(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 395**

(51) Int. CI.:

G06F 21/10 (2013.01)
H04N 21/00 (2011.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2010 PCT/EP2010/070318**

(87) Fecha y número de publicación internacional: **07.07.2011 WO11080150**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2010 E 10795709 (4)**

(97) Fecha y número de publicación de la concesión europea: **05.09.2018 EP 2520042**

(54) Título: **Métodos de descifrado, de transmisión y de recepción de palabras de control, soporte de registro y servidor para estos métodos**

(30) Prioridad:

28.12.2009 FR 0959612

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2019

(73) Titular/es:

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

(72) Inventor/es:

MAGIS, ERWANN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Métodos de descifrado, de transmisión y de recepción de palabras de control, soporte de registro y servidor para estos métodos

La invención se refiere a métodos de cifrado, de transmisión y de recepción de palabras de control. La invención también se refiere a un soporte de registro de informaciones y un servidor de palabras de control para la puesta en práctica estos métodos.

Existen métodos de descifrado de palabras de control para un primero y al menos un segundo terminal mecánica y electrónicamente independientes entre sí, en donde:

- los terminales primero y segundo transmiten, respectivamente, criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ a un mismo servidor de palabras de control,
- en respuesta, el servidor de palabras de control descifra los criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ para obtener, respectivamente, palabras de control $CW_{1,t}$ y $CW_{2,t}$, permitiendo las palabras de control $CW_{1,t}$ y $CW_{2,t}$ decodificar, respectivamente, primero y segundo contenido multimedia emitidos simultáneamente en, respectivamente, el primer y segundo canal, y luego
- el servidor de palabras de control transmite las palabras de control $CW_{1,t}$ y $CW_{2,t}$, respectivamente, a los terminales primero y segundo.

Por contenido multimedia se designa un contenido de audio y/o visual destinado a restituirse bajo una forma directamente perceptible y comprensible para un ser humano. Normalmente, el contenido multimedia corresponde a una sucesión de imágenes que forman una película, un programa de televisión o publicidad. Un contenido multimedia también puede ser un contenido interactivo tal como un juego.

Es conocido difundir varios contenidos multimedia al mismo tiempo. Para ello, cada contenido multimedia se emite en su propio canal. El canal utilizado para transmitir un contenido multimedia también se conoce bajo el térmico de "cadenas". Un canal corresponde normalmente a una cadena de televisión. Esto permite al usuario simplemente elegir el contenido multimedia que desea visualizar al cambiar el canal.

Para asegurar y enviar la visualización de contenido multimedia bajo ciertas condiciones, como la suscripción de un abono pagando, por ejemplo, los contenidos multimedia que se difunden bajo forma codificada y no sin codificar. Más concretamente, cada contenido multimedia se divide en una sucesión de criptoperiodos. Durante toda la duración de un criptoperiodo, las condiciones de acceso al contenido multimedia codificado permanecen sin cambios. En particular, durante toda la duración de un criptoperiodo, el contenido multimedia se codifica con la misma palabra de control. Generalmente, la palabra de control varía de un criptoperiodo a otro. Además, la palabra de control es generalmente específica para un contenido multimedia. Por lo tanto, si en un instante dado N contenido multimedia se transmiten simultáneamente en N canales, existe N palabras de control diferentes utilizadas cada una para codificar uno de estos contenidos multimedia.

En este caso, los términos "codificar" y "cifrar" se consideran como sinónimos.

El contenido multimedia sin cifrar corresponde al contenido multimedia antes de ser codificado. Esto puede ser comprendido directamente por un ser humano sin recurrir a operaciones de decodificación y sin que su visualización se someta a determinadas condiciones.

Las palabras de control necesarias para decodificar los contenidos multimedia se transmiten de forma sincrónica con los contenidos multimedia. Por ejemplo, las palabras de control necesarias para decodificar el (t+1)-ésimo criptoperiodo son recibidas por cada terminal durante el t-ésimo criptoperiodo. Para ello, por ejemplo, las palabras de control se multiplexan con el contenido multimedia codificado.

Para asegurar la transmisión de las palabras de control, estas últimas se transmiten a los terminales en forma de criptogramas. Por criptograma se designa aquí una información insuficiente por sí sola para encontrar la palabra de control sin codificar. Por lo tanto, si se intercepta la transmisión de la palabra de control, el único conocimiento del criptograma de la palabra de control no permite encontrar la palabra de control que permite decodificar el contenido multimedia. Para encontrar la palabra de control sin codificar, es decir, la palabra de control que permite decodificar directamente el contenido multimedia, este último debe combinarse con una información secreta. Por ejemplo, el criptograma de la palabra de control se obtiene al cifrar la palabra de control sin codificar con una clave criptográfica. En este caso, la información secreta y la clave criptográfica permiten descifrar este criptograma. El criptograma de la palabra de control también puede ser una referencia a una palabra de control almacenada en una tabla que contiene una multitud de palabras de control posibles. En este caso, la información secreta y la tabla asocian, a cada referencia, una palabra de control sin codificar.

La información secreta debe ser conservada en un lugar seguro. Para ello, ya se ha propuesto almacenar la información secreta:

- bien sea en procesadores de seguridad como tarjetas inteligentes conectadas directamente a cada uno de los terminales,

- bien sea, más recientemente, en un servidor de palabras de control común a varios terminales.

En este último caso, los terminales están desprovistos de tarjetas inteligentes. Esto se llama terminales sin tarjeta o "cardless terminal" en inglés.

El servidor de palabras de control está conectado a cada uno de los terminales por una red de larga distancia para la transmisión de informaciones, tal como la red de Internet. Cuando se utiliza un servidor de palabras de control, los criptogramas de las palabras de control se transmiten primero a los distintos terminales antes de reenviarse por estos terminales hacia el servidor de las palabras de control. Este procedimiento tiene varias ventajas. En particular, la red de transmisión de informaciones utilizada para transmitir los contenidos multimedia y los criptogramas de las palabras de control pueden ser diferentes de la utilizada para conectar los terminales al servidor de las palabras de control. Por ejemplo, la red para la difusión de los contenidos multimedia y de los criptogramas de las palabras de control es una red unidireccional con un gran ancho de banda, tal como una red satelital. A la inversa, la red que conecta los terminales al servidor de las palabras de control es una red bidireccional cuyo ancho de banda puede ser más reducida.

Entonces, ello simplifica la sincronización temporal entre la difusión de los contenidos multimedia y la difusión de los criptogramas de las palabras de control correspondientes.

El servidor de las palabras de control tiene por función descifrar los criptogramas de las palabras de control transmitidos por los terminales y para retornar luego hacia cada uno de estos terminales la palabra de control descifrada. Por lo tanto, en cierto modo, el servidor de las palabras de control desempeña la función de una tarjeta inteligente común a varios terminales, mecánica y eléctricamente independientes entre sí. Los terminales que son electrónicamente independientes entre sí son terminales capaces de operar de manera autónoma y que no tienen una parte electrónica común entre sí.

Cuando un terminal tiene necesidad de una palabra de control para decodificar un contenido multimedia, envía, al servidor de palabras de control, una demanda que contiene el criptograma de la palabra de control. En respuesta, el servidor de las palabras de control descifra este criptograma y luego devuelve la palabra de control descifrada al terminal que, entonces, puede decodificar el contenido multimedia deseado.

Los contenidos multimedia emitidos en los diferentes canales se coordinan temporalmente entre ellos. Por ejemplo, los instantes de transmisión de los contenidos multimedia se configuran para respetar los horarios de transmisión indicados en rejilla de programación preestablecida. Por lo tanto, cada terminal, en un canal dado, recibe sustancialmente el mismo contenido multimedia al mismo tiempo.

En estas condiciones, a menudo sucede que los usuarios cambian de canal (o cadena) al mismo tiempo. Por ejemplo, tal cambio simultáneo de canal puede ser causado por la transmisión de una secuencia de publicidad en el canal actualmente observado. Se dice que el usuario "zapea".

En respuesta a este cambio de canal, cada terminal transmite inmediatamente una demanda al servidor de las palabras de control para que reciba en respuesta la palabra de control necesaria para decodificar el contenido multimedia que se transmite actualmente en el nuevo canal observado. Por lo tanto, un cambio masivo y simultáneo de un canal a otro da lugar a una sobrecarga de trabajo para el servidor de las palabras de control.

La potencia de cálculo del servidor de las palabras de control es una función de esta sobrecarga. Por lo tanto, cuanto más se eleve la sobrecarga, es decir, cuanto mayor sea el número máximo de demandas a tratar en un intervalo de tiempo predeterminado, tanto mayor será la potencia de cálculo del servidor de las palabras de control.

Estas sobrecargas de trabajo deben reducirse tanto como sea posible para reducir la potencia de cálculo del servidor de las palabras de control y, al mismo tiempo, limitar los cambios realizados en el sistema de transmisión de contenido multimedia codificado.

El estado de la técnica también se conoce a partir de:

- MENEZS, VANSTONE, OORSCHOT: "Manual de criptografía aplicada", 1997, CRC Press LLC, EE. UU., páginas 547-555,

- el documento US2007/124807A1,

- el documento US5719941A,

- L. Francis et al: "Contramedidas para contrarrestar los ataques contra tarjetas de televisión por satélite utilizando receptores abiertos", 2005

- el documento EP1705915A.

En el contexto de un ataque de uso compartido de tarjetas, el artículo de L. Francis describe un servidor que recibe criptogramas de las palabras de control que le son transmitidas por diferentes terminales. En respuesta, este servidor reenvía a cada uno de estos terminales solamente la palabra de control descifrada correspondiente al criptograma recibido. El documento EP1705915A describe una solución para acelerar el cambio de canal en un contexto en donde son los propios terminales los que descifran los criptogramas de las palabras de control.

El objetivo de la invención es limitar las sobrecargas del servidor de las palabras de control. Por lo tanto, tiene por objeto un método de descifrado conforme la reivindicación 1.

Con el método anterior, el primer terminal tiene la palabra de control $CW_{2,t}$ necesaria para decodificar el contenido multimedia emitido simultáneamente en el segundo canal. Por lo tanto, si el usuario cambia del primer canal al segundo canal, no es necesario que el primer terminal transmita inmediatamente una demanda al servidor de las palabras de control para obtener la palabra de control $CW_{2,t}$. De este modo, las sobrecargas del servidor de las palabras de control se reducen al evitar la transmisión sistemática e inmediata de un gran número de demandas simultáneas a este servidor de las palabras de control en respuesta a un cambio de canal.

Para poner en práctica este método, el primer terminal no necesita transmitir el criptograma $CW^*_{2,t}$ al servidor de las palabras de control antes del cambio de canal. Por lo tanto, este método es fácil de poner en práctica y minimiza las modificaciones que se deben realizar en los terminales.

Además, este método también reduce el tiempo de espera antes de que se pueda decodificar el contenido multimedia transmitido en el segundo canal. De hecho, el terminal no tiene que enviar inmediatamente una demanda al servidor de las palabras de control y luego esperar a que aparezca la palabra de control $CW_{2,t}$ si ya se ha transmitido de antemano.

La invención tiene también por objeto un método de transmisión de las palabras de control conforme a la reivindicación 2.

Las formas de realización de este método de transmisión pueden incluir una o más de las características de las reivindicaciones dependientes.

La invención tiene también por objeto un método de recepción de palabras de control conforme a la reivindicación 7.

Las formas de realización de este método de recepción pueden incluir una o más de las características de las reivindicaciones dependientes.

Estas formas de realización del método de recepción además tienen las siguientes ventajas:

- retrasar la transmisión de un criptograma necesario para decodificar un próximo criptoperiodo de un contenido multimedia emitido en el mismo canal permite suavizar la carga de trabajo del servidor de las palabras de control; y

- memorizar solamente el criptograma $E_{K1}(CW_{2,t})$ en el terminal aumenta la seguridad.

La invención también se refiere a un soporte de registro de informaciones que contiene instrucciones para la puesta en práctica de uno de los métodos anteriores, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

Por último, la invención tiene también por objeto el servidor de las palabras de control según la reivindicación 12.

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

la Figura 1 es una ilustración esquemática de un sistema de difusión de contenido multimedia codificado,

la Figura 2 es una ilustración esquemática de una tabla de las palabras de control utilizada en el sistema de la Figura 1,

la Figura 3 es un organigrama de un método para transmitir contenidos multimedia codificados con la ayuda del

sistema de la Figura 1,

la Figura 4 es un organigrama de otro método de transmisión de contenidos multimedia codificados con la ayuda del sistema de la Figura 1, y

la Figura 5 es una ilustración esquemática de otra forma de realización de una tabla de palabras de control utilizada en combinación con el método de la Figura 4.

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

En la siguiente descripción, las características y funciones bien conocidas por los expertos en la técnica no se describen en detalle. Además, la terminología utilizada es la de los sistemas de acceso condicionales a contenidos multimedia. Para obtener más información sobre esta terminología, el lector puede consultar el siguiente documento:

"Modelo funcional del sistema de acceso condicional", Revisión de la EBU, Unión Europea de Radiodifusión Técnica, Bruselas, BE, Nº 266, 21 de diciembre de 1995.

La Figura 1 representa un sistema 2 para transmitir y recibir contenidos multimedia. Un contenido multimedia corresponde, por ejemplo, a una secuencia de un programa audiovisual, tal como un programa de televisión o una película.

Los contenidos multimedia sin codificar se generan por una o más fuentes 4 y se transmiten a un dispositivo 6 para su difusión simultánea hacia una multitud de dispositivos receptores a través de una red 8 de transmisión de informaciones. Los contenidos multimedia transmitidos se sincronizan temporalmente entre sí para, por ejemplo, respetar una rejilla preestablecida de programas.

La red 8 suele ser una red de larga distancia para transmitir informaciones, tal como la red Internet o una red satelital o cualquier otra red de transmisión como la que se usa para la transmisión de televisión digital terrestre (TDT).

Para simplificar la Figura 1, solamente se muestran tres dispositivos 10 a 12 de recepción.

El dispositivo 6 incluye un codificador 16 que comprime los contenidos multimedia que recibe. El codificador 16 procesa contenido multimedia digital. Por ejemplo, este codificador funciona de conformidad con la norma MPEG2 (Grupo de Expertos de Imágenes en Movimiento - Moving Picture Expert Group - 2) o ITU-T H264.

Los contenidos multimedia comprimidos se dirigen hacia una entrada 20 de un codificador 22. El codificador 22 codifica cada contenido multimedia comprimido para condicionar su visualización bajo ciertas condiciones, tales como la compra de un ticket de acceso por parte de los usuarios de los dispositivos de recepción. Los contenidos multimedia codificados se reproducen en una salida 24 conectada a la entrada de un multiplexor 26.

El codificador 22 codifica cada contenido multimedia comprimido usando una las palabras de control $CW_{i,t}$ que se le proporciona, así como a un sistema de acceso condicional 28 más conocido por el acrónimo CAS (Sistema de Acceso Condicional), mediante un generador 32 de claves. El índice i es un identificador del canal en donde se transmite el contenido multimedia codificado y el índice t es un identificador del criptoperiodo codificado con esta palabra de control.

Por lo general, esta codificación está conforme a una norma tal como la norma DVB-CSA (algoritmo de codificación común de transmisión de video digital), ISMA Cryp (Internet Streaming Media Alliance Cryp), IPsec (Internet Protocol Security, Grupo de Trabajo de Registro de Recursos de Informaciones por Desplazamiento), Protocolo de Transporte en Tiempo Real Seguro (SRTP), etc.

El sistema 28 genera mensajes de ECM (Mensaje de Control de Derechos) que contienen al menos el criptograma $CW^*_{i,t}$ de la palabra de control $CW_{i,t}$ generada por el generador 32 y utilizada por el codificador 22 para cada criptoperiodo de cada contenido multimedia. Estos mensajes y los contenidos multimedia codificados son multiplexados por el multiplexor 26, siendo estos últimos proporcionados, respectivamente, por el sistema de acceso condicional 28 y por el codificador 22, antes de ser transmitidos en la red 8.

El sistema 28 también inserta en cada ECM:

- el identificador i del canal,
- un instante t_{diff} de primera difusión del ECM por el dispositivo 6, y
- derechos de acceso destinados a compararse con los títulos de acceso adquiridos por el usuario.

El mismo identificador i se inserta en todos los mensajes de ECM que contienen un criptograma $CW^*_{i,t}$ para la

descodificación de los contenidos multimedia difundidos en un mismo canal.

A modo de ejemplo, en este caso, la codificación y multiplexación de los contenidos multimedia está de conformidad con el protocolo DVB-Simulcrypt. En este caso, el identificador i puede corresponder a un solo par "ID de canal/ID de flujo" en donde se envían todas las demandas de generación de mensajes de ECM para este canal.

Por ejemplo, los terminales 10 a 12 son idénticos y solamente el terminal 10 se describe con más detalle.

El dispositivo receptor 10 comprende un receptor 70 de contenido multimedia difundido. Este receptor 70 está conectado a la entrada de un demultiplexor 72 que transmite, por un lado, el contenido multimedia a un descodificador 74 y, por otro lado, los mensajes ECM y EMM (mensaje de gestión de derechos) a un procesador 76. El procesador 76 trata informaciones confidenciales tales como claves criptográficas. Para preservar la confidencialidad de estas informaciones, está diseñado para ser lo más resistente posible frente a la tentativa de ataques realizadas por piratas informáticos. Por lo tanto, es más resistente con respecto a estos ataques que los otros componentes del dispositivo 10. Esta resistencia, por ejemplo, se obtiene al poner en práctica un módulo de software dedicado a la protección de las informaciones secretas.

El procesador 76 se realiza, por ejemplo, utilizando ordenadores electrónicos programables capaces de ejecutar instrucciones registradas en un soporte de registro de informaciones. Para este propósito, el procesador 76 está conectado a una memoria 78 que contiene las instrucciones necesarias para la puesta en práctica del método de las Figuras 3 o 4.

La memoria 78 también contiene:

- un certificado criptográfico para autenticar el terminal 10, y
- una tabla local 79 de las palabras de control.

El decodificador 74 decodifica el contenido multimedia codificado a partir de la palabra de control transmitida por el procesador 76. El contenido multimedia a decodificar se transmite a un decodificador 80 que lo decodifica. El contenido multimedia descomprimido o decodificado se transmite a una tarjeta gráfica 82 que controla la visualización de este contenido multimedia en un visualizador 84 provisto de una pantalla 86.

El visualizador 84 muestra sin codificar el contenido multimedia en la pantalla 86.

El terminal 10 también comprende un emisor 88 que permite establecer una conexión segura con una cabecera de red 90 a través de una red 92 para transmitir informaciones. Por ejemplo, la red 92 es una red de larga distancia para transmitir informaciones y, más concretamente, una red de conmutación de paquetes, tal como la red Internet. La conexión segura es, por ejemplo, un túnel de seguridad.

La cabecera de red 90 incluye un módulo 100 de gestión de los títulos de acceso de los diferentes usuarios del sistema 2. Este módulo 100 es más conocido por el término en inglés "subscriber authorization system - sistema de autorización de abonados". Este módulo 100 genera y mantiene actualizada una base de datos 102. La base de datos 102 asocia a cada identificador de usuario los títulos de acceso adquiridos por este usuario. Esta base de datos 102 se almacena en una memoria 104.

La cabecera de red 90 también comprende un servidor 106 de palabras de control conectado a un módulo de verificación de derechos de acceso 108 y a una memoria 110 que contiene una tabla 112 de palabras de control. En condiciones normales, el servidor 106 se realiza a partir de ordenadores electrónicos programables capaces de ejecutar instrucciones registradas en un soporte de registro de informaciones. Para este propósito, la memoria 110 también comprende instrucciones para ejecutar el método de la Figura 3 o 4.

Un ejemplo de la estructura de la tabla 112 se muestra con más detalle en la Figura 2. Cada fila de la tabla 112 corresponde a un registro. La tabla 112 contiene varios registros. Cada registro corresponde a un mensaje de ECM. Cada uno de estos registros contiene los siguientes campos:

- un campo i que contiene el identificador del canal difundido,
- un campo CW_t que contiene la palabra de control $CW_{i,t}$ utilizada para codificar el criptoperiodo t del contenido multimedia emitido en el canal i,
- un campo CW_{t+1} que contiene la palabra de control $CW_{i,t+1}$ utilizada para codificar el criptoperiodo t+1 inmediatamente consecutivo del contenido multimedia difundido en el canal i,
- un campo CA que contiene las condiciones de acceso al contenido multimedia,

- un campo DV que contiene la duración de validez de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$,

- un campo MAC que contiene informaciones que permiten verificar la integridad del mensaje ECM recibido, y

- un campo t_{recept} que contiene el instante de recepción del mensaje ECM utilizado para obtener el par de las palabras de control $CW_{i,t}/CW_{i,t+1}$.

La estructura de la tabla 79 es, por ejemplo, idéntica a la estructura de la tabla 112.

El funcionamiento del sistema 2 se describirá ahora con más detalle con respecto al método de la Figura 3.

Inicialmente, durante una etapa 120, el dispositivo 6 emite varios contenidos multimedia diferentes de forma simultánea en diferentes canales. En cada canal, el criptoperiodo t y el siguiente criptoperiodo t+1 se codifican con las palabras de control, respectivamente, $CW_{i,t}$ y $CW_{i,t+1}$. Los mensajes de ECM que contienen los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ de las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ se multiplexan con contenidos multimedia difundidos. Esta multiplexación permite sincronizar la difusión de las palabras de control con la difusión de los contenidos multimedia. Normalmente, los mensajes de ECM se repiten varias veces dentro de un mismo criptoperiodo. Por ejemplo, los mensajes de ECM se repiten cada 0.1 segundos a 0.5 segundos. La duración de un criptoperiodo es mayor que diez segundos y preferiblemente mayor a 5 o 10 minutos con el fin de limitar aún más la demanda de los servidores de palabras de control.

Los contenidos multimedia codificados se reciben sustancialmente al mismo tiempo por cada uno de los terminales 10 a 12. Por lo tanto, las siguientes etapas se realizan prácticamente en paralelo para cada uno de estos terminales. También se supone que los diferentes terminales decodifican simultáneamente la transmisión de contenido multimedia en un canal respectivo. Las siguientes etapas se describen en el caso particular del terminal 10.

Durante una etapa 122, los contenidos multimedia mezclados con mensajes de ECM son recibidos por el receptor 70.

A continuación, durante una etapa 124, el demultiplexor 72 extrae el contenido multimedia codificado correspondiente al canal i cuya decodificación es solicitada actualmente por el usuario. Durante la etapa 124, el demultiplexor 72 también extrae solamente los mensajes de ECM que contienen los criptogramas de las palabras de control que permiten decodificar este mismo canal. El multiplexor 72 transmite el contenido multimedia extraído hacia el descodificador 74. Los mensajes de ECM extraídos se transmiten a su vez al procesador 76.

Durante una etapa 126, el procesador 76:

- busca si la firma MAC del mensaje ECM transmitido está ya presente en su tabla local 79, y

- verifica que las palabras de control asociadas con esta firma sean válidas utilizando la duración de validez DV.

Si las palabras de control que se encuentran en la tabla 79 son válidas, entonces el terminal pasa a una fase 127 para decodificar el contenido multimedia difundido en el canal i.

Más concretamente, durante una etapa 128, el procesador 76 envía al descodificador 74 las palabras de control $CW_{i,t}$ y $CW_{i,t+1}$ asociadas con esta firma MAC en la tabla 79. No se solicita descifrar los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ que no se transmiten inmediatamente al servidor 106.

En respuesta, el decodificador, durante una etapa 130, decodifica el contenido multimedia recibido utilizando este par de las palabras de control $CW_{i,t}/CW_{i,t+1}$.

En una etapa 132, el decodificador 80 descodifica el contenido multimedia y luego se transmite a la tarjeta de video 82.

Por último, en una etapa 134, la tarjeta de video 82 transmite la señal de video al dispositivo de visualización 84 para que el contenido multimedia se muestre en la pantalla 86 de una manera directamente perceptible y comprensible para un ser humano.

Si la firma MAC no se encuentra en la tabla 79 o si las palabras de control asociadas han caducado, entonces el procesador 76 pasa a una etapa 138 en donde verifica si el usuario cambia de canal. Por ejemplo, compara el identificador de canal i contenido en el mensaje ECM recibido con el identificador de canal contenido en el mensaje ECM recibido anteriormente.

En caso afirmativo, durante una etapa 140, el terminal 10 envía inmediatamente una demanda al servidor 106 para descifrar los criptogramas $CW^*_{i,t}$ y $CW^*_{i,t+1}$ contenidos en el mensaje ECM recibido. Esta demanda contiene el mensaje ECM recibido y, por lo tanto, el par de criptogramas $CW^*_{i,t}/CW^*_{i,t+1}$ así como un identificador del usuario del

terminal que envió la demanda. Se transmite al servidor 106 a través del emisor 88 y la red 92. Todos los intercambios de informaciones entre el terminal y el servidor 106 no se realizan a través de un túnel seguro establecido a través de la red 92 El establecimiento del túnel requiere la autentificación y la identificación del terminal por parte del servidor 106, por ejemplo, utilizando el certificado criptográfico contenido en la memoria 78.

En caso negativo, durante una etapa 142, el procesador 76 retrasa la transmisión de esta demanda. Para ello, el procesador 76 determina un tiempo de espera antes de iniciar el envío de la demanda hacia el servidor 106. Este tiempo de espera se determina para suavizar los tiempos de envío de estas demandas por diferentes terminales que han recibido al mismo tiempo este nuevo mensaje de ECM. Sin embargo, el retardo de espera se elige sistemáticamente lo suficientemente corto para permitir recibir el par de palabras de control $CW_{i,t+1}/CW_{i,t+2}$ descifradas antes del final del criptoperiodo t actual. Por ejemplo, durante la etapa 142, el procesador 76 extrae aleatoriamente o pseudoaleatoriamente un número y determina en función de este número aleatorio, el tiempo de espera que debe aplicarse. Después del tiempo de espera, la demanda se envía al servidor 106.

Esta suavización temporal de los instantes de envío de las demandas hacia el servidor 106 por los diferentes terminales que utilizan el mismo servidor de palabras de control hace posible limitar la apariencia de sobrecarga. En particular, ello evita tener una sobrecarga máxima en respuesta a cada primera transmisión de un nuevo ECM.

Durante una fase 144, el servidor 106 responde lo más rápidamente posible a la demanda enviada al final de las etapas 140 o 142.

Por ejemplo, en respuesta a la recepción de una tal demanda, durante una etapa 146, el servidor 106 selecciona registros en la tabla 112 para construir una nueva tabla local para este terminal. Para ello, el módulo 108 extrae de la base 102 los títulos de acceso correspondientes al identificador de usuario contenido en la demanda. A continuación, el servidor 106 selecciona en la tabla 112 solamente las palabras de control asociadas con los derechos de acceso DA correspondientes a los títulos de acceso extraídos. Posteriormente, esta tabla local se limita a los N pares de las palabras de control correspondientes a los N canales a los que es más probable que el usuario haga 'zapping', donde N es un número entero mayor que uno y, preferiblemente, superior a dos o diez. Para este propósito, el servidor 106 construye y utiliza los índices Pi asociados con cada canal i. Estos índices Pi son representativos de la probabilidad de que el usuario cambie al canal i. A modo de ejemplo, aquí el índice Pi es el valor de un contador C_i. Para cada canal i, un contador Ci cuenta el número de veces que una demanda para descifrar un par de palabras de control $CW_{i,t}/CW_{i,t+1}$ fue recibido por el servidor 106 durante una ventana deslizante. Normalmente, la duración S_1 de la ventana deslizante es mayor que al menos uno y preferiblemente más de un criptoperiodo. Por ejemplo, la duración S_1 está comprendida entre 30 segundos y 5 minutos. El contador C_i se incrementa en un paso cualquiera que sea el terminal que haya emitido la demanda para obtener una las palabras de control para decodificar el canal i. El valor del contador C_i es, por lo tanto, igual al número de veces durante las cuales, durante el periodo S_1, el servidor 106 recibió una demanda para descifrar una las palabras de control necesarias para la decodificación de este canal. Por lo tanto, el valor del contador C_i es tanto mayor cuanto más importante es el número de terminales que desembocan en el canal i. El valor de los contadores C_i indica, por lo tanto, cuáles son los canales más solicitados por los usuarios. En esta forma de realización, se considera que cuanto más se solicite un canal i, tanto mayor será la probabilidad de que un terminal cambie su canal actual para decodificar el canal i. Por ejemplo, el contador C_i se almacena en la memoria 110.

A continuación, en una etapa 148, el servidor 106 verifica si el ECM contenido en la demanda del terminal 10 ya se ha recibido. Por ejemplo, para ello, compara la firma MAC del ECM recibido con las firmas MAC contenidas en la tabla 112.

Si la firma MAC no está ya en la tabla 112, ello significa que el servidor 106 recibe este mensaje de ECM por primera vez. El servidor 106 pasa entonces a una fase 150 de actualización de la tabla 112. Esta fase comienza con una etapa 152 durante la cual el servidor 106 descifra el par de criptogramas $CW^*_{i,t}/CW^*_{i,t+1}$ contenidos en el ECM recibido. En la etapa 152, el servidor 106 también calcula también una duración de validez DV para las palabras de control así descifradas. Por ejemplo, esta duración de validez se calcula utilizando la siguiente fórmula:

$$DV = t_{diff} + 2 \times CP - t_{proc}$$

donde

- t_{diff} es el instante de la primera difusión del ECM por el dispositivo 6, estando este instante contenido en el ECM recibido,
- CP es la duración conocida de un criptoperiodo, y
- t_{proc} es un valor predeterminado que corresponde prácticamente al tiempo de transmisión de un mensaje ECM desde el dispositivo 6 al servidor 106 y al procesamiento de este mensaje por el servidor 106 y el terminal.

A continuación, el servidor 106 agrega un nuevo registro en la tabla 112. Este nuevo registro contiene:

- el identificador i del canal contenido en el ECM,
- el nuevo par de las palabras de control CW_t/CW_{t+1},
- los derechos de acceso DA,
- la firma MAC del ECM recibido,
- la duración de validez calculada DV, y
- el instante t_{recept} de recepción del ECM por parte del servidor 106.

La fase 150 también comprende una etapa de gestión 154 de la ventana deslizante durante la cual el servidor verifica si la diferencia entre el instante actual t_c y el instante de recepción t_{recept} de un registro en la tabla 112 no excede la duración S_1. En caso afirmativo, el registro correspondiente se borra de la tabla 112. Al mismo tiempo, el contador C_i asociado con el identificador i del registro suprimido se reduce en un paso. En el caso de que el umbral S_1 no sea franqueado, el registro no se borra y permanece contenido en la tabla 112.

La etapa 154 se repite a intervalos periódicos para eliminar los registros de la tabla 112 que se hagan obsoletos.

Si el mensaje de ECM contenido en la demanda ya está en la tabla 112 o al final de la etapa 152, el servidor 106 continúa con una etapa 160 durante la cual incrementa el contador C_i asociado con el identificador i contenido en el ECM procesado.

En una etapa 162, el servidor 106 verifica si los derechos de acceso DA contenidos en el mensaje ECM recibido corresponden a los títulos de acceso del usuario que transmitió este mensaje ECM. Si es así, y si la tabla de las palabras de control local construida en la etapa 146 no contiene ya el par $CW_{i,t}/CW_{i,t+1}$, el registro creado a partir del ECM recibido se agrega a esta tabla local.

En caso negativo, no se agrega ningún registro que contenga el par $CW_{i,t}/CW_{i,t+1}$ a la tabla local.

Por último, el servidor 106 transmite al terminal 10, en respuesta a su demanda, la tabla local construida por el servidor 106. Esta nueva tabla local recibida por el terminal sustituye entonces a la tabla 79 utilizada anteriormente por el terminal 10.

Gracias a este método, cuando un gran número de usuarios cambian de canal al mismo tiempo, la probabilidad de que la palabra de control necesaria para decodificar el nuevo canal ya esté contenida en la tabla 79 es importante, lo que limita las sobrecargas del servidor 106 consecutivas a un cambio de canal simultáneo por un gran número de usuarios.

Sin embargo, tenga en cuenta que, si la tabla local 79 contiene el par $CW_{i,t}/CW_{i,t+1}$ para el canal i y el cambio de canal se produce durante el criptoperiodo t+1, entonces el terminal envía inmediatamente una demanda al servidor 106 para obtener el par $CW_{i,t+1}/CW_{i,t+2}$. De hecho, la firma MAC del mensaje ECM que contiene el par $CW_{i,t+1}/CW_{i,t+2}$ no es la misma que la del mensaje ECM que contiene el par $CW_{i,t}/CW_{i,t+1}$. Puede ser deseable tener un método similar al de la Figura 3, pero que permita al terminal utilizar la palabra de control $CW_{i,t+1}$ contenida en la tabla local 79 para comenzar a decodificar inmediatamente el contenido multimedia emitido en el canal i sin tener que enviar inmediatamente una demanda al servidor 106.

El método de la Figura 4 permite, además, satisfacer este deseo. Para ello, se inserta un número de orden N_{ECMi} en cada mensaje $ECM_{i,t}$ para identificar el mensaje $ECM_{i,t}$ que precede al mensaje $ECM_{i,t+1}$. El dispositivo 6 inserta el número N_{ECMi} en cada mensaje ECM.

Para la puesta en práctica del método de la Figura 4, la estructura de las tablas 79 y 112 se modifica para corresponder a la de la tabla 200 (Figura 5). La tabla 200 es idéntica a la tabla 112, excepto que comprende para cada registro un campo N_{ECMi} adicional correspondiente al número de orden del mensaje de ECM asociado con un canal i particular.

Además, en el método de la Figura 4, la selección de las palabras de control se modifica para tener en cuenta únicamente el comportamiento pasado del usuario que envió la demanda al servidor 106. Para este fin, cada contador C_i se sustituye por los contadores C_{ij}, donde el índice i es un identificador del canal y el índice j es un identificador del usuario del terminal. Cada contador C_{ij} cuenta el número de veces que el usuario i ha enviado una demanda para decodificar el canal i durante la ventana deslizante de duración S_1. Por lo tanto, este contador C_{ij} no se modifica por las informaciones contenidas en demandas procedentes de otros terminales que el utilizado por el usuario j. El valor de cada uno de estos contadores C_{ij} es, por lo tanto, un índice P_{ij} representativo de la probabilidad de que el usuario j cambie de canal para pasar al canal i. La selección de las palabras de control incorporadas en la

tabla local construida por el servidor 106 para este usuario j se realiza en función del índice P_{ij}. Ello permite adaptar la construcción de la tabla local para el usuario j en función de su comportamiento pasado.

El método de la Figura 4 es idéntico al método de la Figura 3, excepto que la etapa 126 y las fases 127 y 144 se sustituyen, respectivamente, por la etapa 178 y las fases 179 y 192.

En la etapa 178, el procesador 76 verifica si una palabra de control válida requerida para decodificar el contenido multimedia difundido ya está presente en la tabla 79. Para este propósito, la duración de validez DV asociada con el identificador i en la tabla 79 se compara con el instante actual t_c. Además, el procesador 76 también verifica que el número de orden N_{ECMi} contenido en el mensaje ECM recibido sea igual al número de orden N_{ECMi} asociado con el identificador i en la tabla 79 o el número de orden anterior.

En caso afirmativo, el procesador 76 pasa a la fase 179 de decodificación del contenido multimedia difundido en el canal i. Esta fase 179 es idéntica a la fase 127, excepto que la etapa 128 se sustituye por una etapa 182. Esta etapa 182 es idéntica a la etapa 128, pero además de las operaciones descritas anteriormente, el procesador 76 envía al decodificador 74 el par de palabras de control $CW_{i,t-1}/CW_{i,t}$ si el número de orden N_{ECMi} contenido en la tabla 79 es igual al número de orden recibido N_{ECMi-1}.

Por lo tanto, incluso en respuesta al cambio de canal durante el criptoperiodo t+1, la recepción de un mensaje ECM que contiene los criptogramas $CW^*_{i,t}/CW^*_{i,t+1}$ no activa el envío inmediato de una nueva demanda hacia el servidor 106. Por el contrario, esta demanda se retrasa para facilitar la transmisión de estas demandas al servidor 106 para evitar sobrecargas.

La fase 192 es idéntica a la fase 144, con la excepción de que las etapas 146, 160 y 162 se sustituyen por las etapas 194, 196 y 198.

La etapa 194 es idéntica a la etapa 146, excepto que solamente son dos los índices P_{ij} asociados con el usuario j, que se utilizan para seleccionar los registros que se incluirán en la tabla local construida por el servidor 106.

La etapa 196 es idéntica a la etapa 160, excepto que solo el contador C_{ij} específico del usuario j y el canal i se incrementa cada vez que el servidor 106 recibe una nueva demanda para decodificar este canal.

La fase 150 también se sustituye por una fase 197 idéntica a la fase 150, con la excepción de que la etapa 154 se sustituye por otra etapa 198 de gestión de la ventana deslizante. En la etapa 198, todos los contadores C_{ij} asociados con el canal i del registro suprimido se decrementan al mismo tiempo. Por consiguiente, la duración S_1 puede ser mucho mayor que en el caso del método de la Figura 3. Por ejemplo, la duración S_1 está incluida entre una y cuatro semanas.

El método de la Figura 4 tiene varias ventajas. En particular, permite decodificar un nuevo canal sin transmitir inmediatamente una nueva demanda al servidor 106 a partir del momento en que una de las dos palabras de control de un par de palabras de control se puede utilizar válidamente para decodificar este canal.

A continuación, el uso de los índices P_{ij} permite aumentar la probabilidad de que, durante un cambio de canal, la palabra de control necesaria ya esté contenida en la tabla 79. Por lo tanto, esto limita aún más las sobrecargas.

Numerosas otras formas de realizaciones son posibles. En particular, existen muchas otras posibilidades para seleccionar los registros de la tabla 112 utilizada para construir la tabla 79. En una primera variante, la tabla local de las palabras de control se construye combinando los registros dados con referencia a las Figuras 3 y 4. Por ejemplo, la tabla local es construida por el servidor 106 seleccionando registros en función, a la vez, de los índices P_i y P_{ij}.

En otra variante, al menos algunos de los registros que se seleccionan son identificados manualmente por el usuario del terminal 10. Por ejemplo, durante una fase de inicialización, el usuario del terminal 10 interactúa con este último para adquirir una lista de identificadores de canal entre los que el usuario desea poder navegar rápidamente. Esta lista se transmite al servidor 106 que la registra. Posteriormente, cada vez que este terminal transmite un mensaje ECM, los registros correspondientes a los canales a los que se hace referencia en la lista se incorporan sistemáticamente en la tabla local de las palabras de control creada por el servidor 106.

Se pueden usar otros índices de probabilidad distintos de los descritos anteriormente para seleccionar los registros que se incorporarán a la tabla local. Por ejemplo, el índice también puede ser una función del canal de inicio decodificado antes del cambio de canal.

En una forma de realización muy simplificada, el conjunto de las palabras de control contenidas en la tabla 112 y correspondientes a los títulos de acceso del usuario se envían al terminal en respuesta a cada demanda de este terminal. Por lo tanto, los diversos contadores o índices que permiten seleccionar un número limitado de registros entre el conjunto de los registros contenidos en la tabla 112 se omiten.

El identificador de canal incorporado en el mensaje ECM puede ser generado por el propio terminal e incorporado solamente en la demanda transmitida al servidor de las palabras de control. En este caso, no es necesario que este identificador de canal se incorpore en los mensajes ECM construidos por el sistema 28.

La actualización de la tabla 79 no se activa necesariamente por la recepción de un nuevo mensaje de ECM para el canal solicitado actualmente. Por ejemplo, en otra forma de realización, el terminal envía automáticamente una demanda para actualizar la tabla 79 al servidor 106 tan pronto como la duración de validez de las palabras de control contenidas en esta tabla para uno o más canales caduque incluso si estos canales no están actualmente decodificados. El envío de una demanda de actualización de la tabla 79 también se puede activar tan pronto como el número de las palabras de control para las cuales la duración de validez haya expirado exceda un umbral predeterminado. Preferiblemente, este umbral se expresa como un porcentaje del número total de las palabras de control contenidas en la tabla 79. Preferiblemente, estas demandas de actualización de la tabla 79 se suavizan en el tiempo para no causar sobrecargas en el servidor 106.

Como variante, los descifrados de cada criptograma $CW^*_{i,t}$ contenidos en un mensaje ECM transmitido al servidor 106 solo se realizan si los derechos de acceso contenidos en este mismo mensaje ECM corresponden a los títulos de acceso del usuario que ha enviado este mensaje ECM.

Se pueden utilizar otros métodos para suavizar el tiempo de envío de demandas al servidor 106. Estos otros métodos no necesariamente tienen que recurrir a la extracción de un número aleatorio.

En otra variante, la actualización de la tabla 79 se limita a los únicos registros cuya duración de validez haya caducado o esté a punto de hacerlo. Para ello, cada demanda transmitida por un terminal al servidor 106 también contiene una imagen de las palabras de control actualmente contenidas en la tabla 79. Por ejemplo, esta imagen está constituida por el identificador de canal i asociado con el número de orden N_{ECMi} en la tabla 79. En estas condiciones, el servidor 106 identifica el único registro para el que es necesaria una actualización y solamente transmite estos registros en la etapa 162. Ello permite limitar el ancho de banda necesario para el envío de las tablas locales por el servidor 106.

Son posibles otras soluciones además del uso de un túnel seguro para proteger la transmisión de las palabras de control entre un terminal y el servidor 106. Por ejemplo, cada par de las palabras de control está cifrado por el servidor 106 con una clave privada K1 conocida solamente por el terminal hacia el que debe transmitirse este par de palabras de control. La tabla de las palabras de control transmitida al terminal contiene entonces solamente los criptogramas $E_{K1}(CW_{i,t})$ así obtenidos. Las otras informaciones de la tabla local pueden estar no cifradas. En consecuencia, los pares de las palabras de control registrados en el terminal están solamente en forma cifrada. El descifrado de estos pares de palabras de control se produce solamente cuando se controla el decodificado del canal correspondiente. Esta circunstancia aumenta la seguridad.

Existen otras soluciones para asegurar la transmisión de las palabras de control desde el servidor 106 hacia los terminales. Por ejemplo, el dispositivo 6 primero cifra las palabras de control sin codificar con una clave K1 y luego una segunda vez con una clave K2. Los mensajes de ECM contienen entonces el criptograma $E_{K2K1}(CW_{i,t})$ en lugar del criptograma $CW^*_{i,t}$. En respuesta a una demanda de un terminal, el servidor 106 primero descifra el criptograma $E_{K2K1}(CW_{i,t})$ con la clave K2 para obtener la palabra de control $E_{K1}(CW_{i,t})$. Esta las palabras de control $E_{K1}(CW_{i,t})$ se transmiten en respuesta al terminal. La palabra de control $E_{K1}(CW_{i,t})$ permite decodificar el contenido multimedia después de haber sido descifrado por segunda vez por el terminal con la clave K1.

La suavización de las sobrecargas es tanto más efectiva como larga sea la duración de los criptoperiodos. Sin embargo, en lugar de extender la duración de un criptoperiodo, también es posible reutilizar la misma palabra de control en varios criptoperiodos sucesivos. De hecho, ello permite repartir las demandas dirigidas al servidor de las palabras de control durante un período más prolongado. Sin embargo, este método tiene la ventaja de permitir una comparación de los derechos de acceso al título de acceso del usuario durante cada criptoperiodo.

Se puede utilizar un identificador del terminal en lugar del identificador de usuario.

Las características de los métodos de las Figuras 3 y 4 se pueden combinar.

REIVINDICACIONES

1. Método de descifrado de palabras de control para un primer y al menos un segundo terminal mecánica y electrónicamente independientes entre sí, en donde:

- los terminales primero y segundo transmiten (140, 142), respectivamente, criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$, a un mismo servidor de palabras de control,

- en respuesta, el servidor de palabras de control descifra (152) los criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ para obtener, respectivamente, palabras de control $CW_{1,t}$ y $CW_{2,t}$, permitiendo las palabras de control $CW_{1,t}$ y $CW_{2,t}$ decodificar, respectivamente, primero y segundo contenido multimedia emitidos simultáneamente en, respectivamente, el primer y segundo canal, luego

- el servidor de palabras de control transmite (162) las palabras de control $CW_{1,t}$ y $CW_{2,t}$, respectivamente, a los terminales primero y segundo,

caracterizado por cuanto que

- el servidor de palabras de control también transmite (162) al primer terminal la palabra de control $CW_{2,t}$ obtenida al descifrar el criptograma $CW^*_{2,t}$ transmitida por el segundo terminal incluso antes de que el primer terminal cambie de canal decodificado pasando del primero hacia segundo canal, y

- en respuesta al cambio de canal, el primer terminal busca (126; 178) primero si la palabra de control $CW_{2,t}$ ya ha sido transmitida por adelantado por el servidor de palabras de control incluso antes del cambio de canal y, en caso afirmativo, el primer terminal comienza inmediatamente a decodificar (130) el contenido multimedia emitido en este segundo canal con la palabra de control CW2,t transmitida de antemano.

2. Método de transmisión de palabras de control $CW_{1,t}$ y $CW_{2,t}$ al primer y segundo terminales de forma mecánica y electrónica independientemente entre sí para poner en práctica un método conforme con la reivindicación 1, en donde:

- en respuesta a la transmisión de criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ por, respectivamente, los primero y segundo terminal, el mismo servidor de palabras de control descifra (152) los criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ para obtener, respectivamente, palabras de control $CW_{1,t}$ y $CW_{2,t}$, permitiendo las palabras de control $CW_{1,t}$ y $CW_{2,t}$ decodificar, respectivamente, el primer y el segundo contenido multimedia emitidos simultáneamente, en, respectivamente, primero y segundo canales; y luego

- el servidor de palabras de control transmite (162) las palabras de control $CW_{1,t}$ y $CW_{2,t}$, respectivamente, a los terminales primero y segundo,

caracterizado por cuanto que el servidor de palabras de control también transmite (162) al primer terminal la palabra de control $CW_{2,t}$ obtenida al descifrar el criptograma $CW^*_{2,t}$ transmitido por el segundo terminal incluso antes de que el primer terminal cambie de canal decodificado pasando del primero al segundo canal.

3. Método según la reivindicación 2, en donde:

- en respuesta a la transmisión de un criptograma $CW^*_{3,t}$ al mismo servidor de palabras de control por un tercer terminal mecánica y electrónicamente independiente de los primer y segundo terminales, el servidor de palabras de control descifra (152) el criptograma $CW^*_{3,t}$ para obtener una palabra de control $CW_{3,t}$ que permite decodificar un tercer contenido multimedia difundido en un tercer canal simultáneamente con el primer y segundo contenido multimedia, luego

- el servidor de palabras de control selecciona (146; 194) la palabra de control $CW_{2,t}$ en una tabla que contiene al menos las palabras de control $CW_{2,t}$ y $CW_{3,t}$ y no selecciona la palabra de control $CW_{3,t}$, luego transmite (162) solamente las palabras de control seleccionadas en esta tabla al primer terminal.

4. Método según la reivindicación 3, en donde el servidor de palabras de control:

- construye (146; 194), para cada canal asociado con palabras de control contenidas en la tabla, un índice representativo de la probabilidad de que este canal sea próximamente decodificado por el primer terminal, y

- selecciona (146; 194), en la tabla la palabra o palabras de control que se transmitirán al primer terminal en función de este índice.

5. Método según la reivindicación 4, en donde el índice del segundo canal se construye (146) a partir de un recuento del número de transmisiones del criptograma $CW^*_{2,t}$ por otros terminales mecánica y electrónicamente

independientes del segundo terminal.

6. Método de conformidad con una cualquiera de las reivindicaciones precedentes, en donde el servidor de palabras de control transmite (162) cada palabra de control asociada con un identificador del criptoperiodo o criptoperiodos que esta palabra de control permite decodificar.

7. Método de recepción de palabras de control $CW_{1,t}$ y $CW_{2,t}$ por un primer terminal para la puesta en práctica de un método conforme a la reivindicación 1, en donde:

- el primer terminal transmite (140; 142) a un servidor de palabras de control un criptograma $CW^*_{1,t}$ y recibe (162), en respuesta, una palabra de control $CW_{1,t}$ descifrada por este servidor de palabras de control, permitiendo esta palabra de control $CW_{1,t}$ decodificar un contenido multimedia difundido en un primer canal recibido por el primer terminal,

- el primer terminal también recibe (162) una palabra de control CW2,t que permite decodificar otro contenido multimedia emitido simultáneamente en un segundo canal, pudiendo obtenerse esta palabra de control $CW_{2,t}$ solamente mediante el descifrado de un criptograma $CW^*_{2,t}$ por el servidor de palabras de control,

- el primer terminal cambia el canal decodificado pasando del primero hacia el segundo canal,

caracterizado por cuanto que:

- el primer terminal recibe (162) la palabra de control $CW_{2,t}$ incluso antes de que el primer terminal cambie de canal sin haber transmitido nunca el criptograma $CW^*_{2,t}$ previamente al servidor de palabras de control, y

- en respuesta al cambio de canal, el primer terminal busca (126; 178) primero si la palabra de control CW2,t ya ha sido transmitida por adelantado por el servidor de palabras de control incluso antes del cambio de canal y, en caso afirmativo, el primer terminal comienza inmediatamente a decodificar (130) el contenido multimedia emitido en este segundo canal con la palabra de control CW2,t transmitida de antemano.

8. Método según la reivindicación 7, en donde el primer terminal decodifica (130) un t-ésimo criptoperiodo del contenido multimedia emitido en el primer canal con la palabra de control $CW_{1,t}$ y retrasa (142) la transmisión de un criptograma $CW^*_{1,t+1}$, para decodificar un (t+1)-ésimo criptoperiodo del contenido multimedia difundido en este mismo canal con un retraso determinado para escalonar, al menos en toda la duración del t-ésimo criptoperiodo, los instantes de transmisiones de los criptogramas $CW^*_{1,t+1}$ procedentes de diferentes terminales mecánica y eléctricamente independientes entre sí.

9. Método según la reivindicación 7 u 8, en donde si la palabra de control $CW_{2,t}$ no se ha transmitido antes de que el primer terminal cambie los canales, el primer terminal transmite (140) inmediatamente el criptograma $CW^*_{2,t}$ al servidor de palabras de control luego espera haber recibido la palabra de control $CW_{2,t}$ transmitida por el servidor de palabras de control antes de comenzar a decodificar la transmisión de contenido multimedia en el segundo canal.

10. Método según una cualquiera de las reivindicaciones 7 a 9, en donde el primer terminal memoriza solamente la palabra de control $CW_{2,t}$ en forma de un criptograma $E_{K1}(CW_{2,t})$ obtenido al cifrar la palabra de control $CW_{2,t}$ con una clave secreta K1, siendo la clave K1 solamente conocida por el primer terminal y desconocida de los otros terminales.

11. Un soporte de registro de informaciones, caracterizado por cuanto que incluye instrucciones para la puesta en práctica de uno cualquiera de los métodos anteriores, cuando estas instrucciones son ejecutadas por un ordenador electrónico.

12. Un servidor (106) de palabras de control para la transmisión de palabras de control $CW_{1,t}$ y $CW_{2,t}$ a los terminales primero y segundo, mecánica y eléctricamente independientes entre sí, para la puesta en práctica de un método conforme con la reivindicación 1, siendo este servidor capaz de:

- en respuesta a la transmisión de los criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ por, respectivamente, los primero y segundo terminal, para descifrar los criptogramas $CW^*_{1,t}$ y $CW^*_{2,t}$ para obtener, respectivamente, palabras de control $CW_{1,t}$ y $CW_{2,t}$, permitiendo las palabras de control $CW_{1,t}$ y $CW_{2,t}$ decodificar, respectivamente, el primer y el segundo contenido multimedia emitidos simultáneamente en, respectivamente, el primer y segundo canal,

- de transmitir las palabras de control $CW_{1,t}$ y $CW_{2,t}$, respectivamente, a los terminales primero y segundo,

caracterizado porque el servidor de palabras de control también está adaptado para transmitir al primer terminal la palabra de control $CW_{2,t}$ obtenida al descifrar el criptograma $CW^*_{2,t}$ transmitido por el segundo terminal incluso antes de que el primer terminal cambie de canal decodificado pasando del primero hacia el segundo canal.

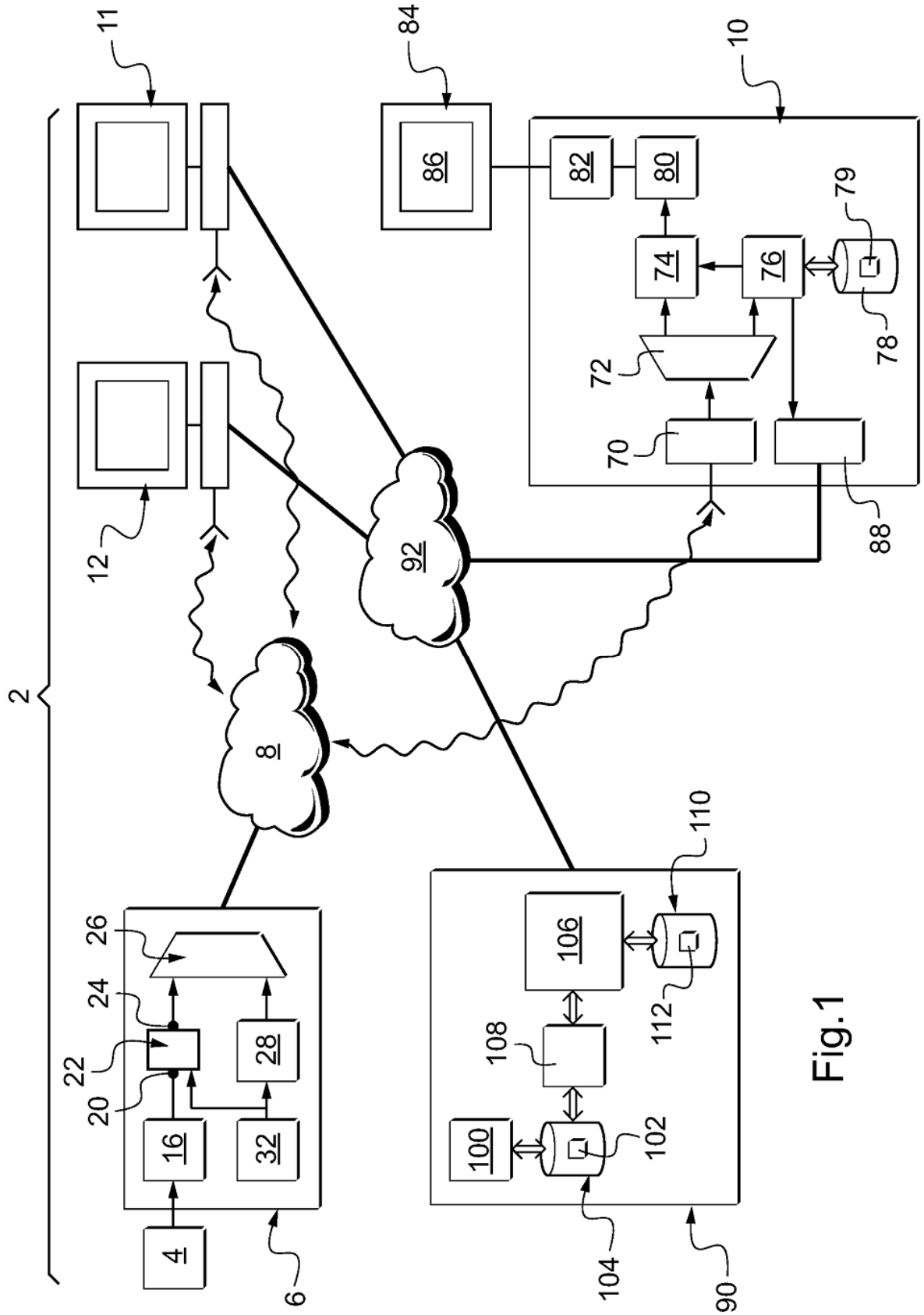
2
11
12
84
86
10
82
80
79
74
76
78
72
70
88
92
8
110
106
108
112
100
102
104
90
26
24
22
20
28
16
32
4
6

Fig.1

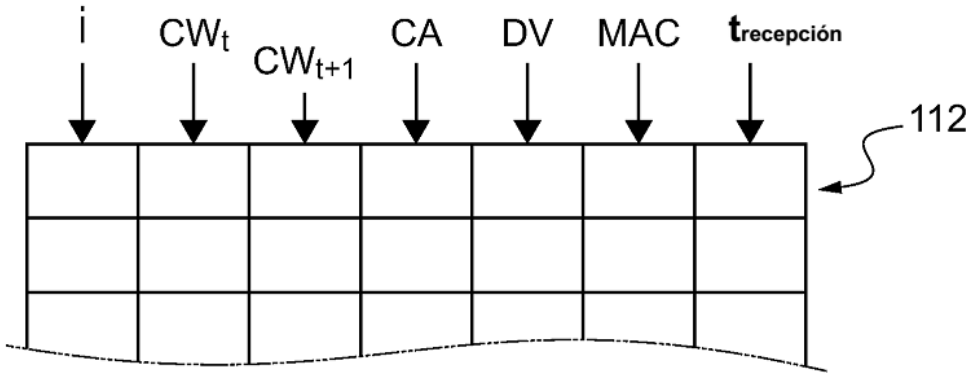
i
CWt
CWt+1
CA
DV
MAC
trecepción
112

Fig.2

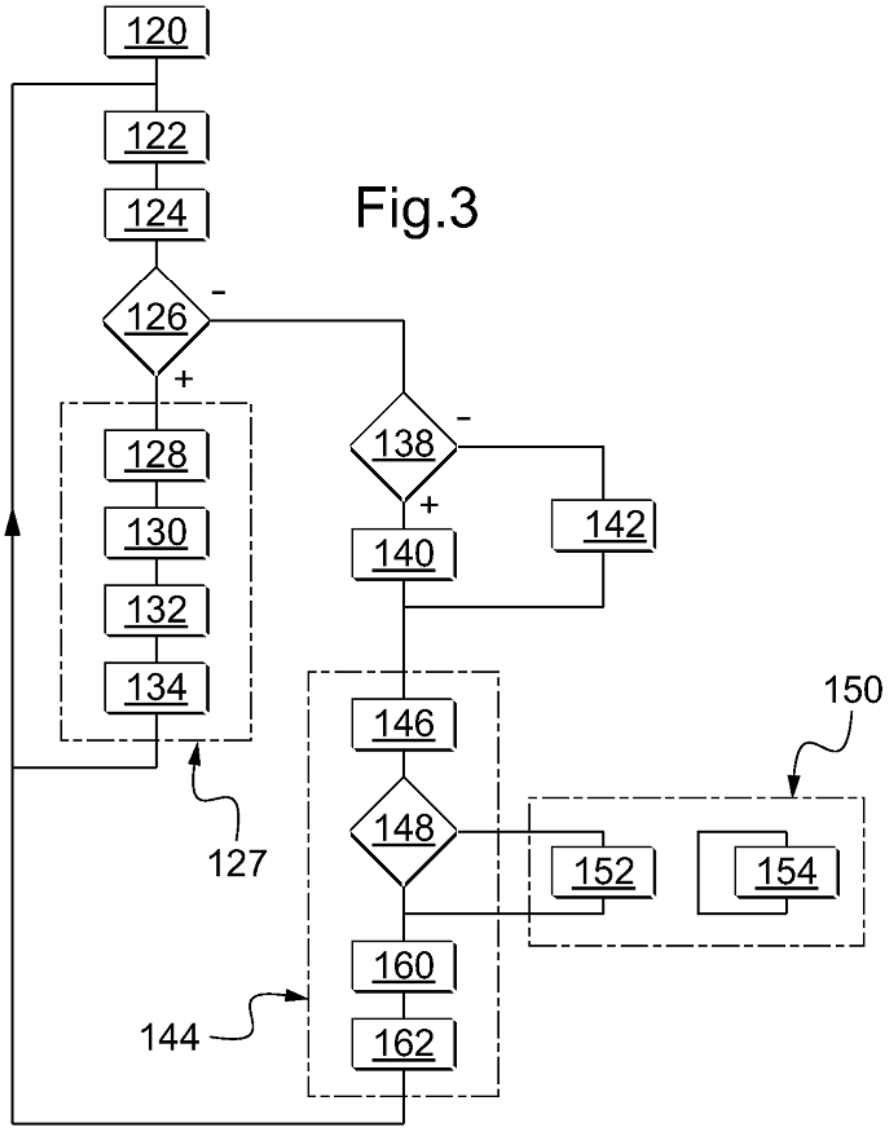
120
122
124
126
-
+
128
130
132
134
127
138
-
+
140
142
146
148
150
152
154
160
162
144

Fig.3

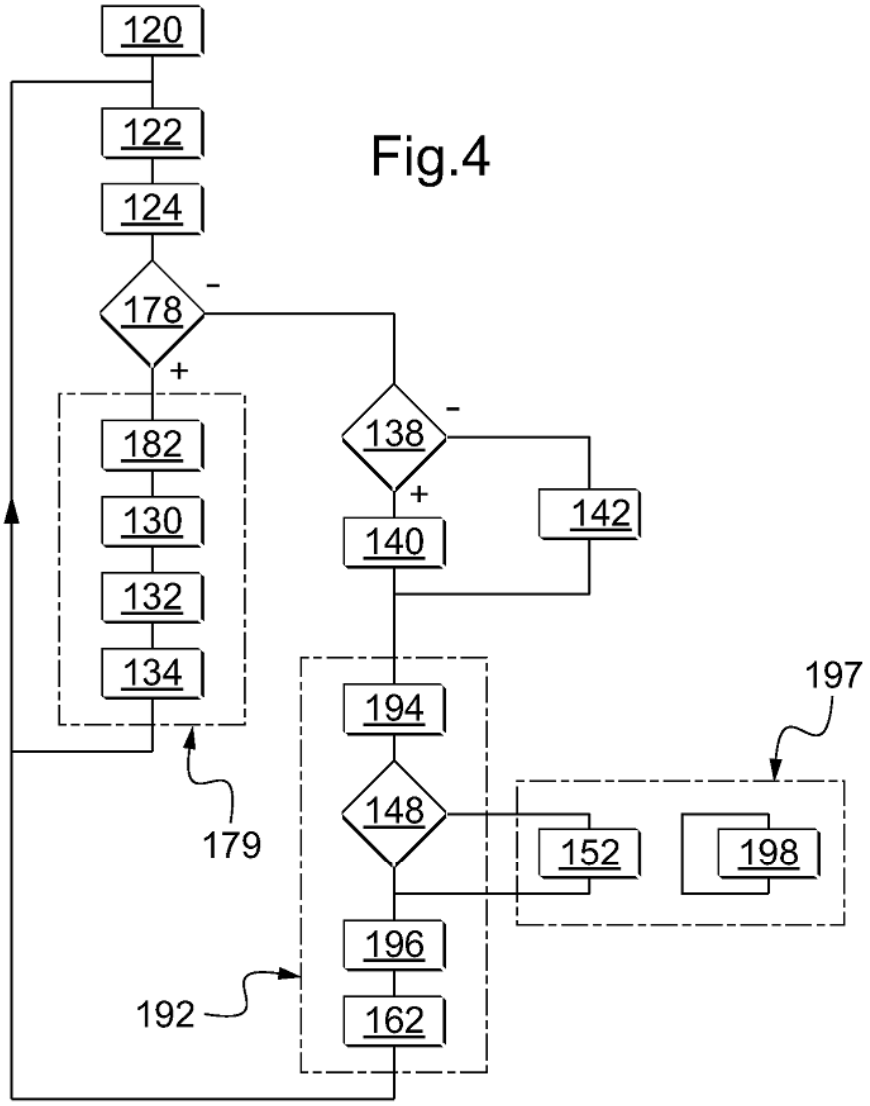
120
122
124
178
-
+
182
130
132
134
179
138
-
+
140
142
194
148
152
198
197
196
162
192

Fig.4

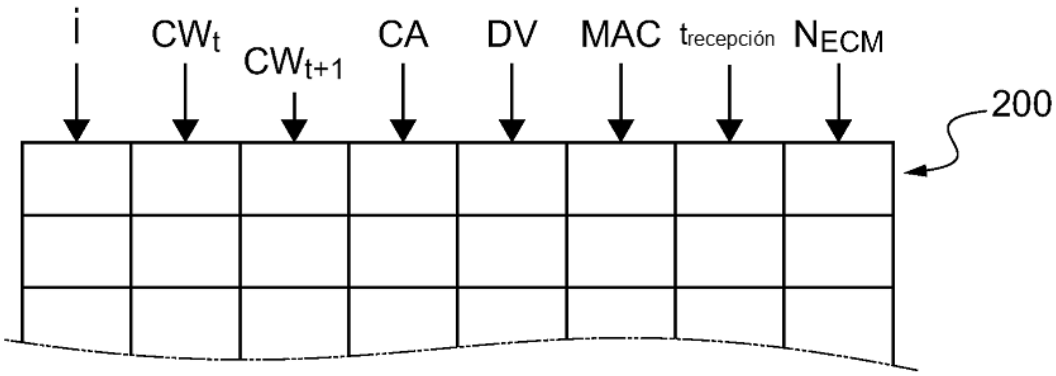
i
CWt
CWt+1
CA
DV
MAC
trecepción
NECM
200

Fig.5