

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 384 965**

51 Int. Cl.:
H04N 7/167 (2011.01)
H04N 7/24 (2011.01)
H04N 5/913 (2006.01)
H04N 7/16 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **03715010 .9**
96 Fecha de presentación: **15.01.2003**
97 Número de publicación de la solicitud: **1470714**
97 Fecha de publicación de la solicitud: **27.10.2004**

54 Título: **Dispositivo seguro para el tratamiento de obras audiovisuales de alta calidad**

30 Prioridad:
30.01.2002 FR 0201100

45 Fecha de publicación de la mención BOPI:
16.07.2012

45 Fecha de la publicación del folleto de la patente:
16.07.2012

73 Titular/es:
NAGRA FRANCE SAS
28, RUE DU COLONEL PIERRE AVIA
75015 PARIS, FR

72 Inventor/es:
LECOMTE, Daniel

74 Agente/Representante:
Tomas Gil, Tesifonte Enrique

ES 2 384 965 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

Dispositivo seguro para el tratamiento de obras audiovisuales de alta calidad

- 5 [0001] La presente invención se refiere al tratamiento, la difusión, el registro y la visualización protegida de datos de video y de programas de televisión, o más habitualmente cualquier programa o secuencia multimedia que utiliza un formato de flujo nominal de tipo MPEG, por usuarios autorizados y propone un sistema protegido para el tratamiento, la difusión, la entrega, el registro, la copia privada y la visualización de programas y de secuencias de video o multimedia interactivos.
- 10 [0002] El problema general es proporcionar un dispositivo capaz de transmitir de manera protegida un conjunto de películas de alta calidad visual a un formato de tipo MPEG (MPEG-1, MPEG-2) en directo hacia una pantalla de televisión y/o para ser registrado sobre el disco duro de una caja que conecta la red de teletransmisión a la pantalla de televisión, mientras que preserva la calidad audiovisual pero evitando toda utilización fraudulenta como la posibilidad de hacer copias piratas de películas o de programas audiovisuales registrados sobre el disco duro de la caja descodificadora.
- 15 [0003] La invención permite igualmente un control total de la utilización de las copias y de los derechos de las obras difundidas.
- 20 [0004] Con las soluciones actuales, es posible transmitir películas y programas audiovisuales en forma digital a través de las redes de difusión de tipo hertziano, cable, satélite, etc. o a través de las redes de telecomunicación tipo DSL (Digital Subscriber Line) o BLR (bucle local de radio) o a través de las redes DAB (Digital Audio Broadcasting). Además, para evitar el pirateo de las obras de este modo difundidas, estas últimas son a menudo encriptadas por diversos medios bien conocidos por el experto en la materia.
- 25 [0005] Sin embargo, el inconveniente principal de todas las soluciones actuales (TiVo Inc., WO00165762) es que necesita transmitir no sólo los datos encriptados hacia los usuarios, sino también las claves de desencriptado. La transmisión de las claves de desencriptado puede hacerse antes, a la vez o después de la transmisión de los programas audiovisuales. Para aumentar la seguridad y por lo tanto la protección de las obras audiovisuales contra una utilización mal intencionada, las claves de desencriptado así como las funciones de desencriptación de los descodificadores audiovisuales pueden contener medios de seguridad mejorados como tarjetas inteligentes u otras llaves físicas que pueden opcionalmente, ser actualizadas a distancia.
- 30 [0006] De este modo, las soluciones actuales aplicadas a una caja descodificadora con posibilidad de registro local de programas audiovisuales en forma digital en un soporte cualquiera de tipo disco duro u otro tipo de memoria, ofrecen a un usuario mal intencionado, la posibilidad de hacer copias no autorizadas de los programas registrados de este modo, ya que a un momento dado, este usuario posee con su caja descodificador digital, asociada o no a los sistemas de tarjetas inteligentes, todas las informaciones, programas y datos que permiten la desencriptación completa de los programas audiovisuales. Debido justamente al hecho de que posee todos los datos, el usuario mal intencionado tendrá la posibilidad de hacer copias ilegales sin que nadie se de cuenta de esta copia fraudulenta en el momento en que ésta se haga.
- 35 [0007] Una solución consistiría por lo tanto en transmitir todo o parte de un programa audiovisual digital únicamente bajo solicitud (servicios de video a la carta) a través una red de telecomunicación de banda ancha de tipo ADSL, cable o satélite, sin autorizar el registro local de los programas audiovisuales. Aquí, el inconveniente es cualquier otro y proviene de los rendimientos de estas redes que no permiten garantizar el flujo continuado de algunos megabits por segundo en cada usuario, como lo exige el flujo MPEG que necesita bandas de paso de algunas centenas de kilobits a varios megabits por segundo.
- 40 [0008] En estas condiciones, una solución consiste en separar el flujo en dos partes de las cuales ninguna sería utilizable sola. Con este objetivo se han depositado varias patentes. De este modo, se conoce por el documento WO09908428 (Gilles Maton) un procedimiento de tratamiento multiaplicativo de un terminal activo localizable en el cual se realiza al menos un enlace con un programa identificable dedicado a la ejecución de una aplicación, dicho programa dictando sus condiciones de explotación al terminal para la puesta a disposición de las funciones. El terminal dialoga puntualmente, por el empleo de un enlace, con el centro de gestión para la realización, si fuera necesario, de las entradas y salidas de las capacidades de este último, el centro de gestión volviéndose esclavo o no del terminal a nivel del aplicativo con respecto del programa entrante. Esta invención se refiere igualmente al procedimiento de identificación del programa y del terminal en explotación. Este procedimiento del estado de la técnica anterior divide el flujo en una parte que sirve para identificar el usuario y una parte que contiene el programa propiamente dicho. En particular, dicho programa no es inutilizable sino solamente cerrado por la primera parte.
- 45 [0009] Por otra parte, el documento EP0778513 (Matsushita) describe un procedimiento que permite prevenir la utilización ilegal de una información añadiéndole una información de control a fin de verificar los derechos del usuario. El sistema
- 50
- 55
- 60

permite saber sin interrupción qué parte de la información se utiliza y por qué usuario y así saber si este usuario está en posición ilegal o no. Este procedimiento asegura por lo tanto los datos añadiéndole las informaciones adicionales que desnaturalizan la información inicial.

5 [0010] El documento WO0049483 (Netquartz) nos ofrece igualmente procedimientos y sistemas para crear una conexión entre los usuarios y un editor de entidades numerizadas. El procedimiento incluye una al menos de las etapas siguientes: la etapa de subdividir dicha entidad digitalizada en dos partes; la etapa de memorizar una parte en una zona memoria de un servidor conectado a una red informática; la etapa de transmitir la otra parte con al menos un usuario que dispone de un equipo informático; la etapa de conectar dicho equipo informático a dicha red informática; la etapa de establecer una
10 conexión funcional entre dicha primera parte y dicha segunda parte. Estos procedimientos y sistemas no especifican si la parte memorizada sobre el servidor se puede almacenar por el usuario lo que le permitiría piratear dicha entidad digitalizada.

[0011] Finalmente, en este enfoque, el estado de la técnica más cercano se encuentra en las patentes de HyperLOCK Technologies de las cuales la más pertinente es el documento US05937164. Esta invención utiliza la solución que consiste en separar el flujo en dos partes de las cuales la más pequeña posee una información necesaria para la utilización de la más grande. Sin embargo, esta patente no es suficiente para responder al problema identificado. De hecho, la supresión de una parte del flujo desnaturaliza el formato del flujo, y no puede por lo tanto ser reconocida como un flujo estándar, explotable con aplicaciones de software generales. Este procedimiento del estado de la técnica anterior necesita a la vez un software específico del lado servidor, para la separación de las dos partes, y otro software específico que asegure no sólo la reconstrucción del flujo, sino también la adquisición del flujo principal y su explotación según un formato propietario de la solución. Este formato propietario no es el formato inicial del flujo antes de la separación en dos partes, en esta solución conocida.

[0012] Esta sociedad ha depositado igualmente otras tres patentes: el documento US5892825 retoma la patente precedente pero en un marco menos amplio porque los flujos son siempre encriptados; el documento US6035329 reposa sobre el mismo principio, se refiere a un procedimiento que permite la lectura de un disco de tipo CD-ROM o DVD-ROM condicionalmente a la identificación de los derechos por la inserción de una tarjeta inteligente sobre la cual se almacenan las informaciones necesarias para la lectura. Este procedimiento todavía no es suficiente para nuestro problema porque no garantiza que el flujo modificado sea del mismo formato que el flujo original. Finalmente, el documento US6185306 se refiere a un procedimiento de transmisión de datos encriptados desde un sitio web hacia un ordenador solicitante. Este procedimiento permite sin embargo al usuario de disponer en un momento dado de todas las herramientas necesarias para copiar los datos.

[0013] El estado de la técnica anterior conoce igualmente, por la solicitud de patente europea EP 1 011 269 (Mindport), un sistema de tratamiento de una señal de información. Este documento tiene como objeto impedir la distribución ilícita de copias comprimidas de flujo de información, particularmente audio, video e imagen. Habitualmente, los sistemas de protección de flujo de información tradicionales se basan en un encriptado o codificación efectuado sobre una copia ya comprimida y formateada del flujo (por ejemplo encriptación de los DVD ya comprimidos ...). De este modo, el contenido descriptado del flujo para estos sistemas de protección "tradicionales" es en forma descomprimida y por lo tanto directamente explotable y distribuible. La presente invención consiste en comenzar por encriptar o codificar el flujo, y luego comprimirlo (en lugar de comprimirlo antes y luego codificarlo). Para ello, la invención incluye un análisis de la entropía del flujo que permite encriptar el flujo no comprimido mientras que se conserva su entropía. Conservar su entropía permite alcanzar la misma eficacia de compresión para el flujo. La codificación consiste en añadir un ruido (de tipo ruido blanco pseudoaleatorio) a la señal. Este ruido se genera con ayuda de una clave de codificación. Esta clave es entonces encriptada para un usuario único a través de un sistema de clave pública - clave privada, la clave privada utilizada siendo específica del sistema de descodificación del cliente en cuestión. La clave de codificación encriptada de este modo se envía al cliente que posee los derechos de visualización al mismo tiempo que el flujo protegido. Por parte del cliente, el flujo es descomprimido, luego una señal de descodificación es añadida (sustraída) que se obtiene gracias a la utilización de la clave de descodificación proporcionada al cliente. En el caso del video, la presente invención se aplica sobre los coeficientes DCT de cada bloque de cada imagen, antes de su compresión (por VLC ...). No se descodifican sólo las imágenes I porque sino, las otras imágenes del flujo MPEG corregirían las imágenes siguientes, por lo tanto hay que codificar todas las imágenes. En el caso de un DVD por ejemplo, en el momento del alquiler, el punto de venta da al cliente un disquete (u otro) conteniendo la clave de descodificación que corresponde al cliente.

[0014] El estado de la técnica anterior conoce igualmente, por la solicitud de patente europea EP 0 975 165 (Sony), un aparato y un procedimiento para transmitir de un emisor a un receptor las señales cuyo acceso es controlado. Este documento se refiere a la gestión de los derechos de copia y visualización de un flujo de video. Ésta permite la transmisión por dos vías separadas de dos flujos conteniendo el video y las informaciones de control de acceso. El flujo de video recibido en el dispositivo cliente es, en una primera realización, descodificado, después encriptado o no por un sistema a base de claves pública y privada. Si el usuario tiene todos los derechos sobre la película, puede copiarla a voluntad y mirarla como desee. Si sólo tiene los derechos para una o algunas visualizaciones, el flujo copiado sobre el equipo del cliente sobre

- un casete o un CD o... habrá sido previamente encriptado. Cuando el flujo en cuestión es visualizado, se desencripta por un desencriptador incluido en el equipo del cliente. Si el usuario ya no tiene los derechos, el flujo codificado que ha copiado o que está leyendo no es desencriptado porque el módulo de control de acceso no autoriza la desencriptación. Los controles de acceso del cliente son gestionados y tratados por un módulo de control de acceso interno al equipo del cliente. Los datos de control de acceso se salvaguardan sobre el casete o CD / DVD sobre el cual el video es registrado. Estos pueden además ser descargados. En otra realización, el mismo procedimiento es utilizado pero el módulo de control de acceso no controla un conjunto encriptador / desencriptador integrado en el equipo del cliente, sino que el descodificador descodifica el flujo de vídeo recibido por el servidor de video.
- 5
- 10 [0015] El estado de la técnica anterior conoce igualmente, por la solicitud de patente PCT WO 00 60846 (Diva Systems), una solución de distribución de Video On Demand a través de un sistema de servidores distribuidos. La protección del contenido de video digital basándose en un sistema a base de claves pública / privada. La principal innovación de esta patente es permitir un encriptado y un desencriptado de los flujos MPEG-TS simplificados. El tiempo de cálculo es de hecho fuertemente disminuido gracias a un análisis del flujo MPEG-TS que permite no encriptar más que ciertas partes del contenido. Este análisis del flujo consiste principalmente en marcar los paquetes TS que contengan una información esencial para la buena descodificación (en el sentido MPEG) del video, de manera que en una segunda fase de encriptado, sólo los payloads de los paquetes TS marcados no sean encriptados. De este modo, la información esencial no está disponible para la descodificación y el flujo no puede por lo tanto ser presentado mientras que se conserva un tiempo de cálculo razonable para el encriptado. Hay que a continuación transmitir en el flujo la información que permite al desencriptador de saber si la payload de un paquete está encriptada o no, eso puede hacerse de varias maneras como por ejemplo la adición de una información antes del byte de sincronización o por la modificación del bit de scrambling control o de una información del campo de adaptación. Los paquetes generados de este modo no son perfectamente conformes a la norma.
- 15
- 20
- 25 [0016] A fin de corregir los diferentes defectos del estado de la técnica anterior, la invención se refiere según su acepción más general a un procedimiento para la distribución de secuencias de videos según un formato de flujo nominal constituidos por una sucesión de tramas [frame] que incluye cada una al menos un bloque I correspondiente a una imagen digital completa I, cada imagen I estando descompuesta en bloques y macrobloques dependiendo los unos de los otros por coeficientes de correlación, caracterizado por el hecho de que se procede, antes de la transmisión al equipo del cliente, a un análisis del flujo para generar un primer flujo modificado, presentando el formato de un flujo nominal, y presentando las imágenes I modificadas por la sustitución de ciertos coeficientes de correlación por coeficientes de misma naturaleza pero aleatorios, y un segundo flujo de un formato cualquiera, incluyendo los coeficientes de correlación sustituidos e informaciones digitales aptas para permitir la reconstrucción de dichas imágenes modificadas, luego para transmitir separadamente los dos flujos generados de este modo desde el servidor hacia el equipo destinatario, y por el hecho de que se calcula sobre el equipo destinatario una síntesis de un flujo al formato nominal en función de dicho primer flujo y de dicho segundo flujo.
- 30
- 35
- [0017] Ventajosamente, dicha síntesis produce un flujo rigurosamente idéntico al flujo original, es decir que el procedimiento es sin pérdida.
- 40
- [0018] Según una variante particular de este procedimiento, el formato de flujo nominal se define por las normas MPEG (MPEG-1, MPEG-2, etc.).
- 45
- [0019] Ventajosamente, dicho análisis puede decidir las imágenes I y los coeficientes de correlación que se deben modificar para obtener dicho primer flujo; estas modificaciones pueden ser: reemplazar los coeficientes de correlación de una imagen I a través de coeficientes de correlación de otra imagen I, invertir dos coeficientes de correlación de una misma imagen I, invertir dos coeficientes de correlación de dos imágenes I del mismo flujo, reemplazar los coeficientes de correlación de una imagen I por valores aleatorios.
- 50
- 55 [0020] Ventajosamente, la secuencia de video según un formato de flujo nominal se constituye por una sucesión de tramas [frame] que incluye cada una al menos un bloque I correspondiente a una imagen digital completa I y al menos un bloque P correspondiente a las diferencias entre una imagen P y al menos otra imagen I y/o P. En tal caso, dicho análisis puede decidir las imágenes P que se deben modificar adicionalmente o en lugar de las imágenes I para obtener dicho primer flujo; las modificaciones aportadas entonces a las imágenes P son del mismo tipo que aquellas aportadas a las imágenes I, a saber la modificación de los coeficientes de correlación.
- [0021] En una puesta en marcha particular de este procedimiento, la transmisión de dicho primer flujo se realiza a través un soporte material distribuido físicamente como un CD-ROM, un DVD, un disco duro o una tarjeta de memoria de tipo memoria flash por ejemplo.
- 60
- [0022] En otra puesta en marcha de este procedimiento, la transmisión de dicho primer flujo se realiza a través de una red

de banda ancha (cable, satélite, fibra óptica, hertziano, DSL, DAB).

5 [0023] Según la puesta en marcha de este procedimiento, la transmisión de dicho segundo flujo se realiza a través de una red por cable, a través de una red telefónica conmutada (RTC analógico o digital), a través de una red telefónica móvil que utiliza las normas GSM, GPRS o UMTS, a través de una red BLR. (bucle local inalámbrico) o a través de una red de tipo DSL.

10 [0024] Según una variante particular de este procedimiento, la transmisión de dicho segundo flujo se realiza a través de una red de banda ancha de mismo tipo que la red utilizada por dicho primer flujo, incluso a través de la misma red.

[0025] Según una variante particular de este procedimiento, la transmisión de dicho segundo flujo se realiza a través de una tarjeta de memoria de tipo memoria flash o a través de una tarjeta inteligente.

15 [0026] Ventajosamente, la transmisión de uno de los dos flujos o de los dos flujos es cifrada.

[0027] Ventajosamente, uno de los dos flujo o los dos flujos es tatuado por técnicas tradicionales de "watermarking". El "watermarking", llamado también filigrana digital o tatuaje digital, es una técnica de marcación de contenido visual o sonoro, digital como las imágenes, del flujo de vídeo o del flujo de audio. La técnica consiste en un tratamiento del contenido de manera que se inserten las informaciones en el contenido. En general, las informaciones insertadas son invisibles en el momento de la visión del contenido pero pueden ser recobradas aplicando tratamientos a dicho contenido. Existen dos tipos de filigranas:

- . la filigrana frágil: las informaciones insertadas son afectadas por una modificación del contenido: este tipo de filigrana se utiliza para detectar si el contenido ha sido modificado;
 - . la filigrana robusta: las informaciones insertadas son conservadas aunque el contenido es modificado; este tipo de filigrana es por ejemplo utilizada para asociar los derechos de autor a una obra.
- 25

[0028] Según la puesta en marcha de este procedimiento, los dos flujos generados se pueden destinar a un único equipo, a un grupo de equipos o a todos los equipos.

30 [0029] Según un modo de realización particular, la reconstrucción y en consecuencia la visualización, se acondiciona por una transacción entre el equipo y el portal como el pago, la inscripción en un registro de abono, etc..

[0030] La reconstrucción puede igualmente ser autorizado para una consulta de una copia privada solicitada por el cliente.

35 [0031] De manera general, el hecho de que la reconstrucción esté condicionada a la autorización del portal permite a todo operador del servicio gestionar todos los derechos vinculados a las obras audiovisuales.

[0032] Además, la invención se refiere a un equipo para la fabricación de un flujo de vídeo en vista de la puesta en marcha de este procedimiento que comporta al menos un servidor multimedia conteniendo las secuencias de videos originales y caracterizado por el hecho de que incluye un dispositivo de análisis del flujo de vídeo proveniente de dicho servidor para generar los dos flujos.

40

[0033] Ventajosamente, este equipo incluye una memoria para el registro de un marcador "copia privada" indicando para cada secuencia los derechos de cada usuario: copia privada que se puede mirar un número ilimitado de veces, copia privada que se puede mirar un número limitado de veces y qué número, copia privada prohibida.

45

[0034] Además, la invención se refiere a un equipo para la explotación de un flujo de vídeo con el fin de la puesta en marcha de este procedimiento que incluye un descodificador estándar de flujo, al menos una interfaz de registro (disco duro, memoria tipo memoria flash) destinado a almacenar el contenido de dicho primer flujo y/o un lector de discos (CD, DVD, etc.) y al menos una interfaz de visualización (pantalla estándar, pantalla inalámbrica, videoprojector) caracterizado por el hecho que incluye un medio para la recomposición del flujo original a partir de los dos flujos.

50

[0035] Según un modo de realización particular, dicho medio es una aplicación de software instalada sobre el equipo.

55 [0036] Según otro modo de realización, dicho medio es un dispositivo electrónico fijo.

[0037] Según otro modo de realización, dicho medio es un dispositivo electrónico portátil (móvil) con su pantalla incorporada.

[0038] Según un modo de realización donde el equipo se instala sobre un ordenador, dicho medio utiliza un recurso específico del producto (tarjeta) con el fin de evitar la copia de la información temporal del segundo flujo en un soporte permanente.

60

[0039] Ventajosamente, dicha interfaz de registro almacena también un marcador de "copia privada" en relación con dicho primer flujo indicando para esta secuencia los derechos del usuario: copia privada que se puede mirar un número ilimitado de veces, copia privada que se puede mirar un número limitado de veces y qué número, copia privada prohibida.

[0040] Ventajosamente, el equipo incluye un lector de tarjetas inteligentes que permite identificar al usuario.

[0041] Ventajosamente, el equipo incluye un lector de tarjetas inteligentes, la tarjeta inteligente conteniendo las aplicaciones de software.

[0042] Ventajosamente, el equipo incluye un lector de tarjetas inteligentes, la tarjeta inteligente conteniendo los datos de dicho segundo flujo para un contenido dado.

[0043] Finalmente, la invención se refiere a un sistema para la transmisión de un flujo de vídeo caracterizado por el hecho de que comprende un equipo de producción de un flujo de vídeo, al menos un equipo de explotación de un flujo de vídeo y al menos una red de comunicación entre el equipo de producción y el(los) equipo(s) de explotación.

[0044] La presente invención se comprenderá mejor con la lectura de la descripción de un ejemplo no limitativo de realización que sigue, refiriéndose a los dibujos anexos donde:

- . la figura 1 describe la arquitectura de conjunto de un sistema para la puesta en marcha del procedimiento según la invención
- . la figura 2 representa un modo de realización particular del sistema de análisis y de síntesis de flujo de tipo MPEG conforme a la invención
- . la figura 3 representa un modo de realización particular del sistema de síntesis de flujo conforme a la invención.

[0045] La invención se refiere a un flujo de datos de un formato nominal, particularmente pero no exclusivamente un flujo de tipo MPEG (MPEG-1, MPEG-2). El formato del flujo audiovisual utilizado debe tener las características siguientes:

- . este formato debe descomponer los datos en tramas [frame], cada trama incluyendo una imagen digital I completa;
- . cada imagen I se descompone en macrobloques de un tamaño dado, dichos macrobloques descomponiéndose ellos mismos en bloques de un tamaño dado;
- . cada imagen I contiene los coeficientes de correlación entre los diferentes bloques y/o macrobloques de las imágenes I.

[0046] En la descripción que sigue, el ejemplo se refiere a un flujo MPEG-1 sin que esto constituya una limitación del alcance de la protección.

[0047] El principio general de un procedimiento de protección de un flujo de vídeo está expuesto a continuación. El objetivo es autorizar los servicios de video a la carta a través de todas estas redes de difusión y el registro local en la caja descodificadora digital del usuario. La solución consiste en conservar permanentemente fuera de la vivienda del usuario, de hecho en la red de difusión y de transmisión, una parte del programa audiovisual registrado, esta parte siendo primordial para visualizar dicho programa audiovisual sobre una pantalla de televisión o de tipo monitor, pero siendo de un volumen muy débil respecto al volumen total del programa audiovisual digital registrado en casa del usuario. La parte faltante será transmitida a través de la red de difusión transmisión en el momento de la visualización de dicho programa audiovisual digital prerregistrado en casa del usuario.

[0048] La más grande parte del flujo audiovisual será por lo tanto transmitida a través de una red de difusión tradicional cuando la parte faltante sea enviada bajo petición a través de una red de telecomunicación de banda estrecha como las redes telefónicas tradicionales o las redes celulares de tipo GSM, GPRS o UMTS o utilizando una pequeña parte de una red de tipo DSL o BLR, o de nuevo utilizando un subconjunto del ancho de banda compartido en una red por cable.

[0049] Sobre el dibujo anexo, la figura 1 es un esquema de principio de un sistema de distribución según la presente invención.

- . La figura 2 representa un modo de realización particular del sistema de análisis y de síntesis de flujo conforme a la invención.
- . La figura 3 representa un modo de realización particular del sistema de síntesis de flujo conforme a la invención.

[0050] En la figura 1, el acondicionamiento de interfaz de video (8) se adapta para conectar al menos un dispositivo de visualización, por ejemplo un monitor, un video proyector o un dispositivo de tipo pantalla de televisión (6), con al menos una interfaz de red de transmisión y de difusión de banda ancha (4) y con al menos una interfaz de red de telecomunicación (10). Según la presente invención, este acondicionamiento está compuesto de un módulo (8) que incluye principalmente, por una parte, una unidad de tratamiento adaptada para tratar, en particular descodificar y desaleatorizar todo flujo de vídeo de tipo MPEG según un programa software de descodificación y desaleatorización precargado, de manera que se visualice, en

tiempo real o diferido, se almacene, se registre y/o se envíe en una red de telecomunicación y, por otra parte, al menos una interfaz de pantalla (7) y una interfaz de conexión a una red local o extendida (5) y/o (9). La red de transmisión y de difusión de banda ancha (4) y la red de telecomunicación (10) pudiendo ser confundidas en una sola red.

- 5 [0051] El disco duro del módulo (8) se puede utilizar como memoria tampón para almacenar momentáneamente al menos una parte del programa o de la secuencia de video por visualizar, en caso de visualización diferida o de limitación en la banda de paso de la red de transmisión. La visualización puede ser retrasada o diferida a la solicitud del usuario o del portal (12).
- 10 [0052] Como lo muestra la figura 1, la interfaz de conexión (5) se conecta a una red de transmisión y de difusión de banda ancha (4) tal como un módem, un módem satélite, un módem por cable, de una interfaz de línea de fibra óptica o de una interfaz de radio o infrarrojos para la comunicación inalámbrica.
- 15 [0053] Es por este enlace tradicional de difusión de video que serán transmitidos los contenidos de los programas audiovisuales como las películas. Sin embargo, de manera que no se deje hacer copias piratas, antes de transmitir el contenido audiovisual desde el servidor (1) o el portal (12) está previsto conservar una pequeña parte del contenido audiovisual en el portal (12).
- 20 [0054] En caso de visualización de un programa audiovisual en tiempo real, esta pequeña parte del contenido audiovisual conservada en el portal (12) será igualmente enviada al módulo (8) a través de la red de telecomunicación (10).
- 25 [0055] Como las imágenes sucesivas de una secuencia de video tienen un gran número de elementos visuales idénticos (como en cine, una imagen se parece a la precedente), MPEG no registra más que los elementos que difieren de la imagen de origen. Se modificará por lo tanto una imagen entera de referencia conservando los coeficientes DC de las modificaciones aportadas en el portal (12) y, para las imágenes sucesivas que dependen de esta imagen I de referencia, no es necesario aportar modificaciones ya que harán divergir el flujo visualizado debido a las perturbaciones aportadas a las imágenes I de referencia. La compresión MPEG comienza por lo tanto, en primer lugar, por descomponer la imagen en diferentes matrices cuadradas que comportan varios puntos o píxeles, teniendo cada uno su propio valor colorimétrico. Un cálculo permite obtener un valor medio para cada matriz dentro de la cual cada punto está ahora sumergido. Este
- 30 tratamiento genera una pixelización y la aparición de aplanamientos uniformes, ahí adonde existían matices de color. La segunda etapa de la compresión MPEG consiste en no conservar de una imagen a la otra más que los elementos cambiantes.
- 35 [0056] Para obtener imágenes animadas de tipo MPEG-1 o MPEG-2, el principio consiste en captar algunas imágenes en el tiempo, las imágenes intermediarias siendo calculadas a partir de éstas. El análisis de las imágenes de referencia completas (llamadas I para Intra-frame) permite predecir las imágenes intermediarias P (Predicted frames). A continuación, se intercala entre imágenes de referencia e imágenes predichas, las imágenes B (Bidirectional Frame).
- 40 [0057] El video se representa como una sucesión de imágenes individuales, de las cuales cada una se trata como una matriz bidimensional de elementos de imagen (píxeles). La representación de los colores de cada píxel incluye tres componentes: una componente de luminancia Y y dos componentes de crominancia, Cb y Cr.
- 45 [0058] La compresión del video digitalizado se realiza por la utilización de varias técnicas: bajo muestreo de informaciones de crominancia para adaptarse a la sensibilidad del sistema visual humano (HVS), cuantificación, compensación del movimiento (MC) para explotar la redundancia temporal, transformación en el ámbito frecuencial por la transformación en coseno discreta (DCT) para explotar la redundancia espacial, codificación de longitud variable (VLC) e interpolación de imágenes.
- 50 [0059] El sistema visual humano (HVS) siendo el más sensible a la resolución de la componente de luminancia de una imagen, los valores de píxel Y se codifican a plena resolución. El sistema visual humano es menos sensible a las informaciones de crominancia. El submuestreo elimina los valores de píxeles basados sistemáticamente en la posición, lo que reduce la cantidad de informaciones por comprimir por otras técnicas. La norma conserva un conjunto de píxeles de crominancia para cada vecindad 2x2 de píxeles de luminancia.
- 55 [0060] La unidad de codificación básica de una imagen es el macrobloque. Los macrobloques de cada imagen son codificados sucesivamente, de izquierda a derecha, y de arriba a abajo. Cada macrobloque está compuesto de 6 bloques 8x8: cuatro bloques de luminancia Y, un bloque de crominancia Cb y un bloque de crominancia Cr. Cabe notar que los cuatro bloques de luminancia cubren la misma zona de la imagen que cada uno de los bloques de crominancia, debido al submuestreo de las informaciones de crominancia, efectuado para adaptar la codificación a la sensibilidad del sistema
- 60 visual humano.

- 5 [0061] Para un macrobloque dado, la primera operación es la elección del modo de codificación que depende del tipo de imagen, de la eficacia de la predicción compensada en movimiento en la región codificada, y de la naturaleza de la señal contenida en el bloque. En segundo lugar, se forma una predicción compensada en movimiento del contenido del bloque, basada en imágenes de referencia anterior o futura. Esta predicción es abstraída de los datos reales del macrobloque
- 10 vecino, para formar una señal de error. En tercer lugar, esta señal de error se divide en 6 bloques 8x8 (4 bloques de luminancia y 2 bloques de crominancia en cada macrobloque) a cada uno de los cuales se aplica una transformación en coseno discreta. El bloque 8x8 de coeficientes DCT resultante es cuantificado. El bloque de dos dimensiones que resulta de ello se barre en zigzag para ser convertido en una cadena unidimensional de coeficientes DCT cuantificados. En cuarto lugar, las informaciones anexas del macrobloque (tipo, vectores, etc.) así como los datos de los coeficientes cuantificados son codificados. Para obtener una eficacia máxima, un cierto número de tablas de codificación de longitud variable se definen para los diferentes elementos de datos. Una codificación de las longitudes de rango se aplica a los datos de los coeficientes cuantificados.
- 15 [0062] El coeficiente DCT del punto (0,0) superior izquierdo del bloque representa una frecuencia horizontal y vertical nula: se llama coeficiente DC (continuo). El coeficiente DC siendo proporcional al valor medio de los píxeles del bloque 8x8, la codificación predictiva permite una compresión suplementaria, porque la diferencia de los valores medios de los bloques 8x8 vecinos tiende a ser relativamente pequeña. Los otros coeficientes representan una o varias frecuencias espaciales horizontales y/o verticales no nulas y se llaman coeficientes AC. Para que el nivel de cuantificación de los coeficientes correspondiente a las frecuencias espaciales elevadas favorezca la creación de un coeficiente nulo, se elige un paso de cuantificación tal que el sistema visual humano (VHS) tenga poca probabilidad de percibir la pérdida de la frecuencia espacial concernida, excepto si el valor del coeficiente se encuentra por encima de este nivel de cuantificación. La codificación estadística de las zonas previstas de coeficientes de orden elevado consecutivos de valor nulo, contribuye considerablemente a la ganancia de compresión. Para reagrupar los coeficientes no nulos al inicio de la serie y para codificar tantos coeficientes nulos como sea posible a continuación del último coeficiente no nulo, su secuencia se da por un barrido en zigzag que concentra las frecuencias espaciales elevadas al final de las series.
- 20 [0063] La codificación de longitud variable (VLC) es una técnica de codificación estadística que afecta las palabras clave con los valores por codificar. Las palabras clave cortas son destinadas a los valores de frecuencia de ocurrencia elevada, y las palabras clave largas a aquellas de ocurrencia poco frecuente. De media, las palabras clave cortas más frecuentes son mayoritarias, de manera que la cadena codificada es más corta que los datos de origen.
- 25 [0064] La invención consiste en utilizar la correlación entre los coeficientes DC en una imagen I, a fin de poder manipular el aspecto y la validez visual de la secuencia a la cual pertenece la imagen I en cuestión.
- 30 [0065] De hecho, dado que las imágenes I son los portadores principales de información en una secuencia MPEG, toda modificación importante que afecte a estas imágenes I tendrá necesariamente un impacto sobre la validez de la secuencia.
- 35 [0066] De este modo, la posibilidad de obtener degradaciones importantes de las imágenes I sin efectuar manipulaciones complicadas se ofrece por la correlación entre los coeficientes DC en esta imagen I. Estos coeficientes, siendo fuertemente dependientes los unos de los otros, determinan en gran parte el valor de los coeficientes de la misma naturaleza que siguen. Es así como, modificando la información que está contenida, se modifica profundamente las imágenes I y en consecuencia toda la secuencia MPEG que sigue a esta imagen I.
- 40 [0067] Cada macrobloque de una imagen I contiene seis bloques, cada uno de entre ellos comenzando por un coeficiente DC. Cuatro bloques corresponden a la luminancia (Y), y dos a la crominancia (C) del macrobloque. El valor escrito en un fichero del flujo MPEG representando un coeficiente DC es de hecho la diferencia entre el verdadero valor de este coeficiente y aquel del coeficiente correspondiente que precede y que, para los bloques Y, puede encontrarse en el mismo macrobloque o en el macrobloque precedente, mientras que para los bloques C se encuentra siempre en el macrobloque precedente. Una modificación de una de estas diferencias acarrearán automáticamente una modificación de información en todos los macrobloques que siguen.
- 45 [0068] Este método es óptimo para la degradación visual del flujo MPEG utilizando los coeficientes DC de los bloques, pero se puede aplicar igualmente a los coeficientes AC. Es de este modo considerable de modificar ciertos de estos coeficientes AC de manera aleatoria, de transmitir por dicho segundo flujo cuales coeficientes han sido modificados y cual es su verdadero valor y de reconstituir el flujo original gracias a estas informaciones. La continuación es desarrollada utilizando los coeficientes DC pero es convenido que toda la continuación se puede aplicar a los coeficientes AC.
- 50 [0069] Cuando éste lee el tren binario, un descodificador tradicional MPEG identifica el principio de una imagen codificada, después el tipo de la imagen. Para evitar cualquier confusión entre una caja descodificadora estándar a menudo llamada "Set Top Box o STB", el descodificador estándar MPEG será llamado "Lector" ("Player" o "Viewer") en la continuación del documento. Este Lector se puede realizar en hardware y/o en software. El lector MPEG descodifica sucesivamente cada
- 55
- 60

macrobloque de la imagen. La imagen se reconstruye cuando todos sus macrobloques han sido tratados. Si se trata de una imagen I, ésta constituye una imagen de referencia para las imágenes subsiguientes y se almacena en lugar de la imagen de referencia más antigua. Las imágenes son de este modo disponibles, en forma digital, para posttratamiento y visualización, a merced de la aplicación.

5

[0070] En el caso de un programa audiovisual de tipo MPEG, todas las características de las imágenes I procedentes del servidor (1) o del portal (12) no se transmiten hacia el módulo (8). En particular, las características conforme a la invención son los coeficientes de correlación DC contenidos en las imágenes I.

10

[0071] Ciertos coeficientes DC de estas imágenes I se conservan en el portal (12). En cambio, en lugar de los coeficientes DC de estas imágenes I no transmitidos, el dispositivo conforme a la invención intercalará falsos coeficientes DC de misma naturaleza que los coeficientes DC liberados y conservados en el portal (12) de manera que el Lector estándar MPEG del módulo (8) no sea perturbado por estas modificaciones que ignorará y reconstituirá en la salida un flujo de salida MPEG que no será correcto desde el punto de vista visual para un ser humano pero correcto desde el punto de vista formato MPEG.

15

[0072] El Lector MPEG de la caja (8) es un Lector estándar MPEG y no es de ningún modo modificado o afectado por los cambios aportados a las imágenes I.

20

[0073] Como lo muestra la figura 1, la interfaz de conexión (9) se conecta a una red de telecomunicación extendida (10), directamente o por una red local que sirve de red de acceso y se constituye por ejemplo de una interfaz de línea de abonado (red telefónica analógica o digital, DSL, BLR, GSM, GPRS, UMTS, etc).

25

[0074] Así pues, los programas audiovisuales se difunden de manera tradicional en modo multidifusión ("broadcast") a través de la red de transmisión de banda ancha (4) de tipo hertziano, cable, satélite, digital hertziano, DSL, etc. desde el servidor (1) directamente a través del enlace (3bis) o a través del portal (12) a través del enlace (2) y (3) hacia el módulo descodificador (8) a través del enlace (5). Cada programa audiovisual de este modo difundido puede ser encriptado o no, y, conforme a la presente invención, el flujo de tipo MPEG contiene las modificaciones a nivel de ciertas imágenes I como se describe arriba. En función de los parámetros elegidos por el usuario o de las informaciones transmitidas por el servidor de difusión, ciertos programas audiovisuales modificados de este modo e incompletos se registran en el disco duro de la caja (8).

30

[0075] Cuando el usuario desea visualizar un programa audiovisual de este modo registrado en el disco duro de su caja (8) hace la solicitud de manera tradicional a través de un mando a distancia conectado a su caja (8) que se conecta entonces automáticamente al portal (12) a través del enlace (9) de tipo red local o acceso directo y a través de la red de telecomunicación (10) él mismo conectado al portal (12) a través del enlace (11). A lo largo de la visualización del programa audiovisual, los enlaces (9) y (11) quedan establecidos y permiten a la caja (8) recibir las funciones y los parámetros de reparación en orden de los coeficientes DC modificados de las imágenes I. Los coeficientes DC modificados de las imágenes I transmitidos de este modo no son nunca registrados en el disco duro de la caja (8) porque las imágenes I reconstituidas son directamente visualizadas sobre la pantalla de visualización (6) a través del enlace (7) después de haber sido tratadas por el Lector de la caja (8) a partir de su memoria local volátil. Una vez tratados y visualizados, los coeficientes DC modificados y/o carentes de las imágenes I que acaban de ser transmitidos por el portal (12) serán borrados de la memoria volátil local de la caja (8).

35

40

45

[0076] Según un modo de realización particular, los coeficientes DC modificados de las imágenes I difundidas de este modo pueden ser encriptados o no, por todo medio de encriptado existente o futuro. Por eso ocurre lo mismo con los algoritmos, las funciones y los parámetros de reparación en orden de los coeficientes DC modificados de las imágenes I.

50

[0077] Cada vez que el usuario quiera mirar un programa registrado en el disco duro de la caja (8) la caja (8) se conectará automáticamente al portal (12). Igualmente cuando el usuario haga una pausa, la transmisión de los coeficientes DC modificados de las imágenes I procedentes del portal (12) será interrumpida hasta la reanudación de la visualización, garantizando así que todas las informaciones de un programa audiovisual no se encuentren en la caja (8) en un momento dado y evitando de este modo a una persona mal intencionada de hacer copias piratas de estos registros.

55

[0078] Según un modo de realización particular, la caja (8) incluye un lector de tarjetas inteligentes que permitirá al portal (12) autenticar el usuario propietario de la caja (8).

[0079] Según un modo de realización particular, para un contenido MPEG dado, la tarjeta inteligente contiene dicho segundo flujo que ha sido memorizado por el portal (12).

60

[0080] Si esto es autorizado, la tarjeta inteligente permite igualmente al usuario efectuar copias privadas de los programas audiovisuales registrados sobre el disco duro de su caja descodificadora (8). Por eso, si el usuario quiere hacer una copia

privada de un programa audiovisual, lo hará de manera tradicional sobre una grabadora de video a través del enlace (7) que conecta la caja (8) a la pantalla de visualización (6).

5 [0081] Sin embargo, si desea conservar una copia privada en el disco duro de su caja, lo indicará a su caja (8) que registrará la información de "copia privada" así como las coordenadas del usuario que se halla sobre la tarjeta inteligente, en un campo particular (84) de este programa audiovisual registrado sobre el disco duro (85) de la caja descodificadora (8). A continuación, cada vez que el usuario quiera visualizar esta copia privada, la caja (8) se conectará automáticamente al portal (12) e indicará a este último que el usuario quiere hacer una lectura de su copia privada; a cambio, si la lectura de la copia privada es posible para este usuario que posee esta tarjeta inteligente conectada a esta caja (8), la caja descodificadora (8) 10 recibirá entonces los coeficientes DC modificados y/o carentes de las imágenes I así como todas las otras informaciones que permiten la visualización del programa audiovisual que constituye la copia privada.

[0082] Según otro modo de realización, si el usuario desea conservar una copia privada en el disco duro de su caja, lo indicará al servidor que registrará en la memoria copia privada (124) del portal (12) la información de "copia privada" para este programa y para este usuario, autenticado por la tarjeta inteligente. A continuación, cada vez que el usuario quiera visualizar esta copia privada, la caja (8) se conectará automáticamente al portal (12) e indicará a este último que el usuario quiere hacer una lectura de su copia privada; a cambio, si la lectura de la copia privada es posible para este usuario que posee esta tarjeta inteligente y para este programa, la caja descodificadora (8) recibirá entonces los coeficientes DC carentes de las imágenes I así como todas las demás informaciones que permiten la visualización del programa audiovisual 20 constituyendo la copia privada.

[0083] Según un modo de realización particular, la copia llamada privada podrá permitir al usuario mirar este mismo programa audiovisual de manera ilimitada o un número de veces determinado anticipadamente por el ofrecedor del servicio que ha autorizado esta copia privada. 25

[0084] La presente invención se refiere igualmente a la caja física (8) utilizada por el consumidor para acceder a los datos. Esta caja física se sitúa en el domicilio del usuario. Proporciona un conjunto de funcionalidades que llevan la información apropiada que se debe presentar según la selección de la audiencia y gestiona la conexión y la comunicación con el servidor distante. 30

[0085] Según un modo de realización particular la caja física correspondiente al acondicionamiento de interfaz de video (8) se realiza como un dispositivo autónomo fijo con disco duro integrado.

[0086] Según un modo de realización particular la caja física correspondiente a la disposición de interfaz de video (8) se realiza como un dispositivo autónomo portátil (móvil) con disco duro integrado y/o lector de discos (CD, DVD, etc.). 35

[0087] Según un modo de realización particular la caja física autónoma (8) incluye un lector de tarjetas inteligentes.

[0088] Según otro modo de realización particular la disposición de interfaz de video (8) se realiza como una tarjeta adicional que será instalada en un ordenador de tipo PC y será conectada con al menos una interfaz de red de transmisión y de difusión de banda ancha (4) y con al menos una interfaz de red de telecomunicación (10). Esta tarjeta utilizará el disco duro del ordenador PC para el registro del primer flujo, pero incluirá su propio calculador y su propia memoria volátil de manera que no deje al usuario del PC mal intencionado el medio de acceder a las informaciones complementarias como los coeficientes DC modificados de las imágenes I del segundo flujo. 40 45

[0089] Según la presente invención, los servidores de video y multimedia (1) y/o (12) comprenden los medios de codificación, de transcodificación y de interferencia de datos de video, en particular los medios de añadir las informaciones criptográficas y de seguridad al inicio y todo al largo de las secuencias.

[0090] Finalmente cabe destacar que la invención degrada el flujo MPEG desde el punto de vista visual hasta que ya no permita el reconocimiento de las escenas transmitidas y visualizadas sin tener acceso a los datos y características complementarias, pero reconstituye totalmente el flujo MPEG en el acondicionamiento de interfaz de video (8) sin ninguna pérdida. 50

[0091] A pesar de que la presente invención esté orientada de una forma más particular sobre los datos audiovisuales, se comprende que toda la información multimedia interactiva y todos los datos interactivos se pueden tratar por la presente disposición y el presente sistema, los datos de video de tipo MPEG siendo los más elaborados. La presente invención se comprenderá mejor gracias a la descripción siguiente que presenta la base física de la presente invención y en referencia a la figura 2 del dibujo anexo representando un modo de realización preferido de esta última en tanto que ejemplo no limitativo de realización particularmente bien adaptada para las redes por cable y de satélites. El flujo MPEG (101) completo se analiza por el dispositivo de análisis (121) del portal (12) y será de este modo separado en un flujo de tipo MPEG pero cuyos 55 60

coeficientes DC carentes de las imágenes I habrán sido tratados y que será enviado a través de la salida (122) del portal hacia la red de difusión transmisión de banda ancha (4).

- 5 [0092] La otra parte del flujo MPEG modificado será memorizada en la memoria tampón (123) del portal (12). Para cada flujo MPEG difundido de este modo, el portal (12) conservará en una memoria tampón (123) las modificaciones que habrán sido aportadas a este flujo MPEG por el analizador (121) del portal (12). Se precisa que, para un mismo flujo de entrada MPEG (101) el tratamiento del flujo puede ser diferente para cada usuario (8) y/o para cada grupo de usuarios (8). De este modo, la memoria tampón (123) del portal (12) incluye una zona de memoria diferente para cada usuario.
- 10 [0093] En los ejemplos realizados, para un primer usuario, cada imagen I del flujo MPEG es modificado; para un segundo usuario, ciertas imágenes I y ciertas imágenes P del flujo MPEG son modificadas; en el tercer ejemplo, el dispositivo (8) es portátil (móvil).
- 15 [0094] Describamos ahora en detalle las diferentes etapas para este primer usuario.
- [0095] El portal (121) ha elegido el flujo MPEG (101) que va a tener que enviar al usuario (8) para ser mirado en diferido sobre su pantalla de televisión (6). Este usuario se conecta a una red por cable digital de difusión (4) y a una red de telecomunicación ADSL (10).
- 20 [0096] El sistema de análisis (121) del portal (12) va a leer por lo tanto el flujo entrante MPEG (101) y, cada vez que detecta una imagen I, la descompone en macrobloques (también en tramos - slices), luego en bloques. Este análisis le permite reconocer en el código los coeficientes DC, y sustituir algunos de entre ellos a través de valores aleatorios, con el fin de volver las imágenes (y en consecuencia la secuencia) ilegibles desde el punto de vista visual humano. Los verdaderos valores de los coeficientes DC serán almacenados en el tampón de salida (123), que permitirá luego la reconstitución de la
- 25 secuencia de salida en la caja (8), siguiendo el esquema inverso. En el ejemplo realizado, un macrobloque sobre dos incluye un bloque (coeficiente DC) modificado, mientras que se respeta la igualdad de las frecuencias de modificación para los seis bloques de un macrobloque.
- 30 [0097] El sistema de análisis (121) inscribe entonces el valor del coeficiente sustituido de la imagen I modificada en el tampón (123). El sistema de análisis (121) continua su análisis hasta el final del flujo de entrada MPEG.
- [0098] El nuevo flujo MPEG modificado es entonces registrado en el tampón de salida (122) para ser difundido sobre la red de difusión (4) a través del enlace (3). Los coeficientes DC sustituidos de las imágenes I modificadas del flujo MPEG entrante (101) se memorizan en el tampón (123) del portal (12).
- 35 [0099] Durante este tiempo, y de manera totalmente no sincronizada, el flujo de salida MPEG modificado en procedencia del tampón de salida (122) del portal (12) se difunde a través de la red de banda ancha (4) hacia uno o varios usuarios (8).
- 40 [0100] Cada caja descodificadora autorizada (8) que desea registrar este flujo MPEG de este modo modificado puede entonces leer este flujo MPEG y registrarlo sobre su disco duro (85). Esta iniciativa de registro es dejada al descodificador (8) bajo el control del portal (12). Para eso, el sistema de análisis (121) había inscrito al principio del flujo MPEG, una información de datos suplementarios que precisaba los destinatarios de este flujo MPEG modificado. Los destinatarios pueden ser de este modo un destinatario (8) particular y él solo, un grupo de destinatarios (8) o el conjunto de los descodificadores (8) conectados a la red (4).
- 45 [0101] La fase descrita arriba corresponde a la primera fase de preparación del flujo MPEG por el portal (12), a su transmisión a través de la red de banda ancha (4) y a su registro en un descodificador (8). Este descodificador puede entonces visualizar este flujo MPEG registrado en su disco duro (85). Por eso, el sistema de síntesis (87) del descodificador (8) va a leer el fichero MPEG desde su disco duro (85) y va a enviarlo hacia un lector tradicional MPEG (81). Si no se recibe ningún dato complementario por el sistema de síntesis (87), entonces el flujo MPEG que alcanza al lector (81) se trata y se visualiza tal cual, lo que provoca una distorsión importante del visualizador sobre la pantalla de visualización (6). De hecho, las imágenes I modificadas que se tratan por el sistema de síntesis (87) no corresponden a las imágenes I que son necesarias para una visualización correcta, puesto que ciertos coeficientes de correlación DC han sido sustituidos a través de coeficientes aleatorios. En cambio, como el flujo registrado es bien un flujo de tipo MPEG, el lector (81) no hace ninguna
- 50 diferencia y visualiza las informaciones sobre la pantalla de salida (6) que aparecen bien como datos de un flujo de vídeo MPEG pero totalmente incoherentes para el ser humano que mire la pantalla (6). Toda copia del flujo MPEG procedente del disco duro (85) de la caja (8) producirá el mismo efecto visual en el momento de su restitución por un lector MPEG cualquiera; toda utilización de esta copia que fuera mal intencionada está por lo tanto abocada al fracaso.
- 55 [0102] Cuando el usuario del descodificador (8) quiere realmente visualizar sobre su pantalla (6) el programa audiovisual registrado sobre su disco duro (85), hace la solicitud al sistema de síntesis (87) con su mando a distancia como lo haría con
- 60

una grabadora de video o un lector de DVD presentando un menú sobre su pantalla de televisión. El sistema de síntesis (87) hace entonces una solicitud al disco duro (85) y comienza a analizar el flujo MPEG modificado procedente del disco duro (85) a través del tampón de lectura (83). El sistema de síntesis (87) establece entonces un enlace con el portal (12) a través de la red de telecomunicación (10) que es en nuestro ejemplo un enlace DSL. Una vez establecido este enlace, y durante toda la duración de visualización de la película o del programa audiovisual, el sistema de síntesis (87) hace llegar de la memoria tampón (123) del servidor (12) los coeficientes de correlación sustituidos y los datos correspondientes a las imágenes I modificadas del flujo registrado sobre el disco duro (85). Estos coeficientes de correlación y estos datos de posición alcanzan al sistema de síntesis (87) a través de la memoria tampón de entrada (86) y se almacenan temporalmente en la memoria volátil (88) del sistema de síntesis (87). A partir del flujo MPEG modificado que llega a través del tampón (83) y a partir de los coeficientes de correlación y de los datos asociados que llegan a través del tampón (86) en la memoria (88), el sistema de síntesis (87) reconstituye de manera inversa al proceso de análisis descrito previamente, las imágenes I modificadas por las imágenes I reales y envía el nuevo flujo MPEG de este modo reconstituido hacia el lector (81) para ser visualizado correctamente sobre la pantalla (6). Desde su utilización, los coeficientes de correlación que se deben sustituir y los datos asociados a estas imágenes I son borrados de la memoria volátil (88).

[0103] En el ejemplo realizado, antes de que el portal (12) autorice el envío de las imágenes I y de los datos asociados desde su tampón (123), el portal (12) ha verificado que el usuario de la caja (8) estaba efectivamente autorizado a hacerlo. Para eso, el portal (12) lee las informaciones contenidas sobre la tarjeta inteligente (82) de la caja (8) y verifica que este usuario está efectivamente autorizado a mirar este programa audiovisual. Es sólo después de esta verificación, que los coeficientes de correlación y los datos asociados son enviados desde el tampón (123) hacia la caja (8) correspondiente a este usuario a través de la red (10).

[0104] En el ejemplo realizado, el usuario ha hecho además una copia privada de su programa audiovisual. El sistema de síntesis (87) ha inscrito por lo tanto en una parte (84) del disco duro (85) datos complementarios así como el número de la tarjeta inteligente (82) y la información "copia privada" como datos asociados a este programa audiovisual. En el momento de la próxima lectura privada de este programa audiovisual, el sistema de síntesis (87) analizará estos datos asociados e informará de este modo al portal (12) de que el usuario del descodificador (8) hace una lectura de la copia privada. Si esta función es autorizada para este usuario (8) por el portal (12), los coeficientes de correlación y los datos asociados serán entonces enviados por el portal (12) hacia el tampón (86) como se describe arriba. En el caso contrario, los coeficientes de correlación y los datos asociados no serán enviados y el usuario del descodificador (8) no podrá mirar el flujo MPEG reconstituido.

[0105] Describimos ahora en detalle las diferentes etapas para el segundo usuario (8).

[0106] En este segundo caso, la red de difusión (4) es una red de satélites y la red de telecomunicación (10) es un sistema de telefonía celular de débil ancho de banda de tipo GSM.

[0107] De manera idéntica a la descripción anterior, el usuario del descodificador (8) va a recibir el flujo MPEG y los datos complementarios desde el portal (12).

[0108] Por el contrario, en el ejemplo realizado, en lugar de modificar cada imagen I, el sistema de análisis (121) no toma más que una imagen I sobre n donde n es un número aleatorio comprendido entre 1 y 12 y tiene en cuenta las imágenes P. De este modo, antes del envío del flujo MPEG a partir del tampón de salida (122), el sistema de análisis (121) leerá el flujo de entrada MPEG, (101) y después del sorteo del número aleatorio n, el sistema de síntesis modifica los coeficientes de correlación de la n-ésima imagen I del flujo MPEG. Después cada imagen I modificada de este modo, el sistema de análisis (121) hará un nuevo sorteo de un número n aleatorio. Cada número aleatorio utilizado de este modo se registra en el tampón (123) del portal (12). Para las imágenes P, el sistema de análisis (121) toma en cuenta una imagen P sobre m donde m es un número aleatorio comprendido entre 1 y 5, en una trama para la cual la imagen I no ha sido modificada.

[0109] El sistema de análisis (121) del portal (12) lee el flujo entrante MPEG (101) y, cada vez que detecta una n-ésima imagen I o una m-ésima imagen P, éste la descompone en macrobloques (también en tramos - slices), luego en bloques. Este análisis le permite reconocer en el código los coeficientes DC, y sustituir algunos de ellos a través de valores aleatorios, con el fin de volver las imágenes (y en consecuencia la secuencia) ilegibles desde el punto de vista visual humano. Los verdaderos valores de los coeficientes DC serán almacenados en el tampón de salida (123), que permitirá luego la reconstitución de la secuencia de salida en la caja (8), siguiendo el esquema inverso.

[0110] Además, en este segundo ejemplo realizado, todos los coeficientes DC de esta cada n-ésima imagen I no serán modificados. Solo un macrobloque sobre dos incluye un bloque (coeficiente DC) modificado, mientras que se respeta la igualdad de las frecuencias de modificación para los seis bloques de un macrobloque. Además, la sustitución de cada coeficiente DC se hace por un coeficiente DC calculado de manera aleatoria, pero su valor se compara al valor del coeficiente DC que se debe sustituir para verificar su separación. Si esta separación es demasiado débil, otro número

aleatorio se calcula para aumentar la separación entre el coeficiente que se debe sustituir y el coeficiente de sustitución.

[0111] Ocurre lo mismo con las imágenes P.

5 [0112] Para la reconstitución del flujo MPEG, el descodificador (8) lee los tampones (86) y (87) y descodifica los elementos de datos del tren binario, conforme a la sintaxis definida.

10 [0113] Cuando éste lee el tren binario, el descodificador identifica el inicio de una imagen codificada, luego el tipo de la imagen. Descodifica sucesivamente cada macrobloque de la imagen. El tipo de macrobloque y los vectores movimiento se utilizan para construir una predicción del macrobloque corriente, basado en imágenes de referencia anterior y futura que han sido almacenados en el descodificador. Los datos de los coeficientes se descodifican y descuantifican. Cada bloque 8x8 de datos de coeficientes se transforma por una DCT inversa. El resultado se agrega a la señal de predicción, con una dinámica definida. Antes de enviar el flujo MPEG al lector (81), el sistema de síntesis (87) reemplaza los coeficientes DC de las imágenes I y P que han sido sustituidas por aquellos del flujo proveniente del tampón (86).

15 [0114] En el momento de la reconstitución del flujo MPEG por el sistema de síntesis (87) del descodificador (8), la lectura de estos números aleatorios y de los coeficientes de correlación sustituidos desde el tampón de salida (123) del portal (12) y la lectura del flujo MPEG de este modo modificado desde el disco duro (85) de la caja (8) permiten al sistema de síntesis (87) reconstituir las imágenes I y P y enviarlo todo al lector (81).

20 [0115] La imagen se reconstruye por el lector (81) cuando todos estos macrobloques han sido tratados. Si se trata de una imagen I o de una imagen P, ésta constituye una imagen de referencia para las imágenes subsiguientes y se almacena en lugar de la antigua imagen de referencia. Antes de su visualización, puede ser necesario reordenar las imágenes, para volver del orden de codificación al orden natural de visualización. Después de haber sido reordenadas, las imágenes están disponibles, en forma digital, para posttratamiento y visualización, al grado de la aplicación.

25 [0116] En el ejemplo realizado para este usuario, ha sido constatado que el segundo flujo pedía un ancho de banda inferior a uno por mil del ancho de banda necesario para transmitir el flujo MPEG de alta calidad, sea tres kilobits por segundo para el segundo flujo frente a tres megabits por segundo para el primer flujo MPEG.

30 [0117] Describimos ahora en detalle las diferentes etapas para la tercera realización representada por la figura 3.

[0118] En esta realización, el flujo MPEG se trata por el sistema de análisis (12) de la misma manera que el flujo MPEG de la segunda realización.

35 Sin embargo, el primer flujo MPEG modificado es inscrito y registrado en un soporte físico (20) de tipo CD a partir de la memoria tampón de salida del sistema de análisis (12).

40 [0119] El segundo flujo se memoriza en el tampón (123) y es igualmente registrado además en un soporte físico (10bis) de formato tarjeta de crédito, constituido por una tarjeta inteligente y una memoria flash. Esta tarjeta (10bis) será leída por el lector de tarjetas (82) del dispositivo (8). El dispositivo (8) es un sistema autónomo, portátil y móvil. En la realización, el dispositivo (8) incluye el sistema de síntesis (87), el lector estándar MPEG (81), las dos memorias tampones (86) y (83) así como el lector de discos (85).

45 [0120] El dispositivo (8) incluye además una pantalla integrada (6bis) de tipo pantalla plana que permite al usuario visualizar directamente sus programas audiovisuales sobre su dispositivo (8) autónomo.

[0121] Para visualizar un programa audiovisual de tipo MPEG, el usuario del dispositivo (8) introduce en su lector de discos (85) un disco (20bis) de tipo (20) idéntico a aquel registrado por el sistema de análisis (12). Este disco (20bis) contiene de este modo un flujo MPEG de tipo primer flujo, es decir con los coeficientes DC de ciertas imágenes I y/o P sustituidos.

50 [0122] El usuario del dispositivo (8) puede por lo tanto visualizar este flujo MPEG sobre su pantalla (6bis) integrada en su dispositivo. Sin embargo, a causa de la sustitución de los coeficientes DC, el flujo MPEG no será correcto desde el punto de vista visual. Para volver el flujo correcto de forma visual, el usuario introduce en el lector de tarjeta inteligente (82) la tarjeta inteligente (10bis) conteniendo el segundo flujo con los coeficientes DC. El sistema de síntesis reconstituye entonces el flujo MPEG correcto a partir del primer flujo proveniente del disco (20bis) y del segundo flujo proveniente de la tarjeta (10bis) conectada al lector (82).

55 [0123] En una disposición particular, la tarjeta inteligente (10bis) contiene igualmente las aplicaciones y los algoritmos que serán ejecutados por el sistema de síntesis (87).

60 [0124] En otra disposición particular, la tarjeta inteligente (10bis) contiene los datos y los coeficientes DC de varios segundos

flujos para la reconstitución de varios flujos MPEG.

[0125] En una disposición particular, el dispositivo (8) incluye un enlace celular hacia una red GSM (10).

REIVINDICACIONES

- 5 1. Procedimiento para la distribución de secuencias de video según un formato de flujo nominal constituidos por una sucesión de imágenes que incluye las imágenes I correspondiente a una imagen digital completa I y de las imágenes P correspondiente a las diferencias entre una imagen P y al menos otra imagen I y/o P, cada imagen I o P estando descompuesta en macrobloques y en bloques, conteniendo coeficientes DCT, caracterizado por el hecho de que se procede, antes de la transmisión al equipo cliente, a un análisis del flujo para generar un primer flujo modificado, presentando el formato de un flujo nominal, y presentando las imágenes 1 modificadas por la sustitución de ciertos coeficientes DC de los bloques DCT a través de coeficientes DC de misma naturaleza de tal manera que este primer flujo es
- 10 correcto desde el punto de vista formato MPEG, y un segundo flujo de un formato cualquiera, que incluye los coeficientes DC sustituidos y las informaciones digitales aptas para permitir la reconstrucción de dichas imágenes modificadas, luego para transmitir separadamente los dos flujos generados de este modo desde el servidor hacia el equipo destinatario, y por el hecho de que se calcula sobre el equipo destinatario una síntesis de un flujo al formato nominal en función de dicho primer flujo y de dicho segundo flujo.
- 15 2. Procedimiento para la distribución de secuencias de video según la reivindicación 1, caracterizado por el hecho de que cada trama incluye al menos un bloque P correspondiente a las diferencias entre una imagen llamada P y al menos otra imagen I y/o P.
- 20 3. Procedimiento para la distribución de secuencias de video según la reivindicación 2, caracterizado por el hecho de que al menos una imagen P se modifica de la misma manera que las imágenes I.
- 25 4. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que el formato de flujo nominal se define por la norma MPEG-1 o MPEG-2.
5. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que dicho análisis puede decidir las imágenes I y/o P que se deben modificar.
- 30 6. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que dicho análisis puede decidir los coeficientes DC que se deben modificar.
- 35 7. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que la transmisión de dicho primer flujo se realiza a través un soporte material distribuido físicamente [CD-ROM, disco duro, tarjeta de memoria flash].
- 40 8. Procedimiento para la distribución de secuencias de video según una de las reivindicaciones 1 a 6, caracterizado por el hecho de que la transmisión de dicho primer flujo se realiza a través una red de banda ancha [cable, satélite, digital hertziano, fibra óptica, DSL (Digital Subscriber Line), BLR (bucle local radio)] o DAB [Digital Audio Broadcasting].
9. Procedimiento para la distribución de secuencias de video según una de las reivindicaciones 1 a 8, caracterizado por el hecho de que la transmisión de dicho segundo flujo se realiza a través de una red telefónica conmutada (RTC analógica o digital), o a través de una red de tipo DSL (Digital Subscriber Line) o a través de una red BLR (bucle local radio) o a través de una red de telefónica móvil que utiliza las normas GSM, GPRS o UMTS.
- 45 10. Procedimiento para la distribución de secuencias de video según una de las reivindicaciones 1 a 8, caracterizado por el hecho de que la transmisión de dicho segundo flujo se realiza a través de un soporte material distribuido físicamente [tarjeta de memoria flash, tarjeta inteligente].
- 50 11. Procedimiento para la distribución de secuencias de video según una de las reivindicaciones 1 a 8, caracterizado por el hecho de que la transmisión de dicho segundo flujo se realiza a través una red de banda ancha de mismo tipo que la red utilizada por dicho primer flujo.
- 55 12. Procedimiento para la distribución de secuencias de video según una de las reivindicaciones 1 a 8, caracterizado por el hecho de que la transmisión de dicho segundo flujo se realiza a través de la misma red de banda ancha que aquella utilizada por dicho primer flujo.
13. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que la transmisión de al menos uno de los dos flujos es cifrada.
- 60 14. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que al menos uno de los dos flujos es tatuado [watermarkado].

- 5 15. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que los dos flujos generados se destinan a un solo equipo, a un grupo de equipos o a todos los equipos.
16. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que la reconstrucción está condicionada por una transacción.
- 10 17. Procedimiento para la distribución de secuencias de video según cualquiera de las reivindicaciones precedentes, caracterizado por el hecho de que la reconstrucción se puede autorizar para una consultación de una copia privada solicitada por el cliente.
- 15 18. Equipo para la fabricación de un flujo de vídeo con el fin de la puesta en marcha del procedimiento según la reivindicación 1, que comporta al menos un servidor multimedia conteniendo las secuencias de video originales y caracterizado por el hecho de que incluye un dispositivo de análisis del flujo de vídeo proveniente de dicho servidor para generar los dos flujos.
- 20 19. Equipo para la fabricación de un flujo de vídeo según la reivindicación 18, caracterizado por el hecho de que incluye una memoria para el registro de un marcador de "copia privada" indicando para cada secuencia los derechos de cada usuario: copia privada que se puede mirar un número ilimitado de veces, copia privada que se puede mirar un número limitado de veces y qué número, copia privada prohibida.
- 25 20. Equipo para la explotación de un flujo de vídeo con el fin de la puesta en marcha del procedimiento según la reivindicación 1, que incluye un descodificador estándar de flujo, al menos una interfaz de registro [disco duro] destinado a almacenar el contenido de dicho primer flujo y al menos una interfaz de visualización caracterizado por el hecho de que incluye un medio para la recomposición del flujo original a partir de los dos flujos.
- 30 21. Equipo para la explotación de un flujo de vídeo según la reivindicación 20, caracterizado por el hecho de que dicho medio es una aplicación de software instalada sobre el equipo.
- 35 22. Equipo para la explotación de un flujo de vídeo según la reivindicación 20, caracterizado por el hecho de que dicho medio es una aplicación de software instalada sobre una tarjeta inteligente.
- 40 23. Equipo para la explotación de un flujo de vídeo según la reivindicación 20, caracterizado por el hecho de que dicho medio es un dispositivo electrónico.
- 45 24. Equipo para la explotación de un flujo de vídeo según una de las reivindicaciones 20 a 23, caracterizado por el hecho de que en el caso de la instalación sobre un ordenador, dicho medio utiliza un recurso específico del producto [tarjeta] con el fin de evitar la copia de la información temporal en un soporte permanente.
- 50 25. Equipo para la explotación de un flujo de vídeo según una de las reivindicaciones 20 a 24, caracterizado por el hecho de que dicha interfaz de registro almacena también un marcador de "copia privada" en relación con dicho primer flujo que indica para esta secuencia los derechos del usuario: copia privada que se puede mirar un número ilimitado de veces, copia privada que se puede mirar un número limitado de veces y qué número, copia privada prohibida.
26. Equipo para la explotación de un flujo de vídeo según una de las reivindicaciones 20 a 25, caracterizado por el hecho que comprende un lector de tarjetas inteligentes que permite identificar el cliente cuando quiere visualizar un programa audiovisual registrado sobre su disco duro.
27. Sistema para la transmisión de un flujo de vídeo que incluye un equipo de producción de un flujo de vídeo según cualquiera de las reivindicaciones 18 a 19, al menos un equipo de explotación de un flujo de vídeo según cualquiera de las reivindicaciones 20 a 26 y al menos una red de comunicación entre el equipo de producción y el(los) equipo(s) de explotación.

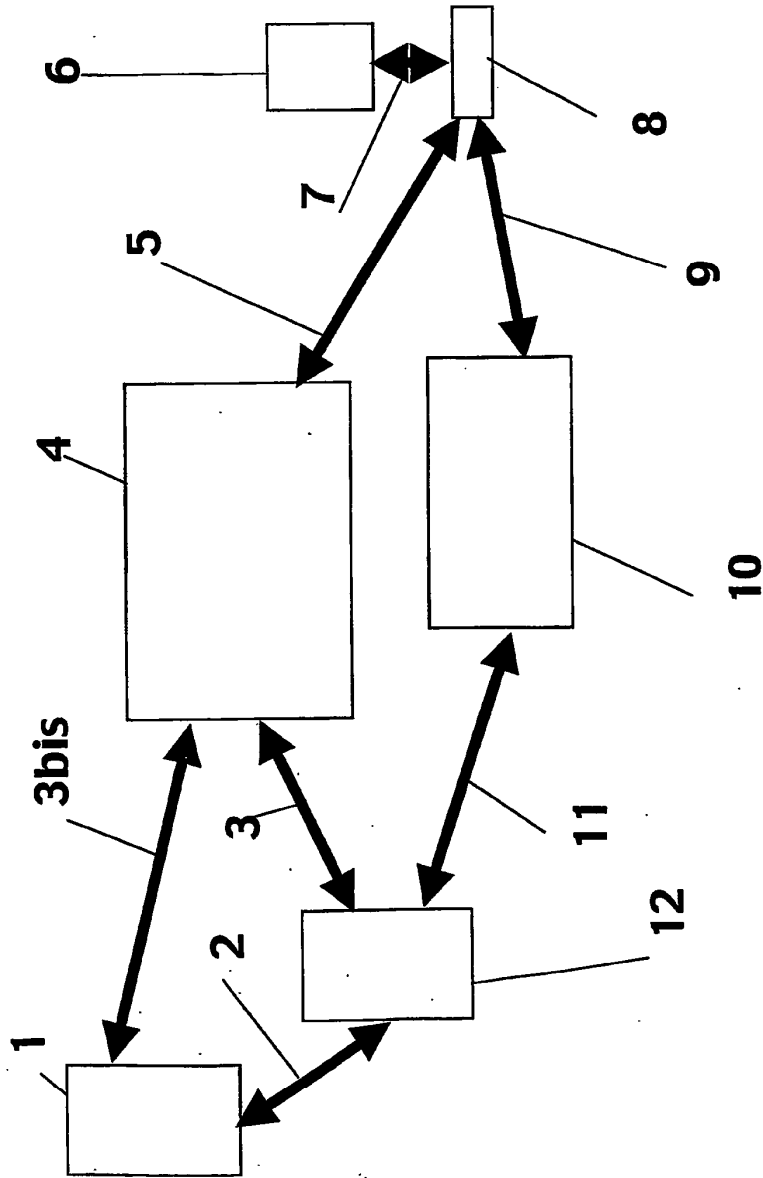


Figura 1

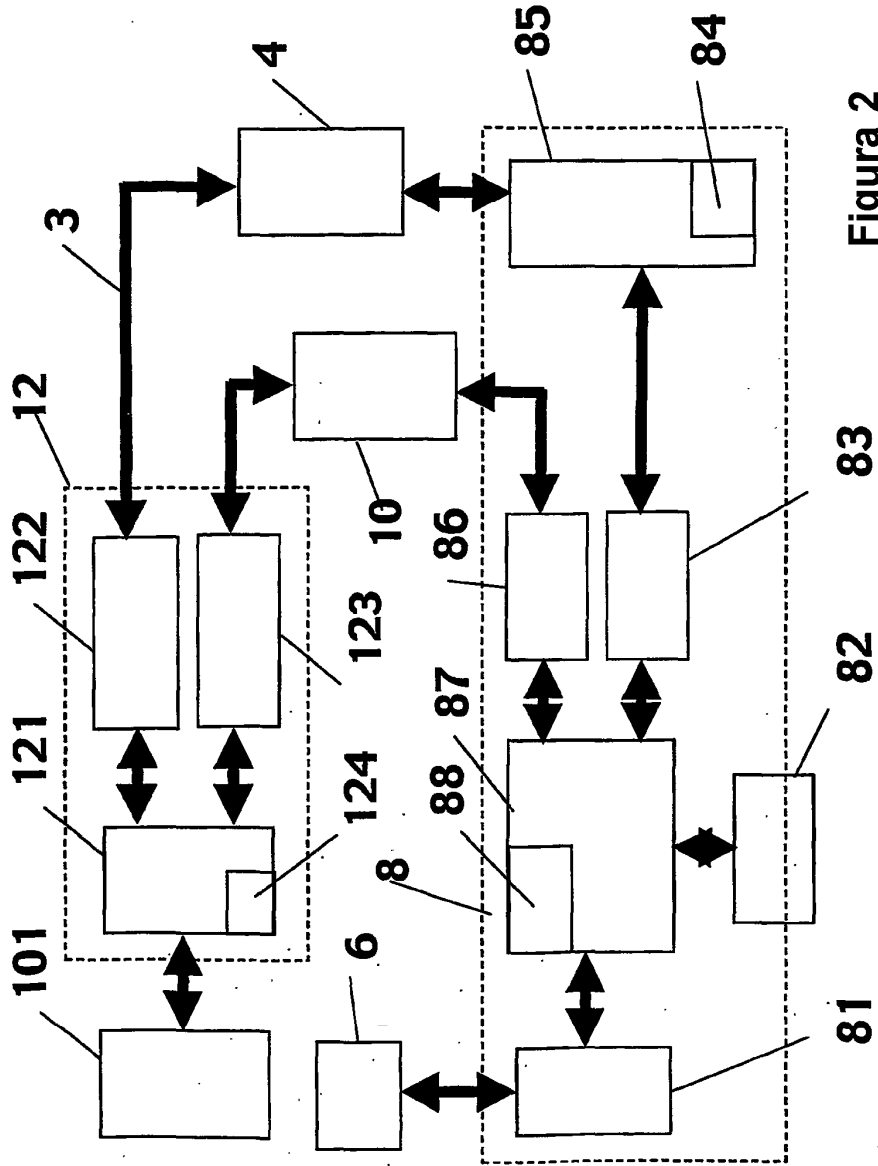


Figura 2

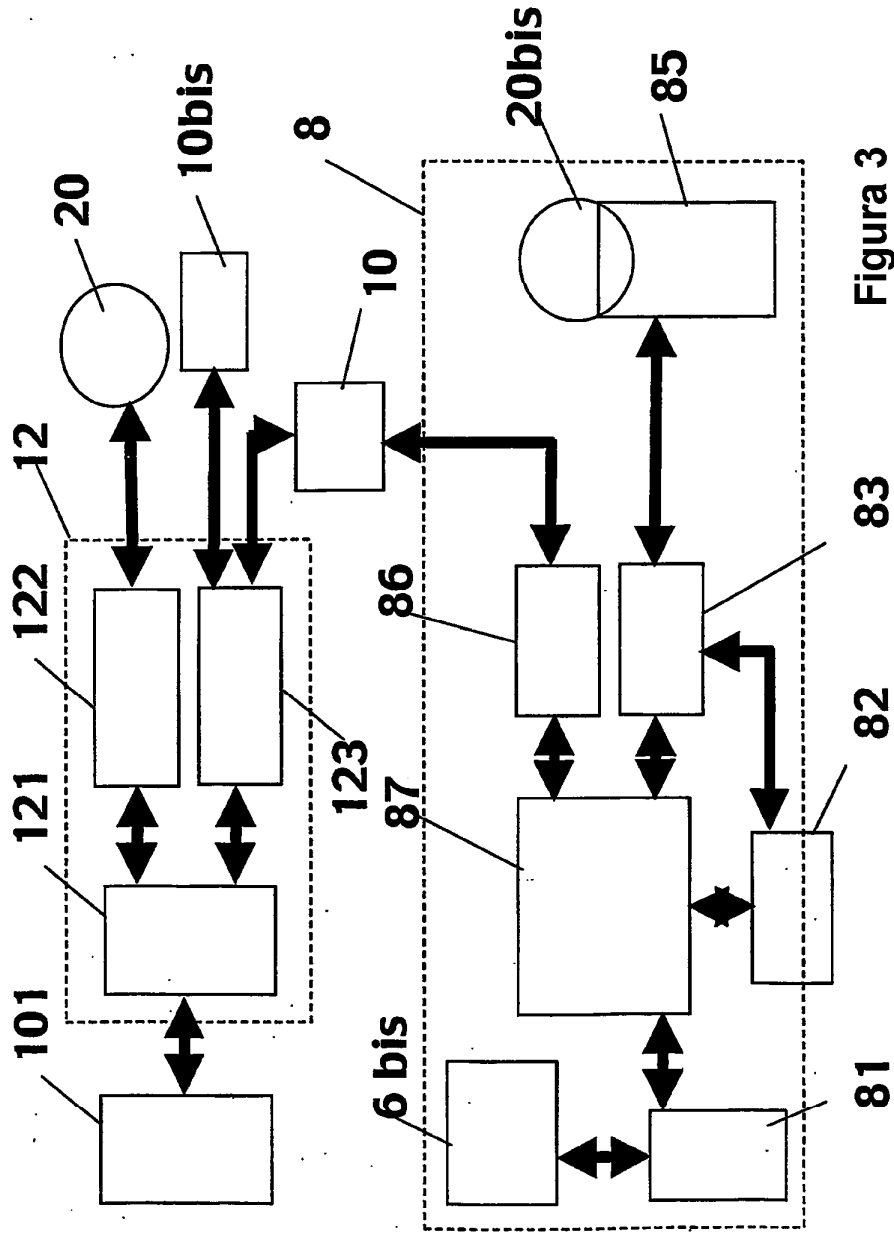


Figura 3