(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 101426123 B
(45)授权公告日 2011.04.20

(21)申请号 200810177841.4
(22)申请日 2008.09.22
(30)优先权数据
96675/07 2007.09.21 KR
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 裵荣圭 金永执 李炳大 金贤澈 金善美
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 李芳华
(51)Int.Cl.
H04N 21/254(2011.01)
H04N 21/266(2011.01)
H04N 21/4627(2011.01)

审查员 罗坤

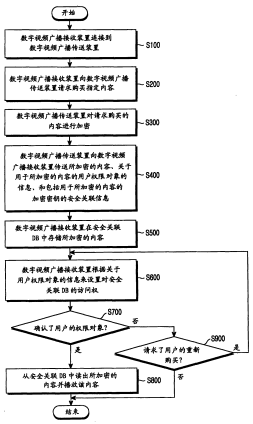
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

用于数字视频广播的数字权限管理的系统和方法

(57)摘要

一种用于数字视频广播(DVB)的数字权限管理(DRM)的系统和方法。用于DVB的DRM的系统包括:数字视频广播传送装置,用于传送DVB的内容和关于该内容的用户权限对象的信息;以及数字视频广播接收装置,用于接收和存储所传送的内容,并根据关于用户权限对象的信息来播放所存储的数据。解决了在DVB期间发生的暗中事后观看问题,并因此有效地保护了DVB内容的数字权限。在解决暗中事后观看问题中,可以使用现有的权限对象和安全关联数据库的构造,而无需添加单独构造。



CN 101426123 B

1. 一种用于数字视频广播 DVB 的数字权限管理 DRM 的系统，包括：

数字视频广播传送装置，用于传送 DVB 的内容和关于该内容的用户权限对象的信息；以及

数字视频广播接收装置，用于接收和存储所传送的内容，并根据关于用户权限对象的信息来播放所存储的数据，

其中数字视频广播接收装置包括：

安全关联数据库 SADB，用于存储从数字视频广播传送装置接收的 DVB 的内容；以及

控制单元，用于根据从数字视频广播传送装置接收的用户权限对象来控制 SADB。

2. 如权利要求 1 所述的系统，其中 DVB 包括：手持数字视频广播 DVB-H、线缆数字视频广播 DVB-C、卫星数字视频广播 DVB-S、和地面数字视频广播 DVB-T 中的一个。

3. 如权利要求 1 所述的系统，其中，根据用户权限对象来控制是否从 SADB 中读出数据。

4. 如权利要求 1 所述的系统，其中，通过设置用于对 SADB 本身的访问权的标记来控制是否从 SADB 中读出数据。

5. 如权利要求 2 所述的系统，其中，数字视频广播传送装置传送通过业务加密密钥 TEK 加密的数据。

6. 如权利要求 5 所述的系统，其中，数字视频广播传送装置安全参数索引 SPI、数字视频广播传送装置和数字视频广播接收装置的因特网协议 IP 信息、TEK 信息、和 TEK 生存期信息，传送作为安全关联 SA 的有关信息。

7. 如权利要求 6 所述的系统，其中，使用 SPI 和 TEK 信息来解密内容。

8. 一种用于数字视频广播 DVB 的数字权限管理 DRM 的方法，包括：

从数字视频广播传送装置向数字视频广播接收装置传送 DVB 的内容和关于该内容的用户权限对象的信息；

在数字视频广播接收装置的安全关联数据库 SADB 中存储 DVB 的数据；

根据所接收的关于权限对象的信息来读出在 SADB 中存储的内容；以及

播放所读出的内容。

9. 如权利要求 8 所述的方法，其中数字视频广播包括：手持数字视频广播 DVB-H、线缆数字视频广播 DVB-C、卫星数字视频广播 DVB-S、和地面数字视频广播 DVB-T 中的任何一个。

10. 如权利要求 8 所述的方法，其中所述根据所接收的关于权限对象的信息来读出在 SADB 中存储的内容的步骤包括：

根据所接收的关于用户权限对象的信息来设置对 SADB 的访问权；以及

根据所设置的访问权来读出在 SADB 中存储的数据。

11. 如权利要求 10 所述的方法，其中当用户权限对象是用于指定时间的权限对象时，根据该指定时间来设置访问权。

12. 如权利要求 8 所述的方法，其中，所述从数字视频广播传送装置向数字视频广播接收装置传送 DVB 的内容和关于该内容的用户权限对象的信息的步骤包括：

数字视频广播传送装置利用业务加密密钥 TEK 来加密 DVB 的内容；以及

向数字视频广播接收装置传送所加密的内容。

13. 如权利要求 12 所述的方法，其中，所述从数字视频广播传送装置向数字视频广播接收装置传送 DVB 的内容和关于该内容的用户权限对象的信息的步骤包括 ：

数字视频广播传送装置传送安全参数索引 SPI、数字视频广播传送装置和数字视频广播接收装置的因特网协议 IP 信息、TEK 信息、和 TEK 生存期信息，作为安全关联 SA 的有关信息。

14. 如权利要求 13 所述的方法，其中所述根据所接收的关于权限对象的信息来读出在 SADB 中存储的内容的步骤包括使用 SPI 和 TEK 信息来解密在 SADB 中存储数据。

15. 如权利要求 14 所述的方法，其中所述播放所读出的内容的步骤包括播放所解密的数据。

用于数字视频广播的数字权限管理的系统和方法

技术领域

[0001] 本发明一般涉及一种用于数字视频广播（DVB）的数字权限管理（DRM， Digital Rights Management）的系统和方法。 更具体地，本发明涉及由开放移动联盟（OMA）制定的 OMA 广播（OMA-BCAST）标准之中的 DVB 技术的 DRM，即，根据内容购买（content purchase）的权限对象（RO）。

[0002] 涉及 OMA-BCAST 标准的 DVB 技术被分类为：应用于便携式接收终端的手持数字视频广播（DVB-H）、应用于线缆（cable）接收终端的线缆数字视频广播（DVB-C）、应用于通过卫星的数字视频广播的卫星数字视频广播（DVB-S）、应用于通过地面波的数字视频广播的地面数字视频广播（DVB-T）等。 可以通过 OMA-BCAST 将本发明应用于所有数字视频广播。

背景技术

[0003] 传统上，当通过数字视频广播（DVB）来提供付费内容时，已应用了用于仅使得已经购买内容的用户能够使用该内容的多种 DRM 技术。在大多数情况下，这样的内容在传送之前被加密。 广播内容以因特网协议（IP）分组的形式在最低层被传送，并且通过使用业务加密密钥（TEK）的 IP 安全（IPSec）方法来加密这个 IP 分组。 如果向 DVB 接收终端提供以流形式的利用 TEK 加密的内容数据，则根据用户的内容购买请求设置的 TEK 生存期（lifetime）信息被添加到利用 TEK 加密的内容的每个数据上。 如果在播放了该内容之后根据 TEK 生存期的时间消逝，则从 DVB 接收终端的存储器中删除该内容以管理数字权限。 该 IPSec 方法需要用于在该内容的 TEK 数据中设置 TEK 生存期信息和利用定时器来操作 TEK 生存期的构造。

[0004] 然而，根据该方法，可能在一个 TEK 数据的转换和下一个 TEK 数据的转换的时间点之间出现时间间隙，即，潜隐期（crypto period）。 考虑到网络延迟，该潜隐期一般被设置为长于 TEK 数据的 TEK 生存期。 然而，为了防止由于这样的网络延迟而造成的广播中断， TEK 生存期应当被设置为长于最初设置的 TEK 生存期。 以供参考，在 OMA-BCAST 标准中，推荐将 TEK 生存期设置为最初设置的 TEK 生存期的三倍。

[0005] 同样，为了克服由于当前 TEK 数据的重放终止而造成的广播中断，内容提供者预先向数字视频广播接收终端传送下一个 TEK 数据。

[0006] 如上所述，即使在内容使用期满之后只要 TEK 生存期被设置为具有边界延长（margin extending）或只要预先提供 TEK 数据，用户就可以另外地观看所购买的内容乃至未购买的内容。 这被称作暗中事后观看（sneak post view）问题。 该暗中事后观看问题在按次付费观看类型的服务中变得更加严重。 例如，实际上尚未购买的整个广播节目可能由于长 TEK 生存期而最终被观看。

[0007] 假设在 DVB 接收终端中接收到具有长潜隐期的内容的 TEK 数据。 在这种情况下，如果当 TEK 数据的重放期满时没有接收到下一个 TEK 数据，则中断该内容的重放以防止流的连续重放。 相应地，内容提供者进一步延长 TEK 数据的生存期以防止广播的中

断，乃至传送下一个 TEK 数据。 结果，即使用户内容的权限对象期满或直到一个 TEK 数据之前，用户也可在与被提供以具有边界的 TEK 生存期差不多的时间中继续观看付费流。

[0008] 如上所述，解决网络延迟的意图导致了关于暗中事后观看的新问题。

发明内容

[0009] 相应地，已经设计本发明以解决在现有技术中出现的以上和其他问题，并提供一种用于数字视频广播 (DVB) 的数字权限管理 (DRM) 的系统和方法。 特别地，本发明提供了一种解决暗中事后观看问题的用于 DRM 的系统和方法。

[0010] 另外，本发明提供了一种用于 DVB 的 DRM 的系统和方法，其可以使用现有的用于内容的用户权限对象和安全关联数据库来解决暗中事后观看问题，而无需添加用于管理 TEK 生存期的单独构造。

[0011] 为了实现上述和其他方面，根据本发明，提供了一种用于 DVB 的 DRM 的系统，其包括：数字视频广播传送装置，用于传送 DVB 的内容和关于该内容的用户权限对象的信息；以及数字视频广播接收装置，用于接收和存储所传送的内容，并根据关于用户权限对象的信息来播放所存储的数据。

[0012] 根据本发明的另一个方面，提供了一种用于 DVB 的 DRM 的方法，其包括：从数字视频广播传送装置向数字视频广播接收装置传送 DVB 的内容和关于该内容的用户权限对象的信息；在数字视频广播接收装置的安全关联数据库 (SADB) 中存储 DVB 的数据；以及根据所接收的关于权限对象的信息来读出并播放在 SADB 中存储的内容。

附图说明

[0013] 通过结合附图的以下详细描述，本发明的以上和其他方面、特征、和优点将变得更加明显，其中：

[0014] 图 1 是图示了根据本发明实施例的用于数字视频广播的数字权限管理的系统的框图；以及

[0015] 图 2 是图示了根据本发明实施例的用于数字视频广播的数字权限管理的方法的流程图。

具体实施方式

[0016] 将在下文中参考附图对本发明的示范实施例进行详细描述。 在该公开中，为了更好地理解本发明，将诸如具体的交通、旅游、或天气信息服务的特定事件作为示例，但是对于本领域的普通技术人员明显的是，本发明可在没有上述特定事件的情况下实现。 同样，当对于与本发明相关的现有技术中的操作或构造的详细描述可能模糊本发明时，将在本公开中省略该详细描述。

[0017] 图 1 是图示了根据本发明实施例的用于数字视频广播 (DVB) 的数字权限管理 (DRM) 的系统的框图。

[0018] 参考图 1，用于 DVB 的 DRM 的系统 100 包括：DVB 传送装置 200 和 DVB 接收装置 300。 更具体地， DVB 传送装置 200 包括：内容存储单元 210、权限对象 (RO) 和

业务加密密钥 (TEK) 编码器 220、RF 单元 230、天线 240、和控制单元 250。 DVB 接收装置 300 包括：天线 310、 RF 单元 320、 RO 解码器 330、安全关联数据库 340、重放单元 350、显示单元 360、和控制单元 370。

[0019] DVB 传送装置 200 广播 DVB 的内容。 根据 OMA-BCAST 标准，该 DVB 可以是 DVB-H、DVB-C、DVB-S、和 DVB-T 中的任何一个。 根据上述 DVB 的类型，可以适当修改 DVB 传送装置 200 的构造。

[0020] 数字视频广播传送装置 200 包括内容存储单元 210，其还可以从该装置中分离出来。 内容存储单元 210 利用适合标准技术的存储类型来存储 DVB 的内容。

[0021] 在内容存储单元 210 中存储的内容被加密以用于 DVB。 在图 1 中，图示了用于使用 TEK 来加密内容的 RO 和 TEK 编码器 220。 然而，RO 和 TEK 编码器 220 可以由使用另一加密密钥来加密内容的编码器来替代。 RO 和 TEK 编码器 220 可以将全部内容加密到一个 TEK 数据中，或可以将该内容加密到不同的 TEK 数据中。

[0022] 利用 TEK 加密的 TEK 数据包括：安全参数索引 (SPI)、所加密的内容、和 TEK 生存期信息。 SPI 和 TEK 生存期信息被用作安全关联 (SA) 信息以在接收 TEK 数据的 DVB 接收装置 300 中播放内容。 另外， TEK 信息（诸如用于在 DVB 接收装置 300 中播放内容的 SA 信息、和 DVB 传送装置 200 以及 DVB 接收装置 300 的 IP 信息）也被传送到 DVB 接收装置 300。 SPI 和 TEK 生存期信息的细节将稍后与 DVB 接收装置 300 的说明一起进行描述。

[0023] RO 和 TEK 编码器 220 利用另一加密密钥来对 TEK 所加密的内容进行加密。 这将仅向购买了内容的用户提供用于该内容的权限对象，并因此仅接收到该加密密钥的用户可以播放并观看该内容。 权限对象的概念基于 DRM。 多种加密密钥可以用作权限对象的加密密钥（以下称作“RO 密钥”）。 当然，RO 和 TEK 编码器 220 可以被分为用于通过 RO 密钥加密的构造和用于通过 TEK 加密的构造。

[0024] RF 单元 230 将利用 TEK 和 RO 密钥加密的内容转换为模拟信号，以便可以根据多种 DVB 传送方法来传送该内容。 通过天线输出如上转换的内容并传送到 DVB 接收装置 300 中。 在 DVB-C 的情况下，通过线缆输出该内容，并因此不需要天线 240。

[0025] 通过可以被分为四层的 DVB 信道来传送模拟信号。 在下文中，将更详细地描述 DVB 信道。

[0026] DVB 信道的第一层用于 DVB 接收终端（在本发明中，是 DVB 接收装置 300）的终端验证，并且通过第一层来传送 / 接收用于终端验证的数据。 第二层用于传送利用 RO 密钥加密的数据，以便给予用于指定内容的用户的权限对象。 第三层用于 TEK 所加密的内容本身的数据。 第四层用于在 TEK 数据之前的未加密数据。 除了所加密的内容之外，也通过信道传送用于解密所加密的内容的安全关联信息。 传送作为安全关联信息的安全参数索引、RO 密钥、TEK 生存期信息、TEK 信息等。

[0027] 控制单元 250 控制上述构成元件的操作。

[0028] DVB 接收装置 300 通过天线 310 接收通过 DVB 信道输入的内容。 RF 单元 320 将所接收的内容转换为数字信号。 在 DVB-C 的情况下，该内容通过线缆输入，并因此不需要天线 310。

[0029] 其后， RO 解码器 330 解码所转换的信号。 使用单独接收的 RO 密钥和 TEK 来

顺序解密所加密的内容数据。 首先，进行 DVB 接收装置 300 本身的验证。 也就是说，验证该 DVB 接收装置 300 是否是购买了该内容的用户的 DVB 接收装置。 在对该装置进行验证中，可以使用多种现有的验证方法。 其后，当验证了该用户是购买该内容的用户时，使用当购买该内容时所接收到的 RO 密钥来解密所加密的内容。 相应地，验证了用于所购买的内容的用户权限对象。

[0030] 在通过 RO 密钥来解密所接收的内容数据之后，利用 TEK 加密的 TEK 数据、被添加到其中的安全参数索引、以及 TEK 信息的 TEK 生存期信息保留下来。所加密的 TEK 数据、安全参数索引、和 TEK 有限期信息被存储在安全关联数据库 340 中。 安全关联数据库 340 可以通过单独的存储器实现，或基本上在 DVB 接收装置 300 中使用的部分存储器可以用作安全关联数据库 340。

[0031] 用户权限对象的验证是本发明的重要方面。 根据用户权限对象，确定对安全关联数据库 340 本身的访问权。 一般，用户可以购买内容本身，或可以根据时间来购买内容。 在这种情况下，如果用户购买的时间期满，则用户内容的权限对象也期满，从而对安全关联数据库的访问权期满。 利用上述构造，可以解决由于 TEK 数据具有被设置为长于其需要的 TEK 生存期或即使在没有购买它的情况下也预先额外地接收 TEK 数据而导致的暗中事后观看问题。 也就是说，即使所购买的 TEK 数据具有长于其需要的 TEK 生存期，或未购买的 TEK 数据被存储在安全关联数据库 340 中，也会根据用户权限对象来控制安全关联数据库 340 的访问，以解决传统问题。

[0032] 例如，对安全关联数据库 340 的访问权通过触发 (toggle) “1” 和 “0” 之间的对应标记来给予。 然而，即使用户权限对象期满，用户也可以重新购买该内容，以便重新确定对安全关联数据库 340 的访问权。 在这种情况下，可以省略重新接收已经接收的 TEK 数据的处理。

[0033] 重放单元 350 使用在安全关联数据库 340 中存储的安全参数索引、 TEK 数据、和 TEK 生存期信息来播放内容。 首先，搜索在安全关联数据库 340 中存储的、与所单独接收的安全参数索引一致的安全参数索引。 然后，读出与所存储的安全参数索引对应的 TEK 数据，并然后使用所单独接收的 TEK 来解密该 TEK 数据。 相应地，获得完整解密的内容数据，以便在显示单元 360 上显示该内容。

[0034] 例如，显示单元 360 可以根据 DVB 接收装置 300 的类型、通过等离子显示面板 (PDP)、液晶显示器 (LCD) 等来实现。 当然，非 DVB 接收装置 300 的单独显示装置也可以用于显示该内容。

[0035] 控制单元 340 控制上述构成元件的全部操作。

[0036] 图 2 是图示了根据本发明实施例的用于 DVB 的 DRM 的方法的流程图。

[0037] 参考图 2，在步骤 S100 中，DVB 接收装置 300 根据用户的请求连接到 DVB 传送装置 200。 这里，用户执行用于用户的数字视频广播接收装置 300 本身的验证过程。 然后，在步骤 S200 中，数字视频广播接收装置 300 请求从 DVB 传送装置 200 中购买用户期望的特定内容，并购买该内容。

[0038] 在购买该内容之后，在步骤 S300 中， DVB 传送装置 200 利用 TEK 来加密所购买的内容。 这里，数字视频广播传送装置 200 将当 DVB 接收装置 300 解密 TEK 数据时所需要的安全参数索引和 TEK 生存期信息添加到 TEK 数据中，并同时利用 RO 密钥来加

密 TEK 数据、对应的安全参数索引、和 TEK 生存期信息。 如以上参考图 1 所述，该 RO 密钥是用于对内容的用户权限对象进行验证的加密密钥。

[0039] 在步骤 S400 中， DVB 传送装置 200 向 DVB 接收装置 300 传送利用 RO 密钥加密的各个 TEK 数据。 DVB 传送装置 200 还向 DVB 接收装置 300 传送 RO 密钥。

[0040] 在这种情况下，用户可以一起传送安全关联信息，以便可以在 DVB 接收装置 300 中播放该内容。 安全关联信息可以包括：安全参数索引 (SPI)、 DVB 传送装置 200 和 DVB 装置 300 的 IP 信息、以及 TEK 信息，其用于验证用户的权限对象和对所传送的内容数据进行解密。

[0041] 在步骤 S500 中， DVB 接收装置 300 验证从 DVB 传送装置 200 接收的用于所加密的内容数据的权限对象，并在安全关联数据库 340 中存储所验证的权限对象。 通过利用单独接收的 RO 密钥来解密所接收的内容数据以执行权限对象的验证。 相应地，在安全关联数据库 340 中，存储利用 TEK 加密的内容数据，作为利用 RO 密钥解密的内容数据。

[0042] 在步骤 S600 中，DVB 接收装置 300 根据关于用户权限对象的信息来设置对安全关联数据库 300 的访问权。 该访问权是对安全关联数据库 340 本身的访问权。 例如，如果按照时间的方式来设置用户权限对象，则访问权也可以被设置为与用户权限对象对应的时间信息。 例如，访问权通过触发 “1” 和 “0” 之间的标记来控制是否访问内容本身，其取决于在安全关联数据库 340 中存储的内容的权限对象是否存在来指示访问权。相应地，对于在没有实际购买的情况下在安全关联数据库 340 中预存储的内容、或对于被设置为长于实际需要的 TEK 生存期的 TEK 生存期尚未期满的内容的读取得到阻止，并因此可以解决上述暗中事后观看问题。

[0043] 在步骤 S700 中，如果用户向 DVB 接收装置 200 发送用于播放所购买的内容的命令，则 DVB 接收装置 200 询问是否已经确认了对于对应内容的用户访问权。 如果用户的访问权已经得到确认，则数字视频广播接收装置 300 从在安全关联数据库 340 中存储的 TEK 数据之中、读取在其中添加了与单独接收的安全参数索引一致的安全参数索引的 TEK 数据，并利用单独接收的 TEK 解密该 TEK 数据。

[0044] 在步骤 S800 中，重放单元 350 播放所解密的 TEK 数据，并且显示单元 360 显示所解密的内容数据。 如果在步骤 S700 中对于用户想要播放的内容的用户访问权没有得到确认、并且该用户没有请求重购该内容，则 DVB 接收装置拒绝重放该内容并终止其操作。 然而，如果用户请求重购该内容，则 DVB 接收装置通过重新执行包括用于重新确定对于对应内容的访问权的步骤 S600 的上述步骤，来播放并显示该内容。

[0045] 如上所述，根据本发明，可以解决在 DVB 期间发生的暗中事后观看问题，并因此可以有效地保护用于 DVB 内容的数字权限。 在解决暗中事后观看问题中，可以使用现有的权限对象和安全关联数据库的构造，而无需添加用于管理 TEK 生存期的单独构造。

[0046] 尽管已经参考本发明的特定示范实施例而示出和描述了本发明，但是该领域技术人员将理解，可以在其中做出形式和细节上的各种改变，而不脱离由所附权利要求限定的本发明的精神和范围。

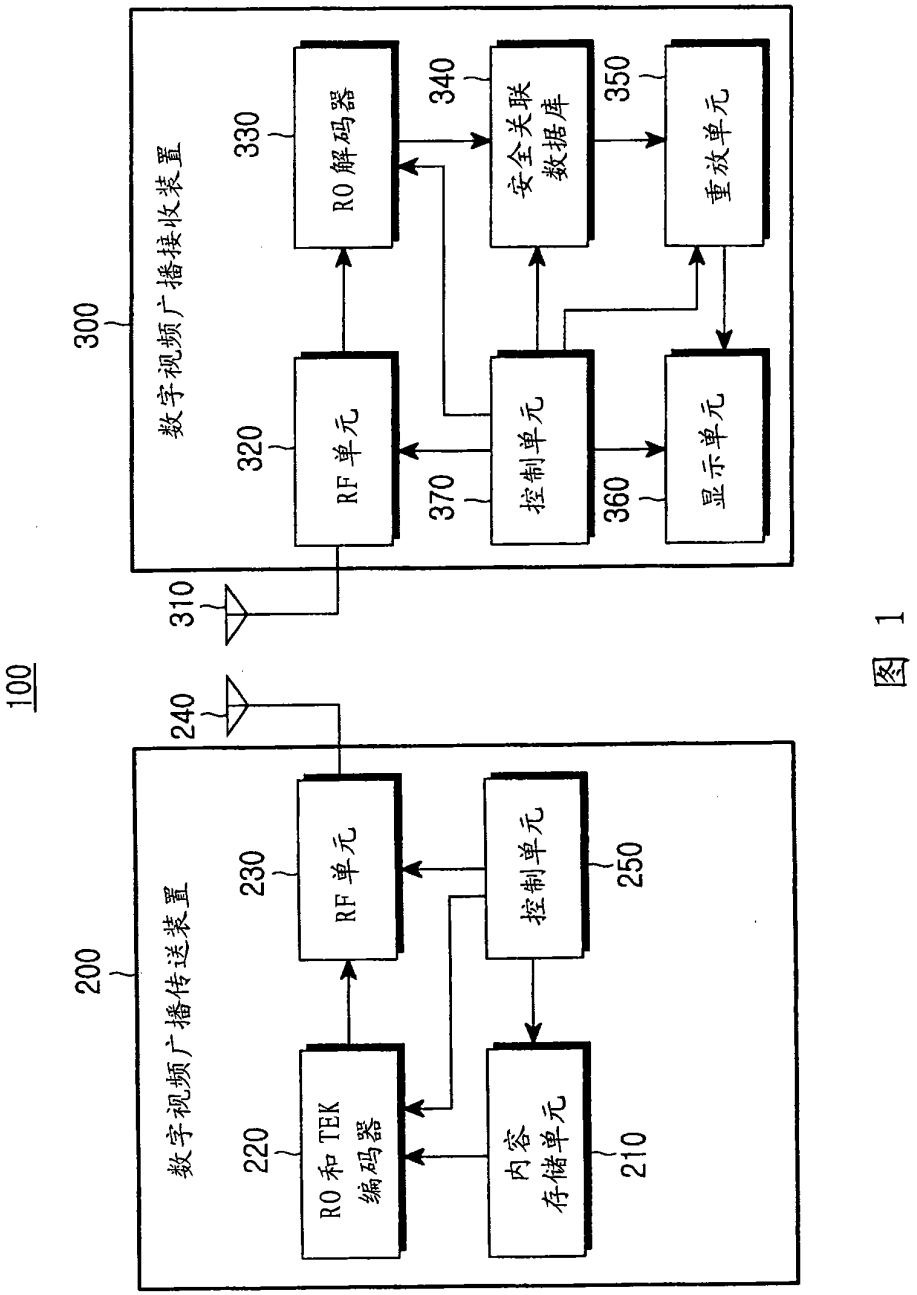

100
200
数字视频广播传送装置
210
内容存储单元
220
RO 和 TEK 编码器
230
RF 单元
240
250
控制单元
300
数字视频广播接收装置
310
320
RF 单元
330
RO 解码器
340
安全关联数据库
350
重放单元
360
显示单元
370
控制单元

图 1

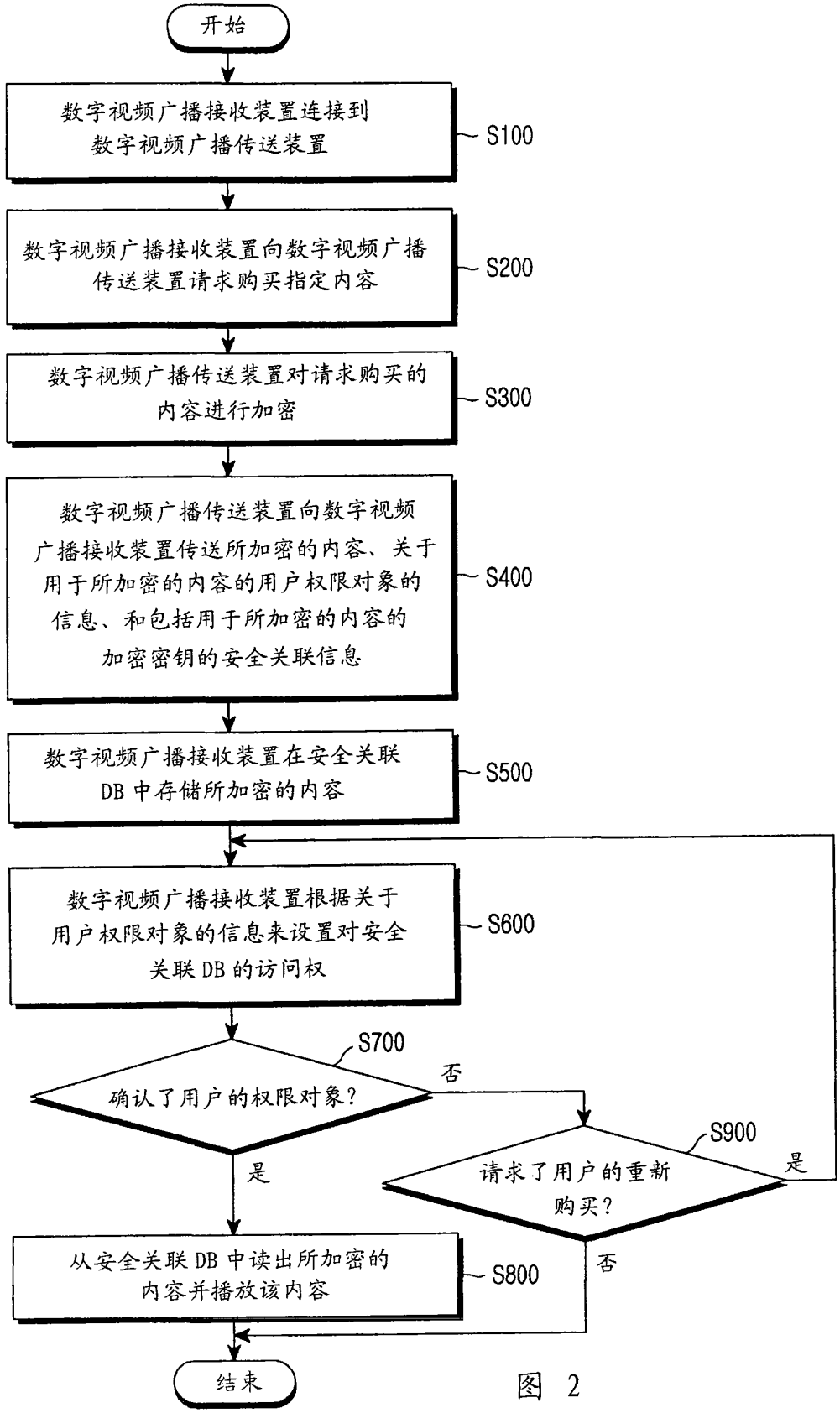

开始
数字视频广播接收装置连接到数字视频广播传送装置
S100
数字视频广播接收装置向数字视频广播传送装置请求购买指定内容
S200
数字视频广播传送装置对请求购买的内容进行加密
S300
数字视频广播传送装置向数字视频广播接收装置传送所加密的内容、关于用于所加密的内容的用户权限对象的信息、和包括用于所加密的内容的加密密钥的安全关联信息
S400
数字视频广播接收装置在安全关联DB中存储所加密的内容
S500
数字视频广播接收装置根据关于用户权限对象的信息来设置对安全关联DB的访问权
S600
S700
确认了用户的权限对象?
否
是
S900
请求了用户的重新购买?
是
否
从安全关联DB中读出所加密的内容并播放该内容
S800
结束

图 2