(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 389 012**

(51) Int. CI.:
G10L 19/00 (2006.01)
G10L 19/12 (2006.01)
H04K 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07801969 .2**
(96) Fecha de presentación: **29.08.2007**
(97) Número de publicación de la solicitud: **2062254**
(97) Fecha de publicación de la solicitud: **27.05.2009**

(54) Título: **Esteganografía en codificadores de señales digitales**

(30) Prioridad:
15.09.2006 DE 102006044181
16.02.2007 DE 102007007627

(45) Fecha de publicación de la mención BOPI:
22.10.2012

(45) Fecha de la publicación del folleto de la patente:
22.10.2012

(73) Titular/es:
TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
164 83 Stockholm , SE

(72) Inventor/es:
GEISER, BERND y
VARY, PETER

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Esteganografía en codificadores de señales digitales.

La invención está dirigida a un método para incorporar una información esteganográfica en una señal de información de un codificador de señal.

Además de la transmisión analógica de audio, de imagen y de vídeo, la transmisión digital gana más y más peso. Esto es en parte también porque la información digital de la señal se procesa más fácilmente, es decir puede ser copiada o comprimida. En particular, la compresión de señales de información digitales lleva a que pueden ser transmitidas por medio de canales de transmisión la información con limitada velocidad de transferencia con alta densidad de información.

Además de la compresión de la información de la señal, como una forma de tratamiento se ha impuesto recientemente también incorporar información esteganográfica "invisible" dentro de la información de la señal. Esta incorporación de información adicional, por ejemplo, permite la identificación de derechos de copyright - si de la información de la señal se trata por ejemplo de una pieza de música - o, más en general, a una indicación general de origen, es decir una "marca de agua digital".

Aunque este tipo de incorporación de información esteganográfica en señales de música y/o de video ha sido ampliamente adoptada, la incrustación de información esteganográfica en una información de la señal codificada, sobre todo cuando se transmite en "tiempo real", continúa estando conectada con dificultades. Esto es debido al hecho de que algunos códigos no tienen redundancia, y por lo tanto no hay espacio para la información esteganográfica, o que la información esteganográfica se pierde durante la decodificación de la señal de información codificada.

Una situación inicial de este tipo en la que información de señal en el caso dado principalmente información de lenguaje se transmite y se recibe a través de un canal, y se codifican y decodifican en tiempo real, y en los que no están disponibles recursos de transmisión ilimitados, por ejemplo, se encuentra en la telefonía móvil. Aquí la red GSM permite en el mejor de los casos una velocidad de transferencia de hasta 13,0 kbit/s. Una información de lenguaje sin codificar, es decir una información de voz no comprimida sería difícil de entender debido a la velocidad de transmisión muy baja en el lado receptor. Con el fin de transmitir información de señal entendible, por ejemplo, de un dispositivo móvil a otro, han surgido denominados los códigos de voz como un medio eficaz de transmisión comprimida señal de voz. Si se debe incrustar información adicional, es decir, la información esteganográfica dentro de tal información de la señal, entonces hay que tener en cuenta de las características resultantes de codificación.

En el sector de las telecomunicaciones móviles, por ejemplo, en las redes inalámbricas de telefonía móvil GSM (Sistema Global para Comunicaciones Móviles) - o red de telefonía móvil UMTS (Universal Mobile Telecommunications Standard) – se codifica información de voz a transferir por medio de la CELP conocida (Code-book Excited Linear Predictive Coding) o ACELP (predicción lineal de código algebraico excited) o en el futuro, la codificación AMR (Adaptive Multi-Rate). Estos códigos de lenguaje se basan todos en un modelo de producción del habla, en el que se produce en una primera aproximación, la formación de la señal de voz en un paso de excitación y una etapa de filtración.

Un codificador de señal, tal como un codificador CELP, un codificador ACELP o un codificador AMR genera una entrada de libro de códigos, generalmente un vector a partir de un libro de códigos, en donde los elementos de código de la entrada libro de códigos - esto es, en general, los componentes del vector - contienen información relativa a la excitación (filtro). Coeficientes del filtro, los factores de amplificación, etc. se codifican como información en tiempo a través de libros de códigos dedicados.

Un libro de códigos para la codificación de excitación es generalmente un conjunto de vectores, por ejemplo con 10 componentes en el ACELP según el estándar de velocidad completa mejorada (FIR) estándar, que codifican la información de voz a transmitir durante una longitud determinada, por ejemplo, 5 milisegundos. Desde el libro de códigos fijo predeterminado, que en total abarca una amplia variedad de vectores, en donde los vectores se construyen de acuerdo con criterios conocidos, generalmente se utiliza un subconjunto de la tabla de codificación, un sublibro de códigos, que es a menudo suficiente para que la información de voz normal es transferida a una buena calidad.

Para distinguir en el marco de la codificación entre el libro de código completo fijado se refiere al libro de subcódigo que se utiliza en la práctica como "un libro de códigos práctica".

Para encontrar rápidamente una entrada de libro de códigos adecuados se busca solamente de forma heurística el libro de códigos, es decir, no se lleva a cabo una búsqueda completa de un registro de código adecuado.

Un método que tiene en cuenta la descomposición de un libro de códigos fijo se revela en el artículo "Water-marking

Combined with CELP Speech Coding for Authentification" por Zhe-Ming Lu y col. (en IEICE TRANS. INF. & SYST., Vol. E88-D, no. 2, Febrero del 2005). En primer lugar, un libro de códigos se descompone en tres sublibros de códigos, de los que se generan de nuevo dos libros de códigos, que tienen propiedades diferentes. Dependiendo de la información esteganográfica a transmitir, ahora se elige un libro de códigos de entrada del designado sublibro de códigos y se utiliza para codificar la información de voz a ser transmitida. Esta información de voz puede ser decodificado en el lado del receptor, en donde el decodificador real también puede detectar simultáneamente, de qué descomposición del libro de códigos proviene la entrada del libro de códigos. Para proporcionar una codificación suficientemente buena para partir de uno de los sublibros de códigos, se describe en la publicación también el método bien conocido del análisis por síntesis. En este método, la palabra de código seleccionado se evalúa, es decir se comprueba la calidad de la codificación. Esto se realiza esencialmente en que, después de una información de voz se ha codificado, se codifica, es decir, se sintetiza la codificación, y el resultado de decodificación, que a su vez representa la información de voz se compara con la información del habla original. Así, antes de enviar en el lado de emisor – lado del codificador – se realiza una síntesis que se realiza asimismo en el lado de receptor después de una posible trasmisión. Con tal un bucle de análisis por síntesis, es posible encontrar una palabra de código, es decir por lo general un vector a partir de un libro de códigos que por una parte presenta la propiedad deseada, es decir proveniente del sublibro de código y en este caso codifica a información de voz con una calidad suficiente.

Parece, sin embargo, que la división de un libro de códigos de práctico - que es de hecho ya un subconjunto de un libro de códigos de mayor importancia - en varios sublibros de códigos, reduce el número de palabras de código utilizadas de cada sublibro de códigos de tal manera que no se descarta una reducción notable en la calidad de voz.

El documento JP 11 272 299 A describe un método para incorporar un bit de marca de agua en el contexto de una codificación del habla basada en ACELP. En este contexto, se selecciona una cuarta posición de pulso m_3, que corresponde al bit de marca de agua a incorporar, de un número de posibles candidatos. Candidatos no adecuados bien se producen y se consideran, en principio, pero se rechazan a continuación un paso de verificación.

La publicación de Nicolas Chetry y de Mike Davies “Embedding side information into a speech doce residual” conferencia europea de procesamiento de señales, 4 de septiembre de 2006 (04/09/2006), 8 de septiembre de 2006, Florencia, Italia, se conoce un método para incorporar información de páginas en el contexto de una codificación la voz. En este contexto, el libro de códigos de un cuantificador se divide en dos sublibros de códigos, en donde a uno de los dos libros de códigos se le asigna un "1" lógico y al otro se le asigna a un "0" lógico. Al seleccionar uno de los dos sublibros de códigos, por lo tanto, se puede incorporar un "1" lógico o un "0" lógico como información de página en el contexto de codificación de voz.

La invención se basa por lo tanto en el objeto de proporcionar una solución que hace posible incorporar una información esteganográfica en una información de señal de un codificador de señal de tal manera que se evita en gran parte una reducción en la calidad de la voz.

Este objeto se consigue mediante un método según la reivindicación 1, así un codificador de señales según la reivindicación 17. En el lado receptor, este objeto se consigue por un método según la reivindicación 21, así como un dispositivo según la reivindicación 23. Las reivindicaciones dependientes se refieren a realizaciones ventajosas y desarrollos de los métodos o bien de los dispositivos.

En un método para incorporar una información esteganográfica en una información de señal de un codificador de señal se consigue el objeto de acuerdo con la invención proporcionando una información de datos, en particular, una información del habla, la selección de una información esteganográfica de un conjunto de informaciones esteganográficas, generando una palabra de código de un libro de código proporcionado por medio de un codificador de señal en base a los elementos de las palabras de código que forman la palabra de código, de tal manera que el uso de la palabra código generado en el contexto de un estándar de transmisión asociable con el libro de códigos la información de datos se codifica información de señal que comprende la palabra de código y/o que hace referencia hacia la palabra de código, y que la palabra de código generada presenta una característica adicional, predecible en base a los elementos de código que forman la palabra de código, en el que la propiedad adicional representa la información esteganográfica.

Tal método para incrustar una información esteganográfica en una información de señal de un codificador de señales, en el que se genera una palabra de código de un libro de código proporcionado por medio de los codificador de señales basado en elementos de código que forman la palabra de código, permite proporcionar una palabra de código, que por un lado presenta una característica calculable, es decir, representa una información esteganográfica y, en segundo lugar, al mismo tiempo proporciona una información de señal que codifica para una información de datos, en particular, la información de voz. Debido a que no se realiza desde el principio, una descomposición del libro de códigos, sino que se genera en su lugar, una entrada libro de códigos, en concreto sobre la base de los elementos de código que forman la palabra de código, se puede tener en cuenta las palabras de código que no estaban en el libro de códigos práctico y/o la descomposición del libro de código práctico. Esto amplía considerablemente el número de elementos de código que se puede recurrir, de manera que se puede

proporcionar o bien a una descomposición en más sublibros de códigos en comparación con el estado de la técnica o bien en el caso de un número igual de sublibros de códigos una mejor calidad de voz en comparación con el estado de la técnica.

De forma preferente se lleva a cabo en una forma de realización de la invención, una revisión de la palabra código generada en el contexto de un estándar de transmisión asociable con el libro de códigos proporcionado por medio de una descodificación de la palabra de código y, posteriormente, comparación la información de datos descodificada con la información de datos original.

Esto tiene la ventaja de que la calidad de la palabra de código generado con respecto a la fidelidad de codificación-decodificación, es decir la pérdida de la calidad (lingüística) debido a la codificación y decodificación, se puede evaluar.

Además, se lleva a cabo preferiblemente en forma de realización del método según la invención de la generación de la palabra de código del libro de códigos mediante el codificador de señal en base a los elementos de código que forman la palabra de código, teniendo en cuenta la evaluación.

La consideración de la evaluación en la generación de palabras de código del libro de código proporcionado permite la generación de palabras de código que tienen una alta calidad de voz con respecto a la información que ha de codificarse.

En una realización de la invención está previsto el uso de un codificador y un libro de códigos basados en el estándar de transmisión GSM (Global System for Mobile Communications) y/o del estándar UMTS (Universal Mobile Telecommunicactions Standard).

Esto tiene la ventaja de que el método para incrustar una información esteganográfica puede ser utilizada también en redes de telefonía móvil.

Para otra realización de la invención está prevista la creación de una palabra de código basada en la codificación ACELP (Algebraic Code Excited Linear Prediction) - y/o la codificación AMR.

La alta prevalencia de la codificación ACELP permite el uso del método según la invención en muchas áreas de la tecnología, especialmente la telecomunicación móvil. Esto se aplica con vistas al futura por analogía a la codificación AMR.

Además, en una realización, se realiza el cálculo de la característica de la palabra de código como resultado de aplicar al menos una operación en al menos uno de los elementos de código que forman la palabra de código.

Por consiguiente, es posible, sobre la base de los elementos de código que forman la palabra de código utilizando al menos una operación, preferiblemente matemática, determinar una característica de la palabra de código, que representa la información esteganográfica.

Además, en la realización del método según la invención se realiza la provisión de la palabra de código de tal manera que la palabra de código cumple implícitamente la característica.

Esto tiene la ventaja de que una palabra de código se puede generar tal que cumple ya durante de su generación la característica que representa la información esteganográfica.

Además, en una realización del método de la invención, se realiza la selección de la información esteganográfica de tal manera que la información esteganográfica para mejorar la señal, especialmente para la transmisión de voz, se utiliza como una ampliación del ancho de banda artificial y/o una reducción de ruido.

Se ha encontrado que la información esteganográfica transferible de forma adicional puede ser utilizada, por ejemplo, para describir una característica de la información de datos a transmitir verdadera de manera que se puede utilizar la información esteganográfica para la mejora de la señala. Esto significa que – si se genera la palabra de código que codifica para la información de datos de acuerdo con el método según la invención - la pérdida marginal en la calidad de transmisión por la información adicional esteganográfica no sólo se puede compensar, sino puede ser compensado incluso en exceso.

Además, en una realización, la selección de la información esteganográfica se realiza de tal manera que la información esteganográfica se utiliza como una marca de agua digital.

Con el uso de la información esteganográfica como una marca de agua digital no sólo se puede identificar la originalidad y el origen de las informaciones de datos, pero también se pueden incorporar derechos de autor de la información de datos utilizando la información esteganográfica en la forma de una marca de agua digital. La

información de datos en el contexto del método según la invención apenas se ve afectada cualitativamente.

Otra realización de la invención, se realiza una transmisión a un receptor de la información de señal que comprende la palabra de código o que hace referencia a la palabra de código.

Ventajosamente, es posible mediante la transmisión a un receptor transmitir la información de datos y la información esteganográfica en la forma de una información de señal a través de una distancia espacial.

Además, en una realización del método según la invención se proporciona en el lado de la recepción una información de datos por medio de la descodificación de la palabra código en el contexto de un estándar de transmisión asociado con el libro de códigos proporcionado.

Por la descodificación de la palabra de código se pueden recuperar y se poder utilizar la información de datos contenida en la información de señal, así como la información esteganográfica.

Además, se lleva a cabo preferiblemente una realización del método según la invención en el lado de la recepción proporcionar la información esteganográfica por medio del cálculo de la propiedad adicional de la palabra de código en base al elemento de código que forma la palabra de código.

Dependiendo del diseño del receptor es posible calcular a la información esteganográfica, que está incluida en la información de señal. Esta posibilidad puede ser utilizada opcionalmente, es decir, los sistemas que no son capaces de calcular atrás la información esteganográfica, sólo extraen la información de datos de la información de señal, sin llegar a la información esteganográfica.

Finalmente, en una realización del método se detalla la ejecución del método en un dispositivo de telefonía móvil.

El método es particularmente adecuado para la transmisión de información de la señal, es decir, información de voz u otra información, por medio de dispositivos de telefonía móviles que son operables en una de telefonía móvil.

Los componentes anteriormente mencionados, así como los reivindicados y descritos para ser utilizados en los ejemplos de realización en cuanto a su tamaño, forma, diseño, selección de materiales y conceptos técnicos no son sujetos a condiciones particulares excepcionales de manera que los criterios de selección el bien conocidos en el campo de aplicación pueden ser aplicados sin restricción.

Otros objetos, características y ventajas del objeto de la invención resultan de las reivindicaciones dependientes, así como de la siguiente descripción de los dibujos adjuntos, en los cuales - como ejemplo – se representa una forma de realización preferida de la invención.

Para el método de codificación descrito de acuerdo con las realizaciones de la invención se proporcionan codificadores correspondientes, así como métodos correspondientes de descodificación y descodificadores correspondientes.

Figura 1 muestra un codificador 100 de acuerdo con una realización de la invención.
Figura 2 muestra un sistema de codificación / descodificación 200 de acuerdo con una realización de la invención.
Figura 3 muestra un codificador 300 de acuerdo con una realización de la invención.
Figura 4 muestra un codificador 400 de acuerdo con una realización de la invención.
Figura 5 muestra un libro de códigos 500, de acuerdo con una realización de la invención.

Al codificador 100 se le suministra con una señal 101que ha de codificarse, por ejemplo, una señal de voz 100. Además, al codificador 100 se le suministra datos 102 para ser incorporado. El codificador genera una señal codificada a partir de la señal que ha de codificarse 101, en la que están incrustados los datos 102 a incorporar, es decir, de la que un decodificador correspondiente puede determinar los datos 102 a incorporar.

La señal codificada 103 está, por ejemplo, transmite a un receptor, por ejemplo por medio de una red de ordenadores o por medio de una red de radio.

En la realización que se describe más adelante, se supone que el codificador 100 se utiliza en una red de telefonía móvil de acuerdo con GSM (Global System for Mobile Communications). En otras realizaciones de la invención, el codificador puede ser utilizado en el marco de una red de radio móvil de acuerdo con UMTS (Universal Mobile Telecommunications Standard), CDMA2000 (CDMA: Code Division Multiple Access) o se utiliza de acuerdo a FOMA (Freedom of Mobile Access).

En la realización se describirá más adelante, se supone que la señal 101 que ha de codificarse, es una señal de voz que debe ser codificada por el codificador 100 de acuerdo con un método de compresión de voz ACELP (Algebraic

Code Excited Linear Prediction) - por ejemplo de acuerdo con un método de compresión de voz ACELP - " tasa completa mejorada ", como se utiliza en una red móvil GSM.

En la realización que se describirá a continuación el codificador 100 utiliza un libro de códigos, que se define como sigue:

El libro de códigos C utilizado en esta realización es el libro de códigos de los códigos GSM EFR (Enhanced Full Rate) y viene dado por los vectores $\underline{c}$ las posiciones del pulso ACELP (en esta realización sin signo) para cada submarco de longitud 5 ms:

$$C = \{\underline{c} = (c_0, \ldots, c_9)\}$$

con

$$c_0, c_5 \in \{0,5,10,15,20,25,30,35\}, c_1, c_6 \in \{1,6,11,16,21,26,31,36\}$$

,

$$c_2, c_7 \in \{2,7,12,17,22,27,32,37\}, c_3, c_8 \in \{3,8,13,18,23,28,33,38\}$$

y

$$c_4, c_9 \in \{4,9,14,19,24,29,34,39\}$$

Una palabra de código $\underline{c}$ del libro de códigos (es decir, el conjunto de todas las palabras de código posibles) C es por lo tanto un vector con diez componentes, en donde cada componente describe una posición de un impulso dentro de un submarco. El libro de códigos C tiene en esta realización, una tamaño de 2 ^ (10 * Log_2 (8)) = 2 ^ 30 palabras de código.

En otra realización, los componentes de los vectores $\underline{c}$, según lo dispuesto en el EER, tienen un signo. El uso de componentes que tienen signo permite la incrustación de información mejorada. En una realización, por razones de complejidad se omite, sin embargo, a la utilización de componentes con signo.

El C libro de códigos, en una forma de realización se divide en dos sublibros de códigos C(1) y C(2) que por cada palabra de código en la señal codificada 103 se puede incrustar un bit de los datos 102a ser incorporados y, en consecuencia, se transmite un bit los datos 102 a incrustar se transmite por submarco, lo que en una duración de submarco de 5 ms corresponde a una velocidad de datos de 200 bits/s.

Las palabras de código de los sublibros de códigos difieren en que la suma de los componentes c_i de una palabra de código de uno de los sublibros de códigos es par y de la otro sublibro de códigos es impar. Por ejemplo, todas las palabras de código de C (1) satisfacen la condición

$$\sum_{i=0}^{9} c_i = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{9} c_i\right),$$

(es decir, la suma de los componentes es par) y todas las palabras de código de C (2) cumplen con la condición

$$\sum_{i=0}^{9} c_i = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{9} c_i\right) + 1$$

(es decir, la suma de los componentes es impar), donde trunc representa a la operación de redondeo, es decir, el redondeo al número entero más próximo.

Si un primer mensaje (en este ejemplo consta de un bit, por ejemplo el valor del bit 0) debe ser transmitido, se utiliza una palabra de código de C(1) para la codificación (los valores de la señal actuales de la señal 101que ha de codificarse) y si se debe transmitir una segundo mensaje (en este ejemplo consta de un bit, por ejemplo el bit de valor 1), entonces se utiliza una palabra de código de C(1) para la codificación. Un receptor o decodificador puede

determinar, basándose en la pertenencia de la palabra código recibido a C(1) o C(2) si se ha incrustado el primer mensaje o el segundo mensaje.

En otra realización, se realiza la subdivisión de C según la paridad par e impar de la suma de los componentes de las palabras de código. Por ejemplo, una palabra de código pertenece a C(1) si $\sum_{i=0}^{9} c_i$ en representación binaria presenta un número par de unos Ani=0 y por lo contrario pertenece a C(2).

En una realización, se incorporan cuatro bits por submarco y con esto se consigue una velocidad de datos de 400 bit/s. Esto se hace mediante una subdivisión del libro de códigos C en cuatro sublibros de códigos C(1) a C(4), en donde las palabras de código de los sublibros de códigos, por ejemplo, cumplen las siguientes condiciones:

$$C(1): \sum_{i=0}^{4} c_{2i} = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{4} c_{2i}\right),$$

$$C(2): \sum_{i=0}^{4} c_{2i+1} = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{4} c_{2i+1}\right),$$

$$C(3): \sum_{i=0}^{4} c_{2i} = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{4} c_{2i}\right) + 1$$

$$C(4): \sum_{i=0}^{4} c_{2i+1} = 2 \cdot \mathrm{trunc}\left(\frac{1}{2}\sum_{i=0}^{4} c_{2i+1}\right) + 1.$$

claramente es este caso la distinción que se hace sobre la base de la paridad o imparidad de la suma de los componentes con un índice par o impar.

De manera análoga a la alternativa anterior puede realizarse sobre la base de la paridad de una representación binaria de la suma de los componentes con índice par o impar, también en la subdivisión del libro de códigos C en cuatro sublibros de códigos, 4 4 por lo tanto, basado en la paridad de $\sum_{i=0}^{4} c_{2i}$ o bien $\sum_{i=0}^{4} c_{2i+1}$.

En las condiciones anteriores para los libros de códigos C(1) y C(2) o C(1) a C(4) alternativamente en lugar de un componente de C_i en sí, se puede utilizar la expresión trunc (C_i / 5), que designa de forma inequívoca una posición de impulso dentro de una denominada pista. Por otra parte, se puede utilizar también la respectiva versión codificada GRAY (c_i) o bien GRAY (trunc (c_i / 5)), tal como está previsto para la codificación de canal en la EER. Teniendo en cuenta la transmisión real de las palabras de código a través de un canal de radio móvil GSM, esta opción de descomposición libro de códigos resulta ser particularmente ventajosa. Esto asegura que las cantidades muy bajas de bits de canal tienen una influencia en los datos integrados, por lo que la tasa de errores de bits de datos transmitidos incrustados disminuye en una transmisión perturbada.

Por lo general, el libro de códigos C en una forma de realización puede ser descompuesto de tal manera que las palabras de código del sublibro de códigos que se utiliza para la codificación, cuando un bit de mensaje se debe transmitir, cumple con la condición $m_i = \bigoplus_{j \in A_i} b_j$, en donde A_i denota un conjunto índice, y b_j los componentes de cada palabra de código. La suma aquí se realiza en módulo 2, por lo que requiere que la suma de módulo 2 de varios bits de palabra de código b_j es igual a los bits de mensaje m_j es ser incrustados.

Con el fin de reconstruir un mensaje incrustado en una palabra de código recibida o a decodificar sólo es necesario que el decodificador determine a que al sublibro de códigos pertenece de la palabra de código. Si las palabras de

código se transmiten sin perturbaciones al descodificador, entonces también la información incrustada puede ser reconstruida sin error.

El procedimiento anteriormente descrito para incrustar información puede ser utilizada también con otros codificadores, por ejemplo, en todos los codificadores de voz CELP, pero también en otros codificadores de señales como los codificadores de vídeo, codificadores de imagen, etc.

La transmisión de información de página (información incrustada) por medio de esteganografía también puede ser utilizada para la mejora de la señal y proporciona una solución para el problema de dar la compatibilidad hacia atrás. Un receptor sin el conocimiento de la información incrustada puede descodificar la señal (voz), en la que ha incrustado la información, como de costumbre, es decir, como en el caso de cualquier incrustación de información con sólo pequeñas pérdidas. Si el receptor, sin embargo, conoce la información incrustada, entonces la información de la página se utiliza para la mejora de la señal. Una realización correspondiente se describe a continuación con referencia a la Figura 2.

La Figura 2 muestra un sistema de codificación/decodificación 200 de acuerdo con otra realización de la invención.

El sistema de codificación/decodificación 200 incluye un codificador 201 como se ha descrito con referencia a la Figura 1. De forma correspondiente al codificador 201 se le alimenta una señal 202 a codificar y datos 203 a incrustar. Los datos a incrustar se utilizan para la mejora de la señal y son generados consecuencia con un dispositivo de análisis de señal 204, al que se alimenta la señal 202 a codificar, en una forma adecuada para la mejora de la señal 202.

De manera análoga a la Figura 1 el codificador 201 emite una señal codificada 205 en la que están incrustados los datos 203 a incrustar. La señal codificada 205 ahora puede ser transmitida a un receptor, por ejemplo, como se ha descrito anteriormente, por medio de una red de radio de comunicación móvil.

Si el receptor presenta a un decodificador "convencional" 206, es decir, un decodificador que no puede determinar los datos incrustados a partir de la señal codificada 205, entonces el descodificar 206 decodifica la señal codificada 205 a una señal descodificada 207, que corresponde (con excepción de errores de transmisión y las pérdidas de codificación/decodificación) a la señal 202 codificada.

Si el receptor presenta una descodificador "extendido" 208, que es un decodificador que puede identificar los datos incrustados de la señal codificada 205, entonces se extraen los datos incrustado y se utilizan los datos extraídos 209 por una unidad de mejora de la señal 210 para el realce de la señal, que genera una señal 211 descodificada y (en comparación con la señal descodificada 207) y mejorada.

Como mejora de la señal puede utilizarse, por ejemplo, la extensión del ancho de banda artificial, o la reducción de ruido. Los coeficientes de un filtro de polo determinado en el lado emisor puede ser transmitidos a través de la esteganografía.

En particular, la aplicación de la extensión del ancho de banda artificial, es ventajosa porque la red telefónica está limitada históricamente a un ancho de banda acústico de 3,1 kHz (300Hz-3.4kHz), sin embargo, la transmisión de voz en banda ancha (50Hz-7 kHz) sólo se podría realizar con un esfuerzo enorme por parte de los operadores de redes y los fabricantes de terminales. Los cambios en la red de transmisión (móvil), sin embargo, para la realización de las realizaciones anteriormente descritas no son necesarios. Correspondientes (potentes) algoritmos de extensión de ancho de banda, por ejemplo, se describen en la publicación de Peter Jax, Bernd Geiser, Stefan Schandl, Hervé Taddei, y Peter Vary, "An Embedded Scalable Wideband Codec Base on the GSM EFR Codec ", en Actas de ICASSP, Toulouse, Mayo de 2006. Por otra parte, en la publicación de Peter Jax y Peter Vary, "Bandwidth Extention of Speech Signals: A Catalyst for the Introduction of Wideband Speech Coding?", IEEE Communications Magazine, vol. 44, nº 5, Mayo de 2006, se menciona la introducción de la transmisión de voz de banda ancha mediante el desvío de la expansión del ancho de banda (posiblemente con la ayuda de la marca de agua digital).

A continuación se describe otra posibilidad para una descomposición del libro de códigos C anteriormente definido (libro de códigos EFR ACELP).

El primer paso para el mejor entendimiento se explica brevemente la estrategia de búsqueda del código EFR:

1) En primer lugar, la primera posición del pulso i_0 Є {0, ... , 39} se determina heurísticamente y no se mueve durante toda la búsqueda. La "pista" correspondiente a i_0, por ejemplo, es x = 4 ó x = 9. Para el x-ésimo componente c_x de la palabra en código correspondiente es $c_x = i_0$.

2) La posición del segundo pulso i_1 Є {0, ..., 39} también se determina heurísticamente, suponiéndose para cada uno de las cuatro iteraciones del algoritmo a continuación (paso 3) un valor diferente. Por ejemplo, pertenecen a la primera iteración a la posición seleccionada de la pista i_1 y = 3 ó y = 8, es decir $c_y = i_1$.

3) Para las demás ocho pistas para cada una de cuatro iteraciones se optimizan los pulsos de forma sucesiva en pares de en cada caso dos pistas mediante una búsqueda exhaustiva. En cada una de las cuatro iteraciones las pistas se componen de nuevo mediante permutación, en donde c_x y c_y no se utilizan de nueva.

Por ejemplo, se lleva a cabo para el par de pistas c_0/c_6 la optimización de acuerdo con el pseudo código siguiente:

for (i = 0,5,10, ..., 35) / / iterar sobre todos los elementos que pueden integrar c_0
for (j = 1, 6, 11, ..., 36) / / iterar sobre todos los elementos que pueden integrar c_6
prueba el par de pulsos (i = c_0, c_6 = j) por el estado óptimo correspondiente al criterio CELP

En esta estrategia de búsqueda, de acuerdo con EFR se examina en total 1024 combinaciones (4 iteraciones * 4 pares de pistas * 8 posiciones de pulso = 1024 combinaciones), y se seleccionaron los pares de impulsos óptimos.

Para la incrustación de información en el siguiente ejemplo de un solo bit b (de marca de agua), en una palabra de código $\underline{c}$ = (c_0, ..., C_9), de acuerdo con una ejemplo de realización de la invención, el algoritmo anterior se modifica como se describe a continuación.

Si una búsqueda ya se determinó un pulso para una pista, por ejemplo, c_1, en la selección de la pista c_6 (de diseño idéntico) puede ser incrustado un bit de marca de agua b en el par de posiciones de pulso c_1 y c_6 , seleccionando c_6 dependiendo del bit b. La búsqueda por pares se modifica para ello, por ejemplo como sigue:

c6_offset = 5 * ((c1 + b + 1) mod 2)
for (i = 0,5,10, ..., 35) / / iterar sobre todos los elementos que pueden integrar c_0
for (j = 1,11,21,31) / / iterar sobre todos los elementos que pueden integrar c_6 (la mitad con respecto el número anterior)
prueba del par de pulso (c_0 = i, c_6 = j + c6_offset) correspondiente al estado óptimo del criterio CELP

El bit b incrustado se puede determinar en el receptor o descodificador a través de la operación

$$b = (c_1 + c_6) \bmod 2$$

En lugar c6_offset = 5 * ((C1 + b + 1) mod 2) también se pueden utilizar otras combinaciones de posiciones del pulso previamente determinados y bits b a incrustar. En el ejemplo anterior, el espacio de búsqueda para la posición del pulso c_6 se dividió en dos partes iguales (valores impar / par). Otras distribuciones (tales como la relación de valores de la primera mitad/ segunda mitad) también son posibles, donde la ecuación se ajusta para c6_offset en consecuencia.

El número de las combinaciones de posición de impulsos investigados ha disminuido de esta manera por el bit incorporado a

4 iteraciones * (3 pares * 8 posiciones * 8 posiciones + 1 par * 8 posiciones * 4 posiciones = 896 combinaciones,

Con el fin de integrar múltiples bits en una palabra de código $\underline{c}$ se puede reducir otra vez a la mitad el espacio de búsqueda de c_6, o se puede aplicar un procedimiento idéntico para un segundo par de pulso. Es ventajoso acoplar precisamente tales pulsos en el contexto de la incrustación de información por c6_offset (o el bit b), que se encuentran en una pista. De lo contrario, debido a la codificación con el signo de la EFR, no se puede realizar en el destinatario una asignación clara de los pulsos. Con el trabajo adicional correspondiente en el transmisor, esta restricción se puede levantar. En el receptor, c_1 y c_6 son indistinguibles unos de otros. La extracción de datos a través de b = (c1 + c6) mod 2 no tiene ningún problema, pero es difícil, por ejemplo, calcular b = (c1 + c5) mod 2, ya que (dependiendo del signo) "accidentalmente" se podría calcular b = (C6 + C5) mod 2. El "esfuerzo adicional" en el laso trasmisor consiste en tener en cuenta la codificación de signos en los bucles de optimización y realizarla por cada paso de optimización. A través del número reducido de combinaciones probadas (896 en lugar de 1024 en el ejemplo anterior) resulta una menor calidad de codificación mediante la inserción de la marca de agua. Esto puede ser compensado mediante una búsqueda más avanzada, es decir, una extensión del espacio de búsqueda. Para ello las pistas ya no se buscan en parejas, sino en grupos de 3 o 4 (o más) pistas juntas. La búsqueda conjunta (sin la incrustación de la marca de agua) para 3 pistas (por ejemplo, c_6 c_0, y c_7), por ejemplo, se realiza como sigue:

for (i2 = 0,5,10, ..., 35) / / iterar a través de los valores permitidos de c_0
for (i3 = 1, 6, 11, ..., 36) / / iterar a través de los valores permitidos de c_6
for (i4 = 2,7,12, ..., 37) / / iterar a través de los valores permitidos de c_7
buscar triple óptimo (c0 = i2, C6 = i3, C7 = i4)

Para cada uno de los triples, esto significa que serán de 8 * 8 * 8 = 512 combinaciones que se buscan. Si toda la

búsqueda de las 8 posiciones de pulsos variables (de acuerdo con los pasos 1 y 2 dos posiciones del pulso de hecho son fijos) se divide de manera que dos triples y un par se optimizan en conjunto, se deduce que

4 iteraciones * (2 triple * 8 posiciones * 8 posiciones * 8 posiciones + 1 triple * 8 posiciones * 8 posiciones) = 4352 combinaciones

se examinan, lo qué significa una carga significativa adicional comparado con las 1024 combinaciones según EFR.

Sin embargo, si por ejemplo en el curso de la optimización del primer triplete se incrustan 3 bits de marca de agua y en el curso de la optimización del segundo triple se incrustan 2 bits de marca de agua como se ha descrito anteriormente, mientras que no se realiza ninguna incrustación para el par de posiciones de pulso, entonces el número de combinaciones para ser examinados resulta en

4 iteraciones * (1 triple * 4 posiciones * 4 posiciones * 4 posiciones + 1 triple * 8 posiciones * 4 posiciones * 4 posiciones + 1 par * 8 posiciones * 8 posiciones) = 1024 combinaciones

es decir exactamente el número de combinaciones examinadas en el código EFR estándar. La velocidad de datos de marca de agua es en este caso está en (2 +3) bit/5 ms = 1 Kbit/s.

Finalmente, otra forma de ampliar el espacio de búsqueda es aumentar el número de iteraciones, es decir la investigación de otras permutaciones de pistas.

La idea en la que se basa un ejemplo de realización puede verse en que la incrustación de información es conocida por el codificador de señal, que se consigue mediante una incrustación de datos común y la codificación de la señal, esto significa que, por ejemplo, la incrustación de marca de agua se integra en el codificador. Esto puede hacerse dentro de un bucle de análisis por síntesis ("bucle cerrado"), tal como se muestra en la Figura 3.

La Figura 3 muestra un codificador 300 de acuerdo con otro ejemplo de realización de la invención.

Al codificador se le suministra una señal a codificar datos 302 a incrustar.

Una señal codificada 303 se genera a partir de la señal 301 a codificar por un bucle que tiene un libro de códigos 304, un sintetizador 305 y un comparador 306. Aquí, una codificación posible de la señal a codificar 301 se genera por el libro de códigos 304 y se comprueba por medio del sintetizador 305 y el comparador 306, lo bien que refleja la señal 301 a codificar y, opcionalmente, se modifica en base a la salida del comparador 306.

Los datos 302 a incrustar están incrustados durante el proceso de codificación en la señal codificada 303, por ejemplo, según uno de los procedimientos descritos anteriormente.

Por ejemplo, se seleccionan en base a los datos 302 a ser incorporados, un libro de códigos de subdel libro de códigos 304, como se muestra en la Figura 4.

La Figura 4 muestra un codificador 400 de acuerdo con otro ejemplo de realización de la invención.

En analogía con el codificador 300 mostrado en la Figura 3 se le alimentar al codificador datos 402 a incrustar y una señal 401 a codificar y genera una señal codificada 403 en la que los datos 402 a incrustar están incrustados. Además de un dispositivo de síntesis 405 y un comparador 406 análogo al codificador 300 en la Figura 3, el codificador 400 presenta una pluralidad de sublibros de códigos 404, pues, un libro de códigos dividido en varios sublibros de códigos 404. Basándose en los datos para ser incorporados son seleccionados los sublibros de códigos en la codificación de la señal 401 que ha de codificarse. Por ejemplo, una palabra de datos de la señal 401 a ser codificada se le asigna una palabra de código de un primer sublibro de códigos, cuando una primera información de página de los datos 402 a ser incorporado, por ejemplo, un bit con el valor 0, debe ser incorporado y se asigna una palabra de código de un segundo sublibro de códigos, cuando se debe incrustar una segunda información de página de los datos 402 a ser incorporado, por ejemplo, un bit que tiene el valor 1.

La división de un libro de códigos en varias sublibros de códigos se ilustra en la Figura 5.

La Figura 5 muestra un libro de códigos 500 de acuerdo con otro ejemplo de realización de la invención.

El libro de códigos 500 se denota por C. Por razones de eficiencia, cuando el tamaño de codificación del libro de códigos 500 es muy grande, en la codificación se examina sólo parcialmente el libro de códigos 500, es decir se seleccionan palabras de código para la codificación sólo de un subconjunto 501 del libro de códigos, que se denomina con C '(libro de códigos práctico).

En los ejemplos de realizaciones anteriores, el libro de códigos 500 para la incrustación de datos tal como se explicó

anteriormente se descompone en los libros de código, por ejemplo, en cuatro sublibros de códigos 502, que están denotados por C(1) a C(4).

Dado que un sublibro de códigos 502 tiene un tamaño de código inferior que el subconjunto 501 de libro de códigos y por lo tanto disminuiría la calidad de codificación de la señal (en función del número de sublibros de códigos 502) en relación con la utilización del subconjunto completo libro de códigos 501, en un ejemplo de realización se expande el tamaño de código de los sublibros de códigos 502, de manera que un total de utiliza un subconjunto expandido 503del libro de códigos para la codificación. Esto aumenta la complejidad algorítmica sólo ligeramente, la calidad de codificación no disminuye y, en casos especiales, incluso se puede conseguir un incremento de la calidad.

En una forma de realización, se utiliza un libro de códigos algebraico. A diferencia de un libro de códigos común en forma de tablas un libro de códigos algebraico sólo existe en el sentido de una especificación de diseño algebraica. Esto significa que las entradas individuales del libro de códigos (palabras de código) en el curso de la codificación de señales son generadas por un generador de palabras de código. El "Esquema Binning" para la incrustación de información, es decir, la descomposición del libro de códigos en sublibros de códigos y la selección del sublibro de códigos utilizado para la codificación en dependencia de la información de incrustar, en el caso de un codificador con libro de códigos algebraico ya no consiste sólo en la distribución del libro de códigos en un número de sublibros de códigos, sino también en la modificación del generador de palabras de código, en el sentido de que en cada caso sólo se emiten palabras de códigos pertenecientes al sublibro de códigos C(i) seleccionado por el mensaje i a ser incorporado actualmente.

REIVINDICACIONES

1. Un método de incorporar una información esteganográfica en una información de señal de un codificador de señal (100), **caracterizado por**

- proporcionar una información de datos, en particular, una información de voz, como señal para ser codificada (101),
- selección de una información esteganográfica como datos (102) para incrustar, en donde la información esteganográfica se selecciona de un conjunto de información esteganográfica,
- generación de una palabra de código de un libro de códigos algebraico proporcionado (500) en el sentido de una especificación de diseño algebraica mediante el codificador de señal (100) sobre la base de los elementos de palabras de código que forman la palabra de código, de tal manera que

  • utilizando la palabra de código generada en el marco de un estándar de transmisión asociable con el libro de códigos, se codifica la información de datos en una información de la señal que comprende la palabra de código y/o que hace referencia a la palabra de código como señal codificada (103), que
  • la palabra de código generada presenta una característica adicional, calculable sobre la base de los elementos de palabra de código que forman la palabra de código, en donde la característica adicional representa la información esteganográfica; y que
  • el libro de códigos (500) en el sentido de las especificaciones de diseño algebraicas se divide en un número de sublibros de códigos, y que por el codificador de señal (100) se emite en cada caso solo una palabra de código perteneciente al sublibro de códigos seleccionado por la información esteganográfica a incrustar actualmente.

2. Un método según la reivindicación 1, **caracterizado por** una evaluación de la palabra código generada en el contexto de un estándar de transmisión asociable con el libro de códigos proporcionado por medio de una descodificación de la palabra código y posterior comparación de la información de datos descodificada con la información de datos original.

3. Un método según la reivindicación 2, **caracterizado por** la generación de la palabra de código a partir del libro de códigos proporcionado mediante del codificador de señal (100) sobre la base de los elementos de código que forman la palabra de código, teniendo en cuenta la evaluación.

4. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** el uso de un codificador (100) y un libro de código sobre la base del estándar de transmisión GSM y/o UMTS.

5. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** la generación de una palabra de código basado en la codificación ACELP o AMR.

6. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** el cálculo de la característica de la palabra de código como resultado de aplicar al menos una operación en al menos un elemento de código que forma la palabra de código.

7. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** la disposición de la palabra de código de tal manera que la palabra de código cumple la característica de forma implícita.

8. Un método según la reivindicación 7, **caracterizado por** la generación de la palabra de código tal que cumple con la característica, que representa la información esteganográfica, ya durante su generación.

9. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** la selección de la información esteganográfica tal que la información esteganográfica en el extremo receptor se puede aplicar para la mejora de la señal, especialmente en el caso de transmisión de voz, como una expansión de ancho de banda artificial y/o reducción de ruido.

10. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** la selección de la información esteganográfica tal que la información esteganográfica se utiliza como una marca de agua digital.

11. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** una transmisión de la información de la señal que comprende la palabra de código o que referencia a la palabra de código hacia un receptor.

12. Un método de acuerdo con la reivindicación 11, **caracterizado por** proporcionar en el lado del receptor una información de datos por medio de la descodificación de la palabra de código bajo un estándar de transmisión asociable con el libro de códigos proporcionado.

13. Un método según la reivindicación 11 o 12, **caracterizado por** proporcionar en el lado del receptor la información esteganográfica por medio del cálculo de la característica adicional de la palabra de código en base a los elementos de código que forma la palabra de código.

14. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, **caracterizado por** la realización del método en un dispositivo de telefonía móvil.

15. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que al codificador de señal (100) se le suministra la información a incorporar.

16. Un método de acuerdo con una cualquiera de las reivindicaciones precedentes, en done el codificador de señal (100) determina un primer elemento de código y un segundo elemento de código de la palabra de código, en donde el segundo elemento de código se determina como una función del primer elemento de código y de la información a insertar.

17. Codificador de señal (100) para incrustar una información esteganográfica en una información de la señal del codificador de señal (100), **caracterizado por**

- medios para recibir una información de datos, en particular, una información de voz, como la señal para ser codificado (101),
- medios para recibir una información esteganográfica como datos (102) para incrustar, en donde la información esteganográfica se selecciona de un conjunto de información esteganográfica,
- medios para generar una palabra de código de un libro de códigos (500) algebraico proporcionado en el sentido de una especificación de diseño algebraica mediante el codificador de señal (100) sobre la base de los elementos de código que forman la palabra de código, de tal manera que

  • utilizando la palabra de código generada en el marco de un estándar de transmisión asociable con el libro de códigos, se codifica la información de datos en una información de la señal que comprende la palabra de código y/o que referencia la palabra de código como señal codificada (103), que
  • la palabra de código generada presenta una característica adicional calculable sobre la base de los elementos de código que forman la palabra de código, en donde la característica adicional representa de información esteganográfica, que
  • el libro de códigos (500) en el sentido de las especificaciones de diseño algebraica se divide en un número de sublibros de códigos, y que por el codificador de señal (100) se emite en cada caso solo una palabra de código perteneciente al sublibro de códigos seleccionado por la información esteganográfica a incrustar actualmente.

18. Codificador de señal según la reivindicación 17, adaptado para proporcionar la palabra de código de tal manera que la palabra de código cumple la característica de forma implícita.

19. Aparato según la reivindicación 18, adaptado para generar la palabra de código de tal manera que cumple la característica, que representa la información esteganográfica, ya durante su generación.

20. Aparato de acuerdo con una cualquiera de las reivindicaciones 17 a 19, en el que el codificador de señal (100) está diseñado para determinar un primer elemento de código y un segundo elemento de código de la palabra de código, en el que el codificador de señal (100) determina el segundo elemento de código como una función del primer elemento de código y de la información a incrustar.

21. Un proceso para proporcionar en el lado del receptor una información esteganográfica que ha incorporado por un codificador de señal (100) en una información de señal mediante la generación de una palabra de código de un libro de códigos algebraico proporcionado (500) en el sentido de una especificación de diseño algebraica mediante el codificador de señal (100) sobre la base de elementos de código que forman la palabra de código, de forma que

• utilizando la palabra de código generada en el marco de un estándar de transmisión asociable con el libro de códigos, se codifica los datos como señal (101) que debe codificarse en una información de señal que comprende la palabra de código y/o hace referencia a la palabra de código como una señal codificada (103), que
• la palabra de código generada presenta una característica adicional calculable sobre la base de los elementos de código que forma la palabra de código, en donde la característica adicional representa la información esteganográfica, y que
• el libro de códigos (500) en el sentido de las especificaciones de diseño algebraica se divide en un número de sublibros de códigos, y que por el codificador de señal (100) se emite en cada caso solo una palabra de código perteneciente al sublibro de códigos seleccionado por la información esteganográfica a incrustar actualmente;

en donde el proporcional de la información esteganográfica en el lado receptor comprende calcular la característica adicional de la palabra de código en base a los elementos de código que forman la palabra de código.

22. El método de la reivindicación 21, en donde en el extremo receptor se determinan un primer elemento de código y un segundo elemento de código de la palabra de código, en donde la información esteganográfica se determina como una función del primer elemento de código y del segundo elemento de código.

23. Un aparato (208) para proporcionar una información esteganográfica en el lado del receptor que se ha incorporado por un codificador de señal (100) en una información de señal mediante la generación de una palabra de código de un libro de códigos algebraico (500) proporcionado en el sentido de una especificación de diseño algebraica mediante el codificador de señal (100) basado en los elementos de código que forman la palabra de código, de tal manera que

- utilizando la palabra de código generada en un marco de un estándar de transmisión asociable con el libro de códigos, se codifica una información de datos como señal (101) que debe codificarse en una información de señal que comprende la palabra de código y/o que hace referencia a la palabra de código como señal codificada (103); que
- la palabra de código generada tiene una característica adicional, calculable sobre la base de los elementos de código que forman la palabra de código, en donde la característica adicional representa la información esteganográfica; y que
- el libro de códigos (500) en el sentido de las especificaciones de diseño algebraica se divide en un número de sublibros de códigos, y que por el codificador de señal (100) se emite en cada caso solo una palabra de código perteneciente al sublibro de código seleccionado por la información esteganográfica a incrustar actualmente;

en donde dicho aparato (208) está configurado para proporcionar en el lado del receptor la información esteganográfica mediante el cálculo de la característica adicional de la palabra de código en base a los elementos de código que forman la palabra de código.

24. El aparato según la reivindicación 23, que está configurado para determinar en el lado del receptor de un primer elemento de código y un segundo elemento de código de la palabra de código, así como para determinar la información esteganográfica en dependencia del primer elemento de código y el segundo elemento de código.

Fig. 1

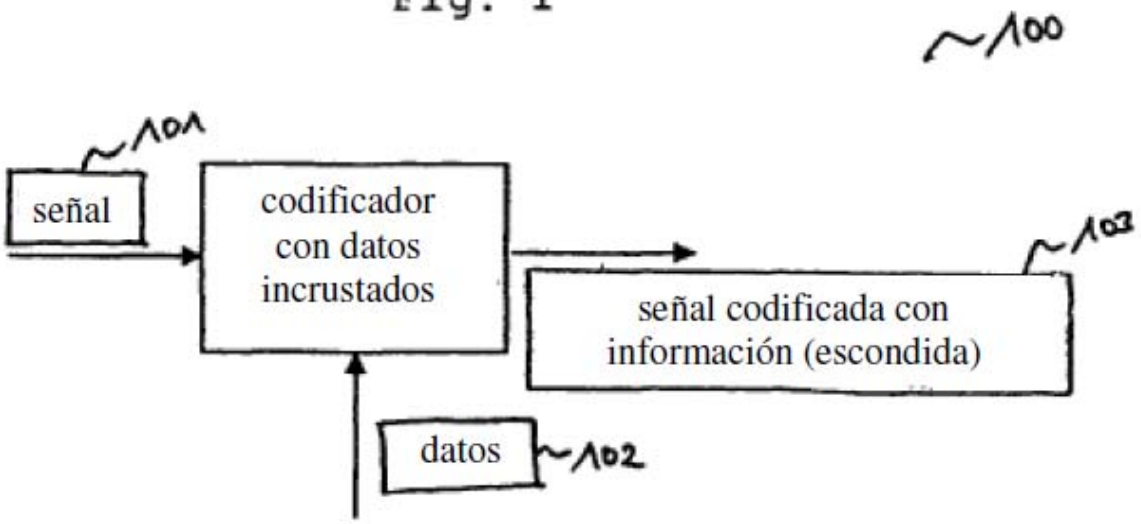

100
101
señal
codificador
con datos
incrustados
103
señal codificada con
información (escondida)
datos
102

Fig. 2

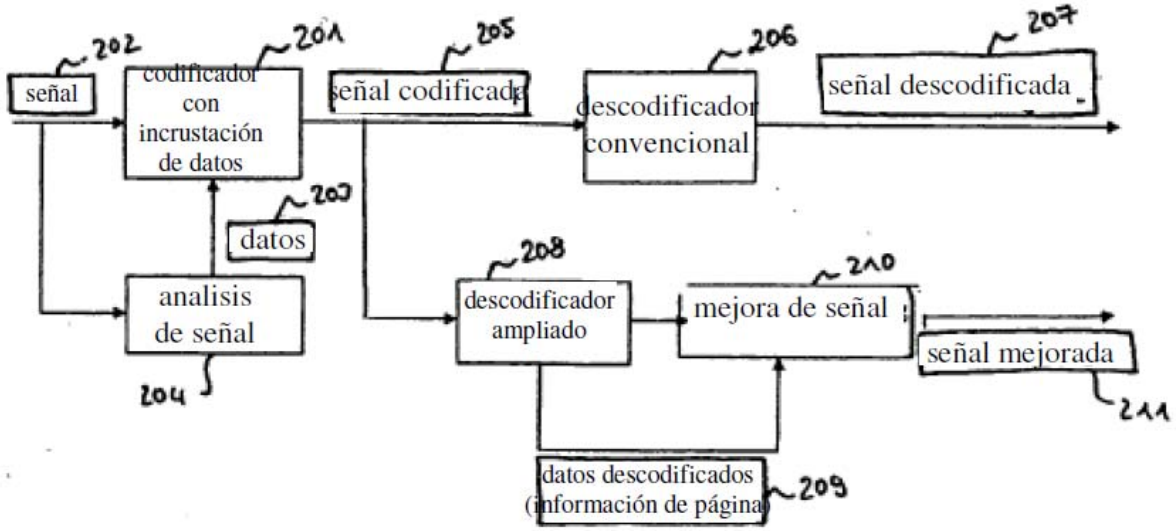

202
señal
201
codificador con incrustación de datos
205
señal codificada
206
descodificador convencional
207
señal descodificada
203
datos
208
descodificador ampliado
210
mejora de señal
señal mejorada
211
analisis de señal
204
datos descodificados (información de página)
209

Fig. 3

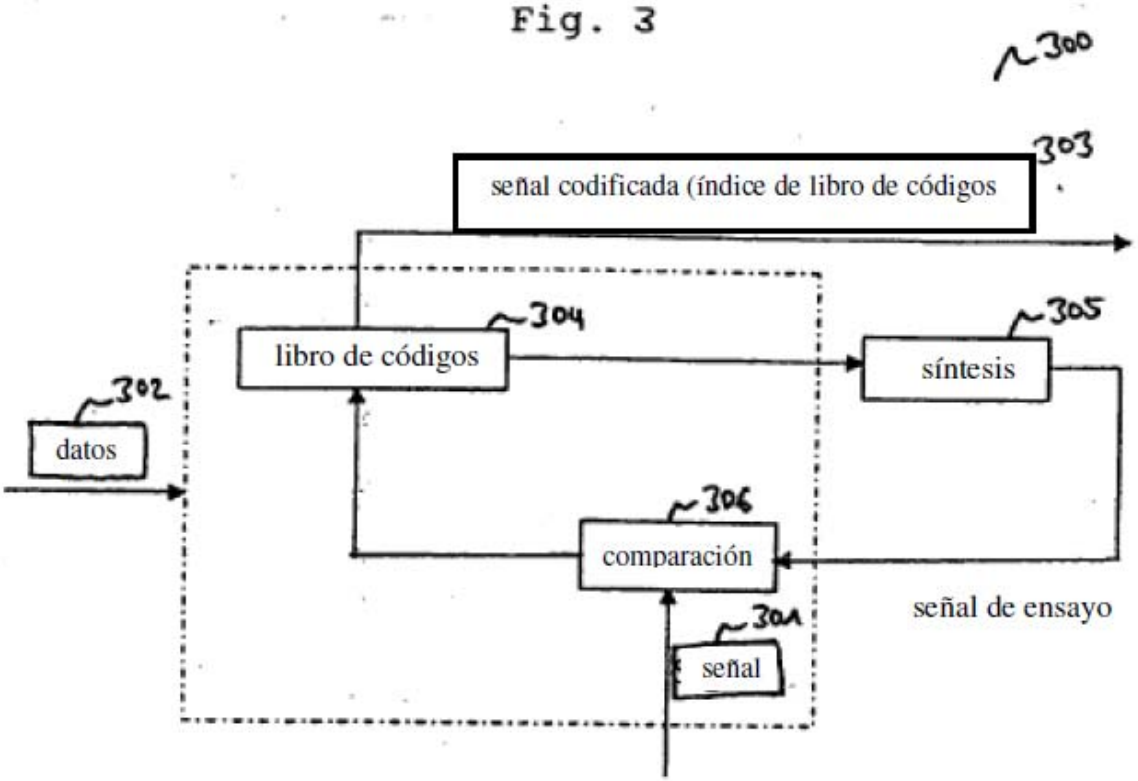

300
señal codificada (índice de libro de códigos
303
libro de códigos
304
síntesis
305
datos
302
comparación
306
señal de ensayo
señal
301

Fig. 4

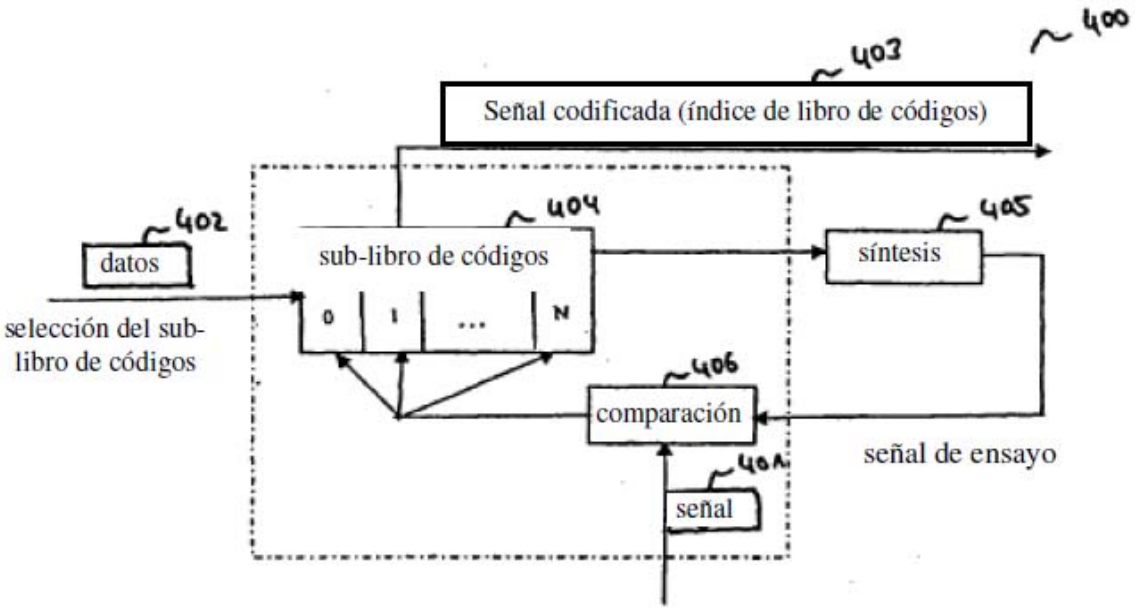
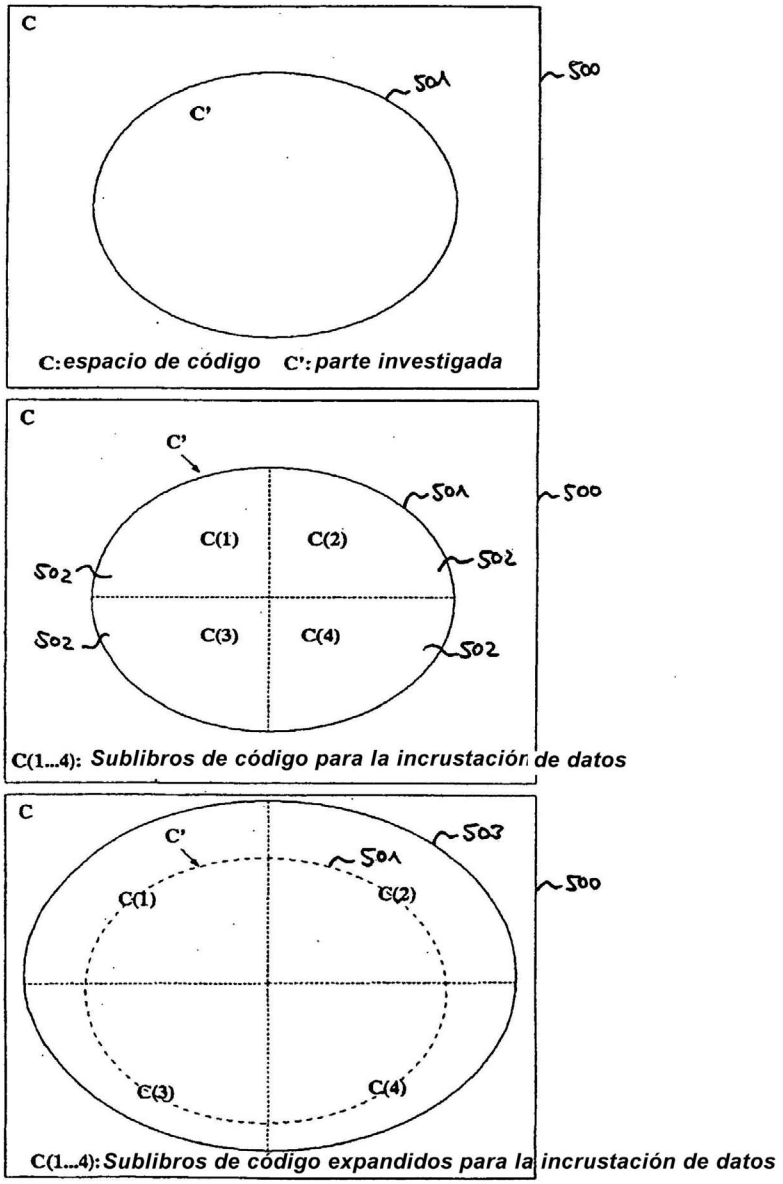

400
403
Señal codificada (índice de libro de códigos)
402
datos
404
sub-libro de códigos
0
1
...
N
405
síntesis
selección del sub-libro de códigos
406
comparación
señal de ensayo
401
señal

Fig. 5


C
C'
501
500
C: espacio de código C': parte investigada
C
C'
501
500
C(1)
C(2)
502
502
502
C(3)
C(4)
502
C(1...4): Sublibros de código para la incrustación de datos
C
C'
503
501
500
C(1)
C(2)
C(3)
C(4)
C(1...4): Sublibros de código expandidos para la incrustación de datos