(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 297 927**

(51) Int. Cl.:
G11B 20/00 (2006.01)
H04H 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99930276 .3**
(86) Fecha de presentación : **16.06.1999**
(87) Número de publicación de la solicitud: **1095376**
(87) Fecha de publicación de la solicitud: **02.05.2001**

(54) Título: **Aparato y método para la inserción y extracción de información en señales analógicas mediante modulación de réplicas.**

(30) Prioridad: **29.06.1998 US 106213**

(45) Fecha de publicación de la mención BOPI:
01.05.2008

(45) Fecha de la publicación del folleto de la patente:
01.05.2008

(73) Titular/es: **Verance Corporation**
4435 Eastgate Mall, Suite 350
San Diego, California 92121, US

(72) Inventor/es: **Petrovic, Rade**

(74) Agente: **Durán Moya, Carlos**

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).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Aparato y método para la inserción y extracción de información en señales analógicas mediante modulación de réplicas.

Antecedentes de la invención

Campo de la invención

La presente invención se refiere a un aparato y métodos para codificar o insertar y decodificar o extraer información en señales analógicas tales como señales de audio, vídeo y datos, tanto transmitidas mediante transmisión por ondas de radio o mediante transmisión por cable, o almacenadas en un medio de grabación tal como discos ópticos o magnéticos, cintas magnéticas o memorias de estado sólido.

Antecedentes y descripción de la técnica relacionada

La presente invención tiene relación con las técnicas para insertar y extraer información auxiliar dentro de una señal existente, tal como una señal de audio o de vídeo.

Un área de particular interés para ciertas realizaciones de la presente invención se refiere al mercado de grabaciones musicales. En la actualidad, un gran número de personal escucha grabaciones musicales en la radio o en la televisión. A menudo oyen una grabación que les gusta lo suficiente como para adquirirla, pero no conocen el nombre de la canción, el artista que la interpreta o el disco, cinta o álbum de CD del que forma parte. Como resultado, el número de grabaciones que adquiere la gente es menor que el que, de otra manera, podría adquirir si hubiera una manera simple en que la gente identificara qué grabaciones de las que oyen en la radio o en la televisión desea adquirir.

Otra área de interés para ciertas realizaciones de la invención es el control de copias (al que también se hace referencia como técnica de marca de agua digital). En la actualidad, existe un gran mercado para productos de software de audio, tales como grabaciones musicales. Uno de los problemas de este mercado es la facilidad de copia de dichos productos sin pagar a los que los producen. Este problema se vuelve particularmente molesto con la llegada de las técnicas de grabación, tales como cintas de audio digitales (DAT), que permiten que las copias sean de muy elevada calidad. De esta manera, sería deseable desarrollar un esquema que evitara la copia no autorizada de las grabaciones de audio, incluyendo la copia no autorizada de trabajos de audio emitidos a través de las ondas. También es deseable, para la aplicación de los derechos de autor, ser capaz de insertar en el material de programa, tal como señales de audio o de vídeo, la información digital de los derechos de autor que identifica al propietario de los mismos, cuya información puede ser detectada mediante los aparatos adecuados para identificar el propietario de los derechos de autor del programa, mientras permanecen imperceptibles para al oyente o espectador.

Un campo adicional de interés relacionado con la presente invención pertenece al seguimiento automático de los derechos de autor y a la prueba de reproducción del material o de los anuncios comerciales con derechos de autor, mediante los cuales los propietarios de los mismos son capaces de rastrear las reproducciones o emisiones de su material para propósitos de pago de derechos de autor, y los anunciantes son capaces de confirmar que los anuncios que han pagado fueron de hecho emitidos a la hora y fecha correctas.

Otra área de interés adicional de la presente invención se refiere a la verificación de la integridad o la detección de falsificaciones, en las que el creador de un trabajo de audio o audiovisual puede determinar si éste ha sido alterado, modificado o incorporado a otro trabajo.

Se conocen diversos métodos en el estado de la técnica anterior de codificación de información adicional sobre una señal fuente. Por ejemplo, es conocida la modulación por amplitud de pulso de una señal para conseguir una señal común o codificada que porta, por lo menos, dos partes de información u otras partes útiles. En la patente U.S.A. número 4.497.060 de Yang (1985), los datos binarios se transmiten como una señal que tiene dos anchos de pulso diferentes para representar “0” y “1” lógicos (por ejemplo, las duraciones del ancho de pulso para un “1” son el doble de la duración de un “0”). Esta correspondencia también permite la determinación de una señal de reloj.

En cuanto a los sistemas en los que las señales de audio generan transmisiones de audio, las patentes U.S.A. número 4.876.617 de Best y otros (1989) y número 5.113.437 de Best y otros (1992) dan a conocer codificadores para formar muescas relativamente delgadas y profundas (por ejemplo, 150 Hz de ancho y 50 dB de profundidad) en el rango de frecuencias medias de una señal de audio. La primera de estas patentes da a conocer filtros de muesca acoplados centrados en torno a las frecuencias de 2.883 Hz y 3.417 Hz; la última patente da a conocer filtros de muesca pero con pares de frecuencias que varían aleatoriamente para evitar el borrado o inhibir el filtrado de la información añadida a las muescas. Los codificadores añaden posteriormente la información digital en forma de señales en la frecuencia más baja indicando un “0” y en la frecuencia más alta indicando un “1”. En la última patente de Best y otros, un codificador muestrea la señal de audio, retarda la señal mientras calcula el nivel de la señal, y determina durante el retardo si añadir o no la señal de datos y, en ese caso, a qué nivel de señal. La última patente de Best y otros también describe que la “forma pseudoaleatoria” de desplazar las muescas, hace más difícil detectar de forma audible las señales de datos.

Otras técnicas del estado anterior de la técnica utilizan el modelo psicoacústico de la característica de la percepción humana para insertar tonos modulados o sin modular en una señal principal, de manera que serán enmascarados por los componentes de la señal existente y, de esta manera, no serán percibidos. *Véase, por ejemplo*, la patente U.S.A. número 5.319.735 de Preuss y otros, y la patente U.S.A. número 5.450.490 de Jensen y otros. Dichas técnicas son muy costosas y complicadas de implementar, a la vez que experimentan una falta de robustez al enfrentarse con distorsiones de señales impuestas por los esquemas de compresión basados en la percepción, diseñados para eliminar los componentes de la señal enmascarada.

La técnica anterior no consigue un método y un aparato para insertar y extraer señales auxiliares de información digitales o analógicas de las señales de frecuencia de audio o de vídeo analógicas para generar transmisiones a percibir por los humanos (*es decir*, sonidos o imágenes), de manera que las señales de frecuencia de audio o de vídeo generan transmisiones a percibir por los humanos sustancialmente idénticas, tanto antes como después de la codificación con las señales auxiliares (en otras palabras, la información insertada es transparente para el oyente o el espectador), que también es robusta hasta un alto grado de distorsiones de la señal generadas por medios de transmisión ruidosos, etc. La técnica anterior tampoco consigue aparatos y métodos relativamente simples y baratos para insertar y extraer señales que definen la información auxiliar en las señales de frecuencia de audio o de vídeo para generar transmisiones de audio a percibir por los humanos.

El documento WO98/53565 da a conocer métodos para insertar datos en una señal portadora comparando una característica de señal distribuida con un conjunto de valores de cuantización predefinidos.

Características de la invención

La presente invención da a conocer un aparato y métodos para insertar o codificar, y extraer o decodificar, información auxiliar (analógica o digital) en una señal principal o portadora analógica, de manera que tiene un impacto mínimo sobre la percepción de la información fuente cuando la señal analógica se aplica a un dispositivo de salida adecuado, tal como un altavoz, un monitor de presentación u otro dispositivo eléctrico/electrónico.

La presente invención da a conocer, además, un aparato y métodos para insertar y extraer señales legibles a máquina en una señal portadora analógica que controla la capacidad de un dispositivo para copiar la señal portadora.

En resumen, la presente invención da a conocer un método para insertar una señal auxiliar en una señal portadora analógica, que comprende las etapas de:

seleccionar por lo menos una parte de dicha señal portadora en un dominio predeterminado según una clave stego;

generar una señal réplica a partir de dicha parte seleccionada de la señal portadora, modificando dicha parte seleccionada de dicha señal portadora según la clave stego;

modificar dicha señal réplica como una función de dicha señal auxiliar; e

insertar la señal réplica modificada en dicha señal portadora analógica.

La invención da a conocer, además, un método de extracción de una señal auxiliar insertada a partir de una señal stego analógica, que comprende las etapas de:

seleccionar por lo menos una parte de dicha señal stego en un dominio predeterminado según una clave stego;

generar una señal réplica a partir de dicha parte seleccionada de la señal stego, modificando dicha parte seleccionada de dicha señal stego según la clave stego;

modificar dicha señal stego como una función de dicha señal réplica; y

extraer dicha señal auxiliar insertada filtrando dicha señal stego modificada.

Según otro aspecto de la invención, se da a conocer un aparato para insertar y extraer señales auxiliares en una señal portadora analógica, que comprende:

medios para seleccionar por lo menos una parte de dicha señal portadora en un dominio predeterminado según una clave stego;

medios para generar una señal réplica a partir de dicha parte seleccionada de la señal portadora, modificando dicha parte seleccionada de dicha señal portadora según la clave stego;

medios para modificar dicha señal réplica como una función de dicha señal auxiliar; y

medios para insertar la señal réplica modificada en dicha señal portadora analógica para generar una señal stego;

medios para recibir dicha señal stego;

medios para seleccionar por lo menos una parte de dicha señal stego en un dominio predeterminado según una clave stego;

medios para generar una señal réplica a partir de dicha parte seleccionada de la señal stego, modificando dicha parte seleccionada de dicha señal stego según la clave stego;

medios para modificar dicha señal stego recibida como una función de dicha señal réplica de dicha señal stego recibida; y

medios para extraer dicha señal auxiliar filtrando dicha señal stego modificada recibida.

El término señal portadora, tal como se utiliza en adelante, se refiere a una señal principal o fuente, tal como una señal de audio, vídeo u otra señal de información, que porta o se pretende que porte datos auxiliares insertados u ocultos.

Breve descripción de los dibujos

Estos y otros aspectos de la presente invención se entenderán de manera más completa a partir de la siguiente descripción detallada de las realizaciones preferentes, en combinación con los dibujos adjuntos, en los que:

la figura 1 es un diagrama de bloques de un proceso para insertar y extraer señales de datos, utilizado por la presente invención;

la figura 2 es un diagrama de bloques de una realización del dispositivo de inserción (10) de la figura 1;

la figura 3 es un diagrama de bloques de una realización del generador de la señal insertada (11) de la figura 2;

la figura 4 es un diagrama de bloques de una realización del dispositivo de extracción (20) de la señal de datos según la presente invención;

la figura 5 es un diagrama de bloques de una realización de un generador de réplicas que genera una réplica de la señal portadora desplazada en frecuencia a partir de la original; y

las figuras 6(a)-6(c) son gráficos que muestran un conjunto de funciones ortogonales utilizadas en la creación de una réplica desplazada en amplitud, según una realización de la presente invención.

Descripción detallada de las realizaciones preferentes

La presente invención se refiere a un método y a un aparato para insertar información o datos en una señal portadora, tal como una señal de audio, una señal de vídeo u otra señal analógica (llamada en adelante una "señal portadora"), generando una réplica de la señal portadora dentro de un dominio de la frecuencia, del tiempo y/o del espacio predefinidos, modulando la réplica con una señal auxiliar que representa la información a añadir a la señal portadora y, posteriormente, insertando la réplica modulada de nuevo en la señal portadora. La invención se puede implementar en un número de maneras diferentes, tanto mediante la programación de software de un procesador digital, en la forma de circuitos integrados de señales analógicas, digitales o mixtas, como un dispositivo electrónico de componentes discretos, o una combinación de dichas implementaciones. La réplica es similar a la señal portadora en el contenido del dominio de la frecuencia y del tiempo, pero diferente en ciertos parámetros según lo especificado por una clave stego, que generalmente no se conoce, pero que es conocida por los aparatos de recepción autorizados.

Haciendo referencia a la figura 1, la invención utiliza un dispositivo de inserción (10) para generar una señal stego (4), que es sustancialmente la misma en términos de contenido y de calidad de la información portada por una señal portadora (2). Por ejemplo, cuando la señal portadora (2) es una señal de vídeo o de audio, la señal stego (4) generará esencialmente el mismo programa o información de vídeo o de audio cuando se aplique a un dispositivo de salida, tal como una pantalla de vídeo o un altavoz.

Se utiliza una clave stego (9) para determinar y especificar la región específica del dominio del tiempo, de la frecuencia y/o del espacio de la réplica, en la que la señal auxiliar (6) va a ser insertada, así como los parámetros del proceso de inserción.

Posteriormente, el dispositivo de inserción modula o modifica adecuadamente la réplica y añade la réplica de nuevo en la señal portadora para obtener una señal stego (4). La señal stego (4) se puede transmitir o se puede almacenar en un medio de almacenamiento tal como una cinta magnética, un CD-ROM, una memoria de estado sólido y similares, para una posterior recuperación y/o transmisión. La señal auxiliar insertada se recupera mediante un dispositivo de extracción (20), que tiene conocimiento de la clave stego (9) o acceso a la misma, que opera sobre la señal stego (4) para extraer la señal auxiliar (6). El proceso de inserción se puede expresar mediante la fórmula:

$$\bar{s}(t) = s(t) + \sum_i w_i(t) \qquad (1)$$

donde $\bar{s}(t)$ representa la señal stego (4), s(t) representa la señal portadora (2) y $w_i(t)$ es la señal oculta (8) de orden i (*ver* la figura 2), también conocida como marca de agua. Con respecto a esto, el dispositivo de inserción se puede utilizar para insertar múltiples señales auxiliares (6) simultáneamente, utilizando una clave stego (9) diferente para cada señal. En el caso en el que únicamente se va a insertar una sola señal auxiliar (6), se utiliza una sola clave stego (9), y existiría únicamente una señal oculta w(t). En la ecuación (1) y a continuación en esta descripción, se considera una señal unidimensional (*es decir*, una señal que varía según una única dimensión, tal como el tiempo) para propósitos de simplicidad en la explicación; no obstante, la presente invención no está limitada a señales unidimensionales, sino que se puede ampliar fácilmente a señales multidimensionales tales como imágenes (dos dimensiones), vídeo (tres dimensiones), etc., definiendo t como un vector.

Según la presente invención, se utiliza una réplica de la misma señal portadora (2) como portadora de la señal auxiliar (6). Debido a que la réplica es inherentemente similar a la señal portadora en términos de contenido de frecuencia, no es necesario ningún análisis de la señal portadora a efectos de ocultar una señal auxiliar, tal como una marca de agua digital.

Por el contrario, según las técnicas del estado de la técnica anterior mencionadas anteriormente, las señales auxiliares se insertan en la forma de una secuencia pseudoaleatoria (Preuss y otros) o en la forma de múltiples tonos distribuidos por toda la banda de frecuencias de la señal portadora (Jensen y otros). A efectos de "ocultar" dichas señales de manera que sean perceptivamente transparentes, fue necesario llevar a cabo un análisis de la señal portadora en el dominio de la frecuencia para hacer que la señal de marca de agua fuera imperceptible para el observador. Dicho análisis está basado en el fenómeno de que la percepción humana no detectará una señal menor en la presencia de una señal mayor si las dos señales son suficientemente similares. Este fenómeno se conoce normalmente como el efecto de enmascarado.

La señal insertada (8), según la presente invención, se puede expresar mediante la fórmula:

$$w_i(t) = g_i\, m_i(t)\, r_i(t) \qquad (2)$$

donde $g_i<1$ es un parámetro de ganancia (factor de escala) determinado por consideraciones de compensación de robustez respecto a transparencia, $m_i(t)$ es la señal auxiliar (6), donde $|m_i(t)|\leq 1$, y $r_i(t)$ es una réplica de la señal portadora (2). El factor de ganancia g_i puede ser una constante predeterminada para una aplicación determinada, o puede ser ajustable de manera que se pueden tener en cuenta los cambios dinámicos en las condiciones de transparencia y robustez. Por ejemplo, en los pasos musicales altamente tonales, las ganancias pueden ser menores, mientras que para las señales de audio ruidosas o espectralmente ricas, las ganancias pueden ser mayores, con niveles equivalentes de transparencia. En una realización alternativa, el dispositivo de inserción puede llevar a cabo una simulación del proceso de extracción para identificar las señales que tienen una capacidad de ser detectadas menor que la deseable y, en consecuencia, aumentar la ganancia.

La figura 2 muestra un diagrama de bloques de una realización preferente del dispositivo de inserción (10). Tal como se muestra, la señal portadora (2), la clave stego (9) y la señal auxiliar (6) son introducidas en un generador de señales insertadas (11). El generador de señales insertadas genera la réplica $r_i(t)$ a partir de la señal portadora (2), según la clave stego (9), modula o modifica la réplica $r_i(t)$ con la señal auxiliar (6) ($m_i(t)$), escala el resultado utilizando el parámetro de ganancia g_i, y genera una señal insertada (8) ($w_i(t)$). La señal insertada (8) se añade posteriormente a la señal portadora (2) (s(t)) en un sumador (12), para generar la señal stego (4) ($\bar{s}(t)$).

La réplica $r_i(t)$ se obtiene tomando una parte de la señal portadora (2) en un dominio específico del tiempo, de la frecuencia y/o del espacio, tal como lo especifica la clave stego (9), y realizando posteriormente ligeras modificaciones a la parte de la señal, también según lo especifica la clave stego (9). Las modificaciones de la parte de la señal deben ser pequeñas para asegurar que la réplica se mantiene similar a la señal portadora, tal como lo juzgan los sistemas psicoacústico-psicovisuales humanos, pero dichas modificaciones deben ser lo suficientemente grandes para ser detectables mediante un dispositivo de extracción adecuadamente diseñado que tiene conocimiento de la clave stego (9) o acceso a la misma. Tal como se tratará más adelante, se han encontrado un número de tipos diferentes de modificaciones para satisfacer estas necesidades.

La ecuación (2) revela que la réplica $r_i(t)$ es modulada por la señal auxiliar $m_i(t)$ según un proceso conocido como modulación de producto. La modulación del producto da como resultado una ampliación del espectro de la señal insertada proporcionalmente a la anchura espectral de la señal auxiliar. A efectos de hacer que el espectro de la señal insertada sea similar al espectro de la señal portadora (para mantener la transparencia del proceso de inserción), el espectro de la señal auxiliar debe ser estrecho en comparación con la menor frecuencia del espectro de la réplica. Este requisito impone un límite a la capacidad del canal auxiliar, e impone que los componentes de baja frecuencia de la señal portadora no son adecuados para incluirlos en la creación de la réplica.

En una realización preferente de la invención, la señal de modulación (señal auxiliar) m(t) es una señal de datos binarios definida por la fórmula:

$$m(t) = \sum_{n=1}^{N} b_n\, h(t - nT) \qquad (3)$$

donde N es el número de dígitos binarios o bits en el mensaje, $b_n \in (-1,1)$ es el valor del bit de orden n, T es el intervalo de bits y h(t) representa la forma del pulso que representa el bit. Típicamente, h(t) se obtiene filtrando un impulso rectangular, mediante un filtro paso bajo, a efectos de limitar la anchura espectral de la señal (auxiliar) de modulación.

La figura 3 ilustra los detalles de un generador (11) de señales insertadas utilizado para generar un único mensaje de datos insertado. La señal portadora (2) se filtra y/o se enmascara en el bloque de filtrado/enmascarado (30) para generar una señal filtrada/enmascarada (31). El bloque de filtrado/enmascarado (30) separa las regiones de la señal portadora utilizadas para diferentes mensajes insertados. Por ejemplo, el bloque de filtrado/enmascarado puede separar la región de la banda de frecuencias 1.000-3.000 Hz a partir de la señal portadora en el dominio de la frecuencia, puede separar la región del intervalo de tiempo t=10 segundos a t=30 segundos a partir de la señal portadora en el dominio del tiempo, o puede separar la región del cuadrante espacial superior derecho de la señal portadora en el dominio del espacio (tal como cuando la señal portadora es una señal MPEG, JPEG o una señal equivalente) de manera que la región separada se utilizaría posteriormente para insertar la señal auxiliar.

La señal de filtrado/enmascarado (31) está compuesta por las regiones seleccionadas de la señal portadora, tal como lo especifica la clave stego (9), que se utilizan posteriormente para la creación de la señal réplica (41). La señal (31) se introduce posteriormente en un creador de réplicas (40), en el que se modifican los parámetros predeterminados de la señal, tal como lo especifica la clave stego (9), para crear la réplica $r_i(t)$ (41). La réplica (41) se modula posteriormente mediante la señal auxiliar $m_i(t)$ en el multiplicador (42a), y la señal resultante se escala posteriormente en el multiplicador (42b), según el factor de ganancia seleccionado g_i, para generar la componente (8) de la señal insertada (*es decir*, $w_i(t)$ en la ecuación (2)). La componente (8) de la señal insertada se añade posteriormente de nuevo a la señal portadora (2) en el sumador (12) (figura 2) para obtener la señal stego (4). A efectos de mantener la sincronización entre la señal portadora (2) y el componente (8) de la señal insertada, los retardos inherentes del procesamiento presentes en el bloque de filtrado/enmascarado (30) y el bloque creador de réplicas (40) se compensan añadiendo un retardo equivalente en la ruta del circuito de la señal portadora (entre la entrada de la señal portadora y el sumador -12-), mostrado en la figura 2.

Además, es posible insertar múltiples señales auxiliares de datos en la señal portadora (2), utilizando múltiples generadores de señales insertadas, utilizando cada uno una clave stego diferente para modificar una característica diferente de la señal portadora y/o utilizar diferentes regiones de la señal portadora, a efectos de generar múltiples componentes de la señal insertada, cada una de las cuales se añade a la señal portadora (2). Alternativamente, las diferentes señales de datos pueden ser insertadas en modo de cascada, siendo la salida de un dispositivo de inserción la entrada de otro dispositivo de inserción que utiliza una clave stego diferente. En ambos la interferencia alternativa entre las componentes de las señales insertadas debe ser minimizada. Esto se puede conseguir utilizando regiones no solapadas de frecuencia, tiempo o espacio de la señal, o seleccionando los parámetros de creación de la réplica adecuados, tal como se da a conocer más adelante.

Un diagrama de bloques de un dispositivo de extracción utilizado para recuperar los datos auxiliares insertados en la señal stego se muestra en la figura 4. La señal stego (4) se filtra/enmascara en el módulo de filtrado/enmascarado (30a) para aislar las regiones en las que se insertan los datos auxiliares. La señal filtrada (31a) se introduce en el creador de réplicas (40a) en el que una réplica $\bar{r}_i(t)$ (41a) de la señal stego se genera de la misma manera que la réplica $r_i(t)$ de la señal portadora en el bloque de creación de la réplica (40) del dispositivo de inserción, utilizando la misma clave stego (9). La réplica $\bar{r}_i(t)$ de la señal stego (4) se puede expresar mediante la fórmula:

$$\bar{r}_i(t) = r_i(t) + \sum_i g_i\, R(m_i(t) r_i(t)) \approx r_i(t) \qquad (4)$$

donde $R(m_i(t)r_i(t))$ representa la réplica de la réplica de la señal portadora modulada. Para factores de ganancia g_i suficientemente pequeños, la réplica de la señal stego es sustancialmente la misma que la réplica de la señal portadora.

En el dispositivo de extracción (20), la réplica $\bar{r}_i(t)$ (41a) se multiplica por la señal stego (31a) en un multiplicador (42c) para obtener el producto de correlación:

$$c(t) = \bar{r}_i(t)\, \bar{s}(t) \approx r_j(t)\, s(t) + \sum g_i\, m_i(t) r_i(t) r_j(t) \qquad (5)$$

En el diseño de la señal réplica, un objetivo es conseguir los espectros de los productos $r_j(t)s(t)$ y $r_i(t)r_j(t)$, $i \neq j$, con poco contenido en bajas frecuencias. Por otra parte, los espectros del producto $r_j(t)r_j(t)=r_j^2(t)$ contienen una fuerte

componente continua (DC) y, de esta manera, el producto de la correlación c(t) contiene un término de la forma $g_i m_i(t)$promedio(r_j^2), *es decir*, c(t) contiene la señal auxiliar escalada $m_i(t)$ como sumando.

A efectos de extraer la señal auxiliar $m_i(t)$ del producto de correlación c(t), se lleva a cabo el filtrado de c(t) mediante el filtro (44), que tiene una característica de filtrado ajustada al espectro de la señal auxiliar. Por ejemplo, en el caso de una señal de datos binarios con una forma de pulso rectangular, el filtrado ajustado corresponde a la integración en el intervalo de bits. En el caso de la transmisión digital de señales, a la operación de filtrado le sigue la regeneración de símbolos en un regenerador (46). Una multiplicidad de los símbolos de datos extraídos es sometida posteriormente a las bien conocidas técnicas de detección de errores, corrección de errores y a las técnicas de sincronización para verificar la existencia de un mensaje real y la interpretación adecuada del contenido del mensaje.

En la figura 5 se muestra una realización preferente de un creador de réplicas (40). En esta realización, se consigue una señal réplica (41) mediante el desplazamiento de la frecuencia de la señal portadora filtrada (31) mediante una frecuencia de desplazamiento f_i predeterminada, tal como lo especifica la clave stego (9). Este proceso de desplazamiento se conoce también como modulación de amplitud de banda lateral única o desplazamiento de la frecuencia. Además del procesamiento mostrado en la figura 5, se dispone de un número de técnicas diferentes conocidas en el estado de la técnica para llevar a cabo este proceso.

Los bloques (52) y (54) representan los respectivos desplazamientos de fase de la señal de entrada s(t). Para conseguir el desplazamiento de frecuencia deseado, la relación entre los desplazamientos de fase debe ser definida como:

$$\varphi_i(f) - \varphi_2(f) = 90^o \qquad (6)$$

Las respectivas señales desplazadas en fase son multiplicadas por las señales sinusoidales con frecuencia f_i en los respectivos multiplicadores (56a) y (56b). El bloque (58) indica un desplazamiento de fase de 90º de la señal sinusoidal aplicada al multiplicador (56b). Las señales resultantes se combinan posteriormente en el sumador (59).

De esta manera, la señal réplica (41) se puede expresar como:

$$r_i(t) = s(t, \varphi_1)\, sen(2\pi f_i t) \pm s(t, \varphi_2) \cos(2\pi f_i t) \qquad (7)$$

donde $s(t, \varphi_i)$ indica la señal s(t) desplazada en fase por φ_i. El signo - o + del proceso de suma representa un desplazamiento respectivo ascendente o descendente por f_i. Según los modelos psicoacústicos publicados en la literatura, se puede conseguir un mejor enmascaramiento cuando el desplazamiento es ascendente. En consecuencia, en la realización preferente se utiliza la resta en la ecuación (7). En un caso especial en el que φ_1=90º y φ_2=0º, dicha ecuación (7) se convierte en:

$$r_i(t) = s_h(t)\, sen(2\pi f_i t) \pm s(t) \cos(2\pi f_i t) \qquad (8)$$

en la que $s_h(t)$ es una transformada de Hilbert de la señal de entrada, definida por:

$$s_h(t) = 1/\pi \int_{-\infty}^{\infty} \frac{s(x)\, dx}{t - x} \qquad (9)$$

La transformada de Hilbert se puede llevar a cabo en el software mediante diversos algoritmos conocidos, siendo adecuada la ecuación (8) para el procesamiento de señales digitales. Para el procesamiento de señales analógicas, es más fácil diseñar un par de circuitos que mantiene los desplazamientos de fase relativos de 90º en todo el espectro de señales, que llevar a cabo una transformada de Hilbert.

El desplazamiento de frecuencia f_i específico se puede elegir a partir de un amplio rango de frecuencias y puede ser especificado por la clave stego. Las múltiples señales auxiliares se pueden insertar en el mismo dominio del tiempo, de la frecuencia y/o del espacio de la misma señal portadora, teniendo un valor de desplazamiento de frecuencia diferente, para conseguir, de esta manera, una "separación por capas" de las señales auxiliares y un aumento del rendimiento del canal auxiliar.

El desplazamiento de la frecuencia también se puede variar en tiempo según un patrón secreto predefinido (conocido como "desplazamiento de frecuencia"), para mejorar la seguridad de una marca de agua digital representada por la información auxiliar.

La elección específica de los valores de desplazamiento de la frecuencia depende de las condiciones y parámetros de la aplicación específica, y pueden ser sintonizados más finamente mediante prueba y error. Según los resultados

experimentales, la robustez óptima de la señal en la presencia de distorsión del canal se conseguía cuando el valor del desplazamiento de frecuencia era mayor que la mayoría de las frecuencias del espectro de la señal auxiliar de modulación m(t). Por otra parte, la transparencia óptima se conseguía cuando el valor del desplazamiento de la frecuencia era sustancialmente menor que la frecuencia más baja de la señal portadora. Como ejemplo, para una señal de audio en la que se inserta una señal portadora por encima de los 500 Hz se utilizó un desplazamiento de frecuencia de 50 Hz, mientras que la señal de modulación era una señal de datos binarios con una proporción de bits de 25 bps.

En una realización alternativa de un creador de réplicas, la réplica se genera desplazando la fase de la parte filtrada/enmascarada (31) de la señal portadora en una cantidad predeterminada definida por una función $\varphi_i(f)$ para una señal insertada de orden i. En este caso, los generadores de réplicas (40) y (40a) son sistemas lineales que tienen una función de transferencia definida como:

$$H_i(f) = A_i \, e^{j\varphi_i(f)} \qquad (10)$$

en la que A_i es constante con respecto a la frecuencia, j es el número imaginario $\sqrt{-1}$ y $\varphi_i(f)$ es la característica de fase del sistema. Los circuitos descritos por la ecuación (10) son conocidos en el estado de la técnica como filtros de paso total o correctores de fase, y su diseño es bien conocido para los expertos en la técnica.

Esta realización es especialmente adecuada para señales auxiliares insertadas en señales de audio, dado que el sistema sensorial auditivo humano es sustancialmente no sensitivo a los desplazamientos de fase. Las funciones $\varphi_i(f)$ se definen para cumplir el objetivo de que el producto de la réplica y la señal portadora contenga el mínimo contenido de baja frecuencia. Esto se puede conseguir manteniendo, por lo menos, un desplazamiento de 90º para todos los componentes de frecuencia en la señal filtrada/enmascarada (31). Se han implementado múltiples mensajes insertados con poca interferencia, cuando el desplazamiento de fase entre las componentes de frecuencia de diferentes mensajes es mayor que el 90º para la mayoría de las componentes del espectro. La elección exacta de la función $\varphi_i(f)$ se controla de otra manera mediante las consideraciones de compensación entre coste y seguridad. En otras palabras, la función debe ser lo suficientemente compleja de manera que sea difícil para personas no autorizadas determinar la estructura de la señal analizando la señal stego, incluso con la señal portadora conocida, aún así no debería ser costoso de implementarse informáticamente. Un patrón de la función de desplazamiento que cambia entre diferentes funciones a intervalos predeterminados como parte de la clave stego puede ser utilizado para mejorar adicionalmente la seguridad.

Una clase especial de funciones de desplazamiento de fase, definidas por

$$\varphi_i(t) = \tau_i \, f \qquad (11)$$

en la que τ_i es una constante, resulta en réplicas desplazadas en tiempo de la señal portadora. Esta clase de funciones tiene propiedades especiales en términos de compensación coste/seguridad, que se encuentran más allá del alcance de la presente descripción y que no se tratarán adicionalmente en este documento.

Según una realización alternativa adicional de la invención, el generador de réplicas obtiene la señal réplica mediante la modulación de amplitud de la señal portadora. La modulación de amplitud se puede expresar mediante la ecuación

$$r_i(t) = a_i(t) \, s(t) \qquad (12)$$

en la que $a_i(t)$ es una clase de funciones ortogonales. Las figuras 6(a)-6(c) ilustran un conjunto de tres funciones elementales $a_1(t)$, $a_2(t)$ y $a_3(t)$, utilizadas para generar señales réplica desplazadas en amplitud, estando cada función definida en el intervalo (0, T), en las que T equivale al intervalo de bits de la señal auxiliar. Réplicas más largas se generan utilizando una cadena de funciones elementales. El filtrado tras la correlación en el dispositivo de extracción se lleva a cabo mediante la integración en el intervalo T, y el bit $b_{j,n}$ del canal auxiliar se extrae según la fórmula $\overline{b}_{j,n} = \text{sign}(A_{j,n})$, en el que:

$$A_{j,n} = \int_{n-1)T}^{nT} c(t)\, dt \approx \int_{n-1)T}^{nT} a_j(t)\, s^2(t)\, dt + \sum_i g_i \int_{n-1)T}^{nT} m_i(t)\, s^2(t)\, a_i(t)\, a_j(t)\, dt$$
$$\approx g_i \int_{n-1)T}^{nT} m_j(t) s^2(t)\, dt \qquad (13)$$

Las anteriores aproximaciones se consideran, dado que

$$\int_0^T a_j(t)\,dt = 0, \quad \int_0^T a_i(t)\,a_j(t)\,dt = 0, \text{ para } i \neq j, \text{ y } a_j^2(t) = 1.$$

Tal como es evidente a partir de la ecuación (13), el signo de $A_{j,n}$ (y el valor de bit recibido) depende del signo de $m_j(t)$ durante el intervalo de bit de orden n, o en otras palabras, el valor de bit transmitido. Las funciones utilizadas para el desplazamiento de amplitud deben tener generalmente un pequeño contenido de baja frecuencia, un espectro por debajo de la frecuencia más baja de la señal filtrada/enmascarada y deberían ser mutuamente ortogonales. La elección específica de las funciones depende de la aplicación específica, y se especifica en la clave stego.

Según otra realización alternativa adicional, una combinación de diferentes desplazamientos en dominios diferentes se puede ejecutar simultáneamente para generar una señal réplica. Por ejemplo, un desplazamiento de tiempo se puede combinar con un desplazamiento de frecuencia, o un desplazamiento de amplitud se puede combinar con un desplazamiento de fase. Dicha combinación de desplazamientos puede mejorar adicionalmente la propiedad de ocultación (seguridad) del sistema de inserción, y también mejorar la capacidad de detección de la señal insertada, aumentando la diferencia con respecto a la señal portadora.

Con respecto a la seguridad, se pueden esperar ataques que incorporan análisis diseñados para revelar los parámetros de la clave stego. Si se llegan a conocer dichos parámetros, entonces la señal insertada se puede sobreescribir o borrar mediante el uso de la misma clave stego. El uso de una combinación de desplazamientos hace dicho análisis más difícil aumentando el espacio del parámetro.

Con respecto a la capacidad de detección, ciertas señales que tienen lugar de manera natural pueden tener un contenido similar a una señal réplica; por ejemplo, el eco en una señal de audio puede generar una señal desplazada en fase, las secciones corales en un programa musical pueden generar una señal desplazada en frecuencia y el trémolo puede generar desplazamientos de amplitud, que pueden interferir en la detección de la señal insertada. El uso de una combinación de desplazamientos reduce la probabilidad de que un fenómeno natural se adapte exactamente con los parámetros de la clave stego, e interfiera en la detección de señales.

La invención, que se ha descrito de esta manera, será evidente para los expertos en la técnica, que puede variar de muchas maneras sin alejarse del alcance de la invención que se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para la inserción de una señal auxiliar en una señal portadora analógica, que comprende las etapas de:

selección como mínimo de una parte de dicha señal portadora en un dominio predeterminado según una clave stego;

generación de una señal réplica a partir de dicha parte seleccionada de la señal portadora modificando dicha parte seleccionada de dicha señal portadora según la clave stego;

modificación de dicha señal réplica como una función de dicha señal auxiliar; e

inserción de la señal réplica modificada en dicha señal portadora analógica.

2. Método, según la reivindicación 1, en el que dicho dominio predeterminado es el dominio de la frecuencia.

3. Método, según la reivindicación 1, en el que dicho dominio predeterminado es el dominio del tiempo.

4. Método, según la reivindicación 1, en el que dicho dominio predeterminado es el dominio del espacio.

5. Método, según la reivindicación 1, en el que dicha señal réplica se obtiene desplazando la frecuencia de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida especificada por dicha clave stego.

6. Método, según la reivindicación 1, en el que dicha señal réplica se obtiene desplazando la fase de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida especificada por dicha clave stego.

7. Método, según la reivindicación 1, en el que dicha señal réplica se obtiene desplazando la amplitud de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida por dicha clave stego.

8. Método, según la reivindicación 1, en el que dicha señal réplica se obtiene desplazando una combinación predeterminada de la frecuencia, la fase y/o la amplitud de dicha parte seleccionada de dicha señal portadora en cantidades predefinidas especificadas por dicha clave stego.

9. Método, según la reivindicación 1, en el que la etapa de modificación comprende la etapa de multiplicación de dicha señal réplica con dicha señal auxiliar.

10. Método de extracción de una señal auxiliar insertada a partir de una señal stego analógica, que comprende las etapas de:

selección, como mínimo, de una parte de dicha señal stego en un dominio predeterminado según una clave stego;

generación de una señal réplica a partir de dicha parte seleccionada de la señal stego modificando dicha parte seleccionada de dicha señal stego según la clave stego;

modificación de dicha señal stego como una función de dicha señal réplica; y

extracción de dicha señal auxiliar insertada filtrando dicha señal stego modificada.

11. Método, según la reivindicación 10, en el que dicho dominio predeterminado es el dominio de la frecuencia.

12. Método, según la reivindicación 10, en el que dicho dominio predeterminado es el dominio del tiempo.

13. Método, según la reivindicación 10, en el que dicho dominio predeterminado es el dominio del espacio.

14. Método, según la reivindicación 10, en el que dicha señal réplica se obtiene desplazando la frecuencia de dicha parte seleccionada de dicha señal stego en una cantidad predefinida especificada por dicha clave stego.

15. Método, según la reivindicación 10, en el que dicha señal réplica se obtiene desplazando la fase de dicha parte seleccionada de dicha señal stego en una cantidad predefinida especificada por dicha clave stego.

16. Método, según la reivindicación 10, en el que dicha señal réplica se obtiene desplazando la amplitud de dicha parte seleccionada de dicha señal stego en una cantidad predefinida especificada por dicha clave stego.

17. Método, según la reivindicación 10, en el que dicha señal réplica se obtiene desplazando una combinación predeterminada de la frecuencia, la fase y/o la amplitud de dicha parte seleccionada de dicha señal stego en una cantidad predefinida especificada por dicha clave stego.

18. Método, según la reivindicación 10, en el que la etapa de modificación comprende la etapa de multiplicación de dicha señal réplica con dicha señal stego.

19. Aparato para insertar y extraer señales auxiliares en una señal portadora analógica, que comprende:

medios (30) para seleccionar por lo menos una parte de dicha señal portadora en un dominio predeterminado según una clave stego;

medios (40) para generar una señal réplica a partir de dicha parte seleccionada de la señal portadora, modificando dicha parte seleccionada de dicha señal portadora según la clave stego;

medios (42) para modificar dicha señal réplica como una función de dicha señal auxiliar; y

medios (12) para insertar la señal réplica modificada en dicha señal portadora analógica para generar una señal stego;

medios para recibir dicha señal stego;

medios (30a) para seleccionar, por lo menos, una parte de dicha señal stego en un dominio predeterminado según una clave stego;

medios (40a) para generar una señal réplica a partir de dicha parte seleccionada de la señal stego modificando dicha parte seleccionada de dicha señal stego según la clave stego;

medios (42c) para modificar dicha señal stego recibida como una función de dicha señal réplica de dicha señal stego recibida; y

medios (44) para extraer dicha señal auxiliar filtrando dicha señal stego recibida modificada.

20. Aparato, según la reivindicación 19, en el que dicho dominio predeterminado es el dominio de la frecuencia.

21. Aparato, según la reivindicación 19, en el que dicho dominio predeterminado es el dominio del tiempo.

22. Aparato, según la reivindicación 19, en el que dicho dominio predeterminado es el dominio del espacio.

23. Aparato, según la reivindicación 19, en el que dicha señal réplica se obtiene desplazando la frecuencia de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida especificada por dicha clave stego.

24. Aparato, según la reivindicación 19, en el que dicha señal réplica se obtiene desplazando la fase de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida especificada por dicha clave stego.

25. Aparato, según la reivindicación 19, en el que dicha señal réplica se obtiene desplazando la amplitud de dicha parte seleccionada de dicha señal portadora en una cantidad predefinida especificada por dicha clave stego.

26. Aparato, según la reivindicación 19, en el que dicha señal réplica se obtiene desplazando una combinación predeterminada de la frecuencia, la fase y/o la amplitud de dicha parte seleccionada de dicha señal portadora en cantidades predefinidas especificada por dicha clave stego.

27. Aparato, según la reivindicación 19, en el que dichos medios para modificar dicha señal réplica comprenden medios (42a) para multiplicar dicha señal réplica con dicha señal auxiliar.

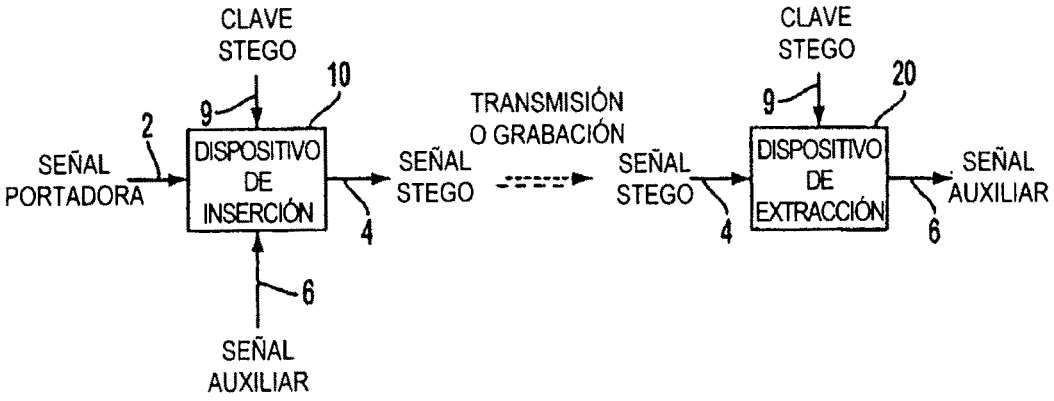
CLAVE STEGO
10
9
2
SEÑAL PORTADORA
DISPOSITIVO DE INSERCIÓN
SEÑAL STEGO
4
6
SEÑAL AUXILIAR
TRANSMISIÓN O GRABACIÓN
CLAVE STEGO
20
9
SEÑAL STEGO
4
DISPOSITIVO DE EXTRACCIÓN
6
SEÑAL AUXILIAR

FIG. 1

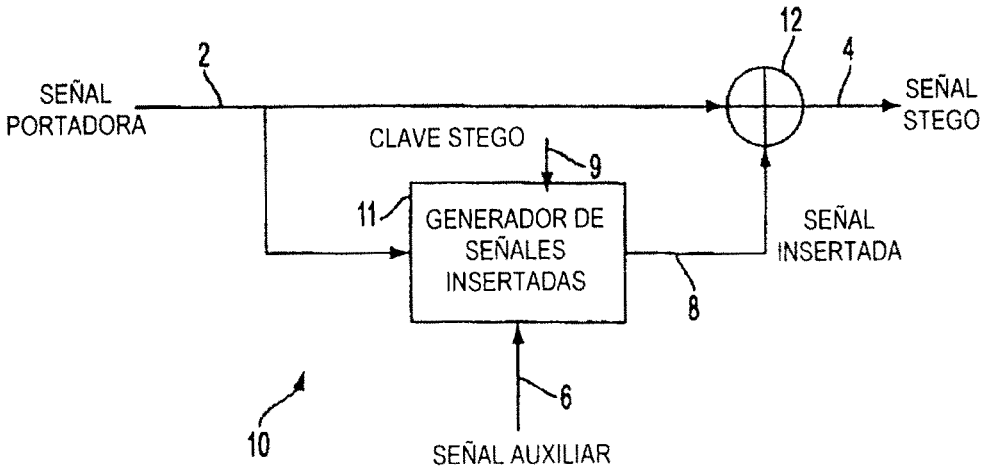
12
4
2
SEÑAL PORTADORA
SEÑAL STEGO
CLAVE STEGO
9
11
GENERADOR DE SEÑALES INSERTADAS
SEÑAL INSERTADA
8
6
10
SEÑAL AUXILIAR

FIG. 2

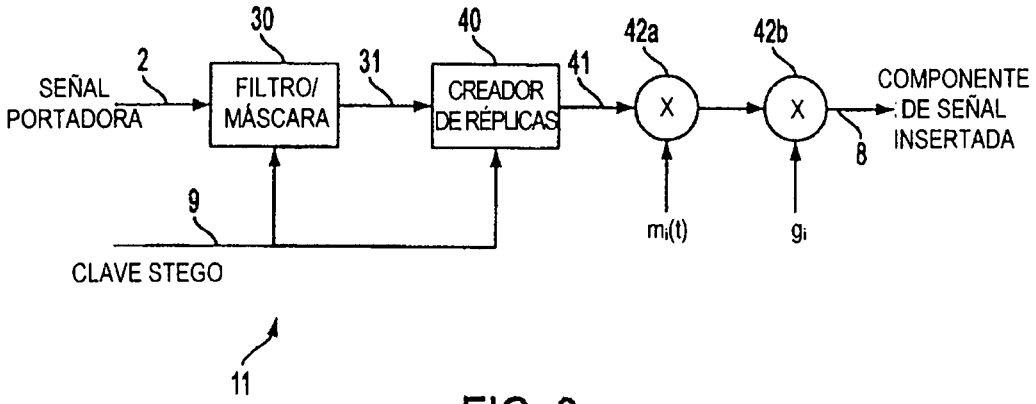
30
40
42a
42b
2
31
41
SEÑAL PORTADORA
FILTRO/ MÁSCARA
CREADOR DE RÉPLICAS
X
X
COMPONENTE DE SEÑAL INSERTADA
8
9
$m_i(t)$
g_i
CLAVE STEGO
11

FIG. 3

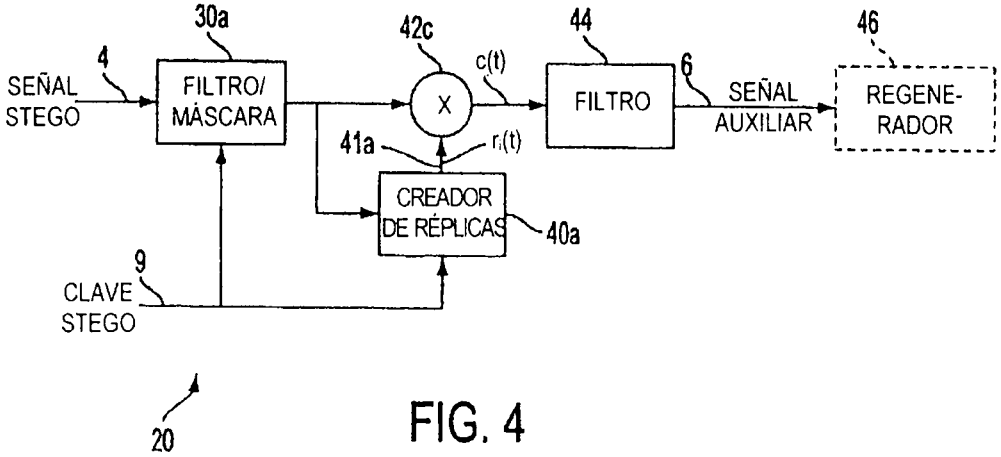
30a
42c
44
46
4
c(t)
6
SEÑAL STEGO
FILTRO/ MÁSCARA
X
FILTRO
SEÑAL AUXILIAR
REGENE-RADOR
41a
$r_i(t)$
CREADOR DE RÉPLICAS
40a
9
CLAVE STEGO
20

FIG. 4

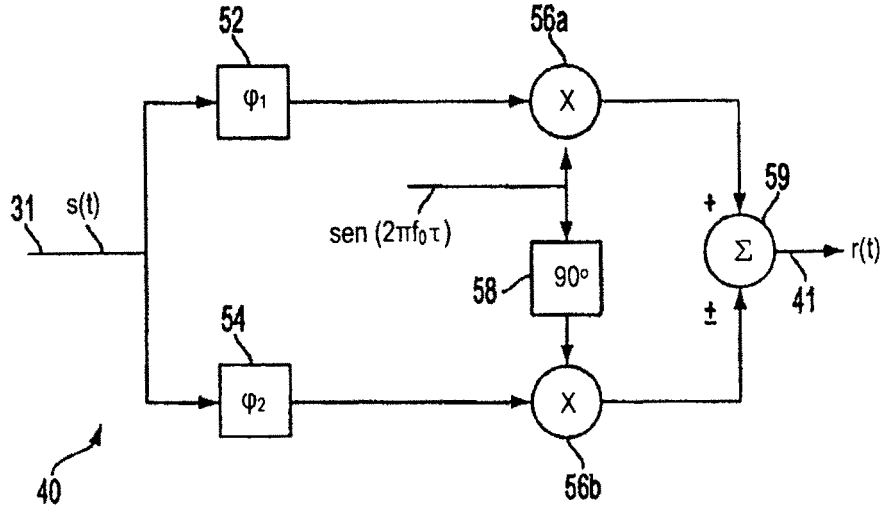

FIG. 5

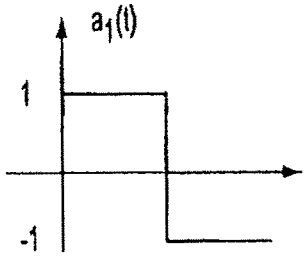

FIG. 6A

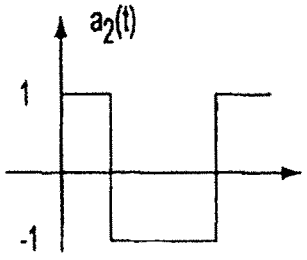

FIG. 6B

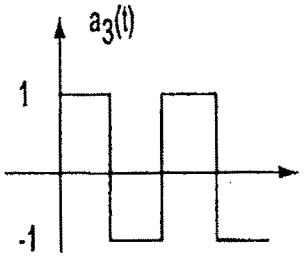

FIG. 6C