(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 266 099**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04N 7/167 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01271726 .0**
(86) Fecha de presentación : **10.12.2001**
(87) Número de publicación de la solicitud: **1348287**
(87) Fecha de publicación de la solicitud: **01.10.2003**

(54) Título: **Punteros para datos encriptados en la cabecera de protocolo en tiempo real (RTP).**

(30) Prioridad: **18.12.2000 EP 00204639**

(45) Fecha de publicación de la mención BOPI:
01.03.2007

(45) Fecha de la publicación del folleto de la patente:
01.03.2007

(73) Titular/es: **Irdeto Eindhoven B.V.**
Jupiterstraat 42
2132 HD Hoofddorp, NL

(72) Inventor/es: **Van Rijnsoever, Bartholomeus, J.**

(74) Agente: **Zuazo Araluze, Alexander**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Punteros para datos encriptados en la cabecera de protocolo en tiempo real (RTP).

Un método y un sistema para la transmisión en tiempo real de datos de usuario formateados en trama a través de la unión a los mismos de datos de localización de trama situados en posiciones de regulación predeterminadas, mientras que con anterioridad a la transmisión se lleva a cabo un procedimiento de encriptación que excluye los citados datos de localización, y un sistema, un aparato transmisor, un aparato receptor, y una señal generada por tal aparato transmisor para su uso con el citado método.

Antecedentes de la invención

La invención se refiere a un sistema como el que se define en el preámbulo de la reivindicación 1. Los datos, y en particular, aunque sin limitación, los datos multimedia, en la actualidad están siendo encriptados para la implementación, entre otros, de diversos esquemas de acceso condicional para permitir a los creadores y distribuidores de un motivo original, recopilar una cantidad apropiada de retribuciones de los usuarios de tal información. En el lado del receptor, los datos de usuario deben ser recuperados con el fin de permitir una representación, visualización, escucha y ejecución de forma ordenada, así como otras operaciones asociadas al usuario. La transmisión real a través de algún medio de transmisión, tal como una red, tendrá lugar a nivel de formación de paquetes, en el que los paquetes están estandarizados para la red o redes en cuestión.

Una primera aproximación consiste en efectuar la encriptación en base al paquete de transmisión de protocolo en tiempo real, el cual es un procedimiento relativamente simple y es excelente para la protección de la transmisión propiamente dicha. Una encriptación de ese tipo se encuentra descrita en el documento WO 99/37056. Alternativamente, puede lograrse un nivel de protección mayor que también se mantendrá vigente en el lado del receptor: esto puede hacerse al tener la encriptación implementada en base a la estructura de trama de los datos fuente o datos de usuario. También es factible implementar una combinación de los dos enfoques anteriores. Ahora, la encriptación deberá ejecutarse ventajosamente en un componente estándar que no tenga necesidad de efectuar ningún procesamiento previo complicado para encontrar el inicio de una trama. Por lo tanto, todos los procedimientos anteriores necesitarán un mecanismo fácil para encontrar directamente el comienzo de las tramas.

Sumario de la invención

En consecuencia, entre otras cosas, es un objeto de la presente invención añadir información de localización específica que permita al mecanismo codificador, y posiblemente también al mecanismo decodificador, encontrar de forma fácil y rápida el comienzo de las distintas tramas.

Ahora, por lo tanto, según uno de sus aspectos, la invención se caracteriza de acuerdo con la parte caracterizadora de la reivindicación 1.

Además de lo anterior, el presente inventor ha reconocido que una ligera modificación a lo anterior, puede permitir que solamente se esté encriptando de manera efectiva una parte de los datos de usuario, mientras que habilita la localización inmediata de tales diversas partes encriptadas, tal como se expone en la reivindicación 2. La invención se refiere también a un sistema que se dispone para la implementación del método según la reivindicación 1, a un aparato transmisor y a un aparato receptor para su uso en tal sistema, y a una señal generada por un aparato transmisor de este tipo. Otros aspectos ventajosos de la invención se exponen en las reivindicaciones dependientes.

Breve descripción de los dibujos

Estos y otros aspectos y ventajas de la invención, se discutirán con mayor detalle a continuación en el presente documento haciendo referencia a la descripción de las realizaciones preferidas, y en particular haciendo referencia a las figuras adjuntas, las cuales muestran:

La figura 1 es un sistema dispuesto para la implementación del método inventivo;

La figura 2 es una implementación de formato de datos para su uso en la presente invención, y

La figura 3 es un formato modificado con respecto a la figura 2, que presenta encriptación parcial.

Descripción detallada de las realizaciones preferidas

La cantidad de información contenida, tal como audio o vídeo en Internet, está mejorando debido a los continuos avances en la tecnología de codificación y en el ancho de banda de transmisión. Los proveedores de contenidos pretenden vender tales contenidos de alto valor, y por lo tanto, está surgiendo la necesidad de efectuar accesos condicionales o gestión de derechos digitales, tal como se conoce. Un sistema de acceso condicional de este tipo encriptará un elemento de contenido y posteriormente gestionará las claves de desencriptación asociadas de tal manera que solamente los usuarios finales autorizados estarán habilitados para desencriptar y reconstituir así el contenido original por completo.

Actualmente, los datos multimedia están estructurados, en general, en tramas, en los que el tamaño de una trama está relacionado con la categoría de la información. Además, el tamaño de una trama transmitida puede estar relacionado con el grado de compactación y con cualquier otro procesamiento al que se haya sometido con anterioridad a la encriptación. De hecho, las tramas pueden ser más grandes y también más pequeñas que los paquetes utilizados para la transmisión real. Por lo tanto, un único paquete de transmisión puede contener una o más tramas, o partes fraccionadas de una trama. El "Streaming" o "Transferencia de datos" es una tecnología en la que un cliente podrá reproducir, o usar de otro modo, el contenido tan pronto como llegue, de modo que no existirá descarga de todos, o de una parte sustancial de, los contenidos completos con anterioridad a la reproducción. La transferencia de datos permitirá la retransmisión de paquetes. El usuario del contenido tendrá que hacer frente a la pérdida de datos.

Ahora, para una protección óptima, el contenido está mejor encriptado a nivel de trama, incluso con un tamaño de trama no uniforme. Tal encriptación a nivel de trama permitirá una encriptación continua, o de extremo a extremo, que se aplica tanto a los contenidos transmitidos como a los contenidos almacenados. Preferiblemente, el componente del sistema que implementa la encriptación real es un componente genérico, y por lo tanto es independiente de servidores específicos de transferencia de datos específicos e independiente de los formatos específicos de las tramas. Una forma de conseguir esto consiste en

definir el componente de encriptación como un Protocolo de Transmisión en Tiempo Real, o traductor RTP. En la actualidad, virtualmente todos los servidores de transferencia de datos están utilizando el protocolo de transferencia de datos RTP. Por lo tanto, el componente de encriptación podría recibir paquetes RTP, encriptar la carga útil, y reenviar posteriormente los paquetes RTP encriptados. Alternativamente, la encriptación puede estar integrada con el servidor de transferencia de datos.

Alternativamente, la encriptación puede ejecutarse al nivel del paquete RTP. Esto protegerá la propia transmisión, mientras que cede parte de la protección en el lado del receptor tras la recepción. También, es posible una combinación de estas dos alternativas de encriptación, tal como asignando el nivel de encriptación apropiado basándose en una estrategia de eventualidad respecto a las instalaciones de hardware disponibles.

Un problema que se ha planteado consiste en que las cabeceras de las tramas deben permanecer sin encriptar, tal como cuando se efectúa la encriptación a nivel de trama. Esto requiere que el componente de encriptación genérica debería analizar las cargas útiles de los paquetes RTP para identificar las posiciones de las cabeceras de trama. Esto no obstante disminuiría el rendimiento del componente de encriptación, y también hará que el componente de encriptación sea dependiente de los formatos de trama reales.

La presente invención proporciona una solución al problema en cuestión, mediante la extensión de las cabeceras de los paquetes RTP de modo que incluyan punteros para aquellas partes de la carga útil del paquete que realmente necesiten ser encriptadas. Los punteros se configuran mediante el servidor de transferencia (streaming). El servidor puede realizar todo esto como parte de lo que se conoce como proceso de indicación, es decir, un análisis fuera de línea de los datos multimedia, de modo que los datos puedan transferirse de una manera más eficiente en un instante de tiempo posterior. El resultado de este proceso de indicación se almacena en paralelo al contenido en una denominada como pista de indicación.

La Figura 1 ilustra un sistema previsto para implementar el método de la invención. La entrada 23 recibe las tramas de datos de usuario, que se almacenan transitoriamente en un almacenamiento 22, que alberga el almacenamiento de una pluralidad de tales tramas. El bloque 24 de procesamiento une después a esos tramas de datos, informaciones de localización de cabecera de trama en el contexto de un paquete RTP, que pueden comprender una pluralidad de tales tramas de usuario, pero no necesariamente un número entero de las mismos. El resultado de este procesamiento se almacena transitoriamente en el bloque 26 que alberga múltiples cargas útiles RTP. Por cuestiones de brevedad, la pista de indicación específica mencionada más arriba no se ha representado separadamente. De hecho, el dispositivo de pista de indicación se reconocerá por los expertos en la técnica como dispositivo estándar. En la práctica, esa pista de indicación se implementará en el lado de entrada del bloque 23 para permitir indicar las diversas posiciones de paquete. Con anterioridad a la transmisión, los datos de usuario se encriptan en el módulo 28 de encriptación, y se transmiten por el dispositivo 30 de comunicación, tal como por Internet. El procedimiento completo en el lado del transmisor del sistema mostrado, puede sincronizarse mediante una unidad 20 de sincronización global, como se indica mediante las líneas punteadas que salen desde la misma.

En el lado de recepción, se efectúa la desencriptación mediante el dispositivo 34 de desencriptación, y el resultado de la misma se almacena transitoriamente en el bloque 36. La reconstitución de las tramas de usuario, se efectúa en el dispositivo 38 de procesamiento, seguido de un almacenamiento transitorio en el bloque 40. La aplicación de usuario se ha simbolizado a continuación mediante el bloque 42. Los bloques 38, 40 de almacenamiento no albergan la descarga de ningún programa completo o de una parte sustancial del mismo, sino que por el contrario proporcionarán alguna sincronización para proveer las variaciones de velocidad de transferencia del dispositivo 30 de comunicación. De nuevo, en el lado del receptor, la sincronización global se efectúa mediante el bloque 32 sincronizador.

La Figura 2 ilustra un ejemplo de implementación de formato de datos para usar según la presente invención. Por brevedad, solamente se muestra una única implementación. Diversos bloques 50-60 de datos de la configuración RTP se han representado en la figura. De éstos, los bloques 54-60 constituyen la carga útil de RTP, conteniendo los bloques 56, 60 en cada caso, una carga útil de trama encriptada, y los bloques 54, 58 contienen las cabeceras de trama asociadas. Obsérvese que las longitudes de los bloques 56, 60 no necesitan ser uniformes. El bloque 50 contiene una cabecera RTP y le sigue el bloque 52 que contiene punteros. Según se muestra en la figura, los punteros 62 indican tanto el comienzo como el final de cada carga útil de trama encriptada. Ahora, la cabecera 50 se encuentra en la pista de indicación; los punteros 52 son extensiones de la cabecera 50 RTP. Esta pista de indicación se utiliza por el servidor de transferencia de datos para el empaquetamiento de los paquetes RTP.

La Figura 3 ilustra un formato modificado con respecto a la Figura 2, que tiene una encriptación parcial de los datos de usuario. Por brevedad, solamente se han indicado específicamente los aspectos que se diferencian de la Figura 2. Dentro de la carga útil de la trama, la discriminación entre los datos de usuario encriptados (E) y desencriptados, se ha indicado mediante una línea inclinada. La información de localización indicada mediante 62, indicará (63, 65) específicamente en este caso los finales de las partes encriptadas respectivas, suponiendo que la encriptación empiece a partir del comienzo de los datos de usuario de la trama. Por supuesto, pueden utilizarse otras encriptaciones parciales. La propia encriptación puede hacerse a nivel de una trama o de una trama parcial, a nivel de un paquete, o estar basada en una combinación de los mismos.

REIVINDICACIONES

1. Método para la transmisión o retransmisión en tiempo real de datos de usuario formateados en tramas, mientras que en los mismos antes de esta (re) transmisión se realiza un procedimiento de encriptación,

estando dicho método **caracterizado** por la etapa de unir a dichos datos de usuario datos apropiados de localización de tramas de datos, en asociación con someter dichos datos de usuario a dicho procedimiento de encriptación, y situar tales datos de localización de tramas en posiciones de regulación predeterminadas que, también como informaciones de cabecera, son excluidos de dicho procedimiento posterior de encriptación.

2. Método según la reivindicación 1, en el que se somete solamente una parte de dichos datos de usuario al procedimiento de encriptación, mientras que se proporcionan datos de localización de encriptación en dichas posiciones de regulación para discriminar las partes encriptadas y no encriptadas de los datos de usuario.

3. Método según las reivindicaciones 1 ó 2, en el que tales posiciones de regulación son posiciones de información de extensión de cabecera.

4. Método según las reivindicaciones 1 ó 2, en el que los datos de usuario tras la encriptación se transmiten en paquetes RTP, y en el que dichos datos de usuario están encriptados a nivel de dicho paquete RTP.

5. Método según se reivindica en las reivindicaciones 1 ó 2, en el que dichos datos de usuario están encriptados a nivel de tramas.

6. Método según las reivindicaciones 4 ó 5, en el que dicha transmisión permite impartir tramas parciales a un paquete, así como permite impartir una pluralidad de tramas a un único paquete.

7. Método según la reivindicación 3, en el que dicha posición de información de extensión de cabecera posee una pluralidad de datos de localización de trama.

8. Método según las reivindicaciones 1 ó 2, en el que tales posiciones de regulación están situadas en el interior de una pista de indicación separada.

9. Sistema previsto para implementar un método según la reivindicación 1, y que tiene medios de transmisión para transmitir o retransmitir en tiempo real datos de usuario formateados en tramas y medios de encriptación para realizar antes de tal (re)transmisión un procedimiento de encriptación en base a dichos datos de usuario,

estando dicho sistema **caracterizado** porque comprende, a continuación de dichos medios de encriptación, medios de unión para unir a dichos datos de usuario, datos de localización de tramas y colocar tales datos de localización de tramas en posiciones de regulación predeterminadas que, al igual que las informaciones de cabecera, son excluidos de dicha encriptación posterior.

10. Sistema según la reivindicación 9, y que está previsto para servir de interfaz para Internet, como medio de transmisión.

11. Aparato transmisor que está previsto para su uso como estación en un sistema según la reivindicación 9.

12. Señal generada por una estación según la reivindicación 11.

13. Aparato receptor que está previsto para su uso en un sistema según la reivindicación 9, y que posee medios de desencriptación para desencriptar, tras la recepción, los datos de usuario que han sido sometidos a dicho procedimiento de encriptación, con el fin de emitir los datos de usuario así desencriptados en base a las tramas que contienen dichos datos de usuario.

14. Aparato receptor según la reivindicación 13, en el que dichos medios de desencriptación son operativos a nivel de tramas.

15. Aparato receptor según la reivindicación 13, en el que dichos medios de desencriptación son operativos a nivel de paquetes.

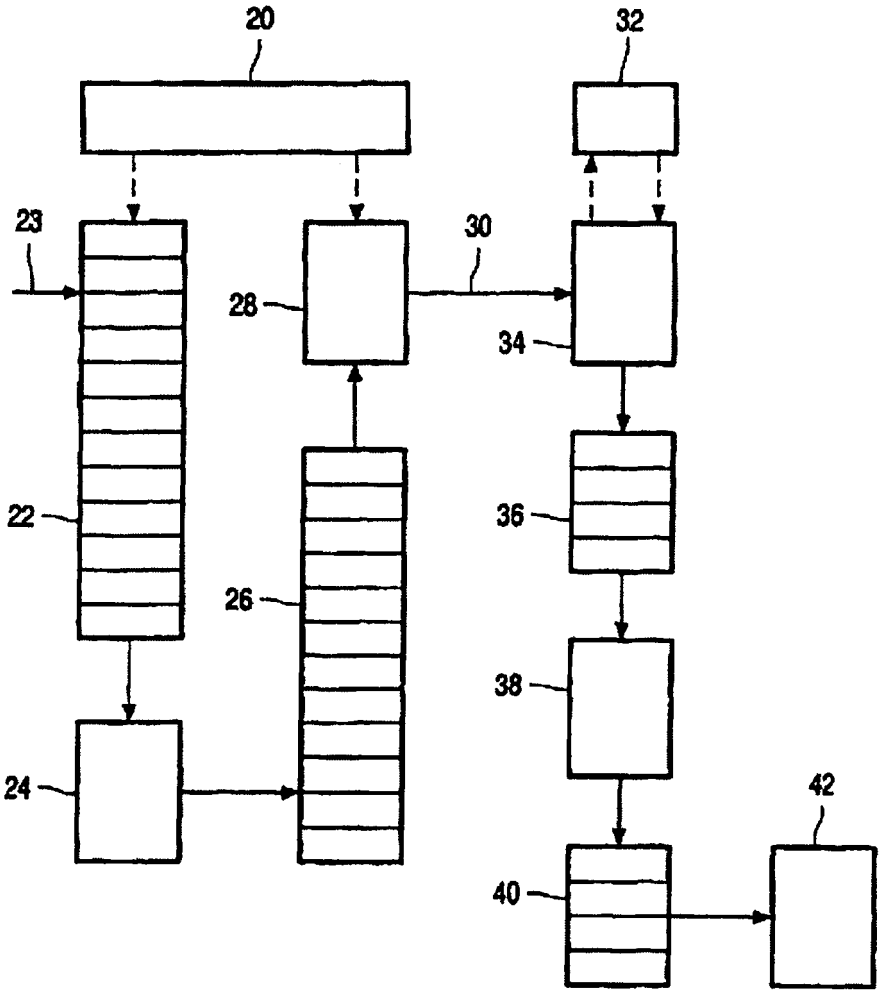

FIG. 1

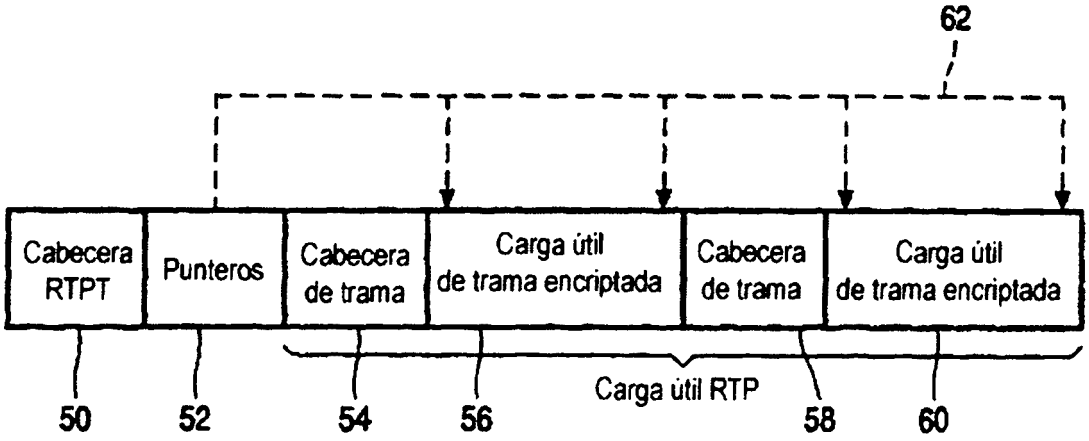
62
Cabecera RTPT
Punteros
Cabecera de trama
Carga útil de trama encriptada
Cabecera de trama
Carga útil de trama encriptada
Carga útil RTP
50
52
54
56
58
60

FIG. 2

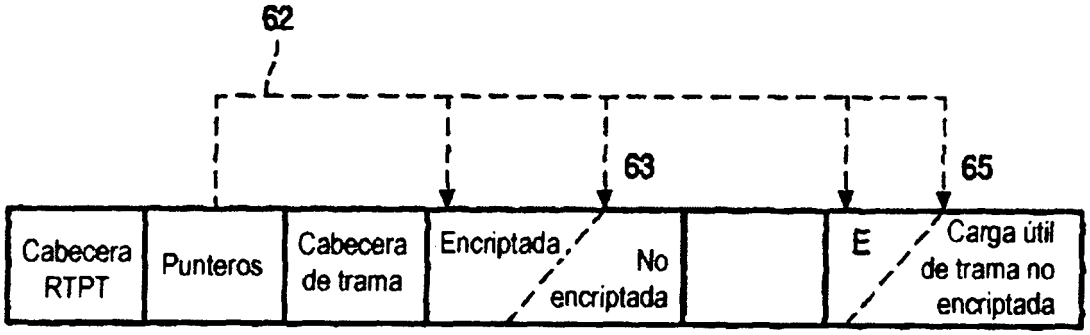
62
63
65
Cabecera RTPT
Punteros
Cabecera de trama
Encriptada
No encriptada
E
Carga útil de trama no encriptada

FIG. 3