



(19)



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 266 481**

(51) Int. Cl.:
H04N 7/167 (2006.01)
H04K 1/02 (2006.01)

(12)

TRADUCCIÓN DE PATENTE EUROPEA

T3

(86) Número de solicitud europea: **02720374 .4**
(86) Fecha de presentación : **09.04.2002**
(87) Número de publicación de la solicitud: **1382202**
(87) Fecha de publicación de la solicitud: **21.01.2004**

(54) Título: **Codificación de audio con encriptación parcial.**

(30) Prioridad: **18.04.2001 EP 01201405**

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

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

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

(72) Inventor/es: **Oomen, Arnoldus, W., J. y**
Van de Kerkhof, Leon, M.

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

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

DESCRIPCIÓN

Codificación de audio con encriptación parcial.

La presente invención se refiere a la codificación y decodificación de señales de audio. En particular, la invención se refiere a la codificación de audio de velocidad de transmisión de bits baja tal como se utiliza en audio de estado sólido o audio de Internet.

La mezcla aleatoria ("mezcla aleatoria") compatible es una técnica para mezclar aleatoriamente (partes de) una corriente de bits de manera que la corriente de bits mezclada aleatoriamente todavía puede decodificarse, pero la señal decodificada resulta en una señal degradada. Así, la mezcla aleatoria compatible puede aplicarse para controlar la calidad después de decodificar una corriente de bits de audio comprimida en un ambiente controlado por copia. Esta técnica se ha descrito para un codificador por transformación de AAC ("Advanced Audio Coding", Codificación de Audio Avanzada) (codificación de audio avanzada de una parte del estándar MPEG-2) en "Secure Delivery of Compressed Audio Bit-Stream Mezcla aleatoria" (Entrega segura de audio comprimido mediante mezcla aleatoria de corriente de bits comprimida), E. Allamanche y J. Herre, Convención 108 de AES, París, 19-22 de Febrero de 2000, o en el documento US-A_6 081 784 por Tsutsui Kyoya.

Aquí, la corriente de bits de AAC se encripta con una clave tal que para que ningún aumento en la velocidad de transmisión de bits, la calidad puede fijarse a cualquier nivel requerido (por debajo de la calidad obtenida para la corriente no mezclada aleatoriamente). Si se conoce la clave de encriptación (mediante alguna transacción), la corriente de bits puede descryptarse a un estado original. Allamanche también afirma que este método de mezcla aleatoria compatible también puede aplicarse a otros esquemas de compresión.

Sin embargo, para un codificador por transformación de AAC o cualquier otro tipo de codificador de forma de onda, el espectro se codifica típicamente utilizando una representación espectral gruesa y una fina. Se utiliza un conjunto de factores de escala para describir una representación gruesa del espectro y se utiliza una división fina entre factores de escala posteriores para describir la estructura fina del espectro. La mezcla aleatoria compatible en Allamanche se realiza mediante la modificación (mezcla aleatoria) de la estructura fina del espectro hasta el punto en que se obtiene una cierta señal de nivel de calidad más baja.

Para un esquema de codificación paramétrico, por ejemplo, el tipo de codificador sinusoidal descrito en la solicitud de patente PCT publicada n° WO-A 0 079 519 (Referencia agente: N 017502), los componentes de señal no se describen en términos de una representación espectral gruesa y una fina. En su lugar, los parámetros sinusoidales describen las llamadas pistas que son sinusoides que comienzan en una instancia de tiempo específica, evolucionan durante una cierta cantidad de tiempo y entonces se detienen. En el periodo en el que la sinusoide está activa, la evolución típicamente varía de manera lenta. Por lo tanto, las técnicas de mezcla aleatoria compatible propuestas en Allamanche no pueden aplicarse a un esquema de codificación sinusoidal.

La patente de los Estados Unidos n° 6 081 784 describe un método de codificación para encriptar y codificar señales de información tal como señales de audio PCM, en el que la información puede reprodu-

cirse con calidad baja incluso en ausencia de la información clave para la encriptación. Una unidad de transformación convierte las señales PCM en componentes de señal de frecuencia que se codifican mediante una unidad de codificación de componentes de señal.

Según la presente invención, se proporciona un método de codificar una señal de audio tal como se expone en la reivindicación 1, un método para decodificar una señal de audio tal como se expone en la reivindicación 15, un codificador de audio tal como se expone en la reivindicación 16, un reproductor de audio tal como se expone en la reivindicación 17, y una corriente de audio tal como se expone en la reivindicación 19.

En una realización preferida de la invención, la representación paramétrica incluye códigos que representan componentes sinusoidales sostenidos de la señal de audio, para los cuales se actualizan parámetros de frecuencia y/o amplitud de manera diferencial durante el periodo en el que una sinusoide está activa. Para mezclar aleatoriamente los valores de frecuencia y/o amplitud codificados diferenciales, se hace una correspondencia de los valores diferenciales con otros valores diferenciales. Mediante la modificación de estos valores, la corriente de bits todavía puede decodificarse pero resulta en pistas con variación de frecuencia y/o amplitud aleatoria. Por consiguiente, la señal se degradará.

Se describirán ahora varias realizaciones con referencia a los dibujos adjuntos, en los que:

La figura 1 muestra una realización de un codificador de audio según la invención;

La figura 2 muestra una realización de la invención de un reproductor de audio según la invención; y

La figura 3 muestra un sistema que comprende un codificador de audio y un reproductor de audio.

En una realización preferida de la presente invención, se describe la aplicación de mezcla aleatoria compatible para un esquema de codificación paramétrica, figura 1, donde el codificador es un codificador sinusoidal. En tanto los casos relacionados como la realización preferida, el codificador 1 de audio muestra una señal de audio de entrada en una determinada frecuencia de muestreo dando como resultado una representación $x(t)$ digital de la señal de audio. Esto hace que la escala t de tiempo sea dependiente de la velocidad de muestreo. Entonces, el codificador 1 separa la señal de entrada muestreada en tres componentes: componentes de señal transitoria, componentes determinísticos (sinusoidales) sostenidos y componentes estocásticos (de ruido) sostenidos. El codificador 1 de audio comprende un codificador 11 transitorio, un codificador 13 sinusoidal y un codificador 14 de ruido. El codificador de audio opcionalmente comprende un mecanismo 12 de compresión (GC) de ganancia.

En esta realización de la invención, la codificación transitoria se realiza antes la codificación sostenida. Esto es ventajoso por que las componentes de señales transitorias no se codifican de manera eficaz y óptima en codificadores sostenidos. Si se utilizan codificadores sostenidos para codificar componentes de señales transitorios, es necesario mucho esfuerzo de codificación; por ejemplo, puede imaginarse que es difícil codificar una componente de señal transitoria con sólo sinusoides transitorias. Por lo tanto, la eliminación de

componentes de señal transitoria de la señal de audio a codificar antes de la codificación sostenida es ventajosa. También se observará que una posición de inicio transitoria derivada en el codificador transitorio puede utilizarse en los codificadores sostenidos para segmentación adaptativa (encuadre adaptativo).

Sin embargo, la invención no se limita al uso particular de codificación transitoria.

El codificador 11 transitorio comprende un detector (TD) 110 transitorio, un analizador (TA) 111 transitorio y un sintetizador (TS) 112 transitorio. En primer lugar, la señal $x(t)$ entra en el detector 110 transitorio. Este detector 110 estima si hay una componente de señal transitoria y su posición. Esta información se alimenta al analizador 111 transitorio. Esta información también puede utilizarse en el codificador 13 sinusoidal y el codificador 14 de ruido para obtener la segmentación inducida por señal ventajosa. Si se determina la posición de una componente de señal transitoria, el analizador 111 transitorio intenta extraer (la parte principal de) la componente de señal transitoria. Hace una correspondencia de una función de forma con una posición de inicio estimada, y determina el contenido debajo de la función de forma empleando por ejemplo, un número (pequeño) de componentes sinusoidales.

En cualquier caso, se observará que donde, por ejemplo, el analizador transitorio emplea una función de forma de tipo Meixner, entonces, el código CT transitorio comprenderá la posición de inicio en la que comienza el transitorio; un parámetro que es sustancialmente indicativo de la velocidad de ataque inicial; y un parámetro que es sustancialmente indicativo de la velocidad de decaimiento; así como los datos de frecuencia, amplitud y fase de los componentes sinusoidales del transitorio.

Si la corriente de bits producida por el codificador 1 ha de sintetizarse por un decodificador independientemente de la frecuencia de muestreo utilizada para generar la corriente de bits, entonces la posición inicial debería transmitirse como un valor de tiempo en vez de, por ejemplo, un número de muestra dentro de una trama; y las frecuencias de las sinusoides deberían transmitirse como valores absolutos o utilizando identificadores indicativos de valores absolutos en vez de valores que sólo pueden derivarse de o proporcionales a la frecuencia de muestreo de la transformación. No obstante, la presente invención puede implementarse con cualquiera de los esquemas anteriores.

También, se observará que la función de forma también puede incluir una indicación de escalón en caso de que la componente de señal transitoria sea un cambio tipo escalonado en la envolvente de amplitud. En este caso, la posición transitoria sólo afecta a la segmentación durante la síntesis para el módulo sinusoidal y de ruido. Una vez más, aunque la invención no se limita a una u otra implementación, la ubicación del cambio tipo escalonado puede codificarse como un valor de tiempo en vez de un número de muestra, que estaría relacionado con la frecuencia de muestreo.

El código CT transitorio se suministra al sintetizador 112 transitorio. La componente de señal transitoria sintetizada se resta de la señal $x(t)$ de entrada en el substractor 16, dando como resultado una señal x_1 . En caso de que se omita la CG 12, $x_1 = x_2$. La señal x_2 se suministra al codificador 13 sinusoidal donde se analiza en un analizador 130 sinusoidal (SA), que determina las componentes sinusoidales (determinís-

ticas). La información resultante se obtiene en el código CS sinusoidal y se proporciona un ejemplo más detallado que ilustra la generación de un código CS sinusoidal ejemplar en la solicitud de patente PCT nº PCT/EP00/05344 (Referencia agente: N 017502). Alternativamente, se describe una implementación básica en "Speech analysis/synthesis based on sinusoidal representation" (Análisis/síntesis del habla basándose en representación sinusoidal), R. McAulay y T. Quartieri, IEEE Trans. Acoust., Speech, Signal Process., 43:744-754, 1986 o "Technical Description of the MPEG-4 audio-coding proposal from the University of Hannover and Deutsche Bundespost Telekom AG (revised)" (Descripción Técnica de la propuesta de codificación de audio de MPEG-4 de la Universidad de Hannover y Deutsche Bundespost Telekom AG (revisado), B. Edler, H. Purnhagen and C. Ferekidis, Nota técnica MPEG95/0414r, Organización internacional para la estandarización ISO/IEC JTC1/SC29/WG11, 1996.

En breve, sin embargo, el codificador sinusoidal de la realización preferida codifica la señal x_2 de entrada como pistas de componentes sinusoidales enlazadas de un segmento de la trama hasta el siguiente. Estas pistas comienzan en una instancia de tiempo específica, evolucionan durante una cierta cantidad de tiempo y entonces se detienen. Las actualizaciones a estas pistas de un segmento al siguiente se describen en términos de información de frecuencia, amplitud y opcionalmente fase. En el periodo en el que la senoide está activa, la evolución típicamente varía de manera lenta. Debido a este motivo, es muy eficaz en la velocidad de transmisión de bits actualizar los parámetros de frecuencia y amplitud de manera diferencial. Así, las pistas se representan inicialmente mediante una frecuencia de inicio, una amplitud de inicio y una fase de inicio para una senoide que comienza en un segmento dado- un nacimiento. A continuación, la pista se representa en segmentos posteriores mediante diferencias de frecuencia, diferencias de amplitud, y posiblemente, diferencias (continúaciones) de fase hasta el segmento en el que termina la pista (muerte). En la práctica, puede determinarse que hay poca ganancia en la codificación de diferencias de fase. Así, no es necesario de ninguna manera codificar información de fase para continuaciones y la información de fase puede regenerarse utilizando reconstrucción de fase continua.

Una vez más, si la corriente de bits se hace independiente de la frecuencia de muestreo, las frecuencias de inicio se codifican dentro del código CS sinusoidal como valores absolutos o identificadores indicativos de frecuencias absolutas para garantizar que la señal codificada sea independiente de la frecuencia de muestreo.

Desde el código CS sinusoidal, la componente de señal sinusoidal se reconstruye mediante un sintetizador SS 131 sinusoidal. Esta señal se resta en el substractor 17 de la entrada x_2 al codificador 13 sinusoidal, dando como resultado una señal x_3 restante que carece de componentes de señal transitoria (grandes) y componentes sinusoidales determinísticas (principales).

La señal x_3 restante se asume principalmente para comprender ruido y el analizador 14 de ruido de la realización preferida produce un código CN de ruido representativo de este ruido. Convencionalmente, como por ejemplo, en la solicitud de patente PCT

nº PCT/EP00/04599, presentada el 17.05.2000 (Referencia agente: PH NL000287) el codificador de ruido se modela un espectro del ruido con parámetros (p_i , q_i) de filtro AR (autoregresivo) y de MA (media móvil) combinados según una escala de ancho de banda rectangular equivalente (ERB). Dentro del decodificador, figura 2, los parámetros de filtros se alimentan a un sintetizador NS 33 de ruido, que es principalmente un filtro, que tiene una respuesta de frecuencia que se aproxima al espectro del ruido. El NS 33 genera ruido yN reconstruido mediante la filtración de una señal de ruido blanco con los parámetros (p_i , q_i) de filtración ARMA y posteriormente añade esto a las señales yT transitorias e yS sinusoidales sintetizadas descritas a continuación.

Sin embargo, los parámetros (p_i , q_i) de filtración ARMA son una vez más dependientes de la frecuencia de muestreo del analizador de ruido, y si la corriente de bits codificada ha de ser independiente de la frecuencia de muestreo, estos parámetros se transforman en frecuencias del espectro lineal (LSF) también conocidas como pares del espectro lineal (LSP) antes de codificarse. Estos parámetros LSF puede representarse sobre una cuadrícula de frecuencias absolutas o una cuadrícula relacionada con la escala ERB o la escala Bark. Puede encontrarse más información sobre LSP en "Line Spectrum Pair (LSP) and speech data compression" (Par del espectro lineal (LSP) y compresión de datos de voz), F. K. Soong y B. H. Juang, ICASSP, pág. 1.10.1, 1984. En cualquier caso, se conoce bien tal transformación de un tipo de coeficientes de tipo filtro predictivos lineales (en este caso, (p_i , q_i) dependientes de la frecuencia de muestreo del codificador) en LSFs que son independientes de la frecuencia de muestreo y viceversa (tal como se requiere en el codificador) y no se describe adicionalmente en el presente documento. Sin embargo, se observará que la conversión de LSFs en coeficientes de filtro (p_i , q_i) dentro del codificador puede hacerse con referencia a la frecuencia con la que el sintetizador 33 de ruido genera muestras de ruido blanco, permitiendo así que el decodificador genere la señal yN de ruido independientemente de la manera en que se muestreó originalmente.

Se observará que, de manera similar a la situación en el codificador 13 sinusoidal, el analizador 14 de ruido también utilizar la posición de inicio de la componente de señal transitoria como una posición para comenzar un bloque de análisis nuevo. Así, los tamaños de segmento del analizador 130 sinusoidal y el analizador 14 de ruido no son necesariamente iguales.

No obstante, tal como se verá a continuación, la presente invención puede implementarse con cualquier esquema de codificación de ruido incluyendo cualquiera de los esquemas referidos anteriormente.

En la realización preferida de la presente invención, la mezcla aleatoria se realiza en el código CS sinusoidal producido por el analizador 130 sinusoidal. En particular, en la realización preferida, se dispone un módulo 18 de cifrado entre el analizador 130 sinusoidal y un multiplexor 15. El módulo 18 de cifrado mezcla aleatoriamente los valores de frecuencia y/o amplitud codificados diferenciales del código CS sinusoidal para segmentos de continuación de pistas utilizando una clave proporcionada. En otras palabras, el módulo 18 hace una correspondencia de los valores diferenciales con otros valores diferenciales para

producir un código CSe sinusoidal cifrado. Mediante la modificación de estos valores, la corriente de bits que comprende los códigos CSe todavía puede decodificarse pero da como resultado pistas con variación de frecuencia aleatorizada y/o variación de amplitud aleatorizada a lo largo de la vida de una pista. Por consiguiente, sin la clave correcta, la calidad de una señal sintetizada producida por un decodificador se degradará.

La cantidad de degradación puede controlarse mediante la cantidad y el intervalo en los que se modifican estas frecuencias y/o amplitudes codificadas de manera diferencial. Así, por ejemplo, puede decidirse que ciertos tipos de señal de audio son más sensibles a la mezcla aleatoria que otros, y de manera similar, que ciertos tipos de señal son más sensibles a la mezcla aleatoria de frecuencia que a mezcla aleatoria de amplitud. Así, si una señal comprende una componente sinusoidal grande y ya que, como en el caso de música clásica, las pistas tenderían a ser largas, es decir, que se extienden sobre varios segmentos y por lo tanto pueden ser más sensibles a la mezcla aleatoria que, por ejemplo, algunas formas de música popular más moderna. Así, la clave y por lo tanto, la correspondencia utilizada para realizar la mezcla aleatoria pueden seleccionarse en consecuencia.

Finalmente, en el multiplexor 15, se constituye una corriente de audio AS que incluye los códigos CT, CSe y CN. La corriente AS de audio se proporciona a por ejemplo, un bus de datos, un sistema de antena, un medio de almacenamiento etc. Por lo tanto, se verá que sólo se transmite o almacena la versión encriptada de la señal.

La figura 2 muestra un reproductor 3 de audio según la invención. Se obtiene una corriente AS' de audio, generada por un codificador según la figura 1 o por un codificador sin mezcla aleatoria, del bus de datos, sistema de antena o medio de almacenamiento etc. La corriente AS de audio se demultiplexa en un demultiplexor 30 para obtener los códigos CT, CSe y CN. Los códigos CT y CN se proporcionan a un sintetizador 31 transitorio y un sintetizador 33 de ruido respectivamente tal como en la solicitud de patente europea nº 00200939.7. Desde el código CT transitorio, las componentes de señal transitoria se calculan en el sintetizador 31 transitorio. En caso de que el código transitorio indique una función de forma, la forma se calcula basándose en los parámetros recibidos. Además, el contenido de la forma se calcula basándose en las frecuencias y amplitudes de las componentes sinusoidales. Si el código CT transitorio indica un escalón, entonces no se calcula ningún transitorio. La señal yT transitoria total es una suma de todos los transitorios.

Si se utiliza el encuadre adaptativo, entonces desde la posiciones transitorias, se calcula una segmentación para la síntesis SS 32 sinusoidal y la síntesis NS 33 de ruido. El código CN de ruido se utiliza para generar una señal yN de ruido. Para hacer esto, las frecuencias de espectro lineal para el segmento de trama se transforman primero en parámetros (p_i , q_i) de filtración ARMA dedicados para la frecuencia a la que el sintetizador de ruido genera ruido blanco y éstos se combinan con los valores de ruido blanco para generar el componente de ruido de la señal de audio. En cualquier caso, se añaden segmentos de trama posteriores mediante, por ejemplo, un método de solapamiento-adición.

Según la presente invención, sin embargo, si está disponible una clave de descifrado, se asume que los códigos CSe se han mezclado aleatoriamente y se alimentan primero en un módulo 38 de descifrado. El módulo de descifrado aplica la clave, adquirida a través de técnicas de transacción convencionales, a los códigos CSe encriptados para producir códigos CS sin mezclar aleatoriamente. Se observará que una vez que se proporciona la clave correcta al decodificador y por lo tanto, al módulo 38 de descifrado, no es necesario de otra forma que el decodificador sepa que la corriente de bits se ha mezclado aleatoriamente o la correspondencia particular que se ha elegido al codificar la señal.

Si no está disponible ninguna clave, por ejemplo, cuando la corriente de bits no se ha mezclado aleatoriamente o cuando la clave simplemente no se ha obtenido, entonces, el código CS sinusoidal, no alterado de los códigos CSe proporcionados, se utiliza para generar la señal yS, descrita como una suma de sinusoides en un segmento dado.

Si la corriente de bits no se ha mezclado aleatoriamente, entonces se sintetizará a su calidad muestreada original, ya que presumiblemente no se habrá proporcionado ninguna clave.

Por otro lado, si la clave correcta está disponible para una señal mezclada aleatoriamente, entonces se generan los códigos CS sinusoidales correspondientes a los códigos originales producidos por el analizador 130 de códigos y éstos pueden proporcionarse al sintetizador 32 para generar la señal yS.

La señal y(t) total comprende la suma de la señal yT transitoria y el producto (g) de cualquier descompresión de amplitud y la suma de la señal yS sinusoidal y la señal yN de ruido. El reproductor de audio comprende dos sumadores 36 y 37 para sumar las señales respectivas. La señal total se proporciona a una unidad 35 de salida que es por ejemplo un altavoz.

Por lo tanto, cuando no está disponible ninguna clave o se utiliza la clave errónea, se obtendrá una señal y(t) degradada en comparación con la señal x(t) muestreada originalmente. Por otro lado, si se utiliza la clave correcta, la componente sinusoidal de la señal y(t) se sintetizará con la calidad muestreada original produciendo así la señal total con la calidad original.

La figura 3 muestra un sistema de audio según la invención que comprende un codificador 1 de audio tal como se muestra en la figura 1 y un reproductor 3 de audio tal como se muestra en la figura 3. Un sistema de este tipo ofrece la reproducción y grabación de características, pero impide la copia no autorizada de material de calidad original. La corriente AS de audio encriptada se proporciona desde el codificador de audio al reproductor de audio sobre un canal 2 de comunicación, que puede ser una conexión inalámbrica, un bus de datos o un medio de almacenamiento. En caso de que el canal 2 de comunicación sea un medio de almacenamiento, el medio de almacenamiento puede fijarse en el sistema, o también puede ser un disco extraíble, un dispositivo de almacenamiento de estado sólido tal como un Memory Stick™ de Sony Corporation, etc. El canal 2 de comunicación puede ser parte del sistema de audio pero, sin embargo, frecuentemente estará fuera del sistema de audio.

Se observará que también son posibles otras variaciones de la realización preferida. Por ejemplo, mientras que por un lado el componente CN de ruido normalmente contribuye con una componente relativa-

mente pequeña de la señal global y por lo tanto, su ausencia puede no resultar ser inaceptable a un oyente, la mezcla aleatoria de la componente de ruido para, por ejemplo, desviar de manera aleatoria las frecuencias espectrales de la componente de ruido de la señal puede proporcionar el efecto requerido. Así, un módulo (no representado) de cifrado puede disponerse entre el analizador 14 de ruido y el multiplexor 15 de manera adicional o alternativa al módulo 18. A continuación, dentro del codificador, un módulo (no representado) de descifrado correspondiente se dispone de manera adicional o alternativa entre el demultiplexor 30 y el sintetizador 33 de ruido para desenmarañar (si se proporciona una clave) los códigos de ruido de la corriente de bits.

Además, mientras que por un lado, las componentes CT transitorias típicamente se codifican solamente de manera periódica dentro de la corriente de bits y por lo tanto, su ausencia puede no resultar ser inaceptable a un oyente, una vez más la mezcla aleatoria de la transitoria para, por ejemplo, desviar de manera aleatoria los parámetros de frecuencia y amplitud de los parámetros sinusoidales que están ponderados mediante la función de envolvente pueden proporcionar el efecto requerido. Así, un módulo (no representado) de cifrado puede disponerse entre el analizador 111 transitorio y el multiplexor 15 de manera adicional o alternativa al módulo 18 y/o cualquier módulo de mezcla aleatoria de ruido. Dentro del codificador, un módulo (no representado) de descifrado correspondiente se dispone de manera adicional o alternativa entre el demultiplexor 30 y el sintetizador 33 transitorio para desembrollar (o no) los códigos transitorios de la corriente de bits.

También debería notarse, que en la implementación de la invención, la mezcla aleatoria de los códigos CS, CT o CN puede ocurrir antes o después de cualquier cuantificación del código realizada antes de la multiplexión.

Además, tal como se ha mencionado anteriormente, los dos módulos de cifrado y descifrado pueden funcionar de varias maneras. Por lo tanto, por ejemplo, no es necesario que la clave simplemente se aplique de manera directa a la corriente de bits, sino que de hecho, puede utilizarse para encriptar y desencriptar una correspondencia para mezclar aleatoriamente o desembrollar la señal. Sin embargo, la correspondencia compuesta y la clave pueden concebirse como la clave de la invención.

La presente invención encuentra aplicación cuando se desea la gestión de derecho de reproducción de audio comprimido, por ejemplo, SSA ("Solid State Audio", audio de estado sólido), EMD ("Electronic Music Distribution", distribución de música electrónica), Super distribución e Internet.

Se observa que la presente invención puede implementarse en hardware dedicado, en software que funciona sobre un DSP (procesador de señal digital) o un ordenador de uso general. La presente invención puede realizarse sobre un medio tangible tal como un CD-ROM o un DVD-ROM que lleva un programa informático para ejecutar un método de codificación según la invención. La invención también puede realizarse como una señal transmitida sobre una red de datos tal como Internet o una señal transmitida por un servicio de radiodifusión.

Debería notarse que las realizaciones mencionadas anteriormente ilustran más que limitan la inven-

ción y los expertos en la técnica serán capaces de diseñar muchas realizaciones alternativas sin desviarse del ámbito de las reivindicaciones adjuntas. En las reivindicaciones, cualquier signo de referencia colocado entre paréntesis no se interpretará como limitativo de la reivindicación. La palabra “que comprende” no excluye la presencia de otros elementos o etapas que aquellos enumerados en la reivindicación. La invención puede implementarse mediante hardware que comprenden diversos elementos bien diferenciados y mediante un ordenador programado adecuadamente. En una reivindicación de dispositivo que enumera varios medios, varios de estos medios pueden realizarse por un único mismo elemento de hardware. El mero hecho de que se enumeren ciertas mediadas en reivindicaciones dependientes mutuamente diferentes no indica que no pueda utilizarse una combinación de estas mediadas de manera ventajosa.

Como resumen, se proporciona una codificación de una señal de audio donde la corriente de bits codificada comprende una representación paramétrica de la señal de audio. Una componente de la representación paramétrica comprende pistas de componentes sinusoidales enlazadas donde las componentes enlazadas posteriormente se codifican de manera diferencial de parámetros de componentes de señales enlazadas ya determinadas. El codificador mezcla aleatoriamente los valores de frecuencia y/o amplitud codificados de manera diferencial mediante la correspondencia de valores diferenciales con otros valores diferenciales. Mediante la modificación de estos valores, la corriente de bits todavía puede decodificarse pero da como resultado pistas con variación de frecuencia y/o amplitud aleatoria. Por consiguiente, la señal se degradará.

REIVINDICACIONES

1. Método de codificación (1) de una señal (x) de audio, comprendiendo el método las etapas de:

- muestrear la señal (x) de audio para generar valores (x(t)) de señal muestreados;
- analizar (13, 14) los valores de señal muestreados para generar una representación paramétrica de la señal de audio, comprendiendo la señal paramétrica parámetros (C_S) sinusoidales y parámetros (C_N) de ruido;
- encriptar (18) al menos algunos de los parámetros de dicha representación paramétrica; y
- generar (15) una corriente (AS) de audio codificada que incluye dicha representación paramétrica encriptada que es representativa de dicha señal de audio y permite que dicha señal de audio se sintetice a un nivel de calidad inferior que el que se produciría utilizando una representación paramétrica descryptada.

2. Método según la reivindicación 1, que además comprende las etapas de:

- modelar (13) una componente de señal sostenida de la señal de audio mediante
 - a) la determinación de pistas representativas de componentes de señal enlazadas presentes en segmentos de señal sucesivos, y
 - b) la extensión de pistas en base a parámetros de componentes de señal enlazadas ya determinadas.

en el que dicha etapa de encriptación comprende la mezcla aleatoria de los parámetros de dichas componentes de señal enlazadas con una clave criptográfica.

3. Método según la reivindicación 2, en el que los parámetros para una primera componente de señal en una pista incluye un parámetro representativo de una frecuencia absoluta de dicha componente de señal y en el que dicha etapa de encriptación comprende la mezcla aleatoria de los parámetros de segmentos de señales posteriores con dicha clave criptográfica.

4. Método según la reivindicación 3, en el que dichos parámetros de segmentos de señales posteriores comprenden valores de amplitud y frecuencia diferenciales de parámetros de componentes de señal enlazadas ya determinadas y en el que dicha etapa de encriptación comprende la mezcla aleatoria de dichas diferencias de amplitud y/o frecuencia.

5. Método según cualquiera de las reivindicaciones anteriores, en el que dicha etapa de generación proporciona una representación paramétrica independiente de una primera frecuencia de muestreo permitiendo así que dicha señal de audio se sintetice independientemente de dicha primer frecuencia de muestreo.

6. Método según cualquiera de las reivindicaciones anteriores, que además comprende la etapa de:

- modelar (14) una componente de ruido de la señal de audio mediante la determinación de parámetros (p_i , q_i) de filtro de un

filtro que tienen una respuesta de frecuencia que se aproxima a un espectro objetivo de la componente de ruido.

7. Método según la reivindicación 6, en el que dicha etapa de encriptación comprende la mezcla aleatoria de dichos parámetros de filtro.

8. Método según la reivindicación 6 ó 7, que comprende la etapa de convertir los parámetros de filtro en parámetros independientes de la primera frecuencia de muestreo.

9. Método según la reivindicación 8, en el que dichos parámetros de filtro son parámetros autoregresivos (p_i) y de media móvil (q_i) y dichos parámetros independientes son indicativos de frecuencias de espectro lineal.

10. Método según la reivindicación 8 ó 9, en el que dicha etapa de encriptación comprende la mezcla aleatoria de dichos parámetros independientes.

11. Método según la reivindicación 9 ó 10, en el que dichos parámetros independientes se representan en una de las frecuencias absolutas o una escala Bark o una escala de ERB.

12. Método según cualquiera de las reivindicaciones anteriores que además comprende las etapas de:

- estimar (110) una posición de una componente de señal transitoria en la señal de audio; y
- hacer una correspondencia (111, 112) de una función de forma que tiene parámetros de forma y un parámetro de posición respecto a dicha señal transitoria;

en el que dicha etapa de encriptación comprende la mezcla aleatoria de dichos parámetros de posición y/o forma; y

en el que dicha etapa de generación incluye los parámetros de posición y forma encriptados en dicha corriente (AS) de audio.

13. Método según la reivindicación 12, en el que dicho parámetro de posición es representativo de una ubicación de tiempo absoluto de dicha componente de señal transitoria en dicha señal (x) de audio.

14. Método según la reivindicación 12 ó 13, en el que dicha etapa de correspondencia es receptiva a que dicha componente de señal transitoria sea un cambio tipo escalonado en amplitud para proporcionar una función de forma que indica un transitorio escalonado.

15. Método de decodificación de una corriente de audio obtenido mediante el método de codificación de la reivindicación 1, que comprende las etapas de:

- leer una corriente (AS') de audio codificada, esta corriente de audio es representativa de una señal (x) de audio e incluye una representación paramétrica de la señal de audio, comprendiendo la representación paramétrica parámetros (C_{Se}) sinusoidales y parámetros (C_N) de ruido;
- receptivo a la disponibilidad de una clave, descifrar (38) al menos algunos de los parámetros de dicha representación paramétrica con dicha clave, y
- emplear (32, 33) dicha representación (C_S , C_N) paramétrica descryptada para sintetizar dicha señal de audio.

16. Codificador (1) de audio que comprende:

- un muestreador para muestrear la señal (x) de audio para generar valores (x(t)) de señal muestreados; 5
- un analizador (13, 14) para analizar los valores de señal muestreados para generar una representación paramétrica de la señal de audio, comprendiendo la representación paramétrica parámetros (C_S) sinusoidales y parámetros (C_N) de ruido; 10
- un módulo (18) de encriptación para la mezcla aleatoria de al menos algunos de los parámetros de dicha representación paramétrica; y 15
- un generador de corriente de bits para generar (15) una corriente (AS) de audio codificada que incluye dicha representación paramétrica encriptada que es representativa de dicha señal de audio y permite que dicha señal de audio se sintetice a partir de dicha corriente de audio codificada a un nivel de calidad inferior que el que se produciría utilizando una representación paramétrica no encriptada. 20 25

17. Reproductor (3) de audio que comprende:

- medios para leer una corriente (AS') de audio codificada recibida del codificador de audio de la reivindicación 16, esta 30

corriente de audio es representativa de una señal (x) de audio e incluye una representación paramétrica de la señal de audio, comprendiendo la representación paramétrica parámetros (C_{Se}) sinusoidales y parámetros (C_N) de ruido

- medios, receptivos a la disponibilidad de una clave, para descifrar (38) al menos algunos de los parámetros de dicha representación paramétrica con dicha clave, y
- un sintetizador (32, 33) dispuesto para emplear dicha representación (C_S , C_N) paramétrica descifrada para sintetizar dicha señal de audio.

18. Sistema de audio que comprende un codificador (1) de audio según la reivindicación 16 y un reproductor (2) de audio según la reivindicación 17.

19. Corriente (AS) de audio que comprende parámetros parcialmente encriptados de una representación paramétrica de una señal de audio, comprendiendo la representación paramétrica parámetros (C_{Se}) sinusoidales y parámetros (C_N) de ruido y permitiendo que dicha señal de audio se sintetice a partir de dicha corriente de audio a un nivel de calidad inferior al que se produciría utilizando una representación paramétrica no encriptada.

20. Medio de almacenamiento en el que se almacena una corriente (AS) de audio según la reivindicación 19.

35

40

45

50

55

60

65

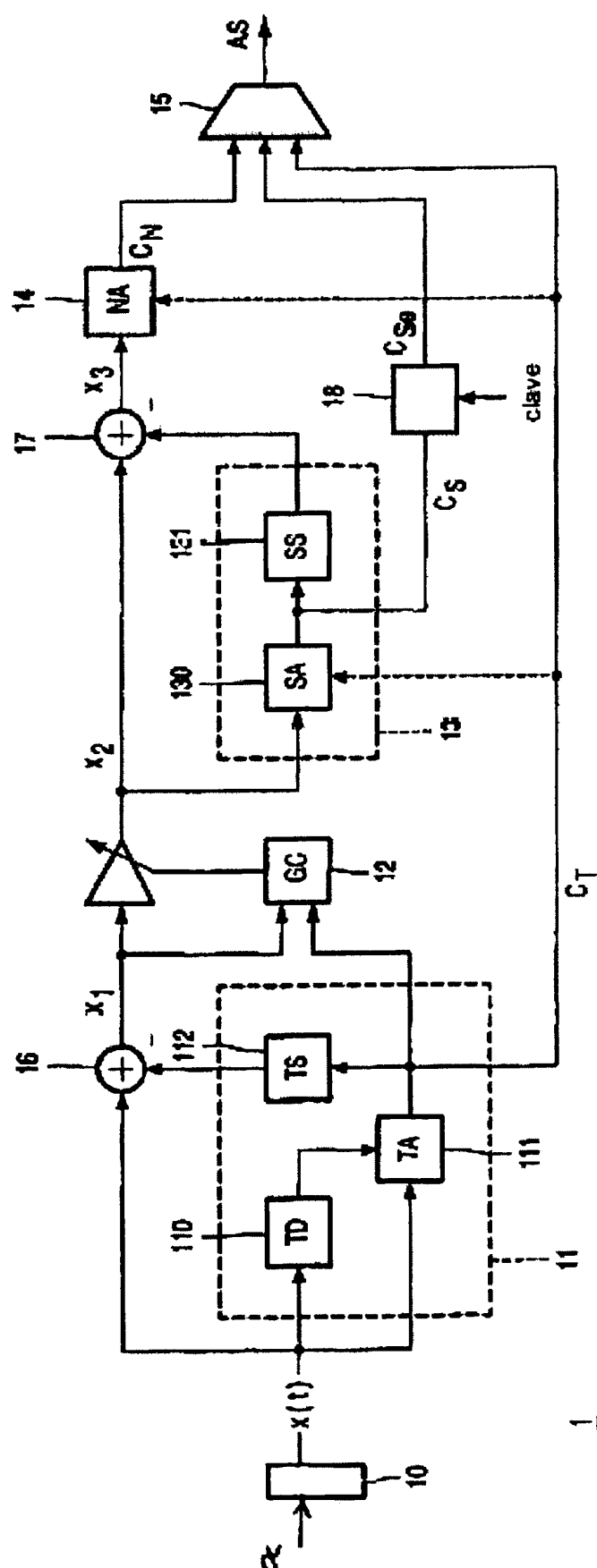


FIG. 1

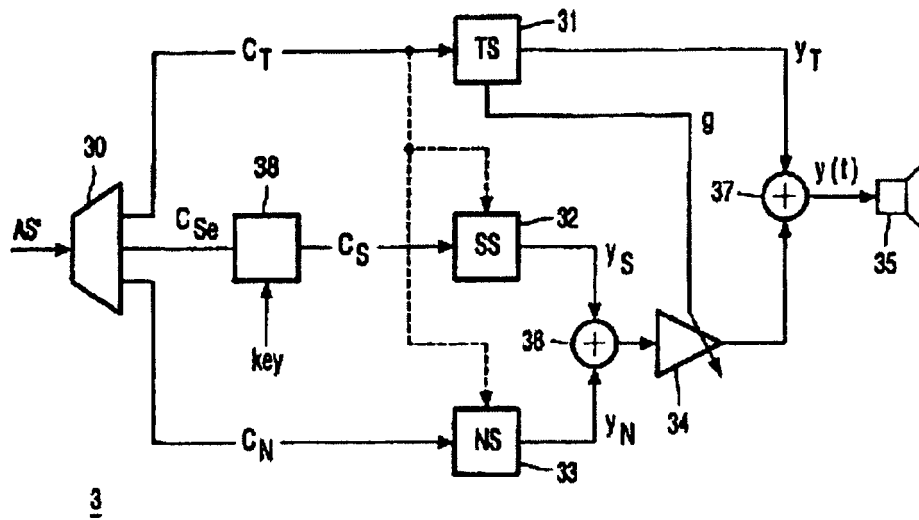


FIG. 2

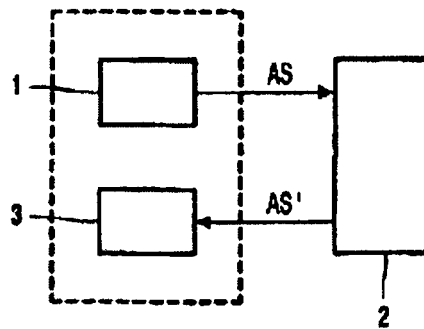


FIG. 3