



UNIVERSIDAD DEL PAPALOAPAN

CAMPUS LOMA BONITA

INGENIERÍA EN MECATRÓNICA

**COMUNICACIÓN SEGURA EMPLEANDO CAOS
EN DOS DISPOSITIVOS**

TESIS PROFESIONAL PARA OBTENER EL TÍTULO DE:
INGENIERO EN MECATRÓNICA

PRESENTA:

JESÚS REYNALDO REYES RIOS

DIRECTOR DE TESIS:

DR. MAURO SÁNCHEZ SÁNCHEZ

LOMA BONITA, OAXACA, MÉXICO

2024



Universidad del Papaloapan

FECHA:	15 de Febrero del 2024
ÁREA:	Vice-Rectoría Académica
OFICIO NÚMERO:	UNPA/VRA/041/2024
ASUNTO:	Autorización de Impresión de tesis.

C. JESÚS REYNALDO REYES RÍOS
P R E S E N T E:

En base al artículo 120 del reglamento de alumnos, por medio de la presente se aprueba la impresión de la tesis titulada **“Comunicación segura empleando Caos en Dos Dispositivos”** así como la programación del examen profesional bajo la dirección del Dr. Mauro Sánchez Sánchez.

Sin más por el momento aprovecho la ocasión para enviarle un cordial saludo.

Atentamente.
terra ubérrima, mens aperta
Bou Lo-tama, chi jí jú

MC. HÉCTOR LÓPEZ ARJONA
Vice-Rector Académico.



C.c.p. M.C. Luis Alberto Hernández Zuccolotto. Jefe de Carrera de la Ing. En Mecatrónica
C.c.p. L.P. Yesenia Barrientos Arenal. Jefa del Departamento de Servicios Escolares
C.c.p. Dr. Mauro Sánchez Sánchez. Directora de Tesis.
C.c.p. Archivo.

OAXACA



UNIVERSIDAD DEL PAPALOAPAN

Campus Loma Bonita

Oficio: IMEC-24-012
Loma Bonita, Oaxaca, a 13 de febrero de 2024

M.E. Yesenia Barrientos Arenal
Jefa del Departamento de Servicios Escolares
PRESENTE

Mediante la presente, le informo que la jefatura de carrera a mi cargo, con visto bueno de la Vice-Rectoría Académica, ha designado a los siguientes profesores como sinodales para examen profesional del **C. Jesús Reynaldo Reyes Ríos**, quien defenderá su trabajo de tesis titulado **“Comunicación Segura Empleando Caos en Dos Dispositivos”**, para obtener el título de Licenciado en Ingeniería en Mecatrónica.

Titulares:

Presidente: **Dr. Francisco Gutiérrez Zainos**
Secretario: **Dr. Hiram Netzahualcóyotl García Lozano**
Vocal: **Dr. Mauro Sánchez Sánchez**

Suplentes:

M.C. Luis Alberto Hernández Zuccolotto
Dr. Jesús Santiaguillo Salinas



Atentamente
terra uberrima, mens aperta
Bou lo-tama, chi, ji, jú

M.C. Luis Alberto Hernández Zuccolotto
Jefe de Carrera de Ingeniería en
Mecatrónica



M.C. Héctor López Arjona
Vice-Rector Académico

c.c.p. M.C. Héctor López Arjona. Vice-Rector académico. Para su conocimiento
c.c.p. Archivo

Agradecimientos

*A mis padres por el apoyo incondicional
que me brindan y por confiar en mí.*

*A toda mi familia por lo mucho que me
brindan.*

*A mi director y sinodales de tesis, por
darme el apoyo necesario para el
desarrollo de este proyecto.*

*A todas las personas que me brindaron su colaboración, sus conocimientos, su
ayuda y sobre todo su amistad.*

Resumen

En este trabajo se presenta el desarrollo de un sistema empleado para comunicación segura, en el cual, para cumplir este objetivo principal, se utilizará como método de encriptación un sistema caótico, específicamente el circuito caótico de Chua. En este caso la configuración del circuito de Chua es para dos enrollamientos, y se obtiene a partir del modelo matemático basado en funciones no lineales saturadas (SNLF). La dinámica del circuito de Chua en SNLF se emula por medio de amplificadores operacionales y se desarrolla en simulación numérica utilizando el software de Matlab/ Simulink®, en el cual se utilizan dos circuitos, uno emisor y otro receptor, sincronizados en una transmisión unidireccional. Se presentan los resultados de simulación más relevantes, entre los cuales se pueden mencionar, las señales caóticas y los diagramas de fase del circuito, el análisis de que el sistema puede presentar aleatoriedad y la cuantificación de los exponentes de Lyapunov como una medida de caos, así como también se muestran la sincronización maestro-esclavo y encriptación de la comunicación.

Palabras clave: circuito Chua, caos, sincronización, encriptación, comunicación.

Abstract

This work presents the development of a system used for secure communication, in which, to meet this main objective, a chaotic system, specifically Chua's chaotic circuit, will be used as an encryption method. In this case, the Chua circuit configuration is for two scroll, and is obtained from the mathematical model based on saturated nonlinear functions (SNLF). The dynamics of the Chua circuit in SNLF is emulated by means of operational amplifiers and is developed in numerical simulation using Matlab/Simulink® software, in which two circuits are used, one emitter and one receiver, synchronized in a unidirectional transmission. The most relevant simulation results are presented, among which we can mention the chaotic signals and the phase diagrams of the circuit, the analysis that the system can present randomness and the quantification of the Lyapunov exponents as a measure of chaos, as well as master-slave synchronization and communication encryption are also shown.

Keywords: Chua circuit, chaos, synchronization, encryption, communication.

Contenido

1. Capítulo I: Introducción General	9
1.1. Introducción	9
1.2. Objetivo general.....	11
1.3. Objetivos específicos	11
2. Capítulo II: Marco de referencia.....	12
2.1. Origen del caos	12
2.2. Entropía.....	12
2.3. Exponentes de Lyapunov.....	13
2.4. Dimensión Kaplan-Yorke.....	15
2.5. Dinámica caótica.....	16
2.6. Atractores extraños.....	18
2.7. Sistemas caóticos en tiempo continuo y en tiempo discreto.....	20
2.7.1.Sistemas caóticos en tiempo continuo.....	20
2.7.2.Sistemas caóticos en tiempo discreto	20
2.8. Condiciones necesarias para sistemas caóticos	21
2.9. Sincronización de sistemas caóticos	22
2.10.	A
plicaciones de los sistemas caóticos	23
3. Capítulo III: Osciladores Caóticos.....	25
3.1. Características de los osciladores caóticos	25
3.2. Oscilador caótico de Chua.....	25
3.2.1.Ecuaciones normalizadas del circuito de Chua.....	27
3.3. Modelado de osciladores caóticos basados SNLF	31
3.4. Oscilador Caótico de Chua basado en SNLF	33
3.5. Oscilador caótico de Chua con amplificadores operacionales.....	38
3.5.1.Modelo del inductor por medio de OpAmp.....	38
3.5.2.Modelo del diodo de Chua por medio de OpAmp.....	40

3.5.3.Simulación de la implementación del diodo de Chua y el inductor emulados con OpAmp's	43
4. Capítulo IV: Sincronización y encriptación con circuito caótico.....	47
4.1. Simulación del circuito caótico de Chua basado en funciones no lineales saturadas.	47
4.2. Aleatoriedad.....	52
4.2.1.Teorema de la frecuencia.	55
4.2.2.Teorema del Monobit.	57
4.3. Teorema de exponentes de Lyapunov.....	58
4.3.1.Variación en la condición inicial de un solo estado.....	58
4.3.2.Variación en la condición inicial de los tres estados del sistema.	59
4.4. Sincronización del circuito caótico de Chua	60
4.4.1.Acoplamiento unidireccional.....	61
4.4.2.Acoplamiento bidireccional	62
4.4.3.Sincronización en dos circuitos de Chua	63
4.5. Encriptación de información usando caos	67
4.5.1.Simulación 1, condiciones iniciales en receptor iguales a cero.	68
4.5.2.Simulación 2, condiciones iniciales en el receptor cercanas al del emisor	69
5. Capítulo V: Conclusiones	70
6. Anexos	74

Índice de figuras

Figura 1. Esquema de un sistema de comunicación seguro.....	10
Figura 2. Sensibilidad a las condiciones iniciales.....	16
Figura 3 Atractor de Lorenz.....	17
Figura 4 Circuito de Chua.	25
Figura 5. Respuesta característica del diodo de Chua.....	26
Figura 6. Respuesta de los estados del circuito caótico de Chua.	29
Figura 7. Espacio de fase del circuito caótico de Chua.	30
Figura 8. Atractor del circuito caótico de Chua.....	31
Figura 9 Función saturada desestabilizante de una SNLF.....	34
Figura 10. Respuesta del circuito caótico de Chua en SNLF.....	36
Figura 11. Espacio de fase, basado en SNLF.....	37
Figura 12. Atractor del circuito de Chua basado en SNLF.....	38
Figura 13. Convertidor de impedancias genérico (GIC).....	39
Figura 14. Esquema representativo del diodo de Chua con OpAmp.....	40
Figura 15. Respuesta del diodo de Chua emulado con OpAmp.....	42
Figura 16. Respuesta de estados del circuito de Chua.....	44
Figura 17. Espacios de fases.....	45
Figura 18. Atractor caótico de Chua, L y Nd emulado con OpAmp's.....	46
Figura 19. Esquema electrónico del circuito caótico de Chua implementado con OpAmps.....	47
Figura 20. Estado "X" del circuito eléctrico.....	49
Figura 21. Estado "Y" del circuito Eléctrico.....	49
Figura 22. Estado "Z del circuito eléctrico".....	50
Figura 23. Espacio de fase "XY".....	50
Figura 24. Espacio de fase "XZ".....	51
Figura 25. Espacio de fase "YZ".....	51
Figura 26. Atractor de Chua basado en SNLF implementado con OpAmps.....	52
Figura 27. Esquema eléctrico para generación de secuencia de bits.....	53

Figura 28. Umbrales U1, U2 en señal X para generación de bits.	53
Figura 29. Generación de bits.	54
Figura 30. Secuencia de bits generados del estado X.	55
Figura 31. Resultado del test de Frecuencia.	56
Figura 32. Acoplamiento unidireccional.	61
Figura 33. Acoplamiento bidireccional.	62
Figura 34. Graficas de error en la sincronización en dos circuitos de Chua.	64
Figura 35, Graficas de error en la sincronización en dos circuitos de Chua condiciones iniciales cercanas.	65
Figura 36. Señales de dos circuitos de Chua sincronizados.	66
Figura 37. Diagrama de bloques para comunicación segura.	67
Figura 38. resultados de simulación de la comunicación 1.	68
Figura 39. resultados de simulación de la comunicación 2.	69

Índice de tablas

Tabla 1. Parámetros y elementos para simulación 1. Variables de estado.	28
Tabla 2. Parámetros y elementos para simulación 2. SNLF.	35
Tabla 3. Elementos para simulación del diodo de Chua.	42
Tabla 4. Parámetros para simulación 3.	43
Tabla 5. Parámetros para simulación.	48
Tabla 6. Cálculo 1 de los exponentes de Lyapunov para cada variable.	59
Tabla 7. Cálculo 2 de los exponentes de Lyapunov para cada variable.	60

Capítulo I: Introducción General

Introducción

En el presente, la comunicación desempeña un papel fundamental en la vida humana, ya sea en el ámbito personal o profesional, la información fluye constantemente a través de diversos dispositivos y medios, facilitando la interacción y la colaboración. Sin embargo, la conectividad también ha dado lugar a un problema crítico: la seguridad de la comunicación.

La seguridad de la comunicación se refiere a la protección de la información transmitida entre dos o más puntos de manera que solo las partes autorizadas puedan acceder a ella.

En este contexto surge la necesidad de abordar esta problemática, haciendo uso de una alternativa a los sistemas de encriptación convencional, los sistemas caóticos. Estos sistemas han recibido importante atención en los recientes años, debido a sus características intrínsecas, esto es, una complicada evolución, alta aleatoriedad y un alto rango dinámico, lo cual resulta útil en la encriptación de los sistemas de comunicación.

En este trabajo se realiza la simulación de un sistema de comunicación de tipo unidireccional emisor-receptor, donde la información transmitida es encriptada por medio de un sistema caótico. Para ello el sistema caótico es desarrollado con base en funciones no lineales saturadas (SNLF de sus siglas en inglés) las cuales describen el comportamiento caótico de un circuito de Chua.

La comunicación se realiza de la siguiente manera, la información a enviar es sumada (modulada) a la señal seleccionada para la encriptación del sistema, el resultado es una nueva señal, "Señal encriptada". Esta señal se envía por medio de un módulo de comunicación inalámbrica al circuito receptor. Una vez recibida,

para que exista la descryptación, el emisor y el receptor deben estar sincronizados, es decir, deben contar con la misma dinámica en el mismo tiempo. En este caso se procede a restar (demodular) la señal encriptada a la generada por el circuito caótico de Chua-receptor, obteniendo como resultado la información original, ver Figura 1.

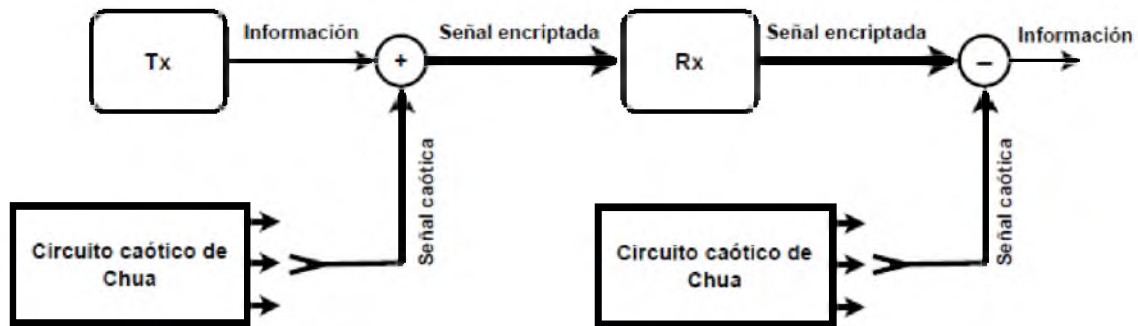


Figura 1. Esquema de un sistema de comunicación seguro.

Hacer uso de los sistemas caóticos como método de encriptación en los sistemas de comunicación es algo que se ha estudiado en los últimos años y sigue en desarrollo. Este trabajo permite el entendimiento necesario para poder llevar a cabo un método de encriptación basado en sistemas caóticos.

Este trabajo está estructurado de la siguiente manera, en el capítulo I, se presenta la introducción de manera general, expresando la idea de una posible solución en la problemática de las comunicaciones seguras. En este mismo capítulo se introducen los objetivos a cumplir. En el capítulo II se abordan los temas necesarios para el desarrollo del trabajo y en el capítulo III se analiza a detalle el oscilador caótico de Chua y la validación de la SNLF por medio de simulación. En el capítulo IV se desarrolla una simulación del circuito eléctrico equivalente al circuito caótico de Chua basado en SNLF. En este capítulo se presentan dos pruebas para validar que el sistema presente aleatoriedad. Además, por medio del cálculo de los exponentes de Lyapunov, se determina si el sistema es sensible a las condiciones iniciales (caótico). Para finalizar el capítulo, se realizan simulaciones del sistema de comunicación, en estas simulaciones se varían los

parámetros de las condiciones iniciales en la sincronización y se muestran los resultados. Por último, en el capítulo V, se mencionan las conclusiones específicas, generales y observaciones del trabajo, así mismo se plantearán futuros trabajos. Un apartado adicional al final de la tesis consta de los apéndices desarrollados en el trabajo.

Objetivo general

- ❖ Analizar y diseñar un sistema caótico para aplicaciones en la transmisión de información encriptada en un sistema de comunicación electrónica.

Objetivos específicos

1. Estudiar y conocer el funcionamiento del caos en los sistemas dinámicos.
2. Analizar el funcionamiento del oscilador caótico de Chua.
3. Desarrollar el oscilador caótico de Chua por medio de funciones no lineales saturadas (SNLF).
4. Simular el circuito del oscilador caótico de Chua basado en SNLF con amplificadores operacionales.
5. Comprobar la aleatoriedad del circuito electrónico y cuantificar el valor de los exponentes de Lyapunov.
6. Realizar una simulación del sistema completo.

Capítulo II: Marco de referencia

Origen del caos

El estudio del caos se deriva de los sistemas dinámicos. Un sistema dinámico es un sistema que cambia con el tiempo, y el caos se presenta en forma natural en diversos sistemas, por ejemplo: en el humo, agua, clima, entre otros. Para describir este comportamiento se han utilizado ecuaciones diferenciales. Un sistema dinámico se dice que tiene un comportamiento caótico cuando cumplen una serie de requisitos como por ejemplo de estar representado por al menos tres ecuaciones diferenciales acopladas entre sí, y que una de esas tres ecuaciones sea no lineal, ser muy sensibles a las condiciones iniciales entre otras. En la teoría del caos, la sensibilidad a las condiciones iniciales implica que pequeñas variaciones en las condiciones iniciales llevarán a resultados completamente diferentes con el tiempo [1]. Uno de los pioneros en este campo fue el matemático y meteorólogo Edward Lorenz, quien en la década de los 60's descubrió que pequeñas variaciones en los datos de entrada en un modelo matemático de predicción del clima pueden tener un impacto significativo en los resultados. Esto llevó al desarrollo de la teoría del caos. Esta teoría es fuente de recientes investigaciones y ha sido aplicada en distintas ramas de la tecnología en particular, las comunicaciones encriptadas. En aplicaciones de tecnología de la información un parámetro empleado para medir el caos es la entropía, la cual se describe a continuación.

Entropía

La entropía se refiere a la medida de incertidumbre o desorden en un sistema. En la teoría de la información, la entropía se utiliza para cuantificar la cantidad de información contenida en una fuente de datos. Se calcula a partir de la

probabilidad de ocurrencia de los diferentes símbolos o eventos en la fuente. Si todos los eventos son igualmente probables, la entropía es máxima, lo que indica que la fuente es muy incierta y contiene una gran cantidad de información. Por el contrario, si un evento es mucho más probable que los demás, la entropía será baja, lo que indica que la fuente es más predecible y contiene menos información [2].

Es importante destacar que la entropía no está limitada a un contexto específico y se utiliza en diversas ramas de la ciencia y las matemáticas para medir el desorden, la incertidumbre o la falta de información en un sistema.

La entropía no es la única característica utilizada para describir los sistemas caóticos. En un sistema dinámico, descrito por ecuaciones diferenciales, se tienen los exponentes de Lyapunov. En la siguiente sección se hace una breve descripción de tales exponentes.

Exponentes de Lyapunov

Los exponentes de Lyapunov son una herramienta matemática utilizada en la teoría del caos para caracterizar la sensibilidad a las condiciones iniciales en un sistema dinámico. Estos exponentes proporcionan información sobre cómo se amplifican o se atenúan las pequeñas perturbaciones en un sistema a lo largo del tiempo.

La evolución en el tiempo de un sistema dinámico depende directamente del conjunto de condiciones iniciales. Las trayectorias del sistema, asociadas a tales condiciones iniciales, divergen o convergen dependiendo de la naturaleza del sistema. Los exponentes de Lyapunov cuantifican esta divergencia o convergencia.

Para un sistema dinámico de dimensiones finitas, como un sistema de ecuaciones diferenciales ordinarias, los exponentes de Lyapunov se definen en términos de

las tasas de crecimiento de las perturbaciones. Supongamos que tenemos un sistema dinámico descrito por un conjunto de tres ecuaciones de la forma:

$$\frac{dx}{dt} = f(x) \quad (1)$$

Donde x es un vector que representa las variables del sistema y $f(x)$ es la función que describe la evolución del sistema.

Los exponentes de Lyapunov se calculan evaluando cómo las perturbaciones evolucionan a lo largo del tiempo, en relación con la distancia entre las condiciones iniciales. Si consideramos una perturbación inicial $\delta x(0)$ en el punto $x(0)$, la evolución de esta perturbación puede describirse como:

$$\delta x(t) = M(t)\delta x(0) \quad (2)$$

donde $M(t)$ es la matriz jacobiana que relaciona las perturbaciones en el tiempo t con las perturbaciones iniciales.

Los exponentes de Lyapunov se definen como los límites de la tasa de crecimiento promedio de las perturbaciones a medida que el tiempo tiende a infinito. Los N exponentes de Lyapunov, $\lambda_1, \lambda_2, \dots, \lambda_N$, se calculan de la siguiente manera:

$$\lambda_i = \lim(t \rightarrow \infty) \frac{1}{t} \ln ||M(t)e_i|| \quad (3)$$

Donde e_i es un vector unitario en la dirección de una perturbación inicial aleatoria.

Los exponentes de Lyapunov proporcionan información sobre la sensibilidad del sistema a las condiciones iniciales. Si alguno de los exponentes de Lyapunov es positivo, indica que las perturbaciones se amplifican exponencialmente con el tiempo, lo que implica un comportamiento caótico en el sistema. Por otro lado, si todos los exponentes de Lyapunov son negativos, las perturbaciones se atenúan con el tiempo, lo que implica un comportamiento estable o convergente en el sistema.

Es importante tener en cuenta que el cálculo de los exponentes de Lyapunov puede ser computacionalmente exigente y depende de la forma específica de las ecuaciones dinámicas del sistema. Además, en sistemas de dimensión infinita o sistemas estocásticos, se requieren métodos más avanzados para calcular los exponentes de Lyapunov [3]. La dimensión de Kaplan-Yorke utiliza los exponentes de Lyapunov para determinar la capacidad de un sistema caótico y predecir su comportamiento futuro. A continuación, se describe este término.

Dimensión Kaplan-Yorke

La dimensión de Kaplan-Yorke, también conocida como dimensión de capacidad de predicción o dimensión de Lyapunov. Fue propuesta por David Ruelle y Floris Takens en 1971, y posteriormente desarrollada por Marvin Kaplan y John Yorke en 1979.

La dimensión de Kaplan-Yorke caracteriza la capacidad de un sistema caótico para predecir su comportamiento futuro. Cuanto mayor sea la dimensión de Kaplan-Yorke, más complejo y caótico será el sistema, lo que implicará una mayor dificultad para realizar predicciones precisas a largo plazo.

$$d_k = j + \frac{\lambda_1 + \lambda_2 + \dots + \lambda_j}{|\lambda_{j+1}|} \quad (4)$$

Donde, λ_i con $i = 1, 2, \dots, j, \dots, n$ es el espectro de Lyapunov y j es el índice del menor exponente de Lyapunov que cumple $\lambda_1 \geq 0$

Para calcular la dimensión de Kaplan-Yorke, se utiliza la teoría de los exponentes de Lyapunov. Estos exponentes miden las tasas de divergencia o convergencia de las trayectorias cercanas en el espacio de fase del sistema dinámico. La dimensión de Kaplan-Yorke se define como la suma de los exponentes de Lyapunov positivos más grandes [4].

Dinámica caótica

La dinámica caótica, también conocida como caos determinista, es un comportamiento característico de ciertos sistemas dinámicos no lineales, en los cuales pequeñas variaciones en las condiciones iniciales pueden llevar a resultados muy diferentes a medida que el sistema evoluciona en el tiempo, lo que significa que incluso pequeñas perturbaciones pueden dar lugar a trayectorias completamente diferentes.

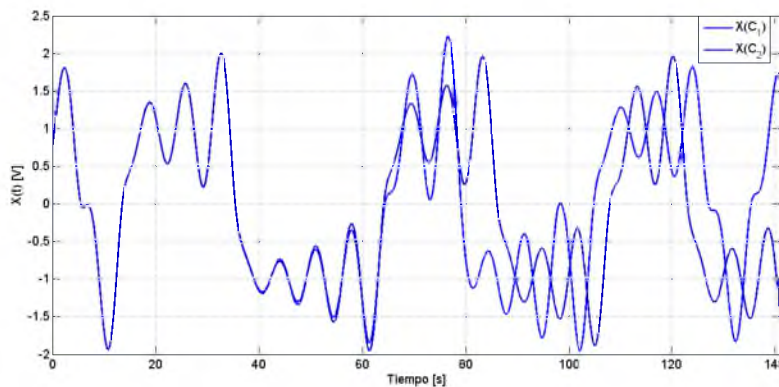


Figura 2. Sensibilidad a las condiciones iniciales.

En la Figura 2, se observa lo que se llama sensibilidad a las condiciones iniciales. Aquí las dos señales pertenecen a una de las variables de un sistema caótico. En estas señales se cambia una milésima en la condición inicial, es decir, para una la condición inicial es $C_1=0.75$ y para la otra la condición inicial es $C_2=0.749$. Se observa que conforme el tiempo crece las señales se separan.

En un sistema caótico, aunque las ecuaciones que describen su evolución son deterministas y no involucran aleatoriedad, el comportamiento a largo plazo parece ser impredecible e irregular, ver Figura 2. Esto se debe a que en este tipo de caos se amplifican exponencialmente de pequeñas perturbaciones, lo que hace que las trayectorias se separen rápidamente y en algunos casos se vuelvan incontrolables.

Un ejemplo clásico de un sistema caótico es el “Atractor de Lorenz”, Figura 3. Este atractor es solución del sistema de ecuaciones diferenciales ordinarias propuesto por Edward Lorenz en 1963 para describir la convección atmosférica. Este sistema exhibe un comportamiento caótico y muestra propiedades interesantes, como la existencia de estructuras fractales en el espacio de fase.

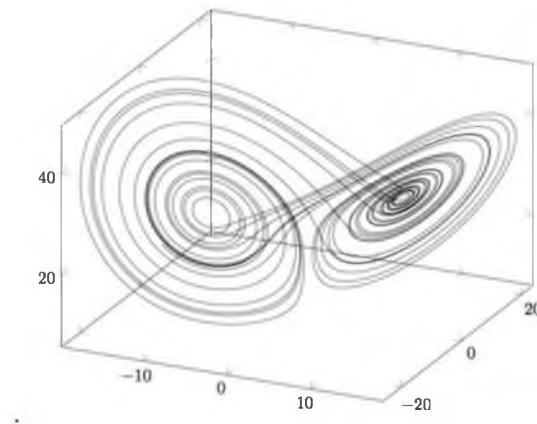


Figura 3 Atractor de Lorenz.

El estudio del caos determinista ha demostrado ser relevante en muchos campos, como la física, las matemáticas, la biología, la química y la economía, entre otros. La dinámica caótica tiene aplicaciones como la criptografía, donde se utiliza la sensibilidad a las condiciones iniciales para generar secuencias pseudoaleatorias seguras [5].

La comprensión del caos y la dinámica caótica es un desafío importante, debido a que proporciona información sobre la complejidad inherente de los sistemas no lineales y ayudar a predecir o entender ciertos fenómenos. Sin embargo, debido a la naturaleza impredecible y sensible a las condiciones iniciales del caos, los sistemas caóticos a menudo se estudian en simulaciones numéricas y métodos analíticos, como los exponentes de Lyapunov y los atractores fractales.

Atractores extraños

Los atractores extraños son una característica distintiva de los sistemas dinámicos caóticos. Estos atractores se llaman "extraños" debido a su apariencia fractal y no periódica en el espacio de fase. A diferencia de los atractores regulares, como los puntos fijos, las órbitas periódicas o las trayectorias estables, los atractores extraños exhiben un comportamiento caótico y son altamente sensibles a las condiciones iniciales [5]. Un atractor extraño se puede visualizar como una estructura geométrica, en el espacio de fase, en la cual el sistema dinámico se "atrapa" y evoluciona de manera no periódica. Estas estructuras suelen ser fractales, lo que significa que exhiben patrones repetitivos a diferentes escalas.

Los atractores extraños no solo se encuentran en sistemas físicos, como la convección atmosférica, también se pueden encontrar en sistemas biológicos, económicos, químicos y otros sistemas complejos. Estos atractores representan una forma de comportamiento dinámico que no se puede describir mediante órbitas periódicas simples y muestran una riqueza y complejidad inherentes.

El atractor de Lorenz es un ejemplo de atractor extraño, el cual tiene una forma característica con dos lóbulos principales entrelazados, y su dinámica exhibe propiedades caóticas, como la dependencia sensitiva a las condiciones iniciales y la mezcla de trayectorias, Figura 3.

Los atractores extraños se pueden analizar y visualizar utilizando herramientas matemáticas y computacionales, como el análisis de Lyapunov, los exponentes de Lyapunov y técnicas de representación gráfica en el espacio de fase. Estas herramientas permiten explorar y comprender la estructura y las propiedades de los atractores extraños, así como también ayudan en la predicción y control de sistemas caóticos.

Sincronización generalizada

La sincronización generalizada se refiere a un fenómeno en el cual un conjunto de sistemas dinámicos, generalmente caóticos o estocásticos, se acoplan y exhiben una sincronización completa o parcial en su comportamiento. A diferencia de la sincronización clásica, donde se busca que los sistemas se sincronicen en un estado particular, la sincronización generalizada implica que los sistemas se sincronicen en múltiples aspectos, como la amplitud, la frecuencia, la fase u otras variables relevantes.

La sincronización generalizada ha sido ampliamente estudiada en el contexto de redes complejas, donde los sistemas dinámicos están conectados mediante interacciones no lineales. Este fenómeno es relevante en una variedad de campos, como la física, la biología, la neurociencia, la ingeniería y las ciencias sociales, debido a que proporciona información sobre la cooperación y la emergencia de comportamientos colectivos en sistemas complejos [6].

Existen diferentes formas de sincronización generalizada, dependiendo de cómo se sincronicen las variables de interés en los sistemas acoplados. Algunas de las formas comunes de sincronización generalizada incluyen: Sincronización de fase, de amplitud y de frecuencia. Una propiedad relevante es que, cuando los sistemas caóticos acoplados logran una sincronización en sus trayectorias caóticas, implica una dependencia sensitiva similar a las condiciones iniciales [7].

En la teoría de redes complejas, la sincronización generalizada puede ayudar a comprender comportamientos colectivos en sistemas complejos y la estabilidad de las redes dinámicas. En aplicaciones prácticas, la sincronización generalizada puede ser utilizada para la comunicación y la transmisión de información segura, la generación de señales complejas y la detección de sincronización en sistemas dinámicos acoplados.

Sistemas caóticos en tiempo continuo y en tiempo discreto

Los sistemas caóticos pueden manifestarse tanto en tiempo continuo como en tiempo discreto, dependiendo de cómo evoluciona el sistema a lo largo del tiempo. A continuación, se describen brevemente los sistemas caóticos en ambos dominios.

Sistemas caóticos en tiempo continuo

En los sistemas caóticos en tiempo continuo, se describen típicamente mediante ecuaciones diferenciales ordinarias (EDOs) o ecuaciones en derivadas parciales (EDPs). Ejemplos clásicos de sistemas caóticos en tiempo continuo incluyen el sistema de Lorenz, el sistema de Rossler y el sistema de Van der Pol.

En los sistemas caóticos en tiempo continuo, las trayectorias pueden ser continuas y en algunos casos suaves, pero exhiben una sensibilidad extrema a las condiciones iniciales.

Sistemas caóticos en tiempo discreto

En los sistemas caóticos en tiempo discreto, la evolución del sistema se produce en pasos discretos o instantes de tiempo separados. Estos sistemas se describen mediante ecuaciones de diferencia o ecuaciones en diferencias finitas. La evolución del sistema se calcula iterativamente a partir de un estado inicial.

Los sistemas caóticos en tiempo discreto también pueden exhibir sensibilidad a las condiciones iniciales y atractores extraños, la diferencia clave es que las trayectorias son discretas y se representan mediante puntos sucesivos en el espacio de fase. Ejemplos de sistemas caóticos en tiempo discreto incluyen el mapa logístico, el mapa de Henon y el mapa del panadero.

Tanto los sistemas caóticos en tiempo continuo como en tiempo discreto tienen características comunes, como la dependencia sensitiva a las condiciones iniciales, la presencia de atractores extraños y la impredecibilidad a largo plazo. Sin embargo, también existen diferencias en la forma en que se modelan y se estudian matemáticamente debido a las características específicas de cada dominio temporal.

Condiciones necesarias para sistemas caóticos

Para que un sistema pueda ser considerado caótico, generalmente se requieren las siguientes condiciones:

No linealidad. El sistema debe tener una dinámica no lineal. La no linealidad es esencial para la aparición del caos, esto por se introducen interacciones complejas y realimenta entre las variables del sistema.

Sensibilidad a las condiciones iniciales. Esto significa que una pequeña perturbación en las condiciones iniciales del sistema se amplifica exponencialmente a medida que pasa el tiempo, produciendo resultados muy diferentes.

Complejidad topológica. El espacio de fase del sistema debe tener una estructura topológica compleja, esto es que las trayectorias del sistema deben ser atractores extraños, es decir, conjuntos fractales de dimensión no entera que ocupan un volumen finito en el espacio de fase.

Ausencia de puntos fijos y ciclos límite estables. En un sistema caótico, no hay puntos fijos ni ciclos límites estables hacia los cuales converjan todas las trayectorias. En cambio, las trayectorias pueden exhibir comportamientos recurrentes y aleatorios.

Suficiente energía. Para que un sistema exhiba un comportamiento caótico, generalmente se requiere la presencia de energía suficiente para mantener la

dinámica no lineal y generar la sensibilidad a las condiciones iniciales. Es posible encontrar sistemas caóticos en diferentes escalas, desde sistemas físicos macroscópicos hasta sistemas microscópicos, como los sistemas cuánticos.

Rango de parámetros adecuado. El ajuste preciso de los parámetros es necesario para mantener el sistema en un estado caótico, por lo tanto, algunos sistemas pueden exhibir caos solo dentro de un rango específico de valores de parámetros. Cambiar los valores de los parámetros puede hacer que el sistema pase de un comportamiento caótico a uno estable o periódico [8].

Sincronización de sistemas caóticos

Los primeros estudios sobre sincronización de sistemas caóticos fueron realizados por Louis M. Pecora y Thomas L. Carroll en 1990, donde se afirmaba que los sistemas dinámicos caóticos desafían la sincronización y que la habilidad de diseñar sistemas caóticos sincronizados podría abrir oportunidades interesantes [9]. La sincronización de los sistemas caóticos se refiere al fenómeno en el cual dos o más sistemas, que inicialmente pueden estar evolucionando de manera independiente, ajustan sus estados dinámicos y comienzan a evolucionar de manera coordinada, mostrando comportamientos similares o idénticos. Esto significa que, a pesar de tener condiciones iniciales ligeramente diferentes, los sistemas se vuelven sincronizados y evolucionan en una forma similar en el tiempo [10].

La sincronización de sistemas caóticos puede ser de diferentes tipos, entre los que se destacan:

Sincronización completa. En este caso, los sistemas caóticos evolucionan de manera idéntica en todo momento. Las variables de estado de los sistemas se vuelven probablemente indistinguibles a medida que el tiempo avanza.

Sincronización lagrangiana o de tiempo desfasado. Aquí, los sistemas caóticos se sincronizan, pero existe un desfase constante en el tiempo entre ellos. Esto

significa que las variables de estado de un sistema están retrasadas o adelantadas con respecto a las del otro sistema, pero siguen mostrando un comportamiento coordinado.

Sincronización de fase. En este caso, los sistemas caóticos ajustan solo la relación de fase entre ellos, lo que significa que sus trayectorias en el espacio de fase están relacionadas de manera proporcional o en una forma específica. La amplitud y otros detalles del comportamiento pueden diferir entre los sistemas sincronizados.

Existen diferentes métodos y técnicas para lograr la sincronización de sistemas caóticos, algunos de los cuales son:

- **Acoplamiento.** Se establece una conexión entre los sistemas caóticos, de modo que influye entre sí y ajustan sus comportamientos dinámicos para alcanzar la sincronización.
- **Realimentación.** Se utiliza una señal de realimentación generada a partir de uno de los sistemas caóticos para guiar el comportamiento del otro sistema.
- **Control de certeza.** Se aplican técnicas de control para estabilizar y ajustar los estados de los sistemas caóticos, facilitando así la sincronización.

La sincronización de los sistemas caóticos es un fenómeno de gran interés tanto en la teoría de sistemas dinámicos como en aplicaciones prácticas. Se ha utilizado en diversas áreas, como comunicaciones seguras, criptografía, generación de números pseudoaleatorios y control de sistemas [11].

Aplicaciones de los sistemas caóticos

Algunas de las aplicaciones más destacadas son [12]:
Modelado en ciencias naturales: Los sistemas caóticos se utilizan para estudiar y modelar fenómenos complejos en diferentes disciplinas, como la física, la biología,

la geofísica y la meteorología. Los modelos caóticos ayudan a comprender y predecir este tipo de comportamiento presente en sistemas naturales.

Criptografía. La propiedad fundamental de los sistemas caóticos de ser altamente sensibles a las condiciones iniciales y generar un comportamiento aparentemente aleatorio los convierte en una herramienta útil para la criptografía. Se han propuesto algoritmos criptográficos basados en sistemas caóticos para generar claves seguras y realizar cifrados de datos.

Generación de números pseudoaleatorios. Debido a su comportamiento aparentemente aleatorio, los sistemas caóticos son utilizados para generar secuencias de números pseudoaleatorios. Estas secuencias se utilizan en simulaciones, pruebas de hipótesis estadísticas, diseño de juegos y en aplicaciones criptográficas.

Sistemas de control. Los sistemas caóticos también se han utilizado en aplicaciones de control. Algunas propiedades de los sistemas caóticos han sido utilizadas en conjunto con herramientas de control permitiendo manipular sistemas complejos, así como la supresión de oscilaciones indeseadas.

Procesamiento de señales. Los sistemas caóticos se utilizan en el procesamiento de señales para diversas tareas, como el análisis de series temporales, la compresión de datos y la detección de patrones. Su comportamiento no lineal permite realizar transformaciones y análisis complejos de las señales.

Comunicaciones seguras. Los sistemas caóticos se utilizan para la generación de señales caóticas para esquemas de comunicaciones seguras. Estas señales caóticas proporcionaron una mayor resistencia al ruido y a los ataques maliciosos, lo que contribuye a la confidencialidad y robustez de las comunicaciones.

Capítulo III: Osciladores Caóticos

Características de los osciladores caóticos

A diferencia de otros tipos de osciladores, los osciladores caóticos muestran un comportamiento no periódico, lo que significa que sus señales no se repiten en ciclos fijos y no siguen patrones predecibles. Recapitulando las características comunes de los osciladores caóticos: Sensibilidad a las condiciones iniciales, banda de frecuencias amplia, no linealidad, dependencia de parámetros, atractores extraños y propiedades estocásticas.

Oscilador caótico de Chua

El oscilador de Chua es un sistema dinámico no lineal que exhibe comportamiento caótico. Fue propuesto por el científico y físico León O. Chua en los años 80 y se ha utilizado como un ejemplo de un sistema caótico en la teoría del caos y la electrónica no lineal [13]. El oscilador de Chua se utiliza en aplicaciones que involucran generación de señales caóticas, comunicación segura y procesamiento de señales, entre otros. El circuito oscilador de Chua se presenta en la siguiente Figura 4.

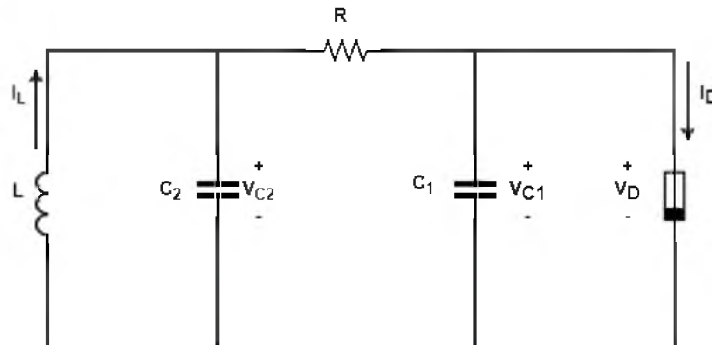


Figura 4 Circuito de Chua.

Analizando el circuito de Chua, por medio de las leyes de Kirchhoff, se obtiene un conjunto de tres ecuaciones diferenciales parciales no lineales que rigen la dinámica del sistema. Estas ecuaciones se presentan a continuación:

$$C_1 \frac{dv_{C1}}{dt} = \frac{1}{R}(v_{C2} - v_{C1}) - f(v_{C1}) \quad (5)$$

$$C_2 \frac{dv_{C2}}{dt} = \frac{1}{R}(v_{C1} - v_{C2}) + (i_L) \quad (6)$$

$$L \frac{di_L}{dt} = -v_{C2} \quad (7)$$

donde v_{C1} y v_{C2} son los voltajes a través de los capacitores C_1 y C_2 , respectivamente. i_L , es la intensidad de corriente a través del inductor L y $f(v_{C1})$ es la función no lineal que describe el diodo de Chua. La función no lineal $f(v_{C1})$ se describe de la siguiente manera

$$f(v_{C1}) = m_1 v_{C1} + \frac{1}{2}(m_0 - m_1)(|v_{C1} + E| - |v_{C1} - E|) \quad (8)$$

En la Figura 5 se muestra la relación voltaje-corriente (respuesta característica) del diodo de Chua.

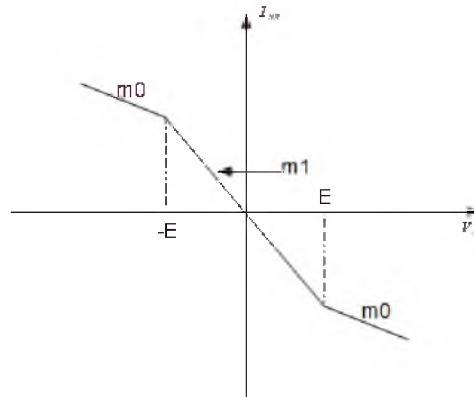


Figura 5. Respuesta característica del diodo de Chua.

donde m_0 es la pendiente de las regiones externas de la función $f(v_{c1})$, mientras que la región interna tiene pendiente m_1 . Los puntos de quiebre en la función no lineal, se encuentran dados por el voltaje $\pm E$.

Ecuaciones normalizadas del circuito de Chua

Debido a que el diodo de Chua es no comercial, y en ocasiones el valor del inductor es difícil de conseguir. A fin de evitar el uso de del diodo de Chua y el inductor, se realiza una transformación del sistema de ecuaciones (5)-(6)-(7), a una forma adimensional [7], asignando las siguientes igualdades:

$$x = \frac{v_{c1}}{E} \quad (9)$$

$$y = \frac{v_{c2}}{E} \quad (10)$$

$$z = i_L \left(\frac{R}{E} \right) \quad (11)$$

donde

$$\alpha = \left(\frac{C_2}{C_1} \right) ; \beta = \left(\frac{R^2 C_2}{L} \right) \quad (12)$$

$$a = Rm_0 ; \quad b = Rm_1 \quad (13)$$

A fin de encontrar ecuaciones adimensionales que describan la dinámica del sistema, se derivan (9)-(10)-(11) con lo que se obtiene $\dot{x} = \frac{dx_1}{d\tau}$, $\dot{y} = \frac{dx_2}{d\tau}$, $\dot{z} = \frac{dx_3}{d\tau}$

donde $\tau = \frac{1}{RC_2}$

con las expresiones anteriores, se obtienen las ecuaciones normalizadas para el circuito de Chua, como a continuación:

$$\dot{x} = \alpha[y - x - f(x)] \quad (14)$$

$$\dot{y} = x - y + z \quad (15)$$

$$\dot{z} = -\beta y \quad (16)$$

Aquí $f(x_1)$ es la función no lineal queda definida por:

$$f(x_1) = bx + \frac{1}{2}(a - b)(|x + 1| - |x - 1|) \quad (17)$$

Por medio de una simulación numérica se obtiene el comportamiento del oscilador caótico de Chua, ecuaciones (14)-(15)-(16) y (17). Los parámetros en la Tabla 1 se utilizan en la simulación.

Elemento ó parámetro	Valor	Tiempo de muestreo	Condiciones iniciales
I_1	0	1 Ms	0.35
I_2	0		0.5
I_3	0		0.75
<i>Alpha</i> α	10		
<i>Beta</i> β	-20		

Tabla 1. Parámetros y elementos para simulación 1. Variables de estado.

donde, I_1 , I_2 , I_3 son los integradores, *Alpha* y *Beta* son coeficientes obtenidos al parametrizar las ecuaciones del circuito de Chua. La simulación se realiza en un tiempo de 100 ms, utilizando el método de integración Ode4 (Runge-Kutta) de

Matlab/Simulink®. En el Anexo 1 se muestra el diagrama de bloques que se utiliza para la simulación.

La Figura 6a) muestra la respuesta del estado 1 “x” del circuito de Chua en su forma adimensional, esta respuesta corresponde al comportamiento de v_{C1} . Figura 6b) muestra la respuesta del estado 2 “y”, esta respuesta corresponde al comportamiento de v_{C2} . Y en Figura 6c) muestra la respuesta del estado 3 “z”, esta respuesta corresponde al comportamiento de i_L .

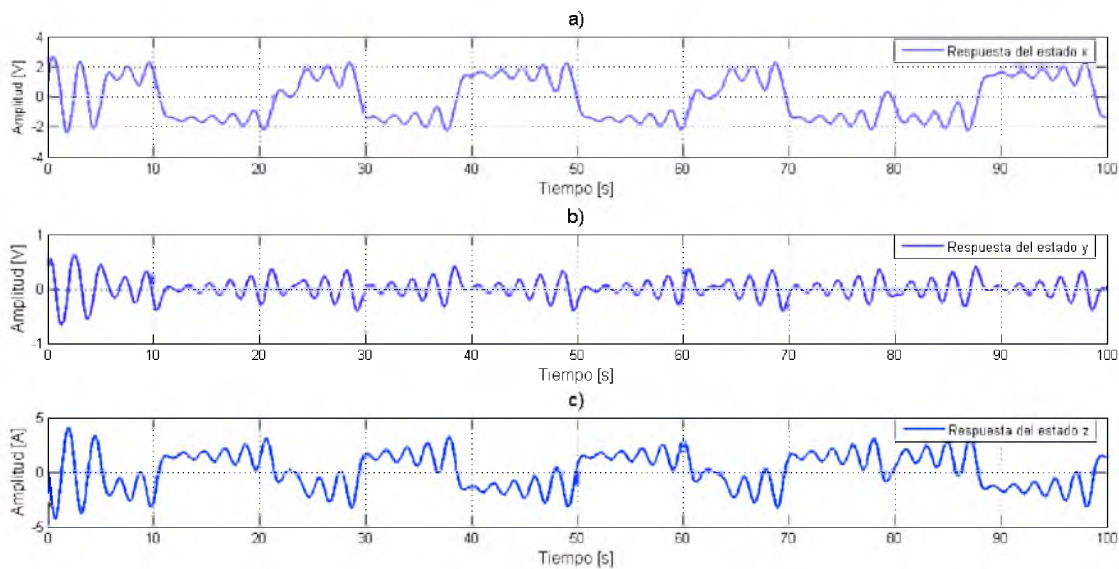


Figura 6. Respuesta de los estados del circuito caótico de Chua.

Como se observa, cada estado del sistema tiene su propia dinámica, cabe mencionar que estas señales son particulares a las condiciones iniciales utilizadas, es decir, si se utilizan otras condiciones iniciales cada señal será diferente.

El espacio de fases es el conjunto de todos los posibles estados en que se puede encontrar un sistema. A continuación, en la Figura 7a), Figura 7b), Figura 7c) se muestran las respuestas en espacio de fases, xy, xz, y yz, respectivamente.

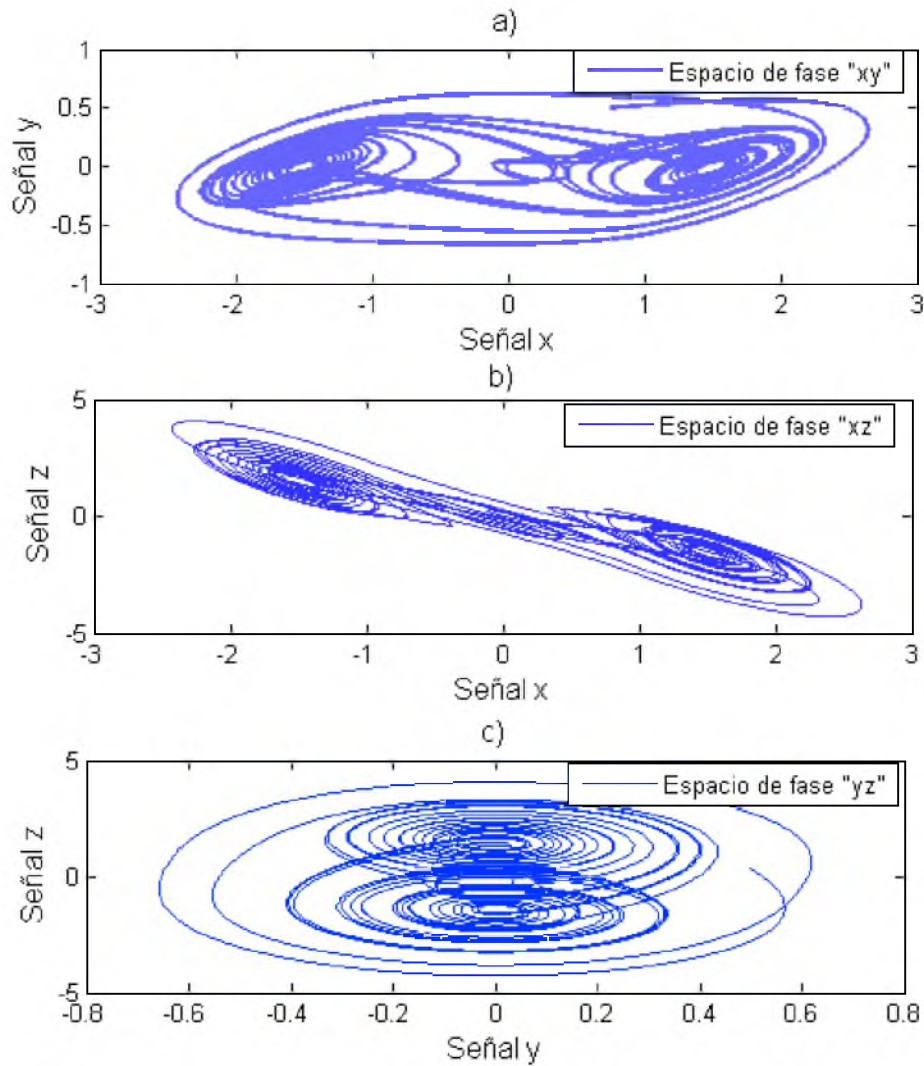


Figura 7. Espacio de fase del circuito caótico de Chua.

En Figura 7, cada gráfica tiene dos enrollamientos, las cuales son obtenidos a partir de las respuestas de los estados del circuito de Chua en variables de estados. Sin embargo, el sistema caótico de Chua, puede presentar n enrollamientos, haciendo más compleja la dinámica.

Un atractor es un conjunto en el cual las trayectorias del sistema tienden a converger a medida que evolucionan en el tiempo. Este sistema cuenta con el atractor en 3 dimensiones, el cual se muestra en la siguiente figura.

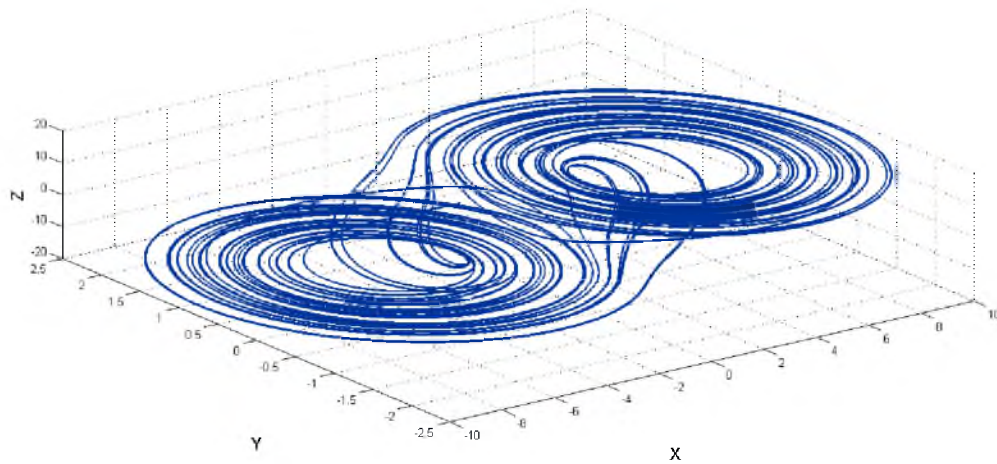


Figura 8. Atractor del circuito caótico de Chua.

El atractor caótico de Chua, Figura 8, en tres dimensiones, es el acoplamiento de los espacios de fase y única solución del sistema en las condiciones dadas, y representa la trayectoria a la cual converge el sistema conforme transcurre el tiempo.

Modelado de osciladores caóticos basados SNLF

El modelado de osciladores caóticos basados en funciones no lineales saturadas (SNLF, por sus siglas en inglés, Saturated Nonlinear Functions) es un campo de investigación en el que se utilizan funciones no lineales saturadas para generar comportamientos caóticos en sistemas dinámicos. En este contexto, una función no lineal saturada es una función matemática que tiene una región de saturación, donde la salida de la función se mantiene constante incluso si la entrada varía.

Los osciladores caóticos generados a través de estas funciones exhiben comportamientos caóticos, como la sensibilidad a las condiciones iniciales y la aperiodicidad, lo que los hace útiles en diversas aplicaciones, como la criptografía, la generación de números pseudoaleatorios y las comunicaciones seguras [14].

Un oscilador caótico basado SNLF puede ser descrito por el siguiente sistema de ecuaciones diferenciales:

$$\frac{dx}{dt} = y \quad (18)$$

$$\frac{dy}{dt} = z \quad (19)$$

$$\frac{dz}{dt} = -ax - by - cz + df(x; k, \alpha, h, p, q) \quad (20)$$

donde a , b , c y d son coeficientes reales positivos, con valores absolutos en el intervalo 0 y 1 y se requiere el valor de las condiciones iniciales $x(0)$, $y(0)$ y $z(0)$ debido a la interdependencia de las variables de estado.

El sistema presenta un comportamiento dinámico no lineal gracias a la función saturada desestabilizante $f(x; k, \alpha, h, p, q)$. El propósito de dicha función es retroalimentar al sistema y mantenerlo oscilando sin la necesidad de una variable de entrada extra en el sistema. La SNLF puede ser descrita mediante una función PWL (Piecewise Linear, de sus siglas en inglés) cuya forma dependerá del número de enrollamientos requeridos en el sistema caótico [14].

Las funciones PWL son funciones que se definen por segmentos lineales en diferentes regiones del dominio. Al utilizar estas funciones para describir el comportamiento de un oscilador caótico, se puede lograr una representación más simple y computacionalmente eficiente.

A continuación, se describe un enfoque general para el modelado de osciladores caóticos basado en funciones PWL:

1. Identificación de la dinámica no lineal. Es necesario identificar la dinámica no lineal del oscilador caótico que se desea modelar. Esto puede implicar el análisis de las ecuaciones de evolución del sistema o la observación empírica de su comportamiento caótico.
2. Definición de funciones PWL. En cada región del dominio discretizado se define una función lineal para describir la relación entre la variable de estado actual y su próxima actualización. Cada función PWL se caracteriza por su pendiente y su punto de corte con el eje de la variable de estado.
3. Iteración de las funciones PWL. Definidas las funciones PWL y establecidos sus parámetros, se puede iterar el modelo utilizando las funciones PWL para obtener la evolución de la variable de estado a lo largo del tiempo. En cada iteración, se determina en que parte del dominio se encuentra la variable de estado actual y se aplica la función PWL correspondiente para obtener la siguiente actualización de la región.

La aproximación PWL de la SNLF está dada por:

$$f(x; k, \alpha, h, p, q) = \sum_{i=-p}^q f_i(x; k, \alpha, h) \quad (21)$$

Oscilador Caótico de Chua basado en SNLF

El oscilador de Chua de n enrollamientos, representado por medio de SNLF, se representa por la siguiente ecuación:

$$f(x) = m_{2n-1}x + \frac{1}{2} \sum_{i=q}^{2n-1} (m_{i-1} - m_i)(|x + E_i| - |x + E_i|) \quad (22)$$

donde, m_i es la pendiente entre los tramos, E_i son los puntos de quiebre de la función, q es el parámetro que varía de acuerdo al número de enrollamientos del sistema, n representa el número de enrollamientos [14]. De acuerdo con [14], se considera que las pendientes tienen el mismo valor, por lo que, la ec.22 se reescribe como:

$$f(x) = m_1x + \frac{1}{2} \sum_{i=1}^{n-1} (-1)^i (m_1 - m_0) (|x + b_{n-i}| - |x + b_{n-i}|) \quad (23)$$

En este trabajo se utiliza un oscilador de Chua de doble enrollamiento, por lo que su función desestabilizante, descrita por una SNLF, es la siguiente

$$f(x) = mx + \frac{1}{2} (m_0 - m_1) (|x + 1| - |x - 1|) \quad (24)$$

donde $f(x; k, \alpha, h, p, q)$ es expresada como

$$f(x) = \begin{cases} -k & x > \alpha \\ sx & \alpha \leq x \leq -\alpha \\ k & x < -\alpha \end{cases} \quad (25)$$

Aquí, k es la saturación del sistema, α es el punto de quiebre en la función y s la pendiente a tramos.

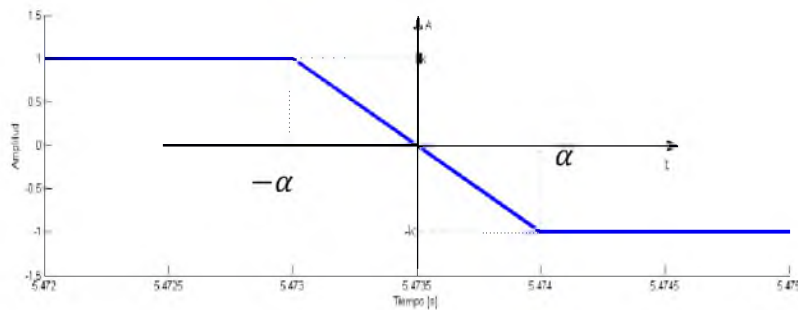


Figura 9 Función saturada desestabilizante de una SNLF.

Simulación de oscilador basado en funciones no lineales saturadas. A continuación, se muestran las gráficas de respuesta del sistema de Chua para dos enrollamientos representado por medio de funciones no lineales saturadas (SNLF). En la Tabla 2, se indican los parámetros utilizados para realizar la simulación.

Elemento o parámetro	Valor	Tiempo de muestreo	Condiciones iniciales
I_1	0	1 ms	0.75
I_2	0		0.5
I_3	0		0.35
α	$6.2 \cdot 10^{-6}$		
k	1		
a, b, c, d	0.7		

Tabla 2. Parámetros y elementos para simulación 2. SNLF.

El oscilador caótico de Chua representado por medio de funciones no lineales saturadas, queda determinado de la siguiente manera, para el estado 1 se usa la variable “x”, estados 2 “y” y por ultimo el estado 3 “z”, los integradores estan relacionado a cada estado, respectivamente. El diagrama de bloques utilizado para la simulación se muestra en Anexo 2.

A continuación, se muestran las señales generadas en la simulación del circuito caótico de Chua basado en SNLF. La Figura 10a) muestra la respuesta del estado 1 “x”, En Figura 10b) muestra la respuesta del estado 2 “y”. Y en Figura 10c) muestra la respuesta del estado 3 “z”.

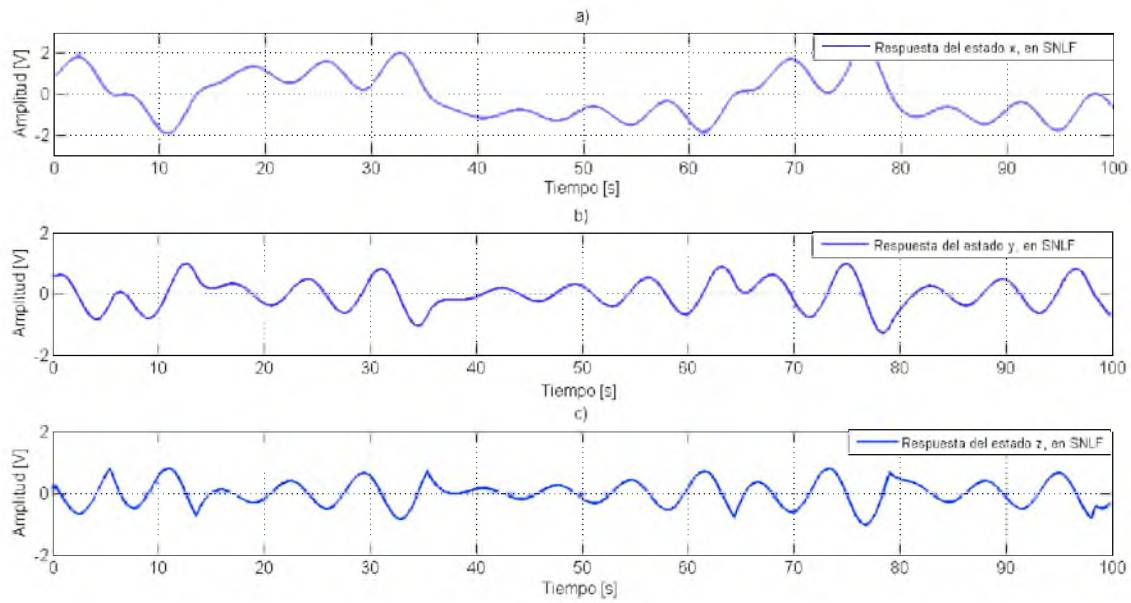


Figura 10. Respuesta del circuito caótico de Chua en SNLF.

En la Figura 10 se observa que cada señal cuenta con su propia dinámica. Se observa que las señales son aperiódicas, concluyendo que esto se debe a la sensibilidad a condiciones iniciales y a la no linealidad del sistema.

Generando el espacio de fases del conjunto de los estados del sistema basado en SNLF, se obtiene lo siguiente; en la Figura 11a) se muestra el espacio de fase “xy”, Figura 11b) el “xz”, y en Figura 11c) el espacio “yz”.

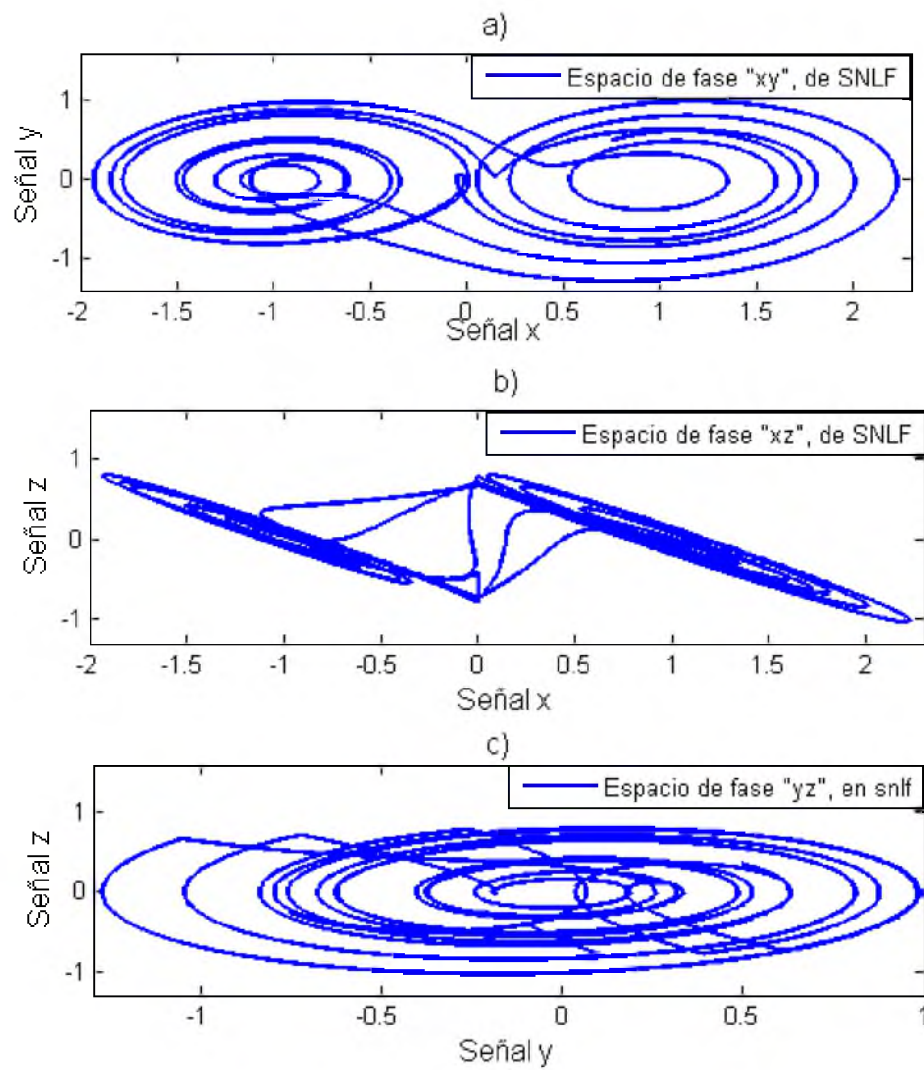


Figura 11. Espacio de fase, basado en SNLF.

Así mismo, en la Figura 12 se muestra el atractor caótico del circuito de Chua basado en SNLF. El cual corresponde a los dos enrollamientos.

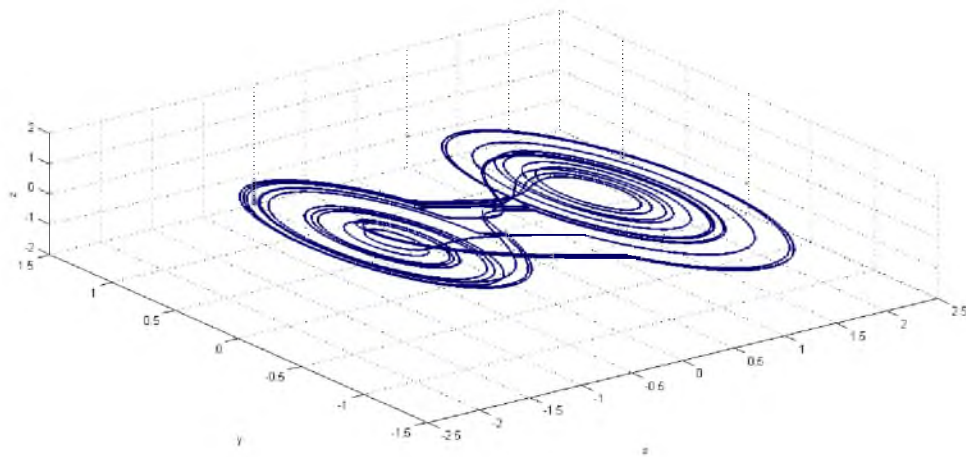


Figura 12. Atractor del circuito de Chua basado en SNLF.

Oscilador caótico de Chua con amplificadores operacionales

Modelo del inductor por medio de OpAmp

En el circuito caótico de Chua (Figura 4), el inductor y el diodo de Chua son indispensables, sin embargo, frecuentemente no están disponibles en el mercado. Debido a esto, es deseable poder emular las características ideales de estos dispositivos mediante el uso de circuitos electrónicos. Estos circuitos son comúnmente llamados *convertidores generales de impedancia*.

La Figura 13 es un convertidor de impedancias genérico la cual permite representar cualquier impedancia por medio de amplificadores operacionales.

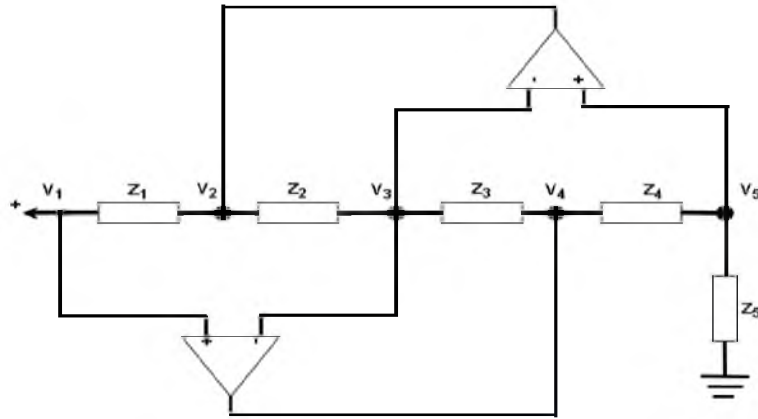


Figura 13. Convertidor de impedancias genérico (GIC).

Este circuito se utiliza para emular la respuesta del inductor. La impedancia equivalente del convertidor de impedancias genérico esta dado por:

$$Z_L = \frac{V}{I} = \frac{Z_1 Z_3 Z_5}{Z_2 Z_4} \quad (26)$$

Supongamos que el convertidor se implementará solo con circuitos RC, asignando las siguientes relaciones

$$R_1 = Z_1, R_2 = Z_2, R_3 = Z_3, R_5 = Z_5, \quad (27)$$

Y

$$Z_4 = C \quad (28)$$

Sustituyendo en la ec. (26) y asumiendo que es el inductor L.

$$L = \frac{R_1 R_3 R_5}{R_2} C \quad (29)$$

Los valores propuestos de las resistencias para emular el inductor son los siguientes: $R_1 = R_2 = R_3 = 1K\Omega$ y considerando que $L = \frac{1}{C}$ en magnitud.

$$\frac{LR_2}{R_1R_3}C = R_5 \quad (30)$$

se obtiene R_5

$$R_5 = 1 K\Omega \quad (31)$$

El circuito determinado para la emulación del inductor se muestra en el Anexo 4.

Modelo del diodo de Chua por medio de OpAmp

El modelo del diodo de Chua está representado por medio de amplificadores operaciones como se presenta en la Figura 14.

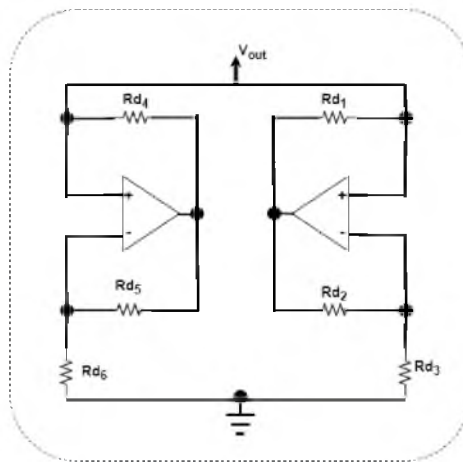


Figura 14. Esquema representativo del diodo de Chua con OpAmp.

Cabe resaltar que, al realizar las simulaciones se pudo percatar que el voltaje de alimentación de los amplificadores operacionales, dedicados a la emulación del diodo de Chua, siempre debe ser menor que la alimentación del resto de los amplificadores. En caso contrario el circuito no funcionará correctamente.

Debido a que la respuesta característica del diodo (niveles de saturación, puntos de quiebre y pendiente) es determinado por la fuente de alimentación, se debe conocer este valor para el óptimo funcionamiento del circuito.

De acuerdo a [15], a partir de la Figura 14. Esquema representativo del diodo de Chua con OpAmp. Figura 14, se proponen que $Rd_1 = Rd_2$, entonces:

$$Rd_3 = \frac{E_{sat}}{(E - E_{sat})m_0 - Em_1} \quad (32)$$

Donde E_{sat} es el voltaje de alimentación del OpAmp también conocido como voltaje de saturación, E son los puntos de quiebre de la función no lineal, y m_0 es la pendiente de las regiones externas de la función, mientras que la región interna tiene pendiente m_1 , ver Figura 5.

Analogamente, Rd_4 se determina por:

$$Rd_4 = \frac{E_{sat}}{E(m_0 - m_1)} \quad (33)$$

Se propone que $Rd_5 = Rd_4$ y de la misma forma en [15], Rd_6 se calcula como a continuación

$$Rd_6 = \frac{E_{sat}}{(E_{sat} - E)(m_0 - m_1)} \quad (34)$$

Debido a que los amplificadores operacionales son elementos no ideales, se realiza un pequeño ajuste en los parámetros de configuración del amplificador, a fin de obtener la mejor aproximación en la emulación el comportamiento del diodo de Chua. Los parámetros modificados se encuentran en la Tabla 3.

Elemento	valor
Rd_1, Rd_2	22 k Ω
Rd_3	2.50378 k Ω
Rd_4, Rd_5	270 k Ω
Rd_6	
Esat	± 6 V
E	1 V

Tabla 3. Elementos para simulación del diodo de Chua.

En la Figura 15 se muestra la respuesta del diodo de Chua obtenida de la emulación

con amplificadores operacionales

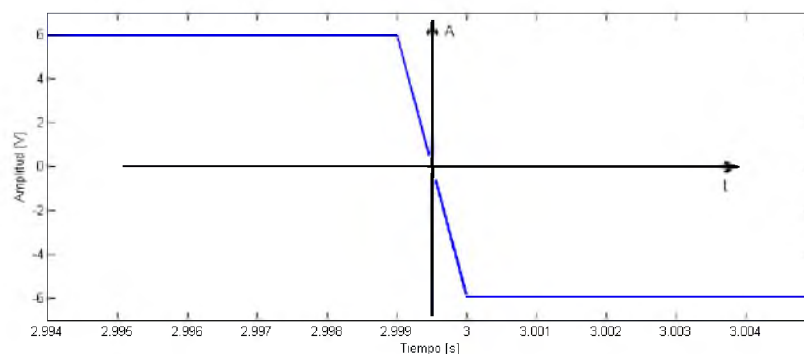


Figura 15. Respuesta del diodo de Chua emulado con OpAmp.

Para esta señal se utiliza una señal de excitación de $E = \pm 1$ V. La salida es saturada en 6 V, y la conmutación se genera en los puntos de quiebre en 2.999 y 3.0.

Simulación de la implementación del diodo de Chua y el inductor emulados con OpAmp's

Esta simulación ocupa dos amplificadores operacionales adicionales a los utilizados en el diodo de Chua. De acuerdo a lo anteriormente comentado, la alimentación de saturación para el diodo de Chua es de 6 V, mientras que para los amplificadores operacionales adicionales debe ser mayor a 6V y menor a 2 veces el valor de alimentación del diodo.

Elemento	Valor	Tiempo de muestreo	Condiciones iniciales
R_1, R_2, R_3, R_4	1 k Ω	1 μ s	
Rd_1, Rd_2	22 k Ω		
Rd_3	2.50378 k Ω		
Rd_4, Rd_5	270 k Ω		
Rd_6	2.50378 k Ω		
C	5.6 nF		0.35 V
R	2.188 k Ω		0.5 V
C ₁	1.4 nF		0.75 V
C ₂	4.3 nF		
V _{diodo}	± 6 V		
V _{OpAm}	± 6.5 V		

Tabla 4. Parámetros para simulación 3.

En el Anexo 4 se puede encontrar el diagrama de bloques para la simulación.

Las siguientes graficas muestran las respuestas del circuito caótico de Chua, con la emulación con amplificadores operacionales de la respuesta del inductor y la del diodo de Chua.

La Figura 16a) corresponde a la respuesta del capacitor C₁, la cual se denomina señal 'x'. en esta grafica se observa que la amplitud de la señal oscila entre ± 600

mV, y es aperiódica, lo cual es una característica del caos. En Figura 16b) se muestra el comportamiento del capacitor C_2 . Esta señal se designa con 'y', en la cual la amplitud oscila alrededor de los ± 120 mV. En la Figura 16c) se muestra el comportamiento del inductor L, esta es la respuesta del convertidor de impedancias, que emula el inductor, llámese a esta señal "z". Se observa que la amplitud oscila alrededor de los ± 400 mV.

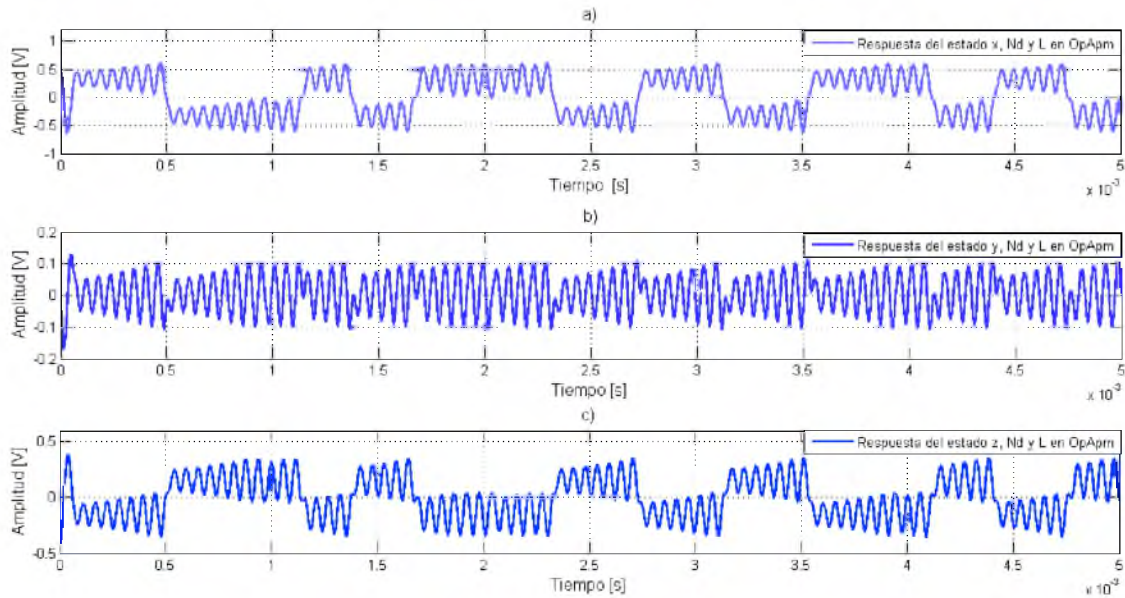


Figura 16. Respuesta de estados del circuito de Chua.

Generando el espacio de fases del conjunto de los estados del sistema basado en SNLF con la dinámica, del diodo de Chua y del inductor, emulada con OpAmp's, se obtiene lo siguiente; en la Figura 17a) se muestra el espacio de fase "xy", Figura 17b) el "xz", y en Figura 17c) el espacio "yz".

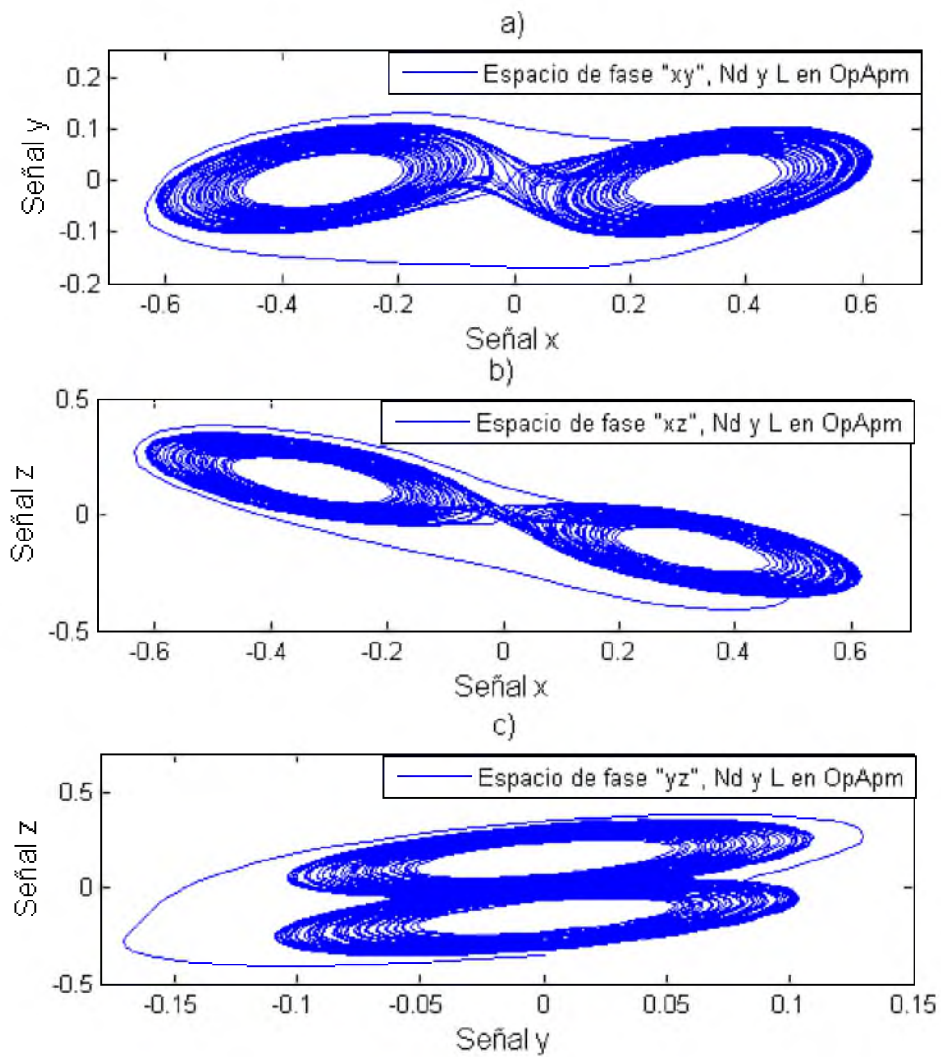


Figura 17. Espacios de fases

Así mismo, en la Figura 18 se muestra el atractor caótico del circuito de Chua basado en SNLF con la dinámica del diodo y el inductor emuladas con OpAmp's.

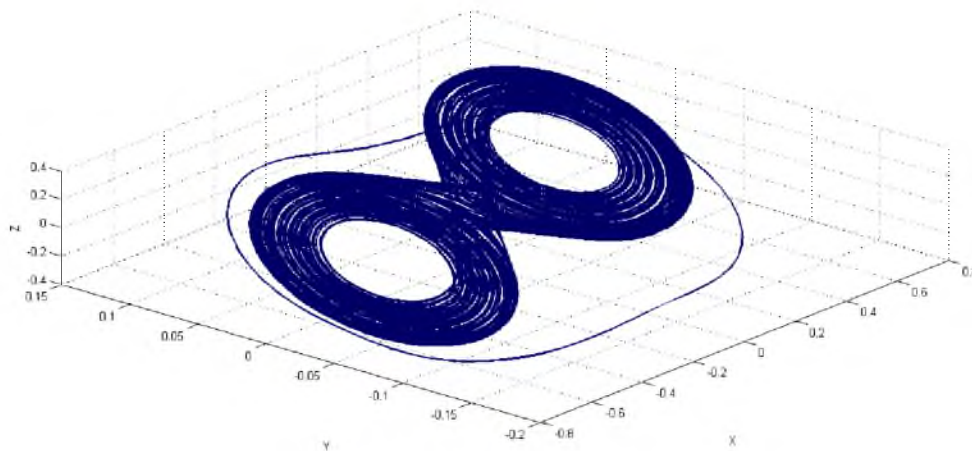


Figura 18. Atractor caótico de Chua, L y Nd emulado con OpAmp's.

Recapitulando lo mostrado en las secciones anteriores, se desarrolló el modelo matemático del circuito de Chua en su forma adimensional y se realizó una simulación con el fin de ver cómo se comporta el sistema. A partir de ese modelado se desarrolló la dinámica del circuito por medio de funciones no lineales saturadas (SNLF), y de la misma manera se comprobó por simulación, que el sistema presente caos y este determinado por dos enrollamientos. Por último, se emula por medio de amplificadores operacionales la dinámica del diodo de Chua y el Inductor, con el fin de evitar las limitaciones al querer realizar la implementación física, además se comprueba por simulación que estos elementos emulados, cumplan con su función, es decir, junto a los demás elementos del circuito de Chua, el sistema debe seguir presentando caos.

Simulación del circuito caótico de Chua basado en funciones no lineales saturadas.

[illegible]

Figura 19. Esquema electrónico del circuito caótico de Chua implementado con OpAmps.

En la Tabla 5 se presentan los elementos y parámetros que se utilizan para obtener las respuestas del sistema.

Elemento	Valor	Tiempo de muestreo	Condiciones iniciales
$R_1 \dots R_4$	1 k Ω	1 ms	
Rd_1, Rd_2	22 k Ω		
Rd_3	2.50378 k Ω		
Rd_4, Rd_5	270 k Ω		
Rd_6	2.50378 k Ω		
$R_5 \dots R_{19}$	10 k Ω		
C_1	10 nF		0.75 V
C_2	10 nF		0.5 V
C_3	12 nF		0.35 V
V_{diodo}	± 7 V		
V_{OpAm}	± 13 V		

Tabla 5. Parámetros para simulación.

Las siguientes graficas muestran las respuestas del circuito de Chua implementado solo con Opamp's, a partir del modelo basado en SNLF, en esta simulación se usó un paso de muestreo de 1 ms.

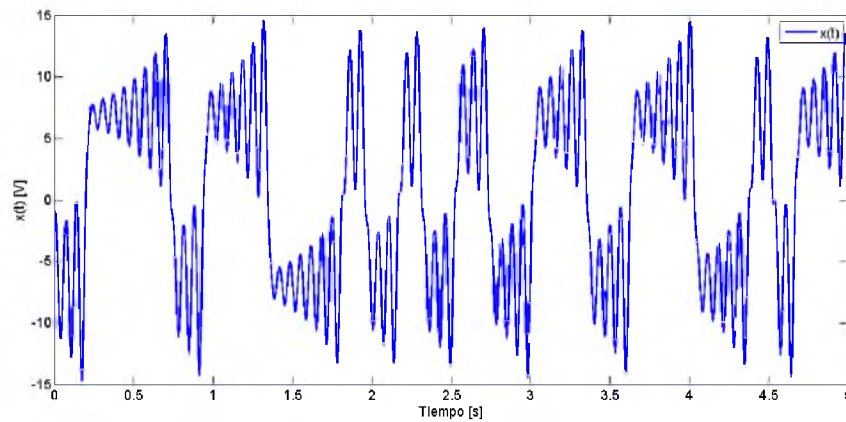


Figura 20. Estado "X" del circuito eléctrico

La Figura 20 representa la dinámica del estado 'x' del sistema, es decir, es el comportamiento del capacitor 1, a simple vista se observa que no es periódica. Esta señal será con la cual se trabaje en lo que sigue del desarrollo de este documento, es decir, a partir de esta señal se aplicaran pruebas de aleatoriedad, cuantificación de caos, sincronización y enmascaramiento de información.

La Figura 21 representa la dinámica del estado 'y' del sistema, es decir, es el comportamiento del capacitor 2, esta señal, al igual que la señal 'x' es aperiódica.

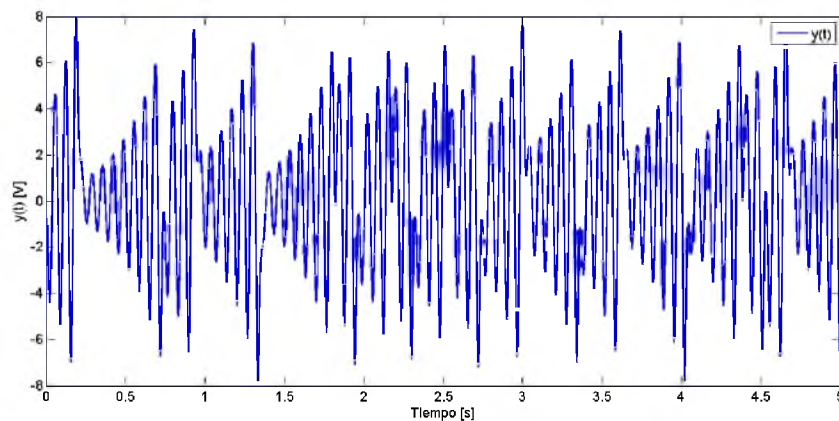


Figura 21. Estado "Y" del circuito Eléctrico

La Figura 22 representa la dinámica del estado 'z' del sistema, es decir, es el comportamiento del inductor, se observa que no es periódica.

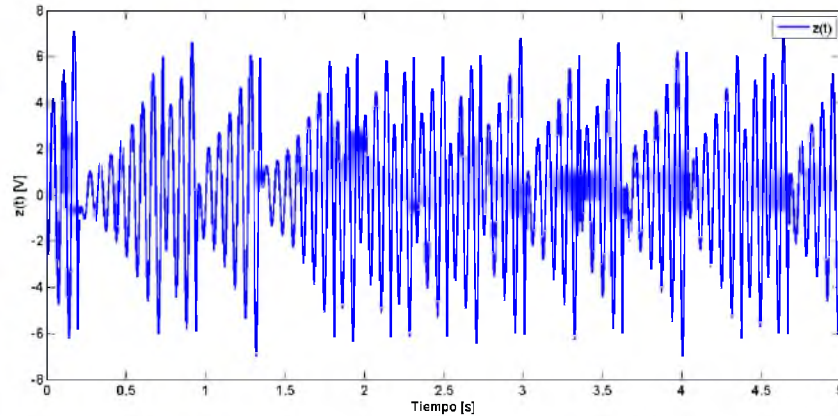


Figura 22. Estado "Z del circuito eléctrico"

En este trabajo se utiliza la señal 'x', no obstante, se puede utilizar cualesquiera de las señales generadas por el circuito.

Generando el espacio de fases del conjunto de los estados del sistema implementado con OpAmp's, se obtienen las siguientes graficas:

En la Figura 23 se muestra el espacio de fase "xy", se observa que el sistema presenta dos enrollamientos.

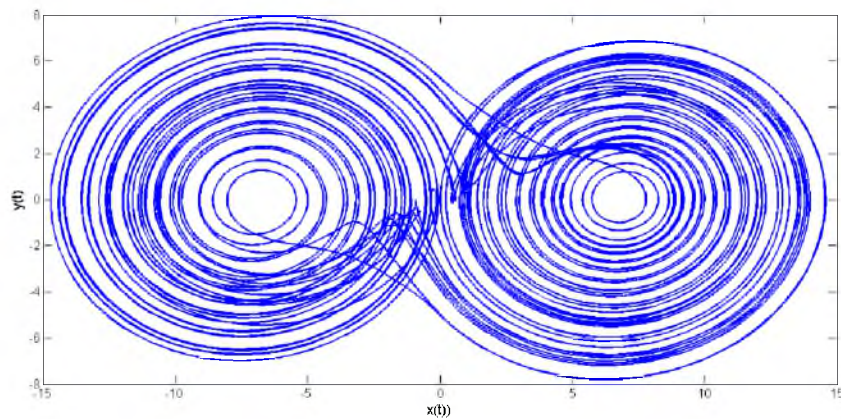


Figura 23. Espacio de fase "XY"

En la Figura 24 se muestra el espacio de fase "xz", la dinámica de estos espacios de fase, son únicos a la solución del sistema con las condiciones iniciales dadas, así como también se encuentran determinados por los parámetros del sistema.

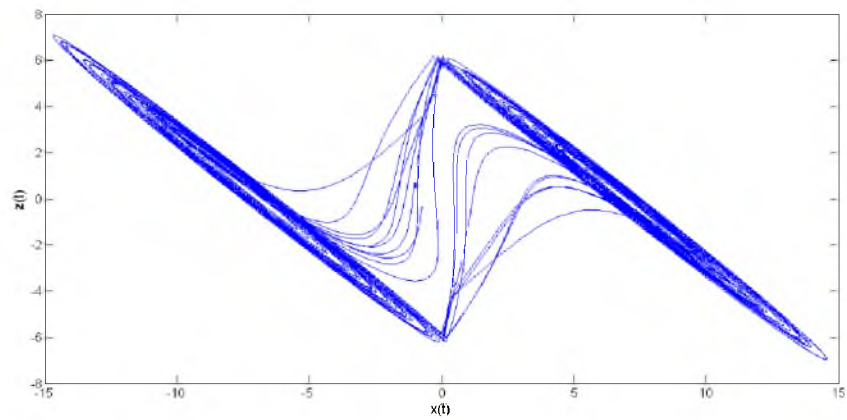


Figura 24. Espacio de fase "XZ"

En la Figura 25 se muestra el espacio de fase "yz".

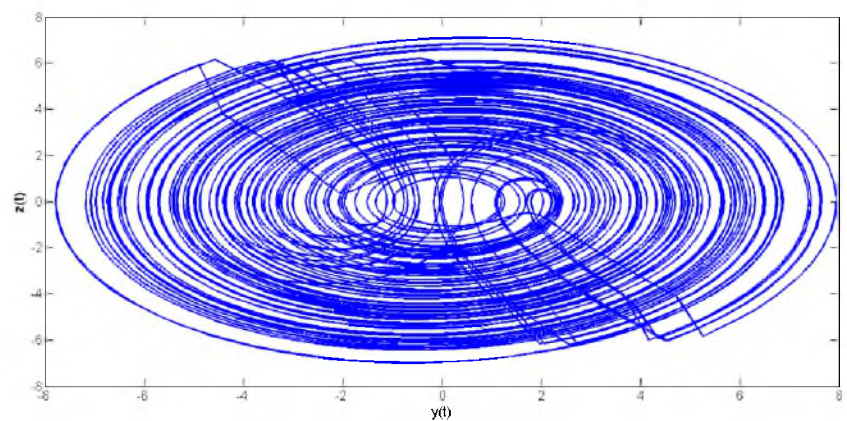


Figura 25. Espacio de fase "YZ"

Las gráficas mostradas en cada una de las figuras de los espacios de fase, es una representación de las dos formas en las que se pueden obtener, es decir, el espacio de fase “xy”, también se puede obtener como “yx”. A demás se hace hincapié de que en este trabajo solo se trabaja con dos enrollamientos en el circuito, pero el sistema puede generar n enrollamientos.

El conjunto al cual las trayectorias del sistema tienden a converger a medida que el tiempo crece, se muestra en la Figura 26 que es el atractor perteneciente al circuito caótico de Chua simulado con la implementación de OpAmp’s basado en las SNLF.

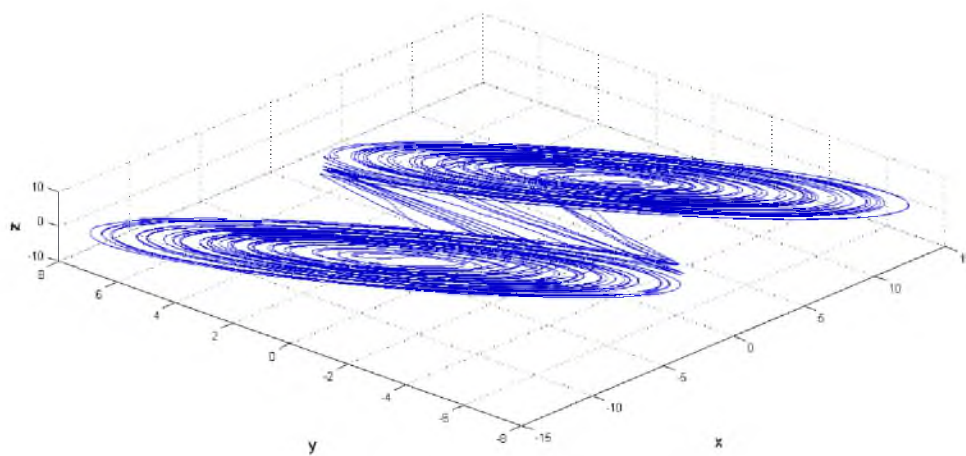


Figura 26. Atractor de Chua basado en SNLF implementado con OpAmps.

Aleatoriedad

Una de las propiedades de los sistemas caóticos es que presentan aleatoriedad. En este contexto se hace el análisis del grado de aleatoriedad del circuito caótico de Chua implementado con amplificadores operacionales. Esto se realiza debido a que en criptografía es fundamental usar claves de cifrado basado en generadores que producen secuencias aleatorias.

Para lograr una secuencia de bits, se utiliza un comparador de voltaje combinado con un sumador, como se muestra en la Figura 27.

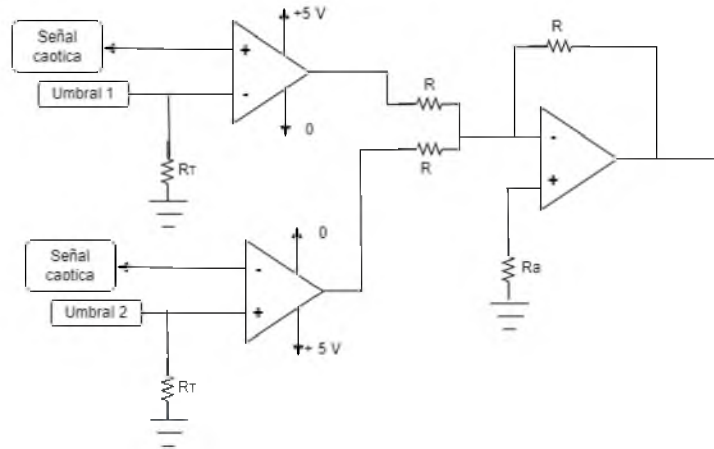


Figura 27. Esquema eléctrico para generación de secuencia de bits.

Esta configuración de amplificadores operacionales tiene tres entradas, de las cuales una es la señal caótica a utilizar para la generación de bits y las otras dos pertenecen a un valor de umbral (umbral 1 y umbral 2). Estos umbrales son establecidos con base al nivel de voltaje de la variable de estado en función de sus puntos de equilibrio, como se observa en la Figura 28.

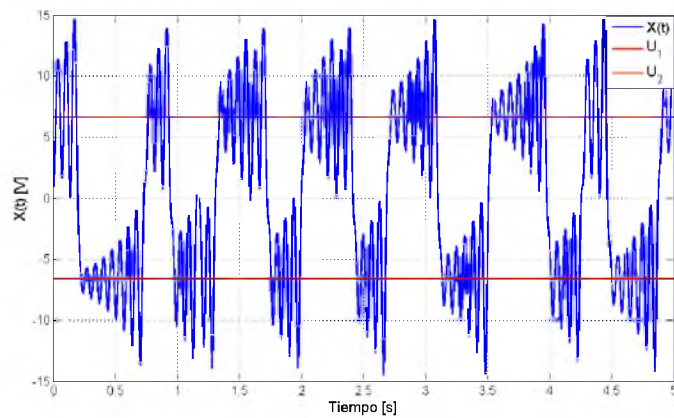


Figura 28. Umbrales U_1 , U_2 en señal X para generación de bits.

Los umbrales propuestos se enfocan en los puntos de equilibrio del sistema, es decir, los puntos donde surge cada enrollamiento, estos puntos de equilibrio son particulares a los parámetros del sistema.

La respuesta de los comparadores queda definida como sigue, definiendo

Umbral $i = U_i$, entonces

$$S^1 = \begin{cases} 1, & f(x) > U_1 \\ 0, & f(x) < U_1 \end{cases} \quad (35)$$

$$S^2 = \begin{cases} 0, & f(x) > U_2 \\ 1, & f(x) < U_2 \end{cases} \quad (36)$$

donde S^1 y S^2 , son la salida de los circuitos comparadores. La respuesta de este sistema se muestra en la Figura 29.

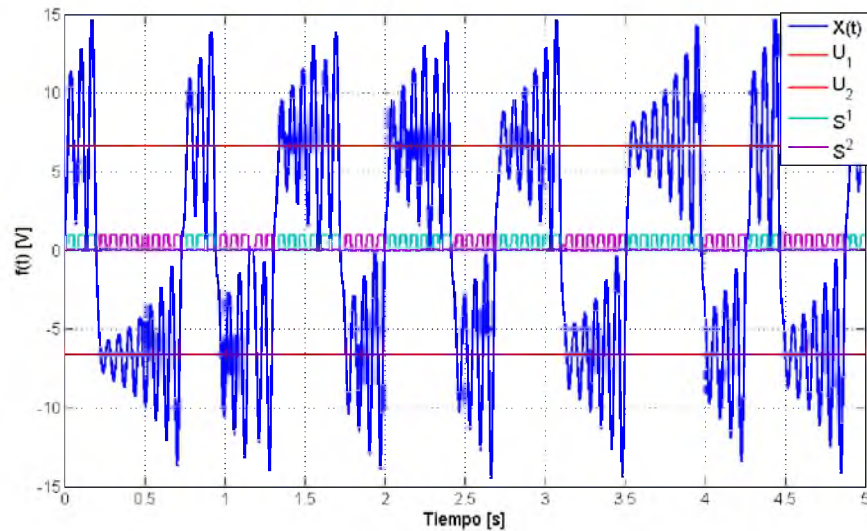


Figura 29. Generación de bits.

En esta figura se observan los bits generados, los cuales se obtienen con la suma de cada comparador, por lo que, en la salida del amplificador operacional sumador se tiene la secuencia completa de bits, Figura 30.

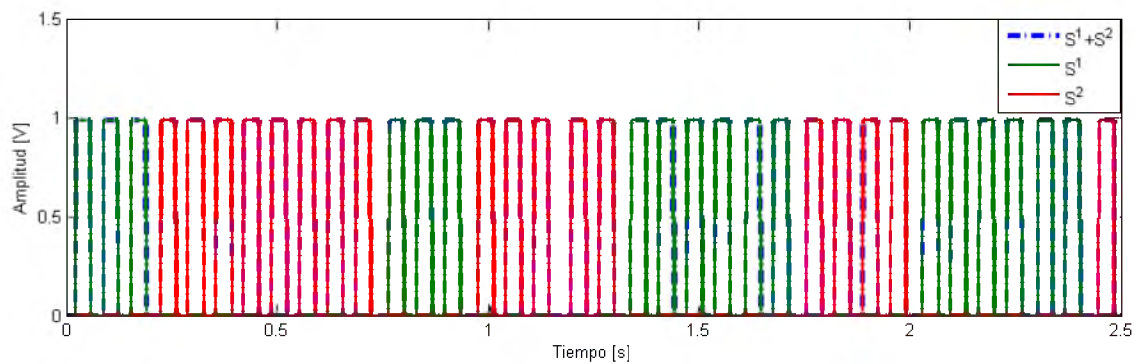


Figura 30. Secuencia de bits generados del estado X.

La secuencia de bits es generada a partir del estado X del oscilador caótico de Chua implementado con amplificadores operacionales. Esta secuencia de bits se genera para verificar que el sistema sea aleatorio. Una forma de comprobar esta característica es aplicando el teorema de frecuencia, y el teorema del monobit.

Teorema de la frecuencia.

Se refiere a la frecuencia de unos y ceros en una secuencia. Establece que, en una secuencia de bits aleatoria, se espera que la frecuencia de unos y ceros sea aproximadamente la misma, es decir, la mitad de los bits deberían ser 0 y la mitad deberían ser 1 para que la secuencia sea "equilibrada" [16].

Para poner a prueba la secuencia de bits generada a partir del oscilador caótico de Chua implementada por amplificadores operacionales, se propone usar al menos una muestra de 20 Kbits, considerando un margen de error del 2%. Cabe mencionar que esta prueba se realiza en simulación, usando un muestreo de 1 ms, tiempo de simulación de 20 s. El diagrama de bloques y el código utilizado para establecer el número de 0's y 1's presentes en la secuencia se muestra en el Anexo 6.

A continuación, se muestran los resultados del test de frecuencia obtenidos a partir de la simulación anteriormente mencionada.

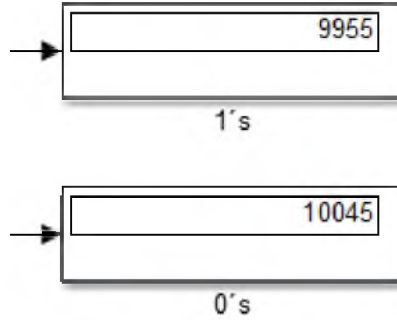


Figura 31. Resultado del test de Frecuencia.

En la Figura 31 se observa el resultado de la prueba de frecuencia. En esta prueba se determinó que en una muestra de 20 Kbits, 9955 bits son 1's y 10045 son 0's. El formato en el cual la simulación muestra los resultados no puede ser presentado en formato de Kbits por las características propias del software.

Se calcula que el margen de error de la secuencia de bits, se busca que sea menor al error aceptado.

$$e = \frac{n}{2} - \left[\frac{n}{2} - n * e\% \right] \quad (37)$$

aquí n es el tamaño de la muestra, $e\%$ es el margen de error y e es el error aceptado en la generación de bits

$$e = \pm 200 \quad (38)$$

Así se tiene que el rango de valores aceptados por el error es de

$$9800 \geq c \leq 10200 \quad (39)$$

Por lo tanto, de acuerdo al teorema de frecuencia se establece que la secuencia de bits generada a partir del oscilado caótico de Chua es aleatoria.

Teorema del Monobit.

Se refiere a la distribución de la suma de bits en una secuencia. El teorema del monobit establece que, para una secuencia de bits de longitud n , la cantidad de unos (X) y la cantidad de ceros ($n-X$) deben seguir una distribución binomial con una media μ de $n/2$ y una desviación estándar σ de $\sqrt{n}/2$, [17].

En este caso, la secuencia se considera de $n=20$ Kbits, con 10045 0's y 9955 1's. La media μ sería $n/2=10000$ y la desviación estándar es

$$\sigma = \frac{\sqrt{20000}}{2} = 70.71 \quad (40)$$

Para verificar la aleatoriedad, se calcula la prueba estadística de Z , que se define como sigue:

$$Z = \frac{X - \mu}{\sigma} \quad (41)$$

En este caso, se tiene:

$$Z = \frac{9955 - 10000}{70.71} \approx -0.636 \quad (42)$$

con un umbral crítico de significancia del 5%. El umbral crítico para una prueba de dos colas sería aproximadamente ± 1.96 . Dado que -0.636 está dentro de este rango, es suficiente evidencia para decir que la secuencia es aleatoria según el teorema del monobit.

Una vez establecida que la secuencia de bits es aleatoria, se corrobora que el sistema sea caótico, para ello se utilizan los exponentes de Lyapunov. El teorema de Lyapunov nos permite establecer condiciones bajo las cuales un sistema es caótico.

Teorema de exponentes de Lyapunov

El teorema de los Lyapunov establece que; si una función de un sistema $f(x)$, evaluada con condiciones diferentes pero infinitesimalmente cerca $f(0)$, $f(0+ \varepsilon)$, divergen de un punto conforme el tiempo tiende a infinito, el sistema es caótico. En otras palabras, los exponentes de Lyapunov miden la rapidez con la que las señales de un sistema crecen en el tiempo, cuando existe una distancia infinitesimalmente pequeña entre dos estados iniciales.

El exponente de Lyapunov se representa por λ y el número de exponentes de Lyapunov depende del número de variables de estado que tiene el sistema. Sin embargo, basta con determinar uno de ellos [18].

Se considera un punto cualquiera x_t en el momento t , el cual es perturbado una distancia ε_t y se obtiene otro punto $x_t + \varepsilon_t$. En los sistemas caóticos la perturbación crece exponencialmente $|\varepsilon_t| \approx |e^{\lambda t}|$ lo que es equivalente a $\ln \frac{|\varepsilon_t|}{|\varepsilon_0|} \approx \lambda t$. Considerando que la perturbación en el instante $t=0$ es muy pequeña el exponente de Lyapunov está definido por: λ

Variación en la condición inicial de un solo estado.

Para la el cálculo 1 del exponente de Lyapunov de cada variable, se utiliza el esquema eléctrico mostrado en la Figura 19. En este cálculo se considera que solo cambia la condición inicial en el estado X, es decir, la condición para el integrador de X varia una milésima. De esta manera la condición inicial en $x_i=0.75$, y para $x_t + \varepsilon_t=0.751$. Los exponentes para λ_x , λ_y , y λ_z , se muestran en Tabla 6.

Tiempo	λ_x	λ_y	λ_z	λ
25 s	0.065	-0.071	0.006	0
50 s	-0.012	0.008	0.004	0
75 s	0.026	-0.008	0.002	0.02
100 s	0.032	0.018	-0.019	0.031
125 s	-0.012	-0.005	0.007	-0.001
150 s	0.004	0.0006	-0.002	0.002

Tabla 6. Cálculo 1 de los exponentes de Lyapunov para cada variable.

En la Tabla 6, se observan los exponentes de Lyapunov para cada estado del sistema. En estos exponentes solo se perturba el estado x, y se evalúa su variación con respecto del tiempo, es decir, cuando el tiempo es $t=25s$, se obtiene un valor específico para cada exponente de cada estado, y así sucesivamente para cada tiempo t presentado en la Tabla 6. En [18] se demuestra que, si al menos un exponente de Lyapunov del total de los exponentes presentes en el sistema es positivo, es un indicador de que en el sistema existe caos. En la Tabla 6 se puede verificar que 1 o 2 exponentes son positivos, por lo que, se dice que el sistema de oscilador caótico de Chua por medio de funciones no lineales saturadas implementado en amplificadores operacionales presenta caos.

Variación en la condición inicial de los tres estados del sistema.

Para el cálculo 2 se considera cambiar la condición inicial en los tres estados x,y,z. La condición para cada integrador se varia una milésima, esto es las condiciones iniciales son: $\varepsilon_{x0} = 0.75$, $\varepsilon_{y0} = 0.5$, $\varepsilon_{z0} = 0.53$ y $\varepsilon_{xt} = 0.751$, $\varepsilon_{yt} = 0.301$, $\varepsilon_{zt} = 0.351$, respectivamente. los exponentes para λ_x , λ_y , y λ_z , se muestran en la Tabla 7

Tiempo	λ_x	λ_y	λ_z	λ
25 s	-0.015	0.027	0.000	0.012
50 s	-0.019	0.001	-0.008	-0.026
75 s	0.012	0.009	-0.013	0.007
100 s	0.038	-0.012	0.009	0.035
125 s	-0.016	-0.019	0.003	-0.032
150 s	-0.003	0.000	0.006	0.003

Tabla 7. Cálculo 2 de los exponentes de Lyapunov para cada variable.

En este apartado, Se diseñó en simulación, el esquema electrónico del circuito de Chua basado en funciones no lineales saturadas. Se indicó que el sistema produce caos, por medio de los exponentes de Lyapunov. De este circuito se seleccionó el estado 'x' como señal para la encriptación, por lo que, a partir de esta señal se generó una secuencia de bits para comprobar la aleatoriedad del sistema. Recordando que para que se cumpla el objetivo de *comunicación segura*, los circuitos emisor- receptor debe estar sincronizados, a continuación, se realiza este punto necesario.

Sincronización del circuito caótico de Chua

Dos o más sistemas caóticos están en sincronización, si transcurrido el transitorio, las dinámicas de los sistemas caóticos convergen a un mismo punto de forma asintótica, aun si inicialmente los sistemas eran totalmente diferentes [19].

Considere dos sistemas caóticos, $\dot{x} = f(x)$ y $\dot{y} = g(y)$, donde f y g son campos vectoriales que contienen estados $x(t)$ y $y(t)$ elementos de $\mathbb{R}^n$. Entonces los sistemas están sincronizados si:

$$\lim_{t \rightarrow \infty} \|x(t) - y(t)\| = 0, \quad x(0) \neq y(0) \quad (43)$$

El error de sincronía esta dado por:

$$e(t) = x(t) - y(t) \quad (44)$$

Para que se cumpla la ec.(43), es necesario que exista un acoplamiento entre los sistemas caóticos, el cual permite la sincronización de los estados. El acoplamiento de sistemas se divide en dos: acoplamiento unidireccional y acoplamiento bidireccional. Esto determina el tipo de sincronización, esto es una sincronización maestro-esclavo (unidireccional), o una sincronización maestro-maestro o mutua (sincronización bidireccional) [19].

Acoplamiento unidireccional

En el acoplamiento unidireccional la dinámica del oscilador esclavo depende de los estados del oscilador maestro, por lo que, después de un tiempo los sistemas se sincronizan. En este tipo de acoplamiento el maestro solo tiene influencia sobre el esclavo.



Figura 32. Acoplamiento unidireccional

En la Figura 32 muestra la analogía de un acoplamiento unidireccional.

La dinámica del oscilador maestro se rige de la siguiente forma

$$\dot{x} = f(x) \quad x \in R^n \quad (45)$$

Donde las componentes de x son $[x_1, x_2, \dots, x_n]^T$. considere que se toma la primer componente de x como una señal acoplante $x_1 = x_1(t)$, el oscilador caótico esclavo recibe esta señal, por lo tanto su dinámica se rige por:

$$\dot{y} = g(\hat{x}) + c(x_1 - \hat{x}_1) \quad \hat{x} \in R^n \quad (46)$$

Donde $g(\hat{x})$ es la dinámica en si del oscilador esclavo, c es una constante de acoplamiento, x_1 es la dinámica deseada de la señal acoplante $\hat{x}_1$ es la dinámica de la señal acoplada.

Acoplamiento bidireccional

En el acoplamiento bidireccional, cada sistema tiene influencia sobre el otro, por lo que se considera que ambos son tipo maestro, de aquí se determina que para el oscilador 1

$$\dot{x} = f(x) + c(x_1 - \hat{x}_1) \quad x \in R^n \quad (47)$$

y para el oscilador 2, el modelado es el siguiente

$$\dot{\hat{x}}_1 = g(\hat{x}) + c(x_1 - \hat{x}_1) \quad \hat{x} \in R^n \quad (48)$$



Figura 33. Acoplamiento bidireccional

Sincronización en dos circuitos de Chua

En las secciones anteriores, se verificó que el circuito caótico de Chua basado en SNLF, implementado en la simulación por medio de amplificadores operacionales, es sensible a las condiciones iniciales. En este apartado se procede a realizar la sincronización tipo unidireccional entre dos circuitos como el antes mencionado (emisor-receptor). Lograr la sincronización es importante, ya que, si los sistemas no están sincronizados no sería posible el descifrar la información. Las ecuaciones (18)- (19)- (20) y (24) describen el modelado del circuito maestro.

En la sincronización, la señal de acoplamiento, es la señal “x”, por lo tanto, las ecuaciones del circuito receptor son las siguientes:

$$\frac{d\hat{x}}{dt} = \hat{y} \quad (49)$$

$$\frac{d\hat{y}}{dt} = \hat{z} \quad (50)$$

$$\frac{d\hat{z}}{dt} = -a\hat{x} - b\hat{y} - c\hat{z} + df(x; k, \alpha, h, p, q) \quad (51)$$

$$f(\hat{x}) = m\hat{x} + \frac{1}{2}(m_0 - m_1)(|\hat{x} + 1| - |\hat{x} - 1|) \quad (52)$$

Para realizar la simulación, para el circuito maestro, se consideran los parámetros mostrados en la Tabla 5 y para el circuito esclavo, solo cambian las condiciones iniciales, las cuales son todas iguales a cero. En el Anexo 7 se muestra el esquema extendido utilizado para la simulación.

La graficas del error generando en la sincronización de los circuitos, se muestran a continuación. En la Figura 34a) se muestra el error de sincronización de la señal 'x', se observa que es el estado con más tarda en converger a cero, en aproximadamente 9 s. En la Figura 34b) y Figura 34c), se muestran los errores de los estados 'y' y 'z', respectivamente. Estos errores tienden a cero en aproximadamente 0.25 s.

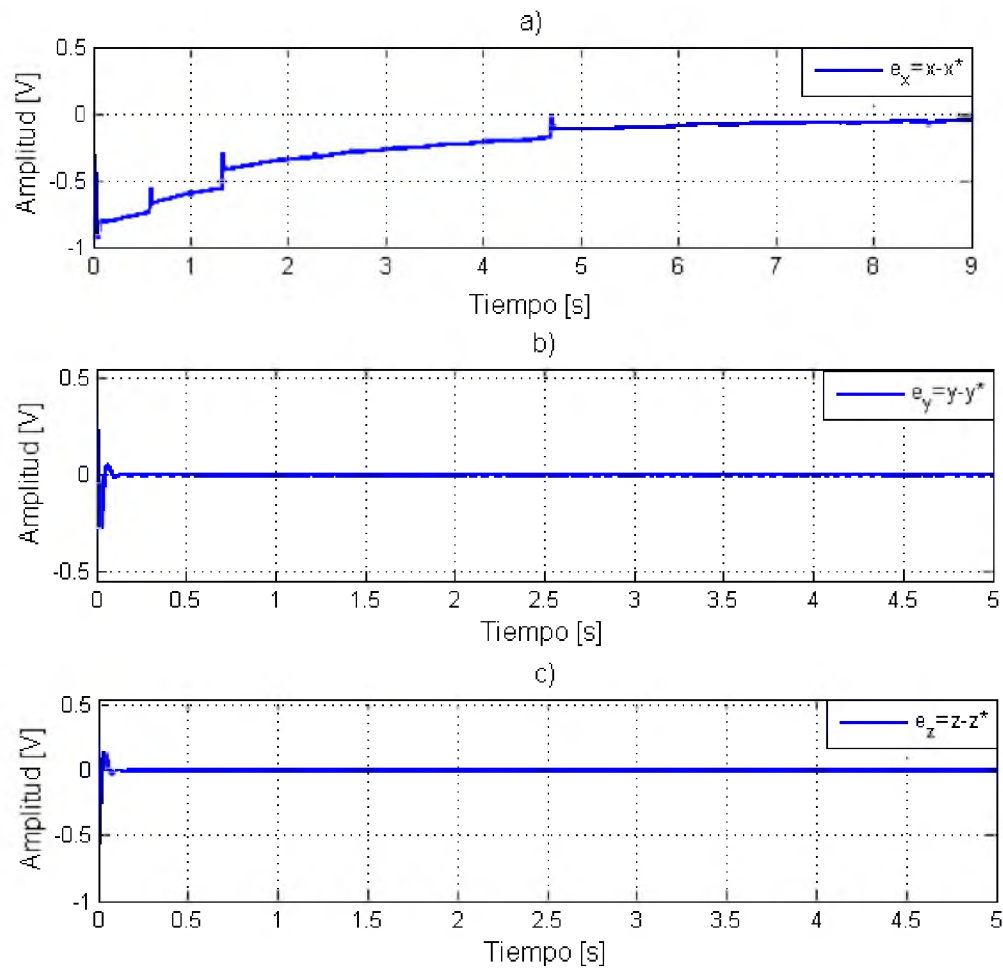


Figura 34. Graficas de error en la sincronización en dos circuitos de Chua.

Para hacer hincapié, de que los sistemas caóticos son sensibles a condiciones iniciales, se realiza nuevamente la simulación anterior, esta vez se consideran

condiciones iniciales con una diferencia de 1 milésima entre los circuitos emisor-receptor. Los graficas del error se muestran en la Figura 35.

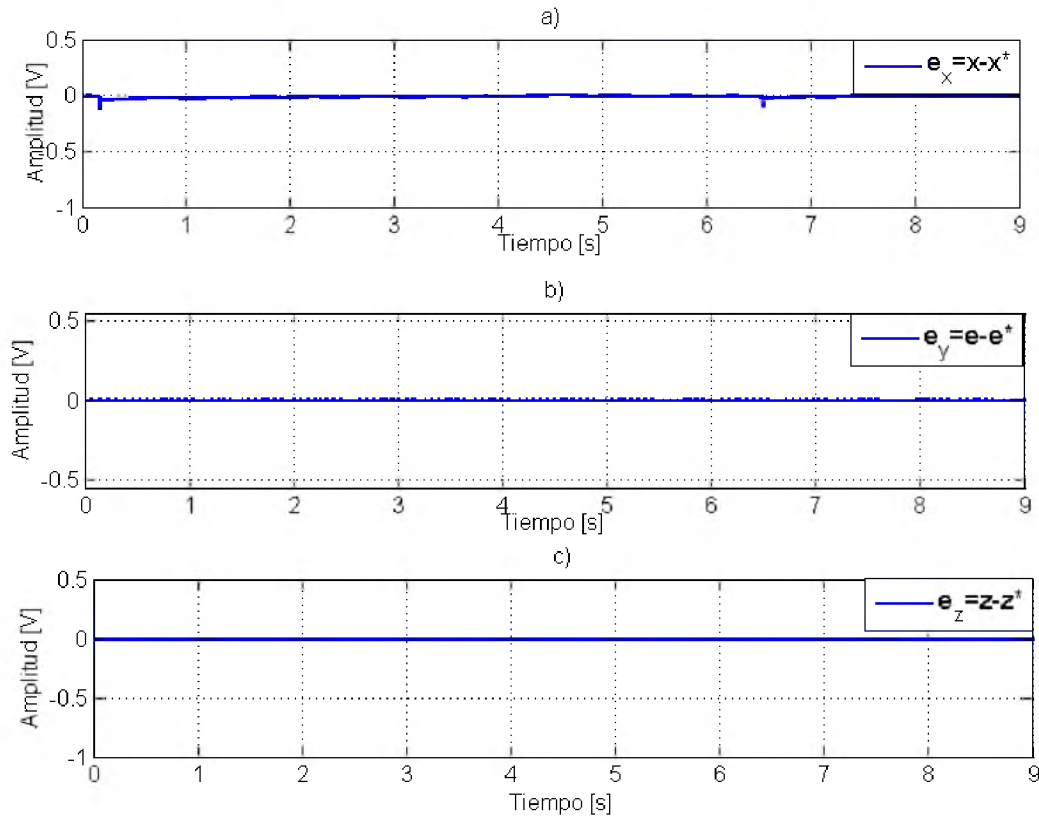


Figura 35, Graficas de error en la sincronización en dos circuitos de Chua condiciones iniciales cercanas.

Se observa, la diferencia de las dinámicas de los errores de la Figura 34 con los de la Figura 35, esta diferencia se debe a las condiciones iniciales, por lo que, se puede decir que seleccionando las condiciones iniciales adecuadas se puede acelerar la sincronización de los circuitos de Chua emisor-receptor.

La dinámica del error estima si los circuitos están sincronizados, es decir, la respuesta de los errores debe tender a cero. De lo contrario, no existiría sincronización.

En las siguientes figuras se muestran los estados acoplados entre los dos circuitos.

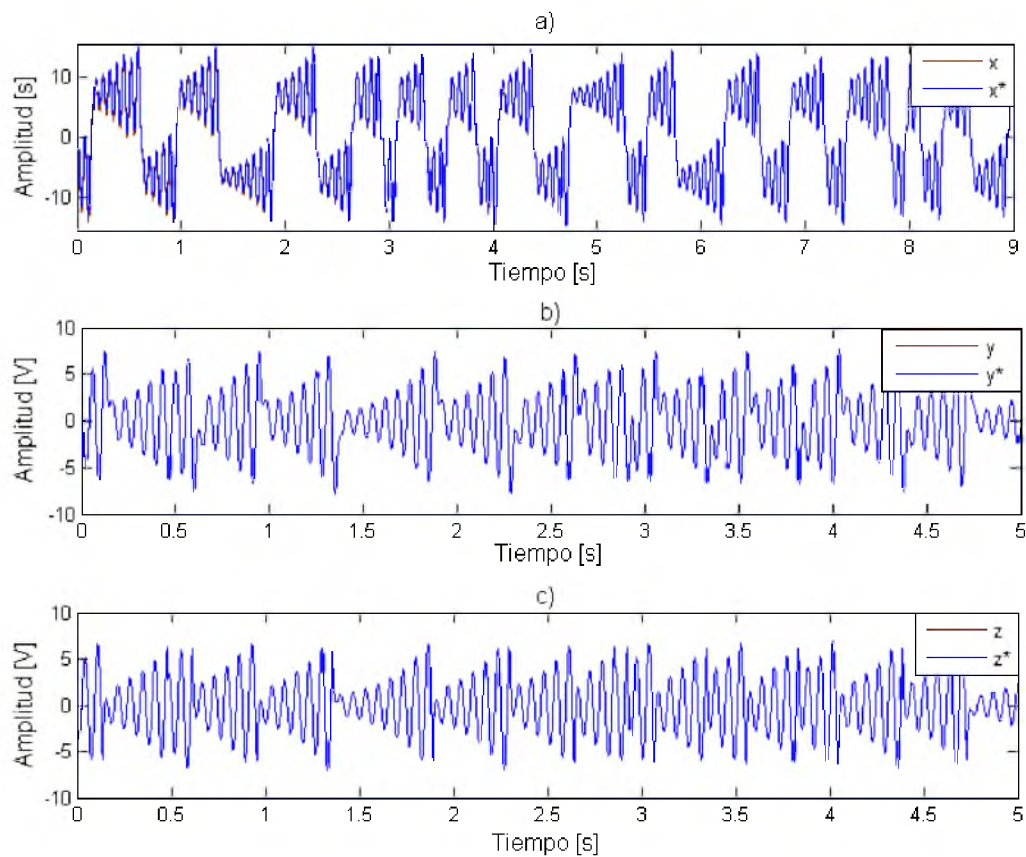


Figura 36. Señales de dos circuitos de Chua sincronizados.

La Figura 36a) pertenece a la comparación del estado ' x ' de circuito emisor y el receptor, en la Figura 34a) se observó que el error de sincronización para esta señal tardó aproximadamente 10 s, no obstante, se observa que aproximadamente en 15s, el estado ' x ' está sincronizado. En Figura 36b) y Figura 36c), se observa la sincronización entre los estados ' y ' y ' z ', respectivamente, a pesar de que las condiciones iniciales son diferentes para cada circuito, la sincronización parece ser instantánea para estos estados.

Dada la sincronización entre los dos circuitos, se realiza una prueba de comunicación segura en el apartado siguiente.

Encriptación de información usando caos

La encriptación de la información, se realiza, modulando la señal analógica que contiene la información (s_i), a una señal del sistema caótico emisor (x_e), una vez realizado este proceso, se envía la nueva señal encriptada al sistema caótico receptor (x_r), el cual, como ya se mencionó debe contener la misma dinámica que el sistema caótico emisor, además, estos sistemas (emisor-receptor) deben estar previamente sincronizados. A continuación, se muestra el proceso de encriptación realizado mediante simulación.

En la siguiente figura se muestra el diagrama de bloques necesario para llevar a cabo la comunicación segura.

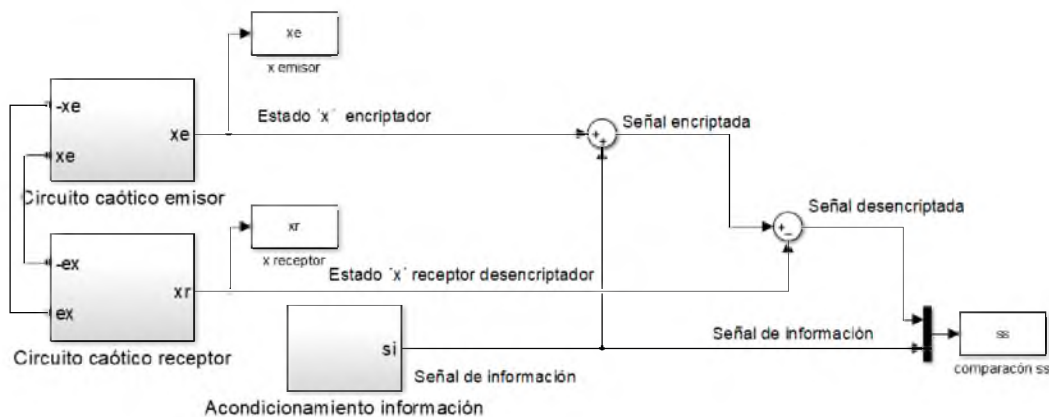


Figura 37. Diagrama de bloques para comunicación segura.

Al igual que en la simulación de sincronización, se realizan dos pruebas en la comunicación del sistema completo, esto, con el fin de observar el comportamiento dinámico de los sistemas ante una variación en las condiciones iniciales. Los resultados de la comunicación se muestran a continuación.

Simulación 1, condiciones iniciales en receptor iguales a cero.

El primer caso, la simulación 1 usa los parámetros de la Tabla 5. En la Figura 38a) se muestra la señal de información (si), esta señal es tipo senoidal de amplitud 1 V, y se activa en 12.5 s de simulación cuando los circuitos emisor-receptor se sincronizan. La Figura 38b) muestra la señal encriptada (se), esta señal es el resultado de la señal del estado 'x', (xe) modulada con la señal de información (si). En la Figura 38c) se muestra la señal recuperada (desencriptada, sd) por el sistema receptor, por último, en la Figura 38d) muestra error de recuperación (e_s), es decir se compara la señal original (si) y la señal desencriptada (sd). Se observa que cuando hay sincronización entre el emisor-receptor, el error es aproximadamente igual a cero.

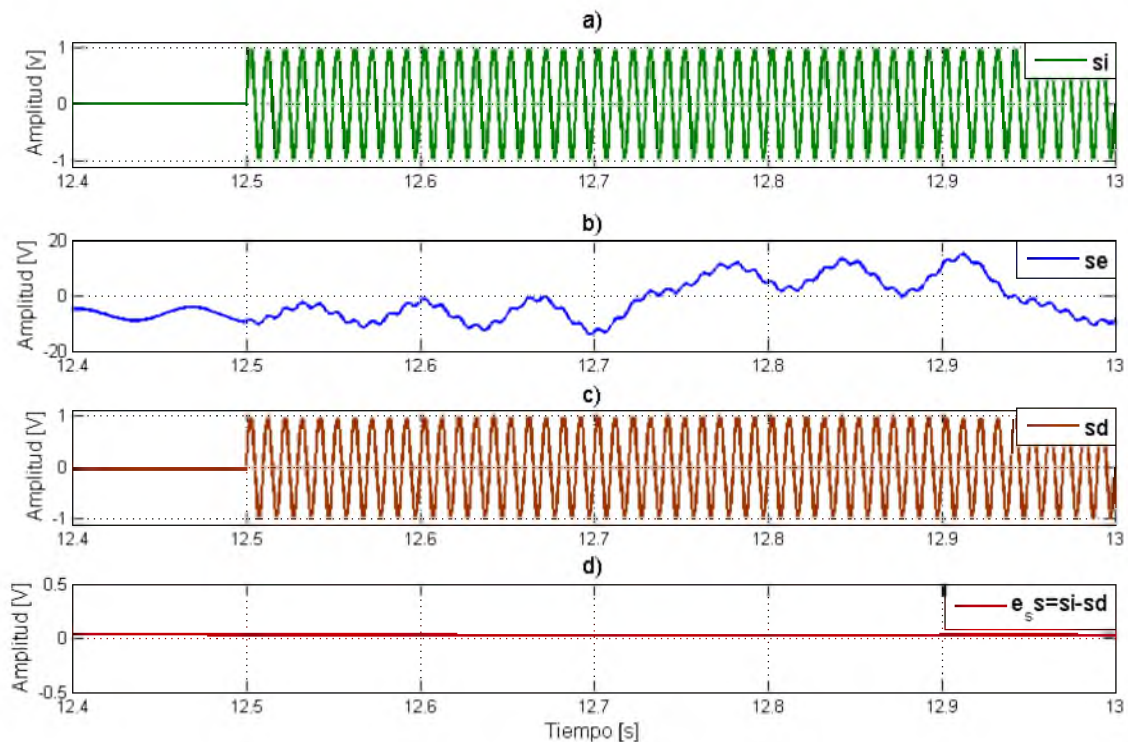


Figura 38. resultados de simulación de la comunicación 1.

En esta simulación, el circuito receptor contiene condiciones iniciales iguales a cero, los circuitos tardaron 12.5 segundos en hacer la sincronización para llevar a cabo la comunicación.

Simulación 2, condiciones iniciales en el receptor cercanas al del emisor

El segundo caso, lo único que cambia son las condiciones iniciales, es decir, el circuito receptor varía una milésima del valor en sus condiciones iniciales respecto a las del circuito emisor. En la Figura 39a) se muestra la señal de información (si), se activa en 2.5 s de simulación cuando los circuitos emisor-receptor se sincronizan. La Figura 39b) muestra la señal encriptada (se). En la Figura 39c) se muestra la señal recuperada (desencriptada, sd) por el sistema receptor, por último, en la Figura 39d) muestra error de recuperación (e_s), se observa que cuando hay sincronización entre el emisor-receptor, el error es aproximadamente igual a cero.

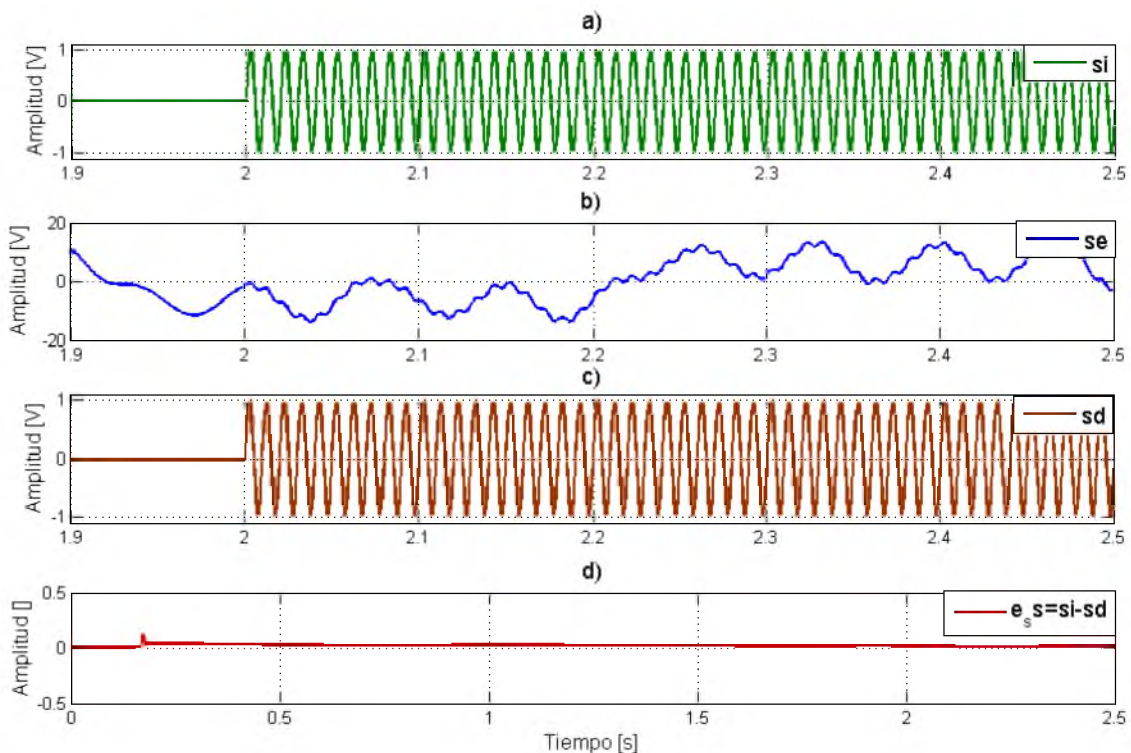


Figura 39. resultados de simulación de la comunicación 2.

Para esta simulación donde el circuito receptor contiene condiciones iniciales iguales a cero, tardó 12.5 segundos en hacer la sincronización para llevar a cabo la comunicación

Capítulo V: Conclusiones

Se estudió el funcionamiento del caos en sistemas dinámicos, sus principales características y su aplicación en las comunicaciones seguras.

Se Analizó el funcionamiento del oscilador caótico de Chua, se obtuvo su dinámica por ecuaciones diferenciales no lineales y a partir de este modelo se emula su comportamiento por medio de funciones no lineales saturadas (SNLF).

Se realizó la dinámica completa del circuito de Chua basado en funciones no lineales saturadas en simulación con el diagrama electrónico, implementando amplificadores operacionales, también se indican algunas consideraciones que se deben tomar en cuenta al momento de usar los amplificadores operacionales en el diodo de Chua.

Se comprobó la aleatoriedad del circuito electrónico de Chua y se cuantificó el valor de los exponentes de Lyapunov. Lo que permitió indicar que el sistema es caótico. Se demostró que con un circuito electrónico de comparadores se pueden generar secuencias aleatorias a partir de cualesquiera de sus estados.

Se realizó la simulación del sistema completo (el cual consiste de un circuito emisor y receptor en una sincronización unidireccional y se emplea una señal analógica simulando información), en esta simulación se determinó que el tiempo de sincronización está ligado a las condiciones iniciales de ambos

circuitos (emisor-receptor), en donde se observó que cuanto más cercanas sean, menor es el tiempo que tardan en sincronizar los circuitos.

En conclusión, este trabajo de tesis se centró en el desarrollo de un sistema de comunicación segura, utilizando el circuito caótico de Chua como encriptación, el cual se basó en funciones no lineales saturadas. La implementación se llevó a cabo exclusivamente en simulación, utilizando amplificadores operacionales para emular el comportamiento del circuito caótico de Chua. La comunicación se estableció de forma unidireccional. Este enfoque permitió explorar la viabilidad y eficacia de utilizar sistemas caóticos en la seguridad de las comunicaciones. Este trabajo proporciona una base sólida para futuras investigaciones en el campo de la seguridad de las comunicaciones, con posibles aplicaciones en la protección de datos sensibles y la transmisión segura de información.

Bibliografía

- [1] I. A. Simón, La teoria del caos, España, 2023.
- [2] C. W. Shannon, A Mathematical Theory of Communication, EEUU, 1948.
- [3] A. L. Valdes, Prueba de eficiencia de contra caos basado en exponentes de Luapunov, México, 2021.
- [4] R. X. R. IZA, Estudio de los exponentes de Lyapunov para, Quito, Ecu., 2020.
- [5] L. P. Pérez, Introducción a la Dinámica caótica y aplicacion a modelos neuronales, Portugal, 2015.
- [6] A. R. Martnez, Sincronización generalizada de sistemas caóticos utilizando el elemento primitivo diferencial, México, 2013.
- [7] A. M. Cano, Diseño e implementación en un FPGA de un sistema de transmisión de información con enmascaramiento caótico, Tijuana, B.C.: IPN, 2018.
- [8] E. M. N. López, «La naturaleza, las matematicas,la ingienería y el caos,» *Revista chilena de ingeniería*, vol. 18, nº 1, pp. 5-7, 2010.
- [9] L. M. P. a. T. L. Carrol, Synchronization in chaotic systems, Washington, 1980.
- [10] O. G. Fernández, Tecnicas de sincronizacion de osciladores caóticos y su implementación electrónica, Puebla : SN, 2018.
- [11] M. B. A. G. F. Alcala Martinez, Circuito de Chua en la sincronizacion de los sistemas caóticos, México, 2013.
- [12] H. d. L. Hidalgo, Diseño de osciladores caóticos integrados, Puebla, 2018.
- [13] L. O. Chua, The double scroll family, EEUU: IEEE, 1986.

- [14] A. B.-R. R. Y. S.-A. G. E.-L. A.-T. J. N.-P. J. F. Cortés-Avilez, Diseño de sistemas caóticos de multi-enrollamientos y multi-direcciones usando SNLF, Baja California, 2018.
- [15] H. C. R. López, Estudio y Diseño de un Oscilador Caótico para Aplicación en Robot Móvil, Chiapas: INAOE, 2013.
- [16] T. G. Chávez, Estudio Experimental de Generación de Números Aleatorios Basados en Circuitos Caóticos, Puebla: BUAP, 2014.
- [17] M. G. d. I. Fuente, GENERACIÓN DE NÚMEROS ALEATORIOS FISICOS EN DISPOSITIVOS ELECTRÓNICOS, VALLADOLID, ESPAÑA, 2016.
- [18] L. A. Q. Téllez, ESTUDIO DE LAS PROPIEDADES DE LOS SISTEMAS DINÁMICOS COMPLEJOS Y APLICACIONES, Mexico, 2016.
- [19] C. P. Castillo, SINCRONIZACIÓN DE OSCILADORES DE LORENZ POR FORMAS HAMILTONIANAS, Baja california, México: CICESE, 2001.
- [20] A. G. F. A. M. M. Berenice, Circuito de Chua en la sincronización de los sistemas caóticos, Mexico, 2013.
- [21] D. K. V. Morales, Encriptador de señal mediante osciladores caóticos implementados en FPGA, Puebla, 2016.

Anexos

Anexo 1. Diagrama de bloques, variables de estado.

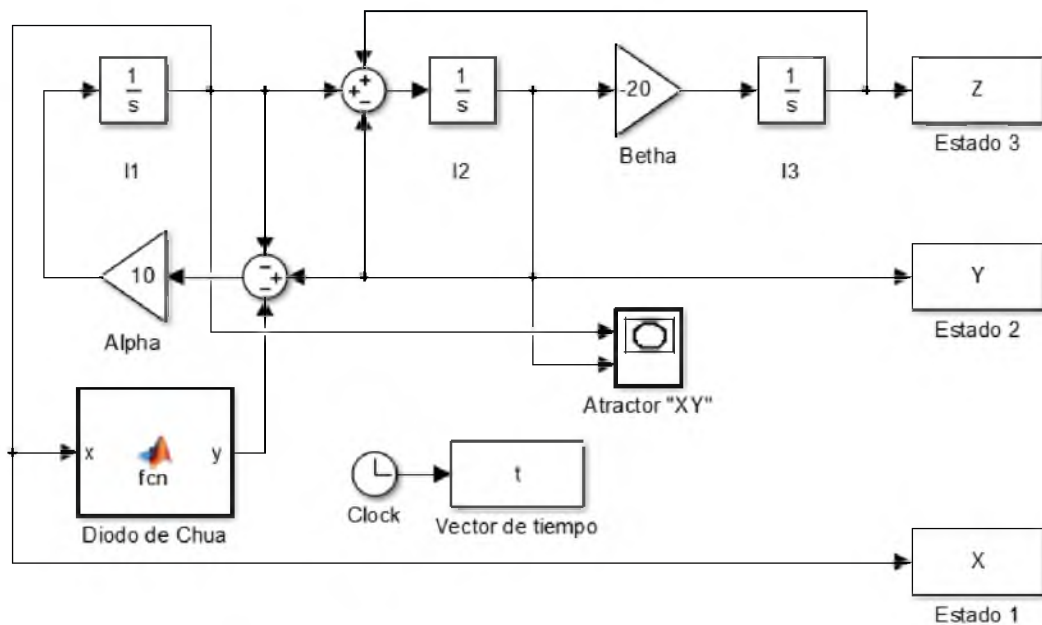


Imagen 1. Diagrama de bloques de variables de estado del diodo de Chua

La función Diodo de Chua está regida por los siguientes segmentos de código

```
function y = fcn(x)
```

```
a=-1.758;
```

```
b=-0.8248;
```

```
y = b*x+(1/2)*(a-b)*(abs(x+1)-abs(x-1));
```

donde y es la función (17) que describe el comportamiento del diodo de Chua.

Anexo 2. Diagrama de bloques del circuito de Chua basado en funciones no lineales saturadas.

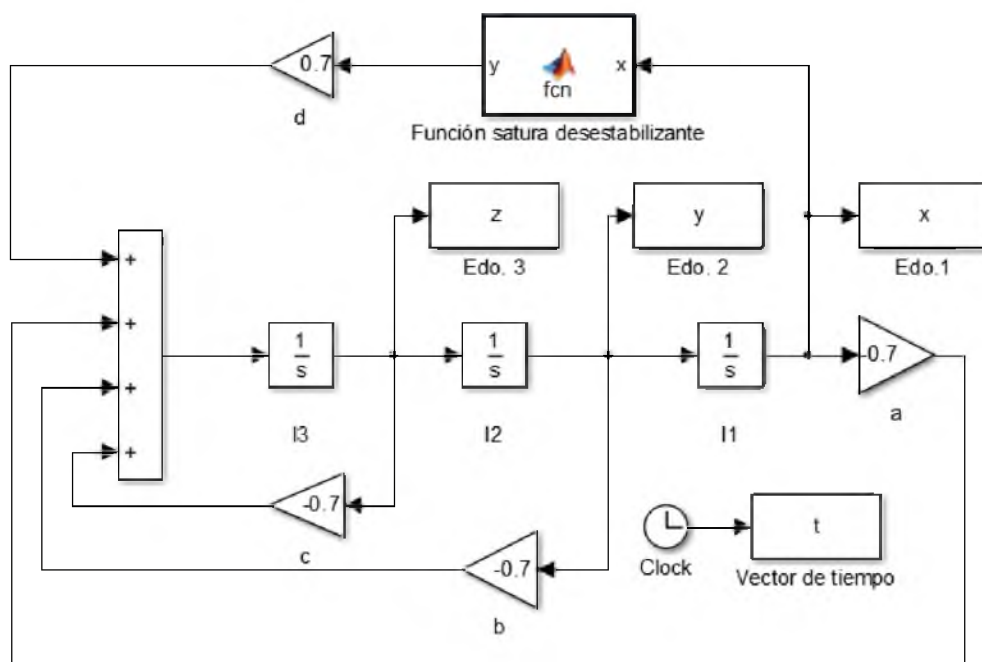


Imagen 2. diagrama de bloques del circuito de Chua basado en SNLF.

Anexo 3. Esquema eléctrico del diodo de Chua.

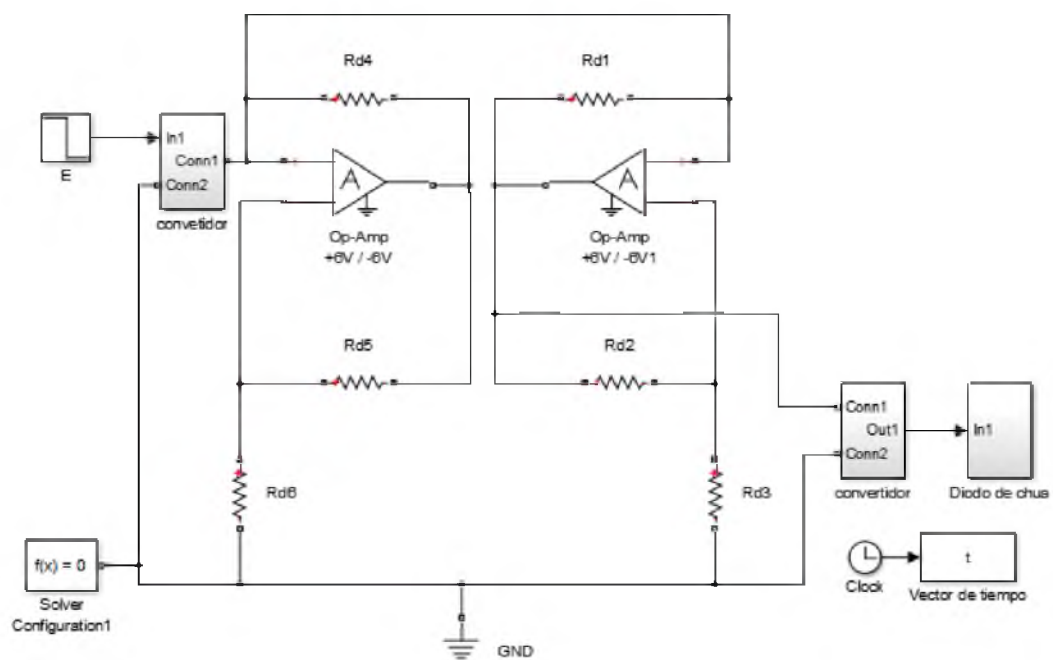


Imagen 3. Esquema electrónico del diodo de Chua.

Anexo 4. Diagrama de bloques, circuito caótico de Chua con amplificadores operacionales en el inductor y el diodo de Chua (Nd).

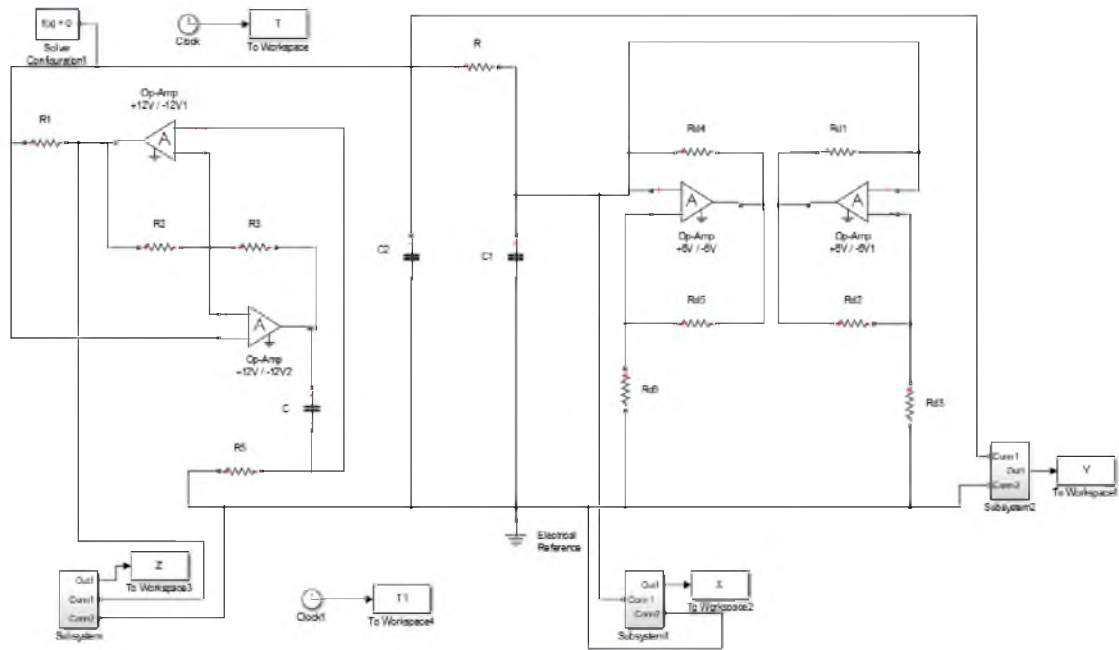


Imagen 4. Esque electrónico del circuito caotico de Chua con el diodo e inductor emulados con OpAmps.

Anexo 5. Esquema del circuito caótico de Chua implementado con amplificadores operacionales.

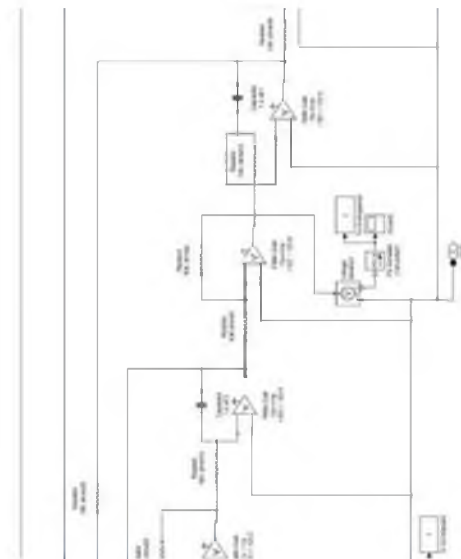


Imagen 5. Circuito electrónico del circuito de Chua implementado con OpAmps.

Anexo 6. Diagrama de bloques para generación de Bits

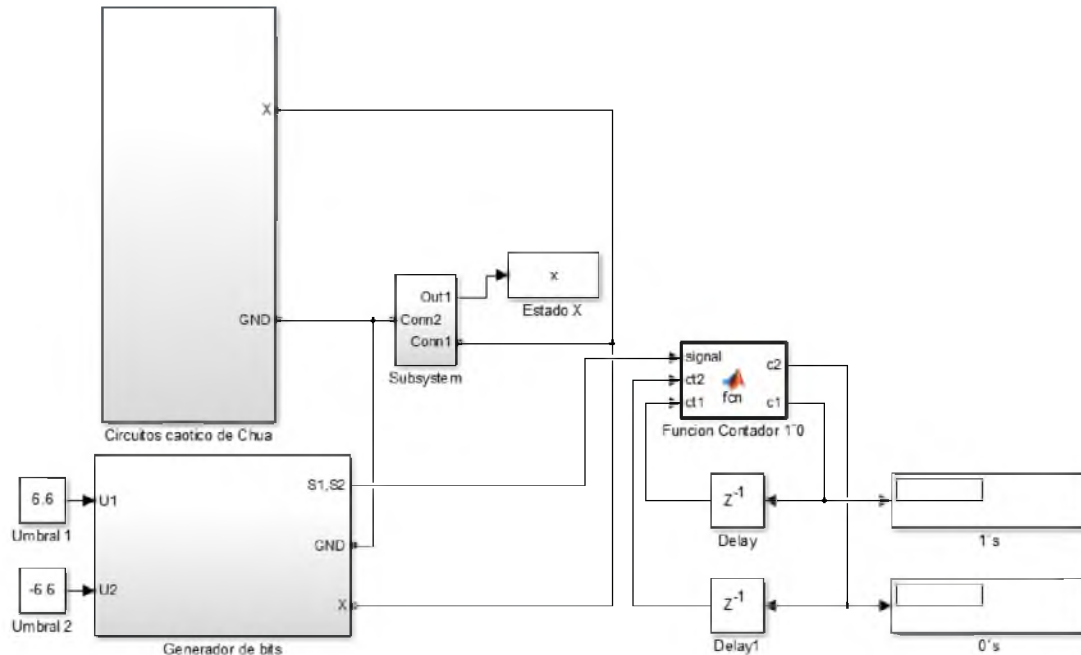


Imagen 6. Diagrama de bloques para generación de bits de una señal caótica del circuito de Chua.

La Función Contador 1'0, está determinada por el siguiente código.

```
function [c2,c1] = fcn(signal,ct2,ct1)
%#codegen
if(signal>0.5)
    c1=ct1+1;
else
    c1=ct1;
end
if(signal<0.00001)
    c2=ct2+1;
else
    c2=ct2;
end
end
```

Anexo 7. Circuitos acoplamos unidireccionalmente para sincronización

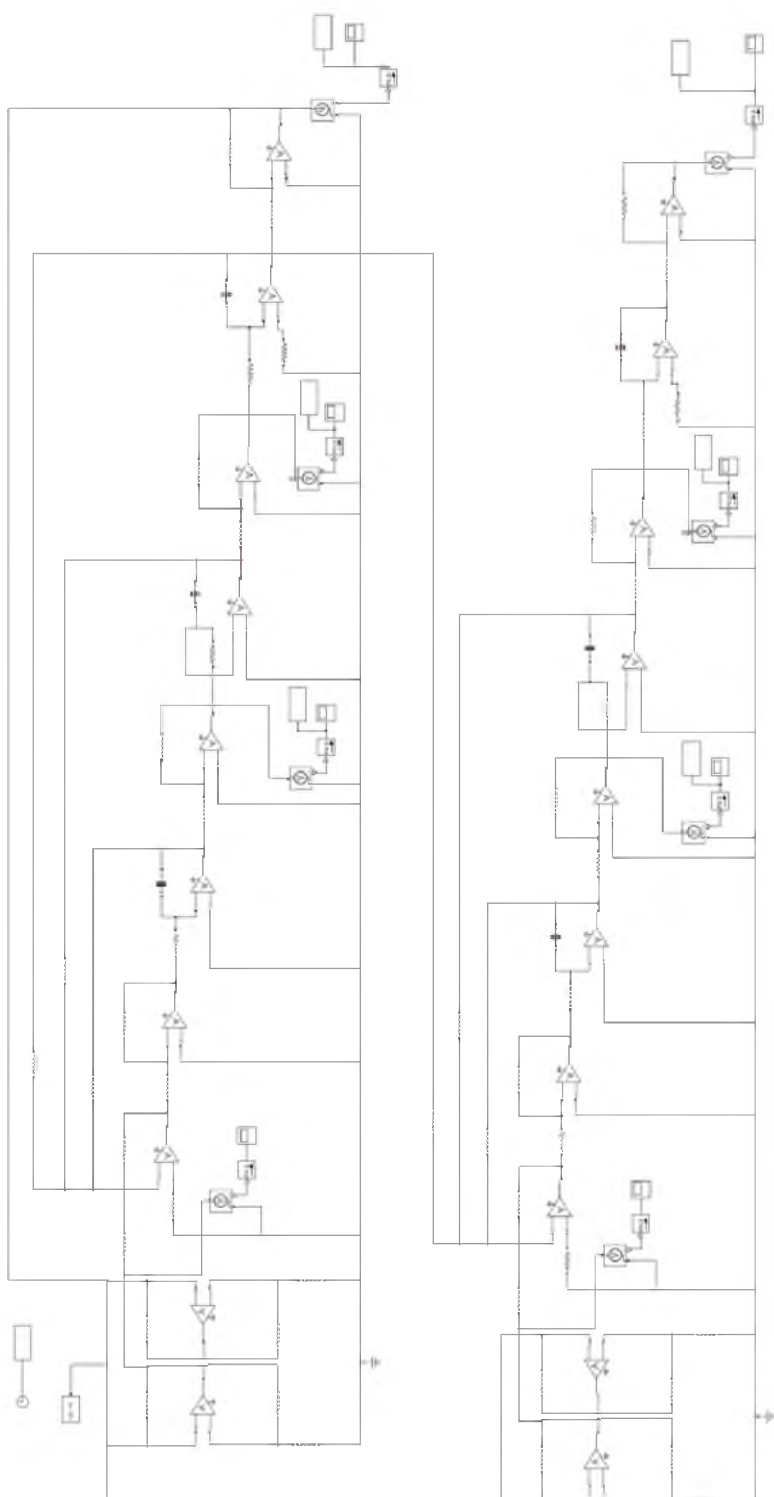


Imagen 7. Esquema electrónico de dos circuitos de Chua sincronizados unidireccionalmente.