(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 637 300**

(51) Int. CI.:

G06F 21/10 (2013.01)
H04N 21/254 (2011.01)
H04N 21/258 (2011.01)
H04N 21/658 (2011.01)
H04N 21/8355 (2011.01)
H04N 21/6334 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.08.2014 PCT/EP2014/066678**

(87) Fecha y número de publicación internacional: **12.02.2015 WO15018775**

(96) Fecha de presentación y número de la solicitud europea: **04.08.2014 E 14748190 (7)**

(97) Fecha y número de publicación de la concesión europea: **14.06.2017 EP 3031000**

(54) Título: **Procedimiento para proporcionar una licencia en un sistema de suministro de contenidos multimedia**

(30) Prioridad:

09.08.2013 FR 1357946

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.10.2017

(73) Titular/es:

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

(72) Inventor/es:

BOIVIN, MATHIEU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCION

Procedimiento para proporcionar una licencia en un sistema de suministro de contenidos multimedia

La invención se refiere a un procedimiento para proporcionar una licencia en un sistema de suministro de contenidos multimedia. La invención se refiere igualmente a un procedimiento de computación de una licencia, para la realización de este procedimiento. La invención se refiere por último a un servidor de licencias y a un soporte de registro de informaciones para la realización de este procedimiento.

El sistema para proporcionar contenidos multimedia considerado, es cualquier sistema de soporte de cualquier servicio de suministro en línea de contenidos multimedia a una pluralidad de terminales de usuarios.

Un terminal de usuario es un terminal asociado con este usuario, es decir del cual un identificador es registrado en relación con un identificador de este usuario. Aquí, este registro es estático, resultante de una toma anterior a la utilización del terminal por el usuario. Por ejemplo, responde a la declaración, por el operador del servicio o por el usuario, de que este último es titular del terminal.

Un terminal es utilizado por un usuario del sistema de suministro de contenidos multimedia para acceder a un contenido multimedia. Acceder a un contenido multimedia, significa aquí jugar claro, registrarlo, o realizar cualquier otra utilización ofrecida por el sistema de suministro de contenidos multimedia.

Los contenidos multimedia suministrados 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 vídeo y/o audio tal como una aplicación informática, un juego, un diaporama, una imagen o cualquier conjunto de datos.

Un contenido multimedia de este tipo, particularmente cuando es objeto de derechos tales como derechos de autor o derechos relacionados, normalmente es proporcionado de forma cifrada a título de su protección por un sistema de gestión de derechos digitales, o DRM, por Digital Rights Management, en inglés. Este cifrado se realiza normalmente por medio de una clave llamada de contenido, por un algoritmo simétrico.

La terminología del ámbito de los sistemas de gestión de derechos digitales se utiliza así en lo que sigue de este documento. El lector interesado podrá por ejemplo encontrar una presentación más completa en los documentos siguientes:

- Relacionados con la arquitectura general de un sistema de DRM: DRM Architecture, Draft versión 2.0, OMA-DRM-ARCH-V2_0-20040518-D, Open Mobile Alliance, 18 de Mayo 2004
- Relacionados más particularmente con las licencias: DRM Specification, Draft versión 2.1, OMA-TS-DRM-DRM-V2_1-20060523-D, Open Mobile Alliance, 23 de Mayo 2006.

En un sistema de gestión de derechos digitales de este tipo, una licencia permite a un terminal de un usuario acceder a un contenido multimedia.

De estructura bien conocida por el experto en la materia, esta licencia contiene al menos un dato de acceso necesario para este terminal para acceder al contenido. Este dato de acceso depende de un identificador del contenido multimedia y de un identificador del usuario o de un terminal del usuario, como máximo. Así, cada dato de acceso está asociado, por una relación inyectiva o biyectiva, con un solo par de identificadores, estando cada par de identificadores formado por:

- el identificador del contenido multimedia, y
- el identificador del usuario o de uno terminal del usuario.

Un dato de acceso es típicamente:

- una regla de acceso, que describe los usos del contenido multimedia que el terminal del usuario está autorizado a realizar, o
- una clave de contenido, necesaria para el descifrado del contenido multimedia por un algoritmo de descifrado, por ejemplo, simétrico.

La clave de contenido se introduce generalmente en la licencia en forma de un criptograma obtenido por cifrado de la clave de contenido con una clave propia del terminal.

El cálculo de cada licencia requiere por consiguiente del servidor de licencias recursos nada despreciables, particularmente para ejecutar algoritmos criptográficos potencialmente complejos.

En un sistema de suministro de contenidos multimedia de este tipo, un terminal que desee acceder a un contenido

multimedia debe por consiguiente haber obtenido la licencia necesaria. Esta obtención puede por ejemplo tener lugar a continuación de un acontecimiento tal como:

- una suscripción al servicio por el usuario al cual está asociado el terminal,
- una renovación de ésta suscripción,
- una compra del contenido multimedia por el usuario, o
- una solicitud de acceso al contenido por el terminal.

Un acontecimiento de este tipo da lugar al sometimiento de una petición de licencia a un servidor de licencias que comprende el sistema, luego, en respuesta, a la computación y al suministro al terminal, por este servidor, de la licencia correspondiente.

Un sistema de suministro de contenidos multimedia de este tipo comprende generalmente un gran número de terminales de usuarios. En este contexto, su servidor de licencias es por consiguiente susceptible de estar sometido a picos de carga, en términos de número de peticiones de licencias a tratar, y de recursos de computación requeridos a este efecto, en ciertos momentos, por ejemplo dedicados a la renovación de las suscripciones, o en la catalogación del servicio, de contenidos esperados.

Por otro lado, la naturaleza de los servicios ofrecidos por un sistema de suministro de contenidos multimedia de este tipo, implica un reparto temporal no homogéneo de las peticiones de licencia. En efecto, en el caso de servicios de televisión, y más precisamente de servicios de tipo «à la demande» (“a demanda”), es conocido que las compras de contenidos multimedia, o las demandas de acceso a estos contenidos, y por consiguiente las peticiones de licencias sometidas al servidor de licencias, sean más numerosas en ciertos momentos del día, principalmente en los momentos en que la mayoría de los usuarios se encuentran en disposición de utilizar el sistema. Este hecho aumenta todavía el riesgo, para el servidor de licencias, de estar sometido a los picos de carga ya mencionados.

La complejidad potencial de la computación de una licencia obtenida, aumenta también este riesgo.

El riesgo identificado de picos de carga del servidor de licencias, amenaza la capacidad de este servidor en emitir, en un tiempo limitado de forma que no penalice la calidad del servicio, las licencias requeridas.

Resulta por consiguiente particularmente interesante limitar este riesgo.

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

-WO0058811A2,

-WO0021239A1.

La invención trata de aumentar la capacidad del servidor de licencias a emitir, en un tiempo limitado, las licencias requeridas.

La invención tiene así por objeto un procedimiento para proporcionar una licencia conforme a la reivindicación 1.

En un procedimiento de este tipo, la operación de pre-computación de al menos un dato de acceso de una licencia, en la etapa e) anterior a la etapa a) de recepción de la petición de licencia, permite, en la etapa b), seleccionar el dato pre-computado sin tener que generarlo en ese momento, y por consiguiente aligerar así la carga de computación del servidor de licencias en respuesta a la recepción de la petición de licencia, si la licencia requerida es la licencia para la cual el indicado dato de acceso ha sido pre-computado.

En un procedimiento de este tipo, la obtención de la primera lista de recomendación para el usuario, y la selección, en esta primera lista, de los identificadores de contenidos utilizados para la operación de pre-computación, permiten aumentar la probabilidad de que la licencia requerida en la etapa a) se encuentre entre aquellas para las cuales un dato de acceso ha sido pre-computado en la etapa e). Se aumenta así la probabilidad de que se produzca de improviso el aligeramiento de la carga de computación del servidor de licencias potencialmente proporcionado por la operación de pre-computación. La primera lista de recomendación se caracteriza en efecto como contenedor de un número limitado de identificadores de contenidos multimedia entre un conjunto mayor de contenidos multimedia disponibles en el sistema, teniendo los contenidos multimedia identificados por esta primera lista una probabilidad mayor de ser accedidos por el terminal del usuario que los otros contenidos multimedia del conjunto mayor.

Los modos de realización de este procedimiento para proporcionar una licencia pueden comprender la característica de la reivindicación 2.

Estos modos de realización de este procedimiento para proporcionar una licencia presentan además la ventaja siguiente:

- las operaciones de transmisión, al terminal o a otro terminal del usuario, de la primera o de una segunda lista de recomendación elaborada para este usuario y de visualizado, por el o el indicado otro terminal del usuario, de esta primera o segunda lista de recomendación, permiten favorecer la selección por el usuario de uno de los identificadores de contenidos multimedia para el cual el dato de acceso ha sido pre-computado.

La invención tiene igualmente por objeto un procedimiento de computación, por un servidor electrónico de licencias, para la puesta en práctica del procedimiento indicado anteriormente, de una licencia.

Los modos de realización de este procedimiento de computación de una licencia, pueden comprender una o varias de las características de las reivindicaciones dependientes de procedimiento de computación.

Estos modos de realización de este procedimiento de computación de una licencia presentan además las ventajas siguientes:

- las operaciones de computación de la carga de trabajo del servidor de licencias y de inhibición o de activación de la etapa e), en función de la carga de trabajo calculada, permiten no activar la etapa e) del procedimiento si la carga de trabajo computada es ya excesiva, y por consiguiente no agravar aún más el pico de carga.

La invención tiene igualmente por objeto un soporte de registro de informaciones que comprende instrucciones para la ejecución de la etapa e) del procedimiento indicado anteriormente de computación de una licencia, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

La invención tiene por último por objeto un servidor de licencias que comprende un ordenador electrónico programado para activar y ejecutar la etapa e) del procedimiento indicado anteriormente de computación de una licencia.

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,

• La figura 2 es una representación esquemática de un procedimiento de suministro de licencia en un sistema de suministro de contenidos multimedia.

En estas figuras, las mismas referencia se facilitan para designar los mismos elementos.

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

La figura 1 representa un sistema 2 de suministro de contenidos multimedia para la realización de un procedimiento para proporcionar una licencia.

Este sistema 2 comprende una pluralidad, típicamente millares, de terminales de usuarios, conectados, por mediación de una red 20, por una parte a un servidor 30 de contenidos multimedia, y por otra parte a una portada 40 de servicio. Aquí, se supone que todos estos terminales de usuario son idénticos. Así, para simplificar la ilustración, solo se representa un terminal 10 en la figura 1.

El terminal 10 comprende un ordenador electrónico 12 programable, una memoria 14 y una interfaz hombre-máquina 16. El ordenador 12 es apto para ejecutar instrucciones registradas en la memoria 14. La memoria 14 comprende las instrucciones necesarias para ejecutar el procedimiento de la figura 2. Además, la memoria 14 comprende un identificador 18 de terminal. Este identificador 18 identifica de forma única el terminal 10 entre el conjunto de terminales de usuario del sistema 2.

La interfaz hombre-máquina 16 comprende típicamente una pantalla y un telemando que permite seleccionar una zona particular de la pantalla.

La red 20 es una red gran distancia de distribución de informaciones que permite establecer una comunicación bidireccional entre uno cualquiera de los terminales del sistema 2 y la portada 40 y el servidor 30. Por ejemplo, la red 20 es la tela de araña mundial, más conocida bajo el término de «réseau Internet» (red internet).

El servidor 30 permite a un terminal cualquiera del sistema 2 obtener, por ejemplo telecargando, un contenido multimedia cifrado. A este efecto, el servidor 30 comprende un ordenador electrónico 32 programable y una memoria 34. El ordenador 32 es apto para ejecutar instrucciones registradas en la memoria 34. La memoria 34 contiene

particularmente las instrucciones necesarias para la ejecución del procedimiento de la figura 2. Esta memoria 34 contiene también una librería 36. Esta librería contiene los contenidos multimedia que cada terminal puede telecargar a través de la red 20. En esta librería 36, los contenidos multimedia están registrados en forma cifrada. Cada contenido multimedia cifrado se obtiene cifrando el contenido multimedia en claro con la ayuda de su propia clave criptográfica K_c y por un algoritmo de cifrado simétrico. Así, la clave K_c utilizada para cifrar un contenido multimedia es únicamente utilizable para descifrar este contenido multimedia y no otro. Por «en clair» (en claro) se designa un contenido multimedia que puede ser restituido por un terminal de forma perceptible y directamente comprensible por un ser humano sin tener que recurrir a una operación de descifrado. A título de ejemplo, la librería 36 contiene un contenido multimedia 38 tal como una película o una música.

La portada 40 permite al terminal 10 obtener una licencia propia para permitirle acceder a un contenido multimedia para el cual su usuario ha adquirido legalmente los derechos de acceso.

La portada 40 se encuentra a este respecto conectada con un motor 50 de recomendación, y con un servidor 60 de licencias.

Aquí, la portada 40 comprende un ordenador electrónico 42 programable y una memoria 44. El ordenador 42 es apto para ejecutar instrucciones registradas en la memoria 44 para poner en práctica el procedimiento de la figura 2.

La memoria 44 contiene además una lista 46 de usuarios del sistema 2. Esta lista 46 contiene una descripción de cada uno de estos usuarios y, particularmente un identificador para cada uno de los usuarios. Este identificador, llamado de usuario, permite identificar de forma única el usuario entre el conjunto de usuarios del sistema 2. Esta descripción comprende también típicamente una descripción de los derechos de acceso del usuario a los contenidos multimedia ofrecidos por el servicio.

La memoria 44 contiene también una lista 48 de terminales de cada uno de los usuarios del sistema. Esta lista contiene una descripción de cada uno de los terminales del usuario. La misma asocia por consiguiente, particularmente, con cada identificador de usuario uno o varios identificadores de terminal.

La portada 40 es apta para mantener estas listas 46 y 48, es decir añadir a las mismas, modificar o suprimir una descripción.

El motor 50 de recomendación es apto para construir automáticamente, a partir de un identificador de un usuario o de su terminal, una lista de recomendación para este usuario. Una lista de recomendación es una lista que contiene un número limitado de identificadores de contenidos multimedia seleccionados entre el conjunto de contenidos multimedia accesibles en el sistema 2. Cada identificador de contenido multimedia identifica de forma única un contenido multimedia entre el conjunto de contenidos multimedia accesibles en el sistema 2. Los contenidos multimedia identificados por esta lista tienen cada uno una probabilidad mayor de ser accedido por el terminal del usuario que los otros contenidos multimedia del sistema 2 no seleccionados. Típicamente, cada lista de recomendación comprende menos de N/4 o N/10 o N/100 o también N/1000 identificadores de contenidos multimedia, donde N es el número total de identificadores de contenidos multimedia accesibles en el sistema 2. Por ejemplo, la lista de recomendación comprende de uno a cien identificadores de contenidos multimedia. Los algoritmos de recomendación que permiten construir automáticamente esta lista son bien conocidos y no se describirán aquí en detalle. Por ejemplo, el lector podrá referirse a la solicitud de patente US 2005/0193414. A este respecto, el motor 50 comprende un ordenador electrónico 52 programable y una memoria 54. El ordenador 52 es apto para ejecutar instrucciones registradas en la memoria 54 para poner en práctica el procedimiento de la figura 2. En particular, la memoria 54 comprende las instrucciones del algoritmo de recomendación. La memoria 54 comprende además una base 56 de datos que permite calcular la probabilidad de que un contenido multimedia dado sea accedido por un terminal o un usuario dado. A este respecto, típicamente, la base 56 contiene para cada terminal o cada usuario:

- un histórico que contiene los identificadores de los contenidos multimedia a los cuales este terminal o este usuario ha accedido ya antes, y/o
- datos respecto al usuario del terminal 10, tal como su edad, su sexo, su nacionalidad o su pertenencia a una categoría predeterminada de usuarios.

Los datos del usuario pueden ser encontrados de nuevo gracias al identificador del terminal y con la ayuda de la lista 48. En efecto, la lista 48 permite encontrar el identificador del usuario al cual pertenece el terminal a partir del identificador de terminal. Seguidamente, es posible consultar la descripción del usuario asociada por la lista 46 con el identificador de usuario encontrado en la lista 48.

El servidor 60 de licencias es apto para computar y para proporcionar una licencia que permita a un terminal de usuario acceder a un contenido multimedia.

El servidor 60 de licencias comprende a este respecto una memoria 64 y un ordenador electrónico 62 programable apto para ejecutar instrucciones registradas en un soporte de registro. A este efecto, el ordenador 64 está conectado

con la memoria 62. Esta memoria 62 comprende las instrucciones necesarias para poner en práctica el procedimiento de la figura 2. Estas instrucciones comprenden particularmente las de un algoritmo de computación de una licencia.

La memoria 64 del servidor 60 de licencias contiene una lista 66 del conjunto de terminales del sistema 2. Esta lista contiene una descripción de cada uno de estos terminales y, particularmente su identificador de terminal. Esta descripción comprende típicamente al menos una clave criptográfica K_T propia de cada terminal considerado o de un grupo de terminales de un usuario. Aquí, la clave K_T es diferente de un terminal a otro.

La memoria 64 contiene también una lista 68 del conjunto de contenidos multimedia accesibles por los terminales en el sistema 2. Esta lista contiene una descripción de cada uno de estos contenidos multimedia y, particularmente, el identificador de cada contenido multimedia. Además, esta lista 68 asocia con cada uno de los identificadores de contenido multimedia:

- la clave K_c de contenido utilizada para cifrar este contenido multimedia, y de preferencia,
- normas de acceso predefinidas a este contenido multimedia.

Las normas de acceso definen típicamente lo que un terminal puede hacer con este contenido multimedia. Por ejemplo, son estas normas de acceso las que precisan:

- el número de veces en que el contenido multimedia puede ser accedido,
- el periodo de tiempo durante el cual puede ser accedido, o
- si el contenido multimedia puede ser registrado o no en un soporte de registro.

El servidor 60 de licencias es apto para mantener estas listas 66 y 68, es decir añadir a las mismas, modificar o suprimir una descripción.

La memoria 64 contiene también una base 69 de datos de acceso pre-computados. Aquí, un dato de acceso es un criptograma K_c* obtenido cifrando la clave K_c asociada con un contenido multimedia por la lista 68, con la clave K_T de un terminal.

Más precisamente, la base 69 asocia juntos un identificador de contenido multimedia, un identificador de terminal y el dato de acceso pre-computado para el contenido multimedia y el terminal especificados por los dos identificadores anteriores. Así, este dato de acceso pre-computado comprende particularmente el criptograma K_c* obtenido cifrando la clave K_c, asociada por la lista 68 con este identificador de contenido multimedia, con la clave K_T asociada por la lista 66 con este identificador de terminal.

La arquitectura anteriormente presentada del sistema de suministro de contenidos es de carácter funcional, y como tal susceptible de ser proyectada en múltiples arquitecturas técnicas. Así, el servidor 30 de contenidos multimedia y la portada 40 de servicio, pueden residir en una misma máquina informática o en máquinas distintas. Sucede lo mismo con la portada 40, el motor 50 y el servidor 60 de licencias. Por último, la portada 40 que reagrupa el conjunto de la lógica del servicio que no está relacionado con el motor 50 de recomendación o del servidor 60 de licencias, su análisis funcional es susceptible de llevar a definir componentes funcionales que puedan a su vez residir en una misma máquina informática, cada una en una máquina distinta, o, de forma intermedia, por grupos en máquinas distintas.

El funcionamiento del sistema 2 se describirá ahora con referencia al procedimiento de la figura 2 en el caso particular en que el terminal 10 se utilice para acceder al contenido multimedia 38.

Inicialmente, el terminal 10 se conecta con la portada 40 a través de la red 20. Durante el establecimiento de esta conexión, el identificador 18 del terminal 10 es transmitido a la portada 40. En respuesta, la portada 40 encuentra en la lista 48 el identificador de usuario asociado con el identificador 18 y transmite este identificador de usuario al motor 50 de recomendación.

Seguidamente, en una etapa 102, el motor 50 de recomendación elabora una lista de recomendaciones para el usuario del terminal 10. La probabilidad de que un contenido multimedia sea accedido a partir del terminal 10 se calcula a partir de los datos contenidos en la base 56 de datos. Aquí, la lista de recomendaciones elaborada es adecuada para cada usuario, es decir que la misma es elaborada en función del identificador de usuario recibido. Por lo tanto, normalmente, la lista de recomendaciones varía de un identificador de usuario a otro. Una vez elaborada, la lista de recomendaciones se transmite a la portada 40.

En una etapa 104, la portada 40 transmite esta lista de recomendaciones construida al terminal 10. En respuesta, el terminal 10 la comunica al usuario por mediación de su interfaz hombre-máquina 16. Por ejemplo, el terminal 10 visualiza la lista de recomendaciones en la pantalla del terminal 10. Aquí, esta lista se visualiza de forma que el usuario pueda fácilmente seleccionar un identificador de contenido multimedia entre los visualizados. Sin embargo, si ninguno de los contenidos multimedia de la lista de recomendaciones interesa al usuario, el terminal 10, por

mediación de su interfaz hombre-máquina 16, permite al usuario seleccionar el identificador de otro contenido multimedia que no forme parte de esta lista de recomendación.

Una vez el usuario ha seleccionado el identificador de un contenido multimedia al cual desea acceder, este identificador es transmitido del terminal 10 a la portada 40 por mediación de la red 20. La portada 40, en respuesta, transmite una petición al servidor 60 conteniendo a la vez el identificador del contenido multimedia seleccionado por el usuario y el identificador del terminal 10. Luego, se supone que el identificador seleccionado corresponde con el contenido multimedia 38.

Así, en una etapa 130, el servidor 60 recibe esta petición.

En respuesta, en una etapa 140, el servidor 60 computa una licencia que contenga las informaciones necesarias para permitir al terminal 10 acceder al contenido multimedia 38. Como se ha indicado anteriormente, esta licencia contiene particularmente al menos un dato de acceso.

Más precisamente, la etapa 140 comienza por una operación 141 en la cual el servidor 60 busca en la base 69 de datos si el identificador 18 está asociado con el identificador del contenido multimedia contenido en la petición recibida. Si el identificador 18 y el identificador 38 no están asociados uno con el otro en la base 69, entonces el servidor 60 procede inmediatamente a una operación 142 de generación de datos de acceso que corresponden a los identificadores 18 y 38 contenidos en la petición recibida en la etapa 130. En particular, en la operación 142, el servidor 60 construye el criptograma K_c* obtenido cifrando las claves K_c utilizada para cifrar el contenido 38 con la clave K_T del terminal 10 y utilizando un algoritmo de cifrado, típicamente simétrico, conocido a la vez por el servidor 60 y el terminal 10. La clave K_T se obtiene buscando la clave asociada con el identificador 18 en la lista 66. La clave K_c es en cuanto a la misma obtenida buscando en la lista 68 la clave de contenido asociada con el identificador 38. Eventualmente, las normas de acceso asociadas con este contenido multimedia 38 por la lista 68 son igualmente extraídas para ser incorporadas a otro dato de acceso elaborado.

A continuación, en una operación 144, el servidor 60 finaliza la computación de la licencia incorporando en ella datos suplementarios tales como una indicación que permita evitar los ataques por reiteración o una fecha de validez de la licencia computada a partir de la fecha de recepción de la petición.

Si en la operación 141, el servidor 60 determina que el identificador 18 y el identificador 38 están asociados uno con el otro en la base 69, entonces en lugar de proceder a una operación 142, el servidor 60 procede inmediatamente a una operación 146.

En la operación 146, el servidor 60 selecciona automáticamente el dato de acceso pre-calculado asociado a la vez, en la base 69, con el identificador 18 y con el identificador 38. Seguidamente, el servidor 60 procede a la operación 144. Sin embargo, en este caso, en la operación 144, los datos de acceso pre-computados se utilizan en lugar de los elaborados en la operación 142. Así, cuando la operación 146 es ejecutada, la operación 142 no lo es. Por lo tanto, la ejecución de la etapa 140 es mucho más rápida ya que ninguna operación de cifrado de la clave K_c con la clave K_T es ejecutada. El servidor 60 es por consiguiente capaz de tratar muchas más peticiones en el mismo tiempo con los mismos recursos materiales con relación al caso donde ningún dato de acceso se ha pre-computado.

La pre-computación de los datos de acceso de realiza antes de la etapa 130, en las etapas 112, 114 y 120 que se describen con detalle más adelante.

Una vez terminado el cálculo de la licencia, en una etapa 150, el servidor 60 transmite la licencia a la portada 40 que la transmite a su vez al terminal 10.

En una etapa 160, el terminal 10 recibe la licencia computada. En respuesta, descifra el criptograma K_c* con su clave K_T para extraer la clave K_C.

En paralelo, en una etapa 162, el terminal 10 telecarga el contenido multimedia 38 a partir del servidor 30 y a través de la red 20. Seguidamente, una vez terminada esta telecarga, accede al contenido multimedia 38. Para ello, el terminal 10 descifra el contenido multimedia 39 con la clave K_c extraída de la licencia recibida con el fin de obtener el contenido multimedia 38 en claro. A continuación, el contenido multimedia 38 en claro es representado en la interfaz hombre-máquina 16 del terminal 10 de forma que sea directamente perceptible y comprensible por un ser humano.

Por ejemplo, la etapa 112 se inicia cuando el servidor 60 de licencias recibe de la portada 40 una lista de identificadores de nuevos usuarios del sistema, una lista de identificadores de nuevos terminales de usuarios, una lista de identificadores de contenidos multimedia nuevamente accedidos por terminales de usuarios, una lista de identificadores de usuarios dados de baja, o una lista de identificadores de terminales dados de baja. Cuando un usuario o un terminal se da de baja, es que ya no forma parte del sistema 2.

La novedad se entiende aquí desde la última realización de la etapa 112. La etapa 112 es por ejemplo realizada, automáticamente o a iniciativa del operador del servicio, según su curso, es decir a medida que se va produciendo el

registro y la baja de usuarios o de terminales de usuarios, y de acceso de terminales de usuarios a contenidos multimedia.

En esta etapa 112, en caso de recepción de una lista de identificadores de nuevos terminales de usuarios o de terminales dados de baja, el servidor 60 de licencias añade o suprime de su lista 66, la descripción de cada uno de estos terminales.

En esta etapa 112, en caso de recepción de una lista de identificadores de contenidos multimedia que han accedido nuevamente por terminales de usuarios o suprimidos del servidor 30, el servidor 60 de licencias añade o suprime de su lista 68, la descripción de cada uno de estos contenidos multimedia.

En esta etapa 112 el servidor 60 de licencias actualiza una lista de usuarios activos desde la última activación de la etapa 120. Esta lista contiene los identificadores de los nuevos usuarios del sistema, los identificadores de los usuarios de los nuevos terminales, y los identificadores de los usuarios de los terminales que han accedido de nuevo a al menos un contenido multimedia. Los identificadores de los usuarios que se han dado de baja se suprimen de esta lista.

A continuación, en una etapa 114, el servidor 60 de licencias computa su propia carga de trabajo en función del número de peticiones que ha recibido en el transcurso de un intervalo de tiempo dado, y de la duración de este intervalo de tiempo. Las peticiones de las que se trata son las recibidas en iteraciones de la etapa 130 para el conjunto de terminales del sistema 2. Este intervalo de tiempo tiene por ejemplo la fecha actual por fecha final, y una duración predeterminada de unos minutos a algunas horas. Se trata por ejemplo de los cinco últimos minutos transcurridos o de la última media hora transcurrida. Desde luego, cualquier otro intervalo de tiempo puede ser tenido en cuenta, particularmente en función del periodo esperado de las fluctuaciones de la carga de trabajo. La carga de trabajo del servidor 60 de licencias es por ejemplo evaluada como el número de peticiones recibidas durante el intervalo de tiempo dividido por la duración de este intervalo de tiempo. Cualquier otro método de evaluación de esta carga de trabajo a disposición del experto en la materia puede sin embargo desde luego ser aplicada.

En la etapa 114, el servidor 60 de licencias inhibe o activa seguidamente la etapa 120. La decisión es tomada en función de la carga de trabajo computada. Típicamente, si la carga de trabajo computada es lo suficientemente baja, la etapa 120 es activada, y de lo contrario es inhibida. Por ejemplo, un umbral S1 se fija previamente y la etapa 120 se inicia si la carga de trabajo computada es inferior a este umbral S1 y, en caso contrario, inhibida.

Para activar la etapa 120, el servidor 60 de licencias transmite, al motor 50 de recomendación, uno al menos de los elementos de la lista de usuarios activos del sistema, y suprime de esta lista los elementos transmitidos.

En la etapa 120, el servidor 60 de licencias pre-computa las licencias.

A este respecto, en una operación 122, el motor 50 de recomendación produce una lista de recomendación para cada terminal de usuarios activos del sistema del cual ha recibido el identificador. Aquí, cada lista de recomendación es elaborada utilizando el mismo algoritmo de recomendación y la misma base 56 que las utilizadas en la etapa 102. Así, cada lista de recomendación comprende, de preferencia, más del 50%, y generalmente más del 80%, de identificadores de contenidos multimedia en común con la lista elaborada para el mismo usuario en una ejecución ulterior de la etapa 102. Sin embargo, las listas elaboradas en la etapa 102 y la operación 122 para el mismo usuario pueden no ser rigurosamente idénticas, por ejemplo, pues la base 56 ha sido modificada entre las ejecuciones de la operación 122 y de la etapa 102.

Aquí, el motor 50 retorna seguidamente cada una de estas listas de recomendación al servidor 60 de licencias, y no, como en una utilización clásica, a la portada 40 para visualizado por un terminal del usuario en cuestión.

A continuación, en una operación 124, el servidor 60 de licencias selecciona, en al menos una de las listas de recomendación recibidas y, típicamente, en cada lista de recomendación recibida, al menos un identificador de contenido multimedia. El modo de selección utilizado aquí es una selección de concepción esencialmente guiada por el tamaño de las listas de recomendación producidas por el motor 50 y por las capacidades de computación del servidor 60 de licencias. Por ejemplo, todos los identificadores de contenidos multimedia de cada lista de recomendación recibida son seleccionados, un número fijo de ellos, o un número dependiente de la carga de trabajo del servidor 60 de licencias previamente computada.

A continuación, en una operación 126, el servidor 60 de licencias pre-computa, para cada identificador seleccionado, el dato de acceso que permite al terminal del usuario en cuestión acceder al contenido multimedia de identificador seleccionado.

El servidor 60 de licencias memoriza seguidamente en la base 69, en relación con el identificador del contenido multimedia seleccionado y con el identificador del terminal considerado del usuario, el dato de acceso pre-computado.

Numerosos otros modos de realización de la invención son posibles. Por ejemplo, la asociación de un terminal con un usuario, es dinámica, por ejemplo resultante de la conexión, por medio del terminal, del usuario con el servicio.

En variante, el identificador de usuario transmitido al motor 50 de recomendación es sustituido por el identificador 18 del terminal de este usuario. En este modo de realización, la lista de recomendación es elaborada para cada identificador de terminal y no por cada usuario.

En otro modo de realización, el contenido multimedia puede ser proporcionado, por el sistema de suministro de contenidos multimedia, cifrado con varias claves a título de su protección por el sistema de gestión de derechos digitales. Varias licencias, conteniendo cada una al menos una de estas claves de contenido, pueden entonces ser necesarias para el terminal para acceder al contenido multimedia. El procedimiento reivindicado se aplica entonces a una, al menos, de estas licencias.

De forma alternativa, el contenido multimedia puede ser proporcionado protegido por un sistema de gestión de derechos digitales sin no obstante estar cifrado. La clave del contenido no figura entonces entre los datos de acceso introducidos en la licencia.

En otro modo de realización, el contenido multimedia se proporciona protegido por un sistema de acceso condicional, o CAS, por Conditional Access System. La terminología 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, Nº 266, el 21 de Diciembre 1995. El procedimiento reivindicado se aplica entonces al suministro de las palabras de control cifradas con la clave K_T del terminal, o mensajes EMM necesarios para el encauzamiento de los derechos o de las claves de explotación, particularmente.

En otro modo de realización, el contenido multimedia puede igualmente ser proporcionado, por el sistema, protegido por cualquier otro tipo de sistema de protección de contenidos, tal por ejemplo como un sistema de protección de datos más clásico que no realiza gestión de derechos de acceso. El procedimiento reivindicado se aplica entonces en el suministro de los mensajes necesarios para la conducción de las claves de cifrado, por ejemplo.

En otro modo de realización, la red 20 es cualquier red de gran distancia de distribución de informaciones distinta de la red Internet, que ofrezca un enlace bidireccional conectado o no, entre los terminales y la portada 40.

De forma alternativa, los terminales están conectados con el servidor 30 de contenidos y con la portada 40 de servicio, por dos redes respectivas distintas, iguales o no.

Las diferentes listas descritas anteriormente pueden ser registradas y mantenidas de forma diferente. Por ejemplo, la lista 46 de usuarios del sistema y la lista 48 de los terminales de cada uno de ellos, están contenidas en, y mantenidas por, un subsistema de gestión de clientes distinto de la portada 40, incluso integrado en el servidor 60 de licencias.

En variante, el dato de acceso es únicamente una norma de acceso asociada con el contenido multimedia y con el terminal en cuestión.

En otra variante, la calve K_T es común a un grupo de terminales y no propia de un solo terminal. Sin embargo, incluso en este caso, el número de terminales que pertenecen a este grupo es 100 o 1000 o 10000 veces más pequeño que el número total de terminales del sistema 2.

En otro modo de realización, la etapa 112 se inicia cuando el servidor 60 de licencias detecta que un tiempo dado ha transcurrido desde la última activación de la etapa 120. Este modo de realización es el de una activación periódica de la etapa 120 de pre-computación.

En otro modo de realización, en la etapa 114, para activar la etapa 120, el servidor 60 de licencias transmite, al motor 50 de recomendación, uno al menos de los elementos de la lista de usuarios activos del sistema, por mediación de la portada 40.

En otro modo de realización, la etapa 114 es ejecutada por cualquier componente del sistema distinto del servidor 60 de licencias, por ejemplo por la portada 40.

En variante, en la etapa 114, la tendencia de los últimos valores computados de la carga de trabajo del servidor 60 de licencias es tenido en cuenta, además de su último valor computado, para decidir la inhibición o la activación de la etapa 120. Por ejemplo, en función de los recursos de computación del servidor 60 de licencias que quedan disponibles y de las estimadas necesarias para la ejecución de la etapa 120, la decisión puede ser tomada de inhibir o activar la etapa 120 para algunos usuarios solamente entre aquellos que están a priori afectados, en función de su número, o de cualquier otro dato que les afecte contenido en el sistema. Cualquier otro método de decisión a disposición del experto en la materia puede sin embargo desde luego ser aplicado.

De forma alternativa, la etapa 114 es omitida.

Los algoritmos de recomendación utilizados para construir las listas de recomendación en la etapa 102 y de la operación 122 no son necesariamente los mismos. La base de datos utilizada para ello en la operación 122 puede también ser diferente de la base de datos 56. Sin embargo, incluso en estos casos, el número de identificadores de contenidos multimedia comunes entre las listas elaboradas para el mismo usuario en la etapa 102 y la operación 122, tiene grandes posibilidades de ser elevado ya que estos dos algoritmos tienen los dos el mismo objetivo, a saber identificar los contenidos multimedia que tienen la mayor posibilidad de ser accedidos por el usuario.

En el caso en que el conjunto de datos necesarios para la computación de una licencia completa sea ya conocido antes de recibir una petición para esta licencia en la etapa 130, entonces, en la operación 126, el servidor 60 de licencias puede computar, es decir pre-computar, y luego memorizar en relación con el identificador del contenido multimedia seleccionado y con el identificador del terminal considerado del usuario, la licencia completa. En este caso, al término de la operación 146, el procedimiento continúa directamente por la etapa 150.

REIVINDICACIONES

1. Procedimiento para proporcionar, por un servidor electrónico licencias, en un sistema de suministro de contenidos multimedia, de una licencia que permita a un terminal de un usuario del sistema acceder a un contenido multimedia, siendo esta licencia función a la vez de un identificador del contenido multimedia y de un identificador del terminal o del usuario, procedimiento en el cual:

a) el servidor recibe (130) una petición que comprende el identificador del contenido multimedia y el identificador del terminal o del usuario,

b) el servidor computa (140) una licencia que comprende al menos un dato de acceso necesario para el terminal para acceder al contenido, siendo este dato de acceso función del identificador del contenido multimedia y del identificador del terminal o del usuario,

c) el servidor transmite (150), en respuesta a la petición, la licencia computada en la etapa b),

d) el terminal recibe (160) la licencia computada en la etapa c), y la utiliza para acceder al contenido multimedia,

caracterizado por que:

- antes de la etapa a) el procedimiento comprende una etapa e) (120) que comprende:
  • la obtención (122) de una primera lista de recomendación para este usuario, conteniendo esta primera lista un número limitado de identificadores de contenidos multimedia entre un conjunto más grande de contenidos multimedia disponibles en el sistema, teniendo los contenidos multimedia identificados por esta primera lista una probabilidad más grande de ser accedidos por el terminal del usuario que los otros contenidos multimedia del conjunto mayor, estando esta primera lista elaborada en función del identificador del usuario y de una base de datos preregistrados a partir de los cuales es posible computar una probabilidad de que un contenido multimedia cualquiera disponible en el sistema sea accedido por el terminal del usuario,
  • la selección (124) automática, en esta primera lista, de al menos un identificador de contenido multimedia, y
  • para cada identificador automáticamente seleccionado, la pre-computación (126) de al menos un dato de acceso utilizando este identificador de contenido multimedia y el identificador del terminal o del usuario, y
- en la etapa b), e servidor busca (141) el identificador del contenido multimedia recibido en la etapa a) entre los identificadores automáticamente seleccionados en la etapa e), luego, en caso de éxito, selecciona el dato de acceso pre-computado correspondiente a este identificador, y, en caso de fallo, genera (142) este dato de acceso.

2. El procedimiento según la reivindicación 1, en el cual la etapa a) es precedida:

- de la transmisión (104), al terminal o a otro terminal del usuario, de la primera o de una segunda lista de recomendación elaborada para este usuario y que contiene al menos uno de los identificadores automáticamente seleccionados en la etapa e),

- de visualizado, por el o el indicado otro terminal del usuario, de esta primera o segunda lista de recomendación, con el fin de favorecer la selección por el usuario de uno de los identificadores de contenidos multimedia automáticamente seleccionados en la etapa e) para su transmisión al servidor de licencia en la etapa a).

3. Procedimiento de computación, por un servidor electrónico de licencias, para la realización del procedimiento de la reivindicación 1, de una licencia que permita a un terminal de un usuario del sistema acceder a un contenido multimedia, siendo esta licencia función a la vez de un identificador del contenido multimedia y de un identificador del terminal o del usuario, procedimiento en el cual el servidor:

a) recibe (130) una petición que comprende el identificador del contenido multimedia y el identificador del terminal o del usuario,

b) computa (140) una licencia que comprende al menos un dato de acceso necesario para el terminal para acceder al contenido, siendo este dato de acceso función del identificador del contenido multimedia y del identificador del terminal o del usuario,

c) transmite (150), en respuesta a la petición, la licencia calculada en la etapa b),

caracterizado por que:

- antes de la etapa a) el procedimiento comprende una etapa e) (120) que comprende:
  • la obtención (122) de una primera lista de recomendación para este usuario, conteniendo esta primera

lista un número limitado de identificadores de contenidos multimedia entre un conjunto más grande de contenidos multimedia disponibles en el sistema, teniendo los contenidos multimedia identificados por esta primera lista una probabilidad más grande de ser accedidos por el terminal del usuario que los otros contenidos multimedia del conjunto más grande, siendo esta primera lista construida en función del identificador del usuario y de una base de datos preregistrados a partir de los cuales es posible computar una probabilidad de que un contenido multimedia cualquiera disponible en el sistema sea accedido por el terminal del usuario,

• la selección (124) automática, en esta primera lista, de al menos un identificador de contenido multimedia, y

• por cada identificador automáticamente seleccionado, la pre-computación (126) de al menos un dato de acceso utilizando este identificador de contenido multimedia y el identificador del terminal o del usuario,

- en la etapa b) el servidor (141) el identificador del contenido multimedia recibido en la etapa a) entre los identificadores automáticamente seleccionados en la etapa e), luego, en caso de éxito, selecciona el dato de acceso pre-computado correspondiente a este identificador, y, en caso de fallo, genera (142) este dato de acceso.

4. El procedimiento según la reivindicación 3, en el cual el procedimiento comprende:

- la computación (141) de la carga de trabajo del servidor en función del número de peticiones a tratar por el servidor en el transcurso de un intervalo de tiempo, y de la duración de este intervalo de tiempo, y

- la inhibición o la activación de la etapa e) en función de la carga de trabajo computada.

5. El procedimiento según una cualquiera de las reivindicaciones 3 o 4, en el cual la etapa e) (120) se activa en respuesta a la recepción:

- de una lista de identificadores de nuevos usuarios del sistema, comprendiendo esta lista el identificador del usuario,

- de una lista de identificadores de nuevos terminales del usuario,

- de una lista de identificadores de contenidos nuevamente accedidos por el usuario,

- de una lista de identificadores de usuarios dados de baja del sistema, o

- de una lista de identificadores de terminales dados de baja del sistema.

6. Soporte de registro de informaciones, caracterizado por que comprende instrucciones para la ejecución de la etapa e) de un procedimiento conforme a una cualquiera de las reivindicaciones 3 a 5, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

7. Servidor de licencias, caracterizado por que este servidor comprende un ordenador electrónico (62) programado para activar y ejecutar la etapa e) de un procedimiento de computación de una licencia conforme a una cualquiera de las reivindicaciones 3 a 5.

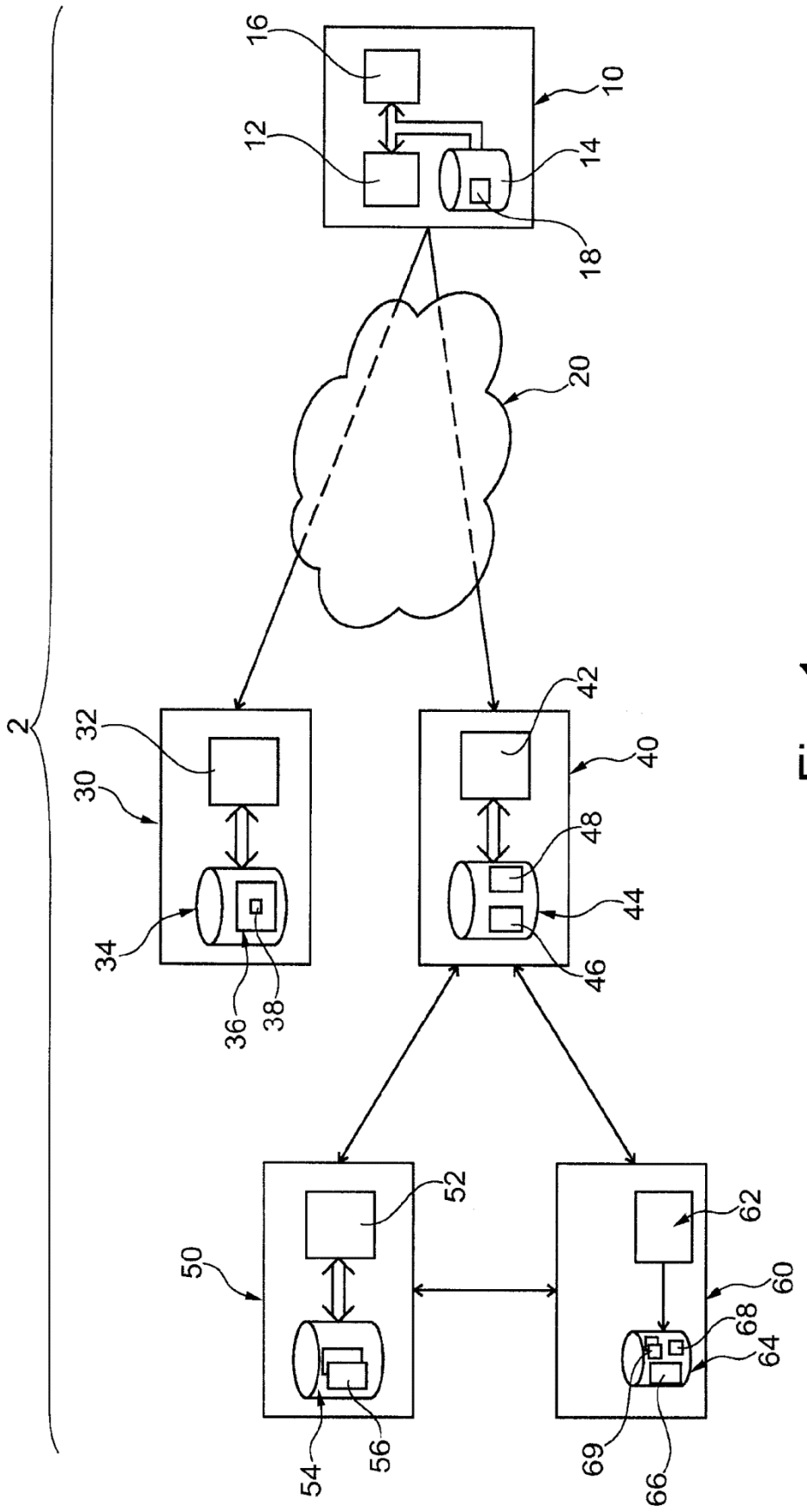
2
10
12
14
16
18
20
30
32
34
36
38
40
42
44
46
48
50
52
54
56
60
62
64
66
68
69

Fig. 1

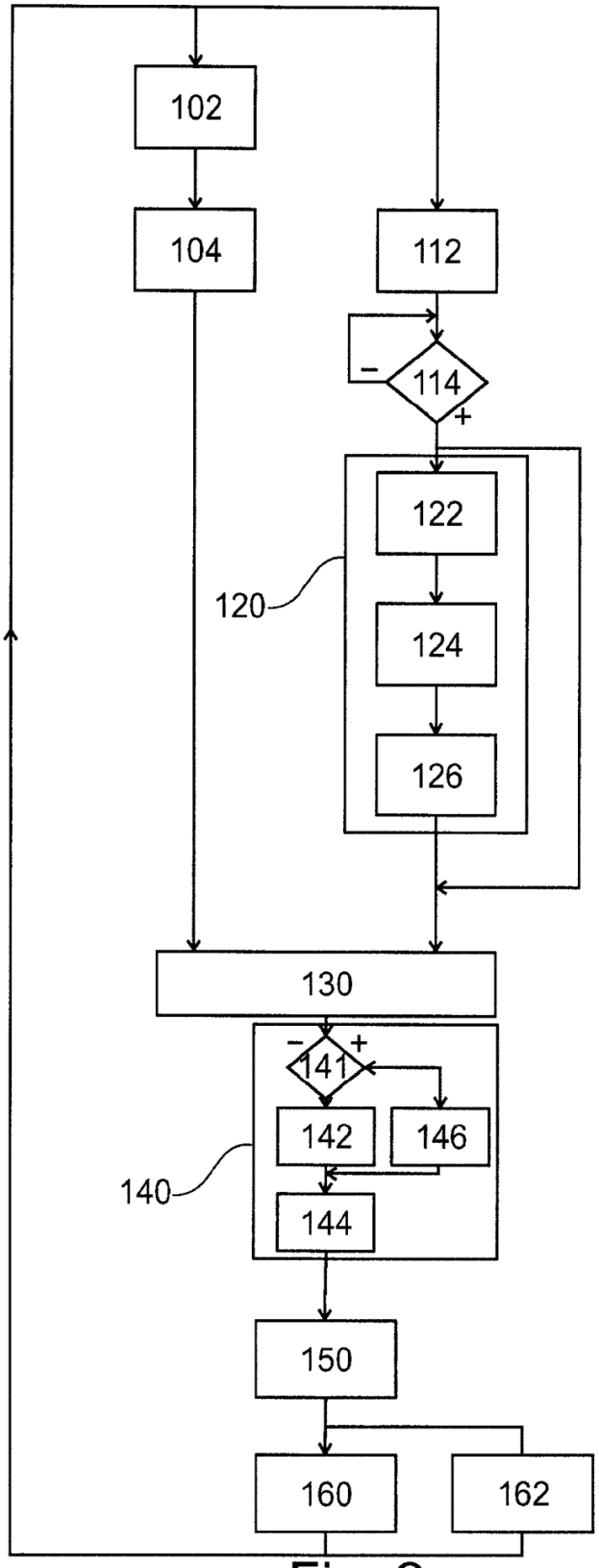
102
104
112
114
122
120
124
126
130
141
142
146
140
144
150
160
162

Fig. 2