JÓVENES EN LA CIENCIA
REVISTA DE DIVULGACIÓN CIENTÍFICA

ENCRIPTACIÓN POR MEDIO DE POLINOMIOS ORTOGONALES

Zavala-Díaz, Jonathan (1), Cabal-Yépez, Eduardo (2)

1 [Licenciatura en Ingeniería en Comunicaciones y Electrónica, Universidad de Guanajuato] | [jonscasac@gmail.com]

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

Resumen

La encriptación es una herramienta muy útil cuando se desea proteger información. En la actualidad es muy importante la encriptación de información, así se asegura que la información sea enviada de forma protegida y solamente el destinatario final pueda tener acceso a ella. Debido a que la tecnología está en constante cambio es necesario encontrar nuevas técnicas para proveer a la información de seguridad, confidencialidad, integridad y autenticación. En este trabajo, se propone una técnica de encriptación basada en la propiedad de ortogonalidad, en específico usamos las matrices de Hadamard que son un caso de funciones ortogonales. Se desarrollo un algoritmo para la encriptación y des-encriptación, posteriormente se validó computacionalmente, mediante el software de Matlab con diferentes señales, el funcionamiento de nuestro algoritmo mostrando la señal encriptada y posteriormente desencriptarla para compararla con la señal original. Los resultados obtenidos demostraron que es posible encriptar y desencriptar una señal utilizando el algoritmo propuesto mediante matrices de Hadamard.

Abstract

Encryption is a very useful tool when you want to protect information. Today, information encryption is quite important; thus, ensuring that information is safely sent and only the final intended recipient will be able to access it. Since technology is constantly changing, it is necessary to find new techniques to provide information with security, confidentiality, integrity and authentication. In this work, an encryption technique is proposed based on the orthogonality property, specifically Hadamard matrices are used, which are a case of orthogonal functions. An algorithm for encryption and de-encryption is developed; then, computationally validated through Matlab utilizing different signals, showing the proposed-algorithm operation for encrypting and decrypting a signal, comparing the obtained result with the original signal. From the obtained results, it was demonstrated that it is possible to encrypt and decrypt a signal using the introduced algorithm utilizing Hadamard matrices.

Palabras Clave Encriptación; ortogonalidad; matrices de Hadamard

INTRODUCCIÓN

Marco teórico

La criptografía es la ciencia de la escritura secreta con el objetivo de ocultar el significado de un mensaje. [1]

En otras palabras, la criptografía es el estudio y aplicación de técnicas para una comunicación segura en presencia de terceros. Hoy en día, el cifrado es una herramienta importante para muchas áreas de ingeniería, medicina, comunicaciones, procesamiento de imágenes y video, entre otros. [2]

Actualmente existen diferentes técnicas para encriptación de información como la transformada wavelet, descomposición de valores singulares, series de Fourier y diseño de algoritmos algebraicos [3] [4].

Los polinomios ortogonales son una clase de polinomios que forman una base ortogonal. Una base de un espacio vectorial es ortogonal cuando los vectores que la forman son perpendiculares entre si.

Matrices de Hadamard

Las matrices de Hadamard son un caso de funciones ortogonales. Una matriz de Hadamard es una matriz cuadrada de +1 y -1 cuyas filas y columnas son mutuamente ortogonales. [5] Si H es una Matriz de Hadamard de N x N; Entonces, el producto de H y su transpuesta H^T es la matriz de identidad I multiplicada por el escalar N.

Así,

$$HH^T = NI \quad (1)$$

Otra propiedad muy importante de las matrices de Hadamard es que sus filas y columnas se pueden intercambiar con otra sin afectar la propiedad de ortogonalidad de la matriz.

La matriz Hadamard de orden más bajo es dos.

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2)$$

Se puede obtener una matriz de Hadamard de orden $N = 2^k$ (3) desde H_2, donde k es un entero [6].

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} \quad (3)$$

En la imagen 1 se obtiene diferentes matrices de Hadamard de orden N.

Matriz Secuencia

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \begin{matrix} 0 \\ 1 \end{matrix}$$

Matriz Secuencia

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad \begin{matrix} 0 \\ 3 \\ 1 \\ 2 \end{matrix}$$

Matriz Secuencia

$$H_8 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \quad \begin{matrix} 0 \\ 7 \\ 3 \\ 4 \\ 1 \\ 6 \\ 2 \\ 5 \end{matrix}$$

IMAGEN 1: Diferentes matrices de Hadamard orden N, para $N=2^k$

La interpretación de la matriz de Hadamard se puede dar en términos del número de cambios de signo para cada fila o columna. Un cambio se llama "Secuencia" de matriz de Hadamard. [7] La imagen 1 muestra la interpretación de secuencias para varias matrices de Hadamard. Por lo tanto, un conjunto de matrices de Hadamard proporcionan un número muy grande de secuencias para satisfacer los requisitos de seguridad para el cifrado de señales.

Antecedentes

Hasta la década de 1970, la criptografía se encontraba casi exclusivamente en aplicaciones diplomáticas, militares y gubernamentales. Durante la década de 1980, las industrias financieras y de telecomunicaciones implementaron dispositivos criptográficos de hardware.

La primera aplicación criptográfica de mercado masivo fue el sistema de telefonía móvil digital de finales de los años ochenta.

Hoy en día, todos usan la criptografía a diario: por ejemplo, desbloquear un coche o una puerta de

garaje con un dispositivo de control remoto, conectarse a una LAN inalámbrica, comprar productos con una tarjeta de crédito o de débito en una tienda o en internet, instalar una actualización de software, hacer una llamada telefónica a través de voz sobre IP, etc. [1]

Justificación

El esquema propuesto para el cifrado de señales se basa en Matrices Hadamard de N-orden, aprovechando sus propiedades ortogonales y sus secuencias de generación.

Por lo tanto, el proceso de encriptado se define como

$$g[x] = f[x] \cdot H_N \quad (4)$$

Donde f[X] es nuestra señal original, g[x] es nuestra señal encriptada, H_N es nuestra matriz de Hadamard de orden N.

La señal descifrada puede obtenerse de manera similar aplicando el mismo principio matemático debido a la propiedad inversa de la matriz de Hadamard.

La señal desencriptada f'[x] se define como

$$f'[x] = \frac{1}{N} g[x] \cdot H_N{}^T \quad (5)$$

Donde g[x] es nuestra señal encriptada y $H_N{}^T$ es nuestra matriz de Hadamard transpuesta de orden N.

En la imagen 2 de muestra un esquema básico para encriptar y desencriptar una señal

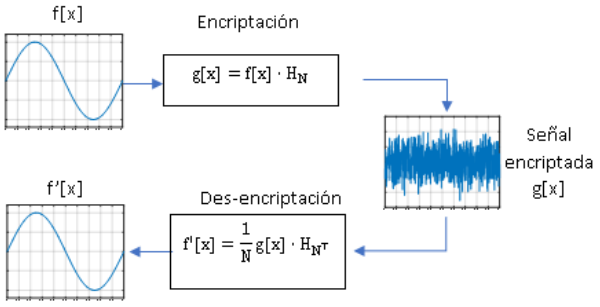

IMAGEN 2: Esquema básico para encriptar y desencriptar una señal

En el presente trabajo se realiza el estudio de las propiedades ortogonales en las matrices de Hadamard. Posteriormente se realiza la encriptación y des-encriptación de diferentes señales.

MATERIALES Y MÉTODOS

Primer grado de seguridad

Dividir nuestra señal segmentos de tamaño L variables, así conseguimos un total de num! combinaciones posibles, donde num es el número de segmento en el cual dividimos la señal. En la imagen 3 se muestra como seria la segmentación de la señal.

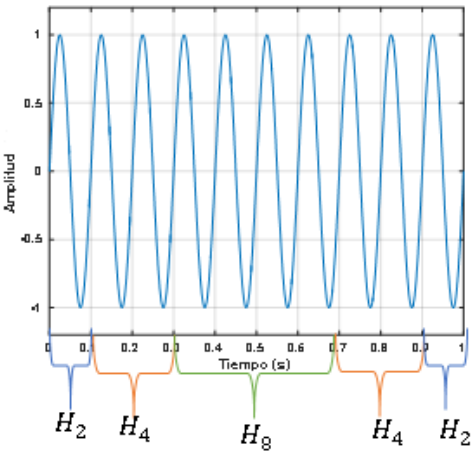

IMAGEN 3: Segmentación de la señal

Segundo grado de seguridad

Generación de una llave para cada segmento de la señal, para esto hacemos uso de la propiedad de Hadamard, intercambiando filas y columnas ya que esto no afecta su propiedad de ortogonalidad. Tenemos un total de 2*N! combinaciones, donde N es el tamaño de la matriz de Hadamard.

En la imagen 4 se muestra una secuencia diferente obtenida para una matriz de Hadamard de orden 4.

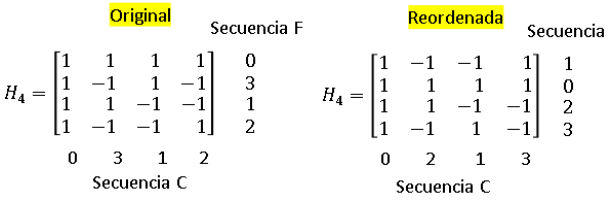

IMAGEN 4: Cambio de secuencias para una matriz de Hadamard de orden 4

Tercer grado de seguridad

Se realiza el mismo procedimiento que en el segundo grado de seguridad, pero ahora para la señal completa sin segmentar. Con un total de 2*N! combinaciones, donde N es el tamaño de la matriz de Hadamard.

RESULTADOS Y DISCUSIÓN

Se realizo la prueba del algoritmo de encriptación y des-encriptación con diferentes señales a continuación de muestra las señales y los resultados obtenidos.

En la imagen 5 se muestra una señal senoidal de 1024 muestras, en la imagen 6 se muestra la señal encriptada y en la imagen 7 la señal desencriptada la cual nos da idéntica a la señal original.

Ahora probamos nuestro algoritmo con una señal cuadrada, en la imagen 8 se muestra una señal cuadrada de 1024 muestras, en la imagen 9 se muestra la señal encriptada y en la imagen 10 la señal desencriptada la cual nos da idéntica a la señal original.

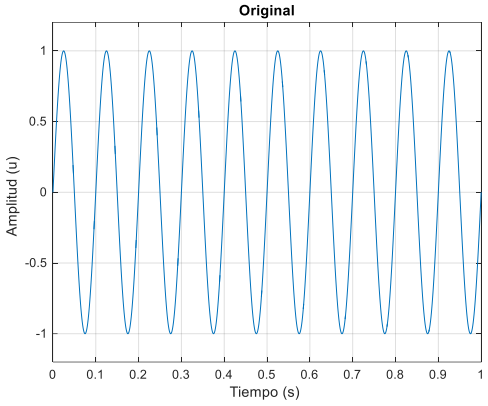

IMAGEN 5: Señal senoidal original de 1024 muestras

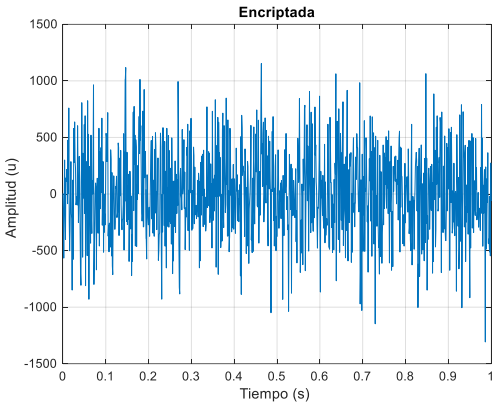

IMAGEN 6: Señal senoidal encriptada de 1024 muestras

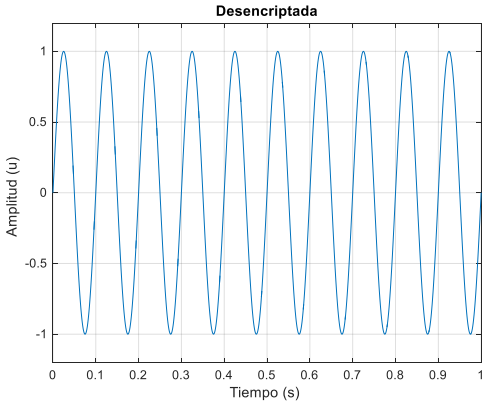

IMAGEN 7: Señal senoidal desencriptada de 1024 muestras

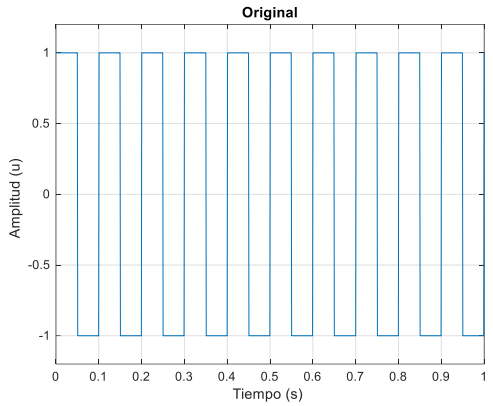

IMAGEN 8: Señal cuadrada original de 1024 muestras

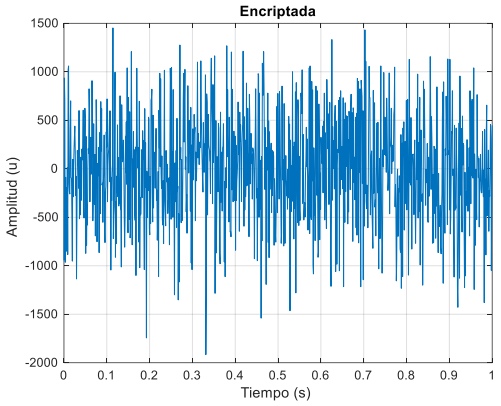

IMAGEN 9: Señal cuadrada encriptada de 1024 muestras

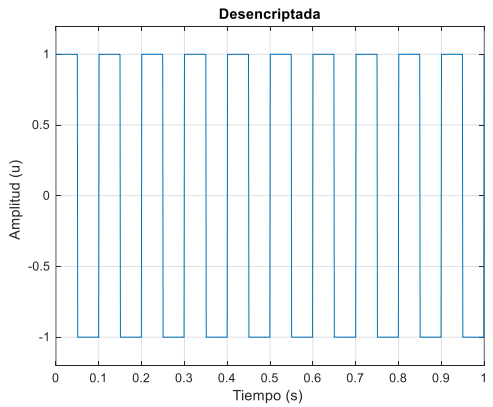

IMAGEN 10: Señal cuadrada desencriptada de 1024 muestras

CONCLUSIONES

Pudimos generar un código de encriptación con su respectiva llave de des-encriptación en el cual su grado de seguridad aumenta exponencialmente al aumentar el número de muestras, para trabajo a futuro se propone implementarlo en algún dispositivo como una FPGA.

AGRADECIMIENTOS

Primeramente, agradecer a mi asesor del proyecto el Dr. Eduardo Cabal Yépez, también para la realización de este proyecto fue imprescindible toda la ayuda que me brindo mi co-asesor le agradezco al M.I. Luis M. Ledesma Carrillo.

También a todas las personas que me aconsejaron en la realización de este trabajo les doy las gracias. Agradezco a la Universidad de Guanajuato, y a mi departamento por las facilidades brindadas, orgullosamente soy UG.

REFERENCIAS

[1] Paar,C. & Pelzl, J., (2010). Understanding Cryptography. New York, NY: Springer.

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

[3] Awasthi, D. & Madhe, S. (2015). Analysis of encrypted ECG signal in steganography using wavelet transforms. Electronics and Communication Systems (ICECS), 2015 2nd International Conference on , 718(723), 26-27.

[4] Bianchi, T., Piva, A. & Barni, M. (2010). Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. Information Forensics and Security, IEEE Transactions on, 5(1), 180-187.

[5] Hadamard, J. (1893). Resolution d'une question relative aux determionants. Bull. des Sciences Math, 17(1), 240-246.

[6] Pratt, W. (1969). An Algorithm for a Fast Hadamard Matrix Transform of Order Twelve. Computers, IEEE Transactions on , C-18(12), 1131-1132.

[7] Ledesma-Carrillo, L.M., Lopez-Ramirez M., Cabal-Yepez, E., Ojeda-Castañeda, J., Rodriguez-Doñate, C. & Lizarraga-Morales R. (2016). FPGA-Based Reconfigurable Unit for Image Encryption Using Orthogonal Functions. Electronics, Communications and Computers (CONIELECOMP), International Conference on, 168-173.