(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 173**

(51) Int. CI.:
G11B 20/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06117438 .9**
(96) Fecha de presentación: **18.07.2006**
(97) Número de publicación de la solicitud: **1746594**
(97) Fecha de publicación de la solicitud: **24.01.2007**

(54) Título: **Método y aparato para desaleatorizar de manera eficaz una parte transformada de contenido**

(30) Prioridad:
19.07.2005 US 700336 P
22.07.2005 US 701493 P
28.07.2005 US 703003 P
12.07.2006 KR 20060065179

(45) Fecha de publicación de la mención BOPI:
10.10.2012

(45) Fecha de la publicación del folleto de la patente:
10.10.2012

(73) Titular/es:
Samsung Electronics Co., Ltd.
129, Samsung-ro Yeongtong-gu
Suwon-si, Gyeonggi-do, 443-742, KR

(72) Inventor/es:
You, Yong-kuk;
Chung, Hyun-Kwon;
Shin, Jun-bum;
Choi, Yun-ho y
Nam, Su-hyun

(74) Agente/Representante:
Curell Aguilá, Mireia

DESCRIPCIÓN

Método y aparato para desaleatorizar de manera eficaz una parte transformada de contenido.

Los métodos y aparatos en concordancia con la presente invención se refieren a la restauración de contenido y más particularmente, un aspecto de la invención se refiere a un método y un aparato para restablecer de manera eficaz una parte transformada de contenido.

La normativa del AACS (Sistema de Contenido de Sistema Avanzado), el cual es un sistema de protección de discos ópticos de la siguiente generación, usa un esquema de cifrado de radiodifusión que no permite que un reproductor al que se le ha revocado un conjunto de claves de dispositivo debido a una acción de piratería informática y otras, descifre contenido cifrado de acuerdo con el esquema de cifrado de radiodifusión. En el esquema de cifrado de radiodifusión, a cada reproductor se le asigna un conjunto de claves de dispositivo diferente, y en los discos que se han distribuido al público no se almacena una clave intermedia cifrada usando un conjunto revocado de claves de dispositivo, lo cual evita que un reproductor al que se le haya revocado el conjunto de claves de dispositivo adquiera la clave intermedia. De este modo, el reproductor al que se le ha revocado el conjunto de claves de dispositivo no puede obtener una clave de descifrado de contenido.

No obstante, incluso si no se da a conocer el conjunto de claves de dispositivo, se puede crear un software de piratería informática basándose en defectos estructurales de un modelo de reproductor específico. En este caso, con el software de piratería informática se puede piratear un número elevado de reproductores, y por lo tanto, resulta imposible revocar todos los conjuntos de claves de dispositivo asignados a los reproductores pirateados con el fin de hacer frente a esta situación.

Para resolver este problema, se ha introducido un esquema de renovación de contenido individual con el fin de controlar la restauración de contenido mediante el uso de código programable para cada contenido. En el esquema de renovación, en un disco se almacena código de seguridad que controla la restauración del contenido. El código de seguridad se ejecuta antes de la reproducción del contenido con el fin de determinar si existen problemas en la reproducción del mismo. Por ejemplo, se determina si se ha revelado un conjunto de claves de dispositivo del reproductor o si se ha instalado o se está ejecutando un software de piratería informática. A continuación, el contenido se restaura únicamente cuando se determina que no existe ningún problema en el proceso de reproducción del mismo. En otras palabras, resulta difícil actualizar un reproductor ya vendido, pero un disco se puede actualizar al nivel de los contenidos almacenando en el mismo el código de seguridad.

La figura 1 es un diagrama de bloques de un reproductor de medios convencional 1. En referencia a la figura 1, el reproductor de medios convencional 1 incluye una interfaz de medios 11, una máquina virtual 12, una memoria 13, una unidad de descifrado/decodificación 14, y una interfaz de salida 15.

La interfaz de medios 11 lee contenido y código de seguridad, el cual es un programa que protege el contenido, a partir de un medio, tal como un disco de vídeo digital (DVD) y un disco compacto (CD).

La máquina virtual 12 ejecuta el código de seguridad leído por la interfaz de medios 11 para generar información del reproductor de medios 1, y compara la información generada con información del reproductor de medios 1 que se ha almacenado en la memoria 13. Seguidamente, la máquina virtual 12 determina si se ha revelado un conjunto de claves de dispositivo de reproductor de medios 1 o si se ha instalado o se está ejecutando un software de piratería informática del mismo basándose en el resultado de la comparación, y adicionalmente ejecuta el código de seguridad para generar información con el fin de controlar la restauración del contenido únicamente cuando se determina que no se ha revelado el conjunto de claves de dispositivo del reproductor de medios 1 ó no se ha instalado o no se está ejecutando el software de piratería informática del mismo que no se ha distribuido.

La unidad de descifrado/decodificación 14 descifra y decodifica el contenido, que es leído por la interfaz de medios 11, usando la información generada por la máquina virtual 12. Si el contenido está cifrado de acuerdo con normativas de protección de contenido, tales como las normativas CSS o las normativas AACS, la unidad de descifrado/decodificación 14 descifra contenido leído por la interfaz de medios 11 de acuerdo con las normativas de protección de contenido usadas para cifrar el contenido. Si el contenido se codifica de acuerdo con las normativas MPEG-2, el contenido se decodifica de acuerdo con las normativas MPEG-2.

La interfaz de salida 15 da salida al contenido, que fue descifrado y decodificado por la unidad de descifrado/decodificación 14, hacia un dispositivo de visualización, tal como una Televisión digital (DTV).

Tal como se ha descrito anteriormente, un esquema de renovación de contenido individual, convencional, proporciona una solución para controlar la restauración de contenido en función de si se ha revelado un conjunto de claves de dispositivo de un reproductor de medios o si el entorno de seguridad correspondiente al reproductor de medios es normal. No obstante, el esquema de renovación de contenido individual, convencional, no proporciona una solución para proteger el contenido, por ejemplo, contra ataques frecuentes de un pirata informático durante toda la reproducción de contenido.

Según la presente invención, se proporciona un aparato y un método de acuerdo con lo expuesto en las reivindicaciones adjuntas. A partir de las reivindicaciones dependientes, y de la descripción que se ofrece a continuación, se pondrán de manifiesto características preferidas de la invención.

Un aspecto de la presente invención proporciona un aparato y un método para restablecer de manera eficaz contenido que se transforma para protegerlo contra ataques frecuentes de un pirata informático durante toda la reproducción del contenido.

Un aspecto de la presente invención proporciona también un medio legible por ordenador que tiene grabado en el mismo un programa de ordenador para ejecutar el método anterior.

Según un aspecto de la presente invención, se proporciona un método de restablecimiento de contenido, el método incluye comprobar información de restablecimiento en relación con un primer paquete de paquetes que constituyen el contenido, usándose la información de restablecimiento para restablecer una parte transformada de contenido; extraer información de ubicación de un segundo paquete de entre los paquetes a partir de la información de restablecimiento del primer paquete comprobado, conteniendo el segundo paquete datos de restablecimiento para restablecer la parte transformada del contenido; y restablecer la parte transformada del contenido usando los datos de restablecimiento del segundo paquete indicado por la información de ubicación extraída.

Según otro aspecto de la presente invención, se proporciona un medio legible por ordenador que tiene grabado en el mismo un programa de ordenador para ejecutar el método anterior.

Según otro aspecto de la presente invención, se proporciona un aparato para restablecer contenido, incluyendo el aparato una unidad de comprobación que comprueba información de restablecimiento en relación con un primer paquete de entre paquetes que constituyen el contenido, y que extrae información de ubicación de un segundo paquete de entre los paquetes a partir de la información de restablecimiento comprobada, en donde la información de restablecimiento se usa para restablecer una parte transformada del contenido y el segundo paquete contiene datos de restablecimiento para restablecer la parte transformada del contenido; y una unidad de restablecimiento que restablece selectivamente la parte transformada del contenido basándose en la información de restablecimiento del primer paquete comprobado por la unidad de comprobación.

Los aspectos y ventajas anteriores y otros de la presente invención se pondrán de manifiesto mediante la descripción detallada de formas de realización ejemplificativas de los mismos en referencia a los dibujos adjuntos, en los cuales:

la figura 1 es un diagrama de bloques que ilustra un reproductor de medios convencional;

la figura 2 es un diagrama que ilustra un método de protección de contenido de acuerdo con una forma de realización de la presente invención;

la figura 3 es un diagrama de bloques de un reproductor de medios de acuerdo con una forma de realización de la presente invención;

la figura 4 es un diagrama que ilustra un proceso de comprobación de información de restablecimiento de acuerdo con una forma de realización de la presente invención; y

las figuras 5 y 6 son diagramas de flujo que ilustran un método de restauración de contenido de acuerdo con una forma de realización de la presente invención.

A continuación, en lo sucesivo en la presente memoria, se describirán detalladamente formas de realización ejemplificativas según la presente invención, en referencia a los dibujos adjuntos.

La figura 2 es un diagrama que ilustra un método de protección de contenido de acuerdo con una forma de realización ejemplificativa de la presente invención.

Tal como se ha descrito anteriormente, el esquema de renovación de contenido individual, convencional, no proporciona una solución para proteger contenido, por ejemplo, contra ataques frecuentes de un pirata informático durante toda la reproducción del contenido. De este modo, es probable que el código de región de un disco de vídeo digital (DVD), por ejemplo, se desactive fácilmente simplemente usando una operación sencilla de un mando a distancia. En particular, cuando la restauración del contenido se controla usando un número pequeño de órdenes de control sencillas, el esquema de renovación de contenido individual, convencional, se puede desactivar con solamente unos pocos ataques durante el estado inicial de reproducción del contenido. Para evitar este problema, según una forma de realización de la presente invención, el contenido se aleatoriza (*scrambled* en inglés) para ser transformado, y diversas informaciones necesarias para desaleatorizar (*descrambled* en inglés) el contenido aleatorizado son independientes entre sí, y el código de seguridad se asigna de manera que contiene las diversas informaciones. Así, el código de seguridad se usa continuamente para desaleatorizar el contenido aleatorizado.

No obstante, la aleatorización del contenido completo puede incrementar la carga sobre el sistema en función de la especificación de este último. Por consiguiente, según una forma de realización de la presente invención, algunas partes separadas del contenido se aleatorizan para transformar el contenido según se ilustra en la figura 2, evitándose así de manera suficiente que un usuario visione el contenido. Partes del contenido transformado por aleatorización se pueden restablecer usando diversos métodos. En primer lugar, el código de seguridad contiene diversa información necesaria para restablecer las partes transformadas del contenido. En este caso, puesto que el código de seguridad contiene una gran cantidad de datos, la carga sobre el sistema se incrementa significativamente en un entorno que requiera que el código de seguridad se ejecute continuamente para reproducir el contenido.

En segundo lugar, el código de seguridad contiene una parte de la información necesaria para restablecer una parte transformada de contenido y el contenido contiene la mayoría de la información. En este caso, es importante determinar fácilmente qué parte del contenido almacena la información para restablecer la parte transformada del contenido. Así, en una forma de realización de la presente invención, información para restablecer una parte transformada del contenido se almacena en una región reservada de un paquete de la tabla de correspondencia de programas ("*program map table",* en inglés), (PMT) de acuerdo con el (MPEG)-2 del Grupo de Expertos de Imágenes en Movimiento. No obstante, resultará evidente para aquellos con conocimientos comunes en la materia que, para almacenar la información, se pueden usar tipos de paquetes diferentes al paquete de PMT.

En tercer lugar, en un paquete de PMT que contiene información para restablecer sustancialmente una parte transformada de contenido se inserta una bandera para diferenciar el paquete de PMT con respecto a paquetes generales. No obstante, en este caso, todos los paquetes se deben analizar sintácticamente para detectar el paquete de PMT que contiene la información para restablecer la parte transformada del contenido. Para resolver este problema, en una forma de realización de la presente invención, en un paquete de PMT se inserta información de ubicación de un paquete de PMT sucesivo que contiene información para restablecer una parte transformada de contenido.

La figura 3 es un diagrama de bloques de un reproductor de medios 3 de acuerdo con una forma de realización ejemplificativa de la presente invención. En referencia a la figura 3, el reproductor de medios 3 incluye una interfaz de medios 31, una máquina virtual 32, una memoria 33, una unidad de descifrado 34, una unidad de comprobación 35, una unidad de restablecimiento 36, una unidad de decodificación 37, y una interfaz de salida 38.

La interfaz de medios 31 lee contenido y código de seguridad, que es un programa para proteger el contenido, a partir de un medio, tal como un DVD o un disco compacto (CD). Además, la interfaz de medios 31 puede soportar el almacenamiento temporal del contenido para adaptarse a la velocidad de descifrado de la unidad de descifrado 34 ó la velocidad de decodificación de la unidad de decodificación 37.

En una forma de realización de la presente invención, un ejemplo representativo de contenido es un título audiovisual (AV) codificado de acuerdo con la normativa MPEG-2. Además, se puede proteger contenido de acuerdo con varios métodos. Por ejemplo, el contenido se puede cifrar usando una clave del sistema de aleatorización de contenidos (CSS) de acuerdo con la normativa CSS o usando una clave de título de acuerdo con la normativa del sistema de contenido de acceso avanzado (AACS). Si no, de acuerdo con una forma de realización ejemplificativa de la presente invención, el contenido se puede transformar aleatorizando partes separadas del mismo.

La máquina virtual 32 ejecuta el código de seguridad leído por la interfaz de medios 31 para generar información del reproductor de medios 3, y compara información del reproductor de medios 3 almacenada en la memoria 33 con la información generada del reproductor de medios 3 en el código de seguridad. Seguidamente, la máquina virtual 32 determina si se ha revelado un conjunto de claves de dispositivo del reproductor de medios 3 ó se ha instalado o se está ejecutando un software de piratería del mismo, basándose en el resultado de la comparación, y además ejecuta el código de seguridad para generar información con el fin de restablecer una parte transformada del contenido (a la que en lo sucesivo se hará referencia como “información de restablecimiento”) únicamente cuando se determina que no se ha revelado el conjunto de claves de dispositivo del reproductor de medios 3 y no se ha instalado o no se está ejecutando un software de piratería del mismo. Por ejemplo, la máquina virtual 32 se puede materializar en forma de una máquina virtual Java, y el código de seguridad se puede materializar en forma de un programa Java al que también se hace referencia como código de bytes Java. La máquina virtual Java interpreta el código de bytes Java, y ejecuta el código interpretado de manera que resulte apropiado para una plataforma (Window, UNIX, McIntosh, etcétera) en la cual está instalada la máquina virtual Java. Resultará evidente para aquellos con conocimientos comunes en la materia que la máquina virtual 32 se puede materializar en un lenguaje de programación diferente al Java.

Si el contenido se transforma aleatorizando partes separadas del mismo en una forma de realización de la presente invención, la información de restablecimiento puede ser información de desaleatorización para restablecer la parte transformada. En particular, de acuerdo con una forma de realización de la presente invención, la información de restablecimiento se puede encubrir para evitar que se interpreten fácilmente valores de la información de restablecimiento. Resultará evidente para aquellos expertos en la materia que el término “encubrimiento” se puede sustituir con otros términos, tales como “enmascaramiento”. Además, si el contenido se transforma aleatorizando partes separadas del mismo en una forma de realización de la presente invención, la información de

restablecimiento puede contener información de ubicación que indique qué parte del contenido está aleatorizada, e información referente al tamaño de una parte aleatorizada del contenido.

La unidad de descifrado 34 descifra el contenido leído por la interfaz de medios 31. Si el contenido está cifrado usando una clave CSS de acuerdo con la normativa CSS, la unidad de descifrado 34 descifra el contenido usando la clave CSS de acuerdo con la normativa CSS. Si el contenido se cifra usando una clave de título de acuerdo con la normativa AACS, la unidad de descifrado 34 cifra el contenido usando la clave de título según la normativa AACS. Si el contenido no se cifra tal como se ha descrito anteriormente, resultará evidente para aquellos con conocimientos comunes en la materia que la unidad de descifrado 34 se puede omitir del reproductor de medios 3 de acuerdo con una forma de realización ejemplificativa de la presente invención.

La unidad de comprobación 35 comprueba la información de restablecimiento para restablecer la parte transformada del contenido en relación con un paquete de PMT de entre los paquetes que constituyen el contenido descifrado por la unidad de descifrado 34, y extrae información de ubicación de un paquete de PMT sucesivo a partir de la información de restablecimiento comprobada del paquete de PMT, conteniendo el paquete de PMT sucesivo datos para restablecer sustancialmente la parte transformada del contenido (a los que se hará referencia en la presente en lo sucesivo como “datos de restablecimiento”).

Además, la unidad de comprobación 35 extrae datos de restablecimiento a partir de la información de restablecimiento del paquete de PMT cuando la información de restablecimiento contiene los datos de restablecimiento. No obstante, la información de restablecimiento contenida en cada paquete de PMT no siempre contiene datos de restablecimiento sino que puede contener solamente información de ubicación relativa de un paquete de PMT sucesivo que contiene datos de restablecimiento. En otras palabras, la información de restablecimiento contenida en cada paquete de PMT contiene siempre información de ubicación de un paquete de PMT sucesivo que contiene datos de restablecimiento pero puede que no contenga datos de restablecimiento.

Por el contrario, un paquete de PMT que no contiene datos de restablecimiento puede contener información para marcas forenses. Si la información de restablecimiento de un paquete de PMT contiene información para marcas forenses, no datos de restablecimiento, la unidad de comprobación 35 extrae la información para marcas forenses a partir de la información de restablecimiento del paquete de PMT. Las marcas forenses son un método de expresar información del reproductor usado para la piratería informática cuando el contenido ha sido pirateado y distribuido sin permiso. Por ejemplo, según las marcas forenses, en el contenido se puede insertar un ID de reproductor.

La figura 4 es un diagrama que ilustra un proceso de comprobación de información de restablecimiento de acuerdo con una forma de realización de la presente invención.

El reproductor de medios 3 de la figura 3 puede reproducir contenido almacenado en un medio comenzando a partir de o bien el inicio del contenido o bien una parte central del mismo, según seleccione el usuario. De este modo, la unidad de comprobación 35 comprueba la información de restablecimiento de un paquete de PMT que aparece en primer lugar a partir de un punto de inicio, el cual es seleccionado por el usuario, desde el cual se reproduce el contenido.

En referencia a la figura 4, la unidad de comprobación 35 se salta la comprobación de información de restablecimiento de paquetes de PMT presentes entre un paquete de PMT actual y un paquete de PMT sucesivo que contiene datos de restablecimiento, basándose en información de ubicación relativa de un paquete de PMT sucesivo, y comprueba directamente la información de restablecimiento del paquete de PMT sucesivo que contiene los datos de restablecimiento. En este caso, la información de ubicación relativa del paquete de PMT sucesivo representa un número de paquete relativo que indica un número total de paquetes entre el paquete de PMT actual y el paquete de PMT sucesivo que contiene los datos de restablecimiento. Es decir, la unidad de comprobación 35 comprueba la información de restablecimiento de paquete de PMT sucesivo presente en una ubicación correspondiente a un valor obtenido mediante la suma del número del paquete de PMT actual más uno al número de paquete relativo del paquete de PMT sucesivo.

Por ejemplo, si el punto de inicio a partir del cual se reproduce el contenido se marca por medio de una flecha en la izquierda 410 de la figura 4, la unidad de comprobación 35 comprueba la información de restablecimiento de un paquete PMT A (41) que aparece en primer lugar a partir del punto de inicio. Seguidamente, la unidad de comprobación 35 extrae un número de paquete relativo de un paquete de PMT sucesivo que contiene datos de restablecimiento, es decir, un paquete de PMT B (42), a partir de la información de restablecimiento del paquete de PMT A (41), y comprueba la información de restablecimiento del paquete de PMT B (42) basándose en el número de paquete relativo extraído. Seguidamente, la unidad de comprobación 35 extrae un número de paquete relativo de un paquete de PMT sucesivo que contiene datos de restablecimiento, es decir, un paquete de PMT D (44), a partir de la información de restablecimiento del paquete de PMT B (42), y comprueba la información de restablecimiento del paquete de PMT D (44) basándose en el número de paquete relativo extraído. En este caso, la comprobación de la información de restablecimiento de un paquete de PMT C (43) se salta, puesto que el paquete de PMT C (43) no contiene datos de restablecimiento.

Si el punto de inicio a partir del cual se reproduce el contenido se marca por medio de una flecha en la derecha 420 de la figura 4, la unidad de comprobación 35 comprueba la información de restablecimiento del paquete de PMT C (43) que aparece en primer lugar desde el punto de inicio. Seguidamente, la unidad de comprobación 35 extrae un número de paquete relativo de un paquete de PMT sucesivo que contiene datos de restablecimiento, es decir, el paquete de PMT D (44), a partir de la información de restablecimiento del paquete de PMT C (43), y comprueba la información de restablecimiento del paquete de PMT D (44) basándose en el número de paquete extraído. En este caso, se comprueba la información de restablecimiento del paquete de PMT C (43), puesto que el paquete de PMT C (43) aparece el primero a partir del punto de inicio desde el cual se reproduce el contenido aunque el paquete de PMT C (43) no contiene datos de restablecimiento.

Es decir, la unidad de comprobación 35 comprueba la información de restablecimiento de un paquete de PMT que aparece en primer lugar desde el punto de inicio en el que comienza a reproducirse el contenido, y a continuación comprueba solamente la información de restablecimiento de un paquete de PMT que contiene datos de restablecimiento sin comprobar la información de todos los paquetes de PMT.

La unidad de restablecimiento 36 restablece selectivamente una parte transformada del contenido basándose en información de restablecimiento generada por la máquina virtual 32 e información de restablecimiento de un paquete de PMT comprobado por la unidad de comprobación 35. Más específicamente, cuando la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35 contiene datos de restablecimiento, la unidad de restablecimiento 36 restablece la parte transformada del contenido usando los datos de restablecimiento incluidos en la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35, es decir, los datos de restablecimiento extraídos por la unidad de comprobación 35.

No obstante, cuando la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35 contiene información para marcas forenses, no datos de restablecimiento, la unidad de restablecimiento 36 inserta la información para marcas forenses en el contenido. Cuando la información de restablecimiento del paquete de PMT contiene datos de restablecimiento, usando los datos de restablecimiento se desaleatorizan partes aleatorizadas, separadas, del contenido. Cuando la información de restablecimiento del paquete de PMT contiene la información para marcas forenses, la información para marcas forenses se inserta en el contenido.

La unidad de restablecimiento 36 puede usar varios métodos para restablecer la parte transformada del contenido. Por ejemplo, la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35 puede incluir una parte encubierta. En este caso, la información de restablecimiento generada por la máquina virtual 32 se usa para desvelar la parte encubierta de la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35. Es decir, la unidad de restablecimiento 36 desvela la parte encubierta de la información de restablecimiento de paquete de PMT comprobado por la unidad de comprobación 35 usando la información de restablecimiento generada por la máquina virtual 32, y restablece la parte transformada del contenido usando la información de restablecimiento desvelada. El desvelamiento de la parte encubierta se puede realizar a través de una operación XOR. Es decir, la información de restablecimiento se puede desvelar realizando una operación XOR sobre la información de restablecimiento y un flujo continuo de bits específico. En este caso, la información de restablecimiento generada por la máquina virtual 32 es el flujo continuo de bits específico. Es decir, la unidad de restablecimiento 36 restaura la información de restablecimiento original realizando la operación XOR sobre la información de restablecimiento generada por la máquina virtual 32, e información de restablecimiento contenida en la información de restablecimiento del paquete de PMT comprobado por la unidad de comprobación 35.

En una forma de realización ejemplificativa de la presente invención, la información de restablecimiento incluye datos de restablecimiento, información para marcas forenses, información de ubicación de un paquete de PMT sucesivo que contiene los datos de restablecimiento, etcétera. La información de ubicación del paquete de PMT sucesivo que contiene los datos de restablecimiento puede no estar encubierta. La información de ubicación del paquete de PMT sucesivo que contiene los datos de restablecimiento se debe comprobar siempre con independencia de si la información de restablecimiento contiene o no los datos de restablecimiento, la información para marcas forenses, etcétera, y por lo tanto puede no estar encubierta para ser usada encubiertamente sin la aplicación de un proceso de desvelamiento.

La unidad de decodificación 37 restaura el contenido original decodificando el contenido descifrado por la unidad de descifrado 34, el contenido restablecido por la unidad de restablecimiento 36, o el contenido en el cual se ha insertado la información para marcas forenses. Si el contenido se codifica de acuerdo con la normativa MPEG-2, la unidad de decodificación 37 restaura el contenido original por medio del contenido restablecido por la unidad de restablecimiento 36 de acuerdo con la normativa MPEG-2.

La interfaz de salida 38 da salida al contenido decodificado por la unidad de decodificación 37 hacia un dispositivo de visualización, tal como una televisión digital (DTV).

Las figuras 5 y 6 son diagramas de flujo que ilustran un método de restauración de contenido de acuerdo con una

forma de realización ejemplificativa de la presente invención. El método ilustrado en las figuras 5 y 6 incluye operaciones de temporización realizadas por el reproductor de medios 3 de la figura 3. Así, aunque no se han descrito en este caso, las operaciones anteriores del reproductor de medios 3 son también aplicables al método de las figuras 5 y 6.

En la operación 501, el reproductor de medios 3 lee contenido y el código de seguridad, el cual es un programa para leer el contenido, desde un medio, tal como un DVD o un CD.

En la operación 502, el reproductor de medios 3 ejecuta el código de seguridad extraído en la operación 501 para generar información del reproductor de medios 3, y compara la información generada del reproductor de medios 3 en el código de seguridad con información del reproductor de medios 3 almacenada en la memoria 33.

En la operación 503, el reproductor de medios 3 determina si se ha revelado un conjunto de claves de dispositivo del reproductor de medios 3 ó se ha instalado o se está ejecutando un software de piratería informática del mismo, basándose en el resultado de la comparación de 502, y ejecuta la operación 504 cuando se determina que no se ha revelado el conjunto de claves de dispositivo del reproductor de medios 3 ó no se ha instalado o no se está ejecutando el software de piratería informática del mismo. Cuando se determina que se ha revelado el conjunto de claves de dispositivo o se ha instalado o se está ejecutando el software de piratería del mismo, el método finaliza.

En la operación 504, el reproductor de medios 3 ejecuta además el código de seguridad para generar información de restablecimiento para restablecer una parte transformada del contenido.

En la operación 505, el reproductor de medios 3 descifra el contenido leído en la operación 501.

En la operación 506, el reproductor de medios 3 comprueba la información de restablecimiento de un paquete de PMT de entre paquetes que constituyen el contenido descifrado en la operación 505, el paquete de PMT que aparece en primer lugar a partir de un punto de inicio, el cual es seleccionado por un usuario, desde el cual se reproduce el contenido.

En la operación 507, el reproductor de medios 3 desvela la información de restablecimiento del paquete de PMT comprobado en la operación 506 usando la información de restablecimiento generada en la operación 504. Tal como se ha descrito anteriormente, la información de ubicación de un paquete de PMT sucesivo que contiene datos de restablecimiento puede no estar encubierta.

En la operación 508, el reproductor de medios 3 realiza la operación 510 cuando la información de restablecimiento desvelada en la operación 507 contiene datos de restablecimiento, y si no, ejecuta la operación 509.

En la operación 509, el reproductor de medios 3 ejecuta la operación 512 cuando la información de restablecimiento encubierta en la operación 507 contiene información para marcas forenses, y si no, ejecuta la operación 514.

En la operación 510, el reproductor de medios 3 extrae datos de restablecimiento a partir de la información de restablecimiento desvelada en la operación 507.

En la operación 511, el reproductor de medios 3 restablece la parte transformada del contenido usando los datos de restablecimiento extraídos en la operación 510.

En la operación 512, el reproductor de medios 3 extrae la información para marcas forenses a partir de la información de restablecimiento desvelada en la operación 507.

En la operación 513, el reproductor de medios 3 inserta la información para marcas forenses extraída en la operación 512 en el contenido.

En la operación 514, el reproductor de medios 3 extrae información de ubicación de un paquete de PMT sucesivo que contiene datos de restablecimiento a partir de la información de restablecimiento del paquete de PMT comprobado en la operación 506.

En la operación 515, el reproductor de medios 3 comprueba directamente la información de restablecimiento del paquete de PMT sucesivo extraído en la operación 514 sin comprobar información de restablecimiento de paquetes de PMT presentes entre un paquete de PMT actual y el paquete de PMT sucesivo. Seguidamente, el reproductor de medios 3 ejecuta la operación 507 para restablecer la parte transformada del contenido usando los datos de restablecimiento en el paquete PMT sucesivo indicado por la información de ubicación extraída en la operación 513.

En la operación 516, el reproductor de medios 3 restaura el contenido original decodificando el contenido descifrado en la operación 505, el contenido restablecido en la operación 511 ó el contenido en el cual se insertó la información para marcas forenses en la operación 513.

En la operación 517, el reproductor de medios 3 da salida al contenido decodificado en la operación 516 hacia un dispositivo de salida, tal como una DTV.

Las anteriores formas de realización de la presente invención se pueden materializar como un programa de ordenador, y se pueden llevar a la práctica en un ordenador digital general a través de un medio legible por ordenador. Además, las construcciones de datos usadas en las anteriores formas de realización se pueden grabar en un medio legible por ordenador a través de varios dispositivos. En este caso, el medio legible por ordenador puede ser, por ejemplo, una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un disco compacto (CD)-ROM, una cinta magnética, un disco flexible, un dispositivo de almacenamiento óptico de datos, y una onda portadora que transmite datos a través de Internet.

Según un aspecto de la presente invención, en un paquete de PMT se almacena información para restablecer contenido que es transformado mediante la aleatorización de partes separadas del mismo, con el fin de detectar fácilmente la ubicación de la información para restablecer el contenido, agilizándose así el restablecimiento de las partes transformadas del contenido. En particular, según la presente invención, cada paquete de PMT contiene información de ubicación de un paquete de PMT sucesivo que incluye datos de restablecimiento para restablecer sustancialmente una parte transformada del contenido, y por lo tanto, es posible comprobar directamente los datos de restablecimiento sin analizar sintácticamente todos los paquetes de PMT.

Aunque se han mostrado y descrito unas pocas formas de realización preferidas, los expertos en la materia apreciarán que se pueden realizar varios cambios y modificaciones sin apartarse, por ello, del alcance de la invención, tal como se define en las reivindicaciones adjuntas.

Préstese atención a todos los textos y documentos que se han presentado simultáneamente con o de manera previa a esta memoria en relación con esta solicitud y que están abiertos a inspección pública con esta memoria, y el contenido de todos estos textos y documentos se incorpora a la presente a título de referencia.

Todas las características dadas a conocer en esta memoria (incluyendo todas las reivindicaciones, resumen y dibujos adjuntos), y/o todas las etapas de cualquier método o proceso dado a conocer, se pueden combinar en cualquier combinación, excepto combinaciones en las que por lo menos de algunas características y/o etapas sean mutuamente exclusivas.

Cada característica dada a conocer en esta memoria (incluyendo todas las reivindicaciones, resumen y dibujos adjuntos) se puede sustituir por características alternativas que presten servicio a una finalidad idéntica, equivalente o similar, a no ser que se exponga expresamente lo contrario. Así, a no ser que se exponga expresamente lo contrario, cada característica dada a conocer es un ejemplo solamente de una serie genérica de características equivalentes o similares.

La invención no se limita a los detalles de la(s) forma(s) de realización anterior(es). La invención se extiende a cualquier característica novedosa, o cualquier combinación novedosa, de las características dadas a conocer en esta memoria (incluyendo todas las reivindicaciones, resumen y dibujos adjuntos), o a cualquier etapa novedosa, o cualquier combinación novedosa, de las etapas de cualquier método o procesado así dado a conocer.

REIVINDICACIONES

1. Método para desaleatorizar contenido, en el que partes separadas del contenido han sido transformadas por aleatorización para protegerlas contra ataques de un pirata informático durante la reproducción del contenido, comprendiendo el método:

a) comprobar la información proporcionada en una región reservada de un primer paquete de la Tabla de Correspondencia de Programas, en lo sucesivo “paquete de PMT”, (41, 43) de entre una pluralidad de paquetes de PMT que constituyen el contenido, usándose la información en un proceso para desaleatorizar una parte transformada del contenido, siendo el primer paquete de PMT el primer paquete de PMT (41, 43) a partir de un punto de inicio, que es seleccionado por un usuario, desde el cual se reproduce el contenido;

b) extraer información de ubicación relativa de un segundo paquete de PMT (42, 44) de los paquetes de PMT a partir de la información del primer paquete de PMT (41, 43) comprobado en la etapa a), en el que la información de ubicación relativa es relativa del primer paquete de PMT (41, 43) con respecto al segundo paquete (42, 44), presentando el segundo paquete de PMT (42, 44) una región reservada que contiene datos de desaleatorización para desaleatorizar la parte transformada respectiva del contenido; y

c) desaleatorizar la parte transformada respectiva del contenido usando los datos de desaleatorización del segundo paquete de PMT (42, 44) indicado por la información de ubicación extraída en la etapa b).

2. Método según la reivindicación 1, que comprende además la etapa siguiente:

d) desaleatorizar selectivamente la parte transformada del contenido basándose en la información del primer paquete de PMT (41, 43) comprobado en la etapa a).

3. Método según la reivindicación 2, en el que, cuando la información del primer paquete de PMT (41, 43) comprobado en la etapa (a) contiene los datos de desaleatorización, la etapa (d) comprende desaleatorizar la parte transformada del contenido usando los datos de desaleatorización en la información del primer paquete de PMT (41, 43) comprobado en la etapa a).

4. Método según cualquiera de las reivindicaciones 1 a 3, en el que la etapa (c) comprende:

c1) comprobar la información del segundo paquete de PMT (42, 44) basándose en la información de ubicación extraída en la etapa (b) sin comprobar la información de paquetes presentes entre el primer paquete de PMT (41, 43) y el segundo paquete de PMT (44); y

c2) desaleatorizar la parte transformada del contenido usando datos de desaleatorización de la información del segundo paquete de PMT (42, 44) comprobado en la etapa c1).

5. Método según la reivindicación 1, en el que la información de ubicación relativa indica un número total de paquetes de PMT presentes entre el primer paquete de PMT (41, 43) y el segundo paquete de PMT (42, 44), y la etapa c) comprende:

c1) comprobar la información del segundo paquete de PMT (44) presente en una ubicación correspondiente a un valor obtenido sumando el número del primer paquete de PMT (41, 43) más uno al número total de los paquetes de PMT; y

c2) desaleatorizar la parte transformada del contenido usando datos de desaleatorización de la información del segundo paquete de PMT (42, 44) comprobado en (c1).

6. Método según la reivindicación 1, que comprende además las etapas siguientes:

d) ejecutar un código de seguridad extraído a partir de un medio para generar información con el fin de desaleatorizar la parte transformada del contenido; y

e) desaleatorizar selectivamente la parte transformada del contenido basándose en la información generada en la etapa d) y la información comprobada en la etapa a).

7. Método según cualquiera de las reivindicaciones anteriores, en el que el primer paquete de PMT (41, 43) y el segundo paquete de PMT (42, 44) son paquetes de la tabla de correspondencia de programas de acuerdo con la normativa del grupo de expertos en imágenes en movimiento 2, MPEG-2, y cada paquete de la tabla de correspondencia de programas de los paquetes de PMT contiene la información.

8. Aparato para desaleatorizar contenido, en el que partes separadas del contenido han sido transformadas mediante aleatorización para protegerlas contra ataques de un pirata informático durante la reproducción del

contenido, comprendiendo el aparato:

una unidad de comprobación (35) que comprueba la información proporcionada en una región reservada de un primer paquete de PMT (41, 43) de entre una pluralidad de paquetes de PMT que constituyen el contenido, comprobando la unidad de comprobación (35) la información del primer paquete de PMT (41, 43) que contiene información que aparece en primer lugar a partir de un punto de inicio, que es seleccionado por un usuario, desde el cual se reproduce el contenido, y extrae información de ubicación relativa que define una ubicación de un segundo paquete de PMT (42, 44) de los paquetes de PMT a partir de la información comprobada, siendo usada la información en un proceso para desaleatorizar una parte transformada del contenido y presentando el segundo paquete de PMT (42, 44) una región reservada que contiene datos de desaleatorización para desaleatorizar la parte transformada respectiva del contenido; y

una unidad de desaleatorización (36) que desaleatoriza selectivamente la parte transformada respectiva del contenido basándose en la información del segundo paquete de PMT (42, 44).

9. Aparato según la reivindicación 8, en el que, cuando la información del primer paquete de PMT (41, 43) comprobado por la unidad de comprobación (35) contiene los datos de desaleatorización para una parte transformada respectiva del contenido, la unidad de desaleatorización (36) desaleatoriza la parte transformada del contenido usando la información comprobada del primer paquete de PMT (41, 43).

10. Aparato según la reivindicación 8 ó 9, en el que:

la unidad de comprobación (35) comprueba la información del segundo paquete de PMT (42, 44) basándose en la información de ubicación extraída, y extrae los datos de desaleatorización para desaleatorizar la parte transformada del contenido a partir de la información comprobada del segundo paquete de PMT (42, 44), y

la unidad de desaleatorización (36) desaleatoriza la parte transformada del contenido usando los datos de desaleatorización extraídos por la unidad de comprobación (35).

11. Aparato según cualquiera de las reivindicaciones 8 a 10, en el que la unidad de comprobación (35) comprueba la información del segundo paquete de PMT (42, 44) basándose en la información de ubicación extraída por la unidad de comprobación (35) sin comprobar la información de paquetes de PMT presentes entre el primer paquete de PMT (41, 43) y el segundo paquete de PMT (42, 44), y

la unidad de desaleatorización (36) desaleatoriza la parte transformada del contenido usando los datos de desaleatorización de la información del segundo paquete de PMT (42, 44) comprobado por la unidad de comprobación (35).

12. Aparato según la reivindicación 8, en el que la información de ubicación relativa indica un número total de paquetes de PMT presentes entre el primer paquete de PMT (41, 43) y el segundo paquete de PMT (42, 44),

la unidad de comprobación (35) comprueba la información del segundo paquete de PMT (42, 44) presente en una ubicación correspondiente a un valor obtenido sumando el primer paquete de PMT (41, 43) más uno al número total de los paquetes de PMT, y

la unidad de desaleatorización (36) desaleatoriza la parte transformada del contenido usando los datos de desaleatorización de la información comprobada por la unidad de comprobación (35).

13. Aparato según cualquiera de las reivindicaciones 8 a 12, que comprende además una máquina virtual (32) que ejecuta un código de seguridad extraído desde un medio para generar información con el fin de desaleatorizar la parte transformada del contenido,

en el que la unidad de desaleatorización (36) además desaleatoriza selectivamente la parte transformada del contenido basándose en la información generada por la máquina virtual (32) y la información del primer paquete de PMT (41, 43) que contiene información comprobada por la unidad de comprobación (35).

14. Aparato según cualquiera de las reivindicaciones 8 a 13, en el que el primer y segundo paquetes de PMT son paquetes de la tabla de correspondencia de programas de acuerdo con la normativa del grupo de expertos en imágenes en movimiento 2, y cada paquete de la tabla de correspondencia de programas de entre los paquetes de PMT contiene la información.

FIG. 1 (TÉCNICA ANTERIOR)

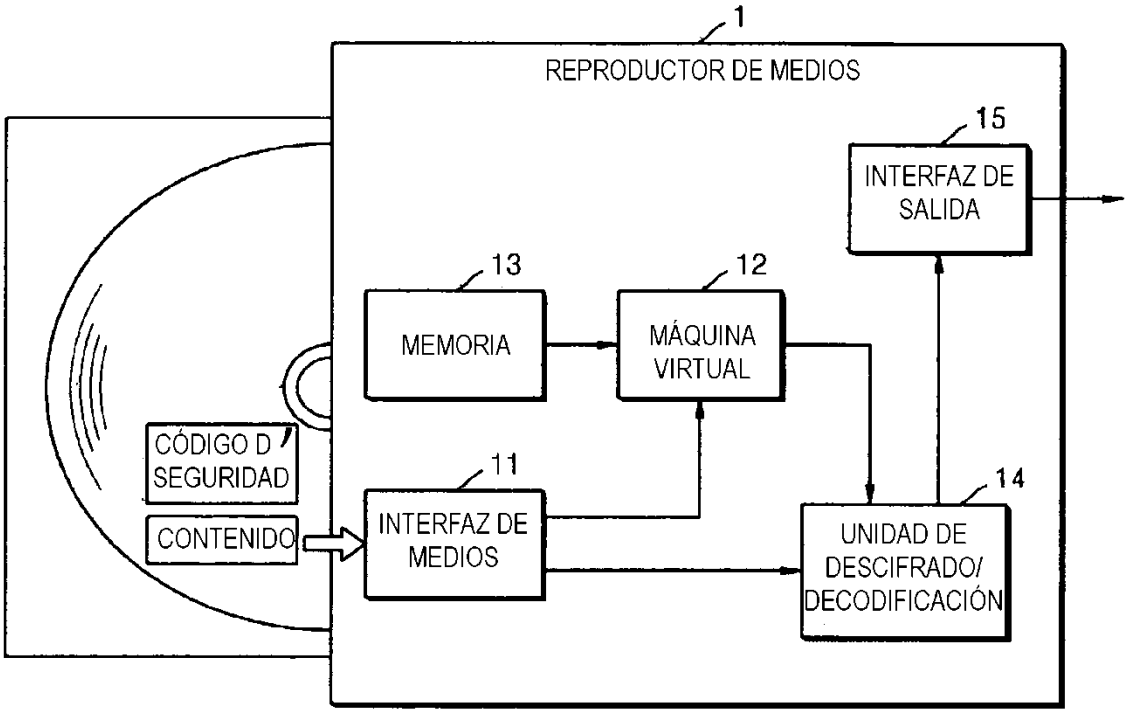


FIG. 2

FIG. 3

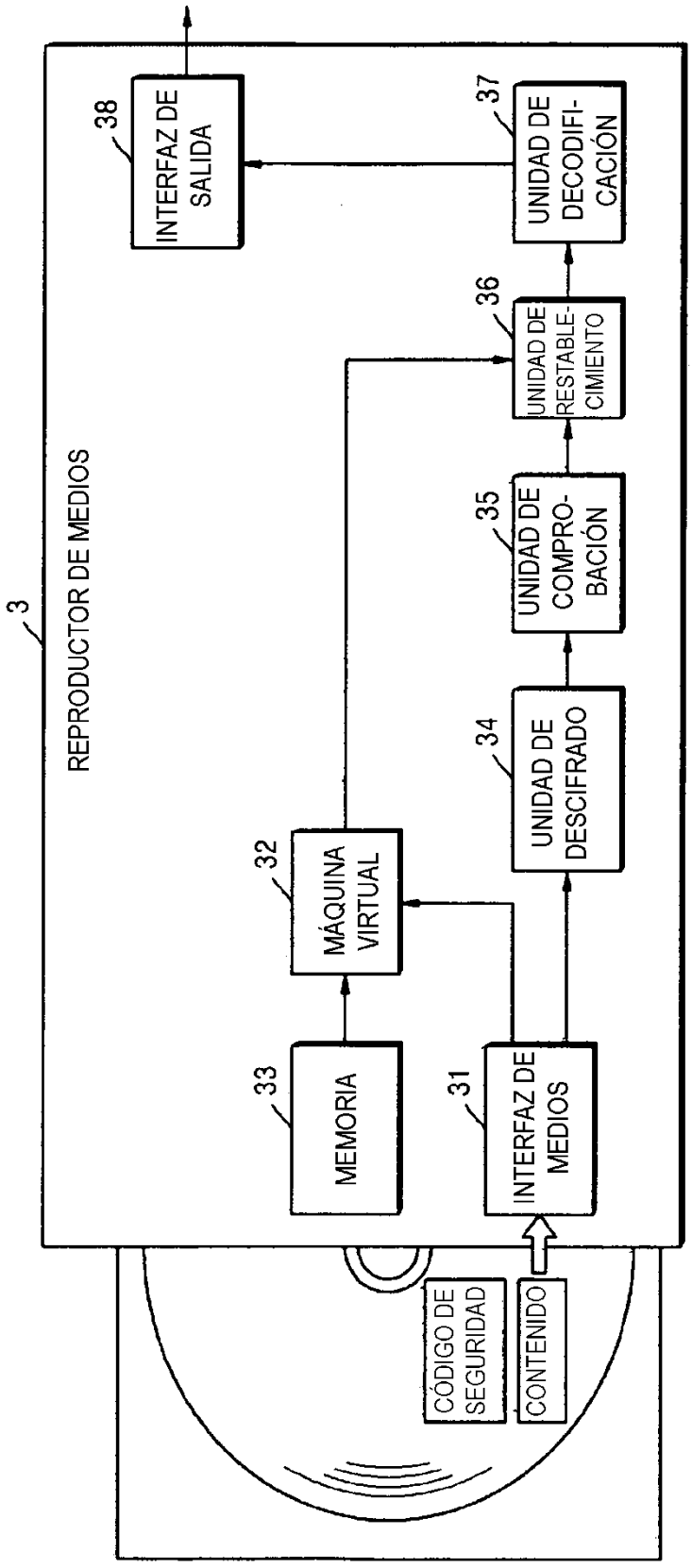

3
REPRODUCTOR DE MEDIOS
38
INTERFAZ DE SALIDA
37
UNIDAD DE DECODIFI-CACIÓN
36
UNIDAD DE RESTABLE-CIMIENTO
35
UNIDAD DE COMPRO-BACIÓN
34
UNIDAD DE DESCIFRADO
32
MÁQUINA VIRTUAL
33
MEMORIA
31
INTERFAZ DE MEDIOS
CÓDIGO DE SEGURIDAD
CONTENIDO

FIG. 4

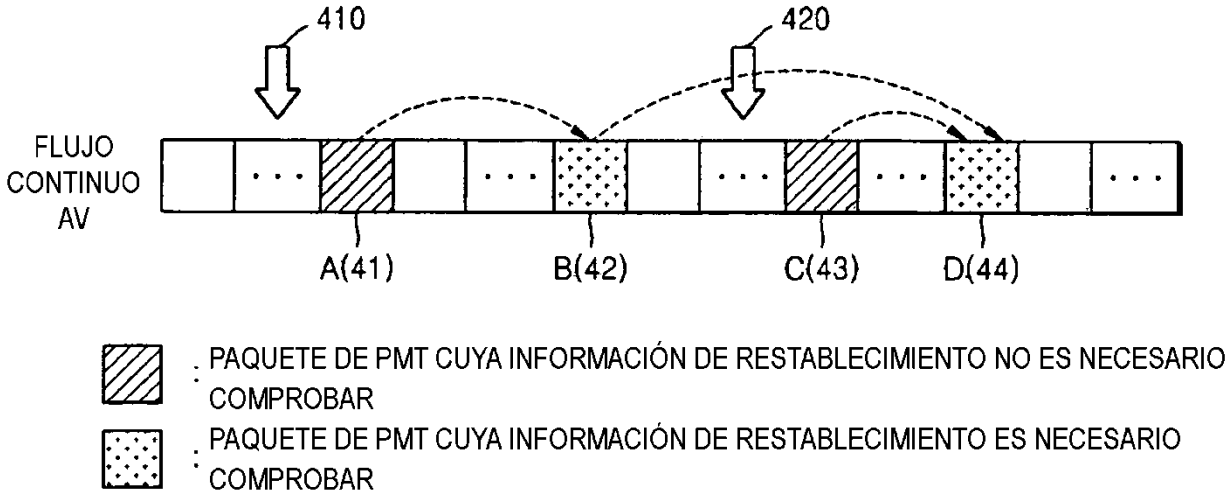

410
420
FLUJO CONTINUO AV
A(41)
B(42)
C(43)
D(44)
: PAQUETE DE PMT CUYA INFORMACIÓN DE RESTABLECIMIENTO NO ES NECESARIO COMPROBAR
: PAQUETE DE PMT CUYA INFORMACIÓN DE RESTABLECIMIENTO ES NECESARIO COMPROBAR

FIG. 5

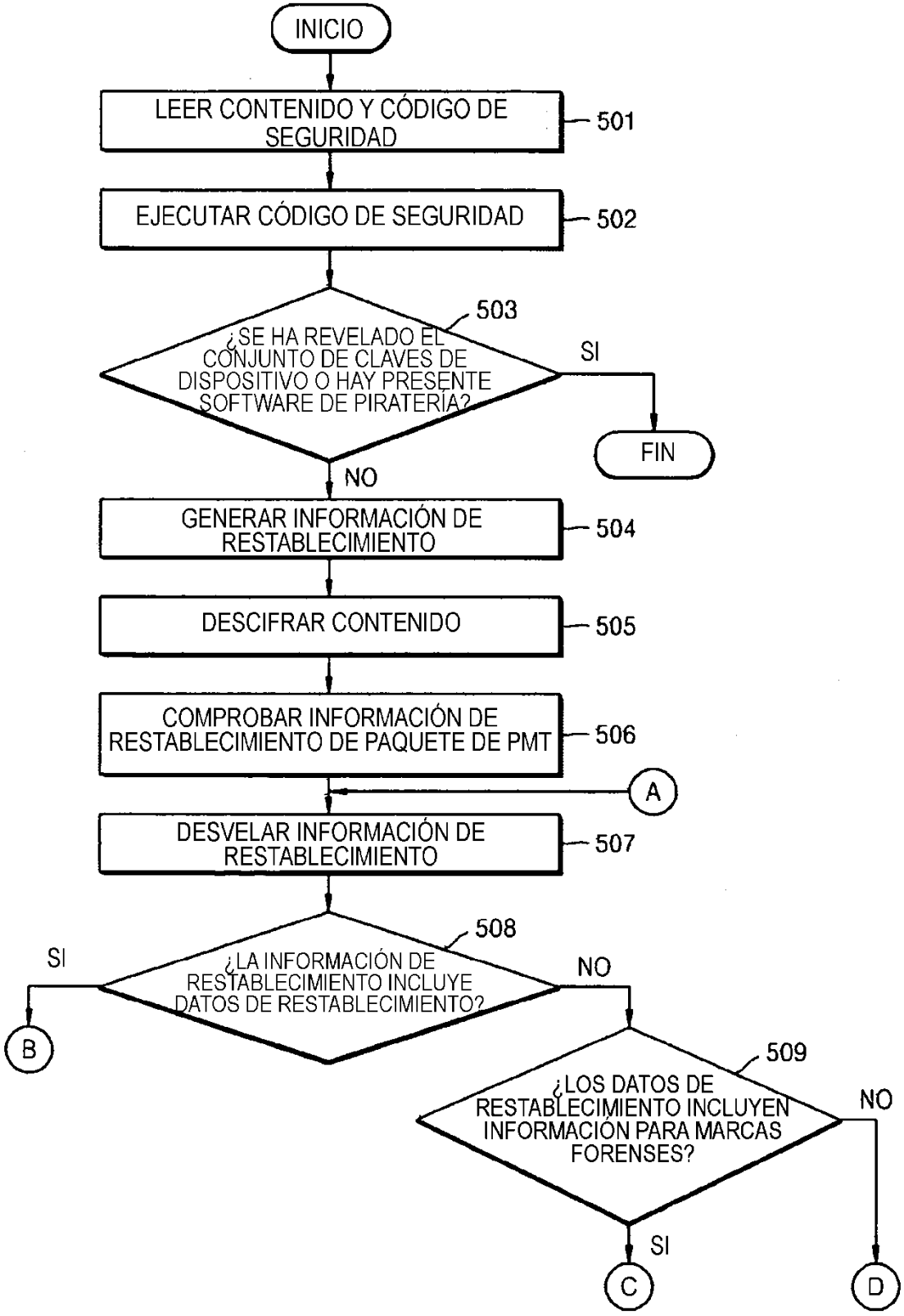
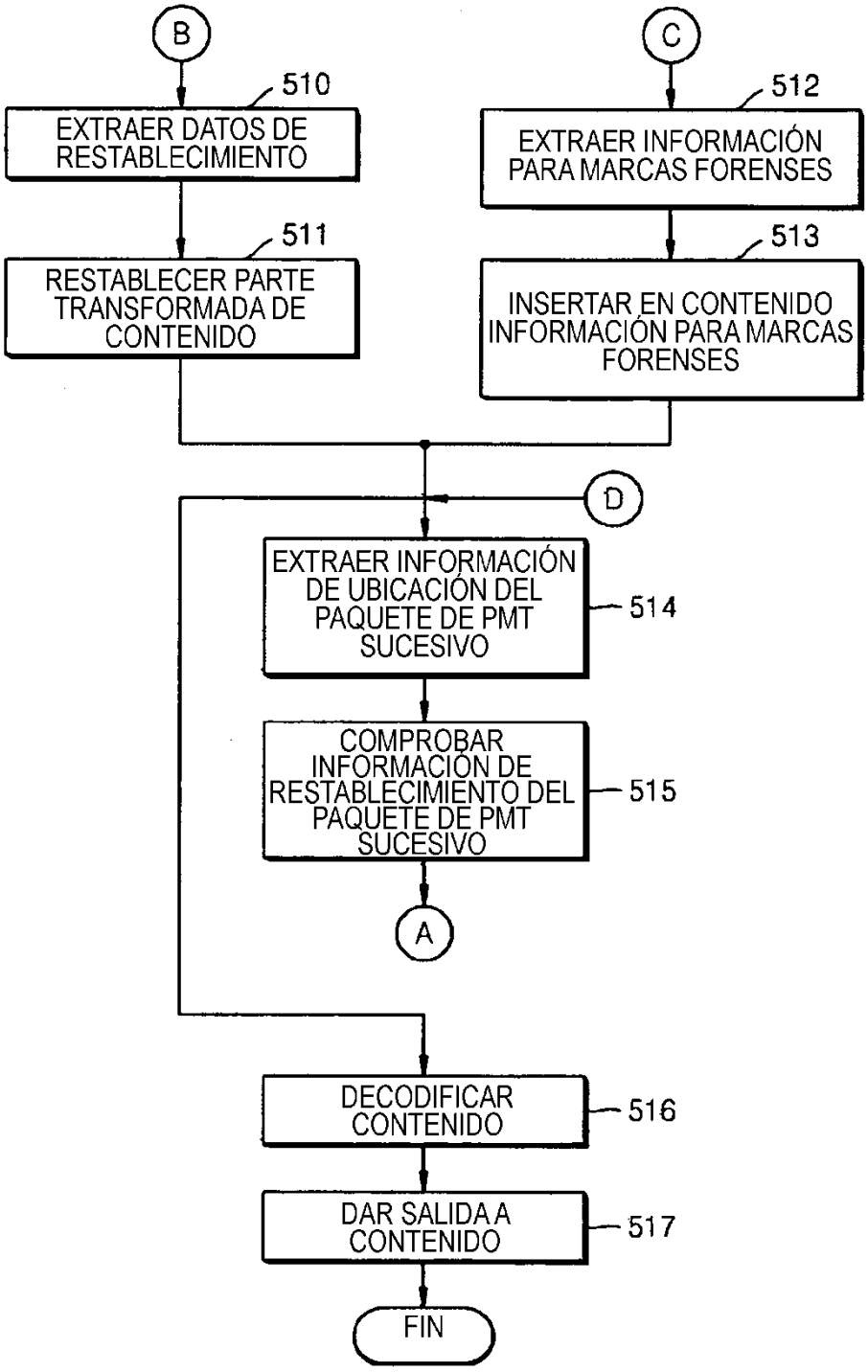

INICIO
LEER CONTENIDO Y CÓDIGO DE SEGURIDAD
501
EJECUTAR CÓDIGO DE SEGURIDAD
502
503
¿SE HA REVELADO EL CONJUNTO DE CLAVES DE DISPOSITIVO O HAY PRESENTE SOFTWARE DE PIRATERÍA?
SI
FIN
NO
GENERAR INFORMACIÓN DE RESTABLECIMIENTO
504
DESCIFRAR CONTENIDO
505
COMPROBAR INFORMACIÓN DE RESTABLECIMIENTO DE PAQUETE DE PMT
506
A
DESVELAR INFORMACIÓN DE RESTABLECIMIENTO
507
508
¿LA INFORMACIÓN DE RESTABLECIMIENTO INCLUYE DATOS DE RESTABLECIMIENTO?
SI
NO
B
509
¿LOS DATOS DE RESTABLECIMIENTO INCLUYEN INFORMACIÓN PARA MARCAS FORENSES?
NO
SI
C
D

FIG. 6


B
C
510
EXTRAER DATOS DE RESTABLECIMIENTO
512
EXTRAER INFORMACIÓN PARA MARCAS FORENSES
511
RESTABLECER PARTE TRANSFORMADA DE CONTENIDO
513
INSERTAR EN CONTENIDO INFORMACIÓN PARA MARCAS FORENSES
D
EXTRAER INFORMACIÓN DE UBICACIÓN DEL PAQUETE DE PMT SUCESIVO
514
COMPROBAR INFORMACIÓN DE RESTABLECIMIENTO DEL PAQUETE DE PMT SUCESIVO
515
A
DECODIFICAR CONTENIDO
516
DAR SALIDA A CONTENIDO
517
FIN