(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101292292 B
(45)授权公告日 2012.12.12

(21)申请号 200680038733.8
(22)申请日 2006.10.17
(30)优先权数据
0510566 2005.10.17 FR
(85)PCT申请进入国家阶段日
2008.04.17
(86)PCT申请的申请数据
PCT/FR2006/002328 2006.10.17
(87)PCT申请的公布数据
WO2007/045756 FR 2007.04.26
(73)专利权人 汤姆森许可贸易公司
地址 法国布洛涅－比郎库尔
(72)发明人 让－路易·迪亚斯科恩 阿兰·迪尔西尔万·勒列夫尔
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 罗松梅
(51)Int.Cl.
G11B 20/00(2006.01)
G11B 20/10(2006.01)
H04N 21/254(2011.01)
H04N 21/835(2011.01)
(56)对比文件
US 2005169118 A1,2005.08.04,【0030】-【0042】段、【0047】-【0053】段、【0073】-【0094】段,附图 1-4、7、8.
CN 1656803 A,2005.08.17, 全文.
审查员 马京京

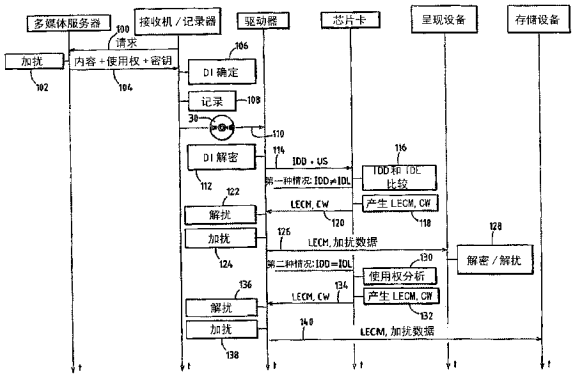
权利要求书 3 页 说明书 8 页 附图 3 页

(54)发明名称

记录并安全分发数字数据的方法、访问设备和记录器

(57)摘要

本发明涉及一种接收并安全记录代表多媒体内容的数字数据的方法，包括如下步骤：由属于确定安全域的记录器／接收机(6,28)在安全盘(30)上记录所述数字数据，所述安全域包括多个设备项目并由标识符(IDD)定义(108)；在安全盘(30)上记录(108)记录器／接收机(6,28)的域标识符(IDD)，以将所述域定义为被授权对多媒体内容进行再现／复制的唯一域；该方法的特征在于，还包括从安全盘(30)恢复盘密钥(DK)的在前步骤，并且由盘密钥(DK)对域标识符(IDD)进行加密，由标题密钥对所记录的数字数据进行加扰，标题密钥由所述盘密钥来加密。本发明还涉及一种安全分发数字数据的方法、一种访问设备和一种记录器／接收机。



CN 101292292 B

1. 一种接收并安全记录代表多媒体内容的数字数据的方法，包括如下步骤：

- 由属于确定安全域的记录器 / 接收机 (6,28) 在安全盘 (30) 上记录所述数字数据，所述确定安全域包括多个设备项目，并且由所述确定安全域的所有设备特有的第一域标识符 (IDD) 来定义 (108)；

- 在所述安全盘 (30) 上记录 (108) 所述记录器 / 接收机 (6,28) 的第一域标识符 (IDD)，以将所述确定安全域定义为授权对多媒体内容进行再现 / 复制的唯一域；

其特征在于，所述盘由用于可记录媒体的数据保护系统来保护，所述第一域标识符 (IDD) 由域中的数据保护系统来定义，所述方法还包括根据所述用于可记录媒体的数据保护系统从所述安全盘 (30) 恢复盘密钥 (DK) 的在前步骤，并且由所述盘密钥 (DK) 对第一域标识符 (IDD) 进行加密，其中由标题密钥对所记录的数字数据进行加扰，所述标题密钥由所述盘密钥 (DK) 来加密。

2. 根据权利要求 1 所述的接收和安全记录的方法，其特征在于，还包括步骤 (108)：在所述安全盘 (30) 上记录多媒体内容所附属的再现权 (US)，所述再现权 (US) 定义多媒体内容是否可自由地再现 / 复制、多媒体内容是否仅在所述确定安全域中才能再现 / 复制、或者多媒体内容是否为不可再现 / 复制。

3. 一种安全分发代表多媒体内容的数字数据的方法，其特征在于，所述方法包括如下步骤：

- 根据用于可记录媒体的数据保护系统从记录器 / 接收机 (6,28) 接收并在安全盘 (30) 上记录 (108) 代表多媒体内容的数字数据，该记录步骤由根据权利要求 1 或 2 所述的接收和记录方法来执行；以及

- 在由根据域中的数据保护系统的第二域标识符 (IDL) 定义的特定安全域中，从用于访问所述特定安全域的访问设备 (40,42,44)，安全供应 (118,122,124,128,130,132,136,138) 所述已记录的数字数据，所述访问设备 (40,42,44) 包括用于存储所述特定安全域的第二域标识符 (IDL) 的装置 (56)，

所述供应步骤包括如下步骤：

- 由所述访问设备 (40,42,44) 在所述安全盘 (30) 上读取 (112) 确定安全域的第一域标识符 (IDD)；

- 把在所述安全盘 (30) 上读取的第一域标识符 (IDD) 与在所述访问设备 (40,42,44) 的存储装置 (56) 中存储的第二域标识符 (IDL) 进行比较 (116)；

- 当在所述安全盘 (30) 上读取的第一域标识符 (IDD) 与在所述访问设备 (40,42,44) 的存储装置 (56) 中存储的第二域标识符 (IDL) 不对应时，由所述访问设备 (40,42,44) 供应 (118,122,124,128) 数字数据，以授权数字数据的第一操作模式；以及

- 当在所述安全盘 (30) 上读取的第一域标识符 (IDD) 与在所述访问设备 (40,42,44) 的存储装置 (56) 中存储的第二域标识符 (IDL) 对应时，由所述访问设备 (40,42,44) 供应 (130,132,136,138) 数字数据，以授权数字数据的第二操作模式。

4. 根据权利要求 3 所述的安全分发方法，其特征在于，当供应数字数据以授权数字数据的第一操作模式时，所述供应步骤包括如下步骤 (124)：根据适当协议，由所述访问设备 (40,42,44) 对数字数据加扰，以禁止对多媒体内容的再现 / 复制，并授权仅当数字数据正在由所述访问设备 (40,42,44) 读取时，才在属于所述特定安全域的呈现设备 (60) 上呈现

多媒体内容。

5. 根据权利要求3或4所述的安全分发方法，其特征在于，当供应数字数据以授权第二操作模式时，所述供应步骤还包括如下步骤：

-在所述安全盘(30)上读取(112)多媒体内容所附属的再现权(US)，所述再现权(US)定义多媒体内容是否可自由再现/复制、多媒体内容是否仅在确定安全域中才能再现/复制、或者多媒体内容是否为不可再现/复制；以及

-根据以在所述安全盘(30)上读取的再现权(US)为依据而定义的协议，由所述访问设备(40,42,44)对数字数据进行加扰(132,138)。

6. 根据权利要求5所述的安全分发方法，其特征在于，当读取的再现权(US)授权仅在所述确定安全域中对多媒体内容进行再现/复制时，所述供应步骤包括如下步骤(138)：根据适当协议，由所述访问设备(40,42,44)对数字数据进行加扰，以授权仅在属于所述确定安全域的设备(60,62)上再现/复制和呈现多媒体内容。

7. 根据权利要求5所述的安全分发方法，其特征在于，当再现权(US)禁止再现/复制多媒体内容时，所述供应步骤包括如下步骤(124)：根据适当协议，由所述访问设备(40,42,44)对数字数据进行加扰，以禁止再现/复制多媒体内容，并仅授权当数字数据正在由所述访问设备(40,42,44)读取时，在属于所述确定安全域的呈现设备(60)上呈现多媒体内容。

8. 根据权利要求5所述的安全分发方法，其特征在于，当再现权(US)授权自由地再现/复制多媒体内容时，所述供应步骤包括如下步骤：根据适当协议，由所述访问设备(40,42,44)对数字数据进行加扰，以授权在任何设备(60,62,64)上再现/复制和呈现多媒体内容。

9. 根据权利要求5所述的安全分发方法，其特征在于，所述方法还包括如下步骤(104)：从远程服务器(10)向所述记录器/接收机(6,28)传输多媒体内容所附属的再现权(US)，在所述安全盘(30)上记录(108)多媒体内容所附属的再现权(US)，该传输步骤(104)在用于记录再现权(US)的步骤(108)之前。

10. 根据权利要求9所述的安全分发方法，其特征在于，所述方法包括对第一域标识符(IDD)和再现权(US)进行加密的步骤(106)，所述加密步骤(106)在记录步骤(108)之前。

11. 一种用于访问特定安全域的访问设备(40,42,44)，所述访问设备(40,42,44)包括：

-用于读取安全盘(30)上记录的代表多媒体内容的数字数据的装置(45)，所述读取装置(45)适于在所述安全盘(30)上读取确定安全域的第一域标识符(IDD)；

-用于存储所述访问设备(40,42,44)所属的特定安全域的第二域标识符(IDL)的装置(56)；

-用于把存储装置(56)中存储的第二域标识符(IDL)与在所述安全盘(30)上读取的第一域标识符(IDD)进行比较、并使用盘密钥(DK)对第一域标识符(IDD)进行解密的装置(56)；

-装置(50)，适于当在所述安全盘(30)上读取的第一域标识符(IDD)与在所述访问设备(40,42,44)的存储装置(56)中存储的第二域标识符(IDL)不对应时，供应数字数据，以授权数字数据的第一操作模式，并且当在所述安全盘(30)上读取的第一域标识符(IDD)与

在所述访问设备 (40,42,44) 的存储装置 (56) 中存储的第二域标识符 (IDL) 对应时,供应数字数据,以授权数字数据的第二操作模式 ;

其特征在于,所述盘由用于可记录媒体的数据保护系统来保护,所述第一域标识符 (IDD) 由域中的数据保护系统来定义,所述访问设备 (40,42,44) 还包括 :

- 加密 / 解密装置 (48),适于从所述安全盘 (30) 恢复盘密钥 (DK),并使用所述盘密钥 (DK) 对第一域标识符 (IDD) 进行解密 ;以及

- 加扰 / 解扰装置 (50),能够使用所述盘密钥 (DK) 对所述安全盘 (30) 上记录的数字数据进行解扰。

12. 一种属于确定安全域的记录器 / 接收机 (6,28),所述安全域包括多个设备项目并由所述确定安全域的所有设备特有的第一域标识符 (IDD) 来定义 ;所述记录器 / 接收机 (6,28) 适于在安全盘 (30) 上记录代表多媒体内容的数字数据 ;所述记录器 / 接收机 (6,28) 适于在所述安全盘 (30) 上记录所述记录器 / 接收机 (6,28) 的第一域标识符 (IDD),以将所述确定安全域定义为被授权对多媒体内容进行再现 / 复制的唯一域,

其特征在于,所述盘由用于可记录媒体的数据保护系统来保护,所述第一域标识符 (IDD) 由域中的数据保护系统来定义,所述记录器 / 接收机 (6,28) 适于从所述安全盘 (30) 恢复盘密钥 (DK),通过由所述盘密钥 (DK) 加密的标题密钥对数字数据进行加扰,使用所述盘密钥 (DK) 对第一域标识符 (IDD) 进行加密,并记录所述已加扰的数字数据和所述已加密的第一域标识符 (IDD)。

13. 根据权利要求 12 所述的记录器 / 接收机 (6,28),其特征在于,所述记录器 / 接收机 (6,28) 适于记录多媒体内容所附属的再现权 (US),所述再现权 (US) 定义多媒体内容是否可自由再现 / 复制、多媒体内容是否仅在确定安全域中才能再现 / 复制的、或者多媒体内容是否为不可再现 / 复制。

14. 根据权利要求 13 所述的记录器 / 接收机 (6,28),其特征在于,多媒体内容所附属的再现权 (US) 包括允许对多媒体数据进行再现的次数。

记录并安全分发数字数据的方法、访问设备和记录器

技术领域

[0001] 本发明涉及记录、提供和安全分发代表多媒体内容的数字数据的方法。

背景技术

[0002] 为了避免非法复制多媒体内容，文献 JP 2001/195826 公开了一种设备，其包括用于存储标识符的存储器，该标识符对于每一个设备是特定的，并与其他设备的标识符不同。该设备适于在每次记录时，将数字数据和自身的标识符存储在存储介质上。在读取数字数据前，将其标识符与在存储介质上读取的标识符相比较，并且仅在存储介质上存储的标识符对应于其标识符时，才呈现数字数据。

[0003] 这种设备遵守产权，但是允许数字数据只在唯一的设备上呈现。

[0004] 为了能够更广泛地分发数字数据，同时遵守数字数据所附属的产权，公知的是通过内容加扰系统 (CSS) 方法之类的数据保护方法来保护在安全 DVD 上记录的数字数据。

[0005] 但是，对于这种方法，记录在安全 DVD 上的数字数据可以被任何授权的驱动器读取，但不能被复制或再现。

[0006] 此外，域 (domain) 中的数据保护方法是已知的，例如文献“SmartRight Technical white paper, Version 1.7, January 2003, Thomson”中描述的具有注册商标“SmartRight”的方法；以及文献“xCPCluster Protocol, IBM Presentation to Copy Protection Technical WorkingGroup, July 18, 2002”中描述的具有注册商标“eXtensible ContentProtection”的方法。这些方法能够根据加密协议对数字数据进行加扰，其只能由属于同一域的设备来解码。适当加密的数字数据只能由属于域的设备来呈现或复制 / 再现。

[0007] 但是，该数字数据无法与未访问该域的人共享。因此，不可能与朋友或熟人共享该数字数据。

[0008] 特别地，根据美国文献 2004/0230532 还可知道一种数字数据复制管理系统，其能够通过同一记录器对数字数据进行一次或更多次再现 / 复制，但是禁止另一记录器进行复制。

[0009] 该系统包括经由互联网可访问的服务器以及针对用户的特定记录器 / 驱动器。每次记录时，每个记录器 / 驱动器适于向服务器传输对于自身特定的标识符、DVD 的标识符和 DVD 上读取的内容的标识符。该服务器包含数据库、用于登记记录器接收到的标识符的装置、以及将数据库中存储的标识符与记录器接收到的标识符相比较以检查由记录器发送的标识符是否与数据库中已存储的标识符相对应的装置。

[0010] 但是，该系统十分复杂，需要对包含大量数据的数据库进行管理。

发明内容

[0011] 本发明的目的是提供一种安全分发数字数据的方法，该方法能够在一定程度上共享数字数据，同时遵守数字数据所附属的产权。

[0012] 为此，本发明的主题是一种接收并安全记录代表多媒体内容的数字数据的方法，包括如下步骤：由属于确定安全域的记录器／接收机在安全盘上记录所述数字数据，所述确定安全域包括多个设备项目，并且由所述域的所有设备特有的标识符来定义；在所述安全盘上记录所述记录器／接收机的域标识符，以将所述域定义为授权对多媒体内容进行再现／复制的唯一域；所述方法的特征在于，还包括从所述安全盘恢复盘密钥的在前步骤，并且由所述盘密钥对域标识符进行加密，由标题密钥对所记录的数字数据进行加扰，所述标题密钥由所述盘密钥来加密。

[0013] 根据具体实施例，该接收和记录方法还包括步骤：在所述安全盘上记录多媒体内容所附属的再现权，所述再现权定义多媒体内容是否可自由地再现／复制、多媒体内容是否仅在所述确定域中才能再现／复制、或者多媒体内容是否为不可再现／复制。

[0014] 根据第二方面，本发明还涉及一种安全分发代表多媒体内容的数字数据的方法，包括如下步骤：

[0015] －从记录器／接收机接收并在安全盘上记录代表多媒体内容的数字数据，该记录步骤由上述接收和记录方法执行；以及

[0016] －在由标识符定义的特定安全域中，从用于访问所述特定安全域的设备，安全供应所述已记录的数字数据，所述用于访问所述特定安全域的设备包括用于存储该特定域的标识符的装置，所述供应步骤包括如下步骤：

[0017] －由访问设备在所述安全盘上读取确定安全域的标识符；

[0018] －把在所述安全盘上读取的标识符与在访问设备的存储装置中存储的标识符进行比较；

[0019] －当在所述安全盘上读取的标识符与在访问设备的存储装置中存储的标识符不对应时，由访问设备供应数字数据，以授权数字数据的第一操作模式；以及

[0020] －当在所述安全盘上读取的标识符与在访问设备的存储装置中存储的标识符对应时，由访问设备供应数字数据，以授权数字数据的第二操作模式。

[0021] 根据具体实施例，该分发方法包括如下特征中的一个或更多个：

[0022] －当供应数字数据以授权数字数据的第一操作模式时，所述供应步骤包括如下步骤：根据适当协议，由访问设备对数字数据加扰，以禁止对多媒体内容的再现／复制，并授权仅当数字数据正在由访问设备读取时，才在属于所述特定域的呈现设备上呈现多媒体内容；

[0023] －当供应数字数据以授权数字数据第二操作模式时，该供应步骤包括如下步骤：

[0024] －由访问设备读取预先记录在所述安全盘上的再现权；

[0025] －在所述安全盘上读取多媒体内容所附属的再现权，所述再现权定义定义多媒体内容是否可自由地再现／复制、多媒体内容是否仅在所述确定域中才能再现／复制、或者多媒体内容是否为不可再现／复制；以及

[0026] －根据以在所述安全盘上读取的再现权为依据而定义的协议，由访问设备对数字数据进行加扰；以及

[0027] －当读取的再现权授权仅在所述确定域中对多媒体内容进行再现／复制时，所述供应步骤包括如下步骤：根据适当协议，由访问设备对数字数据进行加扰，以授权仅在属于所述确定域的设备上再现／复制和呈现多媒体内容；

[0028] - 当再现权禁止再现 / 复制多媒体内容时，所述供应步骤包括如下步骤 :根据适当协议，由访问设备对数字数据进行加扰，以禁止再现 / 复制多媒体内容，并仅授权当数字数据正在由访问设备读取时，在属于所述确定域的呈现设备上呈现多媒体内容 ;

[0029] - 当再现权授权自由地再现 / 复制多媒体内容时，所述供应步骤包括如下步骤 :根据适当协议，由访问设备对数字数据进行加扰，以授权在任何设备上再现 / 复制和呈现多媒体内容 ;

[0030] - 该方法还包括如下步骤 :从远程服务器向所述记录器 / 接收机传输多媒体内容所附属的再现权，该传输步骤在用于记录再现权的步骤之前 ;以及

[0031] - 该方法包括对标识符和再现权进行加密的步骤，所述加密步骤在记录步骤之前。

[0032] 根据第三方面，本发明还涉及一种用于访问特定安全域的设备，该访问设备包括 :

[0033] - 用于读取安全盘上记录的代表多媒体内容的数字数据的装置，所述读取装置适于在所述安全上读取确定安全域的标识符 ;

[0034] - 用于存储所述访问设备所属的特定域的标识符的装置 ;

[0035] - 用于把存储装置中存储的标识符与在所述安全盘上读取的标识符进行比较、并使用盘密钥对域标识符进行解密的装置 ;

[0036] - 装置，适于当在所述安全盘上读取的标识符与在所述访问设备的存储装置中存储的标识符不对应时，供应数字数据，以授权数字数据的第一操作模式，并且当在所述安全盘上读取的标识符与在所述访问设备的存储装置中存储的标识符对应时，供应数字数据，以授权数字数据的第二操作模式 ;其特征在于，所述访问设备还包括 :

[0037] - 加密 / 解密装置，适于从所述安全盘恢复盘密钥，并使用所述盘密钥对域标识符进行解密 ;以及

[0038] - 加扰 / 解扰装置，能够使用所述盘密钥对所述安全盘上记录的数字数据进行解扰。

[0039] 根据第四方面，本发明还涉及一种属于安全域的记录器 / 接收机，所述安全域包括多个设备项目并由所述域的所有设备特有的标识符来定义 ;所述记录器 / 接收机适于在安全盘上记录代表多媒体内容的数字数据 ;所述记录器 / 接收机适于在所述安全盘上记录所述记录器 / 接收机的域标识符，以将所述域定义为被授权对多媒体内容进行再现 / 复制的唯一域，其特征在于，所述记录器 / 接收机适于从所述安全盘恢复盘密钥，通过由所述盘密钥加密的标题密钥对数字数据进行加扰，使用所述盘密钥对标识符进行加密，并记录所述已加扰的数字数据和所述已加密的标识符。

[0040] 根据具体实施例，该记录器 / 接收机包括如下特征中的一个或更多个 :

[0041] - 所述记录器 / 接收机适于记录多媒体内容所附属的再现权，所述再现权定义多媒体内容是否可自由地再现 / 复制、多媒体内容是否仅在所述确定域中才能再现 / 复制、或者多媒体内容是否为不可再现 / 复制 ;以及

[0042] - 多媒体内容所附属的再现权包括允许对多媒体数据进行再现的次数。

附图说明

[0043] 通过阅读如下仅作为示例给出的描述并参照附图，将更好地理解本发明，附图

中：

[0044] - 图 1 是能够实施根据本发明的分发方法的系统的一部分的功能框图；

[0045] - 图 2 是能够实施根据本发明的分发方法的系统的另一部分的功能框图；以及

[0046] - 图 3 是示出了根据本发明的分发方法的步骤的图。

具体实施方式

[0047] 图 1 和 2 示出了用于实施本发明方法的系统 2。系统 2 涉及一组 IT 设备项目，这些设备项目具有 DVD 记录器或 DVD 驱动器，属于不同用户，并很可能交换 DVD。这些设备项目在不同的安全域之间分配。

[0048] 属于一个安全域的设备项目均在存储器中具有代表该域的同一标识符以及域密钥。该域中的设备可以通过网络来传送由该域密钥加扰的数字数据。不属于该安全域或属于另一安全域的设备无法通过该网络读取加扰数据或在网络中的设备上保护的加扰数据。

[0049] 从图 1 可见，系统 2 包括内容提供方 4，适于通过诸如互联网之类的分发网络 8 向接收机设备 6 提供数字数据。

[0050] 内容提供方 4 包括与数据库 12 链接的多媒体服务器 10。

[0051] 数据库 12 适于存储代表多媒体内容的数字数据，例如，音频、视频或文本数据序列，或者用于设置软件的计算机数据文件。

[0052] 例如，根据 MPEG-2 标准 (ISO/IEC 13818-1)，将数字数据以分组形式编码。

[0053] 在数据库 12 中，每个多媒体内容与一个或更多个使用权或再现权相关联，并与依据这些使用权或权限而变化的价格相关联。

[0054] 这些使用权标识了多媒体内容的复制或再现所附属的保护的类型。在所述实施例的示例中，使用权定义了多媒体内容是可自由地复制 / 再现、或是可以复制到安全 DVD 中、还是既可复制到安全 DVD 中又可在与在安全 DVD 上记录该内容的记录器所属的域相对应的单个域中复制 / 再现。

[0055] 多媒体服务器 10 包括向分发网络 8 发送数字数据或从该网络接收数字数据的装置 14、以及对该数字数据进行加扰的模块 16。

[0056] 加扰模块 16 适于根据 CSS 系统对数据进行加扰。

[0057] 接收机设备 6 是计算机或机顶盒。它通常安装在想要通过分发网络 8 访问视频节目的用户的家中。

[0058] 接收机设备 6 属于由诸如具有注册商标 SmartRight 的系统之类的保护系统保护的域。

[0059] 属于该安全域的设备项目均在存储器中具有代表该域的同一标识符 IDD 以及域密钥 DIK。

[0060] 接收机设备 6 具有处理器 18、加密 / 解密模块 20、键盘、屏幕或遥控类型的用户接口 22、以及用于发送或接收数据的网络接口 24。

[0061] 处理器 18 适于执行 SmartRight 数据保护系统的协议以及与加扰模块 16 所用的保护系统相对应的 CSS 保护系统的协议。为此，处理器 18 具体包括主密钥 MK 以及接收机设备 6 所属的域的标识符 IDD。

[0062] 接口 24 适于通过实时下载（或流），从分发网络 8 接收数据流，即，通过在下载的

同时观看内容，或者通过预先下载以使得能够离线观看内容。

[0063] 接收机设备 6 与例如 DVD-R、DVD-RW、DVD+R、DVD+RW 或 DVD-RAM 类型的 DVD 30 的记录器 28 链接。

[0064] DVD 30 包括预先记录有根据 CSS 保护系统的协议而保护的一组盘密钥的起始区 32、存储区 34 和数字数据记录区 36。

[0065] 存储区 34 是 DVD 上可以由任何记录器进行记录的特定区。对于 DVD-R 类型的 DVD，存储区 34 包括例如称作 RMD 区域 (field)2 的区域。在文献“DVD Specifications for Recordable Disk for General，Part 1，Physical Specifications，Version 2.0，May 2000”中定义了该区域。

[0066] 从图 2 可见，根据本发明的系统 2 还包括 DVD 驱动器 40，其构成对 SmartRight 保护系统所保护的域进行访问的设备。该驱动器 40 与设计用于容纳芯片卡 44 的芯片卡读取器 42 相链接。

[0067] 驱动器 40 包括用于读取 DVD 的装置 45、以及与加密 / 解密模块 48 连接的用于存储主密钥 MK’ 的装置 46。

[0068] 驱动器 40 还包括加扰 / 解扰模块 50、以及通过诸如国内网 (domestic network)、内联网 (intranet) 或互联网等分发网络 54 来发送和接收数字数据的网络接口 52。

[0069] 芯片卡 44 包含安全处理器 56。该处理器 56 适于安全地存储对于驱动器 40 所属的域特定的标识符 IDL 以及该域的加密密钥 DOK。

[0070] 处理器 56 适于比较数据、从驱动器 40 接收数据并向驱动器 40 发送数据、产生随机数并根据 SmartRight 保护协议进行编码。

[0071] 系统 2 还包括电视类型的呈现设备 60、记录器 62 和存储设备 64。

[0072] 呈现设备 60 和记录器 62 均包括网络接口 70 和 72，该接口用于从驱动器 40 接收数字数据或者在存储设备 64 上搜索数字数据。呈现设备 60 和记录器 62 属于与驱动器 40 所属相同的安全域。

[0073] 呈现设备 60 包括解扰模块 66。其与容纳芯片卡 47 的芯片卡读取器 43 连接，该芯片卡 47 在安全处理器 57 中存储该域的标识符 IDL 和加密密钥 DOK。

[0074] 存储设备 64 可以由与分发网络 54 连接的任何设备来访问，特别地，还可以由不属于标识符 IDL 所定义的域的设备来访问。

[0075] 在图 3 中，纵轴表示时间轴，水平线示出了图 1 和 2 中表示的系统的设备项目之间的交换。

[0076] 在第一步骤 100，用户使用接收机设备的用户接口 22 来选择视频序列，例如他想要记录在 DVD 30 上的电影或特定传输。

[0077] 记录器 28 读取在 DVD 的起始区 32 上记录的所有安全盘密钥，并将这组安全盘密钥传输至接收机设备 6。

[0078] 接收机设备 6 的加密 / 解密模块 20 从这组安全密钥和主密钥 MK 中恢复盘密钥 DK。

[0079] 然后，接收机设备 6 创建要发送至多媒体服务器 10 的地址的视频内容请求消息。该请求包含所订购的视频序列的标识符、接收机设备 6 的标识符、刚刚获得的盘密钥 DK、对所请求的使用权的指示以及支付指令。

[0080] 在下一步骤 102，多媒体服务器 10 在数据库 12 中搜索所请求的视频内容，使用标题密钥对其进行加扰，并使用根据 CSS 协议所接收的盘密钥 DK 对标题密钥进行加密。

[0081] 在步骤 104，多媒体服务器 10 向接收机设备 6 传输由经盘密钥 DK 加密的标题密钥而加扰的视频内容、以及对用户购买的使用权的指示。

[0082] 在步骤 106 中，接收机设备的加密 / 解密模块 20 确定并加密域信息 DI。该域信息 DI 包括用户购买的使用权和接收机设备所属的域的标识符 IDD。

[0083] 例如，域信息 DI 采用如下形式：

[0084] DI = AES[DDK](IDD ‖ US)

[0085] - 其中 AES 是加密标准（先进加密标准）；

[0086] -“‖”是拼接运算符；

[0087] -DDK 是适用于 AES 加密标准的密钥，从盘密钥 DK 中导出，例如，通过将比特“0”与密钥 DK 的低位比特拼接来获得具有 AES 所要求尺寸的密钥；

[0088] -IDD 是接收机设备所在域的标识符；

[0089] -US 是视频内容所附属的使用权的 SmartRight 格式的转录 (transcription)。

[0090] 在步骤 108，记录器 28 在数据记录区 36 上记录加扰的视频内容，并在存储区 34 上记录域信息 DI。

[0091] 由此，用户具有包括视频内容和标识符 IDD 的 DVD 30，该视频内容是根据 CSS 规范而保护的，该标识符 IDD 描述已记录多媒体内容以及 DVD 所附属的特定域的特征。

[0092] 在步骤 110 中，用户想要使下载的视频内容对于标识符 IDL 所定义的域中的设备是可用的。

[0093] 为此，将 DVD 30 插入属于该域的驱动器 40 中。该驱动器的读取装置 45 读取该 DVD 的起始区 32 中的所有安全盘密钥、以及该 DVD 的存储区 34 中存储的域信息 DI。

[0094] 在步骤 112 中，加密 / 解密模块 48（根据 CSS 规范的原理）从这组安全盘密钥和驱动器 40 中包含的主密钥 MK’中恢复盘密钥 DK。从该盘密钥 DK 中推断出导出密钥 DDK，并使用该密钥 DDK 对域信息 DI 进行解密，以恢复对 DVD 30 进行记录的域的使用权 US 和标识符 IDD。

[0095] 在步骤 114 中，驱动器 40 向芯片卡 44 传输使用权 US 和标识符 IDD。

[0096] 在步骤 116 中，芯片卡的处理器 56 检查 DVD 上记录的标识符 IDD 是否对应于其存储的标识符 IDL。

[0097] 如果 DVD 30 上记录的标识符 IDD 与芯片卡的标识符 IDL 不对应，则 DVD 30 不是由与驱动器 40 属于同一域的记录器所记录的。

[0098] 在这种情况下，在步骤 118 中，芯片卡的处理器 56 产生控制字（一般表示为 CW）和控制消息（表示为 LECM（本地授权控制消息））。控制消息 LECM 包括控制字 CW、驱动器 40 所属域的标识符 IDL、完整性检查和由完整性计算所保护的使用权 US，其中该控制字 CW 被加密，使得仅可使用域密钥 DOK 对其进行解密。这些控制消息 LECM 只能由与驱动器 40 属于同一域的设备解密。

[0099] 当标识符 IDD 不同于标识符 IDL 时，对控制消息 LECM 中包含的控制字 CW 进行超加密 (superencrypt)。

[0100] 根据 SmartRight 域保护协议，包括有超加密控制字 CW 的控制消息 LECM 向接收这

些控制消息 LECM 以及这些控制消息所附属的数字数据的任何设备指示：所接收的数字数据只能在读取 DVD 时被呈现，并且不能被复制或再现。

[0101] 在步骤 120 中，芯片卡的处理器 56 向驱动器 40 传输已产生的控制消息 LECM 和控制字 CW。

[0102] 在步骤 122 中，驱动器的加扰 / 解扰模块 50 使用在步骤 112 获得的密钥 DK，对在 DVD 的区 36 上记录的数字数据进行解扰。

[0103] 在步骤 124 中，驱动器的加扰 / 解扰模块 50 使用由芯片卡的处理器 56 产生的控制字 CW，对在步骤 122 中解扰的数字数据进行加扰。

[0104] 在步骤 126 中，驱动器 40 通过分发网络 54 向呈现设备 60 传输使用控制字 CW 加扰的数字数据以及由处理器 56 产生的控制消息 LECM。

[0105] 在步骤 128 中，与呈现设备 60 连接的芯片卡的处理器 57 对控制消息 LECM 进行解密，并且解扰模块 66 对接收的数字数据进行解扰，以使设备显示通过网络 54 传输的视频。

[0106] 因此，呈现设备 60 在驱动器 40 对 DVD 30 进行读取的同时显示视频内容。

[0107] 记录器 62 也访问通过分发网络 54 传输的数字数据。但是，为了方便用户，记录器 62 可以阻止该数据的再现或向 DVD 的复制，因为如果进行该复制，由于控制字 CW 是被超加密的，所以该复制是不可用的。

[0108] 该数字数据呈现模式在 SmartRight 协议中被称为协议名称“只看 (view only)”，并在文献“SmartRight Technical white paper, Version1.7, January 2003, Thomson”中有具体描述。

[0109] 当标识符 IDD 等于标识符 IDL 时，在步骤 130 中，芯片卡的处理器 56 在记录 DVD 时分析所购买的使用权 US。

[0110] 当这些使用权允许仅在一个域中再现或复制视频内容时，处理器 56 在步骤 132 中产生控制字 CW 以及包含这些控制字 CW 的控制消息 LECM，该控制消息 LECM 是由域密钥 DOK 加密的，从而只能由与驱动器 40 属于同一域（即，属于标识符 IDL ＝ IDD 并包括域密钥 DOK 的域）的设备进行解密。

[0111] 在步骤 134 中，将控制消息 LECM 和控制字 CW 传输至驱动器 40。

[0112] 在步骤 136 中，根据在步骤 122 中描述的相同方法，对 DVD 上读取的数字数据进行解扰。

[0113] 在步骤 138 中，由在步骤 132 中产生的控制字 CW 对在步骤 136 中解扰的数字数据进行加扰。

[0114] 在步骤 140 中，通过分发网络 54 向存储设备 64 传输加扰的数字数据和控制消息 LECM，并将其记录在存储设备 64 中。

[0115] 只有与驱动器 40 属于同一域的设备才可以对控制消息 LECM 进行解密，并再现 / 复制或呈现在设备 64 上存储的数字数据。

[0116] 在步骤 130 中，如果经分析的使用权定义了数字数据是可自由复制 / 再现的，则芯片卡的处理器 56 产生包含有未加密控制字的控制消息 LECM。

[0117] 然后，重复步骤 134 到 140。但是在这种情况下，任何设备，甚至不属于标识符 IDD ＝ IDL 的域的设备都可以读取、呈现或复制数字数据，这是因为数字数据未由安全密钥进行加扰。

[0118] 在步骤 130 中，如果处理器 56 确定数字数据是不可再现 / 复制的，则其产生控制消息 LECM 和经过超加密的控制字 CW，并重复步骤 120 到 128。在这种情况下，数字数据仍然可由属于标识符 IDL 所标识的域的呈现设备来呈现。

[0119] 还可以在根据文献“xCP :eXtensible Content Protection，2003，IBM”和“xCP Cluster Protocol，IBM Presentation to Copy ProtectionTechnical Working Group，July 18，2002”中描述的具有注册商标 xCP(eXtensible Content Protection) 的方法所保护的域保护系统中实施根据本发明的方法。

[0120] 根据该域保护方法，每一个域或设备群由称作“簇 (cluster)ID”的群标识符 ID 来定义。

[0121] 记录器包括存储该群标识符 ID 并适于计算域信息 DI 的装置。通过向包括 DVD 的盘密钥 DK、群标识符 ID 和复制指示符的拼接数据应用散列函数，来获得该信息 DI，其中复制指示符能够依据该复制是否被授权而采用值 0 或 1。

[0122] 记录器适于在 DVD 上记录域信息 DI。

[0123] 接收所记录的 DVD 的接收机设备通过创建自身的域信息 DI’，来确定 DVD 是否已在其域中记录。为此，接收机设备再使用其自身域的标识符，将复制指示符设置为对应于授权复制的值，并再使用在 DVD 上读取的盘密钥 DK。

[0124] 如果 DVD 的域信息 DI 与由此创建的接收机设备的域信息 DI’相对应，则授权该复制，接收机设备根据该域的 xCP 协议解扰并之后加扰数字数据。

[0125] 如果域信息 DI 与由此创建的接收机设备的域信息 DI’不对应，则禁止进行复制操作。

[0126] 作为变体，可以将该安全分发方法与根据 CPPM(预录媒体内容保护) 系统、CPRM(可记录媒体内容保护) 系统、针对蓝光盘的 BDCPS 系统 (蓝光盘副本保护系统) 或针对 DVD+R/DVD+RW 盘的 Vidi 系统而保护的 DVD 一起使用。

[0127] 作为变体，记录器在 DVD 上只记录数字数据和域标识符，而不记录数字数据所附属的使用权或再现权。在这种情况下，当驱动器读取标识符时，芯片卡根据只允许在盘上所标识的域中进行复制 / 再现的协议，产生控制字和控制消息。当 DVD 不包括标识符时，芯片卡根据阻止任何设备进行复制 / 再现的协议，产生超加密的控制字和控制消息。在这种情况下，数字数据仍然可由属于该域的呈现设备呈现。

[0128] 作为变体，销售以如下形式预先记录的 DVD :该 DVD 包含代表多媒体内容及相关使用权的数字数据。在首次使用该 DVD 之前，并且为了使设备项目能够读取该 DVD，该 DVD 必须放置在记录器中，该记录器适于记录其所属的域的标识符。在这种情况下，调整 DVD 或驱动器，以使其仅在 DVD 包含域标识符时才进行操作。

[0129] 有利地，该安全分发方法允许在一定程度上自由地与朋友或熟人共享数字数据，并与链接至相同域的设备共享，同时保护该数字数据所附属的知识产权。

[0130] 有利地，只能在由已记录有多媒体内容的下载版本和域标识符的安全盘上记录的标识符所定义的域中，读取和呈现已记录有多媒体内容的复制 / 再现的安全盘。但是，可以在任何域中被授权的任何 CSS 呈现设备上读取和呈现前一安全盘，即包含多媒体内容的下载版本和域标识符的盘。

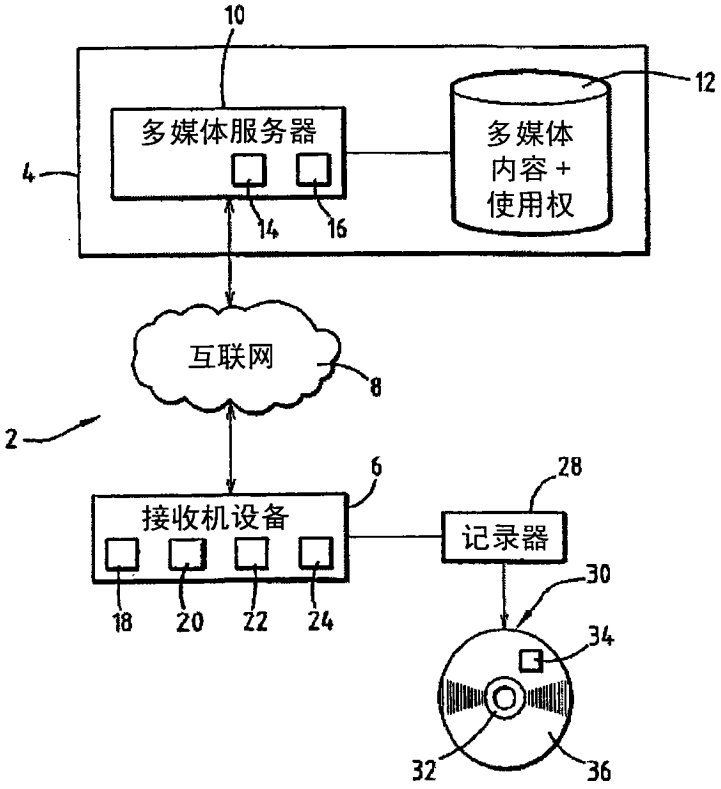

10
12
多媒体服务器
多媒体
内容 +
使用权
4
14
16
互联网
8
2
6
28
接收机设备
记录器
30
34
18
20
22
24
32
36

图 1

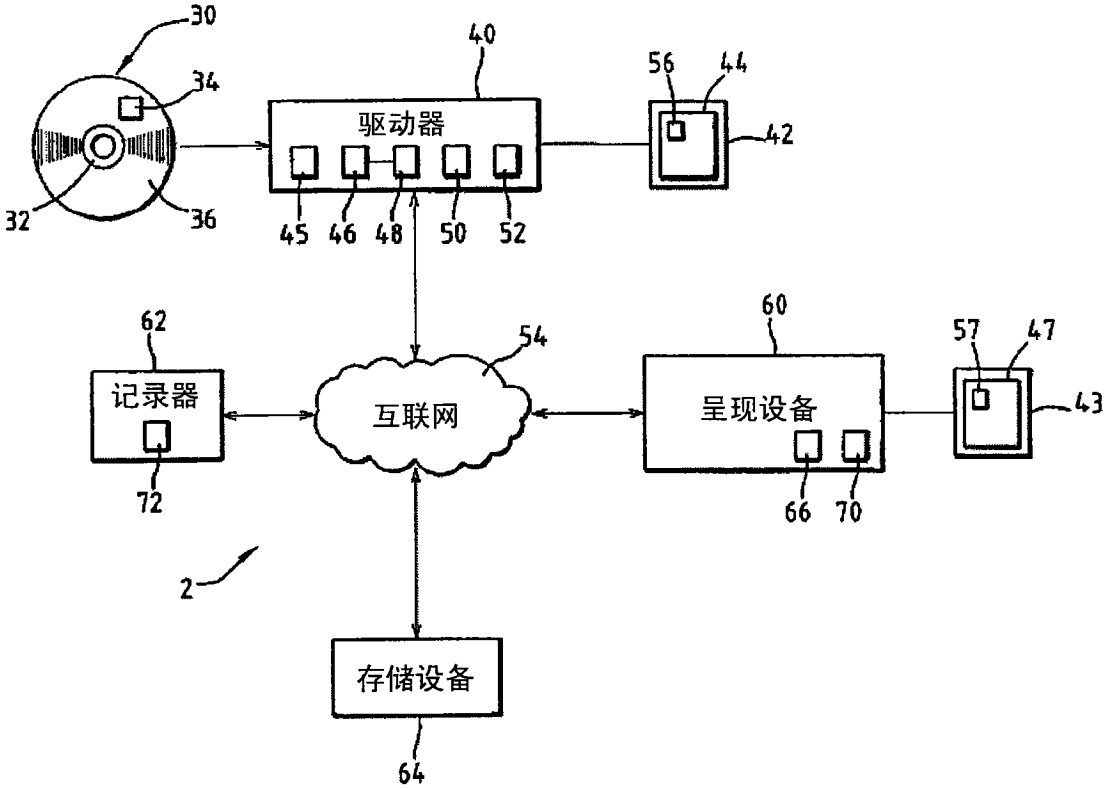

30
34
32
36
40
驱动器
45
46
48
50
52
56
44
42
62
记录器
72
54
互联网
60
呈现设备
66
70
57
47
43
2
存储设备
64

图 2

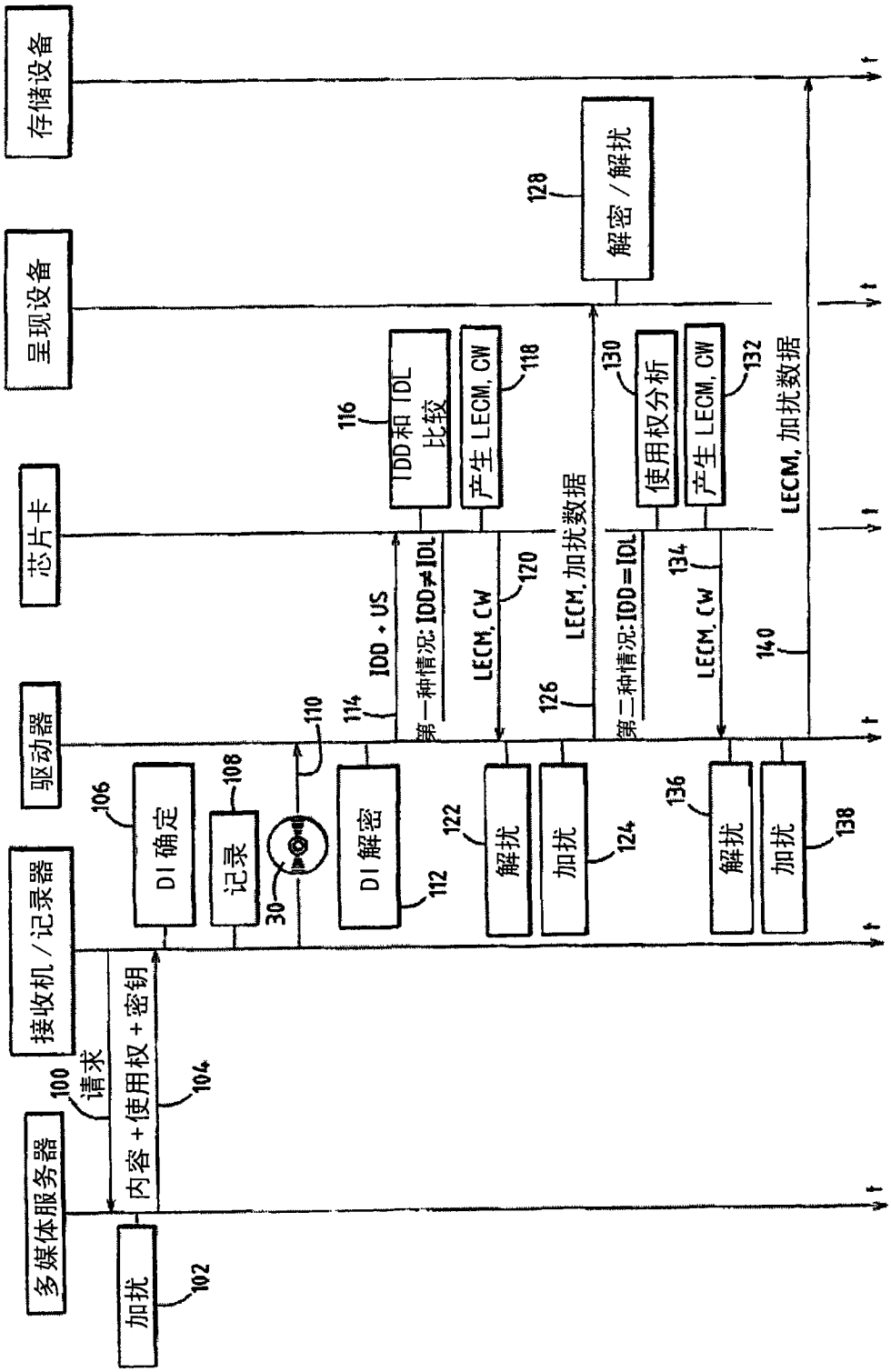

多媒体服务器
接收机／记录器
驱动器
芯片卡
呈现设备
存储设备
加扰
102
请求
100
内容＋使用权＋密钥
104
DI 确定
106
记录
108
30
110
DI 解密
112
IDD • US
114
第一种情况: IDD≠IDL
LECM, CW
120
解扰
122
加扰
124
LECM, 加扰数据
126
TDD和 TDL 比较
116
产生 LECM, CW
118
解密／解扰
128
第二种情况: IDD=IDL
使用权分析
130
产生 LECM, CW
132
LECM, CW
134
解扰
136
加扰
138
LECM, 加扰数据
140

图 3