(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 439 001**

(51) Int. CI.:

***H04N 21/4405*** (2011.01)
***H04N 21/2662*** (2011.01)
***H04N 21/4623*** (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.11.2008 E 08853689 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2013 EP 2223524**

(54) Título: **Procedimiento de acondicionamiento y de control de acceso a contenidos en codificación jerárquica, procesador y emisor para dicho procedimiento**

(30) Prioridad:

**09.11.2007 FR 0758921**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**21.01.2014**

(73) Titular/es:

**VIACCESS (100.0%)**
**LES COLLINES DE L'ARCHE TOUR OPERA C 76, ROUTE DE LA DEMI-LUNE**
**92057 PARIS LA DÉFENSE CEDEX, FR**

(72) Inventor/es:

**DUBROEUCQ, GILLES**

(74) Agente/Representante:

**CURELL AGUILÁ, Mireia**

## DESCRIPCIÓN

Procedimiento de acondicionamiento y de control de acceso a contenidos en codificación jerárquica, procesador y emisor para dicho procedimiento.

La presente invención se refiere a un procedimiento de acondicionamiento y de control de acceso a contenidos en codificación jerárquica aleatorizados, a un procesador y a un emisor para dicho procedimiento.

Un contenido en codificación jerárquica aleatorizado es un programa multimedia codificado y aleatorizado por componentes, cuyas componentes están además organizadas jerárquicamente de manera que corresponden a niveles de completitud ordenados de dicho contenido. La noción considerada de completitud del contenido depende del contexto de aplicación del procedimiento; a continuación en la presente memoria se proporcionará una lista no limitativa de ejemplos.

Un programa multimedia codificado y aleatorizado por componentes es un flujo formado por al menos $\underline{k}$ flujos elementales de información $I_1$ a $I_k$, donde $\underline{k}$ es un número entero superior o igual a dos. Normalmente, cada flujo elemental de información $I_1$ a $I_k$ se transporta por un canal respectivo $C_1$ a $C_k$ de datos. Estos flujos elementales de información $I_1$ a $I_k$ están temporalmente sincronizados entre sí.

En un contenido en codificación jerárquica aleatorizado, estos flujos elementales, o componentes, están además jerárquicamente organizados/organizadas entre sí de la siguiente manera:

- el flujo elemental de información $I_1$ corresponde al nivel de completitud más bajo del contenido y contiene información $I_1$ de tipo vídeo o audio destinada a utilizarse por un dispositivo multimedia, tras la desaleatorización, para hacerse directamente comprensible e inteligible para un ser humano, sin que sea necesario añadir información $I_2$ a $I_k$, estando el flujo elemental de información $I_1$ aleatorizado con una palabra de control $CW_1$,

- el flujo elemental de información $I_i$, para $\underline{i}$ estrictamente superior a 1, corresponde a un nivel de completitud $\underline{i}$ superior al nivel de completitud $\underline{i}$-1 del flujo elemental de información $I_{i-1}$, y mejorándolo directamente, conteniendo el flujo elemental de información $I_i$ información $I_i$, destinada a utilizarse por el dispositivo multimedia, tras la desaleatorización, al mismo tiempo que la información $I_1$ a $I_{i-1}$ para que la combinación de información $I_1$ a $I_i$ así realizada sea directamente comprensible e inteligible para un ser humano, completando la información $I_i$ la información $I_{i-1}$ de modo que la información $I_1$ puede completarse gradualmente, en orden, por la información $I_2$ y siguientes, lo que hace posible la utilización, por un dispositivo multimedia, del programa multimedia en $\underline{k}$ niveles diferentes de completitud, aumentando el nivel de completitud a medida que aumenta el índice $\underline{i}$, estando cada flujo elemental de información $I_i$ aleatorizado con una palabra de control $CW_i$ diferente de las palabras de control $CW_j$, donde $\underline{j}$ es diferente de $\underline{i}$.

Un programa multimedia puede ser una emisión de televisión, una película o cualquier otro contenido multimedia destinado a reproducirse por un dispositivo multimedia. El dispositivo multimedia es, por ejemplo, un equipo de televisión cuando el programa multimedia es una emisión de televisión o una película. Cuando el programa multimedia está compuesto únicamente por un contenido de audio, el dispositivo multimedia puede ser una simple cadena HI-FI.

Se dice que la información es directamente comprensible e inteligible para un ser humano cuando se reproduce por un dispositivo multimedia si este ser humano puede percibir y comprender la información restituida por el dispositivo multimedia sin ayuda de dispositivos electrónicos complementarios.

El solicitante conoce unos procedimientos de control de acceso a contenidos codificados y aleatorizados por componentes, pero sin relación jerárquica, que comprenden:

- la recepción de mensajes $ECM_i$ (*Entitlement Control Message*, mensaje de control de permisos), conteniendo cada mensaje $ECM_i$ condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$,

- la transmisión al menos del mensaje $ECM_k$ a un procesador de seguridad,

- la comparación por el procesador de seguridad de las condiciones de acceso $CA_k$ contenidas en el mensaje $ECM_k$ con títulos de acceso TA previamente registrados en el procesador de seguridad, y

- el descifrado por el procesador de seguridad del primer criptograma $(CW_k)_{CEk}$ contenido en el mensaje $ECM_k$ con ayuda de la clave de explotación $CE_k$ únicamente si las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA y, en caso contrario, la interrupción del tratamiento del mensaje $ECM_k$ recibido.

Los procedimientos conocidos también comprenden:

- la comparación de cada condición de acceso $CA_i$, para $i$ estrictamente inferior a $k$, con los títulos de acceso TA previamente registrados en el procesador de seguridad, y

- el descifrado del primer criptograma $(CW_i)_{CEi}$ contenido en el mensaje $ECM_i$ únicamente si las condiciones de acceso $CA_i$ corresponden a los títulos de acceso TA previamente registrados.

Normalmente, las claves de explotación $CE_i$ y los títulos de acceso TA se actualizan regularmente, por ejemplo mensualmente, utilizando mensajes $EMM_i$ (*Entitlement Management Message*, mensaje de gestión de permisos). Para simplificar esta gestión, varias componentes pueden compartir una misma clave de explotación.

El documento de la técnica anterior WO 2004/57873 describe un aparato para tratar un flujo digital de vídeo por capas; aparato en el que pueden asociarse respectivamente ECM que comprenden palabras de control encriptadas a cada una de las capas.

A continuación en la presente memoria se utiliza la terminología clásica utilizada en el campo técnico de la difusión de programas multimedia aleatorizados hacia una multitud de receptores. Así, los términos tales como “palabra de control”, mensaje “ECM” o “EMM” no se definen con mayor detalle en la presente memoria.

Para una mejor comprensión en relación con la terminología propia de este campo técnico, puede remitirse al documento siguiente: “FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM” EBU REVIEW-TECHNICAL EUROPEAN BROADCASTING UNION. BRUSELAS, BE, n.º 266, 21 de diciembre de 1995.

Un procesador de seguridad es normalmente un calculador programable protegido. Cuando es amovible, puede presentarse en múltiples formas tales como la habitual de una tarjeta de chip, aunque también las de un *dongle* (seguro electrónico), una llave USB u otros formatos más recientes de módulos amovibles de almacenamiento.

La variedad de estos soportes y el objetivo de permitirles la utilización de los mismos contenidos de manera transparente para el usuario, hacen que hoy día sea deseable minimizar la potencia de cálculo requerida para poner en práctica los procedimientos de control de acceso a contenidos codificados y aleatorizados por componentes jerárquicas.

La invención pretende satisfacer esta necesidad proponiendo un procedimiento de control de acceso a contenidos codificados y aleatorizados por componentes jerárquicas, que requiere una potencia de cálculo reducida con respecto a los procedimientos conocidos.

Presenta por tanto como objeto un procedimiento de control de acceso denominado jerárquico, que comprende:

- la recepción y la transmisión al procesador de seguridad de segundos criptogramas $(CW_i)_{Ki}$, para $i$ comprendida entre 1 y $k$-1, obtenidos cifrando las palabras de control $CW_1$ a $CW_{k-i}$ con claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y la clave de explotación $CE_k$,

- el descifrado del primer criptograma $(CW_k)_{CEk}$ y de los segundos criptogramas $(CW_i)_{Ki}$ únicamente si las condiciones de acceso $CA_k$ recibidas en el mensaje $ECM_k$ corresponden a los títulos de acceso TA y sin comparar previamente las condiciones de acceso $CA_i$ con los títulos de acceso TA para $i$ estrictamente inferior a $k$, y en caso contrario,

- la prohibición del descifrado del primer criptograma $(CW_k)_{CEk}$ y de los segundos criptogramas $(CW_i)_{Ki}$ para $i$ comprendida entre 1 y $k$-1, si las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA.

En el procedimiento anterior, no es necesario proceder a la comparación de las condiciones de acceso $CA_i$ con los títulos de acceso TA para todos los mensajes $ECM_i$, donde $i$ es estrictamente inferior a $k$, para poder obtener las palabras de control $CW_1$ a $CW_k$. Dado que estas operaciones de comparación no son sistemáticamente necesarias para obtener las palabras de control $CW_1$ a $CW_k$, se reduce la potencia de cálculo requerida por el procesador de seguridad.

Además, cuando los segundos criptogramas $(CW_i)_{Ki}$ utilizados en la presente memoria se descifran con claves $K_i$ obtenidas a partir de la única información presente en el $ECM_k$ y la clave de explotación $CE_k$, el descifrado de las palabras de control $CW_1$ a $CW_k$ es posible aunque las claves de explotación $CE_1$ a $CE_{k-1}$ no estén actualizadas, por ejemplo. En este caso, en el procedimiento anterior, la gestión y la actualización de las claves $CE_1$ a $CE_{k-1}$ no es necesaria para obtener las palabras de control $CW_1$ a $CW_k$. Esto puede aprovecharse para simplificar la gestión de las claves de explotación $CE_i$ para $i$ comprendida entre 1 y ($k$-1) al tiempo que se mantiene la posibilidad de acceso al nivel $k$.

Las formas de realización de este procedimiento de control de acceso jerárquico pueden comprender una o varias de las características siguientes:

- el procedimiento comprende la construcción de al menos una de las claves Ki, para i comprendida entre 1 y k-1, a partir de información únicamente contenida en el mensaje $ECM_k$ de modo que si se interrumpe el tratamiento del mensaje $ECM_k$ porque las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA, resulta imposible el descifrado de al menos uno de los segundos criptogramas;

- el procedimiento comprende la construcción de al menos una de las claves $K_i$, para i comprendida entre 1 y k-1, a partir de la palabra de control $CW_k$ obtenida tras el descifrado del primer criptograma $(CW_k)_{CEk}$ únicamente cuando las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA;

- el procedimiento comprende la construcción de la clave $K_{k-1}$ a partir de la palabra de control $CW_k$ obtenida tras el descifrado del primer criptograma $(CW_k)_{CEk}$ únicamente cuando las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA, y la construcción de cada clave $K_i$, para i estrictamente inferior a k-1, a partir de la palabra de control $CW_{i+1}$ obtenida tras el descifrado del segundo criptograma $(CW_{i+1})_{Ki+1}$;

- el procedimiento comprende para cada mensaje $ECM_i$ recibido, para i comprendida entre 1 y k, como máximo el descifrado de un sólo segundo criptograma $(CW_j)_{Kj}$ para j comprendida entre 1 e i-1;

- el procedimiento comprende para el mensaje $ECM_k$, además del descifrado del primer criptograma $(CW_k)_{CEk}$, el descifrado del conjunto de los segundos criptogramas, $(CW_i)_{Ki}$ para i comprendida entre 1 y k-1, contenido en este mensaje $ECM_k$;

- cada flujo elemental de información $I_i$, para i estrictamente superior a 1, no contiene bastante de información para ser directamente comprensible e inteligible para un ser humano cuando se reproduce solo por el dispositivo multimedia;

- cada flujo elemental de información $I_1$ a $I_k$ se transporta por medio de un canal respectivo $C_1$ a $C_k$ de datos.

Las formas de realización del procedimiento de control de acceso jerárquico presentan además las ventajas siguientes:

- la construcción de la clave $K_{k-1}$ a partir de la palabra de control $CW_k$, y de cada clave $K_i$, para i estrictamente inferior a k-1, a partir de la palabra de control $CW_{i+1}$ hace que el descifrado de uno cualquiera de los segundos criptogramas sea imposible mientras que el criptograma $(CW_k)_{CEk}$ no se haya descifrado con éxito,

- colocar como máximo un segundo criptograma $(CW_i)_{Ki}$ en cada mensaje $ECM_i$ limita el tamaño de cada mensaje $ECM_i$,

- colocar el conjunto de los segundos criptogramas en el mensaje $ECM_k$ permite la desaleatorización de los flujos de información $I_1$ a $I_k$ sin que sea necesario para ello enviar al procesador de seguridad los mensajes $ECM_1$ a $ECM_{k-1}$.

La invención también presenta como objeto un procedimiento de acondicionamiento de acceso, denominado jerárquico, de un programa multimedia que comprende:

- la aleatorización de los flujos elementales de información $I_1$ a $I_k$ respectivamente con palabras de control $CW_1$ a $CW_k$, siendo cada palabra de control $CW_i$ diferente de las palabras de control $CW_j$, donde i es diferente de j,

- la construcción y la transmisión de mensajes $ECM_i$, donde i es un número entero comprendido entre 1 y k, conteniendo cada mensaje $ECM_i$ condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$,

- la construcción y la transmisión de segundos criptogramas, $(CW_i)_{Ki}$ para i comprendida entre 1 y k-1, obtenidos cifrando las mismas palabras de control $CW_1$ a $CW_{k-i}$ con claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y la clave de explotación $CE_k$.

La invención también presenta como objeto un procesador de seguridad para la puesta en práctica del procedimiento de control de acceso jerárquico anterior, comprendiendo este procesador de seguridad una memoria que almacena títulos de acceso TA previamente registrados y al menos una clave de explotación $CE_k$, siendo este procesador de seguridad apto para:

- comparar las condiciones de acceso $CA_k$ contenidas en el mensaje $ECM_k$ con los títulos de acceso TA previamente registrados en la memoria de este procesador de seguridad, y

- descifrar el primer criptograma $(CW_k)_{CEk}$ contenido en el mensaje $ECM_k$ con ayuda de la clave de explotación $CE_k$ únicamente si las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA y, en caso contrario, interrumpir el tratamiento del mensaje $ECM_k$ recibido.

Este procesador de seguridad también es apto para:

- recibir segundos criptogramas, $(CW_i)_{Ki}$ para $i$ comprendida entre 1 y $k$-1, obtenidos cifrando las palabras de control $CW_1$ a $CW_{k-1}$ con claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por información presente en el $ECM_k$ y la clave de explotación $CE_k$,

- descifrar los segundos criptogramas $(CW_i)_{Ki}$ únicamente si las condiciones de acceso $CA_k$ recibidas en el mensaje $ECM_k$ corresponden a los títulos de acceso TA y sin comparar previamente las condiciones de acceso $CA_i$ con los títulos de acceso TA para $i$ estrictamente inferior a $k$, y en caso contrario,

- prohibir el descifrado de los segundos criptogramas $(CW_i)_{Ki}$ si las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA.

La invención también presenta como objeto un emisor para la puesta en práctica del procedimiento de acondicionamiento de acceso jerárquico anterior, comprendiendo este emisor:

- un aleatorizador apropiado para aleatorizar los flujos elementales de información $I_1$ a $I_k$ respectivamente con palabras de control $CW_1$ a $CW_k$, siendo cada palabra de control $CW_i$ diferente de las palabras de control $CW_j$, donde $j$ es diferente de $i$,

- un generador de mensajes $ECM_i$, donde $i$ es un número entero comprendido entre 1 y $k$, conteniendo cada mensaje $ECM_i$ condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$.

Este emisor es apto para construir y difundir segundos criptogramas, $(CW_i)_{Ki}$ para $i$ comprendida entre 1 y $k$-1, obtenidos cifrando las mismas palabras de control $CW_1$ a $CW_{k-1}$ con claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y la clave de explotación $CE_k$.

La invención se pondrá más claramente de manifiesto a partir de la descripción siguiente, proporcionada únicamente a título de ejemplo no limitativo.

Esta descripción se realiza haciendo referencia a los dibujos, en los que:

- la figura 1 es una ilustración esquemática de un sistema de emisión y de recepción de programas multimedia aleatorizados,

- la figura 2 es una ilustración esquemática de un ejemplo de organización jerárquica de flujos elementales de información de un programa multimedia,

- la figura 3 es una ilustración esquemática de una parte de un flujo de información multiplexada emitido por un emisor del sistema de la figura 1,

- la figura 4 es una ilustración esquemática de una tabla PMT (*Program Map Table*, tabla de mapa de programa) utilizada en el sistema de la figura 1,

- la figura 5 es una ilustración esquemática de una parte de un flujo elemental de información de la figura 2,

- la figura 6 es una ilustración esquemática de un mensaje $ECM_i$ que corresponde a un paquete del flujo de información multiplexada de la figura 3,

- la figura 7 es un organigrama de un procedimiento de acondicionamiento y de control de acceso a un programa multimedia puesto en práctica en el sistema de la figura 1, y

- la figura 8 es un organigrama de otro modo de realización del procedimiento de la figura 7.

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

A continuación en esta descripción, las características y funciones ampliamente conocidas por el experto en la materia no se describen en detalle.

La figura 1 representa un sistema 2 de difusión y de recepción de programas multimedia aleatorizados. Este sistema

2 comprende un emisor 4 de programas multimedia aleatorizados conectado a una multitud de receptores por medio de una red 6 de gran distancia de transmisión de información también conocida por las siglas WAN (*Wide Area Network*, red de área extensa).

La red 6 es, por ejemplo, una red de transmisión de información por medio de satélites o una red WAN en la que se pone en práctica el protocolo IP (*Internet Protocol*, protocolo de Internet) tal como la red mundial más conocida con el nombre de “Internet”.

El emisor 4 recibe flujos elementales de información que forman un programa multimedia $P_a$ que se difundirá hacia el conjunto de los receptores en forma aleatorizada. Para ello, el emisor 4 comprende un aleatorizador 10 adecuado para aleatorizar cada flujo elemental de información $I_i$ con ayuda de una palabra de control respectiva $CW_i$ para obtener un flujo de información aleatorizada.

El emisor 4 también comprende un generador 12 de mensajes $ECM_i$ (*Entitlement Control Message*). Cada mensaje $ECM_i$ contiene un criptograma $(CW_i)_{CEi}$ de la palabra de control $CW_i$ utilizada para aleatorizar un flujo elemental de información. Más precisamente, el criptograma $(CW_i)_{CEi}$ se obtiene cifrando la palabra de control $CW_i$ con ayuda de una clave de explotación $CE_i$. Las palabras de control $CW_i$ y las claves de explotación $CE_i$ se cambian regularmente. No obstante, las palabras de control $CW_i$ se modifican con mucha más frecuencia que las claves de explotación $CE_i$. Por ejemplo, las palabras de control se modifican con una periodicidad inferior al minuto, mientras que las claves de explotación se modifican con una periodicidad superior a varias semanas y, normalmente, superior o igual a cuatro semanas.

El emisor 4 también comprende un multiplexor 14 apto para crear un flujo $F_m$ de información multiplexada que contiene entre otras cosas los flujos elementales de información aleatorizada y los mensajes $ECM_i$ generados.

El emisor 4 es apto para difundir el flujo $F_m$ hacia el conjunto de los receptores conectados a la red 6.

Para simplificar la figura 1, sólo se han representado dos receptores 20, 22 conectados a sus dispositivos multimedia respectivos 24, 26.

Por ejemplo, los dispositivos 24 y 26 son en este caso equipos de televisión.

En este caso, los receptores 20 y 22 son idénticos y sólo se describirá con mayor detalle el receptor 20.

El receptor 20 comprende:

- un decodificador 30 conectado, por ejemplo, a la red 6 por medio de una antena 32 y de una conexión 34 inalámbrica,
- una unidad 36 de desaleatorización adecuada para desaleatorizar la información aleatorizada recibida por medio de la conexión 34, y
- un procesador 38 de seguridad adecuado para descifrar las palabras de control $CW_i$ necesarias para la desaleatorización de la información aleatorizada.

Por ejemplo, el decodificador está equipado con un demultiplexor 39 adecuado para recibir el flujo $F_m$ transmitido por medio de la red 6 y para transmitir los mensajes $ECM_i$ al procesador 38 de seguridad y los flujos elementales de información aleatorizados a la unidad 36 de desaleatorización.

El procesador 38 de seguridad comprende un calculador 40 electrónico programable en el que está implementado un módulo 42 criptográfico adecuado para efectuar las operaciones de descifrado necesarias para la ejecución del procedimiento de la figura 7.

El procesador 38 de seguridad también comprende una memoria 44 conectada al calculador 40. Esta memoria 44 comprende la información necesaria para la desaleatorización del programa multimedia $P_a$. En particular, la memoria 44 comprende:

- las claves de explotación $CE_i$ necesarias para el descifrado de las palabras de control $CW_i$, y
- títulos de acceso TA que permiten autorizar y, en alternancia, prohibir el descifrado de las palabras de control $CW_i$.

Las claves de explotación $CE_i$ y los títulos de acceso TA se registran en la memoria 44 antes de la recepción del programa multimedia $P_a$. Normalmente, las claves de explotación $CE_i$ y los títulos de acceso TA se actualizan por medio de mensajes EMM (*Entitlement Management Message*), recibidos a intervalos regulares por medio de la red 6.

El procesador 38 de seguridad es apto para transmitir a la unidad 36 de desaleatorización las palabras de control descifradas $CW_i$.

La unidad 36 de desaleatorización es apta para desaleatorizar la información aleatorizada con ayuda de las palabras de control $CW_i$ transmitidas por el procesador 38 de seguridad.

El decodificador 30 también es apto para transmitir al dispositivo multimedia 24 señales de vídeo y audio obtenidas a partir del programa multimedia $P_a$ desaleatorizadas para que puedan presentarse de manera clara al usuario. Se considera que la presentación de las señales de vídeo y audio se realiza “de manera clara” si las imágenes y los sonidos presentados por el dispositivo 24 son directamente comprensibles e inteligibles por un ser humano sin pasar por medio de dispositivos electrónicos suplementarios. Más generalmente, puede hacerse una utilización, distinta de su presentación al usuario, del programa multimedia de manera clara.

La figura 2 representa un ejemplo de los diferentes flujos elementales de información que constituyen el programa multimedia $P_a$. En este caso, el programa multimedia $P_a$ se descompone en varios tipos de datos y cada tipo de datos se descompone en uno o varios flujos elementales de información.

Los diferentes flujos elementales de información de un mismo programa multimedia están sincronizados temporalmente entre sí. Además, en este caso, los diferentes flujos elementales de un mismo tipo de datos están organizados jerárquicamente entre sí.

Por ejemplo, en este caso, se distinguen tres tipos de datos, a saber, los datos de vídeo, los datos de audio y los datos alfanuméricos. En este ejemplo, se supone que los datos alfanuméricos y los datos de audio sólo están formados, respectivamente, por un único flujo elemental de información $A_1$ y $D_1$. En cambio, los datos de vídeo están formados por cinco flujos elementales de información $V_1$ a $V_5$.

Los flujos elementales de información $V_1$ a $V_5$ están organizados jerárquicamente entre sí. En este caso, la organización jerárquica de estos flujos se representa en forma de una estructura arborescente en la que:

- el flujo de información $V_1$ está al nivel jerárquico más bajo, indicado en este caso como nivel 1, y constituye el nodo raíz de esta estructura arborescente,
- el flujo de información $V_2$ depende jerárquicamente de manera directa del flujo de información $V_1$ y se encuentra por tanto en el nivel 2 de la jerarquía,
- los flujos de información $V_3$ y $V_5$ dependen jerárquicamente de manera directa del flujo de información $V_2$ y se encuentran por tanto cada uno en el nivel 3 de la jerarquía, y
- el flujo de información $V_4$ depende jerárquicamente de manera directa del flujo de información $V_3$ y se encuentra por tanto en el nivel 4 de la jerarquía.

Esta organización jerárquica define varias secuencias ordenadas por orden creciente de niveles de completitud. Por ejemplo, en este caso, esta organización jerárquica define dos secuencias crecientes de niveles de completitud, a saber $\{V_1, V_2, V_5\}$ y $\{V_1, V_2, V_3, V_4\}$. Para que el índice $\underline{i}$ utilizado a continuación en esta descripción corresponda al nivel jerárquico del flujo de información y por tanto a su nivel de completitud, en cada una de estas secuencias ordenadas, se indica como $I_i$ el flujo de información en el nivel jerárquico $\underline{i}$.

Además, para simplificar, a continuación en esta descripción, se describen en detalle el sistema y los procedimientos de acondicionamiento y de control de acceso jerárquico únicamente en el caso particular de la secuencia $\{V_1, V_2, V_3, V_4\}$ que se indica $\{I_1$ a $I_4\}$ a continuación en la presente memoria. Lo que se describe a continuación en el caso particular de la secuencia $\{V_1, V_2, V_3, V_4\}$ puede trasladarse fácilmente al caso de la secuencia $\{V_1, V_2, V_5\}$ y a todas las secuencias ordenadas por nivel de completitud creciente de flujos de información.

Cuando un flujo de información $I_i$ depende jerárquicamente, de manera directa o no, de otro flujo de información, esto significa que la información $I_i$ no puede aprovecharse independientemente de la información de nivel jerárquico inferior. A este respecto, el flujo de información $I_i$, para $\underline{i}$ superior a 1, no contiene bastante de información en sí mismo para permitir la construcción de una señal de vídeo comprensible e inteligible para un ser humano cuando se reproduce por el dispositivo multimedia 24 sin recurrir a información contenida en los flujos de información $I_1$ a $I_{i-1}$. Sólo el flujo de información $I_1$ contiene bastante información para ser directamente comprensible e inteligible para un ser humano cuando se reproduce solo por el dispositivo 24.

Dicho de otro modo, ninguno de los flujos de información $I_i$, donde $\underline{i}$ es estrictamente superior a 1, es completamente redundante con los flujos elementales de información de niveles jerárquicos inferiores.

A título de ejemplo, se supone en este caso que:

- el flujo de información $V_1$ codifica una señal de vídeo cuya resolución es suficientemente débil para permitir la visualización de este vídeo en una pantalla de un teléfono móvil sin que este teléfono móvil tenga que realizar ningún tratamiento con objeto de reducir la cantidad de información que va a visualizarse tal como, por ejemplo, una cuantificación,

- el flujo de información $V_2$ es adecuado para completar el flujo de información $V_1$ para obtener imágenes en definición simple, es decir, por ejemplo, 625 líneas por imagen y en el formato 4/3,

- el flujo de información $V_5$ completa la información $V_2$ para pasar de la definición simple a la alta definición (más de 1000 líneas por imagen) al tiempo que se mantiene un formato de imagen de 4/3,

- el flujo de información $V_3$ completa el flujo de información $V_2$ para pasar de un formato de visualización 4/3 a un formato de visualización 16/9 al tiempo que se mantiene la definición simple, y

- el flujo de información $V_4$ completa el flujo de información $V_3$ para pasar del formato de visualización 16/9 en definición simple al formato de visualización 16/9 en alta definición.

Los formatos 4/3 y 16/9 así como las resoluciones de imágenes “definición simple” y “alta definición” están definidos en las normas sobre codificación de señales de vídeo.

Se observará que las secuencias $\{V_1, V_2, V_5\}$ y $\{V_1, V_2, V_3, V_4\}$ están organizadas por calidad de imagen creciente. Así, el flujo de información $V_1$ transporta la señal de vídeo cuya calidad es la más mediocre y que, por consiguiente, es susceptible de visualizarse en cualquier dispositivo multimedia.

En este caso, cada flujo elemental de información $V_1$ para $\underline{i}$ comprendida entre 1 y 5 está aleatorizado con ayuda de una palabra de control $CW_i$ diferente de las palabras de control utilizadas para aleatorizar los demás flujos elementales de información $V_j$, donde $\underline{j}$ es diferente de $\underline{i}$.

Así, debido a la organización jerárquica representada en la figura 2, es posible autorizar selectivamente la desaleatorización de los flujos elementales de información $I_1$ a $I_i$ al tiempo que se prohíbe la desaleatorización de los flujos de información $I_{i+1}$ a $I_4$. No obstante, ha de indicarse que dado que el flujo de información elemental $I_i$ no contiene toda la información $I_1$ a $I_{i-1}$, la autorización de desaleatorizar el flujo elemental de información $I_i$ debe ir acompañada necesariamente por la autorización de desaleatorizar los flujos de información $I_1$ a $I_{i-1}$ para permitir presentar un programa multimedia comprensible e inteligible por el usuario.

Cada palabra de control $CW_i$ se comunica por el emisor 4 al receptor por medio de un mensaje $ECM_i$ que contiene un criptograma $(CW_i)_{CEi}$ de la palabra de control $CW_i$. Así, en esta forma de realización, existen tantos mensajes $ECM_i$ como flujos elementales de información aleatorizada se hayan transmitido.

Cada flujo elemental de información $I_i$ se transmite en su propio canal elemental de datos $C_i$ del emisor 4 hacia los receptores. Cada canal elemental de datos comprende un único flujo elemental de información. A continuación en esta descripción, se indica $C_i$ el canal de datos utilizado para transmitir el flujo elemental de información $I_i$.

En este caso, al no estar los flujos elementales de información de audio y alfanumérica organizados jerárquicamente de manera que formen una secuencia creciente de niveles de completitud, su transmisión se considerará como convencional y por tanto no se describe en detalle a continuación.

La figura 3 representa un ejemplo de organización del flujo de información multiplexada $F_m$ transmitido por el emisor 4. Este ejemplo está inspirado en el formato de los flujos de información multiplexada según las normas MPEG2-TS y DVB y algunas de las notaciones utilizadas corresponden a las de estas normas MPEG2 y DVB. No obstante, el lector debe recordar que el ejemplo de organización del flujo $F_m$ dado con respecto a la figura 3 sólo se proporciona a modo de ilustración y que son posibles muchas otras organizaciones para multiplexar en un mismo flujo de información diferentes flujos elementales de información $I_i$ organizados de manera jerárquica. Este ejemplo es trasladable directamente en el marco de los protocolos propios de TCP-IP tales como RTP (*Real Time Protocol*, protocolo en tiempo real) o UDP para la difusión de los flujos de información tanto en unidifusión como en multidifusión, la utilización de Ismacryp para el cifrado de los contenidos y la utilización por ejemplo de SDP (*Session Description Protocol*, protocolo de descripción de sesión) para la descripción de los flujos elementales que forman el programa multimedia según sus direcciones en el sentido de los protocolos citados.

La figura 3 representa solamente las partes del flujo de información multiplexada pertinentes para la descripción siguiente.

En este caso, el flujo de información está multiplexado temporalmente. Este flujo de información multiplexada está por tanto constituido por una sucesión temporal de paquetes. Cada paquete comprende un identificador PID de vía o

de canal. En la figura 3, los valores indicados en hexadecimal corresponden al valor del identificador PID de cada uno de los paquetes representados. La sucesión temporal de los paquetes que presentan el mismo identificador PID forma un canal elemental de datos. A título de ejemplo, todos los paquetes del flujo $F_m$ presentan la misma longitud y comprenden, por ejemplo, 188 octetos.

El identificador PID0x00 identifica un canal elemental reservado para la transmisión de una tabla PAT (*Program Association Table*, tabla de asociación de programa). Esta tabla PAT asocia a cada programa multimedia difundido, el identificador PID del canal elemental utilizado para transmitir una tabla PMT (*Program Map Table*) asociada a este programa multimedia. Por ejemplo, en el flujo $F_m$, la tabla PAT asocia el identificador PID0x80 al programa $P_a$.

El canal elemental identificado por el identificador PID0x80 se utiliza únicamente para transmitir la tabla PMT. La tabla PMT indica para cada tipo de datos que forman el programa multimedia cuáles son los identificadores PID de los canales elementales en los que se transmiten los flujos de información correspondientes. La tabla PMT también indica en qué canales elementales se transmiten los mensajes $ECM_i$ asociados a cada uno de los flujos elementales de información.

La figura 4 representa un ejemplo de tabla PMT susceptible de utilizarse durante la transmisión del programa multimedia $P_a$. Esta tabla comprende una primera columna T-Id. La columna T-Id comprende el identificador del tipo de datos. Una segunda columna PID indica el valor del identificador PID de los canales elementales utilizados para transmitir los datos del tipo considerado. Por ejemplo, en la figura 4, la columna T-Id comprende cuatro identificadores V, A, D y ECM, que corresponden respectivamente a los tipos de datos siguientes: datos de vídeo, datos de audio, datos alfanuméricos y mensajes ECM. La columna PID asocia:

- los valores 0x81 a 0X85 al tipo de datos de vídeo,
- el valor 0x90 al tipo de datos de audio,
- el valor 0x100 al tipo de datos alfanuméricos, y
- los valores 0x111 a 0x115 a los mensajes ECM.

Más precisamente, la tabla PMT de la figura 4 indica que los canales elementales $C_1$ a $C_5$ corresponden, respectivamente, a los identificadores PIDOx81 a 0x85. Asimismo, los canales elementales utilizados para transmitir los mensajes $ECM_1$ a $ECM_5$ corresponden, respectivamente, a los PID 0x111 a 0x115.

Se indica que dado que los datos de vídeo están organizados en una jerarquía de varios flujos elementales de información $V_1$ a $V_5$, el identificador $C_i$ de tipo de datos vídeo está asociado a tantos valores de identificadores PID como flujos elementales de información vídeo $V_1$ a $V_5$. De manera similar, dado que los flujos de información elementales $V_1$ a $V_5$ están aleatorizados con palabras de control respectivas $CW_1$ a $CW_5$, el identificador del tipo de datos ECM está asociado a tantos valores de identificadores PID como flujos elementales de información aleatorizada con palabras de control diferentes.

Cada paquete del flujo $F_m$ también comprende un número de orden que define la posición temporal de este paquete con respecto a los demás paquetes recibidos por medio del mismo canal. Además, la posición de cada paquete en el flujo $F_m$ con respecto a los demás paquetes de los demás canales define la relación temporal que existe entre la información transmitida en cada uno de estos paquetes. Por ejemplo, en la figura 3, los paquetes de los canales $C_1$ a $C_4$ que se encuentran unos al lado de otros en el flujo $F_m$ transportan la información $I_1$ a $I_4$ destinada a reproducirse al mismo tiempo por el dispositivo 24. Así, mediante esto, los flujos elementales de información $I_1$ a $I_4$ se sincronizan temporalmente entre sí.

En la figura 3, los canales elementales utilizados para transmitir los flujos de información de audio $A_1$ y alfanumérica $D_1$ se indican como $CA_1$ y $CD_1$.

Cada canal elemental utilizado para transmitir el mensaje $ECM_i$ se indica $CECM_i$. La posición de los diferentes paquetes de los canales $CA_1$, $CD_1$ y $CECM_i$ con respecto a los paquetes de los canales $C_i$ en el flujo $F_m$ define una relación temporal entre la información de audio $A_1$, alfanumérica $D_1$, los mensajes $ECM_i$ y la información $I_i$. Así, es posible determinar, en cada instante, cuáles son los mensajes $ECM_i$ que deben utilizarse para desaleatorizar la información $I_i$ y la información de audio $A_1$, alfanumérica $D_1$ que deben reproducirse al mismo tiempo.

Los paquetes de cada canal elemental se suceden, por ejemplo, a intervalos de tiempo regulares en el flujo $F_m$.

La figura 5 representa un ejemplo de la arquitectura de un paquete del canal $C_i$. Este paquete comprende el identificador PID y la información $I_i$ aleatorizada con ayuda de la palabra de control $CW_i$. Además, en este caso, cada paquete comprende un identificador $Id\text{-}I_{i-1}$ que indica la posición jerárquica de la información $I_i$ con respecto al resto de información $I_j$, donde j es diferente de i. Por ejemplo, el identificador $Id\text{-}I_{i-1}$ es igual al identificador PID del canal $C_{i-1}$ utilizado para transmitir el flujo elemental de información $I_{i-1}$ que completa directamente el flujo elemental de información $I_i$. Cuando el índice i es igual a 1, es decir la información $I_i$ está en la parte baja de la jerarquía, el identificador $Id\text{-}I_{i-1}$ adopta un valor predeterminado tal como, por ejemplo, cero. Así, gracias a estos identificadores $Id\text{-}I_{i-1}$ cada receptor puede reconstruir la jerarquía de los flujos elementales de información $I_i$ representada en la

figura 2.

La figura 6 representa un ejemplo de arquitectura para un paquete del canal $CECM_i$. Este paquete comprende el identificador PID del canal $CECM_i$ así como los diferentes campos que forman el mensaje $ECM_i$. En este caso, sólo se representan los campos del mensaje $ECM_i$ necesarios para la comprensión de lo que sigue de la descripción. El mensaje $ECM_i$ comprende:

- un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con ayuda de la clave de explotación $CE_i$,
- condiciones de acceso $CA_i$ destinadas a compararse con los títulos de acceso TA previamente registrados en el procesador de seguridad para autorizar o por el contrario prohibir el acceso al programa multimedia por el receptor, y
- un segundo criptograma $(CW_{i-1})_{CWi}$ obtenido cifrando la palabra de control $CW_{i-1}$ con ayuda de la palabra de control $CW_i$.

El criptograma $(CW_{i-1})_{CWi}$ existe únicamente en los mensajes $ECM_i$, donde i es estrictamente superior a 1.

El funcionamiento del sistema 2 va a describirse a continuación con respecto al procedimiento de la figura 7.

El procedimiento de la figura 7 comprende una fase 70 de acondicionamiento del acceso a los flujos elementales de información $I_1$ a $I_4$ y de emisión de estos flujos, seguida por una fase 72 de recepción y de control del acceso, por cada receptor, a los flujos elementales de información $I_1$ a $I_4$ transmitidos.

Durante la fase 70, la información $I_j$ se trata por orden creciente de índice i.

La fase 70 comienza con una etapa 80 de recepción del paquete de información $I_i$ que debe transmitirse. A continuación, durante una etapa 82, el emisor 4 genera una palabra de control $CW_i$.

Durante una etapa 84, el aleatorizador 10 aleatoriza el paquete de información $I_i$ con ayuda de la palabra de control $CW_i$.

Durante una etapa 86, el generador 12 cifra la palabra de control $CW_i$ con la clave de explotación $CE_i$ para obtener el criptograma $(CW_i)_{CEi}$.

Si el índice i es estrictamente superior a 1, durante una etapa 88, el generador 12 también cifra la palabra de control $CW_{i-1}$ con una clave $K_{i-1}$ de manera que se obtiene un segundo criptograma $(CW_{i-1})_{Ki-1}$ de la palabra de control $CW_{i-1}$. La clave $K_{i-1}$ es independiente de las claves de explotación $CE_1$ a $CE_{i-2}$. Preferiblemente, la clave $K_{i-1}$ se obtiene a partir de información contenida en el mensaje $ECM_i$ en proceso de generación. Por ejemplo, en este caso, la clave $K_{i-1}$ se elige igual a la palabra de control $CW_i$. El segundo criptograma $(CW_{i-1})_{Ki-1}$ se indica por tanto a continuación como $(CW_{i-1})_{CWi}$.

Si el índice i es igual a 1, se inscribe el valor 0x00 en el campo previsto para recibir el criptograma $(CW_{i-1})_{CWi}$.

Durante una etapa 90, el generador 12 genera el mensaje $ECM_i$. Este mensaje $ECM_i$ contiene por tanto, en particular, las condiciones de acceso $CA_i$, el criptograma $(CW_i)_{CEi}$ y el criptograma $(CW_{i-1})_{CWi}$. Las operaciones 80 a 90 se repiten para i de 1 a 4. Estas etapas también se ejecutan para aleatorizar la información $V_5$, $A_1$ y $D_1$ y para generar los mensajes ECM correspondientes.

A continuación, durante una etapa 92, el multiplexor 14 multiplexa los diferentes paquetes de información aleatorizados, y los mensajes $ECM_i$ para crear el flujo $F_m$ de información multiplexada descrito con respecto a la figura 3.

Durante una etapa 94, el flujo $F_m$ se difunde hacia el conjunto de los receptores del sistema 2 por medio de la red 6.

La fase 72 comienza con una etapa 100 de recepción del flujo $F_m$ difundido por el emisor 4.

A continuación, durante una etapa 102, el demultiplexor 39 demultiplexa los diferentes canales elementales del flujo $F_m$. Durante una etapa 104, el demultiplexor 39 transmite los flujos elementales de información $I_1$ a $I_4$, $V_5$, $A_1$ y $D_1$ a la unidad 36 de desaleatorización. En paralelo, durante una etapa 106, el demultiplexor 39 transmite los mensajes $ECM_i$ contenidos en los canales $CECM_i$ al procesador 38 de seguridad.

A continuación, en orden decreciente de los índices i, durante una etapa 108, el procesador 38 de seguridad compara las condiciones de acceso $CA_i$ con los títulos de acceso TA previamente registrados. Por tanto, en el ejemplo descrito en la presente memoria, el procesador 38 de seguridad comienza comparando las condiciones de

acceso $CA_4$ con los títulos de acceso TA.

Si las condiciones de acceso $CA_4$ no corresponden a los títulos de acceso TA, entonces, durante una etapa 110, el procesador 38 de seguridad hace que la desaleatorización de la información $I_4$ sea imposible. Por ejemplo, durante la etapa 110, el procesador 38 de seguridad impide el descifrado del criptograma $(CW_4)_{CE4}$. Tras la etapa 110, el procedimiento vuelve a la etapa 108. Durante la nueva generación de la etapa 108, el procesador 38 de seguridad repite las mismas comparaciones que antes pero para el índice i-1. Así, durante la nueva iteración de la etapa 108, el procesador 38 de seguridad compara las condiciones $CA_3$ con los títulos de acceso TA.

Mientras que ninguna de las condiciones de acceso recibidas $CA_i$ corresponda a los títulos de acceso TA, se repite la etapa 108 hasta comparar las condiciones de acceso $CA_1$ con los títulos de acceso TA. Si las condiciones de acceso $CA_1$ no corresponden a los títulos de acceso TA, entonces se ejecuta la etapa 110 y después se interrumpe la fase 72. En efecto, esto significa que este receptor no está autorizado para desaleatorizar el programa multimedia $P_a$.

Si, durante la etapa 108, el procesador 38 de seguridad establece que las condiciones de acceso $CA_k$ recibidas corresponden a los títulos de acceso TA previamente registrados en la memoria 44, entonces, el procesador 38 de seguridad procede a una etapa 114 de descifrado del criptograma $(CW_k)_{CEk}$ con ayuda de la clave de explotación $CE_k$ previamente registrada en su memoria 44. Se indica por tanto k como el mayor valor del índice i para el que las condiciones de acceso $CA_i$ corresponden a los títulos de acceso TA.

A continuación, durante una etapa 116, si k es estrictamente superior a 1, el procesador 38 de seguridad descifra el segundo criptograma $(CW_{k-1})_{Kk-1}$ contenido en el mensaje $ECM_k$ para obtener una palabra de control $CW_{k-1}$. Dado el caso, en esta forma de realización, durante la etapa 116, el procesador 38 de seguridad descifra el criptograma $(CW_{k-1})_{CWk}$ con ayuda de la palabra de control $CW_k$ obtenida tras la etapa 114.

A continuación, durante una etapa 118, los segundos criptogramas $(CW_1)_{K1}$ a $(CW_{k2})_{Kk-2}$ contenidos, respectivamente, en los mensajes $ECM_2$ a $ECM_{k-1}$ se descifran poco a poco en orden decreciente de sus índices.

Una vez obtenido el conjunto de las palabras de control $CW_1$ a $CW_k$, éstas se transmiten, durante una etapa 120, a la unidad 36 de desaleatorización.

Durante una etapa 122, la unidad 36 de desaleatorización desaleatoriza los flujos elementales de información $I_1$ a $I_k$ con ayuda, respectivamente, de las palabras de control $CW_1$ a $CW_k$.

Los flujos elementales de información $I_1$ a $I_k$ desaleatorizados por la unidad 36 de desaleatorización se transmiten entonces al decodificador 30 durante una etapa 124.

En respuesta, durante una etapa 126, el decodificador 30 combine entre sí los flujos de información desaleatorizados $I_1$ a $I_k$ para producir la señal de vídeo construida con ayuda de la información contenida en cada uno de estos flujos elementales de información desaleatorizados. Por último, durante una etapa 128, el dispositivo multimedia 24 presenta en forma de imágenes directamente comprensibles e inteligibles por un ser humano, la señal de vídeo recibida del decodificador 30.

Las etapas 80 a 128 se repiten en bucle.

Se apreciará que durante la fase 72, la obtención de las palabras de control $CW_1$ a $CW_{k-i}$ no requiere la comparación de las condiciones de acceso $CA_1$ a $CA_{k-1}$ con los títulos de acceso previamente registrados TA.

La figura 8 representa otra forma de realización del procedimiento de la figura 7. El procedimiento de la figura 8 es idéntico al procedimiento de la figura 7 a excepción de que:

- la etapa 88 se sustituye por una etapa 140, durante la cual la palabra de control $CW_{i-1}$ se cifra con ayuda de la palabra de control $CW_i$ y las palabras de control $CW_1$ a $CW_{i-2}$ se cifran con ayuda, respectivamente, de las palabras de control $CW_2$ a $CW_{i-1}$,

- la etapa 90 se sustituye por una etapa 142 durante la cual el mensaje $ECM_i$ generado comprende además del criptograma $(CW_{i-1})_{CWi}$ los criptogramas $(CW_1)_{CW2}$ a $(CW_{i-2})_{CWi-1}$, y

- las etapas 116 y 118 se sustituyen por una etapa 146 de descifrado poco a poco del conjunto de los segundos criptogramas $(CW_{i-1})_{CWi}$ contenidos en el mismo mensaje $ECM_i$ de manera que se obtienen las palabras de control $CW_1$ a $CW_{i-1}$.

En el procedimiento de la figura 8, el conjunto de los segundos criptogramas necesarios para la visualización del programa multimedia con un nivel de completitud dado están contenidos en el mismo mensaje $ECM_i$. Por tanto ya no es necesario transmitir al procesador 38 de seguridad los mensajes $ECM_1$ a $ECM_{i-1}$.

Son posibles muchos otras formas de realización. Por ejemplo, la organización jerárquica de los flujos elementales de información no está limitada a cuatro niveles de completitud. De hecho, lo que se ha descrito anteriormente se aplica desde el momento en que existen más de dos niveles de completitud. No obstante, preferiblemente, los procedimientos de acondicionamiento y de control de acceso descritos anteriormente se aplican al caso en el que existe al menos una secuencia de tres niveles sucesivos de completitud.

Lo que se ha descrito anteriormente también se aplica a otros tipos de datos distintos de los datos de vídeo. En particular, es posible adaptar los procedimientos de las figuras 7 y 8 a los casos de datos de audio o alfanuméricos o a otros tipos de datos a partir del momento en que éstos se presenten en forma de una o varias secuencias de flujos elementales ordenados por nivel de completitud creciente. Lo que se ha descrito anteriormente también se aplica a los casos en los que diversos programas multimedia aleatorizados jerárquicamente están multiplexados en el mismo flujo de información.

Las claves $K_i$ utilizadas para obtener los segundos criptogramas $(CW_i)_{Ki}$ también pueden ser todas idénticas y, por ejemplo, tomarse iguales ya sea a la clave de explotación $CE_k$, ya sea a la palabra de control $CW_k$.

Se han descrito el acondicionamiento y el control de acceso jerárquicos en el caso particular en el que los mensajes $ECM_i$ se transmiten por canales elementales diferentes. No obstante, como variante, el conjunto de los mensajes $ECM_i$ pueden transmitirse a los receptores por medio de un único y mismo canal elemental dedicado a esta utilización.

Se ha descrito en la presente memoria la organización jerárquica del programa multimedia en el caso particular en el que la calidad de la señal de vídeo obtenida aumenta a medida que aumenta el índice i. No obstante, la organización jerárquica del programa multimedia puede basarse en otros criterios. Por ejemplo, cada flujo de información complementaria puede corresponder a un objeto o un personaje a añadir en una escena de vídeo con respecto al nivel jerárquico inferior. Puede pensarse, por ejemplo, en el ejemplo siguiente en el que el flujo elemental de información $I_1$ codifica únicamente la información necesaria para la restitución de un único personaje. El flujo elemental de información complementaria $I_2$ codifica únicamente el fondo de la escena multimedia.

Por último, el flujo elemental de información complementaria $I_3$ contiene la información necesaria para añadir un segundo personaje o para añadir un cuadro que contiene información adicional en la escena multimedia.

**REIVINDICACIONES**

1. Procedimiento de control de acceso jerárquico a un programa multimedia, estando este programa multimedia formado por al menos k flujos elementales de información $I_1$ a $I_k$, en el que k es estrictamente superior a 1, estando estos flujos elementales de información $I_1$ a $I_k$ temporalmente sincronizados entre sí y jerárquicamente organizados entre sí de la manera siguiente, de manera que corresponden a niveles de completitud ordenados de dicho programa multimedia:

- correspondiendo el flujo elemental de información $I_1$ al nivel de completitud más bajo y conteniendo información $I_1$ de tipo vídeo o audio destinada a utilizarse por un dispositivo multimedia, tras la desaleatorización, para hacerla directamente comprensible e inteligible para un ser humano, sin que sea necesario añadir a la misma información $I_2$ a $I_k$, estando el flujo elemental de información $I_1$ aleatorizado con una palabra de control $CW_1$,

- estando el flujo elemental de información $I_i$, para i comprendida entre 2 y k, a un nivel de completitud i superior al nivel de completitud i-1 del flujo elemental de información $I_{i-1}$, conteniendo el flujo elemental de información $I_i$ información $I_i$, del mismo tipo que la información $I_{i-1}$, destinada a utilizarse por el dispositivo multimedia, tras la desaleatorización, al mismo tiempo que la información $I_1$ a $I_{i-1}$ para que la combinación de la información $I_1$ a $I_i$ así realizada sea directamente comprensible e inteligible para un ser humano, completando la información $I_i$ la información $I_{i-1}$ de modo que la información $I_1$ puede completarse gradualmente, en orden, por la información $I_2$ y siguientes, lo que hace posible la utilización por el dispositivo multimedia del programa multimedia en k niveles diferentes de completitud, aumentando el nivel de completitud a medida que aumenta el índice i, estando cada flujo elemental de información $I_i$ aleatorizado con una palabra de control $CW_i$ diferente de las palabras de control $CW_j$, en el que j es diferente de i,

comprendiendo este procedimiento:

- recibir (100) mensajes $ECM_i$ (mensaje de control de permisos), en el que i es un número comprendido entre 1 y k, conteniendo cada mensaje $ECM_i$ unas condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$,

- transmitir (106), al menos el mensaje $ECM_k$, a un procesador de seguridad,

- comparar (108), por el procesador de seguridad, las condiciones de acceso $CA_k$ contenidas en el mensaje $ECM_k$, con títulos de acceso TA previamente registrados en el procesador de seguridad, y

- descifrar (114), por el procesador de seguridad, el primer criptograma $(CW_k)_{CEk}$ contenido en el mensaje $ECM_k$ con ayuda de la clave de explotación $CE_k$, únicamente si las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA, y, en caso contrario, interrumpir el tratamiento del mensaje $ECM_k$ recibido,

caracterizado porque este procedimiento comprende:

- recibir (100) y transmitir (106) al procesador de seguridad los segundos criptogramas, $(CW_i)_{Ki}$ para i comprendida entre 1 y k-1, obtenidos cifrando las palabras de control $CW_1$ a $CW_{k-1}$ con claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y por la clave de explotación $CE_k$,

- descifrar (116, 118) los segundos criptogramas $(CW_i)_{Ki}$ únicamente si las condiciones de acceso $CA_k$ recibidas en el mensaje $ECM_k$ corresponden a los títulos de acceso TA, y sin comparar previamente las condiciones de acceso $CA_i$ con los títulos de acceso TA para i comprendida entre 1 y k-1, y, en caso contrario,

- prohibir (110) el descifrado de los segundos criptogramas $(CW_i)_{Ki}$ si las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA.

2. Procedimiento según la reivindicación 1, en el que el procedimiento comprende construir (116) al menos una de las claves $K_i$, para i comprendida entre 1 y k-1, a partir de información únicamente contenida en el mensaje $ECM_k$, de modo que si el tratamiento del mensaje $ECM_k$ se interrumpe porque las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA, resulta imposible el descifrado de al menos uno de los segundos criptogramas.

3. Procedimiento según la reivindicación 2, en el que el procedimiento comprende construir (116) al menos una de las claves $K_i$ a partir de la palabra de control $CW_k$ obtenida tras el descifrado del primer criptograma $(CW_k)_{CEk}$ únicamente cuando las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA.

4. Procedimiento según la reivindicación 3, en el que el procedimiento comprende construir (116) la clave $K_{k-1}$ a partir de la palabra de control $CW_k$ obtenida tras el descifrado del primer criptograma $(CW_k)_{CEk}$ únicamente cuando las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA y construir (118) cada clave $K_i$, para i estrictamente inferior a k-1, a partir de la palabra de control $CW_{i+1}$ obtenida tras el descifrado del segundo criptograma $(CW_{i+1})_{Ki+1}$.

5. Procedimiento según la reivindicación 4, en el que cada mensaje $ECM_i$ recibido para i comprendida entre 2 y k comprende el segundo criptograma $(CW_{i-1})_{Ki-1}$, comprendiendo el procedimiento descifrar (118) poco a poco los segundos criptogramas $(CW_j)_{Kj}$, para j comprendida entre k-2 y 1, contenidos respectivamente en los mensajes $ECM_{k-1}$ a $ECM_2$.

6. Procedimiento según la reivindicación 4, en el que el mensaje $ECM_k$ comprende además los segundos criptogramas $(CW_i)_{Ki}$ para i comprendida entre 1 y k-1, comprendiendo el procedimiento para el mensaje $ECM_k$, además del descifrado del primer criptograma $(CW_k)_{CEk}$, descifrar (146) poco a poco el conjunto de los segundos criptogramas contenidos en este mensaje $ECM_k$.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que cada flujo elemental de información $I_i$, para i estrictamente superior a 1, no contiene bastante información para ser directamente comprensible e inteligible para un ser humano cuando se reproduce solo por el dispositivo multimedia.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que cada flujo elemental de información $I_1$ a $I_k$ se transporta por medio de un canal respectivo $C_1$ a $C_k$ de datos.

9. Procedimiento de acondicionamiento de acceso jerárquico a un programa multimedia, estando este programa multimedia formado por al menos k flujos elementales de información $I_1$ a $I_k$, en el que k es estrictamente superior a 1, estando estos flujos elementales de información $I_1$ a $I_k$ temporalmente sincronizados entre sí y jerárquicamente organizados entre sí de la manera siguiente, de manera que corresponden a niveles de completitud ordenados de dicho programa multimedia:

- correspondiendo el flujo elemental de información $I_1$ al nivel de completitud más bajo y conteniendo información $I_1$ de tipo vídeo o audio destinada a utilizarse por un dispositivo multimedia, tras la desaleatorización, para hacerse directamente comprensible e inteligible para un ser humano, sin que sea necesario añadir a la misma información $I_2$ a $I_k$,

- estando el flujo elemental de información $I_i$, para i comprendida entre 2 y k, a un nivel de completitud i superior al nivel de completitud i-1 del flujo elemental de información $I_{i-1}$, y mejorándolo directamente, conteniendo el flujo elemental de información $I_i$ información $I_i$ del mismo tipo que la información $I_{i-1}$, destinada a utilizarse por el dispositivo multimedia, tras la desaleatorización, con la información $I_1$ a $I_{i-1}$ para que la combinación de la información $I_1$ a $I_i$ así realizada sea directamente comprensible e inteligible para un ser humano, completando la información $I_i$ la información $I_{i-1}$ de modo que la información $I_1$ puede completarse gradualmente, en orden, por la información $I_2$ y siguientes, lo que hace posible la utilización por el dispositivo multimedia del programa multimedia en k niveles diferentes de completitud, aumentando el nivel de completitud a medida que aumenta el índice i,

comprendiendo este procedimiento:

- aleatorizar los flujos elementales de información $I_1$ a $I_k$ respectivamente con las palabras de control $CW_1$ a $CW_k$, siendo cada palabra de control $CW_i$ diferente de las palabras de control $CW_j$, en el que j es diferente de i,

- construir y transmitir los mensajes $ECM_i$, en el que i es un número entero comprendido entre 1 y k, conteniendo cada mensaje $ECM_i$ unas condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$,

caracterizado porque este procedimiento comprende:

- construir y transmitir los segundos criptogramas, $(CW_i)_{Ki}$ para i comprendida entre 1 y k-1, obtenidos cifrando las mismas palabras de control $CW_1$ a $CW_{k-1}$ con las claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y por la clave de explotación $CE_k$.

10. Procesador de seguridad para la puesta en práctica de un procedimiento de control de acceso jerárquico según cualquiera de las reivindicaciones 1 a 6, comprendiendo este procesador de seguridad una memoria que almacena los títulos de acceso TA previamente registrados y al menos una clave de explotación $CE_k$, así como:

- unos medios para comparar las condiciones de acceso $CA_k$ contenidas en un mensaje $ECM_k$ recibido con títulos de acceso TA previamente registrados en la memoria de este procesador de seguridad, y

- unos medios para descifrar el primer criptograma $(CW_k)_{CEk}$ contenido en el mensaje $ECM_k$ con ayuda de la clave de explotación $CE_k$ únicamente si las condiciones de acceso $CA_k$ corresponden a los títulos de acceso TA y, en caso contrario, para interrumpir el tratamiento del mensaje $ECM_k$,

caracterizado porque el procesador de seguridad comprende asimismo:

- unos medios para recibir (100) los segundos criptogramas, $(CW_i)_{Ki}$ para $i$ comprendida entre 1 y $k$-1, obtenidos cifrando las palabras de control $CW_1$ a $CW_{k-1}$ con las claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por información presente en el mensaje $ECM_k$ y por la clave de explotación $CE_k$,

- unos medios para descifrar (116, 118) los segundos criptogramas $(CW_i)_{Ki}$ únicamente si las condiciones de acceso $CA_k$ recibidas en el mensaje $ECM_k$ corresponden a los títulos de acceso TA, y sin comparar previamente las condiciones de acceso $CA_i$ con los títulos de acceso TA para $i$ estrictamente inferior a $k$, y, en caso contrario,

- unos medios para prohibir (110) el descifrado de los segundos criptogramas $(CW_i)_{Ki}$ si las condiciones de acceso $CA_k$ no corresponden a los títulos de acceso TA.

11. Emisor de programas multimedia aleatorizados jerárquicamente, estando estos programas multimedia formados por al menos $k$ flujos elementales de información $I_1$ a $I_k$, en el que $k$ es estrictamente superior a 1, estando estos flujos elementales de información $I_1$ a $I_k$ temporalmente sincronizados entre sí y jerárquicamente organizados entre sí de la manera siguiente, de manera que corresponden a niveles de completitud ordenados de dichos programas multimedia:

- correspondiendo el flujo elemental de información $I_1$ al nivel de completitud más bajo y contiene información $I_1$ de tipo vídeo o audio destinada a utilizarse por un dispositivo multimedia, tras la desaleatorización, para hacerla directamente comprensible e inteligible para un ser humano, sin que sea necesario añadir a la misma información $I_2$ a $I_k$, estando el flujo elemental de información $I_1$ aleatorizado con una palabra de control $CW_1$,

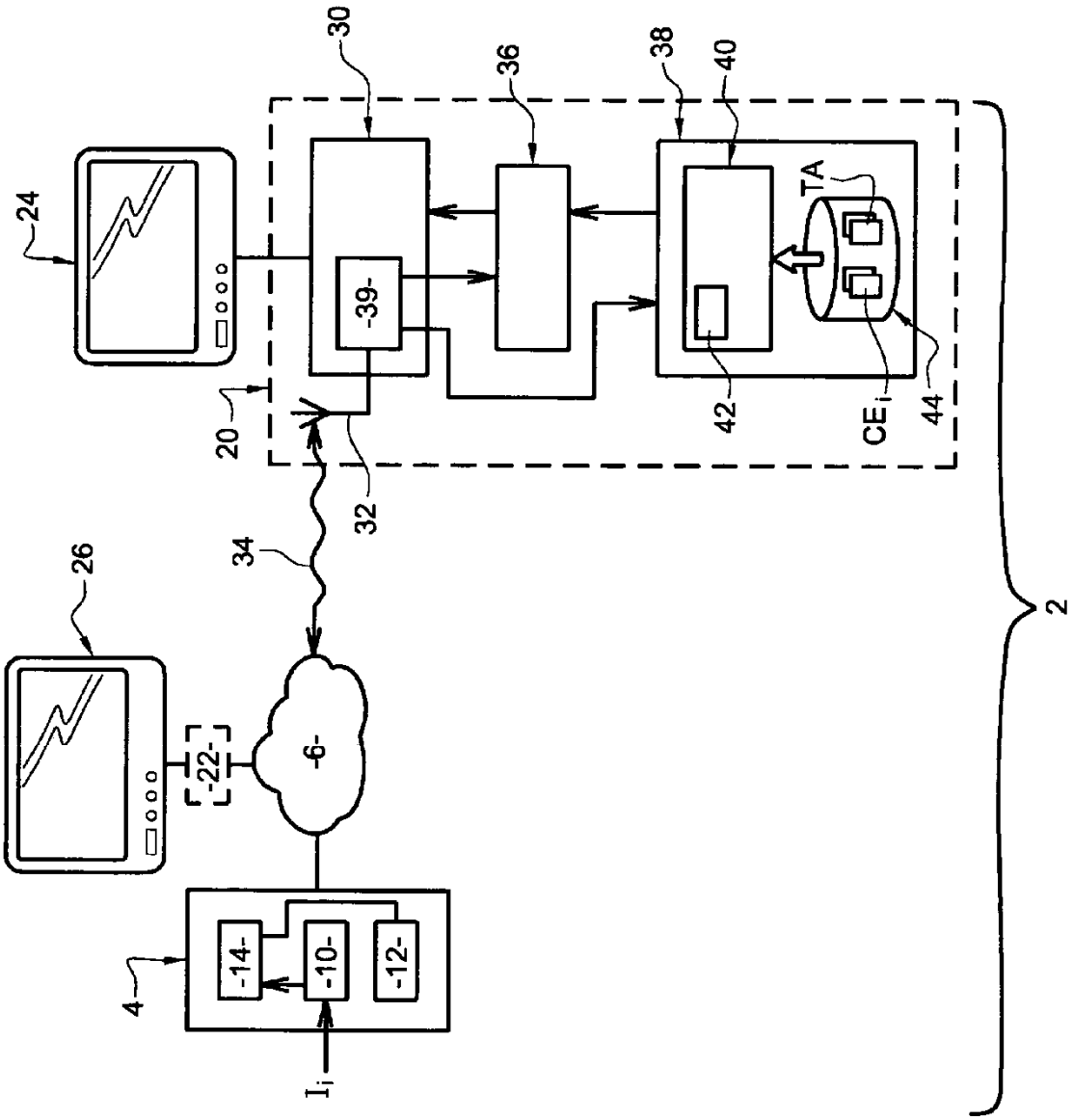
- estando el flujo elemental de información $I_i$, para $i$ comprendida entre 2 y $k$, a un nivel de completitud $i$ superior al nivel de completitud $i$-1 del flujo elemental de información $I_{i-1}$, y mejorándolo directamente, conteniendo el flujo elemental de información $I_i$ información $I_i$, del mismo tipo que la información $I_{i-1}$, destinada a utilizarse por el dispositivo multimedia, tras la desaleatorización, al mismo tiempo que la información $I_1$ a $I_{i-1}$ para que la combinación de la información $I_1$ a $I_i$ así realizada sea directamente comprensible e inteligible para un ser humano, completando la información $I_i$ la información $I_{i-1}$ de modo que la información $I_1$ puede completarse gradualmente, en orden, por la información $I_2$ y siguientes, lo que hace posible la utilización por el dispositivo multimedia del programa multimedia en $k$ niveles diferentes de completitud, aumentando el nivel de completitud a medida que aumenta el índice $i$, estando cada flujo elemental de información $I_i$ aleatorizado con una palabra de control $CW_i$ diferente de las palabras de control $CW_j$, en el que $i$ es diferente de $j$, comprendiendo este emisor:

- un aleatorizador adecuado para aleatorizar los flujos elementales de información $I_1$ a $I_k$ respectivamente con palabras de control $CW_1$ a $CW_k$, siendo cada palabra de control $CW_i$ diferente de las palabras de control $CW_j$, en el que $i$ es diferente de $i$,

- un generador de mensajes $ECM_i$, en el que $i$ es un número entero comprendido entre 1 y $k$, conteniendo cada mensaje $ECM_i$ unas condiciones de acceso $CA_i$ y un primer criptograma $(CW_i)_{CEi}$ obtenido cifrando la palabra de control $CW_i$ con una clave de explotación $CE_i$,

caracterizado porque este emisor es apto para construir y difundir los segundos criptogramas $(CW_i)_{Ki}$ para $i$ comprendida entre 1 y $k$-1, obtenidos cifrando las mismas palabras de control $CW_1$ a $CW_{k-1}$ con las claves respectivas $K_1$ a $K_{k-1}$ construidas con al menos una parte del conjunto formado por la información presente en el $ECM_k$ y por la clave de explotación $CE_k$.

Fig. 1



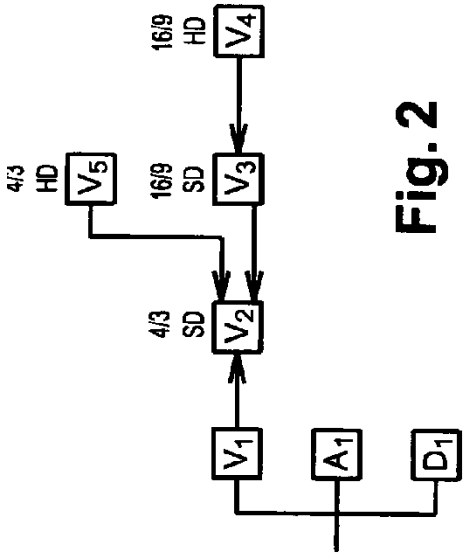

16/9
HD
V4
4/3
HD
V5
16/9
SD
V3
4/3
SD
V2
V1
A1
D1

Fig. 2

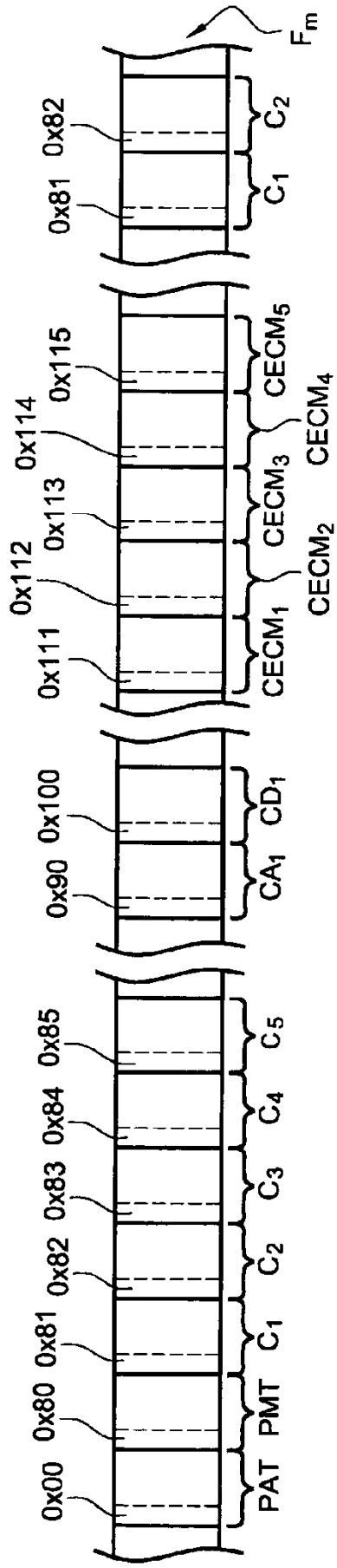

Fm
0x82
0x81
C2
C1
0x115
0x114
0x113
0x112
0x111
CECM5
CECM4
CECM3
CECM2
CECM1
0x100
0x90
CD1
CA1
0x85
0x84
0x83
0x82
0x81
0x80
0x00
C5
C4
C3
C2
C1
PMT
PAT

Fig. 3

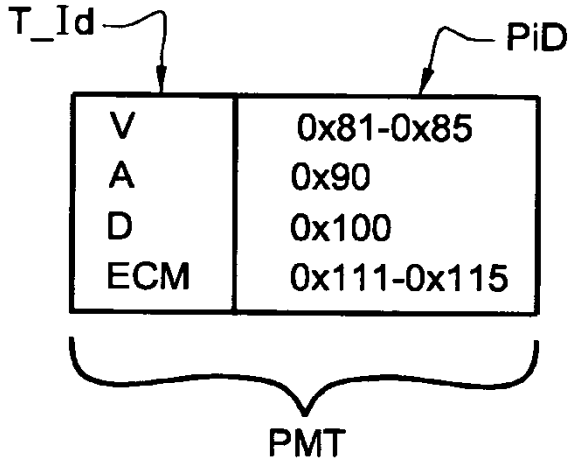



Fig. 4

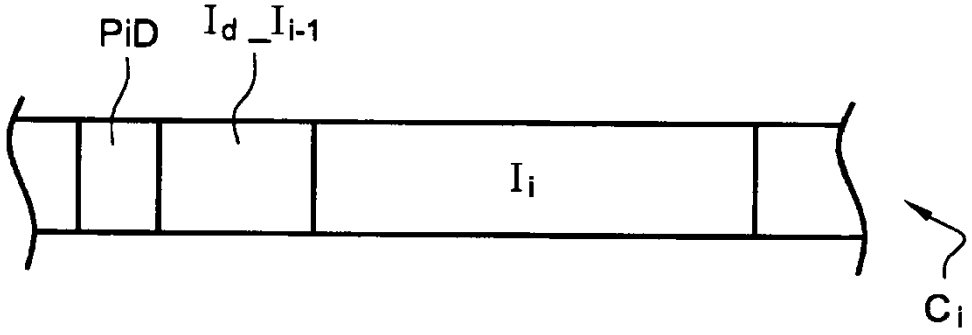



Fig. 5

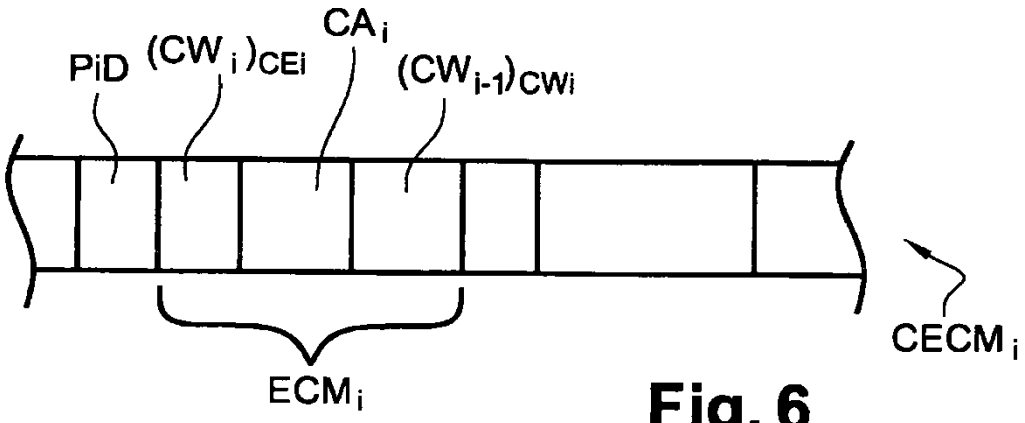



Fig. 6

Fig. 7

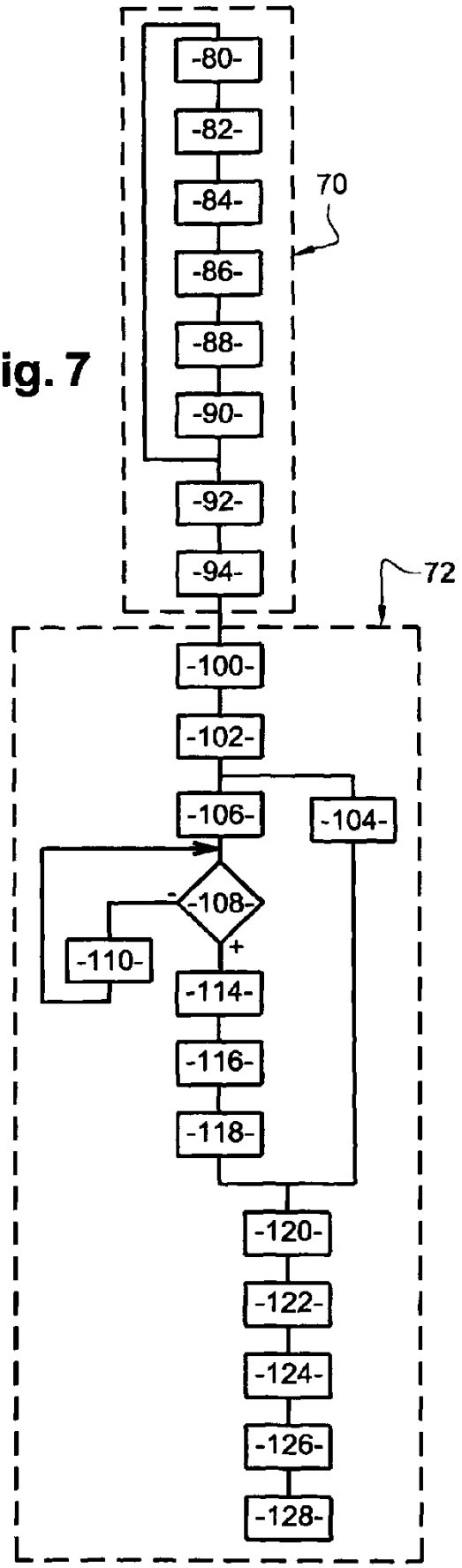
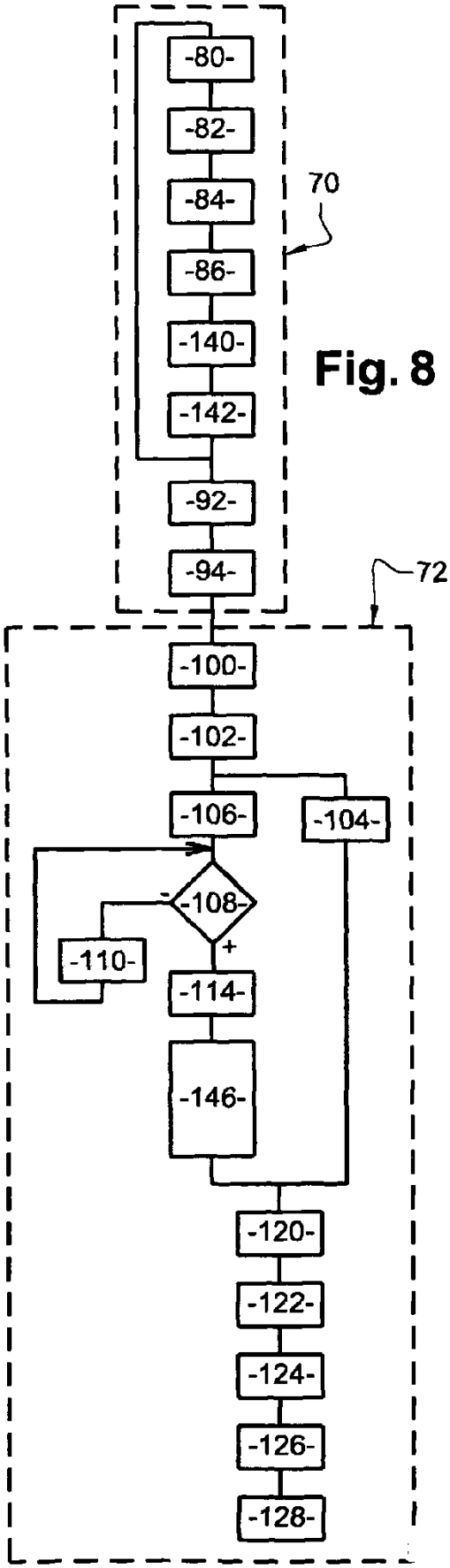

-80-
-82-
-84-
-86-
-88-
-90-
-92-
-94-
70
72
-100-
-102-
-106-
-104-
-108-
-110-
-114-
-116-
-118-
-120-
-122-
-124-
-126-
-128-

Fig. 8


-80-
-82-
-84-
-86-
-140-
-142-
-92-
-94-
70
72
-100-
-102-
-106-
-104-
-108-
-110-
-114-
-146-
-120-
-122-
-124-
-126-
-128-