Implementación de un sistema de cifrado y compresión

Asesor: Dr. José Salomé Murguía Ibarra, ondeleto@uaslp.mx

Co-Asesor: Dra. Marcela Mejía mmc1907@gmail.com

Motivación

En la actualidad un gran número de aplicaciones relacionadas con el manejo y procesamiento de señales multimedia ha crecido de manera considerable. Una característica en dichas aplicaciones es el gran uso de recursos de memoria y cómputo para su funcionamiento. De ahí que se tenga la necesidad de utilizar algún esquema de compresión, que nos permita tener flexibilidad para almacenar y transmitir información. En este ámbito, la transformada wavelet ha resultado ser una herramienta muy potente para procesar de manera eficiente, señales que involucran grandes cantidades de información [1, 2, 3]. Aunado a lo anterior, hoy en día ha aumentado la necesidad de proteger información ya sea almacenada o transmitida para que nadie ajeno pueda hacer uso de ella. Por lo que resulta vital no solo tener un sistema de compresión, sino que, será necesario aplicar algún tipo de clave secreta a la información comprimida para que esto no suceda. Esto se puede hacer mediante el uso de un sistema de cifrado. Actualmente existe un gran número de sistemas de cifrado, donde su principal objetivo es el de proteger información por medio de un algoritmo que hace uso de una o más llaves. Muchos de estos sistemas sacrifican el tiempo de procesamiento para tener un cifrador más confiable o viceversa, el cifrador es menos confiable pero se logra un menor tiempo en el proceso de cifrado y descifrado, y en algunos casos la información se cifra de manera parcial. En la implementación de muchos sistemas de cifrado se han utilizado diferentes esquemas con un enfoque caótico con la finalidad de dar mayor robustez y seguridad a la información que se va a cifrar. Por ejemplo, en algunos trabajos se ha empleado el fenómeno de sincronización de autómatas celulares para implementar un sistema de cifrado [4, 5], mientras que en otros se presenta un esquema de cifrado basado en sistemas dinámicos caóticos, donde se utiliza un mapeo caótico unidimensional para remover correlación, mientras que un sistema hipercaótico realiza el cifrado caótico [6, 7].

Debido a que no se cuenta con diferentes sistemas que contemplen ambas etapas de manera flexible, en este proyecto se propone implementar de manera conjunta las etapas de compresión y cifrado, donde la etapa de compresión se basa en la transformada wavelet, mientras que la de cifrado se hace uso de sistemas dinámicos caóticos.

Objetivo

Implementar un sistema que combina los procesos de compresión y cifrado de diferente tipo de señales. Tal implementación nos permitirá manejar de manera más segura y apropiada grandes

cantidades de información, aunado al fortalecimiento de algunos temas de aplicación en el área de procesamiento de señales.

Metodología

En un principio se espera realizar una buena revisión del arte que contemple las tareas de compresión y cifrado. Después, se considera implementar algunos sistemas dinámicos caóticos, así como procesar y comprimir información con la transformada wavelet. Posteriormente, se pretende realizar la implementación de un sistema de cifrado basado en sistemas dinámicos caóticos. Por último, y después de establecer las condiciones anteriores, se pretende realizar la respectiva conjunción de las etapas anteriores y evaluarlo para diferentes señales.

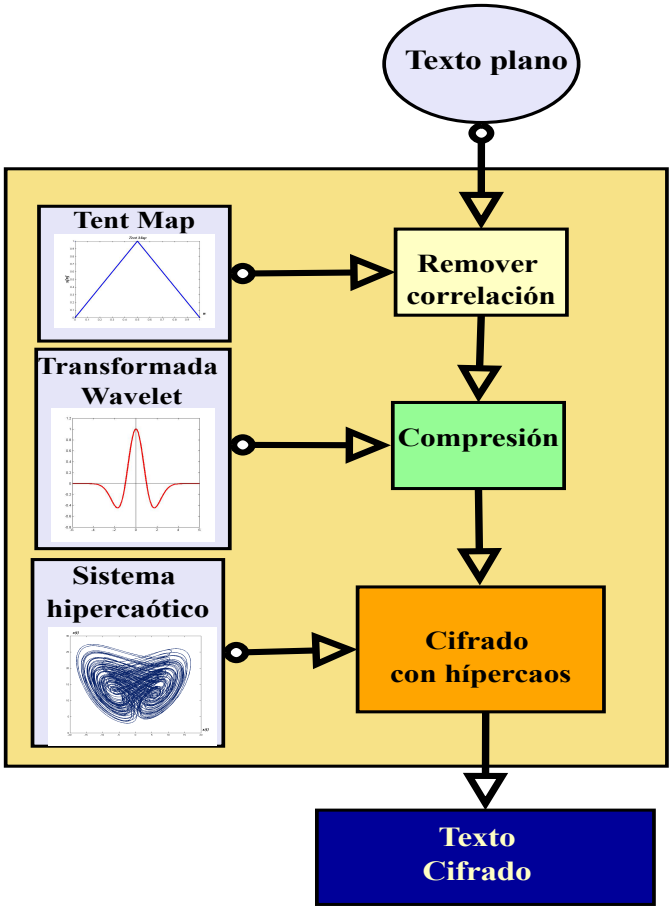

Figure 1: Diagrama a bloques que ilustra el sistema de compresión y cifrado de información.

Calendario de Actividades

- Junio-Agosto 2017 Revisión del estado del arte de la teoría wavelet y de sistemas de cifrado que consideren sistemas dinámicos en su estructura . Además, iniciar con el estudio de sistemas dinámicos que presenten dinámica caótica e hipercaótica.
- Septiembre-Diciembre 2017 Continuar con la revisión bibliográfica. Implementación de

programas basados en variantes de la transformada wavelet que permitan realizar la compresión de información de diferente tipo de señales. Cursar las materias correspondientes al tercer semestre.

- Enero-Marzo 2018 Continuar con la revisión bibliográfica. Establecer un conjunto de herramientas que permitan implementar de manera conjunta la etapa de compresión, así como la del cifrado.
- Abril-Julio 2018 Redacción de tesis.
- Julio-Agosto 2018 Presentación de exámenes previo y final del proyecto de tesis.

Materias por Cursar

En el semestre considerado de agosto a diciembre del año 2017 se sugiere cursar las materias de (a)Procesamiento de señales en tiempo real, (b) Procesamiento digital de imágenes o Codificación de datos.

Bibliografía

[1] Ingrid Daubechies, *Ten lectures on Wavelets*, SIAM, Philadelphia, PA, 1992.

[2] Stéphane Mallat, *A Wavelet Tour of Signal Processing*, 2nd. Edition, Academic Press, 1999.

[3] Shie Qian, *Introduction to Time–Frequency and Wavelet Tarnsform*, Prentice Hall PTR, 2002.

[4] J. Urías, E. Ugalde and G. Salazar, ´´A cryptosystem based on cellular automata", Chaos **8**, 819-822, 1998.

[5] J. S. Murguía, G. Flores-Eraña, M. Mejía Carlos, H.C. Rosu, ´´Matrix Approach of an Encryption System Based on Cellular Automata and its Numerical Implementation", International Journal of Modern Physics C **23**, No. 11, 1250078 (13 pages), 2012.

[6] T. Gao, Z.Chen, ´´A new image encryption algorithm based on hyper-chaos", Physics Letters A **372**, 394-400, 2008.

[7] R. Rhouma, S. Belghith, ´´Cryptanalysis of a new image encryption algorithm based on hyper-chaos", Physics Letters A **372**, 5973-5978, 2008.