Codificación Esteganográfica usando la Transformada de Onditas Haar Discreta Multi-resolución

Alejandro Martínez, Isaac Campeán, Rosa E. Fosado y Raquel Ávila

Universidad Autónoma de San Luis Potosí, Coordinación Académica Región Altiplano, Matehuala, S.L.P., México. (e-mail: alejandro.martinez@uaslp.mx)

Recibido Oct. 30, 2017; Aceptado Ene. 2, 2018; Versión final Mar. 7, 2018, Publicado Ago. 2018

Resumen

Este trabajo presenta un método esteganográfico que realiza el ocultamiento de información en una señal portadora sin que se perciba su presencia. La codificación se realiza aplicando la Transformada de Onditas Haar Discreta Multi-resolución sobre la señal portadora y remplazando los bits menos significativos de una de sus señales componentes con los bits del mensaje que se oculta. El método es capaz de insertar la información en señales portadoras unidimensionales, así como en imágenes una vez que estas han sido acondicionadas como señales unidimensionales. Se presenta también un método para la recuperación del mensaje, en el que aplicando la Transformada de Onditas Haar Discreta Multi-resolución se separa a la estegoseñal en sus señales componentes, y se extrae a los bits del mensaje oculto de la componente en la que se encuentran insertados. Los métodos de codificación y decodificación fueron implementados en MATLAB y en Simulink, y son apropiados para implementarse en sistemas basados en dispositivos CPLD (Dispositivo Lógico Complejo Programable) o FPGA (Arreglos de Compuertas Programables por Campo).

Palabras clave: esteganografía; transformada de onditas Haar discreta; ocultamiento de mensaje; codificación de señales

Steganographic Coding using the Multi-resolution Discrete Haar Wavelet Transform

Abstract

This work introduces a steganographic method that performs the concealment of information in a carrier signal without perceiving its presence. The encoding is done by applying the Multi-resolution Discrete Haar Wavelet Transform to the carrier signal and replacing the least significant bits of one of its component signals with the bits of the message that is being hidden. The method is capable of embedding the information in one-dimensional carrier signals, as well as in images once they have been conditioned as one-dimensional signals. A method for message retrieval is also introduced, in which, by applying the Multi-resolution Discrete Haar Wavelet Transform, the stego-signal is separated into its component signals, and the bits of the hidden message are extracted from the component in which they were inserted. The encoding and decoding methods were implemented in MATLAB and Simulink, and are both suitable to be implemented in systems based on CPLD (Programmable Complex Logic Device) or FPGA (Field Programmable Gate Array) devices.

Keywords: steganography; discrete Haar wavelet transform; message concealment; signal coding

INTRODUCCIÓN

La transformada de ondita Haar discreta ha sido ampliamente utilizada en la codificación y ocultamiento de datos de señales digitales (Agbinya, 1996; Porwik y Agniesszka, 2004; Agaian et al., 2006). Algunos sistemas emplean un banco de filtros multi-resolución de análisis con la transformada de onditas para descomponer una señal y los coeficientes de estas señales componentes son reordenados para su almacenamiento o para su transmisión (Sankhan et al., 2007; Elfouly et al., 2008). Para decodificar a la señal se emplea primero el reordenamiento de los coeficientes y las señales componentes entran a un banco de filtros multi-resolución de síntesis con la transformada de ondita. En Avinash y Madhuri (2015) una imagen portadora es transformada usando la transformada de onditas entera para obtener cuatro sub-bandas: LL, LH, HL, y HH y emplean la modificación de la diferencia entre dos coeficientes para ocultar información secreta en los coeficientes de onditas de todas las cuatro sub-bandas. Kumar y Sailaja (2017) realizan marca de agua en señales de audio digital por medio de la transformada de onditas discreta utilizando división en cuadros y empleando los números de Fibonacci para seleccionar las muestras que serán modificadas insertándoles la información a ocultar. Vasantha y Vidheya (2013) utilizan el esquema de elevación (lifting) de la transformada de onditas Haar discreta para insertar bits de información en los bits menos significativos de los coeficientes de las sub-bandas componentes de una imagen e implementan el método en un microprocesador Micro blaze embebido en un dispositivo FPGA. Raheem y Ghazali (2013) generan imágenes fractales cuyo código se convierte en secuencias binarias para ser insertadas en una imagen por medio de la transformada de onditas Haar discreta en las bandas de alta frecuencia LH-HH-HL.

Roldan et al. (2016) utilizan una imagen de medios tonos para aproximar el canal de luminancia y se codifica a los coeficientes de la transformada coseno discreta bidimensional de los canales de crominancia del espacio de color YCbCr para ser utilizados como marca de agua. La información de luminancia se integra en la sub-banda LL y la información de crominancia se integra en las sub-bandas LH y HL de la Transformada de Onditas Entera. Renza et al. (2016) proponen un algoritmo para inserción de una cadena de texto sobre una imagen previamente modificada por la permutación de elementos usando una clave aleatoria y un generador OVFS (Factor de separación variable ortogonal). La inserción se hace en el dominio de la transformada de ondita y utiliza modulación de índice cuantización (QIM). También establecen las condiciones para revertir el proceso y restaurar la información original. Martínez et al. (2010) desarrollaron un método de codificación y decodificación basado en la transformada de onditas Haar discreta multi-resolución para el ocultamiento del mensaje de señales de voz en un ruido aparente proveniente de una de las sub-bandas de la propia señal, el cual implementaron en dispositivos FPGA (Martínez et al., 2016).

A diferencia de los métodos de codificación mencionados en esta sección, que se limita cada uno de ellos a la formación de un solo tipo de estegoseñal, el objetivo de este trabajo que se presenta es obtener un método esteganográfico que permita formar diferentes tipos de estegoseñales mediante la inserción de señales unidimensionales binarias en señales unidimensionales. Para formar la estegoseñal se emplea la transformada de onditas Haar discreta multi-resolución de cuatro etapas, separando a la señal unidimensional portadora en sus componentes de análisis, y se inserta en los bits menos significativos de las muestras de una señal componente procedente de la cuarta etapa, a los bits correspondientes del mensaje de la señal binaria que se desea ocultar. Se aplican las señales componentes de análisis a las entradas de un banco de filtros de síntesis multi-resolución de cuatro niveles de la transformada de onditas Haar discreta, obteniendo como resultado una señal en la que no se percibe la existencia del mensaje de la señal oculta en ella. En las siguientes secciones de este trabajo se desarrolla el método propuesto para la codificación y también el método para la decodificación, y se muestra como realizar el acondicionamiento para que imágenes, señales de voz y códigos fractales de imágenes puedan ser usados como señales unidimensionales portadoras, en las que se puede insertar información de cualquier señal u objeto que se pueda representar en formato binario. Se muestra también como acondicionar textos como señales binarias. Se prueba el método que se propone insertando texto en imagen, también en señales de voz y en códigos fractales de imagen, mostrando su versatilidad para producir diferentes tipos de estegoseñales a diferencia de los mencionados en esta sección.

METODOLOGÍA

Una forma de realizar la Transformada de Ondita Haar Discreta sobre una señal digital $x(i)$, con $i=1,2,\dots,n$, es separándola en dos señales con la mitad de longitud, llamadas señal de tendencia $x_a(j)$ y señal de fluctuación $x_d(j)$, siendo $j=1,2,\dots,n/2$, como se hace en Welstead (1999). La señal de tendencia es obtenida mediante el promedio de dos muestras consecutivas, tomadas de dos en dos sin repetir cualquiera de ellas, y la señal de fluctuación es tomada como la diferencia media de dos muestras consecutivas también tomadas de dos en dos sin repetir cualquiera de ellas, como se indica en las ecuaciones (1) y (2):

$$x_a(j) = [x(i) + x(i-1)]/2 \quad (1)$$

$$x_d(j) = [x(i) - x(i-1)]/2 \quad (2)$$

Si se requiere reconstruir la señal a partir de sus dos señales componentes, se rehacen dos muestras consecutivas $x(i-1)$ y $x(i)$ de acuerdo a las ecuaciones (3) y (4), con $i=2j$, y $j=1,2,\dots,n/2$.

$$x(i) = x_a(j) + x_d(j) \quad (3)$$

$$x(i-1) = x_a(j) - x_d(j) \quad (4)$$

De esta manera se realiza una etapa de síntesis de la Transformada Haar Discreta. La Fig. 1 muestra a bloques la forma de implementar la transformada de onditas Haar discreta, en su forma directa y en su forma inversa.

Si la señal de tendencia es descompuesta también en dos señales, una de tendencia y la otra de fluctuación, tendremos como resultado la descomposición de la señal original $x(i)$ en cuatro señales: una señal de tendencia $x_{a1}(j)$ una señal de fluctuación $x_{d1}(j)$, una señal de tendencia $x_{a2}(k)$ y una señal de fluctuación $x_{d2}(k)$, donde $k=1,2,\dots,n/4$. Cuando una señal es descompuesta en esta forma se dice que se ha realizado sobre ella un análisis Haar multi-resolución de dos niveles. El análisis multi-resolución puede extenderse a más niveles y, para un banco de filtros de análisis multi-resolución de 4 niveles con la transformada de onditas discreta Haar obtenemos las señales componentes del análisis: $x_{d1}(j)$, $x_{a1}(j)$, $x_{d2}(k)$, $x_{a2}(k)$, $x_{d3}(l)$, $x_{a3}(l)$, $x_{d4}(m)$ y $x_{a4}(m)$. En Martínez et al. (2010) se describe la realización de un banco de filtros de análisis multi-resolución de 4 niveles de la transformada de onditas Haar discreta, así como un banco de filtros de síntesis multi-resolución de 4 niveles de la transformada de onditas Haar discreta.

Si se conectan directamente el banco de filtros de análisis y el banco de filtros de síntesis multi-resolución de la transformada de onditas Haar discreta, y en la entrada se suministra una señal $x(i)$, entonces a la salida se obtendrá la señal de salida $x(i-h)$, que es una versión idéntica de la señal de entrada retardada en h muestras. La Fig. 2 muestra a bloques la implementación de un banco de análisis multi-resolución de 4 niveles seguido de un banco de síntesis multi-resolución de 4 niveles. Si alteramos cualquiera de las señales componentes resultantes de las salidas del filtro de análisis, entonces a la salida del banco de filtros de síntesis obtendremos una señal $x'(i-h) \neq x(i-h)$. En Martínez et al. (2010), la componente $x_{a4}(m)$ de una señal de voz $x(i)$, se escala de manera tal que la señal de salida del banco de síntesis $x'(i-h)$ porta la misma información que $x(i)$ pero en ella ya no se reconoce el mensaje de voz que portaba $x(i)$ y la señal $x'(i-h)$ se percibe como ruido aparente en el que se encuentra oculto el mensaje de voz. En este trabajo se altera una de las componentes $x_{ap}(r)$, donde $p = 1,2,3,4$ y $r = j, k, l, m$, reemplazando los bits menos significativos de sus muestras por los bits del mensaje $z(r)$ que se ocultará, de modo que la señal resultante $x'(i-h)$ sea indistinguible de la señal portadora $x(i)$, esto significa que $x'(i-h) \approx x(i-h)$.

Fig. 1: La transformada de onditas Haar discreta. a) La Transformada directa. b) La transformada inversa

Se asume que la señal portadora está integrada por muestras representadas mediante números enteros, y que para insertar el mensaje a ocultar este se representa como una señal $z(r)$ unidimensional binaria entera de un solo dígito y tiene igual razón de muestreo que la componente $x_{ap}(r)$. La operación descrita en la ecuación (5) y aplicada sobre la señal $x_{ap}(r)$ nos permite sustituir el q -ésimo bit de cada una de las muestras de $x_{ap}(r)$, reemplazándolos por los bits de la señal $z(r)$, donde $q = -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7$. Se prefiere escoger los primeros valores no negativos de q para la posición del bit de remplazo, y se mantiene el mismo para

todas las muestras de la señal componente $x_{ap}(r)$. La Fig. 3 a) muestra cómo realizar la operación de inserción de los bits de la señal $z(r)$. Si escogemos el bit de la posición 0, entonces el proceso se simplifica y podremos realizar la operación de remplazo de la ecuación (6) como se muestra en la Fig. 3 b).

Fig. 2: Bancos de filtros multi-resolución de 4 niveles de la Transformada de Onditas Haar Discreta, a) Banco de análisis para la transformada directa, b) Banco de síntesis para la transformada inversa.

Fig. 3: Diagrama a bloques del procedimiento para insertar información: a) en el q -ésimo bit de las muestras de una señal, b) inserción de información en el bit 0 de las muestras de una señal.

$$x'_{ap}(r) = \text{floor}[(\text{floor}[x_{ap}(r)/2^q] * 2^q) / 2^{(q+1)}] * 2^{(q+1)} + x_{ap}(r) - (\text{floor}[x_{ap}(r)/2^q] * 2^q) + z(r) * 2^q \quad (5)$$

$$x'_{ap}(r) = \text{floor}[(\text{floor}[x_{ap}(r)] / 2) * 2] + x_{ap}(r) - (\text{floor}[x_{ap}(r)]) + z(r) \quad \text{si } q = 0 \quad (6)$$

Se escogió a la señal componente $x_{a4}(m)$ como portadora, y la señal $z(m)$ a ocultar tiene la misma razón de muestreo que ésta. La Fig.4 muestra el banco de filtros de análisis y de síntesis multi-resolución que empleando la transformada de onditas discreta Haar de 4 niveles descompone a la señal portadora, inserta en la componente $x_{a4}(m)$ a la señal $z(m)$ y reintegra a los componentes de la señal para producir la estegoseñal $x'(i-h)$. Para recuperar a la señal $z(m)$ extrayéndola del q -ésimo bit de las muestras de la estegoseñal, se entrega $x'(i-h)$ como señal de entrada a un banco de análisis multi-resolución de cuatro etapas de la transformada de onditas Haar discreta para separarla en sus señales componentes $x_{d1}(j)$, $x_{d2}(k)$, $x_{d3}(l)$, $x_{d4}(m)$ y $x'_{a4}(m)$ y se aplica sobre la componente $x'_{a4}(m)$ la operación de la ecuación (7), que se aplica como en la Fig. 5 a). Si la señal $z(m)$ se encuentra insertada en el plano de bit 0 de las muestras de la estegoseñal, entonces se simplifica la ecuación (7) resultando en la ecuación (8), que se implementa como se muestra en la Fig. 5 b).

$$z(m) = \text{floor}(x'_{a4}(m)/2^q) - \text{floor}(x'_{a4}(m)/2^{(q+1)}) * 2 \quad (7)$$

$$z(m) = \text{floor}(x'_{a4}(m)) - \text{floor}(x'_{a4}(m)/2) * 2 \quad (8)$$

Después de la extracción del mensaje no se conserva la estegoseñal y no se reintegran los componentes de

la señal portadora para obtener una versión $x_0(i-h)$ de donde se extrajo el nivel de bit 0 de todas las muestras de la señal componente $x_{a4}(m)$. Por ello el proceso de la decodificación se simplifica y solo se requiere el banco de análisis multi-resolución de 4 niveles de la transformada discreta de onditas Haar, como se muestra en la Fig. 6.

Fig.4: Codificador esteganográfico que usa un banco de filtros de análisis y de síntesis multi-resolución que empleando la transformada de onditas discreta Haar de 4 niveles

Fig. 5: a) Extracción de los bits de una señal binaria insertada en el q-ésimo bit de las muestras de una señal portadora. b) Extracción de la señal insertada en dígito binario de posición 0 de las muestras de una señal portadora.

Fig. 6: Extracción de la señal $z(m)$, separando la estego señal $x'(i-h)$ en sus señales componentes y extrayendo $z(m)$ de la estego componente $x'_{a4}(m)$

El método esteganográfico se implementó en la herramienta software SIMULINK de Matlab. Para mostrar el funcionamiento del método se realizaron pruebas con tres tipos de señales como portadoras: imagen, señal de voz y código fractal de imagen; las que se acondicionaron para darles el formato de señales unidimensionales. Como señal a ocultar se seleccionó un texto, mismo que se acondicionó al formato de señal binaria unidimensional.

Para realizar la prueba de esteganografía sobre imagen, se utiliza como señal portadora a una imagen en formato .tif, en escala de grises, de tamaño 512x512 píxeles. Se seleccionó como imagen de prueba a la imagen conocida como “Lena” porque es una imagen utilizada en forma estándar en el procesamiento de señales, pero en Esteganografía no se usan imágenes conocidas. Cada uno de los píxeles se representa por un número entero de 8 bits, en el rango de 0 a 255. La imagen se acondiciona para convertirla en una señal vectorial unidimensional $x(i)$, donde $i = 1, 2, \dots, 262144$, compuesta por $N_o = 262144$ muestras. Para formar la señal portadora $x(i)$ se concatenan los renglones de la imagen según el patrón de barrido mostrado en la Fig. 7. Cuando se somete la señal portadora a la entrada del banco de filtros de análisis se producen las señales componentes multi-resolución. La capacidad de cada señal componente para albergar muestras de N bytes es de $N_o/2^{(r+3N)}$, donde r es el nivel de la señal componente. La capacidad total de inserción en todas las señales compontes es de 32768 bytes.

En cada etapa de análisis multi-resolución las señales componentes se reducen en longitud en un factor de dos con respecto su señal de entrada, por ello, la señal componente $x_{a4}(m)$ tiene 16384 muestras. Si cada muestra del mensaje a ocultar se codifica con 8 bits, entonces la señal componente $x_{a4}(m)$ tiene capacidad para ocultar 2048 muestras de 8 bits o 16384 muestras binarias.

Fig. 7: Vectorización de la imagen para convertirla en una señal $x(i)$ de 512x512 muestras.

Se escogió como el mensaje a ocultar a un extracto de 2048 caracteres del primer capítulo de la obra “Don Quijote de la Mancha” de Miguel de Cervantes Saavedra, del que se reproduce aquí un fragmento con 325 caracteres: “PRIMERA PARTE CAPÍTULO 1: Que trata de la condición y ejercicio del famoso hidalgo D. Quijote de la Mancha. En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor. Una olla de algo más vaca que carnero, ...” (Cervantes, 2015). Cada uno de los caracteres de texto se representa con un número entero binario de 8 bits, y la obra de texto se considera como una concatenación de caracteres de texto. Procediendo de esa forma, cualquier mensaje de texto puede representarse como una concatenación de números binarios de 8 bits. Se escribieron rutinas en Matlab para realizar la tarea de acondicionar la imagen como señal unidimensional $x(i)$ y acondicionar también el contenido de un archivo de texto como señal binaria $z(m)$. Las señales $x(i)$ y $z(m)$ se entregan como entradas al modelo del método esteganográfico en SIMULINK para obtener como resultado una estegoseñal $x'(i-h)$.

La prueba de esteganografía en señal de voz se realiza utilizando también señal de voz muestreada a 16000 muestras/s, como señal portadora. La señal de voz se grabó en un archivo de formato .wav y fue acondicionada en Matlab para que las muestras tuvieran una amplitud de 0 a 255 requiriéndose una representación como número entero de 8 bits para cada muestra. Se sometió la señal de voz como señal portadora $x(i)$ de entrada al sistema codificador y para poder insertar en la señal los 2048 caracteres de texto se emplearon 262144 muestras de la señal de audio de las cuales se usaron 16384 muestras en el cuarto nivel de análisis de la transformada de ondita Haar para insertar en ellas el mensaje de texto, por lo que se usó una grabación de voz de más de 16.384 s.

La prueba de esteganografía en código fractal de imagen se hizo utilizando el código fractal de una imagen como señal portadora haciendo la inserción del texto en el código fractal de la imagen, la cual fue codificada

mediante un sistema de funciones iteradas particionado (PIFS por sus siglas en inglés). El Método de Codificación Fractal de Imagen mediante un Sistema de Funciones Iteradas Particionado (FIC – PIFS por sus siglas en inglés) propuesto por Jacquin (1992), establece que una imagen I en escala de grises puede ser representada en forma aproximada por medio de un sistema de $N_R \times N_R$ funciones iteradas $W = w_1 U w_2 U w_3 \dots U w_U \dots U w_{N_R \times N_R}$ las cuales tienen la forma dada en la ecuación (9):

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = w_i \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \\ o_i \end{bmatrix} \quad (9)$$

Al iterar estas, producen un conjunto de bloques de subimágenes que converge a la representación de la imagen I . Cada función perteneciente a ese sistema representa la transformación espacial, la de brillo y la de contraste que se aplican a un sector de la imagen llamado dominio D_i para con el representar a un bloque de menor tamaño de la imagen denominado rango R_i .

Los parámetros (i, e_i, f_i, s_i, o_i) forman el código fractal con el que se forma un bloque rango. Se utiliza el código fractal de la imagen “Lena”, que fue dividida en bloques rango de 4×4 píxeles cada uno de ellos, por lo que se procesó un código fractal compuesto de 16384 conjuntos de parámetros (i, e_i, f_i, s_i, o_i) . Los parámetros (i, e_i, f_i) relacionados con la transformación espacial hacen referencia a un bloque rango en específico y no pueden ser modificados sin alterar de manera significativa la imagen que representan, sin embargo si los parámetros s_i y o_i son alterados en forma poco significativa, se ocasionan cambios poco perceptibles en la imagen que representan. En Martínez et al. (2006) se considera el efecto de tomar el parámetro de ajuste de contraste s_i como constante ($s_i = 0.5$). Se usó esa forma de codificación fractal para propósitos de prueba de nuestro método de codificación esteganográfico y se tiene considera como la señal portadora $x(i)$ a la formada por los parámetros de ajuste de brillo o_i con $i = 1, 2, \dots, 16384$. El mensaje de texto se inserta en los 16384 parámetros o_i relacionados con la transformación en el brillo de cada i -ésimo bloque rango con respecto del i -ésimo bloque dominio asociado del código fractal de la imagen I .

Para los tres tipos de prueba la señal portadora $x(i)$ se procesa con una razón de muestreo $f_{s1} = 16000$ muestras/s, por lo que el periodo de muestreo es de $62.5 \mu s$. La razón de muestreo para las señales componentes pertenecientes al nivel q de análisis está dada por $f_{sq} = f_{s1}/2^{(q-1)}$. Para la realización de las pruebas con imagen y con código fractal de imagen, usadas como señal portadora, la razón de muestreo no impone ninguna limitante, pero se usó esta razón de muestreo porque el método también se probó con señal de voz como portadora y esta se procesó a la razón de 16000 muestras/s.

RESULTADOS

De los resultados de la prueba de esteganografía en imagen, la Fig. 8 a) muestra la comparación entre la señal portadora de entrada $x(i)$ y la estegoseñal $x'(i-h)$. La estegoseñal presenta un retardo $h = 15$ muestras ($937.5 \mu s$) debido a la latencia propia del procesamiento en los bancos de filtros. La Fig. 8 b) muestra la gráfica de las señales $x(i-h)$ y $x'(i-h)$. En la Fig. 9 a) se muestra un acercamiento de la Fig. 8b) y puede observarse que la señal de entrada $x(i-h)$ y la estegoseñal $x'(i-h)$, difieren de valor en 0 o ± 1 en cada una de sus muestras, lo cual era un objetivo a alcanzar, que fueran prácticamente indistinguibles una de la otra. La Fig. 9 b) muestra la señal de error, que es definida como: $x_e(i-h) = x'(i-h) - x(i-h)$.

La señal $z(m)$ con mensaje de texto a ocultar se procesó con una razón de muestreo igual a la de la componente $x_{a4}(m)$, $f_{s4} = 1000$ muestras/s, teniendo un periodo de muestreo de 1 ms. En la Fig. 10 se muestra, en rojo un fragmento de la señal binaria $z(m)$ correspondiente al texto insertado en la imagen portadora $x(i)$, y en color azul a la señal binaria correspondiente al texto $z(m-1)$ extraído de la estegoimagen. La señal recuperada corresponde al texto insertado pero tiene un retardo de una muestra. La señal $z(m)$ se muestra con un nivel añadido de dos unidades para facilitar la visualización simultánea de ambas señales. En la Fig. 11 a) se muestra la imagen “Lena” original y en la Fig. 11 b) se muestra la imagen esteganográfica con el texto insertado. La estegoimagen de “Lena” se forma a partir de la señal $x'(i-h)$ donde $h = 15$ muestras. Se escribió una rutina en Matlab que extrae a partir de la muestra $i = h$ de la señal $x'(i-h)$ a los renglones de la matriz de la imagen. El método de decodificación logró recuperar la señal binaria que se hallaba insertada en la estegoimagen.

Para medir la semejanza entre la imagen original y la estegoimagen se utiliza el criterio de distorsión de la raíz de la media cuadrática δ_{RMSE} (RMSE por sus siglas en inglés), que aplicamos a las señales de imagen y a la estegoimagen según la ecuación (10).

Fig. 8: a) Comparación entre la señal portadora $x(i)$ y la estegoseñal $x'(i-h)$, b) comparación entre la imagen portadora retrasada en h muestras $x(i-h)$ y la estegoseñal $x'(i-h)$

Fig. 9: a) Detalle de la comparación entre la imagen portadora retrasada en h muestras $x(i-h)$ y la estegoseñal $x'(i-h)$, b) señal de error $x_e(i-h)$

Fig. 10: Comparación entre el mensaje oculto $z(m)$ y el mensaje $z(m-1)$ extraído en el decodificador.

Fig. 11: a) Imagen "Lena" original. b) Estegoimagen con el texto insertado

$$\delta_{RMSE} = \frac{1}{n} \sqrt{\sum_{i=h}^{n+h} (x(i-h) - x'(i-h))^2} \quad (10)$$

Otra medida utilizada para expresar la semejanza es la "razón señal a ruido pico en dB" ($PSNR_{dB}$ por sus siglas en inglés), la cual se calcula según la ecuación (11) como:

$$PSNR_{dB} = 20 \cdot \log_{10}(255/\delta_{RMSE}) \quad (11)$$

Para la imagen de "Lena" representada en $x(i-h)$ y la estegoimagen de "Lena" $x'(i-h)$ que tiene insertados los 2048 caracteres del texto $z(m)$ se obtiene $\delta_{RMSE} = 0.7109$ y $PSNR_{dB} = 51.0945$.

En la prueba de esteganografía en señales de voz el método fue probado usando como señal portadora $x(i)$ a señales de voz. La Fig. 12 muestra en: a) la gráfica de una señal de voz portadora $x(i)$ y en b) se muestra la estegoseñal $x'(i-h)$, c) ambas señales son graficadas presentando solo un segmento de ellas, y puede apreciarse el retardo de $h = 15$ muestras ($937.5 \mu s$) de la estegoseñal con respecto a la señal portadora. En d) se muestra la comparación de un segmento de la señal portadora retardada $x(i-h)$ y el segmento correspondiente de la estegoseñal $x'(i-h)$.

Los parámetros de semejanza de la estegoseñal respecto a la portadora son $RMSE = 0.6877$ y $PSNR_{dB} = 51.3834$. La Fig. 13 muestra el mensaje oculto y el mensaje extraído de la estegoseñal.

Fig. 12: a) señal de voz que se usa como portadora, b) estegoseñal de voz en la que se ha insertado un mensaje de texto, c) comparación de la señal de voz portadora y la estegoseñal, d) comparación de la señal portadora retardada en $h = 15$ muestras y la estegoseñal de voz.

Fig. 13: Mensaje de texto insertado $z(m)$ al cual se la han añadido dos unidades para mostrarlo en la misma gráfica ($z(m)+2$) y el mensaje extraído $z(m-1)$, retardado en una muestra ($1 ms$).

En la prueba de esteganografía en código fractal PIFS de una imagen, cuando se usó como señal portadora de entrada $x(i)$ al conjunto de 16384 parámetros α_i del código fractal de la imagen "Lena" para insertar en ellos al mensaje de texto $z(m)$, se obtuvo como señal de salida una estegoseñal que contiene los parámetros correspondientes al brillo en el código fractal. La señal de brillo portadora de entrada $x(i)$ se muestra en la Fig. 14 a). En la Fig. 14 b) se muestra la estegoseñal de brillo correspondiente $x'(i-h)$. En la Fig. 14 c) se comparan la señal de entrada y la estegoseñal de brillo, notándose su similaridad y que la estegoseñal presenta un retraso de 15 muestras ($937.5 \mu s$). La Fig. 14 d) compara a la señal portadora de brillo retrasada en h muestras $x(i-h)$ con la estegoseñal de brillo $x'(i-h)$. En esta gráfica se puede apreciar la similitud de la estegoseñal con la señal portadora. La Fig. 15 muestra la señal binaria del mensaje de texto insertado $z(m)$ al cual se la han añadido dos unidades para mostrarlo en la misma gráfica ($z(m)+2$) y el mensaje de texto recuperado $z(m-1)$, retardado en una muestra ($1 ms$).

Para medir el resultado del método esteganográfico cuando se implementa sobre código fractal, en este caso específico sobre los parámetros de ajuste de brillo, se midió los parámetros de calidad $RMSE = 0.6988$ y $PSNR_{dB} = 51.2441$ de la estegoseñal $x'(i-h)$ con respecto a la señal $x(i-h)$, y también se midió el efecto de la inserción del mensaje de texto en la imagen producto de la iteración del código fractal completo que incluye a nuestra estegoseñal de brillo, en comparación con la imagen que se produce al iterar el código fractal completo original y se obtuvo $RMSE = 1.6846$ y $PSNR_{dB} = 43.6011$. La Fig. 16 a) muestra la imagen de "Lena" generada con el código fractal iterado y la Fig 16 b) muestra la imagen generada con el estegocódigo fractal en el que específicamente se modificaron los parámetros de ajuste del brillo insertando en estos parámetros el mensaje de texto.

Fig. 14: a) señal de brillo α_i que se usa como portadora $x(i)$, b) estegoseñal de brillo $x'(i-h)$ en la que se ha insertado un mensaje de texto, c) comparación de la señal de brillo portadora y la estegoseñal, d) comparación de la señal portadora retardada en $h = 15$ muestras y la estegoseñal de brillo

Fig. 15: Mensaje de texto insertado $z(m)$ al cual se la han añadido dos unidades para mostrarlo en la misma gráfica ($z(m)+2$) y el mensaje de texto recuperado $z(m-1)$, retardado en una muestra (1 ms)

Fig.16: a) Imagen "Lena" generada con codificación fractal PIFS. b) Estegoimagen de "Lena" generada con la codificación fractal PIFS y con el texto insertado en el parámetro de control de brillo α_i

DISCUSIÓN DE LOS RESULTADOS

El método de codificación esteganográfica que se presenta, a diferencia de otros encontrados en la literatura (Avinash y Madhuri, 2015; Raheem y Ghazali, 2013; Roldan et al. 2016), utiliza la transformada de onditas Haar discreta multi-resolución de cuatro niveles y puede insertar información en señales unidimensionales a través de sus señales componentes procedentes de la etapa de análisis. Para extraer el mensaje oculto el método de decodificación utiliza un banco de filtros de análisis multi-resolución de cuatro etapas. El proceso de decodificación es ciego, lo que significa que no necesita conocerse la señal portadora original para lograr extraer el mensaje oculto en la estegoseñal, como lo hacen en Al-Korbi et al. (2016). Por utilizar solamente un banco de filtros multi-resolución de análisis y de síntesis para codificar imágenes, el método propuesto es más simple que aquellos que hacen codificación de imágenes con la transformada de onditas en sus cuatro bandas LL-LH-HL-HH (Al-Korbi et al. 2016; Avinash y Madhuri, 2015; Badescu y Dumitrescu, 2014; Raheem y Ghazali, 2013; Roldan et al. 2016).

En este trabajo se utiliza el método propuesto para ocultar mensajes de texto en imagen, en señales de voz y en código fractal de imagen, acondicionando estas para representarlas como señales unidimensionales. La calidad de la estegoseñal, se midió a través de los parámetros $RMSE$ y $PSNR_{dB}$, obteniéndose resultados comparables al $PSNR_{dB} = 51.93$ reportado por Laskar S. y K. Hemachandran (2012) y mejores que otros métodos que realizan esteganografía de texto en imagen (Renza, D. et al. 2016) o esteganografía de imagen en imagen (Roldan et al., 2016; Avinash y Madhuri, 2015; Badescu y Dumitrescu, 2014; Raheem y Ghazali, 2013). Sin embargo se tiene una menor capacidad de inserción en comparación con todos ellos, porque se utiliza solamente la componente x_{a4} para insertar información.

Cuando se inserta el mensaje de texto en la señal de voz, se obtienen resultados de calidad de la estegoseñal de voz muy similares a los obtenidos para la estegoimagen cuando se inserta texto en imagen. En la estegoseñal de voz no se percibe la presencia de la información insertada y en ambos casos, para cada muestra de la señal portadora, la muestra respectiva de la estegoseñal difiere en 0, en 1 o en -1. Cuando se realiza la inserción de información en códigos de imágenes generadas fractalmente mediante FIC-PIFS, se obtiene una estegoseñal que contiene los parámetros de brillo modificados, y que añadidos al código fractal forman un estegocódigo fractal. Cuando se itera el estegocódigo se produce una estegoimagen generada fractalmente, que tiene gran similitud a la generada con el código fractal original sin modificar, como puede comprobarse en la Fig. 16. Los valores de $RMSE$ y $PSNR_{dB}$ del estegocódigo son similares a los obtenidos con las pruebas de inserción de texto en imagen y de texto en señales de voz. En Raheem y Ghazali (2013), utilizan la transformada de onditas Haar discreta bidimensional de un solo nivel de resolución para insertar en una imagen el estegocódigo fractal de otra imagen, generado por un método al que denominan de "Desplazamiento del Punto Medio". Su método tiene mayor capacidad de inserción que el método que presenta este trabajo, pero no obtiene mejor calidad en la estegoseñal.

Las principales características del método propuesto son: las señales se procesan en forma unidimensional y esto requiere el uso de solamente un banco de filtros de análisis multi-resolución y un banco de filtros de síntesis multi-resolución para formar la estegoseñal; la versatilidad, debido a que pueden emplearse como señales portadoras a diferentes tipos de señales tales como imágenes, señales de voz y códigos fractales de imagen, cuando otros métodos se restringen únicamente a la esteganografía en imágenes (Again et al., 2006; Avinash y Madhuri, 2015; Badescu y Dumitrescu, 2014; Raheem y Ghazali, 2013; Vasantha y Vidheya, 2013); el método de decodificación y extracción del mensaje oculto es aún más simple que el de codificación; el método es ciego, por lo que el decodificador no requiere conocer la imagen portadora original y solamente necesita a la estegoseñal para operar; ambos métodos, el de codificación y el de decodificación tienen baja complejidad porque involucran solamente operaciones como sumas, restas, retardos, multiplicaciones y divisiones en potencias de dos, haciendo factible su implementación en arreglos de compuertas programables por campo y dispositivos lógicos programables complejos (FPGA y CPLD respectivamente, por sus siglas en inglés), como se hace en Martínez et al. (2016); el codificador presenta una latencia de 15 muestras entre la señal portadora y la estegoseñal, que con el periodo de muestreo de 0.000625 s que se usó para las simulaciones, corresponde a una latencia de 937.5 μ s, lo que permite que este método pueda aplicarse al procesamiento esteganográfico de señales de voz en tiempo real.

CONCLUSIONES

En este trabajo se diseñó un método de codificación esteganográfico que inserta mensajes en señales unidimensionales sin que sean perceptibles, utilizando bancos de filtros multi-resolución de análisis y de síntesis de la Transformada de Onditas Haar Discreta. Se diseñó un método para la decodificación y recuperación del mensaje insertado en la estegoseñal. El método de codificación fue diseñado para usarse con señales unidimensionales, y se mostró que es versátil porque puede aplicarse a otro tipo de señales acondicionándolas al formato de señales unidimensionales, pudiendo ser usado para insertar texto en imagen,

texto en señales voz y texto en código fractal de imagen. El método de decodificación es ciego y solamente necesita conocer la estegoseñal para poder extraer el mensaje oculto. El codificador y el decodificador son adecuados para implementarse como sistemas electrónicos, debido a que involucran operaciones de baja complejidad. El codificador tiene una latencia de 15 muestras, que lo hace adecuado para emplearse en aplicaciones de esteganografía en señales de voz en tiempo real.

REFERENCIAS

- Agaian, S.S., O. Caglayan, J. Perez, H. Sarukhanyan, J. Astola, *Golden Ratio-Haar Wavelet Based Steganography*, Proceedings of the 2006 International TICSP Workshop on Spectral Methods and Multirate Signal Processing, SMMSP2006, Florence, Italy, September 2006, TICSP, 121-126 (2006)
- Agbinya, J.I., *Discrete Wavelet Transform Techniques in Speech Processing*, Proceedings. 1996 IEEE TENCON, Digital Signal Processing Applications, 2, 514-519 (1996)
- Al-Korbi, H., A. Al-Ataby, M. Al-Taei y W. Al-Nuaimy, Highly Efficient Image Steganography Using Haar DWT For Hiding Miscellaneous Data, doi: 10.5455/jcit.71-1450117397, Jordanian Journal of Computers and Information Technology (JJCIT), 2(1), 17 - 36 (2016)
- Avinash, K. G. y S. J. Madhuri, An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach, doi:10.1155/2015/684824, Mathematical Problems in Engineering, 1 - 11 (2015)
- Badescu I. y C. Dumitrescu, *Steganography in Image Using Discrete Wavelet Transformation*, Proc. WSEAS Conf. on Advances in Mathematical Models and Production Systems in Engineering, Brasov, Romania, 69-72, 26-28 (2014)
- Cervantes, M., El ingenioso hidalgo don Quijote de La Mancha, 1ª Parte (Ed. Enrique Suárez Figaredo), Lemir 19, p. 19 (2015)
- Elfouly, F.H., M.I. Mahmoud, M.I.M. Dessouky y S. Deyab, Comparison between Haar and Daubechies, Wavelet Transformations on FPGA Technology, International Journal of Electronics and Communication Engineering, 2(1), 96 – 101 (2008)
- Jacquin, A. E., Image Coding Based on a Fractal Theory of Iterated Contractive Image Transformations, IEEE Transactions on Image Processing, 1(1), 18-30 (1992)
- Kumar, M. y M. Sailaja, Digital Audio Watermarking With Discrete Wavelet Transform Using Fibonacci Numbers, International Journal of Innovative Research in Science, Engineering and Technology, 6(9), 18294 - 18299 (2017)
- Laskar, S. y K. Hemachandran, High Capacity Data Hiding Using LSB Steganography and Encryption, doi: 10.5121/ijdm.2012.4605, International Journal of Database Management Systems, 4(6), 57–68 (2012)
- Martínez, A., A. Díaz, M. Linares y J. Vega, Arquitectura Simple y Modular para Compresión Fractal de Imágenes utilizando Árbol Cuádruple Multi-Resolución, doi:10.4067/S0718-07642006000100010, Información Tecnológica 17(1), 77-84 (2006)
- Martínez, A., A. Ramos, I. Compeán y R. Ávila, Message Concealment System of Voice Signals Implemented on FPGA, doi:10.1109/TLA.2016.7786334, IEEE Latin America Transactions, 14(8), 3554 - 3559 (2016)
- Martínez, A., Z. Pineda, A. Ramos, Ocultamiento del Mensaje de Señales de Voz usando la Transformada de Ondita Haar Discreta, doi: 10.4067/S0718-07642010000300015, Información Tecnológica, 21(3), 135-140 (2010)
- Porwik, P. y A. Lisowska, The Haar-Wavelet Transform in Digital Image Processing: Its Status and Achievements, Machine GRAPHICS & VISION, 13(1-2), 79-98 (2004)
- Raheem, A. I., S. Ghazali, Wavelet Fractal Image Watermarking System, IJCSI International Journal of Computer Science Issues, 10(6), No 2, 102–109 (2013)
- Renza, D., D.M. Ballesteros y H.D. Ortiz, Text Hiding in Images Based on QIM and OVSF, doi:10.1109/TLA.2016.7459600, IEEE Latin America Transactions, 14(3), 1206 - 1212, March (2016)
- Roldan, L. R., M. C. Hernández, J. Chao, M. N. Miyatake y H. P. Meana, Watermarking-based Color Image Authentication With Detection And Recovery Capability, doi:10.1109/TLA.2016.7437257, IEEE Latin America Transactions, 14(2), 1050 – 1057 (2016)
- Sankhan, S.B., N. Abdulmuhsen y N.F. Al-Tahan, *A Proposed Analog Speech Scrambler Based on Parallel Structure of Wavelet Transforms*, National Radio Science Conference, 2007, NRSC 2007, 1-12 (2007)
- Vasanth, L.B., R.B. Vidheya, FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor, International Journal of Computer Trends and Technology (IJCTT) ISSN: 2231-2803, 6(1), 6 – 14 (2013)
- Welstead, S., Fractal and Wavelet Image Compression, Tutorial Text in Optical Engineering, Volumen TT40, SPIE Optical Engineering Press, pp. 93-117 (1999)