Artículo **Revista de Cómputo Aplicado**
Septiembre 2017 Vol.1 No.3 38-49

Algoritmo criptográfico con semilla caótica y generador congruencial para fortalecer la seguridad de los datos transmitidos de forma inalámbrica

ELIZALDE-CANALES, Francisca Angélica*†, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y RUEDA-GERMÁN, Clementina

Recibido Julio 13, 2017; Aceptado Septimebre 15, 2017

Resumen

Los algoritmos criptográficos juegan un papel importante en la seguridad de la información, principalmente en el fortalecimiento de la privacidad de los datos. Los sistemas caóticos pueden ser empleados en la codificación de la información, debido a su inestabilidad orbital y ergodicidad. En este trabajo se propone la aplicación de un algoritmo de cifrado de clave simétrica basado en funciones caóticas de mapeo logístico para generar subclaves de cifrado a través semillas impredecibles extraídas de las zonas caóticas para aumentar su nivel de aleatoriedad. El algoritmo es aplicado sobre una señal simulada de consumo de energía eléctrica. Se genera un criptograma, el cual es analizado estadísticamente para determinar el grado de impredecibilidad; se obtienen propiedades adecuadas en términos de calidad de la aleatoriedad, mismos que son validados con las pruebas estadísticas que establece El Instituto Nacional de Estándares y Tecnología (NIST).

Algoritmo de cifrado, pruebas estadísticas, criptograma, descifrado

Abstract

The cryptographic algorithms play an important role in the security of the information for the strengthening of the privacy. Chaotic systems can be used in the coding of information, due to their orbital instability and ergodicity. This work proposes the application of a symmetric key cryptographic algorithm based on chaotic logistical mapping functions to generate encryption subkeys through unpredictable seeds extracted from the chaotic zones to increase their level of randomness. The algorithm is applied on a simulated electrical energy consumption signal. A cryptogram is generated, which is statistically analyzed to determine the degree of unpredictability; appropriate properties are obtained in terms of quality of randomness, which are validated with the statistical tests established by the National Institute of Standards and Technology (NIST). Application of seed Congruential to strengthen the security of the data transmitted wirelessly.

Encryption algorithm, statistical tests, cryptogram, decryption

Citación: ELIZALDE-CANALES, Francisca Angélica, RIVAS-CAMBERO, Iván de Jesús, ARROYO-NÚÑEZ, José Humberto y RUEDA-GERMÁN, Clementina. Algoritmo criptográfico con semilla caótica y generador congruencial para fortalecer la seguridad de los datos transmitidos de forma inalámbrica. Revista de Cómputo Aplicado 2017, 1-3: 38-49

* Correspondencia al Autor (Correo Electrónico: francisca.elizalde@upt.edu.mx)
† Investigador contribuyendo como primer autor.

Introducción

En el contexto de la energía eléctrica, se plantea la importancia de la gestión de la demanda eléctrica con base en los múltiples beneficios que traen tanto a los consumidores como a los proveedores de servicios (Moreno-Dzul, 2016); la medición inteligente puede aportar grandes beneficios, como la posibilidad de devolver información al consumidor acerca de su consumo energético, con lo que puede contribuir hacia el uso eficiente de energía, potenciales ahorros energéticos y progresos al preservar el medio ambiente (Trejo-Guerrero, 2016). Sin embargo los datos de consumo recogidos pueden ser analizados utilizando técnicas de monitoreo de carga para deducir actividades de los consumidores. Las lecturas de los medidores permiten inferir patrones de comportamiento como el momento en que un cliente deja su hogar, enciende la lavadora o se va a la cama. Por esta razón, las soluciones de medición inteligente deberían proporcionar mecanismos para la preservación de la privacidad (Tonyali, Akkaya, Saputro, Uluagac & Nojoumian, 2017).

Por lo tanto, las amenazas típicas de privacidad incluyen, pero no se limitan a la determinación de pautas de comportamiento personal, la determinación de los aparatos específicos utilizados; y realizar la vigilancia en tiempo real (Tonyali, 2016). Por ende, es indispensable utilizar mecanismos de seguridad, que permitan resguardar la información de algún ciberataque, siendo la criptografía unos de los más utilizados, debido a que se encarga de ocultar los datos ante terceros, proporcionando confidencialidad mediante algún método de cifrado identificando fortalezas y debilidades en términos de su complejidad en la implementación, eficiencia, robustez y simplicidad. (Mogollon, 2007).

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 (Rajan & Saumitr, 2006). 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 (Jiménez, Flores, & González, 2015).

Para abordar el problema de seguridad (Li, Luo, & Liu, 2010), 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. Se emplea el cifrado parcialmente homomórfico y datos seguros como esquemas de ofuscación para evitar a fisgones de hacer inferencias acerca de la actividad de los consumidores (Saputro, 2014).

Siendo la clave de cifrado una representación de la información específica que se necesita para el buen funcionamiento de un sistema criptográfico, compuesta por lo general de varios parámetros que se utilizan para inicializar y operar el sistema de cifrado. La criptografía moderna se concentra en sistemas criptográficos que están protegidos contra diferentes ataques cibernéticos. Uno de los ataques más comunes es el ataque de fuerza bruta en el que se trataron todas las combinaciones posibles de la clave de cifrado (Radwan, AbdElHaleem, & Abd-El-Hafiz, 2016).

ISSN-2531-2952

La historia de la criptografía nos da pruebas de que puede ser difícil mantener en secreto los detalles de un algoritmo usado extensamente. Una clave suele ser más fácil de proteger, que todo un sistema de cifrado, y es más fácil de substituir si ha sido descubierta.

Por tanto, la seguridad de un sistema de cifrado descansa en la mayoría de los casos, en que la clave permanezca secreta. 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, 1983), sólo el mantener la clave en secreto proporciona seguridad. En cuanto al periodo de uso: una clave se vuelve más insegura cuanto mayor sea el tiempo que se ha estado utilizando, es por ello que debe renovarse con regularidad, aunque hayan sido generadas con la mayor aleatoriedad posible.

La criptografía ha sido aplicada en varios sectores críticos donde se requiere reforzar la seguridad cibernética. El sector de la energía eléctrica, se vuelve cada vez más vulnerable debido a que, en una red eléctrica inteligente además de la conexión con generación, transmisión, 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 ante la posibilidad cada vez mayor de ataques cibernéticos (Zeadally, Pathan, Alcaraz, & Badra, 2013).

Al realizar un cifrado, se dificulta o imposibilita a comprensión de la información a personas ajenas (Hennawy, Omar, & Kholaif, 2015). Y con ello se aumenta la entropía que se define como el desorden de un sistema, es decir, su grado de homogeneidad.

Shannon, denominado el padre de la teoría de la información en 1948, determina la entropía como la incertidumbre de una fuente de información. Mucha entropía indica gran impredecibilidad. 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 (Kumar, Abhishek, & Singh, 2015).

En este trabajo se propone el desarrollo de un algoritmo de cifrado simétrico ligero, para fortalecer la protección de la privacidad de los datos. El algoritmo se conforma de dos métodos combinados; mapeo logístico acoplado con generador congruencial lineal, con el objetivo de aplicarlo para cifrar una serie de datos de señal de consumo de energía eléctrica simulada. Se hacen pruebas estadísticas al criptograma, se validan y se obtienen resultados aceptables a través de la suite para generadores de números aleatorios y pseudoaleatorios del NIST.

Metodología

A continuación, se describen los métodos acoplados utilizados para el diseño del algoritmo de cifrado; donde se incluye generador congruencial lineal y mapeo logístico debido a sus características computacionales. Consiguiendo 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 averiguarla.

Generador Congruencial Lineal

La generación de números pseudo-aleatorios juega un papel crítico en gran número de aplicaciones tales como, simulaciones numéricas, las comunicaciones o la criptografía.

ISSN-2531-2952

Un generador de números pseudoaleatorios se define como un algoritmo 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 de pseudo-aleatorios producidos. En la práctica, la generación de números pseudo-aleatorios no es trivial y la calidad aleatoriedad de la secuencia producida puede ser esencial en la elección de la aplicación (François, Grosges, Barchiesi, & Erra, 2014).

Los generadores de números pseudoaleatorios son de vital importancia en muchas aplicaciones criptográficas para la generación de claves y códigos de acceso. Uno de los generadores más antiguos y sencillos es el generador de congruencia lineal, propuesto por D.H. Lehmer en 1949, que consiste en, a partir de un número inicial llamado semilla, generar una secuencia por recurrencia; cuya relación es:

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

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 es m-1, por otra parte, las secuencias producidas por un generador congruencial lineal son muy sensibles a cambios en sus parámetros, lo cual es una propiedad útil (Pareek, Patidar, & Sud, 2003).

Mapeo logístico

La aplicación logística ha sido usada como generador de números pseudo-aleatorios.

Para este fin en (Phatak, & Suresh, 1993), se han realizado ciertas pruebas estadísticas sobre las series de números obtenidas de este sistema dinámico discreto y se ha encontrado que cumplen satisfactoriamente y por tanto posee muchas de las propiedades requeridas por un generador de números pseudo-aleatorios.

El mapeo logístico, presenta una dinámica muy rica, y dependiendo del valor de un parámetro, se puede 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 la siguiente función (May, 1976):

$$x_{t+1} = \mu x_t(1 - x_t) \qquad (2)$$

Donde μ, es una constante, llamada parámetro de control, que determina el grado de no-linealidad del mapa, y xt, 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 x0. En el que la constante μ oscila 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 función (2): bajo los parámetros de μ y xt: cuando $0 <= \mu <= 4$, y $0 <= xt <= 1$; f es una parábola, la cual es iterada. $x_1 = f(x_0)$, $x_2 = f(x_1) = f_2(x_0)$... $x_t = f(x_t{-}1) = f_t(x_0)$, donde x_t, es la nueva iteración de x_0 y el conjunto de todas las iteraciones es el mapeo de f.

La función logística es interesante porque reúne, en un solo sistema unidimensional y dependiente solo de un parámetro, un abanico de comportamientos diversos para las trayectorias x_t, cuando se varía el valor de μ y/o x_t,

ISSN-2531-2952

Se dice que sus características dinámicas son universales en ese sentido. 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.

Experimentación

Se hace un acoplamiento del mapeo logístico con el generador congruencia lineal, dadas las características de ambos que al complementarse aumenta la impredecibilidad de la clave de cifrado, y se mejora la seguridad de la información para dificultar la intrusión al código.

Dentro de los sistemas discretos caóticos uno de los más utilizados para codificar información es el mapa logístico, esto se debe a que es muy sencillo, rápido y sensible a las condiciones iniciales y al parámetro de control (Mao, Chen, & Lian, 2004). El mapa logístico se define en la ecuación (2), 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 (Clark, 1995).

Como puede apreciarse en la figura 1 A, 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. Donde para garantizar la impredecibilidad de las secuencias, es necesario utilizar una semilla que se encuentre dentro de la zona en que el sistema se comporta de forma caótica. Por éste motivo se utilizarán los resultados obtenidos 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 garantice un comportamiento impredecible, como se observa en el rectángulo a la derecha en la figura 1B.

El exponente de Lyapunov cuantifica el grado de "sensibilidad a las condiciones iniciales" (es decir, la inestabilidad local en un espacio de estados) mediante la ecuación siguiente:

$$\lambda = \lim_{n\to\infty}\{\frac{1}{2}\sum_{i=0}^{n-1} ln|f'(x_i)|\} \quad (3)$$

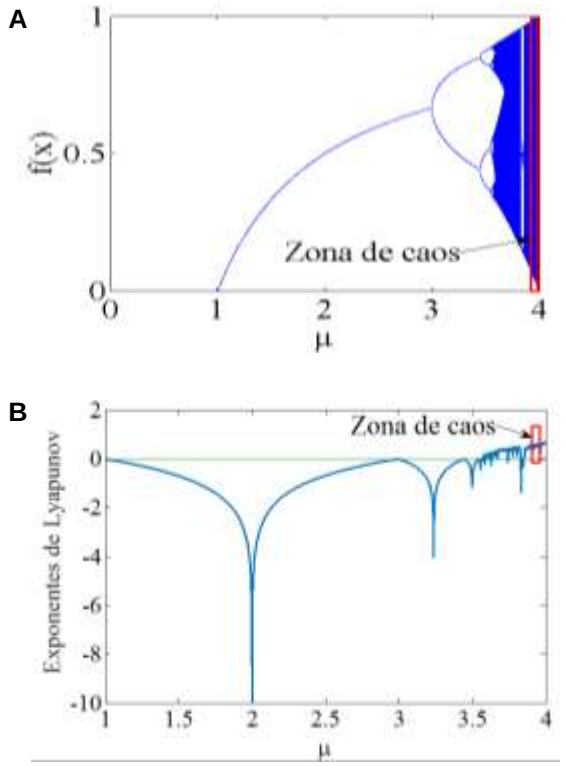

Figura 1 (A) Diagrama de bifurcación de mapeo logístico, (B) Diagrama exponentes de Lyapunov

Fuente: May, 1976.

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.

Con los parámetros y condiciones iniciales se generan series de números 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.

ISSN-2531-2952

Resultados experiemtales

Se propone un algoritmo para fortalecer la seguridad en datos generados por un prototipo 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 los métodos matemáticos antes mencionados, 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.

El diagrama de bloque de la figura 2, representa el esquema compacto del algoritmo propuesto que incluye los procesos y procedimientos que integran el cifrado completo, se ilustra la mezcla de las ecuaciones generadoras de secuencias pseudoaleatorias bajo la función de disyunción exclusiva Xor con el fin de que esta mezcla generada sea útil para obtener las subclaves que cifraran la información de la señal de consumo de energía eléctrica.

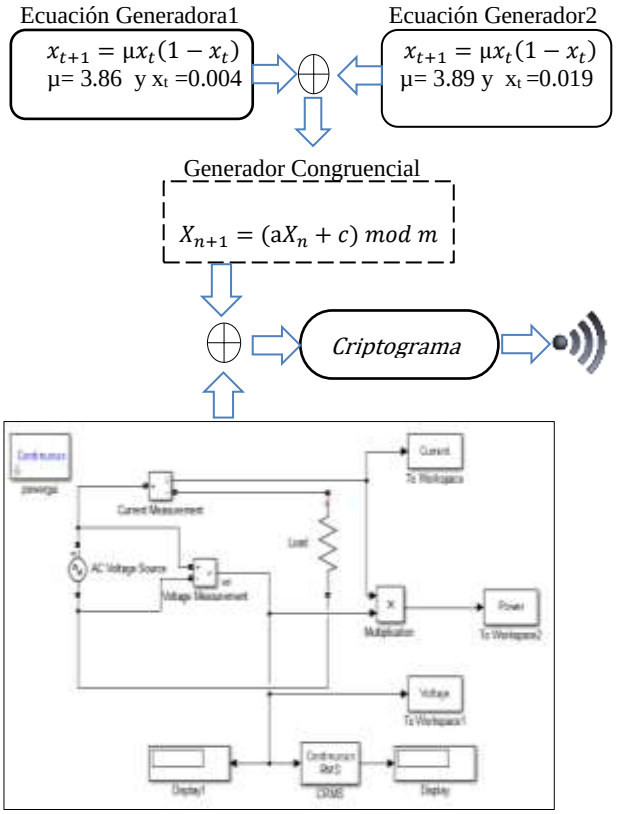

Figura 2 Diagrama de bloques del algoritmo de cifrado

Fuente: elaboración propia

El proceso de descifrado es muy similar al mostrado en la figura 2, no obstante en este caso la señal cifrada es utilizada para realizar la mezcla con la secuencias de los generadores pseudoaleatorios a través de la operación lógica Xor recuperando nuevamente la señal original. Vale la pena señalar que el sistema de generadores pseudoaleatorios utilizado para el descifrado, debe estar perfectamente sincronizado con las condiciones iniciales mencionadas anteriormente, para lograr el descifrado sin pérdida de datos.

ISSN-2531-2952

Evaluación del cifrado

Para evaluar el algoritmo de cifrado propuesto previamente, el cual está enfocado para trabajar con señales de energía eléctrica y datos provenientes de un medidor digital 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 3A, 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 las figuras 3 A y B 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, tendiendo a parecerse a una señal de ruido.

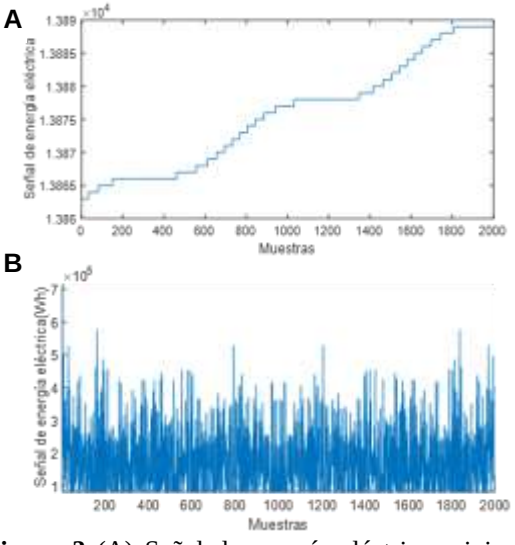

Figura 3 (A) Señal de energía eléctrica original. (B) Señal cifrada con el algoritmo propuesto

Fuente: elaboración propia

En la figura 3B, la señal cifrada; usando el algoritmo propuesto en esta sección. Utilizando como clave de cifrado la misma que para descifrado (simétrico), usando como semilla una serie de números impredecibles inútiles para un supuesto atacante.

La clave de cifrado es una representación de información específica que se necesita para el funcionamiento satisfactorio de un criptosistema. Por lo general, consiste en varios parámetros que se utilizan para inicializar y operar el criptosistema. La criptografía moderna se concentra en criptosistemas que están asegurados computacionalmente contra diferentes ataques. Uno de los ataques más comunes es el ataque de fuerza bruta, en el que se intentan todas las combinaciones posibles de la clave de cifrado. Por lo tanto, una clave de cifrado de longitud 128 bits o más se considera seguro contra ataques de fuerza bruta (Jimenez, 2015). Según el principio de Kerckhoff, la seguridad del algoritmo propuesto dependerá sólo del secreto de la clave utilizada en el proceso criptográfico empleado para ocultar la información sensible, y no en el secreto del algoritmo. En el algoritmo criptográfico propuesto, el espacio de clave es 2n, donde n es la longitud de la clave en bits. En este caso, n = 128, porque se utilizan dos generadores de números pseudoaleatorios y se supone que cada mapa caótico utiliza dos variables con una longitud de 64 bits.

Para evaluar el criptosistema se divide en dos categorías principales, la primera incluye las pruebas estadísticas: coeficientes de correlación de datos, análisis de histogramas y valores de entropía y, la segunda incluye las pruebas de sensibilidad: un cambio de bit en el cifrado clave y el error cuadrático medio (Kumar, Abhishek, & Singh, 2015).

ISSN-2531-2952

Pruebas estadísticas

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.

Con el fin de obtener medidas numéricas se calcula el coeficiente de correlación con la siguiente ecuación:

$$c = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad (4)$$

Donde, n es el número de elementos en los dos vectores adyacentes x y y. Para datos fuertemente cifrados, los coeficientes de correlación se deben aproximar a cero (Weisstein, 2016).

Los histogramas permiten representar de forma gráfica cómo se distribuyen los datos. En las figuras 4 A y B, 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.

Al comparar los histogramas de las figuras 4A y B, se puede observar 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.

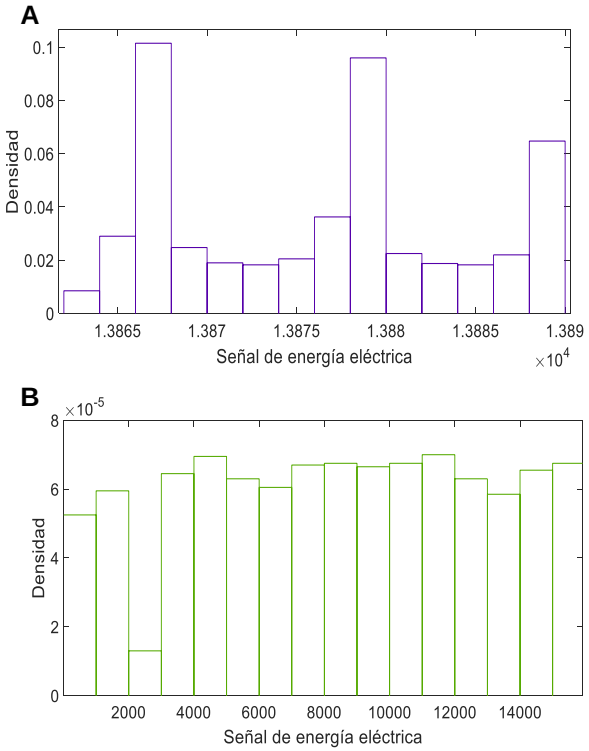

Gráfico 1 (A) Histograma de señal original (B) Histograma de señal cifrada

Fuente: elaboración propia

La entropía mide la incertidumbre de una fuente de información calculando la aleatoriedad de los datos, lo que permite evitar cualquier previsibilidad. La entropía está dado por:

$$H = \sum_{i=1}^{2^8} P(S_i)\log_2 P(S_i) \quad (5)$$

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 este. 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 (Kumar, Abhishek, & Singh, 2015).

Pruebas de sensibilidad

Los algoritmos fuertemente cifrados deben ser sensibles a cualquier pequeño cambio en los valores de entrada y producir una salida totalmente diferente. Cuantitativamente, las diferentes medidas se definen para la evaluación de los niveles de protección contra los ataques diferenciales (Jiménez-Flores, Flores, & González, 2015**)**. La figura 5, corresponde a señales descifradas con el algoritmo propuesto, habiendo modificado sólo un bit en la clave. En la figura 5A, se muestra la señal descifrada con un cambio de bit en la clave y se puede observar que el resultado es completamente diferente al esperado.

Se corrobora que la sensibilidad de clave fue satisfactoria debido a que un cambio de un bit en la clave de cifrado condujo a un comportamiento completamente diferente en el proceso descifrado. En este sentido, ahora se modifica un valor en el parámetro m (número primo suficientemente grande) del generador de subclaves y por tanto se obtiene una señal totalmente diferente a la que representa los datos de la señal original como se puede apreciar en la figura 5B.

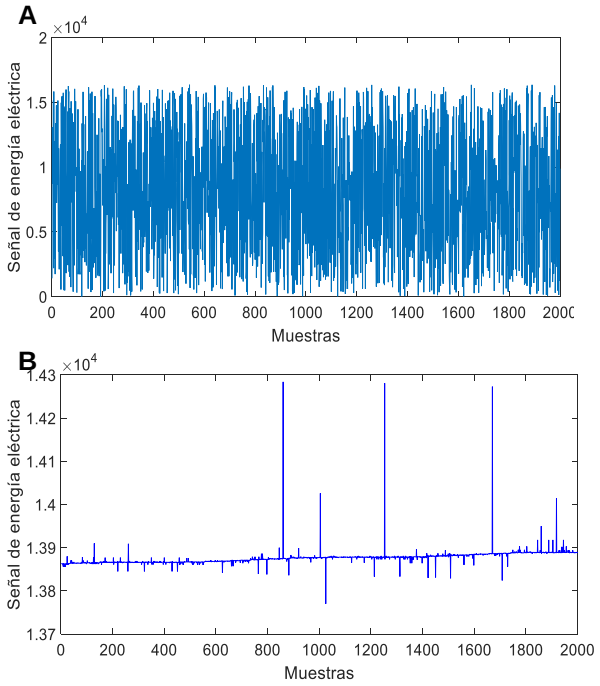

Figura 5 (A)Señal descifrada con cambio de un bit en la clave. (B)Señal descifrada con cambio en parámetro en generador de subclaves

Fuente: *elaboración propia*

Se manifiesta, que un buen proceso de cifrado muestra ser sensible a ligeros cambios en cualquiera de sus parámetros y, por lo tanto, un leve cambio en la clave o en alguno de los parámetros del generador de subclaves conduce a un comportamiento completamente diferente en el proceso de descifrado.

El error mide la variación entre la señal cifrada y la original, arrojando un valor de cero cuando no se efectúa variación en los parámetros. Esta sensibilidad se evaluó usando el error cuadrático medio, que indica hasta qué punto los datos descifrados difieren de los originales (Yamamoto, 1976)). El error cuadrático medio es calculado con la siguiente ecuación:

$$ECM = \frac{1}{n}\sum_{i=1}^{n}(\hat{Y}_i - Y_i)^2 \qquad (6)$$

Donde $\hat{Y}$, es un vector de n predicciones y Y, es el vector de los valores originales.

ISSN-2531-2952

Para la verificación de la aplicación de cifrado y descifrado al usar adecuadamente el algoritmo y la clave, la ecuación arroja un valor de cero. Lo que permite corroborar que la señal original es idéntica a la señal recuperada después del proceso de descifrado.

Para mostrar que los resultados simulados demuestran viabilidad y seguridad del algoritmo propuesto, se emplearon las pruebas estadísticas; 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 1, se muestran los resultados de algunas de las pruebas estadísticas aplicadas al criptosistema después del proceso de cifrado y los valores esperados en base a la evaluación aplicada.

Estadística	Obtenido	Esperado
Coeficiente de correlación	0.0022	0
Entropía	7.9045	8
Error cuadrado medio	0	0

Tabla 1 Concentrado de evaluaciones estadísticas

Fuente: *elaboración propia*

Validación del criptosistema usando el NIST Test Suite para Generadores de Números Aleatorios y Pseudoaleatorios 800-22rev1a **(**Bassham, L, Rukhin A, Soto J, Nechvatal, J, Smid M, Leigh S, et al., 2010).

La suite NIST evalúa la presencia de un patrón e indica si la secuencia es o no aleatoria. En cada prueba, se calcula un valor de P con un nivel de significancia de $\alpha = 1\%$. Un valor P mayor que α significa que la secuencia es aleatoria con un nivel de confianza del 99%.

El rendimiento estadístico del criptosistema se evaluó utilizando un conjunto de pruebas estadísticas con 1 Mbit, bajo un intervalo de parámetros en μ [3.86-4], y un intervalo de condición inicial en x_t [0-1]. Bajo estas condiciones, el 75% de las pruebas experimentales realizadas son satisfactorias debido a las ventanas presentes en el diagrama de bifurcación. Cada valor de P correspondiente a una prueba particular con una significancia del 0.01 se presenta en la tabla 2 e indica la relación de secuencia de 1 Mbit que pasa cada una de las 15 pruebas específicas.

Prueba	**Valor P obtenido**	**Conclusión**
approximate entropy	0.809791	Aceptado
block frequency	0.491789	Aceptado
cumulative sums	0.412876	Aceptado
cumulative sums	0.312923	Aceptado
fft	0.804313	Aceptado
frecuency	0.406539	Aceptado
linear complexity	0.750305	Aceptado
longest runs of ones	0.504821	Aceptado
nonoverlapping template	0.5094025	Aceptado
overlapping template	0.313653	Aceptado
rank	0.885113	Aceptado
runs	0.436975	Aceptado
nonperiodic templates	0.5094025	Aceptado
serial	0.381633	Aceptado
universal statistical	0.877240	Aceptado

Table 2 Evaluación del criptograma a través de la suite NIST

Fuente: *elaboración propia*

Los resultados mostrados en las tablas 1 y 2 demuestran que el algoritmo de cifrado propuesto presenta buenas propiedades de aleatoriedad y, por consiguiente, buenas características criptográficas.

ISSN-2531-2952

Agradecimiento

Este trabajo es apoyado por el Consejo Nacional de Ciencia y Tecnología (CONACYT) para el número de beca 408093

Conclusiones

En este trabajo se propone un algoritmo de cifrado en el que se implementa una técnica que combina el comportamiento impredecible de una función logística, empleada para obtener la semilla que origina una subclave, con un generador de números pseudoaleatorios, dada la combinación de generación caótica y no caótica se produce un algoritmo de cifrado rápido y seguro. El algoritmo se implementa en Matlab para evaluar, tanto el proceso de cifrado y reconstrucción de una señal, como para evaluar el nivel de aleatoriedad, usando diferentes herramientas estadísticas.

Las pruebas estadísticas aplicadas al criptograma, dan como resultado que los datos cifrados provienen de secuencias con alto grado de aleatoriedad, lo que se traduce en un alto nivel de seguridad, dado que el proceso de manipulación conserva su entropía natural, por tanto la hace poco vulnerable a posibles ataques externos. Por otra parte también se comprueba la sensibilidad del algoritmo a ligeros cambios en la clave de cifrado y en los parámetros de generación de subclaves. En este sentido, solo es posible recuperar los datos originales (descifrado) con las respectivas claves de cifrado que son generadas por el propio sistema. Y es asi como se preserva la privacidad para reportar el consumo de energía de los medidores inteligentes cifrando los datos que estos dispositivos procesan.

Referencias

Bassham, L, Rukhin A, Soto J, Nechvatal, J, Smid M, Leigh S, et al.:(2010). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [Internet]. NIST (2010).

François, M., Grosges, T., Barchiesi, D. & Erra, R. (2014). Pseudo-random number generator based on mixing of three chaotic maps. Communications in Nonlinear *Science and Numerical Simulation,* 19(4), pp.887-895.

Hennawy, H., Omar, A. & Kholaif, S. (2015). LEA: Link Encryption Algorithm Proposed Stream Cipher Algorithm.Ain *Shams Engineering Journal*, 6(1), pp.57-65.

Jiménez, M., Flores, F. & González, G. (2015). System for Information Encryption Implementing Several Chaotic Orbits.Ingeniería, *Investigación y Tecnología,* 16(3), 335-343.

Kerckhoffs, A. (1983). La cryptographie militaire, *Journal des sciences militaires*, 9, 161-191.

Kumar, S., Abhishek, K. and Singh, M. (2015). Accessing Relevant and Accurate Information using Entropy. *Procedia Computer Science*, 54, 449-455.

Lehmer, D. H. (1949). Mathematical methods in large-scale computing units. 2 ndsymposium on large-scale digital calculating machinery, *Cambridge, massachussets*, 141-146.

Li, F., Luo B. & Liu P. (2010). Secure information aggregation for smart grids using homomorphic encryption. In: 2010 First IEEE international conference on Smart Grid Communications *(SmartGridComm), Gaithersburg, Mayryland, USA.* 327–332.

Mao, y., Chen, g. & Lian, s. (2004). A novel fast image encryption scheme based on 3d chaotic baker maps. *International Journal of Bifurcation and Chaos*, 14(10), 3613-3624.

May, R. (1976). Simple Mathematical Models with Very Complicated Dynamics, *Nature*, 261, 459-467.

ISSN-2531-2952

Moreno-Dzul, Julio, Álvarez-Ibarra, Maricela, Silva-Dzib, Ismael & Arceo-Díaz, Rocío. (2016).*Sistema de Gestión de demanda eléctrica basada en la Web.* Revista de Aplicaciones de la Ingeniería, 3-8: 65-76

Mogollon, M. (2007). Cryptography and security services: mechanisms and applications. *Hershey, PA: CyberTech*, 51-97

Pavanello, D., Zaaiman, W., Colli, A., Heiser, J. & Smith, S. (2015). Statistical functions and relevant correlation coefficients of clearness index. *Journal of Atmospheric and Solar-Terrestrial Physics*, 130-131,142-150.

Phatak, SC. Suresh Rao S. (1993). Logistic Map: A Possible Random Number Generator,*http://arXiv.org/abs/condmat/9310 004v1*

Radwan, A., AbdElHaleem, S. & Abd-El-Hafiz S. (2016). Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. Journal of Advanced Research. 7(2), 193–208.

Rajan, B. & Saumitr, P. (2006). A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system. *IEEE Transactions on circuits and system* (4) 1 - 53

Shannon, C. (1948). A mathematical theory of communication. *Bell Syst. Tech. J.*, 27, 379–423, 623–656

Saputro, N. & Akkaya K. (2014).On preserving user privacy in smart grid advanced metering infrastructure applications.Secur. Commun. Netw. 7 (1), 206–220

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A., & Nojoumian, M. (2017). *Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems*. Future Generation Computer Systems.

Tonyali, S. Cakmak, O. Akkaya, K. Mahmoud, M. & Guvenc. I. (2016). Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks.IEEE Internet Things J., 3 (5), 709–719

Trejo-Guerrero, César, Flores-Ruiz, Juan, Marroquín-de Jesus, Ángel & JuárezSantiago, Brenda. (2016). *Fotovolt, aplicación móvil, para el dimensionamiento de sistemas fotovoltaicos en la modalidad tipo isla e interconectados a la red.* Revista de Sistemas Computacionales y TIC'S, 2-6: 12-21

Weisstein, E. (2016).Pearson's Skewness Coefficients. *From MathWorld-A Wolfram*
Zeadally, S., Pathan, A. S. K., Alcaraz, C., & Badra, M. (2013). Towards privacy protection in smart grid. *Wireless personal communications*, 73(1), 23-50.

ISSN-2531-2952