(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 539 836**

(51) Int. CI.:

H04L 9/24 (2006.01)
G06Q 10/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.05.2002 E 02741722 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2015 EP 1402680**

(54) Título: **Sistema y método para un sistema comercial de alquiler y distribución de multimedia**

(30) Prioridad:

23.05.2001 US 293364 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.07.2015

(73) Titular/es:

SHARESTREAM, LLC (100.0%)
3301 New Mexico Avenue, N.W.
Washington, DC 20016, US

(72) Inventor/es:

WEINSTEIN, ALLAN, J.;
KLINE, PAUL, A. y
ROBERTS, JON, L.

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Sistema y método para un sistema comercial de alquiler y distribución de multimedia

Campo de la invención

1. La presente invención se refiere a la distribución a demanda de contenido multimedia por una red, y en particular, a un sistema y método para asegurar los derechos de propiedad intelectual en propiedad intelectual distribuida.

Antecedentes de la invención

2. La propiedad intelectual tal como software, juegos, música, vídeo y libros (colectivamente, "contenido multimedia") está ampliamente disponible a través de varios medios de distribución. La distribución se realiza cada vez más mediante una red tal como Internet. Típicamente, un cliente que usa un dispositivo de acceso que está configurado para "reproducir" contenido multimedia (el dispositivo de acceso se denomina aquí "reproductor") conecta con la red y descarga un archivo de contenido multimedia al reproductor. El cliente paga una tarifa de licencia fijada por el propietario o distribuidor del contenido multimedia, tarifa que se puede basar en el tiempo o en el uso. A los efectos de esta descripción, "reproducir" y "reproducción" incluyen: escuchar y escucha; ver y visión; reproducir y reproducción (tal como un juego electrónico); ejecutar y ejecución; y cualquier otra forma de uso y de utilización del contenido multimedia del producto. Un "reproductor" es el dispositivo usado para reproducir la obra. Este "reproductor" podría ser un ordenador personal o cualquier número de dispositivos configurados para reproducir contenido multimedia.

3. Aunque el uso de Internet como un medio de distribución tiene muchas ventajas, Internet también se puede usar para proporcionar acceso no autorizado a propiedad intelectual a escala mundial, denegando por ello al propietario de la propiedad el control sobre su uso. Este uso o distribución no autorizado se denomina popularmente "piratería".

4. Se han realizado varios acercamientos en un intento de limitar la piratería de contenido multimedia distribuido por Internet. El acercamiento más común es exigir que el cliente cree una cuenta y un método de pago con un proveedor de contenidos. Una vez creada la cuenta, el cliente pide el contenido multimedia y recibe el contenido multimedia desde una posición remota por Internet. El cliente usa o reproduce entonces el contenido multimedia en los términos de una licencia de uso concedida al cliente. El problema de este acercamiento es que no asegura los derechos de propiedad intelectual del contenido multimedia después de la distribución al cliente.

5. En cierta medida, este problema se resuelve usando marcas de agua digitales para el seguimiento del proveedor original de obras que han sido pirateadas. Además, la gestión de derechos digitales (GDD), en base a tecnología de filigrana digital, limita la capacidad del cliente de hacer copias del contenido multimedia y el número de veces que el contenido multimedia puede ser usado o reproducido. Sin embargo, ninguno de estos acercamientos asegura que no se acceda al contenido multimedia o que no se copie sin autorización o que el propietario del contenido multimedia reciba la justa compensación por el uso del contenido multimedia distribuido por Internet.

6. Encriptar el contenido multimedia mejora la capacidad del propietario de proteger el contenido multimedia contra el acceso y el uso no autorizados, a condición de que la imposición de la tecnología de clave no afecte adversamente a la experiencia del cliente al comprar una licencia de uso del contenido multimedia. Si se espera que el cliente pague por usar o reproducir el contenido multimedia, es importante que la creación y el intercambio de claves sea simple y fiable. De otro modo, el cliente puede buscar contenido multimedia alternativo o fuentes alternativas del contenido multimedia del propietario.

En contraposición a la presente invención, WO 01/13310 no expone ni sugiere que una clave privada no sea distribuida electrónicamente y que la clave privada se cree usando el al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido dado que la clave descrita en este documento usa componentes determinados todos ellos mucho antes de que el producto sea pedido.

US 5 991 399 describe un método de distribución segura de datos donde una clave es distribuida electrónicamente, lo que está en contradicción directa con la característica expuesta de que "la clave privada no es distribuida electrónicamente".

WO 00/08909 también describe distribuir electrónicamente claves donde las claves desencriptadas son enviadas desde una "Cámara de compensación".

7. Lo que se requiere es un medio barato de proteger los derechos de propiedad intelectual del propietario de contenido multimedia con una cantidad mínima de intrusiones o pasos adicionales que afectan a la representación digital del contenido.

Resumen de la invención

8. El objeto de la presente invención es usar códigos de componente de encriptado de cualquier tipo para asegurar los derechos del titular de propiedad intelectual cuando el contenido multimedia es distribuido digitalmente por una red. En este método la clave privada no es distribuida electrónicamente y la clave privada se crea usando el al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido.

9. Otro objeto de la presente invención es usar DES para encriptar contenido multimedia a distribuir digitalmente.

10. Otro objeto de la presente invención es usar DES para asegurar transacciones financieras entre el proveedor de contenidos multimedia y el cliente que pide distribución digital del contenido multimedia.

11. Otro objeto de la presente invención es proporcionar medidas antipiratería dentro del contenido multimedia distribuido digitalmente a un cliente.

12. Otro objetivo de la presente invención es usar porciones seleccionadas de contenido multimedia para diferenciar copias individuales que son transmitidas a un cliente.

13. Otro objetivo de la presente invención es introducir errores en un registro de contenido multimedia para identificar de forma única un registro concreto para rastrear por ello dicho registro y cualquiera de sus copias.

14. Otro objeto de la presente invención es emplear un sistema de clave de encriptado privada de manera simétrica para asegurar datos de cliente y para asegurar contenido multimedia contra el uso no autorizado.

15. Otro objeto de la presente invención es limitar la reproducción de contenido multimedia en virtud de códigos de hora y fecha usados en la clave privada.

16. Estos y otros objetivos de la presente invención serán evidentes por una revisión de las descripciones general y detallada que siguen. En la presente invención, la representación digital de contenido multimedia es codificada por el proveedor de contenidos multimedia usando un método de encriptado que se basa en una clave privada. Al objeto de que un cliente use o reproduzca contenido multimedia, el contenido multimedia debe ser desencriptado por el cliente usando la misma clave usada en el proceso de encriptado. Así, el cliente y el proveedor de contenidos multimedia comparten la clave privada.

17. En la presente invención, la clave privada compartida usada para encriptar y desencriptar el contenido multimedia se construye a partir de códigos de componente que están disponibles en el reproductor del cliente. En la realización preferida de la presente invención, estos códigos de componente incluyen un código de facturación, un código de hora y fecha, un código específico de ordenador o reproductor (que se denominará “código específico de ordenador”) y un código de cookie último, aunque la invención no se limita a tales componentes. Cada uno de los códigos de componentes usados para construir la clave privada debe estar presente en el reproductor del cliente o el cliente no puede desencriptar el contenido multimedia.

18. La presente invención también usa los códigos de componente procedentes de las instalaciones del cliente para validar la licencia de uso. Se incorpora un algoritmo de verificación en la lógica de derecho y control que es operada por los reproductores. El código de componente de hora y fecha se usa con el algoritmo de verificación para validar limitaciones de tiempo donde la licencia de uso es para un plazo permitiendo que la lógica de derecho y control determine si ha expirado el plazo de la licencia de uso.

19. Los cookies son archivos almacenados en el reproductor del cliente y son específicos del cliente. Los cookies capturan datos acerca del cliente, transacciones con el servidor web y el reproductor de contenidos multimedia del cliente. En una realización de la presente invención, el componente de código de cookie último se usa tanto para construir la clave de desencriptado como para validar restricciones de utilización. En concreto, el número de reproducciones u otras condiciones pueden estar incrustadas en el componente de código de cookie último. Cuando tiene lugar la reproducción, se decrementa el recuento de utilización. Cuando se recogen tarifas adicionales o se le concede al cliente de otro modo tiempo de reproducción, el recuento de utilización se incrementa. Una vez que se logra un nivel de recuento, determinado por la lógica de derecho y control, no se permite más uso del programa hasta que el cliente compre más derechos de uso.

20. En otra realización de la presente invención, el código específico de ordenador se usa para identificar un reproductor concreto. Por ejemplo, los elementos específicos de un reproductor pueden incluir un número de serie, ruido aleatorio generado por componentes del reproductor, dirección de red, dirección de control de acceso al medio (MAC), nombre de propietario, nombre de volumen de unidad y fecha de creación de registro. Estos elementos no se entienden como una limitación, sino que son ilustrativos solamente. Usando un componente de código específico de ordenador, el código de desencriptado se puede restringir a ejecución solamente en una sola posición de reproducción.

21. El componente de código de facturación también se usa para validar los términos de la licencia. Además, se puede crear una cuenta y guardar dentro del reproductor y debitarla cuando se use la obra.

Breve descripción de los dibujos

La figura 1 ilustra los componentes del sistema de distribución y alquiler de multimedia.

La figura 2 ilustra el establecimiento de una relación entre el cliente y el proveedor de contenidos de media.

La figura 3 ilustra los componentes de la instalación del cliente y la instalación del proveedor de contenidos.

La figura 4 ilustra el proceso para pedir contenido multimedia.

La figura 5 ilustra el proceso en una instalación del cliente para reproducir contenido multimedia recibido del proveedor de contenidos.

Descripción detallada de la invención

22. Con referencia en primer lugar a la figura 1, se ilustra la interconectividad de la instalación del cliente y la instalación del proveedor de contenidos. En una instalación del cliente 10 se encuentra un reproductor configurado para reproducir o usar contenido multimedia 12 conectado a una red 20, en este caso Internet. También está conectado a la red un servidor de distribuidor de obras de propiedad intelectual ("proveedor de contenidos") 32 en la instalación del proveedor de contenidos 30. A modo de ejemplo y no como limitación, un reproductor puede ser un ordenador personal fabricado por IBM, Dell o Compact, un asistente de datos personales, o cualquier dispositivo capaz de conectar con una red y recibir y operar la lógica de derecho y control. Igualmente, la red ilustrada en la figura 1 es Internet, pero la invención no se limita por ella. La red puede incluir una pluralidad de redes interconectadas, alámbricas e inalámbricas.

23. La instalación del proveedor de contenidos tiene una base de datos de cliente 34 así como una base de datos de contenido 36. El cliente crea una cuenta con el proveedor de contenidos como una transacción preliminar. Los datos de cuenta del cliente son confirmados o establecidos y actualizados en la base de datos de cliente 34. Unos datos de cuenta del cliente incluyen información de facturación y un medio de pago. En la realización preferida el medio de pago es una tarjeta de crédito. En otra realización, el pago se realiza a través de una transferencia ACH. En otra realización, el cliente paga una cantidad a una cuenta que es debitada en base al uso de contenidos multimedia.

24. Los datos mantenidos en la base de datos de cliente 34 son encriptados usando una clave privada compartida con el fin de asegurar la información y privacidad del cliente. La clave privada compartida está formada por códigos de componente que incluyen información recuperada del reproductor del cliente 12 y datos introducidos por el cliente. En base a esta clave privada compartida, los datos de cliente son enviados codificados y seguros al servidor del proveedor de contenidos 32. En la realización preferida, la clave privada compartida es una clave DES, pero esto no se entiende como limitación. Las actualizaciones del registro del cliente, incluyendo la actividad actual, se efectúan en la base de datos de cliente 34.

25. Antes de que el cliente pueda obtener contenido multimedia del proveedor de contenidos, el cliente debe ser conocido por el proveedor de contenidos. Con referencia a la figura 2, el cliente contacta con el proveedor de contenidos 50. En la realización preferida, este contacto inicial se realiza por la red entre el reproductor del cliente 12 y el servidor del proveedor de contenidos 32 como se ilustra en la figura 1. Sin embargo, se puede usar otros medios para este contacto inicial sin superar el alcance de la presente invención. Por ejemplo, el contacto entre el cliente y el proveedor de contenidos puede ser establecido por teléfono, correo electrónico, por escrito u otros medios de comunicaciones. Una vez realizado el contacto inicial, el proveedor de contenidos presenta un contrato de servicio 52 al cliente para aceptación 54. Si los términos no son aceptables para el cliente, el contacto se termina 56. Si el cliente acepta los términos, el proveedor de contenidos pide información del cliente 58. En la realización preferida, la información del cliente incluye un código de facturación asociado con un medio de pago seleccionado por el cliente y un código específico de ordenador que identifica de forma única el reproductor del cliente. En caso de que el cliente no conozca el código específico de ordenador asociado con el reproductor del cliente, el proveedor de contenidos proporciona instrucciones al cliente sobre cómo determinar el código específico de ordenador. En otra realización de la presente invención, el proveedor de contenidos determina el código específico de ordenador del reproductor del cliente a distancia. El cliente envía entonces la información del cliente al proveedor de contenidos 60 y el proveedor de contenidos guarda la información del cliente en la base de datos de cliente 62.

26. El proveedor de contenidos envía entonces al reproductor del cliente software 64 incluyendo lógica de derecho y control, un motor de encriptado/desencriptado, un primer cookie, y medios para comprobar el cumplimiento de los términos de la licencia asociada con contenido multimedia descargado del servidor del proveedor de contenidos. El cliente instala y configura el software de reproductor y la sesión inicial termina 66.

27. Como será evidente a los expertos en la técnica de la presente invención, los pasos de la sesión inicial pueden

ser realizados de varias formas. Por ejemplo, el intercambio de información de identidad y la distribución del software de reproductor del cliente se pueden realizar fuera de línea. El software de reproductor puede estar integrado en el reproductor o comprarse en un minorista de software. El software de reproductor puede ser distribuido de forma gratuita a los consumidores por el proveedor de contenidos como un medio de invitar a los consumidores a usar los servicios del proveedor de contenidos. Estas y otras variaciones de los medios de implementar la sesión inicial se consideran dentro del alcance de la presente invención.

28. Con el software de reproductor instalado y configurado, el cliente está preparado para hacer una petición de contenido multimedia. Con referencia de nuevo a la figura 1, el contenido multimedia pedido es almacenado en la base de datos de servidor del proveedor de contenidos 36. En una realización de la presente invención, el contenido de medios se almacena en una forma codificada, comprimida. Uno de dichos protocolos de compresión/descompresión es MPEG (Grupo de Expertos de Imágenes en Movimiento), protocolo que se aplica a obras audio/visuales. Una derivada común de MPEG para obras audio es MP3 (MPEG Audio Capa 3). MP3 permite la descarga muy rápida de audio de calidad de la Web. Las obras que no son audio/visuales, como texto, pueden ser comprimidas y descomprimidas por varios programas comercialmente disponibles tales como WinZip™ y PKZip™. Será claro a los expertos en la técnica de la presente invención que se puede usar otros protocolos de compresión, todos los cuales caen dentro del alcance de la presente invención. Como se ilustra en la figura 3, el software de reproductor incluye un decodificador 118. Para cada esquema de codificación implementado por la instalación del proveedor de contenidos, el cliente tendrá un decodificador capaz de decodificar el contenido multimedia con el fin de hacerlo reproducible por el reproductor del cliente.

29. Con referencia a continuación a la figura 3 se ilustran los códigos de componente de la clave privada compartida en la instalación del proveedor de contenidos y los códigos de componente en la instalación del cliente. El contenido multimedia es encriptado con un motor de encriptado 202 usando una clave compartida privada única asociada con el reproductor del cliente 12 y datos de cliente. Como se ilustra en la figura 3, cuatro elementos están disponibles tanto para el reproductor del cliente como para el servidor del proveedor de contenidos para construir la clave privada compartida: código de facturación 110; código de hora y fecha 112; código específico de ordenador 114; y código de cookie último 116. El código específico de ordenador y el código de facturación fueron compartidos por el cliente y el proveedor de servicios durante el contacto inicial ilustrado en la figura 2. El código de cookie último es el cookie distribuido al reproductor del cliente con la distribución más reciente de contenido multimedia. Si el cliente no ha pedido previamente ningún contenido multimedia, el código de cookie último es el cookie inicial incluido en el software de reproductor instalado en el reproductor del cliente. El código de hora y fecha es elegido por el cliente al tiempo en que pide el contenido multimedia. Así, los cuatro códigos son conocidos por el cliente y el proveedor de contenidos al tiempo en que se completa un pedido. Como se ilustra a continuación, estos cuatro códigos se usan para crear una clave privada compartida que, a su vez, se usa para encriptar el contenido de medios antes de la distribución al reproductor del cliente.

30. Con referencia ahora a la figura 4, el cliente pide contenido multimedia al proveedor de contenidos 300. El proveedor de contenidos pide información de entrada en comunicación al cliente 305 y el cliente responde. El proveedor de contenidos comprueba la información proporcionada por el cliente 310 y determina si el proveedor de contenidos conoce al cliente. En caso negativo, el proveedor de contenidos pide de nuevo información de entrada en comunicación al cliente. En la realización preferida, este bucle es limitado por un contador de intentos de entrada en comunicación que permite al cliente un número predeterminado de intentos antes de que el proveedor de contenidos envíe instrucciones adicionales al cliente.

31. A la entrada en comunicación exitosa realizada por el cliente, el proveedor de contenidos pide al cliente 315 el código de cookie último. En la realización preferida, el código de cookie último se usa para autenticar el cliente y para crear una clave compartida. El cliente proporciona al proveedor de contenidos el código de cookie último 320 y el proveedor de contenidos pide al cliente que pida contenido de medios 325. Como será evidente a los expertos en la técnica de la presente invención, la petición de pedir contenido de medios puede tomar muchas formas sin superar el alcance de la presente invención. Por ejemplo, y no como limitación, en una realización de la presente invención, el proveedor de contenidos proporciona al cliente un menú de contenido de medios. En otra realización, al cliente se le indica que busque en la base de datos de medios del proveedor de contenidos el contenido de un título específico.

32. El cliente selecciona el contenido de medios para descargar 330 y revisa los términos de la licencia asociados con dicha selección 335. Si los términos de la licencia no son aceptables, al cliente se le pide que seleccione de nuevo. Si los términos son aceptables, el cliente pide el contenido de medios y envía al proveedor de contenidos un código de hora y fecha 340. El código de hora y fecha establece un punto de tiempo que se usa para determinar la expiración de una licencia a base de tiempo. El código de hora y fecha está asociado con cada selección de contenido de medios descargados por el cliente en una sesión de pedido concreta y se guarda en la base de datos de cliente.

33. El proveedor de contenidos crea una clave privada compartida a partir de los cuatro códigos de componente conocidos tanto por el proveedor de contenidos como por el cliente 345. Como se ha explicado previamente, al tiempo en que se realiza el pedido, el cliente posee el código específico de ordenador, el código de cookie último, el

código de facturación y el código de hora y fecha. Durante la sesión inicial, el proveedor de contenidos recibió del cliente el código de facturación y el código específico de ordenador. El proveedor de contenidos conoce el código de cookie último. A la recepción del código de hora y fecha del cliente, el proveedor de contenidos está en posesión de los cuatro códigos de componente. A partir de estos códigos de componente, una clave privada es "compartida" por el cliente y por el proveedor de contenidos sin intercambiar realmente la clave privada.

34. El proveedor de contenidos encripta el contenido de medios usando la clave privada compartida, crea un nuevo cookie, y envía el cookie y el contenido de medios encriptado al cliente 350. En otra realización de la presente invención, al cliente se le ofrece la opción de que el contenido de medios sea distribuido en una fecha posterior o a una hora específica. Si la distribución es para un tiempo futuro, los datos de pedido son almacenados en la base de datos de cliente. Cuando llega el tiempo de distribución, el servidor del proveedor de contenidos comprueba un enlace con la instalación específica del cliente. Si un enlace no está preparado, se envía un aviso al cliente para iniciar un enlace.

35. El cliente recibe el contenido de medios, asociado con el código de hora y fecha proporcionado al proveedor de contenidos durante la sesión de pedido, y guarda el contenido de medios, el código de fecha, el nuevo cookie 355. En este punto, el cliente está preparado para reproducir el contenido de medios.

36. La reproducción del contenido de medios se ilustra con referencia a la figura 5. Cuando el cliente elige reproducir el contenido de medios 400, el software de reproductor crea la copia de cliente de la clave privada compartida 405 a partir de los mismos cuatro códigos de componente usados por el proveedor de contenidos para crear la clave. El cliente desencripta entonces el contenido de medios usando la clave privada compartida 410 y el software de reproductor efectúa una comprobación para determinar si el cliente cumple los términos de la licencia 415.

37. Como se ha indicado previamente, el software de reproductor incluye un algoritmo de verificación incorporado en la lógica de derecho y control. En otra realización, el algoritmo de verificación específico para un título concreto del contenido de medios está anexo al contenido multimedia e instalado en el reproductor como un plug-in para uso por el software de cliente. El algoritmo de verificación utiliza los códigos de componente individuales para validar restricciones de licencia específicas impuestas a la reproducción del contenido multimedia (tiempo de uso, número de reproducciones) y al reproductor en el que se reproduce el contenido multimedia (donde las copias ilegales del contenido multimedia no se pueden reproducir en un reproductor distinto del reproductor designado). Si el algoritmo de verificación determina que el cliente no cumple los términos de la licencia, se presenta un mensaje al cliente 420. Por ejemplo, un cliente que haya prepagado el uso de contenido de medios puede no tener fondos suficientes para reproducir el contenido de medios. En este caso, el mensaje indica al cliente que recargue su cuenta. Si el algoritmo de verificación determina que la copia del contenido de medios ha sido pirateada, el mensaje toma la forma de un aviso relativo al uso no autorizado del contenido de medios.

38. El componente de código de hora y fecha 112 del código de clave privada identifica la hora y fecha en que se hizo el pedido del contenido multimedia. Una realización usa el código de cookie último 116 en unión con el componente de código de hora y fecha 112. La información puede incluir hora y fecha de la descarga de contenido multimedia, los términos de la licencia de uso y datos de dispositivo únicos tales como la dirección de Internet. Los datos de limitación de tiempo de licencia de uso se pueden hallar en el cookie y se usan, en unión con el código de hora y fecha y la lógica de derecho y control, para restringir la reproducción del contenido multimedia al período de tiempo contractual.

39. El código de cookie también se puede usar para comprobar la Id del usuario y la dirección de protocolo de Internet (IP) para confirmar que el contenido multimedia está siendo reproducido en el dispositivo que tiene licencia para reproducir el contenido multimedia. Estos datos están fácilmente disponibles en los datos de cookie último devueltos al proveedor de contenidos durante el proceso de pedido.

40. Una licencia de pago por reproducción puede ser controlada a través del componente de código de facturación 110 de la clave privada. El código de facturación 110 contiene información acerca de un método de pago. En la realización preferida, el método de pago es una tarjeta de crédito, pero la invención no se limita a ella. En otra realización, el método de pago es una transferencia ACH desde una cuenta bancaria. En otra realización, se crea una cuenta prepagada conteniendo una cantidad de crédito con el código de facturación. Una realización alternativa crea una cuenta prepagada en el archivo de cookies. Antes de que el contenido multimedia sea desencriptado, se verifica la cuenta de crédito usando la lógica de derecho y control para confirmar que hay saldo suficiente para pagar la tarifa de licencia asociada con el contenido multimedia. La tarifa de licencia se resta de la cantidad de crédito según el esquema de pago de la licencia. A modo de ilustración, cuando la tarifa de licencia se basa en tiempo, la cantidad de crédito se decrementa por cada unidad de tiempo en que se reproduce el contenido multimedia. Cuando la tarifa de licencia se basa en el uso, la cantidad de crédito se decrementa cada vez que se reproduce el contenido multimedia.

41. Si el cliente cumple los términos de la licencia, el contenido de medios es reproducido en el reproductor del cliente 425 y se registra 435 la hora y/o la terminación de un ciclo de reproducción. Al cliente se le pregunta si desea una repetición 440. Si desea una repetición, el algoritmo de verificación determina de nuevo si el cliente cumple los

términos de la licencia 415. Si no desea repetición, al cliente se le pregunta si desea reproducir otra selección de contenido de medios 445. Si desea otra selección, el proceso comienza de nuevo 400. Si no, la reproducción finaliza en 450.

42. En otra realización de la presente invención, los aspectos de antipiratería de la presente invención se mejoran introduciendo elementos de datos adicionales en el contenido multimedia. Introduciendo los elementos de datos adicionales en bytes o pistas seleccionados del contenido multimedia, los esquemas de corrección de errores asociados con la reproducción de contenido multimedia excluirán que los elementos de datos adicionales afecten a la reproducción del contenido multimedia. Asociando un conjunto concreto de elementos de datos adicionales con el contenido multimedia distribuido a un cliente concreto, los elementos de datos adicionales pueden ser usados como una “huella” para identificar la fuente de copias pirateadas del contenido multimedia.

REIVINDICACIONES

1. Un método para asegurar la propiedad intelectual distribuida electrónicamente incluyendo:

establecer contacto entre un proveedor de propiedad intelectual y un cliente con un reproductor, donde al menos un código de componente es compartido;

pedir un producto de propiedad intelectual al proveedor de propiedad intelectual;

recibir el producto de propiedad intelectual donde el producto de propiedad intelectual incluye además datos de contenido y datos de derechos en forma digital y se encripta con una clave privada antes de ser distribuido electrónicamente, donde la clave privada no es distribuida electrónicamente y la clave privada se crea usando el al menos único código de componente y al menos un código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido;

guardar el producto de propiedad intelectual en el reproductor, incluyendo además el reproductor un registro de datos de reproductor y donde el registro de datos de reproductor incluye el al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido;

desencriptar el producto de propiedad intelectual con una copia de cliente de la clave privada usada para encriptar el producto de propiedad intelectual, donde la copia de cliente de la clave privada es creada por el reproductor usando una combinación del al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido;

comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido; y

reproducir los datos de contenido en el reproductor si el derecho ha sido determinado.

2. El método para asegurar la propiedad intelectual de la reivindicación 1, donde los datos de derechos incluyen un identificador de reproductor, y donde el registro de reproductor incluye además un identificador específico de reproductor único para el reproductor, y donde comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluye además determinar que el identificador de reproductor y el identificador específico de reproductor son los mismos.

3. El método para asegurar la propiedad intelectual de la reivindicación 1, donde los datos de derechos incluyen un número límite de reproducciones, y donde el registro de reproductor incluye además un número de reproducciones contado, y donde comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluye además determinar que el número de reproducciones contado no excede del número límite de reproducciones.

4. El método para asegurar la propiedad intelectual de la reivindicación 1, donde los datos de derechos incluyen un final de tiempo de reproducción, el registro de reproductor incluye además una hora actual, y comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluye además determinar que la hora actual no es posterior al final del tiempo de reproducción.

5. El método para asegurar la propiedad intelectual de la reivindicación 1, donde los datos de derechos incluyen una fecha final, el registro de reproductor incluye además una fecha actual, y comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluye además determinar que la fecha actual no es posterior a la fecha final.

6. El método para asegurar la propiedad intelectual de la reivindicación 1, donde el al menos único código de componente se selecciona a partir del grupo que consta de un código de facturación, un código de reproductor en forma de un identificador de reproductor, y su combinación.

7. El método para asegurar la propiedad intelectual de la reivindicación 1, donde el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido, se selecciona a partir del grupo que consta de un código de hora y fecha, un código de cookie último, y su combinación.

8. El método para asegurar la propiedad intelectual de la reivindicación 7, donde el al menos único código de componente se selecciona a partir del grupo que consta de un código de facturación, un código de reproductor en forma de un reproductor, y su combinación.

9. El método para asegurar la propiedad intelectual de la reivindicación 8, donde la clave privada se crea usando un código de facturación, un código de reproductor, un código de hora y fecha, y un código de cookie último.

10. Un sistema para asegurar la propiedad intelectual distribuida electrónicamente incluyendo:

una red;

un reproductor conectado a la red, incluyendo el reproductor un procesador, un dispositivo de almacenamiento conectado al procesador, y memoria;

incluyendo además el dispositivo de almacenamiento un registro de datos de reproductor;

incluyendo además el registro de datos de reproductor al menos un código de componente que ha sido compartido con un proveedor de propiedad intelectual durante un contacto previo y al menos un código de componente adicional determinado al tiempo en que un producto de propiedad intelectual es pedido al proveedor de propiedad intelectual; y

incluyendo la memoria instrucciones de software, incluyendo las instrucciones de software instrucciones para:

recibir por la red el producto de propiedad intelectual, donde el producto de propiedad intelectual incluye además datos de contenido y datos de derechos en forma digital y se encripta con una clave privada antes de ser distribuido electrónicamente, y donde la clave privada no es distribuida electrónicamente y la clave privada se crea usando el al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido;

guardar el producto de propiedad intelectual en el dispositivo de almacenamiento,

desencriptar el producto de propiedad intelectual con una copia de cliente de la clave privada usada para encriptar el producto de propiedad intelectual, donde la copia de cliente de la clave privada es creada por el reproductor usando el al menos único código de componente y el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido;

comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido; y

reproducir los datos de contenido en el reproductor si el derecho ha sido determinado.

11. El sistema para asegurar la propiedad intelectual de la reivindicación 10, donde los datos de derechos incluyen un identificador de reproductor, y donde el registro de reproductor incluye además un identificador específico de reproductor único para el reproductor, y donde las instrucciones de software para comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluyen además instrucciones para determinar que el identificador de reproductor y el identificador específico de reproductor son los mismos.

12. El sistema para asegurar la propiedad intelectual de la reivindicación 10, donde los datos de derechos incluyen un número límite de reproducciones, y donde el registro de reproductor incluye además un número de reproducciones contado, y donde las instrucciones de software para comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluyen además instrucciones para determinar que el número de reproducciones contado no excede del número límite de reproducciones.

13. El sistema para asegurar la propiedad intelectual de la reivindicación 10, donde los datos de derechos incluyen un final de tiempo de reproducción, el registro de reproductor incluye además una hora actual, y donde las instrucciones de software para comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluyen además instrucciones para determinar que la hora actual no es posterior al final del tiempo de reproducción.

14. El sistema para asegurar la propiedad intelectual de la reivindicación 10, donde los datos de derechos incluyen una fecha final, el registro de reproductor incluye además una fecha actual, y las instrucciones de software para comparar los datos de derechos y el registro de datos de reproductor para determinar el derecho a reproducir los datos de contenido incluyen además instrucciones para determinar que la fecha actual no es posterior a la fecha final.

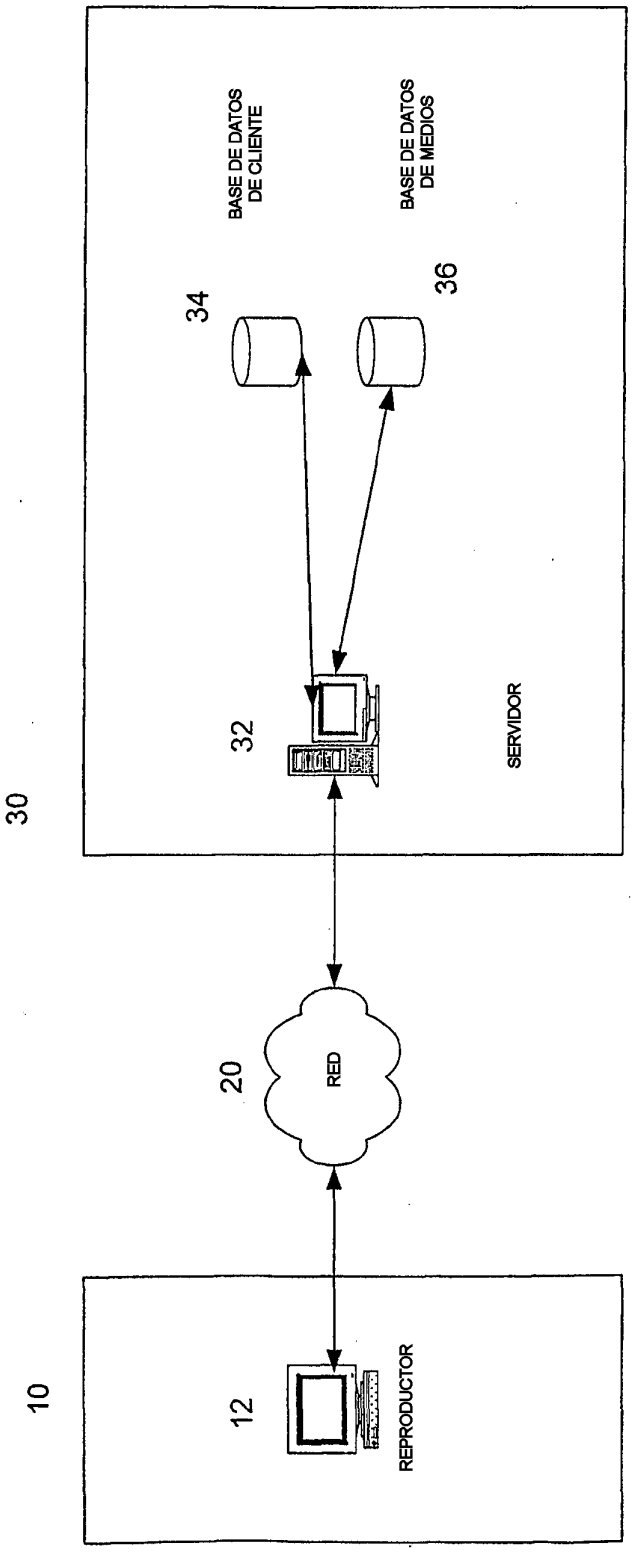
15. El sistema para asegurar la propiedad intelectual de la reivindicación 10, donde el al menos único código de componente se selecciona a partir del grupo que consta de un código de facturación, un código de reproductor en forma de un identificador de reproductor, y su combinación.

16. El sistema para asegurar la propiedad intelectual de la reivindicación 15, donde el al menos único código de componente adicional determinado al tiempo en que el producto de propiedad intelectual es pedido, se selecciona a

partir del grupo que consta de un código de hora y fecha, un código de cookie último, y su combinación.

17. El sistema para asegurar la propiedad intelectual de la reivindicación 15, donde la clave privada se crea usando un código de facturación, un código de reproductor, un código de hora y fecha, y un código de cookie último.

FIG. 1


BASE DE DATOS DE CLIENTE
BASE DE DATOS DE MEDIOS
34
36
32
SERVIDOR
30
20
RED
12
REPRODUCTOR
10

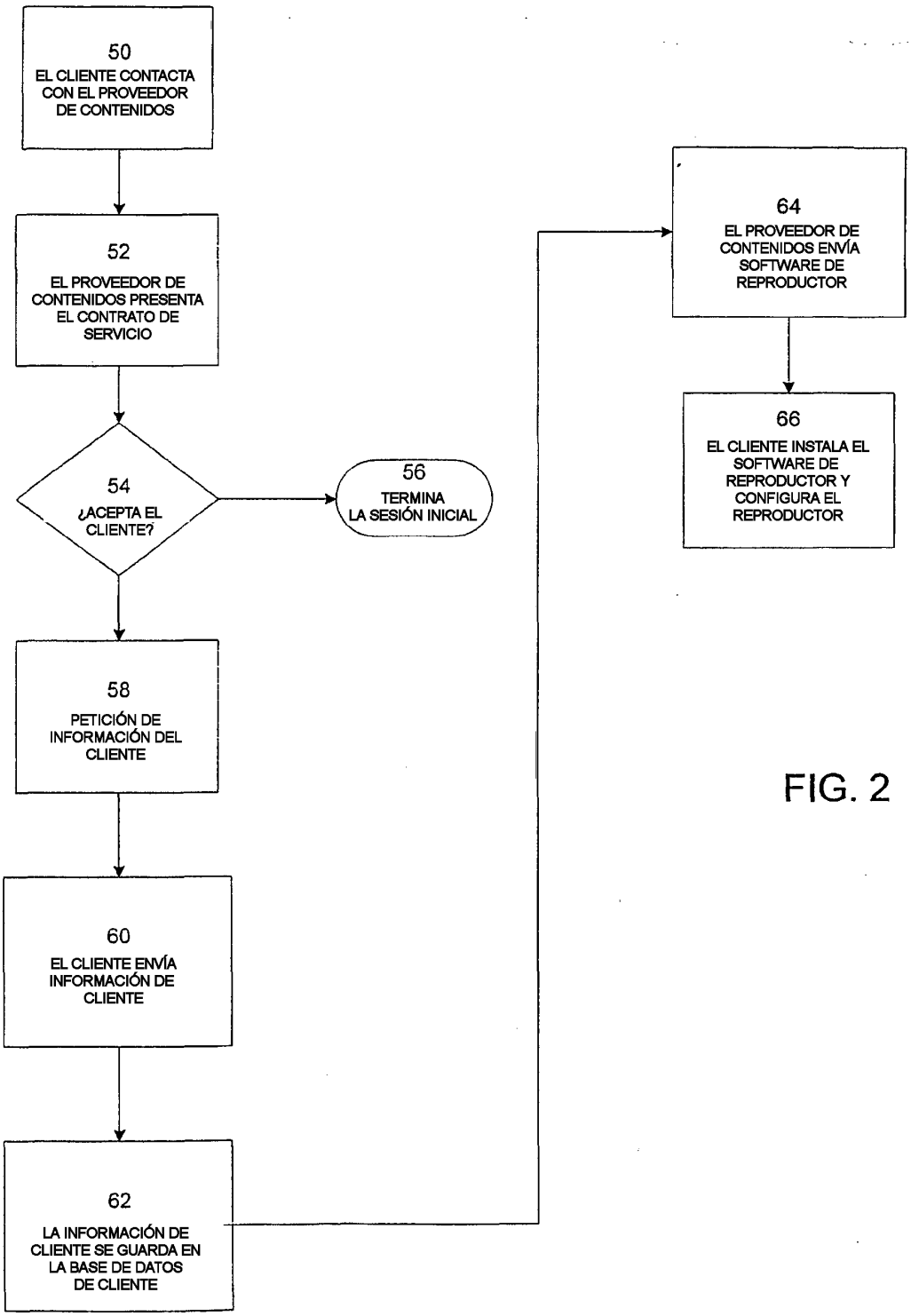

50
EL CLIENTE CONTACTA CON EL PROVEEDOR DE CONTENIDOS
52
EL PROVEEDOR DE CONTENIDOS PRESENTA EL CONTRATO DE SERVICIO
54
¿ACEPTA EL CLIENTE?
56
TERMINA LA SESIÓN INICIAL
58
PETICIÓN DE INFORMACIÓN DEL CLIENTE
60
EL CLIENTE ENVÍA INFORMACIÓN DE CLIENTE
62
LA INFORMACIÓN DE CLIENTE SE GUARDA EN LA BASE DE DATOS DE CLIENTE
64
EL PROVEEDOR DE CONTENIDOS ENVÍA SOFTWARE DE REPRODUCTOR
66
EL CLIENTE INSTALA EL SOFTWARE DE REPRODUCTOR Y CONFIGURA EL REPRODUCTOR

FIG. 2

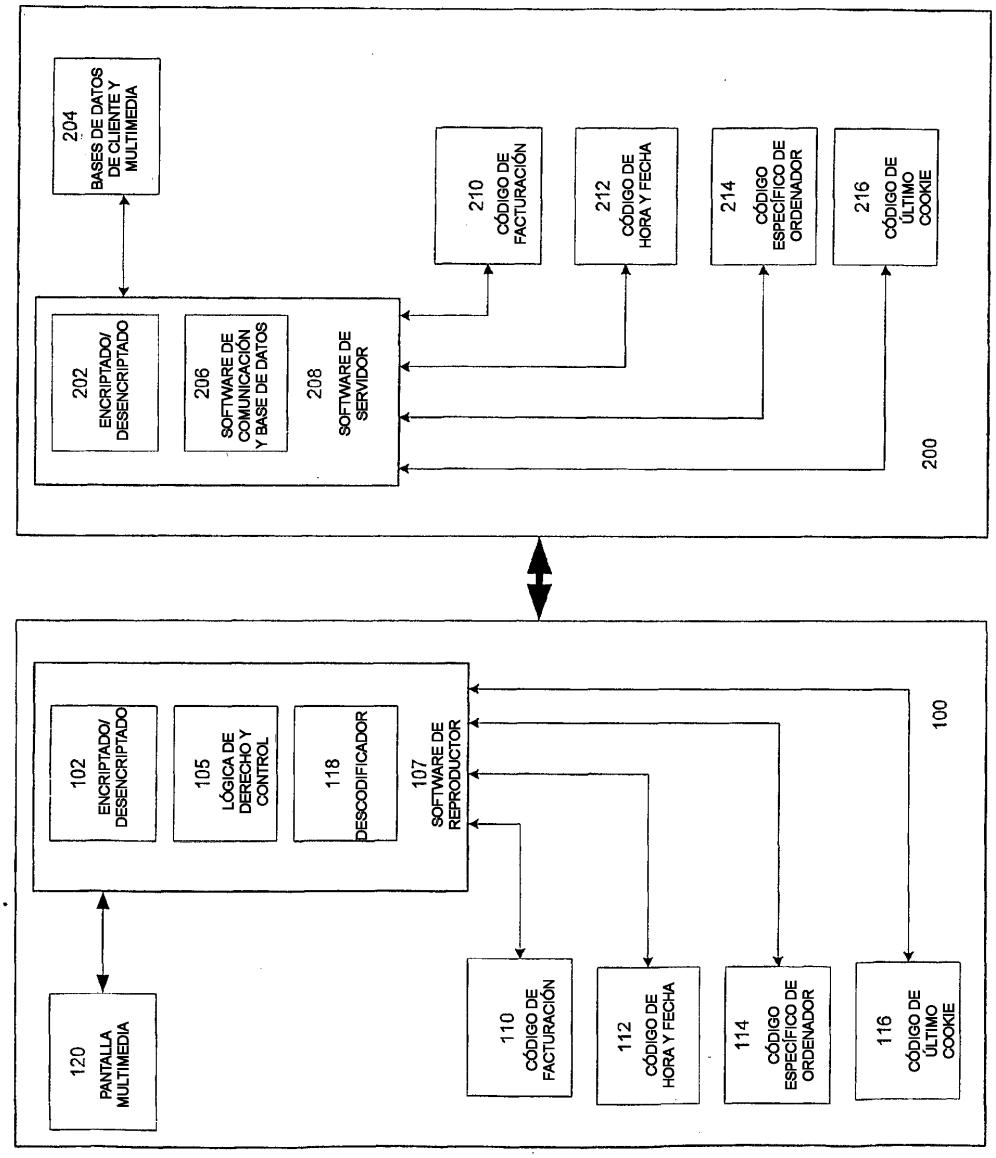

204
BASES DE DATOS DE CLIENTE Y MULTIMEDIA
202
ENCRIPTADO/ DESENCRIPTADO
206
SOFTWARE DE COMUNICACIÓN Y BASE DE DATOS
208
SOFTWARE DE SERVIDOR
210
CÓDIGO DE FACTURACIÓN
212
CÓDIGO DE HORA Y FECHA
214
CÓDIGO ESPECÍFICO DE ORDENADOR
216
CÓDIGO DE ÚLTIMO COOKIE
200
102
ENCRIPTADO/ DESENCRIPTADO
105
LÓGICA DE DERECHO Y CONTROL
118
DESCODIFICADOR
107
SOFTWARE DE REPRODUCTOR
100
120
PANTALLA MULTIMEDIA
110
CÓDIGO DE FACTURACIÓN
112
CÓDIGO DE HORA Y FECHA
114
CÓDIGO ESPECÍFICO DE ORDENADOR
116
CÓDIGO DE ÚLTIMO COOKIE

FIG. 3

FIG. 4

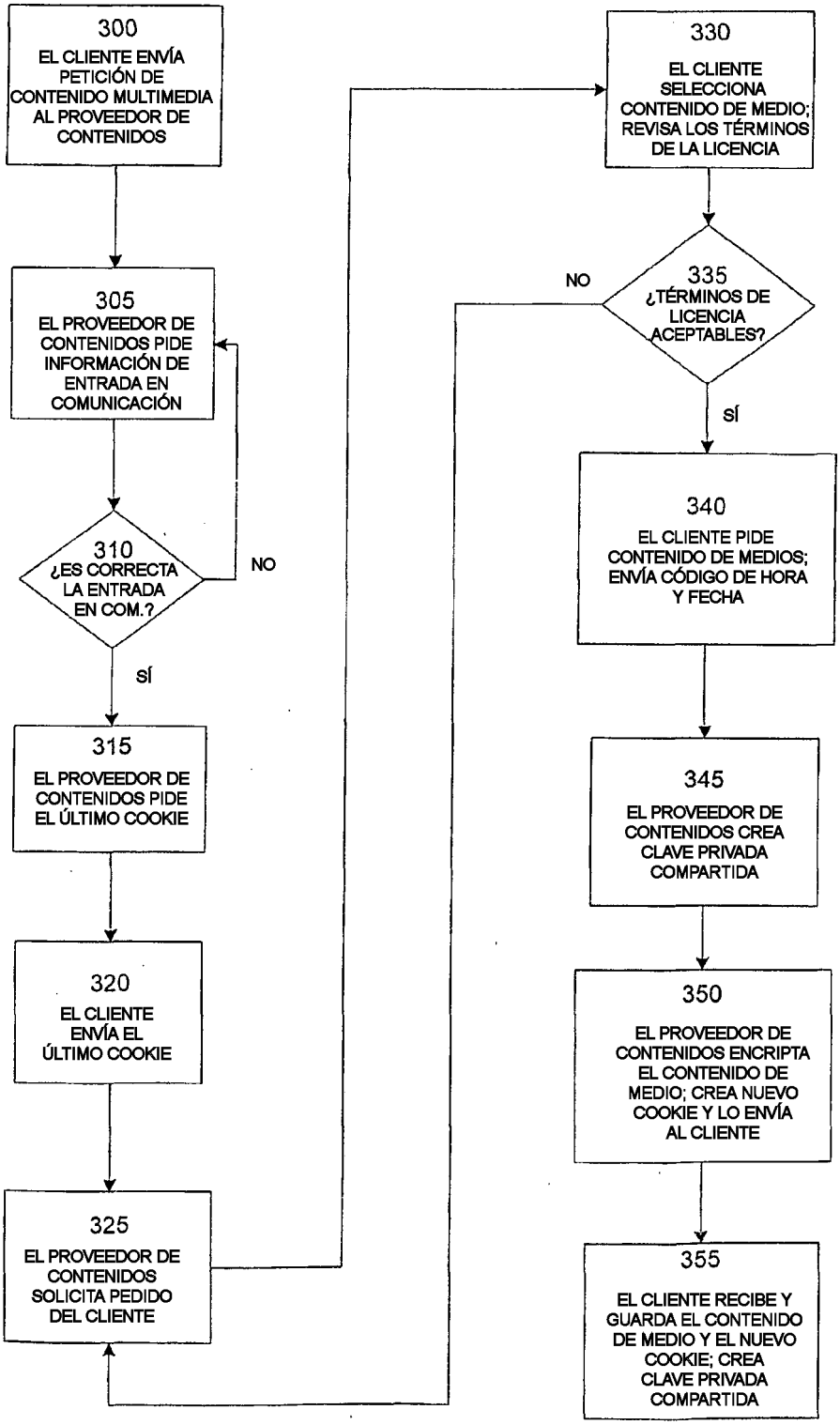
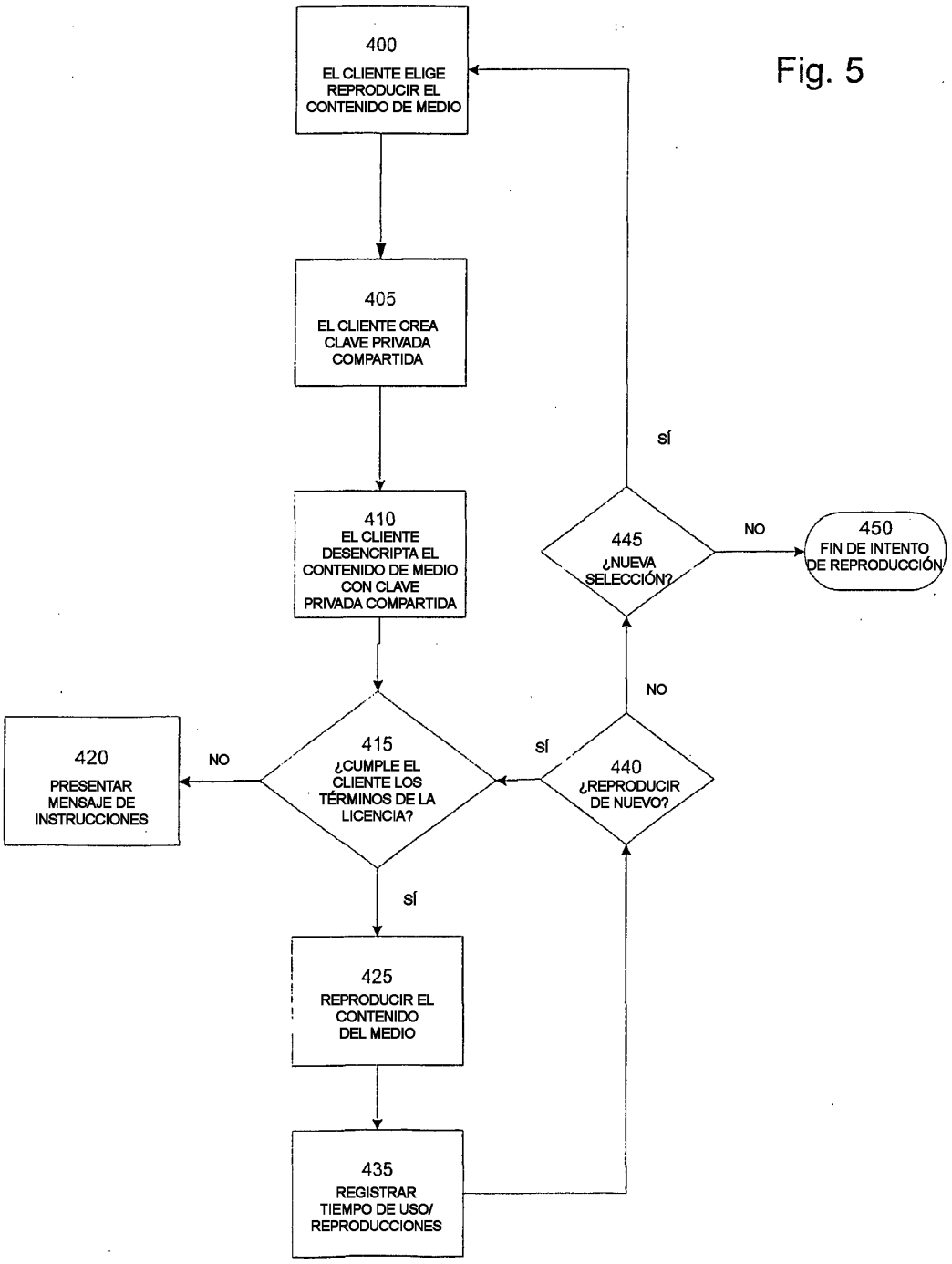

300
EL CLIENTE ENVÍA PETICIÓN DE CONTENIDO MULTIMEDIA AL PROVEEDOR DE CONTENIDOS
305
EL PROVEEDOR DE CONTENIDOS PIDE INFORMACIÓN DE ENTRADA EN COMUNICACIÓN
310
¿ES CORRECTA LA ENTRADA EN COM.?
NO
SÍ
315
EL PROVEEDOR DE CONTENIDOS PIDE EL ÚLTIMO COOKIE
320
EL CLIENTE ENVÍA EL ÚLTIMO COOKIE
325
EL PROVEEDOR DE CONTENIDOS SOLICITA PEDIDO DEL CLIENTE
330
EL CLIENTE SELECCIONA CONTENIDO DE MEDIO; REVISA LOS TÉRMINOS DE LA LICENCIA
335
¿TÉRMINOS DE LICENCIA ACEPTABLES?
NO
SÍ
340
EL CLIENTE PIDE CONTENIDO DE MEDIOS; ENVÍA CÓDIGO DE HORA Y FECHA
345
EL PROVEEDOR DE CONTENIDOS CREA CLAVE PRIVADA COMPARTIDA
350
EL PROVEEDOR DE CONTENIDOS ENCRIPTA EL CONTENIDO DE MEDIO; CREA NUEVO COOKIE Y LO ENVÍA AL CLIENTE
355
EL CLIENTE RECIBE Y GUARDA EL CONTENIDO DE MEDIO Y EL NUEVO COOKIE; CREA CLAVE PRIVADA COMPARTIDA

Fig. 5


400
EL CLIENTE ELIGE REPRODUCIR EL CONTENIDO DE MEDIO
405
EL CLIENTE CREA CLAVE PRIVADA COMPARTIDA
410
EL CLIENTE DESENCRIPTA EL CONTENIDO DE MEDIO CON CLAVE PRIVADA COMPARTIDA
415
¿CUMPLE EL CLIENTE LOS TÉRMINOS DE LA LICENCIA?
NO
420
PRESENTAR MENSAJE DE INSTRUCCIONES
SÍ
425
REPRODUCIR EL CONTENIDO DEL MEDIO
435
REGISTRAR TIEMPO DE USO/ REPRODUCCIONES
440
¿REPRODUCIR DE NUEVO?
SÍ
NO
445
¿NUEVA SELECCIÓN?
NO
450
FIN DE INTENTO DE REPRODUCCIÓN
SÍ