



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 279 611**

51 Int. Cl.:
G11B 23/28 (2006.01)
H04N 7/167 (2006.01)
G06F 12/14 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **99900699 .2**
86 Fecha de presentación : **08.01.1999**
87 Número de publicación de la solicitud: **1046169**
87 Fecha de publicación de la solicitud: **25.10.2000**

54 Título: **Sistema y procedimiento para proteger contra copia señales digitales.**

30 Prioridad: **08.01.1998 US 70764 P**

73 Titular/es: **SAMSUNG ELECTRONICS Co., Ltd.**
416 Maetan-dong, Paldal-gu
Suwon-city, Kyungki-do 442-373, KR

45 Fecha de publicación de la mención BOPI:
16.08.2007

72 Inventor/es: **Chaney, Jack**

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

74 Agente: **Curell Suñol, Marcelino**

ES 2 279 611 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

Sistema y procedimiento para proteger contra copia señales digitales.

5 **Campo técnico**

La presente invención se refiere a un procedimiento para proteger una señal digital que representa información audiovisual, así como al sistema correspondiente.

10 **Antecedentes de la invención**

La proliferación de tecnología digital en la electrónica de consumo ha generado la existencia de un gran número de productos de consumo de tecnología digital que proporciona prestaciones superiores a las de sus predecesores analógicos. No obstante, la distribución de información audiovisual en formato digital unida a la disponibilidad de dispositivos de grabación digitales hace crecer la preocupación sobre la piratería de productos audiovisuales, especialmente en la industria del espectáculo. Como respuesta a este problema la MPAA (Motion Picture Association of America) ha propuesto la protección contra copia de las películas puestas a la venta en formato de Disco de Vídeo Digital (DVD) para evitar que un comprador adquiriera una única copia y efectúe y distribuya copias múltiples.

No obstante, estos problemas no están limitados a la información digital puesta a la venta en DVD. Existe un problema similar en otros medios, por ejemplo en la televisión por cable o de radiodifusión entre otros.

Los distribuidores de televisión por cable están preocupados por la protección de sus transmisiones. Un enfoque ha sido la utilización de acceso condicionado para controlar la distribución de sus transmisiones. El acceso condicional se refiere al control de la distribución de información a ubicaciones locales. Una importante diferencia entre la utilización de un acceso condicional y la protección contra copia para controlar la distribución de material consiste en que el acceso condicional se aplica a sitios o nodos de distribución específica, mientras que la protección de las copias se extiende más allá de los nodos o sitios.

Otro enfoque para proteger la información audiovisual ha consistido en encriptar una señal audiovisual y añadir a los receptores la capacidad de descryptar la señal audiovisual. Un problema de este enfoque es que con frecuencia los receptores requieren una funcionalidad compleja para efectuarla descryptación, por ejemplo en el caso de encriptación/descryptación de clave pública/privada.

Otra propuesta para la protección contra copia de los medios ha sido efectuada por el subcomité del grupo de discusión de transmisión de datos (DTDG) para la protección de copias de tecnología Sección 1394 del Copy Protection Working Group (CPTWG). La tecnología Sección 1394 se refiere a un protocolo de bus de 100Mbit/s ó 400 Mbit/s comúnmente aplicable a los productos electrónicos de consumo.

Otra propuesta está siendo desarrollada por el National Renewable Security Standards Committee (NRSSC) # una norma provisional de seguridad de EIA (Electronics Industry Associates) que define dos interfaces para seguridad de acceso de tipo desmontable. Este procedimiento incluye lo que se ha denominado "tarjeta inteligente" y una tarjeta de PC-MCIA.

La figura 1 ilustra una disposición convencional 100 para protección contra copia de una señal audiovisual utilizando un módulo de seguridad reemplazable que está acoplado a un receptor a través de una interfaz IS679. Se suministran a un transmisor 102 una o más señales audiovisuales identificadas como AVS_1 a AVS_N , normalmente a velocidades del rango de 6 Mbits/s a 100 Mbits/s. Las señales audiovisuales AVS_1 , AVS_2 a AVS_N son codificadas por codificadores E_1 , E_2 a E_N respectivamente, utilizando, por ejemplo, técnicas de codificación MPEG, y separadas en señales de audio AS_1 a AS_N y señales de vídeo VS_1 , VS_2 a VS_N .

Las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N son encriptadas a continuación por aleatorizadores S_1 , S_2 a S_N respectivamente, utilizando, por ejemplo, cualquier número de técnicas de encriptación de claves ampliamente conocidas. Las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N encriptadas se combinan a continuación mediante un combinador 104 en señales audiovisuales únicas. El combinador 104 puede comprender diversos procesos tales como multiplexores y otros procesadores necesarios para proporcionar la señal audiovisual única.

A continuación, la señal audiovisual única se suministra a un receptor 106 a través de un enlace 108. El enlace 108 puede comprender uno o más medios y/o sistemas de comunicación y soportar aparatos que están configurados para transportar la señal audiovisual única entre el transmisor 102 y el receptor 106. Los ejemplos de enlace 108 comprenden, sin estar limitados a ellos, un sistema telefónico, un sistema de televisión por cable, un sistema de transmisión de televisión (directo o indirecto), un sistema de transmisión por satélite (directo o indirecto), una o más redes informáticas y/o buses, internet, una intranet y cualquier software, hardware y demás sistemas de comunicación y equipos asociados con los mismos para transmitir datos codificados entre dos ubicaciones.

Después de la recepción de la señal audiovisual única, el receptor 106 transmite la señal audiovisual al módulo de seguridad reemplazable 110 a través de una interfaz 112. Para aplicaciones IS679, el módulo de seguridad reemplaza-

ble 110 es una tarjeta inteligente o una tarjeta PCMCIA que se acopla comunicativamente al receptor 106 a través de una interfaz compatible IS679 112. No obstante, también pueden utilizarse otros tipos de interfaces para unir el módulo de seguridad reemplazable 110 al receptor 106. El módulo de seguridad reemplazable 110 comprende un desaleatorizador 114 que elimina la encriptación de las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N codificadas mediante aleatorizadores S_1 , S_2 a S_N . La señal audiovisual única desaleatorizada se devuelve seguidamente al receptor 106 y se descodifica con el descodificador 116 contenido en el receptor 106. A continuación, la señal audiovisual desaleatorizada y descodificada se envía a una pantalla 118 para ser reproducida o visualizada de otro modo.

Una de las ventajas de la utilización de este enfoque es que todas las operaciones de desaleatorización se realizan en un módulo de seguridad reemplazable 110. Esto permite a los fabricantes suministrar receptores estándar sin desaleatorización especializada. Para aplicaciones IS679, los módulos de seguridad reemplazables pueden presentar la forma de una tarjeta inteligente o de una tarjeta PCMCIA, que proporcionan seguridad "personalizada".

A pesar de sus ventajas, este enfoque también presenta inconvenientes y limitaciones. Un inconveniente de este enfoque es que en situaciones en las cuales la interfaz 112 es accesible, las señales audiovisuales desaleatorizadas pueden redistribuirse a otras ubicaciones u a continuación ser descodificadas y visualizadas, sorteando la protección contra copia. Por ejemplo, en el caso de un reproductor de DVD que utiliza un módulo de seguridad reemplazable como el ilustrado en la figura 1, si puede accederse a la interfaz 112, la señal audiovisual desaleatorizada (sin proteger) puede distribuirse a múltiples receptores y dispositivos de visualización e incluso grabarse y redistribuirse.

Basándose en la necesidad de disponer una protección adecuada de las señales audiovisuales en la aplicación IS679 y en las limitaciones de los enfoques anteriores, el objetivo de la presente invención consiste en disponer protección contra copia de las aplicaciones IS679 de señales audiovisuales que eviten los problemas asociados con los enfoques anteriores.

Este objetivo se alcanza mediante el procedimiento descrito en las reivindicaciones independientes 1 y 7.

Las reivindicaciones subordinadas describen formas de realización preferidas.

En general, las formas de realización de la presente invención disponen una protección contra copia de material distribuido después de aplicar el acceso condicional, independientemente del lugar de distribución del material. Las soluciones descritas en este documento presentan la ventaja de ser de implementación suficientemente sencilla para calificarlas como soluciones de las conocidas en la técnica como de "alta utilidad". Las soluciones de "alta utilidad" proporcionan un rango de seguridad de un nivel mínimo a un nivel alto de seguridad, al mismo tiempo que exigen para la implementación recursos de sistema relativamente inferiores a los de los enfoques anteriores.

El procedimiento de la forma de realización preferida de la presente invención para proteger contra copia una señal digital que representa información audiovisual, que comprende las etapas siguientes:

- (a) codificación de la señal digital para obtener una señal codificada;
- (b) conversión de la señal codificada en una señal protegida contra copia utilizando una función de protección contra copia, en que la función utiliza una señal de datos que representa datos de protección de copias; y
- (c) aleatorización de la señal protegida contra copia para obtener una señal aleatorizada.

El sistema de la forma de realización preferida de la presente invención para recuperar una señal audiovisual a partir de una señal digital que incluye una señal aleatorizada y una señal de datos de protección contra copia que representa datos de protección de copia, comprende un receptor y un módulo desaleatorizador interconectado a través de un enlace.

El módulo desaleatorizador comprende:

- (1) una primera interfaz de comunicación para comunicar con el receptor a través del enlace;
- (2) un desaleatorizador para desaleatorizar una señal aleatorizada entrante del receptor a través del enlace.

El receptor comprende:

- (1) una segunda interfaz de comunicación para comunicar con el módulo desaleatorizador, a través del enlace
- (2) un procesador para: (i) eliminar dicha señal de datos de la señal digital y almacenar los datos de protección contra copia representados por la señal de datos en un dispositivo de memoria, (ii) extraer dicha señal de datos aleatorizada de la señal digital y enviar la señal aleatorizada al desaleatorizador a través del enlace; y
- (3) un reconvertidor para convertir una señal protegida contra copia entrante procedente del desaleatorizador en dicha señal audiovisual utilizando una función inversa de protección contra copia, empleando la función inversa dichos datos de protección contra copia almacenados.

ES 2 279 611 T3

En esta forma de realización preferida de la presente invención, las señales que fluyen del módulo desaleatorizador al receptor a través del enlace están protegidas contra copia.

La característica anterior y otras características, configuraciones, ventajas y objetivos de la presente invención, que se consideran novedosos, se exponen con detalle en las reivindicaciones subordinadas. La presente invención, tanto en lo que se refiere a su configuración como al modo de operación, junto con otros objetivos y ventajas, se pondrá más claramente de manifiesto a partir de la siguiente descripción detallada considerada conjuntamente con los dibujos adjuntos. Los dibujos incluidos en este documento no deben considerarse representaciones exactas de la presente invención, sino que se incorporan meramente a título ilustrativo y deben interpretarse conjuntamente con la memoria adjunta.

La figura 1 ilustra una disposición convencional para protección contra copia de una señal audiovisual utilizando un módulo de seguridad reemplazable que está unido a un receptor a través de una interfaz IS679.

La figura 2 ilustra una disposición para señales audiovisuales protegidas utilizando un módulo de seguridad reemplazable según una forma de realización de la presente invención.

La figura 3 es un diagrama de bloques de una disposición que ilustra una segunda forma de realización preferida de la presente invención.

La figura 4 es un diagrama de bloques que ilustra un sistema informático en el cual puede implementarse una forma de realización preferida de la presente invención.

La siguiente descripción se dispone para permitir que cualquier persona experta en la materia pueda efectuar y utilizar la invención y expone las mejores formas actualmente consideradas por los inventores para llevar a cabo la invención. No obstante, diversas modificaciones se pondrán de manifiesto para los expertos en la materia, ya que en este documento se definen los principios genéricos de la presente invención.

La figura 2 ilustra una disposición 200 para señales audiovisuales protegidas contra copias utilizando un módulo de seguridad reemplazable según una forma de realización preferida de la presente invención. Una o más señales audiovisuales, identificadas como AVS_1 , AVS_2 a AVS_N , se envían a un transmisor 202, normalmente a velocidades situadas en el rango de 6 Mbits/s a 100 Mbits/s. Las señales audiovisuales AVS_1 , AVS_2 a AVS_N son codificadas por codificadores E_1 , E_2 a E_N respectivamente contenidos en el transmisor 202, utilizando, por ejemplo, técnicas de codificación MPEG, y separadas en señales de audio AS_1 , AS_2 a AS_N y señales de vídeo VS_1 , VS_2 a VS_N .

Se aplica una función a las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N mediante módulos de función F_1 , F_2 a F_N respectivamente para añadir la protección contra copia. Los datos de protección contra copia DATOS CP se envían al transmisor 202 y son utilizados por los módulos de función F_1 , F_2 a F_N para aplicar la función a las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N .

Después de ser procesadas por los módulos de función F_1 , F_2 a F_N , las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N son encriptadas por aleatorizadores S_1 , S_2 a S_N respectivamente utilizando, por ejemplo, cualquier número de técnicas de encriptación de clave ampliamente disponibles y datos de protección contra copias DATOS CP. La información de encriptación requerida por los aleatorizadores S_1 , S_2 a S_N , como por ejemplo información sobre la clave de encriptación, es suministrada por un sistema de administración del acceso condicional (no ilustrado) que normalmente está incluido en el transmisor 202, pero puede residir en cualquier lugar.

A continuación se combinan las señales de audio AS_1 , AS_2 a AS_N y las señales de vídeo VS_1 , VS_2 a VS_N encriptadas y los datos de protección contra copias DATOS CP mediante un combinador 204 para obtener una señal audiovisual única. Des este modo, los datos de protección contra copias DATOS CP se incluyen en la señal audiovisual única. El combinador 204 puede comprender diversos procesadores, tales como multiplexores y otros procesadores, necesarios para obtener la señal audiovisual única.

A continuación, la señal audiovisual única se envía a un receptor 206 a través de un enlace 208. Como en el caso de enlace 108 de la figura 1, el enlace 208 puede incluir uno o más medios o sistemas de comunicación, o ambos, y soportar equipos que están configurados para transportar la señal audiovisual única entre el transmisor 202 y el receptor 206. Los ejemplos de enlace 208 comprenden, sin limitarse a ellos, un sistema telefónico, un sistema de televisión por cable, un sistema de transmisión de televisión (directo o indirecto), un sistema de transmisión por satélite (directo o indirecto), una o más redes informáticas y/o buses, internet, una intranet y cualquier software, hardware y demás sistemas de comunicación y equipos asociados con los mismos para transmitir datos codificados entre dos ubicaciones.

Cuando el receptor 206 recibe la señal audiovisual a través del enlace 208, los datos de protección contra copias DATOS CP son eliminados de la señal audiovisual por el procesador 210. En el caso de aplicaciones en las cuales la señal audiovisual en el enlace 208 está formateada en paquetes, el procesador 210 extrae uno o más paquetes de datos que contienen los datos de protección contra copias DATOS CP de la señal audiovisual y los sustituye por paquetes de datos que contienen datos predeterminados, tales como valores CERO. Por ejemplo, los paquetes de datos que contienen datos de protección contra copias DATOS CP pueden presentar una identificación de paquete de datos determinada, de modo que pueden ser fácilmente identificados por el procesador 210.

A continuación, la señal audiovisual única se envía a un módulo de seguridad reemplazable 212 a través de una interfaz 214. Para aplicaciones IS679, el módulo de seguridad reemplazable 212 es una tarjeta inteligente o una tarjeta PCMCIA que está unida comunicativamente a un receptor 206 a través de una interfaz 214 compatible IS679. El módulo de seguridad reemplazable 212 comprende un desaleatorizador 216 que elimina la encriptación situada en las señales de audio AS_1 a AS_N y la señales de vídeo VS_1 , VS_2 a VS_N por los aleatorizadores S_1 , S_2 a S_N .

A continuación, la señal audiovisual única desaleatorizada es devuelta al receptor 206 a través de una interfaz 214. De este modo, la señal audiovisual desaleatorizada recibida por el receptor 206 desde el módulo de seguridad reemplazable 212 no contiene la encriptación dispuesta por los aleatorizadores S_1 , S_2 a S_N , pero sigue incluyendo la protección contra copias aplicada por los módulos de función F_1 , F_2 a F_N .

Seguidamente, la señal audiovisual desaleatorizada se envía al bloque funcional F^{-1} que aplica una función inversa a F^{-1} para eliminar la protección contra copias aplicada por los módulos de función F_1 , F_2 a F_N utilizando los datos de protección contra copias DATOS CP extraídos de la señal audiovisual por el procesador 210. Según la forma de realización preferida de la presente invención, el bloque funcional F^{-1} basa la aplicación de la función inversa F^{-1} a la señal audiovisual desaleatorizada en la presencia de paquetes de datos que contienen el valor predeterminado. Por ejemplo, cuando el bloque funcional F^{-1} identifica un paquete de datos que contiene el valor predeterminado, los nuevos datos de protección contra copias DATOS CP retenidos por el receptor 206 son utilizados por el bloque funcional F^{-1} para aplicar la función inversa F^{-1} a los paquetes de datos posteriores hasta la identificación del siguiente paquete de datos que contienen el valor predeterminado.

La señal audiovisual desaleatorizada es decodificada, a continuación, por un decodificador 218 contenido en el receptor 106. La señal audiovisual desaleatorizada y decodificada se envía seguidamente a una unidad de pantalla 220 para ser reproducida o visualizada de otro modo.

Este enfoque de la forma de realización preferida de la presente invención proporciona algunas ventajas importantes sobre los enfoques de la técnica anterior para disponer una protección contra copias de la señal de audio. En primer lugar, este enfoque proporciona un nivel de seguridad superior al enfoque de la técnica anterior descrito con referencia a la figura 1, porque la señal desaleatorizada suministrada por el módulo de seguridad reemplazable 212 contiene la protección contra copia proporcionada por los módulos de función F_1 , F_2 a F_N , pero no contienen los datos de protección contra copias DATOS CP, que han sido eliminados por el procesador 210. Una vez eliminados de la señal audiovisual, los datos de protección contra copias DATOS CP se mantienen internamente en el receptor 206. De este modo, la señal desaleatorizada provista por el módulo de seguridad reemplazable 212 no puede ser utilizada por otros receptores y/o dispositivos de grabación, ni siquiera los que contienen un bloque funcional equivalente al bloque funcional F^{-1} , porque no dispondrán de acceso a los datos de protección contra copias DATOS CP, que pueden ser cambiados periódicamente.

Además, este enfoque de protección contra copias es muy flexible y permite a los fabricantes de receptores continuar con un diseño estándar son componentes especiales o algoritmos, ya que el procesador 210 y el bloque funcional F^{-1} pueden implementarse como componentes estándar. La funcionalidad de protección contra copias, incluyendo el nivel de protección contra copias, se define por los datos de protección contra copias DATOS CP enviados al transmisor 202.

Los módulos de función F_1 , F_2 a F_N pueden efectuar una función relativamente sencilla, como por ejemplo una operación lógica OR exclusiva (XOR). La ventaja de utilizar una función sencilla radica en que se requieren recursos de sistema relativamente bajos para implementar las funciones F y F^{-1} en comparación con los enfoques convencionales que utilizan sofisticados algoritmos de encriptación. No obstante, pueden utilizarse funciones más exóticas dependiendo del nivel de protección contra copias deseado para una aplicación específica. En el contexto de la codificación MPEG2, puede utilizarse un paquete único de 184 bytes de datos para realizar una función XOR de 64 a 1000 bits. Además, los datos de protección contra copias DATOS CP pueden cambiarse con tanta frecuencia como sea necesario para los requisitos de una aplicación específica.

Según una segunda forma de realización preferida de la presente invención, los datos de protección contra copias DATOS CP no están incluidos en la señal audiovisual, pero en lugar de ello son generados internamente por el receptor y enviados al módulo de seguridad reemplazable. La figura 3 es un diagrama de bloques de una disposición 300 que ilustra este enfoque. Un receptor 302 recibe una señal audiovisual (AVS) que es enviada a un módulo de seguridad reemplazable 304 a través de una interfaz IS679 306.

El módulo de seguridad reemplazable comprende un desaleatorizador 308 para desaleatorizar la señal AVS. A continuación se envía la AVS a un módulo funcional F que protege contra copia la AVS aplicándole una función utilizando los datos de protección contra copia para generar una AVS procesada. Los DATOS CP son generados aleatoriamente por el receptor 302 y enviados al módulo de seguridad reemplazable 302.

La AVS procesada se vuelve a enviar al receptor 302 a través de la interfaz 306, donde un módulo funcional F^{-1} le aplica una función utilizando los datos de protección contra copias DATOS CP para eliminar la protección contra copia previamente aplicada por el módulo funcional F . A continuación, los datos de la AVS son decodificados por un decodificador D y enviados a la unidad de pantalla 310 para ser reproducidos o visualizados de otro modo. Este enfoque evita tener que incluir los datos de protección contra copias DATOS CP en la AVS. Al poder ser generados

los datos de protección contra copias DATOS CP aleatoriamente, sigue evitándose la utilización de componentes o algoritmos especializados en el receptor 302.

Aunque en este documento se han descrito formas de realización de la invención en el contexto de disponer protección contra copia para la aplicación de la interfaz IS679, los enfoques descritos en este documento son aplicables a otras configuraciones audiovisuales. Por otra parte, los enfoques aquí descritos son aplicables a otros tipos de señales e información además de las señales audiovisuales.

Los diversos componentes descritos anteriormente pueden implementarse como componentes de hardware discretos, uno o más procesos de software, o una combinación de componentes de hardware discretos u uno o más procesos de software. A este respecto, la figura 4 es un diagrama de bloques que ilustra un sistema informático 400 en el cual puede implementarse una forma de realización de la invención.

El sistema informático 400 comprende un bus 402 u otro mecanismo de comunicación para información de comunicación, y un procesador 404 conectado con el bus 402 para procesar información. El sistema informático 400 también comprende una memoria principal 406, como por ejemplo una memoria de acceso aleatorio (RAM) u otro dispositivo de almacenamiento dinámico, conectado al bus 402, para almacenar información e instrucciones que deben ser ejecutadas por el procesador 404. La memoria principal 406 también puede utilizarse para almacenar variables temporales u otra información intermedia durante la ejecución de las instrucciones que deben ser ejecutadas por el procesador 404.

El sistema informático 400 comprende además una memoria de solo lectura (ROM) 408 u otro dispositivo de almacenaje estático conectado al bus 402 para almacenar información estática e instrucciones para el procesador 404. Se dispone un dispositivo de almacenaje 410, como por ejemplo un disco magnético o un disco óptico, y se une al bus 402 para almacenar información e instrucciones.

El sistema informático 400 puede estar conectado a través del bus 402 a una unidad de pantalla 412, como por ejemplo un tubo de rayos catódicos (CRT), para visualizar información para el usuario del ordenador. Un dispositivo de entrada 414, que comprende teclas alfanuméricas y otras teclas, está conectado al bus 402 para comunicar información y efectuar selecciones de órdenes para el procesador 404. Otro tipo de dispositivo de entradas de usuario es el control de cursor 416, como por ejemplo un ratón, un ratón de bola o teclas de dirección del cursor para comunicar información de dirección y selecciones de órdenes al procesador 404 y para controlar los movimientos del cursor en la pantalla 412. Este dispositivo de entrada normalmente presenta dos grados de libertad en dos ejes, un primer eje (por ejemplo x) y un segundo eje (por ejemplo y), lo cual permite al dispositivo especificar posiciones en un plano.

Las formas de realización de la presente invención están relacionadas con la utilización de sistemas informáticos 400 para proporcionar protección contra copia de señales audiovisuales en aplicaciones IS679. Según una forma de realización preferida de la invención, un sistema informático 400 suministra la protección contra copia de señales audiovisuales en aplicaciones IS679, como respuesta a la ejecución por el procesador 404 de una o más secuencias de una o más instrucciones contenidas en la memoria 406. Tales instrucciones pueden ser leídas en la memoria principal 406 desde otro medio legible por ordenador, como el dispositivo de almacenaje 410. La ejecución de las secuencias de instrucciones contenidas en la memoria 406 hacen que el procesador 404 realice las etapas del proceso descritas en el presente documento. También pueden utilizarse uno o más procesadores en una disposición de multiprocesamiento para ejecutar las secuencias de instrucciones contenidas en la memoria principal 406. En formas de realización alternativas, puede utilizarse una circuitería de cableado permanente en lugar de instrucciones de software, o en combinación con las mismas, para implementar las formas de realización de la presente invención. Las formas de realización de la presente invención no se limitan a ninguna combinación específica de circuitería cableada y software.

El término “medio legible por ordenador” tal como se emplea en este documento se refiere a cualquier medio que participe en el envío de instrucciones al procesador 404 para ejecución de las mismas. Tales medios pueden adoptar diversas formas, incluyendo, sin limitarse a ellos, medios no volátiles, medios volátiles y medios de transmisión. Los medios no volátiles comprenden, por ejemplo, discos magnéticos u ópticos, tales como el dispositivo de almacenaje 410. Los medios volátiles comprenden memoria dinámica, como por ejemplo la memoria principal 406. Los medios de transmisión comprenden cables coaxiales, cable de cobre y fibra óptica, incluyendo los cables que comprende el bus 402. Los medios de transmisión también pueden presentar la forma de ondas acústicas o de luz, como por ejemplo las generadas durante la comunicación de datos por ondas de radio e infrarrojos.

Los medios legibles por ordenador corrientes comprenden, por ejemplo, disquetes, discos flexibles, discos duros, cintas magnéticas o cualquier otro medio magnético, CD-ROM, cualquier otro medio óptico, tarjetas perforadas, cintas de papel, cualquier otro medio físico con estampados o perforaciones, RAM, PROM y EPROM, FLASH-EPROM, cualquier otro chip o cartucho de memoria, ondas portadoras como las que se describen más adelante, o cualquier otro medio que el ordenador pueda leer.

En la transmisión de una o más secuencias de una o más instrucciones al procesador 404 para su ejecución pueden estar implicadas varias formas de medios legibles por ordenador. Por ejemplo, las instrucciones pueden transportarse inicialmente en un disco magnético de un ordenador remoto. El ordenador remoto puede cargar las instrucciones en la memoria dinámica y enviarlas a través de una línea telefónica utilizando un módem. Un módem de la zona del sistema informático 400 puede recibir los datos en la línea telefónica y utilizar un transmisor de infrarrojos para convertir los

datos en una señal de infrarrojos. Un detector de señales de infrarrojos conectado al bus 402 puede recibir los datos transportados en la señal de infrarrojos y enviar los datos al bus 402. El bus 402 transporta la memoria principal de datos 406, de la cual el procesador 404 recupera y ejecuta las instrucciones. Las instrucciones recibidas por la memoria principal 406 pueden almacenarse opcionalmente en el dispositivo de almacenaje 410, antes o después de su ejecución por el procesador 404.

El sistema informático 400 también comprende una interfaz de comunicación 418 conectada al bus 402. La interfaz de comunicación 418 dispone una conexión de comunicación de datos de dos vías con un enlace de red 420 que está conectado a la red local 422. Por ejemplo, la interfaz de comunicaciones 418 puede ser una tarjeta red digital de servicios integrada (ISDN) o un módem para proporcionar una conexión de comunicación de datos a un tipo correspondiente de línea telefónica. Como otro ejemplo, la interfaz de comunicación 418 puede ser una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible. También puede implementarse un enlace inalámbrico. En cualquiera de tales implementaciones, la interfaz de comunicaciones 418 envía y recibe señales eléctricas, electromagnéticas u ópticas que transportan trenes de datos que representan diversos tipos de información.

El enlace de red 420 normalmente proporciona comunicación de datos a través de una o más redes a otros dispositivos de datos. Por ejemplo, el enlace de red 420 puede disponer una conexión a través de la red local a 422 a un ordenador principal 424 o a equipos de datos operados por un Proveedor de Servicio Internet (ISP) 426. A su vez, el ISP suministra servicios de comunicación de datos a través de la red mundial de comunicaciones de datos en paquetes, conocida comúnmente como "Internet" 428. Tanto la red local 422 como internet 428 utilizan señales eléctricas, electromagnéticas u ópticas que transportan trenes de datos digitales. Las señales a través de las diversas redes y las señales en el enlace de red 420 y a través de la interfaz de comunicación 418, que transportan los datos digitales hacia y desde el sistema informático 400, son ejemplos de formas de ondas portadoras que transportan la información.

El sistema informático 400 puede enviar mensajes y recibir datos, incluyendo códigos de programas, a través de la(s) red(es), el enlace de red 420 y la interfaz de comunicación 418. En el ejemplo de internet, un servidor 430 podría transmitir un código solicitado para un programa de aplicación a través de internet 428, el ISP 426, la red local 422 y la interfaz de comunicaciones 418. Según la invención, una aplicación descargada de esta clase dispone el suministro de protección contra copia de las señales audiovisuales en aplicaciones IS679, como se ha descrito en el presente documento.

El código recibido puede ejecutarse mediante el procesador 404 al ser recibido y/o almacenado en el dispositivo de almacenaje 410 u otro almacenaje no volátil para posterior ejecución. A este respecto, el sistema informático 400 puede obtener el código de aplicación en forma de una onda portadora.

En la memoria anterior, se ha descrito la invención con referencia a formas de realización específicas de la misma. No obstante, resultará evidente que pueden realizarse diversas modificaciones y cambios sin apartarse del espíritu y el ámbito de la invención. Correspondientemente, la memoria y los dibujos deben considerarse a título ilustrativo más que en sentido limitativo.

La protección contra copia para señales digitales según la presente invención puede aplicarse al campo de la grabación de información audiovisual en conexión con la información audiovisual publicada en DVD, y otros medios tales como televisión por cable, televisión radiodifundida e internet para evitar de forma efectiva que un comprador adquiera una sola copia y efectúe y distribuya copias múltiples.

REIVINDICACIONES

- 5 1. Procedimiento de protección contra copia de una señal digital que representa información audiovisual, que comprende las etapas siguientes:
 - (a) codificación de la señal digital para obtener una señal codificada;
 - 10 (b) conversión de la señal codificada en una señal protegida contra copia utilizando una función de protección contra copia, en que la función utiliza una señal de datos que representa datos de protección de copias; y
 - (c) aleatorización de la señal protegida contra copia para obtener una señal aleatorizada.
- 15 2. Procedimiento según la reivindicación 1, que comprende además la etapa de transmisión de la señal aleatorizada y la señal de datos a un receptor.
3. Procedimiento según la reivindicación 1, que comprende además la etapa de transmisión de la señal aleatorizada y dicha señal de datos como señal única.
- 20 4. Procedimiento según la reivindicación 3, en el que la etapa de transmisión comprende además la combinación de la señal aleatorizada con dicha señal de datos para formar dicha señal única.
5. Procedimiento según la reivindicación 3, que comprende además las etapas siguientes:
 - 25 (a) recepción de dicha señal única en un receptor,
 - (b) eliminación de dicha señal de datos de protección contra copia de la señal única y almacenamiento en un dispositivo de memoria de los datos de protección contra copia representados por la señal de datos de protección contra copia;
 - 30 (c) recuperación de dicha señal aleatorizada de la señal única;
 - (d) desaleatorización de la señal aleatorizada recuperada para volver a obtener dicha señal de protección contra copia;
 - 35 (e) reconversión de la señal protegida contra copia reobtenida en dicha señal codificada utilizando una función inversa de protección contra copia, en la que la función inversa utiliza dichos datos de protección contra copia almacenados; y
 - 40 (f) decodificación de la señal codificada para recuperar dicha señal digital.
6. Procedimiento según la reivindicación 1, que comprende además las etapas siguientes:
 - 45 (a) desaleatorización de la señal aleatorizada para recuperar dicha señal protegida contra copia;
 - (b) reconversión de la señal protegida contra copia recuperada en dicha señal codificada utilizando una función inversa de protección contra copia, utilizando dicha función inversa los datos de protección contra copia de dicha señal de datos; y
 - 50 (c) decodificación de la señal codificada convertida para recuperar dicha señal digital.
7. Sistema para representar una señal digital protegida contra copia que representa información audiovisual, que comprende:
 - 55 (a) un codificador para codificar la señal digital para obtener una señal codificada;
 - (b) un convertidos para convertir la señal codificada en una señal protegida contra copia utilizando una función de protección contra copia, en que la función utiliza una señal de datos que representa datos de protección de copias; y
 - 60 (c) aleatorizador para aleatorizar la señal protegida contra copia para obtener una señal aleatorizada.
8. Sistema según la reivindicación 7, que comprende además un transmisor para transmitir la señal aleatorizada y la señal de datos a un receptor.
- 65 9. Sistema según la reivindicación 7, que comprende además un combinador para combinar la señal aleatorizada con dicha señal de datos para formar dicha señal única, y un transmisor para transmitir dicha señal única.

ES 2 279 611 T3

10. Sistema según la reivindicación 7, que comprende además un transmisor para transmitir la señal aleatorizada y dicha señal de datos como señal única.

11. Sistema según la reivindicación 7, que comprende además:

- (a) un desaleatorizador para desaleatorizar la señal aleatorizada para recuperar dicha señal protegida contra copia;
- (b) un reconvertidor para reconvertir la señal protegida contra copia recuperada en dicha señal codificada utilizando una función inversa de protección contra copia, utilizando dicha función inversa los datos de protección contra copia de dicha señal de datos; y
- (c) un decodificador para decodificar la señal codificada convertida para recuperar dicha señal digital.

FIG. 1

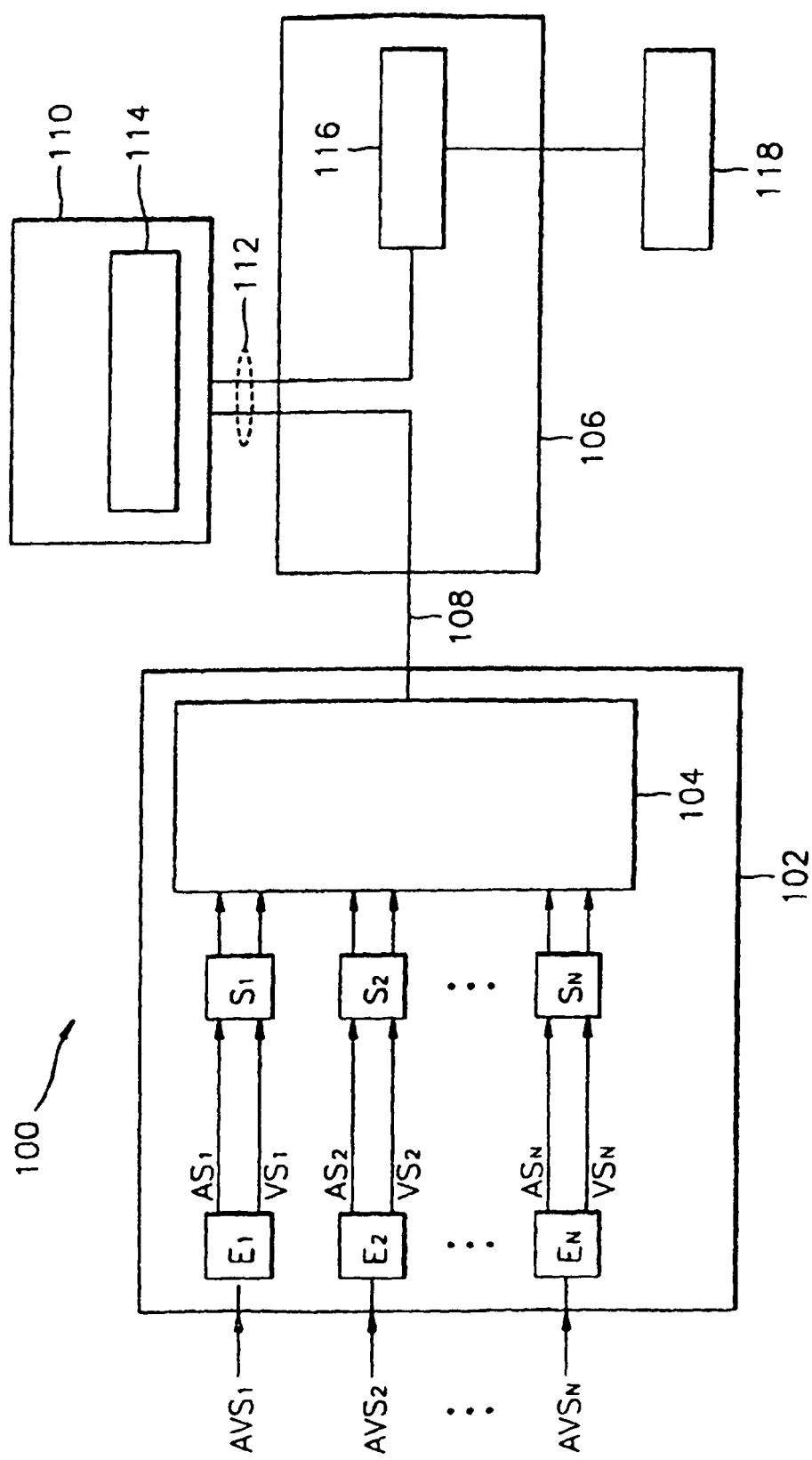


FIG. 2

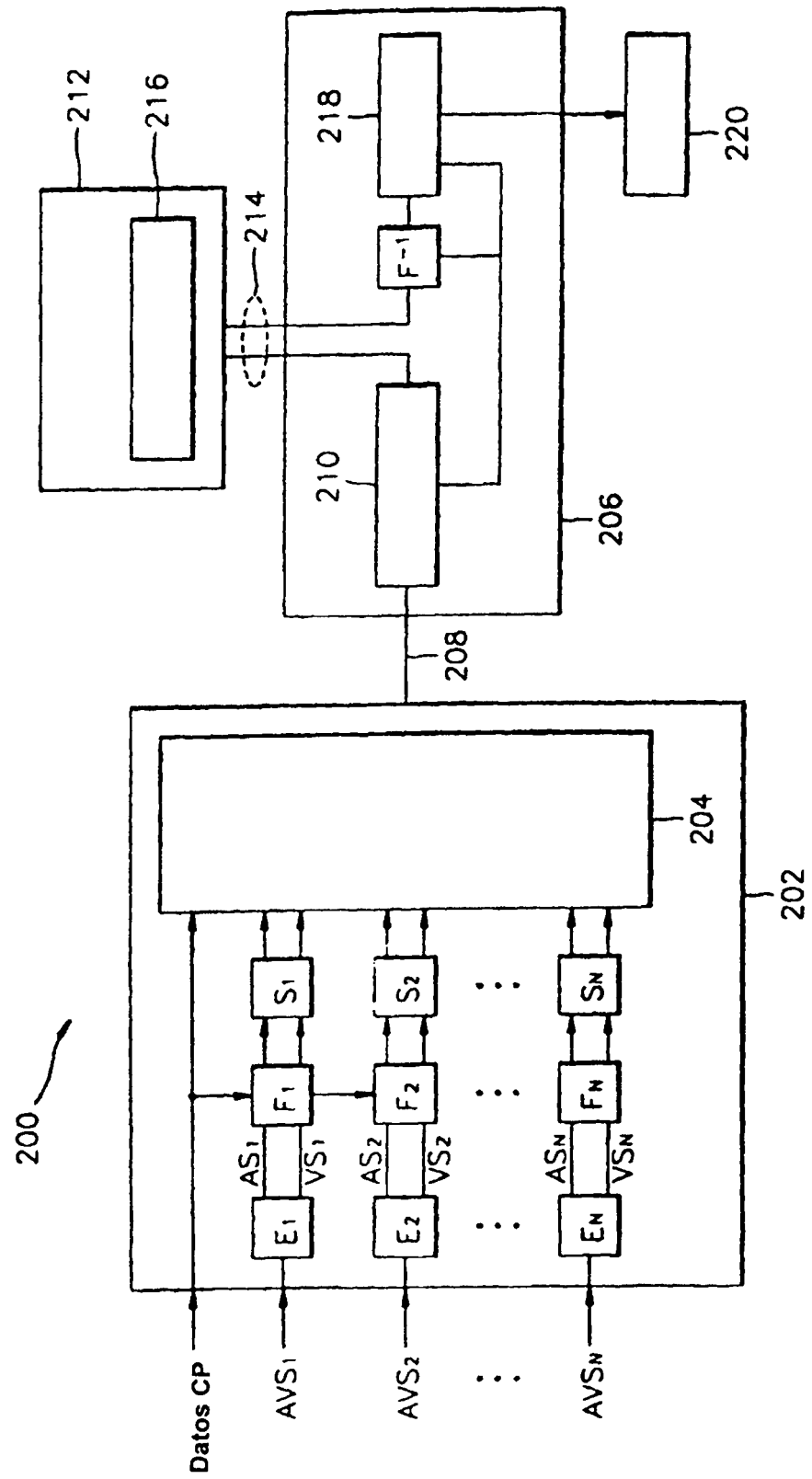


FIG. 3

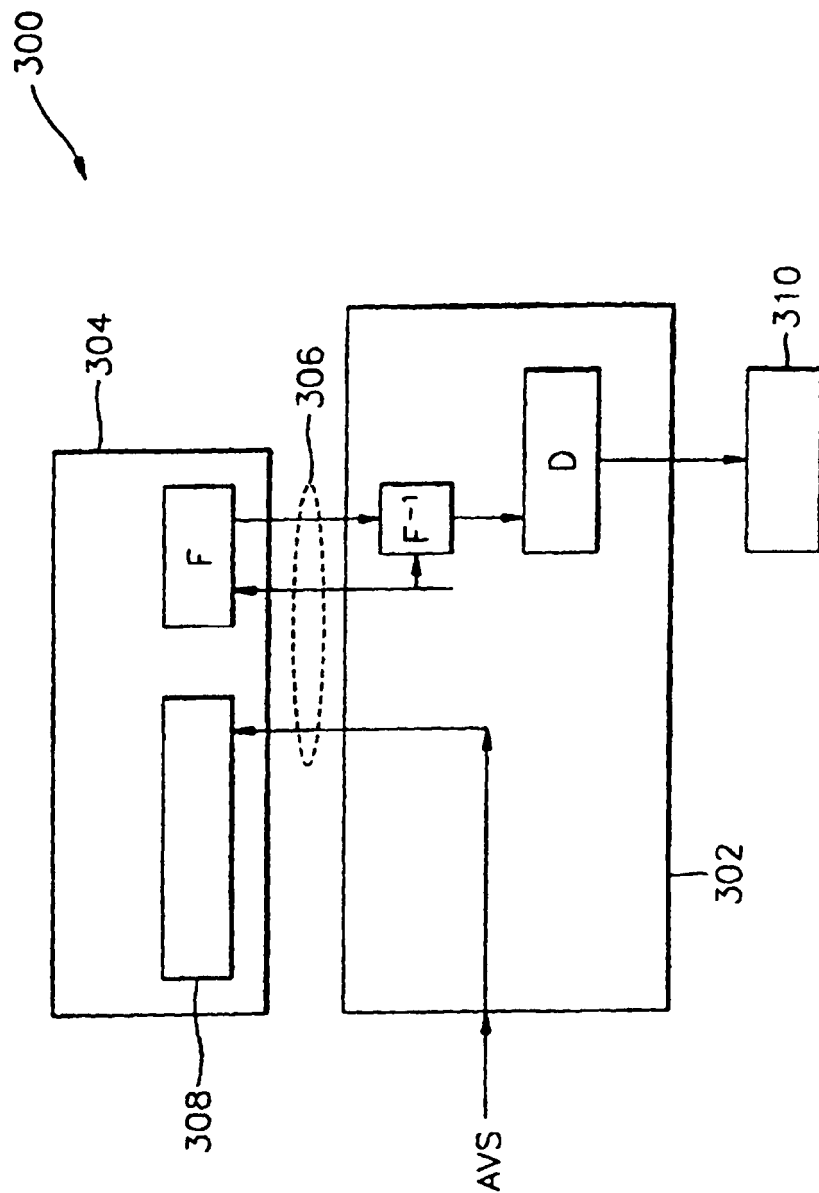


FIG. 4

