ENCRIPTACIÓN DE SEÑALES BINARIAS POR MEDIO DE WAVELETS SEUDOCAÓTICAS

RESUMEN
En este trabajo se explora la Transformada Wavelet Sobrecompleta (OCWT), una descomposición frecuencia-tiempo en funciones de base no ortonormales, para la construcción de un sistema de encriptación de información binaria usando como función wavelet un vector de datos pseudocaótico. Se hace énfasis en los aspectos de implementación del sistema sobre un procesador digital de señales (DSP) de punto flotante tales como: la generación de la wavelet madre, las optimizaciones del cálculo de la Transformada Wavelet Sobrecompleta y la sincronización entre el receptor y transmisor.

PALABRAS CLAVES: Encriptación, Caos, Transformada Wavelet Sobrecompleta, OCWT

ABSTRACT
Overcomplete Wavelet Transform (OCWT) offers a frequency-time decomposition by means of a set of no-orthogonal base functions. In this paper, that transform feature is researched in order to develop an encryption system for binary signal by using a mother wavelet based on a pseudochaotic vector. Implementation details on a floating-point digital signal processor (DSP) such as: generation of the pseudochaotic wavelet mother, optimization for computing the overcomplete wavelet transform and synchronization between transmission and receptor systems, are deeply described.

KEYWORDS: *Encryption, Chaos, Overcomplete Wavelet Transform OCWT.*

JORGE I. MARÍN
Lic. Electricidad y Electrónica, Msc.
Profesor Asistente
Grupo de Procesamiento Digital de Señales y Procesadores-GDSPROC
Universidad del Quindío
jimarinh@ieee.org

ANTONIO RAMOS
Ingeniero Electrónico
Grupo de Procesamiento Digital de Señales y Procesadores-GDSPROC
aramosm2003@yahoo.com.ar

GERMAN A. RAMÍREZ
Ingeniero Electrónico
Grupo de Procesamiento Digital de Señales y Procesadores-GDSPROC
gara613@hotmail.com

1. INTRODUCCIÓN

Actualmente, los sistemas de mayor difusión y amplio uso para encriptar información se basan en criptografía digital. Dicha masificación se justifica por la facilidad de implementación en arquitecturas digitales y a que ofrecen una recuperación perfecta de la información. Sin embargo, recientemente, y ante la vulnerabilidad que han mostrado algunos de estos métodos, se realizan esfuerzos por generar sistemas de criptográfica basados en señales análogas, los cuales prometen tener una mayor seguridad, debido a la alta redundancia, y a la posibilidad de transmisión por medios diferentes a las redes de datos convencionales. Entre los sistemas de encriptación analógica se destacan los basados en caos [1],[2],[3] y los que emplean transformadas [4],[5].

Los sistemas de encriptación con caos fueron propuestos inicialmente por Pecora y Carroll en 1990 [1], como resultado del descubrimiento de la posibilidad de sincronización de dos sistemas caóticos. Aunque la confiabilidad y seguridad de éste y otros sistemas [2] ha sido debatida por ciertos autores [6], han aparecido recientes esquemas de encriptación basados en hipercaos y observadores lineales [3] que vislumbran ser más robustos y confiables que sus predecesores. El caos ha sido principalmente atractivo para encriptar información, debido a que las señales que generan los sistemas caóticos tienen un ancho de banda infinito, y son determinísticas, pues dependen del sistema y su condición inicial.

Por otra parte, en lo referente a los sistemas basados en transformadas, se ha mostrado que es posible emplear la transformada wavelet discreta (DWT, por sus siglas del inglés *Discrete Wavelet Transform*) para generar una señal en espectro esparcido [5], o emplear la transformada wavelet sobrecompleta (OCWT: por sus siglas del inglés *Overcomplete Wavelet Transform*) o transformada wavelet muestreada (SCWT: por sus siglas del inglés *Sampled Continuos Wavelet Transform*) [4]. Las principales ventajas de estos sistemas frente a los caóticos son la mayor facilidad de implementación y de sincronización. El primer esquema, ha tenido buena aceptación en aplicaciones militares, y se fundamenta en que los coeficientes de los filtros de síntesis y reconstrucción se calculan a partir de métodos de optimización que emplean criterios de ortogonalidad y baja probabilidad de intercepción. El segundo método tiene la flexibilidad de poder emplear cualquier función wavelet madre, sin la necesidad de satisfacer condiciones de ortogonalidad de las funciones base. En ambos esquemas se emplea la transformada inversa para sintetizar la señal encriptada y la transformada directa para recuperar la información.
En este trabajo se propone combinar las técnicas de encriptación de señales análogas basadas en caos y transformadas, por medio del empleo de la transformada

Fecha de Recepción: 31 Agosto de 2006
Fecha de Aceptación: 10 Abril de 2007

wavelet sobrecompleta como núcleo básico de síntesis de la señal encriptada y una función wavelet pseudocaótica como función base. Se emplea la OCWT dado que la función wavelet pseudocaótica que se propone no forma una base ortogonal, así mismo, dicha señal se genera a partir de un sistema caótico en tiempo discreto.

2. TRANSFORMADA WAVELET SOBRE-COMPLETA (OCWT)

La representación de la transformada wavelet en tiempo continuo CWT viene dada por el producto interno [4]:

$$F(s,\tau) = \left\langle f(t), \frac{1}{\sqrt{s}}\psi\left(\frac{t-\tau}{s}\right)\right\rangle \quad (1)$$

donde *f(t)* es la señal a transformar, $\psi(t)$ es la wavelet madre o función básica de descomposición y las variables s y τ, corresponden a la escala y la traslación, respectivamente. Para la wavelet madre son condiciones fundamentales el ser una señal de energía y oscilar alrededor de cero, pero no necesariamente formar una base ortogonal. Cuando ésta es una señal de energía arbitraria de base no ortogonal, la versión discreta de la CWT se denomina transformada wavelet sobrecompleta (OCWT: *Overcomplete Wavelet Transform*), y tiene un costo computacional elevado que puede ser reducido al reescribir (1) como un banco de filtros de la forma [4]:

$$F(s,\tau) = f(\tau) * \psi_s(-\tau) \quad (2)$$

con $\psi_s(t)$ la versión escalada de la wavelet madre. La ecuación (2) indica que la representación frecuencia-tiempo F se puede generar a partir del filtrado de la señal f por medio de un conjunto finito de filtros, donde cada filtro tiene una respuesta al impulso $\psi_s(-t)$. Además con el fin de introducir redundancia en la información que facilite el proceso de cálculo de la transformada inversa, se eligen escalas de la forma $s_m = a_0^{-m}$ con $m \in Z$.

Por otra parte, la transformada wavelet sobrecompleta inversa IOCWT se puede calcular a partir de la representación en marcos de la OCWT [4], sin embargo, los algoritmos resultantes son computacionalmente muy costosos y exigen la existencia de la inversa de la matriz de correlación de la función wavelet madre. Como alternativas de solución, de menor precisión pero de factible implementación, está la discretización de la expresión para la Transformada Wavelet Continua Inversa [4]:

$$\hat{f}(\gamma) = C^{-1}\sum_m \hat{F}(s_m,\tau)\hat{\psi}_{s_m}(\gamma) \quad (3)$$

con $\hat{f}(\gamma)$, $\hat{F}(s_m,\tau)$ y $\hat{\psi}_{s_m}(\gamma)$ las transformadas de Fourier de: la señal, coeficientes de la transformada wavelet, y wavelet madre, respectivamente, y C calculado como:

$$C = \sum_m s_m \left|\psi_{s_m}(\gamma)\right|^2 \quad (4)$$

Desde el punto de vista de implementación, el procesamiento de la señal se realiza típicamente por bloques, pues los datos se adquieren por acceso directo a memoria DMA, por lo que la OCWT se puede calcular fácilmente mediante el empleo del algoritmo de la convolución rápida haciendo uso de la técnica de solapamiento y almacenamiento[1] [7]; en cambio la IOCWT se implementa por medio de transformadas rápidas de Fourier (FFT), y para garantizar un procesamiento por bloques se emplea la técnica de solapamiento y suma[2] [7]. Por lo anterior, la complejidad computacional de la OCWT e IOCWT es $O(N\log_2 N)$, lo cual indica que el sistema de encriptación que se propone es más costoso que un sistema basado en DWT.

3. SISTEMA DE ENCRIPTACIÓN PROPUESTO

El esquema de encriptación propuesto en este trabajo se ilustra en la figura 1. En ésta la información a encriptar se introduce al sistema como los coeficientes wavelet de una transformada inversa. Con el fin de facilitar el proceso de decodificación, la señal a encriptar debe ser información binaria. De esta forma, a la salida de la IOCWT se genera una señal unidimensional que puede ser fácilmente transmitida por algún método análogo y en el receptor se emplea la OCWT para recuperar los bits de información. Tanto para el cálculo de la IOCWT como de la OCWT se emplearon bloques de datos de 1024 elementos y para la generación de la función base en cada una de las escalas un factor a_0=1,04.

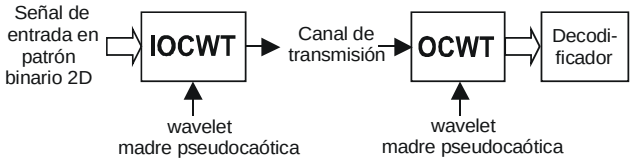

Figura 1. Diagrama de bloques del sistema de encriptación propuesto.

3.1. Generación de la wavelet madre pseudocaótica

La wavelet madre pseudocaótica se generó con el sistema dinámico en tiempo discreto,

$$x[k] = x[k-1]^2 + c \quad (5)$$

tomando c = -1,95 y diferentes condiciones iniciales. A partir de esta función se generan 128 elementos que posteriormente se interpolan para obtener una señal de

[1] Los últimos N_ψ-1 datos de cada bloque de entrada se almacenan para ser introducidos como los primeros datos del siguiente bloque y de la solución se descartan los primeros N_ψ-1 datos

[2] Los últimos N_ψ-1 datos de cada solución se suman a la siguiente trama de salida

longitud 1024, paso siguiente se aplica una ventana y se filtra con un filtro pasabanda IIR de segundo orden. El tomar tan sólo 128 elementos se debe a que el contenido en frecuencia de dos series caóticas con diferente condición inicial tienden a ser similares para una longitud larga. Por otra parte, el objeto de aplicar una ventana es el de concentrar la función wavelet madre en el tiempo y reducir el efecto Gibbs, y el propósito del filtrado es reducir el ancho de banda de la serie, puesto que de no hacerlo se introduce una alta redundancia en la información de todas las escalas que imposibilita el proceso de recuperación de la información. La frecuencia central y ancho de banda de dicho filtro se calculan a partir del valor del último elemento de la serie caótica original. Este preprocesamiento a la serie caótica original hace que la nueva serie, la wavelet madre a usar en el encriptador, no sea por completo caótica, de allí el nombre de wavelet madre pseudocaótica.

Con el método descrito anteriormente se genera la wavelet madre para la escala más alta (en nuestro caso *m=64*), y para las restantes escalas, se diezma por $s_m = a_0^{-m}$ y se añaden ceros para generar un nuevo vector de 1024 datos que corresponden a la wavelet de la escala m deseada. En la figura 2 se muestran las funciones wavelets base para tres diferentes escalas, así como sus respectivas transformadas de Fourier.

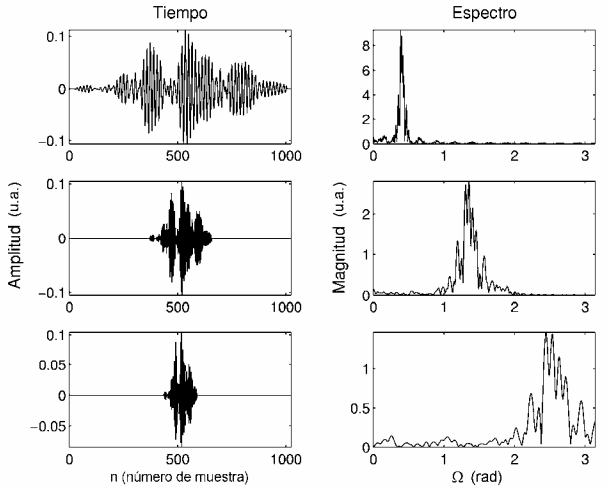

Figura 2. Wavelets pseudocaóticas para diferentes escalas

Debido al principio de incertidumbre, cada una de las funciones base presenta una dispersión en frecuencia y tiempo que reduce dramáticamente el número de bits que se pueden transmitir por cada bloque de datos, comparado con el límite máximo ideal de 1024bits por cada una de las escalas. Estas dispersiones se puede calcular con las expresiones dadas en la referencia [5]. Aunque el número de bits por trama se puede aumentar con la selección de wavelets madre concentradas en el tiempo y escala, su uso no es práctico en un sistema de encriptación, ya que se requiere alta redundancia y traslape entre escalas y tiempo, con el fin de asegurar una buena confiabilidad del sistema. Por esta razón, para generar la señal pseudocaótica, el filtro pasabanda se escoge con una baja selectividad y se seleccionan las escalas más bajas para transmitir la información, debido a que espectralmente las funciones base de estas escalas se encuentran más dispersas en frecuencia y más concentradas en el tiempo (ver figura 2). Se empleó también como criterio de selección de las escalas, la menor razón de bits erróneos (BER: por sus siglas en inglés de *Bit Error Rate*) ante diferentes relaciones señal/ruido en la señal encriptada.

Para ilustrar el efecto de la dispersión en las escalas y tiempos, se presenta en la figura 3 un ejemplo de una señal encriptada con el esquema propuesto y el respectivo mapa escala-tiempo que se detecta en el receptor.

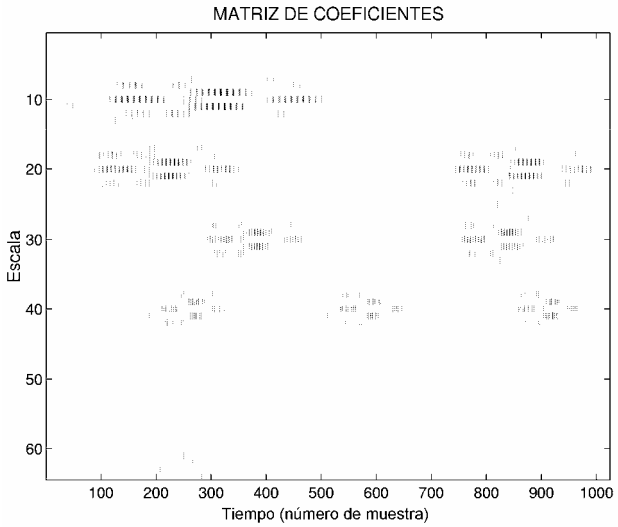

Figura 3. Efecto de la dispersión en frecuencia-tiempo de una cadena binaria encriptada con el sistema propuesto

3.2. Generación de la señal encriptada

Para generar la señal encriptada, se escriben los bits a transmitir en una matriz bidimensional de 1024 elementos por el número de escalas seleccionadas, la que posteriormente sirve de entrada al algoritmo de cálculo de la IOCWT. En esta matriz, inicializada con ceros, los bits se ubican en las posiciones identificadas previamente por medio de la dispersión en el tiempo de la función wavelet madre asociada a la respectiva escala. Por otra parte, para sincronizar la transmisión, por cada uno de los bloques de datos calculados, se transmite un único bit en una escala dada, denominada escala de señalización, que permite determinar en el receptor, el inicio del bloque de datos. Esto último es posible gracias a la propiedad de invarianza en el tiempo de la OCWT.

3.3. Decriptación de la señal

Tal como se ilustra en la figura 1, la recuperación de la información se consigue por medio de una OCWT. Para

el cálculo de la OCWT se incluyen algunas de las escalas que no fueron tenidas en cuenta en el proceso de generación de la señal caótica, esto con el fin de considerar la dispersión en frecuencia que sufren los coeficientes wavelet, lo cual favorece el proceso de detección de bits en el decodificador y aumenta la confiabilidad el sistema. La matriz recuperada se somete a un proceso de reducción de ruido por medio de la técnica de umbral fuerte[8]. Para poder interpretar la matriz de salida de la OCWT se hace necesario identificar el inicio y fin de la trama, lo cual se logra con la detección del bit de sincronización. Dado que el bit transmitido se identifica en el receptor por medio de una forma de onda dispersada en el tiempo, el proceso de búsqueda de dicho bit se realiza por medio del cálculo del centro de masa de los coeficientes wavelet de la escala de señalización para dos bloques consecutivos de 1024 elementos. Una vez se identifica el centro de masa, el inicio de la trama se encuentra localizado un medio de la longitud de dispersión en el tiempo de la función base de la escala de señalización, y se procede a recuperar los bits de información por medio del cálculo de la energía en la región de dispersión del bit. Si dicha energía es superior al umbral de detección el bit se considerará como uno, en caso contrario se considera cero.

3.4. Optimizaciones de cálculo

La OCWT del receptor involucra una mayor cantidad de cálculos que la IOCWT del transmisor, dado a que en la segunda, por la forma del patrón binario de entrada, es posible reducir el número de términos involucrados de la sumatoria de la ecuación (3) a las escalas relevantes; en cambio, para el receptor, en el cálculo de la OCWT se deben considerar un mayor número de escalas, con el fin de abarcar toda la región de dispersión del bit a detectar. Por esta razón, la tasa máxima de transmisión de bits del sistema en tiempo real, depende únicamente de lo optimizado del algoritmo de cálculo de la OCWT.

Para el cálculo de la OCWT y la IOCWT fueron tenidos en cuenta diferentes aspectos de optimización. Primero, la función wavelet base de cada escala es fija, lo cual permite precalcularla. Segundo, estas transformadas asumen datos de entrada completamente reales, lo cual permite emplear un algoritmo eficiente de la FFT [9] para magnitudes de entrada/salida completamente reales. Tercero, el DSP sobre el cual se implementó el sistema, un TMS320C6701, no posee instrucciones especializadas para bit-reversal, por lo cual fue necesario una rutina optimizada que se puede encontrar en referencia [9]. Cuarto, la FFT implica el llamado de las funciones sin y cos de la librería matemática math.h, las cuales consumen demasiados ciclos de reloj, por lo que se decidió generar una tabla precalculada para dichas funciones. Finalmente, y con el fin de aprovechar la capacidad de ejecución en paralelo de las instrucciones del DSP, se hizo necesario emplear una técnica llamada “desenredo de ciclos (*loop-unrolling* por sus siglas en inglés)” [10], por medio de la escritura redundante de líneas de código de lenguaje C. Esta técnica, le permite al optimizador del compilador reordenar las instrucciones según su grado de dependencia y generar así código de máquina que pueda ser ejecutado en paralelo por las diferentes unidades de cómputo del procesador.

4. DESEMPEÑO DEL SISTEMA PROPUESTO

Se realizaron diferentes pruebas de desempeño que consistieron en: la factibilidad de sincronización, la inmunidad al ruido aditivo, y la posibilidad de decriptación con funciones wavelets estándares y pseudocaóticas con diferentes condiciones iniciales y atractores; en todos los casos, se empleó como valor de comparación la razón de bits errados (BER). Los valores cuantitativos fueron obtenidos por medio de simulaciones del sistema en Matlab, resultados que fueron apreciados cualitativamente por medio de la implementación en tiempo real del sistema sobre el DSP utilizado.

Para la sincronización, se realizaron diferentes simulaciones que consistieron en desplazar la señal encriptada un número entero y no entero de muestras de la señal entregada por la IOCWT. Esto permitió mostrar la viabilidad de implementación del sistema, pues en un escenario práctico, el ADC del sistema transmisor y el DAC del receptor no se encuentran perfectamente sincronizados. Dichos resultados fueron verificados posteriormente con la ejecución del sistema sobre el DSP.

Respecto a la inmunidad al ruido se encontró que el sistema de encriptación permite una recuperación de la información para relaciones señal a ruido (SNR) superiores a 8dB, encontrándose a 0dB una BER del 14%. Por otra parte, para verificar la seguridad del sistema se propuso decriptar la señal con: una wavelet pseudocaótica generada con el sistema caótico de (5) y con diferentes condiciones iniciales, una wavelet pseudocaótica logística, una wavelet de Morlet [4] y una wavelet generada con el esquema presentado en este trabajo pero que hace uso de un vector aleatorio en lugar de una serie caótica. En la Tabla 1 se presentan las diferentes BER obtenidas a condiciones favorables del sistema (SNR=100dB) y con la presencia de ruido (SNR=10dB). En todos los casos, la wavelet madre empleada en el sistema transmisor es una serie caótica con condición inicial 0.5.

Wavelet madre	Condición inicial	BER (%)	
		SNR=10dB	SNR=100dB
Original	0.75	37	42
	0.55	44.4	48.2
	0.51	43.5	43.1
	0.49	34.6	20
	0.50	0	0
	0.45	51.8	51.3
	0.25	39.7	40.2
Logística	0.55	49.8	42.1
	0.51	50.5	49.6
	0.5	48.8	50.3
	0.49	48.6	49.7
	0.45	49.8	48.8
Morlet	-	48.1	47.4
Aleatoria	-	47.5	45.4

Tabla 1. BER para diferentes funciones wavelet madre en el transmisor

Nótese que el BER es superior al 35% para esquemas que emplean una diferente serie pseudocaótica (logística o aleatoria) o función wavelet madre (Morlet), inclusive, aún con la misma wavelet pseudocaótica, para valores de la condición inicial ligeramente alejados, no se logra decriptar correctamente la señal. Esto garantiza la adecuada confiabilidad del sistema para una aplicación de encriptación.

5. CONCLUSIONES

Se mostró que es posible usar una serie caótica, sometida a varios procesos de filtrado y aplicación de una ventana, como función wavelet madre, para la construcción de un sistema de encriptación de información. La seguridad del sistema fue probada ante diferentes funciones wavelet madre pseudocaóticas y la función wavelet de Morlet.

Para la implementación eficiente del sistema, se realizaron optimizaciones al cálculo de la transformada wavelet sobrecompleta OCWT y su inversa IOCWT por medio de la Transformada Rápida de Fourier para señales reales, y para su aplicación a bloques consecutivos de datos se emplearon las técnicas de: solapamiento y almacenamiento, para el cálculo de la OCWT y solapamiento y suma para el cómputo de la IOCWT.

6. AGRADECIMIENTOS

Este trabajo se pudo realizar gracias al apoyo financiero de la Universidad del Quindío a través del proyecto 222.

7. BIBLIOGRAFÍA

[1] PECORA, L.M. and CAROLL, T.L. Synchronization in chaotic systems, Phys. Rev. Letters, vol. 64, p. 821, 1990.

[2] CUOMO, K.M., OPPENHEIM A.V. and STROGATZ, S.H. Synchronization in chaotic systems, IEEE Trans Circuits and Systems, vol 40, pag. 626-633, 1993.

[3] GRASSI, G. and MASCOLO, S. A system theory approach for designing cryptosystems based on hyperchaos. IEEE Tran. on Circuits and Systems I: Fundamental Theory and Aplications, vol. 46, pag. 1135-1138, 1999.

[4] TEOLIS, A., Computational Signal Processing with Wavelets. Birkhauser, Boston, 1998.

[5] AKANSU, A. N. and MEDLEY, M. J. Wavelet, Subband and Block Transforms in Communications and Multimedia. Kluwer Academic Publishers, Boston , 1999.

[6] ALVAREZ, G. MONTOYA, F., ROMERA, M., y PASTOR, G. Criptoanálisis del sistema criptográfico basado en la sincronización de osciladores caóticos. Mundo Electrónico, vol. 307, pag. 56–58, 2000.

[7] PROAKIS, J. G. y MANOLAKIS, D. Tratamiento Digital de Señales. Pretince–Hall, 1992.

[8] RAO, R. M. y BOPARDIKAR, A. S. Wavelet Transforms. Addison Wesley, 1998.

[9] EMBEREE, P. M. C++ Algorithms for Digital Signal Processing. Pretince Hall, 1999.

[10] INSTRUMENTS, T. TMS320C6000 Optimizing C/C++ Compiler User's Guide. Jan. 2000.