JÓVENES EN LA CIENCIA
REVISTA DE DIVULGACIÓN CIENTÍFICA

Encriptación por medio de Polinomios Ortogonales

Yuliana Murillo Hurtado (1), Eduardo Cabal Yépez (2)

1 [Licenciatura en Ingeniería en Sistemas Computacionales, Universidad de Guanajuato] | Dirección de correo electrónico: [yuliana.mhu@gmail.com]

2 [Departamento de Estudios Multidisciplinarios, División de Ingenierías, Campus Irapuato-Salamanca, Universidad de Guanajuato] | Dirección de correo electrónico: [educabal@ugto.mx]

Resumen

El proceso de encriptación de información es de gran importancia en la actualidad, ya que garantiza que la información enviada sea ilegible sin que nadie más que el destinatario la pueda interpretar correctamente. Existen varias técnicas para la encriptación de señales. El método que se propone es la encriptación de señales por medio de polinomios ortogonales, específicamente polinomios de Legendre, se encripta y des-encripta una señal de entrada utilizando estos polinomios, se realiza un análisis de ortogonalidad y representación de polinomios para determinar los polinomios necesarios para lograr el proceso de encriptado y des-encriptado, posteriormente se desarrolló el algoritmo que realiza este proceso y finalmente se realizaron pruebas con diferentes señales y parámetros comparando la señal original con la obtenida después del proceso. Se obtienen buenos resultados y efectivamente es posible encriptar y des-encriptar una señal mediante la utilización de polinomios ortogonales de Legendre.

.

Palabras Clave Encriptación, Legendre; Ortogonalidad.

INTRODUCCIÓN

Marco teórico

La criptografía hoy en día es de gran importancia en áreas como ingeniería, medicina, administración entre otras. Garantizar que la información enviada sea ilegible sin que nadie más que el destinatario la pueda interpretar correctamente por medio de algún proceso de codificación se llama encriptación [1].

Actualmente existen diferentes técnicas para encriptación de información como la transformada wavelet, descomposición de valores singulares, series de Fourier y diseño de algoritmos algebraicos [2][3].

Polinomios de Legendre

Los polinomios de Legendre son unos de los ejemplos más importantes de los polinomios ortogonales, aparecen como soluciones en varios problemas de la física y matemáticas. Estos vienen construidos a partir de la fórmula de Rodrigues (Ec. 1) y es posible expresar cualquier función continua en el intervalo cerrado [−1, 1] (Gram–Schmidt orthogonalization) [4][5].

$$P_n(x) = \frac{1}{2^n n!}\left(\frac{d}{dx}\right)^n (x^2-1)^n, \quad \text{n=0,1,2,...} \qquad (1)$$

Donde n es el grado del polinomio, en la tabla 1 se muestran la ecuación de los seis primeros polinomios de Legendre.

Tabla 1: Polinomios de Legendre

Grado (n)	Pn(x)
0	1
1	X
2	$\frac{1}{2}(3x^2-1)$
3	$\frac{1}{2}(5x^2-3x)$
4	$\frac{1}{8}(35x^4-30x^2+3)$
5	$\frac{1}{8}(63x^5-70x^3+15x)$

Antecedentes bibliográficos

Actualmente los polinomios de Legendre son utilizados en diferentes aplicaciones de ingeniería, por citar algunos ejemplos están: un experimento de campo en China que consiste en un método inverso a la tomografía acústica costera (CAT) basado en polinomios de Legendre, en economía para la predicción del consumo de energía per cápita en China también, en análisis de señales para la reconstrucción y compresión de imágenes, la clasificación de formas de onda mediante la proyección de un sub-espacio de polinomios de Legendre, en matemáticas como solución a la ecuación de Langevin Boltzmann mediante polinomios de Legendre. Existen más aplicaciones documentadas y basadas en polinomios de Legendre sin embargo no para la encriptación de señales en el área de ingeniería [6] [7] [8] [9].

Justificación

Desarrollar, analizar y validar el encriptado de señales por medio de funciones ortogonales en nuestro caso los polinomios de Legendre.

De acuerdo a la propiedad de ortogonalidad una función $f(t)$ puede ser representa por de la ecuación 2.

$$f(t) = \sum_{n=-\infty}^{\infty} C_n \psi_n(t) \qquad (2)$$

$$C_n = \int_{-\infty}^{\infty} f(t)\psi_n{}^*(t)dt \qquad (3)$$

Donde C_n son los valores del coeficiente de peso y $\psi_n(t)$ es una función ortogonal, la cual cumple la propiedad descrita en la ecuación 4.

$$\int_{-\infty}^{\infty} \psi_n(t)\psi_m{}^*(t)dt = \delta_{\text{mn}} \qquad (4)$$

$$\delta_{mn} = \begin{cases} 1 & si\ m = n \\ 0 & si\ m \neq n \end{cases} \qquad (5)$$

Donde δ_{mn} es la delta de Kronecker.

De acuerdo a las ecuaciones descritas anterior es posible encriptar y des-encriptar cualquier señal *f(t)* por medio de polinomios ortogonales $\psi_n(t)$,

En el presente trabajo se realiza el estudio de las propiedades ortogonales en los polinomios de Legendre así como las limitaciones computacionales. Posteriormente se realiza la encriptación y des-encriptación de tres diferentes señales.

MATERIALES Y MÉTODOS

Se aplica el proceso de encriptado y des-encriptado para tres diferentes señales a) rectangular b) triangular c) sinusoidal. Los resultados son analizados y validados por medio de un estudio de la ortogonalidad de los polinomios de Legendre y sus limitaciones computaciones con el objetivo de definir un número aproximado de polinomios necesarios para poder aplicar la encriptación. Finalmente se muestran los resultados de encriptado y des-encriptado para cada señal de prueba todo esto implementado con ayuda del software Matlab.

RESULTADOS Y DISCUSIÓN

Los resultados del análisis de ortogonalidad arrojan que se necesitan aproximadamente *n*3* puntos (*n* = grado del polinomio) para expresar una señal de entrada con todos los polinomios, de este número hacia delante se ven más definidos cada vez, mientras más definidos estén los polinomios mejor será la encriptación y des encriptación de la señal. La Fig. 1 muestra la representación de un polinomio de grado 10 con 10 puntos a la izquierda y el mismo polinomio con 30 puntos (*n**3) a la derecha, es importante resaltar que con el software que se está utilizando y el algoritmo desarrollado permite representar 104 polinomios como máximo. El comportamiento es el mismo que en el análisis de ortogonalidad.

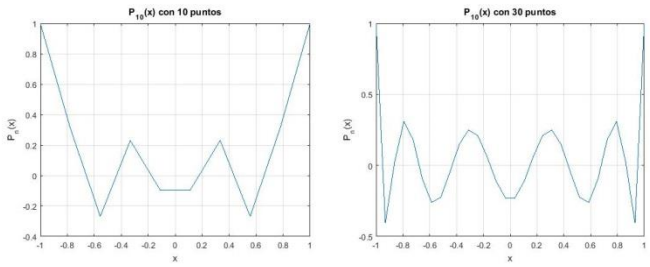

Fig. 1: Representación de un polinomio grado 10 con 10 puntos a la izquierda de la imagen y 30 puntos a la derecha

La Fig. 2 muestra la matriz de ortogonalidad con un factor de 3 con polinomios hasta grado 10, es decir una matriz cuadrada de 10 x 10 en la que cada polinomio se evalúa con 30 puntos (10*3). Los lados *m* y *n* representan los grados de los polinomios, como es de esperarse en polinomios de grado igual (m = n) muestra valores cada vez más próximos a 1, en caso contrario (m ≠ n) muestra datos próximos a 0.

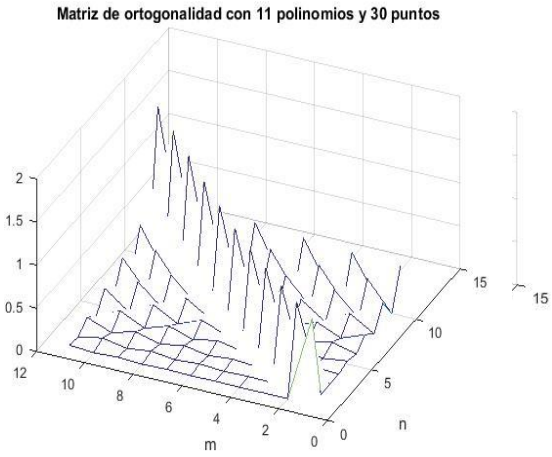

Fig. 2 Matriz de ortogonalidad con 10 x 10 polinomios con evaluación de 30 puntos para cada polinomio.

La Fig. 3 muestra la matriz de ortogonalidad con un factor 10 (100 puntos) y polinomios de grados 0 a 10, muestra los valores mucho más próximos a 1 y 0.

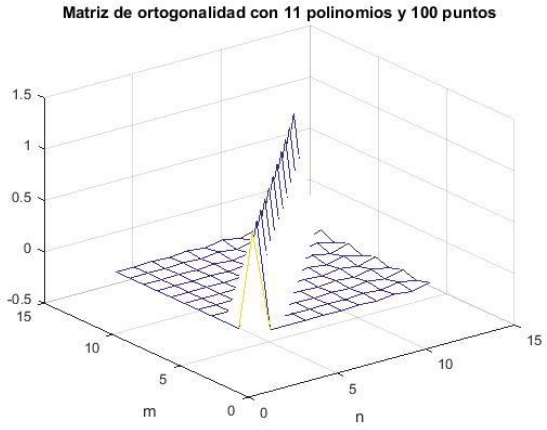

Fig. 3 Matriz de ortogonalidad con 10 x 10 polinomios con evaluación de 100 puntos para cada polinomio.

El método de encriptado y des encriptado es básicamente: Obtener el polinomio, evaluarlo con los puntos de la señal de entrada del cual resulta un nuevo vector, encriptar este nuevo vector y por último aplicar el proceso de des encriptación y comparar señal resultante con la señal original. La Fig. 4 muestra una función rectángulo con 100 puntos que se encripta con 100 polinomios (Fig. 5) y finalmente se des-encripta (Fig. 6). La función

resultante es una aproximación de la original, como se observa varía también la amplitud, esto se soluciona normalizando la función resultante.

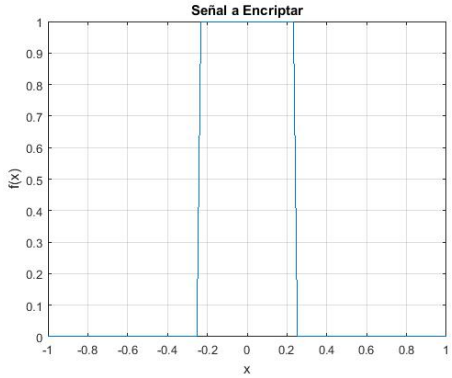

Fig. 4 Función rectángulo con 100 puntos y pulso de -0.25 a 0.25.

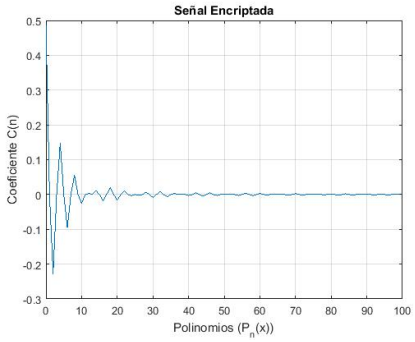

Fig. 5 Señal encriptada con un polinomio de grado 99.

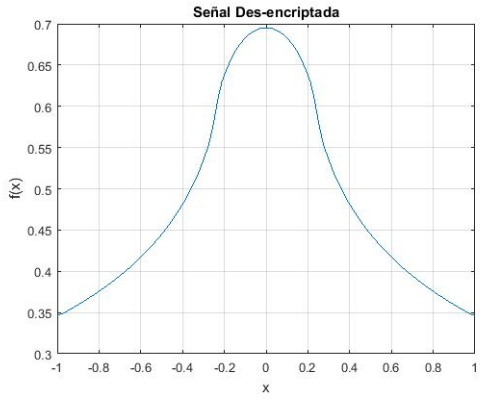

Fig. 6 Función rectángulo des-encriptada.

Se realiza otra prueba con una señal triangular, se utilizan 100 polinomios y 100 puntos, la Fig 7 muestra la señal original y la Fig. 8 muestra la señal después del proceso de encriptación y des-encriptación, al igual que la anterior varia la amplitud.

Fig. 7 Señal triangular con 100 puntos de -1 a 1.

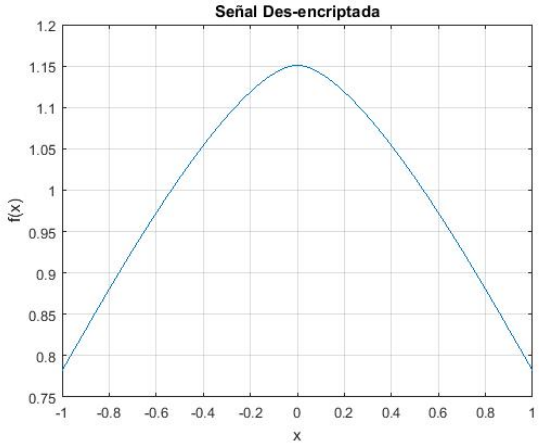

Fig. 8 Señal triangular des-encriptada.

En una prueba más se realiza el procedimiento con una función seno de –pi a pi, utilizando 100 polinomios y 100 puntos. La Fig 9 y Fig. 10 muestran el antes y después de la encriptación.

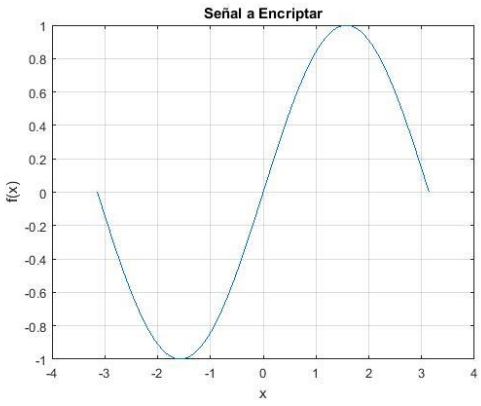

Fig. 9 Señal seno con 100 puntos de [-pi, pi].

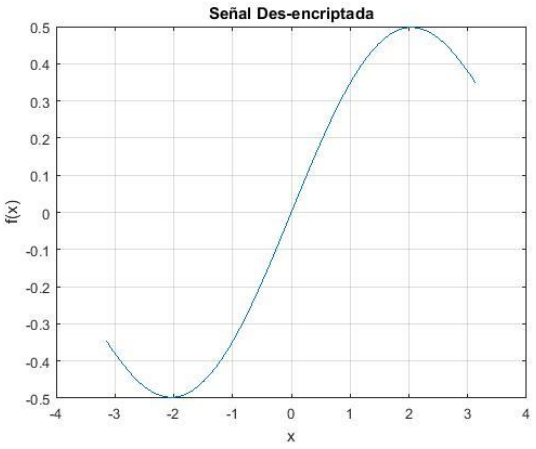

Fig. 10 Función seno des-encriptada.

CONCLUSIONES

Es posible encriptar señales mediante funciones ortogonales (polinomios de Legendre en este caso), el éxito del proceso depende en mayor grado del número de polinomios y puntos que se utilicen, de acuerdo al análisis de ortogonalidad se necesitan más puntos que polinomios pero en esta ocasión el algoritmo que se desarrolló utiliza la misma cantidad de puntos y polinomios lo cual puede ser una limitante así como las limitaciones propias del software que se utiliza, pudiera ser que modificando el algoritmo para tomar diferente número de puntos y polinomios y probando con otro software más potente, se pueda dar solución a estos detalles y con esto obtener una señal mucho más aproximada a la original.

AGRADECIMIENTOS

Agradezco no solo a mi asesor frente al proyecto Dr. Eduardo Cabal Yépez, sino también a mi asesor M. I. Luis M. Ledesma Carrillo que me estuvo asesorando en todo momento y claro a la Universidad por realizar este tipo de eventos que siempre dejarán algo bueno tanto en los alumnos como un granito de arena en los proyectos de investigación.

REFERENCIAS

[1] Patterson, Wayne (1987). Mathematical Cryptology for Computer Scientists and Mathematicians, Rowman & Littlefield

[2] Awasthi, D.; Madhe, S., "Analysis of encrypted ECG signal in steganography using wavelet transforms," Electronics and Communication Systems (ICECS), 2015 2nd International Conference on , vol., no., pp.718,723, 26-27 Feb. 2015

[3] Bianchi, T.; Piva, A.; Barni, M., "Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals," Information Forensics and Security, IEEE Transactions on, vol.5, no.1, pp.180,187, March 2010

[4] George B. Arfken, Hans J. Weber. (2005). Alternate Definitions of Legendre Polynomials. Mathematical Methods for Physicists, (pp. 767 - 768). London, UK: Elsevier Academic Press.x.

[5] George B. Arfken, Hans J. Weber. (2005). Gram – Schmidt Orthogonalization. Mathematical Methods for Physicists, (pp. 642 - 647). London, UK: Elsevier Academic Press.x.

[6] Guanghong Liao, Jun Wang, Xiaohua Xu, Chenghao Yang, Qingsong Wu, Chuanzheng Zhang, Xiaohua Zhu. (2011). A coastal acoustic tomography inverse method based on Legendre polynomials and its application in Sanmen Bay field experiment, China. IEEE Conference Publications, vol.5, no., pp. 2554 - 2558, doi: 10.1109/CISP.2011.6100716.

[7] Zhang, Hong-qin, Gao, Lai-bin. (2011). Application of legendre polynomial in predicting of energy consumption per capital. IEEE Conference Publications, vol., no., pp. 1 - 3, ISSN: 2154-4824.

[8] Jungemann, C.; Meinerzhagen, B. (2004). A Legendre polynomial solver for the Langevin Boltzmann equation. IEEE Conference Publications, vol.5, no., pp. 22 - 23, doi: 10.1109/IWCE.2004.1407299.

[9] Guoqi Li, Changyun Wen. (2010). Legendre polynomials in signal reconstruction and compression. . IEEE Conference Publications, vol.5, no., pp. 1636 - 1640, doi: 10.1109/ICIEA.2010.5514776.