

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 375 343**

51 Int. Cl.:
H04N 21/4623 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **09745663 .6**
96 Fecha de presentación: **04.05.2009**
97 Número de publicación de la solicitud: **2279610**
97 Fecha de publicación de la solicitud: **02.02.2011**

54 Título: **PROCEDIMIENTOS DE RECEPCIÓN Y DE EMISIÓN DE UN CONTENIDO MULTIMEDIA, RECEPTOR, EMISOR Y SOPORTE DE GRABACIÓN Y PROCESADOR DE SEGURIDAD PARA ESTE PROCEDIMIENTO.**

30 Prioridad:
16.05.2008 FR 0802639

45 Fecha de publicación de la mención BOPI:
29.02.2012

45 Fecha de la publicación del folleto de la patente:
29.02.2012

73 Titular/es:
**VIACCESS
LES COLLINES DE L'ARCHE TOUR OPÉRA C
92057 PARIS LA DÉFENSE , FR**

72 Inventor/es:
DUBROEUCQ, Gilles

74 Agente: **Linage González, Rafael**

ES 2 375 343 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimientos de recepción y de emisión de un contenido multimedia, receptor, emisor y soporte de grabación y procesador de seguridad para este procedimiento.

- 5 La invención concierne a un procedimiento de recepción y a un procedimiento de emisión de un primer contenido multimedia cuya visualización está condicionada a la visualización previa de segundos contenidos multimedia. La invención tiene asimismo por objeto un receptor, un emisor, un soporte de grabación de información y un procesador de seguridad para la puesta en práctica de estos procedimientos.
- 10 Un contenido multimedia es un contenido que contiene audio y/o vídeo. Este contenido multimedia está destinado, por ejemplo, a ser reproducido en un televisor. Por ejemplo, un contenido multimedia es una película, un programa audiovisual o una música.

Es conocido un procedimiento de recepción de este tipo por la solicitud de patente US2007294773 a nombre de
15 Microsoft®. Más precisamente, la solicitud de Microsoft describe un procedimiento de recepción de un primer contenido multimedia, es decir, en el presente caso, de un vídeo bajo demanda, y el condicionamiento de la desaleatorización de este vídeo bajo demanda a la visualización previa de un segundo contenido multimedia, es decir, en el presente caso, de espacios publicitarios. El vídeo bajo demanda es más conocido con el acrónimo de VOD (Video On Demand).

20 En el procedimiento de Microsoft, un receptor entrega una licencia que permite el descifrado del vídeo bajo demanda únicamente si se ha visualizado primero el conjunto de los espacios publicitarios. A través de esto, la visualización del vídeo bajo demanda está condicionada a la visualización previa de los espacios publicitarios. Además, este receptor está equipado con diferentes medios que permiten impedir que el usuario eluda o se salte los espacios publicitarios. Por ejemplo, el receptor está equipado con medios que permiten anular el avance rápido.

25 Este procedimiento conocido permite, por tanto, obligar a los televidentes a visualizar el conjunto de los espacios publicitarios que preceden inmediatamente al vídeo bajo demanda.

No obstante, el ámbito de aplicación de este procedimiento conocido está limitado al vídeo bajo demanda. En efecto,
30 si se adaptara este procedimiento para la televisión difundida, entonces un espectador que, por inadvertencia, se perdiera el inicio de los espacios publicitarios que preceden inmediatamente a la emisión que desea ver, estaría privado de la posibilidad de visualizar esa emisión. Tal funcionamiento es inaceptable para un sistema de televisión difundida.

35 Se designa en el presente caso por televisión difundida la difusión simultánea de un mismo contenido multimedia a múltiples receptores. Contrariamente al vídeo bajo demanda, en la televisión difundida, el usuario no puede decidir la hora de inicio de difusión del contenido multimedia.

Por el estado de la técnica se da a conocer asimismo en los documentos US2006/294547 y EP1111924A.

40 La invención tiene pues por objeto proponer un procedimiento de recepción conforme a la reivindicación 1.

Asumimos en el presente caso que el anterior procedimiento se pone en práctica en el ámbito de la televisión difundida para una emisión de televisión que se desea condicionar previamente a la visualización de espacios
45 publicitarios. También asumimos que las instrucciones de progresión incrementan el valor del contador cuando son ejecutadas por el receptor. En este contexto, aun si el usuario se pierde el inicio de los espacios publicitarios que preceden inmediatamente a esa emisión de televisión, a pesar de todo se le puede autorizar a verla. En efecto, en el anterior procedimiento, cada vez que el usuario ve espacios publicitarios, el valor del contador se incrementa. No es necesario que los espacios publicitarios vistos precedan inmediatamente a la emisión de televisión, puesto que el
50 valor del contador se memoriza. Por ejemplo, el usuario puede ver una primera secuencia de espacios publicitarios y luego cambiar de canal para ver una película. La visualización de esa película no modifica el valor del contador. Seguidamente, un tiempo más tarde, el usuario ve otra secuencia de espacios publicitarios, lo cual sigue incrementando el valor del contador. El contador se incrementa por tanto sin ser reinicializado, incluso si la visualización de los espacios publicitarios es entrecortada por la visualización de otros contenidos multimedia. En
55 consecuencia, incluso antes de que aquel empiece a ver la secuencia de espacios publicitarios que precede inmediatamente a la emisión de televisión que desea ver, el valor del contador puede haber alcanzado ya un valor suficiente para autorizar la visualización de esa emisión de televisión. En tales condiciones, aun si se pierde la secuencia de espacios publicitarios que precede inmediatamente a la emisión de televisión, se le autoriza a pesar de todo a verla.

En el anterior procedimiento, no es necesario que el segundo contenido multimedia preceda inmediatamente al primer contenido multimedia. Ello hace posible la utilización de este procedimiento en el ámbito de la televisión difundida.

5

Las formas de realización de este procedimiento de recepción pueden incorporar una o varias de las características de las reivindicaciones dependientes:

Las formas de realización del anterior procedimiento de recepción presentan además las siguientes ventajas:

10

- la multiplexación de los segundos contenidos multimedia y de las instrucciones de progresión permite asociar simplemente esas instrucciones de progresión con los segundos contenidos multimedia,

15

- la utilización de un identificador de contador permite utilizar simultáneamente varios contadores asociados a respectivos contenidos multimedia y, por tanto, por ejemplo, condicionar la visualización de un tercer contenido multimedia a la visualización previa de cuartos contenidos multimedia, siendo los contenidos multimedia tercero y cuarto distintos e independientes de los primeros y segundos contenidos multimedia,

20

- condicionar la modificación del valor del contador a la desaleatorización de uno o varios criptoperíodos permite potenciar la seguridad del sistema,

25

- modificar el valor del contador en un sentido opuesto a las instrucciones de progresión en cada visualización de un primer contenido multimedia permite condicionar nuevamente la visualización de un próximo primer contenido multimedia a la visualización previa de segundos contenidos multimedia suplementarios,

30

- una inscripción de un crédito de acceso que autoriza la visualización completa del primer contenido multimedia cuando el valor del contador alcanza un umbral predeterminado autoriza la visualización del primer contenido multimedia durante un tiempo predeterminado,

35

- imponer un límite máximo al valor del contador permite imponer una alternancia entre la visualización de los segundos contenidos multimedia y de los primeros contenidos multimedia;

40

- crear el contador automáticamente como respuesta a la recepción de instrucciones de progresión de ese contador evita tener que inicializar ese contador en la puesta en servicio del receptor o a partir de comandos específicos emitidos por el emisor.

La invención tiene asimismo por objeto un soporte de grabación de información que incorpora instrucciones para la ejecución del anterior procedimiento cuando estas instrucciones son ejecutadas por un calculador electrónico.

45

La invención tiene asimismo por objeto un procedimiento de emisión conforme a la reivindicación 11.

Las formas de realización de este procedimiento de emisión pueden incorporar la característica de la reivindicación 12.

50

La invención tiene asimismo por objeto un receptor conforme a la reivindicación 13.

La invención tiene asimismo por objeto un procesador conforme a la reivindicación 14.

Finalmente, la invención tiene asimismo por objeto un emisor conforme a la reivindicación 15.

55

Se comprenderá mejor la invención con la lectura de la descripción subsiguiente, dada únicamente a título de ejemplo no limitativo y hecha con referencia a los dibujos, en los que:

la figura 1 es una ilustración esquemática de la arquitectura de un sistema de difusión de contenidos multimedia aleatorizados,

60

la figura 2 es una ilustración esquemática de una parrilla de programas utilizada en el sistema de la figura 1,

la figura 3 es una ilustración esquemática de la arquitectura de un contador utilizado en el sistema de la figura 1,

la figura 4 es un organigrama de un procedimiento de emisión y de recepción de primeros contenidos multimedia
5 cuya visualización está condicionada a la visualización previa de segundos contenidos multimedia,

la figura 5 es una ilustración esquemática de la arquitectura de un mensaje ECM_{CP} utilizado en el sistema de la figura 1,

10 la figura 6 es una ilustración esquemática de un mensaje ECM_{CNP} utilizado en el sistema de la figura 1,

la figura 7 es una ilustración esquemática de cronograma que muestra la evolución del valor de un contador cuando se aplica el procedimiento de la figura 4,

15 la figura 8 es una ilustración esquemática de la arquitectura de otra forma de realización de un mensaje ECM_{CP},

la figura 9 es un organigrama de otra forma de realización de un procedimiento de emisión y de recepción de primer contenido multimedia cuya visualización está condicionada a la visualización previa de otros contenidos multimedia,
y

20

la figura 10 es una ilustración esquemática de la arquitectura de un mensaje ECM_{CNP} utilizado en el procedimiento de la figura 9.

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

25

En la continuación de esta descripción, las características y funciones de sobra conocidas para el experto en la materia no se describen en detalle. Además, la terminología empleada es la de los sistemas de acceso condicionales a contenidos multimedia. Para más información sobre esta terminología, el lector puede remitirse al siguiente documento:

30 «Fonctionnal Model of Conditional Access System» EBU Review - Technical European Broadcasting Union, Bruselas, BE, n.º 266, 21 de diciembre de 1995.

La figura 1 representa un sistema 2 de difusión de pago de contenidos multimedia. Por ejemplo, el sistema 2 es un sistema que permite difundir varios canales de televisión aleatorizados. La desaleatorización de cada uno de estos
35 canales de televisión o grupos de canales de televisión está generalmente condicionada al pago de una suscripción por unos abonados.

El sistema 2 comprende al menos un emisor 4 de contenidos multimedia aleatorizados y una multitud de receptores aptos para desaleatorizar los contenidos multimedia difundidos por el emisor 4. Para simplificar la figura 1, sólo se ha
40 representado un receptor 6. Por ejemplo, los demás receptores son idénticos al receptor 6.

45

El emisor 4 comprende un aleatorizador 10 apto para aleatorizar, con ayuda de una palabra de control CW, unos contenidos multimedia recibidos en claro por intermedio de un puerto 12 según van siendo recibidos. A tal efecto, el aleatorizador 10 utiliza la palabra de control contenida en una memoria 14. El contenido multimedia aleatorizado se
45 transmite a la entrada de un multiplexor 16.

La aleatorización del contenido multimedia es una operación de cifrado y la palabra de control es la clave de cifrado utilizada para aleatorizar el contenido multimedia.

50 El emisor 4 comprende asimismo un generador de palabras de control 18. El generador 18 modifica regularmente la palabra de control contenida en la memoria 14. El intervalo de tiempo entre dos modificaciones de la palabra de control utilizada para aleatorizar un contenido multimedia se denomina «criptoperíodo».

Un generador 20 genera un nuevo mensaje ECM (Entitlement Control Message) cada vez que el generador 18 genera una nueva palabra de control. Cada mensaje ECM comprende además:

55

- un criptograma CW* de la palabra de control, y

- unas condiciones de acceso al contenido multimedia aleatorizado.

60 El criptograma CW* es una información necesaria, pero insuficiente por sí sola, para desaleatorizar el contenido multimedia. Por ejemplo, el criptograma CW* se obtiene cifrando la palabra de control con una clave de explotación

conocida por el receptor o una referencia a una palabra de control o a un criptograma de la palabra de control contenida en el receptor.

Las condiciones de acceso están destinadas a ser comparadas con unos créditos de acceso o derecho de acceso pregrabados en el receptor. La desaleatorización del contenido multimedia se autoriza únicamente si las condiciones de acceso con las que está este asociado se corresponden con unos créditos de acceso pregrabados. Por ejemplo, una condición de acceso puede ser un nivel moral asociado al contenido multimedia.

El mensaje ECM generado por el generador 20 se transmite a la entrada del multiplexor 16.

10

En el presente caso, el generador 20 está unido a una memoria 22 que contiene una parrilla 24 de los programas.

El multiplexor 16 permite multiplexar el contenido multimedia aleatorizado con los mensajes ECM que contienen los criptogramas CW* necesarios para la desaleatorización de este contenido multimedia. El multiplexor 16 crea así un flujo de datos multiplexados difundido hacia el conjunto de los receptores por intermedio de una red 30 de transmisión de información. Esta multiplexación permite sincronizar temporalmente la emisión de los mensajes ECM a la emisión del contenido multimedia aleatorizado.

Por ejemplo, la red 30 es una red de conmutación de paquetes tal como Internet o una red de difusión de televisión vía satélite.

20

El receptor 6 comprende un descodificador 40 provisto de una antena 42 para recibir los contenidos multimedia difundidos por el emisor 4. El descodificador 40 comprende asimismo un desmultiplexor 44 que desmultiplexa los flujos de datos multiplexados recibidos, con el fin de transmitir el contenido multimedia aleatorizado a un desaleatorizador 46 y los mensajes ECM a un procesador 48 de seguridad.

25

El procesador 48 está unido de modo separable al descodificador 40. Por ejemplo, el procesador 48 es una tarjeta inteligente.

Este procesador 48 comprende un calculador electrónico 50 apto para procesar cada mensaje ECM para descifrar el criptograma CW* y obtener la palabra de control CW que permite desaleatorizar el contenido multimedia. El procesador 48 es apto para transmitir al desaleatorizador 46 la palabra de control CW.

30

El calculador 50 está unido a una memoria 52 que contiene instrucciones para la ejecución del procedimiento de la figura 4 cuando éste ejecuta esas instrucciones. Además, en el presente caso, esta memoria 52 incorpora unos créditos 54 de acceso pregrabados y varios contadores. En la figura 1 sólo se ha representado un contador 56. La estructura y la utilización de los demás contadores se deducen de la descripción que se realiza a continuación en el caso particular del contador 56.

35

El receptor 6 está unido a un televisor 60 a propósito para presentar en pantalla el contenido multimedia desaleatorizado por el descodificador 40.

40

La figura 2 representa un ejemplo de estructura de la parrilla 24. Esta parrilla es en el presente caso una tabla que contiene las siguientes columnas:

45

- una columna CM-ID destinada a contener un identificador de un contenido multimedia,
- una columna W-ID destinada a contener un identificador de un contador del receptor 6,
- una columna Nb-TK destinada a contener un número de pasos de incremento del valor del contador,
- una columna TK-C destinada a contener un número de pasos de decremento del valor actual del contador,
- una columna I-TK-A destinada a contener el identificador del contador que ha de crearse, y
- una columna A-Max destinada a contener un umbral máximo para el valor del contador.

50

Los pasos de incremento o de decremento se pueden denominar asimismo «puntos» o «testigos».

Esta parrilla 24 permite por tanto asociar, con un contenido multimedia designado por el identificador de la columna CM-ID, un cierto número de información referente a un contador que ha de incrementarse, de decrementarse o de crearse en los receptores.

55

La figura 3 representa un ejemplo de estructura para el contador 56. En el presente caso, este contador 56 comprende:

60

- un campo W-ID destinado a contener el identificador del contador 56,
- un campo TK-A destinado a memorizar el valor actual del contador 56,

- un campo A-Max destinado a contener un umbral máximo para el valor del contador 56, y
- un campo LUD destinado a contener la fecha de la última actualización del valor del contador 56.

Por ejemplo, la fecha se expresa en día, hora, minuto y segundo.

5

Ahora se va a describir el funcionamiento del sistema 2 con referencia al procedimiento de la figura 4, en el caso particular en que se pretende condicionar la visualización de contenidos no promocionales a la visualización previa de contenidos promocionales. Por ejemplo:

- el contenido no promocional es una película o una emisión de televisión, y
- 10 • el contenido promocional es una secuencia de espacios publicitarios.

El sistema 2 comienza con una fase de emisión 68 de los contenidos multimedia aleatorizados.

- 15 Inicialmente, antes de la difusión de los contenidos multimedia, en una etapa 70, para cada contenido multimedia promocional o no promocional que ha de difundirse, se completa la parrilla 24 a partir de información proporcionada por un operador. Más precisamente, para cada contenido promocional, se indican las columnas CM-ID, W-ID, Nb-Tk, I-TK-A y A-Max y la columna TK-C está vacía. Por ejemplo, en el presente caso, para cada contenido promocional, las columnas CM-ID, W-ID, Nb-TK, I-TK-A y A-Max tienen, respectivamente, los siguientes valores CP1, C1, «10», «10» y «30». El identificador CP1 es el asociado a cada contenido promocional y el identificador C1 es el del
- 20 contador 56.

Para cada contenido promocional, se indican las columnas CM-ID, W-ID y TK-C y las columnas Nb-TK, I-TK-A y A-Max están vacías. En el presente caso, las columnas Nb-TK, I-TK-A y A-Max tienen, respectivamente, los siguientes valores CNP1, C1 y «1». El identificador CNP1 es el asociado a cada contenido no promocional.

25

A continuación, durante una difusión de cada criptoperíodo de un contenido multimedia, en una etapa 74, el generador 20 crea un mensaje ECM que contiene:

- un criptograma CW* de la palabra de control CW utilizada por el aleatorizador 14 para aleatorizar el contenido multimedia durante el próximo criptoperíodo,
- 30 • eventualmente, la o las condición(ones) de acceso necesaria(s) para autorizar la desaleatorización de ese contenido multimedia, y
- eventualmente, unas instrucciones de progresión o de regresión del contador 56.

- 35 En el presente caso, un mensaje ECM que contiene instrucciones de progresión se señala con ECM_{CP}. Un mensaje ECM que contiene instrucciones de regresión se señala con ECM_{CNP}. Un mensaje ECM que no incorpora ni instrucciones de regresión ni instrucciones de progresión del contador 56 se señala con ECM_N.

Más precisamente, el generador 20 crea un mensaje ECM_{CP} cuando el contenido multimedia en curso de difusión es un contenido multimedia promocional.

40

En la figura 5, se representa un ejemplo de posible estructura para este mensaje ECM_{CP}. Este mensaje ECM_{CP} contiene los siguientes campos:

- un campo HD de cabecera del mensaje ECM_{CP} que contiene el conjunto de los datos que permiten la explotación de ese mensaje tales como, por ejemplo, un índice de clave de explotación para descifrar el criptograma CW* y/o un
- 45 identificador de zona de servicio de interés en el procesador de seguridad,

- un campo CW* que contiene el criptograma CW* de la palabra de control CW utilizada para aleatorizar el contenido promocional,

50

- un campo D que contiene la fecha actual,

- una zona AC que contiene, eventualmente, una o varias condiciones de acceso al contenido promocional,

55

- una zona CU que contiene instrucciones de progresión,

- una zona WCR que contiene instrucciones de creación del contador, y

- un campo S que contiene una firma del mensaje ECM_{CP}.

60

Típicamente, en un mensaje ECM_{CP} no existen condiciones de acceso relativas al valor del contador 56.

La zona CU comprende:

- un campo W-ID destinado a contener el identificador del contador que ha de incrementarse, y
- un campo Nb-TK que contiene el número de pasos en que se tiene que incrementar el valor del contador.

5 Por ejemplo, el paso de incremento es igual a «1».

La zona WCR comprende:

- un campo I-TK-A que contiene el valor inicial del contador que ha de crearse, y
- un campo A-Max que contiene un umbral máximo para el contador que ha de crearse.

10

La firma contenida en el campo S permite comprobar la integridad del mensaje ECM_{CP} en su recepción. Por ejemplo, esta firma se obtiene con ayuda de un resumen (Hash) o de un MAC (Message Authentication Code) aplicado al contenido del mensaje ECM_{CP} .

15 Para completar el valor de los campos de las zonas CU y WCR, el generador 20 utiliza el identificador del contenido multimedia difundido y el contenido de la parrilla 24. Por ejemplo, en el presente caso, los campos W-ID, Nb-TK, I-TK-A y A-Max tienen, respectivamente, los siguientes valores C1, «10», «10» y «30».

La figura 6 representa un ejemplo de estructura para un mensaje ECM_{CNP} asociado a cada contenido no promocional difundido. La estructura del mensaje ECM_{CNP} es idéntica a la del mensaje ECM_{CP} a excepción de que:

- este no incorpora zonas CU y WCR, y
- la zona AC contiene una condición de acceso función del valor del contador 56.

En el presente caso, esta condición de acceso se codifica con ayuda de los siguientes campos:

- 25 • un campo A-CND1 destinado a contener un identificador de la condición de acceso,
- un campo W-ID destinado a contener un identificador del contador cuyo valor se tiene que comprobar, y
- un campo TK-C destinado a contener instrucciones de regresión del valor del contador.

En el presente caso, la instrucción de regresión corresponde a un número de pasos de decremento en que se tiene que disminuir el valor actual del contador. El paso de decremento se elige igual a «1».

30

Al igual que para el mensaje ECM_{CNP} , los valores de los campos W-ID y TK-C se obtienen con ayuda del identificador del contenido no promocional y del contenido de la parrilla 24. En el presente caso, los campos W-ID y TK-C contienen, respectivamente, los valores C1 y «1».

35

La zona AC puede contener otras condiciones de acceso. Por ejemplo, en la figura 6 se ha representado el primer campo A-CND2 de una segunda condición de acceso.

La estructura de un mensaje ECM_N puede bien estar desprovista de campos que contienen instrucciones de progresión o de regresión del valor de un contador, o bien incorporar instrucciones de progresión o de regresión del valor de un contador diferente del contador 56. La estructura del mensaje se deduce por tanto de las estructuras de mensajes ECM anteriormente descritas.

40

En paralelo con la etapa 74, en una etapa 82, cada criptoperíodo del contenido multimedia difundido es aleatorizado con ayuda de la palabra de control CW en curso.

45

A continuación, en una etapa 84, se multiplexa un contenido multimedia aleatorizado y los mensajes ECM que tiene asociados, para crear el flujo de datos multiplexados.

50 En una etapa 86, mediante el emisor 4 se difunde el flujo de datos multiplexados a través de la red 30 con destino a los receptores.

Las etapas 74, 82, 84 y 86 son reiteradas en bucle para cada criptoperíodo con el fin de difundir los sucesivos criptoperíodos de los contenidos multimedia.

55

En paralelo, cada receptor efectúa una fase 90 de recepción de los contenidos multimedia aleatorizados.

Inicialmente, en una etapa 92, el descodificador 40 recibe y desmultiplexa el flujo de datos multiplexados recibido. El contenido multimedia aleatorizado se envía entonces al desaleatorizador 46, en tanto que los mensajes ECM se envían al procesador 48.

60

En una etapa 94, el calculador 50 comprueba la firma S del mensaje ECM recibido. En caso de estar corrompido el mensaje ECM, el calculador 50 procede a una etapa 96 de inhibición de la desaleatorización del contenido multimedia. Por ejemplo, en la etapa 96, el procesador 48 inhibe el descifrado del criptograma CW*, de modo que se imposibilita la desaleatorización del contenido multimedia. En la etapa 96, no se autoriza por tanto la visualización en claro del contenido multimedia.

En caso contrario, en una etapa 98, el calculador 50 compara las condiciones de acceso contenidas en el mensaje ECM recibido con los créditos 54 de acceso. En la etapa 98, las condiciones de acceso definidas con ayuda del campo TK-C no son evaluadas. En el caso en que la memoria 52 no incorpora ningún crédito de acceso correspondiente a esas condiciones de acceso, entonces el calculador 50 procede a la etapa 96.

En caso contrario, procede a una etapa 100 de comprobación de la existencia de un identificador de contador en el mensaje ECM recibido. Este identificador se busca bien en el campo W-ID de la zona CU, o bien en el campo W-ID de la zona AC.

En el caso en que el mensaje ECM no contiene ningún identificador de contador, entonces la visualización de ese contenido multimedia no está condicionada a la visualización previa de contenidos promocionales. Por ejemplo, se trata de un mensaje ECM_N desprovisto de zona CU y de condiciones de acceso que hacen intervenir el valor de un contador. En este caso, se procede directamente a una etapa 102 durante la cual el calculador 50 descifra el criptograma CW* para obtener la palabra de control CW y la transmite al desaleatorizador 46. A continuación, el desaleatorizador 46 desaleatoriza el criptoperíodo siguiente del contenido multimedia recibido con ayuda de esa palabra de control y transmite el contenido multimedia desaleatorizado al televisor 60, que lo presenta en pantalla en claro. Así, se autoriza la visualización de ese contenido multimedia, puesto que el contenido multimedia se presenta en pantalla en una forma directamente perceptible y comprensible para un usuario.

En caso contrario, en una etapa 104, el calculador 50 comprueba si el identificador de contador encontrado en la etapa 100 corresponde a un contador ya existente en la memoria 52. En caso negativo, en una etapa 106, el calculador 50 comprueba si existe una zona WCR en el mensaje ECM recibido. En caso negativo, el procesador 48 procede entonces directamente a la etapa 96. En caso afirmativo, en una etapa 108, el calculador 50 crea en la memoria 52 un contador que tiene la estructura descrita con referencia a la figura 3. Los valores de los campos W-ID, TK-A, A-Max y LUD del contador creado se inicializan a partir de los valores, respectivamente, de los campos W-ID, I-TK-A, A-Max y D del mensaje ECM recibido. Así, si el contador 56 aún no existía en la primera recepción de un contenido no promocional, este contador es creado automáticamente en la etapa 108.

Si el contador correspondiente al identificador contenido en el campo W-ID ya existe en la memoria 52 o al término de la etapa 108, el calculador 50 procede a una etapa de comprobación 110 de la existencia del campo Nb-TK en el mensaje ECM recibido.

En caso afirmativo, el mensaje ECM recibido es un mensaje ECM_{CP}. Entonces, en una etapa 112, el calculador 50 comprueba que la fecha contenida en el campo LUD de ese contador es anterior a la fecha contenida en el campo D del mensaje ECM recibido.

En caso afirmativo, en una etapa 114, el calculador 50 incrementa el valor contenido en el campo TK-A de ese contador 56 en el número de pasos indicado en el campo Nb-TK del mensaje ECM recibido. De ser necesario, en la etapa 114, el calculador 50 limita el incremento del valor del contador para no sobrepasar el umbral indicado en el campo A-Max. El nuevo valor del contador se memoriza entonces hasta la próxima iteración de la etapa 114.

En la etapa 114, se actualiza asimismo el campo LUD del contador 56 a partir de la fecha contenida en el campo D del mensaje ECM recibido.

Al término de la etapa 114 o si la última fecha de actualización del contador 56 es posterior a la fecha contenida en el mensaje ECM recibido, el procesador procede directamente a la etapa 102.

En caso de no existir el campo Nb-TK en el mensaje EMC recibido, es porque este mensaje es un mensaje ECM_{CNP}. El calculador 50 procede entonces a una etapa de comprobación 116 de la existencia del campo TK-C en la zona AC del mensaje ECM recibido. Si el mensaje ECM recibido contiene efectivamente este campo, entonces significa que el contenido multimedia actualmente difundido es un contenido multimedia cuya visualización está condicionada a la visualización previa de otros contenidos multimedia.

En tal caso, en una etapa 118, el calculador 50 comprueba que el valor actual del contador en la etapa 100 es superior al valor contenido en el campo TK-C. En caso negativo, se procede directamente a la etapa 96, lo cual

prohíbe la visualización de ese contenido multimedia.

En caso contrario, en una etapa 120, el calculador 50 decreuenta el valor actual del contador identificado en un número de pasos definido por el valor contenido en el campo TK-C del mensaje ECM recibido. En la etapa 120, la fecha contenida en el campo LUD del contador se sustituye asimismo por la fecha contenida en el mensaje ECM recibido.

Al término de la etapa 120 o si, en la etapa 116, el mensaje ECM no contiene el campo TK-C, se procede directamente a la etapa 102.

La figura 7 da un ejemplo de evolución del valor del contador 56.

En la figura 7, la banda de arriba representa la sucesión temporal de un contenido no promocional 130, de un contenido promocional 131 y de un contenido no promocional 132.

Una banda 134 representa ocho criptoperíodos CP1 a CP8 sucesivos que cubren el intervalo temporal durante el cual son recibidos los contenidos 130 a 132.

Una banda 136 representa los instantes de emisión de los mensajes ECM. En el presente caso, cada mensaje ECM es transmitido al receptor durante el criptoperíodo que precede al criptoperíodo del contenido multimedia al que está asociado. Así, los mensajes ECM2 a ECM9 se asocian, respectivamente, a los criptoperíodos CP2 a CP9. El valor entre corchetes representa el valor contenido en el campo TK-C del mensaje ECM cuando aquél es negativo o el valor contenido en el campo Nb-TK cuando aquél es positivo. Se corrobora por tanto que los mensajes ECM5 y ECM6 son mensajes ECM_{CP} asociados a los contenidos 131. Los demás mensajes representados son mensajes ECM_{CNP}.

Una banda 138 representa el valor del campo TK-A del contador 56. Una banda 140 indica en gris los criptoperíodos durante los cuales la visualización de los contenidos no promocionales es posible y, en negro, los criptoperíodos en los que tal visualización no es posible.

Más precisamente, durante el criptoperíodo CP1, el valor del contador 56 es igual a «1». Consecuentemente, se autoriza la desaleatorización del contenido multimedia durante el criptoperíodo CP2, ya que el campo TK-C del mensaje ECM2 es igual a «1». El tratamiento del mensaje ECM2 durante el criptoperíodo CP1 conduce a decrementar el valor del contador 56 en «1», de modo que este valor es de «0» durante el criptoperíodo CP2.

A continuación, en el criptoperíodo CP2, el valor del campo TK-C del mensaje ECM3 se compara con el actual valor del contador 56. Esta vez, el valor del contador 56 es inferior al valor del campo TK-C. Consecuentemente, la desaleatorización del contenido multimedia no promocional se prohíbe durante el criptoperíodo siguiente CP3. En este ejemplo, la ejecución del procedimiento de la figura 4 también conduce a prohibir la visualización del contenido 130 durante el criptoperíodo CP4.

Durante el criptoperíodo CP4, el calculador 50 recibe el mensaje ECM5 en el que el valor del campo Nb-TK es igual a «10». Consecuentemente, el valor del contador 56 se incrementa en 10 y se autoriza la visualización del contenido 131 durante el criptoperíodo CP5.

Durante el criptoperíodo siguiente CP5, se recibe otro mensaje ECM_{CP} de modo que el valor del contador 56 se incrementa nuevamente en «10».

A continuación, para desaleatorizar el contenido 132, sólo se reciben mensajes ECM_{CNP}. Así, el valor del contador 56 es decrementado en «1» al final de cada uno de los criptoperíodos CP6 y CP7. No obstante, la visualización del contenido 132 se autoriza durante los criptoperíodos CP7 y CP8, ya que el valor del contador 56 es superior al valor contenido en el campo TK-C de los mensajes ECM7 y ECM8.

Se comprende por tanto que el procedimiento de la figura 4 autoriza una duración de visualización de un contenido no promocional que es función de la duración de contenidos promocionales visualizados previamente. Por ejemplo, en el presente caso, la duración de visualización autorizada de contenido no promocional es directamente proporcional a la duración de los contenidos promocionales visualizados. Este procedimiento incita por tanto a los usuarios a visualizar los contenidos promocionales, al tiempo que deja al usuario una gran flexibilidad para acumular y gastar los puntos de su contador.

La figura 8 representa otra posible forma de realización para la estructura de un mensaje ECM_{CP}. En esta forma de

realización, el mensaje ECM_{CP} es idéntico al descrito con referencia a la figura 5 con la excepción de que no incorpora la zona WCR. Así, en esta forma de realización, los contadores tales como el contador 56 tienen que ser inicializados en la memoria 52, ya sea en la emisión o la fabricación del procesador 48, ya sea con ayuda de mensajes EMM (Entitlement Management Message).

5

Se va a describir ahora otra forma de realización del procedimiento de la figura 4 con referencia a las figuras 9 y 10.

El procedimiento de la figura 9 es idéntico al procedimiento de la figura 4 con la excepción de que:

- en la etapa 74, la estructura del mensaje ECM_{CP} creada es la representada en la figura 10,
- 10 • se suprimen las etapas 110, 116, 118 y 120, y
- se introducen unas etapas 162 y 164 después de la etapa 114.

La estructura del mensaje ECM_{CP} representada en la figura 10 es idéntica a la del mensaje ECM_{CP} representada en la figura 5, con la excepción de que la zona WCR es sustituida por una zona RI-C. La zona RI-C contiene 15 instrucciones para la inscripción en la memoria 52 de un nuevo crédito de acceso si el valor del contador sobrepasa un umbral predeterminado S₁. Este nuevo crédito de acceso corresponde a una condición de acceso al contenido no promocional. Más precisamente, la zona RI-C contiene:

- un campo TK-S destinado a contener el valor del umbral S₁, y
- un campo RI que contiene el crédito de acceso que ha de inscribirse en la memoria 52 cuando se alcanza el 20 umbral S₁.

Preferentemente, en esta forma de realización, el mensaje ECM_{CNP} está desprovisto de instrucciones de regresión. Así, la estructura del mensaje ECM_{CNP} no se diferencia en nada de la propia de un mensaje ECM convencional.

- 25 Después de haber incrementado el valor del contador en la etapa 114, en la etapa 162, el calculador 50 comprueba si el nuevo valor del contador ha alcanzado el umbral S₁ contenido en el campo TK-S. En caso negativo, se procede directamente a la etapa 102. En caso afirmativo, en la etapa 164, el calculador 50 inscribe en la memoria 52 el crédito de acceso contenido en el campo RI. A continuación, todavía en la etapa 164, se reinicializa el valor del contador 56. Por ejemplo, el valor del contador se repone a cero o se decrementa en el valor S₁. En vez de 30 reinicializar el valor del contador, cabe asimismo la posibilidad de incrementar el valor del umbral S₁ en un paso predeterminado.

En esta forma de realización, cada contenido no promocional está asociado con una condición de acceso A-CND. Mientras la memoria 52 no incorpore un crédito de acceso correspondiente a esta condición de acceso, está 35 prohibida la visualización del contenido no promocional. Cuando el valor del contador alcanza el umbral S₁, entonces se inscribe automáticamente en la memoria 52 un crédito de acceso correspondiente a esta condición A-CND. En consecuencia, se autoriza la visualización del próximo contenido no promocional recibido. Como en la forma de realización de la figura 4, ello incita a los usuarios a visualizar los contenidos promocionales. Además, la inscripción de un crédito de acceso permite ajustar precisamente la duración de contenido no promocional visualizable. Por 40 ejemplo, el nuevo crédito de acceso inscrito en la memoria 52 autoriza únicamente la visualización del canal del día y del día siguiente.

- 45 Son posibles otras numerosas formas de realización. Por ejemplo, la visualización del contenido multimedia no promocional se puede impedir mediante otros medios que no sean la aleatorización de ese contenido. En tal caso, los procedimientos anteriormente descritos se pueden aplicar en un contexto en el que los primeros y segundos contenidos multimedia no están aleatorizados.

Como variante, la antena 42 es sustituida por un adaptador de red cuando el decodificador recibe los contenidos multimedia por intermedio de un cable. Por ejemplo, el cable es un cable Ethernet.

50

En el presente caso, el identificador del contador permite utilizar y poner en práctica los procedimientos de las figuras 4 y 9 para varios contenidos multimedia no promocionales distintos, de manera que se somete la visualización de uno de esos contenidos multimedia no promocionales al valor de un contador particular. En una forma de realización particular, el identificador de contador puede ser función del número del canal visualizado.

55

No obstante, como variante, se puede utilizar un único contador para todos los contenidos no promocionales. En este caso, se puede omitir el identificador del contador.

- 60 Los procedimientos de las figuras 4 y 9 se pueden modificar para no autorizar el incremento del contador más que cuando se ha visualizado en su totalidad un grupo de varios criptoperíodos consecutivos del contenido promocional. A tal efecto, un mensaje ECM incorpora una indicación del inicio de un grupo de criptoperíodos y, luego, un mensaje

ECM ulterior, difundido al final de este grupo de criptoperíodos, incorpora una indicación de final del grupo de criptoperíodos. Además, en cada mensaje ECM recibido durante ese grupo de criptoperíodos, se inserta un identificador de grupo de criptoperíodos y un contador de continuidad de los criptoperíodos del grupo. A partir de esta información, el calculador 50 comprueba que los criptoperíodos de este grupo han sido recibidos todos ellos 5 unos inmediatamente después de los otros. En caso afirmativo, el valor del contador se incrementa en el número de pasos indicado en el campo Nb-TK. En caso negativo, es decir, si uno de los criptoperíodos no se ha desaleatorizado, el valor del contador permanece inalterado. Al sincronizar temporalmente ese grupo de criptoperíodos con un contenido promocional, es posible incitar al usuario a ver el conjunto del contenido promocional sin cambiar entretanto de canal.

10

Otro procedimiento para someter el incremento del contador 56 a la visualización de un segmento completo de contenido promocional que se extiende por varios criptoperíodos consiste en señalar el inicio y el final de ese grupo de criptoperíodos y en agregar, en cada mensaje ECM asociado a ese grupo, un fragmento de firma de un mensaje EMM local que contiene la fecha, el identificador del contador y el valor del campo Nb-TK en que se tiene que 15 incrementar ese contador. Antes de incrementar el contador correspondiente al identificador contenido en ese mensaje EMM construido localmente por el receptor, el calculador 50 comprueba la firma de ese mensaje comparándola con la firma obtenida al concatenar el conjunto de los fragmentos de firma contenidos en los mensajes ECM asociados a ese grupo. En caso de que se correspondan las dos firmas, se autoriza el incremento del valor del contador y, en caso contrario, se prohíbe.

20

En los mensajes ECM, la zona AC se puede omitir si el contenido promocional es en abierto.

Las instrucciones de progresión asociadas a los contenidos promocionales han sido descritas en el caso particular en que éstas corresponden a un paso de incremento constante por criptoperíodo. Así, el incremento del contador es 25 directamente proporcional al número de criptoperíodos de contenidos promocionales visualizados. Como variante, el paso de incremento no es constante y puede variar entre dos criptoperíodos de contenidos promocionales.

En el presente caso, el contador se ha descrito en el caso particular en que su valor se incrementa cuando se visualiza un contenido promocional y se decrementa cuando se visualiza un contenido no promocional. En otra forma 30 de realización, los sentidos de variación del valor de este contador son opuestos, es decir, el contador se decrementa cuando se visualizan contenidos promocionales y se incrementa cuando se visualiza un contenido no promocional.

Es posible sustituir la operación de incremento de valor del contador por una operación de incremento del valor del 35 umbral predeterminado más allá del cual se autoriza la visualización del contenido multimedia no promocional.

El paso de incremento o de decremento no es necesariamente un entero. Puede tratarse de un número racional o de un número real.

40 Cuando se ha descrito en el caso particular de la gestión de claves de cifrado con ayuda de mensajes ECM y EMM es de aplicación en cualquier procedimiento de gestión de claves que implique el envío de criptogramas de la palabra de control utilizada para emitir los contenidos multimedia.

El contador no necesariamente se graba en la memoria del procesador de seguridad. Por ejemplo, como variante, el 45 valor del contador se graba en el descodificador en forma cifrada, con ayuda de una clave contenida en el procesador de seguridad.

El procesador 48 puede venir integrado de modo indismontable en el descodificador o en el desaleatorizador. Por el 50 contrario, el desaleatorizador puede ser separable.

50

Cuando se ha descrito anteriormente se puede aplicar asimismo para condicionar la visualización de un contenido no promocional a la visualización previa de un cierto número de veces de un mismo contenido promocional. En tal caso, el valor del contador se incrementa por ejemplo en función del número de veces que se ha visualizado ese contenido 55 promocional. La estructura de los ECM descrita y los anteriores procedimientos permanecen inalterados, sólo cambia la utilización de los procedimientos.

Cuando se ha descrito se aplica asimismo en el contexto del vídeo bajo demanda. Por ejemplo, los anteriores procedimientos se pueden poner en práctica para condicionar la visualización gratuita de un vídeo bajo demanda a 60 la visualización previa de una cierta duración de contenido promocional. En tal caso, estos contenidos promocionales son, por ejemplo, aquellos que se reproducen justo antes del vídeo bajo demanda.

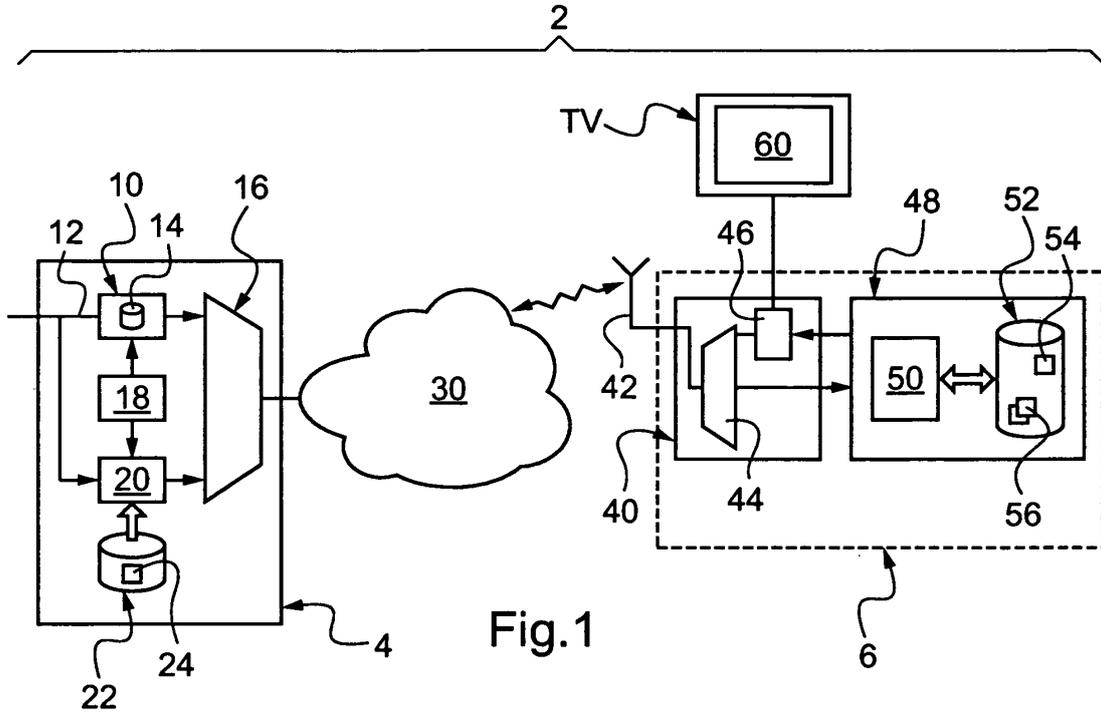
Los primeros y segundos contenidos multimedia pueden ser distintos, respectivamente, de contenidos no promocionales y de contenidos promocionales. Por ejemplo, los segundos contenidos pueden ser unos primeros episodios de una serie televisiva y, los primeros contenidos multimedia, los últimos episodios de esa serie. Así, se incita a los usuarios a ver todos los episodios, incluidos los primeros. Con carácter general, cuanto se ha descrito 5 anteriormente no está limitado a tipos particulares de primeros y segundos contenidos multimedia.

REIVINDICACIONES

1. Procedimiento de recepción de un primer contenido multimedia aleatorizado cuya visualización está condicionada a la visualización previa de segundos contenidos multimedia aleatorizados, siendo estos segundos contenidos multimedia los únicos que están asociados a unos mensajes de control de acceso que contienen un criptograma de una palabra de control para desaleatorizarlos y unas instrucciones de progresión del valor de un mismo contador, instrucciones de progresión estas que modifican toda ellas el valor de ese mismo contador en el mismo sentido cuando son ejecutadas por un receptor electrónico de los primeros y segundos contenidos multimedia, caracterizado porque este procedimiento comprende:
- 5
- 10 - cada vez que un segundo contenido multimedia es visualizado con ayuda del receptor electrónico, la modificación (114) del valor del contador en función de las instrucciones de progresión asociadas a ese segundo contenido multimedia,
- la memorización (114) del valor de ese contador entre visualizaciones no consecutivas de segundos contenidos multimedia entrecortadas por la visualización de otro contenido multimedia que no modifica el valor del contador,
- 15
- el condicionamiento (118; 98) de la visualización del primer contenido multimedia a un valor predeterminado del contador, y
- 20 - cada vez que se autoriza la visualización del primer contenido multimedia con ayuda del receptor electrónico, el procedimiento comprende la modificación (120; 164) del valor del contador en un sentido opuesto a las instrucciones de progresión.
2. Procedimiento según la reivindicación 1, en el que, antes de la visualización de cada segundo contenido multimedia, el procedimiento comprende la desmultiplexación (92) de un flujo de datos multiplexados recibido que contiene el segundo contenido multimedia multiplexado con las instrucciones de progresión y en el que la modificación del valor del contador es función de las instrucciones de progresión multiplexadas con ese segundo contenido multimedia.
- 25
- 30 3. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende la selección (112) del contador cuyo valor se tiene que modificar de entre varios posibles contadores en función de un identificador de ese contador asociado a las instrucciones de progresión.
4. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:
- 35 - la recepción (92) de un grupo de uno o varios criptoperíodos del segundo contenido multimedia y de instrucciones de progresión asociadas a ese grupo, estando aleatorizado cada criptoperíodo del segundo contenido multimedia con una respectiva palabra de control, y
- la modificación (114) del valor del contador cada vez que todos los criptoperíodos de ese grupo son desaleatorizados por el receptor electrónico.
- 40
5. Procedimiento según la reivindicación 4, en el que, antes de un criptoperíodo del segundo contenido multimedia, el procedimiento comprende la recepción (92) de un mensaje difundido simultáneamente al conjunto de los receptores susceptibles de recibir los contenidos multimedia primero y segundo, conteniendo este mensaje un criptograma CW* de la palabra de control necesaria para desaleatorizar ese criptoperíodo y las instrucciones de progresión asociadas al grupo al que pertenece ese criptoperíodo.
- 45
6. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:
- la recepción (92) de un grupo de uno o varios criptoperíodos del primer contenido multimedia y de instrucciones de regresión del valor del contador asociado a ese grupo, estando aleatorizado cada criptoperíodo con una respectiva palabra de control,
- 50
- cada vez que se desaleatorizan todos los criptoperíodos del grupo, la modificación (120) del valor del contador en función de las instrucciones de regresión asociadas a ese grupo en un sentido opuesto a las instrucciones de progresión, y
- 55
- la prohibición (96) de la desaleatorización de un próximo grupo de criptoperíodos del primer contenido multimedia en cuanto el valor del contador alcanza un umbral predeterminado.
- 60 7. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende:

- la recepción (92) del primer contenido multimedia aleatorizado y de condiciones de acceso a este primer contenido multimedia,
 - la prohibición (98, 96) de la desaleatorización del primer contenido multimedia si en el receptor electrónico no está inscrito ningún crédito de acceso correspondiente a las condiciones de acceso y, por el contrario,
 - la autorización (98) de la desaleatorización del primer contenido multimedia si en el receptor electrónico está inscrito un crédito de acceso correspondiente a las condiciones de acceso a este primer contenido multimedia, y
- 10 - la inscripción (164) en el receptor de un crédito de acceso correspondiente a las condiciones de acceso en cuanto el valor del contador ha franqueado un umbral predeterminado.
8. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende la limitación del valor del contador a un umbral predeterminado.
- 15 9. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende la creación automática (108) del contador como respuesta a la recepción de instrucciones de progresión del valor de este contador.
- 20 10. Soporte de grabación de información, caracterizado porque incorpora instrucciones para la ejecución de un procedimiento de recepción conforme a una cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un calculador electrónico.
11. Procedimiento de emisión de un primer contenido multimedia aleatorizado cuya visualización está condicionada a la visualización previa de segundos contenidos multimedia aleatorizados, siendo estos segundos contenidos multimedia los únicos que están asociados a unos mensajes de control de acceso que contienen un criptograma de una palabra de control para desaleatorizarlos y unas instrucciones de progresión del valor de un mismo contador de un receptor electrónico de los primeros y segundos contenidos multimedia, instrucciones de progresión estas que modifican todas ellas el valor de ese mismo contador en el mismo sentido cuando son ejecutadas por el receptor electrónico, caracterizado porque este procedimiento comprende:
- 25 30 - la emisión (86) de los mensajes de control de acceso asociados a cada segundo contenido multimedia emitido,
- la emisión (86), entre dos segundos contenidos multimedia, de otros contenidos multimedia no asociados a mensajes de control de acceso que contienen instrucciones de modificación del valor de ese contador, y
- 35 - la emisión (86) de condiciones de acceso asociadas al primer contenido multimedia emitido, condicionando estas condiciones de acceso la visualización del primer contenido multimedia a un valor predeterminado del contador.
- 40 12. Procedimiento según la reivindicación 11, en el que el procedimiento comprende la emisión (86) de instrucciones de regresión del valor del contador asociadas al primer contenido multimedia emitido, siendo estas instrucciones de regresión a propósito para aumentar la diferencia entre el valor del mismo contador y dicho valor predeterminado cuando se autoriza la visualización del primer contenido multimedia.
- 45 13. Receptor de un primer contenido multimedia aleatorizado cuya visualización está condicionada a la visualización previa de segundos contenidos multimedia aleatorizados, siendo estos segundos contenidos multimedia los únicos que están asociados a unos mensajes de control de acceso que contienen un criptograma de una palabra de control para desaleatorizarlos y unas instrucciones de progresión del valor de un mismo contador, instrucciones de progresión estas que modifican todas ellas el valor de ese mismo contador en el mismo sentido cuando son ejecutadas por el receptor electrónico de los primeros y segundos contenidos multimedia, caracterizado porque este receptor comprende:
- 50 - una memoria (52) apta para almacenar el valor del contador entre visualizaciones no consecutivas de los segundos contenidos multimedia entrecortadas por la visualización de otro contenido multimedia que no modifica el valor del contador, y
- 55 - un calculador electrónico (50) apto:
- para modificar el valor del contador en función de las instrucciones de progresión asociadas a los segundos contenidos multimedia recibidos cada vez que un segundo contenido multimedia es visualizado con ayuda de ese receptor,
- 60

- para condicionar la visualización del primer contenido multimedia a un valor predeterminado del contador, y
 - para, cada vez que se autoriza la visualización del primer contenido multimedia con ayuda del receptor electrónico, 5 modificar el valor del contador en un sentido opuesto a las instrucciones de progresión.
14. Procesador de seguridad apto para su puesta en práctica en un receptor conforme a la reivindicación 13, caracterizado porque este procesador de seguridad comprende un calculador electrónico (50) apto:
- 10 • para modificar el valor del contador en función de las instrucciones de progresión asociadas a los segundos contenidos multimedia recibidos cada vez que un segundo contenido multimedia es visualizado con ayuda de ese receptor, y
- 15 • para condicionar la visualización del primer contenido multimedia a un valor predeterminado del contador, y
- 15 • para, cada vez que se autoriza la visualización del primer contenido multimedia con ayuda del receptor electrónico, modificar el valor del contador en un sentido opuesto a las instrucciones de progresión.
15. Emisor de un primer contenido multimedia aleatorizado cuya visualización está condicionada a la visualización 20 previa de segundos contenidos multimedia aleatorizados, siendo estos segundos contenidos multimedia los únicos que están asociados a unos mensajes de control de acceso que contienen un criptograma de una palabra de control para desaleatorizarlos y unas instrucciones de progresión del valor de un mismo contador de un receptor electrónico de los primeros y segundos contenidos multimedia, instrucciones de progresión estas que modifican todas ellas el valor de ese mismo contador en el mismo sentido cuando son ejecutadas por el receptor electrónico, caracterizado 25 porque el emisor (4) es apto:
- para emitir los mensajes de control de acceso asociados a cada segundo contenido multimedia emitido,
 - para emitir, entre dos segundos contenidos multimedia, otros contenidos multimedia no asociados a mensajes de 30 control de acceso que contienen instrucciones de progresión del valor de ese contador, y
 - para emitir unas condiciones de acceso asociadas al primer contenido multimedia emitido, condicionando estas condiciones de acceso la visualización del primer contenido multimedia a un valor predeterminado del contador.



24

Fig. 2

CM_ID	W-ID	Nb_TK	TK_C	I_TK_A	A_Max
CP1	C1	10		10	30
CNP1	C1		1		



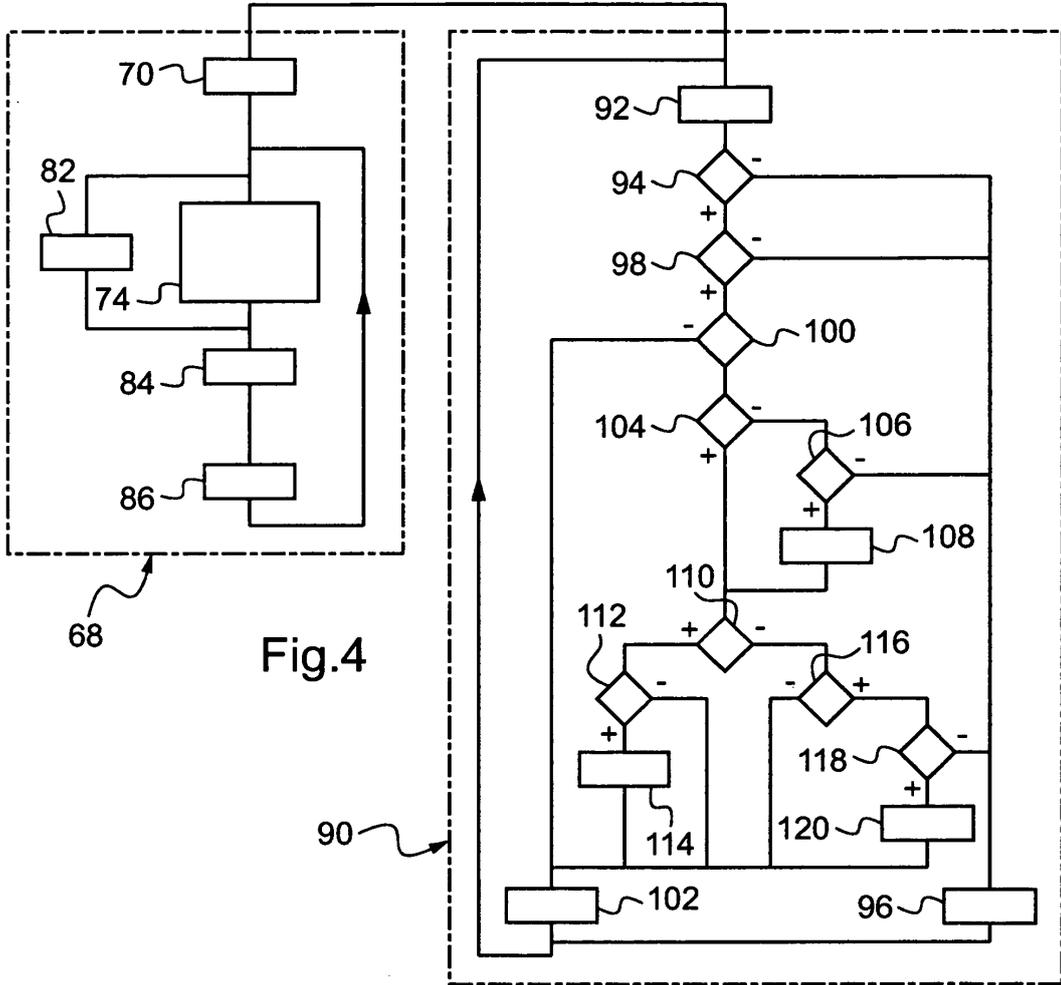


Fig.4

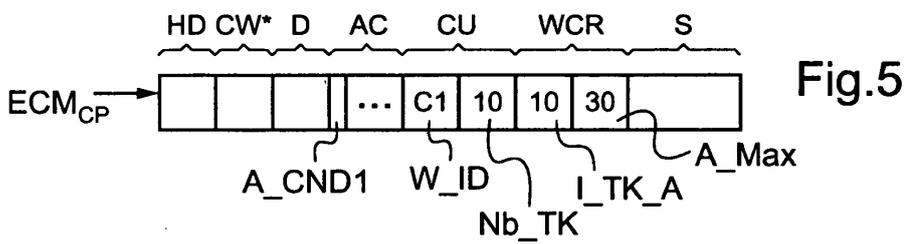


Fig.5

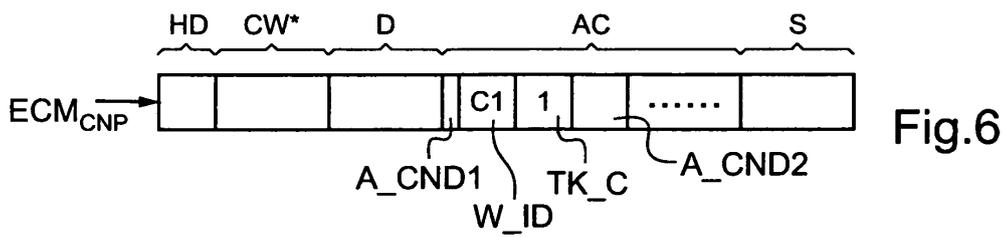


Fig.6

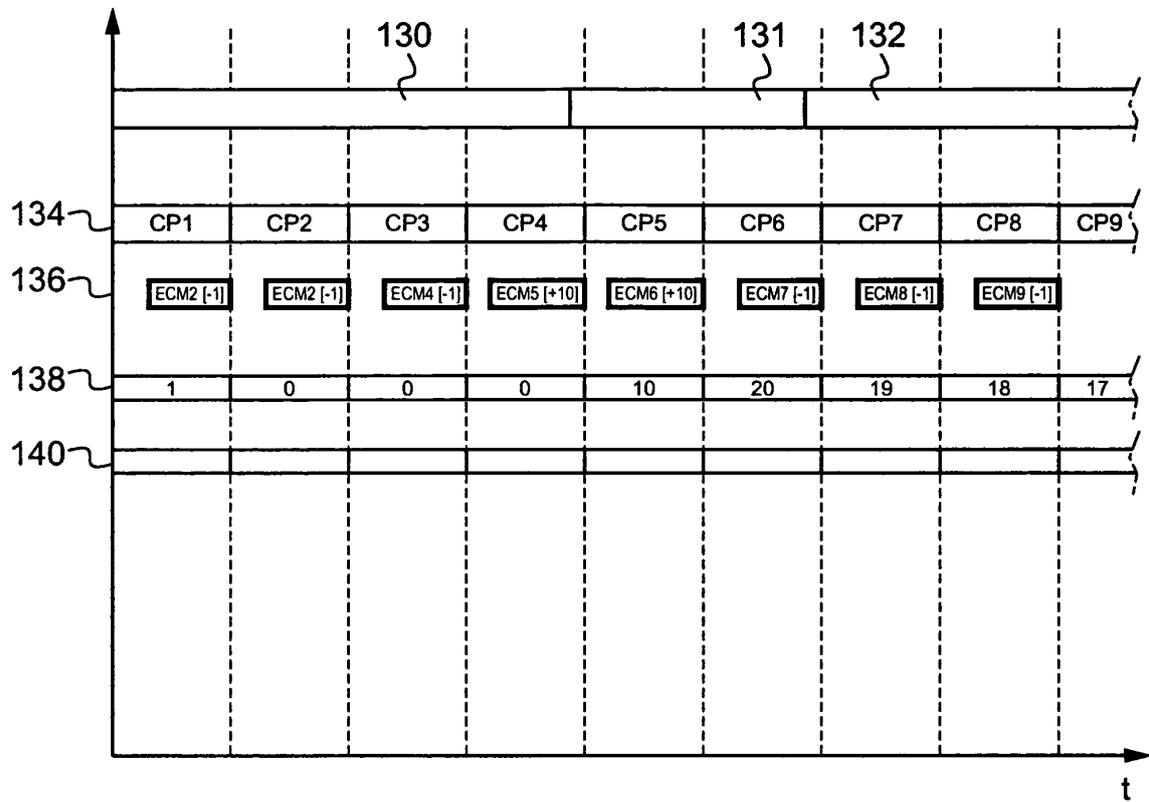


Fig.7

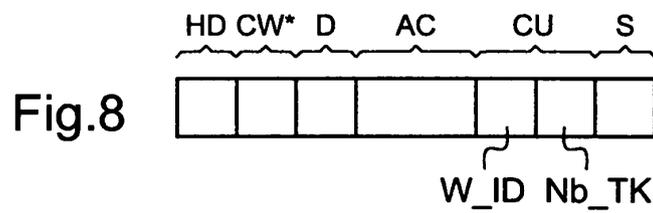


Fig.8

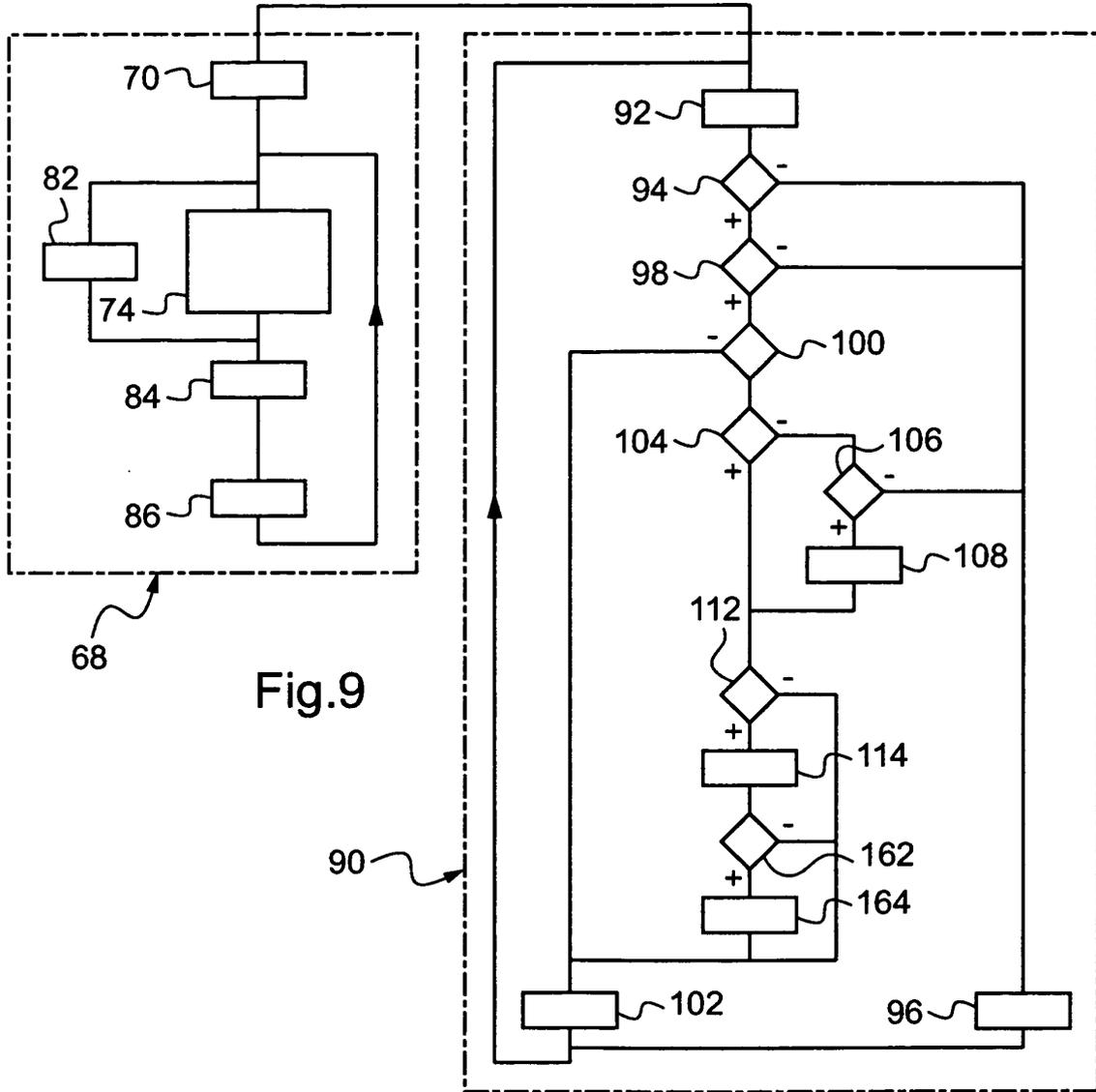


Fig.9

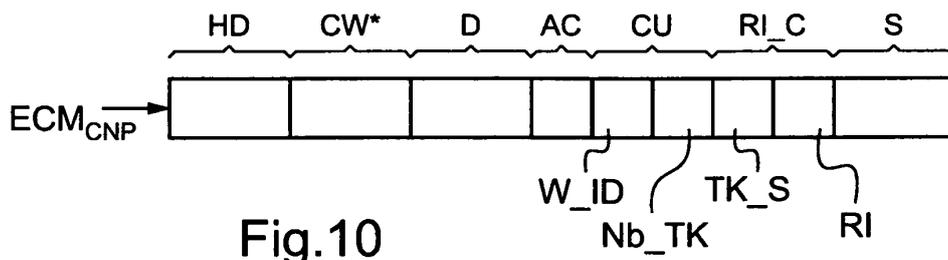


Fig.10