UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO ENSENADA

IMPLEMENTACIÓN DE CIFRADO CAÓTICO DE ELECTROCARDIOGRAMA EN SISTEMA EMBEBIDO PARA TELEMEDICINA SEGURA

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de

INGENIERO EN ELECTRÓNICA

presenta:

DANIEL MURILLO ESCOBAR

Ensenada, Baja California, México, Septiembre de 2018.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO ENSENADA

IMPLEMENTACIÓN DE CIFRADO CAÓTICO DE ELECTROCARDIOGRAMA EN SISTEMA EMBEBIDO PARA TELEMEDICINA SEGURA

TESIS

Que para obtener el grado de Ingeniero en Electrónica presenta:

DANIEL MURILLO ESCOBAR

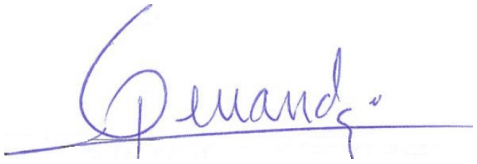
Aprobada por el siguiente comité:

Dr. Miguel Ángel Murillo Escobar
Director del comité

Dra. Rosa Martha López Gutiérrez
Miembro del comité

Dr. Fausto Abundiz Pérez
Miembro del comité

Dr. José Antonio Michel Macarty
Miembro del comité



Dr. César Cruz Hernández
Miembro del comité

Ensenada, Baja California, México. Septiembre de 2018.

RESUMEN de la tesis de **Daniel Murillo Escobar**, presentada como requerimiento para obtener el grado de INGENIERO en ELECTRÓNICA, del programa de Licenciatura de la Universidad Autónoma de Baja California. Ensenada, Baja California, México, Septiembre de 2018.

IMPLEMENTACIÓN DE CIFRADO CAÓTICO DE ELECTROCARDIOGRAMA EN SISTEMA EMBEBIDO PARA TELEMEDICINA SEGURA

Resumen aprobado por:

Dr. Miguel Ángel Murillo Escobar
Director de tesis

En este trabajo de tesis de licenciatura, se diseña e implementa en un sistema embebido, un algoritmo criptográfico basado en caos para brindar confidencialidad a señales de electrocardiograma (ECG) para aplicaciones en telemedicina segura.

Se analizan seis mapas caóticos y se determina utilizar el mapa 2D Seno-Logístico en el algoritmo criptográfico, ya que es un mapa hypercaótico con solo 2 dimensiones, presenta un rango caótico más amplio, genera tiempo de respuesta más rápido, posee mejor ergodicidad y tiene costo de implementación bajo. Además, se realiza una mejora al mapa para obtener mayores propiedades de aleatoriedad y aumentar la seguridad.

Finalmente, el cifrado caótico propuesto se implementa en un sistema embebido basado en un microcontrolador de 32 bits, pantalla de cristal líquido (LCD), botones de presionar y fuente de alimentación, donde la señal clara de ECG es introducida mediante software. El sistema criptográfico es sometido a distintos análisis de seguridad como espacio de claves, sensibilidad a clave secreta, sensibilidad a señal clara, histogramas, correlación, entropía de la información y tiempo de encriptado. Los resultados muestran que el algoritmo de cifrado caótico propuesto es resistente a este tipo de ataques y puede ser aplicado en telemedicina segura a un bajo costo de implementación.

Palabras clave: caos, telemedicina, cifrado caótico, microcontrolador, mapa 2D Seno-Logístico, análisis de seguridad.

Abstract of the thesis presented by **Daniel Murillo Escobar**, as a requirement to obtain the degree in ELECTRONICS ENGINEER, of the program of the Autonomous University of Baja California. Ensenada, Baja California, Mexico, September 2018.

IMPLEMENTATION OF CHAOTIC CIPHER OF ELECTROCARDIOGRAM IN EMBEDDED SYSTEM FOR SECURE TELEMEDICINE

Abstract approved by:

Dr. Miguel Ángel Murillo Escobar
Thesis director

In this thesis work, a cryptographic algorithm based on chaos is designed and implemented in an embedded system to provide confidentiality to electrocardiogram (ECG) signals for applications in secure telemedicine.

Six chaotic maps are analyzed and the 2D Seno-Logistic map is chosed for the criptographic algorithm, since it is a hypercaotic map with only 2 dimensions, it presents a wider chaotic range, it generates faster response time, it has better ergodicity and it has low implementation cost . In addition, an improvement is made to the map to obtain greater randomness properties and increase the security.

Finally, the proposed chaotic encryption is implemented in an embedded system based on a 32-bit microcontroller, liquid crystal display (LCD), push buttons and power supply; where the plain signal ECG is introduced by software. The cryptogram is subjected to different security analyzes such as key space, secret key sensitivity, clear signal sensitivity, histograms, correlation, information entropy and encryption time. The results show that the proposed chaotic encryption algorithm is resistant to this type of attacks and can be applied in secure telemedicine at low cost of implementation.

Keywords: chaos, telemedicine, chaotic encryption, microcontroller, 2D Seno-Logistic map, security analysis.

A mi familia

Agradecimientos

A mis padres, Miguel Ángel y María Rosario. Por brindarme su apoyo y amor incondicional durante toda mi vida.

A mis hermanos, Miguel, Yahaira, Angelina y Araceli. Especialmente a mi hermano Miguel por guiarme en un buen camino, estar siempre a mi lado apoyándome y por sus consejos que me han sido de gran ayuda en mis decisiones.

A mis sobrinos, Milton, David, Sofía y Ximena. Por darme alegría cada día.

A mi novia, Diana. Por estar siempre apoyándome en todo lo que hago en los últimos años. Por su amor y paciencia que me llena de felicidad.

Al Dr. César Cruz Hernández, por todo el apoyo brindado. Permitir aprender de él y aceptarme como tesista.

A la Dra. Rosa Martha López Gutiérrez, por todo su cariño y apoyo brindado durante toda el tiempo que realice mis estudios. Por la invitación a la realización de este trabajo y su ayuda cuando la necesitaba.

A mi comité de tesis, por sus consejos y comentarios para la mejora de este trabajo.

A mis amigos, Alexis, Atondo, Loya, Alma, Carlitos, Riaño y José. Por su amistad y el apoyo que me brindaron cuando lo necesité.

A la Universidad Autónoma de Baja California, por brindarme un espacio íntegro donde realizarme profesionalmente. En especial a la Facultad de Ingeniería, Arquitectura y Diseño Ensenada (FIAD) por ser mi casa de estudios los últimos 4 años y brindarme espacios donde trabajar.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT), por el apoyo económico brindado para la realización de este trabajo a través del Proyecto de Grupos de Investigación en Ciencia Básica, Referencia 166654.

Ensenada, B.C., México.
Septiembre de 2018

Daniel Murillo Escobar

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Capítulo 1

Introducción

Con el avance de la tecnología, particularmente en el campo de la *telemedicina*, se transmite una gran cantidad de información personal y médica todos los días, gracias a la capacidad del computador para comunicarse con otros dispositivos remotos mediante internet, el cual se considera inseguro por lo que, surge la necesidad de brindar confidencialidad a dicha información. Si la información no está debidamente protegida cuando se realiza el proceso de transmisión remota o almacenamiento de datos en telemedicina, puede generar riesgos e incertidumbre como fraudes, robo de identidad, diagnósticos incorrectos, entre otros.

La telemedicina hace posible realizar de forma remota varios procedimientos médicos y clínicos como: exámenes, diagnósticos y supervisión de tratamientos. Utiliza recursos teleinformáticos como computadores, servidores, equipos de procesamiento de imágenes, internet, equipos de transmisión y recepción de información.

Por medio de una red de internet se puede transmitir y recibir información entre doctor y paciente (ver figura 1.1). Así se puede intercambiar opiniones o dar una consulta a distancia sin necesidad de contar con presencia física del paciente.

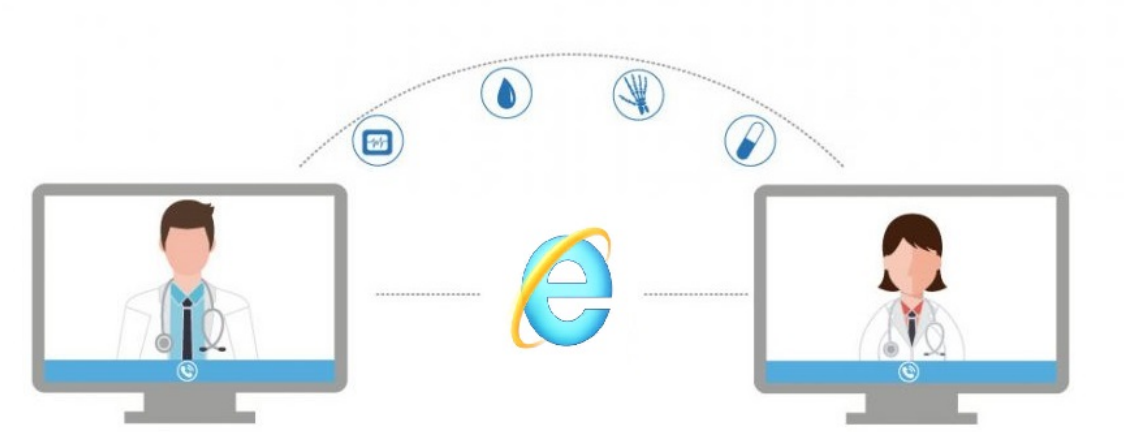


Figura 1.1: Telemedicina: medicina a distancia.

Una red de telemedicina, por lo general está compuesta por pacientes, centros de salud y médicos especialistas, equipos de comunicaciones y medios de transmisión. Una aproximación a este tipo de redes se muestra en la figura 1.2, donde se detalla de manera muy general, los principales componentes de una red de telemedicina. Esta red cuenta con servidores que permiten implementar aplicaciones médicas [1].

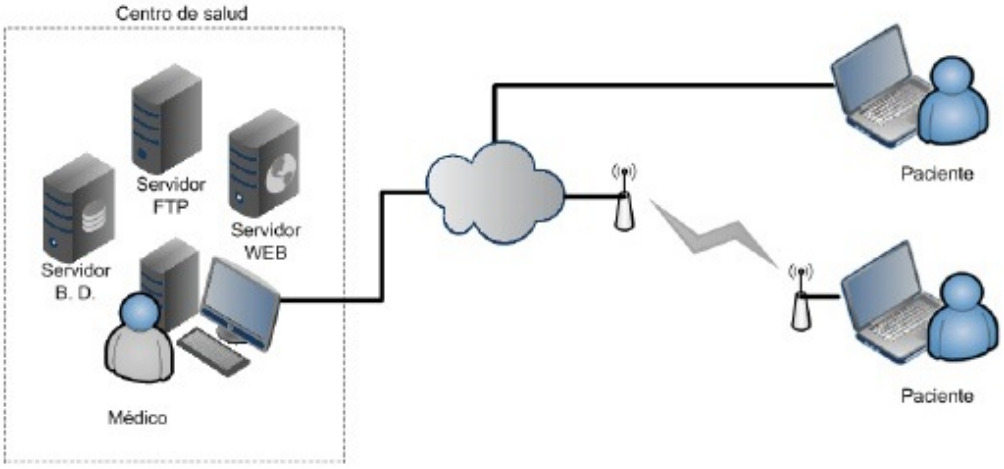


Figura 1.2: Red de telemedicina.

Una red de telemedicina se caracteriza por contar con información. Esta tiene la finalidad de enviar datos mediante una red de comunicación definida por una tecnología en particular (4G, GSM, Internet, etc.). Estos datos se almacenan en un servidor y son accedidos por el especialista médico, para analizar los datos almacenados y al final, dar un diagnóstico [2, 3].

Por otra parte, la *criptografía* es el arte o técnica para escribir datos enigmáticamente mediante claves y protegerlos de otro usuario no autorizado. Un dispositivo de encriptado puede almacenar los datos localmente en una memoria y posteriormente enviarlos mediante un canal inseguro. Esta técnica constituye una opción de seguridad muy útil, ya que proporciona confidencialidad a los datos.

Hoy en día, se utilizan distintos métodos criptográficos conocidos como criptografía convencional y que son aceptados como estándar en EUA. El algoritmo AES (Advanced Encryption Standard) es uno de los algoritmos más seguros que existen hoy en día. Está clasificado por la National Security Agency (NSA), para la más alta seguridad de la información secreta. Se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces. El algoritmo 3DES (Triple Data Encryption Standard), se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES; se basa en aplicarlo tres veces, con tres claves distintas, por lo que resulta mucho más seguro [4].

Por otra parte, se tiene la criptografía no convencional que se basa en herramientas matemáticas en estado de investigación como la criptografía caótica. El *caos* en matemáticas y otras ciencias, es adjudicado a los fenómenos que presentan sistemas dinámicos discretos y continuos no lineales, con comportamiento determinísticos y que poseen propiedades como la alta sensibilidad a condiciones iniciales y a parámetros de control, mezcla de datos, entre otros, lo que hace del caos muy efectivo para el cifrado de información y además cuenta con distintas aplicaciones en ingeniería [5].

El criptoanálisis es la ciencia que se ocupa de corromper un sistema criptográfico y determinar el mensaje original a partir del mensaje cifrado o de la clave de cifrado [6]. Para ello, se utilizan análisis matemáticos y estadísticos que se conocen como ataques criptoanalíticos. Por tanto, un sistema criptográfico debe resistir los distintos ataques criptoanalíticos conocidos en la actualidad para que se considere seguro criptográficamente.

Este trabajo se basa en encriptado caótico digital, donde los valores de *condiciones iniciales* y *paramentos de control* de los sistemas caóticos constituyen la clave secreta, de tal forma que la dinámica caótica generada en el transmisor y receptor son idénticas.

1.1. Motivación

Con el avance de la tecnología, la seguridad y confiabilidad en redes de telemedicina, son aspectos relevantes para el almacenamiento y transmisión de información médica de pacientes. Analizar estos dos aspectos, previene amenazas y ataques a los sistemas de telemedicina. En un sistema de telemedicina como en muchos sistemas, una falla particular puede causar la caída del sistema por completo, como ocurrió en 2011 en el Midstate Medical Center, Estados Unidos. El caso se presentó cuando una empleada quiso trabajar desde su casa y al utilizar la red de la institución dejo vulnerable a la red y se transfirió información confidencial de más de 93,500 pacientes. La información incluía datos privados, como nombres, dirección e información médica [7].

En general, las amenazas y ataques sobre una red de datos obligan a establecer parámetros para prevenir o mitigar estas falencias, por medio de regulaciones y estándares. Por esta razón, surge la necesidad de implementar medidas de seguridad y en este trabajo de tesis, se realizará con el cifrado caótico de señales biomédicas. Los sistemas caóticos tienen muchas propiedades interesantes como ergodicidad, alta sensibilidad a condiciones iniciales, alta sensibilidad a parámetros de control, mezcla de datos, no linealidad, etc. Debido a la estrecha relación entre caos y criptografía [8], existe un gran interés científico de construir esquemas de comunicación segura con el uso de caos, para proteger información y evitar robo o acceso ilegal a la información en su transmisión o en su almacenamiento y particularmente realizar el encriptado caótico de señales de electrocardiogramas para la protección de datos en aplicaciones de telemedicina.

La información médica que se maneja en telemedicina es en general de tipo confidencial y por lo tanto, requiere resguardarse de ataques y amenazas que puedan afectar el derecho a la intimidad, la privacidad y la protección de los datos de los pacientes [9]. Todas las redes de datos son vulnerables a ataques que buscan provocar el colapso de los sistemas y sustraer datos privados. Estos ataques pueden afectar los datos mediante técnicas de hurto de información, como lo son los programas espía, los virus y los troyanos, el acceso no autorizado a la información, la alteración o deterioro total o parcial de la misma. En el caso particular de las redes de telemedicina, éstas pueden ser atacadas por el aprovechamiento de sus vulnerabilidades, entre las cuales, se destacan la falta de sistemas de seguridad informática, sistemas inestables de autenticación, fallos en los procedimientos de transmisión o almacenamiento de la información y manejo inadecuado de la información por parte del personal encargado [10].

1.2. Objetivos y alcances de la tesis

Debido al interés de resguardar la información de forma confidencial en telemedicina, surge la realización de este trabajo de tesis de licenciatura en la que se plantea alcanzar el siguiente *objetivo general*:

Diseñar e implementar un algoritmo de cifrado caótico para señales de electrocardiograma en sistema embebido para telemedicina segura.

Que para cumplir con el objetivo general, se plantea alcanzar los siguientes *objetivos particulares*:

1. Determinar el mapa caótico a utilizar en función de sus características de aleatoriedad y procesamiento.
2. Diseñar un algoritmo de cifrado caótico para señales de ECG.
3. Implementar el algoritmo criptográfico en un sistema embebido basado en microcontrolador de 32 bits para aplicaciones en telemedicina.
4. Determinar la seguridad criptográfica y eficiencia.

1.3. Organización del manuscrito

Este trabajo está compuesto por 8 capítulos, los cuales se describen a continuación:

- **Capítulo 1**: Se presenta la introducción de este trabajo, la motivación y los objetivos.
- **Capítulo 2**: Se introduce a la telemedicina y se dan a conocer algunas de sus características y funciones.

- **Capítulo 3**: Se estudian seis mapas caóticos, sus propiedades y se determinar el mapa caótico a utilizar para el algoritmo de cifrado.
- **Capítulo 4**: Se presentan los datos más relevantes de la criptografía y sus características.
- **Capítulo 5**: Se explica brevemente lo que es un sistema embebido, así como algunas características del sistema que se utiliza.
- **Capítulo 6**: Se presenta el algoritmo de cifrado caótico propuesto para señales de electrocardiograma (ECG).
- **Capítulo 7**: Se implementa el algoritmo de cifrado caótico propuesto en un sistema embebido basado en un en microcontrolador de 32 bits para aplicaciones en telemedicina y se realiza un análisis de seguridad criptográfico.
- **Capítulo 8**: Se presentan las conclusiones de este trabajo y trabajo a futuro.

Capítulo 2

Telemedicina

En este capítulo, se presenta una breve cronología de la telemedicina, así como su definición y clasificación; también se muestran los tipos, ventajas y desventajas de la telemedicina.

2.1. Introducción

El prefijo *"tele"* deriva del griego *"distancia"*, por lo tanto, *telemedicina* es *medicina a distancia*, es decir, la prestación de cuidados médicos y el intercambio de información médica a través de la distancia. La telemedicina implica la transferencia de información acerca de temas relacionados con la salud entre uno o más lugares [11]. En la actualidad, las tecnologías de la información y las comunicaciones se han combinado para dar como resultado la telemedicina, a fin de brindar asistencia médica a quien la requiera en sitios distantes. La telemedicina busca mejorar la salud de un paciente, permitiendo la comunicación interactiva entre el paciente y el médico a distancia (ver figura 2.1).

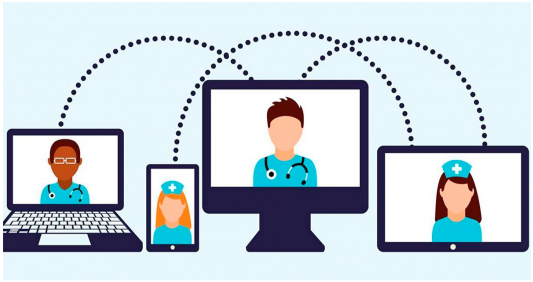


Figura 2.1: Comunicación entre doctor y paciente.

La telemedicina se ha considerado una disciplina científica a medio camino entre la medicina y la tecnología. De esta forma, a lo largo de la última década ha estado influenciada en gran medida por el incesante desarrollo de las tecnologías de la información y las comunicaciones [12]. Desde el punto de vista técnico, la esencia de un sistema de telemedicina es la provisión de servicios multimedia en red para asistencia sanitaria, involucrando la transferencia de audio, vídeo, imágenes fijas, gráficos, datos y textos

entre lugares distantes comunicando pacientes y médicos.

La comunicación a distancia entre dos o más personas puede establecerse en tiempo real o en diferido. Lo mismo sucede con la comunicación entre médicos mediante sistemas de transmisión de información.

En [13], se mencionan dos modos de operación básicos, los cuales son:

1. **En tiempo real o modo síncrono**. Usa el sistema de teleconferencia o videoconferencia (ver figura 2.2) en el que se une la imagen y el sonido para que dos o más personas tengan la posibilidad de comunicarse entre sí en tiempo real. En este caso, la imagen clínica suele ser una imagen de vídeo y tanto el paciente como el médico consultado están presentes físicamente.

2. **En tiempo diferido o modo asíncrono**. También conocido como *almacenar y enviar*. Utiliza el sistema de correo electrónico (ver figura 2.3). En general, el médico consultado recibe un mensaje con una historia clínica, la estudia y emite por correo electrónico su opinión diagnóstica y su consejo terapéutico. No es preciso que el médico consultor y el paciente coincidan en el tiempo con el médico consultado.

Figura 2.2: Comunicación: Sincrónica (Videoconferencia).

Figura 2.3: Comunicación: Asincrónica (Correo electrónico, WEB).

Ambos escenarios se pueden implementar en la realización de este trabajo de tesis. Actualmente es posible adaptar cualquier instrumento médico a un sistema de telemedicina y son múltiples las especialidades que han incorporado la telemedicina a su campo de actuación.

En forma general, un sistema de telemedicina es una estructura compleja cuya estructura y modo de operación depende mucho de la aplicación concreta. Incluye equipos terminales para captación de señales biomédicas, captadores de imágenes, terminales informáticos, estaciones de trabajo, sistemas de videoconferencia, infraestructuras de comunicación, servicios genéricos y servicios específicos.

2.2. Desarrollo histórico

A la fecha, se desconoce con exactitud cuándo se empezó a hablar de telemedicina; sin embargo, se puede decir que surge aproximadamente desde 1960. Los trabajos de Bashur y sus colegas en los 70's son los más mencionados [14, 15].

En épocas antiguas, lo más importante en la medicina era tener acceso físico a un médico que pudiera dar una respuesta a determinadas enfermedades. Las distancias eran grandes, los medios de comunicación y transporte muy lentos. El creciente desarrollo cultural dio oportunidad de estudiar a muchos más individuos y el avance tecnológico creó medios de enlace cada día más rápidos. Con el advenimiento de la máquina de vapor, el telégrafo y luego la telefonía, el mundo se hacía cada vez más pequeño y las posibilidades de acceso a los servicios médicos era cada vez mucho mayores. Luego, las ciencias médicas se especializaron más, la tecnología irrumpió con sus avances y el contacto con un especialista en otra ciudad se hizo un requerimiento cada vez más frecuente. La radiotelefonía, la televisión, las técnicas de diagnóstico por imágenes y el uso de satélites para encauzar esas señales, fueron pasos fundamentales para una nueva medicina que necesita cada día menos presencia física.

A continuación se muestra la historia de la telemedicina cronológicamente [16]:

- **Años cincuenta**:
  La telemedicina se difundió mediante circuitos cerrados de televisión en los congresos de medicina, con conferencias o presentaciones de los principales procedimientos quirúrgicos, estos eventos eran patrocinados por compañías farmacéuticas.

  En **1950**. Holter, Gengerelli y Glasskock, investigan la obtención de parámetros biológicos y consiguen recibir por radio el electrocardiograma de personas que deambulaban por la calle a considerable distancia de la estación receptora.

  En **1955**. En Montreal, el Dr. Albert Jutras realiza teleradiología, a fin de evitar las altas dosis de radiación que incidían en los fluoroscopios.

En **1959**. Se consigue transmitir por primera vez imágenes radiológicas a través de la línea telefónica.

- **Años sesenta**:
  Al principio de los sesenta, la NASA (Nacional Aeronautics and Space Administration) y el servicio de salud pública de Estados Unidos empezaron a proporcionar cuidados sanitarios en zonas remotas a personas que vivían en la reserva india de Papago en Arizona, utilizando personal paramédico y habitáculos médicos como: Rayos X y ECG, conectados por satélites.

  En **1967**. Se estableció una conexión con microondas e imágenes en blanco y negro entre el aeropuerto de Boston y el hospital de Massachusetts con el fin de atender las urgencias del aeropuerto de forma más accesible.

- **Años setenta**:
  En los años 70, la carrera espacial había dado sus frutos y existían varios satélites de comunicaciones que permitían la trasmisión de señales a grandes distancias.

  En **1971**. Se eligieron 26 lugares de Alaska para comprobar si las comunicaciones podrían mejorar la salud de los pueblos. Se utilizó el satélite I de la NASA que fue lanzado en 1966, donde se realizó la transmisión de televisión a blanco y negro. Se determinó que el uso de vídeo a distancia aportaba beneficios en algunos casos que no eran de urgencias, debido a que los casos de urgencias no podían esperar a la agenda de consultas planificadas de acuerdo a la disponibilidad del satélite.

  En **1972**. *Space Technology Applied to Advanced Health Care*, fue una de las primeras aventuras de la telemedicina y sus objetivos fueron dar atención médica a los astronautas en el espacio. En esta experiencia se utilizó una furgoneta cargada con equipos médicos y un par de enlaces de microondas para la transmisión de las señales y el sonido hasta el hospital donde estaban los especialistas.

- **Años ochenta**:
  Casi ninguno de los programas de las décadas de los 60's, 70's y 80's consiguió mantenerse por sí solo. La década de los ochenta dio lugar a muchos proyectos y aparecía la era de las autopistas de la información.

  En **1984**. Se realizó un proyecto piloto en Australia para probar una red experimental por satélites (Q-Network) y se dio servicio a cinco ciudades apartadas. Los servicios incluían telefonía, fax, transmisión de imagen fija y receptores de televisión. Se demostró que ciertos costos se redujeron y que fueron necesarias menos evacuaciones por motivos de emergencia.

En **1986**. La clínica Mayo instaló un sistema dedicado basado en satélites para unir las clínicas de Rochester, Jacksonville y Scottsdale. El sistema permite una comunicación de vídeo con una tasa completa de imágenes.

- **Años noventa**:
  Se produce el verdadero crecimiento y desarrollo de la telemedicina, con el florecimiento de las redes de telecomunicaciones, internet y con la aparición de las principales aplicaciones de la telemedicina (telerradiología, telepatología, telederматología). Esta década supone la gran proliferación de experimentos de telemedicina, muchos de ellos con un objetivo de continuidad y rentabilidad.

  En **1991**. La escuela de medicina de la Universidad de Carolina del Este se conecta con la mayor prisión de Carolina del Norte, eliminando costos de ambulancia y traslado de presos.

  En **1994**. La escuela de medicina de la Universidad de Carolina del Este crea la primera instalación dedicada al uso de telemedicina, consistiendo en cuatro salas de teleconsulta diseñadas específicamente para ese fin.

  En **1998**. Se realiza en España la primera experiencia de telecirugía con robots. Los cirujanos estaban en un barco operando a un paciente situado a cientos de kilómetros.

- **Años 2000**:
  Con el avance tecnológico se desarrollan nuevos tipos derivados de la telemedicina.

  En **2001**. El doctor Marescaus desde New York, elimina la vesícula enferma de un paciente de 68 años en Estrasburgo, Francia, por medio de un brazo robot. Se observa el vínculo de la telemedicina con incipientes avances de la robótica.

Figura 2.4: El cirujano Marescaux a los mandos del robot en Nueva York.

En **2005**. Se realizan las primeras pruebas para seguimiento de patologías crónicas, diabetes e hipertensión por medio de un celular.

En **2010**. Adrián Carbajal, médico cirujano, se conectó mediante una computadora a un robot que estaba a 895 kilómetros de distancia. Carbajal, cirujano en robótica, es el mexicano que introdujo la telemedicina a México.

De acuerdo a toda la información recopilada, se observa ver que el fenómeno de la globalización ha permitido un avance en todos los campos, permitiendo que los accionares más cotidianos estén más inmiscuidos en el campo de la tecnología.

2.3. Tipos y características de la telemedicina

Con el pasar del tiempo, el número de servicios médicos y especialidades aumenta, se suplen distintas necesidades [17, 18]. Los servicios de telemedicina tienen la posibilidad de ser clasificados de diferente manera. Las posibles clasificaciones tienen características principales en común, pero pueden variar un poco en las especialidades consideradas. Por ejemplo, una clasificación por el tipo de información para transmitir (datos, audio o imágenes), por la tecnología usada, o el tipo de especialidades derivadas de los servicios en telemedicina [19].

El alcance de la telemedicina ha cambiado a medida que se desarrolla más tecnología. A continuación se describirán las principales áreas:

Teleconsulta. También llamada telediagnóstico, es la aplicación de las técnicas de telemedicina para hacer posible la comunicación e interacción entre los profesionales (ver figura 2.5) de la salud, con o sin la presencia del paciente, accediendo a la opinión y estableciendo un diagnóstico cooperativo a partir del intercambio de información clínica del paciente.

Figura 2.5: Teleconsulta entre varios doctores.

Teleeducación. Mediante el uso de infraestructuras y comunicaciones, especialmente el internet, se puede ofrecer al usuario aplicaciones que permiten el acceso a

información y a bases de datos. De esta forma, los sistemas de salud pueden utilizar herramientas de teleformación para el apoyo a la toma de decisiones, facilitar contenidos informativos y servicios para los ciudadanos independientemente de su localización.

Telemonitorización. También llamada teleasistencia, es el uso de las telecomunicaciones para la supervisión de pacientes. La tecnología hace posible conocer y realizar un seguimiento a distancia de la situación de un paciente y de sus parámetros vitales (ver figura 2.6), de esta manera permite la provisión de asistencia y cuidados de salud a los pacientes en su entorno habitual. Estos servicios permiten apoyar la atención a determinados grupos de pacientes con necesidades especiales, situados fuera del entorno hospitalario, como procesos crónicos, programas de cuidados paliativos, medicina de urgencias, etc. El sistema capta las señales biológicas del paciente (tensión arterial, trazado electrocardiográfico, oxigeno sanguíneo, glucemia, etc.) y las transmite en formato digital, hasta el centro sanitario o centro de control.

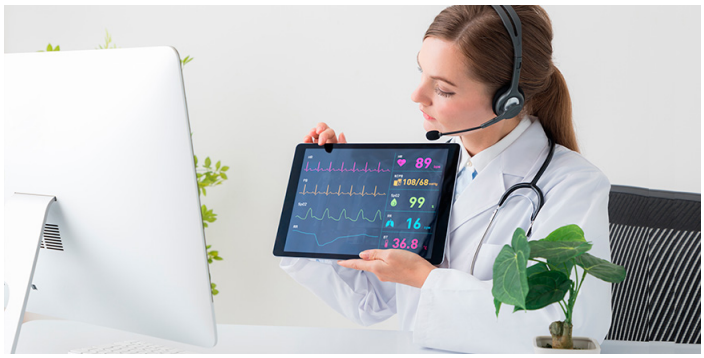


Figura 2.6: Telemonitorizacion: seguimiento a distancia de parámetros vitales.

Telecirugía. En términos simples, la telecirugía es aquella en la que el cirujano no tiene contacto físico directo con el paciente, por lo tanto se aplican las técnicas de telemedicina en conjunto con realidad virtual, robótica e inteligencia artificial para realizar apoyo y supervisión de procedimientos quirúrgicos.

En la tabla 2.1, se muestra en resumen los servicios y especialidades de la telemedicina.

Servicios	**Especialidades**
Teleconsulta	Registro clínico electrónico
Telediagnóstico	Teleendoscopía, Teledermatología, Teleoftamología
Teleterapia	Telepsiquiatría, Telefisioterapia, Teleprescripción
Telemetría	Teleradiología, Telepatología, Telecardiología

Tabla 2.1: Servicios de telemedicina y sus especialidades.

Pero para un correcto manejo de administración e información de la seguridad, la información médica, se debe establecer controles y procedimientos que la preserven ya que la telemedicina almacena y transmite mediante canales inseguros, información

personal de pacientes y médicos. Las diferentes regulaciones buscan mantener la confidencialidad, integridad y disponibilidad de la información médica.

La existencia de estándares regulatorios sobre el manejo de información médica, ha permitido que las entidades de salud alcancen mayores índices de confiabilidad en la transmisión de información. Dentro de los estándares más representativos, se destacan HIPAA y COBIT. Estos estándares establecen parámetros para preservar la regulación de transmisión de información.

A continuación, se hará una breve descripción de los dos estándares más importantes.

1. **HIPPA** (Ley de Transferibilidad y Responsabilidad de Seguros de Salud), es un conjunto de estándares que aseguran la protección de información médica en aspectos como la transmisión, almacenamiento y acceso a la información de salud. La primera parte especifica los requerimientos administrativos generales y la segunda, requerimientos de seguridad para la información médica, registro médico electrónico, fundamentos del análisis de riesgos de seguridad, gestión de riesgos y requerimientos para proteger de la información médica [20].

2. **COBIT** (Objetivos de Control para Información y Tecnologías Relacionadas), es un conjunto de mejores prácticas para seguridad, calidad, eficacia y eficiencia en las tecnologías de la información necesarias para identificar riesgos, gestionar recursos y medir el rendimiento que permitan alcanzar los objetivos de una organización [21].

Los beneficios de la telemedicina son claros y se han constatado a través de experiencias y aplicaciones en diversos países del mundo, aunque existen limitantes e inconvenientes, el principal riesgo es la privacidad de información del paciente.

En la tabla 2.2 se presentan las ventajas y desventajas de la telemedicina. Las desventajas son fáciles de solucionar y las ventajas que proporciona son de gran ayuda para todos aquellos que requieran del uso de la telemedicina.

Ventajas	**Desventajas**
Acorta las distancias	Relación médico-paciente limitada
Ahorra dinero	Puede ser impersonal
Tecnología al alcance de todos	La calidad de información puede ser insuficiente
Mejora el acceso a la educación	Depende de la tecnología
Acceso a sitios remotos	No es conveniente para niños pequeños

Tabla 2.2: Ventajas y desventajas de la telemedicina.

2.4. Seguridad en la telemedicina

Para poder establecer mecanismos de prevención y protección de la información en redes de telemedicina, se debe determinar las debilidades y defectos denominados como vulnerabilidades. En la figura 2.7, se muestra un esquema que permite ver que las amenazas en una red siempre están presentes y pueden afectar las aplicaciones sobre una red de telemedicina [22].

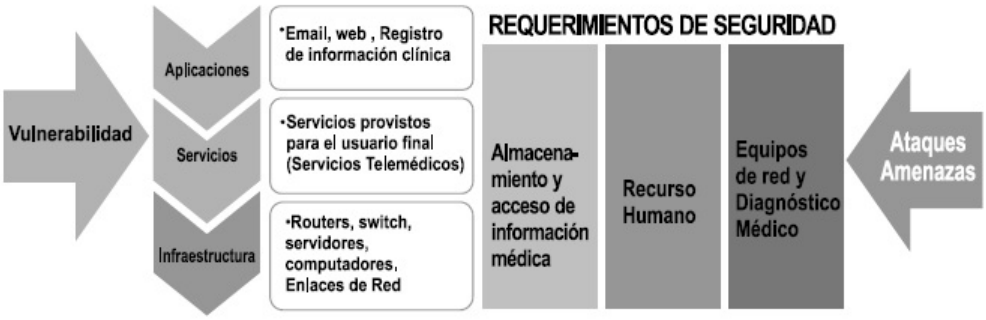


Figura 2.7: Vulnerabilidad en telemedicina.

El análisis de los riesgos a los que se expone la información en una red de telemedicina, permite determinar el alcance de los posibles daños en la integridad de la información médica.

Al igual que las redes de datos, las redes de telemedicina están expuestas a una gran cantidad de amenazas debidas a las vulnerabilidades del sistema. La presencia de vulnerabilidades y amenazas en la red, genera un riesgo asociado a la afectación total o parcial de la información. El riesgo puede definirse como el daño potencial causado por una amenaza que puede explotar las vulnerabilidades de un activo; el activo en el caso de la telemedicina, es la información médica que se maneja sobre la red.

El riesgo se determina por la presencia de una amenaza y al menos, una vulnerabilidad. Las amenazas se refieren a la probabilidad de ocurrencia de un evento que puede afectar el sistema en un tiempo dado y las vulnerabilidades se refieren a la magnitud de la intensidad de los daños sufridos frente al impacto de un evento [23].

La telemedicina promueve una mejor atención a los pacientes, brindando un diagnóstico rápido y eficiente. El uso de la informática y las telecomunicaciones en el área de la salud, debe estar acompañado de medidas de seguridad adecuadas para garantizar la confidencialidad, disponibilidad e integridad de la información médica, ofreciendo protección a los pacientes, los profesionales de la salud y al recurso humano en general.

La tecnología utilizada en las aplicaciones para la telemedicina, en ocasiones, es precisamente denominada tecnología impersonal [24], debido a la falta de confianza tecnológica por parte de los pacientes. Esto se refleja en la preocupación de la privacidad

y confidencialidad de la información, incluyendo factores propios del desarrollo de teleconsultas, como escuchar estas por casualidad por parte de terceros, la filmación de algunos procedimientos y su uso subsiguiente con propósitos educativos.

El rápido desarrollo tecnológico ha provocado un cambio sustancial haciendo que muchos médicos hayan pasado de usar ordenadores de sobremesa para su atención médica a hacerlo mediante pequeños dispositivos inteligentes. En 2015 el 70 % de los médicos usaban sus dispositivos móviles como sistemas embebidos para gestionar la ficha médica de sus pacientes hospitalizados, cuando en 2013 esta cifra era solo del 8 %. Esto implica que más médicos utilizan la tecnología de sistemas embebidos para resguardar y enviar información de forma no segura.

2.5. Conclusiones

En este capítulo, se introdujo a la telemedicina y se dio a conocer algunas de sus características. Se mencionó el tipo de comunicación en tiempo diferido y tiempo real, los cuales se utilizaran en este trabajo de tesis, ya que se almacenará la señal de electrocardiograma cifrada para que posteriormente pueda ser transmitida remotamente mediante canales públicos de forma segura y por otra parte, se podrá leer, encriptar y enviar un ECG en tiempo real.

En general, el uso de la telemedicina avanza rápidamente y podría representar una buena alternativa para complementar a muchos de los programas de salud que se ven alrededor del mundo, ya que facilita la toma de decisiones terapéuticas y diagnósticas en diferentes escenarios clínicos y complementa la formación académica en las escuelas de medicina. Sin embargo, aún existen barreras de infraestructura y confidencialidad de la información.

Capítulo 3

Caos

En este capítulo, se introduce al caos con una breve historia y se explica su definición desde un punto de vista físico-matemático. Se muestran los tipos de sistemas caóticos y sus propiedades. Se presentan seis mapas caóticos (sistemas caóticos), de los cuales, se obtendrá el exponente de Lyapunov para verificar dinámicas caóticas y seleccionar uno de ellos para el cifrado caótico de este trabajo de tesis.

3.1. Introducción

La *teoría del caos* es la denominación en las ciencias exactas, principalmente de física y matemáticas, que trata sobre comportamientos impredecibles en sistemas dinámicos no lineales (sistemas complejos que cambian o evolucionan con el estado del tiempo). La teoría del caos plantea que el mundo no sigue un patrón fijo y previsible, sino que se comporta de manera caótica y que sus procesos y comportamiento dependen, en gran manera, de circunstancias inciertas. Esto plantea que una pequeña variación en el sistema o en un punto del mismo puede provocar que en un lapso de tiempo a futuro, éste presente un comportamiento completamente diferente e impredecible. Esto sucede aunque estos sistemas son en rigor deterministas, es decir; su comportamiento puede ser completamente determinado conociendo sus condiciones iniciales.

Se utiliza la palabra caos para designar el desorden y la teoría que lo expresa se debe principalmente a Henri Poincaré y a Edward Lorenz. La teoría del caos, nacida en los años 60s, se define como "estudio de la incertidumbre y la impredictibilidad en las matemáticas y en la naturaleza". El objeto de estudio de la teoría del caos lo constituyen fenómenos dinámicos fuera de equilibrio de comportamiento no lineal. Esta teoría se utiliza en muchas disciplinas, pero uno de los sistemas caóticos más estudiados ha sido la atmósfera [25]. La teoría del caos explica que el resultado de algo depende de distintas variables y que es imposible de predecir.

El primer hallazgo de un sistema caótico fue revelado por Edward Lorenz (ver figura 3.1), un matemático y meteorólogo que trabajaba en el MIT. Todo ocurrió cuando una falla hizo que se detuviera la prueba en la que estaba trabajando. Edward en vez

de comenzar nuevamente los cálculos desde el principio, archivó algunos resultados intermedios del cálculo inicial del ordenador, para posteriormente cargarlos de nuevo con la intención de que el ordenador siguiera trabajando a partir del punto en que se había detenido [26].

Figura 3.1: Edward Lorenz.

Sorprendentemente, el resultado que consiguió de esta manera fueron distintos a la solución que había conseguido anteriormente realizando los cálculos de una sola vez. Lorenz se había topado por casualidad con el fenómeno de la sensibilidad a las condiciones iniciales, que hacía de su sistema algo en la práctica impredecible. Una pequeña variación en las condiciones iniciales ocasionaba estados completamente diferentes.

El fallo del ordenador al redondear los números, causaba una disparidad en la octava cifra decimal de los números destacados. Esto se convirtió en la primera señal de que los sistemas relevantes en la naturaleza, como los atmosféricos, pueden ser extremadamente sensibles a una minúscula alteración. Lorenz también denominó a este producto de los estados caóticos con el término efecto mariposa. El aleteo de una mariposa en Brasil puede ocasionar un tornado en Texas. Supongamos que una pequeña mariposa está posada sobre un árbol en una remota región del Amazonas. Mientras permanece posada, abre y cierra ocasionalmente sus alas por dos ocasiones. Podría haberlo hecho sólo una vez, pero en este caso ha batido sus alas exactamente dos veces. Como el sistema atmosférico es un sistema caótico, que exhibe dependencia sensible a las condiciones iniciales, la diminuta variación en los remolinos de aire contiguos a la mariposa puede acabar influyendo en que haya o no haya un tornado sobre Texas.

A este descubrimiento, Lorenz lo llamó *Dependencia sensitiva de las condiciones iniciales* y con ello creó la base de una nueva ciencia: *el Caos*. Dependencia sensitiva de las condiciones iniciales significa que, partiendo de dos puntos del espacio de fases, las dos trayectorias correspondientes acaban por diverger, aunque los puntos en cuestión estén tan próximos como queramos. Estos dos puntos representan sendos conjuntos de condiciones iniciales, siendo las trayectorias la distinta evolución del sistema según sea el punto de partida.

Lorenz animado por su descubrimiento, decidió comenzar a experimentar con sus resultados, representó gráficamente los resultados obtenidos con sus tres ecuaciones (3.1a, 3.1b, 3.1c) en una gráfica tridimensional, asignando el valor obtenido de cada ecuación a una de las tres dimensiones del plano.

$$\frac{dx}{dt} = \sigma(y - x), \tag{3.1a}$$

$$\frac{dy}{dt} = \rho x - y - xz, \tag{3.1b}$$

$$\frac{dz}{dt} = xy - \beta z \tag{3.1c}$$

donde x, y y z son los estados del sistema, x_0, y_0 y z_0 son las condiciones iniciales, σ, ρ y β son los parámetros de control y t es el tiempo.

A pesar de lo impredecible del sistema, lejos de ser un comportamiento al azar, tenía una curiosa tendencia a evolucionar dentro de una zona muy concreta del espacio de fases, situando una especie de pseudocentro de gravedad de los comportamientos posibles.

Lorenz descubrió que su sistema contenía una dinámica extremadamente errática. Las soluciones oscilaban irregularmente sin llegar a repetirse, pero en una región acotada del espacio de fases [27]. Al ver el gráfico resultante, las trayectorias rondaban siempre alrededor de lo que ahora definimos como atractor extraño (ver figura 3.2), Lorenz se encontró otra vez con el efecto mariposa, concretamente con sus alas.

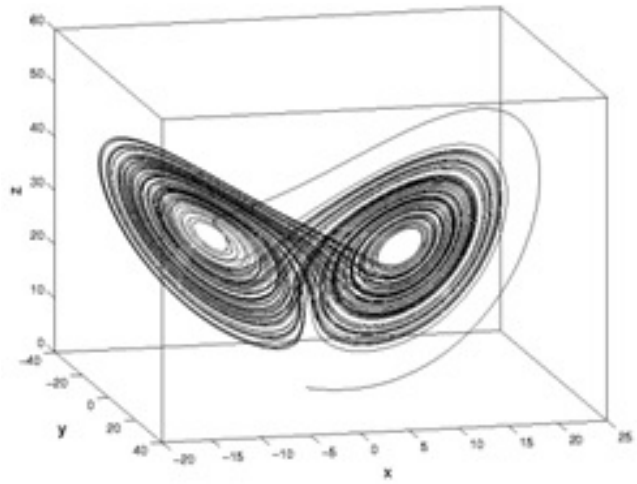


Figura 3.2: Atractor de Edward Lorenz en tres dimensiones.

Los ordenadores son los instrumentos primarios con los que se investiga el caos y gran parte de nuestro entendimiento de los sistemas caóticos proviene del uso de modelos por ordenador que rastrean esos sistemas a través del tiempo.

3.2. Sistemas caóticos y sus propiedades

Es en los sistemas dinámicos donde podemos usar el término caos y donde una variación mínima de las condiciones iniciales supone un comportamiento totalmente distinto del esperado por parte del sistema (ver figura 3.3). Es decir, que un sistema podrá ser caótico cuando su comportamiento sea impredecible [28].

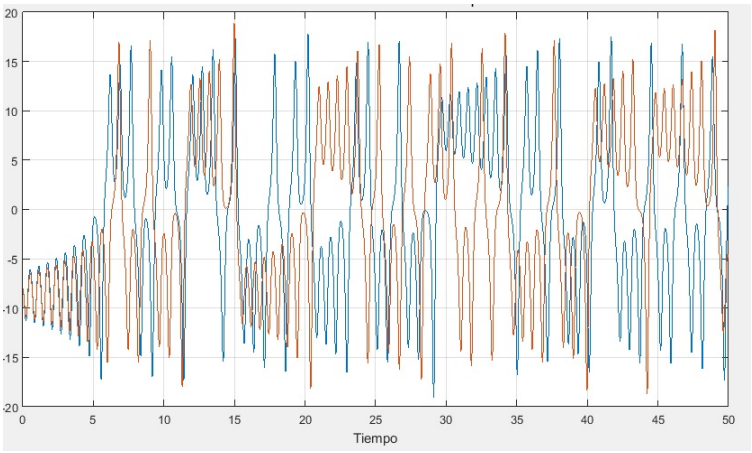


Figura 3.3: Estado x del sistema de Lorenz con distintas condiciones iniciales.

Los sistemas dinámicos, son sistemas que varían con el paso del tiempo, tales como la teoría maltusiana de población y recursos, la meteorología, los sismos, los movimientos que efectúa un chorro de café humeante al entrar en contacto con la leche de un taza (mecánica de fluidos), el giro impredecible de una noria de agua cuando su caudal es inusitadamente acelerado, la gran mancha de Júpiter, las fluctuaciones económicas de los precios, etc.

En [29] habla sobre la clasificación de los sistemas dinámicos, los cuales son:

- **Estables**. Tienden a un punto a lo largo del tiempo o siguen una misma órbita, sus ecuaciones características, condiciones iniciales, sus límites, elementos y relaciones nos permiten conocer su evolución a través del tiempo, es decir, sabemos hacia donde lo dirige su atractor.

- **Inestables**. Cuando dos soluciones con condiciones iniciales diferentes acaban divergiendo por pequeñas que sean las condiciones iniciales. Así un sistema inestable escapa de los atractores.

- **Caóticos**. Las soluciones se mueven en torno al atractor de manera irregular y pasado el tiempo ambas soluciones no son cercanas, si bien suelen ser cualitativamente similares. De esa manera, el sistema permanece confinado en una zona de su espacio de estados. Los sistemas caóticos, por su parte, manifiestan ambos comportamientos. Se pueden conocer sus ecuaciones y sus condiciones iniciales fijas, sin embargo la más mínima variación provoca una evolución radical en su comportamiento.

Uno de los más citados ejemplos de sistema caótico es el clima atmosférico, del cual podemos predecir su comportamiento y elaborar pronósticos en base a ecuaciones, estudios de su comportamiento pasado y el conocimiento de sus condiciones iniciales. Sin embargo, no podemos conocer con exactitud los parámetros que fijan sus condiciones iniciales y esto provoca que aunque se conozca el modelo, éste diverja de la realidad pasado un cierto tiempo. Así mismo, nuestro pronóstico puede verse afectado por variaciones dentro del sistema atmosférico como la actividad humana, actividad volcánica o incluso fuera de éste como la actividad solar.

También se puede identificar a un sistema caótico por la presencia de un atractor extraño. De forma general, se puede decir que un atractor es una región o conjunto cerrado en el espacio de fase, al cual convergen las trayectorias de un sistema, entendiéndose por trayectoria a la evolución temporal del sistema a partir de una condición inicial específica.

Un sistema caótico se puede describir por un conjunto de ecuaciones diferenciales o en diferenciales no lineales, que generan secuencias caóticas que son deterministas, es decir, el valor futuro depende del valor actual y que además, presentan las siguientes propiedades:

- **No linealidad**. Son sistemas de ecuaciones diferenciales (tiempo continuo) o en diferencias (tiempo discreto) no lineales, que no cumple con el principio de superposición.
- **Sensibilidad exponencial a condiciones iniciales y parámetros de control**. La dinámica o trayectoria del sistema caótico se vería altamente modificada si se varía ligeramente una condición inicial o parámetro de control.
- **Mezcla de datos**. Un pequeño rango de condiciones iniciales cubre la mayor parte del espectro caótico.
- **Ergodicidad**. La trayectoria caótica se mantiene confinada en un espacio conocido como atractor extraño con respecto al tiempo cubriendo en su totalidad su espacio para cualquier entrada de condición inicial o parámetro de control.
- **Exponente de Lyapunov positivo**. Un sistema de dimensión n posee n exponentes de Lyapunov; si uno de ellos es positivo, el sistema es caótico; si dos o más son positivos, el sistema es hypercaótico.
- **Atractor extraño con dimensión fractal**. La gráfica de fase del sistema genera lo que se conoce como atractor, que puede ser punto fijo (sistema estable), ciclo límite (sistema periódico) o atractor extraño (sistema caótico).

Muchas de las propiedades mencionadas están estrechamente relacionadas con propiedades criptográficas, por lo que los sistemas caóticos se utilizan para la protección de datos privados en sistemas de comunicaciones inseguros.

3.3. Exponente de Lyapunov

Los exponentes de Lyapunov miden la tasa promedio de divergencia o convergencia exponencial de dos trayectorias cercanas en el espacio de fase. Dado que condiciones iniciales cercanas corresponden a estados iniciales prácticamente idénticos, la divergencia exponencial de las órbitas implica la pérdida de la predictibilidad del sistema. Cualquier sistema que contenga al menos un exponente de Lyapunov positivo, se define como caótico [30].

Propiedades:

- Si el sistema es conservativo (no existe disipación), la suma de todos los exponentes de Lyapunov debe ser cero.
- Si el sistema es disipativo, la suma será negativa.
- En un sistema dinámico hamiltoniano, la suma sólo puede ser positiva
- Si el sistema es un sistema abierto, el espectro de Lyapunov puede ser usado para estimar el radio de producción de entropía de un sistema dinámico.

Esta medida de caos, fue introducida por el célebre matemático ruso Alexander Mijailovic Lyapunov a principios del siglo XX. Los exponentes de Lyapunov, como ahora se les conoce, son un conjunto de números que se emplean usualmente para detectar la presencia del caos en sistemas dinámicos. La idea en general es medir qué tan rápido se alejan o difieren las configuraciones globales contiguas con respecto al tiempo.

La sensibilidad a las condiciones iniciales puede ser cuantificado como:

$$||\delta_x(t)|| \approx ||f^{\lambda t}||\delta x_0|| \tag{3.2}$$

que para sistemas de tiempo discreto se usa

$$||\delta_x(n)|| \approx ||f^{\lambda n}||\delta x_0|| \tag{3.3}$$

El exponente de Lyapunov está definido para una función dinámica con una configuración inicial de acuerdo a la siguiente expresión:

$$\lambda = \frac{1}{T}\ ln\ |\frac{f^n(x_n - \delta_0) - f^n(x_n)}{\delta_0}| \tag{3.4}$$

donde λ es el exponente de Lyapunov, x_0 es una condición inicial, $x_0 = x_0 + \delta_0$ es otra condición inicial extremadamente cercana y T es el número de iteraciones.

Este análisis es aplicado a cada uno de los seis mapas caóticos estudiados para elegir uno que sea factible para ser utilizado en el cifrado caótico con aplicación en un microcontrolador. Si el mapa caótico es de n-dimensiones, se tendrá n exponentes de Lyapunov.

3.4. Mapas caóticos estudiados

3.4.1. Mapa logístico

Este modelo se basa en la función logística común de curva en forma de S que muestra cómo una población crece lentamente, luego rápidamente, antes de disminuir a medida que alcanza su capacidad de carga. Se usa una ecuación en diferencia no lineal para observar los pasos de tiempo discretos. Se llama mapa logístico porque asigna el valor de la población en cualquier paso de tiempo a su valor [31]. El mapa logístico se define como:

$$x_{n+1} = ax_n(x_n - 1), \tag{3.5}$$

donde $x_n \in (0, 1)$ es el estado del mapa discreto, x_n es la condición inicial con valores entre $0 < x_n < 1$ y a es el parámetro de control con $3.57 < a < 4$ para que el mapa genere secuencias caóticas (ver figura 3.4).

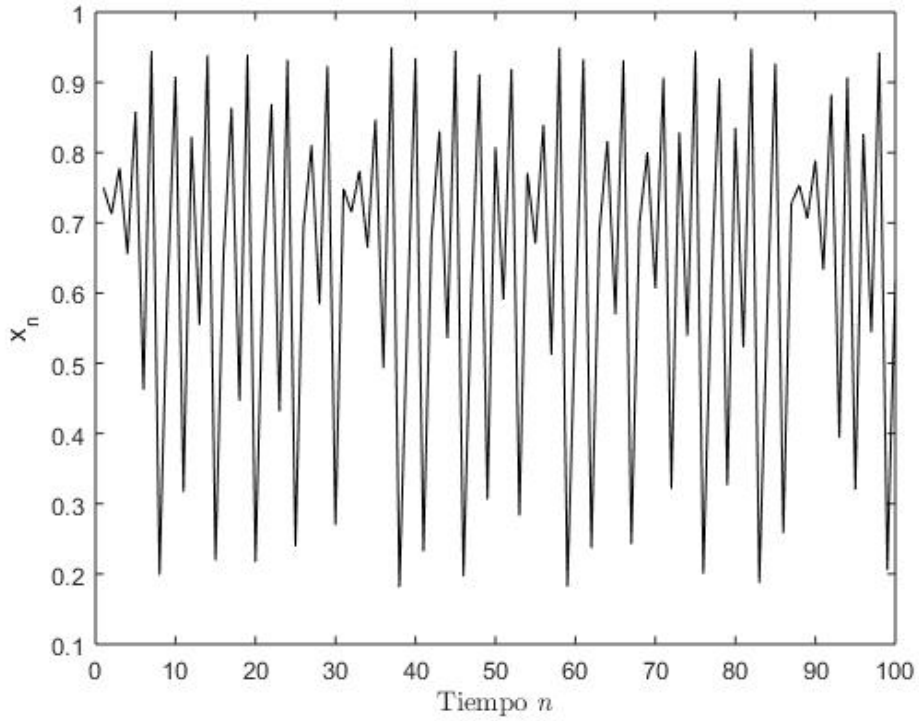


Figura 3.4: Estado x del mapa logístico con dinámicas caóticas.

Para el exponente de Lyapunov se utilizó como parámetro de control $a = 3.800000$, $n = 1000$ y condición inicial de $x_n = 0.750000$. El valor obtenido de Lyapunov es de $\lambda = 0.4237295443$ por lo que se demuestra la existencia de caos.

3.4.2. Mapa Hénon

Michel Hénon descubría en el instituto de Astrofísica de Paris un sistema dinámico de gran sencillez, mediante el cual se podían explicar las pequeñas oscilaciones que ha-

cen que ciertos cuerpos celestes se desvíen levemente de su órbita elíptica [32].

El sistema consta de dos ecuaciones, una de ellas cuadrática y dos constantes:

$$x_{n+1} = 1 - \alpha x_n^2 + y_n, \tag{3.6a}$$
$$y_{n+1} = \beta x_n, \tag{3.6b}$$

donde x y y representan los estados del sistema discreto y n las iteraciones. Para el mapa clásico de Hénon tiene valores de $a = 1.4$ y $b = 0.3$. Con estos valores el mapa de Hénon es caótico.

Para poder observar el atractor extraño del mapa caótico Hénon, se utiliza las condiciones iniciales $x_n = 0.3$ y $y_n = 0.4$, además de $a = 1.4$ y $b = 0.3$ (ver figura 3.5). Estos mismos valores fueron utilizados para calcular el exponente de Lyapunov, los cuales son $\lambda 1 = 0.2365264537$ y $\lambda 2 = -1.1423635344$, lo cual, indica dinámicas caóticas.

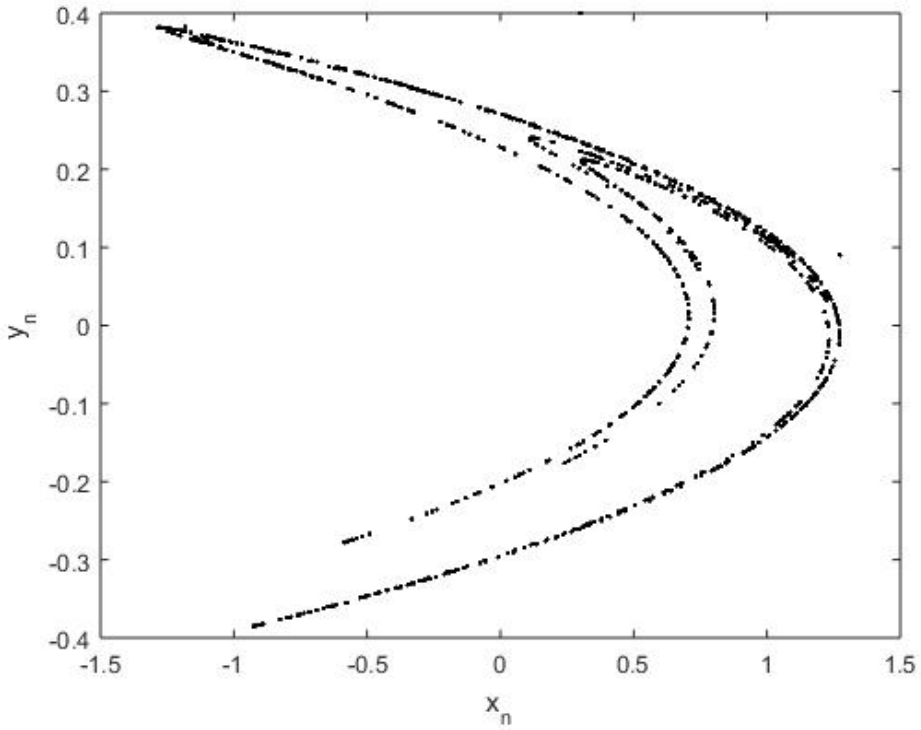


Figura 3.5: Atractor extraño del mapa Hénon.

3.4.3. Mapa Logístico 2D

El mapa logístico 2D tiene un polinomio de segundo orden con el que ambas ecuaciones interaccionan entre sí [33], el cual se define como:

$$x_{n+1} = \alpha_1 x_n(1 - x_n) + \beta_1(y_n^2), \tag{3.7a}$$
$$y_{n+1} = \alpha_2 y_n(1 - y_n) + \beta_2((y_n^2) + x_n y_n), \tag{3.7b}$$

donde x_n y y_n son las condiciones iniciales y α_1, β_1, α_2 y β_2 son los parámetros de control, los cuales deben estar en $2.75 < \alpha 1 < 3.4$, $2.75 < \alpha 2 < 3.45$, $0.15 < \beta 1 < 0.21$ y $0.13 < \beta 2 < 0.15$ para generar dinámicas caóticas (ver figura 3.6).

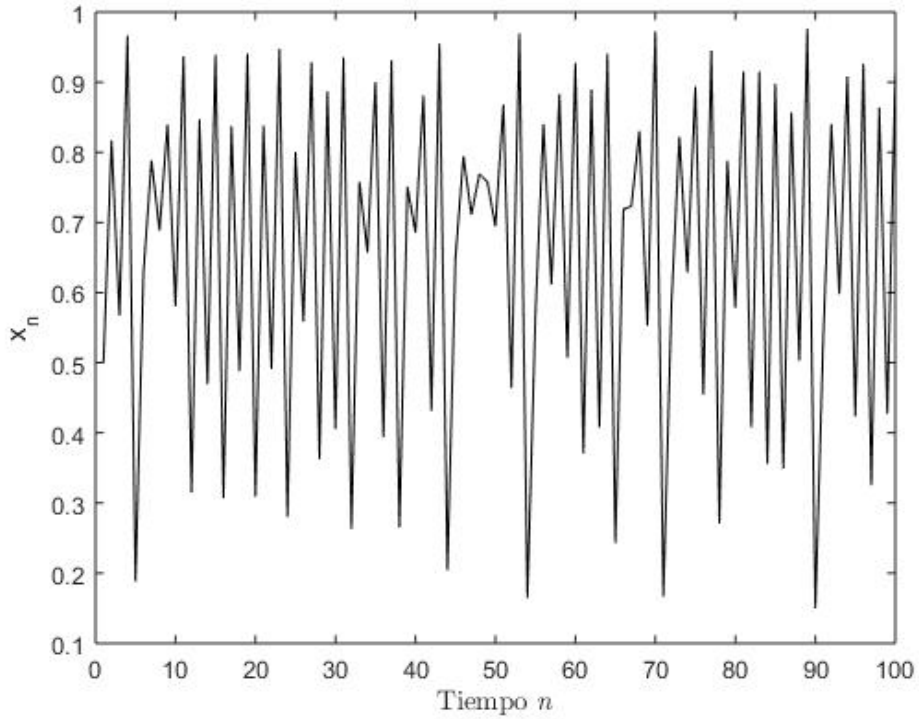


Figura 3.6: Estado x del mapa logístico 2D con dinámicas caóticas.

Para el cálculo del máximo exponente de Lyapunov del mapa logístico 2D, se utiliza las condiciones iniciales $x_n = 0.170000$ y $y_n = 0.500000$. Los parámetros de control son $\alpha_1 = 3.000000$, $\beta_1 = 0.170000$, $\alpha_2 = 3.200000$, $\beta_2 = 0.147500$ con $n = 1000$. Los valores obtenidos son $\lambda 1 = .00772876252$ y $\lambda 2 = 0.1937063845$. Lo que demuestra que genera hypercaos.

3.4.4. Mapa Seno

Cuando la función *seno* tiene entradas dentro del rango de $[0, \pi]$, sus salidas caen dentro del rango de [0, 1]. El mapa Seno se deriva de la función seno transformando sus entradas en [0, 1]. Se define matemáticamente como:

$$x_{n+1} = \beta sin(\pi x_n), \tag{3.8}$$

donde el parámetro $\beta \in (0, 1)$. El mapa sinusoidal es caótico cuando $\beta \in (0.87, 1)$ (ver figura 3.7). Para el exponente de Lyapunov se utilizan los valores de $\beta = 0.96$ con $n = 1000$. El resultado es de $\lambda = 0.1937063845$ lo que demuestra que genera caos.

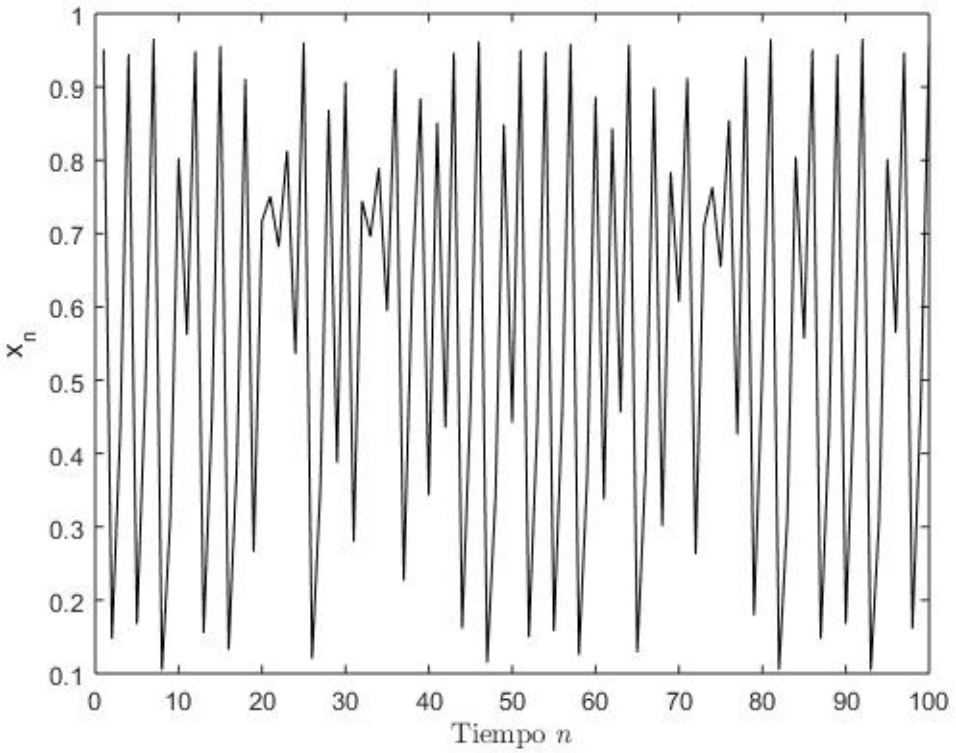


Figura 3.7: Estado x del mapa seno con dinámicas caóticas.

3.4.5. Mapa Chebyshev

Los polinomios de Chebyshev son curvas de coseno con una perturbación en la escala horizontal, pero la vertical se mantiene constante [34].

$$x_{n+1} = cos(\alpha\ cos^{-1}(x_n)), \tag{3.9}$$

donde $x_n \in (-1, 1)$ y α debe ser $1 < \alpha$ para generar dinámicas caóticas (ver figura 3.8).

Para el exponente de Lyapunov se utilizan los valores de $\alpha = 3.7$ con $n = 1000$ y $x_n = 0.6$. El resultado es de $\lambda = 1.3084354758$, lo que demuestra que genera caos.

3.4.6. Mapa 2D Seno-Logístico

Al realizar una combinación del mapa logístico y seno se obtiene las siguientes ecuaciones [35]:

$$x_{n+1} = sin(\pi\mu(y_n + 3))x_n(1 - x_n)), \tag{3.10a}$$
$$y_{n+1} = sin(\pi\mu(x_n + 3))y_n(1 - y_n)), \tag{3.10b}$$

donde μ es el parámetro de control entre $(0 - 1)$, x_n y y_n son las condiciones iniciales entre $(0 - 1)$. Con estos rangos de valores se obtienes dinámicas caóticas (ver figura 3.9 y 3.10).

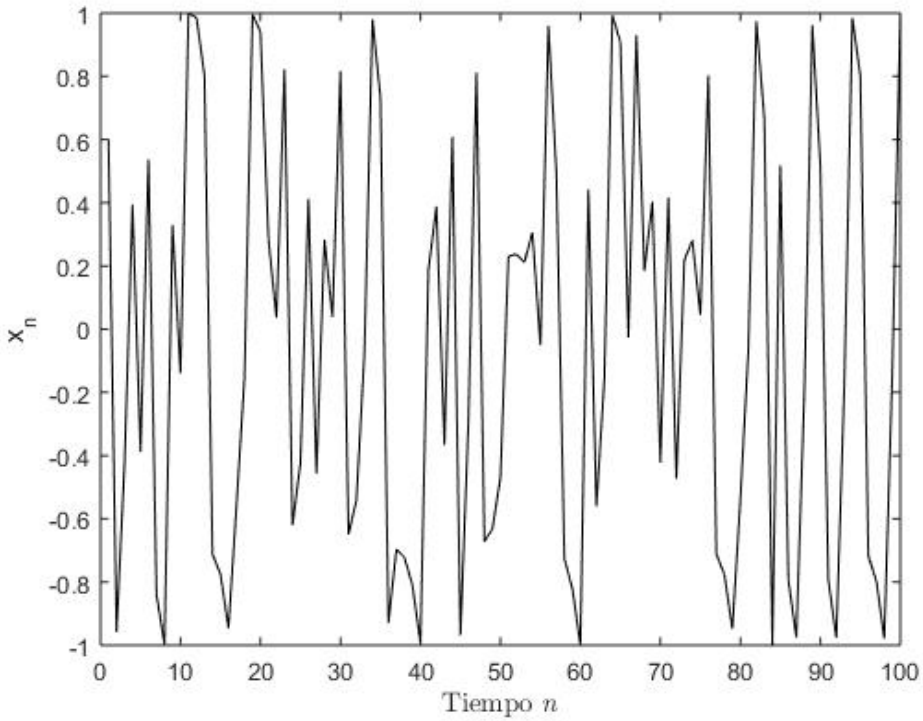


Figura 3.8: Estado x del mapa chebyshev con dinámicas caóticas.

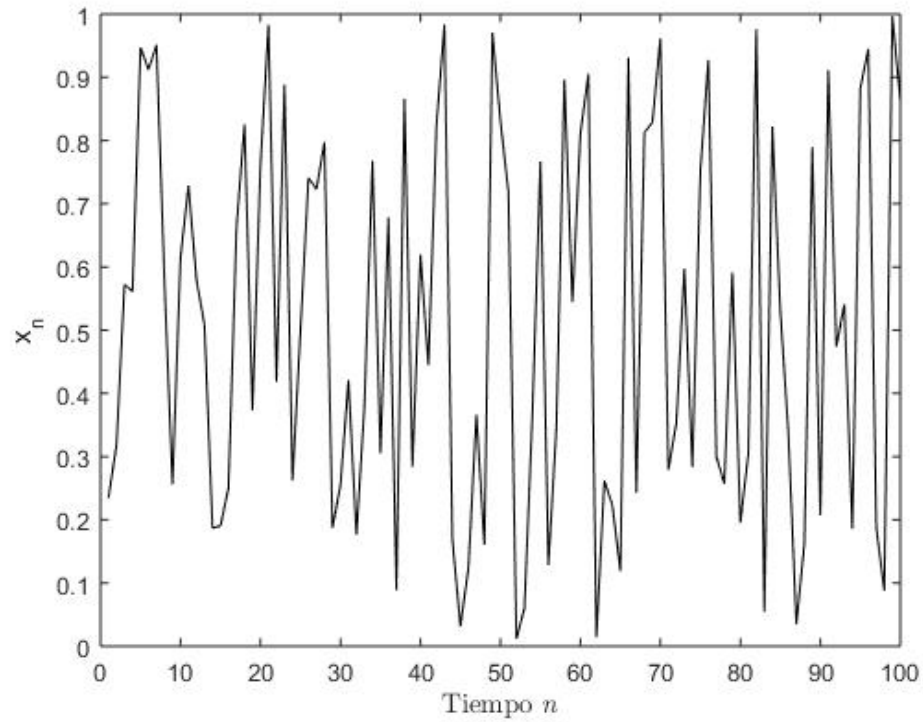


Figura 3.9: Estado x del mapa 2D Seno-Logístico con dinámicas caóticas.

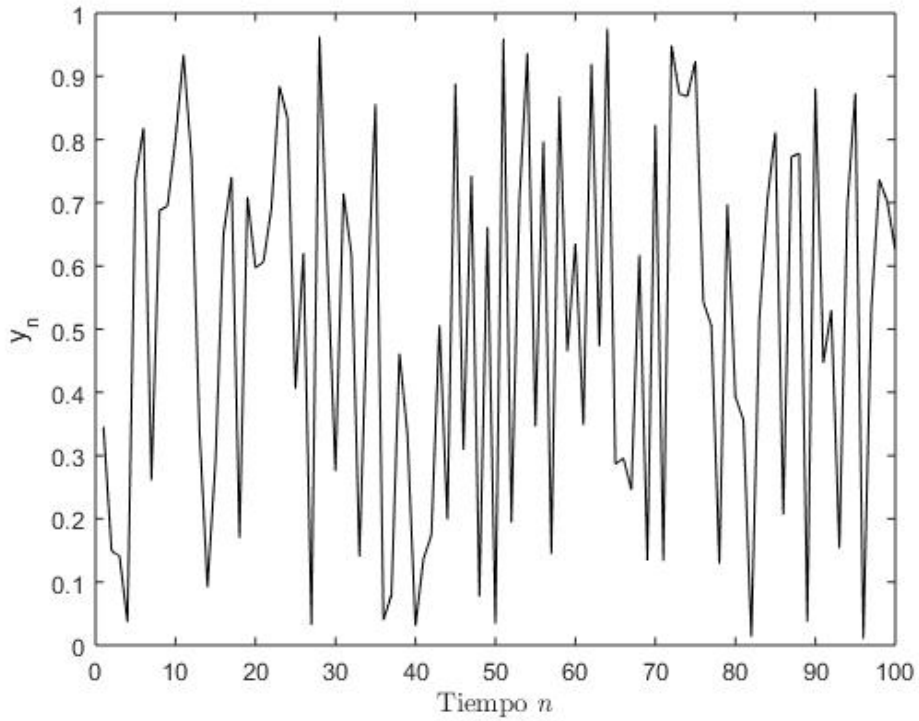


Figura 3.10: Estado y del mapa 2D Seno-Logístico con dinámicas caóticas.

Para el exponente de Lyapunov se utilizan los valores de $\mu = 0.566579$, con $n = 1000$, $x = 0.171234$ y $y = 0.512345$. El resultado es de $\lambda 1 = 0.5985607493$ y $\lambda 2 = 0.6085891569$. Lo cual indica caos, pero al tener los dos valores positivos nos indica que el mapa es hypercaótico.

3.5. Selección de mapa caótico

Para la aplicación criptografía de esta tesis, se utiliza el mapa 2D Seno-Logístico. Además se le realiza una mejora para aumentar sus propiedades pseudoaleatorias. Las razones por las que se escogió son las siguientes:

- Presenta dinámicas hypercaóticas con pocas operaciones aritméticas.
- Tiempo de respuesta más rápido (ver figura 3.11).
- Mejor ergodicidad, ya que la trayectoria se distribuye en regiones mucho más grandes en el plano de fase. Esto significa que es capaz de generar más salidas aleatorias.
- Costo de implementación bajo.

Se puede observar en la figura 3.11 que para todo valor de $\mu \in (0, 1)$ el sistema es caótico.

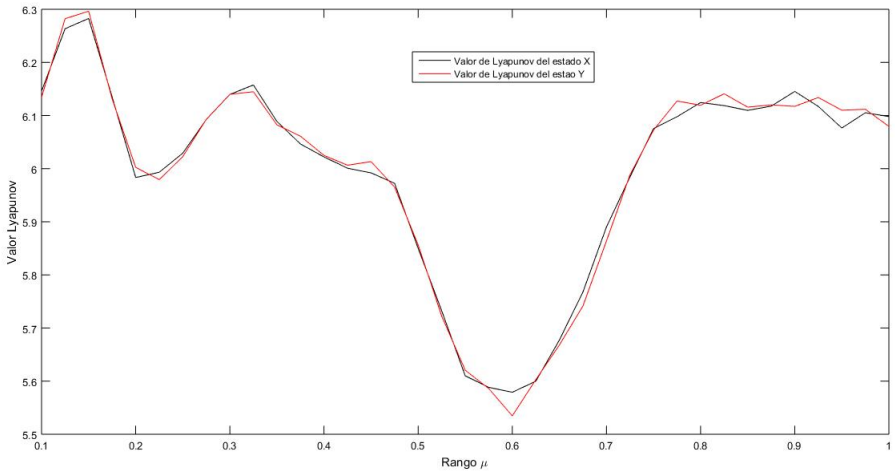


Figura 3.11: Valores de Lyapunov del mapa caótico 2D Seno-Logístico mejorado.

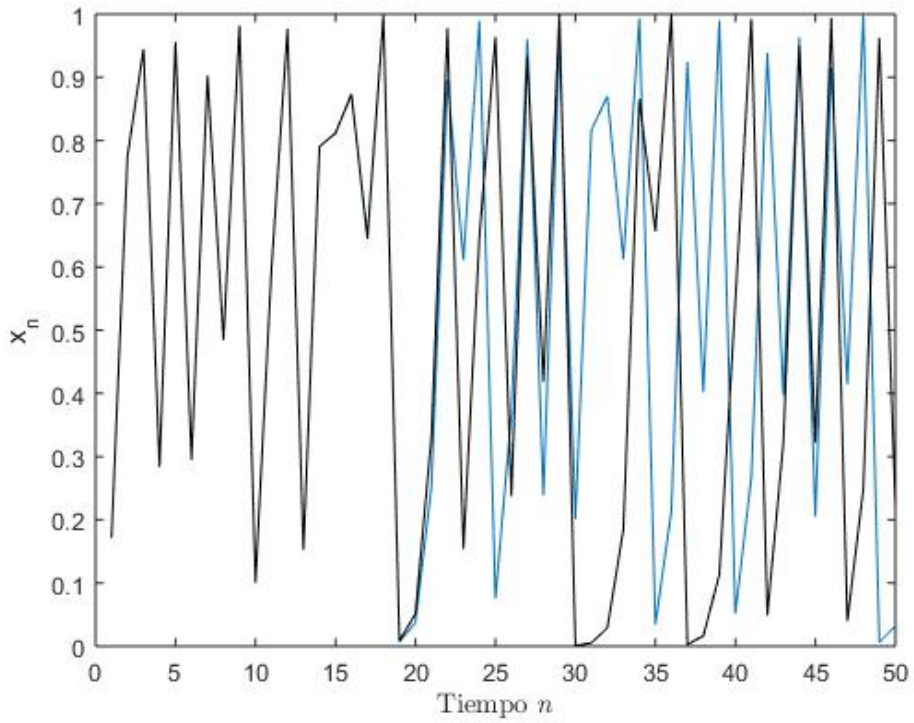


Figura 3.12: El tiempo se respuesta es reducido en el mapa 2D Seno-Logístico.

3.6. Conclusiones

Se presentó una introducción a los sistemas caóticos y sus propiedades. A si como se mostró el inicio del caos y sus principales características representativas como la sensibilidad a condiciones iniciales y parámetros de control. Se implementaron seis mapas caóticos en MatLab de una y dos dimensiones, se determinó su exponente de Lyapunov (ver tabla 3.1), se analizaron y se optó por elegir el mapa 2D Seno-Logístico por las características mencionadas previamente.

Mapa caótico	$\lambda 1$	$\lambda 2$
Logistico	0.4237295443	-
Henon	0.2365264537	-1.1423635344
Logistico	.00772876252	0.1937063845
Seno	0.1937063845	-
Chebyshev	1.3084354758	-
2D Seno-Logístico	0.5985607493	0.6085891569

Tabla 3.1: Exponentes de Lyapunov obtenidos de los seis mapas caóticos.

Capítulo 4

Criptografía

En este capítulo, se presenta el significado de la criptografía y los componentes de un sistema criptográfico. Se muestran los primeros sistemas criptográficos, así como los tipos que existen y las características que se requieren para emplear criptografía caótica.

4.1. Introducción

La palabra *Criptografía* proviene del griego *"kryptos"* que significa oculto y *"grafía"* que significa escritura y su definición es *arte de escribir con clave secreta o de un modo enigmático* [36].

La criptografía es un conjunto de técnicas que tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados y se puede aplicar en dispositivos electrónicos que trasmitan algún tipo de información mediante un canal inseguro (ver figura 4.1). A través de la criptografía, la información puede ser protegida contra el acceso no autorizado, interceptación, modificación y la inserción de información extra. También, puede ser usada para prevenir el acceso o el uso no autorizado de los recursos de una red o sistema informático. Un mensaje codificado por un método de criptografía debe ser privado, solo aquel que envía y aquel que recibe debe tener acceso al contenido del mensaje codificado.

Figura 4.1: La criptografía en dispositivos electrónicos como celulares o computadoras.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entes y en segundo lugar, asegurar que la información que se envía

sea auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, que no haya sido modificado durante su transmisión [37].

Las formas de ocultar el contenido de un mensaje varía, el mensaje es alterado de forma que teóricamente nadie, exceptuando el legítimo destinatario, pueda leer su contenido. Al mensaje a cifrar se le suele denominar texto claro y al proceso de ocultar el contenido mediante una serie de transformaciones regidas por un parámetro o valor secreto como la clave, se le denomina cifrar el mensaje, al mensaje cifrado se le suele denominar texto cifrado o criptograma. Al proceso de obtener el texto claro a partir de un mensaje cifrado se le denomina descifrar el mensaje [38].

El criptoanálisis consiste en la reconstrucción de un mensaje cifrado en texto simple utilizando métodos matemáticos. Por lo general, los criptoanalistas hacen negocios con la información con tal de tener ganancias económicas. Todos los criptosistemas deben ser resistentes a los métodos de criptoanálisis. Cuando un método de criptoanálisis permite descifrar un mensaje cifrado mediante el uso de un criptosistema, decimos que el algoritmo de cifrado ha sido decodificado.

Con la criptografía se intenta garantizar las siguientes propiedades deseables en la comunicación de información de forma segura. A estas propiedades se las conoce como funciones o servicios de seguridad:

- **Confidencialidad**. Solamente los usuarios autorizados tienen acceso a la información.
- **Integridad de la información**. Garantía ofrecida a los usuarios de que la información original no es alterada intencionalmente o accidentalmente.
- **Autentificación de usuario**. Es un proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.

Las aplicaciones de la criptografía son muchas ya que proporciona cualquier tipo de seguridad que sea requerida. Entre las aplicaciones y usos que se destacan más, son las siguientes:

- **Seguridad en las comunicaciones**. Es la principal aplicación de la criptografía a las redes de computadores, ya que permiten establecer canales seguros sobre redes que no lo son.
- **Identificación y Autentificación**. Gracias al uso de firmas digitales y otras técnicas criptográficas es posible identificar a un individuo o validar el acceso a un recurso en un entorno de red con más garantías que con los sistemas de usuario y clave tradicionales.
- **Certificación**. La certificación es un esquema mediante el cual agentes fiables (como una entidad certificadora) validan la identidad de agentes desconocidos

(como usuarios reales). El sistema de certificación es la extensión lógica del uso de la criptografía para identificar y autentificar cuando se emplea a gran escala.

- **Comercio electrónico**. Gracias al empleo de canales seguros y a los mecanismos de identificación se posibilita el comercio electrónico, ya que tanto las empresas como los usuarios tienen garantías de que las operaciones no pueden ser espiadas, reduciéndose el riesgo de fraudes y robos.

4.2. Historia de la criptografía

Entre el Antiguo Egipto e internet, los criptogramas (mensajes cifrados) han protagonizado buena parte de los grandes episodios históricos y un sin fin de anécdotas. Existen mensajes cifrados entre los textos diplomáticos de toda época, indispensables para las órdenes militares y los ejércitos modernos en tiempos de guerra y por supuesto, esenciales en la actividad de los espías. Hoy en día, con las nuevas tecnologías el uso de la criptografía se ha extendido más allá de su tradicional esfera estatal o política y es vital también para la actividad diaria de las empresas y ciudadanos particulares.

Los espartanos utilizaron, hacia el 400 a.C., la Escítala (ver figura 4.2), que puede considerarse el primer sistema de criptografía por transposición, es decir, que se caracteriza por ocultar el significado real de un texto claro alterando el orden de los signos que lo conforman. Los militares de la ciudad de griega escribían sus mensajes sobre una tela que envolvía una vara. El mensaje sólo podía leerse cuando se enrollaba la tela sobre un bastón del mismo grosor, que poseía el destinatario lícito del mensaje.

Figura 4.2: Escítala: considerado el primer sistema de criptografía.

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas una cantidad de posiciones a la derecha (ver figura 4.3).

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado n posiciones a la derecha) y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la

gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

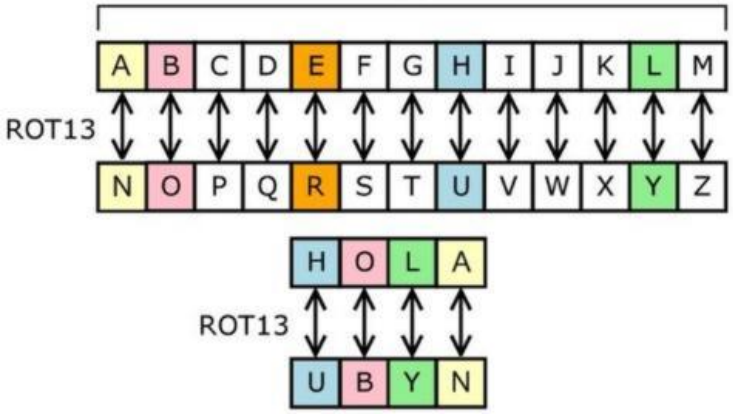


Figura 4.3: Cifrado de César.

A principios del siglo XX, se diseñaron teletipos equipados con una secuencia de rotores móviles. Éstos giraban con cada tecla que se pulsaba. De esta forma, en lugar de la letra elegida, aparecía un signo escogido por la máquina según diferentes reglas en un código polialfabético complejo. Estos aparatos, se llamaron traductores mecánicos. Una de sus predecesoras fue la Rueda de Jefferson, el aparato mecánico criptográfico más antiguo que se conserva.

La primera patente data de 1919 y es obra del holandés Alexander Koch, que comparte honores con el alemán Arthur Scherbius, el inventor de Enigma (ver figura 4.4) una máquina criptográfica a rotor [39].

Figura 4.4: Máquina enigma.

4.3. Tipos de criptosistemas

Puede definirse formalmente un criptosistema (sistema de cifrado) como una quintupla (m, c, K, E, D) (ver figura 4.5), donde:

- ***m***: Representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro) que pueden ser enviados.
- ***c***: Representa el conjunto de todos los posibles mensajes cifrados o criptogramas.
- ***K***: Representa el conjunto de claves que se pueden emplear en el criptosistema.
- ***E***: Es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de c (Función de cifrado).
- ***D***: Es el conjunto de transformaciones de descifrado, análogo a E.

En todo sistema criptográfico se debe cumplir la siguiente condición

$$D_K(E_K(m)) = m \tag{4.1}$$

Es decir, si un mensaje m se cifra con una función E y una clave K y después se descifra con la misma clave K, se obtiene el mensaje original m.

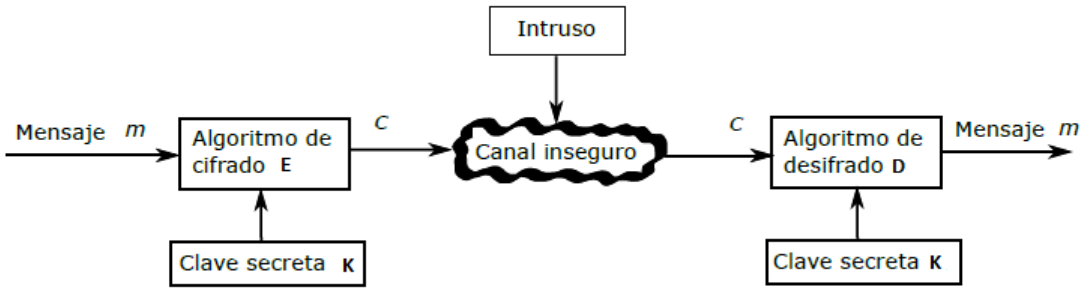


Figura 4.5: Esquema de cifrado caótico.

La clasificación de los sistemas criptográficos es como sigue:

1. **Criptosistemas simétricos o de clave privada**: Son aquellos que emplean una misma clave K tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave K debe estar en posesión tanto en el emisor como en el receptor [40].

   La criptografía simétrica se refiere al conjunto de métodos que permite tener comunicación segura entre las partes, siempre y cuando anteriormente se hayan intercambiado la clave correspondiente de forma segura. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

   Algunas de las características más destacadas de este tipo de algoritmos son las siguientes:

- A partir del mensaje cifrado no se puede obtener el mensaje original ni la clave que se ha utilizado, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado.
- Se utiliza la misma clave para cifrar el mensaje original que para descifrar el mensaje codificado.
- Emisor y receptor deben haber acordado una clave común por medio de un canal de comunicación confidencial antes de poder intercambiar información confidencial por un canal de comunicación inseguro.

El esquema general de cifrado y descifrado mediante algoritmos de clave privada se muestra en la figura 4.6. A partir de un documento original se obtiene un documento cifrado al aplicar cifrado con una clave secreta; esa misma clave secreta se utiliza posteriormente para volver a obtener el documento original.

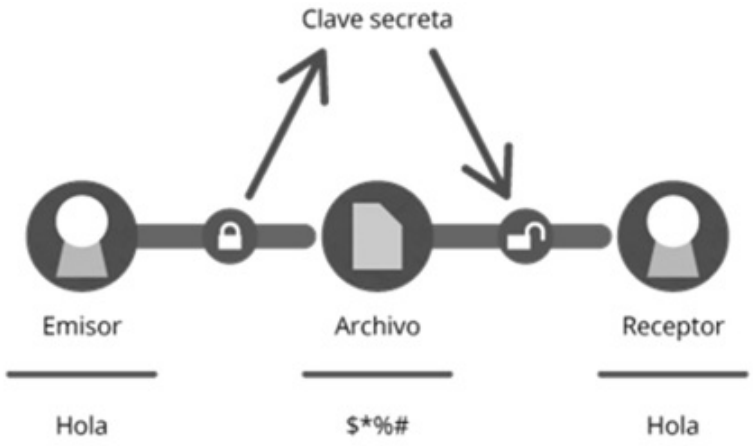


Figura 4.6: Esquema de criptosistema simétrico.

2. **Criptosistemas asimétricos o de clave pública**: Emplean una doble clave (Kp, KP). Kp se la conoce como clave privada y KP se la conoce como clave pública. Una de ellas sirve para la transformación o función de cifrado y la otra para la transformación de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública KP no permita calcular la clave privada Kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros, puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado [41].

Para enviar un mensaje confidencial sólo hace falta conocer la clave pública del destinatario y cifrar el mensaje utilizando dicha clave. En este caso, los algoritmos

asimétricos garantizan que el mensaje original sólo puede volver a recuperarse utilizando la clave privada del destinatario (ver figura 4.7). Dado que la clave privada se mantiene en secreto, sólo el destinatario podrá descifrar el mensaje.

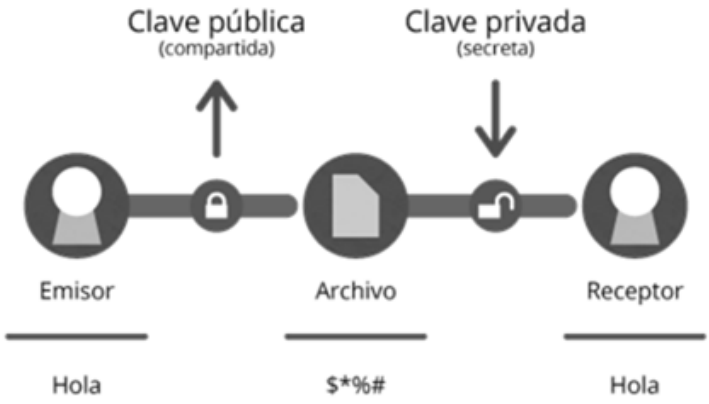


Figura 4.7: Esquema de criptosistema asimétrico.

Para la función del algoritmo hay dos operaciones que se realizan:

- **Confusión**. Consiste en permutar cada elemento del mensaje de manera desordenada en función de la clave secreta.
- **Difusión**. Consiste en cambiar el valor a cada elemento del texto claro de manera desordenada en función a la clave secreta, para transformarlo en otro elemento del mismo tipo.

Para la estructura del algoritmo de cifrado:

- **Cifrado de flujo**. Cifran el mensaje bit a bit (o byte a byte) hasta terminarlo.
- **Cifrado de bloque**. Cifran el mensaje en bloques de k bits simultáneamente hasta terminarlo. Algunos ejemplos de algoritmos convencionales son el DES, 3DES, RC5, AES, Blowfish e IDEA.

En la práctica, se emplea una combinación de estos dos tipos de criptosistemas, puesto que los criptosistemas asimétricos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se hace uso de la criptografía asimétrica para codificar las claves simétricas y poder así enviarlas a los participantes en la comunicación incluso a través de canales inseguros. Después, se codificarán los mensajes intercambiados en la comunicación mediante algoritmos simétricos, que suelen ser más eficientes.

4.4. Seguridad criptográfica

Los métodos de criptografía actuales son seguros, eficientes y basan su uso en una o más llaves. La llave es una secuencia de bits, que puede contener caracteres, letras, dígitos y símbolos (como una contraseña), utilizada por los métodos de criptografía para codificar y decodificar mensajes [42].

El principio de Keckhoff indica que la seguridad de un sistema criptográfico debe recaer en la clave secreta y no sobre el algoritmo de cifrado. El algoritmo de cifrado se considera de dominio público. Un sistema criptográfico se considera vulnerado si un criptoanalista encuentra la forma de determinar la clave secreta y en consecuencia el texto claro.

Para este trabajo se realizará el cifrado cotico digital, pero para el cual, hay unos requerimientos básicos que se deben tomar en cuenta. En [43] presenta una serie de reglas que un sistema criptógrafico basado en caos digital debe incluir.

Los puntos son los siguientes:

1. Se debe describir que sistema caótico utiliza el cifrado.
2. La degradación digital sebe ser evaluada, en caso de que se discretize un sistema continuo.
3. El sistema criptográfico debe ser fácil de implementar con base a costos aceptables y buena velocidad de cifrado.
4. La clave secreta debe ser claramente definida.
5. El espacio de claves debe ser especificada sólo para generar secuencias caóticas.
6. El efecto avalancha debe producirse para cualquier clave secreta, es decir alta sensibilidad a la clave secreta.
7. Información parcial de la clave secreta no debe revelar información parcial del texto claro, tampoco parte de la clave desconocida.
8. El proceso para generar secuencias caóticas a partir de la clave secreta debe estar claramente definido.
9. El cifrado debe tener alta sensibilidad al texto claro.
10. El cifrado debe generar un texto cifrado con distribución de probabilidad uniforme.

Por otra parte, el sistema criptográfico debe resistir los siguientes ataques criptoanalíticos (ver figura 4.8) (de tipo lógico), con base al principio de Kerckhoffs; es decir, se conoce todo sobre el sistema criptográfico, excepto la clave secreta:

1. **Ataques diferenciales**. Son ataques del tipo solo texto claro elegido y conocido, donde se debe mostrar alta sensibilidad del sistema criptográfico a la clave secreta y al texto claro, para que el sistema criptográfico pueda resistirlos.

2. **Ataques estadísticos**. Son ataques de histogramas y correlación, donde se debe mostrar mediante análisis de correlación e histogramas, la uniformidad del texto cifrado, para resistir estos ataques.

3. **Ataque exhaustivo**. Son ataques donde se tratan todas las posibles combinaciones de claves, por lo que, la clave debe contener más de 2^{100} opciones.

Figura 4.8: Criptoanalistas: Son los encargados de corromper los algoritmos de cifrado.

También, algunos ataques de tipo teórico considerados poderosos son: ataque exhaustivo o fuerza bruta donde todas las posibles claves son utilizadas para descifrar un mensaje.

1. **Solo texto cifrado**. En este ataque, el criptoanalista conoce el algoritmo y texto cifrado. Prácticamente es un ataque exhaustivo, por lo que se requiere que el espacio de claves sea suficientemente grande para resistir un ataque exhaustivo.

2. **Texto claro conocido**. Es un ataque diferencial poderoso donde el criptoanalista conoce el texto claro de un texto cifrado y utiliza esta información para intentar determinar la clave secreta y así, descifrar otros criptogramas. Si el algoritmo cae ante este ataque, se considera no seguro.

3. **Texto claro elegido**. Es otro ataque diferencial poderoso en donde el criptoanalista elije su propio texto claro para cifrar, posteriormente hace una ligera modificación (un bit) al texto claro y se vuelve a cifrar para determinar una relación entre la entrada y salida para determinar la clave secreta y descifrar otros criptogramas.

4.5. Conclusiones

En este capítulo, se introdujo a la criptografía y se mencionaron los tipos de criptosistemas. Para este trabajo, se utilizará el criptosistema de clave privada para el cifrado de señal ECG. La criptografía fue desarrollada desde que el hombre requirió tener privacidad en las comunicaciones y es muy notable como a lo largo del tiempo, los distintos métodos para ocultar la información fueron evolucionando gradualmente.

Es por ello que en la actualidad, se está trabajando para brindar seguridad al futuro modificando el desarrollo de distintos métodos para el encriptado de la información, pero a la vez, habrá personas que quieran esta información, es así como ambos se necesitan para coexistir, siempre que se tenga información encriptada habrá alguien que la quiera obtener.

Capítulo 5

Sistemas embebidos

En este capítulo, se presenta una breve introducción a los *sistemas embebidos* así como sus características. El microcontrolador se encarga de la gestión de las tareas del sistema embebido mediante su programación en software y se dan algunas características del microcontrolador que se utilizará para este trabajo de tesis.

5.1. Introducción

Un *Sistema Embebido* es un sistema electrónico diseñado para realizar pocas funciones en tiempo real [44], según sea el caso. Al contrario de lo que ocurre con las computadoras, las cuales tienen un propósito general, ya que están diseñadas para cubrir un amplio rango de necesidades, mientras que los sistemas embebidos se diseñan para cubrir necesidades específicas. En un sistema embebido, la mayoría de los componentes se encuentran incluidos en la placa base (ver figura 5.1), la tarjeta de vídeo, audio, módem y muchas veces los dispositivos resultantes no tienen el aspecto de lo que se suele asociar a una computadora. Algunos ejemplos de sistemas embebidos podrían ser dispositivos como un taxímetro, un sistema de control de acceso, la electrónica que controla una máquina expendedora o el sistema de control de una fotocopiadora entre otras múltiples aplicaciones [45].

Los sistemas embebidos tienen como una de sus partes a una computadora con características especiales, como un microcontrolador que viene a ser el cerebro del sistema. Está formando por un microprocesador y un software que se ejecute sobre éste. Sin embargo, este software necesitará sin duda un lugar donde poder guardarse para luego ser ejecutado por el procesador. Esto podría tomar la forma de memoria RAM, SRAM y ROM [46]. Todo sistema embebido necesitará una cierta cantidad de memoria, la cual puede incluso encontrarse dentro del mismo chip del procesador, en su memoria sólo reside el programa destinado a gobernar una aplicación concreta. Sus líneas de entrada/salida (I/O) soportan el conexionado de los sensores y actuadores del dispositivo a controlar y todos los recursos complementarios disponibles tienen como finalidad atender requerimientos específicos (ver figura 5.2). Normalmente estos sistemas poseen una interfaz externa para efectuar un monitoreo del estado.

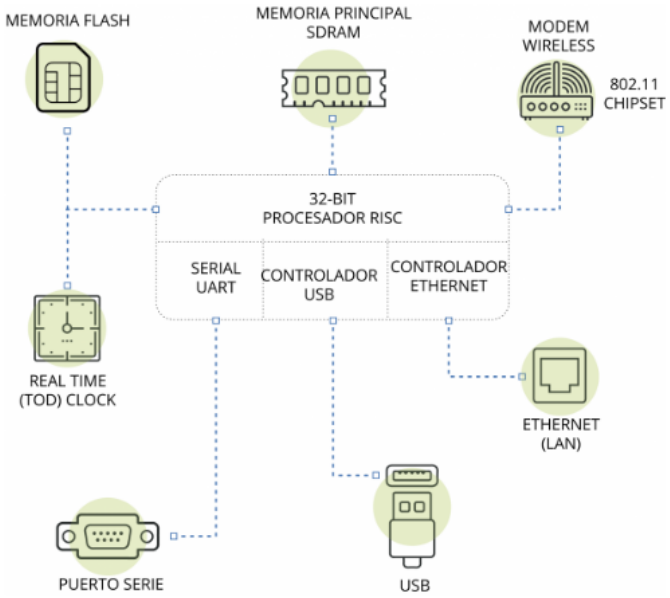


Figura 5.1: Descripción de sistema embebido a nivel físico.

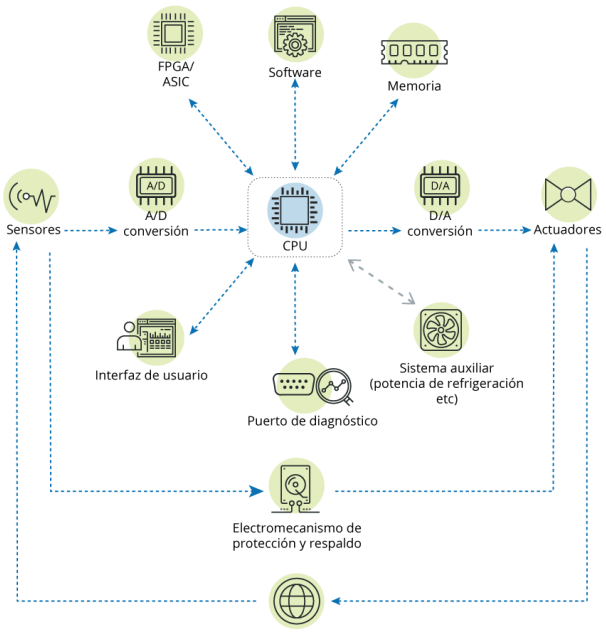


Figura 5.2: Descripción de sistema embebido a nivel lógico.

Por lo general, los sistemas embebidos se pueden programar directamente en el lenguaje ensamblador del microcontrolador o microprocesador incorporado sobre el mismo, o también, utilizando los compiladores específicos que utilizan lenguajes como C o C++ y en algunos casos, cuando el tiempo de respuesta de la aplicación no es un factor crítico, también pueden usarse lenguajes interpretados como Java.

Las principales características de un sistema embebido son el bajo costo y bajo consumo de potencia. Dado que muchos sistemas embebidos son concebidos para ser producidos en miles o millones de unidades, el costo por unidad es un aspecto importante a tener en cuenta en la etapa de diseño.

5.2. Microcontrolador

Un *microcontrolador* es un circuito integrado digital que puede ser usado para diversos propósitos debido a que es programable. Está compuesto por una unidad central de proceso (CPU), memorias (ROM, RAM y Flash), líneas de entrada y salida (periféricos) [47]. Un microcontrolador puede usarse para muchas aplicaciones y algunas de ellas son: manejo de sensores, controladores, juegos, calculadoras, agendas, avisos lumínicos, secuenciador de luces, entre muchas otras.

Como el hardware ya viene integrado en un solo chip, para usar un microcontrolador se debe especificar su funcionamiento por software a través de programas que indiquen las instrucciones que el microcontrolador debe realizar. En una memoria se guardan los programas y el CPU se encarga de procesar paso por paso las instrucciones del programa. Los lenguajes de programación típicos que se usan para este fin son ensamblador y C.

Generalmente, se confunde lo que hace un microcontrolador con un microprocesador. En la tabla 5.1 se puede observar sus diferencias.

	Microcontrolador	**Microprocesador**
CPU	Requiere una unidad de procesamiento	Es una unidad de procesamiento
RAM y ROM	Incluye en un solo circuito	Externos
Velocidad	Más lenta que el microprocesador	Rápida
Costos	Menor que un microprocesador	Alto
Interferencia	Bajo	Alto

Tabla 5.1: Comparativa entre microcontrolador y microprocesador.

En las aplicaciones experimentales realizadas en este trabajo, se utiliza el microcontrolador de 32 bits MCF52259 de Freescale integrado un una tarjeta M52259DEMOKIT (ver figura 5.3). La familia de microcontroladores MCF5225X consiste de dispositivos altamente integrados con comunicación en chip de USB, Ethernet, CAN y funciones de cifrado.

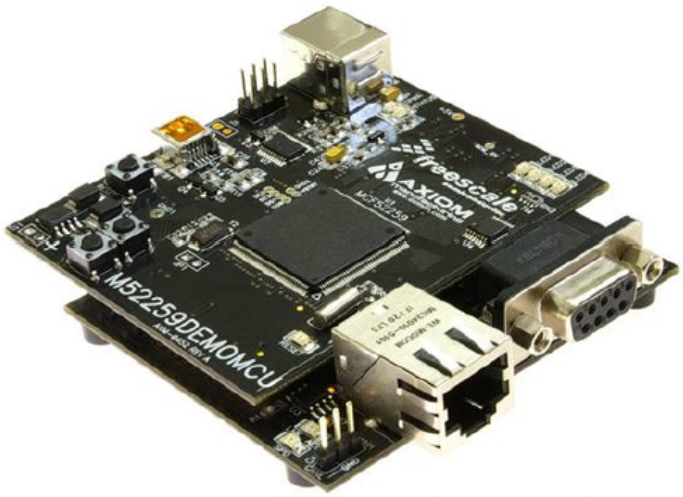


Figura 5.3: Microcontrolador M52259DEMOKIT utilizado en este trabajo de tesis.

Está basado en un procesador de 32 bits ColdFire con una velocidad hasta de 80 MHz, memoria flash de 512 MB y 64 KB de SRAM. Además, posee interfaz externa que proporciona flexibilidad para agregar memoria adicional (ver figura 5.4). Estas y otras características hacen del microcontrolador MCF5225X ideal para aplicaciones en control industrial, redes de internet industriales, sector salud, seguridad, aplicaciones que requieren un amplio rango de conectividad y alto desempeño. Se utiliza programación en lenguaje C en el software CodeWarrior 7.1 de Freescale con soluciones de software MQX 3.5 para alta integración en comunicación USB y Ethernet en tiempo real [48].

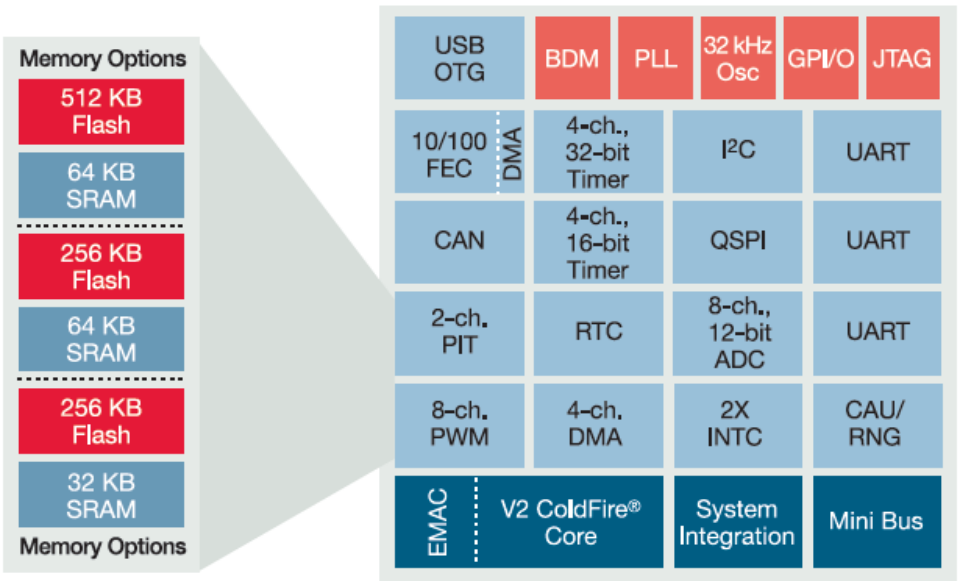


Figura 5.4: Diagrama a bloques del microcontrolador M5225DEMOKIT.

5.3. Conclusiones

Los sistemas embebidos son de gran utilidad hoy en día, ya que se utilizan en casi todos los productos que nos rodean gracias a que se pueden conectar a internet, lo que permite un gran campo de aplicación.

El crecimiento de la tecnología y sistemas de comunicación permitió realizar distintos dispositivos que pueden transmitir y almacenar datos de forma remota. Internet ha traído un principal problema en común, el cual es la seguridad de la información, ya que los datos que se transmiten pueden ser robados para fines maliciosos o fraudulentos y para atacar este problema se utiliza la criptografía caótica.

Capítulo 6

Algoritmo de cifrado caótico propuesto para señales ECG

En este capítulo, se muestra el algoritmo de cifrado caótico propuesto, el cual se basa en una clave simétrica de 192 bits representada por 48 caracteres hexadecimales para generar secuencias caóticas del mapa 2D Seno-Logístico y cifrar los datos de manera secuencial (flujo).

6.1. Introducción

Actualmente, en telemedicina, muchos procesos están conectados a sistemas embebidos que envían información mediante una transmisión inalámbrica. En el área médica, las señales de ECG (ver figura 6.1) cambian de persona a persona. Comparado con un sistema biométrico común, las caracterices biométricas del ECG son extremadamente difíciles de duplicar. Por lo tanto, un ECG puede ser usado como una herramienta biométrica para la identificación de individuos [50].

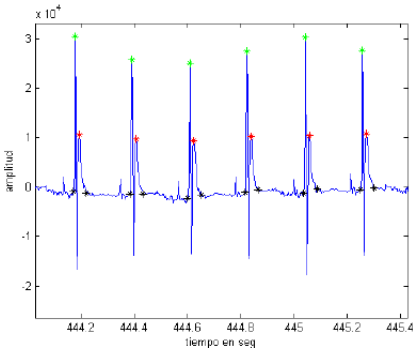


Figura 6.1: Señal de electrocardiograma (ECG).

El ECG se registra en el lugar en que se produce el trastorno y lo interpretan los médicos de urgencias, el personal paramédico de las ambulancias o los cardiólogos que reciben el ECG en el hospital a través de una transmisión inalámbrica (ver figura 6.2) [51]. Este método se ha aplicado con éxito en varios países de todo el mundo [52–54].

Figura 6.2: El electrocardiograma se registra en la ambulancia y se envía vía inalámbrica a un centro de intervención.

Este es un ejemplo claro de aplicación al encriptado de señales biomédicas para evitar el robo de información personal médica o de pacientes.

Actualmente se han propuesto algoritmos de cifrado basado en caos para telemedicina, en la cual se utilizaron señales biomédicas como el ECG [55, 56]. Es importante el diseño de sistemas criptográficos basados en caos, pero más importante es mostrar que son seguros y eficientes.

El algoritmo de cifrado propuesto utilizado en este trabajo, se basa en las siguientes características criptográficas [57]:

- **Cifrado simétrico**. El algoritmo utiliza la misma clave secreta para cifrar y descifrar.
- **Arquitectura de confusión y difusión**. El algoritmo utiliza procesos para cambiar de posición y cambiar de valor a cada elemento claro en una sola operación.
- **Cifrado a flujo**. El algoritmo cifra cada elemento del texto claro, uno a la vez hasta terminarlo.
- **Cifrado no convencional**. El algoritmo utiliza secuencias caóticas del mapa 2D Seno-Logístico, que son determinadas por la clave secreta de 192 bits para generar secuencias pseudoaleatorias para realizar el proceso de confusión y difusión.

En la figura 6.3, se muestra el diagrama a bloques del proceso de cifrado propuesto, el cual se basa en [56]. El mapa 2D Seno-Logístico 2 se itera en base a la clave secreta, después se obtiene el valor de Z relacionado con la señal clara y secuencias caóticas del mapa 2D Seno-Logístico 2, posteriormente se itera el mapa 2D Seno-Logístico 1 en base a la clave secreta y el valor de Z para realizar los proceso de confusión y difusión sobre la señal clara y finalmente se agrega el valor de Z al criptograma para que el usuario autorizado pueda descifrar correctamente la información.

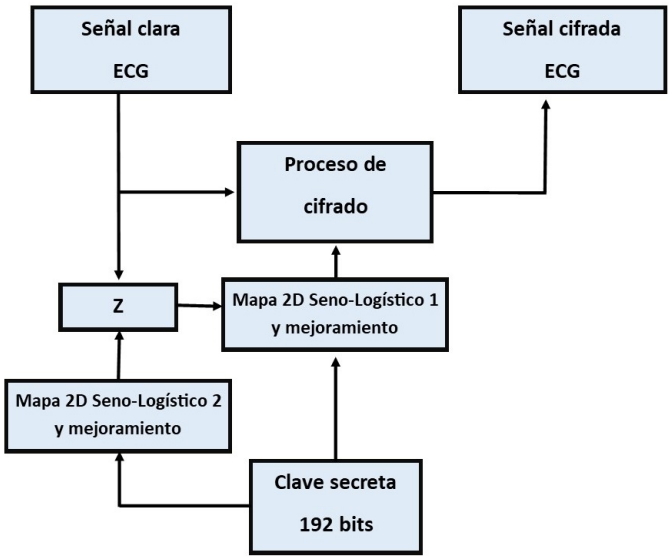


Figura 6.3: Diagrama a bloques del proceso de cifrado.

El proceso de descifrado consta en invertir el proceso de cifrado. En la figura 6.4, se muestra el diagrama a bloques del proceso de descifrado. Primero el valor de Z se extrae del criptograma (Z no se calcula ni se iteran datos caóticos del mapa 2), después 1000 datos caóticos son calculados del mapa 2D Seno-Logístico 1 con el uso de la clave secreta y el valor de Z, finalmente, se realiza los proceso de confusión y difusión inversos para recuperar la señal clara.

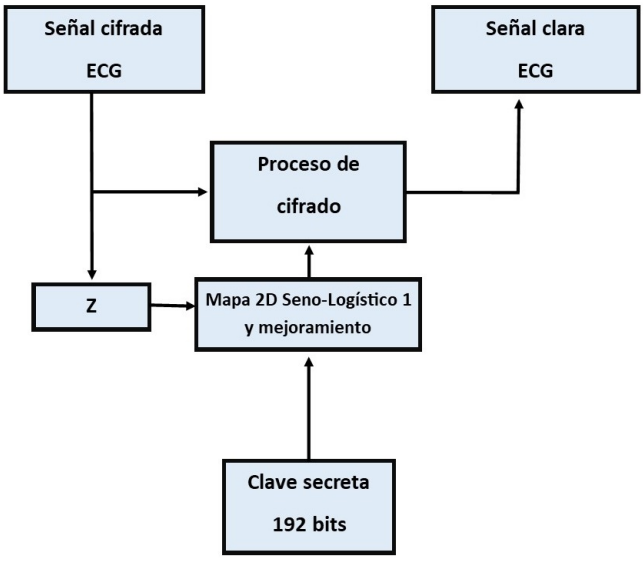


Figura 6.4: Diagrama a bloques del proceso de descifrado.

6.2. Algoritmo de cifrado caótico

El algoritmo de cifrado caotico propuesto esta basado en [56], donde se utiliza la arquitectura de confusión y difusión para el cifrado de señales biomédicas.

6.2.1. Definición de la clave secreta

La clave secreta está definida como una secuencia de 192 bits, caracterizada por 48 caracteres hexadecimales $K \in (0-9, A-F)$; la cual es dividida en 6 secciones (A, B, C, D, E, F). Las condiciones iniciales y el valor de los parámetros de control son calculados de manera indirecta mediante la clave secreta. En la tabla 6.1 se muestran los cálculos correspondientes.

Clave secreta	Parámetro de control			Condiciones iniciales	
48 dígitos Hex	$H_1, H_2, \ldots, H_{48}$ donde $H \in [0-9, A-F]$				
Cálculos	$A = \frac{(H_1, H_2, \ldots, H_8)_{10}}{2^{32}+1}$	$B = \frac{(H_9, H_{10}, \ldots, H_{16})_{10}}{2^{32}+1}$	$C = \frac{(H_{17}, H_{18}, \ldots, H_{24})_{10}}{2^{32}+1}$		
	$D = \frac{(H_{25}, H_{26}, \ldots, H_{32})_{10}}{2^{32}+1}$	$E = \frac{(H_{33}, H_{34}, \ldots, H_{40})_{10}}{2^{32}+1}$	$F = \frac{(H_{41}, H_{42}, \ldots, H_{48})_{10}}{2^{32}+1}$		
2D Seno-Logístico 1	$\mu_1 = 0.1 + [((A+B+Z) \ mod \ 1) * 0.01]$			$x_{1_0} = (C+D+Z) \ mod \ 1$	$y_{1_0} = (E+F+Z) \ mod \ 1$
2D Seno-Logístico 2	$\mu_2 = 0.1 + [((A+B) \ mod \ 1) * 0.01]$			$x_{2_0} = (C+D) \ mod \ 1$	$y_{2_0} = (E+F) \ mod \ 1$

Tabla 6.1: Clave secreta.

6.2.2. Calculo de Z

El valor Z incrementa la sensibilidad a pequeños cambios en la señal clara y a la clave secreta a nivel de bit. Al utilizar el valor de Z hace que el proceso de cifrado sea robusto ante ataques diferenciales como texto claro conocido y ataque de texto claro elegido. Para determinar el valor de Z, todos los elementos de la señal clara se suman con la secuencia de datos caóticos del mapa 2D Seno-Logístico 2. Primero, el mapa 2D Seno-Logístico 2 es iterado I_2 veces con el parámetro de control μ_2 y condiciones iniciales x_{2_0}, y_{2_0} para generar una secuencia caótica de datos $x^{SL2} = x_1^{SL2}, x_2^{SL2}, x_3^{SL2}, \ldots, x_{I_2}^{SL2}$ y $y^{SL2} = y_1^{SL2}, y_2^{SL2}, y_3^{SL2}, \ldots, y_{I_2}^{SL2}$ con $x^{SL2} \in (0,1)$ y una precisión decimal de 10^{-15}.

Posteriormente, la secuencia caótica x^{SL2} es mejorada en uniformidad (ver figura 6.5) con la siguiente expresión:

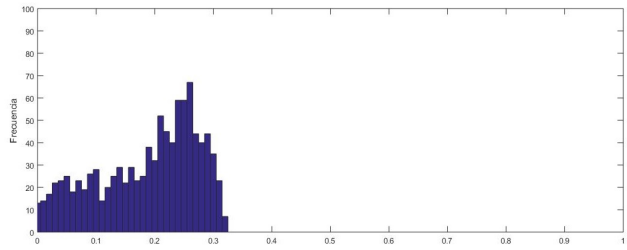
$$x_i^{SL2} = \left(x_i^{SL2} * 1000\right) \quad (\text{mód } 1), \quad para \ i = 1, 2, 3, \ldots, I_2, \tag{6.1}$$

donde I_2 es el número de iteraciones del mapa 2D Seno-Logístico 2 y *mód* es la operación de módulo.

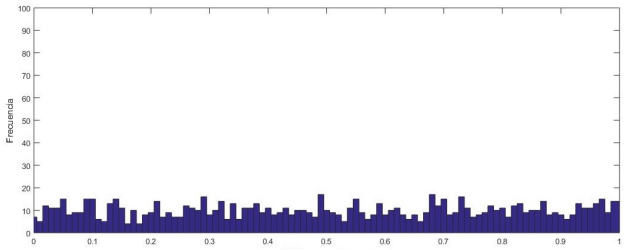
Después, todos los elementos de la señal clara se suman con x^{SL2} como sigue

$$S1 = \left\{S1 + [P_i * x_i^{SL2}] + x_i^{SL2}\right\} \quad (\text{mód } 1), \quad para \ i = 1, 2, 3, \ldots, I_2, \tag{6.2}$$

donde P_i representa el elemento i de la señal clara, $S1$ es una variable inicializada en cero y x^{SL2} corresponde a la secuencia caótica.



(a)



(b)

Figura 6.5: Distribución de 1000 valores del mapa 2D Seno-Logístico con una separación de 0.01: (a) datos del mapa directo y (b) datos del mapa mejorado.

6.2.3. Proceso de cifrado

El mapa 2D Seno-Logístico 1 se itera $I_1 = 1,000$ veces con valores μ_1, x_{1_0} y y_{1_0} tomados de la tabla 6.1, para generar la segunda secuencia caótica de datos $x^{SL1} = x_1^{SL1}, x_2^{SL1}, x_3^{SL1}, \ldots, x_{I_1}^{SL1}$ y $y^{SL1} = y_1^{SL1}, y_2^{SL1}, y_3^{SL1}, \ldots, y_{I_1}^{SL1}$ con $x^{SL1} \in (0,1)$ y una precisión decimal de 10^{-15}.

Posteriormente, la secuencia x^{SL1} es mejorado con la siguiente expresión:

$$x_i^{SL1} = \left(x_i^{SL1} * 1000\right) \quad (\text{mód } 1), \quad para\ i = 1, 2, 3, \ldots, I_1, \tag{6.3}$$

donde I_1 es el número de iteraciones para el mapa 2D Seno-Logístico 1.

De la secuencia caótica x^{SL1} se determinan dos subsecuencias para los procesos de confusión y difusión. Para el proceso de confusión la subsecuencia se calcula con la siguiente expresión:

$$CF_i = \ round\left[x_{I_1-\ell+i}^{SL1} * (\ell - 1)\right] + 1, \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{6.4}$$

donde ℓ es la longitud requerida y $CF \in (1, \ell)$ es el vector pseudoaleatorio para realizar el proceso de confusión. En un proceso de confusión eficiente, todos los elementos del texto claro se deben permutar entre sí mismos; sin embargo, la ec.(6.4) genera valores para reposicionamiento repetido. Por tanto, los valores repetidos de CF son cambiados mediante programación como sigue

$$G_h = [K_h], \quad con\ h \ll \ell, \tag{6.5}$$

donde K_h es el valor que no está en CF ordenados de menor a mayor. El vector de valores repetidos G se divide en dos secciones y cada valor se asigna a CF de manera alternada donde un valor repetido aparece. Cuando este proceso termina, se tiene un vector para confusión con todas las posibles posiciones (confusión optimizada).

Una subsecuencia para difusión se determina de x^{SL1} de la misma longitud ℓ. Aunque el mapa de 2D Seno-Logístico presenta una mejor distribución de los datos, aún hay tendencias marcadas hacia ciertos valores, lo cual puede llevar en un proceso de difusión ineficiente. Una solución a este problema es eliminar los primeros tres decimales de los datos caóticos, proceso que se realiza sólo para una longitud determinada por ℓ y generar un proceso de difusión optimizado. La subsecuencia para difusión se calcula como

$$DF_i = \left(x^{SL1}_{I_1-\ell+i} + Z\right) \quad (\text{mód } 1), \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{6.6}$$

donde $DF_i \in (0, 1)$ es el vector pseudoaleatorio para el proceso de difusión con longitud ℓ.

El proceso de cifrado se calcula con la siguiente expresión

$$E_i = P(CF_i) + DF_i, \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{6.7}$$

donde P es la señal clara y E_i es el criptograma.

El valor de Z debe ser incluido en el criptograma para que el usuario autorizado pueda descifrar correctamente, ya que no se puede calcular directamente de E.

6.2.4. Proceso de descifrado

El proceso de descifrado consiste en invertir todos y cada uno de los pasos desarrollados en el cifrado. Se debe utilizar exactamente la misma clave de 192 bits, ya que si un bit cambia, no se podrá recuperar el mensaje claro correctamente.

Primero, el valor de Z debe ser recuperado. Después, el mapa 2D Seno-Logístico 1 es iterado $1,000$ veces con la clave secreta y el valor de Z. Posteriormente, se calculan las subsecuencias CF y DF para confusión y difusión, respectivamente. Finalmente, el descifrado se realiza con la siguiente expresión

$$D(CF_i) = E_i - DF_i, \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{6.8}$$

donde E_i es el criptograma y D es el mensaje recuperado.

6.2.5. Características de seguridad y eficiencia

El algoritmo de cifrado caótico propuesto en este trabajo de tesis, posee ciertas características de seguridad que aportan robustez ante los ataques criptoanalíticos.

Estas características se muestran a continuación:

1. **Inicialización de secuencias caóticas**. La condición inicial y parámetro de control del mapa 2D Seno-Logístico, se determinan de manera indirecta a partir de una clave de 192 bits.

2. **Mejoramiento de secuencias caóticas**. Los datos caóticos del mapa 2D Seno-Logístico son modificados mediante una simple operación para generar una mejor distribución, lo que genera mejores procesos de confusión y difusión. Por tanto, un criptograma con mejores propiedades estadísticas.

3. **Cálculo del Z**. Al considerar las características del texto claro para realizar el proceso de cifrado, se incrementa por mucho la sensibilidad a pequeños cambios (nivel de bit) en el texto claro. Además, se utilizan datos caóticos de un segundo mapa 2D Seno-Logístico para evitar ataques de sólo texto claro elegido (seleccionar un texto claro en ceros y cancelar el valor de Z en el cifrado). Por tanto, este proceso ayuda a dar robustez al algoritmo criptográfico ante los ataques más poderosos que han quebrantado múltiples algoritmos criptográficos basados en caos.

4. **Confusión y difusión optimizados**. Los vectores para cifrado se calculan de tal forma que la confusión es 100 % aplicada en todo el texto claro. Mientras, el proceso de confusión se aplica sobre el texto claro con datos caóticos que presentan una distribución uniforme, lo que genera un cifrado con excelentes características estadísticas.

5. **Eficiencia de cifrado**. Este sistema caótico posee ventajas de implementación tanto en velocidad de generación de datos como poco espacio de memoria requerido. Además, los procesos de confusión y difusión son aplicados a la señal clara en un mismo proceso.

6.3. Conclusiones

Un algoritmo criptográfico basado en caos debe cumplir con varios aspectos de seguridad para que pueda ser implementado en sistemas embebidos. En este capítulo, se describió el algoritmo criptográfico basado en caos propuesto para este trabajo de tesis, el cual utiliza una clave de 192 bits y se mencionan las características de seguridad y eficiencia que lo componen.

Capítulo 7

Implementación de cifrado caótico en microcontrolador

Se describe la implementación en microcontrolador de 32 bits del algoritmo de cifrado propuesto utilizado para este trabajo de tesis, para brindar confidencialidad a señales biomédicas en sistemas embebidos. Se verifica la seguridad y eficiencia mediante distintos análisis de seguridad como espacio de claves, sensibilidad a la clave y señal clara, histogramas, correlación, entropía de la información y tiempo de cifrado. Todos los análisis, muestran y verifican que el algoritmo de cifrado con el mapa 2D Seno-Logístico, puede implementase en sistemas embebidos para cifrado de señales de electrocardiograma con alta seguridad.

7.1. Revisión de la literatura

La implementación en microcontroladores de algoritmos criptográficos basados en caos es reciente. En los últimos años, este tipo de trabajos se ha incrementado con el tiempo. Los primeros trabajos se mencionan en [58, 59], donde se realizó una implementación en un microcontrolador Atmel AVR de un algoritmo de cifrado basado en caos, donde se utiliza el mapa generalizado de Hénon y la arquitectura de confusión y difusión para cifrar texto alfanumérico, pero no se respalda el procedimiento de cifrado con un análisis de seguridad.

Recientemente en [60], se implementaron osciladores caóticos en sistemas embebidos Se presentan estudios utilizando como base sistemas caóticos de naturaleza discreta y sistemas caóticos en tres dimensiones en sus versiones continuas y discretas. Además, se realiza un estudio para reproducir los algoritmos numéricos en versión discreta utilizando microcontroladores PIC de 8 bits, dsPIC de 16 bits, PIC32 de 32 bits y un FPGA Altera. Se incluyen resultados analíticos, numéricos y experimentales en cada uno de estos estudios reportados.

En [61–63] se ha utilizado cifrado caótico para texto, imágenes y huellas dactilares. Se utilizá el mapa 1D logístico y se implementó en un sistema embebido utilizando

un microcontrolador de 32 bits donde el algoritmo utilizado fue sometido a distintos análisis de seguridad.

7.2. Resultados experimentales

El algoritmo de cifrado se implementa en un microcontrolador de 32 bits con procesador COLDFIRE de Freescale (M52259DEMOKIT) que tiene una frecuencia de operación hasta 80 MHz [64]. Se utiliza el software CodeWarrior para Colfire V7.1 para realizar la programación en lenguaje C y también, se usan librerías de MQX 3.5 para almacenar datos en memoria flash. El programa del algoritmo de cifrado es almacenado en memoria flash del microcontrolador. Para los análisis de seguridad se utiliza la plataforma de MatLab V8.5 (R2015a) en una computadora laptop con procesador Intel Core 1.70 GHz, 4 GB de RAM y sistemas operativo Windows 10 de 64 bits; se utiliza representación punto flotante con precisión doble (64 bits) y una precisión de 10^{-15}. La clave secreta de 48 dígitos hexadecimales y la señal clara son introducidas en el microcontrolador por programación.

Se utiliza $1122334455667889900AABBCCDDEEFF1122334455667788$ como clave secreta y la señal ECG (ver figura 7.1) se utiliza como señal clara, una vez que la señal es cifrada por el microcontrolador, éste se extrae con memoria flash para realizar los distintos análisis de seguridad lógicos en MatLab. La figura 7.2, muestra el criptograma extraído del microcontrolador.

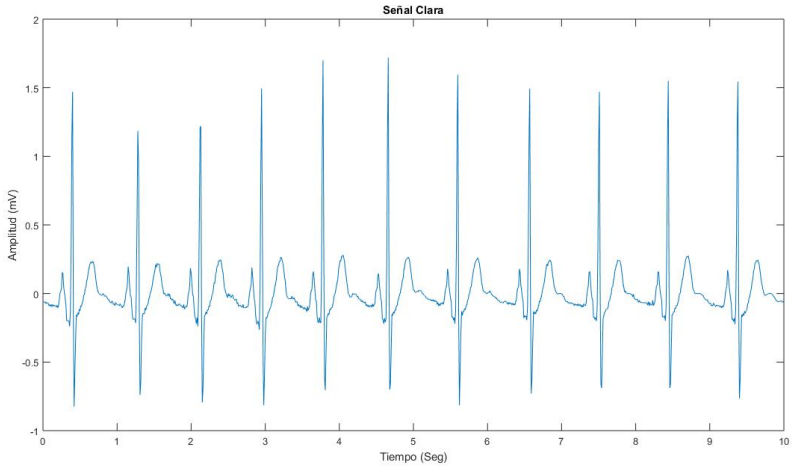


Figura 7.1: Señal clara de electrocardiograma.

Se obtuvo la señal clínica de un ECG de una base de datos de internet PhysioBank ATM *(www.physionet.org)*, la cual se usa para conocer la respuesta del algoritmo criptográfico. El Electrocardiograma (ECG), tiene una duración de 10 segundos, una amplitud en milivolts, ganancia de 200 y frecuencia de muestreo Fs= 100 Hz.

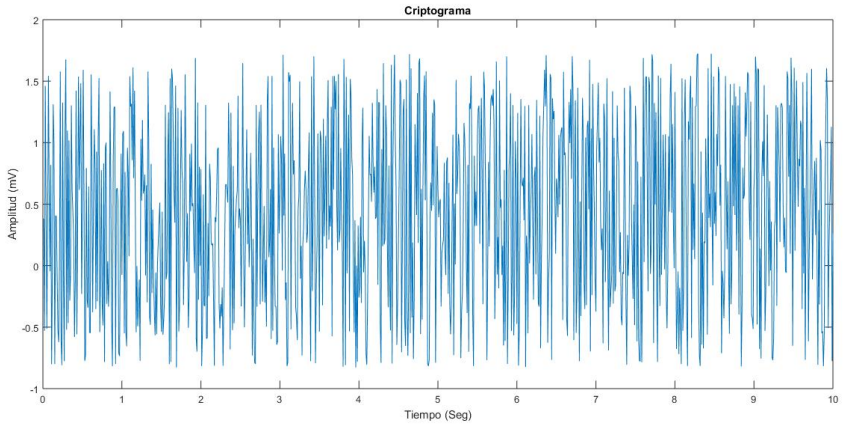


Figura 7.2: Señal encriptada de electrocardiograma.

El proceso del cifrado caótico propuesto en el capítulo 6, se realiza de la siguiente manera:

1. **Definir la clave secreta**.
   Se utiliza una clave secreta de 192 bits definida por 48 caracteres hexadecimales. Esta se divide en seis secciones para la inicializacion de secuencias caóticas de dos mapas 2D Seno-Logístico.

2. **Transformación**.
   El sistema criptográfico (digital) obtiene la señal clara y determina máximos-mínimos para transformar las amplitudes de la misma en amplitudes con valores entre $(0, 1)$. Para obtener una nueva señal clara transformada, se determina el valor de A con $P_{min} = min(A)$, donde $P_{min} \in R$ es un escalar que representa el valor mínimo de A y min representa la función para determinar el valor mínimo de A. También se encuentra el valor máximo en A con $P_{max} = max(A)$, donde $P_{max} \in R$ es un escalar que representa el valor máximo en A y max representa la función para determinar el valor máximo de A. Después se determina la siguiente transformación:
   $$AT = \frac{A - (P_{min} - 0.01)}{P_{max} + 0.01} \tag{7.1}$$
   donde AT representa la señal clara transformada en valores entre $(0, 1)$.

3. **Valor** Z.
   Todos los valores de la señal clara AT se suman con datos caóticos del mapa 2D Seno-Logístico 1 iterado $I = 1000$, con μ_2, x_2 y y_2. Los elementos de AT y datos caóticos se suman como sigue:
   $$Z = Z + (AT_i + x^{SL2}_{I+1-i}) \quad (\text{mód } 1), \tag{7.2}$$
   donde $i = 1, 2, 3, .., \ell, Z \in (0, 1)$ es una variable inicializada en cero para incrementar la seguridad. AT_i son los elementos de la señal clara transformada y x^{SL2}

es la secuencia caótica del mapa 2D Seno-Logístico.

4. **Cifrado**.
El mapa 2D Seno-Logístico 1 es iterado $T = 1000$ con μ_1, x_1 y y_1. Se determina una secuencia para permutación.

$$P_i = round(x_{T+i}^{SL1} * (\ell - 1)) + 1, \tag{7.3}$$

donde $i = 1, 2, 3, .., \ell, P \in [1, \ell]$ es el vector pseudoaleatorio de permutación y *round* es la operación de redondeo al valor más cercano. Sin embargo, P tiene valores repetidos que son determinados por software y remplazados por los faltantes de forma automática para incrementar la seguridad. El vector para el proceso de difusión se determina de la siguiente forma:

$$D_i = (x_{T+i}^{SL1} * 1000) + Z \pmod 1, \tag{7.4}$$

donde $i = 1, 2, 3, .., \ell, D_i \in (0, 1)$. La multiplicación por 1000 se utiliza para obtener una distribución de datos del mapa 2D Seno-Logístico más uniforme.

Finalmente el proceso de cifrado se realiza con la siguiente operación:

$$C_i = (AT(P_i) + D_i) \pmod 1, \tag{7.5}$$

donde $i = 1, 2, 3, .., \ell, C \in (0, 1)$ es el criptograma.

5. **Agregar datos al criptograma**.
El valor de P_{min}, P_{max} y Z son agregados al final del criptograma de la siguiente forma:

$$\begin{aligned}
&C_{\ell+1} = Z, \\
&C_{\ell+2} = 1 \quad si \quad P_{min} < 0 \quad o \quad C_{\ell+2} = 0 \quad si \quad P_{min} \geq 0, \\
&C_{\ell+3} = abs(P_{min})/1000, \\
&C_{\ell+4} = 1 \quad si \quad P_{max} < 0 \quad o \quad C_{\ell+4} = 0 \quad si \quad P_{min} \geq 0, \\
&C_{\ell+5} = abs(P_{max})/1000,
\end{aligned}$$

donde *abs* representa el valor absoluto.

6. **Descifrado**.
El proceso de descifrado consiste en invertir los pasos de cifrado. Para ello, se debe obtener del criptograma los valores de Z, P_{min}, P_{max}. Con el uso de la misma clave secreta, se calculan los vectores pseudoaleatorios de P y D de la misma forma que en el paso 4. El proceso de descifrado se determina como sigue

$$D(P_i) = (C_i - D_i), \quad \pmod 1, \tag{7.7}$$

donde $i = 1, 2, 3, .., \ell$ y $D \in (0, 1)$ es la señal clara transformada descifrada. Para obtener la señal clara con amplitudes originales, se escala D con el uso de P_{min} y P_{max}.

7.3. Sistema embebido utilizado en esta tesis

Para el encriptado y desencriptado de los datos se utiliza el microcontrolador mencionado en la sección 5.2, para desplegar la información e indicaciones se utiliza una pantalla LCD 20X4 matrix orbital modelo LK204-25, los datos son almacenados en la memoria flash interna del microcontrolador con capacidad de 512KB y una memoria flash externa para almacenar de igual manera la información cifrada (criptogramas) y para las salidas digitales se utilizan los puertos GPIO de la pantalla LCD (activar alarmas y LEDs).

En la figura 7.3, se muestra el diagrama a bloques del funcionamiento del sistema embebido propuesto para la parte experimental de este trabajo de tesis, donde se indica la forma en que se conectan y comunican los módulos.

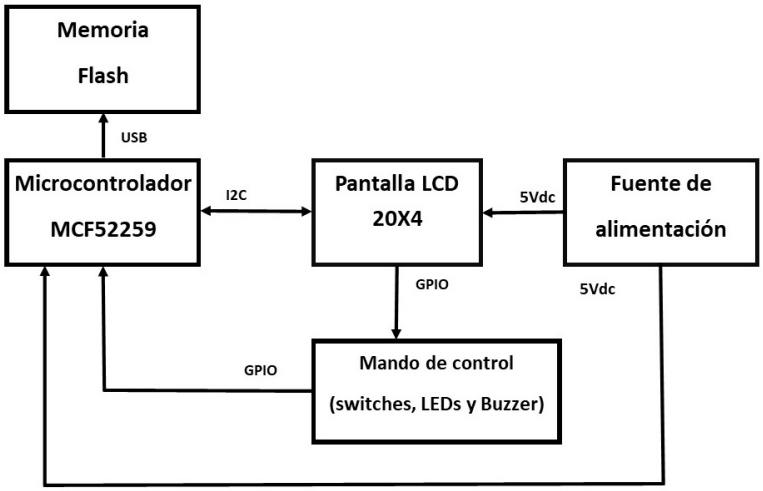


Figura 7.3: Diagrama a bloques del sistema embebido.

El sistema embebido está formado por cuatro módulos independientes, cada una con funciones específicas y controladas directa o indirectamente por la tarjeta de desarrollo MCF5229DEMOKIT:

- **Microcontrolador**. El programa del sistema se ejecuta en este módulo, al iniciar, se establece la comunicación I2C y configura los puertos de entrada y salida. Despliega información en la LCD y reconoce los comandos que solicita el usuario por el mando de control, ya se para encriptar información o desencriptar.
- **Fuente de alimentación**. Se encarga de proporcionar el voltaje para el microcontrolador, LCD y activar los puertos GPIO.
- **Mando de control**. En este módulo se tienen los switches, con los cuales se selecciona si se quiere encriptar (switch 2) o desencriptar (switch 1) (ver figura 7.4).

También tiene 3 LEDs como indicadores, amarillo indica que se ha presionado un switch, el verde indica que se está haciendo un proceso ya sea encriptar o desencriptar y rojo indica que el proceso ha finalizado y la información (criptograma) se ha guardado de forma correcta (ver figura 7.5). Además cuenta con un buzzer el cual suena cuando se presiona un switch y cuando finaliza la operación que se está realizando.

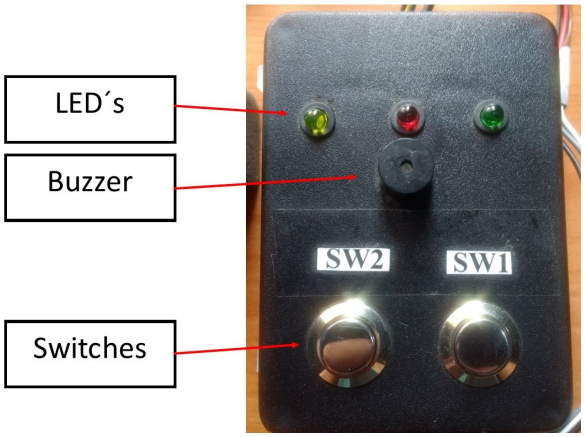


Figura 7.4: Mando de control utilizado.

(a) (b) (c)

Figura 7.5: Funciones de los LEDs del sistema de control: a) LED amarillo indica inicio del proceso, b) LED rojo indica fin del proceso y c) LED verde indica que el proceso se está ejecutando

- **Pantalla LCD 20x4**. La pantalla es un módulo de doble circuito, en el segundo circuito se encuentran los pines de alimentación, comunicaciones y puertos GPIO; este módulo recibe órdenes del microcontrolador por comunicación I2C, en la pantalla se despliegan los mensajes para dar información, indicaciones y de la actividad que está realizando el programa principal. Se usan los GPIO como salidas para los LEDs indicadores y el buzzer, ubicados en el mando de control.

En la figura 7.6, se tiene una fotografía del sistema funcionando y se ubican los módulos del sistema.

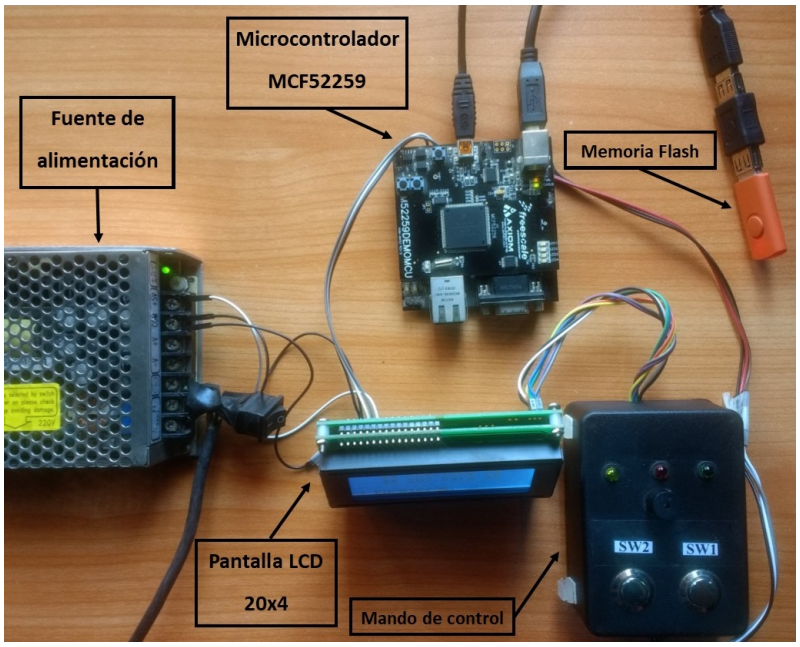
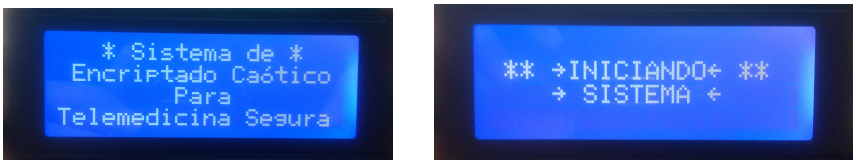


Figura 7.6: Sistema embebido funcionando.

A continuación se muestra el funcionamiento del sistema embebido para encriptar y desencriptar.

Inicio de sistema:

Al inicio se muestra un mensaje de inicio por unos 8 segundos. Después, aparece otro mensaje que indica que el sistema está iniciando (cuando aparece este mensaje en el mando de control los tres LEDs parpadean tres veces y el buzzer se activa indicando que el sistema está listo para funcionar) y se procede al siguiente paso, el cual es encriptar.



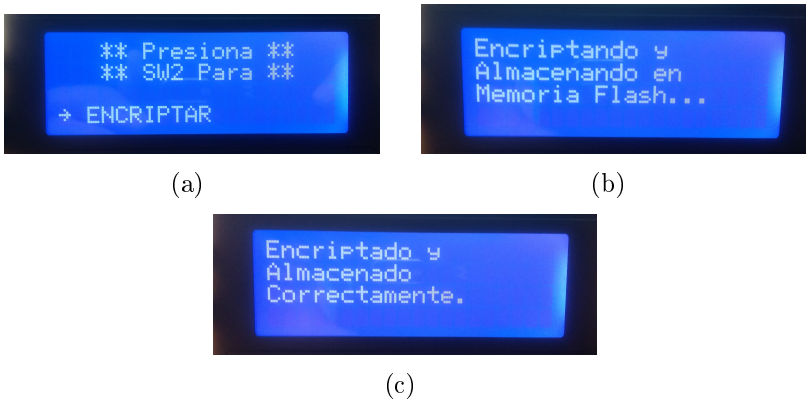
(a) (b)

Figura 7.7: Pantallas de inicio del sistema: a) mensaje de inicio del sistema embebido y b) índica que se está iniciando el sistema.

Encriptado:

Para el proceso de encriptado aparece un mensaje, el cual indica que se debe presionar el switch 2 para realizar el proceso de encriptado (se explica en la Sección 6.1). Cuando se presiona el switch 2, la pantalla cambia y dice que se está encriptando y

almacenando la información, mientras el LED amarillo enciende una vez junto con el buzzer y el LED verde parpadea cinco veces indicando que se está realizando el proceso. Cuando este proceso finaliza, se muestra en la LCD que la información se encriptó y se almacenó correctamente, el buzzer suena y el LED rojo parpadea indicando que el proceso de encriptado ha finalizado con éxito (ver figura 7.8). Los datos (criptograma y clave secreta) se guardan en un arhivo .txt.



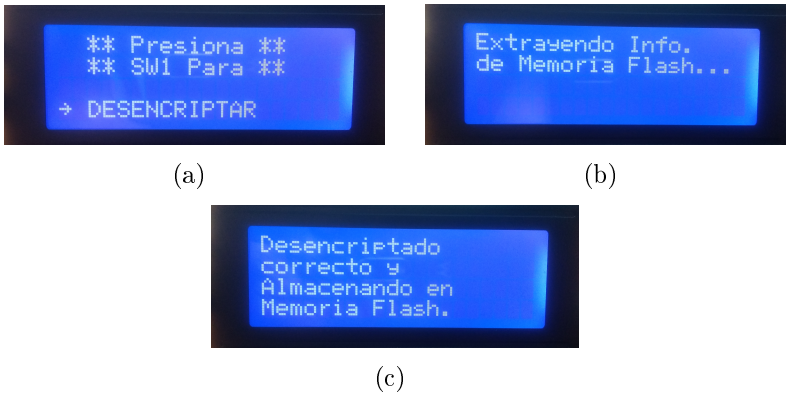
(a) (b)

(c)

Figura 7.8: Proceso de encriptado: a) índica que se debe presionar el SW2 para encriptar, b) índica que se está encriptando la información y c) índica que ha finalizado el proceso de encriptamiento.

Desencriptado:

Para el proceso de desencriptado aparece un mensaje, el cual indica que se debe presionar el switch 1 para realizar el proceso de desencriptado (se explica en la Sección 6.1). Cuando se presiona el switch 1, la pantalla cambia y dice que se está extrayendo la información de la memoria flash para realizar el desencriptando, el LED amarillo enciende una vez junto con el buzzer y el LED verde parpadea cinco veces indicando que se está realizando el proceso. Cuando finaliza, se muestra en el LCD que la información se desencriptó y se almaceno correctamente, el buzzer suena y el LED rojo parpadea indicando que el proceso de desencriptado ha finalizado (ver figura 7.9).



(a) (b)

(c)

Figura 7.9: Proceso de desencriptado: a) índica que se debe presionar el SW1 para desencriptar, b) índica que se está extrayendo la información y c) índica que ha finalizado el desencriptamiento.

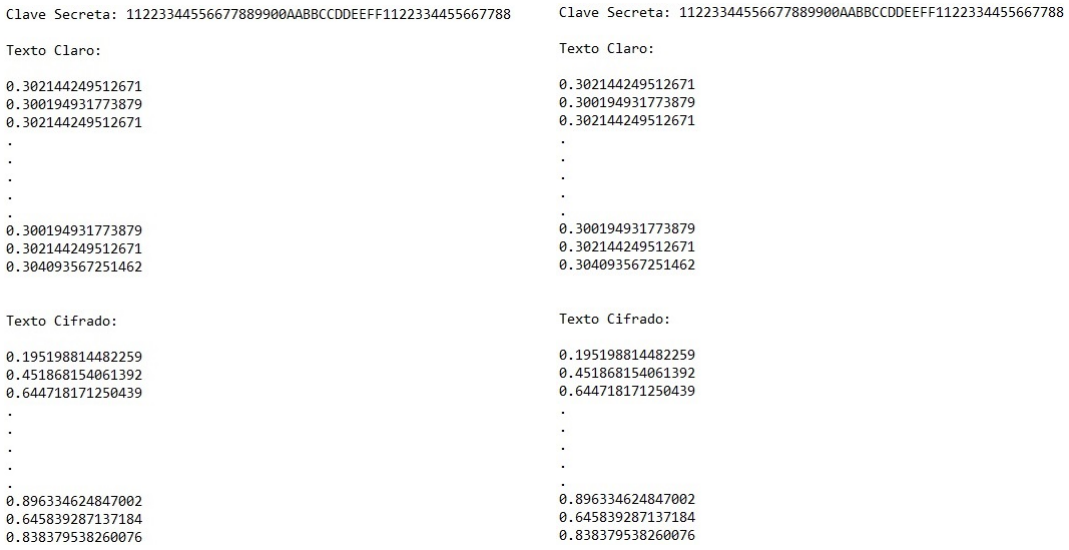


Figura 7.10: Archivos *.txt obtenidos de memoria USB de los proceso de encriptado y desencriptado correspondiente a un ECG de 1000 datos: a) archivo obtenido del proceso de encriptado y b) archivo obtenido del proceso de desencriptado.

Al utilizar sistemas embebidos se debe pensar en la seguridad de la información contenida en el dispositivo y la transmitida por redes como internet. El diseño de un producto que incorpora sistemas embebidos generalmente está orientado a minimizar los costos y maximizar la confiabilidad, por lo que se deben incluir funciones criptográficas, diseño de protocolos y consultoría en análisis y verificación, así como servicios de pruebas de seguridad y evaluaciones específicas.

Como sucede con la mayoría del equipamiento industrial, los sistemas embebidos están pensados para ser seguros a nivel físico, incorporando medidas de reinicio en caso de fallo (watchdog), partes de hardware duplicadas, programación inmune a fallos, etc. A todas las debilidades lógicas hay que sumarle las posibles opciones físicas, ya que la apertura del dispositivo para su análisis y posterior ataque siempre está presente. Estos sistemas embebidos no suelen disponer de mecanismos de detección de apertura, así como tampoco de eliminación de puertos de test utilizados en la fase de diseño del hardware.

Las razones para aplicar medidas de seguridad a los sistemas embebidos son muchas. Del lado del fabricante caen algunas, sobre todo las relacionadas con aspectos físicos; pero por el lado del usuario también se pueden hacer cosas para mejorar la seguridad. Por ello, en este trabajo se implanta un algoritmo de cifrado caótico en el microcontrolador mediante programación para la encriptación de señales de electrocardiograma.

7.4. Análisis de seguridad

7.4.1. Espacio de claves

Todo sistema criptográfico es susceptible a un ataque exhaustivo (consiste en probar cada una de las posibles claves secretas hasta encontrar la señal clara), donde cada posible clave secreta se utiliza para descifrar un criptograma. Si el espacio de claves es pequeño, es decir, menor a 2^{56} posibilidades, el sistema criptográfico no es seguro ante un ataque exhaustivo o de fuerza bruta. Para proporcionar seguridad suficiente contra un ataque exhaustivo, el espacio de claves debe ser mayor a 2^{100} sugerencia reportada en la referencia [65]. Además, cada clave secreta se debe considerar fuerte, es decir, que genere secuencias caóticas y no periódicas. La clave secreta propuesta consiste de 48 dígitos hexadecimales (192 bits) y todas se consideran fuertes, por tanto, el algoritmo propuesto en esta tesis utiliza un espacio de claves de 2^{192} y puede resistir un ataque exhaustivo.

7.4.2. Sensibilidad a clave secreta

Alvarez y Li [65], mencionan que un algoritmo de cifrado debe ser altamente sensible a la clave secreta, incluso a nivel de bit. Esta propiedad aplica para el proceso de cifrado y descifrado; en el proceso de cifrado, si la misma señal clara es cifrado dos veces con dos claves secretas similares (un bit de diferencia), el texto cifrado debe ser muy diferente entre ellos y tener nula correlación; mientras que, en el proceso de descifrado, únicamente la clave secreta correcta puede recuperar el mensaje original.

En esta sección, la sensibilidad de la clave secreta en el proceso de cifrado y descifrado, se prueba y verifica con 2 claves secretas similares (ver tabla 7.1). Para la prueba, la CLAVE 1 y CLAVE 2 generan diferentes criptogramas. Se hace el proceso de correlación de acuerdo con la sección 7.4.5, se explica que para tener correlación nula el valor debe ser muy cercano a 0.

El valor obtenido de la correlación del criptograma de la CLAVE 1 y la CLAVE 2 es de 0.027317915560573, por lo que se puede decir que hay una correlación nula. Por tanto, el algoritmo de cifrado caótico utilizado en esta tesis, es altamente sensible a la clave secreta en proceso de cifrado.

No. clave	Clave secreta
CLAVE 1	11223344556677889900AABBCCDDEEFF1122334455667788
CLAVE 2	11223344556677889900AABBCCDDEEFF**2**1122334455667788

Tabla 7.1: Claves secretas utilizadas para análisis de sensibilidad a la clave en el cifrado.

7.4.3. Sensibilidad a señal clara

Un buen sistema criptográfico debe ser sensible con respecto a la señal clara, es decir, pequeños cambios (un bit) en el texto claro genera un gran cambio en el texto cifrado; si el algoritmo tiene esta propiedad, el cifrado puede resistir un ataque diferencial, el cual, básicamente es un ataque de texto claro conocido. Dos medidas son utilizadas para determinar la sensibilidad a la señal clara: $NPCR$ (del inglés, *Net Pixel Change Rate*), tasa de cambio de pixel neto y $UACI$ (del inglés, *Unified Avarage Changing Intensity*), promedio unificado de cambio de intensidad.

Para resistir un ataque diferencial, se requiere que el algoritmo criptográfico presente sensibilidad a pequeños cambios en la señal clara y se utilizan dos conceptos para determinarlo: NPCR y UACI.

NPCR se calcula con la siguiente expresión:

$$NPCR = \frac{\sum_{i=1}^{\ell} W(i)}{\ell} \times 100 \tag{7.8}$$

con

$$W(i) = \begin{cases} 0 & \text{if } E_1(i) = E_2(i) \\ 1 & \text{if } E_1(i) \neq E_2(i) \end{cases} \tag{7.9}$$

y el valor de UACI se determina con

$$UACI = \frac{100}{\ell \times 95} \sum_{i=1}^{\ell} |E_1(i) - E_2(i)| \tag{7.10}$$

donde ℓ es la longitud del texto, E_1 and E_2 son los dos criptogramas. El proceso para determinar los valores es como sigue: primero, la señal clara se cifra con la CLAVE 1 para generar E_1; después, el bit número 100 de la señal clara se cambia de **100** a **101**, y el proceso de cifrado se repite con la misma CLAVE 1 para generar E_2. La tabla 7.2 muestra los resultados de NPCR y UACI con E_1 and E_2. Por tanto, el esquema propuesto es robusto ante ataques diferenciales, ya que el 99 % de los símbolos son diferentes con una diferencia de magnitud en promedio del 33 %.

Prueba	Prueba
NPCR(%)	99.6019
UACI(%)	33.2580

Tabla 7.2: Resultados de análisis diferencial NPCR y UACI.

7.4.4. Histogramas

El histograma muestra la distribución de información mediante una gráfica y representa información estadística. Un sistema criptográfico es susceptible a un ataque de

histogramas y puede resistir si la señal cifrada tiene un histograma uniforme (información impredecible).

El histograma de la señal cifrada debe ser uniforme para resistir un ataque estadístico en el lenguaje que fue cifrado originalmente. El histograma de la señal clara del ECG se muestra en la figura 7.11 y se puede apreciar la característica estadística de la fuente; sin embargo, el histograma de la señal cifrada es más uniforme, como se aprecia en la figura 7.12. Por tanto, el algoritmo criptográfico propuesto es robusto ante un ataque de histograma, ya que no se puede identificar a qué tipo de bioseñal corresponde.

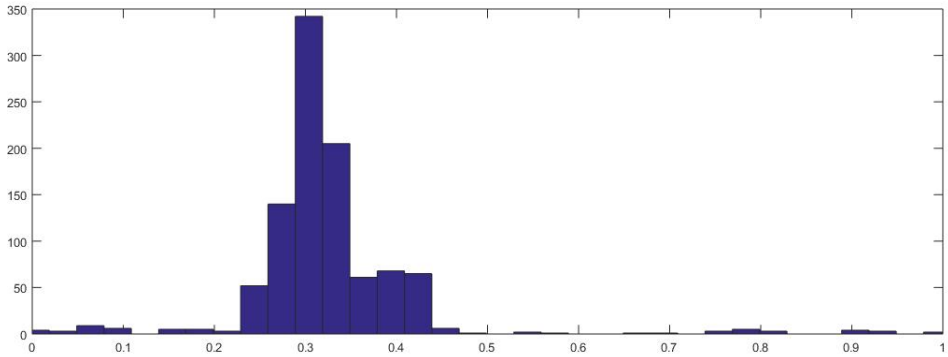


Figura 7.11: Histograma de la señal clara.

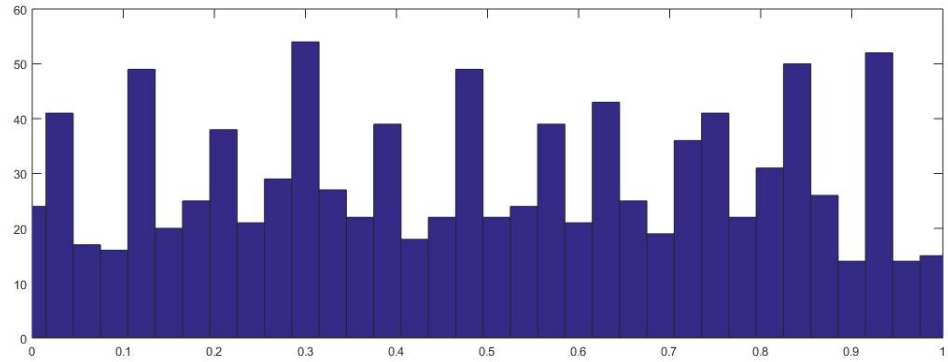


Figura 7.12: Histograma de la señal cifrada.

7.4.5. Correlación

La correlación se puede medir entre -1 y 1, donde 0 significa correlación nula. Un criptoanalista puede utilizar esta información en un ataque estadístico para encontrar la clave secreta y recuperar la señal clara. Por tanto, la señal cifrada debe tener correlación nula.

La fórmula para calcular la correlación es la siguiente

$$Cr = \frac{N \times \sum_{i=0}^{N}(x_i \times y_i) - \sum_{i=0}^{N} x_i \times \sum_{i=0}^{N} y_i}{\sqrt{\left(N \times \sum_{i=0}^{N}(x_i)^2 - \left(\sum_{i=0}^{n} x_i\right)^2\right) \times \left(N \times \sum_{i=0}^{N}(y_i)^2 - \left(\sum_{i=0}^{n} y_i\right)^2\right)}} \tag{7.11}$$

El valor de correlación es $Cr \in (-1, 1)$ donde 0 significa nula correlación y 1 significa alta correlación. Para esta prueba, se generan 50 criptogramas con 50 claves distintas (ver figura 7.13) y se hace la correlación para cada uno. Donde el promedio es de 0.026461839663365, por lo que se puede decir que tiene correlación nula.

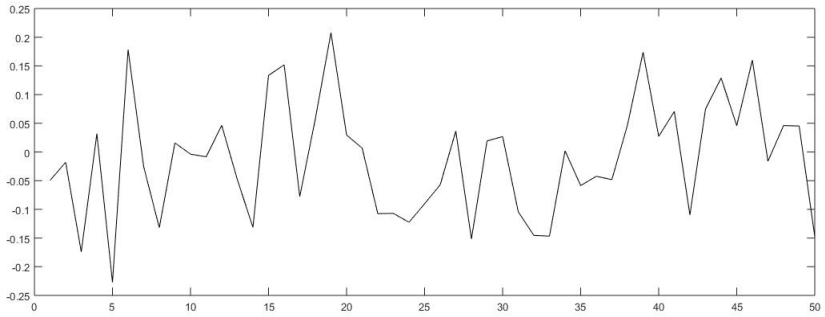


Figura 7.13: 50 muestras de correlación con 50 distintos criptogramas.

7.4.6. Entropía de la información

La *entropía* determina que tan impredecible es un mensaje, es decir, mide cuanto desorden genera el algoritmo de cifrado. Si el proceso de cifrado es bueno, este genera alto desorden en la señal cifrada; por tanto, mayor será la entropía. Caso contrario, si el proceso de cifrado no es suficientemente aleatorio, el algoritmo criptográfico puede estar sujeto a un exitoso ataque de entropía, porque el criptograma es predecible.

En esta sección, el desempeño del cifrado propuesto en la etapa de difusión es probado y verificado. La entropía $H(m)$ de un mensaje m puede calcularse como sigue

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\ log_2(1/p(m_i)), \tag{7.12}$$

donde N es el número de bits que representan la unidad básica del mensaje m, 2^N son todas las combinaciones de la unidad básica, $p(m_i)$ representa una probabilidad de m_i, $\log_2$ es el logaritmo base 2 y la entropía esta expresada en bits, donde la máxima entropía es N. Si un mensaje m es cifrado con 2^N posibles valores, la entropía debería ser idealmente $H(m) = N$, si m es puramente aleatorio.

En este análisis, la señal cifrada entre 0 y 1 se transforma a datos de 8 bits, es decir de 0-255. De manera que, la máxima entropía es de 8. La figura 7.14, muestra

los resultados de la entropía obtenida de 100 criptogramas con 100 claves distintas. El resultado promedio de las 100 muestras es de 7.9210. La entropía de la señal cifrada es cercana a 8, por tanto el proceso de difusión genera alto desorden para resistir un ataque de entropía.

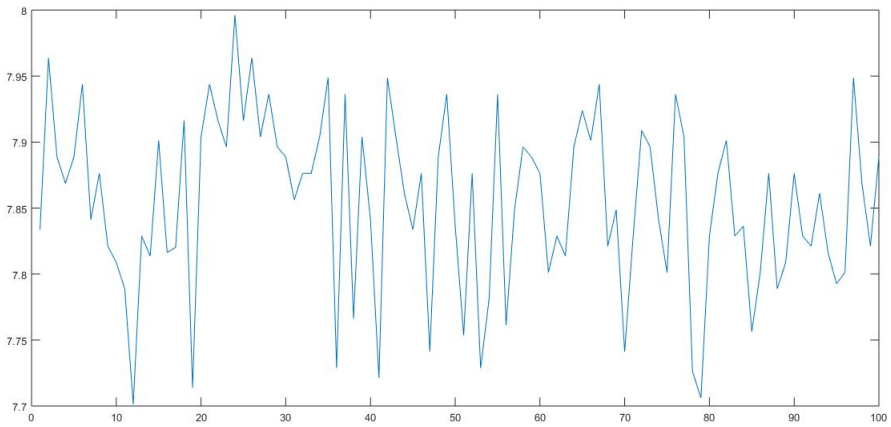


Figura 7.14: 50 muestras de entropía con 50 distintos criptogramas.

7.4.7. Tiempo de cifrado

Un buen algoritmo de cifrado debe ser robusto ante ataques pero además requiere ser rápido para aplicaciones de tiempo real en telemedicina. El tiempo de descifrado es similar al cifrado. La velocidad de cifrado para una señal clara de 10 seg y fs de 100 Hz es de 0.065134 segundos y para el descifrado es de 0.052731 segundos.

7.5. Conclusiones

En este capítulo se presentó el algoritmo criptográfico propuesto basado en caos, el cual fue implementado en un microcontrolador de 32 bits con el propósito de proteger señales biomédicas utilizadas en telemedicina como el ECG. Un análisis de seguridad completo muestra la efectividad de la implementación y la seguridad que brinda el algoritmo criptográfico propuesto por lo que puede utilizarse para proteger la integridad de datos en sistemas embebidos en tiempo real, particularmente para brindar privacidad a señales de ECG.

Los resultados obtenidos muestran que el algoritmo junto con el mapa 2D Seno-Logístico es seguro y eficaz.

Capítulo 8

Conclusiones

8.1. Conclusiones generales

En este trabajo de tesis de licenciatura, se diseñó e implementó en sistema embebido de bajo costo, un algoritmo criptográfico basado en caos para la confidencialidad de señales de ECG en aplicaciones de telemedicina. Se realizó un estudio de seis mapas caóticos: Logístico 1D, Hénon 2D, Logístico 2D, 1D Seno, 1D Chebyshev y Seno-Logístico 2D, de los cuales se obtuvieron el exponente de Lyapunov y con base a sus características de desempeño se eligió el mapa 2D Seno-Logístico para el cifrado caótico, ya que presenta dinámicas hypercaóticas con solo 2 dimensiones y el rango de Lyapunov más extenso.

El algoritmo criptográfico se basó en clave simétrica y arquitectura de permutación y difusión, donde se emplea la misma clave secreta para el proceso de encriptado y desencriptado de información. El sistema embebido utilizó una clave secreta de 48 números hexadecimales (192 bits), la cual es introducida mediante programación junto con el algoritmo criptográfico en el software IDE de Code Warrior, donde se introducen los datos de la señal clara que son cifrados con la clave, los datos encriptados se almacenan en una memoria flash para realizar distintos análisis de seguridad en MatLab. Los resultaron demostraron que el algoritmo criptográfico es seguro para la implementación en sistemas embebidos y para el cifrado de información en telemedicina.

El sistema embebido criptográfico puede ser implementado en hospitales, ambulancias, o en hogares. Para el almacenamiento o transmisión segura de señales ECG de los pacientes.

8.2. Trabajo a futuro

Como trabajo a futuro se plantean las siguientes actividades:

- **Adquisición de señales biomédicas en tiempo real**: Obtener sensado de las señales de electrocardiograma en tiempo real mediante la implementación de un sistema de monitoreo electrónico ECG, de esta manera, los datos podrán ser recabados a partir de los pacientes en tiempo real.

- **Transmitir criptogramas a través de internet**: Realizar programación en el microcontrolador para emplear el conector ethernet y transmitir criptogramas de forma remota.
- **Colocar fuente de alimentación propia al sistema**: Actualmente, se tiene una fuente de alimentación para el sistema, la cual debe estar conectada a la corriente directa de 110VAC. En un futuro, lo ideal sería colocarle algún tipo de fuente de alimentación removible como una batería o fotoceldas.
- **Analizar distintas señales fisiológicas**: En este caso se trabajó con la señal de electrocardiograma. Sin embargo el sistema puede aplicar distintas señales fisiológicas como lo es el electroencefalograma (EEG) o presión de la sangre (BP) y analizar los resultados de seguridad y eficiencia con el algoritmo de cifrado caótico con el mapa seleccionado.
- **Realizar análisis de seguridad a nivel físico del sistema embebido presentado**: Como análisis de la información de tiempo de cálculos, el monitoreo de consumo de energía o remanencia de datos, que puede proporcionar una fuente adicional de información que puede ser explotada para corromper el sistema criptográfico.

Bibliografía

[1] Hu B., Bai J. y Ye D. (1997). An internet based communication server for Telemedicine. *Proceedings of the 19th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Magnificent Milestones and Emerging Opportunities in Medical Engineering*, 981-982.

[2] Shaikh A., Misbahuddin M. y Memon M.S. (2008). A system design for a Telemedicine health care system. *Journal of communications in Computer and Information Science*, **20**: 295-305.

[3] Zvikhachevskaya A., Markarian G. y Mihailova L. (2007). Quality of Service consideration for the wireless Tele-medicine and e-healt services. *IEEE Wireless Communications and Networking Conference, Budapest*, 1-6.

[4] Alanazi B., Zaidan A., Shabbir M. y Al-Nabhani Y. (2010). New Comparative Study Between DES, 3DES and AES. *Journal of Computing*, **2**(3): 2-5.

[5] Martínez-Clark R. y Cruz-Hernández C. (2016). Aplicaciones de la teoría de caos. *Trabajo de investigación, Centro de Investigación Científica y de educación Superior de Ensenada*, 2-10.

[6] Maña A., López J., Pino L. y Maraval C. (1997). Incremento de la seguridad del estándar de cifrado de datos basado en la combinación de datos y clave. *Jornadas de informática y automática*, **2**(1): 423-432.

[7] Pinto G., López R. y Cuesta E. (2011). Análisis de seguridad para el manejo de información médica en telemedicina. *Revista Ciencia e Ingeniería Neogranadina*, **21**(2): 57-89.

[8] Brown R. y Chua L. O. (1996). Clarifying chaos: examples and counterexamples. *International Journal of Bifurcation and Chaos*, **6**(2): 219-249.

[9] Ferrante F. (2006). Maintaining Security and Privacy of Patient Information. *28th IEEE EMBS Annual International Conference*, 3-6.

[10] Maji A., Majumdar M. y Mukhopadhyay T. (2008). Security analysis and implementation of web-based Telemedicine services with a four-tier architecture. *Conference on Pervasive Computing Technologies for Healthcare*, 2-4.

[11] Wooton R. y Craig J. (2005). Introduction to telemedicine. *The Royal Society of Medicine Press*, **11**(1): 2-7.

[12] Taylor P. (1998). A survey of research in telemedicine: telemedicine systems. *Telemed Telecare*, **4**(1): 1-17.

[13] Monteagudo L., Serrano L. y Hernández-Salvador C. (2005). Telemedicine: science or fiction. *Trabajo universitario de la Universidad Pública de Navarra*, **28**(3): 309-323.

[14] Zundel M. (1996). Telemedicine: history, applications, and impact on librarianship. *Bull Media Libre Association*, **84**(1): 71-90.

[15] Bashshur R.L. (1995). On the definition and evaluation of telemedicine. *Telemedicine Journal*, **1**(1): 19-30.

[16] Cuenca P. (2011). Historia de la telemedicina. *Tesis doctoral, departamento de Telesalud*, 3-87.

[17] Xue Y., Huigang H. y Liang H. (2007). Analysis of Tele-medicine Diffusion: The Case of China. *Transactions on information technology in biomedicine*, **2**(11): 231-233.

[18] Francesco S. (2002). Some Aspects on Tele-medicine and Health. *Institute of Biomedical Advanced Technology*, **1**: 23-24.

[19] Montanari A. y Antonio C. (2009). Enabling secure service discovery in mobile healthcare enterprise networks. *Wireless Communications Magazine*, **1**(3): 33-39.

[20] Francesco S. (2003). Health Insurance Portability and Accountability Act. *Small Health Care Practices*, **2**: 3-4

[21] Brand S., Boonen J. y Harry S. (2004). IT Governance based on COBIT 4.0. *Van Haren Publishing*, **2**(4): 15-17

[22] Ilias M. y Elias Z. (2011). Modeling Risk in Distributed Healthcare Information Systems. *Annual International Conference IEEE*, 11-24.

[23] Dillar K., fost P. y Jared T. (2004). Guía de administración de riesgos de seguridad. *Microsoft Corporation: Guia de riesgos*, 1-9

[24] Grigsby J,. Kaehny M. y Sandberg J. (1995). Effects and effectiveness of telemedicine. *Health Care Financ*, **17**(1): 115-310.

[25] Pisemskaya N. (2006). El lenguaje y la teoría del caos. *Tesis doctoral, Universidad de oriente*, 3-76.

[26] Torres N. (2005). Caos en sistemas biológicos. *Revista digital de divulgación matemática de la Real Sociedad Matemática*, **1**(3): 1-5.

[27] Lorenz E. N. (1963). Deterministic non periodic. *Journal of the Atmoferic Sciences*, **20**(109): 130-142.

[28] Rísquez F. (2008). La Teoría del Caos: Modelo de interpretación epistémica e instrumento de solución. *Tesis doctoral, Universidad Central de Venezuela*, 2-86.

[29] Alligood K., Sauer T. y Yorke J. (1997). An introduction to dynamical systems. *Bull Media Libre Association*, **2**(4): 71-80.

[30] Lara L. y Stoico C. (2003). Estimación de los exponentes de Lyapunov. *Revista de Mecánica Computacional*, **22**(1): 1-10.

[31] May R.M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, **2**(261): 459-467.

[32] Hernandez de la Sota C. (2004). Control inteligente de sistemas dinámicos caóticos. *Tesis doctoral, Universidad Politecnica de Madrid*, 2-103.

[33] Ahmad M. y Farooq O. (2010). A Multi-Level Blocks Scrambling Based Chaotic Image Cipher. *Communications in Computer and Information Science*, **2**(94): 171-182.

[34] Prasadh K. y Gnanajeyaraman R. (2009). Analysis of Chaotic-Chabyshev polinomials using on public key cryptosystems. *Journal, Computer science and Telecommunications*, **1**(3): 22-53.

[35] Hua Z. y Zhou Y. (2015) Image encryption using 2D Logistic-adjusted Sinemap. *Department of Computer and Information Science, University of Macau*, **1**(2): 3-15.

[36] Contreras J. (2004). Introducción a la criptografía. *DYNA*, **79**(2): 6-10.

[37] Belmonte I., Noriega U. y Quintero N. (2006). Sincronización de sistemas complejos. *Trabajo de investigación, Centro de Investigación Científica y de Educación Superior de Ensenada*, 1-22.

[38] Ramón J. (2016). Mensajes secretos. La historia de la criptografía española desde sus inicios hasta los años. *Tirant lo Blanch*, 623-633.

[39] Belasco J. (2008). Antecedentes y perspectivas de estudio en historia de la Criptografía. *Tesis doctoral, Universidad carlos III de madrid*, 2-68.

[40] Jesús J. (2017). Criptografía Para Principiantes. *Trabajo de investigación, Comunidad de Programadores*, 3-45.

[41] Días J. (2006). Principios básicos de la criptografia. *Information Sciences*, **1**(3): 47-59.

[42] Delgado V. y Palacios R. (2006). Introducción a la Criptografía: tipos de algoritmos. *Universidad Pontificia Comilla*, **1**(2): 2-5.

[43] Alvarez G. y Li S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, **16**(8): 2129-2151.

[44] Manuel-Cruz J. (2013). Sistemas Embebidos Sistemas de Tiempo Real. *Simposio argentino de sistemas embebidos*, 10-22.

[45] Sager E. (2013). Introducción General a los Sistemas Embebidos. *Simposio argentino de sistemas embebidos*, 5-15.

[46] Manuel-Cruz J. (2008). Controladores industriales de diseño de alto nivel. *PAC-Performance-centered Adaptive*, **1**(1): 5-10.

[47] Camargo-Bareño I. (2000). Programación en campo de microcontroladores. *Tesis maestría, Universidad Nacional de Colombia*, 15-20.

[48] MCF5225X Freescale Semiconductor (2008). MCF5225x Family. *Freescale Semiconductor*, KRN3MCF5225XFS/REV 2.

[49] Murillo Escobar M.A. (2015). Diseño de un algoritmo de cifrado caótico y su implementación en microcontrolador para aplicaciones embebidas. *UABC, Tesis de Doctorado en Ciencias en Eléctrica*, 1-142.

[50] Chen C.K., Lin C.L., Chiang C.T. y Lin S.L. (2012). Personalized information encryption using ECG signals with chaotic functions. *Information Sciences*, **1**(2): 125-140.

[51] Thorsted-Sorensena J., Clemmensenb P. y Sejersten M. (2013). Tele cardiología: pasado, presente y futuro. *Revista Española de Cardiología*, **66**(3): 212-218.

[52] Terkelsen C., Nørgaard, Lassen F., Gerdes J., Ankersen J. y Romer F. (2002). Telemedicine used for remote prehospital diagnosing in patients suspected of acute myocardial infarction. *Journal of Internal Medicine*, **20**(1): 252-412.

[53] Clemmensen P., Sejersten M., Sillesen M., Hampton D., Wagner GS. y Nielsen S. (2005). Diversion of ST-elevation myocardial infarction patients for primary angioplasty based on wireless prehospital. *Jouronal of Electrocardiology*, **38**(4): 22-194.

[54] Adams G.L., Campbell P.T., Adams J.M., Strauss D.G., Wall K. y Patterson J. (2006). New Effectiveness of prehospital wireless transmission of electrocardiograms. *TIME-NE*, **98**(4): 11-60.

[55] Raeiatibanadkooki M., Quchani S.R., KhalilZade M. y Bahaadinbeigy K. (2016). Compression and encryption of ECG signals using wavelet and chaotically human code in telemedicine application. *Journal of Medical Systems*, **40**(3): 1-8.

[56] Murillo-Escobar M.A., Cardoza-Avenda L., Lopez-Gutierrez R.M. y Cruz-Hernandez C. (2017). A double chaotic layer encryption algorithm for clinical signals in telmedicine. *Journal of Medical Systems*, **41**(4): 1-17.

[57] Kotulsk Z. y Szczepanski J. (1997). Discrete chaotic cryptography. *NEEDS*, **2**(3): 1-11.

[58] Stanciu M. y Datcu O. (2012). Atmel AVR microcontroller implementation of a new enciphering algorithm based on a chaotic generalized Hénon map. *9th International Conference on Communications, Bucharest, Rumania*, 319-322.

[59] Andreatos A.S. y Volos C.K. (2014). Secure text encryption based on hardware chaotic noise generator. *2nd International Conference on Cryptography and Its Applications in the Armed Forces, Atenas, Grecia*, 66-104

[60] Méndez-Ramírez R.D. (2018). Implementación de osciladores caóticos en sistemas embebidos y aplicaciones. *Tesis doctoral, Centro de Investigación Científica y de Educación Superior de Ensenada*, 1-133.

[61] Murillo-Escobar M.A., Cruz-Hernández C., Abundiz-Pérez F. y López-Gutiérrez R.M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, **42**(21): 8198-8211.

[62] Amina S. y Kamel-Mohamed F. (2018). An efficient and secure chaotic cipher algorithm for image content preservation. *Communications in Nonlinear Science and Numerical Simulation*, **60**: 12-32.

[63] Murillo-Escobar M.A., Cruz-Hernández C., Abundiz-Pérez F. y López-Gutiérrez R.M. (2014). A novel symmetric text encryption algorithm based on logistic map *Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers*, pp. 2-5.

[64] MCF52259RM. MCF52259 ColdFire integrated microcontroller reference manual. *MCF52259RM* 2009;Rev. 2 8/2009. 65

[65] Alvarez G. y Li S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, **16**(8): 2129-2151.