(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 309 194**

(51) Int. Cl.:
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02765236 .1**
(96) Fecha de presentación : **12.09.2002**
(97) Número de publicación de la solicitud: **1442351**
(97) Fecha de publicación de la solicitud: **04.08.2004**

(54) Título: **Método y sistema para la distribución segura de contenidos.**

(30) Prioridad: **12.10.2001 EP 01203911**

(45) Fecha de publicación de la mención BOPI:
16.12.2008

(45) Fecha de la publicación del folleto de la patente:
16.12.2008

(73) Titular/es: **Koninklijke Philips Electronics N.V.**
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es: **Kelly, Declan, P. y**
Van Gestel, Wilhelmus, J.

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCIÓN

Método y sistema para la distribución segura de contenidos.

La invención se refiere a un sistema para la distribución segura de contenidos.

La tecnología DVD permite a los productores de contenidos ofrecer mucho más que una simple película en un disco. Debido a la gran capacidad de almacenamiento disponible, pueden proporcionarse todas las clases de contenido adicional en el disco. Por ejemplo, pueden incluirse secuencias tras las cámaras, tomas eliminadas, entrevistas con los directores y/o actores, subtítulos en diferentes idiomas y la banda sonora con vídeo clip.

Ahora que cada vez más sistemas de entretenimiento domésticos tienen acceso a Internet de alguna manera, resulta posible proporcionar contenido adicional no sólo en el disco de DVD, sino también en una página web. Esto se conoce como DVD conectado a web. En su forma más básica, un usuario que está viendo una película y una página web conectada para la película y para ver información adicional, ve nuevas entrevistas o reportajes sobre la película, etc. También podría participar en un juego en línea relacionado con la película.

Es deseable proteger este contenido adicional frente a una copia y/o acceso no autorizado. En particular, el acceso al contenido adicional debe restringirse sólo a personas que tienen un ejemplar legítimo del disco.

Una solución sencilla sería verificar en primer lugar de alguna manera que el usuario posee un ejemplar del disco de DVD y distribuir entonces el contenido adicional del servidor. Esto podría realizarse por ejemplo suministrando un identificador almacenado en el disco para la página web, en la que puede compararse con una lista de identificadores correctos. Sin embargo, la solución es muy insegura, ya que el identificador podría copiarse fácilmente de un ejemplar original y usarse mediante dispositivos no autorizados para acceder de manera ilegítima al contenido adicional.

El documento WO98/42098 da a conocer una técnica de gestión de derechos para contenido digital. El contenido se distribuye en un soporte de registro en forma encriptada. Ciertos fragmentos se ocultan y se proporcionan sólo tras la comunicación con un servidor autorizado. Los fragmentos se encriptan con las mismas claves que el contenido en el soporte.

El documento EP-A-1 267 244, que está comprendido en el estado de la técnica en virtud del artículo 54(3) CPE solo, describe un método de transferencia de información en un disco óptico en forma encriptada. El contenido adicional se descarga de un emplazamiento remoto. El contenido adicional se encripta usando una firma segura personalizada para el usuario formada a partir de datos que son únicos para cada disco óptico.

La invención se define mediante las reivindicaciones adjuntas.

Compartiendo la clave secreta y el mecanismo de seguridad, hay menos información sensible que es necesario proteger. En un DVD, la clave de título y la clave de disco sólo pueden obtenerse por un cliente (normalmente un dispositivo de presentación que está conectado a una unidad de DVD) a partir del disco de DVD, de modo que esto también garantiza que sólo los clientes que tienen acceso al soporte de registro puedan desencriptar el contenido adicional. Los mecanismos de seguridad usados para proteger el contenido de un DVD se diseñaron para resistir a los ataques activos de terceros malintencionados, y también pueden usarse para proteger el contenido adicional, que igualmente es atractivo para estos terceros.

Adicionalmente, implicando una clave secreta que sólo la pueda conocer si el receptor del contenido adicional tiene acceso al soporte de registro, la entidad distribuidora puede estar segura de que sólo los receptores que de verdad tienen acceso a ese soporte de registro pueden desencriptar el contenido adicional.

En una realización, el dispositivo comprende además medios de sincronización para sincronizar la obtención del contenido básico con la obtención del contenido adicional. En un DVD, en particular la clave de título puede variarse por sectores. Eligiendo que la clave secreta para proteger el contenido adicional sea la misma que la clave de título, esta clave secreta puede variarse al mismo tiempo que la clave de título. Entonces es necesario sincronizar la obtención de contenido básico y contenido adicional, de modo que la clave secreta correcta esté disponible para desencriptar el contenido adicional.

En una realización adicional, los medios de acceso condicional están dispuestos para ejecutar un protocolo de autenticación con el servidor usando un código de control de autenticación (ACC, *authentication control code*) secreto presente en el soporte de registro para establecer una clave de sesión, y usar la clave de sesión para encriptar el contenido adicional. El dispositivo sólo puede completar satisfactoriamente la autenticación si conoce el ACC, o al menos sólo puede deducir la clave de sesión correcta si conoce el ACC. Esto garantiza que el dispositivo sólo pueda desencriptar el contenido adicional si tiene acceso al soporte de registro.

En una realización, los medios de acceso condicional están dispuestos además para desencriptar el contenido adicional usando una clave de desencriptado que se usó también para desencriptar al menos una parte del contenido básico.

Estos y otros aspectos de la invención resultarán evidentes a partir de y se aclararán con referencia a las realizaciones mostradas en los dibujos, en los que:

la figura 1 muestra esquemáticamente los componentes principales de un sistema para hacer disponible el contenido adicional relacionado con contenido básico, que comprende una unidad de DVD y un dispositivo de presentación;

la figura 2 ilustra el sistema de aleatorización de contenidos de DVD para el caso en el que la unidad de DVD y el dispositivo de presentación estén instalados en un dispositivo de reproducción.

La figura 3 ilustra el sistema de aleatorización de contenidos para el caso en el que la unidad de DVD esté conectada usando una interfaz digital o un bus a un dispositivo de presentación externo;

y la figura 4 muestra esquemáticamente el dispositivo de presentación en más detalle.

En todas las figuras, los mismos números de referencia indican características similares o correspondientes. Algunas de las características indicadas en los dibujos se implementan normalmente en software, y como tales representan entidades de software, tales como objetos o módulos de software.

La figura 1 muestra esquemáticamente los componentes principales de un sistema 100 según la invención. El sistema 100 comprende un dispositivo 110 de reproducción y un dispositivo 120 de visualización. En una realización preferida, el dispositivo 110 de reproducción es un reproductor de DVD que comprende una unidad 111 de DVD y un dispositivo 112 de presentación, que puede realizarse como una tarjeta descodificadora. La unidad 111 de DVD y el dispositivo 112 de presentación también pueden proporcionarse como dispositivos separados físicamente. La unidad 111 de DVD puede instalarse por ejemplo en un ordenador, mediante lo cual el dispositivo 112 de presentación se proporciona como una aplicación de software que se ejecuta en el ordenador. El dispositivo 112 de presentación también puede instalarse en el dispositivo 120 de visualización, al igual que la unidad 111 de DVD.

Un usuario puede colocar un soporte 101 de registro, tal como un disco de DVD, en la unidad 111 de DVD. El contenido almacenado en el soporte 101 de registro se lee entonces y se suministra al dispositivo 112 de presentación, en el que se descodifica y se procesa para generar una señal de audio/vídeo. Esta señal de audio/vídeo se alimenta entonces al dispositivo 120 de visualización para su presentación al usuario. De esta manera, el usuario puede por ejemplo ver una película almacenada en un disco de DVD en su televisión.

El dispositivo 110 de reproducción está conectado además a una red 130 externa, que es preferiblemente Internet. La conexión a la red 130 externa puede realizarse con un módem de cable, una línea de ADSL o módem ordinario instalado en el dispositivo 110 de reproducción y conectado a una línea de teléfono. La conexión también puede realizarse conectando el dispositivo 112 de presentación a una Ethernet u otra red local que proporcione acceso a la red 130 externa. La conexión a la red 130 externa se usará para descargar contenido tal como películas o música, y así es preferiblemente una conexión de ancho de banda elevado.

También está conectado a la red 130 externa un servidor 140. El servidor 140 ofrece elementos 151 de contenido adicional para su descarga por ejemplo desde un almacenamiento 150. Los elementos 151 de contenido están relacionados con y extienden el contenido en el soporte 101 de registro. Por ejemplo, los elementos 151 de contenido pueden comprender diferentes versiones de la banda sonora de una película, doblajes de audio o subtítulos de texto para la película en diferentes idiomas, secuencias tras las cámaras, escenas adicionales, diferentes finales, juegos basados en la película, entrevistas con actores y otros participantes, eventos en directo relacionados con el contenido almacenado en el soporte 101 de registro, etc.

El soporte 101 de registro tendrá normalmente una indicación de algún tipo de que estos artículos 151 de contenido adicional están disponibles. Esto puede ser un mensaje de información impreso sobre la cubierta protectora del soporte 101 de registro, pero puede ser también un indicador legible por ordenador presente en el propio soporte 101 de registro. En ese caso, la unidad 111 de DVD puede detectar automáticamente el indicador. El dispositivo 110 de reproducción puede ofrecer entonces al usuario la opción de acceder a los elementos 151 de contenido adicional. Si el usuario lo aprueba, el dispositivo 110 de reproducción usa su conexión con la red 130 externa para contactar con el servidor 140. Entonces puede obtener una lista de elementos 151 de contenido adicional disponibles de los que el usuario puede seleccionar uno o más para acceder a ellos. Pueden concebirse fácilmente muchas otras maneras para acceder a, presentar y gestionar los elementos 151 de contenido adicional.

El contenido en el soporte 101 de registro comprende una pluralidad de denominados títulos. Un título puede ser por ejemplo un flujo de vídeo, un flujo de audio, etc. Para protegerse frente a una copia no autorizada, los títulos en el soporte 101 de registro pueden protegerse de una variedad de maneras.

En caso de que el soporte 101 de registro sea un disco de DVD, se usa el sistema de aleatorización de contenidos (CSS). En la figura 2, se facilita un resumen de cómo se usa el CSS en caso de que la unidad 111 de DVD y el dispositivo 112 de presentación estén instalados en un dispositivo 110 de reproducción. Este resumen, así como el resumen de la figura 3, se basa en información disponible públicamente en Internet y de otras fuentes tales como la conferencia pública sobre CSS de Gregory Kesden en la Carnegie Mellon University el 6 de diciembre de 2000. Una transcripción de esta conferencia está disponible en Internet en http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/.

El soporte 101 de registro contiene claves de disco encriptadas EDK (*Encrypted Disc Keys*) que están almacenadas en la denominada zona de entrada. La zona de entrada puede ser leída por unidades de DVD compatibles. La clave de disco es la misma para todo el contenido en el disco. Los datos están encriptados en unidades de un sector. Cada sector tiene una clave de título encriptada ETK (*Encrypted Title Key*) en el encabezamiento de sector. La clave de título puede cambiarse por sectores.

El dispositivo 110 de reproducción comprende una o más claves de reproducción, que pueden usarse para desencriptar la clave de disco encriptada EDK en el soporte 101 de registro, asumiendo por supuesto que el dispositivo 110 de reproducción mantiene una clave de reproducción correcta. En la etapa 201 la clave de disco encriptada EDK se obtiene del soporte 101 de registro, y se desencripta en la etapa 202. Habiendo desencriptado la clave de disco, el dispositivo 110 de reproducción recibe una clave de título encriptada ETK en la etapa 203 y usa la clave de disco desencriptada para desencriptar la clave de título en la etapa 204.

A continuación, los títulos encriptados se reciben en la etapa 205. La clave de título desencriptada se usa para desencriptar los datos en la etapa 206. El dispositivo 110 de reproducción puede desencriptar entonces las claves de título para los títulos deseados y acceder de este modo a los propios títulos. Los datos desencriptados pueden descodificarse para obtener una señal de audio/vídeo que se suministra en la etapa 207 al dispositivo 120 de visualización para presentarla al usuario.

En la figura 3 el CSS se ilustra para el caso en el que la unidad 111 de DVD está conectada usando una interfaz digital o un bus a un dispositivo 112 de presentación externo. Estas son las tres etapas principales que han de llevarse a cabo: autenticación, encriptado/desencriptado de bus seguro y desencriptado de datos, indicadas en la figura 3 como AUTH, SECBUS y DDEC, respectivamente.

En el proceso AUTH de autenticación se comprueba si el dispositivo 112 de presentación es un dispositivo compatible con DVD. La autenticación se lleva a cabo de la siguiente manera. El soporte 101 de registro lee el código de control de autenticación ACC mediante la unidad 111 de DVD. Se genera un número aleatorio RN1 en el dispositivo 112 de presentación. Este número RN1 se transmite a la unidad 111 de DVD. En la unidad 111 de DVD el número RN1 junto con el ACC se encripta con un algoritmo secreto en la etapa ER1 y el resultado de la etapa ER1 se transmite al dispositivo 112 de presentación.

En el dispositivo 112 de presentación el número RN1 se encripta múltiples veces en la etapa ER1', cada vez con un número i diferente. El resultado se compara en la etapa CMP1 para cada número i con el resultado de EA recibido desde la unidad 111 de DVD. Si los resultados de ER1 y ER1' coinciden para cierto valor de i, entonces el dispositivo 112 de presentación sabe que ese valor para el número i es el mismo que el valor del ACC tal como se lee desde el soporte 101 de registro.

Se genera un número aleatorio RN2 en la unidad 111 de DVD y se transmite al dispositivo 112 de presentación. El número se encripta en la etapa ER2 junto con el número de ACC en la unidad 111 de DVD. En el dispositivo 112 de presentación, el número aleatorio RN2 se encripta en la etapa ER2' junto con el valor de i que se encontró que era el mismo que el ACC en la etapa CMP1 anterior. En la unidad 111 de DVD, los resultados de las etapas ER2 y ER2' se comparan en la etapa CMP2 y si estos son los mismos, la unidad 111 de DVD concluye que el dispositivo 112 de presentación es un dispositivo compatible.

En la función de bus seguro SECBUS los números aleatorios RN1 y RN2 encriptados (es decir la salida de ER1, ER2 en la unidad 111 de DVD, y la salida de ER1' y ER2' en el dispositivo 112 de presentación) se usan para deducir una clave de bus seguro o clave de sesión SK (*session key*) tanto en la unidad 111 de DVD como en el dispositivo 112 de presentación. Se observa que, si se llevó a cabo satisfactoriamente el procedimiento de autenticación AUTH, las claves de sesión SK establecidas en los respectivos dispositivos son las mismas, y así pueden usarse para un intercambio seguro de datos.

En la unidad 111 de DVD, la clave de disco encriptada EDK y la clave de título encriptada ETK se leen del soporte 101 de registro y se encriptan (de nuevo) con esta clave de bus seguro SK en la etapas SEDK y SETK respectivamente. La clave de disco y clave de título encriptadas doblemente se transmiten entonces al dispositivo 112 de presentación.

En el dispositivo 112 de presentación se usa la clave de bus seguro SK para desencriptar la clave de disco y clave de título encriptadas doblemente en las etapas SDDK y SDTK respectivamente. El dispositivo 112 de presentación tiene ahora acceso a la clave de disco EDK y clave de título ETK encriptadas. El motivo de esta etapa de encriptado doble es garantizar que sea imposible obtener la clave de disco EDK y clave de título ETK encriptadas derivando la interfaz entre la unidad 111 de DVD y el dispositivo 112 de presentación.

En la función de desencriptado de datos DDEC el desencriptado de los sectores tiene lugar de la misma manera que la descrita en la figura 2. Resumiendo brevemente, el dispositivo 112 de presentación desencripta la clave de disco en la etapa DDK usando su clave de reproducción PK (*player key*), y entonces la clave de título en la etapa DTK usando la clave de disco. Usando la clave de disco y clave de título así obtenidas, el dispositivo 112 de presentación puede ahora desencriptar títulos individuales almacenados en el soporte 101 de registro.

La figura 4 muestra esquemáticamente el dispositivo 112 de presentación en más detalle. El dispositivo 112 de presentación comprende en este caso un módulo 401 de interfaz de red IEEE 1394, que está conectado a un bus 400 local de IEEE 1394. En esta realización, las comunicaciones con la unidad 111 de DVD se desplazan a través del bus 400 local. También pueden estar conectados otros dispositivos al bus 400 local.

En el dispositivo 112 de presentación hay un módulo 402 de autenticación que ejecuta las funciones de autenticación AUTH tal como se describió anteriormente con referencia a la figura 3. Hay también un módulo 403 criptográfico que ejecuta la función de encriptado/desencriptado de bus seguro SECBUS y la función de desencriptado de datos DDEC tal como se describió anteriormente con referencia a la figura 3.

El contenido desencriptado se alimenta desde el módulo 403 criptográfico al módulo 404 de salida. El módulo 404 de salida descodifica y procesa el contenido para generar señales de audio y/o vídeo para su salida en el dispositivo 441 de visualización y altavoz 442 respectivamente. El dispositivo 441 de visualización y el altavoz 442 juntos pueden considerarse como el dispositivo 120 de visualización. La generación de una salida de este tipo se conoce bien en la técnica. Resultará evidente que muchos medios 441, 442 audiovisuales diferentes están disponibles para reproducir la salida.

El módulo 404 de salida también puede almacenar el contenido en un medio 443 de almacenamiento. Por supuesto esto sólo se permite cuando los derechos asociados con el contenido recibido lo permiten. El medio 443 de almacenamiento puede ser, por ejemplo, un disco duro, una cinta de vídeo o un disco de DVD regrabable.

El dispositivo de presentación 120 comprende también un módulo 410 de red. Este módulo 410 de red proporciona acceso a la red 130 externa mencionada anteriormente, que preferiblemente es Internet. El módulo 410 de red puede realizarse por ejemplo como una tarjeta de red acoplada a un módem de cable junto con el software apropiado. También puede usarse un módem conectado a una línea de ADSL o una tarjeta de red acoplada a por ejemplo una LAN basada en Ethernet.

Tal como se explicó anteriormente con referencia a la figura 1, el módulo 410 de red en algún momento descarga elementos 151 de contenido adicional del servidor 140. Es deseable proteger los elementos 151 de contenido adicional frente a una copia y/o acceso no autorizado. En particular, el acceso a los elementos 151 de contenido adicional debe restringirse sólo a personas que poseen un ejemplar legítimo del soporte 101 de registro.

Según la invención, los elementos 151 de contenido adicional están protegidos mediante al menos uno de los mecanismos de seguridad que se usa también para proteger el contenido en el soporte 101 de registro. El mecanismo de seguridad emplea una o más claves secretas, tales como el ACC, la clave de disco o las claves de título. Una o más de estas claves secretas pueden usarse también cuando se aplica el mismo mecanismo de seguridad a los elementos 151 de contenido adicional.

Tras recibir los elementos 151 de contenido adicional protegidos, el módulo 410 de red los alimenta al módulo 403 criptográfico de modo que pueden desencriptarse y presentarse mediante el módulo 404 de salida al igual que el contenido básico en el soporte 101 de registro. Esta alimentación puede realizarse de un modo por flujo, por ejemplo alimentando bloques individuales de los elementos 151 de contenido adicional al módulo 403 criptográfico a medida que llegan, empleando preferiblemente alguna clase de mecanismo de almacenamiento intermedio por ejemplo para facilitar el flujo.

En una primera realización, el protocolo de autenticación descrito con referencia a la figura 3 se usa también entre el dispositivo 112 de presentación y el servidor 140. El dispositivo 112 de presentación se acopla ahora en el proceso de autenticación AUTH con el servidor 140 al igual que lo hacía antes con la unidad 111 de DVD. Es decir, el servidor 140 toma ahora el lugar de la unidad 111 de DVD. La red 130 toma ahora el lugar del bus seguro entre la unidad 111 de DVD y el dispositivo 112 de presentación.

En el proceso de autenticación AUTH de la figura 3 el dispositivo 112 de presentación determinó un valor i que es el mismo que el número de ACC del soporte 101 de registro tras una autenticación satisfactoria con la unidad 111 de DVD. El dispositivo 112 de presentación puede usar este valor i para demostrar al servidor 140 que tiene acceso al soporte 101 de registro. El servidor 140 puede suministrar entonces los elementos 151 de contenido adicional al dispositivo 112 de presentación.

El servidor 140 lee el número de ACC de un soporte de registro idéntico al soporte 101 de registro y usa este ACC como entrada para el proceso de autenticación. Al desviarse del proceso AUTH en la figura 3, el servidor 140 suministra ahora en primer lugar un número elegido aleatoriamente RN2" al dispositivo 112 de presentación, en el que se usa como entrada para ER2' junto con dicho valor de i igual al ACC. La salida de ER2' se suministra de vuelta al servidor 140 y se compara en CMP2 con la salida de ER2 usando RN2" y el ACC.

Si CMP2 es satisfactoria, el servidor 140 decide que el dispositivo 112 de presentación conoce el valor del ACC y por tanto debe tener acceso al soporte 101 de registro. Revirtiendo el intercambio de números aleatorios de este modo, no es posible que el dispositivo 112 de presentación pretenda tener acceso al ACC, o aprender el ACC a partir de interacciones con el servidor 140.

Para completar el proceso de autenticación, el dispositivo 112 de presentación genera ahora un número aleatorio RN1" y lo envía al servidor 140, en el que se usa tal como se describió anteriormente con referencia a la figura 3, excepto porque sólo es necesaria una iteración ya que el valor de i correcto ya se conoce. De esta manera se completa el proceso de autenticación y tanto el servidor 140 como el dispositivo 112 de presentación tienen las entradas necesarias para generar la clave de sesión SK. Uno o más de los elementos 151 de contenido adicional pueden transmitirse entonces al dispositivo 112 de presentación a través de la red 130 externa de un modo encriptado. En esta realización, la clave de disco y la clave de título del soporte 101 de registro pueden deducirse en el servidor 140.

Los elementos 151 de contenido adicional proporcionados por el servidor 140 usan la misma clave de disco y las mismas claves de título para toda la información que debe estar presente de manera sincrónica con el contenido original del soporte 101 de registro. Se usa información de temporización para detectar cambios en las claves de título. No es necesario transmitir estas claves a través de la red 130. A través de la red 130 se transmiten los elementos 151 de contenido adicional, comprimidos en sectores y encriptados en primer lugar con la clave de título y después con la clave de sesión. Resulta evidente que en esta realización el soporte 101 de registro y el soporte de registro usado en el servidor 140 deben ser iguales y tener las mismas claves.

En una segunda realización, se aplica la clave de disco del soporte 101 de registro. La autenticación tiene lugar tal como se describió anteriormente. La clave de disco y un clave de título fija se usan para encriptar los sectores. La clave de título fija es por ejemplo el patrón fijo "00" o un número aleatorio. En la última situación debe transmitirse de manera segura al dispositivo 112 de presentación.

La sincronización entre el soporte 101 de registro y el soporte de registro usado por el servidor 140 no es necesaria, ya que la clave de disco se conoce en ambos lados. El soporte 101 de registro correcto es necesario porque el servidor ha usado el número de ACC para deducir una clave de sesión y la clave de disco para encriptar los sectores. Sin embargo, estas claves no se transmiten a través de la red 130 externa.

En otra realización, no es necesaria una autenticación entre el servidor 140 y el dispositivo 112 de presentación. Este método puede usarse para distribuir contenido adicional a todos los propietarios del soporte 101 de registro, al mismo tiempo. El servidor 140 suministra ahora el/los elemento(s) 151 de contenido adicional encriptado(s) con las claves de disco y de título. Si se requiere la sincronización entre el contenido básico y el contenido adicional, entonces puede aplicarse el método descrito en la primera realización.

Si no es necesaria la sincronización, entonces el encriptado del contenido 151 adicional puede llevarse a cabo con la clave de disco del soporte 101 de registro y una clave de título que se elige por el servidor. Si esta clave de título no es fija, entonces se transmite encriptada al dispositivo 112 de presentación. Pueden usarse diferentes claves de título para encriptar diferente partes de un título. La clave necesaria para desencriptar los elementos 151 de contenido adicional puede variarse entonces de manera correspondiente.

También es posible distribuir los elementos 151 de contenido adicional sin ninguna autenticación, usando la clave de disco o clave de título del soporte 101 de registro como una clave de encriptado para encriptar los elementos 151 de contenido adicional antes de distribuirlos.

Debe observarse que las realizaciones mencionadas anteriormente ilustran más que limitan la invención, y que los expertos en la técnica podrán diseñar muchas realizaciones alternativas sin apartarse del alcance de las reivindicaciones adjuntas.

En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no debe interpretarse como que limita la reivindicación. La expresión "que comprende" no excluye la presencia de elementos o etapas distintos de los enumerados en una reivindicación. La palabra "un" o "una" antes de un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede implementarse por medio de hardware que comprende varios elementos distintos, y por medio de un ordenador programado de manera adecuada.

En la reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden realizarse mediante un mismo elemento de hardware. El mero hecho de que ciertas medidas se mencionen en reivindicaciones dependientes diferentes entre sí no indica que no pueda usarse una combinación de estas medidas de manera ventajosa.

REIVINDICACIONES

1. Sistema (100) que comprende:

- un servidor (140),

- un dispositivo (112) de presentación dispuesto para recibir contenido básico disponible en un disco (101) de DVD desde una unidad (111) de DVD y para reproducir dicho contenido básico,

estando al menos una parte del contenido básico protegida mediante el sistema de aleatorización de contenidos (*Content Scrambling System*) que emplea una clave de disco de DVD y una o más claves de título de DVD, comprendiendo el dispositivo (112) de presentación:

- medios (402, 403) de acceso condicional para desencriptar el contenido básico usando dicha clave de disco de DVD y dicha al menos una o más claves de título de DVD,

- medios (410) de recepción para recibir contenido (151) adicional relacionado con el contenido básico del servidor (140),

encriptándose el contenido (151) adicional empleándose al menos una clave de encriptación a partir de dicha clave de disco de DVD y dicha una o más claves de título de DVD usadas para proteger al menos una parte del contenido básico,

estando dispuestos los medios (402, 403) de acceso condicional para desencriptar el contenido (151) adicional usando dicha al menos una clave de encriptación, y

estando configurado el servidor (140) para obtener dicha al menos una clave de encriptación a partir de un soporte de registro adicional que es idéntico a dicho disco (101) de DVD.

2. Sistema según la reivindicación 1, en el que el dispositivo (112) de presentación comprende medios de sincronización para sincronizar el desencriptado del contenido básico con el desencriptado del contenido (151) adicional cuando dicha al menos una clave de encriptación es al menos dicha una o más claves de título de DVD.

3. Sistema según la reivindicación 1, en el que los medios (402, 403) de acceso condicional están dispuestos para ejecutar un protocolo de autenticación con el servidor usando un código de control de autenticación secreto presente en dicho disco de DVD para establecer una clave de sesión, y usando la clave de sesión para encriptar el contenido adicional tras encriptar el contenido adicional con dicha al menos una clave de encriptación.

4. Sistema según la reivindicación 1, que comprende además un dispositivo (110) de reproducción acoplado al dispositivo (112) de presentación.

5. Sistema según la reivindicación 4, que comprende además un dispositivo (120) de visualización acoplado al dispositivo (110) de reproducción y/o al dispositivo (112) de presentación.

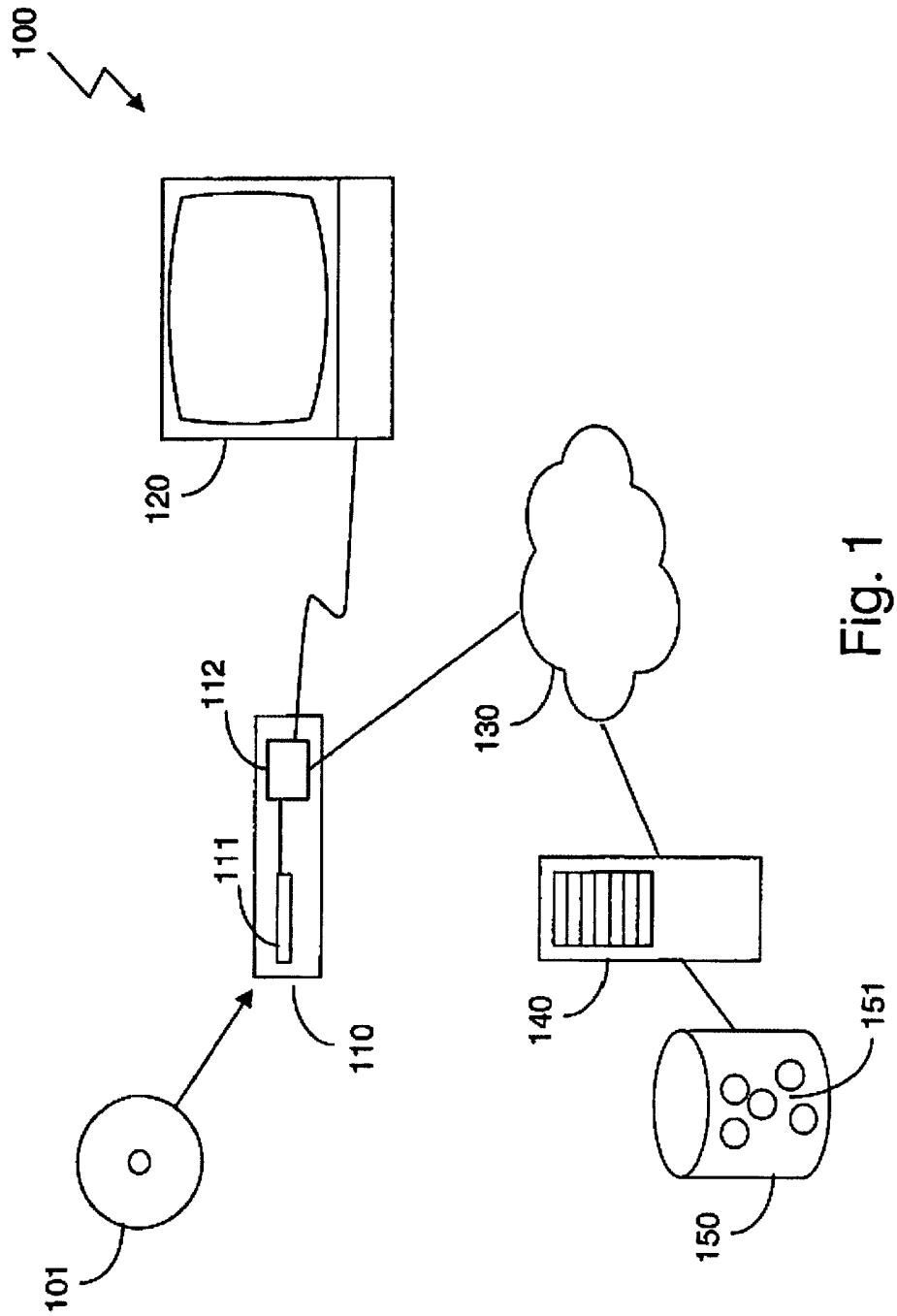

Fig. 1

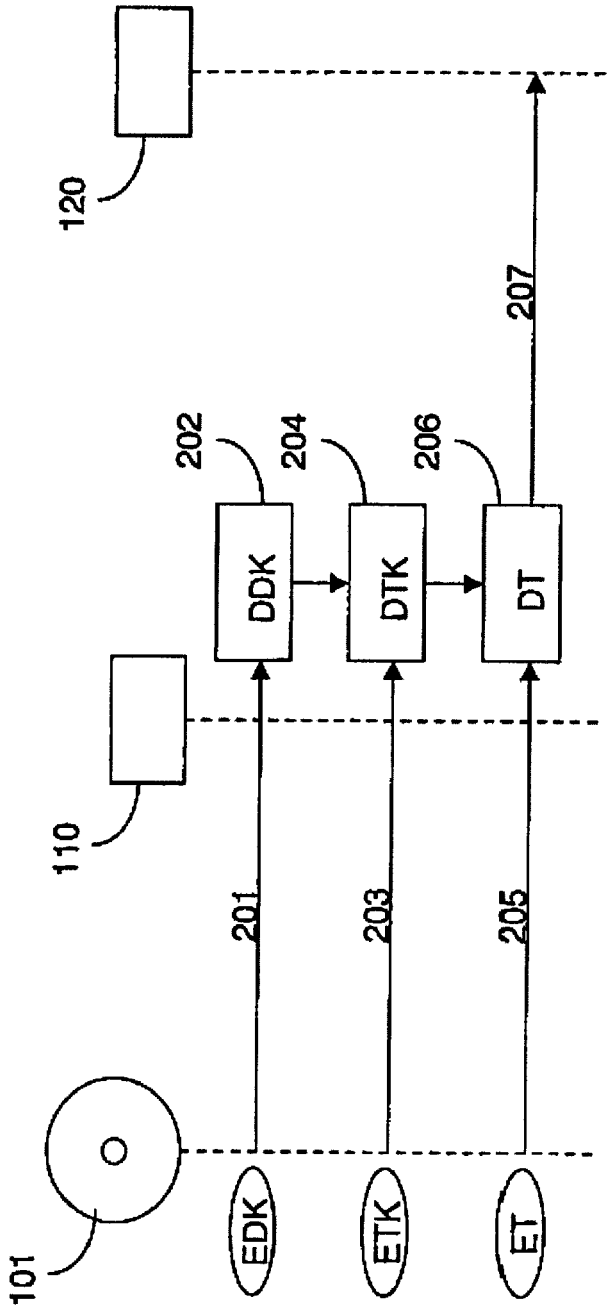

Fig. 2

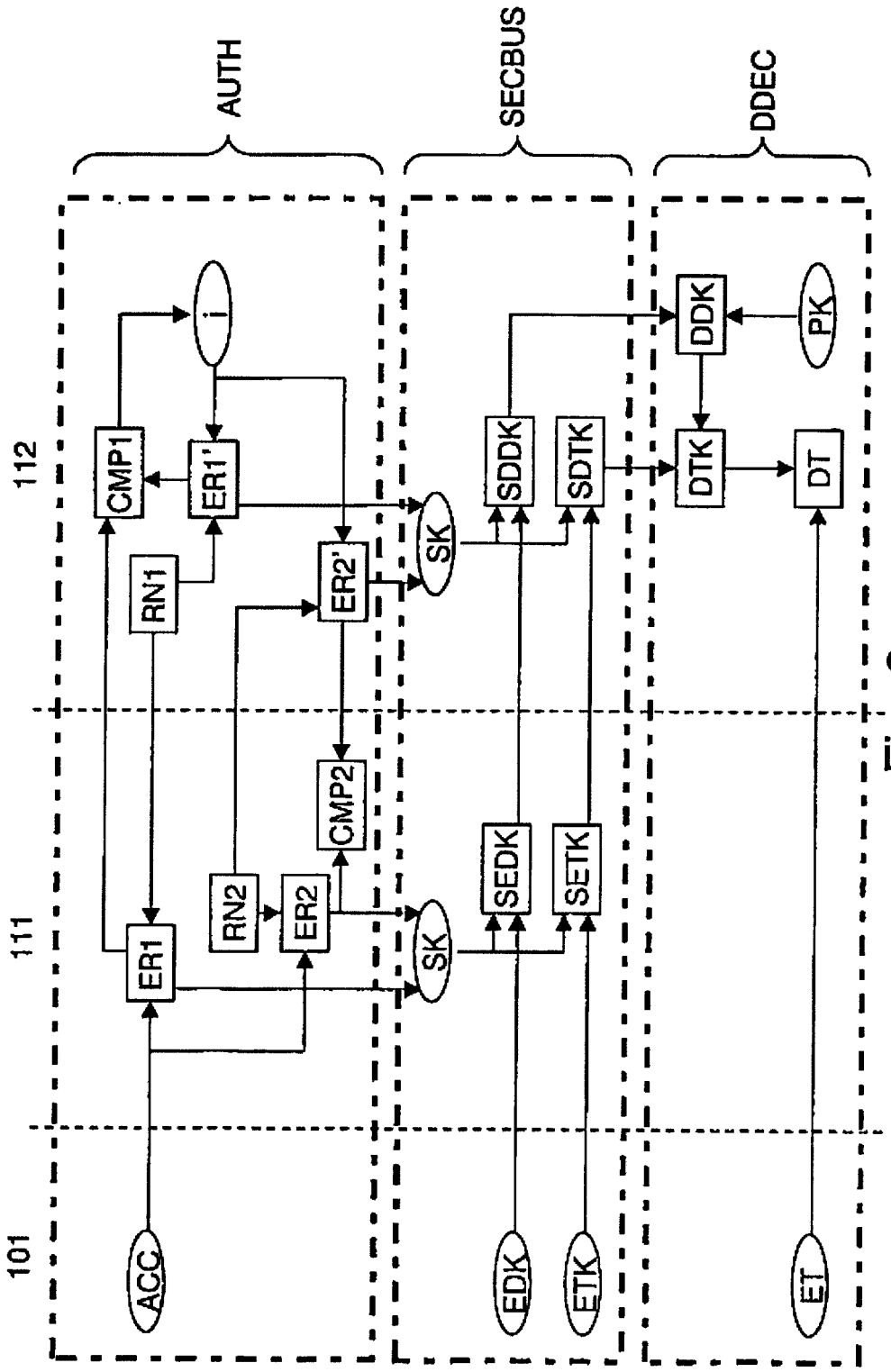
AUTH
SECBUS
DDEC
112
111
101
CMP1
ER1'
i
RN1
ER2'
SK
SDDK
SDTK
DDK
PK
DTK
DT
CMP2
RN2
ER2
ER1
SK
SEDK
SETK
ACC
EDK
ETK
ET

Fig. 3

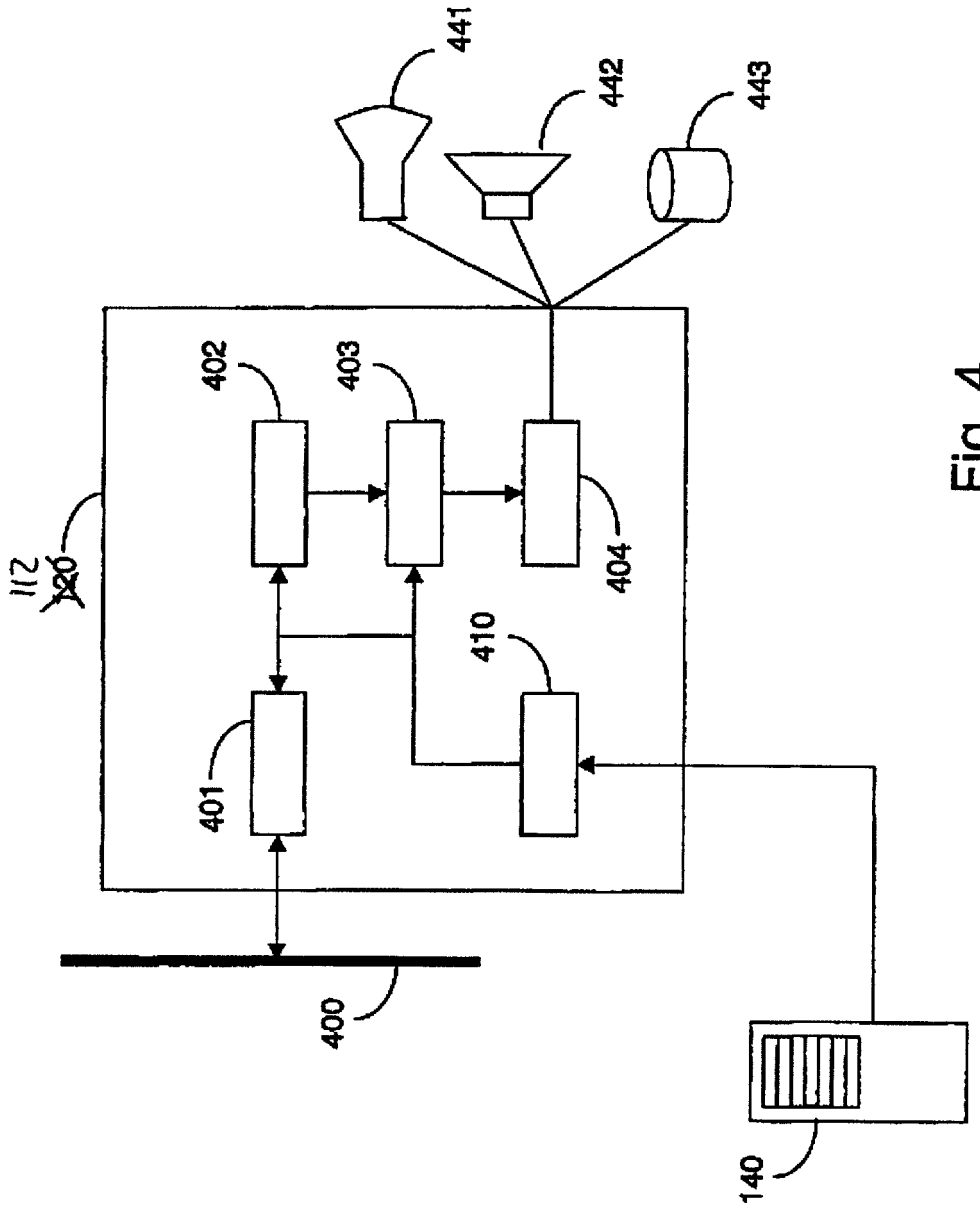

Fig. 4