UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
Facultad de Ingeniería, Arquitectura y Diseño
Maestría y Doctorado en Ciencias e Ingeniería

DISEÑO DE UN PROTOTIPO ENCRIPTADOR-DESENCRIPTADOR HIPERCAÓTICO DE AUDIO CON COMUNICACIÓN WIFI

TESIS

Que para obtener el título de

MAESTRO EN INGENIERÍA

presenta:

Francisco Zamora Arellano

Director de tesis
Dr. Enrique Efren García Guerrero

Ensenada, Baja California, México, diciembre de 2013

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Facultad de Ingeniería, Arquitectura y Diseño

Maestría y Doctorado en Ciencias e Ingeniería

DISEÑO DE UN PROTOTIPO ENCRIPTADOR-DESENCRIPTADOR HIPERCAÓTICO DE AUDIO CON COMUNICACIÓN WIFI

TESIS

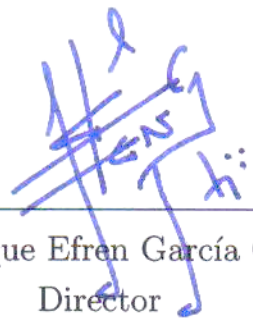
Que para obtener el título de

MAESTRO EN INGENIERÍA

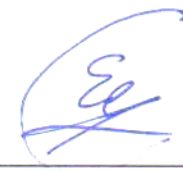
presenta:

FRANCISCO ZAMORA ARELLANO

y aprobada por el siguiente comité:

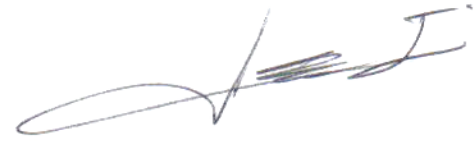


Dr. Enrique Efren García Guerrero
Director

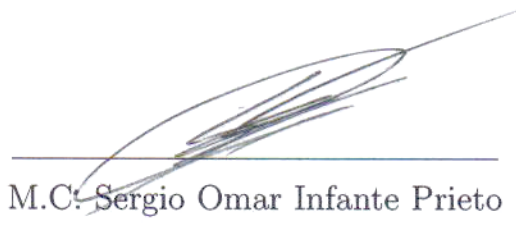


Dr. Everardo Inzunza González
Co-director

Dr. Oscar Roberto López Bonilla
Sinodal



Dr. Juan Iván Nieto Hipólito
Sinodal



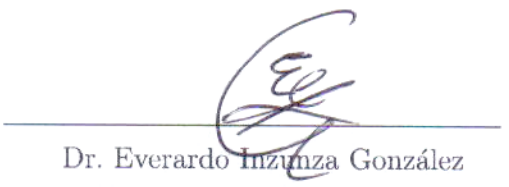
M.C. Sergio Omar Infante Prieto
Sinodal

RESUMEN de la tesis de **Francisco Zamora Arellano**, presentada como requisito para obtener el grado de MAESTRO EN INGENIERÍA, del programa de Maestría y Doctorado en Ciencias e Ingeniería de la UABC. Ensenada, Baja California, México, Diciembre de 2013.

DISEÑO DE UN PROTOTIPO ENCRIPTADOR-DESENCRIPTADOR HIPERCAÓTICO DE AUDIO CON COMUNICACIÓN WIFI

Resumen aprobado por:

Dr. Enrique Efren García Guerrero
Director de Tesis



Dr. Everardo Inzunza González
Co-Director de Tesis

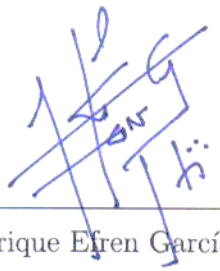
En este trabajo de tesis de maestría, se presenta el diseño e implementación de un prototipo encriptador-desencriptador de audio basado en un microcontrolador RCM5600W con comunicación WiFi. El dispositivo implementado presenta varias ventajas de innovación tecnológica para aplicaciones en comunicaciones seguras: i) permite la elección del mapeo caótico en el proceso de encriptado-desencriptado, que puede ser: Hénon, Ikeda, Kaplan-Yorke, Logístico 2D y el Hipercaótico de Rössler, ii) el sistema criptográfico implementado ejecuta el proceso de encriptado-desencriptado en el dispositivo desarrollado, el cual opera como un periférico de computadora empleando comunicación WiFi y iii) el usuario final interacciona con el dispositivo encriptador-desencriptador a través de una interfaz gráfica y amigable que permite la manipulación en tiempo real de señales de audio. Se validan los niveles de seguridad del sistema criptográfico implementado, a partir del análisis del espacio de claves, análisis de sensibilidad, histogramas estadísticos y entropía de la información. Finalmente se presenta una metodología para obtener ecuaciones con comportamiento caótico, a partir de números aleatorios y procesos de cómputo evolutivo.

Palabras clave: Comunicación WiFi, criptografía caótica, mapeo caótico, rabbit RCM5600W, análisis de seguridad.

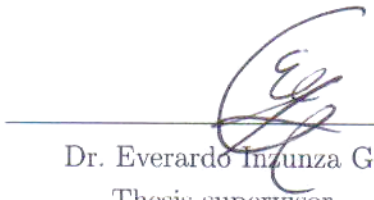
Thesis **ABSTRACT** of **Francisco Zamora Arellano**, presented as requirement to obtain the degree in MASTER IN ENGINEERING, from the program of Master and PhD in Sciences and Engineering of UABC. Ensenada, Baja California, Mexico, December 2013.

DESIGN OF AN AUDIO HYPERCHAOTIC ENCRYPTER-DECRYPTER WITH WIFI COMMUNICATION

Abstract approved by:



Dr. Enrique Efren García Guerrero
Thesis supervisor



Dr. Everardo Inzunza González
Thesis supervisor

In this master's thesis, the design and implementation of a prototype hyperchaotic encryption-decryption based in the RCM5600W microcontroller with WiFi communication is presented. This implemented device has different features and technological innovation advantages, to be applied in secure communications: i) it allows to choose different chaotic maps in the encryption-decryption process, the maps are: Henon, Ikeda, Kaplan-Yorke, Logistic 2D and the hyperchaotic Rössler map, ii) The implemented cryptographic system executes the encryption-decryption process in the developed device, which operates as a computer peripheral using WiFi communication, and iii) The final user interacts with the encrypter-decrypter device through a friendly graphic interface, which allows signal audio manipulation in real time. The different cryptographic levels of security of the system are validated, from a security analysis, key space, analysis of sensibility, statistical histograms and information entropy. Finally, a methodology is presented to obtain equations with chaotic behavior from random numbers and evolutionary computing.

Keywords: WiFi communication, chaotic cryptography, chaotic map, Rabbit RCM5600W, security analysis.

Dedicatoria

A mis padres quienes desde niño me hicieron a la idea que para progresar hay que ganarse las cosas por propios méritos.

A mi hermano Osvaldo y su esposa, mi hermana por ley Dámaris y a mi sobrina Valeria.

A todos mis familiares para que se animen a seguir preparandose profesionalmente.

Al pueblo mexicano y a la población mundial, porque el desarrollo, la ciencia, la tecnología, las artes y las maravillas humanas, no son aportación de una sola persona, sino de cada individuo en este mundo.

A mis compañeros y amigos de la vida, la escuela y de Tae Kwon do con quienes siempre habra el objetivo de mantener mente sana en un cuerpo sano.

Agradecimientos

Al profesor ***Enrique Efrén García Guerrero*** *por el excelente trabajo como director de tesis y guía en mi formación profesional, así como del mutuo apoyo para lograr además de la conclusión de mi maestría, avance y aportaciones a la ciencia y tecnología, esperando convertirnos en futuros colaboradores en el desarrollo de ciencia y avances tecnológicos.*

Al profesor ***Everando Inzunza Gonzalez*** *por su apoyo durante el programa de maestría en sus diferentes etapas, esperando convertirnos en futuros colaboradores en el desarrollo de ciencia y avances tecnológicos.*

A los profesores ***Oscar Roberto López Bonilla, Sergio Omar Infante Prieto y Juan Iván Nieto Hipólito*** *por sus aportaciones y crítica profesional hacia este trabajo de tesis, para lograr la calidad esperada de un proyecto de investigación.*

Al profesor ***Jonathan Blacklegde*** *del Instituto de tecnología de Dublín por haberme recibido y haberme dado la oportunidad de trabajar con él en una estancia de investigación durante septiembre de 2012.*

A mi ***familia y amigos*** *por todos los buenos y malos momentos que hacen la vida.*

Al ***Consejo Nacional de Ciencia y Tecnología*** *por la beca que cubre gastos de manutención durante los estudios de maestría y la beca mixta con la cual pude realizar una estancia de investigación en Dublín, Irlanda.*

Al ***pueblo mexicano*** *quien con sus impuestos hace posible recibir estas becas.*

A la ***Universidad Autónoma de Baja California*** *por la exención de pago de colegiatura y por ser una universidad con grandes expectativas en el desarrollo de nuevos profesionistas, de ciencia y de tecnología a nivel mundial.*

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Capítulo I

1. Introducción

En la actualidad, debido a la necesidad de proteger la información que se transmite mediante distintos medios de comunicación, se utilizan diferentes protocolos de seguridad en los sistemas de telecomunicaciones, ya sea la telefonía, el internet, la televisión, radio, etc. Estos sistemas comprenden tecnologías existentes de telecomunicaciones como satélites, antenas, computadoras, celulares, dispositivos de almacenamiento electrónicos, etc. A estas redes de comunicación se les han adaptado protocolos de encriptado de información como el DES (Data Encryption Standard)[Sánchez 1999] desde 1976 y desde 2002 el AES (Advanced Encryption Standard)[AES 2001]. El protocolo DES ha dejado de ser utilizado en la mayoría de las telecomunicaciones debido a su vulnerabilidad al criptoanálisis actual. Por otro lado el protocolo AES, es hasta el más ampliamente usado para la seguridad informática actual, y por ende, existen muchos intentos de ataque a este protocolo como se menciona en [Sahmoud et al. 2013]. Se sabe bien que conforme la tecnología y el criptoanálisis avancen esto hará que el AES se vuelva vulnerable y por tanto, fácil de descifrar.

Wikileaks es una organización sin fines de lucro que publica información secreta, cables de noticias e información clasificada de fuentes anónimas; mucha información de diferente ámbito fue expuesta al público, desde documentos de embajadas hasta documentación de la guerra de Irak y Afghanistan desde 2001 [Wikileaks 2012], la falta de seguridad de ésta información evidencía la necesidad de implementar nuevos métodos de encriptado y su desarrollo.

Hoy en día existe y es utilizado ampliamente el protocolo 802.11 WiFi [Mustafa Ergen 2002], el cual es un estandar de comunicación inalámbrica para redes LAN utilizado en todo el mundo, muchas de las computadoras portátiles, celulares, tablets, e inclusive algunos electrodomésticos utilizan módulos WiFi para comunicación de datos. El envío de información vía inalámbrica hace que cualquier persona, dentro del espectro de alcance de una señal WiFi, pueda acceder a estos datos, por lo que se hace impresindible emplear protocolos de seguridad para este tipo de señales inalámbricas.

Los protocolos actuales utilizados para la comunicación entre puntos de acceso son el WEP (Wired Equivalent Privacy), WPA(WiFi Protected access) y WPA2. El protocolo WEP es

muy vulnerable y es ahora en la práctica poco recomendable para proteger información, por otro lado WPA y WPA2 tienen muy pocas debilidades y contiene una serie de recomendaciones a seguir para que sea eficiente [Lehembre G. 2006], mientras que los protocolos para encriptar la información son los ya mencionados AES y DES.

A code a la evidencia histórica de que los sistemas de encriptado tienen solo un tiempo determinado de vida útil, nuevas investigaciones en la criptografía cuántica [Gisin et al. 2002] y criptografía caótica [Amigó et al. 2007] indican que estos tipos de criptografía desplazarán los métodos actuales de encriptado. El contínuo estudio del caos y la aplicación en la criptografía, han sido primordiales para una futura estandarización en los sistemas de comunicaciones, es ya evidente la fiabilidad de estos sistemas desde factores de implementación, costos, adaptación y complejibilidad lo que va motivando a una tendencia a la anulación de los métodos actuales de encriptado.

En este trabajo de tesis se implementa un prototipo encriptador-desencriptador de audio en comunicación WiFi. El prototipo se basa en un microcontrolador Rabbit módulo RCM5600W, por medio de una PC se graba y se envía nuestro mensaje de audio hacia el microcontrolador, el microcontrolador se encarga de encriptar o desencriptar según sea el caso la señal de audio. Es el criptograma quién se envia por un canal público y que en nuestro caso empleamos vía WiFi.

En este trabajo de tesis planteamos nuevas formas de obtener ecuaciones caóticas, y se derivan de una estancia de investigación en el instituto de tecnología de Dublín.

El diseño del prototipo encriptador-desencriptador se detalla y presenta con resultados, al manejar un encriptador-desencriptador por medio de WiFi a una zona remota, se prueba la posibilidad del uso de la criptografía caótica via WiFi. Mediante el uso de configuración Ad-Hoc que crea una comunicación punto a punto, se establece una comunicación desde la PC al microcontrolador y se manda un mensaje de audio en forma original o en criptograma para que se realice el proceso de encriptado o desencriptado según sea el caso.

1.1. Antecedentes

Las comunicaciones seguras han existido desde la antigüedad, el primer indicio de criptografía data de hace cuatro milenios, y fue desarrollada por los egipcios al escribir en piedras con un método de sustitución de jeroglíficos [Richard Mollin 2001]. La aplicación de la criptografía ha sido necesaria en varias etapas de la historia del hombre e inclusive han definido el rumbo de la humanidad en muchas ocasiones, por tal motivo, su estudio y desarrollo se convirtió en una necesidad. Cuando el hombre comenzó a utilizar las comunicaciones seguras, muchos de los mensajes definieron batallas, guerras, conquistas; el hombre a su vez, empezó a aplicar el criptoanálisis que se encarga de encontrar debilidades en los mensajes encriptados o seguros al violar la seguridad en estos y así, descubrir su contenido.

Un mensaje potencialmente seguro es aquel en el cual la información que se quiere entregar al destinatario está encriptada, es decir oculta. La criptología es la ciencia que se encarga de estudiar la escritura secreta. La criptología incluye la criptografia, que se refiere a las técnicas para lograr crear un mensaje potencialmente seguro, muchas técnicas de encriptado se han utilizado desde hace miles de años evolucionando con el tiempo gracias al desarrollo de la ciencia y la tecnología. En la actualidad se ha logrado cifrar dichos mensajes de manera más sofisticada con el apoyo de algoritmos matemáticos [Richard Mollin 2001].

Desde la invención de los sistemas de cómputo, empezando con las computadoras mecánicas, los mensajes seguros han alcanzado un avance significativo gracias a la velocidad y capacidad de procesamiento, haciendo más eficiente el encriptado de un mensaje.

El estudio de los sistemas matemáticos caóticos tiene aproximadamente 100 años, desde los estudios del matemático francés Henri Poincaré [Edward Ott 1993], y desde hace unas dos décadas la aplicación de sistemas caóticos para el encriptado de información se ha empezado a estudiar, ejemplo de ello son los circuitos que generan dinámicas caóticas tanto analógicos como digitales [Trejo-Guerra 2009, Kevin M. Cuomo 1993]. En 1989 R. Mathews propuso por primera vez usar un algoritmo caótico para aplicación en criptografía [R. Matthews 1989], un año después Pecora y Carolle propusieron el primer método para sincronizar sistemas caóticos [Louis Pecora et al. 1990], desde hace 24 años se han publicado y expuesto diversas propuestas en relación a la criptografía caótica, año con año científicos de todo el mundo aportan más a la criptografía caótica la cual tiende a desplazar los métodos de encriptamiento

de información actuales.

1.2. Planteamiento del problema

En la actualidad, existe en el estado del arte amplia información sobre la criptografía caótica, además de soluciones propuestas y aplicaciones con sistemas de cómputo. Estudios en sistemas embebidos acerca de esta criptografía son escasos, por lo que no se conoce propiamente la manera en que se comportara el proceso de encriptado y desencriptado caótico en un sistema embebido.

1.3. Solución al problema

En este trabajo de investigación se desarrolla un programa en un microcontrolador RCM5600W, el cual consta de diversos módulos para lograr establecer una comunicación remota via WiFi, que a su vez, se encarga de realizar procesos de encriptado y desencriptado para un mensaje de voz con ciertos parámetros escogidos por el usuario. Los parametros y mensaje de voz son enviados desde una computadora, con un programa desarrollado en Matlab. Dado este diseño y aplicación de un prototipo llamado "VoicE-D", entonces se comprueba que la criptografía caótica es aplicable a los sistemas embebidos. En la figura 1 se aprecia el sistema de comunicación propuesto para dar una solución al problema.

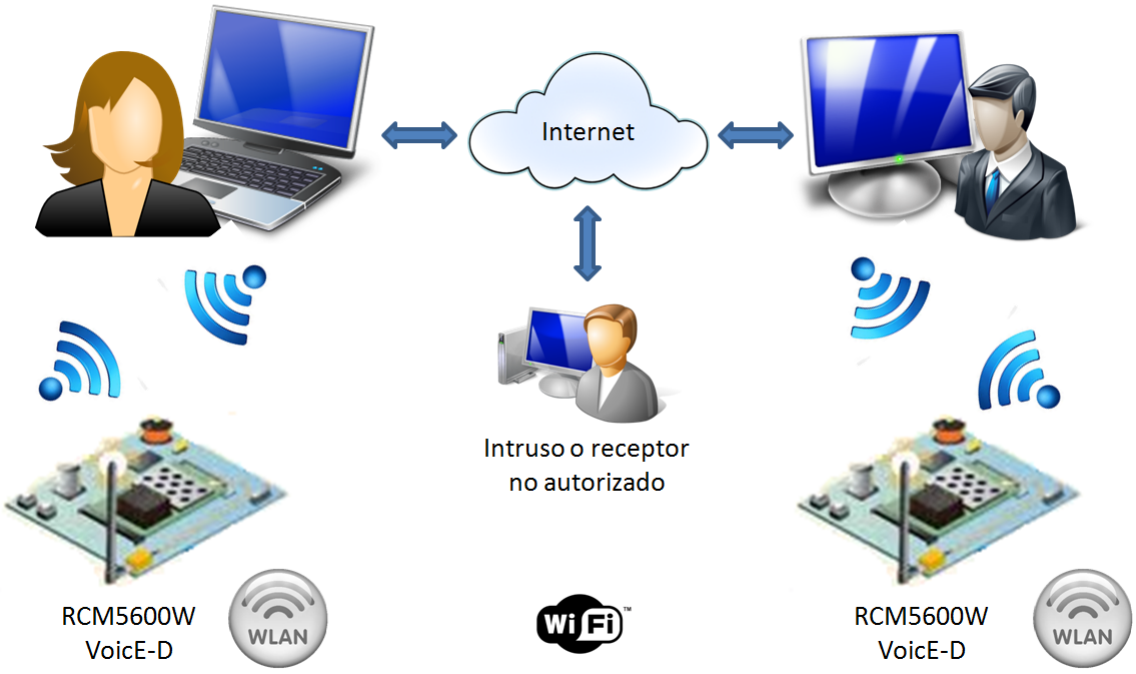


Figura 1: Sistema completo de comunicación segura utilizando el VoicE-D.

1.4. Objetivos

Objetivo general:

1.- Implementar un sistema de comunicación seguro para mensajes de voz, basado en criptografía caótica y en el microcontrolador Rabbit RCM56000W con comunicación WiFi.

Objetivos específicos:

-Lograr encriptar-desencriptar con modelos caóticos e hipercaóticos señales de audio con el microcontrolador Rabbit RCM5600W.

-Habilitar el puerto WI-FI que posee el microcontrolador para recibir y enviar audio en su forma original o como criptograma a través de una réd pública WiFi.

-Establecer la comunicación entre los dispositivos VoicE-D emisor y VoicE-D receptor, para el proceso de encriptado-desencriptado.

-Llevar a cabo un análisis de seguridad a la información generada.

Capítulo II

2. Criptografía Caótica

La Criptología es conocida como una disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que al recibir un proceso de cierta manera, se convierten en difíciles o imposibles de leer por receptores no autorizados o intrusos. La criptología se divide en dos ramas, la criptografía y el criptoanálisis [Fernández S. 2004].

La criptografía consiste en el diseño de las técnicas, algoritmos, protocolos y sistemas que dan seguridad al medio de comunicación y a las entidades que se comunican.

El criptoanálisis se encarga de capturar el significado de los mensajes construidos mediante la criptografía, sin ser el receptor autorizado. Se puede ver como el proceso inverso de la criptografía, y nos ayuda a evaluar la potencia del algoritmo criptográfico para encontrar su debilidad y poder realimentarlo.

Ataque: un ataque es cualquier intento de criptoanálisis, sí éste tiene éxito, entonces el sistema criptográfico se considera roto en el momento que el atacante consigue romper la seguridad que aporta la técnica criptográfica.

2.1. Tipos de encriptado

2.1.1. Encriptado con llave simétrica

El encriptado con llave simétrica es un método para lograr dar seguridad a la información. Consiste en que el receptor y el emisor deberán utilizar la misma clave, tanto para encriptar el mensaje, como para desencriptar el mensaje. El emisor y el receptor entonces, tendrán que ponerse de acuerdo para utilizar la misma clave, o bien, el emisor deberá mandar la clave por otro medio al receptor para que este pueda recuperar el mensaje, un problema que posee este tipo de encriptado es la distribución y manejo de las claves [Inzunza et al. 2009].

2.1.2. Encriptado con llave pública

El encriptado de clave pública es un método que protege información, de tal manera que el emisor y receptor no tengan la necesidad de compartir la clave, si no que cada usuario tiene su propia clave, es muy útil principalmente en redes de gran tamaño como por ejemplo, el internet. El emisor al encriptar el mensaje ya no puede recuperar el mensaje, ya que sólo será recuperable con la clave propia del destinatario, por lo que cada quien tiene su clave y no es necesario este intercambio de claves. Existen dos claves en este sistema, la clave pública, que es distribuida a todos los usuarios y la clave privada que posee cada miembro del sistema y es única para cada usuario, el mensaje es encriptado con la llave pública y desencriptada con la llave privada correspondiente del destinatario [Inzunza et al. 2009].

2.2. Historia de la criptografía

La criptografía tiene sus inicios desde la antigüedad, el primer indicio de criptografía fue desarrollado por los egipcios hace 4 milenios con un sistema de sustitución de jeroglíficos. También se sabe que uno de los primeros dispositivos utilizados para encriptar mensajes fue la escitala espartana, desde entonces, muchos otros métodos de encriptado fueron naciendo a lo largo de la historia, en la figura 2 podemos ver en la línea de tiempo, la aparición de diferentes dispositivos que se han inventado. Distintas técnicas y aparatos se ven simples hoy en día, pero en el tiempo que fueron utilizados, significaron grandes instrumentos para criptografía, principalmente al pobre avance del criptoanálisis de la época, conforme pasaron los siglos, y claramente como se ve en la línea del tiempo, después de la edad media, al principio del renacimiento, nuevos dispositivos fueron desarrollados siendo cada vez mas sofisticados, después de la ilustración a finales del siglo XVIII, los avances en criptografía adquirieron mucha velocidad hasta llegar a mediados del siglo XX, donde en la segunda década del siglo, la tecnología tuvo un avance muy acelerado hasta hoy en día. A continuación, se hablará de los dispositivos así como de técnicas de encriptado [Richard Mollin 2001].

Figura 2: Línea de tiempo de los dispositivos criptográficos.

2.2.1. Escitala Espartana, siglo V a.C.

Es un dispositivo que empleaba una técnica criptográfica elaborada por los éforos espartanos quienes eran elegidos democráticamente para compensar el poder del senado y el rey, para el envío de mensajes secretos. Está formada por dos varas de grosor similar variable y una tira de cuero o papiro. El envío y recepción de mensajes consistía en dos varas del mismo grosor que se entregaban a las personas partícipes de la conversación. Para enviar un mensaje se enrollaba una cinta de forma espiral a una de las varas y se escribía el mensaje longitudinalmente(figura 3), lo que hacia que en cada vuelta de la cinta apareciese una letra cada vez. Una vez escrito el mensaje, se desenrollaba la cinta y esta se enviaba al receptor, quien con una vara gemela al enrollar la cinta, recuperaba el mensaje. Es decir el sistema consistía en dos varas, la tira de cuero o papiro, la clave para recuperar el mensaje era el

grosor de la vara que se utilizaba para encriptar [Fernández S. 2004].

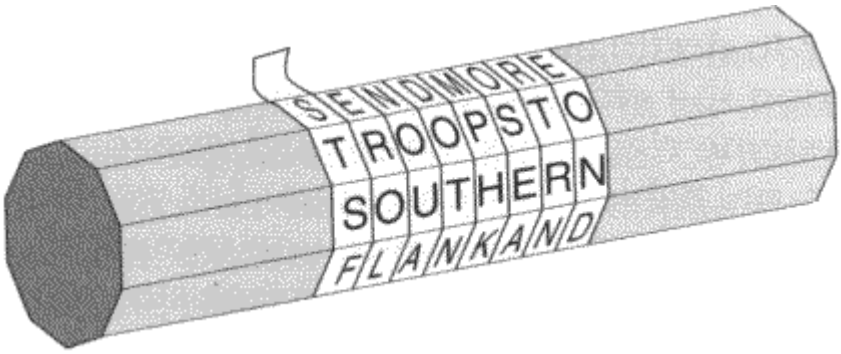


Figura 3: Imagen de una escitala.

2.2.2. Cifrador de Polybios, siglo II a.C.

Este encriptado fue realizado en la antigua Grecia y empleaba el alfabeto griego en su versión original, y esta ahora adaptado a distintos alfabetos. Consiste en colocar las letras del alfabeto en una matríz, normalmente de 5x5, y en las cabeceras de las columnas y filas se le asigna números o letras siguiendo un patrón preestablecido por el usuario del encriptado. en la figura 4 vemos una matriz encriptadora de Polybios [Fernández S. 2004].

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	ij	k
C	l	m	nñ	o	p
D	q	r	s	t	u
E	v	w	x	y	z

Figura 4: Matríz encriptadora de Polybios.

Un ejemplo para esta matríz de encriptado sería:

Mensaje a encriptar: "Buen día"

Para generar el criptograma entonces tomamos las coordenadas de cada letra empezando por fila y luego columna, a "Buen dia" corresponde: "ABDEAECC ADBDAA" la clave de este encriptado es la matríz, y más concretamente el orden del contenido de ésta y los valores que usemos en las cabeceras de las filas y columnas.

2.2.3. Cifrador de César, siglo I a.C

El encriptado de César es también conocido como encriptado por desplazamiento, desplazamiento de César o código de César, es una de las técnicas de codificación más simples y más usadas. Hace el proceso de encriptado por sustitución, en el que cada letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales [Fernández S. 2004].

Figura 5: Cifrador de César.

En la figura 5 vemos un ejemplo del encriptado de César, en la parte superior tenemos el alfabeto español y en la inferior el alfabeto español recorrido 3 letras, entonces a cada letra original le corresponde la letra de abajo. Por ejemplo para encriptar la palabra "nimiedades" nos posicionamos para cada letra en el alfabeto superior, y escribimos la letra inferior, entonces tendriamos como criptograma "PLOLHGDGHV", La clave es entonces, las letras que se recorre en el alfabeto.

2.2.4. Disco de Alberti

En 1466, León Battista Alberti concibió en 1466 el primer sistema polialfabético que se conoce, el cual emplea varios alfabetos, utilizando uno u otro cada tres o cuatro palabras. El emisor y el receptor se ponían de acuerdo para fijar la posición relativa de dos círculos concéntricos, la cual determinaba la correspondencia en los símbolos. Los diferentes alfabetos utilizados eran representados en uno de los discos, mientras que el otro con el alfabeto normal, incluyendoademás los números del 1 al 4. Este disco (Figura 6) define 24 posibles sustituciones dependiendo de la posición del disco interior [Fernández S. 2004].

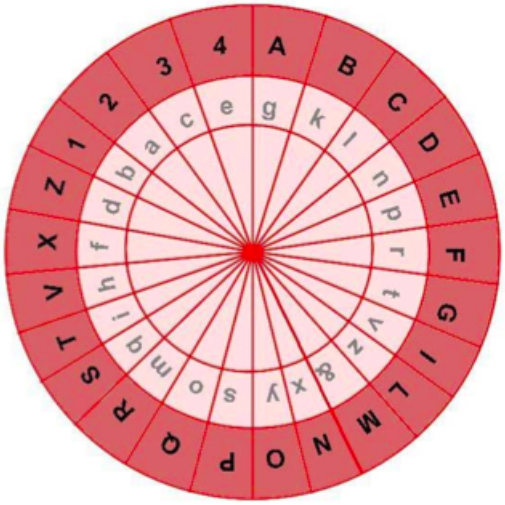


Figura 6: Disco de Alberti.

Una vez establecida la correspondencia entre caracteres de ambos discos por el emisor y receptor, se sustituye el mensaje o texto en claro del disco exterior por cada una de las letras correspondientes del disco interior, cambiando al alfabeto correspondiente cada n palabras, habiendo sido n también prefijada por los comunicantes.

2.2.5. Disco de Wheatstone

El disco de Wheatstone (1802-1875) realiza una sustitución polialfabética, similar a la utilizada por Alberti. Este sistema consistía en dos discos concéntricos: en el circulo exterior se escriben en orden alfabético las 26 letras del alfabeto inglés más el espacio, en el interior se distribuyen esas mismas 26 letras pero aleatoriamente (Figura 7). Sobre los discos hay dos manecillas como de un reloj, de forma que a medida que avanza la mayor por el disco exterior, la menor se desplaza por el disco interior. Cuando el puntero grande recorre una vuelta, el pequeño da una vuelta más una letra. El mensaje en claro se cifraba no permitiendo al disco exterior ir en sentido antihorario, siendo el mensaje secreto lo indicado por el puntero menor [Fernández S. 2004].

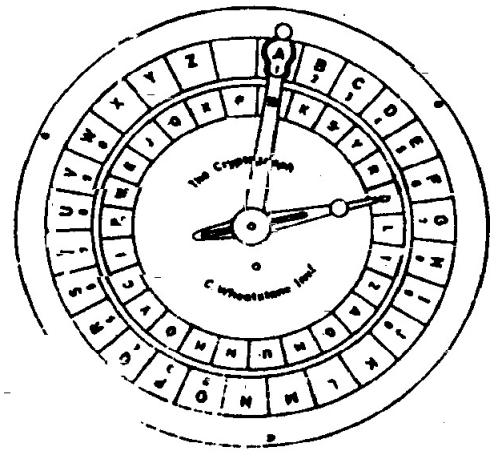


Figura 7: Disco de Wheatstone.

2.2.6. Rueda de Jefferson

Este dispositivo fue inventado por Thomas Jefferson (1743-1826), redactor de la declaración de independencia de Estados Unidos. El primero en fabricarla en serie fue Ettiene Bazeries en 1891. El aparato consiste en una serie de discos que giran libremente alrededor de un mismo eje y llevan impresas las letras del alfabeto escritas en cada disco en diferente orden. El emisor mueve los discos hasta configurar el mensaje en claro, y elige otra línea que será el mensaje cifrado. Tras haber sido transmitido, el receptor no tiene más que poner las letras recibidas en línea y buscar en otra línea el mensaje en claro [Fernández S. 2004].

Figura 8: Rueda de Jefferson.

2.2.7. Máquina Enigma

La máquina enigma fue un dispositivo para encriptar información que fue usado durante la segunda guerra mundial por la Alemania nazi, era de fácil manejo y supuesta inviolabilidad. Era una dispositivo electromecánico, estaba constituido por un teclado similar al de las máquinas de escribir, las teclas eran interruptores eléctricos, tenía un engranaje mecánico y

un panel de luces con las letras del alfabeto. Estaba constituido de varios rotores conectados entre si, los rotores estaban conectados con cables en distintas posiciones, las máquinas enigma utilizadas por el ejercito alemán poseían diferente conexión a los módelos comerciales. Durante el periodo de la segunda guerra mundial los polacos e ingleses trabajaron en conjunto para romper los criptogramas de la máquina enigma, para 1941 se capturaron varias máquinas y manuales de utilización, gracias a esto y a muchos matemáticos y criptoanalistas entre ellos Alan Turing considerado uno de los padres de la informática, se encontró la manera de desencriptar la información de los mensajes, este hecho se considera una de las razones más fuertes que significaron la derrota de los Alemanes [Richard Mollin 2001].

Figura 9: Máquina enigma usada por la Alemania nazi durante la segunda guerra mundial.

2.3. Protocolos actuales de protección de información más utilizados.

2.3.1. DES (Data Encryption standard)

Es un algoritmo desarrollado originalmente por IBM a requerimiento del NBS (National Bureau of Standards, Oficina Nacional de Estandarización, en la actualidad denominado NIST, National Institute of Standards and Technology, Instituto Nacional de Estandarización y Tecnología) de EE.UU., el algoritmo fue modificado y empezó a ser utilizado por el gobierno de EE.UU. En 1977 se convirtió en un estándar de encriptado para las informaciones sensibles no clasificadas, en 1980, el NIST estandarizó los varios modos de operación del algoritmo. Es el más estudiado y utilizado de los algoritmos de clave simétrica. IBM lo nombró originalmente "lucifer", este, trabajaba sobre bloques de 128 bits, teniendo la clave

igual longitud. Estaba basado operaciones lógicas booleanas y era de fácil implementación, tanto en software como en hardware. Tras modificaciones hechas por el NSB, que consistían básicamente en la reducción de la longitud de clave y de los bloques, el DES encripta bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad (esto es, en realidad usa 56 bits), produciendo así 64 bits cifrados [Sánchez 1999].

2.3.2. AES(Advanced Encryption standard)

También conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. A raíz del avance del criptoanálisis, el DES se volvió vulnerable y la necesidad de un nuevo estándar surgió. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) el 26 de noviembre de 2001 después de un proceso de estandarización y concurso que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits. La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado [AES 2001].

2.3.3. Seguridad WiFi WEP

WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una clave de cifrado antes de enviarlo al aire. Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 13 dígitos alfanuméricos[Arunkumar et al. 2008, Tsukaune et al. 2012, Sato et al. 2011].

La activación del cifrado WEP de 128 bits evitará que el algún usuario no autorizado acceda a sus archivos o utilice su conexión a internet. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar

de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo [Lehembre G. 2006].

2.3.4. Seguridad WiFi WPA, WPA2

WPA emplea el cifrado de clave dinámica, esto quiere decir que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica hasta el momento, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves están compuestas de dígitos alfanuméricos sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal [Lehembre G. 2006]. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación: el TKIP para uso domestico y el EAP para uso empresarial.

WPA2 es la segunda generación de WPA y está actualmente disponible en los puntos de acceso más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica. En [Wang et al. 2010] se proponen nuevos protocolos basados en los original WEP y WPA corrigiendo varios parámetros que podrían hacer insegura la comunicación con estos protocolos[Lehembre G. 2006].

2.4. Teoría del caos

Es una rama de las matemáticas además de otras ciencias, que estudia varios tipos de sistemas dinámicos con gran sensibilidad a las variaciones en sus condiciones iniciales, una pequeña variación en las condiciones iniciales implicaría un comportamiento muy diferente complicando la predicción a largo plazo, y aunque sean determinísticos su predicción es muy difícil de lograr [Ivancevic et al. 2008].

Los sistemas dinámicos se clasifican en estables, inestables y caóticos. Un sistema estable llega después de determinado tiempo a un punto, un sistema inestable se aleja de los atractores y un sistema caótico manifiesta ambos comportamientos. El sistema caótico se ve atraído hacia un punto pero a la vez se aleja de éste. Por lo tanto el sistema permanece confinado en una zona de espacios de estados sin poseer un atractor fijo.

Una característica de los sistemas caóticos es que al dar una pequeña diferencia en sus condiciones iniciales se obtienen respuestas completamente distintas en tiempo.

Algunos ejemplos de sistemas caóticos son: El sistema solar, los fluidos, turbulencia, crecimiento de población entre otros [Edward Ott 1993].

Hay una gran variedad de sistemas de ecuaciones diferenciales que nos generan mapeos caóticos entre ellos el sistema de Lorenz, sistema de Chua [Leonov 2013], mapeos discretos como Henon [M. Henon 1976], Chen [Chen 2001] entre otros, un mapeo es aquel que se forma al visualizar los atractores de los sistemas caóticos o hipercaóticos, es decir graficar sus estados uno en contra de otro o todos al mismo tiempo.

2.4.1. Condición inicial

Es aquel valor en el cual un sistema tiene como punto de partida, en una ecuación con dinámica caótica. La condición inicial es aquel valor que tendrá una relación de recurrencia para poder empezar a generar una dinámica de valores, es decir, las ecuaciones de recurrencias dependen de un valor inicial propuesto para generar una serie de valores dinámicos con parte transitoria a una estacionaria o bien con una dinámica caótica generando un mapeo caótico. Algunas relaciones de recurrencia necesitan de más de una condición inicial, como se verá en los mapeos caóticos [Leonov 2013].

2.4.2. Sistema caótico contínuo

Un sistema hipercaotico 4D continuo [Qi et al. 2008] es el siguiente:

$$\begin{aligned}
\dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 \\
\dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 \\
\dot{x}_3 &= -cx_3 - ex_4 + x_1 x_2 \\
\dot{x}_4 &= -dx_4 + fx_3 + x_1 x_2
\end{aligned} \tag{1}$$

valores de las constantes para generar el comportamiento hipercaótico específico

$a = 50, b = 24, c = 13, d = 8, e = 33, f = 30$ y con condiciones iniciales arbitrarias. Del cual se obtienen su respuesta en tiempo así como sus atractores, siendo un sistema de 4 estados nos dan 6 combinaciones en 2D (figura 10) y 3 combinaciones en 3D(figura 11).

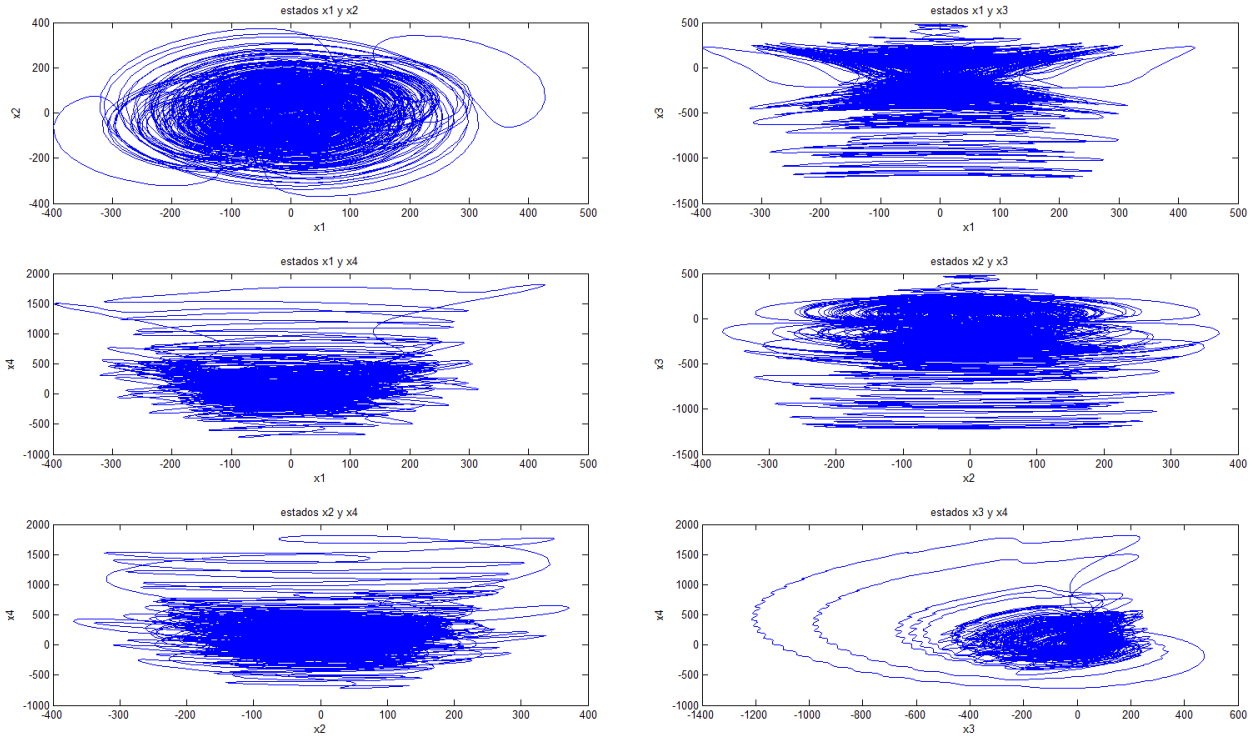


Figura 10: Atractores de los estados, 6 combinaciones 2D con 4 estados (sin unidades).

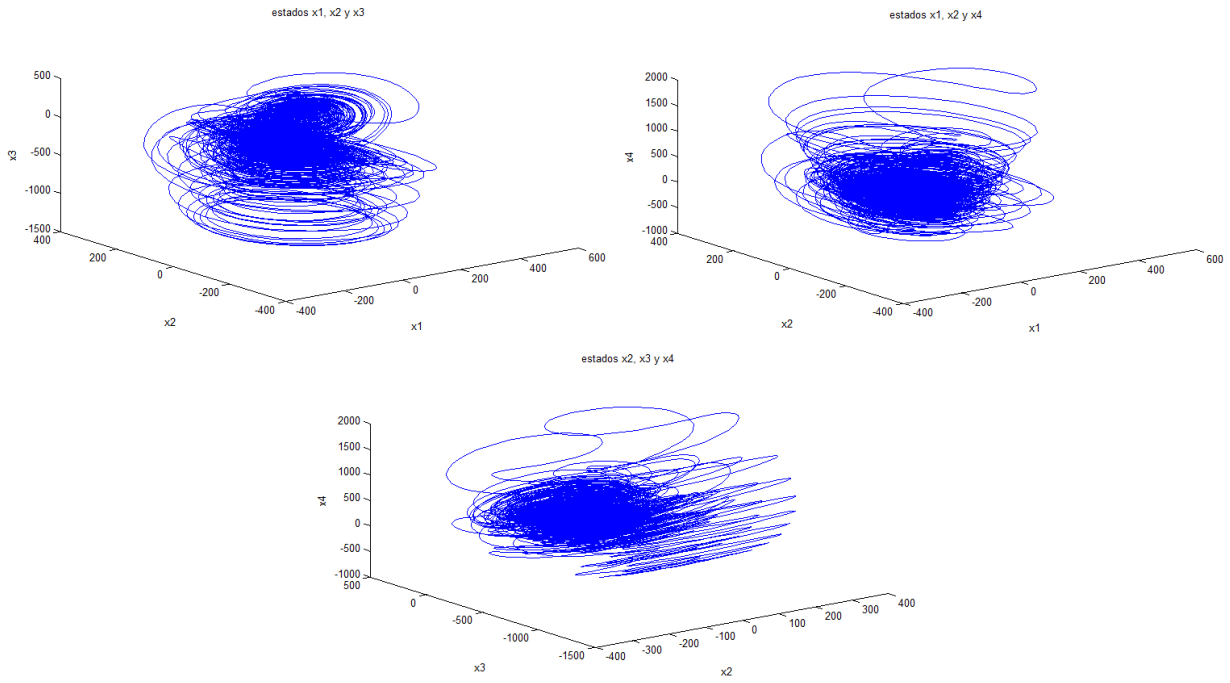


Figura 11: Atractores de los estados, 3 combinaciones 3D con 4 estados.

2.4.3. Mapeo caótico

Un mapeo caótico es un sistema dinámico discreto que consta de una o varias ecuaciones de iteraciones (relaciones de recurrencias), en [Hong-Li An et al. 2009] se pueden ver varios ejemplos de mapeos caóticos, estas ecuaciones generan una serie de resultados que poseen una dinámica caótica, es decir entre varios aspectos, un cambio muy pequeño en las condiciones iniciales de las iteraciones genera un comportamiento totalmente distinto a la condición de valor cercano como a continuación se ve en la Figura 12 la sensibilidad a las condiciones iniciales.

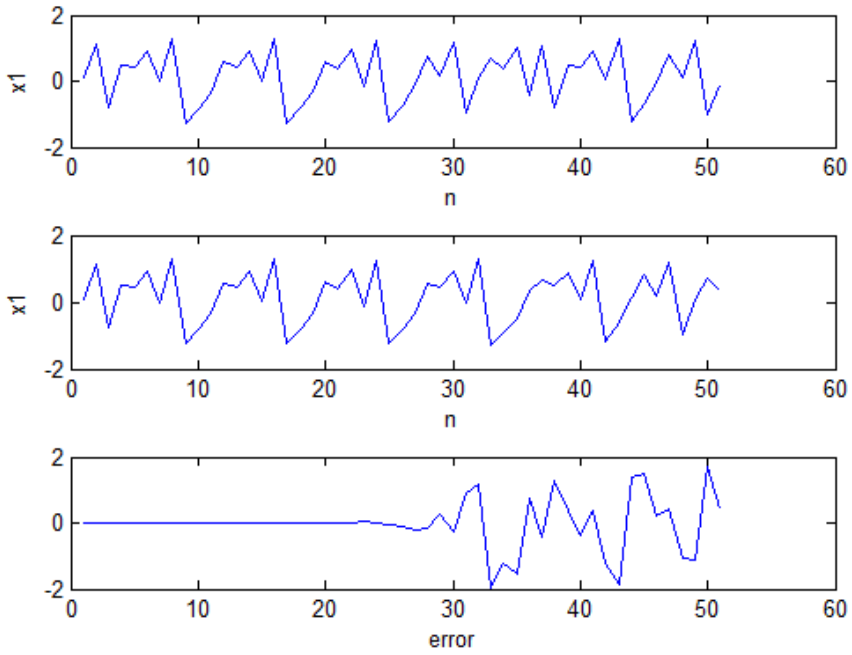


Figura 12: Sensibilidad a las condiciones iniciales o efecto mariposa.

En la primer gráfica de la figura 12 tenemos la condición inicial de $x_1 = 0{,}15$, en la segunda gráfica la condición inicial es $x_1 = 0{,}150001$ para el mapeo de henon $x_1(n+1) = x_2(n) + 1 - ax_1(n)^2$ y $x_2(n+1) = bx_1(n)$, mostrando la evolución de valores de x_1, en la tercera gráfica tenemos el error calculado con las dos primeras gráficas se obtiene a través de $error = x_n(0{,}15) - x_n(0{,}15001)$, con lo que se puede visualizar la sensibilidad a las condiciones iniciales o efecto mariposa. Ejemplos de mapeos caóticos:

2.4.4. Mapeo de Henon [M. Henon 1976]

Ecuaciones que definen el mapeo de Henon:

$$\begin{aligned} x_1(n+1) &= 1 - 2(x_1(n)^2) \\ x_2(n+1) &= ax_2(n) + x_1(n) \end{aligned} \tag{2}$$

donde los parámetros $a = 1{,}4$ y $b = 0{,}3$ generan el comportamiento caótico.

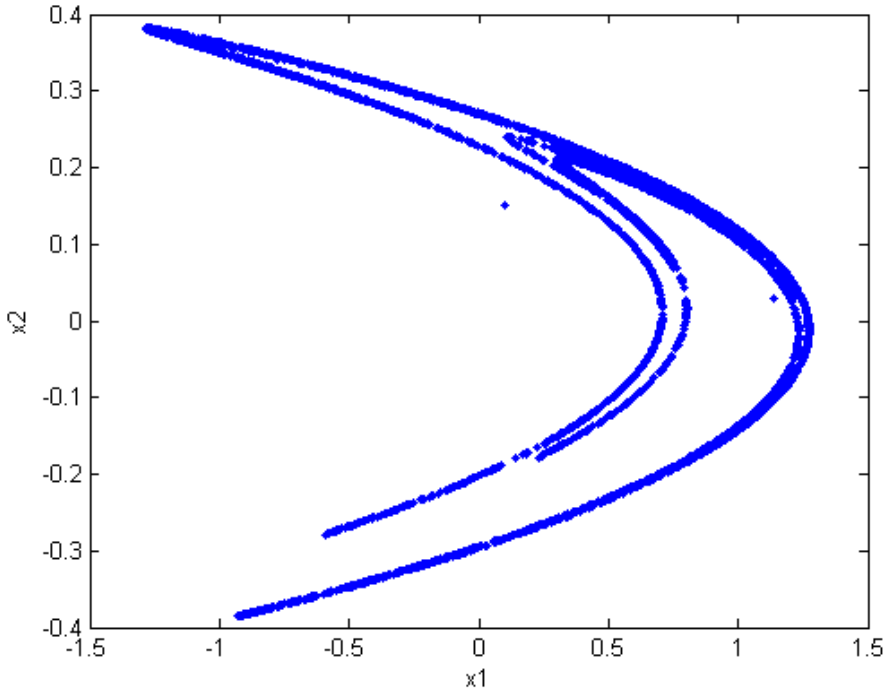


Figura 13: Mapeo de Henon generado con matlab.

2.4.5. Mapeo de Ikeda [Kuldeep Singh 2011]

Ecuaciones que definen el mapeo de Ikeda:

$$t(n) = 0{,}4 - \frac{6}{1 + x_1(n)^2 + x_2(n)^2}$$
$$x_1(n+1) = 1 + u(x_1(n)cos(t(n)) - x_2(n)sin(t(n)))$$
$$x_2(n+1) = u(x_1(n)sin(t(n)) + x_2(n)cos(t(n))) \quad (3)$$

donde el parámetro $u = 0{,}9$ genera el comportamiento caótico.

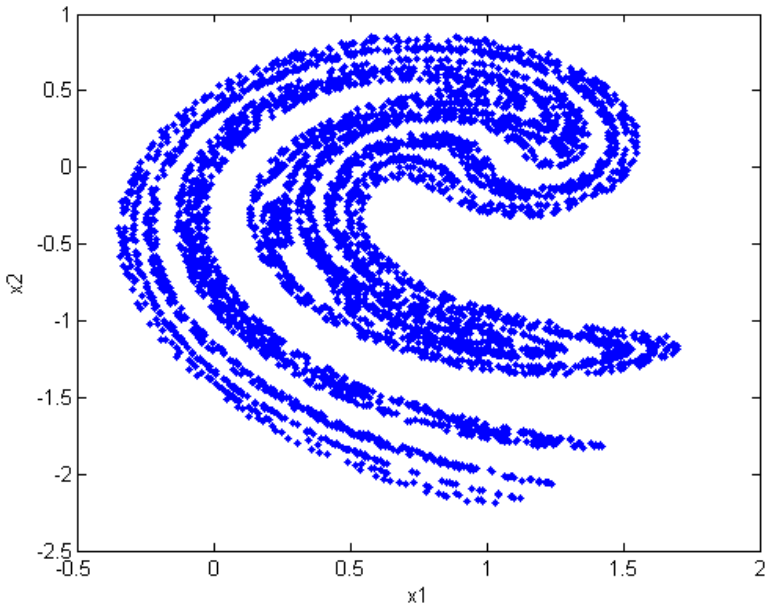


Figura 14: Mapeo de Ikeda generado con matlab.

2.4.6. Mapeo de Kaplan-Yorke [Mohan et al. 2010]

Ecuaciones que definen el mapeo de Kaplan-Yorke:

$$x_1(n+1) = 1 - 2(x_1(n)^2)$$
$$x_2(n+1) = ax_2(n) + x_1(n) \tag{4}$$

donde los parámetros $a = 0{,}4$ generan el comportamiento caótico.

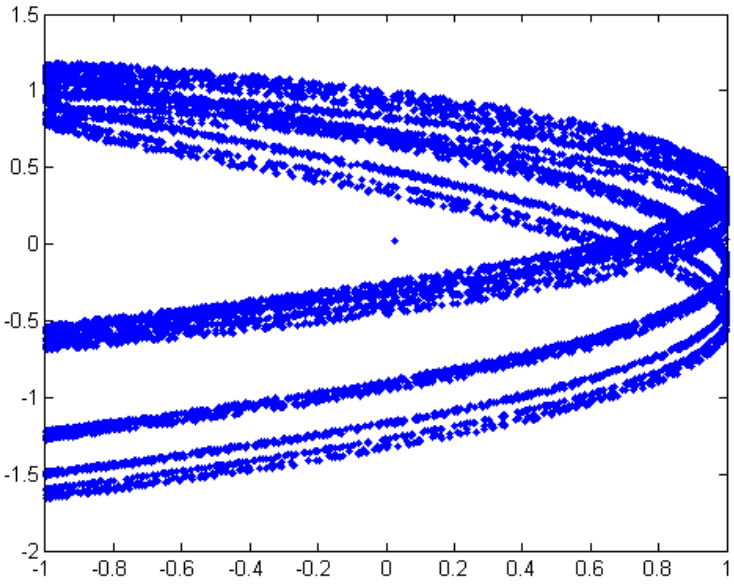


Figura 15: Mapeo de Kaplan-Yorke generado con matlab.

2.4.7. Mapeo logístico 2D [Dongming et al. 2012]

Ecuaciones que definen el mapeo logístico 2D:

$$x_1(n+1) = \mu 1 x_1(n)(1 - x_1(n)) + \gamma_1 x_2(n)^2$$
$$x_2(n+1) = \mu_2 x_2(n)(1 - x_2(n)) + \gamma_2(x_1(n)^2 + x_1(n)x_2(n)) \quad (5)$$

donde los parámetros $\mu_1 = 3$ $\mu_2 = 3{,}4$ $\gamma_1 = 0{,}2$ $\gamma_2 = 0{,}14$ generan el comportamiento caótico.

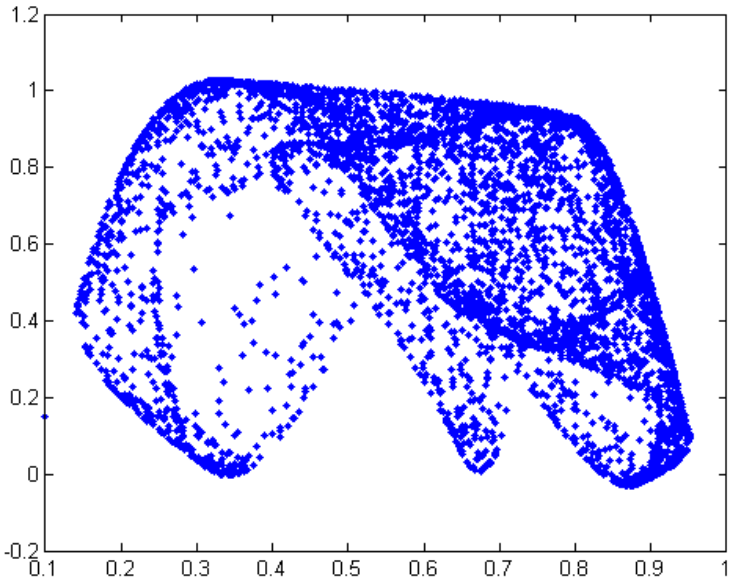


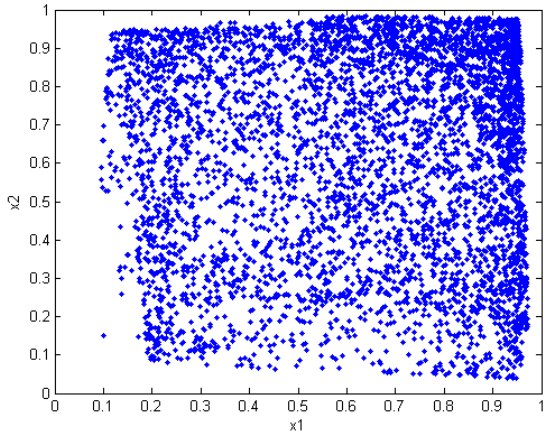
Figura 16: Mapeo logístico 2D generado con matlab.

2.4.8. Mapeo de Rössler [Inzunza et al. 2013]

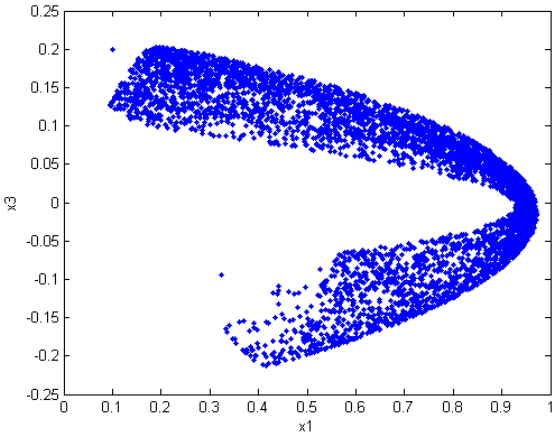
Ecuaciones que definen el mapeo de Rössler:

$$\begin{aligned} x_1(n+1) &= \alpha x_1(n)(1-x_1(n)) - \beta(x_3(n)+\gamma)(1-2x_2(n)) \\ x_2(n+1) &= \delta x_2(n)(1-x_2(n)) + \tau x_3(n) \\ x_3(n+1) &= \nu((x_3(n)+\gamma)(1-2x_2(n))-1)(1-\theta x_1(n)) \end{aligned} \tag{6}$$

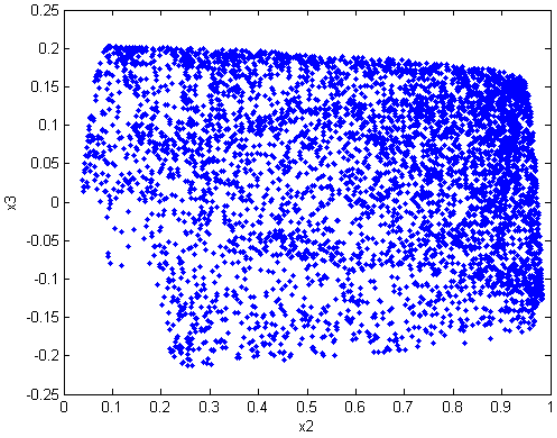
donde los parámetros $\alpha = 3{,}8$ $\beta = 0{,}05$ $\gamma = 0{,}35$ $\delta = 3{,}78$ $\tau = 0{,}2$ $\nu = 0{,}19$ $\theta = 1{,}9$ generan el comportamiento caótico, y sus atractores pueden verse en la figura 17.



(a) Estado x_1 Vs x_2



(b) Estado x_1 Vs x_3



(c) Estado x_2 Vs x_3

Figura 17: Mapeo de Rössler.

2.5. Ejemplos de criptografía caótica

Una vez entendida y estudiada tanto la criptografía como la teoría del caos, entonces podemos concluír que la criptografía caótica es el conjunto de técnicas basadas en caos para lograr ocultar información confidencial que será enviada por un canal inseguro. Existen muchos trabajos reportados sobre criptografía caótica, en su mayoría sobre imágenes y audio, en [Abdullah Sharaf 2011] los autores utilizan un algoritmo caótico para encriptar una imagen para un sistema satelital llamado C4I y lograr asi, tener imágenes encriptadas de fotografías desde satélite, el autor de [Huang 2011] propone un algoritmo para encriptar imágenes, estudiando varios tipos de esquemas de encriptado, entre ellos, el hipercaos. Un ejemplo de encriptado de audio es hecho por [Cruz et al. 2010] donde mediante el uso de la configuración esclavo maestro de sincronización de sistemas caóticos, se transmite audio encriptado por caos a través de un canal inseguro de comunicación. En la referencia [Patidar et al. 2011] los autores proponen un esquemas para encriptado de imágenes basándose en el mapeo estandar.

2.5.1. Ejemplo de encriptado de imagen

En la figura 18 se muestra una imagen que es encriptada con el mapeo del gato de Arnold, la imagen encriptada es la que viaja por el canal de comunicación inseguro, la figura 19 nos muestra entonces lo que recibe el receptor, que es un criptograma y mediante el algoritmo inverso y clave el receptor recupera la imagen original. Por último, es importante mencionar que una de las ventajas de la criptografía caótica es la sensibilidad a las condiciones iniciales como se muestra en la figura 20 donde la clave tiene una diferencia de 1×10^{-10} y a pesar de ser mínima la diferencia, observamos que no obtenemos la imagen original.

Figura 18: Imagen Lena a encriptar con resolución 256x256 RGB e imagen Lena encriptada con caos.

Figura 19: Imagen encriptada recibida con resolución 256x256 RGB e imagen Lena recuperada.

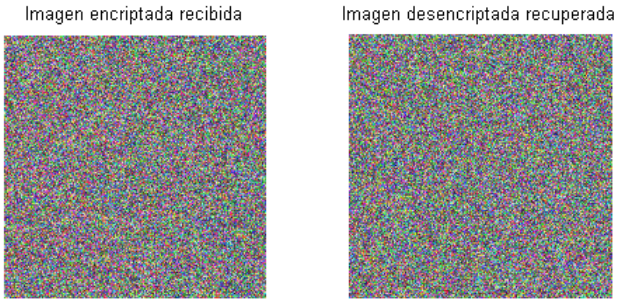


Figura 20: Imagen encriptada recibida con resolución 256x256 RGB e imagen no recuperada debido a clave erronea.

En la figura 21 se muestra el histograma de la imagen original y el histograma de la imagen una vez encriptada, podemos ver que la imagen encriptada posee un historial uniforme, lo que evidencia que es una imagen resistente a ataques estadísticos de criptoanálisis, esto obtenido a partir del mapeo del gato de Arnold, diferentes mapeos pueden generar diferentes tipos de histogramas.

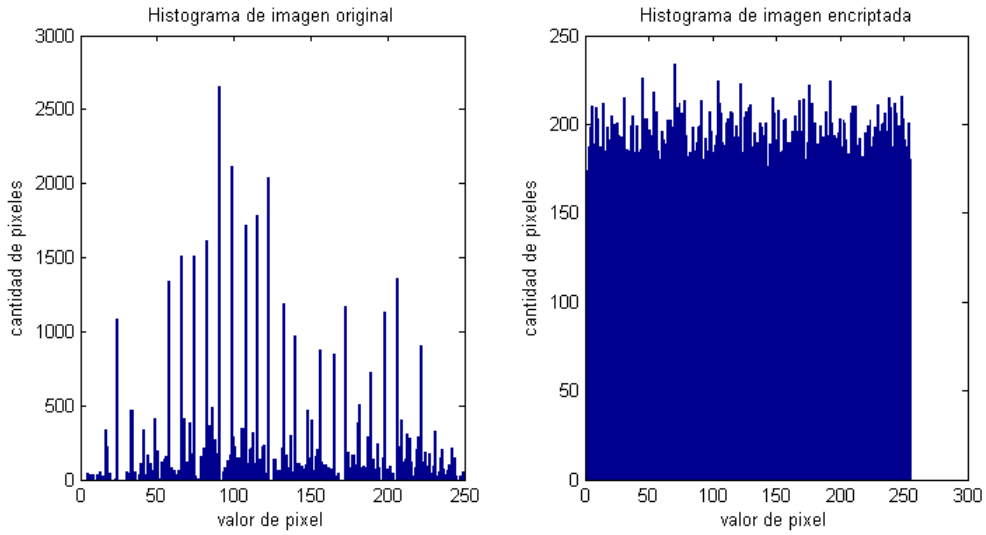


Figura 21: Histograma de la imagen original y la encriptada.

2.5.2. Ejemplo de encriptado de audio

En la figura 22 podemos ver un mensaje de voz que es encriptado usando el mapeo de Henon, nuestro mensaje original es encriptado para enviarlo por el canal inseguro de comunicación y entonces es recuperado por el receptor quien tiene el algoritmo inverso y la clave correcta. Para la figura 23 tenemos que el receptor no tiene la llave correcta y se hace una prueba con una clave que tiene un error de 1×10^{-10} para comprobar una vez mas la ventaja que nos proporciona la criptografía caótica al ser sensible a las condiciones iniciales, que en este caso corresponde a la clave.

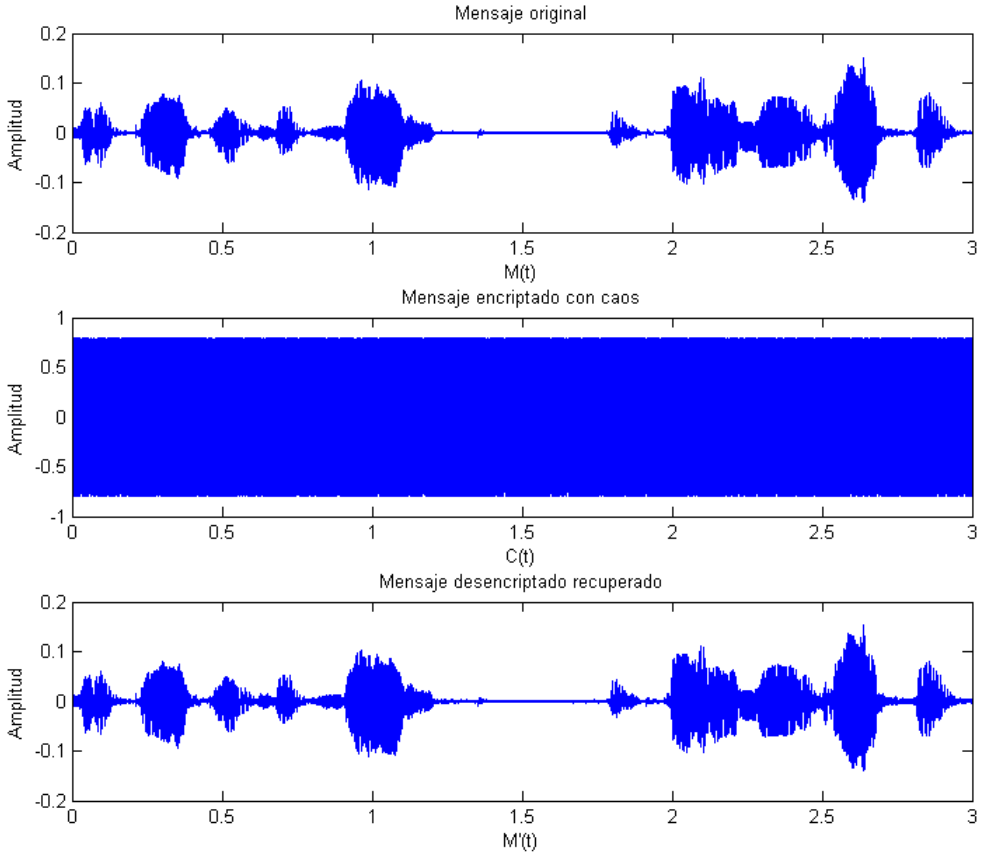


Figura 22: Mensaje de voz de 3 segundos, encriptado y recuperado con la clave correcta.

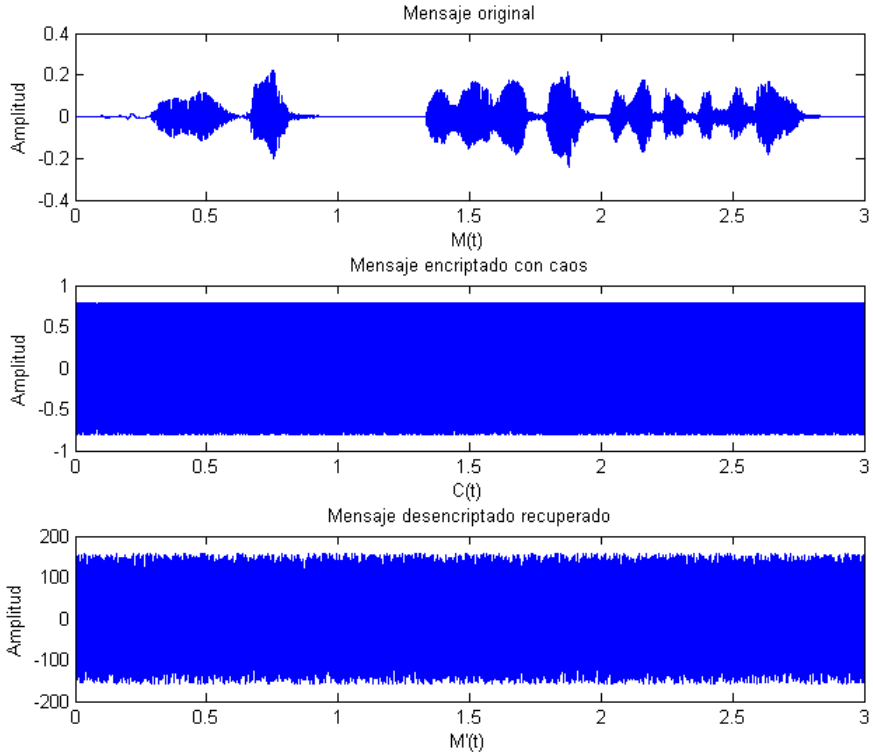


Figura 23: Mensaje de voz de 3 segundos, encriptado y no recuperado por haber usado clave incorrecta.

Otro posible análisis de seguridad es obtener el espectro de Fourier de nuestro mensaje de voz, en la figura 24 se muestra la FFT del mensaje de voz original y del mensaje de audio encriptado o criptograma. Se puede decir que al añadir caos, hacemos que aparezcan una gama de frecuencias en el espectro, esto también es propiedad de las ecuaciones caóticas, es importante señalar que con el mapeo de Henon obtenemos este resultado, existen mapeos con dinámicas caóticas más complejas que nos darían un espectro contínuo y uniforme a nuestro criptograma, haciendolo resistente a ataques estadísticos de criptoanálisis.

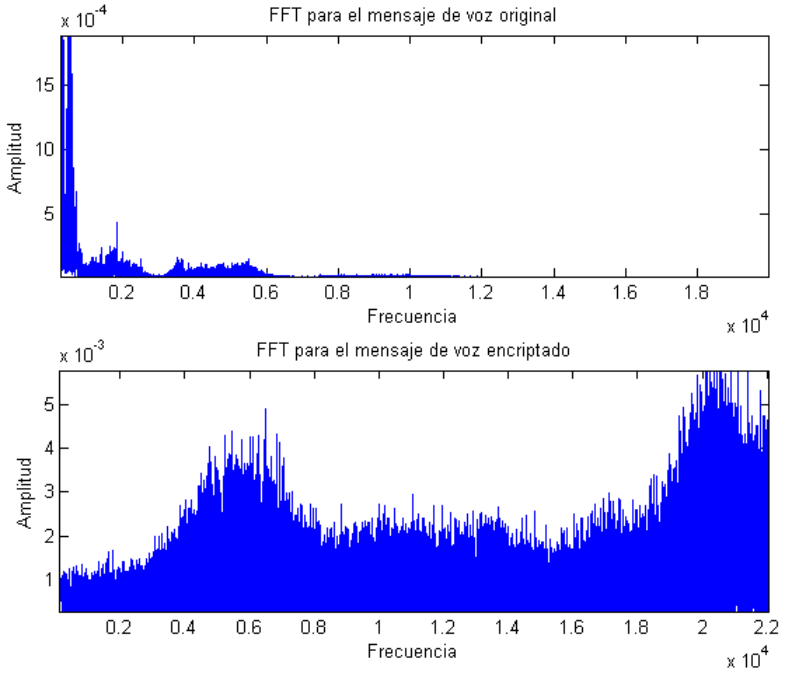


Figura 24: Transformada rápida de fourier (FFT) para el archivo de audio original y el encriptado.

2.6. Conclusión

En este capítulo se estudiaron conceptos relativos a la criptología, se dió una breve historia de la criptografia y una explicación de la teoría del caos, para al fin comprender bien la criptografía caótica. Los ejemplos mostrados de criptografía caótica son resultado de miles de años de evolución en la criptografía, que junto con recientes avances en sistemas complejos, se ha logrado desarrollar esta técnica que ofrece una alta seguridad y que puede ser la base de nuevos estándares de seguridad en los sistemas de comunicaciones y telecomunicaciones. Cabe señalar que su estudio aún esta en desarrollo y cada vez más algoritmos y propuestas son publicadas por diferentes instituciones, la importancia de esta criptografía en desarrollo, es su aplicación para evidenciar su fiabilidad, rendimiento y practicidad en los sistemas actuales. Al comprender en un contexto general la criptografía caótica, entonces podemos aportar más a su estudio así como comprender su importancia en estos tiempos modernos.

Capítulo III

3. Parámetros de análisis de seguridad

Para la evaluación de la fortaleza y resistencia de un criptograma ante el criptoanálisis, existen varias pruebas realizables. Varios artículos donde el análisis se realiza a imágenes encriptadas, [Huang 2011, Chong Fu et al. 2011] presentan distintos análisis de seguridad, como por ejemplo, el estudio del histograma del criptograma, el espacio de claves y la resistencia a ataques diferenciales. Por otra parte [Liu et al. 2009] además incluyen una prueba visual de las imágenes encriptadas, para asegurarse que no se asemejen a la original, también aplican el análisis por histograma y un análisis de coeficientes de correlación. Es básico también el análisis de sensibilidad a las condiciones iniciales, [Behnia et al. 2007] menciona que la seguridad es muy importante en un criptosistema, y realiza en su artículo varias pruebas de seguridad en las que además de hacer los procedimientos anteriormente mencionados, incluye la correlación de dos pixeles adyacentes y la entropía de la información. Estos autores trabajan con encriptado de imágenes, para este trabajo, el análisis de seguridad se hace a los criptogramas de audio, el análisis es parecido al de imágenes pero limitado por el tipo de información, a continuación se detallan las pruebas de seguridad hechas a los criptogramas de audio resultantes.

3.1. Histograma estadístico

Recapitulando, según la estadística, un histograma es una representación gráfica de una variable en forma de barras, cuya superficie de cada barra es proporcional a la frecuencia de los valores representados, en el caso del audio el histograma nos indica los valores que existen en la señal de audio y que tantas veces estos se repiten, la señal de audio es de 8 bits, por lo que poseerá 256 valores posibles distintos, esto dependiendo del mensaje de voz. Para que un histograma nos indique que el criptograma es resistente a ataques de criptoanálisis, este deberá tener una frecuencia uniforme en cada valor posible de la información de audio. El histograma del criptograma debe de ser muy distinto al histograma de la señal de audio original y deberá además, no poner en evidencia el histograma original de ninguna manera. [Huang 2011, Chong Fu et al. 2011, Patidar et al. 2011, Behnia et al. 2007] utilizan este

método en las imágenes que encriptan con los algoritmos que proponen, en el caso de audio se realiza el mismo proceso.

3.2. Transformada rápida de Fourier (FFT)

La transformada rápida de Fourier (Fast Fourier Transform, FFT), es un algoritmo que permite calcular la transformada de Fourier discreta y su inversa, es de gran importancia en una amplia variedad de aplicaciones, desde el tratamiento digital de señales y filtrado digital [Pei-Chen Lo et al. 1999, Xiang An et al. 2011].

$$X[k] = \sum_{n=0}^{N_{F-1}} X[n] e^{-j2\pi(kn/N_F)} \tag{7}$$

En el análisis de seguridad del criptograma de audio, la FFT es muy útil ya que nos permite conocer las frecuencias que componen la señal de audio, un criptograma de audio altamente resistente a ataques de criptoanálisis deberá de poseer un espectro uniforme, o dicho de otra manera, contener todas las frecuencias posibles, ya que a partir de una FFT se puede encontrar información importante en las señales, pero si este es contínuo, se podría considerar una especie de ruido, o señal sin sentido alguno, que oculta perfectamente nuestro mensaje de voz original.

3.3. Análisis de sensibilidad a las condiciones iniciales

Como ya se mencionó en capitulos anteriores, una de las ventajas de los sistemas caóticos, es su sensibilidad a las condiciones iniciales, las cuales generan una dinámica caótica única, y al ser modificadas aunque sea por una mínima cantidad, nos dan una dinámica totalmente distinta a la condición inicial inmediata anterior o siguiente. Estas condiciones tienen un límite y este dependerá de la resolución del sistema digital en el que se apliquen.

3.4. Análisis de espacio de claves

El espacio de claves se refiere a la cantidad total de distintas claves que pueden ser utilizadas en el encriptado o desencriptado [Inzunza 2013]. Un sistema criptográfico efectivo y seguro debe de ser suficientemente grande para hacer inviable un ataque de fuerza bruta. La

clave del sistema criptográfico está compuesto de dos partes. La primera son las condiciones iniciales del mapeo y la segunda los parámetros de control de dicho mapeo. Si el espacio de clave es mayor a 128 bits, se considera seguro para la mayoría de las aplicaciones criptográficas considerando la velocidad de las computadoras actuales, por lo tanto el ataque de fuerza bruta es inviable [Chong Fu et al. 2012, Patidar et al. 2011].

3.5. Entropía de la información

La entropía de la información, es un criterio que muestra la aleatoriedad de los datos, este criterio puede ser utilizado para evaluar la seguridad de encriptado. Para calcular la entropía $H(s)$[Behnia et al. 2007, Inzunza 2013, Patidar et al. 2011] de una fuente (s) que en este caso es el audio, se utiliza la siguiente ecuación:

$$H(s) = \sum_{n=0}^{2^N-1} P(S_i) \cdot Log_2(\frac{1}{P(S_i)})bits \tag{8}$$

donde $P(S_i)$ representa la probabilidad del simbolo S_i. Para una fuente aleatoria, que está emitiendo 2^N símbolos con la misma probabilidad, después de evaluar la ecuación (8), se tiene una entropía $H(S) = N$, el mensaje de voz original y encriptado son de 8 bits, su entropía es entonces $H(s) = 8bits$. Un criptograma de audio ideal deberá tener una entropía de 8. Cuando un sistema criptográfico emite criptogramas con entropía menor a 8, este encriptador tiene cierto grado de predicibilidad, por lo que su seguridad se pone en riesgo [Inzunza 2013].

Capítulo IV

4. Diseño del prototipo Encriptador-Desencriptador Wi-Fi, "VoicE-D"

En este capítulo se detalla la estructura, el funcionamiento y fiabilidad del prototipo encriptador-desencriptador WiFi hipercaótico. El prototipo tiene como base dos programas, el primero es aquel programado en Dynamic C y compilado a la memoria Flash del módulo RCM5600W rabbit, este programa recibe los paquetes de datos, claves y selección de método. Toda la información que le llega es de manera inalámbrica y es utilizando particularmente WiFi, es en este programa donde se incluye el proceso de operaciones xor byte a byte para lograr encriptar o desencriptar según sea el caso, los datos de audio enviados [Muhammad et al. 2007, F. Zamora et al. 2013]. El segundo programa se encuentra en la computadora personal y es desarrollado sobre la plataforma Matlab, este es el encargado de grabar o seleccionar los datos de audio en su forma original o de criptograma, para entonces mandarlos junto con los parámetros de claves y el método de encriptado, al módulo RCM5600W rabbit a través de la conexión WiFi.

La señal de audio es un mensaje de voz a 8KHz de frecuencia de muestreo y 8 bits de resolución. La etapa de encriptado-desencriptado está directamente relacionada con la "longitud" o tamaño del audio enviado, conforme este se incremente el tiempo de encriptado aumentará. El módulo rabbit mediante WiFi se comunica con la computadora que envía los datos, este tipo de conexión se hace, ya sea por medio de conexión Ad-Hoc que es una red inalámrica centralizada que no requiere punto de acceso, o por medio de conexión tipo infraestructura la cual se conecta a un punto de acceso. Para este trabajo se utiliza la conexión Ad-Hoc.

Figura 25: Diagrama de comunicación entre dispositivos a utilizar.

4.1. Microcontroladores

Un microcontrolador es un circuito integrado programable capáz de ejecutar los comandos grabados en su memoria. Está compuesto de varios bloques funcionales cada uno diseñado para realizar una tarea específica. Un microcontrolador está compuesto de las tres principales unidades funcionales de una computadora: unidad central de procesamiento, memoria y periféricos de entrada y salida. Para el desarrollo de este trabajo, se utilizó el microcontrolador RCM5600W, existen microcontroladores más sencillos y con amplias aplicaciones, hoy en dia los microcontroladores están alrededor de todos en distintos aparatos electrónicos, como microoondas, impresoras, celulares, monitores, televisores, video juegos, relojes, etc. Cada uno de ellos está programado para realizar tareas especificas que son parte de la funcionalidad de los aparatos que los incluyen [Martínez 2008].

4.2. Microcontrolador Rabbit 5000

El procesador rabbit 5000 pertenece a una familia de microprocesadores los cuales fueron creados por Rabbit Semiconductor para diseñar un mejor microprocesador para uso en computadoras de una sola tarjeta de pequeña y mediana escala, los primeros fueron las versiones rabbit 2000, 3000, 4000.

Rabbit 5000 es un microcontrolador de alto rendimiento con baja interferencia electromagnética y fue diseñado especialmente para control de sistemas empotrados, comunicaciones y conectividad de redes. Ofrece una facilidad en su programación utilizando el lenguaje Dynamic C que ofrece una capacidad de desarrollo eficiente inclusive en las tareas mas complejas.

Velocidad de reloj : 74 MHz

Memoria: 1 MB SRAM, 4 MB de memoria flash

Voltaje de operación 1.8 a 3.3 V i/o

8 canales de DMA(Acceso directo a memoria)

Salida PWM

Conectividad 10/100Base-T Ethernet MAC con interface estándar MII PHY y transceptor inalámbrico 802.11b/g MAC compatible con varios estándares de Wi-Fi.

El microcontrolador que se utilizó en este trabajo fue el módulo RCM5600W, con las caracteristicas antes mencionadas.

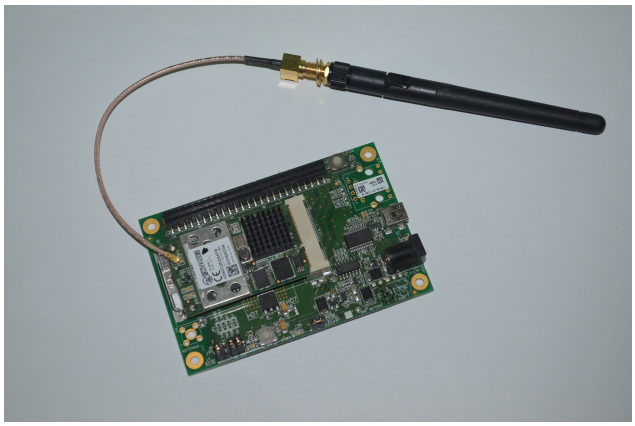


Figura 26: Microcontrolador Rabbit con microprocesador 5600W.

4.3. Estructura y funcionamiento del programa en el módulo Rabbit RCM5600W

Los programas encargados de realizar todo proceso para manejar nuestro mensaje de audio, se presentan en la figura 27,en esta, se presenta el diagrama de flujo del programa que esta compilado en el módulo Rabbit RCM5600W, está compuesto de 4 módulos primordiales llamados módulos K, R, Z y T, que realizan los procesos más importantes para lograr el encriptado-desencriptado de nuestra señal de audio. El diagrama muestra detalladamente la manera en que el programa evoluciona y realiza sus procesos para lograr el objetivo de asegurar la información.

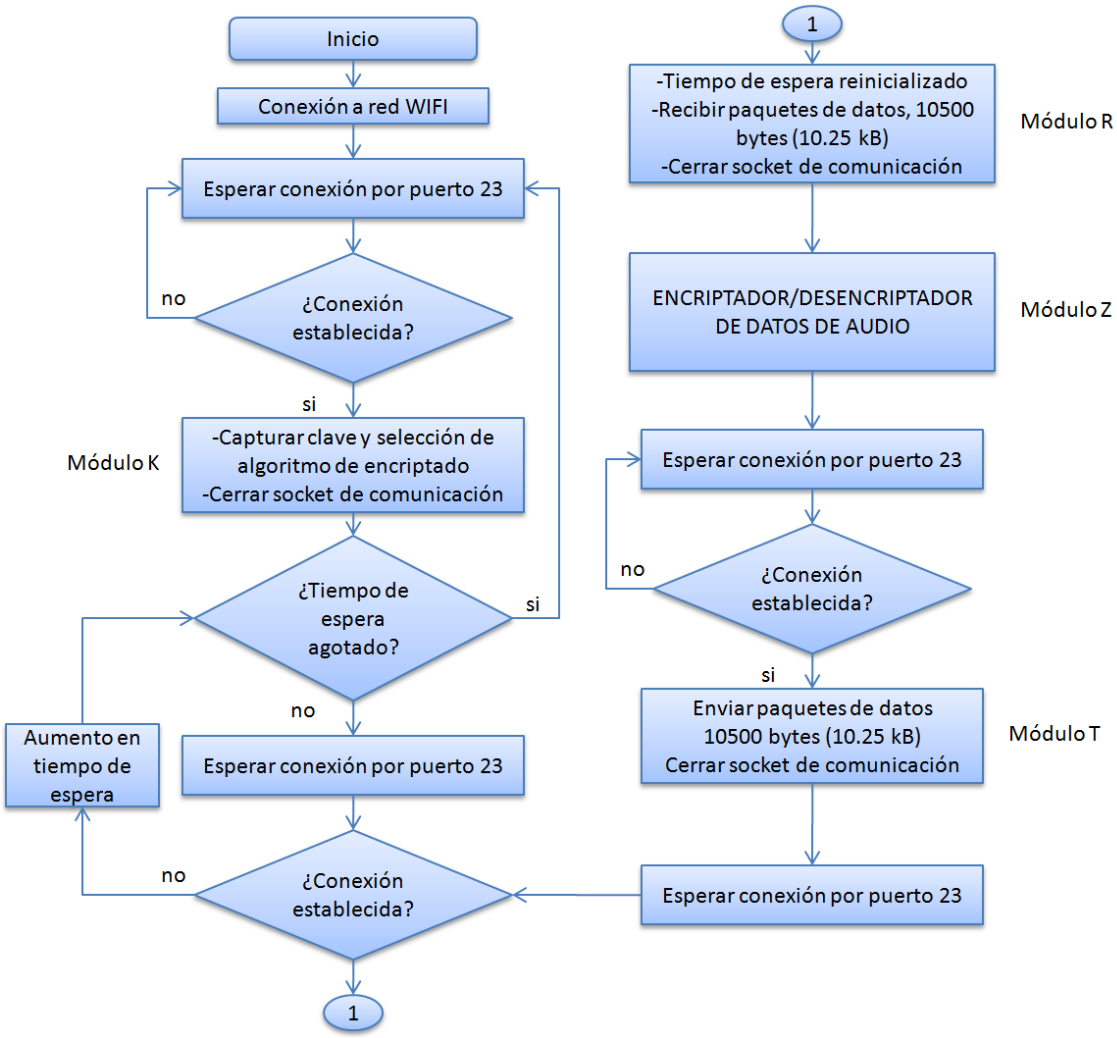


Figura 27: Diagrama de flujo del prototipo de encriptador-desencriptador WiFi.

4.3.1. Módulo K

En la figura 28 se presenta el diagrama de flujo de la primera conexión TCP/IP que realiza el programa, llamado módulo K, este módulo realiza una conexión que se encarga de recibir 3 datos, las dos claves para encriptar-desencriptar y el método o algoritmo que se utilizará que en este caso un número del 1 al 5. Cuando se recibe esta información, el módulo K cierra el socket TCP/IP y prosigue el funcionamiento normal del programa.

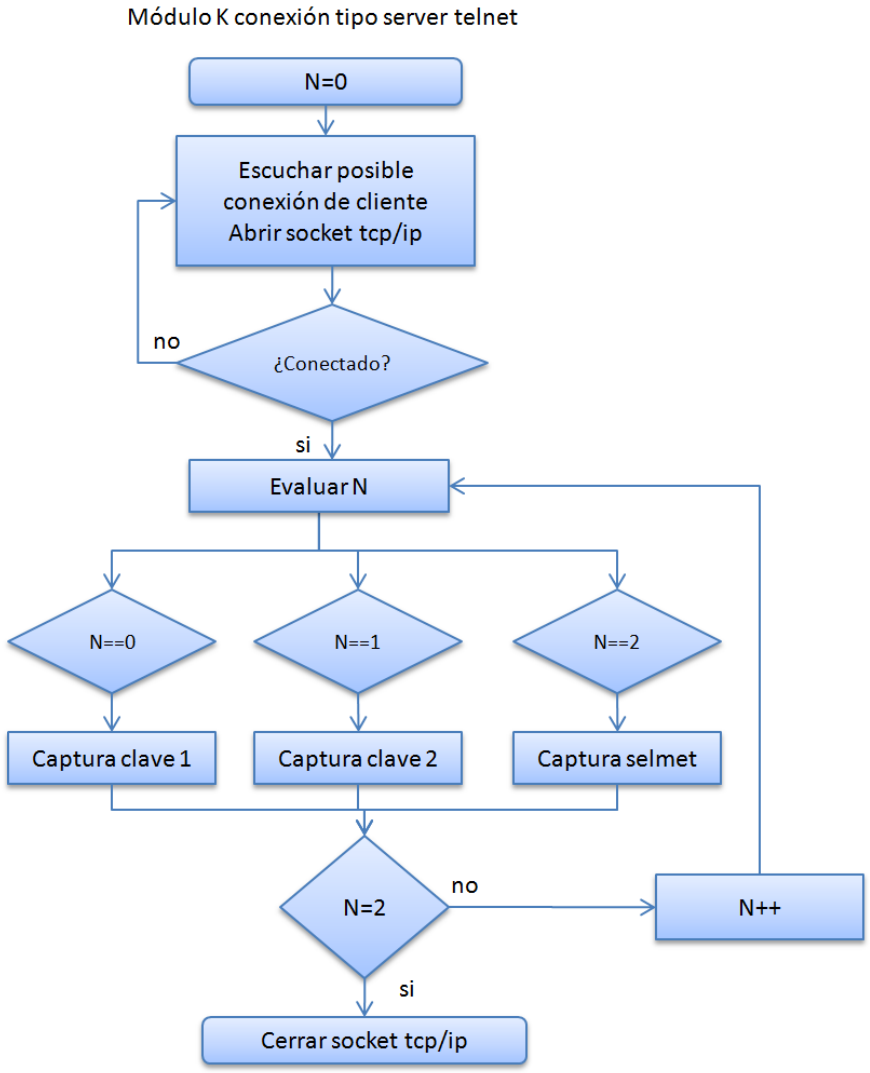


Figura 28: Diagrama de flujo del módulo K que recibe parámetros de claves y método de encriptado.

4.3.2. Módulo R

El módulo R se muestra en la figura 29, este módulo se encarga de establecer una nueva conexión y en ésta, recibir paquetes de datos de audio, que en nuestro caso corresponde a 10500 bytes que son aproximadamente 10.25KB los cuales se almacenan en un arreglo llamado "buffer"dentro de la memoria del microcontrolador RCM5600W rabbit, cuando se termina la recepción de paquetes, el módulo R prosigue a cerrar el socket TCP/IP y los datos entrarán a la parte de encriptado-desencriptado realizada por el módulo Z.

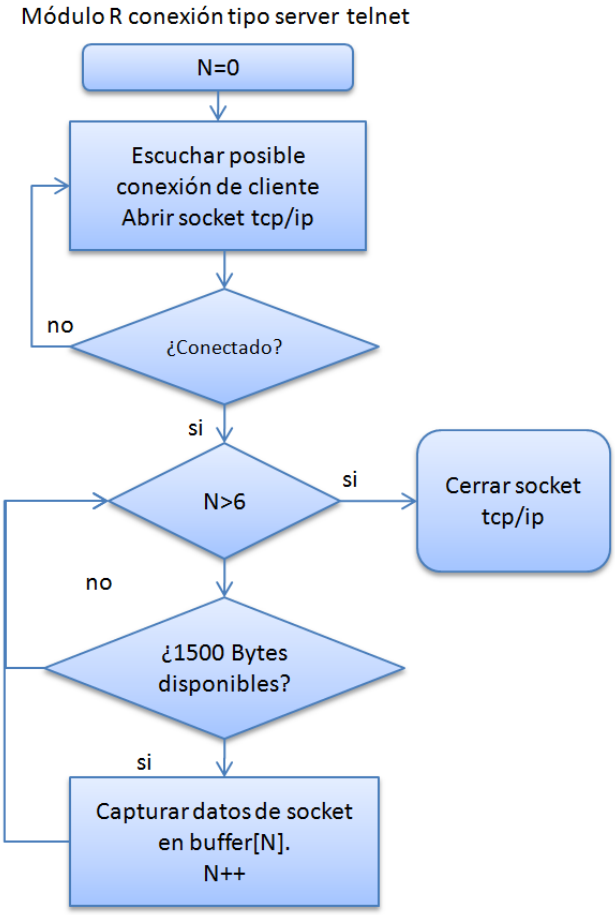


Figura 29: Diagrama de flujo del módulo R que recibe paquetes de datos de audio.

4.3.3. Módulo Z

El módulo Z se puede considerar la parte medular de todo el programa, es en este módulo donde se lleva a cabo el proceso de encriptar-desencriptar, según sea el caso. Es aqui donde se requieren las dos claves y la selección de método de encriptado adquiridos por el módulo K. En la figura 30 se presenta el diagrama de flujo del programa, se observa que tiene dos

sentencias "FOR" anidadas, las cuales van permutando la posición del arreglo "buffer" que contiene los datos de audio o criptograma, dependiendo del valor de la variable "selmet", la cual da la selección del método de encriptado-desencriptado. Acorde a la sentencia de la selección de método de encriptado-desencriptado se generan los valores de x_1 y x_2 los cuales generan un byte con información pseudoaleatoria ya que se generan a través de caós. Con este byte, la operación XOR es hecha byte a byte para encriptar-desencriptar la información. Si la clave o la selección de método es erronea por ejemplo, en caso de mandar un criptograma, este no recuperara los datos originales.

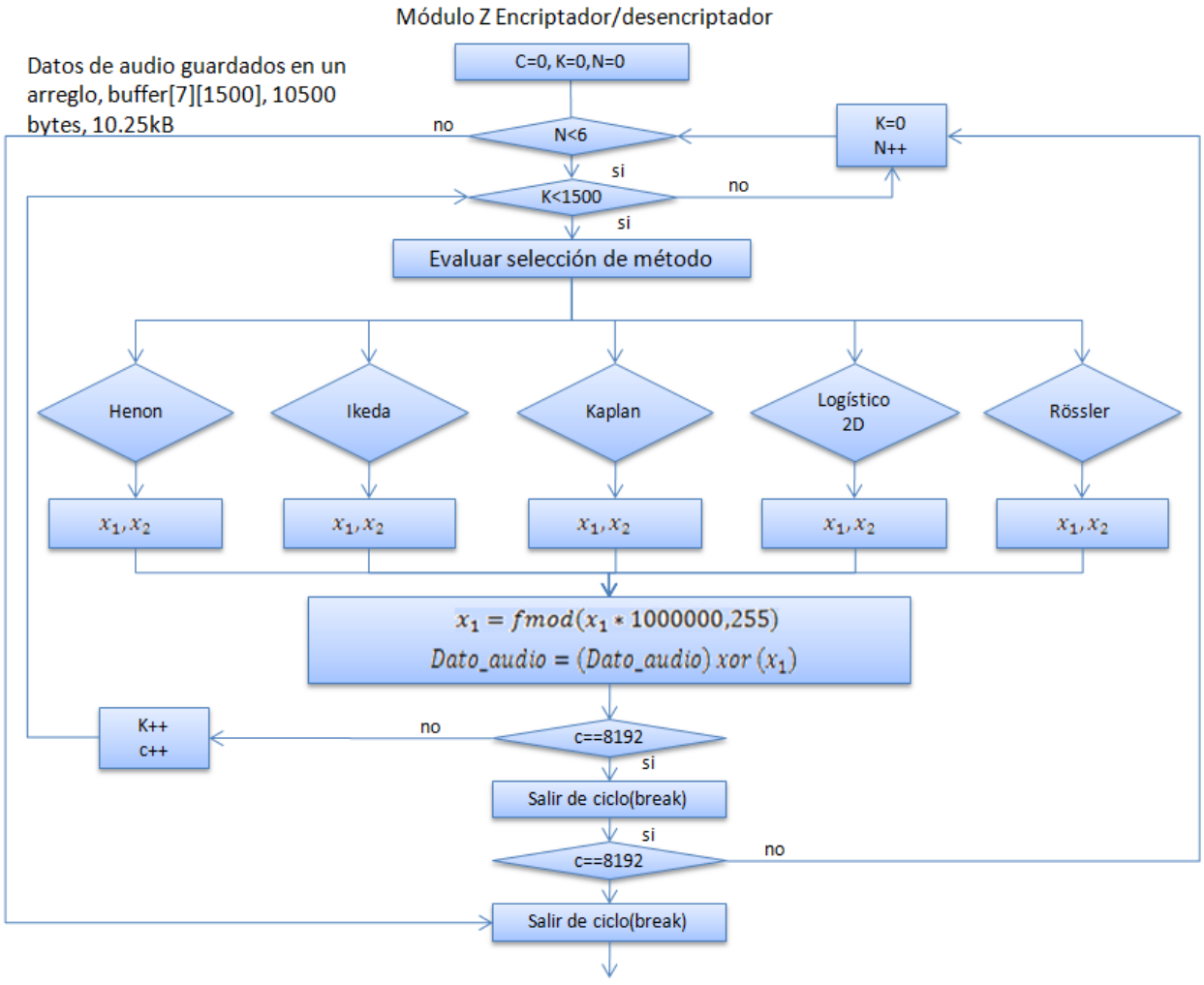


Figura 30: Diagrama de flujo del módulo Z que encripta o desencripta los datos de audio

4.3.4. Módulo T

El módulo T que se muestra en la figura 31, lleva a cabo el proceso de envío del mensaje encriptado o desencriptado de regreso por un nuevo socket TCP/IP que abre este módulo, cuando se encuentra abierto, los 10.25KB de datos se envían por el socket, y al finalizar se cierra el socket, cuando esta etapa concluye, el programa regresa a una etapa de espera de conexión establecida por el módulo R en caso de que haya más paquetes de datos por encriptar-desencriptar, si después de un tiempo, no se reciben paquetes, entonces el programa automáticamente regresa hacia el módulo K donde espera una nueva conexión para recibir audio o un criptograma.

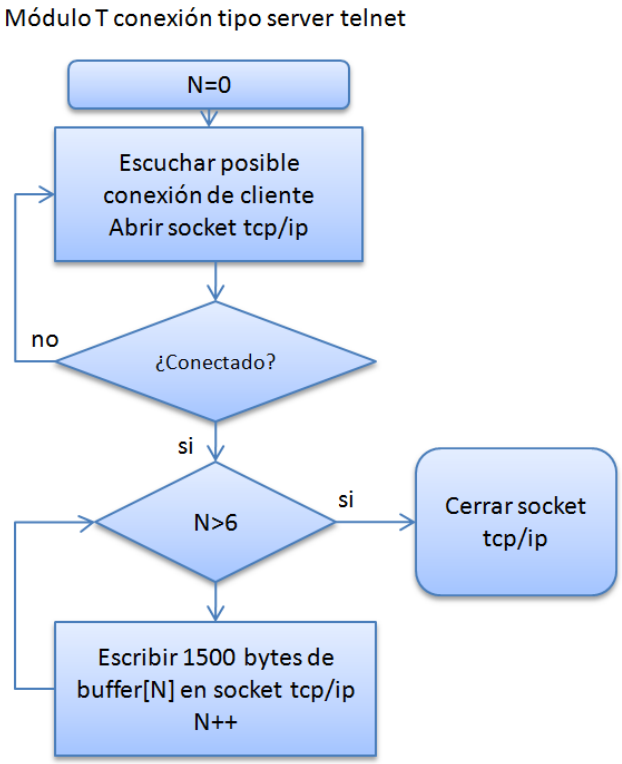


Figura 31: Diagrama de flujo del módulo T que envía datos de audio.

4.4. Estructura y funcionamiento del programa en la plataforma Matlab

El segundo programa es desarrollado en la plataforma Matlab, este programa por una parte graba un mensaje de voz o escoge un archivo de audio susceptible a encriptarse. Por otra parte el programa envía un criptograma respectivo para recuperar los datos de audio

originales, en la figura 32 se muestra el diagrama de flujo de dicho programa. En cada etapa de conexión la computadora personal se conecta a través de WiFi al módulo RCM5600 rabbit, para enviar parámetros y enviar y recibir paquetes de datos de 10.25KB. Éste funciona mediante un GUI de matlab lo que lo hace más amigable para el usuario, una plataforma de este tipo, se muestra en la figura 33.

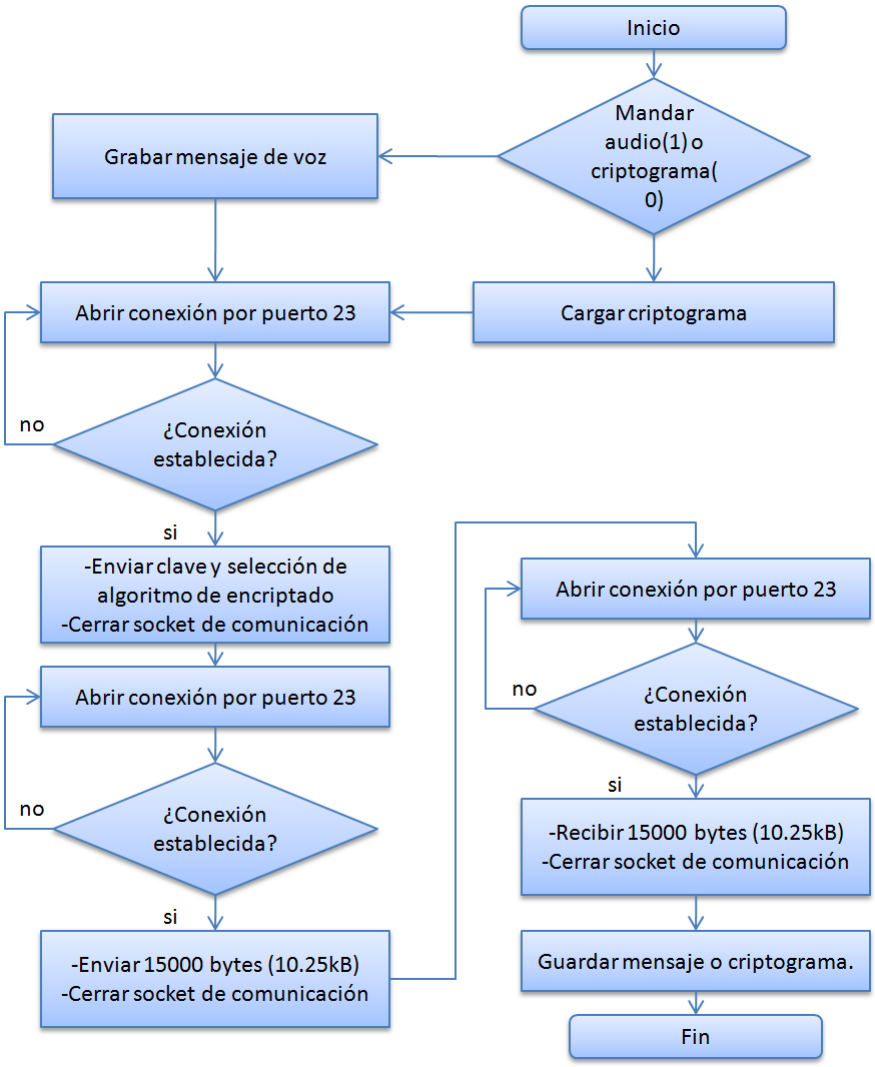


Figura 32: Diagrama de flujo del programa en la plataforma Matlab para enviar y recibir datos al modulo RCM5600W rabbit.

Figura 33: Interfaz gráfica del programa realizado en Matlab para establecer comunicación con el VoicE-D.

La interfaz gráfica elaborada en el Guide de la plataforma Matlab, proporciona una interacción mas amigable para el usuario, haciendo más sencilla la manipulación de los mensajes de voz y los criptogramas, para ello el usuario tiene varias opciones:

1.-Grabar el mensaje de voz oprimiendo el boton "grabar mensaje de voz", con un intervalo de tiempo en segundos, seleccionado previamente por el usuario. El usuario puede escuchar el mensaje grabado presionando el boton "reproducir mensaje".

2.-Cargar un archivo recibido para su desencriptado oprimiendo el boton "cargar archivo", se puede escuchar su contenido al oprimir "reproducir archivo".

3.-Para encriptar o desencriptar la información de audio, se debe introducir la clave respectiva. Se tiene la posibilidad se seleccionar el mapeo de encriptado. Cabe hacer mención, que para el caso del proceso de desencriptado deben coincidir las claves respectivas y el tipo de

mapeo seleccionado en la etapa de encriptado.

4.-Se debe seleccionar la opción de "mandar archivo" para mandar un archivo previamente cargado o bien "mandar mensaje de voz" para encriptar el mensaje de voz grabado por el usuario.

-El programa e interfaz gráfica, son el complemento del dispositivo, el programa puede ser simplemente un ejecutable e instalarse al usuario.

4.5. Conclusión

En este capítulo se abordaron los detalles de diseño y diagramas que explican el funcionamiento del prototipo de encriptador-desencriptador VoicE-D, en primera instancia, bloques de diagramas de flujo que explican el proceso de la información y de la comunicación a través de WiFi, así como la explicación de su programa complementario en la plataforma Matlab. La programación en el módulo RCM5600W se realizó en lenguaje Dynamic C, mientras que la programación de su programa complementario fue directamente en Matlab, que nos da la oportunidad de procesar diferentes tipos de información y se especializa en manipulación de matrices. El funcionamiento total del prototipo fue satisfacctorio, y tuvo lugar a varias mejoras en su rendimiento y fiabilidad.

Capítulo V

5. Resultados obtenidos

En este capítulo se presentan los resultados del prototipo "VoicE-D', mediante el envío de varios mensajes de voz con diferentes frecuencias de muestreo, así como la cantidad de bits para la calidad del sonido. Sin embargo, hay que estar seguros de que tan fiables son los criptogramas obtenidos por el "Voice-D", recordando que el "VoicE-D" utiliza el mapeo de Henon, mapeo de Ikeda, mapeo de Kaplan-Yorke, mapeo logistico 2D y el mapeo de Rössler. Para comprobar la fortaleza del criptograma se realiza un análisis y se presentan sus resultados.

5.1. Pruebas del "VoicE-D"

5.1.1. Encriptado con el mapeo de Henon

En la figura 34 podemos observar la gráfica del mensaje de voz enviado con longuitud de 5 segundos, a una frecuencia de muestro de $8KHz$ y 8 bits de resolución, así como el criptograma resultante, usando el mapeo de Henon de la ecuación 2.

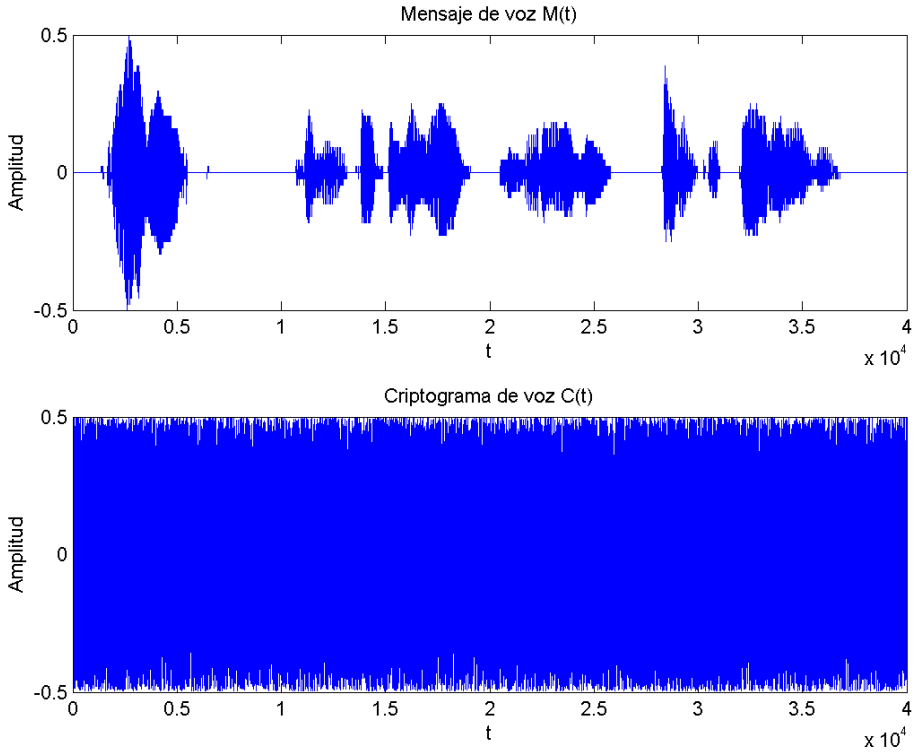


Figura 34: Mensaje de voz y su criptograma.

Para el análisis del histograma estadístico tenemos la figura 35, donde se observa el histograma del mensaje original a la izquierda, y el del criptograma a la derecha, se puede apreciar que tiene una uniformidad, así mismo se observa una componente de amplitud más repetida tanto en el mensaje original como en el criptograma de distinto valor.

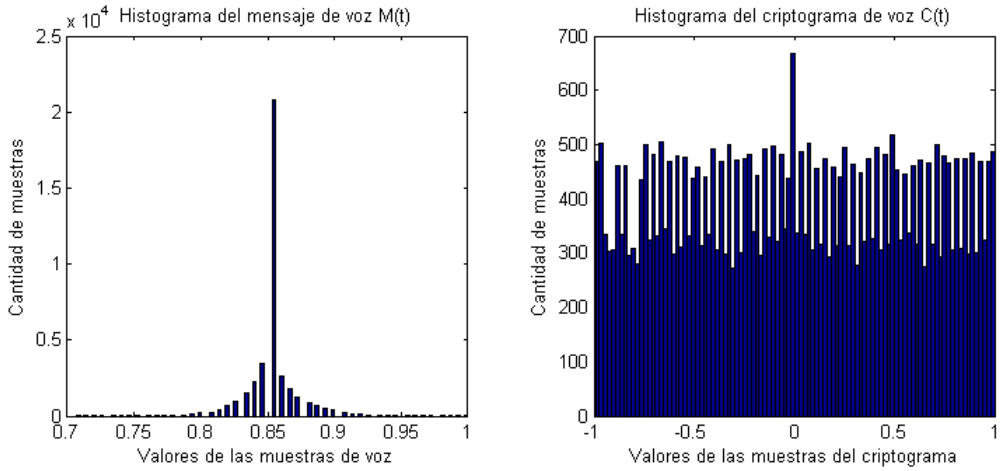


Figura 35: Histograma del mensaje de voz y de su criptograma.

La FFT para el mensaje original y el criptograma se muestra en la figura 36, vemos

la frecuencia original que corresponde al mensaje de voz, y notamos que el espectro del criptograma es contínuo, lo que hace fuerte al algoritmo ante ataques estadísticos relacionados con frecuencia.

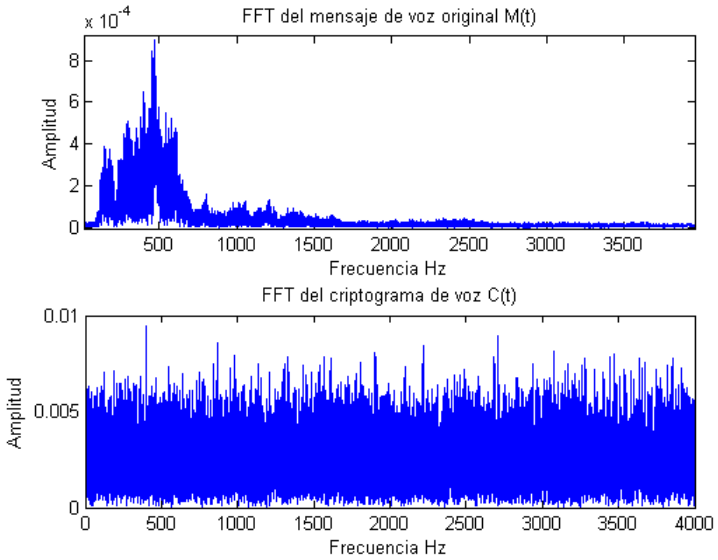


Figura 36: Transformada rápida de Fourier para el mensaje de voz y su criptograma.

En la figura 37 se muestra el mensaje recuperado a partir del criptograma, para ello, se necesita la clave correcta.

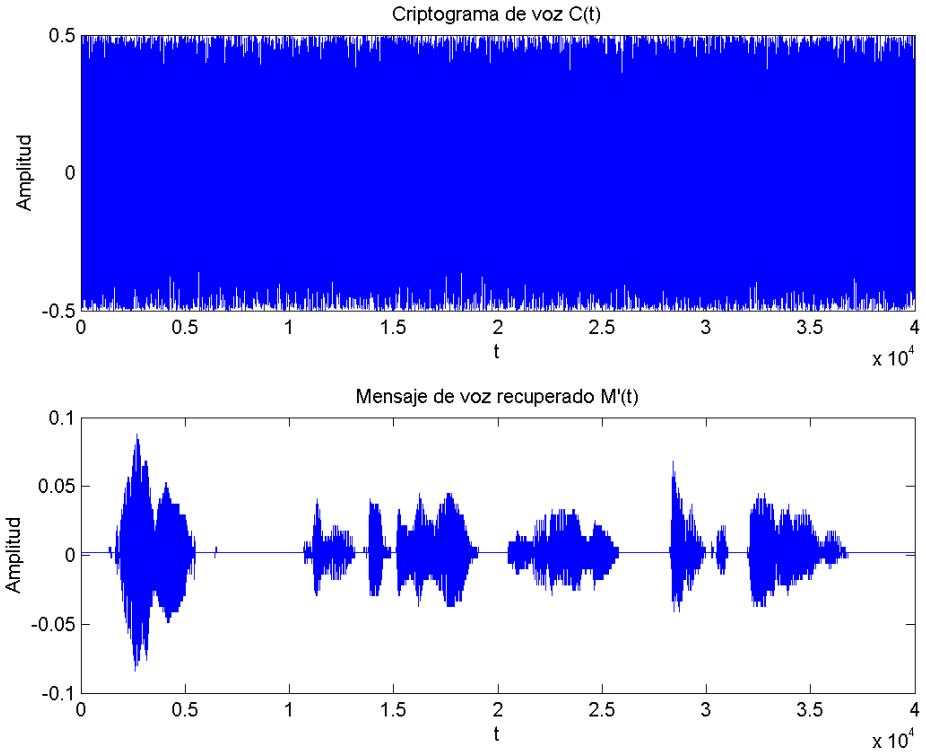


Figura 37: Mensaje recuperado con la clave correcta.

En la figura 38 tenemos el mensaje recuperado empalmado al original para corroborar que obtenemos exactamente la misma información en el proceso de desencriptado con las claves correctas.

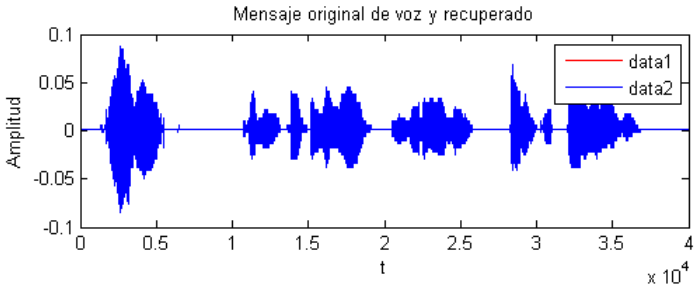


Figura 38: Mensaje de voz original y recuperado.

La figura 39 nos presenta el análisis a la sensibilidad de condiciones iniciales, la clave seleccionada para desencriptar posee un error de $1 \times 10^{-}5$ y vemos como efectivamente no se recupera nada parecido al mensaje original.

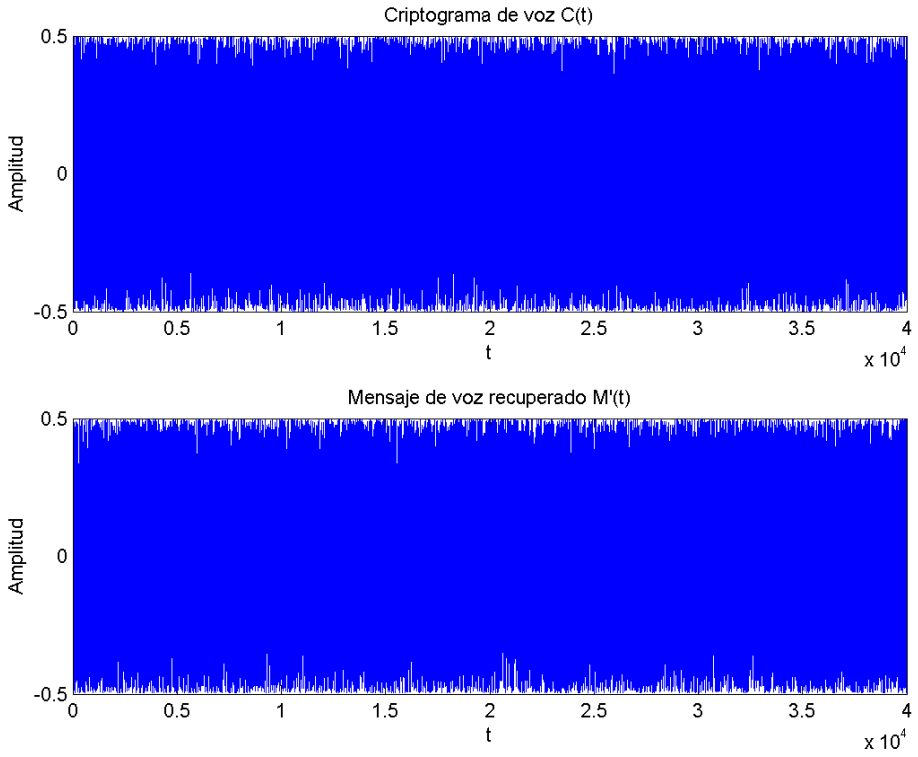


Figura 39: Mensaje recuperado con un error en la clave de 1×10^{-5}.

5.1.2. Encriptado con el mapeo de Ikeda

En la figura 40 se puede observar la prueba de encriptado con el mapeo de Ikeda de la ecuación 3, podemos observar el mensaje de voz con una $fs = 8KHz$, 8 bits de resolución y 5 segundos de duración, así mismo observamos el criptograma obtenido.

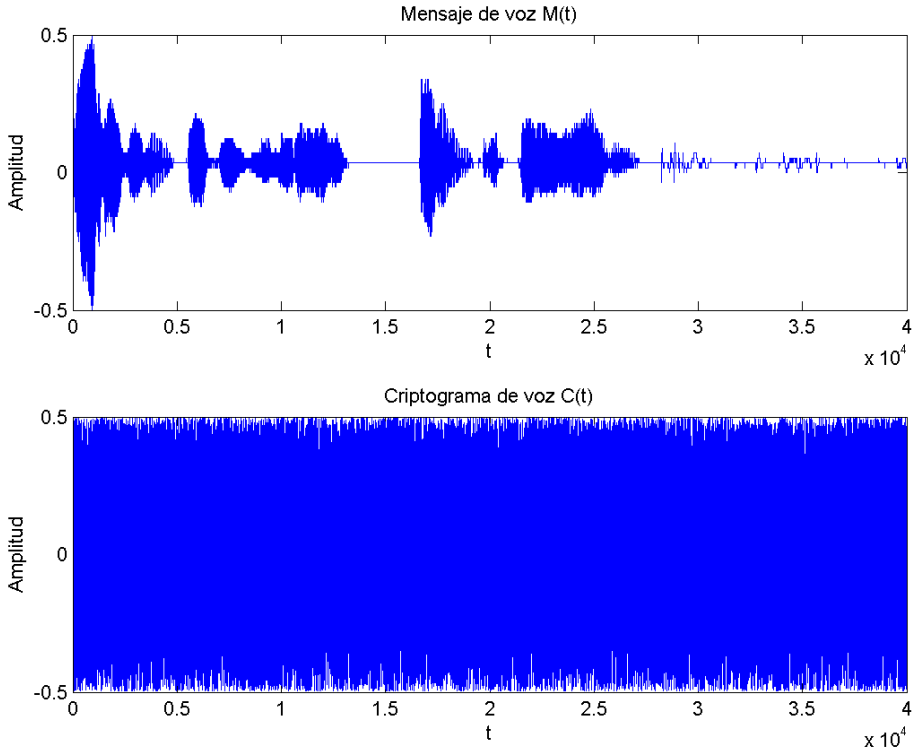


Figura 40: Mensaje de voz y su criptograma.

El histograma estadístico generado se muestra en la figura 41, se observa un histograma parcialmente uniforme, también se observa una componente de amplitud más repetida tanto en el mensaje original como en el criptograma, siendo la componente de amplitud más repetitiva diferente en el mensaje original y el criptograma.

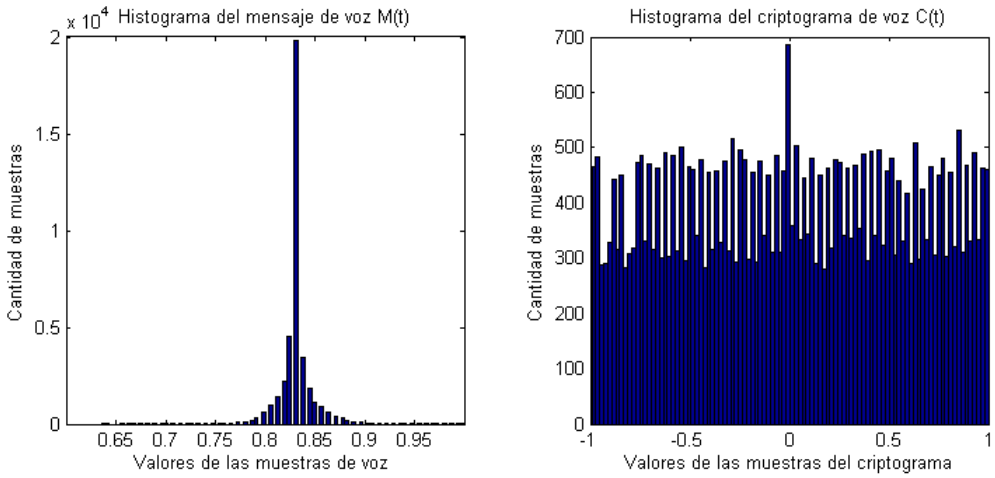


Figura 41: Histograma del mensaje de voz y de su criptograma.

Tenemos ahora en la figura 42 la FFT del mensaje de voz y del criptograma generado con el algoritmo de encriptado basado en el mapeo de Ikeda, la FFT del mensaje original evidencia las frecuencias originales, una vez encriptado, el espectro se vuelve contínuo, ocultando toda la información espectral.

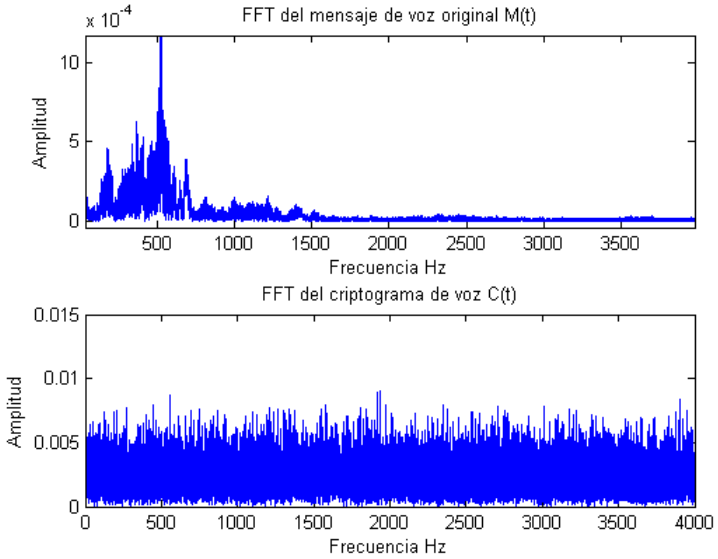


Figura 42: Transformada rápida de Fourier para el mensaje de voz y su criptograma.

Una vez encriptado el mensaje, se vuelve a mandar el VoicE-D para desencriptarlo y en la figura 43 observamos que el mensaje se recupera correctamente, comprobando su correcto proceso inverso, todo esto usando la clave correcta seleccionada para el primer encriptado.

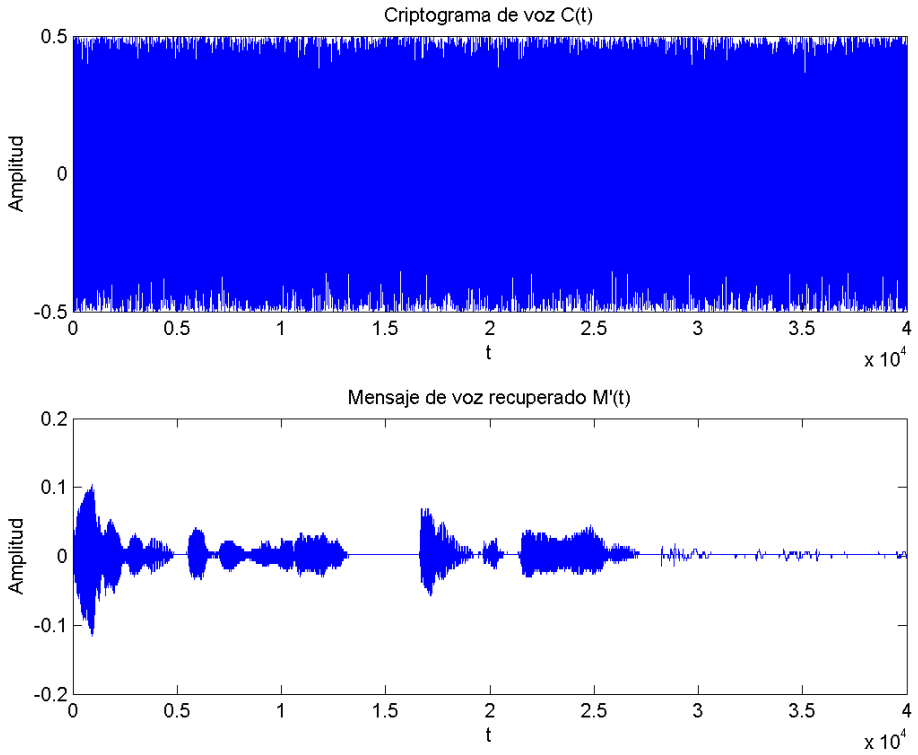


Figura 43: Mensaje recuperado con la clave correcta.

En la figura 44 se presenta el mensaje recuperado empalmado al original para corroborar que obtenemos exactamente la misma información en el proceso de desencriptado con las claves correctas.

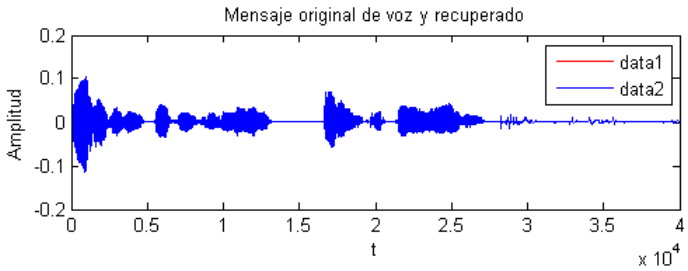


Figura 44: Mensaje de voz original y recuperado.

Para el análisis de sensibilidad se escoge una clave con un error de 1×10^{-5} y en la figura 45, comprobamos esta cualidad de la criptografía caótica para el mapeo de Ikeda.

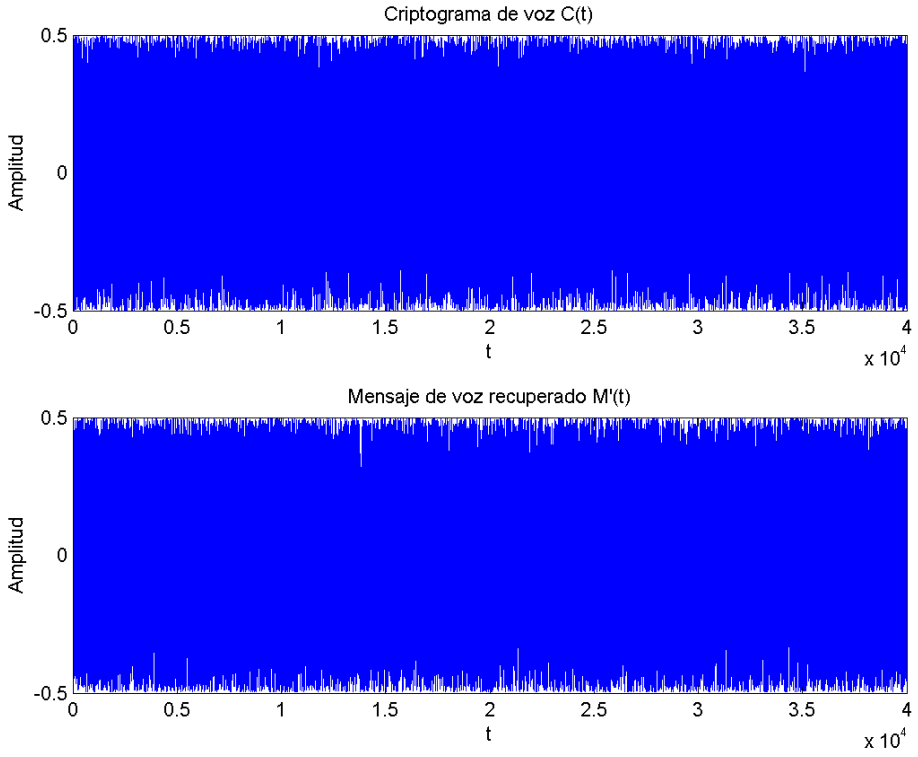


Figura 45: Mensaje recuperado con un error en la clave de 1×10^{-5}.

5.1.3. Encriptado con el mapeo de Kaplan-Yorke

La figura 46 nos muestra el mensaje de voz y su criptograma generado con el mapeo de Kaplan-Yorke de la ecuación 4, con longitud de 5 segundos, $fs = 8KHz$, y 8 bits de resolución.

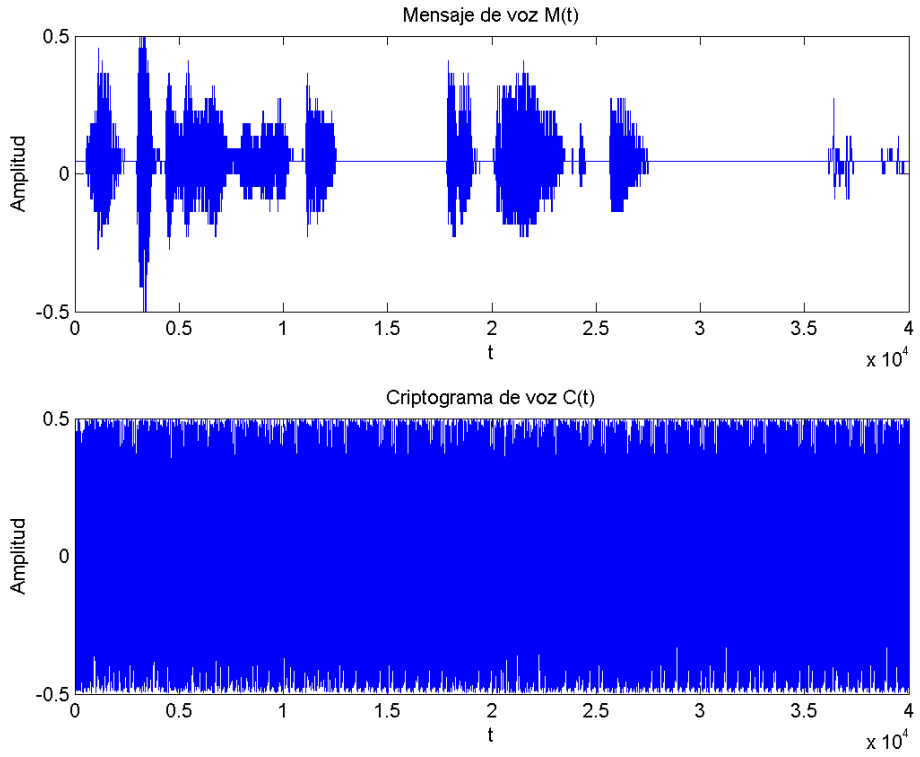


Figura 46: Mensaje de voz y su criptograma.

El histograma estadístico se muestra en la figura 47, observamos que no es uniforme, sin embargo varia en todos los valores, confundiendo el histograma original, en este caso, se observa una componente de amplitud más repetida tanto en el mensaje original como en el criptograma, siendo la componente de amplitud más repetitiva diferente en el mensaje original y el criptograma.

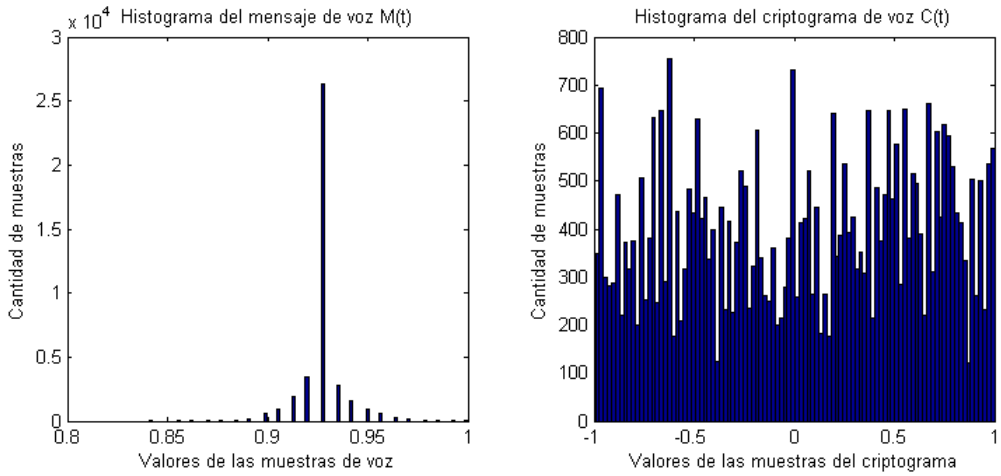


Figura 47: Histograma del mensaje de voz y de su criptograma.

La FFT del mensaje de voz y criptograma se muestra en la figura 48, se puede observar como la FFT del criptograma no precisamente contínua, ya que posee muchas frecuencias de información, pero esconde muy bien la información original del mensaje de voz.

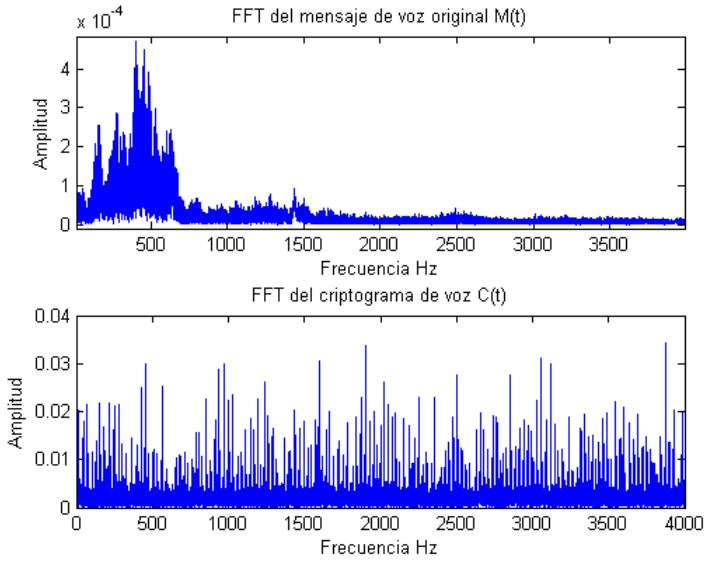


Figura 48: Transformada rápida de Fourier para el mensaje de voz y su criptograma.

Comprobamos el correcto proceso de recuperación del mensaje con las claves correctas como se observa en la figura 49.

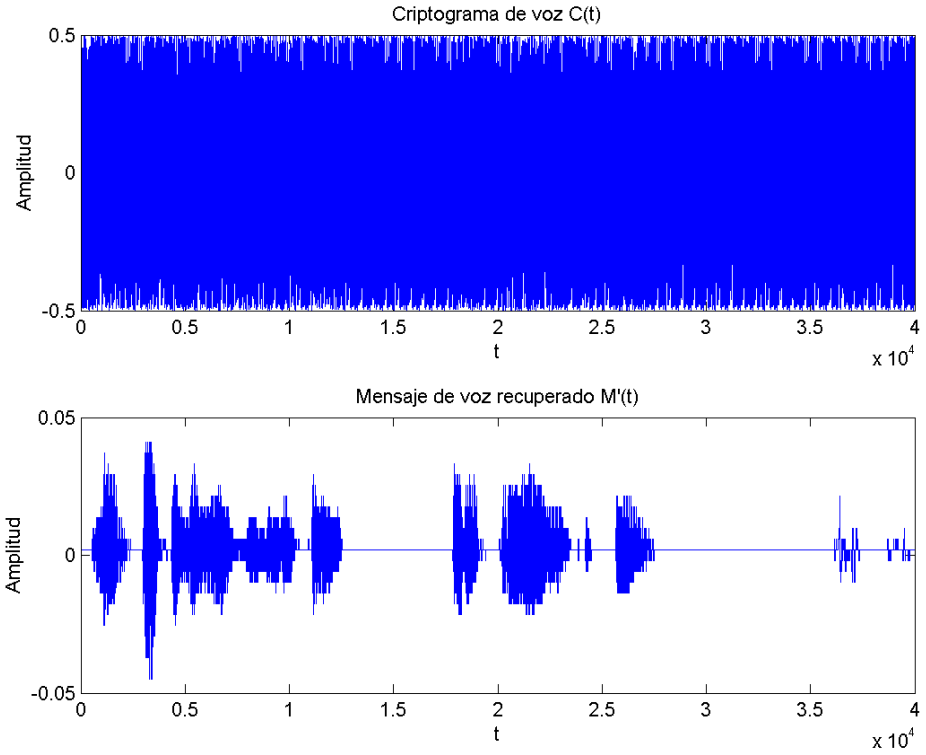


Figura 49: Mensaje recuperado con la clave correcta.

En la figura 50 tenemos el mensaje recuperado empalmado al original para corroborar que obtenemos exactamente la misma información en el proceso de desencriptado con las claves correctas.

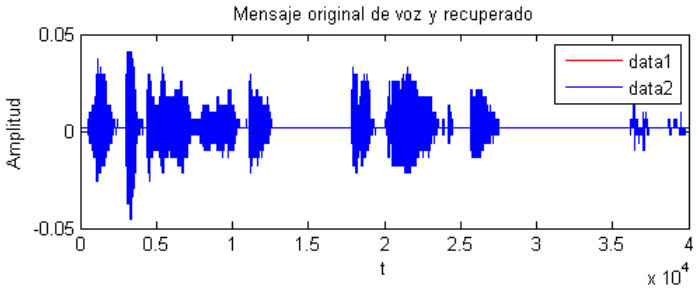


Figura 50: Mensaje de voz original y recuperado.

En la figura 51 se muestra el análisis de sensibilidad al escoger una clave con un error de 1×10^{-5}.

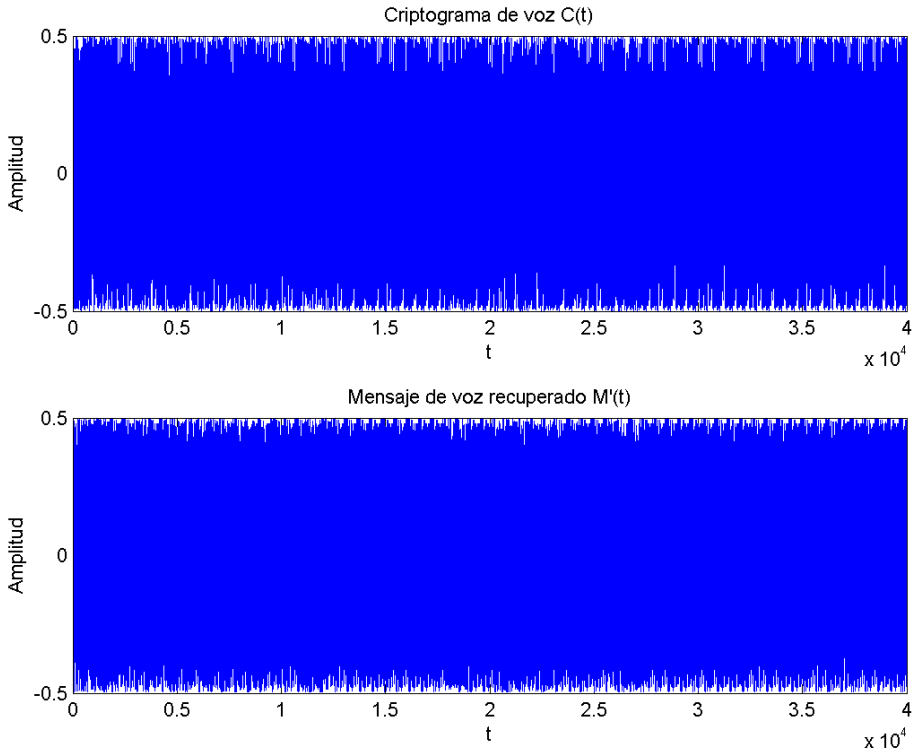


Figura 51: Mensaje recuperado con un error en la clave de 1×10^{-5}.

5.1.4. Encriptado con el mapeo logístico 2D

El mensaje original y el criptograma generado con el algoritmo que utiliza el mapeo logístico 2D, de la ecuación 5 se muestra en la figura 52, con una $fs = 8KHz$, 8 bits de resolución y una longitud de 5 segundos.

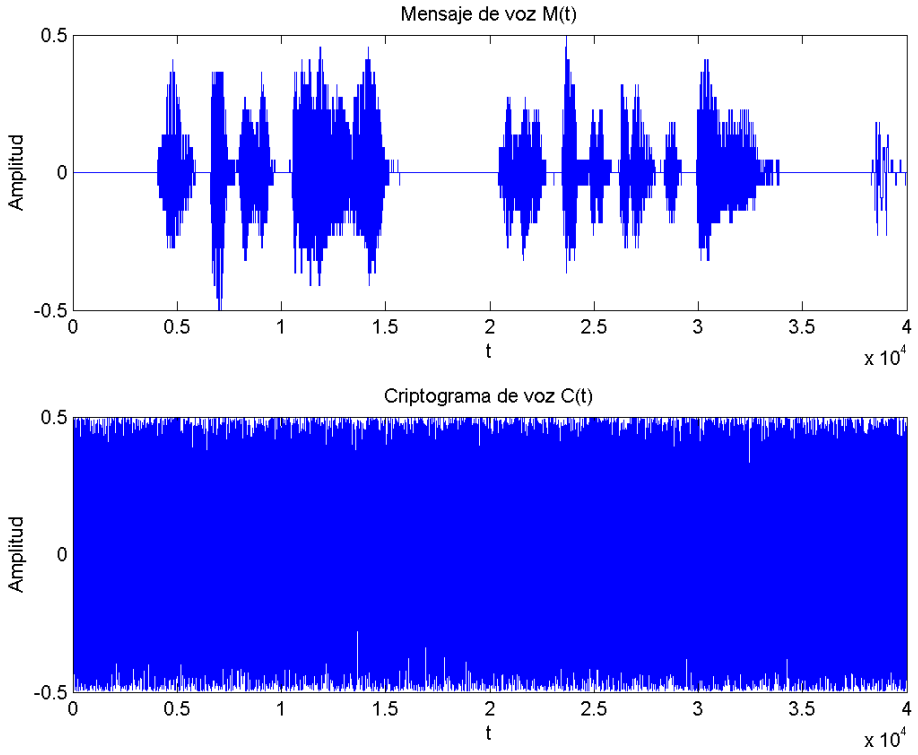


Figura 52: Mensaje de voz y su criptograma.

En la figura 53 se puede observar el histograma estadístico generado, el histograma del criptograma es uniforme, se observa al igual que los resultados anteriores una componente de amplitud más repetida tanto en el mensaje original como en el criptograma, siendo la componente de amplitud más repetitiva de distinto valor.

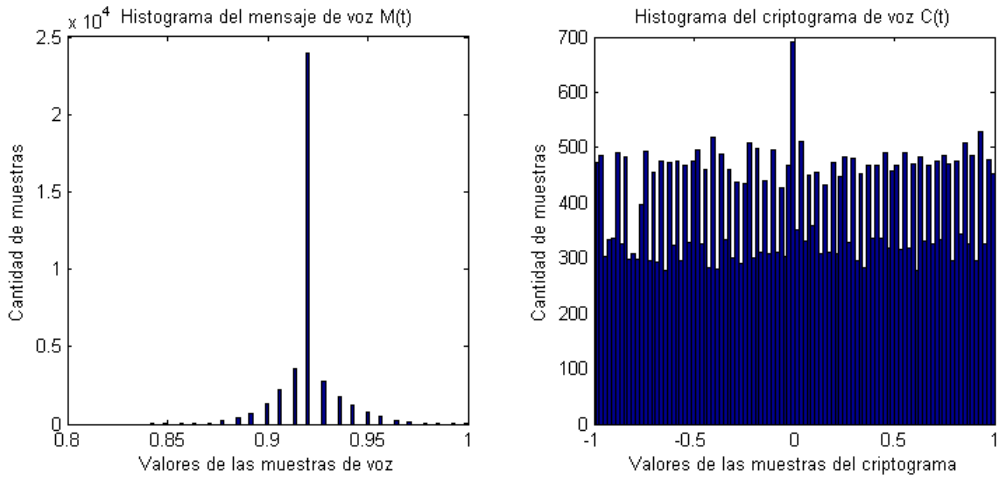


Figura 53: Histograma del mensaje de voz y de su criptograma.

La figura 54, nos muestra las FFT para el mensaje original y su criptograma, podemos observar como el criptograma oculta perfectamente la información original creando un espectro contínuo.

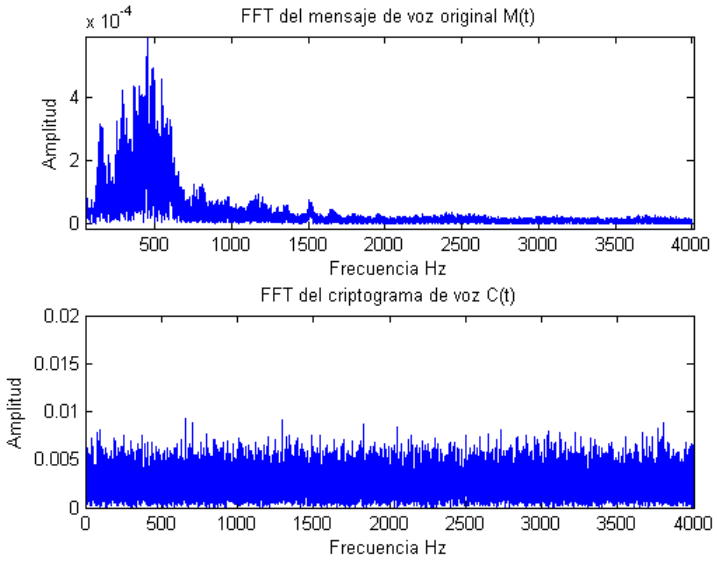


Figura 54: Transformada rápida de Fourier para el mensaje de voz y su criptograma.

En la figura 55 se observa el mensaje correctamente recuperado, con las claves correctas.

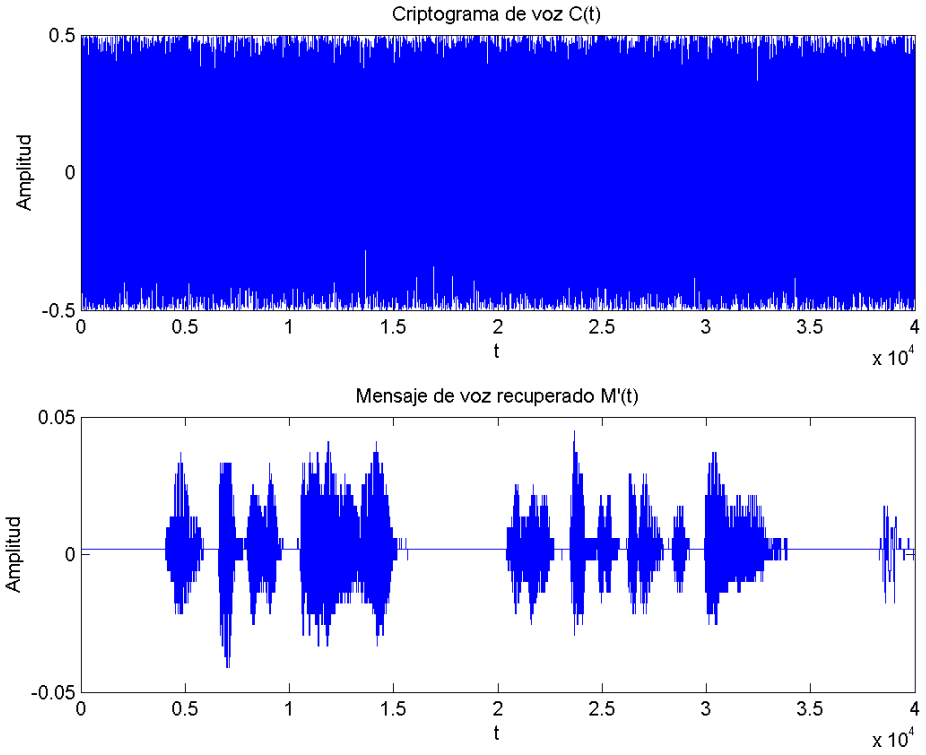


Figura 55: Mensaje recuperado con la clave correcta.

En la figura 56 se presenta el mensaje recuperado empalmado al original para corroborar que obtenemos exactamente la misma información en el proceso de desencriptado con las claves correctas.

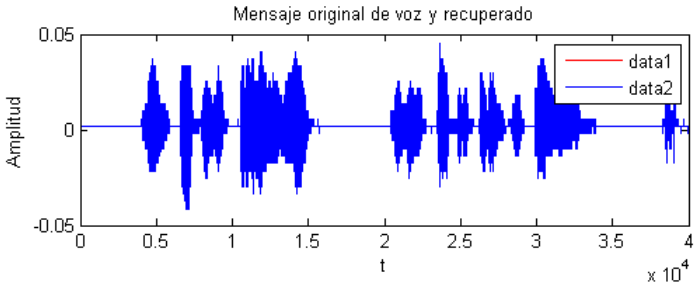


Figura 56: Mensaje de voz original y recuperado.

En la figura 57 se observa el análisis de sensibilidad y obtenemos una respuesta positiva, al escoger una clave con 1×10^{-5} de diferencia con respecto a la original.

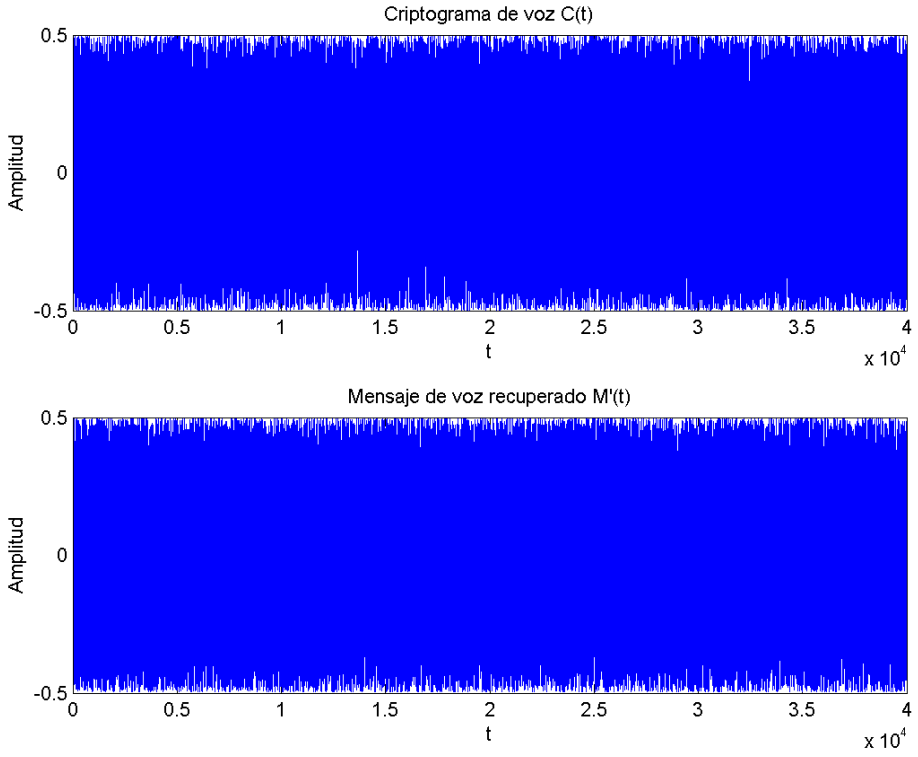


Figura 57: Mensaje recuperado con un error en la clave de 1×10^{-5}.

5.1.5. Encriptado con el mapeo de Rössler

En la figura 58 se observa el mensaje de voz original y el criptograma usando el mapeo de Rössler que es definido por la ecuación6, el mensaje es de una longitud de 5 segundos, $fs = 8KHz$ y una calidad de 8 bits.

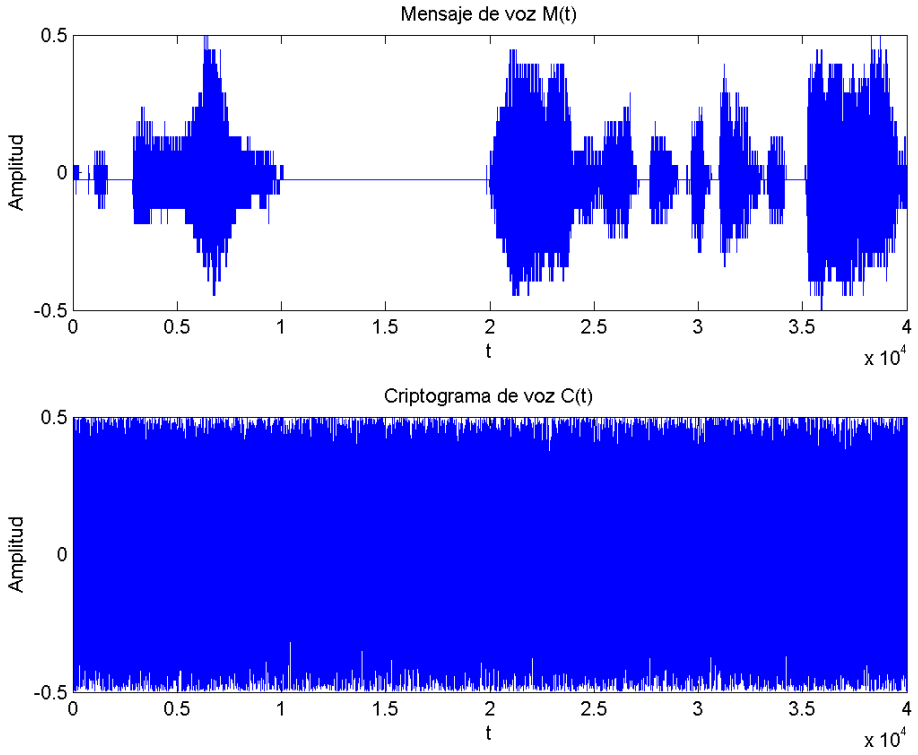


Figura 58: Mensaje de voz y su criptograma.

El histograma estadístico es mostrado en la figura 59, podemos observar que el histograma del criptograma esconde la información del histograma del mensaje original, también se observa una componente de amplitud más repetida tanto en el mensaje original como en el criptograma, siendo la componente de amplitud más repetitiva de distinto valor.

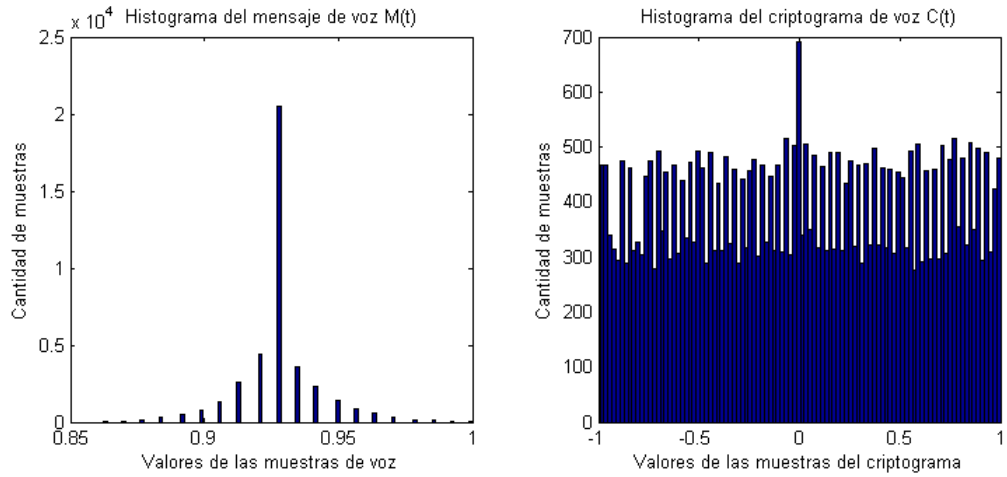


Figura 59: Histograma del mensaje de voz y de su criptograma.

La figura 60 nos muestra la FFT del mensaje original y de su criptograma, observamos bien como el espectro del criptograma es contínuo y oculta la información espectral original.

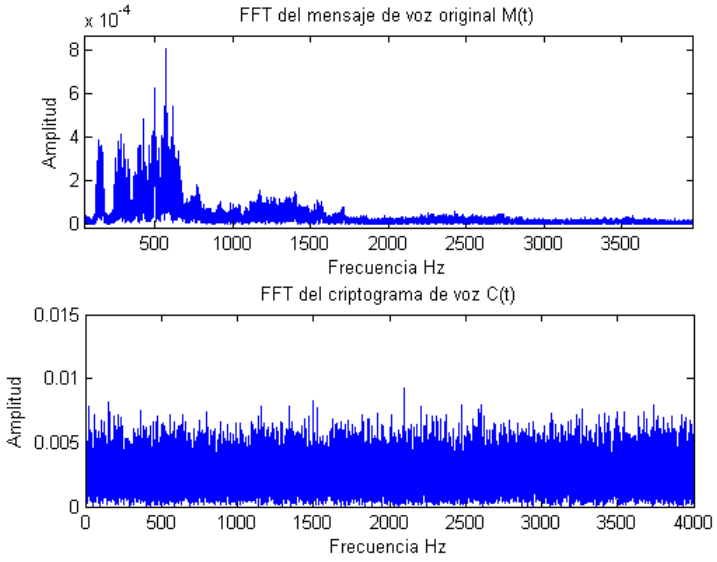


Figura 60: Transformada rápida de Fourier para el mensaje de voz y su criptograma.

Se recupera entonces el mensaje original y en la figura 61 se puede observar que este proceso es satisfactorio, escogiendo obviamente las claves correctas para el desencriptado.

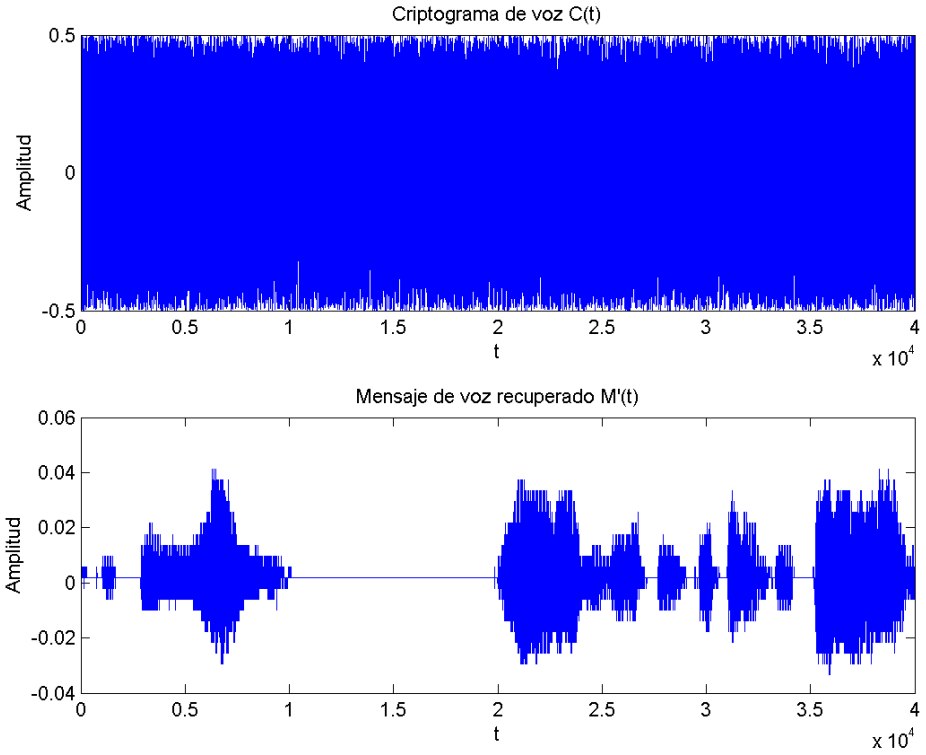


Figura 61: Mensaje recuperado con la clave correcta.

En la figura 62 se muestra el mensaje recuperado empalmado al original para corroborar que obtenemos exactamente la misma información en el proceso de desencriptado con las claves correctas.

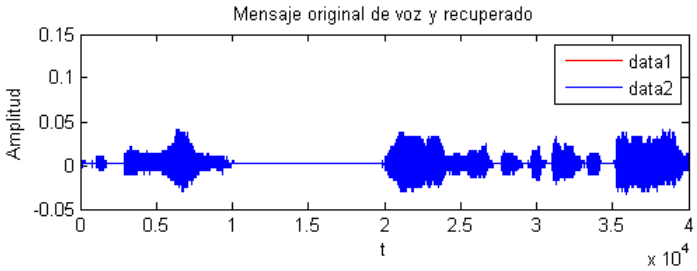


Figura 62: Mensaje de voz original y recuperado.

El análisis de sensibilidad a las condiciones iniciales, se muestra en la figura 63, podemos observar como no recuperamos el mensaje original a pesar de haber utilizado una clave con un error de 1×10^{-5} lo cual es una de las cualidades de la criptografía caótica.

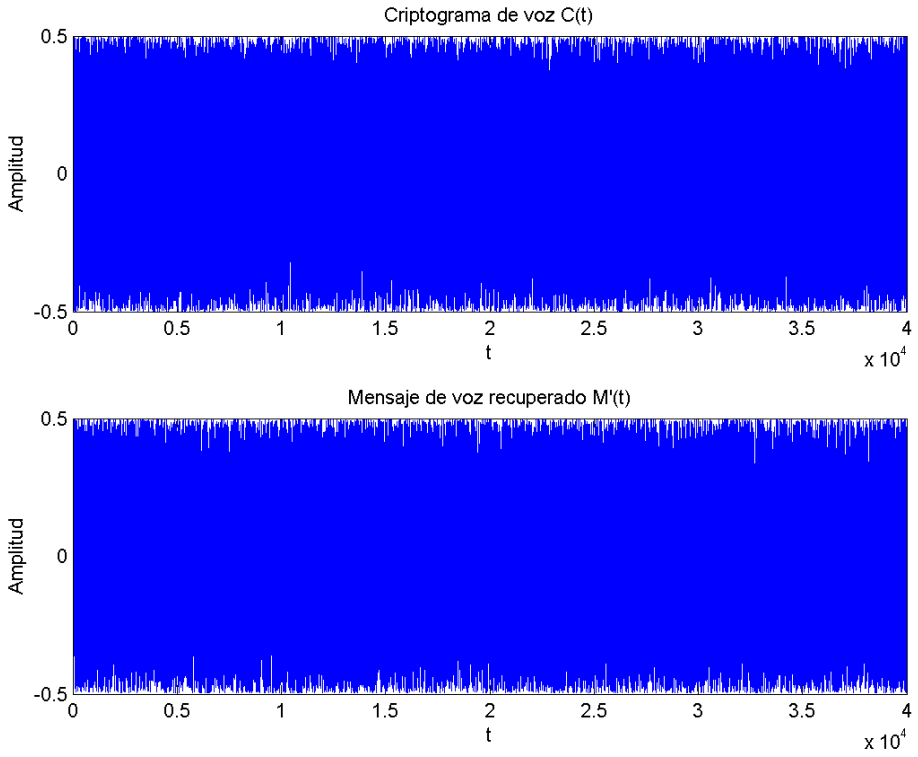


Figura 63: Mensaje recuperado con un error en la clave de 1×10^{-5}.

Cuadro 1: Comparación de resultados de encripción para cada mapeo utilizado

Parametro	**Henon**	**Ikeda**	**Kaplan-Yorke**	**Logístico 2D**	**Rössler**
Clave 1	51258	74815	48512	85631	85631
Clave 2	24575	25301	98621	01425	01425
Tiempo de encriptado	19.1145s	35.2947s	19.1046s	22.6513	26.4605s
Tiempo de desencriptado	19.1052s	35.1632s	19.1389s	22.6927	26.4483
Histograma resistente	Si	Si	Si	Si	Si
FFT de espectro continuo	Si	Si	Si	Si	Si
Mensaje recuperado	√	√	√	√	√
Análisis de sensibilidad	√	√	√	√	√
Espacio de claves	2^{83}	2^{66}	2^{49}	2^{99}	2^{149}
Entropía del mensaje de voz	2.8417	2.8692	1.9697	2.2894	2.5901
Entropía del criptograma	7.9761	7.9749	7.8327	7.9714	7.9736

En el cuadro de comparación podemos observar los diferentes resultados para cada uno de los mapeos caóticos utilizados, las claves son arbitrarias y constan de 5 digitos numéricos cada una, que es la máxima resolución que soporta para cálculos el módulo RCM5600W.

-El mapeo que realiza el proceso de encriptado más rapido (esto es para 5 segundos de duración) es el mapeo de Kaplan-Yorke, siguiéndole el de Henon, el mapeo logístico 2D, el mapeo de Rössler y por último el mas lento el mapeo de Ikeda.

-Todos los histogramas generados, aunque no son completamente uniformes, poseen una alta resistencia a ataques estadísticos ya que ocultan muy bien la información original como se vio anteriormente.

-La FFT de cada mapeo genera un espectro contínuo, logrando ocultar completamente el espectro original, comprobando su resistencia a ataques estadísticos al espectro.

-El análisis a la sensibilidad fue satisfactorio en todos los casos, como se esperaba, ya que se están utilizando mapeos caóticos.

-El espacio de claves mayor, pertenece al mapeo de Rössler, podemos ver claramente que en cuestión de espacio de claves y de velocidad de encriptado y desencriptado esta es la mejor opción de encriptado, el mapeo de Ikeda además de ser el más lento en encriptar posee un bajo espacio de claves, como también Kaplan-Yorke, si de cuestión de tiempo se trata, Henon es una mejor opción ya que es prácticamente igual de rápido que Kaplan-Yorke con un espacio de claves mucho más extenso. El mapeo logístico 2D posee una buena velocidad de encriptado

y un espacio de claves considerable, habría que considerar la aplicación de nuestro prototipo para determinar cual es la mejor opción de encriptado.

-Como ya mencionamos, la entropía de un criptograma ideal sería de 8 ya que estamos utilizando 8 bits, todo los mapeos nos dan valores aproximados, siendo el más bajo el mapeo de Kaplan-Yorke quien a su vez tiene el menor espacio de claves, los otros mapas manejan una entropía mayor a 7,97 es decir casi de 8, recordando que cuando un sistema criptográfico emite criptogramas con entropía menor a 8, este encriptador tiene cierto grado de predicibilidad, por lo que su seguridad se pone en riesgo [Inzunza 2013].

5.2. Conclusión

En este capítulo se mostraron y comentaron los resultados obtenidos con el prototipo de encriptador-desencriptador VoicE-D, al explicar y realizar los análisis de seguridad, damos fiabilidad a los criptogramas generados mediante el uso de la criptografía caótica en combinación con programación de sistemas embebidos, y aplicación de estos en comunicaciones y telecomunicaciones. La seguridad es el factor clave de estas aplicaciones, ya que uno de los objetivos prioritarios es proteger la información del mensaje de voz generado, el criptoanálisis va en desarrollo al mismo tiempo que la tecnología y las técnicas de encriptado, quizá pasen décadas antes de que se desarrollen métodos para atacar criptografía caótica, pero como ya sabemos, todos los sistemas criptográficos tienen un tiempo de vida. Al mostrar estos resultados, comprobamos que nuestra solución al problema es completamente viable, y que su aplicación puede ser inmediata con los sistemas ya existentes en la actualidad.

Capítulo VI

6. Resumen y conclusiónes

En este trabajo de tesis de maestría, se implementó un sistema criptográfico basado en el microcontrolador rabbit RCM5600W, que opera como un periférico de computadora con comunicación WiFi y que en combinación con un programa desarrollado en Matlab, que permite la manipulación en tiempo real de señales de audio.

Primeramente se prueba el envío de información con dinámica caótica a través del protocolo 802.11 de la IEEE, empleando en este trabajo , los mapeos de Henon, Ikeda, Kaplan-Yorke, logístico 2D y Rössler. Estos modelos caóticos son generados por ecuaciones de recurrencias de manera digital, por lo que su dinámica caótica se observa en la distribución binaria de los datos no afectando la comunicación.

Se valida experimentalmente la operatividad del sistema criptográfico implementado VoicE-D y se vislumbra su potencialidad en aplicaciones en sistemas de telecomunicación.

El prototipo encriptador-desencriptador desarrollado en un sistema embebido en combinación con criptografía caótica tiene una potencial implementación en sistemas de comunicación portátiles. Hoy en día un gran porcentaje de personas utilizan telefonos inteligentes, los cuales poseen procesadores de hasta 1 GHz y los de última generación hasta 8 nucleos en su procesador, considerando que el módulo RCM5600W tiene una frecuencia de reloj de 74MHz, por lo que es factible su implementación en dispositivos móviles modernos.

6.1. Trabajos a futuro

• Realizar encriptado en otros módulos de sistemas embebidos, con diferentes caracteristicas en velocidad, capacidad de memoria y portabilidad, utilizando otros mapeos caóticos, y eliminando la interfaz de computadora, haciéndolo directamente con un prototipo electrónico compacto.

• Realizar encriptado de información en comunicación con otro tipo de tecnologías inalambricas como de telefonia celular 3G, 4G, bluetooth, comunicación zigbee, CDMA, para comprobar la aplicación universal de la criptografía caótica.

• Considerar el encriptado de otro tipo de datos, como imágenes, documentos, programas, para realizar una comunicación completa y segura, haciendo nuevamente análisis de seguridad para corroborar la resistencia a ataques estadísticos y de fuerza bruta a los criptogramas obtenidos.

• Realizar el encriptado de audio con tarjetas FPGA's que poseen mucha más capacidad de procesamiento y memoria, además de muchos puertos de comunicación.

• Crear una especie de nube en un servidor de internet, que posea una base de datos protegida con criptografía caótica, comparándose con los servicios actuales de nubes de información pública.

7. Apéndice A: Ecuaciones caóticas a partir de números aleatorios

En este apéndice se detalla un trabajo de investigación innovador para lograr obtener ecuaciones con comportamiento caótico, siendo obtenidas estas, a través de números aleatorios y procesos de cómputo evolutivo realizado por un software llamado Eureqa de Cornell Creative Machines Lab [Eureqa 2013].

7.1. Números aleatorios

Los números aleatorios son números que se manifiestan en una secuencia en las cuales se tienen las siguientes dos condiciones:

1.-Los valores están distribuidos uniformemente sobre un intervalo definido.

2.-Es imposible predecir valores futuros basados en valores pasados o presentes.

Para obtener números aleatorios reales, se usaron diferentes métodos, mediante la página de internet www.random.org, que pertenece a la universidad Trinity College de Dublín, se obtuvieron números aleatorios originados de ruido atmosférico. Además se obtuvieron al grabar sonido ambiental, revisar colores de imágenes, consultar información financiera, y valores de radioactividad.

7.2. Eureqa

Eureqa es una herramienta de software que se utiliza para detectar ecuaciones y relaciones matemáticas ocultas en datos. Su meta es identificar las más simples fórmulas matemáticas que pueden describir los mecanismos subyacientes que producen esos datos. Eureqa es un programa de libre uso y descarga que utiliza programación genética, esta consiste en una metodología basada en los algoritmos evolutivos, y tiene su inspiración en la evolución biológica para desarrollar automáticamente programas de computadoras que realicen una tarea que el usuario define. En el caso de Eureqa, sus algoritmos evolutivos nos ayudan a obtener ecuaciones que pueden definir un arreglo de datos, en este caso números aleatorios reales.

7.3. Autocorrelación

En probabilidad y estadística, la correlación indica la fuerza y la dirección de una relación lineal y proporcionalidad entre dos variables estadísticas, en este caso la autocorrelación es una herramienta matemática utilizada frecuentemente en el procesado de señales, y es definida como la correlación cruzada de la señal consigo misma por lo que estas dos variables terminan siendo la misma. La función de autocorrelación resulta de gran utilidad para encontrar patrones repetitivos dentro de una señal, como por ejemplo, la periodicidad de una señal enmascarada bajo el ruido o para identificar la frecuencia fundamental de una señal que no contiene dicha componente, pero aparecen numerosas frecuencias armónicas de esta. Esta utilidad de la autocorrelación nos permitirá saber si nuestra ecuación caótica nueva es única, es decir, no posee varias frecuencias [León-García 2008].

7.4. Histograma

En estadística, un histograma es una representación gráfica de una variable en forma de barras, donde la longitud de cada barra es proporcional a la frecuencia de los valores representados. Sirven para obtener una "primera vista" general, o panorama, de la distribución de la población, o la muestra, respecto a una característica, cuantitativa y contínua, de la misma y que es de interés para el observador. En el caso de las ecuaciones caóticas, obtener el histograma nos ayuda a saber que tipo de distribución tienen los datos con dinámica caótica y en que umbral se encuentran [León-García 2008].

7.5. Exponente de Lyapunov

El exponente de Lyapunov o exponente característico de Lyapunov de un sistema dinámico, es una cantidad que caracteriza el grado de separación de dos trayectorias infinitesimalmente cercanas. Es importante para la cuantificación de sistemas dinámicos, caracteriza el atractor completo y no sus propiedades locales [Sergey et al. 1998], el exponente de Lyapunov es calculado para las ecuaciones de recurrencias generadas con la ecuación 9

$$\sigma = \frac{1}{N}\sum_{n=1}^{N-1} ln(|\frac{x_1(n+1)}{x_1(n)}|) \tag{9}$$

Se dice que si al menos uno de los exponentes de Lyapunov calculados es mayor a 0, esto es si es positivo, entonces se considera que el sistema posee dinámica caótica [Inzunza 2013]

7.6. Mapa de Feigenbaum

En matemáticas, un mapa de Feigenbaum o diagrama de bifurcación de un sistema dinámico es una estratificación de su espacio de parámetros inducida por la equivalencia topológica, junto con los retratos de fase representativos de cada estrato. Las soluciones estables suelen representarse mediante líneas contínuas, mientras que las soluciones inestables se representan con líneas punteadas [Lawrence 1998].

7.7. Generación de ecuaciones caóticas

1.-Se utilizan datos aleatorios y entonces introducimos estos datos en el programa eureqa, haciendo que cada valor del arreglo aleatorio tenga como entrada el valor anterior a este.

2.-Eureqa nos da una serie de ecuaciones las cuales evolucionan y van siendo más precisas a los datos que introducimos, pero entre más precisas también más complejas son las ecuaciones. Estas ecuaciones se toman al azar considerando cual nos conviene mas con respecto a su error y complejidad y se le hace un análisis de su histograma, autocorrelación y exponente de lyapunov, que nos muestran si la ecuación tiene o no una dinámica caótica.

3.-Si la ecuación encontrada no es una ecuación con dinámica caótica, entonces se procede a utilizar otros datos aleatorios, pero en caso de encontrarse una respuesta positiva al hecho de que nuestra ecuación es caótica, entonces se obtiene el mapa de Feigenbaum para conocer todos los valores de ciertos parámetros de la ecuación en los cuales un comportamiento caótico existe, para tener de una simple ecuación al variar un parametro diferentes ecuaciones.

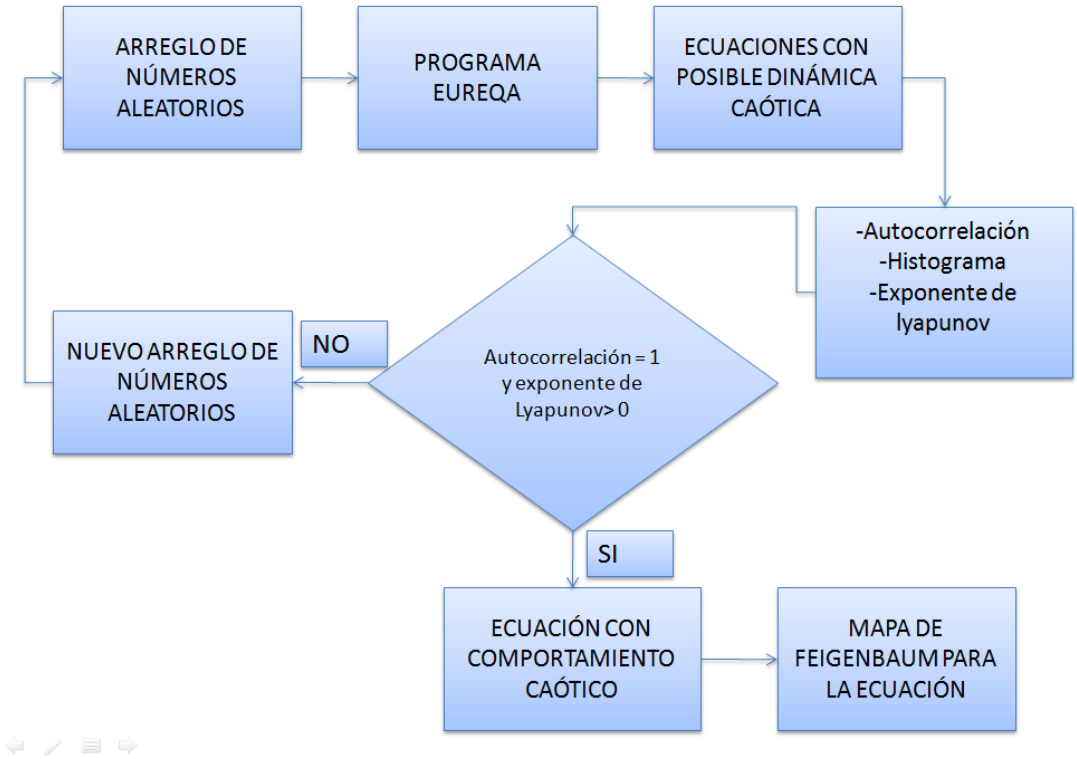


Figura 64: Diagrama de flujo que explica como encontrar nuevas ecuaciones caóticas.

En la figura 64 se muestra el proceso para encontrar nuevas ecuaciones caóticas:

1.-Empezando tenemos el arreglo de números aleatorios.

2.-Esos números se introducen al software Eureqa como se vera más adelante.

3.-Se obtienen diferentes ecuaciones y se elige una arbitrariamente con base en el error y complejidad.

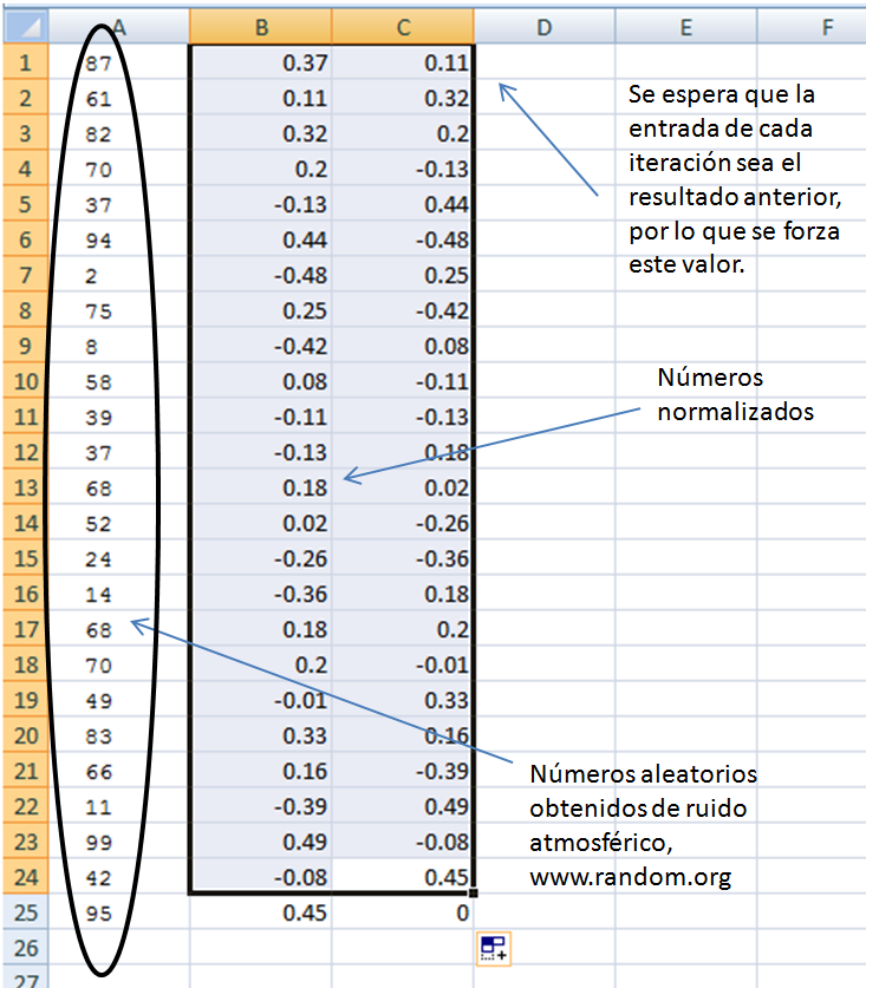
4.-A la ecuación obtenida se la aplican los procesos de autocorrelación, se obtiene su histograma y se calcula su exponente de Lyapunov.

5.-En caso de que la ecuación nos de una autocorrelación en la cual evidencíe que no está compuesta de varias frecuencias la ecuación, y además que su exponente de Lyapunov sea mayor que cero, entonces se dice que tenemos una ecuación con dinámica caótica y se obtiene su mapa de Feigenbaum, en caso contrario se puede intentar con otra ecuación o bien, introduciendo un nuevo arreglo de números aleatorios.

7.8. Ejemplo de obtención de una ecuación caótica.

A continuación se muestra el proceso para obtención de una ecuación caótica a partir de números aleatorios.

Para el paso 1 entonces tenemos nuestros números aleatorios enteros entre 0 y 100 obtenidos de www.random.org, en la figura 65 se muestran estos números y luego se normalizan para su proceso de computo evolutivo. Como la ecuación caótica es de tipo iterativa, su valor anterior es la entrada al valor futuro, por lo que se acomoda de tal manera que $x(n+1) = f(x(n))$.



	A	B	C
1	87	0.37	0.11
2	61	0.11	0.32
3	82	0.32	0.2
4	70	0.2	-0.13
5	37	-0.13	0.44
6	94	0.44	-0.48
7	2	-0.48	0.25
8	75	0.25	-0.42
9	8	-0.42	0.08
10	58	0.08	-0.11
11	39	-0.11	-0.13
12	37	-0.13	0.18
13	68	0.18	0.02
14	52	0.02	-0.26
15	24	-0.26	-0.36
16	14	-0.36	0.18
17	68	0.18	0.2
18	70	0.2	-0.01
19	49	-0.01	0.33
20	83	0.33	0.16
21	66	0.16	-0.39
22	11	-0.39	0.49
23	99	0.49	-0.08
24	42	-0.08	0.45
25	95	0.45	0
26			

Figura 65: Números aleatorios enteros y normalizados entre 1 y -1.

Para el paso 2 introducimos los datos de nuestra ecuación $x(n+1) = f(x(n))$ como se ilustra en la figura 66 en el programa eureqa que se encargará de calcular una ecuación matématica que satisfaga los valores introducidos

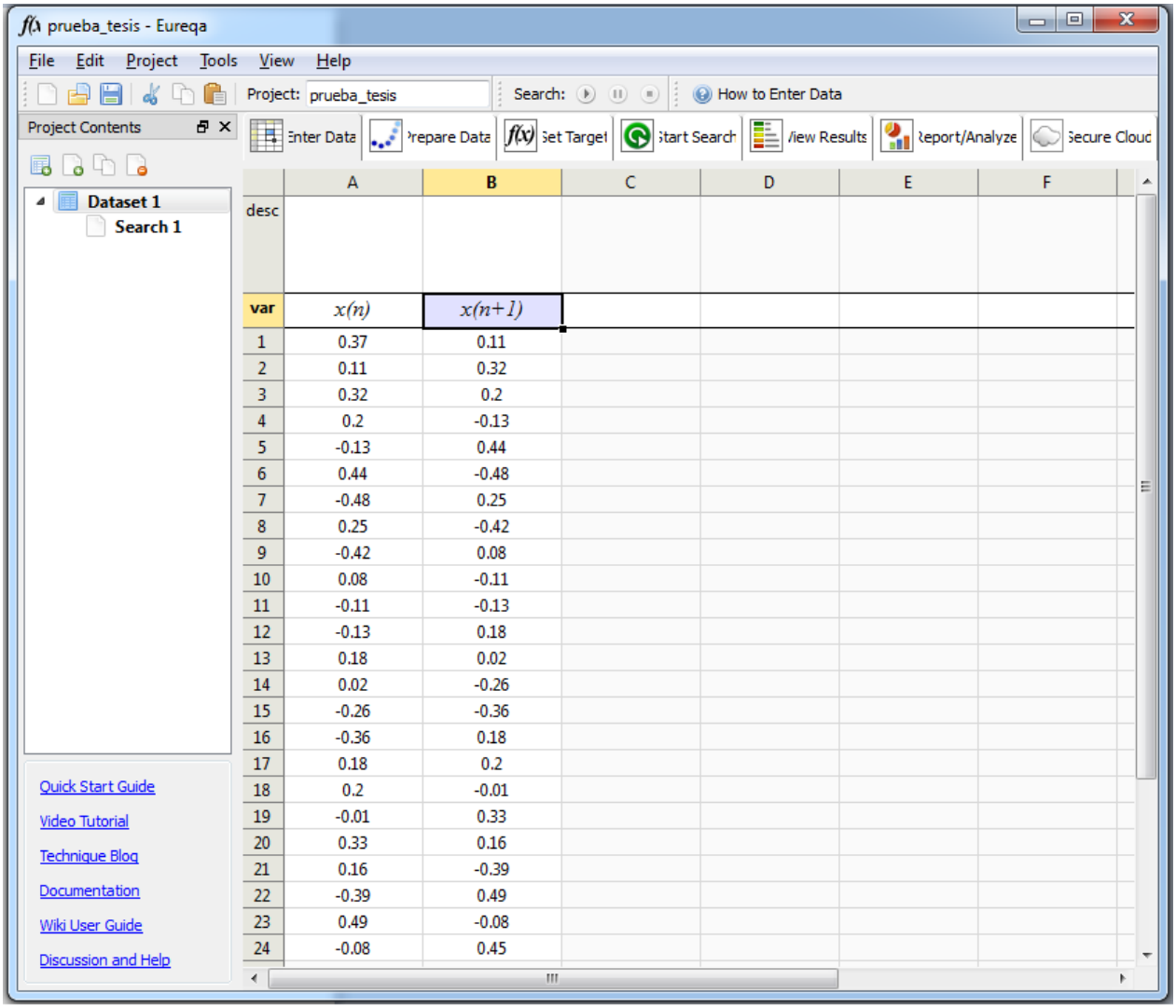


Figura 66: Datos introducidos en Eureqa para el cálculo de ecuaciones.

En la figura 67 vemos como Eureqa nos proporciona una gráfica de ambos arreglos de datos $x(n+1)$ y $x(n)$ listos para ser procesados en búsqueda de una ecuación que los genere. Eureqa es utilizado ya que nos proporciona mediante cómputo evolutivo, soluciones de distinto tipos que aproximan una solución real, en caso de no tener este programa, puede ser sustituido con un programa que realice cálculos similares.

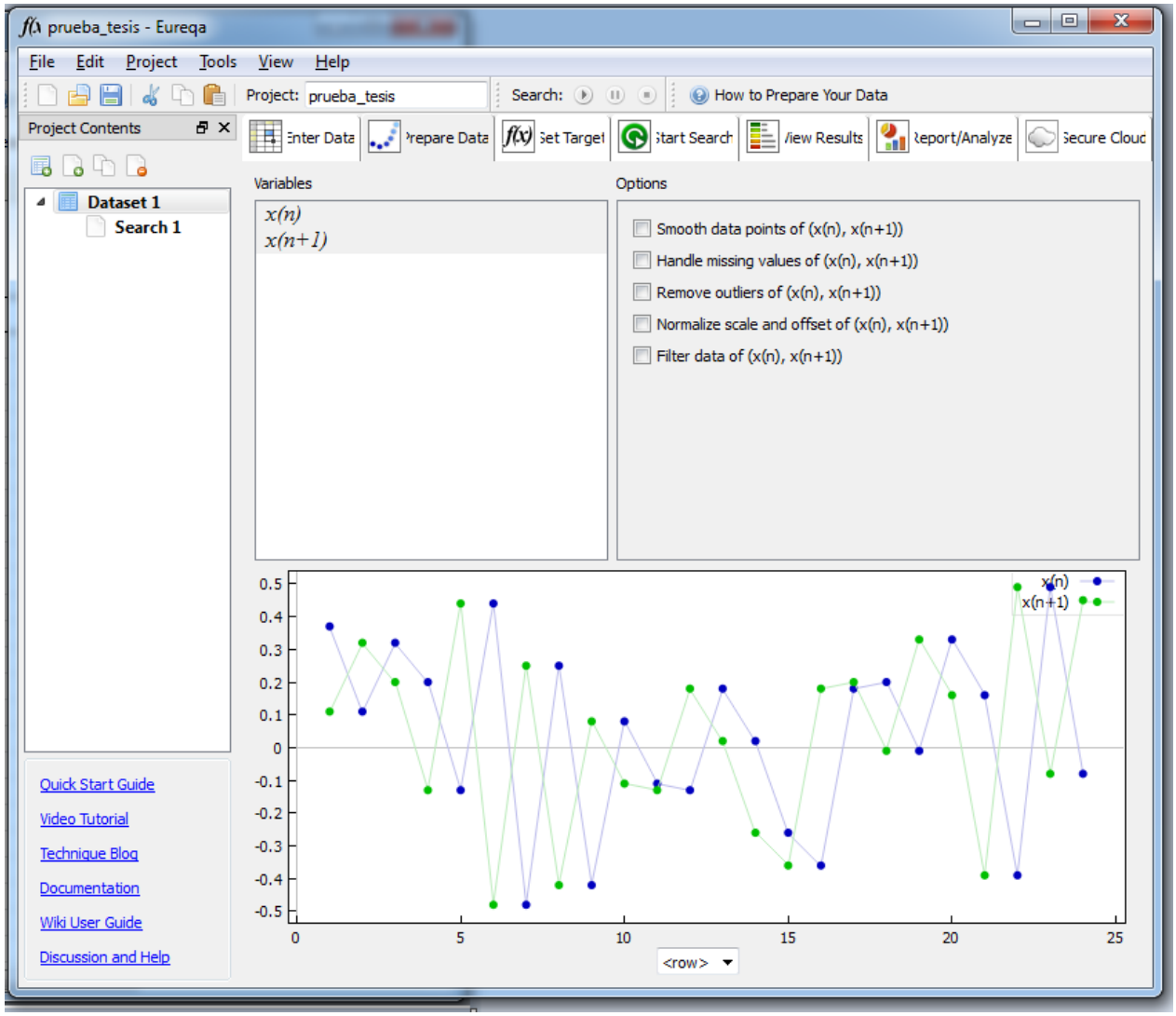


Figura 67: Eureqa con los datos listos para empezar a hacer cálculos.

Para el paso 3, vemos en la figura 68 las ecuaciones que va proponiendo el programa Eureqa, escogemos la ecuación 23 que nos da la aproximación que muestra la parte superior derecha de la figura, observamos en la parte inferior derecha su aproximación graficada en relación a su precisión contra complejidad, la ecuación que escogemos es la siguiente:

$$x(n+1) = 0{,}6109x(n)cos(5{,}831 + 19{,}82x1(n)) - 0{,}3903cos(4{,}192 + 162{,}5x1(n)) \qquad (10)$$

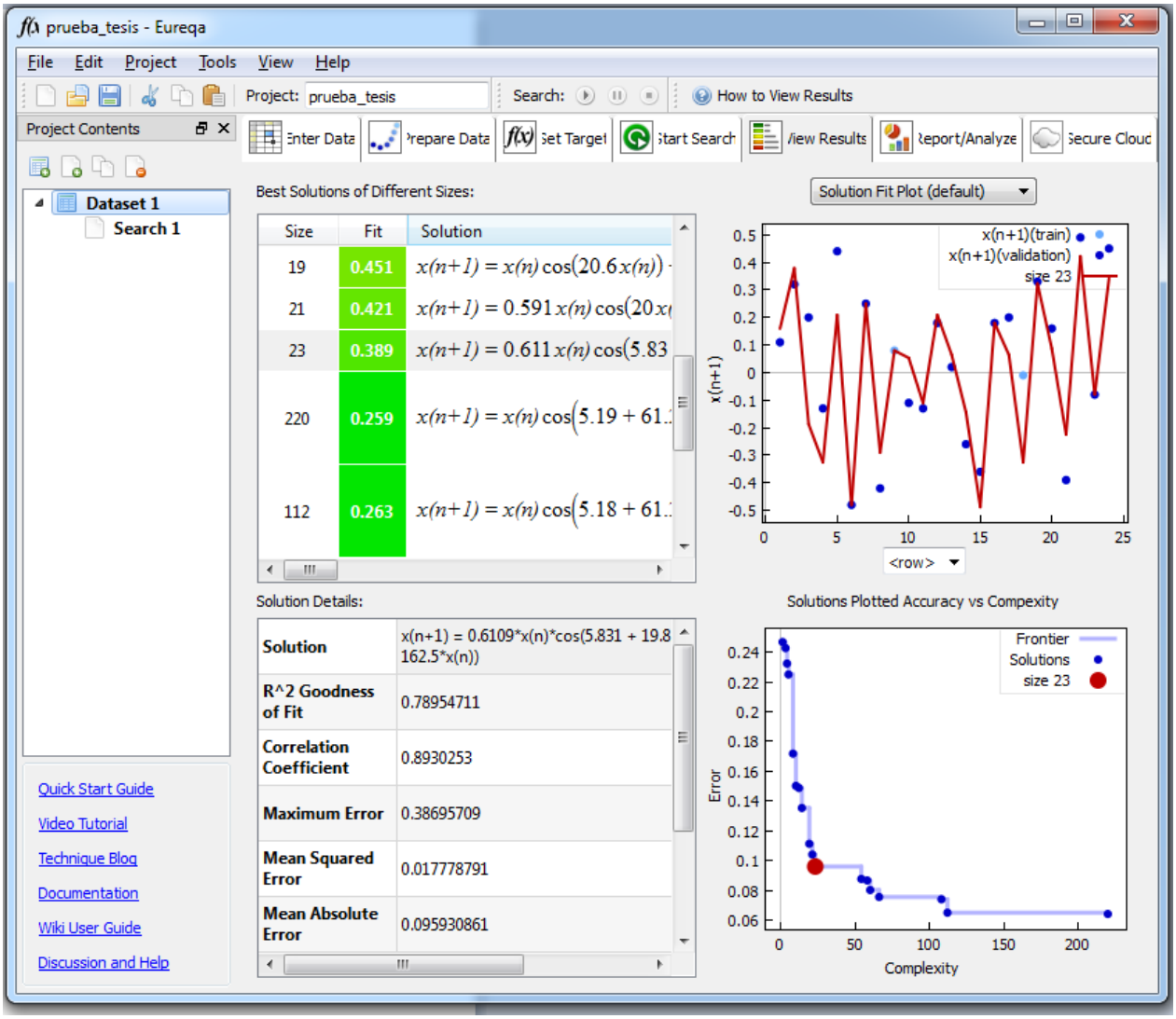


Figura 68: Resultados de búsqueda de solución de los datos introducidos por Eureqa.

En el paso 4 encontramos positivo el hecho de que la autocorrelación solo nos da presencia en el valor de 1, esto es que la señal obtenida no posee varios armónicos, su histograma presenta una distribución gaussiana y el exponente de Lyapunov es positivo al menos una vez. Todo esto para un proceso de $1'000,000$ de datos generados con la ecuación obtenida, recordando que para el cálculo del exponente de Lyapunov el número de datos tiene que tender a infinito (vease figura 69).

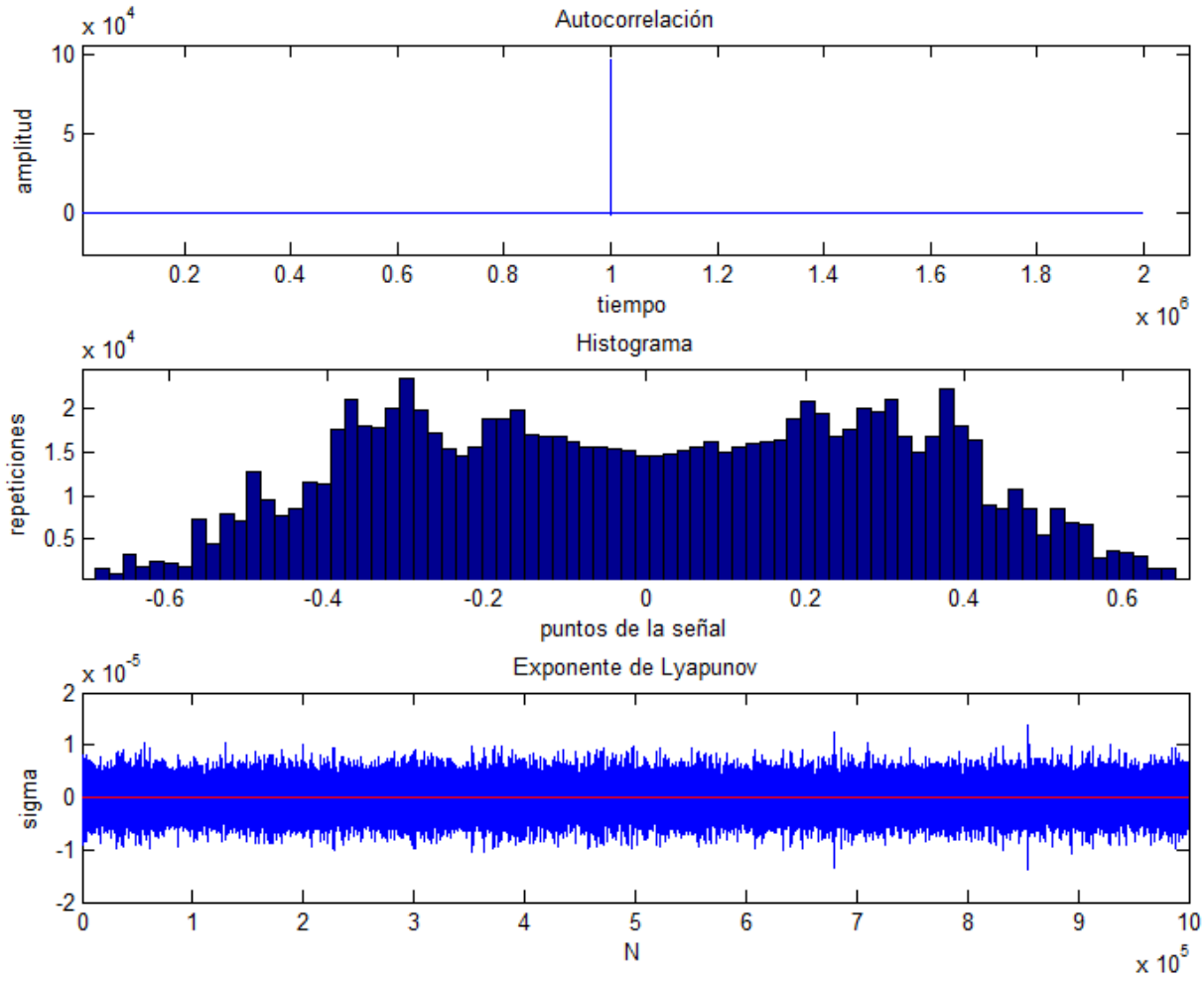


Figura 69: Autocorrelación, histograma y cálculo del exponente de Lyapunov de la ecuación 10.

7.9. Conclusión

La creación de nuevas ecuaciones caóticas es de suma importancia para aumentar las posibilidades de la criptografía caótica, el propósito principal de este capítulo es evidenciar la facilidad con la que una persona completamente ajena al area de criptografía caótica, o bien sistemas dinámicos, pueda crear sus propios algoritmos para encriptar información confidencial quebrantando el principio de Kerchoff, el cual dice que un criptosistema debe de ser seguro inclusive si se sabe todo acerca de este, excepto la clave [Kerckoff A. 1883], esto es, solo el usuario conocería su propio algoritmo y por tanto sería aún mas segura la información confidencial. Al crear estas nuevas ecuaciones caóticas podemos hacer pruebas con ellas y

evaluar su desempeño comparándolas con otros sistemas ya estudiados.

Referencias

[Abdullah Sharaf 2011] Abdullah Sharaf Alghamdi, Hanif Ullah, Muhammad Usama Khan, Iftikhar Ahmad and Khalid Alnafajan, Satellite Image Encryption for C4I System,International Journal of the Physical Sciences Vol. 6(17), pp. 4255-4263, Septiembre de 2011.

[AES 2001] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, Noviembre de 2001.

[Amigó et al. 2007] J.M. Amigó, L. Kocarevb, J. Szczepanski, Theory and practice of chaotic cryptography, Physics Letters A 366 211–216, 2007.

[Arunkumar et al. 2008] S.Chandramathi, K.V. Arunkumar, S.Deivarayan and P.Sendhilkumar,Fuzzy based Dynamic WEP keymanagement for WLAN Security Enhancement, Communication Systems Software and Middleware and Workshops, 2008.

[Behnia et al. 2007] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan,A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,Physics Letters A 366, 391–396, 2007.

[Blackledge 2011] Jonathan Blackledge, Cryptography and Steganography: New Algorithms and Applications, Center for advances studies, Varsaw Poland, 2011.

[Chen 2001] Chen, L. An open-plus-closed-loop control for discrete chaos and hyperchaos. Physics Letters A, 281(5): 327 – 333, 2001.

[Chong Fu et al. 2011] Chong Fu, Bin-bin Lin, Yu-sheng Miao, Xiao Liu, Jun-jie Chen, A novel chaos-based bit-level permutation scheme for digital image encryption, Optics Communications 284, 5415–5423, 2011.

[Chong Fu et al. 2012] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy,Optics Express, Vol. 20, Issue 3, pp. 2363 - 2378, 2012.

[Cruz et al. 2010] C. Cruz-Hernández, E. Inzunza-González, R.M. López-Gutiérrez H. Serrano-Guerrero, and E.E.García-Guerrero, Encrypted audio communication based on

synchronized unified chaotic systems, World Academy of Science, Engineering and Technology 42, 2010.

[DES url] Break DES in less than a single day, http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html

[DES url 2] Has DES been broken? http://www.rsa.com/rsalabs/node.asp?id=2227

[DES url 3] http://www.rsa.com/rsalabs/node.asp?id=2227

[Dongming et al. 2012] Dongming Chen, Deding Qing, Dongqi Wang, AES Key Expansion Algorithm Based on 2D Logistic Mapping, Fifth International Workshop on Chaos-fractals Theories and Applications, 2012.

[Edward Ott 1993] Edward Ott, Chaos in dynamical systems, Editorial CAMBRIDGE UNIVERSITY PRESS, Estados Unidos de América, 1993.

[Eureqa 2013] http://creativemachines.cornell.edu/eureqa

[F. Zamora et al. 2013] F. Zamora-Arellano, E. E. García-Guerrero, E. Inzunza-González, and A. Flores-Vergara, Application of Steganography and Chaotic Encryption to Send a Safety Text Message by Email, World Academy of Science, Engineering and Technology 76, Paris, Abril de 2013.

[Fernández S. 2004] Santiago Fernández,la criptografia clásica, Revista sigma 24, Abril de 2004.

[Ferreira 2008] Ferreira, J. C. V. Alfaomega grupo editor, S. d. C. (Ed.) Microcontroladores motorola-freescale Alfaomega, 2008.

[Gisin et al. 2002] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland,Reviews of modern physics, Volume 74, Enero de 2002.

[Hong-Li An et al. 2009] Hong-Li An, Yong Chen, The function cascade synchronization scheme for discrete-time hyperchaotic systems, Commun Nonlinear Sci Numer Simulat 14, 1494–1501, 2009.

[Huang 2011] Xiaoling Huang, Image encryption algorithm using chaotic Chebyshev generator, Springer Science Business Media B.V. 2011.

[IEEE 2008] IEEE Computer Society. IEEE Standard for Floating-Point arithmetic. In: IEEE std 754 – 2008, New York,1–58, 2008.

[Inzunza 2013] Everardo Inzunza González, Encriptado caótico en sistemas biométricos, tesis de doctorado, Universidad Autónoma de Baja California 2013.

[Inzunza et al. 2009] E. Inzunza-Gonzalez, C. Cruz-Hernandez, R. M. Lopez-Gutierrez, E. E. Garcia-Guerrero, L. Cardoza-Avendaño, H. Serrano-Guerrero, Software to Encrypt Messages Using Public-Key Cryptography, World Academy of Science, Engineering and Technology 54, 2009.

[Inzunza et al. 2013] E. Inzunza-González, C. Cruz-Hernández, Double Hyperchaotic Encryption for Security in Biometric Systems, Nonlinear Dynamics and Systems Theory, 13 (1), 55–68, 2013.

[Ivancevic et al. 2008] Vladimir G. Ivancevic, Tijana T. Ivancevic, Complex nonlinearity, Editorial Springer pp 1-171(Basics of Nonlinear and Chaotic Dynamics), 2008.

[Jain et al. 2002] Jain, A. K., Uludag, U., Rein-Lien Hsu, Hiding a face in a fingerprint image, Pattern Recognition. Proceedings 16th International Conference, Vol.3, pp. 756 - 759, 2002.

[Jain et al. 2003] Jain, A. K., Uludag, U., Hiding Biometric Data, IEEE Transactions On Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, pp. 1494 - 1498, Noviembre 2003.

[Kerckoff A. 1883] A. Kerckhoff, La cryptographie militaire, Journal des Sciences Militaires, Vol. IX, pp.583, January 1883, pp. 161191, February 1883.

[Kevin M. Cuomo 1993] Kevin M. Cuomo, Alan V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, Physical review letters, Volume 71, number 1, 5 de julio de 1993.

[Kuldeep Singh 2011] Kuldeep Singh, Komalpreet Kaur, Image Encryption using Chaotic Maps and DNA Addition operation and Noise Effects on it, International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, Junio de 2011.

[Lawrence 1998] Ernest Lawrence Rossi, The Feigenbaum scenario as a model of the limits of conscious information processing, BioSystems 46, 113–122, 1998.

[León-García 2008] León-García Alberto, Probability, Statistics, and Random Processes For Electrical Engineering, tercera edición, Prentice Hall 2008.

[Lehembre G. 2006] Guillaume Lehembre Seguridad Wi-Fi, WEP, WPA y WPA2, www.hakin9.org, hakin9 No 1/2006.

[Leonov 2013] Leonov G.A., Kuznetsov N.V. . Hidden attractors in dynamical systems. From hidden oscillations in Hilbert-Kolmogorov, Aizerman, and Kalman problems to hidden chaotic attractor in Chua circuits. International Journal of Bifurcation and Chaos 23 (1): art. no. 1330002. doi:10.1142/S0218127413300024, 2013.

[Liu et al. 2009] Shubo Liu, Jing Sun, Zhengquan Xu, An Improved Image Encryption Algorithm based on Chaotic System, JOURNAL OF COMPUTERS, VOL. 4, NO. 11, Noviembre de 2009.

[Louis Pecora et al. 1990] Louis M. Pecora and Thomas L. Carroll, Synchronization in Chaotic Systems, physical review letters, volume 64, number 8, 1990.

[M. Henon 1976] M. Henon . A two-dimensional mapping with a strange attractor. Communications in Mathematical Physics 50 (1): 69?77. Bibcode: 1976CMaPh..50...69H. doi: 10.1007/BF01608556. 1976.

[Martínez 2008] Martínez, J. M. A.; Martínez, I. A. y Ruíz, A. E. González, C. S. (Ed.) Microcontroladores PIC, Diseño práctico de aplicaciones 1era parte Mc Graw Hill, 2007.

[Mohan et al. 2010] Mohan Harshana Perera Ranmuthugala, Chandana Gamage, Chaos Theory Based Cryptography in Digital Image Distribution, International Conference on Advances in ICT for Emerging Regions (ICTer), 978-1-4244-9042-4/10, IEEE, 2010.

[Muhammad et al. 2007] Muhammad Khurram Khan, Jiashu Zhang, Lei Tian, Chaotic secure content-based hidden transmission of biometric templates, Chaos, Solitons and Fractals 32, 1749 – 1759, 2007.

[Municio 2008] Microcontrolador PIC16F84, Desarrollo de proyectos Ra-Ma Editorial, Municio, E. P.; Domínguez, F. R. y Pérez, A. (Ed.), 2009.

[Mustafa Ergen 2002] Mustafa Ergen, Department of Electrical Engineering and Computer Science, University of California Berkeley, Junio de 2002

[Patidar et al. 2011] Patidar Vinod, N.K. Pareekb, G. Purohita, K.K. Suda, A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption,Volume 284, Issue 19, Pages 4331 - 4339, Septiembre de 2011.

[Pei-Chen Lo et al. 1999] Pei-Chen Lo, Yu-Yun Lee, Real-time implementation of the moving FFT algorithm, Signal Processing 79, 251-259, 1999.

[Qi et al. 2008] Guoyuan Qi, Michaël Antonie van Wyk , Barend Jacobus van Wyk , Guanrong Chen. On a new hyperchaotic system. Physics Letters A 372, 124–136, 2008.

[R. Matthews 1989] R. Matthews. On the derivation of a "chaotic" encryption algorithm. Cryptologia, XIII(1):29 – 42, 1989.

[Richard Mollin 2001] Richard Mollin, an introduction to cryptography, editorial CHAPMAN HALL/CRC, Estados Unidos de América, 2001.

[Rosziati et al. 2011] Rosziati Ibrahim, Teoh Suk Kuan, Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application, 102-108, 2011.

[Sánchez 1999] Sánchez Arriazu Jorge, Descripción del algoritmo DES (Data Encryption Standard), Diciembre de 1999.

[Sahmoud et al. 2013] Shaaban Sahmoud, Wisam Elmasry and Shadi Abudalfa, Department of computer engineering, Islamic University of Gaza. International Arab Journal of e-Technology, Vol. 3, No 1, Enero de 2013.

[Sakthidasan 2011] Sakthidasan Sankaran and B.V. Santhosh Krishna, A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images International Journal of Information and Education Technology vol. 1, no. 2, pp. 137 - 141, 2011.

[Santosa 2005] Santosa Rully Adrian, Paul Bao, Audio-to-Image Wavelet Transform based Audio Steganography,47th International Symposium ELMAR-2005,08-10 , Zadar, Croatia, Junio de 2005.

[Sato et al. 2011] Tomoaki Sato, Phichet Moungnoue, Masaaki Fukase, Compatible WEP Algorithm for Improved Cipher Strength and High-Speed Processing, Communication Systems Wireless Mobile Communications and Technologies Paper ID 1477, 2011.

[Sergey et al. 1998] Sergey V. Ershov, Alexei B. Potapov, On the concept of stationary Lyapunov basis, Physica D 118, 167-198, 1998.

[Shujun Li 2003] Shujun Li, Xuanqin Mou and Yuanlong, Chaotic Cryptography in Digital World: State-of-the-Art, Problems and Solutions 710049, P. R. China, Enero de 2003.

[Smarthphone 2013] http://elproyectodealejandro.wordpress.com/2012/07/18/los-smartphones-en-el-mundo-infografia/

[Trejo-Guerra 2009] R. Trejo-Guerra, E. Tlelo-Cuautle, C. Cruz-Hernández, C. Sánchez–López, Chaotic communication system using Chua's Oscillators Realized with CCII+s,International Journal of Bifurcation and Chaos, Vol. 19, No. 12 (2009) 4217–4226, Abril de 2009.

[Tsukaune et al. 2012] Tsubasa Tsukaune, Yosuke Todo, Masakatu Morii, Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation, Seventh Asia Joint Conference on Information Security, 2012.

[Wang et al. 2010] Ying Wang, Zhigang Jin, Ximan Zhao,Practical Defence against WEP and WPA-PSK Attack for WLAN, IEEE, septiembre de 2010.

[Wikileaks 2012] BBC News, Wikileaks revelations http://www.bbc.co.uk/news/world-11863274, Febrero de 2012.

[Xiang An et al. 2011] Xiang An, Zhi-Qing Lü, Fast analysis of electrically large electromagnetic scattering/radiation problems using the adaptive cross approximation with FFT,785–790, 2011.

[Zhu 2012] Congxu Zhu, A novel image encryption scheme based on improved hyperchaotic sequences,Optics Communications 285 29–37, 2012.

[Zoran et al. 2005] Zoran Duric, Michael Jacobs, Sushil Jajodia, Information Hiding: Steganography and Steganalysis, In: C.R. Rao, E.J. Wegman and J.L. Solka, Editor(s), Handbook of Statistics, Elsevier, Volume 24, Pages 171-187, 2005.