

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 600 512**

51 Int. Cl.:

G06F 21/00 (2013.01)

G06F 21/10 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **22.05.2012** **E 12168931 (9)**

97 Fecha y número de publicación de la concesión europea: **27.07.2016** **EP 2544118**

54 Título: **Método para proteger contenidos de datos**

30 Prioridad:

04.07.2011 EP 11172574

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

09.02.2017

73 Titular/es:

**SIEMENS CONVERGENCE CREATORS GMBH
(100.0%)**

**Autokaderstrasse 29
1210 Wien, AT**

72 Inventor/es:

**GUDENUS, GABRIEL y
WEISS, PETER**

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 600 512 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para proteger contenidos de datos

Área técnica

- 5 La presente invención hace referencia a un método para proteger contenidos de datos, en particular datos de video. Los contenidos de datos son puestos a disposición desde una aplicación de distribución disponible en una red de comunicaciones (por ejemplo YouTube, Maxdome, Apple iTunes, etc.) y pueden ser cargados desde allí en una unidad de salida. Los contenidos de datos son reproducidos entonces en la unidad de salida (por ejemplo ordenador personal, ordenador portátil, tableta, etc.).

Estado del arte

- 10 Mediante las aplicaciones de distribución de contenidos de datos que se encuentran actualmente disponibles por lo general en una red de comunicaciones, como por ejemplo en Internet, como YouTube, Maxdome, Apple iTunes, etc., es posible cargar o transmitir esos contenidos de datos, los cuales en su mayoría son datos de video, en unidades de salida (por ejemplo ordenadores personales, ordenadores portátiles, equipos terminales móviles, tabletas, etc.). Generalmente, los contenidos de datos - ante todo los de pago obligatorio, de elevada calidad - están protegidos
15 principalmente frente un acceso no autorizado y/o de reproducción no autorizada a través de los así llamados sistemas de gestión de derechos digitales (Digital Right Management) o sistemas DRM.

- 20 Como gestión de derechos digitales (DRM) o administración de derecho digital se entienden métodos y/o sistemas mediante los cuales debe controlarse una utilización, así como eventualmente también una difusión, de contenidos de datos digitales. La gestión de derechos digitales (DRM), así como la seguridad de utilización, se emplea ante todo para contenidos de audio y/o de video, pero también puede utilizarse con respecto a software, documentos electrónicos y/o libros electrónicos. A través de la gestión de datos digitales, para los proveedores de contenidos de datos es posible realizar un control de utilización para sus contenidos de datos, desarrollar posibilidades de contabilidad principalmente nuevas (por ejemplo remuneración de licencias, autorizaciones, etc.) y, con ello, cobrar por los derechos de utilización de los contenidos de datos, en lugar de cobrar por los propios contenidos de datos.

- 25 Un sistema DRM o un sistema para la gestión de derechos digitales representa por tanto una medida de seguridad técnica para brindar al titular de un derecho o proveedor de contenidos de datos, los cuales representan los así llamados bienes de información, una posibilidad de limitar técnicamente el tipo de utilización de su propiedad (es decir, de los contenidos de datos) a través de los usuarios, a un convenio de uso previamente acordado. Para ello se utilizan mecanismos electrónicos de protección para los contenidos de datos, a través de los cuales se posibilita un
30 aprovechamiento de los contenidos de datos, más allá de una remuneración estrictamente global, donde adicionalmente se permite por ejemplo la concesión/liquidación de una licencia según la frecuencia de uso, la duración de la utilización y/o el alcance de la utilización, así como se impide un uso no autorizado (por ejemplo copia, reproducción, etc.). De este modo, por una parte, puede restringirse la utilización ilimitada y, por otra parte, se posibilitan los así llamados modelos comerciales a demanda, los cuales sin sistemas DRM apenas pueden ser
35 realizados o sólo pueden realizarse con gran dificultad.

- A través de los sistemas DRM son codificados contenidos de datos como por ejemplo contenidos de audio y/o de video, etc. antes de una transmisión digital en una unidad de salida - es decir que el flujo de datos es codificado por el sistema DRM (por ejemplo una así llamada video stream (retransmisión de video), etc.). El flujo de datos codificado es decodificado directamente en una unidad de salida, como por ejemplo un ordenador personal,
40 ordenador portátil, etc. - por ejemplo en el caso de la autorización correspondiente, después de la verificación de las autorizaciones a través del sistema DRM, etc. De este modo se impide que los contenidos de datos sean interceptados en el caso de una transmisión entre la aplicación de distribución y la unidad de salida, por ejemplo mediante una red de comunicaciones como Internet, así como una visualización en la unidad de salida. Sin embargo, para una visualización posterior, así como para observar los contenidos de datos, en particular datos de
45 video, por ejemplo en una pantalla perteneciente a la unidad de salida, los contenidos de datos deben presentarse completamente decodificados. Es decir que los contenidos de datos deben ponerse a disposición completamente decodificados, por ejemplo de una tarjeta gráfica de la unidad de salida (por ejemplo PC, ordenador portátil, etc.) o de una aplicación para visualizar los respectivos contenidos de datos.

- 50 No obstante, en particular en el caso de contenidos de datos de elevada calidad (por ejemplo contenido de video antes de estar disponibles en los así llamados DVDs, etc.), existe el peligro de que esos contenidos de datos sean grabados de forma digital o copiados mediante así llamados Screen Capture Software (software de captura de pantalla) - por ejemplo durante una reproducción en la unidad de salida -, para entonces poder reutilizar o aprovechar los contenidos de datos sin protección, así como en contra de un convenio de uso (por ejemplo en mercados de intercambio de datos, etc.).

Mediante los software de captura de imágenes más antiguos (por ejemplo Camtasia, Tunebite, WM Capture, etc.), debido a las elevadas exigencias de recursos, así como del sistema, al registrar contenidos de video aún no era posible capturar las imágenes y/o grabar contenidos de datos con elevada calidad - en particular datos de video. De este modo, por ejemplo una visualización de esos contenidos de datos en una unidad de salida, como una pantalla, se encuentra descomprimida. Eso significa que por ejemplo en el caso de los datos de video, en la así llamada alta definición o alta calidad, (es decir 1080p@60Hz, así como 1920 x 1080 puntos de imagen en la exploración entrelazada y 60 campos por segundo) se presentan 124,4 megapíxeles por segundo (Mpx/s).

En la así llamada captura de pantalla, esa enorme velocidad de transmisión de datos debe ser procesada por ejemplo por la unidad de salida, ante todo por el procesador de la unidad de salida, en la cual se reproduce y visualiza el contenido de datos. Después, para una copia correspondiente del contenido de datos, se almacena de forma intermedia en una así llamada memoria principal de la unidad de salida y finalmente se registra en un medio (por ejemplo en el disco duro de la unidad de salida, etc.). Además, de manera opcional, puede realizarse también una así llamada codificación. Debido a ello se incrementa aún más la utilización de la unidad de salida, en particular del procesador, así como de la memoria principal, y se reduce sólo la utilización del medio de almacenamiento (por ejemplo disco duro, etc.). A través de la elevada carga de la unidad de salida, por tanto, con el software de captura de pantalla más antiguo apenas si era posible o sólo era posible con dificultad grabar contenidos de datos - en particular grabar contenidos de datos en alta calidad - durante la reproducción en la unidad de salida.

Por lo tanto - principalmente para reducir la utilización de la unidad de salida (por ejemplo procesador, memoria principal) - durante la grabación de contenidos de datos con el así llamado software de captura de pantalla, existe la posibilidad de registrar o copiar los contenidos de datos con una resolución más reducida y/o con una frecuencia de trama de la imagen más reducida. Debido a ello, sin embargo, se reduce la calidad de los contenidos de datos grabados/copiados. Los contenidos de datos grabados o copiados presentan de este modo una calidad como por ejemplo la de una captura con una filmadora o una cámara en una sala de cine.

Sin embargo, las capacidades del hardware de las unidades de salida (por ejemplo PC, ordenador portátil, etc.) mejoran y aumentan permanentemente. Por lo tanto, cada vez es posible manejarse mejor con la así llamada captura de pantalla o grabado/copiado de contenidos de datos que se reproducen en una unidad de salida, en particular datos de video. A través de las capacidades del hardware mejoradas o aumentadas de las unidades de salida, de forma sencilla en cuanto a la técnica, es posible "grabar" de forma digital o copiar contenidos de datos protegidos, en particular datos de video, principalmente mediante software de captura de imágenes, así como reutilizarlos o difundirlos por ejemplo a través de mercados de intercambio, sin una protección o consideración de los derechos de uso o de la protección legal digital. Esto significa que los contenidos de datos, como por ejemplo los datos de video de alta calidad, etc. ya no están asegurados ni protegidos de forma suficiente a través de un cifrado o a través de la utilización de los sistemas DRM. Por lo tanto, debe realizarse una protección adecuada contra un grabado, fotografiado y/o copiado no autorizados - en particular en contra de la así llamada captura de imágenes.

A este respecto ya existen algunos principios, como por ejemplo una aplicación de la empresa widevine, sobre la cual puede hallarse información en la página principal <http://www.widevine.com>, perteneciente a la empresa Google. La empresa widevine ofrece una así llamada Digital Copy Protection (protección de copia digital) - en particular en combinación con un sistema DRM. Esta protección de copia digital mencionada se describe por ejemplo en el documento US 2007/ 0083937 A1. En el método descrito en dicho documento, para la protección de datos digitales o de activos digitales, se opera de forma similar a un así llamado escáner de virus. En dicho método, de manera adicional con respecto a los datos protegidos, se envían así llamados detectores, los cuales, durante una utilización de activos digitales o datos, monitorean todos los procesos en la unidad de salida del usuario en cuanto a procesos sospechosos, como software de captura de pantalla, etc. Los procesos sospechosos son reconocidos por los detectores y, por ejemplo a través de Internet, por los detectores son enviados avisos correspondientes a un sistema de monitoreo central, para tomar medidas correspondientes, previamente definidas, y eventualmente impedir un copiado ilegal. Las medidas de esa clase abarcan por ejemplo desde la observación silenciosa de los procesos sospechosos hasta la revocación inmediata de los derechos de uso en los contenidos de datos.

Sin embargo, el método descrito en el documento US 2007/0083937 A1 presenta la desventaja de que un comportamiento de la unidad de salida debe ser analizado de manera permanente y mediante Internet debe presentarse a un sistema de monitoreo, donde adicionalmente los detectores igualmente deben ser ajustados. Los nuevos patrones de comportamiento críticos de la unidad de salida son transmitidos nuevamente a la unidad de salida por ejemplo mediante Internet, en forma de detectores nuevos o ajustados. Es decir que durante una reproducción de contenidos de datos se realizan - parcialmente sin el conocimiento del usuario - un monitoreo durante el funcionamiento y un intercambio de datos de monitoreo (por ejemplo avisos de los detectores, ajuste de los detectores, etc.) entre la unidad de salida y el sistema de monitoreo central. Esto no es completamente seguro en cuanto a razones de protección de los datos, ya que por ejemplo un así software de captura de pantalla podría ser instalado en la unidad de salida también para fines no ilegales, es decir, para una copia permitida de contenidos de datos, etc.). Asimismo, en el método presentado en el documento US 2007/0083937 A1 es necesario que el sistema de distribución, desde el cual se ponen a disposición los contenidos de datos, deba disponer de un sistema de monitoreo correspondiente o de una vinculación al mismo. De manera adicional, también puede ser necesario un

ajuste de de la solución de monitoreo durante el funcionamiento, para detectar siempre las patrones de comportamiento sospechosos más actuales, así como modificados, de las unidades de salida.

Descripción de la invención

5 El objeto de la presente invención consiste en proporcionar un método a través del cual, de manera sencilla y sin una gran inversión, así como sin ajustes durante el funcionamiento, se impida un copiado ilegal de contenidos de datos, en particular de datos de video, en una unidad de salida, en particular sin utilizar información relevante en cuanto a la protección de los datos.

10 De acuerdo con la invención, dicho objeto se alcanzará a través de un método de la clase indicada en la introducción con las características descritas en la reivindicación 1. En las reivindicaciones dependientes se indican variantes ventajosas del método.

15 De acuerdo con la invención, dicho objeto se alcanzará a través de un método de la clase mencionada en la introducción, en el cual, durante una reproducción de contenidos de datos cargados en la unidad de salida, en particular datos de video, se monitorea una utilización del sistema actual de la unidad de salida. De este modo, la utilización del sistema actual de la unidad de salida se compara con una utilización del sistema estándar estimada de la unidad de salida. Si la utilización del sistema estándar estimada es excedida de forma significativa y unívoca por la utilización del sistema actual, entonces se toman medidas de protección correspondientes para los contenidos de datos.

20 El aspecto principal de la solución sugerida de acuerdo con la invención reside ante todo en el hecho de que, de manera sencilla, se impide en la unidad de salida un copiado ilegal de contenidos de datos protegidos, por ejemplo a través de un software de copiado, en particular del así llamado software de captura de pantalla. Además, a través del método de acuerdo con la invención, un copiado ilegal de esa clase, de contenidos de datos, puede ser utilizado también para futuras unidades de salida, así como para su hardware, sin una gran inversión. El método de acuerdo con la invención no requiere ninguna comunicación durante el funcionamiento a través de una red de comunicaciones con un sistema de monitoreo y/o actualizaciones regulares de un software de monitoreo, así como aplicaciones de protección correspondientes, para detectar un software de copiado correspondiente en la unidad de salida. De manera adicional, a través del método de acuerdo con la invención tampoco es necesario instalar aplicaciones de protección y/o sistemas de monitoreo correspondientes en las aplicaciones de distribución. El procedimiento de acuerdo con la invención puede adecuarse de forma sencilla y simple a la respectiva unidad de salida para proteger los datos cargados por las aplicaciones de distribución.

30 De este modo, un posible uso incorrecto de los contenidos de datos puede detectarse de manera sencilla - en particular durante la reproducción, consulta, etc. de contenidos de datos, como por ejemplo contenidos de video, etc. Si se detecta un uso indebido de esa clase, entonces pueden tomarse medidas de protección correspondientes para los contenidos de datos. Para ello tampoco se utiliza información relevante en cuanto a la protección de los datos, como por ejemplo procesos en curso, software instalado, etc. y/o no se realiza una transmisión a una aplicación externa -eventualmente sin el conocimiento del usuario de la unidad de salida. A través de un cálculo "absoluto" de las utilidades del sistema, en primer lugar, no se produce ninguna ventana entre una mejora de un así llamado software de captura de pantalla y una actualización del software de protección correspondiente, el cual se requiere para una detección del copiado en la unidad de salida. En segundo lugar, se impide de ese modo un ciclo interminable entre uso incorrecto o aplicaciones correspondientes (por ejemplo software de captura de pantalla, etc.) y un software de protección que se adapta de forma correspondiente.

45 Se considera ventajoso que para una estimación de la utilización del sistema estándar de la unidad de salida se emplee una utilización del sistema para una decodificación y descifrado de los contenidos de datos que se están reproduciendo, así como una utilización del sistema para aplicaciones básicas que se encuentran en curso de manera predefinida en la unidad de salida. De este modo, el método de acuerdo con la invención puede utilizarse de forma muy sencilla para cualquier contenido de datos cifrado o codificado (por ejemplo a través de los así llamados sistemas DRM), puesto que siempre se considera la utilización del sistema correspondiente para la respectiva decodificación y para el respectivo descifrado de los contenidos de datos. Además, se consideran también aplicaciones básicas que se encuentran en curso de manera predefinida en la unidad de salida, como por ejemplo aplicaciones del sistema operativo, aplicaciones internas, etc. De este modo se impide que las aplicaciones básicas conduzcan a una interpretación errónea de la utilización del sistema actual. De manera adicional, a través de una consideración correspondiente al estimar la utilización del sistema estándar, es posible considerar un copiado o una instalación de software de copiado fiable (por ejemplo software de captura de pantalla) para fines legales, en caso de encontrarse presentes las autorizaciones correspondientes.

55 También es conveniente que se efectúe un monitoreo de la utilización del sistema actual de la unidad de salida durante un lapso predeterminable y que se compare con la utilización del sistema estándar estimada de la unidad de salida durante ese lapso. De este modo, de manera sencilla, es posible limitar un período dentro del cual, durante la reproducción de contenidos de datos, tiene lugar un monitoreo o un control del copiado no permitido de los

contenidos de datos. Si dentro de ese período no se determina ninguna desviación significativa de la utilización del sistema con respecto a la utilización del sistema estándar estimada, entonces los contenidos de datos con gran probabilidad no son copiados, ya que en particular en el caso de los contenidos de video los contenidos de datos son copiados durante la totalidad de la reproducción. Si durante el lapso predeterminable se determina una gran diferencia entre la utilización del sistema actual y la utilización del sistema estándar estimada, prevista, entonces es probable un copiado mediante un software de copiado o un así llamado capturador de pantalla, y medidas para la protección de los contenidos de datos pueden tomarse rápidamente de forma correspondiente.

En un perfeccionamiento preferente del procedimiento de acuerdo con la invención se prevé que, en el caso de que la utilización del sistema actual exceda la utilización del sistema estándar estimada, como medida de protección se interrumpa la reproducción de los contenidos de datos. De este modo se impide de manera sencilla un copiado de datos protegidos. Como variantes de esas medidas de seguridad son posibles por ejemplo una detención o una interrupción de la reproducción de los contenidos de datos en la unidad de salida, una detención o interrupción de una transmisión de los contenidos de datos por la aplicación de distribución correspondiente (por ejemplo Maxdome, Apple iTunes, etc.) en la unidad de salida y/o en particular en el caso de datos de video, pero también de datos de audio que son emitidos en directo (es decir que la reproducción de los contenidos de datos en la unidad de salida comienza ya durante la transmisión de los contenidos de datos o casi al mismo tiempo que la misma), una detención de la emisión en directo.

En otra variante de la invención, en el caso de que la utilización del sistema actual exceda la utilización del sistema estándar, como medida de protección para los contenidos de datos, un mensaje es enviado a la respectiva aplicación de distribución desde la cual han sido transmitidos o emitidos en directo los contenidos de datos. A través de esa medida de protección para los contenidos de datos, un copiado ilegal de los contenidos de datos puede ser informado por ejemplo al proveedor de contenidos de datos. A modo de ejemplo, el mensaje puede ser enviado también sin embargo a un así llamado sistema de unidad final con el fin de un análisis o al titular de los derechos de los contenidos de datos. El envío del mensaje, a modo de ejemplo, de manera alternativa o adicional, puede efectuarse para interrumpir la reproducción de los contenidos de datos en la unidad de salida.

Además, se considera ventajoso predeterminar un valor límite o eventualmente también varios valores límite para una diferencia entre la utilización del sistema actual y la utilización del sistema estándar estimada. A través de un valor límite, por ejemplo, puede determinarse con mucha facilidad si una superación de la utilización del sistema estándar estimada a través de la utilización del sistema actual ya es significativa y llamativa o si se encuentra dentro de un margen tolerable. A través de la predeterminación de uno o de eventualmente varios valores límite para la diferencia pueden determinarse también medidas de protección respectivamente diferentes para los contenidos de datos. De este modo, un mensaje puede ser enviado a la aplicación de distribución cuando la utilización del sistema actual de la unidad de salida excede la utilización del sistema estándar estimada pero la diferencia se ubica por debajo de un valor límite predeterminado. Por ejemplo en el momento en el cual la diferencia entre la utilización del sistema actual y la utilización del sistema estándar estimada de la unidad de salida se ubica por debajo del valor límite predeterminado, puede interrumpirse por ejemplo la reproducción de los contenidos de datos en la unidad de salida.

Breve descripción del dibujo

A continuación, la invención se explica a modo de ejemplo mediante la figura añadida, la cual a modo de ejemplo y de forma esquemática muestra un desarrollo del método de acuerdo con la invención para la protección de contenidos de datos.

Ejecución de la invención

A modo de ejemplo y de forma esquemática, la figura 1 muestra un desarrollo del método de acuerdo con la invención para proteger contenidos de datos, los cuales son cargados en una unidad de salida desde una aplicación de distribución como por ejemplo YouTube, Maxdome, Apple iTunes, etc. mediante una red de comunicaciones, como por ejemplo Internet. Como unidad de salida puede utilizarse por ejemplo un ordenador personal, un ordenador portátil, una tableta, etc.

El método de acuerdo con la invención comienza con un paso de inicio 1. En un segundo paso del método 2, contenidos de datos, en particular datos de video, son cargados en la unidad de salida desde la aplicación de distribución - por ejemplo como la así llamada emisión de video en directo. En la unidad de salida, en un tercer paso del método 3, los contenidos de datos comienzan a visualizarse o reproducirse en la unidad de salida, así como en la pantalla correspondiente. En el tercer paso del método 3, de manera adicional, los contenidos de datos son decodificados y/o descifrados de forma correspondiente, para que puedan ser mostrados para un usuario en la unidad de salida.

- En un cuarto paso del método 4, durante la visualización o la reproducción de los contenidos de datos se analiza y monitorea una utilización del sistema actual de la unidad de salida (por ejemplo utilización del procesador, memoria principal, etc.). De manera paralela, en un quinto paso del método se estima una utilización del sistema estándar de la unidad de salida. De este modo, por ejemplo, se supone una utilización del sistema previsible de forma correspondiente para una visualización o una reproducción de contenidos de datos. Es decir que se emplea una utilización del sistema de la unidad de salida para aplicaciones básicas que se encuentran en curso de acuerdo con el estándar, como por ejemplo aplicaciones del sistema operativo, aplicaciones internas, etc., ya que esas aplicaciones básicas generalmente se ejecutan en la unidad de salida y desde éstas se encargan de una utilización del sistema correspondiente cuando la unidad de salida se encuentra en funcionamiento. De manera adicional, para una estimación de la utilización del sistema estándar de la unidad de salida se considera también una utilización del sistema para una decodificación y un descifrado de los contenidos de datos a ser reproducidos, para que la utilización del sistema, la cual es causada a través de la decodificación y el descifrado de los contenidos de datos, no conduzca a una falsa activación de medidas de protección.
- Después de la estimación de la utilización del sistema estándar de la unidad de salida, en un sexto paso del procedimiento 6, la utilización del sistema estándar esperada para una reproducción de contenidos de datos se compara con la utilización del sistema actual de la unidad de salida. De este modo, el monitoreo de la utilización del sistema actual, así como la estimación de la utilización del sistema estándar, se realizan para un lapso predeterminable.
- Si en el sexto paso del método 6 se determina que la utilización del sistema actual de la unidad de salida no excede o sólo excede mínimamente la utilización del sistema estándar esperada, estimada para una reproducción de contenidos de datos, en particular de datos de video o de emisión de video en directo, entonces en un séptimo paso del método 7 continúa la emisión o la reproducción de los contenidos de datos. Sin embargo, si en el sexto paso del método 6 se determina una superación, en particular una superación significativa, de la utilización del sistema estándar estimada a través de la utilización del sistema actual, entonces en un octavo paso del método se toman medidas correspondientes para proteger los contenidos de datos - ante todo en contra de un copiado ilegal a través de la utilización de un software de copiado, en particular de un así llamado captador de pantalla.
- Como medida de protección correspondiente, por ejemplo en el octavo paso del método 8, se envía un mensaje a la aplicación de distribución desde la cual los contenidos de datos son solicitados mediante la red de comunicaciones. De manera adicional o alternativa, en el octavo paso del método 8, también es posible detener la visualización o la reproducción de los contenidos de datos en la unidad de salida, así como por ejemplo finalizar una así llamada emisión de video en directo, para que el usuario, por ejemplo, no pueda generar en la unidad de salida una copia utilizable de los contenidos de datos.
- Para una mejor estimación de si eventualmente se realiza un copiado adicional de los contenidos de datos en la unidad de salida o no, en el sexto paso del método 6, no sólo es posible verificar si la utilización del sistema actual de la unidad de salida excede la utilización del sistema estándar estimada, sino determinar una diferencia entre la utilización del sistema actual y la utilización del sistema estándar estimada. Para esa diferencia puede determinarse entonces un valor límite. Si en el sexto paso del método 6 se determina que la diferencia supera el valor límite, entonces en el octavo paso del método 8 se introducen medidas de protección correspondientes para los contenidos de datos (por ejemplo un mensaje a la aplicación de distribución, detención de la reproducción, etc.).
- De este modo, de manera muy sencilla puede impedirse un copiado ilegal, en particular de contenidos de datos protegidos, en una unidad de salida, también en el caso de un hardware de alto rendimiento correspondiente, así como también para un hardware futuro. Además, tampoco se requiere una instalación o un ajuste durante el funcionamiento de las aplicaciones de protección, y desde el método de acuerdo con la invención tampoco se solicita o utiliza información relevante en cuanto a la protección de datos (por ejemplo procesos en curso, software instalado en la unidad de salida, etc.).

REIVINDICACIONES

- 5 1. Método para proteger contenidos de datos de un copiado ilegal, donde los contenidos de datos son cargados en una unidad de salida (1, 2) desde una aplicación de distribución disponible en una red de comunicaciones y son reproducidos en la unidad de salida (3), caracterizado porque durante una reproducción de contenidos de datos cargados en la unidad de salida se monitorea una utilización del sistema actual de la unidad de salida (4), porque la utilización del sistema actual se compara con una utilización del sistema estándar estimada de la unidad de salida para una reproducción de contenidos de datos (5, 6), y porque en el caso de que la utilización del sistema actual exceda la utilización del sistema estándar estimada se toman medidas de protección correspondientes, donde como medida de protección para los contenidos de datos se interrumpe la reproducción de los contenidos de datos (8).
- 10 2. Método según la reivindicación 1, caracterizado porque una utilización del sistema para decodificar y descryptar los contenidos de datos que se reproducen en la unidad de salida, así como una utilización del sistema para aplicaciones básicas que se ejecutan por defecto en la unidad de salida, son usadas (5) para estimar la utilización del sistema estándar de la unidad de salida.
- 15 3. Método según una de las reivindicaciones 1 a 2, caracterizado porque se realiza un monitoreo de la utilización del sistema actual de la unidad de salida durante un lapso predeterminable (4) y se compara con la utilización del sistema estándar estimada de la unidad de salida para ese lapso (6).
4. Método según una de las reivindicaciones 1 a 3, caracterizado porque en el caso de que la utilización del sistema actual exceda la utilización del sistema estándar un mensaje es enviado a la respectiva aplicación de distribución como medida de protección para los contenidos de datos (8).
- 20 5. Método según una de las reivindicaciones 1 a 4, caracterizado porque se predetermina un valor límite para una diferencia entre la utilización del sistema actual y la utilización del sistema estándar estimada (6).

