(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 357**

(51) Int. CI.:

G06F 21/10 (2013.01)
H04N 21/254 (2011.01)
H04N 21/262 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.06.2016 PCT/FR2016/051533**

(87) Fecha y número de publicación internacional: **05.01.2017 WO17001747**

(96) Fecha de presentación y número de la solicitud europea: **23.06.2016 E 16750886 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 3317799**

(54) Título: **Procedimiento de suministro de un contenido multimedia protegido**

(30) Prioridad:

01.07.2015 FR 1556223

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2019

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche, Tour Opéra C
92057 Paris La Défense Cedex, FR

(72) Inventor/es:

PHIRMIS, MATHIEU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento de suministro de un contenido multimedia protegido

La invención se refiere a un procedimiento de suministro, por una cabecera de red, de un contenido multimedia protegido por un sistema de protección de contenidos multimedia, en terminales mecánicamente independientes los unos de los otros y conectados con un mismo servidor de derechos de acceso por mediación de una red de gran distancia de transmisión de informaciones. La invención se refiere igualmente a un procedimiento de emisión, por una cabecera de red, de un contenido multimedia protegido para la realización de este procedimiento de suministros de contenidos multimedia. La invención se refiere además a un procedimiento de obtención, por un terminal, de un contenido multimedia protegido para la realización de este procedimiento de suministro de un contenido multimedia. La invención se refiere por último a una cabecera de red, a un terminal y a un soporte de registro de informaciones para la realización de estos procedimientos.

Los procedimientos considerados, pueden ser realizados a título de cualquier servicio de suministro de contenidos multimedia protegidos, en cualquier sistema de suministro en línea de contenidos multimedia protegidos en el cual una cabecera de red asegura la protección de los contenidos y su transmisión a una pluralidad de terminales.

Una conexión punto a punto es una conexión «unicast». Se designa igualmente aquí por el término conexión punto a multipuntos una conexión seleccionada entre el grupo compuesto por una conexión de teledifusión, más conocida bajo los términos de conexión « broadcast », y por una conexión multidifusión, más conocida bajo el término de conexión « multicast ». La conexión punto a punto es una conexión bidireccional. La conexión punto a multipuntos es una conexión unidireccional del emisor a los receptores.

Un terminal es utilizado por un cliente del servicio para acceder a un contenido. Acceder a un contenido multimedia, signifca aquí cargarlo en memoria y en quitar la protección, en el momento que lo recibe, o desde un soporte de registro en el cual ha sido previamente registrado, con miras a jugarlo, registrarlo, o de realizar cualquier otra utilización ofrecida por el servicio de suministro de contenidos multimedia protegidos.

Los contenidos proporcionados son contenidos audiovisuales, por ejemplo programas de televisión, contenidos de audio solamente, por ejemplo un programa radiofónico, o más generalmente cualquier contenido digital que contenga video y/o audio tal como una aplicación informática, un juego, un diaporama, una imagen o cualquier conjunto de datos.

Entre estos contenidos, se considerarán más particularmente en lo que sigue contenidos llamados temporales. Un contenido multimedia temporal es un contenido multimedia cuyo juego es una sucesión, en el tiempo, de sonidos, en el caso de un contenido temporal de audio, o de imágenes, en el caso de un contenido temporal de video, o de sonidos y de imágenes temporalmente sincronizados entre ellos en el caso de un contenido multimedia temporal audiovisual. Un contenido multimedia temporal puede igualmente comprender componentes temporales interactivas sincronizadas con los sonidos o las imágenes.

Para ser suministrado, dicho contenido es primeramente codificado, es decir comprimido, de forma que su transmisión requiera una menor anchura de banda.

A este respecto, la componente de video del contenido se codifica según un formato video, tal como MPEG-2. El lector interesado podrá encontrar una presentación completa de este formato en el documento publicado por la Organisation internationale de normalisation bajo la referencia ISO/IEC 13818-2:2013 y el título « Technologies de l'information - Codage générique des images animées et du son associé - Partie 2: Donnée vidéo ». Numerosos otros formatos, tales como MPEG-4 ASP, MPEG-4 Part 2, MPEG-4 AVC (o Parte 10), HEVC (High Efficiency Video Coding), o WMV (Windows Media Video) pueden alternativamente ser utilizados, y se basan en los mismos principios.

Un método de codificado de este tipo recurre a procedimientos generales de compresión de datos. Para las imágenes fijas, explota particularmente la redundancia espacial interna en una imagen, la correlación entre los puntos próximos y la menor sensibilidad del ojo a los detalles. Para las imágenes animadas, explota la fuerte redundancia temporal entre imágenes sucesivas. La explotación de esta última permite codificar algunas imágenes del contenido, aquí llamadas deducidas, en referencia a otras, aquí llamadas fuentes, por ejemplo por predicción o interpolación, de forma que su decodificado solo sea posible después del de las mencionadas imágenes fuente. Otras imégenes, aquí llamadas iniciales, se codifican sin referencia a tales imágenes fuente, es decir que contienen cada una, cuando son codificadas, el conjunto de las informaciones necesarias para su descodificado y por consiguiente que puedan ser completamente descodificadas independientemente de las otras imágenes. Las imágenes iniciales son así el punto de entrada obligatorio durante el acceso al contenido. El contenido codificado resultante no comprende por consiguiente los datos necesarios para el descodificado de cada una de las imágenes independientemente de las otras, pero está constituido por « secuencias » según la terminologia MPEG-2. Una

secuencia realiza la compresión de al menos un « grupo d'imágenes » (o GOP, para Group Of Pictures, en MPEG-2). Un grupo de imágenes es una secuencia de imágenes consecutivas en la cual cada imagen es, bien sea inicial y fuente para al menos una imagen deducida contenida en la misma secuencia de imágenes consecutivas, o deducida y tal que cada una de las imágenes fuente necesarias para su descodificado pertenezcan a la misma secuencia de imágenes consecutivas, y sin contener secuencia de imágenes consecutivas más pequeña y teniendo estas mismas propiedades. El grupo de imágenes es así la parte más pequeña de contenido a la cual se puede acceder sin tener que descodificar antes otra parte de este contenido. Una secuencia está delimitada por una « cabecera » y un « final », cada una identificada por un primer código específico. La cabecera comprende parámetros que caracterizan propiedades esperadas de las imágenes descodificadas, tales particularmente como anchuras de imagen y alturas, ratio, frecuencia. El standard recomienda repetir la cabecera entre los grupos de imágenes de la secuencia, de forma que sus apariciones sucesivas sean espaciadas aproximadamente algunos segundos en el contenido codificado.

Por ejemplo, un grupo de imágenes comprende lo más corriente de 10 a 12 imágenes, que representan un tiempo de juego comprendido entre 0,4 y 0,5 segundos, en un sistema de 25 imágenes por segundo.

Un contenido multimedia temporal puede comprender varias componentes de video. En este caso, cada una de estas componentes se codifica como se ha descrito más arriba.

La composante audio del contenido es por otro lado codificada según un formato audio tal como MPEG-2 Audio. El lector interesado podrá encontrar una presentación completa de este formato en el documento publicado por la Organisation internationale de normalisation bajo la referencia ISO/IEC 13818-3:1998 y el título « Technologies de l'information - Codage générique des images animées et des informations sonores associées - Partie 3: Son ». Numerosos otros formatos, tales como MPEG-1 Layer III, mejor conocido bajo la denominación MP3, AAC (Advanced Audio Coding), Vorbis o WMA (Windows Media Audio), pueden alternativamente ser utilizados, y se basan en los mismos principios.

Un método de comprensión de un contenido temporal audio de este tipo obedece a los mismos principios anteriormente descritos para el de un contenido temporal de video. El contenido codificado resultante está por consiguiente, de forma análoga, constituido por « tramas ». Una trama es la análoga, en audio, de un grupo de imágenes en video. La trama es por consiguiente particularmente la parte más pequeña de contenido audio a la cual se puede acceder sin tener que descodificar otra parte de este contenido audio. La trama contiene además el conjunto de informaciones útiles para su descodificado.

Por ejemplo, una trama comprende 384 o 1152 muestras que codifican cada una un sonido, que representa, según la frecuencia de muestreo de la señal, una duración de juego de 8 a 12, o de 24 a 36 milisegundos, o sea típicamente algunas decenas de milisegundos.

Un contenido multimedia temporal puede comprender varias componentes audio. En este caso, cada una de estas componentes está codificada como se ha descrito anteriormente.

Las componentes codificadas del contenido multimedia, igualmente calificadas de corrientes elementales de datos, son seguidamente multiplexadas, es decir, particularmente, sincronizadas, y luego combinadas en una sola corriente de datos, igualmente llamada flujo multimedia, o flujo.

Un contenido de este tipo, particularmente cuando es objeto de derechos tales como los derechos de autor o los derechos colindantes, es suministrado protegido por un sistema de protección de contenidos multimedia, que permite asegurar el respeto de condiciones de acceso al contenido que se desprenden de estos derechos.

Entonces se proporciona típicamente cifrado en virtud de su protección por un sistema de gestión de derechos digitales, o DRM, para Digital Rights Management, en inglés. Este cifrado se realiza generalmente por medio de una clave de cifrado, por un algorítmo simétrico. Se aplica al flujo resultante del multiplexado o, antes del multiplexado, a las componentes del contenido codificado.

Un sistema de DRM es en efecto un sistema de protección de contenidos multimédia. La terminologia del ámbito de los sistema de gestión de derechos digitales es así utilizada en lo que sigue de este documento. El lector interesado podrá por ejemplo encontrar una presentación más completa en los documentos siguientes :

- respecto a la arquitectura general de un sistema de DRM : DRM Architecture, Draft version 2.0, OMA-DRM-ARCH-V2_0-20040518-D, Open Mobile Alliance, 18 mayo 2004,
- respecto más particularmente a las licencias : DRM Spécification, Draft version 2.1, OMA-TS-DRM-DRM-V2_1-20060523-D, Open Mobile Alliance, 23 mayo 2006.

Acceder a un contenu multimedia temporal así protegido, significa aquí más precisamente, sucesivamente acceder, al momento mientras los recibe, en segmentos sucesivos, es decir :

- cargar en memoria los segmentos sucesivos del contenido multimedia, luego
- quitar la protección, luego
- descodificarlos, luego
- transmitirlos a un aparato multimedia apto para jugarlos, registrarlos, o realizar cualquier otra utilización ofrecida por el servicio de suministro de contenidos multimedia protegidos. El acceso al contenido multimedia temporal protegido solo se describirá en lo que sigue con miras a su juego. Es idéntico en el caso de cualquier otra utilización ofrecida por el servicio de suministro de contenidos multimedia protegidos.

Por « segmento », se designa una parte restringida del flujo multimedia en claro del cual el juego tiene una duración inferior a la del juego del flujo multimedia en entero. Un segmento comprende por consiguiente una parte restringida de cada componente de video o audio del flujo multimedia en claro, del cual el juego tiene una misma duración inferior a la del juego del flujo multimedia en entero. Estas partes restringidas de componentes están sincronizadas en el en el flujo para ser jugadas simultáneamente. Un segmento comprende por consiguiente la parte restringida de la secuencia temporal de secuencias de video o de grupos de imágenes, o de tramas de audio que realizan el codificado de esta parte restringida de componente del flujo multimedia en claro. Esta parte restringida está constituida por una pluralidad de secuencias de video o de grupos de imágenes, o de tramas de audio sucesivas. Por sucesivas se entiende aquí como se siguen inmediatamente, es de cir sin estar separadas, en el desarrollo temporal del contenido, por otras secuencias de video o de grupos de imágenes, o de tramas de audio. Típicamente, un segmento comprende más de diez, cién, mil o diez mil, grupos de imágenes de video sucesivas de una misma componente de video codificada del flujo, o más de diez a cién veces más de tramas de audio sucesivas de una misma componente de audio codificada del flujo.

Aquí, por « en claro », se designa el hecho de que el flujo multimedia o el segmento no tiene ya necesidad de ser descodificado para ser jugado, por un aparato multimedia, de forma directamente perceptible e inteligible por un ser humano.

Por « aparato multimedia », se designa además cualquier dispositivo apto para jugar el flujo multimedia en claro, tal como un televisor o un lector multimedia.

Aquí, por « al vuelo », se designa el hecho de que los segmentos del contenido multimedia son tratados a medida que se va produciendo su recepción, sin esperar a que el contenido multimedia esté completo, es decir el conjunto de sus segmentos, haya sido completamente recibido.

En un sistema de gestión de derechos digitales de este tipo, con el fin de mejorar la proteción, el contenido es proporcionado, por el sistema de suministro de contenidos multimedia protegidos, escindido en varios segmentos sucesivos de contenido individual protegidos por el sistema de gestión de derechos digitales. Estos segmentos son por consiguiente ordenados temporalmente los unos con relación a los otros.

Más precisamente, cada segmento S_i es cifrado por un algorítmo simétrico por medio de una clave de contenido específico K_{si}. Esta clave K_{si} se dice « específica » pués se utiliza únicamente para cifrar este segmento S_i entre el conjunto de segmentos del contenido multimedia.

Un segmento S_i no se caracteriza por consiguiente por su estructura, sino por la clave K_{si} utilizada para cifrarlo. Un segmento es por consiguiente la pluralidad de secuencias de videos y de tramas de audios inmediatamente sucesivas cifradas con una misma clave K_{si}.

En dicho sistema de gestión de derechos digitales, la obtención de una licencia intermedia L_i, permite a un terminal acceder a un segmento S_i. La licencia intermedia L_i comprende un derecho de acceso necesario a un terminal para acceder a un segmento del contenido. El derecho de acceso comprende típicamente el criptograma $(K_{si})*K_{Gp}$. El derecho de acceso puede igualmente comprender una regla de acceso que describa las utilizaciones del contenido multimedia protegido que el terminal está autorizado a hacer.

Para mejorar aún la protección del contenido, se utiliza un nivel intermedio de cifrado de las claves K_{si}. Permite cambiar, en el transcurso del desarrollo temporal del contenido, las claves de cifrado K_{Gp} utilizadas para calcular los criptogramas $(K_{si})*K_{Gp}$ transportados en las licencias L_i.

Se reagrupan a este respecto los segmentos en bloques de segmentos. Cada bloque solo contiene una parte limitada de los segmentos del contenido. Típicamente, cada bloque contiene como mínimo un segmento y, generalmente, varios segmentos sucesivos. Por sucesivos se entiende aquí como siguientes inmediatamente, es decir sin ser separados, en el desarrollo temporal del contenido, por segmentos que no pertenecen al bloque considerado. Se asocia con cada uno de estos bloques una clave intermedia K_{Gp}. La clave K_{si} necesaria para el descifrado de un segmento, se cifra con la clave K_{Gp} asociada con el bloque al cual pertenece este segmento. El

criptograma resultante $(K_{si})*K_{Gp}$ es seguidamente insertado en la licencia L_i transmitida conjuntamente con este segmento.

La licencia L_i comprende un identificador de una licencia L_p, llamado « de terminal », que comprende ella misma el criptograma $(K_{Gp})*K_T$ de la clave intermedia K_{Gp} obtenido por cifrado de esta clave K_{Gp} con la clave K_T de terminal.

Un bloque de segmentos no se caracteriza por consiguiente por su estructura, sino por la clave intermedia K_{Gp} utilizada para cifrar cada clave K_{si} de todos los segmentos de este bloque. Un bloque está por consiguiente formado por el conjunto de segmentos cuya clave K_{si} está cifrada con una misma clave intermedia K_{Gp}.

En dicho sistema, un terminal recibe por consiguiente, conjuntamente con un segmento cifrado, una licencia intermedia L_i que comprende el criptograma $(K_{si})*K_{Gp}$ de la clave de contenido necesaria para el descifrado de este segmento.

Para acceder al contenido con miras a realizar una utilización dada deseada, el terminal extrae el derecho de acceso de la licencia L_i.

Con el fin de acceder al segmento, el terminal debe primeramente obtener la licencia L_p de terminal que comprende el criptograma $(K_{Gp})*K_T$. El terminal obtiene esta licencia L_p sometiendo al servidor de derechos de acceso una petición de derecho de acceso. Esta petición sometida « out-of-band », es decir a una conexión punto a punto entre el terminal y el servidor de derechos de acceso. La respuesta del servidor de derecho de acceso es también transmitida al terminal por esta misma conexión punto a punto.

El terminal puede seguidamente evaluar la licencia L_p. Si el resultado de esta evaluación es positivo, descifra el criptograma $(K_{Gp})*K_T$ que comprende, por medio de su clave K_T de terminal. Si el resultado de esta evaluación es negativo, el termina inhibe la explotación de la licencia L_p, y no descifra particularmente el criptograma $(K_{Gp})*K_T$ que comprende. Eso impide así el acceso al bloque de segmentos protegidos gracias a las claves K_{si} cifradas con la ayuda de esta clave intermedia K_{Gp}.

En el caso en que el terminal no haya recibido la licencia L_p, inhibe del mismo modo su tratamiento, e impide así el acceso al bloque de segmentos protegido en curso de recepción. Se produce, para el usuario del terminal, una interrupción del juego del contenido.

Por consiguiente, es importante que el terminal obtenga la licencia L_p asociada con el próximo bloque de segmentos para recibir con suficiente anticipo con relación al comienzo de la recepción de este próximo bloque de segmentos. El comienzo de la recepción del próximo bloque de segmentos es igualmente designado como siento el momento de la próxima rotación de clave intermedia en el flujo. A este respecto, el experto en la materia habla de « suministro anticipado de licencia », o « license pre-delivery », en inglés.

Con el fin de garantizar el suministro anticipado de la licencia L_p, cualquier licencia L_p transmitida a un terminal comprende una fecha límite antes de la cual este terminal debe requerir la próxima licencia L_{p+1} de terminal respecto al servidor de derechos de acceso. La próxima fecha en la cual el terminal debe conectarse con el servidor de derechos de acceso para requerir la próxima licencia de terminal es llamada « vencimiento de renovación ». Cuando este vencimiento de renovación ha llegado, el terminal somete una petición de derechos de acceso al servidor de derechos de acceso, que le transmite, en respuesta, la próxima licencia L_{p+1} de terminal.

De vez en cuando, es deseable retrasar la fecha límite antes de la cual el terminal debe requerir la próxima licencia L_{p+1} de terminal respecto al servidor de derechos de acceso. Por ejemplo, es el caso cuando existen problemas de conexión entre el terminal y el servidor de derechos de acceso o cuando el servidor de derechos de acceso no está disponible. Puede también ser deseable avanzar esta fecha límite. Por ejemplo, eso puede ser utilizado a título de contramedida en respuesta a ataques contra la seguridad del servicio y del sistema de suministro de contenidos multimedia protegidos.

Por el estado de la técnica se conocen igualmente los documentos :

-US2012/008781A1,

- US2014/281481A1, y

- WO2005/091635A2.

Los procedimientos conocidos presentan el primer inconveniente según el cual es muy difícil modificar ulteriormente la fecha límited antes de la cual el terminal debe requerir la próxima licencia L_{p+1} de terminal respecto al servidor de

derechos de acceso. En efecto, a este fin, sería preciso redifundir nuevas licencias de terminal actuales a cada uno de los terminales con una nueva fecha límite.

Los procedimientos conocidos presentan además el segundo inconveniente según el cual el vencimiento de renovación es sistemáticamente seleccionado igual a esta fecha límite. Por consiguiente, el vencimiento de la renovación es el mismo para todos los terminales. Por lo tanto, todos los terminales someten simultáneamente, en este vencimiento de renovación, una petición de derechos de acceso al servidor de derechos de acceso. Eso provoca un pico de carga de cálculo del servidor de derechos de acceso y de tráfico de red.

La invención trata de remediar el primer inconveniente indicado anteriormente.

La invención tiene así por objeto un procedimiento, conforme a la reivindicación 1, de suministro, por una cabecera de red, de un contenido multimedia protegido.

En dicho procedimiento, un dato temporal es transmitido por la conexión punto a multipunto al conjunto de terminales. Este dato temporal permite determinar si la fecha límite para transmitir al servidor de derecho de acceso la petición de derecho de acceso ha cambiado. Así, su transmisión permite notificar al terminal un eventual cambio de esta fecha límite. En respuesta a dicho cambio, cada terminal puede modificar su vencimiento de renovación. Este vencimiento de renovación permite al terminal decidir, en función de su valor y en un instante dado, transmitir al servidor de derechos de acceso una petición de derechos de acceso. Un procedimiento de este tipo permite por consiguiente modificar el vencimiento de renovación del terminal, y por consiguiente el instante dado anteriormente, sin tener que transmitir una nueva licencia por mediación de una conexión punto a punto en cada uno de los terminales y por consiguiente remediar el primer inconveniente citado. Esta solución de notificación, que se basa ampliamente en la existente y que precisa poco desarrollo en la cabecera de red y los terminales, es además sencilla y poco costosa.

La invención tiene igualmente por objeto un procedimiento de emisión, por una cabecera de red, para la realización del procedimiento de suministro reivindicado, de un contenido multimedia protegido.

La invención tiene igualmente por objeto un procedimiento de obtención, por un terminal, para la realización del procedimiento de suministro reivindicao, de un contenido multimedia.

Los modos de realización de este procedimiento de obtención de contenidos multimedia protegidos presentan además las ventajas siguientes :

- El ensayo de una de las condiciones $DS_i > DS_{i-1} + \Delta T_1$ y $DS_i \geq DS_{i-1} + \Delta T_1$, permite modificar solo el vencimiento de renovación predeterminado cuando la fecha límite ha sido retrasada por al menos ΔT_1.

- El ensayo de una de las condiciones $DS_i < DS_{i-1} - \Delta T_2$, y $DS_i \leq DS_{i-1} - \Delta T_2$, permite modificar solo el vencimiento de renovación predeterminada cuando la fecha límite ha sido avanzada por al menos ΔT_2.

- Modificar el vencimiento de renovación predeterminado asignándole un valor calculado por medio de una función apta para repartir uniformemente los vencimientos de renovación predeterminados de los terminales, permite suavizar la carga de cálculo del servidor de derechos de acceso y el tráfico de red.

- Iniciar la transmisión inmedita, al servidor de derechos de acceso, de la petición de derechos de acceso, si el último dato temporal recibido es igual a un código preregistrado, permite utilizar el dato temporal para cumplir dos funciones diferentes, a saber modificar el vencimiento de renovación y, alternativamente, iniciar la transmisión de la petición de derecho de acceso independientemente del vencimiento de renovación predeterminado.

La invención tiene igualmente por objeto un soporte de registro de informaciones que comprende instrucciones para la realización de uno de los procedimientos reivindicados, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

La invención tiene igualmente por objeto una cabecera de red para la realización del procedimiento de emisión reivindicado.

La invención tiene por último por objeto un terminal para la realización del procedimiento de obtención reivindicado.

La invención se comprenderá mejor con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitativo, y realizada con referencia a los dibujos en los cuales :

- la figura 1 es una representación esquemática de la arquitectura de un sistema de suministro de contenidos multimedia protegidos,

- la figura 2 es una representación esquemática de una licencia intermedia,

- la figure 3 est une représentation esquemática de una licencia de terminal,

- la figura 4 es una representación esquemática de un flujo transmitido por una cabecera de red a un terminal,

- la figura 5 es una representación esquemática de un procedimiento de suministro de contenidos multimedia protegidos utilizando la arquitectura de la figura 1.

En estas figuras, las mismas referencias se utilizan para designar los mismos elementos.

En lo que sigue de esta descripción, las características bien conocidas por el experto en la materia no se describirán en detalle.

La figura 1 representa un sistema de suministro de contenidos multimedia protegidos.

Este sistema comprende una pluralidad, típicamente millares, de terminales, mecánicamente independientes los unos de los otros, conectados, por mediación de una red 3, por una parte a una cabecera 1 de red, y por otra parte a un servidor 2 de derechos de acceso. Aquí, se supone que todos estos terminales son idénticos. Así, para simplificar la ilustración, solo un terminal 4 se ha representado en la figura 1.

El terminal 4 es apto para acceder a un contenido con miras a jugarlo. A este respecto, el terminal 4 comprende un ordenador electrónico 44 programable y una memoria 46. El ordenador 44 es apto para ejecutar instrucciones registradas en la memoria 46. Típicamente se trata de un microprocesador tal como un microprocesador Itanium de la sociedad Intel. La memoria 46 comprende las intrucciones necesarias para la ejecución del procedimiento de la figura 5. La memoria 46 comprende un vencimiento de renovación predeterminado DRP. El vencimiento DRP permite al terminal decidir, en función de su valor y en un instante dado, transmitir al servidor de derechos de acceso una petición de derechos de acceso. Aquí, el vencimiento DRP es expresado bajo la forma de un tiempo que queda antes de la próxima fecha en la cual el terminal 4 iniciará automáticamente la transmisión de una petición de derecho de acceso al servidor 2.

La red 3 es una red de gran distancia de distribución de informaciones que permite establecer una conexión de comunicación punto a multipuntos 32 entre la cabecera 1 de red y el terminal 4. La red 3 permite también establecer una conexión de comunicación punto a punto 34 entre el terminal 4 y el servidor 2. Por ejemplo, la red 3 es la tela de araña mundial, más conocida bajo el término de « red Internet ».

La cabecera 1 es apta para proteger un contenido, y para transmitirlo al terminal 4. A este respecto, la cabecera 1 comprende un ordenador electrónico 14 programable y una memoria 6. El ordenador 14 es apto para ejecutar instrucciones registradas en la memoria 16. Típicamente, se trata de un microprocesador tal como un microprocesador Tegra de la sociedad Nvidia, o un procesador Cortex-A8 de la sociedad ARM. La memoria 16 comprende las instrucciones necesarias para la ejecución del procedimiento de la figura 5.

El servidor 2 de derechos de acceso es apto para proporcionar al terminal 4, en respuesta a una petición, una licencia de terminal que comprende un derecho de acceso necesario para acceder a un contenido multimedia y previamente adquirido por el terminal 4.

Aquí, para la cabecera 1, el servidor 2 y el terminal 4, solo las únicas diferencias con relación a una cabecera de red convencional, un servidor de derecho de acceso convencional y con un terminal convencional se describen con detalle. Paras las informaciones respecto a una cabecera de red convencional, un servidor de derecho de acceso convencional y un terminal convencional, el lector puede referirse al estado de la técnica citado en la introducción de esta solicitud de patente.

La figura 2 representa una licencia intermedia L_i. Esta licencia L_i comprende particularmente un criptograma $(K_{si})*K_{Gp}$ obtenido cifrando una clave de contenido K_{si} con una clave intermedia K_{Gp}. La clave K_{si} es la clave utilizada para cifrar el segmento S_i del contenido multimedia. La clave K_{Gp} es la clave utilizada para cifrar las claves K_{si} de todos los segmentos del bloque G_p. La licencia L_i comprende igualmente un identificador $Id(K_{Gp})$ de esta clave intermedia K_{Gp}. La licencia L_i comprende además un dato temporal DS_i que permite determinar si la fecha limite D_{Gp} para transmitir al servidor 2 la petición de derecho de acceso ha cambiado, es decir si esta fecha limite ha sido adelantada o, por el contrario, retrasada. Además, el dato temporal DS_i permite igualmente modificar el vencimiento DRP en respuesta a este cambio de fecha límite D_{Gp}.

Aquí, el dato temporal DS_i es un tiempo que queda antes de que se alcance una fecha límite D_{Gp}. La fecha limite D_{Gp} es la fecha antes de la cual el terminal debe transmitir, al servidor 2, una petición de derecho de acceso para podeer obtener la licencia L_{p+1} antes de comenzar a recibir el bloque G_{p+1}. La licencia L_{p+1} comprende el derecho de acceso

necesario para acceder a cualquier segmento del bloque siguiente G_{p+1}. La fecha límite es por consiguiente una fecha anterior al comienzo de la transmisión del bloque G_{p+1} y, generalmente posterior a la fecha de comienzo de la transmisión del bloque G_p. Típicamente, la fecha límite es igual a la fecha planificada para comenzar la transmisión del bloque G_{p+1} menos un márgen ΔDL de seguridad predeterminada.

En este modo de realización, el dato DS_i está relacionado con la fecha límite D_{Gp} por la relación siguiente : $D_{Gp} = Deb_{Si} + DS_i$, donde Deb_{Si} es igual a la fecha de comienzo de la recepción del segmento S_i.

El dato temporal DS_i es típicamente calculado, por la cabecera 1, en función del tiempo de juego de un segmento por el terminal, igualmente llamado criptoperiodo, y por el número de segmentos que quedan antes del final del bloque G_p actual de segmentos. El mismo se expresa por ejemplo en segundos o en número de criptoperiodos. Aquí, su valor es contado tomando como origen de los tiempos la fecha Deb_{Si} de comienzo de la recepción del segmento S_i. Así, mientras la fecha límite D_{Gp} no haya cambiado, el dato temporal DS_i disminuye el tiempo de un criptoperiodo en cada envío de un nuevo segmento del bloque Gp. En el caso particular donde el dato temporal DS_i está comprendido entre cero y un umbral ΔTc positivo o nulo, igual a cero, o negativo, la fecha límited D_{Gp} es, respectivamente, llamada inminente, igual a la fecha actual, o pasada. Por ejemplo, ΔTc es igual a nxΔt, donde :

- Δt es el tiempo medio que transcurre entre el instante donde el terminal 4 envía una petición de derecho de acceso y el instante en que, en respuesta, recibe la licencia L_{p+1}, y
- n es un número predeterminado superior o igual a 1 y, generalmente, inferior a 2 o 3. Aquí, n es igual a uno. Aquí, en este caso donde la fecha límited D_{Gp} es inminente, igual a la fecha actual, o pasada, la cabecera 1 asigna para valor, al dato temporal DS_i, un código preregistrado. Por ejemplo, el código preregistrado tiene por valor cero.

La figura 3 representa una licenccia L_p de terminal. Esta licencia comprende un derecho 52 de acceso. El derecho 52 comprende la clave K_{Gp} o un criptograma de esta clave. La licencia L_p comprende también el identificador $Id(K_{Gp})$ de la clave K_{Gp}. Finalmente, la licencia L_p puede comprender un dato temporal 54, que permite calcular una fecha límite inicial para transmitir al servidor 2 la petición de derecho de acceso. Por ejemplo, este dato temporal 54 es una fecha calculada e inicialmente utilizada como en la técnica anterior descrita más arriba. La misma ya no se puede por consiguiente modificar un avez que la licencia L_p ha sido recibida y tratada por el terminal 4, sin transmisión, por el servidor 2, de una nueva licencia al mismo terminal.

La figura 4 representa un flujo 6 transmitido par la cabecera 1 hacia todos los terminales. El flujo 6 comprende varios bloques de segmentos de contenido multimedia. Por ejemplo, el flujo 6 comprende más de dos, diez o cién bloques de segmentos. Aquí, se supone que todos estos bloques son estructuralmente idénticos y difieren los unos de los otros únicamente por el contenido codificado en cada uno de los segmentos. En particular, todos los bloques comprenden el mismo número de segmentos. Para simplificar la figura 4, solo un bloque G_p ha sido representado, y se describirá ahora con más detalle.

El bloque G_p comprende una pluralidad de segmentos. Típicamente, el bloque G_p comprende más de diez o cién segmenetos sucesivos. El bloque G_p comprende solamente una parte restringida del conjunto de segmentos cuya concatenación forma la totalidad del contenido multimedia difundido. Solo tres segmentos S_i, S_{i+1} y S_{i+2} han sido representados en la figura 4. Aquí, todos estos segmentos son estructuralmente idénticos y difieren los unos de los otros únicamente por las informaciones codificadas en cada uno de ellos.

Con el segmento S_i está asociada la licencia intermedia L_i, transmitida conjuntamente con este segmento en el flujo 6. Aquí, esta asociación es realizada por sincronización temporal del segmento S_i y de la licencia intermedia L_i en el flujo. Aquí, esta sincronización es en sí misma realizada por la adyacencia del segmento S_i y la licencia intermedia L_i en el flujo, y, llegado el momento, por su transmisión conjunta. En la figura 4, las licencias intermedias asociadas con los segmentos S_{i+1} y S_{i+2} llevan, respectivamente, las referencias digitales L_{i+1} y L_{i+2}.

El funcionamiento del sistema de la figura 1 se describirá ahora con referencia al procedimiento de la figura 5.

El procedimiento comienza por una fase 100 de acondicionamiento del contenido multimedia. Al comienzo de esta fase 100, durante una etapa 102, la cabecera 1 recibe del terminal 4 una petición tratando de obtener el contenido. Esta petición contiene particularmente un identificador de una clave K_T de terminal. La clave K_T es aquí única para cada terminal. De forma conocida por el experto en la materia, la clave K_T ha sido obtenida por el terminal durante su fase de fabricación o de personalización. La misma es seguidamente obtenida por la cabecera 1 durante una fase de registro del terminal antes de la realización del procedimiento de la figura 5.

Luego, durante una etapa 104, la cabecera 1 adquiere un contenido multimedia temporal en claro, lo codifica, y luego lo protege por medio de un sistema de protección de contenidos multimedia.

Con el fin de protegerlo, la cabecera 1 escinde el contenido multimedia codificado en varios segmentos S_i sucesivos de contenido. Estos segmentos S_i son ordenados temporalmente los unos con relación a los otros, y su secuencia

completa constituye el contenido multimedia. En lo que sigue de esta descripción, el índice « i » es el número de orden del segmento S_i en esta secuencia temporal de segmentos.

La cabecera 1 asegura seguidamente la protección individual, por un sistema de gestión de derechos digitales, de cada uno de los segmentos S_i. A este respecto, cifra cada segmento S_i con una clave específica K_{si}. La clave K_{si} no es utilizada para cifrar otro segmento de la misma secuencia de segmentos.

Seguidamente, la cabecera 1 constituye los bloques G_p de segmentos sucesivos. El índice « p » es el numero de orden del bloque en la secuencia de bloques sucesivos así constituida. Aquí, la cabecera 1 fija a este respecto el número de segmentos contenidos en cada bloque. Para cada bloque que comprenda este número de segmentos sucesivos, la misma genera seguidamente una clave intermedia K_{Gp}. Luego cifra, con la clave K_{Gp}, cada clave K_{si} asociada con un segmento S_i de este bloque G_p. Por consiguiente, obtiene para cada segmento S_i del bloque G_p, el criptograma $(K_{si})*K_{Gp}$. La cabecera 1 introduce seguidamente el identificador $Id(K_{Gp})$ de la clave K_{Gp} y el criptograma $(K_{si})*K_{Gp}$ en la licence L_i que asocia con este segmento S_i como se ha descrito con referencia a la figura 4.

La cabecera 1 continua entonces mediante una fase 110 de emisión del contenido multimedia acondicionado durante la fase 100. Más precisamente, la fase 110 comienza por una etapa 112 durante la cual la cabecera 1 cifra cada clave K_{Gp}, con la clave K_T de terminal, para obtener el criptograma $(K_{Gp})*K_T$. Luego para cada bloque G_p, introduce, como derecho 52 de acceso a este bloque, el criptograma $(K_{Gp})*K_T$ en la licencia L_p de terminal destinada al terminal 4. El identificador $Id(K_{Gp})$ de la clave K_{Gp} es además introducido en la licencia L_p. El identificador $Id(K_{Gp})$ al estar igualmente contenido en la licencia L_i asociada con cualquier segmento S_i del bloque G_p, la licencia L_p se asocia así igualmente con cada uno de los segmentos S_i, y por consiguiente con el bloque G_p.

Durante esta etapa 112, opcionalmente, la cabecera 1 introduce, en la licencia L_p, el dato temporal 54. Se apreciará que el procedimiento descrito en lo que sigue funciona incluso si el dato 54 no está introducido en la licencia L_p.

A continuación, durante una etapa 114, la cabecera 1 asocia con cada uno de los aegmentos S_i su dato temporal DS_i. Luego, introduce este dato temporal DS_i en la licencia L_i asociada con el segmento S_i. El dato temporal DS_i es de preferencia introducido, protegido en su totalidad, en la licencia L_i. Así, aquí, un dato temporal DS_i respectivo está asociado con cada segmento S_i del bloque G_p.

La cabecera 1 genera así poco a poco un flujo 6 que comprende cada uno de los segmentos S_i del bloque G_p y, para cada segmento S_i, su licencia L_i asociada que comprende por si misma el dato temporal DS_i.

La cabecera 1 transmite por último la licencia L_p construida para el terminal 4 al servidor 2 que la registra.

A continuación, durante una etapa 116, el servidor 2 transmite la licencia L_p al terminal 4 por mediación de la conexión 34. Típicamente, esta transmisión tiene lugar en respuesta a la recepción por el servidor 2, en la conexión 34, de una petición de derecho de acceso transmitida por el terminal 4.

Durante una etapa 118, la cabecera 1 transmite, por mediación de la conexión 32, el flujo 6 al terminal 4. Las etapas 116 y 118 son sincronizadas por el procedimiento según la invención de tal forma que la etapa 116 preceda a la etapa 118 de forma que la licencia L_p sea recibida y tratada por el terminal 4 antes que el bloque G_p sea jugado.

El procedimiento se continua por una fase 120 de recepción. Durante la fase 120, el terminal recibe, durante una etapa 122, la licencia L_p, y, durante una etapa 124, el flujo 6. Debido a la sincronización de las etapas 116 y 118, las etapas 122 y 124 se sincronizan ellas mismas de forma que la etapa 122 preceda a la etapa 124.

Durante la etapa 124, el terminal recibe uno después del otro cada uno de los segmentos S_i del bloque G_p y la licencia L_i asociada.

A continuación, el terminal ejecuta una fase 130 de juego del contenido. Durante esta fase, procede, sucesivamente para cada uno de los segmentos S_i del flujo 6 recibido, en la realización de las etapas 132 a 148.

Durante la etapa 132, el terminal extracta el segmento S_i, y su licencia L_i del flujo 6.

Durante la etapa 134, el terminal 4 extracta de la licencia L_i el identificador $Id(K_{Gp})$ de la clave K_{Gp}. Luego, el terminal 4 busca la licencia L_p que comprende el mismo identificador $Id(K_{Gp})$.

A continuacón, si el derecho 52 de la licencia L_p encontrada no ha sido ya extractada desde el comienzo de la fase de juego, entonces el terminal 4 la extracta.

Durante la etapa 136, el terminal 4 utiliza el derecho 52 para permitir y, de lo contrario, impedir el acceso al segmento S_i. En este modo de realización, a este respecto, el terminal 4 extracta del derecho 52 el criptograma $(K_{Gp})*K_T$. Luego, el terminal 4 descifra el criptograma $(K_{Gp})*K_T$ con su clave K_T. Obtiene así la clave K_{Gp} en claro. El terminal 4 descifra entonces el criptograma $(K_{si})*K_{Gp}$ con esta clave K_{Gp}. Obtiene así la clave K_{si} en claro. Por último,

el terminal 4 descifra el criptograma del segmento S_i con esta clave K_{si} y obtiene el segmento S_i en claro. El segmento S_i en claro es transmitido por el terminal 4 a un aparato multimedia que lo juega. En este modo de realización, el acceso al segmento S_i se impide si el derecho 52 no contiene criptograma $(K_{Gp})*K_T$ o un criptograma erróneo que no puede ser correctamente descifrado con la clave K_T. El acceso al segmento S_i puede también ser prohibido si el derecho 52 comprende una regla de acceso que describe las utilizaciones del contenido multimedia protegido que el terminal 4 está autorizado a realizar, y entre las cuales no figura el juego por un aparato multimedia requerido por el terminal 4.

Paralelamente a las etapas 134 y 136, si la licencia L_{p+1} de terminal no ha sido ya obtenida por el terminal 4, el termina realiza las etapas 138 y 148.

Durante la etapa 138, el terminal 4 extrae de la licencia L_i el dato temporal DS_i asociado con el segmento S_i.

Luego, durante la etapa 140, el terminal 4 compara el dato temporal DS_i con el código preregistrado. Si el valor del dato temporal DS_i es igual al código preregistrado, entonces el terminal procede inmediatamente a la etapa 148. De lo contrario, el terminal pone en práctica la etapa 142.

Durante la etapa 148, el terminal 4 transmite inmediatamente, al servidor 2 una petición de derechos de acceso. En respuesta, el servidor 2 realiza una nueva realización de la etapa 116, para transmitir al terminal la licencia L_{p+1}. La licencia L_{p+1} comprende el derecho de acceso necesario para acceder a cualquier segmento del bloque G_{p+1}.

Así, cuando, durante la etapa 140, el dato temporal DS_i es igual al código preregistrado, el terminal 4 inicia la transmisión de la petición de derecho de acceso independientemente del vencimiento de renovación predeterminado DPR registrado en su memoria 46.

Durante la etapa 142, el terminal determina si el dato temporal DS_i cumple una al menos de las condiciones siguientes:

- Condición 1) : $DS_i > DS_{i-1} + \Delta T_1$, y
- Condición 2) : $DS_i < DS_{i-1} - \Delta T_2$,

donde ΔT_1 et ΔT_2 son constantes predefinidas nulas o positivas.

La condición 1) es comprobada en los casos en que la fecha límite D_{Gp} para transmitir al servidor 2 la petición de derecho de acceso ha sido rechazada por al menos ΔT_1. Por ejemplo, ici $\Delta T_1 = 0$.

La condición 2) es comprobada en los casos en que la fecha límite D_{Gp} para transmitir al servidor 2 la petición de derecho de acceso ha sido avanzada por al menos ΔT_2.

Por ejemplo, aquí ΔT_2 es igual a un múltiplo estrictamente positivo del tiempo de un criptoperiodo. Por ejemplo ΔT_2 es entonces superior a 2 o 3 veces el tiempo de un criptoperiodo.

Si una de las condiciones 1) y 2) es cumplida, el terminal pone seguidamente en práctica las etapas 144 y luego 146. En el caso contrario, procede directamente a la etapa 146.

Durante la etapa 144, el terminal modifica el vencimiento de renovación DRP actual en función del dato temporal DS_i recibido para obtener un nuevo vencimiento de renovación. Este nuevo vencimiento DRP permite al terminal decidir, en función de su valor y en un instante dado anterior o igual a la fecha límite modificada, transmitir al servidor de derechos de acceso una petición de derechos de acceso.

Para eso, aquí, el nuevo vencimiento de renovación es obtenido aleatoriamente, o pseudo-aleatoriamente, dentro del intervalo comprendido entre 0 y el último dato temporal DS_i recibido. Este nuevo vencimiento de renovación DRP sustituye entonces al precedente vencimiento de renovación en la memoria 46.

Durante la etapa 146, el terminal 4 determina, si el vencimiento DRP registrado en su memoria es alcanzado. Para eso, compara el vencimiento de renovación DRP registrado en su memoria 46 en un umbral ΔTd positivo o nulo predeterminado. Si el vencimiento DRP es negativo, nulo, o comprendido entre 0 y ΔTd, el terminal 4 pone entonces en práctica la etapa 148. En caso contrario, el terminal 4 inhibe la realización de la etapa 148, memoriza DS_i en vez y lugar de DS_{i-1} como último dato temporal recibido, y actualiza el vencimiento DRP. Aquí la actualización del vencimiento DRP consiste en disminuir el vencimiento DRP del tiempo $DS_{i-1} - DS_i$. Aquí, este tiempo es la duración de un criptoperiodo. Seguidamente, el vencimiento DRP actualizado es registrado en la memoria 46 en sustitución del antiguo vencimiento. Por ejemplo, ΔTd es igual a $n x \Delta t$, donde :

- Δt es el tiempo medio que transcurre entre el instante en que el terminal 4 envía una petición de derecho de acceso y el instante en que, en respuesta, recibe la licencia L_{p+1}, y
- n es un número predeterminado superior o igual a 1 y, generalmente, inferior a 2 o 3. Aquí, n es igual a uno.

Por ejemplo, ΔTd es igual a ΔTc.

Numerosos otros modos de realización de la invención son posibles. Por ejemplo, el contenido es proporcionado protegido por un sistema de gestión de derechos digitales sin no obstante estar cifrado. El criptograma $(K_{Si})*K_{Gp}$ no figura entonces necesariamente entre los datos de acceso introducidos en la licencia L_i.

En otro modo de realización, el contenido multimedia es proporcionado protegido por un sistema de acceso condicional, o CAS, para Conditional Access System. La terminologia del ámbito de los sistemas de acceso condicional es entonces utilizada. El lector interesado podrá por ejemplo encontrar una presentación más completa en el documento : « Functional Model of a Conditional Access System », EBU Review, Technical European Broadcasting Union, Bruxels, BE, N° 266, el 21 diciembre 1995. Un segmento es entonces por ejemplo un criptoperiodo, una licencia de terminal L_p un EMM (Entitlement Management Message), y la licencia intermedia L_i un ECM (Entitlement Control Message). El dato temporal DS_i es entonces típicamente introducido en un ECM.

En otro modo de realización, el contenido es proporcionado, por el sistema, protegido por cualquier otro tipo de sistema de protección de contenidos, tal como por ejemplo un sistema de protección de datos más clásico que no realiza gestión de derechos de acceso. El procedimiento reivindicado se aplica entonces al suministro de los mensajes necesarios para el encaminamiento de las claves de descifrado, por ejemplo.

En otro modo de realización, todos los segmentos de un bloque de segmentos de contenido no se siguen inmediatamente en el desarrollo temporal del contenido. Algunos de estos segmentos son entonces separados por segmentos que no pertenecen al bloque considerado.

En variante, un terminal de partición con al menos otro terminal, su clave K_T de descifrado.

En variante, ningún código pre-registrado es asignado al dato temporal DS_i si la fecha límite es inminente, igual a la fecha actual o pasada. En este caso, durante la etapa 140, el dato temporal DS_i se compara con el umbral ΔTc. Si el dato temporal DS_i es inferior a este umbral, entonces se ejecuta directamente la etapa 148. En caso contrario, el procedimiento se continua mediante la ejecución de la etapa 142. En este modo de realización, no es necesario utilizar un código pre-registrado.

En variante, el vencimiento DRP es la proxima fecha en la cual el terminal 4 iniciará automáticamente la transmisión de una petición de derecho de acceso al servidor 2. En este caso, durante la etapa 146, el termina 4 compara el vencimiento DRP registrado en su memoria en la fecha actual. Si el vencimiento DRP está pasado, es igual a la fecha actual, o inminente, entonces el terminal 4 pone en práctica la etapa 148. En el caso contrario, el terminal 4 inhibe la puesta en práctica de la etapa 148. Se califica de inminente un vencimiento DRP cuando está comprendido entre la fecha actual Dc y Dc + ΔTd, donde ΔTd es el umbral anteriormente definido.

En este caso, una fecha corriente se obtiene por el terminal 4 por cualquier medio. Por ejemplo, ante un servidor de fechas al cual el terminal 4 está conectado por mediación de la red 3, por un reloj integrado en el terminal 4, o calculada a partir de una magnitud que represente el tiempo que transcurre y que es transmitido al flujo 6. Además, en esta variante, la etapa 144 consiste, por ejemplo, en obtener aleatoriamente o pseudo-aleatoriamente un nuevo vencimiento DRP dentro del margen de fechas comprendido entre la fecha actual y la fecha límite cambiada D_{Gp}. La fecha límite cambiada D_{Gp} es por ejemplo calculada con la ayuda de la relación siguiente : $D_{Gp} = Deb_{Si} + DS_i$.

En variante, la red 3 comprende una primera subred soporte de la conexión punto a multipuntos 32 y una segunda subred soporte de la conexión punto a punto 34. Por ejemplo, la primera subred es una red de transmisión por satélite y la segunda subred es la red Internet.

En variante, el servidor 2 está integrado en el interior de la cabecera 1.

En variante, cada licencia L_i no comprende sistemáticamente un dato temporal DS_i. Por ejemplo, entre las licencias L_i asociadas a los segmentos de un mismo bloque G_p, solo menos de una de dos o menos de una de cinco, o menos de una de diez, o menos de una de cincuenta comprende un dato temporal DS_i. Los únicos segmentos S_i del bloque G_p que están asociados con un dato temporal DS_i forman una lista de segmentos del bloque G_p. En este caso, las etapas 138 a 148 son ejecutadas únicamente para los segmentos de esta lista. Entonces, cuanto más importante es el efectivo de esta lista, más numerosas son las oportunidades de modificar el vencimiento de renovación DRP, y más flexible es por consiguiente el procedimiento. Por otro lado, cuanto más regularmente repartidos están los segmentos de la lista en el bloque G_p, más son las oportunidades de modificar el vencimiento de renovación en si mismas. Esto hace igualmente el procedimiento más flexible.

En un último ejemplo, un dato temporal DS_i solo es introducido según se necesite en la licencia L_i, es decir cuando el vencimiento de la renovación deba ser modificado. Entonces, por ejemplo, una sola de las licencias L_i comprende un dato temporal DS_i

En variante, el dato temporal DS_i es una fecha. Esta fecha es por ejemplo la fecha límite D_{Gp} en la cual el terminal debe transmitir, al servidor 2, una petición de derecho de acceso con miras a obtener la licencia L_{p+1} antes de comenzar a recibir el bloque G_{p+1}. El dato temporal DS_i puede también ser una fecha DL_i tal como la nueva fecha límite se calcula de la forma siguiente : $D_{Gp} = DL_i - \Delta Tl$, donde ΔTl es un tiempo predeterminado positivo o nulo. Por ejemplo, ΔTl es igual a ΔTc.

En este caso, durante la etapa 144, el nuevo vencimiento de renovación es obtenido aleatoriamente, o pseudo-aleatoriamente, en el intervalo comprendido entre la fecha actual Dc y el dato temporal DS_i recibido. Alternativamente, el nuevo vencimiento de renovación DRP es sistemáticamente tomado igual al dato temporal DS_i recibido. En otro ejemplo, el nuevo vencimiento de renovación DRP es fijado en un subintervalo del intervalo comprendido entre la fecha actual Dc y el dato temporal DS_i recibido. Por ejemplo, este subintervalo se determina en función de un identificador del terminal. Por ejemplo, el nuevo vencimiento de renovación DRP es obtenido aleatoriamente, o pseudo-aleatoriamente, en este subintervalo. Alternativamente, el nuevo vencimiento de renovación es tomado sistemáticamente igual al límite superior de este subintervalo.

En variante, el dato temporal DS_i asociado con el segmento S_i es introducido en un mensaje o una estructura de datos distinta de la licencia L_i asociada con el mismo segmento. Sin embargo, este mensaje o esta estructura de datos distinta es transmitida conjuntamente al segmento S_i y a la licencia L_i. Por ejemplo, el dato temporal es adyacente a cada segmento transmitido en el flujo pero no forma parte de la estructura de datos que forman una licencia L_i.

En variante, cada bloque comprende un solo segmento. En este modo de realización particular, la utilización de la clave K_{Gp} puede ser omitida. La licencia L_i no comprende entonces el criptograma$(K_{Si})*K_{Gp}$ y el derecho de acceso 52 de la licencia L_p comprende el criptograma $(K_{Si})*K_T$ en lugar del criptograma $(K_{Gp})*K_T$. El experto en la materia sabe adaptar el procedimiento de la figura 5 en este caso particular. Más precisamente, durante la etapa 112, la cabecera 1 cifra cada clave K_{si}, con la clave K_T, para obtener el criptograma $(K_{si})*K_T$. Luego para cada bloque G_p, introduce, como derecho 52 de acceso a este bloque, el criptograma $(K_{si})*K_T$ en la licencia L_p destinada al terminal 4. El identificador $Id(K_{Gp})$ de la clave K_{Gp} es igualmente introducido en la licencia L_p. El identificador $Id(K_{Gp})$ al estar igualmente contenido en la licencia L_i asociada con cualquier segmento S_i del bloque G_p, la licencia L_p está así igualmente asociada con cada uno de los segmentos S_i, y por consiguiente con el bloque G_p.

En otro modo de realización, todos los bloques no comprenden el mismo número de segmentos.

En variante, durante la etapa 112, la cabecera 1 asocia ademas con el bloque G_p al menos una regla de acceso, que describe los usos del contenido multimedia que el terminal está permitido realizar, o un identificador de esta regla de acceso. Esta regla de acceso, o este identificador, conjuntamente con el criptograma $(K_{si})*K_T$, es introducido, como derecho 52 de acceso a este bloque, en la licencia L_p de terminal destinada al terminal 4. En este caso, durante la etapa 134, el terminal 4 extrae además esta regla de acceso del derecho 52 de la licencia L_p encontrada, luego explota esta regla de acceso para permitir y, alternativamente, inhibir, el acceso de este terminal al segmento S_i, es decir la puesta en práctica de la etapa 136. En variante, en el mismo caso el terminal 4 explota también esta regla de acceso para permitir, y alternativamente inhibir, la realización de la etapa 138.

Las condiciones 1) y 2) utilizadas durante la etapa 142 pueden también escribirse, respectivamente, donde $DS_i \geq DS_{i-1} + \Delta T_1$ y $DS_i \leq DS_{i-1} - \Delta T_2$.

ΔT_1 puede ser nulo. ΔT_2 puede ser igual a un múltiplo estrictamente positivo del criptoperiodo. Por ejemplo, ΔT_2 es entonces superior a 3, 10, 30, 60, 100, 200 u 800 veces el tiempo de un criptoperiodo. Este último caso es por ejemplo utilizado cuando solo menos de un segmento S_i de dos o menos de uno de cinco, o menos de uno de diez, o menos de uno de cincuenta, está asociado con un dato temporal DS_i.

En variante, la etapa 142 es omitida. En este caso, si durante la etapa 140 el terminal determina que el dato temporal DS_i es diferente del código pre-registrado, entonces el procedimiento se continua directa y sistemáticamente por la etapa 144. Por lo tando, la actualización del vencimiento DRP durante la etapa 146 puede omitirse.

En variante, durante la etapa 144, el nuevo vencimiento de renovación DRP es obtenido aleatoriamente o pseudo-aleatoriamente en un intervalo comprendido entre $DS_i - \Delta Te$ y DS_i, donde ΔTe es un umbral positivo. Por ejemplo, ΔTe es igual a 1, 2, 5, 10, 50, 100 ou 500 veces el tiempo de un criptoperiodo.

El nuevo vencimiento de renovación DRP es sistemáticamente tomado igual al dato temporal DS_i recibido. En otro ejemplo, el nuevo vencimiento de renovación DRP es fijado en un subintervalo del intervalo comprendido entre 0 y el

dato temporal DS_i recibido. Por ejemplo, este subintervalo está determinado en función de un identificador del terminal. Por ejemplo, el nuevo vencimiento de renovación DRP es obtenido aleatoriamente o pseudo-aleatoriamente, en este subintervalo. Alternativamente, el nuevo vencimiento de renovación es tomado sistemáticamente igual al límite superior de este subintervalo.

REIVINDICACIONES

1. Procedimiento de suministro, por una cabecera de red, de un contenido multimedia protegido por un sistema de protección de contenidos multimedia, a terminales mecánicamente independientes los unos de los otros y conectados con un mismo servidor de derechos de acceso por mediación de una red de gran distancia de transmisión de informaciones, procedimiento en el cual :
durante una fase (110) de emisión, la cabecera de red :

a) asocia (112) respectivamente, a un primero y un segundo bloques (G_p) de segmentos (S_i) de contenido multimedia, un primero y un segundo derechos (52) de acceso necesarios con un terminal para acceder a cualquier segmento de este primero o de este segundo bloque con miras a jugarlo, comprendiendo cada uno de estos segmentos al menos una secuencia de grupos de imágenes de video o de tramas de audio, comprendiendo este primero y este segundo bloques cada uno uno o varios segmentos, y siendo este primer bloque seguido de este segundo bloque en el contenido multimedia protegido,
b) transmite (116, 118) al terminal, por mediación de una conexión (34) punto a punto, una primera licencia (L_p) que comprende el primer derecho (52) de acceso, y transmite hacia cada uno de los terminales, por mediación de una conexión (32) punto a multipuntos, un flujo (6) que comprende cada segmento (S_i) del primer bloque (G_p), durante una fase (120) de recepción, el terminal:
c) recibe (122) la primera licencia,
d) recibe (124) el flujo, y luego, durante una fase (130) de juego, el terminal :
e) extrae (134) el primer derecho de acceso de la primera licencia, luego utiliza (136) este primer derecho de acceso extraído para permitir y, alternativamente inhibir, el acceso de este terminal a los segmentos del primer bloque, o para descifrar los segmentos del primer bloque,
f) cuando un vencimiento de renovación predeterminado ha llegado, transmite (148), al servidor de derechos de acceso, una petición de derechos de acceso,
g) en respuesta a la petición de derechos de acceso, el servidor de derechos de acceso transmite (116), al terminal, una segunda licencia (L_{p+1}) que comprende el segundo derecho de acceso, procedimiento **caracterizado por que** :

- durante la etapa a), la cabecera de red asocia con cada segmento de una lista de al menos un segmento del primer bloque, un dato temporal (DS_i) que permite determinar si una fecha límite (D_{Gp}) para transmitir al servidor de derecho de acceso la petición de derecho de acceso ha cambiado,

- durante la etapa b) la cabecera de red transmite (118) al terminal, conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado,

- durante la etapa c), el terminal recibe (124), conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado, luego,

- durante una etapa h) anterior a la etapa f), modifica (144) el vencimiento de renovación predeterminado (DRP) en función del último dato temporal recibido para obtener un nuevo vencimiento de renovación predeterminado que permite al terminal decidir, en función de su valor y en un instante dado anterior o igual a la fecha límite (D_{Gp}) que ha cambiado, transmitir al servidor de derechos de acceso una petición de derechos de acceso.

2. Procedimiento según la reivindicación 1, en el cual cualquier derecho de acceso comprende al menos un dato de acceso que pertenece al grupo compuesto por :

- una regla de acceso, que describe los usos del contenido multimedia que el terminal está autorizado a realizar,

- un identificador de esta regla de acceso,

- una dirección de esta regla de acceso,

- una clave(K_{Gp}) criptográfica necesaria para acceder a cualquier segmento del bloque (G_p) de contenido multimedia al cual está asociado el derecho de acceso,

- un identificador de esta clave criptográfica,

- una dirección de esta clave criptográfica, y

- un valor de inicialización que permite calcular ésta clave criptográfica.

3. Procedimiento de emisión, por una cabecera de red, para la realización del procedimiento de la reivindicación 1, de un contenido multimedia protegido, en el cual la cabecera de red :
a) asocia (112) respectivamente, a un primero y un segundo bloques (G_p) de segmentos (S_i) de contenido multimedia, un primero y un segundo derechos (52) de acceso necesarios con un terminal para acceder a cualquier segmento de este primero o de este segundo bloque con miras a jugarlo, comprendiendo cada uno de estos segmentos al menos una secuencia de grupos de imágenes de video o de tramas de audio, comprendiendo este primero y este segundo bloques cada uno uno o varios segmentos, y siendo este primer bloque seguido de este segundo bloque en el contenido multimedia protegido,
b) transmite (116/118) al terminal una primera licencia (L_p) que comprende el primer derecho de acceso, y un flujo que comprende cada segmento del primer bloque, procedimiento caracterizado por que la cabecera de red :
- durante la etapa a), asocia con cada segmento de una lista de al menos un segmento del primer bloque, un dato temporal (DS_i) que permite determinar si una fecha límite (D_{Gp}) para transmitir al servidor de derecho de acceso la petición de derecho de acceso ha cambiado,
- durante la etapa b), transmite (118) al terminal, conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado.

4. Procedimiento de obtención, por un terminal, para la realización del procedimiento de la reivindicación 1, de un contenido multimedia protegido, en el cual el terminal :
durante la fase (120) de recepción :
c) recibe (122) la primera licencia,
d) recibe (124) el flujo, luego,
durante la fase (130) de juego :
e) extrae (134) el primer derecho de acceso de la primera licencia y luego utiliza (136) este primer derecho de acceso extraido con el fin de acceder a los segmentos del primer bloque, al menos para permitir y, alternativamente, para inhibir, el acceso de este terminal a los segmentos del primer bloque, o para descifrar los segmentos del primer bloque,
f) en un vencimiento de renovación predeterminado, transmite (148), al servidor de derechos de acceso, una petición de derechos de acceso,
g) en respuesta a la petición de derechos de acceso, el servidor de derechos de acceso transmite (116), al terminal, una segunda licencia (L_{p+1}) que comprende el segundo derecho de acceso, procedimiento caracterizado por que :
durante la fase (120) de recepción, el terminal :
- durante la etapa c) recibe (124), conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado, y luego,
- durante una etapa h) anterior a la etapa f), modifica (144) el vencimiento de renovación predeterminado (DRP) en función del último dato temporal recibido para obtener un nuevo vencimiento de renovación predeterminado que permite al terminal decidir, en función de su valor y en un instante dado anterior o igual a la fecha límite (D_{Gp}) que ha cambiado, transmitir al servidor de derechos de acceso una petición de derechos de acceso.

5. Procedimiento de obtención según la reivindicación 4, en el cual, durante la etapa h), el terminal :

- determina (142) una de las condiciones $DS_t > DS_{t-1} + \Delta T_1$ y $DS_t \geq DS_{t-1} + \Delta T_1$, donde DS_t es el último dato temporal recibido, DS_{t-1} es el penúltimo dato temporal recibido, y ΔT_1 es un primer umbral predeterminado positivo o nulo,

- si la condition determinada es comprobada, inicia la modificación (144) del vencimiento de renovación predeterminado (DRP) y, sino, no inicia esta modificación del vencimiento de renovación predeterminado.

6. Procedimiento de obtención según la reivindicación 4, en el cual, durante la etapa h), el terminal :

- determina (142) una de las condiciones $DS_t < DS_{t-1} - \Delta T_2$ y $DS_t \leq DS_{t-1} - \Delta T_2$, donde DS_t es el último dato temporal recibido, DS_{t-1} es el penúltimo dato temporal recibido, y ΔT_2 es un segundo umbral predeterminado positivo o nulo,

- si la condition determinada es comprobada, inicia la modificación (144) del vencimiento de renovación predeterminado (DRP) y sino, no inicia esta modificación del vencimiento de renovación predeterminado.

7. Procedimiento según la reivindicación 4, en el cual, durante la etapa h), el terminal modifica (144) el vencimiento de renovación predeterminado (DRP) asignándole un valor calculado en función del último dato temporal recibido y por medio de una función apta para repartir de forma uniforme los vencimientos de renovación predeterminados de los terminales, en un intervalo limitado cuyo límite superior permite al terminal ejecutar la etapa f) en un instante

dado anterior o igual a la fecha límite (D_{Gp}) que ha cambiado, siendo este reparto uniforme y por que los vencimientos de renovación son equiprobables en cualquier subintervalo de amplitud dada comprendido dentro de este invervalo.

8. Procedimiento de obtención según la reivindicación 4, en el cual, en la etapa h), el terminal compara (140) el último dato temporal recibido con un código preregistrado, luego si el último dato temporal es igual a este código preregistrado, el terminal procede inmediatamente a la realización de la etapa f) independientemente del vencimiento de renovación predeterminado (DRP), sin, antes, modificar el vencimiento de renovación predeterminado en función del último dato temporal recibido, y, en el caso contrario, el terminal modifica (144) el vencimiento de renovación predeterminado en función del último dato temporal recibido y luego procede a la realización de la etapa f) (146, 148) únicamente cuando el vencimiento de renovación predeterminado es alcanzado.

9. Soporte de registro de informaciones (16, 46), caracterizado por que comprende instrucciones para la realización de un procedimiento conforme a una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un ordenador electrónico (14, 44).

10. Cabecera (1) de red para la realización de un procedimiento de emisión de un contenido multimedia protegido conforme a la reivindicación 3, en el cual la cabecera de red es apta :

a) para asociar respectivamente, a un primero y un segundo bloques de segmentos de contenido multimedia, un primero y un segundo derechos de acceso necesarios para un terminal (4) para acceder a cualquier segmento de este primero o de este segundo bloque con miras a jugarlo, comprendiendo cada uno de estos segmentos al menos una secuencia de grupos de imágenes de video o de tramas de audio, comprendiendo este primero y este segundo bloques cada uno uno o varios segmentos, y siendo este primer bloque seguido de este segundo bloque en el contenido multimedia protegido,

b) para transmitir al terminal (4) una primera licencia que comprende el primer derecho de acceso, y un flujo que comprende cada segmento del primer bloque,

cabecera de red caracterizada por que comprende un ordenador electrónico (14) programado para :

- durante la etapa a), asociar con cada segmento de una lista de al menos un segmento del primer bloque, un dato temporal que permite determinar si una fecha límite para transmitir al servidor (2) de derecho de acceso la petición de derecho de acceso ha cambiado,

- durante la etapa b), transmitir al terminal, conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado.

11. Terminal (4) para la realización de un protecimiento de obtención de un contenido multimedia protegido conforme a una cualquiera de las reivindicaciones 4 a 8, en el cual el terminal es apto :
durante la fase de recepción :
c) para recibir la primera licencia,
d) para recibir el flujo, luego,
durante la fase de juego :
e) para extraer el primer derecho de acceso de la primera licencia, luego para utilizar este primer derecho de acceso extraido con el fin de acceder a los segmentos del primer bloque, al menos para permitir y, alternativamente, para inhibir, el acceso de este terminal a los segmentos del primer bloque, o para descifrar los ssegmentos del primer bloque,
f) cuando un vencimiento de renovación predeterminado es alcanzado, para transmitir, al servidor (2) de derechos de acceso, una petición de derechos de acceso,
terminal caracterizado por que comprende un ordenador electrónico (44) programado para:
durante la fase de recepción :
- durante la etapa c), recibir, conjuntamente con cada segmento de la lista de segmentos del primer bloque, su dato temporal asociado, luego,
- durante la etapa h), modificar el vencimiento de renovación predeterminado en función del último dato temporal recibido para obtener un nuevo vencimiento de renovación predeterminado que permita al terminal decidir, en función de su valor y en un instante dado anterior o igual a la fecha límite que ha cambiado, transmitir al servidor de derechos de acceso una petición de derechos de acceso.

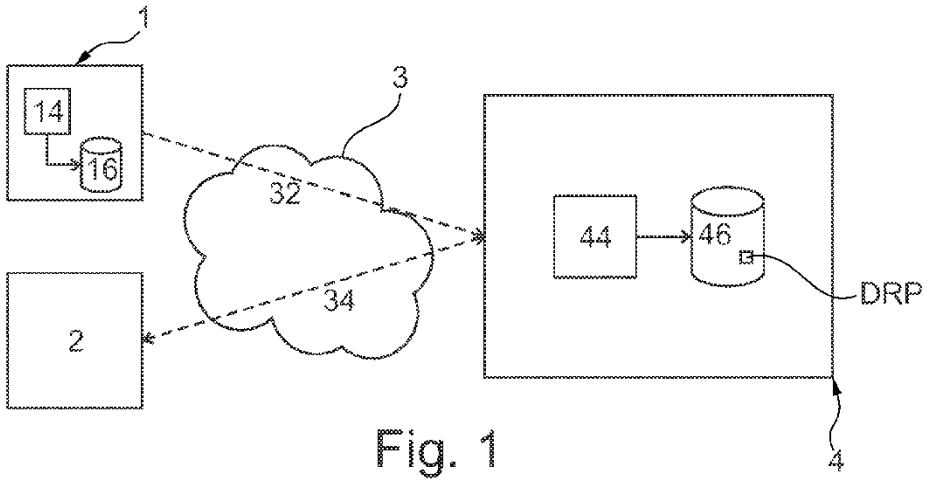

Fig. 1

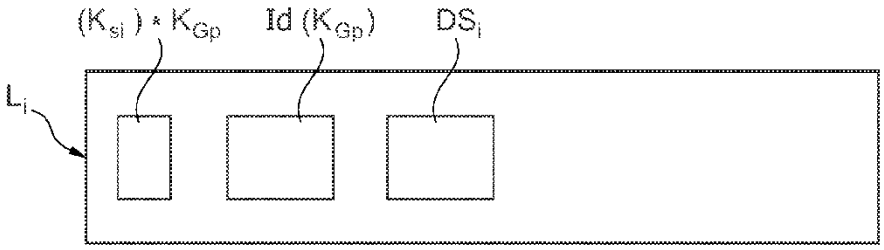

Fig. 2

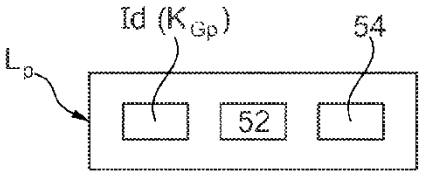

Fig. 3

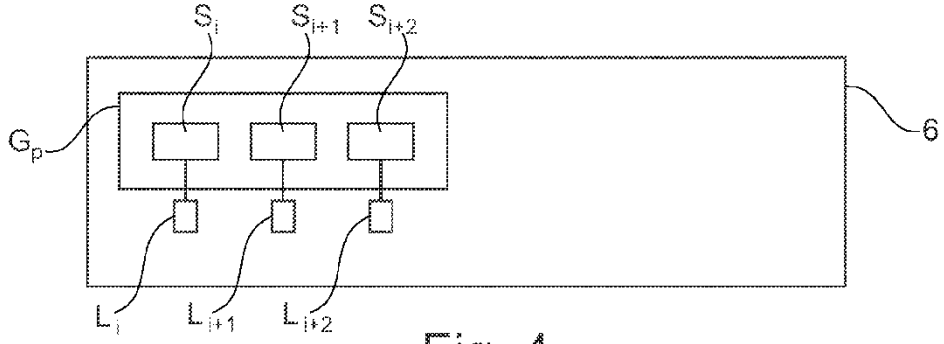

Fig. 4

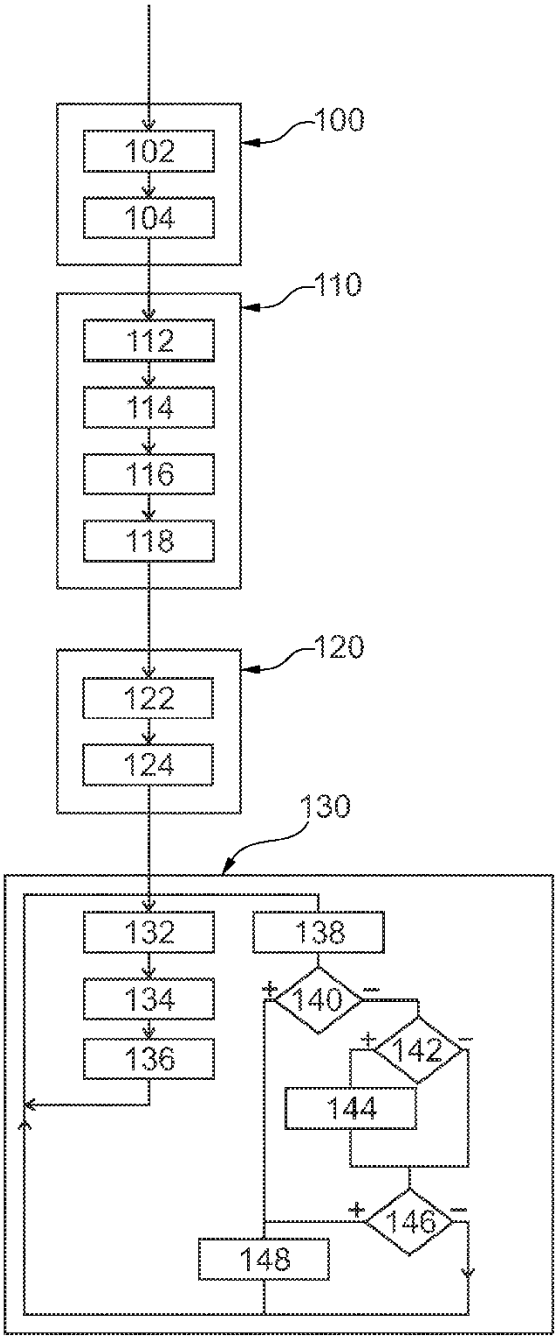
100
102
104
110
112
114
116
118
120
122
124
130
132
134
136
138
140
142
144
146
148
+
−
+
−
+
−

Fig. 5