



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 306 683**

(51) Int. Cl.:
H04N 5/913 (2006.01)
H04N 7/167 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(86) Número de solicitud europea: **01117556 .9**
(86) Fecha de presentación : **20.07.2001**
(87) Número de publicación de la solicitud: **1175096**
(87) Fecha de publicación de la solicitud: **23.01.2002**

(54) Título: **Almacenamiento seguro y reproducción de programas de medios de difusión empleando un receptor y un dispositivo de almacenamiento emparejados.**

(30) Prioridad: **21.07.2000 US 620833**

(73) Titular/es: **The DIRECTV Group, Inc.**
2230 East Imperial Highway
El Segundo, California 90245, US

(45) Fecha de publicación de la mención BOPI:
16.11.2008

(72) Inventor/es: **Kahn, Raynold M.;**
Gagnon, Gregory J.;
Ha, David D.;
Klauss, Peter M.;
Curren, Christopher P. y
James, Thomas H.

(45) Fecha de la publicación del folleto de la patente:
16.11.2008

(74) Agente: **Elzaburu Márquez, Alberto**

ES 2 306 683 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Almacenamiento seguro y reproducción de programas de medios de difusión empleando un receptor y un dispositivo de almacenamiento emparejados.

La presente invención se refiere a sistemas y métodos para suministrar material de programas de vídeo a abonados y, en particular, a un método y sistema para almacenar y reproducir con seguridad programas de medios de difusión.

En años recientes ha habido un interés creciente en permitir que abonados de televisión por cable y por satélite graben programas de medios de difusión para visión posterior. Esta capacidad, denominada en lo sucesivo videograbación personal (PVR: personal vídeo recording), puede ser usada para proporcionar servicios de vídeo a petición (VOD: video-on-demand), o para permitir simplemente que el abonado conserve programas de medios de difusión con fines de visión repetida y/o archivo.

En el pasado, magnetoscopios han sido usados para tal videograbación personal. Recientemente, sin embargo, discos duros, similares que los usados en ordenadores personales, han sido usados para almacenar programas de medios de difusión para visión posterior. A diferencia de los magnetoscopios, tales dispositivos no incluyen típicamente un sintonizador y en cambio están acoplados al receptor por satélite o descodificador de cable. También a diferencia de los magnetoscopios, estos dispositivos son usados típicamente para grabar contenido digital, no vídeo analógico. Esta diferencia es tanto ventajosa como desventajosa.

Una ventaja de tales dispositivos es que permiten almacenamiento a largo plazo y reproducciones múltiples sin degradación sustancial. Otra ventaja es que permiten funciones de trucaje más rápidas tales como avance y rebobinado rápidos. Una desventaja de tales dispositivos es que también son capaces de hacer copias de generación múltiples del material de programa y sin degradación importante. Esto provoca la posibilidad muy real de que las copias de generación múltiple de los programas de medios de difusión sean producidas y distribuidas sin permiso. Esta posibilidad ha causado que algunos proveedores de medios de difusión estén poco dispuestos a permitir que sus programas de medios de difusión sean grabados por tales dispositivos.

Para mejorar este problema, es crítico proteger los programas de medios de difusión almacenados con seguridad fuerte y control de copia. Los dispositivos actuales no mezclan los programas de medios de difusión antes del almacenamiento ni almacenan información de protección contra copia. En cambio, tales dispositivos graban contenido de programa descifrado en el disco de almacenamiento usando un esquema de hardware emparejado en el que el controlador de disco duro y el disco duro están emparejados entre sí específicamente a través de una interfaz específica. Como el controlador de disco duro y el propio disco están emparejados esencialmente entre sí, el almacenamiento o la reproducción no funcionará si el disco fuera separado y transferido a otro reproductor. La debilidad de este esquema de seguridad es que solo confía en el hardware emparejado para garantizar seguridad..... los programas de medios de difusión almacenados en la propia unidad de disco no están cifrados.

Aunque supuestamente sería posible almacenar simplemente la corriente de datos cuando es recibida desde el emisor de radiodifusión para reproducción posterior, esta técnica tiene desventajas claras. Una desventaja tal es que proporcionaría a los piratas una versión grabada permanentemente de la corriente de datos cifrada, proveyendo así al pirata de información que puede ser usada para realizar análisis detallados de la propia corriente de datos para determinar las técnicas y códigos de cifrado.

Un método para grabar y reproducir datos de vídeo según la técnica anterior es descrito en el documento EP-A-0 975 165. El documento se refiere a un sistema de radiodifusión por satélite para difundir datos de vídeo a solicitud de un usuario. Una reproducción de los datos de vídeo recibidos es controlada transmitiendo adicionalmente señales de control de acceso. Las señales de control de acceso indican cualquier condición a ser puesta para la reproducción de los datos de vídeo recibidos. Después de la recepción y el desmezclado de las videoseñales difundidas, el procesamiento adicional depende de las condiciones indicadas por las señales de control de acceso recibidas. En una realización de pago posterior, por ejemplo, si las señales de control de acceso indican que el videoprograma recibido no puede ser reproducido, la indicación respectiva es almacenada y los datos de vídeo desmezclados son cifrados de acuerdo con una clave criptográfica. La clave criptográfica es prealmacenada, suministrada por un controlador de acceso, incluida en las videoseñales o incluidas en las señales de control de acceso. Las videoseñales cifradas son grabadas en un soporte de almacenamiento. Previo pago por el usuario, una señal de control de acceso es transmitida por el emisor de radiodifusión que indica que el videoprograma grabado en forma cifrada puede ser reproducido ahora. Por consiguiente, la videoseñal grabada es descifrada de acuerdo con la clave criptográfica. Otro ejemplo de un sistema de grabación/reproducción de datos de audio/vídeo es descrita en el documento EP-A-0 989 557. El sistema incluye un descodificador (STB: set top box) y un magnetoscopio (VTR: video tape recorder). El descodificador (STB) recibe desde un receptor de radiodifusión por satélite datos de audio/vídeo mezclados junto con una clave mezcladora cifrada (Ks) junto con información (ECM: Entitlement Control Message = mensaje de control de autorización, EMM: Entitlement Management Message = mensaje de gestión de autorización) necesaria para descifrar la clave Ks sobre la base de una identificación de usuario. La clave cifrada Ks es necesaria para desmezclar los datos de audio/vídeo recibidos. Un recifrado adicional de los datos de audio/vídeo desmezclados es realizado empleando una clave Kco de contenido. La clave Kco de contenido generada también es cifrada basada en una clave pública STB Pa almacenada en el descodificador (STB) y que es individual para cada descodificador (STB). Tanto los datos de audio/vídeo cifrados Kco (D) como la clave de contenido cifrada STB Pa (Kco) son transmitidos al magnetoscopio (VTR) y grabados en

él. Durante la reproducción, una clave secreta STB Sa, que corresponde a la clave pública STB Pa, es usada para descifrar la clave de contenido cifrada STB Pa (Kco). La clave secreta es individual e inherente para cada descodificador (STB). Después, los datos de audio/vídeo cifrados Kco (D) son descifrados para reproducción empleando la clave de contenido descifrada Kco. Por tanto, la reproducción solo es posible por el sistema que tiene la clave secreta inherente en el descodificador (STB).

Lo que es necesario es un sistema y método para grabar con seguridad programas de medios de difusión (incluyendo programas de pago por visión de compra impulsiva) para reproducción de uso limitado en un momento posterior. Tal sistema podría ser usado para soportar vídeo a petición, permitiendo así que el abonado adquiera programas de medios de difusión y juegos desde el descodificador (STB) instantáneamente sin preocuparse de la hora de comienzo del programa. Lo que también es necesario es un sistema y método que no precise cambios sustanciales en el hardware de abonado, tal como el receptor/descodificador integrado (IRD: integrated receiver/decoder) o el módulo de acceso condicional (CAM: conditional access module) que es usado para proporcionar una clave para descifrar los programas de medios de difusión para presentación a los abonados.

Esto es conseguido por las características de las reivindicaciones independientes.

La presente invención elimina inquietudes con respecto a la proliferación de copias digitales no autorizadas de los programas de medios de difusión mediante el uso de un método de cifrado fuerte. Además, la presente invención asegura que el material almacenado no puede ser distribuido puesto que tal descifrado del material solo puede ser realizado satisfactoriamente por el receptor/descodificador integrado (IRD) de cifrado. Al mismo tiempo, la presente invención puede ser implementada con cambios mínimos en el receptor/descodificador integrado (IRD) y sin cambios en la interfaz de módulo de acceso condicional (CAM). La presente invención también proporciona una base para un trayecto de crecimiento a técnicas de cifrado/descifrado más avanzadas.

Refiriéndose ahora a los dibujos en los que números de referencia iguales representan partes correspondientes en todos ellos:

la Figura 1 es un diagrama que muestra una vista general de un sistema de distribución de vídeo;

la Figura 2 es un esquema de bloques que muestra una configuración de enlace ascendente típico que muestra como material de videoprograma es enlazado hacia arriba con un satélite para la transmisión a abonados que usan un solo transpondedor;

la Figura 3A es un diagrama de una corriente de datos representativa recibida desde un satélite;

la Figura 3B es un diagrama que ilustra la estructura de un paquete de datos;

la Figura 4 es un esquema de bloques que ilustra un esquema de bloques de alto nivel del receptor/descodificador integrado (IRD); y

la Figura 5 es un esquema que ilustra el almacenamiento y la recuperación de datos desde un dispositivo de almacenamiento de medios de difusión.

En la descripción siguiente se hace referencia a los dibujos adjuntos que forman una parte de esto y que muestran, a modo de ilustración, varias realizaciones de la presente invención.

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

El centro 104 de enlace ascendente recibe material de programas e información de control de programas desde el centro 102 de control y, usando una antena 106 de enlace ascendente, transmite el material de programas y la información de control de programas al satélite 108. El satélite 108 recibe y procesa esta información y transmite los videoprogramas y la información de control al receptor/descodificador integrado 132 en la estación receptora 130 por vía del enlace descendente 118. El receptor/descodificador integrado 132 recibe esta información usando una antena 112 de abonado acoplada comunicativamente.

El sistema 100 de distribución de vídeo puede comprender pluralidad de satélites 108 para proporcionar cobertura terrestre más extensa, proporcionar canales adicionales o proporcionar anchura de banda adicional por canal. En una realización de la invención, cada satélite comprende 16 transpondedores para recibir y transmitir material de programas y otros datos de control desde el centro 104 de enlace ascendente y suministrarlo a los abonados 110. Sin embargo, usando técnicas de compresión y multiplexación de datos, las capacidades de canales son mucho mayores.

ES 2 306 683 T3

Por ejemplo, dos satélites 108 trabajando conjuntamente pueden recibir y difundir más de 150 canales de audio y vídeo convencionales (no de televisión de alta definición (HDTV)) por vía de 32 transpondedores.

Aunque la invención expuesta en esto será descrita con referencia a un sistema 100 de distribución de vídeo basado en satélite, la presente invención también puede ser puesta en práctica con transmisión de base terrestre de información de programas, tanto por medios de radiodifusión tradicionales, cable u otros medios. Además, las funciones diferentes asignadas colectivamente entre el centro 102 de control y el centro 104 de enlace ascendente como se describió antes pueden ser reasignadas como se desee sin apartarse del alcance propuesto de la presente invención.

Aunque lo anterior ha sido descrito con respecto a una realización en la que el material de programa suministrado al abonado es material de programa de vídeo (y audio) tal como una película, el método anterior puede ser usado para suministrar material de programa que comprende puramente información de audio o datos también.

La Figura 2 es un esquema de bloques que muestra una configuración de enlace ascendente típico para un solo transpondedor de satélite 108, que muestra como el material de videoprograma es enlazado hacia arriba con el satélite 108 por el centro 102 de control y el centro 104 de enlace ascendente. La Figura 2 muestra tres videocanales (que podrían ser aumentados respectivamente con uno o más audiocanales para música de alta fidelidad, información de pista sonora de película o un audioprograma secundario para transmitir idiomas extranjeros), y un canal de datos procedente de una fuente 206 de datos de ordenador.

Los videocanales son proporcionados por una fuente 200A-200C de programas de material de vídeo (designada colectivamente en lo sucesivo como fuente(s) 200 de vídeo). Los datos procedentes de cada fuente 200 de videoprogramas son proporcionados a un codificador 202A-202C (designado colectivamente en lo sucesivo como codificador(es) 202). Cada uno de los codificadores acepta una marca cronológica de presentación (PTS: presentation time stamp) procedente del controlador 216. La marca cronológica de presentación (PTS) es una marca cronológica binaria envolvente que es usada para garantizar que la información de vídeo es sincronizada apropiadamente con la información de audio después de codificar y descodificar. Un marcador cronológico de presentación (PTS) es enviado con cada cuadro I de los datos codificados MPEG.

En una realización de la presente invención, cada codificador 202 es un codificador MPEG-2 (Motion Picture Experts Group) de segunda generación pero también pueden ser usados otros descodificadores que implementan otras técnicas de codificación. El canal de datos puede ser sometido a un esquema de compresión similar por un codificador (no mostrado) pero tal compresión es usualmente innecesaria o realizada por programa de ordenador en la fuente de datos de ordenador (por ejemplo, los datos fotográficos son comprimidos típicamente en archivos *.TIF (Tagged Image File) o archivos *.JPG (Joint Photographic Group) antes de la transmisión). Después de codificar mediante los codificadores 202, las señales son convertidas en paquetes de datos por un empaquetador 204A-204F (designado colectivamente en lo sucesivo como empaquetador(es) 204) asociado con cada fuente 200, 206-210.

Los paquetes de datos son ensamblados usando una referencia procedente del reloj 214 del sistema (SCR: system clock reference), una palabra de control (CW: control Word) generada por el gestor 208 de acceso condicional y un generador 210 de identificadores de canales del sistema (SCID: system channel identifier) que asocia cada uno de los paquetes de datos que son difundidos al abonado con un canal de programa. Esta información es transmitida a los empaquetadores 204 para uso en generar los paquetes de datos. Después, estos paquetes de datos son multiplexados en datos en serie, codificados, modulados y transmitidos. Un paquete especial conocido como un paquete de palabra de control (CWP: control word packet), que comprende datos de control que incluyen la palabra de control (CW) y otros datos de control usados como soporte para proporcionar acceso condicional al material de programa, también es cifrado y transmitido.

La Figura 3A es un diagrama de una corriente de datos representativa. El segmento 302 de primer paquete comprende información del videocanal 1 (datos procedentes, por ejemplo, de la primera fuente 200A de videoprogramas). El segmento 304 de paquete siguiente comprende información de datos de ordenador que fue obtenida, por ejemplo, de la fuente 206 de datos de ordenador. El segmento 306 de paquete siguiente comprende información del videocanal 5 (procedente de una de las fuentes 200 de videoprogramas), y el segmento de paquete siguiente incluye información del videocanal 1 (nuevamente, procedente de la primera fuente 200A de videoprogramas). Por tanto, la fuente de datos comprende una serie de paquetes procedentes de una cualquiera de las fuentes de datos en un orden determinado por el controlador 216. La corriente de datos es cifrada por el módulo 218 de cifrado, modulada por el modulador 220 (que usa típicamente un esquema de modulación por desplazamiento de fase en cuadratura (QPSK)) y suministrada al transmisor 222 que difunde la corriente de datos modulada en una anchura de banda de frecuencias al satélite por vía de la antena 106.

Los abonados 110 reciben programas de medios de difusión por vía de un receptor o receptor/descodificador integrado 132 de abonado. Usando el identificador de canal del sistema (SCID), el receptor/descodificador integrado (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, paquetes nulos creados por el módulo 212 de paquetes nulos pueden ser insertados en la corriente de datos como se desee.

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 un número de segmentos de paquete. El primer segmento 320 de paquete comprende

ES 2 306 683 T3

dos bytes de información que contiene el identificador de canal del sistema (SCID) y señalizadores. El identificador de canal del sistema (SCID) es un número único de 12 bits que identifica unívocamente el canal de datos de paquete de datos. Los señalizadores incluyen 4 bits que son usados para controlar si el paquete está cifrado y que clave debe ser usada para descifrar el paquete. El segundo segmento 322 de paquete está formado por un indicador de tipo de 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 nulo). Cuando es combinado con el identificador de canal del sistema (SCID), el tipo de paquete determina como será usado el paquete de datos. El contador de continuidad incrementa una vez para cada tipo de paquete e identificador de canal del sistema (SCID). El segmento siguiente 324 de paquete comprende 127 bytes de datos de carga útil, que es una porción del videoprograma provista por la fuente 200 de videoprogramas. El segmento final 326 de paquete son datos necesarios para realizar la corrección de errores hacia delante (FEC: forward error correction).

Los programas de medio de difusión son cifrados por el módulo 218 de cifrado antes de la transmisión para garantizar que son recibidos y vistos solo por abonados autorizados. Cada programa de medios de difusión es cifrado según una clave criptográfica alfanumérica denominada en lo sucesivo una palabra de control (CW). Esto puede ser efectuado por diversas técnicas de cifrado de datos que incluyen algoritmos simétricos, tal como la norma de cifrado de datos (DES: data encryption standard), y algoritmos asimétricos tal como el algoritmo Rivest-Shamir-Adleman (RSA).

Para descifrar los programas de medios de difusión, el receptor/descodificador integrado 132 de abonado 110 también debe tener acceso a la palabra de control (CW). Para mantener la seguridad, las palabras de control (CWs) no son transmitidas al texto en claro de receptor/descodificador integrado 132. En cambio, las palabras de control (CWs) son cifradas antes de la transmisión al receptor/descodificador integrado 132 de abonado. La palabra de control (CW) cifrada es transmitida al receptor/descodificador integrado 132 de abonado en un paquete de palabra (datos) de control.

En una realización, los datos en el paquete de palabra de control (CWP), que incluye la palabra de control (CW), son cifrados y descifrados por medio de lo que es denominado en lo sucesivo como un algoritmo indescifrable de entrada/salida.

Un algoritmo indescifrable de entrada/salida es un algoritmo que es aplicado a una corriente de datos de entrada para producir una corriente de datos de salida. Aunque la corriente de datos de entrada determina unívocamente la corriente de datos de salida, el algoritmo seleccionado es tal que sus características no pueden ser descifradas a partir de una comparación de incluso un gran número de corrientes de datos de entrada y salida. La seguridad de este algoritmo puede ser incrementada más añadiendo elementos funcionales adicionales que no son fijos (es decir, cambian en función del tiempo). Cuando tal algoritmo es provisto de corrientes de entrada idénticas, la corriente de salida provista en un instante dado puede ser diferente que la corriente de salida provista en otro instante.

Siempre que el módulo 218 de cifrado y el receptor/descodificador integrado 132 compartan el mismo algoritmo indescifrable de entrada/salida, el receptor/descodificador integrado 132 puede descodificar la información en el paquete de palabra de control (CWP) para recuperar la palabra de control (CW). Después, usando la palabra de control (CW), el receptor/descodificador integrado 132 puede descifrar el programa de medios de difusión de modo que puede ser presentado al abonado 110.

Para desalentar más la piratería, los datos de control necesarios para descifrar y ensamblar paquetes de datos en programas visibles de medios de difusión pueden ser variables en el tiempo (cambia con el tiempo la validez de los datos de control en un paquete de palabra de control (CWP) para descodificar un programa particular de medios de difusión). Esto puede ser implementado de varios modos.

Por ejemplo, como cada paquete de palabra de control (CWP) está asociado con un identificador de canal del sistema (SCID) para cada programa de medios de difusión, el identificador de canal del sistema (SCID) relacionado con cada paquete de palabra de control (CWP) podría cambiar en el tiempo.

Otro modo de implementar datos de control variables en el tiempo es asociar marcas cronológicas con la corriente de datos recibida y los datos de control de paquete de palabra de control (CWP). En este caso, la descodificación satisfactoria del paquete de palabra de control (CWP) para producir la palabra de control (CW) necesitaría la relación apropiada entre las marcas cronológicas para la corriente de datos y los datos de control en el paquete de palabra de control (CWP). Esta relación puede ser definida, por ejemplo, cambiando el esquema de descifrado usado para generar la palabra de control (CW) a partir del paquete de palabra de control (CWP) según la marca cronológica recibida para la corriente de datos. En este caso, si la marca cronológica de la corriente de datos recibida no coincide con el valor previsto, el esquema de descifrado incorrecto será seleccionado y la palabra de control (CW) apropiada (para descifrar el material de programa) no será producida. Sin embargo, si la marca cronológica de la corriente de datos recibida coincide con el valor previsto, el esquema de descifrado apropiado será seleccionado y el esquema de descifrado del paquete de palabra de control (CWP) producirá la palabra de control (CW) apropiada.

Los datos necesarios para recibir programas de medios de difusión de pago por visión (PPV) son almacenados en el paquete de palabra de control (CWP) y en otro paquete de datos conocido como el paquete de información de compra (PIP: purchase information parcel). Tanto el CWP como el PIP son difundidos al abonado por vía del sistema 100 de distribución de vídeo en tiempo real. Como se describe a continuación, el paquete de palabra de control (CWP)

ES 2 306 683 T3

es usado por el receptor/descodificador integrado 132 para recuperar programas de medios de difusión de pago por visión (PPV).

5 Generalmente, los servicios de pago por visión pueden incluir servicios de pago por visión asistido por operador (OPPV) y de pago por visión de compra impulsiva (IPPV). Cuando solicita servicios de pago por visión asistido por operador (OPPV), el abonado 110 debe decidir por adelantado si desea acceder a un programa particular de medios de difusión. Entonces, el abonado 110 llama a una entidad tal como el centro 102 de control y solicita acceso al programa de medios de difusión. Cuando solicita servicios de pago por visión de compra impulsiva, el abonado 110, mientras observa la guía de programas, mueve el cursor sobre el canal de televidente asociado con el programa deseado de medios de difusión y selecciona “entrar” (“enter”). Después de que la decisión y los derechos para adquirir un programa de pago por visión (PPV) son confirmados (por ejemplo, comprobando los bloqueos de canal, los límites de tarificación y los límites de compra), un paquete de información de compra (PIP) es recibido y almacenado en el módulo de acceso condicional (CAM) 406 de abonado (que es descrito con más detalle a continuación) para uso adicional. El módulo 406 de acceso condicional (CAM) asocia la información en el paquete de palabra de control (CWP) y el paquete de información de compra (PIP) y usa el PIP en conjunción con el CWP para verificar que el abonado 110 debería ser provisto de acceso al programa de medios de difusión y a descifrar el programa de medios de difusión.

20 Sin embargo, pedir programas de medios de difusión de pago por visión (PPV) por adelantado usando el paquete de información de compra (PIP) es limitado puesto que el PIP es difundido hasta 24 horas antes de que el propio programa de medios de difusión sea difundido. Puesto que el PIP es difundido en tiempo real, el receptor/descodificador integrado 132 no adquiere el PIP hasta que el abonado 110 no solicita realmente la compra de programa de medios de difusión de pago por visión.

25 La Figura 4 es un esquema de bloques simplificado de un receptor/descodificador integrado (IRD) 132. El IRD 132 recibe y descifra los programas de medios de difusión difundidos por el sistema 100 de distribución de vídeo. Estos programas de medios de difusión son dirigidos como corriente de datos al IRD 132 en tiempo real y pueden incluir, por ejemplo, servicios de vídeo, audio o datos.

30 El IRD 132 es comunicativamente acoplable a un módulo de acceso condicional (CAM) 406. El módulo 406 de acceso condicional (CAM) es implementado típicamente en una tarjeta inteligente o dispositivo similar que es provista al abonado 110 para ser insertada dentro del IRD 132. El CAM 406 interconecta con un verificador de acceso condicional (CAV: conditional access verifier) 408 que realiza al menos algunas de las funciones necesarias para verificar que el abonado 110 está autorizado para acceder a los programas de medios de difusión. El verificador 408 de acceso condicional (CAV) está acoplado comunicativamente a un módulo de análisis de metadatos (MAM) 411. Usando la información en la tabla de metadatos (por ejemplo, la Tabla 1 descrita a continuación), el MAM 411 actúa como un portero para determinar si los programas almacenados de medios de difusión serán descifrados y presentados al abonado 110. Esto es efectuado comparando los valores de metadatos con valores medidos o acumulados. El CAV 408 y el MAM 411 pueden ser implementados como módulos separados desde el módulo 412 de transporte/desmultiplexación/descifrado y del microcontrolador y memoria 414 como se muestra, o pueden ser implementados por medio de instrucciones de software almacenadas en la memoria y realizadas por el microcontrolador 414.

45 El IRD 132 comprende un sintonizador 410, un módulo de transporte y desmultiplexación (TDM) 412, que funciona bajo control de un microcontrolador y memoria asociada 414, un descodificador fuente 416 y la memoria de acceso aleatorio (RAM) 418 acoplada comunicativamente, y un dispositivo de entrada/salida (E/S) de usuario para aceptar órdenes del abonado 110 y para suministrar información de salida al abonado.

50 El sintonizador 410 recibe los paquetes de datos desde el sistema de distribución de vídeo y suministra los paquetes al módulo 412 de transporte y desmultiplexación (TDM). Usando los identificadores de canales del sistema asociados con cada programa de medios de difusión, el TDM 412 vuelve a ensamblar los paquetes de datos según el canal seleccionado por el abonado 110 y descifra los programas de medios de difusión usando la clave de palabra de control (CW). El TDM 412 puede ser implementado por un solo chip seguro (protegido) y está acoplado comunicativamente a un microcontrolador y memoria 414.

55 Una vez que los programas de medios de difusión son descifrados, son suministrados al descodificador fuente 416 que descodifica los datos de programas de medios de difusión según normas MPEG (Motion Picture Experts Group) o JPEG (Joint Photographic Experts Group) como se apropiado. Después, el programa descodificado de medios de difusión es suministrado a un convertidor digital/analógico (D/A) (si es necesario) y suministrado a interfaces externas 404 que pueden incluir un dispositivo de presentación de programa de medios de difusión tal como una televisión, un sistema de audio o un ordenador. El descodificador fuente 416 utiliza la memoria RAM 418 acoplada comunicativamente para realizar estas funciones.

60 La clave de palabra de control (CW) es obtenida del paquete de palabra de control (CWP) usando el verificador 408 de acceso condicional (CAV) y el módulo 406 de acceso condicional (CAM). El TDM 412 suministra el CWP al CAM 406 por vía del CAV 408. El CAM 406 usa el algoritmo indescifrable de entrada/salida para generar la CW que es devuelta al TDM 412. El TDM 412 usa la CW para descifrar los programas de medios de difusión. En la mayoría de los receptores/descodificadores integrados (IRDs) 132, el CAV 408 y el CAM 406 son capaces de descifrar un programa de medios de difusión de vídeo/audio/datos (V/A/D) cada vez.

ES 2 306 683 T3

Como se describió antes, para desalentar a posibles piratas, los datos de control en el CWP usado para descodificar un programa particular de medios de difusión pueden cambiar con el tiempo de modo que solo produce la CW apropiada cuando es aplicado a un programa de medios de difusión que tiene la marca cronológica apropiada. En este caso, el CAM 406 puede seleccionar y/o controlar el esquema de descifrado (por ejemplo, el algoritmo indescifrable de entrada/salida) según la marca cronológica asociada con la corriente de datos que transporta el programa de medios de difusión. Si el programa de medios de difusión está suficientemente separado en el tiempo, el esquema de descifrado incorrecto será usado y no será producida la palabra de control (CW) apropiada para descodificar el programa de medios de difusión.

Detalles adicionales con respecto al cifrado y descifrado de programas de medios de difusión pueden ser hallados en la Solicitud de Patente de EE.UU. n° de serie 09/491.959 en tramitación junto con la presente y cedida comúnmente.

La Figura 5 es un diagrama que presenta pasos de método ejemplar usados para poner en práctica una realización de la presente invención. Una corriente de datos es suministrada por la antena 112 de abonado y recibida por el sintonizador 410 y el módulo 412 de transporte y demultiplexación (TDM), como se muestra en el bloque 502. La corriente de datos incluye una pluralidad de paquetes de datos que incluyen el paquete de palabra de control (CWP), y material de programa que es cifrado según una primera clave criptográfica (CW). La corriente de datos también puede incluir metadatos que tienen derechos de reproducción. Los derechos de reproducción son parámetros necesarios para controlar la reproducción de servicios de pago por visión de compra impulsiva o pago por reproducción.

Cuando el abonado 110 elige adquirir el programa de medios de difusión, una solicitud de visión es suministrada y un módulo 504 de control de pago por visión de compra impulsiva (IPPV) en el módulo 406 de acceso condicional (CAM) controla si será proporcionado acceso al programa solicitado de medios de difusión. Si lo es, el módulo 506 de historial de compra recoge la información necesaria para enviar una factura para el programa de medios de difusión al abonado 110. Después de que el módulo 506 de historial de compra ha adquirido y grabado la información necesaria, el módulo 504 de control de pago por visión de compra impulsiva (IPPV) ordena al módulo 508 de extracción de palabra de control (CW) descifrar el paquete de palabra de control (CWP) para obtener la primera clave criptográfica (CW). En una realización, esto es realizado usando una forma complementaria del algoritmo indescifrable de entrada/salida que fue usado para cifrar la CW y otra información para formar el CWP. La clave criptográfica de CW resultante es suministrada a un módulo 510 de descifrado de difusión. El módulo 510 de descifrado de difusión usa la clave de CW para descifrar el programa de medios de difusión (denominado alternativamente en lo sucesivo como material de programa) para producir una versión en claro (no cifrada) del programa 512 de medios de difusión. El programa en claro resultante 512 de medios de difusión es aplicado a un módulo 514 de cifrado de almacenamiento donde el programa de medios de difusión es cifrado nuevamente según una segunda clave criptográfica 516 de protección contra copia (CP: copy protection). Esto es ilustrado en la casilla 514. En una realización, la clave 516 de protección contra copia (CP) es usada para cifrar y descifrar el programa de medios de difusión por medio de una técnica de cifrado tal como RSA (Rivest-Shamir-Adleman) o, preferiblemente, encadenamiento de bloques cifrados de DES-X, DES de 56 bits triple. DES (data encryption standard = norma de cifrado de datos) es preferida porque es computacionalmente más eficiente que RSA para realizar computaciones relacionada con el tiempo. En una realización, la clave 516 de protección contra copia (CP) es una clave que es única para cada receptor/descodificador integrado 132 y es almacenada en él.

Después, la propia clave 516 de protección contra copia (CP) es suministrada a un módulo 522 de cifrado de clave donde es cifrada con una tercera clave criptográfica (descodificador) 520 para producir una cuarta clave criptográfica (ilustrada en la Figura 5 como clave cifrada 524 de protección contra copia (CP)). La clave criptográfica 520 descodificador es única para cada receptor/descodificador integrado (IRD) 132 y está codificada típicamente de forma permanente en el IRD 132.

El material 518 de programa cifrado nuevamente y la clave cifrada 524 de protección contra copia (CP) son almacenados después en el dispositivo 528 de almacenamiento de medios de difusión como se muestra en el bloque 526. El dispositivo 528 de almacenamiento de medios de difusión podría incluir una unidad de disco duro, similar que la que es empleada en ordenadores personales, una unidad de disco duro magnetoóptico, una unidad de disco óptico o cualquier otro soporte en los que pueden ser grabados datos para reproducción subsiguiente.

Cuando el abonado 110 decide observar el material de programa grabado, una orden es suministrada al receptor/descodificador integrado (IRD) 132 por vía de la interfaz 420 de entrada/salida (E/S) de usuario. Después, el material de programa cifrado nuevamente y la clave cifrada 524 de protección contra copia (CP), almacenados en el dispositivo 528 de almacenamiento de medios de difusión, son recuperados como se muestra en el bloque 530. Después, la clave cifrada 524 de protección contra copia (CP) es suministrada al módulo 523 de descifrado donde es descifrada con la clave 520 de descodificador para producir la clave 516 de protección contra copia (CP).

La clave criptográfica 516 de protección contra copia (CP) es suministrada después al módulo 534 de descifrado de almacenamiento donde el material de programa es descifrado según la clave 516 de protección contra copia (CP). El material de programa descifrado (y ahora en claro) es suministrado ahora a una pantalla 536 u otro dispositivo de presentación.

En una realización, la clave 516 de protección contra copia (CP) es modificada con (por ejemplo, adjuntando o añadiendo) algunos o todos los metadatos recibidos en la corriente de datos de difusión antes de ser cifrada según la clave 520 de descodificador. En este caso, la clave cifrada 524 de protección contra copia (CP) no solo incluye el valor

ES 2 306 683 T3

de la clave 516 de protección contra copia (CP) sino también los metadatos. Cuando la clave cifrada 524 de protección contra copia (CP) es recuperada después desde el dispositivo 528 de almacenamiento de medios de difusión y es descifrada con la clave 520 de descodificador, la clave 516 de protección contra copia y los metadatos son recuperados también. Estos metadatos pueden ser comparados con otros datos (por ejemplo, la fecha y la hora del día) para imponer los derechos de reproducción como sea necesario.

La clave 516 de protección contra copia (CP) puede ser almacenada en un chip de transporte dentro del módulo 412 de transporte y desmultiplexación. Esto permite que la presente invención sea usada con un módulo 406 de acceso condicional (CAM) no modificado. Esto permite también el cifrado y el descifrado rápidos de información almacenada en el dispositivo 528 de almacenamiento de medios de difusión, lo que es particularmente ventajoso donde se desean funciones de trucaje.

Conclusión

La descripción anterior de la realización preferida de la invención ha sido presentada con fines de ilustración y descripción. No pretende ser exhaustiva o limitar la invención a la forma precisa expuesta. Muchas modificaciones y variaciones son posibles a la luz de la enseñanza anterior. Por ejemplo, las funciones de cifrado descritas en esto podrían ser realizadas por módulos de cifrado/descifrado separados o un solo módulo polivalente de cifrado/descifrado puedes ser utilizado para realizar las funciones de cifrado/descifrado de muchos módulos separados.

REIVINDICACIONES

1. Un método para almacenar material de programa para reproducción subsiguiente, que comprende los pasos de:
5 recibir una corriente de datos que comprende material de programa cifrado según una primera clave criptográfica;
descifrar el material de programa;
10 volver a cifrar el material de programa descifrado según una segunda clave criptográfica (516);
cifrar la segunda clave criptográfica (516); y
15 almacenar el material de programa cifrado nuevamente en un dispositivo (528) de almacenamiento de medios de difusión;

caracterizado porque

la corriente de datos recibida comprende además metadatos que incluyen información que describe derechos de
20 reproducción para el material de programa;

la segunda clave criptográfica (516) es derivada al menos en parte de los metadatos; y

la segunda clave criptográfica (516) es cifrada según una tercera clave criptográfica (520) para producir una segunda
25 clave criptográfica cifrada (524).

2. El método de la reivindicación 1, que comprende además los pasos de:

recuperar el material de programa cifrado nuevamente almacenado; y

30 descifrar el material de programa cifrado nuevamente recuperado.

3. El método de la reivindicación 1 o 2, que comprende además el paso de almacenar la segunda clave criptográfica
cifrada (524).

4. El método de la reivindicación 3, en el que el paso de descifrar el material de programa cifrado nuevamente
35 recuperado comprende los pasos de:

leer la segunda clave criptográfica cifrada almacenada (524);

40 descifrar la segunda clave criptográfica cifrada (524) con la tercera clave criptográfica (520) para producir la
segunda clave criptográfica (516); y

descifrar el material de programa cifrado nuevamente (518) usando la segunda clave criptográfica (516).

45 5. El método de la reivindicación 4, que comprende además los pasos de:

aceptar una solicitud de visión antes de leer la segunda clave criptográfica cifrada almacenada (524); y

50 grabar la información de facturación relativa al material de programa.

6. El método de la reivindicación 1, en el que la segunda clave criptográfica (516) es derivada al menos en parte de
una hora de difusión del material de programa.

7. El método de cualquiera de las reivindicaciones 1 a 6, en el que el paso de cifrar cifra la segunda clave crypto-
55 gráfica (516) y los metadatos según una tercera clave criptográfica (520) para producir la segunda clave criptográfica
cifrada (524) y comprende los pasos de

modificar la segunda clave criptográfica (516) con los metadatos; y

60 cifrar la segunda clave criptográfica modificada según una tercera clave criptográfica para producir la segunda
clave criptográfica cifrada.

8. Un receptor para almacenar material de programa para reproducción subsiguiente, que comprende:

65 un sintonizador (410), para recibir una corriente de datos que comprende información cifrada de control de acceso,
y material de programa cifrado según una primera clave criptográfica, incluyendo la información de control de acceso,
la primera clave criptográfica;

ES 2 306 683 T3

un módulo (406) de acceso condicional, comunicativamente acoplable al sintonizador (410), para descifrar la información cifrado de control de acceso para producir la primera clave criptográfica;

5 un primer módulo (510) de descifrado, acoplado comunicativamente al sintonizador (410) y comunicativamente acoplable al módulo (406) de acceso condicional para descifrar el material de programa usando la primera clave criptográfica;

10 un módulo de cifrado, acoplado comunicativamente al primer módulo (510) de descifrado y comunicativamente acoplable a un dispositivo (528) de almacenamiento de medios de difusión, para volver a cifrar el material de programa descifrado (512) según una segunda clave criptográfica (516) y para cifrar la segunda clave criptográfica (516); y

un dispositivo (528) de almacenamiento de medios de difusión para almacenar y recuperar el material de programa cifrado nuevamente (518);

15 **caracterizado** porque

la corriente de datos recibida por el sintonizador (410) comprende además metadatos que tienen información que describe derechos de reproducción para el material de programa;

20 el módulo de cifrado cifra la segunda clave criptográfica (516) según una tercera clave criptográfica (520) para producir una segunda clave criptográfica cifrada (524);

la segunda clave criptográfica (526) es derivada al menos en parte de los metadatos.

25 9. El receptor de la reivindicación 8, en el que el dispositivo (528) de almacenamiento de medios de difusión está adaptado además para almacenar y recuperar la segunda clave criptográfica cifrada (524).

30 10. El receptor de la reivindicación 9, que comprende además un segundo módulo de descifrado, comunicativamente acoplable al dispositivo (528) de almacenamiento de medios de difusión, para descifrar la segunda clave criptográfica cifrada (524) para producir la segunda clave criptográfica (516) usando la tercera clave criptográfica (520), y para descifrar el material de programa cifrado nuevamente (518) usando la segunda clave criptográfica (516).

11. El receptor de cualquiera de las reivindicaciones 8 a 10, que comprende además:

35 un dispositivo (420) de entrada/salida (E/S) de usuario para aceptar una solicitud de visión; y

un módulo (506) de facturación para aceptar y almacenar información de facturación con respecto al material de programa.

40 12. El receptor de cualquiera de las reivindicaciones 8 a 11, en el que la segunda clave criptográfica (516) y la tercera clave criptográfica (520) son únicas de receptor.

45 13. El receptor de cualquiera de las reivindicaciones 8 a 12, en el que el módulo de cifrado cifra la segunda clave criptográfica (516) y los metadatos modificando la segunda clave criptográfica (516) con los metadatos y cifrando la segunda clave criptográfica (516) modificada según la tercera clave criptográfica para producir la segunda clave criptográfica cifrada.

50

55

60

65

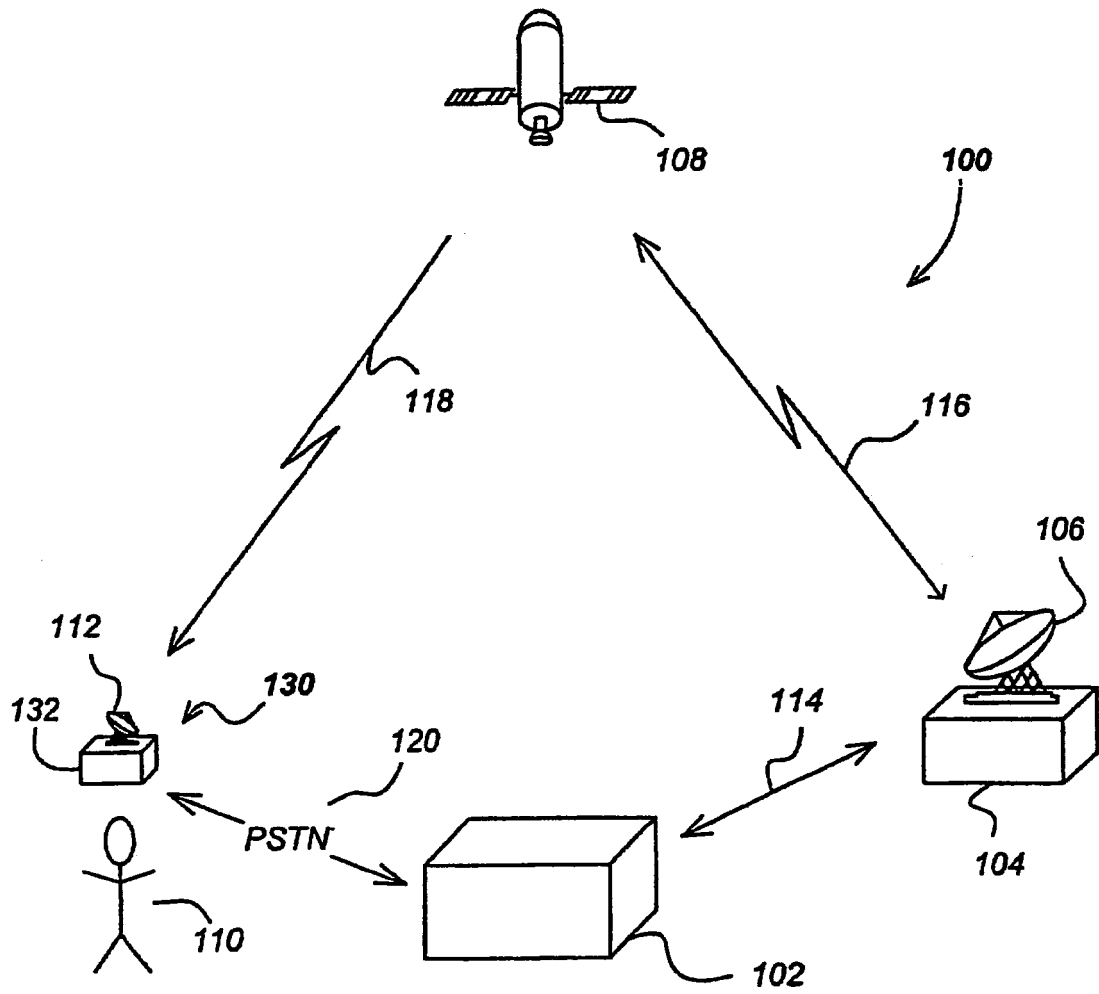


FIG. 1

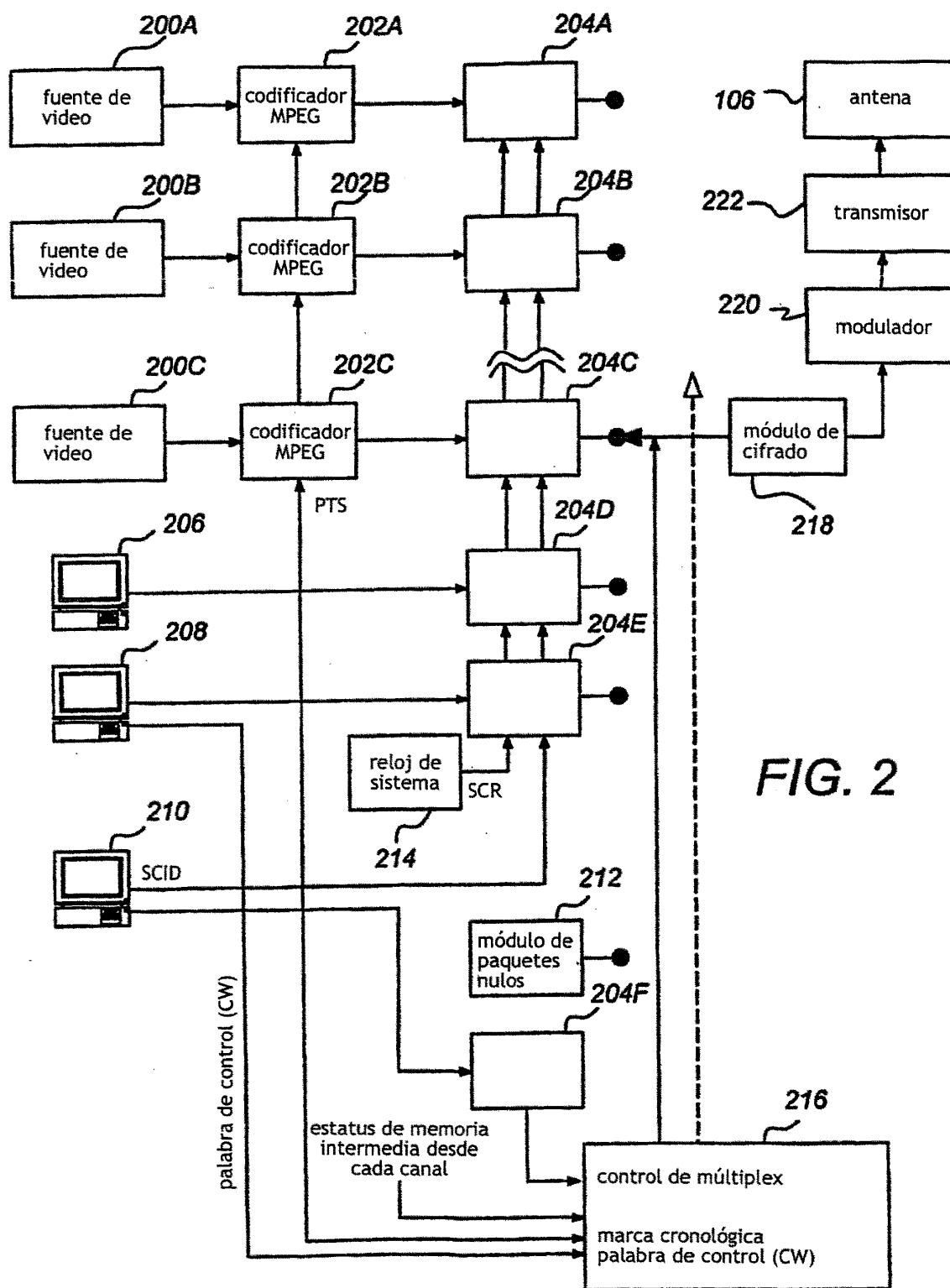


FIG. 2

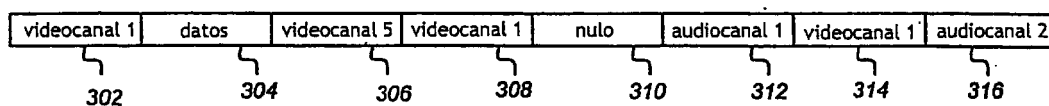


FIG. 3A

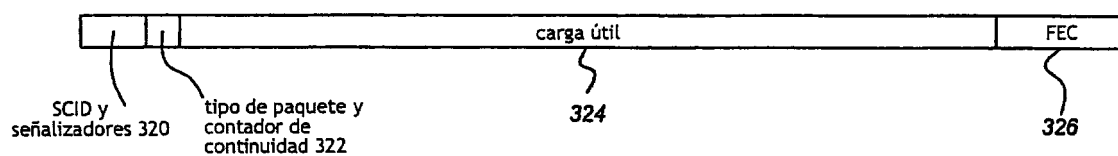
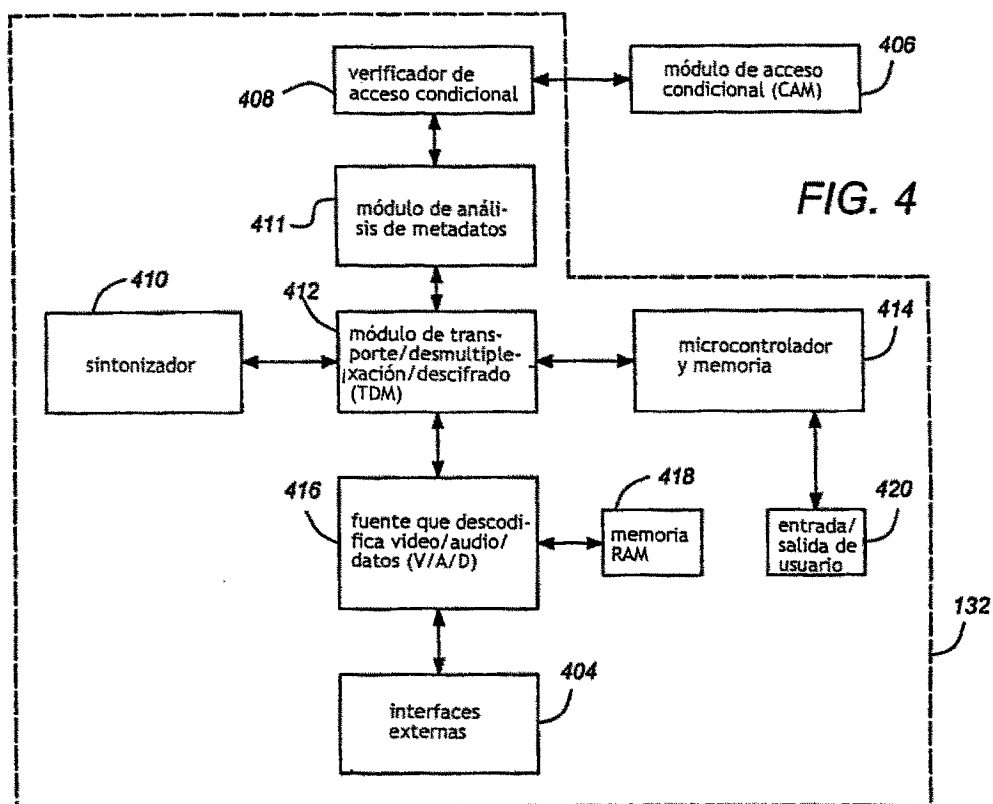


FIG. 3B



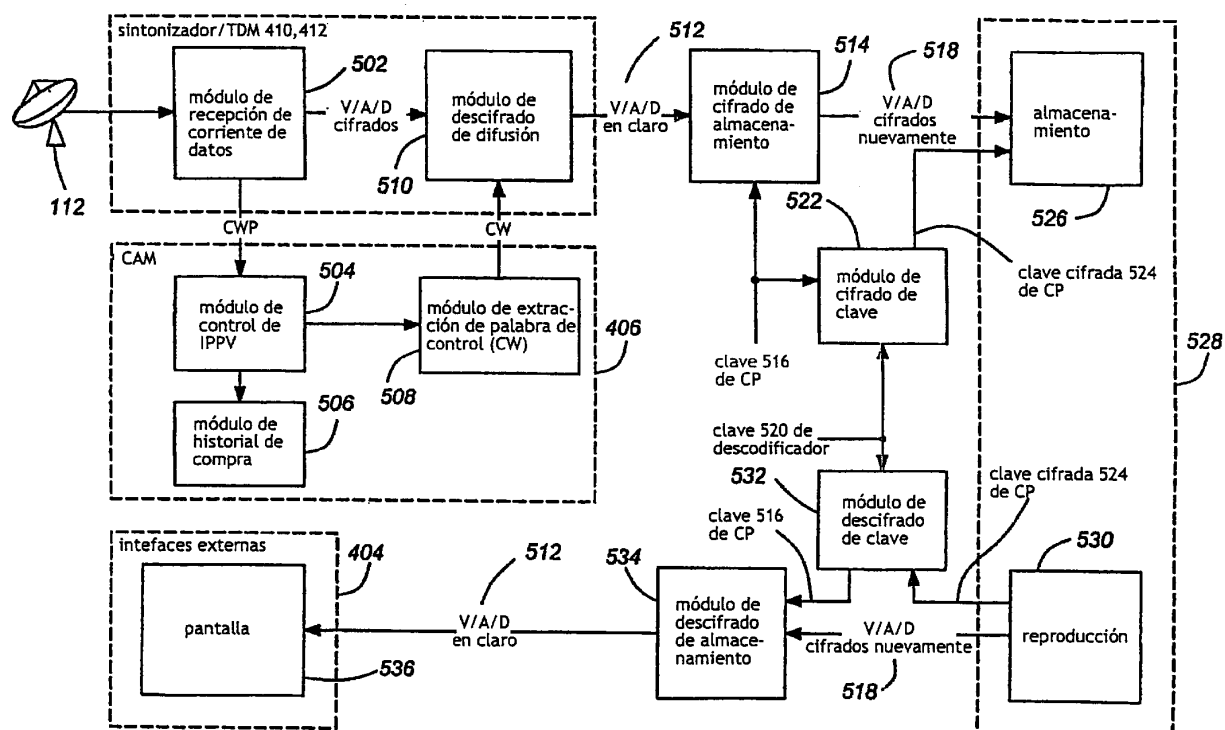


FIG. 5