(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 848**

(51) Int. CI.:

H04N 21/2347 (2011.01) ***G11B 20/00*** (2006.01)
H04N 21/2389 (2011.01) ***H04N 7/167*** (2011.01)
H04N 21/266 (2011.01)
H04N 21/4147 (2011.01)
H04N 21/4385 (2011.01)
H04N 21/4405 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/4627 (2011.01)
H04N 21/8355 (2011.01)
H04N 21/845 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2007 PCT/FR2007/002137**

(87) Fecha y número de publicación internacional: **14.08.2008 WO08096066**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2007 E 07872422 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 2098073**

(54) Título: **Procedimiento de gestión del número de visualizaciones, procesador de seguridad y terminal para este procedimiento**

(30) Prioridad:

21.12.2006 FR 0611194

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.04.2020

(73) Titular/es:

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

(72) Inventor/es:

PLESSE, EMMANUEL

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de gestión del número de visualizaciones, procesador de seguridad y terminal para este procedimiento

[0001] La presente invención se refiere a un procedimiento de gestión del número de visualizaciones, un procesador de seguridad y un terminal para este procedimiento.

[0002] Existen unos procedimientos de gestión del número de visualizaciones de un contenido audiovisual. Estos procedimientos constan, por ejemplo:

- del suministro de un contenido audiovisual numérico grabado en un medio de grabación de información, estando este contenido dividido en varios segmentos temporales consecutivos y destinados a ser leídos automáticamente en un orden prescrito,
- del suministro de un número de visualizaciones autorizadas de este contenido audiovisual,
- de la lectura del contenido audiovisual grabado, con la ayuda de un lector electrónico, permitiendo el lector electrónico, en particular, saltar hacia atrás para leer un segmento anterior antes de llegar al final del contenido audiovisual,
- del cálculo del número de visualizaciones del contenido audiovisual ya efectuadas, y
- de la prohibición de cualquier nueva visualización del contenido audiovisual si el número de visualizaciones ya efectuadas es superior o igual al número de visualizaciones autorizadas y, en caso contrario, la autorización de una nueva visualización del contenido audiovisual en su conjunto.

[0003] Los contenidos audiovisuales numéricos son, por ejemplo, unos videogramas tales como unas películas o una emisión televisada.

[0004] Un segmento corresponde a una secuencia ordenada y consecutiva de imágenes y/o de sonidos. Este segmento se graba en un formato adaptado para ser leído por el lector electrónico y después visualizado en una pantalla. Durante la visualización en una pantalla, las imágenes y sonidos de un segmento se encadenan uno tras otro a una frecuencia superior o igual a 50 Hz para crear una impresión de continuidad visual y auditiva entre las diferentes imágenes y sonidos de un mismo segmento

[0005] Se dice que dos segmentos son consecutivos, si durante la lectura de estos segmentos en el orden prescrito, el intervalo de tiempo que separa el instante en que el segmento anterior deja de reproducirse del instante en que el siguiente segmento comienza a reproducirse es inferior a 1/50 de segundo. Así, cuando dos segmentos son consecutivos, se garantiza una continuidad visual y auditiva entre estos dos segmentos para el usuario.

[0006] Estos procedimientos de gestión son particularmente útiles para limitar el número de veces que un usuario puede visualizar un contenido audiovisual grabado.

[0007] El documento EP 1 182 874 describe un procedimiento de acceso condicional a unos contenidos audiovisuales, con una limitación del número de visualizaciones autorizadas.
Se observa aquí que se limita el número de veces que se puede visualizar el contenido audiovisual mediante el uso de un cálculo del número de veces que el usuario ya ha visualizado el contenido audiovisual. Este primer enfoque debe distinguirse de un segundo enfoque competitivo que también tiene como objetivo limitar el número de veces que se puede visualizar el contenido. Este enfoque competitivo autoriza inicialmente una duración de visualización DVA. A continuación, la duración DVA se reduce proporcionalmente al tiempo de visualizaciones efectuadas del contenido audiovisual. Este enfoque competitivo es simple, ya que solo necesita medir el tiempo de visualización. Sin embargo, es muy poco flexible, en particular, es muy difícil al medir únicamente el tiempo de visualizaciones ya transcurrido tener en cuenta las diferentes posibilidades de visualizaciones del contenido audiovisual que son posibles por los saltos hacia atrás o, por el contrario, hacia delante, que se pueden realizar bajo el control del usuario.

[0008] Potencialmente, el recuento del número de visualizaciones del contenido audiovisual no presenta el inconveniente de este enfoque competitivo. Sin embargo, debido a la posibilidad de efectuar saltos hacia atrás y, posiblemente, hacia delante, existe un gran número de estrategias diferentes para calcular el número de visualizaciones ya efectuadas.

[0009] Por ejemplo, se puede decidir que el contenido audiovisual se haya visualizado una vez cuando cada uno de sus segmentos se haya visualizado al menos una vez. Esta estrategia es muy permisiva puesto que permite además al usuario visualizar tantas veces como quiera un segmento dado volviendo sistemáticamente hacia atrás después de la visualización de este segmento.

[0010] Una estrategia un poco menos permisiva consiste en incrementar un contador cada vez que se visualiza un segmento del contenido audiovisual. Este contador se compara a continuación con un umbral predeterminado. Si se supera el umbral, el número de visualizaciones ya efectuadas se incrementa en uno. Con esta estrategia, el usuario ya no puede visualizar tantas veces como quiera el mismo segmento sin que el número de visualizaciones ya

efectuadas se incremente. Por el contrario, a la inversa, el número de visualizaciones ya efectuadas puede incrementarse incluso si ciertos segmentos nunca se han visualizado.

[0011] Por lo tanto, es conveniente proponer un procedimiento de gestión del número de visualizaciones que sea lo suficientemente flexible como para permitir la implementación de nuevas estrategias de cálculo del número de visualizaciones ya efectuadas sin conllevar modificaciones importantes del procedimiento.

[0012] La invención tiene como objetivo satisfacer este deseo. Por lo tanto, tiene como objeto un procedimiento de gestión del número de visualizaciones de un contenido audiovisual que consta de:

- el suministro de una tabla que contiene tantas celdas como segmentos temporales, estando cada celda asociada de forma biunívoca a un segmento respectivo del contenido audiovisual, siendo cada celda apta para contener un número,
- cuando un segmento del contenido audiovisual es leído por el lector electrónico, el incremento o la disminución de un paso predeterminado del número contenido en la celda asociada a este segmento, y
- el cálculo del número de visualizaciones ya efectuadas realizado a partir de los números registrados en cada una de las celdas de la tabla.

[0013] En el procedimiento anterior, la tabla permite memorizar una representación del número de veces que se ha visualizado cada segmento del contenido audiovisual. En particular, el contenido de esta tabla permite además detectar el uso de saltos hacia atrás. Por lo tanto, la granulometría de la información contenida en esta tabla es suficiente para poder implementar un gran número de estrategias diferentes de cálculo del número de visualizaciones ya efectuadas. Por lo tanto, el procedimiento es lo suficientemente flexible como para que cada operador o proveedor de contenido audiovisual pueda definir su propia estrategia de cálculo del número de visualizaciones ya efectuadas.

[0014] Sin embargo, en el caso de cambio de estrategia de cálculo, solo debe modificarse la forma de calcular el número de visualizaciones ya efectuadas y/o el paso predeterminado de incremento o disminución sin que sea necesario modificar las operaciones de gestión y actualizar la tabla. Por lo tanto, las modificaciones que se van a aportar al procedimiento de gestión son limitadas.

[0015] Los modos de realización de este procedimiento pueden constar de una o varias de las características siguientes:

- la grabación en una memoria no volátil de una licencia de visualización múltiples, constando esta licencia al menos de:
  - el número de visualizaciones autorizadas,
  - la tabla que contiene las celdas asociadas de forma biunívoca a los segmentos temporales del contenido audiovisual,
  - una redundancia criptográfica, tal como una firma realizada con la ayuda de una clave criptográfica, de al menos una parte de cada una de las informaciones anteriores,

- la verificación de la redundancia criptográfica antes de cada nuevo uso del lector para visualizar el contenido audiovisual, y
- la prohibición de cualquier nueva visualización en el caso de que la redundancia criptográfica no haya podido verificarse correctamente;
- la licencia consta de un identificador T_Anti_Reuse de su uso anterior,
- un procesador de seguridad equipado con medios de almacenamiento de información que contengan:
  - una clave criptográfica que se puede utilizar para verificar la redundancia criptográfica de la licencia y/o una clave criptográfica que permita realizar la redundancia criptográfica de la licencia, y
  - un identificador C_Anti_Reuse del uso anterior de la licencia,

- después de cada uso del lector para visualizar el contenido audiovisual, los identificadores T_Anti_Reuse y C_Anti_Reuse se modifican para que sus nuevos valores respectivos correspondan, y
- antes de cada nuevo uso del lector para visualizar el contenido audiovisual, la visualización del contenido audiovisual se autoriza únicamente si el valor del identificador T_Anti_Reuse corresponde al valor del identificador C_Anti_Reuse;
- la selección de un algoritmo de cálculo del número de visualizaciones efectuadas que se van a ejecutar durante el cálculo del número de visualizaciones, en función del contenido de la licencia, entre un conjunto de varios algoritmos de cálculo diferentes que se pueden ejecutar, siendo dos algoritmos de cálculo considerados como diferentes si existe un mismo contenido de las celdas de la tabla a partir del cual los dos algoritmos dan resultados diferentes;
- el suministro de varios contenidos audiovisuales diferentes y varias licencias, teniendo cada una un identificador de contenido audiovisual que la vincula de manera biunívoca a uno de los contenidos audiovisuales, y
- durante el cálculo del número de visualizaciones ya efectuadas, solo la información contenida en la licencia que contiene el identificador del contenido audiovisual actualmente leído se utiliza para el cálculo del número de visualizaciones ya efectuadas;

- el suministro de un procesador de seguridad apto para tratar unos mensajes ECM (*Entitlement Control Message*) y EMM (*Entitlement Management Message*),
- la transmisión de la licencia en forma de un mensaje EMM al procesador de seguridad, conteniendo este mensaje EMM un identificador del único procesador de seguridad al que se dirige;
- diferentes segmentos del contenido audiovisual están cifrados con diferentes palabras de control, constando el procedimiento para cada segmento de:
- la transmisión de al menos un mensaje ECM a un procesador de seguridad, conteniendo cada mensaje ECM:

  • un criptograma de la palabra de control necesaria para descifrar al menos una parte de este segmento del contenido audiovisual, y
  • un identificador de la celda de la tabla que se incrementará o disminuirá cuando este mensaje ECM se use para obtener la palabra de control necesaria para descifrar este segmento del contenido audiovisual,

- el incremento o la disminución del número contenido en la celda correspondiente al identificador de celda contenido en el mensaje ECM,
- el descifrado, por el procesador de seguridad, de la palabra de control contenida en el mensaje ECM transmitido, y
- la transmisión de la palabra de control descifrada a un decodificador para descifrar al menos una parte del segmento de contenido audiovisual;
- el cálculo del número de visualizaciones ya efectuadas consta de:

  - la determinación del número de celdas de la tabla que contiene un número que se ha incrementado o disminuido desde la última visualización del contenido audiovisual, y
  - el cálculo del número de visualizaciones ya efectuadas en función del resultado de esta determinación;

- durante el cálculo del número de visualizaciones ya efectuadas, el paso predeterminado utilizado para incrementar o disminuir el número contenido en la celda asociada a un segmento disminuye o aumenta en función del número de veces que este segmento ya ha sido visualizado.

[0016] Estos modos de realización del procedimiento presentan además las ventajas siguientes:

- la conservación de la información necesaria para el cálculo del número de visualizaciones ya efectuadas en una licencia firmada dificulta la falsificación de esta información,
- la comparación de los identificadores T_Anti_Reuse y C_Anti_Reuse impide que una licencia se pueda reiniciar en un estado anterior,
- la posibilidad de seleccionar diferentes algoritmos de cálculo del número de visualizaciones ya efectuadas permite utilizar diferentes estrategias de control del número de visualizaciones para diferentes contenidos audiovisuales,
- la utilización de un identificador de contenido audiovisual en cada licencia permite gestionar individualmente el cálculo del número de visualizaciones para cada uno de los contenidos audiovisuales,
- la transmisión de la licencia en forma de mensaje EMM limita las adaptaciones que se realizarán al procesador de seguridad para que pueda recibir y tratar la licencia,
- la presencia de un identificador de la celda de la tabla que debe incrementarse o disminuirse en el mensaje ECM que contiene el criptograma de la palabra de control simplifica enormemente la gestión de la tabla por parte del procesador de seguridad,
- incrementar el número de visualizaciones ya efectuadas en función del número de celdas de la tabla que se han modificado desde la última visualización del contenido audiovisual permite tener en cuenta la proporción del contenido audiovisual que se ha visualizado para aumentar o disminuir el número de visualizaciones ya efectuadas, y
- hacer variar el paso de incremento o disminución en función del número de veces que el segmento ya ha sido visualizado permite atribuir una importancia diferente a la primera visualización de un segmento con respecto a las siguientes visualizaciones de este mismo segmento.

[0017] La invención tiene igualmente como objeto un procesador de seguridad que contiene unas instrucciones para la ejecución del procedimiento de gestión anterior cuando estas instrucciones son ejecutadas por un calculador electrónico.

[0018] Finalmente, la invención tiene igualmente como objeto un terminal de lectura de un contenido audiovisual, constando este terminal de:

- un soporte de grabación de información que contiene el contenido audiovisual numérico grabado, estando este contenido dividido en varios segmentos temporales consecutivos y destinados a ser leídos automáticamente en un orden prescrito,
- un número entero de visualizaciones autorizadas para este contenido audiovisual,
- un lector electrónico de contenidos audiovisuales, que permite especialmente unos saltos hacia atrás para leer un segmento anterior antes de que se llegue al final del contenido audiovisual,
- siendo el terminal apto para:

• calcular el número de visualizaciones de este contenido audiovisual ya efectuadas, y
• prohibir cualquier nueva visualización del contenido audiovisual si el número de visualizaciones ya efectuadas es superior o igual al número de visualizaciones autorizadas y, en caso contrario, autorizar una nueva visualización del contenido audiovisual en su conjunto,

- el terminal comprende una tabla que contiene tantas celdas como segmentos temporales, estando cada celda asociada de forma biunívoca a un

[0019] segmento respectivo del contenido audiovisual, siendo cada celda apta para contener un número, y

- el terminal es apto:

• cuando un segmento del contenido multimedia es leído por el lector electrónico, para incrementar o disminuir en un paso predeterminado el número contenido en la celda asociada a este segmento, y
• para calcular el número de visualizaciones ya efectuadas a partir de los números grabados en cada una de las celdas de esta tabla.

[0020] La invención se comprenderá mejor con la lectura de la descripción que aparece a continuación, dada únicamente a título de ejemplo no limitativo y realizada en referencia a los dibujos en los que:

- la figura 1 es una ilustración esquemática de un terminal de lectura de contenidos audiovisuales numéricos grabados,
- la figura 2 es una ilustración esquemática de un contenido audiovisual que se puede ver con la ayuda del terminal de la figura 1,
- la figura 3 es una ilustración esquemática de un ECM (*Entitlement Control Message*) grabado con el contenido audiovisual de la figura 2.
- la figura 4 es una ilustración esquemática de una licencia utilizada en el terminal de la figura 1,
- la figura 5 es una ilustración de la estructura de una tabla contenida en la licencia de la figura 4,
- la figura 6 es una ilustración de una lista anti-repetición contenida en un procesador de seguridad del terminal de la figura 1,
- las figuras 7A y 7B son unos diagramas de flujo de un procedimiento de gestión del número de visualizaciones del contenido audiovisual implementado en el terminal de la figura 1,
- la figura 8 es una ilustración esquemática de la estructura de un EMM-U (*Entitlement Management Message* con dirección única) generado durante la ejecución del procedimiento de la figura 7, y
- las figuras 9 a 11 son unos diagramas de flujo, respectivamente, de tres algoritmos de cálculo del número de visualizaciones ya efectuadas.

[0021] En estas figuras, se usan las mismas referencias para designar los mismos elementos.

[0022] En el resto de esta descripción, las características y funciones bien conocidas por el experto en la materia no se describen en detalle.

[0023] La figura 1 representa un terminal 2 de lectura de contenido audiovisual numérico. Este terminal 2 es apto para controlar la visualización en una pantalla 4 de contenido audiovisual leído para que pueda ser visto por un usuario. Por usuario, aquí se entiende un ser humano.

[0024] La pantalla 4 es, por ejemplo, típicamente una pantalla de televisión.

[0025] El terminal 2 comprende un decodificador 6 conectado a un soporte 8 de grabación de información. El contenido audiovisual se graba en este soporte 8. Por ejemplo, aquí, a título de ilustración, dos contenidos audiovisuales CAN_1 y CAN_2 así como sus respectivas licencias L_1 y L_2 se graban en el soporte 8. Los contenidos CAN_1 y CAN_2 son, por ejemplo, unos contenidos audiovisuales codificados con la ayuda de palabras de control CW.

[0026] La estructura de uno de estos contenidos audiovisuales se ilustra en la figura 2.

[0027] El contenido audiovisual se divide en una multitud de segmentos temporales CAN_1 a CAN_N. Estos segmentos CAN_i se siguen en un orden prescrito. Por ejemplo, el segmento CAN_1 corresponde al primer segmento que debe ser leído y el segmento CAN_N corresponde al último segmento que debe ser leído. Aquí, cada segmento CAN_i se codifica con la ayuda de una sola palabra de control CW diferente de la utilizada para codificar los segmentos anteriores y los segmentos siguientes. Así, en este modo de realización particular, cada segmento corresponde a un criptoperíodo.

[0028] A título de ejemplo, la duración de un criptoperíodo es generalmente de 10 segundos.

[0029] Cada segmento o criptoperíodo CAN_i está asociado a un mensaje ECM (*Entitlement Control Message*) indicado como ECM_i. El mensaje ECM_i contiene un criptograma CW* de la palabra de control CW utilizada para

codificar el segmento CAN_i. Los mensajes ECM_i se graban en el soporte 8 al mismo tiempo que los segmentos CAN_i.

[0030] La estructura de estos mensajes ECM_i es, por ejemplo, conforme a la norma UTE C90-007 «Sistema de acceso condicional para sistemas de difusión numérica» utilizada en el campo de la transmisión de señales multimedia codificadas por medio de redes de larga distancia de transmisión de información tal como, por ejemplo, redes que involucran satélites.

[0031] En la figura 3, solo se representan las porciones de la estructura del mensaje ECM_i útiles para la comprensión del resto de la descripción. El mensaje ECM_i comprende un campo SOID que contiene a la vez un identificador del operador que ha difundido este contenido audiovisual así como un identificador del contexto criptográfico que se va a aplicar. El identificador del contexto criptográfico que se va a aplicar permite especialmente a un procesador de seguridad identificar cuál es la o cuáles son las claves criptográficas que se van a utilizar para tratar este mensaje ECM.

[0032] El mensaje ECM_i comprende igualmente:

- un campo C_Id que contiene un identificador C_Id de una celda de una tabla,
- un campo CW* que contiene el criptograma CW* de una palabra de control CW,
- un campo CdA que contiene unas condiciones de acceso de CdA al contenido audiovisual, y
- un campo ECM_R que contiene una redundancia criptográfica tal como un MAC (*Message Authentication Code*) o una firma criptográfica del ECM_i relacionada con una parte de la información contenida en cada uno de los campos anteriores de este mensaje ECM_i.

[0033] El identificador C_Id establece una relación biunívoca entre este mensaje ECM_i y una celda de la tabla de la figura 5.

[0034] La estructura de las licencias L_1 y L_2 es, por ejemplo, conforme a la estructura de licencia representada en la figura 4. Más precisamente, cada licencia comprende los campos siguientes:

- un campo SOID que tiene el mismo contenido que el campo SOID de los mensajes ECM_i asociados al contenido audiovisual correspondiente a esta licencia,
- un campo UA que contiene un identificador único UA de un procesador de seguridad,
- un campo Content_Id que contiene un identificador Content_Id del contenido audiovisual al que corresponde esta licencia,
- un campo L_Id que contiene un identificador L_Id de esta licencia que permite especialmente distinguir esta licencia de otra licencia que contiene exactamente los mismos identificadores SOID, UA y Content_Id,
- un campo NVA que contiene un número entero positivo NVA correspondiente al número de visualizaciones autorizadas para el contenido audiovisual identificado por el identificador Content_Id,
- un campo NCV que contiene un número entero NCV utilizado para memorizar el número de segmentos ya visualizados durante la lectura anterior del contenido audiovisual asociado a esta licencia,
- un campo T_Anti_Reuse que contiene un identificador T_Anti_Reuse del uso anterior de la licencia, utilizado para evitar que una misma licencia pueda ser reutilizada varias veces; normalmente este identificador es un número cuyo valor aumenta estrictamente con cada nuevo uso de la licencia,
- un campo Params que contiene varios parámetros de un algoritmo de cálculo del número de visualizaciones ya efectuadas,
- un campo Tab que contiene la tabla de la figura 5, y
- un campo L_R que contiene una redundancia criptográfica L_R tal como un MAC o una firma criptográfica relacionada con al menos una parte de la información contenida en cada uno de los campos anteriores.

[0035] A título de ejemplo, el campo Params contiene unos valores para los parámetros siguientes:

- C_Size,
- S_1,
- S_2, y
- Algo_Id.

[0036] El interés de estos parámetros aparecerá en relación con la descripción de las figuras 9 a 11.

[0037] La redundancia criptográfica L-R se construye implementando un algoritmo criptográfico y una clave criptográfica.

[0038] La figura 5 representa esquemáticamente un ejemplo de estructura posible para la tabla Tab. Aquí, esta tabla está formada por N celdas sucesivas clasificadas en el orden que va de 1 a N. N es un número entero igual al número de segmentos contenidos en el contenido audiovisual al que está asociada la licencia. Cada celda está

destinada a contener un número codificado en un número de bits parametrizables con la ayuda del parámetro C_Size contenido en el campo Params de la licencia.

[0039] Los valores 1, 2, 3, …, i, i+1, …,N indicados arriba de cada una de estas celdas representan el valor del identificador C_Id que permite identificar la celda situada justo debajo.

[0040] El decodificador 6 comprende:

- un lector electrónico 10 apto para leer y escribir información en el soporte 8,
- un filtro 12 apto para orientar el contenido audiovisual codificado hacia un decodificador y un decodificador 14 y enviar los mensajes ECM_i asociados a este contenido audiovisual codificado hacia una interfaz decodificador/tarjeta 16,
- el decodificador y decodificador 14.

[0041] El decodificador 6 comprende aquí, a título de ilustración únicamente, un receptor 18 apto para recibir por medio de una red inalámbrica 20 de transmisión de información unos contenidos audiovisuales codificados y los mensajes ECM asociados a este contenido audiovisual. Por ejemplo, los contenidos audiovisuales codificados así como los mensajes ECM son difundidos por un emisor distante 24 hacia una multitud de terminales distantes, tal como el terminal 2.

[0042] El terminal 2 comprende igualmente un procesador de seguridad 30 conectado al decodificador 6. Este procesador de seguridad 30 está concebido para tratar unos mensajes ECM y EMM (*Entitlement Management Message*) y efectuar las operaciones de cifrado y descifrado necesarias para el funcionamiento del terminal 2.

[0043] A tal efecto, el procesador 30 consta de:

- una interfaz 32 apta para cooperar con la interfaz 16 del decodificador para recibir de este último unos mensajes ECM y EMM,
- un calculador 34 apto para tratar los mensajes EMM y ECM recibidos por medio de la interfaz 32,
- una memoria no volátil 36 en la que se almacena, además, la diferente información necesaria para las operaciones de cifrado/descifrado, y
- una memoria volátil 38 en la que se almacenan los resultados temporales de tratamiento.

[0044] Por ejemplo, el procesador 30 es un procesador de seguridad extraíble tal como una tarjeta inteligente.

[0045] La memoria 36 contiene:

• un identificador UA único del procesador de seguridad que permite distinguir el procesador 30 del conjunto de los procesadores de seguridad que se pueden usar en el decodificador 6,
• tres algoritmos Algo1, Algo2 y Algo3 diferentes que permiten cada uno calcular el número de visualizaciones ya efectuadas.

[0046] Para cada identificador de contexto criptográfico, la memoria 36 contiene también la información siguiente:

- unos títulos de acceso TdA destinados a ser comparados con las condiciones de acceso CdA contenidas en un mensaje ECM a fin de determinar si este mensaje ECM puede ser o no tratado por el procesador 30,
- una lista CAR destinada a impedir la reutilización de una licencia,
- unas claves criptográficas K_i que permiten efectuar las operaciones de cifrado y descifrado necesarias para el tratamiento de los mensajes ECM y EMM.

[0047] La figura 6 representa un ejemplo de estructura posible para la lista CAR. Esta lista consta, por ejemplo, de una primera columna que contiene los identificadores Content_Id y una segunda columna que consta del identificador C_Anti_Reuse asociado al identificador Content_Id. La lista CAR contiene tantas líneas como licencias ya leídas por el lector 10.

[0048] La memoria 36 comprende igualmente una tabla TabIncrement destinada a ser utilizada en conjunto con el algoritmo Algo3. La tabla TabIncrement es, por ejemplo, la siguiente:

X	0	1	2	3	4	5	6	7	X+1
Y	0	1	0,5	0,3	0,2	0,2	0,2	0,2	0,1
Z	0	1	1,5	1,8	2	2,2	2,4	2,6	Y+0,1

[0049] La primera línea X de esta tabla contiene unos números enteros correspondientes cada uno a un número de veces en que un segmento ha sido visualizado. La segunda línea Y asocia a cada uno de estos números enteros un paso de incremento. Se observará que este paso de incremento es aquí una función de disminución monótona del número de veces en que un segmento ya ha sido leído. La línea Z da el número efectivamente tomado en cuenta por el algoritmo para cada número de visualización de un segmento.

[0050] Por último, el terminal 2 consta de un mando a distancia 40 que permite controlar por medio de una conexión inalámbrica 42 el decodificador 6. Para simplificar la ilustración, solo se representan las teclas siguientes del mando a distancia 40:

- una tecla 44 que permite activar la lectura de un contenido audiovisual seleccionado entre los diferentes contenidos audiovisuales grabados en el soporte 8,
- una tecla 45 que permite detener la lectura de un contenido audiovisual a fin de, por ejemplo, pasar a la lectura de otro contenido audiovisual o simplemente de detener toda lectura,
- una tecla 46 que permite hacer unos saltos hacia atrás, es decir pasar directamente del segmento actualmente leído a un segmento anterior sin que sea por ello necesario leer los segmentos intermedios entre el segmento actualmente leído y el segmento anterior, y
- una tecla 47 que permite efectuar unos saltos hacia delante, es decir que permiten pasar del segmento actualmente leído directamente a un segmento siguiente sin tener que leer los segmentos intermedios situados entre el segmento actualmente leído y el segmento siguiente.

[0051] El funcionamiento del terminal 2 va a ser descrito ahora con respecto al procedimiento de la figura 7. Inicialmente, durante una etapa 70, el emisor 24 envía al terminal 2 un contenido audiovisual codificado y los mensajes ECM correspondientes por medio de la red 20. Durante una etapa 72, el terminal 2 graba este contenido audiovisual codificado y los mensajes ECM correspondientes en el soporte 8 para obtener, por ejemplo, el contenido audiovisual grabado CAN_1.

[0052] A continuación, durante una etapa 74, el emisor 24 transmite por medio de la red 20 o por otro modo de comunicación, la licencia L_1 al terminal 2. Se trata aquí de la versión inicial de la licencia L_1, que contiene en particular el valor inicial del número NVA de visualizaciones autorizadas de este contenido. De preferencia, este valor inicial permite al menos dos visualizaciones completas del contenido. Por ejemplo, durante la etapa 74, esta licencia se transmite en un mensaje EMM-U cuya estructura se representa en la figura 8. Más precisamente, la estructura de este mensaje EMM-U es conforme a la norma UTE C90-007 (ya citada) del campo de la transmisión de señales multimedia codificadas. En la figura 8, solo se representan los elementos necesarios para la comprensión del resto de la descripción.

[0053] Más precisamente, el mensaje EMM_U comprende los mismos campos que los ya descritos con referencia a la figura 4, de modo que su descripción no se retomará aquí en detalle.

[0054] Durante una etapa 76, solo el terminal 2 cuyo procesador de seguridad corresponde al identificador UA contenido en el mensaje EMM-U registra la licencia recibida en el soporte 8.

[0055] Se comprende que la licencia se puede enviar antes o al mismo tiempo que el contenido, así como para su grabación en el soporte 8. Las etapas 70 y 74 pueden ser así simultáneas o permutadas, así como las etapas 72 y 76, siempre que las etapas 72 y 76 permanezcan posteriores respectivamente a las etapas 70 y 74.

[0056] Más tarde, el usuario del terminal 2 activa la lectura de uno de los contenidos audiovisuales grabados en el soporte 8 con la ayuda del mando a distancia 40, por ejemplo. Aquí se supone que se activa la lectura del contenido CAN_1. Una fase 80, denominada de apertura de sesión, comienza entonces.

[0057] Inicialmente, durante una etapa 82, si existen varias licencias para el mismo contenido audiovisual, el usuario selecciona la licencia que se va a utilizar para visualizar este contenido. Aquí, la licencia L_1 se selecciona automáticamente ya que solo esta licencia está asociada al contenido CAN_1.

[0058] A continuación, durante una etapa 84, el terminal envía la licencia seleccionada al procesador 30 por medio de las interfaces 16 y 32. A tal efecto, el decodificador transmite el mensaje EMM-U que representa la licencia L_1, siendo este mensaje EMM-U idéntico al de la figura 8.

[0059] Durante una etapa 86, el procesador 30 verifica que el identificador UA contenido en el mensaje EMM-U recibido corresponde al identificador UA grabado en la memoria 36. Por ejemplo, durante la etapa 86, el procesador 30 verifica si estos identificadores UA son idénticos.

[0060] En caso afirmativo, procede a una etapa 88 durante la cual el procesador 30 verifica la autenticidad de la licencia recibida con la ayuda de la redundancia criptográfica L_R. Más precisamente, durante la etapa 88, el

procesador 30 procede a partir del contenido de los campos de la licencia recibida a las operaciones similares a las efectuadas previamente para obtener la redundancia L_R. En particular, durante la etapa 88, al menos una de las operaciones implica un cifrado o un descifrado con una clave criptográfica. Por ejemplo, la clave criptográfica utilizada en la redundancia criptográfica se identifica gracias al identificador de contexto contenido en el campo SOID del mensaje EMM-U. Si el tratamiento de la redundancia criptográfica por el procesador 30 conduce a un resultado positivo, por ejemplo, si la redundancia construida por el procesador 30 es idéntica a la redundancia contenida en el campo L_R, entonces la licencia se considera auténtica e íntegra y el procesador procede a una etapa 90.

[0061] Durante la etapa 90, el procesador 30 busca el identificador C_Anti_Reuse asociado al identificador Content_Id contenido en la licencia recibida. Si ningún identificador de la lista CAR corresponde al identificador Content_Id recibido, entonces el procesador 30 añade, durante una etapa 92, el identificador Content_Id recibido a la lista CAR y asocia este identificador a un identificador C_Anti_Reuse de valor inicializado a cero.

[0062] En el caso contrario, durante una etapa 94, el procesador 30 compara el valor del identificador T_Anti_Reuse de la licencia recibida con el valor del identificador C_Anti_Reuse asociado al identificador Content_Id en la lista CAR. Si los identificadores corresponden, por ejemplo, si los valores son idénticos, entonces el procesador 30, durante una etapa 96, verifica que el número NVA contenido en la licencia recibida sea estrictamente superior a cero. En caso afirmativo, durante una etapa 98, el procesador 30 graba en su memoria 38 los parámetros contenidos en el campo Params, los números NVA, NCV y la tabla Tab contenidos en la licencia recibida.

[0063] Si una de las verificaciones efectuadas durante unas etapas 86, 88, 94 o 96 falla, el procesador 30 procede a una etapa 100 de parada del tratamiento de la licencia recibida y de parada del descifrado del contenido audiovisual codificado.

[0064] Al final de la etapa 98, se completa la fase 80 y comienza automáticamente una fase 104 de lectura del contenido audiovisual.

[0065] Al comienzo de la fase 104, durante una etapa 106, el primer segmento CAN_1 del contenido audiovisual CAN_1 se lee y se transmite al decodificador 14. En paralelo, durante una etapa 108, el mensaje ECM_1 asociado se transmite al procesador 30.

[0066] A continuación, durante una etapa 110, las condiciones de acceso CdA contenidas en el mensaje ECM_1 se comparan con los títulos de acceso TdA contenidos en la memoria 36. En el caso en que las condiciones de acceso correspondan a los títulos de acceso TdA, entonces el procedimiento continúa con una etapa 112 de extracción del identificador C_Id contenido en el mensaje ECM_1 recibido.

[0067] A continuación, durante una etapa 114, el procesador 30 incrementa en un paso específico la celda de la tabla Tab recibida correspondiente al identificador C_Id extraído. El paso especificado depende aquí del parámetro Algo_Id. El paso 114 se ejecuta únicamente si aún no se ha alcanzado el tamaño máximo de la celda especificada por el identificador C_Id.

[0068] Durante una etapa 116, el procesador 30 incrementa igualmente el número NCV en un paso específico.

[0069] A continuación, durante una etapa 120, el procesador determina si se ha efectuado una nueva visualización del contenido audiovisual. Esta determinación se efectúa ejecutando el algoritmo correspondiente al identificador Algo_Id. Los algoritmos correspondientes respectivamente a los identificadores Algo1, Algo2 y Algo3 se describen, respectivamente, con referencia a las figuras 9 a 11.

[0070] En caso afirmativo, procede a una etapa 122, durante la cual se incrementa el número NVA y, si es necesario, se actualizan la tabla Tab y el número NVC.

[0071] Durante una etapa 124, el procesador 30 verifica que el número NVA es estrictamente superior a cero. Si el número NVA es siempre estrictamente superior a cero, entonces, durante una etapa 126, el procesador procede a la extracción del criptograma CW* contenido en el mensaje ECM_1 recibido y después descifra este criptograma con una clave de descifrado grabada en el contexto asociado al contenido del campo SOID. A continuación, durante una etapa 128, la palabra de control CW descifrada se transmite al decodificador 14.

[0072] Si durante la etapa 110, las condiciones de acceso recibidas no corresponden a los títulos de acceso grabados, o si durante la etapa 124, el número NVA es inferior o igual a cero, entonces el procesador 30 procede inmediatamente a una etapa 130 de parada del tratamiento de los mensajes ECM_i recibidos. En consecuencia, no se proporciona ninguna nueva palabra de control CW al descifrador lo que impide el descifrado correcto del contenido audiovisual grabado en el soporte 8.

[0073] Si durante la etapa 120 se ha determinado que no se ha efectuado ninguna visualización nueva, entonces el procedimiento pasa de la etapa 120 directamente a la etapa 126.

[0074] Al final de la etapa 128, durante una etapa 132, el decodificador 14 descifra el segmento CAN_1 utilizando la palabra de control CW recibida del procesador 30. A continuación, durante una etapa 134, el segmento descifrado se muestra en claro en la pantalla 4.

[0075] Al final de la etapa 134, el procedimiento vuelve automáticamente a las etapas 106 y 108 para leer el siguiente segmento del contenido audiovisual CAN_1.

[0076] En ausencia del uso de saltos hacia delante o hacia atrás activados con la ayuda de las teclas 46 y 47, las etapas 106 a 134 se repiten para cada uno de los segmentos CAN_i del contenido CAN_1 en el orden de estos segmentos.

[0077] Durante la fase 104, el usuario puede utilizar igualmente las teclas 46 y 47 para saltar hacia delante o hacia atrás. En estas condiciones, los segmentos del contenido CAN_1 ya no se leen en el orden prescrito. Sin embargo, las etapas 106 a 134 continúan aplicándose a cada uno de los segmentos leídos. En otros términos, el uso de las teclas 46 y 47 no termina la sesión de lectura en curso.

[0078] Después de haber visualizado el contenido audiovisual, el usuario puede decidir finalizar esta visualización, por ejemplo, pulsando la tecla 45. En este momento, el procesador 30 procede a una fase 140 de cierre de la sesión en curso. Al comienzo de la fase 140, durante una etapa 142, el procesador 30 incrementa el número que constituye el identificador C_Anti_Reuse asociado al identificador Content_Id en la lista CAR. A continuación, durante una etapa 144, el procesador genera una licencia actualizada de nuevo, es decir que la licencia actualizada de nuevo contiene los nuevos valores de los números NVA, NCV, T_Anti_Reuse y Tab, así como un valor L_R reconstituido.

[0079] El valor del identificador T_Anti_Reuse de la licencia actualizada de nuevo es idéntico al del identificador C_Anti_Reuse asociado al identificador Content_Id en la lista CAR.

[0080] La redundancia L_R se construye a partir de los nuevos valores de la licencia y utilizando la clave criptográfica adecuada grabada en el contexto asociado con el identificador SOID.

[0081] A continuación, durante una etapa 146, el procesador 30 transmite la licencia L_1 actualizada al decodificador 6, que la registra en lugar de la licencia L_1 previamente registrada en el soporte 8.

[0082] Ahora se describirán tres ejemplos de algoritmos de cálculo del número de visualizaciones tales que puedan implementarse en la etapa 120. Cada algoritmo está designado por un valor particular del parámetro Algo_Id contenido en la licencia.
La figura 9 ilustra el algoritmo Algo1 de cálculo del número de visualizaciones ya efectuadas. El algoritmo Algo1 utiliza dos parámetros contenidos en la licencia, a saber, el umbral S_1 y el parámetro C_Size. Para la ejecución del algoritmo Algo1, el parámetro C_Size se fija en un bit.

[0083] Durante la ejecución del algoritmo Algo1, durante una etapa 150, el procesador 30 detecta una discontinuidad en la lectura del contenido audiovisual. Por ejemplo, esta discontinuidad se puede detectar en respuesta a la pulsación de una de las teclas 46 o 47. La discontinuidad se puede detectar igualmente observando una discontinuidad en los valores de los identificadores C_Id contenidos en los ECM_i recibidos.

[0084] Entonces, cuando se detecta esta discontinuidad, durante una etapa 152, el procesador 30 considera que se ha efectuado una nueva visualización del contenido audiovisual si el número de celdas de la tabla Tab que contiene un «1» es superior o igual al umbral S_1. En caso afirmativo, durante la etapa 122, el número NVA se reduce en uno y todas las celdas de la tabla Tab se restablecen al valor cero.

[0085] La etapa 152 también se ejecuta automáticamente cuando se alcanza el final del último segmento del contenido audiovisual.

[0086] El algoritmo Algo1 permite la visualización repetida de una parte restringida por el umbral S_1 del contenido, pero limita el número de visualizaciones tan pronto como la parte del contenido visualizada sea mayor.

[0087] La figura 10 ilustra el algoritmo Algo2 de cálculo del número de visualizaciones ya efectuadas. Este algoritmo Algo2 utiliza los parámetros C_Size, S_1 y S_2 contenidos en la licencia. Aquí, el parámetro C_Size es igual a un bit.

[0088] Durante una etapa 160, por ejemplo idéntica a la etapa 150, se detecta una discontinuidad en la lectura del contenido audiovisual. En respuesta, durante una etapa 162, se determina que se ha efectuado una nueva visualización si el número de celdas de la tabla Tab que contiene un «1» es superior al umbral S_1 o si el número NCV es superior o igual al umbral S_2.

[0089] En el caso en el que se determina que se ha efectuado una nueva visualización o al final de la lectura del último segmento, durante la etapa 122, el número NVA se reduce en uno y todas las celdas de la tabla Tab así como el valor del número NCV se restablece al valor cero.

[0090] El algoritmo Algo2 se diferencia de Algo1 en que limita la visualización de una parte restringida del contenido, por acción del umbral S_2.

[0091] La figura 11 ilustra el algoritmo Algo3. El algoritmo Algo3 utiliza los parámetros C_Size y S_2 de la licencia recibida. Además, el identificador del algoritmo Algo3 indica al procesador 30 que el paso de incremento utilizado durante la etapa 116 se determina a partir de la tabla TabIncrement.

[0092] A continuación, durante una etapa 170, el procesador 30 detecta una discontinuidad en la lectura del contenido audiovisual. En respuesta o al final de la lectura del último segmento, durante una etapa 172, se determina que se ha efectuado una nueva visualización si el número NCV es superior al umbral S_2. En caso afirmativo, durante la etapa 122, el número NVA se reduce en uno y el número NCV así como todas las celdas de la tabla Tab se restablecen a cero. Se observará que en este último modo de realización, el número NCV se incrementa en uno cuando un segmento se visualiza por primera vez. Por otro lado, cuando este mismo segmento se visualiza una segunda vez, el número NCV solo se incrementa en 0,5. Entonces, si este segmento todavía se visualiza otras veces, el incremento utilizado durante la etapa 116 es aún más pequeño. Así, de esta manera, se asigna una importancia menor a las visualizaciones posteriores de un mismo segmento que a la primera visualización.

[0093] Son posibles muchas otros modos de realización. Por ejemplo, la licencia puede transmitirse desde el transmisor al decodificador y, después, desde el decodificador al procesador de seguridad utilizando otro mensaje que no sea un mensaje EMM-U. Por ejemplo, se puede usar cualquier estructura firmada de datos.

[0094] El procesador de seguridad 30 se ha descrito aquí como un procesador extraíble. Como variante, el procesador 30 está integrado al decodificador 6 y fijado de forma permanente a este último.

[0095] Como variante, la licencia no contiene un campo L_R y, por lo tanto, no está protegida por una firma.

[0096] En el caso de que solo exista una única licencia por contenido audiovisual, se puede omitir el campo L_Id.

[0097] En el caso de que existan varias licencias posibles para un mismo contenido audiovisual, la selección de la licencia que se va a utilizar puede ser automática. Por ejemplo, la licencia más antigua se puede utilizar primero.

[0098] Aquí, cada segmento corresponde a un criptoperíodo. Como variante, un segmento corresponde a varios criptoperíodos sucesivos. En este caso, varios mensajes ECM_i incluirán el mismo identificador C_Id.

[0099] En otro modo de realización, las celdas de la tabla Tab pueden disminuirse en lugar de incrementarse.

[0100] En unos modos de realización en los que la tabla Tab nunca se restablecería, el campo NCV puede omitirse.

[0101] La licencia puede ser igualmente común a varios contenidos audiovisuales grabados en el soporte 8. En este caso, el identificador Content_Id identifica no un solo contenido audiovisual, sino un grupo de contenidos audiovisuales que se pueden visualizar con la ayuda del terminal 2.

[0102] Ciertas etapas del procedimiento de la figura 4 se pueden cambiar. Por ejemplo, la etapa 110 puede efectuarse después de la etapa 124.

[0103] Aquí, el control del número de visualizaciones ya efectuadas se realiza después de la lectura de cada segmento. Como variante, este control solo se puede realizar al final de la sesión de lectura. Así, en este modo de realización, nada impide que un usuario visualice tantas veces como desee un contenido audiovisual durante una sola y misma sesión. Sin embargo, el número de sesiones será limitado.

[0104] En otra variante, el paso de incremento utilizado por el algoritmo puede ser proporcionado por un parámetro del mensaje ECM para tener en cuenta el interés variable de una parte u otra del contenido.

[0105] El soporte 8 puede ser un soporte extraíble tal como, por ejemplo, un DVD-RW (*Digital Video Disc-Rewritable*) o un CD-RW (*Compact Disc-Rewritable*). Puede ser un soporte extraíble no regrabable (DVD-R, CD-R), en cuyo caso la licencia se almacena en una memoria no volátil del lector electrónico.

[0106] Lo que se ha descrito aquí en el caso del contenido audiovisual se puede aplicar igualmente a contenido audiofónico sin vídeo.

[0107] Lo que se ha descrito aquí en el caso de mostrar un contenido audiovisual puede aplicarse igualmente a la redistribución controlada de tal contenido en una red local o doméstica.

REIVINDICACIONES

1. Procedimiento de gestión del número de visualizaciones de un contenido audiovisual, constando este procedimiento de:

- el suministro (72) de un contenido audiovisual numérico grabado en un soporte de grabación de información, estando este contenido dividido en varios segmentos temporales consecutivos y destinados a ser leídos automáticamente en un orden prescrito,
- el suministro (74) de un número de visualizaciones autorizadas de este contenido audiovisual,
- la lectura (106) del contenido audiovisual grabado, con la ayuda de un lector electrónico, permitiendo el lector electrónico en particular unos saltos hacia atrás para leer un segmento anterior antes de llegar al final del contenido audiovisual, - el cálculo (120, 122) del número de visualizaciones del contenido audiovisual ya efectuadas, y
- la prohibición (130) de cualquier nueva visualización del contenido audiovisual si el número de visualizaciones ya efectuadas es superior o igual al número de visualizaciones autorizadas y, en caso contrario, la autorización de una nueva visualización del contenido audiovisual,

caracterizado porque el procedimiento consta de:

- el suministro (84) de una tabla que contiene tantas celdas como segmentos temporales, estando cada celda asociada de forma biunívoca con un segmento respectivo del contenido audiovisual, siendo cada celda apta para contener un número,
- cuando un segmento del contenido audiovisual es leído por el lector electrónico, el incremento (114) o la disminución de un paso predeterminado del número contenido en la celda asociada a este segmento, siendo dado el paso predeterminado por un algoritmo de cálculo del número de visualizaciones efectuadas o suministrado por un parámetro de un mensaje recibido y
- el cálculo (120; 152; 162; 172) del número de visualizaciones ya efectuadas por dicho algoritmo de cálculo a partir de los números registrados en cada una de las celdas de la tabla, que consta de:

  - la determinación (152; 162) del número de celdas de la tabla que contiene un número que se ha incrementado o disminuido desde la última visualización del contenido audiovisual, y
  - el cálculo (122) del número de visualizaciones ya efectuadas en función del resultado de esta determinación.

2. Procedimiento según la reivindicación 1, en el que el procedimiento consta de:

- la grabación (76) en una memoria no volátil de una licencia de visualización múltiple, constando esta licencia al menos de:

  • el número de visualizaciones autorizadas,
  • la tabla que contiene las celdas asociadas de forma biunívoca a los segmentos temporales del contenido audiovisual,
  • una redundancia criptográfica realizada con la ayuda de una clave criptográfica y de al menos una parte de cada una de las informaciones anteriores,

- la verificación (88) de la redundancia criptográfica antes de cada nuevo uso del lector para visualizar el contenido audiovisual, y
- la prohibición (100) de cualquier visualización nueva en el caso de que la redundancia criptográfica no se haya podido verificar correctamente.

3. Procedimiento según la reivindicación 2, en el que:

- la licencia consta de un identificador T_Anti_Reuse de su uso anterior,
- un procesador (30) de seguridad equipado con medios de almacenamiento de información que contienen:

  • una clave criptográfica que se puede utilizar para verificar la redundancia criptográfica de la licencia y/o una clave criptográfica que permita realizar la redundancia criptográfica de la licencia, y
  • un identificador C_Anti_Reuse del uso anterior de la licencia,

- después de cada uso del lector para visualizar el contenido audiovisual, los identificadores T_Anti_Reuse y C_Anti_Reuse se modifican (142, 144) para que sus nuevos valores respectivos correspondan, y
- antes de cada nuevo uso del lector para visualizar el contenido audiovisual, la visualización del contenido audiovisual se autoriza (94) únicamente si el valor del identificador T_Anti_Reuse corresponde al valor del identificador C_Anti_Reuse.

4. Procedimiento según una de las reivindicaciones 2 o 3, en el que el procedimiento consta de la selección (120) de un algoritmo de cálculo del número de visualizaciones efectuadas que se van a ejecutar durante el cálculo

del número de visualizaciones, en función del contenido de la licencia, entre un conjunto de varios algoritmos de cálculo diferentes que se pueden ejecutar, siendo considerados dos algoritmos de cálculo como diferentes si hay un mismo contenido de las celdas de la tabla de la que los dos algoritmos dan unos resultados diferentes.

5. Procedimiento según cualquiera de las reivindicaciones 2 a 4, en el que el procedimiento consta de:

- el suministro de varios contenidos audiovisuales diferentes y varias licencias, teniendo cada una un identificador de contenido audiovisual que la vincula de manera biunívoca a uno de los contenidos audiovisuales, y
- durante el cálculo del número de visualizaciones ya efectuadas, solo la información contenida en la licencia que contiene el identificador del contenido audiovisual actualmente leído se utiliza para el cálculo del número de visualizaciones ya efectuadas.

6. Procedimiento según cualquiera de las reivindicaciones 2 a 5, en el que el procedimiento consta de:

- el suministro de un procesador de seguridad apto para tratar unos mensajes ECM (*Entitlement Control Message*) y EMM (*Entitlement Management Message*),
- la transmisión (84) de la licencia en forma de un mensaje EMM al procesador de seguridad, conteniendo este mensaje EMM un identificador del procesador de seguridad único al que se dirige.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que diferentes segmentos del contenido audiovisual se mezclan con diferentes palabras de control, comprendiendo el método para cada segmento:

- la transmisión (108) de al menos un mensaje ECM a un procesador de seguridad, conteniendo cada mensaje ECM: un criptograma de la palabra de control necesaria para descifrar al menos parte de este segmento del contenido audiovisual y un identificador (CJd) de la celda de la tabla se incrementará o disminuirá cuando este mensaje ECM se use para obtener la palabra de control necesaria para descifrar este segmento del contenido audiovisual,
- el incremento (114) o la disminución del número contenido en la celda correspondiente al identificador de celda contenido en el mensaje ECM,
- el descifrado (126), por el procesador de seguridad, de la palabra de control contenida en el mensaje ECM transmitido, y
- la transmisión (128) de la palabra de control descifrada a un decodificador para descifrar al menos una parte del segmento del contenido audiovisual.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que, durante el cálculo del número de visualizaciones ya efectuadas, el paso predeterminado utilizado para incrementar (114) o disminuir el número contenido en la celda asociada a un segmento disminuye o aumenta en función del número de veces que este segmento ya ha sido visualizado.

9. Procesador de seguridad, **caracterizado porque** consta de unas instrucciones para la ejecución de un procedimiento conforme a cualquiera de las reivindicaciones anteriores, cuando estas instrucciones son ejecutadas por un calculador electrónico (34).

10. Terminal de lectura de un contenido audiovisual que consta de:

- un soporte (8) de grabación de información que contiene el contenido audiovisual numérico grabado, estando este contenido dividido en varios segmentos temporales consecutivos y destinados a ser leídos automáticamente en un orden prescrito,
- un número entero (NVA) de visualizaciones autorizadas para este contenido audiovisual,
- un lector electrónico (10) de contenidos audiovisuales, que permiten especialmente unos saltos hacia atrás para leer un segmento anterior antes de llegar al final del contenido audiovisual,
- siendo el terminal apto:

  para calcular el número de visualizaciones de este contenido audiovisual ya efectuadas, y
  para prohibir cualquier nueva visualización del contenido audiovisual si el número de visualizaciones ya efectuadas es superior o igual al número de visualizaciones autorizadas y, en caso contrario, autorizar una nueva visualización del contenido audiovisual,

caracterizado porque el terminal comprende una tabla (figura 5) que contiene tantas celdas como segmentos temporales, estando cada celda asociada de forma biunívoca a un segmento respectivo del contenido audiovisual, siendo cada celda apta para contener un número, y **porque** el terminal es apto:

- cuando un segmento del contenido multimedia es leído por el lector electrónico, para aumentar o disminuir, en un paso predeterminado, el número contenido en la celda asociada a este segmento, siendo dado el paso predeterminado por un algoritmo de cálculo del número de visualizaciones efectuadas o suministrado por un

parámetro de un mensaje recibido, y
- para calcular por dicho algoritmo de cálculo el número de visualizaciones ya efectuadas a partir de los números registrados en cada una de las celdas de esta tabla,
siendo el terminal apto para:

- determinar (152; 162) el número de celdas de la tabla que contiene un número que se ha incrementado o disminuido desde la última visualización del contenido audiovisual, y
- calcular (122) el número de visualizaciones ya efectuadas en función del resultado de esta determinación.

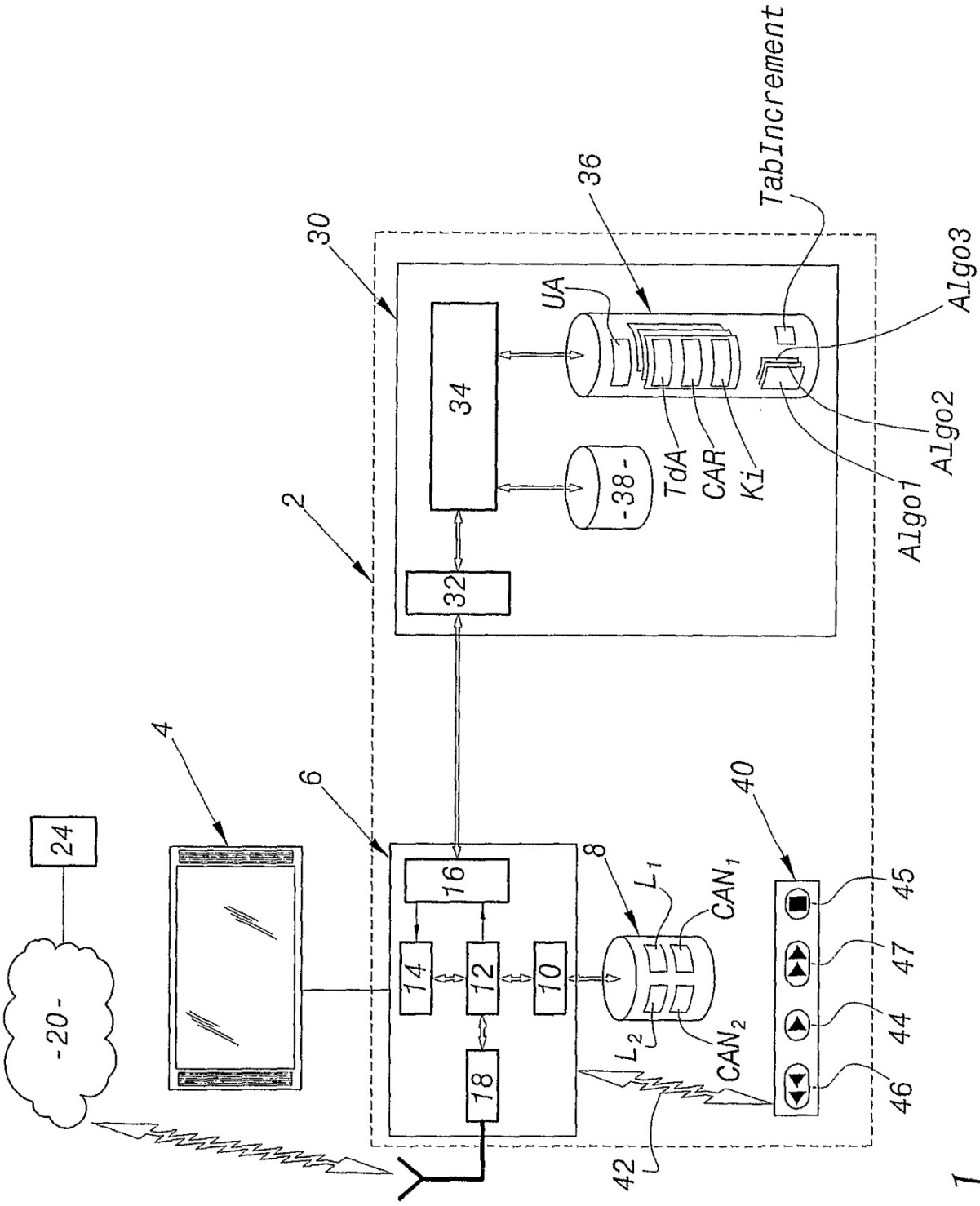
TabIncrement
36
30
UA
34
Algo3
Algo2
Algo1
TdA
CAR
Ki
-38-
2
32
4
6
40
24
-20-
16
8
L_1
CAN_1
45
14
12
10
47
44
18
L_2
CAN_2
46
42

Fig. 1

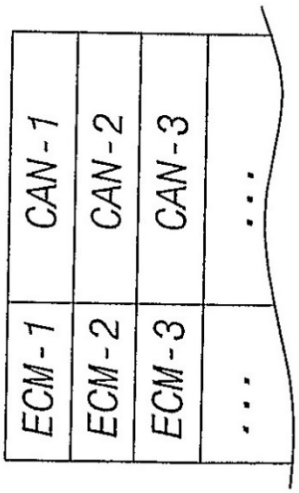

Fig.2

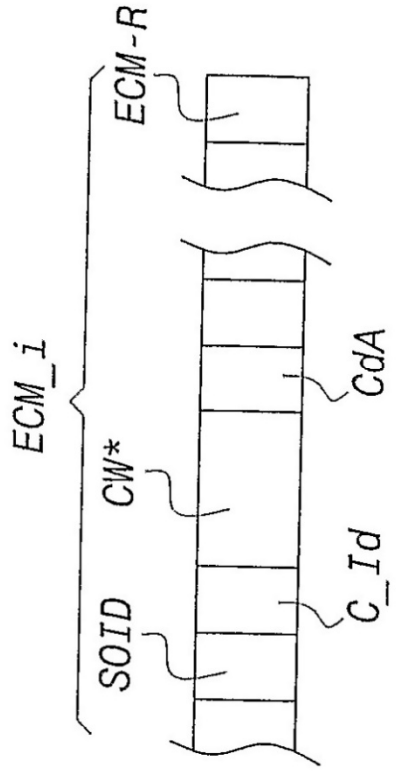

Fig.3

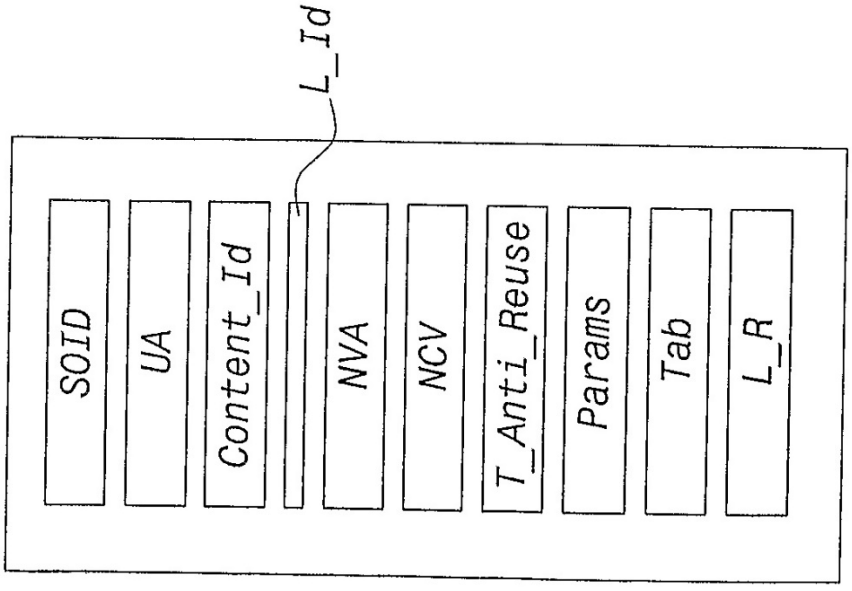

Fig.4

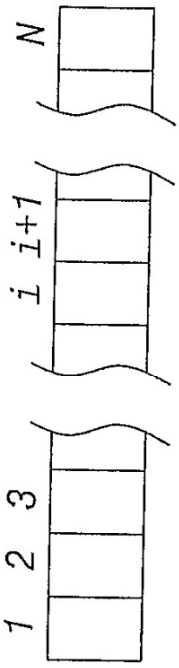

Fig.5

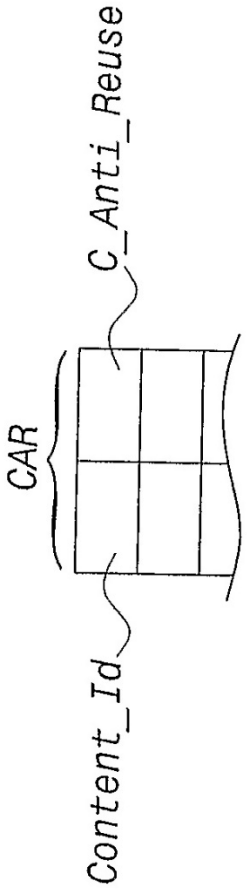

Fig.6

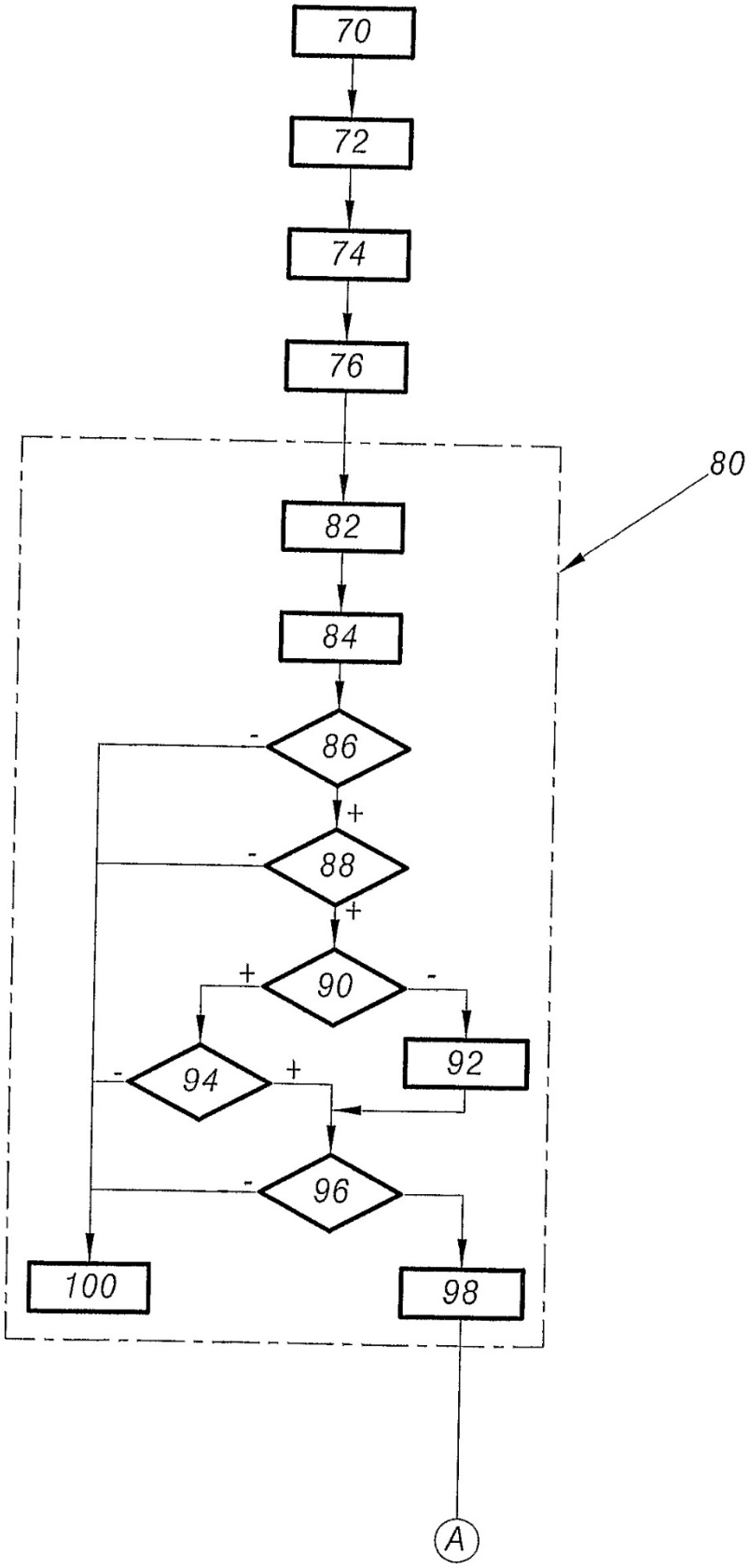

Fig. 7A

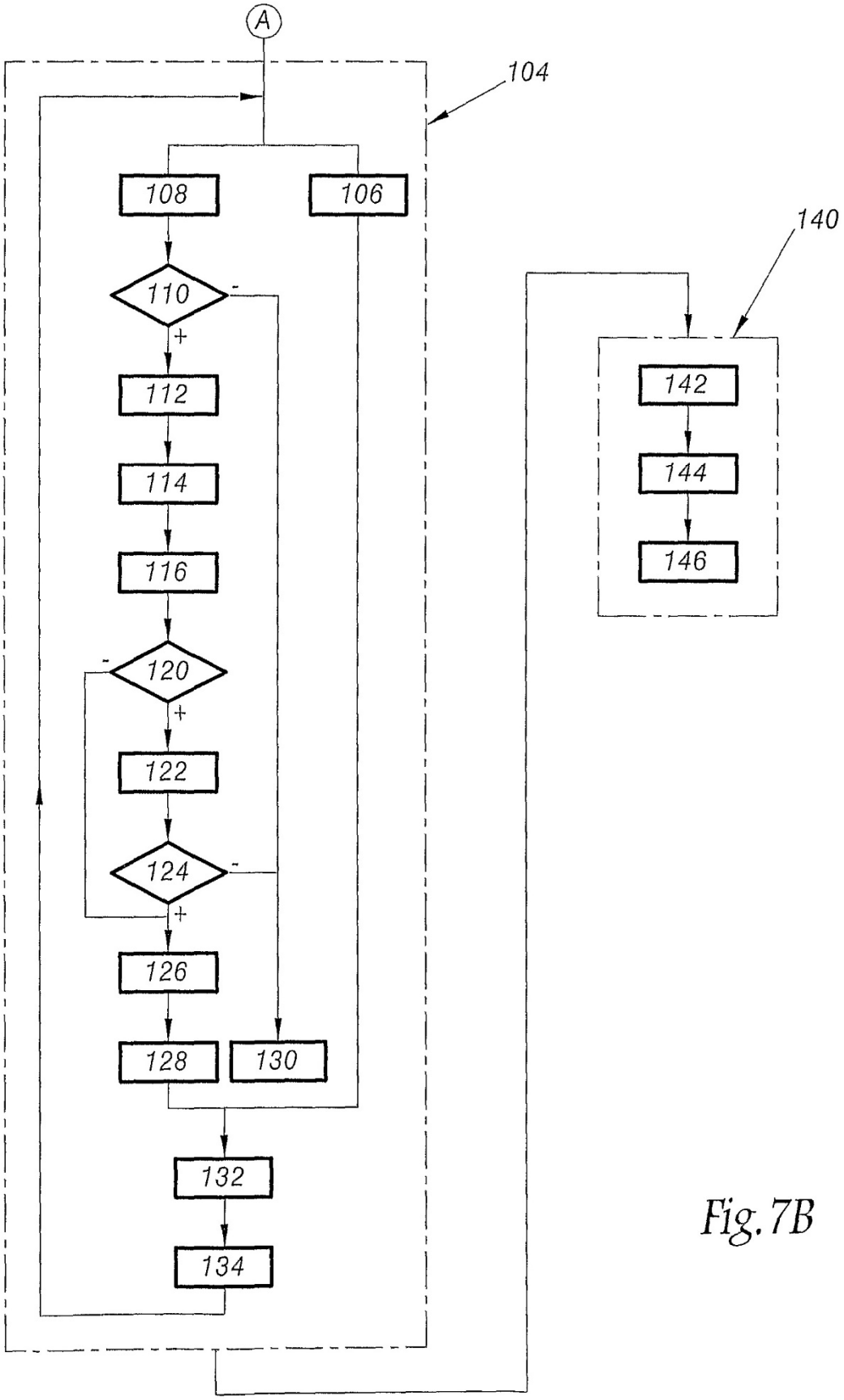
A
104
108
106
140
110
-
+
112
114
116
142
144
146
120
-
+
122
124
-
+
126
128
130
132
134

Fig. 7B

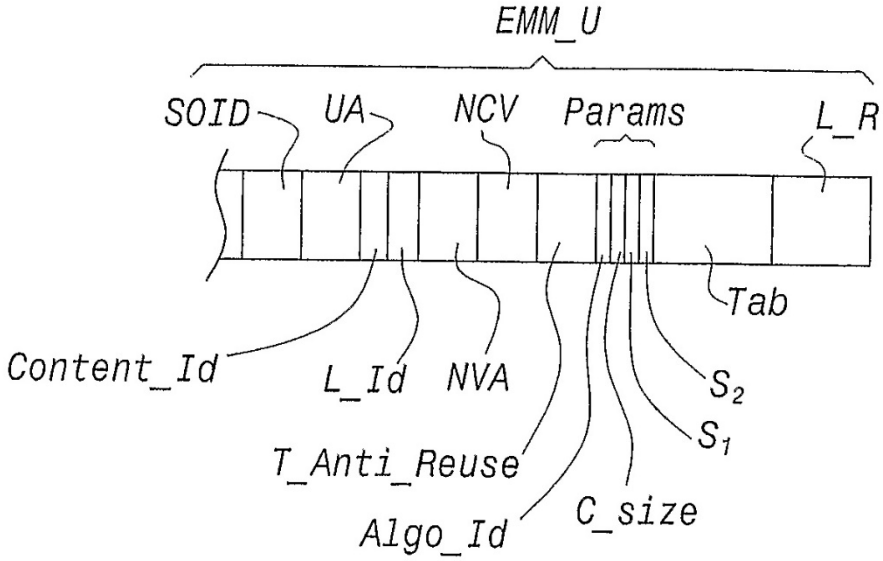

Fig.8

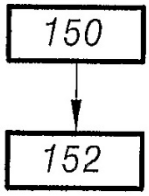

Fig.9

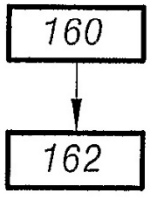

Fig.10

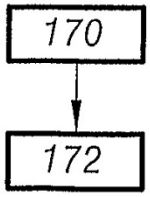

Fig.11