(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 742 286**

(51) Int. CI.:

H04L 1/18	(2006.01)	***H04N 7/167***	(2011.01)
H04L 29/06	(2006.01)	***H04W 12/06***	(2009.01)
H04L 9/08	(2006.01)	*H04L 1/00*	(2006.01)
H04N 21/2343	(2011.01)		
H04N 21/2347	(2011.01)		
H04N 21/266	(2011.01)		
H04N 21/2662	(2011.01)		
H04N 21/61	(2011.01)		
H04N 21/6377	(2011.01)		
H04N 21/647	(2011.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.03.2011 PCT/US2011/029908**

(87) Fecha y número de publicación internacional: **29.09.2011 WO11119909**

(96) Fecha de presentación y número de la solicitud europea: **25.03.2011 E 11713559 (0)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 2550806**

(54) Título: **Codificación de red segura para transmisión por secuencias de vídeo, inalámbrica de multirresolución**

(30) Prioridad:

25.03.2010 US 317532 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.02.2020

(73) Titular/es:

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (50.0%)
77 Massachusetts Avenue
Cambridge, MA 02139, US y
UNIVERSIDADE DO PORTO (50.0%)

(72) Inventor/es:

LIMA, LUISA;
GHEORGHIU, STELUTA;
BARROS, JOAO;
MEDARD, MURIEL;
LOPEZ TOLEDO, ALBERTO y
DA SILVA MACHADO GARCIA VILELA, JOAO PAULO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Codificación de red segura para transmisión por secuencias de vídeo, inalámbrica de multirresolución.

Campo de la invención

Los conceptos descritos en la presente memoria se refieren, en general, a esquemas de codificación de red y, más concretamente, a la codificación de red segura para la transmisión por secuencias de vídeo, inalámbrica de multirresolución.

Antecedentes de la invención

Como se conoce en la técnica, ha habido abundante investigación que ha ayudado a asegurar una calidad razonable de experiencia de vídeo para usuarios inalámbricos.

Como también se conoce, la tarea de proveer transmisión por secuencias de vídeo de calidad variable a un conjunto heterogéneo de receptores con diferentes niveles de abono es aún un problema no resuelto. Un desafío es servir a usuarios inalámbricos con trenes de vídeo que: (i) sean de diferente calidad, dependiendo del nivel de abono; y (ii) provean garantías de seguridad para garantizar que solo los usuarios autorizados tendrán acceso a los trenes de vídeo protegidos.

Con el fin de ilustrar el presente problema, uno puede considerar el escenario ilustrado en la Figura 1, en el cual los nodos *A*, *B* y *C* están interesados en un tren de vídeo servido por el nodo *S*, pero aquellos han pagado por calidades de vídeo diferentes, por ejemplo, diferentes capas de un tren de vídeo multirresolución. El nodo *S* puede conectarse a los receptores a través de tres nodos de retransmisión R1, R2, R3 en un rango inalámbrico, pero con calidad de canal pobre. Debido a al menos en parte la naturaleza ruidosa del medio inalámbrico, al menos algunos paquetes transmitidos por el nodo S se pierden. La transmisión de vídeo fiable, sin embargo, requiere que el nodo *S* retransmita los paquetes perdidos mediante el uso de la realimentación recibida de los nodos *A*, *B* y *C*. Además, los retransmisores R1, R2, R3 necesitan sincronizar y planificar transmisiones para asegurar que cada nodo A, B, C reciba todos los paquetes sin duplicados. En el presente escenario, la calidad de vídeo puede reducirse, dado que algunas tramas de vídeo no se entregan de manera oportuna y, por lo tanto, se saltan.

Además, dada la propiedad de radiodifusión del medio inalámbrico, los nodos que no han tenido acceso de abono a ciertas capas pueden, potencialmente, escuchar los paquetes transmitidos. En la Figura 1, por ejemplo, el nodo *B* puede escuchar las tramas de la capa 3. El evitar el acceso no autorizado a ciertas capas en presencia de nodos de retransmisión impone, por consiguiente, un problema de seguridad desafiante, en particular, porque el cifrado del tren de vídeo completo se considera, con frecuencia, no viable en terminales móviles de recursos limitados.

Además, la decodificación en tiempo real de vídeo de alta calidad ya consume una gran cantidad de potencia de procesamiento, y puede convertirse en abrumadora en conjunto con recursos requeridos para el descifrado de grandes archivos. Además, un medio inalámbrico con pérdidas impone requisitos adicionales a los mecanismos de seguridad como, por ejemplo, robustez con respecto a las pérdidas y sincronización limitada para evitar problemas de planificación.

Con el fin de reducir la cantidad de potencia de procesamiento requerida, uno puede reducir la complejidad de la decodificación mediante el cifrado parcial de los datos de vídeo. Sin embargo, es relativamente difícil evaluar el grado de seguridad provisto por esquemas de cifrado parcial. El uso de la codificación en capas en escenarios inalámbricos se ha visto como prometedor, pero probablemente provoque problemas de priorización y planificación. Por ejemplo, cierto trabajo de la técnica anterior ha demostrado que incluso una priorización relativamente simple de una capa base no es una tarea insignificante.

Compendio de la invención

Con el fin de abordar los problemas de más arriba y otros, puede usarse una técnica conocida como codificación de red. El enfoque de la codificación de red permite que los nodos en una red combinen diferentes flujos de información por medio de operaciones algebraicas. El presente principio lleva a una manera no convencional de aumentar el caudal y la robustez de redes altamente volátiles como, por ejemplo, redes inalámbricas, redes de sensor y sistemas entre pares. También se conoce que la codificación de red tiene beneficios para las comunicaciones inalámbricas. Asimismo, se conoce que la codificación de red puede también reducir o, en algunos casos, incluso minimizar, el retardo en la decodificación con realimentación, haciéndola apropiada para la transmisión multimedia. La publicación "*Towards secure multiresolution network coding*" de Lima y otros, 2009 *IEEE Information Theory Workshop on Networking and Information Theory*, propone una cantidad de esquemas diferentes para la transmisión de medios escalable segura mediante el uso de la codificación de red.

En la presente memoria se describen un método y un sistema para el vídeo inalámbrico jerárquico con codificación de red que limita las operaciones de cifrado a un conjunto predeterminado de coeficientes de codificación de red en

combinación con la codificación de vídeo multirresolución. Dichos método y sistema logran niveles de fidelidad jerárquicos, robustez frente a la pérdida de paquetes inalámbricos y seguridad eficaz mediante la explotación de la estructura algebraica de la codificación de red.

La protección de un tren de vídeo inalámbrico, mientras aumenta la robustez general con respecto a pérdidas y fallos, reduce problemas de planificación y añade resiliencia, también es posible mediante el uso de la codificación de red. Al ver el código de red como una cifra, es posible crear un esquema criptográfico liviano que reduce la complejidad computacional general. Por consiguiente, la codificación de red inspira una reformulación de la típica separación entre cifrado y codificación para la resiliencia de errores.

No es necesario llevar a cabo operaciones de seguridad dos veces, dado que uno puede aprovechar la seguridad inherente del presente paradigma. Según se describe en la presente memoria, es posible aprovechar los beneficios de más arriba de la codificación de red para desarrollar y analizar una arquitectura de codificación de red segura e innovadora para el vídeo inalámbrico. En la presente memoria se describe una configuración multidifusión en la cual varios dispositivos, que son, en general, heterogéneos y tienen capacidades de procesamiento limitadas, se abonan al vídeo de flujo continuo multirresolución en una red inalámbrica con pérdidas.

También se describen operaciones de seguridad llevadas a cabo en la capa de codificación de red que permiten: (i) una reducción del número de operaciones de cifrado mientras satisfacen las garantías de seguridad establecidas, (ii) que el esquema de seguridad liviano resultante se combine con códigos en capas eficaces y protocolos de flujo continuo para el vídeo inalámbrico y (iii) combinar la codificación de red con trenes de vídeo escalables, dependiendo de la operación asíncrona de la codificación de red y de la robustez inherente con respecto a fallos de enlace y pérdida de paquetes. Las contribuciones descritas en la presente memoria son las siguientes: (1) un método codificado de red escalable seguro para la transmisión por secuencias de vídeo diseñado para aplicaciones sensibles al retardo que explota la robustez de la codificación de red con complejidad manejable y niveles de seguridad cuantificables; (2) demostración de cómo los códigos jerárquicos para vídeo escalable según refinamiento sucesivo pueden combinarse con la codificación de red en escenarios donde no todos los nodos están autorizados para recibir la mejor calidad; (3) evaluación analítica de las propiedades de seguridad del esquema innovador descrito en la presente memoria, y la descripción de rendimiento e implementación en un servicio de transmisión inalámbrico; (4) una descripción de percepciones y consideraciones del sistema con respecto a la implementación en escenarios reales; y (5) prueba de concepto preliminar para una arquitectura de vídeo codificado de red en varios escenarios inalámbricos mediante simulación.

Se ha descubierto que mediante la explotación de la estructura algebraica de la codificación de red, el triple objetivo de niveles de fidelidad jerárquicos, la robustez contra la pérdida de paquetes inalámbricos y la seguridad eficaz puede lograrse y un método codificado de red escalable seguro y un sistema para la transmisión por secuencias de vídeo diseñado para aplicaciones sensibles al retardo que explota la robustez de la codificación de red con complejidad manejable y niveles de seguridad cuantificables se provee.

Según los conceptos, sistemas y técnicas descritas en la presente memoria, las operaciones de cifrado se encuentran limitadas a un conjunto crucial de coeficientes de codificación de red provistos por un nodo de origen en combinación con la codificación de vídeo de multirresolución. El nodo de origen utiliza una matriz triangular inferior **A** de n x n, en la cual n es el número de capas en un grupo de imágenes (GoP, por sus siglas en inglés). La matriz **A** se usa para la codificación en la fuente solamente y cada entrada diferente de cero de la matriz **A** es un elemento a_{ij} elegido, de manera uniforme, de forma aleatoria de todos los elementos diferentes de cero del campo $F_q \setminus \{0\}$. El GoP se divide en múltiples vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, cada uno de los vectores que tienen K símbolos S_1 - S_K en los cuales el $k^{\text{ésimo}}$ símbolo de cada vector pertenece a una capa correspondiente de las n capas en el GoP y en donde el número de vectores creados se computa como el tamaño de GoP / n. Al menos un símbolo de cada vector $\underline{b}^{(i)}$ se cifra para cada uso de la matriz de codificación en donde la salida de la operación de un cifrado de tren se denota como un símbolo P con una clave aleatoria $\underline{K}$ como $E(P,\underline{K})$. La matriz de codificación **A** se aplica sucesivamente a los símbolos de información que se enviarán para proveer símbolos de información codificada que comprenden una carga útil de uno o más paquetes. Cada uno del único o más paquetes comprenden un encabezamiento y la carga útil y el encabezamiento comprende coeficientes bloqueados y desbloqueados. Cada línea de una primera matriz **A** se encuentra cifrada con una clave de capa correspondiente en donde la primera matriz **A** corresponde a una matriz de coeficientes bloqueados. Una matriz de identidad de $n \times n$ correspondiente a los coeficientes desbloqueados se provee. El único o más paquetes se codifican en nodos de retransmisión según un protocolo de codificación de red lineal aleatoria (RLNC, por sus siglas en inglés) en donde la codificación algebraica se lleva a cabo en coeficientes desbloqueados, coeficientes bloqueados y la carga útil. Los nodos de retransmisión identifican la capa de un paquete mirando la primera posición diferente de cero en los coeficientes desbloqueados, y los paquetes se mezclan con paquetes de la misma capa o capas inferiores solamente.

Según un aspecto adicional de los conceptos, sistemas y técnicas descritas, un método transmitir datos de vídeo en una red que incluye un nodo de servidor, múltiples nodos de retransmisión y uno o más nodos de receptor, comprende llevar a cabo una distribución de clave única entre el nodo de origen y cada uno del único o más nodos de receptor y dividir los datos de vídeo en más de un grupo de imágenes (GoP), cada uno del más de un grupo de

imágenes teniendo una duración predeterminada. Para cada grupo de imágenes (GoP), mediante la generación en el nodo de origen de una matriz triangular inferior **A** de n × n, en la cual n es el número de capas en el GoP y mediante el uso de la matriz **A** para la codificación en la fuente solamente con cada entrada diferente de cero de la matriz **A** siendo un elemento a_{ij} elegido de manera uniforme de forma aleatoria de todos los elementos diferentes de cero del campo $F_q \setminus \{0\}$. El método además incluye dividir el GoP en múltiples vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, cada uno de los vectores teniendo K símbolos S_1 - S_K en los cuales el $k^{ésimo}$ símbolo de cada vector pertenece a una capa correspondiente de las n capas en el GoP y en donde el número de vectores creados se computa como tamaño de GoP / n. El método además comprende cifrar al menos un símbolo de cada vector $\underline{b}^{(i)}$ para cada uso de la matriz de codificación en donde la salida de la operación de un cifrado de tren se denota como un símbolo P con una clave aleatoria $\underline{K}$ como $E(P,\underline{K})$ y aplicar la matriz de codificación **A** sucesivamente a los símbolos de información que se enviarán para proveer símbolos de información codificada que comprenden una carga útil de uno o más paquetes con cada uno del único o más paquetes comprendiendo un encabezamiento y una carga útil. El método además comprende cifrar cada línea de una primera matriz **A** con una clave de capa correspondiente en donde la primera matriz **A** corresponde a una matriz de coeficientes bloqueados y generar una matriz de identidad de $n \times n$ correspondiente a los coeficientes desbloqueados en donde el encabezamiento del paquete comprende los coeficientes bloqueados y desbloqueados. El método además comprende la codificación del único o más paquetes en nodos de retransmisión según un protocolo de codificación de red lineal aleatoria (RLNC) en donde la codificación algebraica se lleva a cabo en coeficientes desbloqueados, coeficientes bloqueados y carga útil y los nodos de retransmisión identifican la capa de un paquete mirando la primera posición diferente de cero en los coeficientes desbloqueados, y los paquetes se mezclan con paquetes de la misma capa o capas inferiores solamente.

En una realización, la división de los datos de vídeo en más de un grupo de imágenes (GoP), comprende dividir los datos de vídeo en más de un GoP con una duración de un (1) segundo.

En una realización, llevar a cabo la codificación algebraica en coeficientes desbloqueados, coeficientes bloqueados y la carga útil comprende llevar a cabo la codificación algebraica de manera indistinguible en coeficientes desbloqueados, coeficientes bloqueados y la carga útil.

En una realización, el método además comprende aplicar, mediante los receptores, la eliminación gaussiana siguiendo la RLNC estándar en los coeficientes desbloqueados y recuperar los coeficientes bloqueados mediante el descifrado de cada línea de la matriz con la clave correspondiente y obtener texto claro por un proceso de sustitución.

En una realización, los símbolos protegidos se encuentran cifrados con la clave para el nivel más bajo en la red de modo que todos los participantes legítimos en el protocolo pueden descifrar los símbolos bloqueados.

En una realización, el método además comprende enviar una primera línea de la matriz no cifrada y comenzar el cifrado de símbolos en el símbolo 2 de modo que la capa 1 es accesible por todos los nodos en la red.

En una realización, solo una clave única por capa se usa para el cifrado multirresolución y en donde la clave única se comparte entre todos los receptores.

En una realización, el cifrado comprende cifrar la capa base del GoP con el fin de lograr la máxima seguridad.

En una realización, la composición de una carga útil de los paquetes incluye formar la carga útil mediante la concatenación de todos los vectores $\mathbf{A}(E(b_1,\underline{K}), b_2, \ldots, b_x)^T$.

En una realización, el cifrado de cada línea de matriz **A** con una clave de capa correspondiente comprende cifrar cada línea de matriz **A** con una clave de capa correspondiente mediante la fuente.

En una realización, un paquete de una $n^{ésima}$ capa corresponde a la $n^{ésima}$ línea de matriz **A** de modo que cada paquete de capa x incluye paquetes de las capas 1, .. . , x - 1, x.

En una realización, el método además comprende enviar una primera línea de la matriz no cifrada y comenzar el cifrado de símbolos en el símbolo 2 de modo que la capa 1 es accesible por todos los nodos en la red.

En una realización, cuando se lleva a cabo una combinación lineal de un paquete de capa x con un paquete de capa $y > x$, el paquete resultante pertenece a la capa *y*.

Según un aspecto incluso adicional de los conceptos, sistemas y técnicas descritas en la presente memoria, un método de generación de paquetes para la transmisión en una red comprende generar una matriz triangular inferior de n x n en la cual cada elemento diferente de cero se elige uniformemente de manera aleatoria de todos los elementos diferentes de cero de un campo finito, dividir texto claro en vectores de elementos en donde una primera posición de cada vector se cifra mediante el uso de un cifrado de tren y multiplicar la matriz por cada uno de los vectores para generar una carga útil.

En una realización, los coeficientes de la matriz se bloquean mediante el uso de una clave diferente para cada línea de la matriz y se colocan en un encabezamiento de los paquetes.

En una realización, el método además incluye generar una línea de una matriz de identidad para cada línea de los coeficientes bloqueados y enviar los paquetes fuera de la red.

En una realización, la generación de una matriz triangular inferior de n x n comprende generar una matriz triangular inferior de 3 x 3.

En una realización, la división de texto claro en vectores de elementos comprende dividir texto claro en vectores de 3 elementos.

Según un aspecto adicional de los conceptos, sistemas y técnicas descritas, un sistema para la transmisión de datos de vídeo en una red comprende un nodo de servidor, múltiples nodos de retransmisión y uno o más nodos de receptor.

Con la presente disposición particular, se provee un sistema codificado de red escalable seguro para la transmisión de datos de vídeo en una red que incluye un nodo de servidor, múltiples nodos de retransmisión y uno o más nodos de receptor.

Breve descripción de los dibujos

Las anteriores características de la presente invención, así como la propia invención, pueden comprenderse de forma más completa a partir de la siguiente descripción de los dibujos en los cuales:

La Figura 1 es un diagrama de bloques de una fuente S que transmite vídeo a tres nodos sumideros A, B y C a través de los nodos de retransmisión R1, R2 y R3 en una configuración inalámbrica.

La Figura 2 es un diagrama de bloques de un sistema de codificación en el cual un nodo de origen genera vídeo multicapa que se provee a un codificador de red y se transmite mediante una transmisión inalámbrica.

La Figura 3 es un modelo de capa en el cual los datos de vídeo se dividen en grupos de imágenes (GoP) con la duración de 1 segundo. Los GoP se subdividen luego en capas.

La Figura 4 es una ilustración diagramática de operaciones llevadas a cabo en un nodo de origen.

La Figura 5 es una ilustración del cifrado de los coeficientes bloqueados.

La Figura 6 es un diagrama de bloques que ilustra módulos de una implementación de sistema a modo de ejemplo (entidades que son externas al sistema, a saber, distribución de clave y generación de un tren multirresolución, se encuentran en forma punteada).

La Figura 7 es un gráfico de tamaño de datos que se cifrarán para el esquema descrito en la presente memoria versus cifrado tradicional (cifrado de todos los datos).

La Figura 8 es un gráfico de velocidad reproducida como una función de probabilidad de pérdida $P_{pérdida}$, para el esquema descrito en la presente memoria (NC1), tres trenes con codificación de red (NC2) y sin codificación de red *(WoNC*, por sus siglas en inglés).

La Figura 9 es un gráfico de la carga en el servidor como una función de la probabilidad de pérdida $P_{pérdida}$.

La Figura 10 es un gráfico de CDF versus tiempo de decodificación para la probabilidad de pérdida $P_{pérdida} = 0,4$, para la capa 3. 0 0,2 0,4 0,6 0,8 1

La Figura 11 es un gráfico de porcentaje de segmentos saltados versus probabilidad de pérdida, $P_{pérdida}$, para la capa 3.

La Figura 12 es un gráfico de porcentaje de segmentos reproducidos en calidad inferior como una función de la probabilidad de pérdida $P_{pérdida}$.

La Figura 13 es un gráfico de retardo de almacenamiento temporal inicial como una función de probabilidad de pérdida, $P_{pérdida}$, para la capa 3.

La Figura 14 es un gráfico de calidad reproducida como una función de ID de segmento para $P_{pérdida} = 0,4$.

Descripción detallada de las realizaciones preferidas

Con referencia, ahora, a la Figura 1, un nodo de origen o de servidor S transmite vídeo a tres nodos sumideros o de receptor A, B y C (o, más simplemente, "sumideros" o "receptores") a través de los nodos de retransmisión R1, R2 y R3 en una configuración inalámbrica. La probabilidad de eliminación de un paquete en cada enlace (en línea punteada) se denota como $P_{pérdida}$. Los sumideros, A, B, C han abonado para diferentes calidades de vídeo, por consiguiente, uno debe concebir mecanismos para asegurar la entrega fiable en el medio inalámbrico, y la protección contra el acceso no autorizado. El funcionamiento del nodo de origen S se describe en detalle más abajo (y, en particular, en conjunto con la Figura 4 de más abajo).

Con referencia, ahora, a la Figura 2, un nodo de origen S genera vídeo multicapa y provee el vídeo multicapa a un codificador de red. El codificador de red codifica el vídeo (a saber, el vídeo se alimenta al codificador de red) y se transmite posteriormente a través de una red inalámbrica que tiene nodos de retransmisión R1, R2, R3 (p.ej., como se muestra en la Figura 1) a uno o más nodos de destino o receptores (p.ej., nodos A, B, C como es muestra en la Figura 1). El vídeo se alimenta a un codificador de red y luego se somete a la transmisión en una red inalámbrica.

Un concepto descrito en la presente memoria se dirige hacia cómo generar un tren seguro, escalable mediante la concordancia del vídeo multicapa generado por el nodo de origen S con el codificador de red.

Teniendo en cuenta un modelo de red y abstracciones, uno puede considerar una abstracción de una red inalámbrica donde los nodos de origen S y de retransmisión R1, R2, R3 solo tienen acceso a los identificadores de los sumideros (p.ej., las direcciones IP). Por consiguiente, no hay conocimiento centralizado de la topología de red o de las funciones de codificación.

Con referencia brevemente a la Figura 3, se muestra un modelo de capa. Uno puede adoptar un modelo de capas de vídeo según se describe en el documento de Z. Liu, Y. Shen, S. S. Panwar, K. W. Ross, y Y. Wang, "*Using layered video to provide incentives in p2p live streaming*" en *P2P-TV '07: Proceedings of the 2007 workshop on Peer-to-peer streaming and IP-TV*, Nueva York, NY, USA, 2007, pp. 311-316, ACM. Debe, sin embargo, apreciarse que otros modelos de capa pueden también usarse según los conceptos, sistemas y técnicas descritas en la presente memoria.

Según se ilustra en la Figura 3, los datos de vídeo se dividen en "grupos de imágenes" o GoP (a los cuales también se hace referencia, de manera intercambiable, en la presente memoria como "segmentos de vídeo") con una duración constante. En la realización a modo de ejemplo descrita, en la presente memoria los GoP tienen una duración de un (1) segundo. Otras duraciones también pueden, por supuesto, usarse. Los datos se codifican entonces en *L* capas (con cuatro (4) capas que se muestran en la Figura 3); cada capa se divide en un número fijo de paquetes. Debe notarse que cada capa depende de todas las capas previas. Es decir, la capa 1 es necesaria para decodificar la capa 2, la capa 2 es necesaria para decodificar la capa 3, etc.

Consideremos una amenaza planteada por un atacante pasivo con las siguientes características: (1) el atacante puede observar cada transmisión en la red; (2) el atacante tiene acceso total a la información sobre los esquemas de codificación y decodificación; (3) el atacante se encuentra computacionalmente limitado y, por consiguiente, no puede romper primitivas criptográficas duras.

El objetivo del atacante es recuperar el tren de vídeo de multidifusión con la calidad más alta posible.

La codificación de red y la seguridad pueden lograrse mediante la codificación de red lineal aleatoria (RLNC). RLNC es un esquema completamente distribuido para implementar protocolos de codificación de red, por medio de lo cual los nodos extraen varios coeficientes de manera aleatoria y los usan para formar combinaciones lineales de paquetes entrantes. El paquete resultante se envía junto con el vector de codificación global, que registra el efecto acumulativo de las transformaciones lineales soportadas por el paquete original mientras se encuentra en su propio trayecto del origen al destino. El vector de codificación global permite que los receptores decodifiquen por medio de la eliminación gaussiana.

A continuación, se describen conceptos, técnicas y sistemas relacionados con la codificación de red segura para la transmisión por secuencias de vídeo.

Con referencia, ahora, a la Figura 4, las funciones en un nodo de origen (p.ej., el nodo de origen S en las Figuras 1 y 2) se ilustran en la Figura 4. En un resumen general con referencia a la realización a modo de ejemplo ilustrada en la Figura 4, un nodo de origen genera una matriz triangular inferior de 3 x 3 en la cual cada elemento diferente de cero se elige uniformemente de manera aleatoria de todos los elementos diferentes de cero de un campo finito. El texto claro se divide en vectores de 3 elementos y la primera posición de cada vector se cifra mediante el uso de un cifrado de tren. La matriz se multiplica por cada uno de los vectores para generar la carga útil. Los coeficientes de la matriz **A** se bloquean mediante el uso de una clave diferente para cada línea de la matriz y se colocan en el encabezamiento de los paquetes. Una línea de la matriz de identidad se genera para cada línea de los coeficientes bloqueados. Los paquetes se envían entonces fuera de la red.

Continuando ahora en mayor detalle, el esquema comienza con una distribución de clave única entre el nodo de origen y los nodos de receptor (también conocidos como nodos sumideros). Dado que las claves pueden reutilizarse, solo una clave por capa se necesita para el cifrado multirresolución (una sola clave para el caso de vídeo de resolución único), que se compartirá entre todos los nodos de receptor. Entonces, para cada GoP, el nodo de origen genera una matriz triangular inferior **A** de n x n, en la cual n es el número de capas en el GoP. La matriz **A** se usa para la codificación en el nodo de origen solamente. Cada entrada diferente de cero de **A** es un elemento a_{ij} elegido uniformemente de manera aleatoria de todos los elementos diferentes de cero del campo $F_q\{0\}$.

El GoP se divide entonces en vectores $\underline{b}^{(1)}$... $\underline{b}^{(w)}$, en los cuales el primer símbolo de cada vector pertenece a la capa 1, el siguiente símbolo pertenece a la capa 2, etc. El número de vectores creados es [tamaño de GoP / n] (debe apreciarse que, en aras de la claridad, las inconsistencias con respecto a la proporción entre el número de símbolos en las capas se ignoran). Entonces, al menos un símbolo de cada vector $\underline{b}^{(i)}$ se cifra para cada uso de la matriz de codificación. Dado que las capas son dependientes - la capa *i* se necesita para decodificar la capa i + 1 - un enfoque preferido es cifrar la capa base más informativa del GoP con el fin de lograr la máxima seguridad (en el presente caso, b_1 para cada vector $\underline{b}^{(i)}$). La salida de la operación de un cifrado de tren se denota como un símbolo P con una clave aleatoria $\underline{K}$ como $E(P,\underline{K})$. Finalmente, la carga útil de los paquetes se compone mediante la aplicación de la matriz de codificación **A** sucesivamente a los símbolos de información que se enviarán, a saber, la carga útil se forma mediante la concatenación de todos los vectores $\mathbf{A}(E(b_1,\underline{K}), b_2, ..., b_x)^T$.

A continuación, la fuente cifra cada línea de la matriz **A** con la clave de capa correspondiente. La matriz **A** es la matriz de coeficientes bloqueados. La fuente entonces genera una matriz de identidad **I** de $n \times n$, que corresponde a los coeficientes desbloqueados. Los paquetes están compuestos del encabezamiento y de la carga útil. El encabezamiento incluye los bloqueados y desbloqueados. Es preciso notar, debido a la estructura anidada de la codificación, determinada por la matriz triangular, un paquete de la capa 1 corresponde a la primera línea de la matriz **A**, un paquete de la capa 2 corresponde a la segunda línea de la matriz **A**, etc., de modo que cada paquete de capa x incluye paquetes de las capas 1, ... , $x - 1, x$ (a saber, un paquete de una $n^{ésima}$ capa corresponde a la $n^{ésima}$ línea de la matriz **A** de modo que cada paquete de capa x incluye paquetes de las capas 1, ... , x - 1, x). Es preciso notar también que cuando se lleva a cabo una combinación lineal de un paquete de capa x con un paquete de capa $y > x$, el paquete resultante pertenece a la capa *y*.

Las retransmisiones codifican paquetes según las reglas de protocolos RLNC estándares. La codificación algebraica se lleva a cabo de manera indistinguible en coeficientes desbloqueados, coeficientes bloqueados y carga útil. Las retransmisiones identifican la capa de un paquete mirando la primera posición diferente de cero en los coeficientes desbloqueados, y los paquetes se mezclan con paquetes de la misma capa o capas inferiores solamente.

Los nodos de receptor aplican la eliminación gaussiana siguiendo la RLNC estándar en los coeficientes desbloqueados. Los coeficientes bloqueados se recuperan mediante el descifrado de cada línea de la matriz con la clave correspondiente. El texto claro se obtiene entonces por la sustitución de reenvío. Es preciso notar que los símbolos protegidos deben cifrarse con la clave para el nivel más bajo en la red (es decir, $\underline{K}_1$), de modo que todos los participantes legítimos en el protocolo pueden descifrar los símbolos bloqueados. Si la capa 1 será accesible por todos los nodos en la red, la primera línea de la matriz debe enviarse no cifrada y el cifrado de símbolos debe comenzar en el símbolo 2.

La Tabla I resume el funcionamiento del esquema. Lo que sigue es una elaboración con respecto a la concordancia de vídeo de multirresolución y seguridad, cuestiones de priorización y planificación, así como un análisis de seguridad.

TABLA I

Inicialización (nodos de origen):

- Un mecanismo de gestión de claves se usa para intercambiar n claves compartidas con los nodos sumideros (uno para cada capa);
- El nodo de origen genera una matriz triangular inferior **A** de n x n en la cual cada una de las entradas diferentes de cero es un elemento del grupo multiplicativo del campo finito, $\alpha \varepsilon F_q \setminus \{0\}$;
- Los coeficientes correspondientes a una línea distinta de la matriz de identidad n x n se añaden al encabezamiento de cada paquete codificado. Estos corresponden a los coeficientes desbloqueados.
- Cada línea / de la matriz **A** se cifra con clave compartida $\underline{K}_1$ y se coloca en el encabezamiento de cada paquete. Dichos coeficientes corresponden a los coeficientes bloqueados;

Inicialización (nodos de origen):

- El nodo de origen aplica la matriz **A** los paquetes que se enviarán, y los coloca en su memoria.

Inicialización (nodos de retransmisión):

- Cada nodo inicializa n memorias intermedias, una para cada capa en la red.

Funcionamiento en nodos de retransmisión:

- Cuando un paquete de capa l se recibe por un nodo, el nodo almacena el paquete en la memoria intermedia correspondiente;

- Con el fin de transmitir un paquete de capa l en un enlace saliente, el nodo produce un paquete mediante la formación de una combinación lineal aleatoria de los paquetes en las memorias intermedias 1, ... , *l*, modificando tanto los coeficientes desbloqueados como bloqueados sin distinción, según las reglas de los protocolos basados en RLNC estándar.

Decodificación (nodos sumideros):

Cuando suficientes paquetes se reciben:

- Los nodos sumideros llevan a cabo la eliminación gaussiana en la matriz de coeficientes desbloqueados, mediante la aplicación de las mismas operaciones al resto del paquete y, de esta manera, se obtienen los coeficientes bloqueados originales y los paquetes codificados;

- El receptor entonces descifra los coeficientes bloqueados mediante el uso de las claves Ki correspondientes para el nivel i;

- El receptor lleva a cabo la sustitución de reenvío en los paquetes mediante el uso de los coeficientes bloqueados para recuperar los paquetes originales;

- El receptor descifra los símbolos cifrados para formar el texto claro original.

El llevar seguridad al vídeo de multirresolución puede lograrse mediante una matriz de codificación triangular. Como puede verse, tras generar un nuevo GoP, la fuente lo divide en vectores $\underline{b}^{(1)}$ ... $\underline{b}^{(w)}$, mezclando todas las capas, y aplica la matriz **A** cada uno de ellos para obtener la carga útil, es decir: $c^{(i)} = \mathbf{A}\underline{b}^{(i)}$.

Con referencia, ahora, a la Figura 5, múltiples capas claves diferentes se usan para cifrar múltiples líneas diferentes correspondientes de una matriz A. Como se ilustra en la Figura 5, el cifrado de los coeficientes bloqueados incluye una primera capa que corresponde a la primera línea de la matriz y se cifra con la clave para la capa 1. Los restantes coeficientes bloqueados se cifran línea por línea según un mecanismo similar. El presente concepto logra la seguridad dado que solo los receptores con las claves correspondientes pueden decodificar la línea cifrada y, en consecuencia, la capa.

Debe apreciarse que las operaciones de codificación de red estándares pueden emplearse en los coeficientes desbloqueados también cuando las capas se cifran con diferentes claves. Además, incluso si los paquetes de diferentes capas se combinan, la inversión de las operaciones a través del uso de coeficientes desbloqueados posteriormente invierte todas las combinaciones de diferentes capas, de modo que la información original puede recuperarse (en aras de la simplicidad de la descripción, y sin pérdida de generalidad, uno considera que la matriz A tiene una fila por capa 3).

Debe notarse que la RLNC tradicional mezcla todos los paquetes mediante el uso de una matriz cuadrada completa. Ello, sin embargo, no es apropiado para la codificación en capas, dado que no es posible extraer capas individuales a menos que una matriz se usa para cada capa. La codificación de matriz triangular descrita en la presente memoria mezcla, de manera eficaz, las capas y, así, permite la recuperación diferenciada de capas sucesivas por nodos con diferentes niveles de acceso, mientras depende de la diseminación de paquetes de nivel inferior para lograr la resiliencia necesaria para paquetes de nivel superior que se entregarán de manera oportuna. Además, la forma de matriz triangular provee prioridad a la capa base, dado que todos los paquetes de capa superior contienen la capa base. Por consiguiente, la priorización y planificación comunes de la capa base se resuelven de manera natural. Más

abajo se provee una comparación del concepto y esquema descritos en la presente memoria con RLNC tradicional que tratan cuestiones de planificación y priorización.

La elección de una matriz triangular además satisface dos requisitos importantes. Primero, permite retirar el retardo arbitrario introducido por una matriz completa RLNC típica en la fuente, dado que la fuente puede codificar paquetes tan pronto como se generan y no tiene que esperar al final de la generación para enviarlos. Además, el uso de una matriz triangular permite también un mapeo único entre los coeficientes desbloqueados y bloqueados que no compromete la seguridad: un coeficiente desbloqueado diferente de cero en la columna i corresponde a la combinación de paquetes p_1, ..., p_i dentro del paquete correspondiente. Esta es una manera de determinar la capa de un paquete en nodos de retransmisión y permitir el uso de las estrategias de realimentación para minimizar el retardo de decodificación mencionado más arriba.

A continuación se describe un modelo usado para llevar a cabo un análisis de seguridad. Dejemos que $\mathbf{A} = (a_{ij})$ sea la matriz de codificación triangular inferior de $n \times n$ usada para llevar a cabo la codificación en la fuente. Cada uno de los coeficientes diferentes de cero a_{ij}, $i \geq j$ se distribuye uniformemente en todos los elementos diferentes de cero de un campo finito F_q, $q = 2^u$, y mutuamente independientes.

Dejemos que los datos originales, o texto claro, sean una secuencia de w vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, en la cual $\underline{b}^{(x)} = (b_1^{(x)}, b_2^{(x)}, \ldots, b_n^{(x)})^T$, $1 \leq x \leq w$. Todos los vectores $\underline{b}^{(x)}$ son independientes de $\mathbf{A}$. Se supone que el algoritmo de refinamiento sucesivo usado para generar el vídeo escalable es óptimo. Por consiguiente, $P(B_i = b_i) = (q-1)^{-1}$, $\forall b_i \in F_q \backslash \{0\}$. En aras de la simplicidad en las pruebas, se supone que el texto claro se encuentra precodificado para retirar ceros. Ello puede lograrse mediante el mapeo de elementos F_q hacia F_{q-1}, y, de esta manera, incurrir en una penalidad de tasa insignificante de $(q-1)/q$.

Las pruebas se generalizan para incluir más de un símbolo cifrado por uso de la matriz de codificación. Asimismo, m representa el número de símbolos cifrados por reutilización de los símbolos de codificación. Nos abstraemos del cifrado particular usado para bloquear los coeficientes. Para el texto claro, el uso de un cifrado de tren se supone de modo que la probabilidad de la salida de la operación de codificación E(P, $\underline{K}$) es independiente del texto claro P y la distribución de la salida es uniforme entre todos los elementos diferentes de cero de $F_q \backslash \{0\}$, es decir, $P(E(P, \underline{K})) = (q-1)^{-1}$. Los parámetros del cifrado deben ajustarse para aproximarse a dichos criterios. En las pruebas, para obtener dichas propiedades, uno considera el uso de una libreta de un solo uso en la cual un símbolo de la clave se usa para cada símbolo del texto claro que se cifra. La clave se representa por w vectores aleatorios $K^{(1)} \ldots K^{(w)}$, cada uno con m posiciones (es decir, con wm símbolos de clave en total). Además, $P(K_i = k_i) = (q-1)^{-1}$, $\forall k_i \in F_q \setminus \{0\}$.

El vector al cual la matriz se aplica, es decir, el vector $(E(b_1, K_1^{(1)}, \ldots, E(b_m^{(x)}, K_m^{(x)}), b_{m+1}^{(x)}, \ldots, b_n^{(x)})^T$, se denota $\underline{e}^{(x)}$. Cada vector de carga útil se representa por $\underline{c}^{(x)} = (c_1^{(x)})^T$, donde x corresponde a la reutilización x de $\boldsymbol{A}$ y

$$C_i^{(x)} = \left(\sum_{j=1}^{\min(i,n)} a_{ij} E(b_j^{(x)}, K_j^{(x)}\right) + \left(\sum_{l=m+1}^{i} a_{il} b_l^{(x)}\right).$$

En la descripción en la presente memoria, variables aleatorias se describen en letras mayúsculas e instancias de variables aleatorias se representan en letras minúsculas. Los vectores se representan por letras subrayadas y las matrices se representan en negrita. Sin pérdida de generalidad, uno puede abstraerse de la estructura de red y considerar la carga útil de todos los paquetes juntos en las pruebas de seguridad. Caracterizada más abajo se encuentra la información mutua (denotada por $I(\bullet; \bullet)$) entre los datos codificados y los dos elementos que pueden llevar a la descripción de información: la matriz de codificación y los propios datos originales. El teorema 1 evalúa la información muta entre la carga útil y la matriz de codificación, y el teorema 2 evalúa la información muta entre la carga útil y los datos originales.

Teorema 1: La información mutua entre $\boldsymbol{A}$ y $\boldsymbol{A}E(1)$, $\boldsymbol{A}E(2)$, ... , $\boldsymbol{A}E(w)$ es cero:

$$I(\boldsymbol{A}; \boldsymbol{A}\underline{E}^{(1)}, \boldsymbol{A}\underline{E}^{(2)}, \ldots, \boldsymbol{A}\underline{E}^{(w)}) = 0.$$

El teorema 1 es una generalización del resultado en la Ecuación 24 y muestra que el coste de un ataque estadístico en la matriz de codificación es el coste de un ataque de fuerza bruta en todas las entradas de la matriz, independientemente del número de reutilizaciones.

Teorema 2: La información muta entre $\underline{B}^{(1)}, \ldots, \underline{B}^{(w)}$ y $\boldsymbol{A}\underline{E}^{(1)}, \ldots, \boldsymbol{A}\underline{E}^{(w)}$ se provee por la expresión:

$$I(\underline{B}^{(1)}, \ldots, \underline{B}^{(w)} \text{ and } \boldsymbol{A}\underline{E}^{(1)}, \ldots, \boldsymbol{A}\underline{E}^{(w)}) = \log(q-1) \max(f(w, n, m), 0),$$

donde $f(w, n, m) = w(n - m) - \binom{n(n+1)}{2}$.

La ecuación en el teorema 2 muestra que el coste del ataque del texto claro es el coste del descubrimiento de la matriz de codificación. Por consiguiente, uno obtiene un umbral en el cual hay una reducción del espacio de búsqueda que se necesita para atacar el texto claro debido a múltiples reutilizaciones de la matriz **A**. Es preciso notar que no hay divulgación alguna del texto claro con un solo uso de la matriz de codificación. Debajo del número de usos en el umbral, la información mutua es 0 y, por consiguiente, no es posible llevar a cabo un ataque estadístico en la carga útil. Cuando el número de usos de la matriz de codificación supera el umbral, la información mutua crece con *w*. En el caso extremo en el cual el número de símbolos cifrados es igual al número de símbolos en la matriz, la información mutua es siempre cero (sin embargo, en el presente caso, uno no requerirá que la matriz de codificación esté oculta).

La matriz triangular otorga protección desigual a las capas del texto claro. Uno puede fácilmente ver que el espacio de búsqueda para descubrir la capa *i + 1* es más grande que el espacio de búsqueda para descubrir la capa *i.* Tomemos, por ejemplo, el caso en el cual *m = 0* - entonces, para las capas *i* e *i + 1,* un atacante necesita adivinar, respectivamente, *i e i* + 1 entradas de la matriz.

Se cree que la expresión en el teorema 2 permite el ajuste fino del compromiso entre complejidad y seguridad mediante la variación de *n* (el tamaño de la matriz), *m* (el número de símbolos cifrados) y el tamaño del campo.

Con referencia, ahora, a la Figura 6, un sistema a modo de ejemplo incluye un nodo de origen S, un nodo de retransmisión R y un receptor que comprende un decodificador D. También se muestran en la Figura 6 un tren de multirresolución y un sistema de distribución de clave K que se ilustran en modo fantasma dado que son externos al sistema. Consideremos un escenario como, por ejemplo, el de la Figura 1, con una arquitectura de sistema según se ilustra en la Figura 6, los diferentes componentes del sistema y sus implicaciones prácticas se describen a continuación.

La técnica descrita en la presente memoria requiere claves compartidas entre nodos de origen y nodos de destino. Mientras los detalles específicos de un mecanismo de distribución de clave particular no son relevantes con respecto a los conceptos descritos en la presente memoria, técnicas de distribución de clave a modo de ejemplo incluyen, pero sin limitación a, la predistribución fuera de línea de claves o protocolos de autenticación como, por ejemplo, Kerberos o una Infraestructura de Clave Pública (PKI, por sus siglas en inglés). Debe notarse que la necesidad de que las claves se compartan entre varios nodos legítimos en una red surge con frecuencia en escenarios de multidifusión y se denomina comúnmente como cifrado de radiodifusión o distribución de clave de multidifusión. Los nodos de la capa *l* deben mantener *l* claves (una para cada capa) y, por consiguiente, el número de claves intercambiadas es igual a $\sum_{l=1}^{L} l t_l$, en la cual t_l representa el número de receptores de la capa *l* en la red y *L* el número total de capas en el tren.

Con respecto a la codificación de codificador de multirresolución y a la seguridad, los principales requisitos de los protocolos de seguridad para trenes multimedia son: (i) funcionar con baja complejidad y alta eficacia de cifrado, (ii) mantener el formato de archivo e información de sincronización y (iii) mantener el tamaño de datos originales y la relación de compresión. Como puede verse a partir de la descripción provista en la presente memoria, el esquema descrito en la presente memoria se ha diseñado para satisfacer el criterio (i). El criterio (ii) depende del códec pero, en general, el esquema descrito en la presente memoria puede satisfacerlo. Tomando, por ejemplo, el códec4 de vídeo MJPEG, uno puede usar la opción JPEG2000 de colocar todos los encabezamientos de todos los bloques de la imagen en el encabezamiento principal del archivo y satisfacer el criterio (ii). Finalmente, la codificación de red no cambia el tamaño o la relación de compresión del tren, de modo que el esquema descrito en la presente memoria satisface el criterio (iii).

Como también se muestra en la presente memoria, el nivel máximo de seguridad se obtiene cuando la compresión es óptima y produce un resultado que es casi uniforme. Por consiguiente, el esquema descrito en la presente memoria impone un conjunto de parámetros para el códec con el fin de maximizar la entropía del archivo. En el códec MJPEG, dos de dichas decisiones de codificación serán elegir tamaños de losa más grandes y la tasa de compresión máxima en la etapa de codificación aritmética. Otro enfoque será llevar a cabo una etapa de protección de datos adicional junto con la compresión. El tamaño de la capa base puede verse como otro parámetro para aumentar la relación de compresión. A modo de ejemplo, en JPEG2000, cada símbolo codificado aumenta la resolución del tren, por lo tanto, es posible variar el tamaño de cada capa tomando las limitaciones del mecanismo de seguridad en consideración.

El nodo de codificador de origen S incluye módulos de seguridad, recuperación de pérdidas y codificación de red. El módulo de seguridad y su interoperación con la codificación de red se describen en la presente memoria, p.ej., en conjunto con la Figura 4 de más arriba.

Sin embargo, debe apreciarse que se usa más de una fila de la matriz para cada capa. En dicho caso, el mapeo entre los coeficientes desbloqueados y bloqueados sufre un desplazamiento: si se usan 2 paquetes por capa, un paquete con vector de coeficientes desbloqueados (1, 1, 0, ... 0) pertenece a la capa 1 y un paquete con vector (1, 1, 1, 0, ... 0) pertenece a la capa 2. La división de la carga útil en vectores debe también contener dicho

desplazamiento. Los códecs en los cuales cada nuevo símbolo (decodificados en orden) contribuye a la resolución aumentada del vídeo de salida (como, por ejemplo, MJPEG2000) pueden beneficiarse de un enfoque con una granularidad más fina. Dicha granularidad puede ajustarse de manera fina por el número de líneas de la matriz de codificación que pertenecen a cada capa. Otro requisito de sistema importante es usar un mecanismo de cifrado para el cual el texto de cifrado es del mismo tamaño que el texto claro (p.ej., AES en el modo de cifrado de tren) con el fin de mantener el tamaño de los símbolos constante.

Un aspecto importante del codificador es la velocidad a la cual los nodos intermedios generan y envían combinaciones lineales al receptor. Si un retransmisor genera y reenvía una combinación lineal cada vez que un paquete innovador del servidor se recibe, entonces muchos paquetes redundantes pueden llegar a los destinos. Con el fin de resolver la presente cuestión, el servidor genera un crédito para cada paquete codificado, que se asigna además a uno de los retransmisores intermedios. A continuación, solo el retransmisor que recibe también el crédito asociado al paquete puede enviar una combinación lineal.

Después de transmitir una generación completa, y antes de transmitir la siguiente, el servidor comienza el proceso de recuperación de pérdidas. Con el fin de recuperar paquetes perdidos, el servidor envía combinaciones lineales redundantes para cada capa, mezclando todos los paquetes de la capa. El presente proceso continúa hasta que todos los receptores para dicha capa puedan decodificar o el servidor tenga otro segmento para transmitir.

El codificador de red es un componente de los retransmisores inalámbricos de la red e incluye la clasificación de capas y la codificación de red. Según se describe más arriba, los paquetes de la capa I solo deben combinarse con los paquetes de capas inferiores, a saber, *l*, *l*-1, ... 1. Ello se lleva a cabo con el fin de mantener la diversidad de capas en la red, dado que cuando se combina un paquete de la capa *l* con la capa *l+1,* la capa del paquete resultante es *l + 1.* Después de clasificar el paquete, un retransmisor genera y reenvía una combinación lineal si ha recibido el crédito asignado a dicho paquete.

El decodificador es un componente del receptor que incluye seguridad, decodificación y almacenamiento temporal y realimentación. Cuando se reciben suficientes paquetes, el receptor lleva a cabo la eliminación gaussiana para decodificar paquetes mediante el uso de los coeficientes desbloqueados. El proceso de seguridad corresponde a la recuperación de los coeficientes bloqueados y símbolos cifrados de la carga útil y se explica más arriba.

Dado que en el esquema descrito en la presente memoria los nodos de retransmisión llevan a cabo la codificación en los paquetes de las mismas capas (inferiores), la forma de la matriz triangular enviada por la fuente no se mantiene a través de la red. Por consiguiente, un paquete recibido, incluso si es innovador en términos de rango, puede no ser decodificable inmediatamente. Por lo tanto, el sistema descrito en la presente memoria requiere una memoria intermedia de decodificación en los receptores. La memoria intermedia de decodificación toma en cuenta el retardo máximo admisible del tren de vídeo, similar a la memoria intermedia de reproducción en los receptores, y liberará, de manera preferente, los paquetes no decodificados actuales si el requisito de retardo no se satisface. Una vez que la capa total se haya decodificado, se almacena en la memoria intermedia de reproducción.

Un nodo comienza la reproducción una vez que decodifica un número de segmentos en la calidad más baja. Si una trama no se recibe hasta el tiempo de reproducción, entonces se descarta y la trama posterior se reproduce en su lugar. Asimismo, si la trama se encuentra disponible en una calidad inferior, esta se reproduce en una calidad inferior a aquella con respecto a la cual el nodo tiene acceso. En la etapa de tiempo *k* el nodo reproduce el segmento k en la calidad en la cual se encuentra disponible. Si el segmento no se ha decodificado (ni siquiera en la calidad más baja), entonces el nodo detiene el proceso de reproducción y comienza el almacenamiento temporal. Si después de cierta temporización de almacenamiento temporal, el nodo decodifica el segmento *k,* entonces lo reproduce en la calidad en la cual está disponible; de lo contrario, el nodo salta el segmento *k* y reproduce el siguiente.

Teniendo en cuenta un sistema con realimentación mínima, con el fin de liberar los canales inalámbricos de transmisiones innecesarias, los receptores envían realimentación positiva al servidor cuando decodifican un segmento en la calidad deseada. Por ejemplo, un receptor de capa 3 envía un paquete de realimentación único cuando ha decodificado las capas 1, 2 y 3.

A continuación se describe una evaluación del sistema descrito en la presente memoria en términos de complejidad de seguridad así como una evaluación del rendimiento del sistema en un escenario inalámbrico con pérdidas.

Con referencia, ahora, a la Figura 7, un volumen de datos que se cifrarán según el tamaño del texto claro para el esquema descrito en la presente memoria se compara con el cifrado tradicional, para tamaños de paquete típicos de 500 bytes (para paquetes de vídeo en redes celulares), 1.000 bytes (por ejemplo, para vídeo en redes wifi) y 1.500 bytes (el tamaño de paquete IP típico). En el presente ejemplo, se supone un símbolo cifrado por generación. Para mecanismos de cifrado tradicionales, que llevan a cabo el cifrado de extremo a extremo de toda la carga útil, el volumen de datos que debe cifrarse aumenta linealmente con el tamaño de la carga útil protegida. No es difícil ver que el esquema descrito en la presente memoria reduce sustancialmente el tamaño de la información que se cifrará. Las ganancias se convierten en más altas mientras el tamaño máximo del paquete aumenta, dado que el número de

matrices que se generarán es más pequeño, y más datos pueden enviarse en cada paquete que contiene la misma matriz de coeficientes.

Naturalmente, el número requerido de operaciones criptográficas está directamente relacionado con el volumen de datos que se cifrarán. Si uno considera un cifrado de tren, el número de operaciones de cifrado aumenta linealmente con dicho volumen y, por lo tanto, la complejidad computacional se reduce ampliamente por el esquema innovador descrito en la presente memoria como se muestra en la Figura 7. Es preciso notar que dichos valores son solamente indicativos, y corresponden a las ganancias teóricas cuando el tamaño del paquete es el único parámetro que determina el número de reutilizaciones de la matriz de codificación. La penalidad de seguridad, que se cuantifica más arriba, no se considera a los fines del presente análisis. Es preciso notar que los valores de extremo dependen del diseño del códec, así como del tamaño elegido para cada capa.

Comunicación y sobrecarga computacional se describen a continuación.

La capacidad de reducir el volumen de datos que se cifrarán es a expensas de incluir coeficientes bloqueados en el paquete de datos.

La Tabla II muestra la sobrecarga introducida por el esquema innovador descrito en la presente memoria para cada paquete y para coeficientes con tamaño de 8 y 16 bits, para algunos valores de referencia para redes inalámbricas con nodos con varias capacidades de procesamiento.

TABLA II

SOBRECARGA DE VOLUMEN DE COEFICIENTES BLOQUEADOS (POR PAQUETE).

IP MÁXIMO	#CODIFICADO	SOBRECARGA EN F_q	
TAMAÑO DE PAQUETE	PAQUETES h	$q = 2^8$	$q = 2^{16}$
500	4	0,80%	1,60%
	8	1,60%	3,20%
	12	3,20%	6,40%
1.000	4	0,40%	0,80%
	8	0,80%	1,60%
	12	2,40%	4,80%
1.500	4	0,27%	0,53%
	8	0,53%	1,07%
	12	0,80%	1,60%

Es preciso notar que la inclusión de coeficientes bloqueados y desbloqueados permite evitar el uso de funciones de troceo homomórfico, que son muy costosas en términos de cálculo.

Debido a la inclusión de un conjunto adicional de coeficientes (los coeficientes bloqueados), el esquema innovador descrito en la presente memoria requiere operaciones adicionales, que se muestran en la Tabla III. A los fines del análisis descrito en la presente memoria, se considera que, en comparación con la multiplicación, la operación de suma produce una complejidad insignificante.

TABLA III

COSTE COMPUTACIONAL DE INCLUIR LOS COEFICIENTES BLOQUEADOS			
NODO	OPERACIÓN	COSTE DETALLADO	COSTE TOTAL
Nodo de Origen	Generación de vectores de matriz de identidad	insignificante	-
	Cifrado de coeficientes bloqueados	Es preciso ver Sección V-A1	
Nodo de Retransmisión	Llevar a cabo operaciones lineales aleatorias adicionales en coeficientes bloqueados (combinando t paquetes)	nh operaciones de multiplicación y (n - 1)h operaciones de suma	O(nt)
Nodo sumidero	Descifrar coeficientes bloqueados para obtener la matriz ML de coeficientes bloqueados de texto claro	Es preciso ver Sección V-A1	O(n2)
	Sustitución de reenvío mediante el uso de coeficientes bloqueados recuperados	O(n2)	
	Descifrar un símbolo cifrado por uso de la matriz de codificación	Es preciso ver Sección V-A1	

A continuación se describe el rendimiento de vídeo inalámbrico. Se provee una evaluación del rendimiento del protocolo descrito más arriba en el escenario de múltiple trayecto de múltiples saltos de la Figura 1, en el cual el servidor S envía vídeo a tres (3) receptores heterogéneos A, B y C, a través de los retransmisores *R1, R2 y R3,* en enlaces inalámbricos con pérdidas. En la descripción en la presente memoria más abajo, el centro se ubica solamente en el rendimiento del esquema en términos de caudal y robustez con respecto a las pérdidas, y su capacidad de entregar vídeo de calidad a un conjunto heterogéneo de receptores. El modelo de codificación de red en capas innovador (esquema NC1) descrito en la presente memoria se compara con una RLNC estándar (esquema NC2) y también con una implementación sin codificación de red (esquema *WoNC*). En el esquema NC2 el servidor envía un tren diferente para cada capa. Cada segmento se codifica en diferentes calidades, mediante el uso de una matriz de coeficiente total para cada capa. Los nodos de retransmisión llevan a cabo operaciones RLNC en los paquetes recibidos que pertenecen a la misma generación y a la misma capa o capas inferiores. En el presente caso, dado que un sumidero de capa L necesita recibir una matriz de rango completo para las capas 1, 2, ...*L*, los sumideros reconocen cada capa que decodifican. La recuperación de errores es similar al esquema NC1. En el esquema *WoNC,* el servidor envía los paquetes nativos sin codificarlos. En el presente caso, los nodos intermedios simplemente reenvían paquetes no codificados de manera normal. Los sumideros envían como realimentación los id de los paquetes que han recibido. Si algunos paquetes se pierden, el servidor los retransmite.

Una configuración de simulación se describe a continuación. El ns-2 simulador 2.33 descrito en S. Mccanne, S. Floyd, y K. Fall, "*ns2 (network simulator 2)*", http://www-nrg.ee.lbl.gov/ns/ con el generador de número aleatorio por defecto se usa para la presente versión. Las bibliotecas de codificación de red se programan de manera independiente. El tren de vídeo es un tráfico de velocidad binaria constante en UDP, donde el servidor transmite a 480 kbps durante 100 segundos. Cada capa tiene un tamaño fijo de 20 paquetes y tres (3) capas para el sistema se consideran. Ello produce una generación de 60 paquetes, correspondientes a 1 segundo de vídeo. El tamaño de paquete es de 1.000 bytes. Como un modelo de propagación, tierra de dos rayos se usa y la probabilidad de pérdida $P_{pérdida}$ se toma como un parámetro de simulación. Dado que se ha demostrado que RTS/CTS tiene un impacto negativo en el rendimiento, se ha deshabilitado para todos los experimentos. Con el fin de simular condiciones de pérdida pesada, las retransmisiones de capa MAC también se han deshabilitado. La velocidad en la capa MAC es de 11 Mbps.

Los receptores comienzan a reproducir el tren de vídeo una vez que han decodificado al menos cinco (5) segmentos de la calidad más baja. La temporización de almacenamiento temporal para un segmento que no se ha decodificado hasta que su plazo para la reproducción llegue se establece en un (1) segundo. Además, se supone un canal de realimentación perfecto (es decir, no se pierde ningún paquete de realimentación). Con el fin de aprovechar la naturaleza de radiodifusión del medio inalámbrico, los retransmisores escuchan los paquetes transmitidos en modo promiscuo.

La siguiente métrica: (i) velocidad reproducida en los receptores, (ii) retardo de almacenamiento temporal inicial, intervalo de tiempo de la recepción del primer paquete al comienzo de la reproducción, (iii) retardo en la decodificación, el tiempo transcurrido desde la recepción del primer paquete de un segmento hasta que dicho segmento se decodifica, (iv) segmentos saltados, porcentaje de segmentos saltados en la reproducción, (v) segmentos de calidad inferior, porcentaje de segmentos reproducidos en calidad inferior a la solicitada, (vi) calidad de reproducción, calidad promedio en la cual cada segmento se reproduce y (vii) carga en el servidor, definida como la relación entre la tasa total enviada por el servidor y la tasa de transmisión. En todos los gráficos, cada punto es el promedio de 10 ejecuciones y las líneas verticales muestran el desvío estándar.

Las Figuras 8-14 ilustran resultados logrados mediante los conceptos, técnicas y sistemas descritos en la presente memoria.

Con referencia, ahora, a la Figura 8, se muestra la velocidad reproducida por cada receptor vs. probabilidad de pérdida. Se muestra la velocidad reproducida como una función de probabilidad de pérdida $P_{pérdida}$, para la técnica descrita en la presente memoria (NC1), tres trenes con codificación de red (NC2) y sin codificación de red *(WoNC).* Como puede verse a partir de la examinación de la Figura 8, el esquema NC1 y el esquema NC2 se ven menos afectados por las pérdidas, debido a la fiabilidad inherente de la codificación de red en entornos volátiles, con el esquema descrito en la presente memoria teniendo un rendimiento coherentemente mejor. El esquema *WoNC,* según lo esperado, tiene un rendimiento pobre dado que el medio se convierte en no fiable.

Con referencia, ahora, a la Figura 9, se muestra la carga en el servidor en función de la pérdida de probabilidad $P_{pérdida}$. Uno puede ver en la Figura 9 que la carga en el servidor crece exponencialmente mientras la pérdida se reduce. En general, los enfoques de codificación de red necesitan enviar menos paquetes codificados para recuperar pérdidas. En $P_{pérdida}$ = 0,9, la carga es ligeramente más alta para la codificación de red dado que el servidor envía, de manera preferente, paquetes redundantes hasta que recibe la realimentación del receptor de que el segmento se ha decodificado, mientras que para el esquema *WoNC* el servidor retransmite paquetes solo cuando recibe realimentación de los receptores. Dado que la mayoría de los paquetes se eliminan, el esquema *WoNC* nunca retransmite.

Con referencia, ahora, a la Figura 10, se muestra CDF de retardo de decodificación para la probabilidad de pérdida $P_{pérdida}$ = 0,4, para la capa 3. La Figura 10 muestra que los enfoques de codificación de red pueden decodificar segmentos en un segundo mientras el servidor envía combinaciones lineales redundantes en una manera de reenvío de alimentación. El esquema *WoNC* necesita un tiempo de decodificación más largo, dado que el servidor espera la realimentación antes de retransmitir. El gráfico que se muestra corresponde a un receptor de capa 3 y el comportamiento para otras capas es similar.

Con referencia, ahora, a las Figuras 11 y 12, dichas figuras muestran el porcentaje de segmentos que se saltan y reproducen en calidad inferior, respectivamente. Es preciso notar que, con la codificación de red, no se saltan segmentos para las capas y, según lo esperado, más segmentos se reproducen en calidad inferior mientras las pérdidas aumentan. Por otro lado, sin la codificación de red, hay menos segmentos reproducidos en calidad inferior, pero al menos tiempo el porcentaje de saltos crece de forma significativa dado que los paquetes retransmitidos por el servidor no llegan a los receptores a su debido tiempo. Dicho efecto se encuentra exacerbado en pérdidas más altas, donde nunca se reproducen segmentos (y, por lo tanto, tampoco se saltan).

Con referencia, ahora, a la Figura 13, se muestra el retardo de almacenamiento temporal inicial en función de la probabilidad de pérdida para la capa 3. Uno puede ver en la Figura 13 que, para nuestro esquema, los receptores almacenan, de forma temporal, durante un tiempo más corto antes de comenzar la reproducción. El retardo de almacenamiento temporal inicial crece lentamente con la probabilidad de pérdida, dado que un solo paquete codificado de red puede recuperar múltiples pérdidas. Para el esquema *WoNC,* cuando las pérdidas son altas, los receptores no pueden decodificar nada y, por lo tanto, nunca comienzan a reproducir el archivo.

Los gráficos que se muestran en las Figuras 11 y 13 corresponden a la capa 3. El comportamiento para otras capas es similar y ligeramente mejor, dado que los receptores de capa 3 necesitan recibir más paquetes que los nodos de capa inferior.

Con referencia, ahora, a la Figura 14, se muestra un gráfico de calidad reproducida para $P_{pérdida}$ = 0,4. La Figura 14 muestra la calidad promedio en la cual cada segmento se reproduce, cuando $P_{pérdida}$ = 0,4. Un segmento saltado se representa como reproducido en una calidad igual a 0. Es preciso notar que los enfoques de codificación de red muestran una alta resiliencia a errores y el archivo de vídeo se reproduce constantemente en la calidad deseada por cada receptor en comparación con el esquema *WoNC,* nuevamente con nuestro esquema mostrando un mejor rendimiento.

Finalmente, debe notarse que el esquema descrito en la presente memoria supera el esquema NC2 debido a la matriz de codificación triangular usada para la codificación y a la estructura anidada de las capas de vídeo. Dichas características resultan en una robustez más alta con respecto a las pérdidas (Figura 8), mejor calidad de vídeo con

menos saltos y menos segmentos reproducidos en menor calidad (Figura 12) y retardo de almacenamiento temporal más corto (Figura 13).

En la presente memoria se describe un esquema práctico para la transmisión por secuencias de vídeo escalable que explota las características algebraicas de la codificación de red lineal aleatoria (RLNC).

Por un lado, los conceptos, sistemas y esquemas descritos en la presente memoria aseguran niveles diferenciados de seguridad para usuarios distintos. Por otro lado, las propiedades del paradigma de codificación de red aseguran la resiliencia a pérdidas de paquetes en canales inalámbricos. La evaluación de seguridad demuestra que es posible reducir, de manera significativa, el número de operaciones de cifrado (o, de manera equivalente, los requisitos de complejidad) mientras se cuantifican los niveles de seguridad.

Debe notarse que el sistema y las técnicas descritas en la presente memoria se han centrado en ataques de escuchas indiscretas. Los ataques de contaminación de la red pueden tratarse mediante el uso de técnicas convencionales, aunque algunas técnicas convencionales han sumado en términos de retardo y complejidad.

Como parte de nuestro continuo trabajo, estamos mirando maneras de mitigar los efectos de dichos ataques bizantinos bajo las limitaciones en tiempo real de servicios de transmisión.

Habiendo descrito las realizaciones preferidas de la invención, ahora será aparente para las personas con experiencia ordinaria en la técnica que otras realizaciones que incorporan dichos conceptos pueden usarse. Por consiguiente, se establece que la invención no debe limitarse a las realizaciones descritas sino, más bien, que debe estar limitada solamente por el alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Un método para transmitir datos de vídeo en una red que incluye un nodo de origen, múltiples nodos de retransmisión y uno o más nodos de receptor y que incluye un conjunto de operaciones de seguridad y operaciones de transmisión por secuencias de vídeo con codificación de red, el método comprendiendo:

llevar a cabo una distribución de clave única entre el nodo de origen y cada uno del único o más nodos de receptor;

dividir los datos de vídeo en uno o más grupos de imágenes "GoP", cada uno del más de un grupo de imágenes teniendo una duración predeterminada;

para cada grupo de imágenes "GoP", generar en el nodo de origen de una matriz triangular inferior **A** de n × n, en la cual l es un número de capas en el GoP en donde hay al menos una fila en la matriz **A** para cada capa, en donde la matriz **A** se usa para la codificación en la fuente solamente y cada entrada diferente de cero de la matriz **A** es un elemento a_{ij} elegido de manera uniforme de forma aleatoria de todos los elementos diferentes de cero del campo $F_q \setminus \{0\}$;

dividir el GoP en múltiples vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, cada uno de los vectores teniendo K símbolos S_1 - S_k en los cuales el $k^{ésimo}$ símbolo de cada vector pertenece a una capa correspondiente de l capas en el GoP;

cifrar múltiples símbolos de cada vector $b^{(i)}$ para cada uso de la matriz de codificación;

aplicar la matriz de codificación **A** de manera sucesiva a los símbolos de información que se enviarán para proveer una carga útil de uno o más paquetes, conformados por símbolos de información codificada;

cifrar cada línea de una primera matriz **A** con una clave de capa correspondiente en donde la primera matriz **A** cifrada corresponde a una matriz de coeficientes bloqueados;

generar una matriz de identidad de *n* × *n* correspondiente a coeficientes desbloqueados, en donde cada uno del único o más paquetes comprenden un encabezamiento y la carga útil y en donde el encabezamiento comprende los coeficientes bloqueados y desbloqueados; y

codificar el único o más paquetes en nodos de retransmisión según un protocolo de codificación de red lineal aleatoria "RLNC" en donde la codificación algebraica se lleva a cabo en coeficientes desbloqueados, coeficientes bloqueados y carga útil; y los nodos de retransmisión identifican la capa de un paquete mirando los coeficientes desbloqueados, y los paquetes se mezclan con paquetes de la misma capa o capas inferiores solamente.

2. El método de la reivindicación 1, en donde la duración es de un segundo.

3. El método de la reivindicación 2, en donde llevar a cabo la codificación algebraica en coeficientes desbloqueados, coeficientes bloqueados y carga útil comprende llevar a cabo la codificación algebraica de manera indistinguible en coeficientes desbloqueados, coeficientes bloqueados y carga útil.

4. El método de la reivindicación 1, que además comprende:

aplicar, mediante los receptores, la eliminación gaussiana siguiendo la RLNC estándar en los coeficientes desbloqueados;

recuperar los coeficientes bloqueados mediante el descifrado de cada línea de la matriz con la clave correspondiente; y

obtener texto claro por un proceso de sustitución de reenvío.

5. El método de la reivindicación 4, en donde el cifrado de múltiples símbolos de cada capa incluye cifrar cada símbolo con la clave para la capa correspondiente en el GoP.

6. El método de la reivindicación 5, que además comprende:

enviar una primera línea de la matriz no cifrada.

7. El método de la reivindicación 1, en donde solo una clave única por capa se usa para el cifrado multirresolución.

8. El método de la reivindicación 7, en donde el cifrado de cada línea de una primera matriz A con una clave de capa correspondiente comprende cifrar cada línea de primera matriz A con una clave de capa correspondiente mediante la fuente.

9. El método de la reivindicación 1, en donde más de una fila de la matriz A para cada capa se usa.

10. Un sistema para transmitir datos de vídeo en una red, el sistema comprendiendo:

(a) un nodo de origen para dividir los datos de vídeo en más de un grupo de imágenes "GoP", cada uno del más de un grupo de imágenes teniendo una duración predeterminada en donde para cada grupo de imágenes "GoP", el nodo de origen genera una matriz triangular inferior **A** de n × n, en la cual l es el número de capas en el GoP en donde la matriz **A** se usa para codificar en la fuente solamente y cada entrada diferente de cero de la matriz **A** es un elemento a_{ij} elegido uniformemente de manera aleatoria de todos los elementos diferentes de cero del campo $F_q \setminus \{0\}$ y el nodo de origen divide el GoP en múltiples vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, cada uno de los vectores teniendo K símbolos S_1 - S_k en los cuales el símbolo de cada vector pertenece a una capa correspondiente de las l capas en el GoP y en donde el nodo de origen cifra múltiples símbolos de cada vector $\underline{b}^{(l)}$ para cada uso de la matriz de codificación A, los múltiples símbolos incluyendo al menos un primer símbolo asociado a una primera capa del GoP y un segundo símbolo asociado a una segunda capa diferente del GoP, en donde la salida de la operación de un cifrado de tren de un símbolo P con una clave aleatoria $\underline{K}$ se denota como $E(P,\underline{K})$ y el nodo de origen aplica la matriz de codificación **A** sucesivamente a los símbolos de información que se enviarán para proveer símbolos de información codificada que comprenden una carga útil de uno o más paquetes, y el nodo de origen cifra cada línea de una primera matriz **A** con una clave de capa correspondiente, en donde la primera matriz **A** corresponde a una matriz de coeficientes bloqueados y el nodo de origen genera una matriz de identidad de $n \times n$ correspondiente a coeficientes desbloqueados, en donde cada uno del único o más paquetes comprenden un encabezamiento y la carga útil, en donde el encabezamiento comprende los coeficientes bloqueados y desbloqueados;

(b) múltiples nodos de retransmisión; y

(c) uno o más nodos de receptor;

en donde los nodos de retransmisión codifican el único o más paquetes según un protocolo de codificación de red lineal aleatoria "RLNC" en donde la codificación algebraica se lleva a cabo en coeficientes desbloqueados, coeficientes bloqueados y carga útil y los nodos de retransmisión identifican la capa de un paquete entrante mirando los coeficientes desbloqueados, y los paquetes se mezclan con paquetes de la misma capa o capas inferiores solamente en los nodos de retransmisión.

11. Un nodo de origen configurado para transmitir transmisión por secuencias de vídeo hacia uno o más nodos de receptor mediante múltiples nodos de retransmisión en donde dicho nodo de origen también se configura para dividir los datos de vídeo en más de un grupo de imágenes "GoP", cada uno del más de un grupo de imágenes teniendo una duración predeterminada en donde para cada grupo de imágenes "GoP", el nodo de origen genera una matriz triangular inferior **A** de n × n, en la cual l es el número de capas en el GoP en donde la matriz **A** se usa para codificar en la fuente solamente y cada entrada diferente de cero de la matriz **A** es un elemento a_{ij} elegido uniformemente de manera aleatoria de todos los elementos diferentes de cero del campo $F_q \setminus \{0\}$ y el nodo de origen divide el GoP en múltiples vectores $\underline{b}^{(1)} \ldots \underline{b}^{(w)}$, cada uno de los vectores teniendo K símbolos S_1 - SK en los cuales el símbolo de cada vector pertenece a una capa correspondiente de las l capas en el GoP y en donde el nodo de origen cifra múltiples símbolos de cada vector $\underline{b}^{(l)}$ para cada uso de la matriz de codificación A, los múltiples símbolos incluyendo al menos un primer símbolo asociado a una primera capa del GoP y un segundo símbolo asociado a una segunda capa diferente del GoP, en donde la salida de la operación de un cifrado de tren de un símbolo P con una clave aleatoria $\underline{K}$ se denota como $E(P,\underline{K})$ y el nodo de origen aplica la matriz de codificación **A** sucesivamente a los símbolos de información que se enviarán para proveer símbolos de información codificada que comprenden una carga útil de uno o más paquetes, y el nodo de origen cifra cada línea de una primera matriz **A** con una clave de capa correspondiente, en donde la primera matriz **A** corresponde a una matriz de coeficientes bloqueados y el nodo de origen genera una matriz de identidad de $n \times n$ correspondiente a coeficientes desbloqueados, en donde cada uno del único o más paquetes comprenden un encabezamiento y la carga útil, en donde el encabezamiento comprende los coeficientes bloqueados y desbloqueados.

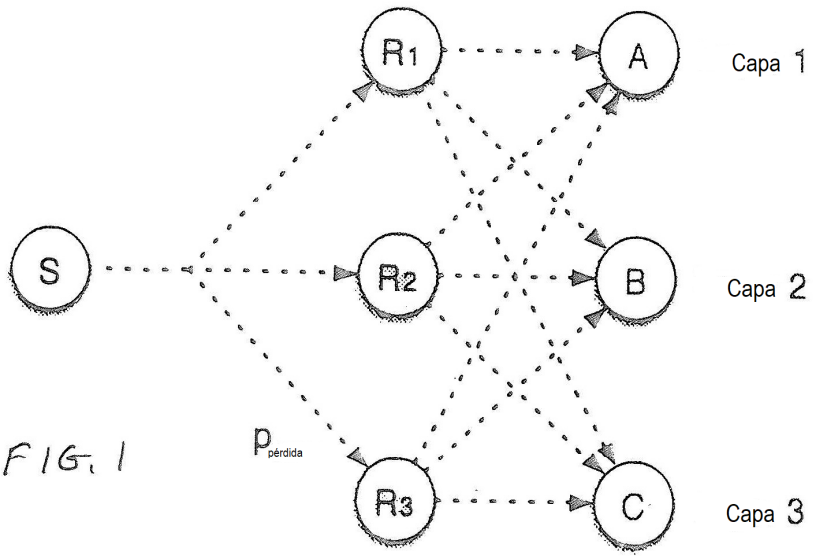


FIG. 1

FIG. 2

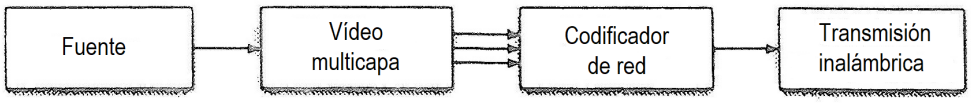
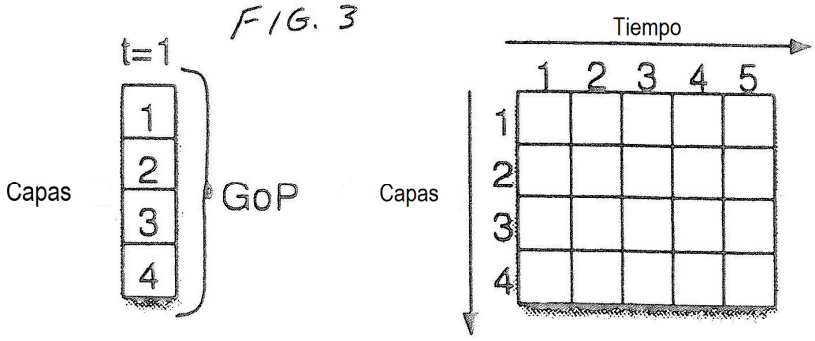


FIG. 3



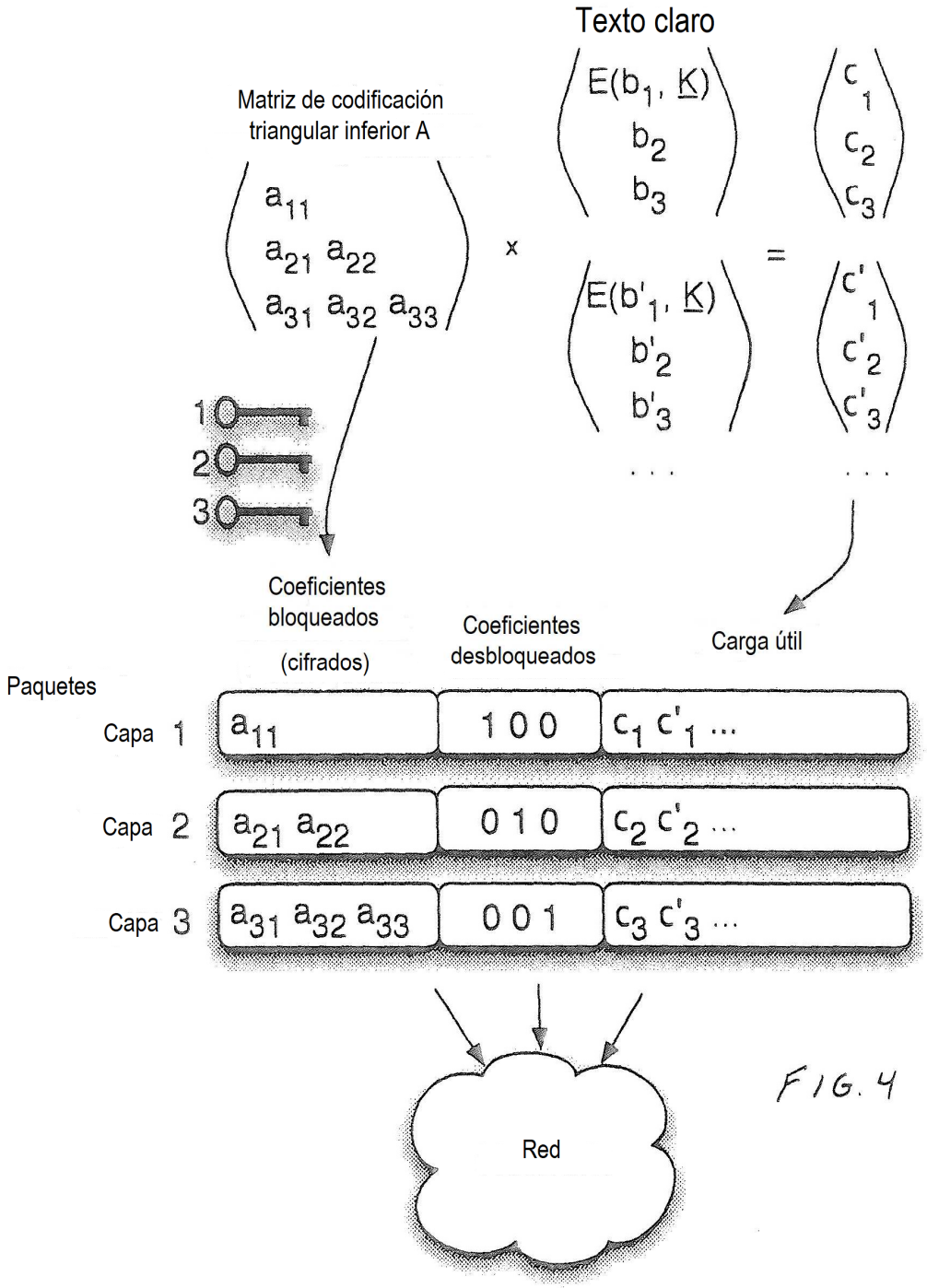

Texto claro
Matriz de codificación triangular inferior A
x
=
1
2
3
Coeficientes bloqueados (cifrados)
Coeficientes desbloqueados
Carga útil
Paquetes
Capa 1
Capa 2
Capa 3
100
010
001
Red

FIG. 4

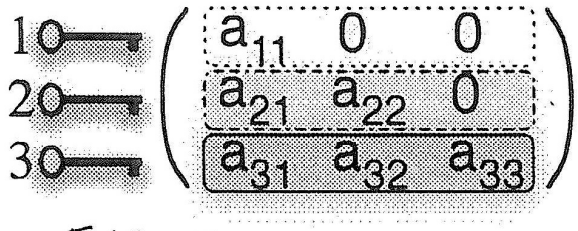

10
20
30
a_{11} 0 0
a_{21} a_{22} 0
a_{31} a_{32} a_{33}

FIG. 5

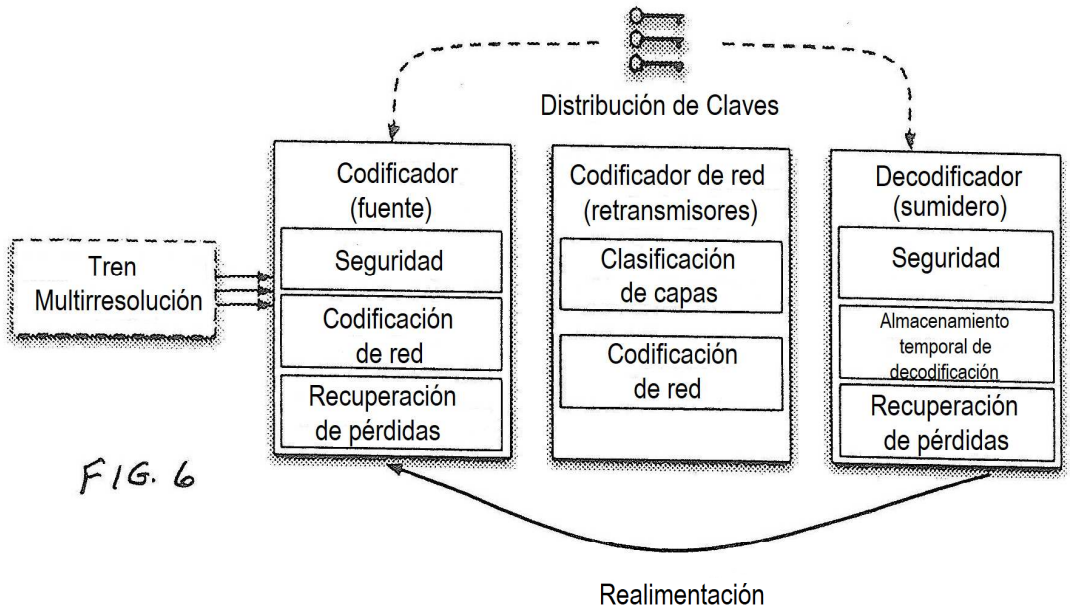

Distribución de Claves
Tren Multirresolución
Codificador (fuente)
Seguridad
Codificación de red
Recuperación de pérdidas
Codificador de red (retransmisores)
Clasificación de capas
Codificación de red
Decodificador (sumidero)
Seguridad
Almacenamiento temporal de decodificación
Recuperación de pérdidas
Realimentación

FIG. 6

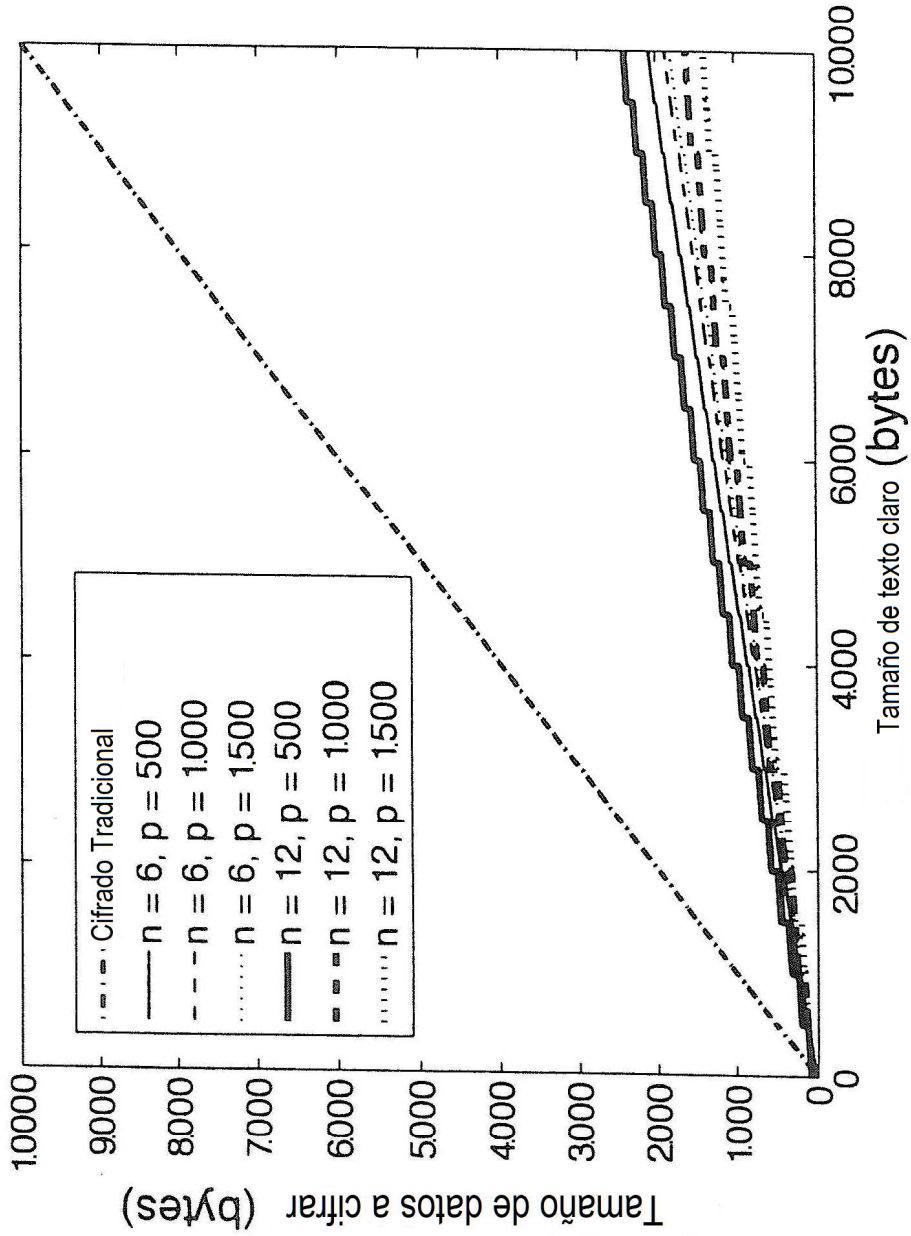

Tamaño de datos a cifrar (bytes)
10.000
9.000
8.000
7.000
6.000
5.000
4.000
3.000
2.000
1.000
0
0
2000
4.000
6.000
8.000
10.000
Tamaño de texto claro (bytes)
Cifrado Tradicional
n = 6, p = 500
n = 6, p = 1.000
n = 6, p = 1.500
n = 12, p = 500
n = 12, p = 1.000
n = 12, p = 1.500

FIG. 7

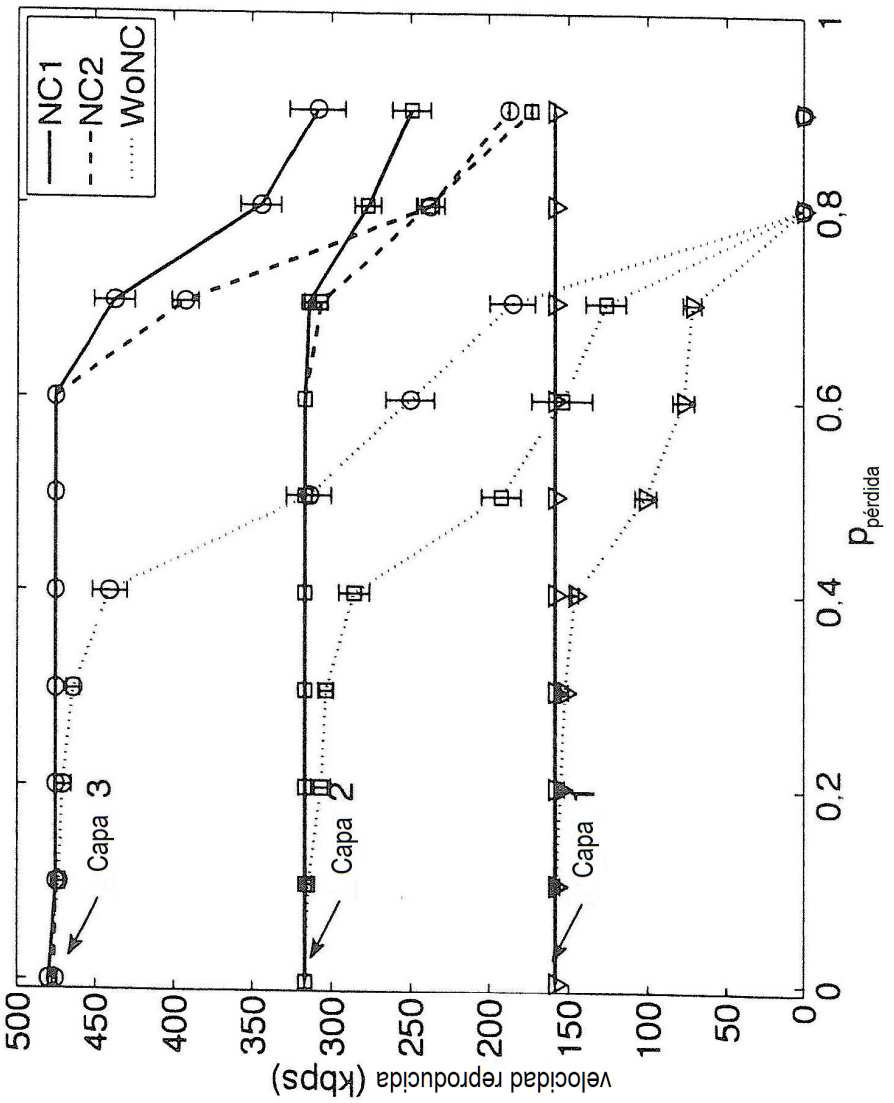

NC1
NC2
WoNC
Capa 3
Capa 2
Capa 1
velocidad reproducida (kbps)
500
450
400
350
300
250
200
150
100
50
0
0
0,2
0,4
0,6
0,8
1
$p_{pérdida}$

FIG. 8

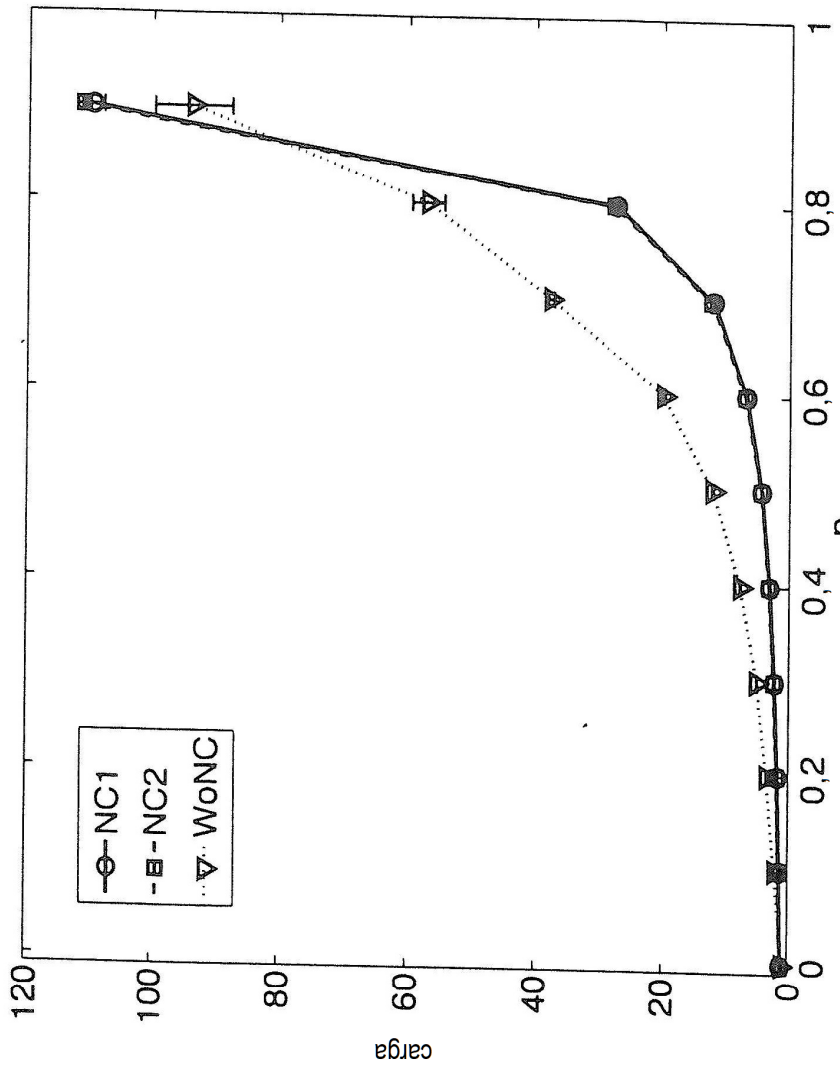


FIG. 9

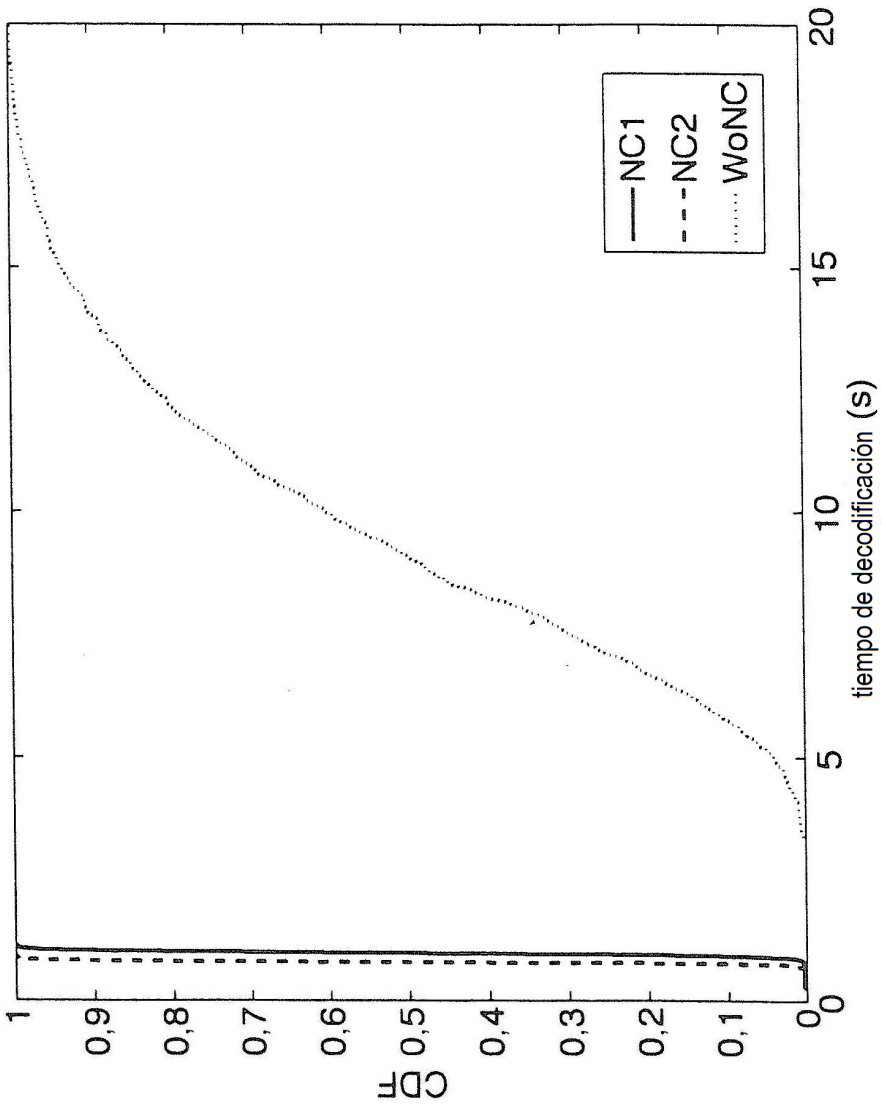

CDF
1
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0
0
5
10
15
20
tiempo de decodificación (s)
NC1
NC2
WoNC

FIG. 10

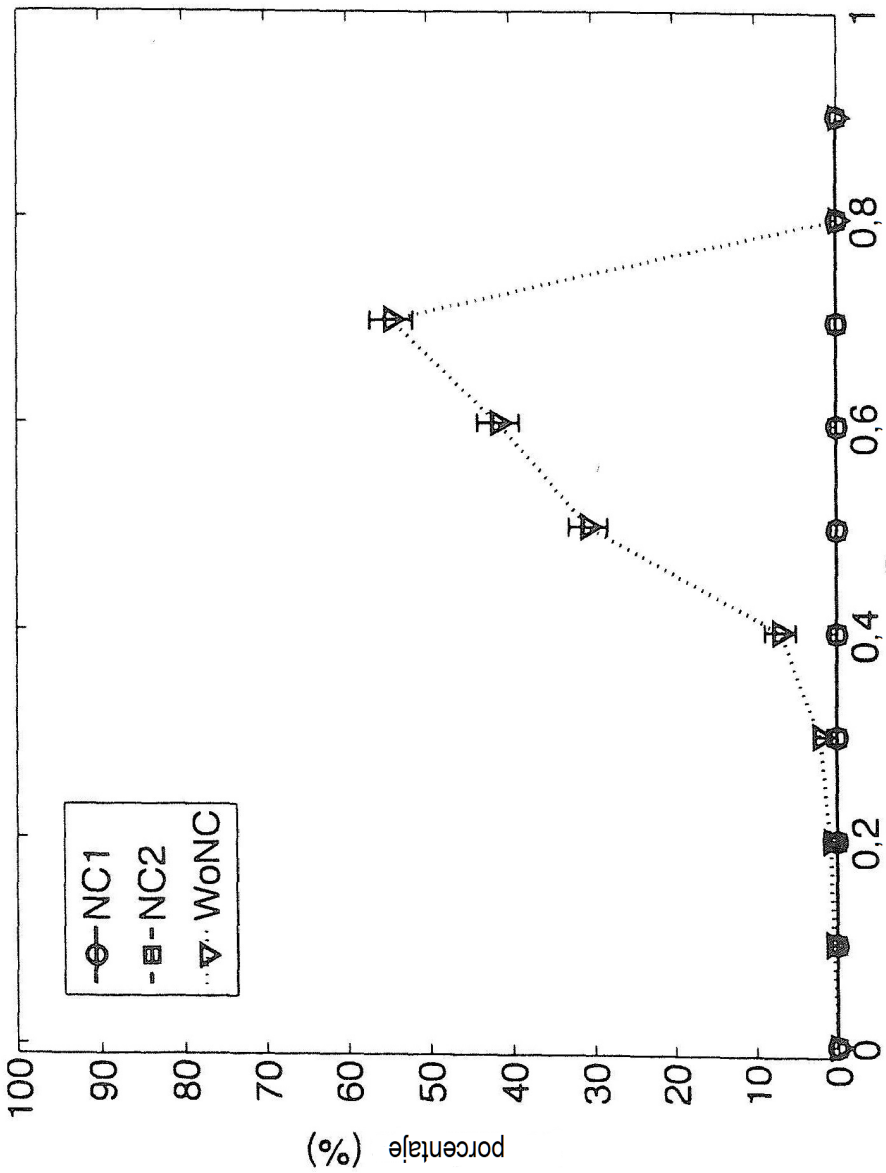

porcentaje (%)
100
90
80
70
60
50
40
30
20
10
0
0
0,2
0,4
0,6
0,8
1
$p_{pérdida}$
NC1
NC2
WoNC

FIG. 11

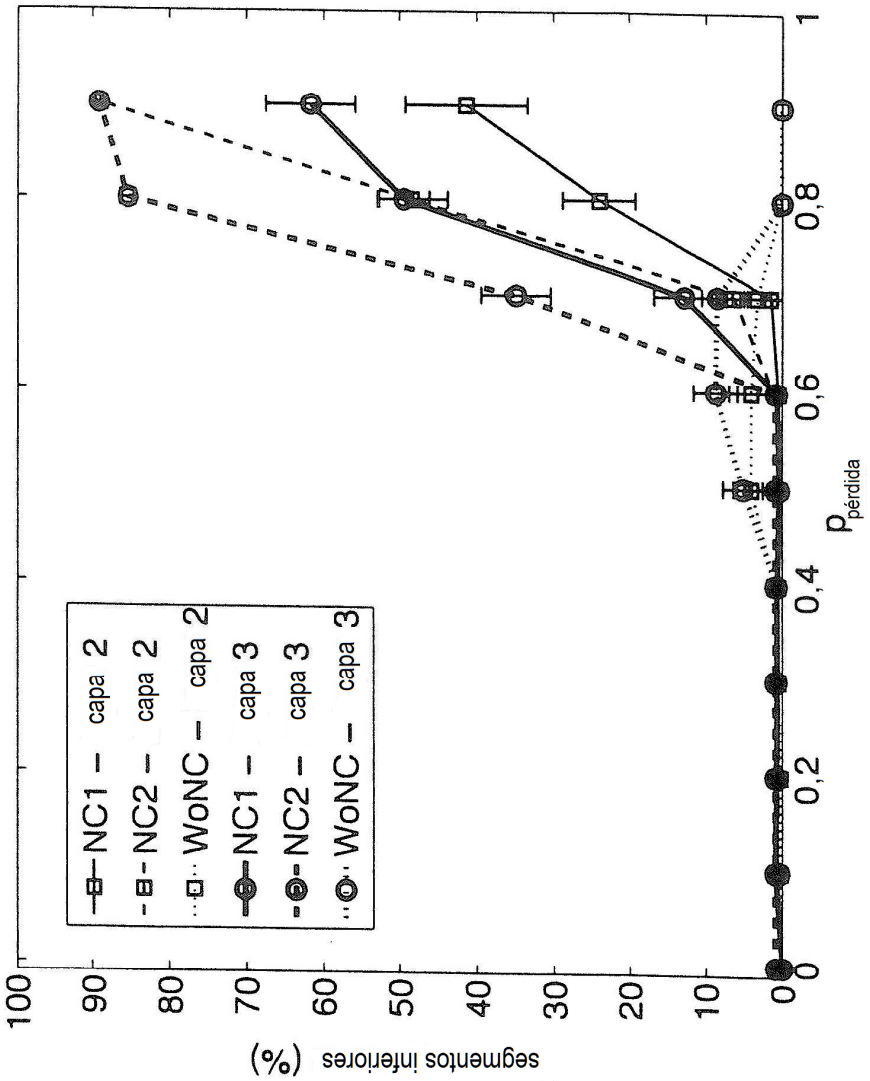

segmentos inferiores (%)
100
90
80
70
60
50
40
30
20
10
0
0
0,2
0,4
0,6
0,8
1
$p_{pérdida}$
NC1 – capa 2
NC2 – capa 2
WoNC – capa 2
NC1 – capa 3
NC2 – capa 3
WoNC – capa 3

FIG. 12

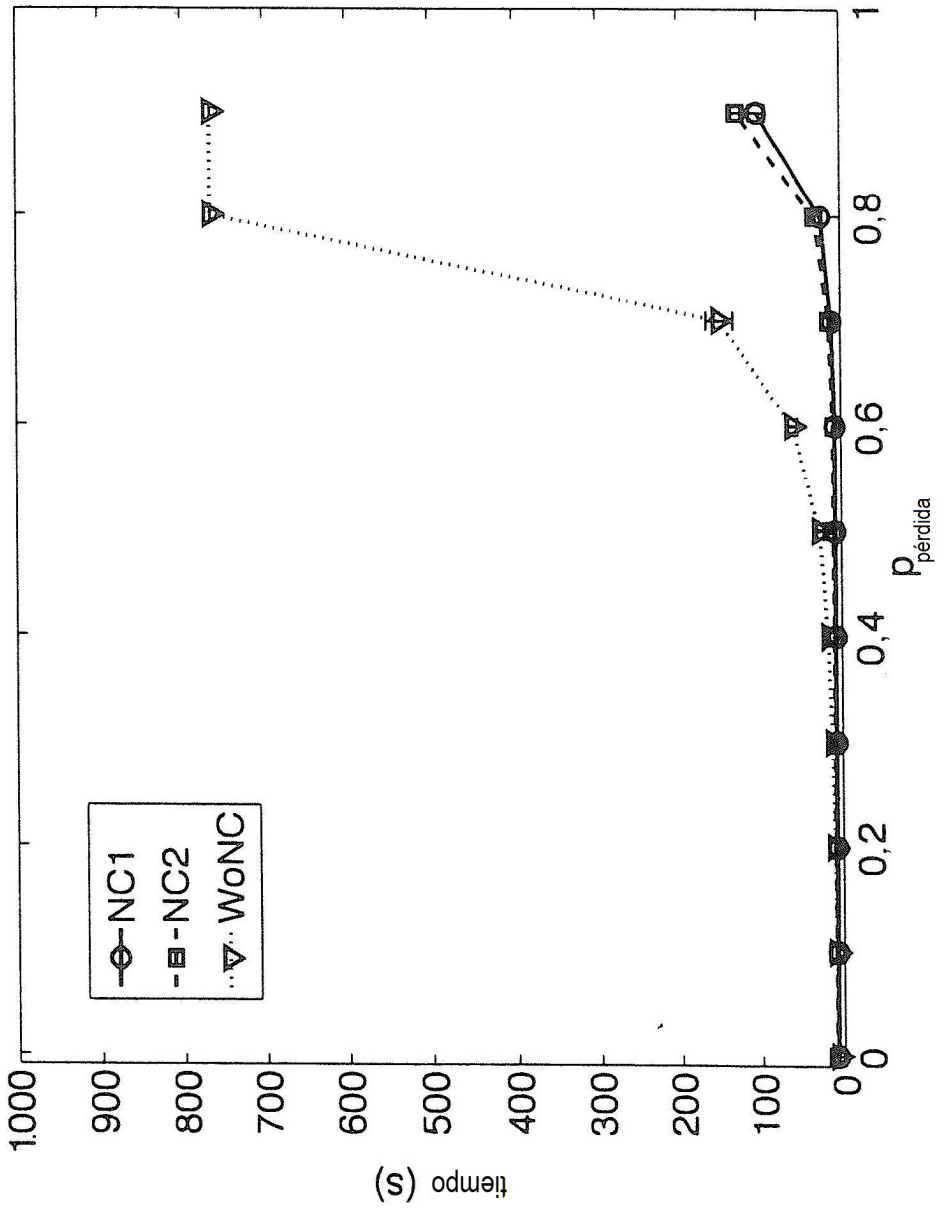

NC1
NC2
WoNC
tiempo (s)
1.000
900
800
700
600
500
400
300
200
100
0
0,2
0,4
0,6
0,8
1
$p_{pérdida}$

FIG. 13

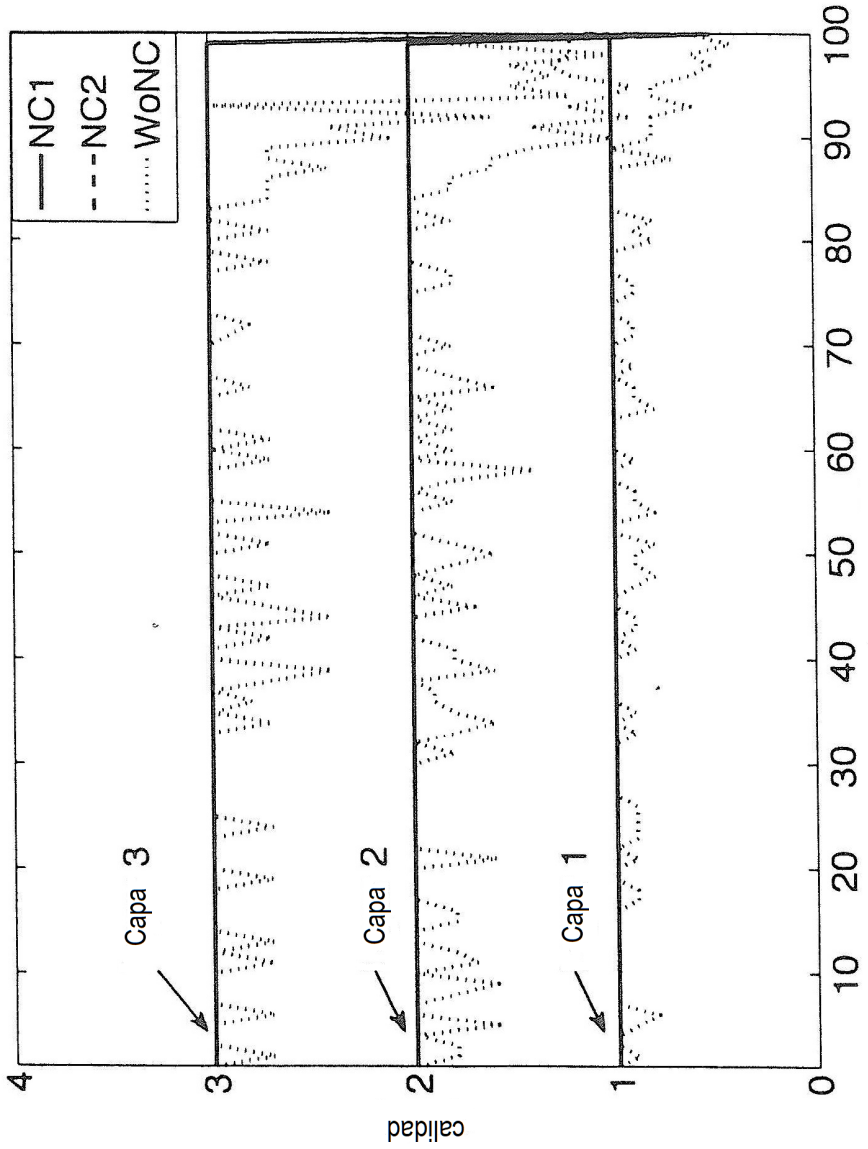

NC1
NC2
WoNC
Capa 3
Capa 2
Capa 1
calidad
id de segmento
0
1
2
3
4
10
20
30
40
50
60
70
80
90
100

FIG. 14