(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 278 226**

(51) Int. Cl.:
H03M 13/35 (2006.01)
H04L 1/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03808793 .8**
(86) Fecha de presentación : **19.09.2003**
(87) Número de publicación de la solicitud: **1554812**
(87) Fecha de publicación de la solicitud: **20.07.2005**

(54) Título: **Sistema y método para proporcionar una recuperación frente a errores para vídeo codificado por FGS en flujo continuo en una red IP.**

(30) Prioridad: **15.10.2002 US 418634 P**
01.05.2003 US 467040 P

(45) Fecha de publicación de la mención BOPI:
01.08.2007

(45) Fecha de la publicación del folleto de la patente:
01.08.2007

(73) Titular/es: **Koninklijke Philips Electronics N.V.**
Groenewoudseweg 1
5621 BA Eindhoven, NL

(72) Inventor/es: **Li, Qiong;**
Van der Schaar, Mihaela y
Chen, Richard

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

DESCRIPCIÓN

Sistema y método para proporcionar una recuperación frente a errores para vídeo codificado por FGS en flujo continuo en una red IP.

La presente invención reivindicada se refiere al campo de datos multimedia en flujo continuo, particularmente datos codificados de manera escalable. De manera más específica, la presente invención reivindicada se refiere a la protección de tales datos.

La transmisión de vídeo o flujo continuo de vídeo dentro de redes de comunicación, tales como redes RDSI (Red Digital de Servicios Integrados) o Internet se ha convertido en una aplicación importante de tales redes de comunicaciones. En el futuro, se utilizarán normalmente redes móviles orientadas a paquetes como GPRS (Servicio General de Radio por Paquetes) y UMTS (Estándar/Sistema Universal de Telecomunicaciones Móviles) para conectar usuarios de móviles a redes de comunicación fijas tales como las redes RDSI o Internet anteriormente mencionadas. Por lo tanto es importante emplear un soporte eficaz e inteligente de flujo continuo de vídeo de alta calidad en redes de radio inalámbricas.

El problema de la ocultación de errores en comunicaciones de vídeo se está haciendo cada vez más importante debido al interés creciente en la entrega de vídeo comprimido a través de canales inalámbricos. Se han propuesto varios modos de transmisión orientados a paquetes para estándares inalámbricos de siguiente generación tales como EGPRS (Servicio General de Radio por Paquetes Realzado) o UMTS, que se basan en su mayor parte en el mismo principio: bloques de mensajes largos, normalmente paquetes IP (Protocolo de Internet) que introducen la parte inalámbrica de la red, se dividen en segmentos de longitud deseada, que pueden multiplexarse en paquetes de la capa de enlace de tamaño fijo. Los paquetes se transmiten entonces secuencialmente a través del enlace inalámbrico, se vuelven a reunir, y se pasan al siguiente elemento de la red. Sin embargo, comparado con las características del canal algo propicias de las redes de líneas de cables o fijas, los enlaces inalámbricos sufren de estados graves de desvanecimiento de la señal, ruido, e interferencia en general, dando como resultado por lo tanto una tasa de errores de bits residual relativamente alta tras la detección y decodificación.

Normalmente se utilizan dos tipos de métodos para recuperación frente a errores para soportar el flujo continuo de vídeo a través tanto de redes inalámbricas como cableadas: retransmisión y Corrección de Errores hacia Delante (FEC). La codificación FEC es una técnica bien conocida para conseguir una detección y corrección frente a errores en comunicaciones de datos. FEC tiene la desventaja de aumentar la sobrecarga de transmisión y por tanto, de reducir el ancho de banda utilizable para los datos de carga útil. Por lo tanto se utiliza en general con criterio en servicios de vídeo, debido a que los servicios de vídeo son muy demandantes de banda ancha pero pueden tolerar un cierto grado de pérdida. El método de retransmisión tiene la ventaja de una alta utilización de banda ancha, pero sufre de largos retardos de recuperación que pueden no ser tolerables para aplicaciones que tengan limitaciones estrictas de retardo.

En el pasado, ha habido una línea definida entre la utilización de uno u otro método. Un diseño de aplicación elige o bien retransmisión o bien FEC. Sin embargo, las redes basadas en IP, son heterogéneas y están en evolución. Es concebible que las aplicaciones pudieran funcionar en entornos de redes completamente diferentes, haciendo difícil predecir los estados de red. La situación hace difícil elegir el método adecuado para la recuperación frente a errores para todas las situaciones hipotéticas de funcionamiento posibles.

Una solución ideal para la recuperación frente a errores sería combinar retransmisión y FEC para de este modo permitir a una aplicación elegir dinámicamente una u otra, o si no combinarlas en tiempo real según estados de red percibidos.

La ARQ (arquitectura) híbrida y FEC adaptativa son dos métodos que combinan las virtudes de retransmisión y FEC. En la ARQ híbrida, los datos de vídeo se codifican previamente mediante algún esquema de codificación FEC, tal como un esquema de codificación Reed Solomon, y entonces el emisor y el receptor utilizan un protocolo de tipo ARQ especialmente diseñado para realizar la protección. En la FEC adaptativa, los datos FEC se separan de los flujos de datos multimedia originales, y se emplean comandos de “darse de alta”/“darse de baja” (“join”/“leave”) para conseguir una protección adaptativa. Sin embargo, la FEC adaptativa está limitada de dos maneras. En primer lugar, utiliza el Protocolo de Administración de Grupos de Internet (IGMP) para señalar la acción de darse de alta/darse de baja, lo que puede introducir una latencia muy larga en el proceso de señalización que finalmente anula el propósito de protección, tal como la retransmisión. En segundo lugar, mientras enfatiza el algoritmo de codificación de FEC, carece de una arquitectura y protocolos para llevar a cabo las metas de la FEC adaptativa.

El documento WO 97/33402-A1 da a conocer un sistema para transmitir un flujo de datos a través de una red, en el que se produce un flujo de bits de protección a partir del flujo de datos utilizando una técnica de codificación de canal.

Sería un avance en la técnica proporcionar una arquitectura realista que especificara los protocolos que son necesarios para llevar a cabo una protección adaptativa y eficaz, permitiendo de este modo a las aplicaciones conmutar entre diferentes estrategias de protección de manera dinámica.

Según ciertos aspectos de la presente invención, se proporcionan métodos y sistemas que permiten a un dispositivo de recepción (cliente) elegir dinámicamente recibir datos de protección y determinar el tipo de datos de protección que van a recibirse.

Por ejemplo, según ciertas implementaciones a modo de ejemplo de la presente invención, se proporciona un método para su uso en un servidor y un dispositivo de recepción correspondiente en comunicación con el servidor. El método incluye las acciones de: una primera acción de codificación para producir un capa base codificada a partir del flujo de bits utilizando una técnica de codificación de predicción de la trama; una segunda acción de codificación para producir una capa de mejora codificada a partir del flujo de bits utilizando una técnica de codificación escalable de grano fino (FGS); una primera acción de generación para generar al menos un flujo de bits de protección; una segunda acción de generación para generar una primera capa base que indica el flujo de bits; una tercera acción de generación para generar una primera capa de mejora que indica el flujo de bits; y una cuarta acción de generación para generar un primer flujo de bits de indicación de protección.

Según otro aspecto, la presente invención es un sistema que incluye: medios para producir una capa base codificada a partir del flujo de bits utilizando una técnica de codificación de predicción de la trama; medios para producir una capa de mejora codificada a partir del flujo de bits utilizando una técnica de codificación escalable de grano fino (FGS); medios para generar al menos un flujo de bits de protección; medios para generar un primer flujo de bits de indicación de capa base; medios para generar una primer flujo de bits de indicación de capa de mejora; y medios para generar un primer flujo de bits de indicación de protección.

El sistema y método de protección frente a errores propuesto al que se hace referencia en el presente documento como de protección bajo demanda, proporciona un número de ventajas sobre la técnica anterior, que incluyen: (1) el método puede ajustarse de manera ventajosa en una arquitectura de flujo continuo FGS global; (2) el método soporta tanto aplicaciones multidifusión como unidifusión; (3) el método aprovecha al máximo el formato de archivo MPEG-4, permitiendo de ese modo a un servidor de MPEG-4 de uso general realizar una protección frente a errores adaptativa en aplicaciones de flujo continuo; (4) los datos de protección están separados de los datos protegidos. De esta manera, el cambio de datos de protección puede cambiar la estrategia o el nivel de protección, aunque los procedimientos de protección continúan siendo los mismos; (5) el método permite a las aplicaciones elegir dinámicamente entre la protección de tipo retransmisión o la protección de tipo FEC o la ARQ híbrida, consiguiendo de este modo un mejor rendimiento de la protección; (6) el método utiliza el Protocolo de Transporte de Tiempo Real (RTSP) en vez del Protocolo de Administración de Grupos de Internet (IGMP) que puede conseguir una protección más rápida y proporcionar más flexibilidad a las aplicaciones.

La invención se define en la reivindicación 1 del método independiente y en la reivindicación 11 del sistema independiente.

Haciendo referencia ahora a los dibujos en los que los números de referencia iguales representan siempre partes correspondientes:

la figura 1 ilustra una red a modo de ejemplo para realizar una transmisión de extremo a extremo de datos multimedia de flujo continuo en la que puede realizarse la presente invención; y

la figura 2 ilustra, a modo de ejemplo, una arquitectura y los protocolos asociados para implementar el esquema de protección de la invención.

Los siguientes términos se definen para entender mejor la presente invención:

Transmisión en flujo continuo de datos multimedia ("Streaming media"), significa de manera esencial la entrega en tiempo real o en tiempo casi real de contenido crítico (por ejemplo, datos de audio y/o vídeo) a un dispositivo o dispositivos cliente del usuario que se suscribe. El dispositivo/dispositivos cliente interpreta los datos multimedia transmitidos de una manera que es apropiada para el dispositivo cliente y los datos multimedia.

Protocolo RTP, se utiliza como el método estándar para formar paquetes basado en tiempo real en muchos entornos y se sitúa justo por encima de las capas de transporte en un pila de protocolos, tales como UDP (Protocolo de Datagramas de Usuarios)/IP(Protocolo de Internet). De manera general, el RTP es un protocolo de transporte para datos en tiempo real, y proporciona un marcado de la hora, número de secuencia, detección de pérdida de datos, seguridad, identificación de contenido, y otros datos relevantes para la entrega de datos en tiempo real. El RTP puede utilizarse en un contexto multidifusión o unidifusión.

Protocolo RTSP, un protocolo a nivel de aplicación, que significa Protocolo de Sesión en Tiempo Real, se ha desarrollado también para ofrecer un mecanismo de descripción de contenido y gestión de sesión. El RTSP describe cómo transmitir el contenido desde un servidor a un cliente. La transmisión en flujo continuo comprende dividir el contenido en paquetes que tienen tamaños razonables (con respecto a características de red intermedias) para la transmisión entre el servidor y cliente.

FEC, Corrección de Errores hacia Delante es una técnica de corrección frente a errores bien conocida que proporciona un mecanismo mediante el que un dispositivo de envío proporciona a un dispositivo de recepción datos de

FEC adicionales que el dispositivo de recepción puede utilizar posteriormente para detectar y corregir errores en los datos recibidos. Por lo tanto, para soportar la FEC el dispositivo de envío incluye normalmente un codificador de FEC y el dispositivo de recepción incluye normalmente un decodificador de FEC. La FEC permite diferentes niveles de codificación. Los diferentes niveles de codificación pueden expresarse mediante una relación de densidad en base a la cantidad de datos de FEC generados para una cantidad determinada de datos. Por lo tanto, por ejemplo, en ciertos sistemas el nivel de codificación de FEC puede ser "alto" cuando hay una relación de un paquete de FEC por cada paquete de datos. En otros sistemas, el nivel de codificación de FEC puede ser "inferior" de modo que hay una relación de un paquete de FEC por cada cuatro paquetes de datos.

En la siguiente descripción, con fines explicativos más que de limitación, se exponen detalles específicos tales como la arquitectura particular, interfaces, técnicas, etc., con el fin de proporcionar un entendimiento perfecto de la presente invención. Con el fin de simplificar y clarificar, se omiten descripciones detalladas de dispositivos, circuitos, y métodos bien conocidos para no confundir la descripción de la presente invención con detalles innecesarios.

En el presente documento se supone que el Protocolo de Transporte de Tiempo Real (RTP) y el Protocolo de Transferencia en Tiempo Real (RTSP) subyacen a la entrega de contenido al cliente, puesto que estos protocolos son bien conocidos. Un experto en la técnica apreciará que estos protocolos se tratan en el presente documento con fines a modo de ejemplo debido sólo a su amplia familiaridad para los expertos y a que puede utilizarse cualquier protocolo que proporcione las características de señalización a las que se hace referencia en el presente documento.

En un aspecto, la presente invención se refiere a un sistema y métodos asociados para proporcionar al menos un flujo de protección de datos multimedia, independiente de un flujo de datos multimedia asociado, y que además proporciona al menos una pista de indicación de datos multimedia para facilitar la transmisión del flujo de datos multimedia por una red y al menos un flujo de datos de protección para facilitar la transmisión del al menos un flujo de protección de datos multimedia a través de la red.

En un aspecto relacionado, la presente invención se dirige a un sistema y métodos asociados para permitir a una aplicación la libertad de elegir dinámicamente un esquema de protección frente a errores a petición.

Aunque lo siguiente se dirige en particular a FGS de MPEG-4, para un experto en la técnica será evidente que la invención puede aplicarse de manera ventajosa a cualquier esquema de codificación escalable.

Los principios y funcionamiento del método y un sistema para proporcionar un esquema de protección frente a errores por una red IP pueden entenderse mejor con referencia a los dibujos y la descripción adjunta.

Las figuras 1 y 2, tratadas a continuación, y las diversas realizaciones utilizadas para describir los principios de la presente invención en este documento de patente son sólo a modo de ilustración y no deben considerarse de ningún modo como limitativas del alcance de la invención. Los expertos en la técnica entenderán que los principios de la presente invención pueden implementarse en cualquier decodificador y codificador de vídeo dispuesto adecuadamente.

La presente invención proporciona protocolos específicos y una arquitectura novedosa para proporcionar una capacidad para proporcionar un esquema de protección frente a errores eficaz y que puede adaptarse, para su utilización en una red, tal como el mostrado en la figura 1, permitiendo con ello que las aplicaciones conmuten dinámicamente entre diferentes estrategias de protección frente a errores, tal como se describirá.

La figura 1 ilustra una representación simplificada de una realización de un sistema 100 que incorpora la invención. Tal como se muestra, un cliente 130 y un servidor 118 están en comunicación a través de una red 120. El sistema 100 a modo de ejemplo es sólo un ejemplo de un sistema adecuado y no pretende sugerir ninguna limitación con respecto al alcance de utilización o funcionalidad de los aparatos y métodos mejorados descritos en el presente documento.

Con fines ilustrativos, la siguiente descripción supondrá que se ha convertido una señal de vídeo o de audio en un flujo de datos digitales (un flujo de datos multimedia) y debe transmitirse en una red desde un nodo 110 fuente, a través de un servidor 118, hasta un nodo 130 destino (por ejemplo, el cliente). La descripción supondrá además a modo de ejemplo que el flujo de datos digitales, o carga útil, se ha dividido en una secuencia de tramas o paquetes de carga útil. Según la realización de la presente invención, el codificador 110 de vídeo (nodo fuente) incluye una fuente 112 de tramas de vídeo, un codificador de vídeo que incluye un codificador 114a de capa base y un codificador 114b de capa de mejora y una memoria 116 intermedia del codificador. La fuente 112 de tramas de vídeo puede ser cualquier dispositivo que pueda generar una secuencia de tramas de vídeo no comprimidas, incluyendo una antena de televisión y una unidad de recepción, un reproductor de videocasete, una cámara de vídeo, un dispositivo de almacenamiento en disco que pueda almacenar un video clip "en bruto", y similares. Las tramas de vídeo sin comprimir, procedentes de la fuente 112 de tramas de vídeo, entran en el codificador 114 de vídeo a una tasa de imágenes determinada (o "tasa de flujo continuo") y se comprimen según cualquier dispositivo o algoritmo de compresión conocido, tal como un codificador de MPEG-4. El codificador 114 de vídeo transmite entonces las tramas de vídeo comprimidas a la memoria 116 intermedia del codificador para almacenar en memoria intermedia como preparación para la transmisión por la red 120 de datos a través del servidor 118. Se indica que el codificador 110 de vídeo puede ejecutar o bien externamente a o bien dentro de un servidor 118 de uso general.

La red 120 de datos puede ser cualquier red adecuada y puede incluir partes tanto de redes de datos públicas, tal como Internet, y redes de datos privadas, tales como una red de área local (LAN) perteneciente a una empresa, una red de área metropolitana (MAN) o una red de área amplia (WAN).

En función de la aplicación, el nodo 130 destino (cliente), que recibe los datos multimedia de flujo continuo, puede realizarse de muchas maneras diferentes, incluyendo un ordenador, un dispositivo de entretenimiento de mano, un módulo de conexión "set-top box", una televisión, un Circuito Integrado para Aplicaciones Específicas (ASIC), etc. El nodo 130 destino (cliente) incluye una memoria 132 intermedia del decodificador, un decodificador 134 de vídeo y una visualizador 136 de vídeo.

La figura 2 ilustra, a modo de ejemplo, una arquitectura y protocolos asociados para implementar el esquema de protección de la invención que tiene acciones 1-5 mostradas como A1-A5.

Acción 1

En la acción 1 de la figura 2 se muestra un archivo mp4 codificado mediante FGS. El archivo .mp4 puede codificarse tal como en el codificador 112 de vídeo (véase la figura 1) usando técnicas de FGS en las que en primer lugar se utiliza una parte de los datos de vídeo para producir una capa 202 base (BL). A continuación se genera una capa 204 de mejora (EL) usando las imágenes residuales compensadas por movimiento. A continuación se generan las imágenes residuales compensadas por movimiento a partir de los datos de vídeo y la capa 202 base (BL) utilizando una técnica de codificación de grano fino. Tal como se conoce bien en la técnica, la codificación FGS representa un tipo de escalabilidad de vídeo. Las imágenes codificadas con este tipo de escalabilidad pueden decodificarse progresivamente. En otras palabras, el decodificador puede empezar a decodificar y visualizar la imagen sin necesidad de recibir todos los datos utilizados para codificar esa imagen. A medida que se reciben más datos, se mejora progresivamente la calidad de la imagen decodificada hasta que se recibe, decodifica y visualiza toda la información.

Además de generar la capa 204 de mejora y la capa 202 base de FGS, según los principios de la invención, se generan múltiples flujos de datos de protección, pudiendo seleccionar cada uno de manera dinámica mediante el cliente según demanda. Se muestran flujos de datos de protección separados e independientes, asociado cada uno con el archivo .mp4. Puede construirse una primera pista 206 de protección (EP1), por ejemplo, según los principios de la protección frente a errores FEC. Puede construirse una segunda pista 208 de protección (EP2), por ejemplo, según los principios de protección frente a errores de retransmisión. Puede construirse una tercera pista 210 de protección (EP3), por ejemplo, según un esquema híbrido que incorpora características de protección frentes a errores FEC y protección frente a errores de retransmisión. Cada uno de los tres esquemas de protección puede seleccionarse de manera dinámica mediante el cliente según demanda.

Acción 2

Los principios de indicación multipista se enseñan en la solicitud de patente de los EE.UU. en tramitación junto con la presente número de serie 60/451.916 presentada el 4 de marzo, 2003, titulada "System and Method for transmitting scalable coded video over an IP network". Según los principios de la indicación multipista enseñados en la misma, un método de procesamiento previo, al que se hace referencia como indicación de multipista, compatible hacia atrás con el estándar de formato de archivo de datos multimedia MPEG-4 actual, hace posible utilizar un servidor de flujo continuo de MPEG-4 de uso general para transmitir el vídeo por capas de manera eficaz según características de canal variables, restricciones de complejidad y preferencias de usuario. Esto es, el servidor, sin una gran modificación, puede usar automáticamente múltiples canales (es decir, conexiones RTP), proporcionando con ello al sistema de flujo continuo la flexibilidad para adaptarse a estados de red (por ejemplo, ancho de banda disponible) ajustando el número de capas escalables que han de transmitirse. A medida que disminuye el ancho de banda disponible de la red, el servidor requiere menos pistas de indicación porque una parte menor del flujo de vídeo se transmite de forma escalable para cumplir con el ancho de banda disminuido.

Tal como muestra la figura 2, un módulo 214 de indicador genera una pista 216a de indicación (es decir, una indicación 1) para facilitar la transmisión de la capa 202 base codificada de FGS por una red de datos tal como, por ejemplo, la red 120 de datos. Además, el módulo 214 de indicador genera una pluralidad de pistas de indicación, es decir (pistas 2-5 de indicación) 216b-e, asociándose cada una con una capa 204 de mejora (EL).

Una característica de la presente invención es que cada una de las pistas de protección, es decir, EP1, EP2 y EP3, puede utilizar de manera ventajosa los principios del método de indicación de múltiples pistas para de este modo proporcionar una protección frente a errores según los estados de red predominantes. Esto es, pueden usarse múltiples pistas de indicación para transmitir la pista de protección a través de múltiples conexiones RTP en gran parte de la misma manera a como se realiza para el archivo de datos padre .mp4, tal como se describe en la solicitud en tramitación junto con la presente 60/451.916, a la que se hizo referencia anteriormente. Esta flexibilidad para transmitir la pista de protección por la red se ilustra a modo de ejemplo en la figura 2 en la que se muestran múltiples pistas de indicación asociadas con cada una de las pistas de protección, por ejemplo, EP1-3. Específicamente, para la primera pista 206 de protección EP1, el indicador 214 genera pistas 6 y 7 de indicación, designadas como 216f y 216g. Para la pista 208 de protección EP2, el indicador 214 genera pistas 8, 9 y 10 de indicación, designadas respectivamente como 216h, 216i y 216j. Asociado con la pista 210 de protección EP3, el indicador 214 genera una única pista 11 de indicación, 216k.

En el presente contexto, las enseñanzas de la solicitud en tramitación junto con la presente 60/451.916, a la que se hizo referencia anteriormente, siguen siendo verdaderas, sin embargo, adicionalmente, se utilizan pistas de indicación para transmitir pistas de protección para proteger flujos de datos que se transmiten por la red. Específicamente, los flujos de datos de protección pueden transmitirse de forma escalable por la red en conformidad con un estado de red medido. Sin embargo, el estado de red de interés en el presente contexto no es el ancho de banda, como lo es para el flujo de datos de vídeo, sino por el contrario la tasa de pérdida de paquetes medida. Debido a que la tasa de pérdida de paquetes se determina para ser creciente existe una necesidad o una protección frente a los errores creciente. En consecuencia, se utilizarán pistas de indicación adicionales superiores al número usado inicialmente para facilitar la transmisión de los flujos de datos de protección para compensar el aumento medido en la tasa de pérdida de paquetes.

Como un ejemplo específico, se hace referencia a la pista 208 de protección a modo de ejemplo EP2, que tiene asociadas con ella tres pistas 8-10 de indicación, 216h-j, que se generaron simultáneamente con la pista 208 EP2. Supongamos que la tasa de pérdida de paquetes medida inicialmente es tal que sólo se requiere inicialmente un subconjunto de las tres pistas de indicación para facilitar la parte escalable del flujo 208 de datos de protección EP2 necesario para satisfacer un umbral de pérdida de paquetes predeterminado, por ejemplo, la pista 8 de indicación 216h. Supongamos ahora que la tasa de pérdida de paquetes aumenta en algún punto. Entonces puede ser necesario utilizar una o varias pistas de indicación adicionales asociadas con el flujo 208 de datos de protección EP2 para compensar el estado de red degradado (es decir, aumentar la tasa de pérdida de paquetes). Por ejemplo, puede ser necesario en algún punto utilizar las tres pistas 8-10 de indicación 216h-j para de este modo proporcionar la mayor parte escalable del flujo 208 de datos de protección EP2.

La descripción anterior se proporciona para ilustrar una característica de la invención. Es decir, los flujos de datos de protección novedosos pueden transmitirse de manera escalable por la red de la misma manera que el flujo de datos de vídeo padre siendo la distinción que el flujo de vídeo padre se modifica de manera escalable según un cambio medido en el ancho de banda de la red mientras que los flujos de datos de protección se modifican de manera escalable según el cambio medido en la tasa de pérdida de paquetes. En el caso anterior, cuando disminuye el ancho de banda, se requiere menos pistas de indicación. De forma similar, y en el último caso, cuando la tasa de pérdida de paquetes disminuye, se requieren menos pistas de indicación.

Acción 3

Según los principios de la invención, el cliente 130, en cualquier punto en el tiempo, puede suscribirse o darse de baja de forma dinámica para recibir un canal de protección. En consecuencia, el cliente 130 necesita monitorizar su calidad de recepción y activar el canal de protección de manera activa cuando lo considere necesario. Para iniciar la protección frente a errores según el método de la invención, un cliente debe conocer en primer lugar el tipo de protección frente a errores disponible en el servidor. Como tal, se requiere un mecanismo para informar a los clientes de la disponibilidad y descripción de los tipos de protección frente a errores disponibles desde el servidor. Este mecanismo se ejecuta preferiblemente realizando inicialmente un Protocolo de Descripción de Sesión (SDP) entre el cliente y el servidor.

Generalmente, el SDP es un protocolo que pretende describir sesiones multimedia para el anuncio de sesiones, invitaciones a sesiones, y otras formas de inicio de sesiones multimedia. También se mantiene mediante el IETF ("Internet Engineering Task Force", Grupo de Trabajo en Ingeniería de Internet), y la información adicional referente a SDP se encuentra en Internet en www.ietf.org en general, y en www.ietf.org/rfc/rfc2327.txt en particular. La presente invención amplía la funcionalidad del SDP para incluir protocolos que transportan información adicional al cliente con respecto la disponibilidad y características de protección frente a errores disponible desde el servidor.

En funcionamiento, el protocolo SDP se realiza entre cliente y servidor antes de hacer una petición de suscripción para un archivo de datos de vídeo, por ejemplo, un archivo .mp4. La sesión de protocolo SDP permite que el cliente aproveche diferente información sobre la sesión. Lo que es más importante, el cliente conoce qué opciones están disponibles referentes a la protección frente a errores. Concretamente, los tipos de protección frente a errores disponibles, los números de pistas, etc. El cliente almacena esta información que puede usarse posteriormente si el cliente debiera, en algún punto durante la transmisión del archivo fuente de vídeo, determinar que la protección frente a los errores está garantizada.

En el evento el cliente realiza una determinación de que la protección frente a errores está garantizada, el cliente pide la protección frente a errores haciendo en primer lugar una petición de suscripción al servidor usando el protocolo RTSP. Tal como se describió anteriormente, el protocolo RTSP es un protocolo de nivel de aplicación, que ofrece un mecanismo de descripción de contenido y gestión de sesión. Esto es, el protocolo RTSP describe cómo transmitir un contenido desde un servidor hasta un cliente. La petición se transmite por la red 120 IP usando una tecnología de conmutación de paquetes basada en IP común tal como el Protocolo de Control de Transmisión (TCP). Tal como bien se conoce en la técnica, el protocolo TCP es un sistema de protocolo de red que es independiente del sistema operativo de red u ordenador y las diferencias arquitectónicas. Suponiendo que no existe un canal de comunicación preexistente entre el cliente y el servidor, un servidor recibe una petición de suscripción de cliente. Una petición de suscripción de cliente a modo de ejemplo puede tener la forma siguiente:

Cliente -> Servidor

1. SET_PARAMETER rtsp://130.140.67.83/sample.mp4 RTSP/1.0
2. CSec:32
3. Sesión: 3453643
4. Longitud-Contenido: 35
5. Tipo-Contenido: texto/booleano/número entero
6. Pista 11: 1 .//debe ajustarse la pista 11ª a 1(ACTIVA)
7. Intervalo: 34521- 34570 // se requieren 50 paquetes,
8. (start seq. #

- end seq. #) //

De particular importancia en la petición de suscripción anterior, son las líneas 6 y 7. Específicamente, el cliente ha realizado una petición de suscripción para activar la pista 11 de protección para el intervalo de paquetes designados por los identificadores 34521- 34570 de paquetes. Esto es, el cliente ha realizado una determinación de que el intervalo específico de paquetes especificado se ha alterado o caído y desea recuperarlos a través del canal 11 de protección. El canal 11 de protección puede ser análogo a cualquier número de esquemas de protección frente a errores proporcionados por el servidor incluyendo la protección frente a errores FEC, la protección frente a errores de retransmisión, o un esquema híbrido.

Siguiendo con referencia a la figura 2, el canal 11 de protección puede ser análogo a la pista EP1 o EP2 o EP3 de protección, por ejemplo.

Como respuesta a la petición de suscripción basada en el cliente, el servidor puede responder al cliente con una confirmación que puede tener la forma siguiente:

Servidor -> Cliente

1. RTSP/1.0 200OK
2. CSec:32
3. Fecha: 28 Ene 2002 15:33:10 GMT

Tal como se destacó en la línea 6 de la petición de suscripción anterior, debería observarse que una característica de la presente invención, es la flexibilidad proporcionada en permitir a un cliente seleccionar dinámicamente un esquema de protección de entre una pluralidad de posibilidades de protección frente a errores disponibles del servidor. Esta flexibilidad representa un contraste con respecto a enfoques de la técnica anterior que limitan a un cliente a seleccionar sólo un único método de protección frente a errores inmodificable, por ejemplo, o bien protección FEC o de retransmisión. De manera ventajosa, al mantener el(los) canal(es) de protección como flujos de datos definidos separados del flujo de datos correspondiente, se ponen a disposición del cliente múltiples opciones de protección frente a errores según demanda. Además, al separar los datos de protección de los datos protegidos, el cambio de los datos de protección puede cambiar la estrategia o el nivel de protección, aunque los procedimientos de protección permanecen iguales.

A continuación, se describirá con más detalle cómo un cliente selecciona un esquema de protección de entre los esquemas de protección que se han puesto a disposición en el servidor.

Según una realización, el cliente puede seleccionar un esquema de protección a través del parámetro de intervalo (véase línea 7 anterior, es decir, intervalo 34521-34570). Esto es, siempre que el número de secuencia final en el intervalo, por ejemplo, 34570, se especifique para ser infinito como parte de la petición, el servidor puede suponer que el cliente desea un modo de protección frente a errores de tipo FEC, por ejemplo. Alternativamente, siempre que el número de secuencia terminal sea igual al número de secuencia de inicio + 1, puede suponerse que el cliente desea un modo de protección de tipo de retransmisión. Si no se selecciona ninguna de estas dos opciones, se supone que el cliente desea un modo de transmisión híbrido (por ejemplo, una combinación de FEC y retransmisión), tal como se indica en el ejemplo anterior (es decir, el número de secuencia final > 1 + número de secuencia de inicio y no igual a infinito).

Otros modos para seleccionar un esquema de protección, no enumerados explícitamente en el presente documento, también se encuentran dentro del propósito de la invención.

Siguiendo con referencia a la figura 2, posteriormente al envío de confirmación en respuesta a la petición de suscripción del cliente, el servidor carga las pistas de indicación apropiadas y crea una conexión RTP para cada pista de indicación. En el ejemplo mostrado, la conexión 218a RTP se crea para la pista 1 de indicación, 216a, las conexiones 218b-e RTP se crean para pistas 216b-e de indicación, respectivamente. Supongamos, con fines explicativos que el cliente 130 selecciona la pista de protección EP1, en este caso las pistas 6 y 7 de indicación, 216f y 216g, respectivamente se cargan y se crean las conexiones 218f y 218g RTP. Debe apreciarse que se crean conexiones RTP dedicadas adicionales, por ejemplo 218f y 218g, para facilitar la transferencia de datos de protección.

Acción 4

En la acción 4, el cliente 130 crea una conexión RTP correspondiente a la descrita anteriormente en la acción 3 para facilitar la transferencia de datos de vídeo y los datos de pistas de protección correspondientes.

Acción 5

En la acción 5, los flujos de datos de vídeo codificados por FGS transmitidos, es decir BL 202 y EL 204 se decodifican y visualizan.

Las anteriores descripciones de realizaciones específicas de la presente invención se han presentado con fines de ilustración y descripción. No pretenden ser exhaustivos o limitar la invención a las formas precisas descritas, y evidentemente son posibles muchas modificaciones y variaciones en vistas de la enseñanza anterior. Las realizaciones se eligieron y describieron para explicar de la mejor manera los principios de la invención y su aplicación práctica, para de este modo permitir a otros expertos en la técnica utilizar de la mejor manera la invención y diversas realizaciones con diversas modificaciones adecuadas al uso particular considerado. Se pretende definir el alcance de la invención mediante las reivindicaciones adjuntas al presente documento.

REIVINDICACIONES

1. Método de transmisión de un flujo (202, 204) de bits a través de una red (120) desde un dispositivo (114) de envío a un dispositivo (130) de recepción, comprendiendo el método:

- una acción de codificación para producir al menos un flujo (206) de bits de protección a partir de dicho flujo (202, 204) de bits utilizando una técnica de codificación de canal y para producir al menos un flujo (208) de bits de protección adicional a partir de dicho flujo (202, 204) de bits utilizando una técnica de codificación de canal adicional;

caracterizado porque el método comprende además

- una acción de generación para generar al menos una pista (216f, 216g) de indicación a partir de dicho flujo (206) de bits de protección y para generar al menos dos pistas (216h, 216i, 216j) de indicación adicionales a partir de dicho flujo (208) de bits de protección adicional, en la que dicha al menos una pista (216f, 216g) de indicación se asocia con dicho al menos un flujo (206) de bits de protección en una relación de varios a uno y

en el que dichas al menos dos pistas (216h, 216i, 216j) de indicación adicionales se asocian con dicho al menos un flujo (208) de bits de protección adicional en una relación de varios a uno.

2. Método según la reivindicación 1 que comprende adicionalmente una acción de almacenamiento para almacenar dicho al menos un flujo (206) de bits de protección y dicho al menos un flujo (208) de bits de protección adicional y dicha al menos una pista (216f, 216g) de indicación y dichas al menos dos pistas (216h, 216i, 216j) de indicación adicionales en un medio de almacenamiento.

3. Método según la reivindicación 1 que comprende adicionalmente las acciones de:

- recibir a partir de dicho dispositivo (130) de recepción una petición de corrección de errores; y

- extraer un primer flujo (206) de bits de protección de entre dichos flujos (206, 208) de bits de protección según las pistas (216f, 216g) de indicación asociadas de entre dichas pistas (216f-216j) de indicación.

en el que dicho primer flujo (206) de bits de protección se produce en dicha acción de codificación y dichas pistas (216f, 216g) de indicación asociadas se generan en dicha acción de generación.

4. Método según la reivindicación 3, que comprende adicionalmente las acciones de:

- recibir posteriormente desde dicho dispositivo (130) de recepción una petición de corrección de errores modificada para la protección frente a errores en respuesta a un cambio del estado de red; y

- extraer al menos un flujo (208) de bits de protección modificado de entre dichos flujos (206, 208) de bits de protección producidos en dicha acción de codificación según las pistas (216h-216j) de indicación asociadas;

en el que dicho al menos un flujo (208) de bits de protección modificado se produce en dicha acción de codificación y dichas pistas (216h-216j) de indicación asociadas se generan en dicha acción de generación.

5. Método según la reivindicación 1, en el que dicho flujo (202, 204) de bits es una salida de flujo de datos según un método de codificación de fuentes.

6. Método según la reivindicación 1, en el que dichos flujos (206, 208) de bits de protección son flujos de datos producidos según métodos de codificación de protección de datos.

7. Método según la reivindicación 1, en el que dichas pistas (216h-216j) de indicación son flujos de datos generados según algoritmos de indicación.

8. Método según la reivindicación 7, en el que dichos algoritmos de indicación se optimizan según al menos un estado de red, protocolo de red y tipo de red.

9. Método según la reivindicación 1, en el que el dispositivo (130) de recepción es un dispositivo cliente y el dispositivo (114) de envío es un dispositivo servidor.

10. Medio legible por ordenador que lleva instrucciones para realizar una protección frente a errores, disponiéndose dichas instrucciones, tras la ejecución mediante uno o varios procesadores, para realizar las acciones del método según la reivindicación 1.

11. Sistema de protección frente a errores para trasmitir un flujo (202, 204) de bits a través de una red (120) desde un dispositivo (114) de envío a un dispositivo (130) de recepción y que comprende:

- medios para producir al menos un flujo (206) de bits de protección a partir de dicho flujo (202, 204) de bits utilizando una técnica de codificación de canal y para producir al menos un flujo (208) de bits de protección adicional a partir de dicho flujo (202, 204) de bits utilizando una técnica de codificación de canal adicional;

caracterizado porque el sistema de protección frente a errores comprende adicionalmente

- medios para generar al menos una pista (216f, 216g) de indicación a partir de dicho al menos un flujo (206) de bits de protección y para generar al menos dos pistas (216h, 216i, 216j) de indicación adicionales a partir de dicho flujo (208) de bits de protección adicional, en el que dicha al menos pista (216f, 216g) de indicación se asocia con dicho al menos un flujo (206) de bits de protección en una relación de varios a uno y

en el que dichas al menos dos pistas (216h, 216i, 216 j) de indicación adicionales se asocian con dicho al menos un flujo (208) de bits de protección adicional en una relación de varios a uno.

12. Sistema de protección frente a errores según la reivindicación 11, que comprende adicionalmente medios para almacenar dicho al menos un flujo (206) de bits de protección y dicho al menos un flujo (208) de bits de protección adicional y dicha al menos una pista (216f, 216g) de indicación y dichas al menos dos pistas (216h, 216i, 216j) de indicación adicionales en un medio de almacenamiento.

13. Sistema de protección frente a errores según la reivindicación 11, que comprende adicionalmente:

- medios para recibir de dicho dispositivo (130) de recepción una petición de corrección de errores para la protección frente a errores; y

- medios para extraer un primer flujo (206) de bits de protección de entre dichos flujos (206, 208) de bits de protección según las pistas (216f, 216g) de indicación asociadas de entre dichas pistas (216f-216j) de indicación;

en el que dicho primer flujo (206) de bits de protección se produce en dicha acción de codificación y dichas pistas (216f, 216g) de indicación asociadas se generan en dicha acción de generación.

14. Sistema de corrección de errores según la reivindicación 13, que comprende adicionalmente:

- medios para recibir posteriormente de dicho dispositivo (130) de recepción una petición de corrección de errores modificada para la protección frente a errores en respuesta a un cambio en el estado de red; y

- medios para extraer al menos un flujo (208) de bits de protección modificado de entre dichos flujos (206, 208) de bits de protección producidos en dicha acción de codificación según las pistas (216h-216j) de indicación asociadas;

en el que dicho flujo (208) de bits de protección modificado se produce en dicha acción de codificación y dichas pistas (216h-216j) de indicación asociadas se generan en dicha acción de generación.

15. Sistema de corrección de errores según la reivindicación 11, en el que dicho flujo (202, 204) de bits es una salida de flujo de datos según un método de codificación de fuente.

16. Sistema de corrección de errores según la reivindicación 11, en el que dichos flujos (206, 208) de bits de protección son flujos de datos producidos según métodos de codificación de protección de datos.

17. Sistema de corrección de errores según la reivindicación 11, en el que dichas pistas (216h-216j) de indicación son flujos de datos generados según algoritmos de indicación.

18. Sistema de corrección de errores según la reivindicación 17, en el que dichos algoritmos de indicación se optimizan según al menos un estado de red, protocolo de red y tipo de red.

19. Sistema de corrección de errores según la reivindicación 11, en el que el dispositivo (130) de recepción es un dispositivo cliente y el dispositivo (114) de envío es un dispositivo servidor.

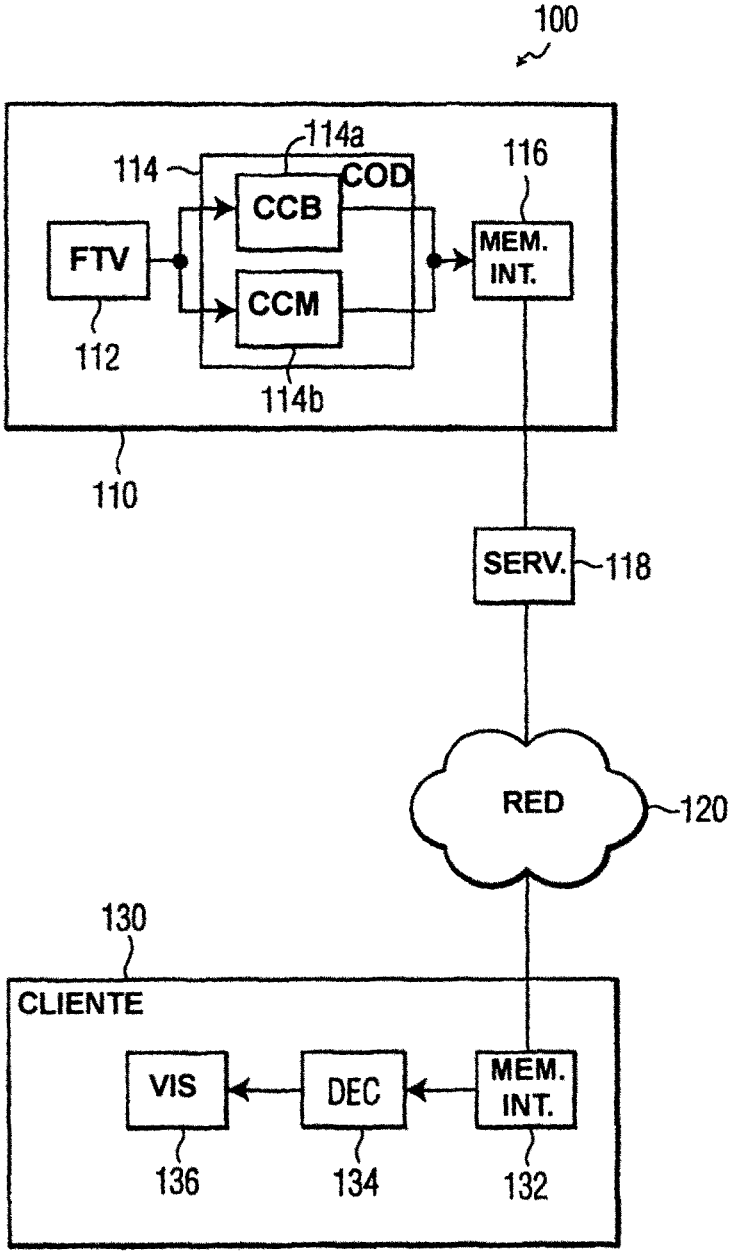
100
114a
114
COD
116
CCB
FTV
MEM.
INT.
CCM
112
114b
110
SERV.
118
RED
120
130
CLIENTE
VIS
DEC
MEM.
INT.
136
134
132

FIG. 1

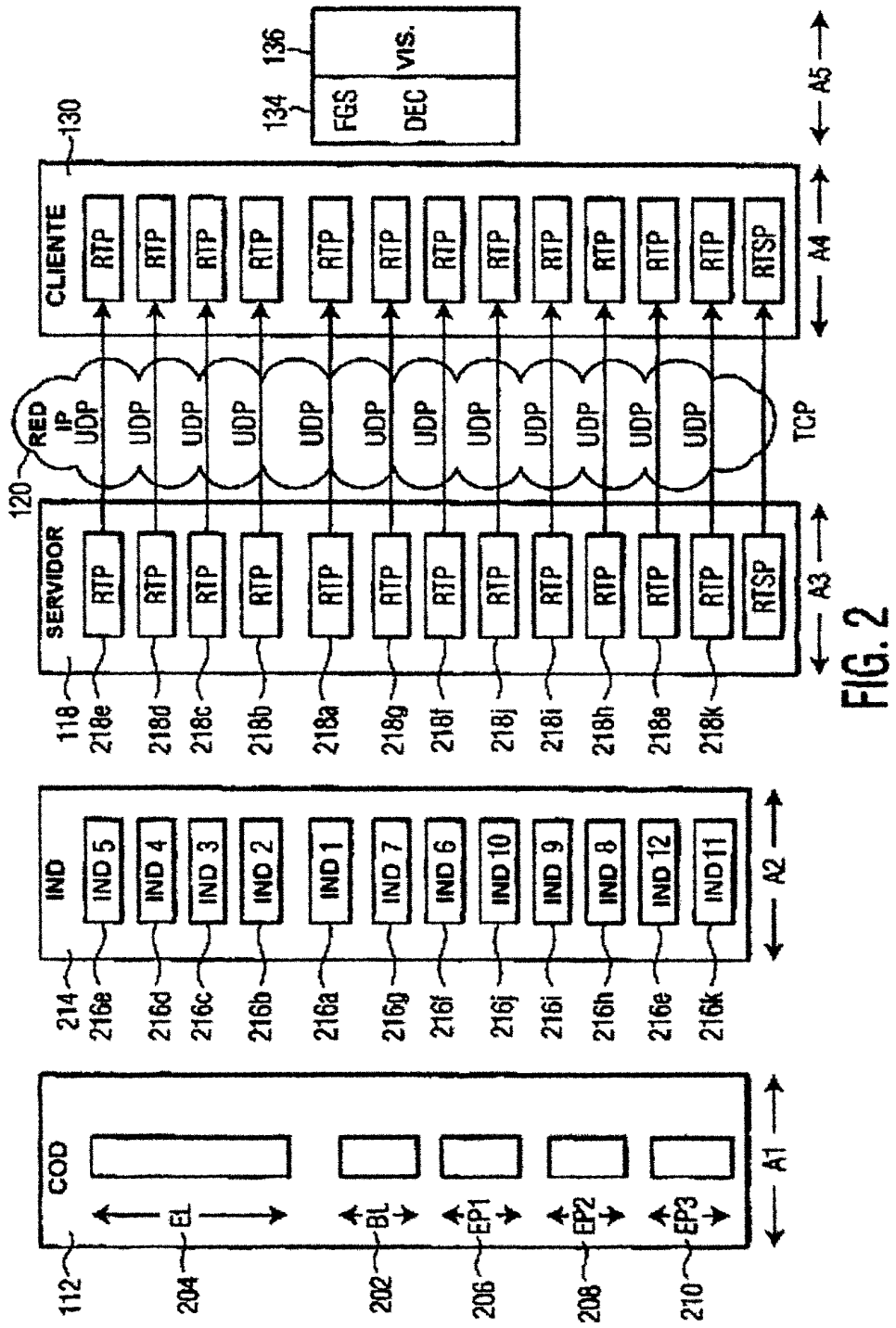
COD
E1
BL
EP1
EP2
EP3
A1
IND
IND 5
IND 4
IND 3
IND 2
IND 1
IND 7
IND 6
IND 10
IND 9
IND 8
IND 12
IND11
A2
SERVIDOR
RTP
RTSP
A3
RED IP
UDP
TCP
CLIENTE
A4
FGS
DEC
VIS.
A5
112
204
202
206
208
210
214
216a
216b
216c
216d
216e
216f
216g
216h
216i
216j
216k
118
218a
218b
218c
218d
218e
218f
218g
218h
218i
218j
218k
120
130
134
136

FIG. 2