(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 169**

(51) Int. Cl.:
G11B 20/00 (2006.01)
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **99947521 .3**
(96) Fecha de presentación : **11.10.1999**
(97) Número de publicación de la solicitud: **1123545**
(97) Fecha de publicación de la solicitud: **16.08.2001**

(54) Título: **Método copiar datos digitales que evita la duplicación bit a bit y dispositivo de lectura para llevar a cabo dicho método.**

(30) Prioridad: **19.10.1998 FR 98 13074**

(45) Fecha de publicación de la mención BOPI:
29.06.2011

(45) Fecha de la publicación del folleto de la patente:
29.06.2011

(73) Titular/es: **Thomson Multimedia**
46 quai Alphonse Le Gallo
92100 Boulogne Billancourt, FR

(72) Inventor/es: **Furon, Teddy;**
Chevreau, Sylvain y
Diehl, Eric

(74) Agente: **Arpe Fernández, Manuel**

DESCRIPCIÓN

Método copiar datos digitales que evita la duplicación bit a bit y dispositivo de lectura para llevar a cabo dicho método.

La presente invención se refiere a un método para copiar en un soporte de grabación datos digitales, obtenidos a partir de una primera fuente que evita la duplicación bit a bit. También se refiere a un dispositivo utilizado para llevar a cabo dicho método.

Los datos digitales presentan la peculiaridad de poder copiarse sin una notable pérdida de calidad. Efectivamente, la copia consiste en transmitir desde la fuente hacia el dispositivo de grabación una serie de informaciones binarias, es decir, “unos” y “ceros”. Los errores que se producen habitualmente durante el proceso de copia se corrigen fácilmente utilizando los conocidos métodos de corrección de error. De este modo, cuando un medio de soporte de información o una fuente de datos contiene datos digitales, resulta relativamente sencillo grabarlos de forma idéntica en un soporte registrable.

Para proteger los datos digitales contra las copias ilegales se utilizan diversos métodos.

Normalmente, el proveedor proporciona al soporte de grabación de datos digitales, que puede ser un disquete, en el caso de un programa, de una marca que impide cualquier copia.

En los documentos EP-A-0773490 y EP 0802527 se propone un sistema de protección de la información almacenada en medios de grabación, en el que cada medio incluye un identificador.

Otra forma de proteger los datos digitales contra la copia consiste en dotarlos de un tatuaje o “marca de agua”, es decir, datos auxiliares que se adjuntan a los datos digitales. El tatuaje debe ser imposible de modificar y de borrar. En este caso, la lectura de los datos se efectúa con la ayuda de una clave privada que identifica el tatuaje. Cuando eventualmente se produce una copia de los datos digitales tatuados se requiere una clave privada para incluir el tatuaje en la copia, en ausencia de la cual la copia pasará a ser una copia ilegal, al estar desprovista del tatuaje. Los datos digitales copiados sin tatuaje no pueden ser leídos por el lector, ya que este no identifica el tatuaje en el lugar en el que debería encontrarse. De este modo, el tatuaje no permite efectuar una copia sin la clave privada.

Estos conocidos métodos de protección de las copias son generalmente eficaces cuando el soporte se procesa mediante dispositivos de lectura y grabación legales. No obstante, estos métodos no evitan su duplicación por parte de un pirata, que crea un doble o un clon lo más parecido posible al original, realizando lo que se denomina una copia bit a bit.

La presente invención tiene por objeto proponer un método de copia que evite la duplicación no autorizada, en un soporte de grabación, de datos digitales obtenidos a partir de una primera fuente, de forma que dicho método no permita una copia bit a bit de la información digital.

La presente invención también tiene por objeto facilitar un dispositivo de lectura que incorpore circuitos que permitan llevar a cabo dicho método.

Por consiguiente, la presente invención tiene por objeto un método de copia que evite la duplicación bit a bit, en un soporte de grabación, de los datos obtenidos a partir de una fuente de datos digitales.

Las características de la presente invención se definen en las reivindicaciones adjuntas.

Se apreciarán otras características y ventajas de la presente invención mediante la lectura de la descripción de un modo de realización preferido, haciendo referencia a la figura adjunta, en la cual:

La figura 1 es una vista esquemática, en forma de organigrama, de un dispositivo de lectura y un dispositivo de grabación que permite la copia de un primer soporte en un segundo soporte.

La presente invención se describirá haciendo referencia a la lectura de datos digitales grabados en un soporte digital, tal como un DVD, o Disco Versátil Digital, y su copia en un segundo soporte virgen constituido asimismo por un DVD, que en este caso debe ser registrable, a saber, un DVD-R. No obstante, es evidente para cualquier experto en la materia que pueden utilizarse otras fuentes de información digital, concretamente las informaciones digitales obtenidas a partir de un decodificador y enviadas a través de un canal de radiodifusión, o informaciones digitales almacenadas en soportes tales como una cinta magnética, un disco óptico, grabable o no, a saber, un CD, un CD-R, CD-RW, DVD, DVD-R, un disco magneto-óptico o similar. El soporte de grabación está constituido por una cinta magnética grabable, un CD-R, un CD-RW, un DVD-R o un disco magneto-óptico que permitan almacenar la información de audio y/o vídeo en formato digital.

Como se muestra en la figura 1, el método de copia de acuerdo con la presente invención permite copiar las informaciones digitales D grabadas en un DVD 1 utilizando un dispositivo de lectura 2 equipado con un circuito de formateado 3, y los datos formateados FD que pueden duplicarse se graban en un DVD-R 4 insertado en un dispositivo de grabación 5.

De acuerdo con la presente invención, el DVD-R 4 constituido por un DVD-R virgen incluye un número de serie que se graba de forma que no pueda falsificarse en el momento de la fabricación del DVD-R. Este número de serie, que se selecciona de forma que resulte único o que presente una escasa probabilidad de estar presente en dos soportes diferentes se almacena una zona oculta del disco, como la zona denominada “área lead-in”, o lo que es lo mismo, el inicio de la pista. Como se explica de forma más detallada a continuación, este número de serie se utiliza para formatear los datos digitales leídos a partir del DVD 1 original.

De acuerdo con el método reivindicado en la presente invención, los datos leídos en el DVD 1 por el dispositivo de lectura 2 se envían a un circuito de formateado 3 que lleva a cabo el formateado de los datos utilizando el número de serie leído en el DVD-R virgen. De este modo se obtienen en el dispositivo de lectura unos datos FD formateados de una forma específica, que se envían al dispositivo de grabación 5, en el que se graban en el DVD-R 4.

Para realizar un formateado de los datos de forma que los datos grabados en el DVD-R no puedan copiarse bit a bit, pero puedan volver a leerse posteriormente en el dispositivo de lectura, o lo que es lo mismo, para realizar una copia legal, pueden utilizarse diferentes procedimientos de formateado. Uno de los procedimientos de formateado clásicos, es un algoritmo de encriptado con clave secreta, como el D.E.S., o "Data Encryption Standard", perfectamente conocido por los especialistas. Para evitar que se realicen copias piratas, la clave utilizada en este caso será una clave construida con la ayuda de una clave secreta y del número de serie que se ha leído en el DVD virgen. Para llevar a cabo el formateado utilizando este algoritmo, los datos grabados en el DVD de origen se descomponen en bloques de 64 bits y después son formateados por la D.E.S. utilizando una clave de 56 bits obtenida a partir de los números de serie. Como resultado de ello, se obtienen unos paquetes de datos formateados o cifrados de 64 bits, que se graban mediante el dispositivo de grabación 5 en el DVD-R 4. Si la clave está constituida por el propio número de serie, el número de serie tendrá 54 bits. No obstante, el número de bits del número de serie se facilita a título de ejemplo. En efecto, es posible aplicar la invención a soportes cuyos números de serie tengan longitudes superiores o inferiores a 56 bits. En este caso, se puede aplicar un truncamiento o una codificación por canal para que estos números de serie tengan la longitud adecuada. Si, por razones de seguridad, la clave es una función del número de serie, podrá obtenerse de la forma siguiente:

Sabiendo que NS es el número de serie del soporte de grabación, y PS es el parámetro almacenado en los dispositivos de lectura legales de forma segura:

- se lleva a cabo la concatenación de NS y PS para tener una palabra (NS/PS),
- se aplica la función de troceo (hash), tal como la función SHA-1 (norma del National Institute of Standards and Technologies) y se obtiene como resultado la palabra SHA (NS/PS) con una longitud de 64 bits, y
- se lleva a cabo un truncamiento de esta palabra para obtener una palabra de 56 bits, que servirá como clave para la DES.

La longitud de las palabras binarias NS y PS no es fija, ya que SHA 1 no requiere una longitud precisa para la palabra de entrada. La función 1 se adapta a cualquier longitud de número de serie.

El DVD-R 4 copiado legalmente de este modo puede ser leído por el dispositivo de lectura 2, y los datos digitales originales se recuperan utilizando el correspondiente algoritmo de descifrado.

También es posible llevar a cabo el formateado de los datos digitales a duplicar, utilizando un algoritmo de clave pública como el algoritmo R.S.A. Este algoritmo de clave pública es un algoritmo asimétrico que no permite, a menos que se conozca la clave pública, copiar fácilmente los datos formateados cuando se leen en el dispositivo de lectura 2.

Los datos que se encuentran en el DVD-R de copia y que no tienen la misma estructura que los datos del DVD original sólo podrán recuperarse mediante un dispositivo de lectura legal. Por otra parte, si se ha efectuado una copia bit a bit del DVD original, el dispositivo de lectura de la presente invención no recupera las informaciones digitales de origen, por lo que no se leerá dicha información.

De acuerdo con una característica suplementaria de la presente invención, el método de copia puede ir precedido de una etapa de verificación de la autorización de copia, tal como la que se describe en la solicitud de patente francesa Nº 9811860, presentada el 23 de septiembre de 1998 en nombre de THOMSON multimedia, y titulada "Protección contra la copia de datos digitales almacenados en un soporte de grabación de información". Esta verificación de la autorización de copia se aplica a un soporte de grabación de información que comprende una primera identificación de un cifrado de los datos digitales, una segunda identificación de un tatuaje de los datos digitales, una primera determinación de una primera marca en caso que el cifrado y el tatuaje hayan podido ser identificados, una tercera identificación de un tipo de soporte de grabación de la información, una segunda determinación de una segunda marca, en el caso de que la primera marca se hubiese podido determinar, y si se hubiese podido identificar un tipo determinado de soporte de grabación de la información, una cuarta identificación de los datos de firma criptográfica que acompaña a los datos digitales, una tercera determinación de una tercera marca en caso de haberse podido determinar la segunda marca, y si se hubiese podido identificar un dato de firma criptográfica, un primer otorgamiento de un permiso de copia digital de los datos digitales, en caso de que se hubiese determinado la tercera marca.

El conjunto de las características que se describen en esta solicitud de patente francesa se incorporan a la presente solicitud para llevar a cabo la verificación de la autorización de copia.

De acuerdo con la presente invención, el dispositivo de lectura 2 de los datos digitales, que puede ser un lector de DVD, un decodificador, un lector de CDs o similar incluye un circuito de formateado 3 constituido esencialmente por un circuito integrado que incluye todos los medios necesarios para la realización del algoritmo seleccionado para el formateado, y que permite almacenar de forma infalsificable una serie de datos, tales como una clave secreta o unos medios de autorización de copia.

El modo de realización que se ha descrito anteriormente se facilita a título de ejemplo, y puede modificarse sin alejarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para copiar en un soporte de grabación (4) datos digitales obtenidos a partir de una fuente de datos digitales (1) que evita la duplicación bit a bit, caracterizado porque dicho método incluye:
- una etapa de formateado de los datos digitales obtenidos a partir de dicha fuente de datos digitales en función de un número de serie (NS) contenido en dicho soporte de grabación (4) y de un parámetro secreto (PS) almacenado en todos los dispositivos de lectura (2) adaptados para la lectura de los datos digitales obtenidos a partir de dicha fuente, siendo el número de serie (NS) un número único para cada soporte de grabación, o que presenta una baja probabilidad de ser común a dos soportes, y
- una etapa de escritura de dichos datos formateados (FD) en dicho soporte de grabación.

2. Método de acuerdo con la reivindicación 1, caracterizado porque el número de serie (NS) se graba de forma infalsificable en el soporte de grabación (4) en el momento de su fabricación.

3. Método de acuerdo con cualquiera de las reivindicaciones 1 o 2, caracterizado porque la etapa de formateado de los datos digitales a duplicar se lleva a cabo utilizando un algoritmo de encriptado con clave secreta, como el D.E.S., o con clave pública, como el R.S.A.

4. Método de acuerdo con la reivindicación 3, caracterizado porque la clave de encriptado es una función del número de serie (NS) y del parámetro secreto (PS).

5. Método de acuerdo con la reivindicación 1, caracterizado porque dichos datos se leen mediante un dispositivo de lectura (2), y porque el número de serie (NS) grabado en el soporte (4) se envía al dispositivo de lectura (2).

6. Método de acuerdo con la reivindicación 5, caracterizado porque la etapa de formateado de los datos digitales se lleva a cabo en el dispositivo de lectura (2).

7. Método de acuerdo con cualquiera de las reivindicaciones 5 o 6, caracterizado porque el dispositivo de lectura (2) incluye medios que permiten la lectura del soporte que contiene los datos digitales formateados.

8. Método de acuerdo con cualquiera de las reivindicaciones 5 a 7, caracterizado porque antes de efectuarse la duplicación de los datos digitales incluye una etapa de verificación de la autorización de copia.

9. Dispositivo de lectura (2) que permite llevar a cabo un método de copia de acuerdo con una las reivindicaciones 1 a 8, caracterizado porque contiene un parámetro secreto (PS) y porque el dispositivo de lectura comprende un circuito de formateado (3) adaptado para recibir el número de serie (NS) del soporte en el que deben copiarse los datos digitales y que proporciona unos datos formateados (FD) en función de dicho número de serie (NS) y del parámetro secreto (PS) destinados a ser copiados en dicho soporte.

10. Soporte de grabación (4) de datos digitales que incluyen un número de serie (NS) único o que presente una escasa probabilidad de estar presente en otro soporte, caracterizado porque también incluye unos datos digitales (FD) grabados, estando formateados dichos datos digitales (FD) en función de dicho número de serie (NS) y de un parámetro secreto (PS) contenido en un dispositivo de lectura adaptado para la lectura de los datos digitales.

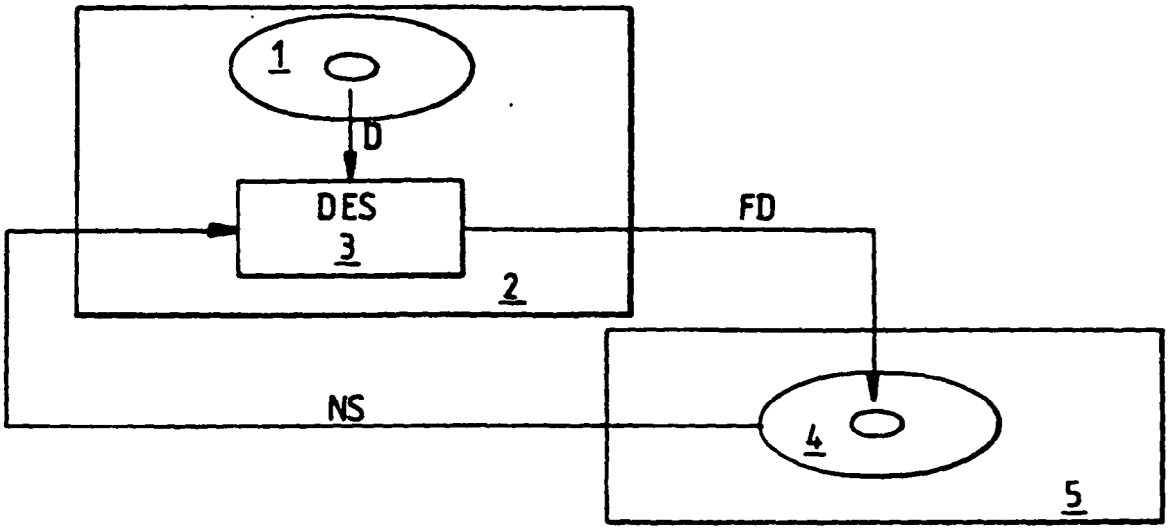

FIG.1

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- EP 0773490 A **[0005]**
- EP 0802527 A **[0005]**
- FR 9811860 **[0022]**