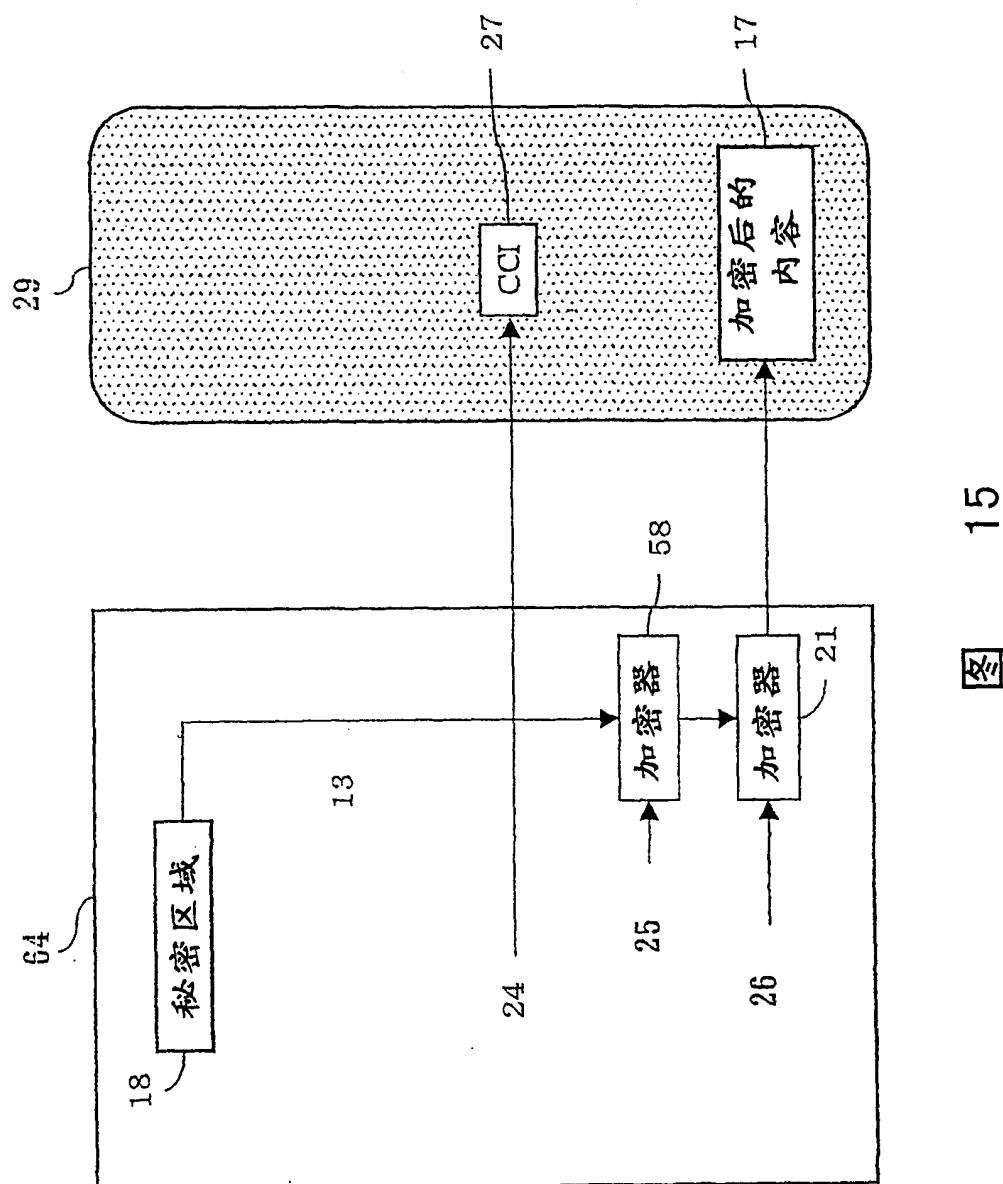


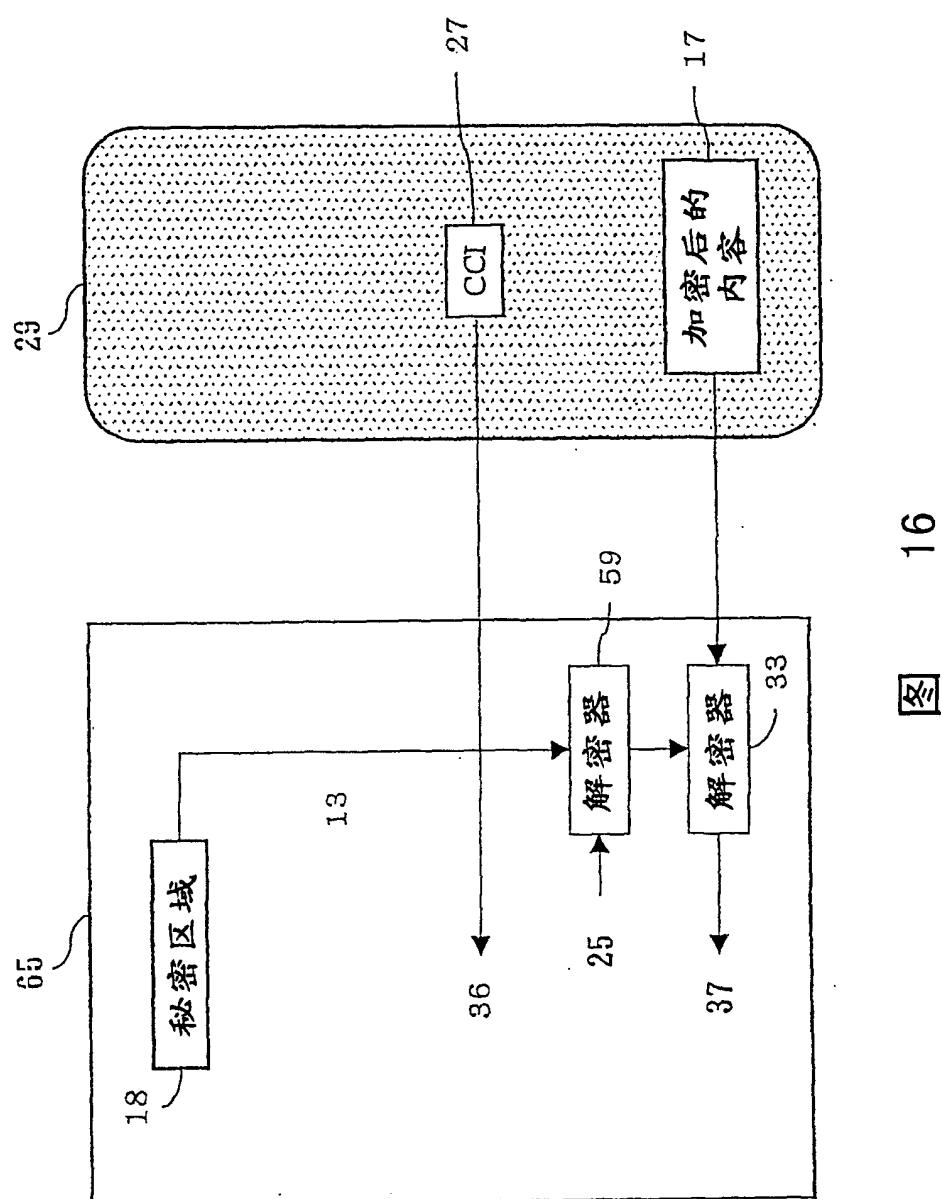












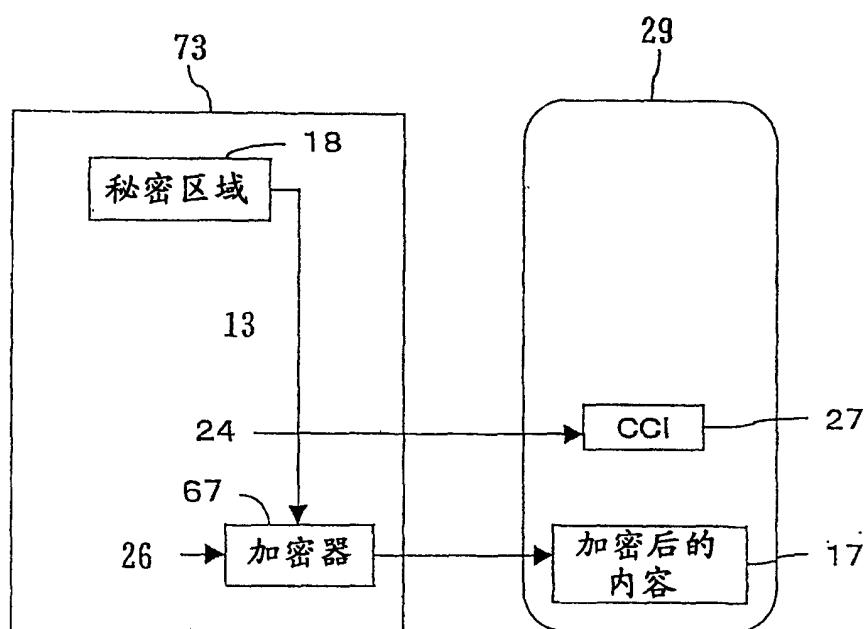


图 17(a)

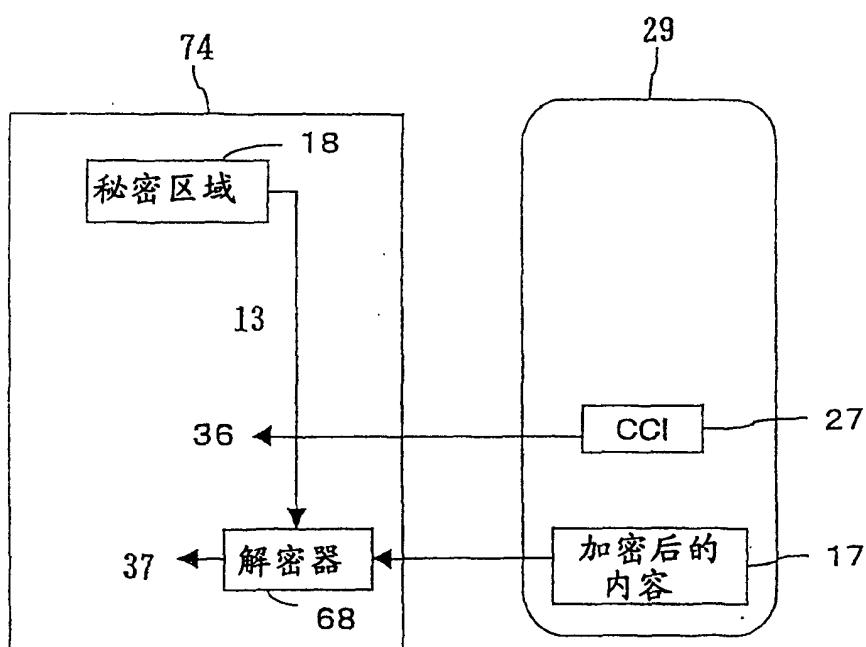


图 17(b)

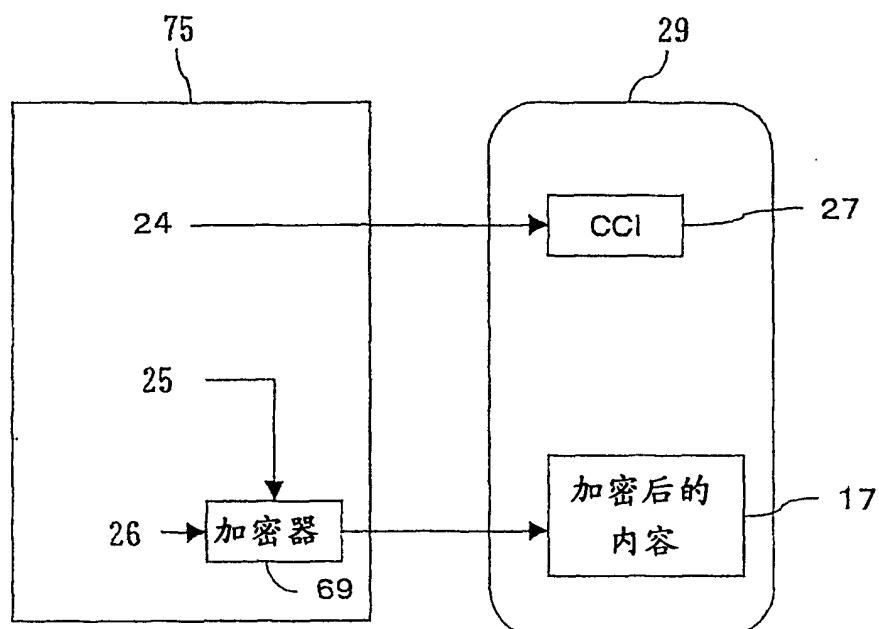


图 18(a)

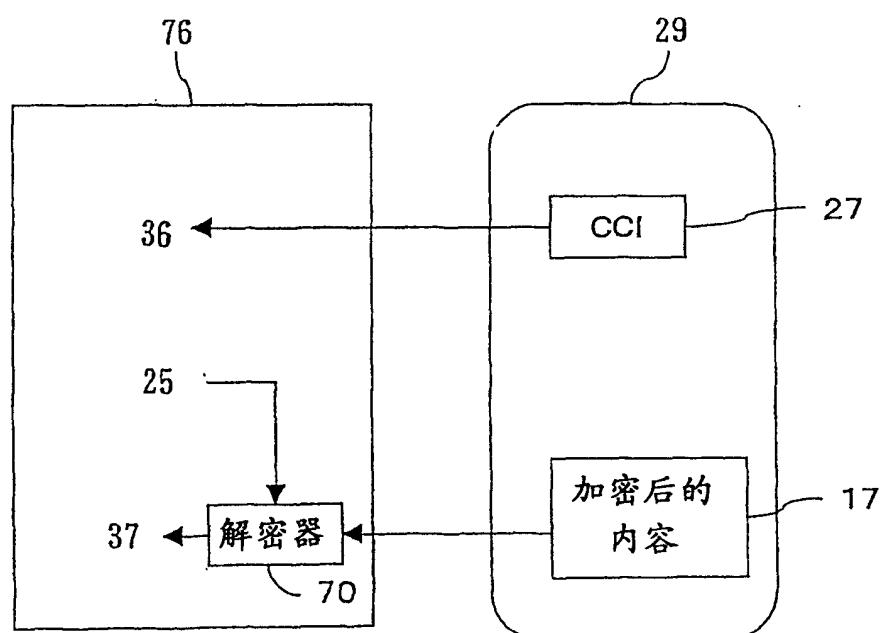
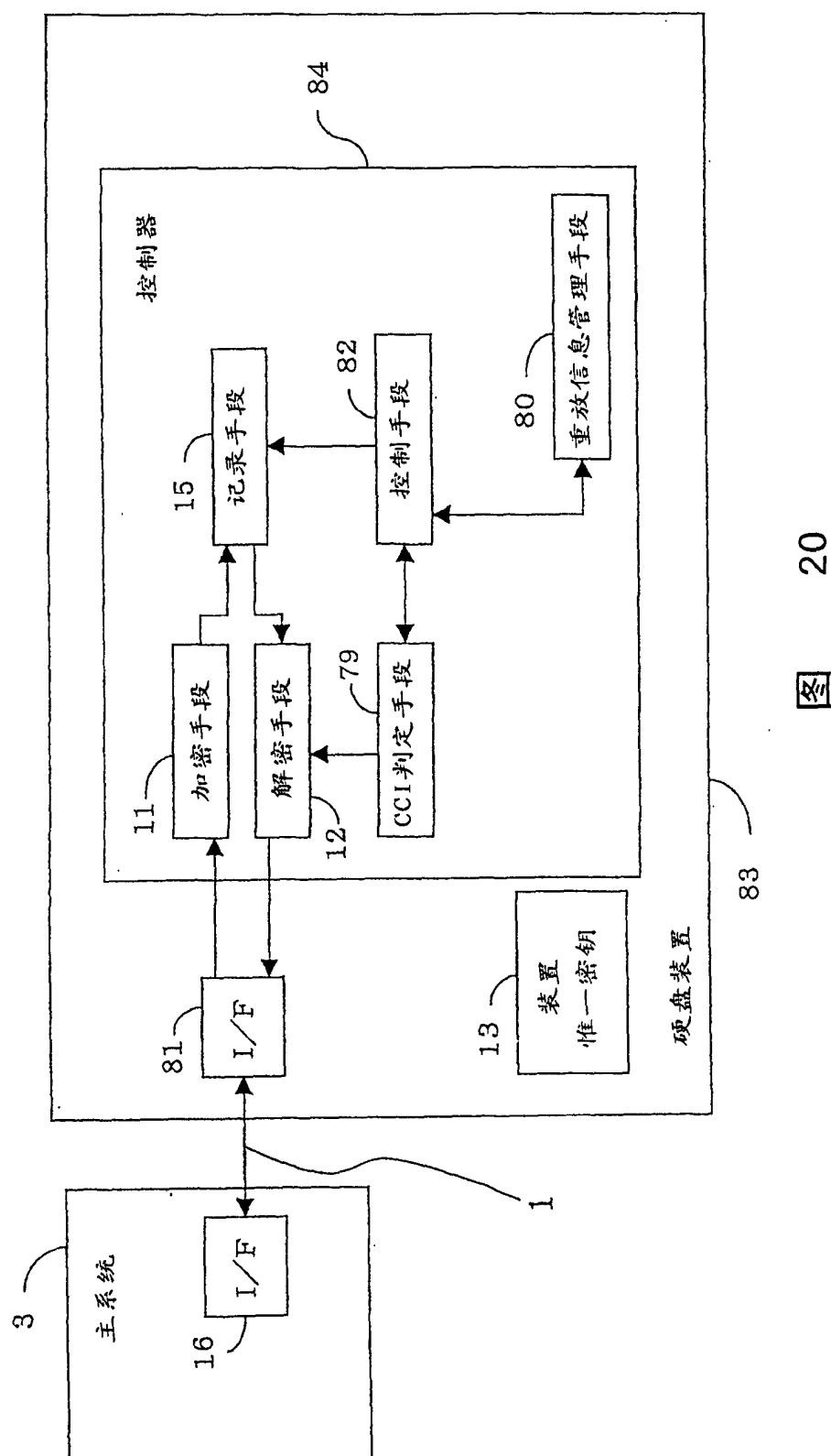


图 18(b)



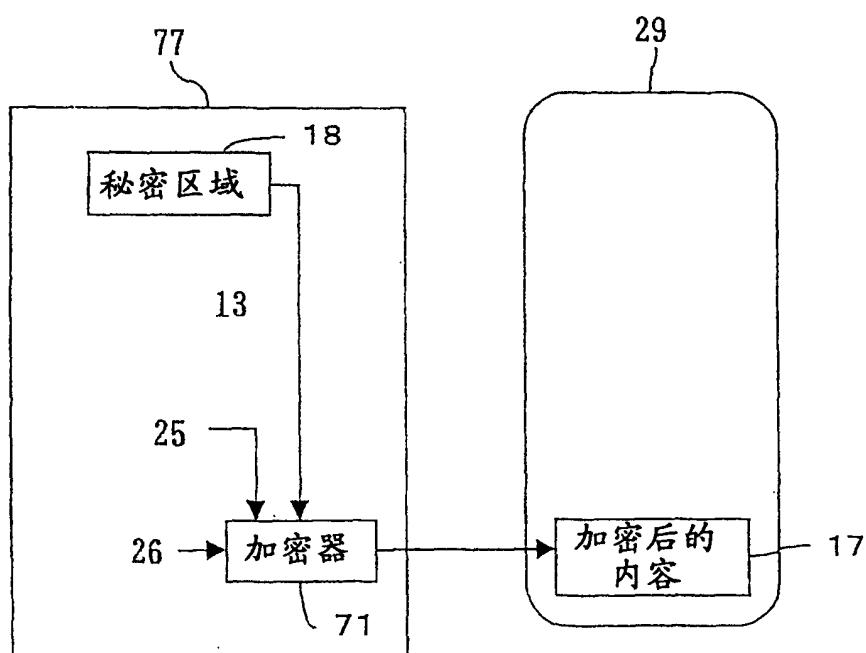


图 19(a)

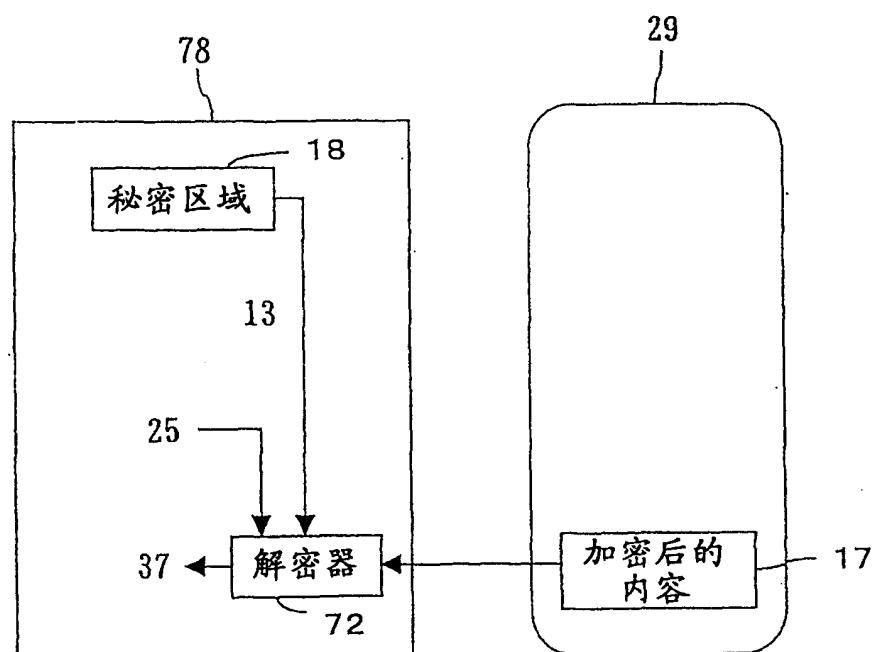


图 19(b)

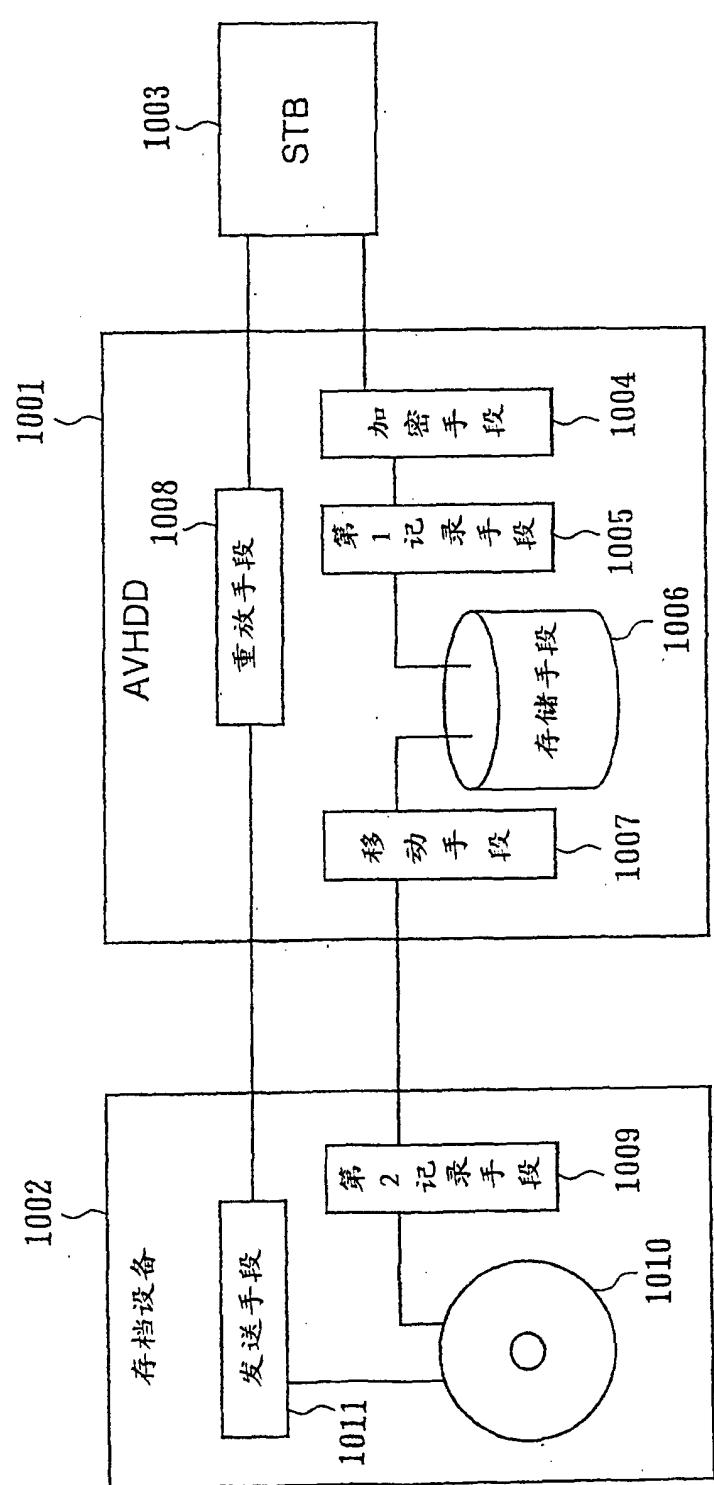


图 21

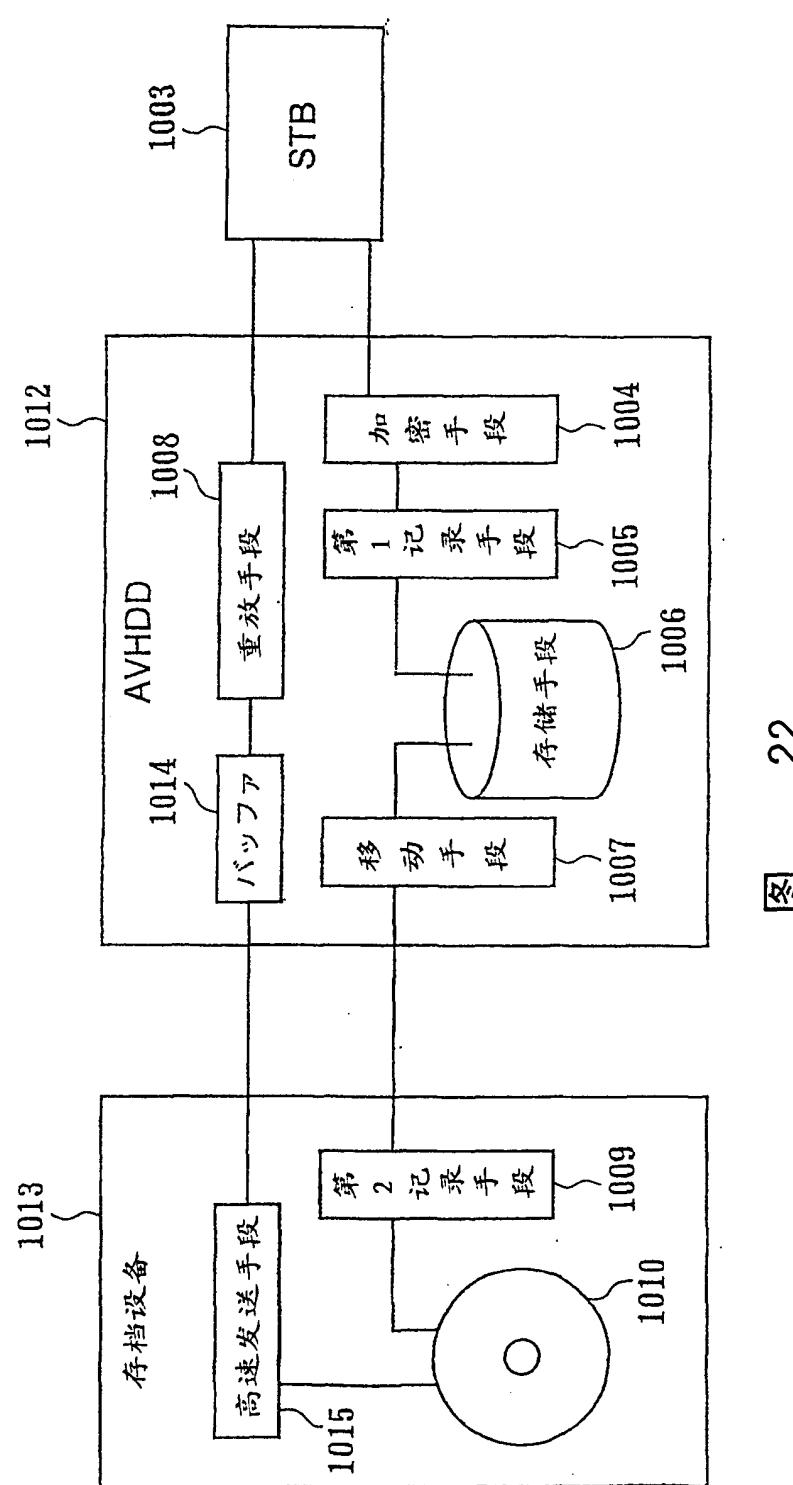


图 22

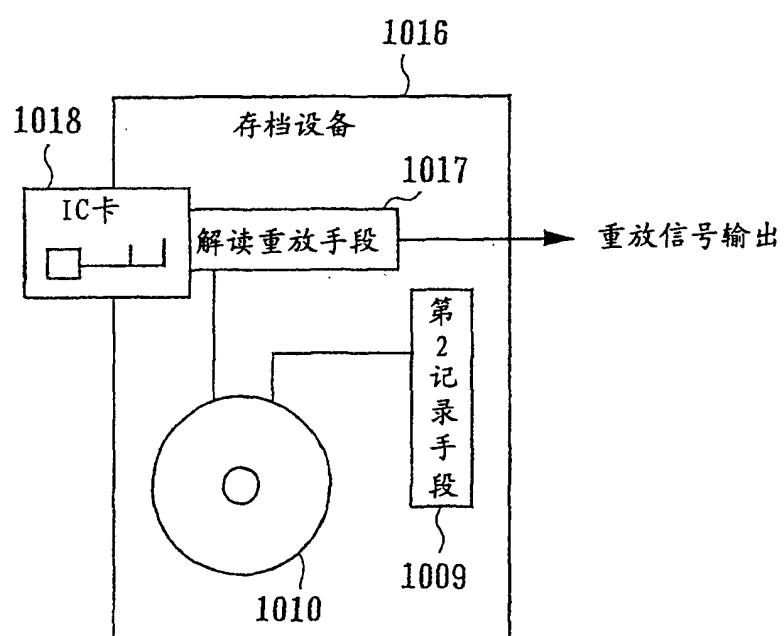


图 23

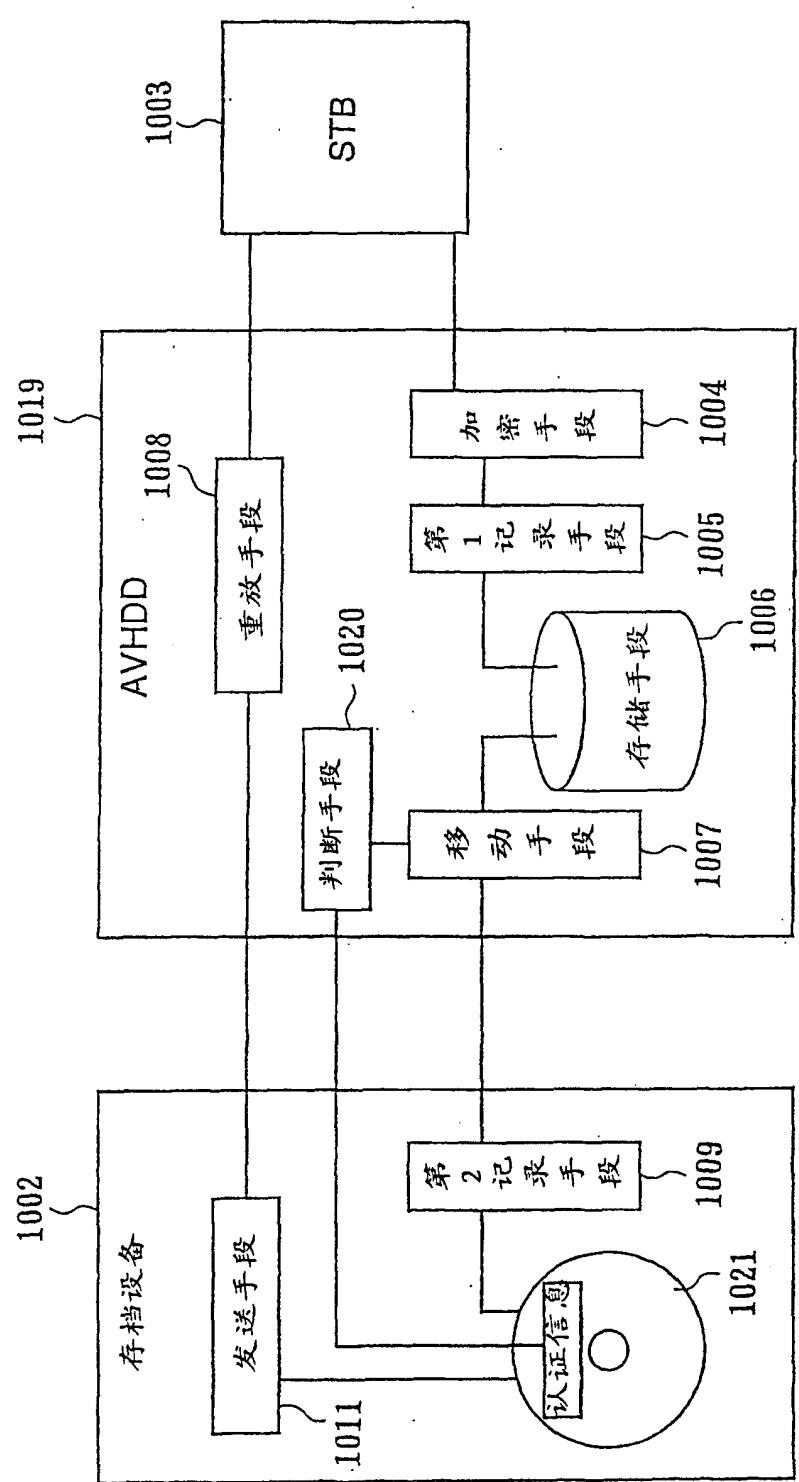
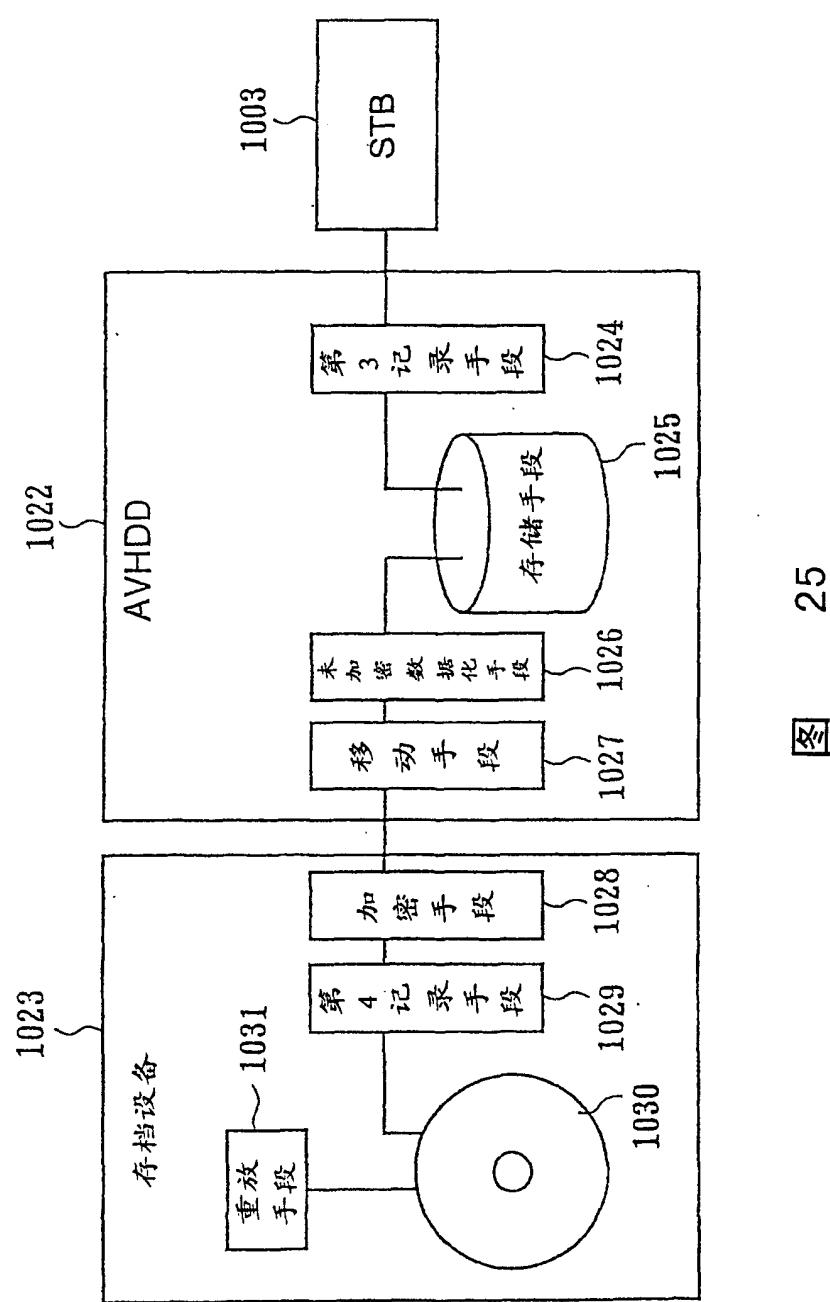


图 24



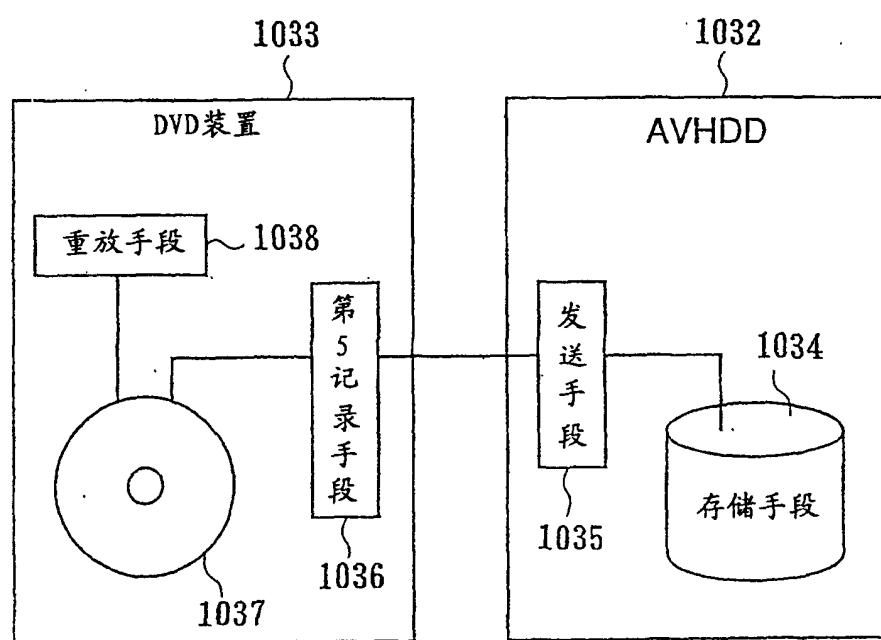


图 26

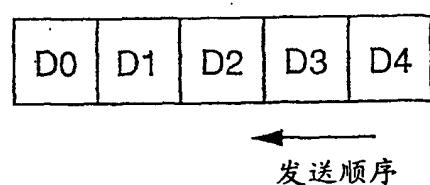


图 27

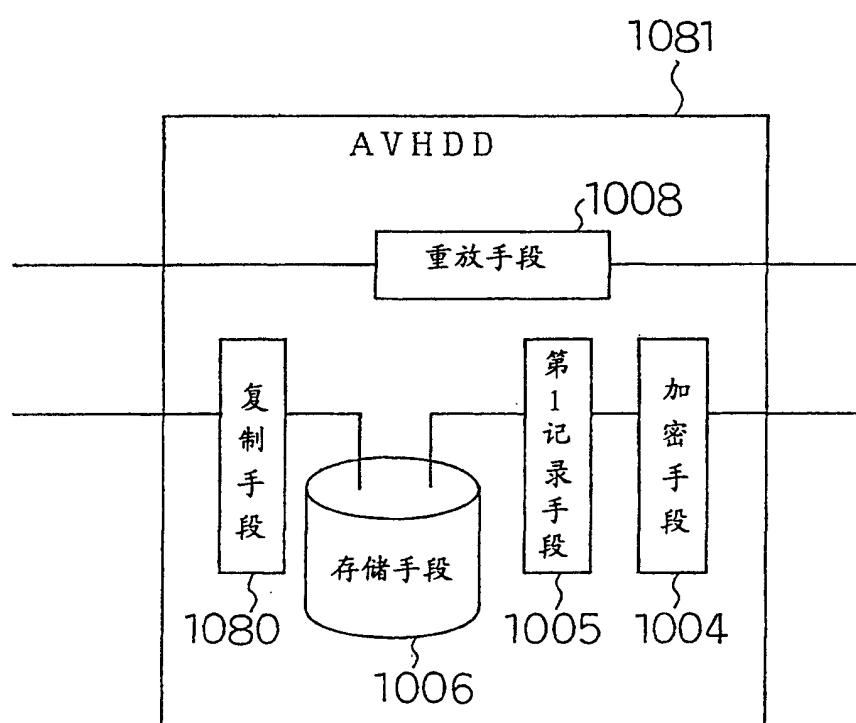


图 28

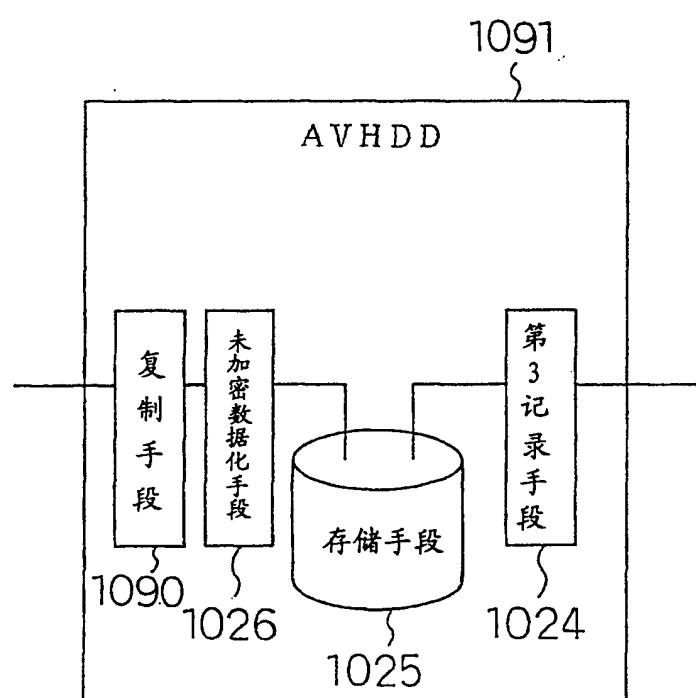


图 29

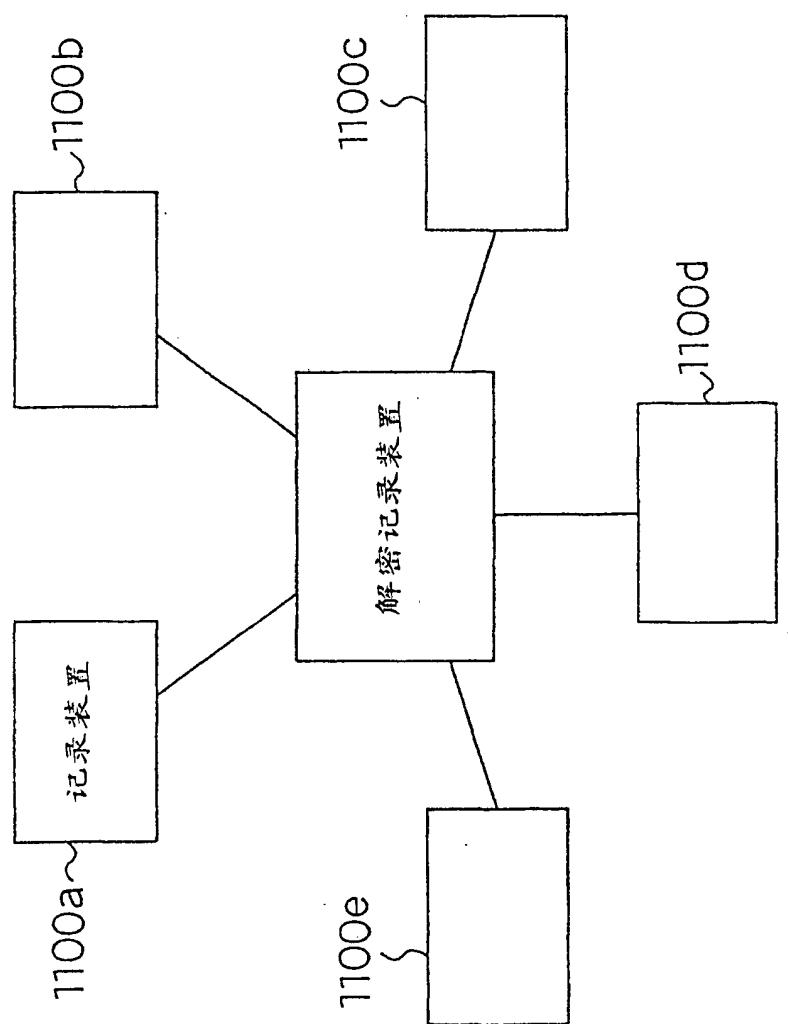
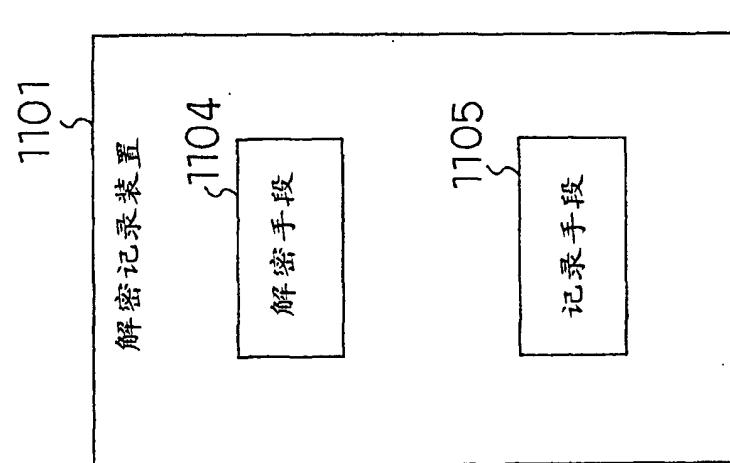
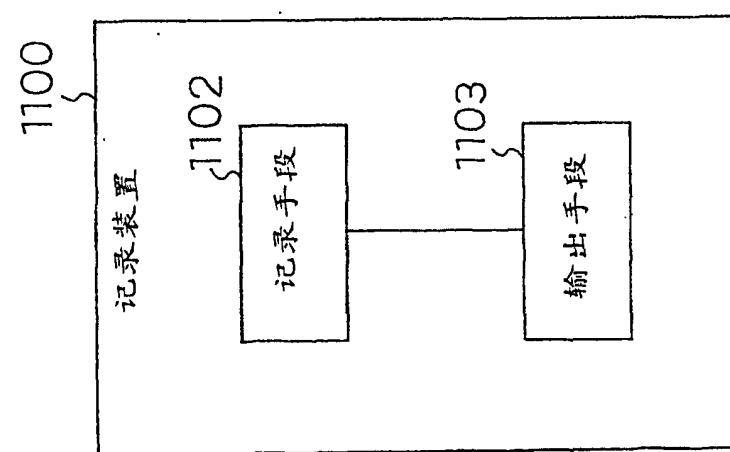


图 30



32

图



31

图

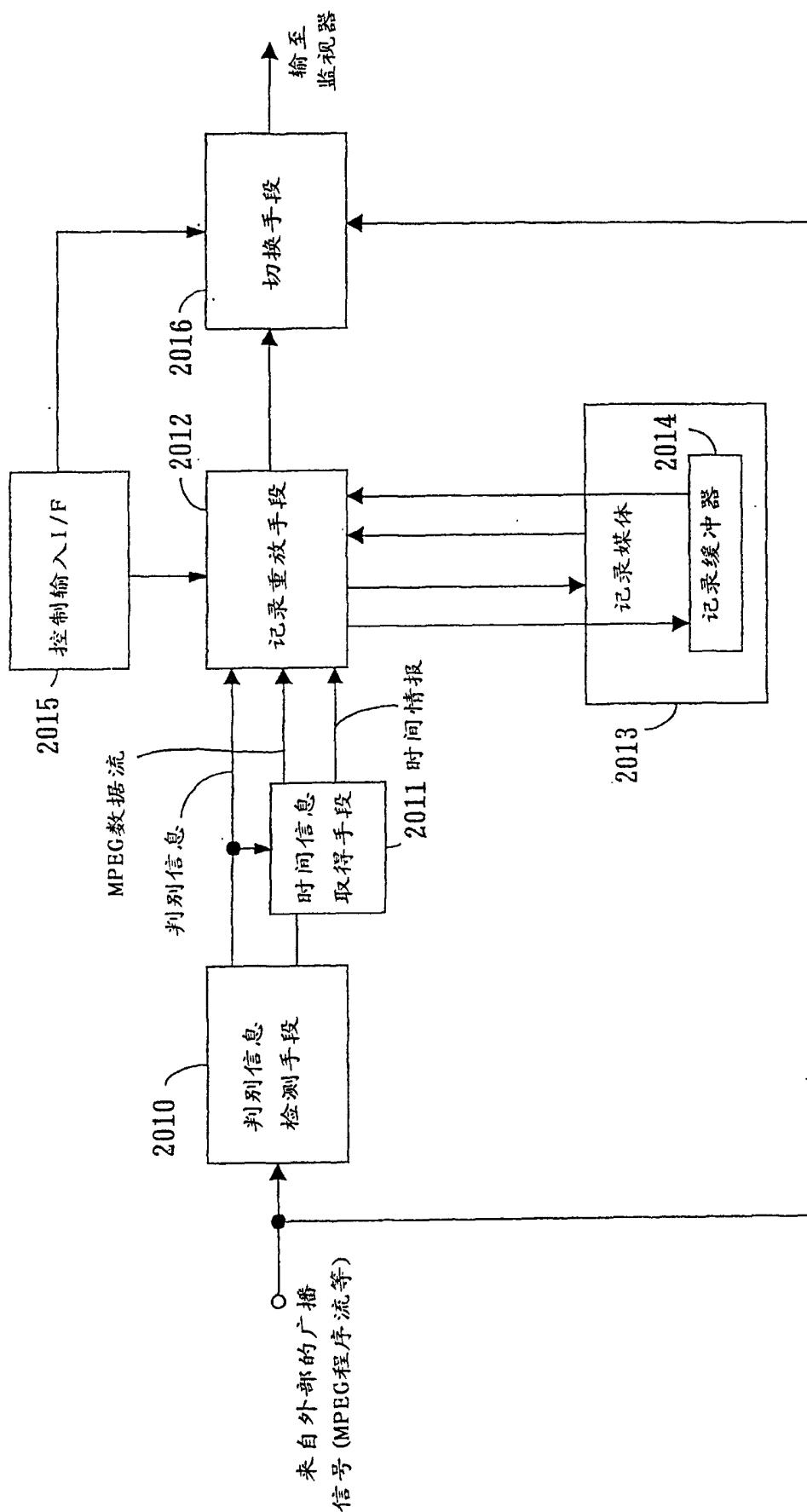
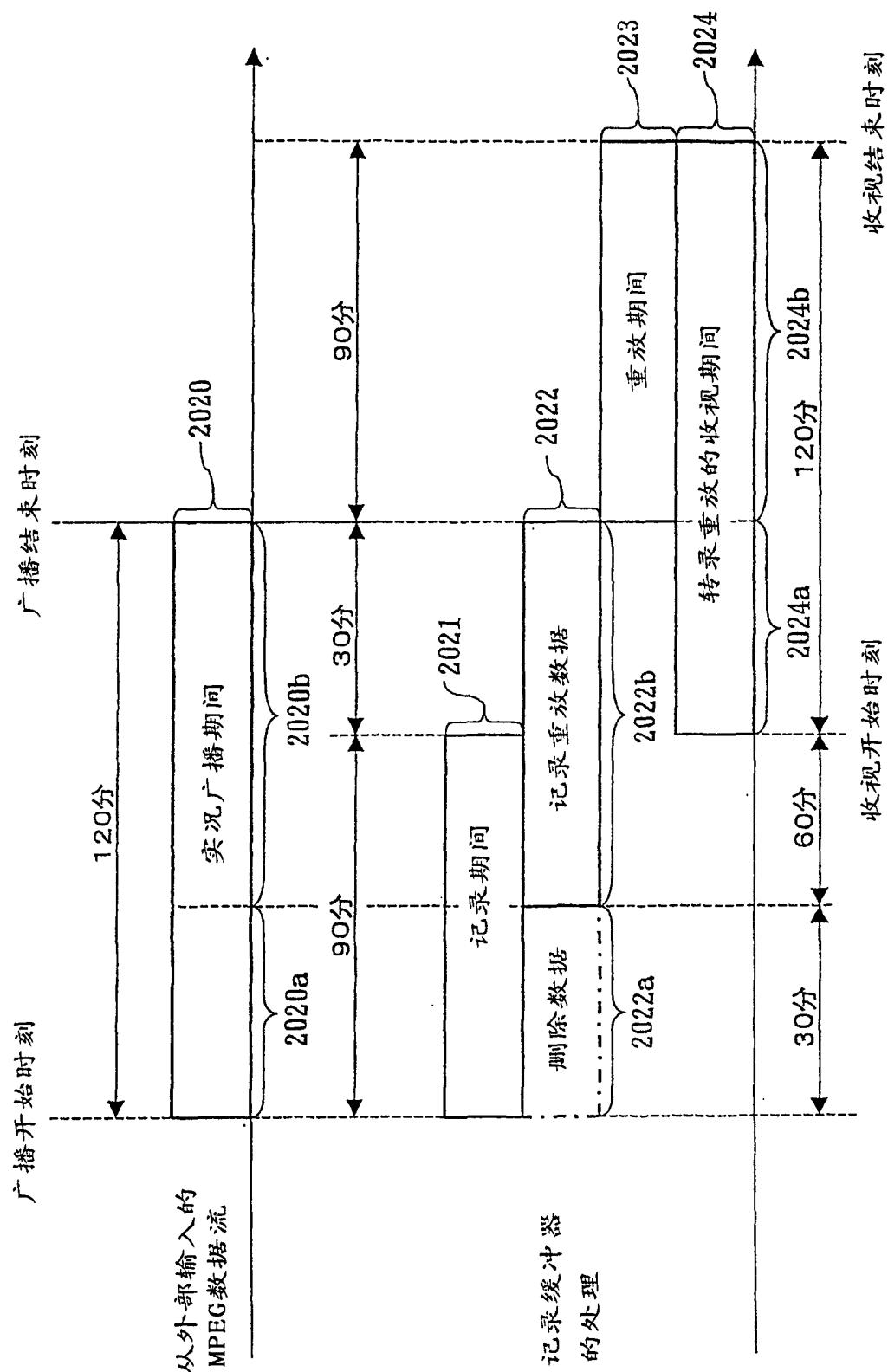
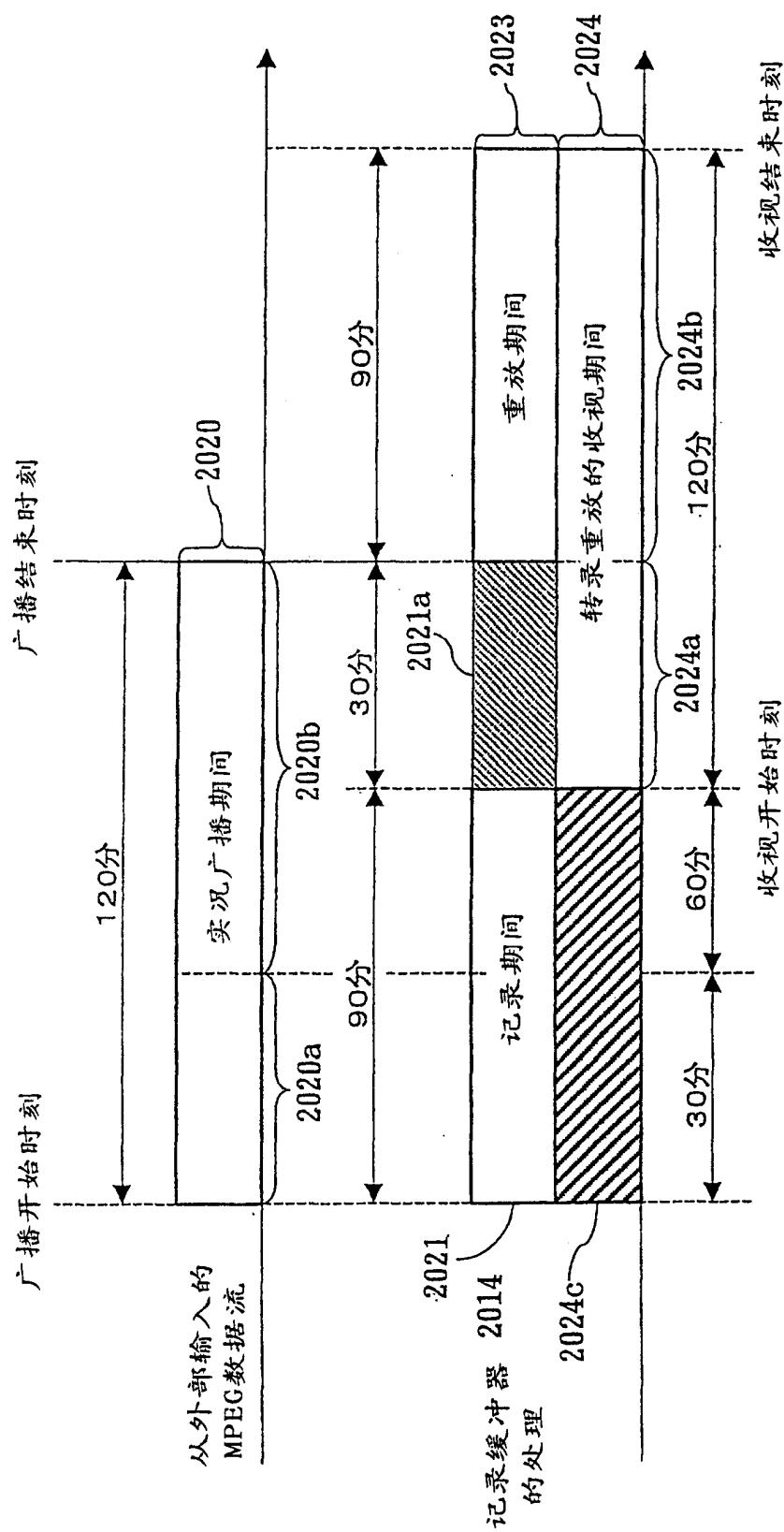


图 33





图

35

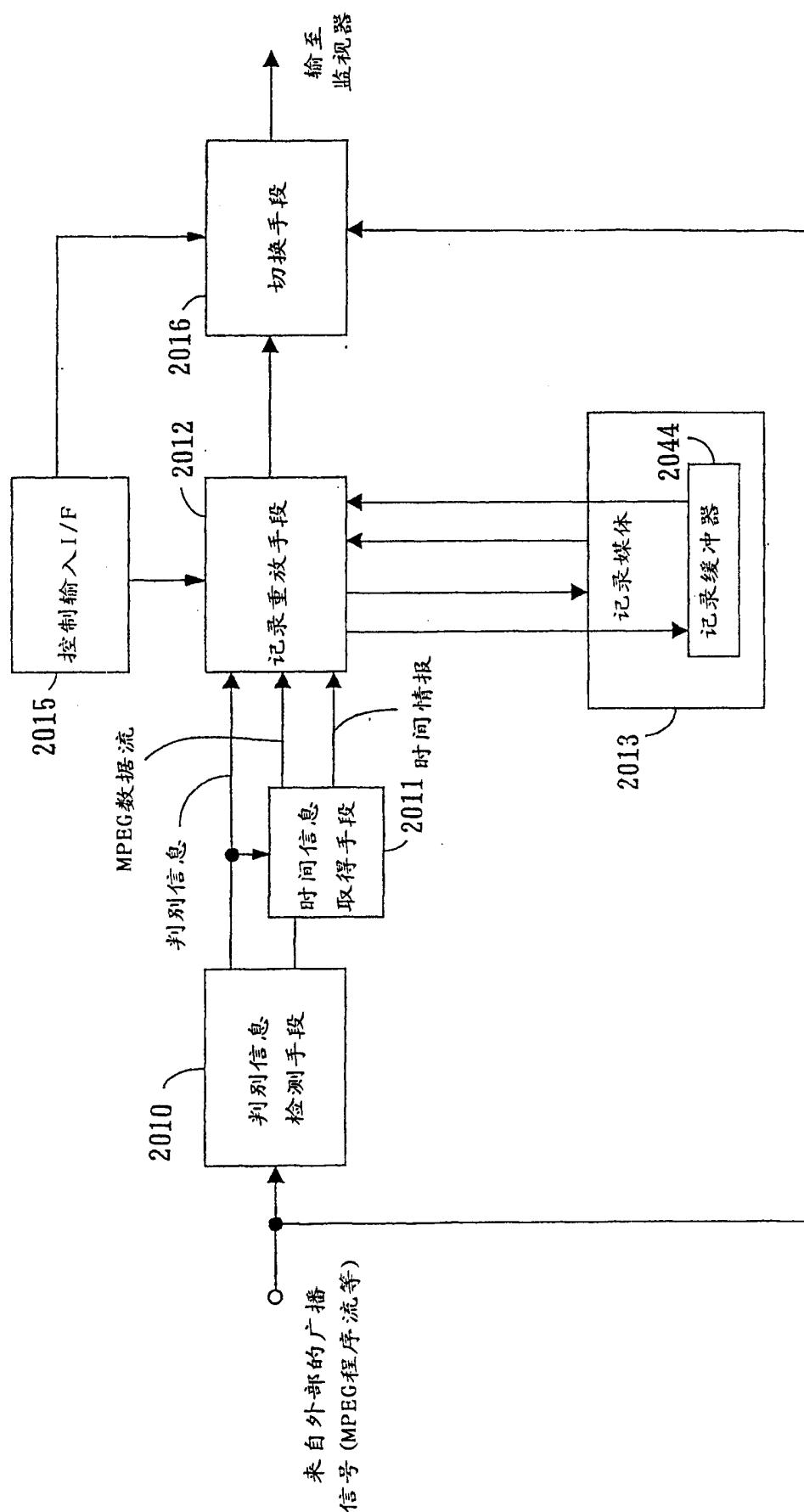
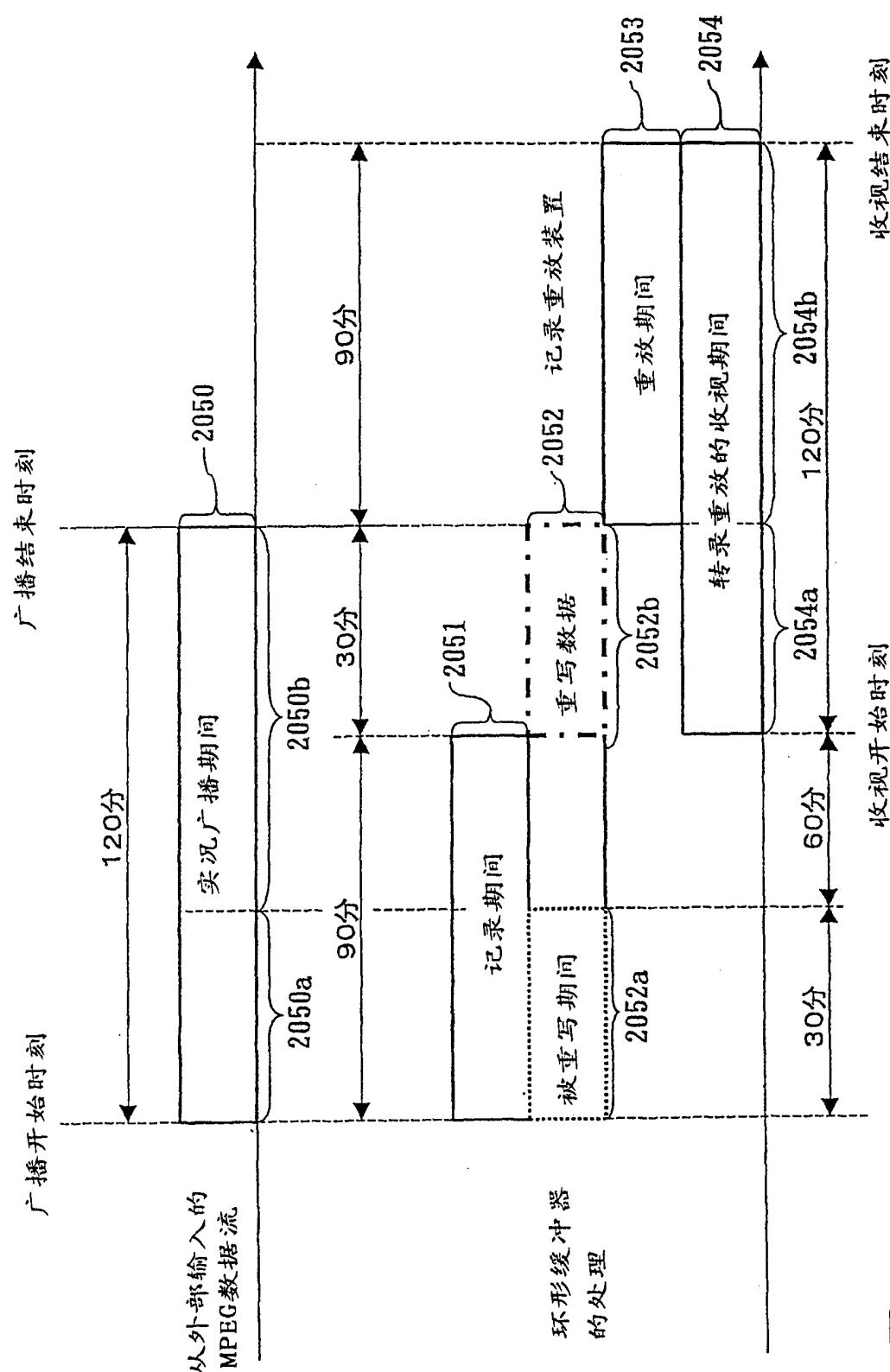


图 36



37

图

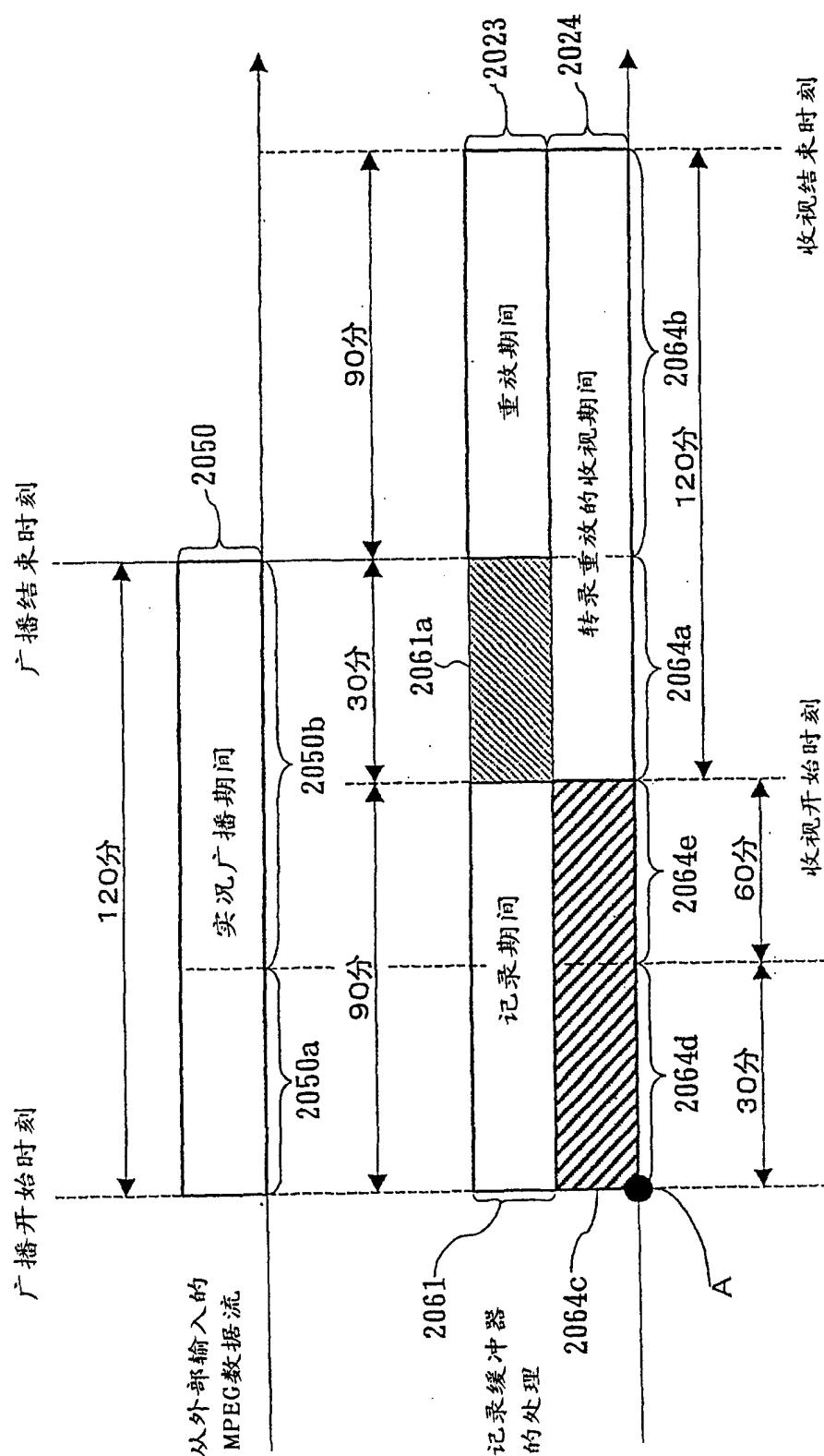
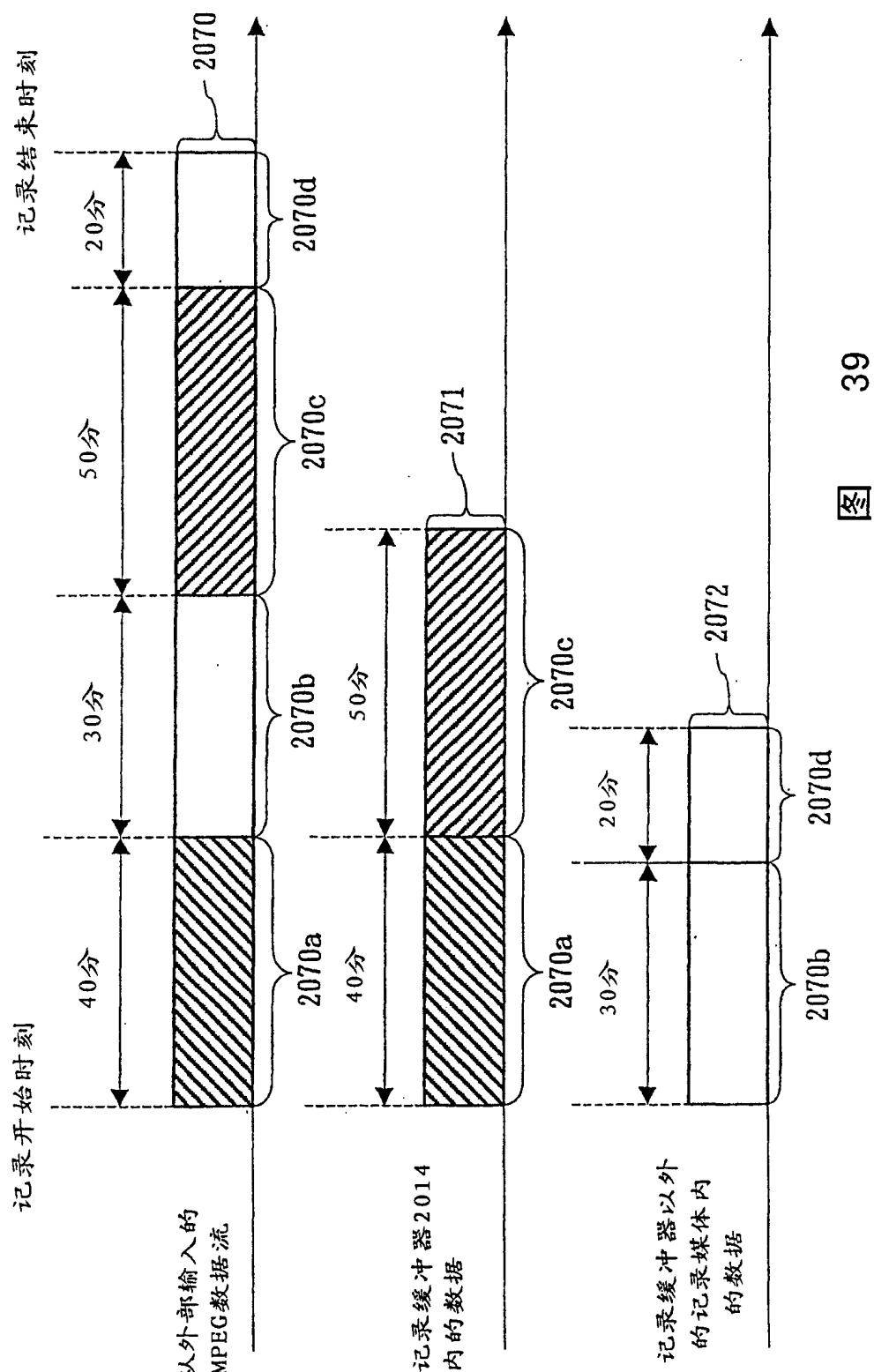
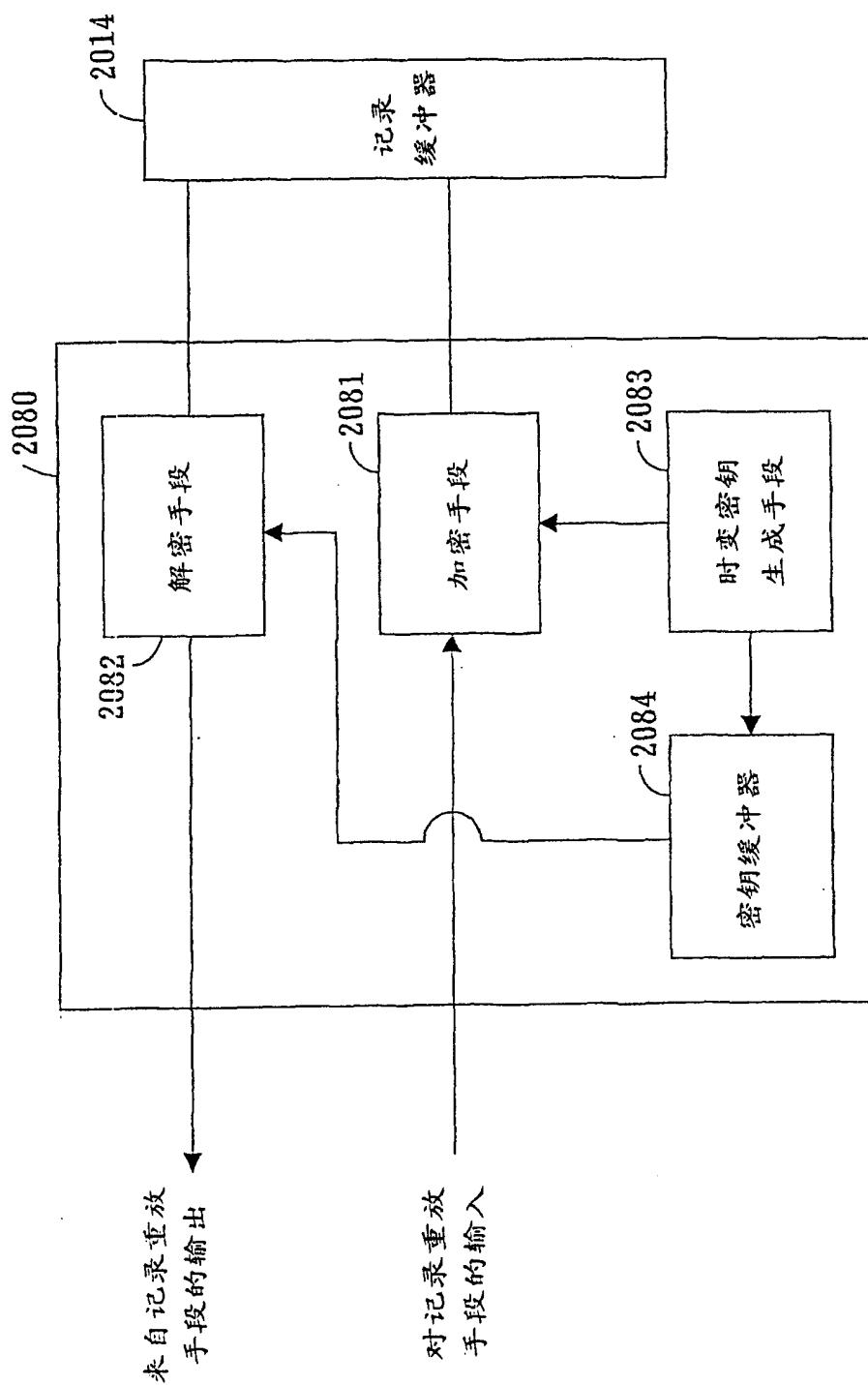


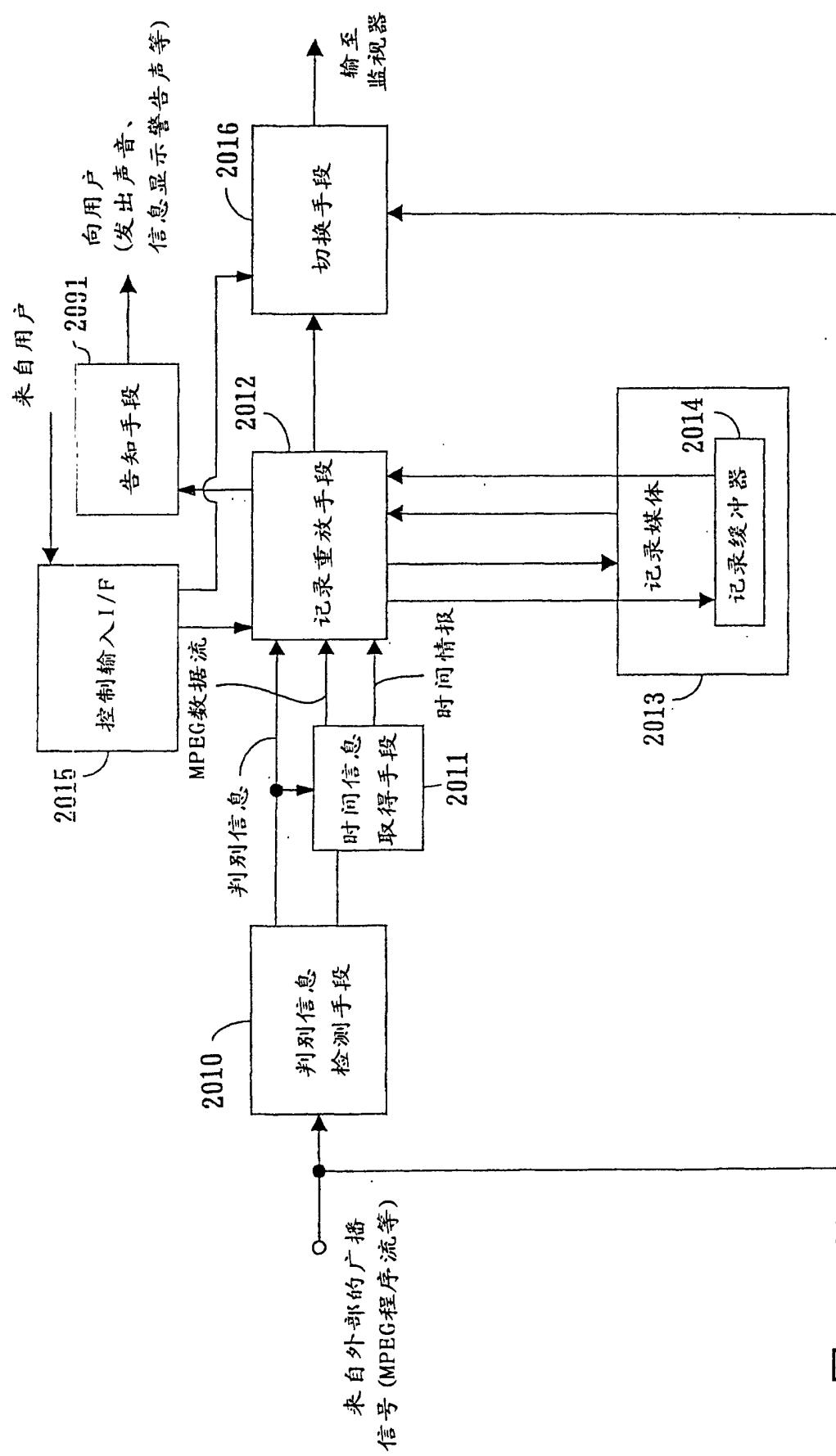
图 38





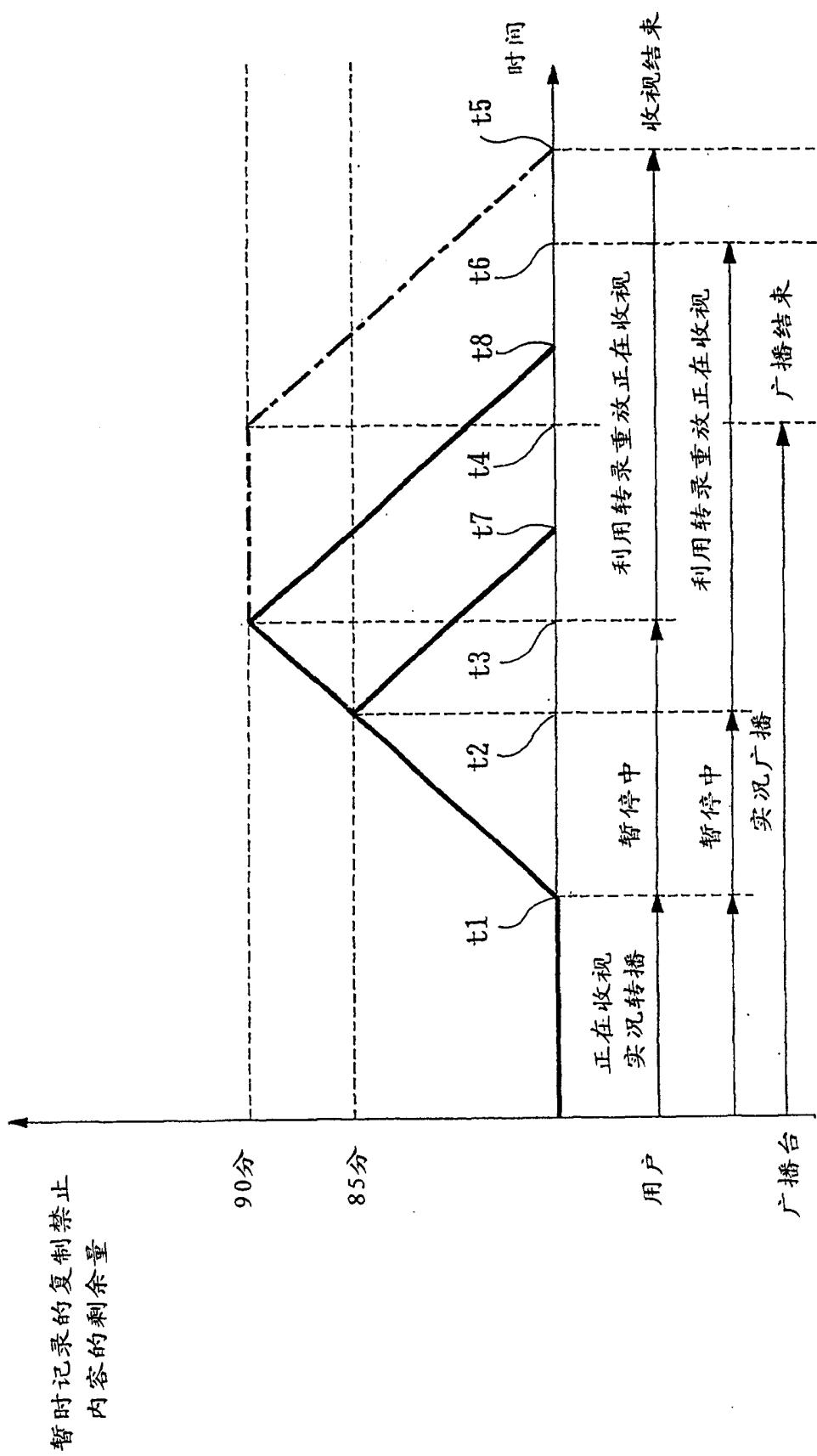
40

图



41

图



冬

42

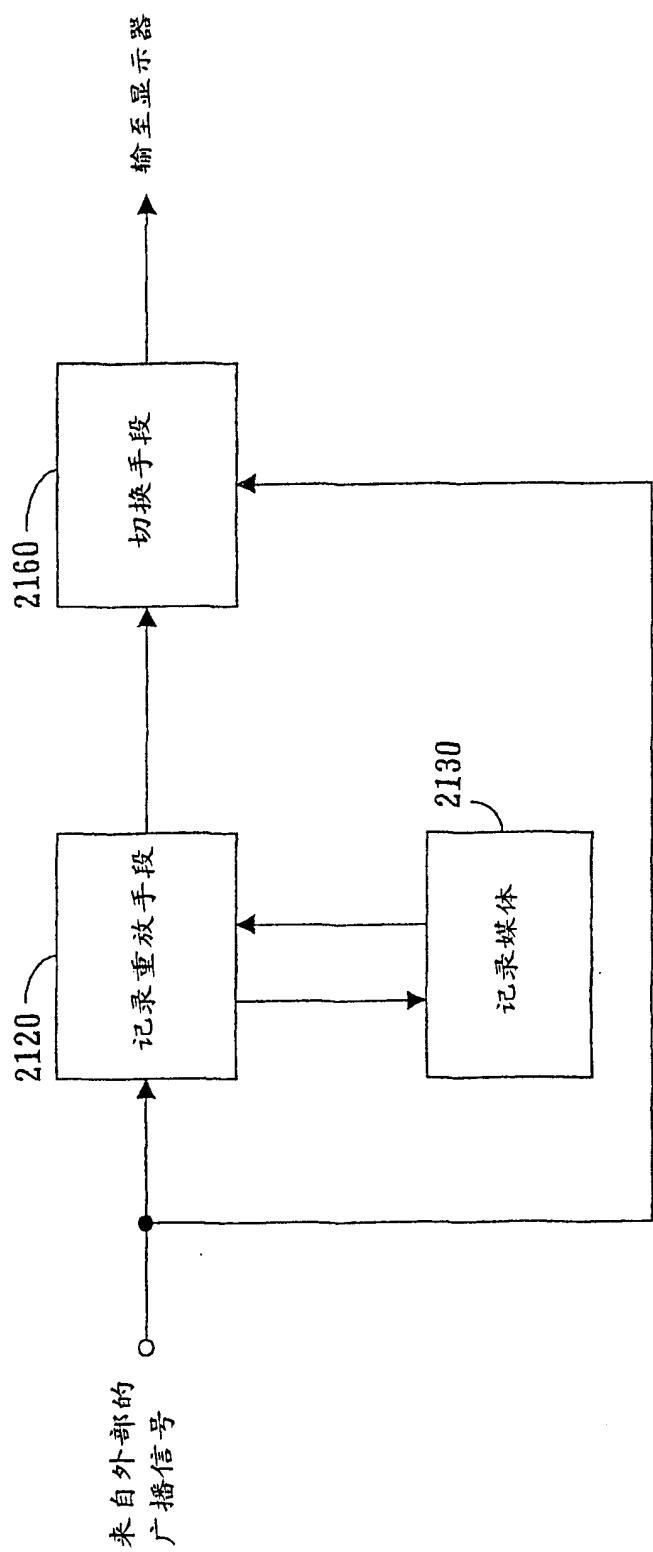


图 4.3
冬