(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 396 249**

(51) Int. CI.:

H04N 7/16 (2011.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.03.2007 E 07731677 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.10.2012 EP 1994745**

(54) Título: **Procedimiento para la distribución protegida de sucuencias audiovisuales, descodificador y sistema para la puesta en marcha de este procedimiento**

(30) Prioridad:

10.03.2006 FR 0650814

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.02.2013

(73) Titular/es:

NAGRA FRANCE SAS (100.0%)
28, RUE DU COLONEL PIERRE AVIA
75015 PARIS, FR

(72) Inventor/es:

LECOMTE, DANIEL y
FOLEA, OCTAVIAN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Procedimiento para la distribución protegida de secuencias audiovisuales, descodificador y sistema para la puesta en marcha de este procedimiento

[0001] La presente invención se refiere al ámbito de la distribución protegida de secuencias audiovisuales.

[0002] Una técnica de protección de una secuencia audiovisual consiste en alterar, en el momento de la difusión, el flujo audiovisual digital para que sea compatible con los formatos estándar y pueda ser reconocido por un equipo de lectura, pero no pueda ser visto o comprendido, es decir, consumido en estas condiciones de una manera satisfactoria por un destinatario. Se transmite una información complementaria por una vía separada. Sólo la combinación del flujo digital principal y de esta información complementaria permite el consumo de la secuencia audiovisual inicial.

[0003] El usuario dispone de un descodificador que recibe dicho flujo digital principal, igualmente llamado flujo audiovisual modificado, así como la información complementaria. Este descodificador debe disponer de un medio de almacenamiento masivo para asegurar un tampón entre el flujo que entra, que se puede limitar por la cantidad de conexión entre el descodificador y la red, y el procesador audiovisual que asegura la recomposición. Además, el almacenamiento masivo debe estar protegido contra los eventuales intentos de recuperación de la secuencia audiovisual inicial. Se trata, por lo tanto, de un equipo relativamente caro, limitando las posibilidades de difusión de secuencias según esta técnica.

[0004] A fin de dar respuesta a este problema general, la solicitud WO 2004/066627 propone la puesta en marcha de un descodificador simplificado, siempre garantizando una gran seguridad contra el pirateo, por un procedimiento para la distribución de secuencias de vídeo que consiste en difundir un flujo digital principal y una información complementaria necesaria para la visualización de la secuencia de vídeo, y en reconstruir en el sito de recepción el flujo de vídeo visualizable en un equipo provisto de una pantalla, caracterizado por el hecho de que el sito de recepción incluye un ordenador personal que cuenta con una conexión de alta velocidad y medios de almacenamiento masivo, y un periférico de tratamiento vídeo provisto de medios de comunicación con dicho ordenador personal y de transmisión del flujo visualizable a un dispositivo de visualización, el flujo digital principal siendo recibido por dicho ordenador personal, la aplicación de software de reconstrucción del flujo de visualización siendo ejecutada en el periférico de tratamiento vídeo y no en el ordenador personal.

[0005] Sin embargo, este tipo de procedimiento presenta el inconveniente de que proporciona un nivel de seguridad limitado con respecto a los ataques que tienen como objetivo la recuperación ilícita de la secuencia de vídeo. Esta limitación viene dada por el ordenador personal que se encarga de la identificación y la autentificación del usuario, así como de la transmisión de la información complementaria hacia el periférico de tratamiento de vídeo.

[0006] La arquitectura física del ordenador personal es abierta, lo que permite a todos sus usuarios un acceso total y no restrictivo a cada uno de sus componentes del sistema: la memoria de acceso aleatorio, el procesador, los medios de almacenamiento o las interfaces de entrada/salida. De este modo, un pirata dispone de todos los medios para interceptar la información complementaria claramente en las interfaces de entrada/salida o memoria de acceso aleatorio en el momento de su tratamiento por el ordenador personal.

[0007] A la vista del documento WO 2004/066627, el problema resuelto por la invención es mejorar la seguridad del procedimiento de distribución de secuencias de vídeo.

[0008] Este problema se resuelve gracias a un procedimiento tal y como se ha descrito en la reivindicación 1.

[0009] Gracias a la utilización de la pasarela protegida, la presente invención permite controlar la transmisión protegida de dicha información complementaria hacia el periférico de tratamiento de vídeo por una pasarela protegida en lugar de un ordenador personal como en el documento anteriormente mencionado.

[0010] Es conocido que una pasarela protegida es un dispositivo que incluye:

- una arquitectura física cerrada que impide el acceso no autorizado a al menos un componente de software o físico por medios materiales,
- un núcleo protegido que regula el acceso autorizado a al menos un componente de software o físico por diferentes niveles de seguridad, que varían desde un acceso total hasta la prohibición total.

[0011] De manera optativa, dicha pasarela protegida puede igualmente ser de manera que el compuesto incluya los medios para almacenar una información que permita la identificación única de la pasarela protegida, dicha información siendo grabada en el momento de la creación de dicho componente y no pudiendo ser modificada posteriormente.

[0012] Es evidente para el experto en la materia que el ordenador personal tal y como el empleado por la solicitud WO 2004/066627 no contiene ningún componente que responda a los criterios que definen la pasarela protegida dado que:

- la arquitectura física del ordenador personal es abierta, lo que permite un acceso total y no restrictivo a todos los componentes de dicho ordenador personal (la memoria de acceso aleatorio, el procesador, los medios de

almacenamiento, las interfaces de entrada/salida, etc.);
- el ordenador personal ofrece al usuario los medios (el teclado, la pantalla, la impresora, etc.) para la visualización y la modificación de los datos que son tratados o transportados por dichos componentes en cada momento durante su estado operativo;
- la arquitectura abierta del ordenador facilita al usuario la extracción de cada componente y su utilización con ayuda de otro ordenador personal o un tipo de dispositivo de tratamiento totalmente distinto;
- el ordenador personal no contiene ningún componente capaz de impedir la modificación de una información capaz de identificar de manera única dicho ordenador personal.

[0013] Un ejemplo no limitativo de un dispositivo que responde a los criterios de una pasarela protegida es la tarjeta de chip. Dicha tarjeta contiene un núcleo protegido que protege el acceso a sus componentes: las memorias tipo ROM (Read Only Memory), PROM (Programable Read Only Memory) y EEPROM (Electrically Erasable read Only Memory). La memoria ROM es escrita por el fabricante y no puede ser modificada después. La memoria PROM contiene una información que permite la identificación única de la tarjeta de chip. El acceso a la memoria EEPROM se permite según los niveles de seguridad. La tarjeta de chip es por ejemplo del formato estándar ISO 7816, e incluye, de manera conocida en sí una arquitectura física cerrada que impide el acceso no autorizado a sus componentes de software o físicos por unos medios materiales como la miniaturización y la explotación de los campos magnéticos. Gracias a estas características, el acceso no autorizado a los componentes de una tarjeta de chip requiere dispositivos y componentes extremadamente sofisticados y costosos que no están al alcance del público.

[0014] Las tarjetas de chip tienen una multitud de usos en dispositivos heterogéneos: teléfonos móviles, tarjetas bancarias, tarjetas de acceso, etc. Con respecto a los ordenadores personales, los teléfonos portátiles con una tarjeta de chip (la tarjeta SIM - Subscriber Identity Module) tienen una presencia más amplia en el mercado y aportan al usuario una mejor ergonomía y sencillez de uso.

[0015] El estado de la técnica conoce cada vez más la proliferación de equipos de red que contienen los componentes protegidos que permiten, de un lado, la protección de flujos de datos que circulan en la red y, de otro lado, el acceso a los parámetros de configuración de dichos equipos. A la vista de estas características, el experto en la materia considera dichos equipos como pasarelas protegidas.

[0016] Es sorprendente para el experto en la materia que la protección de un flujo audiovisual pueda ser realizada por una tarjeta de chip, particularmente por el hecho de que la tarjeta de chip tiene poca capacidad de memoria y una potencia de cálculo limitada. La solicitante ha descubierto, sin embargo, que dicha tarjeta de chip puede realizar esta función de protección del flujo audiovisual asegurando y, particularmente, realizando las operaciones criptográficas sobre una información complementaria diferenciada del flujo audiovisual nominal.

[0017] La información complementaria depende del tipo de contenido audiovisual que se va a transmitir. Esta información complementaria puede, por ejemplo, ser generada como en la solicitud WO 2004/032418 para una secuencia de audio, o como en la solicitud WO 2003/063445 para una secuencia audiovisual de formato MPEG. La información complementaria puede igualmente incluir informaciones personalizadas en función del destinatario como en la solicitud WO 2004/073311, o informaciones de marcación visible como en la solicitud WO 2004/062281 o invisible como en la solicitud 06/55315. Al igual que en estas solicitudes, el flujo digital principal es preferentemente generado extrayendo al menos un coeficiente del flujo nominal y insertando este o estos coeficientes extraídos en la información complementaria.

[0018] En todos estos casos, como en la invención, el tratamiento de la información complementaria y del flujo digital principal por un módulo de síntesis permite consumir el flujo nominal, por ejemplo reconstruyendo este flujo de forma idéntica, o añadiéndole los datos visibles o invisibles cuando el flujo digital principal no es consumible en el equipo destinatario en ausencia de información complementaria.

[0019] Puesto que la información complementaria puede ser de tamaño reducido, y normalmente es el 1% del tamaño del flujo audiovisual nominal, la protección por tarjeta de chip es posible realizando las operaciones criptográficas sobre la información complementaria y no sobre el conjunto del contenido del flujo audiovisual nominal.

[0020] La invención se refiere por lo tanto ventajosamente a la utilización de una tarjeta de chip para proteger la distribución de un flujo audiovisual, particularmente realizando operaciones criptográficas de la información complementaria.

[0021] Se puede observar que en la solicitud WO 2004/066627 el ordenador personal incluye un lector de tarjeta y es susceptible de recibir una tarjeta de chip. Sin embargo, en este documento, la tarjeta de chip no realiza ninguna función criptográfica, únicamente funciones de autentificación y de almacenamiento. En la solicitud WO 2004/066627, todas las funciones criptográficas de protección son realizadas por el ordenador personal, con las desventajas mencionadas anteriormente.

[0022] La pasarela protegida según la invención puede, además, realizar las funciones de autentificación y de almacenamiento como lo hacía el ordenador asociado al lector de tarjeta de chip de la solicitud WO 2004/066627.

[0023] La utilización de la pasarela protegida permite mejorar la seguridad del procedimiento de distribución y permite, por lo tanto, particularmente resolver el problema anteriormente mencionado.

[0024] Además, el flujo digital principal es transmitido por el servidor por medio de una red digital, el periférico de tratamiento audiovisual (2) incluye una conexión de banda ancha para recibir dicho flujo digital principal.

[0025] Ventajosamente, el flujo digital principal se transmite por el servidor por medio de un soporte físico, el periférico de tratamiento audiovisual (2) incluye un lector para explotar dicho soporte físico y leer dicho flujo digital principal.

[0026] Ventajosamente, el flujo digital principal se transmite por la pasarela protegida o por un ordenador personal v mediante las conexiones alámbricas, por ejemplo del tipo Ethernet, FIREWIRE o USB-2, o por una de las conexiones inalámbricas, por ejemplo del tipo Bluetooth, WiFi o AirPort, el periférico de tratamiento audiovisual (2) incluye una o varias interfaces capaces de recibir dicho flujo digital principal.

[0027] Según una primera variante, el flujo digital principal es recibido directamente por el periférico de tratamiento audiovisual.

[0028] Según una segunda variante, el flujo digital principal es recibido por un ordenador personal situado cerca del periférico de tratamiento audiovisual, dicho flujo digital principal es transmitido por una conexión de red local al periférico de tratamiento audiovisual.

[0029] Según una tercera variante, el flujo digital principal se almacena en un periférico de almacenamiento que puede ser leído por el periférico de tratamiento audiovisual.

[0030] Según una cuarta variante, el flujo digital principal es recibido por la pasarela protegida antes de ser transmitido al periférico de tratamiento audiovisual.

[0031] En todos los casos, la información complementaria es recibida por la pasarela protegida antes de ser transmitida al periférico de tratamiento audiovisual.

[0032] En otra variante, el flujo digital principal es conforme con la norma o los estándares del flujo audiovisual original.

[0033] Ventajosamente, los derechos digitales sobre el consumo del flujo digital principal se transmiten por un servidor y se adquieren a través de la pasarela protegida.

[0034] En un modo de realización, la pasarela protegida incluye un módulo de protección para la recepción de la información complementaria transmitida por el servidor. Además, ésta incluye un módulo de enrutamiento para la información complementaria entre la pasarela protegida y el periférico de tratamiento audiovisual del descodificador.

[0035] Ventajosamente, la pasarela protegida incluye un gestor de derechos digitales que condiciona el consumo de flujo digital principal por el periférico de tratamiento audiovisual (2).

[0036] Ventajosamente, se efectúa una autentificación entre el servidor audiovisual y la pasarela protegida en el momento de la solicitud de información complementaria.

[0037] Ventajosamente, se efectúa una autentificación requerida por el protocolo de transmisión de la información complementaria entre la pasarela protegida y el periférico de tratamiento audiovisual del descodificador. Ventajosamente, un componente de la autentificación es la verificación de los derechos digitales adquiridos anteriormente.

[0038] La invención se refiere igualmente a un descodificador que dispone de una entrada para recibir un flujo digital, un circuito de tratamiento audiovisual para recomponer un flujo consumible a partir de dicho flujo digital y de una información complementaria y una salida que entrega una señal audiovisual visualizable a un dispositivo de visualización y/o de escucha.

[0039] Preferentemente, el descodificador incluye un medio de comunicación con una red para recibir información complementaria.

[0040] Según una variante, éste incluye un medio de comunicación con la pasarela protegida para la recepción del flujo digital principal.

[0041] Según un modo de realización preferido, el descodificador incluye medios de comunicación inalámbricos con un ordenador personal para recibir el flujo digital.

[0042] La presente invención describe también un sistema para la puesta en marcha del procedimiento que incluye un descodificador, una pasarela protegida, el dispositivo incluyendo un lector de discos en los que se registran los flujos

digitales principales y el descodificador incluyendo medios de comunicación con dicho dispositivo para recibir el flujo digital principal.

[0043] La invención se comprenderá mejor tras la lectura de la descripción que sigue, haciendo referencia a los dibujos anexos que corresponden a los ejemplos no limitativos de realización, donde:

- la figura 1 representa el esquema de un descodificador según la invención;
- la figura 2 representa una primera variante de un descodificador según la invención.

[0044] Para la recepción y la explotación de las secuencias audiovisuales difundidas, cada usuario deberá disponer de dos equipos que son complementarios:

- una pasarela protegida (1),
- un descodificador (2).

[0045] En la figura 1, el descodificador (2) incluye una salida para conectar al menos un dispositivo de visualización y/o de escucha, por ejemplo un monitor, un vídeo proyector, un dispositivo tipo pantalla de televisión, un lector de contenidos de audio, una PDA o cualquier otro aparato como por ejemplo una cadena audiovisual (6).

[0046] El descodificador (2) incluye principalmente, por una parte, una unidad de tratamiento adaptada para tratar, particularmente descodificar, todo flujo audiovisual digital, por ejemplo tipo MPEG según un programa de software de descodificación precargado, para visualizarlo en tiempo real y, por otra parte, al menos una interfaz audiovisual (7).

[0047] El descodificador está también conectado a una pasarela (1) por una o varias conexiones con cable, por ejemplo tipo Ethernet, FIREWIRE o USB-2, o por conexiones inalámbricas, por ejemplo tipo Bluetooth, WiFi o AirPort. La conexión (3) encauza la información complementaria y la conexión (4) encauza el flujo audiovisual modificado por el servidor para volverlo impracticable en estas condiciones.

[0048] Ventajosamente la conexión (3) se confunde con la conexión (4).

[0049] Cuando el usuario del descodificador (2) quiere realmente consumir en su cadena audiovisual (6) el programa audiovisual, realiza la solicitud al sistema de síntesis (8) con su mando a distancia como lo haría con una grabadora de video o un lector de DVD mediante un menú en su pantalla de televisión (6). El descodificador dialoga con la pasarela protegida (1) para iniciar el envío del flujo audiovisual modificado. El sistema de síntesis (8) comienza a analizar el flujo digital modificado que proviene del disco duro (10) del descodificador a través del tampón de lectura (11) del descodificador. El descodificador (2) establece entonces una conexión con el servidor audiovisual a través de la red de telecomunicación (12) que es en nuestro ejemplo una conexión a Internet tipo ADSL o una conexión a una red local.

[0050] Ventajosamente, el mando a distancia está integrado en la pasarela protegida (1).

[0051] El disco duro (10) del descodificador (2) se puede utilizar como memoria tampón para almacenar, al menos momentáneamente, una parte del programa o de la secuencia audiovisual que se va a consumir, en caso de visualización diferida o de limitación del ancho de banda de la red de transmisión (12). El consumo puede ser retardado o diferido a petición del usuario o del servidor audiovisual.

[0052] Ventajosamente, el lector de disco (10) se sitúa fuera del descodificador (2) y está conectado a éste por una conexión alámbrica de tipo USB-2, FIREWIRE o una conexión del descodificador (2).

[0053] Como se muestra en la figura 1, la interfaz de conexión (5) del descodificador (2) está conectada a una red de transmisión y de difusión de banda ancha (12) tal como un módem, un módem satélite, un módem de cable, de una interfaz de línea de fibra óptica o de una interfaz de radio o infrarroja para comunicación inalámbrica.

[0054] Esta conexión tradicional de difusión audiovisual es a través de la cual se transmitirán los contenidos de los programas audiovisuales como por ejemplo películas. Sin embargo, para no permitir hacer copias piratas, antes de transmitir el contenido audiovisual desde el servidor está previsto conservar una pequeña parte del contenido audiovisual en el portal o el servidor audiovisual.

[0055] En caso de consumo de un programa audiovisual en tiempo real, esta pequeña parte del contenido audiovisual, llamada también información complementaria, que se conserva en el servidor será enviada también al módulo de interfaz (15) a través de la red de telecomunicación (13) que puede ser la misma red que la de transmisión y difusión del ancho banda (12).

[0056] Ventajosamente, el módulo (15) incluye una función de enrutamiento (14) que permite transferir los datos entre el servidor audiovisual y el descodificador (2) de manera que la pasarela protegida (1) no efectúe ningún tratamiento específico sobre dichos datos.

[0057] Dado que las imágenes sucesivas de una secuencia audiovisual tienen un gran número de elementos visuales idénticos (como en el cine, una imagen se asemeja a la precedente), MPEG no registra más que los elementos que

difieren de la imagen de origen. Por ejemplo, y sin que este ejemplo sea limitativo de la invención, se modifica una imagen entera de referencia conservando los coeficientes DC de las modificaciones enviadas al portal y para las imágenes sucesivas que dependen de esta imagen I de referencia no es necesario aportar las modificaciones ya que éstas harán divergir el flujo consumido debido a las perturbaciones aportadas a las imágenes I de referencia. La compresión en MPEG comienza por lo tanto, en primer lugar, por descomponer la imagen en diferentes matrices cuadradas que incluyen varios puntos o píxeles, cada uno con su propio valor colorimétrico. Un cálculo permite obtener un valor medio para cada matriz dentro de la cual cada punto está ahora ahogado. Este tratamiento genera una pixelación y la aparición de colores uniformes allí adonde existan matices de color. La segunda etapa de la compresión en MPEG consiste en conservar de una imagen a otra sólo los elementos cambiantes.

[0058] En el caso de un programa audiovisual tipo MPEG, todas las características de las imágenes I que provienen del servidor audiovisual no se transmiten hacia el módulo (5). En particular, las características pueden ser los coeficientes de correlación DC contenidos en las imágenes I.

[0059] Ciertos coeficientes DC de estas imágenes I se conservan en el servidor audiovisual. En cambio, en lugar de los coeficientes DC de estas imágenes I no transmitidos, el servidor intercalará falsos coeficientes DC de la misma naturaleza que los coeficientes DC liberados y conservados en el portal, de manera que el Lector estándar de MPEG del módulo (8) no sea perturbado por estas modificaciones que ignorará y reconstituirá al sacar un flujo de salida MPEG que no será correcto desde el punto de vista visual para un ser humano pero será correcto desde el punto de vista del formato MPEG, es decir, el flujo digital principal que contiene los falsos coeficientes DC concuerda con la norma MPEG. De manera general, las modificaciones en los coeficientes se efectúan de tal manera que el flujo digital principal modificado concuerde estrictamente con la norma o el estándar de flujo audiovisual digital original.

[0060] El lector MPEG (8) del descodificador (2) es un lector estándar MPEG y no está modificado o afectado de ningún modo por los cambios de las imágenes I.

[0061] Como se muestra en la figura 1, la interfaz de conexión de la pasarela protegida (1) está conectada a una red de telecomunicación extendida directamente o por una red local que sirve de red de acceso y está constituida, por ejemplo, por una interfaz de línea de abonado (red telefónica analógica o digital, ADSL, BLR, GSM, GPRS, UMTS, etc.).

[0062] Por lo tanto, los programas audiovisuales son difundidos de manera tradicional en modo multidifusión («broadcast») a través de la red de transmisión de banda ancha (12) tipo hertziana, por cable, por satélite, hertziana digital, ADSL, etc. Cada programa audiovisual difundido de este modo puede ser codificado o no y los flujo tipo MPEG tienen modificaciones en ciertas imágenes I como se ha descrito anteriormente. En función de los parámetros elegidos por el usuario o de las informaciones transmitidas por el servidor de difusión, ciertos programas audiovisuales modificados de este modo e incompletos se graban en el disco duro del ordenador (1).

[0063] Cuando el usuario desea consumir un programa audiovisual grabado de este modo en el disco duro (10) de su descodificador (2) se conectará entonces al portal a través de la conexión de tipo red local o acceso aleatorio o directo y a través de la red de telecomunicación se conecta él mismo al servidor audiovisual.

[0064] Durante todo el tiempo que dura el consumo del programa audiovisual, las conexiones permanecen establecidas y permiten que la pasarela protegida (1) reciba a través de la conexión (13) las funciones y los parámetros de reparación en el orden de los coeficientes DC modificados de las imágenes I. El flujo digital principal proveniente del disco duro del descodificador (2) y la información complementaria proveniente del servidor audiovisual a través de la conexión (13) se transmiten al descodificador (2) a través de las conexiones (4) y (3) respectivamente. La combinación del flujo digital principal y de esta información complementaria permite sólo el consumo de la secuencia audiovisual inicial. Los coeficientes DC modificados de las imágenes I transmitidos de este modo no se graban nunca en el disco duro del descodificador (2) porque las imágenes I reconstituidas aparecen directamente en la pantalla de visualización (6) a través del tratamiento efectuado por el descodificador (2) después de haber sido tratadas por el Lector (8) desde su memoria local volátil (81). Una vez tratados y visualizados, los coeficientes DC modificados y/o que faltan de las imágenes I que acaban de ser transmitidas por el servidor audiovisual serán borrados de la memoria volátil local (81) del descodificador (2).

[0065] Cada vez que el usuario quiera ver un programa grabado en el disco duro (10) del descodificador (2) éste se conectará automáticamente a la pasarela protegida (1). Según un modo de realización particular, la pasarela protegida (1) incluye un lector de tarjetas de chip (9) que permitirá al portal autenticar el usuario propietario de la pasarela protegida (1). La autentificación se efectúa entre el servidor audiovisual y la pasarela protegida en el momento de la solicitud de información complementaria. Cuando se lleva a cabo esta etapa de autentificación, la información relativa a dicha autentificación transita a través de la pasarela protegida (1).

[0066] Según un modo de realización particular, para un contenido audiovisual MPEG dado, la tarjeta de chip contiene dicha información complementaria.

[0067] Según un modo de realización particular, el consumo de un contenido audiovisual MPEG dado está condicionado por los derechos digitales. Los derechos digitales representan la información que precisa cuáles son las condiciones en

las que un contenido puede ser consumido: (a) el número de consumiciones del contenido, (b) la fecha de validez a partir de la cual el contenido puede ser consumido, (c) la fecha de expiración a partir de la cual el contenido ya no puede ser consumido, (d) el ámbito para el cual el consumo está permitido, (e) el tipo de descodificador (2) que permite el consumo, (f) etcétera.

[0068] Según una primera variante, los derechos digitales se reciben por la pasarela protegida (1) a través de la conexión (13).

[0069] Según una segunda variante, los derechos digitales se reciben por la pasarela protegida (1) a través del lector de tarjetas de chip (9).

[0070] La figura 2 representa una variante de realización en la que la pasarela protegida (1) se encarga de la recepción del flujo digital principal enviado por el servidor audiovisual y la transmisión de dicho flujo principal hacia el descodificador (2) por la red (13).

[0071] La primera etapa de autentificación se efectúa entre el servidor audiovisual y la pasarela protegida (2) en el momento de la solicitud de información complementaria.

[0072] La segunda etapa de autentificación se efectúa entre la pasarela protegida (1) y el descodificador (2) en el momento de la solicitud de consumo de las secuencias audiovisuales.

[0073] Ventajosamente, en las figuras 1 y 2 el descodificador (2) y respectivamente la pasarela protegida (1) tienen un lector de discos (16), por ejemplo un lector de CD o de DVD, para leer directamente los flujos digitales principales grabados en discos. Los flujos digitales principales se graban de antemano en dichos discos.

[0074] Ventajosamente, los derechos digitales son recibidos por la pasarela protegida (1) a través de la red de transmisión (12).

REIVINDICACIONES

1. Procedimiento para la distribución de un flujo audiovisual nominal a un sitio de recepción, el flujo audiovisual nominal incluyendo coeficientes nominales, el procedimiento incluye:

- una etapa que consiste en extraer en el flujo audiovisual nominal al menos un coeficiente nominal de dichos coeficientes nominales para generar un flujo digital principal según la norma o estándar del flujo audiovisual original;
- generar una información complementaria incluyendo los coeficientes extraídos del flujo nominal de manera que el flujo audiovisual nominal sea susceptible de ser consumido a partir de la información complementaria y del flujo digital principal que se encuentra en el sito de recepción,
- realizar operaciones criptográficas sobre la información complementaria,

el procedimiento se caracteriza por el hecho de que el sitio de recepción recibe el flujo digital principal y la información complementaria e incluye una pasarela protegida, y por el hecho de que el procedimiento incluye las etapas en las cuales:

- la pasarela protegida realiza las operaciones criptográficas sobre la información complementaria;
- la pasarela transmite la información complementaria a un periférico de tratamiento audiovisual para permitir el consumo del flujo audiovisual nominal a nivel d el periférico de tratamiento audiovisual, dicha pasarela incluye una arquitectura física cerrada que impide el acceso no autorizado a al menos un componente de software o físico por medios materiales, y un núcleo protegido que regula el acceso autorizado a al menos un componente de software o físico por diferentes niveles de seguridad, que varían desde un acceso total hasta la prohibición total.

2. Procedimiento según la reivindicación 1 en el cual la pasarela protegida incluye medios para almacenar una información que permite la identificación única de la pasarela protegida, dicha información se graba en el momento de la creación de dicho componente y no puede ser modificada posteriormente.

3. Procedimiento según cualquiera de las reivindicaciones precedentes en el que la pasarela protegida es una tarjeta de chip.

4. Procedimiento para la distribución de secuencias audiovisuales según cualquiera de las reivindicaciones 1 a 3, caracterizado por el hecho de que la información complementaria se recibe y transmite al periférico de tratamiento audiovisual por la pasarela protegida (1).

5. Procedimiento para la distribución de secuencias audiovisuales según la reivindicación 4, caracterizado por el hecho de que el flujo digital es recibido por la pasarela protegida (1) antes de ser transmitido al periférico de tratamiento audiovisual.

6. Procedimiento para la distribución de secuencias audiovisuales según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que se efectúa una primera autentificación entre un servidor audiovisual y la pasarela protegida cuando hay una solicitud de información complementaria a dicho servidor audiovisual.

7. Procedimiento para la distribución de secuencias audiovisuales según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que se efectúa una segunda autentificación entre la pasarela protegida y el periférico de tratamiento audiovisual cuando hay una solicitud de consumo.

8. Pasarela protegida para la puesta en marcha del procedimiento según una de las reivindicaciones 1 a 7, caracterizado por el hecho de que ésta incluye medios de recepción instalados para recibir la información complementaria y medios criptográficos instalados para realizar las operaciones criptográficas en la información complementaria.

9. Pasarela protegida según la reivindicación 8 que incluye una tarjeta de chip.

10. Pasarela protegida según una de las reivindicaciones 8 o 9, donde la pasarela protegida incluye al menos un componente físico cuyo acceso está regulado por al menos un nivel de seguridad.

11. Pasarela protegida según la reivindicación 10 en la que el componente incluye los medios para almacenar una información que permite la identificación única de la pasarela protegida, dicha información se graba en el momento de la creación de dicho componente y no se puede modificar posteriormente.

12. Pasarela protegida según una de las reivindicaciones 8 a 11, caracterizada por el hecho de que incluye un medio para la gestión de los derechos sobre el contenido.

13. Sistema para la puesta en marcha del procedimiento que incluye un descodificador que comporta un lector de discos en los cuales se graban los flujos digitales principales y además el descodificador incluye los medios de comunicación con la pasarela protegida (1) según una de las reivindicaciones 8 a 12, para recibir la información complementaria.

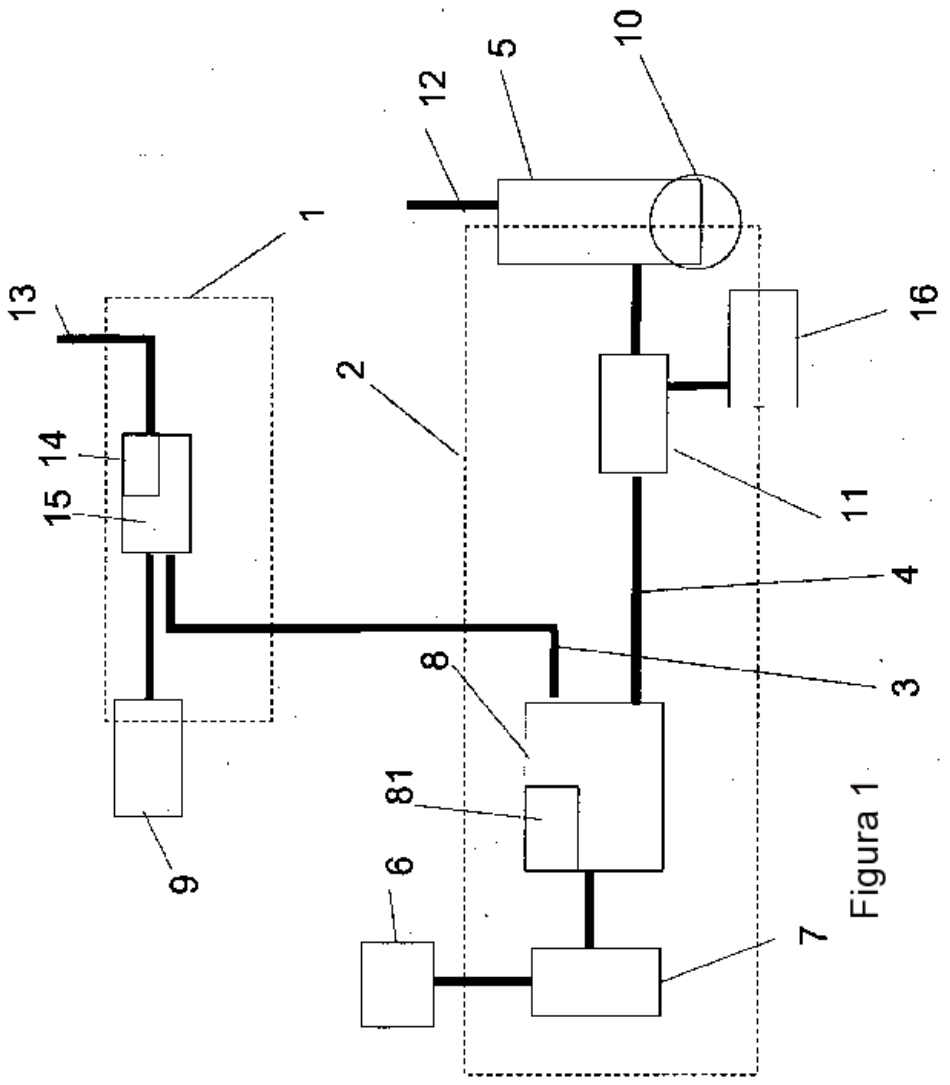

Figura 1

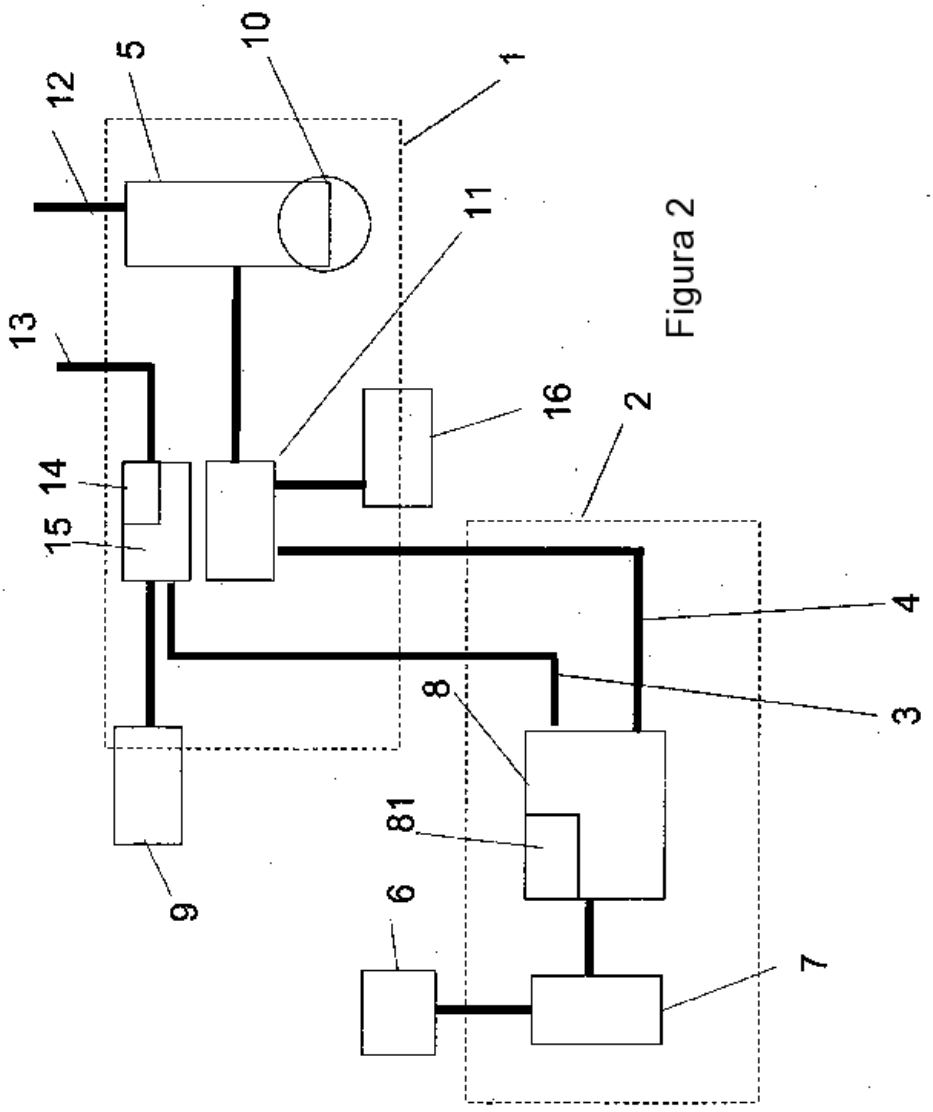

Figura 2