(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 143 396**

(21) Número de solicitud: 009800213

(51) Int. Cl.[7]: G10L 19/14

(12) PATENTE DE INVENCION B1

(22) Fecha de presentación: **04.02.1998**

(43) Fecha de publicación de la solicitud: **01.05.2000**

Fecha de concesión: **03.11.2000**

(45) Fecha de anuncio de la concesión: **16.12.2000**

(45) Fecha de publicación del folleto de patente: **16.12.2000**

(73) Titular/es: **Universidad de Málaga**
Plaza de El Ejido s/n
29071 Málaga, ES

(72) Inventor/es: **Ríos Gómez, Francisco J. y**
Romero Sánchez, Jorge

(74) Agente: **No consta**

(54) Título: **Circuito integrado monolítico codec-encriptador de baja tasa para señales de voz.**

(57) Resumen:
Circuito integrado monolítico codec-encriptador de baja tasa para señales de voz que incorpora un vocoder y un encriptador-descifrador compuesto por los siguientes módulos funcionales: Módulo de Preénfasis, (a), Módulo de enventanado (b), Módulo de autocorrelación (c), Módulo de cálculo de los coeficientes de predicción lineal del filtro (d), Módulo Detector de Pitch y Decisión Voz - Novoz (e), Módulo Cuantificador (f), Módulo Encriptador (g), Módulo Descifrador (h), Módulo Descodificador de Trama (i), Módulo Escalador (j), Módulo Generador de Residuo (k), Módulo de Ganancia (l), Módulo Filtro Todo - Polos (m), Módulo de Deénfasis (n), Módulo de Transmisión (o) y Módulo de Recepción (p).

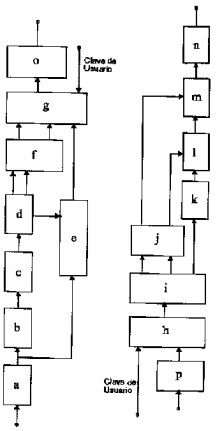

Figura Unica

ES 2 143 396 B1

DESCRIPCION

Circuito integrado monolítico codec-encriptador de baja tasa para señales de voz.

Sector de la técnica

La presente invención tiene su aplicación en el campo de la Industria Electrónica en todos aquellos sistemas de comunicación de voz que hagan uso de un canal inseguro de bajo ancho de banda o saturado. Se presenta como solución para la comunicación digital segura de voz en sistemas de banda estrecha (telefonía tradicional e inalámbrica), almacenamiento seguro y masivo de voz (buzones seguros de voz), aplicaciones multimedia (procesos de conversación simultánea segura en redes saturadas -Internet) y aplicaciones militares en transmisión segura de voz.

Estado anterior de la técnica

Los modelos de producción del habla proporcionan una vía para la eliminación de redundancia y la codificación digital. Los modelos lineales de producción de la voz propuestos por Fant, G.C.M.: *Acoustic Theory of Speech Production*. Mouton and Co.'s-Gravenhage, The Netherlands, 1960 y Flanagan, J. L.: *Speech Analysis Synthesis and Perception*, Springer-Verlag, Berlin, 1972 y los modelos de predicción lineal propuestos por Atal, B.S. Schroeder, M.R.: *Predictive Coding of Speech Signals*. Proc 1967 Conf. Commun. And Process, pp360-361 (1967), Markel J.D. y Gray, Jr A.H. : *Linear Prediction of Speech*. Springer-Verlag, 1976, Capítulo 8; constituyen el punto de partida y la base teórica en lo que respecta al procedimiento de codificación digital de la voz. El modelo de producción básicamente consta de dos generadores, uno periódico y otro ruidoso, que actúan sobre un filtro todos polo cuya función de transferencia es, en el dominio de la transformada z:

$$A(z) = V_{ef} \ / \ (1+a_1 z^{-1}+ a_2 z^{-2} +...+ a_L z^{-L})$$

donde z es la variable compleja, a_1 ... a_L, son los coeficientes del filtro y V_{ef} es el valor eficaz del marco actual.

Un proceso de decisión basado en la característica Voz - Novoz de la señal, conmuta la excitación periódica o ruidosa respectivamente en el citado filtro.

Para extraer los parámetros del modelo, se analiza la señal de, voz en intervalos de tiempo finito: La señal de voz continua y una vez muestreada se divide en marcos de duración constante. En el proceso de análisis y para cada marco, se extraen los parámetros:

Valor eficaz de la excitación: V_{ef}
Parámetro Voz - Novoz: VNV
Tono fundamental o Pitch: T
Coeficientes del filtro a_K en formato coeficiente de reflexión o PARCOR (PARtial CORrelation).

En el proceso de síntesis, se conjugan dichos parámetros para, de acuerdo con el modelo, construir de nuevo la señal original.

Entre los procesos de análisis y síntesis, tiene lugar una fase cuantificación - escalado en la que se decide sobre el nivel de compresión, función de la tasa de transmisión-recepción, en relación inversa con la calidad o precisión de la voz transmitida/recibida y una fase de encriptado/descifrado en la que la señal se transforma para proporcionar un grado de protección frente a cualquier observador ajeno.

En el proceso de cuantificación se minimiza el error entre el valor original y el cuantificado para un número determinado de bits. En la invención se utilizan un modelo de cuantificación escalar no uniforme basado en la Técnica de Max y Lloyd que obtiene un cuantificador subóptimo simplificado (Modelo de cuantificación Jain A. K. *Fundamentals of Digital Image Processing*. Prentice-Hall International Ed. 1989. Capítulo 4).

El proceso de cuantificación conlleva un proceso de truncación en la precisión numérica que añade errores que se manifiestan en las componentes de alta frecuencia. Es posible corregir este fenómeno mediante, la aplicación de un proceso previo de preénfasis.

El encriptado sigue la técnica definida como One Time Pad (Schneier B. *Applied Cryptography 2ª Ed.* John Wiley & Son Inc. 1996. Capítulos 1,2,16) que es un proceso de cifrado de trama en el cual la señal se enmascara con un ruido pseudoaleatorio (ruido blanco cuya síntesis es programable mediante clave).

El problema fundamental es que todas estas operaciones necesarias para una comunicación segura no están integradas.

Explicación de la invención

La presente invención, partiendo del estado de la Técnica Microelectrónica actual, plantea soluciones a este problema de falta de integración de estas operaciones, de tal modo que todo este conjunto de operaciones, dentro de una arquitectura definida, se incluye en un solo circuito integrado monolítico. La invención se presenta en un formato "circuito integrado" en Tecnología CMOS de 0.35 micrómetros.

El circuito integrado codec-encriptador de baja tasa para señales, de voz objeto de la presente invención se caracteriza por el hecho de ser un único circuito integrado monolítico que incorpora un vocoder y un encriptador-descifrador con las siguientes características funcionales:

- Encriptado/descifrado para transmisión segura.
- Transmisión/recepción serie de baja tasa programable (3500bps-9600bps). Coeficientes de reflexión programables en función de la tasa.
- Full-Dúplex.
- 4.294.1967.295 claves diferentes en modo no manual y 99.999.999 claves diferentes en modo manual (Claves de 8 cifras).
- Memoria de 10 claves diferentes.
- Modo de bajo consumo.
- Circuito de medida de tiempo de espera (Watch Dog Timer) programable.
- Control manual (entrada directa por teclado) o por μControlador.
- Tasa de almacenamiento masivo máxima de 38 minutos/Megabyte.

- Trama sincronismo independiente de los datos.
- Periodo de la secuencia de encriptado comprendido entre 5.3 y 15.7 días.

El circuito integrado codec-encriptador, tiene los siguientes bloques funcionales básicos:

- Módulo de Preénfasis (a)
- Módulo de enventanado (b)
- Módulo de autocorrelación (c)
- Módulo de cálculo de los coeficientes de predicción lineal del filtro (d)
- Módulo Detector de Pitch y Decisión Voz - Novoz (e)
- Módulo Cuantificador (f)
- Módulo Encriptador (g)
- Módulo Descifrador (h)
- Módulo Descodificador de Trama (i)
- Módulo Escalador (j)
- Módulo Generador de Residuo (k)
- Módulo de Ganancia (l)
- Módulo Filtro Todo - Polos (m)
- Módulo de Deénfasis (n)
- Módulo de Transmisión (o)
- Modulo de Recepción (p).

El circuito integrado está compuesto por un sistema completo para transmisión/ recepción segura de voz a dos líneas serie, punto a punto y full-dúplex. Posee una interfaz paralela que permite la programación de los distintos modos de funcionamiento a petición del usuario, y se puede controlar de formas distintas:

1. Por medio de un microcontrolador (μC) ó microprocesador (μP). El CI se puede emplear como un elemento más del sistema μC ubicado en memoria ó en el mapa de Entrada/Salida (E/S). En este modo el μC, ve linealmente los registros internos del sistema, programándolos como posiciones de memoria ó puertos de E/S. Con el μC se puede acceder a todos los recursos de programación del CI: Velocidad de transmisión/ recepción, Programación de claves, activación / desactivación de encriptado (modo seguro), modo de bajo consumo, etc.
2. De forma manual. En este modo, tan sólo se puede programar una clave a través de un teclado y activar el modo seguro de comunicación. Este modo es útil si se quiere emplear la mínima cantidad de circuitos electrónicos y es por tanto la opción adecuada para una solución de bajo costo y complejidad del circuito.

Explicación de la figura

Se ha empleado una figura única que representa el sistema a nivel funcional. Cada bloque representa un subsistema del circuito integrado. El nombre de cada bloque indica la funcionalidad específica de cada uno, y el orden de concatenación de los bloques muestra el secuenciamiento del proceso de análisis y síntesis seguido por el circuito integrado. La descripción del sistema global así como los subsistemas, que lo componen está recogida en el apartado descriptivo de la realización preferente de la invención.

Realización preferente de la invención

La Figura muestra el diagrama general de bloques de la invención en lo que respecta a sus bloques funcionales básicos, representando cada bloque un subsistema del circuito integrado. Estos son:

- Módulo de Preénfasis (a). Aplica a la ventana de análisis una operación de realce espectral cuya función de transferencia en el dominio de la transformada z es:

$$H_{Preénf} = 1 - \mu z^{-1}$$

  Donde μ es un parámetro que define el grado de realce espectral. En la invención se usa una pendiente de 6 decibelios correspondiente a μ=0.95, compensando la caída propia de atenuación provocada por la radiación labial y características espectrales de la onda glótica; esto es necesario debido a que el orden del modelo empleado (orden 10) no regresiona correctamente la señal en los casos de marcos de voz sonoros, lo cual puede inducir inestabilidades numéricas en el proceso de inversión matricial durante la ejecución del algoritmo de Levinson - Durbin. Además, esta operación justifica la compensación necesaria por la truncación numérica en procesos de cuantificación.
- Módulo de Enventanado (b). Necesario para la correcta estimación de la función de autocorrelación de la señal disminuyendo el error cometido. El enventanado produce una estimación estadística centrada de la función de autocorrelación real. El tipo de ventana empleado es trapezoidal con solapamiento de 2ms con el marco anterior (16 muestras) y conservación de la potencia intermarco. El tamaño de la ventana efectiva y, por tanto del marco de voz procesado es de 20ms.
- Módulo de Autocorrelación (c). Realiza la estimación de la función de autocorrelación del marco en curso. El proceso que realiza viene dado por:

$$Rss[m]=\Sigma s[n+m]s[n]/N. \quad n=1 \ldots L+1$$

  Donde R_{ss}[m] es la secuencia de autocorrelación, s[n] el marco de señal enventanado, L el orden del filtro y N la longitud del marco. En la invención N=160 (20ms) y L=10. Se calculan L+1 muestras de la secuencia de autocorrelación para el cálculo de los coeficientes de predicción lineal.
- Módulo de Cálculo de los Coeficientes de Predicción Lineal del Filtro (d). Basado en el procedimiento de Levinson - Durbin que

permite la resolución de un sistema lineal de ecuaciones con matriz de Toeplitz (Levinson N. *The Wiener RMS Criterión in Filter Design and Prediction*. Journal of Mathematics and Physics. Vol 25. 1947. Durbin J. *The Fitting of Time Series Models*. Revue L'Institut Internationale de Statisque. Vol 28. 1960). Este, tipo de sistema es el que aparece en los problemas de predicción lineal como resultado del problema de minimización de la norma cuadrática. El cálculo de los coeficientes del filtro se plantea en estos términos y se puede expresar del siguiente modo (Papotilis A. *Probability, Random Variable and Stochastics Processes*. 3ª Ed. McGraw - Hill. 1986. Capítulo 14):

$$\min\| s[n] + \Sigma\ a_i\ s[n\text{-}i]\|^2\ i = 1\ ....\ L$$

La norma empleada es la esperanza matemática del cuadrado de la señal. Los coeficientes de predicción lineal del filtro a_i se codifican como coeficientes de reflexión cual es conveniente por su rango de variabilidad (-1,1), la facilidad para chequeo de inestabilidad y su cuantificación inmediata. El error residual que proporciona el método, es el parámetro de ganancia V_{ef} que se utiliza en el proceso de síntesis. Los dos primeros coeficientes de reflexión se emplean, además, como elementos de cálculo en el módulo de detección de Pitch y de decisión Voz - Novoz.

– Módulo Detector de Pitch y Decisión Voz - Novoz (e). Este módulo calcula los parámetros: período fundamental (T) del marco en curso ó Pitch y la decisión de si el marco es sonoro (Voz) ó sordo (Novoz). La definición del concepto "sonoro" se asocia al hecho de la vibración de la cuerda vocal durante la producción de la voz, por tanto, la ausencia de vibración se clasifica como marco "sordo", lo que no significa que el marco no suene. En general, en marcos sordos se reproducen las voces en las que no existe vibración cordal junto con los silencios ausentes de potencia. Existen términos medios durante las transiciones entre sílabas que permiten una clasificación mas "fina", pero con los dos niveles definidos es suficiente para obtener una calidad aceptable durante el proceso de síntesis (Spanias A.S. *Speech Coding: A Tutorial Review*. Proc of the IEEE Vol 82. N°10. October 1994. Pp 1541 - 1582). En efecto, el filtro todo polo, es un buen resonador de sonidos consonánticos cuando éste se excita con una fuente ruidosa y, desde el punto de vista perceptivo, no provoca ningún problema de inteligibilidad o distorsión. Estos dos parámetros son dependientes el uno del otro y se han de calcular conjuntamente. Para ello se ha desarrollado un algoritmo extracción del parámetro Voz- Novoz original y propio de esta invención que hace uso de criterios perceptivos de la audición humana y basado en la teoría de la decisión bayesiana. El resultado es un autómata de estados finitos que hace uso de indicadores obtenidos durante la detección de pitch y que toma la decisión de clasificar el marco en curso como sonoro ó sordo. Evaluado el riesgo bayesiano que generan las funciones que definen las reglas de decisión (256 funciones), se ha elegido la de riesgo mínimo que cumple el siguiente criterio perceptivo: "la mayor pérdida se produce cuando la decisión errónea se produce en marcos Novoz". La regla es la siguiente:

$$\delta(n) = \text{not}[\xi 1(n)]\ \text{or}\ [\xi 0(n)\ \text{and}\ \delta(n\text{-}1)]$$

Donde $\delta(n)$ es la decisión en el marco actual (1 para marco voz y 0 para marco no voz). $\xi 1$ y $\xi 0$ son indicadores de tasa entre máximo y mínimo de la función de diferencia de magnitudes.

El Pitch se obtiene a partir de dicha función realizada sobre la señal original filtrada (800Hz), para evitar interacciones con el primer formante que podría falsear la medida (Markel J.D. and Gray, Jr A.H.: *Linear Prediction of Speech*. Springer-Verlag.1976. Capítulo 8) y que posteriormente es blanqueada con el filtro formado con los dos coeficientes de reflexión calculados en la etapa de Levinson -Durbin (Spanias A.S. *Speech Coding: A Tutorial Review*. Proc of the IEEE Vol 82. N°10. October 1994. Pp 1541 - 1582). Una vez calculada la Función de diferencia de Magnitudes el Módulo calcula el mínimo y anota el índice que corresponde al período fundamental de la señal. El rango de tonos (Pitch) posible para la voz humana está comprendido entre 80 y 40OHz. La dependencia directa entre los parámetros Pitch y Voz - Novoz nos permite codificar su transmisión teniendo en cuenta sólo el parámetro Pitch. Dado que éste presenta valores comprendidos entro 80 y 40OHz en marcos tipo voz, cualquier número fuera de este rango representa un marco de tipo Novoz.

– Módulo Cuantificador (f). Su función es la de acondicionar los parámetros coeficientes de reflexión y V_{ef} para producir una secuencia de bits de longitud predeterminada por las características de calidad de la señal a transmitir. Para la cuantificación de los coeficientes de reflexión se emplea el método basado en el cuantificador óptimo de Max-Lloyd (Jain A. K. *Fundamentals of Digital Image Processing*. Prentice-Hall International Ed. 1989. Capítulo 4), modificado en esta invención de modo que la curva de cuantificación no uniforme de Max-Lloyd se linealiza por tramos de forma óptima según un criterio de mínimos cuadrados, respecto a la original. La operación de cuantificación así descrita implica implícitamente una operación de escalado previa a la truncación. El método de cuantificación así planteado presenta una arquitectura sencilla y de bajo coste computacional. La cuantificación del

parámetro ganancia V_{ef} se realiza según un cuantificador no uniforme que implementa la operación matemática raíz cuadrada.

– Módulo Encriptador (g). Procesa la trama de voz codificándola de acuerdo con el procedimiento One-Time Pad consistente en sumar linealmente una secuencia de bits generados por una fuente de ruido pseudoaleatoria cuya secuencia se inicia a partir de una clave que actúa como semilla del generador de ruido (Condición Inicial) (clave de usuario en figura única)(Schneier B. *Applied Cryptography 2ªEd.* John Wiley & Son Inc. 1996. Capítulos 1,2,16). La estructura del generador de ruido es la de un registro de desplazamiento realimentado linealmente (RDRL) de longitud 32 y con realimentación generada por un polinomio primitivo de la forma:

$$P(x) = x^{32} + x^7 + x^5 + x^3 + x^2 + x$$

Donde x es la variable independiente del polinomio P(x). Este polinomio garantiza el periodo máximo posible de repetición de la secuencia y fija el campo de claves a 2^{32}-1. El periodo está comprendido entre 15.7 días (caso de transmisión a 3500bps), y 5.3 días (9600bps).

– Módulo Descifrador (h). Su misión es la de procesar la trama recibida por el módulo de recepción (r) para descifrar, de acuerdo con la clave, preestablecida (clavo de usuario en figura única), y aplicar la operación inversa a la de encriptado produciendo el cuerpo de trama de voz original. Las operaciones de sincronismo se llevan de tal modo que la secuencia de la semilla es inicializada siempre que exista sincronismo lógico entre los sistemas remotos. Una vez sincronizados, realiza una operación inversa One-Time Pad.

– Módulo Descodificador de Trama (i). Realiza la extracción de las palabras - código de los parámetros del modelo y se las entrega al módulo escalador. Este módulo posee un sistema verificador de la estabilidad de los coeficientes de reflexión recibidos. Si se detecta error de paridad en la capa lógica, el descodificador de trama repita todos los parámetros del modelo del marco anterior. Si detecta un error de estabilidad repite solamente los coeficientes de reflexión.

– Módulo Escalador (j). Este módulo se encarga de adaptar las palabras - código de los parámetros del modelo al rango numérico original. Realiza la operación inversa a la realizada en el cuantificador. Una vez realizada esta operación, se distribuyen los parámetros a los correspondientes módulos de síntesis. En el proceso de escalado del valor eficaz V_{ef}, los valores de potencia nula se escalan según un valor mínimo que proporciona la sensación de confort del usuario durante los silencios.

– Módulo Generador de Residuo (k). A partir de los parámetros T y Voz - Novoz, procedentes del módulo escalador, éste módulo sintetiza la excitación que será aplicada al filtro Todo - Polos. La excitación consiste en dos fuentes de señal multiplexadas, una de señal, periódica (un tren de deltas de Kronecker) y otra de ruido blanco. Si el parámetro Voz - Novoz es cero, se conecta la fuente de ruido, y si es distinto de cero se conecta a la fuente periódica. Con independencia de la fuente, la excitación conserva siempre su valor medio nulo, condición necesaria y suficiente para que el filtro Todo - Polos no genere componentes de continua que produzcan saturación. Igualmente, se aplica el concepto de tono síncrono, consistente en la conservación de la fase de la secuencia de deltas de Kronecker entre marcos manteniendo entre todas ellas, mientras se produzcan, la distancia temporal del pitch. El parámetro T se almacena en un registro de seguimiento cuando el indicador Voz - Novoz es cero. Entre una secuencia de Voz Sonora - Sorda Sonora, se mantiene el contenido del registro para inicializar la fase de comienzo de emisión de deltas. Los dos generadores de señal se encuentran normalizados proporcionando una amplitud constante. El Módulo generador de residuo representa a la excitación glotal. Las deltas de Kronecker reproducen al actuar con el Filtro Todo - Polos, la vibración sonora modulada por el tracto, al igual que el ruido reproduce vibración sorda. Para mantener en el usuario un determinado nivel de confort durante los silencios (sonidos Novoz con potencia nula), La potencia se transforma en una potencia umbral que proporciona un 'murmullo' semejante a la respiración humana durante los periodos de silencio absoluto (aspecto perceptivo).

– Módulo de Ganancia (l). Se encarga de modular en amplitud la señal de residuo. Su característica esencial es la del mantenimiento de la Potencia real de la señal original producida en el marco en curso.

– Módulo Filtro Todo - Polos (m). Filtro autoregresivo de orden L=10, cuyos coeficientes son los de reflexión recibidos desde el módulo escalador. Tiene una estructura en celosía (Lattice) que presenta gran inmunidad al ruido. Este filtro se asocia a las características resonantes del tracto vocal. La decisión de usuario en la tasa de transmisión condiciona la precisión en la que este filtro emula o reproduce las características del tracto vocal del hablante emisor.

– Módulo de Deénfasis (n). Se encarga de realizar la operación inversa a la de preénfasis como una operación que recupera las características de decaimiento en frecuencia y de radiación labial propias de la señal de voz. Consiste en una estructura de filtro inverso IIR de preénfasis. Además, teniendo en cuenta las características de la distorsión de la fase de conversión Digital Analógica (no incluida en ésta invención), el Módulo de deénfasis incluye la compensación que cancela dicha distorsión mediante la aplicación

de un filtro ecualizador. La operación global se realiza como un solo módulo de filtrado general en el que el numerador se representa la ecualización y el denominador el propio deénfasis. La función de transferencia en el dominio de la transformada z es:

$$H(z)=(b_0\ z^{-0}+....+b_{M-1}z^{-M+1})/(1-\mu z^{-1})$$

donde $b_0..b_{M-1}$, son los coeficientes de ecualización, M es el orden de la ecualización μ el factor de deénfasis.

– Módulo de Transmisión (o). Es el encargado de transmitir a tasa programada la secuencia de bits a enviar. A su vez, se encarga de añadir al cuerpo de trama de voz dos capas de protocolo, una física de sincronismo y otra lógica de control. En la capa física se generan tres bits de sincronismo físico, dos de arranque y uno de parada, y en la capa lógica se genera una trama de control de sincronismo (sincronismo lógico), formada por tres bits, dos de identificación de trama y uno de paridad. La función de la capa física es la sincronización hardware. La función de la capa lógica es la coordinación y el diálogo entre el emisor y el receptor en los casos de inicialización reprogramación y pérdida de trama. Este módulo posee un circuito de medida de tiempo de espera (Watch Dog Timer) programable por usuario y cuya función es la de inhibir el dialogo en el caso en que se haya superado una cota temporal por el mal funcionamiento del canal de transmisión ó de los sistemas transmisor ó receptor.

– Módulo de Recepción (p). El dialogo entre las etapas transmisor remoto y receptor local se establece entre dos sistemas distintos. El módulo de recepción se encarga de leer e identificar las tramas de sincronismo físico ($1^{\underline{a}}$ capa) y de sincronismo lógico ($2^{\underline{a}}$ capa). El mantenimiento de un diálogo estable entre módulos de transmisión y recepción implica que en los procesos de inicialización se establezca un primer nivel de sincronización física. La Salida del módulo de recepción esta conformada ya como un vector de datos que se corresponden con el cuerpo de la trama de voz encriptada.

REIVINDICACIONES

1. Circuito integrado monolítico codec-encriptador de baja tasa para señales de voz **caracterizado** por el hecho de que incorpora un vocoder y un encriptador-descifrador compuesto por los siguientes módulos funcionales: Módulo de Preénfasis (a), Módulo de enventanado (b), Módulo de autocorrelación (c), Módulo de cálculo de los coeficientes de predicción lineal del filtro (d), Módulo Detector de Pitch y Decisión Voz - Novoz (e), Módulo Cuantificador (f), Módulo Encriptador (g), Módulo Descifrador (h), Módulo Descodificador de Trama (i), Módulo Escalador (j), Módulo Generador de Residuo (k), Módulo de Ganancia (l), Módulo Filtro Todo - Polos (m), Módulo de Deénfasis (n), Módulo de Transmisión (o) y Modulo de Recepción (p).

2. Circuito integrado codec-encriptador, según la reivindicación 1, en el que la parte vocoder se **caracteriza** por:

a) El marco de 20ms con trama fija de 160 bits con ventana tipo trapezoidal con característica de conservación de la potencia media temporal intermarco. Solapamiento temporal de 2ms.

b) La regla de decisión de riesgo mínimo para la detección del parámetro Voz - Novoz definida: $\delta(n) = not[\xi 1(n)]$ or $[\xi 0(n)$ and $\delta(n-1)]$.

c) La codificación de coeficientes de reflexión programable de longitud variable, bien en función de la calidad de voz deseada por usuario o bien condicionada por la limitación en banda del canal de transmisión.

d) La estructura de marco constante con mantenimiento del Pitch intermarco.

e) La cuantificación escalar óptima basada en el cuantificador de Max and Lloyd modificado para obtener un cuantificador subóptimo simplificado, existiendo una linealización por tramos del cuantificador Max-Lloyd.

3. Circuito integrado codec-encriptador, según la reivindicación 1, en el que la parte encriptador se **caracteriza** por:

a) El periodo de la secuencia de encriptado, siendo el periodo máximo de 15.7 días de conversación continua y el Periodo Mínimo de 5.3 días de conversación continua. Estos periodos máximo y mínimo se corresponden con las velocidades mínima (3500 bps) y máxima (9600 bps) programables en el circuito.

b) El uso del polinomio $P(x) = x^{32} + x^7 + x^5 + x^3 + x^2 + x$ como elemento realimentador del RDRL.

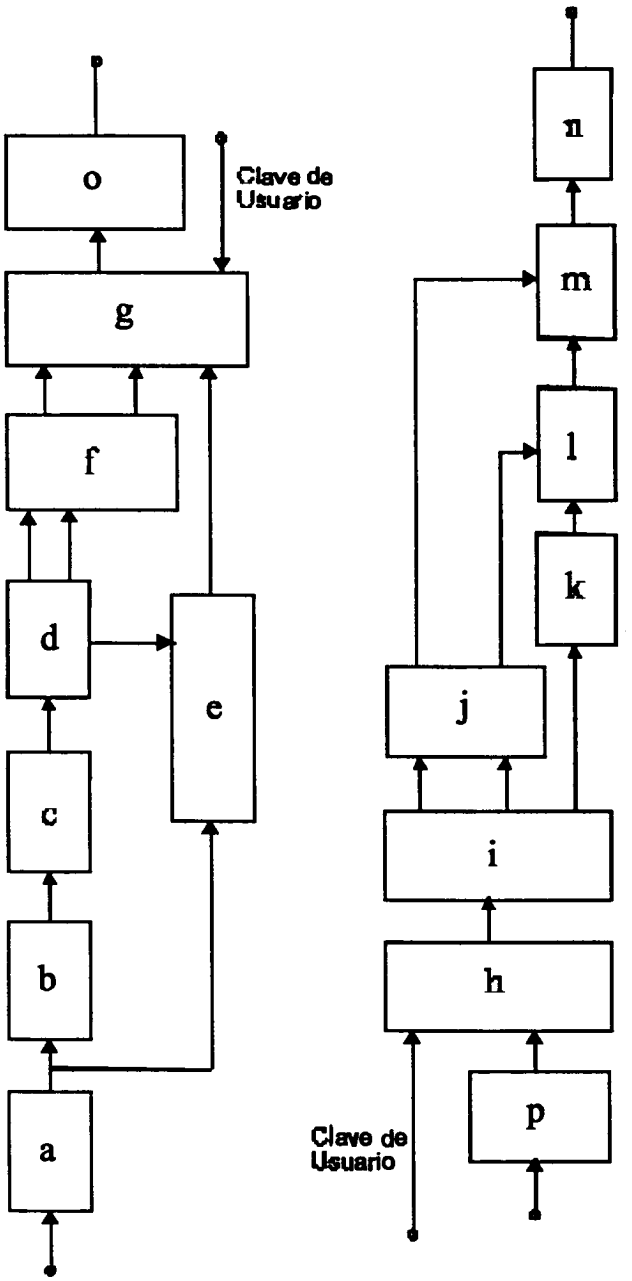

Figura Unica

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 143 396

(21) N.° solicitud: 009800213

(22) Fecha de presentación de la solicitud: **04.02.1998**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl.**[7]**:** G10L 19/14

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	EP 0712213 A2 (MOTOROLA) 13.05.1996, columna 10, línea 47 - columna 12, línea 10; columna 14, líneas 15-34; columna 19, líneas 10-18; figuras 3,4.	1-3
A	WO 8303917 A1 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY) 10.11.1983, página 4, línea 20 - página 6, línea 8; reivindicaciones 1,3,4; figuras 1,2.	1,2
A	WO 8602726 A1 (M/A-COM LINKABIT) 09.05.1986, página 4, línea 17 - página 7, línea 8.	1

Categoría de los documentos citados

X: de particular relevancia

Y: de particular relevancia combinado con otro/s de la misma categoría

A: refleja el estado de la técnica

O: referido a divulgación no escrita

P: publicado entre la fecha de prioridad y la de presentación de la solicitud

E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

[×] para todas las reivindicaciones

[ ] para las reivindicaciones n°:

Fecha de realización del informe	Examinador	Página
16.03.2000	M. Alvarez Moreno	1/1