(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 745 401**

(51) Int. CI.:

***H04N 21/8355*** (2011.01)
***H04N 21/8358*** (2011.01)
***H04N 21/4405*** (2011.01)
***H04N 21/6334*** (2011.01)
*G06F 21/10* (2013.01)
*G06F 21/16* (2013.01)
*H04N 7/167* (2011.01)
*H04N 1/32* (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.04.2014 PCT/EP2014/058628**

(87) Fecha y número de publicación internacional: **30.10.2014 WO14174122**

(96) Fecha de presentación y número de la solicitud europea: **28.04.2014 E 14720130 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2019 EP 2989805**

(54) Título: **Procedimiento y dispositivo para el marcado de agua de un contenido comprimido cifrado mediante, por lo menos, una clave de contenido**

(30) Prioridad:

**26.04.2013 EP 13165597**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**02.03.2020**

(73) Titular/es:

**NAGRAVISION S.A. (100.0%)**
**22-24, route de Genève**
**1033 Cheseaux-sur-Lausanne, CH**

(72) Inventor/es:

**HUNACEK, DIDIER;**
**SERVET, PATRICK;**
**TRAN, MINH SON y**
**SARDA, PIERRE**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Procedimiento y dispositivo para el marcado de agua de un contenido comprimido cifrado mediante, por lo menos, una clave de contenido

**Técnica anterior**

El marcado de agua es una técnica utilizada para etiquetar contenidos protegidos. Esta etiqueta se utiliza para detectar utilización no autorizada o copias ilegales de los contenidos protegidos. La técnica de marcado de agua consiste en incrustar una marca digital en el contenido. Desde el punto de vista del aspecto, la marca digital incrustada puede ser invisible o visible. Desde el punto de vista de la naturaleza de la información, esta marca digital podría ser un valor único o un símbolo genérico, en función de qué desea monitorizar el propietario del contenido. Especialmente en el caso del valor único, la inserción de marcas de agua se podría realizar en el dispositivo cliente final, debido a que la marca deberá contener un identificador de este dispositivo.

El objetivo de la técnica de marcado de agua es ocultar tanto como sea posible la información oculta/de marcas incrustadas, mediante dispersar una de sus representaciones en el contenido. Para garantizar la discreción de la inserción de marcas sin comprometer la calidad, la inserción requiere generalmente una capacidad de computación compleja e incluso excesiva para determinados dispositivos. Por consiguiente, el cálculo completo se divide a menudo en procesos previo y posterior. El proceso previo lleva a cabo la mayor parte de las operaciones pesadas que generan algunas colas denominadas metadatos de marcado de agua (WMD, Watermarking Metadata), lo cual ayuda al proceso posterior, mucho más ligero, a insertar la marca de manera efectiva. "Dónde modificar", "cómo modificar" es habitualmente la información contenida en los WMD. Esto podría ser en forma de un archivo de registros previos al marcado, que contiene cada uno un índice de contenido en forma de una dirección del bloque a marcar y con, por lo menos, un valor alternativo. En el dispositivo cliente, cada registro es procesado y el valor alternativo es seleccionado (o no seleccionado) de acuerdo con el bit del identificador a incluir en el contenido.

Por lo tanto, la confidencialidad de los WMD así como su inserción se deberán garantizar, especialmente cuando se lleva a cabo el proceso posterior, dentro del dispositivo cliente, para evitar la posibilidad de filtrarlos, eliminarlos y/o cortarlos. En el dispositivo cliente, las técnicas existentes de procesamiento de marcado de agua digital están controladas generalmente por software de aplicación (CPU de anfitrión) del dispositivo, lo que significa que, en algunos casos, el contenido no protegido y todavía no marcado podría ser accesible por el software del dispositivo cliente. Por lo tanto, la seguridad del proceso de marcado de agua digital depende de la seguridad del software que corre en el dispositivo, es decir, de cómo de fácil es modificar y a continuación puentear el proceso de marcado de agua digital cuando el dispositivo es atacado satisfactoriamente, o simplemente abierto (sin autentificación de software).

El documento US2010/128871 describe una solución en la que se genera un flujo secundario que comprende los datos que permiten reconstruir el flujo principal y al mismo tiempo marcar el flujo reconstruido. Como consecuencia, el mismo flujo contiene los datos de aleatorización y los datos de marcado de agua. En la recepción, este flujo es procesado como un conjunto de datos a sustituir en el flujo modificado.

El documento EP 2 391 125 describe una solución para permitir un marcado individual (en el dispositivo de recepción), basado en un flujo común a todos los dispositivos. El objeto de control contiene el valor original, un valor alternativo y una localización. La unidad de seguridad determina una operación matemática a aplicar sobre el valor alternativo para recuperar el valor original. La operación matemática se modifica en función de un parámetro interno del dispositivo de recepción, de tal modo que la operación matemática será única por dispositivo, permitiendo rastrear este dispositivo si se analiza el flujo de datos de desaleatorización.

**Breve descripción de la invención**

El objetivo de la presente invención es imponer el marcado de agua sobre un contenido recibido por un dispositivo cliente, en particular para contenido de video comprimido.

La presente invención propone un procedimiento para el marcado de agua de un contenido comprimido recibido por un dispositivo cliente, recibiendo dicho dispositivo cliente un contenido comprimido cifrado, cifrado mediante por lo menos una clave de contenido (clave CA), datos CAS cifrados que comprenden dicha por lo menos una clave de contenido (clave CA), datos previos al marcado (WMD) y una firma de los datos previos al marcado, siendo dichos datos CAS cifrados mediante una primera clave de transmisión, comprendiendo dicho dispositivo cliente:

- un dispositivo condicionador (200) que comprende un identificador y la primera clave de transmisión,

- un desaleatorizador (103) que tiene una entrada para recibir el contenido comprimido cifrado y una salida para producir un contenido comprimido descifrado,

- un dispositivo de inserción de WM (104) conectado directamente a la salida del desaleatorizador, estando dicho desaleatorizador y dicho dispositivo de inserción de WM conectados con el dispositivo condicionador (200), comprendiendo dicho procedimiento las siguientes etapas ejecutadas por el dispositivo condicionador (200):

- recibir los datos CAS,

- descifrar los datos CAS con la primera clave de transmisión y extraer la clave de contenido (clave CA), los datos previos al marcado y la firma de los datos previos al marcado,

- verificar la firma de los datos previos al marcado y, si la firma es válida,

- transferir los datos previos al marcado y el identificador al dispositivo de inserción de WM,

- transferir la clave de contenido (clave CA) al desaleatorizador (103),

comprendiendo además dicho procedimiento:

- realizar marcado de agua mediante el dispositivo de inserción de WM (104) del contenido descifrado recibido por el desaleatorizador (103) utilizando los datos previos al marcado y el identificador, comprendiendo dichos datos previos al marcado por lo menos un índice de contenido, que define la localización en la que se puede realizar una modificación, y por lo menos un valor alternativo para insertar en dicha localización.

**Breve descripción de las figuras**

La presente invención se comprenderá mejor gracias a las figuras adjuntas, en las cuales:

- la figura 1 muestra un ejemplo del flujo de marcado de agua,

- la figura 2 muestra un diagrama de bloques del proceso de inserción de marcado de agua,

- la figura 3 muestra un diagrama de flujo del proceso de marcado de agua,

- la figura 4 muestra un ejemplo en el que los datos de marca de agua están contenidos en el flujo de datos.

**Descripción detallada**

Los datos de acceso condicional comprenden un contenido (datos de video o de audio, o una combinación de los mismos) cifrado mediante una o una serie de claves de contenido. El acceso a este contenido es posible gracias a los datos CAS, comprendiendo estos datos la clave o claves (clave CA) para descifrar el contenido cifrado, y los datos previos al marcado WM. Los WMD son un conjunto de registros que permiten al dispositivo de inserción de WM determinar dónde se puede realizar una modificación en el contenido desaleatorizado. Esto tiene generalmente la forma de un conjunto de registros, comprendiendo cada registro una localización (o dirección, desplazamiento, índice) y, por lo menos, un valor alternativo. Este valor alternativo puede (o no, dependiendo del bit a incrustar) sustituir el valor original en la localización específica en el contenido. En el caso de dos valores alternativos, el bit a incrustar como marca de agua se puede utilizar para seleccionar un valor o el otro. Los datos CAS comprenden asimismo condiciones de acceso asociadas con el contenido, que describen la condición que tiene que cumplir el descodificador para descifrar el contenido. El dispositivo condicionador comprende derechos de acceso que describen las condiciones de acceso del dispositivo cliente. Los derechos de acceso son cargados preferentemente en el dispositivo condicionador mediante un mensaje de gestión de habilitación (EMM, *Entitlement Management Message*) cifrado por una clave única para dicho dispositivo condicionador. Los datos de acceso condicional son difundidos, unidifundidos o enviados a petición del receptor. Los datos CAS pueden ser parte de los datos de acceso condicional (por ejemplo, un flujo secundario con un valor PID particular) o ser enviados independientemente al dispositivo cliente.

En el lado del servidor, el contenido comprimido es cifrado mediante una o una serie de claves, en el segundo caso, el contenido se divide y cada división es cifrada mediante una clave diferente. El servidor prepara asimismo los datos de marca de agua (WMD) como un conjunto de registros, mediante un módulo de análisis, con el fin de detectar posiciones de marcado posibles en el contenido comprimido (antes de la etapa de cifrado). El resultado del módulo de análisis es para producir por lo menos un valor alternativo por registro, este valor alternativo, cuando se sustituye en el contenido comprimido, no modifica visualmente el contenido pero puede ser detectado posteriormente. Los WMD o registros previos al marcado comprenden, para cada registro, un índice de contenido (es decir, la localización en la que se puede realizar la modificación) del contenido a modificar y el valor alternativo a introducir. Los registros previos al marcado no se determinan de acuerdo con un identificador particular, son tan sólo valores que pueden ayudar a que la marca de agua en el dispositivo cliente incruste la marca según un identificador local, sin procesamiento adicional (por lo tanto, reducen la complejidad requerida del dispositivo cliente).

Una vez recibidos en el dispositivo cliente, en caso de que los datos CAS estén incrustados en los datos de acceso condicional, estos son extraídos y transmitidos a un dispositivo condicionador (ver la figura 2) a cargo de la aplicación de las medidas de seguridad definidas en las condiciones de acceso condicional. Este módulo comprende la primera clave de transmisión necesaria para descifrar los datos CAS y para extraer de los datos CAS la clave (clave CA), para transferirla a continuación al desaleatorizador CA con el fin de descifrar el contenido. Además de la clave, este módulo extrae asimismo el WMD, cifrado mediante una segunda clave de transmisión. En caso de que los WMD estén en el mismo mensaje que la clave CA, una clave de transmisión se utiliza para cifrar el mensaje. En

una realización particular, la primera y la segunda clave es la misma transmisión y se utiliza para descifrar los datos CAS y el WMD. Se debe observar que la comunicación entre el dispositivo condicionador y el desaleatorizador CA está cifrada y protegida por una clave inicializada en ambos elementos. Otro procedimiento para garantizar que la comunicación entre estos dos elementos es segura es utilizar un bus dedicado, es decir, no accesible mediante la CPU de anfitrión (203) que corre en el dispositivo cliente.

Una protección similar aplica sobre la comunicación entre el dispositivo condicionador y el dispositivo de inserción de WM.

La solución propuesta protege a los WMD frente a espionaje, pero protege asimismo los WMD frente a cualquier filtrado o eliminación. La solución impone asimismo detecciones robustas de los WMD y garantiza también una inserción correcta de la marca. Aspectos similares de la invención pueden comprender un dispositivo condicionador que recibe los WMD, un desaleatorizador CA que desaleatoriza el contenido y un dispositivo de introducción de marcas de agua que inserta la marca utilizando los WMD.

La figura 1 es una aplicación a modo de ejemplo del proceso de marcado de agua. Por ejemplo, la cabecera 100 procesa previamente el contenido para encontrar las posiciones correctas para insertar una marca en el contenido comprimido con el fin de formar los WMD. En esa fase, los datos de marcado de agua son independientes del dispositivo cliente y son comunes a todos los dispositivos cliente. Esta información, junto con el contenido protegido por el sistema de acceso condicional (CAS, Conditional Access System) se transmite a continuación 101 al dispositivo cliente final, por ejemplo, utilizando el satélite. El contenido protegido 110 entra en el dispositivo. En este ejemplo mostrado por la figura 1, la clave CA utilizada para desaleatorizar el contenido y los WMD son transmitidos en el propio contenido. El dispositivo condicionador 102 extrae la clave CA protegida y los WMD protegidos del canal utilizado para transmitirlos. También descifra y autentica estas bi-tuplas: clave CA-WMD.

De acuerdo con una realización alternativa, el dispositivo condicionador transmite los datos CAS a un elemento seguro, es decir, la CPU segura 205 (ver la figura 2). Este elemento seguro puede ser parte del dispositivo cliente, por ejemplo, un entorno de software protegido dedicado a las operaciones de seguridad. Puede ser asimismo un elemento de seguridad desacoplable, tal como una tarjeta inteligente, un adaptador ("dongle") o un módulo PCMCIA. Una vez que los datos CAS son descifrados y autenticados por el elemento de seguridad, la clave CA y el WMD se devuelven al dispositivo condicionador. La comunicación entre estos dos elementos está preferentemente asegurada mediante una clave de emparejamiento, es decir, se carga la misma clave durante la fase de inicialización en el dispositivo condicionador y el elemento de seguridad.

El contenido protegido 111 es transmitido al desaleatorizador CA 103. Si el dispositivo condicionador 102 descifra satisfactoriamente la clave CA protegida y los WMD protegidos y autentica la clave CA y los WMD, podría transmitir la clave CA al desaleatorizador CA 103 y los WMD al dispositivo de inserción de WM 104. El desaleatorizador CA 103 utiliza la clave CA para desproteger el contenido 112. El contenido desprotegido va al dispositivo de inserción de WM 104. El dispositivo de inserción de WM 104 es responsable de sincronizar los WMD (que proceden del dispositivo condicionador 102) y el contenido para insertar la marca en las posiciones correctas. A continuación, el contenido marcado y desaleatorizado 113 se pasa al descodificador 105, que descodifica el contenido marcado. La TV 106 recibe un contenido marcado y descomprimido.

La autenticación se basa en firmas. Por ejemplo, los datos de marca de agua comprenden una firma para autenticar el origen de los datos. La firma es el resultado del cifrado de un compendio de la carga útil (por ejemplo, los registros previos al marcado). El compendio es calculado por el preprocesamiento de cabecera 100 (utilizando, por ejemplo, una función resumen) y cifrado mediante una clave de firma para producir la firma. La firma se añade al mensaje, y el mensaje es preferentemente cifrado mediante una clave de transmisión. En el lado de recepción, el mensaje es primero descifrado y se calcula el compendio sobre la carga útil. Con la clave correspondiente a la clave de firma, la firma recibida es descifrada y el resultado se compara con el compendio calculado. Si ambos valores son iguales, el mensaje es auténtico. La clave de firma puede ser una clave simétrica o una clave asimétrica (claves pública/privada).

La figura 2 es un diagrama de bloques que muestra un sistema robusto de inserción de marcas de agua. El dispositivo puede comprender un dispositivo condicionador 102, un desaleatorizador CA 103, una CPU de anfitrión 203, un dispositivo de inserción de WM 104 y, opcionalmente, una CPU segura 205.

La CPU segura 205, si se utiliza, puede comprender circuitos, lógica y/o código que garanticen el control y la personalización del proceso de marcado de agua. La CPU segura 205 deberá estar completamente aislada de la CPU de anfitrión 203, de tal modo que en la misma no se pueda ejecutar software (software inalterable) no de confianza.

El dispositivo condicionador 102 puede comprender circuitos, lógica y/o código que recibe (extrae), descifra y autentica la clave CA protegida y los WMD protegidos. Si se utiliza un código, este código deberá ser cifrado y autenticado por la CPU segura 205. El dispositivo condicionador 102 deberá asimismo tener acceso a un valor no modificable y de confianza 204 (identificador, marca de tiempo,…). El dispositivo condicionador 102 está asimismo a cargo de activar el dispositivo de inserción de WM 104. Las condiciones contenidas en los datos CAS pueden contener instrucciones para elegir el identificador que será implementado como marca de agua en el contenido. Este

podría ser un identificador único del dispositivo cliente, preferentemente almacenado en el entorno seguro del dispositivo condicionador, o un identificador contenido en los datos CAS (por ejemplo, un identificador del originador del contenido).

El desaleatorizador CA 103 puede comprender circuitos, lógica y/o código para desaleatorizar un contenido protegido con una clave CA procedente del dispositivo condicionador 102. Si se utiliza un código, este código deberá ser descifrado y autenticado por la CPU segura 205 y almacenado de manera segura.

El dispositivo de inserción de WM 104 puede comprender circuitos, lógica y/o código para insertar una marca en el contenido no protegido con las WMD y el identificador procedente del dispositivo condicionador 102. Si se utiliza un código, este código deberá ser descifrado y autenticado por la CPU segura 205. Otra tarea importante del dispositivo de inserción de WM 104 es sincronizar los WMD, que indican dónde insertar la marca, con el contenido.

La CPU de anfitrión 203 puede comprender circuitos, lógica y/o código que garanticen las funciones globales del dispositivo. La CPU de anfitrión 203 podría no tener acceso a la clave CA, a los WMD y al contenido no protegido entre el desaleatorizador CA 103 y el dispositivo de inserción de WM 104.

El enlace seguro 210, 211 y 212 puede comprender un bus privado, lógica y/o RAM no accesible por la CPU de anfitrión 203. Solamente las entidades conectadas mediante el enlace seguro podrían tener acceso a los datos transmitidos. Por ejemplo, solamente el desaleatorizador CA 103 y el dispositivo condicionador 102 podrían tener acceso a la clave CA.

Aparte de los procesos mencionados anteriormente, el objetivo de esta invención es asimismo impedir un filtrado fácil de los WMD protegidos. La clave CA protegida no podría ser eliminada por un atacante, o bien el contenido no sería descifrado. Para los WMD protegidos, el objetivo es ocultar lo máximo posible su detección, desde la perspectiva de la CPU de anfitrión 203. El escenario ideal será que los WMD protegidos puedan solamente ser extraídos y visibles desde el dispositivo condicionador 102. Sin embargo, en la mayor parte de los casos, los WMD protegidos son, sin embargo, accesibles mediante la CPU de anfitrión 203 y, por lo tanto, el objetivo es forzar a la CPU de anfitrión 203 a pasar los WMD protegidos al dispositivo condicionador 102. Antes de comentar algunos medios para obligar a que los WMD protegidos se pasen al dispositivo condicionador 102, la lista siguiente resume algunos posibles canales desde los que podrían proceder la clave CA protegida y los WMD protegidos:

- La clave CA protegida y los WMD protegidos podrían llegar directamente a través de Ethernet desde un servidor.

- La clave CA protegida y los WMD protegidos se podrían almacenar en un archivo de manifiesto (tal como DASH).

- La clave CA protegida y los WMD protegidos podrían ser incrustados en el contenido. Por ejemplo, el dispositivo condicionador 102 podría recibir la clave CA protegida en un ECM y los WMD protegidos podrían ser extraídos por el dispositivo condicionador 102 antes del desaleatorizador CA 103 (figura 1). Otro ejemplo mostrado en la figura 2 muestra que los WMD son incrustados en el contenido y están disponibles solamente después del desaleatorizador CA (línea de puntos 230 desde la salida del desaleatorizador). Los WMD son a continuación protegidos, es decir, cifrados con la clave CA. Un filtro está situado a la salida del desaleatorizador CA, de tal modo que el flujo secundario de los WMD es extraído y transferido al dispositivo condicionador. Los WMD extraídos del desaleatorizador CA pueden cifrarse adicionalmente mediante una clave WM específica conocida por el dispositivo condicionador. Para controlar la autenticidad de los WMD, estos datos pueden contener además una firma. Estos datos están organizados en paquetes, y cada paquete contiene una firma del paquete. La firma, como un ejemplo de realización, es el valor resumen de los otros datos del paquete, siendo este valor de resumen cifrado mediante una clave de firma. Cuando el dispositivo condicionador recibe los WMD, descifra a continuación la firma del paquete y la compara con un valor resumen de los datos del paquete. Si la firma es verificada satisfactoriamente, el dispositivo condicionador valida la clave CA actual y sigue alimentando el desaleatorizador CA con las claves CA futuras; en caso contrario, se habilita el mecanismo de bloqueo descrito anteriormente.

En esta configuración, el dispositivo condicionador 200 debería cargar primero la clave CA en el desaleatorizador CA 103 antes de recibir los WMD. Para este propósito, el dispositivo condicionador comprende un temporizador que se inicializa cuando la clave CA se carga en el desaleatorizador. Si después de un primer tiempo predeterminado los WMD no son recibidos por el dispositivo condicionador, este bloquea el desaleatorizador. Esto se puede realizar enviando una clave CA falsa al desaleatorizador, o bloqueando la transmisión adicional de las nuevas claves CA. El temporizador puede ser utilizado para liberar el bloqueo después de un segundo tiempo predefinido. Cuando este segundo tiempo se cumple, el dispositivo condicionador transfiere la clave CA actual y espera la recepción de los WMD. El temporizador se reinicializa si los WMD no se reciben durante el primer tiempo predefinido, el dispositivo condicionador vuelve a entrar en el modo de bloqueo.

En la realización en que se envían juntos la clave CA y los WDM, la idea principal para forzar que los WMD protegidos sean proporcionados al dispositivo condicionador 102 es vincular de forma criptográfica la clave CA y los WDM con un mecanismo de firma (por ejemplo, SHA-256). Este cálculo podría ser gestionado solamente en el dispositivo condicionador 102. Por ejemplo, un contenido de video a la carta es cifrado con una clave CA única y todos los WMD protegidos son almacenados en un archivo. Para descifrar el contenido, el dispositivo condicionador 102 deberá recibir la clave CA protegida y todos los WMD protegidos, de lo contrario la verificación de firma

realizada sobre la clave CA y los WMD fallará y el contenido no será descifrado debido a que el dispositivo condicionador 102 no proporcionará la clave CA al desaleatorizador CA 103.

Sin embargo, la vinculación criptográfica entre la clave CA y los WMD no siempre es posible. Por ejemplo, la clave CA está completamente no correlacionada con los datos de medios protegidos, que están estrechamente enlazados con los WMD en una transmisión MPEG-TS. Los propios WMD pueden ser asimismo protegidos con una clave CA, como una clase de datos de medios. En este caso, los WMD protegidos serán invisibles para la perspectiva de la CPU de anfitrión 203. Solamente el dispositivo condicionador 102 puede detectarlos y utilizarlos. Para ilustrar esto, la figura 4 muestra la transmisión de contenido MPEG-2 TS. En este ejemplo, los WMD son incluidos en un flujo elemental paquetizado (PES, *Packetized Elementary Stream*) particular y a continuación se mezclan conjuntamente con otros PES del contenido. La carga útil de estos PES es cifrada mediante una clave, conocida solamente por el dispositivo condicionador 102. Estos PES y los PES normales son encapsulados en paquetes TS, y a continuación cifrados por el aleatorizador (por ejemplo, DVB-CSAV2). Desde la perspectiva de la CPU de anfitrión 203, no existen diferencias entre un paquete TS que contiene un PES normal y el que contiene un PES WMD. El desaleatorizador CA 103 descifra el paquete TS, y a continuación el dispositivo condicionador 102 detecta los WMD protegidos utilizando indicadores específicos. A continuación, este podría descifrarlos y pasarlos al dispositivo de inserción de WM 104.

Otro ejemplo mostrado en la figura 1 se centra en cómo imponer el proceso de marcado de agua. El dispositivo condicionador 102 está situado antes del desaleatorizador CA 103. El dispositivo condicionador 102 extrae los WMD protegidos y a continuación los descifra. En este caso, la detección de los WMD protegidos es más sencilla y, potencialmente, puede ser realizada por la CPU de anfitrión 203. Para impedir el filtrado de los WMD protegidos, se utiliza la técnica de marcado descrita en la solicitud de patente publicada con el número EP2458890. Con esta técnica, si se filtran los WMD protegidos, el contenido sufrirá una considerable degradación. De acuerdo con este ejemplo, el contenido desaleatorizado por el desaleatorizador CA no es igual que el original y se denomina contenido modificado. Este contenido modificado sigue comprendiendo algunos valores (por ejemplo, coeficientes de correlación) alterados por la cabecera, los valores originales formando parte de los datos de marcado de agua. Durante el proceso de marcado de agua, ejecutado por el dispositivo de inserción de WM, el registro previo a la marca de agua comprende dos valores, siendo uno el valor original y el otro un valor alternativo. Este valor alternativo se elige de manera que el impacto visual sea mínimo.

La figura 3 es un diagrama de flujo de un proceso de marcado de agua de ejemplo. En la etapa 301, después del inicio en la etapa 300, el dispositivo condicionador 102 está a cargo de recibir, descifrar y autenticar la clave CA y los WMD. En la etapa 302, el dispositivo condicionador descifra y verifica la firma realizada en la clave CA y los WMD. Si la clave CA y los WMD no pudieran ser autenticados correctamente, el contenido no se descifraría debido a que el dispositivo condicionador 102 no proporcionará la clave CA al desaleatorizador CA 103 (etapa 304). Usando este artificio, se obliga a que la CPU de anfitrión 203 pase la clave CA protegida y los WMD protegidos al dispositivo condicionador 102 sin ninguna modificación o filtrado. Si todo es correcto, el dispositivo condicionador 102 está asimismo a cargo de proporcionar los WMD y el valor de confianza al dispositivo de inserción de WM al mismo tiempo que la clave CA para el desaleatorizador CA 103 (etapa 303). El valor de confianza se utiliza para identificar de manera única el dispositivo. Por ejemplo, este valor de confianza podría establecerse y bloquearse en la configuración del dispositivo.

Este valor de confianza, como parte del dispositivo, es accesible por el dispositivo condicionador y además no es modificable por ninguna entidad del dispositivo. Se pueden realizar algunos cálculos sobre este valor de confianza dentro del dispositivo condicionador antes de que sea utilizado como carga útil de marca de agua, para mejorar la robustez de esta carga útil. Por ejemplo, el valor de confianza podría ser un identificador único que puede ser transformado/mejorado por medio de un ECC o un código anti-colusión, tal como un código Tardos.

A continuación, en la etapa 305, el desaleatorizador CA desaleatoriza el contenido protegido. Después de esto, en la etapa 307, este contenido no protegido se proporciona al dispositivo de inserción de WM para ser marcado. El dispositivo de inserción de WM utiliza los WMD y el valor de confianza para insertar correctamente la marca en el contenido. El contenido no protegido nunca es accesible por la CPU de anfitrión antes de que haya sido marcado correctamente. En la etapa 308, si están entrando otra clave CA y/o nuevos WMD protegidos, el proceso saltará a la etapa 301.

El dispositivo de inserción de WM puede comprender un módulo de verificación a cargo de comprobar que el contenido comprimido es uno que es realmente descifrado por el desaleatorizador. La primera verificación se basa en la recepción de datos comprimidos. Si no se reciben datos a la entrada del dispositivo de inserción de WM, se devuelve un mensaje al dispositivo condicionador, que como consecuencia se detiene para proporcionar la clave CA al desaleatorizador.

Otra verificación, que puede ser añadida a la anterior o implementada independientemente, se dirige a reconocer el contenido a someter a marca de agua. Los registros WM no solamente comprenden el índice de contenido y un valor alternativo, sino asimismo el valor original del contenido en la localización señalada por el índice de contenido. Durante la etapa de marcado de agua, el dispositivo de inserción de WM decide cambiar el valor original del contenido por un valor alternativo (o dejar el original), de acuerdo con el valor de un bit del identificador. Además de

esta operación, el dispositivo de inserción de WM puede leer el valor original del contenido comprimido desaleatorizado y compararlo con el valor original contenido en el registro previo al marcado. Si los valores son iguales, el contenido actualmente en proceso es el genuino. Si el valor original leído del contenido es diferente, esto significa que se alimenta otro contenido comprimido a la entrada del dispositivo de inserción de WM. En este caso, se envía un mensaje al dispositivo condicionador para adoptar la acción apropiada (deshabilitar la clave CA, por ejemplo).

**REIVINDICACIONES**

1. Procedimiento para el marcado de agua de un contenido comprimido recibido por un dispositivo cliente, recibiendo dicho dispositivo cliente un contenido comprimido cifrado, cifrado mediante por lo menos una clave de contenido (clave CA), datos CAS cifrados que comprenden dicho por lo menos una clave de contenido (clave CA), datos previos al marcado (WMD) y una firma de los datos previos al marcado, estando cifrados dichos datos CAS mediante una primera clave de transmisión, comprendiendo dicho dispositivo cliente:

- un dispositivo condicionador (200) que comprende un identificador y la primera clave de transmisión,

- un desaleatorizador (103) que tiene una entrada para recibir el contenido comprimido cifrado y una salida para producir un contenido comprimido descifrado,

- un dispositivo de inserción de WM (104) conectado directamente a la salida del desaleatorizador,

estando conectados dicho desaleatorizador y dicho dispositivo de inserción de WM con el dispositivo condicionador (200), comprendiendo dicho procedimiento las siguientes etapas ejecutadas por el dispositivo condicionador (200):

- recibir los datos CAS,

- descifrar los datos CAS con la primera clave de transmisión y extraer la clave de contenido (clave CA), los datos previos al marcado y la firma de los datos previos al marcado,

- verificar la firma de los datos previos al marcado y, si la firma es válida,

- transferir los datos previos al marcado y el identificador al dispositivo de inserción de WM,

- transferir la clave de contenido (clave CA) al desaleatorizador (103),

dicho procedimiento comprende además:

- realizar marcado de agua mediante el dispositivo de inserción de WM (104) del contenido descifrado recibido por el desaleatorizador (103) utilizando los datos previos al marcado y el identificador, comprendiendo dichos datos previos al marcado por lo menos un índice de contenido, que define la localización en la que se puede realizar una modificación, y por lo menos un valor alternativo para insertar en dicha localización.

2. Procedimiento según la reivindicación 1, en el que los datos previos al marcado están organizados en paquetes, comprendiendo cada paquete una firma y un conjunto o registros, comprendiendo cada registro un índice de contenido y un valor alternativo, para un determinado índice de contenido, decidiendo el dispositivo de inserción de WM cambiar o mantener el valor original del contenido en el índice de contenido en base a un bit del identificador.

3. Procedimiento según cualquiera de las reivindicaciones 1 a 2, en el que el dispositivo cliente comprende una CPU de anfitrión a cargo de hacer funcionar un sistema operativo, y en el que el dispositivo condicionador, el desaleatorizador y el dispositivo de inserción de WM están localizados en un entorno seguro y las conexiones entre estos elementos no son accesibles por la CPU de anfitrión.

4. Procedimiento según la reivindicación 1, en el que los datos previos al marcado son incrustados en el contenido cifrado, y descifrados mediante el desaleatorizador CA, comprendiendo dicho procedimiento las etapas de:

- extraer a la salida del desaleatorizador CA los datos previos al marcado, y transferirlos al dispositivo condicionador.

5. Procedimiento según cualquiera de las reivindicaciones 2 a 4, en el que el registro previo al marcado comprende además el valor original en el índice de contenido, verificando dicho dispositivo de inserción de WM (104) que el valor en el contenido es el mismo que el valor original del registro previo al marcado, e informando además al dispositivo condicionador (200) del resultado de la verificación.

6. Procedimiento según la reivindicación 5, en el que los datos CAS comprenden condiciones de acceso, siendo comprobadas estas condiciones de acceso mediante el dispositivo condicionador (200) antes de que la clave de contenido sea transferida al desaleatorizador CA (103).

7. Dispositivo cliente para el descifrado y marcado de agua de un contenido comprimido cifrado, utilizando datos CAS que comprenden dicho por lo menos una clave de contenido (clave CA), datos previos al marcado (WMD) y una firma de los datos previos al marcado, estando dichos datos CAS cifrados mediante una primera clave de transmisión, comprendiendo dicho dispositivo cliente:

- un dispositivo condicionador (200) que comprende un identificador y la primera clave de transmisión,

- un desaleatorizador (103) que tiene una entrada para recibir el contenido comprimido cifrado y una salida para producir un contenido comprimido descifrado,

- un dispositivo de inserción de WM (104) conectado directamente a la salida del desaleatorizador, estando dicho desaleatorizador y dicho dispositivo de inserción de WM conectados con el dispositivo condicionador (200),

comprendiendo dicho dispositivo condicionador (200) medios para:

- recibir los datos CAS,
- descifrar los datos CAS con la primera clave de transmisión y extraer la clave de contenido (clave CA),
- descifrar los datos previos al marcado,
- verificar la firma de los datos previos al marcado y, si la firma es válida,
- transferir los datos previos al marcado y el identificador al dispositivo de inserción de WM, y
- transferir la clave de contenido (clave CA) al desaleatorizador (103),

comprendiendo dicho dispositivo de inserción de WM (104) medios para:

- realizar marcado de agua del contenido descifrado recibido por el desaleatorizador (103) utilizando los datos previos al marcado y el identificador, comprendiendo dichos datos previos al marcado por lo menos un índice de contenido, que define la localización en la que se puede realizar una modificación, y por lo menos un valor alternativo para insertar en dicha localización.


Fig. 1

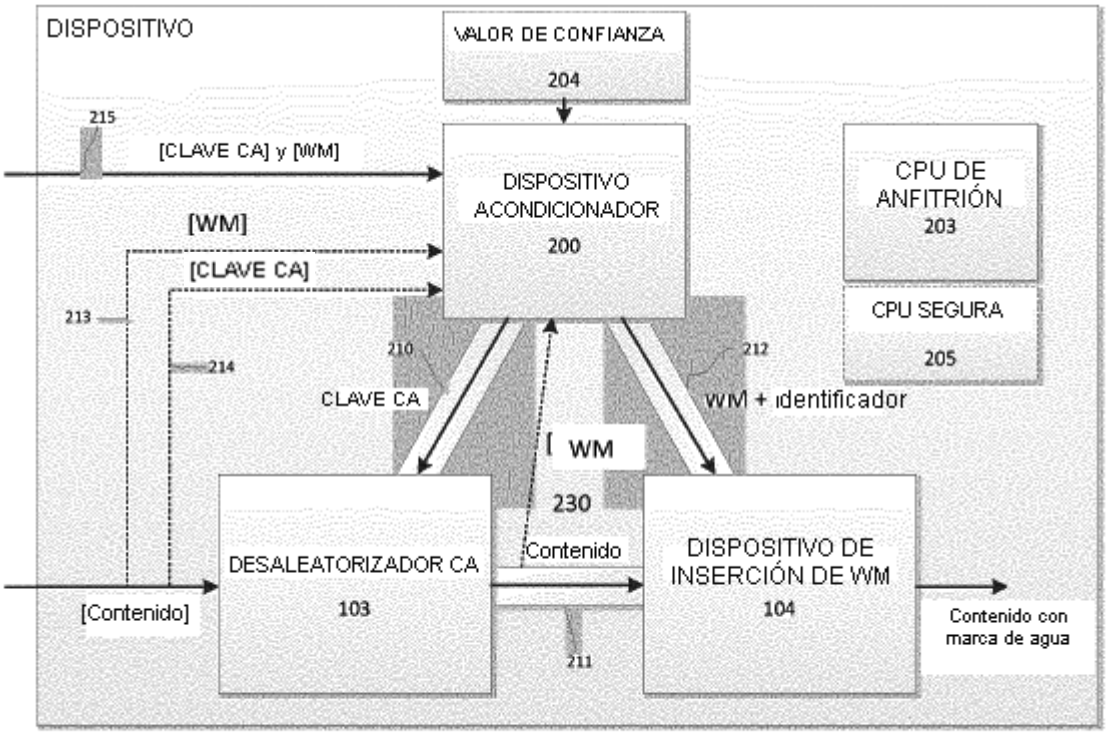


Fig. 2

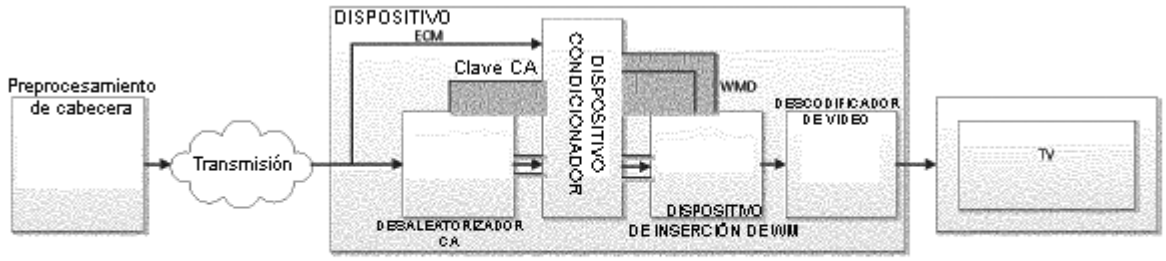


Fig. 4

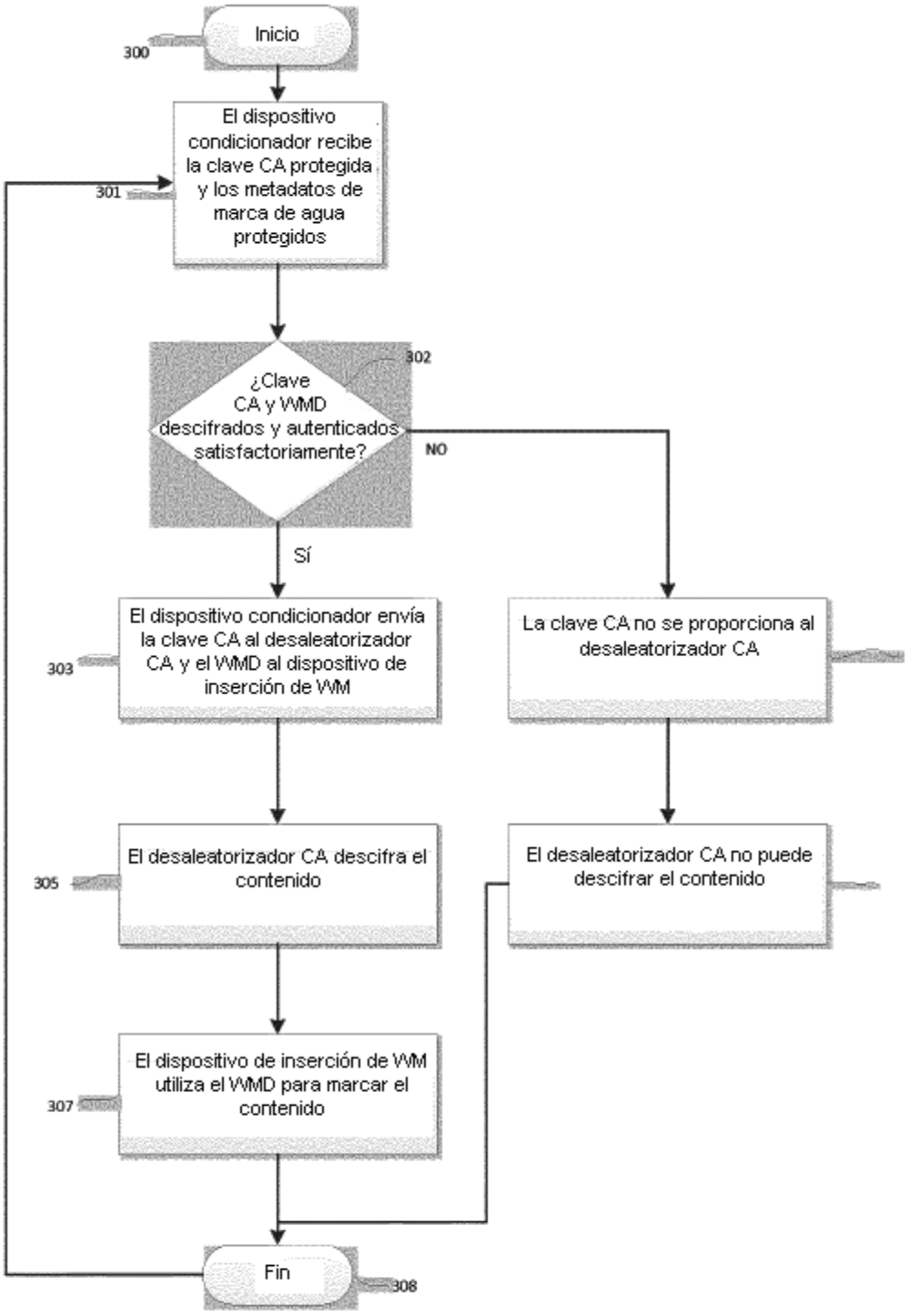
Inicio
300
El dispositivo condicionador recibe la clave CA protegida y los metadatos de marca de agua protegidos
301
¿Clave CA y WMD descifrados y autenticados satisfactoriamente?
302
NO
Sí
El dispositivo condicionador envía la clave CA al desaleatorizador CA y el WMD al dispositivo de inserción de WM
303
La clave CA no se proporciona al desaleatorizador CA
El desaleatorizador CA descifra el contenido
305
El desaleatorizador CA no puede descifrar el contenido
El dispositivo de inserción de WM utiliza el WMD para marcar el contenido
307
Fin
308

Fig. 3