(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 276 222**

(51) Int. Cl.:
H04L 9/00 (2006.01)
H04N 7/167 (2006.01)
H04H 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04101698 .1**
(86) Fecha de presentación : **28.04.2004**
(87) Número de publicación de la solicitud: **1487147**
(87) Fecha de publicación de la solicitud: **15.12.2004**

(54) Título: **Método, aparato y sistema para encriptar y desencriptar un tren de datos.**

(30) Prioridad: **06.05.2003 CN 03123416**

(45) Fecha de publicación de la mención BOPI:
16.06.2007

(45) Fecha de la publicación del folleto de la patente:
16.06.2007

(73) Titular/es:
International Business Machines Corporation
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es: **Yan, Rong;**
Zhang, Jian y
Xie, Dong

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método, aparato y sistema para encriptar y desencriptar un tren de datos.

Campo técnico

La presente invención se refiere a la encriptación de datos y en particular, a un método y a un aparato para encriptar y desencriptar un tren de datos y a un sistema para hacer segura la transmisión del tren de datos.

Técnica anterior

Con la tendencia a la digitalización de la información de audio y vídeo y el desarrollo de la tecnología informática y de redes, los trabajos digitalizados de audio y vídeo son distribuidos a los usuarios a través de redes en forma de trenes de datos (tales como trenes en formato MPEG o MP3), las cuales han sido ampliamente empleadas. Surge un problema de seguridad con los trenes de datos que se transmiten en un entorno de red.

La protección de un tren de datos en una red es realizada habitualmente por medio de encriptación. Actualmente se han propuesto muchos enfoques para la encriptación de trenes de MPEG, por ejemplo el Algoritmo Naive, el Algoritmo Selectivo, el Algoritmo de Permutación en Zigzag, etc. Estos algoritmos proporcionan una serie de enfoques de encriptación, desde la simple a la compleja, para trenes de datos.

Sin embargo, en estos enfoques tradicionales de la encriptación de trenes de datos, un tren de datos es encriptada habitualmente con una única política sin considerar la situación del receptor, el emisor y el canal entre ellos. Como resultado, o se derrochan los recursos o se degrada la calidad de reproducción de la información.

La solicitud de patente de EEUU 2001/053221 describía una técnica de cifrado en la cual el texto ordinario es dividido en bloques y se establece el atributo de cifrado para cada bloque. Por tanto, el atributo de cifrado puede variar entre bloques.

En primer lugar las operaciones de encriptación y desencriptación consumen fuertemente los recursos del sistema, incluyendo capacidad informática del procesador, espacios de almacenamiento y anchos de banda del emisor y del receptor. Por tanto, si no se puede ajustar en el momento adecuado la intensidad de la encriptación y de la desencriptación para ajustarse al consumo de los recursos del sistema, ni el tren de datos puede obtener mejor protección cuando los recursos no están utilizados por completo ni se puede encriptar y desencriptar el tren de datos en tiempo real y se degrada la calidad de reproducción cuando los recursos están sobreutilizados.

Además, el entorno de red puede variar con el tiempo, dando lugar a frecuentes cambios de calidad de canal. Por ejemplo, la Tasa de Error de Bits (BER), la Tasa de Pérdida de Paquetes (PLR), el retraso en tiempo, etc., de un canal pueden variar grandemente, especialmente en los entornos de la comunicación inalámbrica de redes de área amplia, como Internet. Así, si se adopta la misma política de encriptación para la totalidad del volumen de un tren de datos, se puede degradar la calidad de reproducción, debido a que el receptor no puede recibir suficientes datos para desencriptar a tiempo.

Descripción de la invención

A fin de resolver los problemas anteriormente mencionados en las técnicas existentes, según un aspecto de la presente invención se proporciona un método para encriptar un tren de datos que se transmite de un emisor a un receptor a través de un canal, después de que al menos una parte de la misma haya sido encriptada, comprendiendo dicho método ajustar los atributos de encriptación durante la transmisión, y transmitir dicho tren de datos encriptados e información sobre dichos atributos de encriptación a dicho receptor.

Según otro aspecto de la presente invención, se proporciona un método para encriptar un tren de datos que se transmite de un emisor a un receptor a través de un canal, después de que al menos una parte del mismo haya sido encriptado, comprendiendo dicho método recibir los atributos de encriptación ajustados durante la recepción del tren de datos encriptados, y desencriptar el tren de datos según dichos atributos de encriptación.

Según todavía otro aspecto, se proporciona un aparato para encriptar un tren de datos que se transmite de un emisor a un receptor a través de un canal, después de que al menos una parte del mismo haya sido encriptado, comprendiendo dicho aparato para encriptar: unos medios para ajustar los atributos de encriptación durante la transmisión, y transmitir dicha tren de datos para generar información sobre los atributos de encriptación; y un aleatorizador para realizar la encriptación de dicha al menos parte del tren de datos según los atributos de encriptación ajustados por dichos medios de ajuste de los atributos de encriptación.

Según todavía otro aspecto de la presente invención, se proporciona un aparato para desencriptar un tren de datos que se transmite de un emisor a un receptor a través de un canal, después de que al menos una parte del mismo haya sido encriptada, comprendiendo dicho aparato para desencriptar: una unidad receptora de información de ajuste de encriptación para recibir la información de atributos de encriptación del emisor, y un desaleatorizador para realizar

la desencriptación de dicha tren de datos según la información sobre los atributos de encriptación recibida por dicha unidad de información de ajuste de encriptación.

Según todavía otro aspecto de la presente invención, se proporciona un aparato para enviar un tren de datos de forma segura, que comprende el aparato anteriormente mencionado para la encriptación.

Según todavía otro aspecto de la presente invención, se proporciona un aparato para recibir un tren de datos de forma segura, que comprende el aparato anteriormente mencionado para la desencriptación.

Según todavía otro aspecto de la presente invención, se proporciona un sistema para la transmisión segura de un tren de datos comprendiendo el aparato anteriormente mencionado para enviar un tren de datos, el aparato anteriormente mencionado para recibir un tren de datos, y un canal que conecta dicho aparato para enviar un tren de datos, y dicho aparato para recibir un tren de datos.

Breve descripción de los dibujos

Las anteriores características, ventajas y objetivos de la presente invención resultarán obvios a través de la descripción de las realizaciones preferidas de la presente invención haciendo referencia a los dibujos anexos:

la Figura 1 es un diagrama de flujo que muestra un método para encriptar un tren de datos según una realización de la presente invención;

la Figura 2 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según otra realización de la presente invención;

la Figura 3 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según otra realización de la presente invención;

la Figura 4 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según todavía otra realización de la presente invención;

la Figura 5 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según todavía otra realización de la presente invención;

la Figura 6 muestra esquemáticamente la estructura del sistema para dar seguridad de transmisión del tren de datos en la técnica anterior; y

la Figura 7 muestra esquemáticamente una estructura de un sistema para dar seguridad de transmisión del tren de datos según una realización de la presente invención.

Modo(s) de realizar la invención

A continuación se dará una descripción detallada de las realizaciones preferidas de la presente invención haciendo referencia a los dibujos.

La Figura 1 es un diagrama de flujo que muestra un método para encriptar un tren de datos según una realización de la presente invención.

El proceso para encriptar y desencriptar un tren de datos en la técnica anterior habitualmente incluye: en primer lugar, se predetermina una política de encriptación; a continuación, el emisor encripta la totalidad del tren de datos (Algoritmo Naive) o una parte de ella (Algoritmo Selectivo) según la política y transmite el tren de datos encriptados al receptor a través de un canal que conecta al emisor y al receptor; finalmente, el receptor desencripta los datos recibidos según la política de desencriptación definida y reproduce la información portada por el tren de datos.

Como se muestra en la Figura 1, según la realización de la presente invención, durante el proceso de encriptación y desenciptación del tren de datos, se efectúa una determinación sobre si la complejidad actual es mayor que un umbral de límite superior en la Etapa 105. En la presente realización, la complejidad actual es una medida del consumo de recursos del emisor, el receptor o ambos. La complejidad actual puede ser la carga del procesador o el uso de almacenamiento por el emisor, o una medida de conjunto que tiene en cuenta la carga de los procesadores y el uso tanto por el emisor como por el receptor, según la presente realización.

Si la medida de la complejidad actual incluye el consumo de recursos por el receptor, la información sobre el consumo de recursos por el receptor, tal como la anteriormente mencionada carga del procesador y uso del almacenamiento necesita ser retroalimentada al emisor. Los expertos en la técnica pueden anticipar varios modos de retroalimentar esta información, por ejemplo por medio de paquetes de reconocimiento, un enlace o canal de vuelta separado, etc., la presente invención no tiene limitación especial siempre que el emisor pueda obtener la información sobre el consumo de recursos del receptor.

En los casos en los que el receptor es un dispositivo de terminal con un procesador relativamente débil y un almacenamiento relativamente pequeño, tal como una caja de descodificación de colocación superior, un terminal móvil de telecomunicaciones o elemento análogo, preferiblemente la complejidad actual tiene en cuenta principalmente el consumo de recursos por el receptor, tal como la carga del procesador del receptor. Por consiguiente, el umbral superior predeterminado puede ser, por ejemplo, el 80% de la carga máxima del procesador.

Si la determinación resultante en la Etapa 105 es "Sí" (por ejemplo, la carga del procesador del receptor ha excedido del 80%), entonces el proceso pasa a la Etapa 110, ajustando los atributos de encriptación para reducir el consumo de recursos. Los atributos de encriptación en la presente invención se refieren a aquellos atributos ajustables relacionados con el procesamiento de la encriptación, tales como el algoritmo de encriptación, el modo de encriptación, los parámetros de encriptación, etc. Existen muchos algoritmos para la encriptación de datos conocidos en la técnica, por ejemplo, DES, 3DES, AES, RC4, etc., cada uno de estos algoritmos tiene diferentes modos de encriptación, tales como ECB, CBC, OFB, etc., y algunos de ellos también incluyen parámetros de encriptación, por ejemplo, en el algoritmo de encriptación RC4, se puede escoger diferentes longitudes de claves de encriptación ajustando los parámetros de encriptación. Los diferentes algoritmos de encriptación tienen diferentes intensidades de encriptación en diferentes modos de encriptación o con unos parámetros de encriptación. En consecuencia, los algoritmos con diferentes intensidades tienen diferentes consumos de recursos del sistema (tales como carga de procesador, uso de almacenamiento, etc.).

La presente realización utiliza los atributos de encriptación para ajustar las intensidades de encriptación, haciendo así la encriptación del tren de datos adaptada a la condición de consumo de recursos en el receptor o en el emisor, y a la condición del canal (que se describe más adelante), de manera que se puede alcanzar un equilibrio entre los recursos del sistema, la seguridad de los datos (intensidad de encriptación) y la calidad de la reproducción de la información transmitida. Por ejemplo, en la Etapa 110, los recursos informáticos usados por la encriptación y la desenciptación pueden ser reducidos por el cambio del algoritmo de encriptación de "3DES" a "DES" o acortando la longitud de la clave de encriptación, como resultado de lo cual se puede reducir el consumo de recursos.

A continuación, si el resultado de la determinación en la Etapa 105 es "No", el proceso pasa a la Etapa 115, determinando si la complejidad actual es menor que un umbral inferior predeterminado. En esta realización, el umbral inferior es un 50% de la carga máxima del procesador.

A continuación, si el resultado de la determinación en la Etapa 115 es "Sí", el proceso pasa a la Etapa 120, en la cual se ajustan los atributos de encriptación para aumentar la intensidad de encriptación.

A través de las Etapas 115 y 120, el método de la presente invención utiliza plenamente los recursos del sistema para garantizar la seguridad de los datos. Si el consumo de recursos del sistema mejora, por ejemplo cuando la carga del procesador en el receptor se ha reducido por debajo del 50%, se ajustarán los atributos de encriptación para aumentar la intensidad de encriptación.

A continuación, si el resultado de la determinación en la Etapa 115 es "No", o después de la Etapa 110 ó de la Etapa 120, el proceso pasa a la Etapa 125, determinando si la BER del canal ha aumentado en un valor predeterminado. Si el resultado de la determinación de la Etapa 125 es "Sí", se puede realizar la Etapa 130, en la que se ajustan los atributos de encriptación para reducir la longitud de propagación de error de la encriptación.

Si el resultado de la determinación en la Etapa 125 es "No", se realizará la Etapa 135, determinando si la BER del canal ha disminuido en un valor predeterminado. Si el resultado de la determinación de la Etapa 135 es "Sí", se realizará la Etapa 140, en la que se ajustan los atributos de encriptación para aumentar la longitud de propagación de error de la encriptación.

En la presente aplicación, la longitud de propagación de error se refiere al intervalo afectado de los datos desencriptados. Habitualmente, la longitud de propagación de error se puede ajustar cambiando el modo de encriptación, por ejemplo, en el modo de Bloque de Código Electrónico (ECB) los datos a codificar se dividen en bloques, el tamaño de cada bloque es el mismo que la longitud de la clave de encriptación, y se encripta cada bloque con la misma clave de encriptación, por tanto la longitud de propagación de error del ECB es igual a la longitud de la clave de encriptación, es decir, un bloque. En el modo de Encadenamiento de Bloques de Cifrado (CBC) en primer lugar el texto claro es también dividido en bloques de longitud fija (tal como 64 bits), luego se realiza una operación de XOR entre la salida de código encriptada del bloque encriptado previo y el bloque de código claro a encriptar, se encripta el resultado de la operación XOR con la clave de encriptación para obtener el código encriptado, por tanto la longitud de propagación de error es igual a la longitud de los dos bloques, el Modo de Retroalimentación Cifrada (CFB), el Modo de Retroalimentación de Salida (OFB), etc., tienen características de propagación de error diferentes. Adicionalmente a los modos de encriptación, los diferentes algoritmos de encriptación pueden causar también diferentes longitudes de propagación de error, por ejemplo, si se usa un algoritmo de encriptación como el RC4, la longitud de propagación de error sería muy pequeña, la cual es sólo igual al propio error.

Generalmente, cuanto mayor es la longitud de propagación de error, es decir, más fuertemente se asocian los datos encriptados entre sí, más difícil es fraccionar los datos, así que la seguridad es mejor, al mismo tiempo, sin embargo, es más alta la calidad de canal requerida. Durante la transmisión, el método de la presente realización ajusta la longitud de propagación de error en base a la calidad de canal actual, para equilibrar entre la calidad de canal, la seguridad de los datos y la calidad de reproducción de la información transmitida.

Alternativamente, en la Etapa 135 y en las Etapas 130, 140, se puede hacer la determinación para ajustar el modo de encriptación comparando la BER del canal con un conjunto de umbrales predeterminados, por ejemplo, cuando la BER actual es 10E-4, se escoge el modo CBC, y cuando empeora la calidad de canal y aumenta la BER actual para ser 10E-3, se puede usar el modo ECB para reducir la propagación de error en la capa de encriptación.

Como se muestra en la Figura 1, si el resultado de la determinación en la Etapa 135 es "No", o después de las Etapas 130 ó 140, se realizará la Etapa 145, en la cual se transmiten al receptor los atributos de encriptación ajustados y el tren de datos encriptados correspondiente. Si se han ajustado los atributos de encriptación, es necesario informar al receptor de la información ajustada, a fin de que el receptor realice correctamente la desenciptación. En la presente realización, se registra la información sobre los atributos de encriptación en el encabezamiento del paquete de datos para el tren de datos en forma de metadatos; preferiblemente la información de los atributos de encriptación es también encriptada. La siguiente Tabla 1 muestra a título de ejemplo el contenido de la información sobre los atributos de encriptación según la presente realización.

TABLA 1

Contenido de la información de atributos de encriptación

Campo	Valor
Algoritmo de encriptación	3DES
Modo de Encriptación	CBC
Parámetro de Encriptación	Ninguno

Por supuesto, se pueden usar otros muchos enfoques para transmitir la información de atributos desde el emisor al receptor, la presente invención no está limitada a la anterior realización, por ejemplo, es también posible transmitir la información de atributos de encriptación al receptor con un paquete de datos separado o incluso a través de otro canal.

Con el método anterior de la presente invención, durante la encriptación, la transmisión y la recepción, se ajusta la política de encriptación según el consumo de recursos y la calidad del canal, y se encripta adecuadamente el tren de datos bajo la condición de asegurar el funcionamiento de rutina de los sistemas del emisor y del receptor, pudiéndose lograr de este modo el estado óptimo de equilibrio entre las prestaciones del sistema, la seguridad de los datos y la calidad de reproducción de los datos.

Adicionalmente, según otra realización de la presente invención, se proporciona un método adecuado para encriptar un tren de vídeo comprimido. Los métodos de compresión de vídeo actualmente usados registran habitualmente los datos de vídeo como tres clases de datos de trama, es decir, datos de trama-I, datos de trama-P y datos de trama-B. Entre ellos, una trama-I (Intratrama) registra una imagen completa independiente; una trama-P (Trama de Predicción) sólo contiene la diferencia entre el cuadro de la trama presente y la imagen previamente descomprimida. Una trama-B (Trama de Predicción Bidireccional) tiene el mismo principio de la trama-P, pero adicionalmente a hacer referencia a la imagen previamente descomprimida, se puede hacer referencia también a la imagen subsiguiente no comprimida. Puesto que no es necesario almacenar la imagen completa, se ahorra en gran medida espacio de almacenamiento. Generalmente, el orden de tramas en un tren de datos MPEG es IBBPBBPBBPBBPbbIBBIPBBP.....

Desde el punto de vista de la seguridad de los datos, la importancia relativa de estas tres clases de datos de trama es sucesivamente trama-I>trama-P>trama-B>. Esto se debe a que si sólo se obtienen datos de trama-P o datos de trama-B sin datos de trama-I correctamente desencriptados, no se puede reproducir correctamente la totalidad del tren de datos. En la presente realización, aprovechando las características de un tren de vídeo comprimido, se ajustan los atributos de encriptación con respecto a las tres clases de datos de trama respectivamente, de modo que el tren de datos puede ser encriptada más eficientemente.

La Figura 2 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según otra realización de la presente invención. Las diferencias entre esta realización y la realización previa son la etapa de ajustar los atributos de encriptación para reducir el consumo de recursos (es decir, la Etapa 110 de la Figura 1) y la etapa de ajustar los atributos de encriptación para elevar la intensidad de encriptación (es decir, la Etapa 120 de la Figura 1). La Figura 2 muestra el flujo detallado de la etapa para ajustar los atributo de encriptación a fin de reducir el consumo de recursos (Etapa 110) en el método para encriptar un tren de datos según la presente realización.

Como se muestra en la Figura 2, si el resultado de la determinación en la Etapa 105 (Figura 1) es "Sí", se hace una determinación en primer lugar sobre si la intensidad de encriptación de la trama-B ha alcanzado la intensidad de encriptación menor en la Etapa 205. Si el resultado de la determinación de la Etapa 205 es "No", se realizará la Etapa

210 para reducir la intensidad de encriptación de los datos de la trama-B, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es "Sí", se realizará la Etapa 215, determinando si la intensidad de encriptación de los datos de la trama-P ha alcanzado la menor intensidad de encriptación.

A continuación, si el resultado de la determinación de la Etapa 215 es "No", el proceso pasa a la Etapa 220, reduciendo la intensidad de encriptación de los datos de la trama-P, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es "Sí", se realizará la Etapa 225, determinando si la intensidad de encriptación de los datos de la trama-I ha alcanzado la menor intensidad de encriptación.

A continuación, si el resultado de la determinación de la Etapa 225 es "No", se realizará la Etapa 230, reduciendo la intensidad de encriptación de los datos de la trama-I, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es "Sí", esto significa que las intensidades de encriptación para los datos de los tres tipos de tramas ha alcanzado el menor valor. En ese caso, la encriptación y la transmisión pueden esperar hasta que se hayan recuperado los recursos del sistema o se haya llevado a cabo el proceso con las menores intensidades de encriptación.

Aquí, la intensidad de encriptación se refiere al grado de dificultad para fraccionar los datos encriptados según atributos de encriptación concretos, lo cual habitualmente se asocia con la complejidad del algoritmo de encriptación, la complejidad del modo de encriptación, la complejidad de la clave de encriptación y elementos análogos, y el aumento de la intensidad de encriptación conduciría habitualmente al aumento del consumo de recursos del sistema. La siguiente Tabla 2 muestra a título de ejemplo una lista de combinaciones de métodos de encriptación y de modos de encriptación comúnmente usados en la técnica anterior, y su comparación.

TABLA 2

Una comparación de intensidades de encriptación

Rango de intensidad	1	2	3	4	5	6
Atributos de encriptación	AES (CBC)	3DES (CBC)	AES (ECB)	3DES (ECB)	DES (CBC)	DES (ECB)

En la presente realización, se pueden establecer las menores intensidades de encriptación para diversas clases de datos en trama, respectivamente. Preferiblemente, las menores intensidades de encriptación se hacen sucesivamente más bajas para los datos de trama-I, los datos de trama-P y los datos de trama-B. Y la intensidad de encriptación más baja puede ser cero, es decir, ausencia de encriptación. Por ejemplo, según el establecimiento de una realización preferida, la intensidad de encriptación más baja para las tramas-I es DES (CBC), la intensidad de encriptación más baja para las tramas-P es DES (ECB), y la intensidad de encriptación más baja para las tramas-B es "ausencia de encriptación". Así, en los casos de consumo de recursos relativamente grande, cuando se ajustan todas las intensidades de encriptación al mínimo según el método de la presente realización, es también posible asegurar una protección suficiente para las tramas-I que tienen una elevada importancia, con lo cual se garantiza la seguridad de toda el tren de datos de vídeo, en cuyo caso el consumo de recursos del sistema para la encriptación se reduce significativamente y la calidad de reproducción se asegura debido a la reducción de las intensidades de encriptación de las tramas-P y tramas-B.

La Figura 3 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según otra realización de la presente invención, mostrando en particular el flujo detallado de la etapa para ajustar los atributos de encriptación a fin de elevar la intensidad de encriptación (Etapa 120) en un método para encriptar un tren de datos según la presente realización.

Como se muestra en la Figura 3, si el resultado de la determinación en la Etapa 115 (Figura 1) es "Sí", se hace una determinación en primer lugar sobre si la intensidad de encriptación de los datos de la trama-I ha alcanzado la intensidad de encriptación más elevada en la Etapa 305. Si el resultado de la determinación de la Etapa 305 es "No", se realizará la Etapa 310 aumentando la intensidad de encriptación de los datos de trama-I, luego se realizará la etapa siguiente del método (Etapa 125 en la Figura 1); si es "Sí", se realizará la Etapa 315, determinando si la intensidad de encriptación de los datos de trama-P ha alcanzado la intensidad de encriptación más alta.

A continuación, si el resultado de la determinación de la Etapa 315 es "No", se realizará la Etapa 320, aumentando la intensidad de encriptación de los datos de la trama-P, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es "Sí", se realizará la Etapa 325, determinando si la intensidad de encriptación de los datos de la trama-B ha alcanzado la intensidad de encriptación más alta.

A continuación, si el resultado de la determinación de la Etapa 325 es "No", se realizará la Etapa 330, aumentando la intensidad de encriptación de los datos de la trama-B, luego se realizará la etapa siguiente del método (Etapa 125

de la Figura 1); si es "Sí", esto significa que las intensidades de encriptación para los datos de los tres tipos de tramas ha alcanzado los valores más altos. En ese caso, simplemente continúa el proceso.

De manera similar, se puede también establecer las intensidades de encriptación más altas para los datos de diferentes tramas, respectivamente, pero en esta realización se establece la misma intensidad de encriptación más alta, tal como AES (CBC), para todas las tramas.

De forma correspondiente, la siguiente Tabla 3 muestra a título de ejemplo el contenido de la información sobre atributos de encriptación según la presente realización.

TABLA 3

Contenido de la información de atributos de encriptación

Campo	Valor
Algoritmo de encriptación para tramas-I	3DES
Modo de encriptación para tramas-I	CBC
Parámetro de encriptación para tramas-I	Ninguno
Algoritmo de encriptación para tramas-P	DES
Modo de encriptación para tramas-P	CBC
Parámetro de encriptación para tramas-P	Ninguno
Algoritmo de encriptación para tramas-B	Ninguno
Modo de encriptación para tramas-B	Ninguno
Parámetro de encriptación para tramas-B	Ninguno

Según esta realización, cuando se alivia el consumo de recursos del sistema, se puede aumentar las intensidades de encriptación en el orden de trama-I, trama-P y trama-B, haciendo de esta forma que se maximice la seguridad de los trenes de datos encriptados dentro del límite de recursos del sistema.

Aunque se usan diferentes algoritmos de encriptación para diferentes tipos de tramas de vídeo en la presente realización, también se pueden usar diferentes algoritmos para el mismo tipo de tramas de vídeo en base a su importancia en la práctica. Por ejemplo, para las tramas-P, una trama-P situada en una posición precedente dentro de un GOP (Grupo de Imágenes) es más importante que otra trama-P situada en una posición siguiente dentro del GOP, de manera que se puede usar la intensidad de encriptación más elevada para la trama-P precedente dentro de un GOP.

Además, aunque en la presente invención se ajustan los atributos de encriptación según la importancia relativa de la trama I, la trama-P y la trama-B, no se limita el ajuste sólo a este modo. Por ejemplo, la intensidad de encriptación más baja para las tramas-I se establece en "ausencia de encriptación", la intensidad de encriptación más baja para las tramas-P se establece en DES (ECB); la intensidad de encriptación más baja para las tramas-B se establece en DES (CBC); y la intensidad de encriptación más alta para las tramas-I se establece en "ausencia de encriptación", la intensidad de encriptación más alta para las tramas-P se establece en 3DES (CCB); la intensidad de encriptación más alta para las tramas-B se establece en AES (CBC); al mismo tiempo, en las etapas que se muestran en la Figura 2, las intensidades de encriptación aumentan en el orden de trama-B > trama-P > trama-I. De este modo, aquellos receptores que no han obtenido permiso pueden ver imágenes intermitentes, esto es, trama-I, pero no pueden ver el vídeo completo, esto es una ventaja para aquellos proveedores de servicio que quieren atraer más usuarios y obtienen asimismo una protección fiable.

Con el método de esta realización, las intensidades de encriptación se pueden ajustar con mayor precisión para diferentes porciones del tren de datos, de manera que se puede equilibrar de forma óptima el consumo de recursos y la seguridad. Debido a la utilización de la relación dependiente entre los tipos de tramas en el sistema de vídeo comprimido, es posible reducir la intensidad de compresión para una parte de los datos significativamente, con lo cual se ahorra los recursos del sistema tanto del receptor como del emisor. Además, por medio de la selección de las intensidades de encriptación más alta y más baja para los datos de diferentes tipos de tramas, se puede obtener diversos resultados que constituyen una ventaja para los proveedores de trenes de datos.

Según todavía otra realización de la presente invención, se proporciona un método para encriptar un tren de datos en capas. La técnica para dividir el tren de datos comprimidos en capas es ampliamente utilizada en este campo. Por ejemplo, según MPEG-2 y normas posteriores, se divide un tren de datos en una capa de base y una o más capas de mejora. Entre ellas, la capa base proporciona una resolución de vídeo relativamente baja y puede ser descodificada y

reproducida independientemente, y la capa de mejora proporciona una resolución más alta y necesita ser descodificada basada en la capa de base. En el caso de tener una pluralidad de capas de mejora (tales como una primera capa de mejora, una segunda capa de mejora, etc.), la descodificación de la capa de mejora de resolución más elevada depende de la descodificación de la(s) capa(s) de mejora de resolución más baja. Esto es, se puede descodificar la capa de base independientemente para reproducir el vídeo de baja calidad; se puede descodificar la primera capa de mejora basada en la capa de base descodificada, para obtener la resolución más alta; adicionalmente, se puede descodificar la segunda capa de mejora basada en la primera capa de mejora descodificada, para obtener una calidad de reproducción de vídeo todavía más alta y así sucesivamente. De este modo, desde el punto de vista de la seguridad, la capa de base tiene la mayor importancia, luego la primera capa de mejora, la segunda capa de mejora, etc. El método de esta realización aprovecha las características del tren de datos en capas de este tipo, ajustando las intensidades de encriptación para las diferentes capas respectivamente.

Las diferencias entre esta realización y la realización precedente de la Figura 1 son la etapa de ajustar los atributos de encriptación para reducir el consumo de recursos (es decir, la Etapa 110 de la Figura 1) y la etapa de ajustar los atributos de encriptación para aumentar la intensidad de encriptación (es decir, la Etapa 120 de la Figura 1).

La Figura 4 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según todavía otra realización de la presente invención, mostrando en particular el flujo detallado de la etapa de ajustar los atributos de encriptación a fin de reducir la intensidad de encriptación (Etapa 110). Se supone que el tren de datos tiene tres capas, capa básica, primera capa de mejora y segunda capa de mejora.

Como se muestra en la Figura 4, si el resultado de la determinación en la Etapa 105 (Figura 1) es “Sí”, se hace una determinación en primer lugar sobre si la intensidad de encriptación de la segunda capa de mejora ha alcanzado la intensidad de encriptación más baja en la Etapa 405. Si el resultado de la determinación de la Etapa 405 es “No”, se realizará la Etapa 410 reduciendo la intensidad de encriptación de la segunda capa de mejora, luego se realizará la etapa siguiente del método (Etapa 125 en la Figura 1); si es “Sí”, se realizará la Etapa 415, determinando si la intensidad de encriptación de la primera capa de mejora ha alcanzado la intensidad de encriptación más baja.

Si el resultado de la determinación de la Etapa 415 es “No”, se realizará la Etapa 420, reduciendo la intensidad de encriptación de la primera capa de mejora, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es “Sí”, se realizará la Etapa 425, determinando si la intensidad de encriptación de la capa de base ha alcanzado la intensidad de encriptación más baja.

A continuación, si el resultado de la determinación de la Etapa 425 es “No”, se realizará la Etapa 430, reduciendo la intensidad de encriptación de la capa de base, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es “Sí”, esto significa que las intensidades de encriptación de todas las capas han alcanzado el valor más bajo. En ese caso, se puede detener el proceso de encriptación y transmisión hasta que se liberen recursos del sistema por otras aplicaciones o se puede continuar con las intensidades de encriptación más bajas.

En esta realización, se puede establecer las intensidades de encriptación más bajas para las diferentes capas, respectivamente, preferiblemente la intensidad de encriptación más baja para la capa de base se establece como la más alta, la intensidad de encriptación más baja para la primera capa de mejora se establece como la segunda más alta, y la intensidad de encriptación más baja para la segunda capa de mejora se establece como la más baja. Además, la intensidad de encriptación más baja puede ser cero, esto es ausencia de encriptación. Por ejemplo, la intensidad de encriptación más baja para la capa de base es DES (CBC), la intensidad de encriptación más baja para la primera capa de mejora es DES (ECB), y la intensidad de encriptación más baja para la segunda capa de mejora es “ausencia de encriptación”. Así, en los casos de consumo de recursos relativamente grande, cuando todas las intensidades de encriptación se ajustan para ser las más bajas según el método de la presente invención, se garantiza todavía una protección suficiente para la capa de base de gran importancia, con lo cual se garantiza la seguridad de todo el tren de vídeo, aunque se puede reducir significativamente el consumo de recursos del sistema y se puede asegurar la calidad de reproducción debido a la reducción de las intensidades de encriptación de las primera y segunda capas de mejora.

La Figura 5 es un diagrama de flujo que muestra las etapas de ajustar los atributos de encriptación en un método para encriptar un tren de datos según todavía otra realización de la presente invención, mostrando en particular el flujo detallado de la etapa de ajustar los atributos de encriptación a fin de aumentar la intensidad de encriptación (Etapa 120) en el método para encriptar un tren de datos.

Como se muestra en la Figura 5, si el resultado de la determinación en la Etapa 115 (Figura 1) es “Sí”, se hace una determinación en primer lugar sobre si la intensidad de encriptación de la capa de base ha alcanzado la intensidad de encriptación más alta en la Etapa 505. Si el resultado de la determinación de la Etapa 505 es “No”, se realizará la Etapa 510, aumentando la intensidad de encriptación de la capa de base, luego se realizará la etapa siguiente del método (Etapa 125 en la Figura 1); si es “Sí”, se realizará la Etapa 515, determinando si la intensidad de encriptación de la primera capa de mejora ha alcanzado la intensidad de encriptación más alta.

A continuación, si el resultado de la determinación de la Etapa 515 es “No”, se realizará la Etapa 520, aumentando la intensidad de encriptación de la primera capa de mejora, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es “Sí”, se realizará la Etapa 525, determinando si la intensidad de encriptación de la segunda capa de mejora ha alcanzado la intensidad de encriptación más alta.

A continuación, si el resultado de la determinación de la Etapa 525 es "No", se realizará la Etapa 530, aumentando la intensidad de encriptación de la segunda capa de mejora, luego se realizará la etapa siguiente del método (Etapa 125 de la Figura 1); si es "Sí", esto significa que las intensidades de encriptación de todas las capas han alcanzado los valores más altos. En ese caso, se puede continuar simplemente el proceso.

De manera similar, se puede establecer también las intensidades de encriptación más altas para las diferentes capas, respectivamente, pero en la presente realización se establece la misma intensidad de encriptación más alta, tal como AES (CBC) para todas las capas.

De forma correspondiente, la siguiente Tabla 4 muestra a título de ejemplo el contenido de la información de atributos de encriptación en esta realización.

TABLA 4

Contenido de la información de atributos de encriptación

Campo	Valor
Algoritmo de encriptación para la capa de base	3DES
Modo de encriptación para la capa de base	CBC
Parámetro de encriptación para la capa de base	Ninguno
Algoritmo de encriptación para la primera capa de mejora	DES
Modo de encriptación para la primera capa de mejora	CBC
Parámetro de encriptación para la primera capa de mejora	Ninguno
Algoritmo de encriptación para la segunda capa de mejora	Ninguno
Modo de encriptación para la segunda capa de mejora	Ninguno
Parámetro de encriptación para la segunda capa de mejora	Ninguno

Según la presente realización, cuando se alivia el consumo de recursos del sistema, se puede aumentar las intensidades de encriptación en el orden de la capa de base, la primera capa de mejora y la segunda capa de mejora, haciendo de esta forma que se maximice la seguridad de los trenes de datos dentro del límite de recursos del sistema.

Además, según una realización alternativa, en las etapas mostradas en la Figura 4, las intensidades de encriptación se reducen en el orden de la capa de base, la primera capa de mejora y la segunda capa de mejora; en las etapas mostradas en la Figura 5, las intensidades de encriptación se elevan en el orden de la segunda capa de mejora, la primera capa de mejora y la capa de base; las intensidades de encriptación más bajas de la capa de base, la primera capa de mejora y la segunda capa de mejora se establecen en "ausencia de encriptación", DES (CBC) y 3DES (CBC) respectivamente; y la intensidad de encriptación más alta para la capa de base, la primera capa de mejora y la segunda capa de mejora se establecen en "ausencia de encriptación", AES (CBC) y AES (CBC) respectivamente. Así, aquellos receptores que no tienen permiso pueden ver vídeo reproducido de baja resolución, mientras tanto, las capas de mejora que proporcionan vídeo reproducido de alta calidad son protegidas adecuadamente, esto es una ventaja para aquellos proveedores de servicio que quieren atraer más usuarios y obtener asimismo una protección fiable.

Además, según todavía otra realización de la presente invención, se proporciona un método adecuado para encriptar un tren de vídeo comprimido en capas. Por ejemplo, un tren de datos de vídeo MPEG-2 incluye una capa de base y una o varias capas de mejora, mientras que cada capa contiene datos de trama-I, trama-P y trama-B. Por tanto, la presente realización combina las realizaciones descritas haciendo referencia a las Figuras 2 y 3 y a las Figuras 4 y 5, proporcionando un método de encriptación que puede ajustar las intensidades de encriptación para las diferentes tramas de la misma capa.

Particularmente, en las Etapas 410, 420 y 430 como se muestra en la Figura 4, se realiza el proceso mostrado en la Figura 2 con respecto a la capa de base, la primera capa de mejora y la segunda capa de mejora, respectivamente; en las Etapas 510, 520 y 530, como se muestra en la Figura 5, se realiza el proceso como se muestra en la Figura 3 con respecto a cada tipo de tramas dentro de la capa de base, la primera capa de mejora y la segunda capa de mejora, respectivamente; adicionalmente, cuando las intensidades de encriptación para todos los tipos de tramas dentro de una capa han alcanzado su valor más bajo, se determina la intensidad de encriptación de esta capa como la más baja (Etapas 405, 415 y 425), por otra parte, cuando las intensidades de encriptación para todos los tipos de tramas dentro de una capa han alcanzado su valor más alto, se determina la intensidad de encriptación de esta capa como la más alta (Etapas 505, 515 y 525).

Para el tren de vídeo comprimido en capas, el método para encriptar de la presente realización no sólo puede ajustar las intensidades de encriptación con respecto a las diferentes capas, sino que también puede ajustar las intensidades de encriptación con respecto a los diferentes tipos de trama dentro de la misma capa, de manera que se puede ajustar los atributos de encriptación de manera más flexible y más precisa, realizando un equilibrio entre los recursos del sistema, la seguridad de los datos y la calidad de reproducción de la información transmitida. Como resultado, el método de esta realización puede mejorar la eficiencia del funcionamiento del sistema y maximizar la calidad de reproducción.

Además, según otros aspectos de la presente invención, se proporciona un aparato para encriptar y desencriptar un tren de datos, un aparato para enviar con seguridad un tren de datos y un aparato para recibir con seguridad un tren de datos, así como un sistema para dar seguridad en la transmisión de un tren de datos. A continuación se da una descripción detallada haciendo referencia a las figuras 6 y 7.

La Figura 6 muestra esquemáticamente la estructura del sistema para una transmisión con seguridad de un flujo de datos en la técnica anterior. Como se muestra en la Figura 6, el sistema incluye: un aparato emisor (emisor) 600, un aparato receptor (receptor) 700 y un canal 800 que conecta el receptor y el emisor. El emisor 600 comprende un codificador 601, unos medios de encriptación 602 y un codificador de canal 603; el receptor 700 comprende un descodificador de fuente 701, unos medios 702 de desencriptación y un descodificador 703 de canal.

La transmisión segura de un tren de datos en la técnica anterior es como sigue: en el emisor, en primer lugar son codificados en la fuente los datos originales (tales como datos de audio, vídeo u otros) por el codificador 601 de fuente, por ejemplo, los datos originales de vídeo son comprimidos y codificados en un tren de datos en formato MPEG2, etc. Aquí, el tren de datos original puede proceder de una tarjeta de toma de vídeo u otros dispositivos de adquisición, también puede proceder de un medio de registro de datos, tal como un accionamiento de CD, un accionamiento de DVD, un accionamiento de disco y elementos análogos. Y cuando se han guardado los datos en un formato adecuado en el medio de registro, se puede omitir el codificador 601 de fuente. A continuación, según una cierta política de encriptación, los medios 602 de encriptación encriptan el tren de datos, aquí la política de encriptación puede estar predeterminada, o puede ser determinada a través de un "apretón de manos" antes de la encriptación y la transmisión. Finalmente, el tren de datos encriptados es codificado en canal por el codificador 603 de canal y transmitido por los medios 700 de recepción a través del canal 800.

En el receptor, en primer lugar se descodifican por canal los datos recibidos por el descodificador 703 de canal, formando el tren de datos recibidos. A continuación, según la política de encriptación anterior, los medios de desencriptación desencriptan el tren de datos recibidos. Finalmente, el descodificador 701 de fuente desencripta por fuente el tren de datos recibidos, para formar los datos reproducidos.

La Figura 7 muestra esquemáticamente una estructura de un sistema para la transmisión segura de un tren de datos según una realización de la presente invención. Como se muestra en la Figura 7, el sistema para la transmisión segura de un tren de datos comprende: un aparato que emite (emisor) 600, un aparato que recibe (receptor) 700 y un canal 800 que conecta el receptor y el emisor. Entre ellos, el emisor 600 comprende un codificador 601 de fuente, unos aparato de encriptación 610 y un codificador 603 de canal; el receptor 700 comprende un descodificador 701 de fuente, un aparato 710 de desencriptación y un descodificador 703 de canal.

Según esta realización, en el emisor 600, durante la encriptación el aparato 601 de encriptación encripta el tren de datos que viene del codificador 601 de fuente o de un dispositivo de lectura para medio de registro de datos (no representado), y transmite el tren de datos encriptados al codificador 602 de canal, esto es, durante el proceso de encriptación y transmisión del tren de datos, se ajusta la política de encriptación en base a la condición de consumo de recursos y calidad de canal.

El aparato 610 de encriptación incluye un aleatorizador 614 para encriptar un tren de datos según atributos de encriptación específicos; una unidad 611 que calcula la complejidad para calcular la complejidad según el consumo de recursos del emisor y del receptor (el término "complejidad" se ha explicado en la anterior descripción); una unidad 613 de detección de calidad de canal para detectar la calidad actual del canal 800 usado para transmitir el tren de datos, tal como la Tasa de error de Bit (BER), la Tasa de Pérdida de Paquetes (PLR), la anchura de banda y otros análogos, y para enviar los datos detectados de calidad de canal a una unidad 612 de ajuste y determinación; la unidad 612 de ajuste y determinación para determinar si se necesita ajustar los atributos de encriptación en base a la información de la unidad 611 de cálculo de la complejidad y la unidad 613 de detección de la calidad de canal, y si se necesita, ajustar los atributos de encriptación para el tren de datos y transferir los atributos de encriptación al aleatorizador 614, con lo cual se controla el aleatorizador 614 para realizar la encriptación. Específicamente, la unidad 612 de determinación y ajuste como se muestra anteriormente realiza las etapas de determinar y ajustar como se muestra anteriormente en el diagrama de flujo de la Figura 1. La unidad 612 de determinación y ajuste puede ser realizada en forma de hardware o de software correspondiendo a las etapas del flujo, como es conocido por los expertos en la técnica.

La unidad 612 de determinación y ajuste, la unidad 611 de cálculo de la complejidad y la unidad 613 de detección de la calidad de canal a partir de los medios de ajuste de los atributos de encriptación realizan la política de encriptación basada en el consumo de recursos y en la calidad de canal durante la encriptación y la transmisión del tren de datos, en esta realización de la presente invención.

Según esta realización, se registra la información ajustada de atributos en el encabezamiento del paquete de datos en forma de metadatos y se transmite al receptor (medios 700 de recepción) junto con el tren de datos; preferiblemente, se encripta también la información de atributos. El contenido de la información de atributos de encriptación según esta realización se muestra a título de ejemplo en la tabla 1.

En el receptor 700, el descodificador 703 de canal realiza la descodificación por canal de los datos recibidos para formar un tren de datos recibidos. La información de atributos de encriptación en el encabezamiento de los paquetes del tren de datos se transfiere a la unidad 711 receptora de información de ajuste de encriptación y se extrae de la misma, y luego se transfiere la información extraída al desaleatorizador 712, controlando el desaleatorizador para desencriptar los datos correspondientes del tren de datos de manera adecuada.

Debería observarse que el método para transmitir los atributos de encriptación no se limita a los metadatos de la realización anterior, y también es posible que los atributos de encriptación sean transmitidos a través de un canal separado seguro, por consiguiente, la unidad 711 receptora de la información de atributos de encriptación necesita recibir la información de atributos encriptación del canal seguro, el cual está también dentro del objeto de la presente invención.

Adicionalmente, según otra realización de la presente invención, cuando el tren de datos a encriptar y transmitir es un tren de vídeo comprimido que contiene datos de trama-I, datos de trama-P y datos de trama-B, la unidad 612 de determinación y ajuste ajusta los atributos de encriptación de los datos de trama-I, datos de trama-P y datos de trama-B; el aleatorizador 614 encripta los datos de trama-I, datos de trama-P y datos de trama-B, respectivamente, según la información de atributos de encriptación. Específicamente, la unidad 612 de determinación y ajuste realiza las etapas de comprobar y ajustar como se muestra en las Figuras 2 y 3. El contenido de la información de atributos de encriptación según la presente invención se muestra a título de ejemplo en la Tabla 3.

En consecuencia, la unidad 711 receptora de la información de atributos de encriptación de la presente invención recibe la información de atributos encriptación para los datos de trama-I, datos de trama-P y datos de trama-B, respectivamente, el desaleatorizador 712 desencripta los datos de trama-I, los datos de trama-P y los datos de trama-B, respectivamente, según la información de atributos de encriptación.

Además, según otra realización todavía de la presente invención, cuando el tren de datos a encriptar y transmitir es un tren de vídeo comprimido que contiene una capa de base, una primera capa de mejora y una segunda capa de mejora, la unidad 612 de determinación y ajuste ajusta los atributos de encriptación para la capa de base, la primera capa de mejora y la segunda capa de mejora, respectivamente, el aleatorizador 614 encripta la capa de base, la primera capa de mejora y la segunda capa de mejora, respectivamente, según la información de atributos de encriptación. Específicamente, la unidad 612 de determinación y ajuste realiza las etapas de determinar y ajustar como se indica en las Figuras 4 y 5. El contenido de la información de atributos de encriptación según la presente realización se muestra a título de ejemplo en la Tabla 4.

Por consiguiente, la unidad 711 receptora de la información de ajuste de encriptación de la presente invención recibe la información de atributos de encriptación para la capa básica, la primera capa de mejora y la segunda capa de mejora, respectivamente; el desaleatorizador 712 desencripta la capa de base, la primera capa de mejora y la segunda capa de mejora, respectivamente, según la información de atributos de encriptación.

Los expertos en la técnica deberían apreciar que, en las realizaciones anteriores, los componentes del aparato de encriptación y desencriptación, y del emisor y el receptor, tales como el codificador 601 de fuente, el aparato 610 y el codificador 603 de canal, el descodificador 701 de fuente, el aparato 710 de desencriptación y el descodificador 703 de canal, pueden ser llevados a cabo en forma de hardware o software.

Además, aunque se muestra un emisor 600 y un receptor 700 en el sistema representado en la Figura 7, los expertos en la técnica pueden anticipar fácilmente un sistema con unos medios de emisión y una pluralidad de medios de recepción, por ejemplo, en un sistema de VOD, en el que un servidor de VOD da servicio a una pluralidad de terminales de VOD.

Aunque se ha dado una descripción detallada del método de encriptación y desencriptación, el aparato para enviar con seguridad un tren de datos, el aparato para recibir con seguridad un tren de datos y un sistema para transmitir con seguridad un tren de datos de la presente invención a través de algunas realizaciones a título de ejemplo, no se han agotado las realizaciones anteriormente mencionadas, pudiendo los expertos en la técnica hacer diversos cambios y modificaciones dentro del objeto de la presente invención. Por tanto, la presente invención no se limita a estas realizaciones, sino que el objeto de la presente invención sólo se define por las reivindicaciones anexas.

REIVINDICACIONES

1. Un método para encriptar un tren de datos que se transmite de un emisor a un receptor a través de un canal (800), comprendiendo dicho método ajustar (110-120) los atributos de encriptación durante la transmisión en base a las características de uno o varios de (i) el consumo de recursos actual del emisor, el receptor o ambos; y (ii) la calidad del canal; encriptar el tren de datos según los atributos de encriptación ajustados;, y transmitir el tren de datos encriptados e información de dichos atributos de encriptación ajustados a dicho receptor.

2. El método de la reivindicación 1, en el que dicha etapa de ajustar los atributos de encriptación comprende: determinar si la complejidad actual es más alta que un primer umbral predeterminado, siendo dicha complejidad actual una medida del consumo de recursos del emisor, el receptor o ambos; y si dicha complejidad actual es más alta que dicho primer umbral predeterminado, ajustar los atributos de encriptación para reducir el consumo de recursos del emisor o del receptor.

3. El método de la reivindicación 2, en el que dicha etapa de ajustar los atributos de encriptación comprende: determinar si la complejidad actual es más baja que un segundo umbral predeterminado, siendo el segundo umbral más bajo que dicho primer umbral predeterminado, y si dicha complejidad actual es más baja que dicho segundo umbral predeterminado, ajustar los atributos de encriptación para reducir el consumo de recursos del emisor o del receptor.

4. El método de la reivindicación 1, en el que dicha etapa de ajustar los atributos de encriptación comprende: determinar si la BER actual del canal ha aumentado en una primera cantidad predeterminada; si dicha BER actual del canal ha aumentado en la primera cantidad predeterminada, ajustar los atributos de encriptación para reducir una longitud de propagación de error de la encriptación; determinar si la BER actual del canal ha disminuido en una segunda cantidad predeterminada; y si dicha BER actual del canal ha disminuido en la segunda cantidad predeterminada, ajustar los atributos de encriptación para aumentar la longitud de propagación de error de la encriptación.

5. El método de la reivindicación 1, en el que dicha etapa de ajustar los atributos de encriptación comprende: determinar si la BER actual del canal es más alta que un primer umbral predeterminado, si dicha BER actual del canal es más alta que un primer umbral predeterminado, ajustar los atributos de encriptación para reducir la longitud de propagación de error de la encriptación; determinar si la BER actual del canal es más baja que el segundo umbral predeterminado; si dicha BER actual del canal es más baja que el segundo umbral predeterminado, ajustar los atributos de encriptación para aumentar la longitud de propagación de error de la encriptación.

6. El método de la reivindicación 1, en el que dicho tren de datos es un tren de vídeo comprimido que contiene datos de trama-I, datos de trama-P y datos de trama-B, donde dicha etapa de ajustar los atributos de encriptación ajusta los atributos de encriptación para los datos de trama-I, datos de trama-P y datos de trama-B, respectivamente.

7. El método de la reivindicación 2, en el que dicho tren de datos es un tren de vídeo comprimido que contiene datos de trama-I, datos de trama-P y datos de trama-B, y donde dicha etapa de ajustar los atributos de encriptación para reducir el consumo de recursos de dicho emisor o de dicho receptor incluye respectivamente ajustar los atributos de encriptación para los datos de trama-I, datos de trama-P y datos de trama-B, en el orden de trama-B, trama-P y trama-I.

8. El método de la reivindicación 3, en el que dicho tren de datos es un tren de vídeo comprimido que contiene datos de trama-I, datos de trama-P y datos de trama-B, y donde dicha etapa de ajustar los atributos de encriptación para aumentar el consumo de recursos de dicho emisor o de dicho receptor incluye respectivamente ajustar los atributos de encriptación para los datos de trama-I, datos de trama-P y datos de trama-B, en el orden de trama-I, trama-P y trama-B.

9. El método de la reivindicación 1, en el que dicho tren de datos contiene una capa de base y al menos una capa de mejora, donde dicha etapa de ajustar los atributos de encriptación ajusta los atributos de encriptación para dicha capa de base y dicha al menos una capa de mejora, respectivamente.

10. El método de la reivindicación 2, en el que dicho tren de datos contiene una capa de base y al menos una capa de mejora, donde dicha etapa de ajustar los atributos de encriptación ajusta los atributos de encriptación para reducir el consumo de recursos de dicho emisor o de dicho receptor incluye sucesivamente ajustar los atributos de encriptación en el orden desde dicha capa de mejora a dicha capa de base.

11. El método de la reivindicación 3, en el que dicho tren de datos contiene una capa de base y al menos una capa de mejora, donde dicha etapa de ajustar los atributos de encriptación para aumentar el consumo de recursos de dicho emisor o de dicho receptor incluye respectivamente ajustar los atributos de encriptación para dicha capa de base y para dicha al menos una capa de mejora en el orden desde dicha capa de base a dicha capa de mejora.

12. Un aparato para encriptar un tren de datos que se transmite desde un emisor a un receptor a través de un canal (800), comprendiendo dicho aparato de encriptación: unos medios (612) para ajustar los atributos de encriptación durante la transmisión de dicho tren de datos para generar información de atributos de encriptación, ajustando dichos

medios de ajuste los atributos de encriptación en base a las características de uno o varios de (i) el consumo de recursos actual del emisor, el receptor o ambos; y (ii) la calidad del canal; y un aleatorizador (614) para realizar la encriptación de al menos una parte de dicho tren de datos según los atributos de encriptación ajustados por dichos medios de ajuste de atributos de encriptación.

13. El aparato de la reivindicación 12, en el que dichos medios para ajustar los atributos de encriptación incluyen una unidad de detección de calidad de canal, y enviar información sobre la calidad del canal a dicha unidad de determinación y ajuste; y dicha unidad de determinación y ajuste ajusta adicionalmente los atributos de encriptación en base a la información sobre la calidad de canal procedente de dicha unidad de detección de calidad de canal.

14. El aparato de la reivindicación 12, en el que dicho tren de datos es un tren de vídeo comprimido que contiene datos de trama-I, datos de trama-P y datos de trama-B, donde dichos medios de ajuste de los atributos de encriptación ajustan los atributos de encriptación para los datos de trama-I, datos de trama-P y datos de trama-B, respectivamente; donde dicho aleatorizador encripta los datos de trama-I, datos de trama-P y datos de trama-B, respectivamente; según la información de atributos de encriptación.

15. El aparato de la reivindicación 12, en el que dicho tren de datos contiene una capa de base y al menos una capa de mejora; donde dichos medios de ajuste de los atributos de encriptación ajustan los atributos de encriptación para dicha capa de base y dicha al menos una capa de mejora respectivamente según la información de atributos de encriptación.

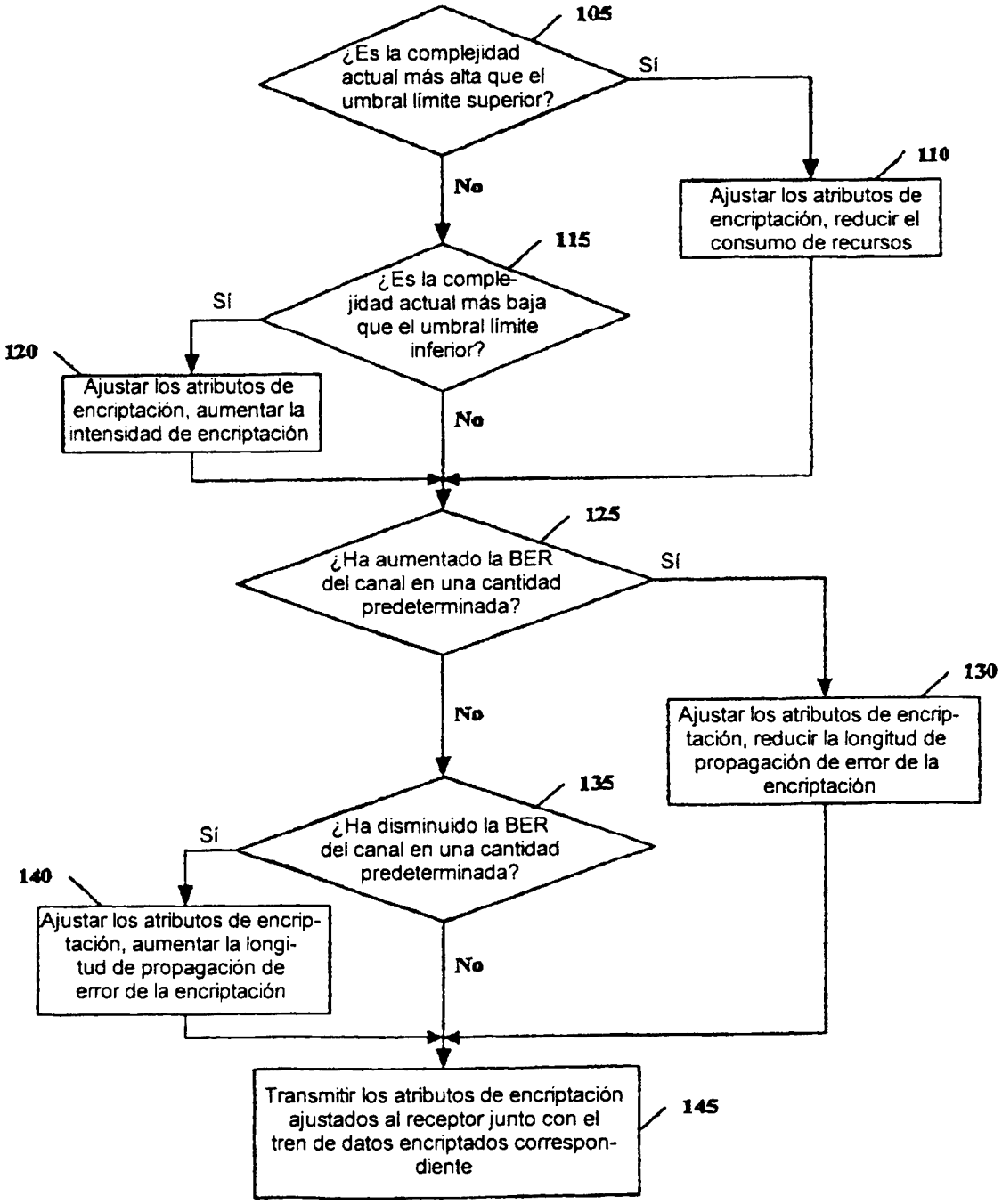
105
¿Es la complejidad actual más alta que el umbral límite superior?
Sí
No
110
Ajustar los atributos de encriptación, reducir el consumo de recursos
115
¿Es la complejidad actual más baja que el umbral límite inferior?
Sí
120
Ajustar los atributos de encriptación, aumentar la intensidad de encriptación
No
125
¿Ha aumentado la BER del canal en una cantidad predeterminada?
Sí
130
Ajustar los atributos de encriptación, reducir la longitud de propagación de error de la encriptación
No
135
¿Ha disminuido la BER del canal en una cantidad predeterminada?
Sí
140
Ajustar los atributos de encriptación, aumentar la longitud de propagación de error de la encriptación
No
Transmitir los atributos de encriptación ajustados al receptor junto con el tren de datos encriptados correspondiente
145

Fig. 1

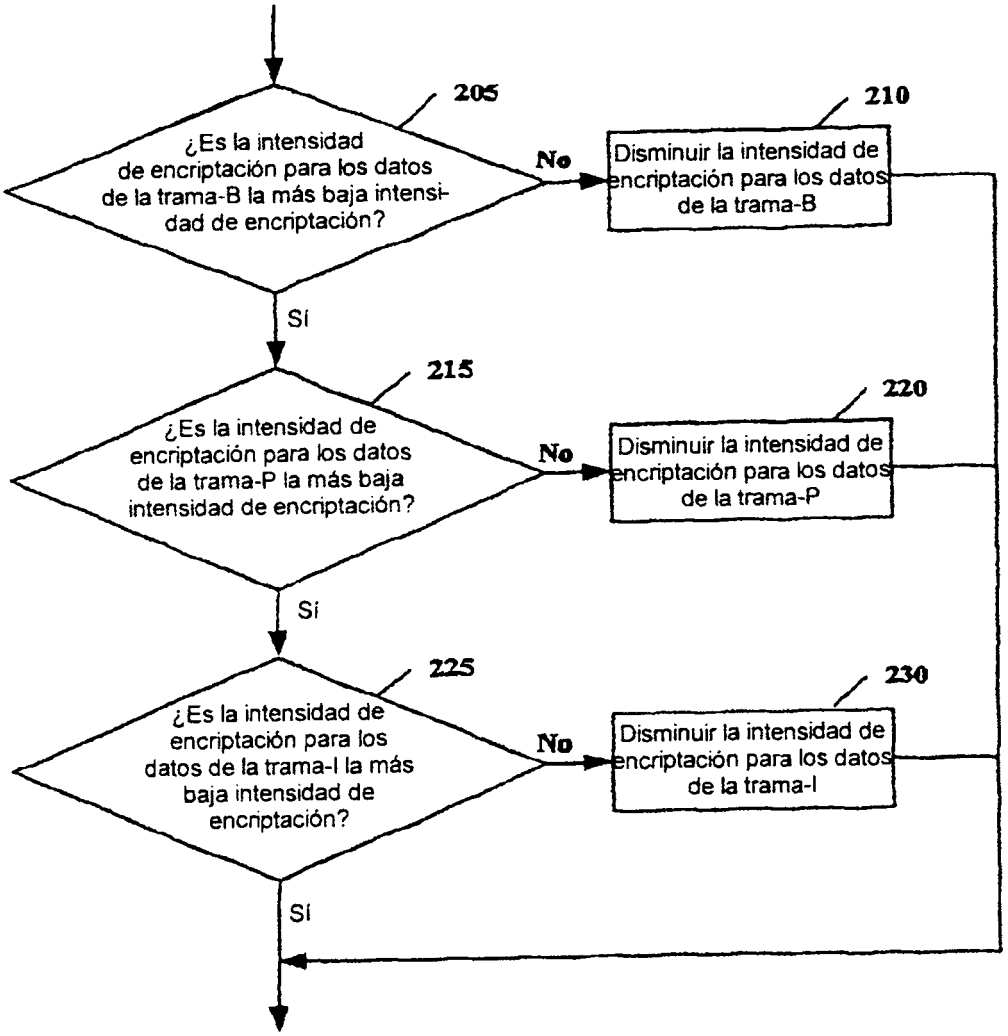
205
¿Es la intensidad de encriptación para los datos de la trama-B la más baja intensidad de encriptación?
No
210
Disminuir la intensidad de encriptación para los datos de la trama-B
Sí
215
¿Es la intensidad de encriptación para los datos de la trama-P la más baja intensidad de encriptación?
No
220
Disminuir la intensidad de encriptación para los datos de la trama-P
Sí
225
¿Es la intensidad de encriptación para los datos de la trama-I la más baja intensidad de encriptación?
No
230
Disminuir la intensidad de encriptación para los datos de la trama-I
Sí

Fig.2

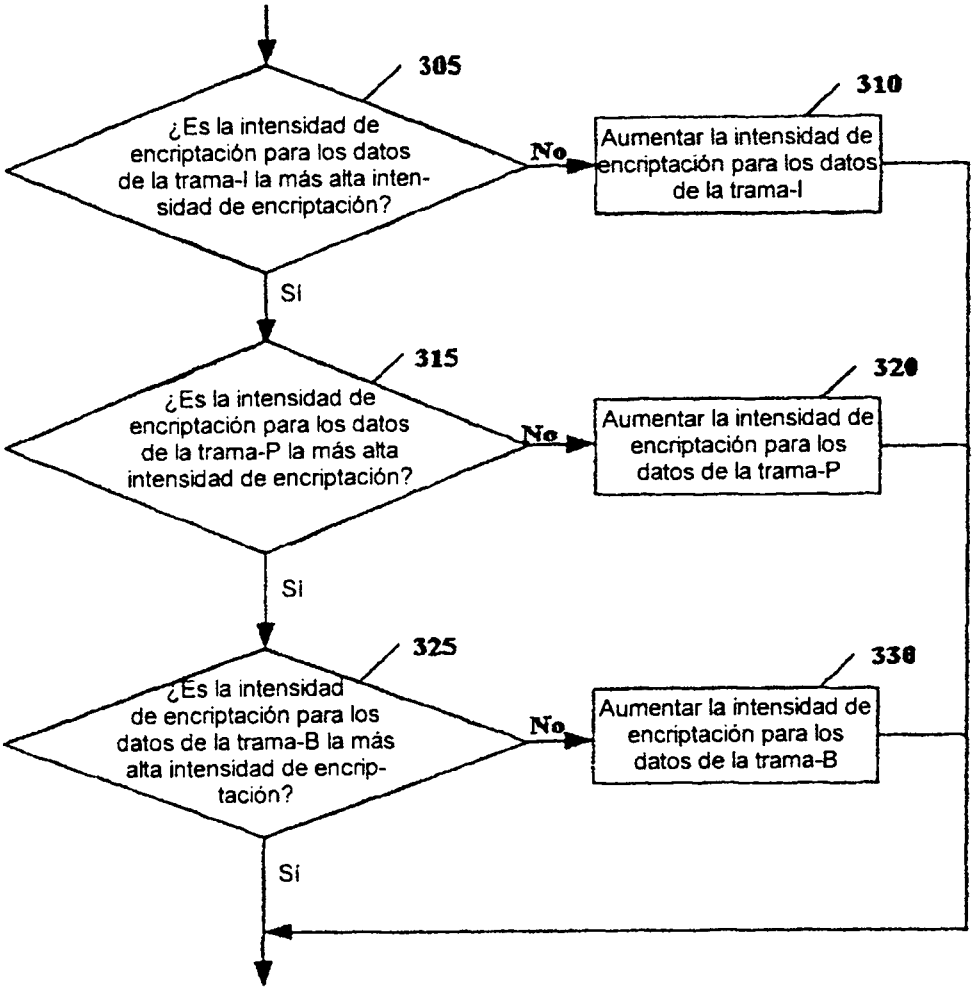
305
¿Es la intensidad de encriptación para los datos de la trama-I la más alta intensidad de encriptación?
No
310
Aumentar la intensidad de encriptación para los datos de la trama-I
Sí
315
¿Es la intensidad de encriptación para los datos de la trama-P la más alta intensidad de encriptación?
No
320
Aumentar la intensidad de encriptación para los datos de la trama-P
Sí
325
¿Es la intensidad de encriptación para los datos de la trama-B la más alta intensidad de encriptación?
No
330
Aumentar la intensidad de encriptación para los datos de la trama-B
Sí

Fig.3

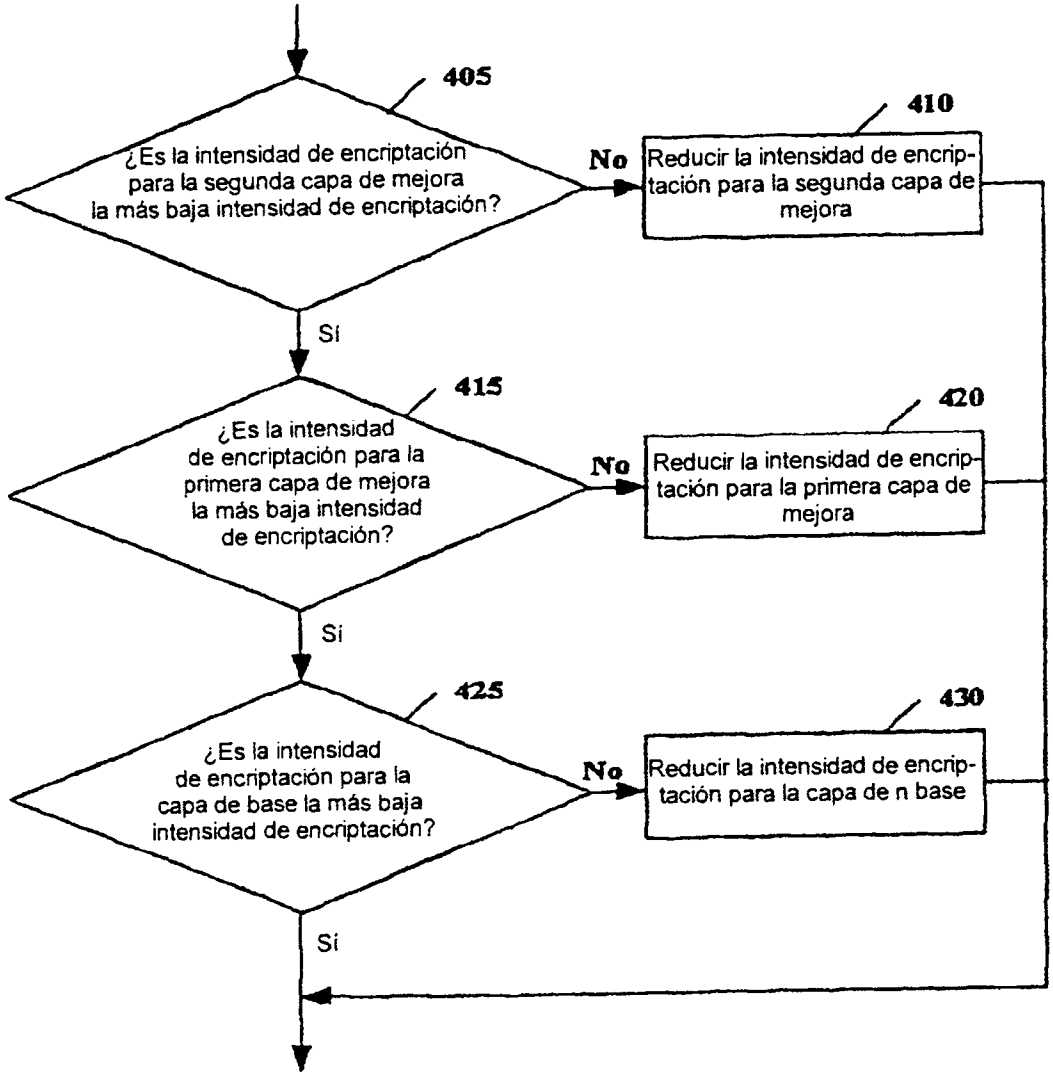
405
¿Es la intensidad de encriptación para la segunda capa de mejora la más baja intensidad de encriptación?
No
410
Reducir la intensidad de encriptación para la segunda capa de mejora
Sí
415
¿Es la intensidad de encriptación para la primera capa de mejora la más baja intensidad de encriptación?
No
420
Reducir la intensidad de encriptación para la primera capa de mejora
Sí
425
¿Es la intensidad de encriptación para la capa de base la más baja intensidad de encriptación?
No
430
Reducir la intensidad de encriptación para la capa de n base
Sí

Fig.4

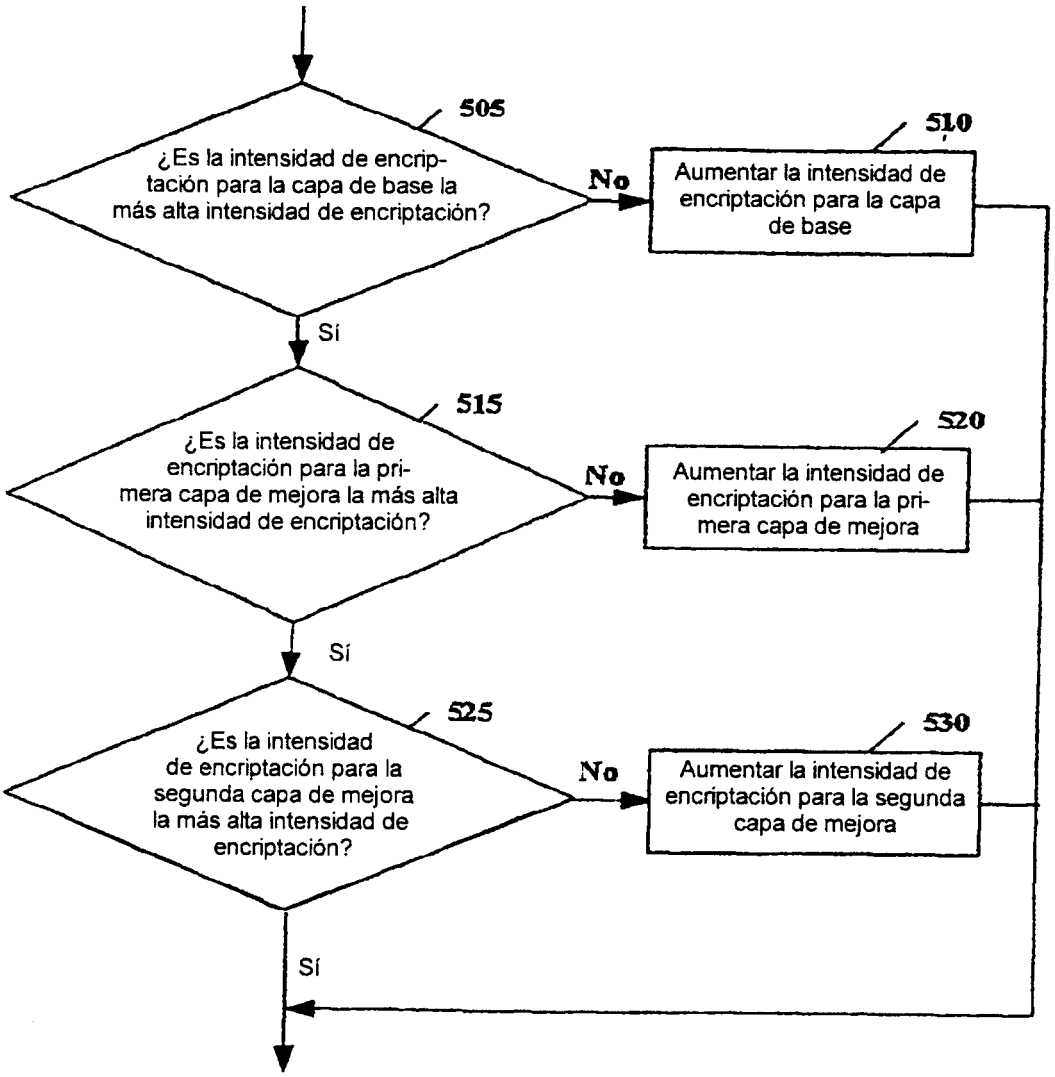
505
¿Es la intensidad de encriptación para la capa de base la más alta intensidad de encriptación?
No
510
Aumentar la intensidad de encriptación para la capa de base
Sí
515
¿Es la intensidad de encriptación para la primera capa de mejora la más alta intensidad de encriptación?
No
520
Aumentar la intensidad de encriptación para la primera capa de mejora
Sí
525
¿Es la intensidad de encriptación para la segunda capa de mejora la más alta intensidad de encriptación?
No
530
Aumentar la intensidad de encriptación para la segunda capa de mejora
Sí

Fig.5

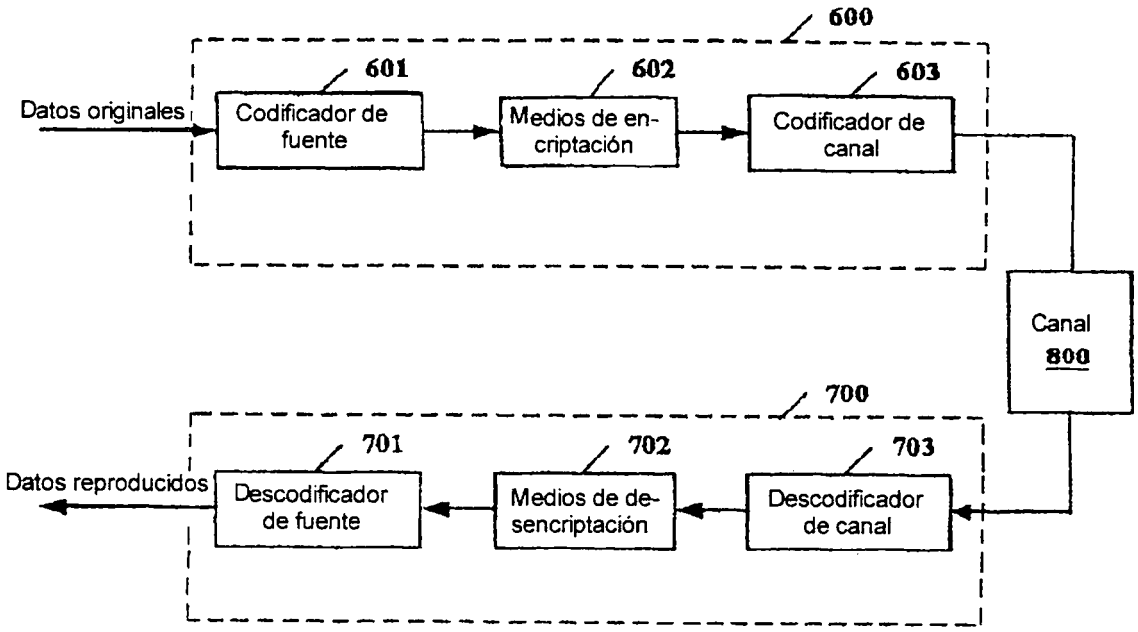
600
601
602
603
Datos originales
Codificador de fuente
Medios de encriptación
Codificador de canal
Canal
800
700
701
702
703
Datos reproducidos
Descodificador de fuente
Medios de desencriptación
Descodificador de canal

Fig.6

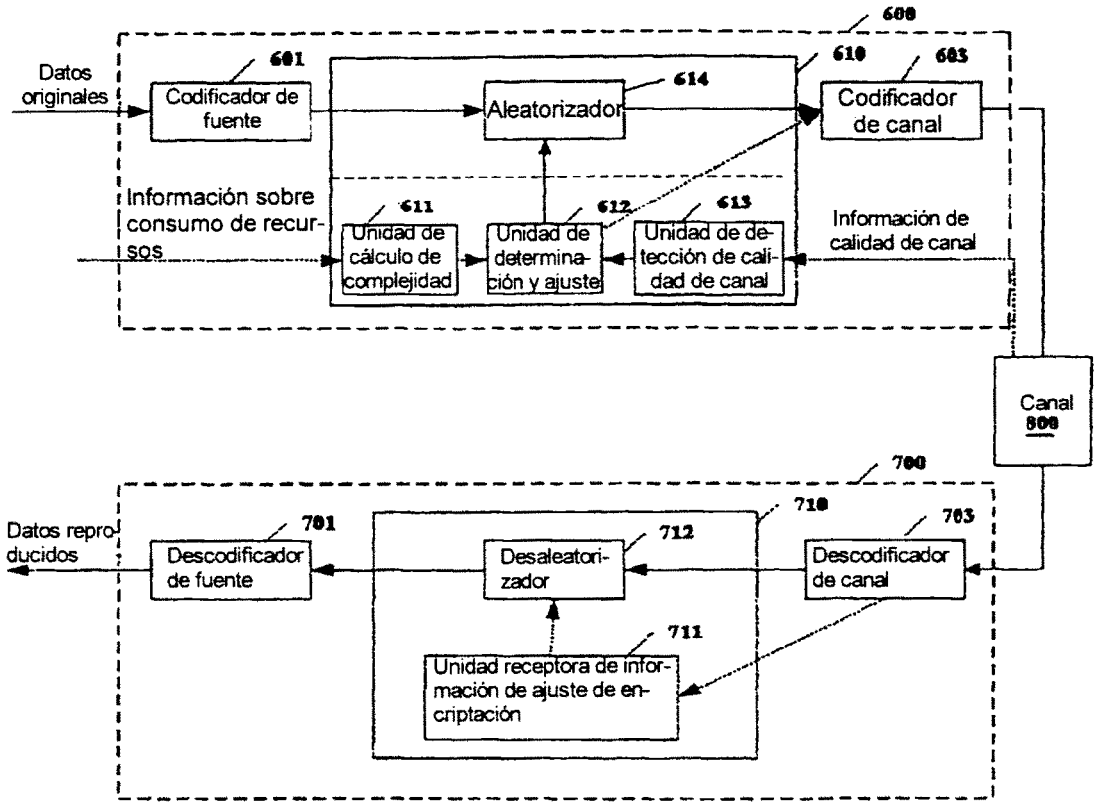
600
Datos originales
601
Codificador de fuente
610
614
Aleatorizador
603
Codificador de canal
Información sobre consumo de recursos
611
Unidad de cálculo de complejidad
612
Unidad de determinación y ajuste
613
Unidad de detección de calidad de canal
Información de calidad de canal
Canal 800
700
710
Datos reproducidos
701
Descodificador de fuente
712
Desaleatorizador
703
Descodificador de canal
711
Unidad receptora de información de ajuste de encriptación

Fig.7