



EDUCACIÓN

SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO

Tecnológico Nacional de México

**Centro Nacional de Investigación
y Desarrollo Tecnológico**

Tesis de Maestría

**Diseño de un observador de tiempo finito con
aplicación a sistemas de comunicación**

presentada por

Ing. Evelyn Bahena Bustamante

como requisito para la obtención del grado de

**Maestra en Ciencias en
Ingeniería Electrónica**

Director de tesis

Dra. Gloria Lilia Osorio Gordillo

Codirector de tesis

Dr. Rodolfo Amalio Vargas Méndez

Cuernavaca, Morelos, México. Agosto de 2025.



Centro Nacional de Investigación y Desarrollo tecnológico
Departamento de Ingeniería Electrónica

Cuernavaca, Mor; 04 julio 2025

Oficio No. DIE/101/2025

Asunto: Aceptación de documentos.

DR. CARLOS MANUEL ASTORGA ZARAGOZA
SUBDIRECTOR ACADÉMICO
PRESENTE

Por este conducto, los integrantes de Comité Tutorial de la **C. Evelyn Bahena Bustamante**, con número de control **M23CE094** de la Maestría en Ciencias en Ingeniería Electrónica, le informamos que hemos revisado el trabajo de tesis profesional titulado **"Diseño de un observador de tiempo finito con aplicación a sistemas de comunicación"**, y hemos encontrado que se han realizado todas las correcciones y observaciones que se le indicaron, por lo que hemos acordado aceptar el documento de tesis y le solicitamos la autorización de Impresión definitiva.

DIRECTOR DE TESIS

Dra. Gloria Lilia Osorio Gordillo
Doctora en Ciencias en Ingeniería Electrónica
Cédula profesional 9968714

CODIRECTOR DE TESIS

Dr. Rodolfo Amalio Vargas Méndez
Doctor en Ciencias en Ingeniería Electrónica
Cédula profesional 9526506

REVISOR 1

Dr. Carlos Manuel Astorga Zaragoza
Doctor en Ingeniería Electrónica
Cédula profesional 5505019

REVISOR 2

Dr. Juan Reyes Reyes
Doctor en Ciencias en la Especialidad de Control Automático
Cédula profesional 4214833

C.p. Mtra. Verónica Sotelo Boyas. Jefa del Departamento de Servicios Escolares
Estudiante
JGM/kmqh



2025
Año de
La Mujer
Indígena

Interior Internado Palmira S/N, Col. Palmira,
C. P. 62496, Cuernavaca, Morelos Tel. 01 (777) 3627776, ext. 2234,
e-mail: ce@cenidet.tecnm.mx

cenidet
Centro Nacional de Investigaciones
y Desarrollo Tecnológico





Centro Nacional de Investigación y Desarrollo tecnológico
Subdirección Académica

Cuernavaca Mor, 04/julio/2025

Oficio No. SAC/179/2025

Asunto: Autorización de impresión de tesis

EVELYN BAHENA BUSTAMANTE
CANDIDATA AL GRADO DE MAESTRA EN CIENCIAS
EN INGENIERÍA ELECTRÓNICA
P R E S E N T E

Por este conducto, tengo el agrado de comunicarle que el Comité Tutorial asignado a su trabajo de tesis titulado **"Diseño de un observador de tiempo finito con aplicación a sistemas de comunicación"**, ha informado a esta Subdirección Académica, que están de acuerdo con el trabajo presentado. Por lo anterior, se le autoriza a que proceda con la impresión definitiva de su trabajo de tesis.

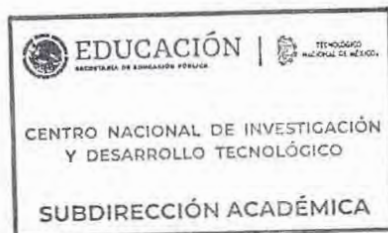
Esperando que el logro del mismo sea acorde con sus aspiraciones profesionales, reciba un cordial saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®

"Conocimiento y Tecnología al Servicio de México"

CARLOS MANUEL ASTORGA ZARAGOZA
SUBDIRECTOR ACADÉMICO



c.c.p. Departamento de Ingeniería Electrónica
Departamento de Servicios Escolares

CMAZ/lmz



2025
Año de
La Mujer
Indígena

Interior Internado Palmira S/N, Col. Palmira,
C. P. 62490, Cuernavaca, Morelos Tel. 01 (777) 3627770, ext. 4104,
e-mail: acad_cenidet@tecnm.mx tecnm.mx | cenidet.tecnm.mx

cenidet
Centro Nacional de Investigación
y Desarrollo Tecnológico



Dedicatoria

“Dedico esta tesis a Dios, por ser mi guía y fortaleza en cada etapa de este proceso; a mi familia, por su amor incondicional, su apoyo constante y por creer siempre en mí; y a mis amigos, por su compañía, palabras de aliento y comprensión en los momentos más desafiantes”.

Agradecimientos

Agradezco primeramente a Dios, por haberme dado la vida, la fortaleza, la sabiduría y la fe necesarias para concluir esta etapa tan importante en mi formación académica.

A mis padres, Margarita Bustamante Urióstegui y Jorge Luis Bahena Cano, por su amor incondicional, por enseñarme con su ejemplo el valor del esfuerzo y por apoyarme en todo momento. A mi hermana, Karyme Bahena Bustamante, por su cariño, comprensión y por ser una inspiración constante en mi vida.

A mi asesora de tesis, la Dra. Gloria Lilia Osorio Gordillo, por su orientación, paciencia y compromiso durante el desarrollo de este trabajo, y al Dr. Rodolfo Amalio Vargas Méndez, mi co-asesor, por su constante apoyo a lo largo de este proceso.

A mis amigos, por estar presentes en los momentos más importantes, por sus palabras de aliento y por acompañarme en este camino con alegría y solidaridad.

A mis revisores, el Dr. Carlos Manuel Astorga Zaragoza y el Dr. Juan Reyes Reyes, por su tiempo, dedicación y observaciones que enriquecieron este trabajo.

Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI) por el apoyo económico brindado durante este periodo para así poder culminar con mis estudios. Así también al CENIDET por permitirme ser parte de ellos y hacer uso del plantel.

Resumen

En esta tesis se propone el diseño de un esquema criptográfico basado en el enmascaramiento caótico utilizando el sistema de Lorenz, modelado mediante el enfoque Takagi-Sugeno. El objetivo principal es garantizar la comunicación segura sin alterar la estructura del mensaje, superando los desafíos que presentan los sistemas caóticos en cuanto a sincronización y estimación de estados.

La investigación aborda el desarrollo de un sistema transmisor y dos tipos de receptores: un observador proporcional y un observador con convergencia en tiempo finito. Estos observadores permiten estimar con precisión las variables de estado necesarias para descifrar el mensaje, siendo el observador en tiempo finito especialmente relevante al asegurar la sincronización en un intervalo acotado, lo cual es esencial para evitar pérdida de información.

El trabajo destaca por su originalidad en el diseño de los observadores aplicados a sistemas caóticos con fines criptográficos, aportando soluciones que no se han reportado en la literatura existente. Las simulaciones realizadas validan la viabilidad del esquema propuesto bajo condiciones ideales, contribuyendo al fortalecimiento de la seguridad en comunicaciones mediante técnicas novedosas de control y sincronización basadas en dinámicas no lineales.

Palabras clave: Sistemas de comunicación, sistema caótico, Observador Proporcional, Observador de tiempo finito, Lorenz

Abstract

This thesis proposes the design of a cryptographic scheme based on chaotic masking using the Lorenz system, modeled through the Takagi-Sugeno approach. The main objective is to ensure secure communication without altering the structure of the transmitted message, overcoming key challenges in chaotic systems such as synchronization and state estimation.

The research develops a transmitter system and two types of receivers: a proportional observer and a finite-time convergence observer. These observers enable precise estimation of the system's state variables required for message decryption. The finite-time observer is particularly relevant as it ensures synchronization within a bounded time, which is critical to avoid information loss during transmission.

This work stands out for its originality in the design of observers applied to chaotic systems for cryptographic purposes, offering solutions not previously reported in the consulted literature. The proposed scheme is validated through simulations under ideal and controlled conditions, contributing to enhanced communication security through innovative control and synchronization techniques based on nonlinear dynamics.

Índice general

Índice general	v
Lista de figuras	viii
Lista de tablas	x
Nomenclatura	xi
1 Introducción	1
1.1 Planteamiento del problema	1
1.2 Objetivos	2
1.2.1 Objetivo general	2
1.2.2 Objetivos particulares	2
1.3 Estudio del estado del arte	3
1.3.1 Cifrado en sistemas caóticos	3
1.3.2 Modelo Takagi-Sugeno	4
1.3.3 Observadores para sistemas caóticos	5
1.4 Alcances	7
1.5 Originalidad	7
1.6 Estructura del documento	8
2 Marco Teórico	10
2.1 Sistemas de comunicación	10
2.2 Sistemas caóticos	12
2.3 Teoría de sistemas Takagi-Sugeno	13
2.3.1 Enfoque basado en sector no lineal	15

2.3.2	Observabilidad en modelos Takagi-Sugeno	16
2.4	Observadores	17
2.5	Conclusiones del capítulo	19
3	Representación Takagi-Sugeno del sistema caótico de Lorenz	20
3.1	Modelo no lineal del sistema caótico	20
3.1.1	Simulación del sistema no lineal	20
3.2	Representación Takagi-Sugeno del sistema caótico	22
3.2.1	Simulación del modelo no lineal y del modelo Takagi-Sugeno	24
3.3	Conclusiones del capítulo	26
4	Diseño del sistema transmisor	27
4.1	Objetivo de diseño	27
4.2	Observador Luenberguer	28
4.2.1	Análisis de estabilidad del observador	29
4.2.2	Simulación del sistema transmisor	30
4.3	Conclusiones del capítulo	33
5	Diseño del observador proporcional	35
5.1	Objetivo de diseño	35
5.2	Observador Proporcional	35
5.2.1	Parametrización de las matrices del observador proporcional	37
5.2.2	Análisis de estabilidad del observador	38
5.2.3	Simulación del observador proporcional	39
5.2.4	Estimación del mensaje	43
5.3	Conclusiones del capítulo	44
6	Diseño del observador con convergencia en tiempo finito	45
6.1	Objetivo de diseño	45
6.2	Observador maestro-esclavo	45
6.2.1	Parametrización del observador	46
6.2.2	Simulación del observador	48
6.2.3	Estimación del mensaje	52

6.3	Conclusiones del capítulo	53
7	Enmascaramiento Caótico de Señales de Audio: Cifrado y Descifrado	54
7.1	Objetivo de diseño	54
7.1.1	Algoritmo de cifrado caótico	55
7.1.2	Algoritmo de descifrado caótico	57
7.1.3	Validación de cifrado y descifrado caótico	58
7.2	Conclusión del capítulo	63
8	Conclusiones generales	64
8.1	Trabajos futuros	65
	Bibliografía	66

Lista de figuras

2.1	Diagrama de un sistema de comunicación	11
2.2	Representación general de un observador.	18
3.1	Sistema caótico de Lorenz	21
3.2	Estados del sistema no lineal	22
3.3	Comparación del estado $x_1(t)$ del modelo NL y T-S	24
3.4	Comparación del estado $x_2(t)$ del modelo NL y T-S	25
3.5	Comparación del estado $x_3(t)$ del modelo NL y T-S	25
3.6	Funciones de pertenencia del sistema Takagi-Sugeno	26
4.1	Mensaje enmascarado	32
4.2	Comparación del estado $x_1(t) + p(t)$ del modelo NL y T-S	32
4.3	Comparación del estado $x_2(t) + p(t)$ del modelo NL y T-S	33
4.4	Comparación del estado $x_3(t) + p(t)$ del modelo NL y T-S	33
5.1	Comparación del estado $x_1(t)$ del Observador Proporcional y Sistema No Lineal	40
5.2	Comparación del estado $x_2(t)$ del Observador Proporcional y Sistema No Lineal	41
5.3	Comparación del estado $x_3(t)$ del Observador Proporcional y Sistema No Lineal	41
5.4	Error del Observador Proporcional con el Sistema No Lineal	42
5.5	Mensaje estimado con el Observador Proporcional	44
6.1	Comparación del estado $x_1(t)$ del Observador Maestro-Esclavo y Sistema No Lineal	49
6.2	Comparación del estado $x_2(t)$ del Observador Maestro-Esclavo y Sistema No Lineal	50
6.3	Comparación del estado $x_3(t)$ del Observador Maestro-Esclavo y Sistema No Lineal	50
6.4	Error del Observador Maestro-Esclavo con el Sistema No Lineal	51
6.5	Mensaje estimado con el Observador Maestro-Esclavo	52

7.1	Diagrama del algoritmo de cifrado caótico	56
7.2	Diagrama del algoritmo de descifrado caótico	58
7.3	Señal de audio Hola Mundo con voz robotizada	59
7.4	Señal binaria correspondiente al audio Hola Mundo con voz robotizada	59
7.5	Señal de audio recuperada Hola Mundo con voz robotizada	60
7.6	Señal de audio de secuencia de números del 1 al 6	60
7.7	Señal binaria correspondiente al audio de secuencia de números del 1 al 6	61
7.8	Señal de audio recuperada de secuencia de números del 1 al 6	61
7.9	Señal de audio Hola Mundo con entonación natural	62
7.10	Señal binaria correspondiente al audio Hola Mundo con entonación natural	62
7.11	Señal de audio recuperada Hola Mundo con entonación natural	63

Lista de tablas

Tabla 5.1	Valores de los índices de desempeño del observador proporcional.	42
Tabla 6.1	Valores de los índices de desempeño del observador maestro-esclavo	51

Notación y acrónimos

Conjuntos

$\mathbb{R}$	Conjunto de todos los números reales.
$\mathbb{R}^n$	Conjunto de vectores reales de dimensión n ,
$\mathbb{R}^{n \times n}$	Conjunto de vectores reales de dimensión $n \times n$.

Notación referente a vectores y matrices

$A > 0$	Matriz real A simétrica positiva definida.
$A < 0$	Matriz real A simétrica negativa definida.
A^+	Inversa generalizada de la matriz A .
A^T	Transpuesta de la matriz A .

Acrónimos

LMI	Desigualdad Matricial Lineal.
PO	Observador Proporcional.
T-S	Takagi-Sugeno.

Capítulo 1

Introducción

Desde tiempos remotos, la humanidad ha buscado garantizar la confidencialidad y la integridad de la información, utilizando diversos métodos para asegurar la privacidad en las comunicaciones. Desde los cifrados antiguos, como la escítala espartana o el cifrado de César, hasta los sistemas criptográficos modernos, la evolución de la criptografía ha estado estrechamente ligada al desarrollo tecnológico y a la creciente necesidad de proteger información crítica.

En la actualidad, con el auge de las tecnologías digitales y el aumento exponencial en la transmisión de datos, la seguridad en las comunicaciones se ha convertido en una prioridad fundamental. Esta necesidad ha impulsado la búsqueda de métodos criptográficos más robustos, capaces de resistir ataques cada vez más sofisticados. En este contexto, los sistemas caóticos han emergido como una alternativa prometedora en el diseño de esquemas criptográficos, gracias a su sensibilidad a las condiciones iniciales y a su comportamiento aparentemente impredecible.

Particularmente, el sistema de Lorenz ha sido objeto de estudio por sus propiedades dinámicas, que permiten el enmascaramiento efectivo de señales. Sin embargo, para que estos sistemas sean aplicables en entornos reales, se requiere garantizar la sincronización precisa entre emisor y receptor, así como mantener la integridad de la estructura del mensaje transmitido.

1.1. Planteamiento del problema

El uso de sistemas caóticos en criptografía ha demostrado ser una alternativa viable para el desarrollo de esquemas de comunicación segura. No obstante, su implementación práctica enfrenta retos

técnicos importantes, entre ellos, la correcta sincronización del sistema caótico entre el transmisor y el receptor, y la estimación precisa de las variables de estado para permitir la recuperación del mensaje sin alteraciones.

Una de las principales dificultades radica en el diseño de receptores capaces de sincronizarse con el sistema emisor en un tiempo finito, ya que durante este proceso no debe haber pérdida de información. Si se omite una parte crítica del mensaje mientras ocurre la sincronización, dicha información no podrá recuperarse, comprometiendo así la integridad y utilidad del mensaje transmitido.

Ante este panorama, surge la necesidad de diseñar un esquema criptográfico basado en el enmascaramiento caótico utilizando el sistema de Lorenz, modelado mediante el enfoque Takagi-Sugeno, junto con la implementación de dos tipos de observadores: uno proporcional y otro en tiempo finito. Esta propuesta busca superar las limitaciones actuales, aportando una solución innovadora y eficaz en el ámbito de la criptografía basada en sistemas caóticos.

1.2. Objetivos

1.2.1. Objetivo general

Diseñar un esquema criptográfico basado en el enmascaramiento caótico mediante el enfoque Takagi-Sugeno y un observador de tiempo finito que permita garantizar la comunicación sin alterar la estructura del mensaje.

1.2.2. Objetivos particulares

- Modelar el sistema caótico de Lorenz utilizando el enfoque Takagi Sugeno.
- Diseñar un sistema transmisor del mensaje basado en el uso de sistemas caóticos en su representación.
- Diseñar un observador proporcional como receptor que permita estimar las variables de estado del sistema de Lorenz.
- Diseñar un observador en tiempo finito como receptor que permita estimar las variables de estado del sistema de Lorenz, asegurando la sincronización en un tiempo determinado.

1.3. Estudio del estado del arte

1.3.1. Cifrado en sistemas caóticos

La comunicación ha sido un pilar fundamental en el desarrollo de las sociedades, ya que la integridad del mensaje es crucial para garantizar su correcta recepción. Para protegerlo de posibles interceptaciones, manipulaciones o suplantaciones por parte de individuos no autorizados, se recurre a la criptografía, un componente esencial desde tiempos remotos (Bonilla, 2021).

La criptografía, cuyo propósito principal es salvaguardar datos críticos almacenados en dispositivos o transmitidos a través de canales inseguros (Alenezi et al., 2020), despliega su importancia en la era digital actual. Un sistema de comunicación se considera seguro cuando es capaz de preservar la confidencialidad de la información ante cualquier intento de acceso no autorizado (Augustine et al., 2015).

Durante las últimas dos décadas, se ha prestado especial atención por parte de científicos e ingenieros en las aplicaciones del caos en el ámbito de las comunicaciones seguras, debido a que estos son sistemas no lineales que exhiben trayectorias limitadas y un comportamiento no periódico. Este comportamiento se caracteriza por oscilaciones erráticas o irregulares que no se repiten, y se manifiesta en condiciones deterministas, ya que siguen leyes bien definidas sin ninguna aleatoriedad (Rodríguez Liñán and León Morales, 2007a).

Otra característica, dada la naturaleza de las señales caóticas, es que tienden a ser de banda ancha, similares al ruido y difíciles de prever; se pueden emplear en diversos contextos para ocultar formas de onda que contengan información (Cuomo et al., 1993a).

Los sistemas criptográficos basados en el caos poseen múltiples características que los hacen idóneos para cifrar datos multimedia como: imágenes, vídeos o archivos de audio. Algunas de estas características incluyen un comportamiento impredecible, sensibilidad a los parámetros de control y condiciones iniciales (Albahrani, 2017).

El trabajo de Alenezi et al. (2020), expone los principios fundamentales del cifrado simétrico y

asimétrico, resaltando que ambos mecanismos se basan en el uso de llaves criptográficas para garantizar la seguridad de la información. En el caso del cifrado simétrico, se utiliza una única llave secreta compartida entre el emisor y el receptor para llevar a cabo tanto el cifrado como el descifrado de los datos. Por su parte, el cifrado asimétrico emplea un par de llaves —una pública y una privada— que, al estar matemáticamente relacionadas, permiten una transmisión más segura, aunque con un rendimiento inferior en comparación con el enfoque simétrico.

1.3.2. Modelo Takagi-Sugeno

En los últimos años, el interés por el control de sistemas dinámicos utilizando lógica difusa ha aumentado notablemente debido a su capacidad para abordar la incertidumbre. Este enfoque se ha destacado como una herramienta valiosa en el diseño de controladores para sistemas complejos, siendo el diseño de control basado en modelos difusos Takagi-Sugeno (T-S) fundamental en diversas aplicaciones (Wang et al., 2005).

El modelo dinámico difuso T-S se origina por Takagi y Sugeno (Takagi and Sugeno, 1985), el cual representa los sistemas dinámicos no lineales mediante reglas IF-THEN difusas en las cuales las dinámicas locales en diferentes regiones del espacio de estado se representan mediante modelos lineales.

Se ha evidenciado que los modelos difusos T-S tienen la capacidad de aproximar con precisión cualquier función no lineal suave en cualquier región específica del espacio, independientemente del grado de precisión requerido (Al-Hadithi et al., 2012).

Los sistemas caóticos son descritos como sistemas autónomos debido a su capacidad para exhibir comportamientos complejos y aparentemente impredecibles sin la necesidad de entradas externas significativas, por tal motivo se han realizado varios trabajos sobre estabilidad y estimación de estados para modelos difusos Takagi-Sugeno (T-S), especialmente para aquellos que tienen entradas desconocidas (Chadli, 2010; Chadli and Karimi, 2012).

1.3.3. Observadores para sistemas caóticos

El mecanismo de sincronización de dos señales caóticas se conoce como sincronización caótica (Pecora and Carroll, 1990). Sin embargo, durante la sincronización caótica de sistemas continuos, la convergencia del error siempre es asintótica (Grassi and Mascolo, 1997).

La comunicación segura es fundamental en diversos contextos, y un claro ejemplo de su aplicación es en la navegación marítima, donde la integridad y confidencialidad de los datos son esenciales para garantizar la seguridad de las operaciones. En este sentido, Xu et al. (2020), presentan un sistema de comunicación seguro para la navegación marítima, utilizando un observador de estado diseñado mediante desigualdades matriciales lineales (LMI) para asegurar la protección de las comunicaciones. Además, emplea un sistema no lineal con la técnica de Lipschitz, que controla la tasa de cambio de las señales y garantiza la estabilidad y robustez del sistema ante las perturbaciones y entradas desconocidas.

Un observador en tiempo finito es una herramienta que permite estimar funciones del estado de un sistema dinámico en un tiempo limitado, lo cual es esencial en aplicaciones donde se requiere una respuesta rápida y precisa. A diferencia de los observadores convencionales con convergencia asintótica, estos garantizan resultados en un intervalo de tiempo finito. En el trabajo de Ríos-Ruiz et al. (2024), se propone un diseño basado en observadores funcionales generalizados para sistemas descriptores, permitiendo la estimación simultánea del estado y de fallas, incluso en presencia de incertidumbres paramétricas. Por su parte, Aguilar-López and Mata-Machuca (2016) presentan un enfoque orientado a la sincronización idéntica en tiempo finito de sistemas caóticos, aplicando observadores no lineales en una configuración maestro-esclavo. Ambos trabajos destacan la versatilidad de los observadores en tiempo finito y su utilidad en contextos como el control tolerante a fallas y la transmisión segura de información mediante sincronización caótica.

En aplicaciones de comunicación segura, la sincronización asintótica resulta ineficiente, ya que los retrasos en alcanzar la sincronía pueden impedir la correcta recuperación del mensaje, especialmente cuando los primeros datos transmitidos contienen información sensible. Por ello, se vuelve fundamental el uso de métodos de sincronización en tiempo finito que garanticen una convergencia exacta y dentro de un tiempo predefinido (Djenoune et al., 2019).

Otro ejemplo de comunicaciones seguras se presenta en Lian et al. (2001), que propone un diseño de observadores difusos para sistemas caóticos utilizando modelos Takagi-Sugeno. Este enfoque asegura un rendimiento robusto frente a incertidumbres y perturbaciones, y garantiza la recuperación asintótica del mensaje. Las simulaciones realizadas demuestran la efectividad del método en aplicaciones de sincronización caótica.

En Chadli and Zelinka (2014), se propone un enfoque basado en desigualdades matriciales lineales (LMI), pero en este caso utilizando el modelo Takagi-Sugeno (T-S) junto con el tratamiento de entradas desconocidas. El objetivo de este enfoque es estimar tanto las variables de estado como las entradas desconocidas del sistema, aplicando las condiciones de LMI. Este método se utiliza en el contexto de comunicación segura, y se incluye un ejemplo de simulación para demostrar su efectividad.

Assali (2021) diseñó y analizó un esquema de sincronización en tiempo predefinido para sistemas caóticos con diferentes dimensiones, es decir, sistemas que tienen un número distinto de variables o estados. Esto representa una extensión relevante respecto a estudios previos que se enfocan únicamente en sistemas de igual dimensión. El autor propuso un protocolo de control capaz de garantizar la sincronización en un tiempo exacto y preestablecido, independientemente de las condiciones iniciales del sistema. Para ello, se aplicaron herramientas de la teoría de estabilidad en tiempo predefinido, el método de Lyapunov, el cálculo de derivadas de funciones de error y el uso de controles adaptativos para manejar la incertidumbre en los parámetros del sistema. Asimismo, se diseñaron y probaron diversos controladores y leyes de adaptación para sincronizar pares de sistemas caóticos, como el sistema de Lü con el de Chen, o el de Lorenz con el de Duffing.

Hassan and Hammuda (2019) desarrollaron un método para mejorar la seguridad en la comunicación de datos utilizando caos sincronizado con restricciones dinámicas. Acoplaron dos sistemas caóticos y aplicaron restricciones temporales variables a sus señales para dificultar su predicción y descifrado. En el receptor, emplearon un Observador de Mínimos Cuadrados Regularizados y Suavizados con Restricciones (CSRLS) para sincronizar estas señales y recuperar la información transmitida. Este enfoque demuestra que la combinación de caos, restricciones dinámicas y técni-

cas avanzadas de estimación puede fortalecer los sistemas de comunicación segura.

El trabajo de Zhou et al. (2018), presenta un observador funcional acotado en tiempo finito para sistemas no lineales con retardo, basado en funcionales de Lyapunov-Krasovskii y desigualdades matriciales lineales (LMI). La metodología garantiza la estabilidad del error de observación dentro de límites predefinidos, permitiendo mejorar la precisión en sistemas con incertidumbre. Sus aplicaciones incluyen comunicación segura y robótica, donde es fundamental contar con estimaciones rápidas y confiables del estado del sistema.

1.4. Alcances

El presente trabajo aborda el diseño de un esquema criptográfico basado en sistemas caóticos, específicamente el sistema de Lorenz, modelado mediante el enfoque Takagi-Sugeno. Se desarrolla una estrategia para garantizar la comunicación segura a través del enmascaramiento de señales caóticas, permitiendo transmitir mensajes de audio sin alterar su estructura y asegurando la sincronización en un tiempo finito.

El estudio incluye el diseño de un sistema transmisor y dos receptores: un observador proporcional y un observador de tiempo finito, este último garantizando la estimación precisa de las variables de estado en un tiempo determinado. Los resultados obtenidos se basan en simulaciones bajo condiciones y parámetros controlados.

1.5. Originalidad

La novedad principal de esta investigación radica en el diseño de los observadores utilizados como receptores, específicamente el observador proporcional y el observador de tiempo finito, los cuales no se encuentran reportados en la literatura consultada para este tipo de sistemas caóticos aplicados a la comunicación segura. Esta contribución representa un avance en el campo, al proponer soluciones nuevas que mejoran la sincronización y la estimación de variables de estado en sistemas criptográficos basados en dinámicas caóticas.

1.6. Estructura del documento

El presente trabajo de investigación se encuentra dividido en 8 capítulos:

En el Capítulo 1 se plantea el problema a resolver, así como los objetivos general y particulares del proyecto. También se expone un análisis del estado del arte relacionado con los sistemas caóticos, observadores y métodos de control, así como los alcances, la originalidad del trabajo y una descripción general de la estructura del documento.

En el Capítulo 2 se desarrolla el marco teórico necesario para sustentar la investigación. Se explican conceptos fundamentales sobre sistemas de comunicación, sistemas caóticos y la teoría de sistemas Takagi-Sugeno (T-S), incluyendo sus enfoques de linealización y del sector no lineal, así como la observabilidad en dichos sistemas. Además, se aborda la teoría de observadores, elemento clave en el desarrollo de esta tesis.

En el Capítulo 3 se presenta la representación del sistema caótico de Lorenz en su forma T-S. Se modela primero el sistema en su forma no lineal y se realizan simulaciones para analizar su comportamiento. Posteriormente, se lleva a cabo la conversión a un modelo Takagi-Sugeno, comparando ambos modelos mediante simulaciones.

En el Capítulo 4 se lleva a cabo el diseño del sistema transmisor utilizando un observador de tipo Luenberger. Se expone el objetivo de diseño, se realiza un análisis de estabilidad del observador y se valida el funcionamiento del sistema transmisor por medio de simulaciones.

En el Capítulo 5 se propone un diseño de observador proporcional aplicado al sistema caótico modelado. Se describen las parametrizaciones utilizadas, el análisis de estabilidad correspondiente y la validación del desempeño del observador.

En el Capítulo 6 se desarrolla el diseño de un observador con convergencia en tiempo finito bajo un esquema maestro-esclavo. Se especifica la parametrización y se presentan resultados que validan su efectividad para la estimación de estados en tiempo finito.

En el Capítulo 7 se integra el proceso de cifrado y descifrado de mensajes en el sistema de comunicación. Se detallan los algoritmos utilizados, tanto para cifrar como para descifrar, así como su validación mediante simulaciones que demuestran la viabilidad del enfoque propuesto.

Finalmente, en el Capítulo 8 se exponen las conclusiones generales del trabajo, los logros obtenidos, las limitaciones encontradas y se sugieren posibles líneas de trabajo futuro que podrían extender o complementar esta investigación.

Capítulo 2

Marco Teórico

2.1. Sistemas de comunicación

La meta primordial de un sistema de comunicación consiste en trasladar información de un sitio a otro. En consecuencia, se podría afirmar que las comunicaciones electrónicas comprenden la transmisión, recepción y procesamiento de información entre dos o más lugares (Tomasi, 2003).

Como menciona Mesiya Mesiya (2013), una fuente de información genera un mensaje, que puede ser una señal analógica o una secuencia de símbolos o caracteres de un alfabeto finito. El habla, la música, las imágenes y el vídeo son ejemplos de señales analógicas. Si la señal del mensaje no se origina como una señal eléctrica, un transductor de entrada la convierte a una forma eléctrica. Ejemplos de transductores de entrada incluyen micrófonos, cámaras fotográficas y cámaras de televisión. Los archivos de texto, web y de audio MP3 son ejemplos de mensajes digitales.

Independientemente de la aplicación, un sistema de comunicación consta de tres componentes funcionales para transmitir el mensaje a un usuario final en un destino remoto:

- **Transmisor:** El transmisor convierte el mensaje en una forma adecuada para su transmisión a través de un medio físico o canal. Evidentemente, la señal de salida del transmisor contiene la información necesaria que se está transmitiendo en el mensaje original.
- **Receptor:** La función del receptor es recuperar el mensaje original a partir de la señal recibida. Esto es factible solo si la señal no se degrada más allá de cierto límite. Este límite está determinado por el procesamiento de señales realizado conjuntamente por el transmisor

y el receptor.

- **Medio de transmisión o canal:** El canal de comunicación es el medio de transmisión que lleva la energía de una señal electromagnética desde el transmisor hasta un receptor. La presencia del caos en estos canales proporciona un entorno dinámico y altamente impredecible, lo que contribuye significativamente a fortalecer la seguridad en las comunicaciones. La complejidad inherente y la naturaleza imprevisible de los sistemas caóticos dificultan que terceros intercepten o descifren la información transmitida a través de dichos canales, haciendo que su aplicación sea una estrategia efectiva para la protección de datos sensibles.

Dado lo anterior, una propuesta para garantizar la seguridad en el sistema de comunicación consiste en diseñar un esquema que utiliza encriptación y descryptación caótica. En este esquema, la comunicación se realiza mediante un canal público, mientras que el proceso de encriptación se efectúa utilizando señales caóticas. En el receptor, un observador estima el mensaje enmascarado para proceder con la descryptación. El diagrama que se presenta en la Figura 2.1 ilustra este esquema general, mostrando el flujo desde la encriptación del mensaje hasta su recuperación a través del observador y la descryptación caótica.

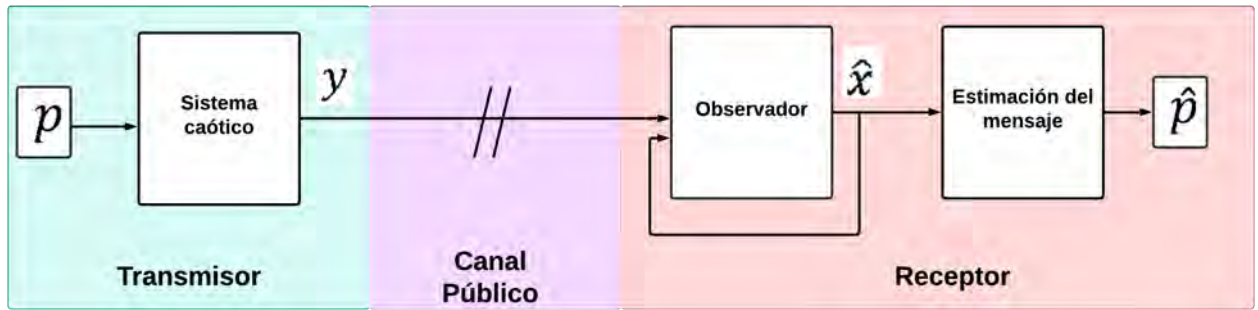


Fig. 2.1. Diagrama de un sistema de comunicación

Donde p es el mensaje original que se desea transmitir desde el transmisor, y es la salida generada por el sistema caótico que incorpora el mensaje p , $\hat{x}$ son las variables estimadas en el receptor que intentan replicar el comportamiento del sistema caótico en el transmisor, y $\hat{p}$ es el mensaje estimado, obtenido en el receptor.

2.2. Sistemas caóticos

El caos, según el Diccionario Real Academia Española, es el comportamiento aparentemente errático e impredecible de algunos sistemas dinámicos, aunque su formulación matemática sea en principio determinista. Debido a esta imprevisibilidad es de gran interés en los sistemas de comunicación, ya que posibilita la encriptación de información, proporcionando un alto nivel de seguridad.

Los sistemas catalogados como caóticos son sistemas no lineales que exhiben trayectorias limitadas y un comportamiento no periódico. Este comportamiento se caracteriza por oscilaciones erráticas o irregulares que no se repiten, y se manifiesta en condiciones totalmente deterministas, ya que siguen leyes bien definidas sin ninguna aleatoriedad. Un aspecto destacado de estos sistemas es su alta sensibilidad a las variaciones en sus condiciones iniciales (Rodríguez Liñán and León Morales, 2007b). Otra característica dada la naturaleza de las señales caóticas, es que tienden a ser de banda ancha, similares al ruido y difíciles de prever; se pueden emplear en diversos contextos para ocultar formas de onda que contengan información (Cuomo et al., 1993b).

Ramirez (2018) menciona que la teoría del caos se caracteriza por ser el estudio cualitativo del comportamiento dinámico aperiódico que se manifiesta en sistemas deterministas no lineales.

A continuación, se mencionan algunas características principales que identifican a los sistemas caóticos:

- **Determinista:** Schuster and Just (2006) menciona que los sistemas caóticos carecen de entradas o parámetros que sean aleatorios o ruidosos. La irregularidad en el comportamiento (aperiódico) surge de la no linealidad del sistema en lugar de fuerzas impulsoras ruidosas.
- **Múltiples órbitas periódicas:** Cardoza-Avendano et al. (2011) señala que hay trayectorias que no tienden a converger hacia puntos fijos, y que el conjunto de órbitas periódicas o cuasiperiódicas contribuye a que los sistemas caóticos exhiban un espectro de frecuencia distintivo, comparable al de una señal de ruido cuando el tiempo tiende a infinito.
- **Dependencia sensible de las condiciones iniciales:** Según Chen (1993), partiendo de condiciones iniciales diferentes, las trayectorias resultantes tienden a diferenciarse o divergir

de manera exponencial a medida que transcurre el tiempo, sin que exista correlación alguna entre dichas trayectorias.

- **Generación de atractores extraños:** De igual forma Chen (1993), menciona que una característica distintiva de los sistemas caóticos es la manifestación, en sus diagramas de fase, de estructuras geométricas con formas inusuales, como puntos fijos o ciclos límites, que carecen de similitud con objetos geométricos convencionales. Estas estructuras se conocen como *atractores extraños*. Estos atractores caóticos ejercen atracción sobre los puntos cercanos al atractor, mientras que las órbitas de puntos próximos entre sí tienden a divergir.

2.3. Teoría de sistemas Takagi-Sugeno

Una de las metodologías empleadas para el análisis y modelado de sistemas no lineales, ya sean de índole física, química, biomecánica o cualquier otra área, consiste en la utilización de sistemas Takagi-Sugeno, los cuales se describen a continuación.

El modelo difuso T-S fue introducido por Takagi and Sugeno (1985). Una característica fundamental de esta modelación es la capacidad para describir la dinámica local asociada a cada regla difusa mediante modelos lineales válidos en regiones acotadas localmente. De esta forma, el modelo global se construye a partir de una interpolación de dichos modelos lineales locales. La parte antecedente de una regla divide un conjunto de variables en subconjuntos difusos. Así, cada regla puede expresarse matemáticamente; la regla i -ésima se presenta como:

$$\xi_1 \text{ es } \Delta_1^i \text{ y } \cdots \text{ y } \xi_\eta \text{ es } \Delta_\eta^i \Rightarrow y = F_i(\xi(t)) \quad (2.1)$$

donde el vector $\xi(t)$ tiene η componentes, $\xi_j, j = 1, 2, \dots, \eta$, que representan variables pasadas o variables de programación, pues sus valores determinan el grado de activación de cada regla. Los conjuntos Δ_j^i con $j = 1, 2, \dots, \eta$ e $i = 1, \dots, r$ (donde r es el número total de reglas) son denominados conjuntos difusos.

El grado de pertenencia de una variable de programación $\xi_j(t)$ al conjunto difuso Δ_j^i está dado por una función de membresía $\mu_{ij} : \mathbb{R} \rightarrow [0, 1]$. El valor global de activación de la regla completa se calcula a partir de las funciones individuales de pertenencia utilizando un operador lógico de

conjunción, como el mínimo:

$$\varphi_i(\xi(t)) = \min_j \left(\mu_{ij}(\xi_j(t)) \right) \quad (2.2)$$

o bien, mediante el producto algebraico:

$$\varphi_i(\xi(t)) = \prod_{j=1}^{\eta} \mu_{ij}(\xi_j(t)) \quad (2.3)$$

A continuación, se normalizan estos valores de activación con la expresión:

$$\mu_i(\xi) = \frac{\varphi_i(\xi(t))}{\sum_{j=1}^r \varphi_j(\xi(t))} \quad (2.4)$$

bajo la condición de que $\sum_{i=1}^r \varphi_i(\xi(t)) \neq 0$, es decir, que para cualquier combinación válida de variables de programación, al menos una regla tenga un valor de activación distinto de cero.

En resumen, el modelado Takagi-Sugeno se basa en la interpolación de modelos lineales en el espacio de estados, fundamentándose en reglas condicionales del tipo SI-ENTONCES, cuya dinámica varía según las no linealidades propias del sistema (Lendek et al., 2011).

Se expresa formalmente como:

$$\begin{aligned} \dot{x}(t) &= \sum_{i=1}^r \mu_i(\xi(t)) (A_i x(t) + B_i u(t)), \\ y(t) &= C x(t) \end{aligned} \quad (2.5)$$

donde r es el número de modelos lineales locales, A_i , B_i y C son matrices constantes conocidas con dimensiones adecuadas, $\xi(t)$ es el vector de variables premisas y $\mu_i(\xi(t))$ son funciones de pertenencia normalizadas. Estas funciones deben satisfacer las siguientes condiciones:

$$1 \geq \mu_i(\xi(t)) \geq 0, \quad \text{y} \quad \sum_{i=1}^r \mu_i(\xi(t)) = 1 \quad (2.6)$$

Existen dos enfoques principales para representar sistemas T-S:

- Linealización.
- Sector no lineal.

Sin embargo, debido a que el enfoque de sector no lineal proporciona una representación más precisa de la dinámica de sistemas no lineales, en el presente trabajo se ha optado exclusivamente por esta metodología, la cual se describe en detalle a continuación.

2.3.1. Enfoque basado en sector no lineal

El método de sector no lineal es uno de los esquemas más populares para sintetizar modelos T-S, dado que permite una representación fiel de la dinámica no lineal dentro de un espacio de estados compacto (Flores-Hernández et al., 2018).

Este enfoque fue concebido originalmente para sistemas no lineales descritos por:

$$\begin{aligned}\dot{x}(t) &= f^m(x(t), u(t)) x + g^m(x(t), u(t)) u, \\ y(t) &= h^m(x(t), u(t)) x\end{aligned}\tag{2.7}$$

donde f^m , g^m y h^m son funciones suaves, $x(t)$ es el vector de estados, $u(t)$ el vector de entradas y $y(t)$ el de salidas.

Para aplicar este enfoque, se procede por etapas:

1. Reformulación del sistema en forma de espacio de estados:

$$\dot{x}(t) = A(x, u) x(t) + B(x, u) u(t),\tag{2.8}$$

donde algunas entradas de A y B dependen de x o de u .

2. Identificación de los componentes no constantes, que se denotan como:

$$\eta l_j, \quad j = 1, 2, \dots, r.\tag{2.9}$$

presentes en $A(x, u)$ y/o $B(x, u)$.

3. Definición del escenario de prueba: se establece un rango para la entrada y, con ello, los límites superior e inferior para las variables de programación. Es decir:

$$\xi_j \in [\underline{\eta l_j}, \overline{\eta l_j}].\tag{2.10}$$

4. Construcción de funciones de ponderación: para cada ξ_j se definen dos funciones:

$$\eta_0^j(\xi_j) = \frac{\overline{\eta l_j} - \xi_j}{\overline{\eta l_j} - \underline{\eta l_j}}, \quad (2.11)$$

$$\eta_1^j(\xi_j) = 1 - \eta_0^j(\xi_j). \quad (2.12)$$

5. Formulación de las reglas difusas: para cada regla i -ésima se define:

$$\mu_i(\xi(t)) = \prod_{j=1}^{\eta} \mu_{ij}(\xi_j), \quad (2.13)$$

donde μ_{ij} corresponde a η_0^j o η_1^j , dependiendo de la regla. Estas funciones están normalizadas y cumplen: $\mu_i(\xi(t)) \geq 0$ y $\sum_{i=1}^r \mu_i(\xi(t)) = 1$.

6. Determinación de los modelos lineales locales: a partir de los valores extremos de cada ηl_j , se generan todas las combinaciones posibles, dando lugar a $r = 2^\eta$ modelos lineales con:

$$\dot{x}(t) = A_i x(t) + B u(t). \quad (2.14)$$

El modelo global T-S queda entonces como la interpolación de estos modelos:

$$\begin{aligned} \dot{x}(t) &= \sum_{i=1}^r \mu_i(\xi(t)) (A_i x(t) + B u(t)), \\ y(t) &= C x(t). \end{aligned} \quad (2.15)$$

2.3.2. Observabilidad en modelos Takagi-Sugeno

En los sistemas basados en el modelo Takagi-Sugeno, el concepto de observabilidad hace referencia a la capacidad de reconstruir el estado interno del sistema a partir de las señales de entrada y salida que se encuentran disponibles para medición. Aunque este tipo de sistemas presenta una estructura no lineal, la aplicación directa de los criterios clásicos de observabilidad para sistemas no lineales puede no ser apropiada.

Esto se debe a que, en los sistemas Takagi-Sugeno, el diseño de observadores se realiza considerando una ganancia específica para cada regla del sistema. En consecuencia, la evaluación de la

observabilidad no se lleva a cabo sobre el sistema global como un todo, sino que debe garantizarse de manera individual en cada uno de los modelos lineales locales asociados a las distintas reglas difusas que componen el sistema (Zaidi et al., 2013).

Durante el proceso de diseño, se asume que cada par de matrices (A_i, C_i) , con $i = 1, 2, \dots, r$, satisface la condición de observabilidad. Esto implica que, para cada modelo local, la siguiente matriz de observabilidad debe tener rango completo:

$$\text{rango} \left(\begin{bmatrix} C \\ CA_i \\ \vdots \\ CA_i^{n_s-1} \end{bmatrix} \right) = n_s, \quad \forall i = 1, \dots, r. \quad (2.16)$$

donde n_s representa el número de estados que caracterizan el comportamiento dinámico del sistema.

2.4. Observadores

Un observador es una estructura que permite estimar las variables de estado de un sistema dinámico utilizando las señales disponibles de entrada y salida. El diseño de un observador solo es posible si se cumple la condición de observabilidad en el sistema considerado (Ogata, 2010).

Considérese el siguiente sistema Takagi-Sugeno descrito por:

$$\begin{aligned} \dot{x}(t) &= \sum_{i=1}^r \mu_i(\xi(t)) A_i x(t) + Bu(t), \\ y(t) &= Cx(t) \end{aligned} \quad (2.17)$$

El modelo del observador incluye un término corrector que permite ajustar la estimación del estado, tomando en cuenta las posibles desviaciones en las matrices del sistema y el error inicial en la estimación del estado. Este error inicial corresponde a la discrepancia entre el estado real en el instante inicial y la estimación proporcionada en dicho instante. En la Figura 2.2 se muestra un esquema general que ilustra la estructura típica de un observador.

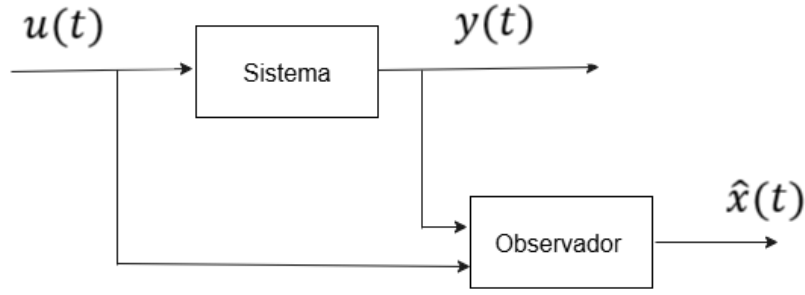


Fig. 2.2. Representación general de un observador.

El modelo matemático del observador se expresa como:

$$\begin{aligned}\dot{\hat{x}}(t) &= A\hat{x}(t) + Bu(t) + L(y - C\hat{x}(t)), \\ \hat{y}(t) &= C\hat{x}(t)\end{aligned}\tag{2.18}$$

donde:

- $\hat{x}(t)$ representa el vector de estado estimado.
- $C\hat{x}(t)$ es la salida calculada a partir de la estimación del estado.
- L corresponde a la matriz de ganancia del observador.

Clasificación de observadores

Los observadores pueden clasificarse según el número de variables que estiman en relación con el total de estados del sistema:

- **Observador de orden completo:** Este tipo de observador realiza la estimación de todas las variables de estado del sistema, independientemente de que algunas de ellas puedan ser medidas directamente.
- **Observador de orden reducido:** En este caso, el observador se encarga únicamente de estimar un subconjunto de las variables de estado, es decir, menos de n , siendo n la dimensión total del vector de estados.
- **Observador de orden mínimo:** Se refiere a un observador de orden reducido que estima la menor cantidad posible de variables de estado. Si el sistema cuenta con n estados y m

salidas disponibles para medición, el observador estima entonces las $n - m$ variables que no pueden medirse directamente.

2.5. Conclusiones del capítulo

En este capítulo se abordaron los fundamentos teóricos necesarios para el desarrollo de la propuesta de comunicación segura basada en sistemas caóticos y modelos Takagi-Sugeno. Se establecieron los principios generales de los sistemas de comunicación, destacando la necesidad de garantizar la integridad y confidencialidad de la información transmitida, especialmente en entornos donde los canales de transmisión son públicos y susceptibles a intervenciones externas.

Posteriormente, se exploró la teoría del caos, enfatizando sus propiedades deterministas, la sensibilidad a las condiciones iniciales y la generación de señales impredecibles, lo cual las convierte en una herramienta eficaz para la encriptación de mensajes. Estas características permiten el desarrollo de esquemas criptográficos robustos basados en señales caóticas, como el propuesto en este trabajo.

Asimismo, se presentó la teoría de los sistemas Takagi-Sugeno como una estrategia versátil para representar dinámicas no lineales mediante la interpolación de modelos lineales locales. Este enfoque, especialmente en su formulación basada en el sector no lineal, permite modelar de manera precisa sistemas complejos, facilitando el análisis y el diseño de observadores. Se detalló también el concepto de observabilidad en este contexto y se expuso la estructura general de un observador, subrayando su relevancia en la estimación de estados cuando no todas las variables son accesibles directamente.

Con lo anterior, se sientan las bases teóricas necesarias para la implementación de un sistema de comunicación encriptado mediante señales caóticas, cuya recuperación en el receptor se lleva a cabo mediante observadores diseñados bajo la estructura T-S. Esta combinación representa una solución innovadora y efectiva para fortalecer la seguridad en la transmisión de datos.

Capítulo 3

Representación Takagi-Sugeno del sistema caótico de Lorenz

3.1. Modelo no lineal del sistema caótico

Como uno de los modelos más conocidos y estudiados de sistemas caóticos, el sistema de Lorenz cuenta con una extensa base de investigación y aplicaciones que respaldan su idoneidad para el cifrado.

El sistema clásico de Lorenz está compuesto por un conjunto de tres ecuaciones diferenciales ordinarias (EDO) acopladas de primer orden, las cuales se expresan en coordenadas adimensionales (Munmuangsaen and Srisuchinwong, 2018), tal como se describe en la Ecuación (3.1).

$$\begin{cases} \dot{x}_1(t) = a(x_2(t) - x_1(t)) \\ \dot{x}_2(t) = x_1(t)(b - x_3(t)) - x_2(t) \\ \dot{x}_3(t) = x_1(t)x_2(t) - cx_3(t) \end{cases} \quad (3.1)$$

donde x_1 , x_2 y x_3 son variables de estado, $a = 10$, $b = 28$ y $c = 8/3$ son parámetros constantes del sistema, los cuales han resultado en la generación de un atractor caótico autoexcitado, que comúnmente se visualiza como la forma de una mariposa (Lorenz, 1963).

3.1.1. Simulación del sistema no lineal

Objetivo de la simulación: El objetivo de la simulación es observar el comportamiento no lineal del sistema. Para llevarla a cabo, se utilizan los parámetros mencionados anteriormente. El método de

integración empleado en la configuración de *Matlab R2019a* corresponde a `ode4` (Runge-Kutta de 4º orden) con paso fijo, utilizando un tiempo de muestreo de $T_e = 0.001$. Las condiciones iniciales fueron $x(0) = [1, 1, 1]^T$.

En la Figura 3.1 se muestra la simulación del sistema caótico de Lorenz, con los parámetros designados y con las condiciones iniciales elegidas canteriormente.

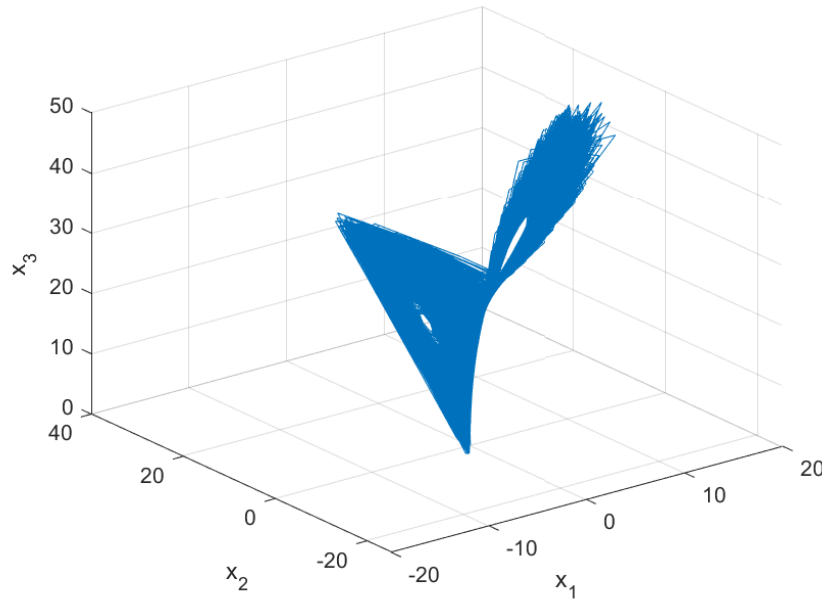


Fig. 3.1. Sistema caótico de Lorenz

Donde se puede apreciar la forma "mariposa" del comportamiento caótico del sistema de Lorenz en su representación gráfica en el espacio tridimensional. Esta representación visualiza cómo evolucionan las variables del sistema en función del tiempo, proporcionando una visión única de su dinámica.

En la Figura 3.2, se muestra el comportamiento de las variables de estado del modelo no lineal.

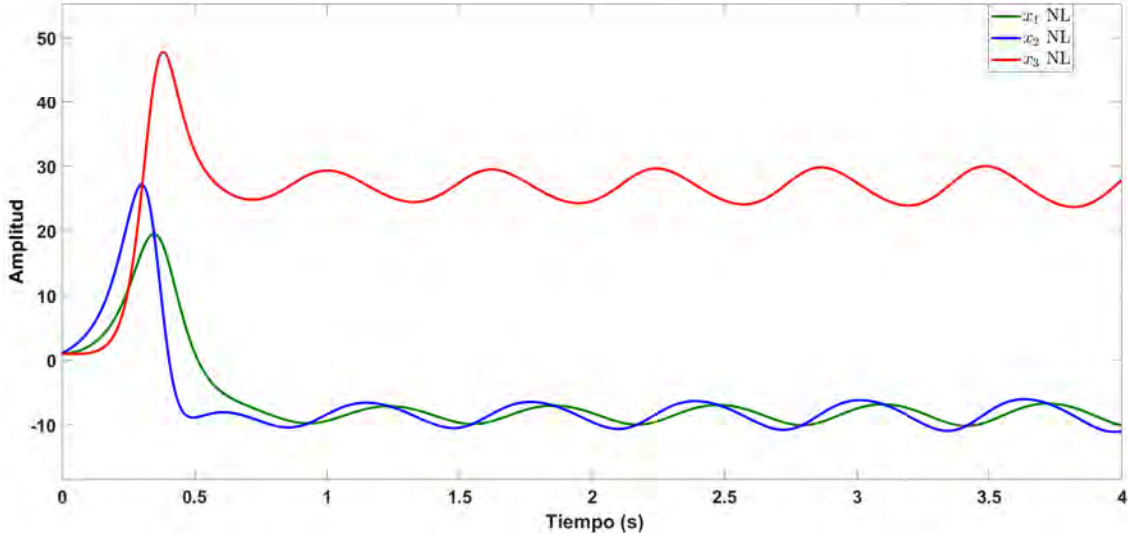


Fig. 3.2. Estados del sistema no lineal

3.2. Representación Takagi-Sugeno del sistema caótico

La representación del modelo no lineal (3.1) se puede expresar como:

$$\begin{cases} \dot{x}(t) = A(x)x(t), \\ y(t) = Cx(t). \end{cases} \quad (3.2)$$

donde $x(t)$ es el vector de estado $x(t) = [x_1(t) \ x_2(t) \ x_3(t)]$ y $A(x)$, C son matrices de dimensiones apropiadas.

En la matriz $A(x)$ se incluye un término no lineal dependiente de las variables de estado, el cual se destaca de color rojo en la siguiente Ecuación:

$$\begin{pmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \\ \dot{x}_3(t) \end{pmatrix} = \begin{pmatrix} -a & a & 0 \\ b & -1 & -\mathbf{x}_1(t) \\ 0 & \mathbf{x}_1(t) & -c \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{pmatrix} \quad (3.3)$$

La determinación de los valores límite de la no linealidad requiere establecer las condiciones iniciales del modelo (3.1). Al asignar $x(0) = [1 \ 1 \ 1]$, en el sistema autónomo, se obtienen los límites $-30 \leq x_1(t) \leq 30$.

El sistema de Lorenz cuenta con dos funciones de pertenencia, dadas por $r = 2^R$, donde R representa el número de no linealidades presentes en el sistema, por lo que $r = 2^1 = 2$. Estas funciones de pertenencia son:

$$\mu_1(x(t)) = \frac{1}{2} \left(1 + \frac{x_1(t)}{\underline{x}_1} \right), \quad \mu_2(x(t)) = \frac{1}{2} \left(1 - \frac{x_1(t)}{\underline{x}_1} \right) \quad (3.4)$$

Considerando estos conjuntos difusos, el modelo T-S cuenta con dos reglas. Para cada una de ellas, se asocia un modelo matemático lineal local con la siguiente forma:

$$\dot{x}(t) = A_i x(t); \quad i = 1, 2 \quad (3.5)$$

El modelo T-S que representa de manera precisa la dinámica del sistema no lineal original es:

$$\begin{cases} \dot{x}(t) = \mu_1(x_1(t))A_1x(t) + \mu_2(x_1(t))A_2x(t), \\ y(t) = Cx(t). \end{cases} \quad (3.6)$$

donde

$$A_1 = \begin{pmatrix} -a & a & 0 \\ b & -1 & -\underline{x}_1 \\ 0 & \underline{x}_1 & -c \end{pmatrix}, \quad A_2 = \begin{pmatrix} -a & a & 0 \\ b & -1 & -\underline{x}_1 \\ 0 & \underline{x}_1 & -c \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

El modelo matemático del sistema caótico en la forma T-S puede expresarse como:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i x(t)), \\ y(t) = Cx(t). \end{cases} \quad (3.7)$$

donde $x(t)$ representa el vector de estado del sistema caótico, y $y(t)$ es la salida. Las funciones de pertenencia cumplen con las siguientes condiciones:

$$0 \leq \mu_i(x(t)) \leq 1, \quad \sum_{i=1}^2 \mu_i(x(t)) = 1. \quad (3.8)$$

Los polos de los modelos locales se muestran a continuación:

$$\lambda(A_1) = \begin{bmatrix} -12.7782 + 0.0000i \\ -0.4442 + 25.4516i \\ -0.4442 - 25.4516i \end{bmatrix}, \quad \lambda(A_2) = \begin{bmatrix} -12.7782 + 0.0000i \\ -0.4442 + 25.4516i \\ -0.4442 - 25.4516i \end{bmatrix}. \quad (3.9)$$

por lo que los sistemas son estables, al tener polos con parte real negativa en el plano complejo.

3.2.1. Simulación del modelo no lineal y del modelo Takagi-Sugeno

Objetivo de la simulación: El objetivo de la simulación es observar el comportamiento del sistema caótico en su representación no lineal y el modelo Takagi-Sugeno. Para llevar a cabo la simulación se utilizan los parámetros mencionados anteriormente. El método de integración empleado en la configuración de *Matlab R2019a* corresponde a `ode4` (Runge-Kutta de 4º orden) con paso fijo, utilizando un tiempo de muestreo de $T_e = 0.001$, las condiciones iniciales en ambos modelos fueron $x(0) = [1, 1, 1]^T$.

En la Figura 3.3, se muestra la comparación del estado $x_1(t)$ del sistema no lineal con el modelo Takagi-Sugeno. De forma similar, en la Figura 3.4 se presenta la comparación correspondiente al estado $x_2(t)$, y en la Figura 3.5 se observa la comparación del estado $x_3(t)$.

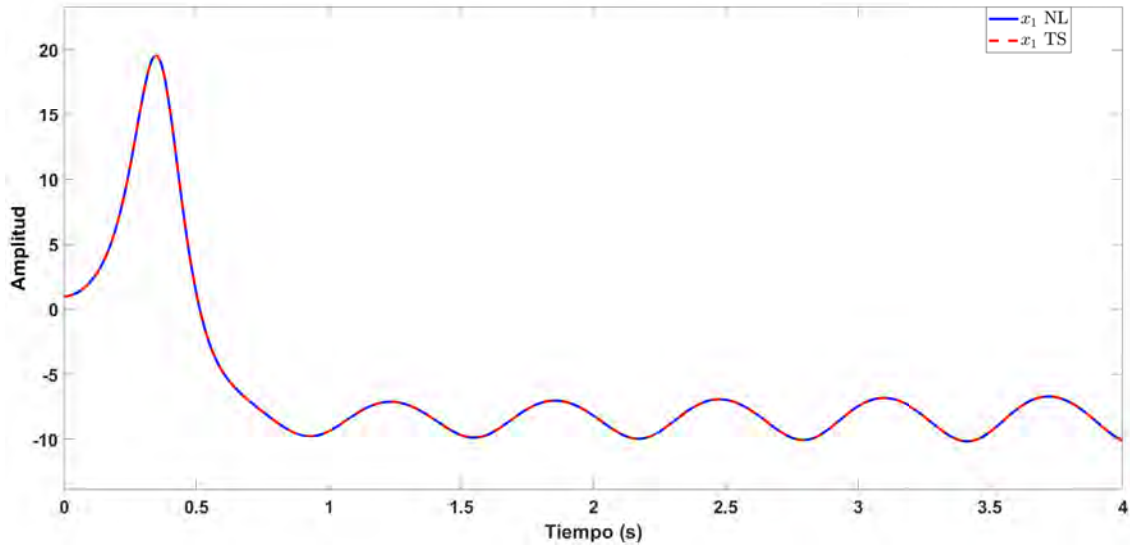


Fig. 3.3. Comparación del estado $x_1(t)$ del modelo NL y T-S

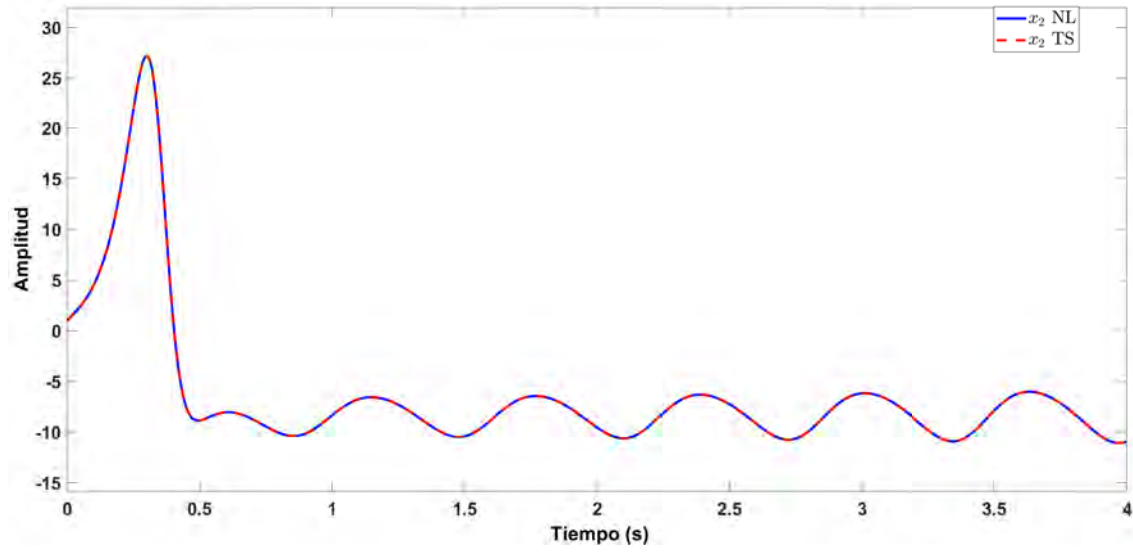


Fig. 3.4. Comparación del estado $x_2(t)$ del modelo NL y T-S

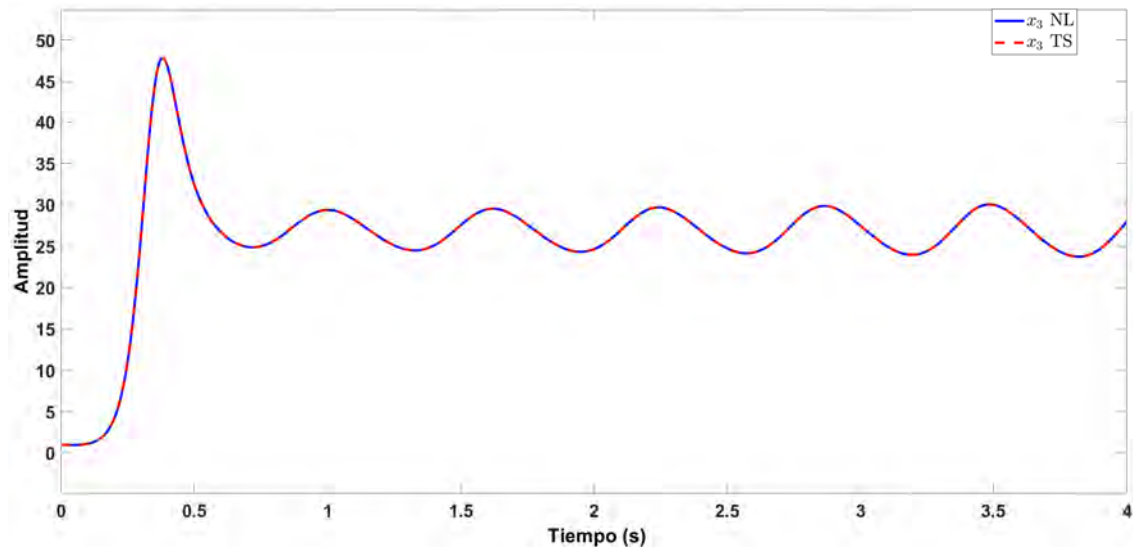


Fig. 3.5. Comparación del estado $x_3(t)$ del modelo NL y T-S

En la Figura 3.6 se presenta el comportamiento de las funciones de pertenencia, donde cada señal representa la presencia de cada modelo local, las cuales nos permiten obtener la dinámica del modelo no lineal.

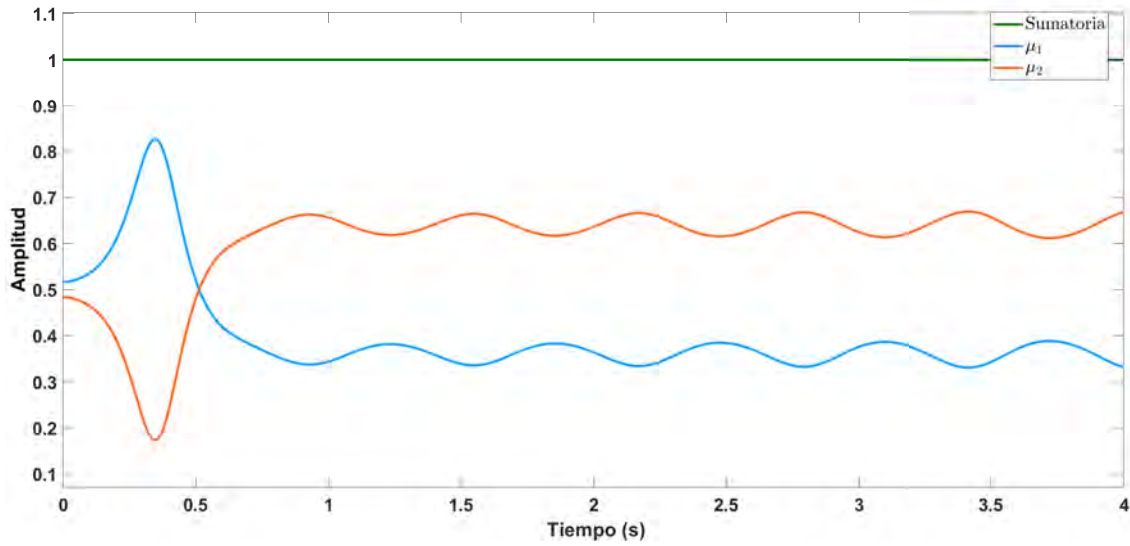


Fig. 3.6. Funciones de pertenencia del sistema Takagi-Sugeno

3.3. Conclusiones del capítulo

En este capítulo se presentó el modelo no lineal del sistema caótico de Lorenz, el cual destaca por su comportamiento dinámico complejo y su sensibilidad a las condiciones iniciales. A partir de dicho modelo, se desarrolló una representación equivalente utilizando la estructura difusa de Takagi-Sugeno (T-S), que permite aproximar sistemas no lineales mediante una combinación ponderada de modelos lineales locales.

El sistema T-S se obtuvo considerando la no linealidad presente en la dinámica del sistema, y utilizando funciones de pertenencia dependientes del estado $x_1(t)$, lo que dio lugar a dos modelos locales. La simulación mostró que los estados del modelo T-S siguen de manera exacta la evolución del sistema no lineal.

Capítulo 4

Diseño del sistema transmisor

4.1. Objetivo de diseño

El objetivo de diseño en este capítulo es construir un sistema transmisor basado en el modelo Takagi-Sugeno (T-S) del sistema caótico de Lorenz, donde el mensaje se enmascara dentro de las variables del sistema. Para garantizar la sincronización del transmisor, se diseña un observador de tipo Luenberger cuyo propósito es calcular las ganancias L_i necesarias. Estas ganancias, una vez obtenidas, se integran directamente en el sistema transmisor para asegurar la estabilidad del error de estimación, la cual se verifica mediante funciones de Lyapunov y desigualdades matriciales lineales (LMIs).

Aunque el sistema transmisor y el observador de Luenberger emplean las mismas ganancias L_i , su función dentro de cada sistema es distinta pero complementaria. En el transmisor, las ganancias L_i se utilizan para inyectar el mensaje $p(t)$ en las variables del sistema caótico mediante el término $L_i E p(t)$, permitiendo enmascarar la señal de información dentro de la dinámica del sistema. Por otro lado, en el observador, estas mismas ganancias sirven para retroalimentar el error de salida y corregir la estimación del estado, asegurando que el error de estimación converja a cero y, por ende, la sincronización entre transmisor y observador.

De este modo, el uso conjunto de las ganancias L_i en ambos sistemas permite una integración coherente entre el enmascaramiento del mensaje y la sincronización, facilitando la recuperación precisa del mensaje en el receptor.

4.2. Observador Luenberguer

El modelo Takagi-Sugeno (T-S) del sistema caótico de Lorenz se convierte en un canal a través del cual el mensaje se transmite enmascarado dentro de la variable $p(t)$, y se expresa como se muestra en la siguiente Ecuación:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i x(t) + L_i E p(t)), \\ y(t) = C x(t) + E p(t). \end{cases} \quad (4.1)$$

donde $x(t)$ es el vector de estados n , $y(t)$ representa el vector m variables de salidas medidas, las matrices $A_i \in \mathbb{R}^{n \times n}$, $C \in \mathbb{R}^{m \times n}$ son matrices conocidas, L_i es la matriz de ganancia del observador, que se calculará más adelante, y E es una matriz de distribución del mensaje en la salida, dada por $E = [0, 1]^T$. El mensaje $p(t)$ se transmite únicamente a la segunda variable del estado $x_2(t)$, enmascarándose en la salida $y_2(t)$, mientras que $y_1(t)$ refleja solo la primera componente de $x(t)$, sin contener información sobre el mensaje.

Para llevar a cabo el diseño de un observador, es indispensable que se cumpla la condición de observabilidad, la cual, puede expresarse de la siguiente manera:

$$\text{rango} \begin{bmatrix} C \\ C A_1 \\ C A_1^2 \end{bmatrix} = 3, \quad \text{rango} \begin{bmatrix} C \\ C A_2 \\ C A_2^2 \end{bmatrix} = 3$$

Las ganancias L_i garantizan que el sistema caótico actúe como transmisor, permitiendo la sincronización entre el transmisor y el receptor para la correcta estimación del mensaje. Para determinar los valores de L_i , se diseña un observador de tipo Luenberger, que se expresa matemáticamente en la siguiente Ecuación:

$$\begin{cases} \dot{\hat{x}}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i \hat{x}(t) + L_i (y(t) - \hat{y}(t))), \\ \hat{y}(t) = C \hat{x}(t). \end{cases} \quad (4.2)$$

donde $\hat{x}(t)$ es el vector de estados estimados, $\hat{y}(t)$ representa el vector de las variables estimadas.

Se define el error de estimación del estado de la siguiente forma:

$$e(t) = x(t) - \hat{x}(t) \quad (4.3)$$

la dinámica del error en la estimación del estado se puede describir de la siguiente manera:

$$\dot{e}(t) = \dot{x}(t) - \dot{\hat{x}}(t) \quad (4.4)$$

sustituyendo las expresiones $\dot{x}(t)$ y $\dot{\hat{x}}(t)$, se obtiene:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) (A_i x(t) + L_i E p(t) - A_i \hat{x}(t) - L_i (y(t) - \hat{y}(t))) \quad (4.5)$$

reemplazando $y(t)$ y $\hat{y}(t)$

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) (A_i x(t) + L_i E p(t) - A_i \hat{x}(t) - L_i (C x(t) + E p(t) - C \hat{x}(t))) \quad (4.6)$$

reorganizando los términos, se obtiene:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) (A_i x(t) + \textcolor{red}{L_i E p(t)} - A_i \hat{x}(t) - L_i C x(t) - \textcolor{red}{L_i E p(t)} + L_i C \hat{x}(t)) \quad (4.7)$$

agrupando los términos que dependen de $x(t)$ y $\hat{x}(t)$, se obtiene:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) ((A_i - L_i C)(x(t) - \hat{x}(t))) \quad (4.8)$$

entonces la dinámica del error en el observador, puede expresarse como:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) ((A_i - L_i C)e(t)) \quad (4.9)$$

4.2.1. Análisis de estabilidad del observador

En esta sección se presentan las condiciones para garantizar la estabilidad del observador Luenberger.

Se considera la función candidata de Lyapunov:

$$V(e(t)) = e^T(t) X e(t) > 0 \quad (4.10)$$

con $X = X^T > 0$. Su derivada a lo largo de la trayectoria de (4.9) está dada por

$$\dot{V}(e(t)) = \sum_{i=1}^2 \mu_i(x(t)) (e^T(t) [(A_i - L_i C)^T X + X (A_i - L_i C)] e(t)) < 0 \quad (4.11)$$

La estabilidad asintótica del sistema está garantizada si y solo si $\dot{V}(e(t)) < 0$ lo que conduce a la siguiente LMI.

$$(A_i - L_i C)^T X + X (A_i - L_i C) < 0, \quad i = 1, 2. \quad (4.12)$$

para garantizar un rendimiento específico en la convergencia del error de estimación del estado, se define la región $S_r(\alpha, \beta)$ como la intersección entre un círculo con centro en $(0, 0)$ y radio β .

$$A_i^T X - C^T W_i^T + X A_i - W_i C < 0 \quad (4.13a)$$

$$\begin{bmatrix} -\beta X & X A_i - W_i C \\ (X A_i - W_i C)^T & -\beta X \end{bmatrix} < 0, \quad i = 1, 2. \quad (4.13b)$$

donde $W_i = X L_i$.

4.2.2. Simulación del sistema transmisor

Objetivo de la simulación: El objetivo de la simulación es analizar el comportamiento del sistema caótico tanto en su representación no lineal como en el modelo Takagi-Sugeno, con el mensaje enmascarado en la dinámica de los estados. Para ello, se emplean los parámetros mencionados anteriormente. El método de integración empleado en la configuración de *Matlab R2019a* corresponde a `ode4` (Runge-Kutta de 4º orden) con paso fijo, utilizando un tiempo de muestreo de $T_e = 0.001$, las condiciones iniciales para ambos sistemas fueron $x(0) = [1, 1, 1]^T$.

Resolviendo las LMIs de la Ecuación 4.13 se obtienen las siguientes matrices.

$$X = \begin{bmatrix} 1.6364 & 0 & 0 \\ 0 & 0.0330 & 0 \\ 0 & 0 & 2.0005 \end{bmatrix},$$
$$W_1 = \begin{bmatrix} -13.7008 & 16.3635 \\ 0.9246 & 0.0347 \\ 0 & 59.5457 \end{bmatrix}, \quad W_2 = \begin{bmatrix} -13.7008 & 16.3635 \\ 0.9246 & 0.0347 \\ 0 & -59.5457 \end{bmatrix},$$
$$L_1 = \begin{bmatrix} -8.3728 & 10 \\ 28 & 1.0520 \\ 0 & 29.7660 \end{bmatrix}, \quad L_2 = \begin{bmatrix} -8.3728 & 10 \\ 28 & 1.0520 \\ 0 & -29.7660 \end{bmatrix}.$$

Para validar el modelo T-S con el sistema no lineal, se utilizó el modelo T-S descrito en la Ecuación (4.1) y al insertar el mensaje en el modelo no lineal se obtiene la siguiente representación descrita en la Ecuación (4.14), donde el vector LE depende del estado $x_1(t)$ y, a su vez, este será nuestro sistema transmisor. Para representar el sistema no lineal a partir del modelo T-S, se consideró el vector LE utilizando un valor dinámico basado en el estado $x_1(t)$. Esta proporción permite ajustar las funciones de pertenencia $\mu_i(x(t))$ en función de la evolución de $x_1(t)$, facilitando así la transición del modelo T-S al comportamiento no lineal del sistema.

$$\begin{cases} \dot{x}(t) = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & -x_1(t) \\ 0 & x_1(t) & -8/3 \end{bmatrix} x(t) + \begin{bmatrix} 10 \\ 1.0520 \\ 0.9922x_1(t) \end{bmatrix} p(t) \\ y(t) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} p(t) \end{cases} \quad (4.14)$$

El mensaje enmascarado en el modelo no lineal se muestra en la Figura 4.1, mientras que las Figuras 4.2-4.4 presentan las comparaciones de los estados del sistema no lineal con respecto al modelo Takagi-Sugeno (T-S).

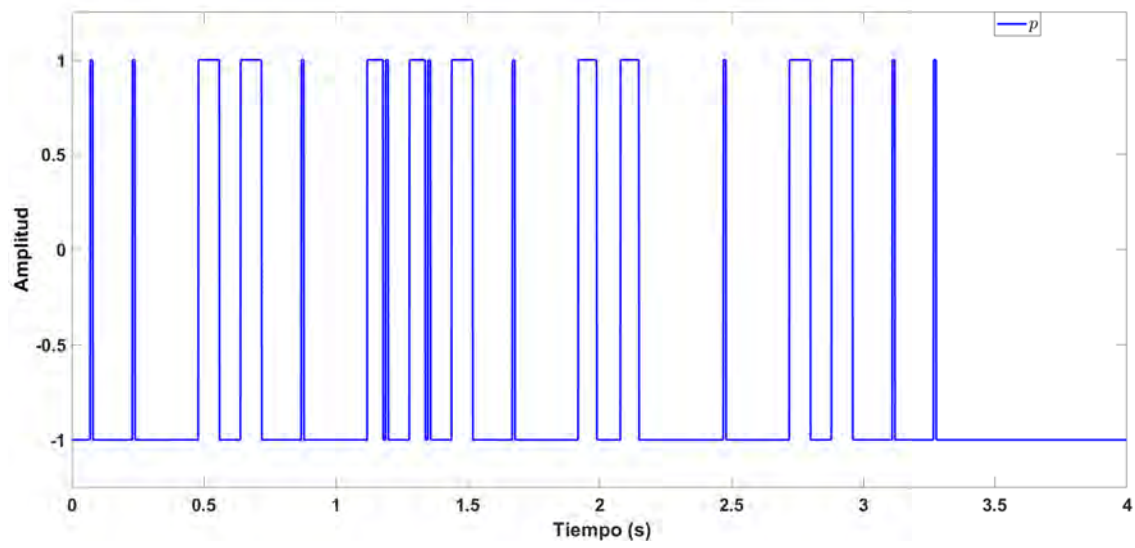


Fig. 4.1. Mensaje enmascarado

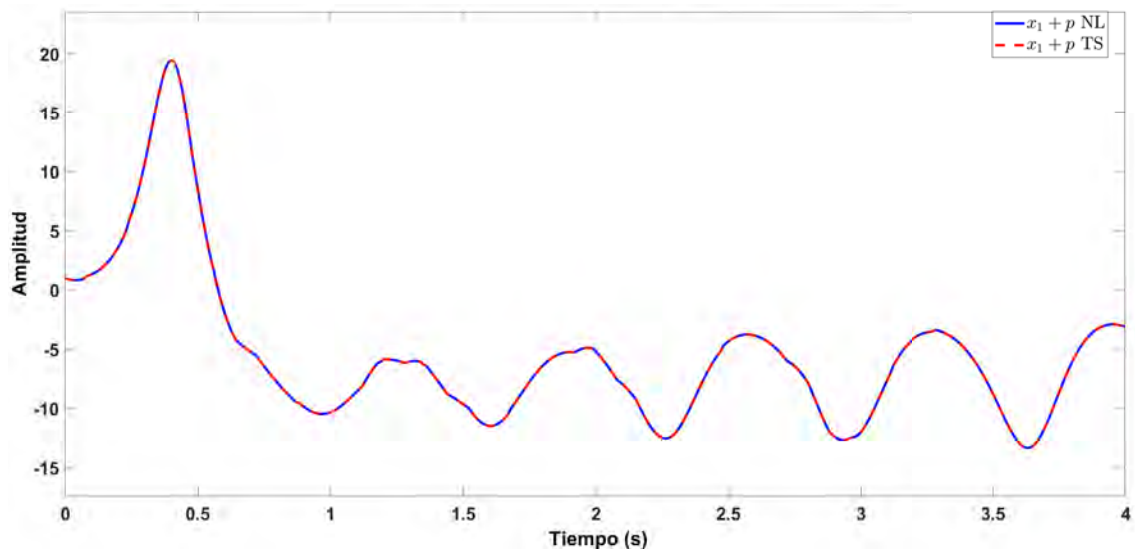


Fig. 4.2. Comparación del estado $x_1(t) + p(t)$ del modelo NL y T-S

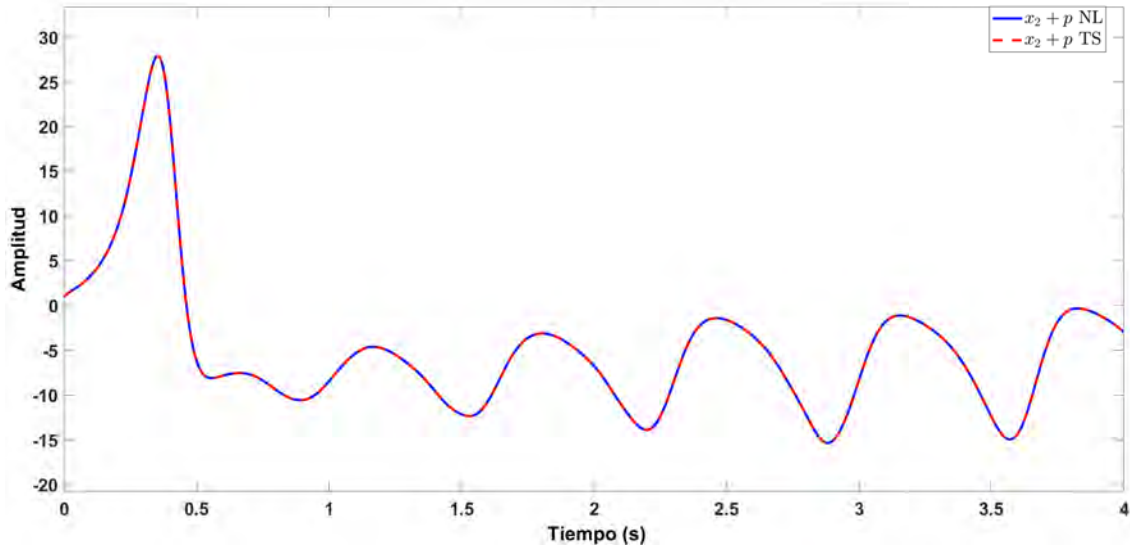


Fig. 4.3. Comparación del estado $x_2(t) + p(t)$ del modelo NL y T-S

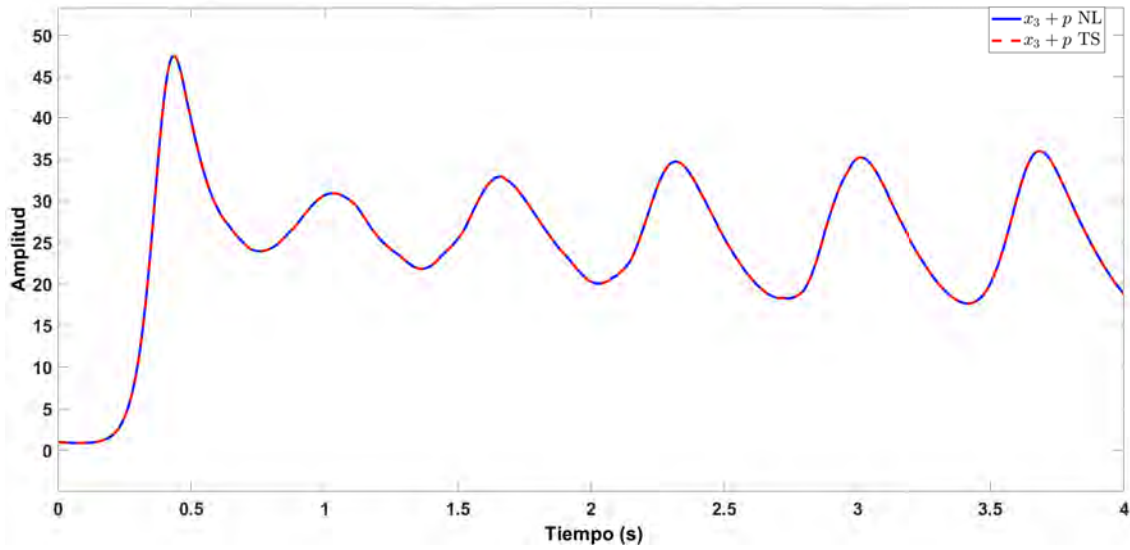


Fig. 4.4. Comparación del estado $x_3(t) + p(t)$ del modelo NL y T-S

4.3. Conclusiones del capítulo

Los resultados obtenidos demuestran que el modelo T-S diseñado logra replicar adecuadamente la dinámica del sistema no lineal de Lorenz, incluyendo el enmascaramiento del mensaje en sus

variables de estado. A través del observador de tipo Luenberger, se calcularon las ganancias L_i que al ser incorporadas en el sistema transmisor, permiten garantizar la sincronización y la estabilidad del error de estimación. La validez del modelo T-S frente al sistema no lineal, bajo condiciones iniciales iguales, confirma que esta aproximación es efectiva para representar el comportamiento caótico del sistema y viable para su uso en esquemas de transmisión segura basados en caos.

Capítulo 5

Diseño del observador proporcional

5.1. Objetivo de diseño

El objetivo de este capítulo es diseñar un observador proporcional capaz de estimar los estados de un sistema caótico modelado mediante una representación tipo Takagi-Sugeno (T-S), incluso en presencia de un mensaje cifrado que perturba las salidas del sistema. A través de la formulación de restricciones algebraicas y la resolución de desigualdades matriciales lineales (LMIs), se busca garantizar la estabilidad asintótica del error de estimación y lograr una reconstrucción precisa del mensaje transmitido.

5.2. Observador Proporcional

Retomando el modelo T-S del sistema transmisor descrito anteriormente, se tiene la siguiente Ecuación:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i x(t) + L_i E p(t)), \\ y(t) = C x(t) + E p(t). \end{cases} \quad (5.1)$$

Para lograr la estimación del estado del sistema caótico con el mensaje cifrado, se considera el siguiente observador proporcional (PO):

$$\begin{cases} \dot{\zeta}(t) = \sum_{i=1}^2 \mu_i(x(t))(N_i \zeta(t) + F_i y(t)), \\ \hat{x}(t) = \zeta(t) + Q y(t). \end{cases} \quad (5.2)$$

donde $\zeta(t)$ representa el vector de estados del observador, $\hat{x}(t) \in \mathbb{R}^n$ representa el vector de estados

estimados. Las matrices $N_i \in \mathbb{R}^{n \times n}$, $F_i \in \mathbb{R}^{n \times m}$, $Q \in \mathbb{R}^{n \times m}$ son las ganancias del observador. Para asegurar la convergencia del estado estimado, es fundamental calcular estas matrices de manera adecuada. Con este propósito, se define el error de estimación del estado de la siguiente forma:

$$e(t) = \hat{x}(t) - x(t) \quad (5.3)$$

sustituyendo la expresión de $\hat{x}(t)$, se obtiene:

$$e(t) = \zeta(t) + Qy(t) - x(t) \quad (5.4)$$

se reemplaza $y(t)$ utilizando la ecuación del sistema, lo que da como resultado:

$$e(t) = \zeta(t) + Q(Cx(t) + Ep(t)) - x(t) \quad (5.5)$$

agrupando los términos que dependen $x(t)$, se obtiene:

$$e(t) = \zeta(t) - (I - QC)x(t) + QEp(t) \quad (5.6)$$

definiendo una matriz auxiliar $T = (I - QC)$, la ecuación del error de estimación toma la forma:

$$e(t) = \zeta(t) - Tx(t) + QEp(t) \quad (5.7)$$

de la cual se obtiene $\zeta(t)$:

$$\zeta(t) = e(t) + Tx(t) - QEp(t) \quad (5.8)$$

Así, la dinámica del error en la estimación del estado se puede describir de la siguiente manera:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t))(\dot{\zeta}(t) - (I - QC)\dot{x}(t) + QE\dot{p}(t)) \quad (5.9)$$

sustituyendo $\dot{\zeta}(t)$ y $\dot{x}(t)$

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t))(N_i\zeta(t) + F_iy(t) - (I - QC)(A_ix(t) + L_iEp(t)) + QE\dot{p}(t)) \quad (5.10)$$

ahora reemplazando $\zeta(t)$ y $y(t)$

$$\begin{aligned}\dot{e}(t) = & \sum_{i=1}^2 \mu_i(x(t)) \left(N_i(e(t) + (I - QC)x(t) - QEp(t)) \right. \\ & + F_i(Cx(t) + Ep(t)) - A_i x(t) - L_i Ep(t) \\ & \left. + A_i QCx(t) + QCL_i Ep(t) + QE\dot{p}(t) \right)\end{aligned}\quad (5.11)$$

agrupando los términos que dependen de $x(t)$ y $p(t)$

$$\begin{aligned}\dot{e}(t) = & \sum_{i=1}^2 \mu_i(x(t)) \left(N_i e(t) + (N_i + (F_i - N_i Q)C - (I - QC)A_i) x(t) \right. \\ & \left. + ((F_i - N_i Q)E - (I - QC)L_i E) p(t) + QE\dot{p}(t) \right)\end{aligned}\quad (5.12)$$

Usando la expresión de $\hat{x}(t)$ y $y(t)$, se puede obtener:

$$\hat{x}(t) = \sum_{i=1}^2 \mu_i(x(t)) (e(t) + (I - QC)x(t) - QEp(t) + QCx(t) + QEp(t)) \quad (5.13)$$

reorganizando los términos se obtiene:

$$\hat{x}(t) = \sum_{i=1}^2 \mu_i(x(t)) (e(t) + (T + QC)x(t)) \quad (5.14)$$

reemplazando $T = (I - QC)$ y $K_i = (F_i - N_i Q)$ para simplificar la dinámica del error de estimación (5.12), se consideran las siguientes restricciones:

$$\begin{aligned}(a) \quad & N_i + K_i C - T A_i = 0 \\ (b) \quad & K_i E - T L_i E = 0 \\ (c) \quad & T + QC = I \\ (d) \quad & QE = 0\end{aligned}\quad (5.15)$$

Entonces las ecuaciones (5.12) y (5.14) se pueden reescribir como:

$$\begin{aligned}\dot{e}(t) = & \sum_{i=1}^2 \mu_i(x_1(t)) (N_i e(t)) \\ \hat{x}(t) = & \sum_{i=1}^2 \mu_i(x_1(t)) (e(t) + (T + QC)x(t))\end{aligned}\quad (5.16)$$

5.2.1. Parametrización de las matrices del observador proporcional

Antes de presentar la solución al problema de diseño de PO, se proporcionará la parametrización de las soluciones que satisfacen las restricciones algebraicas (a) a (d) de la Ecuación (5.15).

Las condiciones (c) y (d) pueden expresarse como:

$$\begin{bmatrix} T & Q \end{bmatrix} \Sigma = \Omega \quad (5.17)$$

donde $\Sigma = \begin{bmatrix} I & 0 \\ C & E \end{bmatrix}$ y $\Omega = \begin{bmatrix} I & 0 \end{bmatrix}$.

La solución particular de la Ecuación (5.17) es:

$$\begin{bmatrix} T & Q \end{bmatrix} = \Omega \Sigma^+ \quad (5.18)$$

o equivalente a

$$T = \Omega \Sigma^+ \begin{bmatrix} I \\ 0 \end{bmatrix}, \quad (5.19)$$

$$Q = \Omega \Sigma^+ \begin{bmatrix} 0 \\ I \end{bmatrix}. \quad (5.20)$$

donde Σ^+ es la inversa generalizada de Σ , tal que satisface $\Sigma \Sigma^+ \Sigma = \Sigma$.

De las condiciones (a) y (c), se obtiene

$$\mathbf{N}_i = T A_i - \mathbf{K}_i C \quad (5.21)$$

donde

$$\mathbf{K}_i = F_i - \mathbf{N}_i Q \quad (5.22)$$

entonces la matriz F_i , se deduce como

$$F_i = \mathbf{K}_i + \mathbf{N}_i Q \quad (5.23)$$

5.2.2. Análisis de estabilidad del observador

Considerando la dinámica del error de estimación, esta puede expresarse como:

$$\dot{e}(t) = \sum_{i=1}^2 \mu_i(x(t)) ((T A_i - K_i C) e(t)) \quad (5.24)$$

Se considera la función candidata de Lyapunov

$$V(e(t)) = e^T(t) X e(t) > 0 \quad (5.25)$$

con $X = X^T > 0$. Su derivada a lo largo de la trayectoria de 5.24 está dada por

$$\dot{V}(e(t)) = \sum_{i=1}^2 \mu_i(x(t)) (e^T(t) [(TA_i - K_i C)^T X + X (TA_i - K_i C)] e(t)) < 0 \quad (5.26)$$

La estabilidad asintótica del sistema está garantizada si y solo si $\dot{V}(e(t)) < 0$ lo que conduce a la siguiente LMI.

$$(TA_i - K_i C)^T X + X (TA_i - K_i C) < 0, \quad i = 1, 2. \quad (5.27)$$

Para garantizar un rendimiento específico en el error de estimación del estado, deben cumplirse las siguientes condiciones. La condición descrita en la Ecuación (5.28b) se deriva de la restricción b , descrita en la Ecuación (5.15), la cual se multiplica por X .

$$A_i^T T^T X - C^T W_i^T + X A_i - W_i C < 0 \quad (5.28a)$$

$$X T L_i E = W_i E, \quad i = 1, 2. \quad (5.28b)$$

donde $W_i = X K_i$.

5.2.3. Simulación del observador proporcional

Objetivo de la simulación: El objetivo de la simulación es analizar el comportamiento del observador proporcional. El método de integración empleado en la configuración de *Matlab R2019a* corresponde a `ode4` (Runge-Kutta de 4º orden) con paso fijo, utilizando un tiempo de muestreo de $T_e = 0.001$. Las condiciones iniciales del observador proporcional se definieron como $x(0) = [0, 0, 0]^T$, mientras que las del sistema transmisor se establecieron como $x(0) = [1, 1, 1]^T$. Estas condiciones permiten evaluar la capacidad del observador para estimar los estados del sistema a partir de condiciones iniciales diferentes.

Resolviendo las LMIs de la Ecuación 5.28 se obtienen las siguientes matrices.

$$\begin{aligned}
 X &= \begin{bmatrix} 1.0001 & 0 & 0 \\ 0 & 0.0105 & 0 \\ 0 & 0 & 0.4085 \end{bmatrix}, \\
 W_1 &= \begin{bmatrix} -4.5003 & 5.0006 \\ 0.2951 & 0.0111 \\ 0.0001 & 12.1587 \end{bmatrix}, \quad W_2 = \begin{bmatrix} -4.5003 & 5.0006 \\ 0.2951 & 0.0111 \\ 0.0001 & -12.1587 \end{bmatrix}, \\
 T &= \begin{bmatrix} 0.5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad Q = \begin{bmatrix} 0.5 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},
 \end{aligned}$$

$$\begin{aligned}
 N_1 &= \begin{bmatrix} -0.5000 & 0 & 0 \\ -0.0002 & -2.0520 & -30.000 \\ 0.0001 & 0.2340 & -2.6667 \end{bmatrix}, \quad N_2 = \begin{bmatrix} -0.5000 & 0 & 0 \\ 0.0002 & -2.0520 & 30.000 \\ 0.0001 & -0.2340 & -2.6667 \end{bmatrix}, \\
 F_1 &= \begin{bmatrix} -4.7500 & 5.0000 \\ 28.0001 & 1.0520 \\ 0.0000 & 29.7660 \end{bmatrix}, \quad F_2 = \begin{bmatrix} -4.7500 & 5.0000 \\ 27.9999 & 1.0520 \\ 0.0000 & -29.7660 \end{bmatrix}.
 \end{aligned}$$

En las Figuras 5.1-5.3 presentan las comparaciones de los estados del Observador Proporcional y del sistema no lineal.

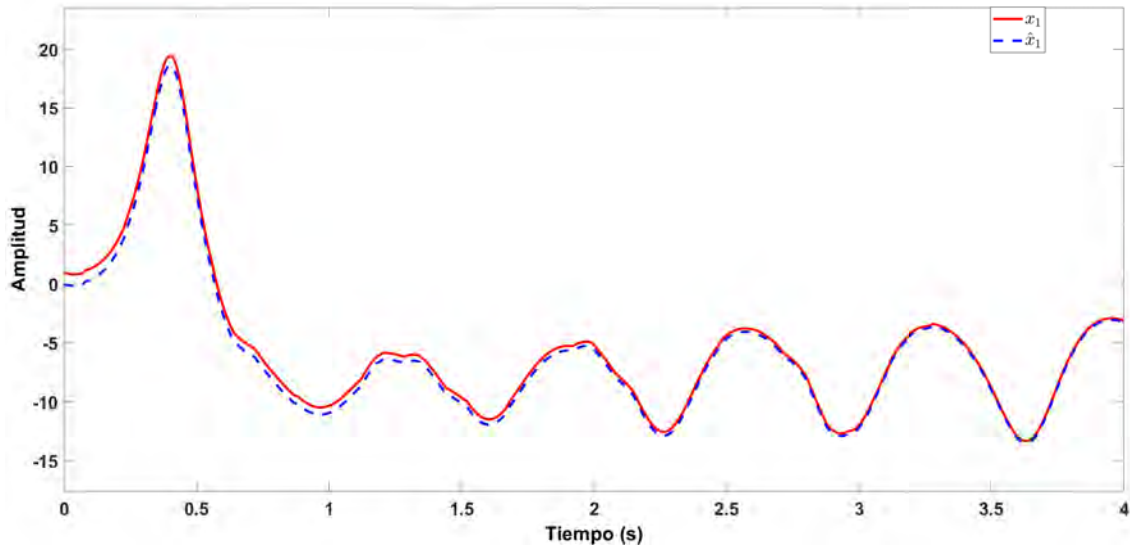


Fig. 5.1. Comparación del estado $x_1(t)$ del Observador Proporcional y Sistema No Lineal

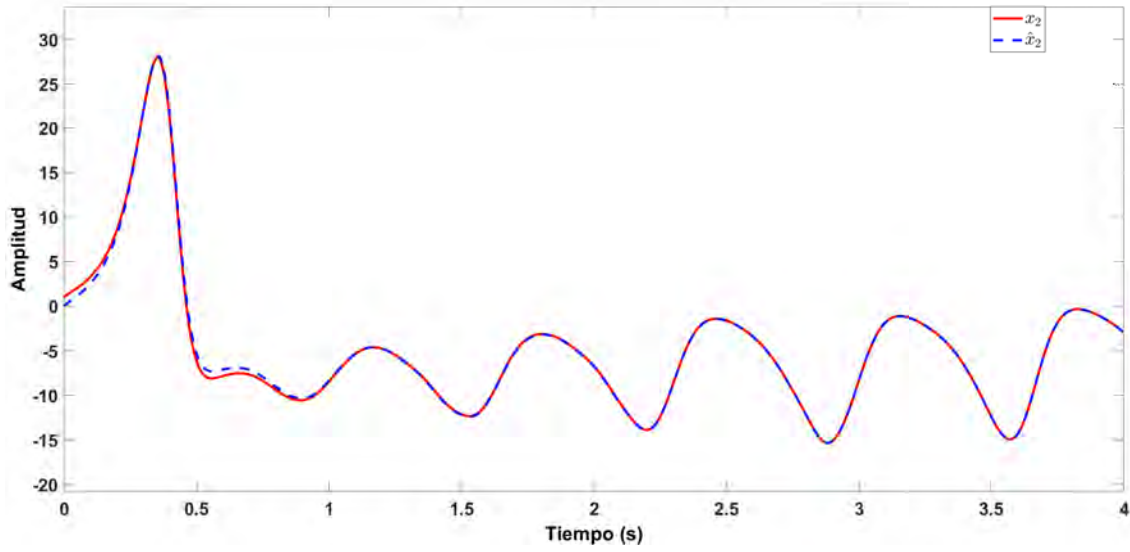


Fig. 5.2. Comparación del estado $x_2(t)$ del Observador Proporcional y Sistema No Lineal

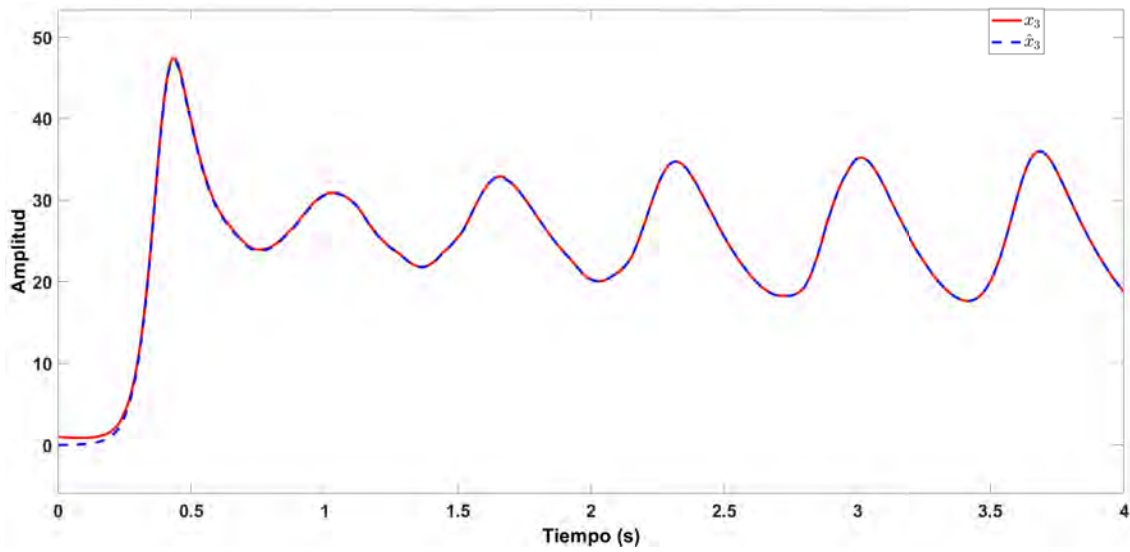


Fig. 5.3. Comparación del estado $x_3(t)$ del Observador Proporcional y Sistema No Lineal

En la Figura 5.4 se presentan las mediciones del error entre los estados del Observador Proporcional y los estados del sistema no lineal.

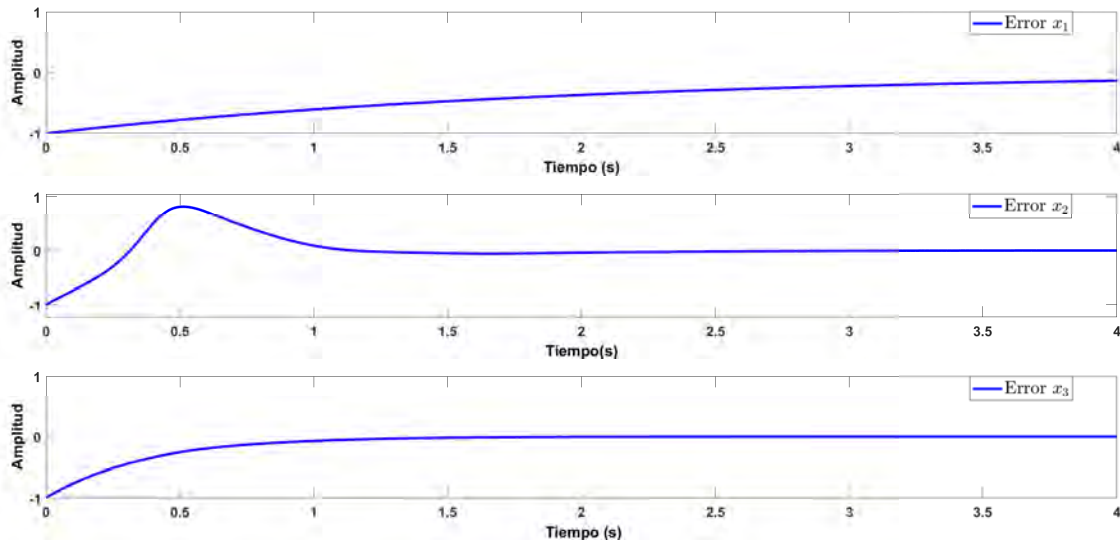


Fig. 5.4. Error del Observador Proporcional con el Sistema No Lineal

La evaluación del Observador Proporcional se llevó a cabo mediante el análisis del error entre sus estados y los correspondientes del modelo no lineal. Los resultados obtenidos se resumen en la Tabla 5.1. A continuación, se presentan las expresiones utilizadas para calcular los índices de desempeño.

La integral del cuadrado del error, ISE, el cual se define como:

$$ISE = \int_0^T e^2(t)dt. \quad (5.29)$$

La integral del valor absoluto de la magnitud del error, IAE, el cual se define como:

$$IAE = \int_0^T |e(t)|dt. \quad (5.30)$$

Tabla 5.1. Valores de los índices de desempeño del observador proporcional.

Estados	ISE	IAE
$x_1(t)$	0.9817	1.729
$x_2(t)$	0.3144	0.5619
$x_3(t)$	0.1871	0.3729

A partir de los resultados presentados en la Tabla 5.1, se observa que el Observador Proporcional presenta un desempeño aceptable en la estimación de los estados del sistema no lineal. El estado

$x_1(t)$ presenta los mayores valores tanto de ISE como de IAE, lo que indica que fue el más difícil de estimar con precisión. En contraste, los estados $x_2(t)$ y $x_3(t)$ muestran menores niveles de error, lo que refleja una mejor calidad en su estimación. En general, los índices obtenidos confirman la capacidad del observador para seguir las dinámicas del sistema, aunque con variaciones en el nivel de precisión entre los distintos estados.

5.2.4. Estimación del mensaje

Cuando el error en la estimación del estado es cero, se puede considerar que $\hat{x}(t) = x(t)$ en la Ecuación (5.1), lo que permite obtener la siguiente aproximación:

$$\hat{y}(t) = C\hat{x}(t) + E\hat{p}(t) \quad (5.31)$$

Debido a que la matriz E posee un rango de columna completo, es posible llevar a cabo la estimación del mensaje de la siguiente manera:

$$\hat{p}(t) = E^+ (y(t) - \hat{y}(t)) \quad (5.32)$$

donde E^+ es cualquier inversa generalizada de E tal que $EE^+E = E$.

En la Figura 5.5 se presenta el resultado de la estimación del mensaje realizada por el observador proporcional. Se observa que, a partir del segundo 1.12, la estimación del mensaje se vuelve precisa, lo cual indica que el sistema logra reconstruir correctamente la señal cifrada a partir de ese instante. Sin embargo, se evidencia una pérdida de información antes de dicho tiempo.

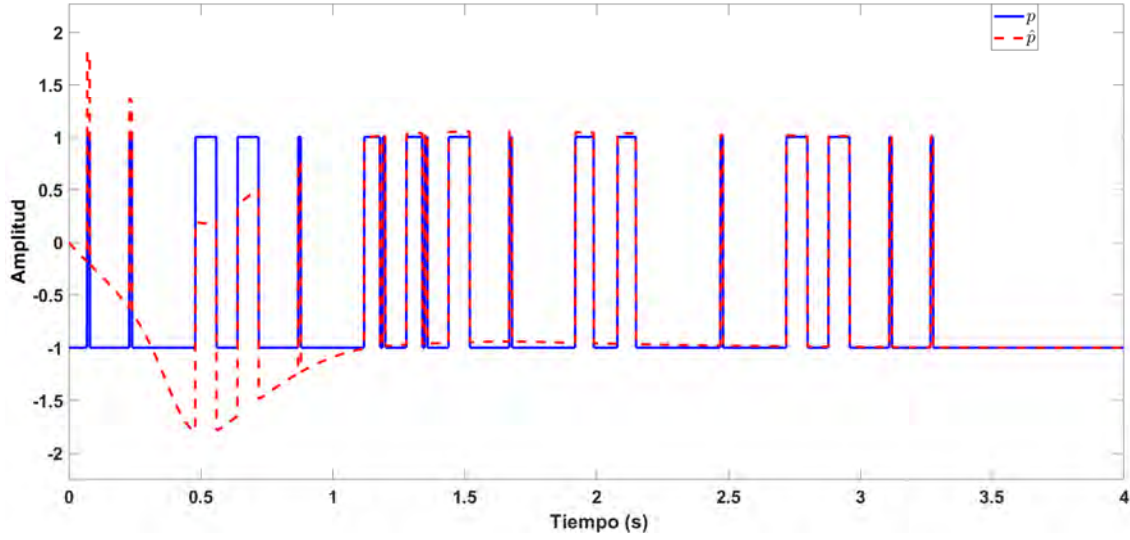


Fig. 5.5. Mensaje estimado con el Observador Proporcional

5.3. Conclusiones del capítulo

En este capítulo se desarrolló el diseño de un observador proporcional (PO) para un sistema no lineal representado en forma T-S, con el objetivo de estimar sus estados internos y el mensaje cifrado. Se establecieron restricciones necesarias para asegurar la convergencia del error de estimación, y se propuso una estrategia de diseño basada en LMIs para garantizar estabilidad asintótica.

La simulación del observador demostró que, a pesar de condiciones iniciales distintas entre el sistema y el observador, el esquema propuesto logra estimar con precisión los estados del sistema. Además, la estimación del mensaje cifrado fue exitosa a partir de un tiempo transitorio, confirmando la efectividad del observador en la recuperación de la información.

Los índices de desempeño calculados (ISE e IAE) reflejan un comportamiento satisfactorio del observador, aunque con diferencias en el nivel de precisión entre los distintos estados. En conjunto, los resultados obtenidos validan la factibilidad y eficiencia del observador proporcional como herramienta para la estimación de estados y decodificación de mensajes en sistemas caóticos.

Capítulo 6

Diseño del observador con convergencia en tiempo finito

6.1. Objetivo de diseño

El objetivo de este capítulo es diseñar e implementar un observador de estados con convergencia en tiempo finito utilizando una configuración maestro-esclavo. Este observador tiene como finalidad sincronizarse con la dinámica de un sistema no lineal basado en el modelo de Lorenz, permitiendo una estimación precisa de los estados en un tiempo limitado.

6.2. Observador maestro-esclavo

El modelo del sistema maestro se representa mediante:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i x(t)) \\ y(t) = Cx(t) \end{cases} \quad (6.1)$$

donde $x(t) \in \mathbb{R}^n$ representa el vector de estados, $y(t) \in \mathbb{R}^m$ representa el vector de salidas medidas, las matrices $A_i \in \mathbb{R}^{n \times n}$, $C \in \mathbb{R}^{m \times n}$ son matrices conocidas

La dinámica correspondiente al sistema esclavo es:

$$\begin{cases} \dot{\hat{x}}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i \hat{x}(t)) - k_1(|\tilde{e}| - k_2) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \quad (6.2)$$

donde $k_1 = \begin{bmatrix} k_{11} & 0 & 0 \\ 0 & k_{12} & 0 \\ 0 & 0 & k_{13} \end{bmatrix}$, $k_2 = \begin{bmatrix} k_{21} \\ k_{22} \\ k_{23} \end{bmatrix}$, $\tilde{\varepsilon} = \begin{bmatrix} \varepsilon_1^{-1/p} \\ \varepsilon_2^{-1/p} \\ \varepsilon_3^{-1/p} \end{bmatrix}$ son las ganancias del observador, se define el error de sincronización como un vector $\varepsilon_j = x_j - \hat{x}_j$. Se considera que $p > 1$ y es un número entero impar, y que cada elemento k_{1j} y k_{2j} para $j = [1, 2, 3]$ de k_1 y k_2 son matrices constantes positivas.

Se define el error de estimación del estado de la siguiente forma:

$$\varepsilon(t) = x(t) - \hat{x}(t) \quad (6.3)$$

La expresión matemática del error de estimación del estado es:

$$\dot{\varepsilon}(t) = \dot{x}(t) - \dot{\hat{x}}(t) \quad (6.4)$$

Al reemplazar las expresiones $\dot{x}(t)$ y $\dot{\hat{x}}(t)$, se obtiene:

$$\dot{\varepsilon}(t) = \sum_{i=1}^2 \mu_i(x(t))(A_i x(t) - A_i \hat{x}(t)) + k_1(|\tilde{\varepsilon}| - k_2) \quad (6.5)$$

6.2.1. Parametrización del observador

Existe un vector constante F que establece una cota para la diferencia entre las funciones dinámicas del sistema maestro y el observador (esclavo), lo que implica una especie de continuidad o comportamiento acotado del sistema.

$$|A_i x(t) - A_i \hat{x}(t)| \leq F \quad (6.6)$$

para todo $x, \hat{x} \in \Omega \subset \mathbb{R}^n$.

Las ganancias del sistema esclavo k_1 y k_2 se deben elegir de manera que:

$$F \approx k_1 k_2 \quad (6.7)$$

Lemma 1 (La desigualdad de Cauchy–Schwarz) puntanen2011cauchy. Sean $\mathbf{x}$ y $\mathbf{y}$ vectores reales no nulos de dimensión $n \times 1$. Entonces:

$$(\mathbf{x}^\top \mathbf{y})^2 \leq \mathbf{x}^\top \mathbf{x} \cdot \mathbf{y}^\top \mathbf{y}, \quad \text{para todo } \mathbf{x}, \mathbf{y} \quad (6.8)$$

es la versión vectorial de la desigualdad de Cauchy-Schwarz. La igualdad en se cumple si y solo si $\mathbf{x}$ y $\mathbf{y}$ son linealmente dependientes, es decir,

$$(\mathbf{x}^\top \mathbf{y})^2 = \mathbf{x}^\top \mathbf{x} \cdot \mathbf{y}^\top \mathbf{y} \iff \text{tal que } \lambda \in \mathbb{R} : \mathbf{x} = \lambda \mathbf{y}. \quad (6.9)$$

Aplicando la desigualdad de Cauchy-Schwarz en la Ecuación (6.5) y la Ecuación (6.6)

$$|\dot{\varepsilon}| \leq F - k_1 k_2 + k_1 |\tilde{\varepsilon}|^{-1/p} \quad (6.10)$$

considerando la Ecuación (6.7)

$$|\dot{\varepsilon}| \leq k_1 |\tilde{\varepsilon}| \quad (6.11)$$

donde

$$\begin{bmatrix} |\dot{\varepsilon}_1| \\ |\dot{\varepsilon}_2| \\ |\dot{\varepsilon}_3| \end{bmatrix} \leq \begin{bmatrix} K_{11} & 0 & 0 \\ 0 & K_{12} & 0 \\ 0 & 0 & K_{13} \end{bmatrix} \begin{bmatrix} \varepsilon_1^{-1/p} \\ \varepsilon_2^{-1/p} \\ \varepsilon_3^{-1/p} \end{bmatrix} \quad (6.12)$$

Nótese que la desigualdad anterior es una clase de función de estabilización de tiempo finito, donde el parámetro $p > 1$ se considera un entero impar. Entonces la solución es

$$|\varepsilon_j| \leq \text{sign}(\varepsilon_{0j}) (|\varepsilon_{0j}| - k_{1j} \frac{t}{p})^p \quad (6.13)$$

en estado estacionario $\varepsilon_j(t) = 0$, para $j = [1, 2, 3]$

$$t \geq p \frac{|\varepsilon_{0j}|^{1/p}}{k_{1j}} \quad (6.14)$$

Entonces, el sistema dinámico (6.2) actúa como un observador de estados con convergencia en tiempo finito para el sistema (6.1), donde el tiempo de convergencia está dado por:

$$t_{ft} = p \frac{|\varepsilon_{0j}|^{1/p}}{k_{1j}} \quad (6.15)$$

siendo $\varepsilon_j(0) = \varepsilon_{0j}$ el valor inicial del error de sincronización.

6.2.2. Simulación del observador

Objetivo de la simulación: Es evaluar el desempeño de un observador con convergencia en tiempo finito, estructurado mediante una configuración maestro-esclavo. El sistema maestro representa la dinámica real del transmisor, mientras que el esclavo actúa como observador de estados. Para llevar a cabo la simulación, se utilizó el método de integración `ode4` (Runge-Kutta de cuarto orden) con paso fijo en el entorno *Matlab R2019a*, empleando un tiempo de muestreo de $T_e = 0.001$. Las condiciones iniciales se fijaron como $x(0) = [1, 1, 1]^T$ para el sistema maestro y $\hat{x}(0) = [0, 0, 0]^T$ para el observador. Esta configuración permite analizar la capacidad del observador esclavo para sincronizarse con el sistema maestro, partiendo de condiciones iniciales distintas, y verificar su convergencia en tiempo finito.

Las ganancias del sistema esclavo fueron determinadas considerando la ubicación de los polos del sistema y su influencia en la velocidad de convergencia del error. Esta elección se realizó con el objetivo de asegurar un comportamiento dinámico adecuado del observador, priorizando una convergencia rápida y estable.

$$\begin{cases} F_1 \approx 80 \\ F_2 \approx 170 \\ F_3 \approx 100 \end{cases} \quad (6.16)$$

Desarrollando la primera ganancia de (6.7). Dado que $F_1 = 80$ y $k_{21} = 1$, se despeja k_{11} como:

$$k_{11} \approx \frac{F_1}{k_{21}} = \frac{80}{1} = 80 \quad (6.17)$$

luego aplicando los demás despejes con respecto a (6.16), las ganancias del esclavo se fijan como:

$$\begin{cases} k_{11} = 80 \\ k_{12} = 170 \\ k_{13} = 100 \\ k_{21} = 1 \\ k_{22} = 1 \\ k_{23} = 1 \end{cases} \quad (6.18)$$

En consecuencia, las matrices de ganancia quedan establecidas como:

$$k_1 = \begin{bmatrix} 80 & 0 & 0 \\ 0 & 170 & 0 \\ 0 & 0 & 100 \end{bmatrix},$$

$$k_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

$$\tilde{\varepsilon} = \begin{bmatrix} \varepsilon_1^{-1/3} \\ \varepsilon_2^{-1/3} \\ \varepsilon_3^{-1/3} \end{bmatrix}.$$

En las Figuras 6.1-6.3 se ilustran las comparaciones entre los estados del sistema no lineal y los estimados por el observador maestro-esclavo.

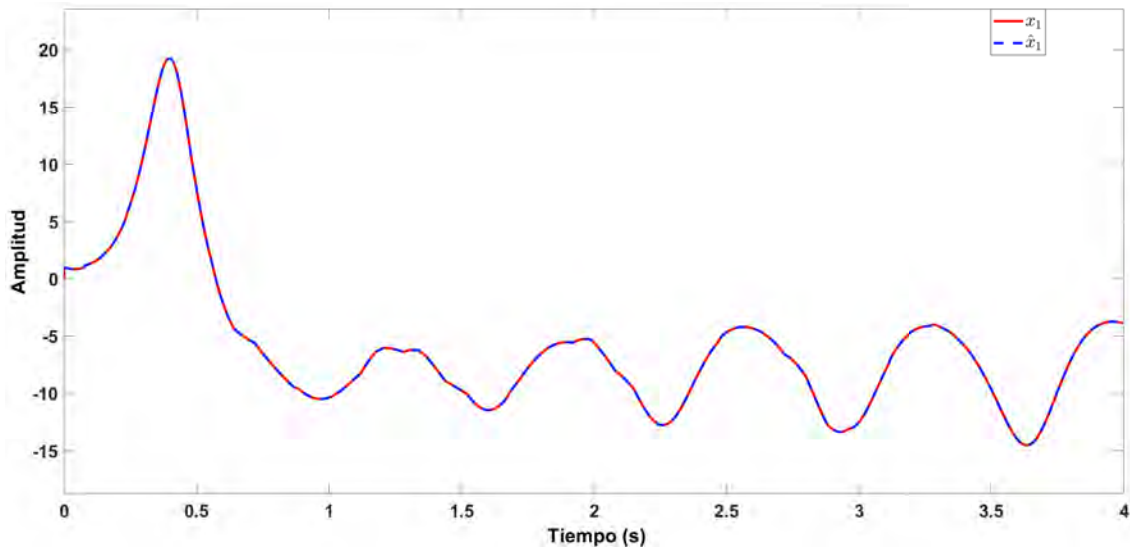


Fig. 6.1. Comparación del estado $x_1(t)$ del Observador Maestro-Esclavo y Sistema No Lineal

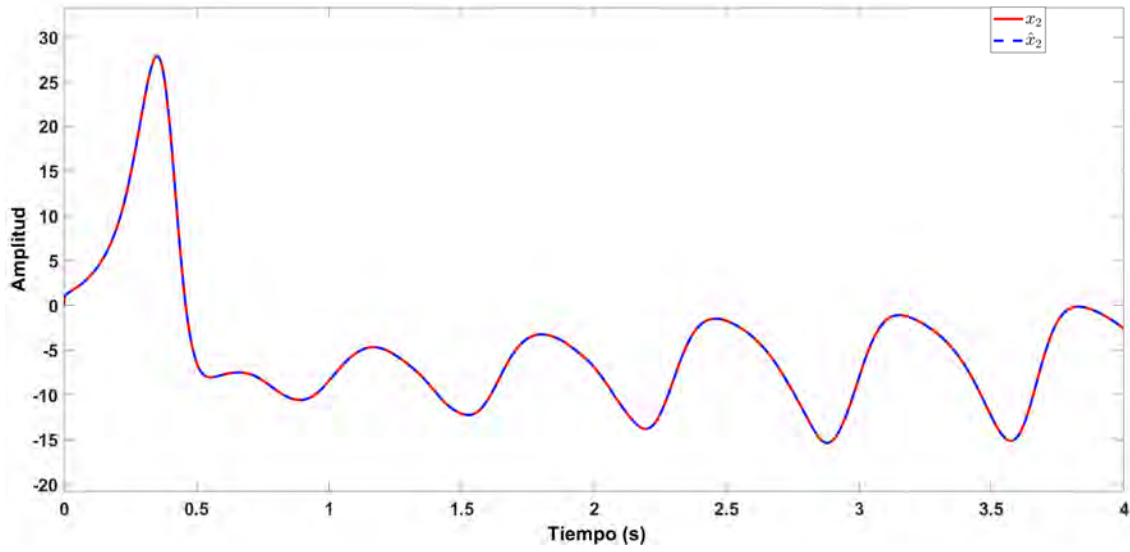


Fig. 6.2. Comparación del estado $x_2(t)$ del Observador Maestro-Esclavo y Sistema No Lineal

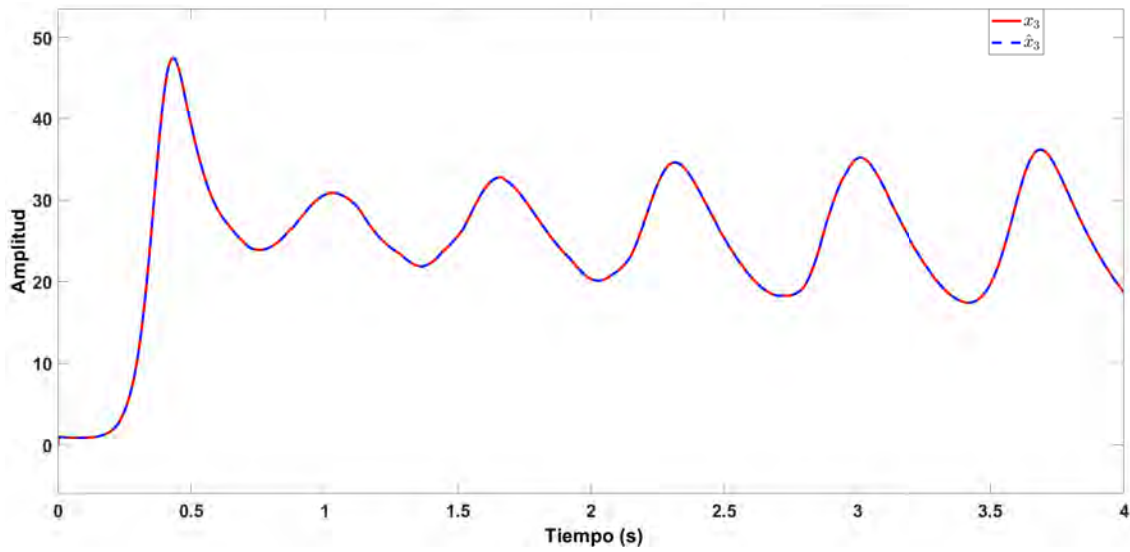


Fig. 6.3. Comparación del estado $x_3(t)$ del Observador Maestro-Esclavo y Sistema No Lineal

La Figura 6.4 muestra la evolución del error entre los estados del observador maestro-esclavo y los del sistema no lineal.

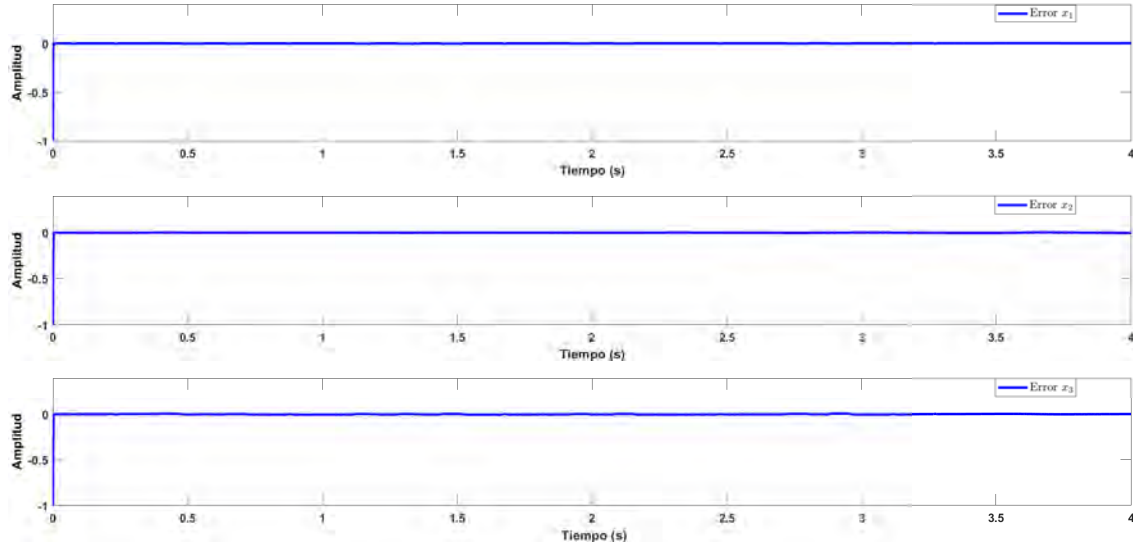


Fig. 6.4. Error del Observador Maestro-Esclavo con el Sistema No Lineal

Para evaluar el observador maestro-esclavo, se analizó el error entre sus estados y los del sistema no lineal. La Tabla 6.1 resume los resultados obtenidos, y enseguida se presentan las fórmulas utilizadas para calcular los respectivos índices de desempeño.

La integral del cuadrado del error, ISE, el cual se define como:

$$ISE = \int_0^T e^2(t)dt. \quad (6.19)$$

La integral del valor absoluto de la magnitud del error, IAE, el cual se define como:

$$IAE = \int_0^T |e(t)|dt. \quad (6.20)$$

Tabla 6.1. Valores de los índices de desempeño del observador maestro-esclavo

Estado	ISE	IAE
$x_1(t)$	1.23×10^{-4}	7.93×10^{-3}
$x_2(t)$	2.17×10^{-4}	3.54×10^{-3}
$x_3(t)$	2.97×10^{-4}	9.70×10^{-3}

Como puede observarse en la Tabla 6.1, los valores obtenidos para los índices ISE e IAE son bajos en los tres estados, lo que indica que el observador maestro-esclavo presenta un buen desempeño en la estimación del sistema no lineal, logrando una convergencia precisa y eficiente.

6.2.3. Estimación del mensaje

Durante la simulación, se utilizó el sistema transmisor completo que incluye la señal cifrada $p(t)$; sin embargo, para el diseño del observador únicamente se consideró el modelo base del sistema de Lorenz. En este contexto, cuando el error de estimación del estado tiende a cero, se puede asumir que $\hat{x}(t) \approx x(t)$, lo que permite obtener la siguiente aproximación:

$$\hat{y}(t) = C\hat{x}(t) + E\hat{p}(t) \quad (6.21)$$

Debido a que la matriz E posee un rango de columna completo, es posible llevar a cabo la estimación del mensaje de la siguiente manera:

$$\hat{p}(t) = E^+ (y(t) - \hat{y}(t)) \quad (6.22)$$

donde E^+ es cualquier inversa generalizada de E tal que $EE^+E = E$.

En la Figura ?? se muestra el resultado de la estimación del mensaje obtenida mediante el observador proporcional. Se aprecia que la estimación del mensaje cifrado es prácticamente inmediata, logrando una estimación precisa desde los primeros instantes, sin que se presente pérdida de información significativa durante el proceso.

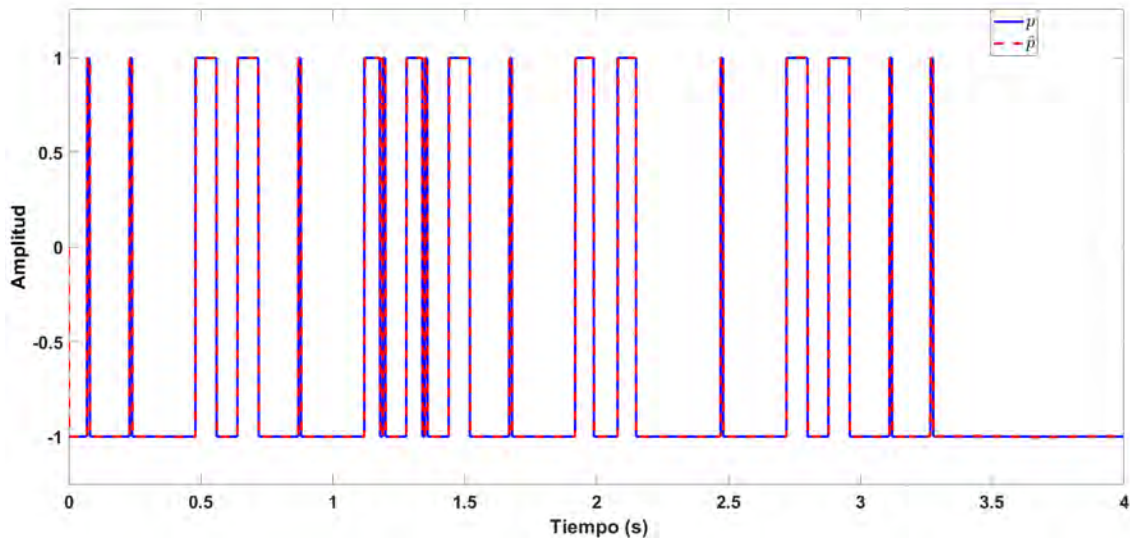


Fig. 6.5. Mensaje estimado con el Observador Maestro-Esclavo

6.3. Conclusiones del capítulo

En este capítulo se desarrolló un observador de estados con convergencia en tiempo finito, basado en una arquitectura maestro-esclavo. Utilizando la dinámica del sistema maestro junto con un término correctivo en el sistema esclavo que permite alcanzar la sincronización de estados en un tiempo limitado, siempre que se cumplan ciertas condiciones relacionadas con las ganancias y la estructura del error.

La validez teórica del diseño fue respaldada por simulaciones numéricas, en las cuales el observador fue capaz de estimar con alta precisión los estados del sistema no lineal a pesar de partir de condiciones iniciales diferentes. Los resultados obtenidos, evaluados mediante los índices de desempeño ISE e IAE, evidencian un bajo error de estimación, confirmando la efectividad del observador propuesto.

Finalmente, se mostró que, una vez alcanzada la sincronización, es posible aplicar el modelo para estimar correctamente un mensaje cifrado en un sistema caótico, destacando su potencial utilidad en aplicaciones de comunicación segura.

Capítulo 7

Enmascaramiento Caótico de Señales de Audio: Cifrado y Descifrado

7.1. Objetivo de diseño

En la actualidad, la protección de datos digitales es fundamental, especialmente cuando se trata de información sensible transmitida a través de canales públicos. El cifrado de señales de audio utilizando sistemas caóticos se presenta como una solución robusta y eficiente, debido a la naturaleza impredecible y altamente sensible a los parámetros iniciales.

El proceso comienza con la conversión de la señal analógica a digital, ya que el procesamiento y cifrado se realizan sobre una secuencia binaria que representa la información. Esta representación permite manipular la señal para realizar el enmascaramiento caótico permitiendo incorporar los bits de audio dentro de las variables de un sistema dinámico caótico.

Para el proceso de descifrado, se emplean observadores, herramientas utilizadas para estimar las variables internas de un sistema dinámico a partir de salidas observables. En este caso, el observador permite recuperar la señal binaria original a partir de la dinámica caótica cifrada, aun sin acceso directo a todas las variables del sistema.

Finalmente, la señal estimada se convierte de digital a analógica mediante la reconstrucción de muestras, permitiendo la reproducción del archivo de audio y evaluando la efectividad de los observadores implementados.

7.1.1. Algoritmo de cifrado caótico

A continuación, se describe el preprocesamiento realizado sobre un archivo de audio antes de su integración en un sistema de cifrado caótico. Este procedimiento transforma la señal analógica en una secuencia binaria adecuada para su posterior manipulación digital. Cada paso busca facilitar el manejo computacional del audio y preparar sus datos para ser enmascarados mediante técnicas basadas en sistemas dinámicos caóticos, como se ilustra en la Figura 7.1.

1. Cargar archivo de audio (.wav):

Se emplea un archivo de audio en formato `.wav`, debido a que es un formato sin compresión que permite un acceso directo a las muestras.

2. Usar solo un canal (mono):

En caso de que el audio esté en estéreo, se selecciona únicamente uno de los canales (generalmente el izquierdo), con el objetivo de simplificar el procesamiento. Esto reduce la señal a una única serie de muestras.

3. Convertir audio a enteros (formato `int16`):

Las muestras del archivo de audio se convierten al formato de enteros con signo de 16 bits (`int16`), que es estándar en procesamiento de audio. Cada muestra queda representada por un valor entre -32768 y 32767 .

4. Convertir a ceros y unos (formato binario):

Cada valor entero obtenido se transforma a su equivalente en binario de 16 bits. Esto permite representar la señal en formato digital puro, como una secuencia de bits (ceros y unos).

5. Unir todos los bits en fila (crear tira de bits):

Los bits binarios generados se concatenan uno tras otro para formar una larga cadena binaria o tira de bits, que representa toda la señal original de audio de manera continua.

6. Guardar los bits (formato `.mat`):

La tira binaria se almacena en un archivo con formato `.mat`, compatible con MATLAB. Este formato permite guardar vectores, matrices u otras estructuras complejas de datos.

7. Agregar al sistema caótico (enmascaramiento caótico):

Finalmente, los bits son incorporados a un sistema caótico para aplicar el proceso de *enmascaramiento caótico*.

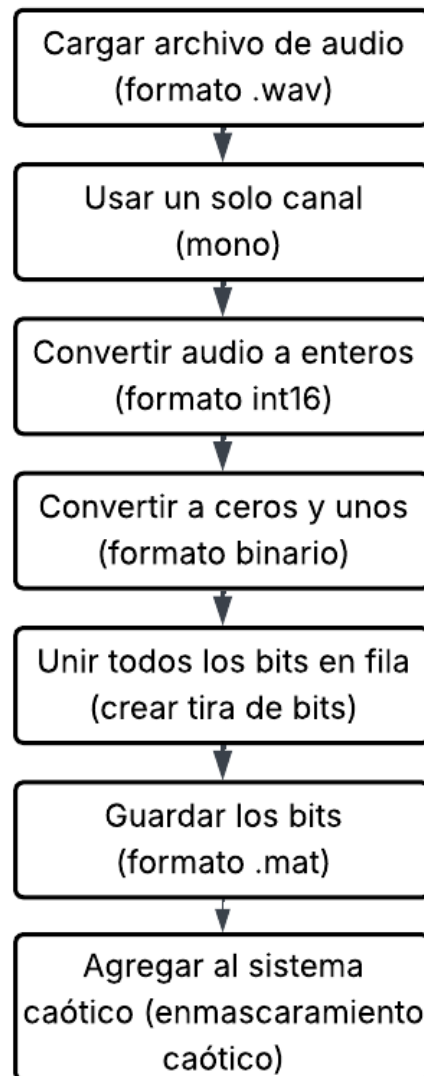


Fig. 7.1. Diagrama del algoritmo de cifrado caótico

7.1.2. Algoritmo de descifrado caótico

En esta etapa se lleva a cabo el proceso de reconstrucción de la señal de audio a partir de su representación binaria estimada. El objetivo es revertir las transformaciones aplicadas previamente, recuperando las muestras originales a partir de la tira de bits almacenada. Una vez restaurada la señal, se genera un nuevo archivo de audio para evaluar la efectividad del proceso de cifrado y descifrado caótico, como se muestra en la Figura 7.2.

1. **Cargar bits (formato `.mat`):**

Se carga el archivo con extensión `.mat`, el cual contiene la tira de bits generada en el proceso de enmascaramiento. Este archivo debe contener una secuencia binaria en formato vectorial.

2. **Verificar que los bits se pueden agrupar de 16:**

Dado que cada muestra de audio original fue convertida a un entero de 16 bits, es necesario comprobar que la longitud total de la tira de bits es un múltiplo de 16.

3. **Agrupar cada 16 bits (muestra de sonido):**

La tira de bits se divide en bloques de 16 bits consecutivos, donde cada grupo representa una muestra de audio en su forma binaria original.

4. **Convertir cada grupo a número (entre -1 y 1):**

Cada grupo de 16 bits se convierte a un número entero con signo (formato `int16`), y luego se normaliza dividiéndolo por el valor máximo (2^{15}) para obtener una señal con valores entre -1 y 1 .

5. **Crear archivo de audio (formato `.wav`):**

A partir del conjunto de muestras reconstruidas, se genera un nuevo archivo de audio en formato `.wav`

6. **Reproducir audio:**

Finalmente, el archivo generado puede ser reproducido utilizando cualquier reproductor compatible, lo que permite verificar la fidelidad de la reconstrucción y evaluar el éxito del proceso de cifrado y descifrado.

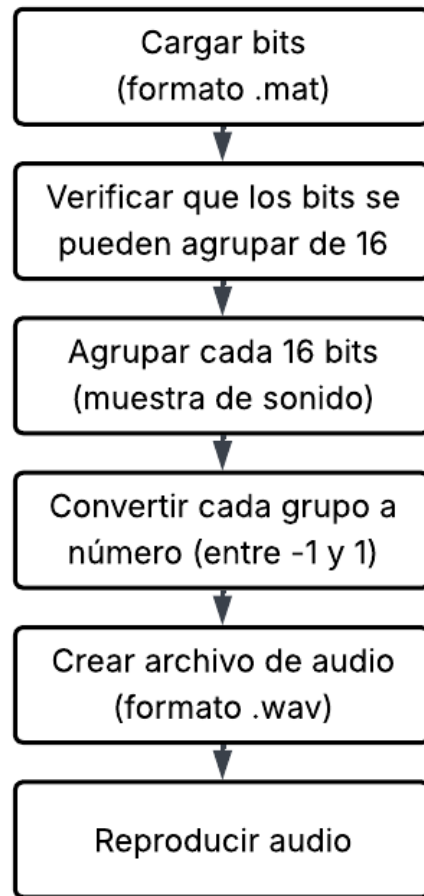


Fig. 7.2. Diagrama del algoritmo de descifrado caótico

7.1.3. Validación de cifrado y descifrado caótico

A continuación se presentan los resultados obtenidos al validar el sistema de cifrado y descifrado caótico utilizando tres diferentes archivos de audio. Para cada caso, se muestran las tres etapas principales del proceso: la señal del audio original, la señal de bits resultante después de aplicar el algoritmo de cifrado, y la señal de audio recuperada tras el algoritmo de descifrado.

Prueba 1: Hola Mundo con voz robotizada

En las Figuras 7.3-7.5 se muestran la señal de audio original, la señal binaria obtenida tras aplicar el algoritmo de cifrado y finalmente el audio recuperado tras el proceso de descifrado.

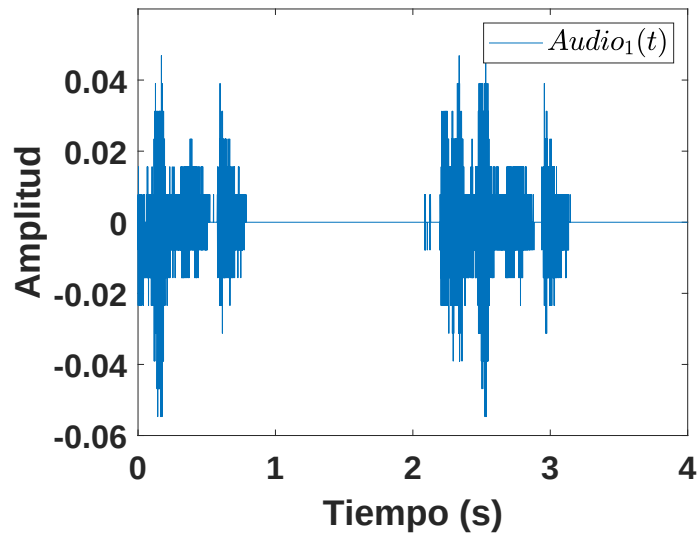


Fig. 7.3. Señal de audio Hola Mundo con voz robotizada

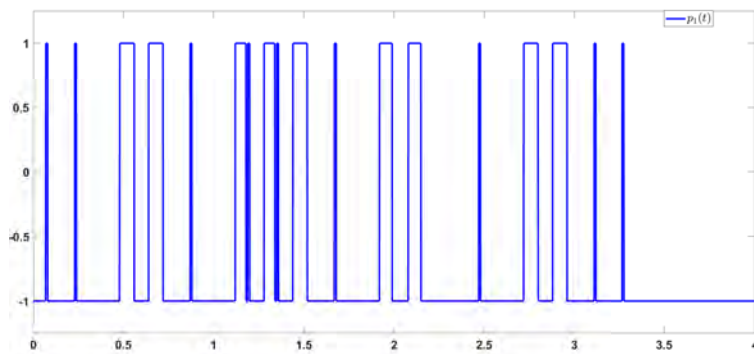


Fig. 7.4. Señal binaria correspondiente al audio Hola Mundo con voz robotizada

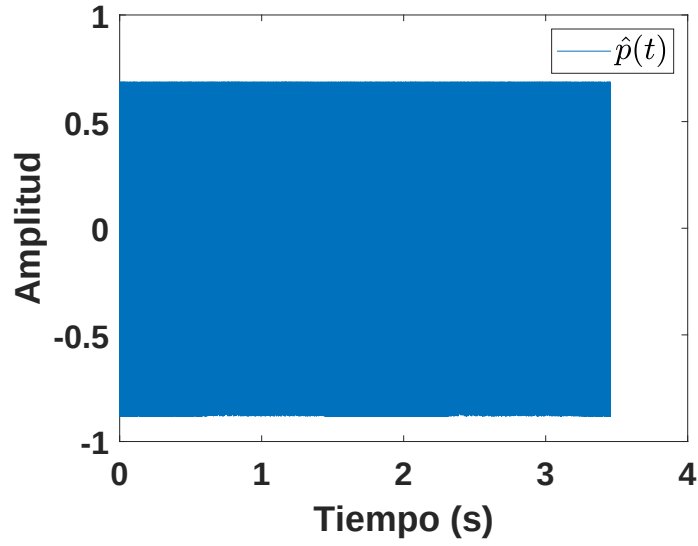


Fig. 7.5. Señal de audio recuperada Hola Mundo con voz robotizada

Prueba 2: Secuencia de números del 1 al 6

Para el segundo audio, que corresponde a una secuencia numérica de los dígitos del 1 al 6, se presentan también en las Figuras 7.6-7.8 las tres etapas de análisis: señal original, señal de bits y audio descifrado.

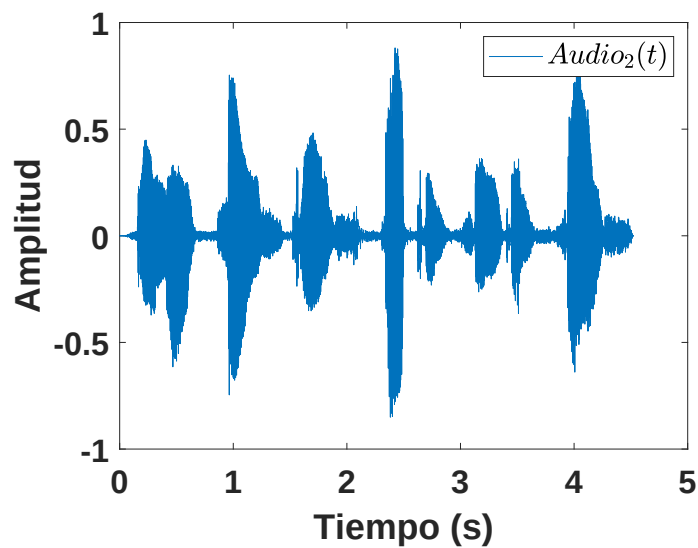


Fig. 7.6. Señal de audio de secuencia de números del 1 al 6

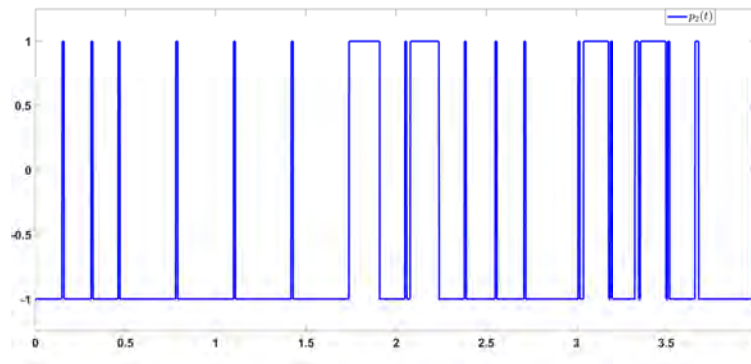


Fig. 7.7. Señal binaria correspondiente al audio de secuencia de números del 1 al 6

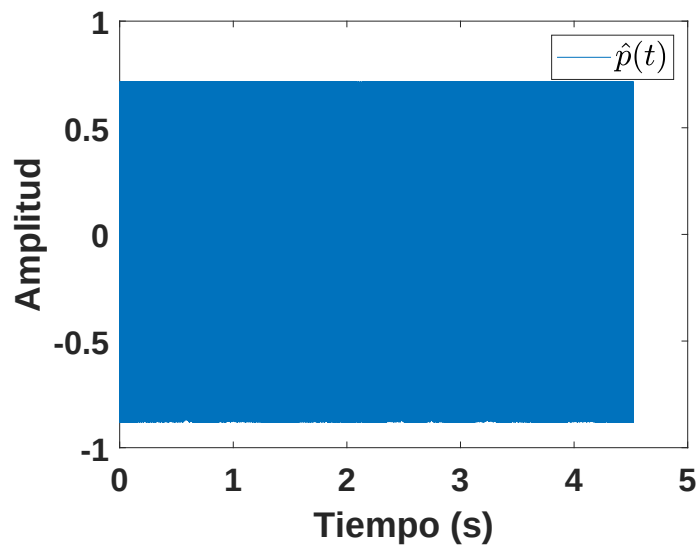


Fig. 7.8. Señal de audio recuperada de secuencia de números del 1 al 6

Prueba 3: Hola Mundo con entonación natural

Finalmente, para el tercer audio, que corresponde al mensaje Hola Mundo pronunciado con voz natural, en las Figuras 7.9-7.11 se presentan las tres etapas del proceso.

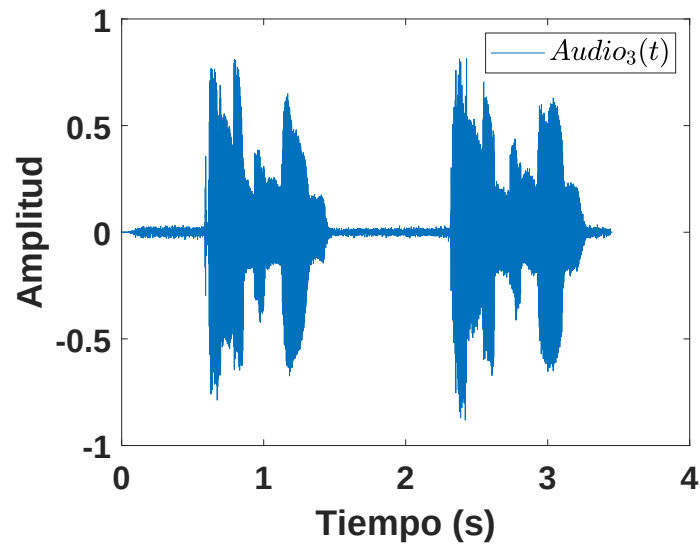


Fig. 7.9. Señal de audio Hola Mundo con entonación natural

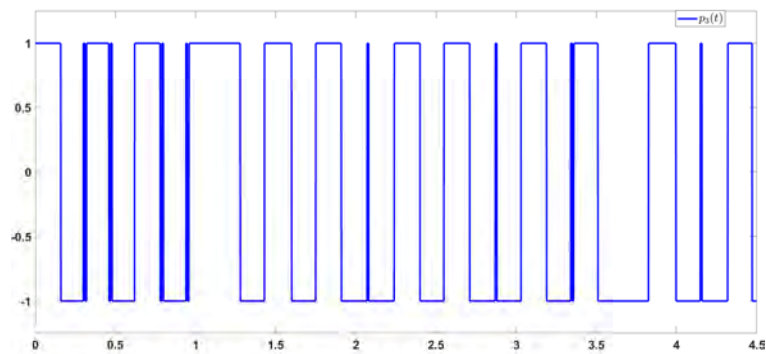


Fig. 7.10. Señal binaria correspondiente al audio Hola Mundo con entonación natural

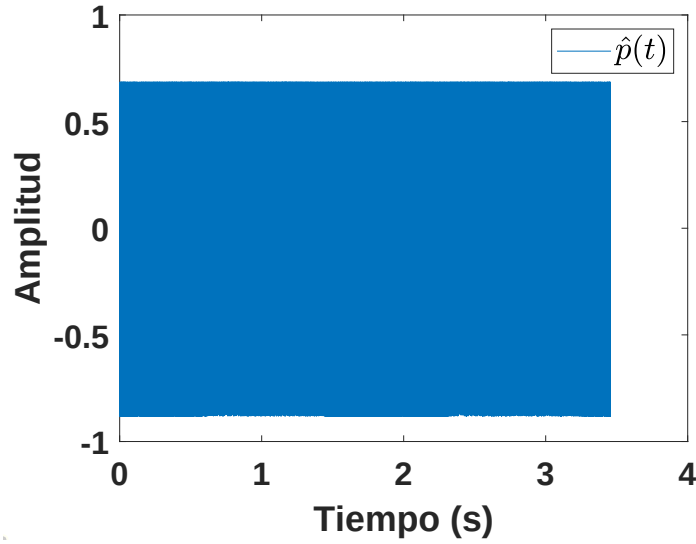


Fig. 7.11. Señal de audio recuperada Hola Mundo con entonación natural

7.2. Conclusión del capítulo

En este capítulo se implementó un algoritmo de cifrado y descifrado de señales de audio utilizando sistemas caóticos, destacando su capacidad para proporcionar un alto nivel de seguridad en la transmisión de información. El enfoque propuesto aprovecha la naturaleza compleja y no lineal de los sistemas dinámicos caóticos para ocultar eficazmente la información binaria de la señal.

El algoritmo transformó las señales de audio a un formato binario apto para su integración en un sistema caótico, facilitando su encriptación mediante el enmascaramiento de los bits dentro de las variables del sistema. Posteriormente, el proceso inverso, guiado por el diseño de observadores, permitió la estimación precisa de la señal original, incluso sin conocer todas las variables internas del sistema, resaltando la utilidad de esta herramienta en escenarios de descifrado.

Las pruebas experimentales con diferentes archivos de audio confirmaron que el sistema es capaz de recuperar fielmente las señales originales tras el proceso de cifrado y descifrado. Si bien las señales descifradas presentan un leve nivel de ruido, la información auditiva es completamente comprensible. Esta distorsión mínima genera ligeros cambios en la forma de onda respecto a la señal original, sin comprometer su inteligibilidad.

Capítulo 8

Conclusiones generales

A lo largo del desarrollo de esta tesis, se abordó el diseño de un esquema criptográfico innovador basado en el enmascaramiento caótico, utilizando como base el sistema dinámico de Lorenz modelado mediante la representación Takagi-Sugeno (T-S). La elección de esta metodología respondió a la necesidad de implementar sistemas de comunicación seguros que, además de preservar la confidencialidad de la información, permitan garantizar la sincronización precisa entre transmisor y receptor sin alterar la estructura del mensaje original.

El principal aporte de este trabajo radica en la integración de técnicas de control con enfoques de criptografía, ofreciendo una solución novedosa a un problema vigente en el ámbito de la seguridad en comunicaciones. Para ello, se diseñaron y analizaron dos tipos de observadores: un observador proporcional y otro con convergencia en tiempo finito, ambos desarrollados con base en representaciones difusas del sistema caótico. Mientras que el observador proporcional logró una estimación precisa de las variables de estado bajo un esquema de convergencia asintótica, el observador de tiempo finito se destacó por su capacidad de garantizar dicha estimación en un intervalo temporal acotado, lo que lo hace especialmente adecuado para escenarios donde la inmediatez en la sincronización es crítica.

Las simulaciones realizadas demostraron la eficacia del modelo propuesto al reproducir con alta fidelidad la dinámica del sistema original, así como al permitir el cifrado y descifrado de señales de audio sin pérdida de información. Estos resultados validan no solo la viabilidad del enfoque bajo condiciones ideales, sino también su potencial aplicación en sistemas de comunicación reales donde

se requiere un alto grado de seguridad y sincronización.

Adicionalmente, se resalta la originalidad de la propuesta, al no haberse encontrado en la literatura consultada aplicaciones que combinen observadores proporcionales y de tiempo finito en esquemas criptográficos basados en caos y modelados mediante Takagi-Sugeno. Este hecho evidencia la contribución significativa que representa esta tesis para el campo de la ingeniería electrónica, particularmente en el área de control no lineal y criptografía basada en sistemas dinámicos.

8.1. Trabajos futuros

A partir de los resultados obtenidos en esta investigación, se abren diversas líneas de trabajo que pueden fortalecer y ampliar los alcances del esquema criptográfico propuesto. A continuación, se presentan algunas recomendaciones para futuras investigaciones:

Implementación en plataformas físicas: Una de las proyecciones más relevantes es llevar a cabo la implementación del sistema en hardware embebido, como FPGAs, microcontroladores o procesadores DSP. Esto permitiría validar el desempeño del esquema en tiempo real y bajo restricciones de recursos computacionales.

Extensión a otros sistemas caóticos: Se propone investigar la aplicabilidad del diseño de observadores en otros sistemas caóticos de mayor complejidad o con diferentes estructuras, como los sistemas de Chen, Lü, o Rössler, para evaluar su desempeño.

Cifrado de otros tipos de señales multimedia: Extender el esquema de cifrado propuesto para trabajar con señales de video o imágenes podría ampliar su campo de aplicación a áreas como la videovigilancia, telemedicina o transmisión segura de contenido digital.

Estas posibles líneas de trabajo representan una continuación lógica del presente estudio y tienen el potencial de aportar soluciones avanzadas y aplicables en contextos reales donde la seguridad, eficiencia y sincronización precisa sean factores determinantes.

Bibliografía

- Aguilar-López, R. and Mata-Machuca, J. L. (2016). A new finite-time observer for nonlinear systems: Applications to synchronization of lorenz-like systems. *The Scientific World Journal*, 2016(1):p. 8342089.
- Al-Hadithi, B. M., Jiménez, A., and Matía, F. (2012). A new approach to fuzzy estimation of takagi–sugeno model and its applications to optimal control for nonlinear systems. *Applied Soft Computing*, 12(1):280–290.
- Albahrani, E. A. (2017). A new audio encryption algorithm based on chaotic block cipher. In *IEEE. Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, pages 22–27.
- Alenezi, M. N., Alabdulrazzaq, H., and Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, 12(2):256–272.
- Assali, E. A. (2021). Predefined-time synchronization of chaotic systems with different dimensions and applications. *Chaos, Solitons & Fractals*, 147:p. 110988.
- Augustine, N., George, S. N., and Pattathil, D. P. (2015). An audio encryption technique through compressive sensing and arnold transform. *International Journal of Trust Management in Computing and Communications*, 3(1):74–92.
- Bonilla, S. J. (2021). Algoritmo de cifrado de audio digital mediante atractores caóticos. Master’s thesis, Universidad Distrital Francisco José de Caldas.
- Cardoza-Avendano, L., Spirin, V., López-Gutiérrez, R., López-Mercado, C., and Cruz-Hernández,

- C. (2011). Experimental characterization of dfb and fp chaotic lasers with strong incoherent optical feedback. *Optics & Laser Technology*, 43(5):949–955.
- Chadli, M. (2010). An lmi approach to design observer for unknown inputs takagi-sugeno fuzzy models. *Asian Journal of Control*, 12(4):524–530.
- Chadli, M. and Karimi, H. R. (2012). Notice of violation of iee publication principles: Robust observer design for unknown inputs takagi-sugeno models. *IEEE Transactions on Fuzzy Systems*, 21(1):158–164.
- Chadli, M. and Zelinka, I. (2014). Chaos synchronization of unknown inputs takagi-sugeno fuzzy: Application to secure communications. *Computers & Mathematics with Applications*, 68(12):2142–2147.
- Chen, G. (1993). Yet another chaotic attractor. *Intl. J. of Bif. & Chaos*, 2(3):705–708.
- Cuomo, K., Oppenheim, A., and Strogatz, S. (1993a). Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II*.
- Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H. (1993b). Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on circuits and systems II: Analog and digital signal processing*, 40(10):626–633.
- Djennoune, S., Bettayeb, M., and Al Saggaf, U. M. (2019). Impulsive observer with predetermined finite convergence time for synchronization of fractional-order chaotic systems based on takagi-sugeno fuzzy model. *Nonlinear Dynamics*, 98:1331–1354.
- Flores-Hernández, A., Reyes-Reyes, J., Astorga-Zaragoza, C., Osorio-Gordillo, G., and García-Beltrán, C. (2018). Temperature control of an alcoholic fermentation process through the Takagi-Sugeno modeling. *Chemical Engineering Research and Design*, 140:320–330.
- Grassi, G. and Mascolo, S. (1997). Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(10):1011–1014.

- Hassan, M. F. and Hammuda, M. (2019). A new approach for constrained chaos synchronization with application to secure data communication. *Journal of the Franklin Institute*, 356(12):6697–6723.
- Lendek, Z., Guerra, T. M., Babuška, R., and De Schutter, B. (2011). *Stability Analysis and Nonlinear Observer Design Using Takagi-Sugeno Fuzzy Models*. Springer Berlin Heidelberg.
- Lian, K.-Y., Chiu, C.-S., Chiang, T.-S., and Liu, P. (2001). Secure communications of chaotic systems with robust performance via fuzzy observer-based design. *IEEE Transactions on fuzzy systems*, 9(1):212–220.
- Lorenz, E. (1963). Deterministic nonperiodic flow. *Journal of atmospheric sciences*.
- Mesiya, M. F. (2013). *Contemporary communication systems*. McGraw-Hill New York, NY.
- Munmuangsaen, B. and Srisuchinwong, B. (2018). A hidden chaotic attractor in the classical lorenz system. *Chaos, Solitons & Fractals*, 107:61–66.
- Ogata, K. (2010). *Ingeniería de control moderna*. Number 5 ed. Pearson Education.
- Pecora, L. M. and Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical review letters*, 64(8):821.
- Ramirez, R. D. M. (2018). Implementación de osciladores caóticos en sistemas embebidos y aplicaciones. *Ensenada, Baja California, México:[sn]*.
- Ríos-Ruiz, C., Osorio Gordillo, G. L., Darouach, M., Souley Ali, H., and Astorga-Zaragoza, C. M. (2024). Design of finite-time convergent functional observer for descriptor systems: Application to fault estimation. *Asian Journal of Control*.
- Rodríguez Liñán, J. Á. and León Morales, J. D. (2007a). Sincronización de caos mediante observadores para cifrado en comunicaciones. *Ingenierías*, 10(34):44–50.
- Rodríguez Liñán, J. Á. and León Morales, J. d. (2007b). Sincronización de caos mediante observadores para cifrado en comunicaciones. *Ingenierías*, 10(34):44–50.
- Schuster, H. G. and Just, W. (2006). *Deterministic chaos: an introduction*. John Wiley & Sons.

- Takagi, T. and Sugeno, M. (1985). Fuzzy identification of systems and its applications to modeling and control. *IEEE transactions on systems, man, and cybernetics*, (1):116–132.
- Tomasi, W. (2003). *Sistemas de comunicaciones electrónicas*. Pearson educación.
- Wang, Y.-W., Guan, Z.-H., and Wang, H. O. (2005). Impulsive synchronization for takagi–sugeno fuzzy model and its application to continuous chaotic system. *Physics letters A*, 339(3-5):325–332.
- Xu, X., Ngoc Cuong, T., Lee, S.-D., and You, S.-S. (2020). Secure communication system in maritime navigation using state observer with linear matrix inequality. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 4(3):70–75.
- Zaidi, I., Tadeo, F., and Chaabane, M. (2013). Positive observer design for continuous-time takagi–sugeno systems. In *52nd IEEE Conference on Decision and Control*, pages 5030–5035.
- Zhou, C., Li, Q., Li, F., and He, P. (2018). Finite-time bounded functional observer design for a class of nonlinear systems. In *37th IEEE Chinese Control Conference (CCC)*, pages 36–41.