UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

PROGRAMA DE POSGRADO

MAESTRÍA Y DOCTORADO EN CIENCIAS E INGENIERÍA

SISTEMA DE ACCESO SEGURO BIOMÉTRICO BASADO EN CRIPTOGRAFÍA CAÓTICA Y SISTEMA EXPERTO

TESIS

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

DOCTOR EN CIENCIAS

presenta:

DANIEL MURILLO ESCOBAR

Ensenada, Baja California, México, Marzo de 2024.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

SISTEMA DE ACCESO SEGURO BIOMÉTRICO BASADO EN CRIPTOGRAFÍA CAÓTICA Y SISTEMA EXPERTO

TESIS

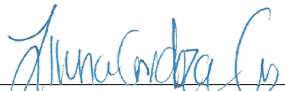
Que para obtener el grado de Doctor en Ciencias presenta:

DANIEL MURILLO ESCOBAR

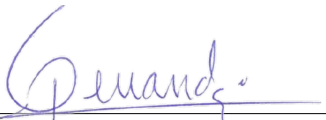
Aprobada por el siguiente comité:

Dra. Rosa Martha López Gutiérrez
Directora

Dr. Miguel Ángel Murillo Escobar
Codirector



Dra. Liliana Cardoza Avendaño
Miembro del comité



Dr. César Cruz Hernández
Miembro del comité

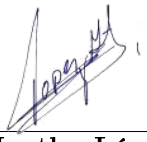
Dr. Adrian Arellano Delgado
Miembro del comité

Ensenada, Baja California, México, Enero de 2024.

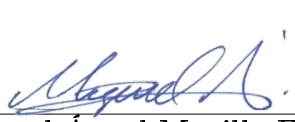
RESUMEN de la tesis de **Daniel Murillo Escobar**, presentada como requerimiento para obtener el grado de DOCTOR en CIENCIAS en ELÉCTRICA, del programa Maestría y Doctorado en Ciencia e Ingeniería de la Universidad Autónoma de Baja California. Ensenada, Baja California, México, Enero de 2024.

SISTEMA DE ACCESO SEGURO BIOMÉTRICO BASADO EN CRIPTOGRAFÍA CAÓTICA Y SISTEMA EXPERTO

Resumen aprobado por:



Dra. Rosa Martha López Gutiérrez
Directora



Dr. Miguel Ángel Murillo Escobar
Codirector

En este trabajo de tesis doctoral, se diseña e implementa en un sistema embebido de bajo costo, un sistema de acceso seguro basado en criptografía caótica y sistema experto para brindar seguridad y evitar suplantación biométrica a los sistemas de acceso basados en rasgos biométricos.

El sistema se basa en un microcontrolador de 32 bits donde se realizan todos los procesos, el módulo médico de electrocardiograma, módulo biométrico de huella dactilar, pantalla de cristal líquido, memoria micro SD, botones de presionar y fuente de alimentación. Se utilizan dos rasgos biométricos para el desarrollo del sistema de acceso seguro, la señal de electrocardiograma se utiliza para identificar al usuario mediante el sistema experto y la huella dactilar para autenticar al usuario y brindarle el acceso al sitio restringido.

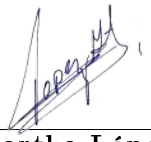
La plantilla de la huella dactilar se encripta mediante un algoritmo basado en el mapa hypercaótico Hénon-Seno donde las dinámicas caóticas se obtiene de un generador de números pseudoaleatorios. Se realizan diferentes análisis de seguridad para validar el algoritmo de encriptado caótico como espacio de clave secreta, sensibilidad a la clave secreta, sensibilidad a la plantilla clara, histogramas y entropía de la información. Los resultados muestran que el algoritmo de encriptado caótico propuesto es resistente a este tipo de ataques y el sistema de acceso seguro puede ser aplicado para aplicaciones de acceso digital a sitios restringidos.

Palabras clave: caos, biometría, encriptado caótico, huella dactilar, sistema experto, mapa Hénon-Seno, análisis de seguridad.

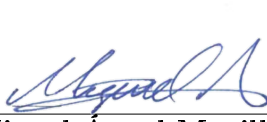
Abstract of the thesis presented by **Daniel Murillo Escobar**, as a requirement to obtain the DOCTOR in SCIENCE degree in ELECTRIC, of the program of Master and Doctorate in Science and Engineering of the Autonomous University of Baja California. Ensenada, Baja California, Mexico, January 2024.

SECURE BIOMETRIC ACCESS SYSTEM
BASED ON CHAOTIC CRYPTOGRAPHY AND EXPERT SYSTEM

Abstract approved by:



Dra. Rosa Martha López Gutiérrez
Directora



Dr. Miguel Ángel Murillo Escobar
Codirector

In this doctoral thesis work, a secure access system based on chaotic cryptography and expert system is designed and implemented in a low-cost embedded system to provide security and avoid biometric impersonation to access systems based on biometric traits.

The system is based on a 32-bit microcontroller where all processes are carried out, the electrocardiogram medical module, biometric fingerprint module, liquid crystal display, micro-SD memory, push buttons and power supply. Two biometric features are used for the development of the secure access system, the electrocardiogram signal is used to identify the user through the expert system and the fingerprint to authenticate the user and provide access to the restricted site.

The fingerprint template is encrypted using an algorithm based on the Hénon-Sine hyperchaotic map where the chaotic dynamics are obtained from a pseudorandom number generator. Different security analyzes are performed to validate the chaotic encryption algorithm such as secret key space, secret key sensitivity, clear template sensitivity, histograms and information entropy. The results show that the proposed chaotic encryption algorithm is resistant to this type of attacks and the secure access system can be applied for digital access applications to restricted sites.

Keywords: chaos, biometrics, chaotic encryption, fingerprint, expert system, Hénon-Sine map, security analysis.

A mi familia

Agradecimientos

A mis padres, Miguel Ángel y María Rosario. Por su apoyo durante estos 4 años y toda mi vida para la realización de este trabajo el cual sin ustedes no podría haberlo realizado.

A mis hermanos, Miguel, Yahaira, Angelina y Araceli. Por su cariño y buenos deseos que me alentaron a seguir adelante. En especial a mi hermano Miguel por sus consejos y apoyo brindado para la realización de este trabajo de doctorado.

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

A mi futura esposa, Kathya. Por apoyarme siempre cuando ya no tenía energía o motivación, alentarme cada día a seguir superándome y por la futura familia que formaremos que me llena de alegría y felicidad.

A mis codirectores de tesis, Dra. Rosa Martha López Gutiérrez y Dr. Miguel Ángel Murillo Escobar, por dirigirme durante mis estudios de doctorado y sus consejos para la culminación de mis estudios.

A mi comité de tesis, Dra. Liliana Cardoza Avendaño, Dr. César Cruz Hernández y Dr. Adrián Arellano Delgado, por sus consejos y observaciones durante el desarrollo de mis estudios de doctorado para mejorar la calidad del trabajo.

Al grupo de investigación Sistemas Complejos, por su amistad, los consejos y los buenos momentos que pasamos juntos.

A mis amigos, 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, por permitirme trabajar en el laboratorio de sistemas complejos el tiempo necesario para la realización de este trabajo. En especial a la Facultad de Ingeniería, Arquitectura y Diseño Ensenada.

Al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), por el apoyo económico recibido a través de la beca doctoral con número 001866 y del proyecto de investigación en ciencia básica entre instituciones "Sincronización de Sistemas Complejos y Algunas Aplicaciones". Ref. 166654 (A1-S-31628).

Ensenada, Baja California, México, Enero de 2024.

Daniel Murillo Escobar

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Capítulo 1

Introducción

En los últimos años, varios investigadores se han interesado en el diseño de sistemas de autenticación biométrica confiables y de bajo costo que cumplan con los requisitos de los sistemas embebidos actuales en términos de velocidad, costo, consumo de energía, etc. La biometría es una técnica mecanizada que utiliza atributos medibles, físicos o fisiológicos o características de comportamiento para percibir la personalidad o validar el carácter garantizado de una sola persona. Los sistemas de autenticación basados en rasgos biométricos de un ser humano pueden superar las limitaciones de los sistemas tradicionales. Los determinantes biométricos se clasifican como características fisiológicas que están relacionadas con el cuerpo humano, como el electrocardiograma (ECG), el ADN, las huellas dactilares, el reconocimiento facial, la huella palmar, el iris y el reconocimiento del olfato (Fig. 1.1).

Figura 1.1: La huella dactilar es el rasgo biométrico más utilizado.

Debido al rápido avance de la tecnología, la biometría se usa ampliamente para autenticar a una persona. El problema principal en la autenticación biométrica es la protección de plantillas, que protege la privacidad del usuario. Estos sistemas también deben cumplir con una amplia gama de aplicaciones de uso cotidiano tales como control de acceso, comercio electrónico, verificación de identidad, etc., donde se requieren prestaciones en cuanto a seguridad y confidencialidad de la información. En un sistema de autenticación biométrica tradicional, una vez que el dispositivo de entrada captura la plantilla biométrica, pasará por pasos de adaptación y procesamiento antes de almacenarse en la base de datos.

En este caso, los datos son objeto de ataques en diferentes niveles del sistema de autenticación biométrica. Estos ataques pueden ocurrir durante la transmisión o en el servidor (base de datos). El reconocimiento de huellas dactilares se ha utilizado en muchos escenarios de aplicación, como estacionamiento comunitario, compras en supermercados, préstamo de libros, acceso a edificios y otras actividades diarias. La huella dactilar nos proporciona una forma fiable y eficaz de reconocer la identidad individual. Los sistemas biométricos pueden lograr el objetivo de la identidad personal comparando las características biológicas, la huella dactilar es única y fácil de recolectar.

Hay una serie de puntos en los que un sistema biométrico puede ser atacado durante la recolección de datos en una red informática. Algunos trabajos iniciales han identificado varios posibles puntos de ataque, como el ataque al sensor, el ataque al canal entre el sensor y la extracción de características biométricas, etc. En general, la modalidad multi biométrica sufren los mismos problemas de privacidad, aunque podrían ser incluso más graves debido a que se almacenan múltiples plantillas de diferentes modalidades (y eventualmente se ven comprometidas). Por lo tanto, la protección de plantillas biométricas merecen atención urgente.

Los sistemas de autenticación basados en biometría reconocen a las personas en función de sus rasgos anatómicos o de comportamiento y, por lo tanto, ofrecen varias ventajas sobre los métodos de autenticación tradicionales, como contraseñas y documentos de identidad (Fig. 1.2). La cantidad de servicios y múltiples aplicaciones electrónicas modernas que utilizan información confidencial a través de dispositivos electrónicos o sistemas embebidos (ES) está creciendo exponencialmente (Fig. 1.3). Estos desarrollos hacen necesario el descubrimiento de nuevos métodos para garantizar que la información que se utiliza es segura frente a ataques conocidos. La seguridad de la información es un problema importante en la situación actual. La criptografía es la solución al problema de la seguridad de la información, tiene la finalidad de alterar el mensaje confidencial de modo que sea incompresible a toda persona distinta al destinatario.

Figura 1.2: Sistema de verificación de huella dactilar comercial.

Figura 1.3: Sistema multi biométrico basado en huella dactilar y detección de rostro.

En los últimos años, el caos ha sido ampliamente utilizado en criptografía. Por encriptado, se entiende un proceso de conversión de información a una forma disfrazada para mantenerla de forma segura. El proceso inverso de denomina desencriptado. El uso de técnicas de encriptado basado en caos, permite que información valiosa pueda ser protegida contra organizaciones criminales, hackers o espías de potencias militares extranjeras. La criptografía es una de las metodologías básicas para la seguridad. Esta técnica se basa tanto en conceptos teóricos como matemáticos. La teoría del caos juega un papel importante en la criptografía. Este sistema dinámico tiene una gran importancia en el campo del algoritmo de encriptado. Una función caótica proporciona un conjunto de números pseudoaleatorios y define una predicción a largo plazo imposible. El sistema caótico tiene varias características, como la sensibilidad a las condiciones iniciales, la mezcla, la ergodicidad, la no periodicidad, la aleatoriedad, etc. Un pequeño cambio en la condición inicial de este sistema crea un gran cambio dinámico en el comportamiento del sistema.

Los sistemas caóticos se utilizan a menudo como fuente de aleatoriedad en generadores de números pseudoaleatorios (PRNG). Las ecuaciones de Lorenz descritas a continuación, es un ejemplo de un sistema caótico.

$$\frac{dx}{dt} = \sigma(y - x), \tag{1.1a}$$

$$\frac{dy}{dt} = \rho x - y - xz, \tag{1.1b}$$

$$\frac{dz}{dt} = xy - \beta z \tag{1.1c}$$

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. En la Fig. 1.4, se observa su gráfica de fase.

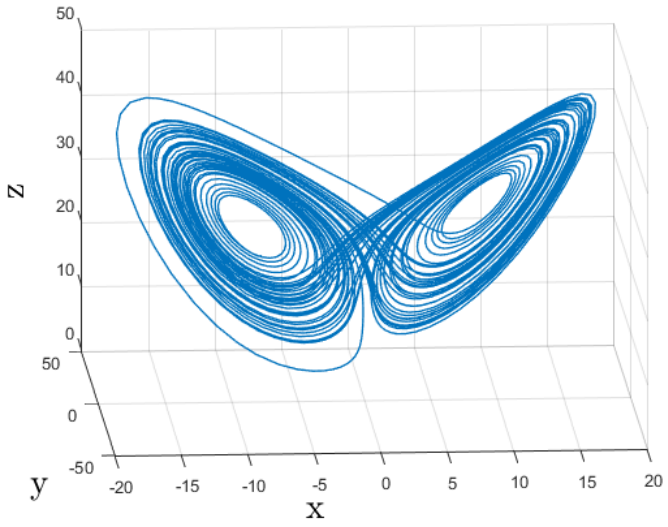


Figura 1.4: Atractor caótico del sistema de Lorenz.

Hay muchos ejemplos de aplicaciones e implementaciones de mapas caóticos para la generación de números aleatorios, que se han propuesto recientemente. El PRNG es un componente muy importante de los esquemas de encriptado, porque la seguridad del sistema criptográfico depende de la aleatoriedad de la secuencia pseudoaleatoria producida. Los generadores de números pseudoaleatorios son componentes fundamentales de los sistemas criptográficos, ya que se encargan de generar los valores clave impredecibles que se utilizan en los algoritmos de encriptado para proteger la integridad, confidencialidad y autenticidad de la información. A pesar de ser deterministas, los sistemas caóticos pueden usarse como fuente de entropía debido a su extrema sensibilidad a las condiciones iniciales, espectro de potencia similar al ruido y exponente de Lyapunov positivo, con dos o más exponentes de Lyapunov positivos, los sistemas hypercaóticos también se pueden usar para la generación de números aleatorios y tienen comportamientos más complejos, lo que dificulta la predicción de la serie temporal de salida.

Cada sistema de encriptado se compone de dos partes principales: (1) clave confidencial de encriptado y (2) algoritmo de encriptado. De acuerdo con el segundo principio de los seis principios de Kerckhoffs, el algoritmo de encriptado se considera conocido para todos, pero la clave de encriptado debe ser confidencial para personas no autorizadas, por lo que la seguridad del sistema debe recaer en la clave secreta. Los modelos criptográficos basados en el caos se han utilizado para desarrollar métodos novedosos para diseñar sistemas de encriptación eficientes. En un sistema embebido se aplica mediante programación un sistema experto, el cual es un sistema que emplea conocimiento humano capturado en un sistema embebido para resolver problemas que normalmente requieran de expertos humanos. Los sistemas bien diseñados imitan el proceso de razonamiento que los expertos utilizan para resolver problemas específicos.

1.1. Motivación

La autenticación por verificación biométrica es cada día más común, los principales identificadores biométricos dependen de características fisiológicas o de comportamiento. En el caso de los identificadores fisiológicas se relacionan con la composición del usuario que se autentica. El interés de proteger la información de identificadores biométricos se ha incrementado en los últimos años debido a la facilidad con la que se puede manipular la información, riesgos de seguridad en las redes de comunicaciones y al uso limitado del identificador biométrico. Con lo cual surge un problema que debe resolverse, el cual es como identificar la identidad de una persona con precisión y además de garantizar la seguridad de la información con la que se trabaja.

La autenticación de personas es de vital importancia en el control de acceso a sitios restringidos tanto físicos (bancos, hospitales, universidades, etc.) como digitales (celulares, computadoras, banca en línea, etc.). Los métodos de autenticación convencionales pueden utilizar contraseñas, número de identificación personal (NIP) o tarjetas inteligentes. Sin embargo, los métodos de autenticación biométricos permiten identificar a una persona por alguna característica fisiológica o del comportamiento único en cada persona, como la huella dactilar, iris, rostro, voz o forma de caminar, por lo que pueden proporcionar mayor seguridad ante los métodos convencionales. Actualmente, los identificadores biométricos como la huella dactilar, el iris, o la voz de una persona son ampliamente utilizados en sistemas de autenticación biométrica en muchas aplicaciones para el control de acceso restringido. No obstante, el robo de identidad biométrica (plantillas o imágenes biométricas digitales) y la suplantación de falsos identificadores biométricos (huellas de plástico, fotografía del iris o audio grabado) generan graves problemas de seguridad como pérdida de identificación biométrica y acceso de usuarios no autorizados.

Para contrarrestar estos problemas de seguridad, se implementa en un sistema embebido de bajo costo, criptografía caótica y un sistema experto, para proporcionar confidencialidad al identificador biométrico y determinar de forma "inteligente" la autenticación del usuario empleando herramientas de la inteligencia artificial como el sistema experto.

1.2. Objetivos y alcances de la tesis

Con el crecimiento de la tecnología de la información, cada vez se requiere más, un sistema de autenticación de identidad confiable, ya que, existe un problema clave que debe resolverse, el cual es como identificar la identidad de una persona con precisión y además de garantizar la seguridad de la información con la que se trabaja, por lo cual surge la realización de este trabajo de tesis de doctorado en el cual se planteó alcanzar el siguiente *objetivo general*:

Diseñar e implementar un sistema de acceso seguro biométrico basado en criptografía caótica y sistema experto.

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

1. Seleccionar e implementar en sistema embebido, un mapa caótico o hypercaótico que genere uniformidad y eficiencia, en dinámicas caóticas.
2. Diseñar e implementar en sistema embebido, un sistema de control de acceso seguro basado en uno o dos identificadores biométricos.
3. Diseñar e implementar en sistema embebido, un algoritmo criptográfico basado en caos para proteger los datos del identificador biométrico.
4. Diseñar e implementar en sistema embebido, un sistema experto para evitar suplantación biométrica.
5. Determinar la seguridad y eficiencia, del sistema de control de acceso seguro biométrico.

La investigación de este trabajo de tesis permitirá desarrollar conocimientos nuevos teóricos y prácticos, sobre la combinación de procesos de encriptado caótico y de sistemas expertos como herramientas de la inteligencia artificial, para brindar confidencialidad y evitar suplantación de falsos identificadores biométricos, para incrementar la seguridad de los sistemas de control de acceso.

1.3. Organización del manuscrito

Este trabajo de tesis de doctorado está compuesto por 9 capítulos, los cuales se describen de manera breve a continuación:

- **Capítulo 1**: Se presenta la introducción a este trabajo de investigación, la motivación y los objetivos.
- **Capítulo 2**: Se introduce a la biometría, su definición, propiedades y algunas aplicaciones del uso diario. Además, se analizan los sistemas biométricos y sus propiedades para aplicaciones de seguridad.
- **Capítulo 3**: Se describe el caos, sus características, propiedades y algunas aplicaciones como en encriptado de información. Se muestra el mapa Logístico de una dimensión como ejemplo para demostrar las características del caos y sus cualidades mediante gráficas y análisis experimentales.
- **Capítulo 4**: Se da a conocer lo que es un sistema criptográfico, las principales características de los sistemas criptográficos modernos y se analizan las principales debilidades y consideraciones para el uso de la criptografía en aplicaciones de seguridad.

- **Capítulo 5**: Se describen de manera breve los sistemas expertos, donde se da a conocer los módulos básicos que lo componen, sus características, ventajas y su estrecha relación con los sistemas embebidos.
- **Capítulo 6**: Se presenta el mapa hypercaótico propuesto con algunos análisis para validar la generación caótica, además, el generador de números pseudoaleatorios propuesto mediante distintos análisis experimentales aplicado en microcontrolador.
- **Capítulo 7**: Se muestra el algoritmo de encriptado caótico propuesto con los detalles para los procesos de encriptado y desencriptado.
- **Capítulo 8**: Se describe el sistema de acceso seguro biométrico propuesto, se muestran los detalles de los procesos del sistema experto y autenticación, además, la implementación en un sistema embebido basado en un microcontrolador de 32 bits y algunos análisis de seguridad.
- **Capítulo 9**: Se mencionan las conclusiones de este trabajo doctoral de manera general, las publicaciones que generó este trabajo de investigación, las contribuciones más sobresalientes y algunos comentarios para trabajos futuros.

Capítulo 2

Biometría

En este capítulo, se dará a conocer su definición, propiedades y algunas aplicaciones del uso diario. Además, se analizan los sistemas biométricos y sus propiedades para aplicaciones de seguridad, se mostrarán las principales ventajas y desventajas a la hora de aplicarlo en la vida real.

2.1. Introducción

A medida que nuestra sociedad se ha vuelto más móvil y conectada electrónicamente, no se puede confiar en las representaciones sustitutas de la identidad, como las contraseñas (que prevalecen en el control de acceso electrónico) y las tarjetas (que prevalecen en las aplicaciones bancarias y gubernamentales) para establecer la identidad de una persona. Las tarjetas pueden perderse o ser robadas y las contraseñas o el PIN pueden, en la mayoría de los casos, adivinarse. Además, las contraseñas y las tarjetas se pueden compartir fácilmente, por lo tanto, no proporcionan la seguridad deseada y surgen cada vez más informes de intrusión en estos sistemas de seguridad, existe una gran demanda de mayor seguridad para el acceso a lugares y/o datos confidenciales/personales. En estos días, las tecnologías biométricas se utilizan normalmente para analizar las características humanas con fines de seguridad [1].

La palabra biometría se deriva de las palabras griegas *"bios"* (que significa vida) y *"metron"* (que significa medida). Los identificadores biométricos son medidas del cuerpo humano vivo. El reconocimiento biométrico (o simplemente "*biometría*") se refiere al uso de características anatómicas distintivas (huellas dactilares, cara, iris) y de comportamiento (voz, forma de andar), denominadas identificadores biométricos o características para reconocer automáticamente a las personas (Fig. 2.1) [2]. La biometría se está convirtiendo en un componente esencial de las soluciones efectivas de identificación de personas porque los identificadores biométricos no se pueden compartir ni extraviar.

La biometría no es solo un fascinante problema de investigación de reconocimiento de patrones, sino que, si se usa con cuidado, es una tecnología habilitadora con el potencial de hacer que nuestra sociedad sea más segura, reducir el fraude y brindar comodidad al usuario (interfaz hombre-máquina fácil de usar) [3].

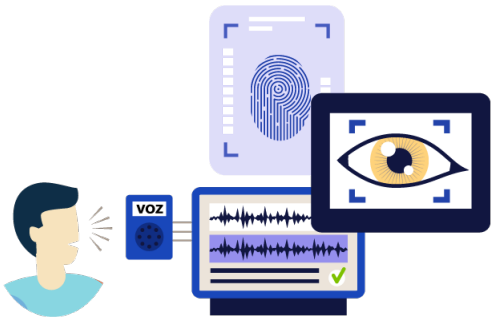


Figura 2.1: Características anatómicas distintivas y de comportamiento.

El brote repentino de la pandemia de COVID-19 presento un desafío importante para el campo de la biometría de dos maneras. En primer lugar, el virus permanece activo en las superficies durante un largo período de tiempo, lo que desalienta a los usuarios a interactuar físicamente con dispositivos biométricos compartidos entre varias personas. En consecuencia, la biometría sin contacto se volvió más crucial en presencia de COVID-19. En segundo lugar, también se propaga por el aire, lo que llevó a las autoridades sanitarias de todo el mundo a instar al público en general a usar mascarillas con regularidad para reducir la propagación del virus, lo que suponía una desventaja debidos a las mascarillas utilizadas, debido a eso se desarrollaron nuevas formas de aplicar la tecnología en identificadores biométricos [4].

A continuación, se describen los rasgos biométricos más comunes:

- Iris: La textura visual del iris humano está determinada por los procesos morfogenéticos durante el desarrollo embrionario y se postula que es distinta para cada persona y cada ojo [5].
- Rostro: El rostro es uno de los rasgos biométricos más aceptables porque es uno de los métodos de reconocimiento más comunes que usan los humanos en sus interacciones visuales diarias [6].
- Geometría de la mano y los dedos: Algunas características relacionadas con la mano humana (longitud de los dedos) son relativamente invariantes y peculiares (aunque no muy distintivas) para un individuo [7].
- Vena de la mano o del dedo: Se utilizan imágenes de infrarrojo cercano para escanear la parte posterior de un puño cerrado para determinar la estructura de la vena de la mano. Las venas también podrían detectarse en un dedo usando sensores infrarrojos [8].

- Electrocardiograma: El sistema de autenticación biométrica mediante electrocardiograma (ECG) puede proteger la privacidad de las personas y prevenir los fraudes de identidad. Los investigadores han demostrado que el ECG es adecuado para el uso biométrico debido a su omnipresencia, inmutabilidad, mensurabilidad, aceptación e individualidad [9].

  Una prueba de ECG a menudo se usa para verificar los comportamientos eléctricos del corazón del paciente y monitorear las actividades cardíacas de las funcionalidades eléctricas del corazón del paciente durante la prueba [10]. Las señales de ECG pueden diagnosticar la mayoría de las enfermedades cardíacas; por lo tanto, el desarrollo de instalaciones de monitoreo de sensores corporales ha aumentado recientemente. El motivo del dolor o la presión en el pecho inexplicables que pueden ser causados por un ataque al corazón se puede encontrar aplicando la señal de ECG. Las propiedades de las señales de ECG son exclusivas de un individuo y falsificar las señales no es fácil. Incluye cinco picos llamados ondas T, S, Q, P y R [11, 12].

  - Onda P: Indica la activación secuencial de las aurículas derecha e izquierda.
  - Onda Q: Corresponde a la despolarización del tabique interventricular.
  - Onda R: Refleja la despolarización de la masa principal de los ventrículos.
  - Onda S: Significa la despolarización final de los ventrículos en la base del corazón.
  - Intervalo PR: Indica el tiempo que tarda la actividad eléctrica en moverse entre las aurículas y los ventrículos.
  - Complejo QRS: Indica la activación simultánea del derecho y ventrículos izquierdos.
  - Segmento ST: Refleja el periodo de potencial cero entre la despolarización y la repolarización ventricular.
  - Onda T: Indica repolarización ventricular.
  - Onda QT: Indica el tiempo que tardan los ventrículos en despolarizarse y luego repolarizarse.

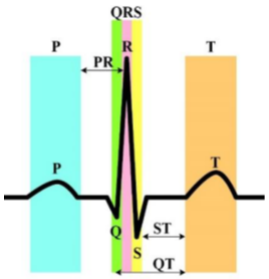


Figura 2.2: Ondas PQRST de señal ECG.

Se han diseñado algunas soluciones de seguridad biométrica basadas en estas señales que brindan servicios de seguridad: autenticación, autenticación anónima, privacidad y control de acceso [13, 14]. La señal de ECG juega un papel vital en un sistema de salud electrónico para detectar enfermedades del corazón. El pico más significativo de las señales del ECG es el pico R, mientras que en el complejo QRS se concentra la energía. En la detección de características de la señal de ECG, encontrar el pico de la onda R es esencial, ya que cuando se encuentra el pico de la onda R, se puede encontrar la ubicación de las ondas P, Q, S y T. Por lo tanto, la detección del complejo QRS está directamente asociada con la detección de los latidos del corazón. La duración de la onda P, el complejo QRS y la onda T consisten en información útil sobre la enfermedad del corazón del paciente.

- Voz: La captura de voz es discreta y puede ser el único biométrico factible en aplicaciones que requieren reconocimiento de personas a través de un teléfono [15].
- Firma: Se sabe que la forma en que una persona firma su nombre es una característica de ese individuo. Las firmas han sido aceptables en transacciones gubernamentales, legales y comerciales como método de verificación durante mucho tiempo [16].
- Huella dactilar: Las plantillas de huellas dactilares incluyen casi toda la información sobre las huellas dactilares de una persona y la validación del usuario está totalmente determinada por las características de las minucias de las huellas dactilares. Debido al tipo de ataques, la tarea más desafiante es proteger las plantillas de huellas dactilares (o características de minucias) [17]. Una minucia es un punto de interés de la huella y se conforman de diferentes tipos [18]:
  - Terminación: Es donde la cresta termina y no continua en ningún otro lado.
  - Bifurcación: Es donde una cresta de divide en dos caminos.
  - Laguna: Una corta separación que se vuelve a unir inmediatamente.
  - Línea independiente: Una línea que aparece, de manera similar a la terminación, pero vuelve a continuar.
  - Punto: Aparece en medio de dos líneas como si fuera a terminar.
  - Spur: Una separación donde una línea continua derecha y la otra se termina rápidamente quedando la forma de un gancho.
  - Cruce: La unión de dos crestas en algún punto, en lugar de mantenerse separados por un valle.

La biometría es de interés en cualquier área donde sea importante verificar y autenticar la verdadera identidad de un individuo. Las tecnologías biométricas son cada vez más atractivas debido a los métodos de autenticación seguros para el acceso de los usuarios, el comercio electrónico, la autenticación remota y el control de acceso. Las tecnologías biométricas se están convirtiendo en la base de una amplia gama de soluciones de identificación y verificación personal altamente seguras [19].

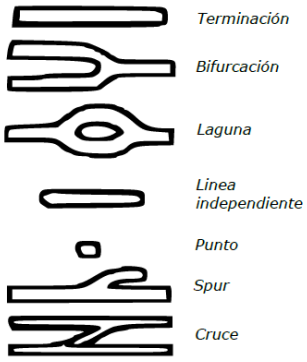
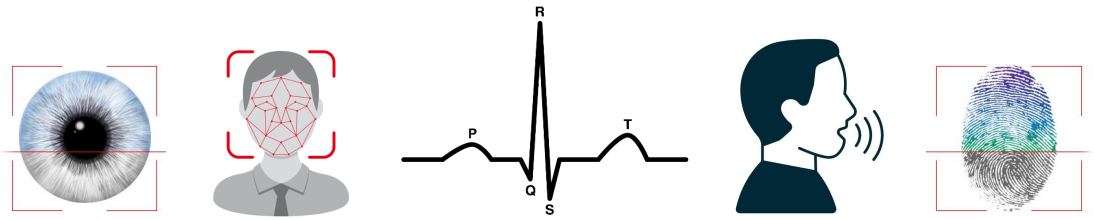


Figura 2.3: Tipos de minucias.



(a) (b) (c) (d) (e)

Figura 2.4: Rasgos biométricos: a) Iris, b) Rostro, c) ECG, d) Voz y e) Huella dactilar.

2.2. Sistemas biométricos

Cualquier rasgo anatómico o de comportamiento humano puede ser utilizado como identificador biométrico para reconocer a una persona siempre que cumpla con los siguientes requisitos:

- Carácter distintivo: Dos personas cualesquiera deben ser lo suficientemente diferentes en cuanto a sus rasgos biométricos.
- Coleccionabilidad: El rasgo biométrico se puede medir cuantitativamente.
- Permanencia: El rasgo biométrico debe ser invariable en el tiempo.
- Universalidad: Cada persona debe poseer el rasgo biométrico.

Un sistema biométrico se basa en varias características extraídas del iris, la huella dactilar, la cara, etc., para identificar a una persona en tiempo real. Estas características extraídas de las características biométricas construyen las plantillas biométricas [20]. El sistema biométrico de huellas dactilares, es un sistema de reconocimiento táctil que se utiliza principalmente para aceptar o rechazar a una persona para una determinada aplicación o servicio, un sistema biométrico puede denominarse sistema de verificación o sistema de identificación [21].

Un **sistema de verificación** (Fig. 2.5), auténtica la identidad de una persona comparando la característica biométrica capturada con su plantilla de referencia biométrica capturada previamente (registrada) y almacenada previamente en el sistema. Realiza una comparación uno a uno para confirmar si la afirmación de identidad del individuo es verdadera. Un sistema de verificación rechaza o acepta la declaración de identidad presentada.

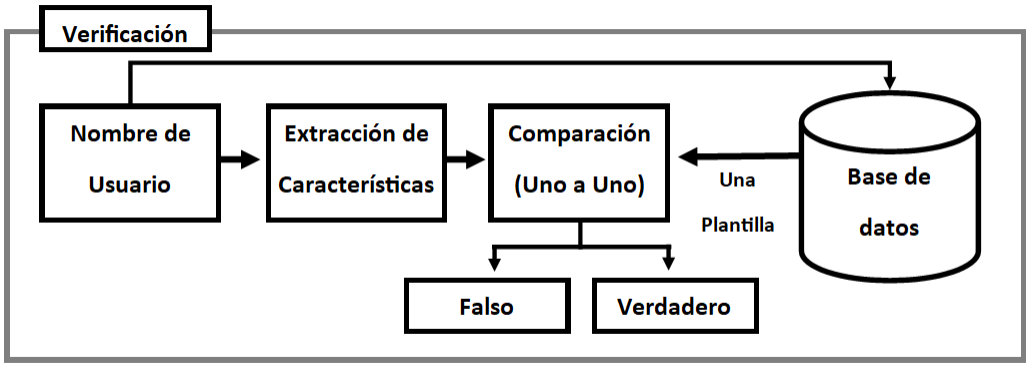


Figura 2.5: Diagrama de flujo de sistema de verificación.

Un **sistema de identificación** (Fig. 2.6), reconoce a una persona al buscar una coincidencia en toda la base de datos de plantillas de inscripción. Realiza comparaciones de uno a muchos para establecer si el individuo está presente en la base de datos y de ser así, devuelve el identificador de la referencia de inscripción que coincidió. En un sistema de identificación, el sistema establece la identidad de un sujeto (o determina que el sujeto no está registrado en la base de datos del sistema) sin que el sujeto tenga que reclamar una identidad.

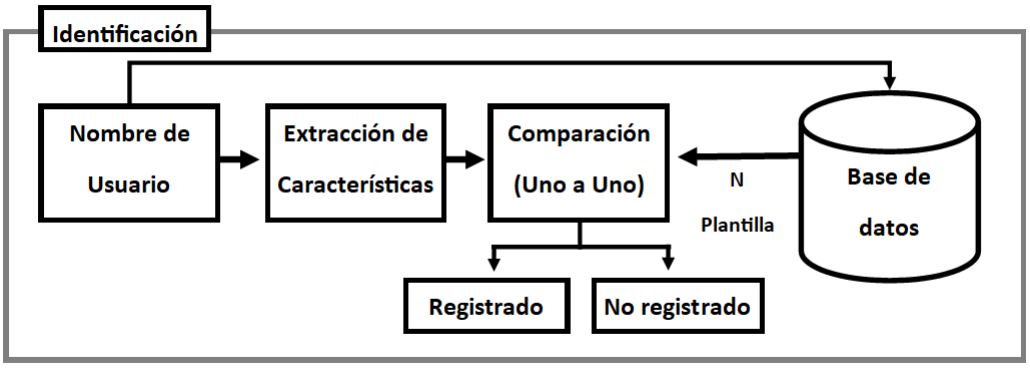


Figura 2.6: Diagrama de flujo de sistema de identificación.

El término autenticación también se utiliza en el campo biométrico, en ocasiones como sinónimo de verificación; en realidad, en el lenguaje de la tecnología de la información, autenticar a un usuario significa permitir que el sistema conozca la identidad del usuario independientemente del modo (verificación o identificación).

Los procesos de alta, verificación e identificación involucrados en el reconocimiento de usuarios hacen uso de los siguientes módulos del sistema:

- Captura: Es necesario detectar y capturar una representación digital de la característica biométrica. Un sensor biométrico, como un escáner de huellas dactilares, es una de las piezas centrales de un módulo de captura biométrica. La representación digital capturada de la característica biométrica a menudo se conoce como muestra.
- Extracción de características: Para facilitar el emparejamiento o la comparación, la representación digital sin procesar (muestra) suele ser procesada adicionalmente por un extractor de características para generar una representación compacta pero expresiva, denominada conjunto de características.
- Creación de plantillas: El módulo de creación de plantillas organiza uno o más conjuntos de características en una plantilla de inscripción que se guardará en algún almacenamiento persistente.
- Preselección y emparejamiento: La etapa de preselección (o filtrado) se utiliza principalmente en un sistema de identificación cuando el número de plantillas registradas es grande. Su función es reducir el tamaño efectivo de la base de datos de plantillas para que la entrada deba coincidir con un número relativamente pequeño de plantillas. La etapa de emparejamiento (o comparación) toma un conjunto de funciones y una plantilla de inscripción como entradas y calcula la similitud entre ellos en términos de una puntuación de coincidencia.
- Almacenamiento de datos: Se dedica a almacenar plantillas y otra información demográfica sobre el usuario. Según la aplicación, la plantilla se puede almacenar en dispositivos de almacenamiento internos o externos.

Usando estos cinco módulos, se pueden realizar tres procesos principales, a saber: registro, verificación e identificación. Un sistema de verificación utiliza los procesos de inscripción y verificación, mientras que un sistema de identificación utiliza los procesos de inscripción e identificación. Los tres procesos son:

- Registro (Fig. 2.7): El registro de usuarios es un proceso que se encarga de registrar a las personas en el almacenamiento del sistema biométrico. Durante el proceso de inscripción, la característica biométrica de un sujeto es capturada primero por un escáner biométrico para producir una muestra.
- Verificación: El proceso de verificación se encarga de confirmar la afirmación de identidad del sujeto, produce una decisión de coincidencia/no coincidencia.
- Identificación: En el proceso de identificación, el sujeto no reclama explícitamente una identidad y el sistema compara el conjunto de características (extraído de la muestra biométrica capturada) con las plantillas de todos (o un subconjunto de) los sujetos en el almacenamiento del sistema.

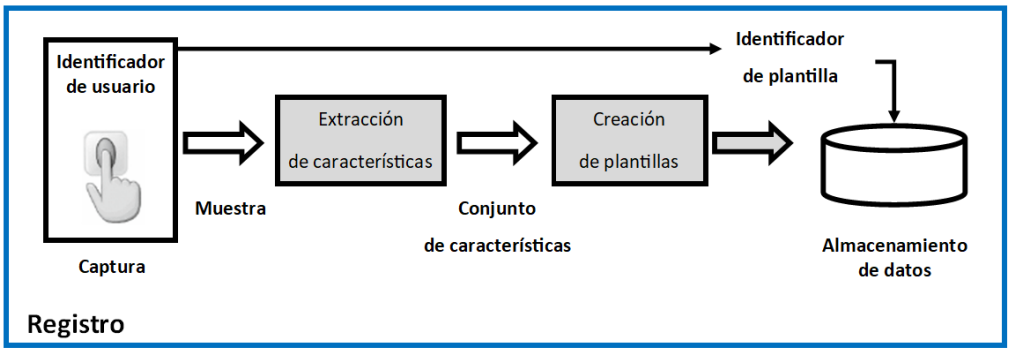


Figura 2.7: Proceso de registro.

Un sistema biométrico ideal debería evitar el mal uso de los datos biométricos mientras conserva su rendimiento biométrico. Un sistema biométrico debe garantizar que los usuarios genuinos puedan acceder al sistema sin ninguna dificultad y que todos los impostores estén identificados. Un sistema ideal debería aspirar a una tasa baja de aceptación falsa y una tasa baja de rechazo falso. Además de lograr un alto rendimiento de reconocimiento. Las preocupaciones de seguridad y privacidad plantean la necesidad de diseñar un esquema de protección biométrica.

Existen numerosas aplicaciones de los sistemas de reconocimiento biométricos. Básicamente, se utilizan para vigilancia, aplicación de la ley, tiempo, asistencia, control de acceso lógico y control de acceso físico, para asegurar los sistemas de vigilancia y también para los edificios físicos para varias aplicaciones como redes informáticas, verificación, investigaciones, autenticación, banca en línea, control fronterizo, e-comercio, gestión de registros médicos y monitoreo de seguridad. Además, mejora el nivel de confianza después de la verificación del individuo [22].

Los sistemas biométricos brindan a los usuarios varias ventajas y desventajas en comparación con los sistemas tradicionales de varias maneras, estas ventajas se muestran en la Tabla 2.1 y las desventajas se muestran en la Tabla 2.2.

Tabla 2.1: Ventajas de los sistemas biométricos.

Ventajas
Facilidad de reconocimiento cercano
Requisitos de seguridad digital
Autenticación e identificación en aplicaciones complejas
Basada en la información de los rasgos humanos
Sistemas multi biométricos
Más confiables para probar la identidad que los métodos tradicionales
Menos amenazas a la seguridad y fraudes financieros
Facilitar la personalización y la comodidad

Tabla 2.2: Desventajas de los sistemas biométricos.

Desventajas
Sensibilidad de los datos biométricos
Amenazas a la seguridad
Fuga de información de identidad
Ataques directos e indirectos
Algoritmos de clasificación y extracción de características débiles
Canal de comunicación débil
Falsa aceptación
La falta de distinción y los ataques falsos

2.3. Seguridad biométrica

Aunque la definición de la noción de seguridad para un sistema basado en biometría es una tarea muy desafiante, la comunidad científica ha realizado un esfuerzo significativo para resaltar las principales preocupaciones de seguridad relacionadas con un sistema de reconocimiento basado en biometría. En términos generales, un sistema biométrico puede ser vulnerable debido a una falla intrínseca o debido a ataques intencionales. Un sistema caracterizado por una alta tasa de falsas aceptaciones es muy propenso a ser corrompido, ya que, es probable que una característica biométrica arbitraria presentada al sistema coincida [23]. La promesa crítica del rasgo biométrico ideal es que cuando se presente una muestra al sistema biométrico, ofrecerá la decisión correcta. En la práctica, un sistema biométrico es un sistema de reconocimiento de patrones que inevitablemente toma algunas decisiones incorrectas.

Hay tres razones principales que explican los errores cometidos por un sistema [24]:

- Limitación de la información: El contenido de información invariable y distintiva en las muestras biométricas puede estar inherentemente limitado debido a la capacidad de señal intrínseca (por ejemplo, información de individualidad) del identificador biométrico.
- Limitación de representación: El esquema de representación ideal debe diseñarse para retener toda la invariancia, así como la información discriminatoria en las mediciones detectadas.
- Limitación de invariancia: El diseño de un emparejador ideal debería modelar perfectamente la relación de invariancia entre diferentes patrones de la misma clase (usuario), incluso cuando se representan en diferentes condiciones de presentación.

En la literatura se han propuesto un gran número de algoritmos automáticos de comparación de huellas dactilares. La mayoría de estos algoritmos no tienen dificultad para hacer coincidir imágenes de huellas dactilares de buena calidad. Los enfoques para la comparación de huellas dactilares se pueden clasificar a grandes rasgos en dos familias:

Coincidencia basada en correlación: Se superponen dos imágenes de huellas dactilares y se calcula la correlación entre los píxeles correspondientes para diferentes alineaciones.

Coincidencia basada en minucias: Esta es la técnica más popular y ampliamente utilizada, siendo la base de la comparación de huellas dactilares realizada por los examinadores de huellas dactilares. Las minucias se extraen de las huellas dactilares y se almacenan como conjuntos de puntos en el plano bidimensional. La coincidencia basada en minucias consiste esencialmente en encontrar la alineación entre la plantilla y los conjuntos de características de minucias de entrada que dan como resultado el número máximo de emparejamientos de minucias.

Una plantilla protegida debe satisfacer las cuatro propiedades mencionadas a continuación [25]:

1. La generación de los datos biométricos originales a partir de la plantilla almacenada debe ser prácticamente inviable.
2. La puntuación de similitud no debe variar considerablemente debido al ruido de adquisición o cambios ambientales.
3. Debe garantizar la privacidad del usuario.
4. Debe garantizar la prohibición del uso de una plantilla segura recuperada por el adversario de una base de datos para su comparación en otra base de datos para el mismo usuario sin su consentimiento.

Recientemente, ha habido un tremendo crecimiento en el interés por la biometría y la criptografía debido a los requisitos de seguridad de datos en muchas aplicaciones, incluido el gobierno electrónico, el voto electrónico, la salud electrónica, el comercio electrónico y la seguridad pública [26–28].

El objetivo es autenticar la identidad de una persona. En esquemas criptográficos, los usuarios usan contraseñas o claves secretas para mantener seguros sus datos confidenciales. La biometría utiliza rasgos fisiológicos y de comportamiento, como la cara, la palma de la mano, la voz y la forma de andar, es fácil de usar, confiable, conveniente de usar, no se puede compartir y no se puede perder ni olvidar, lo que genera gran interés en utilizar rasgos biométricos, pero, además, resguardar la información utilizando la criptografía [29].

2.4. Conclusiones

En este capítulo se presentó una breve introducción a la biometría y sistemas biométricos, la biometría es utilizada hoy en día por casi todas las personas con acceso a la tecnología, desde dispositivos móviles que cuentan con desbloqueo facial o mediante huella dactilar o sistemas que controlan el acceso a un lugar. Los sistemas de reconocimiento biométrico son los sistemas que se han desarrollado continuamente para mejorar los niveles de seguridad y comodidad en el entorno laboral. El desarrollo es posible solo con el reconocimiento de patrones. En este trabajo de tesis doctoral, se desarrolla un sistema de acceso seguro basado en huella dactilar donde se encripta la información biométrica para brindar mayor confidencialidad a la información utilizada.

Capítulo 3

Caos

En este capítulo se verá una breve introducción a la teoría del caos, su definición, como fue descubierta, sus características, propiedades y algunas aplicaciones como en encriptado de información, donde se explotan la propiedad del caos y la criptografía para el desarrollo de algoritmos. Se analizará el mapa Logístico de una dimensión como ejemplo para mostrar las características del caos y sus cualidades mediante gráficas y análisis experimentales.

3.1. Introducción

La palabra caos deriva del griego "khaos", que era utilizada para referirse a un "abismo profundo y oscuro". En la mitología griega se establece que "Caos" era una divinidad sin personalidad que fue la encargada de darle forma a Erebo, el dios de las tinieblas, y a Nyx, la diosa de la noche. Por lo general la idea de caos alude a la falta de orden, a la desorganización o al desconcierto (Fig. 3.1). Algo que es un caos carece de estructura, de lógica o de criterios que le permitan una disposición adecuada. Por ejemplo: "¡Esta casa es un caos! Tenemos que limpiar y ordenar de manera urgente".

Figura 3.1: La palabra caos se asocia con el desorden.

En matemáticas, caos se refiere al comportamiento aparentemente impredecible de los sistemas dinámicos no lineales que generaran números pseudoaleatorios. La teoría del caos es una rama de las matemáticas, la física y otras ciencias que trata ciertos tipos de sistemas dinámicos, es decir aquellos sistemas cuyo estado evoluciona con el tiempo con la particularidad de ser muy sensibles a las variaciones en las condiciones iniciales.

Entonces un sistema caótico es un sistema dinámico muy sensible a condiciones iniciales, pequeñas variaciones en dichas condiciones iniciales pueden implicar grandes diferencias en el comportamiento futuro, haciendo complicada la predicción a largo plazo [30]. Por medio de la teoría del caos también se puede estudiar fenómenos tales como el control de la población, epidemias, el movimiento de bancos de peces, aves e insectos migratorios, el comportamiento del cerebro, los espasmos del corazón en pleno ataque cardiaco, la predicción del tiempo, etc. En los años ochenta, los físicos, biólogos, astrónomos y economistas crearon un modo de comprender la complejidad en la naturaleza. La nueva ciencia, llamada caos, ofrece un método para ver orden donde antes sólo se observaba azar e irregularidad, traspasando las disciplinas científicas tradicionales y enlazando especies inconexas de desorden.

El caos fue re-descubierto accidentalmente por el matemático Edward Lorenz, usaba su ordenador Royal McBee para desentrañar la maraña matemática que él mismo había creado con sus doce ecuaciones para predecir el tiempo atmosférico en el Massachusetts Institute of Technology. Era el año 1960, la predicción del tiempo se debía regir por ecuaciones, al igual que las órbitas de los planetas, satélites y galaxias, quizá más complicadas. Para ello escogió 12 funciones, unas establecían el vínculo entre velocidad y viento, otras entre presión y temperatura y así unas cuantas variables más. No le promovía un interés meramente físico sino también matemático. Hojeando los rollos y rollos de papel con datos numéricos que escupía su impresora, Lorenz ideó un método para que el ordenador señalara cada minuto el paso de un día imprimiendo una hilera de números. En 1961, Lorenz cansado de observar ese vaivén numérico salido de la impresora de su ordenador, intentó atajar partiendo de una sucesión anterior, pero al traspasar los dígitos sólo tecleó 3 en vez de los 6 originales, esperando que el comportamiento no cambiara. Los resultados obtenidos trajeron de cabeza a Lorenz pues no eran los esperados y revisó el software y hardware hasta darse cuenta finalmente, que el error lo cometió al truncar el valor inicial de la función cambiando el input de 0.506127 a 0.506. Había dado con "el efecto mariposa". Este redondeo insignificante era el aleteo de la mariposa; y el comportamiento anómalo, o digamos inesperado, de la función del huracán que se produciría el próximo mes en Tokio. A su descubrimiento lo llamó Lorenz "Dependencia sensitiva de las condiciones iniciales" (Fig. 3.2), con ello creó la base de una nueva ciencia: el caos.

Lorenz animado por su descubrimiento, decidió comenzar a experimentar con sus resultados en el campo de las corrientes de fluidos y sus 12 fórmulas se vieron reducidas a 3 simples ecuaciones no lineales. Lorenz representó gráficamente los resultados obtenidos con sus 3 ecuaciones en una gráfica tridimensional, el diagrama manifestó una complejidad infinita, permanecía siempre dentro de ciertos límites, sin nunca repetirse. Reveló una configuración extraña, característica, algo por el estilo de una espiral doble en tres dimensiones, como una mariposa con su par de alas. La figura denotó desorden puro, puesto que ningún punto, o pauta de ellos, se repetía jamás. A pesar de todo, señaló una nueva clase de orden. Al ver el gráfico resultante, llamado en adelante "atractor de Lorenz" (Fig. 3.3) [31].

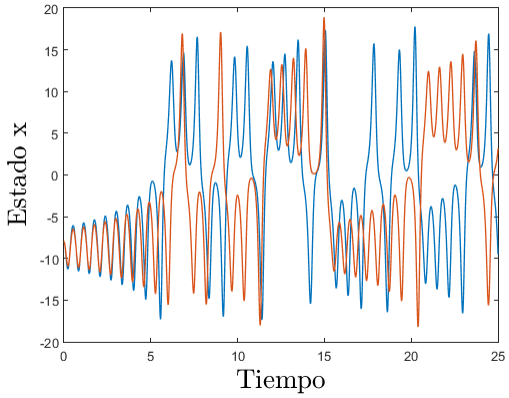


Figura 3.2: Sensibilidad a la condición inicial diferente de la Ec. (1.1a).

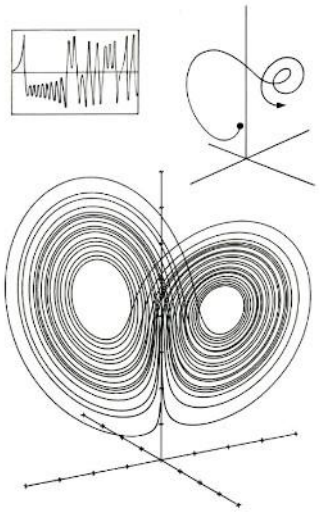


Figura 3.3: Gráficas del atractor de Lorenz.

Desde la década de 1990, los sistemas dinámicos caóticos han sido ampliamente utilizados en el diseño de nuevas estrategias para el encriptado de información, su crecimiento brinda la posibilidad de utilizar el caos como base de nuevos sistemas criptográficos [32]. El caos se conoce como un fenómeno pseudoaleatorio generado en un sistema determinista, se ha utilizado ampliamente en muchas áreas como la biología, las finanzas y la ingeniería electrónica debido a sus excelentes propiedades, incluida la alta sensibilidad a los estados iniciales [33, 34], la imprevisibilidad [35, 36] y la ergodicidad [37, 38]. Por ejemplo, la sincronización caótica se estudia exhaustivamente para explorar el fenómeno que acopla dos o más sistemas caóticos disipativos, que se ha utilizado popularmente en la seguridad de la información [39–41]. Los sistemas caóticos básicos, como el mapa Logístico, el mapa Seno y el mapa de Tent, suelen tener un rendimiento deficiente en términos de rangos caóticos y grietas resistentes [42]. En los últimos años, se han propuesto sistemas más caóticos desde diversas perspectivas. Para sistemas caóticos 1D, se han desarrollado muchos métodos mejorados para superar las limitaciones utilizando diferentes operaciones como cascada [43], combinación no lineal [44] y control de interruptores [45]. Estas operaciones compensan las carencias de los mapas caóticos básicos a expensas de construir estructuras caóticas más complejas [46]. Además, estos nuevos mapas caóticos se utilizan en aplicaciones como el encriptado de imágenes [47–49] y la generación de números pseudoaleatorios [50–52], donde se debe establecer un estado inicial en cada iteración [53].

3.2. Sistemas caóticos y sus propiedades

La teoría del caos puede definirse como el estudio cualitativo del comportamiento dinámico aperiódico mostrado por algunos sistemas deterministas no lineales. Un sistema complejo es un sistema compuesto por varias partes interconectadas o entrelazadas cuyos vínculos entre ellas contienen información adicional y oculta al observador. Como resultado de las interacciones entre elementos, surgen propiedades nuevas que no pueden explicarse a partir de las propiedades de los elementos aislados. Dichas propiedades se denominan propiedades emergentes. El mapa caótico es uno de los sistemas caóticos más representativos que posee estas propiedades [54].

Para la parte demostrativa, se utilizará el sistema de Lorenz en algunos ejemplos y el mapa Logístico, el sistema no lineal más simple que puede tener comportamiento caótico y también uno de los más estudiados. El mapa Logístico es un mapeo polinómico de grado dos. El mapa fue popularizado en por el biólogo Robert May. En parte como un modelo demográfico de tiempo discreto análogo a la ecuación logística. 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 y la relativa simplicidad del mapa Logístico lo convierte en un punto de entrada ampliamente utilizado para considerar el concepto de caos [55].

Matemáticamente, el mapa Logístico se muestra en la siguiente ecuación:

$$x_{n+1} = \mu x_n(x_n - 1), \tag{3.1}$$

donde x_n es la condición inicial con valores entre $0 < x_n < 1$ y μ es el parámetro de control entre $3.57 < \mu < 4$. Con valores en estos rangos se generan dinámicas caóticas discretas (Fig. 3.4).

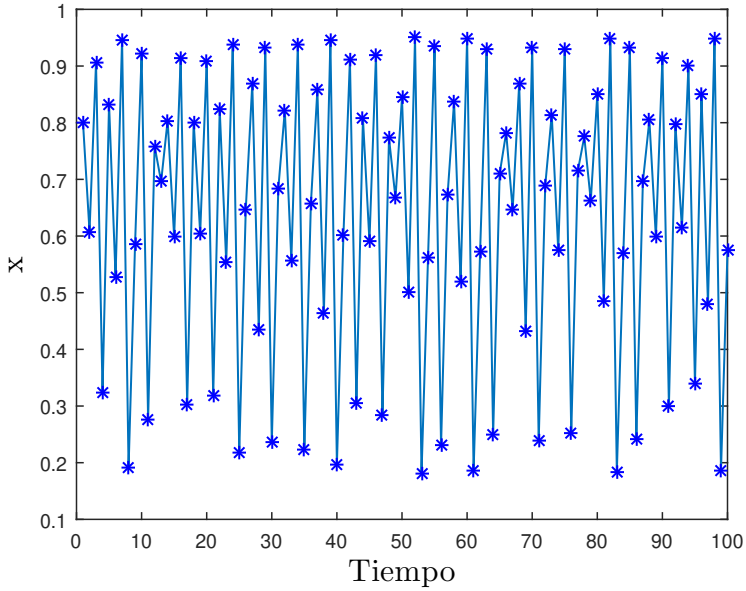


Figura 3.4: Gráfica temporal del mapa Logístico.

A continuación, se mencionan algunas características principales que identifican a los sistemas caóticos [56]:

- Generación de atractores extraños: Una forma de visualizar el movimiento caótico o cualquier tipo de movimiento es realizar un diagrama de fase del movimiento, los diagramas temporales y fase pueden exhibir una ergodicidad y pseudoaleatoriedad superiores derivadas de sistemas caóticos. Por más caótico que parezca, un sistema sigue una trayectoria hacia determinados puntos, a esos puntos a los que el sistema tiende a ir se les conoce como "atractores". Las series temporales, tradicionales (arriba), y las trayectorias en el espacio de fases (abajo) (Fig. 3.5), son dos formas de poner de manifiesto los mismos datos y de conseguir una imagen del comportamiento a largo plazo de un sistema. El primer sistema (izquierda) converge en un estado estable, un punto en el espacio de fases. El segundo se repite de forma periódica, formando una órbita cíclica. El tercero se reitera en un ritmo de vals más complejo, un ciclo de período tres. El cuarto es caótico. Por tanto, todas las trayectorias tienden a un conjunto llamado atractor. En algunos casos, el atractor es simplemente un punto (punto de equilibrio estable) o una curva cerrada (ciclo límite). Pero en otros casos el atractor tiene una estructura mucho más compleja, esto se conoce como un atractor extraño [57].

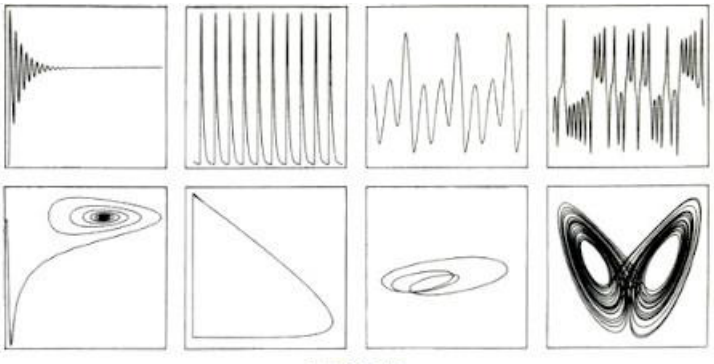


Figura 3.5: Gráfica temporal y de fase del sistema de Lorenz.

- Dimensión fraccionaria: Los fenómenos del caos están descritos por ejemplo en la matemática fractal, que captura la infinita complejidad de la naturaleza. Siempre que un sistema manifiesta dinámica caótica, esta aparece asociada con un tipo de objetos geométricos caracterizados por su dimensión no entera. Dentro del atractor, las trayectorias vagan de manera aparentemente errática. El conjunto de atractores de un sistema forma los llamados "fractales". Un fractal es algo que es "autosimilar", es un objeto matemático en el que, si miras de cerca cualquier sección, esa sección en sí misma se parece al objeto completo. Como figura geométrica no tiene una dimensión entera, como sucede con los puntos, segmentos de líneas, superficies planas, etc. El fractal más famoso es el conjunto de Mandelbrot, el cual esta asociado al diagrama de bifurcación del mapa Logístico (Fig. 3.6).

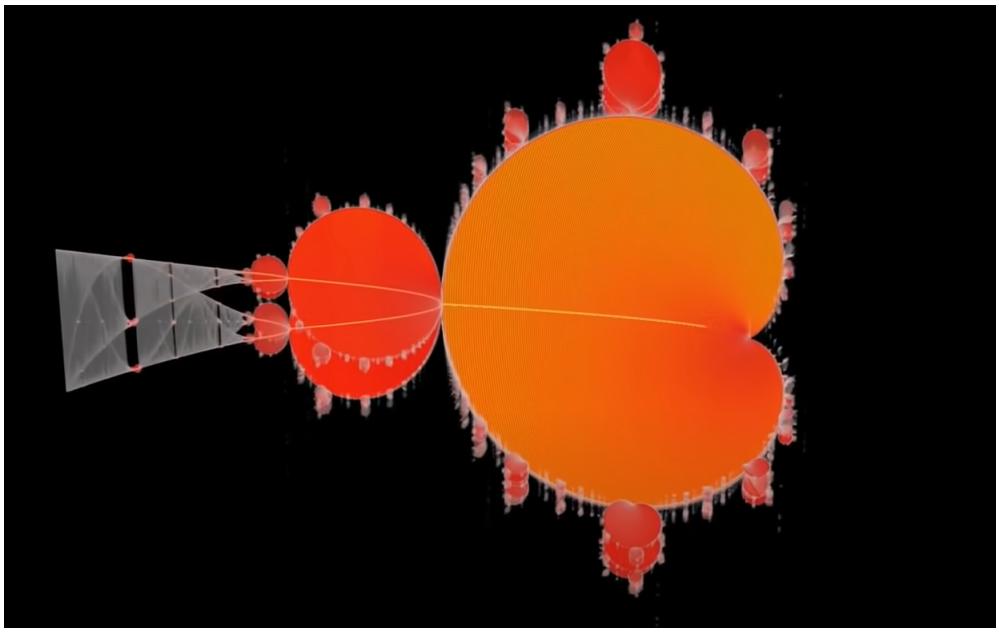


Figura 3.6: Conjunto de Mandelbrot.

- Dependencia sensible de las condiciones iniciales y parámetros de control: Una de las principales características de un sistema caótico es la dependencia de la sensibilidad a los valores iniciales y los parámetros de control. En otras palabras, un pequeño cambio en los valores iniciales o parámetros de control se incrementará significativamente en cada iteración (Fig. 3.7). Cuando los valores iniciales se cambian ligeramente, las dos secuencias pueden ser dramáticamente diferentes. Los sistemas caóticos con excelente sensibilidad son utilizados en la aplicación de algoritmos criptográficos, son más resistentes a ataques exhaustivos [58].

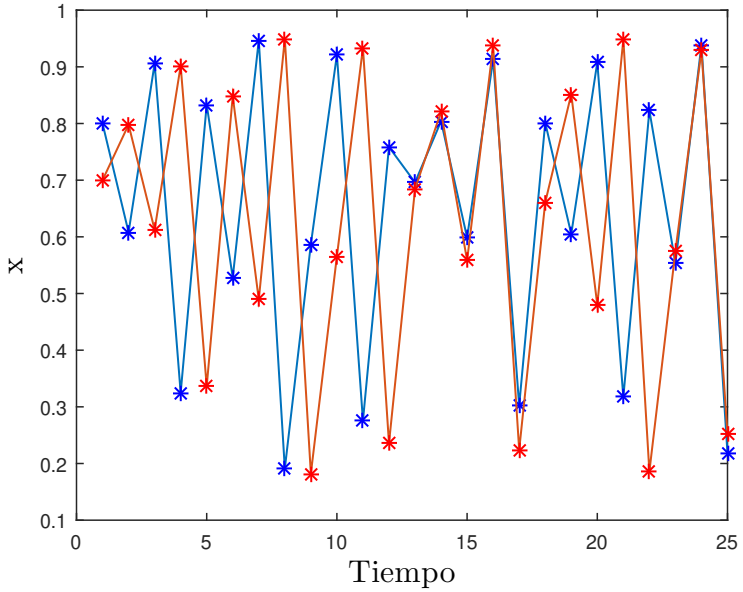


Figura 3.7: Sensibilidad a condiciones iniciales del mapa Logístico,

- Exponentes de Lyapunov positivos: Exponente de Lyapunov (LE) es una cantidad que mide las tasas exponenciales de convergencia o divergencia de dos trayectorias adyacentes de un sistema dinámico. Un valor positivo de LE indica que las trayectorias del sistema dinámico se separan en cada iteración. Por tanto, el sistema dinámico es caótico cuando tiene un valor positivo de LE, e hypercaótico si tiene más de uno. Un sistema se considera caótico ya que posee al menos un LE con valor > 0. El enorme valor LE puede reflejar el sentido más robusto del sistema a los valores iniciales, lo que puede insinuar aún más que sus propiedades dinámicas son complejas [59].

  Para calcular el exponente de Lyapunov se utilizó como parámetro de control $\mu = 3.800000$, $n = 100$ y condición inicial de $x_n = 0.800000$. El valor obtenido del exponente Lyapunov es de $\lambda = 0.693100216810785$, por lo que se demuestra la existencia de caos.

- El diagrama de bifurcación permite observar la variación en el comportamiento caótico para diferentes valores de parámetros (Fig. 3.8). En general, cuanto mayor sea el rango de parámetros que producen un comportamiento caótico, mayor será la resistencia a los ataques exhaustivos. La trayectoria de un sistema de tiempo discreto es una secuencia de valores que muestra las rutas de movimiento de las salidas del sistema (Fig. 3.9) [60].

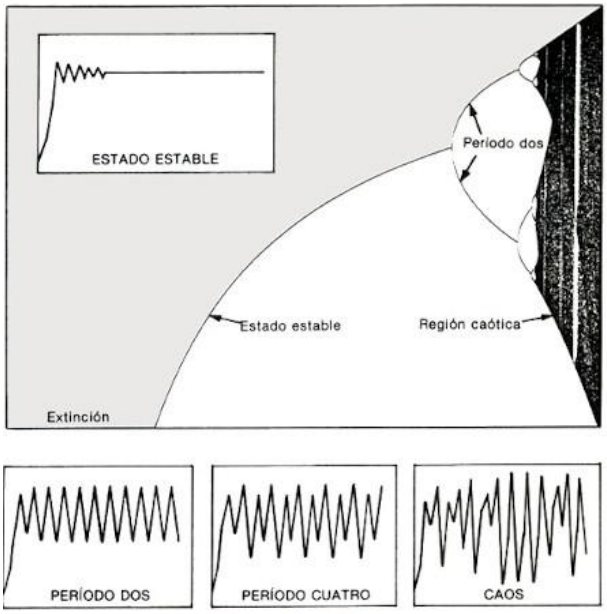


Figura 3.8: Fases de un diagrama de bifurcación.

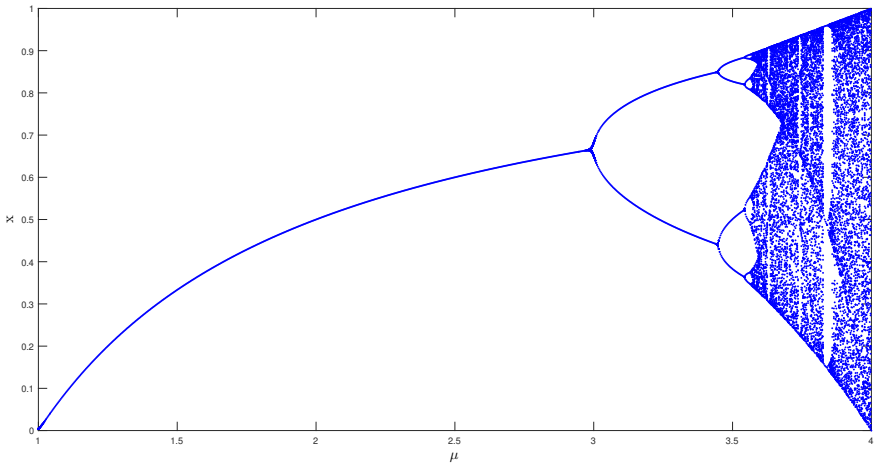


Figura 3.9: Diagrama de bifurcación del mapa Logístico.

3.3. Aplicaciones del caos

Se aprovechan las características caóticas de algunos sistemas para crear caos y aplicarlo por ejemplo a las comunicaciones seguras, el diseño de antenas o la planeación de trayectorias. A continuación, se presentan algunos casos en los que se aplica la teoría del caos en sistemas de ingeniería [61, 62]:

- Diseño de antenas fractales. La evolución de los sistemas de comunicación obliga a los dispositivos manejar antenas multibanda. Una de las soluciones que mejor desempeño presentan es el uso de antenas con patrones fractales [63].
- Control de movimiento en robots móviles. Los sistemas caóticos, aplicados a la robótica móvil, son utilizados para guiar robots autónomos para exploración de terrenos, vigilancia, búsqueda y desactivación de bombas (Fig. 3.10) [64].

Figura 3.10: Robot móvil khepera.

- Sistemas criptográficos basados en caos: Algunas de las características del caos se encuentran implementadas experimentalmente en sistemas embebidos, donde es deseable que los algoritmos de los sistemas criptográficos basado en caos sean de menor orden, en el cual el tiempo de complejidad permita que el sistema criptográfico soporte y procese grandes cantidades de información. La sensibilidad a las condiciones es una característica altamente deseable donde al variar levemente los valores de los parámetros definidos en una clave secreta, ocasionaría que la encriptación de la información sea altamente segura y difícil de desencriptar [65].
- La gran mancha roja de Júpiter. El problema de la gran mancha roja de Júpiter se resolvió con la teoría del caos, un modesto enigma cósmico: la gran Mancha Roja de Júpiter, óvalo colosal y giratorio, semejante a una tempestad titánica, que jamás se desplaza y jamás se debilita (Fig. 3.11). El conocimiento de que un sistema complejo puede suscitar, a la vez, turbulencia y coherencia. La sonda espacial Voyager reveló que la superficie de Júpiter es un fluido bullidor y turbulento, con bandas horizontales que corren de este a oeste. El color muestra la dirección de giro de partes especiales de fluido: las que voltean en sentido contrario al de las agujas del reloj aparecen en rojo, y las que rotan en la dirección de ésas, en azul. Sea cual fuere la configuración de partida, las agrupaciones azules propenden a separase, y las rojas, a unirse en una sola mancha, estable y coherente, en medio del tumulto circunstante [66].

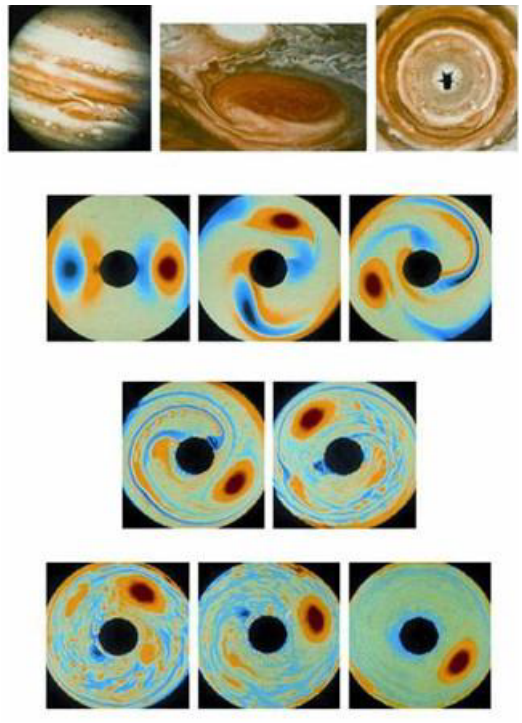


Figura 3.11: Gran macha roja de Júpiter.

3.4. Conclusiones

En este capítulo se explicó de manera breve la definición de caos y se mostraron sus propiedades como la sensibilidad a condiciones iniciales y parámetros de control, exponente de Lyapunov, atractor extraño y dimensión fractal mediante el análisis del mapa Logístico. El caos no es desorden; simplemente, es un orden diferente que debe verse de otro modo, porque muchas variables no necesariamente han de seguir un comportamiento determinista. El caos tiene una estrecha relación con la criptografía mediante las propiedades que comparten, dando esto al desarrollo de algoritmos de encriptado basado en caos, en los próximos capítulos se mostrara más información sobre criptografía y algoritmos de encriptado.

Capítulo 4

Criptografía

En este capítulo, se presenta una breve introducción a la criptografía, donde se menciona su definición, uso y los objetivos. Además, se muestran las principales características de los sistemas criptográficos modernos y se analizan las principales debilidades y consideraciones para el uso de la criptografía en aplicaciones de seguridad.

En muchos libros y/o artículos sobre criptografía, aparecen términos como encriptar y desencriptar, adoptados del verbo "*encrypt*". Este tipo de expresiones ha sido utilizado en el presente texto, debido a que su uso es más común en el ámbito de la investigación, aunque también está la existencia de palabras perfectamente validas que pertenecen al idioma español, como son cifrar–descifrar y codificar–decodificar.

Se llamara "*texto claro*", a toda información para encriptar.

4.1. Introducción

Desde sus inicios, la criptografía llegó a ser una herramienta muy usada, se encontró evidencia de que los antiguos egipcios, babilonios y romanos, usaban el encriptado y que los romanos fueron los primeros en usarlo con fines militares [67]. En la segunda guerra mundial tuvo un papel determinante, una de las máquinas de encriptado que tuvo gran popularidad se llamó Enigma (Fig. 4.1). Al terminar la guerra las agencias de seguridad de las grandes potencias invirtieron muchos recursos para su investigación. La criptografía como se conoce hoy, surgió con la invención de la computadora.

Figura 4.1: Máquina Enigma utilizada en la segunda guerra mundial.

La criptografía es la ciencia de la escritura secreta con el objetivo de ocultar el significado de un mensaje. La criptografía no sólo se emplea para proteger información, también se utiliza para permitir su autenticación, es decir, para identificar al autor de un mensaje e impedir que nadie suplante su personalidad. La palabra criptografía proviene del griego "*kryptos*", que significa esconder y "*gráphein*", escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (desencriptar) (Fig. 4.2).

La criptografía moderna se centra en tres aspectos clave: Definiciones, esquemas y pruebas [68].

- Definiciones: El primer desafío al que se enfrenta la criptografía moderna es llegar a una definición matemática concreta de lo que significa que un mecanismo criptográfico en particular sea seguro.
- Esquemas: Una vez que se tiene una definición de seguridad para un mecanismo criptográfico específico, se necesita diseñar esquemas que se espera cumplan con seguridad.
- Pruebas: En este enfoque, se diseña un esquema basado en ciertos bloques de construcción para realizar pruebas.

El objetivo principal de la criptografía es, precisamente, garantizar la confidencialidad de dicha información, de manera que solo sus destinatarios u otras partes autorizadas puedan tener conocimiento de su contenido. Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son: La privacidad, la integridad, la autenticación y el no rechazo.

- La privacidad: La información sólo pueda ser leída por personas autorizadas.
- La integridad: La información no pueda ser alterada en el transcurso de ser enviada.
- La autenticidad: Se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.
- El no rechazo: No se pueda negar la autoría de un mensaje enviado.

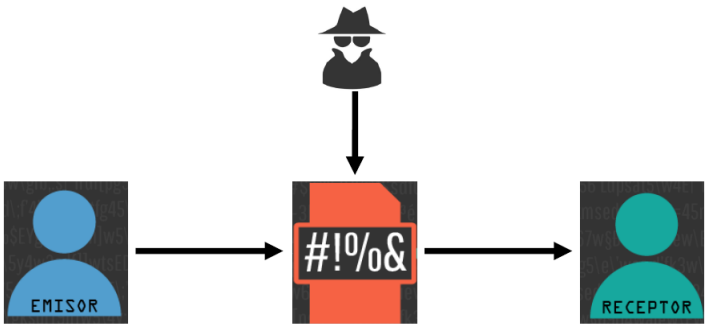


Figura 4.2: Comunicación a través de un canal inseguro.

Existen dos trabajos fundamentales sobre los que se apoya prácticamente toda la teoría criptográfica actual. Uno de ellos, desarrollado por Claude Shannon en sus artículos: "A Mathematical Theory of Communication" (1948) [69] y "Communication Theory of Secrecy Systems" (1949) [70], los cuales sientan las bases de la teoría de la información y de la criptografía moderna. El segundo, publicado por Whitfield Diffie y Martin Hellman en 1976, se titula: "New directions in Cryptography" [71], e introducía el concepto de criptografía asimétrica, abriendo enormemente el abanico de aplicación de esta disciplina.

La palabra criptografía sólo hace referencia al uso de algoritmos, por lo que no engloba a las técnicas que se usan para romper dichos algoritmos, conocidas en su conjunto como criptoanálisis. En cualquier caso, ambas disciplinas están íntimamente ligadas, cuando se diseña un sistema para encriptar información, hay que tener muy presente su posible criptoanálisis. El criptoanálisis es la ciencia de desencriptar criptosistemas. Podría pensar que el desencriptado de algoritmos es para la comunidad de inteligencia o quizás para el crimen organizado y no debería incluirse en una clasificación seria de una disciplina científica. Sin embargo, la mayoría de los criptoanálisis son realizados por investigadores respetables en la academia hoy en día. El criptoanálisis es de vital importancia para los criptosistemas modernos, sin personas que intenten desencriptar nuestros métodos criptográficos, nunca se sabrá si son realmente seguros o no.

4.2. Sistemas criptográficos

La criptografía se utiliza para enviar y recibir un mensaje de forma remota y segura a través de un canal no seguro. Un buen encriptado no debería ser demasiado complejo, ya que, de serlo, la persona que realiza el encriptado corre el riesgo de cometer errores, comprometiendo de esta forma la seguridad de todo el sistema de encriptado. Hoy en día, casi todas las computadoras pueden encriptar y desencriptar información [72].

Se define un sistema criptográfico como una quíntupla (m, c, K, E, D), compuesta por los siguientes elementos [73]:

- $\boldsymbol{m}$: Representa el conjunto de todos los mensajes sin encriptar (lo que se denomina texto claro) que pueden ser enviados.
- $\boldsymbol{c}$: Representa el conjunto de todos los posibles mensajes encriptados o criptogramas.
- $\boldsymbol{K}$: Representa el conjunto de claves que se pueden emplear en el criptosistema.
- $\boldsymbol{E}$: Es el conjunto de transformaciones de encriptado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de c.
- $\boldsymbol{D}$: Es el conjunto de transformaciones de desencriptado, 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 encripta con una función E y una clave K y después se desencripta con la misma clave K, se obtiene el mensaje original m.

Hay dos criptosistemas disponibles en criptografía: Criptografía de clave simétrica y criptografía de clave asimétrica, cada criptografía tiene sus ventajas y desventajas.

La **criptografía simétrica**, se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que se llamara clave secreta (Fig. 4.3). Son muy rápidos, por lo que son apropiados para manejar grandes cantidades de datos a alta velocidad. La simetría se refiere a que las partes tienen la misma clave tanto para encriptar como para desencriptar [74]. La criptografía simétrica ha sido la más usada en toda la historia, ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere encriptar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así desencriptar.

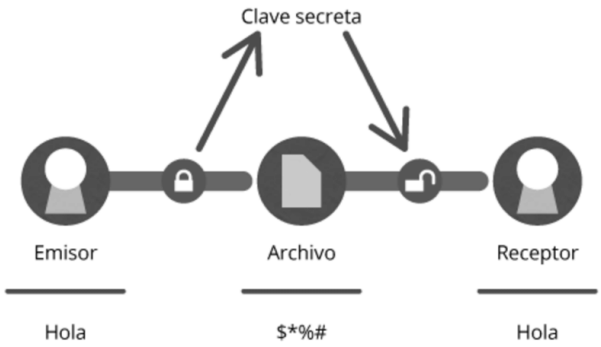


Figura 4.3: Encriptado de clave simétrico.

Los criptosistemas de clave simétrica se subdividen en dos categorías: Encriptado en bloque y en flujo. Dicho esto, hay que añadir, que esta diferencia reside a veces más bien en el modo de operación que en el encriptado en sí [75].

Encriptado de bloque: Encriptan el mensaje original agrupando los símbolos en bloques de dos o más elementos, de modo que cada bloque se encripta/desencripta siempre de la misma manera [76]. El encriptado de bloque generalmente consiste en una transformación inicial, una función criptográfica iterada n veces y una transformación final. La clave secreta se expande utilizando algún algoritmo para tener suficientes claves para usar en cada ronda de encriptado. Entre los encriptados de bloques más utilizados se encuentran los algoritmos criptográficos convencionales como AES, Triple DES, IDEA, DES, RC5 [77].

Encriptado en flujo: Supone una encriptación que varía con cada símbolo. El encriptado en flujo, encripta los bits individualmente. Esto se logra agregando un bit de un flujo de clave a un bit de texto sin formato. Hay encriptados de flujo sincrónico en los que el flujo de clave depende solo de la clave y asincrónicos en los que el flujo de clave también depende del texto encriptado.

La seguridad depende del emisor y el receptor, dentro del encriptado simétrico existen dos conceptos relacionados con la teoría de la información y las comunicaciones seguras: La confusión y la difusión. Según la Teoría de Shannon, las dos técnicas básicas para ocultar la redundancia en un texto claro son la confusión y la difusión. Estos conceptos, a pesar de su antigüedad, poseen una importancia clave en la criptografía moderna.

Confusión: Trata de ocultar la relación entre el texto claro y el texto encriptado. Recordemos que esa relación existe y se da a partir de la clave k empleada, puesto que, si no existiera, jamás se pudiera desencriptar los mensajes. El mecanismo más simple de confusión es la sustitución, que consiste en cambiar cada ocurrencia de un símbolo en el texto claro por otro. La sustitución puede ser tan simple o tan compleja como se requiera.

Difusión: Diluye la redundancia del texto claro repartiéndola a lo largo de todo el texto encriptado. El mecanismo más elemental para llevar a cabo una difusión es la transposición, que consiste en cambiar de sitio elementos individuales del texto claro.

La **criptografía asimétrica**, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para encriptar que se le llama clave pública y otra para desencriptar que es la clave privada (Fig. 4.4). Por lo general, una clave del par se conoce públicamente mientras que la otra se mantiene privada. Estos algoritmos son mucho más lentos porque en general implican operaciones aritméticas costosas con números enteros grandes, como logaritmo discreto o exponenciación de módulo. Como consecuencia, se utilizan para tareas que implican el encriptado de una pequeña cantidad de datos, como acuerdos de claves secretas, firmas digitales y autenticación [78].

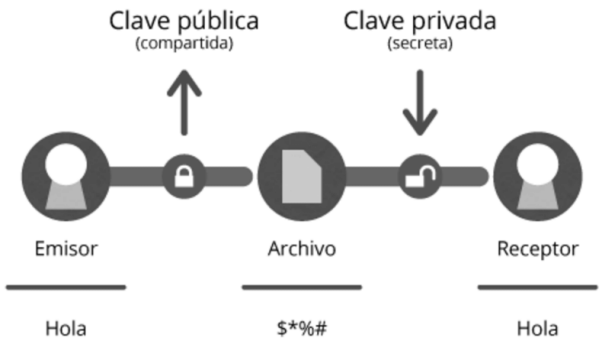


Figura 4.4: Encriptado de clave asimétrico.

El origen de la criptografía se remonta sin duda a los orígenes del hombre, desde que aprendió a comunicarse. Entonces, tuvo que encontrar medios de asegurar la confidencialidad de una parte de sus comunicaciones. El encriptado por difusión y confusión son dos procedimientos de encriptado básico que se ha ido repitiendo en épocas posteriores hasta llegar a nuestros días.

Las herramientas que se utiliza en la criptografía convencional para diseñar los algoritmos de encriptado, son teoría de números, algebra, curvas elípticas, entre otras, como los ya mencionados Triple DES y AES. Por otro lado, existe la criptografía no convencional para algoritmos de encriptado en la que se utilizan herramientas matemáticas en estado de investigación como la criptografía cuántica [79], criptografía con ADN [80] y criptografía caótica [81].

La criptografía caótica, es la que nos interesa en este trabajo de tesis doctoral, se basa en ecuaciones no lineales diferenciales o en diferencias, las cuales, generan secuencias desordenadas o caóticas, pero que son deterministas y que presentan sensibilidad a condiciones iniciales. Lo que da una ventaja para su aplicación en la criptografía, eliminando las desventajas fundamentales de la criptografía convencional. Las características de los sistemas caóticos los hacen aptos para ser utilizados en un sistema criptográfico, pues, además de añadir ventajas al sistema, su aplicación no es tan costosa como lo es en los sistemas de criptografía no convencional de ADN.

4.3. Seguridad criptográfica

La protección de la privacidad consiste en impedir que la información que un individuo desea mantener en privado pase a estar disponible para el dominio público (Fig. 4.5) [82]. La pregunta central en criptografía es ¿qué es la seguridad?. Esta pregunta puede responderse en dos niveles diferentes: Teórico y práctico [83].

A nivel teórico, la propiedad básica que caracterizan a un objeto seguro es: “Aumento de la aleatoriedad”. Los generadores de números pseudoaleatorios (PRNG) son importantes y se han utilizado en varias aplicaciones de seguridad [84].

Figura 4.5: El criptoanálisis son técnicas que se usan para romper algoritmos.

En el nivel práctico, la seguridad criptográfica de un objeto criptográfico, puede verificarse solo mediante la prueba de su resistencia a varios tipos de ataques conocidos. En esta parte, describimos los ataques básicos. En la comunidad criptográfica, hay dos dichos muy conocidos: "Es bastante fácil diseñar un encriptado seguro pero muy lento" y "Es bastante fácil diseñar un encriptado seguro pero muy grande". Una cuestión fundamental de todo tipo de criptosistemas es la clave. Siguiendo el principio de Kerckhoffs [85]. La seguridad de un criptosistema debería depender únicamente de su clave, no importa qué tan fuerte y qué tan bien diseñado sea el algoritmo de encriptado, si la clave se elige mal o el espacio de la clave es demasiado pequeño, el sistema criptográfico se romperá fácilmente.

Cuando se realiza un criptoanálisis en un algoritmo de encriptado, se supone generalmente que el criptoanalista conoce exactamente el diseño del algoritmo y cómo funciona el criptosistema, es decir, sabe todo sobre el criptosistema, excepto la clave secreta. Cuando se trata de criptoanálisis, existen diferentes niveles de ataques a los criptosistemas. Estos se enumeran a continuación, ordenados del tipo de ataque más difícil al más fácil de acuerdo con la literatura.

1. Ataque sólo con texto encriptado. Situación complicada y comprometida para el criptoanalista, puesto que surge cuando sólo tiene conocimiento del criptograma.

2. Ataque con texto original conocido. Consiste en acceder a una correspondencia de texto inicial y encriptado.

3. Ataque con texto original escogido. Se presenta cuando el criptoanalista puede conseguir, no sólo el criptograma a desencriptar, sino también el encriptado de cualquier texto que él escoja.

4. Ataque con texto encriptado escogido. Aparece en el supuesto de que el enemigo pueda obtener el texto original correspondiente a específicos textos encriptados de su preferencia.

En cada uno de estos cuatro ataques, el objetivo es determinar la clave que se utilizó en el encriptado/desencriptado. El criptoanálisis clásico se entiende como la ciencia de recuperar el texto claro del texto encriptado y/o, alternativamente, recuperar la clave k del texto encriptado.

El criptoanálisis se puede dividir en ataques analíticos, que explotan la estructura interna del método de encriptado y ataques de fuerza bruta, que tratan el algoritmo de encriptado como una caja negra y prueban todas las claves posibles. Los atacantes siempre buscan el punto más débil de un criptosistema. Por ejemplo, un espacio de clave grande por sí solo no garantiza que un encriptado sea seguro; el encriptado aún podría ser vulnerable contra ataques analíticos.

Un algoritmo, debe satisfacer una serie de propiedades de seguridad, además, de garantizar la aleatoriedad con el uso de sistemas caóticos [86].

- Los verdaderos generadores de números aleatorios (TRNG), se caracterizan por el hecho de que su salida no se puede reproducir. Por ejemplo, si se lanza una moneda 100 veces y se registra la secuencia resultante de 100 bits, será prácticamente imposible para cualquier persona en la Tierra generar la misma secuencia de 100 bits [87].
- Los generadores de números pseudoaleatorios (PRNG), generan secuencias que se calculan a partir de un valor conocido como semilla inicial [88]. Un requisito común de los PRNG es que posean buenas propiedades estadísticas, lo que significa que su salida se aproxima a una secuencia de números aleatorios verdaderos.
- Los generadores de números pseudoaleatorios criptográficamente seguros (CSPRNG), son un tipo especial de PRNG que poseen la siguiente propiedad adicional: Un CSPRNG es un PRNG que es impredecible [89].

En general, el criptoanálisis se suele llevar a cabo estudiando grandes cantidades de pares mensaje–criptograma generados con la misma clave. El mecanismo que se emplee para obtenerlos es indiferente y puede ser resultado de escuchar un canal de comunicaciones, o de la posibilidad de que el objeto de nuestro ataque responda con un criptograma cuando se le envié un mensaje. Cuanto mayor sea la cantidad de pares, más probabilidades de éxito tendrá el criptoanálisis. Se denomina ataque a cualquier técnica que permita recuperar un mensaje encriptado empleando menos esfuerzo computacional que el que se usaría por la fuerza bruta.

Cuanto más rápido sea el ataque de fuerza bruta, más débil será el encriptado. Los ataques de fuerza bruta se basan en un concepto simple; el atacante, tiene el texto encriptado y tiene un fragmento corto del texto claro sin formato, por ejemplo, el encabezado de un archivo que fue encriptado, ahora simplemente desencripta la primera pieza de la información encriptada con todas las claves posibles [90]. Uno de los tipos de análisis más interesantes es el de texto claro escogido, que parte de que se conoce una serie de pares de textos claros y sus criptogramas correspondientes. Esta situación se suele dar cuando se tiene acceso al dispositivo de encriptado y este nos permite efectuar operaciones, pero no nos permite leer su clave.

4.4. Conclusiones

El principal objetivo de la criptografía es establecer comunicación segura por un canal inseguro, la criptografía intenta resolver el problema anterior diseñando criptosistemas [91]. La criptografía depende en gran medida del diseño de un buen algoritmo criptográfico, ya que, por un lado, se debe de asegurar que el usuario legítimo, que posee la clave, puede encriptar y desencriptar la información de forma rápida y cómoda, mientras que por otro hay que garantizar que un atacante no dispondría de ningún algoritmo eficiente capaz de comprometer el sistema. La seguridad es muy esencial en el mundo de la electrónica moderna. Como se puede apreciar, la gran variedad de sistemas criptográficos produce necesariamente gran variedad de técnicas de criptoanálisis, cada una de ellas adaptada a un algoritmo o familia de ellos. Con toda seguridad, cuando en el futuro aparezcan nuevos mecanismos de protección de la información, surgirán con ellos nuevos métodos de criptoanálisis.

Por eso es necesario la implementación de distintas técnicas en el diseño de los algoritmos para mejorar las propiedades. El uso de sistemas caóticos para el diseño de PRNG es esencial para aplicaciones criptográficas debido a las mejores que provee. De una manera intencionalmente vaga, se denomina criptografía caótica a toda aquélla que se basa o inspira, directa o indirectamente, en los conceptos o métodos de la teoría de los sistemas dinámicos caóticos. Para este trabajo de tesis de doctorado, se desarrolla un algoritmo basado en criptografía no convencional utilizando la teoría del caos, donde se diseñará un PRNG para mejorar las propiedades pseudoaleatorias. El algoritmo se basa en una única clave de encriptado y desencriptado, utiliza operaciones de confusión y difusión para realizar un encriptado en flujo.

Capítulo 5

Sistema experto

En este capítulo se verá una breve introducción a los sistemas expertos (SE), donde se darán a conocer los módulos básicos que componen a un sistema experto, sus características y ventajas. Se analizará su origen, el cual proviene de la inteligencia artificial (IA) y su estrecha relación con los sistemas embebidos (ES) donde se verán algunas características de Arduino, el cual se utiliza para la parte experimental de este trabajo.

En algunos trabajos la abreviatura "SE" se considera para abreviar Sistema Embebido, por lo cual podría resultar confuso. En este trabajo de tesis doctoral se utilizará la abreviatura "SE" para Sistema Experto y "ES" para sistema embebido por sus siglas en ingles.

5.1. Introducción

La conferencia de Darmouth, en 1956, marca el comienzo de la inteligencia artificial (IA) en el ámbito de la actividad informática. En ese año se empieza a recorrer un largo camino que ha proporcionado menos resultados de los esperados en aquellos comienzos esperanzadores. El término inteligencia artificial se refiere a la capacidad de emular las funciones inteligentes del cerebro humano, como la propiedad de una máquina por la que es capaz de realizar funciones similares a las que realiza la inteligencia humana (Fig. 5.1). El empleo de la IA es variada y actualmente se utiliza principalmente en áreas de informática y la robótica [92]. Los problemas que surgieron hicieron rápidamente pensar en un cambio radical de la orientación investigadora, indicando que se debía acudir a la incorporación a los sistemas informáticos de una considerable cantidad de conocimientos con los que se pudieran tratar los datos en la materia específica donde se estuviera analizando el problema. Pero con esta nueva orientación no se solucionó el problema, ya que los conocimientos y los datos, almacenados en un sistema convencional, necesitan una estructura lógica de unión para poder ser relacionados y aplicados. De alguna forma hay que "explicar" al sistema cuándo y cómo se aplican unos determinados conocimientos en el razonamiento de resolución de un problema a partir de unos datos dados, el sistema debe "saber" las reglas de aplicación de esos conocimientos.

Es a partir de aquí cuando surgen los sistemas expertos (SE), como una herramienta de la inteligencia artificial mediante la que se puede analizar y dar solución a determinados problemas aplicando un razonamiento similar al que aplicaría un experto en esa materia al resolver el mismo problema.

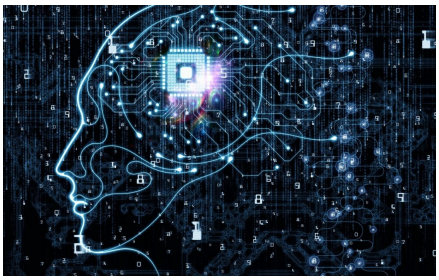


Figura 5.1: La inteligencia artificial se refiere a la capacidad de emular las funciones inteligentes del cerebro humano.

Los sistemas expertos (SE) son considerados como un subconjunto de la IA (Fig. 5.2). El nombre sistema experto deriva del término "sistema experto basado en conocimiento". Un sistema experto es un sistema que emplea conocimiento humano capturado en sistema embebido para resolver problemas que normalmente requieran de expertos humanos [93]. Los sistemas expertos se destacan entre las herramientas de soporte para la toma de decisiones donde han sido diseñados para facilitar tareas en múltiples campos de aplicación y proporcionar equivalentes resultados que un especialista, emulando la capacidad humana de tomar decisiones de acuerdo a las condiciones del contexto. Algunas aplicaciones basadas en sistemas expertos incluyen tareas como el diagnóstico médico, la localización de fallas en equipos, la interpretación de datos cuantitativos, los sistemas de recomendación, su objetivo principal es recomendar contenido adecuado al usuario en función de varios parámetros. Es utilizado para respaldar la toma de decisiones del usuario y recomendar productos, información o servicios adecuados como en las tiendas en línea [94] y turismo [95].

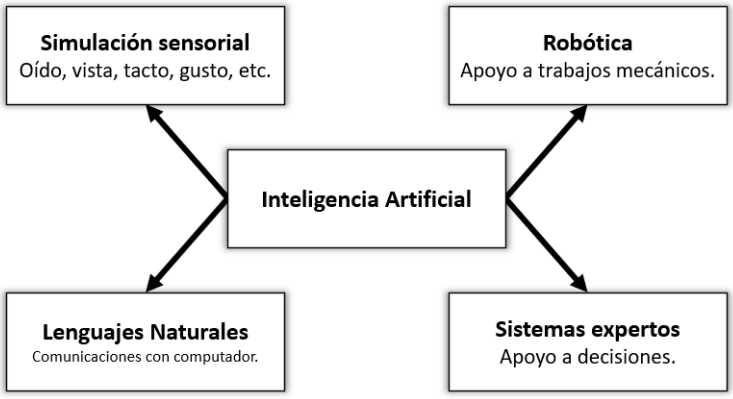


Figura 5.2: Subconjuntos de la inteligencia artificial.

Los sistemas expertos se aplican en los sistemas embebidos, los sistemas embebidos son herramientas de computación utilizadas para ejecutar tareas de control (Fig. 5.3).

En este sentido, cada sistema embebido se encarga de llevar a cabo una o varias funciones dedicadas [96]. De este modo, esta tecnología tiene la finalidad de cubrir necesidades concretas. En los sistemas embebidos, casi todos los componentes están integrados en la placa base, así, se reduce el tamaño de la solución tecnológica. La característica principal es que emplea para ello uno o varios procesadores digitales (CPUs) en formato microprocesador, microcontrolador o DSP lo que le permite aportar "inteligencia" al sistema anfitrión al que ayuda a gobernar y del que forma parte. Los sistemas embebidos se aplican en varios ámbitos profesionales. Entre ellos, se encuentra el de la automoción, la salud, la electrónica de consumo, el militar y las telecomunicaciones.

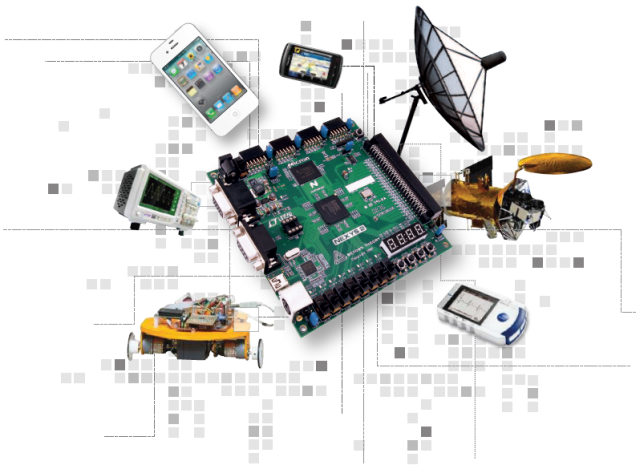


Figura 5.3: Ejemplos de sistemas embebidos.

5.2. Características de los sistemas expertos

Un sistema experto es un sistema informático que procesa conocimientos e indica decisiones a tomar en la resolución de determinados problemas, razonando sus propios procesos. En este sentido, pueden considerarse como intermediarios entre el experto humano, que transmite su conocimiento al sistema, y el usuario que lo utiliza para resolver un problema con la eficacia del especialista [97]. El sistema experto utilizará para ello el conocimiento que tenga almacenado y algunos métodos de inferencia. Por tanto, un sistema experto:

- Es un sistema informático que procesa conocimientos, representados mediante símbolos y sus relaciones, que son razonados por medio de un conjunto de reglas adecuadas a una rama o dominio del saber.
- Archiva y procesa conocimientos, junto con datos, ofreciendo una opción de entre varias en la toma de una decisión.
- Comunica al usuario la decisión tomada, a la vez que le ofrece el razonamiento de por qué ha elegido esa opción.

Para que un sistema experto pueda realizar las funciones que se han enumerado y, consecuentemente, trabajar con los conocimientos, debe estar compuesto por una serie de elementos o unidades lógicas que puedan ser desarrolladas de forma autónoma e independiente unas de otras. No existe una estructura de sistema experto común. Sin embargo, la mayoría de los sistemas expertos tienen unos componentes básicos: base de conocimientos, base de datos y motor de inferencia (Fig. 5.4).

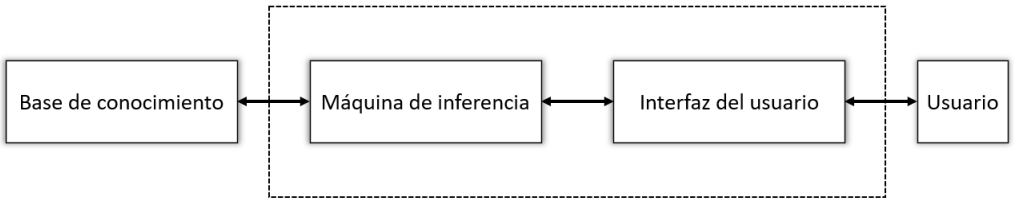


Figura 5.4: Partes básicas de un sistemas experto.

- La base de conocimientos contiene el conocimiento especializado extraído del experto en el dominio. Es decir, contiene conocimiento general sobre el dominio en el que se trabaja. El método más común para representar el conocimiento es mediante reglas de producción. El dominio de conocimiento representado se divide en pequeñas fracciones de conocimiento o reglas SI . . . ENTONCES . . . Cada regla constará de una parte denominada condición y de una parte denominada acción, y tendrá la forma; SI condición ENTONCES acción. Una característica muy importante es que la base de conocimientos es independiente del mecanismo de inferencia que se utiliza para resolver los problemas. De esta forma, cuando los conocimientos almacenados se han quedado obsoletos, o cuando se dispone de nuevos conocimientos, es relativamente fácil añadir reglas nuevas, eliminar las antiguas o corregir errores en las existentes. No es necesario reprogramar todo el sistema experto. Las reglas suelen almacenarse en alguna secuencia jerárquica lógica, pero esto no es estrictamente necesario. Se pueden tener en cualquier secuencia y el motor de inferencia las usará en el orden adecuado que necesite para resolver un problema.

- La base de datos o base de hechos es una parte de la memoria del sistema embebido que se utiliza para almacenar los datos recibidos inicialmente para la resolución de un problema. Contiene conocimiento sobre el caso concreto en que se trabaja. También se registrarán en ella las conclusiones intermedias y los datos generados en el proceso de inferencia.

- El motor de inferencias es un programa que controla el proceso de razonamiento que seguirá el sistema experto. Utilizando los datos que se le suministran, recorre la base de conocimientos para alcanzar una solución. La estrategia de control puede ser de encadenamiento progresivo o de encadenamiento regresivo. En el primer caso se comienza con los hechos disponibles en la base de datos, y se buscan reglas que satisfagan esos datos, es decir, reglas que verifiquen la parte SI.

Las ventajas de los sistemas expertos son en comparación con los humanos son [98]:

- El experto humano tiene limitaciones y percances propias de su condición humana, es decir; se enferma, envejece, migra a otras empresas, el sistema experto, no sufre de estas cuestiones y se convierte en una herramienta estable para su entorno y fiable.
- Debido a la escasez de expertos humanos en determinadas áreas, los SE pueden almacenar su conocimiento para cuando sea necesario poder aplicarlo.
- Los SE pueden ser utilizados por personas no especializadas para resolver problemas.
- La velocidad de procesamiento que es mayor al de un ser humano.
- Las actividades son completamente replicables.

Las limitaciones es que para actualizar se necesita de reprogramación, son poco flexibles a cambios y de difícil acceso a información no estructurada, carecen de sentido común, para un SE no hay nada obvio, para un sistema experto es muy complicado de aprender de sus errores y de errores ajenos. No son capaces de distinguir cuales son las cuestiones relevantes de un problema y separarlas de cuestiones secundarias.

El propósito del sistema experto en este trabajo es identificar al usuario mediante el rasgo biométrico de ECG, es una forma de detectar la presencia del usuario físicamente para poder colocar la huella dactilar para su autenticación en el sistema de acceso seguro, a fin de garantizar que solo la persona autorizada esté utilizando el sistema, además, la detección de vida mediante la señal de ECG actúa como protección contra los ataques de suplantación de identidad [99].

5.3. Sistema embebido: Arduino

La mayoría de las personas están familiarizadas con los dispositivos informáticos de propósito general, como computadoras de escritorio y portátiles. Su uso es común y soportan una amplia variedad de aplicaciones, muchas de las cuales implican un mayor acceso a aplicaciones distribuidas a través del Internet de las cosas (IoT) [100]. Los usuarios interactúan con computadoras de propósito general directamente a través de teclados, ratones y pantallas de monitor. Hay muchos dispositivos de consumo, como teléfonos móviles, tabletas y dispositivos de navegación por satélite, que se clasifican como sistemas embebidos. Admiten la interacción del usuario a través de pantallas táctiles, micrófonos y altavoces de audio. No obstante, muchos sistemas embebidos funcionan en segundo plano con poca o ninguna interacción humana directa [101].

En 2005, Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino y David Mellis, se les ocurrió la idea de un dispositivo programable fácil de usar para proyectos de diseño de arte interactivo en el Interaction Design Institute Ivrea en Ivrea, Italia.

El dispositivo debía ser simple, fácil de conectar a varias cosas (como relés, motores y sensores) y fácil de programar. También tenía que ser económico para que fuera rentable para estudiantes y artistas. Seleccionaron una familia AVR de dispositivos de microcontrolador de 8 bits (MCU) de Atmel y diseñaron una placa de circuito autónoma con conexiones fáciles de usar, escribieron el firmware del cargador de arranque para el microcontrolador y lo integraron todo en un entorno de desarrollo simple que usaba programas llamados "sketches". El resultado fue Arduino.

Arduino es un microcontrolador de código abierto que permite la programación y la interacción; está programado en C/C++ con una biblioteca Arduino para permitirle acceder al hardware. Esto permite una programación más flexible y la capacidad de usar componentes electrónicos que pueden interactuar con Arduino. Debido a que Arduino es de código abierto, los planos de los circuitos están disponibles en línea de forma gratuita para cualquier persona que quiera usar y crear su propia placa basada en los esquemas, siempre y cuando compartan lo que crean. Esto permite una personalización considerable en los proyectos; Hasta la fecha, los usuarios han construido Arduinos de diferentes tamaños, formas y niveles de potencia para controlar sus proyectos. Arduino se compone de dos partes principales:

1. La placa Arduino, que es una pieza de hardware en la que se trabaja cuando se construye el proyecto (Fig. 5.5).

2. El IDE (entorno de desarrollo integrado) de Arduino, que es una pieza de software que se ejecuta en una computadora. Se utiliza el IDE para crear un sketch (un pequeño programa de computadora) que se carga en la placa Arduino (Fig. 5.6).

Arduino se diferencia de otras plataformas en el mercado por las siguientes características:

1. Es un entorno multiplataforma; puede ejecutarse en Windows, iOS y Linux.

2. Se basa en un IDE de programación de procesamiento, que es un entorno de desarrollo fácil de usar utilizado.

3. Se programa a través de un cable USB, no un puerto serie. Esta característica es útil porque muchas computadoras modernas no tienen puertos seriales.

4. Es hardware y software de código abierto; si lo desea, puede descargar el diagrama del circuito, comprar todos los componentes y hacer su propia placa Arduino, sin pagar nada a los fabricantes de Arduino.

5. El hardware es barato.

6. Hay una comunidad activa de usuarios, por lo que hay muchas personas que comparten su ayuda.

7. El proyecto Arduino se desarrolló en un entorno educativo y es, por lo tanto, excelente para que los recién llegados hagan que las cosas funcionen rápidamente.

Figura 5.5: Placa Arduino UNO R3.

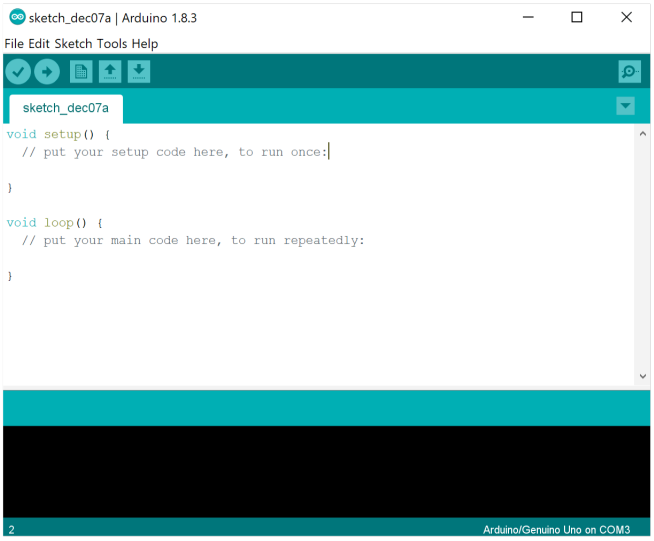


Figura 5.6: IDE de Arduino.

Arduino se está convirtiendo rápidamente en uno de los microcontroladores más populares utilizados. Hay muchos tipos diferentes de microcontroladores Arduino que difieren no solo en diseño y características, sino también en tamaño y capacidades de procesamiento. Sin embargo, solo hay dos modelos que usan chips completamente diferentes; el Estándar (UNO) y el Mega. El estándar es el Arduino básico, mientras que el Mega es una placa Arduino diferente con más pines de E/S y usa el chip Atmega2560 [102].

5.4. Conclusiones

Los sistemas expertos son una de las investigaciones más activas y productivas en el campo de la inteligencia artificial en la actualidad [103]. Los sistemas expertos han sido diseñados para facilitar las tareas en múltiples campos de aplicación y proporcionar equivalentes resultados a los de un experto humano. La base principal del sistema embebido será Arduino, en el cual se programa el sistema experto. El trabajo que desempeñara el sistema experto es poder distinguir si es la persona correcta la que está utilizando el sistema de acceso seguro mediante una serie de decisiones basado en la detección de la señal de electrocardiograma.

Capítulo 6

Mapa caótico y generador de números pseudoaleatorios propuesto

En la literatura, se han considerado mapas caóticos para diseñar generadores de números pseudoaleatorios PRNG, por sus siglas en ingles. Sin embargo, algunos mapas caóticos presentan desventajas de seguridad, como propiedades de baja uniformidad y baja aleatoriedad. Hoy en día, los PRNGs basados en el caos se utilizan como fuente principal para el desarrollo de algoritmos criptográficos. En este capítulo, se propone un novedoso mapa hypercaótico 2D basado en retroalimentación en tiempo discreto utilizando el mapa de Hénon y el mapa de Seno. Además, la dinámica del mapa hypercaótico se mejora mediante el uso de la función de resto después de la división (rem), donde se obtienen mejores propiedades estadísticas aleatorias. Se realiza una comparación entre el mapa hypercaótico mejorado de Hénon-Seno (EHSHM) y el mapa hypercaótico de Hénon-Seno (HSHM) a través del análisis del exponente de Lyapunov, la trayectoria del atractor, los histogramas y la sensibilidad en la inicialización. Después, se diseña un generador de números pseudoaleatorios de 8 bits basado en el mapa hypercaótico propuesto (PRNG-EHSHM) y se calcula la semilla inicial del PRNG mediante una clave secreta de 60 caracteres hexadecimales. Se implementa tanto en MATLAB como en el microcontrolador Arduino Mega para obtener resultados experimentales. Finalmente, se presenta un completo análisis de seguridad desde el punto de vista criptográfico.

6.1. Introducción

En los últimos dos años se ha incrementado el uso de la comunicación digital, especialmente Internet y las aplicaciones móviles debido a la demanda de los usuarios y más recientemente al COVID-19, donde se transmiten y almacenan en la nube diversos tipos de información personal mediante el uso de diferentes tipos de redes en telemedicina [104]. Existe una creciente demanda de desarrollar técnicas de encriptación utilizando el caos como núcleo principal para diseñar un PRNG que brinde confidencialidad y proteja la información digital de usuarios no autorizados.

Los sistemas caóticos son sistemas no lineales, muy sensible a las condiciones iniciales a los parámetros de control y a la imprevisibilidad, lo que los hace muy atractivos en las aplicaciones de seguridad [105]. Los algoritmos de encriptado basados en el caos ofrecen muchos beneficios, como alta velocidad en encriptado de flujo, alto nivel de seguridad, mayor modularidad, flexibilidad y facilidad de ejecución. En los últimos años, se han utilizado algoritmos de encriptado basados en mapas caóticos para encriptar información como imágenes [106, 107], texto [108], señales clínicas [109] y características biométricas [110].

El PRNG es un algoritmo para producir secuencias deterministas de números pseudoaleatorios con fórmulas matemáticas y los mapas caóticos son el núcleo principal para generar dichos números para ser aplicados en criptografía [111]. Básicamente, el propósito de la criptografía es permitir la transmisión y/o almacenamiento de información privada, de manera que cualquier intruso que acceda a la información no entienda su significado. Además, los problemas de seguridad se pueden resolver con las propiedades intrínsecas del caos que son muy similares a las propiedades criptográficas, donde se pueden desarrollar algoritmos de encriptado con PRNG como fuente principal para la generación de datos aleatorios. Estas propiedades son; las rondas de encriptado de un algoritmo criptográfico conducen a las propiedades deseadas de difusión y confusión del algoritmo y las iteraciones de un mapa caótico extienden la región inicial sobre todo el espacio de fase, la clave del algoritmo de encriptado puede representar los parámetros del mapa caótico, mientras que el espacio de clave secreta es más grande, se pueden obtener más opciones de valores para los parámetros de control y las condiciones iniciales y con más opciones de valores, más sensible es el sistema caótico y el proceso de difusión para el algoritmo (Tabla 6.1) [112]. Aunque en la literatura se propusieron varios sistemas caóticos para servir para las aplicaciones de encriptación, estos sistemas tienen estructuras complejas que pueden limitar su implementación debido a la baja aleatoriedad, la poca cantidad de datos y la baja velocidad de tiempo [113].

Tabla 6.1: Similitudes y diferencias entre sistemas caóticos y algoritmos criptográficos.

Sistemas caóticos	Algoritmos criptográficos
Espacio de fase: (sub)conjunto de números reales	Espacio de fase: conjunto finito de enteros
Iteraciones	Rondas
Parámetros	Clave
Sensibilidad a las condiciones y parámetros iniciales	Difusión
Ergodicidad	Confusión

Los sistemas caóticos unidimensionales discretos, como el mapa Logístico y el mapa Tent, generalmente tienen un desempeño deficiente en términos de rangos caóticos y resistencia a las grietas [114]. En algunos de los esquemas de PRNG basados en el caos en la literatura, los datos caóticos no son uniformes o los análisis se limitan a pruebas de aleatoriedad sin verificar las propiedades estadísticas para aplicaciones criptográficas, se prefieren los mapas caóticos de tiempo discreto en lugar de los sistemas continuos debido a la conveniencia para las realizaciones digitales. Sin embargo, la mayoría de los mapas caóticos tienen un espacio de claves limitado y sus pequeñas dimensiones brindan una seguridad débil.

En este trabajo de tesis doctoral, motivado por la discusión anterior, para superar la baja uniformidad y la baja aleatoriedad, se propone un novedoso mapa hypercaótico bidimensional de Hénon-Seno con auto-retroalimentación (2D-HSHM) a partir de la retroalimentación del mapa 1D-Hénon y 1D-Seno. Además, se mejoran las propiedades pseudoaleatorias del mapa caótico propuesto aplicando la función de resto después de la división (*rem*) y generando el 2D-EHSHM, se presenta una comparación de los dos mapas hypercaóticos con un análisis de Lyapunov, trayectoria del atractor, diagrama de bifurcación, histogramas y sensibilidad en la inicialización para mostrar las ventajas obtenidas, donde el mapa mejorado presenta mejores propiedades estadísticas, alta complejidad y sensibilidad a la condición inicial y parámetros de control. El 2D-EHSHM se utiliza para un diseño de un algoritmo de generador de números pseudoaleatorios, donde la semilla inicial se calcula mediante una clave secreta de 60 caracteres hexadecimales. El algoritmo propuesto se implementa tanto en MATLAB como en Arduino Mega. Se presenta un análisis de seguridad para validar el PRNG en aplicaciones criptográficas, donde tanto las implementaciones de software como de hardware pasaron la prueba NIST 800-22.

6.1.1. Revisión de la literatura

La primera parte de los trabajos relacionados incluye el diseño de PRNG. A continuación, se comentan trabajos de esquemas criptográficos basados en el caos para el encriptado de datos. Recientemente, se ha propuesto el desarrollo de generadores de números pseudoaleatorios basados en mapas caóticos con implementación en MATLAB [115, 116] y microcontroladores [117–119], donde en algunos trabajos, las condiciones iniciales y los parámetros de control son considerada la semilla del generador de números pseudoaleatorios. En 2022 [120], los autores presentan un PRNG utilizando el mapa caótico lineal por partes, es un sistema caótico simple que se usa popularmente para generar números y propusieron una arquitectura de hardware. En 2021 [121], los autores propusieron un PRNG usando el mapa Logístico donde la turbulencia se rellena en el mapa existente para mejorar su comportamiento caótico y aumentar la periodicidad, los autores presentan un análisis de seguridad, sin embargo, mencionan que es para aplicaciones criptográficas ligeras. En el mismo año, en [122], los autores utilizaron dos controladores de retroalimentación diferentes basados en sistemas hypercaóticos de cuatro dimensiones (4D) para diseñar un PRNG y se implementa en un microcontrolador para encriptar imágenes y presentan un análisis de seguridad. En [123], Wang y Cheng, también presentaron un PRNG basado en el mapa Logístico, donde seleccionan la semilla del PRNG manualmente utilizando las condiciones iniciales y los parámetros de control. En [124], los autores propusieron un análisis de zoom profundo de la composición del mapa Logístico y el mapa de Tent, la técnica de zoom profundo transforma cada punto de una órbita caótica dada eliminando los primeros dígitos k después del separador decimal. En [125], los autores propusieron un nuevo sistema caótico 4D con ricas características dinámicas, como atractores ocultos y atractores coexistentes, propusieron un PRNG usando el nuevo sistema caótico 4D, las condiciones iniciales y los parámetros de control se introducen manualmente.

Li-Hua *et al*, propusieron un nuevo sistema caótico 4D y un PRNG para encriptación de imágenes, presenta las propiedades dinámicas del nuevo sistema caótico 4D y el diseño PRNG fue validado con el NIST 800-22 [126]. En 2021, se propone un nuevo algoritmo cuántico de compresión y encriptado de imágenes múltiples para imágenes, que combina la transformada de coseno discreta cuántica con el mapa hypercaótico 4D de Hénon y presenta un ataque de análisis estadístico, como histograma, correlación y rendimiento de compresión [127]. En [128], los autores propusieron un método para mejorar los mapas caóticos para encriptar imágenes digitales en un esquema de comunicación inalámbrica, muestra que la función módulo (*mod*) 255 mejora la aleatoriedad de los generadores de números pseudoaleatorios y se verificó su desempeño.

6.2. Propuesta de mapa hypercaótico mejorado

En esta sección, se presenta el modelo de mapa hypercaótico 2D basado en el mapa 1D Hénon (1) y el mapa 1D Seno (2) y el proceso mejorado propuesto. El diagrama de estructura del modelo propuesto se muestra en la Fig. 6.1.

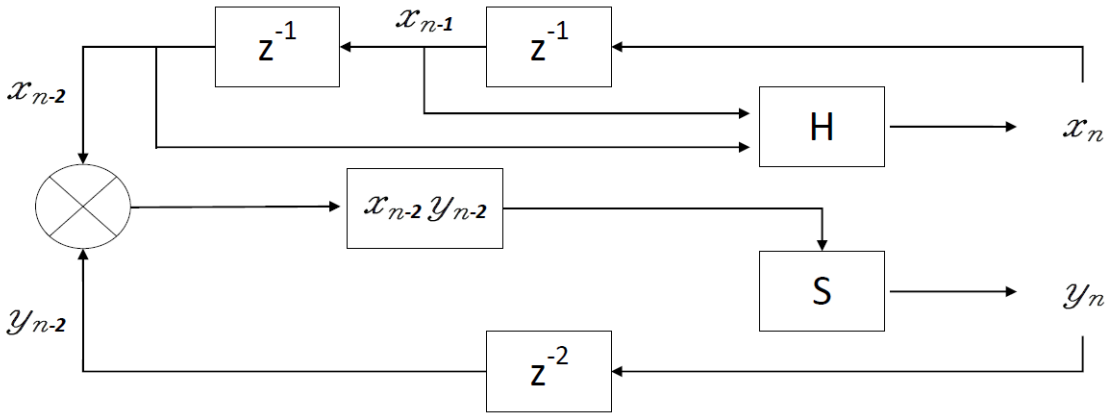


Figura 6.1: Diagrama estructural del mapa hypercaótico 2D propuesto.

En la Fig. 6.1, el símbolo $\otimes$ representa un multiplicador, z^{-1} representa un retraso en tiempo discreto, H y S son el mapa de Hénon y el mapa Seno, respectivamente.

El mapa de Hénon se puede representar como un mapa caótico unidimensional para producir secuencias caóticas no lineales, se usa como unidimensional basado en el mapa clásico de Hénon [129]. El mapa de Hénon se puede describir matemáticamente como un mapa unidimensional de la siguiente manera:

$$x_{n+1} = 1 - \alpha x_n^2 + \beta x_{n-1}, \tag{6.1}$$

donde x_n es el estado del mapa, x_0 es la condición inicial, α y β son los parámetros de control y $n = 0, 1, 2, ...N$ es el número de iteraciones. El mapa de Hénon presenta dinámicas caóticas con $\alpha = 1.40$ y $\beta = 0.30$.

El mapa Seno es un mapa caótico unidimensional [130]. El mapa Seno se puede describir matemáticamente de la siguiente manera:

$$x_{n+1} = \gamma sin(\pi x_n), \tag{6.2}$$

donde x_n es el estado del mapa, x_0 es la condición inicial, $\gamma \in (0, 4)$ es el parámetro de control y $n = 0, 1, 2, ...N$ es el número de iteraciones.

Basado en el mapa Hénon y el mapa Seno con el diagrama estructural propuesto en la Fig. 6.1, el mapa hypercaótico 2D Hénon-Seno propuesto se describe de la siguiente manera:

$$x_n = 1 - \alpha(x_{n-1})^2 + \beta x_{n-2}, \tag{6.3a}$$
$$y_n = \gamma sin(\pi x_{n-2} y_{n-2}), \tag{6.3b}$$

donde x_n y y_n son los estados del mapa, α, β y γ son los parámetros de control.

Se propone un método para mejorar la dinámica caótica del mapa hypercaótico propuesto para producir mejores secuencias pseudoaleatorias, aumentar el rango de los parámetros de control y la sensibilidad a las condiciones iniciales aplicando la función matemática resto después de la división (rem).

El mapa hypercaótico mejorado de Hénon-Seno tiene la siguiente expresión:

$$x_{n+1} = rem((1 - \alpha x_n^2 + \beta x_{n-1}) * 101, 1), \tag{6.4a}$$
$$y_{n+1} = rem((\gamma sin(\pi x_{n-1} y_{n-1})) * 101, 1), \tag{6.4b}$$

donde x_n y y_n son los estados del mapa hypercaótico, x_0 y y_0 son las condiciones iniciales y α, β y γ son los parámetros de control, la función rem es la operación de resto después de la división considerando aritmética de punto flotante de 32 bits.

$$rem(a, b) = a - (INT(a/b) * b), \tag{6.5}$$

donde a es el dividendo, b es el divisor y INT redondea un número al entero más cercano, básicamente calcula el resto después de realizar la división de enteros en la expresión del dividendo por la expresión del divisor.

Aplicando la función rem y multiplicando la dinámica caótica por 101 en (6.4a y 6.4b), se obtiene una distribución mucho más uniforme de la dinámica caótica, ya que se transforman todos los datos originales a datos con valores entre -1 y 1. Estos resultados se muestran comparando el HSHM y el EHSHM a través del exponente de Lyapunov, la trayectoria del atractor, el diagrama de bifurcación, los histogramas y la sensibilidad en la inicialización en las siguientes subsecciones.

6.2.1. Exponente de Lyapunov

Se verifica la dinámica caótica numéricamente con el exponente de Lyapunov (LE). El exponente de Lyapunov mide la tasa promedio de divergencia o convergencia de dos trayectorias cercanas en el espacio de fase. Un exponente de Lyapunov positivo indica caos [131], un mapa 1D tiene solo un exponente de Lyapunov y un mapa 2D tiene dos exponentes de Lyapunov, cuanto mayor sea el valor del exponente de Lyapunov, el mapa caótico es más sensible a las condiciones iniciales y los parámetros de control. Se calcula el exponente de Lyapunov con (6.6) del mapa de Hénon, mapa Seno, HSHM y EHSHM con dos trayectorias usando los mismos parámetros de control, pero condiciones iniciales muy cercanas.

$$\lambda = \frac{1}{I}\ ln\ \left|\frac{f^n(x_n - \delta_0) - f^n(x_n)}{\delta_0}\right| \tag{6.6}$$

donde λ es el exponente de Lyapunov, x_0 es la condición inicial, $x_0' = x_0 + \delta_0$ es otra condición inicial muy cercana y I es el número de iteraciones. Los valores utilizados para las condiciones iniciales son $x_0 = 0.5123456$ y $y_0 = 0.5765432$, para los parámetros de control son $\alpha = 1.4000000$, $\beta = 0.3000000$ y $\gamma = 0.8123578$, una perturbación de $\delta_0 = 5 \times 10^{-6}$ y la iteración $I = 10000$. En la Tabla 6.2, se presentan los resultados obtenidos de λ, donde se observa que EHSHM tiene exponentes de Lyapunov más grandes (6.2466 y 6.0612), lo que indica que es más sensible a las condiciones iniciales y parámetros de control en comparación con HSHM que tiene valores bajos de LE. Además, tiene dos LE positivos, lo que indica hypercaos, el sistema hypercaótico se define matemáticamente como un sistema caótico, lo que implica que su dinámica se distribuye en muchas direcciones diferentes simultáneamente, mejorando las características caóticas del mapa. El atractor hypercaótico tiene comportamientos dinámicos más complejos en comparación con el sistema caótico [132, 133].

Tabla 6.2: Exponentes de Lyapunov del mapa Hénon, mapa Seno, HSHM y EHSHM.

λ	mapa Hénon	mapa Seno	mapa HSHM	mapa EHSHM
x	0.1718367	0.4152323	0.6570296	6.2466736
y	—	—	0.5953513	6.0612888

6.2.2. Trayectoria del atractor

La trayectoria del atractor caótico es un método de observación directa, se distribuye en un espacio de fase limitado del sistema caótico. Para el sistema caótico, si el movimiento de la trayectoria del atractor se distribuye en un rango amplio y uniforme, indica que los valores de salida del sistema tienen mejor aleatoriedad. Se itera 20000 veces y se muestra la trayectoria del mapa de Hénon (Fig. 6.2(a)), el mapa Seno (Fig. 6.2(b)), HSHM (Fig. 6.2(c)) y EHSHM (Fig. 6.2(d)). Los resultados en la Fig. 6.2(d) muestran que la trayectoria del atractor EHSHM se distribuye más uniformemente en todo el espacio de fases. Por lo tanto, los valores de salida tienen mejor aleatoriedad, debido a que los datos se distribuyen a lo largo de todo el espacio de fase.

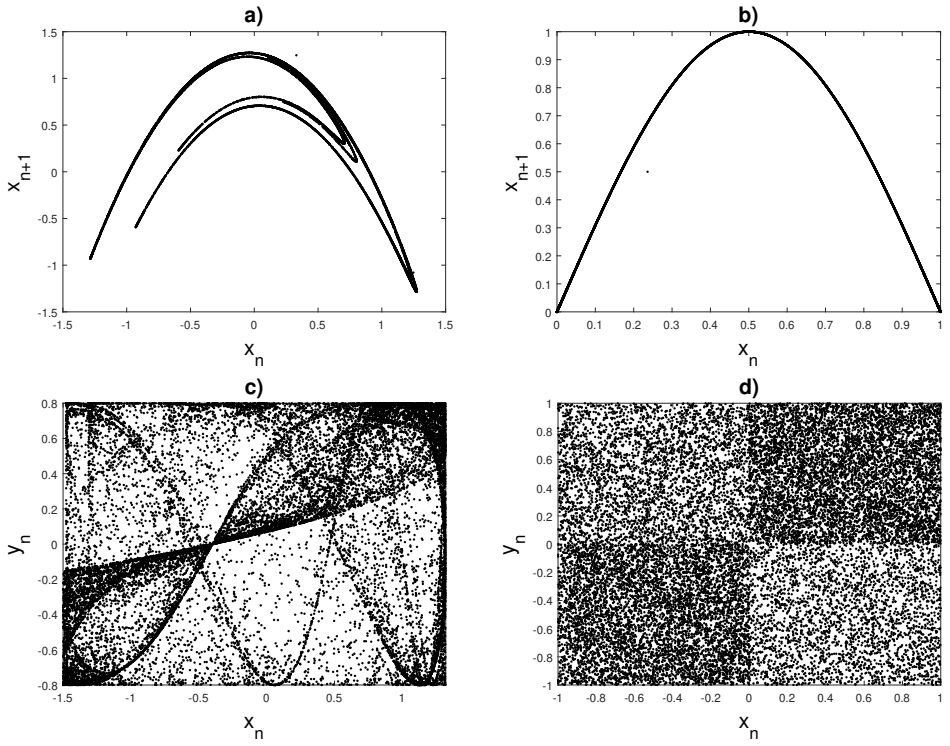


Figura 6.2: Trayectoria del atractor: a) Mapa de Hénon, b) Mapa de Seno, c) HSHM y d) EHSHM.

6.2.3. Diagrama de bifurcación

Cuando se cambia el parámetro del sistema, también se cambia el estado de movimiento del sistema. El diagrama de bifurcación puede ver visualmente el proceso de cambio de estado del sistema con los parámetros de control. El diagrama de bifurcación de HSHM y EHSHM del estado x con β fijo se muestra en la Fig. 6.3(a) y la Fig. 6.3(b) respectivamente. Los resultados en la Fig. 6.3(b), demuestran que el EHSHM no tiene ningún estado periódico, es un estado caótico entre el rango $\alpha = [0, 1.4]$. Por lo tanto, el estado caótico tiene una amplia gama de parámetros, lo que indica que puede aumentar el espacio de claves para aplicaciones criptográficas.

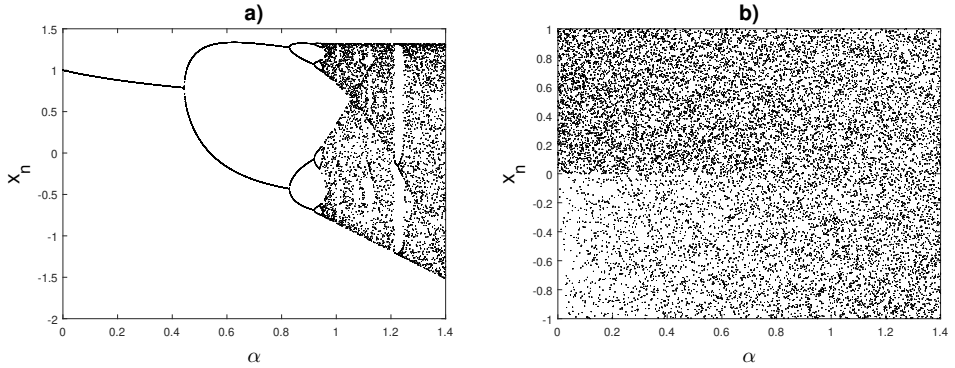


Figura 6.3: Diagrama de bifurcación: a) HSHM y b) EHSHM.

6.2.4. Histograma

Un histograma muestra la frecuencia de cada elemento de forma gráfica, es decir, cuántas veces aparece cada símbolo en una secuencia. En la Fig. 6.4(a) y la Fig. 6.4(b), se muestra el histograma de 10000 valores del estado x de HSHM y EHSHM, es claro que el estado x de HSHM no presenta una buena distribución de datos caóticos, donde las altas frecuencias están cerca de -1.5 y 1.4. Sin embargo, en EHSHM después de aplicar la función *rem*, los resultados muestran una mejor distribución de datos caóticos con valores entre -1 y 1. En la Fig. 6.4(c) y la Fig. 6.4(d), es el mismo caso con el estado y.

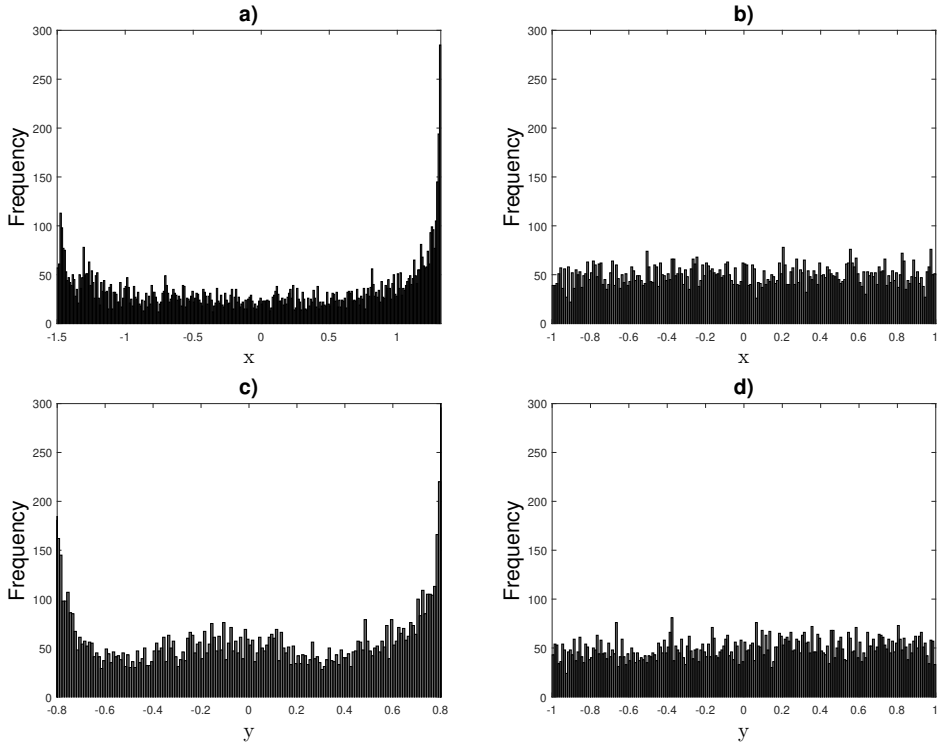


Figura 6.4: Histograma del estado x: a) HSHM y b) EHSHM, histograma del estado y: c) HSHM y d) EHSHM.

6.2.5. Sensibilidad en la inicialización

Se presenta la divergencia en el tiempo de dos trayectorias con condiciones iniciales similares $IC1 = 0.5067886$ y $IC2 = 0.5067887$. En la Fig. 6.5(a) y la Fig. 6.5(b), el estado x y el estado y para HSHM, la Fig. 6.5(c) y la Fig. 6.5(d), el estado x y y para EHSHM. En la Fig. 5(c) y la Fig. 5(d), se observa que el EHSHM es más sensible a las condiciones iniciales, las trayectorias comienzan a divergir alrededor de la iteración 30 para HSHM y 3 para EHSHM. Como resultado, el mapa hypercaótico mejorado de Hénon-Seno, presenta mejores propiedades estadísticas uniformes y mayor sensibilidad en las condiciones iniciales y parámetros de control, según el análisis presentado, se utiliza en la propuesta de un PRNG para producir números pseudoaleatorios con alta aleatoriedad que se describe en la siguiente sección.

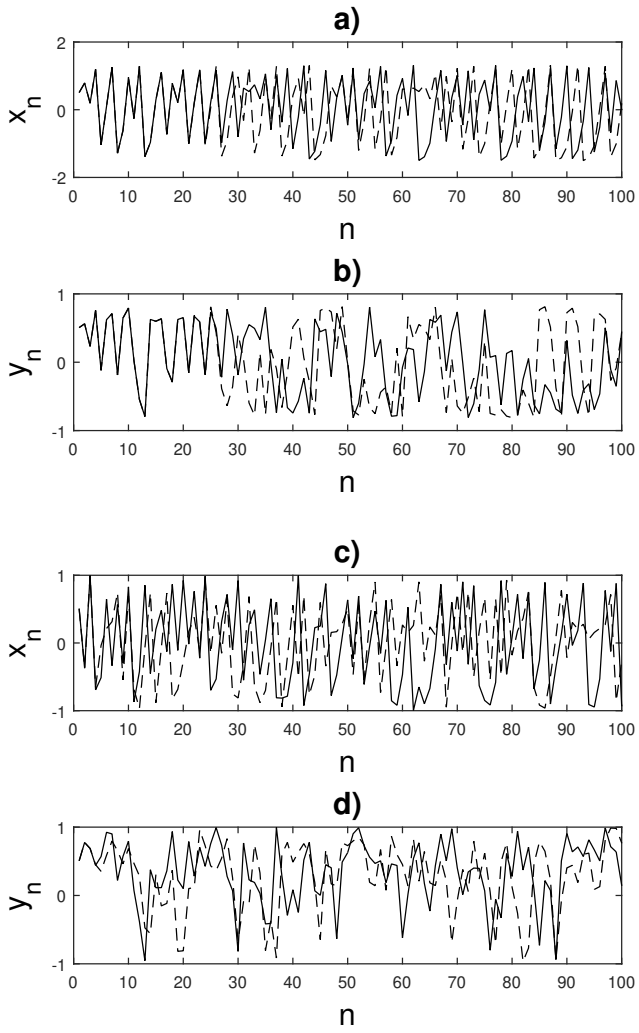


Figura 6.5: Gráfica de sensibilidad a las condiciones iniciales: a) Estado x, b) Estado y de HSHM, c) Estado x y d) Estado y de EHSHM.

6.3. Generador de números pseudoaleatorios basado en mapa hypercaótico 2D Hénon-Seno mejorado

Un generador de números pseudoaleatorios es un algoritmo que produce secuencias de números que es una muy buena aproximación a un conjunto aleatorio de números. Para el algoritmo PRNG-EHSHM propuesto, se usan las secuencias caóticas de la expresión (6.4a) y la expresión (6.4b), para aumentar la aleatoriedad. Se implementa una forma indirecta de calcular las condiciones iniciales y los parámetros de control mediante el uso de 60 caracteres hexadecimales basados en el trabajo en [134].

Los pasos del algoritmo PRNH-EHSHM propuesto se describen a continuación:

1. **Definir la clave secreta**. Las condiciones iniciales y los parámetros de control del EHSHM, se determinan a partir de 60 caracteres hexadecimales seleccionados de forma manual o aleatoria. La clave de 230 bits $K \in [0-9, A-F]$, se divide en 10 secciones $(A, B, C, D, E, F, G, H, I, J)$, como se muestra en Tabla 6.3.

Tabla 6.3: Definición de clave secreta.

Clave secreta	PRNG-EHSHM		
60 Caracteres Hex	$H_1, H_2, \ldots, H_{60}$ donde $H \in [0-9, A-F]$		
Valores	$A = \frac{(H_1,H_2,\ldots,H_6)_{10}}{2^{23}+1}$	$B = \frac{(H_7,H_8,\ldots,H_{12})_{10}}{2^{23}+1}$	$C = \frac{(H_{13},H_{14},\ldots,H_{18})_{10}}{2^{23}+1}$
	$D = \frac{(H_{19},H_{20},\ldots,H_{24})_{10}}{2^{23}+1}$	$E = \frac{(H_{25},H_{26},\ldots,H_{30})_{10}}{2^{23}+1}$	$F = \frac{(H_{31},H_{32},\ldots,H_{36})_{10}}{2^{23}+1}$
	$G = \frac{(H_{37},H_{38},\ldots,H_{42})_{10}}{2^{23}+1}$	$H = \frac{(H_{43},H_{44},\ldots,H_{48})_{10}}{2^{23}+1}$	$I = \frac{(H_{49},H_{50},\ldots,H_{54})_{10}}{2^{23}+1}$
	$J = \frac{(H_{55},H_{56},\ldots,H_{60})_{10}}{2^{23}+1}$		
Parámetros de control	$\alpha = rem(A+B,1)$	$\beta = rem(C+D,1)$	$\gamma = rem(E+F,1)$
Condiciones iniciales	$x = rem(G+H,1)$	$y = rem(I+J,1)$	

2. **Iterar EHSHM**. El mapa hypercaótico se itera N veces usando la expresión (6.4a) y la expresión (6.4b), para producir una secuencia pseudoaleatoria con números decimales entre $(0, 1)$ considerando aritmética de punto flotante de 32 bits, para obtener una precisión decimal de 10^{-7}.

3. **Las secuencias del paso 2 se convierten de decimal a entero de 8 bits**. Cada valor de la secuencia caótica se transforma en un número entero de 8 bits con las siguientes expresiones:

$$PRNGX = round(x_n \times 255), \tag{6.7a}$$
$$PRNGY = round(y_n \times 255), \tag{6.7b}$$

donde $n = 0, 1, 2, ..., N$ es el número de iteraciones, *round* es el redondeo a la operación más cercana y $PRNGX \in [0, 255]$, $PRNGY \in [0, 255]$ son las secuencias pseudoaleatorias.

6.3.1. Análisis de PRNG-EHSHM en MATLAB

Primero se implementa el PRNG-EHSHM a nivel de software en MATLAB para observar las gráficas temporales, histogramas, verificar la entropía de la información y la aleatoriedad con el conjunto de pruebas estadísticas NIST 800-22, ya que es necesario determinar la seguridad, eficiencia y pseudoaleatoriedad para aplicaciones en criptografía. En la Fig. 6.6, se observa las gráficas temporales del PRNG-EHSHM, las primeras 100 iteraciones donde se muestra la evolución en el tiempo de las trayectorias del estado x y y, se obtuvieron valores entre 0 y 1. En la Fig. 6.7, el histograma de 10000 datos de valores de 0-255 se obtienen de las secuencias de estados x y y, donde se observa una distribución uniforme de los datos obtenidos.

La entropía de la información mide la aleatoriedad de la secuencia en valores enteros y los valores altos de entropía significan un PRNG robusto. Cuando más caótica es una secuencia, mayor es la entropía de la información. La entropía $H(m)$ de una secuencia m se define como sigue:

$$H(m) = \sum_{i=0}^{2^N-1} p\left(m_i\right) log_2 \left(\frac{1}{p\left(m_i\right)}\right), \tag{6.8}$$

donde N es el número de bits de cada elemento de la secuencia m, 2^N son todos los símbolos posibles en la secuencia, $p(m_i)$ representa una probabilidad del elemento m_i en la secuencia y la entropía se expresa en bits. En el PRNG-EHSHM propuesto, la entropía máxima es 8. En la Fig. 6.8, se muestra el resultado de la entropía calculada a partir de 50 secuencias pseudoaleatorias utilizando 50 claves seleccionadas al azar. La entropía promedio de 50 pruebas es 7.9934. Por lo tanto, el PRNG-EHSHM propuesto tiene altas propiedades pseudoaleatorias.

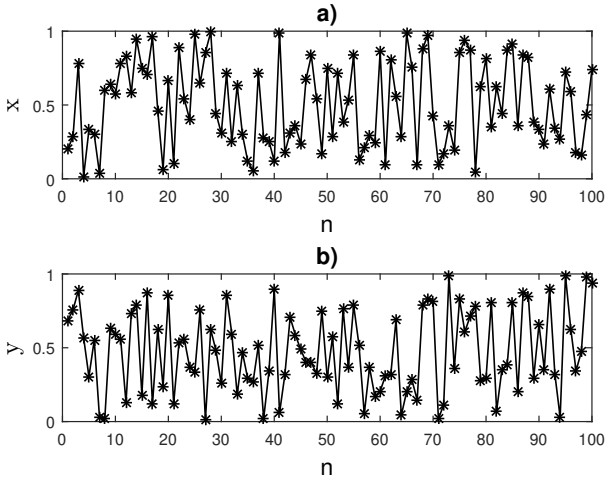


Figura 6.6: Gráficas temporales del PRNG-EHSHM: a) Estado x y b) Estado y.

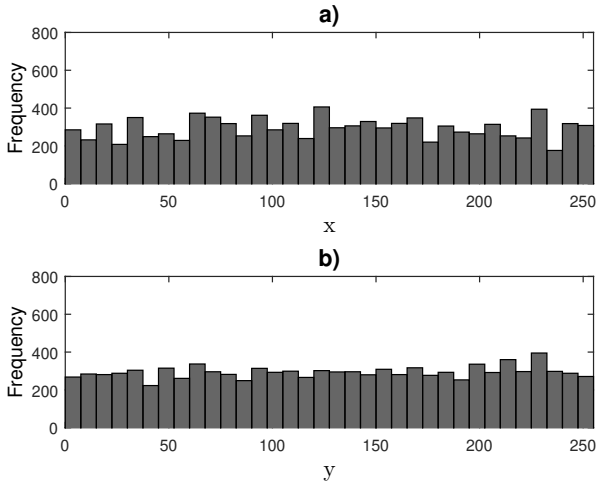


Figura 6.7: Histograma del PRNG-EHSHM: a) Estado x y b) Estado y.

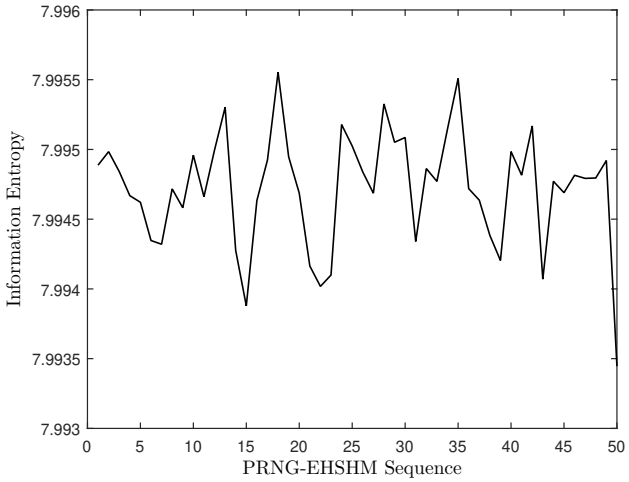


Figura 6.8: Análisis de entropía de la información para la implementación de MATLAB.

6.3.2. Prueba de aleatoriedad NIST 800-22

El NIST 800-22 es un conjunto de pruebas estadísticas para determinar el nivel de aleatoriedad en generadores de números pseudoaleatorios para aplicaciones criptográficas. La Tabla 6.4, presenta el nombre en inglés de las 15 pruebas del NIST 800-22 [135].

Tabla 6.4: Definición de pruebas NIST 800-22.

Number	NIST 800-22 test
1	Frequency test (FT)
2	Frequency test within a block (FBT)
3	Cumulative sum test (CST)
4	Runs test (RT)
5	Test for the longest run of ones in a block (LROBT)
6	Binary matrix rank test (BMRT)
7	Discrete Fourier transform test (DFTT)
8	Non-overlapping template matching test (NTMT)
8	Overlapping template matching test (OTMT)
10	Maurer's universal statistical test (MUST)
11	Approximate entropy test (AET)
12	Random excursions test (RET)
13	Random excursions variant test (REVT)
14	Serial test (ST)
15	Linear complexity test (LCT)

Las 15 pruebas se aplican a 1000 secuencias PRNG-EHSHM generadas por 1000 claves diferentes seleccionadas al azar. Con base en [136], se calcula la probabilidad *P-value*. El *P-value* debe ser mayor que un umbral predefinido $\alpha = 0.01$ para pasar la prueba. Si todas las pruebas pasan, la secuencia se considera aleatoria con una confianza de $1 - \alpha$; de lo contrario, la secuencia no se considera aleatoria. En la Tabla 6.5, se muestra el resultado de las 15 pruebas realizadas, donde todas las pruebas están por encima del intervalo aceptable según [136], el rango de proporción aceptable es [0.9833245, 0.9966745], se obtiene que la mayoría de las secuencias pasan todas las pruebas de aleatoriedad y el valor promedio es 99 %.

Tabla 6.5: Resultados de la prueba NIST 800-22 basados en la implementación de MATLAB.

No.	Prueba estadística	Recuento de secuencias con $P\text{-}value \geq 0.01$	Recuento de secuencias con $P\text{-}value < 0.01$	Proporción Exitosa
1	FT	993	7	0.993
2	FTB	999	1	0.999
3	CST	999	1	0.999
4	RT	989	11	0.989
5	LROBT	983	17	0.983
6	BMRT	984	16	0.984
7	DFTT	984	16	0.984
8	NTMT	984	16	0.984
9	OTMT	999	1	0.999
10	MUST	990	10	0.990
11	AET	993	7	0.993
12	RET	984	16	0.984
13	REVT	993	7	0.993
14	ST	983	17	0.983
15	LCT	988	12	0.988

6.4. Implementación del PRNG-EHSHM en microcontrolador

El PRNG-EHSHM propuesto se implementa a nivel de hardware en el microcontrolador Arduino Mega (Fig. 6.9) [137]. Arduino Mega utiliza el microcontrolador ATmega2560, el microcontrolador de bajo consumo y alto rendimiento, el microchip AVR de 8 bits basado en RISC y 32 registros de trabajo de propósito general. El dispositivo alcanza un rendimiento de 16 MIPS a 16 MHz y opera entre $4.5-5.5$ voltios, entre otras características importantes para casi cualquier aplicación. El software Arduino (IDE) de código abierto facilita la escritura del código y la carga en la placa.

El PRNG-EHSHM se implementa en Arduino Mega con aritmética de punto flotante de 32 bits y la salida se define como un entero sin signo de 8 bits. La Fig. 6.10, muestra el histograma de 20000 datos de 8 bits (valores entre 0 y 255), que se almacenan en un archivo **.tex* para ser analizados en MATLAB.

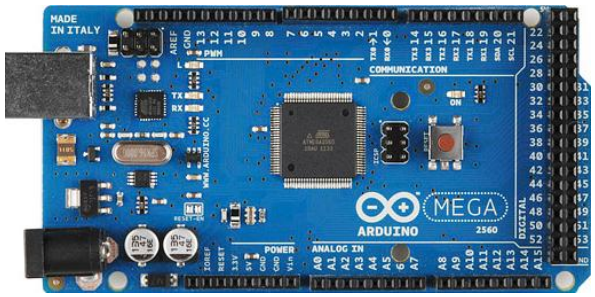


Figura 6.9: Placa Arduino Mega.

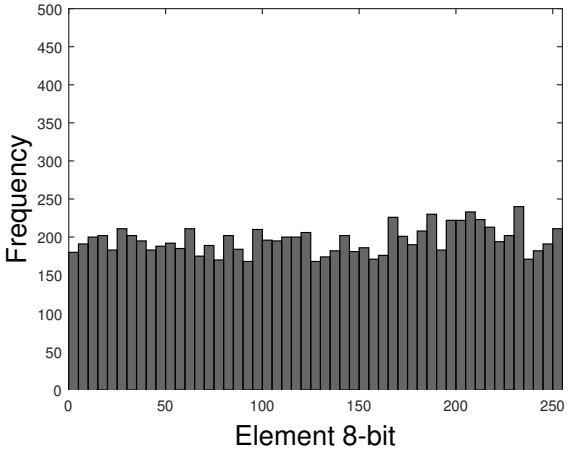


Figura 6.10: Histograma de datos de 8 bits extraídos de Arduino Mega.

Se determina el exponente de Lyapunov del PRNG-EHSHM a partir de tres secuencias obtenidas de Arduino Mega con tres claves aleatorias. En la Tabla 6.6, se presentan los resultados, que indican que las secuencias en Arduino Mega son caóticas y muy sensibles a las condiciones iniciales y los parámetros de control.

Tabla 6.6: Exponente de Lyapunov para PRNG-EHSHM en microcontrolador.

Sequence	λ x	λ y
1	6.2245	6.0351
2	6.2512	6.0187
3	6.2685	6.0415

6.5. Análisis de seguridad basado en la implementación en microcontrolador

Se realizan varios análisis de seguridad desde un punto de vista criptográfico mediante criptogramas extraídos del microcontrolador y utilizando MATLAB para los diferentes análisis de seguridad. El PRNG debe resistir todos los ataques conocidos, como espacio de claves, sensibilidad de claves, frecuencia flotante, histogramas, correlación, autocorrelación y entropía de la información. Además, la prueba NIST 800-22 para verificar la aleatoriedad del PRNG-EHSHM propuesto para aplicaciones en criptografía.

6.5.1. Espacio de claves

La clave secreta de un PRNG debe tener más de 2^{100} claves secretas posibles como se menciona en [138], para resistir un ataque exhaustivo. En el PRNG propuesto, la clave viene dada por 60 caracteres hexadecimales y de acuerdo con [139] de punto flotante estándar de IEEE, específicamente binario 32, la precisión computacional del número de precisión simple de 32 bits es de aproximadamente 10^{-9}. Si asumimos la precisión de 10^{-7} y aritmética de punto flotante de 32 bits, donde solo se consideran 23 bits para la clave, el PRNG-EHSHM propuesto tiene 2^{230} claves posibles, donde todos de ellos se consideran fuertes.

6.5.2. Sensibilidad de clave

Una propiedad básica de los mapas caóticos y los PRNG es ser sensibles a pequeños cambios en las condiciones iniciales. La sensibilidad de la clave secreta significa que solo un pequeño cambio en la clave provoca grandes cambios en la salida, generando una secuencia pseudoaleatoria totalmente diferente. Las siguientes pruebas de sensibilidad de clave del algoritmo PRNG-EHSHM se realizaron utilizando cuatro claves similares, que difieren en solo un bit (Tabla 6.7).

En la Fig. 6.11, se presenta la trayectoria pseudoaleatoria (las primeras 20) generadas por el PRNG propuesto usando las cuatro claves. Después de tres iteraciones, las dinámicas son totalmente diferentes entre sí.

Tabla 6.7: Claves secretas utilizadas para el análisis de sensibilidad de claves.

Número de clave	Clave secreta
CLAVE 1	1122334455667788990AABBCCDDEEFF1122334455667788112233445566
CLAVE 2	**2**122334455667788990AABBCCDDEEFF1122334455667788112233445566
CLAVE 3	**3**122334455667788990AABBCCDDEEFF1122334455667788112233445566
CLAVE 4	**4**122334455667788990AABBCCDDEEFF1122334455667788112233445566

Otro análisis que se utiliza para medir la diferencia entre dos secuencias es NPCR (Net Pixel Change Rate), que se determina con (6.9). Determina cuántos elementos son diferentes entre las secuencias en porcentaje:

$$NPCR = \frac{\sum_{n=0}^{I} W(n)}{N} \times 100 \tag{6.9}$$

donde

$$W(n) = \begin{cases} 0 & \text{si } S_1(n) = S_2(n) \\ 1 & \text{si } S_1(n) \neq S_2(n) \end{cases} \tag{6.10}$$

UACI (Intensidad de cambio promedio unificado) que se determina con (6.11), mide cuánto difiere una secuencia de otra en magnitud en promedio.

$$UACI = \frac{100}{N} \sum_{n=0}^{N} |S_1(n) - S_2(n)| \tag{6.11}$$

En este análisis, se determina una secuencia de PNRG-EHSHM usando la CLAVE 1 de la Tabla 6.7 para producir S_1. Se generan 20 secuencias para S_2 con 20 claves con un bit diferente a la CLAVE 1. Los resultados de NPCR y UACI se muestran en la Tabla 6.8, donde el algoritmo propuesto es altamente sensible a nivel de bit en la clave secreta, ya que las secuencias probadas son más del 99.60 % diferentes con una magnitud del 33.29 % de media.

Tabla 6.8: Resultados de sensibilidad clave.

Análisis	Resultados
NPCR	99.6077 %
UACI	33.2951 %

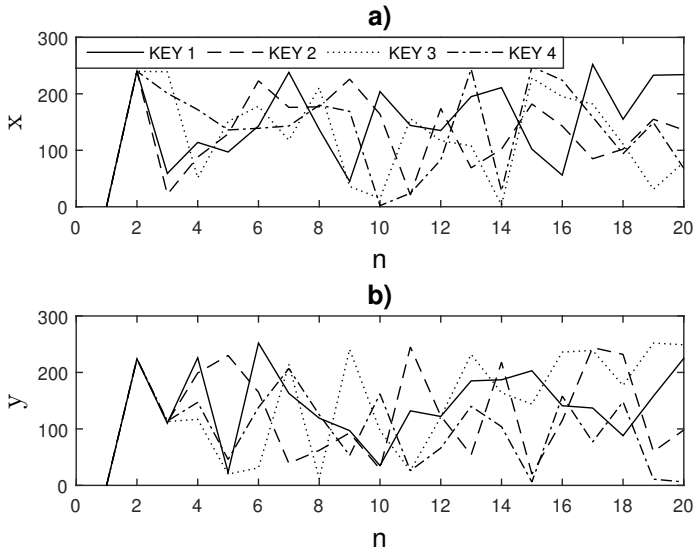


Figura 6.11: Sensibilidad a la clave de las primeras 20 iteraciones para PRNG-EHSHM en Arduino Mega: a) Estado x y b) Estado y.

6.5.3. Frecuencia flotante

El análisis de frecuencia flotante (FF) se utiliza para determinar si las secuencias pseudoaleatorias exhiben secciones fuertes o débiles. En el PRNG-EHSHM propuesto se evalúan ventanas de 256 símbolos, esperando tener la mayor cantidad de elementos diferentes. Primero, se selecciona una ventana de los 256 símbolos y se comprueba cuántos elementos son diferentes, luego se desplaza la ventana un elemento a la derecha y se obtiene de nuevo la frecuencia flotante. La Fig. 6.12, muestra el resultado de la frecuencia flotante para cuatro secuencias de 2500 elementos (8 bits) usando las cuatro claves de la Tabla 6.7.

Los resultados muestran uniformidad en Fig. 6.12(a): 161.69, Fig. 6.12(b): 161.96, Fig. 6.12(c): 161.84 y Fig. 6.12(d): 162.66, tienen diferentes elementos en promedio, Por lo tanto, el PRNG produce propiedades pseudoaleatorias uniformes.

6.5.4. Histogramas

Un buen PRNG debe presentar un histograma uniforme con cualquier clave secreta. En la Fig. 6.13, se obtienen cuatro histogramas con 5000 números de 8 bits del PRNG-EHSHM con cuatro claves secretas diferentes de la Tabla 6.7. Basado en los histogramas, el PRNG propuesto genera salidas uniformes.

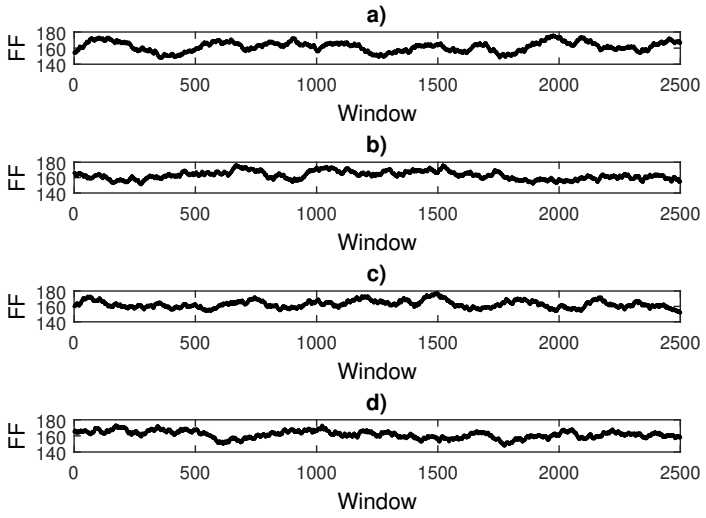


Figura 6.12: Análisis de frecuencia flotante: a) Resultados FF para CLAVE 1, b) Resultados FF para CLAVE 2, c) Resultados FF para CLAVE 3 y d) Resultados FF para CLAVE 4.

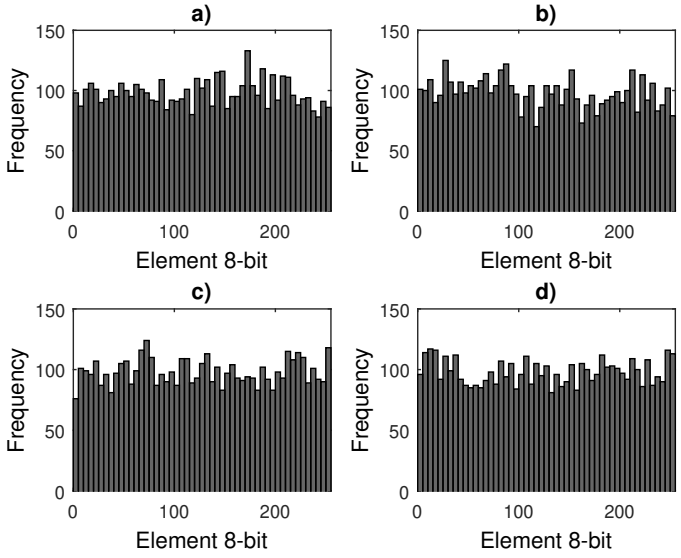


Figura 6.13: Histogramas de PRNG-EHSHM: a) Histograma para CLAVE 1, b) Histograma para CLAVE 2, c) Histograma para CLAVE 3 y d) Histograma para CLAVE 4.

6.5.5. Correlación

La correlación determina si existe una relación entre dos secuencias de la misma longitud, se calcula con (6.12). El valor de correlación es $Cr \in (-1, 1)$, donde 0 significa correlación nula y 1 correlación alta.

$$Cr = \frac{N\sum_{i=0}^{N}(x_i y_i) - \sum_{i=0}^{N} x_i \sum_{i=0}^{N} y_i}{\sqrt{\left(N\sum_{i=0}^{N}(x_i)^2 - \left(\sum_{i=0}^{n} x_i\right)^2\right)\left(N\sum_{i=0}^{N}(y_i)^2 - \left(\sum_{i=0}^{n} y_i\right)^2\right)}} \tag{6.12}$$

donde x y y son valores de dos secuencias y N es el número de elementos en una secuencia.

El promedio de correlación es $Cr = 0.0012$ a partir de 10 secuencias pseudoaleatorias generadas por 10 claves seleccionadas aleatoriamente. El resultado es cercano a 0, lo que indica que las secuencias son independientes sin relación entre sí.

6.5.6. Autocorrelación

La autocorrelación (AC) se calcula con (6.13) y determina si el PRNG-EHSHM genera secuencias o patrones repetitivos.

$$AC(k) = \frac{A - D}{N}, \tag{6.13}$$

donde $AC \in [-1, 1]$, la autocorrelación del PRNG desplazado k posiciones, A es el número de coincidencias entre la secuencia original y desplazada, D es el número de desajustes y N es la longitud de la secuencia. Los valores cercanos a 1 significan que muchos bits son idénticos, los valores cercanos a -1 significan que muchos bits son opuestos y los valores de 0 significan que hay el mismo número de bits idénticos y opuestos.

En este análisis, se calcula la autocorrelación a nivel de bit, la autocorrelación se logra hasta $k = 500$ a la derecha usando desplazamiento circular. En la Fig. 6.14, se muestran los resultados de AC de tres secuencias de 2500 datos de 8 bits, generados a partir de las primeras tres claves de la Tabla 6.7. Los resultados presentan una AC cercana a cero para todas las pruebas. Por lo tanto, el PRNG-EHSHM produce números pseudoaleatorios uniformes sin patrones repetitivos ni periodicidad.

6.5.7. Entropía de la información

La entropía de la información mide cuánto desorden tiene el PRNG en la salida, ya que el PRNG debe producir números impredecibles. Valores altos de entropía significan un generador pseudoaleatorio robusto, mientras que valores bajos de entropía significan un generador pseudoaleatorio débil con cierto grado de previsibilidad. El resultado promedio de 10 secuencias con 10 claves seleccionadas aleatoriamente del PRNG-EHSHM implementado en Arduino Mega es 7.9965. Por lo tanto, las secuencias son impredecibles.

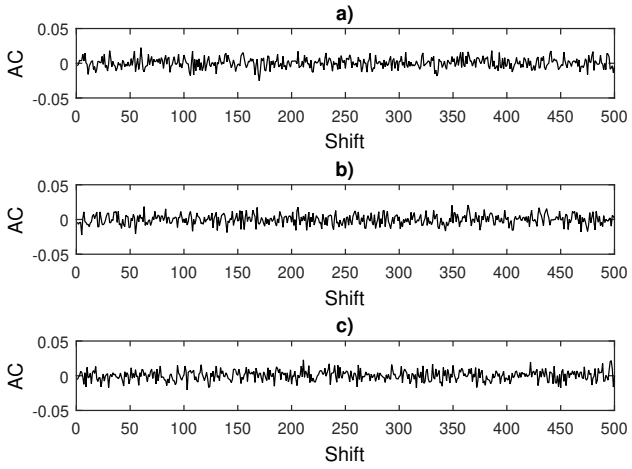


Figura 6.14: Análisis de autocorrelación: a) AC para CLAVE 1, b) AC para CLAVE 2 y c) AC para CLAVE 3.

6.5.8. Prueba NIST 800-22

En los criptosistemas basados en el caos, es importante verificar el PRNG. Las secuencias generadas por el PRNG-EHSHM implementado en Arduino Mega, están sujetas a NIST 800-22 para verificar la aleatoriedad. Se extraen 20 secuencias de Arduino Mega y los resultados promedio se muestran en la Tabla 6.9, donde el PRNG-EHSHM implementado en Arduino Mega puede generar secuencias pseudoaleatorias que superan el conjunto de pruebas NIST 800-22.

6.5.9. Rendimiento

Se calcula el tiempo que tarda el PRNG en generar 1000 datos caóticos en MATLAB y Arduino Mega, se generan 10 secuencias caóticas con 10 claves secretas diferentes y se obtiene la media. En la Tabla 6.10 se muestran los resultados obtenidos con una velocidad satisfactoria.

6.5.10. Discusión y comparaciones con la literatura

Las propiedades del caos, como el comportamiento aleatorio, el comportamiento ergódico y la extrema sensibilidad a las condiciones iniciales, hacen que los sistemas caóticos sean muy atractivos para el diseño PRNG y las aplicaciones criptográficas. Los mapas caóticos con datos uniformes y alta velocidad de procesamiento son importantes para el desarrollo de un PRNG, ya que generan más datos aleatorios y reducen la repetibilidad. Además, la velocidad de generación de estos datos es necesaria cuando se utiliza en aplicaciones de seguridad. El PRNG es un módulo importante en el desarrollo de criptosistemas para ser robustos frente a diferentes tipos de ataques de seguridad. Por lo tanto, es necesario el desarrollo de un PRNG con buenas cualidades aleatorias y alta velocidad de procesamiento.

Tabla 6.9: Resultados de NIST 800-22 basados en la implementación en microcontrolador.

No.	Prueba estadística		*P-value*	Resultados
1	FT		0.1768	Aprobado
2	FTB		0.8736	Aprobado
3	CST		0.5016	Aprobado
4	RT		0.2407	Aprobado
5	LROBT		0.4275	Aprobado
6	BMRT		0.8794	Aprobado
7	DFTT		0.8203	Aprobado
8	NTMT		0.9040	Aprobado
9	OTMT		0.8103	Aprobado
10	MUST		0.9967	Aprobado
11	AET		0.6105	Aprobado
12	RET		0.2562	Aprobado
13	LCT		0.3621	Aprobado
14	ST		0.1768	Aprobado
		-3	0.6030	
		-2	0.8239	
		-1	0.9614	
15	REVT	1	0.7371	Aprobado
		2	0.5880	
		3	0.9562	

Tabla 6.10: Tiempo obtenido para generar 1000 datos caóticos.

Implementación	Tiempo (Mbit/s)
MATLAB	237.38
Arduino Mega	20.76

El EHSHM presenta mejores resultados que el mapa original (HSHM) de acuerdo a los análisis anteriores, la mejora del mapa caótico es satisfactoria ya que se obtienen mejores dinámicas que benefician el desarrollo del PRNG propuesto. Los resultados obtenidos en el esquema propuesto se resumen en la Tabla 6.11.

Tabla 6.11: Resultados generales del mapa caótico propuesto EHSHM.

Característica	Descripción
Alto exponente de Lyapunov	Mayor sensibilidad a las condiciones iniciales y parámetros de control
Atractor hypercaótico	Comportamientos dinámicos más complejos (alta aleatoriedad)
Buen diagrama de bifurcación	Amplia gama de parámetros
Mejor histograma	Excelente uniformidad de datos caóticos
Clave secreta	60 caracteres hexadecimales

Las ventajas del PRNG son: un alto valor del exponente de Lyapunov, lo que lo hace aún más sensible a las condiciones iniciales y a los parámetros de control, dinámicas más complejas, más aleatoriedad, un gran espacio clave de 2^{230}, en [140] es 2^{212} y 2^{148} en [141], mejor distribución y generación rápida de datos caóticos, 20.76 Mbit/s en el microcontrolador Arduino Mega, en [142] es 14.48 Mbit/s. Además, el nivel de seguridad frente a diversos ataques y la sencillez de implementación. Las desventajas del esquema propuesto: el mapa hypercaótico con una función trigonométrica no se podría implementar en algunos microcontroladores y el proceso de retroalimentación reduce ligeramente la velocidad de procesamiento. Las comparaciones del PRNG-EHSHM con esquemas similares en la literatura se presentan en la Tabla 6.12.

Tabla 6.12: Comparaciones con esquemas similares en la literatura.

	PRNG-EHSHM	**Ref. 2022** [120]	**Ref. 2021** [121]	**Ref. 2021** [122]
Propiedades del caos				
Mapa caótico	Hénon-Seno mapa	Piece-wise linear mapa	Duffing and 2D-Logístico mapa	4D-Hypercaótico mapa
Exponente de Lyapunov	✓	✓	✓	✓
Trayectoria del atractor	✓	–	–	✓
Diagrama de bifurcación	✓	✓	✓	✓
Histograma	✓	–	–	–
Sensibilidad a la inicialización	✓	–	–	–
Análisis de seguridad				
Espacio de clave	✓	–	✓	✓
Sensibilidad de clave	✓	✓	✓	–
NPCR y/o UACI	✓	–	–	✓
Frecuencia flotante	✓	–	–	–
Histograma	✓	–	–	✓
Correlación	✓	✓	✓	✓
Autocorrelación	✓	✓	✓	–
Entropía de la información	✓	✓	✓	✓
Análisis estadístico				
NIST 800-22	✓	✓	✓	✓
Otro	–	–	–	–
Implementación				
MATLAB	✓	✓	✓	✓
Microcontrolador	✓	✓	–	✓

6.6. Conclusiones

En esta sección, se presentó un mapa hypercaótico bidimensional basado en el mapa 1D Hénon y el mapa 1D Seno, la aleatoriedad y la uniformidad se mejoraron con la función de resto después de la división, se obtuvo el mapa hypercaótico mejorado bidimensional Hénon-Seno (2D-EHSHM) que produce mejores propiedades pseudoaleatorias que el mapa original de acuerdo con el análisis del exponente de Lyapunov, la trayectoria del atractor, el diagrama de bifurcación, los histogramas y la sensibilidad en la inicialización. Además, se propuso un nuevo algoritmo generador de números pseudoaleatorios que produce números pseudoaleatorios de 8 bits generados con alta aleatoriedad según el análisis presentado, donde la semilla del PRNG se calcula indirectamente mediante una clave secreta de 60 caracteres hexadecimales para obtener las condiciones iniciales y parámetros de control. Fue implementado tanto en MATLAB como en el microcontrolador Arduino Mega. El PRNG-EHSHM fue validado con el conjunto más complejo de pruebas de aleatoriedad, el NIST 800-22, se realizaron diferentes análisis de seguridad desde el punto de vista criptográfico, donde los resultados obtenidos son satisfactorios para aplicarlo en criptografía, particularmente en seguridad embebida usando microcontroladores de bajo costo.

Capítulo 7

Algoritmo de encriptado caótico para huella dactilar propuesto

En este capítulo, se muestra el algoritmo de encriptado caótico propuesto para un sistema de acceso seguro biométrico, el cual se basa en una clave simétrica de 512 bits conformada por una clave personal de 256 bits y una clave HASH de 256 bits obtenida directamente de la plantilla clara de huella dactilar. La clave está representada por 128 caracteres hexadecimales para generar las secuencias caóticas del mapa hypercaótico Hénon-Seno para realizar los procesos de encriptado.

7.1. Introducción

En matemáticas, lógica y ciencias de la computación, un algoritmo es un conjunto de instrucciones o reglas definidas y no-ambiguas, ordenadas y finitas que permite solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo otras tareas o actividades. Dado un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución (Fig. 7.1).

Los algoritmos tienen tres partes básicas las cuales son:

1. Input (entrada): Información que se da al algoritmo con la que va a trabajar para ofrecer la solución esperada.

2. Proceso: Conjunto de pasos para que, a partir de los datos de entrada, llegue a la solución deseada.

3. Output (salida): Resultados, a partir de la transformación de los valores de entrada durante el proceso.

De este modo, un algoritmo informático parte de un estado inicial y de unos valores de entrada, sigue una serie de pasos sucesivos y llega a un estado final en el que ha obtenido una solución. Asimismo, los algoritmos presentan una serie de características comunes:

- Precisos: Objetivos, sin ambigüedad.
- Ordenados: Presentan una secuencia clara y precisa para poder llegar a la solución.
- Finitos: Contienen un número determinado de pasos.
- Concretos: Ofrecen una solución determinada para la situación o problema planteados.
- Definidos: El mismo algoritmo debe dar el mismo resultado al recibir la misma entrada.

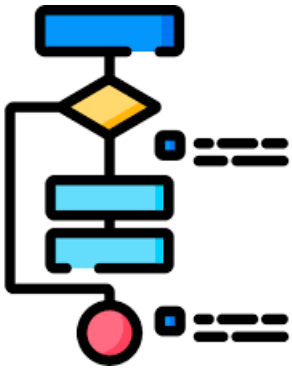


Figura 7.1: Estructura de un algoritmo.

En resumen, un algoritmo es cualquier cosa que funcione paso a paso, donde cada paso se pueda describir sin ambigüedad y sin hacer referencia a una computadora en particular y además tiene un límite fijo en cuanto a la cantidad de datos que se pueden leer/escribir en un solo paso [143].

7.2. Algoritmo de encriptado caótico

El algoritmo de encriptado propuesto utilizado en este trabajo, se basa en las siguientes características criptográficas [144]:

- *Encriptado simétrico.* El algoritmo utiliza la misma clave secreta de 512 bits para encriptar y desencriptar.
- *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.
- *Encriptado a flujo.* El algoritmo encripta cada elemento de la plantilla clara, uno a la vez hasta terminarlo.
- *Encriptado no convencional.* El algoritmo utiliza secuencias caóticas del mapa hypercaótico Hénon-Seno, que son determinadas por la clave secreta de 512 bits para generar secuencias pseudoaleatorias para realizar el proceso de confusión y difusión.

En la Fig. 7.2, se muestra el diagrama a bloques del proceso de encriptado propuesto. Se asume una plantilla clara $PC \in [0, 255]$ de longitud $\ell = 512$ basado en datos extraídos del módulo As608 que están representados por 8 bits en decimal. Primero se obtiene los datos de la plantilla clara (PC), se genera una clave HASH (CH) de 256 bits a partir de la plantilla clara, la cual se suma con otra clave secreta personal (CP) de 256 bits, obteniendo una clave secreta final (CSF) de 512 bits representada por 128 caracteres hexadecimales, esta clave se utiliza para generar las dinámicas caóticas mejoradas del mapa hypercaótico Hénon-Seno junto con la mediana (M) de la plantilla clara para realizar los procesos de confusión (C) y difusión (D), finalmente la mediana se agrega al final del criptograma para que el usuario autorizado pueda desencriptar correctamente.

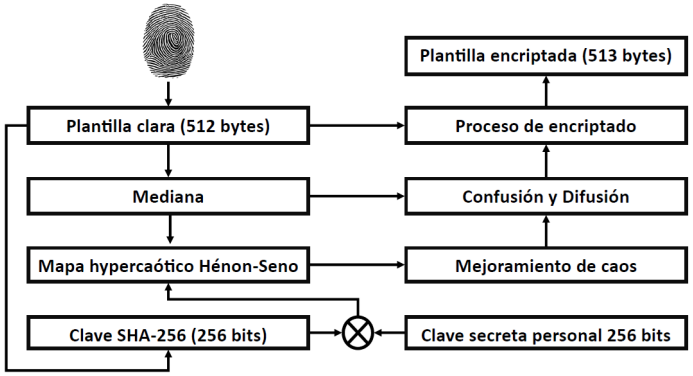


Figura 7.2: Diagrama a bloques del proceso de encriptado.

El proceso de desencriptado consta en invertir el proceso de encriptado. En la Fig. 7.3, se muestra el diagrama a bloques del proceso de desencriptado. Primero la mediana se extrae del criptograma, después se itera el mapa hypercaótico Hénon-Seno con la clave secreta de 512 bits y el valor de la mediana, finalmente, se realizan los procesos de confusión y difusión inversos para recuperar los datos de la plantilla clara.

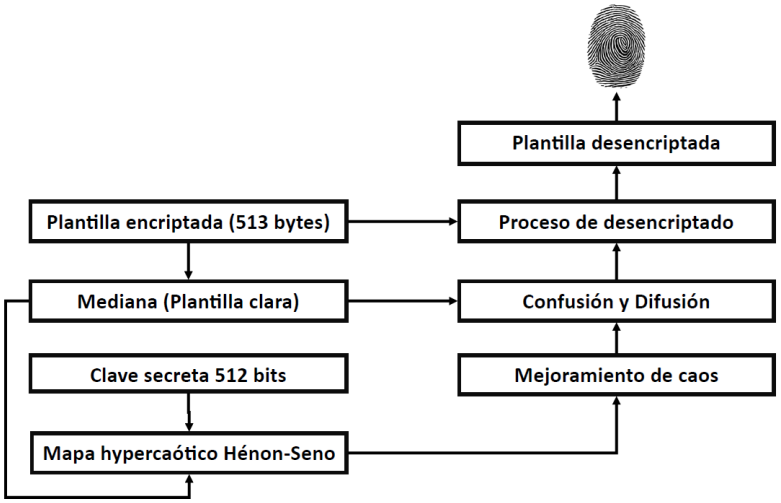


Figura 7.3: Diagrama a bloques del proceso de desencriptado.

7.2.1. Definición de la clave secreta

La clave secreta está definida como una secuencia de 512 bits, caracterizada por 128 caracteres hexadecimales $K \in (0-9, A-F)$; la cual es dividida en 10 secciones $(A, B, C, D, E, F, G, H, I, J)$. Las condiciones iniciales y el valor de los parámetros de control son calculados de manera indirecta mediante la clave secreta. En la tabla 7.1, se muestran los cálculos correspondientes.

Se utilizan 256 bits de la clave secreta personal (CP) la cual puede ser obtenida manualmente, para la clave HASH (CH) de 256 bits se utiliza la función SHA-2, el cual es una función que transforma un fichero cualquiera en un valor de longitud fija único, llamado hash, se obtiene una clave de 256 bits a partir de la plantilla clara.

Tabla 7.1: Definición de clave secreta.

Clave secreta			
128 Hex Caracteres	$H_1, H_2, \ldots, H_{128}$ donde $H \in [0-9, A-F]$		
Valores	$A = \frac{(H_1, H_2, \ldots, H_{13})_{10}}{2^{53}+1}$	$B = \frac{(H_{14}, H_{15}, \ldots, H_{26})_{10}}{2^{53}+1}$	$C = \frac{(H_{27}, H_{28}, \ldots, H_{39})_{10}}{2^{53}+1}$
	$D = \frac{(H_{40}, H_{41}, \ldots, H_{52})_{10}}{2^{53}+1}$	$E = \frac{(H_{53}, H_{54}, \ldots, H_{65})_{10}}{2^{53}+1}$	$F = \frac{(H_{66}, H_{67}, \ldots, H_{78})_{10}}{2^{53}+1}$
	$G = \frac{(H_{79}, H_{80}, \ldots, H_{91})_{10}}{2^{53}+1}$	$H = \frac{(H_{92}, H_{93}, \ldots, H_{104})_{10}}{2^{53}+1}$	$I = \frac{(H_{105}, H_{106}, \ldots, H_{117})_{10}}{2^{53}+1}$
	$J = \frac{(H_{118}, H_{119}, \ldots, H_{128})_{10}}{2^{53}+1}$		
Parámetros de control	$\alpha = rem(A + B + M, 1)$	$\beta = rem(C + D + M, 1)$	$\gamma = rem(E + F, 1)$
Condiciones iniciales	$x = rem(G + H + M, 1)$	$y = rem(I + J + M, 1)$	

7.2.2. Mediana

El valor de la mediana M incrementa la sensibilidad a pequeños cambios en la plantilla clara y a la clave secreta a nivel de bit. Al utilizar el valor de M hace que el proceso de encriptado sea robusto ante ataques diferenciales como texto claro conocido y ataque de texto claro elegido.

$$M = median(PC)/256, \tag{7.1}$$

7.2.3. Proceso de encriptado

El mapa hypercaótico Hénon-Seno se itera I veces con valores α, β, γ, x_0 y y_0 tomados de la tabla 7.1, para generar las secuencias caótica de datos $x = x_1, x_2, x_3, \ldots, x_I$ y $y = y_1, y_2, y_3, \ldots, y_I$ con x y $y \in (0, 1)$ y una precisión decimal de 10^{-15}.

Posteriormente, la secuencias x y y son mejoradas con la siguiente expresión:

$$x_i = (rem(x_i * 101), 1), \quad para\ i = 1, 2, 3, \ldots, I, \tag{7.2a}$$

$$y_i = (rem(y_i * 101), 1), \quad para\ i = 1, 2, 3, \ldots, I, \tag{7.2b}$$

De la secuencia caótica x se determinan una subsecuencia para el proceso de confusión. Para el proceso de confusión la subsecuencia se calcula con la siguiente expresión:

$$C_i = \ round\left[x_{I-\ell+i} * (\ell - 1)\right] + 1, \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{7.3}$$

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

$$G_h = [K_h], \quad con\ h \ll \ell, \tag{7.4}$$

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

Una subsecuencia para difusión se determina de y de la misma longitud ℓ. La subsecuencia para difusión se calcula como:

$$D_i = rem((y_{I+1-\ell+i} * 1000) + M, 1), \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{7.5}$$

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

El proceso de encriptado se calcula con la siguiente expresión:

$$E_i = mod(PC(C_i) + D_i, 256), \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{7.6}$$

donde PC es la plantilla clara y E es el criptograma.

7.2.4. Proceso de desencriptado

El proceso de desencriptado consiste en invertir todos y cada uno de los pasos desarrollados en el encriptado. Se debe utilizar exactamente la misma clave de 512 bits, ya que, si un bit cambia, no se podrá recuperar la plantilla clara correctamente.

Primero, el valor de M debe ser recuperado, después, el mapa hypercaótico Hénon-Seno es iterado con la clave secreta y el valor de M. Posteriormente, se calculan las subsecuencias C y D para confusión y difusión, respectivamente. Finalmente, el desencriptado se realiza con la siguiente expresión:

$$PC(C_i) = mod(E_i - D_i, 256) \quad para\ i = 1, 2, 3, \ldots, \ell, \tag{7.7}$$

donde E es el criptograma y PC es la plantilla clara.

7.2.5. Características de seguridad y eficiencia

El algoritmo de encriptado 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 hypercaótico Hénon-Seno, se determinan de manera indirecta a partir de una clave de 512 bits.

2. **Mejoramiento de secuencias caóticas**. Los datos caóticos del mapa hypercaótico Hénon-Seno 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. **Mediana**. Al considerar las características de la plantilla clara para realizar el proceso de encriptado, se incrementa por mucho la sensibilidad a pequeños cambios en la plantilla clara. Por tanto, este proceso ayuda a dar robustez al algoritmo criptográfico ante los distintos ataques.

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

5. **Eficiencia de encriptado**. El 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 plantilla clara en un mismo proceso.

7.3. Conclusiones

En este capítulo, se presentó el algoritmo de encriptado propuesto y las características de seguridad y eficiencia que el algoritmo posee. Un algoritmo criptográfico basado en caos debe cumplir con varios aspectos de seguridad para poder ser implementado en aplicaciones prácticas como en sistemas embebidos en donde se requiere resguardar información de forma segura. El algoritmo propuesto se basa en encriptado simétrico ya que utiliza la misma clave de 512 bits para encriptar y desencriptar, realiza procesos de confusión y difusión en una sola operación, encripta la secuencia de datos en flujo y utiliza secuencias caóticas del mapa hypercaótico Hénon-Seno.

Capítulo 8

Sistema de acceso seguro biométrico con sistema experto propuesto

En este capítulo, se describe la implementación del sistema de acceso seguro en un sistema embebido de bajo costo basado en un microcontrolador de 32 bits. Se implementa el algoritmo de encriptado caótico para incrementar la seguridad del sistema embebido para evitar suplantación biométrica y robo de identidad. Además, se dan algunos detalles teóricos sobre los sistemas de autentificación actuales y sistemas expertos mediante un análisis de la literatura.

Se explica el proceso de identificación del usuario mediante el sistema experto propuesto con la señal de electrocardiograma y la autentificación de usuario mediante la huella dactilar donde primero se hace el registro del usuario y se encripta la plantilla clara para después ser desencriptada en el proceso de comparación de plantillas para brindar acceso al sitio restringido.

Se realiza un análisis de seguridad de la plantilla clara y criptograma obtenidos en el software MATLAB como espacio de clave, sensibilidad a la clave, sensibilidad a plantilla clara, histogramas, frecuencia flotante, correlación, autocorrelación, entropía de la información y se muestran los recursos utilizados y el desempeño, finalmente, una comparación con la literatura y las conclusiones.

8.1. Introducción

Con la nueva era de la tecnología, todo se convierte en dispositivos inteligentes que desafían la transferencia o almacenamiento de datos de forma segura [145]. Además, la rápida revolución de las tecnologías ha creado muchos problemas de seguridad. Actualmente, los sistemas biométricos son un tema de alto interés en la comunidad científica, debido a que proporcionan una forma práctica en el diseño sistemas de control de acceso seguros [146].

Los sistemas biométricos tienen una amplia variedad de aplicaciones en servicios forenses, comerciales y gubernamentales. Estos sistemas utilizan rasgos biométricos como la huella dactilar, el iris, la oreja, ECG, cara, venas de los dedos y geometría de manos para identificar a los individuos. Los sistemas biométricos unimodales suelen carecer de precisión suficiente y son vulnerables a ataques de suplantación de identidad [147]. En comparación, los métodos multibiométricos, que utilizan múltiples rasgos biométricos, pueden lograr un rendimiento final dramáticamente mayor [148, 149].

El reconocimiento de características biométricas es la tecnología que utiliza diferentes características biométricas o comportamientos personales de un individuo para identificar a una persona. En comparación con otras funciones biométricas, la tecnología de reconocimiento de huellas dactilares tiene muchas ventajas: Es común, estable, preciso y no se puede falsificar fácilmente. La probabilidad de encontrar dos huellas dactilares iguales es sólo de una entre cinco mil millones. Por lo tanto, se convierte en la tecnología más aplicada en el campo del reconocimiento de características biométricas [150]. Un sistema de acceso seguro basado en huella dactilar, además del uso de un sistema experto el cual es un sistema informático que procesa conocimientos e indica decisiones a tomar en la resolución de determinados problemas, razonando sus propios procesos hacen más seguro el sistema al aplicar otro rasgo biométrico como la señal de ECG. En las siguientes subsecciones se explica más a detalle la implementación.

8.1.1. Revisión de la literatura

En [151], los autores implementan un marco de encriptado caótico para mejorar la seguridad de las imágenes biométricas durante la transmisión. El marco propuesto se basa en la transformada de paquetes wavelet fraccional (FrWPT), el mapa caótico Piece-wise y la descomposición de Hessenberg. La eficiencia y robustez de la técnica se validan mediante diferentes tipos de simulaciones y análisis de imágenes de huellas dactilares. En [152], desarrollan un criptosistema biométrico no lineal de dimensiones superiores basado en el caos para mejorar la seguridad de las plantillas biométricas almacenadas en la base de datos. El esquema utilizado realiza procesos de confusión y difusión. En la confusión, los elementos de las plantillas se permutan utilizando los valores clave de la serie caótica ordenada y, en la difusión, los elementos confusos se sustituyen utilizando dinámicas caóticas. Los análisis de seguridad mostrados indica que el esquema tiene buenas propiedades de encriptado.

En [153], se desarrolla un algoritmo el cual se basa en una combinación de procesos de permutación y confusión. El mapa caótico se utiliza para permutar las direcciones de los píxeles de la imagen de la huella digital, mientras que la confusión a nivel de bits se utiliza para confundir los valores de los píxeles de la imagen a fin de mejorar la seguridad. Los resultados experimentales se llevan a cabo con un análisis detallado para demostrar que el esquema de encriptado posee un gran espacio de claves para resistir ataques de fuerza bruta y posee buenas propiedades estadísticas.

En [154], se diseña un esquema de encriptado basado en el caos eficiente y seguro que tiene un comportamiento complejo que es difícil de predecir y analizar. Se utiliza el mapa Arnold cat para mezclar los píxeles de los datos biométricos. Este método utiliza el sistema caótico Chen 3-D para cambiar las propiedades estadísticas de los datos biométricos a fin de resistir ataques estadísticos. En [155], se diseña y analiza el encriptado de imágenes biométricas donde las características biométricas de la señal de electrocardiografía (ECG) y el comportamiento caótico del mapa de Duffing se combinan para proporcionar un encriptado personalizado único. En este método, el mapa de Duffing se utiliza como una función caótica que tiene una propiedad dinámica muy distintiva y puede ser muy sensible a sus valores iniciales. En [156], se diseña un novedoso sistema de autenticación basado en biometría que utiliza dos servidores: un servidor de coincidencia criptográfica y un servidor de almacenamiento que no es de confianza. El sistema utiliza criptosistema de imágenes biométricas, hash criptográfico y criptosistema Paillier. En el criptosistema, los flujos de claves se generan a partir de mapas Logísticos y de Hénon. Los parámetros de control de estos mapas caóticos se calculan a partir de la imagen biométrica de entrada. El encriptado biométrico propuesto es capaz de resistir ataques estadísticos y diferenciales y su nivel de seguridad también está validado mediante diversos análisis. En [157], se emplea una protección de plantilla biométrica multimodal utilizando proyección aleatoria local y encriptado, las plantillas se encriptan mediante un encriptado totalmente homomórfico, para minimizar el coste computacional, se utiliza un esquema por lotes, que realiza varias multiplicaciones de forma encriptada mediante una única operación.

8.2. Resultados experimentales

Se describe los procesos del sistema experto para identificar al usuario mediante la señal biomédica de electrocardiograma y la autenticación mediante el rasgo biométrico de huella dactilar.

8.2.1. Sistema experto

En los últimos años se ha desarrollado una gran cantidad de sistemas expertos para diversos sectores [158]. Un esquema de autenticación biométrica basado en sistema experto permite a un usuario identificarse para verificar que es propietario de información biométrica y permitir el control del acceso [159]. Los sistemas expertos se destacan entre las herramientas de soporte para la toma de decisiones. Han sido diseñados para facilitar tareas en múltiples campos de aplicación y proporcionar equivalentes resultados que un especialista, emulando la capacidad humana de tomar decisiones de acuerdo a las condiciones del contexto.

Se usa el motor de inferencia el cual es el cerebro del SE, también conocido como estructura de control o interpretador de reglas. Este componente es esencialmente un programa de computadora que provee metodologías para razonamiento de información y está basado en reglas previamente establecidas.

Los sistemas basados en reglas trabajan mediante la aplicación de reglas y comparación de resultados. Por lo tanto, el sistema experto propuesto consiste en la detección del pico R de una señal de electrocardiograma.

La electrocardiografía es el proceso de monitorización de signos vitales más común y ampliamente utilizado en los sistemas sanitarios modernos. Las grabaciones de electrocardiograma (ECG) capturan el potencial eléctrico en la superficie del cuerpo. Recientemente, las señales de electrocardiograma (ECG) han recibido un alto nivel de atención como señal fisiológica en el campo de la biometría [160]. El ECG es la representación eléctrica de la actividad cardíaca. Cada latido del corazón es desencadenado por un impulso eléctrico generado por un nódulo sinusal especial en la aurícula. Una señal de ECG se compone de un grupo de componentes temporales y de amplitud. Un ECG típico de un objeto sano consta de tres componentes principales: los componentes P, el complejo QRS y los componentes T. Cada uno de estos componentes tiene su propia característica, comportamiento y origen [161, 162].

Por lo tanto, el sistema experto propuesto se basa en una serie de reglas establecidas en la cual identifica al usuario mediante la detección del pico R de la señal de electrocardiograma. El diagrama a bloques del proceso se muestra en la Fig. 8.1.

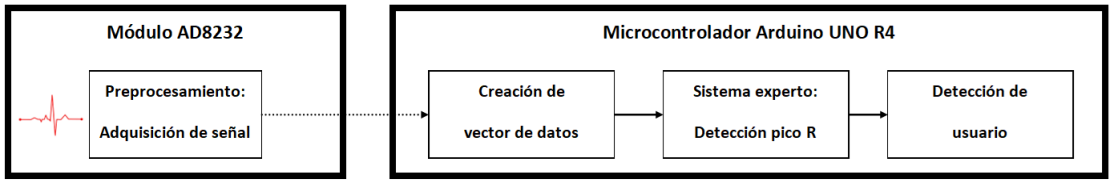


Figura 8.1: Diagrama a bloques del sistema experto.

8.2.2. Autenticación

Los sistemas de autenticación basados en sistemas biométricos y de microcontroladores se utilizan en todo el mundo para controlar el acceso de los usuarios en sitios restringidos como oficinas, bancos u hospitales. Los sistemas biométricos se basan en los siguientes pasos: primero, se toma una muestra biométrica de un individuo, como la huella dactilar; luego, de esa muestra se extraen algunos datos que constituyen una plantilla biométrica; finalmente, la plantilla, se almacena en una base de datos (local o remota). Todos estos pasos, constituyen el proceso conocido como registro (Fig. 8.2).

Una vez que una persona realiza el proceso de registro, puede autenticarse (una muestra biométrica presentada por una persona se compara con una muestra almacenada) presentando su muestra biométrica en el sistema, que comparará la muestra enviada con la muestra almacenada y si el proceso de comparación tiene éxito, la persona será reconocida y el sistema la aceptará (Fig. 8.3) [163].

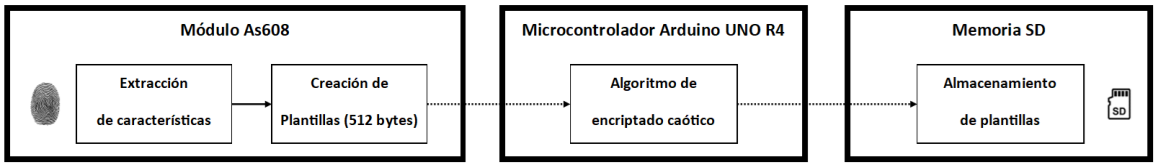


Figura 8.2: Diagrama a bloques del proceso de registro de usuario.

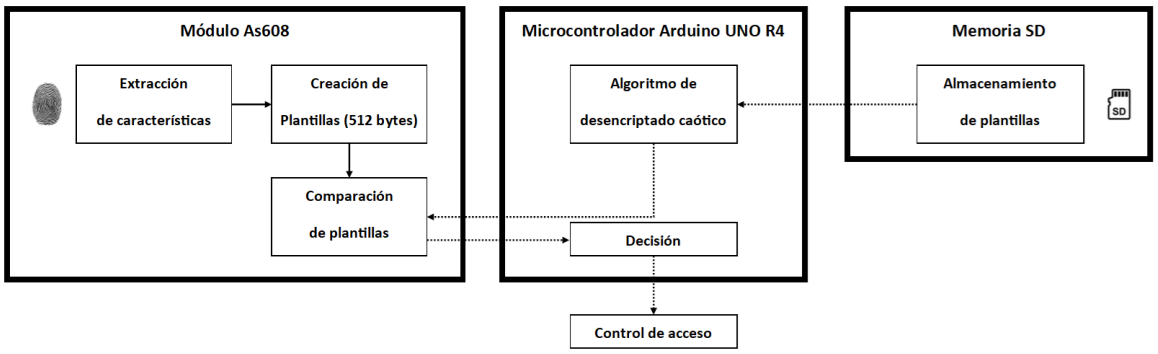


Figura 8.3: Diagrama a bloques del proceso de autenticación.

Estos sistemas tienen algunos puntos vulnerables, como ataque a los módulos (sensor, extracción de características, coincidencia, base de datos, etc.). Los ataques utilizan programas maliciosos que emula la función de algunos módulos del sistema biométrico y podría rechazar a un usuario autorizado o robar las características de la información biométrica. Es importante considerar los aspectos de seguridad de cualquier sistema de autenticación biométrica propuesto, ya que las amenazas dirigidas a los datos de las plantillas biométricas son graves. Dado que los datos biométricos originales no son revocables, si se ven comprometidos, se pierden para siempre [164].

Es por eso que se aplica un algoritmo de encriptado para proteger la plantilla biométrica. Los criptosistemas biométricos ofrecen soluciones para la protección de plantillas, las plantillas biométricas originales son reemplazadas por una plantilla encriptada la cual es la que se almacena. Por lo tanto, el encriptado biométrico es eficaz, seguro y privado. El esquema de autentificación propuesto se muestra en la Fig. 8.4.

Hay dos métricas para medir la precisión de un sistema biométrico, la tasa de falso rechazo (FRR) y la tasa de falsa aceptación (FAR). FRR es el número de rechazos (incorrectos) que realiza el sistema biométrico, es decir, cuando el sistema rechaza a un usuario legítimo. FAR es cuántas aceptaciones (incorrectamente) realiza el sistema biométrico, es decir, cuando el sistema relaciona incorrectamente una muestra biométrica con una muestra de referencia almacenada incorrectamente, lo que resulta en una identificación errónea. El enfoque de transformación de características se basa en una función de transformación (algoritmo), que se aplica a la plantilla biométrica y el resultado se almacena en la base de datos. La plantilla transformada se caracteriza por una clave secreta o una contraseña.

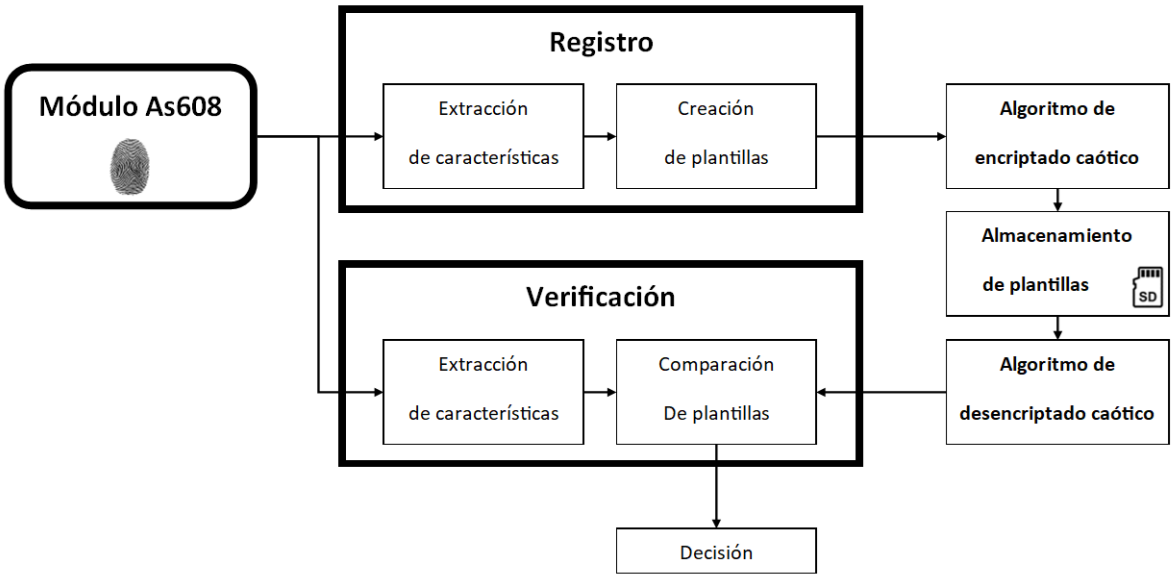


Figura 8.4: Diagrama a bloques del proceso de autenticación propuesto.

8.3. Implementación en sistema embebido

El algoritmo de encriptado se implementa en Arduino UNO R4 WiFi que cuenta con un microcontrolador de 32 bits y un módulo ESP32-S3 Wi-Fi. Cuenta con un microcontrolador de la serie RA4M1 de Renesas (R7FA4M1AB3CFMAA0), basado en un microprocesador Arm Cortex-M4 de 48 MHz. La memoria del UNO R4 cuenta con 256 kB flash, 32 kB SRAM y 8 kB de EEPROM [165]. Para la programación, se utiliza el software Arduino IDE con la versión 1.8.13, el programa es almacenado en la memoria flash del microcontrolador. Para realizar el análisis de seguridad, se utiliza el software MATLAB con la versión R2015a en una computadora personal con un procesador AMD Ryzen 2.10 Ghz, 8 Gb de memoria RAM y sistema operativo windows 10 de 64 bits; se utiliza representación punto flotante con precisión doble y una precisión de 10^{-15}. La clave secreta es de 128 caracteres hexadecimales, la señal de ECG se obtiene mediante el módulo AD8232 [166] y la huella dactilar del módulo As608 [167], la cual se someterá al proceso de encriptado para obtener el criptograma y posteriormente realizar el análisis de seguridad.

Para realizar los procesos de encriptado y desencriptado, se utiliza el microcontrolador RA4M1 de Renesas donde por medio de programación en el software Arduino IDE se realizan los procesos. Para visualizar información e indicaciones del programa se utiliza una pantalla LCD 20 x 4, matrix orbital modelo LK204-25, donde se muestran distintos mensajes. Para el mando de control se utilizan los puertos GPIO del microcontrolador para activar los 3 LED's, una alarma y dos botones de presionar que interactúan con el programa y los datos obtenidos son almacenados en una memoria micro SD.

En la Fig. 8.5, se muestra el diagrama a bloques del funcionamiento del sistema embebido propuesto para la parte experimental de este trabajo, donde se indica la forma en que se conectan y comunican los módulos.

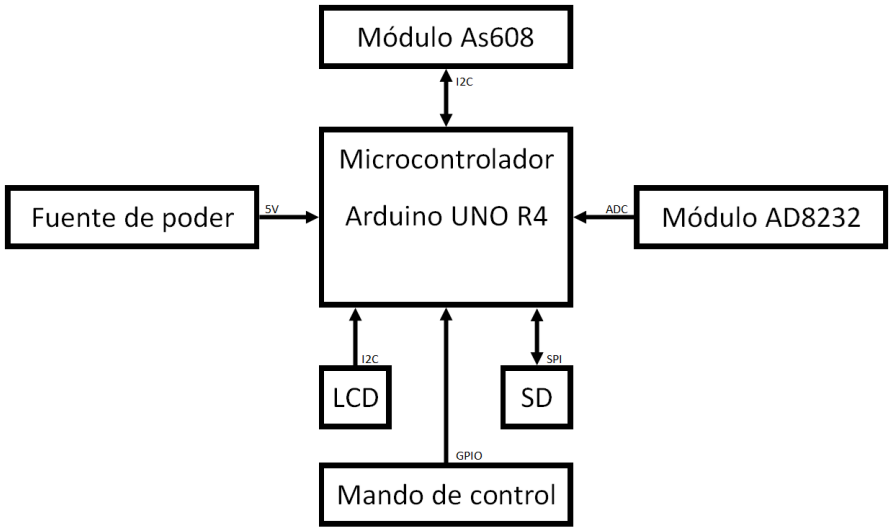


Figura 8.5: Diagrama a bloques del sistema embebido.

El sistema embebido está conformado por 7 módulos independientes, cada uno con funciones específicas y controlados directo o indirectamente por el microcontrolador (Fig. 8.6).

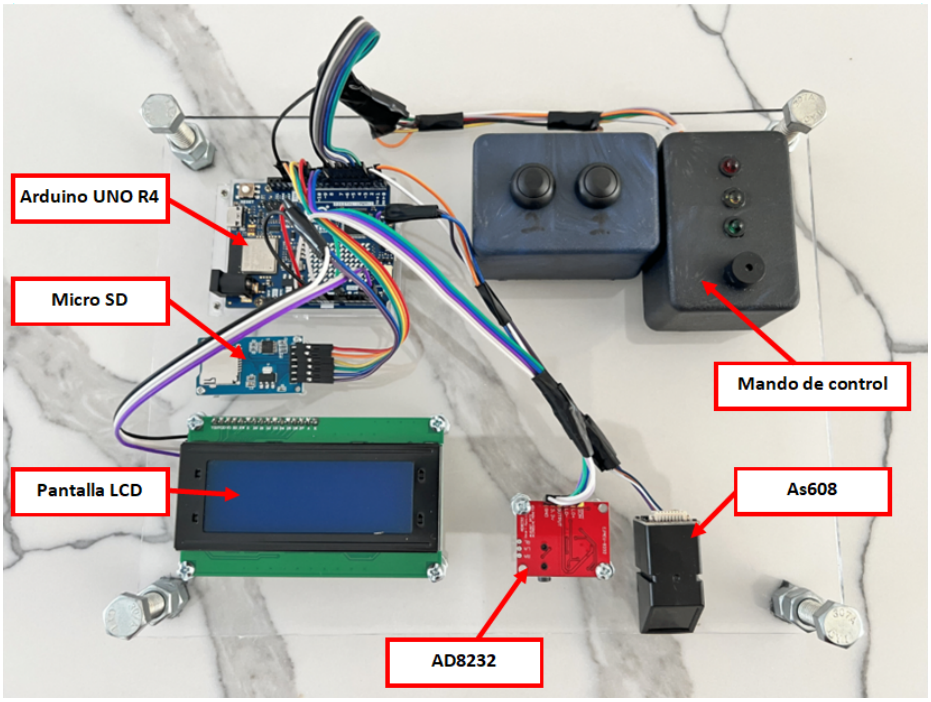
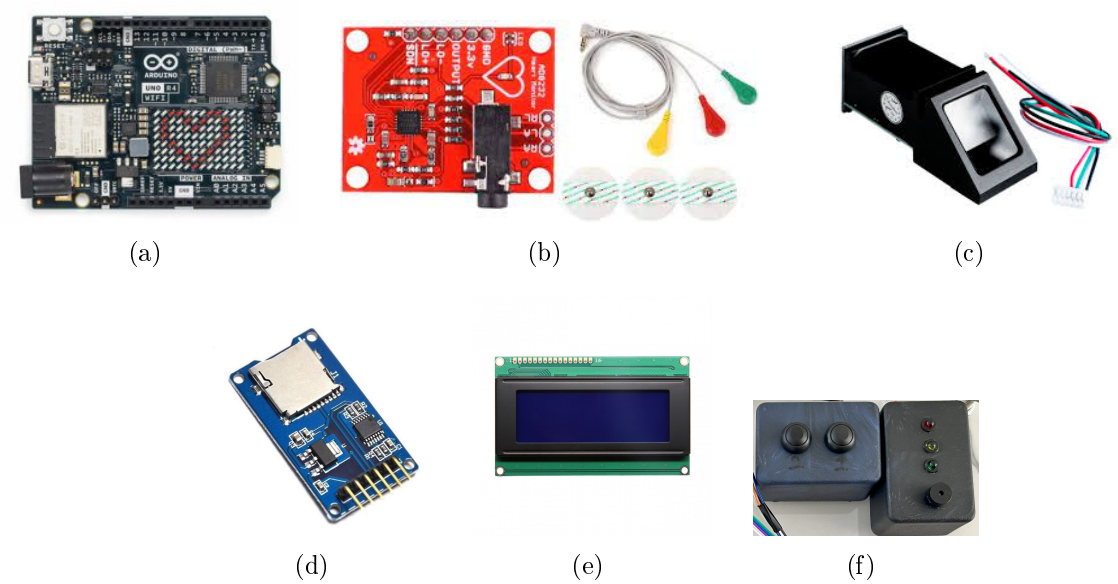


Figura 8.6: Sistema embebido desarrollado para pruebas experimentales.

- **Microcontrolador**. El programa del sistema se ejecuta en este módulo, al iniciar, se establece la comunicación I2C con la LCD y el módulo As608, 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 (Fig. 8.7(a)).
- **Módulo AD8232**. Se encarga de adquirir la señal de electrocardiograma en un vector de 1000 datos durante 10 segundos, con una frecuencia de muestreo de 100 Hz (Fig. 8.7(b)).
- **Módulo As608**. Adquiere las plantillas dactilares de 512 bytes y realiza el proceso de comparación (Fig. 8.7(c)).
- **Fuente de alimentación**. Se encarga de proporcionar voltaje al sistema para su correcto funcionamiento.
- **Memoria micro SD**. Es donde se almacena la plantilla dactilar encriptada (Fig. 8.7(d)).
- **Pantalla LCD 20x4**. 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 (Fig.8.7 (e)).
- **Mando de control**. En este módulo se tienen dos botones de presionar, también tiene 3 LED's como indicadores. Además, cuenta con una alarma para interacción con el usuario (Fig. 8.7(f)).



(a) (b) (c)

(d) (e) (f)

Figura 8.7: Componentes del sistema embebido: a) Arduino UNO R4, b) Módulo AD8232 para adquisición de electrocardiograma, c) Módulo As608 para adquisición de plantillas dactilares, d) Memoria micro SD, e) Pantalla LCD y f) Mando de control.

El diagrama a bloques del proceso general se muestra en la Fig. 8.8. En el cual primero que todo el usuario ya está registrado en el sistema y su plantilla biométrica esta encriptada.

El primer paso es realizar la adquisición de la señal de electrocardiograma con el módulo AD8232, se extraen las características de la señal ECG en un vector de 1000 datos adquiridos durante 10 segundos a 100 Hz (Fig. 8.9) y se someten al sistema experto que mediante la detección del pico R de la señal identifica al usuario.

Ya que se identificó al usuario se procede a leer la huella dactilar con el módulo As608 (si no se identifica correctamente al usuario en el proceso del sistema experto, el sistema no va detectar la huella dactilar), se realiza una comparación de las plantillas, la nueva que se introduce y la que estaba previamente almacenada encriptada, para esto se debe desencriptar la plantilla para poder realizar la comparación, si las plantillas coinciden el sistema toma una decisión permitiendo el acceso al sitio restringido.

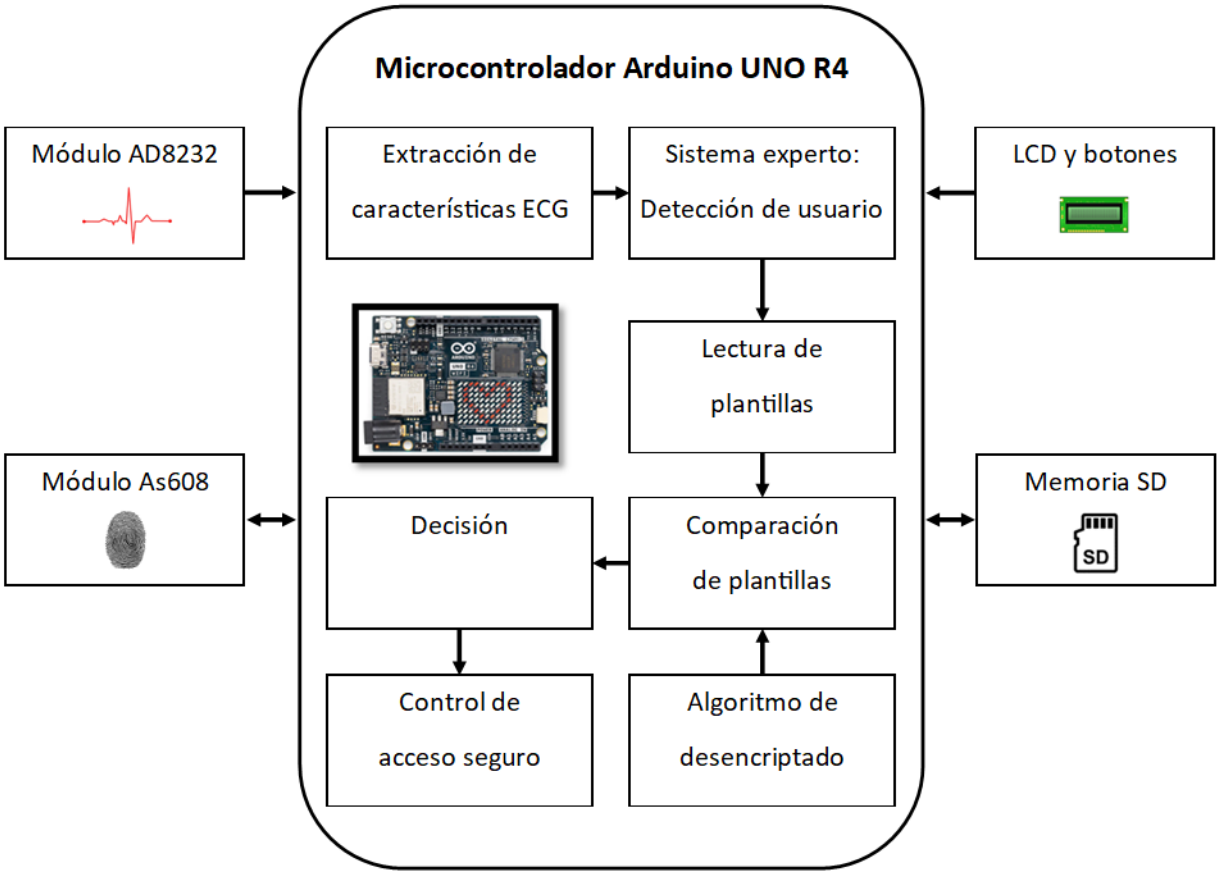


Figura 8.8: Diagrama a bloques del proceso general del sistema de acceso seguro propuesto.

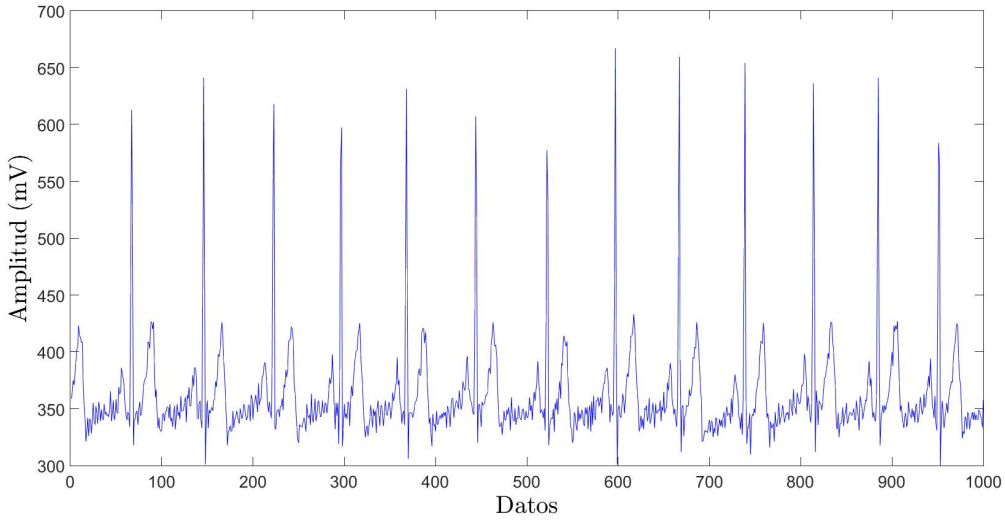


Figura 8.9: Señal ECG adquirida de usuario 1.

A continuación, se muestra los mensajes mediante la pantalla LCD del funcionamiento del sistema embebido.

Registro del usuario:
Al encender el sistema, la LCD se muestra algunos mensajes con indicaciones a seguir para registrar al usuario, al iniciar pide que se coloque la huella dactilar en el módulo As608, después, aparece otro mensaje que indica que se debe retirar y volver a colocar la huella, esto para obtener de mejor manera los datos de la plantilla dactilar, finalmente, un mensaje que indica que el usuario fue registrado y la huella dactilar almacenada y encriptada (Fig. 8.10). En la Tabla 8.1, se muestran los primeros 65 bytes de 512 bytes de la huella dactilar clara y de la huella dactilar encriptada.

Tabla 8.1: Plantilla clara y encriptada utilizada para resultados experimentales.

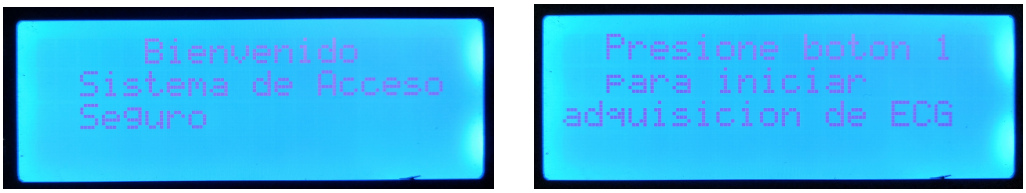
Huella dactilar	Plantilla clara (Primeros 65 bytes)
Usuario 1	0365322C01EF01880000000000000000000000000000 00000000000000000000000000000000000000000000000000 F000000B5000101010101011BD5EF01FFFFFFFF0200
Huella dactilar	Plantilla encriptada (Primeros 65 bytes)
Usuario 1	3B21DA9A0A45DB0EC85C45F9AD7040AD4376F1E91CCB2 A65A568AF67273F2F582320DB9E036BDCB9F5D0E5A2A6A 3CD047B253F3533771AF28D76F4BACA2FD5F664D7AA18

Inicio de sistema:
Al iniciar el sistema se muestra un mensaje de bienvenida indicando que es un sistema de acceso seguro, luego, un mensaje que indica que se debe presionar el botón 1 para iniciar con la adquisición de la señal de ECG, la cual tarda 5 segundos en calibrar y adquiere una señal de 10 segundos (Fig. 8.11).

(a) (b)

(c)

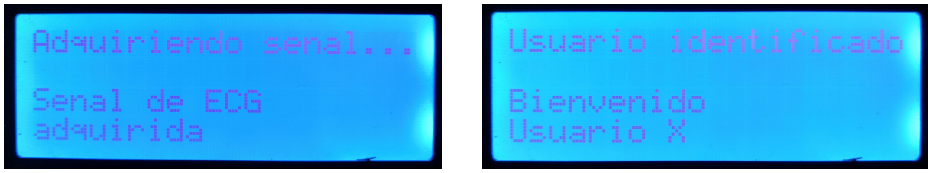
Figura 8.10: Mensajes de registro de usuario: a) Mensaje para colocar huella dactilar, b) Mensaje para retirar y volver a colocar huella dactilar y c) Mensaje de usuario registrado y plantilla almacenada.



(a) (b)

Figura 8.11: Mensajes de inicio de sistema: a) Mensaje de bienvenida y b) Mensaje para presionar botón 1.

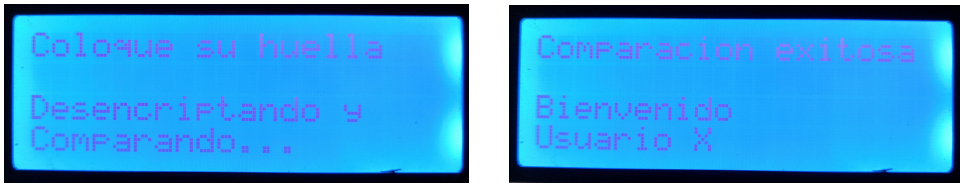
Adquisición de señal ECG: Sistema experto:
Después de presionar el botón 1, se despliega un mensaje que indica que se está tomando la señal de ECG, ya que se adquiere la señal, se muestra un mensaje indicando que la señal se adquirió y mediante el sistema experto detecta al usuario con el cual se muestra un mensaje dándole la bienvenida (Fig. 8.12).



(a) (b)

Figura 8.12: Mensajes de adquisición de señal ECG: a) Mensaje de adquiriendo señal y b) Mensaje de usuario identificado.

Huella dactilar: Colocación de huella y comparación.
En el proceso de la colocación de huella y comparación, ya que se identificó al usuario, el sistema pide que coloque su huella dactilar en el módulo As608, después aparece un mensaje el cual indica que se está comparando la plantilla colocada vs la plantilla previamente almacenada la cual esta encriptada, se realiza el proceso de desencriptado y comparación, si fue exitoso aparece un mensaje que indica comparación exitosa y le da la bienvenida al usuario de nuevo (Fig. 8.13).



(a) (b)

Figura 8.13: Mensajes de proceso de huella dactilar: a) Mensaje de colocar huella y comparación y b) Mensaje de comparación exitosa.

Decisión del sistema:
Ya que se comparó la plantilla y le dio de nuevo la bienvenida al usuario, el sistema le da acceso al usuario al sitio restringido (Fig. 8.14).

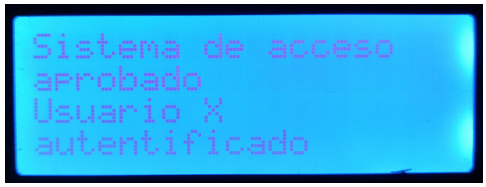


Figura 8.14: Mensaje de usuario aprobado.

8.4. Análisis de seguridad

Para los análisis de seguridad [168], se extrae del microcontrolador la plantilla clara y su respectiva plantilla encriptada para realizar los distintos análisis de seguridad en MATLAB. En las siguientes subsecciones, se presentan los diferentes análisis de seguridad a los que se somete el criptograma con el algoritmo propuesto implementado en microcontrolador.

8.4.1. Espacio de clave

Todo sistema criptográfico es susceptible a un ataque exhaustivo, donde cada posible clave secreta se utiliza para desencriptar 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. Para proporcionar seguridad suficiente contra un ataque exhaustivo, el espacio de claves debe ser mayor a 2^{100} [169]. Además, cada clave secreta se debe considerar fuerte, es decir, que genere secuencias caóticas. La clave secreta propuesta consiste de 128 caracteres hexadecimales (512 bits), por tanto, el algoritmo propuesto en esta tesis utiliza un espacio de clave de 2^{512} y puede resistir un ataque exhaustivo.

8.4.2. Sensibilidad a la clave

Una de las características fundamentales del caos es que una pequeña variación en las condiciones iniciales representa un gran cambio en la trayectoria de los mapas caóticos, esto es aprovechado en el algoritmo de encriptado utilizando la clave secreta en el mapa caótico, el encriptado responde drásticamente a pequeños cambios en la clave secreta [170]. Si la misma plantilla clara es encriptada tres veces con tres claves secretas similares, la plantilla encriptada debe ser muy diferente entre sí, mientras que, en el proceso de desencriptado, únicamente la clave secreta correcta puede recuperar la plantilla original.

Para este análisis, propusimos una plantilla clara de 50 elementos fijos en 150. La Fig. 8.15 muestra la sensibilidad de la clave secreta en el proceso de encriptado utilizando las claves secretas de la Tabla 8.2. Cada plantilla encriptada tiene su propia ruta, por lo que el algoritmo de encriptado es muy sensible a la clave secreta. La Fig. 8.16 muestra la sensibilidad de la clave secreta en el proceso de desencriptado, donde solo la clave secreta correcta recupera la plantilla original. Por lo tanto, el algoritmo de encriptado es muy sensible a la clave secreta de 512 bits.

8.4.3. Sensibilidad a plantilla clara

El algoritmo debe mostrar sensibilidad a pequeños cambios en la plantilla clara, es decir, pequeños cambios en la plantilla clara generan un gran cambio en la plantilla encriptada; si el algoritmo tiene esta propiedad, el encriptado puede resistir un ataque diferencial. Para realizar este análisis se utilizan las pruebas $NPCR$ y $UACI$ para demostrar la sensibilidad [171].

Tabla 8.2: Claves secretas utilizadas para el análisis de sensibilidad a la clave secreta.

Número de clave	Clave secreta
Clave 1	335533445566778899 77AABBCCDDEEFF
	1122334455667788122334455667788985223D9177FC58
	8D22DF9CB2EE0B358A7F097D27D88E7D9B78784B48791011FB
Clave 2	**4**3553344556677889977AABBCCDDEEFF
	1122334455667788122334455667788985223D9177FC58
	8D22DF9CB2EE0B358A7F097D27D88E7D9B78784B48791011FB
Clave 3	**5**3553344556677889977AABBCCDDEEFF
	1122334455667788122334455667788985223D9177FC58
	8D22DF9CB2EE0B358A7F097D27D88E7D9B78784B48791011FB

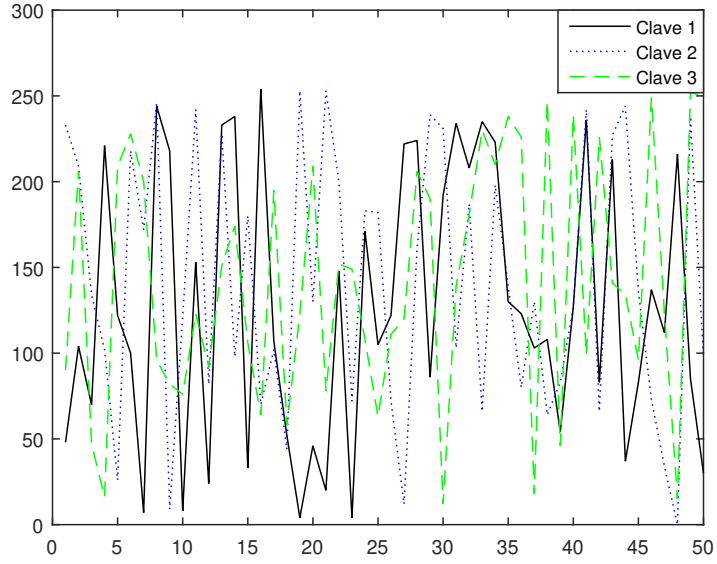


Figura 8.15: Sensibilidad a la clave en el proceso de encriptado.

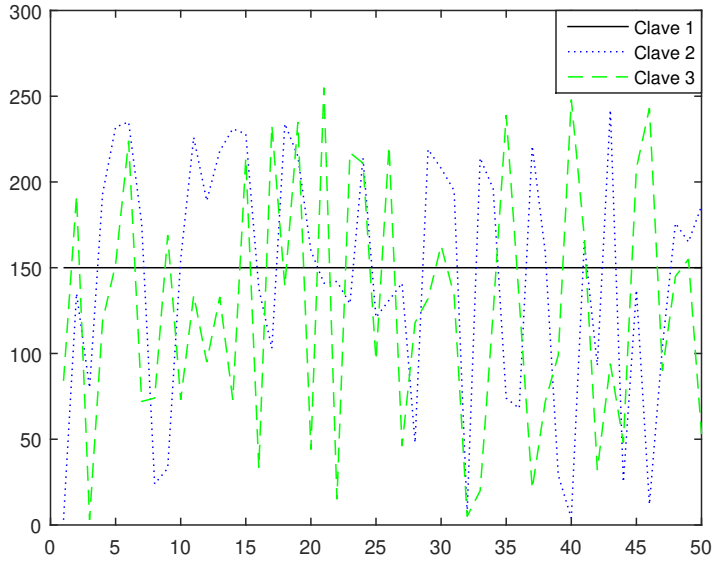


Figura 8.16: Sensibilidad a la clave en el proceso de desencriptado.

NPCR (del inglés, *Net Pixel Change Rate*), tasa de cambio de pixel neto, mide cuántos elementos son diferentes entre E1 y E2 en porcentaje, donde 100 % significa que son totalmente diferentes; se calcula con la siguiente expresión

$$NPCR = \frac{100}{\ell} \sum_{i=1}^{\ell} W_i \times 100 \tag{8.1}$$

con

$$W_i = \begin{cases} 0 & \text{if } E1_i = E2_i \\ 1 & \text{if } E1_i \neq E2_i \end{cases} \tag{8.2}$$

UACI (del inglés, *Unified Avarage Changing Intensity*), promedio unificado de cambio de intensidad, mide cuántas magnitudes en promedio son diferentes entre E1 y E2, donde 100 % significa que ambos son totalmente diferentes en magnitud; está determinado por la siguiente expresión

$$UACI = \frac{100}{\ell} \sum_{i=1}^{\ell} |E1_i - E2_i| \tag{8.3}$$

donde ℓ es la longitud de los datos, E_1 and E_2 son los dos criptogramas. El proceso para determinar los valores es como sigue: Primero, la plantilla clara se encripta con la Clave 1 de la Tabla 8.2 para generar E_1; después, el primer carácter hexadecimal de la plantilla clara se cambia de 03 a 04, lo que produce una clave hash diferente y E_2. Los resultados nos dan un 99.41 % en *NPCR* y un 83.70 % en *UACI*, lo que indica que ambos criptogramas son 99.41 % diferentes entre sí con un promedio en magnitud de 83.70 %. El resultado verifica la alta sensibilidad ante pequeños cambios en la plantilla clara en el esquema de encriptado propuesto.

8.4.4. Histogramas

El histograma es una visualización gráfica sencilla de la distribución de frecuencia de un conjunto de datos continuos utilizando barras de diferentes alturas y representa información estadística [172]. El histograma de la plantilla clara se muestra en la Fig. 8.17(a), se puede apreciar la característica estadística de la fuente; sin embargo, el histograma de la plantilla encriptada tiene un rango con una distribución uniforme, como se aprecia en la Fig. 8.17(b). Por tanto, el proceso de difusión produce un histograma uniforme para resistir un ataque estadístico.

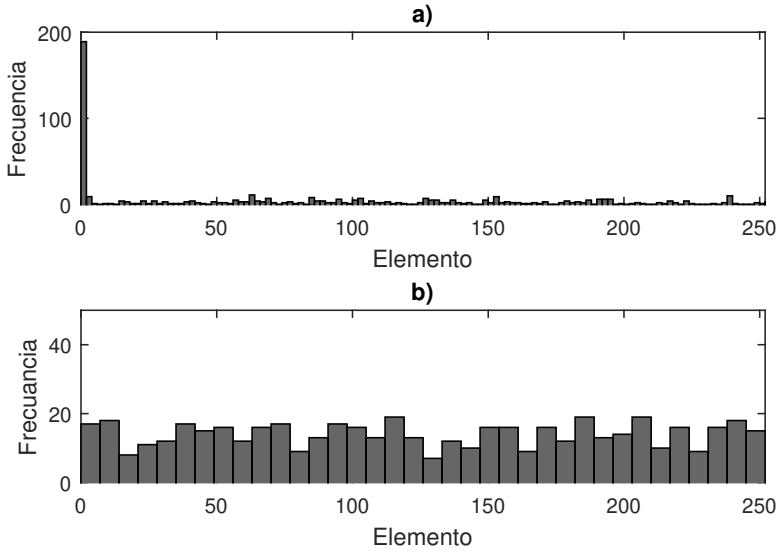


Figura 8.17: Histogramas: a) Plantilla clara y b) Plantilla encriptada.

8.4.5. Frecuencia flotante

La frecuencia flotante prueba si el criptograma presenta secciones débiles midiendo cuántos símbolos diferentes entre [0, 255] hay en ventanas de 256 elementos. Si el encriptado produce una sección débil, se puede utilizar para encontrar la plantilla clara o la clave secreta; por lo tanto, la frecuencia flotante debe ser uniforme y debe tener todos los símbolos posibles [173]. La prueba consiste en seleccionar los primeros 256 elementos de la plantilla y luego, se mueve la ventana una posición hacia la derecha y se repite la prueba sucesivamente hasta formar un escaneo de todo el mensaje y finalizar en la posición inicial. En la Fig. 8.18(a), se observa que la frecuencia flotante de la plantilla clara tiene el 41.01 % de todos los elementos posibles. La Fig. 8.18(b), de la plantilla encriptada tiene el 64.45 % de todos los elementos posibles. Por tanto, el encriptado propuesto no tiene secciones débiles.

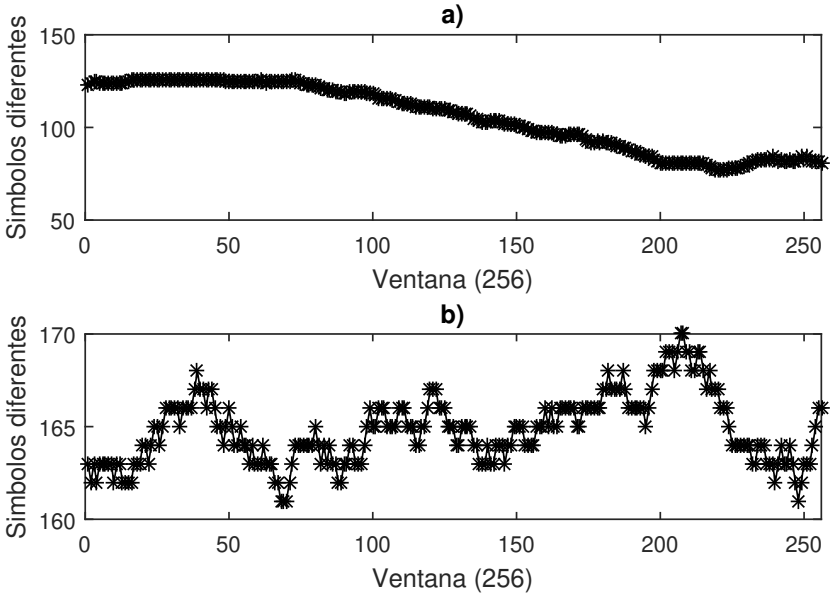


Figura 8.18: Frecuencia flotante: a) Plantilla clara y b) Plantilla encriptada.

8.4.6. 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 plantilla clara. Por tanto, la señal encriptada debe tener correlación nula [174].

La fórmula para calcular la correlación es la siguiente

$$Cr = \frac{N \times \sum_{i=0}^{N}(x_i \times y_i) - \sum_{i=0}^{N} x_i \times \sum_{i=0}^{N} y_i}{\sqrt{\left(N \times \sum_{i=0}^{N}(x_i)^2 - \left(\sum_{i=0}^{n} x_i\right)^2\right) \times \left(N \times \sum_{i=0}^{N}(y_i)^2 - \left(\sum_{i=0}^{n} y_i\right)^2\right)}} \tag{8.4}$$

El valor de correlación es $Cr \in (-1, 1)$ donde 0 significa nula correlación y 1 significa alta correlación. El resultado es de -0.038244250127816, por lo que se puede decir que tiene correlación nula.

8.4.7. Autocorrelación

La autocorrelación determina si la plantilla encriptada tiene patrones repetitivos, recurrencia o dependencias, esto se calcula con

$$AC(k) = \frac{A - D}{N}, \tag{8.5}$$

donde AC es la es la autocorrelación del mensaje desplazado k posiciones, A es el número de elementos que concuerdan entre el mensaje original y el mensaje desplazado,

D es el número de elementos que no concuerdan y N es la longitud del mensaje. Grandes valores positivos de AC significan que muchos bits son idénticos y grandes valores negativos de AC significa que muchos bits son opuestos; mientras que un valor de AC nulo significa que se tiene el mismo número de 1's y 0's [175].

En este análisis, se calcula la autocorrelación a nivel bit y se utilizan 8 bits para representar cada elemento de la plantilla. Primero, la autocorrelación de la plantilla clara se calcula como sigue: los elementos se transforman a bits, después, se determina la autocorrelación del mensaje con un valor de hasta $k = 500$ hacia la derecha. La Fig. 8.19, muestran la autocorrelación de la plantilla clara (línea discontinua) y de la plantilla encriptada (línea continua). La autocorrelación de la plantilla clara tiene patrones repetitivos con altos valores positivos, mientras que la plantilla encriptada tiene una autocorrelación cercana a 0, es decir, el proceso de encriptado genera números pseudoaleatorios uniformemente.

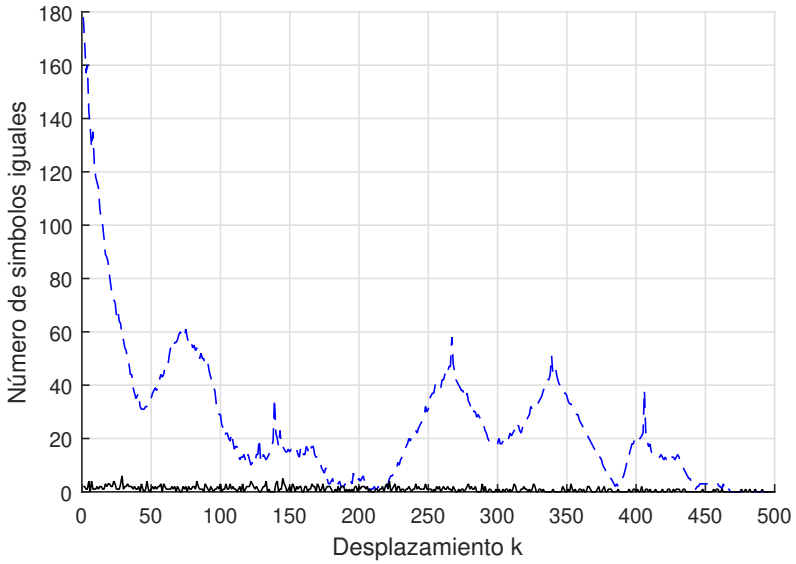


Figura 8.19: Autocorrelación: Linea discontinua para plantilla clara y linea continua para plantilla encriptada.

8.4.8. Entropía de la información

La entropía determina que tan impredecible es un mensaje, es decir, mide cuanto desorden genera el algoritmo de encriptado. Si el proceso de encriptado es bueno, este genera alto desorden en la señal encriptada; por tanto, mayor será la entropía. Caso contrario, si el proceso de encriptado no es suficientemente aleatorio, el algoritmo criptográfico puede estar sujeto a un exitoso ataque de entropía, porque el criptograma es predecible [176].

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

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\ log_2(1/p(m_i)), \tag{8.6}$$

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 encriptado con 2^N posibles valores, la entropía debería ser idealmente $H(m) = N$, si m es puramente aleatorio.

La plantilla tiene 256 símbolos diferentes y su entropía máxima es $H = 8$, es decir, todos los elementos aparecen con la misma probabilidad. La entropía de la plantilla clara es $H = 5.54$, mientras que la entropía de la plantilla encriptada es $H = 7.64$. Por tanto, el encriptado propuesto genera todos los símbolos con aproximadamente la misma probabilidad para generar gran desorden en la plantilla encriptada.

8.4.9. Desempeño y recursos utilizados

En cualquier implementación es importante determinar los recursos de implementación empleados, como memoria requerida del programa, arquitectura del microcontrolador, módulos de comunicación, etc., que están relacionados con el costo de la aplicación.

La implementación está basada en un microcontrolador de 32 bits con arquitectura Arm Cortex M4, el algoritmo de encriptado se programa con lenguaje C mediante el software Arduino IDE, se programa en la memoria flash del microcontrolador. La frecuencia de operación es de 48 MHz, se utiliza I2C para la comunicación con el módulo As608 y para la pantalla LCD, para el módulo AD8232 y mando de control se usa los pines GPIO y SPI para el adaptador de la memoria micro SD.

El sistema de autentificación propuesto posee la precisión del módulo As608 con una tasa de falsa aceptación de 10^3 (uno en un cien mil acepta un falso usuario) y una tasa de falso rechazo de 10^2 (una de cada cien rechaza a un usuario autorizado). El tiempo de registro de un nuevo usuario requiere de 4 segundos, lo que incluye lectura de huella dactilar, encriptado en microcontrolador y almacenamiento en memoria micro SD. El proceso de autentificación requiere de 5 segundos que incluye leer la huella dactilar, desencriptar el criptograma del usuario y proceso de comparación. El costo de implementación es menor a \$50 USD. Por tanto, el esquema propuesto puede ser implementado en aplicaciones en tiempo real.

La Tabla 8.3, muestra los recursos utilizados en la implementación en microcontrolador del algoritmo de encriptado propuesto.

Tabla 8.3: Recursos de implementación.

Característica	Usada/Total
Memoria Flash (kB)	(30 %)/256
Puerto de comunicación	USB 3.0
Frecuencia (MHz)	(60 %)/48
Voltaje (VDC)	5V
Costo del sistema embebido (USD)	50
Dimensiones (cm)	30×30
Tasa de Falsa Aceptación	<0.001 % (Nivel de seguridad 3)
Tasa de Falso Rechazo	<1.0 % (Nivel de seguridad 3)

8.4.10. Comparación con la literatura

Se utiliza el módulo As608 para leer, generar y verificar plantillas de huellas dactilares, lo hace de forma independiente con sus algoritmos internos, lo que facilita el desarrollo de este tipo de sistemas. El tiempo de registro de un nuevo usuario requiere aproximadamente 4 segundos, lo que incluye leer la muestra de huella dactilar, procesar la plantilla, enviar la plantilla al microcontrolador, encriptado caótico de la plantilla en el microcontrolador y almacenamiento en memoria micro SD. El proceso de autenticación requiere 5 segundos, lo que incluye tomar la muestra del usuario, leer el criptograma de la base de datos (memoria micro SD), proceso de desencriptado y enviar la plantilla para compararla con la muestra del usuario para la autenticación. El número de aceptaciones falsas (FAR) y el número de rechazos falsos (FRR) es igual que el módulo As608.

El uso de la clave hash SHA-2 de 256 bits relacionada con una plantilla clara agregó alta sensibilidad a la biometría y combinada con la clave personal de 256 bits genera criptogramas con distribución uniforme y autocorrelación nula, con una entropía de información cercana al valor máximo de 8. Considerando el análisis de seguridad presentado, el sistema de acceso seguro propuesto proporciona contramedidas contra suplantación biométrica y evita principalmente el robo de identidad. La principal desventaja del esquema propuesto es que la programación debe ser pulida para disminuir el tiempo de procesamiento. En la Tabla 8.4, se presentan las comparaciones con esquemas biométricos de protección de huellas dactilares similares en la literatura.

Tabla 8.4: Comparaciones con esquemas similares en la literatura.

	Esquema propuesto	**Ref.**[151]	**Ref.**[156]	**Ref.**[157]
Plantilla biométrica	Huella dactilar	Huella dactilar	Huella dactilar	Huella dactilar
Dominio coincidente	Dominio Simple	Dominio Simple	Dominio Simple	Dominio Simple
Revocabilidad	No	–	–	No
Diversidad	Si	–	–	Si
Seguridad	Si	–	–	Si
FAR y FRR afectados	No	–	–	No
Análisis de seguridad				
Espacio de clave secreta	✓	✓	–	✓
Sensibilidad a la clave secreta	✓	–	✓	–
Secuencia caótica optimizada	✓	–	–	–
Sensibilidad a la plantilla clara	✓	–	–	–
Histogramas	✓	✓	✓	–
Frecuencia flotante	✓	–	–	–
Correlación	✓	✓	✓	–
Autocorrelación	✓	–	–	–
Entropía de la información	✓	✓	✓	–
Desempeño	✓	–	✓	–
Recursos implementados	✓	–	✓	–
Implementación				
Sistema embebido	✓	–	–	–
Computadora personal	–	✓	✓	✓
Técnica de clasificación				
Algoritmo	Algortimo SHA-2	–	Señal ECG	–
Encriptado	hypercaótico	caótico	caótico	homomórfico
Mapa	Hénon-Seno	Piece-wise	Logístico y Hénon	–

8.5. Conclusiones

En este capítulo se presentó el sistema de acceso seguro basado en sistema experto y encriptado de huella dactilar para proteger las plantillas dactilares y evitar suplantación biométrica y robo de identidad. Se implementó en un sistema embebido basado en un microcontrolador de 32 bits donde el proceso consistió en dos pasos, primero se identificó al usuario mediante la señal biomédica de electrocardiograma con un sistema experto que consistió en la detección del pico R, después, ya que se identificó al usuario, pasaba al proceso de autenticación mediante la huella dactilar para poder finalmente dar acceso al sitio restringido.

Los análisis de seguridad mostraron la efectividad de la implementación y seguridad que brinda el algoritmo criptográfico, además, los recursos de implementación son mínimos y a bajo costo, por lo cual, el sistema de acceso seguro puede aplicarse para uso al control de acceso a sitios restringidos.

Capítulo 9

Conclusiones

9.1. Conclusiones generales

En este trabajo doctoral, se diseñó e implementó en un sistema embebido de bajo costo un sistema de acceso seguro basado en encriptado caótico y sistema experto. Se propuso un novedoso mapa hypercaótico Hénon-Seno 2D basado en retroalimentación en tiempo discreto utilizando el mapa de Hénon 1D y el mapa de Seno 1D donde la dinámica del mapa hypercaótico se mejora mediante el uso de la función de resto después de la división (*rem*) para obtener mejores propiedades estadísticas aleatorias y evitar la baja uniformidad y baja aleatoriedad. El mapa hypercaótico propuesto se validó mediante los análisis de exponente de Lyapunov, la trayectoria del atractor, los histogramas y la sensibilidad en la inicialización. Además, se diseñó un generador de números pseudoaleatorios de 8 bits basado en el mapa hypercaótico propuesto y se calcula la semilla inicial del PRNG mediante una clave secreta. También, un nuevo algoritmo de encriptado caótico basado en el mapa hypercaótico y PRNG propuesto fue diseñado, el cual está basado en una clave simétrica con arquitectura de confusión y difusión. Se caracteriza por ser seguro y eficiente para aplicaciones en sistemas embebidos (y no embebidos) para brindar confidencialidad a la información cuando se almacena en base de datos.

El funcionamiento del sistema de acceso seguro se basó en dos procesos; primero, la detección del usuario mediante un sistema experto con la señal biomédica de electrocardiograma basado en la detección del pico R de la señal de ECG, luego, la autenticación mediante la huella dactilar del usuario para posteriormente brindar acceso al sitio restringido. Se utilizó una clave secreta de 512 bits con al cual se obtuvieron las condiciones iniciales y los parámetros de control de manera indirecta del mapa hypercaótico Hénon-Seno para realizar el proceso de encriptado. El criptograma de la plantilla dactilar se almaceno en una memoria micro SD para después ser desencriptada en el proceso de autenticación y comparación de plantillas. Los resultados demostraron que el algoritmo criptográfico es seguro para la implementación en sistemas embebidos de bajo costo y para el encriptado de plantillas dactilares evitando el robo de identidad de usuarios.

Además, el uso del sistema experto mediante la señal de ECG permite prevenir el uso de falsos identificadores biométricos, lo que aumenta la seguridad del sistema. El sistema de acceso seguro puede ser implementado para el acceso a sitios restringidos como oficinas, bancos, hospitales y cualquier lugar con acceso controlado.

9.2. Principales contribuciones de este trabajo doctoral

La siguiente lista muestra a manera de resumen, las principales contribuciones de este trabajo de investigación doctoral:

1. Se propuso un nuevo mapa hypercaótico de 2D basado en dos mapas caóticos de 1D.

2. Se desarrolló un nuevo generador de números pseudoaleatorios el cual fue implementado en un microcontrolador de 8 bits.

3. Se diseñó un algoritmo basado en el PRNG y mapa hypercaótico propuestos, basado en una clave simétrica de 512 bits implementado en un microcontrolador de 32 bits.

4. Se desarrolló un sistema experto para detección de usuario mediante la señal biomédica de electrocardiograma para la prevención de falsos identificadores biométricos.

5. Se encriptaron plantillas dactilares con el algoritmo propuesto y se almacenaron en una memoria micro SD para aumentar la seguridad y prevenir el robo de identidad.

6. Se implementó en un sistema embebido de bajo costo un sistema de acceso seguro para aplicaciones en acceso seguro para hospitales, oficinas del gobierno, bancos, universidades, entre otros.

7. En cada caso, se analizaron las propiedades caóticas y el algoritmo de encriptado mediante distintos análisis de seguridad.

9.3. Trabajo a futuro

Como trabajo a futuro se plantean las siguientes actividades:

- Realizar análisis de seguridad a nivel físico de los sistemas embebidos presentados en este trabajo, como análisis de la información de tiempo de cálculos, el monitoreo de consumo de energía, fugas electromagnéticas, análisis de sonido o remanencia de datos, que puede proporcionar una fuente adicional de información que puede ser explotada para romper el sistema.

- Almacenar criptograma en la nube (internet) para mayor seguridad en la plantilla dactilar, ya que, al almacenar la plantilla junto con el sistema embebido mediante una memoria flash corre el riesgo de robo o extravió de la memoria.
- Analizar distintos rasgos biométricos para comparar rapidez, seguridad y eficiencia en los pasos de verificación e identidad del usuario.
- Mejorar el sistema experto agregando otro dato único de la señal de ECG para brindar mayor seguridad en el momento de identificación del usuario.
- Validar el algoritmo criptográfico propuesto con el estándar FIPS-140-2: requerimientos de seguridad para sistemas criptográficos con nivel de seguridad 3 donde se requiere seguridad física.

9.4. Productos derivados de este trabajo doctoral

Los estudios doctorales consistieron de cuatro años, durante los cuales, se realizaron trabajos de investigación relacionados con encriptado caótico y su implementación en sistema embebido. Estos trabajos están publicados en revistas indexadas en JCR (del inglés, *Journal Citation Reports*), participación en congresos nacionales e internacionales y revistas de divulgación. Estos productos se listan a continuación:

I) Revistas indexadas (JCR)

1. **Murillo-Escobar D.**, Murillo-Escobar M.A., Cruz-Hernández C., Arellano-Delgado A. y López-Gutiérrez R.M. (2023). Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation. *Nonlinear Dyn*, 111, 6773-6789, https://doi.org/10.1007/s11071-022-08101-2. Factor de Impacto: 5.6.

2. **Murillo-Escobar D.**, Cruz-Hernández C., López-Gutiérrez R.M. y Murillo-Escobar M.A. (2023). Chaotic encryption of real-time ECG signal in embedded system for secure telemedicine. *Integration*, 89, 261-270, https://doi.org/10.1016/j.vlsi.2023.01.004. Factor de Impacto: 1.9.

3. **Murillo-Escobar D.**, Vega-Pérez K., Murillo-Escobar M.A., Arellano-Delgado A. y López-Gutiérrez R.M. (2024). Comparison of two new chaos-based pseudorandom number generators implemented in microcontroller. *Integration*, 96, 102130, https://doi.org/10.1016/j.vlsi.2023.102130. Factor de Impacto: 1.9.

4. **En proceso: Murillo-Escobar D.**, Murillo-Escobar M.A., Cruz-Hernández C., Arellano-Delgado A. y López-Gutiérrez R.M. (2024). Secure access expert system based on fingerprint and ECG with hyperchaotic encryption implemented in embedded system.

II) Trabajos en colaboración - Revistas indexadas (JCR)

1. Murillo-Escobar M.A., Cruz-Hernández C., Cardoza-Avendaño L., **Murillo-Escobar D.** y López-Gutiérrez R.M. (2022). Multibiosignal chaotic encryption scheme based on spread spectrum and global diffusion process for e-health. *Biomedical Signal Processing and Control*, 78, 104001, https://doi.org/10.1016/j.bspc.2022.104001. Factor de Impacto: 5.1.

2. Murillo-Escobar M.A., López-Gutiérrez R.M., Cruz-Hernández C., Espinoza-Peralta E.E. y **Murillo-Escobar D.** (2023). Secure access microcontroller system based on fingerprint template with hyperchaotic encryption. *Integration*, 90, 27-39, https://doi.org/10.1016/j.vlsi.2023.01.002. Factor de Impacto: 1.9.

III) Participación en congresos nacionales e internacionales

1. Exposición de poster en: 3er Encuentro para la Divulgación de la Investigación en el Estudio de Sistemas Complejos y sus Aplicaciones (EDIESCA2022), 27 al 30 de septiembre 2022, UABC-FIAD, Ensenada, Baja California, México.

2. Conferencia en: 4to Encuentro para la Divulgación de la Investigación en el Estudio de Sistemas Complejos y sus Aplicaciones (EDIESCA2023), 20 al 22 de septiembre 2023, UANL-FIME, Monterrey, Nuevo León, México.

IV) Actividades de divulgación de la ciencia

1. **Murillo-Escobar D.**, Murillo-Escobar M.A. y López-Gutiérrez R.M. (2021). Control de LEDS mediante el uso de voz con Arduino. Exposición poster, *XXVIII Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC.*

2. **Murillo-Escobar D.**, Murillo-Escobar M.A. y López-Gutiérrez R.M. (2021). Obtención de señal ECG en tiempo real con Arduino. Exposición vídeo, *XXVIII Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC*, Modalidad virtual.

3. **Murillo-Escobar D.**, Vega-Pérez K., Murillo-Escobar M.A. y López-Gutiérrez R.M. (2022). Sistema multimodular basado en microcontrolador Arduino. Exposición vídeo, *XXIX Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC*, Modalidad virtual.

4. **Murillo-Escobar D.**, Vega-Pérez K., Murillo-Escobar M.A. y López-Gutiérrez R.M. (2023). Sistema de acceso seguro basado en palabra y clave secreta. Exposición vídeo, *XXX Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC*, Modalidad virtual.

5. **Murillo-Escobar D.** (2023). Detección de usuario mediante señal de electrocardiograma. *La noche de las ciencias, FIAD-UABC.*

V) Artículos de divulgación de la ciencia

1. **Murillo-Escobar D.**, Murillo-Escobar M.A. y López-Gutiérrez R.M. (2021). Control de LEDS mediante el uso de voz con Arduino. Libro de la Expo Ciencia y Tecnología, *XXVIII Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC.*

2. **Murillo-Escobar D.**, Murillo-Escobar M.A. y López-Gutiérrez R.M. (2021). Obtención de señal ECG en tiempo real con Arduino. Libro de la Expo Ciencia y Tecnología, *XXVIII Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC.*

3. **Murillo-Escobar D.**, Vega-Pérez K., Murillo-Escobar M.A. y López-Gutiérrez R.M. (2022). Sistema multimodular basado en microcontrolador Arduino. Libro de la Expo Ciencia y Tecnología, *XXIX Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC.*

4. **Murillo-Escobar D.**, Vega-Pérez K., Murillo-Escobar M.A. y López-Gutiérrez R.M. (2023). Sistema de acceso seguro basado en palabra y clave secreta. Libro de la Expo Ciencia y Tecnología, *XXX Jornadas de Ingeniería Arquitectura y Diseño, FIAD-UABC.*

Parte de las actividades de formación en los estudios doctorales, fue participar en la revisión de trabajos que fueron sometidos en revistas indexadas y congresos, estos se listan a continuación:

VI) Arbitraje de artículos para revistas indexadas y congresos

1. *Image adaptive encryption algorithm using a novel 2D chaotic system.* Original Research (SCI). Trabajo revisado en enero 2023.

2. *Design of pseudorandom number generator for controllable multidouble-scroll chaotic system.* Original Research (SCI). Trabajo revisado en abril 2023.

3. *Electronic Health File System based on Fingerprint Sensor Technology.* Original Research (SCI). Trabajo revisado en mayo 2023.

4. *On the divide-and-conquer attack of a plaintext related image chaotic encryption.* Original Research (SCI). Trabajo revisado en junio 2023.

5. *Hierarchical Refined Composite Multiscale Fluctuation-Based Dispersion Entropy: Application to feature extraction of underwater target signal.* Original Research (SCI). Trabajo revisado en junio 2023.

6. *Color image encryption algorithm based on novel 2D hyper-chaotic system and DNA crossover and mutation.* Original Research (SCI). Trabajo revisado en agosto 2023.

7. *LMI-based Design of a Robust Affine Control law for the Position Control of a Knee Exoskeleton Robot: Comparative Analysis of Stability Conditions.* Manuscrito para congreso. Trabajo revisado en septiembre 2023.

8. *Exploring Finite-Precision Error for Novel Plain-Image Encryption: Leveraging Chaotic Dynamics.* Original Research (SCI). Trabajo revisado en octubre 2023.

Bibliografía

[1] Han F., Hu J., Yu X., Feng Y. and Zhou J. (2005). A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications. *International Conference on Biometrics*, pp. 675-681.

[2] Thenuwara S.S., Premachandra C. and Kawanaka H. (2022). A multi-agent based enhancement for multimodal biometric system at border control. *Array*, 14, 100171.

[3] Maltoni D., Maio D., Jain A.K. and Prabhakar S. (2009). *Handbook of Fingerprint Recognition*, Bologna, Italy, Springer.

[4] Mohamed M.M., *et al.* (2022). Face mask recognition from audio: The MASC database and an overview on the mask challenge. *Pattern Recognition*, 122, 108361.

[5] Kausar F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, 22(4), 447-453.

[6] Bisogni C., Iovane G., Landi R.E. and Nappi M. (2021). ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions. *Journal of Information Security and Applications*, 59, 102814.

[7] Iula A. (2021). Biometric recognition through 3D ultrasound hand geometry. *Ultrasonics*, 111, 106326.

[8] Kuzu R.S., Maiorana E. and Campisi P. (2022). On the intra-subject similarity of hand vein patterns in biometric recognition. *Expert Systems With Applications*, 192, 116305.

[9] Srivastva R., Singh Y.N. and Singh A. (2022). Statistical independence of ECG for biometric authentication. *Pattern Recognition*, 127, 108640.

[10] Serhani M.A., El Kassabi H., Ismail H. and Navaz A.N. (2020). ECG Monitoring Systems: Review, Architecture, Processes, and Key Challenges. *Sensors*, 20(6), 1796.

[11] Masdari M. (2023). Towards ECG-Based Security WBANs and E-Healthcare Systems: A Comprehensive Literature Review and Survey. *Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran.*

[12] Manikandana M.A. and Soman K.P. (2012). A novel method for detecting R-peaks in electrocardiogram (ECG) signal. *Biomedical Signal Processing and Control*, 7, 118-128.

[13] Masdari M. and Ahmadzadeh S. (2017). A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems. *Journal of Network and Computer Applications*, 87, 1-19.

[14] Masdari M. and Ahmadzadeh S. (2016). Comprehensive analysis of the authentication methods in wireless body area networks. *Security and communication networks*, 9(17), 4777-4803.

[15] Shakil S., Arora D. and Zaidi T. (2022). Feature based classification of voice based biometric data through Machine learning algorithm. *Materials Today: Proceedings*, 51(1), 240-247.

[16] Zhang R., *et al.* (2022). Triboelectric biometric signature. *Nano Energy*, 100, 107496.

[17] Rahman M.M., Mishu T.I. and Bhuiyan M.A. (2022). Performance analysis of a parameterized minutiae-based approach for securing fingerprint templates in biometric authentication systems. *Journal of Information Security and Applications*, 67, 103209.

[18] Rosales-Cruz A. (2009). Clasificación de huellas digitales mediante minucias. *Instituto Nacional de Astrofísica, Óptica y Electrónica*, 1-9.

[19] Khan M.K., Zhang J. and Tian L. (2005). Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Solitons and Fractals*, 32(5), 1749-1759.

[20] Bansal V. and Garg S. (2022). A cancelable biometric identification scheme based on bloom filter and format-preserving encryption. *Journal of King Saud University*, 34(8), 5810-5821.

[21] Han F., Hu J. and Yu X. (2006). A Biometric Encryption Approach Incorporating Fingerprint Indexing in Key Generation. *International Conference on Intelligent Computing*, pp. 342-351.

[22] Dargan S. and Kumar M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems With Applications*, 143, 113114.

[23] Campisi P. (2013). *Security and Privacy in Biometrics*, Rome, Italy, Springer.

[24] Jain A.K. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

[25] Joshi M., Mazumdar B. and Dey S. (2020). A comprehensive security analysis of match-in-database fingerprint biometric system. *Pattern Recognition Letters*, 138, 247-266.

[26] Meligy A.M., Diab H. and El-Danaf M.A. (2016). Chaos Encryption Algorithm using Key Generation from Biometric Images. *International Journal of Computer Applications*, 149(11), 14-20.

[27] Wang X., Xu T. and Zhang W. (2011). Chaos-Based Biometrics Template Protection and Secure Authentication. *State of the art in Biometrics*, 15, 293-314.

[28] Bhatnagar G. (2012). Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission. *IEEE Transactions on Instrumentation and Measurement*, 61(4), 876-887.

[29] Olanrewaju L., Yebiyi O., Misra S. and Damasevicius R. (2020). Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose–Chaudhuri–Hocquenghem error-correcting codes. *Signal, Image and Video Processing*, 14, 847-855.

[30] Chen Y. and Leung Y.T. (1998). *Bifurcation and Chaos in Engineering*, London, UK, Springer.

[31] Gleick J. (1987). *Caos: Haciendo una nueva ciencia*, New York, USA, Penguin Putnam.

[32] Nezhad S., Safdarian N. and Zadeh S. (2020). New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik*, 224, 165661.

[33] Frank M.R., Mitchell L., Dodds P.S. and Danforth C.M. (2014). Standing swells surveyed showing surprisingly stable solutions for the Lorenz 96 model. *Int. J. Bifurcation Chaos*, 24(10), 1430027.

[34] Wang D., Zhang B., Qiu D. and Xie F. (2018). On the super-Lorenz chaotic model for the virtual synchronous generator. *Trans. Circuits Syst*, 65(4), 511-515.

[35] Zhou C., Hu W., Wang L. and Chen G. (2018). Turbo trellis-coded differential chaotic modulation. *Trans. Circuits Syst*, 65(2), 191-195.

[36] Hua Z. and Zhou Y. (2017). Design of image cipher using block-based scrambling and image filtering. *Inf. Sci.*, 396, 97-113.

[37] Zhang L.Y., Zhang Y., Liu Y., Yang A. and Chen G. (2017). Security analysis of some diffusion mechanisms used in chaotic ciphers. *Int. J. Bifurcation Chaos*, 27(10), 1750155.

[38] Wong K.E., Lin Q. and Chen J. (2010). Simultaneous arithmetic coding and encryption using chaotic maps. *Trans. Circuits Syst.*, 57(2), 146-150.

[39] Chai X., Chen Y. and Broyde L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.*, 88, 197-213.

[40] Zhang Y., Xiao D., Shu Y. and Li J. (2013). A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal Process. Image Commun.*, 28(3), 292-300.

[41] Cho K. and Miyano T. (2015). Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution. *Trans. Circuits Syst.*, 62(2), 478-487.

[42] Persohn J.K. and Povinelli R.J. (2012). Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. *Chaos Solitons Fractals*, 45(3), 238-245.

[43] Zhou Y., Hua Z., Pun C.M. and Chen C.L.P. (2015). Cascade chaotic system with applications. *Trans. Cybern.*, 45(9), 2001-2012.

[44] Zhou Y., Bao L. and Chen C.L.P. (2014). A new 1D chaotic system for image encryption. *Signal Process.*, 97, 172-182.

[45] Wu Y., Noonan J.P. and Agaian S. (2011). A wheel-switch chaotic system for image encryption. *Proc. Int. Conf. Syst. Sci. Eng.*, pp. 23-27.

[46] Zhou Y., Bao L. and Chen C.L.P. (2013). Image encryption using a new parametric switching chaotic system. *Signal Process.*, 93(11), 3039-3052.

[47] Xie E.Y., Li L., Yu S. and Lü J. (2016). On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Process.*, 132, 150-154.

[48] Zhang Y.Q. and Wang X.Y. (2014). A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Inf. Sci.*, 273(8), 329-351.

[49] Zhu S., *et al.* (2023). Secure image encryption scheme based on a new robust chaotic map and strong S-box. *Mathematics and Computers in Simulation*, 207, 322-346.

[50] Hua Z. and Zhou Y. (2018). One-dimensional nonlinear model for producing chaos. *Trans. Circuits Syst.*, 65(1), 235-246.

[51] Pareschi F., Setti G. and Rovatti R. (2010). Implementation and testing of high-speed CMOS true random number generators based on chaotic systems. *Trans. Circuits Syst.*, 57(12), 3124-3137.

[52] Liu Y., Li X.Z., Cheung R.C.C., Chan S.C. and Wong H. (2018). Highspeed discrete Gaussian sampler with heterodyne chaotic laser inputs. *Trans. Circuits Syst.*, 65(6), 794-798.

[53] Lan R., He J., Wang S., Liu Y. and Luo X. (2019). A Parameter-Selection-Based Chaotic System. *Transactions on Circuits and Systems*, 66(3), 492-496.

[54] Lan R., He J., Wang S., Gu T. and Luo X. (2018). Integrated chaotic systems for image encryption. *Signal Processing*, 147, 133-145.

[55] May M. (1976). Simple Mathematical Models With Very Complicated Dynamics. *Nature*, 261, 459-467.

[56] Zamorano-Aguilar A. (2012). Teorías del caos y lingüística: aproximación caológica la comunicación verbal humana. *Signa*, 21, 679-705.

[57] Wang J., Liu L., Xu M. and Li X. (2022). A novel content-selected image encryption algorithm based on the LS chaotic model. *Journal of King Saud University – Computer and Information Sciences*, 34, 8245-8259.

[58] Wang X., Liu C. and Jiang D. (2022). Visually meaningful image encryption scheme based on new-designed chaotic map and random scrambling diffusion strategy. *Chaos, Solitons and Fractals*, 164, 112625.

[59] Çavuşoğlu Ü., Akgül A., Zengin A. and Pehlivan I. (2017). The design and implementation of hybrid RSA algorithm using a novel chaos based RNG. *Chaos, Solitons and Fractals*, 104, 655-667.

[60] Natiq H., Al-Saidi N.M.G., Said M.R.M. and Kilicman A. (2018). A new hyperchaotic map and its application for image encryption. *Eur. Phys. J. Plus*, 133(6), 1-14.

[61] Cetina-Denis J.J. (2017). *Diseño de trayectorias caóticas en robots móviles*, CICESE, Ensenada.

[62] Méndez-Ramírez R.D. (2018). *Implementación de osciladores caóticos en sistemas embebidos y aplicaciones*, CICESE, Ensenada.

[63] Malar K.A. and Ganesh R.S. (2022). Novel aperture coupled fractal antenna for Internet of wearable things (IoWT). *Measurement: Sensors*, 24, 100533.

[64] Volos C.K., Doukas N., Kyprianidis I., *et al.* (2013). Chaotic Autonomous Mobile Robot for Military Missions. *Recent Advances in Telecommunications and Circuit Design*, pp. 97-202.

[65] Lai Q., *et al.* (2020). Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption. *Chinese Journal of Physics*, 67, 615-630.

[66] Parisi M., *et al.* (2020). A mascon approach to estimating the depth of Jupiter's Great Red Spot with Juno gravity measurements. *Planetary and Space Science*, 181, 104781.

[67] Elghandour A., Salah A. and Karawia A. (2022). A new cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal*, 13(1), 101489.

[68] Smart N.P. (2016). *Cryptography Made Simple*, Bristol, UK, Springer.

[69] Shannon C.E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(3), 379-423.

[70] Shannon C.E. (1949). Communication Theory of Secrecy Systems. *Communication Theory of Secrecy Systems*, 28(4), 656-715.

[71] Diffie W. and Hellman M.E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

[72] Tawalbeh L., Alicea M. and Alsmadi I. (2022). New and Efficient Lightweight Cryptography Algorithm for Mobile and Web Applications. *Procedia Computer Science*, 203, 111-118.

[73] Lucena-López M.J. (2022). *Criptografía y Seguridad en Computadores*, Jaén, España, Creative Commons.

[74] Lohachab A., Lohachab A. and Jangra A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet of Things*, 9, 100174.

[75] Millérioux G., Hernández A. and Amigo J.M. (2020). Criptografía caótica con reinyección de la información. *III Congreso Iberoamericano di Seguridad Informática*, pp. 207-220.

[76] Jakimoski G. and Ljupço K. (2001). Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. *IEEE Transactions on Circuits and Systems*, 48(2), 163-169.

[77] Alanazi H.O., Zaidan B.B., Zaidan A.A., Jalab H.A., Shabbir M. and Al-Nabhani Y. (2010). New Comparative Study Between DES, 3DES and AES within Nine Factors. *Journal of Computing*, 2(3), 152-157.

[78] Kumaraswamy P., Janaki V., Srinivas K. and Naveen D. (2021). Public key authentication schemes in asymmetric cryptography. *Materials Today: Proceedings*, https://doi.org/10.1016/j.matpr.2021.02.182.

[79] Kumar M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array*, 15, 100242.

[80] Pavithran P., Mathew S., Namasudra S. and Lorenz P. (2021). A novel cryptosystem based on DNA cryptography and randomly generated mealy machine. *Computers and Security*, 104, 102160.

[81] Teh J.S., Alawida M. and Cheng Y. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, 50, 102421.

[82] Zheng Z. (2022). *Modern Cryptography*, Beijing, China, Springer.

[83] Padilla-López J.R., Chaaraoui A.A. and Flórez-Revuelta F. (2015). Visual privacy protection methods: A survey. *Expert Systems with Applications*, 42(9), 4177-4195.

[84] Aljohani M., Ahmad I., Basheri M. and Alassafi M.O. (2019). Performance Analysis of Cryptographic Pseudorandom Number Generators. *IEEE Access*, 7, 39794-39805.

[85] Kerckhoffs A. (1883). La Cryptographie Militaire. *Journal des sciences militaires*, 9, 161-191.

[86] Ferdous M.D., Morshed-Chowdhury M.J. and Hoque M.A. (2021). A Survey of Consensus Algorithms in Public Blockchain Systems for Crypto currencies. *Journal of Network and Computer Applications*, 182, 103035.

[87] Benkhaddra I., Senouci M.R., Madoune S.A., Senouci A., Tanougast C., Sadoudi S. and Hang L. (2022). High randomness hyperchaos-based parameterizable TRNG: Design, FPGA implementation and exhaustive security analysis. *Displays*, 74, 102274.

[88] Murillo-Escobar M.A., Cruz-Hernández C., Cardoza-Avendaño L. and Méndez-Ramírez R. (2016). A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 87, 407-425.

[89] Chen S., Li B. and Zhou C. (2018). FPGA implementation of SRAM PUFs based cryptographically secure pseudo-random number generator. *Microprocessors and Microsystems*, 59, 57-68.

[90] Paar C. and Pelzl J. (2010). *Understanding Cryptography*, Lovaina, Bélgica, Springer.

[91] García E., López M.A. and Ortega J.J. (2005). *Una introducción a la criptografía*, Ciudad Real, España, Academia.

[92] Zhang T., Hu X., Xiao J. and Zhang G. (2022). A survey of visual navigation: From geometry to embodied AI. *Engineering Applications of Artificial Intelligence*, 114, 105036.

[93] Sahin S., Tolun M.R. and Hassanpour R. (2012). Hybrid expert systems: A survey of current approaches and applications. *Expert Systems with Applications*, 39, 4609-4617.

[94] Walek B. and Fajmon P. (2023). A hybrid recommender system for an online store using a fuzzy expert system. *Expert Systems With Applications*, 212, 118565.

[95] Logesh R. and Subramaniyaswamy V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. *Electronic Government*, 14, 91-113.

[96] Ruiz-Barroso P., Castro F.M., Delgado-Escaño R., Ramos-Cózar J. and Guil N. (2022). High performance inference of gait recognition models on embedded systems. *Sustainable Computing: Informatics and Systems*, 36, 100814.

[97] Richard C., Bil C., Sardina S. and O'bree T. (2022). Designing an expert system to support aviation occurrence investigations. *Expert Systems With Applications*, 207, 117994.

[98] Saibene A., Assale M. and Giltri M. (2021). Expert systems: Definitions, advantages and issues in medical field applications. *Expert Systems With Applications*, 177, 114900.

[99] Singh A., Joshi P. and Nandi G. (2016). Development of a Fuzzy Expert System based Liveliness Detection Scheme for Biometric Authentication. *Conference on Signal and Image Processing*, pp. 1-8.

[100] Reggio G., Leotta M., Cerioli M., Spalazzese R. and Alkhabbas F. (2020). What are IoT systems for real? An experts' survey on software engineering aspects. *Internet of Things*, 12, 100313.

[101] Holt A. and Huang C.Y. (2014). *Embedded Operating Systems: A Practical Approach*, Bristol, UK, Springer.

[102] Pan T. and Zhu Y. (2018). *Designing Embedded Systems with Arduino: A Fundamental Technology for Makers*, Zhenjiang, China, Springer.

[103] Dong A.H., Shan D., Ruan Z., Zhou L.Y. and Zuo F. (2013). The Design and Implementation of an Intelligent Apparel Recommend Expert System. *Mathematical Problems in Engineering*, 2013, 343171.

[104] Payán D., Frehn L., Garcia L., Tierney A. and Rodriguez P. (2022). Telemedicine implementation and use in community health centers during COVID-19: Clinic personnel and patient perspectives. *SSM - Qualitative Research in Health*, 2, 100054.

[105] Arboleda E., Balaba J. and Espineli J. (2017). Chaotic Rivest-Shamir-Adlerman algorithm with data encryption standard scheduling. *Bulletin of Electrical Engineering and Informatics*, 6, 219-227.

[106] Huang Z.W. and Zhou N.R. (2022). Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion. *Optics and Laser Technology*, 149, 107879.

[107] Gao X. (2021). Image encryption algorithm based on 2D hyperchaotic map. *Optics and Laser Technology*, 142, 107252.

[108] Song W., Wang B., Wang Q., Peng Z., Lou W. and Cui Y. (2017). A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. *Journal of Parallel and Distributed Computing*, 99, 14-27.

[109] Michel-Macarty J.A., Murillo-Escobar M.A., López-Gutiérrez R.M., Cruz-Hernández C. and Cardoza-Avendaño L. (2018). Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine. *Comput Methods Programs Biomed.*, 162, 165-175.

[110] Nagakrishnan R. and Revathi A. (2020). A Robust Cryptosystem to Enhance the Security in Speech Based Person Authentication. *Multimedia Tools and Applications*, 79, 20795-20819.

[111] Pushpalatha G.S. and Ramesh S. (2021). Chaotic based encryption algorithms for speech signal and cryptographic requirements: A brief survey. *Materials Today: Proceedings*, https://doi.org/10.1016/j.matpr.2021.01.244.

[112] Kocarev L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine,* 1, 6-21.

[113] Hamsa A., Abdullah-Hikmat N., Abdullah-Waleed A. and Mahmoud A.J. (2019). A hybrid chaotic map for communication security applications. *International Journal of Communication Systems*, 33, 1-20.

[114] Mondal B., *et al.* (2022). A secure image encryption scheme based on cellular automata and chaotic skew tent map. *Journal of Information Security and Applications*, 45, 117-130.

[115] Lambić D. (2018). Security analysis and improvement of the pseudo-random number generator based on quantum chaotic map. *Nonlinear Dyn.*, 94, 1117-1126.

[116] Lambić D. and Nikolić M. (2017). Pseudo-random number generator based on discrete-space chaotic map. *Nonlinear Dyn.*, 90, 223–232.

[117] Meranza-Castillón M.O., Murillo-Escobar M.A., López-Gutiérrez R.M. and Cruz-Hernández C. (2019). Pseudorandom number generator based on enhanced Hénon map and its implementation. *AEU - International Journal of Electronics and Communications*, 107, 239-251.

[118] Elmanfaloty R.A. and Abou-Bakr E. (2019). Random property enhancement of a 1D chaotic PRNG with finite precision implementation. *Chaos, Solitons and Fractals*, 118, 134-144.

[119] Rezk A.A., Madian A.H., Radwan A.G. and Soliman A.M. (2019). Reconfigurable chaotic pseudo random number generator based on FPGA. *AEU - International Journal of Electronics and Communications*, 98, 174-180.

[120] Kopparthi V.R., Kali A., Sabat S.L., Anumandla K.K., Peesapati R. and Eyebe-Fouda J.S. (2022). Hardware architecture of a digital piecewise linear chaotic map with perturbation for pseudorandom number generation. *AEU - International Journal of Electronics and Communications*, 147, 154138.

[121] Krishnamoorthi S., Jayapaul P., Dhanaraj R.K., Rajasekar V., Balusamy B. and Islam H. (2021). Design of pseudo-random number generator from turbulence padded chaotic map. *Nonlinear Dynamics*, 104, 1627-1643.

[122] Deep-Gupta M. and Chauhan R.K. (2021). Secure image encryption scheme using 4D-Hyperchaotic systems based reconfigurable pseudo-random number generator and S-Box. *Integration*, 81, 137-159.

[123] Wang L. and Cheng H. (2019). Pseudo-Random Number Generator Based on Logistic Chaotic System. *Entropy*, 21, 960.

[124] Valle J., Machicao J. and Odemir M. (2022). Chaotical PRNG based on composition of logistic and tent maps using deep-zoom. *Chaos, Solitons and Fractals*, 161, 112296.

[125] Li-Hua G., Rouqing W. and Nan-Run Z. (2020). A New 4D Chaotic System with Coexisting Hidden Chaotic Attractors. *International Journal of Bifurcation and Chaos*, 30, 2050142.

[126] Li-Hua G., Hui-Xin L., Rou-Qing W. and Nan-Run Z. (2022). New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG. *Physica A*, 591, 126793.

[127] Jing-Yi D., Yan M. and Nan-Run Z. (2021). Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map. *Quantum Information Processing*, 20, 246.

[128] García-Guerrero E.E., Inzunza-González E., López-Bonilla O.R., Cárdenas-Valdez J.R. and Tlelo-Cuautle E. (2020). Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos, Solitons and Fractals*, 113, 109646.

[129] Hénon M. (1976). A two-dimensional mapping with a strange attractor. *Commun. Math. Phys.*, 50, 69–77.

[130] Mahaboob-Basha S., Mathivanan P. and Balaji-Ganesh A. (2022). Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map. *Optik*, 259, 168956.

[131] Wolf A. (1986). Quantifying chaos with Lyapunov exponents. *Princeton University Press.*, 13, 273-289.

[132] Lai Q., Lai C., Zhang Z. and Li C. (2022). Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption. *Chaos, Solitons and Fractals*, 158, 112017.

[133] Bonny T. (2020). Chaotic or hyper-chaotic oscillator? Numerical solution, circuit design, MATLAB HDL-coder implementation, VHDL code, security analysis, and FPGA realization. *Circ. Syst. Signal Process*, 40, 1061-1088.

[134] Murillo-Escobar M.A., Cruz-Hernández C., Abundiz-Pérez F., López-Gutiérrez R.M. and Acosta Del Campo O.R. (2015). A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos. *Signal Processing*, 109, 119-131.

[135] Liu X., Tong X., Wang Z. and Zhan M. (2022). A new n-dimensional conservative chaos based on Generalized Hamiltonian System and it's applications in image encryption. *Chaos, Solitons and Fractals*, 154, 111693.

[136] Wang Y., Liu Z., Ma J. and He H. (2016). A pseudorandom number generator based on piecewise logistic map. *Nonlinear Dyn.*, 83, 2373–2391.

[137] Atmel Corporation. (2005). 8-bit Microcontroller with 256K Bytes In-System Programmable Flash. *Atmel*, 2549A–AVR–03/05.

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

[139] IEEE Computer Society. (1985). IEEE standard for binary floating-point arithmetic. *ANSI/IEEE Std.*, 754.

[140] Tutueva A.V., Nepomuceno E.G., Karimov A.I., Andreev A.S. and Butusov D.N. (2020). Adaptive chaotic maps and their application to pseudo-random numbers generation. *Chaos, Solitons and Fractals*, 133, 109615.

[141] Nesa N., Ghosh T. and Banerjee I. (2019). Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map. *Journal of Information Security and Applications*, 47, 320-328.

[142] Alhadawi H.S., Zolkipli M.F., Ismail S.M. and Lambić D. (2019). Designing a pseudorandom bit generator based on LFSRs and a discrete chaotic map. *Cryptologia*, 42, 1-22.

[143] Liu Y. and Sun X. (2023). Towards more legitimate algorithms: A model of algorithmic ethical perception, legitimacy, and continuous usage intentions of e-commerce platforms. *Computers in Human Behavior*, 150, 108006.

[144] Arroyo D., Alvarez G. and Li S. (2008). Some Hints for the Design of Digital Chaos-Based Cryptosystems: Lessons Learned from Cryptanalysis. *IFAC Proceedings Volumes*, 42, 171-175.

[145] Remya krishnan P. and Arun Raj Kumar P. (2022). A biometric secured anonymous communication protocol for Vehicular Ad hoc Network. *Computers and Electrical Engineering*, 100, 107889.

[146] Abundiz-Pérez F., Cruz-Hernández C., Murillo-Escobar M.A., López-Gutiérrez R.M. and Arellano-Delgado A. (2016). Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map. *Mathematical Problems in Engineering*, 2016, 2670494.

[147] Heidari H. and Chalechale A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. *Expert Systems With Applications*, 19, 116276.

[148] Kaur G. (2019). Multimodal Biometrics Feature Level Fusion for Iris and Hand Geometry Using Chaos-based Encryption Technique. *Fifth International Conference on Image Information Processing (ICIIP)*, Shimla, India, pp. 304-309.

[149] Maheshwari A. and Dorai Rangaswamy M.A. (2016). Multimodal Biometrics Security System For Authentication. *Second International Conference on Science Technology Engineering and Management (ICONSTEM)*, Chennai, India, pp. 146-150.

[150] Yang Y., Yu J., Zhang P. and Wang S. (2015). A Fingerprint Encryption Scheme Based on Irreversible Function and Secure Authentication. *Computational and Mathematical Methods in Medicine*, 2015, 673867.

[151] Bhatnagar G. and Wu J. (2014). Enhancing the transmission security of biometric images using chaotic encryption. *Multimedia Systems*, 20, 203-214.

[152] Rajendran S. and Doraipandian M. (2018). Biometric Template Security Triggered by Two Dimensional Logistic Sine Map. *Procedia Computer Science*, 143, 794-803.

[153] Liu R. (2012). Chaos-Based Fingerprint Images Encryption Using Symmetric Cryptography. *9th International Conference on Fuzzy Systems and Knowledge Discovery*, Chongqing, China, pp. 2153-2156.

[154] Mehta G., Dutta M.K and SooKim P. (2016). Biometric Data Encryption using 3-D Chaotic System. *2nd International Conference on Communication Control and Intelligent Systems (CCIS)*, Mathura, India, pp. 72-75.

[155] Hasan M.M., Faruqi T.M., Tazrean M. and Chowdhury T.H. (2017). Biometric Encryption using Duffing Map. *4th International Conference on Advances in Electrical Engineering (ICAEE)*, Dhaka, Bangladesh, pp. 737-742.

[156] Falmari V.R and Brindha M. (2021). Privacy preserving biometric authentication using Chaos on remote untrusted server. *Measurement*, 177, 109257.

[157] Vallabhadas D.K. and Sandhy M. (2022). Securing multimodal biometric template using local random projection and homomorphic encryption. *Journal of Information Security and Applications*, 70, 103339.

[158] Chakraborty P. and Chakrabarti D.K. (2008). A brief survey of computerized expert systems for crop protection being used in India. *Short communication*, 18, 469-473.

[159] Babamir F.S. and Mürvet K. (2020). A multibiometric cryptosystem for user authentication in client-server networks. *Computer Networks*, 181, 107427.

[160] Sakr A.S, Pławiak P., Tadeusiewicz R. and Hammade M. (2020). Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication. *Information Sciences*, 585, 127-143.

[161] Jahiruzzaman M. and Hossain A.B.M.A. (2015). ECG Based Biometric Human Identification Using Chaotic Encryption. *International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, Savar, Bangladesh, pp. 1-5.

[162] Kaur G., Singh D. and Kaur S. (2015). Electrocardiogram (ECG) as a Biometric Characteristic: A Review. *International Journal of Emerging Research in Management and Technology*, 4, 202-206.

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

[164] Yang W., Wang S., Kang J.J, Johnstone M.N. and Bedari A. (2022). A linear convolution-based cancelable fingerprint biometric authentication system. *Computers and Security*, 114, 102583.

[165] Arduino UNO R4 WiFi. (2023). Product Reference Manual. *Arduino*, ABX00087.

[166] AD8232. (2013). Single-Lead, Heart Rate Monitor Front End. *Analog Devices*, D10866-0-2/13(A).

[167] As608. (2020). Adafruit Optical Fingerprint Sensor. *Adafruit Industries*, 1-28.

[168] Murillo-Escobar M.A., Meranza-Castillón M.O., López-Gutiérrez R.M. and Cruz-Hernández C. (2019). Suggested Integral Analysis for Chaos-Based Image Cryptosystems. *Entropy*, 21, 815.

[169] Ekani-Mebenga V.B., Kopparthi V.R., Nzeuga H.D., Eyebe-Fouda J.S., Djeufa-Dagoumguei G.M., Bitjoka G.B., Rangababu P. and Sabat S.L. (2023). An 8-bit integer true periodic orbit PRNG based on delayed Arnold's cat map. *AEU - International Journal of Electronics and Communications*, 162, 154575.

[170] Al-Mhadawi M.M., Albahrani E.A. and Lafta S.H. (2023). Efficient and secure chaotic PRNG for color image encryption. *Microprocessors and Microsystems*, 101, 104911.

[171] Wu Y., Noonan J. and Agaian S. (2011). NPCR and UACI Randomness Tests for Image Encryption. *Journal of Selected Areas in Telecommunications*, 2, 31-38.

[172] Wang X. and Gao S. (2020). Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. *Information Sciences*, 539, 195-214.

[173] Murillo-Escobar M.A., López-Gutiérrez R.M, Cruz-Hernández C., Espinoza-Peralta E.E. and Murillo-Escobar D. (2023). Secure access microcontroller system based on fingerprint template with hyperchaotic encryption. *Integration, the VLSI Journal*, 90, 27-39.

[174] Anukul P., Butta S., Barjinder S. and Neetu S. (2016). A joint application of optimal threshold based discrete cosine transform and ASCII encoding for ECG data compression with its inherent encryption. *Australasian Physical and Engineering Sciences in Medicine*, 39, 833-855.

[175] Yu F., Li L., He B., Liu L., Qian S., Zhang Z., Shen H., Cai S. and Li Y. (2021). Pseudorandom number generator based on a 5D hyperchaotic four-wing memristive system and its FPGA implementation. *The European Physical Journal Special Topics*, 230, 1763-1772.

[176] Cang S., Kang Z. and Wang Z. (2021). Pseudo-random number generator based on a generalized conservative Sprott-A system. *Nonlinear Dynamics*, 104, 827-844.