(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 350 848**

(51) Int. Cl.:
H04L 25/03 (2006.01)
H04L 1/06 (2006.01)
H04B 7/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05791647 .0**
(96) Fecha de presentación : **26.08.2005**
(97) Número de publicación de la solicitud: **1782592**
(97) Fecha de publicación de la solicitud: **09.05.2007**

(54) Título: **Encriptación de bits codificados para comunicación de múltiples flujos en un canal MIMO.**

(30) Prioridad: **27.08.2004 US 605183 P**
30.09.2004 US 615567 P
08.10.2004 US 617502 P
25.08.2005 US 212239

(45) Fecha de publicación de la mención BOPI:
27.01.2011

(45) Fecha de la publicación del folleto de la patente:
27.01.2011

(73) Titular/es: **QUALCOMM INCORPORATED**
5775 Morehouse Drive
San Diego, California 92121, US

(72) Inventor/es: **Kim, Byoung-Hoon**

(74) Agente: **Carpintero López, Mario**

Descripción

ANTECEDENTES

Campo

La presente invención se refiere, en general, a comunicaciones inalámbricas y, más específicamente, a la transmisión de múltiples flujos en un canal de múltiples entradas-múltiples salidas (MIMO) en un sistema de comunicación inalámbrica.

Antecedentes

El reciente éxito de los sistemas de antenas de múltiples entradas-múltiples salidas (MIMO) en canales inalámbricos se debe al menos en parte al hecho de que pueden lograr un crecimiento lineal de capacidad en proporción con el número de antenas de transmisión y recepción. Para la transmisión de múltiples flujos en un sistema de acceso múltiple por división de código (CDMA), de múltiples entradas-múltiples salidas (MIMO), generalmente se asignan o bien múltiples códigos de Walsh diferentes o bien el mismo código de Walsh para los múltiples flujos. Una estrategia de asignación de códigos es empezar con una asignación de códigos de Walsh distintos y luego compartir de manera creciente los códigos a medida que aumenta la tasa de transmisión de datos o el número de códigos requerido para cada flujo. Sin embargo, eventualmente, se asignarán los mismos códigos para todos los flujos con el fin de lograr la capacidad máxima que puede proporcionar un sistema MIMO. En un sistema MIMO de banda estrecha, en el que la ampliación de ancho de banda no está permitida, los múltiples flujos se transmiten generalmente sin ninguna separación entre canales mediante cobertura de códigos de Walsh.

Dependiendo del movimiento de la estación móvil, los vectores de coeficientes de canal de cada flujo de datos en el sistema MIMO tendrán diversas realizaciones instantáneas. Los vectores de coeficientes pueden ser casi ortogonales entre sí en un instante mientras que pueden tener valores muy próximos o una alta correlación instantánea a continuación. Cuando los vectores de coeficientes de canal de los múltiples flujos se vuelven próximos, cada uno de los flujos interfiere con los otros flujos. En el caso extremo, cuando los vectores de coeficientes de canal de múltiples flujos adoptan casi los mismos valores, el decodificador de cada flujo experimenta la métrica de trayectoria de decodificación competitiva entre el flujo deseado y los flujos interferentes. Puede producirse a menudo el caso extremo si la estación móvil ve una fuerte señal de línea de visión (LOS) procedente de la estación base, en el que el canal MIMO se vuelve próximo a un canal matricial de AWGN o a un canal matricial de tipo Rice con un alto factor de Rice. Existe por tanto una necesidad en la técnica de sistemas y procedimientos de comunicación que superen estos problemas.

Se presta atención adicionalmente al documento US 2003/021355, que da a conocer un procedimiento y sistema de transmisión y recepción de señales en un sistema de comunicación móvil dotado de una pluralidad de antenas. El procedimiento de transmisión de señales en el sistema de comunicación móvil que transmite una señal a través de una pluralidad de antenas incluye separar por capas y codificar de manera primaria datos de entrada para una generación de señales independientes que entrelaza en espacio y tiempo los datos codificados de manera primaria de las capas respectivas, recibir y codificar de manera secundaria los datos entrelazados, y transmitir los datos codificados de manera secundaria a través de la pluralidad de antenas.

También se presta atención al documento WO 2004/038951, que describe técnicas para facilitar el acceso aleatorio en sistemas de comunicación de acceso múltiple inalámbricos. Un canal de acceso aleatorio (RACH) se define como que comprende un RACH “rápido” (F-RACH) y un RACH “lento” (S-RACH). Los F-RACH y S-RACH pueden soportar eficazmente terminales de usuario en diferentes estados operativos y emplear diferentes diseños. El F-RACH puede usarse para acceder rápidamente al sistema, y el S-RACH es más robusto y puede soportar terminales de usuario en diversas condiciones y estados operativos. El F-RACH puede usarse por terminales de usuario que se han registrado en el sistema y puede compensar sus retardos de ida y vuelta (RTD) adelantando apropiadamente el momento de su transmisión. El S-RACH puede usarse por terminales de usuario que pueden haberse registrado o no en el sistema, y puede compensar o no sus RTD. Los terminales de usuario pueden usar el F-RACH o el S-RACH, o ambos, para obtener acceso al sistema.

Además, se presta atención al documento WO 2004/039011, que describe un sistema WLAN MIMO de múltiple acceso que emplea MIMO, OFDM y TDD. El sistema (1) usa una estructura de canales con varios canales de transporte configurables, (2) soporta múltiples tasas y modos de transmisión, que son configurables basándose en las condiciones de canal y las capacidades de los terminales de usuario, (3) emplea una estructura piloto con varios tipos de piloto (por ejemplo, pilotos de baliza, MIMO, de referencia controlada y portadores) para diferentes funciones, (4) implementa lazos de control de potencia, sincronización y tasa de transmisión para una operación apropiada del sistema, y (5) emplea acceso aleatorio para el acceso al sistema por los terminales de usuario, rápido acuse de recibo y rápidas asignaciones de recursos.

Finalmente, se presta atención al documento WO 03/085875, que describe la selección de un modo de codificación espaciotemporal para su uso cuando se transmite con diversidad espacial basada en la diversidad de recepción asociada con un dispositivo receptor y la calidad de los canales de transmisión basándose en información realimentada desde el dispositivo

receptor. Los modos de codificación en espaciotemporal seleccionables son preferiblemente codificación con diversidad de transmisión espaciotemporal y una versión de codificación de tipo BLAST. Además, los modos de modulación, las tasas de codificación de errores, o una combinación de los mismos, también pueden basarse en la calidad de los canales de transmisión y la diversidad disponible del dispositivo receptor.

SUMARIO DE LA INVENCIÓN

Según la presente invención, se proporcionan un aparato, según se expone en las reivindicaciones 1, 12, 13 y 18, y un procedimiento según se expone en las reivindicaciones 19, 30, 31 y 36. Se reivindican realizaciones de la invención en las reivindicaciones dependientes.

Las realizaciones dadas a conocer en el presente documento tratan las necesidades establecidas anteriormente encriptando los bits codificados de cada flujo para impedir un rendimiento de decodificación degenerativo del sistema MIMO cuando los vectores de coeficientes de canal de múltiples flujos se vuelven relativamente próximos o correlacionados. En una realización, se multiplican diferentes códigos de encriptación por el bit codificado de cada flujo para impedir el rendimiento de decodificación degenerativo de un sistema MIMO cuando los vectores de coeficientes de canal de múltiples flujos se vuelven relativamente próximos o correlacionados. Esto convierte palabras de código competidoras de un flujo interferente en palabras aleatorias inválidas desde el punto de vista del decodificador del flujo deseado. Una realización proporciona la encriptación y desencriptación de cada flujo.

Mediante la encriptación (que generalmente se produce en el transmisor) y la desencriptación (que generalmente se produce en el receptor) de bits codificados de cada flujo, el decodificador de cada flujo evita colisiones de palabras de código. Durante la desencriptación, la palabra de código potencialmente competidora del flujo interferente pierde su legitimidad como palabra de código candidata y se convierte en una palabra aleatoria inocua. En muchos casos, la palabra aleatoria no genera una métrica de trayectoria competitiva para una hipotética palabra de código candidata en el decodificador. El efecto del distinto patrón de entrelazado o distinto patrón de perforación (*puncturing*) y repetición (por ejemplo, versión de redundancia) es similar a la encriptación distinta.

Una realización incluye un aparato que comprende un codificador para codificar una pluralidad de flujos de bits fuente para producir una pluralidad de flujos de bits codificados, un procesador de flujos de bits para encriptar cada uno de dichos flujos de bits codificados con un encriptador configurado de diferente manera para producir una pluralidad de flujos de bits encriptados de diferente manera, y un mapeador para mapear grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión.

Otra realización incluye un aparato que comprende un codificador para codificar una pluralidad de flujos de bits fuente para producir una pluralidad de flujos bits codificados, un procesador de flujos de bits para entrelazar cada uno de los flujos de bits codificados con un patrón de entrelazado diferente para producir una pluralidad de flujos de bits entrelazados de diferente manera, y un mapeador para mapear grupos de bits de dicha pluralidad de flujos de bits entrelazados de diferente manera en símbolos de transmisión.

Otra realización incluye un aparato que comprende un codificador para codificar una pluralidad de flujos de bits fuente para producir una pluralidad de flujos bits codificados, un procesador de flujos de bits para adaptar las tasas de transmisión de cada uno de los flujos de bits codificados con un patrón de perforación o repetición diferente en cada flujo de bits codificados para producir una pluralidad de diferentes flujos de bits, y un mapeador para mapear grupos de bits de dicha pluralidad de diferentes flujos de bits en símbolos de transmisión.

Otra realización incluye un aparato que comprende un desmapeador para traducir símbolos recibidos en grupos de bits y para producir una pluralidad de flujos bits recibidos, un procesador de flujos de bits para aplicar un algoritmo de desencriptación diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desencriptados de diferente manera, y un decodificador para decodificar dichos de flujos de bits desencriptados de diferente manera para producir una pluralidad de flujos de bits decodificados.

Otra realización incluye un aparato que comprende un desmapeador para traducir símbolos recibidos en grupos de bits y para producir una pluralidad de flujos bits recibidos, un procesador de flujos de bits para aplicar un patrón de desentrelazado diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desentrelazados de diferente manera, y un decodificador para decodificar dichos de flujos de bits desentrelazados de diferente manera para producir una pluralidad de flujos de bits decodificados.

Otra realización incluye un aparato que comprende un desmapeador para traducir símbolos recibidos en grupos de bits y para producir una pluralidad de flujos bits recibidos, un procesador de flujos de bits para aplicar un patrón de desperforación (*depuncturing*) diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desperforados de diferente manera, y un decodificador para decodificar dichos de flujos de bits desperforados de diferente manera para producir una pluralidad de flujos de bits decodificados.

Otra realización incluye un procedimiento de transmisión de información en un sistema de comunicación de múltiples entradas-múltiples salidas. El procedimiento comprende codificar una pluralidad de flujos de bits fuente para producir una pluralidad de bits codificados, encriptar cada uno de dichos flujos de bits codificados con un encriptador configurado de

diferente manera para producir una pluralidad de flujos de bits encriptados de diferente manera, y mapear grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión.

Otra realización incluye un procedimiento de transmisión de información en un sistema de comunicación de múltiples entradas-múltiples salidas. El procedimiento comprende codificar una pluralidad de flujos de bits fuente para producir una pluralidad de bits codificados, entrelazar cada uno de los flujos de bits codificados con un patrón de entrelazado diferente para producir una pluralidad de flujos de bits entrelazados de diferente manera, y mapear grupos de bits de dicha pluralidad de flujos de bits entrelazados de diferente manera en símbolos de transmisión.

Otra realización incluye un procedimiento de transmisión de información en un sistema de comunicación de múltiples entradas-múltiples salidas. El procedimiento comprende codificar una pluralidad de flujos de bits fuente para producir una pluralidad de flujos de bits codificados, adaptar las tasas de transmisión de cada uno de los flujos de bits codificados con un patrón de perforación o repetición diferente en cada flujo de bits entrelazados para producir una pluralidad de diferentes flujos de bits, y mapear grupos de bits de dicha pluralidad de diferentes flujos de bits en símbolos de transmisión.

Otra realización incluye un procedimiento para recibir información en un dispositivo de comunicación. El procedimiento comprende traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos bits recibidos, aplicar un algoritmo de desencriptación diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desencriptados de diferente manera, y decodificar dichos de flujos de bits desencriptados de diferente manera para producir una pluralidad de flujos de bits decodificados.

Otra realización incluye un procedimiento para recibir información en un dispositivo de comunicación. El procedimiento comprende traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos bits recibidos, aplicar un patrón de desentrelazado diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desentrelazados de diferente manera, y decodificar dichos de flujos de bits desentrelazados de diferente manera para producir una pluralidad de flujos de bits decodificados.

Otra realización incluye un procedimiento para recibir información en un dispositivo de comunicación. El procedimiento comprende traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos bits recibidos, aplicar un patrón de desperforación diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desperforados de diferente manera, y decodificar dichos de flujos de bits desperforados de diferente manera para producir una pluralidad de flujos de bits decodificados.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1A es un diagrama de bloques de una realización de un sistema CDMA de múltiples códigos MIMO basado en multiplexación espacial y codificación individual;

la figura 1B es un diagrama de bloques de otra realización de un sistema CDMA de múltiples códigos MIMO basado en multiplexación espacial y codificación individual;

la figura 1C es un diagrama de bloques de una realización de un sistema OFDM MIMO basado en multiplexación espacial y codificación individual;

la figura 2 es un gráfico de rendimiento global frente a pT para un sistema MIMO 2x2, donde Ec = Ior = -3 dB y pR = 0;

la figura 3 es un gráfico de rendimiento de FER frente a Ec/Ior con una variación de pT para un sistema MIMO 4x4, donde G = 10 dB y pR = 0;

la figura 4 es un gráfico de rendimiento de FER frente a Ec/Ior con una variación de pR para un sistema MIMO 4x4, donde G = 10 dB y pT = 0;

la figura 5 es un gráfico de rendimiento de FER frente a tasa de transmisión de código efectiva para un sistema MIMO 4x4, donde G = 10 dB, Ec = Ior = -3 dB y pR = 0;

la figura 6 es un diagrama de flujo de un procedimiento de transmisión de información en un sistema de múltiples entradas-múltiples salidas; y

la figura 7 es un diagrama de flujo de un procedimiento de recepción de información en un sistema de múltiples entradas-múltiples salidas.

DESCRIPCIÓN DETALLADA

En una realización, palabras de código de flujos de datos paralelos que se transmiten a través de múltiples antenas en un canal inalámbrico de múltiples entradas-múltiples salidas (MIMO) se procesan, encriptan o aleatorizan independientemente. Cuando los vectores de coeficientes de canal de dos o más flujos paralelos se vuelven próximos o correlacionados, esta encriptación de palabras de código convierte posiblemente palabras de código competidoras de flujos interferentes en palabras aleatorias inválidas desde el punto de vista del decodificador del flujo deseado. Como se explica adicionalmente a continuación, la encriptación de palabras de código también proporciona una reducción de la varianza de la interferencia efectiva cuando la tasa de transmisión de código es lo suficientemente baja como para utilizar adaptación de tasa de repetición tras una codificación de canal de referencia. La encriptación mejora el rendimiento de decodificación, especialmente cuando el canal MIMO está muy correlacionado en el lado del transmisor o cuando la tasa de repetición es alta.

La figura 1A y la figura 1B son diagramas de bloques simplificados de sistemas 100, 101 CDMA de múltiples códigos MIMO basados en codificación individual. Aunque lo que se

explica en el presente documento se refiere principalmente a un sistema CDMA de múltiples códigos, debe entenderse que la explicación completa y los resultados de rendimiento también son aplicables a transceptores MIMO generales. Por ejemplo, eliminando los bloques funcionales del ensanchador y desensanchador en la figura 1A o la figura 1B, el sistema, aparato y procedimientos explicados en el presente documento son aplicables a sistemas de transmisión de banda estrecha, tal como el sistema global para comunicaciones móviles (GSM) y los sistemas de acceso múltiple por división de tiempo (TDMA).

En la realización ilustrada de la figura 1A, el sistema 100 MIMO incluye un transmisor 102 y un receptor 104. Se proporciona un total de M flujos 106 de bits fuente a un codificador 108. El codificador 108 proporciona la entrada a un adaptador 110 de tasa de transmisión. La salida del adaptador 110 de tasa de transmisión se dirige a un entrelazador 112, que proporciona la entrada a un encriptador 114. Un mapeador 116 está acoplado a las salidas del encriptador 114, y proporciona la entrada a un ensanchador 118. El mapeador agrupa bits de los flujos de bits en símbolos de transmisión para un tipo de modulación predeterminado. La salida del ensanchador 118 se dirige a antenas 120 de transmisión.

En una realización alternativa ilustrada en la figura 1B, el sistema 101 MIMO también incluye un transmisor 102 y un receptor 104. Un total de M flujos 106 de bits fuente se proporcionan a un codificador 108, y el codificador 108 proporciona la entrada a un adaptador 110 de tasa de transmisión, como en la realización de la figura 1A. Sin embargo, en la realización de la figura 1B, la salida del adaptador 110 de tasa de transmisión se proporciona al encriptador 114, que proporciona la entrada al entrelazador 112. La salida del entrelazador 112 se dirige al mapeador 116, que proporciona la entrada a un ensanchador 118. Como en la figura 1A, la salida del ensanchador 118 se dirige a antenas 120 de transmisión.

Cada uno de los bloques funcionales individuales en los diagramas de bloques de las figuras 1A-1C son ampliamente conocidos por los expertos en la técnica, y no se describen adicionalmente en detalle en el presente documento los detalles de su construcción y funcionalidad. Un codificador traduce un flujo de bits en un flujo de bits diferente, siendo el objeto habitual convertir el flujo de bits original en uno diferente que tenga características que son más deseables para la transmisión o el almacenamiento que las del flujo de bits original. Los codificadores pueden implementarse generalmente en software o hardware. En el lado de transmisión, el adaptador 110 de tasa de transmisión, el entrelazador 112 y el encriptador 114 forman juntos un circuito de procesamiento de flujos de bits que opera sobre el flujo de bits codificados procedente del codificador 108. La perforación y la repetición de flujos de bits para la adaptación de la tasa de transmisión es ampliamente conocida, al igual que la reorganización de flujos de bits mediante entrelazado en sistemas de transmisión. El diseño y

la función del encriptador también se conocen bien en una variedad de aplicaciones. Es un aspecto de la invención que el procesamiento de flujos de bits realizado entre el codificador y el mapeador se realice de diferente manera sobre cada uno de la pluralidad de flujos de bits que salen del codificador. La salida del entrelazador para cada flujo de bits es una serie de grupos de bits denominados en el presente documento palabras de código que dependen del contenido del flujo de bits de entrada del codificador. Dado que la salida del entrelazador contiene normalmente más bits que la entrada del codificador, no son posibles todas las salidas arbitrarias en todo momento. Según se usa en el presente documento, una palabra de código "válida" o palabra de código "legítima" es una palabra de código de salida que está dentro del conjunto de posibles palabras de código de salida que podrían producirse por los circuitos de procesamiento concatenados del codificador, adaptador de tasa de transmisión y entrelazador. Una palabra de código "inválida" es una palabra de código que está fuera de este conjunto.

Haciendo referencia de nuevo a la figura 1A, se emiten señales de comunicación desde las antenas 120 de transmisión, y las reciben antenas 122 de recepción de otro sistema 100 MIMO. Las antenas 122 de recepción están acopladas a un ecualizador 124 espaciotemporal, que proporciona la entrada a un desensanchador 126. El desensanchador 126 está acoplado a un desmapeador 128, que está acoplado a un desencriptador 130. El desencriptador 130 tiene salidas que están acopladas a un desentrelazador 132. El desentrelazador 132 está acoplado a un adaptador 134 de tasa de transmisión, que proporciona la entrada a un decodificador 136. La salida del decodificador 136 incluye M flujos 138 de bits decodificados, a los que se hace referencia en el presente documento como flujos de bits 0 a M-1.

En la realización de la figura 1B, se emiten señales de comunicación desde las antenas 120 de transmisión, y las reciben antenas 122 de recepción, como en la realización de la figura 1A. Las antenas 122 de recepción están acopladas a un ecualizador 124 espaciotemporal, que proporciona la entrada a un desensanchador 126. El desensanchador 126 está acoplado a un desmapeador 128, que está acoplado a un desentrelazador 132. El desentrelazador 132 tiene salidas que están acopladas a un desencriptador 130. El desencriptador 130 está acoplado a un adaptador 134 de tasa de transmisión, que proporciona la entrada a un decodificador 136. La salida del decodificador 136 incluye M flujos 138 de bits decodificados, a los que se hace referencia en el presente documento como flujos de bits 0 a M-1.

En cualquiera de los sistemas 100, 101 CDMA, los M flujos 106 de bits de información se codifican independientemente por los codificadores 108, se repiten o perforan por los adaptadores 110 de tasa de transmisión para adaptarlos a la tasa de transmisión de símbolos de transmisión, y se entrelazan por los entrelazadores 112 dentro del intervalo de trama. Cada secuencia de bits entrelazados se agrupa y mapea por los mapeadores 116 en la secuencia de

símbolos de transmisión o puntos de constelación dependiendo del tipo de modulación (por ejemplo, QPSK o 16QAM), se ensancha mediante el subconjunto común de códigos de Walsh disponibles y el código de encriptación de elementos de código específico del transmisor por los ensanchadores 118, y luego se transmite a través de cada antena 120 de transmisión. Aunque la tasa de errores de decodificación puede reducirse asignando diferentes subconjuntos de códigos de Walsh a las diferentes antenas 120 de transmisión siempre que estén disponibles, en esta realización el subconjunto común de códigos de Walsh se reutiliza para al menos una parte de múltiples antenas 120 de transmisión.

La potencia de transmisión total se divide y se asigna a cada antena 120 de transmisión. Los múltiples flujos transmitidos llegan a las N antenas 122 de recepción tras distorsionarse mediante un canal de desvanecimiento MIMO y un vector de ruido gaussiano blanco aditivo (AWGN). Se supone que N ≥ M y que el canal MIMO variable en el tiempo tiene una característica de desvanecimiento plano para mayor simplicidad, aunque puede ampliarse fácilmente a los casos de N < M y canales de desvanecimiento selectivo en frecuencia. La variación de canal es relativamente pequeña dentro de la duración de la trama de transmisión. El ecualizador 124 espaciotemporal genera las secuencias de elementos de código blandos de los M flujos de transmisión y el desensanchador 126 genera las correspondientes secuencias de símbolos blandos. Usando los símbolos blandos, el desmapeador 128 genera las secuencias de razón de probabilidad logarítmica de bit (LLR), que se alimentan a las cadenas individuales del desentrelazador 132, los adaptadores 134 de tasa de transmisión y el decodificador 136 para restaurar los múltiples flujos 106 fuente.

La matriz de canal de desvanecimiento N X M se denomina H ≡ [h0, h1,..., hM-1], el vector de símbolos de transmisión M X 1, x(k) ≡ [x0(k), x1(k),..., xM-1(k)]T, y el vector AWGN N X 1 obtenido tras el desensanchamiento (sin la multiplicación de coeficientes de ecualizador espaciotemporal), n(k) ≡ [n0(k), n1(k),..., nN-1(k)]T para el índice temporal de símbolo k. El vector hi es el vector de coeficientes de canal N X 1 asociado con el símbolo de transmisión xi(k). El símbolo blando de entrada del desmapeador yi(k) correspondiente al flujo de datos de orden 1 se representa como:

$$y_i(k) = w_i^H Hx(k) + w_i^H n(k) \quad (1)$$

$$= \sum_{j=0}^{M-1} w_i^H h_j x_j(k) + w_i^H n(k) \quad (2)$$

$$= \sum_{j=0}^{M-1} a_{ij} x_j(k) + v_i(k) \quad i = 0,1,\cdots,M-1 \quad (3)$$

donde el vector N X 1 w_i indica el vector de coeficientes de ponderación de orden i del ecualizador espaciotemporal, $a_{ij} \equiv w_i^H h_j$ y $v_i(k) \equiv w_i^H n(k)$. Usando un ecualizador espaciotemporal de relación señal a ruido de interferencia (MSINR) máxima lineal, el vector de ponderación de orden i adopta el valor de:

$$w_i = [\sum_{j=0, j\neq i}^{M-1} E_s h_j h_j^H + N_o I]^{-1} h_i \qquad (4)$$

para la energía de símbolo de modulación promedio E_s y la varianza de ruido N_o, y la SNR de símbolo resultante se convierte en:

$$SINR_i = E_s h_i^H [\sum_{j=0, j\neq i}^{M-1} E_s h_j h_j^H + N_o I]^{-1} h_i. \qquad (5)$$

Cuando el tamaño de la constelación es 2^B, el desmapeador 128 genera la LLR $\Lambda^l_i(k)$ del bit de orden i $b_i^l(k)$ (l = 0, 1,..., B-1) asociada con el símbolo blando observado $y_i(k)$ tomando

$$\Lambda_i^l(k) = \log \frac{p(b_i^l(k) = 0 | y_i(k))}{p(b_i^l(k) = 1 | y_i(k))} \qquad (6)$$

para la función de densidad de probabilidad condicional de α dado β, $p(\alpha|\beta)$. $\Lambda^l_i(k)$ se calcula con la suposición de una probabilidad igual a priori para cada punto de la constelación y a través de una aproximación gaussiana de las componentes de ruido e interferencia de $y_i(k)$.

Los expertos en la técnica apreciarán que lo anterior puede aplicarse a una variedad de sistemas de comunicación, incluyendo un sistema de acceso múltiple por división de frecuencia ortogonal (OFDM), como el sistema 103 OFDM ilustrado en la figura 1C. El sistema 103 OFDM incluye un transmisor 102 y un receptor 104. El receptor 102 del sistema 103 OFDM ilustrado incluye muchos de los mismos componentes de un sistema CDMA, como los sistemas 100, 101 CDMA descritos anteriormente. Por ejemplo, un sistema 103 OFDM incluye M flujos 106 de bits fuente que se proporcionan a un codificador 108. La salida del codificador 108 se dirige a un adaptador 110 de tasa de transmisión, que está acoplado a la entrada de un entrelazador 112. La salida del entrelazador 112 se dirige a un encriptador 114, que está acoplado a la entrada de un mapeador 116. Se apreciará que en esta realización de OFDM, el encriptador puede situarse entre el adaptador de tasa de transmisión y el entrelazador en el transmisor y entre el desentrelazador y el adaptador de tasa de transmisión en el receptor, según se muestra en la realización de CDMA de la figura 1B.

Sin embargo, en el sistema 103 OFDM, la salida del mapeador 116 se dirige a un asignador 140 de subportadora, que recibe un subconjunto asignado de subportadoras. La salida del asignador 140 de subportadora está acoplada a la entrada de un transformador 142 de Fourier discreto inverso (IDFT). El IDFT 142 está acoplado a un insertador 144 de prefijo cíclico, que tiene salidas acopladas a m antenas 120 de transmisión.

El sistema 103 OFDM recibe información con M antenas 122, que están acopladas a la entrada de un eliminador 146 de prefijo cíclico. La salida del eliminador 146 de prefijo cíclico está acoplada a un transformador 148 de Fourier discreto, que está acoplado a un ecualizador 150 espacial. La salida del ecualizador 150 espacial está acoplada a un selector 152 de subportadora, que recibe un conjunto asignado de subportadoras. La salida del selector 152 de subportadora está acoplada a un desmapeador 128, desencriptador 130, desentrelazador 132, adaptador 132 de tasa de transmisión y decodificador 136, como en cualquiera de las realizaciones 100, 101 de sistema CDMA, descritas anteriormente.

Los encriptadores y desencriptadores de las figuras 1A-1C mejoran el rendimiento de decodificación cuando se ve afectado adversamente por la correlación entre los vectores columna o fila de la matriz de canal instantánea.

Se produce interferencia degenerativa cuando la tasa de transmisión de datos de los dos primeros flujos es igual y los dos primeros vectores columna de la matriz de canal son próximos entre sí, por ejemplo, h0 ≈ h1. Cuando se decodifica el primer flujo {x0(k)}, el símbolo blando de entrada del desmapeador correspondiente al primer flujo se convierte en:

$$y_0(k) \approx a_{00}[x_0(k) + x_1(k)] + \sum_{j=2}^{M-1} a_{0j} x_j(k) + v_0(k). \qquad (7)$$

El decodificador 136 de canal del primer flujo calcula la métrica de trayectoria de las palabras de código candidatas legítimas (tras el desentrelazado y la adaptación de tasa de transmisión) acumulando los valores de LRR de bit generados basándose en la secuencia de observación {y0(k)}, y los compara para determinar los bits de información transmitidos del primer flujo. Como la secuencia de bits codificados (y adaptados en cuanto a la tasa de transmisión y entrelazados) del segundo flujo {x1(k)} también es una de las palabras de código candidatas legítimas para la decodificación del primer flujo y proporciona un valor de métrica de trayectoria comparable, el decodificador del primer flujo podría realizar una detección de secuencia incorrecta, al menos con una probabilidad de 0,5. Es decir, el decodificador 136 para el primer flujo podría decodificar el segundo flujo en vez del primer flujo cuando los vectores columna de canal correspondientes son próximos. Si más de dos vectores de coeficientes de canal están muy correlacionados, la probabilidad de detección de secuencia errónea

aumentaría adicionalmente. Es probable que el transmisor 102 seleccione la misma tasa de transmisión o formato de transmisión para los flujos primero y segundo, incluso cuando el transmisor 102 ajusta adaptativamente la tasa de transmisión de datos de cada flujo dependiendo del estado del canal, puesto que la SINR de realimentación notificada desde el receptor es casi la misma para los dos flujos cuando los dos vectores de coeficientes de canal son relativamente próximos.

La selección del mismo formato de transmisión para los dos flujos legitima desafortunadamente la secuencia de bits codificados del segundo flujo como palabra de código candidata competidora al decodificar el primer flujo, y viceversa. Si el receptor 104 transmite la información de correlación de los vectores de coeficientes de canal así como la SINR de cada flujo al transmisor 102, pueden activarse y desactivarse selectivamente flujos para evitar esta colisión. Sin embargo, hacer eso aumentará la cantidad de información de realimentación y experimentará retardo de medición y realimentación.

El problema de la competencia de palabras de código se produce con más frecuencia cuando las antenas 120 de transmisión están más correlacionadas, ya que aumentará la probabilidad de que múltiples vectores columna de la matriz de canal se vuelvan próximos instantáneamente. Con el fin de impedir la competencia de palabras de código entre múltiples flujos cuando los vectores columna de canal están instantáneamente próximos, en una realización, como la ilustrada en la figura 1, se proporciona una operación de O-exclusivo (XOR) entre la secuencia de encriptación pseudoaleatoria (PN) binaria de orden i {si(n)} y la secuencia de bits codificados de orden i {ci(n)} en la salida del entrelazador 112 en el lado del transmisor, donde n indica el índice temporal de la secuencia de bits codificados, adaptados en cuanto a la tasa de transmisión y entrelazados. Usando las notaciones k,1, B, y $b^{l}_{i}(k)$ de la ec. (6), entonces las relaciones n = kB + 1 y $b^{l}_{i}(k)$ =ci(n) $\oplus$ si(n), donde $\oplus$ indica la operación de O-exclusivo entre valores binarios.

Las secuencias de encriptación para los múltiples flujos son de manera ventajosa independientes entre sí. En el lado receptor, la secuencia de LLR de bit del flujo de orden i se multiplica por la secuencia de desencriptación de valores reales de orden i {1 - 2si(n)}, para deshacer el efecto de la secuencia de encriptación de orden i. Usando las secuencias de encriptación independientes para los flujos paralelos, la palabra de código competidora que proviene del flujo de interferencia cuyo vector de coeficientes de canal es próximo al del flujo deseado, por lo general se transforma en una palabra aleatoria a través del proceso de encriptación y desencriptación. Por tanto, el decodificador 136 del flujo deseado (por ejemplo, {x0(k)} en la ec. (7)) no seleccionará la palabra de código del flujo de interferencia (por ejemplo, {x1(k)} en la ec. (7)). Como la tasa de transmisión de código efectiva definida por la razón del

número de bits de información con respecto al número de bits codificados, adaptados en cuanto a la tasa de transmisión y entrelazados se vuelve menor, la probabilidad de que la palabra aleatoria resultante sea una palabra de código legítima o esté próxima a una palabra de código se vuelve menor. Las figuras 1A-1C muestran el encriptador 114 de bits codificados CBS en el transmisor 102 y el desencriptador 130 correspondiente en el receptor 104.

Existe una variedad de variaciones de implementación para lograr un efecto similar, incluyendo el uso de patrones de entrelazador de canal a nivel de bit distintos para flujos paralelos, o pueden usarse patrones de perforación y repetición distintos en la adaptación de la tasa de transmisión para los flujos paralelos. En estas realizaciones, no se requiere necesariamente un encriptador separado.

El encriptador 114 proporciona otro beneficio para la transmisión de múltiples flujos en canales MIMO cuasiestáticos. Dependiendo de la tasa de transmisión de código efectiva, el adaptador 110 de tasa de transmisión repite o perfora los bits de salida del codificador 108 de canal. El encriptador 114 aplicado a la salida del entrelazador 112 o el adaptador 110 de tasa de transmisión produce una mejora significativa de la SINR de palabra de código cuando se produce la adaptación de tasa de repetición. Por ejemplo, si la tasa de transmisión de código del codificador 108 de canal de referencia es de 1/3 y sucede que la tasa de transmisión de código efectiva es de 1/6 para el primer flujo y el segundo flujo, el adaptador 110 de tasa de transmisión repite los bits de salida del codificador 108 de los dos flujos 106 una vez más.

Cuando el decodificador 136 de canal (combinado con el adaptador 134 de tasa de transmisión) del primer flujo acumula una métrica de ramificación para generar la métrica de trayectoria de las palabras de código candidatas, las componentes de interferencia correspondientes a los pares de bits repetidos del segundo flujo se acumulan con sus fases alineadas. Mediante la encriptación independiente de las secuencias de bits adaptados en cuanto a la tasa de transmisión, las componentes de interferencia repetidas se acumulan con sus fases aleatorizadas cuando se acumulan coherentemente las componentes de señal repetidas, y por tanto, las varianzas de interferencia de la métrica de trayectoria se reducen. Esta reducción de las varianzas de interferencia es efectiva en la mayoría de realizaciones de canal a menos que los vectores columna de canal sean perfectamente ortogonales.

Con el fin de evaluar la ganancia a partir de la encriptación de bits codificados (CBS) en el sistema 100 MIMO, el rendimiento global de enlace y la tasa de errores de trama (FER) del sistema WCDMA HSDPA de tasa de transmisión de datos fija se compararon con múltiples antenas y un ecualizador espaciotemporal de MSINR lineal. En HSDPA, los flujos de datos se ensanchan mediante múltiples códigos de Walsh cuyo factor de ensanchamiento es de 16 (a la tasa de transmisión de elementos de código de 3,84 Mcps) y el número máximo de códigos de

Walsh disponible para la transmisión de datos es de 15. Las simulaciones siguientes reutilizaron un subconjunto fijo de los códigos de Walsh disponibles para transmitir múltiples flujos. Se usó un turbocodificador con la tasa de transmisión de código de referencia de 1/3 y se aplicó adaptación de tasa de transmisión, entrelazado y mapeo de constelación. El número de símbolos de modulación transmitidos por código de Walsh en una trama era de 480 y la duración de trama de 2 ms (7680 elementos de código). Para el canal MIMO, el canal de desvanecimiento de Rayleigh correlacionado H(t) se genera, por ejemplo, mediante:

$$H(t) = C_R^{1/2} H_0(t) C_T^{1/2} \qquad (8)$$

donde $\mathbf{C}_R$ y $\mathbf{C}_T$ son las matrices de correlación de las antenas de transmisión y recepción cuyos elementos diagonales son iguales a 1,0 y los elementos de $\mathbf{H}_o(t)$ son procesos aleatorios gaussianos complejos independientes, siendo t el índice temporal. Para mayor simplicidad, los elementos fuera de la diagonal de $\mathbf{C}_R$ y $\mathbf{C}_T$ se fijaron a los coeficientes de correlación reales ρ_R y ρ_T que oscilaban desde 0,0 hasta 1,0. Las simulaciones usan un proceso de desvanecimiento de Rayleigh de trayectoria única de 30 kn/h para cada elemento de $\mathbf{H}_o(t)$ con la frecuencia portadora de 2 GHz y suponían la estimación de varianza de ruido y canal perfecto para el ecualizador espaciotemporal.

La figura 2 es un gráfico del rendimiento global de enlace de los sistemas MIMO con dos antenas de transmisión y dos de recepción para las constelaciones de QPSK y 16QAM. En la figura 2, 16QAM-CBS o QPSK-CBS indica el caso en el que se aplicó la CBS a los flujos de transmisión paralelos. Cada flujo de antena se transmitió a una tasa de transmisión fija de 1.250 bits fuente por trama para la QPSK (por ejemplo, tasa global objetivo de 1,25 Mbps) y 2.500 bits fuente por trama para la 16QAM (por ejemplo, tasa global objetivo de 2,5 Mbps). El número de códigos de Walsh asignados fue de 4 y por tanto, la tasa de transmisión de código efectiva es de aproximadamente 1/3 para ambas constelaciones, lo que es igual a la tasa de transmisión de código de referencia del tubocodificador. La solicitud de repetición híbrida automática (HARQ) se basó en una combinación de *Chase* de un máximo de 4 retransmisiones. La simulación entrelazó 6 procesos HARQ independientes de tipo parada y espera a lo largo del tiempo, siendo el intervalo de tiempo de transmisión de cada proceso de 6 tramas (por ejemplo, utilización de canal del 100%). La parte de potencia de transmisión asignada al tráfico de datos Ec/lor se fijó en el 50% (por ejemplo, -3 dB) de la potencia de transmisión total y el valor de geometría G definido por la razón de la potencia de señal recibida total con respecto a la potencia AWGN total se fijó en 0 dB para la QPSK y 10 dB para la 16QAM, respectivamente. La figura 2 muestra el rendimiento global total sumado sobre los dos flujos de transmisión variando pT desde 0 hasta 1, siendo pR 0. Cuando pT llega a ser mayor que 0,7, la CBS

mejora el rendimiento global sustancialmente. Cuando pT es 1,0, un sistema MIMO 16QAM convencional no puede comunicarse, pero el sistema basado en CBS todavía puede transportar una cantidad sustancial de información. La ganancia de rendimiento global del sistema basado en CBS se origina a partir del efecto de la reducción de la varianza de interferencia durante la combinación de *Chase*, así como porque se evita la competencia de palabras de código entre flujos.

Las figuras 3-4 comparan la FER de los sistemas MIMO con cuatro antenas de transmisión y cuatro de recepción a medida que se varía Ec/Ior. El valor de geometría G se fija en 10 dB. En la figura 3, se cambia pT mientras pR se mantiene en 0. En la figura 4, se cambia pR mientras pT se mantiene en 0. Cada uno de los cuatro flujos de antena transmiten de manera continua a una tasa fija de 1.250 bits fuente por trama (por ejemplo, una tasa global objetivo de 2,5 Mbps) usando la constelación de QPSK. El número de códigos de Walsh asignados es de 8 y, por tanto, la tasa de transmisión de código efectiva es de aproximadamente 1/6. Como resultado, el bloque de adaptación de tasa de transmisión repite la mayoría de los bits de salida del codificador dos veces. Debido a la capacidad de reducción de la varianza de interferencia entre flujos, la CBS puede mejorar enormemente la FER incluso cuando pT y pR son iguales a 0. La mejora se vuelve mayor cuando pT aumenta pero no cambia tanto cuando aumenta pR. El efecto asimétrico de la CBS sobre las correlaciones de transmisor y receptor puede explicare en parte porque el problema de competencia de palabras de código se produce en el caso de la correlación del transmisor.

La figura 5 muestra la FER de los mismos sistemas MIMO investigados en la figura 3, pero con Ec/Ior fijado en -3 dB, G en 10 dB y el número de códigos de Walsh asignados se cambia desde 2 hasta 8 de modo que la tasa de transmisión de código efectiva oscila desde aproximadamente 2/3 hasta aproximadamente 1/6. Como la tasa de transmisión de código de referencia del turbocodificador es de 1/3, el bloque de adaptación de tasa de transmisión lleva a cabo la repetición y perforación cuando la tasa de transmisión de código es menor y mayor que 1/3, respectivamente. Debido a la capacidad de reducción de la varianza de interferencia, la CBS provoca ganancias significativas a medida que aumenta la tasa de repetición. En tales casos, disminuye la tasa de transmisión de código efectiva.

Según se explicó anteriormente, existen posibles problemas en un sistema de transmisión MIMO multiplexado espacialmente y codificado independientemente cuando los vectores columna de canal se vuelven próximos. El caso extremo de que dos o más flujos tengan casi los mismos vectores columna de canal instantáneos es poco probable que se produzca en el canal práctico, pero provoca un problema de competencia de palabras de código en los sistemas MIMO multiplexados espacialmente una vez que se produce. Se aplica

encriptación independiente a la secuencia de bits codificados y adaptados en cuanto a la tasa de transmisión de uno o más flujos de transmisión para reducir el problema. La encriptación de bits codificados reduce la varianza efectiva de la interferencia entre flujos en cuanto a la calidad de la métrica de trayectoria de decodificación cuando la tasa de transmisión de código efectiva se vuelve menor que la tasa de transmisión de código del codificador de canal de referencia. La mejora del rendimiento a través de la encriptación puede lograrse también en sistemas MIMO basados en control de tasa de transmisión de código adaptativo.

La figura 6 es un diagrama de flujo de un procedimiento 600 de transmisión de información en un sistema de múltiples entradas-múltiples salidas. En el bloque 602, se procesan flujos de bits para generar secuencias de bits codificados. En el bloque 604, se generan secuencias de encriptación, donde diferentes flujos generan diferentes secuencias de encriptación. En el bloque 606, se encriptan secuencias de bits codificados para generar secuencias de bits encriptados. En el bloque 608, se procesan los flujos de bits encriptados para generar secuencias de bits de transmisión. Finalmente, en el bloque 610, se transmiten los flujos de bits de transmisión.

La figura 7 es un diagrama de flujo de un procedimiento 700 de recepción de información en un sistema de múltiples entradas-múltiples salidas. En el bloque 702, se reciben flujos de bits de información. En el bloque 704, se procesan los flujos de bits de información para generar secuencias de razón de probabilidad logarítmica de bit. En el bloque 706, se desencriptan las secuencias de razón de probabilidad logarítmica de bit para generar flujos de bits blandos desencriptados. Finalmente, en el bloque 708, se procesan los flujos de bits blandos desencriptados para generar flujos de bits decodificados.

Los expertos en la técnica entenderán que la información y las señales pueden representarse usando una variedad de diferentes tecnologías y técnicas. Por ejemplo, datos, instrucciones, órdenes, información, señales, bits, símbolos y elementos de código a los que puede hacerse referencia a lo largo de la descripción anterior, pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, partículas o campos magnéticos, partículas o campos ópticos, o cualquier combinación de los mismos.

Los expertos en la técnica también apreciarán que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con las realizaciones dadas a conocer en el presente documento pueden implementarse como hardware electrónico, software informático, o combinaciones de ambos. Para ilustrar esta intercambiabilidad de hardware y software, se han descrito anteriormente diversos componentes, bloques, módulos, circuitos y etapas ilustrativos de forma general en cuanto a su funcionalidad. El que tal funcionalidad se implemente como hardware o software depende de las limitaciones de diseño

y aplicación particulares impuestas sobre el sistema global. Los expertos pueden implementar la funcionalidad descrita de diversas maneras para cada aplicación particular, pero tales decisiones de implementación no deben interpretarse como que provocan un alejamiento del alcance de la presente invención.

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con las realizaciones dadas a conocer en el presente documento pueden implementarse o realizarse con un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado de aplicación específica (ASIC), una disposición de puertas programables en campo (FPGA) u otro dispositivo lógico programable, puerta discreta o lógica de transistor, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador, pero como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos de cálculo, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP, o cualquier otra configuración de este tipo.

Las etapas de un procedimiento o algoritmo descrito en relación con las realizaciones dadas a conocer en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador, o en una combinación de ambos. Un módulo de software puede residir en una memoria RAM, memoria *flash*, memoria ROM, memoria EPROM, memoria EEPROM, registros, disco duro, un disco extraíble, un CD-ROM, u otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento está acoplado al procesador, de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. El procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

La descripción anterior de las realizaciones dadas a conocer se proporciona para permitir a un experto en la técnica realizar o utilizar la presente invención. Diversas modificaciones a estas realizaciones resultarán fácilmente evidentes para los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden aplicarse a otras realizaciones sin apartarse del espíritu o alcance de la invención. Por tanto, la presente invención no pretende limitarse a las realizaciones mostradas en el presente documento, sino que ha de concedérsele el alcance más amplio de manera consecuente con los principios y

características novedosas dados a conocer en el presente documento. Por tanto, la invención sólo está limitada por las reivindicaciones.

REIVINDICACIONES

1. Un aparato para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

un codificador (108) para codificar una pluralidad de flujos (106) de bits fuente para producir una pluralidad de flujos de bits codificados,

un procesador de flujos de bits para encriptar cada uno de dichos flujos de bits codificados con un encriptador (114) configurado de diferente manera para producir una pluralidad de flujos de bits encriptados de diferente manera, y

un mapeador (116) para mapear grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión,

en el que el procesador de flujos de bits comprende además un adaptador (110) de tasa de transmisión para adaptar la tasa de transmisión de los flujos de bits codificados.

2. El aparato según la reivindicación 1, en el que el procesador de flujos de bits comprende además un entrelazador (112) para entrelazar cada uno de dicha pluralidad de flujos (106) de bits codificados.

3. El aparato según la reivindicación 2, en el que el entrelazador (112) entrelaza los flujos de bits codificados antes de la encriptación de cada uno de los flujos (106) de bits codificados.

4. El aparato según la reivindicación 2, en el que el entrelazador (112) entrelaza cada uno de los flujos de bits encriptados.

5. El aparato según la reivindicación 1, en el que la encriptación realiza una operación de O-exclusivo entre diferentes secuencias de encriptación pseudoaleatoria y la pluralidad de flujos de bits codificados.

6. El aparato según la reivindicación 1, en el que dicho mapeador (116) mapea además grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión basándose en un tipo de modulación predeterminado para generar una pluralidad de flujos de símbolos.

7. El aparato según la reivindicación 6, en el que dicho tipo de modulación comprende modulación por desplazamiento de fase en cuadratura (QPSK).

8. El aparato según la reivindicación 6, en el que dicho tipo de modulación comprende modulación de amplitud en cuadratura (QAM).

9. El procedimiento según la reivindicación 6, que comprende además un ensanchador (118) para ensanchar la pluralidad de flujos de símbolos mapeados mediante un subconjunto común de códigos de Walsh para generar una pluralidad de señales

ensanchadas.

10. El aparato según la reivindicación 1, que comprende además: una pluralidad de antenas (120) para transmitir los símbolos sobre un medio de comunicación inalámbrica.

11. El aparato según la reivindicación 10, en el que dicha transmisión de los símbolos se produce sobre al menos uno de un sistema de acceso múltiple por división de código (CDMA) o de acceso múltiple por división de frecuencia ortogonal (OFDM).

12. Un aparato para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

un codificador (108) para codificar una pluralidad de flujos (106) de bits fuente para producir una pluralidad de flujos de bits codificados;

un procesador de flujos de bits para entrelazar cada uno de los flujos de bits codificados con un patrón de entrelazado diferente para producir una pluralidad de flujos de bits entrelazados de diferente manera; y

un mapeador (116) para mapear grupos de bits de dicha pluralidad de flujos de bits entrelazados de diferente manera en símbolos de transmisión;

en el que el procesador de flujos de bits comprende además un adaptador (110) de tasa de transmisión para adaptar la tasa de transmisión de los flujos de bits codificados.

13. Un aparato para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

un desmapeador (128) para traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos de bits recibidos;

un procesador de flujos de bits para aplicar un algoritmo de desencriptación diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desencriptados de diferente manera; y

un decodificador (136) para decodificar dichos de flujos de bits desencriptados de diferente manera para producir una pluralidad de flujos de bits decodificados

en el que el procesador de flujos de bits comprende además un adaptador (134) de tasa de transmisión para adaptar la tasa de transmisión de los flujos de bits recibidos.

14. El aparato según la reivindicación 13, en el que cada algoritmo de desencriptación elimina una secuencia de encriptación aplicada previamente.

15. El aparato según la reivindicación 13, que comprende además: un ecualizador (122) en espacio-tiempo para generar secuencias de elementos de código blandos de los símbolos recibidos; y un desensanchandor (126) para generar una pluralidad de secuencias de símbolos blandos.

16. El aparato según la reivindicación 15, en el que el desmapeador (128) genera además

una pluralidad de secuencias de razón de probabilidad logarítmica de bit (LLR) basadas al menos en parte en dicha pluralidad de secuencias de símbolos blandos.

17. El aparato según la reivindicación 13, en el que dicho procesador de flujos de bits multiplica el flujo de bits recibidos por una secuencia de desencriptación de valores reales que comprende {1 - 2si(n)}, en el que si(n)) comprende una secuencia de encriptación pseudoaleatoria binaria de orden i.

18. Un aparato para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

un desmapeador (128) para traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos de bits recibidos;

un procesador de flujos de bits para aplicar un patrón de desentrelazado diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desentrelazados de diferente manera; y

un decodificador (136) para decodificar dichos de flujos de bits desentrelazados de diferente manera para producir una pluralidad de flujos de bits decodificados,

en el que el procesador de flujos de bits comprende además un adaptador (134) de tasa de transmisión para adaptar la tasa de transmisión de los flujos de bits recibidos.

19. Un procedimiento para la transmisión de información en un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

codificar una pluralidad de flujos (106) de bits fuente para producir una pluralidad de flujos de bits codificados;

adaptar la tasa de trasmisión de los flujos de bits codificados;

encriptar cada uno de dichos flujos de bits codificados con un encriptador (114) configurado de diferente manera para producir una pluralidad de flujos de bits encriptados de diferente manera; y mapear grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión.

20. El procedimiento según la reivindicación 19, que comprende además el entrelazado de cada uno de dicha pluralidad de flujos de bits codificados.

21. El procedimiento según la reivindicación 20, en el que dicho entrelazado comprende entrelazar los flujos de bits codificados antes de la encriptación de cada uno de los flujos de bits codificados.

22. El procedimiento según la reivindicación 20, en el que el entrelazado comprende además entrelazar cada uno de los flujos de bits encriptados.

23. El procedimiento según la reivindicación 19, en el que la encriptación comprende realizar una operación de O-exclusivo entre diferentes secuencias de encriptación pseudoaleatoria y la pluralidad de flujos de bits codificados.

24. El procedimiento según la reivindicación 19, en el que dicho mapeado comprende mapear grupos de bits de dicha pluralidad de flujos de bits encriptados de diferente manera en símbolos de transmisión basándose en un tipo de modulación predeterminado para generar una pluralidad de flujos de símbolos.

25. El procedimiento según la reivindicación 24, en el que dicho tipo de modulación comprende modulación por desplazamiento de fase en cuadratura (QPSK).

26. El procedimiento según la reivindicación 24, en el que dicho tipo de modulación comprende modulación de amplitud en cuadratura (QAM).

27. El procedimiento según la reivindicación 24, que comprende además ensanchar la pluralidad de flujos de símbolos mapeados mediante un subconjunto común de códigos de Walsh para generar una pluralidad de señales ensanchadas.

28. El procedimiento según la reivindicación 29, que comprende además transmitir los símbolos sobre un medio de comunicación inalámbrica.

29. El procedimiento según la reivindicación 28, en el que la transmisión de los símbolos se produce sobre al menos uno de un sistema de acceso múltiple por división de código (CDMA) o de acceso múltiple por división de frecuencia ortogonal (OFDM).

30. Un procedimiento para la transmisión de información en un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

codificar una pluralidad de flujos (106) de bits fuente para producir una pluralidad de flujos de bits codificados;

adaptar la tasa de trasmisión de los flujos de bits codificados;

entrelazar cada uno de los flujos de bits codificados con un patrón de entrelazado diferente para producir una pluralidad de flujos de bits entrelazados de diferente manera; y

mapear grupos de bits de dicha pluralidad de flujos de bits entrelazados de diferente manera en símbolos de transmisión.

31. Un procedimiento para la recepción de información en un dispositivo de comunicación para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos de bits recibidos;

aplicar un algoritmo de desencriptación diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desencriptados de diferente manera;

adaptar la tasa de trasmisión de los flujos de bits desencriptados; y

decodificar dichos de flujos de bits desencriptados de diferente manera para producir una pluralidad de flujos de bits decodificados.

32. El procedimiento según la reivindicación 31, en el que cada algoritmo de desencriptación elimina una secuencia de encriptación aplicada previamente.

33. El procedimiento según la reivindicación 31, que comprende además: generar secuencias de elementos de código blandos de los símbolos recibidos; y generar una pluralidad de secuencias de símbolos blandos.

34. El procedimiento según la reivindicación 33, que comprende además generar una pluralidad de secuencias de razón de probabilidad logarítmica de bit (LLR) basadas al menos en parte en dicha pluralidad de secuencias de símbolos blandos.

35. El procedimiento según la reivindicación 31, que comprende además multiplicar el flujo de bits recibidos por una secuencia de desencriptación de valores reales que comprende {1 - 2si(n)}, en el que si(n)) comprende una secuencia de encriptación pseudoaleatoria binaria de orden i.

36. Un procedimiento para la recepción de información en un dispositivo de comunicación para un sistema de comunicación de múltiples flujos, de múltiples entradas-múltiples salidas, denominado MIMO, que comprende:

traducir símbolos recibidos en grupos de bits y producir una pluralidad de flujos de bits recibidos;

aplicar un patrón de desentrelazado diferente a cada flujo de bits recibidos para producir una pluralidad de flujos de bits desentrelazados de diferente manera;

adaptar la tasa de trasmisión de los flujos de bits desentrelazados; y

decodificar dichos de flujos de bits desentrelazados de diferente manera para producir una pluralidad de flujos de bits decodificados.

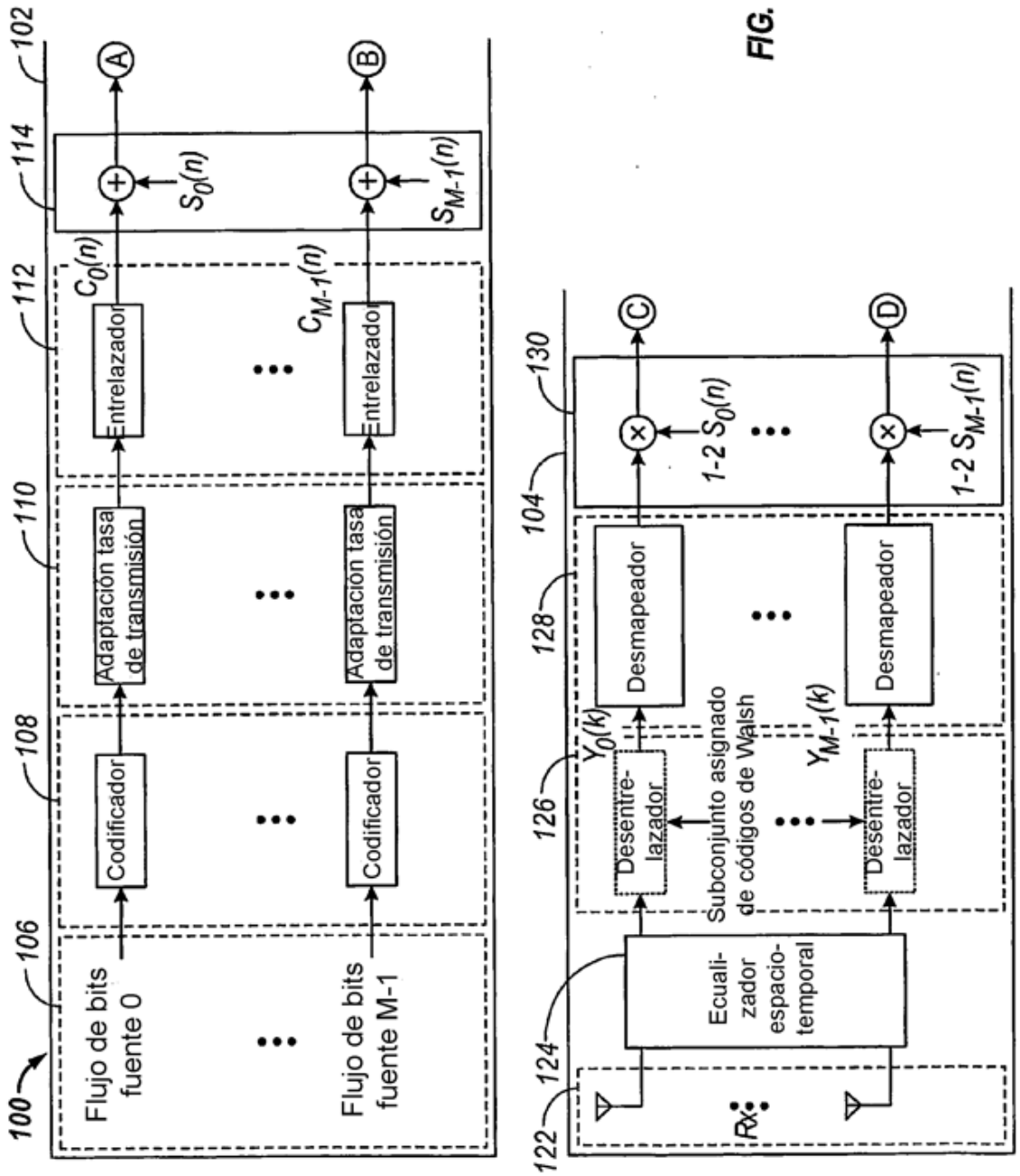
100
102
106
108
110
112
114
Flujo de bits fuente 0
Flujo de bits fuente M-1
Codificador
Adaptación tasa de transmisión
Entrelazador
$C_0(n)$
$C_{M-1}(n)$
$S_0(n)$
$S_{M-1}(n)$
A
B
122
124
126
128
130
104
Rx
Ecualizador espacio-temporal
Desentrelazador
Subconjunto asignado de códigos de Walsh
$Y_0(k)$
$Y_{M-1}(k)$
Desmapeador
1-2 $S_0(n)$
1-2 $S_{M-1}(n)$
C
D

FIG. 1A

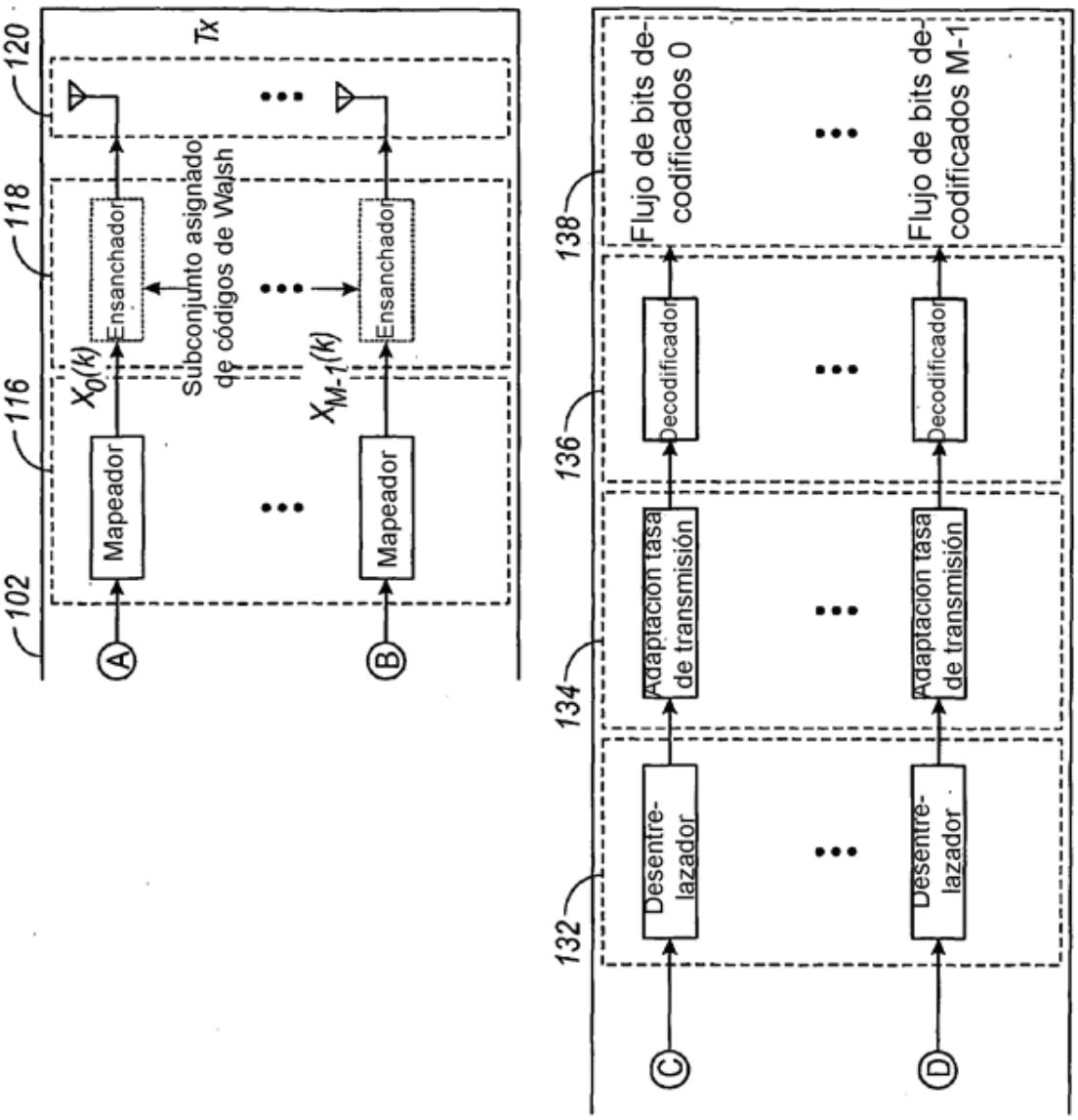
102
116
118
120
Tx
Mapeador
Mapeador
Ensanchador
Ensanchador
Subconjunto asignado de códigos de Walsh
$X_0(k)$
$X_{M-1}(k)$
A
B
132
134
136
138
Desentre-lazador
Desentre-lazador
Adaptacion tasa de transmisión
Adaptacion tasa de transmisión
Decodificador
Decodificador
Flujo de bits de-codificados 0
Flujo de bits de-codificados M-1
C
D

FIG. 1A
(cont.)

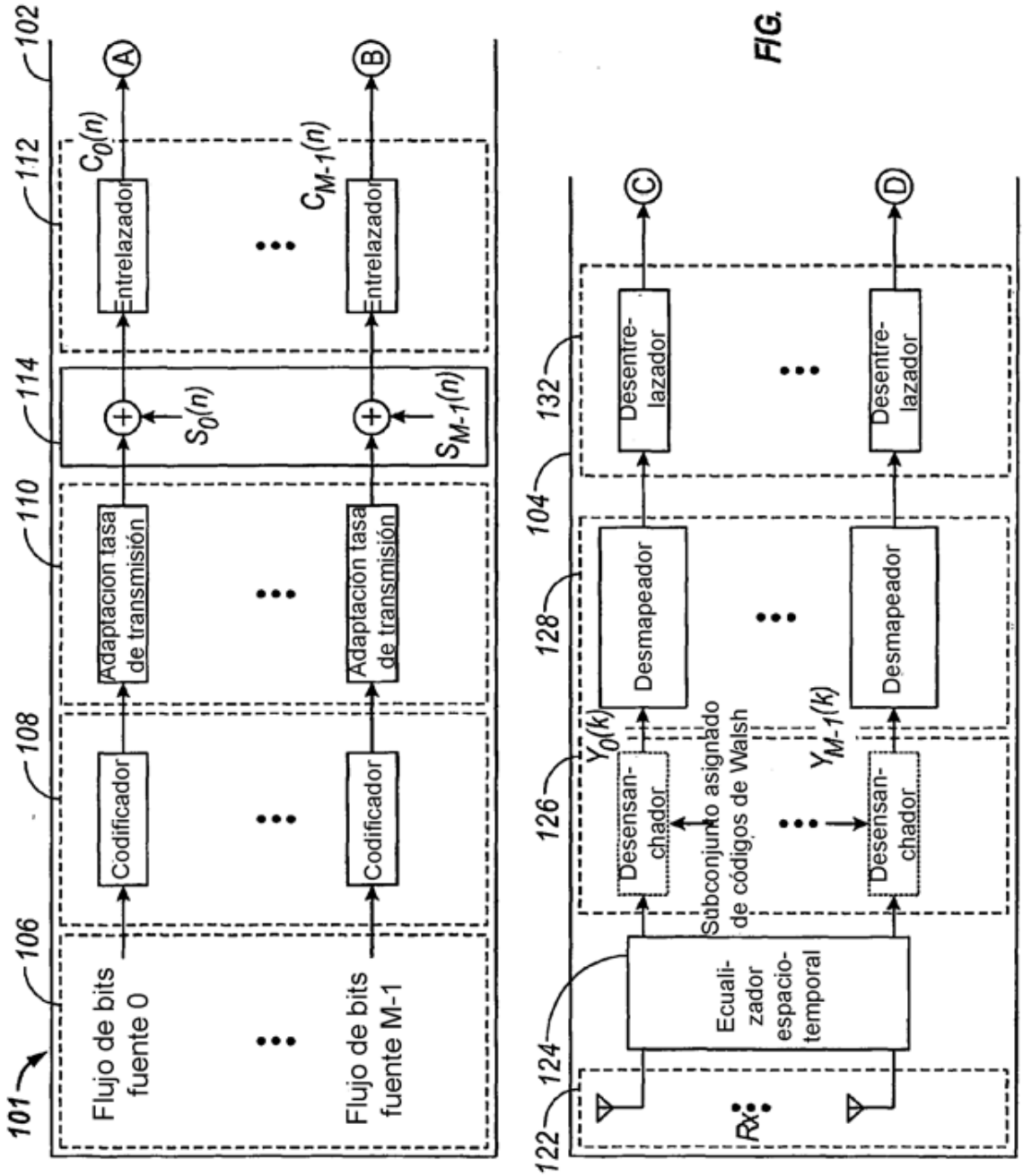
101
106
108
110
112
114
102
Flujo de bits fuente 0
Flujo de bits fuente M-1
Codificador
Adaptación tasa de transmisión
Entrelazador
$S_0(n)$
$S_{M-1}(n)$
$C_0(n)$
$C_{M-1}(n)$
A
B
122
124
126
128
104
132
Rx
Ecualizador espacio-temporal
Desensanchador
Subconjunto asignado de códigos de Walsh
$Y_0(k)$
$Y_{M-1}(k)$
Desmapeador
Desentrelazador
C
D

FIG. 1B

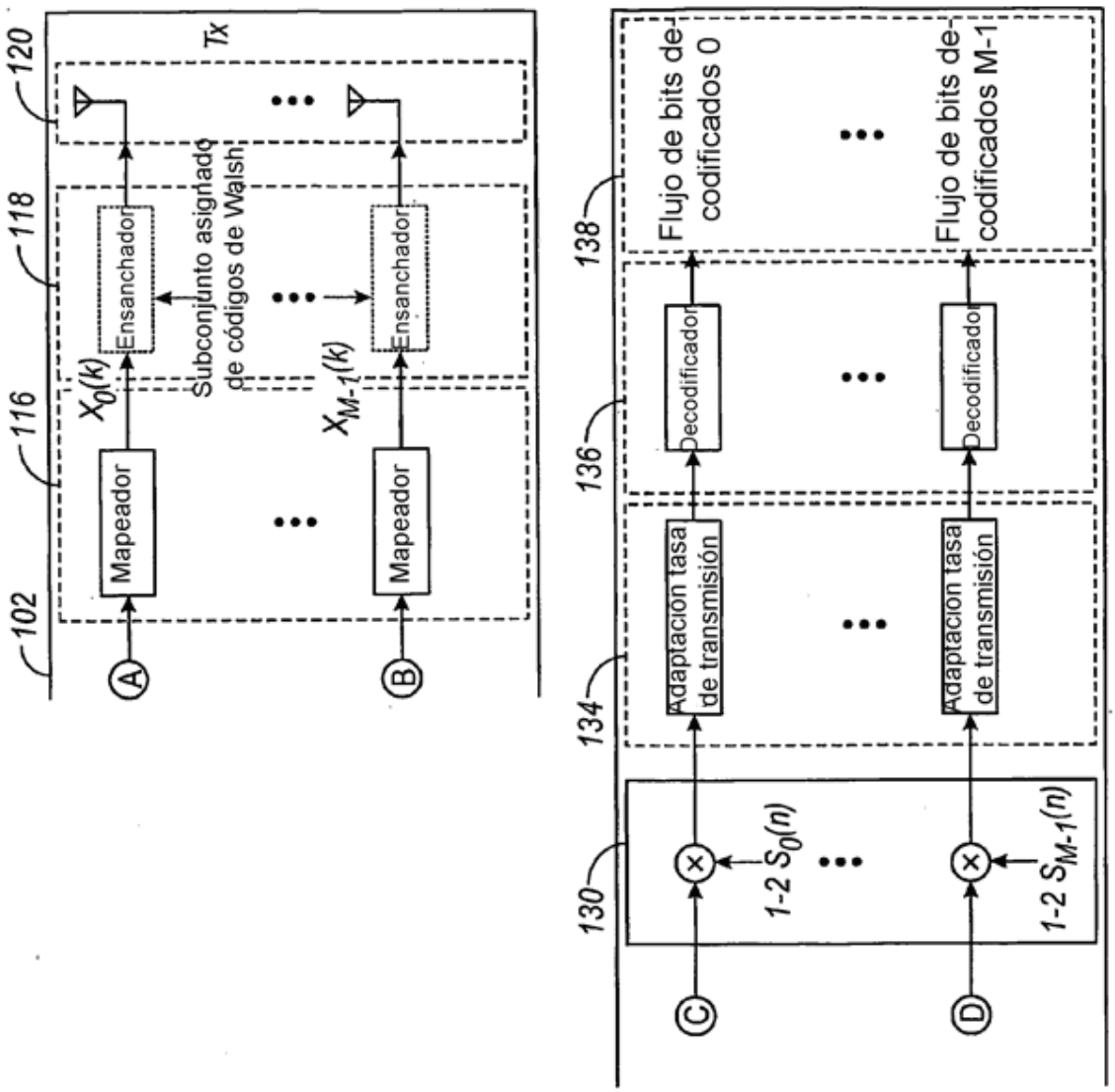
102
116
118
120
Tx
Mapeador
Mapeador
Ensanchador
Ensanchador
Subconjunto asignado de códigos de Walsh
$X_0(k)$
$X_{M-1}(k)$
A
B
130
134
136
138
1-2 $S_0(n)$
1-2 $S_{M-1}(n)$
Adaptación tasa de transmisión
Adaptación tasa de transmisión
Decodificador
Decodificador
Flujo de bits de codificados 0
Flujo de bits de codificados M-1
C
D

FIG. 1B
(cont.)

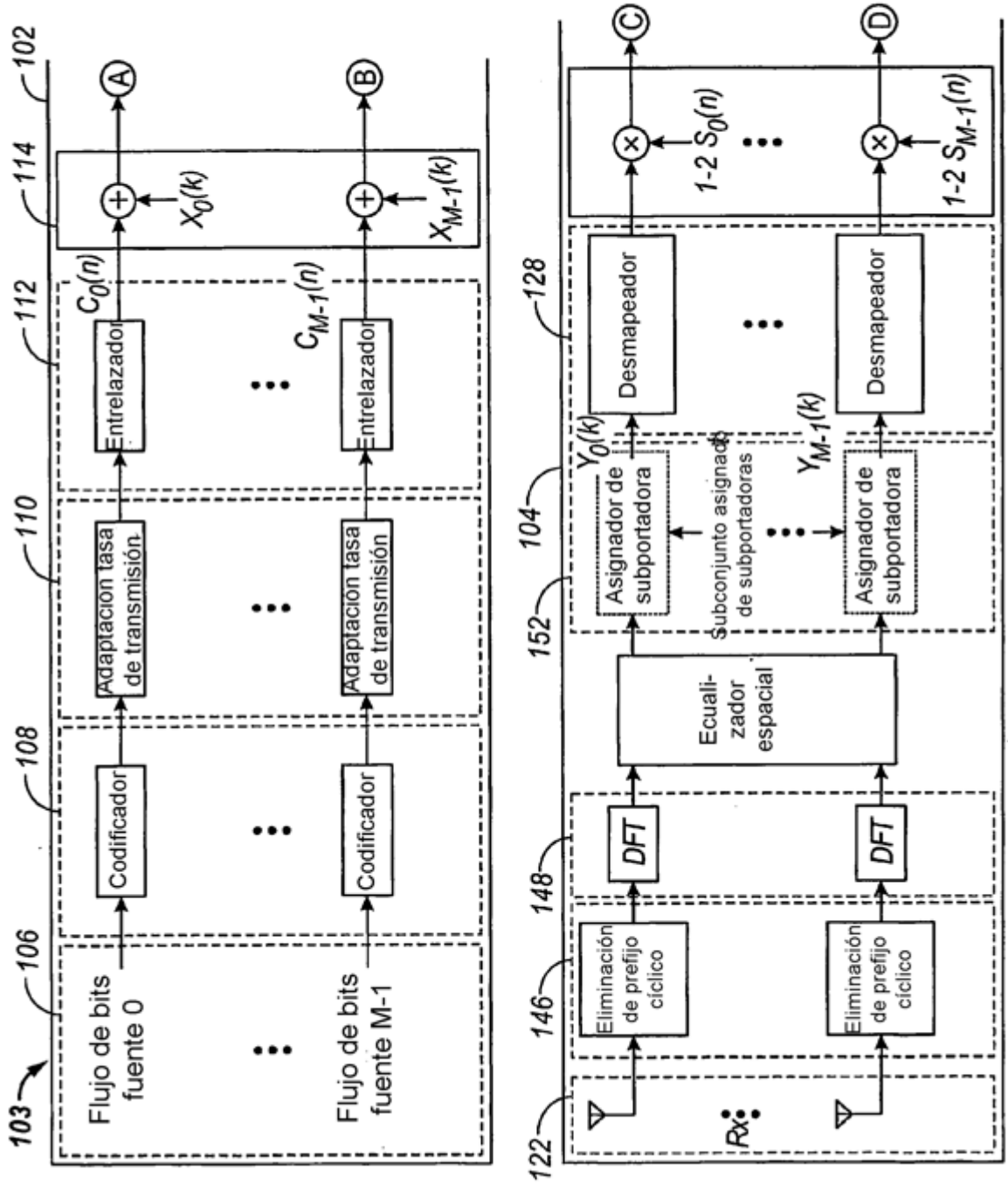
103
106
Flujo de bits fuente 0
Flujo de bits fuente M-1
108
Codificador
Codificador
110
Adaptación tasa de transmisión
Adaptación tasa de transmisión
112
Entrelazador
Entrelazador
$C_0(n)$
$C_{M-1}(n)$
114
$X_0(k)$
$X_{M-1}(k)$
A
B
102
122
Rx
146
Eliminación de prefijo cíclico
Eliminación de prefijo cíclico
148
DFT
DFT
Ecualizador espacial
152
104
Asignador de subportadora
Asignador de subportadora
Subconjunto asignado de subportadoras
$Y_0(k)$
$Y_{M-1}(k)$
128
Desmapeador
Desmapeador
1-2 $S_0(n)$
1-2 $S_{M-1}(n)$
C
D

FIG. 1C

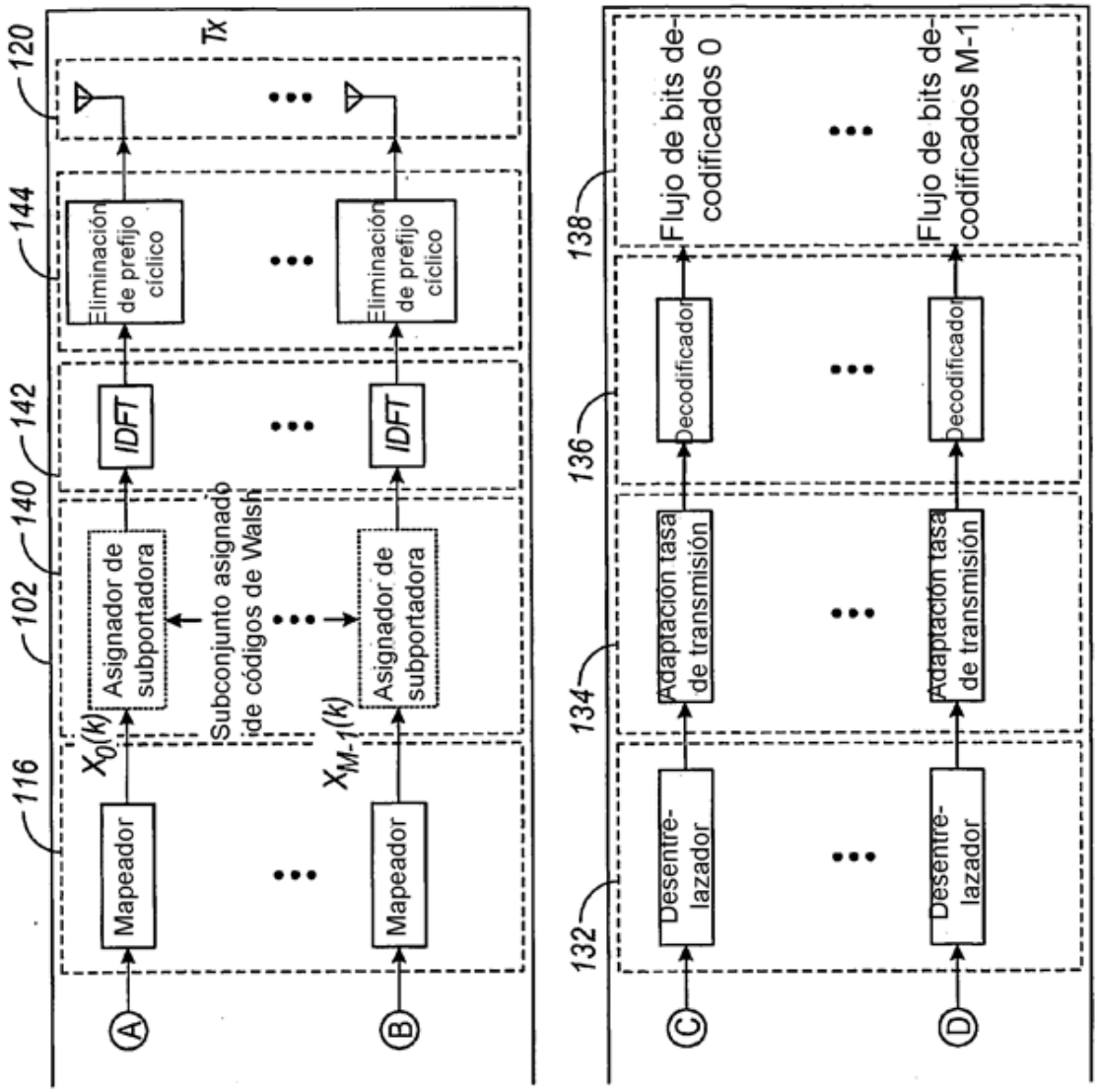
Tx
120
144
142
140
102
116
Eliminación de prefijo cíclico
IDFT
Asignador de subportadora
Subconjunto asignado de códigos de Walsh
Mapeador
$X_0(k)$
$X_{M-1}(k)$
A
B
138
136
134
132
Flujo de bits de-codificados 0
Flujo de bits de-codificados M-1
Decodificador
Adaptación tasa de transmisión
Desentre-lazador
C
D

FIG. 1C
(cont.)

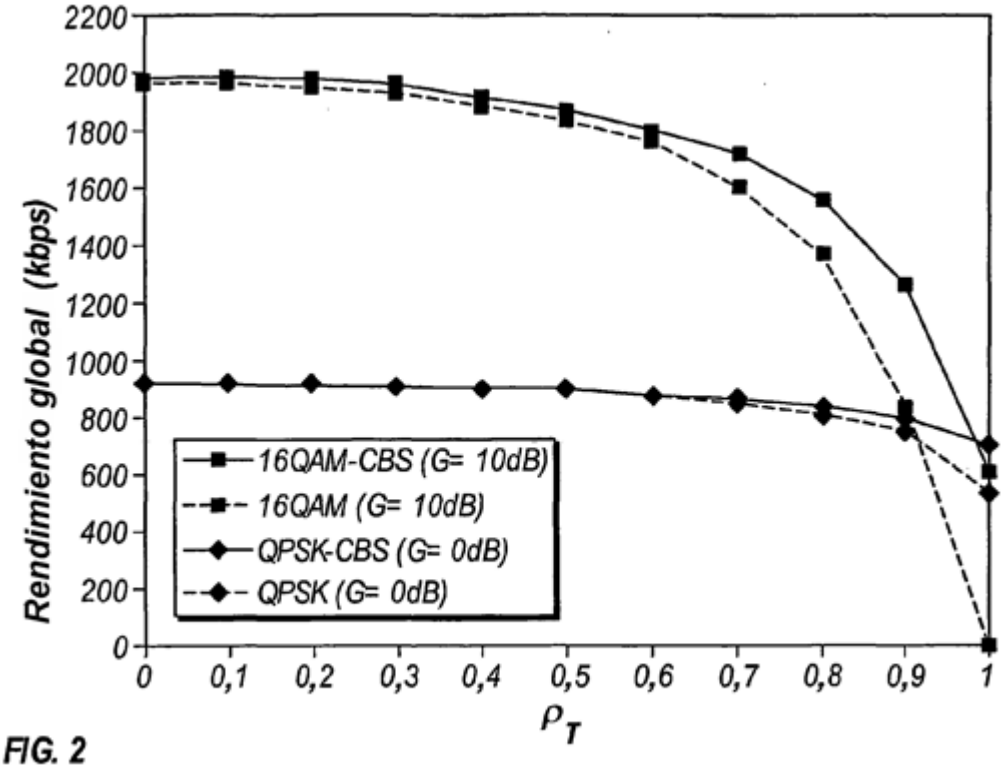
Rendimiento global (kbps)
2200
2000
1800
1600
1400
1200
1000
800
600
400
200
0
0
0,1
0,2
0,3
0,4
0,5
0,6
0,7
0,8
0,9
1
ρ_T
16QAM-CBS (G= 10dB)
16QAM (G= 10dB)
QPSK-CBS (G= 0dB)
QPSK (G= 0dB)

FIG. 2

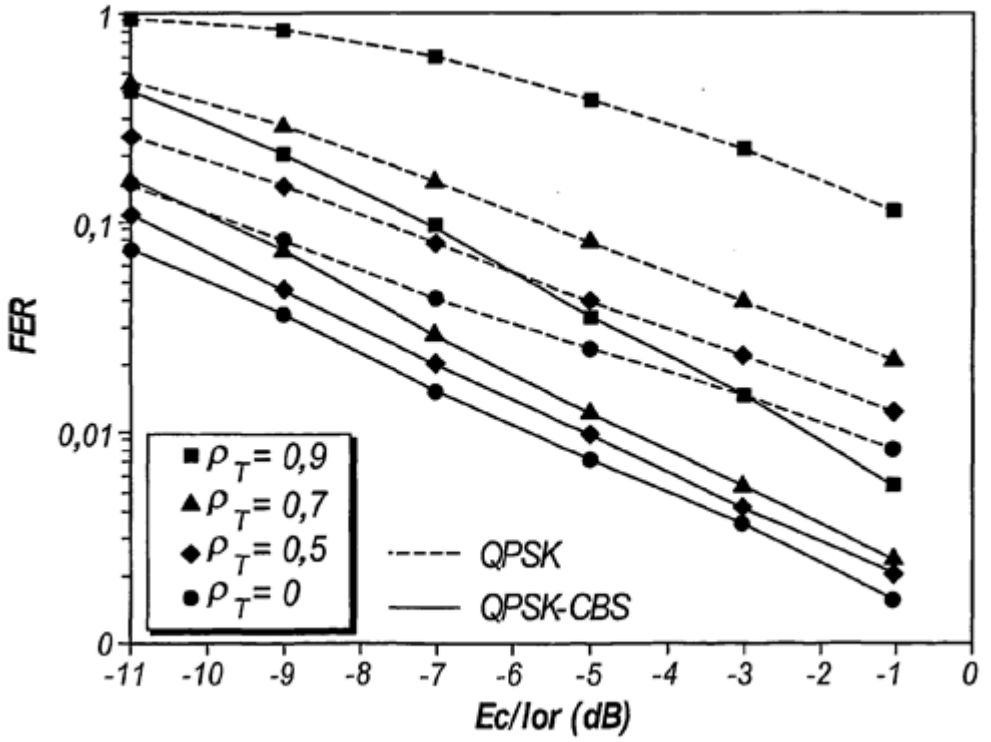
FER
1
0,1
0,01
0
-11
-10
-9
-8
-7
-6
-5
-4
-3
-2
-1
0
Ec/Ior (dB)
ρ_T= 0,9
ρ_T= 0,7
ρ_T= 0,5
ρ_T= 0
QPSK
QPSK-CBS

FIG. 3

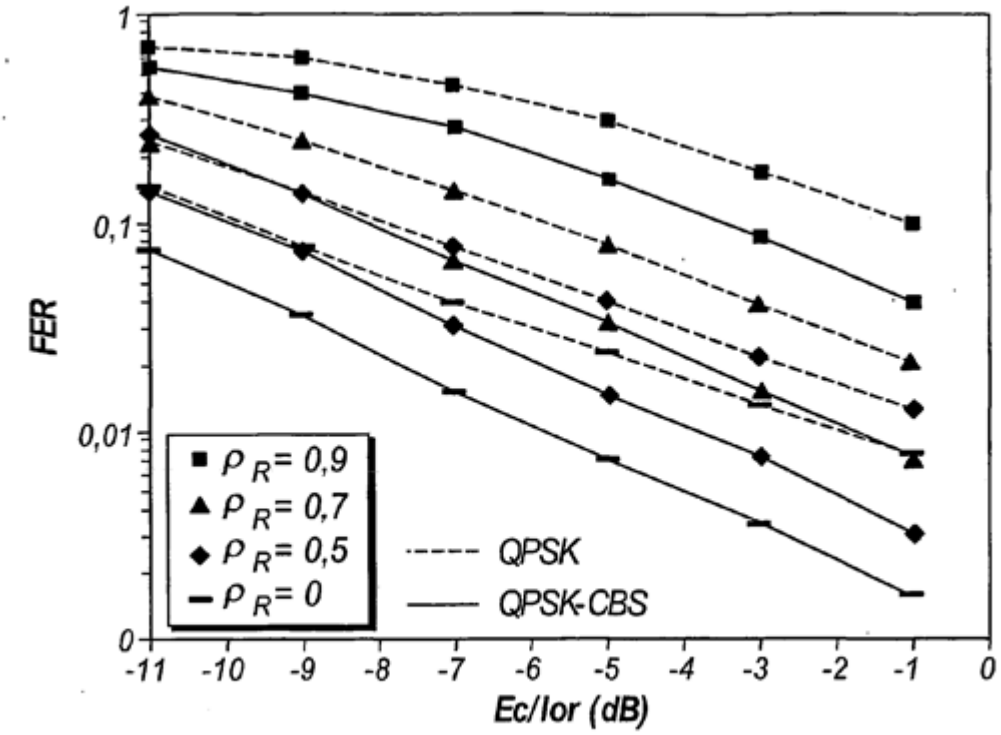
1
0,1
0,01
0
FER
ρ R= 0,9
ρ R= 0,7
ρ R= 0,5
ρ R= 0
QPSK
QPSK-CBS
-11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0
Ec/Ior (dB)

FIG. 4

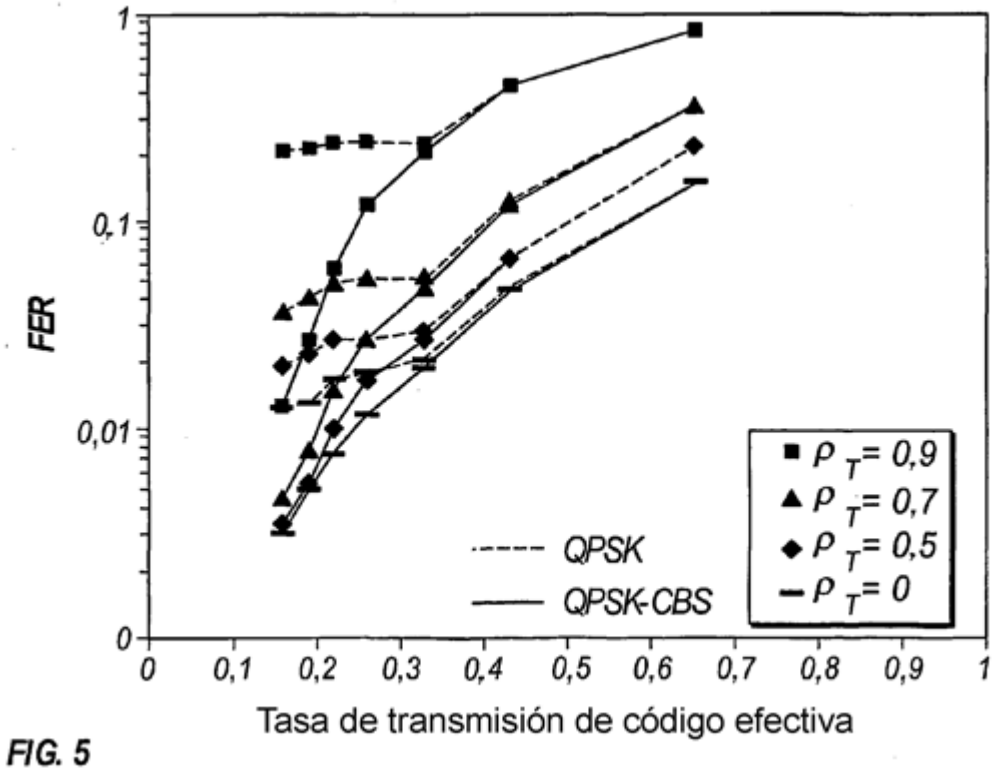
1
0,1
0,01
0
FER
ρ T= 0,9
ρ T= 0,7
ρ T= 0,5
ρ T= 0
QPSK
QPSK-CBS
0 0,1 0,2 0,3 0,4 0,5 0,6 0,7 0,8 0,9 1
Tasa de transmisión de código efectiva

FIG. 5

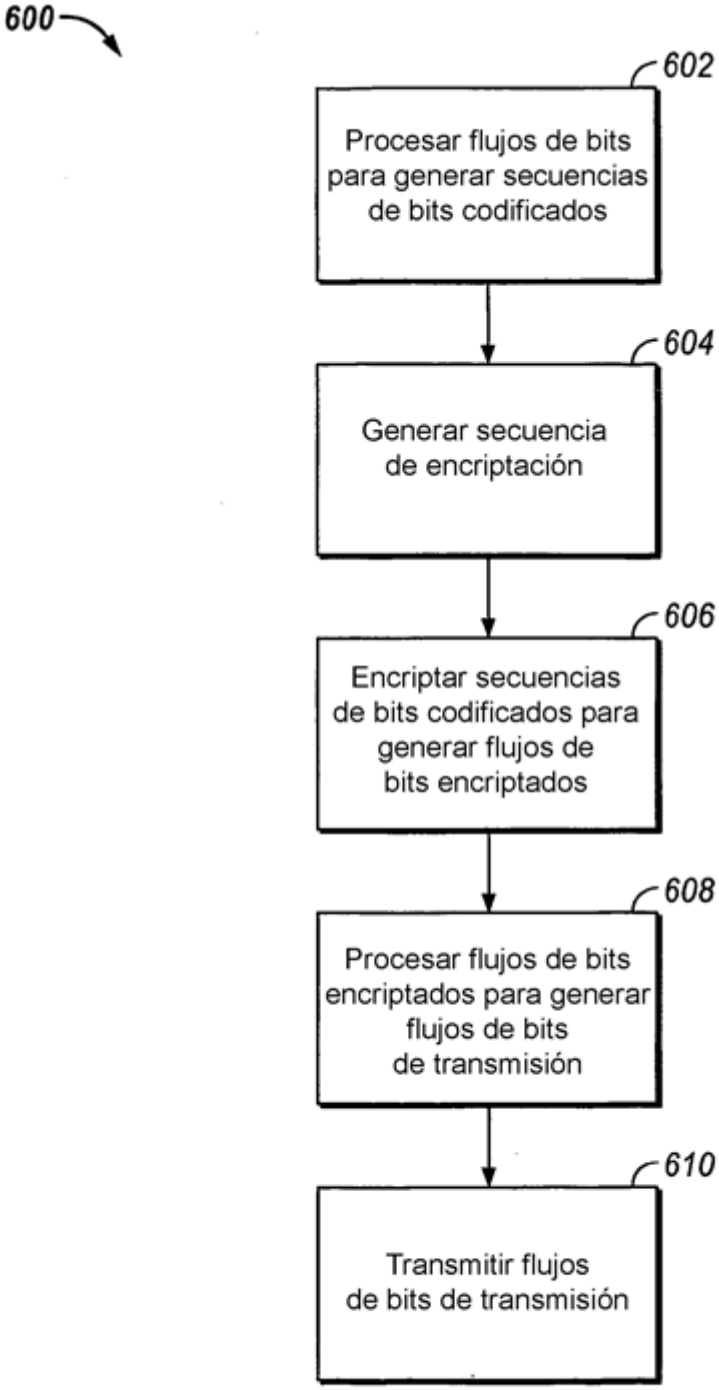
600
602
Procesar flujos de bits para generar secuencias de bits codificados
604
Generar secuencia de encriptación
606
Encriptar secuencias de bits codificados para generar flujos de bits encriptados
608
Procesar flujos de bits encriptados para generar flujos de bits de transmisión
610
Transmitir flujos de bits de transmisión

FIG. 6

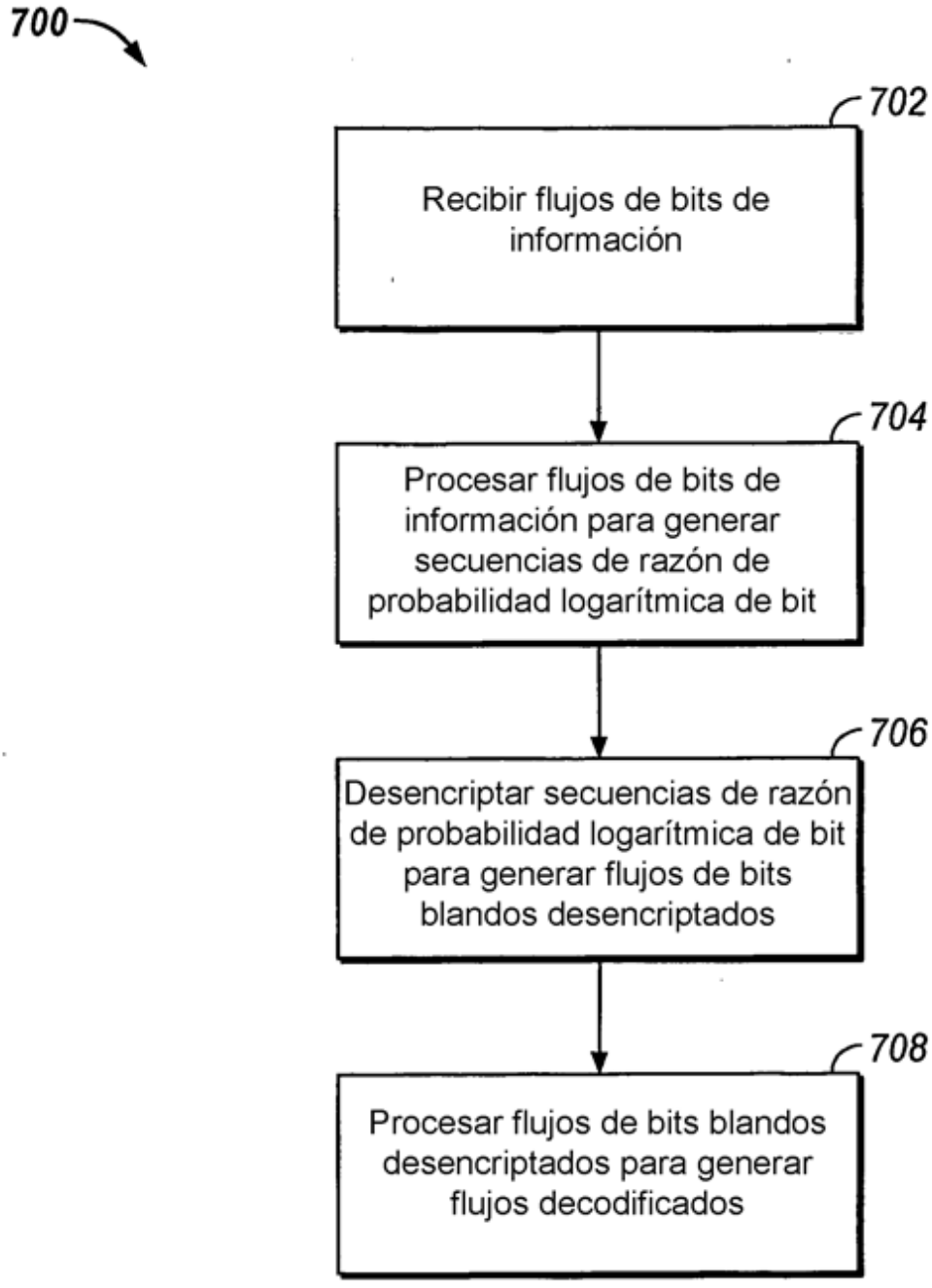
700
702
Recibir flujos de bits de información
704
Procesar flujos de bits de información para generar secuencias de razón de probabilidad logarítmica de bit
706
Desencriptar secuencias de razón de probabilidad logarítmica de bit para generar flujos de bits blandos desencriptados
708
Procesar flujos de bits blandos desencriptados para generar flujos decodificados

FIG. 7