(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 395 398**

(51) Int. CI.:

H04N 7/167 (2011.01)
H04N 21/432 (2011.01)
H04N 21/418 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/4627 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4408 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.07.2001 E 07020302 (1)**

(97) Fecha y número de publicación de la solicitud europea: **23.01.2008 EP 1881704**

(54) Título: **Almacenamiento super encriptado y recuperación de programas audiovisuales con claves generadas por tarjeta inteligente**

(30) Prioridad:

21.07.2000 US 620772

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.02.2013

(73) Titular/es:

THE DIRECTV GROUP, INC. (100.0%)
2230 E. Imperial Highway
El Segundo, CA 90245 , US

(72) Inventor/es:

KAHN, RAYNOLD M.;
GAGNON, GREGORY J.;
HA, DAVID D.;
KLAUSS, PETER M.;
CURREN, CHRISTOPHER P. y
JAMES, THOMAS H.

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Almacenamiento super encriptado y recuperación de programas audiovisuales con claves generadas por tarjeta inteligente.

ANTECEDENTES DE LA INVENCIÓN

1. Campo de la Invención

La presente invención se refiere a sistemas y métodos para proporcionar material de programa de vídeo a abonados, y en especial a un método para almacenar con seguridad programas de medios de comunicación.

2. Descripción de la técnica relacionada

En los últimos años ha existido un interés creciente en permitir que los abonados a televisión por cable y satélite graben programas de medios de comunicación de difusión para su visionado posterior. Esta capacidad, a la que se hace referencia a partir de ahora como grabación de vídeos personales (PVR), puede usarse para proporcionar servicios de vídeo a la carta (VOD), o simplemente para permitir que el abonado grabe programas de medios de comunicación para fines de visionado repetido y/o almacenamiento.

En el pasado se usaban grabadoras de cintas de videocasete (VCRs) para este tipo de grabación de vídeos personales. Sin embargo, recientemente se han utilizado discos duros, similares a los usados en ordenadores personales, para almacenar programas de medios de comunicación para su visionado posterior. Al contrario que los VCRs, estos dispositivos o incluyen normalmente un sintonizador, y en lugar de ello están acoplados al receptor de satélite o al decodificador. También al contrario que los VCRs. Estos dispositivos se usan normalmente para grabar contenido digital, no vídeo analógico. Esta diferencia tiene ventajas e inconvenientes.

Una ventaja de estos dispositivos es que permiten un almacenamiento a largo plazo y múltiples reproducciones sin una degradación sustancial. Otra ventaja es que permiten funciones no estándar (trick-play) más rápidas como avance y rebobinado rápidos. Un inconveniente de estos dispositivos es que son capaces de realizar también copias de generación múltiple del material de programa, sin una degradación grave. Esto aumenta la posibilidad real de que las copias de generación múltiple de los programas de medios de comunicación se produzcan y distribuyan sin permiso. Esta posibilidad ha hecho que algunos proveedores de medios de comunicación sean contrarios a permitir que sus programas de medios de comunicación sean grabados por estos dispositivos.

Para solucionar este problema es esencial proteger los programas de medios de comunicación almacenados con una seguridad y un control de copias severos. Los dispositivos actuales no codifican los programas de medios de comunicación antes de su almacenamiento y tampoco almacenan la información sobre protección de copias. En lugar de ello, estos dispositivos almacenan el contenido del programa descifrado en el disco de memoria usando un esquema de hardware emparejado, en el que el controlador del disco duro y el disco duro están emparejados entre sí específicamente a través de un interfaz específico. Debido a que el controlador del disco duro y el propio disco están esencialmente emparejados entre sí, el almacenamiento o la reproducción no funcionarán si el disco se ha extraído y transferido a otro reproductor. El punto débil de este esquema de seguridad es que se basa sólo en el hardware emparejado para garantizar la seguridad… los programas de medios de comunicación almacenados en la propia unidad de disco no están cifrados.

Aunque presumiblemente sería posible almacenar sencillamente el flujo de datos según se recibe del difusor para una reproducción posterior, esta técnica tiene diferentes inconvenientes. Uno de estos inconvenientes es que proporcionaría a los piratas una versión grabada permanentemente del flujo de datos cifrado, proporcionando de este modo al pirata una información que puede usarse para realizar análisis detallados del propio flujo de datos, para determinar las técnicas y los códigos de cifrado.

Lo que se necesita es un sistema y un método para grabar con seguridad programas de medios de comunicación de difusión (incluyendo programas de pago por visión de compra impulsiva) para una reproducción de uso limitado en un momento posterior. Un sistema de este tipo podría usar para apoyar el vídeo a la carta (VOD), permitiendo de este modo que el abonado compre programas de medios de comunicación y juegos en el decodificador de señal, instantáneamente, sin preocuparse de la hora de comienzo del programa. Lo que también se necesita es un sistema y un método que no requieran cambios sustanciales en el hardware del abonado, como un receptor/decodificador integrado (IRD), o el módulo de acceso condicional (CAM) que se usa para proporcionar una clave de descifrado de lo programas de medios de comunicación para su presentación a los abonados.

A este respecto, la segunda edición del libro “Applied Cryptography” de B. Schneier define el cifrado enlace por enlace como un sistema de cifrado de usuario en el que la información es cifrada en un nodo y enviada a otro en el que es descifrada y de nuevo cifrada con otra clave. Adicionalmente, Schneier prevé el uso del cifrado para almacenar cualquier clase de dato, asumiendo que las mismas claves se utilizarán para el cifrado y descifrado.

Además, Schneier, menciona el cifrado de un fichero con una clave, y cifrar esa clave con otra clave conocida por el usuario.

El documento EP-A-0 989 557 describe almacenar material de programa en un dispositivo de almacenamiento de medios acoplado a un receptor para su posterior reproducción, con los pasos de: aceptar información de control de acceso cifrada y el material de programa cifrado de acuerdo con una primera clave de cifrado en el módulo de acceso condicional que se puede insertar en el receptor; descifrar la información de control de acceso recibida para producir la primera clave de cifrado; descifrar el material de programa utilizando la primera clave de cifrado; volver a cifrar o recifrar el material de programa de acuerdo con la segunda clave de cifrado; cifrar la segunda clave de cifrado de acuerdo con la tercera clave de cifrado para producir la cuarta clave de cifrado; y proporcionar el material de programa recifrado y la cuarta clave de cifrado para almacenamiento.

En el documento EP-A-0 912 052 una palabra de control descodificada, junto con cualquier otro dato que forme la ECM, tal como la información de control de acceso, etc. se pasa al microprocesador incrustado en una tarjeta inteligente. Utilizando una segunda clave de cifrado y un segundo algoritmo de cifrado, la tarjeta inteligente genera un nuevo ECM.

SUMARIO DE LA INVENCIÓN

Resumiendo, la presente invención describe un método para almacenar material de programa para su reproducción posterior. El método comprende los pasos definidos en la reivindicación 1.

Un objeto de la presente invención es proporcionar la recepción y descifrado de programas de medios de comunicación, incluyendo programas de pago por visión impulsivo (IPPV), que pueden ser reproducidos y grabados en medios de almacenamiento y permite la reproducción en un tiempo posterior con un uso limitado. Los datos en sí mismo pueden ser colocados en almacenamiento de corta duración, pero la reproducción de los programas de medios pueden desempeñarse con funciones de reproducción no estándar (trick-play) tales como funciones de avance, retroceso, avance rápido, retroceso rápido, avance fotograma a fotograma, y pausa.

Otro objeto de la presente invención es proporcionar funciones de PVR que proporciona grabar, reproducir con retardo y reproducción no estándar (trick-play) de programas de medios de IPPV desde el medio de almacenamiento sin requerir una compra previa del programa de medios de IPPV. Esto permitiría que el programa de medios de IPPV fuera visto sin requerir que el programa de IPPV tuviera que ser comprado antes de almacenarlo. De manera ideal, dicho sistema permitiría al usuario seleccionar el programa de medios de IPPV desde el dispositivo de almacenamiento, sometido a derechos de reproducción limitados.

Aún otro objeto de la presente invención es proporcionar un emparejamiento entre el medio de almacenamiento y los elementos de los IRD de los abonados para asegurar que la reproducción de los programas de medios desde el dispositivo de almacenamiento sea permitida solamente con el IRD apropiado.

Aún otro objeto de la presente invención es proporcionar unos medios seguros para almacenar flujos de datos de comunicaciones (incluyendo IPPV y juegos) en un dispositivo de almacenamiento de datos, mientras que se establezca la protección de copia adecuada.

Aún otro objeto de la presente invención es proporcionar un sistema y un método para gestionar el archivo y recuperación de programas de medios y otros datos, incluso si el dispositivo de almacenamiento da datos falla.

Aún otro objeto de la presente invención es proporcionar un sistema y un método que permite que las compras de programas de medios se graben de una manera que sea análoga a las que se emplea para programas que se emiten o salen al aire en tiempo real.

Aún otro objeto de la presente invención es proporcionar un sistema que proporcione unas pautas de crecimiento a un sistema que permite programas de medios de IPPV para ser visionados previamente sin cargo durante un periodo de tiempo inicial con la opción de comprar el programa de medios o cancelar la compra, sin tener en cuenta si el programa es recuperado del dispositivo de almacenamiento u obtenido de una emisión en tiempo real.

La presente invención elimina lo concerniente a la proliferación de copias digitales no autorizadas de los programas de medios mediante el uso de un método de cifrado reforzado. Además, la presente invención asegura que el material almacenado no puede ser distribuido ya que dicho descifrado del material puede solamente realizarse con éxito mediante el IRD de cifrado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Haciendo ahora referencia a los dibujos en los que los números de referencia iguales representan partes totalmente correspondientes:

La figura 1 es un diagrama que muestra una vista general de un sistema de distribución de vídeo;
la figura 2 es un diagrama en bloques que muestra una configuración de enlaces ascendentes normal, que muestra cómo el material de programa de vídeo se enlaza con un satélite para su transmisión a abonados usando un único transpondedor;
la figura 3A es un diagrama en bloques de un flujo de datos representativo recibido desde un satélite;
la figura 3B es un diagrama que ilustra la estructura de un paquete de datos;
la figura 4 es un diagrama en bloques que ilustra un diagrama en bloques de alto nivel del IRD; y
la figura 5 es un diagrama que ilustra el almacenamiento y la recuperación de datos desde un dispositivo de almacenamiento de medios de comunicación.

DESCRIPCIÓN DETALLADA DE REALIZACIONES PREFERIDAS

En la siguiente descripción se hace referencia a los dibujos adjuntos que forman parte de la misma y que muestran, por medio de ilustraciones, varias realizaciones de la presente invención. Se entiende que pueden utilizarse otras realizaciones y que pueden realizarse cambios estructurales sin alejarse del alcance de la presente invención, según se define en las reivindicaciones adjuntas.

SISTEMA DE DISTRIBUCIÓN DE VÍDEO

La figura 1 es un diagrama que ilustra una vista general de un sistema de distribución de vídeo 100. El sistema de distribución de vídeo 100 comprende un centro de control 102 en comunicación con un centro de enlace ascendente 104 a través de un enlace terrestre 114 y un receptor/decodificador integrado (IRD) 132 en la estación receptora 130, a través de una red telefónica conmutada pública (PSTN) u otro enlace 120. El centro de control 102 proporciona material de programa al centro de enlace ascendente 104, coordina con la estación receptora 130 para ofrecer a los abonados 110 servicios de programa pago por visión (PPV), incluyendo facturación y descripción asociada de programas de vídeo.

El centro de enlace ascendente 104 recibe material de programa e información de control del programa desde el centro de control 102 y, usando una antena de enlace ascendente 106, transmite el material de programa y la información de control del programa al satélite 108. El satélite 108 recibe y procesa esta información, y transmite los programas de vídeo y la información de control al IRD 132 en la estación receptora 130 a través del enlace descendente 118. El IRD 132 recibe esta información usando la antena de abonado 112 a la que está acoplado de forma comunicativa.

El sistema de distribución de vídeo 100 puede comprender varios satélites 108 con objeto de proporcionar una cobertura terrestre más amplia, para proporcionar canales adicionales, o para proporcionar anchura de banda adicional por canal. En una realización de la invención, cada satélite comprende 16 transpondedores para recibir y transmitir material de programa y otros datos de control desde el centro de enlace ascendente 104, y proporcionarlos a los abonados 110. Sin embargo, si se usan técnicas de compresión y multiplexado de datos las capacidades de canales son mucho mayores. Por ejemplo, dos satélites 108 trabajando juntos pueden recibir y retransmitir más de 150 canales convencionales (no de HDTV) de audio y vídeo a través de 32 transpondedores.

Aunque la invención descrita aquí se describirá haciendo referencia a un sistema de distribución de vídeo 100 basado en satélite, la presente invención también puede materializarse con transmisión basada en tierra de información de programas, ya se mediante medios de difusión tradicionales, cable u otros medios. Aparte de esto, las diferentes funciones asignadas colectivamente entre el centro de control 102 y el centro de enlace ascendente 104, según lo descrito anteriormente, pueden reasignarse según se desee sin alejarse del alcance buscado de la presente invención.

Aunque lo anterior se ha descrito con respecto a una realización en la que el material de programa entregado al abonado es material de programa de vídeo (y audio) como por ejemplo una película, el método anterior puede usarse para entregar también material de programa que comprenda sólo información de audio o datos.

La figura 2 es un diagrama en bloques que muestra una configuración de enlace ascendente normal para un único transpondedor de satélite 108, que muestra cómo el material de programa de vídeo se enlaza con el satélite 108 desde el centro de control 102 y el centro de enlace ascendente 104. La figura 2 muestra tres canales de vídeo (que podrían ampliarse respectivamente con uno o más canales de audio para música de alta fidelidad, información sobre bandas sonoras o un programa de audio secundario para transmitir idiomas extranjeros), y un canal de datos desde una fuente de datos de ordenador 206.

Los canales de vídeo son proporcionados por una fuente de programa de material de vídeo 200A-200C (llamada en conjunto a partir de ahora fuente(s) de vídeo 200). Los datos procedentes de cada fuente de programa de vídeo 200 se proporcionan a un codificador 202A-202C (llamado en conjunto a partir de ahora codificador(es) 202). Cada uno de los codificadores acepta una marca de tiempo de presentación (PTS) desde el controlador 216. La PTS es una

marca de tiempo binaria que se reinicia cíclicamente, que se usa para garantizar que la información de vídeo está sincronizada de forma apropiada con la información de audio después de la codificación y decodificación. Una marca de tiempo PTS se envía con cada marco incorporado de los datos codificados MPEG.

En una realización de la presente invención, cada codificador 202 es un codificador de Grupo de Expertos de Imágenes en Movimiento de segunda generación (MPEG-2), pero pueden usarse igualmente otros decodificadores que implementen otras técnicas de codificación. El canal de datos puede ser objeto de un esquema de compresión similar por parte de un codificador (no mostrado), pero esta compresión es o bien innecesaria o llevada a cabo por programas de ordenador en la fuente de datos del ordenador (por ejemplo, los datos fotográficos se comprimen normalmente en ficheros *.TIF o ficheros *.JPG antes de la transmisión). Después de codificarse mediante los codificadores 202, las señales se convierten en paquetes de datos mediante un empaquetador 204A-204F (llamado en conjunto a partir de ahora paquetizador(es) 204), asociado a cada fuente 200, 206-210.

Los paquetes de datos se agrupan usando una referencia procedente del reloj del sistema 214 (SCR), una palabra de control (CW) generada por el administrador de acceso condicional 208, y un generador identificador de canales del sistema (SCID) que asocia cada uno de los paquetes de datos que se difunde al abonado con un canal de programa. Esta información se transmite a los empaquetadores 204 para usarse en la generación de los paquetes de datos. Estos paquetes de datos se multiplexan después en datos en serie, se codifican, modulan y transmiten. También se cifra y transmite un paquete especial conocido como paquetes de palabras de control (CWP), que comprende datos de control incluyendo la palabra de control (CW) y otros datos de control usados para apoyar el acceso condicionado al material de programa.

La figura 3A es un diagrama de un flujo de datos representativo. El primer segmento de paquete 302 comprende información del canal de vídeo 1 (datos procedentes de, por ejemplo, la primera fuente de programa de vídeo 200A). El siguiente segmento de paquete 304 comprende información de datos de ordenador que se han obtenido, por ejemplo, de la fuente de datos de ordenador 206. El siguiente segmento de paquete 306 comprende información del canal de vídeo 5(desde una de las fuentes de programa de vídeo 200), y el siguiente segmento de paquete incluye información del canal de vídeo 1 (de nuevo procedente de la primera fuente de programa de vídeo 200A). El flujo de datos comprende para ello una serie de paquetes procedentes de una cualquiera de las fuentes de datos, en un orden determinado por el controlador 216. El flujo de datos es cifrado por el módulo de cifrado 218, modulado por el modulador 220 (usando normalmente un esquema de modulación QPSK), y proporcionado al transmisor 222, que difunde el flujo de datos modulado en una anchura de banda de frecuencia al satélite a través de la antena 106.

Los abonados 110 reciben programas de medios de comunicación a través de un receptor de abonado o IRD 132. Usando el SCID, el IRD 132 vuelve a ensamblar los paquetes para regenerar el material de programa para cada uno de los canales. Como se muestra en la figura 3A, los paquetes cero creados por el módulo de paquetes cero 312 pueden insertarse en el flujo de datos si se desea.

La figura 3B es un diagrama de un paquete de datos. Cada paquete de datos (por ejemplo, 302-316) tiene una longitud de 147 bytes, y comprende varios segmentos de paquete. El primer segmento de paquete 320 comprende dos bytes de información que contienen el SCID e indicadores. El SCID es un número exclusivo de 12 bits que identifica específicamente el canal de datos del paquete de datos. Los indicadores incluyen 4 bits que se usan para controlar si el paquete está cifrado, y qué clave debe usarse para descifrar el paquete. El segundo segmento de paquete 322 está formado por un indicador de tipo paquete de 4 bits y un contador de continuidad de 4 bits. El tipo de paquete identifica el paquete como uno de los cuatro tipos de datos (vídeo, audio, datos o cero). Cuando se combina con el SCID, el tipo de paquete determina cómo se usará el paquete de datos. El contador de continuidad se incrementa una vez por cada tipo de paquete y SCID. El siguiente segmento de paquete 324 comprende 127 bytes de datos de carga útil, que es una parte del programa de vídeo proporcionada por la fuente de programa de vídeo 200. El segmento de paquete final 326 son datos requeridos para realizar corrección de errores avanzada.

CIFRADO DE PROGRAMAS DE MEDIOS DE COMUNICACIÓN

Los programas de medios de comunicación se cifran mediante el módulo de cifrado 218 antes de la transmisión, para garantizar que se reciben y visualizan sólo por parte de abonados autorizados. Cada programa de medios de comunicación está cifrado de acuerdo con una clave de cifrado alfanumérica, llamada a partir de ahora palabra de control (CW). Esto puede llevarse a cabo mediante una variedad de técnicas de cifrado de datos, incluyendo el estándar de cifrado de datos (DES) y el algoritmo de Rivest-Shamir-Adleman (RSA).

Para descifrar los programas de medios de comunicación, el IRD 132 del abonado 110 también tiene acceso a la CW. Para mantener la seguridad, las CWs no se transmiten a los textos simples de IRD 132. En lugar de ello, las CWs se cifran antes de la transmisión al IRD 132 del abonado. La CW cifrada se transmite al IRD 132 del abonado en un paquete (de datos) de palabra de control.

En una realización los datos en los CWP, incluyendo la CW, se cifran y descifran a través de lo que se llama a partir de ahora algoritmo indescifrable de entrada/salida (I/O).

Un algoritmo indescifrable de I/O es un algoritmo que se aplica a un flujo de datos de entrada para producir un flujo de datos de salida. Aunque el flujo de datos de entrada determina exclusivamente el flujo de datos de salida, el algoritmo seleccionado es tal que sus características no pueden cifrarse mediante una comparación de un número todavía mayor de flujos de datos de entrada y salida. La seguridad de este algoritmo puede ampliarse adicionalmente mediante la adición de elementos funcionales adicionales, que no son estacionarios (es decir, cambian en función del tiempo). Cuando un algoritmo de este tipo recibe flujos de entrada idénticos, el flujo de datos de salida proporcionado en un momento dado puede ser diferente que el flujo de salida proporcionado en otro momento.

Siempre que el módulo de cifrado 218 y el IRD 132 compartan el mismo algoritmo indescifrable de I/O, el IRD 132 puede decodificar la información en los CWP para recuperar la CW. Después, usando la CW, el IRD 132 puede descifrar el programa de medios de comunicación de tal manera que éste puede presentarse al abonado 110.

Para desalentar además a la piratería, los datos de control necesarios para descifrar y agrupar paquetes de datos en programas de medios de comunicación visionables pueden variar en el tiempo (la validez de los datos de control en un CWP para decodificar un programa de medios de comunicación particular cambia con el tiempo). Esto puede implementarse de diferentes formas.

Por ejemplo, debido a que cada CWP está asociado a un SCID para cada programa de medios de comunicación, el SCID relacionado con cada CWP podría variar con el tiempo.

Otra forma de implementar datos de control variables en el tiempo es asociar marcas de tiempo al flujo de datos recibido y a los datos de control de CWP. En este caso, una decodificación con éxito de los CWP para producir la CW exigiría la relación adecuada entre las marcas de tiempo para el flujo de datos y los datos de control en los CWP. Esta relación puede definirse, por ejemplo, cambiando el esquema de descifrado usado para generar la CW desde los CWP, de acuerdo con a marca de tiempo recibida para el flujo de datos. En este caso, si la marca de tiempo del flujo de datos recibido no se ajusta al valor esperado, se elegirá el esquema de descifrado erróneo y no se producirá la CW adecuada. Sin embargo, si la marca de tiempo del flujo de datos recibidos se ajusta al valor esperado, se elegirá el esquema de descifrado adecuado, y el esquema de descifrado de CWP producirá la CW adecuada.

SOLICITUD DE SERVICIOS DE PAGO POR VISIÓN

Los datos requeridos para recibir programas de medios de comunicación de pago por visión (PPV) se almacenan en los CWP y en otro paquete de datos conocido como la parcela de información de compra (PIP). Tanto los CWP como la PIP se difunden al abonado a través del sistema de distribución de vídeo 100 en tiempo real. Como se describe a continuación, el CWP es usado por el IRD 132 para recuperar programas de medios de comunicación de PPV.

En general los servicios PPV pueden incluir servicios de pago por visión asistidos por operador (OPPV) y de pago por visión impulsivo (IPPV). Cuando solicita servicios OPPV, el abonado 110 debe decidir con antelación que desea acceder a un programa de medios de comunicación particular. El abonado 110 llama a una entidad como el centro de control 102, y requiere acceso al programa de medios de comunicación. Cuando solicita servicios de paso por visión impulsivo (IPPV), el abonado 110, mientras visiona la guía de programa, mueve el cursor sobre el canal de visionado asociado al programa de medios de comunicación deseados, y selecciona “enter”. Una vez que se han confirmado la decisión y los derechos de compra de un programa PPV (por ejemplo mediante la revisión de bloqueos de canal, límites de cuota de pantalla y límites de compra), se recibe y almacena una parcela de información de compra (PIP) en el módulo de acceso condicional 406 (que se describe a continuación con más detalle) para su uso posterior. El módulo de acceso condicional 406 asocia la información en el CWP y el PIP, y usa el PIP junto con los CWP para verificar que el abonado 110 debe recibir acceso al programa de medios de comunicación y para descifrar el programa de medios de comunicación.

Sin embargo, la petición de programas de medios de comunicación PPV anticipadamente usando la PIP está limitada, ya que la PIP se difunde hasta 24 horas antes de que se difunda el propio programa de medios de comunicación. Como la PIP se difunde en tiempo real, el IRD 132 no adquiere la PIP hasta que el abonado 110 solicita realmente la compra de programa de medios de comunicación PPV.

RECEPCIÓN Y DESCIFRADO POR PARTE DEL ABONADO DE PROGRAMAS DE MEDIOS DE COMUNICACIÓN

La figura 4 es un diagrama en bloques simplificado de un IRD 132. El IRD 132 recibe y descifra los programas de medios de comunicación difundidos por el sistema de distribución de vídeo 100. Estos programas de medios de

comunicación se canalizan al IRD 132 en tiempo real, y pueden incluir, por ejemplo, servicios de vídeo, audio o datos.

El IRD 132 puede acoplarse comunicativamente a un módulo de acceso condicional (CAM) 406. El CAM 406 se implementa normalmente en una tarjeta inteligente o un dispositivo similar, que se proporciona al abonado 110 para que lo inserte en el IRD 132. El CAM 406 se interconexiona con un verificador de acceso condicional (CAV) 408, que lleva a cabo al menos algunas de las funciones necesarias para verificar que el abonado 110 está autorizado a acceder a los programas de medios de comunicación. El CAV 408 está acoplado comunicativamente a un módulo de análisis de meta-datos (MAM) 411. Usando la información en la tabla de meta-datos (por ejemplo, la tabla 1 descrita más adelante), el MAM 411 actúa como guardabarrera para determinar si los programas de medios de comunicación almacenados se descifrarán y presentarán al abonado 110. Esto se realiza comparando los valores de meta-datos con valores medidos o acumulados. El CAV 408 y el MAM 411 pueden implementarse como módulos separados del descifrador/demux/transporte 412 y del microcontrolador y de la memoria 414, según se muestra, o pueden implementarse a través de instrucciones de software almacenadas en la memoria y realizadas por el microcontrolador 414.

El IRD 132 comprende un sintonizador 410, un módulo de transporte y demultiplexado (TDM) 412, que funciona bajo el control de un microcontrolador y una memoria asociada 414, un decodificador fuente 416 y una memoria de acceso aleatorio (RAM) 418 acoplada comunicativamente, así como un dispositivo de I/O de usuario para aceptar órdenes del abonado 110 y para proporcionar información de salida al abonado.

El sintonizador recibe los paquetes de datos desde el sistema de distribución de vídeo y proporciona los paquetes al TDM 412. Usando los SCIDs asociados a cada programa de medios de comunicación, el TDM 412 reagrupa los paquetes de datos de acuerdo con el canal seleccionado por el abonado 110, y descifra los programas de medios de comunicación usando la clave de CW. El TDM 412 puede implementarse mediante un único chip seguro, y está acoplado comunicativamente a un microcontrolador y a la memoria 414.

Una vez que los programas de medios de comunicación se han descifrado, se proporcionan al decodificador fuente 416, que descodifica los datos de los programas de medios de comunicación de acuerdo con estándares MPEG o JPEG, según sea apropiado. El programa de medios de comunicación descodificado se proporciona después a un convertidor D/A (en caso necesario) y se proporciona a interfaces externos 404, que pueden incluir un dispositivo de presentación de programas de medios de comunicación como una televisión, un sistema de audio o u ordenador. El decodificador fuente 416 hace uso de la RAM 418 acoplada comunicativamente para realizar estas funciones.

La clave de CW se obtiene del CWP usando el CAV 408 y el CAM 406. El TDM 412 proporciona el CWP al CAM 406 a través del CAV 408. El CAM 406 utiliza el algoritmo indescifrable de I/O para generar la CW, que se devuelve al TDM 412. El TDM 412 utiliza la CW para descifrar los programas de medios de comunicación. En la mayoría de los IRDs 132, el CAV 408 y el CAM 406 son capaces de descifrar un programa de medios de comunicación de vídeo/audio/datos a la vez.

Según lo descrito anteriormente, para desalentar a los posibles piratas, los datos de control en el CWP usados para decodificar un programa de medios de comunicación específico pueden variar con el tiempo, de tal modo que sólo produce la CW apropiada si se aplica a un programa de medios de comunicación que tenga la marca de tiempo apropiada. En este caso, el CAM 406 puede seleccionar y/o controlar el esquema de descifrado (por ejemplo, el algoritmo indescifrable de I/O) de acuerdo con la marca de tiempo asociada al flujo de datos que lleva el programa de medios de comunicación. Si el programa de medios de comunicación está suficientemente disociado en el tiempo, se usará el esquema de descifrado inadecuado, y no se producirá la CW apropiada para decodificar el programa de medios de comunicación.

Pueden encontrarse detalles adicionales sobre el cifrado y el descifrado de programas de medios de comunicación en la solicitud de patente estadounidense, co-pendiente y de asignación común, Nº US 2004/0148634 A1.

ALMACENAMIENTO Y RECUPERACIÓN DE PROGRAMAS DE MEDIOS DE COMUNICACIÓN EN FORMA CIFRADA

La figura 5 es un diagrama que presenta pasos de un método a modo de ejemplo para materializar una realización de la presente invención. La antena de abonado 112 proporciona un flujo de datos que es recibido por el sintonizador 410 y el TDM 412, según se muestra en al bloque 502. El flujo de datos incluye varios paquetes de datos, que incluyen paquetes de datos con el material de programa 503 cifrado de acuerdo con una primera clave de cifrado (clave de CW 509), e información de control de acceso que está contenida en uno o más paquetes de palabra de control (CWP) 504. Los CWPs 504 incluyen una versión cifrada de la clave de CW 509. El flujo de datos también puede incluir meta-datos que describen la información incluyendo los derechos asociados al material de programa (que pueden incluir, por ejemplo, derechos de reproducción y/o derechos de copia). Estos derechos

incluyen los parámetros necesarios para controlar la reproducción del material de programa, incluyendo servicios IPPV o de pago por visión.

El material de programa cifrado 503 (llamado V/A/D cifrado en la figura 5 para indicar que el material de programa puede incluir vídeo, audio u otros datos) se proporciona al módulo de descifrado de difusión 510. El módulo de descifrado de difusión 510 descifra el material de programa cifrado de acuerdo con la clave de CW 509.

Los CWPs 504 se proporcionan a un módulo de compra previa 506 en el CAM 406. El módulo de compra previa 506 acepta los meta-datos en el CWP 504 y genera datos de derecho de reproducción y/o copia que se usan si el abonado 110 decide posteriormente reproducir el material de programa. Estos datos de derecho de reproducción se proporcionan a un módulo de control de IPPV (IPPV CM) acoplado comunicativamente, que utiliza esta información también para adquirir (o comprar) información proporcionada por el abonado 110 para determinar si el material de programa almacenado debe reproducirse. El módulo IPPV CM 538 también está acoplado comunicativamente a un módulo de historial de compra 540 (PHM) que reúne información requerida para facturar al abonado 110 el material de programa que está visionando el abonado 110.

El IPPV CM 538 también proporciona información usada para determinar si el material de programa recibido por el sintonizador/TDM 410, 412 se graba en el dispositivo de almacenamiento de medios de comunicación 528. En una realización, la información puede obtenerse del flujo de datos difundido por el proveedor del material de programa.

Si el material de programa se va a almacenar en el dispositivo de programas de medios de comunicación 528, el CWP 504 (que en este punto incluye datos de control variables temporalmente) se proporciona después a y se descifra mediante un módulo de descifrado de CWP 508. En una realización de la presente invención el CWP 506 se cifra de acuerdo con un algoritmo indescifrable de I/O, y el módulo de descifrado de CWP 508 incluye la aplicación del algoritmo indescifrable de I/O. En otra realización de la presente invención, el CWP 504 se cifra con una clave y un algoritmo DES o RSA, y el módulo de descifrado de CWP 504 implica la aplicación de la clave para reconstruir los datos cifrados dentro del CWP 504. El módulo de descifrado de CWP 508 puede ser invocado por todos los flujos de datos recibidos por el IRD 132, o puede ser invocado sólo para flujos de datos asociados a programas de medios de comunicación que se han seleccionado para ser grabados por el abonado 110. El módulo de compra previa 506 admite datos procedentes del I/O de usuario 420 o del difusor, indicando que al abonado 110 le gustaría comprar y grabar un programa de medios de comunicación en particular. Si se ha requerido una compra de este tipo (con antelación o de compra previa), las operaciones de descifrado de CWP descritas en el bloque 508 comienzan cuando se difunde el programa de medios de comunicación. En otra realización de la presente invención el difusor determina qué programas se almacenarán en el dispositivo de almacenamiento de medios de comunicación 528, y el abonado 110 no tiene que decidir con antelación qué programas de medios de comunicación deben almacenarse para su visionado posterior. Por ejemplo, el difusor puede almacenar las diez películas más famosas en el dispositivo de almacenamiento de medios de comunicación 528, y sólo factura al abonado 110 cuando el abonado opta por visionar el programa de medios de comunicación. En este caso, el módulo de compra previa 506 recibe la orden de almacenar el programa de medios de comunicación recibido desde el difusor e inicia las operaciones llevadas a cabo por el módulo de descifrado de CWP 508.

El CW 509 se proporciona al módulo de descifrado de difusión 510, que admite el material de programa cifrado 503 para producir el material de programa descifrado 512. El material de programa descifrado 512 se proporciona, desde el módulo de descifrado de difusión 510, a un módulo de cifrado de almacenamiento de protección de copias (CP) acoplado comunicativamente. El módulo de cifrado de almacenamiento 514 recifra o vuelve a cifrar el material de programa descifrado 512 de acuerdo con una clave de protección de copias (CP) 516, para producir material de programa recifrado 518. Aunque la clave de CP 516 puede generarse en otro lugar, en la realización preferida la clave de CP 516 se genera dentro del CAM 406.

En una realización la clave de CP 516 se deriva usando un módulo de generación de CP en el CAM 406 o en otro lugar en el IRD 132, a partir de los meta-datos en el flujo de datos que se difunde hasta el sintonizador 410. Dependiendo de los meta-datos, la clave de CP 516 puede variar también en el tiempo con el material de programa de difusión. En otra realización la clave de CP 516 puede ampliarse en al menos una parte de los meta-datos, antes de se cifrada con la clave de caja 516 y almacenada en el dispositivo de almacenamiento de medios de comunicación 528 como la clave de CP cifrada 524 (que es en sí misma una “clave”). En esta realización, cuando se ha descifrado la clave de CP cifrada 524, se producen tanto la clave de CP 516 como los meta-datos relacionados. Los meta-datos pueden usarse después para verificar y/o controlar la reproducción del material de programa. La clave de CP 516 también puede generarse internamente mediante el IRD 132 sin los meta-datos.

La clave de CP 516 también se proporciona a un módulo de cifrado de clave 522 (KEM), que cifra la clave de CP 516 con una clave de módulo de acceso condicional (CAM) 520, cuyo valor es normalmente exclusivo para cada CAM 406. El resultado de este proceso es una clave de protección de copia cifrada 524. El material de programa recifrado 518 y la clave de CP cifrada 524 se proporciona después al dispositivo de almacenamiento de medios de

comunicación 528 para su almacenamiento. La clave de CAM 520 podría ser un número de serie electrónico (ESN) interno de un circuito integrado que implementa algunas o todas las funciones del CAM 406. El dispositivo de almacenamiento de medios 528 es normalmente un disco duro, pero puede ser un dispositivo con capacidad y tiempo de acceso suficientes para apoyar operaciones de grabación y/o reproducción de los datos almacenados dentro del mismo.

Cuando el abonado 110 decide reproducir los programas de medios de comunicación almacenados, se proporciona una entrada de usuario apropiada en el dispositivo de I/O de usuario 420. La entrada de usuario puede comprender una orden de reproducción, una orden de avance rápido, una orden de rebobinado, una orden de reproducción rápida o rebobinado rápido, o una orden de pausa. En respuesta a la entrada de usuario, el IPPv CM 538 determina si el material de programa en el dispositivo de almacenamiento de medios de comunicación 528 debe presentarse al abonado 110. En una realización la entrada de usuario comprende datos de compra, que identifican al abonado 110, y el material de programa requerido. Estos datos de compra son admitidos por un módulo de compra 550, y se comparan con los datos de derechos de material de programa obtenidos de los meta-datos, para determinar si el material de programa requerido debe proporcionarse al abonado 110. Si se determina que el material de programa debe proporcionarse, se transmite la información al módulo de historial de compras 540. El módulo de historial de compras 540 almacena la información requerida para facturar al abonado la cantidad apropiada por el uso del material de programa. Además de esto, si se determina que el material de programa debe proporcionarse, un módulo de control 552 ordena que el material de programa recifrado 518 y la clave de cifrado de CP cifrada 524 se recuperen del dispositivo de almacenamiento de medios de comunicación 528. El módulo de control 552 también puede controlar cuándo el módulo de descifrado de clave 532 descifra la clave de cifrado de CP 524 para producir la clave de CP 516.

La clave de cifrado de CP 524 se descifra usando la clave de CAM 520, para producir la clave de CP 516. Esta clave de CP 516 y el material de programa recifrado 518 se proporcionan al módulo de descifrado de almacenamiento 534. El módulo de descifrado de almacenamiento 534 descifra el materia de programa de medios de comunicación 518 también cifrado para producir el material de programa 503.

Después de un procesamiento adecuado (es decir, decodificación MPEG y/o JPEG, descompresión, conversión a una señal analógica, etc.), el programa de medios de comunicación se proporciona a un dispositivo de interfaz externo 404, que puede incluir un dispositivo de presentación como una pantalla 536.

Una ventaja de la presente invención es que el procesamiento de datos necesario para proporcionar servicios de pago por visión reside en el CAM 406. Por ello, una vez que el usuario inicia la compra del material de programa o requiere funciones de no estándar (trick-play), el procesamiento requerido utiliza datos extraídos del dispositivo de almacenamiento de medios de comunicación 528 y no de los datos que fluyen en vivo. Debido a que el rebobinado y el avance entre visionado en tiempo real y datos que fluyen en vivo se minimizan o eliminan, se minimiza la sincronización de los datos recuperados del dispositivo de almacenamiento de medios de comunicación 528.

En una realización de la presente invención el flujo de datos recibidos en el IRD 132 comprende además meta-datos, incluyendo datos para control derechos de reproducción y protección de copias. Estos meta-datos pueden cifrarse y almacenarse en el dispositivo de almacenamiento de medios de comunicación 528, para un descifrado y un uso cuando se reciba una solicitud de visionado del programa de medios de comunicación. Alternativamente, los meta-datos pueden cifrarse y difundirse en el flujo de datos en tiempo real para todos los programas de medios de comunicación con capacidad PPV, evitando de este modo la necesidad de almacenar la información en el dispositivo de almacenamiento de medios de comunicación 528.

Según lo descrito anteriormente, la relación entre el CWP 504 y el programa de medios de comunicación cifrado puede variar en el tiempo. En la realización anterior de la presente invención, el tiempo de expiración asociado a los SCIDs para el material de programa procedente del CWP 506 puede sencillamente ignorarse.

Aunque lo anterior se ha descrito con respecto a los diferentes módulos de cifrado (por ejemplo, módulos 514 y 522) y a los módulos de descifrado (por ejemplo, módulos 508, 510, 532 y 534), lo anterior puede implementarse con un único módulo de cifrado, un único módulo de descifrado, o uno o más módulos de cifrado/descifrado. En una realización de la presente invención, las operaciones ejecutadas por los módulos 508, 522 y 532 se ejecutan en un único dispositivo de circuito integrado, por ejemplo el CAM 406.

Conclusión

La presente invención describe un sistema y un método para grabar material de programa para su reproducción subsiguiente, en los que vídeo/audio/flujos de datos cifrados con el material de programa se descifran antes de almacenarse en disco. La clave de CW 509 se decodifica desde el CWP 504 a través del CAM 406. Esto requiere que se creen nuevas funciones de CAM 406 para permitir la compra previa del programa de IPPV, con antelación, y que se almacene esta información de compra previa en el CAM 406 o la unidad de disco. Estas nuevas funciones de

CAM 406 pueden usarse para correlacionar diferentes derechos de reproducción de un servicio de difusión, para controlar la duración de tiempo durante el cual puede reproducirse el servicio de difusión. Las nuevas funciones de CAM 406 incluyen también nuevos paquetes de datos de derecho de nueva reproducción, que no tienen una relación de fecha de expiración con los SCIDs asociados al material de programa. El derecho de reproducción o de nueva reproducción y la expiración del programa no limitan el servicio de recuperación desde la unidad de disco. Esta realización no requiere que el CWP 504 se almacene en la unidad de disco.

Además del procesamiento de los meta-datos de derecho de reproducción, el CAM 406 gestiona la generación, el cifrado y el descifrado de la clave de CP 516 y de la clave de CAM 520. Una versión de la clave de CP 516 cifrada por la clave de CAM 520 se almacena en la unidad de disco. Durante la recuperación, los meta-datos de reproducción se extraen del disco (en la forma de la clave de CP cifrada 516) y se entregan al CAM 406. Alternativamente, los meta-datos de reproducción pueden almacenarse y recuperarse en el CAM 406 en lugar (o además) del disco duro. La clave de CP 516 también se recupera del disco y se usa para descifrar el material de programa recifrado 518. En una realización, el CAM 406 incluye también un módulo para instalar y restaurar claves de CP 516 y claves de CAM 520. Preferiblemente la clave CP 516 y la clave de CAM 520 se generan, almacenan y mantienen en un dispositivo a prueba de falsificaciones. Aunque el CWP 504 no se almacena normalmente en el dispositivo de almacenamiento de medios de comunicación 528, los nuevos meta-datos que correlacionan derechos de reproducción y copia con el flujo de difusión se almacenan en el dispositivo de almacenamiento de medios de comunicación 528.

Durante la recuperación, el CAM 406 genera la clave de CP 516 usada para descifrar los datos almacenados en el dispositivo de almacenamiento de medios de recuperación 528. Con las propiedades de la clave de CP cifrada 524 y las funciones adicionales del CAM 406, el CAM 406 descifra la clave de CP cifrada 524 usando la clave de CAM 520.

En la presente invención las funciones de cifrado, descifrado y generación de la clave de CP se realizan fuera del CAM 406. En lugar de una única clave de CAM 520 almacenada dentro del propio CAM 406, podría usarse una única clave de IRD o caja almacenada en el IRD 132. Para aumentar todavía más la seguridad, todas estas funciones de generación de clave y cifrado/descifrado podrían integrarse en el chip de transporte del IRD 132. Esto hace muy difícil de ejecutar el examen de las funciones de cifrado/descifrado y generación de clave. Esto ayuda a garantizar la integridad del sistema, minimiza el número de cambios en la arquitectura actual del CAM 406, y permite que el sistema sea menos dependiente del CAM 406.

La anterior descripción de la realización preferida de la invención se ha presentado con fines de ilustración y descripción. No pretende ser exhaustiva ni limitar la invención a la forma precisa descrita. Son posibles muchas modificaciones y variaciones a la luz de las enseñanzas anteriores. Se pretende que el alcance de la invención no esté limitado por esta descripción detallada, sino más bien por las reivindicaciones adjuntas a la misma. La presente memoria, ejemplos y datos proporcionan una descripción completa de la fabricación y utilización de la composición de la invención que reside en las reivindicaciones adjuntas a la misma.

REIVINDICACIONES

1.- Un método de almacenamiento de material de programa en un dispositivo de almacenamiento de medios, acoplado comunicativamente a un receptor para su subsiguiente reproducción, que comprende los pasos de:

(a) admitir información de control de acceso cifrada y el material de programa cifrado de acuerdo con una primera clave de cifrado en el receptor, incluyendo la información de control de acceso una primera clave de cifrado y los datos de control;
(b) descifrar la información de control de acceso recibida en un módulo de acceso condicional (CAM) (406) acoplado comunicativamente y que puede ser insertado por el abonado en el receptor para producir la primera clave de cifrado;
(c) descifrar el material de programa usando la primera clave de cifrado;
(d) recifrar o volver a cifrar el material de programa, de acuerdo con una segunda clave de cifrado (516);
(e) cifrar la segunda clave de cifrado (516) en el CAM (406) de acuerdo con una tercera clave de cifrado (520) para producir una cuarta clave de cifrado (524); y
(f) proporcionar el material de programa recifrado (518) y la cuarta clave de cifrado (524) para su almacenamiento;

en el que la información de control de acceso comprende además meta-datos que describen al menos un derecho para el material de programa;
comprendiendo además el paso de:
generar la segunda clave de cifrado al menos en parte desde los meta-datos.

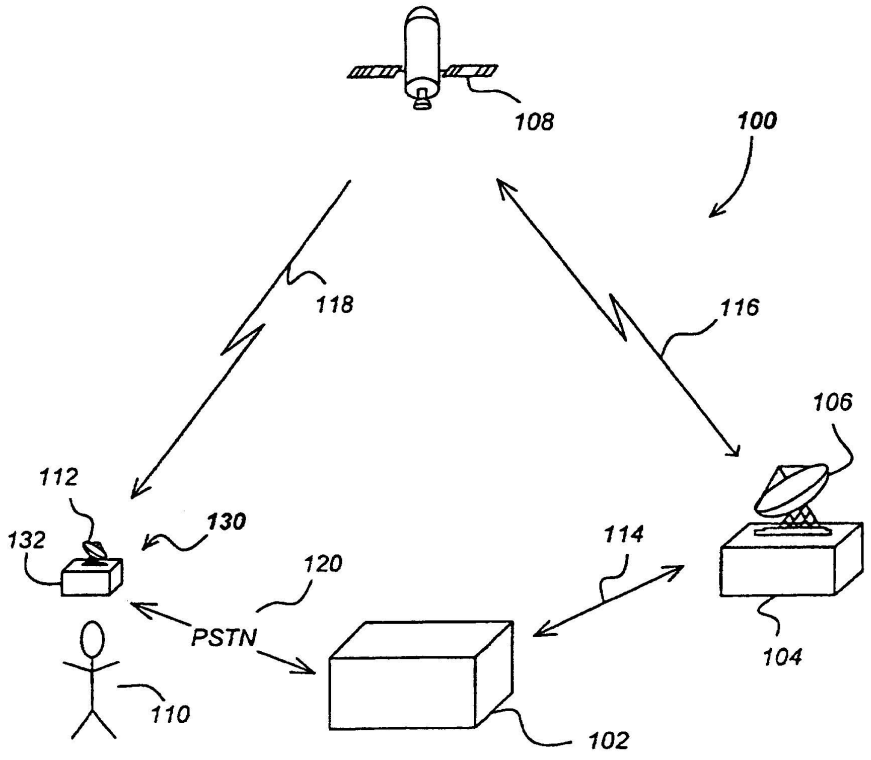

FIG. 1

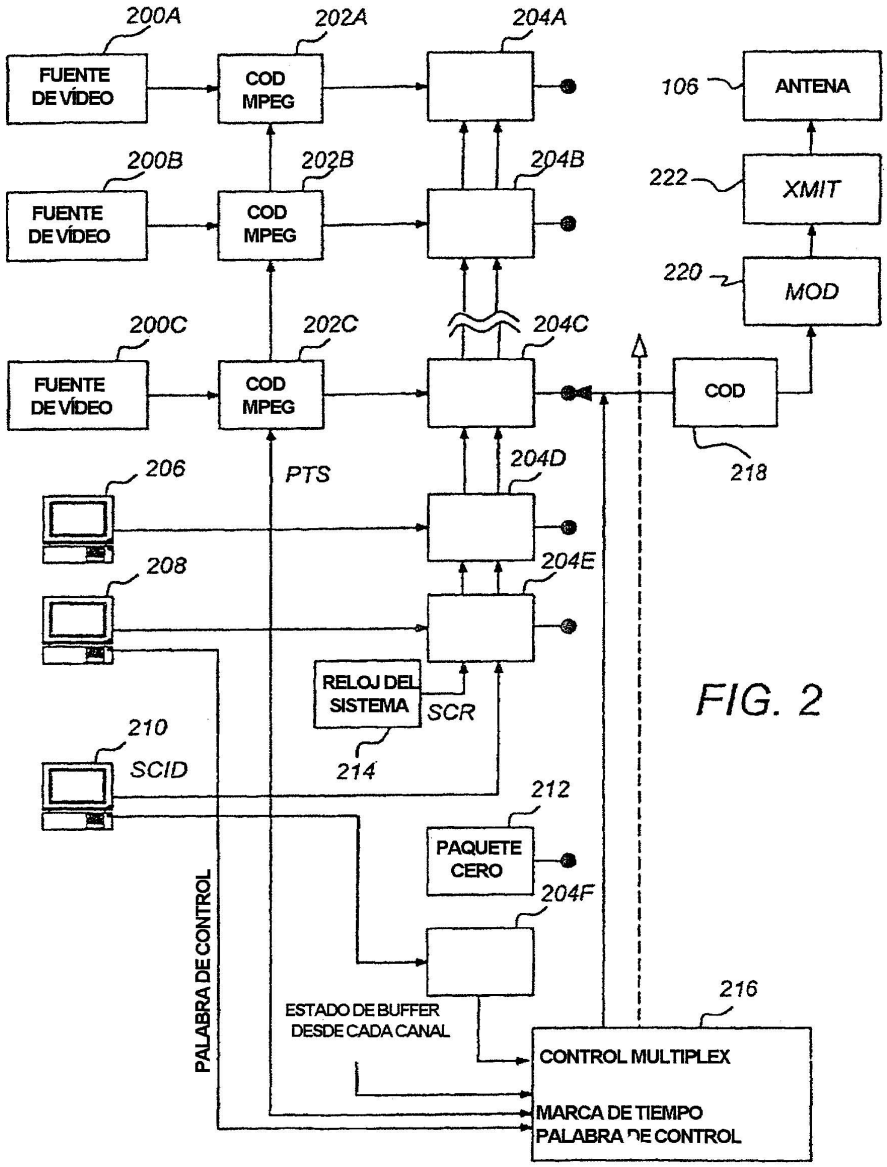
200A
FUENTE DE VÍDEO
202A
COD MPEG
204A
106
ANTENA
200B
FUENTE DE VÍDEO
202B
COD MPEG
204B
222
XMIT
220
MOD
200C
FUENTE DE VÍDEO
202C
COD MPEG
204C
COD
218
206
PTS
204D
208
204E
RELOJ DEL SISTEMA
SCR
214
210
SCID
212
PAQUETE CERO
204F
PALABRA DE CONTROL
ESTADO DE BUFFER DESDE CADA CANAL
216
CONTROL MULTIPLEX
MARCA DE TIEMPO
PALABRA DE CONTROL

FIG. 2

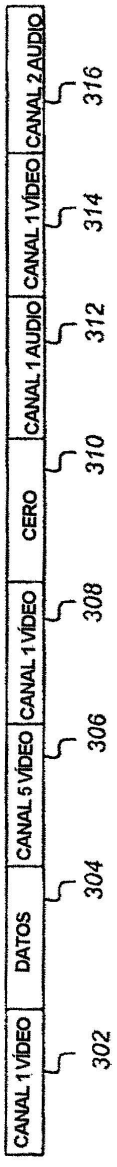
CANAL 1 VÍDEO
DATOS
CANAL 5 VÍDEO
CANAL 1 VÍDEO
CERO
CANAL 1 AUDIO
CANAL 1 VÍDEO
CANAL 2 AUDIO
302
304
306
308
310
312
314
316

FIG. 3A

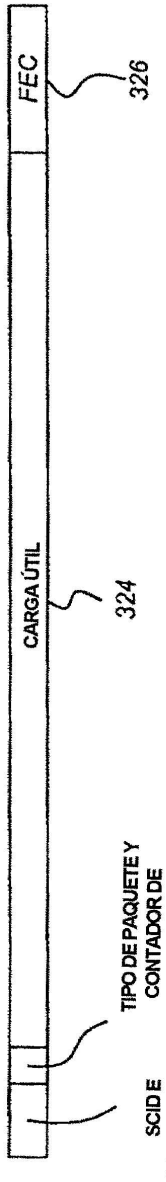
CARGA ÚTIL
FEC
326
324
TIPO DE PAQUETE Y CONTADOR DE CONTINUIDAD
SCID E INDICADORES 320

FIG. 3B

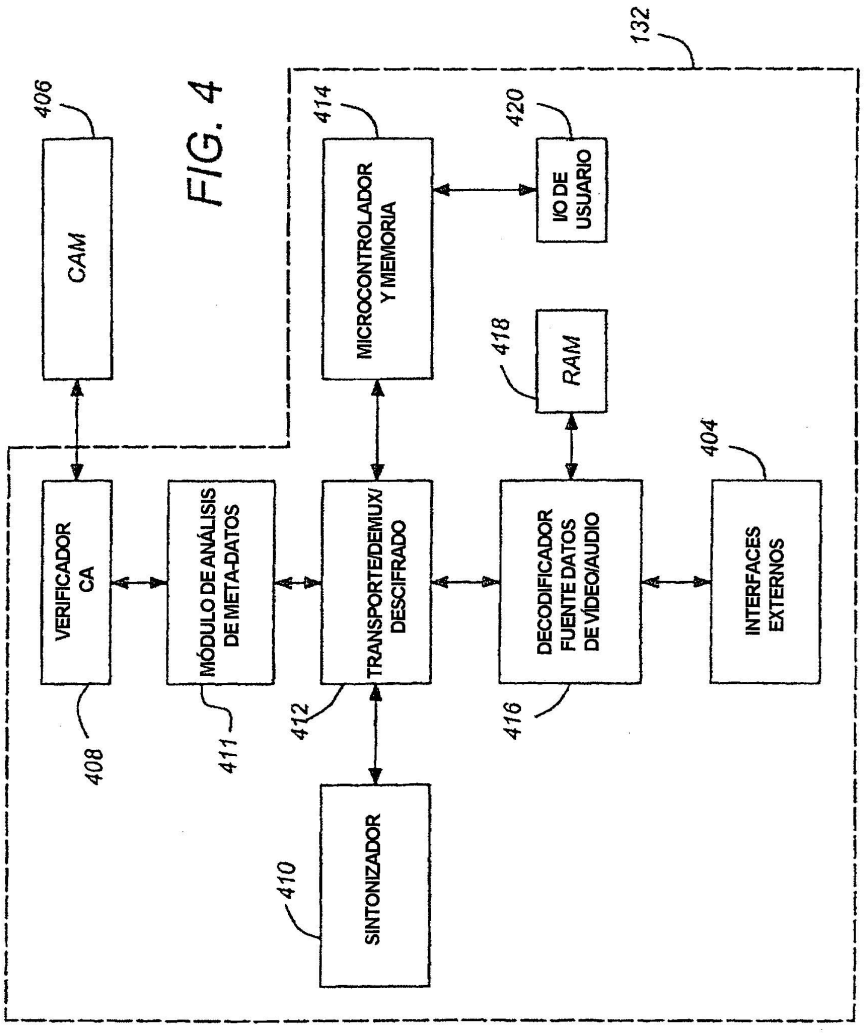
132
406
CAM
414
MICROCONTROLADOR Y MEMORIA
420
I/O DE USUARIO
418
RAM
404
VERIFICADOR CA
MÓDULO DE ANÁLISIS DE META-DATOS
TRANSPORTE/DEMUX/ DESCIFRADO
DECODIFICADOR FUENTE DATOS DE VÍDEO/AUDIO
INTERFACES EXTERNOS
408
411
412
416
SINTONIZADOR
410

FIG. 4

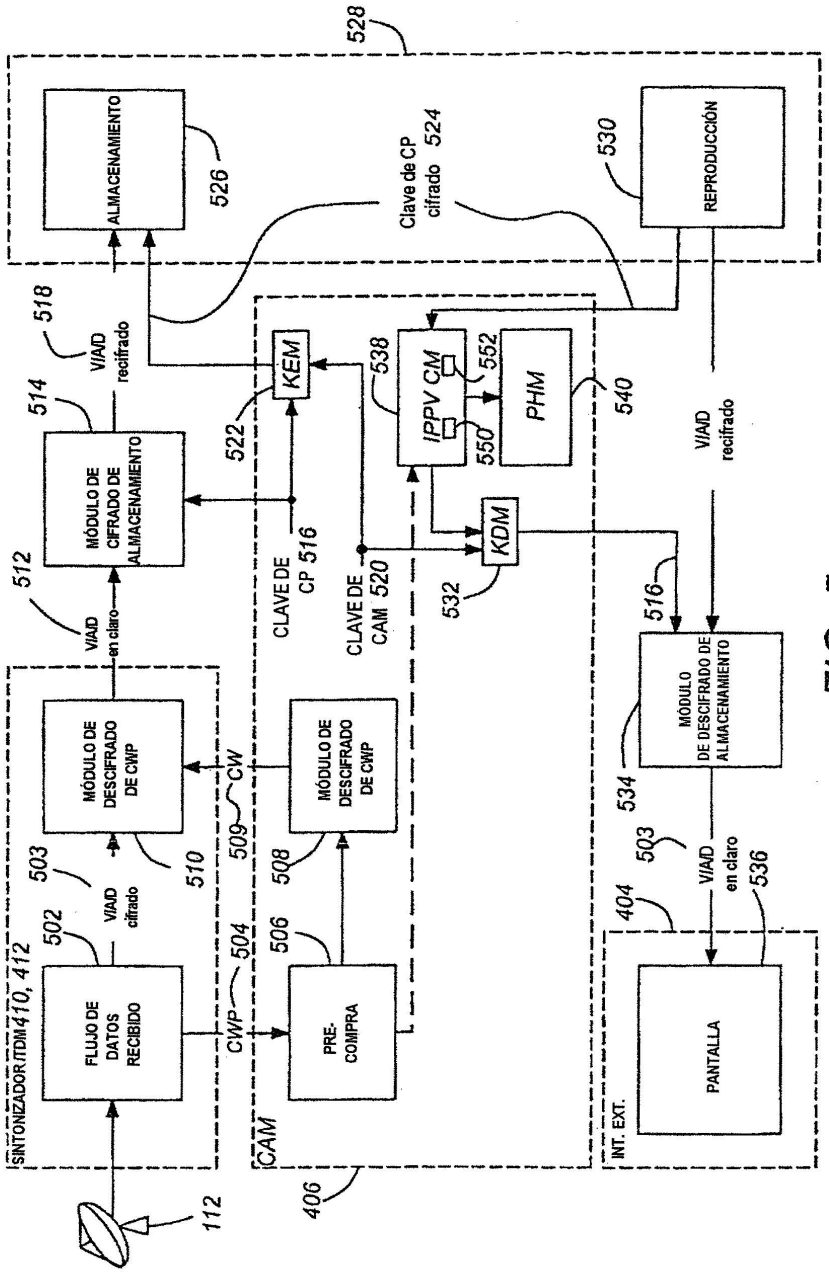
528
ALMACENAMIENTO
526
Clave de CP cifrado 524
530
REPRODUCCIÓN
518
V/AD recifrado
514
MÓDULO DE CIFRADO DE ALMACENAMIENTO
512
V/AD en claro
KEM
522
538
IPPV CM
552
PHM
540
550
KDM
532
CLAVE DE CP 516
CLAVE DE CAM 520
V/AD recifrado
516
MÓDULO DE DESCIFRADO DE ALMACENAMIENTO
534
503
V/AD en claro
536
404
INT. EXT.
PANTALLA
MÓDULO DE DESCIFRADO DE CWP
MÓDULO DE DESCIFRADO DE CWP
CW
509
508
510
503
V/AD cifrado
502
FLUJO DE DATOS RECIBIDO
504
CWP
506
PRE-COMPRA
SINTONIZADOR/DM 410, 412
CAM
406
112

FIG. 5