

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 402 266**

51 Int. Cl.:

H04L 29/08 (2006.01)

H04L 29/06 (2006.01)

G06F 21/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **19.05.2004 E 04752783 (3)**

97 Fecha y número de publicación de la concesión europea: **11.07.2012 EP 1625479**

54 Título: **Procedimiento y sistema para compartir medios controlados en una red**

30 Prioridad:

21.05.2003 US 443929

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

30.04.2013

73 Titular/es:

**MUSIC PUBLIC BROADCASTING, INC. (100.0%)
55 RIVER STREET, SUITE 200
SANTA CRUZ, CALIFORNIA 95060, US**

72 Inventor/es:

**RISAN, HANK y
FITZGERALD, EDWARD V.**

74 Agente/Representante:

GARCÍA-CABRERIZO Y DEL SANTO, Pedro

ES 2 402 266 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

Procedimiento y sistema para compartir medios controlados en una red

5 Campo técnico

La presente descripción se refiere a la distribución de los medios dentro de una red. Más particularmente, la presente descripción se refiere a permitir compartir medios controlados entre una pluralidad de nodos en una red.

10 Antecedentes

Con los avances en tecnología de hardware y software, los ordenadores son herramientas integrales utilizadas en diversas aplicaciones, tales como finanzas, CAD (diseño asistido por ordenador), manufactura, salud, telecomunicaciones, educación, etc. Además, una mejora en la funcionalidad del ordenador puede ser realizada por acoplando comunicativamente ordenadores entre sí para formar una red. Dentro de un entorno de red, los sistemas de ordenador permiten a los usuarios intercambiar archivos, compartir información almacenada en bases de datos comunes, combinar o reunir recursos, por medio del correo electrónico (e-mail), y acceder a información en Internet. Además, los ordenadores conectados a un entorno de red, por ejemplo, Internet, proporcionan a sus usuarios acceso a datos e información de todo el mundo.

Algunos de los diferentes tipos de datos a los que un usuario puede tener acceso y compartir incluyen, pero no están limitados a, datos de texto como el que se encuentra en un documento de Word, los datos gráficos como la que se encuentra en las imágenes, por ejemplo, JPEGs, GIFs, TIFFs, datos de audio, tales como los que se encuentran en archivos de música, por ejemplo, archivos MP3, y datos de vídeo, como los que se encuentran en archivos de imágenes en movimiento, por ejemplo, archivos MPEG, MOV, y AVI, para nombrar unos pocos. De hecho, casi cualquier tipo de datos se pueden almacenar y compartir con otros sistemas de ordenador. En muchos casos, el material contenido dentro de los diversos tipos de datos es material con derechos de autor.

Hay muchos diferentes tipos de entornos de red que se pueden implementar para facilitar el intercambio de datos entre sistemas de ordenador. Algunos de los diferentes tipos de entornos de red incluyen Ethernet, cliente-servidor, y entornos de red por cable y/o inalámbricos. Una utilización común de un tipo de entorno de red es para uso compartido de archivos, tal como en una red P2P o red de punto a punto. La mayoría de las redes P2P se basan en modelos de negocio basados en la transmisión y la redistribución de material con derechos de autor, por ejemplo, archivos de audio, entre ordenadores acoplados a una red, por ejemplo, la Internet. Una red P2P permite a un usuario adquirir el material con derechos de autor desde un ordenador, una fuente del sitio web, o un organismo de radiodifusión de música, y almacenar y compartir el material con otros usuarios en toda la red, en algunos casos, actúan como una fuente de sitio web o una emisora de música.

También es común que los usuarios compartan archivos de forma incontrolada para utilizar aplicaciones de reproducción de medios libremente distribuidos o disponibles comercialmente para experimentar, por ejemplo, escuchar, ver y/o mirar los archivos compartidos. En muchos casos, estas aplicaciones de reproducción de medios también proporcionan descargar del archivo multimedia de una red P2P o de las emisoras web bajo licencia, guardarlo localmente y luego cargar el archivo multimedia en una red P2P ilegal o similar y/o en dispositivos de grabación del consumidor. Guardar ilegalmente un archivo multimedia puede ser tan simple como seleccionar la función de salvar o de grabar en una aplicación de reproducción de medios.

Además, muchos de los ordenadores, sitios web y emisoras web que comparten material con derechos de autor normalmente no controlan ni supervisan los archivos que se intercambian entre los equipos. Además, cuando los sitios web tratan de controlar o restringir la distribución de material con derechos de autor, por ejemplo, archivos de audio, los usuarios que buscan eludir los controles o restricciones pueden, en muchos casos, simplemente utilizar la funcionalidad de grabación de una aplicación de reproductor multimedia y guardar el material con derechos de autor, cambiar el nombre del archivo de audio en particular, y cargar el archivo renombrado, haciendo insignificantes los intentos de controlar o restringir su distribución.

Una desventaja de la distribución incontrolada de los archivos, más concretamente, la descarga, la grabación, y la carga de material con derechos de autor, por ejemplo, archivos de música, es que no existe actualmente ningún medio eficaz para indemnizar al propietario (por ejemplo, la compañía de discos, letrista, músico, etc.) del material con derechos de autor. Los estudios tienen pérdidas de ingresos de miles de millones debido a la copia no autorizada y la información inexacta de compensaciones por derechos de autor.

Los procedimientos actuales de intercambio de archivos de música no proporcionan suficientes controles de la distribución de archivos o de rendición de cuentas adecuada con respecto a los acuerdos de concesión de licencias y/o restricciones de derechos de autor asociados a material con derechos de autor compartido.

Además, los titulares de derechos de autor de archivos de medios se están vendiendo en la premisa de que un archivo de medios degradado es mejor que el original porque no se puede controlar el original en el ordenador. Por

lo tanto, los usuarios pueden ser menos propensos a usar un ordenador para grabar/capturar/reproducir una versión de baja calidad. Una vez que el usuario captura el archivo de medios, es una copia de sonido mediocre. Este concepto fundamental de las compañías discográficas que dan una versión de datos menos que la ideal es con la esperanza de que la falta de calidad de sonido disuadirá a los usuarios de grabar, copiar, etc., los archivos de medios.

Las solicitudes están fácilmente disponibles a través de Internet con el propósito expreso de producir una copia exacta de archivos de medios de audio. Un ejemplo es Exact Audio Copy, un programa de software gratuito disponible gratuitamente en Internet, que produce una copia exacta de audio en formato de archivo .wav. Además, hay aplicaciones de "realzado", fácilmente disponibles a través de Internet, que van a las pistas de audio donde se puede "realzar" el archivo de audio o vídeo.

Además, muchas de las aplicaciones de reproductor multimedia/grabador están diseñadas para capturar y grabar archivos multimedia entrantes de una forma que elude los controles implementados por una aplicación de reproducción de medios inherente a un sistema operativo, por ejemplo, QuickTime de Apple, Media Player para Windows™, etc. o descargable desde Internet, por ejemplo, RealPlayer, LiquidAudio, o las provistas por difusores de Internet, por ejemplo, PressPlay, para controlar la grabación no autorizada de archivos multimedia. Además, muchos dispositivos de grabación digital, por ejemplo, grabadoras de mini-disco, grabadoras de MP3, y similares, pueden ser acoplados a una salida digital de un sistema de ordenador, por ejemplo, un puerto USB, un DIF OUT S/P, y similares, para capturar el archivo multimedia.

Se desea evitar que las aplicaciones de grabación, tales como Total Recorder, Sound Forge, y muchos otros, que están adaptadas para establecer una conexión con un controlador de nivel de núcleo operable dentro de un sistema operativo para capturar y redirigir el archivo de medios para crear una reproducción no autorizada de un archivo multimedia. También se desea evitar que las aplicaciones de grabación accedan a un controlador de modo de núcleo de dispositivos de medios y la realización de copias no autorizadas de material con derechos de autor a través de alguna red disponible, por ejemplo, cable, inalámbrico, P2P, etc., o por medio de un acoplamiento comunicativo. Además, es deseable evitar el acceso a una unidad de dispositivo de medios de modo de núcleo mediante una aplicación de grabación con el propósito de hacer copias no autorizadas de archivos multimedia desde y hacia fuentes alternativas, por ejemplo, reproductores de CD, reproductores de DVD, discos duros extraíbles, dispositivos electrónicos y/o de grabación personales, por ejemplo, grabadores de MP3, y similares.

El documento US 2003/0014496 describe un sistema para la entrega de archivos de medios a un dispositivo de reproducción de medios digitales.

Los procedimientos actuales de control de la distribución de los medios de comunicación entre una pluralidad de nodos en un entorno de red son inadecuados.

Sumario

En consecuencia, existe una necesidad de un procedimiento y un sistema que controla el intercambio de medios entre una pluralidad de sistemas de ordenador en una red. La invención se define por un procedimiento de acuerdo con la reivindicación 1, un sistema de acuerdo con la reivindicación 10 y un medio legible por ordenador según la reivindicación 19. Realizaciones descritas en la presente memoria satisfacen las necesidades anteriormente mencionadas.

En una realización descrita en la presente memoria, un procedimiento para controlar los medios de comunicación que se comparten en una red incluye descodificar localmente en un nodo de origen una instancia de contenido de medios y la aplicación de un cifrado intermedio a la instancia de contenido de medios para la transferencia a un nodo solicitando la instancia de contenido de medios.

En otra realización descrita en la presente memoria, un procedimiento para controlar los medios de comunicación que se comparten en una red incluye proporcionar una ubicación de contenido de medios desde un nodo administrativo a un nodo solicitante del contenido de medios para transferir un ejemplo del contenido de medios desde un nodo fuente en la ubicación para la nodo que solicita el contenido de medios.

En otra realización, se describe un procedimiento para compartir los medios de comunicación de control entre una pluralidad de nodos de una red. El presente procedimiento se compone de hacer uso de la red de una instancia de contenido de medios para el intercambio de información entre la pluralidad de nodos mediante un nodo de origen acoplado con comunicación a la red. El presente procedimiento incluye además descifrar la instancia de contenido de medios desde un cifrado local al nodo de origen. El presente procedimiento incluye, además, el cifrado de la instancia de contenido de medios en un sistema de codificación intermedia. El presente procedimiento incluye, además, la transferencia de la instancia de contenido de medios a un nodo, mientras que el ejemplo de contenido de medios está en el cifrado intermedio. El nodo está asociado con la red. El descifrado y el cifrado y la transferencia son en respuesta a la recepción de una solicitud de la instancia de contenido de medios desde el nodo.

5 En otra realización, se describe otro procedimiento para compartir los medios controlados entre una pluralidad de nodos en una red. El presente procedimiento se compone de iniciar una búsqueda de una instancia de contenido de medios disponibles en la red. Un nodo acoplado en comunicación con la red inicia dicha búsqueda. El presente procedimiento incluye, además, recibir una ubicación de origen de la instancia de contenido de medios desde un nodo administrativo acoplado a la red. El presente procedimiento incluye, además, solicitar a la ubicación de origen de la instancia de contenido de medios. El presente procedimiento incluye, además, recibir la instancia de contenido de medios desde la ubicación. La instancia de contenido de medios se descifra desde un cifrado local a la ubicación de origen y cifrado en un cifrado intermedio antes de la entrega al nodo.

10 En otra realización, se describe otro procedimiento para compartir medios de comunicación controlados entre una pluralidad de nodos en una red. El presente procedimiento se compone de transmitir una ubicación de un nodo de origen que tiene una instancia de contenido multimedia a un nodo solicitante de la instancia de contenido de medios. El nodo de origen está acoplado en comunicación con la red. La transmisión es en respuesta a la red que recibe una solicitud de la instancia de contenido de medios. El presente procedimiento incluye, además, recibir desde el nodo de origen una solicitud de una clave de cifrado intermedio para cifrar la instancia de contenido de medios con una encriptación intermedia. El presente procedimiento incluye, además, el envío de la clave de cifrado intermedio al nodo de origen, permitiendo que el nodo de origen descifre la instancia de contenido de medios desde un cifrado local para el nodo de origen y para cifrar la instancia de contenido de medios en el cifrado intermedio para la transferencia. El presente procedimiento incluye, además, recibir un indicador de reconocimiento que indica la recepción con éxito de la instancia de contenido de medios por el nodo.

25 En todavía otra realización, se describe otro procedimiento para compartir medios controlados entre una pluralidad de nodos en una red. El presente procedimiento se compone de la transmisión de una instancia de contenido de medios desde un nodo fuente a un nodo. El nodo de origen, el nodo, y un nodo administrativo están acoplados con comunicación a la red. El presente procedimiento incluye, además, la transmisión desde el nodo al nodo administrativo de un indicador para indicar una transferencia exitosa de la instancia de contenido de medios desde el nodo de origen al nodo. El presente procedimiento incluye además generar una transacción correspondiente al nodo y asociada a la instancia de contenido de medios para la transmisión de la instancia de contenido de medios en el nodo. La generación de transacción se lleva a cabo por el nodo administrativo. El nodo y el nodo de origen actualmente están asociados con la red.

35 Estos y otros objetos y ventajas serán evidentes para los expertos de habilidad normal en la técnica después de haber leído la siguiente descripción detallada de las realizaciones preferidas que se ilustran en las distintas figuras de los dibujos.

Breve descripción de los dibujos

40 Los dibujos adjuntos, que se incorporan en y forman una parte de esta especificación, ilustran formas de realización que, junto con la descripción, sirven para explicar los principios reivindicados en la presente.

La Figura 1 es un diagrama de bloques de un sistema de ordenador ejemplar que puede utilizarse de acuerdo con una realización reivindicada aquí.

45 La Figura 2 es un diagrama de bloques de un entorno de red ejemplar que puede utilizarse de acuerdo con una realización reivindicada aquí.

La Figura 3 es un diagrama de bloques de los diversos componentes funcionales ejemplares de un mecanismo de cumplimiento de los derechos de autor de acuerdo con una realización reivindicada aquí.

50 La Figura 4 es una ilustración de un sistema ejemplar para la implementación de un mecanismo de cumplimiento de los derechos de autor de acuerdo con una realización reivindicada aquí.

55 La Figura 5A es un diagrama de bloques de flujo de datos que muestra una implementación de un mecanismo de cumplimiento de los derechos de autor para la prevención de la grabación no autorizada de los archivos de medios, de acuerdo con una realización reivindicada aquí.

60 La Figura 5B es un diagrama de bloques de flujo de datos que muestra una implementación de un componente de un mecanismo de cumplimiento de los derechos de autor para la prevención de la grabación no autorizada de los archivos de medios, de acuerdo con otra realización reivindicada aquí.

La Figura 5C es un diagrama de bloques de flujo de datos que muestra una implementación de un mecanismo de cumplimiento de los derechos de autor para prevenir la salida no autorizada de los archivos de medios, de acuerdo con una realización reivindicada aquí.

65 La figura 5D es un diagrama de bloques de flujo de datos que muestra una implementación de un mecanismo de cumplimiento de derechos de autor para la prevención de la salida no autorizada de los archivos de medios a

través de la captura de archivo de medios en un nivel de núcleo, de acuerdo con una realización reivindicada aquí.

5 La Figura 6A es un diagrama de bloques de un entorno para evitar la copia no autorizada de un archivo multimedia, de acuerdo con una realización reivindicada aquí.

10 Las Figuras 7A, 7B y 7C son un diagrama de flujo de las etapas realizadas de acuerdo con una realización reivindicadas en este documento para proporcionar un mecanismo de cumplimiento de los derechos de autor a una red de sistemas de ordenador de cliente y servidor.

15 La Figura 8 es un diagrama de un ejemplo de sistema global de entrega de medios en el que puede ser implementado un mecanismo de cumplimiento de los derechos de autor de acuerdo con una realización reivindicada aquí.

20 La figura 9 es un diagrama de bloques de componentes de un mecanismo de cumplimiento de derechos de autor instalable desde un dispositivo de almacenamiento de medios en los que están dispuestos los archivos de medios protegidos, de acuerdo con una realización reivindicada aquí.

25 La Figura 10 es un diagrama de bloques de un entorno de comunicación para la actualización dinámica de un mecanismo de cumplimiento de derechos de autor instalado desde un dispositivo de almacenamiento de medios en un sistema de ordenador del cliente, de acuerdo con una realización reivindicada aquí.

30 La Figura 11 es un diagrama de bloques de flujo de datos que muestra una implementación de un mecanismo de cumplimiento de los derechos de autor para impedir la reproducción no autorizada de un archivo de medios protegido situado en un dispositivo de almacenamiento de medios, de acuerdo con una realización reivindicada aquí.

35 La Figura 12 es un diagrama de bloques de componentes de un mecanismo de cumplimiento instalable desde un dispositivo de almacenamiento de medios en los que los archivos de medios protegidos están dispuestos, de acuerdo con una realización reivindicada aquí.

40 La Figura 13 es un diagrama de bloques de los componentes de un mecanismo de cumplimiento uso y de contenido dispuesto en un dispositivo de almacenamiento de medios, de acuerdo con una realización reivindicada aquí.

45 La Figura 14 es un diagrama de bloques de un entorno de comunicación para controlar la presentación de contenido en un dispositivo de almacenamiento de medios, de acuerdo con una realización reivindicada aquí.

50 La Figura 15 es un diagrama de bloques de flujo de datos que muestra una implementación de un mecanismo de cumplimiento de uso para controlar la presentación de contenido dispuesto en un dispositivo de almacenamiento de medios, de acuerdo con una realización reivindicada aquí.

55 La Figura 16 es un diagrama de flujo de un proceso para controlar la presentación del contenido dispuesto en un dispositivo de almacenamiento de medios, de acuerdo con una realización reivindicada aquí.

La Figura 17 es un diagrama de bloques de un entorno de red para el intercambio de contenido de medios entre los nodos dentro de la red de acuerdo con una realización reivindicada aquí.

La Figura 18 es un diagrama de bloques de los componentes dentro de un mecanismo de uso de cumplimiento ejemplar configurado para su utilización en una topología de red distribuido para el control de los medios que se comparten entre los sistemas de ordenador en la red, de acuerdo con una realización reivindicada aquí.

La Figura 19 es un flujo de datos que se ilustra de un sistema ejemplar para el control de los medios de comunicación compartido entre varios sistemas de ordenador acoplados con comunicación en una red de acuerdo con una realización reivindicada aquí.

Descripción detallada

60 Se hará ahora referencia en detalle a realizaciones de la invención, cuyos ejemplos se ilustran en los dibujos que se acompañan. Aunque la invención se describirá en conjunción con las realizaciones, se entenderá que no se pretende limitar la invención a estas realizaciones. Por el contrario, la invención está destinada a cubrir alternativas, modificaciones y equivalentes, como se define por las reivindicaciones adjuntas. Además, en la siguiente descripción detallada de realizaciones alternativas de la presente invención, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de la presente invención. Sin embargo, para un experto normal en la técnica, la presente invención puede ponerse en práctica sin estos detalles específicos. En otros casos, los procedimientos, procedimientos, componentes y circuitos bien conocidos no se han descrito en detalle para no

oscurecer innecesariamente aspectos de la presente invención.

5 Algunas porciones de la descripción detallada que sigue se presentan en términos de procedimientos, bloques lógicos, tratamiento y otras representaciones simbólicas de operaciones sobre bits de datos dentro de un sistema de la competencia o sistema de memoria digital. Estas descripciones y representaciones son los medios utilizados por los expertos en la técnica de procesamiento de datos a transmitir lo más efectivamente la sustancia de su trabajo a otros expertos en la técnica. Un procedimiento, bloque lógico, proceso, etc., es aquí, y generalmente, concebido para ser una secuencia de auto-consistente de pasos o instrucciones que conducen a un resultado deseado. Los pasos son los que implican manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas manipulaciones físicas toman la forma de señales eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas y manipuladas de otro modo en un sistema de ordenador o dispositivo similar de computación electrónica. Por razones de conveniencia, y con referencia al uso común, estas señales se conocen como bits, valores, elementos, símbolos, caracteres, términos, números, o similares, con referencia a la presente invención.

15 Debe tenerse en cuenta, sin embargo, que todos estos términos se han de interpretar como referencia a manipulaciones físicas y cantidades y son simplemente etiquetas convenientes y se han de interpretar además, en vista de los términos comúnmente utilizados en la técnica. A menos que se especifique lo contrario como evidente a partir de las discusiones siguientes, se entiende que la discusión de la presente invención se refiere a acciones y procesos de un sistema de ordenador, o dispositivo informático electrónico similar que manipula y transforma los datos. Los datos se representan como cantidades físicas (electrónicas) dentro de los registros y memorias del sistema de computación y se transforman en otros datos representados de manera similar como cantidades físicas dentro de las memorias del sistema de ordenador o de registros, u otros dispositivos tales de almacenamiento, transmisión, o de visualización de información.

25 Las realizaciones de la presente invención se describen principalmente en el contexto de una red de sistemas de ordenador, tales como una red de escritorio, de estación de trabajo, ordenador portátil, ordenador de mano y/o de otro dispositivo electrónico portátil. Para los fines de la presente solicitud, el término "dispositivo electrónico portátil" no se pretende que esté limitado únicamente a los ordenadores convencionales portátiles o de bolsillo. En cambio, el término "dispositivo electrónico portátil" también pretende incluir muchos dispositivos electrónicos móviles. Tales dispositivos móviles incluyen, pero no están limitados a, los reproductores de CD portátiles, reproductores de MP3, teléfonos móviles, dispositivos portátiles de grabación, radios satelitales, dispositivos portátiles de reproducción de vídeo (proyectores digitales), gafas de vídeo personal y otros dispositivos digitales personales. Además, las realizaciones de la presente invención también son adecuadas para la implementación de sistemas de presentación de teatro para la presentación pública y/o privada en teatros, auditorios, centros de convenciones, etc.

30 La Figura 1 es un diagrama de bloques que ilustra un sistema de ordenador ejemplar 100 que se puede utilizar de acuerdo con una realización de la presente invención. Se hace notar que el sistema de ordenador 100 puede ser casi cualquier tipo de sistema de ordenador o dispositivo de cálculo electrónico, incluyendo, pero no limitado a, un ordenador servidor, un ordenador de sobremesa, un ordenador portátil u otro dispositivo electrónico portátil. En el contexto de la presente invención, ciertos procesos, procedimientos y etapas discutidos se realizan como una serie de instrucciones (por ejemplo, un programa de software) que residen dentro de las unidades de memoria del sistema de ordenador del sistema de ordenador 100 y que son ejecutados por un procesador(es) del sistema de ordenador 100, en una realización. Cuando se ejecutan, las instrucciones hacen que el sistema de ordenador 100 realice acciones específicas y muestran un comportamiento específico que se describe aquí en detalle.

40 El sistema de ordenador 100 de la figura 1 comprende un bus de direcciones/datos 110 para comunicar la información, uno o más procesadores centrales 101 acoplados al bus 110 para procesar la información y las instrucciones. El procesador(es) 101 puede ser un microprocesador o cualquier tipo alternativo de procesador. El sistema de ordenador 100 también incluye un memoria volátil utilizable por ordenador 102, por ejemplo, la memoria de acceso aleatorio (RAM), RAM estática (SRAM), RAM dinámica (DRAM), RAM dinámica sincrónica (SDRAM), RAM doble velocidad de datos (DDR RAM), etc., acoplado al bus 110 para almacenar información e instrucciones para el procesador(es) 101. El sistema de ordenador 100 incluye además una memoria no volátil utilizable por el equipo 103, por ejemplo, memoria de sólo lectura (ROM), ROM programable electrónicamente, ROM programable (EPROM), ROM que se puede borrar eléctricamente (EEPROM), memoria flash (un tipo de EEPROM), etc., acoplada al bus 110 para almacenar información estática e instrucciones para el procesador(es) 101. En una realización, la memoria no volátil 103 puede ser desmontable.

50 El sistema 100 también incluye uno o más generadores de señales y recepción de los dispositivos, por ejemplo, dispositivo(s) de entrada/salida la señal 104 acoplado al bus 110 para permitir al ordenador 100 interconectar con otros dispositivos electrónicos. La interfaz de comunicación 104 puede incluir cable y/o la funcionalidad de la comunicación inalámbrica. Por ejemplo, en una realización, la interfaz de comunicación 104 es un puerto de comunicación de serie, pero alternativamente puede ser uno de un número de estándares y protocolos de comunicación bien conocidos, por ejemplo, un puerto paralelo, un adaptador Ethernet, un puerto FireWire (IEEE 1394), un bus de serie universal (USB), una interfaz de sistema de un pequeño ordenador (SCSI), un puerto de comunicación de infrarrojos (IR), un adaptador de comunicación inalámbrica Bluetooth, una conexión de banda

ancha, un enlace por satélite, un canal de Internet, un módem de cable, y similares . En otra realización, una línea de abonado digital (DSL) puede ser implementada como dispositivo de señal de entrada/salida 104. En tal caso, la interfaz de comunicación 104 puede incluir un módem DSL.

5 El ordenador 100 de la figura 1 también puede incluir uno o más dispositivo(s) de almacenamiento de datos utilizables por ordenador 108 acoplados al bus 110 para almacenar instrucciones e información, en una realización de la presente invención. En una realización, el dispositivo de almacenamiento de datos 108 puede ser un dispositivo de almacenamiento magnético, por ejemplo, una unidad de disco duro, una unidad de disquete, una unidad zip, o cualquier otro dispositivo de almacenamiento magnético. En otra realización, el dispositivo de
10 almacenamiento de datos 108 puede ser un dispositivo de almacenamiento óptico, por ejemplo, un CD (disco compacto), un DVD (disco versátil digital), u otro dispositivo de almacenamiento óptico alternativo. Alternativamente, cualquier combinación de dispositivos de almacenamiento magnético, óptico, y alternativo se puede implementar, por ejemplo, una configuración RAID (matriz aleatoria de discos independientes o matriz aleatoria de discos baratos). Se observa que el dispositivo de almacenamiento de datos 108 puede estar situado interna y/o
15 externamente del sistema 100 y acoplado en comunicación con el sistema 100 utilizando la tecnología por cable y/o de comunicación inalámbrica, proporcionando de ese modo de almacenamiento expandido y funcionalidad al sistema 100. Se observa además que casi cualquier dispositivo electrónico portátil, por ejemplo, el dispositivo 100a, también puede estar acoplado con comunicación con el sistema 100 a través de la utilización de cable y/o la tecnología inalámbrica, expandiendo de esta manera la funcionalidad del sistema 100.

20 El sistema 100 también puede incluir un dispositivo de visualización opcional 105 acoplado al bus 110 para la visualización de vídeo, gráficos y/o caracteres alfanuméricos. Se observa que el dispositivo de visualización 105 puede ser un CRT (tubo de rayos catódicos), una CRT delgada (TCRT), una pantalla de cristal líquido (LCD), una pantalla de plasma, una pantalla de emisión de campo (FED), gafas de vídeo, un dispositivo de proyección (por
25 ejemplo, una pantalla LCD o proyector DLP, un sistema de proyección de una sala de cine, y similares), o cualquier otro dispositivo de visualización adecuado para la visualización de vídeo, gráficos y caracteres alfanuméricos reconocibles para el usuario

30 El sistema de ordenador 100 de la Figura 1 incluye además un dispositivo alfanumérico de entrada opcional 106 acoplado al bus 110 para comunicar información y selecciones de comandos al procesador(es) 101, en una realización. El dispositivo de entrada alfanumérico 106 está acoplado al bus 110 e incluye teclas alfanuméricas y de función. También se incluye en el ordenador 100 un dispositivo de control del cursor opcional 107 acoplado al bus
35 110 para comunicar la información de entrada del usuario y las selecciones de comandos al procesador(es) 101. El dispositivo de control de cursor 107 puede ser implementado utilizando un número de dispositivos bien conocidos tales como un ratón, una bola de seguimiento, una almohadilla táctil, una palanca de mando, un dispositivo de seguimiento óptico, una pantalla táctil, etc. Se observa que un cursor puede ser dirigido y/o activado a través de la entrada del dispositivo de entrada alfanumérico 106 utilizando teclas especiales y comandos de secuencia de teclas. Además, se observa que la dirección y/o la activación del cursor pueden llevarse a cabo por medios alternativos, por
40 ejemplo, comandos activados por voz, proporcionados sistema de ordenador 100 está configurado con tal funcionalidad.

45 La Figura 2 es un diagrama de bloques de una red ejemplar 200 en el que las realizaciones de la presente invención pueden ser implementadas. En un ejemplo, la red 200 permite que uno o más sistemas de ordenadores de los clientes autorizados (por ejemplo, 210, 220, y 230), cada uno de los cuales están acoplados a Internet 201, recibir contenidos multimedia desde un servidor de contenido de medios, por ejemplo, 251, a través de la Internet 201 al tiempo que evita los sistemas de ordenador no autorizados tengan acceso a los medios de comunicación del cliente almacenados en una base de datos de servidor de contenido 251.

50 La red 200 incluye un servidor web 250 y un servidor de contenido 251 que están acoplados con comunicación a la Internet 201. Además, el servidor Web 250 y el servidor de contenidos 251 pueden estar comunicados sin utilizar Internet 201, como se muestra. El servidor Web 250, el servidor de contenidos 251, y los ordenadores de los clientes 210, 220, y 230 pueden comunicarse entre sí. Cabe señalar que los ordenadores y servidores de red 200 están bien adaptados a estar acoplados con comunicación en varias implementaciones. Por ejemplo, el servidor Web 250, el
55 servidor de contenido 251, y los sistemas de ordenador de los clientes 210, 220, y 230 de la red 200 pueden estar acoplados con comunicación a través de la tecnología de comunicación por cable, por ejemplo, cables de par trenzado, fibra óptica, cable coaxial, etc., o tecnología de comunicación inalámbrica, o una combinación de la tecnología de comunicación por cable e inalámbrica.

60 Todavía con referencia a la Figura 2, se observa que los servidores Web 250, el servidor de contenido 251, y los sistemas de ordenador de los clientes 210, 220 y 230 de la red 200 pueden, en una realización, ser aplicados cada uno de una manera similar al sistema de ordenador 100 de la Figura 1. Sin embargo, el servidor y los sistemas de ordenador en la red 200 no se limitan a dicha aplicación. Además, los servidor de web 250 y el servidor de contenidos 251 pueden realizar varias funcionalidades dentro de la red 200. También se observa que, en una
65 realización, el servidor web 250 y el servidor de contenidos 251 pueden tanto estar dispuestos en un único o en una pluralidad de sistemas de ordenador físicos, por ejemplo, el sistema de ordenador 100 de la Figura 1.

Además, se observó que la red 200 puede operar con y entregar cualquier tipo de contenido de medios, (por ejemplo, audio, vídeo, multimedia, gráficos, información, datos, programas de software, etc.) en cualquier formato. En un ejemplo, un servidor de contenidos 251 puede proporcionar archivos de audio y vídeo en los equipos del cliente 210-230 a través de Internet 201.

5 La Figura 3 es un diagrama de bloques de un mecanismo de cumplimiento de los derechos de autor ejemplar (CCM) 300, para controlar la distribución de, el acceso a, y/o el cumplimiento de los derechos de autor de archivos de medios, de acuerdo con una realización de la presente invención. En una realización, el CCM 300 contiene uno o más componentes de software e instrucciones para facilitar el cumplimiento con las restricciones de la DMCA (Digital Millennium Derechos de autor Act) y/o los acuerdos de licencia de la RIAA (Recording Industry Association of America) con respecto a los archivos multimedia. Además, los componentes de software del CCM 300 y las instrucciones más permitir el cumplimiento de las restricciones de grabación internacionales tales como los definidos por la IFPI (Federación Internacional de la Industria Fonográfica) y/o el ISRC (industria internacional de grabación estándar) y/u otras asociaciones de grabación extranjeras o internacionales y/o restricciones de licencias extranjeras o internacionales. En una realización, el CCM 300 puede estar integrado en reproductores multimedia y aplicaciones de grabadora existentes y/o de nuevo desarrollo. En otra realización, el CCM 300 puede ser implementado como independiente, pero en combinación con aplicaciones reproductor/grabador de medios existentes, de tal manera que el CCM 300 está acoplado con comunicación a las aplicaciones de reproductor/grabador de medios existentes. Alternativamente, el CCM 300 puede ser instalado como un mecanismo solo dentro de un sistema de ordenador de cliente 210. Además, el CCM 300 puede ser instalado como un solo mecanismo y/o como parte de una aplicación incluida en un dispositivo de almacenamiento de medios, por ejemplo, un CD, un DVD, una tarjeta SD (tarjeta digital segura), y/o como parte de un paquete de instalación. En otro ejemplo, el CCM 300 puede ser instalado en conjunto con una presentación de contenido de medios deseada, por ejemplo, escuchar un archivo de audio en un CD de música, la lectura de un documento, visualización de un vídeo, etc. Se observa que, en una realización, el CCM 300 puede ser instalado en el sistema del cliente 210 en forma clandestina, relativa a un usuario.

Actualmente hay dos tipos de licencias de derechos de autor reconocidas por la Digital Millennium Derechos de autor Act (DMCA) para la protección de los materiales con derechos de autor difundidos. Una de las licencias de difusión de derechos de autor es una licencia obligatoria, también conocida como una licencia legal. Una licencia estatutaria es definida como una licencia no-interactiva, es decir, el usuario no puede seleccionar la canción. Además, una advertencia de este tipo de licencia de transmisión es que un usuario no debe ser capaz de seleccionar un archivo de música particular con el propósito de grabarla en el sistema de ordenador del usuario o en otro dispositivo de almacenamiento. Otra advertencia de una licencia legal es que un archivo de medios no está disponible más de una vez durante un período de tiempo determinado. En un ejemplo, el período de tiempo puede ser de tres horas.

El otro tipo de licencia de transmisión reconocida por la DMCA es un acuerdo de licencia interactivo. Un acuerdo de licencia es comúnmente interactivo con el titular del derecho de autor, por ejemplo, una compañía discográfica, el artista, cuando el titular de derechos de autor otorga permiso para un servidor, por ejemplo, un servidor web 250 y/o un servidor de contenido 251 de la Figura 2 para emitir material con derechos de autor. En virtud de un acuerdo de licencia interactiva, hay una variedad de maneras en que el material con derechos de autor, por ejemplo, archivos de música, pueden ser difundidos. Por ejemplo, una manera en la que los archivos de música pueden ser transmitidos es permitir al usuario seleccionar y escuchar una grabación de sonido en particular, pero sin que el usuario esté habilitado para realizar una grabación de sonido. Esto se conoce comúnmente como un sistema interactivo de licencia "sin grabar", lo que significa que el usuario final no es capaz de guardar o almacenar el archivo de contenido de medios de una manera relativamente permanente. Además, otra forma en que archivos de música pueden ser transmitidos es permitir que un usuario no sólo seleccione y escuche un archivo de música particular, pero, además, permite al usuario guardar particularmente un archivo de música en el disco y/o grabar el archivo de música en CD, reproductor de MP3 u otro dispositivo electrónico portátil. Esto se conoce comúnmente como un sistema interactivo con licencia para "grabar", lo que significa que el usuario está habilitado para guardar, almacenar o grabar en un CD, el archivo de contenido de medios.

Se observa que la DMCA permite la "perfecta" reproducción de la grabación de sonido. Una copia perfecta de una grabación de sonido es una asignación uno a uno de la grabación de sonido original en una forma digitalizada, de tal manera que la copia perfecta es virtualmente indistinguible y/o no tiene diferencias acústicas con la grabación original.

En una realización, el CCM (mecanismo de cumplimiento de derechos de autor) 300 se puede almacenar en el servidor web 250 y/o servidor de contenido 251 de la red 200 y está configurado para ser instalado en cada sistema de ordenador de cliente, por ejemplo, 210, 220 y 230, habilitado para acceder los archivos multimedia almacenados en servidor de contenido 251 y/o servidor web 250. Alternativamente, el mecanismo de cumplimiento de derechos de autor 300 puede ser dispuesto externamente y acoplado en comunicación con un sistema de ordenador de cliente 200 a través de, por ejemplo, un dispositivo de medios portátil 100a de la Figura 1. En aún otra realización, el CCM 300 puede ser configurado para ser operable desde un dispositivo de almacenamiento de medios en los que los archivos de medios pueden ser dispuestos.

El mecanismo de cumplimiento de los derechos de autor 300 está configurado para ser operativo mientras que tiene partes de componentes, componentes enteras, combinaciones de componentes, dispuestos dentro de una o más unidades de memoria y/o dispositivos de almacenamiento de datos de un sistema de ordenador, por ejemplo, 210, 220, y/o 230.

5 Además, parte de los componentes, componentes completos y/o combinaciones de los componentes de CCM 300 pueden ser fácilmente actualizados, por ejemplo, a través de Internet 201, para reflejar los cambios o desarrollos en la DMCA, cambios o desarrollos en las restricciones de derechos de autor y/o acuerdos de concesión de licencias que se refieren a cualquier archivo de medios, cambios en las actuales aplicaciones de reproducción de medios y/o
10 el desarrollo de nuevas aplicaciones de reproductor de medios, o para contrarrestar los intentos subversivos y/o a modo de pirata para obtener ilegítimamente uno o más archivos de medios.

Haciendo referencia a la Figura 3, en una realización, el CCM 300 se muestra incluyendo instrucciones 301 para permitir al sistema de ordenador cliente 210 interactuar con el servidor web 250 y el servidor de contenido 251 de la red 200. Las instrucciones 301 permiten al sistema de ordenador cliente 210 interactuar con los servidores, por
15 ejemplo, 250 y 251 en una red, por ejemplo, 200.

El mecanismo de cumplimiento de los derechos de autor 300 también incluye, en una realización, un generador de ID de usuario 302, para la generación de una ID de usuario o clave de usuario, y una o más cookie(s) que
20 contiene(n) la información específica del usuario y el sistema de ordenador del usuario, por ejemplo, 210. En una realización, la ID de usuario y la cookie(s) se instalan en el sistema de ordenador 210 antes de la instalación de los componentes restantes del mecanismo de cumplimiento de derechos de autor 300. Se observa que la presencia de una cookie(s) válida y una ID de usuario/clave válida de usuario son verificadas por el servidor web 250 antes de que los restantes componentes de un CCM 300 se pueda instalar, en una realización de la presente invención.
25 Además, la identificación de usuario/clave de usuario puede contener, pero no se limita a, el nombre del usuario, la dirección del usuario, el número de tarjeta de crédito del usuario, un número de cuenta de pago en línea, una dirección de correo electrónico verificada, y una identidad (nombre de usuario) y la contraseña seleccionado por el usuario.

30 Además, la cookie puede contener, pero no se limita a, información específica para el usuario, información sobre el sistema de ordenador del usuario 210, por ejemplo, los tipos de aplicaciones operacionales de medios dentro de la misma, un identificador único asociado con el sistema de ordenador 210, por ejemplo, una dirección MAC (código de dirección de máquina), una dirección IP, y/o el número de serie de la unidad central de procesamiento (CPU) que funciona en el sistema de ordenador 210 y otra información específica del usuario y del sistema de ordenador
35 operado por el usuario.

Adicionalmente, en otra realización, los datos biométricos del usuario se pueden combinar con el sistema de ordenador 210 y los datos de usuario y los datos incorporados en la generación de una ID de usuario. Alternativamente, los datos biométricos pueden ser utilizados en una aplicación independiente en la generación de la
40 ID de usuario. Tipos de datos biométricos que se pueden utilizar para proporcionar una ID de usuario y/o autorización pueden incluir, pero no se limitan a, datos de huellas dactilares, datos de escaneo de retina, datos de huella de la mano, los datos de reconocimiento facial, y similares.

Se observa que la información referente al sistema de ordenador del cliente, por ejemplo, 210, el usuario del sistema
45 210, y una clave de acceso aquí descritos pueden ser denominados colectivamente como datos de autorización.

Ventajosamente, con la información sobre el usuario y el sistema de ordenador del usuario, por ejemplo, 210, el servidor web 250 puede determinar cuándo un usuario de un sistema de ordenador, por ejemplo, 210, ha dado su nombre de usuario y contraseña a otro usuario utilizando otro sistema de ordenador, por ejemplo, 220. Debido a que
50 el nombre de usuario, la contraseña y el sistema de ordenador del usuario 210 están estrechamente relacionados, el servidor web 250 puede prevenir el acceso no autorizado a contenido de medios con derechos de autor, en una realización. Cabe señalar que si el servidor web 250 detecta intercambio no autorizado de nombres de usuario y contraseñas, se puede bloquear al usuario del sistema de ordenador 210, así como a otros usuarios que ilícitamente han obtenido el nombre de usuario y contraseña, de futuro acceso a medios con derechos de autor de los medios disponibles a través del servidor web 250. El servidor web 250 puede invocar el bloqueo por cualquier período de
55 tiempo especificado, por ejemplo, por una cuestión de minutos o de horas a meses, años, o más.

Todavía con referencia a la Figura 3, el mecanismo de cumplimiento de derechos de autor 300 incluye además uno o más codificador/decodificadores (códec) 303 que, en una realización, está/están adaptados para realizar, pero no
60 está/están limitado a, codificación/decodificación de archivos de medios, compresión/descompresión de archivos de medios, detectando que los archivos de medios entregados se cifran según lo prescrito por CCM 300. En la presente realización, el codificador/decodificador 303 también puede extraer campos de clave de un encabezado asociado a cada archivo de contenido de medios para, en parte, la verificación de que el archivo se originó a partir de un servidor de contenido, por ejemplo, 251.

65

En la presente realización, el codificador/decodificador 303 también puede realizar una comprobación periódica y repetida del archivo de medios, mientras que el archivo de medios se pasa a la aplicación de reproductor de medios, por ejemplo, en una base marco a marco o en una base de memoria intermedia a memoria intermedia, para garantizar que las reglas CCM 300 se están aplicando en un momento determinado durante una reproducción. Se observa que diferentes codificador/decodificadores 303 pueden ser utilizados conjuntamente con varios tipos de contenido de medios con derechos de autor incluyendo, pero no limitado a, archivos de audio, archivos de vídeo, archivos gráficos, archivos alfanuméricos y similares, de manera que cualquier tipo de archivo de contenido de medios puede ser protegido de acuerdo con realizaciones de la presente invención.

Con referencia todavía a la Figura 3, el mecanismo de cumplimiento de derechos de autor 300 también incluye uno o más programas de agente 304 que están configurados para acoplarse en los cuadros de diálogo y negociar y coordinar la transferencia de información entre un sistema de ordenador, por ejemplo, 210, 220, o 230, un servidor, por ejemplo, el servidor web 250 y/o el servidor de contenidos 251, y/o aplicaciones de reproductor de medios, con o sin función de grabación, que son operables dentro de un sistema de ordenador de cliente, en una realización. En la presente realización, el programa de agente 304 también puede ser configurado para mantener el estado del sistema, verificar otros componentes que están siendo utilizados simultáneamente, para ser funcionales de forma autónoma sin el conocimiento del cliente, y también puede presentar los mensajes, por ejemplo, mensajes de error, información de medios, publicidad, etc., a través de una ventana de la pantalla o correo electrónico. Esta aplicación permite la detección de la implementación de la interfaz adecuada y la detección de las aplicaciones que se estén ejecutando. Se observó que los programas de agente se conocen bien en la técnica y pueden ser implementados en una variedad de maneras de acuerdo con la presente realización.

El mecanismo de cumplimiento de derechos de autor 300 también incluye uno o más ganchos de sistema 305, en una realización de la presente invención. Un gancho de sistema 305 es, en una realización, una biblioteca que está instalada en un sistema de ordenador, por ejemplo, 210, e intercepta eventos de ancho del sistema. Por ejemplo, un gancho de sistema 305, en conjunción con las interfaces 306, puede gobernar ciertas propiedades y/o funcionalidades de las aplicaciones de reproducción de medios que operan dentro del sistema de ordenador del cliente, por ejemplo, 210, incluyendo, pero no limitado a, los accesos directos de clic del ratón, atajos de teclado, aceleradores del sistema estándar, barras de progreso, funciones de guardado, funciones de pausa, funciones de rebobinado, omitir funciones de la pista, vista previa de la pista siguiente, copiar en un CD, copiar en un dispositivo electrónico portátil, y similares.

Se observa que el término gobierno o gobernar, para los propósitos de la presente invención, puede referirse a una deshabilitar, desactivar, permitir, activar, etc., de una propiedad o función. Gobernar también puede referirse a una exclusión de esa función o propiedad, de tal manera que una función o propiedad puede ser operable pero sin la posibilidad de realizar en la forma que se pretendía originalmente. Por ejemplo, durante la reproducción de un archivo de medios, la barra de progreso se puede seleccionar y trasladar de un lugar en la línea de avance a otro sin tener un efecto sobre la reproducción del archivo de medios.

Además, se observa que el códec 303 compara la información para la aplicación del reproductor de medios que opera en el sistema del equipo del cliente, por ejemplo, 210, con una lista de "firmas" asociadas con aplicaciones conocidas de grabación de medios. En una realización, la firma puede ser, pero no se limita a ser, un identificador único de una aplicación de reproductor de medios y que puede consistir en la clase de ventana de la aplicación, junto con una cadena de nombre de producto que es parte del título de la ventana para la aplicación. Ventajosamente, cuando las nuevas aplicaciones de reproducción de medios se desarrollan, sus firmas puede ser fácilmente añadidas a la lista de firmas a través de una actualización de CCM 300 se describe en la presente memoria.

El siguiente código fuente C++ es ejemplo de ejecución de la porción de un código 303 para la realización de detección de aplicación de reproductor de medios, de acuerdo con una realización de la presente invención. En otra realización, el siguiente código fuente puede ser modificado para detectar mecanismos del núcleo de emisión se abren dentro del sistema de cliente 210.

```

55     Int
        IsRecorderPresent (TCHAR * szAppClass,
                           TCHAR * szProdName)
    {
    { TCHAR szWndText [MAX_PATH];/* buffer to receive title string for window */
      HWND hWnd;/* handle to target window for operation */
60     Int nRetVal;/* return value for operation */.
        /* initialize variables */
        nRetVal = 0;
        if (_tcscmp (szAppClass, _T ("# 32770"))
            = 0)
65     {/ * attempt to locate dialog box with specified window title */
            if (FindWindow ((TCHAR *) 32770, szProdName)

```

```

        != (HWND) 0)
    {
        /* indicate application found */
        nRetVal = 1;
5    }
    )
    else
    { /* attempt to locate window with specified class */
        if ((hWnd = FindWindow = (szAppClass, (LPCTSTR) 0))
10        != (HWND) 0)
            /* attempt to retrieve title string for window */
            if (GetWindowText (hWnd,
                                szWndText,
                                _MAX_PATH)
15                != 0)
                /* attempt to locate product name within title string */
                if (_tcsstr (szWndText, szProdName)
                    != (TCHAR *) 0)
                {
                    /* indicate application found */
                    nRetVal = 1;
20                }
            }
        }
    }
25    /* return to caller */
    return nRetVal;
}

```

30 Además, se observa que el códec 303 también puede suprimir selectivamente operaciones de entrada/ salida de forma de onda para impedir la grabación de los medios con derechos de autor en un sistema de ordenador del cliente 210. Por ejemplo, el códec 303, posterior a la detección de paquetes de aplicaciones de reproducción de medios operativos en un sistema de ordenador de cliente, por ejemplo, 210, puede detener o interrumpir la reproducción de un archivo de contenido de medios. Esto se puede lograr, en una realización, mediante la reorientación y/o el desvío de las vías de datos determinados que se utilizan comúnmente para la grabación, de tal manera que la vía de datos utilizada se rige por el mecanismo de cumplimiento de los derechos de autor 300. En una realización, esto se puede realizar dentro de una cuña de controlador, por ejemplo, la cuña del controlador de onda 309 de las Figuras 5A y 5B.

40 Una cuña de controlador puede ser utilizada para casi cualquier dispositivo de salida de software, por ejemplo, un dispositivo de salida de forma de onda estándar de Windows™, por ejemplo, Windows™ Media Player, o dispositivo de salida de hardware, por ejemplo, altavoces o auriculares. El sistema de ordenador del cliente 210 está configurado de tal manera que la cuña de controlador (por ejemplo, 309 de las Figuras 5A, 5B, 5C y 5D) aparecerá como el dispositivo de medios de forma de onda predeterminado para programas de aplicación de nivel de cliente.

45 Por lo tanto, las peticiones de procesamiento medios en forma de onda de entrada y/o de salida pasarán a través de la cuña de controlador antes de ser enviadas al controlador de audio de forma de onda real, el controlador de dispositivos de medios 505 de las Figuras 5A y 5B. Dicha supresión de la forma de onda de entrada/salida puede ser provocada por otros componentes del CCM 300, por ejemplo, el agente 304, que se activa cuando una operación de grabado es iniciada por un sistema de ordenador del cliente, por ejemplo, 210, durante la reproducción de los

50 archivos de medios que están sujetos a la DMCA.

Se observa que las cuñas alternativas del controlador pueden ser implementadas para casi cualquier dispositivo de salida de forma de onda incluyendo, pero no limitado a, un Windows™ Media Player. Se observó además que la cuña del controlador puede ser implementada por casi cualquier medio de comunicación en casi cualquier formato, incluyendo, pero no limitado a, los archivos de medios de audio y dispositivos de entrada y de salida de audio, vídeo, gráficos y/o archivos de medios alfanuméricos y dispositivos de entrada y salida de video.

55

El siguiente código fuente C++ es un ejemplo de implementación de una porción de un códec 303 y/o un controlador de dispositivos de medios personalizado 307 para desviar y/o redirigir determinadas vías de datos que se utilizan comúnmente para la grabación de contenido de medios, de acuerdo con una realización de la presente invención.

60

```

    DWORD
    _stdcall
65    widMessage (UINT uDevId,
                UINT uMsg,
                DWORD dwUser,

```

```

        DWORD dwParam1,
        DWORD dwParam2)
{BOOL bSkip; /* flag indicating operation to be skipped */
5   HWND hWndMon; /* handle to main window for monitor */
    DWORD dwRetVal; /* return value for operation */
    /* initialize variables */
    bSkip = FALSE;
    dwRetVal = (DWORD) MMSYSERR_NOTSUPPORTED;
10   if (= uMsg WIDM_START)
    { /* attempt to locate window for monitor application */
        if ((hWndMon = FindMonitorWindowo)
            != (HWND) 0)
            { /* obtain setting for driver */
                bDrvEnabled = (SendMessage(hWndMon,
15                                     uiRegMsg,
                                                0,
                                                0)
                               = 0) ? FALSE: TRUE;
            }
20         if (bDrvEnabled = TRUE)
            {
                /* indicate error in operation */
                dwRetVal = MMSYSERR_NOMEM;
                /* indicate operation to be skipped */
25                 bSkip = TRUE;
            }
        } if (bSkip = FALSE)
        { /* invoke entry point for original driver */
            dwRetVal = CallWidMessage(uDevM, uMsg, dwUser, dwParam1, dwParam2);
30         }
        /* return to caller */
        return dwRetVal;
    }
}

```

35 Se observa que cuando se configura correctamente, el gancho del sistema 305 puede gobernar casi cualquier función o propiedad dentro de casi cualquier aplicación del reproductor de medios que puede ser operativo dentro de un sistema de ordenador del cliente, por ejemplo, 210-230. En una realización, el gancho del sistema 305 es un archivo DLL (Librería de Enlace Dinámico). Se observa además que los ganchos del sistema son bien conocidos en la técnica, y son una instalación estándar en un entorno operativo Microsoft Windows™, y en consecuencia puede ser implementado en una variedad de maneras. Sin embargo, también se observa que el gancho del sistema 305 puede ser fácilmente adaptado para su aplicación en sistemas operativos alternativos, por ejemplo, sistemas operativos Apple™, sistemas operativos Sun Solaris™, sistemas operativos Linux, y casi cualquier otro sistema operativo.

45 En la Figura 3, el mecanismo de cumplimiento de derechos de autor 300 también incluye una o más interfaces 306, que pueden ser diseñadas para ser instaladas en un sistema de ordenador de cliente, por ejemplo, 210-230. En una realización, las interfaces 306 se utilizan para ayudar en el cumplimiento del lado del cliente con la DMCA (Digital Millennium Copyright Act) con respecto a contenidos de medios con derechos de autor. Las interfaces 306 son interfaces personalizables que, en una realización, se muestran en un dispositivo de pantalla (por ejemplo, 105) del sistema de ordenador 210 y proporcionan funcionalidades para la interacción del usuario de contenidos de medios distribuidos. Además, las interfaces 306 también pueden proporcionar una visualización de la información relativa al archivo de contenido de medios, incluyendo, pero no limitado a, título de la canción, nombre del artista, título del álbum, biografía del artista, y otras características tales como solicitudes de compra, publicidad y similares.

55 Además, cuando el gancho del sistema 305 no puede gobernar una función de la aplicación de reproductor de medios operable en un sistema de ordenador de cliente, por ejemplo, 210, de tal manera que sistema de ordenador cliente podría estar en situación de incumplimiento de DMCA y/o restricciones RIAA, se puede implementar una interfaz 306 para proporcionar el cumplimiento.

60 Diferentes interfaces 306 puede ser implementado, dependiendo de la DMCA y/o restricciones RIAA aplicables a cada archivo de contenido de medios. Por ejemplo, en una realización, una interfaz 306a puede estar configurada para su utilización con un archivo de contenido de medios protegido bajo un acuerdo no interactivo (DMCA), de tal manera que la interfaz 306a puede no incluir una función de pausa, una función de parada, un selector de funciones, y/o una función de almacenamiento, etc. Otra interfaz, por ejemplo, la interfaz 306b puede, en una realización, ser configurada para ser utilizada con un archivo de contenido de medios protegidos por un sistema interactivo de acuerdo "sin guardar" (DMCA), de tal manera que la interfaz 306b puede incluir una función de pausa, una función

65

de parada, una función de selector, y para los archivos de medios que tienen un sistema con acuerdo interactivo de "guardar", una función guardar o grabar en un CD.

5 Todavía con referencia a la Figura 3, se observó además que en la presente realización, cada interfaz 306 puede tener un nombre y firma exclusivos. En una realización, la interfaz 306 puede aplicarse, en parte, a través de la utilización de una tabla hash MD (Message Digest) 5 o algoritmo similar. Una tabla hash MD5 puede, en una implementación, ser un algoritmo de verificación de suma. Es bien conocido en la técnica que una interfaz, por ejemplo, la interfaz 306, puede cambiarse el nombre y/o modificarse para incorporar características adicionales y/o funcionalidades de forma no autorizada. Dado que la modificación de la interfaz sería cambiar la suma de comprobación y/o hash MD5, sin el conocimiento de la tabla hash MD5, cambiar el nombre o modificar la interfaz puede servir simplemente para desactivar la interfaz, de acuerdo con una realización de la presente invención. Dado que el mecanismo de cumplimiento de derechos de autor 300 verifica la interfaz 306, las tablas hash MD5 proporcionan ventajosamente un elemento disuasorio contra modificaciones realizadas en la interfaz.

15 En una realización, el mecanismo de cumplimiento de derechos de autor 300 también incluye uno o más controlador(es) de dispositivo de medios personalizado 307 para proporcionar una medida aún mayor de control sobre el flujo de medios mientras que aumenta la fiabilidad de cumplimiento. Un sistema de ordenador de cliente, por ejemplo, 210, puede ser configurado para utilizar una aplicación del dispositivo de medios personalizada, por ejemplo, un dispositivo de medios personalizado 310 (mostrado en la Figura 5B, 5C y 5D), para controlar la grabación no autorizada de los archivos de contenido de medios. Una aplicación personalizada de medios dispositivo puede ser, pero no se limita a, una aplicación de dispositivo personalizado medios de audio para los archivos de medios que tienen un contenido de sonido, aplicación de dispositivo de vídeo personalizado para los archivos multimedia que tienen contenido gráfico y/o alfanumérico, etc. En una realización, el dispositivo de medios personalizada 310 de la figura 5B es una emulación del controlador de dispositivo de medios personalizado 307. Con referencia a los medios de audio, la emulación se realiza en un controlador de audio de forma de onda asociado con el dispositivo de medios personalizado 310. El controlador 307 está configurado para recibir un archivo de medios al que se da salida por el sistema 210 antes de que el archivo de medios se envíe a un dispositivo de salida de medios, por ejemplo, un dispositivo de medios de salida 570, y/o una aplicación de salida de medios, por ejemplo, la aplicación de grabación 502. Ejemplos de un dispositivo de salida de los medios incluye, pero no está limitado a, una tarjeta de vídeo para archivos de vídeo, una tarjeta de sonido para archivos de audio, etc. Ejemplos de una aplicación de grabación pueden incluir, pero no se limita a, las aplicaciones de grabadora de CD para escribir a otros CDs, aplicaciones de ripeado que capturan el archivo de medios y cambian el formato del archivo de medios, por ejemplo, a partir de un archivo de audio de un CD a un archivo de audio de formato mpeg., y/o un archivo. wav, y/o un archivo ogg vorbis, y varios otros formatos de medios. En una realización, el sistema de ordenador de cliente 210 está configurado con un controlador de dispositivo de medios personalizado 307 emulando a un dispositivo de medios personalizado 310, y que es el controlador de dispositivo por defecto 210 del sistema para la salida del archivo de medios. En una realización, una GUI existente (interfaz gráfica de usuario) puede ser utilizada o una interfaz gráfica de usuario se puede proporcionar, por ejemplo, mediante la utilización de la interfaz 306 o una aplicación de jugador basado en la Web personalizada o como parte de un paquete de instalación CCM 300, para forzar a o requerir al sistema 210 tener un controlador 307 como el controlador predeterminado.

Por lo tanto, cuando un archivo de contenido de medios se recibe por el sistema 210 de servidor 251, el archivo de contenido de medios se puede reproducir, siempre que el archivo de contenido de medios pase a través de la aplicación del dispositivo de medios personalizado (por ejemplo, 310 de la Figura 5B), emulado por el controlador de dispositivo de medios personalizado 307, antes de ser emitido. Sin embargo, si se selecciona una aplicación de reproducción de medios alternativos, archivos de medios entregados desde un servidor 251 no se ejecutarán en el sistema 210.

Por lo tanto, aplicaciones de reproducción de medios garantizadas podría emitir una solicitud de medios para el controlador, por ejemplo, 307, para el dispositivo de medios personalizado 310 que realiza entonces la necesaria supresión de entrada de los medios, por ejemplo, la supresión de forma de onda para archivos de audio, antes de transmitir la solicitud al controlador de medios predeterminado de Windows™, por ejemplo, de controlador de audio de forma de onda para archivos de audio.

55 Se observa que las peticiones de archivos de medios no restringidos pueden pasar directamente a través del controlador de dispositivo de medios personalizado 307 a un controlador de audio de forma de onda de Windows™ operable en el sistema 210, lo que reduce los casos de incompatibilidades con las aplicaciones existentes de reproductor de medios que utilizan los medios de forma de onda, por ejemplo, audio, vídeo, etc. Además, las aplicaciones de reproducción de medios que no son compatibles con los medios seguros no se verían afectadas. Se observa además que para cualquiera de los medios garantizados o medios no restringidos, por ejemplo ficheros de medios de audio, la supresión de entrada de la forma de onda puede ser activada por otros componentes del CCM 300, por ejemplo, los agentes 304, gancho del sistemas 305, y interfaces 306, o una combinación de los mismos, para ser activados cuando una operación de grabación se inicia simultáneamente con la reproducción de archivos de medios garantizados, por ejemplo ficheros de audio. Controladores de dispositivos personalizados son bien conocidos y pueden ser codificados e implementados en una variedad de formas incluyendo, pero sin limitarse a, las que se encuentran en los sitios web de los desarrolladores de red, por ejemplo, sitios Web de desarrollo de

Microsoft™ o OS alternativo (sistema operativo).

Ventajosamente, en virtud de que el sistema 210 está configurado con un dispositivo de medios personalizable como por ejemplo el controlador de dispositivo por defecto, el dispositivo 310 de las figuras 5B, 5C y 5D, emulado por un controlador de dispositivo de medios personalizado 307, las aplicaciones de reproducción de medios que requieren que su controlador de dispositivo en particular sea el controlador predeterminado, por ejemplo, Total Recorder, etc., se convierten en no-funcionales para la música protegida. Es adicionalmente ventajoso que un dispositivo emulado multimedia personalizado no proporcione soporte nativo para aquellas aplicaciones de reproducción de los medios utilizados como un mecanismo de registro, por ejemplo, la captura de DirectSound, (sonido directo 504 de las Figuras 5A, 5B, 5C y 5D), etc., que son capaces de eludir controladores en modo de usuario para la mayoría de dispositivos de medios. Además, en virtud del contenido de medios que se envían a través del controlador de dispositivo 307, por lo tanto, desactiva la grabación no autorizada/registro de archivos de medios, en una realización, los archivos de medios que se entregan en un sistema de entrega asegurada no tienen que ser cifrados, aunque, en otra realización, todavía pueden estar encriptados. En virtud de la los archivos de medios no cifrados que utilizan menos espacio de almacenamiento y recursos de red que los archivos de medios cifrados, las redes que tienen recursos limitados pueden utilizar las funcionalidades del controlador 307 de CCM 300 para proveer el cumplimiento de las restricciones de derechos de autor y/o acuerdos de licencia aplicables con un archivo de contenido de medios sin tener la sobrecarga de procesamiento de archivos de medios cifrados.

La Figura 4 es una ilustración de un sistema ejemplar 400 para la aplicación de un mecanismo de cumplimiento de derechos de autor de acuerdo con una realización de la presente invención. Específicamente, el sistema 400 ilustra los servidores Web 250, servidor de contenido 251, o una combinación de servidor de web 250 y el servidor de contenido 251 instalando un mecanismo de cumplimiento de los derechos de autor (por ejemplo, 300) en el sistema de ordenador de un cliente (por ejemplo, 210) para controlar la distribución de archivos de medios y controlar el acceso de usuario y la interacción con derechos de autor de los archivos de medios, en una realización de la presente invención.

El sistema de ordenador del cliente 210 puede comunicativamente acoplarse con una red (por ejemplo, 200) para solicitar un archivo de medios, una lista de los archivos de medios disponibles, o una lista de reproducción de archivos de audio, por ejemplo, MP3, etc. En respuesta, el servidor web 250 determina si la solicitud se origina en un usuario registrado autorizado para recibir archivos de medios asociados a la solicitud. Si el usuario no está registrado en la red, el servidor web 250 puede iniciar un proceso de registro con el cliente solicitante 210. El registro del cliente se puede lograr en una variedad de maneras. Por ejemplo, el servidor web 250 puede entregar a un cliente 210 un formulario de registro que tiene varios campos de entrada de texto en los que el usuario puede introducir información que necesita. Una variedad de información puede ser necesaria desde el usuario por el servidor web 250 incluyendo, pero no limitado a, nombre de usuario, dirección, número de teléfono, número de tarjeta de crédito, número de cuenta de pago en línea, identificación biométrica (por ejemplo, huella digital, escáner de retina, etc.), dirección de correo electrónico verificable, y similares. Además, el registro puede, en una realización, incluir un requisito para que el usuario seleccione un nombre de usuario y contraseña.

Todavía con referencia a la Figura 4, el servidor web 250 puede, en una realización, detectar la información relacionada con el sistema de ordenador del cliente, por ejemplo, 210, y almacenar dicha información en una base de datos de usuario/medios 450. Por ejemplo, el servidor web 250 puede detectar un identificador único del sistema de ordenador del cliente 210. En una realización, el identificador único puede ser la dirección MAC (código de dirección de máquina), dirección de una NIC (tarjeta de interfaz de red) de sistema de ordenador del cliente 210 o la dirección MAC del adaptador de interfaz de red integrada en la placa base de sistema 210. Se entiende que una NIC permite a un sistema de ordenador del cliente 210 acceder al servidor web 250 a través de Internet 201. Es bien conocido que cada NIC tiene típicamente un número único de identificación de dirección MAC. Además, el servidor web 250 puede, en una realización, detectar y almacenar (también en la base de datos 450) información sobre los tipos(s) de las aplicación(es) de reproducción de medios, por ejemplo, Windows Media Player™, Real Player™, iTunes Player™ (Apple), reproductor Live 365™, y las aplicaciones de reproducción de medios que tienen una funcionalidad de grabación, por ejemplo, Total Recorder, Cool Edit 2000, Sound Forge, Sound Recorder, Super MP3 Recorder, y similares, que están presentes y operativas en el sistema del equipo del cliente 210. En una realización, la información del cliente se verifica por la precisión, y se almacena en una base de datos de usuario (por ejemplo, 450) dentro del servidor web 250.

Posteriormente a la finalización de registro, la creación de la ID de usuario y contraseña, y obtener información relativa sistema de ordenador del cliente 210, la totalidad o parte de esta información se puede instalar en sistema de ordenador del cliente 210. En una realización, la información del sistema del equipo del cliente 210 puede estar en la forma de una cookie. El servidor web 250 entonces verifica que el usuario y los datos del sistema de ordenador de cliente 210 están correctamente instalados en el mismo y que su integridad no ha sido comprometida. Posteriormente, el servidor web 250 instala un mecanismo de cumplimiento de los derechos de autor (por ejemplo, 300) en el sistema de ordenador del cliente, por ejemplo, 210, en una realización de la presente invención. Se hace notar que el servidor web 250 no puede iniciar la instalación de CCM 300 hasta que la información del ID de usuario, la contraseña y sistema de ordenador de cliente 210 se verifican. Una variedad de técnicas comunes pueden ser empleadas para instalar un CCM 300 entero, porciones de componentes, componentes enteros, y/o combinaciones

o una función de componentes. Por ejemplo, el mecanismo de cumplimiento de derechos de autor 300 se puede instalar en un directorio oculto dentro de sistema de ordenador del cliente 210, lo que impide el acceso no autorizado al mismo. En una realización de la presente invención, se hace notar que, a menos CCM 300 está instalado en el sistema de ordenador del cliente 210, su usuario no será capaz de solicitar, acceder, o se que se entreguen al mismo, archivos multimedia almacenados por el servidor web 250 y/o contenido de servidor 251.

Haciendo referencia todavía a la Figura 4, al completarse el registro de cliente y la instalación de CCM 300, el sistema de ordenador del cliente 210 puede entonces solicitar una lista de reproducción de medios o una pluralidad de listas de reproducción, etc. En respuesta, el servidor web 250 determina si el usuario del sistema de ordenador del cliente 210 está autorizado para recibir la lista de reproducción de medios asociada con la solicitud. En una realización, el servidor web 250 puede solicitar el nombre de usuario y contraseña. Alternativamente, el servidor web 250 puede utilizar la base de datos de usuario 450 para verificar que el ordenador 210 está autorizado para recibir una lista de reproducción de medios. Si el ordenador del cliente 210 no está autorizado, el servidor web 250 puede iniciar el registro del cliente, como se describe en la presente memoria. Además, el servidor web 250 puede desconectar ordenador 210 o redirigir a un sitio web alternativo. En cualquier caso, si el usuario y el sistema del equipo del cliente 210 no están autorizados, el servidor web 250 no proporcionará la lista de reproducción solicitada al sistema del equipo del cliente 210.

Sin embargo, si el sistema del equipo del cliente 210 está autorizado, el servidor web 210 puede comprobar el cumplimiento del mecanismo de derechos de autor 300 dentro de la base de datos 450 para determinar si él o alguno de los componentes del mismo, se han actualizado desde la última vez que el sistema de ordenador del cliente 210 se conectó a la web servidor 250. Si un componente de CCM 300 ha sido actualizado, el servidor web 250 puede instalar el componente de actualización y/o una versión más actual del CCM 300 en el sistema de ordenador del cliente 210, por ejemplo, a través de Internet 201. Si el CCM 300 no ha sido actualizado, el servidor web 250 puede entregar la lista de reproducción de medios solicitada en el sistema 210 a través de Internet 201 junto con una clave de usuario o identificación de usuario (ID) añadida. Se observa que la base de datos de usuario 450 puede también incluir datos correspondientes a uno o más medios de listas de reproducción que se pueden utilizar para proporcionar una lista de reproducción de medios al sistema de ordenador del cliente 210. Posteriormente, el usuario del sistema de ordenador del cliente 210 puede utilizar la lista de reproducción de medios recibida en combinación con la aplicación de reproductor multimedia de funcionamiento en el sistema 210 para transmitir una solicitud de entrega de unas o más piezas deseadas de contenido de medios desde el servidor web 250. Se observa que la solicitud de suministro contiene la clave de usuario con fines de validación.

Todavía con referencia a la Figura 4, al recibir la solicitud de entrega de contenido de medios, el servidor web 250 puede entonces comprobar la validez de la aplicación que solicita los medios y la clave de usuario adjunta. En una realización, el servidor web 250 puede utilizar la base de datos de usuario 450 para comprobar su validez. Si uno o ambos no son válidos, el servidor web 250, en una realización, puede redirigir al sistema del ordenador del cliente no autorizado 210 a un destino alternativo para evitar el abuso del sistema. Sin embargo, si tanto la aplicación que solicita los medios y la clave de usuario son válidas, MCP 300 verifica que las interfaces 306 se instalan en el sistema de ordenador del cliente 210. Además, CCM 300 comprueba además que el gancho(s) del sistema 305 se ha ejecutado o se está ejecutando para gobernar ciertas funciones de las aplicaciones de reproducción de medios operables dentro del sistema del equipo del cliente 210 que son conocidos por proporcionar el incumplimiento de la DMCA y/o la RIAA. Además, el CCM 300 adicionalmente desvía y/o redirige ciertas vías que se utilizan comúnmente para la grabación, por ejemplo, controlador 307 de la Figura 5A, el dispositivo 310 de la Figura 5B, el dispositivo 570 de la Figura 5C, y el controlador 505 de la Figura 5D. Una vez que el CCM 300 ha realizado las funciones descritas anteriormente, el servidor web 250 entonces, en una realización, entrega al equipo del cliente 210 un comando de redirección para la ubicación de dirección actual del contenido del archivo de medios que desee, junto con una tecla de acceso sensible al tiempo opcional, por ejemplo, para esa hora, día u otro plazo definido.

En respuesta al sistema de ordenador del cliente 210 que recibe el comando de redirección desde los servidores Web 250, la aplicación del reproductor de medios que funciona en el sistema del ordenador del cliente 210 transmite automáticamente una nueva petición y la clave de acceso en tiempo sensible al servidor de contenidos 251 para la entrega de una o más piezas deseadas de contenido de medios. La validez de la clave de acceso en tiempo sensible está marcada por el servidor de contenido 251. Si no es válido, el equipo del cliente no autorizado 210 es redirigido por el servidor de contenidos 250 para proteger contra el abuso del sistema y el acceso no autorizado al servidor de contenidos 251. Si la clave de acceso en tiempo sensible es válida, el servidor de contenido 251 recupera el contenido de medios deseado desde la base de datos de contenido 451 y lo entrega al sistema de ordenador del cliente 210. Se observa que, en una realización, el contenido de medios entregado puede ser almacenado en directorios ocultos y/o sistemas de archivos personalizados que pueden estar ocultos dentro de sistema de ordenador del cliente 210 previniendo la distribución no autorizada en el futuro. En una realización, un sistema de entrega de archivos HTTP (protocolo de transferencia de hipertexto) se utiliza para entregar los archivos de medios solicitados, lo que significa que los archivos multimedia son entregados en su totalidad al sistema de ordenador del cliente 210, en comparación con los medios de transmisión que ofrecen pequeñas porciones del archivo de medios.

Todavía con referencia a la figura 4, se observa que cada archivo de medios, en una realización, tenía un encabezado unido con el mismo antes de la entrega del archivo de medios. En una realización, el encabezado puede contener información relacionada con el archivo multimedia, por ejemplo, título o ID de medios, datos de medios tales como el tamaño, el tipo de datos, y similares. El encabezado también puede contener una secuencia o una clave que es reconocible para el mecanismo de cumplimiento de derechos de autor 300 que identifica el archivo de medios como procedentes de un servidor de contenido 251. En una realización, la secuencia de encabezado/clave también puede contener instrucciones para invocar a los acuerdos de licencia y/o restricciones de derechos de autor que son aplicables a ese archivo de medios en particular.

Además, si los acuerdos de licencia o restricciones de derechos de autor se cambian, desarrollan o crean, o si las nuevas aplicaciones de reproducción de medios, con o sin función de grabación, se desarrollan, CCM 300 tendría las modificaciones pertinentes hechas a partes de componentes, componentes enteros, combinaciones de componentes, y/o todo el CCM 300 para permitir el cumplimiento continuo con los acuerdos de licencia y restricciones de derechos de autor. Además, después de la modificación del mecanismo de cumplimiento de derechos de autor 300, las porciones modificadas de, o el CCM de actualización completo 300 puede ser fácilmente instalado en sistema de ordenador del cliente 210 en una variedad de maneras. Por ejemplo, la versión actualizada del CCM 300 puede ser instalada durante la interacción del cliente con el servidor web 250, durante el inicio de sesión de usuario y/o mientras el sistema de ordenador del cliente 210 está recibiendo la lista de reproducción con la clave.

Haciendo referencia todavía a la Figura 4, se observó además que, en una realización, los archivos de medios y encabezados adjuntos pueden ser encriptados antes de ser almacenados dentro del servidor de contenido 251. En una realización, los archivos de medios pueden ser encriptados utilizando las claves generadas aleatoriamente. Alternativamente, las claves de longitud variable pueden ser utilizadas para el cifrado. Se observa que la clave para descifrar los archivos cifrados de medios puede ser almacenada en una base de datos 450, base de datos de contenido 451 o en alguna combinación de bases de datos 450 y 451. Se observa además que los mensajes que se pasan de ida y vuelta entre el sistema del ordenador del cliente 210 y el servidor web 250 también pueden ser encriptados, protegiendo así a los archivos multimedia y los datos que se intercambian del uso o acceso no autorizado. Hay una variedad de mecanismos y programas de encriptación que se pueden implementar para cifrar estos datos incluyendo, pero no limitado a, OR exclusivo, cambiando con anuncios, programas de cifrado de dominio público tales como Blowfish, y mecanismos de cifrado de dominio no públicos. También se observa que cada archivo de medios puede ser especialmente encriptado, de tal manera que si el código de cifrado es pirateado por un archivo de medios, no es aplicable a otros archivos de medios. Alternativamente, los grupos de archivos de medios pueden ser igualmente encriptados. Además, en otra realización, los archivos de medios pueden no estar cifrados cuando se entregan a una difusión por Internet conocida por la utilización de una aplicación reproductora de medios propietaria, por ejemplo, un controlador de dispositivo de medios personalizado 307.

Con posterioridad al descifrado del archivo de medios, el archivo de medios se puede hacer pasar a través de CCM 300, por ejemplo, un codificador/decodificador 303, a una aplicación de reproductor multimedia de funcionamiento en el sistema de ordenador del cliente 210, por ejemplo, la aplicación de reproducción 501 de las Figuras 5A, 5B, 5C, 5D, y 6A, que puede acceder y utilizar la entrega de contenido de medios de alta fidelidad, lo que permite a su usuario(s) experimentar el contenido de medios, por ejemplo, escucharlo, mirarlo, verlo, o similares. En una realización de la presente invención, un reproductor de medios especializado o personalizado puede o no puede ser obligado a experimentar el contenido de los medios, por ejemplo, la interfaz 306 de la Figura 3. Una interfaz 306 puede ser necesaria cuando CCM 300 no puede modificar una aplicación de reproductor de medios estándar de la industria para cumplir con las restricciones de derechos de autor y/o acuerdos de concesión de licencias de conformidad con la DMCA. Alternativamente, un reproductor de medios estándar de la industria puede ser utilizado por sistema de ordenador del cliente 210 para experimentar el contenido de los medios. Por lo general, muchas aplicaciones de reproducción de medios están disponibles y pueden incluir, pero no están limitados a, Windows™ Media Player™ para PCs (ordenadores personales), iTunes™ Player o QuickTime™ para ordenadores de Apple, y el reproductor XMMS para los ordenadores que utilizan el sistema operativo Linux. Independientemente de la aplicación de reproductor de medios utilizada, mientras que el archivo de medios se pasa a la aplicación de reproductor de medios, por ejemplo, en una base de marco a marco o en una memoria intermedia, codificador/decodificador 303 repetidamente se asegurará de que las reglas CCM 300 están siendo aplicadas en cualquier momento particular durante la reproducción de medios, que se muestra como la etapa 650 de la Figura 6C.

Cuando el contenido del archivo de medios se entrega a la aplicación de reproductor de medios, de forma periódica, por ejemplo, después de un número determinado de marcos, después de un período de tiempo definido, o cualquier periodo de tiempo o datos deseado, el codificador/decodificador 303 repetidamente determina si todas las reglas se hacen cumplir o no, de acuerdo con las reglas definidas por CCM 300. Si las reglas no se aplican, por ejemplo, cambio debido a que un usuario abre una aplicación de grabación, por ejemplo, Total Recorder o aplicación alternativa, la presentación del contenido de medios es, en una realización, suspendida o interrumpida. En otra realización, la presentación del contenido de medios puede ser modificada para dar salida al contenido de los medios no audible, por ejemplo, el silencio. En aún otra realización, el contenido de medios puede ser audible, pero la funcionalidad de grabación se puede desactivar, de forma que el contenido de medios no se pueden grabar. Estas interrupciones de presentación se muestran colectivamente como la etapa 651 de la Figura 6C.

Si las reglas, de acuerdo con el CCM 300, se aplican, el codificador/decodificador 303 recibe una porción subsiguiente del contenido de medios que se almacena localmente en el sistema de ordenador del cliente 210. La porción recién recuperada de los archivos multimedia se presenta entonces por la aplicación de reproducción de medios del cliente. Si bien la parte recién recuperada se presenta, el CCM 300 luego vuelve a comprobar que se cumplen las normas, y recupera una porción adicional del archivo de medios o suspende la presentación del archivo de medios si las reglas no se están aplicando, y estos pasos se realizan repetidamente a lo largo la reproducción del archivo de medios, en un entorno de bucle, hasta que el contenido del archivo de medios ha sido presentado en su totalidad. Ventajosamente, mediante el monitorización constante durante la reproducción de archivos de medios, el CCM 300 puede detectar actividades no deseadas y hace cumplir las reglas definidas por el CCM 300.

La Figura 5A es un diagrama de bloques de pasaje lógico/bit ejemplar 500A mostrando la utilización de un controlador de cuña de onda, por ejemplo, la onda 309 del controlador de la cuña de la Figura 3, en relación con el mecanismo de cumplimiento de derechos de autor 300, para controlar selectivamente la grabación de medios con derechos de autor recibidos por un sistema del equipo del cliente, por ejemplo, el sistema 210, en una realización de la presente invención. El mecanismo de cumplimiento de derechos de autor 300 es, en una realización, instalado y operativo en el sistema de cliente 210 de la manera descrita en la presente memoria.

En una realización, un mecanismo de cumplimiento de los derechos de autor 300 se muestra como estando acoplado en comunicación con una aplicación de reproducción de medios 501 a través de la conexión 520. Por lo tanto, el CCM 300 está habilitado para comunicarse con aplicación de reproducción 501. En una realización, el CCM 300 se puede integrar en una aplicación de reproducción de medios. El CCM 300 está también acoplado a, y controla un conmutador seleccionable 311 en un controlador de cuña de onda 309 (como se describe en la Figura 3) a través de la conexión 522. El CCM 300 está acoplado además a y controla un conmutador seleccionable 511 en sonido directo 504 a través de la conexión 521. Dependiendo de las restricciones de derechos de autor y acuerdos de licencia aplicables a un archivo de medios entrante, por ejemplo, 499, el CCM 300 controla si los conmutadores 311 y 511 están abiertos (como se muestra), evitando así que los medios de comunicación entrantes 499 alcancen una aplicación de grabación de medios, o cerrados (no mostrado) para permitir la grabación de los medios de comunicación entrantes 499.

Por ejemplo, los medios entrantes 499 pueden originarse a partir de un servidor de contenido, por ejemplo, 251, acoplado al sistema 210. En otro ejemplo, los medios de comunicación entrantes 499 puede originarse a partir de un dispositivo de grabación personal/electrónico, por ejemplo, un reproductor/grabador de MP3 o dispositivo similar, acoplado al sistema 210. Alternativamente, los medios de comunicación entrante 499 pueden originarse a partir de un dispositivo de almacenamiento magnético, óptico o de medios alternativos insertados en un dispositivo reproductor de medios acoplado al sistema 210, por ejemplo, un CD o DVD insertado en un reproductor de CD o DVD, un disco duro en un disco duro intercambiable en caliente, una tarjeta SD (tarjeta digital segura) que se inserta en un lector de SD, y similares. En otro ejemplo, los medios entrante 499 pueden originarse desde otra aplicación de reproductor multimedia o aplicación de medios de grabación. Los medios entrantes 499 también pueden provenir de una fuente de radio por satélite (por ejemplo, radio XM), un dispositivo de comunicación personal (por ejemplo, un teléfono móvil), la entrada de radio de la televisión por cable (por ejemplo, DMX (digital music express)), una distribución digital y/o una fuente de exposición pública a través de una red, Internet u otra conexión de comunicación, pago por visión y/o el sistema pago por reproducción, o una caja de ajuste superior. Se observa que los medios entrantes 499 pueden originarse a partir de casi cualquier fuente, que puede ser acoplada al sistema 210. Sin embargo, independientemente de la fuente de entrada de medios 499, las realizaciones de la presente invención, que se describen en la presente memoria, pueden impedir la grabación no autorizada de los medios.

La Figura 5A muestra una aplicación de reproducción de medios 501, por ejemplo, un reproductor de audio, vídeo u otra aplicación reproductor de medios, operable dentro del sistema 210 y configurado para recibir los medios de comunicación entrantes 499. La aplicación de reproducción 541 puede ser una aplicación de reproducción proporcionada por un sistema operativo, por ejemplo, Media Player para Windows™ de Microsoft, una aplicación de reproducción de distribución gratuita descargable desde Internet, por ejemplo, RealPlayer o LiquidAudio, una aplicación de reproducción proporcionada por una difusión por Internet, por ejemplo, PressPlay, o una aplicación de reproducción disponible comercialmente.

La Figura 5A muestra controlador de dispositivo de medios 505 que, en una implementación, puede ser un controlador de software para una tarjeta de sonido junto con el sistema 210 que tiene un dispositivo de salida de los medios 570, por ejemplo, altavoces o auriculares, acoplado con el mismo para los archivos de medios con contenido de audio. En otra aplicación, el controlador de dispositivo de los medios 505 puede ser un controlador de software para una tarjeta de vídeo junto con un dispositivo de visualización, por ejemplo, 105, para la visualización de los archivos de medios que tienen un contenido alfanumérico y/o gráfica, y así sucesivamente. Con referencia a archivos de audio, es bien sabido que la mayoría de las aplicaciones de grabación asumen que un sistema de ordenador, por ejemplo, 210, tiene una tarjeta de sonido dispuesta en el mismo, proporcionando la funcionalidad de sonido de dúplex completo al sistema 210. Este significa que el controlador de medios de salida 505 al mismo tiempo puede causar la reproducción y grabación de archivos de medios entrantes 499. Por ejemplo, el controlador de dispositivo de medios 505 puede reproducir los medios 499 junto con la línea de onda de salida 539 a un

dispositivo de salida de medios 570 (por ejemplo, los altavoces para la reproducción sonora) a través de la onda de salida de línea 580 mientras se emite los medios 499 en línea de salida de onda 540 para llegar eventualmente a la aplicación de grabación 502.

5 Para los propósitos de las figuras 5A, 5B, 5C y 5D, los términos línea de onda de entrada y de onda de línea de salida hacen referencia desde la perspectiva del controlador de dispositivo de los medios 505. Adicionalmente, para la mayor parte, las líneas de onda de entrada están representadas hacia abajo y las líneas de onda hacia afuera fuera están representadas hacia arriba en las figuras 5A, 5B, 5C y 5D.

10 Continuando con la Figura 5A, la reproducción de aplicación 501 está acoplada con un subsistema multimedia del sistema operativo (O/S) 503 y de sonido directo 504 a través de líneas de onda entrantes 531 y 551 respectivamente. El subsistema multimedia O/S 503 está acoplado a un controlador de cuña de onda 309 a través de línea de onda entrante 533 y la línea de onda de salida 546. El subsistema multimedia de O/S 503 se acopla también a una aplicación de grabación 502 a través de la línea de onda de salida 548. El subsistema multimedia del sistema operativo (O/S) 503 puede ser cualquier subsistema de O/S multimedia, por ejemplo, un subsistema multimedia de Windows™ para el sistema operativo 210 que opera bajo un Microsoft O/S, un subsistema multimedia QuickTime™ para el sistema operativo 210 que opera bajo Apple/OS, y así sucesivamente. La aplicación de reproducción 501 se acopla también con sonido directo 504 a través de la línea de onda de entrada 551.

20 El sonido directo 504, en un caso, puede representar el acceso a una función de aceleración de hardware en un dispositivo de audio estándar, permitiendo menor nivel de acceso a los componentes dentro del controlador de dispositivo de medios 505. En otro ejemplo, el sonido directo 504 puede representar una ruta de acceso que puede ser utilizada por una aplicación de grabación, por ejemplo, Total Recorder, que puede estar configurada además para evitar el controlador de dispositivo por defecto, por ejemplo, el controlador de dispositivos de medios 505 para capturar los medios de comunicación entrantes 499 para la grabación. Por ejemplo, el sonido directo 504 puede estar en condiciones de capturar medios de entrada 499 a través de la línea de onda entrante 551 y medios de salida ilícitos 499 a una aplicación de grabación 502 a través de la línea de onda de salida 568, así como los medios 499 que eventualmente van al controlador de dispositivo de medios 505, el controlador predeterminado estándar.

30 Haciendo referencia a la Figura 5A, el controlador de cuña de onda 309 está acoplado con controlador del dispositivo de medios 505 a través de la línea de onda de entrada 537 y la línea de onda de salida 542. El controlador del dispositivo de medios 505 se acopla con el sonido directo 504 a través la línea de onda de entrada 553 que se muestra que converge con la línea de onda de entrada 537 en el controlador de dispositivo de medios 505. El controlador de dispositivo de medios 505 se acopla también con sonido directo 504 a través de la línea de onda de salida 566.

Las líneas de onda de salida 542 y 566 se muestran que divergen de la línea de onda de salida 540 en el controlador de dispositivo de medios 505 en rutas separadas. La línea de onda de salida 542 se alimenta del controlador de cuña de onda 309 y la línea de onda de salida 566 se alimenta en sonido directo 504. Cuando el conmutador seleccionable 311 y 511 están abiertos (mostrado), los medios entrantes 499 no pueden fluir a la aplicación de grabación 502, lo que impide la grabación no autorizada de los mismos.

45 Por ejemplo, los medios entrantes 499 son recibidos en la aplicación de reproducción 501. La aplicación de reproducción 501 se activa y comunica a CCM 300 en relación a las restricciones de derechos de autor y/o acuerdos de licencia aplicables a los medios entrantes 499. Si las restricciones de grabación se aplican a los medios 499, el CCM 300 puede, en una realización, abrir los conmutadores 311 y 511, bloqueando de esta manera el acceso a la aplicación de grabación 502, lo que impide la grabación no autorizada de los medios 499. En una realización, el CCM 300 puede detectar si el sistema 210 está configurado con sonido directo 504 seleccionado como el controlador predeterminado para capturar los medios entrantes 499, a través de la línea de onda de entrada 551, o una aplicación de grabación se detecta y/o un acelerador de hardware está activo, de tal manera que el controlador de cuña de onda 309 puede ser anulado por el sonido directo 504. Tras la detección, el CCM 300 puede controlar el conmutador 511 de tal manera que la ruta de salida, la línea de onda de salida 568, a la aplicación de grabación 502 está bloqueada. Se observa además que el CCM 300 puede detectar aplicaciones de medios de grabación y los dispositivos como se describe en la presente memoria, con referencia a la Figura 3.

55 Alternativamente, si se seleccionó un controlador de dispositivos de medios 505 como el controlador predeterminado, los medios entrantes 499 son la salida de aplicación de reproducción 501 al subsistema multimedia O/S 503 en la línea de onda de entrada 531. Desde el subsistema 503, los medios 499 se emiten al controlador de cuña de ondas 309 a través de la línea de onda de entrada 533. El controlador de cuña de onda 309 se describe aquí con referencia a la Figura 3. Los medios 499 se emiten desde el controlador de cuña de onda 309 al controlador del dispositivo de medios 505 a través de línea de onda de entrada 537. Una vez recibidos por controlador de dispositivo de medios 505, los medios 499 se pueden emitir a través de línea de onda de salida 539 a un dispositivo de salida de medios 570 acoplado con los mismos mediante la línea de onda de salida 580. Además, el controlador de dispositivos de medios 505 simultáneamente puede dar salida a medios 499 en la línea de onda de salida 540 de nuevo al controlador de cuña de onda 309. Dependiendo de las restricciones de grabación aplicables a los medios 499, el CCM 300 puede, en una realización, cerrar el conmutador 311 (no se muestra como cerrado),

5 permitiendo así que los medios 499 se emitan desde el controlador de cuña de ondas 309 al subsistema 503 (a través de la línea de onda de salida 546) y luego a la aplicación de grabación 502 a través de la línea de onda de salida 548. Alternativamente, el CCM 300 también puede abrir el conmutador 311, evitando de este modo a los medios 499 llegar a la aplicación de grabación 502.

10 Se destaca especialmente que, en virtud de CCM 300 el control de ambos conmutadores 311 y 511, y por lo tanto el control de la línea de onda de salida 548 y la onda de línea de salida 568 que conduce a la aplicación de grabación 502, los archivos multimedia entrantes, por ejemplo, los medios 499, se puede impedir que se estén grabando de forma no autorizada, de acuerdo con las restricciones de derechos de autor aplicables y/o acuerdos de concesión de licencias relacionadas con los medios entrantes. También se observa que las realizaciones de la presente invención de ninguna manera interfieren con o inhiben la reproducción de los medios entrantes 499.

15 La Figura 5B es un diagrama de bloques de ruta lógica/bit ejemplar 500B de un sistema de ordenador del cliente, por ejemplo, 210, configurado con un mecanismo de cumplimiento de los derechos de autor 300 para que impida la grabación no autorizada de los medios con derechos de autor de acuerdo con una realización de la presente invención. El mecanismo de cumplimiento de derechos de autor 300 está, en una realización, acoplado a y operativo en el sistema de cliente 210 de la manera con referencia a las Figuras 4, 5A, 5C, 5D, 6, y 7.

20 El diagrama 500B de la Figura 5B es similar al diagrama 500A de la figura 5A, con algunos cambios. En particular, el diagrama 500B incluye un dispositivo de soportes personalizados 310 comunicativamente interpuesto entre y junto al subsistema multimedia O/S 503 y el controlador de cuña de onda 309. El dispositivo multimedia personalizado 310 está acoplado al subsistema multimedia O/S a través de la línea de onda de entrada 533 y la línea de onda de salida 546. El dispositivo de medios personalizado 310 se acopla con los controladores de cuñas de onda 309 a través de la línea de onda de entrada 535 y la línea de onda de salida 544. Además, el dispositivo multimedia personalizado 310 está acoplado con sonido directo 504 a través de la línea de onda de entrada 553 que converge con la línea de onda de entrada 533 y la línea de onda de salida 566 que diverge de la línea de onda de salida 546, en una realización.

30 También se ha añadido a la Figura 5B un dispositivo de salida de hardware de medios 570 que está acoplado al controlador de hardware del dispositivo de medios 505 a través de la línea 580. El dispositivo de salida de hardware de medios 570 puede ser, pero no se limita a, una tarjeta de sonido para la reproducción de audio, una tarjeta de vídeo para vídeo, gráfico alfanumérico, etc., de salida, y similares.

35 En una realización, el CCM 300 está acoplado en comunicación con la aplicación de reproducción 501 a través de la conexión 520, la cuña de controlador de forma de onda 309 a través de la conexión 522, y el dispositivo de medios personalizado 310, a través de la conexión 521. El CCM 300 está acoplado a, y controla un conmutador seleccionable 311 en la cuña del controlador de forma de onda 309 a través de la conexión 522. El CCM 300 está también acoplado a, y controla un conmutador seleccionable 312 en el dispositivo de audio personalizado 310 a través de la conexión 521. Dependiendo de las restricciones de derechos de autor y acuerdos de licencia aplicables a un archivo de medios entrante, por ejemplo, los medios 499, el CCM 300 controla si los conmutadores 311 y 312 están abiertos (como se muestra), lo que impide a los medios entrantes 499 llegar a una aplicación de grabación, o cerrado (no se muestra) a fin de permitir la grabación de medios entrantes 499.

45 Continuando con la Figura 5B, el sonido directo 504 se muestra acoplado con el dispositivo de medios personalizable 310 a través de la línea de onda de entrada 553, en lugar de estar acoplado con el controlador de dispositivo de los medios 505 (Figura 5A). En una realización, el dispositivo de audio personalizable 310 ordena una selección explícita a través del sistema 210, lo que significa que el dispositivo de audio personalizado 310 tiene que ser seleccionado como controlador predeterminado del sistema 210. En virtud de que la selección de un dispositivo de medios personalizable 310 como el controlador por defecto del sistema 210, la ruta de datos necesaria para que el sonido directo 504 para capturar el contenido de medios es selectivamente cerrada.

50 Por ejemplo, los medios entrantes 499 procedentes de casi cualquier fuente, con referencia a la Figura 5A son recibidos por la aplicación de reproducción de medios 501 del sistema 210. La aplicación de reproducción 501 se comunica con el CCM 300, a través de la conexión 520, para determinar si los medios entrantes 499 está protegidos por las restricciones de derechos de autor y/o acuerdos de licencia. La aplicación de reproducción 501 se comunica con el CCM 300 para controlar el conmutador 311 y 312 en consecuencia. En el presente ejemplo, la grabación de los medios de comunicación entrantes 499 viola las restricciones aplicables y/o acuerdos y por lo tanto el conmutador 312 está en una posición abierta, de tal manera que la ruta de salida a la aplicación de grabación 502, por ejemplo, la onda de salida de línea 548 y/o de onda salida de línea 568, está bloqueada, lo que impide la grabación no autorizada de los medios 499.

65 Alternativamente, si el controlador de dispositivos de medios 505 se selecciona como el controlador predeterminado; los medios entrantes 499 continúan a partir del subsistema multimedia del O/S 503, a través del dispositivo de audio personalizado 310, la cuña del controlador de onda 309, y el controlador del dispositivo de medios 505, donde los medios 499 pueden ser simultáneamente emitidos al dispositivo de salida de los medios 570 a través de la línea 580, y emitidos en la línea de onda de salida 540 a la onda y reproducidas por el controlador de dispositivo de

medios 505 al controlador de cuña de onda 309 en la línea de onda de salida 542. Sin embargo, en virtud del CCM 300 el conmutador de control 311, la línea de onda de salida 544, que eventualmente conduce a la aplicación de grabación 502 está bloqueada, lo que efectivamente impide la grabación no autorizada de los medios 499.

5 Se destaca especialmente que, en virtud de que el CCM 300 controla ambos conmutadores 311 y 312 y por lo tanto controla la línea de onda de salida 548 y la línea de onda de salida 568, cualquier archivo de medios entrante, por ejemplo, los medios entrantes 499, se puede evitar que sean grabados en una manera no autorizada, de acuerdo con las restricciones de derechos de autor y/o acuerdos de concesión de licencias relacionadas con los medios entrantes.

10 Haciendo referencia todavía a la Figura 5B, se señala además que el dispositivo multimedia personalizado 310 permite la reproducción sin restricciones de los medios entrantes 499. Además, en cualquier momento durante la reproducción de los medios 499, el dispositivo de medios personalizado 310 puede ser dinámicamente activado por CCM 300.

15 La Figura 5C es un diagrama de bloques de ejemplo de ruta lógica/bit 500C de un sistema de ordenador del cliente, por ejemplo, 210, configurado con un mecanismo de cumplimiento de los derechos de autor 300 para impedir la salida no autorizada y la grabación no autorizada de los medios con derechos de autor de acuerdo con una realización de la presente invención. El mecanismo de cumplimiento de derechos de autor 300 es, en una
20 realización, junto con y operativo en el sistema del cliente 210 de la manera con referencia a las Figuras 4, 5A, 5B, 5D, 6, y 7.

El diagrama 500C de la Figura 5C es similar al diagrama 500B de la Figura 5B, con algunos cambios. Particularmente, el diagrama 500C incluye un dispositivo de salida de hardware de medios 570 que está acoplado
25 con un controlador de dispositivo de los medios 505. En una realización, el dispositivo de salida de hardware de medios 570 puede ser una tarjeta S/PDIF (Sony/Philips Digital Interface) para proporcionar múltiples salidas, por ejemplo, una salida analógica 573 y una salida digital 575. Un dispositivo de salida de hardware de medios alternativo que proporciona una salida digital similar también puede ser implementado como el dispositivo 570, incluyendo, pero no limitado a, un dispositivo de salida USB (bus serie universal) y/o un puerto USB accesible desde
30 el exterior situado en el sistema 210, un puerto FireWire (IEEE1394) del dispositivo de salida y/o un puerto FireWire accesible desde el exterior situado en el sistema 210, con una funcionalidad fija o móvil. En la presente realización, el dispositivo de salida de hardware de medios 570 se muestra incluyendo un conmutador 571 controlado por el CCM 300 a través de la línea de comunicación 523, similar a los conmutadores 311 y 312, para controlar la salida de los medios entrantes 499.

35 En una realización, el CCM 300 está acoplado en comunicación con la aplicación de reproducción 501 a través de la conexión 520, la cuña de controlador de forma de onda 309 a través de la conexión 522, el dispositivo de medios personalizado 310, a través de la conexión 521, y el dispositivo de salida de hardware de medios 570 a través de la conexión 523. El CCM 300 está acoplado a, y controla un conmutador seleccionable 311 en la cuña del controlador de forma de onda 309 a través de la conexión 522. El CCM 300 está también acoplado a, y controla a un conmutador 312 seleccionable en el dispositivo de audio personalizado 310 a través de la conexión 521. El CCM 300 está acoplado además a y controla a un conmutador seleccionable 571 en un dispositivo de medios de salida de hardware 570 a través de la conexión 523. Dependiendo de las restricciones de derechos de autor y acuerdos de licencia aplicables a un archivo de medios entrante, por ejemplo, los medios 499, el CCM 300 controla si los
45 conmutadores 311 y 312 están abiertos (como se muestra), lo que impide que los medios entrantes 499 lleguen a una aplicación de grabación, o cerrado (no se muestra) a fin de permitir la grabación de los medios entrantes 499. Además, el CCM 300 controla si el conmutador 571 está abierto (como se muestra), evitando así que los medios entrantes 499 se emitan desde la salida digital 575 del dispositivo de salida de hardware de medios 570, o cerrado (no mostrado) para permitir que los medios entrantes 499 se emitan desde el dispositivo de salida de hardware de
50 medios 570.

En una realización, el CCM 300 está acoplado en comunicación con la aplicación de reproducción 501 a través de la conexión 520, la cuña de controlador de forma de onda 309 a través de la conexión 522, el dispositivo de medios personalizado 310, a través de la conexión 521, y el dispositivo de salida del hardware de medios 570 a través de la
55 conexión 523. El CCM 300 está acoplado a, y controla un conmutador seleccionable 311 en la cuña de controlador de forma de onda 309 a través de la conexión 522. El CCM 300 está también acoplado a, y controla un conmutador seleccionable 312 en el dispositivo de audio personalizado 310 a través de la conexión 521. El CCM 300 está acoplado además a y controla un conmutador seleccionable 571 en un dispositivo de medios de salida de hardware 570 a través de la conexión 523. Dependiendo de las restricciones de derechos de autor y acuerdos de licencia aplicables a un archivo de medios entrante, por ejemplo, los medios 499, el CCM 300 controla si los conmutadores
60 311 y 312 están abiertos (tal como se muestra), lo que impide que los medios entrantes 499 lleguen a una aplicación de grabación, o cerrados (no mostrado) para permitir la grabación de los medios entrantes 499. Además, el CCM 300 controla si el conmutador 571 está abierto (tal como se muestra), evitando así que los medios entrantes 499 se envíen desde la salida digital 575 del dispositivo de salida de hardware de los medios 570, o cerrado (no mostrado) para permitir que los medios entrantes 499 se envíen desde el dispositivo de salida de hardware de medios 570.
65

Mediante el control del dispositivo de salida de hardware de medios 570, el mecanismo de cumplimiento de derechos de autor 300 puede impedir la salida no autorizada de los medios entrantes 499 a, por ejemplo, un dispositivo de grabación digital que puede estar acoplado con la salida digital 575 del dispositivo de salida de hardware de medios 570. Por consiguiente, en una realización, el CCM 300 está habilitado para detectar también los dispositivos de grabación digital que puede estar acoplados a una línea de salida digital, por ejemplo, 571, de un dispositivo de salida de hardware de los medios, por ejemplo, 570. Ejemplos de un dispositivo de grabación digital que pueden estar acoplados a un dispositivo de salida de hardware de medios 570 puede incluir, pero no se limitan a, grabadoras mini-disc, grabadoras MP3, grabadoras digitales personales, dispositivos de grabación digital acoplados con sistemas multimedia, dispositivos de comunicación personal, cajas de ajuste superior, y/o casi cualquier dispositivo digital que pueda capturar medios entrantes 499 que son enviados desde un dispositivo de salida de hardware de medios 570, por ejemplo, una tarjeta de sonido.

Continuando con la figura 5C, el sonido directo 504 se muestra acoplado con el dispositivo de medios personalizado 310 a través de la línea de entrada de onda 553, en lugar de acoplarse con el controlador del dispositivo de medios 505 (figura 5A). En una realización, el dispositivo de audio personalizado 310 manda la selección explícita a través del sistema 210, lo que significa que el dispositivo de audio personalizado 310 debe seleccionarse como controlador predeterminado del sistema 210. En virtud de que la selección de un dispositivo de medios personalizado 310 como el controlador por defecto del sistema 210, se cierra selectivamente la trayectoria de datos necesaria para el sonido directo 504 para capturar el contenido de medios.

Por ejemplo, los medios entrantes 499 procedentes de casi cualquier fuente, con referencia a la figura 5A, son recibidos por la aplicación de reproducción de medios 501 del sistema 210. La aplicación de reproducción 501 se comunica con el CCM 300, a través de la conexión 520, para determinar si los medios entrantes 499 están protegidos por las restricciones de derechos de autor y/o acuerdos de licencia. La aplicación de reproducción 501 se comunica con el CCM 300 para controlar el conmutador 311, 312, y 571 en consecuencia. En el presente ejemplo, la grabación de los medios entrantes 499 viola las restricciones y/o los acuerdos aplicables y por lo tanto, el conmutador 312 está en una posición abierta, de tal manera que la trayectoria de salida a la aplicación de grabación 502, por ejemplo, la línea de salida de onda 548 y/o línea de salida de onda 568, está bloqueada, lo que impide la grabación no autorizada de los medios 499.

Alternativamente, si el controlador de dispositivos de medios 505 se selecciona como el controlador predeterminado, los medios entrantes 499 continúan desde el subsistema multimedia O/S 503, a través del dispositivo de audio personalizado 310, la caña de controlador de ondas 309, y el controlador del dispositivo de los medios 505, donde los medios 499 pueden enviarse simultáneamente al dispositivo de salida de los medios 570 a través de la línea 580, y enviarse a la línea de la onda de salida 540 y reproducirse por el controlador del dispositivo de medios 505 a la caña de controlador de ondas 309 en la línea de salida de onda 542. Sin embargo, en virtud del CCM 300, del conmutador de control 311, la línea de salida de onda 544, que finalmente conduce a la aplicación de grabación 502 se bloquea, lo que efectivamente impide la grabación no autorizada de los medios 499.

Se destaca particularmente que, en virtud al CCM 300 que controla ambos conmutadores 311 y 312 y, por lo tanto, controla la línea de salida de onda 548 y la línea de salida de onda 568, los archivos de medios entrantes, por ejemplo, los medios entrantes 499, se puede evitar que se graben de una manera no autorizada, de acuerdo con las restricciones de derechos de autor y/o acuerdos de concesión de licencias relacionadas con los medios entrantes.

Todavía con referencia a la figura 5C, se observa particularmente que aunque el CCM 300 puede impedir la grabación no autorizada de los medios entrantes 499 mediante el control de los conmutadores 311 y 312, impidiendo así que los medios entrantes 499 alcancen la aplicación de grabación 502, el control de los conmutadores 311 y 312 no hace nada para prevenir que los medios entrantes 499 sean capturados por un dispositivo digital periférico, por ejemplo, una grabadora de mini-disc, etc., acoplado a una salida digital 575 del dispositivo 570. Así, controlando también la salida, a través de la salida digital 575 del dispositivo de salida de hardware de medios 570, a través del control del conmutador 571, el CCM 300 puede prevenir la captura no autorizada de los medios entrantes 499 durante la salida, por ejemplo, en una tarjeta de sonido para archivos de audio, un vídeo tarjeta de vídeo y/o archivos gráficos, independientemente de si los medios entrantes 499 se han recibido de una manera segura y codificada. Sin embargo, cuando el conmutador 571 está en una posición cerrada, los medios entrantes 499 pueden ser reproducidos de una manera ilimitada. Además, en cualquier momento durante la reproducción de los medios 499, el conmutador 312 del dispositivo de medios personalizado 310, el conmutador 311 del controlador del dispositivo de medios 309, y/o el conmutador 571 del dispositivo de salida de hardware de medios 570 pueden ser activados dinámicamente por el CCM 300.

La figura 5D es un ejemplo de un diagrama de bloques de la trayectoria lógica/de bits 500D de un sistema de ordenador del cliente, por ejemplo, 210, configurado con un mecanismo de cumplimiento de los derechos de autor 300 para prevenir la salida basada en el núcleo no autorizado y basado en la grabación no autorizada de los medios con derechos de autor de acuerdo con una realización de la presente invención. El mecanismo de cumplimiento de derechos de autor 300 está, en una realización, acoplado con y operativo en el sistema del cliente 210 de la manera descrita aquí con referencia a las figuras 4, 5A, 5B, 5C, 6, y 7.

El diagrama 500D de la figura 5D es similar al diagrama 500C de la figura 5C, con algunos cambios. Particularmente, el diagrama 500D incluye un mecanismo de transmisión del núcleo 515, por ejemplo, DirectKS, que está acoplado con un controlador del dispositivo de medios 505. En una realización, DirectKS 515 se puede utilizar para establecer una conexión directa con el controlador del dispositivo de medios 505. En la presente realización, el controlador del dispositivo de medios 505 se muestra incluyendo un conmutador 511 controlado por el CCM 300 a través de la línea de comunicación 524, que es similar a los conmutadores 311, 312, y 571, para controlar la salida de los medios entrantes 499.

En una realización, el CCM 300 está acoplado en comunicación con: la aplicación de reproducción 501 a través de la conexión 520, la cuña de controlador de forma de onda 309 a través de la conexión 522, el dispositivo de medios personalizado 310 a través de la conexión 521, y el controlador del dispositivo de medios 505 a través de la conexión 524. Específicamente, el CCM 300 está acoplado a, y controla un conmutador seleccionable 311 en la cuña de controlador en forma de onda 309 a través de la conexión 522. El CCM 300 está también acoplado a, y controla un conmutador 312 seleccionable en el dispositivo de audio personalizado 310 a través de la conexión 521. El CCM 300 está también acoplado a y controla un conmutador seleccionable 511 en el controlador del dispositivo de medios 505 a través de la conexión 524. Dependiendo de las restricciones de derechos de autor y acuerdos de licencia aplicables a una archivo de medios entrante, por ejemplo, los medios 499, el CCM 300 controla si los conmutadores 311 y 312 están abiertos (tal como se muestra), lo que impide que la entrada de medios 499 llegue a una aplicación de grabación, o cerrado (no mostrado) para permitir la grabación de la entrada de medios 499. Además, el CCM 300 511 controla si el conmutador está abierto (tal como se muestra), evitando así que los medios entrantes 499 sean devueltos desde el controlador del dispositivo de medios 505 a la aplicación de reproducción 501, donde DirectKS 515 puede capturar los medios entrantes 499 y redirigirlos a la aplicación de grabación 502 para crear un copia no autorizada o la grabación de los medios entrantes 499. El CCM 300 también puede controlar si el conmutador 511 está cerrado (no mostrado) para permitir que los medios entrantes 499 sean devueltos a la aplicación de reproducción 501, donde DirectKS 515 puede capturar y redirigir los medios entrantes 499 a la aplicación de grabación 502.

DirectKS 515, en una realización, puede representar un mecanismo de transmisión de núcleo que está adaptado para establecer una conexión directa con un controlador del dispositivo de medios 505 de un sistema operativo operable en el sistema de ordenador del cliente 210, permitiendo el acceso al nivel de núcleo del controlador del dispositivo de medios 505. Un mecanismo de transmisión del núcleo se puede implementar con el fin de impedir la utilización de audio estándar de APIs (interfaces de programación de aplicaciones) para reproducir o grabar contenidos de los medios, con especial atención a las aplicaciones de reproducción con los requisitos de baja latencia. DirectKS 515 puede pasar por alto las API existentes y comunicarse con los controladores del dispositivo de medios 505. DirectKS 515 se puede adaptar fácilmente para trabajar en conjunto con una aplicación de reproducción, por ejemplo, 501, para capturar y redirigir los medios entrantes 499 a la aplicación de grabación 502, a través de la línea de onda de salida 588. En consecuencia, DirectKS 515 se puede implementar para crear grabaciones de medios no autorizados.

Mediante el control del controlador del dispositivo de medios 505, el mecanismo de cumplimiento de derechos de autor 300 puede impedir la salida no autorizada de los medios entrantes 499 a, por ejemplo, un dispositivo de grabación digital 529 que puede acoplarse con la aplicación de grabación 502. En una realización, el controlador del dispositivo de medios 505 se configura a través del mezclador del núcleo (no mostrado) para controlar la trayectoria de datos. Adicionalmente, en una realización, el CCM 300 está habilitado para detectar también un mecanismo de transmisión de núcleo 515 (por ejemplo, DirectKS) que puede ser operable en el sistema de ordenador del cliente 210, tal como se describe en la presente memoria con referencia a la figura 3.

En una realización, el dispositivo de medios personalizado 310 manda la selección explícita a través del sistema 210, lo que significa que el dispositivo de medios personalizado 310 es necesario para seleccionar un controlador por defecto del sistema 210. En virtud de que la selección de un dispositivo de medios personalizado 310 tal como el controlador por defecto del sistema 210, la trayectoria de datos necesaria para el sonido directo 504 que captura el contenido de medios se cierra selectivamente.

Por ejemplo, los medios entrantes 499 procedentes de casi cualquier fuente, con referencia a la figura 5A, son recibida por la aplicación de reproducción de los medios 501 del sistema 210. La aplicación de reproducción 501 se comunica con el CCM 300, a través de la conexión 520, para determinar si los medios entrantes 499 están protegidos por restricciones de derechos de autor y/o acuerdos de licencia. La aplicación de reproducción 501 se comunica con el CCM 300 para controlar los conmutadores 311, 312, 571, y 511, en consecuencia. En el presente ejemplo, la grabación de los medios entrantes 499 violarían las restricciones aplicables y/o acuerdos y, por lo tanto, el conmutador 511 está en una posición abierta, de tal manera que la trayectoria de salida de la aplicación de grabación 502, por ejemplo, la línea de salida de onda 548 y/o línea de salida de onda 568 y/o la línea de salida de onda 588, está bloqueada, lo que impide la grabación no autorizada de los medios 499.

Todavía con referencia a la figura 5D, se indica particularmente que aunque el CCM 300 puede impedir la grabación no autorizada de los medios entrantes 499 mediante el control de los conmutadores 311, 12 y 571, evitando así que los medios entrantes 499 alcancen la aplicación de grabación 502, el control de los conmutadores 311, 312, y 571,

no hace nada para evitar que los medios de entrada 499 vuelvan a la aplicación de grabación 502 mediante un mecanismo retransmisión del núcleo 515 (por ejemplo, DirectKS), que permite capturar y redirigir los medios entrantes 499 a la aplicación de grabación 502, a través de la línea de salida de onda 588. Así, también controlando el conmutador 511 del controlador del dispositivo de medios 505, el CCM 300 puede prevenir que el mecanismo de transmisión del núcleo 515 devuelva los medios entrantes 499 a la aplicación de grabación 502, impidiendo así que los medios entrantes 499 sean capturados y redirigidos a la aplicación de grabación 502 en un intento de crear una copia no autorizada y/o grabar los medios entrantes 499. Sin embargo, cuando el conmutador 511 está en una posición cerrada, los medios entrantes 499 pueden ser devueltos a una aplicación de grabación 502, de tal manera que la grabación podría ser posible, previendo que la grabación no viola las restricciones de derechos de autor aplicables a los medios entrantes 499. Además, en cualquier momento durante la reproducción de los medios 499, el conmutador 312 del dispositivo de medios personalizado 310, el conmutador 311 de la cuña de controlador de ondas 309, y/o el conmutador 511 de controlador del dispositivo de medios 505 puede activarse dinámicamente mediante el CCM 300.

La figura 6A es un diagrama de bloques de un archivo de medios, por ejemplo, los medios entrantes 499, adaptado para ser recibido por una aplicación de reproducción, por ejemplo, 501 de las figuras 5A, 5B, 5C y 5D, configurado con un indicador 605 para permitir que los medios entrantes 499 cumplan con las reglas de acuerdo con el SCMS (sistema de gestión de copia en serie). Cuando sea aplicable a un archivo de medias, por ejemplo, 499, el SCMS permite hacer una copia de un archivo de medios con derechos de autor, pero no para hacer copias de copias. Así, si los medios entrantes 499 pueden ser capturados por una aplicación de grabación, por ejemplo, 502 de las figuras 5A, 5B, 5C, y/o 5D, y/o un dispositivo de grabación, por ejemplo, 529, y/o un dispositivo de grabación periférico y/o una aplicación de grabación acoplada a una salida digital de un dispositivo de salida de medios de hardware, por ejemplo, la salida digital 575 del dispositivo de medios de salida de hardware 570 de las figuras 5B, 5C y 5D, y/o a un mecanismo de transmisión de núcleo 515, por ejemplo, DirectKS de la figura 5D, se puede lograr una copia no autorizada y/o la grabación.

La aplicación de reproducción 501 se acopla con el CCM 300 a través de la línea de comunicación 520 de una manera análoga a las figuras 5A, 5B, 5C, y/o 5D. Aunque no se muestra en la figura 6, se observa que el CCM 300 está acoplado también a los conmutadores 311 y 511 tal como se muestra en la figura 5A, los conmutadores 311 y 312 en la figura 5B, los conmutadores 311, 312, y 571 en la figura 5C, y los conmutadores, 311, 312, 571, y 511, en la figura 5D.

En una realización, un indicador 605 está unido a los medios entrantes 499 para impedir la copia no autorizada o la grabación de acuerdo con el SCMS. En una realización, el indicador 605 puede ser un bit que puede ser transmitido antes de comenzar la distribución de los medios entrantes 499 a la aplicación de reproducción 501. En otra realización, el indicador 605 puede colocarse al principio de la cadena de bits de los medios entrantes 499. En otra realización, el indicador 605 puede colocarse en de un período de marcos de los medios entrantes 499, por ejemplo, cada quinto marco, o cualquier otro período deseado de marcos. En otra realización, el indicador 605 puede transmitirse en un intervalo de tiempo particular o en intervalos durante el suministro del archivo de medios, por ejemplo, los medios entrantes 499. Así, el indicador 605 puede colocarse casi en cualquier lugar dentro de o unido a la cadena de bits relacionada con los medios entrantes 499.

El indicador 605 puede comprender varios indicadores, por ejemplo, un indicador de nivel 0, un indicador de nivel 1, y un indicador de nivel 2, en una realización de la presente invención. En la presente realización, un indicador de nivel puede ser 0 para indicar al CCM 300 que la copia se permite sin restricción, por ejemplo, que los medios entrantes 499 no tienen derechos de autor o que el derecho de autor no se afirmó. En la presente realización, un nivel 1 puede ser indicador para indicar al CCM 300 que se puede hacer una generación de copias de los medios entrantes 499, de tal manera que los medios entrantes 499 son una copia original y que se puede realizar una copia. En la presente realización, un nivel 2 puede ser indicador para indicar al CCM 300 que los medios entrantes 499 están protegidos por copyright y/o una copia de la misma, y como tal, la copia digital no está permitida.

Por ejemplo, los medios entrantes 499 son recibidos por aplicación de reproducción 501. La aplicación 501 detecta un indicador 605 unido con la misma, en este ejemplo, un nivel de 2 bits se coloca en el flujo de bits para indicar al CCM 300 que la copia no está permitida.

Por ejemplo, cuando el CCM 300 está configurado en el sistema 210 tal como el mostrado en la figura 5A, en respuesta a un bit indicador de nivel 2, el CCM 300, mientras controla la trayectoria del audio, a continuación, activa los conmutadores 311 y 511 para evitar cualquier grabación de los medios entrantes 499.

Cuando el CCM 300 está configurado en el sistema 210 tal como el mostrado en la figura 5B, en respuesta a un bit indicador de nivel 2, el CCM 300, mientras controla la trayectoria de audio, a continuación, activa los conmutadores 311 y 312 para evitar cualquier grabación de los medios entrantes 499.

Cuando el CCM 300 está configurado en el sistema 210 tal como el mostrado en la figura 5C, en respuesta a un bit indicador de nivel 2, el CCM 300, mientras controla la trayectoria de audio, a continuación, activa los conmutadores 311, 312, y 571 para evitar cualquier grabación de los medios entrantes 499.

Se observa que el CCM 300 puede activar o desactivar los conmutadores acoplados con el mismo, tal como se describe en la presente memoria con referencia a las figuras 5A, 5B, 5C y 5D, así canalizando los medios entrantes 499 a través de la trayectoria de los medios segura, en este ejemplo la trayectoria de audio, para evitar una copia no autorizada de los medios entrantes 499. Se observa además que el CCM 300 puede detectar aplicaciones de grabación de medios y los dispositivos tal como se describe en la presente memoria, con referencia a la figura 3.

Las figuras 7A, 7B y 7C son un diagrama de flujo 700 de las etapas realizadas de acuerdo con una realización de la presente invención para controlar la interacción del usuario final de los medios electrónicos suministrados. El diagrama de flujo 700 incluye procesos de la presente invención que, en una realización, se llevan a cabo por los procesadores y componentes eléctricos bajo el control de instrucciones ejecutables por ordenador y legibles por ordenador. Las instrucciones ejecutables por ordenador y legibles por ordenador residen, por ejemplo, en las funciones de almacenamiento de datos, tal como memoria volátil utilizable por el ordenador 104 y/o memoria no volátil utilizable por el ordenador 103 de la figura 1. Sin embargo, las instrucciones ejecutables por ordenador y legibles por ordenador pueden residir en cualquier tipo de medios legibles por ordenador. Aunque las etapas específicas se describen en diagrama de flujo 700, estas etapas son a modo de ejemplo. Esto es, la presente invención se adapta bien a la realización de varias otras etapas o variaciones de las etapas indicadas en las figuras 7A, 7B y 7C. Dentro de la presente realización, se debe apreciar que las etapas del diagrama de flujo 700 pueden realizarse mediante software, hardware o mediante cualquier combinación de software y hardware.

La presente realización proporciona un mecanismo para restringir la grabación del contenido de medios de alta fidelidad suministrado a través de una o más redes de comunicación. La presente realización proporciona contenido multimedia de alta fidelidad a los clientes registrados, mientras se evita que clientes no autorizados reciban contenido multimedia directamente desde una base de datos de origen. Una vez que el sistema de ordenador del cliente recibe el contenido de los medios, que pueden ser almacenados en directorios ocultos y/o en sistemas de archivos personalizados que pueden estar ocultos para evitar el intercambio no autorizado posterior con otros. Se observa que las diversas funcionalidades se pueden implementar para proteger y monitorizar el contenido de los medios suministrados. Por ejemplo, la dirección física del contenido de los medios se puede ocultar de los receptores de los contenidos de los medios. En otro ejemplo, la dirección del directorio del contenido de los medios puede cambiarse periódicamente. Además, un procedimiento de clave de acceso y de restricción de control de la frecuencia también puede implementarse para controlar y restringir solicitudes sospechosas de contenido de medios. Además, un mecanismo de cumplimiento de los derechos de autor, por ejemplo, el CCM 300, se puede instalar en el sistema de ordenador del cliente 210 para proporcionar el cumplimiento en el lado del cliente de los acuerdos de licencia y restricciones de derechos de autor aplicables al contenido de los medios. Mediante la implementación de estas y otras funcionalidades, la presente realización restringe el acceso y la distribución de contenidos de medios distribuidos y proporciona unos medios para la compensación de derechos de autor del propietario de los medios.

Se observa que el diagrama de flujo 700 se describe en conjunción con las figuras 2, 3, 4, 5A, 5B, 5C y 5D, con el fin de describir más completamente el funcionamiento de la presente realización. En la etapa 702 de la figura 7A, un usuario de un sistema de ordenador, por ejemplo, 210, hace que el equipo se acople comunicativamente a un servidor web, por ejemplo, 250, a través de una o más redes de comunicación, por ejemplo, Internet 201, y procede a intentar iniciar la sesión. Se entiende que el registro en el proceso de la etapa 702 se puede realizar en una variedad de maneras de acuerdo con la presente invención.

En la etapa 704 de la figura 7A, el servidor web 250 accede a una base de datos de usuarios, por ejemplo, 450, para determinar si el usuario y el registro del sistema de ordenador 210 están registrados en la misma. Si el usuario y el sistema de ordenador 210 se han registrado en el servidor web 250, la presente realización pasa a la etapa 714. Sin embargo, si el usuario y el sistema de ordenador 210 inician la sesión por primera vez, el servidor web 250 puede iniciar un proceso de registro del usuario y del sistema de ordenador 210 en la etapa 706.

En la etapa 706, se inicia el registro del usuario y del sistema de ordenador 210. El proceso de registro del usuario y del sistema de ordenador puede implicar que el usuario del sistema de ordenador 210 proporcione información personal, incluyendo pero no limitado a, su nombre, dirección, número de teléfono, número de tarjeta de crédito, número de cuenta de pago en línea, identificación biométrica (por ejemplo, huellas dactilares, escaneado de la retina, etc.), y similares. El servidor web 250 puede verificar la exactitud de la información proporcionada. El servidor web 250 también puede adquirir información sobre el sistema de ordenador del usuario 210 incluyendo, pero no limitado a, la identificación de los reproductores de medios dispuestos y el sistema operativo 210, un identificador único correspondiente al sistema de ordenador, etc. En una realización, el identificador único correspondiente al sistema de ordenador puede ser una dirección MAC. Además, el servidor web 250 puede además solicitar que el usuario del sistema de ordenador 210 seleccione un nombre de usuario y una contraseña.

En la etapa 708 de la figura 7A, con posterioridad a la finalización del proceso de registro, el servidor web 250 genera una identificación de usuario (ID) única o clave de usuario asociada con el usuario del sistema de ordenador del cliente 210. El ID de usuario único, o clave de usuario, se almacena entonces por el servidor web 250 de manera que está asociada con ese usuario registrado. Además, una o más cookies que contienen la información específica

de ese usuario y el sistema de ordenador del usuario 210 se instalan en un dispositivo de memoria no volátil, por ejemplo, 103 y/o el dispositivo de almacenamiento de datos 108 del sistema de ordenador 210. Se hace notar que la ID del usuario y la cookie se pueden almacenar en un directorio oculto dentro de uno o más dispositivos de memoria no volátiles dentro del sistema de ordenador 210, evitando de este modo el acceso del usuario y/o la manipulación de esa información. Se observa además que, si la ID de usuario único, o clave de usuario, ha sido previamente generada por el usuario y el ordenador 210 que inicialmente se registran en la etapa 702, la presente realización pasa a la etapa 714

En la etapa 710, el servidor web 250 verifica que el ID del usuario y la(s) cookie(s) están instaladas correctamente en el sistema de ordenador 210 y verifica la integridad de la(s) cookie(s) y el ID del usuario, asegurando así que no se hayan producido alteraciones no autorizadas para el ID del usuario o la cookie. Si el ID del usuario no está instalado y/o no es válido, el servidor web 250 puede volver a iniciar el proceso de registro en la etapa 706. Alternativamente, el servidor web 250 puede disociar el sistema de ordenador 210 de la red, lo que requiere un registro previo por parte del usuario del ordenador 210. Si la(s) cookie(s) y el ID del usuario son válidos, la presente realización sigue a la etapa 712.

En la etapa 712 de la figura 7A, el servidor web 250 puede instalar una versión de un mecanismo de cumplimiento de los derechos de autor, por ejemplo, 300, sobre uno o más dispositivos de memoria no volátiles del sistema de ordenador 210. La instalación del CCM 300 en el sistema de ordenador del usuario 210 puede facilitar el cumplimiento en el lado del cliente de los contratos de licencia de derechos de autor y las restricciones aplicables a determinados contenidos de medios entregados con derechos de autor. En la etapa 712, los componentes del CCM 300, tal como las instrucciones 301, el codificador/decodificador (códec) 303, los programas de agente 304, el sistema de ganchos 305, las interfaces 306, y controladores de dispositivos de medios personalizados 307 (por ejemplo, el dispositivo de medios personalizado 310 de las figuras 5B, 5C y 5D), se instalan en el sistema de ordenador 210, tal como el mostrado en las figuras 5A, 5B, 5C y 5D. En una realización, el sistema de suministro de archivos del protocolo de transferencia de hipertexto puede ser utilizado para instalar el CCM 300 en el sistema de ordenador 210. Sin embargo, la etapa 712 es muy adecuada para instalar el CCM 300 en el sistema de ordenador 210 en una amplia variedad de formas de acuerdo con la presente realización. Por ejemplo, el CCM 300 puede instalarse como un componente integrado en una aplicación de reproducción de medios, aplicación de grabación de medios y/o aplicaciones de reproductor/grabador de medios. Alternativamente, el CCM 300 puede instalarse como un solo mecanismo dentro de un sistema de ordenador del cliente 210. Además, el CCM 300 puede ser instalado como un solo mecanismo y/o como parte de una aplicación incluida en un dispositivo de almacenamiento de medios, por ejemplo, un CD, un DVD, una SD, y/o como parte de un paquete de instalación. En otra realización, el CCM 300 puede instalarse en conjunto con una presentación de contenidos de medios deseado, por ejemplo, escuchar un archivo de audio en un CD de música, leer un documento, visualizar un video, etc. Se observa que, en una realización, el CCM 300 puede instalarse en el sistema del cliente 210 en forma clandestina, relativa a un usuario.

En la etapa 714, el servidor web 250 puede solicitar el nombre de usuario previamente establecido y la contraseña del usuario del sistema de ordenador del cliente 210. En consecuencia, el usuario del sistema de ordenador del cliente 210 hace que se transmita al servidor web 250 el nombre de usuario previamente establecido y la contraseña. Tras la recepción de los mismos, el servidor web 250 puede acceder a una base de datos del usuario, por ejemplo, 450, para determinar su validez. Si el nombre de usuario y la contraseña no son válidos, el servidor web 250 en el que se niega el acceso al diagrama de flujo 500 puede ser interrumpido (no mostrado). Alternativamente, si el nombre de usuario y la contraseña son válidos, la presente realización sigue a la etapa 716.

En la etapa 716 de la figura 7A, el servidor web 250 puede acceder a la base de datos de archivos multimedia 450 para determinar si el mecanismo de cumplimiento de derechos de autor 300 ha sido actualizado para reflejar los cambios realizados en la DMCA ("Digital Millennium Copyright Act") y/o a los acuerdos de licencias interactivas/no interactivo reconocidos por la DMCA. Se observa que los acuerdos de licencia alternativos pueden ser incorporados en el mecanismo de cumplimiento de derechos de autor 300. Ventajosamente, se proporciona un mecanismo de cumplimiento de derechos de autor que puede ser fácilmente actualizado para reflejar los cambios en las restricciones de derechos de autor existentes y/o la introducción de otros tipos de acuerdos de licencia y/o cambios a las aplicaciones existentes de reproducción de medios, o el desarrollo de nuevas aplicaciones de reproducción de medios, el mecanismo de cumplimiento de derechos de autor 300 puede proporcionar el cumplimiento de las restricciones de derechos de autor vigentes.

Continuando con la etapa 716, si el servidor web 250 determina que el CCM 300, o sus componentes, del ordenador 210 ha sido actualizado, el servidor web 250 inicia la instalación de los componentes más nuevos y/o la versión más actual del CCM 300 en el sistema de ordenador 210, que se muestra como la etapa 718. Si el servidor web 250 determina que la versión actual del CCM 300 instalado en el sistema 210 no tiene que actualizarse, la presente realización pasa a la etapa 720 de la figura 7B.

En la etapa 720 de la figura 7B, el usuario del sistema de ordenador del cliente 210 hace que se transmita al servidor web 250, por ejemplo, a través de Internet 201, una solicitud de una lista de reproducción de archivos de medios disponibles. Se observa que la lista de reproducción puede contener todo o parte del contenido de medios disponibles en un servidor de contenidos, por ejemplo, 251.

En la etapa 722, en respuesta al servidor web 250 que recibe la solicitud de lista de reproducción, el servidor web 250 transmite al sistema de ordenador del cliente 210 una lista de reproducción del contenido de medios junto con el ID del usuario único asociado con el usuario que ha iniciado la sesión. El ID del usuario o clave de usuario se puede unir a la lista de reproducción de contenido de medios de una manera invisible para el usuario. Se observa que el contenido de los medios en el servidor de contenido 251 puede ser, pero no se limita a, música de alta fidelidad, audio, vídeo, gráficos, multimedia, datos alfanuméricos, y similares. El contenido de los medios de la lista de reproducción de la etapa 720 se puede implementar de diversas maneras. En un ejemplo, un servidor web 250 puede generar una lista de reproducción de contenido multimedia mediante la combinación de todos los contenidos de los medios disponibles en una lista de reproducción simple. Alternativamente, todos los títulos de contenido de medios, o listas de títulos diferentes, se pueden cargar desde el servidor de contenidos 251 y pasan a un programa CGI (interfaz de puerta común) operativo en el servidor web 250 donde los títulos de medios, o las listas de títulos diferentes, se pueden concatenar en una sola matriz dimensionada que se puede proporcionar al sistema de ordenador del cliente 210. Se entiende que el CGI puede estar escrito en casi cualquier lenguaje de software de computación.

En la etapa 724 de la figura 7B, el usuario del sistema de ordenador del cliente 210 puede utilizar el contenido de medios recibido de lista de reproducción en conjunción con una aplicación de reproducción de medios con el fin de hacer el sistema de ordenador del cliente 210 para transmitir una solicitud al servidor web 250 para la entrega del contenido de medios deseado, y en el que el ID del usuario se incluye automáticamente con el mismo. El contenido de los medios de la lista de reproducción proporcionada al sistema de ordenador del cliente 210 por el servidor web 250 puede permitir al usuario crear una o más listas de reproducción personalizadas para el usuario, seleccionando títulos de contenidos de medios deseados. Se observa que una lista de reproducción de medios personalizada puede establecer el contenido de los medios que eventualmente será entregado al sistema de ordenador del cliente 250 y el orden en que el contenido es distribuido. Además, el usuario del sistema de ordenador del cliente 250 puede crear una o más listas de reproducción personalizadas y almacenar las listas de reproducción en el sistema 250 y/o dentro del servidor web 250. Se observa que la lista de reproducción personalizada no contiene realmente los títulos del contenido de medios deseados, sino que más bien la lista de reproducción incluye uno o más identificadores asociados con el contenido deseado de los medios que puede incluir, pero no se limita a, una canción, un clip de audio, un clip de vídeo, una imagen, un clip multimedia, un documento alfanumérico, o porciones particulares de los mismos. En otra realización, el contenido medios recibido de la lista de reproducción puede incluir un contenido de medios aleatorio de elección de entrega que el usuario del sistema de ordenador del cliente 210 puede transmitir al servidor web 250, con el ID de usuario, para solicitar la entrega del contenido de medios en una forma aleatoria.

En la etapa 726, al recibir la solicitud de contenido de medios del sistema de ordenador del cliente 210, el servidor web 250 determina si el funcionamiento solicitando medios de aplicación en el sistema de ordenador del cliente 210 es una aplicación de medios válida. Una de las funciones de una aplicación de medios válida es ser un reproductor de contenidos de medios en contraposición a una aplicación que se descarga de contenido de medios de forma no autorizada o no regulada. Si el servidor web 250 determina que la aplicación de medios que opera en el sistema 210 no es una aplicación de medios válida, la presente realización pasa a la etapa 727, que en una realización, redirige el sistema de ordenador del cliente 210 a un sitio web cuando el usuario del sistema 210 puede descargar una solicitud válida de reproductor de medios o una aplicación de software que puede identificar el sistema de ordenador del cliente 210, el registro del sistema 210 del servidor web 250 y/o prevenir un registro futuro para un período de tiempo definido, por ejemplo, 15 minutos, una hora, un día, una semana, un mes, un año, o cualquier cantidad de tiempo especificada. Si el servidor web 250 determina que la aplicación de los medios que opera en el sistema 210 es una aplicación multimedia válida, la presente realización pasa a la etapa 728.

En la etapa 728 de la figura 7B, la presente realización hace que el servidor web 250 determine si el ID del usuario (o clave del usuario) que acompañaba a la solicitud de suministro de medios enviada por el sistema de ordenador del cliente 210 es válido. Si el servidor web 250 determina que el ID del usuario no es válido, la presente realización pasa a la etapa 729, donde el sistema de ordenador del cliente 210 puede ser desconectado del servidor web 250 o el sistema de ordenador del cliente 250 puede ser devuelto a la etapa 706 (de la figura 7A) para volver a registrarse y tener otro ID de usuario único generado por el servidor web 250. Cabe señalar que el orden en que las etapas 726 y 728 se llevan a cabo se puede alterar de tal manera que la etapa 728 puede realizarse antes de la etapa 726. Si el servidor web 250 determina que el ID del usuario es válido, la presente realización pasa a la etapa 730.

En la etapa 730, antes de que el servidor web 250 autorice la entrega de la clave y acceder a redirigir el contenido de los archivos de medios solicitados, que se muestra como la etapa 732, el CCM 300 regula determinadas aplicaciones de reproducción de medios y/o funciones de las mismas que son operativas en el sistema de ordenador del cliente 210. Estas funciones reguladas pueden incluir, pausar, detener, barra de progreso, guardar, etc. Se observa que, en una realización, el CCM 300 puede utilizar ganchos del sistema 305 para llevar a cabo la funcionalidad de la etapa 730.

En la etapa 732 de la figura 7C, la presente realización hace que el servidor web 250 transmita al sistema de ordenador del cliente 210 un comando de redireccionamiento junto con una clave de acceso sensible al tiempo (para

esa hora, día o durante el período de tiempo definido) permitiendo así al sistema de ordenador del cliente 210 recibir el contenido de medios solicitado. El comando de redirección puede incluir una dirección sensible al tiempo de la ubicación del contenido en el servidor de contenido de medios 251. La dirección es sensible al tiempo, ya que, en una realización, el servidor de contenidos 251 periódicamente cambia el nombre de todos o algunos de los directorios de las direcciones de los medios, haciendo así que las direcciones fuente de los contenido previas sean obsoletas. Alternativamente, se cambia la dirección del contenido de los medios. En otra realización, la ubicación del contenido de los medios se puede cambiar junto con las direcciones. Independientemente, los usuarios y/o aplicaciones no autorizados se limitan directamente a partir de la recuperación y/o la copia del contenido de los medios desde el servidor de contenidos 251. Por lo tanto, si alguien con intenciones inapropiadas o ilegales es capaz de encontrar dónde se almacena el contenido de medios, los intentos posteriores producirán un error, ya que la trayectoria anterior ya no existe, lo que impide el acceso no autorizado futuro.

Se hace notar que en una realización de la presente invención, las direcciones (o trayectorias) del servidor de contenidos 251 que están activamente acopladas a uno o más sistemas de ordenador del cliente (por ejemplo, 210 - 230) se mantienen mientras que las direcciones futuras, o trayectorias, se crean para dispositivos de nuevos clientes. Además, se observa que a medida que los sistemas de ordenador del cliente se desconectan de la fuente de contenido de los medios del servidor de contenidos 251, esa dirección de directorio, o enlace, se puede cambiar inmediatamente, evitando así que el acceso al sistema del cliente no autorizado o a la aplicación.

En otra realización, la redirección del sistema de ordenador del cliente 210 al servidor de contenidos 251 puede implementarse mediante la utilización de un servidor de red donde múltiples servidores son los proveedores de contenidos, (por ejemplo, 251), o mediante el enrutamiento de un sistema de ordenador del cliente solicitante (por ejemplo, 210, 220 ó 230) a través de varios servidores. En aún otra realización, el suministro de contenido de medios desde un proveedor de contenido central (por ejemplo, 251) se puede encaminar a través de uno o más servidores intermedios antes de ser recibido por el sistema de ordenador del cliente solicitante, por ejemplo, 210 - 230.

La funcionalidad de la etapa 732 es, además, muy adecuada para proporcionar la inscripción del Protocolo de Internet (IP) de los sistemas de ordenador del cliente, por ejemplo, 210, el contenido de los medios solicitados y el tamaño de la transferencia, lo que permite un seguimiento preciso de los pagos de derechos, uso del reloj y transferencias, y la popularidad del contenido de los medios.

En la etapa 734 de la figura 7C, al recibir el comando de redirección, la presente realización hace que la aplicación de reproducción de medios 501 (figuras 5A, 5B, 5C y 5D) que funcionan en el sistema de ordenador del cliente 210 para transmitir automáticamente al servidor de contenidos 251 una nueva solicitud de suministro de medios que puede incluir la clave de acceso sensible al tiempo y la dirección del contenido de los medios deseados.

En la etapa 726 de la figura 7C, el servidor de contenidos 251 determina si la clave de acceso sensible al tiempo asociada con la solicitud de suministro de los nuevos medios es válida. Si el servidor de contenidos 251 determina que la clave de acceso sensible al tiempo es válida, la presente realización pasa a la etapa 738 de la figura 7C. Sin embargo, si el servidor de contenidos 251 determina que la clave de acceso de tiempo no es válida, la presente realización pasa a la etapa 737, un cliente de redirección.

En la etapa 737, el servidor de contenidos redirige el ordenador del cliente 210 a la etapa 732 (no mostrada), donde se genera una nueva clave de acceso. Alternativamente, la etapa 737 hace que la presente realización vuelva a la etapa 704 de la figura 7A. En aún otra realización, la etapa 737 hace que el sistema de ordenador del cliente 210 se desconecte del servidor de contenidos 251.

En la etapa 738 de la figura 7C, el servidor de contenidos 251 transmite el contenido de medios solicitado de alta fidelidad al sistema de ordenador del cliente 210. Se observa que cada archivo de contenido de medios entregado al sistema de ordenador del cliente 210 puede tener un encabezado unido al mismo, antes de la entrega, tal como se describe con referencia a la figura 4. Además, se observa que tanto el contenido de medios y su encabezado adjunto se pueden encriptar. En una realización, el contenido de los medios y el encabezado se pueden encriptar de una manera diferente. Alternativamente, cada archivo de contenido de medios es encriptado de manera diferente. En otra realización, grupos de archivos de medios son encriptados de manera análoga. Se observa que pueden ser utilizados mecanismos de encriptado de dominio público, por ejemplo, Blowfish, y/o mecanismos de encriptado de dominio no públicos.

Todavía con referencia a la etapa 738, el servidor de contenidos 251 transmite el contenido de los medios solicitados en una carga de rotura (en comparación con una velocidad de datos fija), transfiriendo de ese modo el contenido al sistema de ordenador del cliente 210 tan rápido como la velocidad de transferencia de la red permite. Además, el servidor de contenidos 251 puede tener su velocidad de descarga adaptada para ser igual a la tasa de transferencia de la red a la que está acoplado. En otra realización, la tasa de descarga del servidor de contenidos 251 puede adaptarse para igualar la velocidad de transferencia de la red del sistema de ordenador del cliente 210 al que se suministra el contenido de medios. Por ejemplo, si el sistema de ordenador del cliente 210 está acoplado a Internet 201 a través de una conexión T1, entonces el servidor de contenidos 251 transfiere el contenido de medios a

velocidades de transmisión admitidas por la línea de conexión T1. Como tal, una vez que el contenido de medios solicitado se transmite al sistema de ordenador del cliente 210, el servidor de contenidos 251 es entonces capaz de transmitir el contenido de los medios solicitado a otro sistema de ordenador del cliente, por ejemplo, 220 ó 230. Ventajosamente, esto proporciona un medio eficaz para transmitir el contenido de medios, en términos de distribución estadística con el tiempo y no sobrecarga la(s) red(es) de comunicación.

Se hace notar que la entrega del contenido de medios solicitado por el servidor de contenidos 250 al sistema de ordenador del cliente 210 puede ser implementado en una variedad de maneras. Por ejemplo, un protocolo de transferencia de archivos HTTP (Hypertext Transfer Protocol) puede ser utilizado para transferir el contenido de los medios solicitado, así como un mecanismo de cumplimiento de los derechos de autor 300 al cliente 210. De esta manera, el mecanismo de cumplimiento de los derechos de autor, así como cada archivo/título del contenido de medios puede ser entregado en su totalidad. En otra realización, el servidor de contenidos 251 puede transmitir al sistema de ordenador del cliente 250 una memoria intermedia grande de contenido de medios, por ejemplo, clips de audio, clips de video y similares.

En la etapa 740 de la figura 7C, después de recibir el pedido de alta fidelidad del contenido de medios desde el servidor de contenidos 251, la presente realización hace que el sistema de ordenador del cliente 210 almacene el contenido de los medios entregado de una manera que está listo para su presentación, por ejemplo, su reproducción. El contenido de medios está almacenado en el sistema de ordenador del cliente 210 en un sentido que limita la distribución no autorizada. Por ejemplo, la presente realización puede hacer que el contenido de medios de alta fidelidad se almacene en un dispositivo de memoria volátil, utilizando uno o más directorios ocultos y/o sistemas de archivos personalizados que pueden estar ocultos, donde puede ser almacenado en caché durante un período de tiempo limitado. Alternativamente, la presente realización puede hacer que el contenido de medios de alta fidelidad se almacene en un dispositivo de memoria no volátil, por ejemplo, 103 o el dispositivo de almacenamiento de datos 108. Se observa que la manera en la que cada uno de los archivos de contenido de medios entregado que se almacena, de manera volátil o no volátil, puede ser dependiente de las restricciones de licencias y acuerdos de derechos de autor aplicables a cada archivo de contenido de medios. Se observa además que, en una realización, cuando un usuario del sistema de ordenador del cliente 210 enciende el ordenador o hace que el sistema de ordenador del cliente 210 se desconecte de la red, el contenido de medios almacenado en un dispositivo de memoria volátil se elimina normalmente del mismo.

Todavía con referencia a la etapa 740, en otra realización, la presente realización puede causar que el sistema de ordenador del cliente 210 almacene el contenido recibido los medios de una manera no volátil dentro de una aplicación multimedia que opere en el mismo, o dentro de una de las aplicaciones del navegador de Internet (por ejemplo, Netscape Communicator™, Microsoft Internet Explorer™, Opera, Mozilla™, y similares), de modo que el contenido de medios entregado puede ser utilizado de una manera repetitiva. Además, el contenido de medios recibido puede ser almacenado de una manera, por lo que es difícil para un usuario redistribuirlo de manera no autorizada, al tiempo que permite la utilización al usuario de los contenidos recibidos a los medios, por ejemplo, mediante la utilización de uno o más directorios ocultos y/o sistemas de archivos personalizados que también pueden estar ocultos. Cabe señalar que mediante el contenido de los medios de almacenamiento con el sistema de ordenador del cliente 210 (cuando esté permitido por los acuerdos de licencia aplicables y las restricciones de derechos de autor), el servidor de contenidos 251 no necesita volver a entregar el mismo contenido de los medios al sistema de ordenador del cliente 210 cada vez que su usuario desea experimentar (por ejemplo, escuchar, mirar, ver, etc.) el archivo de contenido de medios.

En la etapa 742 de la figura 7C, el archivo del contenido de medios recibido se suministra entonces a una aplicación de reproducción de medios (por ejemplo, la aplicación de reproducción 501 de las figuras 5A, 5B, 5C y 5D), que entonces se ejecuta a través de un códec, por ejemplo, codificador/decodificador 303 del CCM 300, en una realización. En respuesta, el codificador/decodificador 303 envía una solicitud de autorización al servidor, por ejemplo, 251, con los datos de autorización adjuntos, tal como se describe en la presente memoria. En respuesta a la recepción de la solicitud de autorización del códec 303, el servidor 251 compara los datos de la autorización recibida con la almacenada en el servidor 251, y posteriormente, la presente realización pasa a la etapa 744.

En la etapa 744, el servidor 251 responde con una autorización de aceptación o fallo. Si el servidor 251 responde con un fallo, de tal manera que los datos de la autorización recibida no son válidos, el presente procedimiento puede continuar con la etapa 745, donde el servidor 251 puede, en una realización, notificar al usuario del sistema del cliente 210, por ejemplo, mediante la utilización de una interfaz 306, que había una autorización fallida del archivo del contenido de medios solicitado. Se observa que mensajes que tienen significados alternativos similares también pueden ser presentados al usuario del sistema de ordenador del cliente 210, con lo cual se informa al usuario de que la entrega ha fallado. Sin embargo, si los datos de autorización son aprobados, el presente procedimiento pasa a la etapa 746.

En la etapa 746, el servidor 251 envía ciertos datos de vuelta a la aplicación de reproducción de medios, que permite la aplicación de reproducción de medios para presentar el contenido del archivo de medios a través de la aplicación de reproducción de los medios 501 de las figuras 5A, 5B, 5C y 5D. En una realización, una clave de descifrado se puede incluir en los datos transmitidos para descifrar el archivo de contenido de medios suministrado. En otra

realización, una clave de encriptado/descriptado puede incluirse en los datos transmitidos para permitir el acceso a los contenidos del archivo de medios. El presente procedimiento pasa después a la etapa 748.

5 En la etapa 748 de la figura 7C, después de descriptado del archivo de medios, el archivo de medios se puede hacer pasar a través del CCM 300, por ejemplo, un codificador/decodificador 303, a una aplicación de reproducción de medios que funciona en el sistema de ordenador del cliente 210, por ejemplo, la aplicación de reproducción 501 de las figuras 5A, 5B, 5C y 5D, que puede acceder y utilizar la entrega de contenido de medios de alta fidelidad, lo que permite a su(s) usuario(s) experimentar el contenido de los medios, por ejemplo, escucharlo, mirarlo, verlo, o similares. En una realización de la presente invención, un reproductor de medios especializados o personalizados 10 puede estar implicado para experimentar el contenido de los medios, por ejemplo, la interfaz 306 de la figura 3. La interfaz 306 puede aplicarse cuando el CCM 300 no puede modificar una aplicación de reproducción de medios estándar de la industria para cumplir con las restricciones de derechos de autor y/o acuerdos de concesión de licencias de conformidad con la DMCA. Alternativamente, un reproductor de medios especializado o personalizado puede no ser necesario para experimentar el contenido de los medios. En su lugar, un reproductor de medios estándar de la industria puede ser utilizado por el sistema de ordenador del cliente 210 para experimentar el contenido de los medios. Por lo general, muchas aplicaciones de reproducción de medios están disponibles y pueden incluir, pero no están limitados a, Windows™ Media Player™ para PCs (ordenadores personales), iTunes™ 15 Player o QuickTime™ para ordenadores de Apple, y el reproductor XMMS para los ordenadores que utilizan el sistema operativo Linux. Independientemente de la aplicación de reproducción de medios utilizada, mientras que el archivo de medios pase a la aplicación de reproducción de medios, por ejemplo, en una base de marco a marco o en un base de memoria intermedia a memoria intermedia, el codificador/decodificador 303 repetidamente se asegurará de que las reglas del MCP 300 se estén aplicando en un momento determinado durante la reproducción de los medios, que se muestra como la etapa 750.

25 En la etapa 750, como el contenido del archivo de medios se entrega a la aplicación de reproducción de medios, por ejemplo, la aplicación de reproducción de medios 501 de las figuras 5A, 5B, 5C y 5D, de forma periódica, por ejemplo, después de un número determinado de marcos, después de un período definido de tiempo, o en cualquier período de tiempo o datos deseado, el codificador/decodificador 303 repetidamente determina si todas las reglas se aplican o no, de conformidad con las reglas definidas por el CCM 300. Si las reglas no se aplican, por ejemplo, cambian debido a que un usuario abre una aplicación de grabación (por ejemplo, Total Recorder o una aplicación alternativa) el presente procedimiento avanza a la etapa 751. Si las reglas, de acuerdo con el CCM 300, se aplican, el presente procedimiento pasa después a la etapa 752.

35 En la etapa 751 de la figura 7C, si las reglas de acuerdo al CCM 300 no se aplican, la presentación del contenido de medios, en una realización, es suspendida o interrumpida. En una realización, el CCM 300 puede controlar selectivamente los conmutadores 311 y 511 (figura 5A) para prevenir la salida de los medios entrantes 499 (figuras 5A, 5B, 5C y 5D) para una aplicación de grabación 502 (figuras 5A, 5B, y 5C, a través un controlador de cuña de ondas 309 y el sonido directo 504, respectivamente, lo que impide la grabación no autorizada de los medios entrantes 499. En otra realización, el CCM 300 puede controlar selectivamente los conmutadores 311 y 312 (figura 5B) para prevenir la salida de los medios entrantes 499 a la aplicación de grabación 502 a través del controlador de cuña de ondas 309 y el dispositivo de medios personalizados 310, evitando así que la grabación no autorizada de los medios entrantes 499. En aún otra realización, el CCM 300 puede controlar selectivamente los conmutadores 311, 312, no sólo para evitar que los medios de entrada 499 graben de manera no autorizada, sino que también puede controlar selectivamente el conmutador 571 (figura 5C) para impedir la salida no autorizada de los medios entrantes 499 a través de la salida digital 575 del dispositivo de salida de hardware de los medios 570. En aún otra realización, el CCM 300 puede controlar selectivamente los conmutadores 311, 312, 571, y 511 para evitar un mecanismo de transmisión de núcleo 515, por ejemplo, DirectKS de la figura 5D, que puede establecer una conexión con el controlador del dispositivo de medios 505 de la figura 5D, a partir de la captura del contenido de medios de entrada y devolviéndolo a una aplicación de grabación (por ejemplo, 502) para crear una grabación no autorizada del contenido de medios. En una realización, los medios entrantes 499 no se emiten desde la salida digital 575. En otra realización, los medios entrantes 499 pueden emitirse a través de la salida digital 575 pero de una manera inaudible, por ejemplo, silencio. En aún otra realización, los medios entrantes 499 son audibles, pero la funcionalidad de grabación se puede desactivar, de forma que el contenido de los medios no se puede grabar.

55 En la etapa 752, si se cumplen las normas de acuerdo con el CCM 300, el codificador/decodificador 303 recibe una porción posterior del contenido de medios almacenado localmente en el sistema de ordenador del cliente 210. La porción recién recuperada del archivo de medios es presentada entonces por la aplicación de reproducción del cliente, que se muestra en el presente procedimiento que en la etapa 748. Mientras la porción recién recuperada se presenta, las realizaciones del presente procedimiento realizan de nuevo la etapa 750, entonces la etapa 752 ó 751, entonces la etapa 748, luego 750, etc., en un bucle continuo hasta que el contenido del archivo de medios se presenta en su totalidad. Ventajosamente, monitorizando constantemente la reproducción de archivos de medios, el CCM 300 puede detectar actividades no deseadas y hace cumplir las reglas definidas por el CCM 300.

65 La figura 8 es un diagrama de un ejemplo del sistema de suministro de contenido de medios global a alta velocidad 800, de acuerdo con una realización de la presente invención. En una realización, el sistema 800 puede ser utilizado para suministrar contenido de medios a nivel global, por ejemplo, medios de audio, medios de vídeo, medios

gráficos, multimedia, alfanuméricos, etc., a un sistema de ordenador del cliente, por ejemplo, 210, 220, y/o 230, en conjunción con una forma de entrega similar a la descrita en la presente memoria. En una realización, el sistema 800 incluye una red global de entrega 802 que puede incluir varios servidores de contenido, por ejemplo, 804, 806, 808, 810, 812, 814, y 816, que pueden estar ubicados en todo el mundo y que pueden denominarse como puntos de presencia o punto(s) de distribución de medios. Cada servidor de contenidos 804-816 puede almacenar una porción, una porción sustancial, o todo el contenido de una biblioteca de contenido de medios que se puede enviar a los sistemas de ordenador del cliente a través de una red, por ejemplo, Internet 201, o una WAN (red de área amplia). En consecuencia, cada servidor de contenidos 804-816 puede proporcionar contenido de medios a los sistemas de ordenador del cliente en su proximidad respectiva en el mundo. Alternativamente, cada servidor de contenidos puede proporcionar contenido de medios a un gran número de sistemas de ordenador del cliente.

Por ejemplo, un punto de suministro de medios (MDP) 816, localizado en Tokio, Japón, es capaz de proporcionar y suministrar contenido de medios de la biblioteca de contenido de medios almacenado en su base de datos de contenido, por ejemplo, 451, a los sistemas de ordenador del cliente de las regiones asiáticas del mundo, mientras que un punto de suministro de medios 812, ubicado en Nueva York, Nueva York, EE.UU., es capaz de ofrecer y suministrar contenido de medios desde su biblioteca de contenidos de medios almacenados en los dispositivos del cliente en el este de Estados Unidos y Canadá. Se observa que cada nombre de la ciudad, por ejemplo, Londres, Tokio, Hamburgo, San José, Ámsterdam, o Nueva York, asociado con uno de los puntos de suministro de medios 804-816 representa la ubicación desde ese punto de suministro de medios o punto de presencia particular. Sin embargo, se observa además que estos nombres de ciudades son a modo de ejemplo porque los puntos de entrega de los medios 804-816 se pueden ubicar en cualquier lugar en el mundo, y como tal, no se limitan a las ciudades que se muestran en la red global 802.

Todavía con referencia a la figura 8, se observó además que el sistema global 802 se describe en conjunción con las Figuras 2, 3, 4, 5A-D, y 6, con el fin de describir más completamente la operación de la realización de la presente invención. Particularmente, con posterioridad a un sistema de ordenador del cliente, por ejemplo, el sistema de ordenador del cliente 210 de la figura 2, interactuando con un servidor web, por ejemplo, el servidor web 250 de la figura 2, tal como se describe en la presente memoria, los servidores web 250, en una realización, pueden redirigir el sistema de ordenador del cliente 210 para recibir el contenido de medios deseado desde un MDP (por ejemplo, 804 a 816) sobre la base de uno o más criterios diferentes.

Por ejemplo, el sistema de ordenador 210 puede estar situado en Brattleboro, Vermont, y su usuario hace que se inicie la sesión con un servidor web 250 que puede estar situado en cualquier parte del mundo. Se hace notar que las etapas 702-730 de las figuras 7A y 7B se pueden realizar tal como se describe en la presente memoria, de tal manera que la presente realización pasa a la etapa 732 de la figura 7C. En la etapa 732, la presente realización puede determinar qué puntos de suministro de medios, por ejemplo, 804, 806, 808, 810, 812, 814, ó 816, posteriormente pueden proporcionar y suministrar el contenido de medios deseado al sistema de ordenador del cliente 210.

Todavía con referencia a la figura 8, se pueden utilizar uno o más criterios diferentes para determinar qué punto de distribución de medios se selecciona para el suministro del contenido de medios deseado. Por ejemplo, la presente realización puede basar su determinación en que el punto de distribución de medios está en cercana proximidad al sistema de ordenador del cliente 210, por ejemplo, el punto de suministro de medios 816. Esto se puede realizar mediante la utilización de la información del registro almacenado, por ejemplo, la dirección, proporcionada por el usuario del sistema de ordenador del cliente 210. Como alternativa, la presente realización puede basar su determinación en que este punto de distribución de medios ofrece contenido multimedia en la parte del mundo en que se encuentra el sistema de ordenador del cliente. Sin embargo, si cada punto de suministro de medios (por ejemplo, 804 a 816) almacena diferentes contenidos de los medios, la presente realización puede determinar que uno realmente puede proporcionar el contenido de medios deseado. Se observa que estos son los criterios de determinación de ejemplo y las realizaciones de la presente invención no se limitan a dicha aplicación.

Posteriormente a la determinación de qué punto de suministro de medios proporciona el contenido de los medios al sistema de ordenador del cliente 210 en la etapa 732, el servidor web 250 transmite al sistema de ordenador del cliente 210 un comando de redirección al punto de suministro de medios/servidor de contenidos 812 junto con una clave de acceso sensible al tiempo, también se refiere como una clave de sesión (por ejemplo, para qué horas, días, o cualquier período de tiempo definido) permitiendo así que el sistema de ordenador del cliente 210 reciba eventualmente el contenido de los medios solicitados. Dentro del sistema 800, el comando de redirección puede incluir una dirección sensible al tiempo de la ubicación del contenido de medios en el punto de suministro de medios 812. En consecuencia, el punto de suministro de medios 812 de la ciudad de Nueva York posteriormente puede proporcionar y suministrar el contenido de medios que se desee en el sistema de ordenador del cliente 210. Se hace notar que las etapas 732-742 y la etapa 737 de la figura 7C pueden realizarse mediante el punto de suministro de medios 812 de una manera similar al servidor de contenidos 251 descrito en la presente memoria.

Ventajosamente, mediante la utilización de varios servidores de contenidos, por ejemplo, el punto de suministro de medios 804-816, para ofrecer un contenido de medios de alta fidelidad a los sistemas de ordenador del cliente, por ejemplo, 210-230, ubicados en todo el mundo, los sistemas de comunicación de la red Internet 201 no se vuelven

excesivamente congestionados. Además, la red global 802 puede entregar contenido de medios a un gran número de sistemas de ordenador del cliente (por ejemplo, 210 a 230) de una manera más eficiente. Además, mediante la utilización de tecnología de comunicación que tienen tasas de transferencia de datos de hasta 320 Kbps (kilobits por segundo) o más, las realizaciones de la presente invención proporcionan un suministro rápido del contenido de medios en una aplicación en todo el mundo.

Haciendo referencia todavía a la figura 8, se observa que los puntos de suministro de medios/servidores de contenidos 804-816 de la red global 802 se pueden acoplar en una amplia variedad de formas de acuerdo con la presente realización. Por ejemplo, el punto de suministro de medios 804-816 puede ser acoplado utilizando cableado y/o tecnologías de comunicación inalámbrica. Además, se señala que los puntos de suministro de medios 804-816 pueden acoplarse funcionalmente de tal manera que si uno de ellos falla, otro punto de suministro de medios puede asumir y cumplir sus funciones. Además, uno o más servidores web similares al servidor web 250 pueden estar acoplados a la red mundial 802 utilizando cableado y/o tecnologías de comunicación inalámbrica.

Dentro del sistema 800, el servidor de contenidos/punto de suministro de medios 804 incluye una infraestructura de red que, en una realización, es una arquitectura de sistema completamente redundante. Se observa que cada MDP/servidor de contenidos 806-816 de la red mundial 802 puede implementarse para incluir una infraestructura de red de una manera similar a la realización mostrada en el MDP 804.

Específicamente, la infraestructura de red de punto de suministro de medios 804 incluye servidores de seguridad 818 y 820 que están acoplados a cada red global 802. Los cortafuegos 818 y 820 se pueden acoplar a la red global 802 de diversas maneras, por ejemplo, utilizando cableados y/o tecnologías de comunicación inalámbrica. Particularmente, los cortafuegos 818 y 820 pueden estar acoplados a cada red global 702 a través de una transferencia Ethernet 10/100. Sin embargo, el sistema 800 no está limitado de ninguna manera a esta aplicación específica. Se observa que los cortafuegos 818 y 820 se aplican para evitar que usuarios maliciosos accedan a cualquier parte de la infraestructura de red de los medios de 1836, por ejemplo, un enrutador u otro mecanismo de conmutación, acoplada con el mismo y una DB (base de datos) del servidor 840 acoplado al dispositivo 836, mientras el servidor de seguridad 820 incluye un dispositivo 838, por ejemplo, un enrutador u otro mecanismo de conmutación, acoplado con el mismo y una DB (base de datos) del servidor 842 acoplado al dispositivo 838. Además, el servidor de base de datos 840 está acoplado con el dispositivo 838 y el servidor de DB 842 está acoplado con el dispositivo 836.

Todavía con referencia a la figura 8, y en el punto de suministro de medios 804, un cortafuegos 818 está acoplado a un dispositivo de dirección 822 que está acoplado al servidor de aplicación web interna 826 y 828, y un servidor concentrador 830. Un cortafuegos 820 está acoplado a un director 824 que está acoplado a servidores internos de aplicaciones web 826 y 828, y el servidor concentrador 830. El servidor concentrador 830 puede implementarse en una variedad de formas incluyendo, pero no limitado a, un servidor concentrador Linux. El servidor concentrador 780 está acoplado a un dispositivo de almacenamiento de datos 832 capaz de almacenar el contenido de medios. El dispositivo de almacenamiento de datos 832 puede implementarse en una variedad de formas, por ejemplo, como un aparato RAID (matriz redundante de discos de bajo costo/independientes).

Se observa que los puntos de suministro de medios 804-816 pueden implementarse de cualquier manera similar al servidor de contenidos 250 descrito en la presente memoria. Además, los puntos de suministro de medios 804-816 de la presente realización pueden implementarse cada uno como uno o más dispositivos informáticos físicos, por ejemplo, el sistema de ordenador 100 de la figura 1.

En otra realización, el CCM 300 puede adaptarse para colocarse en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999 de las figuras 10 y 11. El dispositivo de almacenamiento de medios 999 puede ser, pero no se limita a, un CD, un DVD u otro dispositivo de almacenamiento óptico o magnético. Gracias a la disposición de una versión del CCM 300 en un dispositivo de almacenamiento de medios 999, las realizaciones de la presente invención pueden proporcionar protección contra copias para audio, vídeo, multimedia, gráficos, información, datos, programas de software, y otras formas de medios que pueden contener material con copyright, y que puede estar dispuesto en un dispositivo de almacenamiento de medios. Alternativamente, el CCM 300 puede estar adaptado para ser instalado en un sistema de ordenador, por ejemplo, el sistema de ordenador del cliente 210, a través de un dispositivo de almacenamiento de medios 999 en el que puede estar dispuesto.

La figura 9 es un diagrama de bloques de un mecanismo de cumplimiento de derechos de autor/dispositivo de almacenamiento de medios (CCM/MSD) 900, una versión del CCM 300 adaptada para colocarse en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999 de las figuras 10 y 11. Se observa que el CCM 300 en el CCM/MSD 900 es análogo al CCM 300 tal como se describe en las figuras 3, 4, 5A-D, 6A y 7A-C. Además, el CCM/MSD 900 puede ser fácilmente actualizado de acuerdo con el sistema de suministro global 800, tal como se describe en las figuras 7A-C, y en la figura 8.

En una realización, el CCM/MSD 900 está adaptado para proporcionar un cumplimiento independiente de las restricciones de derechos de autor y acuerdos de licencia aplicables a los archivos de medios que pueden estar

dispuestos en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999. En otra realización, el CCM/MSD 900 está adaptado para ser instalado en un sistema de ordenador, por ejemplo, el sistema de ordenador del cliente 210 para proporcionar el cumplimiento de las restricciones de copyright y acuerdos de licencia aplicables a los archivos de medios que se describen en las figuras 3, 4, 5A-D, 6A y 7A-C.

5 Haciendo referencia a la figura 9, el CCM/MSD 900 incluye un componente de protocolo de ejecución automática 910 para invocar la instalación automática del CCM 300. Para disuadir a los usuarios de los intentos de saltarse varias características propias del CCM 300, por ejemplo, la función de ejecución automática, el programa de monitorización del CCM 300, el programa de agente 304, se verifica que esas características que han de estar en funcionamiento estén operativas, y si no, el CCM 300 prohíbe al usuario experimentar el contenido del dispositivo de almacenamiento de medios.

15 Si un usuario de alguna manera se salta la función de ejecución automática, y el usuario intenta utilizar una aplicación para capturar una imagen del contenido, la aplicación creará una imagen del contenido en el dispositivo de almacenamiento de medios, que también forma imágenes de la protección de derechos de autor que figura al respecto, y cuando la imagen se reproduce, el CCM 300 reconoce que la protección de copia está presente, y el CCM 300 sólo permitirá al usuario experimentar el contenido cuando esté autorizado, una vez que el CCM 300 esté instalado.

20 En virtud de las protecciones como las descritas anteriormente proporcionadas por el CCM 300, los usuarios serán capaces de experimentar el contenido del dispositivo de almacenamiento de medios en el formato original de alta calidad del contenido, obviando con ello la necesidad de comprimir el archivo de medios utilizado en el sistema del cliente 210. Ventajosamente, el usuario ya no tendrá que sufrir por la producción de baja calidad como resultado de archivos de medios muy comprimidos.

25 Se observa que cuando se adapta para ser implementado en conjunción con un formato de archivo seguro, lo que significa que el formato del archivo es, sin la autorización apropiada, no morfogénico, las realizaciones de la presente invención proporcionan también el cumplimiento efectivo de las restricciones de derechos de autor y acuerdos de licencia con archivos de formatos seguros. El CCM 300 puede controlar los tipos de formatos de archivo en los que el archivo de medios puede transformarse, por ejemplo, wav, mp3, etc.

35 En una realización, la función de ejecución automática asociada con unidad del dispositivo de almacenamiento de medios 1112 del sistema del cliente 210 se activa y es operativa. Alternativamente, un anuncio de la activación de la reproducción automática requerida dentro del sistema del cliente 210 puede visualizarse en el dispositivo de almacenamiento de medios y/o el caso en el que se almacene el dispositivo de almacenamiento de medios.

40 En otra realización, si el CCM 300 está presente o si el usuario está acoplado a un servidor, entonces los mensajes que contienen instrucciones sobre cómo activar la función de ejecución automática de sistema de cliente 210 pueden presentarse al usuario.

En una realización, el componente del protocolo de ejecución automática 910 puede detectar las unidades del dispositivo de almacenamiento de medios residentes en un sistema de ordenador, por ejemplo, el sistema de ordenador del cliente 210.

45 El siguiente código fuente C++ es un ejemplo de implementación de una porción del componente de protocolo de ejecución automática 910 para la detección de unidades del dispositivo de almacenamiento de medios que residen y son operables en el sistema de ordenador del cliente 210, de acuerdo con una realización de la presente invención.

```

50     if ((dwRetVal GetLogicalDrives = ())
        != (DWORD) 0)
        {
            /* initialize variables */
            dwMask = (DWORD) 1;
            /* initialize path to root of current drive */
55         _tcscpy (szDrive, _T ("A: \ \"));
            for (nIndex = 0, dwMask = (DWORD) 1;
                dwMask!= (DWORD) 0;
                nIndex ++, dwMask <<= 1)
            {If ((dwRetVal y dwMask)!= 0)
60                {
                    /* construct path to root of drive */
                    szDrive [0] = (TCHAR) 'A' + nIndex;
                    if (GetDriveType (szDrive) = DRIVE_CDROM)
65                        {
                            MessageBox ((HWND) 0,
                                _T ("unidad de CD-ROM encontrada."),

```

```

szDrive,
MB_OK);
    }
    else
5      { /* clear bit at current position */
        dwRetVal &= (~ dwMask);
    }
}
10 }

```

En otra realización, el componente de protocolo de ejecución automática 910 puede detectar si un dispositivo de almacenamiento de medios que contiene los archivos de medios se ha insertado en una unidad del dispositivo de almacenamiento de medios acoplado con el sistema de ordenador del cliente 210, por ejemplo, la unidad 1112 de la figura 10. En otra realización, el CCM 300 puede incluir instrucciones para la monitorización de la unidad del dispositivo de almacenamiento de medios 1112, y después de la detección de la activación de la unidad, el CCM 300 determina qué tipo de dispositivo de almacenamiento de medios ha sido insertado en el mismo. Posteriormente, el CCM 300 puede detectar diversos factores desencadenantes en el dispositivo de almacenamiento de medios para invocar su protección, por ejemplo, un archivo oculto en los nuevos dispositivos de almacenamiento de medios y/o el bit indicador de copyright en dispositivos de almacenamiento de medios heredados, obviando la necesidad de ejecución automática. Tras la detección, el CCM 300 puede invocar la protección adecuada para el archivo de medios asociado.

El siguiente código fuente C ++ es un ejemplo de implementación de una porción del componente de protocolo de ejecución automática 910 para la detección de un dispositivo de almacenamiento de medios insertado en una unidad del dispositivo de almacenamiento de medios que reside y es operable en el sistema de ordenador del cliente 210, de acuerdo con una realización de la presente invención.

```

/* set error mode for operation */
30 uiErrMode = SetErrorMode (SEM_FAILCRITICALERRORS);
/* initialize path to root of current drive */
tcscopy (szDrive, _T ("A: \\"));
for (nIndex = 0, dwMask = (DWORD) 1;
    dwMask!= (DWORD) 0;
35     nIndex ++, dwMask <<= 1)
if ((dwCDROMMask y dwMask)!= 0)
    { /* construct path to root of drive */
        szDrive [0] = (TCHAR) 'A' + nIndex;
        if (GetDiskFreeSpace (szDrive,
40                               &dwSectors,
                                &dwBytes,
                                &dwClustersFree,
                                &dwClusters)
            != 0)
45             { /* add bit for drive to mask */
                dwRetVal |= dwMask;
            }
    }
}
50 /* restore original error mode */
SetErrorMode (uiErrMode);

```

Además, el componente de protocolo de ejecución automática 910 también puede detectar cambios en los medios, por ejemplo, la inserción de un dispositivo de almacenamiento de medios 999. Además, otros cambios de medios pueden ser detectados con posterioridad a la adaptación del código fuente, incluyendo, pero no limitado a, la detección de un archivo de medios de acceso previo, la detección de un dispositivo de almacenamiento de medios insertado previamente.

El siguiente código fuente C ++ es un ejemplo de implementación de una porción del componente de protocolo de ejecución automática 910 para detectar un cambio en los medios, de acuerdo con una realización de la presente invención.

```

/* initialize path to root of current drive */
tcscopy (szDrive, _T ("A: \\"));
65 for (nIndex = 0, dwMask = (DWORD) 1;
    dwMask!= (DWORD) 0;

```

```

nIndex ++, dwMask <= 1)
{ /* check for presence of CD-ROM media in drive */
  if ((dwCurrMask & dwMask) != 0)
  { /* check if media previously in drive */
    if ((dwPrevMask & dwMask) = 0)
    { /* construct path to root of drive */
      szDrive [0] = (TGHAR) 'A' + nIndex;
      /* check for presence of marker on drive */
      if (IsMPBMarkerPresent (szDrive) != 0)
      {
        /* process autorun proceso information present on drive */
        nRetVal = ProcessAutorun (szDrive);
      }
    }
  }
}

```

20 Todavía con referencia a la figura 9, el CCM/MSD 900 también incluye un controlador filtro del nivel del núcleo 920 para controlar una trayectoria de entrada de datos de un sistema operativo acoplado con y operable en el sistema de ordenador del cliente 210.

El CCM/MSD 900 también incluye un controlador de filtro generalizado 930 para controlar la extracción y aplicaciones de quemado, por ejemplo, Nero, Roxio, Exact Audio Copy, y otros, evitando así estas actividades.

25 El siguiente código fuente C ++ es un ejemplo de implementación de una porción de controlador de filtro generalizado 930 para controlar las aplicaciones de extracción y de grabación que pueden ser residentes en y operativas en el sistema de ordenador del cliente 210, de acuerdo con una realización de la presente invención.

```

bool bDisabled; /* CD * flag indicating CD reads disabled */
30
    /* initialize variables */
    bDisabled = false;
    if (bProtected == true)
    {
35      {if (type = IRP_MJ_DEVICE_CONTROL)
          {
              ULONG UlloControlCode = stack-
> Parameters.DeviceIoControl.IoControlCode;
              if (= ulloControlCode IOCTL_SCSI_PASS_THROUGH)
40              {SCSI_PASS_THROUGH * pspt = (SCSI_PASS_THROUGH *)
Irp-> AssociatedIrp.SystemBuffer;
                  if ((pspt != NULL)
                      && (pspt-> Cdb [0] = SCSIOP_READ_CD))
45                  {
                      pspt-> DataTransferLength = 0;
                      pspt-> ScsiStatus = 0;
                      bDisabled = true;
                  }
              else if (ulloControlCode == IOCTL_SCSI_PASS_THROUGH_DIRECT)
50              {
                  SCSI_PASS_THROUGH_DIRECT * = psptd
(SCSI_PASS_THROUGH_DIRECT *)
Irp-> AssociatedIrp.SystemBuffer;
                  if ((psptd != NULL)
55                  {&& (psptd-> Cdb [0] = SCSIOP_READ_CD))
                      psptd-> DataTransferLength = 0;
                      psptd-> ScsiStatus = 0;
                      bDisabled = true;
                  }
60              }
          }
      }
    }
    if (bDisabled = true)
    { /* complete current request */
65      status = CompleteRequest (Irp, STATUS_SUCCESS, 0);
    }

```

```

else
  {/ * pass request down without additional processing */
    status = IoAcquireRemoveLock (&pdx-> RemoveLock, Irp);
    if (INT_SUCCESS (status))
5      return CompleteRequest (Irp, estatus, 0);
    IoSkipCurrentIrpStackLocation (Irp);
    status = IoCallDriver (pdx-> LowerDeviceObject, Irp);
    IoReleaseRemoveLock (&pdx-> RemoveLock, Irp);
10  }

```

Todavía con referencia a la figura 9, el CCM/MSD 900 incluye un MCP 300, análogo al CCM 300 de la figura 3, que está adaptado para ser instalado en sistema de ordenador del cliente 210 en la forma descrita en la presente memoria.

15 En una realización, el controlador del filtro del nivel del núcleo 920, el controlador del filtro generalizado 930 y el CCM 300 del CCM/MSD 900 se instalan automáticamente en sistema de ordenador del cliente 210, después de la inserción del dispositivo de almacenamiento de medios 999 en una unidad de dispositivo de almacenamiento de medios, por ejemplo, la unidad del dispositivo de almacenamiento de medios 1112 de las figuras 10 y 11. El componente de protocolo de ejecución automática 910, tal como se ha descrito anteriormente, detecta la inserción de un dispositivo de almacenamiento de medios 999 en una unidad adecuada, e inicia la instalación de los componentes, por ejemplo, el CCM 300, el controlador 920 y el controlador 930. En una realización, los controladores 920 y 930 pueden instalarse temporalmente y pueden eliminarse después de la retirada del dispositivo de almacenamiento de medios 999 de la unidad del dispositivo de almacenamiento de medios 1112. En aún otra realización, los controladores 920 y 930 se pueden instalar en directorios ocultos y/o en archivos en el sistema de ordenador del cliente 210. En otra realización, algunos componentes del CCM 300 pueden permanecer instalados en el sistema del cliente 210, por ejemplo, el programa de control (programa agente 304). En otra realización, otros componentes, por ejemplo, el controlador del filtro del nivel del núcleo 920 se puede cargar y descargar dinámicamente según sea necesario de acuerdo con las restricciones de derechos de autor y los acuerdos de licencia aplicables al archivo multimedia.

30 Las realizaciones de la presente invención utilizan software, por ejemplo, el CCM/MSD 900, que se coloca en el dispositivo de almacenamiento de medios 999, en conjunción con el software de control del CCM 300 instalado en el sistema de ordenador del cliente 210, y el servidor web 250 y/o el servidor de contenidos 251, en el que cada componente está acoplado en comunicación con el otro a través de Internet, lo que permite la actualización dinámica de CCM 300 de la manera tal como se describe con referencia a la figura 4, y las etapas 716 y 718 de las figuras 7A-C.

40 En la presente realización, el CCM/MSD 900 proporciona un soporte solo de DRM que es mucho más sofisticado que las soluciones de gestión de derechos digitales. Esto es porque el CCM/MSD 900 entra en la trayectoria de datos del sistema operativo operable en el sistema de ordenador del cliente 210 y obtiene el control de la trayectoria de datos, por ejemplo, el controlador del filtro 1108 de la figura 11, en lugar de explotar las ineficiencias o errores en el sistema de ordenador.

45 La figura 10 es un diagrama de bloques de un entorno comunicativo 1000 para controlar la reproducción no autorizada de los archivos multimedia protegidos dispuestos en un dispositivo de almacenamiento de medios. Incluido en el entorno comunicativo 1000 hay un dispositivo de almacenamiento de medios 1112 acoplado con un sistema de ordenador del cliente 210 a través de un bus de datos/dirección 110. El sistema de ordenador del cliente 210 está acoplado con el servidor web 250 y el servidor de contenidos 251 a través de Internet 201. Un dispositivo de almacenamiento de medios 999, en la que puede estar dispuesto un CCM/MSD 900, se inserta en la unidad del dispositivo de almacenamiento de medios 1112. El componente de protocolo de reproducción automática 910 detecta la inserción y se invoca automáticamente la instalación del CCM 300, el controlador del filtro del nivel del núcleo 920 y el controlador del filtro generalizado 930 desde un dispositivo de almacenamiento de medios 999 en el sistema de ordenador del cliente 210. Posteriormente a la instalación, el CCM 300 inicia una actualización dinámica en el servidor web 250 y/o el servidor de contenidos 251, a través de Internet 201. Mediante la instalación del CCM 50 300 en el sistema de ordenador del cliente, el programa de agente 304 (figura 3) del CCM 300 es capaz de controlar la integridad del software. Además, al consultar con los servidores 250 y/o 251 a través de Internet 201 en línea, la versión de software del CCM 300 en el dispositivo de almacenamiento de medios 999 e instalado en el sistema de ordenador del cliente 210 puede actualizarse cuando se producen elusiones y mantenerse al día de plataforma en plataforma.

60 Ventajosamente, el mecanismo de monitorización del programa de agente 304 permite una formación constante de la versión del CCM 300 dispuesto en el dispositivo de almacenamiento de medios 999 mediante la comunicación con el servidor 250 y/o 260 y utilizando las capacidades de actualización dinámica de la red global 800 para actualizar fácilmente la que ha sido instalado en el sistema de ordenador del cliente 210, a través del dispositivo de almacenamiento de medios 999.

65

En una realización, la instalación se realiza clandestina respecto al usuario y se inicia mediante la inserción de un dispositivo de almacenamiento de medios 999 en una unidad de dispositivo de almacenamiento de medios apropiada, por ejemplo, una unidad de disco magnético/óptico o una unidad de dispositivo alternativo acoplado con el sistema de cliente 210. Si el usuario no está registrado con el CCM 300, tal como se describe en la presente memoria con referencia a la figura 4 y a las figuras 7A-7C, una vez instalado, el CCM 300 inicia un proceso de actualización con los servidores web 250 y/o el servidor de contenidos 251 para incluir fácilmente actualizaciones que han sido invocadas posteriores a la liberación del archivo de medios en el dispositivo de almacenamiento de medios 999. En virtud de las capacidades de actualización dinámica del CCM 300, independientemente de la versión del CCM 300 en el dispositivo de almacenamiento de medios 999, el CCM 300 proporciona el cumplimiento de las restricciones de derechos de autor y acuerdos de licencia aplicables al archivo de medios en el dispositivo de almacenamiento de medios 999. Ventajosamente, el permiso de la capacidad de adaptación dinámica del CCM 300 proporciona la interoperabilidad continuada con sistemas operativos nuevos y actualizados, avances en la tecnología electrónica, tecnologías y protocolos de comunicación, y similares, para garantizar la eficacia del CCM 300 en el futuro.

En otra realización, si el usuario es un usuario registrado con el sistema de suministro global 800, el CCM 300 puede detectar qué versión es la más actual. En consecuencia, cuando la versión existente en el sistema de cliente 210 está más actualizada que la versión (para la instalación) en el dispositivo de almacenamiento de medios 999, el CCM 300 puede pasar por alto el proceso de instalación y presentar los contenidos que figuran en el dispositivo de almacenamiento de medios 999 al usuario para que puedan experimentar.

Ventajosamente, esta tecnología es compatible con las unidades del dispositivo de almacenamiento de medios fabricados con posterioridad a 1982. Además, el CCM 300 es compatible con dispositivos de almacenamiento de medios que tienen un bit indicador de copyright dispuesto sobre el mismo. El bit indicador de copyright ha sido incluido en todos los CDs lanzados desde 1982.

En la presente realización de la figura 10, el archivo de medios no está encriptado en un dispositivo de almacenamiento de medios 999. En una realización, si el archivo de medios está encriptado en el ordenador 210, que puede ser descifrado en el ordenador 210. Sin embargo, los reproductores domésticos y/o dispositivos de reproducción de medios independientes rara vez incluyen un mecanismo de descifrado, y para experimentar la música en un equipo doméstico, la música no se encripta convencionalmente.

En una realización, un componente adicional del CCM 300 es que el disparador del programa del agente 304 puede ser el indicador de bits de derechos de autor. Esto significa que cuando el indicador de bits de derecho de autor es detectado por el CCM 300, se inician las funciones del CCM 300. Alternativamente, en otra realización, cuando el indicador de bits de derechos de autor no se detecta, el CCM 300 puede permanecer en un estado no invocado o inactivo. Si el CCM 300 puede detectar el indicador de bits de derechos de autor, el CCM 300 puede proporcionar el debido cumplimiento en lo que respecta a las restricciones de derechos de autor y acuerdos de licencia aplicables a los archivos de medios.

En una realización alternativa, un control de disparo en la tabla de contenidos de un dispositivo de almacenamiento de medios 999 incluye instrucciones para activar el protocolo de ejecución automática 910 del CCM/MSD 900 y puede utilizar el indicador de bits de derechos de autor o la implementación alternativa para desencadenar la tecnología. De esta manera, el CCM 300 puede controlar las obras protegidas, mientras que el material de dominio público puede ser experimentado y reproducido a discreción del usuario. Debido a que la ejecución automática es un problema para los fabricantes de dispositivos de almacenamiento de medios, las realizaciones del CCM/MSD 900 pueden incluir programas alternativos de ejecución automática que realizan análogos a la ejecución automática.

En otra realización, el CCM 300 puede invocar su propio reproductor de propiedad, por ejemplo, el dispositivo de medios personalizado 310, tal como se describe con referencia a la figura 3, lo que permite un mayor control de las restricciones de copyright y/o acuerdos de licencia aplicables a los medios. Al invocar el dispositivo de medios personalizado 310, el CCM 300 permite una experiencia de usuario de los medios al tiempo que proporciona protección contra la reproducción no autorizada de los medios dispuestos en el dispositivo de almacenamiento de medios 999.

En una realización alternativa, los archivos de medios y el CCM/MSD 900 dispuesto en un dispositivo de almacenamiento de medios 999 están encriptados. Esta aplicación es especialmente ventajosa para versiones de demostración (demo) de los archivos multimedia, versiones beta de prueba, y similares, que pueden ser eliminados en el dispositivo de almacenamiento de medios 999. Se observa que la presente realización es operable en un entorno en línea, lo que significa que sistema de ordenador del cliente 210 está acoplado en comunicación con el servidor web 250 y/o el servidor de contenidos 251 para permitir una experiencia de usuario de los contenidos de una versión de demostración del dispositivo de almacenamiento de medios 999. En esta implementación, el CCM 300 permite reproducciones específicas para usuarios específicos, que pueden ser controladas a través de una red, por ejemplo, la red 1000 de la figura 10, y el servidor 250 y/o 251.

En otra realización, el CCM 300 puede ser implementado para demostración y/o protección previa al lanzamiento. En esta realización, el CCM 300 utiliza tecnología de encriptación sofisticada para encriptar la tabla de contenidos y el CCM 300 con una clave de desencriptado correspondiente ubicada en el sistema de ordenador del cliente. El encriptado del CCM 300 también puede disuadir los intentos nefastos para revertir la ingeniería del CCM 300. El desencriptado se puede realizar utilizando una clave de desencriptado asociada. Alternativamente, el desencriptado puede ser efectuado por un residente de aplicación del reproductor de medios propietario o personalizado en el dispositivo de almacenamiento de medios de demostración, por ejemplo, 999.

El contenido del dispositivo de almacenamiento de medios 999 es encriptado, utilizando varios niveles de encriptado para proporcionar niveles de protección acorde con los titulares de derechos de autor y la protección deseada requerida. Por ejemplo, el dispositivo de almacenamiento de medios 999 se entrega a un usuario o crítico a efectos de revisión, el usuario inserta un dispositivo de medios de almacenamiento 999 en el lector del dispositivo de almacenamiento adecuado o conector junto con el ordenador del periodista y el CCM 300 está instalado en el sistema de cliente 200 de manera clandestina para el usuario. Una vez instalado, el CCM 300 inicia una sesión de comunicación con el servidor web 250/servidor de contenidos 251, donde el servidor de contenidos 251 puede proporcionar autorización para que el usuario experimente los medios en el dispositivo de almacenamiento de medios 999.

En consecuencia, si el usuario, a quien se le ha liberado la demostración del dispositivo de almacenamiento de medios 999, ha robado la demostración del dispositivo de almacenamiento de medios 999, o si el usuario ha permitido que partes alternativas traten de experimentar el contenido del dispositivo de almacenamiento de medios 999, la parte no autorizada tendría que intentar romper las claves de encriptado y el encriptado del contenido real del dispositivo de almacenamiento de medios 999, con un consumo no trivial de cantidades de tiempo.

Por lo tanto, el CCM 300 es capaz de controlar qué usuarios reciben autorización para experimentar los medios del dispositivo de almacenamiento de medios 999, las veces que el usuario puede experimentar los medios, y el CCM 300 también puede definir un período de tiempo hasta que los medios ya no pueden ser accesibles. Esto puede permitir a los titulares de derechos de autor liberar el contenido en un dispositivo de almacenamiento de medios autorizado, por ejemplo, 999, antes de que las copias piratas inunden el mercado.

En consecuencia, un dispositivo de almacenamiento de medios de demostración 999 puede estar configurado de tal manera que un primer usuario pueda obtener una copia, un segundo usuario pueda obtener una copia, y, si se sabe que el segundo usuario comparte la demostración con un tercer y un cuarto usuarios a continuación, los usuarios conocidos estarían capacitados para experimentar los medios. Ventajosamente, en virtud de la definición de la que los usuarios pueden acceder y experimentar los medios, cualquier intercambio no autorizado de los medios por uno de los usuarios autorizados se puede detectar fácilmente, y además se puede detener la compartición o la experimentación de los medios. Además, debido a que el usuario autorizado compartió los medios de forma no autorizada, en un escenario del peor caso, podrían presentarse cargos criminales contra ese usuario.

Se hace notar que la colocación del CCM/MSD 900 en un dispositivo de almacenamiento de medios, por ejemplo, 999, para permitir la instalación del CCM 300 en el sistema del cliente 210 es una manera en la que el CCM 300 se puede instalar en el sistema del cliente 210. Una manera alternativa en la que el CCM 300 se puede instalar en el sistema de ordenador del cliente 210 a través de "polinización cruzada". Por ejemplo, la difusión por Internet transmite el archivo multimedia al usuario. El archivo de medios tiene un CCM 300 acoplado con el archivo de medios, y al descargar el archivo de medios en el sistema de ordenador del cliente 210, las realizaciones de la presente invención permiten la instalación del CCM 300 en el sistema de ordenador del cliente 210. De otra manera, el CCM 300 se incorpora y se convierte en parte de un sistema operativo en funcionamiento en el sistema del cliente 210. Como alternativa, se aprueban leyes que mandan la inclusión del CCM 300 en cada sistema de ordenador del cliente 210.

La figura 11 es un ejemplo de un diagrama de bloques de la trayectoria lógica/de bits 1100 de un sistema de ordenador del cliente, por ejemplo, 210, configurado con un mecanismo de cumplimiento de derechos de autor (CCM) 300 para impedir la reproducción no autorizada de los medios con derechos de autor de acuerdo con una realización de la presente invención. El mecanismo de cumplimiento de derechos de autor 300 está acoplado, en una realización, con y es operativo en el sistema del cliente 210 en cualquier manera descrita con referencia a las figuras 4, 5a-5d, 6A, 7A y 7C, 9, y 10.

El diagrama 1100 de la figura 11 incluye una aplicación de extracción/creación de medios de un dispositivo de almacenamiento de medios 1102 acoplado en comunicación con el subsistema de entrada/salida del sistema operativo 1104 a través de la onda en línea 1121 y de la onda fuera de línea 1138. El subsistema de entrada/salida del sistema operativo 1104 se acopla con el controlador de clase del dispositivo de almacenamiento de medios 1106 a través de la onda en línea 1123 y de la onda fuera de línea 1136. El controlador de clase del dispositivo de almacenamiento de medios 1106 se acopla con el controlador de filtro de onda 1108 a través de la línea 1125 y de la onda fuera de línea 1134. El controlador de filtro 1108 se acopla con el controlador del puerto del dispositivo de almacenamiento de medios 1110 a través de la onda en línea 1127 y de la onda fuera de línea 1132. El controlador del filtro 1108 se muestra incluyendo un conmutador 1111, controlado por el CCM 300 a través del acoplamiento

1160. El controlador del puerto del dispositivo de almacenamiento de medios 1110 es, junto con la unidad del dispositivo de almacenamiento de medios 1112 a través de la línea de onda en 1129 y la línea fuera de onda 1130. El dispositivo de almacenamiento de medios 999, que se muestra incluyendo el CCM/MSD 900 se puede recibir mediante la unidad del dispositivo de almacenamiento de medios 1112. Además, el CCM 300 está acoplado con el
 5 subsistema de entrada/salida del sistema operativo 1104 a través de la onda en línea 1150 y de la onda fuera de línea 1151.

En una realización, el CCM 300 está acoplado y controla el conmutador seleccionable 1111 en el controlador del filtro 1108. Dependiendo de las restricciones de copyright y/o acuerdos de licencia aplicables a un archivo de medios
 10 dispuesto en el dispositivo de almacenamiento de medios 999, el CCM 300 controla si el conmutador está abierto 1111 (mostrado), impidiendo así que el archivo de medios llegue a la aplicación de extracción/creación de los medios 1102, o cerrado (no mostrado) para permitir la reproducción del archivo de medios protegido. La aplicación de extracción/creación de medios 1102 puede ser una aplicación de copia o quemado como Nero, Roxio, Exact Audio Copy, u otra aplicación disponible.

Continuando con la figura 11, el dispositivo de almacenamiento de medios 999 es recibido por la unidad del dispositivo de almacenamiento de medios 1112. El CCM 300 determina si el dispositivo de almacenamiento de medios 999 o los medios dispuestos al respecto están protegidos por las restricciones de derechos de autor y/o
 20 acuerdos de concesión de licencias, por ejemplo, a través de la detección de un bit indicador de autor. El CCM 300 se comunica con controlador del filtro 1108 para controlar el conmutador 1111 en consecuencia. En el presente ejemplo, el dispositivo de reproducción de almacenamiento de medios 999, y/o el mismo contenido, violan las restricciones y/o los acuerdos aplicables, y por lo tanto el conmutador 1111 está en una posición abierta, de tal manera que la trayectoria de salida a la aplicación de extracción/creación de los medios 1102, por ejemplo, línea de onda de salida 1138, se bloquea impidiendo la reproducción no autorizada del dispositivo de almacenamiento de
 25 medios 999.

Se destaca especialmente que, en virtud del conmutador de control 1111 del CCM 300, y por lo tanto el control de onda fuera de línea 1138, cualquier medio protegido de los derechos de autor entrantes dispuesto en un dispositivo de almacenamiento de medios 999 se puede evitar que se reproduzca de forma no autorizada, de acuerdo con las
 30 restricciones de derechos de autor aplicables y/o acuerdos de concesión de licencias relacionadas con los medios entrantes.

Ventajosamente, como se desarrollan nuevos formatos de archivo propietarios o seguros, el CCM 300 puede adaptarse fácilmente para ser funcional con el mismo. Además, el CCM/MSD 900 puede impedir que los usuarios realicen reproducciones no autorizadas de archivos de medios, grabación, copia, extracción, quema, etc. Mediante el uso de los controladores del nivel del filtro del núcleo, por ejemplo, el controlador del filtro 1108, y llegando a un nivel lo suficientemente bajo en el sistema operativo (OS) en el sistema del cliente 210, el CCM 300 puede detectar aplicaciones particulares y cuando se solicita la unidad del dispositivo de almacenamiento de medios 1112 para
 35 sondear los medios de archivo para la copia, extracción, etc., y se desactiva la trayectoria de entrada de datos. El CCM 300, en esta realización, se ocupa de la trayectoria de entrada.

En una realización, las aplicaciones alternativas que monitorizan el estado del sistema de ordenador del cliente 210 puede activar la función de ejecución automática del sistema de ordenador del cliente 210 o alternativamente, invocar un mecanismo automático similar a la reproducción automática para garantizar la invocación del CCM 300
 45 para el cumplimiento de las restricciones de derechos de autor y/o licencias de acuerdos aplicables al dispositivo de almacenamiento de medios 999 y/o los medios protegidos por copyright dispuestos en el mismo.

En una realización, el CCM 300 puede invocar un reproductor de medios de propiedad desde el dispositivo de almacenamiento de medios 999, o activar un reproductor de medios propietario residente y operable en el sistema de ordenador del cliente 210, o un reproductor de medios autorizado residente alternativo en el sistema de ordenador del cliente 210, tal como se describe en la presente memoria con referencia a la figura 3.

Cuando el dispositivo de almacenamiento de medios 999 es un dispositivo de múltiples sesiones, por ejemplo, un disco compacto que tiene una sesión de datos y una sesión de música (audio), y se inserta en la unidad del dispositivo de almacenamiento de medios 1112, el CCM 300 examina el contenido del dispositivo de almacenamiento de medios 999, y en algunos sistemas operativos las pistas de audio no se mostrarán. En su lugar, se muestra la sesión de datos, tal como es un archivo de ejecución automática, por ejemplo, el componente de protocolo de ejecución automática 910, y al hacer clic, invoca una aplicación de reproducción. El CCM 300 puede tener una sesión de datos y archivos a los que el usuario no puede tener acceso a menos que se invoque una
 55 aplicación de reproducción.

En una realización, la aplicación de reproducción podría depositar una porción de monitorización (por ejemplo, programa de agente 304) en el sistema del cliente 210, que en una realización puede residir en el sistema de ordenador del cliente 210 después de la retirada del dispositivo de almacenamiento de medios 999 desde la unidad de dispositivo de almacenamiento de medios 1112.
 65

En virtud del contenido en un dispositivo de almacenamiento de medios de múltiples sesiones 999, que pueden no ser directamente accesibles a la mayoría de las aplicaciones de reproducción, en algún momento se invoca la aplicación del reproductor que puede instalar entonces el CCM 300 en el sistema del cliente 210, de acuerdo con una realización de la presente invención.

5 En una realización, una aplicación de reproducción de medios del propietario se almacena en el dispositivo de almacenamiento de medios 999. Sin embargo, no se invoca automáticamente. Tras la intervención del usuario, por ejemplo, la inserción de un dispositivo de almacenamiento de medios 999 en la unidad del dispositivo de almacenamiento de medios 1112, la aplicación de reproducción multimedia se carga en el sistema del cliente 210 que tiene el CCM 300 integrado en el mismo. Por lo tanto, el CCM 300 se pone en marcha, independientemente de que la ejecución automática esté activada o no activada, y manda que el usuario utilice la aplicación propietaria de reproducción de medios que experimenta el contenido de los archivos de medios en el dispositivo de almacenamiento de medios 999.

15 En una realización alternativa, el sistema de ordenador del cliente 210 ha desactivado la ejecución automática, en el que es común que el usuario sea incapaz de reproducir un archivo de medios a menos que se invoque una aplicación de reproducción de medios del propietario. La activación de la aplicación de reproducción de medios del propietario puede iniciar la instalación de los componentes del CCM 300 que fueron anulados cuando la ejecución automática no está activa.

20 Ventajosamente, al proporcionar un mecanismo de cumplimiento de derechos de autor, por ejemplo, 300, que puede ser fácil y rápidamente instalado en un sistema de ordenador del cliente, por ejemplo, 210, las realizaciones de la presente invención puede ser implementadas para controlar el acceso a, la entrega de, y la experiencia del usuario con el contenido de medios sometido a restricciones de derechos de autor y/o acuerdos de concesión de licencias, por ejemplo, tal como se define por el DMCA. Además, mediante la estrecha asociación con un sistema de ordenador del cliente, por ejemplo, 210, con el usuario del mismo y el contenido de los medios que reciben, las realizaciones de la presente invención también proporcionan una grabación precisa.

30 La figura 12 es un diagrama de bloques de un mecanismo de cumplimiento de uso 1200, una versión alternativa del mecanismo de cumplimiento de derechos de autor 300 que está configurada para colocarse en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999 de las figuras 10, 11, 13, 14, y 15. En una realización de la presente invención, se observa que el CCM 300 en el mecanismo de cumplimiento de uso 1200 es análogo al CCM 300 tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5a-5d, 6A, 7A-7C, 8, 9, 10, y 11. Además, el mecanismo de cumplimiento de uso 1200 puede actualizarse fácilmente de acuerdo con el sistema de entrega global 800, tal como se describe en la presente memoria con referencia a las figuras 7A-7C, y a la figura 8.

40 En una realización, el mecanismo de cumplimiento de uso 1200 está adaptado para colocarse en un dispositivo de almacenamiento de medios 999. El contenido dispuesto en el mismo puede, en una realización, ser contenido de demostración y/o previo al lanzamiento. Ejemplos de contenido de demostración y/o previo al lanzamiento pueden incluir, pero no está limitado a, audio, vídeo, multimedia, gráficos, información, datos, programas informáticos, etc. El contenido de demostración y/o previo al lanzamiento puede incluir, pero no está limitado a, películas digitales o música que puede ser distribuida a las personas en el campo relacionado con los medios para su revisión, por ejemplo, un miembro de la Academia de cine para la revisión de una película, un crítico de la industria de grabaciones para revisar canciones que pueden ser lanzadas en un nuevo disco compacto, etc. Alternativamente, el contenido de demostración y/o previo al lanzamiento también puede contener, pero no se limita a, una versión beta de un programa de software, y similares.

50 Alternativamente, el contenido dispuesto en el dispositivo de almacenamiento de medios 999 puede, en otra realización, ser una versión comercial de contenido de audio, contenido de vídeo, aplicaciones de software, etc. Las realizaciones de la presente invención son muy adecuadas para implementarse en un entorno comercial, por ejemplo, sistemas públicos de presentación tales como aquellos en cines, auditorios, estadios y similares. Además, las realizaciones de la presente invención son fácilmente adaptables para implementarse en los puntos de distribución comercial, por ejemplo, audio, vídeo, y/o software al por menor y/o establecimientos de alquiler, así como implementaciones para pago por visión y/o de pago por reproducción.

60 Por otra parte, las obras literarias, documentos, gráficos, tal como imágenes, pintura, dibujos, y similares pueden comprender el contenido en un dispositivo de almacenamiento de medios. Se observa que una variedad casi interminable de contenidos de demostración, previos al lanzamiento, y/o distribuido comercialmente pueden estar dispuestos en un dispositivo de almacenamiento de medios 999.

65 Haciendo referencia a la figura 12, el mecanismo de cumplimiento de uso (UCM) 1200 incluye un protocolo de ejecución automática 910 para invocar la instalación de los componentes del UCM 1200 en un sistema de ordenador del cliente, por ejemplo, 210, en una realización de la presente invención. El protocolo de ejecución automática 910 de la figura 12 es análogo al protocolo de ejecución automática 910 de la figura 9. También se incluyen en el UCM 1200 un controlador del sistema de filtro de archivos 1220, en una realización de la presente invención.

5 El controlador de filtro del sistema de archivos 1220 puede, en una realización, ser un filtro de nivel superior y/o de nivel inferior para los dispositivos de bus individuales dentro de sistema de ordenador del cliente 210, por ejemplo, el controlador del dispositivo de almacenamiento de medios 1112 de las figuras 10, 11, 13, 14, y 15. El controlador de filtro del sistema de archivos 1220 está habilitado para enganchar sobre el acceso a una unidad del dispositivo de almacenamiento de medios 1112, por ejemplo, una unidad de CD, e intercepta las lecturas de datos asociadas con el acceso al contenido en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999.

10 El controlador del filtro del sistema de archivos 1220 incluye un descryptador 1221 para proporcionar el descryptado de los encriptados aplicados al contenido encriptado, por ejemplo, los encriptados 2351-2N aplicados a los encriptados 1351-1N del contenido de medios 2001-N de la figura 13, en una realización de la presente invención. El descryptador 1221 puede proporcionar el descryptado dinámico de los encriptados aplicados a los contenidos de medios encriptados en un dispositivo de almacenamiento de medios 999 cuando los contenidos, por ejemplo, 2001-N, son accedidos y leídos por unidad del dispositivo de almacenamiento de medios 1112.

20 Todavía con referencia a la figura 12, el UCM 1200 también incluye un reproductor de medios seguro 1210. El reproductor de medios seguro 1210 puede ser, en una realización, similar al dispositivo de medios personalizado 310, una emulación del controlador de dispositivo de medios personalizado 307, tal como se describe en la presente memoria con referencia a las figuras 3 y 5B-5D. Alternativamente, el reproductor de medios seguro 1210 puede ser un reproductor de medios alternativo que tiene propiedades de control análogas al dispositivo de medios personalizados 310. El reproductor de medios seguro 1210 incluye un descryptador 1211 para el descryptado de del encriptado aplicado a cada instancia de medios dispuestos en un dispositivo de almacenamiento de medios 999, por ejemplo, los encriptados 1351 a 1N aplicados al contenido de medios 2001 a N de la figura 13, respectivamente.

25 El reproductor de medios seguro 1210 también incluye un marcador de marcas de agua 1212 para el flujo de datos de salida. En una realización, el marcador de agua 1212 opera al mismo tiempo que el reproductor de medios seguro 1210 y durante la transformación del contenido del reproductor 1210, el marcado de agua 1212, fijará un número de serie, por ejemplo, el número de serie 1380 de la figura 13, asociado con cada dispositivo de almacenamiento de medios 999 en la corriente de datos saliente.

30 La figura 13 es un diagrama de bloques de contenidos y componentes que pueden estar dispuestos en un dispositivo de almacenamiento de medios, por ejemplo, 999, de acuerdo con las realizaciones de la presente invención. La figura 13 se muestra con varias instancias de contenido, por ejemplo, contenido de medios 2001-200N, dispuestos sobre el mismo. El contenido de medios 2001-N puede ser, pero no se limitan a, películas, grabaciones de audio, software beta, documentos, obras literarias, etc. Se hace notar que cualquier medio digital puede estar dispuesto en un dispositivo de almacenamiento de medios 999 o en una pluralidad de dispositivos de almacenamiento de medios 999.

40 El dispositivo de almacenamiento de medios 999 de la figura 13 es análogo al dispositivo de almacenamiento de medios 999 de las figuras 10 y 11, 14, y 15. En una realización de la presente invención, el dispositivo de almacenamiento de medios 999 está configurado para su uso en conjunción con el contenido de demostración y/o previo al lanzamiento.

45 El dispositivo de almacenamiento de medios 999 de la figura 13 se muestra que se ha dispuesto sobre el mismo un UMC (mecanismo de cumplimiento de uso) 1200 para controlar la presentación de los contenidos, por ejemplo, el contenido de los medios 2001-N, dispuesto en el dispositivo de almacenamiento de medios 999. El UCM 1200 en las figuras 13, 14 y 15 es análogo al UCM 1200 aquí descrito con referencia a la figura 12. Cabe señalar que el protocolo de ejecución automática 910 del UCM 1200 está, en una realización, dispuesto en el dispositivo de almacenamiento de medios 999 de una forma no encriptada.

50 También se muestra en el dispositivo de almacenamiento de medios 999 un identificador único para proporcionar una identificación única del dispositivo de almacenamiento de medios, por ejemplo, el número de serie 1380, en una realización de la presente invención. El número de serie 1380 puede ser, pero no está limitado a, casi cualquier tipo de identificación distinguible del indicador, por ejemplo, un número generado aleatoriamente, un número secuencial, una combinación de números y caracteres alfanuméricos, y similares.

60 Ventajosamente, mediante la disposición de un identificador único en un dispositivo de almacenamiento de medios 999, por ejemplo un número de serie 1380, se permite esta estrecha asociación del contenido dispuesto en el mismo, por ejemplo, el contenido de medios 2001-N, con el receptor previsto del dispositivo de almacenamiento de medios, por ejemplo, un crítico de cine, un crítico musical, un miembro premio de la Academia, un probador beta del software, etc. Por lo tanto, mediante la estrecha asociación de un dispositivo de almacenamiento de medios, por ejemplo, 999, con un receptor previsto, por ejemplo, el usuario del sistema de ordenador 210, las realizaciones de la presente invención pueden evitar que personas no autorizadas experimenten contenido en un dispositivo de almacenamiento de medios, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 7A-7C, y

65 8. También es ventajoso tener un identificador único para cada dispositivo de almacenamiento de medios 999, proporcionando las realizaciones también la seguridad al nivel del patrón del dispositivo de almacenamiento de

medios. Esto significa que un empleado que trabaja en un centro de patronado que roba ilegalmente una copia del dispositivo de almacenamiento de medios todavía puede ser capaz de copiar el contenido y convertirlo en copias piratas (versiones no autorizadas) del dispositivo de almacenamiento de medios en un intento de inundar el mercado. Sin embargo, gracias a que cada dispositivo de almacenamiento de medios 999 tiene un identificador
 5 único, y cada dispositivo de almacenamiento de medios 999 se asocia con su destinatario, las personas que no están asociadas con un dispositivo de almacenamiento de medios 999 en particular no serán capaces de experimentar el mismo contenido. Aunque el mercado todavía puede ser inundado con copias piratas, los que adquieren una copia pirata de un dispositivo de almacenamiento de medios 999, de acuerdo con la presente invención, no será capaz de experimentar el mismo contenido, con lo que posiblemente haga que el público sea
 10 menos receptivo a la idea de una copia pirata barata de algo que no se puede utilizar.

En una realización, el dispositivo de almacenamiento de medios 999 puede distribuirse a sus destinatarios en una variedad de maneras. Las formas de distribuir un dispositivo de almacenamiento de medios 999 a sus destinatarios pueden incluir, pero no está limitado a, procedimientos de entrega de correo, por ejemplo, el servicio postal de
 15 Estados Unidos, los servicios de entrega de paquetería, tal como UPS (United Parcel Service) y/o Federal Express servicios de entrega de mensajería, y similares. En otra realización, el receptor previsto de un dispositivo de almacenamiento de medios 999 puede ser requerido para recoger físicamente el dispositivo 999 desde un punto de distribución.

20 También se muestra en el dispositivo de almacenamiento de medios 999 múltiples instancias de contenido, por ejemplo, contenido de medios 2001-N, en una realización de la presente invención. El contenido de medios 2001-N puede ser cualquier tipo de contenido de medios digitales, incluyendo, pero no limitado a, audio, vídeo, multimedia, gráficos, información, datos, programas de software, etc.

25 Todavía con referencia a la figura 13, en una realización de la presente invención, cada instancia de medios 2001-N está sujeta a un primer encriptado, por ejemplo, el encriptado 1351 a 1 N, respectivamente. En una realización, una primera clave de desencriptado para cada encriptado, por ejemplo, el encriptado 1351-1N, puede ser almacenada en un servidor, por ejemplo, el servidor web 250 y/o el servidor de contenidos 251 de las figuras 2, 4, 10, y 14. En una
 30 realización, el reproductor de medios seguro 1210 puede utilizar el desencriptador 1211 y la clave de desencriptado almacenada en el servidor web 250 y/o en el servidor de contenidos 251 y desencriptar los encriptados 1351-1N durante la representación del contenido. Se observa que el reproductor de medios seguro 1210 está acoplado en comunicación con el servidor web 250 y/o el servidor de contenidos 251 durante la representación y la presentación del contenido dispuesto en el dispositivo de almacenamiento de medios 999.

35 Además, el contenido de los medios 2001-N que tiene un primer encriptado aplicado a los mismos, por ejemplo, los encriptados 1351-1N, están cada uno sujeto a un segundo encriptado, por ejemplo, el encriptado 2351-2N, respectivamente, antes de la eliminación del contenido de los medios 2001-N en un dispositivo de almacenamiento de medios 999. En una realización, una segunda clave de desencriptado para desencriptar los encriptados 2351-2N
 40 puede almacenarse en un servidor, por ejemplo, el servidor web 250 y/o el servidor de contenido 251 de las figuras 2, 4, 10, y 14. En una realización, el controlador del filtro del sistema de archivos 1220 puede utilizar el desencriptador 1221 y la segunda clave de desencriptado almacenada en el servidor web 250 y/o el contenido del servidor 251 y se desencriptan los encriptados 2351-2N durante la lectura del contenido en el dispositivo de almacenamiento de medios 999 mediante la unidad del dispositivo de almacenamiento de medios 1112. Se observa que el controlador del filtro de sistema de archivos 1220 está acoplado en comunicación con el servidor web 250 y/o
 45 el servidor de contenido 251 durante la representación y la presentación.

En una realización, los encriptados 1351-1N pueden ser encriptados menos computacionalmente intensivos que los encriptados 2351-2N. Alternativamente, en una realización, los encriptados 1351-1N pueden ser más computacionalmente intensivos que los encriptados 2351-2N.
 50

Hay muchos procedimientos de encriptado disponibles que pueden ser implementados como los encriptados 1351-1 N y/o los encriptados 2351-2N. Ejemplos de encriptado que pueden ser implementados como los encriptados 1351-1N y/o 2351-2N pueden incluir, pero no se limitan a, triple DES, AES, Blowfish, y muchos otros. En una realización, los encriptados 1351-1 N y/o 2351-2N pueden estar compuestos, cada uno, de una serie y/o una mezcla de los
 55 encriptados. Un encriptado diferente, por ejemplo, una pluralidad de encriptados generados al azar, puede implementarse para cada instancia de medios en un dispositivo de almacenamiento de medios, en lugar de utilizar un formato. En una realización, se utilizan numerosas variaciones de Blowfish para proporcionar los encriptados deseados.

60 Ventajosamente, mediante la utilización de múltiples encriptados diferentes para cada instancia de medios, por ejemplo, 2001-N, si una persona/hacker intenta obtener acceso al contenido rompiendo el encriptado se aplica a un contenido de medios, por ejemplo, el segundo encriptado 2352 se aplica al contenido de medios encriptado 2002, y tiene éxito, simplemente han roto el segundo encriptado para el contenido de medios 2002. Sin embargo, el encriptado restante 1352 permanece intacto gracias a los diferentes encriptados. Por lo tanto, la persona/hacker
 65 tendría que realizar todo el proceso de rotura del encriptado de nuevo para acceder al contenido de medios 2002 mediante el dispositivo de almacenamiento de medios 999. Así, después de pasar cantidades de tiempo no triviales

rompiendo dos encriptados diferentes aplicados a una instancia de medios, por ejemplo, el contenido 2002, el contenido restante en el dispositivo de almacenamiento de medios 999 está todavía encriptado, cada uno con su propio encriptado múltiple diferente.

5 La figura 14 es un diagrama de bloques de un entorno comunicativo 1400 para el control de la presentación de contenido de medios dispuestos en un dispositivo de almacenamiento de medios. Incluido en el entorno comunicativo 1400 hay una unidad de dispositivo de almacenamiento de medios 1112 acoplado con un sistema de ordenador del cliente 210 a través de un bus de datos/dirección 110. El sistema de ordenador del cliente 210 está acoplado con el servidor web 250 y/o el servidor de contenido 251 a través de Internet 201. Un dispositivo de
10 almacenamiento de medios 999, en lo cual puede estar dispuesto un mecanismo de cumplimiento de uso 1200, se inserta en la unidad de dispositivo de almacenamiento de medios 1112. El componente de protocolo de ejecución automática 910 detecta la inserción e invoca automáticamente la instalación del CCM 300, el controlador de filtro del sistema de archivos 1220 y el reproductor de medios seguro 1210 del dispositivo de almacenamiento de medios 999 en el sistema de ordenador del cliente 210. Posteriormente a la instalación, el UCM 1200 inicia una actualización dinámica con el servidor web 250 y/o el servidor de contenidos 251, a través de Internet 201, tal como se describe en la presente memoria con referencia a las figuras 3, 4 y 7A-7C, controlando de este modo la integridad del software. Además, al consultar con los servidores 250 y/o 251 a través de Internet 201 en línea, la versión de software del UCM 1200 en el dispositivo de almacenamiento de medios 999 e instalado en el sistema del equipo cliente 210 puede actualizarse cuando se producen elusiones y mantiene al día de plataforma a plataforma.

20 Ventajosamente, el mecanismo de monitorización del programa agente 304 permite una formación constante de la versión del CCM 300 dispuesto en el dispositivo de almacenamiento de medios 999 mediante la comunicación con el servidor 250 y/o 251 y utilizando las capacidades de actualización dinámica de la red global 800 para actualizar fácilmente que la que ha sido instalado en el sistema de ordenador del cliente 210, a través del dispositivo de
25 almacenamiento de medios 999.

En una realización, la instalación se realiza clandestina respecto al receptor del dispositivo de almacenamiento de medios 999 y se inicia mediante la inserción de un dispositivo de almacenamiento de medios 999 en una unidad de dispositivo de almacenamiento de medios apropiada, por ejemplo, una unidad de disco magnético/óptico o
30 dispositivo de accionamiento alternativo acoplado con el sistema del cliente 210. Algunas partes del UCM 1200 determinan si el destinatario está registrado en el servidor web 250 y/o el servidor de contenido 251. Si el destinatario no está registrado con los servidores 250 y/o 251, tal como se describe en la presente memoria con referencia a la figura 4 y a las figuras 7A-7C, y la figura 8, las porciones del UCM 1200 inician un proceso de instalación tal como se describe en la presente memoria con referencia a las figuras 3, 4, 7A-7C, y 11.

35 Si el sistema de ordenador 210 se ha registrado en los servidores 250 y/o 251, el UCM 1200 puede iniciar un proceso de actualización con el servidor web 250 y/o el servidor de contenido 251 al incluir fácilmente las actualizaciones que se han invocado posteriores a la distribución del dispositivo de almacenamiento de medios 999. En virtud de las capacidades de actualización dinámica del UCM 300, independientemente de la versión del CCM 300 en el dispositivo de almacenamiento de medios 999, el UCM 1200 proporciona el cumplimiento con las restricciones de derechos de autor y acuerdos de licencia aplicables al contenido de los medios en el dispositivo de almacenamiento de medios 999, por ejemplo, el contenido de medios 2001-N. Ventajosamente, el permiso de la capacidad de adaptación dinámica del UCM 1200 prevé la interoperabilidad continuada con sistemas operativos nuevos y actualizados, avances en la tecnología electrónica, tecnologías y protocolos de comunicación, y similares,
45 para garantizar la eficacia del UCM 1200 en el futuro.

En otra realización, si el usuario es un usuario registrado en el sistema de entrega global 800, el UCM 1200 puede detectar qué versión es la más actual. En consecuencia, cuando la versión existente en el sistema del cliente 210 está más actualizada que la versión (para la instalación) en el dispositivo de almacenamiento de medios 999, el UCM 1200 puede pasar por alto el proceso de instalación y presentar los contenidos que figuran en el dispositivo de almacenamiento de medios 999 al usuario para que puedan experimentar.

Ventajosamente, esta tecnología es compatible con una unidad del dispositivo de almacenamiento de medios fabricada con posterioridad a 1982. Además, el UCM 1200 es compatible con dispositivos de almacenamiento de medios que tienen un bit indicador de copyright dispuesto sobre el mismo. El bit indicador de copyright ha sido incluido en todos los CDs lanzados desde 1982.

En la presente realización de la figura 14, cada instancia de medios está encriptada en el dispositivo de almacenamiento de medios 999, tal como se describe en la presente memoria con referencia a la figura 13. Sin embargo, la mayoría de los reproductores locales y/o dispositivos de reproducción de medios independientes rara vez incluyen un mecanismo de desencriptado, y para experimentar la música en un equipo doméstico, la música no se encripta convencionalmente. En consecuencia, el dispositivo de almacenamiento de medios 999, en su realización actual, no puede ser operable en un dispositivo de reproducción doméstico y/o independiente.

65 En una realización, el UCM 1200 puede invocar su propio reproductor de propiedad, por ejemplo, el reproductor de medios seguro 1210, tal como se describe con referencia al dispositivo de medios del cliente 310 de la figura 3, lo

que permite un mayor control de las restricciones de copyright y/o acuerdos de licencia aplicables al contenido de los medios. Al invocar un reproductor de medios seguro 1210, el UCM 1200 permite una experiencia de usuario de los contenidos de los medios, protegiéndolo de la presentación de la reproducción no autorizada de los medios dispuestos en el dispositivo de almacenamiento de medios 999.

5 Todavía con referencia a la figura 14, en una realización, el contenido de los medios, por ejemplo, el contenido de los medios 2001-N, y el UCM 1200 dispuesto en un dispositivo de almacenamiento de medios 999 están encriptados, con la excepción del protocolo de ejecución automática 910, tal como se describió anteriormente. En una realización de la presente invención, el UCM 1200 se encripta diferente que el contenido de los medios 2001-N, impidiendo así el pirateado de un encriptado sea utilizado en otro encriptado. Esta aplicación es especialmente ventajoso para las versiones de demostración (demo) de los archivos de medios, versiones beta de prueba, y similares, que pueden ser eliminadas en el dispositivo de almacenamiento de medios 999. Se observa que la presente realización es operable en un entorno en línea, lo que significa que el sistema de ordenador del cliente 210 está acoplado en comunicación con el servidor web 250 y/o el servidor de contenidos 251 para permitir una experiencia de usuario de los contenidos de una versión de demostración del dispositivo de almacenamiento de medios 999. En esta implementación, el UCM 1200 permite reproducciones específicas para usuarios específicos, que pueden ser controlados a través de una red, por ejemplo, la red 1400 de la figura 14, y el servidor 250 y/o 251.

20 En la presente realización, el UCM 1200 puede implementarse para la demostración y/o protección previa a la emisión del contenido dispuesto en un dispositivo de almacenamiento de medios 999. Sin embargo, el contenido dispuesto en el dispositivo de almacenamiento de medios 999 también puede ser contenido lanzado comercialmente, por ejemplo, software de audio, vídeo, y similares. En esta realización, una tecnología de encriptado sofisticada, por ejemplo, Blowfish, se utiliza para encriptar el contenido de los medios 2001-N en el dispositivo de almacenamiento de medios 999 con una clave de desencriptado asociada ubicada en el servidor web 250 y/o el servidor de contenido 251. En una realización, una pluralidad de encriptados se aplican al contenido de los medios 2001-N y una pluralidad de claves de desencriptado se almacenan en el servidor web 250 y/o el servidor de contenido 251. El desencriptado se puede realizar utilizando una clave de desencriptado asociada en conjunción con un reproductor de medios seguro 1210 y el controlador de filtro del sistema de archivos 1220 instalado en el sistema de ordenador 210 a través de dispositivo de almacenamiento de medios 999.

30 Todavía con referencia a la figura 14, el contenido del dispositivo de almacenamiento de medios 999, por ejemplo, el contenido de medios 2001-N se encripta utilizando varios niveles de encriptado para proporcionar niveles de protección en consonancia con los titulares de derechos de autor y la protección requerida deseada. Por ejemplo, el dispositivo de medios de almacenamiento 999 se entrega a un usuario o crítico a efectos de revisión, el usuario inserta un dispositivo de almacenamiento de medios 999 en el lector del dispositivo de almacenamiento adecuado o el conector junto con el equipo del destinatario, y el protocolo de ejecución automática 910 inicia el UCM 1200 de instalación del CCM 300, el controlador de filtro del sistema de archivos 1220, el reproductor de medios seguro 1210 en el sistema cliente 210 de una forma clandestina al usuario. Una vez instalado, el UCM 1200 inicia una sesión de comunicación con el servidor web 250/servidor de contenidos 251, donde el servidor de contenidos 251 puede proporcionar la autorización para que el usuario experimente los medios en el dispositivo de almacenamiento de medios 999.

45 En consecuencia, si el usuario, a quien se le ha liberado la demostración del dispositivo de almacenamiento de medios 999, tenía robado la demostración del dispositivo de almacenamiento de medios 999, o si el usuario ha permitido partes alternativas tratando de experimentar el contenido del dispositivo de almacenamiento de medios 999, la parte no autorizada tendría que intentar para romper las claves de encriptado y el encriptado del contenido real del dispositivo de almacenamiento de medios 999, un consumo no trivial de cantidades de tiempo.

50 Así, el UCM 1200 es capaz de controlar que los destinatarios reciban autorización para experimentar el contenido de los medios en el dispositivo de almacenamiento de medios 999, cuántas veces el destinatario puede experimentar los medios, y el UCM 1200 también puede definir un período de tiempo hasta que el contenido de los medios ya no puede ser accesible. Esto puede permitir a los titulares de derechos de autor liberar el contenido de los medios en un dispositivo de almacenamiento de medios autorizado, por ejemplo, 999, antes de que las copias piratas que inundan el mercado.

55 Todavía con referencia a la figura 14, en consecuencia, un dispositivo de almacenamiento de medios 999 puede estar configurado de tal manera que un primer usuario puede obtener una copia, un segundo usuario puede obtener una copia, y si se sabe que el segundo usuario comparte la demostración con un tercer y un cuarto usuario, a continuación, a los usuarios que se les permite experimentar los medios. Ventajosamente, en virtud de la definición de que los usuarios pueden acceder y experimentar los medios, cualquier intercambio no autorizado de los medios por uno de los usuarios autorizados se puede detectar fácilmente, y además compartir o experimentar que los medios pueden ser detenidos. Además, debido a que el usuario autorizado compartió los medios de forma no autorizada, en un escenario del peor caso, cargos criminales podrían presentarse contra ese usuario.

65 Se hace notar que la colocación del UCM 1200 en un dispositivo de almacenamiento de medios, por ejemplo, 999, para permitir la instalación del CCM 300 en el sistema del cliente 210 es una manera en la que el CCM 300 se

puede instalar en el sistema del cliente 210. Una manera alternativa en la que el CCM 300 se puede instalar en el sistema de ordenador del cliente 210 es a través de "polinización cruzada". Por ejemplo, difusión por Internet de archivos de medios al usuario. El archivo de medios tiene un CCM 300 acoplado con el archivo de medios, y al descargar el archivo de medios en el sistema de ordenador del cliente 210, las realizaciones de la presente invención permiten la instalación del CCM 300 en el sistema de ordenador del cliente 210. En otra forma, el CCM 300 se incorpora y se convierte en parte de un sistema operativo en funcionamiento del sistema del cliente 210. Como alternativa, se aprueban leyes que mandan la inclusión del CCM 300 en cada sistema de ordenador del cliente 210.

La figura 15 es un ejemplo de un diagrama de bloques de la trayectoria lógica/de bits 1500 de un sistema de ordenador del cliente, por ejemplo, 210, configurado con un mecanismo de cumplimiento de uso 1200 para controlar la presentación de contenidos en un dispositivo de almacenamiento de medios 999, de acuerdo con una realización de la presente invención. El mecanismo de cumplimiento de uso 1200 de la figura 15 es análogo al mecanismo de cumplimiento de uso 1200 de la figura 12. Por lo tanto, el CCM 300 del mecanismo de cumplimiento de uso 1200 es análogo a un mecanismo de cumplimiento de los derechos de autor 300 acoplado e instalado en un sistema de ordenador del cliente, por ejemplo, 210, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5a-5d, 6A, 7A- 7C, 8, 9, 10, 11, 14, 15, y 16.

El diagrama 1500 de la figura 15 incluye una unidad del dispositivo de almacenamiento de medios 1112 junto con un controlador del sistema de archivos del dispositivo de almacenamiento de medios 1114 a través de la línea 1571. El controlador del sistema de archivos del dispositivo de almacenamiento de medios 1114 permite que un sistema operativo, por ejemplo Windows de Microsoft, Apple de Apple, Linux de Linux, etc., en un sistema de ordenador del cliente, por ejemplo, el cliente 210, para reconocer y controlar la unidad de dispositivo de almacenamiento de medios, por ejemplo, el controlador 1112. Acoplado al controlador del sistema de archivos del dispositivo de almacenamiento de medios 1114 hay un controlador del filtro del sistema de archivos 1220, a través de la línea 1572. Acoplado al controlador del filtro del sistema de archivos 1220 hay un reproductor de medios seguro 1210 a través de la línea 1573. Acoplado al reproductor de medios seguro 1210 hay un subsistema de medios del sistema operativo 503 a través de la línea 1577 y un dispositivo de salida de hardware de medios 1370 a través de la línea 1574. El UCM 1200 es acoplado con el subsistema de medios del sistema operativo 503 a través de la línea 1576.

La unidad del dispositivo de almacenamiento de medios 1112 de la figura 15 es análoga a la unidad del dispositivo de almacenamiento de medios 1112 de las figuras 11 y 15. La unidad del dispositivo de almacenamiento de medios 1112 está configurada para recibir un dispositivo de almacenamiento de medios 999, donde el dispositivo de almacenamiento de medios 999 es apropiado para la unidad 1112. En una realización, la unidad 1112 puede ser una unidad de CD y, en consecuencia, el dispositivo de almacenamiento de medios 999 sería un CD. En otra realización, la unidad 1112 puede ser una unidad de DVD y en consecuencia, el dispositivo de almacenamiento de medios 999 sería un DVD, y así sucesivamente. Por lo tanto, la unidad del dispositivo de almacenamiento de medios 1112 puede recibir, cuando así se ha configurado, cualquier dispositivo de almacenamiento de medios 999 sobre el cual pueden ser eliminados datos o contenidos.

El controlador del filtro del sistema de archivos 1220 puede ser un filtro de nivel superior y/o de nivel inferior para los dispositivos de bus individuales dentro de sistema de ordenador del cliente 210, por ejemplo, una unidad del dispositivo de almacenamiento de medios 1112, y es análogo al controlador del filtro del sistema de archivos 1220 de la figura 12. El controlador del filtro del sistema de archivos 1220 es capaz de acoplarse al acceso a una unidad del dispositivo de almacenamiento de medios 1112, por ejemplo, una unidad de CD, e intercepta los datos leídos asociados con el acceso al contenido, por ejemplo, el contenido de medios 2001-N, en un dispositivo de almacenamiento de medios, por ejemplo, el dispositivo de almacenamiento de medios 999. El controlador del filtro del sistema de archivos 1220 también está habilitado, a través del descifrador 1221 y una clave de descifrado en los servidores 250 y/o 251, para proporcionar un descifrado dinámico del contenido de medios encriptados en un dispositivo de almacenamiento de medios 999 de los contenidos a los que se accede y son leídos por unidad del dispositivo de almacenamiento de medios 1112.

En virtud del controlador del filtro del sistema de archivos 1220 que funciona a nivel de sistema de archivos en lugar de operar a un nivel de clase de la unidad del dispositivo, por ejemplo, un nivel de clase CD, es capaz de reconocer qué archivos están siendo accedidos desde el dispositivo de almacenamiento de medios 999 para una operación en particular. Ventajosamente, esto obvia la necesidad de implementar un sistema de archivos dentro de un controlador para determinar si los datos que se leen necesitan descifrarse.

Todavía con referencia a la figura 15, el reproductor de medios seguro 1210 es análogo al reproductor de medios seguro 1210 de la figura 11. El reproductor de medios seguro 1210 puede, en una realización, ser un dispositivo de medios personalizado 310 emulado por un controlador del dispositivo de medios personalizado 307, tal como se describe en la presente memoria con referencia a la figura 3. En otra realización, el reproductor de medios seguro 1210 puede ser un reproductor propietario configurado para la utilización con demostración y/o liberación previa del contenido dispuesto en un dispositivo de almacenamiento de medios, por ejemplo, el contenido de medios 2001-N. Otros reproductores de medios autorizados también pueden ser utilizados para presentar contenido de medios en un dispositivo de almacenamiento de medios 999, siempre que los otros reproductores de medios puedan cumplir con

las restricciones de uso y acuerdos de licencia aplicables al contenido de los medios y proporcionados por el reproductor de medios seguro 1210.

5 El dispositivo de salida de hardware de medios 1370 es un dispositivo de salida adecuado para el contenido de medios en el dispositivo de almacenamiento de medios 999. Si el contenido de los medios 2001-N son pistas de audio o canciones, entonces el dispositivo de salida 1370 es una tarjeta de audio o de sonido para la salida de música a través de altavoces. Alternativamente, si el contenido de los medios 2001-N son pistas de vídeo, películas, obras literarias, programas de software, etc., entonces el dispositivo de salida 1370 es una tarjeta gráfica para emitir películas, texto, y similares a través de un dispositivo de visualización, por ejemplo, el dispositivo de visualización
10 105 de la figura 1.

Continuando con la figura 15, un dispositivo de almacenamiento de medios 999 es recibido por una unidad de dispositivo de almacenamiento de medios 1112. Un protocolo de ejecución automática 910 inicia un proceso para determinar la presencia de un mecanismo de cumplimiento 1200 y un reproductor de medios de uso seguro 1210 operable en el sistema de ordenador 210. Si cualquiera y/o los dos del mecanismo de cumplimiento de uso 1200 y el reproductor de medios seguro 1210 no están presentes en el sistema de ordenador 210, el protocolo de ejecución automática inicia la instalación de los componentes, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5a a 5d, 6, 7A a 7C, 8 a 16. Si el UCM 1200 y el reproductor de medios seguro 1210 están presentes, la ejecución automática 910 se aparta de la instalación de los mismos. El controlador de sistema de archivo del dispositivo de almacenamiento de medios 1114 accede al contenido en el dispositivo de almacenamiento de medios, por ejemplo, al contenido de medios 2001-N, y lee los datos.
15
20

El controlador del filtro del sistema de archivos 1220 intercepta la operación de lectura se realiza por el controlador 1114 y dinámicamente descripta un segundo encriptado aplicado al contenido de los medios 2001-N, por ejemplo, los encriptados 2351-2N de la figura 13, a través del descriptador 1221 y una segunda clave de descriptado almacenada en y recuperada desde los servidores 250 y/o 251. En una realización, si el controlador del filtro del sistema de archivos 1220 no está acoplado en comunicación con el servidor 250 y/o 251, lo que permite recuperar la segunda clave de descriptado, no se permite la presentación de los contenidos en un dispositivo de almacenamiento de medios 999.
25
30

Continuando con la figura 15, después de descriptar los segundos encriptados 2351-2N, el contenido de los medios 2001-N, todavía encriptado con un primer encriptado, por ejemplo, el encriptado 1351-N, respectivamente, se envía al reproductor de medios seguro 1210 a través de la línea 1573. El reproductor de medios seguro 1210, en relación con el UCM 1200 se comunica con el servidor 250 y/o 251 y determina si el sistema de ordenador 210 y el usuario del mismo están autorizados para experimentar el contenido de los medios 2001-N. Si el sistema 210 y el usuario del mismo están autorizados a experimentar el contenido de los medios 2001-N, el reproductor de medios seguro 1210 comienza a representar el contenido de los medios para su presentación a través de un dispositivo de salida de hardware de los medios 1370.
35

Al mismo tiempo con la representación del contenido en los medios 2001-N, el reproductor de medios seguro 1210, puede, en una realización, comunicarse con el servidor 250 y/o 251 y recuperar la clave de descriptado asociada a cada encriptado, por ejemplo, 1351-1 N, y con el descriptador 1211 de la figura 12, descriptando de forma dinámica cada instancia de los medios, por ejemplo, 2001-N, ya que el contenido se está representando y se envía a través de la línea 1574 a un dispositivo de salida de hardware de los medios 1370.
40
45

Debido a que el contenido representado es vulnerable a la captura y/o a la formación de imágenes, y convirtiéndose así en objeto de pirateo, quemado, copia, y similares, el reproductor de medios seguro 1210 puede realizar una marca de agua, a través de un marcador de agua 1212, en el flujo de datos de salida que se envía a un dispositivo de salida de hardware de los medios 1370 a través de la línea 1574. En una realización, utilizando el marcador de agua 1212, el flujo de datos saliente se marca mediante con agua junto con la representación realizada por el reproductor de medios seguro 1210. Además, el reproductor de medios seguro 1210 atribuye un identificador único a cada contenido de medios representados 2001-N. En una realización, el número de serie 1380 está unido a cada contenido multimedia 2001-N, ya que se está representando y enviando a un dispositivo de salida de hardware de los medios 1370. De esta manera, si la salida del contenido representado de alguna manera está siendo capturado, fotografiado, etc., en virtud de la asociación con el número de serie 1380 del dispositivo de almacenamiento de medios 999 y el contenido de los medios dispuesto sobre el mismo, por ejemplo, el contenido 2001-N, y el sistema 210 con el que está asociado el destinatario del dispositivo de almacenamiento de medios 999, se evita la presentación no autorizada y la reproducción del contenido de medios.
50
55

La figura 16 es un diagrama de flujo 1600 de las etapas implementadas por ordenador realizadas de acuerdo con una realización de la presente invención para controlar la presentación de contenido de medios dispuestos en un dispositivo de almacenamiento de medios. El diagrama de flujo 1600 incluye procesos de la presente invención, que, en una realización, se llevan a cabo por procesadores y componentes eléctricos bajo el control de instrucciones ejecutables por ordenador y legibles por ordenador. Las instrucciones ejecutables por ordenador y legibles por ordenador residen, por ejemplo, en las funciones de almacenamiento de datos, tales como la memoria volátil utilizable del ordenador 104 y/o la memoria no volátil utilizable del ordenador 103 de la figura 1. Sin embargo, las
60
65

instrucciones ejecutables por ordenador y legibles por ordenador pueden residir en cualquier tipo de medios legibles por ordenador. Aunque las etapas específicas se describen en el diagrama de flujo 1600, estas etapas son de ejemplo. Esto es, la presente invención se adapta bien a la realización de otras etapas o variaciones de las etapas indicadas en la figura 16. Dentro de la presente realización, se debe apreciar que las etapas del diagrama de flujo 5 1600 se pueden realizar mediante software, mediante hardware o mediante cualquier combinación de software y hardware.

Se observa que el diagrama de flujo 1600 se describe en conjunción con las figuras 2, 3, 4, 5a-5d, 6, 7A-7C, 8-15 para describir más completamente el funcionamiento de la presente realización. En la etapa 1610, un mecanismo de ejecución automática dispuesto en un dispositivo de almacenamiento de medios 999, por ejemplo, el protocolo de ejecución automática 910, se activa en respuesta a un sistema de ordenador 210 que recibe el dispositivo de almacenamiento de medios 999 en una unidad de dispositivo apropiado, por ejemplo, la unidad del dispositivo de almacenamiento de medios 1112.

En la etapa 1612 de la figura 16, un programa de monitorización dentro del UCM 1200 dispuesto en el dispositivo de almacenamiento de medios 999 determina si un mecanismo de cumplimiento uso, por ejemplo, el UCM 1200, está instalado en el sistema de ordenador que recibe el dispositivo de almacenamiento de medios 999, por ejemplo, el sistema de ordenador 210. En una realización, los programas de agente 304 pueden realizar la determinación. Sin embargo, en otra realización, pueden ser utilizadas combinaciones de componentes de un CCM 300, tal como se describe aquí con referencia a las figuras 3, 4, 7A-7C.

Si el UCM 1200 no está presente en el sistema de ordenador 210, el presente procedimiento avanza a la etapa 1611. La etapa 1611 instala un mecanismo de cumplimiento del uso del sistema de ordenador 210, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5a-5d, 6, 7A-7C, y 8-15. Alternativamente, si el UCM 1200 está presente en el sistema de ordenador 210, el presente procedimiento avanza a la etapa 1614.

En la etapa 1614, un mecanismo de monitorización dentro del UCM 1200 dispuesto en el dispositivo de almacenamiento de medios 999 determina si un reproductor de medios seguro 1210 está presente y es operable en el sistema de ordenador 210. En una realización, el programa de agente 304 del CCM 300 de la figura 3 puede proporcionar la determinación.

Si un reproductor de medios seguro 1210 no está presente y es operable en el sistema de ordenador 210, el presente procedimiento avanza a la etapa 1611. La etapa 1611 instala un reproductor de medios seguro 1210 en el sistema de ordenador 210, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5a-5d, 6, 7A-7C, y 8-15. Se observa que si el mecanismo de cumplimiento de uso 1200 y/o el reproductor de medios seguro 1210 no puede ser instalado apropiadamente en el sistema de ordenador 210, el presente procedimiento continúa a la etapa 1622, que termina la sesión y que impide que el sistema de ordenador 210 presente el contenido en el dispositivo de almacenamiento de medios 999. Alternativamente, si un reproductor de medios seguro 1210 está presente y es operable en el sistema de ordenador 210, el presente procedimiento avanza a la etapa 1616.

En la etapa 1616, el UCM 1200 se comunica con los servidores 250 y/o 251 en las redes 200, 400, 1000, y/o 1400 y determina si el sistema de ordenador 210 y el usuario del mismo están autorizados para experimentar el contenido de los medios 2001-N en el dispositivo de almacenamiento de medios 999, tal como se describe en la presente memoria con referencia a las figuras 3, 4, las etapas 704-708 de las figuras 7A y 8-15. Si el sistema de ordenador 210 y su usuario no están autorizados para experimentar el contenido en el dispositivo de almacenamiento de medios 999, el presente procedimiento avanza a la etapa 1615. Alternativamente, si el sistema de ordenador 210 y los mismos usuarios están autorizados a experimentar el contenido en el dispositivo de almacenamiento de medios 999, el presente procedimiento avanza a la etapa 1618.

En la etapa 1618 de la figura 16, el UCM 1200 determina si el reproductor de medios seguro 1210, el mecanismo de cumplimiento de uso 1200 y el sistema de ordenador 210 están todos acoplados en comunicación con las redes 200, 400, 1000, y/o 1400. Si una o más de las condiciones no se cumplen, el presente procedimiento continúa a la etapa 1615. Alternativamente, si el reproductor de medios seguro 1210, el mecanismo de cumplimiento de uso 1200, y el sistema de ordenador se acoplan todos en comunicación con las redes 200, 400, 1000, y/o 1400, el presente procedimiento avanza a la etapa 1620.

La etapa 1615 de la figura 16 impide la presentación de contenido en un dispositivo de almacenamiento de medios, por ejemplo, los contenidos de medios 2001-N en el dispositivo de almacenamiento de medios 999, para el usuario del sistema de ordenador 210. Alternativamente, el sistema de ordenador 210 y el usuario del mismo pueden comunicarse con las redes 200, 400, 1000, y/o 1400 e intentan establecer las credenciales y/o volver a establecer un acoplamiento comunicativo con las redes 200, 400, 1000, y/o 1400, que permitiría la presentación del contenido, tal como se describe en la presente memoria con referencia a las figuras 3, 4, y las etapas 704-708 de la figura 7A.

En la etapa 1620, el contenido de los medios 2001-N en el dispositivo de almacenamiento de medios 999 es leído por la unidad del dispositivo de almacenamiento de medios 1112. El controlador de filtro del sistema de archivos 1220 intercepta la operación de lectura que se realiza mediante el controlador del sistema de archivo del dispositivo

almacenamiento de medios 1114 y descrypta dinámicamente un segundo encriptado aplicado al contenido de los medios 2001-N, por ejemplo, el encriptado 2351-2N de la figura 13, a través del descryptador 1221 y una segunda clave de descryptado almacenada en y recuperada de los servidores 250 y/o 251. Se observa que si el controlador de filtro del sistema de archivo 1220 no está acoplado en comunicación con el servidor 250 y/o 251, permitiendo la recuperación de la segunda clave de descryptado, no se permite la presentación del contenido en un dispositivo de almacenamiento de medios 999.

Continuando con la etapa 1620 de la figura 16, con posterioridad al segundo encriptado 2351-2N que descrypta contenido de medios 2001-N, todavía encriptada con un primer encriptado, por ejemplo, el encriptado 1351-1 N, respectivamente, se envía al reproductor de medios seguro 1210. En una realización, el reproductor de medios seguro 1210, en conjunción con el UCM 1200, se comunica con el servidor 250 y/o 251 y comienza a hacer que el contenido de los medios se represente a través de un dispositivo de salida de hardware de medios 1370.

Al mismo tiempo que la representación del contenido de medios 2001-N, el reproductor de medios seguro 1210, puede comunicarse, en una realización, con el servidor 250 y/o 251 y recuperar la clave de descryptado asociada a cada encriptado, por ejemplo, 1351-1 N, y con el descryptador 1211 de la figura 12, descryptando de forma dinámica cada instancia de los medios, por ejemplo, 2001-N, ya que el contenido se está representando y se envía el contenido representado al del dispositivo de salida de hardware de medios 1370.

Debido a que el contenido representado es vulnerable a la captura y/o la formación de imágenes, y convirtiéndose así en objeto de pirateo, quemado, copia, y similares, el reproductor de medios seguro 1210 puede realizar marcas de agua, a través del marcador de agua 1212, en el flujo de datos de salida que se envía a un dispositivo de salida de hardware de medios 1370. En una realización, el flujo de datos saliente está marcado con agua junto con la representación realizada por el reproductor de medios seguro 1210. Además, el reproductor de medios seguro 1210 atribuye un identificador único a cada contenido de medios representado 2001-N. En una realización, el número de serie 1380 está unido a cada contenido de medios 2001-N, ya que se está representando y enviando a un dispositivo de salida de hardware de medios 1370. De esta manera, si la salida del contenido representado de alguna manera está siendo capturado, fotografiado, etc., en virtud de la asociación con el número de serie 1380 del dispositivo de almacenamiento de medios 999 y el contenido de los medios dispuesto sobre el mismo, por ejemplo, el contenido 2001-N, y el sistema de ordenador 210 con el que está asociado el destinatario del dispositivo de almacenamiento de medios 999, se evita la representación no autorizada y la reproducción del contenido de medios.

En otra implementación, las realizaciones de la presente invención pueden ser utilizadas en una topología de red distribuida para el control de distribución de medios entre el sistema de ordenador dentro de la red. Algunas de las topologías de red distribuidas en las que las realizaciones de la presente invención pueden ser utilizadas son, pero no se limitan a, un sistema centralizado, de anillo, jerárquica, y una topología distribuida descentralizada. Una topología de red distribuida descentralizada comúnmente se conoce como red "peer-to-peer" (P2P). En una red P2P, cada sistema de ordenador/nodo de la red es capaz de comunicarse con cualquier otro sistema de ordenador/nodo dentro de la red. Un sistema de ordenador en una red P2P puede solicitar datos de la red, así como proporcionar datos a la red. Por lo tanto, un sistema de ordenador puede ser a la vez un sistema de ordenador solicitante (nodo solicitante) y un sistema de ordenador de origen (nodo de origen) en una red P2P. Además, puede ser un servidor central o una pluralidad de servidores de sistema presentes en la red que se pueden utilizar solos o en combinación unos con otros (por ejemplo, como un nodo administrativo, supemodo, etc.) para proporcionar funcionalidades administrativas a los sistemas de ordenador dentro del mismo y para proporcionar el contenido a la red P2P.

Se sabe que muchas implementaciones de una topología de red distribuida, por ejemplo, una topología descentralizada, no están configuradas para controlar de forma adecuada y/o monitorizar el intercambio o el comercio de los medios entre los sistemas de ordenador en la red P2P. Las realizaciones de la presente invención proporcionan una solución nueva e inventiva para este problema.

La figura 17 es un diagrama de bloques de un entorno de red 1700 para compartir contenido multimedia entre los sistemas de ordenador acoplados en comunicación entre sí, en una realización de la presente invención. La red 1700 incluye un sistema de ordenador del cliente 1705, un sistema de ordenador de origen 1715 y un sistema de ordenador del servidor 1770, que están acoplados en comunicación a través del enlace de comunicación 1710. El enlace de comunicación 1710 puede ser por cable, inalámbrico, o una combinación de las tecnologías de telefonía fija y móvil y protocolos de comunicación que facilitan la interacción entre los sistemas de ordenador. Además, en la presente realización, los sistemas 1705, 1715, y 1770 pueden cada uno aplicarse de una manera similar a la descrita en la presente memoria con referencia a la figura 1. Además, el entorno de red 1700 puede ser implementado de una manera similar, tal como se describe en la presente memoria con referencia a la red 200 de la figura 2 y a la red 800 de la figura 8.

En una realización, el sistema de ordenador del cliente 1705 puede implementarse de una manera similar a un sistema de ordenador del cliente 210, tal como se describe en la presente memoria con referencia a las figuras 2, 4-8, 10, 11, 14, y 15. El sistema de ordenador de origen 1715 puede, en una realización, ser un sistema de ordenador del cliente 1705 que pone a disposición de la red 1700 el contenido de medios que se puede almacenar dentro de la misma. En otra realización, el sistema de ordenador de origen 1705 puede ser un punto de distribución de medios

(MDP) tal como se describe en la presente memoria con referencia a la figura 8, configurado para poner a disposición de la red 1700 el contenido de medios que se puede almacenar dentro de la misma. En virtud de la funcionalidad inherente a una red P2P, el sistema de ordenador de origen 1715 puede ser un sistema de ordenador del cliente 1705 y el sistema de ordenador del cliente 1705 puede ser un sistema de ordenador de origen 1715.

5
10
15
20
25
30
35
40
45
50
55

Todavía con referencia a la figura 17, el sistema de ordenador del servidor 1770 puede, en una realización, aplicarse de una manera similar a un servidor web 250 y/o al contenido del servidor 251, tal como se describe en la presente memoria con referencia a las figuras 2 y 4. Como tal, el sistema de ordenador del servidor 1770 también puede estar acoplado a una base de datos, por ejemplo, la base de datos 451 y/o 451 de la figura 4. En consecuencia, el sistema de ordenador del servidor 1770 puede, en una realización, configurarse para proporcionar funcionalidades de gestión de una red, por ejemplo, de la red 1700 o de la red 800 de la figura 8. Tipos de funcionalidades de gestión que pueden proporcionarse mediante el sistema de ordenador del servidor 1770 pueden incluir, pero no se limitan a, la gestión de la red, la gestión del usuario, el encriptado y la gestión de claves de desencriptado, la gestión de autorización, la gestión de medios, la gestión de transacciones, la gestión de la aplicación de reproducción, y la gestión de la memoria caché. El sistema de ordenador del servidor 1770 también puede implementarse como un sistema de ordenador de origen 1715 y/o como un punto de suministro de medios tal como se describe aquí con referencia a la figura 8.

La gestión de la red puede incluir, pero no se limita a, la determinación de la ruta a través de la cual se transfiere un ejemplo de medios a otro sistema de ordenador en la red 1700. Por ejemplo, y haciendo referencia a la figura 8, un ejemplo de medios se encuentra en una pluralidad de ubicaciones dentro de la red 800, por ejemplo, puntos de entrega de medios 808 (San José), 816 (Tokio), y 812 (Nueva York). El sistema de ordenador del cliente 1705 ubicado en Washington DC solicita esa instancia particular de contenido multimedia. El sistema de ordenador del servidor 1770 es capaz de determinar, para este ejemplo, que la menor cantidad de recursos de red necesarios para transferir el contenido de los medios al sistema de ordenador del cliente solicitante 1705 transferiría la instancia de contenido de medios desde el punto de entrega de medios 812 (Nueva York).

Se anticipa que muchas instancias de una instancia particular de los medios pueden estar dispuestas en toda la red, por ejemplo, la red 1700, en la que no puede ser varios grados de calidad entre el contenido de las instancias de los medios. Además, se sabe que los diferentes sistemas de ordenador de origen 1715 puede tener diferentes tasas de transferencia, por ejemplo, un sistema de ordenador de origen 1715 se puede acoplar a la red 1700 a través de una línea de abonado digital (DSL), mientras que otro sistema de ordenador de origen 1715 se puede acoplar a la red 1700 a través de un módem de 56K, que es sustancialmente más lento que una conexión DSL. Además, las rutas de transferencia que irían a través de una conexión de red que puede estar experimentando dificultades técnicas o tiempos de inactividad pueden desviarse. Ventajosamente, el sistema de ordenador del servidor 1770 puede incorporar la calidad del contenido de los medios, la salud de la conexión, y/o información de la velocidad de entrega en su determinación de qué sistema de ordenador de origen 1715 se va a entregar la instancia de medios.

Todavía con referencia a la figura 17, la gestión de usuarios, en una realización, puede incluir, pero no se limita a, mantener y verificar la información del usuario actual, por ejemplo, el nombre del usuario, la contraseña, la dirección de facturación, un número válido de tarjeta de crédito, pago en línea válido o servicios de pago electrónicos alternativos, dirección MAC, etc., tal como se describe en la presente memoria con referencia a las figuras 3 y 4, y las etapas 704 a 710 de las figuras 7A - 7C.

En una realización, la gestión de las claves de encriptado y desencriptado incluye, pero no se limita a, almacenar una clave de encriptado asociada con un sistema de ordenador de cliente para su uso mediante el sistema de ordenador del cliente para encriptar el mismo contenido de medios en un encriptado local para ese sistema de ordenador del cliente, gestionando una pluralidad de claves de encriptado y de desencriptado intermedias para su utilización con contenidos de medios que se transmiten a un sistema de ordenador del cliente, etc.

En una realización, la gestión de la autorización puede incluir la verificación de que un sistema de ordenador del cliente 1705 está autorizado para conectarse a la red 1700, estando asociado así con la red. Alternativamente, la gestión de la autorización también puede incluir, pero no está limitado a, autorizar/prohibir el intercambio de una instancia de medios con la red 1700 que cumple/no cumple con las restricciones de derechos de autor o acuerdos de licencia aplicables al caso particular de los medios.

Todavía con referencia a la figura 17, la gestión de los medios puede incluir, pero no se limita a, el almacenamiento de una lista de instancias disponibles de contenido de medios y su ubicación asociada dentro de la red 1700, almacenando información relacionada con cada instancia de medios, por ejemplo, título, artista, género, longitud/duración de los contenidos de los medios, información de configuración de bits relacionada con una instancia particular de los medios para la identificación, el almacenamiento de información respecto a los derechos (en su caso) que pueden aplicarse a una instancia de contenidos de los medios cada vez que se transmiten dentro de la red, almacenando información para permitir la expiración del contenido de medios en un sistema de ordenador, cuando el sistema de ordenador ya no tiene autorización para acceder y/o ya no está asociado con la red 1700, y similares.

- Además, la gestión de los medios también puede incluir la utilización de un filtro de Ethernet y otros mecanismos para obtener información relacionada a las instancias de los medios transmitidas y/o recibidas, las instancias de los medios que han entrado recientemente en la red, y similares. En una realización, un filtro de Ethernet puede ser acoplado a un dispositivo de interfaz de red (por ejemplo, módem, NIC, receptor inalámbrico, etc.) acoplado al sistema de ordenador que recibe la instancia del contenido de medios, por ejemplo, el dispositivo de señal 104 acoplado al sistema de ordenador 100 de la figura 1. La información obtenida por un filtro de Ethernet se puede utilizar en la identificación de una instancia particular de los medios, determinando los derechos correspondientes, etc.
- En una realización, la gestión de la transacción puede incluir la generación de una transacción para cada transferencia exitosa del contenido de los medios desde un sistema de ordenador a otro sistema de ordenador en la red, por ejemplo, desde el sistema de ordenador de origen 1715 al sistema de ordenador del cliente 1705 en la red 1700. En una realización, el sistema de ordenador del cliente 1705 que recibe acusa recibo exitoso del contenido de medios y, en consecuencia, el sistema de ordenador del servidor 1770 genera una transacción aplicable al sistema de ordenador que recibe y que está asociado con esa instancia particular de los medios. Debido a que las diferentes instancias de contenido de los medios pueden tener diferentes tarifas de uso y/o derechos asociadas con las mismas, las realizaciones de la presente invención proporcionan los mecanismos para tener en cuenta en cada transmisión, generar una transacción para cada transmisión, y generar un pago por parte del destinatario de la instancia de medios y, en una realización, ofrecer una remuneración adecuada al titular del derecho de autor del contenido de medios.
- Ventajosamente, una transacción de derechos también se puede aplicar a una instancia con copyright de los medios donde antes no era posible el pago de derechos. Por ejemplo, supongamos que una copia pirata de una actuación en directo de un artista ha sido libremente disponible desde hace años. Esta copia pirata puede haber sido hecha a partir de un grabador portátil en una actuación en vivo y se usó para registrar la actuación. En este ejemplo, una persona adquiere una copia pirata analógica y la convierte a un formato digital o adquiere un formato digital de la copia pirata. La copia digital está entonces disponible en la red 1700 para el intercambio entre el sistema de ordenador acoplado a la misma. Cabe señalar que cuando una instancia de medios entra en la red 1700, se convierte en protegida tal como se describe en la presente memoria con referencia a las figuras 3, 4-9, 11, 12, y 15.
- En consecuencia, cuando un sistema de ordenador cliente 1705 recibe correctamente la copia digital, se genera una transacción, invocando así a un pago de derechos cuando este pago de derechos no era posible anteriormente. Ventajosamente, esto puede proporcionar unos medios para distribuir las remuneraciones correspondientes a los titulares de los derechos de autor y licencias, que de otra manera no recibirían ningún pago.
- Continuando, cuando una instancia de medios puede ser distribuida libremente, una transacción se sigue generando. Esto proporciona ventajosamente un registro de los números de solicitudes de una instancia particular de los medios, la ubicación desde donde se originaron esas solicitudes y similares, proporcionando así datos que pueden ser utilizados en estudios de mercado e implementando estrategias de marketing, etc.
- Se observa particularmente que en una implementación alternativa, las realizaciones de la presente invención pueden configurarse fácilmente para proporcionar un mecanismo que puede generar una transacción de impuestos de venta/uso relacionada con la transferencia de una instancia de medios. Las realizaciones de la presente invención pueden configurarse fácilmente para calcular las cantidades apropiadas de impuestos relativos a ventas/usos en la ubicación del sistema de ordenador del cliente receptor. Ventajosamente, esto permitiría a las municipalidades, condados, estados y otras agencias gubernamentales aumentar los ingresos, con lo que, posiblemente, se realizaría una reducción de un déficit asociado a un gobierno. Se prevé que la generación de transacciones fiscales de ventas/usos podría proporcionar de decenas a cientos de millones de dólares de ingresos sin explotar a esos organismos gubernamentales.
- Todavía con referencia a la figura 17, la gestión del reproductor, en una realización, puede incluir, pero no se limita a, mantener la integridad de la aplicación de reproducción segura, la adición de aplicaciones de reproducción adicionales a una lista de aplicaciones de reproducción de aprobadas, la eliminación de aplicaciones de reproducción que no cumplen con los requisitos de restricción de uso aplicables a un archivo multimedia, la modificación de una aplicación de reproducción segura para mejorar su funcionalidad, la modificación para contrarrestar los nefastos intentos de pirateo, la deshabilitación de la aplicación de reproducción segura cuando el sistema de ordenador en el que es operable ya no está autorizado a participar o a asociarse con la red 1700, etc.
- La gestión de la memoria caché, en una realización, puede incluir, pero no se limita a, el mantenimiento del archivo contenedor de los medios protegidos, su modificación para mejorar la funcionalidad o para contrarrestar las actividades nefastas detectadas, deshabilitar el archivo contenedor de medios protegido cuando el sistema de ordenador en el que está dispuesto el archivo contenedor de los medios protegidos no está autorizado a acceder y/o ya no está asociado con la red 1700.
- En la presente realización, el sistema de ordenador del cliente 1705 y el sistema de ordenador de origen 1715 tienen cada uno una instancia de un mecanismo de cumplimiento uso (UCM) 1800 acoplado con el mismo. En la presente

realización, UCM 1800 de la figura 17 y tal como se describe en detalle en la figura 18, es similar a un mecanismo de cumplimiento de derechos de autor 300 y/o el uso de un mecanismo de cumplimiento 900 y/o 1200, tal como se describe en la presente memoria con referencia a las figuras 3, 4, 5A-5D, 6A, y/o 9, 11, 12, y 15, respectivamente.

5 La figura 18 es un diagrama de bloques de los componentes en un mecanismo de cumplimiento de uso (UCM) 1800 que está configurado para ser instalado y funcionar en un sistema de ordenador del cliente 1705 y/o un sistema de ordenador de origen 1715 de las figuras 17 y 19, en una realización de la presente invención. En la presente realización, el UCM 1800 incluye un mecanismo de cumplimiento de los derechos de autor 300 análogo a un mecanismo de cumplimiento de los derechos de autor 300 tal como se describe en la presente memoria con
10 referencia a las figuras 3, 4, 5a-5d y 6A. Se observa que el UCM 1800 también incluye aquellas características y aquellos componentes que se proporcionan en un UCM 900 y un UCM 1200 tal como se describe en la presente memoria con referencia a las figuras 9, 11, 12, y 15, respectivamente.

En la presente realización, el UCM 1800 también incluye una aplicación de reproducción segura 1810, una
15 aplicación de comunicación del cliente 1820, y un creador contenedor de almacenamiento de medios 1830. El creador contenedor de almacenamiento de medios 1830 está configurado para asignar una parte de una unidad de memoria acoplada al sistema de ordenador en el que está instalado el UCM 1800, por ejemplo, la memoria volátil 102 y/o la memoria no volátil 103 del sistema de ordenador 100 de la figura 2. El creador contenedor de almacenamiento de medios 1830 utiliza la porción asignada de una unidad de memoria y crea un archivo contenedor de medios protegido (por ejemplo, un sistema de archivo personalizado) en el que se almacenan instancias de
20 medios que se reciben y/o están disponibles, por ejemplo, archivos de audio, archivos de vídeo, archivos multimedia, documentos, software, y similares. Se hace notar que en una realización, el contenido multimedia que se almacena en un archivo contenedor de medios protegidos se encripta, además de otros encriptados aplicables a la instancia de los medios locales, en el sistema de ordenador en el que está dispuesto el archivo contenedor de medios protegidos. En un ejemplo, una instancia de los medios 9090 se almacena en el sistema de ordenador del cliente 1705 y en el sistema de ordenador de origen 1715 de la figura 17. En consecuencia, el contenido de los medios 9090 es el único sistema de encriptado local 1705 y es el único sistema de encriptado local 1715. Además, en el contexto de la presente invención, el término dispuesto y/o disponible se refiere a la puesta a disposición en una red, por ejemplo, la red 1700, de una instancia de medios que pueden almacenarse en un archivo contenedor de medios
30 protegidos.

Todavía con referencia a la figura 18, el UCM 1800 también incluye, en una realización, una aplicación de comunicación del cliente 1820. La aplicación de comunicación del cliente es una aplicación de comunicación del cliente personalizada configurada para proporcionar la funcionalidad de comunicación entre los nodos en una red descentralizada distribuida, por ejemplo, la red 1700. Alternativamente, la aplicación de comunicación del cliente 1820 es también muy adecuada para aplicarse en casi cualquier red, incluyendo, pero no limitado a, la red 1700. La aplicación de comunicación del cliente 1820 puede ser una aplicación de comunicación bien conocida y fácilmente disponible, y que puede estar escrita en un lenguaje de programación utilizado comúnmente, incluyendo, pero sin limitarse a, C, C++, Java, Fortran, etc.
40

En una realización, la aplicación de comunicación del cliente 1820 está configurada para desencriptar el contenido de medios desde un encriptado local a un sistema de ordenador en el que la aplicación 1820 es operable. La aplicación de comunicación del cliente 1820 también está configurada para encriptar el contenido multimedia en un encriptado intermedio para transferir el contenido de medios a otro sistema de ordenador acoplado en comunicación con una red, por ejemplo, la red 1700. La aplicación 1820 está además configurada para desencriptar el contenido de los medios que se reciben en un encriptado intermedio de un sistema de ordenador acoplado con la red 1700. La aplicación de comunicación del cliente 1820 está configurada además para encriptar el contenido de los medios en un encriptado local al sistema de ordenador en el que la aplicación 1820 es operable.
45

En una realización, la aplicación de comunicación del cliente 1820 puede utilizar una clave de encriptado intermedio proporcionado por un sistema de ordenador del servidor, por ejemplo, el servidor 1770 de la figura 17, para encriptar el contenido de los medios en el encriptado intermedio para su transferencia. La aplicación 1820 también puede utilizar una clave de desencriptado intermedia, también proporcionada por el servidor 1770, para desencriptar el contenido de los medios que se reciben en un encriptado intermedio de un sistema de ordenador acoplado con la
50 red 1700.
55

En una realización, la aplicación de comunicación del cliente 1820 puede transmitir una señal de reconocimiento o indicadora que indica que el contenido multimedia recibido desde otro sistema de ordenador en la red 1700 se ha recibido correctamente. En una realización, una señal de confirmación recibida por el ordenador servidor 1770 puede generar una transacción aplicable al sistema de ordenador que recibe el contenido de los medios y que está asociado con el contenido de los medios que se recibieron.
60

Todavía con referencia a la figura 18, el UCM 1800 también incluye una aplicación de reproducción segura 1810 configurada para acceder al contenido de un archivo contenedor de medios protegidos, por ejemplo, una instancia de medios, y también está configurado para proporcionar la presentación del contenido de medios al sistema de ordenador en el que el contenido multimedia está almacenado. La aplicación de reproducción segura 1810 está
65

además configurada para utilizar su acceso al archivo contenedor de medios protegidos y poner su contenido a disposición de la red. En una realización, la aplicación de reproducción segura 1810 puede presentar el contenido multimedia para el sistema de ordenador en el que es operable, mientras que el sistema de ordenador no esté fuera de línea, por ejemplo, no acoplado con la red 1700, pero todavía asociado con la misma.

5 La aplicación de reproducción segura 1810 puede ser específica para el tipo de medios, lo que significa que puede haber una aplicación de reproducción de audio segura para archivos de audio, una aplicación de reproducción de vídeo segura para archivos de vídeo, una aplicación alfanumérica segura para archivos de texto, una aplicación de software de reproducción segura para archivos de software, y así sucesivamente. Se observa que la aplicación de reproducción segura 1810 se puede configurar para interactuar con casi cualquier tipo de medios.

10 En una realización, la aplicación de reproducción segura 1810 puede ser un dispositivo de medios personalizado 310 que puede ser una emulación de un controlador de un dispositivo de medios personalizado 307 tal como se describe en la presente memoria con referencia a las figuras 3, 4, y a las figuras 5A-5D. En otra realización, la aplicación de reproducción segura 1810 puede ser una aplicación de reproducción aprobada tal como se describe en la presente memoria con referencia a la figura 3.

15 La figura 19 es un sistema de ejemplo 1900 para controlar el intercambio de medios entre varios sistemas de ordenador acoplados en comunicación en una red de acuerdo con una realización de la presente invención.

20 El sistema 1900 incluye un sistema de ordenador del cliente 1705 análogo al sistema de ordenador del cliente 1705 de la figura 17, un sistema de ordenador del servidor 1770 análogo al sistema de ordenador del servidor 1770 de la figura 17, y un sistema de ordenador de origen 1715 análogo al sistema de ordenador de origen 1715 de la figura 17. Los sistemas 1705, 1715 y 1770 se implementan y se acoplan en comunicación con una red 1700 en una realización de la presente invención. En una realización, la red 1700 es una red distribuida descentralizada, por ejemplo, la red 800 de la figura 8.

25 En una implementación, el sistema de ordenador de origen 1715 y el sistema de ordenador cliente 1705 se han conectado a la red 1700, tal como se describe en la presente memoria con referencia a la figura 4, y las etapas 702 y 716 de la figura 7A. El sistema de ordenador del cliente 1705 solicita una instancia de medios desde la red 1700, por ejemplo, la instancia de medios 4321, que se muestran como la comunicación 1810. La red 1700 recibe la solicitud y el sistema de ordenador del servidor 1770 determina la ubicación de una instancia de medios 4321. El sistema de ordenador del servidor 1770 responde al sistema de ordenador del cliente 1705 con la ubicación de la instancia de medios 4321, que se muestra como la comunicación 1820.

30 En este ejemplo, el sistema de ordenador del servidor 1770 es consciente de que el sistema de ordenador de origen 1715 tiene una instancia de medios 4321 dispuesta en el mismo. En la presente realización, la instancia de contenidos de medios 4321 se almacena en un archivo contenedor de medios protegidos en una unidad de memoria acoplada al sistema de ordenador de origen 1715. Además, la instancia de los medios 4321 se encripta localmente en el sistema de ordenador de origen 1715, que se muestra como una línea punteada 1716 que abarca los medios 4321.

35 A continuación, el sistema de ordenador de origen 1715 envía una solicitud al sistema de ordenador del servidor 1770 para una clave de encriptado intermedia para encriptar la instancia de medios 4321 para su transferencia al sistema de ordenador del cliente 1705, que se muestra como la comunicación 1830. El sistema de ordenador del servidor 1770 transmite una clave de encriptado intermedia, por ejemplo, la clave 1775, al sistema de ordenador de origen 1715. Tras la recepción de la clave de encriptado intermedia 1775 por el sistema de ordenador de origen 1715, una aplicación de comunicación del cliente 1820 operable en el sistema de ordenador de origen 1715, descripta los medios 4321 de su encriptado local, por ejemplo, el encriptado 1716, y encripta los medios 4321 en un encriptado intermedio, tal como se indica mediante la línea de puntos 1775 que abarca los medios 4321.

40 Haciendo referencia a la figura 19, una vez que la aplicación de comunicación del cliente 1820 del sistema de ordenador de origen 1715 encripta los medios 4321 en el encriptado intermedio 1775, la aplicación de comunicación del cliente 1820 transmite los medios 4321 en el encriptado intermedio 1775 al sistema de ordenador del cliente 1705, que se muestra como la comunicación 1850. Cuando el sistema de ordenador del cliente 1705 recibe los medios 4321 en el encriptado intermedio 1775, el sistema de ordenador del cliente 1705 envía una solicitud al sistema de ordenador del servidor 1770 para una clave de descryptado intermedia, por ejemplo la clave 1776, que se muestra como la comunicación 1860. La clave de descryptado intermedia 1776 permite una aplicación de comunicación del cliente 1820 operable en el sistema de ordenador del cliente 1705 para descryptar los medios 4321 a partir de su encriptado intermedio 1775. Se observa que hasta que el encriptado intermedio 1775 es descryptado, el reproductor seguro 1810 operable en el sistema de ordenador del cliente 1705 no es capaz de presentar medios 4321 al sistema 1705. Además, se observa que si otro sistema de ordenador en la red 1700 se ha interceptado los medios 4321 durante la transferencia, el encriptado intermedio 1775 impide el uso de los medios 4321 mediante la interceptación del sistema de ordenador.

65

Continuando, el sistema de ordenador del servidor 1770 responde a la solicitud del sistema de ordenador del cliente 1705 para una clave de descifrado intermedia y transmite la clave 1776 al sistema de ordenador del cliente 1705, que se muestra como la comunicación 1870. Una vez que la clave 1776 es recibida por el sistema de ordenador del cliente 1705, una aplicación de comunicación del cliente 1830 operable en el sistema 1705 descifra los medios 4321 del cifrado intermedio 1775 y cifra los medios 4321 en un cifrado local al sistema de ordenador del cliente, por ejemplo, el cifrado 1776 que abarca los medios 4321.

Cuando los medios 4321 se ha recibido satisfactoriamente y son cifrados en un cifrado local al sistema de ordenador del cliente 1705, por ejemplo, los medios 4321 con el cifrado 1706, el sistema de ordenador del cliente 1705 transmite un indicador de acuse de recibo que indica la recepción con éxito de los medios 4321, que se muestra como la comunicación 1880. En consecuencia, tras la recepción de un indicador de acuse de recibo, el sistema de ordenador del servidor 1770 genera una transacción aplicable al sistema de ordenador del cliente 1705 y que está asociada con los medios 4321.

Ventajosamente, las realizaciones de la presente invención proporcionan componentes que permiten a los medios controlados compartir en una red descentralizada distribuida (una red P2P), por ejemplo, la red 800 de la figura 8 y/o la red 1700 de la figura 17. Una ventaja adicional es que las realizaciones de la presente invención también pueden hacer un seguimiento de la distribución, generar derechos aplicables a un sistema de ordenador que recibe y se asocian con una instancia particular de los medios. También es ventajoso que las realizaciones de la presente invención permiten que instancias externas de los medios entren en la red y proporcionen el cumplimiento de las restricciones de copyright y acuerdos de licencia asociados a la instancia de medios.

La descripción anterior respecto a realizaciones específicas de la presente invención se ha presentado con fines de ilustración y descripción. No se pretende que sea exhaustiva o limite la invención a las formas precisas descritas, y muchas modificaciones y variaciones son posibles a la luz de las enseñanzas anteriores. Las realizaciones se han elegido y descrito con el fin de explicar mejor los principios de la invención y su aplicación práctica, para permitir así que otros expertos en la técnica utilicen mejor la invención y las diversas realizaciones con diversas modificaciones tal como sean adecuadas para el uso particular contemplado. Se pretende que el alcance de la invención esté definido por las reivindicaciones adjuntas y sus equivalentes.

30

REIVINDICACIONES

1. Procedimiento para controlar la compartición de medios entre una pluralidad de nodos en una red (1700), comprendiendo dicho procedimiento:

5 poner a disposición de dicha red (1700) una instancia de contenido de medios (4321) para compartir entre dicha pluralidad de nodos mediante un nodo de origen (1715) acoplado comunicativamente a dicha red;
 en un nodo servidor (1770) acoplado comunicativamente a dicha red (1700), recibir una solicitud desde un nodo de cliente (1705) acoplado comunicativamente a dicha red (1700) para una instancia de contenido de medios (4321) y responder al nodo de cliente (1705) con la ubicación de dicha instancia de contenido de medios (4321);
 10 en el nodo servidor (1770), recibir una solicitud (1830) desde el nodo de origen (1715) para una clave de encriptado intermedio (1775), y transmitir (1840) la clave de encriptado intermedia (1775) hasta el nodo de origen (1715);
 en dicho nodo de origen (1715), desencriptar dicha instancia de contenido de medios (4321) desde un primer encriptado (1716) local en dicho nodo de origen (1715);
 15 en dicho nodo de origen, encriptar dicha instancia de contenido de medio (4321) en un segundo encriptado intermedio (1775) utilizando dicha clave de encriptado intermedia (1775); y
 transferir dicha instancia de contenido de medios (4321) al nodo de cliente (1705) mientras dicha instancia de contenido de medios (4321) está en dicho encriptado intermedio (1775).
 20

2. Procedimiento según la reivindicación 1, que también comprende:

cuando el nodo de cliente (1705) recibe la instancia de contenido de medios (4321) en el encriptado intermedio (1775) a partir de dicho nodo de origen, el nodo de cliente (1705) envía una solicitud a dicho nodo servidor (1770) para una clave de desencriptado intermedia (1776).
 25

3. Procedimiento según la reivindicación 2, que también comprende
 en el nodo servidor, al recibir la solicitud de dicha clave de desencriptado intermedia (1776), se coloca dicha clave de desencriptado intermedia (1776) en el nodo de cliente (1705); y
 30 en el nodo de cliente (1705), al recibir dicha clave de desencriptado intermedia (1776), desencriptar dicha instancia de contenido de medios (4321) de dicho encriptado intermedio (1775) y encriptar dicha instancia de contenido de medios (4321) en un encriptado local al nodo de cliente (1705).

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que una aplicación de comunicación de cliente (1820) acoplada a dicho nodo de origen (1715) realiza dicho desencriptado y dicho encriptado.
 35

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que una aplicación de reproducción segura (1810) acoplada a dicho nodo de origen (1715) pone dicha instancia de contenido de medios (4321) a disposición de dicha red (1700).
 40

6. Procedimiento según la reivindicación 5, que también comprende:

desactivar dicha aplicación de reproducción segura (1810) cuando dicho nodo de origen (1715) ya no está asociado con dicha red (1700), dicha deshabilitación evitando que dicho nodo de origen (1715) ponga dicha red (1700) a disposición de dicha instancia de contenido de medios (4321).
 45

7. Procedimiento según la reivindicación 5, que también comprende:

evitar que dicho nodo de origen (1715) presente dicha instancia de contenido de medios (4321) cuando dicho nodo de origen (1715) ya no está asociado con dicha red (1700).
 50

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, que también comprende cumplir con una restricción de uso aplicable a dicha instancia de contenido de medios (4321) con un mecanismo de cumplimiento de uso (1800) acoplado a dicho nodo de origen (1715).
 55

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8, que también comprende:

almacenar dicha instancia de contenido de medios (4321) en un archivo contenedor de medios protegidos en una unidad de memoria acoplada a dicho nodo de origen (1715), siendo dicho sistema de archivo personalizado accesible para una aplicación de reproducción segura (1810) acoplada a dicho nodo de origen (1715).
 60

10. Sistema de medios controlados que se comparten entre una pluralidad de nodos en una red (1700), comprendiendo dicho sistema:

un nodo de origen (1715) acoplado comunicativamente con dicha red, comprendiendo dicho nodo de origen medios para poner dicha red (1700) a disposición de un instancia de contenido de medios (4321) para compartir
 65

entre dicha pluralidad de nodos;

un nodo servidor (1770) acoplado comunicativamente con dicha red (1700);

un nodo de cliente (1705) acoplado comunicativamente con dicha red (1700), proporcionándose el nodo de cliente para solicitar un instancia de contenido de medios (4321) desde dicha red (1700);

5 proporcionándose el nodo servidor (1770) para, al recibir dicha solicitud de una instancia de contenido de medios (4321), en respuesta al nodo de cliente (1705) con la ubicación de dicha instancia de contenido de medios (4321);

10 proporcionándose también el nodo servidor (1770) para, tras la recepción de una solicitud (1830) desde el nodo de origen (1715) para una clave de encriptado intermedia (1775), transmitir (1840) la clave de encriptado intermedia (1775) hasta el nodo de origen (1715);
proporcionándose el nodo de origen para:

desencriptar dicha instancia de contenido de medios (4321) desde un primer encriptado (1716) local a dicho nodo de origen (1715);

15 encriptar dicha instancia de contenido de medios (4321) en un segundo encriptado intermedio (1775) usando dicha clave de encriptado intermedio (1775) desde el nodo servidor (1770); y

transferir dicha instancia de contenido de medios (4321) a dicho nodo de cliente (1705) mientras dicha instancia de contenido de medios (4321) está en dicho encriptado intermedio (1775).

20 11. Sistema según la reivindicación 10, en el que:

el nodo de origen (1715) tiene una aplicación de reproducción segura (1810) instalada y operable en el mismo; y una aplicación de comunicación de cliente (1820) está acoplada a dicho nodo de origen (1715) para comunicarse con dicha pluralidad de nodos.

25 12. Sistema según la reivindicación 11, que también comprende:

un archivo contenedor de medios protegido dispuesto sobre una unidad de memoria acoplada a dicho nodo de origen (1715), dicho archivo contenedor de medios protegido para almacenar dicha instancia de contenido de medios (4321).

30 13. Sistema según cualquiera de las reivindicaciones 10 a 12, en el que:

35 el nodo de cliente también se proporciona (1705) al recibir la instancia de contenido de medios (4321) en el encriptado intermedio (1775) desde dicho nodo de origen, para enviar una solicitud a dicho nodo servidor (1770) para una clave de desencriptado intermedia (1776).

14. Sistema según la reivindicación 13, en el que:

40 el nodo servidor (1770) también se proporciona para, al recibir la solicitud de dicha clave de desencriptado intermedia (1776), enviar dicha clave de desencriptado intermedia (1776) al nodo de cliente (1705); y

el nodo de cliente (1705) se proporciona también para, al recibir dicha clave de desencriptado intermedia (1776), desencriptar dicha instancia de contenido de medios (4321) fuera de dicho encriptado intermedio (1775) y encriptar dicha instancia de contenido de medios (4321) en un encriptado local en el nodo de cliente (1705).

45 15. Sistema según la reivindicación 11, en el que dicha aplicación de reproducción segura (1810) está configurada para poner dicha instancia de contenido de medios (4321) disponible en dicho nodo de origen (1715) a dicha red (1700).

50 16. Sistema según la reivindicación 15, en el que dicha aplicación de reproducción segura (1810) deja de estar disponible para evitar que haga uso de dicha instancia de contenido de medios (4321) en dicha red (1700) cuando dicho nodo de origen (1715) ya no está asociado con dicha red (1700).

55 17. Sistema según la reivindicación 15, en el que dicha aplicación de reproducción segura (1810) deja de estar disponible para evitar la presentación de dicho instancia de contenido de medios (4321) en dicho nodo de origen (1715) cuando dicho nodo de origen ya no está asociado con dicha red (1700).

60 18. Sistema según cualquiera de las reivindicaciones 11 a 17, que también comprende: un mecanismo de cumplimiento de uso (1800) acoplado a dicho nodo de origen (1715) para proporcionar el cumplimiento con una restricción de uso aplicable a dicha instancia de contenido de medios (4321).

19. Medio legible por ordenador para almacenar instrucciones implementadas por ordenador, siendo dichas instrucciones para hacer que un sistema de ordenador realice un procedimiento según cualquiera de las reivindicaciones 1 a 9.

65

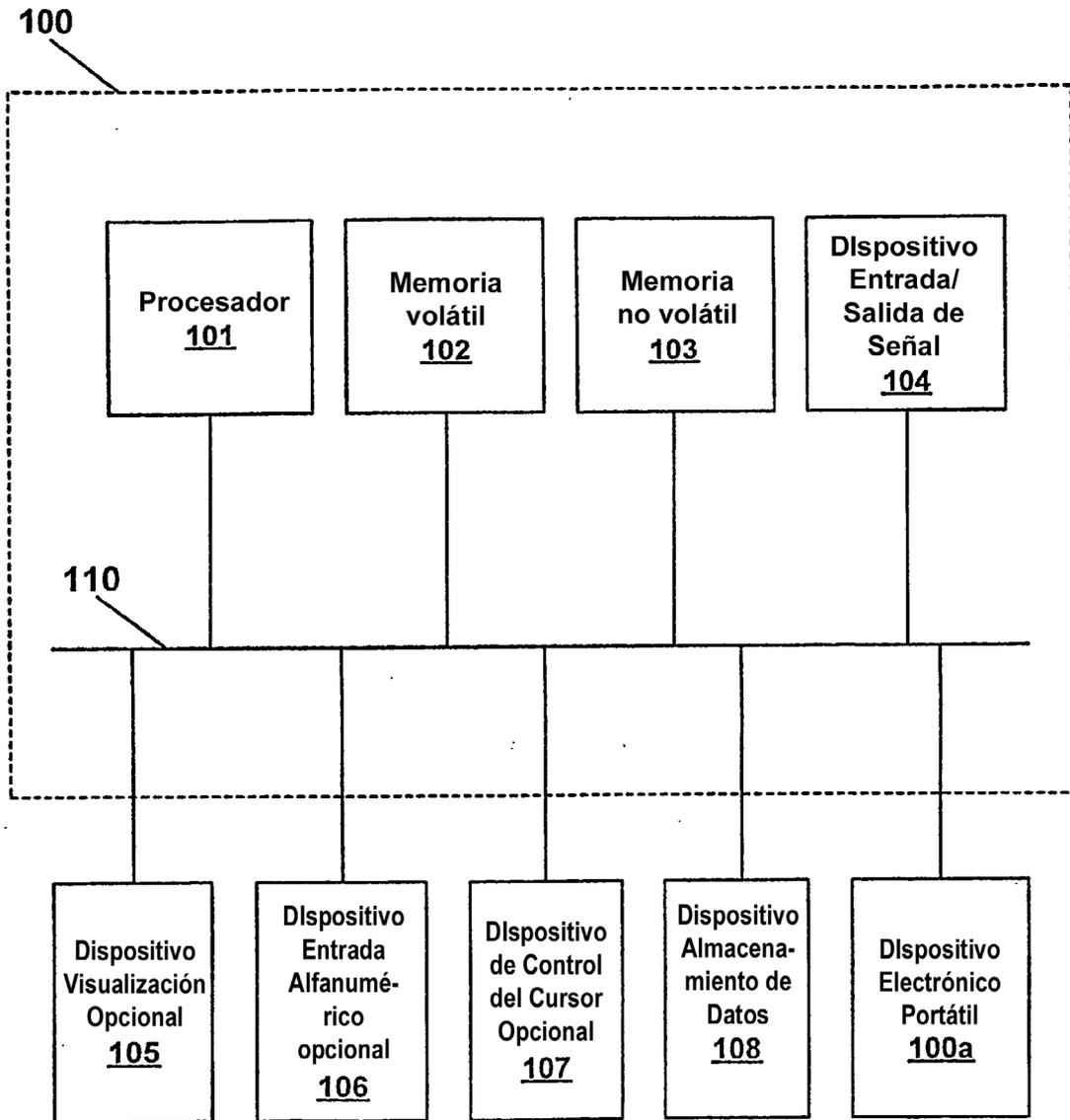


FIG. 1

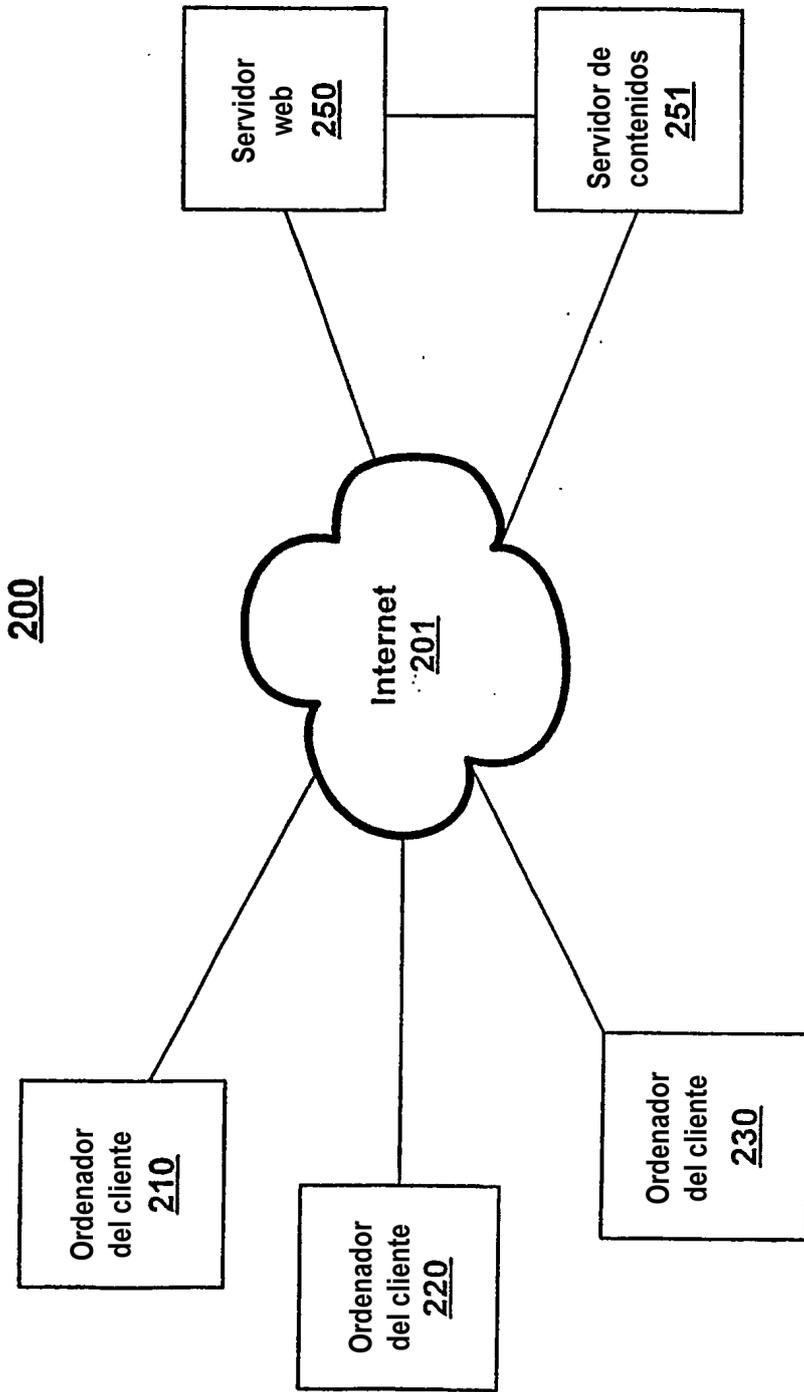


FIG. 2

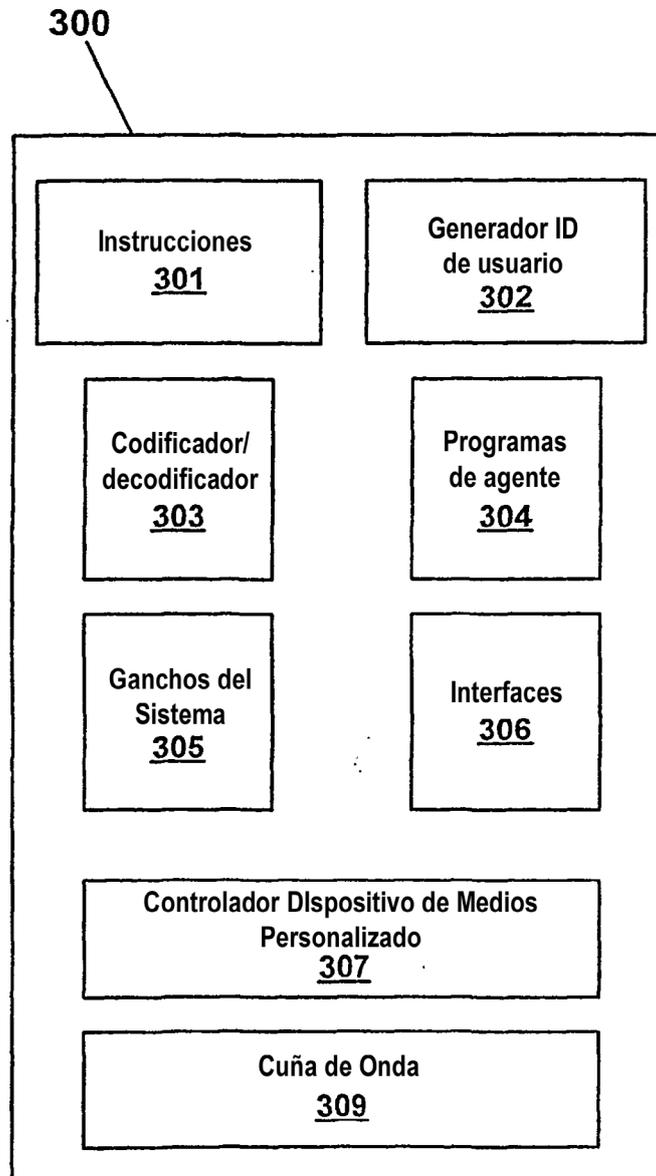


FIG. 3

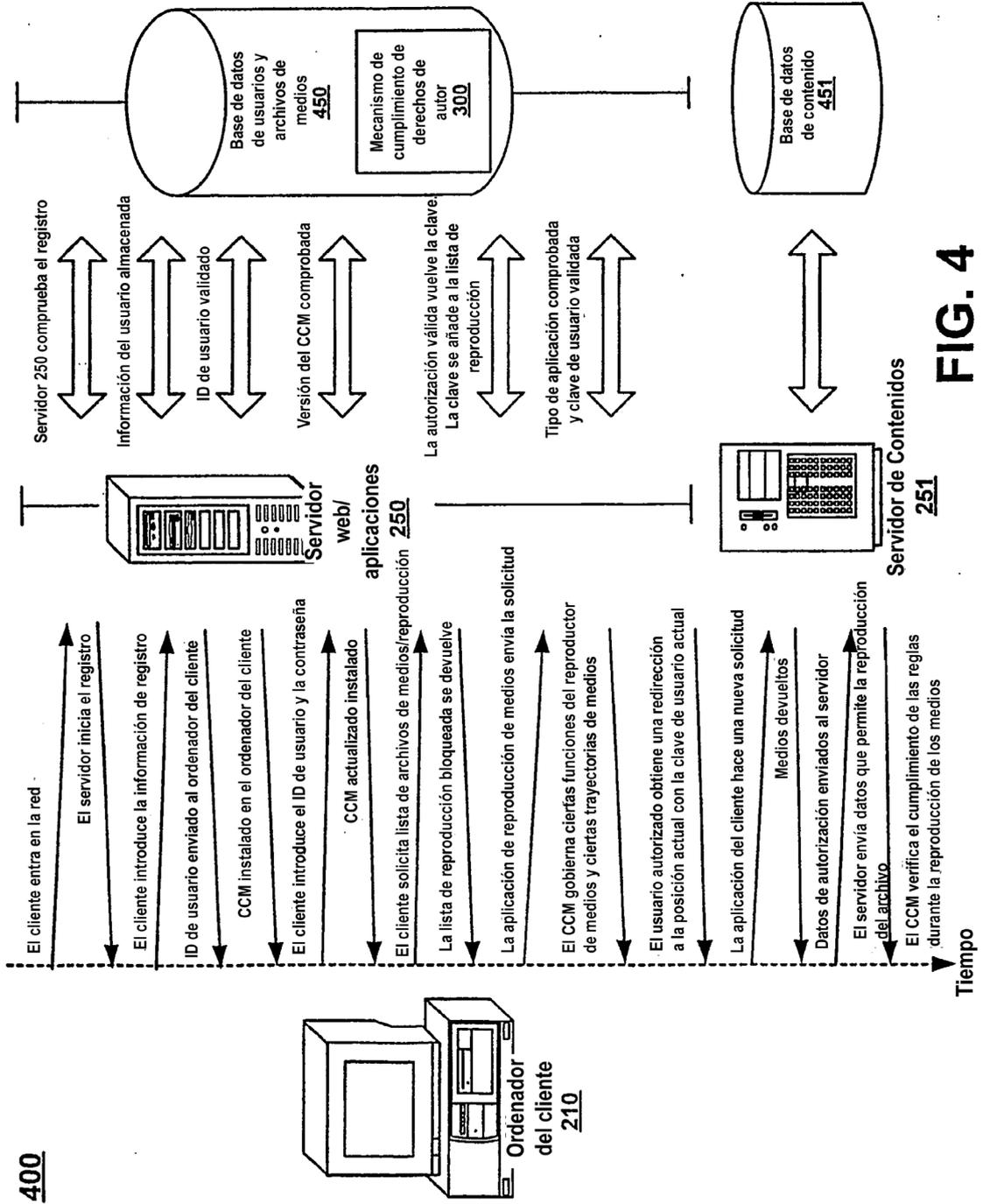


FIG. 4

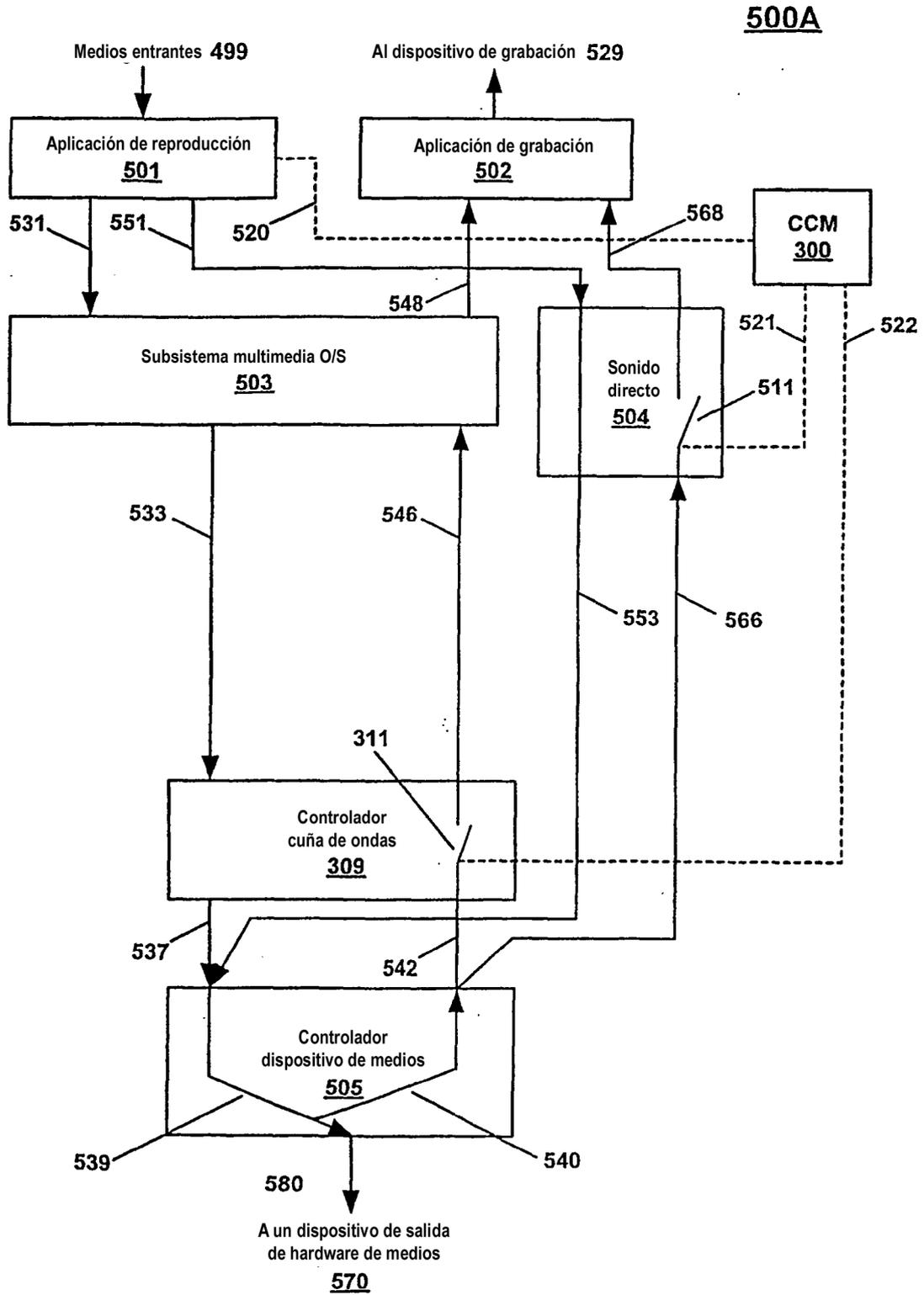


FIG. 5A

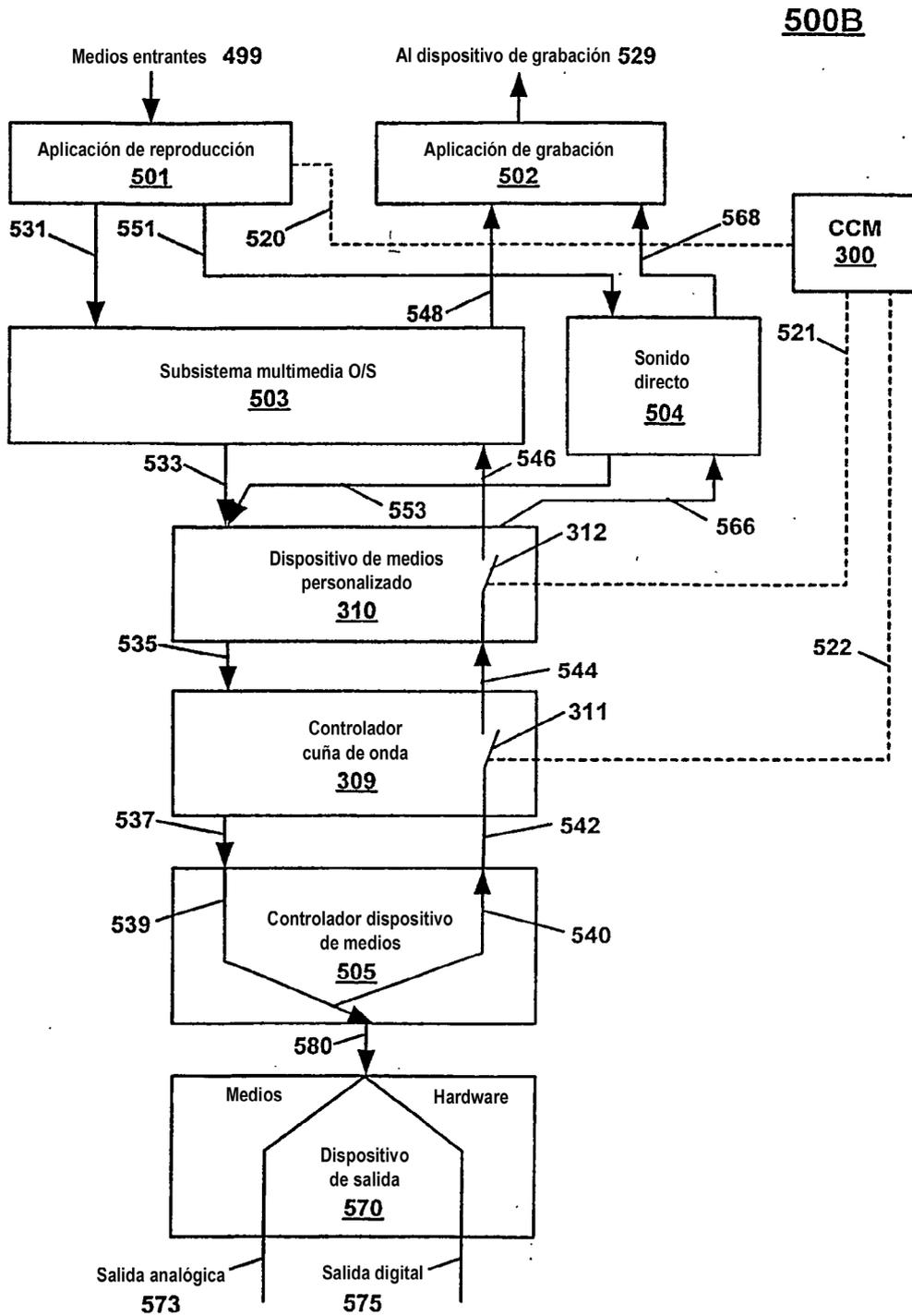


FIG. 5B

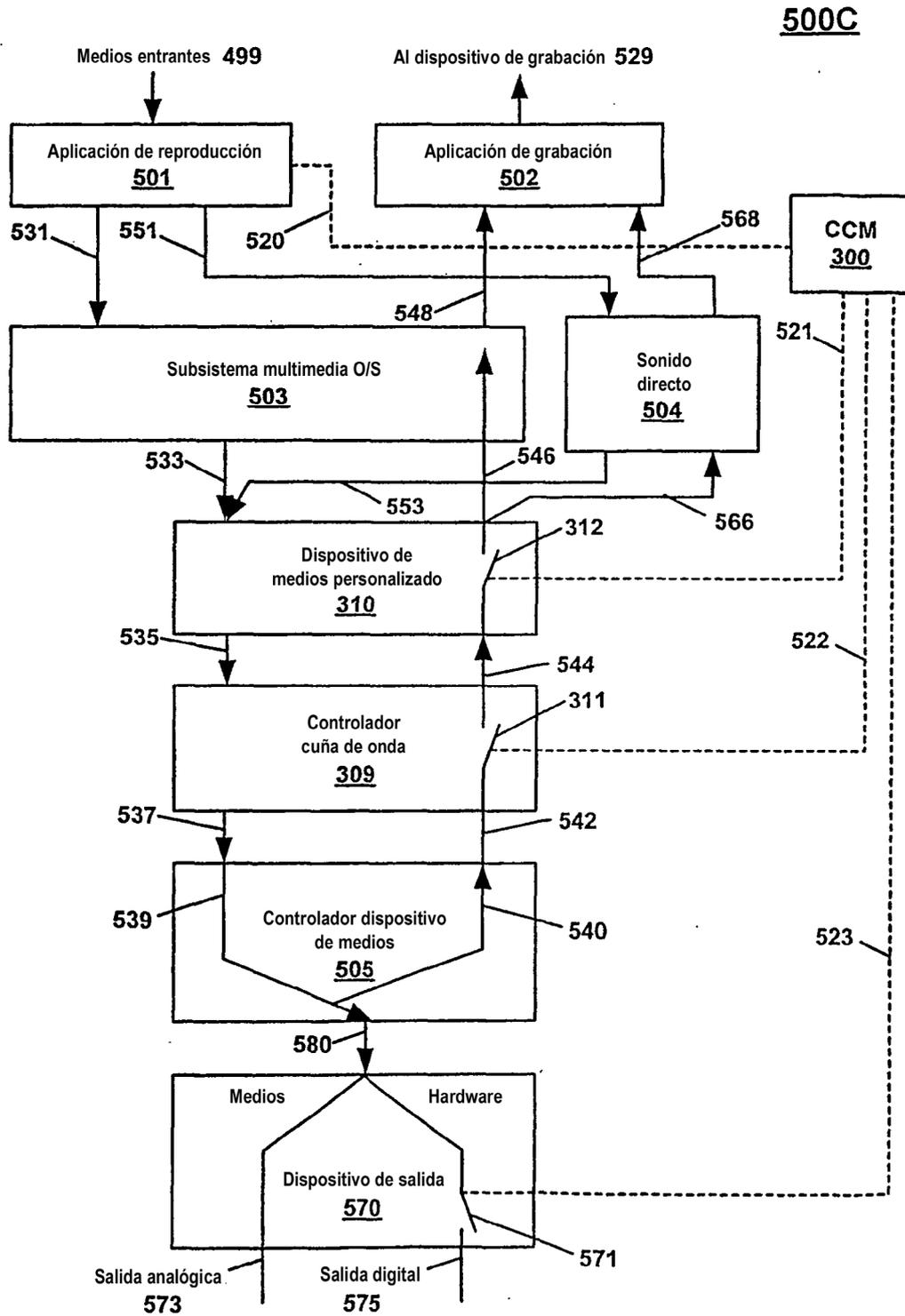


FIG. 5C

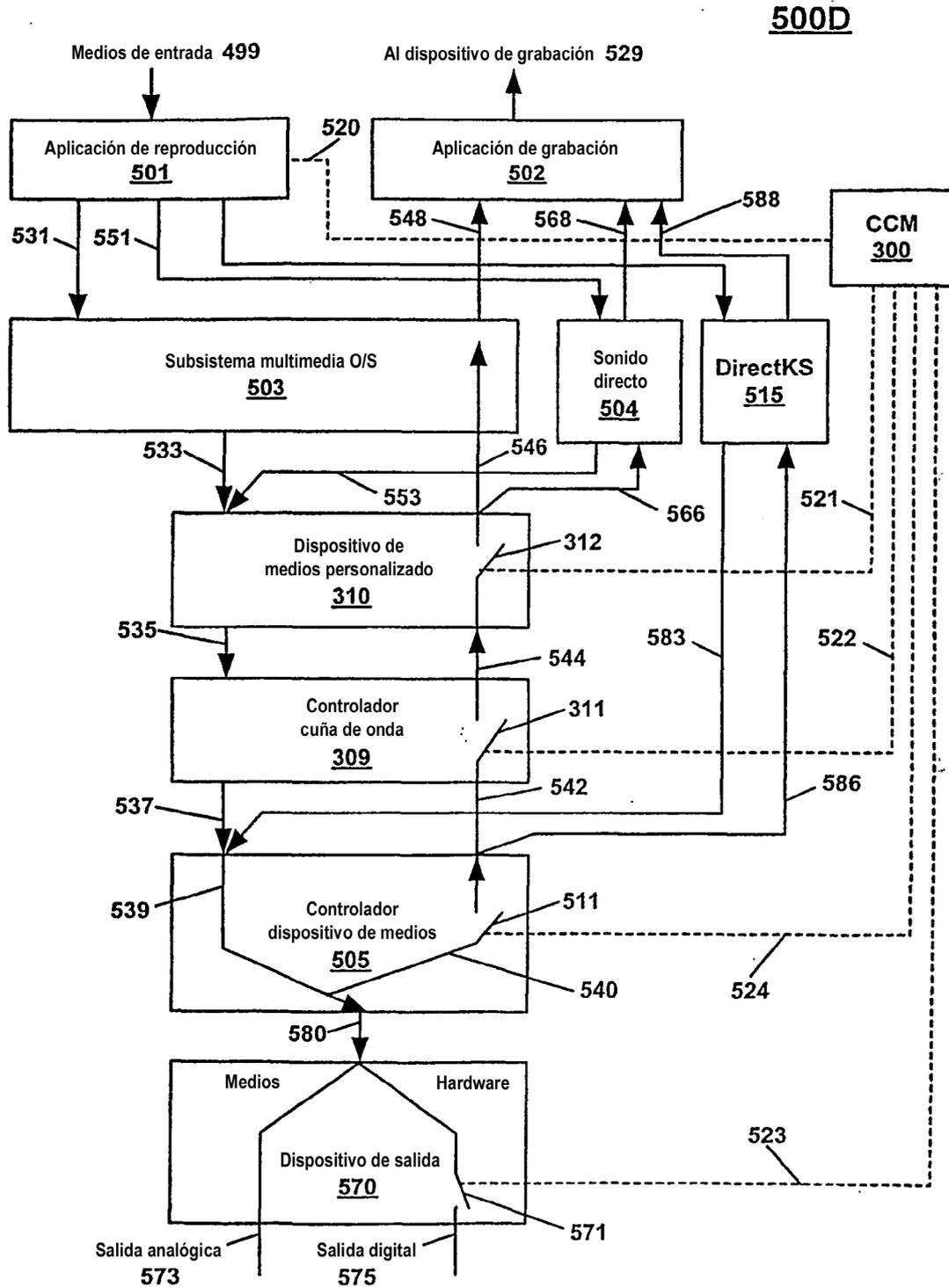


FIG. 5D

600

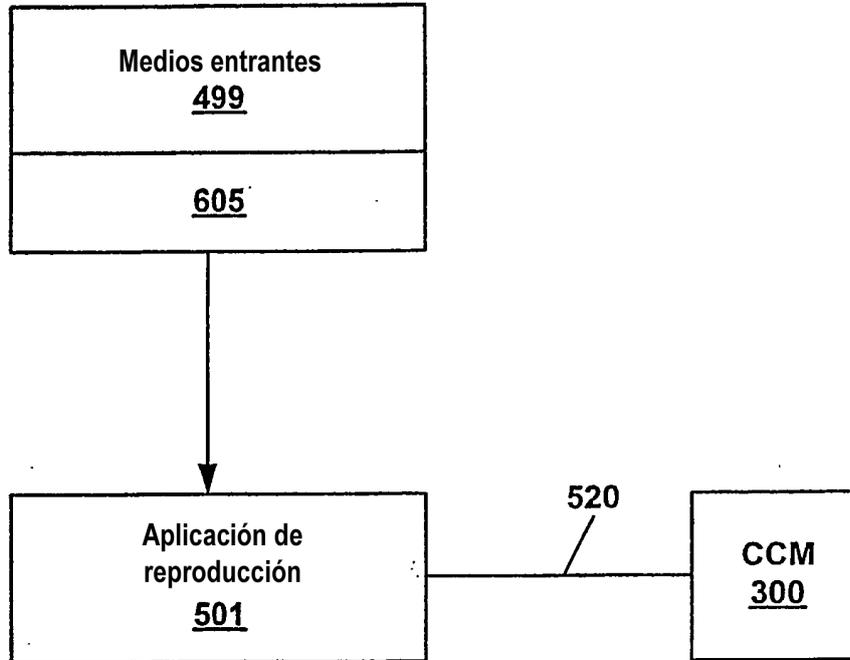


FIG. 6A

700

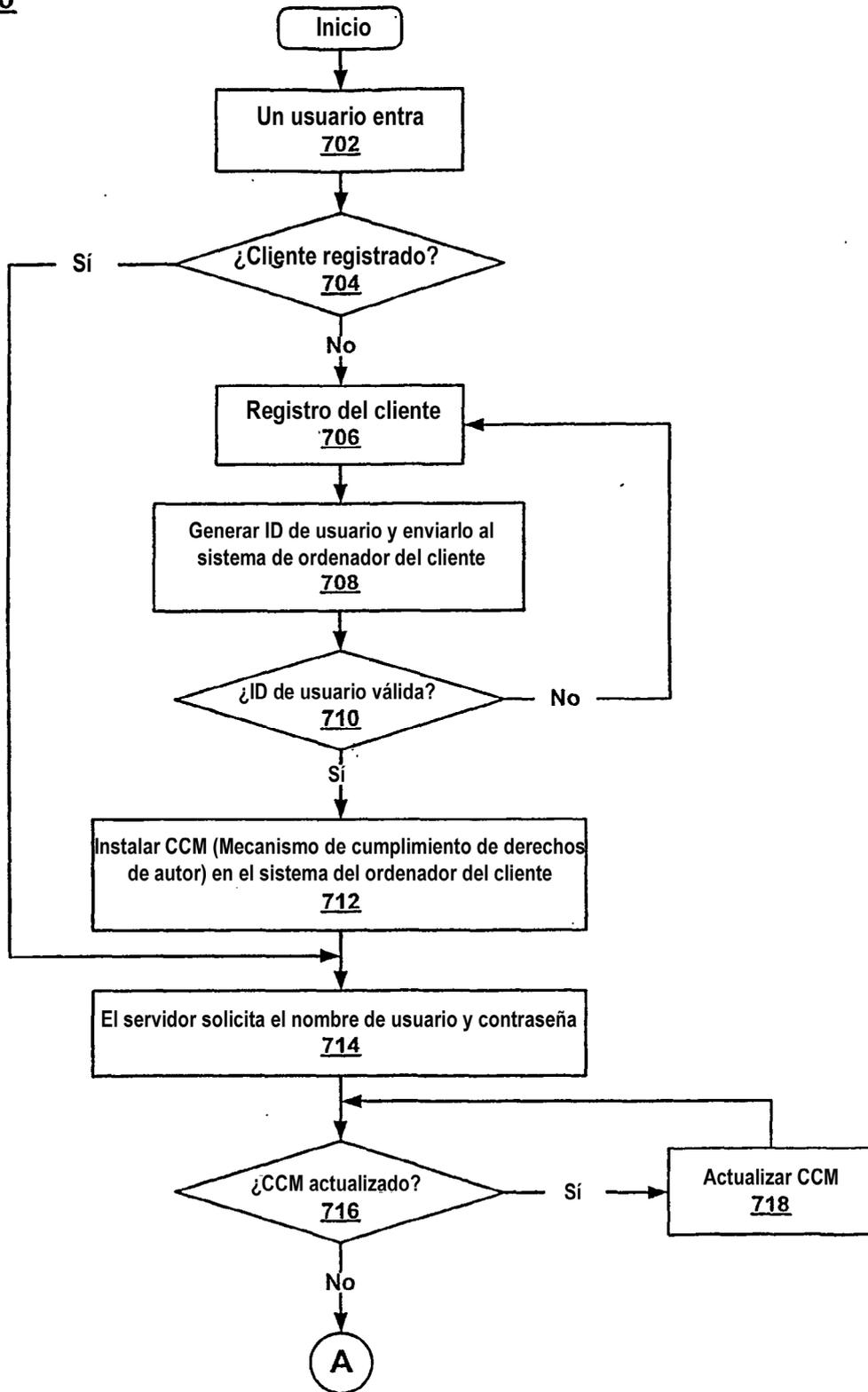


FIG. 7A

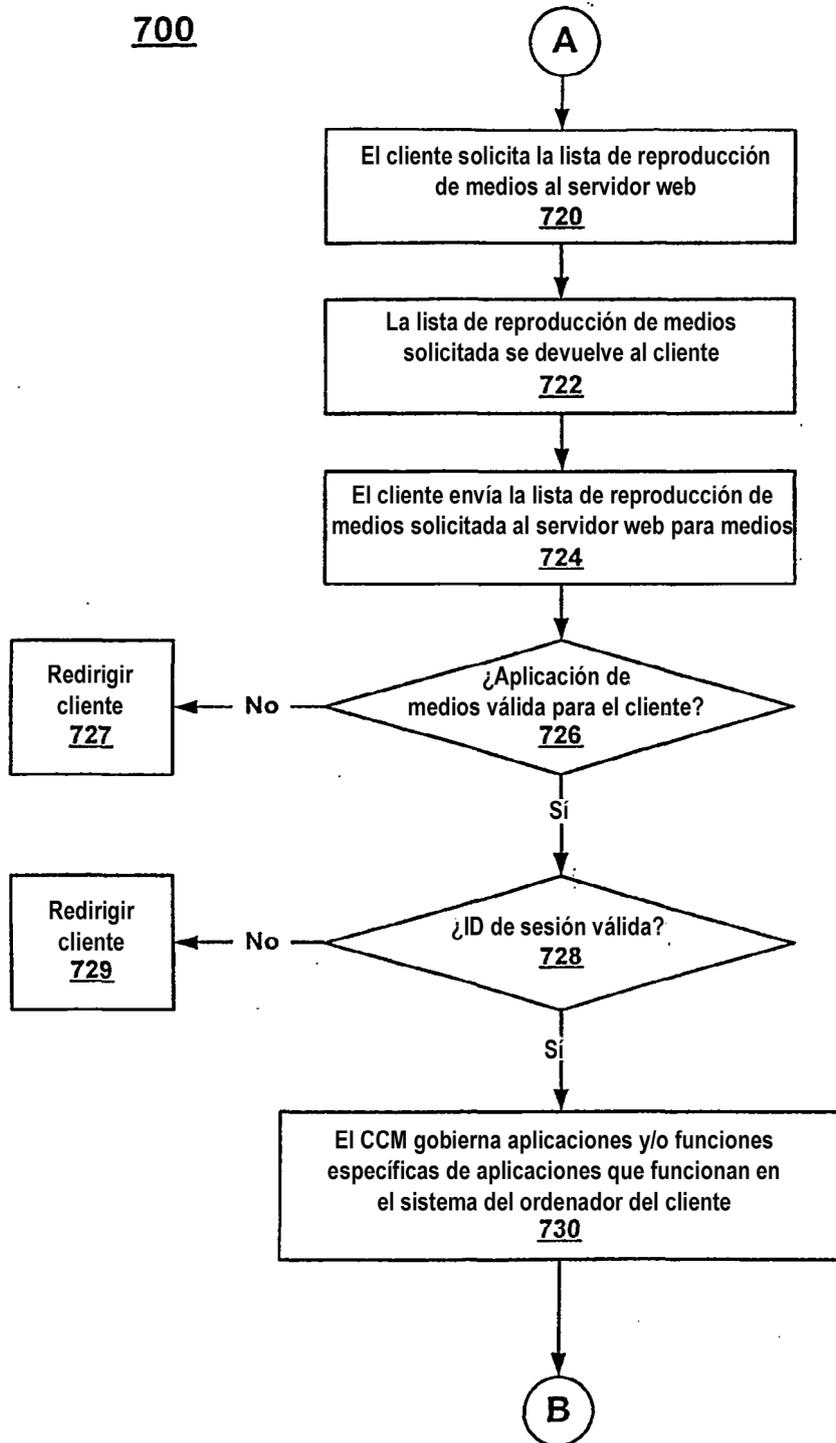


FIG. 7B

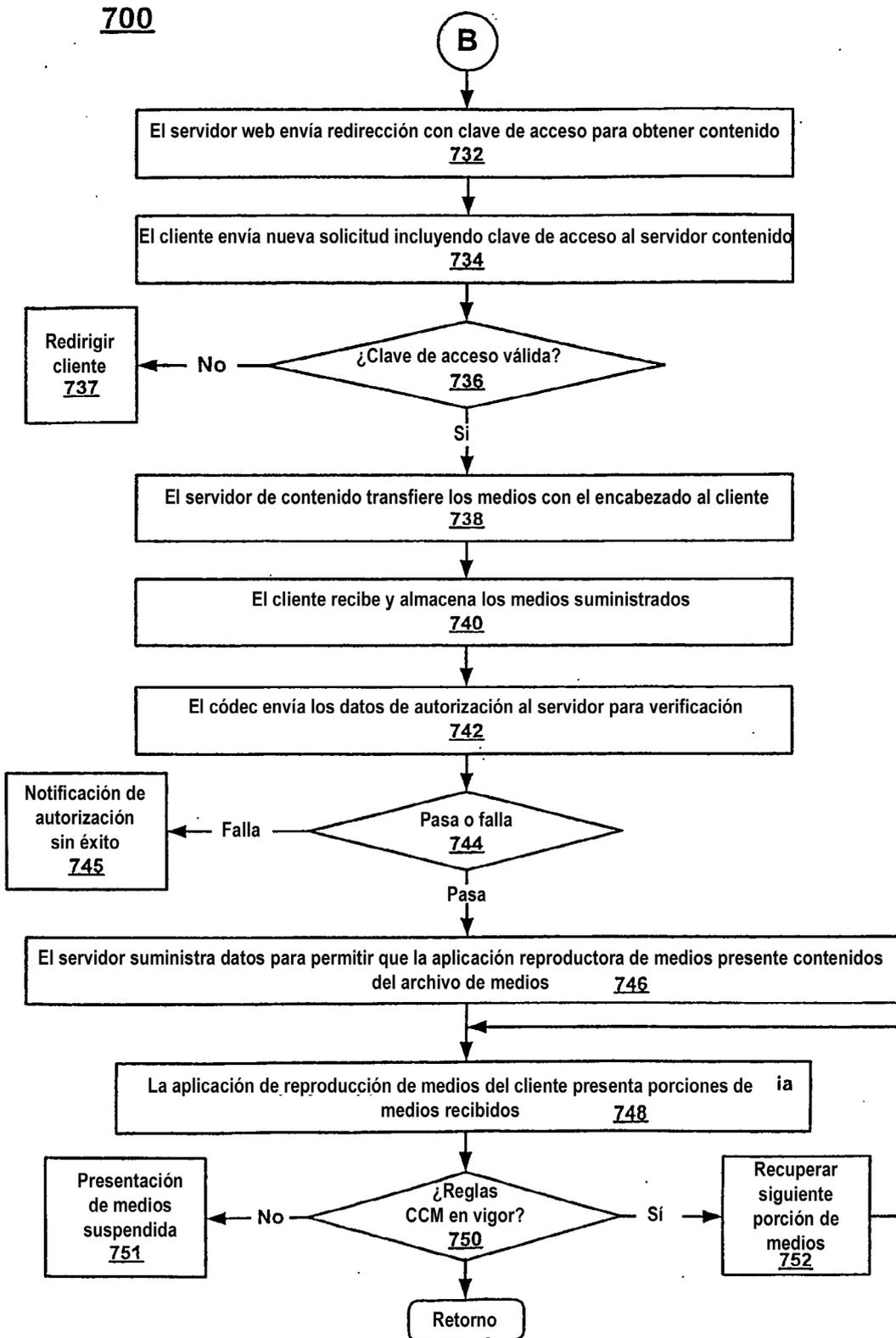


FIG. 7C

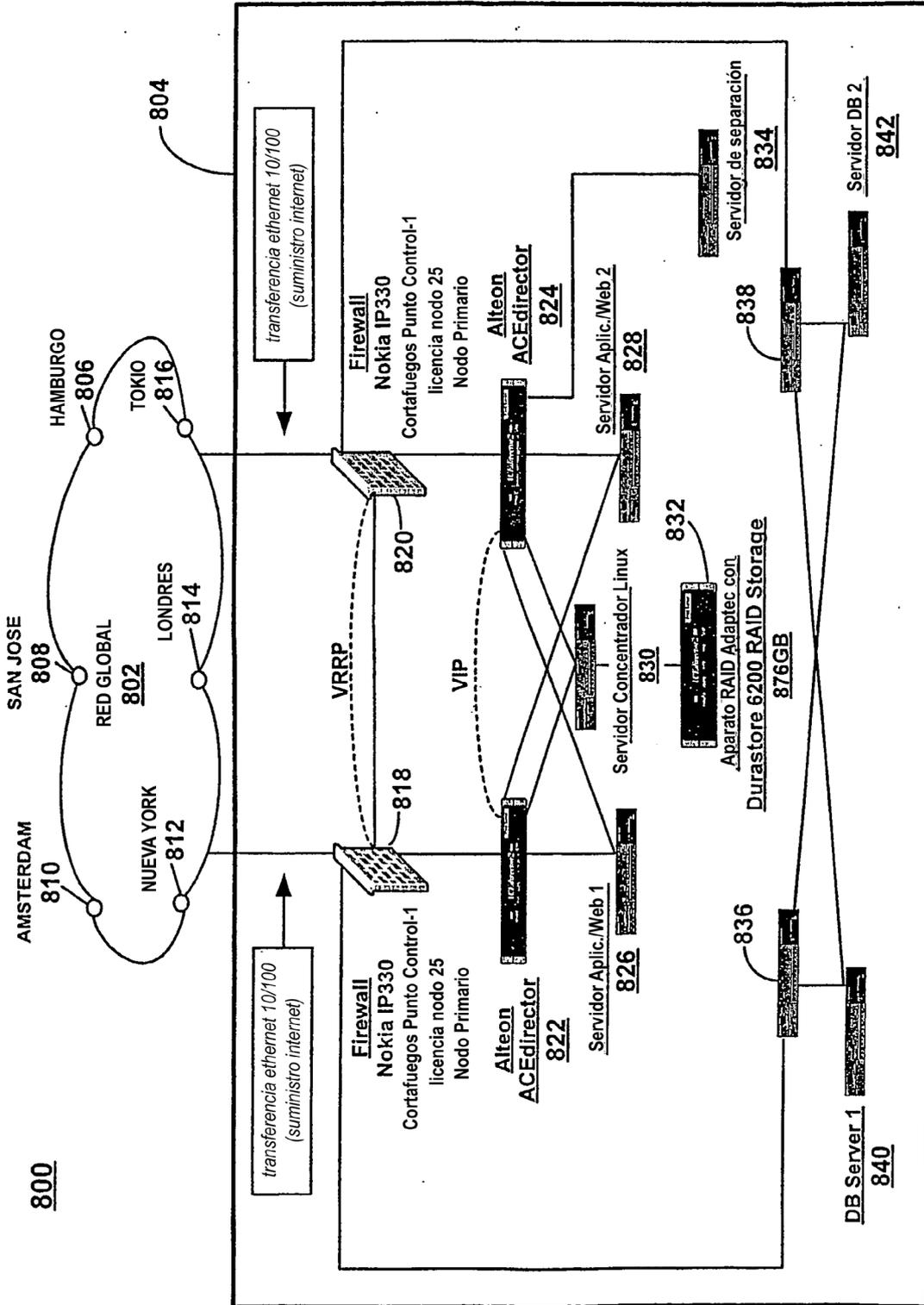


FIG. 8

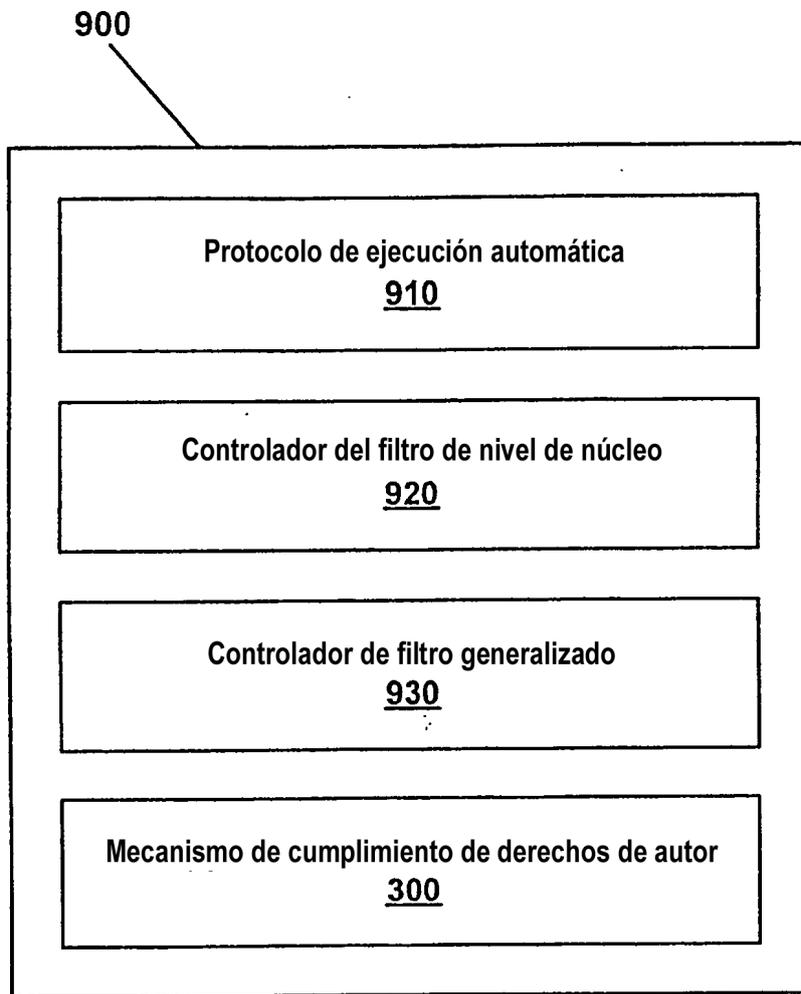


FIG. 9

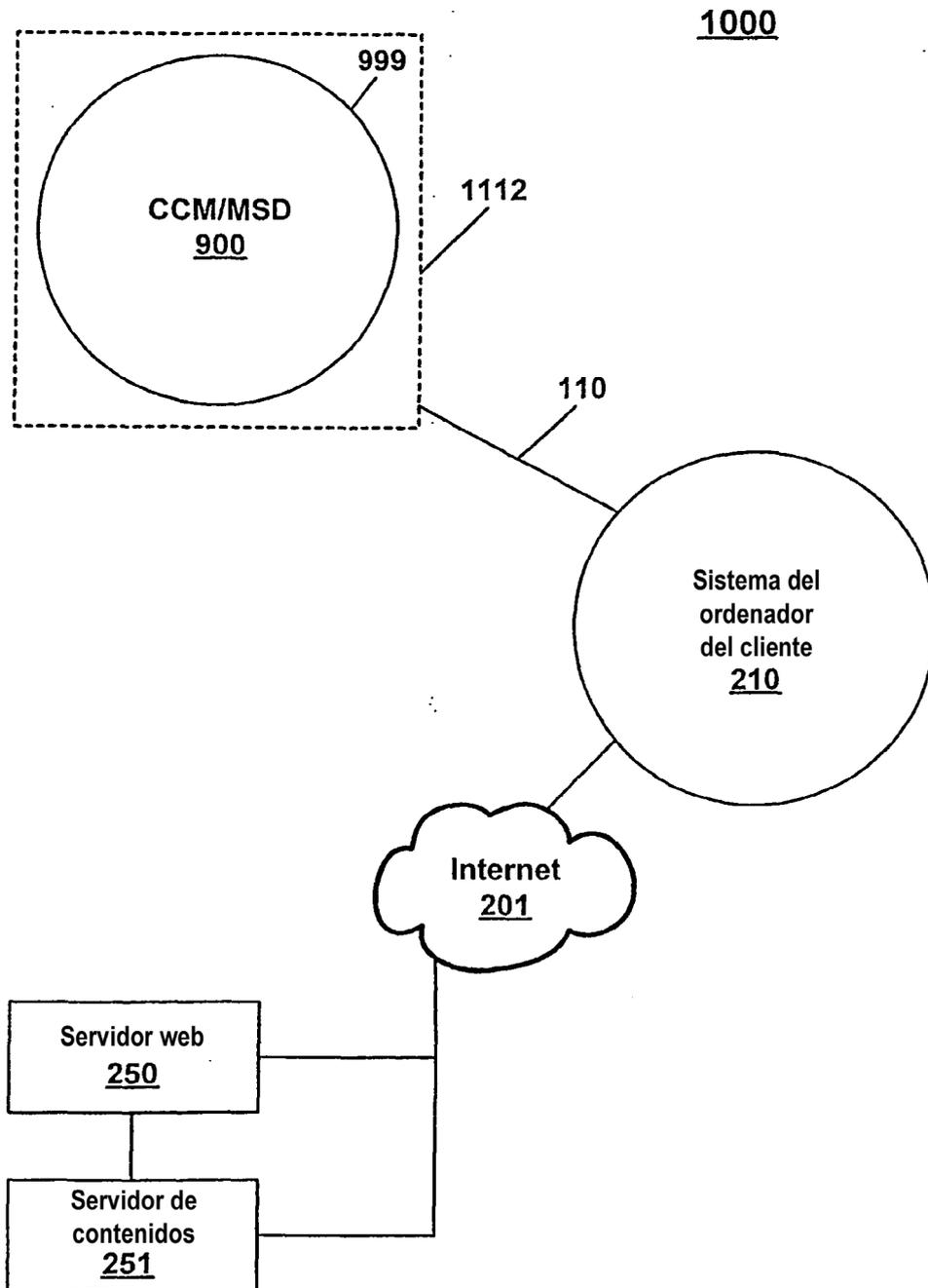


FIG. 10

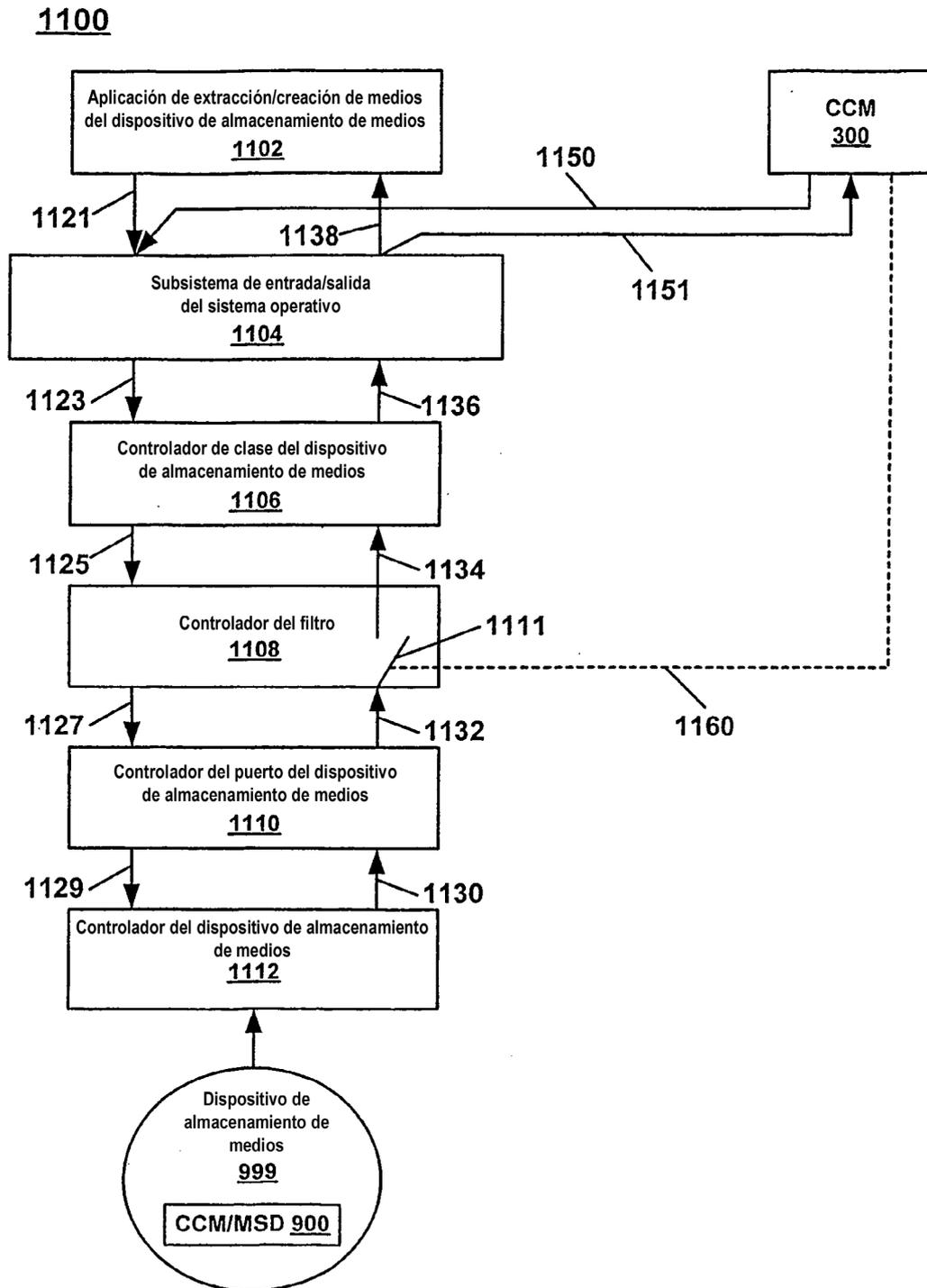


FIG. 11

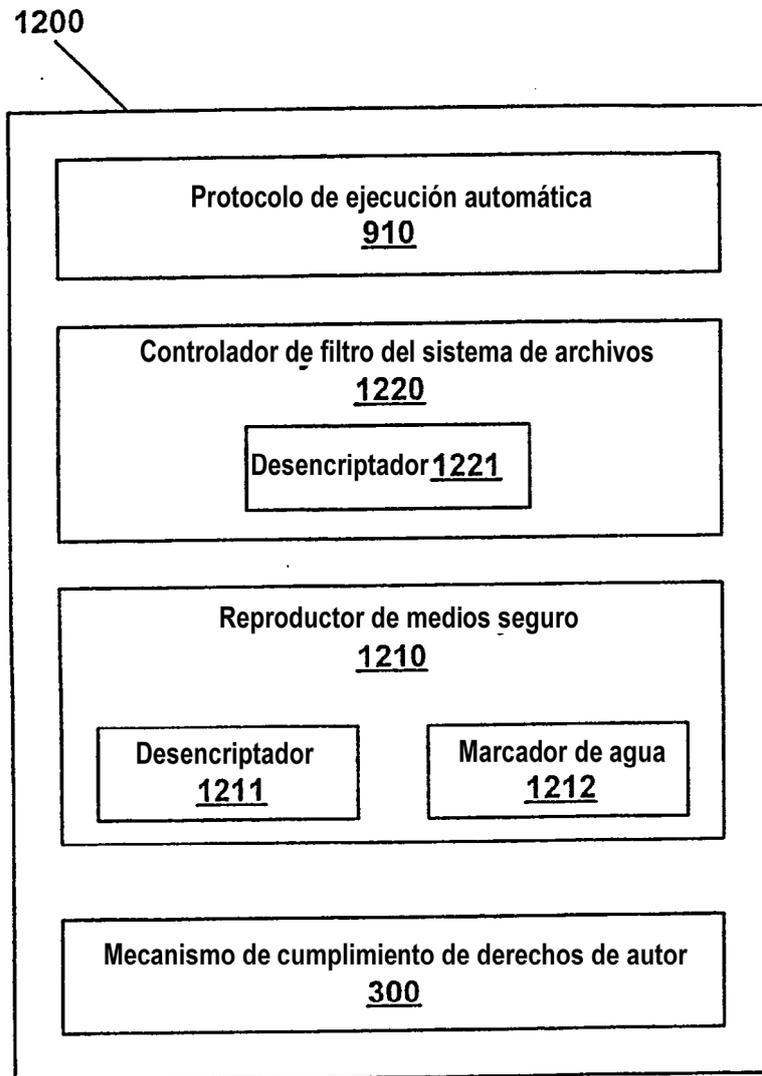


FIG. 12

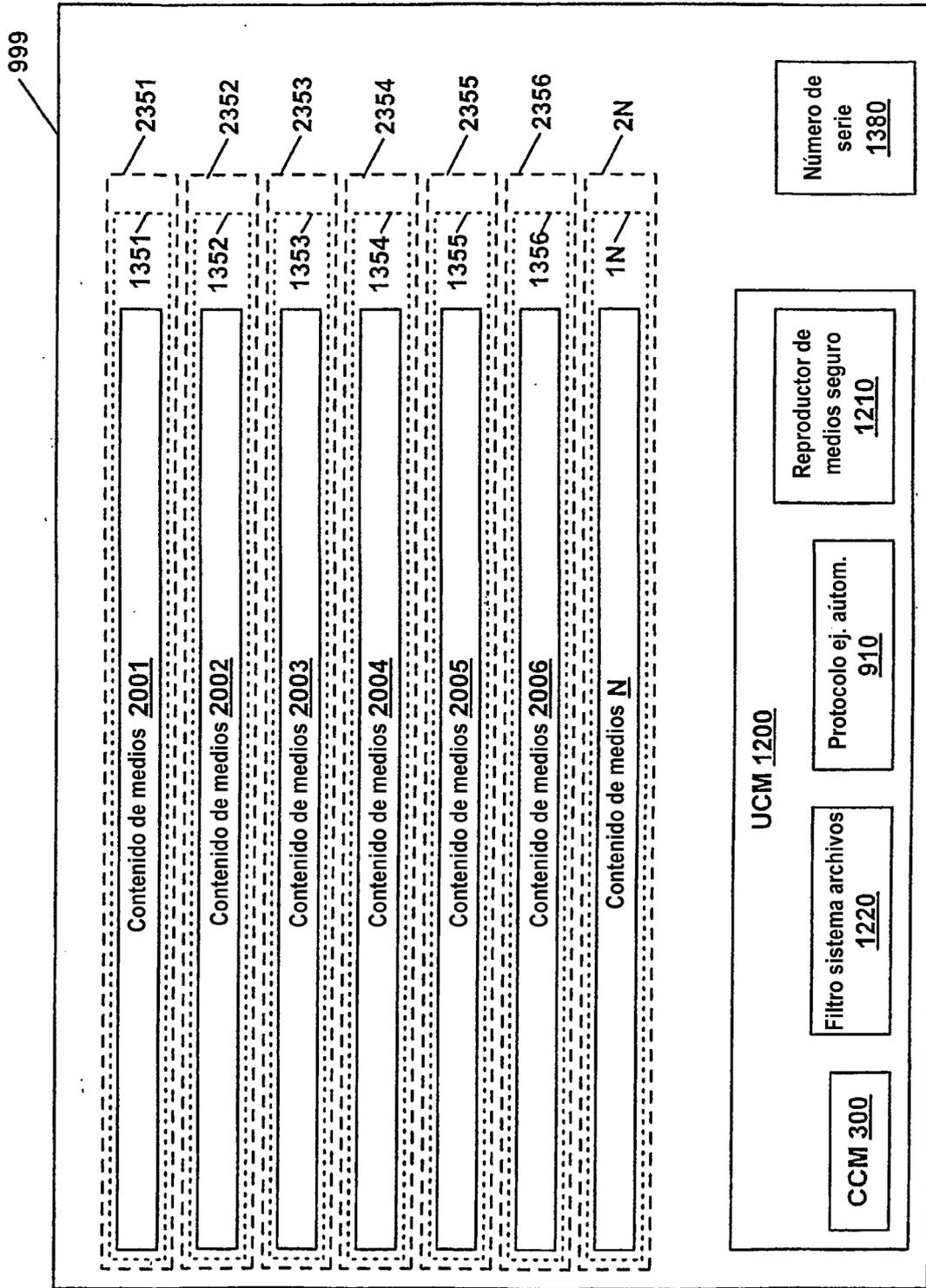


FIG. 13

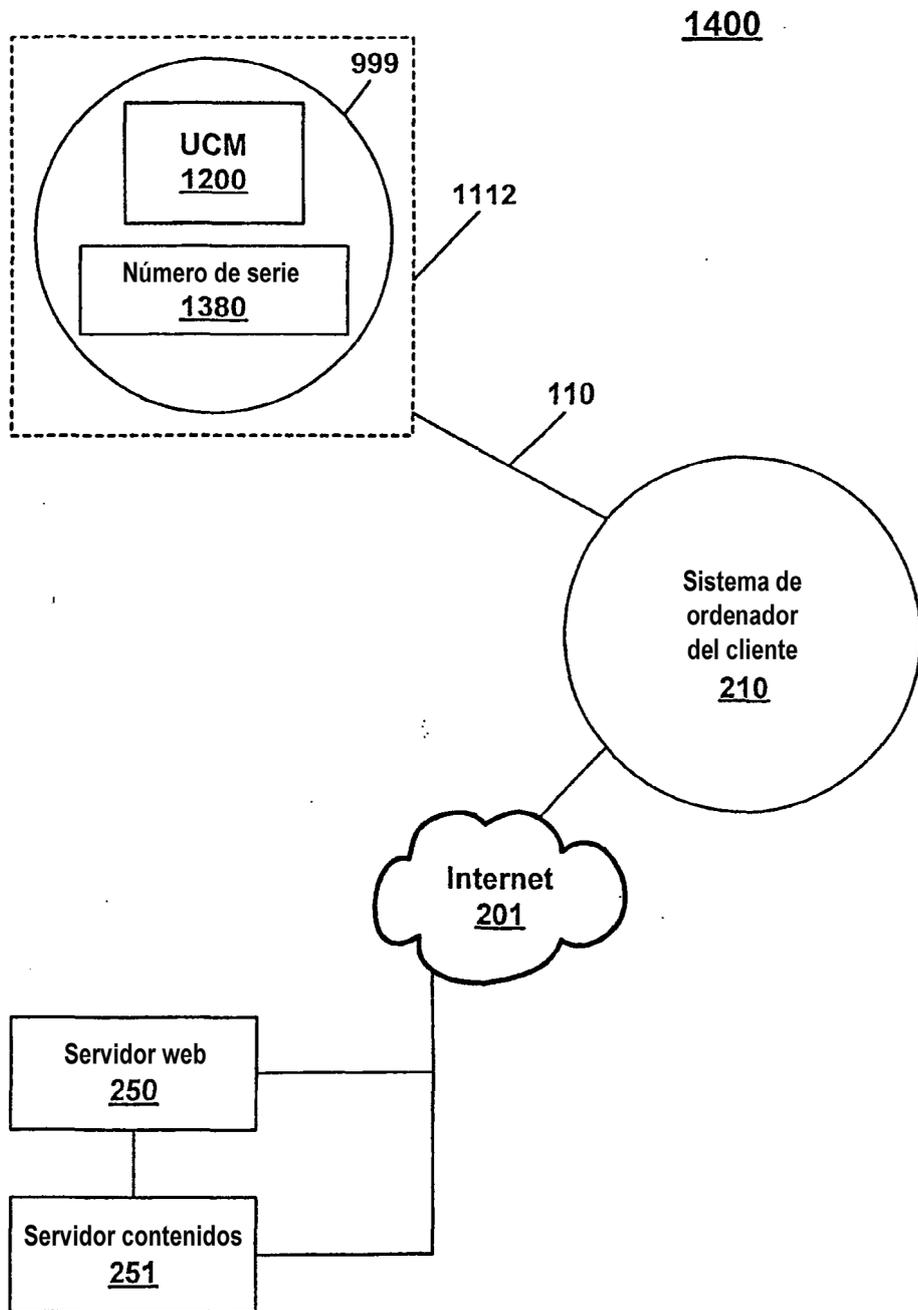


FIG. 14

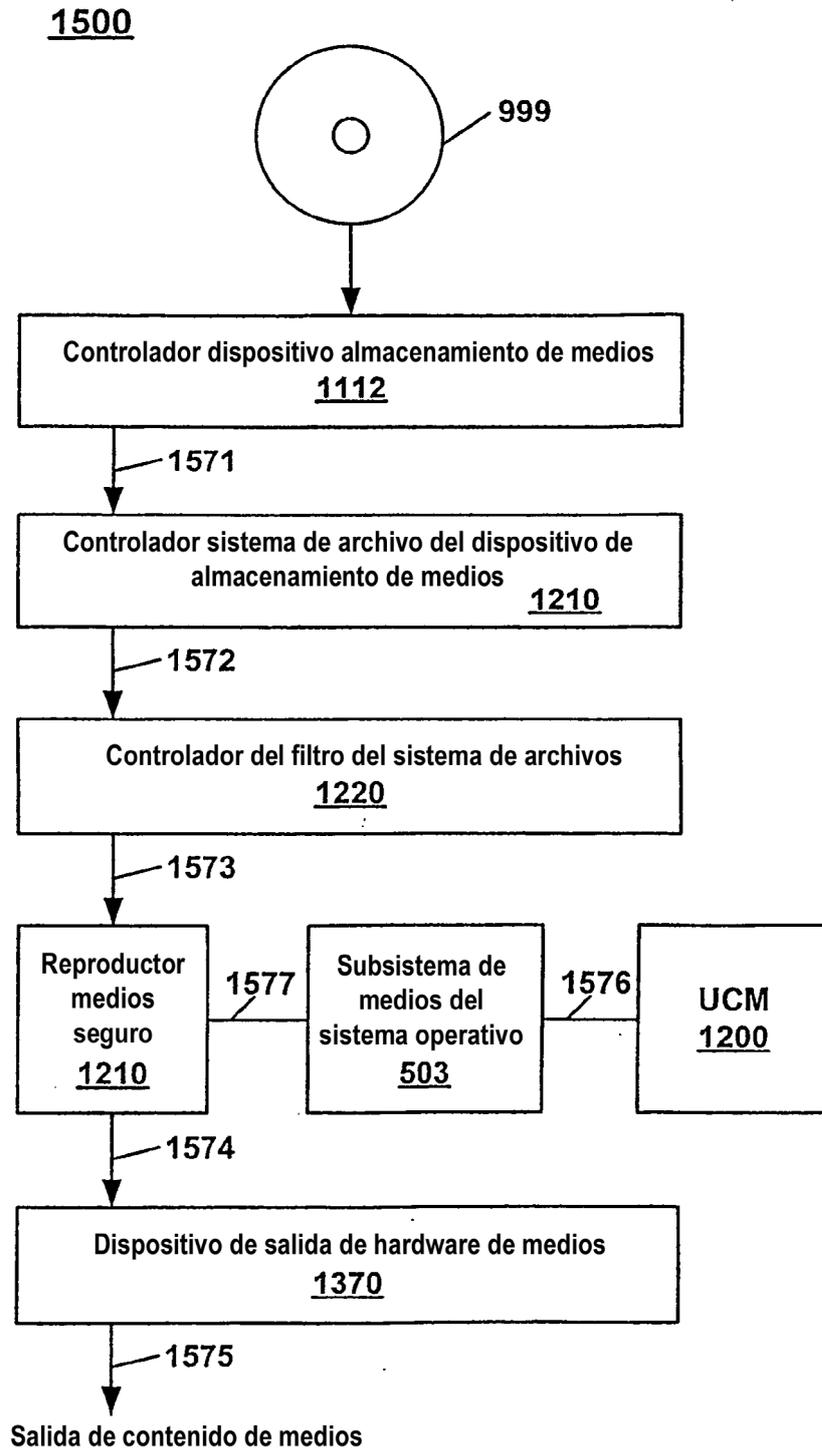


FIG. 15

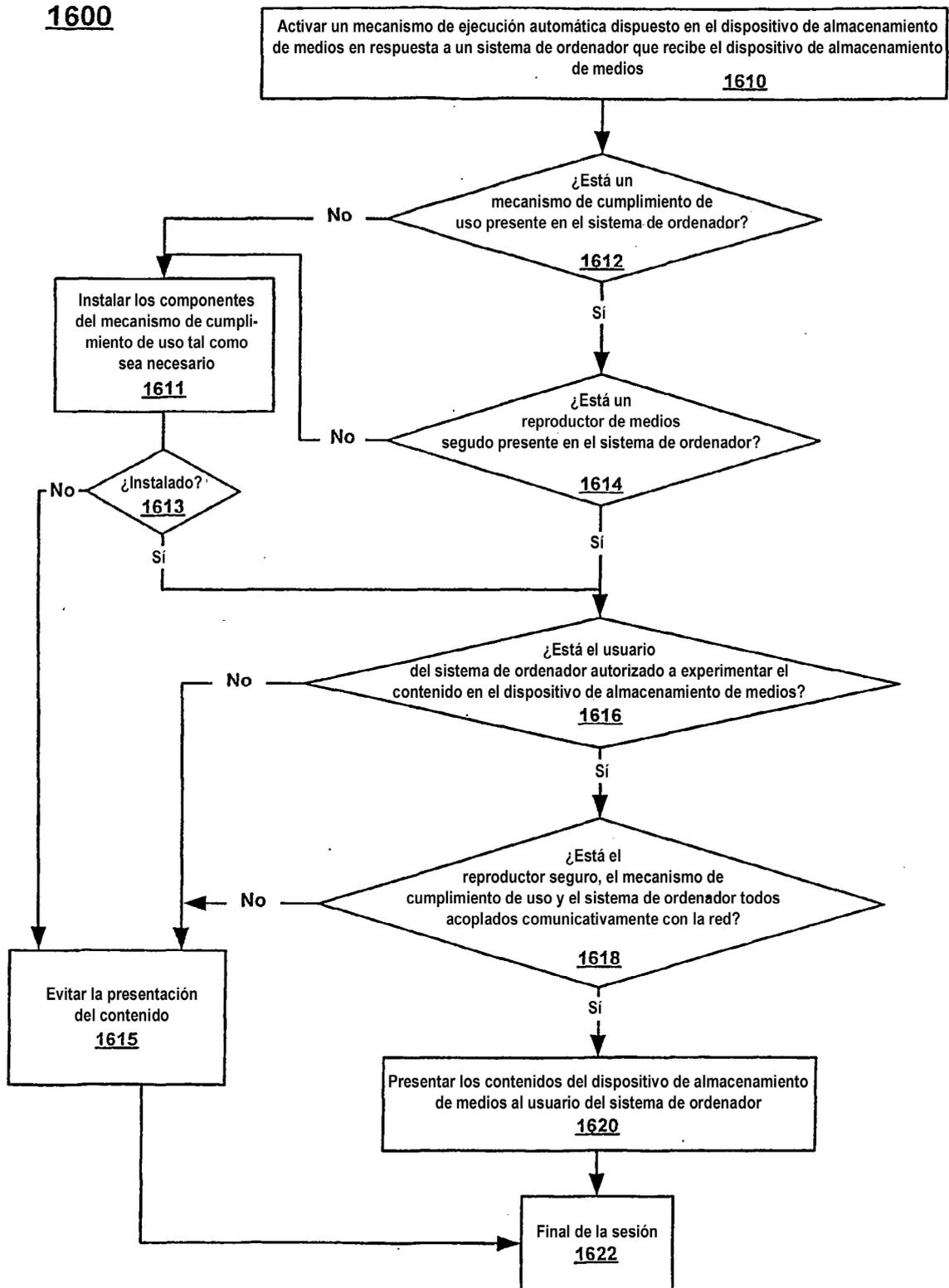


FIG. 16

1700

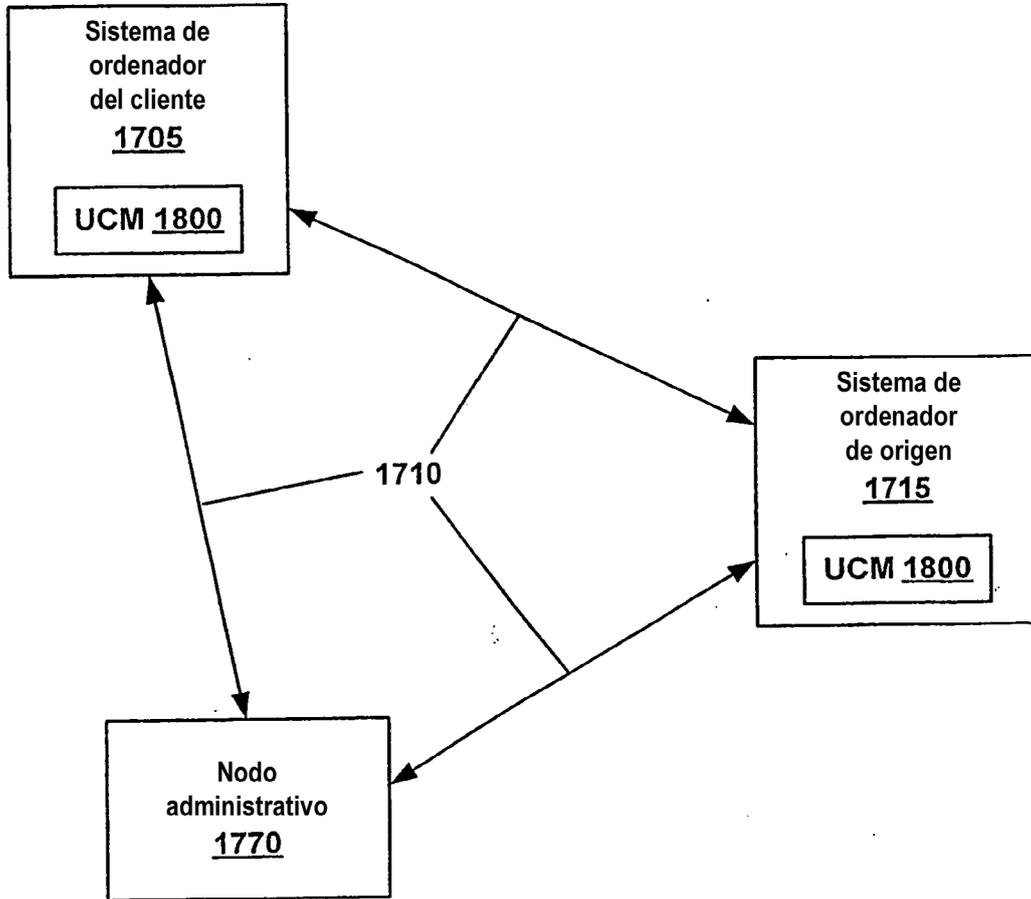


FIG. 17

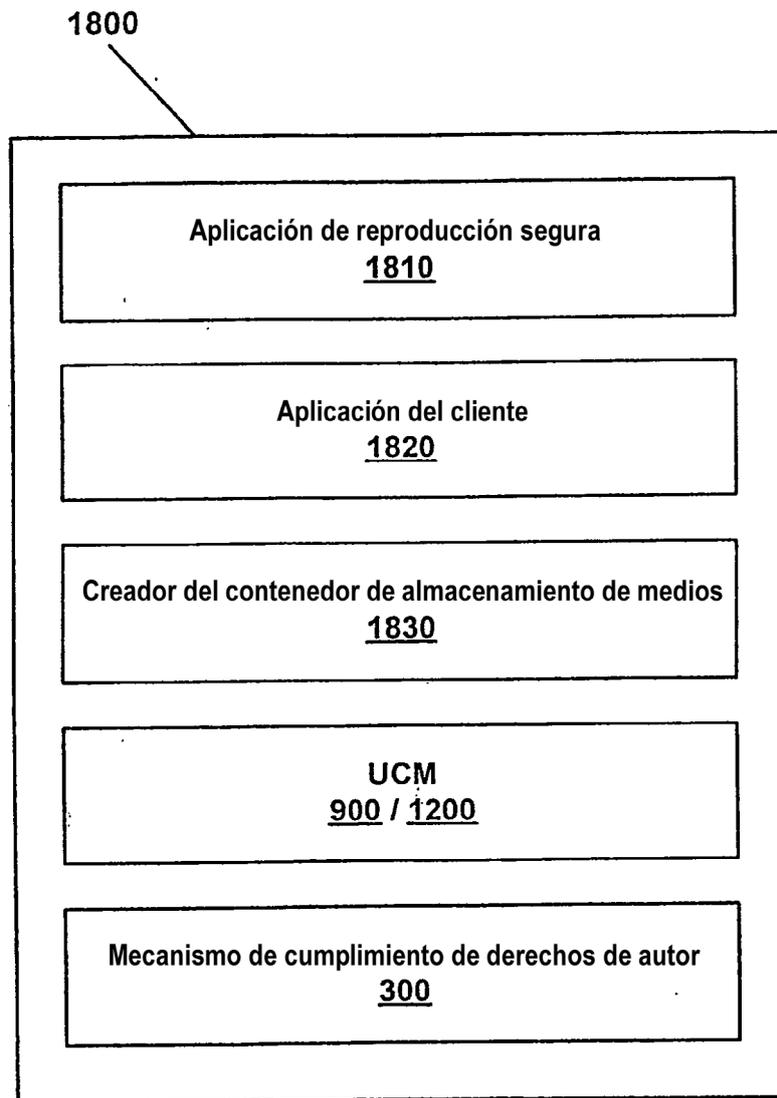


FIG. 18

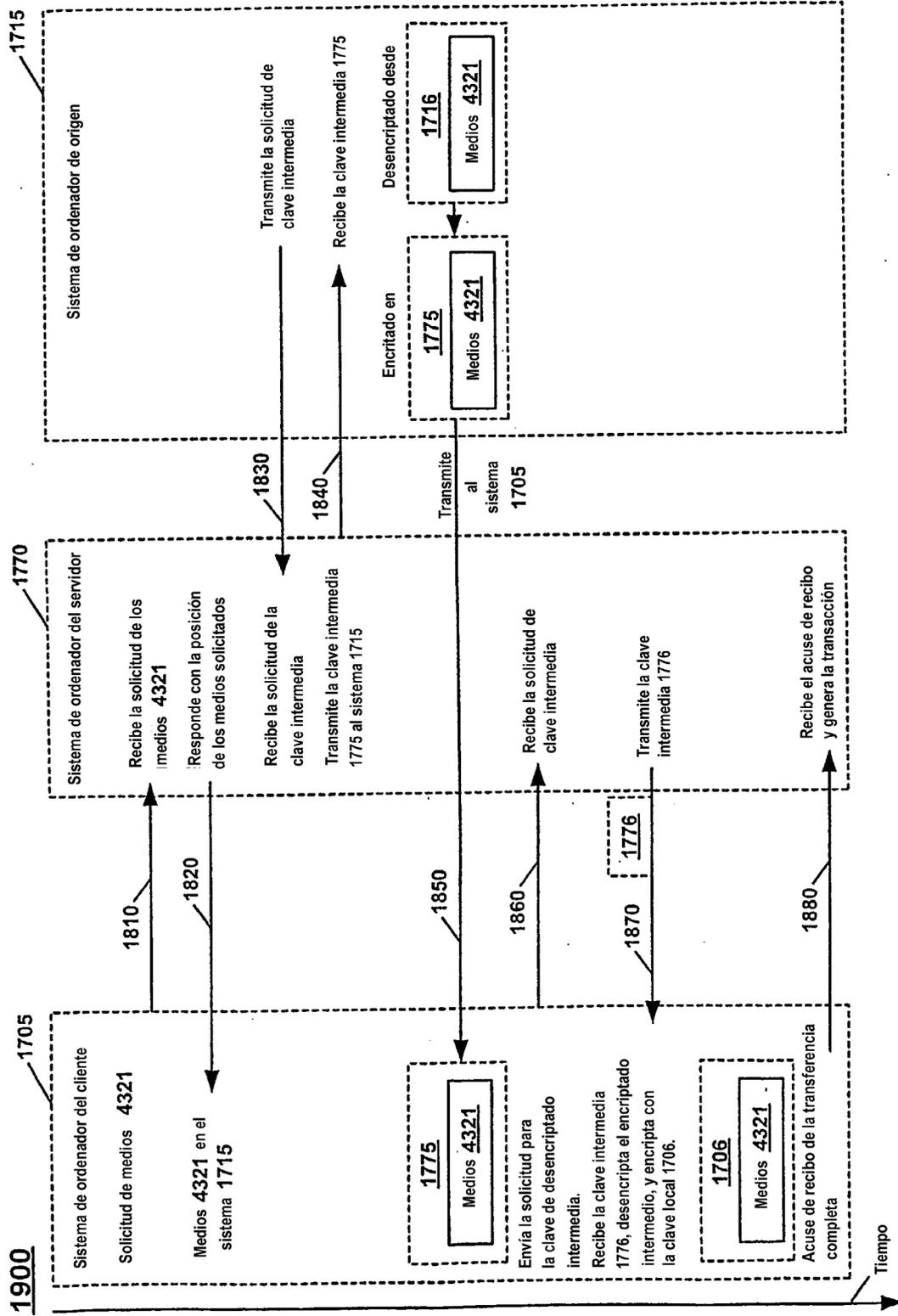


FIG. 19