(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 616**

(51) Int. CI.:

G11B 20/00 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07113366 .4**
(96) Fecha de presentación: **02.08.2001**
(97) Número de publicación de la solicitud: **1843343**
(97) Fecha de publicación de la solicitud: **10.10.2007**

(54) Título: **Método y dispositivo para controlar la distribución y el uso de obras digitales**

(30) Prioridad:

16.08.2000 EP 00202888

(45) Fecha de publicación de la mención BOPI:

26.12.2012

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

26.12.2012

(73) Titular/es:

KONINKLIJKE PHILIPS ELECTRONICS N.V. (100.0%)
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es:

TREFFERS, MENNO A. y
STARING, ANTONIUS A.

(74) Agente/Representante:

ZUAZO ARALUZE, Alexander

DESCRIPCIÓN

Método y dispositivo para controlar la distribución y el uso de obras digitales

La presente invención se refiere a un método y a un dispositivo para controlar la distribución y el uso de una obra digital. Además, la presente invención se refiere a un soporte de grabación para almacenar la obra digital.

Un problema fundamental al que se enfrentan las industrias de publicación e información cuando consideran la publicación electrónica es cómo impedir la distribución no autorizada y no contabilizada del uso de materiales publicados electrónicamente. Los materiales publicados electrónicamente se distribuyen normalmente en forma digital y se crean en un sistema basado en ordenador que puede recrear los materiales. Grabaciones de audio y vídeo, software, libros y obras multimedia están publicándose todos electrónicamente. Se pagan regalías por cada una cuya entrega se ha contabilizado, de manera que cualquier distribución no contabilizada da como resultado una regalía no pagada.

La transmisión de obras digitales a través de redes tales como la ampliamente utilizada Internet es hoy en día una práctica habitual. Internet es una instalación de red generalizada mediante la cual usuarios de ordenadores en muchas universidades, empresas y entidades gubernamentales se comunican e intercambian ideas e información. Por tanto, sería deseable usar tales redes para la distribución de obras digitales sin el temor a copias no autorizadas generalizadas.

Las evidentes conversiones entre aparatos eléctricos de consumo y ordenadores, el aumento de las velocidades de red y módem, los costes descendentes de potencia de ordenador y anchos de banda, y el aumento de la capacidad de los medios ópticos se combinarán para crear un mundo de modelos de negocio híbridos en el que contenidos digitales de todo tipo puedan distribuirse en medios ópticos leídos en aparatos eléctricos y/u ordenadores al menos conectados ocasionalmente, en el que los modelos de compra de una sola vez comunes en CD de música y ofertas de películas en DVD (disco de vídeo digital) iniciales se aumentan con otros modelos, por ejemplo, arrendamiento, pago por visión, y alquiler con derecho a compra, por nombrar sólo unos pocos. Puede ofrecerse a los consumidores la opción entre estos y otros modelos de los mismos o de diferentes distribuidores y/u otros proveedores. El pago por el uso puede darse a través de una red y/u otros canales de comunicación para algún servicio de satisfacción de pago. El uso del consumidor y la información de pedido puede volver a los creadores, distribuidores, y/u otros participantes.

Las tecnologías de protección de copia elementales para discos ópticos grabables que se están introduciendo actualmente no pueden soportar éstos y otros modelos sofisticados.

El documento US-A 5 629 980 da a conocer un método y un dispositivo para controlar la distribución y el uso de una obra digital según se define en el preámbulo de las reivindicaciones 1 y 13, en el que un derecho digital o de uso se adquiere junto con la compra. Este derecho de uso limita cómo puede usarse una pista de música comprada en Internet, descargada, y almacenada en forma codificada en un disco óptico grabable. Estos derechos digitales también se denominan reglas de uso o derechos de uso. Por ejemplo, puede permitirse al comprador hacer tres copias para uso personal, se denegará una cuarta copia. Alternativamente, puede permitirse al comprador leer una pista específica cuatro veces, por lo que la unidad de disco óptico no leerá una quinta vez.

Los derechos de uso se almacenan preferiblemente en el disco óptico. En este caso, los derechos de uso van con la música y el disco se leerá en todos los lectores de disco que soporten esta característica.

Una aplicación de descarga de música electrónica (EMD) usada para descargar la pista de música de Internet tiene que almacenar diversa información en el disco, por ejemplo la pista de audio codificada, la clave necesaria para decodificar la pista de audio, y una descripción de los derechos de uso. Algunos de los derechos de uso pueden disminuir (es decir, consumirse) cuando se usan.

La regla “tres copias para uso personal”, por ejemplo, se vuelve “dos copias para uso personal” después de hacer una copia. Por tanto, el derecho de uso contiene contadores que pueden actualizarse cuando se ha ejercido un derecho de uso.

Cualquier equipo que está dispuesto para acceder a la pista descargada debe cumplir con las reglas subyacentes a los derechos de uso comprados. Es decir, sólo un equipo de lectura autorizado, legal, debe poder leer la clave, y ajustar los derechos de uso o contadores.

Por tanto, debe impedirse una aplicación no conforme que pueda copiar pistas sin actualizar el contador, incrementar los contadores sin pagar tarifas adicionales, o hacer una copia idéntica del disco con los mismos derechos de uso.

En lo que respecta a una operación de copia bit a bit usando una unidad de disco convencional, se ha sugerido un identificador de disco unitario (UDI), que el fabricante de discos puede escribir en el disco de modo que puede leerse

por el equipo de lectura, pero no puede modificarse. Si un disco grabable tiene un UDI, este identificador puede combinarse con o incorporarse en una clave de codificación de la pista de audio. Una copia bit a bit del disco en cuestión en otro soporte de grabación ya no puede decodificarse, puesto que el otro soporte de grabación tendrá un UDI diferente, de manera que la clave de decodificación ya no puede recuperarse.

Sin embargo, puede usarse un “ataque de copia y restablecimiento” o “ataque de relectura” para sortear la solución de UDI anterior. En este caso, una unidad de disco convencional se usa para determinar los bits que se han cambiado en el disco cuando se consume un derecho de uso. Estos bits normalmente están relacionados con los contadores de los derechos de uso y por tanto se copian en otro medio de almacenamiento. Entonces, el derecho de uso se consume, por ejemplo, al hacer copias, hasta que un contador de copias llega a cero y no se permite hacer más copias. Los bits determinados y almacenados se restablecen del medio de almacenamiento de vuelta al disco. Ahora, el disco está en un estado que simula que los derechos de uso no se han consumido o ejercido, de manera que el usuario puede continuar haciendo copias. En este caso, la clave de codificación que depende de UDI no tiene influencia en la operación de copia, puesto que el disco no se ha cambiado.

Además, el documento WO-A-97/43761 da a conocer una disposición de gestión de derechos para medios de almacenamiento tales como discos de vídeo digital óptico, en la que se usa un “contenedor de software” seguro para encapsular de manera protectora una obra digital y su correspondiente información de derecho de uso. Además, un bloque de clave encriptada se almacena en el disco, lo que proporciona una o más claves criptográficas para su uso en el desencriptado de la obra digital. Las claves de desencriptado para desencriptar el bloque de claves también se almacenan en el soporte de grabación en forma de una información oculta, almacenada en una ubicación que puede permitirse físicamente mediante un correspondiente firmware o puente de conexión de la unidad de disco, de manera que puede ser accesible para lectores de disco pero no para ordenadores personales. Por tanto, cualquier intento de copiar físicamente el disco por un ordenador personal daría como resultado la incapacidad de copiar las claves ocultas.

Sin embargo, incluso este método de protección criptográfica no puede impedir un “ataque de copia y restablecimiento”, dado que un posible pirata informático restablece los datos de derecho de uso detectados y copiados de nuevo a su ubicación original en el mismo disco. Entonces, el pirata informático puede leer de nuevo la pista para la que se han ejercido los derechos de uso, sin pagar de nuevo. Se observa que el pirata informático no tiene que leer o escribir las claves ocultas para sortear el mecanismo de protección. Por tanto, el “ataque de copia y restablecimiento” es útil para derechos que se consumen, tal como un derecho para leer una vez, un derecho para hacer un número limitado de copias (incrementándose un contador de copias en el disco después de cada copa), o un derecho para mover una pista de un disco a otro (borrándose la pista en el disco original).

Por tanto un objeto de la presente invención es proporcionar un método y un dispositivo para controlar la distribución y el uso de una obra digital basándose en una información de derecho de uso adscrito, y un correspondiente soporte de grabación, por medio del cual puede impedirse sortear los derechos de uso mediante un “ataque de copia y restablecimiento”.

Este objeto se logra mediante un método según las reivindicaciones 1 y 10 y mediante un dispositivo según la reivindicación 17.

Por consiguiente, se reescribe la información de derecho de uso y se almacena una nueva información oculta usada para encriptar o verificar la información de derecho de uso, cuando la información de derecho de uso ha cambiado. Por tanto, una simple operación de restablecimiento de la información de derecho de uso durante un “ataque de copia y restablecimiento” únicamente restablece la información de derecho de uso previa pero no restablece la información oculta previa. Sin embargo, debido al hecho de que la información oculta cambiada ya no se ajusta ni corresponde a la información de derecho de uso previa u original, ya no es posible un desencriptado ni una verificación de la información de derecho de uso, de manera que el sistema de protección del lector de disco reconocerá el intento de fraude. Un “ataque de copia y restablecimiento” del canal oculto no funcionará, puesto que los dispositivos no conformes no pueden leer o escribir en el canal oculto.

Según un desarrollo ventajoso, la información oculta puede ser una suma de control sobre un bloque de datos que contiene la información de derecho de uso. En este caso, la información de derecho de uso no tiene que encriptarse en el soporte de grabación. Cualquier manipulación del contenido de la información de derecho de uso puede impedirse calculando la suma de control y almacenando esta suma de control en el canal oculto. Un ataque de “copia y restablecimiento” no funciona, puesto que la suma de control oculta que se ha cambiado con la actualización de la información de derecho de uso ya no será válida para la información de derecho de uso original restablecida.

Alternativamente, según otro desarrollo ventajoso, la información oculta puede ser una clave usada para un desencriptado de la información de derecho de uso, en el que la clave se cambia aleatoriamente y la información de derecho de uso se reencripta usando la clave cambiada, cuando la información de derecho de uso ha cambiado. El restablecimiento de la antigua versión de la información de derecho de uso no funcionará, puesto que la clave cambiada no puede usarse para desencriptar la información de derecho de uso original.

Preferiblemente, la clave previa se destruye después del cambio de la clave. De este modo, la clave usada para encriptar la información de derecho de uso original ya no puede recuperarse y un pirata informático potencial no puede desencriptar la información de derecho de uso original.

Preferiblemente, el canal oculto puede generarse: almacenando la información oculta en errores deliberados que pueden corregirse de nuevo; almacenando la información oculta en bits de fusión de un código de coordenada diferencial limitada; controlando una polaridad de una coordenada diferencial predeterminada de una palabra predeterminada de un código de coordenada diferencial limitada, según la información oculta; almacenando la información oculta en errores deliberados en una base de tiempo; o almacenando la información oculta en una memoria intercalada con un controlador de disco. De este modo, puede proporcionarse un canal oculto que no puede leerse o escribirse por unidades de disco convencionales o existentes. Incluso para una actualización de firmware, no pueden leer o escribir en el canal oculto. En particular, se requiere una modificación de los respectivos circuitos integrados para copiar o leer el canal oculto. Esto, sin embargo, es caro y requiere conocimientos de experto correspondientes. Las áreas de entrada conocidas de soportes de grabación no son suficientes para proporcionar un canal oculto de este tipo, puesto que las unidades de disco convencionales pueden dar acceso a estas áreas por una simple operación de pirateo informático de firmware.

Según una modificación ventajosa adicional, la información de derecho de uso adscrita puede almacenarse en una tabla junto con una información de clave usada para desencriptar la obra digital. Por tanto, la información de clave requerida para desencriptar la obra digital ya no puede desencriptarse después de un “ataque de copia y restablecimiento”. La obra digital puede ser una pista de audio descargada de Internet a un disco óptico grabable.

Preferiblemente, la información de derecho de uso comprende una información de contador que puede actualizarse cuando se ha ejercido el derecho de uso. Por tanto, el cambio de la información de contador lleva a una operación de reescritura y reencriptado con una nueva clave oculta, de manera que una detección y restablecimiento de los valores de contador actualizados es inútil debido al cambio de la clave de desencriptado oculta.

Según una modificación ventajosa adicional, cada pista del medio de grabación puede comprender su propia información de derecho de uso y su propia información oculta. En este caso, se proporciona una clave oculta para cada pista del soporte de grabación, siempre y cuando el canal oculto proporcione suficiente capacidad.

A continuación, se describirá la presente invención en mayor detalle basándose en una realización preferida con referencia a los dibujos adjuntos, de los que: la figura 1 muestra una modificación de una tabla de bloqueo de claves y una clave oculta después de una operación de copia, según la realización preferida de la presente invención, la figura 2 muestra un diagrama de bloques básico de un dispositivo de accionamiento para accionar un soporte de grabación según la realización preferida de la presente invención, y la figura 3 muestra un diagrama de flujo básico de una actualización segura de una información de derecho de uso, según la realización preferida de la presente invención.

La realización preferida se describirá ahora basándose en una EMD de Internet a un soporte de grabación tal como un disco óptico grabable, en la que una pista de música se compra, se descarga y se almacena en el soporte de grabación.

No obstante, en la presente solicitud, el término “obra digital”, se refiere a cualquier obra que se haya reducido a una representación digital. Esto incluye cualquier obra de audio, vídeo, texto o multimedia y cualquier interprete que lo acompañe (por ejemplo, software) que puede requerirse para recrear la obra. El término “derechos de uso” se refiere a cualquier derecho concedido a un destinatario de una obra digital. Generalmente, estos derechos definen cómo puede usarse una obra digital y si puede distribuirse adicionalmente. Cada derecho de uso puede tener una o más condiciones especificadas que deben satisfacerse para el derecho que va a ejercerse. Los derechos de uso están “adscritos” de manera permanente a la obra digital. Las copias hechas de una obra digital también tendrán derechos de uso adscritos. Por tanto, los derechos de uso y las tarifas asociadas asignados por un creador y distribuidor posterior siempre permanecerán con una obra digital.

Según la realización preferida, todos los secretos, por ejemplo derechos de uso, claves, contadores, una identificación propia del disco o cualquier información que vaya a almacenarse sin manipulación, se almacenan juntos en una tabla que se denomina tabla de bloqueo de claves KLT. La tabla de bloqueo de claves KLT se encripta, por ejemplo, mediante un algoritmo DES y se almacena en el disco en cualquier ubicación conveniente. La clave usada para encriptar la KLT de bloqueo de claves se denomina clave de bloqueo de claves KLK. Esta clave KLK se almacena en el disco en un canal oculto especial o canal secundario seguro que no puede leerse o escribirse por unidades de disco existentes o convencionales. En particular, el canal oculto debe disponerse de manera que una actualización de firmware de unidades de disco existentes no sea suficiente para permitir una operación de lectura o escritura del canal oculto.

El canal oculto debe ocultarse de manera muy profunda en las características físicas del flujo de datos grabados, soporte de grabación o unidad de disco, de manera que se requiere un cambio de los circuitos integrados para leer o

escribir en el canal oculto con las unidades de disco existentes. Algunas posibilidades para implementar un canal oculto de este tipo son:

(i) almacenar la información oculta (clave) en errores deliberados del flujo de datos, que pueden corregirse de nuevo;

(ii) almacenar la información oculta en bits de fusión de una secuencia de código de coordenada diferencial limitada;

(iii) almacenar la información oculta controlando la polaridad de una coordenada diferencial predeterminada de datos predeterminados o símbolo de control de una secuencia de código de coordenada diferencial limitada, según la información oculta ; o

(iv) almacenar la información oculta en errores deliberados en la base de tiempo del flujo de datos.

Sin embargo, puede implementarse cualquier otro canal oculto adecuado para impedir una lectura o escritura de la información oculta con unidades de disco existentes.

La tabla de bloqueo de claves KLT se reescribe cada vez que se cambia su contenido, por ejemplo, cuando se consume el derecho de uso. Por tanto, se usa una nueva clave de bloqueo de claves KLK aleatoria cada vez que se reescribe la tabla de bloqueo de claves KLT.

La figura 1 muestra una versión comprada de la tabla de bloqueo de claves KLT escrita en un disco óptico grabable, que se encripta por una primera clave de bloqueo de claves KLK-1 almacenada en un canal oculto del disco óptico, por ejemplo, como se indicó anteriormente. En el ejemplo mostrado en la figura 1, el usuario ha comprado un derecho para hacer tres copias de la pista n.º 2. En la tabla de bloqueo de claves KLT mostrada en la figura 1, sólo se muestra el contenido relevante para la pista n.º 2, en el que la tabla comprende una parte de identificador y una parte de datos y en el que la parte de identificador incluye una información usada para identificar los datos respectivos en la parte de datos. En particular, una clave (indicada en notación hexadecimal) va seguida de un derecho de uso de pista n.º 2 para la pista n.º 2 (indicada en notación binaria) y de un valor de contador de la pista n.º 2, que se ajusta a “3” en línea con el derecho de uso comprado.

Tras la operación de copia de la pista n.º 2, una nueva clave de bloqueo de claves KLK-2 se selecciona aleatoriamente por la unidad de disco, usada para reencriptar la tabla de bloqueo de claves KLT actualizada, y se almacena en el canal oculto. Por tanto, como se indica en la parte inferior de la figura 1, después de la primera copia de la pista dos, la tabla de bloqueo de claves KLT se ha reencriptado mediante la nueva clave de bloqueo de claves KLK-2 y actualizado disminuyendo el valor de contador en la tabla de bloqueo de claves KLT a”2”.

Por consiguiente, una extracción y almacenamiento intermedio de la tabla de bloqueo de claves KLT original o comprada, seguidos de un realmacenamiento después de que la primera operación de copia es inútil, puesto que la nueva clave de bloqueo de claves KLK-2 está almacenada ahora en el canal oculto y un desencriptado de la tabla de bloqueo de claves KLT por la unidad de disco ya no sería posible.

Por consiguiente, cualquier “ataque de copia y restablecimiento” se detecta inmediatamente por la unidad de disco o al menos lleva a un error.

La figura 2 muestra un diagrama de bloques básico de una unidad de disco según la realización preferida de la presente invención, que se dispone para generar y escribir una tabla de bloqueo de claves KLT junto con una obra digital DW (es decir, una pista de música o similar) en un disco 10 grabable basándose en el derecho de uso adquirido junto con una compra en Internet. En particular, una aplicación de EMD que puede ejecutarse en un sistema informático para proporcionar una correspondiente función de descarga almacena la obra digital codificada comprada junto con la clave requerida para decodificar la obra digital, y una descripción de los derechos de uso en una memoria 23 de la unidad de disco. Como alternativa, la diversa información comprada puede almacenarse en una memoria del sistema informático desde la que se leen por un controlador 21 de unidad de la unidad de disco.

El controlador 21 de unidad lee la diversa información comprada de la memoria 23 y suministra la clave y los derechos de uso a una unidad 22 de actualización y encriptado de bloqueo de claves que se dispone para generar una correspondiente tabla de bloqueo de claves KLT y para seleccionar aleatoriamente una clave de bloqueo de claves KLK usada para encriptar la tabla de bloqueo de claves KLT. El controlador 21 de unidad recibe la tabla de bloqueo de claves KLT y la clave de bloqueo de claves KLK generadas y controla una unidad 20 de lectura y escritura (RW) para escribir la obra digital DW comprada (es decir pista de música) y la tabla de bloqueo de claves KLT en posiciones predeterminadas en el disco 10 grabable. Además, el controlador 21 de unidad controla la unidad 20 de RW para almacenar la clave de bloqueo de claves KLK en un canal oculto del disco 10 grabable, que no es accesible por unidades de disco o lectores de disco convencionales. Con cada cambio del derecho de uso comprado debido a un consumo (es decir, operación de copia o lectura), el controlador 21 de unidad suministra una correspondiente señal de control a la unidad 22 de actualización y encriptado de bloqueo de claves que actualiza la

tabla de bloqueo de claves KLT de manera correspondiente, genera una nueva clave de bloqueo de claves KLK seleccionada aleatoriamente, y encripta la tabla de bloqueo de claves KLT usando la nueva clave de bloqueo de claves KLT. El controlador 21 de unidad recibe la tabla de bloqueo de claves KLT actualizada y codificada y la nueva clave de bloqueo de claves KLK y controla la unidad 20 de RW para escribir la tabla de bloqueo de claves KLT recodificada en el disco 10 grabable y la nueva clave de bloqueo de claves KLK en el canal oculto.

Esta actualización y reencriptado usando una nueva clave de bloqueo de claves KLK se realiza por tanto después de cada cambio dentro de la tabla de bloqueo de claves KLT.

Si la tabla de bloqueo de claves KLT actualizada indica que los derechos de uso se han ejercido o consumido, el controlador 21 de disco deniega el uso de la respectiva obra digital, por ejemplo, transmitiendo un correspondiente mensaje de error o señal de control a la aplicación de EMD.

Debe observarse que la unidad 22 de actualización y encriptado de bloqueo de claves puede implementarse como una rutina de software del controlador 21 de unidad

La figura 3 muestra un diagrama de flujo básico del procedimiento anterior para una actualización segura de los derechos de uso. Según la figura 3 una nueva clave de bloqueo de claves KLK-2 aleatoria se genera en la etapa S 100 después de que el disco grabable se haya cargado en la unidad de disco y haya comenzado una correspondiente operación de uso de la obra digital. Entonces, el contenido de la tabla de bloqueo de claves KLT se actualiza y se encripta con la nueva clave de bloqueo de claves KLK-2 por la unidad 22 de actualización y encriptado de bloqueo de claves (etapa S101). A continuación, la nueva clave de bloqueo de claves KLK-2 se escribe por la unidad 20 de RW en el canal oculto HC del disco 10 grabable (etapa S 102). A esta etapa pueden seguir las etapas opcionales de verificar que la nueva clave de bloqueo de claves KLK-2 y la tabla de bloqueo de claves KLT reencriptada se han escrito correctamente en el disco 10 grabable.

Finalmente, la clave de bloqueo de claves KLK-1 previa puede destruirse por la unidad 20 de RW (etapa S103).

Según una modificación alternativa de la realización preferida, la unidad 22 de actualización y encriptado de bloqueo de claves puede reemplazarse por una unidad de actualización y verificación de bloqueo de claves dispuesta para calcular una suma de control sobre el contenido de la tabla de bloqueo de claves KLT y para almacenar esta suma de control en el canal oculto HC (en lugar de la clave de bloqueo de claves KLK). En este caso, la tabla de bloqueo de claves KLT ni siquiera necesita encriptarse. Cualquier manipulación del contenido de la tabla de bloqueo de claves KLT puede verificarse por la unidad de actualización y verificación de bloqueo de claves mediante una operación de comprobación que usa la suma de control oculta. Cualquier cambio de la tabla de bloqueo de claves KLT que resulta de un consumo o ejercicio de los derechos de uso comprados lleva a una suma de control cambiada que se escribe en el canal oculto HC. Por tanto, el “ataque de copia y restablecimiento” llevará a un desajuste entre la suma de control real de la tabla de bloqueo de claves KLT restablecida y la suma de comprobación oculta. Este desajuste se detectará por la unidad de actualización y verificación de bloqueo de claves, de manera que puede iniciarse un mecanismo de procesamiento de errores o de protección.

Por tanto, la presente invención proporciona la ventaja de que un “ataque de copia y restablecimiento” lleva a un desajuste entre la clave de bloqueo de claves KLK oculta o la suma de control alternativa oculta y la tabla de bloqueo de claves KLT restablecida. Este desajuste o bien impide decodificar la tabla de bloqueo de claves KLT o lleva a un error en el procesamiento de verificación.

Por tanto, el ataque fraudulento puede detectarse en la unidad de disco.

En otra realización, el canal oculto comprende datos aleatorios que se usan para calcular una suma de control sobre el contenido de la tabla de bloqueo de claves KLT, suma de control que se almacena en los datos de usuario, por tanto de libre acceso, tanto para dispositivos conformes como no conformes. Si se determina que el contenido del canal oculto no puede cambiarse de manera determinística por un dispositivo no conforme, el contenido del canal oculto puede ser de libre acceso. Un dispositivo conforme puede calcular la suma de control leyendo los datos aleatorios en el canal oculto y comprobar si la suma de control calculada corresponde a la suma de control presente en los datos de usuario. Una suma de control calculada que difiera de la suma de control presente en los datos de usuario indica que el contenido del canal oculto podría haberse manipulado.

Se observa que la presente invención no se limita a las realizaciones anteriores, sino que puede aplicarse a cualquier aplicación de grabación o escritura que deba protegerse frente a “ataques de copia y restablecimiento”. La EMD puede realizarse mediante una distribución libre de la obra digital DW codificada en un disco prensado o a través de un canal de difusión.

Sin embargo, la clave no se distribuye entonces junto con el contenido de la obra digital. Puede comprarse a través de Internet. En tal caso, no es necesaria una descarga de la obra digital comprimida, sólo tienen que descargarse las claves. De este modo, puede disminuirse la carga de red y los costes de transmisión.

Además, la tabla de bloqueo de claves KLT puede disponerse como una tabla de bloqueo de claves por pista. En este caso, se requiere suficiente capacidad del canal oculto para almacenar una clave de bloqueo de claves KLK aleatoria para cada tabla de bloqueo de claves KLT. La tabla de bloqueo de claves KLT podría dividirse en una pluralidad de tablas de bloqueo de claves si su tamaño se vuelve demasiado grande para realizar una operación de reescritura en cada transacción. Entonces, cada tabla de bloqueo de claves KLT tendrá su propia clave de bloqueo de claves KLK aleatoria almacenada en el canal oculto.

La presente invención también puede aplicarse para proteger discos duros frente a “ataques de copia y restablecimiento”. En este caso, el canal oculto podría disponerse como una memoria incrustada en el controlador de HDD. Una aplicación similar es posible para tarjetas de memoria flash o similares. Generalmente, la presente invención puede aplicarse para proteger cualquier medio de grabación adicional, por ejemplo, medio de grabación magneto-óptico (*minidisc*) o cinta magnética.

REIVINDICACIONES

1. Método para controlar la distribución y el uso de una obra digital, que comprende las etapas de:

escribir la obra digital y la información relativa a un derecho de uso de la obra digital en un soporte de grabación, definiendo la información relativa al derecho de uso una o más condiciones que deben satisfacerse a fin de ejercer el derecho de uso;

actualizar el derecho de uso adscrito en cada consumo del derecho de uso; y

denegar el uso de la obra digital si no se satisfacen la una o más condiciones;

caracterizado porque:

el derecho de uso se verifica usando información oculta almacenada en el soporte de grabación, cambiando la información oculta cuando el derecho de uso se actualiza.

2. Método según la reivindicación 1, caracterizado además porque el derecho de uso se almacena en una tabla de bloqueo de claves (KLT) y la información oculta es una suma de control calculada sobre el contenido de la tabla de bloqueo de claves.

3. Método según la reivindicación 1, caracterizado además porque la información oculta se almacena en un canal oculto.

4. Método según la reivindicación 1, en el que puede accederse libremente a la información oculta.

5. Método según la reivindicación 1, caracterizado además porque la información oculta comprende datos aleatorios.

6. Método según la reivindicación 5, caracterizado además porque los datos aleatorios se usan para calcular una suma de control.

7. Método según la reivindicación 1, caracterizado además porque las condiciones de uso comprenden una o más de varias copias autorizadas de la obra digital que pueden hacerse y varias veces que la obra digital puede leerse.

8. Método según la reivindicación 1, caracterizado además porque el consumo del derecho de uso se produce cuando la obra digital o bien se lee o bien se reproduce.

9. Método según la reivindicación 1, caracterizado además porque la información oculta es información dispuesta para no ser accesible por al menos uno de dispositivos de reproducción comerciales y dispositivos de lectura comerciales.

10. Método de control de distribución y uso de una obra digital, que comprende las etapas de:

escribir la obra digital y la información adscrita relativa a un derecho de uso de la obra digital en un soporte de grabación, definiendo la información relativa al derecho de uso una o más condiciones que deben satisfacerse a fin de ejercer el derecho de uso;

actualizar la información adscrita relativa al derecho de uso en cada consumo del derecho de uso; y

denegar el uso de la obra digital cuando las condiciones no se satisfacen;

caracterizado porque:

el derecho de uso se encripta usando información oculta almacenada en el soporte de grabación, cambiando la información oculta siempre que el derecho de uso se actualiza.

11. Método según la reivindicación 10, caracterizado además porque la información oculta se almacena en errores deliberados de un flujo de datos que comprende la obra digital, pudiendo corregirse los errores.

12. Método según la reivindicación 10, caracterizado además porque la información oculta se almacena en bits de fusión de una secuencia de código de coordenada diferencial limitada.

13. Método según la reivindicación 10, caracterizado además porque la información oculta se almacena controlando la polaridad de una coordenada diferencial predeterminada de datos predeterminados o

símbolo de control de una secuencia de código de coordenada diferencial limitada.

14. Método según la reivindicación 10, caracterizado además porque la información oculta se almacena en errores deliberados en la base de tiempo de un flujo de datos que comprende la obra digital.

15. Método según la reivindicación 10, caracterizado además porque la información oculta es una clave usada para desencriptar la información relativa al derecho de uso, en el que la clave se cambia aleatoriamente siempre que el derecho de uso se actualiza y la información relativa al derecho de uso se reencripta usando la clave cambiada.

16. Método según la reivindicación 10, caracterizado además porque la información oculta se dispone para no ser accesible por dispositivos de reproducción comerciales.

17. Aparato para controlar la distribución y el uso de una obra digital que comprende:

un elemento de escritura que escribe la obra digital y la información adscrita relativa a un derecho de uso de la obra digital en el soporte de grabación, definiendo la información relativa al derecho de uso una o más condiciones que deben satisfacerse a fin de ejercer el derecho de uso;

una unidad de actualización que actualiza la información adscrita relativa al derecho de uso cuando se consume el derecho de uso; y

un controlador que deniega el uso de la obra digital cuando las condiciones no se satisfacen;

caracterizado porque:

la unidad de actualización actualiza información oculta almacenada en el soporte de grabación cuando el derecho de uso se actualiza.

18. Aparato según la reivindicación 17, caracterizado además porque la información oculta se usa para encriptar el derecho de uso.

19. Aparato según la reivindicación 17, caracterizado además porque la información oculta se usa para verificar el derecho de uso.

20. Aparato según la reivindicación 17, caracterizado además porque el derecho de uso se consume cuando la obra digital contenida en el soporte de grabación o bien se lee o bien se reproduce.

21. Aparato según la reivindicación 17, caracterizado además porque la información oculta se almacena en el soporte de grabación en un canal oculto.

22. Aparato según la reivindicación 17, caracterizado además porque puede accederse libremente a la información oculta.

23. Aparato según la reivindicación 17, caracterizado además porque la información oculta comprende datos aleatorios.

24. Aparato según la reivindicación 17, caracterizado además porque la información oculta es información dispuesta para no ser accesible por al menos uno de dispositivos de reproducción comerciales y dispositivos de lectura comerciales.

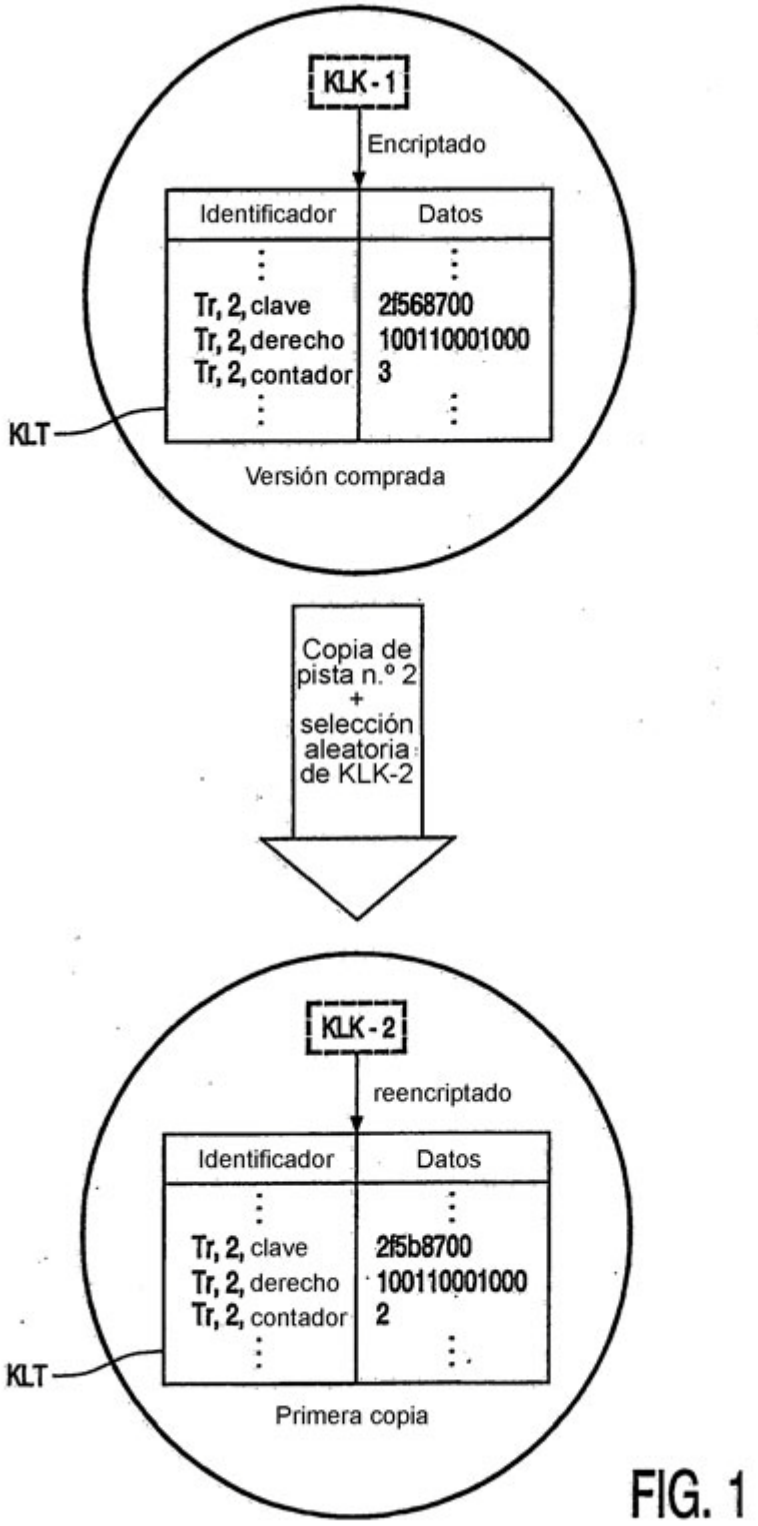
KLK-1
Encriptado
Identificador
Datos
Tr, 2, clave
Tr, 2, derecho
Tr, 2, contador
2f568700
100110001000
3
KLT
Versión comprada
Copia de pista n.º 2 + selección aleatoria de KLK-2
KLK-2
reencriptado
Identificador
Datos
Tr, 2, clave
Tr, 2, derecho
Tr, 2, contador
2f5b8700
100110001000
2
KLT
Primera copia

FIG. 1

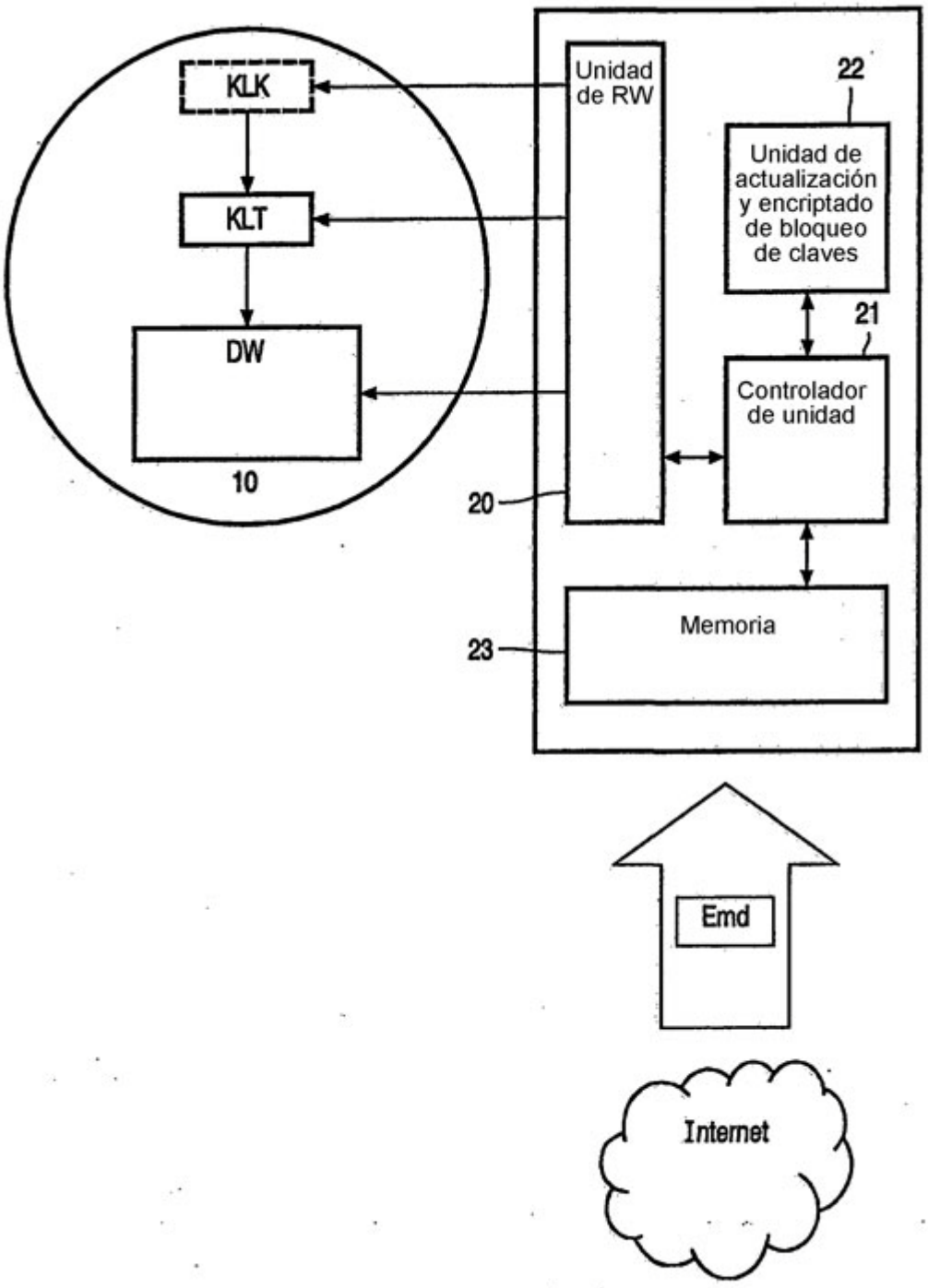
KLK
KLT
DW
10
Unidad de RW
22
Unidad de actualización y encriptado de bloqueo de claves
21
Controlador de unidad
20
Memoria
23
Emd
Internet

FIG. 2

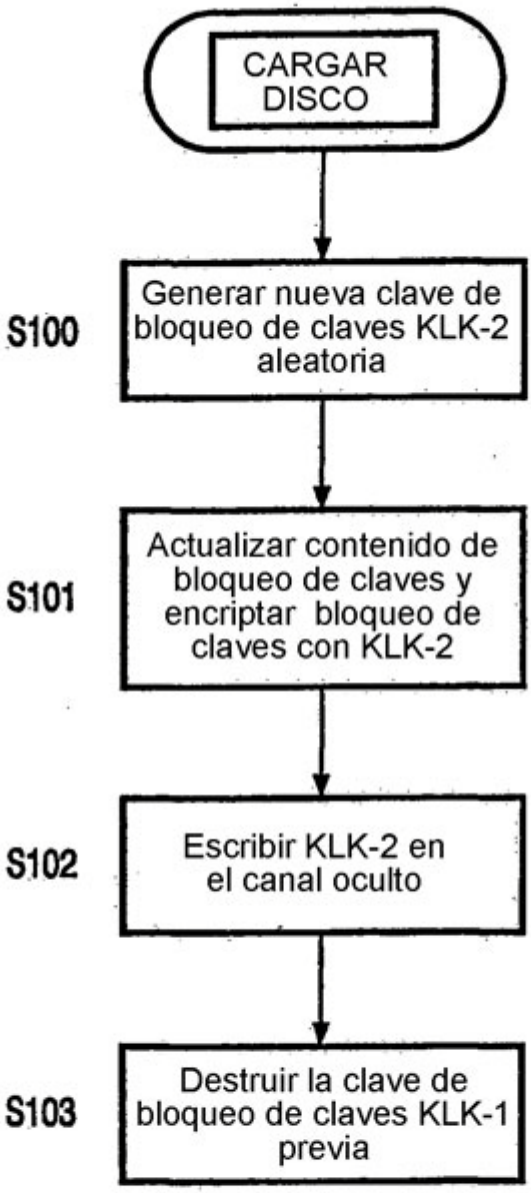
CARGAR DISCO
S100
Generar nueva clave de bloqueo de claves KLK-2 aleatoria
S101
Actualizar contenido de bloqueo de claves y encriptar bloqueo de claves con KLK-2
S102
Escribir KLK-2 en el canal oculto
S103
Destruir la clave de bloqueo de claves KLK-1 previa

FIG. 3