

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 628 427**

51 Int. Cl.:

H04N 19/176 (2014.01)

H04N 19/467 (2014.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **23.01.2012** **E 12152042 (3)**

97 Fecha y número de publicación de la concesión europea: **12.04.2017** **EP 2485488**

54 Título: **Decodificador multimedia y método de decodificación que permite el rastreo del decodificador multimedia**

30 Prioridad:

02.02.2011 US 201161438654 P

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

02.08.2017

73 Titular/es:

**NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH**

72 Inventor/es:

**LE BUHAN, CORINNE y
BODO, YANN**

74 Agente/Representante:

TOMAS GIL, Tesifonte Enrique

ES 2 628 427 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

Decodificador multimedia y método de decodificación que permite el rastreo del decodificador multimedia.

5 Campo de la invención

[0001] Esta invención concierne el campo de la supervisión y del rastreo de un trabajo multimedia hasta una fuente de distribución para identificar editores o distribuidores de medios que sean ilegales o indeseables.

10 Antecedentes técnicos

[0002] El desarrollo de las redes digitales combinado con el del procesamiento multimedia durante las dos últimas décadas ha dado como resultado que se comparta cada vez más contenido digital. Esto plantea una serie de cuestiones específicas tanto a los proveedores de contenido comercial que pierden una fuente significativa de ingresos cuando los consumidores comparten contenido libremente o lo publican en Internet, como a los usuarios finales que desean limitar el acceso a su contenido personal a su red privada de amigos y familiares por cuestiones de privacidad.

[0003] La protección del contenido multimedia contra el acceso, redistribución o uso no autorizado del mismo se ha llevado a cabo durante mucho tiempo mediante la encriptación de los paquetes de distribución de contenido. Sin embargo, en última instancia, el contenido tiene que estar a salvo para que pueda acceder a él el usuario final, por lo que la protección del contenido contra el acceso, redistribución o uso no autorizado del mismo es un problema que fundamentalmente está mal planteado. Sin embargo, en la práctica, gracias a las limitaciones que impone la realidad en cuanto al diseño de un sistema de *hackeo* perfecto a un coste y en un tiempo razonables, todavía es posible abordar este problema en el mundo real diseñando sistemas pragmáticos de protección de contenido basados en una serialización inteligente de barreras de seguridad que deben adaptarse regularmente a las amenazas de *hackeo*, sujetas a las capacidades técnicas de la ingeniería inversa que evolucionan rápidamente y a la accesibilidad de costes. Ejemplos de tales barreras son:

- diseños de *hardware* resistentes a la manipulación, como por ejemplo las tarjetas inteligentes y conjuntos de chips de decodificación segura que típicamente se serializan en un diseño estructural seguro de STB (decodificador);
- diseños de *software* resistentes a la manipulación, como por ejemplo los que se basan en la configuración en cascada en las claves, en la criptografía de caja blanca y en la diversidad de aplicación que típicamente se combinan en un diseño estructural de *software* ofuscado.

[0004] En aplicaciones de difusión, los sistemas iniciales se diseñaron para proteger cuidadosamente las claves de gestión de derechos y, más directamente, las claves de contenido. Sin embargo, al fin y al cabo el contenido todavía se encuentra a salvo, así que el siguiente desafío de la ingeniería de seguridad reside en el diseño de esquemas de protección de contenido lo más cercanos posible a la fase de decodificación del contenido, o bien en la aplicación de chip de silicio decodificador en el conjunto de chips de un dispositivo del consumidor (como por ejemplo un *Set-Top-Box* o decodificador de televisión STB, una televisión, una tableta o un dispositivo de mano) o en la aplicación de un decodificador de *software* en un reproductor multimedia para dispositivos móviles o PC.

[0005] Como un término medio entre la complejidad del diseño de protección del contenido y la eficiencia de seguridad del contenido de principio a fin puede no ser ya económicamente viable, el rastreo del contenido suscita un interés particular. Con este fin, el contenido se marca de forma individual para posibilitar el rastreo desde su fuente de origen y, por consiguiente, permitir repuestas legales o técnicas dirigidas a esa fuente de manera específica.

[0006] El rastreo del contenido también se puede usar en combinación con mecanismos convencionales de protección de contenido. Es de importancia particular en la estructura de aplicaciones de *software* en dispositivos abiertos tales como ordenadores personales que facilitan intrínsecamente la ingeniería inversa del diseño de seguridad, los algoritmos y las claves.

[0007] Se ha propuesto una serie de soluciones para tratar el problema del rastreo de contenido, como insertar una marca de agua en el contenido para incorporar una señal invisible que lleve información de identificación en la señal de audio, de imagen o de vídeo. El principal inconveniente de esas soluciones de rastreo es que en una aplicación de difusión convencional, estas requieren o bien reprocesar el contenido, por ejemplo, su extraprocésamiento, su almacenamiento o su ancho de banda cuando este está en el lado del distribuidor, antes de su difusión con una transmisión de canales importantes, o bien implementar el procesamiento de una señal compleja de manera alternativa cuando el contenido se encuentra en el lado del receptor que se tiene que diseñar otra vez de forma cuidadosa contra el pirateo del receptor.

[0008] Los métodos para insertar una marca de agua en el contenido multimedia se conocen en el estado de la

técnica. El propietario del contenido añade la marca de agua a su contenido y lo distribuye. En algunos métodos, el propietario de un contenido que más tarde encuentra una copia del contenido que ha distribuido es capaz de identificar su marca de agua y de forma simple llegar a la conclusión de que esa copia en concreto es una copia pirata, sin ser capaz de localizar de dónde ha venido. En otros métodos, la marca de agua puede permitir que se identifique la fuente del contenido que se ha distribuido ilegalmente. Según tales métodos, el propietario del contenido emite contenido multimedia, con una marca de agua particular, a un receptor en concreto. Si el propietario más tarde recupera el contenido a partir de una fuente diferente a la del receptor, puede extraer la marca de agua identificando de esta forma al receptor. Entonces este llega a la conclusión de que el receptor ha retransmitido el contenido ilegalmente. La marca de agua se añade al contenido en el momento de la codificación. Uno de los requisitos de la marca de agua es que esta no debería reducir la calidad de la señal que contiene dicha marca. Otro requisito, aunque entra en conflicto con el primer requisito, es que la marca de agua debería ser lo suficientemente resistente como para que una tercera persona no pueda eliminarla con facilidad. Como se sabe, un algoritmo de codificación puede incluir una operación de transformación de dominio de frecuencia, como una transformada de coseno discreta directa. El algoritmo de codificación también puede incluir un proceso de cuantificación. En el lado de decodificación, se conoce que el algoritmo de decodificación incluye un proceso de descuantificación, una operación de transformación de dominio de frecuencia, como una transformada de coseno discreta inversa, que coincide o que se aproxima lo máximo posible a la operación de transformación de dominio de frecuencia en el algoritmo codificador (la transformada de coseno discreta directa). El algoritmo de decodificación puede comprender además pasos de postprocesamiento como la filtración y el sobremuestreo.

Resumen de la invención

[0009] La presente descripción se refiere a un dispositivo, un sistema y un método para rastrear al menos un decodificador de flujo de vídeo, donde el decodificador se configura para insertar al menos una variante de un algoritmo de descompresión de imágenes estándar de manera que la aproximación de la imagen descomprimida resultante varía según el decodificador en concreto que se utiliza.

[0010] Los inconvenientes de las soluciones convencionales de rastreo se superan mediante un método para decodificar vídeo, esto es, el método que se utiliza en un decodificador, el método que produce una salida de reconstrucción de vídeo que presenta unas características que permiten que se rastree un identificador único asociado al decodificador, donde el decodificador comprende medios para decodificar vídeo comprimido según un algoritmo de compresión de imágenes, donde el método comprende:

la descompresión del vídeo comprimido según un algoritmo de descompresión de imágenes de rastreo, donde el identificador único parametriza el algoritmo de descompresión de imágenes de rastreo para proporcionar una variante de un algoritmo de descompresión de imágenes que coincide con el algoritmo de compresión de imágenes y dicha coincidencia se lleva a cabo según un esquema de compresión de imágenes estándar.

[0011] Según otro aspecto de la presente descripción, se proporciona un decodificador para decodificar un vídeo para producir una salida de reconstrucción de vídeo que permite el rastreo del decodificador; el decodificador cuenta con un módulo de descompresión configurado para descomprimir vídeo que se ha comprimido según un algoritmo de compresión de imágenes y dicha descompresión se ha hecho según un algoritmo de descompresión de imágenes; el decodificador se caracteriza por:

el algoritmo de descompresión de imágenes es una variante de un algoritmo de descompresión de imágenes que coincide con el algoritmo de compresión de imágenes y dicha coincidencia se lleva a cabo según un esquema de compresión de imágenes estándar; el algoritmo de descompresión de imágenes de rastreo se encuentra parametrizado por un identificador único asociado al decodificador; el rastreo es posible gracias a la salida de reconstrucción de vídeo que presenta características que permiten que se halle el identificador único.

[0012] Otro objeto más de la descripción es un sistema para rastrear e identificar de manera única un decodificador de flujo de vídeo que comprende una pluralidad de decodificadores y al menos un codificador de flujo de vídeo configurado para la difusión a dicha pluralidad de decodificadores de flujos de vídeo comprimidos mediante un algoritmo de compresión de imágenes estándar que presenta limitaciones de desvío intrínseco que dan como resultado que la salida del vídeo comprimido sea ligeramente variable, donde el sistema se caracteriza por el hecho de que: se configura al menos un decodificador para procesar el flujo de vídeo de la difusión usando al menos una variante del algoritmo de descompresión de imágenes cuyo desvío se define en función de un identificador de dicho decodificador, donde el vídeo descomprimido que emite el decodificador comprende una pluralidad de imágenes ligeras y únicamente modificadas según el algoritmo de descompresión que modifica el identificador del decodificador.

[0013] Según otro aspecto más de la presente descripción, se ha proporcionado un sistema que comprende una pluralidad de decodificadores para decodificar el vídeo comprimido según un algoritmo de compresión de imágenes para producir una pluralidad de salidas de reconstrucción de vídeo que presentan características que permiten que se rastree al menos un identificador único asociado a al menos un decodificador, donde cada decodificador está configurado para llevar a cabo el método proporcionado por un aspecto de la invención.

[0014] La solución propuesta en el presente documento se basa en un método diferente para aprovechar directamente las limitaciones físicas de las aplicaciones del decodificador de contenido para desencadenar la decodificación de contenido diversificado y rastreable dentro del propio proceso de decodificación.

[0015] La presente invención pretende superar de este modo los inconvenientes de los métodos convencionales de rastreo de contenido que requieren un reprocesamiento del contenido, como por ejemplo su extraprocésamiento, su almacenamiento o su ancho de banda en el lado del distribuidor o aplicar de forma alternativa un procesamiento de señal compleja en el lado del receptor que debe protegerse contra los ataques de los *hackers* antes de su difusión mediante la transmisión de un canal de gran importancia. La presente invención es tal y como la definen las reivindicaciones.

Breve descripción de los dibujos

[0016] La invención se entenderá mejor con la siguiente descripción detallada, que se refiere a las figuras adjuntas que se proporcionan como ejemplos no limitativos.

La Figura 1 muestra el diagrama de bloques de un algoritmo de procesamiento de imágenes convencional, que incluye la compresión y la descompresión, que implementa un codificador de vídeo (ENC) y su correspondiente decodificador de vídeo (DEC).

La Figura 2 muestra decodificadores diferentes (DEC1, DEC2, DEC3) que controlan una combinación de los pasos de la transformada de coseno discreta inversa originales y modificados (IDCTO, IDCTV) como parte de una variante de una operación de transformada de coseno discreta inversa que da como resultado imágenes descomprimidas individuales cuya salida se encuentra ligeramente modificada (IMG0000, IMG0001, IMG0010).

La Figura 3 muestra la aplicación de una variante de la transformada de coseno discreta inversa (IDCTV) específicamente en el decodificador (DEC1).

La Figura 4 muestra la aplicación de una variante de la transformada de coseno discreta directa (FDCTV) en el codificador (ENC) y la aplicación de la operación de transformada de coseno discreta inversa original (IDCTO), así como el codificador que se corresponde con la variante de la transformada de coseno discreta inversa (IDCTO) en los decodificadores capaces de rastreo (DEC2, DEC3), mientras que los decodificadores que no son capaces de rastreo (DEC) solo aplican la operación de transformada de coseno discreta inversa original (IDCTO).

Descripción detallada de la invención

[0017] La presente invención se refiere a un sistema y un método para identificar de manera única al decodificador de un flujo de vídeo donde el decodificador comprende un módulo de descompresión que aplica al menos una variante de un algoritmo de descompresión de imágenes estándar y donde la aproximación de la imagen descomprimida resultante varía según el identificador del decodificador. El algoritmo de descompresión de imágenes que se emplea de esta manera se conoce como algoritmo de descompresión de imágenes de rastreo.

[0018] En una forma de realización preferida, la solución propuesta aprovecha la limitación fundamental de cualquier esquema de compresión de imágenes con pérdida de datos, es decir, la imprecisión del contenido tal como la transformación de dominio de frecuencia IDCT (transformada de coseno directa discreta inversa) que se usa en un número de operaciones de decodificación como especifican los estándares de compresión de vídeo principales, para derivar una aproximación única de la salida de reconstrucción de vídeo que caracteriza la aplicación del decodificador.

[0019] De hecho, la IDCT en la decodificación sería la operación inversa perfecta de la FDCT (transformada de coseno discreta directa) en la fase de codificación si sus resultados pudieran computarizarse como valores de coma flotante de precisión infinita, lo que no es posible con las actuales tecnologías de procesamiento. Por lo tanto, las aplicaciones más populares de la FDCT y de la IDCT las aproximan mediante una secuencia de operaciones de número entero. En las publicaciones previas se han propuesto varias aproximaciones de número entero que darán como resultado una imagen reconstruida de forma ligeramente diferente tras la descompresión. La imprecisión resultante se llama discordancia IDCT o desvío IDCT y ha sido el sujeto de múltiples optimizaciones realizadas por expertos en compresión de vídeo para asegurarse de que no se desvía hasta llegar a tener un impacto visual en el vídeo descomprimido. De hecho, aplicaciones diferentes del IDCT decodificador típicamente darán como resultado imágenes decodificadas diferentes de la misma fuente de flujo de vídeo de difusión, aunque los no expertos no siempre percibirán la diferencia.

[0020] En las especificaciones previas de estándares de compresión de vídeo tales como MPEG-1 y MPEG-2, la elección de los algoritmos de FDCT y de IDCT le corresponde a los implementadores. Al elegir una transformada utilizada en pocas ocasiones, es posible obtener una salida única de reconstrucción de vídeo que difiera de la de las aplicaciones de los algoritmos más populares. La invención consiste en usar esta limitación de desvío intrínseco para definir aplicaciones de la diversidad del decodificador con un impacto muy secundario en el diseño del decodificador, que puede ser en forma de chip de silicio o de *software*: cada aplicación diversificada aplica de forma sencilla un algoritmo de redondeo IDCT y da como resultado una salida diferente de reconstrucción de vídeo que permite rastrear el vídeo hasta su decodificador de origen.

[0021] En los estándares de compresión de vídeo más recientes como H.264, tal como se representa en la Figura 1, se han especificado completamente las aplicaciones de transformación de dominio de frecuencia (transformada de coseno discreta directa o FDCTO, y transformada de coseno discreta inversa o IDCTO) para evitar resultados de descompresión que se desvíen cuando se usan algoritmos no coincidentes en la codificación y en la decodificación. Todavía es posible desviarse de la aplicación estándar de ciertas aplicaciones, siempre y cuando la representación de flujo de *bits* de la salida del codificador comprimido (CV) siga en conformidad con la especificación estándar.

[0022] En aquellos estándares o como mejoras en las aplicaciones relacionadas, también se han propuesto operaciones adicionales tales como la cuantificación mejorada (Q) en la codificación y la descuantificación coincidente (DQ) en la fase de decodificación teniendo en cuenta las propiedades del sistema visual humano, o la postfiltración de las imágenes reconstruidas en la fase de decodificación para mejorar su cualidad subjetiva, por ejemplo, aplicando un *deblocking filter* (DBF) y un *deringing filter* (DRF) a las imágenes de salida de la transformada inversa, también en el nivel de expansión (OS) de las imágenes en color del submuestreo (planos U y V de un vídeo YUV) de nuevo a resolución completa (del submuestreo de 420 para la compresión a 444 para la visualización, por ejemplo). Por lo tanto, además de la personalización de la transformada inversa (IDCTO) o como sustitución de la misma, la descuantificación (DQ) o cualquiera de los pasos de postprocesamiento (PP) que incluyen la postfiltración (DBF, DRF) o el algoritmo de sobremuestreo de la imagen en color (OS) también se puede adaptar para producir una reconstrucción de la imagen diferente de la de la cuantificación convencional y popular, de la postfiltración o de los algoritmos del sobremuestreo de la imagen en color.

[0023] Siguiendo con lo anterior, cabe observar que, cuando hablamos de los estándares de compresión de vídeo, incluimos tanto el algoritmo de codificación, que realiza un codificador, como el algoritmo de decodificación, que realiza el decodificador. Estos dos algoritmos también se pueden llamar respectivamente algoritmos de compresión y de descompresión. De ello se deduce que un algoritmo de codificación puede incluir operaciones o procesos tales como una transformación de dominio de frecuencia (por ejemplo, una transformada de coseno discreta directa) y un paso de cuantificación. Asimismo, un algoritmo de decodificación puede incluir pasos u operaciones tales como un paso de descuantificación que coincida con el paso de cuantificación, una transformación de dominio de frecuencia que coincida con la transformación de dominio de frecuencia del algoritmo codificador y un paso de postprocesamiento, que incluye la filtración (como un *deblocking filter* o un *deringing filter*) y el sobremuestreo de visualización. A partir de lo anterior, resulta aparente, pero merece la pena mencionarlo otra vez, que el uso de la palabra "coincidir" en el caso de la descuantificación significa la inversión del paso de cuantificación, y el uso de la palabra "coincidir" en el caso de la transformada de coseno discreta inversa significa una aproximación lo más próxima posible a la inversión de la transformada de coseno discreta directa. Las especificaciones sobre cómo debería ser esta proximidad se dan en los estándares de compresión de vídeo.

[0024] Una característica deseable de la invención es rastrear el contenido que se filtra hasta su decodificador individual o su fuente de reproducción. Con este fin, en particular, en aplicaciones de difusión donde millones de receptores pueden recibir el contenido de manera conjunta y procesarlo, se necesitaría una diversidad de aplicaciones del orden de millones que plantean cuestiones importantes sobre la utilización en un ecosistema de difusión. Por lo tanto, en una forma de realización preferida, se aplican tanto un algoritmo estándar (IDCTO) como una variante de la desviación del algoritmo (IDCTV) en el decodificador (DEC1, DEC2, DEC3) y la elección de aplicar el original (IDCTO) o la variante (IDCTV) la determina a nivel de secuencia de bloque, de píxel o de vídeo el propio decodificador (DEC1, DEC2, DEC3), en función de un identificador único (ID) que permite rastrearlo, por ejemplo, pero que no se limita a un número de serie, a una clave única de decodificador, a un anfitrión que caracteriza información sobre los parámetros o a un identificador de certificado.

[0025] Esto se ilustra, por ejemplo, en la Figura 2, donde se representan tres decodificadores (DEC1, DEC2, DEC3) y cada uno de ellos se aplica tanto a un algoritmo IDCT original u operación (IDCTO) como a una variante del algoritmo IDCT (IDCTV). Para generar una imagen modificada de forma ligera y única (IMG0000, IMG0001, IMG0010), cada decodificador (DEC1, DEC2, DEC3) selecciona una opción en cuanto al algoritmo (IDCTV, IDCTO) basada en su identificador (ID). De esta forma, el algoritmo de descompresión completo, que se conoce como el algoritmo de descompresión de imágenes de rastreo (DCAV1, DCAV2, DCAV3), puede comprender pasos de la operación IDCT original y de la operación IDCT variante, dependiendo del identificador único asociado al decodificador. Por ejemplo, el decodificador 0000 siempre puede aplicar la variante del algoritmo

(IDCTV), mientras que el decodificador 0001 cambia al algoritmo original (IDCTO) en bloques de número par en una imagen dada, como se representa en la Figura 2; el decodificador 0010 cambia al algoritmo original (IDCTO) en bloques de número impar en una imagen dada; mientras que un decodificador sin rastreo 0011 (identificador reservado para decodificadores heredados en este ejemplo - no se muestra en la Figura 2) aplica el algoritmo original (IDCTO) en todos los bloques pares e impares, etc., de manera que las modificaciones de la imágenes resultantes discriminan entre estos. Mientras que la Figura 2 ilustra específicamente la diferenciación de rastreo en el caso de a aplicación de la variante del algoritmo IDCT, es posible, por supuesto, aplicar el mismo principio a una variante de la descuantificación (DQ) o de los algoritmos de postprocesamiento (DBF, DRF, OS) o incluso una combinación de las aplicaciones de variantes, posiblemente también a diferentes niveles en el proceso de decodificación en general (filas de macrobloques, decodificación de bloques, compensación de movimiento, etc.).

[0026] Además, el proceso de rastreo del decodificador individual lo puede ejecutar sistemáticamente cada decodificador pasiva y autónomamente o lo pueden desencadenar de manera alternativa los comandos de control de seguridad que se transmiten desde un centro de control a cada decodificador con el contenido o de forma separada, por ejemplo, mediante Mensajes de Gestión de Derechos (EMM) enviados por un Sistema de Acceso Condicional (SAC). Esto permite el diseño y la utilización de mecanismos como medida contra la piratería diversificada activando la característica de rastreo solo en determinadas circunstancias, desencadenada por la transmisión de un mensaje de control específico a los decodificadores. En una posible aplicación, este tipo de mensajes se pueden dirigir específicamente a un subconjunto de decodificadores en el campo de utilización, como dictan las necesidades de controlar la piratería al compartir contenido. Para optimizar las necesidades de este tipo de mensajes, especialmente en un entorno de difusión, también es posible dirigir decodificadores en grupos predefinidos, por ejemplo, para rastrear la liberación de un determinado decodificador de software de manera global en lugar de individualmente.

[0027] En una forma de realización, como se muestra en la Figura 3, solo la implementación del decodificador (DEC1) se ve modificada por una o varias variantes del algoritmo (IDCTV), mientras que el codificador todavía aplica los algoritmos de codificación convencionales (FDCTO) que se han optimizado para una mejor calidad de la reconstrucción de vídeo a una velocidad de transmisión dada. En ese caso, los decodificadores que soportan las características de rastreo emitirán vídeos reconstruidos alterados ligeramente mientras que los decodificadores estándares (DEC) disponibles en el mercado todavía emiten vídeos completamente conformes (IMG) de mejor calidad a los ojos de los expertos. Para superar este inconveniente, en una forma de realización como se ilustra en la Figura 4, la aplicación de la codificación (ENAV) también se modifica para reemplazar el algoritmo convencional de FDCT, IDCT o cuantificación por uno específico que dará como un resultado un efecto de desvío de las aplicaciones de decodificadores estándares, mientras que los algoritmos inversos coincidentes se implementan específicamente en los decodificadores capaces de rastreo (DEC2, DEC3), de modo que los vídeos reconstruidos rastreables (IMG001, IMG0010) presentan una mejor calidad que las salidas de los decodificadores (DEC) heredados no coincidentes (IMGMOD). Preferiblemente, los decodificadores de rastreo implementan tanto los algoritmos convencionales como los específicos y los aplican de forma selectiva a nivel de bloque, imagen o secuencia de vídeo para mantener cierto desvío en el vídeo reconstruido emitido que caracteriza de forma única el decodificador (DEC2, DEC3).

REIVINDICACIONES

- 5 1. Decodificador (DEC1, DEC2, DEC3) para decodificar vídeo para producir una salida de reconstrucción de vídeo (IMG0000, IMG0001, IMG0010);
 el decodificador (DEC1, DEC2, DEC3) comprende un módulo de descompresión configurado para descomprimir vídeo (CV) que se ha comprimido según un algoritmo de compresión de imágenes (ENAO, ENAV) y dicha descompresión se realiza según un algoritmo de descompresión de imágenes;
 el decodificador (DEC1, DEC2, DEC3) **se caracteriza por el hecho de que:**
- 10 el algoritmo de descompresión de imágenes es un algoritmo de descompresión de imágenes de rastreo (DCAV1, DCAV2, DCAV3) **caracterizado por el hecho de que** produce una aproximación de la imagen descomprimida que varía según un identificador único asociado al decodificador;
 el algoritmo de descompresión de imágenes incluye un número de operaciones de decodificación, al menos una de las operaciones de decodificación la pueden llevar a cabo cualquiera de una pluralidad de diferentes versiones de al menos un subalgoritmo, el decodificador incluye una pluralidad de las diferentes versiones del subalgoritmo y está configurado para conmutar entre al menos dos de las versiones diferentes del subalgoritmo dependiendo del identificador único, donde dicha conmutación se determina a nivel de bloque, de píxel o de secuencia de vídeo;
- 15 dicho decodificador (DEC1, DEC2, DEC3) siendo rastreable así debido a la salida de reconstrucción de vídeo (IMG0000, IMG0001, IMG0010) variable según el identificador único.
- 20 2. Decodificador (DEC1, DEC2, DEC3) según la reivindicación 1, donde una pluralidad de las operaciones de decodificación la puede realizar cualquiera de una pluralidad de diferentes versiones de una pluralidad de diferentes subalgoritmos para las respectivas operaciones de decodificación, el decodificador incluye una pluralidad de diferentes versiones de los subalgoritmos para las respectivas operaciones de decodificación y está configurado para cambiar entre al menos dos de las diferentes versiones de una combinación de subalgoritmos de las diferentes operaciones de decodificación.
- 25 3. Decodificador (DEC1, DEC2, DEC3) según la reivindicación 2, donde el decodificador también está configurado de manera que dicha conmutación se determina en una fila a nivel de macrobloque o a nivel de compensación de movimiento.
- 30 4. Decodificador (DEC1, DEC2, DEC3) según la reivindicación 1, donde una de las operaciones de decodificación es una función de transformación de dominio de frecuencia y el módulo de descompresión incluye:
- 35 un primer módulo decodificador de transformación de dominio de frecuencia (IDCTV, IDCTO);
 al menos un segundo módulo decodificador de transformación de dominio de frecuencia (IDCTO, IDCTV), diferente del primer módulo decodificador de transformación de dominio de frecuencia (IDCTO, IDCTV);
 un conmutador para la conmutación entre el primer módulo decodificador de transformación de dominio de frecuencia (IDCTV, IDCTO) y el segundo módulo decodificador de transformación de dominio de frecuencia (IDCTO, IDCTV) de manera que el primer y el segundo módulo decodificador de transformación de dominio de frecuencia procesan partes diferentes del vídeo comprimido (CV) y
 40 medios para activar el conmutador, cuyo accionamiento se basa en un valor que forma al menos parte del identificador único (ID).
- 45 5. Decodificador (DEC1, DEC2, DEC3) según la reivindicación 4, donde el decodificador (DEC1, DEC2, DEC3) está configurado para emplear los medios para activar el conmutador dependiendo de la recepción de un agente desencadenante predeterminado.
- 50 6. Decodificador (DEC1, DEC2, DEC3) según la reivindicación 5, donde el decodificador (DEC1, DEC2, DEC3) está configurado para cooperar con un módulo de seguridad, donde el módulo de seguridad está configurado para emitir el agente desencadenante tras la recepción de un mensaje de seguridad predeterminado desde un centro de control.
- 55 7. Método para decodificar vídeos, donde el método se utiliza en un decodificador (DEC1, DEC2, DEC3), donde el método produce una salida de reconstrucción de vídeo (IMG0000, IMG0001, IMG0010) que presenta características que permiten rastrear un identificador único (ID) asociado al decodificador (DEC1, DEC2, DEC3), donde el decodificador (DEC1, DEC2, DEC3) comprende medios para decodificar el vídeo comprimido (CV) según un algoritmo de compresión de imagen (ENA), donde el método comprende:
- 60 descomprimir el vídeo comprimido (CV) según un algoritmo de descompresión de imágenes de rastreo (DCAV1, DCAV2, DCAV3) para producir una aproximación de la imagen descomprimida que varía según un identificador único asociado al decodificador, donde el algoritmo de descompresión incluye un número de
- 65

operaciones decodificadoras y al menos una de las operaciones decodificadoras la puede llevar a cabo cualquiera de una pluralidad de diferentes versiones de al menos un subalgoritmo; y conmutar entre al menos dos de las diferentes versiones del subalgoritmo dependiendo del identificador único, donde dicha conmutación está determinada a nivel de bloque, de píxel o de secuencia de vídeo.

5

8. Método según la reivindicación 7, donde una pluralidad de operaciones de decodificación la puede llevar a cabo cualquiera de una pluralidad de diferentes versiones de una pluralidad de diferentes subalgoritmos para las respectivas operaciones de decodificación, donde la conmutación implica una combinación de diferentes versiones de subalgoritmos de diferentes operaciones de decodificación.

10

9. Método según la reivindicación 8, donde dicha conmutación se realiza en una fila a nivel de macrobloque o a nivel de compensación de movimiento.

15

10. Método según la reivindicación 7, donde el algoritmo de compresión de imágenes (ENAO, ENAV) comprende una operación codificadora de transformación de dominio de frecuencia (FDCTO, FDCTV) y el algoritmo de descompresión de imágenes de rastreo (DCAV1, DCAV2, DCAV3) comprende una operación decodificadora de transformación de dominio de frecuencia, donde la operación codificadora de transformación de dominio de frecuencia (FDCTO, FDCTV) y la operación decodificadora de transformación de dominio de frecuencia (IDCTV, IDCTO) son transformadas de coseno discretas y la operación decodificadora de transformación de dominio de frecuencia comprende:

20

evaluar una primera parte del identificador único (ID);
procesar una primera parte del vídeo comprimido (CV) según un primer paso decodificador de transformación de dominio de frecuencia (IDCTO, IDCTV);

25

procesar otra parte del vídeo comprimido (CV) o bien según el primer paso decodificador de transformación de dominio de frecuencia (IDCTO, IDCTV) o según un segundo paso decodificador de transformación de dominio de frecuencia (IDCTV, IDCTO), diferente del primer paso de transformación de dominio de frecuencia, dependiendo del valor de la parte evaluada en este momento del identificador único (ID); y

30

evaluar otra parte del identificador único (ID) y repetir el paso de procesamiento inmediatamente anterior hasta que todas las partes del identificador único (ID) se hayan evaluado.

11. Método según la reivindicación 10, donde la evaluación de la otra parte del identificador único (ID) se realiza dependiendo del vídeo comprimido (CV) píxel a píxel, bloque a bloque o por secuencia de vídeo.

35

12. Método según cualquiera de las reivindicaciones 7,10 u 11, donde el identificador único (ID) es un identificador seleccionado del grupo que comprende un número de serie, una clave única de decodificador, un identificador de la versión de *software* del decodificador, un identificador de certificado o un dato que caracteriza un huésped con el que el decodificador está configurado para cooperar o un dato que caracteriza un módulo de seguridad con el que el decodificador está configurado para cooperar.

40

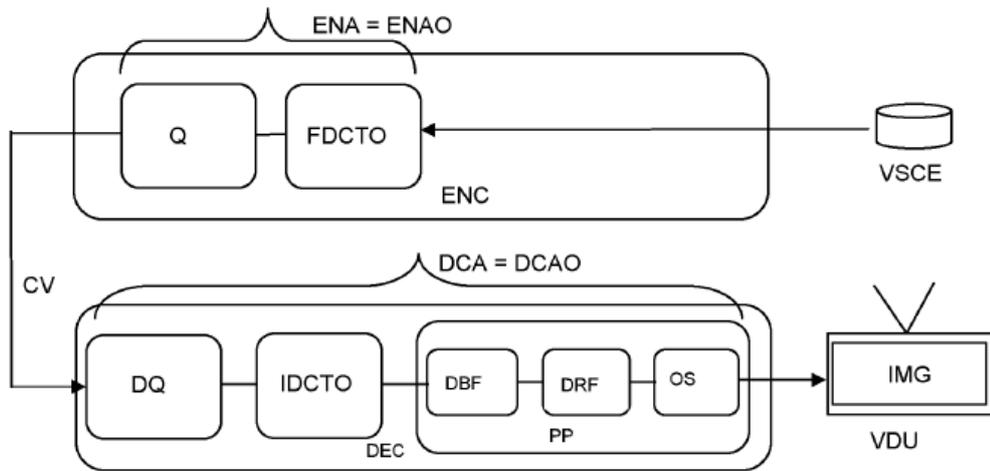


Figura 1 - Estado de la técnica

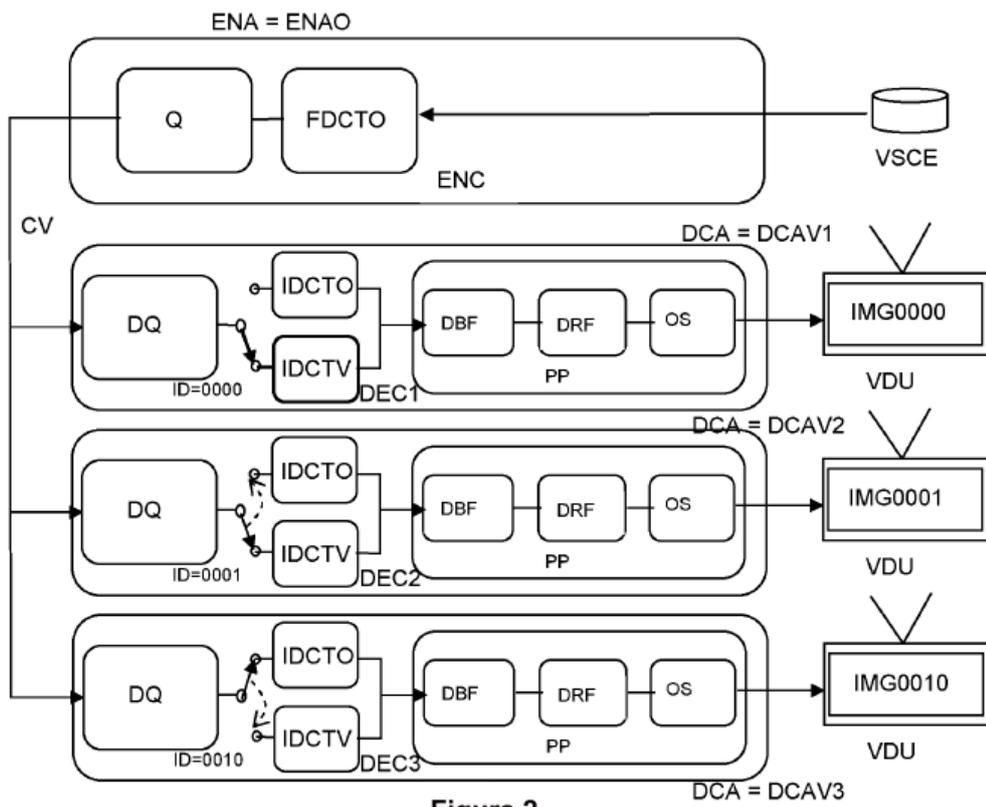


Figura 2

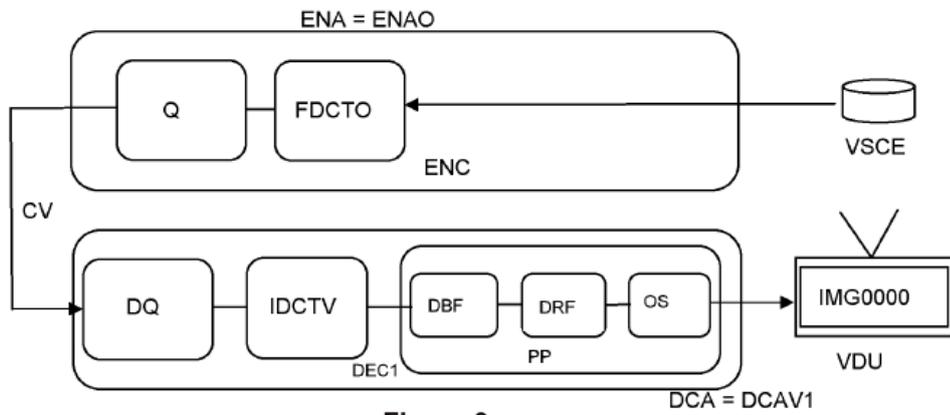


Figura 3

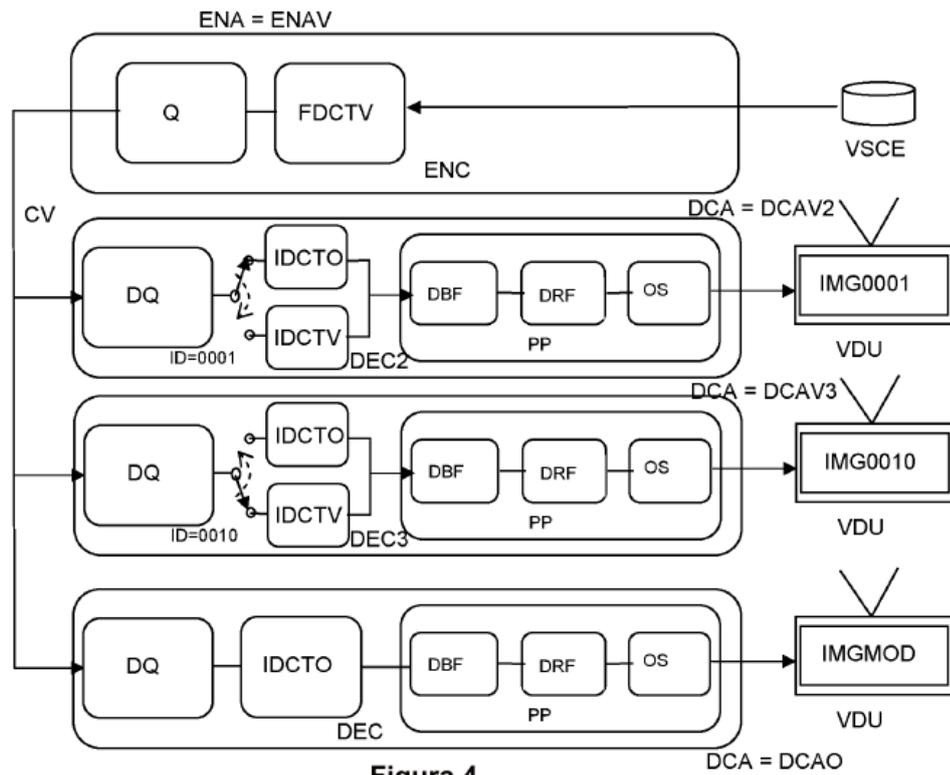


Figura 4