ALGORITMO DE CIFRADO SIMÉTRICO BASADO EN MAPEO LOGÍSTICO Y TRANSFORMADA RÁPIDA DE FOURIER

Francisca Angélica Elizalde Canales

Universidad politécnica de Tulancingo

Francisca.elizalde@upt.edu.mx

Iván de Jesús Rivas Cambero

Universidad politécnica de Tulancingo

Ivan.rivas@upt.edu.mx

Resumen

Las herramientas estadísticas utilizadas en la criptografía desde la antigüedad hasta nuestros días, son muy útiles en el criptoanálisis de sistemas de cifrado dado que ofrecen un buen instrumento para la identificación del sistema de cifrado utilizado en un criptograma. Los algoritmos criptográficos son cada vez más necesarios para garantizar la confidencialidad de los datos en la transmisión de forma segura a través de canales de comunicación inseguros.

En éste trabajo se presenta un algoritmo de cifrado simétrico, cuya implementación está basada en el acoplamiento de mapeo logístico, un generador congruencial lineal, y la trasformada rápida de Fourier. Como parte del proceso se generan subclaves de cifrado a través de una semilla extraída de una zona caótica para aumentar su nivel de aleatoriedad. Se realiza un análisis al criptograma, en particular, con pruebas estadísticas sobre datos cifrados, con el fin de determinar su impredecibilidad en secuencias generadas, evaluando las propiedades de independencia y aleatoriedad. Se obtienen resultados en simulación que muestran una notable distorsión en los datos cifrados con respecto a los originales, que, en términos de seguridad, disminuye su vulnerabilidad ante ataques externos.

Palabra(s) Clave(s): Algoritmo de cifrado, criptograma, descifrado, pruebas estadísticas.

1. Introducción

El uso de pruebas estadísticas en la criptografía parece que se remontan al primer milenio después de Cristo, debido a Abu Yaqub Yusuf Ibn Ishaq al-Sabah Al-Kindi (801-873), que fue un pionero en el criptoanálisis y criptología [1], se le atribuye el desarrollo de un método en el que se podría analizar las variaciones en la frecuencia de la aparición de cartas y utilizarlo para romper el cifrado; es decir criptoanálisis por análisis de frecuencias. Más tarde, en 1863, Friedrich Kasiski publicó un libro, que fue el primer relato divulgado de un procedimiento para atacar cifras de sustitución polialfabéticos, especialmente el sistema de cifrado de Vigenère, cuyo método se basó en el análisis de las diferencias entre los fragmentos repetidos en el texto cifrado; este tipo de análisis puede dar pistas sobre la longitud de la clave utilizada [2]. Posteriormente, durante la Segunda Guerra Mundial, se transmitieron códigos secretos a través de redes de comunicaciones de radio que usaban códigos formales e informales desarrollados en sus lenguas maternas [3].

Hoy día es imprescindible implementar mecanismos de seguridad que permitan resguardar los datos sensibles ante algún ciberataque, dado el avance tecnológico que ha propiciado el incremento del uso sistemas de información, lo que ha generado vulnerabilidad a ataques cibernéticos, siendo la criptografía uno de los mecanismos de protección más utilizados, debido a que se encarga de ocultar los datos ante terceros, proporcionando confidencialidad mediante algún método de cifrado [4].

Bajo la consideración de que, el caos es un comportamiento de un sistema dinámico que cambia de manera irregular en el tiempo, muchos métodos o esquemas de comunicación segura se han desarrollado para cifrar información basándose en sistemas discretos caóticos [5]. Existe una relación cercana entre el caos y la criptografía porque los sistemas caóticos tienen características de ergodicidad, propiedades de mezcla, sensibilidad en los parámetros y en las condiciones iniciales, que pueden considerarse análogos a las técnicas de difusión y confusión, integrados en muchos sistemas criptográficos [6,7].

La criptografía ha sido aplicada en varios sectores críticos donde se requiere reforzar la seguridad cibernética, un ejemplo es el sector de la energía eléctrica, que se vuelve cada vez más vulnerable debido a que, en una red eléctrica inteligente además de la conexión con generación, transmisión y distribución, también se incluyen a los consumidores, todos ellos interconectados bajo las tecnologías de la comunicación y la información, proporcionada esta interacción por medio de medidores inteligentes que podrían exhibir accesos no autorizados a la privacidad del consumidor, lo que se convierte en una preocupación en el manejo de información para adopción de redes inteligentes ante la posibilidad cada vez mayor de ataques cibernéticos [8,9].

En [10] proponen una infraestructura de privacidad amigable para conservar la confidencialidad en el consumo de energía eléctrica por medio de un algoritmo criptográfico que no expone el patrón de consumo de energía así como la identidad de los consumidores, basado en el esquema de compartición de secretos de Shamir que permite ocultar información con el fin de preservar la privacidad de los consumidores. Para mantener la seguridad con demandas computacionales bajas, en [11] hacen uso de diferentes variantes de la transformada Wavelet en combinación con cifrado selectivo para permitir a los consumidores denegar el acceso a diferentes datos.

Para abordar el problema de inseguridad, [12] presentan una distribución gradual en el que agregan cifrado homomórfico a los medidores inteligentes implicados en el envío de datos, desde la fuente hasta la unidad de recolección para garantizar que los resultados intermedios no sean revelados a cualquier dispositivo en la ruta. La historia de la criptografía nos da pruebas de que puede ser difícil mantener en secreto los detalles de un algoritmo usado extensamente, siendo una clave más sencilla de proteger, que todo un sistema de cifrado, y es más fácil de substituir si ha sido descubierta. Al diseñar un sistema de seguridad, es recomendable asumir que los detalles del algoritmo de cifrado ya son conocidos por el hipotético atacante, como se enuncia en el Principio de Kerckhoff [13], sólo el mantener la clave en secreto proporciona seguridad.

El objetivo de realizar un cifrado, es el de dificultar o imposibilitar la comprensión de la información a personas ajenas [14]. Shannon, denominado el padre de la teoría de la información [15], determina la entropía como la incertidumbre de una fuente de información. Cuanto mayor sea la entropía aumenta la impredecibilidad de los datos. El concepto de entropía basado en la teoría de la información es en realidad la medida de la inconsistencia, los datos no estructurados o la aleatoriedad de las variables, siendo menos vulnerable cuanta más entropía contenga [16,17].

En este trabajo se realiza una valoración estadística, a un algoritmo criptográfico simétrico, que tiene como propósito fortalecer la protección de la privacidad de los datos adquiridos y procesados por la simulación de un dispositivo de medición de energía eléctrica, buscando mejorar la seguridad de los datos enmascarando éstos ante posibles ataques mal intencionados. El algoritmo se conforma de tres técnicas: mapeo logístico, acoplado con generador congruencial lineal con el propósito de maximizar la imprevisibilidad de la secuencia de cifras aplicado como primera etapa de cifrado y posteriormente la transformada rápida de Fourier para incrementar la técnica de confusión. En la sección de resultados se presentan las representaciones obtenidas con el algoritmo al aplicarlo para codificar una serie de datos de consumo de energía eléctrica, donde se puede apreciar el comportamiento de los datos después de ser alterados por el algoritmo de cifrado propuesto.

2. Técnicas

A continuación, se refieren las técnicas utilizadas para el diseño del algoritmo de cifrado simétrico, dadas sus características computacionales, en donde se incluye mapeo logístico como generador de semilla, generador congruencial para generar subclaves, y trasformada rápida de Fourier para aumentar la confusión. Consiguiendo con los dos primeros robustecer la clave, dado que la fortaleza de la criptografía reside en la elección de las claves, las cuales son parámetros secretos y no debe haber posibilidad de que un intruso pueda inferirla.

Mapeo logístico

El caos muestra que un comportamiento complejo puede aparecer de reglas deterministas simples cuando no hay linealidad. Dado que los mapas caóticos son capaces de generar señales de aspecto estocástico y las implementaciones prácticas basadas en sistemas caóticos son más simples que las requeridas para sistemas estocásticos es natural que se proponga utilizar el caos como generador de ruido en diversas aplicaciones. La aplicación logística ha sido usada como generador de números pseudo-aleatorios. Para este fin en [18], han realizado ciertas pruebas estadísticas sobre las series de números obtenidas de sistemas dinámicos discretos y han encontrado que cumplen satisfactoriamente y por tanto posee muchas de las propiedades requeridas por un generador de números pseudo-aleatorios.

El mapeo logístico, puede presentar una dinámica muy amplia, variando el valor de un parámetro, se pueden tener trayectorias que tienden a un punto fijo, que son periódicas o bien caóticas. Este sistema dinámico, es uno de los modelos discretos más simples utilizado para el estudio de la evolución de población en sistemas cerrados, que viene dado por ecuación 1 [19].

$$x_{t+1} = \mu x_t(1 - x_t) \tag{1}$$

Donde μ, es una constante, llamada parámetro de control, que determina el grado de no-linealidad del mapa, y x_t, es la variable de estado que determina la secuencia (x_0, x_1, x_2…) de la trayectoria u orbita correspondiente a la condición inicial x_0. En el que la constante μ varía entre $0 < \mu < 4$. El espacio de fases del sistema es en el intervalo [0,1]. Los sistemas dinámicos discretos evolucionan en el tiempo por el proceso de iteración, en el que el siguiente estado del sistema viene determinado por su estado actual. El comportamiento de la ecuación (1): bajo los parámetros de μ y x_t: cuando $0 <= \mu <= 4$, y $0 <= x_t <= 1$. Cuando, $x_1 = f(x_0)$, $x_2 = f(x_1) = f_2(x_0)$... $x_t = f(x_t-1) = f_t(x_0)$, donde x_t, es la nueva iteración de x_0 y el conjunto de todas las iteraciones es el mapeo de la función f que forma una parábola. Se dice que sus características dinámicas son universales. Ejemplos de estos rasgos son la sensibilidad a las condiciones iniciales, la ruta al caos por duplicación de periodo o el fenómeno de la intermitencia.

Generador Congruencial

La generación de números pseudo-aleatorios juega un papel crítico en gran número de aplicaciones tales como, simulaciones numéricas, las comunicaciones o la criptografía, dado que permite generar secuencias de números con algunas propiedades de aleatoriedad. Las principales ventajas de tales generadores son la rapidez y la repetitividad de las secuencias pseudo-aleatorias producidas. En la práctica, la generación de números pseudo-aleatorios no es trivial y la calidad aleatoria de las secuencias producidas puede ser esencial en la elección de su aplicación [20].

El generador de congruencia lineal, es uno de los generadores más antiguos y sencillos es propuesto por Lehmer en 1949, que consiste en, a partir de un número inicial llamado semilla, generar una secuencia por recurrencia; ecuación 2.

$$X_{n+1} = (\mathrm{a}X_n + c)\ mod\ m \tag{2}$$

Donde debe tenerse en cuenta que los valores *a*, X_n y *c* tienen que ser mayores que cero y, la variable *m*, tiene que ser un número primo suficientemente mayor que los tres anteriores.

Este tipo de generador es computacionalmente rápido y de fácil implementación; sin embargo, posee propiedades no tan ideales, como la producción de secuencias de valores que se repiten con un período máximo de *m*-1, sin embargo, las secuencias producidas por un generador congruencial lineal son muy sensibles a cambios en sus parámetros, lo cual es una propiedad útil [21,22].

Transformada rápida de Fourier

La transformada rápida de Fourier, un método matemático para la transformación de una función del dominio del tiempo al dominio de frecuencia. Es un eficiente algoritmo que permite calcular la transformada de Fourier discreta y su inversa. Siendo uno de los algoritmos aritméticos ampliamente utilizados, debido a su eficiencia en cuanto al tiempo de cómputo para grandes arreglos de entrada cuya longitud es una potencia entera de dos. La transformada de Fourier de una señal en tiempo discreto se calcula mediante ecuación 3.

$$X(w) = \sum_{n=-\infty}^{\infty} x[n] . e^{-j\omega n} \quad (3)$$

Y su inversa ecuación 4.

$$x[n] = \frac{1}{2\pi} \int_{-\pi}^{\pi} X . e^{-j\omega n} d\omega \quad (4)$$

La cual proporciona un medio oportuno para mejorar el rendimiento de los algoritmos para un conjunto de problemas aritméticos comunes [23].

Dichos métodos se implementan en el algoritmo de cifrado dadas sus características, como son la velocidad de procesamiento y el bajo costo en términos de recursos computacionales. El generador lineal, posee gran sensibilidad a cambios en sus parámetros, además de rapidez para generar números pseudoaleatorios, sin embargo, presenta cierta vulnerabilidad a los ataques de fuerza bruta; para evitar tal inconveniente se acopla con un sistema para la generación de números pseudoaleatorios a través de la aplicación caótica, capaz de generar de forma recursiva números impredecibles, con un bajo costo en recursos y resistente a los ataques externos, con posibilidad de generar secuencias de números con características de aleatoriedad altas. Con el fin de aportarle robustez al sistema de criptográfico, se hace uso de la transformada rápida de Fourier, la cual ofrece un seguro, eficiente y rápido flujo de información, debido a la gran velocidad que posee para procesar datos.

3. Experimentación

Para el diseño del algoritmo se recurre a las tres técnicas señaladas en la sección anterior, haciendo un acoplamiento del mapeo logístico con el generador congruencia lineal, dadas las características de ambos se complementan para aumentar la imprevisibilidad de la clave de cifrado, y se mejora la seguridad de encriptado agregando la trasformada rápida de Fourier para dificultar la intrusión a los datos. Las tres técnicas presentan gran eficiencia en cuanto a rendimiento de cómputo.

Dentro de los sistemas discretos caóticos uno de los más utilizados para codificar información es el mapa logístico debido a su sencillez, rapidez y sensibilidad a

condiciones iniciales y parámetro de control [22,24]. En nuestro caso de estudio la variable $x_t \in (0,1)$ y $\mu \in (3.85, 4)$ para estar dentro de la zona de caos [25].

Como puede apreciarse en la figura 1, el sistema presenta bifurcación de periodo con μ cercano a 3, de este punto en adelante la bifurcación de periodo es cada vez más frecuente generando comportamiento caótico. En la figura se señala con un rectángulo el área que será aprovechada en este caso.

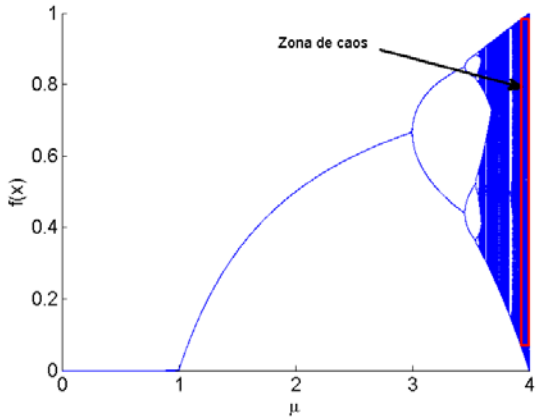

Figura 1 Diagrama de bifurcación del mapeo logístico.

Para garantizar secuencias impredecibles, es necesario utilizar una semilla que se encuentre dentro de la zona en que el sistema se comporta de forma inestable. Por éste motivo se utilizarán los resultados obtenidos en donde se muestra el análisis dinámico de generadores caóticos, evaluándolos a través de los exponentes de Lyapunov, con el fin de delimitar el rango del parámetro que muestre un comportamiento impredecible. En donde el exponente de Lyapunov cuantifica el grado de inestabilidad local en un espacio de estados mediante ecuación 5.

$$\lambda = \lim_{n\to\infty}\{\frac{1}{2}\sum_{i=0}^{n-1} ln|f'(x_i)|\} \quad (5)$$

Que puede definirse como el promedio del logaritmo natural del valor absoluto de las derivadas de la función del mapeo evaluadas en los puntos de la trayectoria [6]. El horizonte de predecibilidad de un sistema es caótico, es temporalmente limitado. El límite está asociado con su exponente positivo de Lyapunov. La secuencia temporal, generada a partir de una de sus trayectorias caóticas, no

puede comprimirse por un factor arbitrario, es decir es algorítmicamente compleja. En un sistema caótico, una pequeña perturbación produce una separación, creciente con el tiempo, entre una trayectoria y la misma perturbada. Se tiene de esta manera una rápida amplificación (exponencial) de un error en las condiciones iniciales. Por el contrario, una trayectoria regular puede comprimirse fácilmente.

La tabla 1, muestra un resumen de los rangos seguros del parámetro y condiciones iniciales en los que la ecuación logística presenta y mantiene temporalmente comportamiento caótico.

Tabla 1 Rangos seguros del parámetro y condiciones iniciales.

Ecuación logística	Parámetro	Condición inicial
$x_{t+1} = \mu x_t(1 - x_t)$	$3.96 < \mu < 4$	$0 < x_t < 1$

Con este parámetro y condiciones iniciales se generan series de números impredecibles que son utilizados como semilla para complementar la llave de cifrado aplicando la técnica de confusión que consiste en ocultar la relación entre la información original, la cifrada y la clave.

La figura 2 muestra un diagrama de bloques del algoritmo compacto propuesto, que incluye los procedimientos que integran el encriptado completo y sus etapas que implican el desarrollo de encriptación.

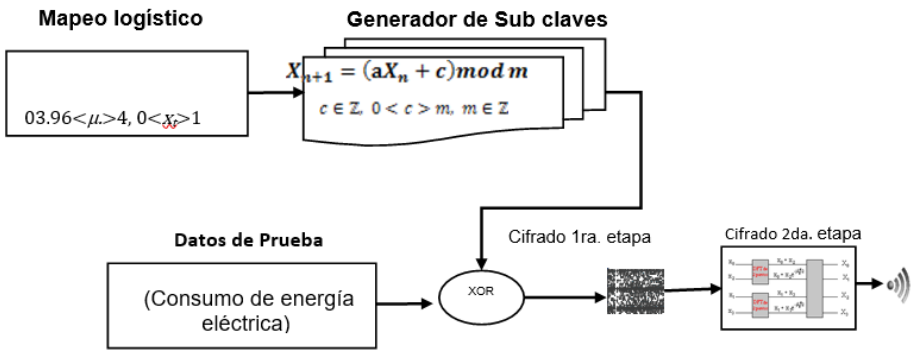

Figura 2 Diagrama de bloques del algoritmo de encriptación.

En el bloque de la señal eléctrica, se adquieren las señales de voltaje y corriente y la obtención del consumo de energía, datos que serán encriptados. El bloque

generador de sub-claves representa el procedimiento a seguir para generar una semilla con números impredecibles a través de mapeo logístico unidimensional; localizada una zona caótica que mantenga temporalmente el comportamiento de inestabilidad siendo esta zona evaluada por el exponente de Lyapunov; de la serie de números impredecibles obtenidos, se selecciona aleatoriamente uno de ellos el cual sufrirá una trasposición geométrica y, se fusiona con un generador de números pseudoaleatorios para obtener las subclaves, que encriptarán los datos a través del operador lógico de disyunción exclusiva Xor, con una señal de consumo de energía eléctrica y con ello se genera la primera etapa del diagrama de proceso de encriptación [26].

Con el propósito de fortalecer los datos encriptados en la primera etapa, se aplica un procedimiento iterativo, que incluye una mejora aleatoria con la compensación de la técnica de trasformada rápida de Fourier como segunda etapa, representada bajo ecuación 6.

$$X(w_k) = X(k) = \sum_{n=-\infty}^{\infty} x[n] \cdot e^{-j(2\pi k/N)n} \quad (6)$$

k=0, 1…, N-1

Finalmente se obtienen, los datos totalmente enmascarados y preparados para ser enviados de forma inalámbrica por algún canal probablemente inseguro.

Una vez que se reciben los datos enviados, estos deben ser descifrados con la clave de cifrado y el uso de un algoritmo de recuperación; el cual realiza la operación reversible para reconstruir el mensaje de los datos recibidos. Siendo el proceso de descifrado muy similar al cifrado, excepto porque se aplican los métodos de manera inversa.

4. Resultados

Se evalúa estadísticamente un algoritmo que tiene como propósito fortalecer la seguridad en datos generados por medio de un dispositivo de medición de consumo de energía eléctrica, buscando mantener el equilibrio entre la seguridad y el rendimiento, sin comprometer el costo en términos de recursos computacionales. El algoritmo está conformado por la fusión de las técnicas antes

mencionadas, debido a su facilidad y alto rendimiento en esta clase de procesos, añadiendo pruebas para su desarrollo y compilación que permiten el análisis de resultados.

Análisis al criptograma

Para evaluar el algoritmo de cifrado propuesto previamente, el cual está enfocado para trabajar con medición de datos de energía eléctrica en el marco de las redes inteligentes; se desarrolla un circuito de prueba de corriente alterna a 60 Hz, en el que se mide el voltaje y la corriente para calcular la potencia, y con ello la energía que consume una carga resistiva. En la figura 3, se presenta la curva de consumo de energía eléctrica obtenida, cuando la carga resistiva es de 144Ω. Para este caso demostrativo, solo se presenta el consumo de energía en el trascurso de un tiempo de 10 segundos. En la figura 3, se muestra la señal de los datos originales antes de aplicar el algoritmo de cifrado, y en esta figura se sobrepone la señal recuperada (descifrada) después del proceso.

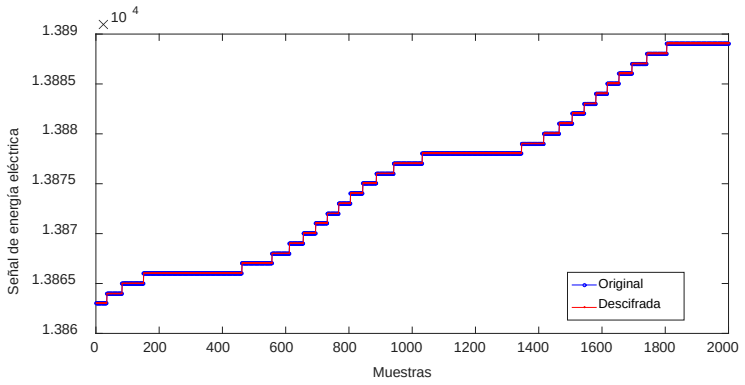

Figura 3 Señal de energía eléctrica original y señal descifrada.

Tanto en las figuras 3 y 4 puede apreciarse, el comportamiento de la señal original, que representa el consumo de energía, y su equivalente cifrada, respectivamente, esta última presenta un comportamiento con variación en la señal una vez que es afectada por el algoritmo de cifrado, en sus propiedades básicas (frecuencia, amplitud), tendiendo a parecerse a una señal de ruido.

En la figura 4, se presenta la señal cifrada usando el algoritmo propuesto en esta sección; utilizando como clave de cifrado la misma que para descifrado (simétrico),

empleando como semilla una serie de números impredecibles inútiles para un supuesto atacante.

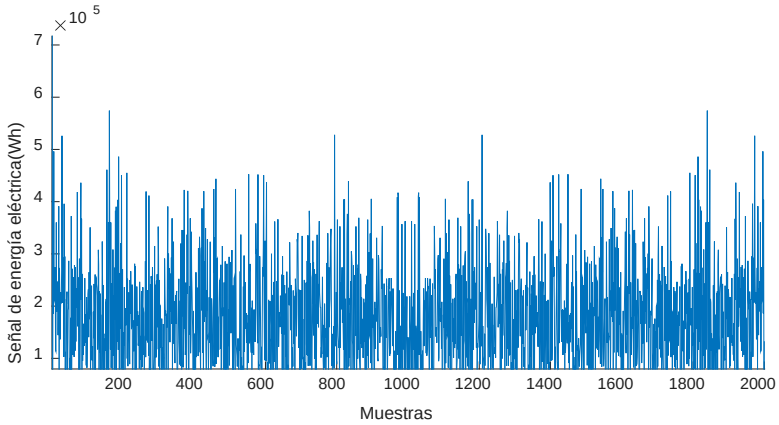

Figura 4 Señal cifrada con el algoritmo propuesto.

Se realiza un análisis bajo herramientas estadísticas, para valorar las características de independencia, distribución y correlación entre la sucesión datos cifrados. Se realiza un análisis de correlación donde se mide la asociación lineal entre los datos originales y los datos cifrados, posteriormente se realiza la correlación con los datos cifrado y los descifrados, con la finalidad de determinar si existe alguna perdida de información al utilizar el algoritmo; las métricas se concentran en la tabla 2.

Tabla 2 Concentrado de métricas estadísticas al criptograma.

Métricas estadísticas	
Coeficientes de correlación	-0.0251
Entropía	3.5156e+12
Desviación estándar	4.7287e+03
Media	8.5264e+03
Mediana	8.6835e+03
Varianza	2.2360e+07
Corrida ascendente y descendente	0
Información mutua normalizada	0.6098

Coeficientes de correlación

Con el fin de obtener medidas numéricas se calcula el coeficiente de correlación con ecuación 7.

$$c = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad (7)$$

Donde, n es el número de elementos en los dos vectores adyacentes *x* y *y*. Para datos fuertemente encriptados, los coeficientes de correlación se deben aproximar a cero [26, 27].

Histogramas

En las figuras 5 y 6, se muestra la distribución de los valores tanto en la señal original como en la señal cifrada, respectivamente. En el primer caso el histograma exhibe en el eje horizontal los valores de la señal en el rango de 13865 a 13890, donde, las barras más altas indican los valores que se repiten con mayor frecuencia. Por otra parte, en el segundo caso, el histograma de la señal cifrada, con el algoritmo propuesto, en el eje horizontal presenta valores de 0 a 16000.

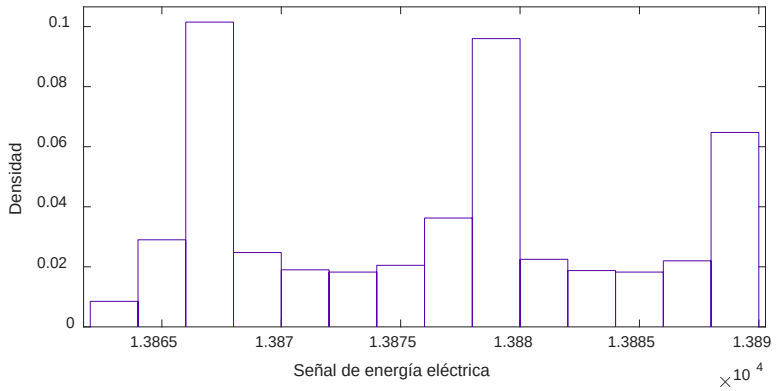

Figura 5 Histograma de señal original.

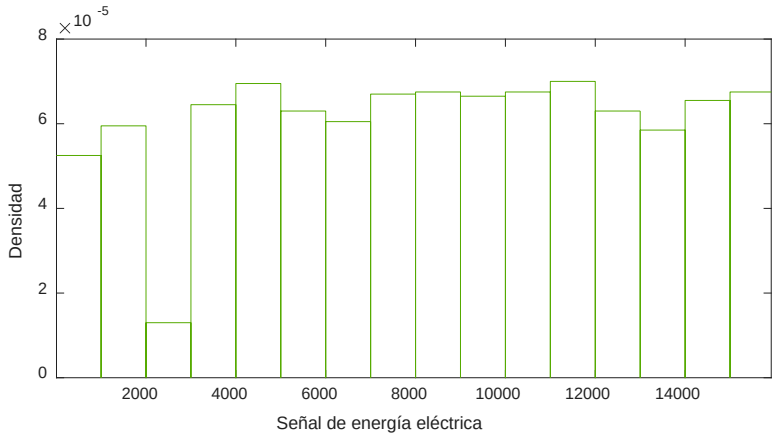

Figura 6 Histograma de señal cifrada.

Al comparar ambos histogramas de las figuras 5 y 6, se observa que tienen diferente distribución en las frecuencias de la señal original respecto a la señal cifrada, mostrando rangos diferentes en el eje horizontal, lo cual, aumenta la dificultad al posible atacante para analizar y descifrar los datos codificados.

Entropía

La entropía mide la incertidumbre de una fuente de información calculando la aleatoriedad de los datos, lo que permite evitar cualquier previsibilidad, así como también se mide la independencia entre variables a través de la información mutua normalizada. La entropía está dada por ecuación 8.

$$H = \sum_{i=1}^{2^8} P(S_i) \log_2 P(S_i) \quad (8)$$

Donde H, representa (entropía de Shannon) la sorpresa de un evento o su nivel de incertidumbre, S, un símbolo y P la probabilidad de aparición de éste. Se considera que, entre más alto es el valor de H, más inesperado se hace la ocurrencia de dicho evento, en otras palabras, se torna más aleatorio e impredecible [17].

La teoría de la información de Shannon permitió la caracterización estadística de fuentes deterministas caóticas. Estos esfuerzos para describir la impredescibilidad de sistemas dinámicos condujeron a la definición de cantidades tales como la entropía métrica y los exponentes de Lyapunov que pueden emplearse para detectar la presencia y para cuantificar el comportamiento caótico determinista. Un sistema periódico produce un conjunto de puntos. Un sistema en que un estado es función de los anteriores produce una curva. Un sistema aleatorio produce una nube de puntos. Para mostrar que los resultados simulados demuestran viabilidad y seguridad del algoritmo propuesto, se emplean pruebas estadísticas de distribución, dispersión, correlación, histogramas y entropía; se comprueba que efectivamente los datos que se obtienen provienen de secuencias con alto grado de aleatoriedad; con lo cual se dificulta para un atacante determinar algún orden en los datos, por lo que el cifrado se puede considerar válido y confiable.

En la tabla 2, se muestra el comportamiento de la señal resultante después del proceso de cifrado y los valores resultantes en base a la evaluación aplicada

donde las propiedades importantes esperadas son uniformidad e independencia en los datos cifrados.

El criptograma muestra una distribución uniforme de los datos, sin asociación entre las variables, el coeficiente de correlación indica que no hay correlación al estar muy cercano a cero, La entropía es equivalente al "desorden", así que, si aumenta la entropía, significa que creció el desorden. Dado el resultado de corridas ascendentes y descendentes se acepta la aleatoriedad.

Si bien existen en la literatura bancos de prueba de propósito general para la evaluación de generadores de números pseudoaleatorios, no están diseñados tomando en cuenta las características particulares de los mapas caóticos, la naturaleza determinista del caos deja su marca en la serie temporal y deben buscarse cuantificadores adecuados para descubrir esa firma.

5. Conclusiones

En este trabajo se presenta una evaluación estadística a un nuevo algoritmo de cifrado, el cual combina el comportamiento impredecible de una función logística, usada para obtener subclaves a partir de una semilla y un generador de números pseudoaleatorios, ambos mezclados con la transformada de Fourier para agregar la técnica de confusión al cifrado. El algoritmo se implementa en Matlab para apreciar el proceso de cifrado y descifrado y sobre todo evaluar la aleatoriedad, usando diferentes herramientas estadísticas.

Las pruebas aplicadas al algoritmo se desarrollan bajo la consideración de cifrar un conjunto de datos que representan el consumo de energía eléctrica, obtenidos por la simulación de la adquisición de las variables eléctricas que puede entregar un medidor inteligente, bajo el contexto de las redes inteligentes, conocidas como Smart Grid, donde se busca aumentar la confidencialidad de los datos implicados durante el proceso de medición y transmisión por medios inseguros de comunicación, entre dispositivo de medición, usuario y proveedor.

La información presentada en este artículo forma parte de un proyecto mayor, en donde se está desarrollando un prototipo de medición de consumo de energía eléctrica en el que se implementará el algoritmo propuesto, en este sentido, se

requiere hacer una evaluación de las demandas computacionales y los tiempos de ejecución en hardware para desarrollar la etapa de implementación.

6. Bibliografía y Referencias

[1.] S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. 1999. Anchor Books.

[2.] D. Kahn, The Codebreakers - The Story of Secret Writing. 1996. revised ed. Scribner.

[3.] N. Aaseng, Navajo Code Talkers: Americas Secret Weapon in World War II. 1992. Walker & Company. New York.

[4.] M. Mogollon, Cryptography and security services: mechanisms and applications. 2007. Hershey, PA: CyberTech. Pp. 51-97.

[5.] B. Rajan, P. Saumitr, “A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system”. IEEE Transactions on circuits and system. Vol. 4. 2006. Pp. I- 53.

[6.] M. Jiménez, F. Flores, G. González, “System for Information Encryption Implementing Several Chaotic Orbits”. Ingeniería, Investigación y Tecnología. Vol. 16. Issue 3. 2015. Pp. 335-343.

[7.] Radwan, S. AbdElHaleem, S. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review”. Journal of Advanced Research. Vol. 7. No. 2. 2016. Pp. 193–208.

[8.] F. Li, B. Luo, P. Liu, “Secure information aggregation for smart grids using homomorphic encryption”. First IEEE international conference on Smart Grid Communications (SmartGridComm). Pp. 327–332.

[9.] Kerckhoffs, “La cryptographie militaire, Journal des sciences militaires”. Vol. 9. 1983. Pp. 161-191.

[10.] Rottondi, G. Verticale, “Privacy-friendly load scheduling of deferrable and interruptible domestic appliances in Smart Grids”. Computer Communications. Vol. 58. No. 1. 2015. Pp. 29–39.

[11.] Engel, Wavelet-based load profile representation for smart meter privacy. Innovator Smart Grid Technologies (ISGT), IEEE PES. 2013. Pp. 1-6.

[12.] McKenna, I. Richardson, M. Thomson, “Smart meter data: Balancing consumer privacy concerns with legitimate applications”. Energy Policy. Vol. 41. 2012. Pp. 807-814.

[13.] S. Zeadally, A. S.K. Pathan, C. Alcaraz, M. Badra, “Towards privacy protection in smart grid”. Wireless personal communications. Vol. 73. No. 1. 2013. Pp. 23-50.

[14.] H. Hennawy, A. Omar, S. Kholaif, “LEA: Link Encryption Algorithm Proposed Stream Cipher Algorithm”. Ain Shams Engineering Journal. Vol. 6. No. 1. 2015. Pp. 57-65.

[15.] Shannon, A mathematical theory of communication. 1948. Bell Syst. Tech. Pp. 27, 379–423, 623–656.

[16.] S. Kumar, K. Abhishek, M. Singh, “Accessing Relevant and Accurate Information using Entropy”. Procedia Computer Science. 2015. Pp. 54, 449-455.

[17.] Shannon, Teoría de la Comunicación de Secrecy Systems. Bell Tech System. Vol. 28. 1949. Pp. 656-715.

[18.] Rao Logistic Map: A Possible Random Number Generator. http://arXiv.org/abs/cond-mat/9310004v1

[19.] R. May, Simple Mathematical Models with Very Complicated Dynamics, Nature. 1976. Pp. 261, 459-467.

[20.] M. François, T. Grosges, D. Barchiesi, R. Erra, “Pseudo-random number generator based on mixing of three chaotic maps”. Communications in Nonlinear Science and Numerical Simulation. Vol. 19. No. 4. 2014. Pp.887-895.

[21.] D.H. Lehmer, “Mathematical methods in large-scale computing units”. 2 ndsymposium on large-scale digital calculating machinery, cambridge, massachussets. 1949. Pp. 141-146.

[22.] N. Pareek, V. Patidar, K. Sud, “Discrete chaotic cryptography using external key”. Physics Letters A. Vol. 309. Issue 1-2. 2003. Pp. 75-82.

[23.] J. Vilardy, C. Torres, L. Mattos, “Encriptación de Imágenes Digitales Via Transformada Fraccional de Fourier Discreta y Transformada Jigsaw”. Revista Colombiana de Física. Vol. 41. No. 2. 2009. Pp. 1-4.

[24.] Y. Mao, G. Chen, and S. Lian, “A novel fast image encryption scheme based on 3d chaotic baker maps”. International Journal of Bifurcation and Chaos. Vol. 14. Issue 10. 2004. Pp. 3613-3624.

[25.] R. Clark, Dynamical systems: stability, symbolic dynamics, and chaos CRC Press. 1995.

[26.] B. Wichmann, I. Hill, “Generating good pseudo-random numbers”. Computational Statistics & Data Analysis. Vol. 51. Issue 3. 2006. Pp. 1614-1622.

[27.] Pavanello, W. Zaaiman, A. Colli, J. Heiser, S. Smith. “Statistical functions and relevant correlation coefficients of clearness index”. Journal of Atmospheric and Solar-Terrestrial Physics. 2015. Pp. 130-131,142-150.

7. Autores

Francisca Elizalde-Canales, estudiante de doctorado en Optomecatrónica, obtuvo título de Maestra en ciencias de la información y administración del conocimiento en el Instituto Tecnológico de Monterrey campus Hidalgo. Especialidad en Sistemas y Planeación y Licenciatura en Computación en Universidad Autónoma del Estado de Hidalgo. Su área de interés es sobre el fortalecimiento de la ciberseguridad en sistemas de medición de energía eléctrica en el escenario de la red inteligente.

Iván Rivas-Cambero, profesor investigador en el Área de Control y automatización obtuvo su título de Doctor en Ciencias con especialidad en Ingeniería Industrial en la Universidad Autónoma del Estado de Hidalgo; el título de Maestro en Ciencias en Ingeniería Eléctrica por el Cinvestav unidad Guadalajara. Su área de interés es sobre sistemas eléctricos inteligentes y control difuso.