JÓVENES EN LA CIENCIA
REVISTA DE DIVULGACIÓN CIENTÍFICA

Encriptación de Señales por medio de Polinomios Ortogonales

Roberto Morales Feria (1), Dr. Eduardo Cabal Yepez (2)

1 [Ingeniería en Sistemas Computacionales, Instituto Tecnológico Superior de los Ríos] | [robert_lalito@hotmail.com]

2 [División de Ingenierías, Campus Irapuato-Salamanca, Institución Universidad de Guanajuato] | [educabal@ugto.mx]

Resumen

La encriptación hoy en día es una herramienta muy útil cuando se desea proteger datos en cualquier sistema de información. Debido a los constantes cambios de la tecnología y al aumento de ataques realizados, se hace imprescindible crear nuevas técnicas de encriptación para garantizar la seguridad en la información transmitida o recibida. Es por esta razón que se propone la creación de una nueva técnica de encriptación basada en la propiedad que poseen los polinomios ortogonales como fundamento base de nuestro proyecto. Se simuló mediante el software Matlab el comportamiento de los polinomios de Hermite mostrando las limitaciones computacionales. Adicionalmente se obtuvo el análisis entre el grado del polinomio *n* y la cantidad de puntos que soporta sin perder su propiedad. Se generó la encriptación de una señal sintética rectangular mostrando su forma encriptada.

Abstract

Nowadays encryption is a very useful tool for protecting data on any information system. Due to constant changes in technology and the increase on information attacks, it is essential to develop new encryption techniques for protecting the transmitted or received information. Therefore, a new encryption technique is proposed, which is based on the property of orthogonal polynomial for developing this project. Experimentation through simulation in Matlab was performed to assess the suitability and computational limitations of Hermite polynomials for this task. Besides, an analysis regarding the connection between polynomial degree *n* and the number of point used for representing the polynomial was carried out. Finally, a synthetic rectangular signal was obtained and encrypted to demonstrate the use of the proposed approach.

Palabras Clave Matlab, Clave, Análisis, Formulas, Ortogonalidad, Encriptación.

INTRODUCCIÓN

Actualmente el avance de las tecnologías principalmente en el área de comunicaciones es de suma importancia proteger la información que se transmite, la cual puede ser interceptada fácilmente, se hace imprescindible la idea de agregar seguridad extra a los datos, por lo que la encriptación cobra un papel importante en este tema.

La criptografía es una técnica de seguridad que consiste en proteger la información por medio de técnicas para que resulte incomprensible para todo aquel que no esté autorizado en acceder a ella, únicamente permitiendo el acceso por medio de una llave ò código de des encriptación.

En los últimos años, los esquemas de encriptación están siendo estudiados cada vez más, ante la demanda que existe de desarrollar un sistema de encriptación más seguro, para la transmisión de datos [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].

ANTECEDENTES

Las organizaciones, a lo largo de la historia, han hecho del secreto de sus comunicaciones un principio fundamental de su actividad. Dicho secreto se intentó proteger mediante la encriptación, es decir, la codificación del lenguaje mediante una clave secreta sólo conocida por la organización emisora del mensaje y el destinatario del mensaje determinado por dicha organización. El anecdotario histórico abunda con ejemplos de batallas e, incluso, guerras supuestamente pérdidas o ganadas mediante la interceptación y desencriptación de mensajes decisivos entre los centros de poder. El origen de la informática contemporánea durante la Segunda Guerra Mundial parece estar relacionado con los esfuerzos de matemáticos extraordinarios, como el inglés Turing, para desarrollar algoritmos capaces de descifrar los códigos del enemigo [4].

En el campo de la encriptación son bastante conocidos los algoritmos de cifrado digital, sin embargo, la encriptación analógica de señales ha sido un tema muy complejo, para ciertos autores [5][6], plantean como alternativas de solución el uso de moduladores/demoduladores caóticos, sin embargo, la sincronización entre el transmisor y el receptor es muy compleja y en algunos casos impráctica [7], además, la calidad de la señal recuperada no es lo suficientemente aceptable.

El origen de algunos de los polinomios ortogonales clásicos que tuvieron una importancia no solo en el desarrollo de este tema sino también en las aplicaciones a otras ciencias. [8] [9].

Se clasifican en tres grandes familias: Jacobi, Laguerre y Hermite. En función de las características del intervalo de definición [a; b], según se trate de un intervalo acotado [a; b], semi-infinito [a; ∞) o infinito (R).

Haciendo uso, si fuese necesario, de transformaciones lineales elementales, basta estudiar los intervalos [-1; 1]; [0, ∞) y R = (−∞, ∞), quedando así cubiertos todos los casos posibles [9].

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

MATERIALES Y MÉTODOS

Objetivo

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

Sistema de Encriptación Propuesto

El esquema de encriptación propuesto en este trabajo se ilustra en la figura 1. En ésta la señal a encriptar se introduce al sistema, utilizando los polinomios de Hermite como llave, la señal es encriptada, esta viaja por el canal de transmisión y al llegar al receptor se aplica el proceso de decodificación utilizando los polinomios de Hermite nuevamente para reconstruir la señal encriptada y dar fin al proceso.

Figura 1: Sistema de encriptación propuesto.

Polinomios de Hermite

Los polinomios de Hermite Hn(x) son un conjunto de polinomios ortogonales sobre el dominio (−∞, ∞) con función de ponderación e^(−x^2) , para n = 1, 2, 3, y 4.,[10]

Los polinomios de Hermite se definen con la fórmula de Rodrigues generalizada como:

$$Hn(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2} \qquad (1)$$

En la tabla 1, se muestran los primeros 10 polinomios de Hermite aplicando la ecuación 1, la figura 2 y figura 3 muestra la simulación numérica de los primeros 10 polinomios respectivamente.

Tabla 1: Primeros 10 polinomios de Hermite

n	$Hn(x)$
0	$H_0(x) = 1$
1	$H_1(x) = 2x$
2	$H_2(x) = 4x^2 - 2$
3	$H_3(x) = 8x^3 - 12x$
4	$H_4(x) = 16x^4 - 48x^2 + 12$
5	$H_5(x) = 32x^5 - 160x^3 + 120x$
6	$H_6(x) = 64x^6 - 480x^4 + 720x^2 + 120$
7	$H_7(x) = 128x^7 - 1344x^5 + 3360x^3 - 1680x$
8	$H_8(x) = 256x^8 - 3584x^6 + 13440x^4 - 13440x^2 + 1680$
9	$H_9(x) = 512x^9 - 9216x^7 + 48384x^5 - 80640x^3 + 30240x$

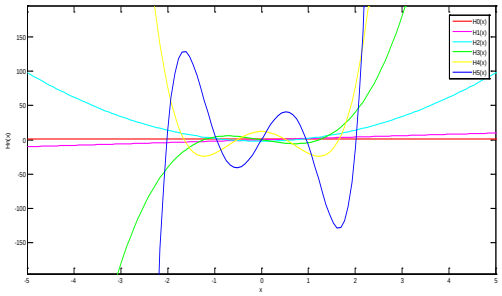

Figura 2: Simulación numérica de los primeros 5 polinomios de Hermite

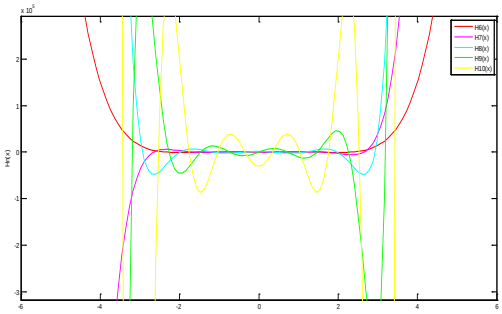

Figura 3: Simulación numérica de los polinomios de Hermite grado 6 al 10

Ortogonalidad de los polinomios de Hermite

$$\int_{-\infty}^{\infty} Hm(x)Hn(x)\ e^{-x^2}\ dx = 2^x n!\sqrt{\pi}\ \delta nm \qquad (2)$$

Donde δnm denota la delta de Kronecker, igual a 1 si m = n y 0 para otros casos.

Podemos expresar este resultado diciendo que los polinomios de Hermite son ortogonales, pero con una función de peso p(x) = e^{-x^2} [11][12].

Proceso de Encriptación

De acuerdo a la propiedad de Ortogonalidad una función $f(t)$ puede ser representa por la ecuación 3.

$$f(t) = \sum_{n=-\infty}^{\infty} C_n \psi_n(t) \qquad (3)$$

$$C_n = \int_{-\infty}^{\infty} f(t)\psi_n{}^*(t)dt \qquad (4)$$

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 5.

$$\int_{-\infty}^{\infty} \psi_n(t)\psi_m{}^*(t)dt = \delta_{\mathrm{mn}} \qquad (5)$$

$$\delta_{mn} = \begin{cases} 1 & si\ m = n \\ 0 & si\ m \neq n \end{cases} \qquad (6)$$

Donde δ_{mn} es la delta de Kronecker.

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

RESULTADOS Y DISCUSIÓN

Análisis de Ortogonalidad con Software Matlab.

La tabla 2 y tabla 3 muestran el análisis de Ortogonalidad para la simulación numérica de los polinomios de Hermite, variando el rango y número de puntos.

Tabla 2: Análisis de Ortogonalidad

Hn(x)	Rango de (x)	No. De Puntos
1	[-4,4]	16 →
2	[-4,4]	16 →
3	[-4,4]	16 →
4	[-4,4]	16 →
5	[-6,6]	32 →
6	[-6,6]	32 →
7	[-6,6]	32 →
8	[-6,6]	32 →
9	[-6,6]	32 →
10	[-6,6]	32 →

Tabla 3: Análisis de Ortogonalidad

Hn(x)	Rango de (x)	No. De Puntos
11	[-10,10]	128 →
12	[-10,10]	128 →
13	[-10,10]	128 →
14	[-10,10]	128 →
15	[-10,10]	128 →
16	[-10,10]	128 →
17	[-10,10]	128 →
18	[-10,10]	128 →
19	[-18,18]	1024 →
20	[-18,18]	1024 →
21	[-18,18]	1024 →
22	[-18,18]	1024 →

Un inconveniente fue la complejidad que presentan los polinomios de Hermite al estar en el intervalo de [-∞, ∞] esto ocasiona que al representar numéricamente la señal, se tenga que variar el rango de x y los puntos entre ese rango como se muestra en la figura 4 y 5 ya que a mayor número de puntos la señal se define mucho mejor.

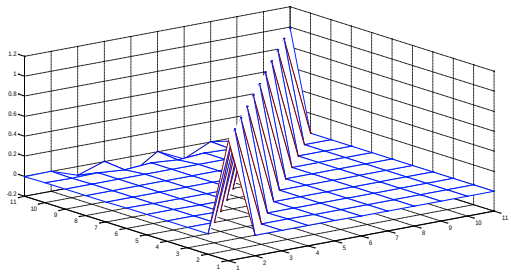

Figura 4: Representación de Ortogonalidad variando el rango de x [-5,5]

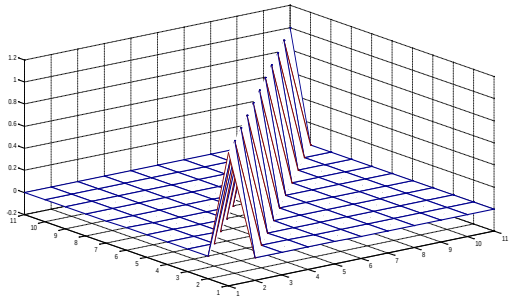

Figura 5: Representación de Ortogonalidad variando el rango de x [-10,10]

La implementación básica consistió en que con la ayuda de la herramienta Matlab se generó una señal cuadrática como muestra la figura 6, la cual se sometió al proceso de encriptación utilizando como llave los polinomios de Hermite generando la señal encriptada de la figura 7, luego de este proceso se realizó la des encriptación de la señal aplicando de nuevo el polinomio como llave para obtener así la señal des encriptada , en este proceso se logró obtener una señal aproximada, con algunas limitaciones debido a que la herramienta Matlab no puede realizar cálculos de polinomios de mayor complejidad.

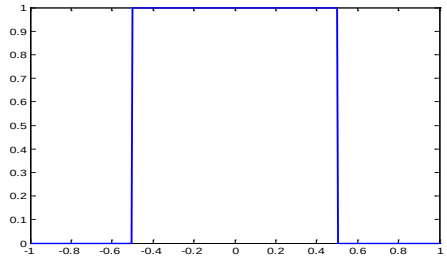

Figura 6: Señal Cuadra $f(t)$

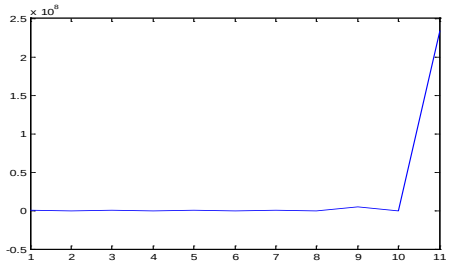

Figura 7: Simulación de la señal Encriptada

CONCLUSIONES

Se ha realizado un sistema experimental de transmisión segura para una señal basado en la encriptación por medio de polinomios ortogonales en este caso los polinomios de Hermite, logrando que se transmita a un receptor que también utiliza el mismo polinomio, como llave permitiéndole reconstruir la señal encriptada. Debido a las limitaciones de tiempo y hardware no se obtuvo una imagen de la señal des encriptada pero si se obtuvieron resultados alentadores que dan pauta para trabajos futuros.

AGRADECIMIENTOS

Se agradece al Dr. Eduardo Cabal Yepez por su apoyo y consejos para poder realizar el verano de investigación, también al CONACYT por hacer posible la realización de este verano de investigación, al Instituto Tecnológico Superior de los Ríos por brindarnos todas las facilidades para

asistir a este verano y en general a todas las personas que me dedicaron su tiempo y paciencia.

REFERENCIAS

[1] Li S., Alvarez G.,Li Z., Halang W. A. (2007). “Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey”.

[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] Levy, S. (2001). Crypto. How the code rebels beat the government - saving privacy in the digital age. New York: Viking.

[5] Pecora, L. M. and Carroll, T. L. Synchronization in chaotic systems. (1990) *Phys. Rev. Lett.* 64, 821824.

[6] Strogatz, Steven H (2001). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry and Engineering*. Perseus Book Group.

[7] Álvarez, G. et al. Criptoanálisis de sistema Criptográfico. Basado en la sincronización de osciladores caóticos (2000). Mundo Electrónico Marzo 2000, 307.

[8] H. Michael Moller. Introduction to Orthogonal Polynomials, Lecture held at University of Dortmund in summer 2002/03, University of Dortmund, Dortmund,2003.

[9] G. Szeg}o. Orthogonal Polynomials, volume 23 of Amer. Math. Soc. Colloq. Publ.,fourth edition, Amer. Math. Soc., Providence, RI, 1975.

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

[11] George B. Arfken y Hans J. Weber. (2005). "Mathematical Methods for Physicists". Sixth Editio. Elsevier Academic Press.Neva York; pp 821.

[12] Harary, F. Teoría de Grafos. Reading, MA: Addison-Wesley, p. 35, 1994.