(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 583 927**

(51) Int. CI.:

G06T 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.12.2007 E 07856751 (8)**

(97) Fecha y número de publicación de la concesión europea: **04.05.2016 EP 2122569**

(54) Título: **Método de marcado de un documento digital**

(30) Prioridad:

14.12.2006 ES 200603214
13.04.2007 DE 102007017525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.09.2016

(73) Titular/es:

TREDESS 2010, S.L. (100.0%)
Volta do Castro s/n
15706 Santiago de Compostela, A Coruña, ES

(72) Inventor/es:

FERNÁNDEZ CARNERO, JOSÉ LUIS;
REY REQUEJO, SANTIAGO;
PÉREZ GONZALES, FERNANDO;
ROCAFORT CIMADEVILA, JORGE;
COMESAÑA ALFARO, PEDRO;
PÉREZ FREIRE, LUIS;
MOSQUERA NARTALLO, CARLOS y
DOMÍNGUEZ CONDE, GABRIEL

DESCRIPCIÓN

Método de marcado de un documento digital

La presente invención se refiere a un método según el preámbulo de la reivindicación 1 y a un método según el preámbulo de la reivindicación 8.

Antecedentes de la invención

En un sistema de video supervisión un elemento fundamental es la cámara. Actualmente, las cámaras analógicas son sustituidas por cámaras de seguridad digitales. estas, en muchos casos, están diseñadas para utilizar las redes de comunicaciones digitales existentes, lo que conlleva una reducción de los costes de instalación. Ese factor es el causante del rápido aumento del número de ese tipo de sistemas digitales. Otros dispositivos comunes en los sistemas de video supervisión digitales son los servidores de video. Su función principal es digitalizar la señal de vídeo analógica. Otra característica habitual es que realizan las funciones de interfaz entre las cámaras analógicas y las redes de comunicaciones digitales. Esto permite pasar de forma gradual de un sistema video supervisión analógico a uno digital.

Los servidores centrales son los otros dispositivos que componen, con los presentados anteriormente, el conjunto de elementos básicos de un sistema de video supervisión digital. Su cometido esencial es la configuración del sistema y el control general de las cámaras digitales y los servidores de video. Además, es muy común que se archiven en ellos las secuencias de vídeo obtenidas.

Estos nuevos sistemas digitales de video supervisión aparecen fruto del enorme avance en las tecnologías de la información en las últimas décadas. Paralelamente a su aparición surgen numerosas aplicaciones para la edición de imágenes fijas y vídeo. Con ellas no es complicado conseguir alterar una imagen, de tal forma que no se pueda discernir entre una original y una falsa. Además, el número de potenciales manipuladores ha aumentado de manera enorme, ya que debido a Internet esas herramientas de edición están al alcance de un gran número de usuarios. Una consecuencia de lo anterior es que, desde el punto de vista de la autenticidad, la validez de las imágenes fijas y los videos digitales está cada vez mas cuestionada.

EI marcado de agua digital es una de las soluciones propuestas para resolver el problema mencionado anteriormente. Es un conjunto de técnicas empleadas para insertar información en un documento digital (imagen, vídeo, audio, etc.). La introducción de la información se realiza modificando el documento original (huésped) con la restricción principal de que la distorsión producida por el marcado sea tolerable (en función de la aplicación). Una de sus ventajas esenciales es que los datos insertados están ligados al huésped, de ahí que no sea necesario ningún archivo adicional como ocurre en el caso de la criptografía.

Para la clasificación de una técnica concreta de marcado de agua digital se emplean varias características. Dos de las más importantes son la robustez y la necesidad o no del huésped para hacer posible la extracción de la información. Sobre esta última característica, se dice que una técnica es ciega si para la extracción de la información no necesita el huesped y no ciega en el caso contrario.

En la video supervisión, una condición imprescindible es que no se necesiten las imágenes originales para poder extraer la información, para evitar doblar la capacidad de almacenamiento requerida. Como

consecuencia se desprende que una técnica de marcado de agua para sistemas de vídeo supervisión debe ser preferiblemente ciega.

Una técnica de marcado de agua es robusta si la marca que tiene insertada resiste las alteraciones, pudiendo ser casuales o intencionadas. En el caso opuesto se encuentran las técnicas frágiles, que son aquéllas en las que la marca se corrompe tras la a la más mínima alteración. Para la detección de manipulaciones de contenidos digitales se usan las técnicas frágiles o semifrágiles, pues ellas permiten demostrar la autenticidad del contenido analizando la integridad de la marca.

Actualmente, una de las grandes familias de técnicas de marcado de agua digital es la de espectro ensanchado, otra es aquélla formada por las llamadas técnicas de marcado de agua digital con información lateral en el codificador. Una característica particular de las técnicas de marcado de agua digital de espectro ensanchado en esquemas ciegos es que sufren la interferencia del propio huésped. En contraposición, las técnicas con información lateral en el codificador no sufren dicha interferencia. Dada que, como se indicó anteriormente, la autenticación de las imágenes de un sistema de video supervisión es preciso que sea ciega, los esquemas más avanzados usan técnicas con información lateral en el codificador.

Un ejemplo de técnica de marcado de agua digital con información lateral en el codificador y extracción ciega se puede encontrar en el artículo de B. Chen y G. W. Wornell: "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", publicado en IEEE Transactions on Information Theory, Vol. 47, No. 4, Mayo 2001. En este documento se muestra la posibilidad de usar cuantificadores para insertar información en el huésped. Básicamente, la idea propuesta es tener un conjunto de cuantificadores de los cuales se selecciona uno dependiendo del mensaje que se quiera insertar. La obtención de ese conjunto de cuantificadores no es trivial. Los autores proponen un procedimiento práctico para obtenerlos de manera eficiente y estructurada. Partiendo de un cuantificador prototipo se desplazan los puntos de reconstrucción, con el efecto de la obtención de un cuantificador distinto; esta técnica se llama modulación Dither. Por otra parte, se muestra como es posible aumentar la robustez bajando la tasa de transmisión. Uno de los procesos expuestos consiste en proyectar los valores del huésped antes de insertar la marca, de este modo el ruido que sea ortogonal al vector sobre el que se proyecta no influirá en la comunicación. En este documento se presenta la técnica llamada compensación de distorsión DC (Distortion-Compensated) mediante ella se puede controlar la diferencia entre el documento marcado y el documento original. Como resultado, existe otro valor con el que se puede llegar a una solución válida entre la robustez de la marca de agua y la imperceptibilidad.

Otro enfoque de la proyección en el marcado de agua digital se puede encontrar en el artículo de Fernando Pérez-González, Felix Balado, y Juan R. Hernández: "Performance analysis of existing and new methods for data hiding with known-host information in additive channels", publicado en IEEE Transactions an Signal Processing, 51(4):960-980, Abri! 2003. Special Issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery. En este documento los autores dan una visión más amplia de la proyección de los valores del huésped, pues llegan a una solución de compromiso entre las técnicas de inserción con información lateral en el codificador y las técnicas de espectro ensanchado.

Otra implementación práctica de las técnicas basadas en cuantificadores está en el documento de Joachim J. Eggers, Robert Bäum!, Tomas Tzschoppe y Bernd Girod: "Scalar Costa Scheme for Information Embedding", publicado en IEEE Transactions on Signal Processing, VOL. 51, NO. 4, Abril 2003. En este documento se muestra una técnica cercana a la modulación Dither, pero centrada exclusivamente sobre cuantificadores escalares.

Los artículos presentados anteriormente tienen como denominador común el enfoque teórico de los esquemas de marcado de agua que proponen. Un ejemplo de ello es modelar el canal ruidoso de comunicación como un canal con ruido blanco gausiano aditivo, mientras que en muchas ocasiones el canal está caracterizado por un ruido de cuantificación; como es el caso de la codificación de imágenes fijas en JPEG o vídeos en MPEG-1.

Hay varias patentes centradas en el campo del marcado de agua para la autenticación de imágenes. La patente US2004131184 tiene como fin demostrar la validez de videos para ser usados como pruebas irrefutables ante la justicia. Utiliza técnicas de marcado de agua Dither-QIM, introduciendo dos tipos de información: uno es de identidad y el otro de control. La información de identidad se usa para identificar la secuencia del vídeo, y la de control se utiliza para determinar si la imagen fue manipulada. Otra característica básica en esta patente es que menciona unicamente el estándar MPEG. Ese estándar divide los coeficientes de cada bloque por una matriz de cuantificación, por lo tanto hay grandes distorsiones en la información insertada en el momento de la compresión del grupo de imágenes, como consecuencia para introducir la información necesita alterar una gran cantidad de coeficientes por cada bloque. Al marcar un número de coeficientes elevado la diferencia entre la imagen original y la imagen con la marca es, normalmente, bastante perceptible. Está ideada para implementarse en un computador portátil que acompañe a los sistemas de grabación de los coches patrulla.

La patente EP1001604 muestra un método para introducir información en imágenes. Opera con imágenes fijas codificadas con el estándar JPEG o JPEG2000, y utiliza para insertar la información una adaptación de SCS (Scalar Costa Scheme de Eggers et al.). Fija los valores del tamaño de los escalones de cuantificación usados para introducir la información reduciendo, por tanto, la versatilidad del método original. Además, no contempla ninguna técnica que permita introducir la información con un grado mayor de robustez, como pueden ser las técnicas de proyección.

Una patente usada para autenticar flujos de imágenes es US2003172275, con el objetivo de garantizar los derechos de autor. En ella se clasifican las imágenes que forman en el flujo síncronas y asíncronas. En las imágenes síncronas se introduce una marca en los bloques seleccionados pseudoaleatoriamente. En la introducción de la información utiliza técnicas de inserción con información lateral en el codificador. Debido a que la marca no se introduce toda la imagen, no es posible localizar las alteraciones.

Una idea para unir las técnicas de marcado de agua y las cámaras de red, los servidores de cámaras de red o los servidores video digitales se muestra en la patente US2004071311. En ella se indica un solución posible para integrar las cámaras y el proceso de inserción de la marca de agua desde un punto de vista físico. En la actualidad hay numerosos fabricantes de cámaras de red, por lo que es más factible diseñar un método que se adapte perfectamente a las cámaras ya existentes que tratar de diseñarlas desde el principio. El proceso de introducción de la marca está caracterizado por insertar una robusta para poder

demostrar la autenticidad y otra frágil para localizar las alteraciones. No obstante, en la patente no se describe un método lo suficientemente completo para poder abordar los problemas propios de la compresión en JPEG o en cualquiera de los estándares MPEG.

De lo expuesto anteriormente se deduce la necesidad encontrar una solución práctica para el problema de la detección y localización de manipulaciones espaciales y/o temporales en imagenes fijas o flujos de imágenes generados por sistemas de video supervisión digitales. Donde dicha solución debe proporcionar un alto grado de fiabilidad y seguridad, de tal manera que lo que muestren las imágenes sea irrefutable. Otro requisito necesario, que no ha sido solventado aún, es la perfecta adaptación de los métodos de autenticación a las particularidades de los sistemas de video supervisión digitales existentes, tales como la resistencia a la transcodificación de JPEG a MPEG o la adaptabilidad a las limitaciones computacionales de los dispositivos que integran esos sistemas, por ejemplo: las cámaras de seguridad digitales.

Resumen de la invención

Partiendo de este estado de técnica la invención tiene por objeto proporcionar un método de marcado de un documento digital, en particular de una imagen digital, con un marcado de agua digital para la detección y localización de manipulaciones espaciales y/o temporales de imágenes que posee un alto grado de fiabilidad.

La invención se refiere en un lado a un método de inserción y en otro lado a un método de extracción.

En el método de inserción se introducen en la imagen al menos dos mensajes y la información de integridad. Uno de los mensajes es un identificador temporal que permite asociar a una imagen el instante en el que fue obtenida. Otro de los mensajes es un identificador único del origen de la imagen. De esta manera, el método de extracción de la información de la imagen puede determinar el dispositivo que originó la imagen, el momento en el que fue tomada y comprobar la integridad con la información de integridad extraída. Los datos obtenidos de origen y de referencia temporal pueden ser cotejados para verificar su validez.

Los dispositivos de los sistemas de video supervisión digitales capaces de tomar imágenes o generarlas utilizan, usualmente, el estándar de imagen fija JPEG o algún estándar de video de la familia MPEG. El sistema expuesto en la invención está diseñado para imágenes y videos codificados con dichos estándares; siendo robusto a la transcodificación entre ellos.

La minimización de la distorsión introducida al insertar la marca de agua digital en una imagen es una restricción intrínseca de la invención, puesto que se requiere validar el contenido y no modificarlo. Esto se alcanza adaptando los sistemas al ruido introducido en el canal de comunicación propio de la codificación de imágenes en los estándares anteriormente mencionados. Acorde con esto, la información se introduce en el dominio transformado DCT de los bloques de la imagen, concretamente en unos predeterminados coeficientes. La meta es reducir la alteración de los coeficientes predeterminados y el número de coeficientes necesarios para introducir la marca con una determinada fiabilidad. En este sentido, los sistemas de la invención tienen una clara ventaja, ya que en ellos la generación y inserción de la marca tienen en cuenta el ruido de cuantificación que va sufrir la información que se introduce.

Desde un punto de vista funcional, la primera parte del método e inserción de información de la invención es la selección de los bloques de la imagen y los coeficientes de cada bloque que van albergar cada bit de cada mensaje y la información de integridad. Una manera de resolverlo eficientemente y además garantizando que la comunicación sea oculta es seleccionar los bloques de la imagen con una clave secreta. La resolución de la detección y localización de las manipulaciones está fuertemente relacionada con los bloques en los que se introduzca la información de integridad; si se inserta esta información en toda la imagen se podrá detectar y localizar las alteraciones en toda ella.

La segunda parte consiste en proyectar los valores de los coeficientes seleccionados para los mensajes y para la información de integridad sobre unos vectores de proyección, donde el tamaño de los vectores proyectados, que son los vectores resultantes del proceso de proyección, es un parámetro variable del método. Para aumentar más la privacidad se pueden generar los vectores de proyección de los mensajes con una clave secreta. Para originar el vector de proyección sobre el que se proyectan los coeficientes que contendrán la información de integridad se utiliza una función cuyo parámetro es alguno de los mensajes y la clave secreta. Uno de esos mensajes es la referencia o sello temporal, con lo que la información de integridad de una imagen será dependiente del momento en que se obtiene Al existir esta dependencia temporal, no se podrán usar imágenes marcadas de instantes anteriores para falsificar una secuencia de video, pues el sello temporal no se corresponderá al período de tiempo y se detectará ese intento de falsificación. EI tamaño de los vectores proyectados seleccionado permite llegar a un equilibrio entre la robustez de la marca y la tasa de transmisión. Además, los valores que forman cada uno de los vectores de proyección, sobre los que proyectan los coeficientes que albergaran cada bit de los mensajes o cada parte de la información de integridad, pueden ser ponderados en función de los valores de la tabla de cuantificación usada para codificar los coeficientes en el estándar JPEG o algunos de los estándares MPEG, o de cualquier otra tabla obtenida a partir de consideraciones perceptuales.

La tercera parte en la inserción es la cuantificación de los valores de los vectores proyectados con un cuantificador seleccionado de un conjunto según sea el valor del bit del mensaje o la parte de la información de integridad que se quiera introducir. Cada cuantificador se produce modificando un prototipo y usando un vector de desplazamiento acorde con el valor que se quiera introducir. Para obtener este vector se usa la clave secreta para el caso de los mensajes, y para la información de integridad la clave secreta y el valor de los mensajes de los que se precise que sea dependiente.

La última parte del método de inserción consiste en actualizar cada coeficiente de los bloques de la imagen seleccionados, para portar los mensajes y la información de integridad, con el resultado de la cuantificación de los vectores proyectados. Al marcar en los valores de los vectores proyectados se logra que el ruido ortogonal a cada uno de los vectores de proyección no tenga influencia en la comunicación, con el consiguiente aumento de la robustez.

EI método de extracción propuesto por la invención permite extraer los mensajes y determinar si la imagen fue manipulada espacial y/o temporalmente. EI método de inserción y extracción coinciden en el modo en que seleccionan los bloques de la imagen y la proyección de los coeficientes, con la clave secreta. Por tanto, sin conocer la clave secreta no se pueden obtener los mensajes reconstruidos.

Una vez se hayan obtenido los vectores con los valores proyectados de los mensajes y de la información de integridad, se procede a la extracción de la información. Ello se logra sometiendo esos vectores a una cuantificación sincronizada a partir de la clave. Analizando las distancias a cada centroide del resultado de la cuantificación se obtienen los mensajes reconstruidos y se decide para cada bloque con la información de integridad la autenticidad del mismo.

Para poder decidir acerca de la integridad de la imagen es necesario, para sincronizar la extracción, usar la clave secreta y el mensaje del que depende como elemento de sincronización de la extracción. Normalmente dicho mensaje es la referencia temporal. Si no se corresponde la referencia temporal con la información de integridad se señalarán los bloques de la imagen como falsos. Si la referencia temporal y la marca se corresponden, se comprobará que el valor de la referencia temporal este dentro de los umbrales permitidos; en caso contrario el método indicará que hubo una ruptura de secuencialidad de un grupo de imágenes.

En cuanto al nivel de robustez, la introducción de los mensajes tiene asociada un nivel de robustez mayor que para la información de integridad. Esta característica se deriva de la necesidad de la perfecta decodificación de los mensajes necesarios para determinar la integridad de la imagen. Sin esos mensajes, como se ha dicho, es imposible sincronizarse y, por lo tanto, tomar una decisión correcta sobre la autenticidad de los bloques de la imagen. Por otra parte, la información de integridad debe ser muy sensible a toda alteración distinta a la distorsión propia de la codificación JPEG o MPEG; de ahí que tenga una robustez baja.

Otro objeto de la invención es la alta fiabilidad del sistema expuesto. Esto se consigue logrando que la generación de la información de integridad para una imagen concreta en un instante concreto y un dispositivo concreto, sin conocer la clave secreta, sea un problema computacionalmente inabordable. Además, determinar la clave secreta usada para insertar la información analizando las imágenes fijas o vídeos marcados resulta también computacionalmente difícil, lo que proporciona un alto grado de seguridad.

La invención facilita la implementación del método de inserción en el interior de las cámaras de red que componen un sistema de video supervisión digital, donde esas cámaras de red tienen unas restricciones muy elevadas en cuanto a los recursos computacionales disponibles. Para poder acometerlo, el sistema propuesto está diseñado para minimizar el número de cálculos y accesos a memoria. Par ejemplo, marcar en el dominio transformado descarga a la CPU de numerosos ciclos de instrucción del cálculo de la transformada. Otro ejemplo es el uso del menor número de coeficientes para insertar la información minimizando el número de valores para realizar el cálculo, así como una mejora perceptual.

La invención favorece la máxima versatilidad posible, pudiendo configurar el sistema de forma que se pueda llegar a una solución de compromiso entre velocidad, distorsión, volumen de datos introducidos y/o tasa de error. Uno de los posibles parámetros configurables es el número de coeficientes asociados a cada bit de información de los mensajes o cada parte de la información de integridad. La relación entre la longitud entre el vector originario y el vector proyectado es otra de las posibilidades. El factor de control de la distorsión es el valor que más nítidamente permite balancear el método entre la distorsión y la probabilidad de detectar un error, dos características contrapuestas en la aplicación. Otra posibilidad es

usar codificadores de canal en los mensajes; de esta forma se aumenta su robustez bajando la tasa de error.

Otras ventajas y características del método serán aparentes en las figuras presentadas en conjunción con la descripción que viene a continuación.

Breve Descripción de los dibujos

Para complementar la descripción que se esta realizando y con objeto de ayudar a una mejor comprensión de las características del invento, de acuerdo con un ejemplo preferente de realización práctica del mismo, se acompaña un conjunto de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

La FIG. 1 muestra esquemáticamente a estructura general del sistema que comprende la invención.

La FIG. 2 muestra en un esquema los módulos en los que está dividido el método de inserción.

La FIG. 3 muestra en un esquema los módulos en los que está dividido el método de extracción.

La FIG. 4 representa un diagrama de flujo del proceso método de introducción de un mensaje con la dirección IP en una imagen.

La FIG. 5 representa un diagrama de flujo del método de introducción de un mensaje con una referencia temporal en una imagen.

La FIG. 6 representa un diagrama de flujo del método de introducción de la información de integridad en una imagen.

La FIG. 7 representa un diagrama de flujo del método de extracción de un mensaje con una dirección IP de una imagen.

La FIG. 8 representa un diagrama de flujo del método de extracción de un mensaje con una referencia temporal de una imagen.

La FIG. 9 representa un diagrama de flujo del método de comprobación de integridad de una imagen.

La FIG. 10 muestra la división de una imagen en bloques y en macrobloques, además representa la ordenación de los coeficientes según el orden en zigzag.

La FIG. 11 representa la selección y ordenación de los coeficientes de los bloques que forman un macrobloque de integridad.

La FIG. 12 representa un diagrama del método de inserción de marcado de agua digital con información lateral en el codificador.

La FIG. 13 representa esquemáticamente un diagrama interno de una cámara digital de red implementando el método de inserción propuesto en la presente invención.

La FIG. 14 representa esquemáticamente un sistema computacional que ejecuta los métodos con detección de manipulación propuestos en la presente invención, reflejando la interconexión entre los dispositivos de un sistema digital de video supervisión.

Realización preferente de la invención

La FIG. 1 muestra esquemáticamente los elementos individuales que comprenden la realización preferente seleccionada para la presente invención. En estos elementos es donde se somete a una secuencia de imágenes, obtenida por un sistema de vídeo supervisión digital, a unas técnicas de marcado de agua digital que permiten detectar y localizar las alteraciones espaciales y/o temporales que sufrieron.

Después de que una cámara digital de red obtiene una imagen digital, ésta se procesa en un codificador 100 donde está implementado el método de inserción de marcado de agua digital propuesto en la presente invención. La imagen marcada puede ser guardada formando parte de un vídeo con alguno de los estándares MPEG o como una imagen individual codificada acorde al estándar JPEG, en ambos casos se almacena en una unidad de almacenamiento 300. Si se opta por almacenar una secuencia de imágenes individuales marcadas formando un vídeo MPEG, se codifican en un codificador MPEG 400.

La comprobación de la integridad de las imágenes marcadas comienza por recuperar, de la unidad de almacenamiento 300, las imágenes archivadas individualmente o en forma de vídeo MPEG. Si el flujo de imágenes está codificado con alguno de los estándares de MPEG la información de las imágenes se extrae en un decodificador MPEG 500. En un decodificador 200, que implementa el método de marcado de agua digital con detección de manipulación propuesto en la invención, es donde se procesa con el fin de detectar y localizar las alteraciones de la información obtenida del decodificador MPEG 500 o de las imágenes individuales almacenadas en la unidad de almacenamiento 300.

Los datos generados por el decodificador 200 son relativos al origen de la imagen marcada, al instante en el que fue tomada, a las alteraciones detectadas, etc. Además, se puede configurar para que genere una imagen resultado señalando las modificaciones halladas.

Estándares de imagen fija y de video

En los sistemas de inserción y extracción de marcas de agua los estándares de codificación contemplados son el JPEG para la imagen fija y los estándares de la familia MPEG para el vídeo.

Una de las razones para emplear en la codificación de imágenes fijas de esta realización práctica el estándar JPEG es la buena relación entre la reducción de tamaño lograda y la distorsión introducida. Otra de las razones es su uso mayoritario en los sistemas de vídeo supervisión digitales actuales, permitiendo que la presente invención se adapte perfectamente a ellos.

Entre las imágenes fijas que componen una secuencia la redundancia existente es elevada. Este factor se puede explotar para alcanzar una notable reducción de tamaño, logrando que su almacenamiento sea más eficiente. En los sistemas propuestos en la presente invención, para la codificación de una secuencia de imágenes se utiliza un miembro de la familia de estándares MPEG. Ello se debe a los numerosos puntos coincidentes entre los estándares MPEG y el estándar JPEG, permitiendo que los métodos propuestos se adapten fácilmente a ambos.

EI estándar JPEG utiliza como espacio de color de tres componentes el YCC.. Las componentes son la de luminancia (Y) y las de color (C y C). Cada componente de la imagen se divide en bloques no solapados de 8□8 muestras. JPEG utiliza un cambio de coordenadas con el objetivo de que se concentre la mayor parte de la energía en un menor número de dimensiones que la representación original (RGB), hecho que se explota para reducir el tamaño de la imagen. Concretamente, JPEG utiliza la transformada discreta del

coseno (DCT) en cada bloque de la imagen de las componentes Y, C o C.. Cada bloque transformado de la imagen se somete a la cuantificación de los 64 coeficientes ue lo forman, dividiendolos por unos elementos que constituyen una matriz de cuantificación JPEG de dimensiones 8□8, obteniendo como resultado unos coeficientes cuantificados $c_{quant,j}$, como se muestra

$$c_{quant,j} = \text{round}(\ /),$$

donde en la expresión anterior round() denota una función que devuelve el valor entero más cercano. A los coeficientes cuantificados $c_{quant,j}$ de los bloques B_i se les aplica una codificación entrópica sin pérdidas para generar el archivo JPEG con la imagen, donde la codificación está especialmente diseñada para almacenar eficientemente aquellos $c_{quant,j}$ cuyo valor sea cero.

Para recuperar los bloques transformados reconstruidos $\hat{B}_i$, que forman la imagen, hay que realizar el proceso inverso a la cuantificación. Se debe multiplicar cada coeficiente cuantificado $c_{quant,j}$ perteneciente a cada $\hat{B}_i$ por su respectivo elemento c, es decir,

$$\hat{c} = c_{quant,j} \cdot q_j .$$

De la forma en que se codifica y decodifica una imagen en el estándar JPEG se deduce que cuanto mayores sean los valores de la matriz de cuantificación JPEG la distorsión introducida será mayor, aunque la compresión también será mayor. La energía de la imagen se concentra en las frecuencias mas bajas de los bloques transformados de la imagen y, por otra parte, el sistema visual humano es más sensible a esas frecuencias; por lo tanto, en la generación de se deben tener en cuenta estas características para lograr una buena codificación JPEG asignando los tamaños de los escalones de cuantificación menores a las frecuencias más bajas. Muchas veces, el resultado de aplicar atendiendo a esas consideraciones es que numerosos de las frecuencias más altas son cero y, como se mencionó anteriormente, se logra una considerable reducción del tamaño.

La FIG. 10 muestra la división de las imágenes 1003 en el estándar JPEG formando bloques de 8,8 pixels 1001. Además, se puede observar la ordenación en zigzag de los coeficientes que forman los bloques, representada por una flecha que empieza en el coeficiente en la posición (1,1) (coeficiente de continua) y acaba en el coeficiente (8,8).

En la presente descripción de la realización preferente se contempla que las imágenes JPEG que forman un flujo de imágenes obtenidas por un sistema de video supervisión se compriman con el estándar MPEG-1. Un secuencia de video MPEG-1 comprende varios tipos de imágenes, siendo los tipos 1, B y P. Atendiendo a esta característica, las imágenes que contendrán la marca son las codificadas tipo 1 y P, dejando las codificadas como tipo B sin marca para que puedan soportar una mayor compresión.

Cuando se codifica una secuencia de imágenes fijas individuales como un flujo MPEG-1 se usa un patrón de codificación. A modo ilustrativo consideraremos el patrón IBBBBPBBBB. Ese patrón indica que la primera imagen se codifica como una imagen tipo 1, las cuatro siguientes tipo B, después como tipo P y las cuatro ultimas tipo B. Los métodos de marcado de agua propuestos no utilizan las imágenes marcadas codificadas como B. Si se quiere aumentar el grado de compresión de un vídeo de imágenes marcadas se debe aumentar la proporción de imágenes codificadas como tipo B. Corno consecuencia, el número de imágenes 1 y P del flujo disminuye y, con ello, la capacidad de detección de alteraciones. Usando el patrón antes señalado, si una cámara digital de red genera imágenes marcadas con una tasa de 10 por segundo y se codifican en el codificador MPEG 400, sólo se podrá detectar alteraciones con una resolución de 0.2 s. Acorde con esto, es necesario en el momento en el que el usuario del sistema configure la codificación MPEG-1, se llegue a un compromiso entre el grado compresión y la resolución temporal de las alteraciones.

lnformación ligada a las imágenes.

En la presente realización preferente de la invención la marca insertada está compuesta por un mensaje de metadatos, un mensaje con una referencia temporal y la información de integridad.

En el mensaje de metadatos se podrá insertar y extraer de la imagen la información arbitraria que se desee. A modo de ejemplo ilustrativo y no limitativo se utiliza un identificador único del elemento generador de imágenes de video supervisión. Debido al contexto habitual en el que se encuentra un sistema de video supervisión digital se selecciona en la presente realización práctica la dirección IP. Nótese que existen numerosas alternativas como identificador único, tales como: número de serie, MAC (del inglés Media Access Control), etc.

La información es introducida en la imagen digital en los coeficientes transformados de los bloques de luminancia que forman la imagen. Los bloques en los que se introduce la información de integridad se agrupan en macrobloques. Las dimensiones de los macrobloques para la inserción de la información de integridad son configurables y, además, determinan la granularidad de la detección de las alteraciones espaciales. Cuanto mayor sea el macrobloque más difícil es señalar los puntos concretos de la imagen que fueron modificados, aunque esta opción tiene la ventaja de la posibilidad de utilizar un mayor número de coeficientes para determinar su autenticidad. Por ejemplo, un macrobloque de la información de integridad puede estar formado por 2 2 bloques. En la FIG. 10 se representa un macrobloque 1002 usado en la detección de alteraciones espaciales.

Módulos del codificador

En la FIG. 2 se muestra el esquema interno del codificador 100, que consta de un módulo de inserción de la dirección IP (metadatos) 110, un módulo de inserción de la referencia temporal 130, un módulo de inserción de la información de integridad 150 y un registro con el valor de la referencia temporal 170.

Cuando una imagen codificada con el estándar JPEG se introduce en el codificador 100, se procesa en el módulo de inserción de dirección IP 11O para introducir en cada imagen la dirección IP del dispositivo del sistema de vídeo supervisión digital que la obtuvo. Después, la imagen se pasa al módulo de inserción de

la referencia temporal 130 para introducir en la imagen la referencia temporal (almacenada en el registro 170); con esa información se podrá saber el instante en el que se obtuvo la imagen y, además, determinar si se alteró el orden en una secuencia de imágenes (alteraciones temporales). Cada imagen en la salida del módulo 130 se pasa al módulo de inserción de la información de integridad 150; en ese módulo se introduce la información de integridad con la cual se pueden detectar las alteraciones espaciales. En la inserción de la información de integridad se utiliza la referencia temporal del registro 170 para que no se pueda falsificar una imagen usando otra, pues la información de integridad no es válida en otro momento distinto a aquel en que se generó. Los módulos 110, 130 y 150 utilizan una clave secreta K, de tal forma que introducir esos dos mensajes o la información de integridad sin dicha clave sea un problema computacionalmente muy complicado.

Módulos del decodificador

La FIG. 3 muestra el esquema interne de decodificador 200, formado por un módulo de extracción de la dirección IP 210, un módulo de extracción de la referencia temporal 230 y un módulo de extracción de la información de integridad 250.

El módulo de extracción de la dirección IP 210 recupera la dirección de IP insertada en la imagen. El módulo de extracción de la referencia temporal 230 recupera la referencia temporal que está ligada a la imagen. El módulo de extracción de la información de integridad 250 recupera la información de integridad y determina si una imagen fue manipulada espacialmente, es decir, si se modificó algun cuadro de la imagen original. Si la imagen fue manipulada, el módulo de extracción de la información de integridad 250 puede generar una imagen indicando gráficamente la posición de las alteraciones detectadas. Los módulos de extracción 210, 230 y 250 utilizan la misma clave secreta K para extraer la información que la usada para introducir la información.

Ordenación interna del codificador y el decodificador

Aunque los esquemas internos del codificador 100 y del decodificador 200 de la FIG. 2 y FIG.3 muestran una conexión en cascada entre los módulos, esta característica no es restrictiva. Es posible disponer los módulos paralelamente o incluso agruparlos en un solo módulo.

Codificador

Las FIG. 4, FIG. 5 y FIG. 6 representan el diagrama de flujo de los sistemas de los módulos de inserción que forman el codificador 100, que se pueden apreciar en la FIG. 2.

Los diagramas de flujo son configurables mediante la asignación de valores a unos determinados parámetros del sistema. Uno de los parámetros del sistema es el número de coeficientes de la imagen por bit de información utilizados en el caso de los mensajes o el número de coeficientes de cada macrobloque para la introducción de la información de integridad. En los diagramas son representados por N°COEF_IP, N°COEF_REF o N°COEF_INT (”Nº“ = number), para el caso del mensaje con dirección IP, el mensaje con la referencia temporal y la información de integridad respectivamente. Otro parámetro de los diagramas de introducción de los mensajes es el número de bits de información de cada mensaje, que en los diagramas son representados por N°BITS_IP y N°BITS_REF, en el caso de la dirección IP y la referencia temporal respectivamente. Otro posible modo de configurar el sistema es mediante la selección de los coeficientes de bloque que serán utilizados para insertar el mensaje con la dirección IP (metadatos), el mensaje con la

referencia temporal y la información de integridad. EI tamaño de los vectores de proyección sobre los que se proyectan los valores de los coeficientes, de los que se obtienen los valores proyectados en los que se insertan la información, es otro valor configurable, representandolo por LONG_IP, LONG_REF y LONG_INT para la dirección IP, la referencia temporal y la información de integridad respectivamente.

La FIG. 4 muestra el diagrama de flujo del sistema de inserción de la dirección IP (metadatos) 110, en el cual se procesará cada imagen obtenida por un sistema de video supervisión. Si es la primera vez que se ejecuta el método (paso 111) en un flujo de imagenes, en el paso 112 se seleccionan pseudoaleatoriamente (en función de la clave secreta K) los bloques transformados de 8 8 coeficientes en que está dividida la imagen, para utilizarlos en la inserción de la dirección IP. En el paso 113 se inicializa la variable BIT, usada para determinar el número de bits del mensaje de la dirección IP que han sido introducidos en la imagen. En el paso 114 se decide si ya han sido introducidos todos los bits de este mensaje en la imagen; si la respuesta es afirmativa la parte de inserción de la dirección IP en la imagen habra concluido. En caso contrario, se sigue en el paso 116 en el que se inicializa el contador de coeficientes per bit COEF a cero. En el paso 117 se determina si ya se ha introducido el valor del bit BIT en los N°COEF_IP coeficientes que tenía asignados, en caso afirmativo se avanzará al paso 115 que sumará uno al valor del contador BIT y volverá al paso 114 descrito anteriormente. Si aún no se han alterado los coeficientes de la imagen asociados a ese bit de la dirección IP se pasa al paso 118, donde se genera un vector de proyección pseudoaleatorio (en función de la clave secreta K) de longitud LONG_IP. Después de obtener el vector de proyección se continua en el paso 119, donde se computa el producto escalar entre el vector proyección y el vector formado por los coeficientes seleccionados (en el paso 112) cuyos Indices están entre (N°BITS_IPxBIT)+COEF y (N°BITS_IPxBIT) +COEF+ LONG_I P-1, guardando el resultado de la proyección en RES_PROY. En el paso 120 se suma LONG_IP al valor COEF, que se empleará para determinar los coeficientes usados en el cálculo de la siguiente proyección. En el paso 124 se inserta el valor del bit BIT de la dirección IP en RES_PROY y en el paso 125 se actualizan los coeficientes con los que se calculó la proyección actual con el resultado obtenido en el paso anterior (124).

La FIG.5 muestra el diagrama de flujo del módulo de inserción de la referencia temporal 130. lgual que en la FIG. 4, en el inicio se introduce una imagen digital obtenida del sistema de video supervisión. En el paso 131 se determina si es la primera vez que se ejecuta el método para ese determinado flujo de datos. Si es asi, se avanza al paso 132 que seleccionara pseudo-aleatoriamente (en función de la clave secreta K) los bloques de la imagen que van a albergar el mensaje con la referencia temporal. En el paso 133 se somete al mensaje con la referencia temporal a una codificación de canal, cuyo objetivo es aumentar su robustez produciendo un mensaje codificado de la referencia temporal. En el paso 134 se inicializa a cero la variable BIT usada para controlar el número de bits del mensaje codificado de la referencia temporal que se han insertado en la imagen. En el paso 135 se verifica si el mensaje codificado de la referencia temporal ha sido totalmente insertado en la imagen; para ello se comprueba si el valor de BIT es menor que el número de bits totales signados para la inserción del mensaje codificado con la referencia temporal N°BITS_REF. En caso de que no se cumpla esta condición, el trabajo del módulo de inserción de la referencia temporal 130 habrá acabado. Si aún restan bits de la referencia temporal por introducir se continua en el paso 136, que inicializa el valor COEF a cero. La variable COEF se usa para controlar el número de coeficientes que se han introducido del bit BIT del mensaje codificado de la referencia

temporal. En el paso 138 se comprueba si se han computado los se comprueba si se han computado los N°COEF_REF coeficientes asignados para albergar cada bit de la referencia temporal, si es el caso. Si ya se han completado, se continúa en el paso 137 que actualiza el valor de BIT sumándole uno, indicando que a continuación se procederá a la inserción del bit siguiente del mensaje codificado de la referencia temporal. Si aún no se han utilizado todos los coeficientes correspondientes a cada bit de la referencia temporal, se avanza del paso 138 al 139. En el paso 139 se genera un vector de proyección de longitud LONG_REF, obtenido pseudoaleatoriamente con la clave secreta. Este vector de proyección será el usado para proyectar los valores de los coeficientes LONG_REF siguientes. En el paso 140 se calcula el producto escalar entre el vector de proyección (obtenido en el paso 139) y un vector formado por los coeficientes seleccionados en el paso 132 cuyos Indices se encuentran entre (N°BITS_REFx BIT)+COEF y (N°BITS_REFxBIT)+COEF+LONG_REF-1, almacenando el resultado de la proyección en RES_PROY. En el paso 144 se suma al valor de COEF el valor de LONG_REF. Después, se pasa al paso 145, en el cual se inserta en el valor proyectado RES_PROY el bit del mensaje codificado de la referencia temporal cuyo índice es BIT. En el paso 146 se actualizan los coeficientes que se usaron para computar la proyección actual con el valor de RES_PROY, resultado del paso 145.

La FIG. 6 muestra el diagrama de flujo correspondiente al módulo de inserción de la información de integridad 150. A este sistema se le pasa como parámetro el valor de la referencia temporal que es introducida en la imagen por el módulo de inserción de la referencia temporal 130 obtenida del registro 170 y la clave secreta K. En el paso 151 se sincroniza el sistema para conseguir que la introducción de la información de integridad en la imagen sea dependiente del instante en que se tomó la imagen que se está procesando, además se utiliza en la sincronización la clave secreta K para garantizar que sólo los usuarios autorizados puedan introducir la información de integridad válida. Si no se conoce la referencia temporal, el proceso de introducir la información de integridad sin que en el decodificador 200 de la FIG. 1 se detecte resulta muy complejo. En el paso 152 se inicializa el valor índice i, cuya función es la de contar la fila de macrobloque en la que se encuentra el método de inserción durante su ejecución. En esta figura, el ancho en bloques (8 8) de la imagen se denota por ANCHO y la altura en bloques por ALTO, el ancho en bloques de cada macrobloque M y el alto en bloques de cada macrobloque N. En el paso 153 se comprueba si ya se ha introducido la información de integridad en toda la imagen, si ha sido asi se termina el proceso de inserción de la información de integridad. Si aún no se ha computado la totalidad de la imagen se avanza al paso 154 en el que se inicializa a cero el valor del índice de las columnas de macrobloques j. En el paso 156 se verifica si ya se han computado todas las columnas de macrobloques de la fila de macrobloques actual, la fila i. Si ya se han computado se sigue al paso 155 que suma una unidad al índice i para procesar la siguiente fila de macrobloques o acabar, decidiéndose esto en el paso 153. Si el resultado de la decisión tomada en el paso 156 es que quedan macrobloques de la fila i por procesar se continua en el paso 157, donde se crea un vector VEC_INT de longitud N°COEF_INT, tomando de cada bloque, que forma el macrobloque de coordenadas (i,j) de la imagen, N°COEF_INT coeficientes. El orden de disposición de los coeficientes de cada bloque en dicho vector VEC_INT es de izquierda-derecha y de arriba-abajo respecto a la posición de los bloques en el macrobloque actual, como se representa en la

FIG. 11. El orden de disposición de los coeficientes pertenecientes a cada bloque en el vector VEC_INT sigue el orden de los coeficientes según la ordenación zigzag de esos propios coeficientes en el bloque. En el paso siguiente, el 159, se inicializa el valor COEF a cero. Después, en el paso 160 se verifica si ya se ha insertado la información de integridad en el macrobloque actual (i,j), en caso afirmativo se suma una unidad a j en el paso 158 y se continúa en el paso 156. Si se decide (paso 160) que aún quedan bloques sin marcar (COEF<N°COEF_INT) se continúa con el paso 161. En el paso 161 se genera pseudo-aleatoriamente a partir de la referencia temporal y de la clave secreta un vector de proyección de longitud LONG_INT, donde la generación de este vector es resultado de la sincronización llevada a cabo en el paso 151 de la FIG. 6. En el paso 162 se computa la proyección, para ello se calcula el producto escalar entre el vector de proyección (obtenido en el paso 161) y un vector formado por los coeficientes de VEC_INT con Indices comprendidos entre COEF y COEF+LONG_INT-1, donde el resultado de esta proyección se guarda en RES_PROY. En el paso 163 se suma el valor LONG_INT al valor de COEF. Luego, se continúa en el paso 168. En él se inserta el valor de esa parte de la información de integridad en el valor RES_PROY, que es el resultado de la proyección de los coeficientes de la imagen sobre el vector de proyección. En el paso 169 se actualizan los coeficientes utilizados para calcular la proyección actual con el valor el valor RES_PROY marcado, resultado del paso 168.

Decodificador

En la FIG. 7, FIG. 8 y FIG. 9 se representan los diagramas de flujo de los procesos que se realizan en los módulos de extracción que forman el decodificador 200 y que se pueden apreciar en la FIG. 3. Los valores de los parámetros empleados en el codificador 100 deben ser los mismos que los que usa el decodificador 200. Por ejemplo: N°COEF_IP, ANCHO, M, N°BITS_REF, etc.

La FIG. 7 muestra el diagrama de flujo del proceso de extracción de la dirección IP correspondiente al módulo de extracción de la dirección IP (metadatos) 210. Al inicio se encuentra una imagen digital de la cual el módulo 210 va extraer la dirección IP. En el primer paso (211) se comprueba si es la primera vez que se ejecuta el diagrama de flujo en la secuencia a la que pertenece la imagen que se va a procesar. En caso afirmativo se continua en el paso 212 en el cual se seleccionan pseudoaleatoriamente con la clave secreta K los bloques de la imagen JPEG de los cuales se va extraer el mensaje con la dirección IP. El paso siguiente es el 213, en el que se inicializa el valor BIT a cero. Ese valor permite controlar el número de bits de la dirección que son extraídos. Es en el paso 214 donde se verifica si el total de bits del mensaje con la dirección IP fueron recuperados; si es así, se finaliza la extracción de la dirección IP de la imagen actual que se procesa en este módulo. Si aún no se ha acabado con el total de los bits que forman la dirección IP N°BITS_IP se continua en el paso 21ó, donde se inicializa a cero el valor COEF. El valor COEF es un contador del número de coeficientes que han sido usados para recuperar el valor del bit BIT de la dirección IP. La decisión sobre si ya han sido utilizados el total de coeficientes N°COEF_IP necesarios para extraer el valor de un bit de la dirección IP se toma en el paso 218. Si ya se ha acabado se sigue con el pya se ha acabado se sigue von el paso 217, en el cual se decide el valor del bit BIT de la dirección IP usando un vector VEC_DIS de longitud N°COEF_IP/LONG_IP formado por los valores

almacenados en el paso 226. En el paso 215 se actualiza el valor de la variable BIT para proseguir o terminar con la extracción de la dirección IP, que se decide en el paso 214. Se llega al paso 219 si la decisión tomada en 218 es que aún restan grupos de coeficientes por procesar para poder calcular el valor del bit BIT de la dirección IP. En el paso 219 se genera un vector de proyección de longitud LONG_IP, donde ese vector debe ser igual al generado en 118 de la FIG. 4, para ello debe conocerse el valor de clave secreta K. En el paso 220 se computa la proyección mediante el producto escalar entre el vector proyección y un vector formado por los coeficientes (seleccionados en el paso 212) cuyos Indices se encuentran entre (N°BITS_IPxBIT)+COEF y (N°BITS_IPxBIT) +COEF+ LONG_I P-1, para finalmente almacenar el valor en RES_PROY. En el paso 221 se suma el valor LONG_IP a COEF. En el paso 226 se guarda en la posición COEF/LONG_IP del vector VEC_DIS el resultado del calculo de la distancia entre RES_PROY y un vector de referencia. Este último cálculo será explicado posteriormente en esta descripción de la realización preferente de forma pormenorizada.

La FIG. 8 muestra el diagrama de flujo del proceso de extracción de la referencia temporal 230. lgual que los anteriores diagramas de flujo descritos, al inicio se encuentra una imagen digital de la cual se quiere extraer la referencia temporal que tiene ligada. EI primer paso (231) del diagrama determina si es la primera ocasión en que se extrae de la imagen del presente flujo de imágenes, si es así, se avanza al paso 232, y en caso contrario al paso 233. En el paso 232 se seleccionan pseudoaleatoriamente con la clave secreta K los bloques de la imagen codificada que van ser usados para extraer la referencia temporal. EI paso 233 inicializa el valor BIT a cero; con ese valor se puede saber cuando ha finalizado el proceso de extracción de la referencia temporal en la imagen. En el paso 234 se decide si ya se han extraído todos los bits del mensaje de la referencia temporal en la imagen, continuando en el paso 235, o si aún quedan, prosiguiendo en el paso 237. EI paso 235 esta compuesto por un decodificador de canal que obtiene el valor del mensaje de la referencia temporal procesando los valores del vector VEC_DIS, siendo el proceso inverso al del paso 133 de la FIG. 5. Después de la decodificación de canal llega al final del proceso descrito por el diagrama de flujo. En el paso 237 se introduce el valor cero en COEF, que se usa como contador del número de los coeficientes usados en un determinado instante para extraer la métrica correspondiente al bit BIT del mensaje codificado de la referencia temporal. En el paso 238 se decide si ya se han computado todos los coeficientes usados para extraer la métrica correspondiente a un bit del mensaje codificado de la referencia temporal. Si ya se han computado todos los coeficientes asociados a un determinado bit BIT se prosigue con la suma de una unidad al valor BIT para calcular los valores de RES_PROY del siguiente bit del mensaje, si es que existe. En caso de que aún no se hayan procesado todos los coeficientes necesarios para extraer la información insertada en la imagen relativa a un bit se continúa en el paso 239. En el paso 239 se genera un vector de proyección de longitud LONG_REF sobre el que se proyectarán los valores de coeficientes. En el paso 240 se calcula el producto escalar entre el vector proyección y un vector formado por los coeficientes seleccionados para insertar la referencia temporal (seleccionados en el paso 232) cuyos indices se encuentran entre (N°BITS_REFxBIT) +COEF y (N°BITS_REFx BIT)+COEF +LONG_REF -1, el valor obtenido se almacena en RES PROY. En el paso 244 se actualiza el valor de COEF sumándole LONG REF. En el paso 246 se toma el valor RES_PROY y se calcula su distancia respecto a un vector de referencia, cuyo resultado se almacena en un vector VEC DIS en la posición COEF/LONG_REF+B1Tx(N0COEF _REF/LONG_REF), donde VEC_DIS será usado en el paso 235 para determinar el mensaje de la referencia temporal, como se indicó

anteriormente. La manera para calcular la distancia de RES_PROY será abordado posteriormente en la descripción.

La FIG. 9 muestra el diagrama de flujo correspondiente al proceso de extracción de la información de integridad 250. Este método tiene como parámetro la referencia temporal extraída en el módulo 230 y la clave secreta K; sin el valor correcto de la referencia temporal no se podría recuperar la información de integridad y se señalaría la imagen como falsa al no corresponderse la referencia temporal que tiene ligada con la información de integridad. El diagrama de flujo tiene como entrada una imagen de la que se va a extraer la información de integridad y comprobar su autenticidad espacialmente. En el paso 251 el método se sincroniza con la referencia temporal y la clave es la referencia temporal y la clave secreta K, que permitirá generar correctamente los valores pseudoaleatorios necesarios para el presente proceso de extracción. En el paso 252 se inicializa al valor cero el índice i que será usado por el método para saber en que fila de macrobloques se encuentra. En el paso 253 se determina si la extracción de la información de integridad ha llegado a su fin, sabiéndolo al comprobar si ya se han computado todas las filas de macrobloques. Si aún no se han computado todas las filas se continúa con el paso 254, en el cual se inicializa el valor j que permite controlar el número de columnas de macrobloques de una fila de macrobloques i que han sido computadas. En el paso 254 se decide si ya se ha extraído la información de integridad de todas las columnas de macrobloques que forman cada fila. Si eso es así, se suma una unidad al contador i en el paso 255 y se vuelve al paso 253. En caso de que aún no se hayan computado todas las columnas se pasa al paso 258 en el que se genera el vector de coeficientes del macrobloque con coordenadas (i,j) usado para extraer la información de integridad. La forma de generar el vector es la misma que la mostrada anteriormente en el paso 157 de la FIG. 6. En el paso 2ó0 se inicializa a cero el valor COEF, que permite controlar el número de coeficientes usados para extraer la información por cada macrobloque. La decisión sobre si ya se han computado todos los coeficientes de un macrobloque se toma en el paso 262. Si es asf, se avanza al paso 261 en el que se analiza el vector distancias VEC_DIST y se decide si el macrobloque fue manipulado; si es el caso, se continúa en el paso 259. La función del paso 259 es señalar un macrobloque como falso; esto se puede hacer señalando el macrobloque de alguna forma visible y/o emitiendo una serial que permita a un usuario saber que ese macrobloque ha sido alterado. Si en el paso 261 no se decide que se ha manipulado el bloque estudiado, se prosigue, igual que a continuación del paso 259, con el paso 257. En el paso 257 se añade una unidad al contador j, indicando que la extracción de la información de integridad de un macrobloque ha acabado. Par otro lado, si en el paso 262 se decide que aun se ha recuperado la información de integridad correspondiente a ese macrobloque se continua en el paso 2ó3. En el paso 263 se genera un vector de proyección de longitud LONG_INT sincronizado con el generador en 161 en la FIG. 6. Su generación es dependiente de la referencia temporal y de la clave, de ahí que y de la clave, de ahí que si no se conoce la referencia temporal o la clave secreta se determinará con alta probabilidad que el macrobloque es falso. En el paso 265 se realiza el producto escalar entre el vector de proyección y un vector formado por coeficientes de VEC_INT con Indices comprendidos entre COEF y COEF+LONG_I NT-1, donde el resultado de la proyección se almacena en RES_PROY. En el paso 266 se actualiza el valor COEF añadiéndole el valor LONG_INT. Después de que la proyección actual se haya finalizado, se continúa con el paso 264. En ese

paso se introduce el valor resultado de computar la distancia entre RES_PROY y un vector de referencia en la posición resultado de la división COEF/LONG_INT del vector de distancias VEC_DIST. La explicación del cálculo de la distancia será abordado posteriormente en la descripción.

Selección pseudoaleatoria de bloques

En la presente realización práctica, los bloques transformados DCT que albergan los mensajes de una imagen digital fija codificada acorde al estándar JPEG son seleccionados pseudoaleatoriamente. Se lleva a cabo en las parejas de pasos 112 (FIG. 4) - 212 (FIG. 7) y 132 (FIG. 5) - 232 (FIG. 8) para el mensaje con la dirección IP y el mensaje con la referencia temporal respectivamente. Si los bloques seleccionados en codificación y decodificación no son los mismos los datos recuperados son inválidos.

La selección se realiza permutando los bloques que forman la imagen usando un generador de números pseudoaleatorios, en el cual se emplea como semilla el valor de la clave secreta o una función de ella. Los bloques transformados de la imagen se disponen formando un vector de bloques atendiendo al orden de izquierda-derecha y de arriba-abajo respecto a la posición de los bloques en la imagen. Con el generador pseudoaleatorio se permuta la posición de cada bloque en el vector de bloques obteniendo un vector de bloques desordenado.

Se fijan los coeficientes de los bloques que forman el vector de bloques desordenados para cada uno de los mensajes que van a ser ocultados en la imagen. Los coeficientes asociados a cada mensaje se disponen formando un vector de coeficientes c. El vector de coeficientes del mensaje con la dirección IP se denota por y tiene una longitud de N°BITS_IPxN°COEF_IP. El mensaje con la referencia temporal se denota por c_{REF} con una longitud de N°BITS_REFxN°COEF_REF.

Si los vectores o las matrices de proyección no son ortogonales, se debe cumplir que los conjuntos de coeficientes asociados a cada mensaje sean disjuntos. Si esto no se cumpliera, los procesos de inserción de cada mensaje se estarían interfiriendo mutuamente y la información insertada no podría ser recuperada.

La selección pseudoaleatoria de los bloques se puede realizar cuando se vaya a procesar cada imagen y no sólo al comienzo de un flujo de imágenes. Esta posibilidad tiene el inconveniente de que el tiempo de ejecución de la inserción o de la extracción aumenta por lo que esta solución no es aconsejable en aquellos casos en que existan restricciones temporales.

Sincronización función de la referencia temporal y la clave secreta

La sincronización de la introducción y la extracción de la información de integridad se realiza en los pasos 151 (FIG. 6) y 251 (FIG. 9). Se usa la clave secreta K para garantizar que la información de integridad se introduce por un usuario autorizado del sistema. La sincronización con el sello temporal se implementa con el objetivo de crear una dependencia entre el proceso de inserción de la información de integridad y el valor de la referencia temporal. Corno resultado, no es posible utilizar imágenes marcadas en un instante de tiempo anterior para falsificar una imagen obtenida en otro instante diferente sin que se detecte. Esta sincronización se logra inicializando un generador pseudoaleatorio de integridad con un valor que sea función de la referencia temporal y de la clave secreta. El generador pseudoaleatorio se utiliza en la parte correspondiente al control de integridad en la obtención de valores en los pasos 161 (FIG. 6) y 168 (FIG. 6) en la introducción, 263 (FIG. 9) y 264 (FIG. 9) en la extracción.

Generación de los vectores de proyección

Las parejas de pasos 118 (FIG. 4) - 219 (FIG. 7) del mensaje con la dirección IP, 139 (FIG. 5) - 239 (FIG. 8) del mensaje de la referencia temporal y 161 (FIG. 6) - 263 (FIG. 9) de la información de integridad generan los vectores de proyección,y de longitud LONG_IP, LONG_REF y LONG_INT respectivamente. Los vectores de proyección se obtienen pseudoaleatoriamente haciendolos dependientes de la clave secreta para los mensajes o la referencia temporal y la clave secreta para la información de integridad.

EI primer paso para generar los vectores de proyección es crear un vector con todos sus elementos puestos a uno y determinar el signo de los elementos del vector pseudoaleatoriamente. A continuación, se le aplica una máscara para obtener el vector de proyección. La máscara puede ser generada respondiendo a características psicovisuales humanas u otro tipo de requisito.

Un ejemplo para producir la máscara es crearla de forma que el peso de los coeficientes en la proyección sea el mismo desde la perspectiva del estándar JPEG; para ello los valores de la máscara se generan como función de la relación del tamaño de los escalones de cuantificación asociados a la cuantificación JPEG de cada coeficiente. Anteriormente se indicó que cada coeficiente de los bloques 8 8 en los que está dividida una imagen en el estándar JPEG se somete a una cuantificación, donde el tamaño del escalón del cuantificador es función de su posición en el bloque. Por lo tanto, la máscara se genera de forma que al proyectar los coeficientes sobre el vector de proyección el valor de la máscara sea tal que el producto del escalón de cuantificación JPEG de cada coeficiente por el valor de la máscara que lo multiplica sea constante.

Esta igualación se logra asignándole en la máscara el valor mayor (por ejemplo 1) al elemento asociado al coeficiente cuantificado con el escalón mas pequeño y haciendo que el resto de los elementos del vector sean proporcionales a él. Por ejemplo, si un coeficiente tuviese asociado un tamaño de escalón cuyo valor es el .doble que el del coeficiente más pequeño le correspondería a en la máscara la mitad del valor asociado al más pequeño. Particularizando, si sólo se marcara un coeficiente de cada bloque para introducir un determinado mensaje, la máscara generada sería un vector con sus elementos iguales a la unidad. Esta manera de generar la máscara queda ilustrada en el siguiente ejemplo

$$\mathbf{c}_{\mathbf{quant}} = \{1,1,2,1\}$$
$$\mathbf{q} = \{5,5,6,6\}.$$

En el caso anterior representa el vector formado por los coeficientes cuantificados, el vector q representa los valores de la matriz de cuantificación JPEG con los que se obtienen los coeficientes cuantificados. Atendiendo a esto, la máscara m resulta

$$m=\{1,1,5/6,5/6\}.$$

Pudiendo corresponderse a vector de proyección p={1,-1,5/6,-5/6}.

Inserción de la marca de agua

En el resultado de las proyecciones RES_PROY se introduce un bit de los mensajes o una parte de la información de integridad. Este proceso se lleva a cabo en los pasos 124 de la FIG. 4, 145 de la FIG. 5 y 168 de la FIG. 6 para la dirección IP, la referencia temporal y la información de integridad

respectivamente. Los tres pasos son análogos, difiriendo sólo en la información que se introduce en cada uno.

En el sistema propuesto en la presente invención se usan técnicas de marcado de agua con información lateral en el codificador, y en la presente descripción preferente se usa una técnica basada en cuantificadores escalares uniformes y codificación por repetición.

Los mensajes a insertar se representan mediante vectores binarios (sus elementos solo pueden tomar los valores {O,1}) en los que cada elemento representa un bit de información:

El mensaje correspondiente a la dirección IP se denota por b_{IP} y tiene una longitud de 32 bits, donde este valor se denota en los diagramas de flujo de FIG. 4 y FIG. 7 por N°BITS_IP.

El mensaje de la referencia temporal se denota por y tiene una longitud variable, dependiendo de la codificación de canal que se aplique en el paso 133 de la FIG. 5. Este valor de longitud se denota en FIG 5 y FIG. 8 por N°BITS_REF.

La información de integridad también se representa mediante un vector binario b_{INT} que representa el valor de un mensaje de referencia, introduciéndose un bit en cada macrobloque, y por lo tanto su longitud es igual al número de macrobloques de la imagen. Este mensaje de referencia es arbitrario, debiendo ser conocido por el decodificador para poder verificar su presencia en la imagen.

El objetivo del proceso de marcado de agua que se describe en esta realización práctica preferente es codificar cada mensaje o la información de integridad en un vector y que representa una palabra código, la cual se insertara en la imagen original.

En el método usado en esta descripción, cada palabra código y tiene L veces la longitud del vector binveces la longitud del vector binario que representa el mensaje a insertar, siendo L la tasa de repetición utilizada N°COEF_IP/LONG_IP, N°COEF_REF/LONG_ REF o N°COEF_INT/LONG_INT según corresponda a la dirección IP, la referencia temporal o la información de integridad respectivamente; en general L sera distinto para cada mensaje o para la información de integridad. El proceso para introducir información en la imagen propuesto en esta descripción de la realización preferente de la invención comprende tres pasos: cuantificación, obtención de vectores de error y actualización de los coeficientes Estos pasos serán descritos en detalle a continuación.

En el primer paso, para insertar un mensaje o la información de integridad de longitud N representados por un vector binario $\mathbf{b} = (b_1, b_2, \ldots, b_N)$ se generan los elementos de la palabra código y, de manera que para un elemento y_i con índice i dentro del intervalo [j-1) L+1j L] se utilizará el bit b_j del vector binario 1⬆*j*⬆*N* correspondiente, siendo 1 j 1 N. Donde b denota a los vectores o para el caso de los mensajes b_{INT} para la información de integridad. El valor i-ésimo se calcula como·

$$y_i = Q_\Delta\left(x_i - \left(\frac{b_i}{2} + k_i\right)\cdot\Delta\right) + \left(\frac{b_i}{2} + k_i\right)\cdot\Delta \qquad \textbf{(1)}$$

donde es el denominado escalón de cuantificación, que determinará la distorsión introducida por el proceso de marcado. Par otra parte, en la expresión anterior (1) k_i representa un valor pseudoaleatorio

distribuido uniformemente en el intervalo [-1/2, 1/2] y es conocido sólo por el codificador y el decodificador; además, denota x_i el resultado de la proyección i-ésima RES_PROY del correspondiente proceso de inserción en una imagen según se lleve a cabo en el módulo de inserción de la dirección IP (FIG. 4), en el de la dirección IP (FIG. 5) o en el de la información de integridad (FIG. 6), y donde representa la operación de cuantificación, que debido a la particular estructura de las palabras código viene dada simplemente por

$$Q_{\Delta}(x) = \Delta \cdot \mathrm{round}\left(\frac{x}{\Delta}\right).$$

La obtención de se representa gráficamente en la FIG. 12, donde los círculos y los cuadrados simbolizan los puntos de reconstrucción que representan a los bits 0 y 1, respectivamente. Respecto al valor pseudoaleatorio k_i, este puede obtenerse a partir de la clave secreta K o bien a partir de la referencia temporal para los mensajes y la clave secreta en el caso de la información de integridad. En general, se utilizará un valor k_i de diferente para cada valor x_i con el fin de proporcionar privacidad al proceso de marcado. El vector formado k_i por los de cada mensaje o información de integridad se representa por k_{IP} para la dirección IP k_{REF}, para la referencia temporal, y k_{INT} para la información de integridad.

El segundo paso del proceso de marcado consiste en la obtención del vector de error de cuantificación d, donde d_i se obtiene simplemente como.

Cada elemento es el resultado de los pasos 124 (FIG. 4), 145 (FIG. 5) y 168 (FIG. 6).

El tercer paso del proceso de marcado es la actualización, operación mediante la cual se dispersa el valor de cada sobre todos los coeficientes de la imagen original que han sido usados para obtener el valor de (que se corresponde con un cierto valor valor RES_PROY). La actualización se lleva a cabo en los pasos 125 (FIG. 4), 146 (FIG. 5) y 169 (FIG. 6). Se supone que los coeficientes de la imagen, que se han usado para obtener mediante la operación de proyección el valor de RES_PROY que ha dado lugar a en el paso anterior, se encuentran dispuestos en el vector $\mathbf{c} = (c_1, c_2 \ldots, c_M)$, donde M es igual a LONG_IP, LONG_REF o LONG_INT, dependiendo de si el mensaje insertado se corresponde con la dirección IP, la referencia temporal, o la información de integridad, respectivamente. La obtención del j-ésimo coeficiente marcado, denotado por c_j^* viene dada por la siguiente expresión:

$$c_j^* = c_j + \alpha \cdot \frac{d_i^*}{p_j}$$

$d_i^* = d_i / M$ es el elemento j-ésimo del vector de proyección correspondiente (es decir, , o), y α es el denominado factor de compensación de distorsión, que puede tomar valores reales en el intervalo [O, 1].

Controlando el valor α se puede llegar a una solución de compromiso entre la distorsión introducida y la robustez de la marca.

Para concluir el proceso de marcado, los coeficientes originales c_j se reemplazan por los coeficientes marcados c_j^*.

Distorsión introducida por JPEG

La imagen digital resultado de alterar los coeficientes en la inserción de información se vuelve a codificar según el estándar JPEG. Corno se indicó anteriormente el estandar JPEG cuantifica los coeficientes de cada bloque 8x8 que forman la imagen por los elementos de la matriz de cuantificación JPEG , introduciendo un ruido de cuantificación.

Es necesario conocer los valores de en el proceso de inserción de la información de la imagen, de modo que se pueda establecer un valor mínimo del tamaño de escalón □ necesario para insertar la información. Este proceso de generación de los elementos de las palabras código y se describe en la expresión (1), denotando cada tamaño de escalón por , y , y, para el caso del mensaje con la dirección IP, mensaje con la referencia temporal y la información de de integridad respectivamente.

La determinación del tamaño de los escalones de los cuantificadores (, y) depende del valor mínimo del tamaño del escalón de cuantificación de ($q_{IP,min}$, $q_{REF,min}$,o $q_{INT,min}$,); este valor divide los coeficientes usados para insertar cada tipo de información. De ese modo se consigue que la comunicación establecida entre el codificador 100 y el decodificador 200 sea posible con una distorsión muy pequeña. La condición que se debe cumplir es

$$\Delta_{IP} \geq 2q_{IP,min},$$
$$\Delta_{REF} \geq 2q_{REF,min}$$
$$\Delta_{INT} \geq 2q_{INT,min}.$$

Respetando esta condición se logra que la información introducida resista la compresión JPEG a un determinado factor de calidad, donde ese factor Q_{JPEG} controla. Esto queda claro con el ejemplo que se describe a continuación. Se supone un factor α =1, sin proyección y el resultado del error de cuantificación para la introducción de un bit, cuyo valor es cero, es el máximo valor posible *d*=Δ/2. El coeficiente marcado resulta $c^* = c + \Delta/2$. Si no se cumpliera la condición anteriormente mencionada, el valor marcado cuantificado obtenido c^*_{quant} sería lor sin marcar cuantificado original por lo tanto en el decodificador 200 produciría un error al recuperar el valor del bit insertado ya que $\hat{c} = c^*_{quant} \times q$ estaría más cerca de una palabra código del subconjunto asociado al valor uno que al de valor cero.

Extracción de la información

EI proceso de extracción de la información insertada es similar al proceso de marcado, y se puede descomponer en dos etapas. Para explicarlo, se parte de un conjunto de vectores de coeficientes

$\mathbf{c} = (c_1, c_2 \ldots, c_M)$, $j = 1 \ldots N$, que han sido marcados para transmitir información acerca del j-esimo bit de un mensaje que tiene una longitud total de N bits, correspondiendose este valor con N°BITS_IP o N°BITS_REF para el caso de la dirección IP y de la referencia temporal respectivamente o el numero de macrobloques de la imagen para la información de integridad. Además, el valor L es la tasa de repetición utilizada, es decir, N°COEF_IP/LONG_IP, N°COEF_REF/LONG_REF y N°COEF_ INT/LONG_INT para la dirección IP, la referencia temporal y la información de integridad respectivamente.

EI primer paso del proceso de decodificación consiste en obtener un vector de distancias $\mathrm{VEC\_DIS} = (v_1, v_2, \ldots, v_N)$. De la proyección del vector c_j usando los parámetros adecuados se obtiene como resultado un vector s_j de longitud L, con 1□ j↑N, y denotamos la concatenación de dichos N vectores como s. EI valor de v_i se obtiene mediante la expresión

$$v_j = \sum_{i=(j-1)\cdot L+1}^{j\cdot L} Q_\Delta(s_i - k_i \cdot \Delta) - s_i + k_i \cdot \Delta,$$

con los valores de y ⚛ definidos anteriormente. EI valor v_j representa el valor absoluto del error de cuantificación de! subvector s_j con el conjunto de palabras código que representan el bit 0 en el j-ésimo bit, donde el conjunto palabras código tiene la forma de! Vector $\big(\Delta(t_1 + k_1), \Delta(t_2 + k_2), \ldots, \Delta(t_L + k_L)\big)$, donde t_i es un número entero y los valores pseudoaleatorios k_i deben corresponderse con los usados en la fase codificación. La operación (2) se lleva a cabo en los pasos 226 (FIG. 7), 246 (FIG. 8) y 264 (FIG. 9). Dependiendo del tipo de mensaje considerado, el siguiente paso en el proceso de decodificación es como se describe a continuación.

Para obtener el j-ésimo bit de la dirección IP (paso 217 de la FIG. 7), la regla de decisión viene dada por

$$\hat{\mathbf{b}} = \begin{cases} 0, \text{si } v_j \le L\Delta/4 \\ 1, \text{si } v_j > L\Delta/4 \end{cases} \qquad \text{b} = \qquad \}$$

esto es, se seguirá un criterio de mínima distancia. EI mensaje relativo a la referencia temporal se codifica contra errores usando un código de canal (p.ej. convolucional). En este caso, el vector de distancias es la entrada al bloque 235 de la FIG. 8, que obtiene a la salida el vector binario $\hat{\mathbf{b}}_{\mathrm{REF}}$, el cual representa el mensaje estimado.

En el sistema propuesto en la presente invención se contempla la detección de alteraciones temporales en las imágenes procesadas por el. Esto ocurre cuando se intenta modificar una imagen o se sustituye una secuencia de imágenes. Se implementa utilizando una ventana temporal compuesta por las referencias temporales válidas que se han de cotejar con la referencia temporal extraída de cada imagen. Si la referencia temporal esta dentro de la ventana, la ventana se actualiza con el valor de la nueva referencia

temporal. Si la referencia temporal extraída no es válida se indica que esa imagen determinada o secuencia de imágenes no es válida.

La información de integridad se extrae en el paso 261 de la FIG. 9. En este paso, se calculará la distancia entre el conjunto de palabras código asociadas a un mensaje de referencia, y la versión proyectada de los coeficientes dedicados a integridad del j-ésimo macrobloque s_j. Si dicha distancia es menor que un determinado umbral, entonces se decidirá que la señal es auténtica, y en otro caso que ha sido editada.

Integración en dispositivos

Nótese que los diagramas de flujo no utilizan ninguna sintaxis especial, ni ningún lenguaje de programación. Más bien, representan la información necesaria para que una persona familiarizada en este campo de la tecnología pueda fabricar circuitos integrados o generar el software que ejecuten los procesos necesarios. Por ejemplo, cada función representada por un bloque o un diagrama de flujo puede ser implementada por un conjunto de instrucciones software, por un procesador digital de serial DSP, por un circuito digital configurable FPGA, por un circuito de aplicación específica ASIC o cualquier combinación de ellos.

Con el fin de ilustrar una posible implementación de los métodos de inserción de marcado de agua propuestos en la presente invención se muestra en la FIG. 13 un esquema de bloques de una cámara digital de red 1300. La cámara comprende una lente 1301 que focaliza un imagen sobre un sensor de imagen 1302, un circuito generador de imágenes 1303 que utiliza la imagen capturada por el sensor de imagen 1303 originando una imagen digital codificada acorde a algún estándar (p.ej. JPEG) y un circuito de control 1304 teniendo como una de sus funciones el control de la obtención, la generación y la codificación de las imágenes, siendo otra de sus funciones la comunicación con una red de comunicaciones 1306. Además, el circuito de control 1304 tiene la capacidad de ejecutar operaciones almacenadas en una memoria 1305, siendo en está donde estan guardadas las operaciones necesarias para llevar a cabo los métodos de inserción propuestos en esta invención. Generalmente, la poca capacidad de cálculo de los circuitos de control presentes en las actuales cámaras digitales de red hacen idónea la presente invención al conjugar perfectamente un elevado grado de seguridad con la necesidad de un número de operaciones bajo.

Los métodos de marcado de agua digital para detección de manipulación propuestos en la presente invención se podrían implementar en un sistema computacional 1400, como se muestra en la FIG. 14, donde tal sistema computacional 1400 comprendería un procesador 1401 y una memoria 1403. Tal sistema de computación 1400 estaría conectado a dispositivos de un sistema de vigilancia 1407 a través de una red comunicaciones digitales 1405. El procesador 1401 ejecuta las operaciones almacenadas en la memoria 1403; por lo tanto los procesos descritos que forman parte de los métodos para la detección de alteraciones pueden ser implementados en estos sistemas computacionales.

A modo de ejemplo, el sistema computacional 1400 podría ser un ordenador central que controla los parámetros de las cámaras digitales que forman el sistema global o, simplemente, un DSP configurado para que de manera aleatoria analice unas grabaciones de una base de datos.

Reivindicaciones

1.- Método de marcado de un documento digital, en particular de una imagen digital, con un marcado de agua digital para la detección de manipulaciones insertando una información (150) de integridad y al menos un mensaje con una pluralidad de bits, donde bloques de la imagen y coeficientes de cada bloque son seleccionados con una clave secreta (K),

caracterizado por que el método comprende los pasos siguientes:

- transformar la imagen digital en una imagen digital transformada,
- dividir la imagen digital transformada en una pluralidad de bloques, teniendo cada bloque una pluralidad de coeficientes;
- generar una pluralidad de valores proyectados de mensaje para el al menos un mensaje proyectando una pluralidad de coeficientes predeterminados sobre un vector dependiente de la clave secreta (K),
- insertar cada bit de cada mensaje al menos en uno de dichos valores proyectados de mensaje;
- generar una pluralidad de valores proyectados de integridad para dicha información de integridad (150) proyectando una pluralidad de coeficientes sobre un vector dependiente de mensaje, siendo dicho vector dependiente de mensaje derivado a partir de al menos uno de dichos mensajes y de la clave secreta (K);
- insertar cada parte de la información de integridad (150) al menos en uno de dichos valores proyectados de integridad;
- actualizar cada coeficiente usado para generar los valores proyectados de mensaje con los valores proyectados insertados de mensaje, logrando que la proyección de los primeros coeficientes actualizados de mensaje sobre el vector dependiente de la clave secreta y los valores proyectados insertados de mensaje sean idénticos;
- actualizar cada coeficiente usado para calcular los valores proyectados de integridad con los valores proyectados insertados de integridad, logrando que la proyección de los coeficientes actualizados de integridad sobre dicho vector dependiente de mensaje y los valores proyectados insertados de integridad sean idénticos;
- el insertar de cada parte de la información de integridad (150) se calcula sometiendo dichos valores proyectados de integridad a una cuantificación empleando un cuantificador de celosía con un tamaño de escalón predeterminado y moviendo los centroides del cuantificador de celosía con un vector de desplazamiento sincronizado con al menos uno de dichos mensajes y la clave secreta (K) ;
- el insertar de cada bit de cada mensaje se calcula sometiendo dichos valores proyectados de mensaje a una cuantificación empleando un cuantificador de celosia con un tamaño de escalón predeterminado y moviendo los centroides del cuantificador de celosía con un vector de desplazamiento sincronizado con la clave secreta (K); y
- sincronizar el insertar y el extraer de la información de integridad (150) por inicialisar un generador de integridad pseudoaleatorio con un valor que es una función de una referencia temporal (130) y de la clave secreta (K).

2.- Método según la reivindicación 1, **caracterizado por** que cada coeficiente de la pluralidad de coeficientes predeterminados usado para insertar los mensajes es seleccionado pseudoaletoriamente con la clave secreta (K).

3.- Método según la reivindicación 1, **caracterizado por** que cada valor de dicho vector dependiente de mensaje teniendo una posición específica en dicho vector dependiente de mensaje y cada valor del vector dependiente de la clave secreta teniendo una posición específica en el vector dependiente de la clave secreta se ponderan por un factor, donde dicho factor se deriva de dicha posición específica de cada valor en el vector.

4.- Método según la reivindicación 3, **caracterizado por** que dicha imagen digital se codifica con un estándar de imagen digital obteniendo una imagen digital codificada, donde dicho estándar de imagen digital es seleccionado del grupo constituido por el estándar JPEG y cualquiera de los estándares MPEG; cada coeficiente se codifica dividiéndolo por un valor de la tabla de cuantificación del estándar, donde dicho valor de la tabla de cuantificación es función de la posición del coeficiente en el bloque concreto al que pertenece; y el valor de cada factor que pondera a un valor concreto del vector dependiente es una función del valor de la tabla de cuantificación que divide a un coeficiente concreto en la imagen codificada, donde dicho coeficiente concreto multiplica dicho valor concreto del vector dependiente al proyectar en los pasos de obtención de las pluralidades de valores proyectados.

5.- Método según la reivindicación 1, **caracterizado por** que uno de dichos mensajes es una referencia temporal (130).

6.- Método según la reivindicación 1, **caracterizado por** que uno de dichos mensajes es un identificador único de un dispositivo, donde dicho dispositivo captura dicha imagen digital.

7.- Método de marcado de un documento digital, en particular de una imagen digital, con un marcado de agua para la detección de manipulaciones extrayendo datos de la imagen digital con marcados de agua, siendo los datos una información (150) de integridad y al menos un mensaje con una pluralidad de bits, en donde bloques de la imagen y coeficientes de cada bloque son seleccionados con una clave secreta (K), **caracterizado por** que el método comprende los pasos siguientes:

- transformar la imagen digital en una imagen digital transformada,
- dividir la imagen digital transformada en una pluralidad de bloques, teniendo cada bloque una pluralidad de coeficientes;
- generar una pluralidad de valores proyectados para cada de los mensajes proyectando una pluralidad de coeficientes sobre un vector dependiente de la clave secreta (K),
- extraer varios bits de cada mensaje de dichos valores proyectados de mensaje;

- para cada mensaje determinar un mensaje reconstruido basado en los bits extraídos de cada mensaje;
- obtener una pluralidad de valores proyectados de integridad para la información de integridad proyectando una pluralidad de coeficientes sobre un vector dependiente de mensaje, el cual se deriva al menos de uno de los mensajes reconstruidos y de la clave secreta (K);
- el extraer una pluralidad de partes de la información de integridad (150) de dicha pluralidad de valores proyectados de integridad;
- determinar si la imagen digital con marcados de agua fue alterada o no analizando las partes extraídas de la información de integridad,
- extraer una pluralidad de partes de la información de integridad (150) se calcula sometiendo dichos valores proyectados de integridad a una cuantificación empleando un cuantificador de celosía con un tamaño predeterminado de escalón y moviendo sus centroides de cuantificador de celosía con un vector de desplazamiento sincronizado con al menos uno de dichos mensajes reconstruidos y la clave secreta (K);
- el extraer una pluralidad de bits de cada mensaje de los valores proyectados se calcula sometiendo dicho valor proyectado de mensaje a una cuantificación empleando un cuantificador de celosía con un tamaño predeterminado de escalón moviendo sus centroides de cuantificador de celosía con un vector de desplazamiento sincronizado con la clave secreta y
- sincronizar el insertar y el extraer de la información de integridad (150) por inicialisar un generador de integridad pseudoaleatorio con un valor que es una función de una referencia temporal (130) y de la clave secreta (K).

8.- Método según la reivindicación 7, **caracterizado por** que cada coeficiente de la pluralidad de coeficientes predeterminados usado para descodificar el mensaje reconstruido es seleccionado pseudoaletoriamente con la clave secreta (K).

9.- Método según la reivindicación 7, **caracterizado por** que cada valor de dicho vector dependiente de mensaje teniendo una posición específica en dicho vector dependiente de mensaje y cada valor del vector dependiente de la clave secreta teniendo una posición específica en el vector dependiente de la clave secreta se ponderán por un factor, donde dicho factor se deriva de dicha posición específica de cada valor en el vector.

10.- Método según la reivindicación 9, **caracterizado por** que dicha imagen digital se codifica con un estándar de imagen digital obteniendo una imagen digital codificada, donde dicho estándar de imagen digital es seleccionado del grupo constituido por el estándar JPEG y cualquiera de los estándares MPEG; cada coeficiente se codifica dividiéndolo por un valor de la tabla de cuantificación del estándar, donde dicho valor de la tabla de cuantificación es una función de la posición del coeficiente en el bloque concreto al que pertenece; y el valor de cada factor que ponderá a un valor concreto del vector dependiente es función del valor de la tabla de cuantificación que divide a un coeficiente concreto en la imagen codificada,

donde dicho coeficiente concreto multiplica dicho valor concreto del vector dependiente al proyectar en los pasos de obtención de las pluralidades de valores proyectados.

11.- Método según la reivindicación 7, **caracterizado por** que uno de dichos mensajes es una referencia temporal (130) que es usada para decidir si la imagen digital con marca de agua fue obtenida en un periodo válido de tiempo o sufrió una manipulación temporal.

12.- Método según la reivindicación 7, **caracterizado por** que uno de dichos mensajes es un identificador único de un dispositivo, donde dicho dispositivo capturó dicha imagen; dicho identificador único es usado para verificar si la imagen digital fue alterada o no.

13.- Cámara digital de red (1300), que está **caracterizada por** que comprende:

- una lente (1301) para focalizar una imagen sobre un sensor de imagen (1302);
- un circuito de generación de imagen (1303) para generar una imagen digital a partir de una imagen capturada por dicho sensor de imagen (1302);
- un circuito de control (1304) para controlar las comunicaciones entre la cámara digital (1300) y la red (1306) a la que está conectada; y dicho circuito de control (1304) está preparado para para llevar a cabo un método acorde con alguna de las reivindicaciones de 1 a 6.

14.- Sistema de computación incluyendo un procesador (1401) y una memoria (1403), **caracterizado por** que está preparado para llevar a cabo un método acorde con alguna de las reivindicaciones de 1 a 6 y/o acorde con alguna de las reivindicaciones de 7 a 12.

15.- Sistema de computación según la reivindicación 14, **caracterizado por** que está integrado en un sistema de video supervisión

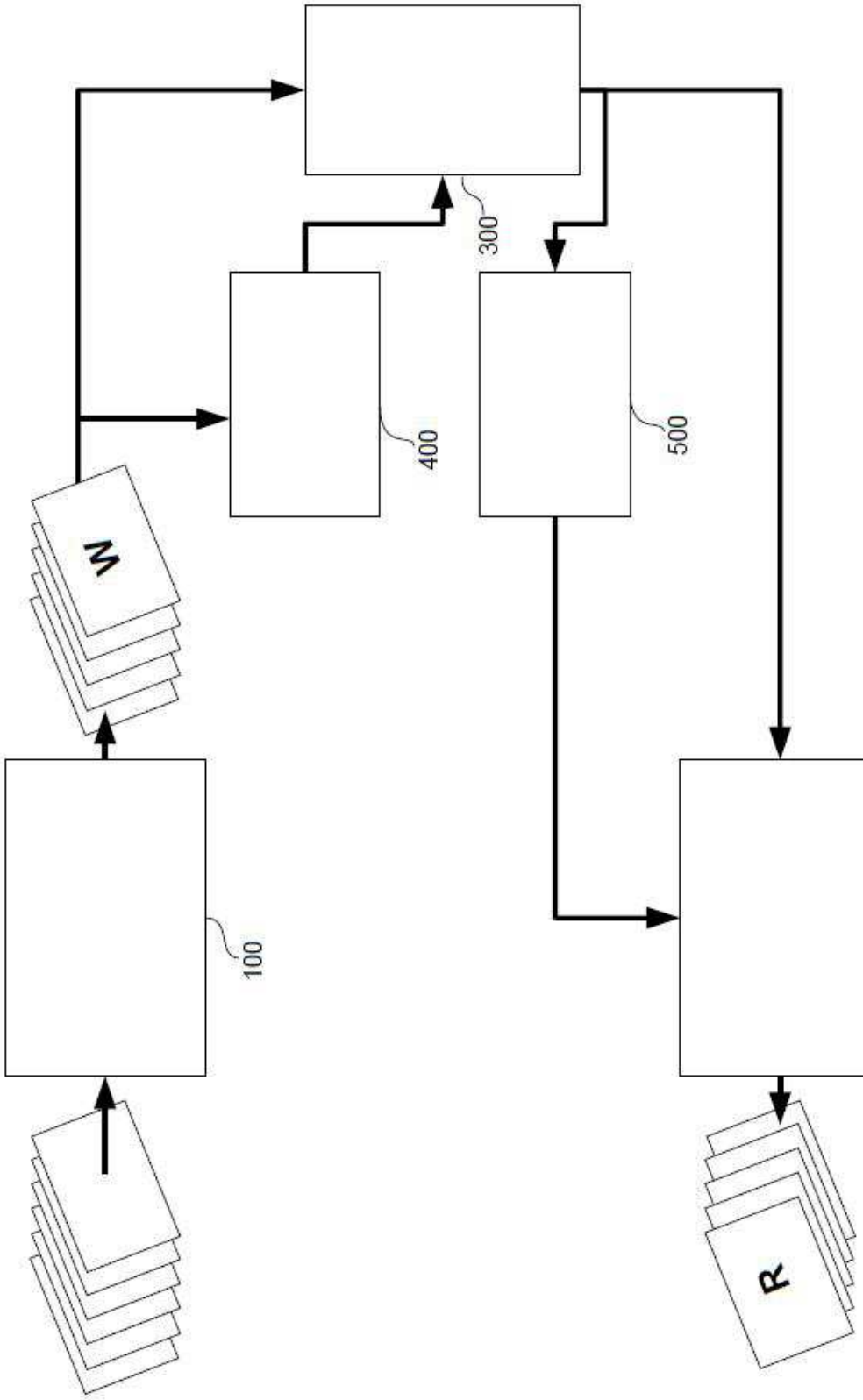

FIG. 1

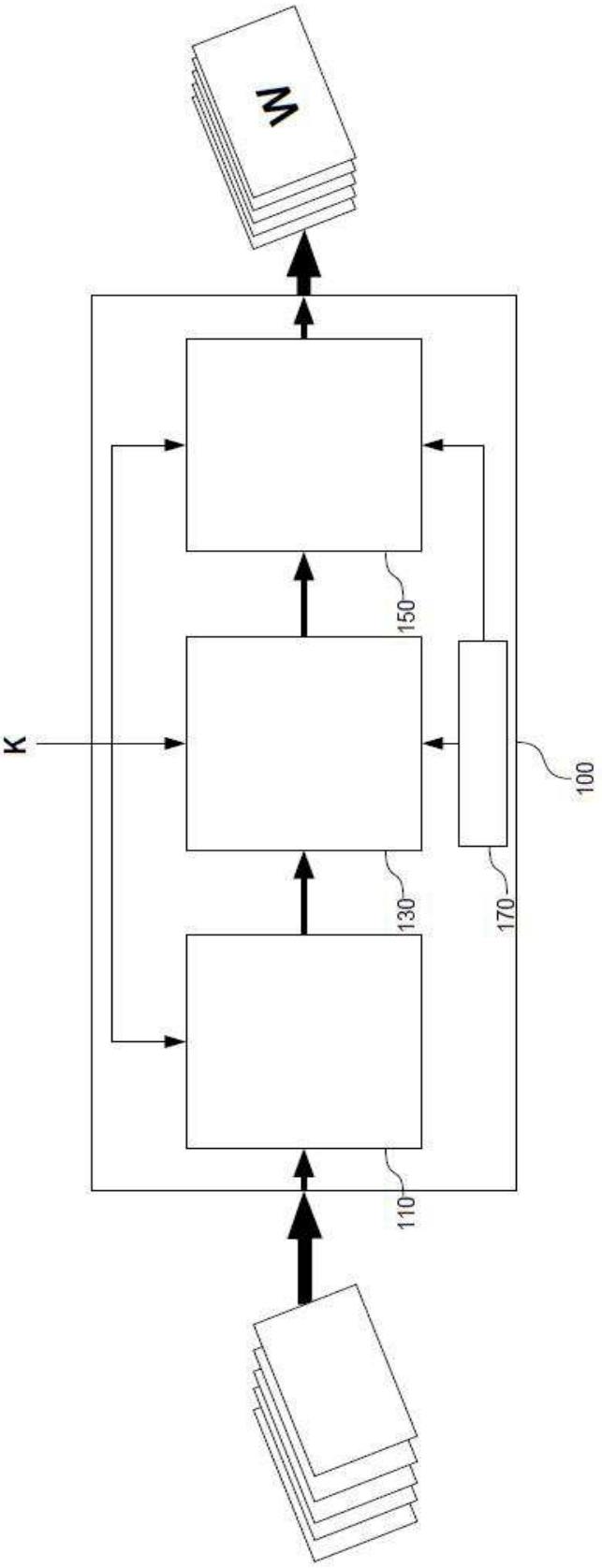

FIG. 2

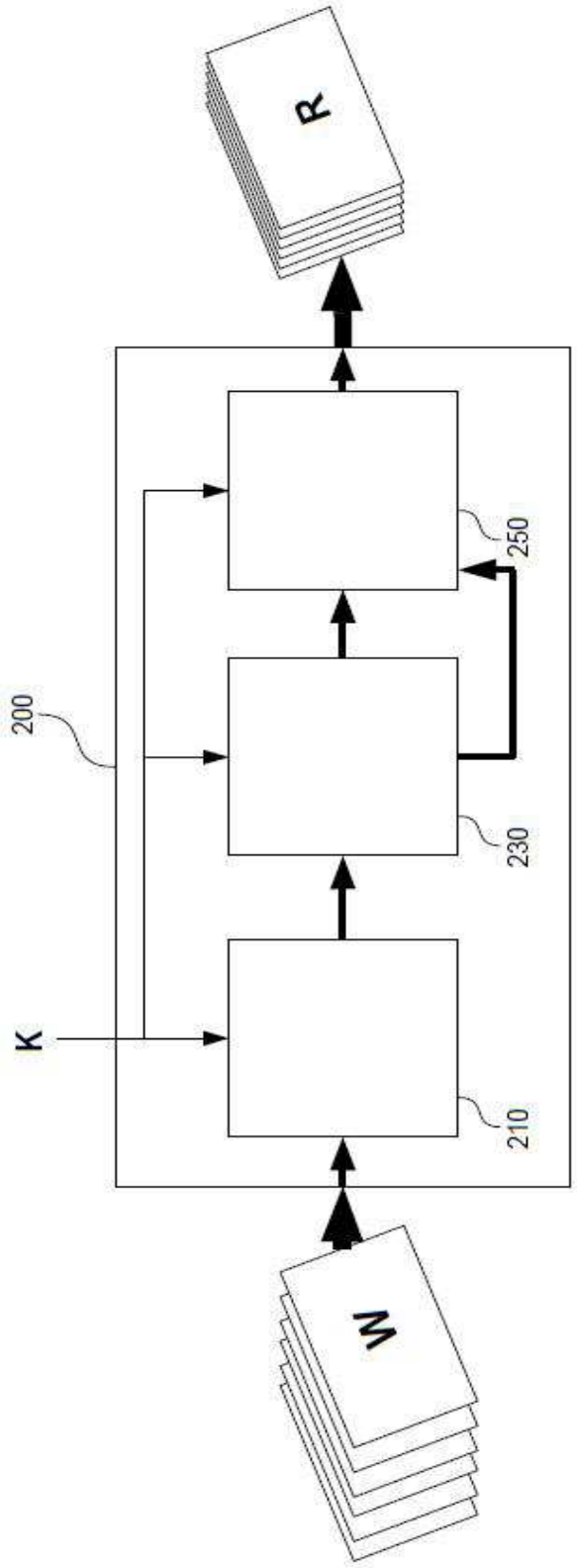

FIG. 3

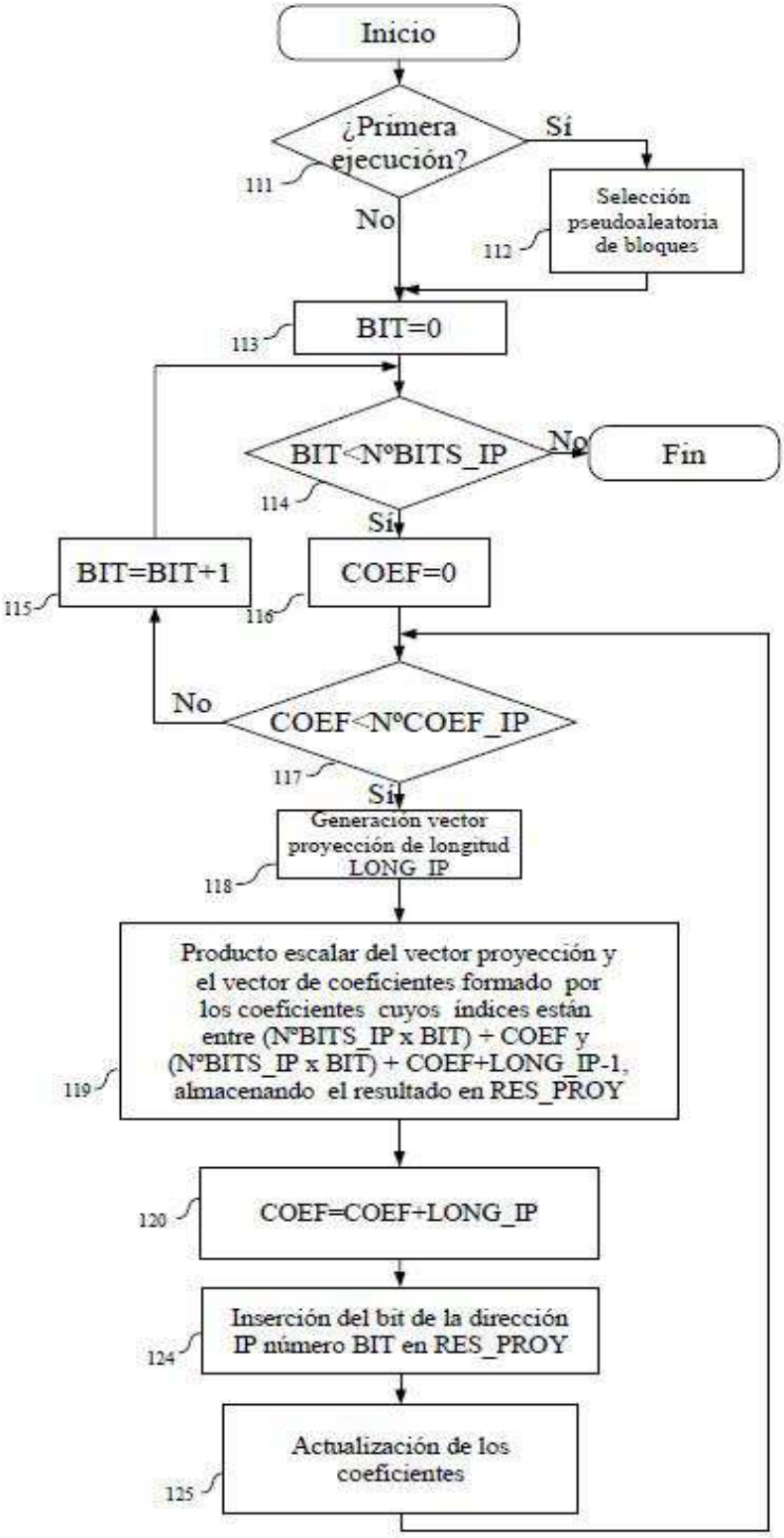
Inicio
¿Primera ejecución?
Sí
No
111
Selección pseudoaleatoria de bloques
112
BIT=0
113
BIT<NºBITS_IP
No
Fin
114
Sí
BIT=BIT+1
115
COEF=0
116
No
COEF<NºCOEF_IP
117
Sí
Generación vector proyección de longitud LONG_IP
118
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes cuyos índices están entre (NºBITS_IP x BIT) + COEF y (NºBITS_IP x BIT) + COEF+LONG_IP-1, almacenando el resultado en RES_PROY
119
COEF=COEF+LONG_IP
120
Inserción del bit de la dirección IP número BIT en RES_PROY
124
Actualización de los coeficientes
125

FIG. 4

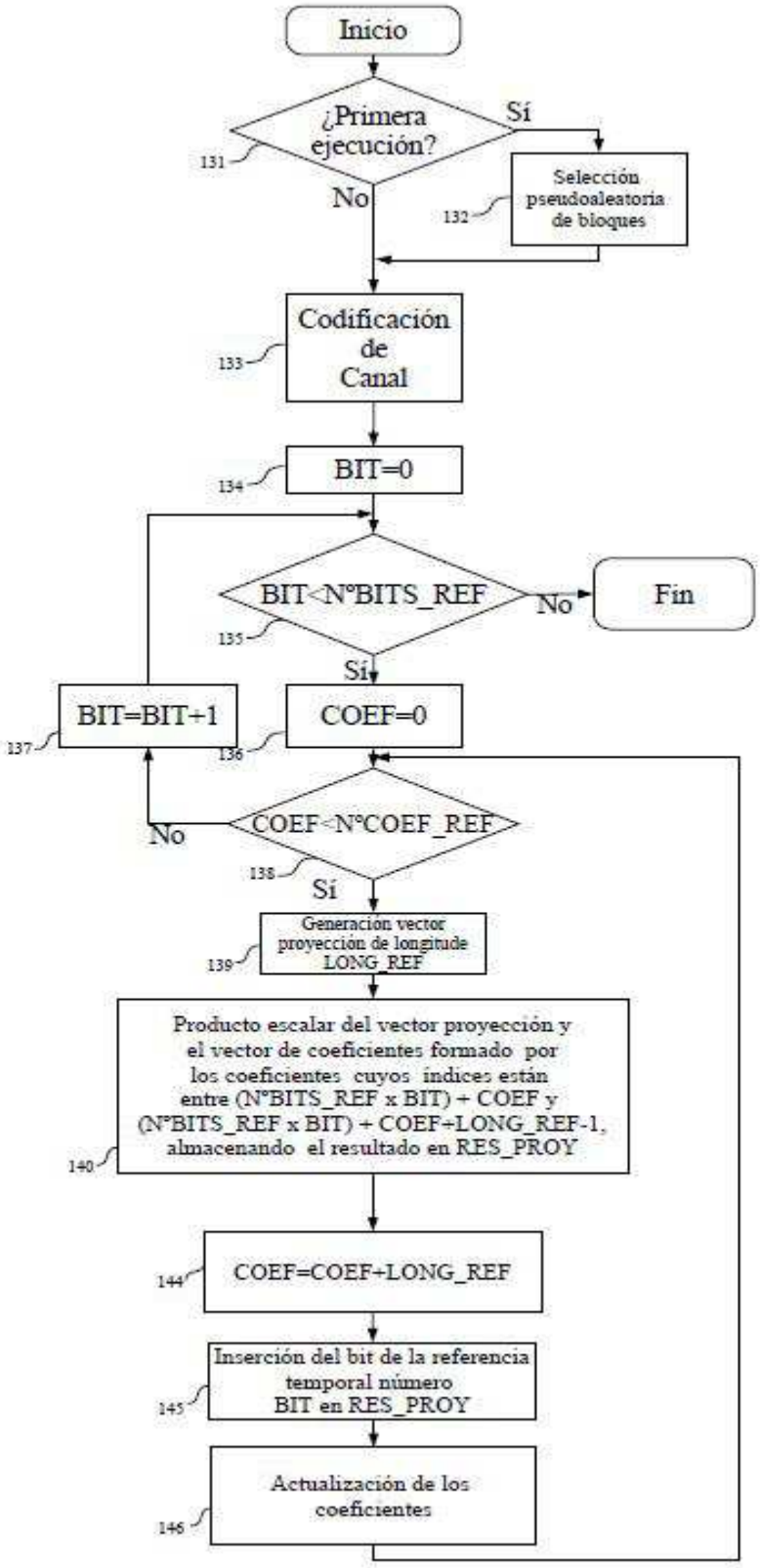
Inicio
¿Primera ejecución?
131
Sí
No
Selección pseudoaleatoria de bloques
132
Codificación de Canal
133
BIT=0
134
BIT<N°BITS_REF
135
No
Fin
Sí
BIT=BIT+1
137
COEF=0
136
No
COEF<N°COEF_REF
138
Sí
Generación vector proyección de longitude LONG_REF
139
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes cuyos índices están entre (N°BITS_REF x BIT) + COEF y (N°BITS_REF x BIT) + COEF+LONG_REF-1, almacenando el resultado en RES_PROY
140
COEF=COEF+LONG_REF
144
Inserción del bit de la referencia temporal número BIT en RES_PROY
145
Actualización de los coeficientes
146

FIG. 5

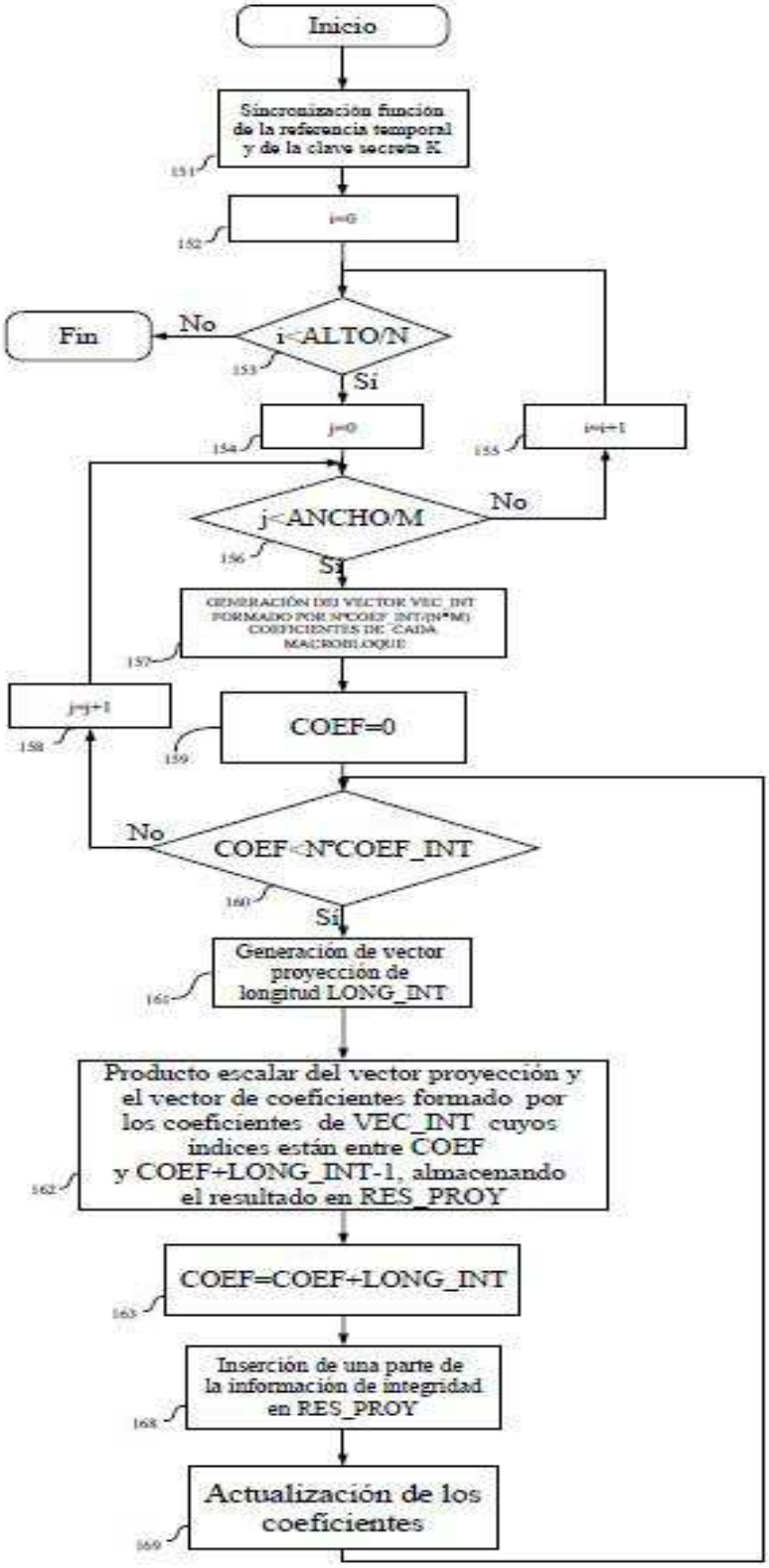
Inicio
Sincronización función de la referencia temporal y de la clave secreta K
151
i=0
152
Fin
No
i<ALTO/N
153
Si
j=0
154
i=i+1
155
j<ANCHO/M
No
156
Si
GENERACIÓN DEL VECTOR VEC_INT FORMADO POR N°COEF_INT·(N*M) COEFICIENTES DE CADA MACROBLOQUE
157
j=j+1
158
COEF=0
159
No
COEF<N°COEF_INT
160
Si
Generación de vector proyección de longitud LONG_INT
161
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes de VEC_INT cuyos índices están entre COEF y COEF+LONG_INT-1, almacenando el resultado en RES_PROY
162
COEF=COEF+LONG_INT
163
Inserción de una parte de la información de integridad en RES_PROY
168
Actualización de los coeficientes
169

FIG. 6

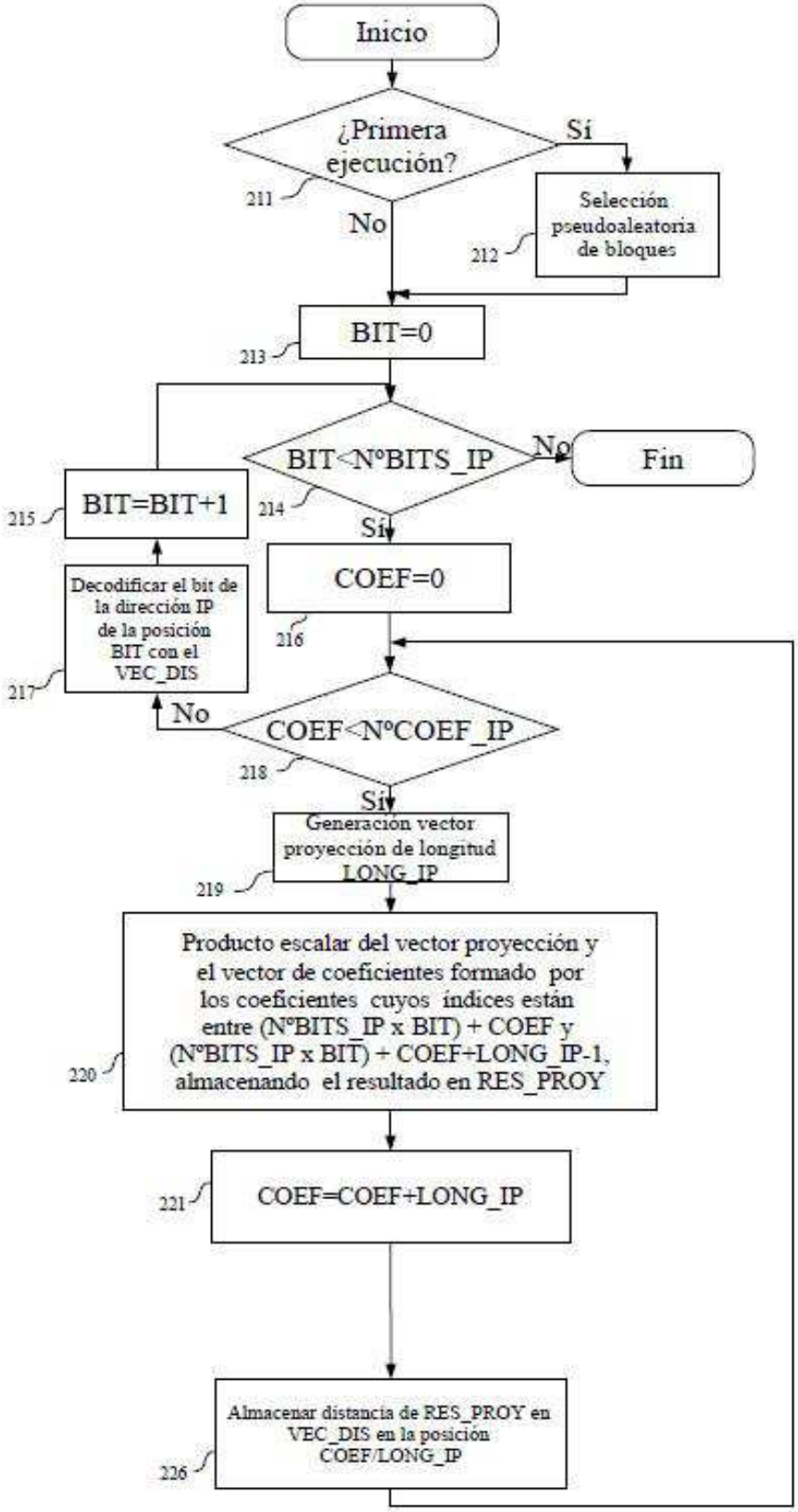
Inicio
¿Primera ejecución?
Sí
No
211
Selección pseudoaleatoria de bloques
212
BIT=0
213
BIT<NºBITS_IP
No
Fin
214
Sí
BIT=BIT+1
215
COEF=0
216
Decodificar el bit de la dirección IP de la posición BIT con el VEC_DIS
217
No
COEF<NºCOEF_IP
218
Sí
Generación vector proyección de longitud LONG_IP
219
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes cuyos índices están entre (NºBITS_IP x BIT) + COEF y (NºBITS_IP x BIT) + COEF+LONG_IP-1, almacenando el resultado en RES_PROY
220
COEF=COEF+LONG_IP
221
Almacenar distancia de RES_PROY en VEC_DIS en la posición COEF/LONG_IP
226

FIG. 7

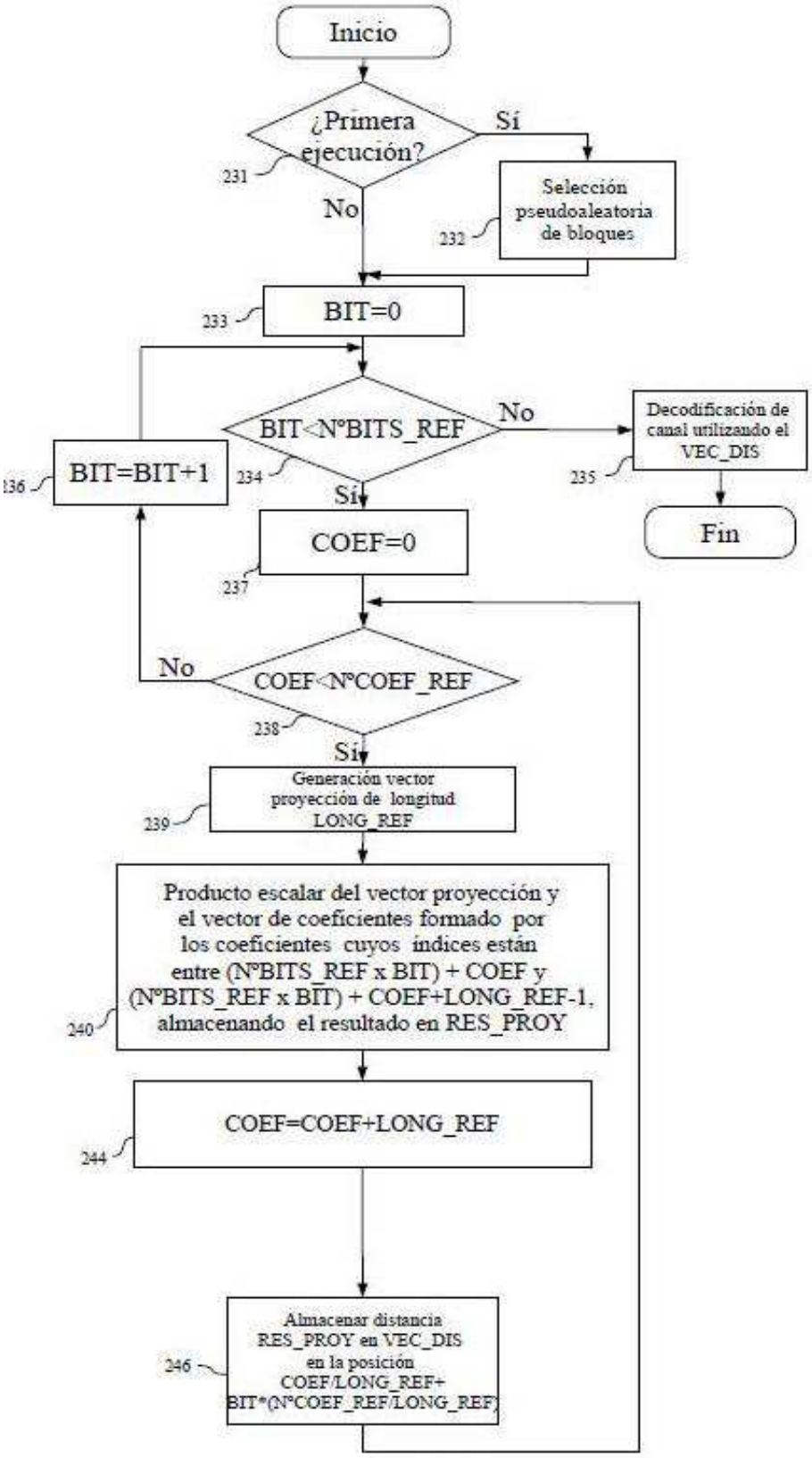
Inicio
¿Primera ejecución?
231
Sí
No
Selección pseudoaleatoria de bloques
232
BIT=0
233
BIT<N°BITS_REF
234
No
Sí
Decodificación de canal utilizando el VEC_DIS
235
Fin
BIT=BIT+1
236
COEF=0
237
No
COEF<N°COEF_REF
238
Sí
Generación vector proyección de longitud LONG_REF
239
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes cuyos índices están entre (N°BITS_REF x BIT) + COEF y (N°BITS_REF x BIT) + COEF+LONG_REF-1, almacenando el resultado en RES_PROY
240
COEF=COEF+LONG_REF
244
Almacenar distancia RES_PROY en VEC_DIS en la posición COEF/LONG_REF+ BIT*(N°COEF_REF/LONG_REF)
246

FIG. 8

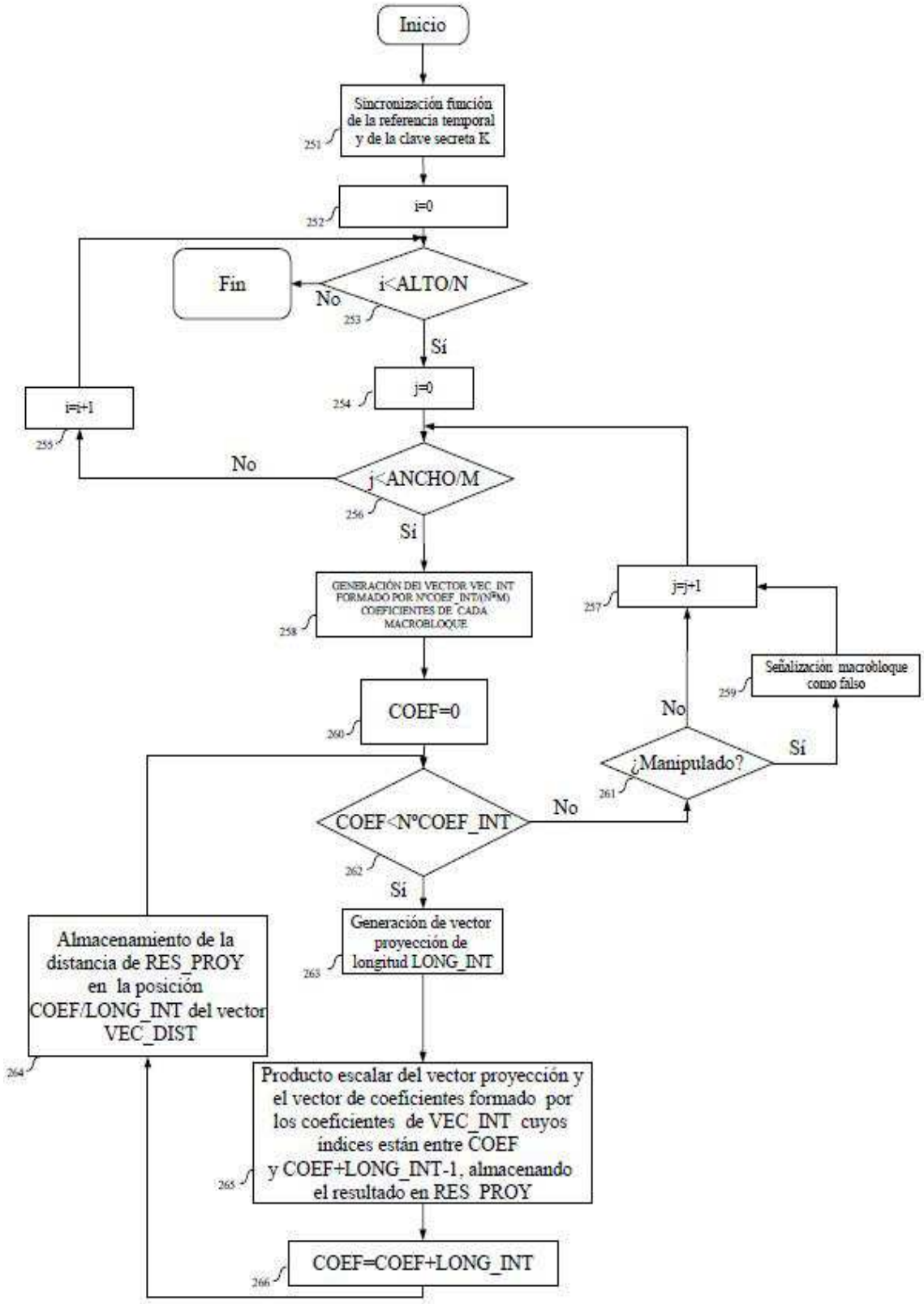
Inicio
Sincronización función de la referencia temporal y de la clave secreta K
251
i=0
252
Fin
No
i<ALTO/N
253
Sí
j=0
254
i=i+1
255
No
j<ANCHO/M
256
Sí
GENERACIÓN DEL VECTOR VEC_INT FORMADO POR N°COEF_INT/(N*M) COEFICIENTES DE CADA MACROBLOQUE
258
j=j+1
257
Señalización macrobloque como falso
259
COEF=0
260
No
¿Manipulado?
261
Sí
COEF<N°COEF_INT
262
No
Sí
Generación de vector proyección de longitud LONG_INT
263
Almacenamiento de la distancia de RES_PROY en la posición COEF/LONG_INT del vector VEC_DIST
264
Producto escalar del vector proyección y el vector de coeficientes formado por los coeficientes de VEC_INT cuyos índices están entre COEF y COEF+LONG_INT-1, almacenando el resultado en RES_PROY
265
COEF=COEF+LONG_INT
266

FIG. 9

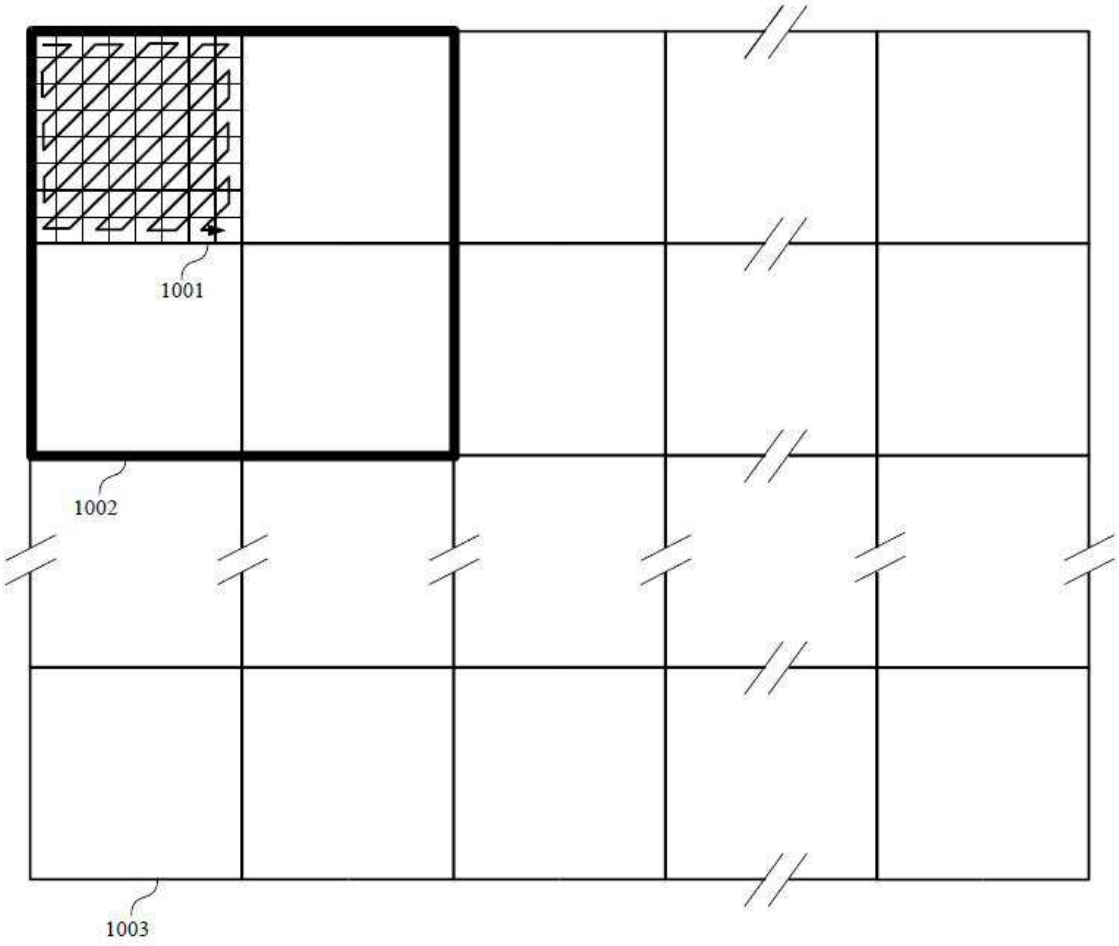

FIG. 10

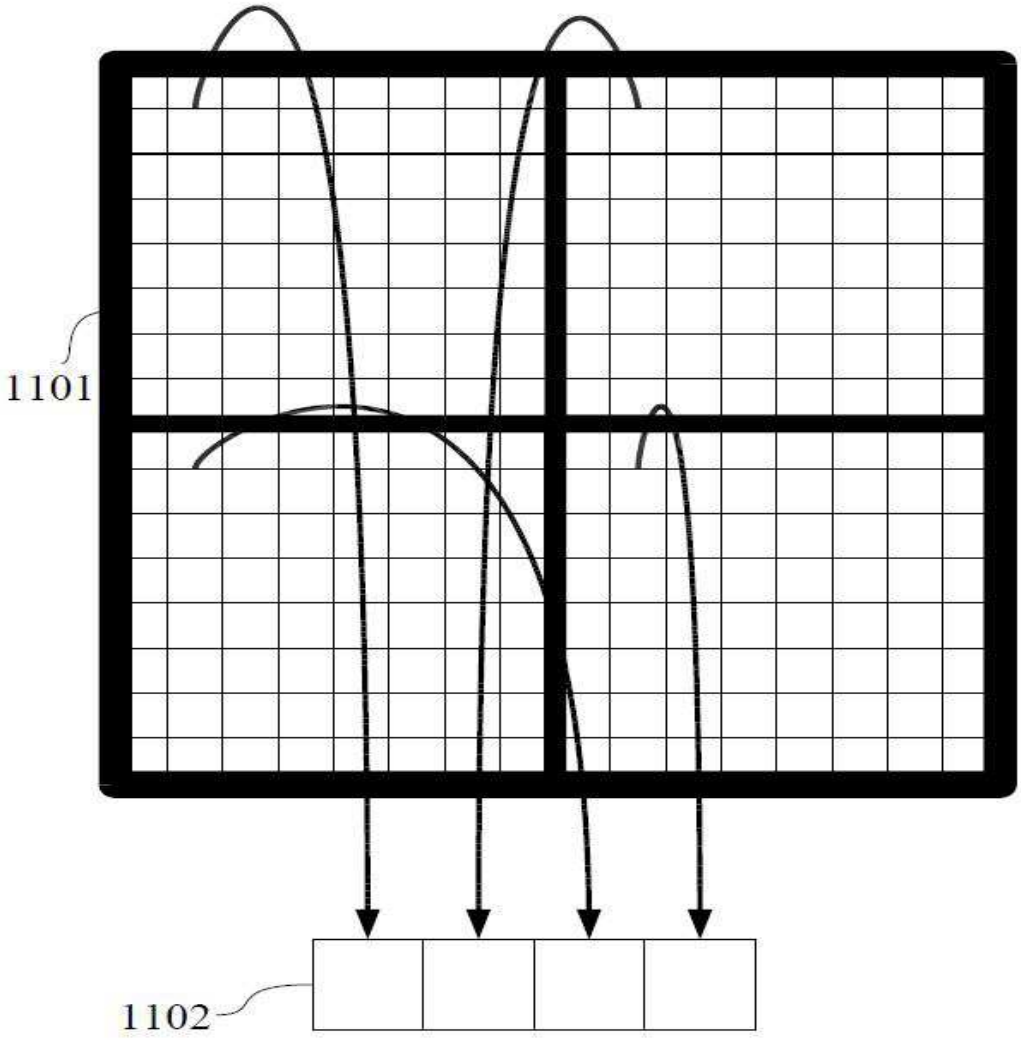

FIG. 11

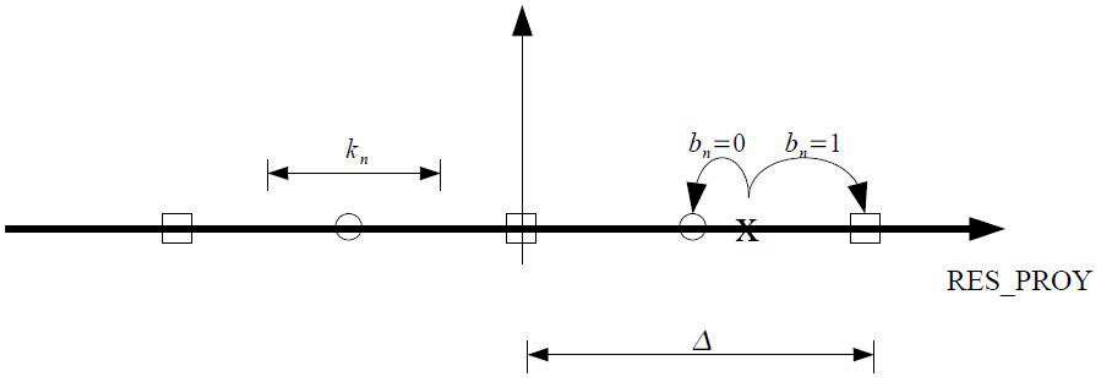

FIG. 12

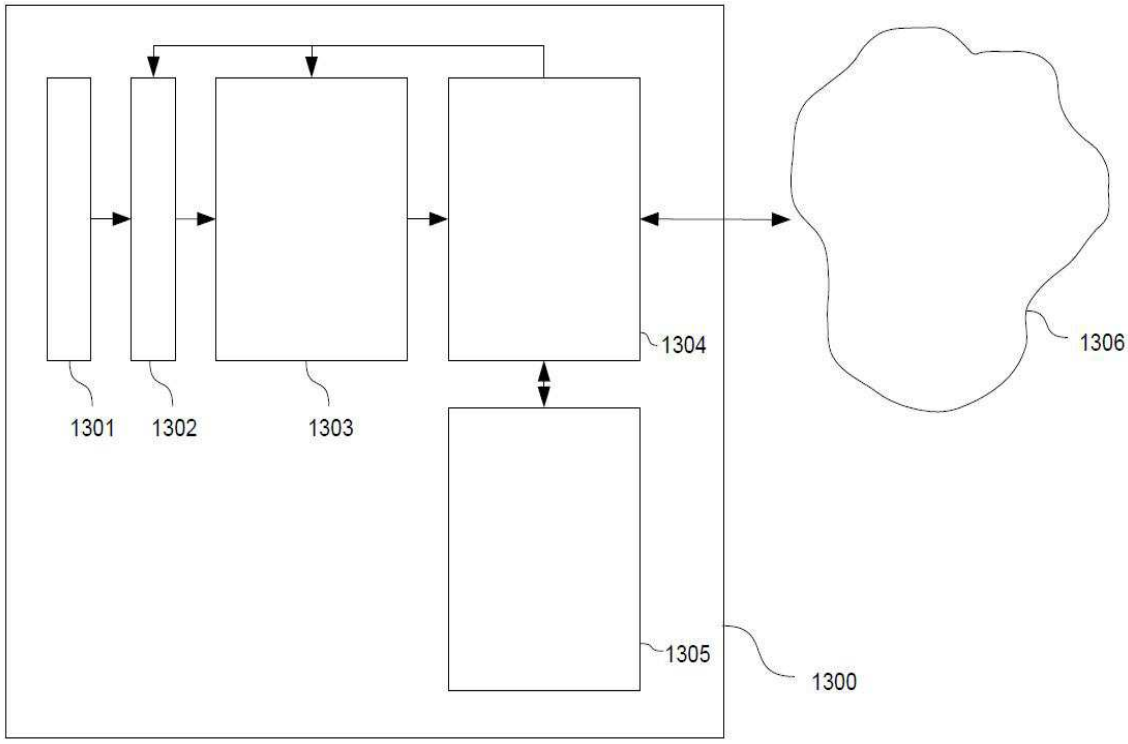

FIG. 13

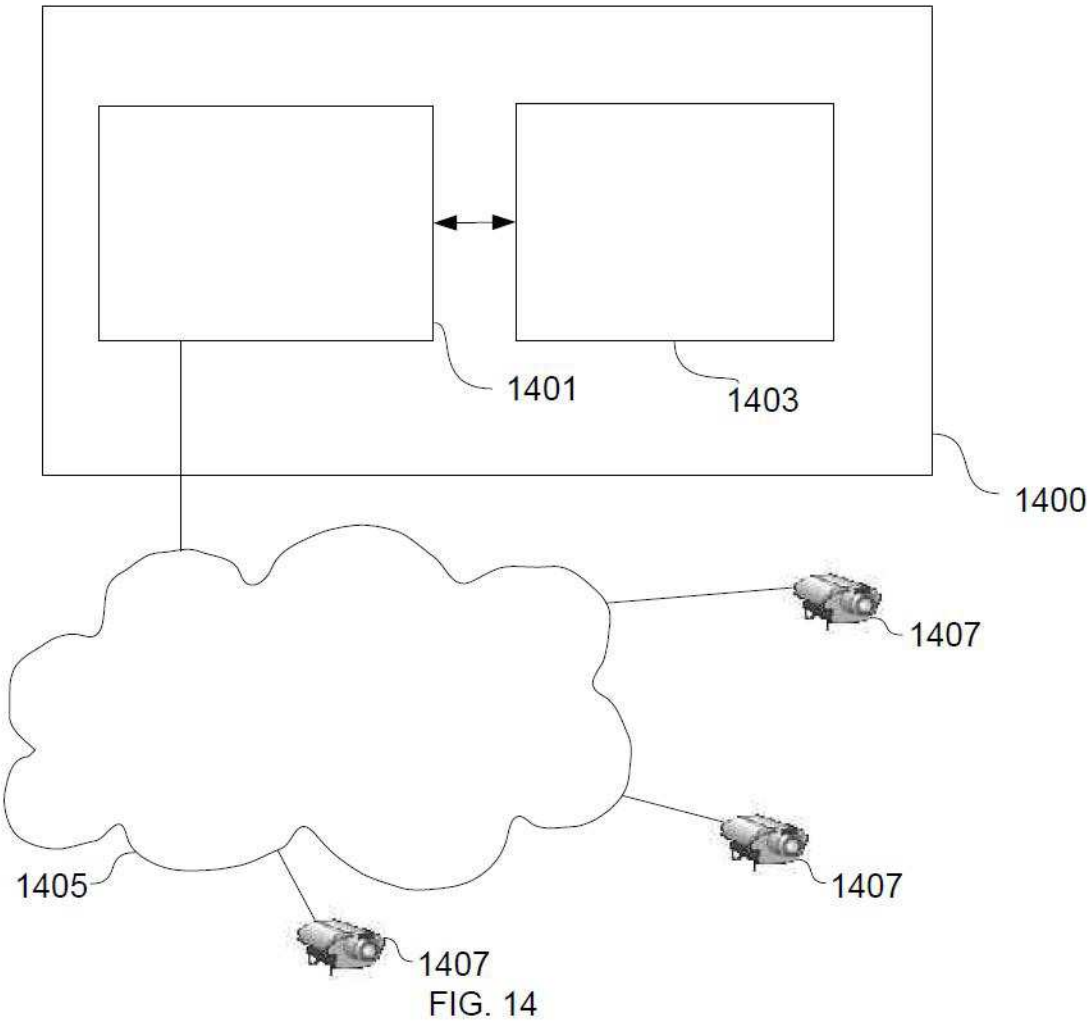

FIG. 14