(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 279 634**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99943037 .4**
(86) Fecha de presentación : **23.09.1999**
(87) Número de publicación de la solicitud: **1116228**
(87) Fecha de publicación de la solicitud: **18.07.2001**

(54) Título: **Método para protección contra copia de datos digitales almacenados en un soporte de información.**

(30) Prioridad: **23.09.1998 FR 98 11860**

(45) Fecha de publicación de la mención BOPI:
16.08.2007

(45) Fecha de la publicación del folleto de la patente:
16.08.2007

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

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

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

DESCRIPCIÓN

Método para protección contra copia de datos digitales almacenados en un soporte de información.

La invención se refiere a un método y a un dispositivo que permiten proteger contra copia los datos digitales almacenados en un soporte de información.

Una posibilidad inherente a los datos digitales es que pueden ser copiados sin una pérdida notable de calidad, debido a que la copia consiste en la transmisión desde la fuente al dispositivo de grabación de una serie de "1" y "0". La mayor parte de los errores que pueden surgir en el momento de la copia pueden paliarse utilizando unos métodos de corrección de error. De este modo, cuando un soporte de información contiene datos digitales, resulta en principio relativamente fácil grabar en un soporte registrable de forma idéntica el contenido del soporte de información.

Se utilizan numerosos tipos de soportes de información para almacenar informaciones de todo tipo en formato digital. Por ejemplo, se puede almacenar información de audio y/o vídeo en formato digital en una banda magnética, un disco óptico, registrable o no (CD, CD-R, CD-RW, DVD, DVD-R, disco magneto-óptico, etc., que son respectivamente las iniciales en inglés de Compact Disc, CD-Recordable, CD-Read Write, Digital Versatile Disc, DVD-Recordable).

A fin de proteger mejor, por ejemplo, el interés de los autores de la información almacenada o el de los fabricantes de soportes de información pregrabados, resulta deseable limitar la posibilidad de copiar los datos digitales libremente y con facilidad. En la actualidad existen diversos mecanismos y posibilidades de protección de los datos digitales contra una copia ilegal.

Como es conocido, los datos digitales pueden cifrarse cuando se almacenan en el soporte de información. El cifrado permite limitar la utilización de los datos digitales al poseedor de una clave pública o privada de descifrado. Por ejemplo, el cifrado se utiliza para proteger datos en los DVD, discos ópticos utilizados para almacenar datos de vídeo en formato digital. De este modo, un dispositivo de lectura de DVD necesita una clave adecuada para descifrar los datos leídos en el DVD.

Una forma de proteger los datos digitales contra la copia consiste en dotarlos de una marca de agua, es decir unos datos auxiliares adjuntos a los datos digitales. La marca de agua debe ser no modificable y no debe poderse borrar. La lectura de los datos se efectúa con ayuda de una clave pública que identifica la marca de agua. La clave pública es un código bien conocido por el público, o más exactamente incorporado a la mayor parte de dispositivo de lectura es de soportes de información. Cuando se efectúa una eventual copia de los datos digitales con marca de agua, se requiere una clave privada para volver a insertar la marca de agua en la copia, sin que la copia sea ilegal, ya que está desprovista de marca de agua. La clave privada está en poder del autor o del fabricante de la información marcada de este modo. Los datos digitales copiados en la marca de agua no pueden ser leídos por el dispositivo de lectura, pues este no identifica la marca de agua en el lugar donde debería encontrarla. De este modo, la marca de agua no permite realizar copias sin la clave privada. Si es necesaria una copia, el dispositivo dispositivo de grabación debe integrar dicha clave privada.

La marca de agua no impide la copia de los datos digitales a través de un sistema analógico, es decir una copia que precisaría previamente una conversión de los datos digitales a una señal analógica y que tomaría la señal analógica como origen de la copia.

Una solución conocida para evitar la copia de un soporte digital por vía analógica, y más concretamente en el ámbito del vídeo y de la televisión, consiste en integrar la señal analógica de tal forma que pueda ser utilizada para visualizar una imagen en la pantalla de un televisor por medio de una entrada analógica de dicho televisor, pero que la misma señal no pueda ser utilizada para hacer una copia con un magnetoscopio. Más concretamente, se utiliza un circuito electrónico para influir sobre los parámetros de sincronización de imagen. Estos parámetros de sincronización son percibidos de forma diferente por un televisor y por un magnetoscopio. Esta solución no permite impedir la copia digital de datos digitales.

Otra solución para limitar las copias digitales de datos digitales consiste en dotar a estos de informaciones de gestión de generaciones. En principio, esta información incorpora la información "no copiar jamás" en el caso de los datos que carecen de derecho a ser copiados, y la información "copia" o "copia número X" si los datos son una copia de primera o x-ésima generación de un original. De este modo, con la ayuda de esta información, un dispositivo de grabación puede saber si los datos digitales a copiar tienen derecho a ser copiados digitalmente e impedir la copia si esta se encuentra prohibida para la segunda o (X+1)-ésima generación. Cada vez que se efectúa una copia, se actualiza la información de gestión de generaciones. Esta manipulación de la información de gestión de generaciones hace que sea vulnerable a las falsificaciones. Efectivamente, la información de gestión de generaciones se encuentra en una fase de la copia disponible en abierto, es decir en un formato descodificado. La manipulación también requiere que el dispositivo de grabación digital esté equipado en ese sentido.

La información de gestión de generaciones no permite por sí misma evitar las copias analógicas.

El documento WO-A-9713248 describe un método de marca de agua de datos digitales codificados de acuerdo con la norma MPEG en el cual la marca de agua se inserta mediante la selección de parámetros de codificación particulares, por ejemplo el número de tramas por imagen. También se describe un sistema de protección contra copia que utiliza una combinación de marcador de soporte y de marcador de contenido (como marca de agua) para autorizar o no la descodificación de datos por parte de un dispositivo de lectura de discos ópticos.

Un objeto de la invención consiste en encontrar una solución de protección contra copia digital en la que no se disponga en abierto de ninguna información relativa a la generación de copia durante el proceso de copiado.

Otro de los objetos de la invención consiste en encontrar una solución en la que no se efectúe ninguna modificación de los datos relativos a la protección contra copia al efectuarse la grabación de una copia.

Una solución propuesta por la invención prevé un método para protección contra copia de datos digitales almacenados en un soporte de información que consiste en expedir un permiso o una prohibición de

copia y/o de lectura de dichos datos digitales en función de la identificación o no de al menos:

- un cifrado de dichos datos digitales; y
- una marca de agua de dichos datos digitales.

De acuerdo con una característica especial de la invención, se expide un permiso o una prohibición de copia y/o de lectura de dichos datos digitales en función además de la identificación de un tipo registrable o no registrable de dicho soporte de información.

De acuerdo con otra característica especial de la invención, se expide un permiso o una prohibición de copia y/o de lectura de dichos datos digitales en función además de la identificación o no de una firma criptográfica que acompaña a dichos datos digitales.

Una primera realización ventajosa de la invención prevé que se otorgue un permiso de copia digital cuando:

- se haya identificado un cifrado de dichos datos digitales;
- se haya identificado una marca de agua de dichos datos digitales;
- se haya identificado un tipo de soporte no registrable; y
- se haya identificado una firma criptográfica acompañando a dichos datos digitales.

Una segunda realización ventajosa de la invención prevé que se otorgue un permiso de copia digital cuando:

- no se haya identificado un cifrado de dichos datos digitales; y
- no se haya identificado una marca de agua de dichos datos digitales.

Una tercera realización ventajosa de la invención prevé que se expida una prohibición de lectura de dichos datos digitales cuando:

- no se haya identificado un cifrado de dichos datos digitales; y
- se haya identificado una marca de agua de dichos datos digitales.

Una cuarta realización ventajosa de la invención prevé que se expida una prohibición de copia cuando:

- se haya identificado un cifrado de dichos datos digitales;
- se haya identificado una marca de agua de dichos datos digitales; y
- se haya identificado un tipo se soporte registrable.

Una quinta realización ventajosa de la invención prevé que se expida una prohibición de copia cuando:

- se haya identificado un cifrado de dichos datos digitales;
- se haya identificado una marca de agua de dichos datos digitales;
- se haya identificado un tipo se soporte no registrable; y
- no se haya identificado firma criptográfica alguna acompañando a dichos datos digitales.

Una sexta realización ventajosa de la invención prevé una conversión de los datos digitales en señales analógicas y una alteración de las señales analógicas si se ha expedido una prohibición de copia digital.

Una séptima realización ventajosa de la invención prevé que la prohibición de copia digital incluya una supresión de salida de datos digitales.

Otra solución propuesta por la invención prevé un dispositivo de lectura de datos digitales almacenados en un soporte de información que incluya, al menos,

- una salida digital para proporcionar señales representativas de los datos digitales al efectuar la lectura de dichos datos digitales;
- una salida analógica para facilitar señales analógicas representativas de los datos digitales al efectuar la lectura de dichos datos digitales;
- unos medios de detección de:
  - el cifrado de dichos datos digitales;
  - la marca de agua de dichos datos digitales;
  - un tipo registrable o no registrable de dicho soporte de información;
  - una firma criptográfica que acompañe a dichos datos digitales;
  - un sistema para descifrar dichos datos digitales cuando se detecta un cifrado;
- un sistema de protección contra copia de dichos datos digitales que recibe señales procedentes de dichos medios de detección y que genera una señal de autorización de copia o una señal de prohibición de copia, y que incorpora la primera, la segunda, la cuarta o la quinta de las realizaciones descritas anteriormente;
- medios de control de la grabación que suprimen las señales transmitidas a la salida digital cuando dichos medios de control reciben una señal de prohibición de copia por parte del sistema de protección;
- un sistema de protección de lectura que recibe las señales procedentes de dichos medios de detección y que genera una señal de prohibición de lectura e incorpora la cuarta realización descrita anteriormente; y
- medios de control de lectura que interrumpen la lectura de los datos o su salida hacia la salida analógica cuando dichos medios de control reciben una señal de prohibición de lectura por parte del sistema de protección.

Seguidamente, se presentan unos ejemplos de realización que permiten ilustrar y comprender mejor la invención haciendo referencia a las figuras 1 a 8 descritas brevemente a continuación:

La figura 1 contiene un organigrama que muestra un modo de realización de la invención;

Las figuras 2 a 5 contienen organigramas que muestran aspectos de la invención;

La figura 6 contiene un organigrama que muestra una conversión digital-analógica de acuerdo con la invención,

La figura 7 contiene un esquema que muestra un dispositivo de acuerdo con la invención.

La figura 1 incluye un organigrama en el que los datos digitales almacenados en un soporte de información 1 se someten a una primera identificación de un cifrado 2 a fin de verificar si los datos digitales están almacenados en formato cifrado, y posteriormente a una segunda identificación de una marca de agua 3 para ver si los datos están provistos de una marca de agua digital. Una primera bifurcación 4 permite distinguir los casos en los que se identifica un cifrado 5 o no 6. Una segunda bifurcación 7 permite distinguir los casos en los que se identifica una marca de agua 8 o no 9. Si se verifican los casos 5 y 8, una primera determinación 10 genera una primera marca #1.

Una tercera identificación 11 de un tipo de soporte de información 1 sirve para comprobar si el soporte de información es, por ejemplo, de tipo no registrable o registrable. Los datos digitales propiamente dichos

pueden contener información sobre el tipo, que también puede obtenerse a partir de medidas físicas de parámetros del soporte de información 1 por ejemplo cuando se produce la inicialización en un dispositivo de lectura del soporte de información 1. Una tercera bifurcación 12 permite distinguir los casos en los que el tipo sería de un tipo determinado 13, por ejemplo un soporte de información no registrable tal como un disco óptico impreso o no 14. Si se verifica el caso 13 y se ha generado la primera marca #1, una segunda determinación 15 generará entonces una segunda marca #2.

Una cuarta identificación 16 de datos de firma criptográfica sirve para comprobar si los datos digitales poseen una firma criptográfica. Una cuarta bifurcación 17 permite distinguir los casos en los que la firma criptográfica está presente 18 o no 19. Si se verifica el caso 18 y se ha generado la segunda marca #2, una tercera determinación 20 generará entonces una tercera marca #3.

En presencia de la tercera marca #3 se lleva a cabo una primera expedición 21 de una autorización de copia digital 22 de los datos digitales.

En su conjunto, el organigrama de la figura 1 muestra cómo diversos criterios relativos a los datos digitales pero también al soporte de información pueden tener como consecuencia la expedición de una autorización de copia digital, siendo la idea el no permitir la copia excepto en unas condiciones definidas. Por ejemplo, los datos no deben haber sido manipulados ni deben haber sido cifrados y con marca de agua. Seguidamente, los datos no deben haber sido copiados todavía. Si los datos se encuentran en un disco no registrable, los datos estarán entonces *a priori* en un soporte de información original. Finalmente, los datos deben poseer una firma criptográfica. Esta indica que los datos pueden ser copiados. En este punto los datos reciben la autorización de copia digital. El resultado de la copia de los datos será idéntico al original, salvo en lo que respecta al soporte de información, que deberá ser registrable. Una nueva copia de los datos a partir del soporte de información registrable resultaría imposible, pues la segunda marca #2 no podría ser generada después de la tercera identificación 11. Efectivamente, la tercera bifurcación 12 nos situaría en el caso 14.

Pueden preverse otras situaciones cuando, por ejemplo, no se puedan identificar el cifrado o la marca de agua de los datos digitales. Normalmente, el cifrado y la marca de agua van unidos y la ausencia de una u otro son un síntoma de manipulación ilícita de los datos digitales. En este caso, se trata de ir más allá que simplemente prohibir la copia de los datos digitales. Es preciso impedir su lectura.

El organigrama de la figura 2 muestra dos ejemplos en los que el cifrado y la marca de agua no se han identificado conjuntamente. Un ejemplo prevé que la primera bifurcación 4 nos lleve al caso 6, es decir que la primera identificación de un cifrado sea negativa, y que la segunda bifurcación 7 nos lleve al caso 9, es decir que la segunda identificación de una marca de agua sea negativa. En este otro caso, la segunda concesión genera la prohibición de lectura 24.

El método descrito permite copiar libremente los datos digitales que no están protegidos, por ejemplo aquellos datos desprovistos de cifrado y de marca de agua. La figura 3 contiene un organigrama en el que la primera y la segunda bifurcación 4 y 7 nos llevan, cada una de ellas, a un caso de identificación negativa, respectivamente el caso 6, en lo tocante al cifrado, y el caso 9, en lo que se refiere a la marca de agua. Así pues, una tercera concesión genera directamente el permiso de copia digital 22.

En este último caso importa poco el que los datos se encuentren en un soporte de información registrable o no. La ausencia de codificación y de marca de agua indica un nivel de protección de datos mínimo.

En ciertos casos, los datos deben poder ser leídos y utilizados, pero no copiados. Esto es lo que sucede, por ejemplo, cuando se adquiere un soporte de información que contiene datos digitales cuyo autor o fabricante desea evitar que se copien. Esto es también lo que sucede cuando se lee un soporte de información registrable que contiene datos copiados legalmente. Este caso se ilustra con la ayuda de un organigrama en la figura 4, en la que una cuarta concesión 26 comprueba si se ha expedido la primera marca #1 y que ha tenido lugar el caso 14 de identificación de un tipo de soporte de información diferente del tipo determinado, antes de generar una prohibición de copia 27. En la práctica, el dispositivo de lectura debería implementar un dispositivo que impida la copia de los datos digitales, por ejemplo, inhibiendo una salida digital del dispositivo de lectura.

Se muestra otro caso con ayuda de un organigrama de la figura 5. Si se identifica la segunda marca #2 y el caso 19 señala una cuarta identificación negativa, es decir, que no se encuentra presente ninguna firma criptográfica que permita la copia de los datos, una quinta concesión 28 generará entonces la prohibición de copia 27.

Queda entendido que el hecho de no identificar firma criptográfica alguna que permita una copia de los datos no excluye la presencia de una firma criptográfica específica que prohíba la copia.

Ya se ha mencionado a lo largo de la descripción el hecho de que el soporte de información 1 se utiliza en un dispositivo de lectura apropiado. Los datos digitales almacenados en el soporte de información 1 pueden ser dirigidos, en ciertos casos, hacia una salida digital del dispositivo de lectura. En el ejemplo de un dispositivo de lectura de DVD (disco óptico para datos digitales de vídeo y audio) puede preverse una salida digital para la salida de una señal representativa de los datos hacia un dispositivo de lectura/dispositivo de grabación DVD-R (o de otro tipo) con fines de copia, o hacia un ordenador, para efectuar el tratamiento de las imágenes. En general, el dispositivo de lectura prevé también una salida analógica a fin de poder transmitir una señal analógica representativa de los datos digitales hacia la entrada analógica, por ejemplo, de un televisor.

El organigrama de la figura 6 indica mediante una flecha discontinua que el soporte de información ofrece datos digitales 29. Una conversión 30 permite convertir los datos digitales 29 en señales analógicas 31. La presencia del permiso de copia digital 22, junto con una cualquiera de las marcas primera, segunda o tercera (#1, #2, #3) o una presencia de la prohibición de copia digital 27 se detecta mediante un proceso de detección 32, lo que en su caso desencadena una alteración 33 de las señales analógicas para obtener unas señales analógicas alteradas 34. Las señales analógicas se alteran, por ejemplo, de forma que puedan ser utilizadas para obtener imágenes en un televisor, pero

que sea imposible copiarlas con la ayuda de un magnetoscopio con entrada analógica.

Ventajosamente, se ha previsto una supresión en una salida digital del dispositivo de lectura de datos digitales 35 en presencia de la prohibición de copia digital 27.

El cifrado de los datos digitales en el soporte de información se lleva a cabo normalmente por el fabricante.

Los datos digitales, así como la firma criptográfica que está eventualmente asociada a ellos son descodificados en el dispositivo de lectura de datos. Pero cuando estos datos deben transmitirse a través de una salida digital del dispositivo de lectura, los datos son cifrados.

Un dispositivo de lectura de datos digitales 42, como el mostrado en la figura 7, incluye una salida digital 43 que permite facilitar señales representativas de los datos digitales al efectuar una lectura de los datos digitales de un soporte de información. Esta salida 43 puede, por ejemplo, ser realizada con la ayuda de un bus digital acorde con la norma IEEE 1394. Una salida analógica 44 permite proporcionar las señales analógicas representativas de los mismos datos digitales. Un sistema de decodificador 45 permite descifrar los datos digitales si estos están codificados, pero también identificar la posible marca de agua y los datos de la firma criptográfica. El sistema de decodificador permite llevar a cabo, por ejemplo, las identificaciones 2, 3, 11 y 16 del método mostrado en la figura 1.

Un sistema de protección contra copia de los datos digitales 46 utiliza las señales emitidas por el sistema de descifrado 45, y las evalúa llevando a cabo las determinaciones 10, 15 y 20 del método mostrado en la figura 1, y emite, después de haber determinado las marcas #1, #2 y #3 una señal de autorización de copia.

Una parte de control de grabación 47 permite gestionar un flujo de datos digitales hacia la salida digital. Concretamente, esta parte permite activar el flujo cuando se obtiene del sistema de protección 46 la señal de autorización de copia.

El sistema de protección contra copia de los datos digitales 46 puede también desempeñar la función de un sistema de protección contra lectura. Este último sistema genera, con la ayuda de las señales recibidas desde el sistema de codificación 45 una señal de prohibición de lectura cuando los datos digitales no están descifrados, sino con marca de agua, o incluso cuando los datos digitales están cifrados pero no con marca de agua.

Una sección de control de la lectura 48 permite interrumpir la lectura de los datos digitales al recibir la señal de prohibición del sistema de protección contra lectura 46.

Lista de referencias

1. soporte de información
2. primera identificación de un cifrado
3. segunda identificación de una marca de agua
4. primera bifurcación
5. cifrado identificado
6. cifrado no identificado
7. segunda bifurcación
8. marca de agua identificada
9. marca de agua no identificada
10. primera determinación

#1. primera marca

11. tercera identificación de un tipo de soporte de información
12. cuarta bifurcación
13. tipo determinado
14. no es el tipo determinado
15. segunda determinación

#2. segunda marca

16. cuarta identificación de datos de firma criptográfica
17. cuarta bifurcación
18. firma criptográfica presente
19. firma criptográfica no presente
20. tercera determinación

#3. tercera marca

21. primera concesión
22. autorización de copia digital
23. segunda concesión
24. prohibición de lectura de datos digitales
25. tercera concesión
26. cuarta concesión
27. prohibición de copia
28. quinta concesión
29. datos digitales
30. conversión
31. señales analógicas
32. detección
33. alteración
34. señales analógicas alteradas
35. supresión de salida de los datos digitales
42. dispositivo de lectura de datos digitales
43. salida digital
44. salida analógica
45. sistema de descifrado
46. sistema de protección para copia de datos digitales
47. parte de control de grabación
48. parte de control de la lectura.

REIVINDICACIONES

1. Método para protección contra copia de datos digitales almacenados en un soporte de información, consistente en expedir una autorización o una prohibición de copia y/o de lectura de dichos datos digitales en función de la identificación o no de al menos:

- un cifrado de dichos datos digitales; y
- una marca de agua de dichos datos digitales.

2. Método de acuerdo con la reivindicación 1, **caracterizado** porque se expide una autorización o una prohibición de copia y/o de lectura de dichos datos digitales en función, entre otros, de la identificación de un tipo registrable o no registrable de dicho soporte de información.

3. Método de acuerdo con una de las reivindicaciones 1 o 2, **caracterizado** porque se expide una autorización o una prohibición de copia y/o de lectura de dichos datos digitales en función, entre otros, de la identificación o no de una firma criptográfica que acompañe dichos datos digitales.

4. Método de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado** porque se expide (21) una autorización de copia digital (22) cuando:

- Se ha identificado un cifrado (2) de dichos datos digitales;
- Se ha identificado una marca de agua (3) de dichos datos digitales;
- Se ha identificado un tipo de soporte (11) no registrable; y
- Se ha identificado una firma criptográfica (16) que acompaña a dichos datos digitales.

5. Método de acuerdo con la reivindicación 1, **caracterizado** porque se expide (25) una autorización de copia digital (22) cuando:

- No se ha identificado un cifrado (2) de dichos datos digitales; y
- No se ha identificado una marca de agua (3) de dichos datos digitales;

6. Método de acuerdo con la reivindicación 1, **caracterizado** porque se expide una prohibición de lectura (24) de dichos datos digitales cuando:

- No se ha identificado un cifrado (2) de dichos datos digitales; y
- No se ha identificado una marca de agua (3) de dichos datos digitales.

7. Método de acuerdo con una de las reivindicaciones 1 o 2, **caracterizado** porque se expide (26) una prohibición de copia (27) cuando:

- Se ha identificado un cifrado (2) de dichos datos digitales;
- Se ha identificado una marca de agua (3) de dichos datos digitales; y
- Se ha identificado un tipo de soporte (11) registrable.

8. Método de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado** porque se expide (28) una prohibición de copia (27) cuando:

- Se ha identificado un cifrado (2) de dichos datos digitales;
- Se ha identificado una marca de agua (3) de dichos datos digitales;
- Se ha identificado un tipo de soporte (11) no registrable; y
- No se ha identificado una firma criptográfica (16) que acompaña a dichos datos digitales.

9. Método de acuerdo con una de las reivindicaciones 1 a 4, 7 u 8, **caracterizado** porque comprende:

- una conversión (30) de los datos digitales (29) en señales analógicas (31); y
- una alteración (33) de las señales analógicas cuando se ha expedido una prohibición de copia digital (27).

10. Método de protección de acuerdo con cualquiera de las reivindicaciones 7 u 8, **caracterizado** porque la prohibición de copia digital (27) comprende una supresión (35) de salida de los datos digitales.

11. Dispositivo de lectura de datos digitales almacenados en un soporte de información, que incluye al menos:

- Una salida digital (43) para emitir señales representativas de los datos digitales cuando se efectúa la lectura de dichos datos digitales;
- Una salida analógica (44) para emitir señales analógicas representativas de los datos digitales cuando se efectúa la lectura de dichos datos digitales;
- Medios (45) de detección de:
    - un cifrado de dichos datos digitales;
    - una marca de agua de dichos datos digitales;
    - un tipo registrable o no de dicho soporte de información;
    - una firma criptográfica que acompaña a dichos datos digitales;
- Un sistema para descifrar dichos datos digitales cuando se detecta un cifrado;
- Un sistema de protección (46) contra copia de dichos datos digitales, que recibe señales de dichos medios (45) de detección y que genera una señal de autorización de copia (22) o una señal de prohibición de copia (27) cuando se lleva a cabo el método de acuerdo con una de las reivindicaciones 4, 5, 7 u 8;
- Medios de control (47) de grabación, que suprimen las señales emitidas hacia la salida digital (43) cuando dichos medios de control reciben una señal de prohibición de copia (27) del sistema de protección (46);
- Un sistema de protección (46) de lectura que recibe señales procedentes de dichos medios (45) de detección, y que genera una señal de prohibición de lectura (24) cuando se lleva a cabo el método de acuerdo con la reivindicación 6; y
- Medios de control de lectura (48) que interrumpen la lectura de los datos o su salida hacia la salida analógica (44) cuando dichos medios de control reciben una señal de prohibición de lectura procedente del sistema de protección (46).

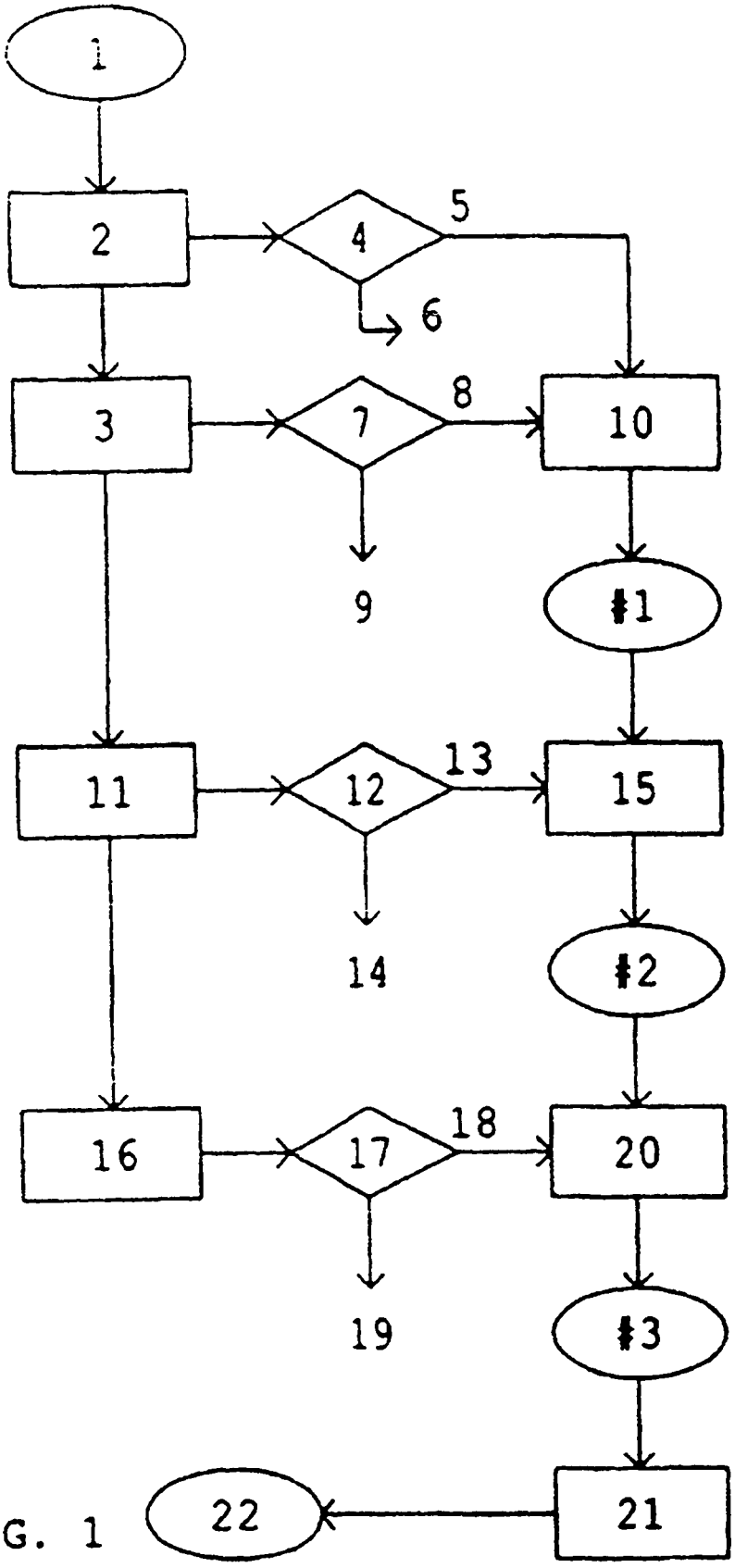

FIG. 1

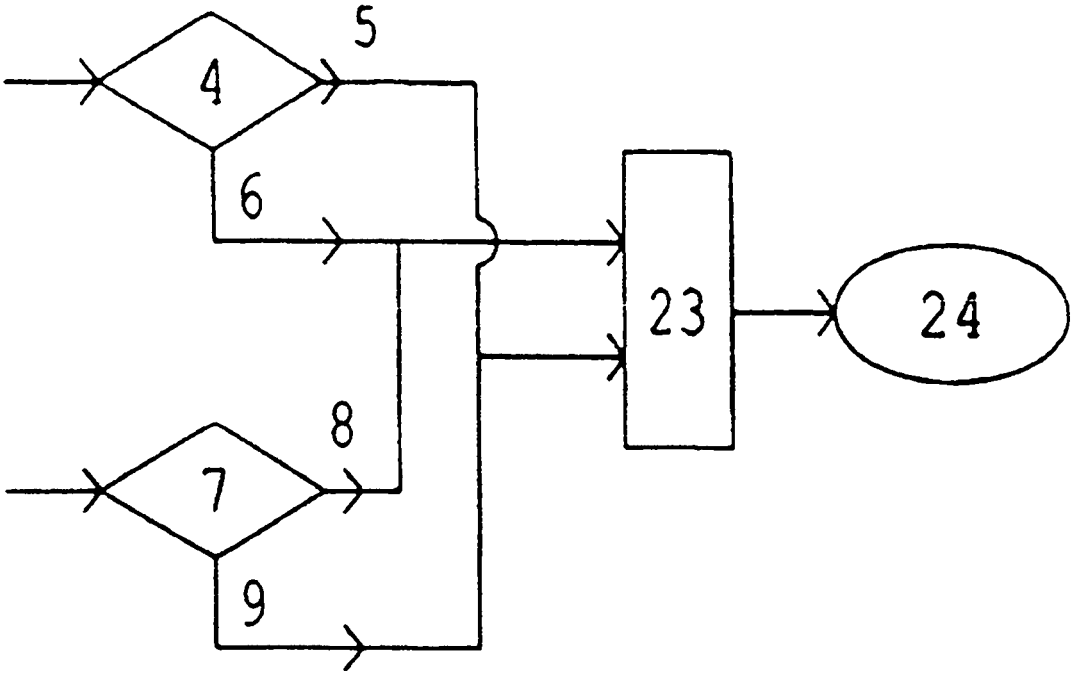

FIG. 2

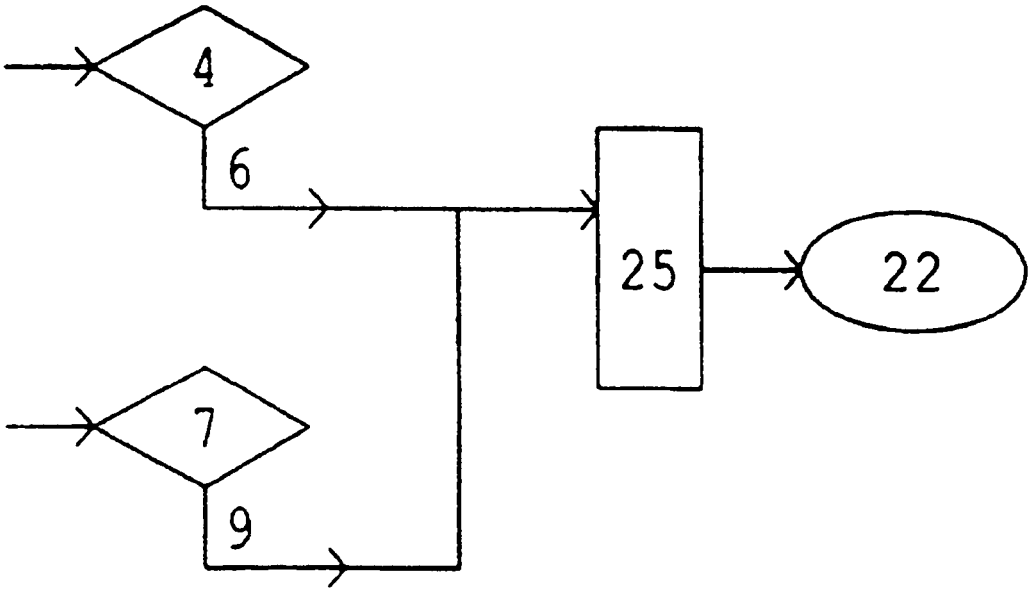

FIG. 3

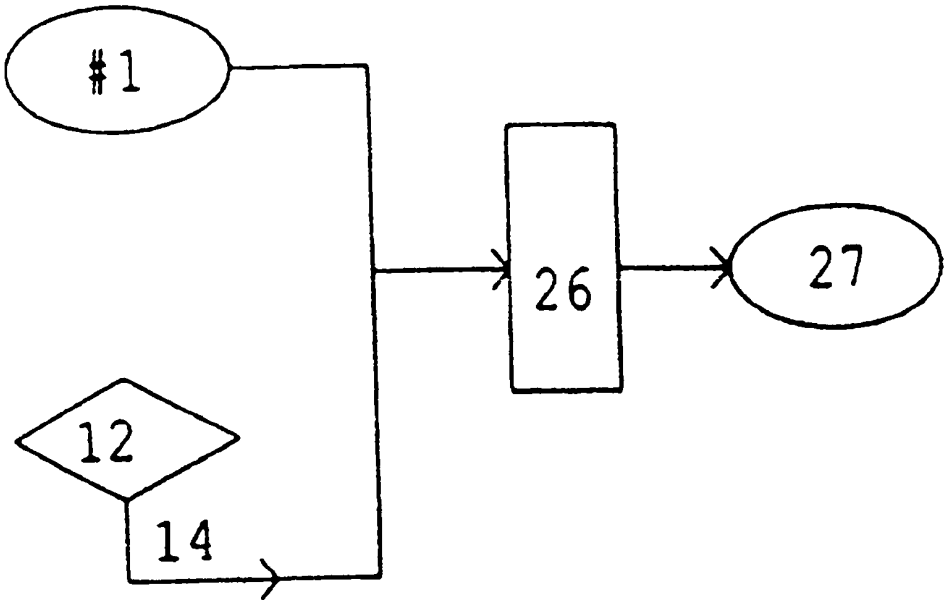

FIG. 4

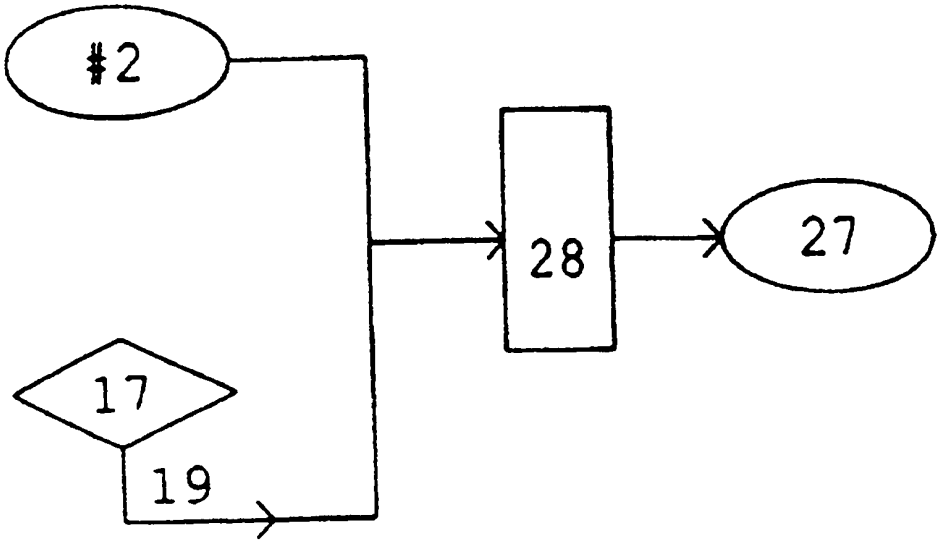

FIG. 5

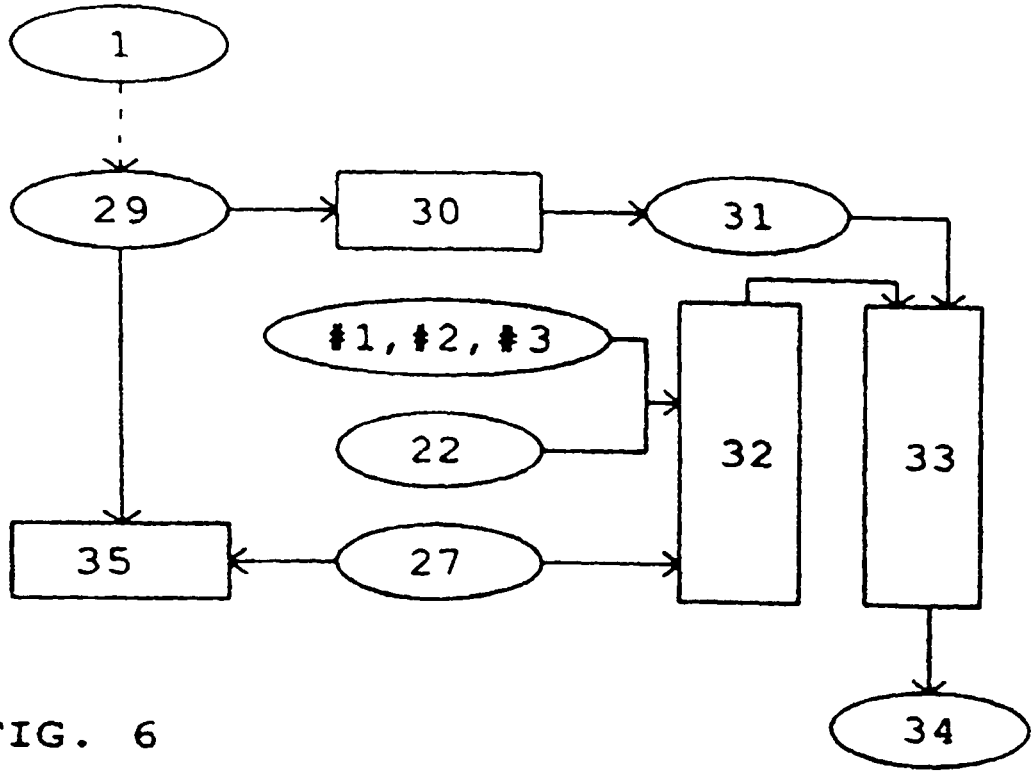

FIG. 6

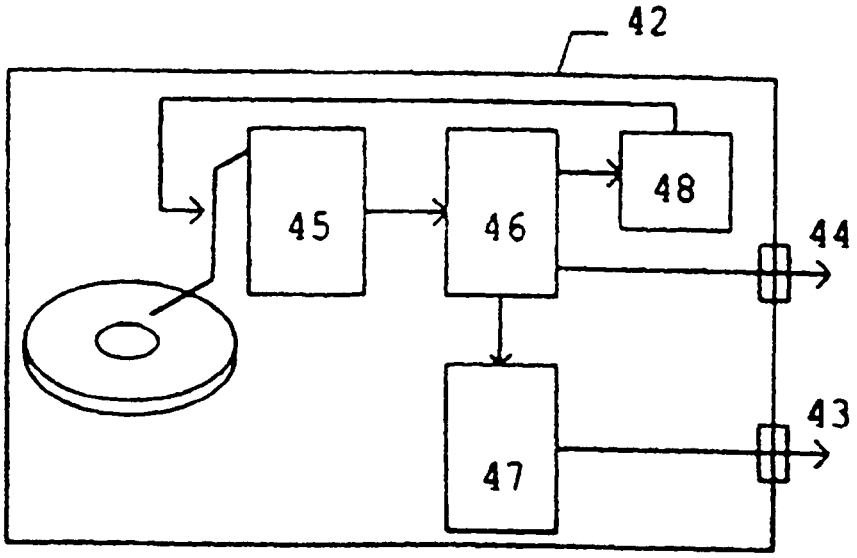

FIG. 7