UNIVERSIDAD AUTONÓMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERIA, ARQUITECTURA Y DISEÑO.

PROGRAMA DE POSGRADO

MAESTRIA Y DOCTORADO EN CIENCIAS E INGENIERIA

# “TRANSMISION SEGURA DE INFORMACION BIOMÉDICA”

TESIS

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

DOCTOR EN CIENCIAS

Presenta:

José Antonio Michel Macarty

Ensenada, Baja California, agosto del 2018

**UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA**

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

# Transmisión segura de información biomédica

## TESIS

Que para obtener el grado de Doctor en Ciencias presenta:

**José Antonio Michel Macarty**

Aprobada por:

Rosa Martha López Gutiérrez
Co- Director de tesis

Juan Iván Nieto Hipólito
Co- Director de tesis

Humberto Cervantes de Avila
Miembro del comité

Liliana Cardoza Avendaño
Miembro del comité

César Cruz Hernández
Miembro del comité

Ensenada Baja California, México. Junio 2018

# Resumen

De la tesis de **José Antonio Michel Macarty** presentada como requerimiento parcial para obtener el grado de DOCTOR EN CIENCIAS en ELÉCTRICA, del programa de Maestría y Doctorado en Ciencias e Ingeniería de la Universidad Autónoma de Baja California. Ensenada, Baja California, México. Agosto 2018

Resumen aprobado por:

Rosa Martha López Gutiérrez — *CoDirector de tesis*

Juan Iván Nieto Hipólito — *CoDirector de tesis*

En este trabajo de tesis doctoral, se propone un esquema criptográfico basado en caos para la transmisión de datos biomédicos de forma segura. El desarrollo de la telemedicina moderna requiere de la mejora de tecnologías de redes de comunicaciones, particularmente de las redes de sensores inalámbricos de área corporal (BASN) por sus siglas en inglés. En esta tecnología la solución de la seguridad es un reto de la mayor importancia. Los nodos de sensores se interconectan en soluciones de biomedicina, dejando expuesta la información que los sensores generan, por lo que es necesario utilizar alguna técnica criptográfica, para proteger de intrusos maliciosos, la información privada de los pacientes.

En este artículo se explora el uso de generadores caóticos para mezclar las señales que generan los sensores, utilizando técnicas de espectro expandido, para proteger esta información.

**Palabras clave:** cifrado caótico, análisis de seguridad.

# Abstract

Of the thesis presented by José Antonio Michel Macarty, as a partial 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. Aug 2018.

Resumen aprobado por:

Rosa Martha López Gutiérrez — *CoDirector de tesis*

Juan Iván Nieto Hipólito — *CoDirector de tesis*

Currently, telemedicine is levered upon the improvement in communication network technology such as Body Area Sensor Networks (BASN) to provided biomedicine solutions. Nevertheless, information security is an important issue since biomedical data is exchanged through insecure channels, which exposes private information that can be intercepted by malicious intruder. Therefore, secure communication protocols for multiuser networks in telemedicine applications are a big challenge. Recent chaos-based encryption works have been conducted in the area of medical secure communications with high security capabilities. However, none of them has considered multiuser network, which is used in several e-health applications. Up to our knowledge, the proposed protocol is the first attempt to consider this service in secure telemedicine. In this paper, we propose a novel scheme based on binary

phase-shift key (BPSK) and chaos to provide information security at biosignals in a multiuser network system transmitting data over single channel.

**Keywords:** chaotic cipher, security analysis.

*A mi Familia*

(Noemi, José, Rosa Adriana, Claudia Adriana y Aldo Antonio)

# Agradecimientos

A la Dra. Rosa Martha López Gutiérrez, por su invaluable guía, su apoyo incondicional, consejos, ideas y estrategias que definitivamente propiciaron la culminación de este proyecto doctoral.

A los integrantes del comité de tesis: Dra. Liliana Cardoza Avendaño, Dr. Humberto Cervantes de Ávila, Dr. Cesar Cruz Hernández, y al Codirector Juan Iván Nieto Hipólito por apoyarme en los avances semestrales con comentarios que han moldeado el resultado de este proyecto, así como por la motivación que me dieron para continuar y culminar este proceso.

Al Dr. Miguel Ángel Murillo Escobar por su apoyo técnico y académico que aprecio infinitamente.

A la Universidad Autónoma de Baja California, por brindarme un espacio y todas las facilidades para realizarme profesionalmente. En especial a la Facultad de Ingeniería, Arquitectura y Diseño Ensenada (FIAD), a mis profesores del doctorado, directivos y personal administrativo.

Ensenada, Baja California, agosto del 2018

José Antonio Michel Macarty

# Contenido

# Capítulo 1. Introducción

La Telemedicina se ha desarrollado rápidamente en las ultimas décadas, sus aplicaciones han ido incrementando, desde sus inicios con las consultas o tratamientos de pacientes ubicados en locaciones remotas, a través de un canal de audio, hasta la gran variedad de servicios de apoyo médico que actualmente se proporcionan usando las tecnologías de comunicaciones y los artefactos biomédicos diseñados para este propósito. Por ejemplo: diagnostico remoto de padecimientos tales como diabetes, hipertensión, asma; transferencia de información clínica (tratamientos, prescripciones de drogas, pruebas de laboratorio, monitoreo de señales fisiológicas), y operaciones quirúrgicas a distancia.

El desarrollo de nuevos dispositivos médicos electrónicos y las nuevas tecnologías de telecomunicaciones han evolucionado los sistemas de salud haciéndolos más complejos y con muchas ventajas sobre los sistemas tradicionales. Por ejemplo, la información proporcionada por dispositivos electrónicos de parámetros fisiológicos es más confiable y puede ser transmitida, para su interpretación de forma remota, a través de redes de comunicaciones como el internet. Sin embargo, Internet es un canal compartido, diseñado para optimizar la distribución de información, no para la seguridad de esta. Por lo tanto, información privada puede ser interceptada por terceros, cuando viaja a través de los nodos de internet, por lo que la información medica debe ser procesada, para proporcionar confidencialidad y privacidad, para evitar diagnósticos incorrectos o un mal uso de información privada.

Recientemente, se está produciendo una evolución de las plataformas de servicios médicos, cambiando de computadoras de escritorio a dispositivos móviles e inalámbricos. Las tecnologías inalámbricas tienen el potencial de reemplazar miles de cables en un hospital, es muy confiable y permite la movilidad de pacientes y médicos. Además, es una solución de bajo costo para mejorar la accesibilidad del paciente y mejora la calidad de vida de los pacientes [1]. Este soporte médico se conoce como salud móvil o e-health. E-health incluye dispositivos médicos portátiles interconectados con tecnologías inalámbricas [2]. La seguridad médica se ha estudiado previamente en este contexto, p. ver [3-7]. Los avances en los sistemas integrados permiten que los nuevos dispositivos médicos sean menos invasivos [8]. Los datos de Bioseñales pueden almacenarse en ubicaciones remotas e incluso en la "nube". A medida que la información médica privada viaja a través de redes públicas, es importante proporcionar seguridad de la información porque los intrusos malintencionados podrían acceder a dicha información personal [9]. Los pacientes pueden ser perjudicados o dañados si un intruso malintencionado accede a información sobre enfermedades o problemas de salud. Los sensores inalámbricos se utilizan en pacientes ubicados en diferentes salas del hospital con el fin de tener un monitoreo continuo y esta información privada podría ser accedida por personas no autorizadas. Por lo tanto, es necesario proteger de los datos personales desde su origen en redes multiusuario.

En los últimos años, la criptografía digital basada en el caos se ha propuesto en la literatura para cifrar información de: imágenes, biometría, telemedicina, texto alfanumérico, entre otros, ya que los sistemas caóticos presentan varias propiedades tales como ser sistemas determinísticos, no lineales, tener dinámica aparentemente

aleatoria, amplio ancho de banda inherentemente, alta sensibilidad a la condición inicial, entre otros, que están relacionados con la confusión, difusión, complejidad y aleatoriedad de los criptosistemas. Por ejemplo, los autores presentaron en [10] un esquema de criptoanálisis y la mejora de un algoritmo de cifrado de imagen basado en el caos con permutación de nivel de bits circular entre intrapíxeles. En [11] se propuso un método eficiente para el cifrado de imágenes basado en la teoría del caos y una base de datos de secuencias de ADN (ácido desoxirribonucleico). En [12], los autores presentaron una encuesta detallada de criptosismos biométricos y biometría cancelable junto con los problemas y desafíos abiertos. Se ha demostrado que el cifrado basado en caos es muy útil en trabajos previos que logran una alta seguridad, véase p. [13-18]. Actualmente, algunos avances de la criptografía basada en el caos en la telemedicina se han propuesto en la literatura. En [19], los autores propusieron un algoritmo de cifrado simétrico basado en un mapa logístico con cifrado de doble capa caótica (DCLE) para proporcionar privacidad a información clínica, como electrocardiogramas (ECG), electroencefalogramas (EEG) y presión arterial (BP) En [20], Kenfack y Tiedeu presentaron un sistema para el cifrado basado en el caos para cifrar señales electrocardiográficas con un oscilador colpitts caótico. En [21], Lin propuso un criptosistema visual caótico utilizando un algoritmo de descomposición en modo empírico (EMD) para señales electroencefalográficas (EEG) clínicas. El concepto de diseño básico es integrar codificadores de cifrado basados en el caos bidimensional (2D), el algoritmo EMD y un método de intercalación de bloques en 2D para lograr un mecanismo de cifrada visual robusto impredecible. En 2017, Pandey et al presentó un esquema de ocultación de datos confidenciales del paciente en señal de

electrocardiograma (ECG) y su posterior transmisión inalámbrica. Los datos personales están integrados en el ECG (llamado stego-ECG) mediante el uso de un mapa caótico y el enfoque de diferencia de valores de muestra. Se presentaron medidas de rendimiento estadístico y clínico para validar el esquema propuesto [22].

Sin embargo, la mayoría de las implementaciones criptográficas anteriores encriptan datos de un solo usuario y no presentan robustez contra el ataque de ruido [19,21].

Por otro lado, la codificación de desplazamiento de fase binaria (BPSK) es un proceso de modulación digital para transmitir datos cambiando dos fases de una señal de referencia senoidal. BPSK es una técnica ampliamente implementada en varios estándares de comunicaciones inalámbricas para lograr una mayor eficiencia energética y mayores velocidades de datos, como en Acceso múltiple por división de código (CDMA), Red de área local inalámbrica (WLAN), Módem por cable, Bluetooth, entre otros. En entornos de comunicaciones hostiles, la modulación de espectro esparcido se puede utilizar para proporcionar seguridad mediante el incremento del ancho de banda, para proporcionar robustez contra el ruido y la interferencia. En relación con trabajos previos relacionados con la manipulación por desplazamiento de fase (PSK) y el caos, Carroll presentó en 2017 una alternativa al problema de sincronización del transmisor y el receptor para codificar información. Las señales caóticas son de banda ancha e impredecibles, lo que las hace potencialmente útiles cuando el objetivo son las comunicaciones de baja interferencia o incluso las comunicaciones de baja probabilidad de detección (LPD). Se utiliza un conjunto de secuencias caóticas elegidas al azar para sincronizar un transmisor caótico a un receptor y se presentan dos métodos para codificar información [23]. En [24], los

autores propusieron un sistema de codificación de cambio de fase binaria-banda ultra ancha (BPSK-UWB) en el que los accesos múltiples se definen mediante salto de tiempo caótico. Mostraron que el rendimiento del sistema propuesto depende de la densidad de probabilidad invariante de la transformación caótica utilizada. Además, los esquemas de modulación de espectro ensanchado multiusuario y el caos se han propuesto en la literatura, véase p. [25-27].

### *1.1 Motivación*

Motivados por toda esta situación, en este artículo proponemos un nuevo esquema multiusuario seguro para proporcionar privacidad en bio-señales basadas en caos y BPSK, para que los pacientes puedan ser monitoreados y diagnosticados oportunamente de forma remota y toda su información médica se transmita de manera segura a el especialista correcto utilizando solo un canal. Además, si el médico correcto tiene acceso a su información médica correspondiente (por ejemplo, cardiología o medicina deportiva para ECG y PB, neurología o neurocirugía para EEG, ortopedia, cirugía plástica, pediatría o psiquiatría para EMG, etc.), la red multiusuario - el trabajo puede ser más eficiente con un diagnóstico más rápido. Hasta donde sabemos, este trabajo que utiliza espectro ensanchado con caos para señales médicas en BASN no se ha informado anteriormente. El esquema propuesto se basa en N número de pacientes con M especialistas, donde el paciente puede tener diferentes sensores inalámbricos para monitorear y enviar sus datos médicos a diferentes especialistas. El especialista a su vez debe distinguir qué paciente está involucrado. El método de

cifrado admite ruido aditivo e interferencia de otras señales, así como protección contra intrusos. En las pruebas de simulación, las señales biológicas del ECG y la presión arterial se codifican y transmiten a través de canales inalámbricos compartidos y el personal médico autorizado puede recuperar dicha información de los criptogramas que aparecen como ruido para cualquier intruso. La figura 1.1 muestra el esquema general propuesto en esta tesis.

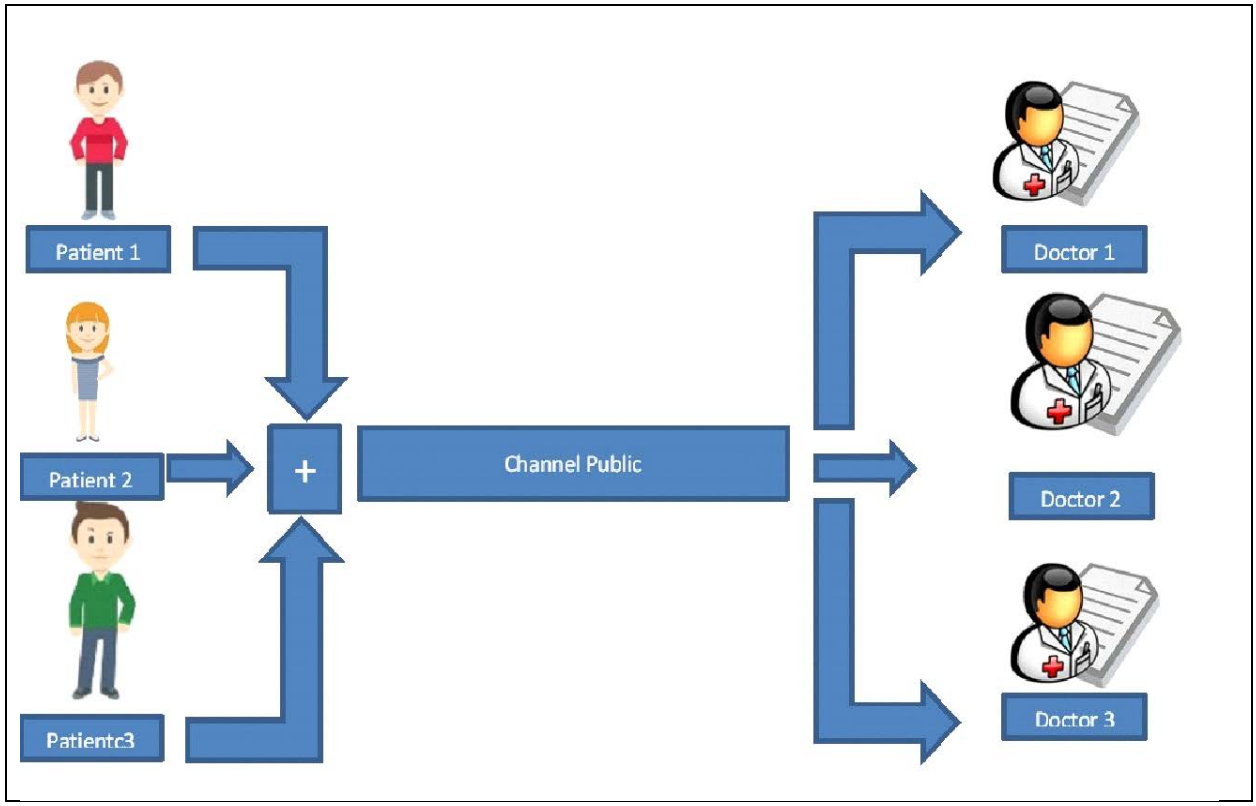



Figura 1.1 muestra el esquema general propuesto

# Capítulo 2 Criptología.

Criptología es una disciplina moderna con una estrecha relación con varios dominios como teoría de la información o códigos de corrección errores. Es una ciencia matemática que abarca la criptografía (la construcción de criptosistemas) y criptoanálisis (la búsqueda de fallas en criptosistemas).

La criptografía es una técnica matemática que permite la transmisión de datos confidenciales en un medio no seguro sin que un intruso descubra el contenido. Estos datos serán descifrados solo por el destinatario o el que conoce el clave de cifrado. La criptografía garantiza, entre otras cosas, integridad, no repudio y la autenticidad de los datos además de la confidencialidad.

 Confidencialidad asegura que solo el destinatario o guardián de la clave puede descubrir el mensaje en claro.

 Integridad permite la no modificación o no alteración de los datos durante el almacenamiento o transmisión.

 El no repudio impide negar la participación en un intercambio o tratamiento de datos.

 La autenticidad garantiza el origen y la identidad del emisor.

Una teoría fundamental fue anunciada en 1883 por A. Kerckhoffs (criptólogo holandés). Supone que el intruso conoce todos los detalles del criptosistema excepto la clave. El secreto debe rodear solo la clave de cifrado. La clave debe ser entonces el sésamo que conduce a la solución. La seguridad de un sistema de cifrado es mucho más segura si criptoanálisis hace un tiempo que no es mejor que el de la investigación exhaustiva de la

la clave. Esta evaluación se llama seguridad computacional. Otros dos criterios ya anunciados en la introducción son esenciales para construir un cifrado seguro, estas dos técnicas básicas utilizadas para oscurecer la redundancia en un mensaje son, según Shannon, confusión y difusión. Una encriptación que verifica estas dos propiedades resulta difícil de romper.

La confusión es la relación compleja entre el mensaje claro y el mensaje cifrado. El método más sencillo de aplicar confusión es la sustitución. Ejemplos de cifrado por sustitución son: Vigenère, Xor, César, Enigma.

La difusión distribuye la redundancia del mensaje claro y la clave sobre el más grande posible duración del mensaje cifrado. Podemos tener la propiedad de difusión por simple

transposición o permutación.

El principio de cifrado y descifrado es el siguiente: El texto claro es encriptado usando la relación de encriptación C = E(Ke (M)) y la recuperación de este mensaje está hecho por la función de descifrado M = D(Kd (C)) donde Ke y Kd son las claves utilizadas. Además, el cifrado y el descifrado (respectivamente la función E y D) se basan en dos métodos: criptografía simétrica y criptografía asimétrica.

## 2.1 Criptografía simétrica

En el caso de la criptografía simétrica (clave secreta), la relación entre las claves Ke y Kd es Ke = Kd. El transmisor y el receptor usan la misma clave que debe ser privada o una clave se puede deducir de la otra.

El cifrado y el descifrado simétrico de un mensaje se pueden realizar en dos formas:

a) Cifrado de flujo (continuo):

Cada bit se procesa directamente; es decir, uno opera en un flujo continuo de datos. Este modo es especialmente adecuado para la comunicación en tiempo real.

b) Cifrado de bloque:

Cada mensaje se divide en bloques de tamaños fijos. Es necesario agregar bits nulos al final del mensaje para obtener bloques enteros. La seguridad aumenta cuando los bloques aumentan de tamaño, pero la duración del proceso aumenta significativamente.

Los ejemplos de cifrado de bloques simétricos son muchos, incluidos DES y AES

 El algoritmo DES

El estándar DES fue adoptado por la NSA en 1967. Es un cifrado de bloques reúne las dos técnicas básicas: confusión (sustitución) y difusión (Permutación).

Este estándar funciona con una clave de 64 bits, de los cuales 56 se usan para el cifrado, los bits restantes se usan como bits de paridad. El algoritmo consta de tres pasos:

1) Aplicamos una permutación P a un bloque x de 64 bits y obtenemos una cadena x0 tal que:

x0 = P (x) = L0 R0 (2.1)

L0 contiene los primeros 32 bits de x0 y R0 los 32 bits restantes.

2) Se realizan 16 rondas de una determinada función. Calculamos Li y Ri, 1 <i <16 tales que:

Li = Ri-1

Ri = Li-1□f (Ri-1, Ki)  (2,2)

f es una función de dos variables: una a 32 bits correspondiente a Ri-1, y la otra de 48 bits que es la clave Ki. Ki se obtiene mediante la diversificación de la clave K de tamaño 56 bits.

3) La permutación inversa P-1 se aplica a R16L16 para obtener un bloque encriptado. El poder se encuentra en las 16 iteraciones donde el mensaje fuente será indetectable.

Durante mucho tiempo inviolable, el DES no resistió el aumento del poder de las computadoras. Aun cuando una clave de 56 bits ofrece una enorme cantidad de posibilidades, muchos procesadores pueden calcular millones de claves por segundo. Con lo que, cuando se utilizan al mismo tiempo una gran cantidad de máquinas, es posible que se encuentre la clave correcta en poco tiempo.

TDES (Triple DES), es una alternativa para DES. El algoritmo consiste en que se encadenen tres cifrados DES mediante dos claves de 56 bits, esto equivale a una clave de 112 bits.

□ El algoritmo AES

Rijndael es el cifrado de bloques que utiliza el estándar AES elegido por el NIST en 2001 para reemplazar DES. Es una encriptación por bloques de codificación de 128 bits con claves de 128, 192 o 256 bits.

- Principio de AES

Se basa en 'red de sustitución-permutación'. Se compone de una serie de operaciones vinculadas, algunas de las cuales implican reemplazar las entradas por salidas específicas (sustituciones) y otras implican mezclar bits (permutaciones).

Las entradas y salidas AES constan de secuencias de 128 bits. Cualquier flujo de bytes está organizado en una matriz que constará de 4 filas y un número de columnas variable dependiendo del tamaño del flujo. El número de rondas en AES es variable y depende de la longitud de la clave. AES utiliza 10 rondas para claves de 128 bits, 12 rondas para claves de 192 bits y 14 rondas para claves de 256 bits. Cada una de estas rondas usa una clave redonda diferente de 128 bits, que se calcula a partir de la clave AES original.

Proceso de encriptación

A continuación, se presenta la descripción de una ronda típica de encriptación AES. Cada ronda se compone de cuatro subprocesos. El primer proceso de ronda es la Sustitución de bytes. Los 16 bytes de entrada se sustituyen utilizando una tabla fija dada en el diseño. El resultado está en una matriz de cuatro filas y cuatro columnas. Después se corren las filas; cada una de las cuatro filas de la matriz se desplaza hacia la izquierda. Las entradas que se "caen" se vuelven a insertar en el lado derecho de la fila. Shift se lleva a cabo de la siguiente manera: La primera fila no está cambiada. La segunda fila se desplaza una posición (byte) hacia la izquierda. La tercera fila se desplaza dos posiciones hacia la izquierda. La cuarta fila se desplaza tres posiciones hacia la izquierda. El resultado es una nueva matriz que consta de los mismos 16 bytes, pero desplazados entre sí. El siguiente paso es mezclar las columnas; cada columna de cuatro bytes ahora se transforma usando una función matemática especial. Esta función toma como entrada los cuatro bytes de una columna y emite cuatro bytes completamente nuevos, que reemplazan la columna original. El resultado es otra matriz nueva que consta de 16 nuevos bytes. Cabe señalar que este paso no se realiza en la

última ronda. Finalmente se hace una operación lógica XOR con los 16 bytes de la matriz y la clave de 128 bits. Si esta es la última ronda, la salida es el texto cifrado. De lo contrario, los 128 bits resultantes se interpretan como 16 bytes y comenzamos otra ronda similar.

Proceso de descifrado

El proceso de descifrado de un texto cifrado AES es similar al proceso de cifrado en el orden inverso. Cada ronda consta de los cuatro procesos realizados en el orden inverso.

Ventajas del cifrado simétrico:

- Garantiza la confidencialidad de los datos.
- Algoritmo de cifrado de alto rendimiento.
- Más utilizado para la transmisión de mensajes largos.
- Las claves son relativamente pequeñas.

Desventajas del cifrado simétrico:

- Problema de distribución de claves: es necesario encontrar un canal perfectamente seguro para transmitir la clave.
- Problema de gestión de claves.

## 2.2 Criptografía asimétrica (clave pública)

En criptosistemas asimétricos (clave pública), el conocimiento de la clave Ke (la clave para cifrado) no permite deducir el de Kd (la clave de descifrado).

La clave Ke también se llama clave pública y la clave Kd se llama clave privada. En la mayoría de las implementaciones, el cifrado de clave pública se usa para asegurar y

distribuir claves, que se usan con algoritmos simétricos. Las ventajas y las desventajas de la encriptación asimétrica son:

Ventajas:

- La distribución de claves se simplifica:
- La clave privada nunca se revela o es transmitida y la clave pública está disponible para todos los usuarios.
- Certificación de claves públicas por firma digital.
- El par de claves privadas / públicas permanece sin cambios durante mucho tiempo.
- El número de claves distribuidas en una gran red es pequeño en comparación con el de una criptografía de clave simétrica.

Desventajas:

 Visiblemente más lento que algoritmos simétricos.

 Es necesario de que la clave pública utilizada es la de la persona a quien deseamos enviar información encriptada.

 El tamaño de las teclas es mucho más importante que las claves simétricas.

Criptografía de clave pública.

El algoritmo RSA fue inventado por Rivest Shamir y Adleman en 1977. Este algoritmo es una encriptación que utiliza una clave pública (o encriptación asimétrica). Los

usuarios de este algoritmo deben tener dos claves una privada y una pública. Entre los puntos fuertes del RSA está la dificultad de factorizar grandes números. Las claves públicas y privadas son funciones de un número primo muy grande de 100 y 200 dígitos.

Creación de claves.

Para formar las claves, es necesario elegir dos números primos p y q diferentes, donde n es el módulo de cifrado tal que $n = p \times q$. Luego se calcula el siguiente indicador con la función de Euler: $\varphi(n) = (p-1)(q-1)$, posteriormente se elige y que es un entero primo, llamado el exponente de cifrado de manera que: $p, q < e < \varphi(n)$. Se determina d tal que $(d \times e \bmod (\varphi(n))) = 1$ y $p, q < d < \varphi(n)$.

Luego formamos las dos claves: la clave privada (n, d) y la clave pública (n, e)

RSA establece que, si el tamaño de las teclas es mayor que 2048, el algoritmo se considera irrompible.

Cifrado

Sea M un número entero menor que n, que denota el mensaje a encriptar, el mensaje cifrado C tendrá la forma: $C = Me \bmod (n)$.

Descifrado

El descifrado es posible conociendo d, encontramos el mensaje claro aplicando la siguiente fórmula: $M = Cd \bmod (n)$.

## 2.3 Criptografía híbrida.

Los algoritmos de clave pública son muy lentos por lo que se propuso el cifrado híbrido que fusiona las características de los dos modos: simétrico y asimétrico. El proceso hibrido de cifrado se reduce a los cuatro pasos siguientes:

1) Bob envía su clave pública a Alice.

2) Alice genera una clave de sesión aleatoria, K, y la encripta usando la clave pública de Bob, y lo envía como la nueva clave será EB (K).

3) Bob descifra el mensaje de Alice usando su clave privada para restaurar la clave de sesión DB (EB (K)) = K.

4) Posteriormente encriptan sus mensajes usando esta clave de sesión.

El uso del cifrado de clave pública resuelve el problema de distribución de claves.

## 2.4 Criptoanálisis.

Es el estudio de la información encriptada para encontrar debilidades y descubrir el secreto y descifrar los textos encriptados. El descifrado es el arte de encontrar el mensaje original sin conocer la clave de cifrado.

Las técnicas de criptoanálisis se pueden resumir en cinco tipos de ataques:

- Ataque de fuerza bruta: el criptoanalista prueba todas las posibles combinaciones de claves hasta la adquisición del texto claro (mensaje original).
- Ataque de solo texto cifrado: el criptoanalista solo conoce el mensaje cifrado por el algoritmo e intenta deducir la clave o el texto claro.
- Ataque de texto claro conocido: el criptoanalista tiene el texto o partes del texto sin formato y su correspondencia encriptada.

- El ataque de texto plano seleccionado (ataque de texto plano elegido): el criptoanalista puede elegir el texto sin formato, y puede producir la versión encriptada de este texto (tiene acceso a la máquina para encriptar) con el algoritmo considerado como una caja negra. Las técnicas de la encriptación asimétrica son particularmente sensibles a este tipo de ataque.
- Ataque de texto cifrado elegido: el criptoanalista tiene el texto encriptado y puede obtener el texto plano asociado.

Para verificar la seguridad de un criptosistema es indispensable analizar algunos elementos. Se han diseñado algoritmos criptoanalíticos que implementan los ataques mencionados.

En lo que sigue, detallaremos algunas nociones esenciales para medir el nivel de seguridad de un criptosistema.

Criptoanálisis lineal

Para romper el algoritmo DES, Mitsuri Matsui diseñó en 1993 esta técnica de criptoanálisis lineal Este algoritmo es un conocido ataque de texto claro. Su principio se basa en aprovechar las altas probabilidades de ocurrencias de expresiones lineales derivadas de texto plano y texto cifrado. Estas expresiones lineales se construyen a partir de una aproximación lineal del algoritmo para encriptar. La vulnerabilidad de DES se encuentra en una cierta característica lineal de su S-Box (tabla de sustitución) que debería ser no lineal. Todo algoritmo de cifrado debe resistir este ataque.

Criptoanálisis diferencial

El criptoanálisis diferencial fue ideado por Biham y Shamir en 1993. Es un ataque de texto claro elegido. El atacante debe tener extractos de texto encriptado de

un texto claro. Estudia el efecto de las diferencias entre los textos de entrada sobre las diferencias en sus salidas donde busca diferencias constantes.

Criptoanálisis algebraico

La mayoría de los algoritmos de encriptación modernos están diseñados para que sean resistentes a ataques clásicos (lineales y diferenciales).

Courtois y Pieprzyk han estudiado la seguridad de estos algoritmos evocando otra hipótesis: el sistema puede escribirse en forma de ecuaciones algebraicas. Resolvieron el AES que contiene 23 ecuaciones cuadráticas linealmente independientes que pueden ser resueltas usando su nuevo algoritmo de criptoanálisis "XSL".

# Capítulo 3. Caos

La teoría del caos es una de las ciencias más recientes y se ha convertido en una de las más utilizadas en la investigación contemporánea.

Durante años, el caos se consideró incontrolable e incluso inutilizable, a pesar de la demostración del determinismo en aspectos de apariencia aleatoria.

La teoría del caos estudia los de sistemas dinámicos no lineales complejos o sistemas complejos que se expresan por recurrencias y algoritmos matemáticos y que son dinámicos no constantes y no periódicos. Incluye el estudio del comportamiento inestable no periódico y sistemas dinámicos no lineales deterministas aleatorios. En todas las definiciones que pueden existir para el caos, un fenómeno fundamental es indispensable: la sensibilidad a condiciones iniciales.

De hecho, programando su computadora y cambiando mínimamente las condiciones iniciales de sus ecuaciones de pronóstico del tiempo, Edward Lorenz descubrió que, para cierto sistema de ecuaciones no lineales, los resultados muestran una gran sensibilidad a las condiciones iniciales.

Podemos decir que esta anécdota es la base del caos determinista.

La teoría del caos influye en la explicación de varios fenómenos y encuentra su aplicación en varias áreas tales como:

 Economía: Predicción de ciclos económicos, movimientos comerciales y mercados financieros.

 Tiempo: pronóstico del tiempo.

 Salud: Predicción de ataques epilépticos.

 Ciencias sociales: comportamiento de los sistemas sociales.

 Cifrado de información.

## 3.1 Definición y propiedades de sistemas caóticos.

Se pueden dar varias definiciones para el caos. Caos en su sentido lingüístico es la confusión general de los elementos de la materia, antes de la creación del mundo. Otra definición considera el caos como un elemento de la dinámica no lineal determinista, en el que existe un espacio de estado o un espacio de fase que contiene cualquier estado posible del sistema y le corresponde una ley de evolución que describe su futuro cuando se tiene los estados del presente.

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

No linealidad. Son sistemas de ecuaciones diferenciales (tiempo continuo) o en diferencias (tiempo discreto) no lineales, que no cumple con el principio de superposición.

Sensibilidad exponencial a condiciones iniciales y parámetros de control. La dinámica o trayectoria es altamente modificada si se varía ligeramente una condición inicial o parámetro de control.  Por ejemplo, al truncar algunos números de condiciones iniciales de su sistema de pronóstico del tiempo, Lorenz destacó la naturaleza más importante de un sistema caótico, que es la sensibilidad a las condiciones iniciales, ya que los

pronósticos del tiempo varían fuertemente.  Hacia el final del siglo XIX, Poincaré mostró que las tres órbitas de 3 cuerpos se mueven bajo una fuerza central debido a la gravedad cambian drásticamente con una pequeña modificación de las condiciones iniciales.

Mezcla de datos. Un pequeño rango de condiciones iniciales cubre la mayor parte del espectro caótico.

Ergodicidad. La trayectoria caótica se mantiene confinada en un espacio conocido como atractor extraño con respecto al tiempo cubriendo en su totalidad su espacio para cualquier entrada.

Exponente de Lyapunov positivo. Un sistema de dimensión N posee N exponentes de Lyapunov; si uno de ellos es positivo, el sistema es caótico; si dos o más son positivos, el sistema es hipercaótico.

Existen varios sistemas caóticos que se usan para generar señales caóticas. En esta sección, presentaremos dos clases: sistemas caóticos continuos y sistemas caóticos de tiempo discreto.

## 3.2 Sistemas caóticos continuos

El sistema de Lorenz tiene un comportamiento dinámico descrito por las siguientes ecuaciones diferenciales no lineales:

$dx / dt = \sigma(y-x)$,

$dy / dt = \rho x - y - xz$

$dz / dt = xy - \beta z$

donde x, y y z son los estados del sistema, x0, y0 y z0 son las condiciones iniciales, σ, ρ y β son los parámetros de control y t es el tiempo. La figura 3.1 muestra el atractor extraño generado por del sistema de Lorenz proyectado en el plano xyz. Con σ = 10, β = 8/3  ρ = 28.

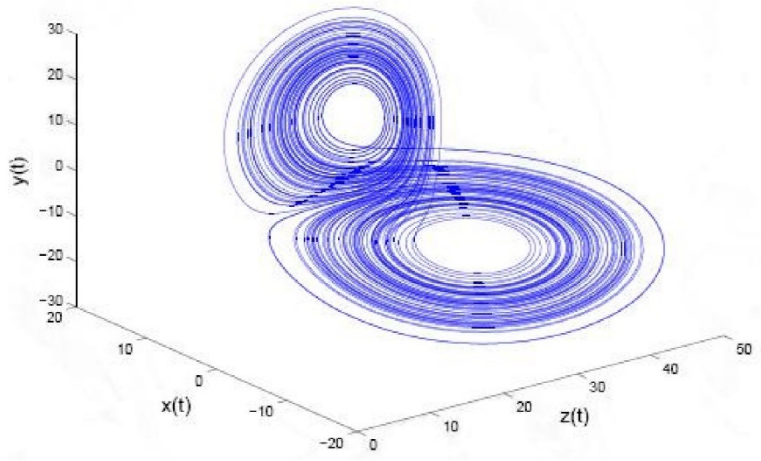



Figura 3.1 Atractor de Lorenz

El sistema de Chen está determinado por las ecuaciones siguientes:

x/dt = a(y-x)

y/dt = (c-a)x – xz + cy

z/dt = xy – bz

Donde x, y, z son las variables del sistema, y los parámetros son a, b y c. En la figura 3.2 se muestra el atractor cuando a = 35, b = 3 y c = 28.

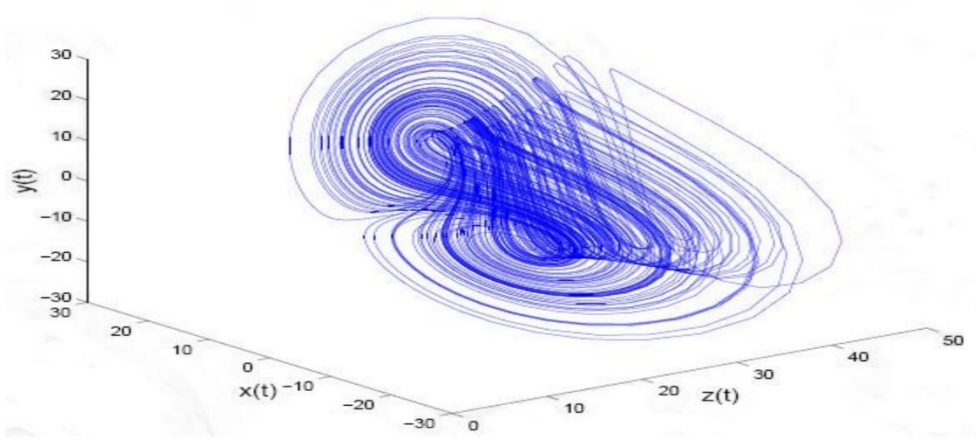



Figura 3.2 Atractor de Chen

Sistema de Rossler.

El sistema de Rossler, está determinado por las ecuaciones siguientes:

x/dt = - (y+z)

y/dt = x + ay

z/dt = (x - c) z + b.

Cuando a = 0.2, b = 0.2 y c = 5.7 se obtiene el atractor mostrado en la figura 3.3.

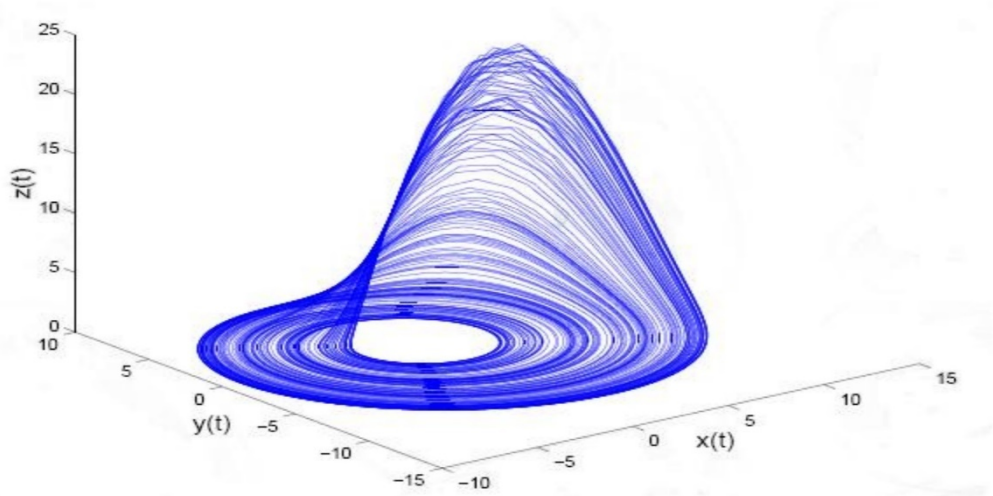


Figura 3.3 Atractor de Rossler

## 3.3 Sistemas caóticos discretos.

### Mapa Logístico 1D

Robert May estudio un modelo matemático no lineal en tiempo discreto, con el cual, explico la dinámica poblacional de especies animales. En su modelo, considero la población proporcional entre 0 y 1, donde 0 representa cero individuos y 1 el máximo número de individuos que pueden existir; para la estimación de la población en un instante de tiempo, considero la población en un instante de tiempo previo multiplicado por una constante a (que depende del clima, alimento, ambiente, etc.) y esto a su vez multiplicado por 1 menos la población en un instante previo (a mayor población, esta crece con más dificultad). El hecho de que el modelo generaba dinámicas complejas deterministas para ciertos valores de la constante, genero gran interés en la comunidad

científica y fue uno de los modelos matemáticos no lineales que fue base para estudios en la teoría de caos.

El mapa logístico unidimensional es conocido como el sistema no lineal más simple que existe y que exhibe claramente la ruta al caos, esta descrito por la siguiente ecuación en diferencias:

$$X_{n+1} = a\, X_n\, (1 - X_n)$$

donde $X \in (0,1)$ es el estado del mapa discreto, $X_0$ es la condición inicial con valores entre $0 < X_0 < 1$ y a es el parámetro de control, con $3.57 < a < 4$ el mapa genera secuencias caóticas. En la Figura 3.4 se muestra la bifurcación del crecimiento de la población, cuando se varía el parámetro a que demuestra la existencia de un sistema caótico.

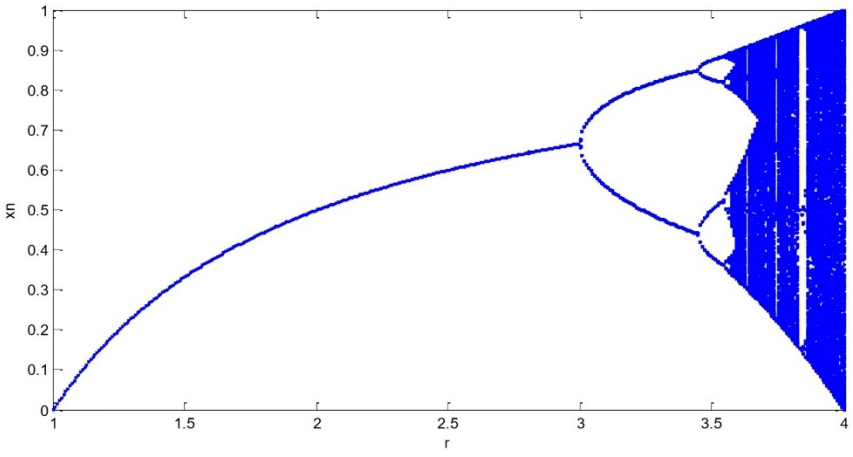



Figura 3.4 Diagrama de bifurcación.

Mapa de Hénon.

Constituye un sistema dinámico de tiempo discreto introducido por el astrónomo Michel Hénon en 1976. Lo determina el par de ecuaciones siguiente:

$X_{n+1} = Y_n + 1 - (X_n)^2$

$Y_{n+1} = b\, X_n$.

La Figura 3.5 muestra el atractor de Hénon con a = 1.4 y b = 0.3.

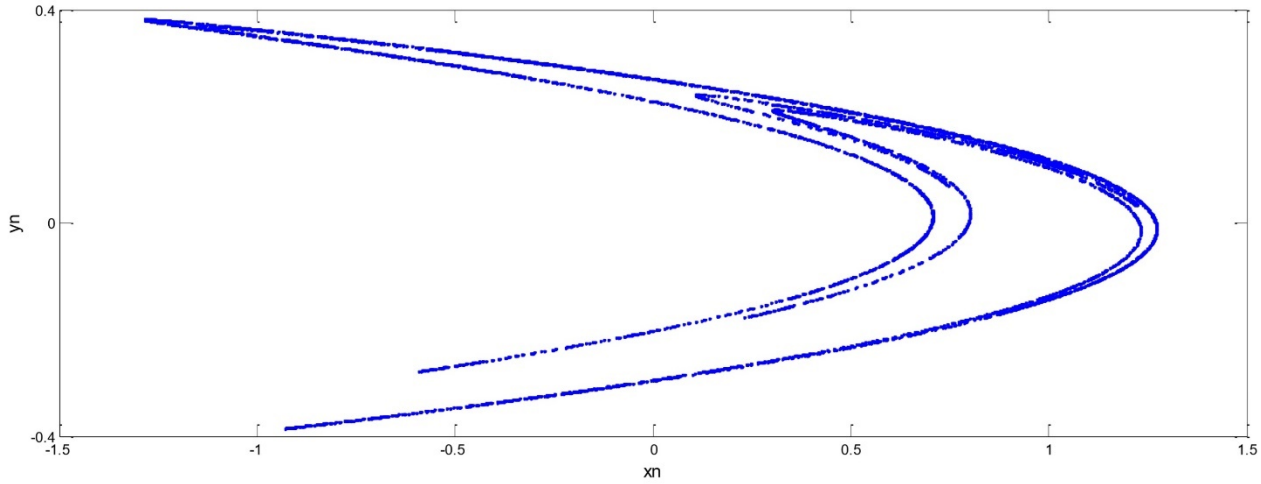



Figura 3.5 Mapa de Hénon.

## 3.4 Pruebas estadísticas.

Las pruebas del Instituto Nacional de Estándares y Tecnología (NIST) forman un paquete estadístico de pruebas que están diseñadas para detectar la aleatoriedad de las secuencias binarias de generadores de números aleatorios o pseudoaleatorios

utilizados en aplicaciones que requieren criptografía. La salida de los generadores de números pseudoaleatorios debe ser impredecible cuando no se conoce la entrada. Las pruebas NIST se enfocan en diferentes tipos de aspectos no aleatorios que se pueden encontrar en una secuencia y los comparan con una secuencia aleatoria. Algunas pruebas se pueden descomponer en un conjunto de subpruebas. El orden de aplicación de las pruebas es arbitrario. Sin embargo, la prueba de frecuencia debe aplicarse primero, ya que proporciona la evidencia más obvia del aspecto no aleatorio, que es la no uniformidad. Si la prueba no tiene éxito, la probabilidad de falla de las pruebas posteriores es alta. El resultado de cada prueba viene dado por un valor P que representa la probabilidad de que un generador de números aleatorios perfecto produzca una secuencia menos aleatoria que la secuencia ya probada. Esta variable tiene una distribución uniforme durante el intervalo [0 1]. P = 1: apariencia aleatoria perfecta. P= 0: apariencia no aleatoria. Una constante α se establece en el intervalo [0.001-0.01]. Se llama "nivel de significado". Si el P es mayor o igual que α, entonces la secuencia pasa la prueba o, de lo contrario, falla.  A continuación, se presentan las pruebas NIST.

Prueba estadística.

Se formula una prueba estadística para probar una hipótesis nula específica (H0). La hipótesis nula es que la secuencia probada es aleatoria. Una hipótesis alternativa (Ha) es que la secuencia no es aleatoria. Para cada prueba, se propone una decisión o conclusión para aceptar o rechazar la hipótesis nula. Se selecciona una estadística de

aleatoriedad apropiada y se utiliza para determinar la aceptación o el rechazo de la hipótesis nula. Una estadística tiene una distribución de valores posibles. Una distribución de referencia teórica se determina mediante métodos matemáticos. A partir de esta distribución de referencia, se determina un valor crítico. Durante la prueba, se calcula un valor estadístico de la prueba (en la secuencia probada). Si el valor excede el valor crítico, entonces la hipótesis nula para la aleatoriedad es rechazada. De lo contrario, la hipótesis nula es aceptada. En la práctica, la razón por la cual la hipótesis de la prueba estadística funciona es que la distribución de referencia y el valor crítico dependen y se generan con una suposición de apariencia aleatoria. Si se verifica la aleatoriedad, el valor de la prueba estadística calculada tendrá una baja probabilidad (0,01%) de exceder el valor crítico. La probabilidad de concluir que los datos no son aleatorios se fija antes de la prueba y se denota a.  Una secuencia puede parecer no aleatoria, incluso si es producida por un buen generador. Otra probabilidad β, es la probabilidad de que la prueba concluya que una secuencia es aleatoria cuando no lo es. La prueba estadística se usa para calcular un valor P. Cada valor P es la probabilidad de que un generador de números aleatorios perfecto produzca una secuencia menos aleatoria que la secuencia probada. Un valor P igual a 1 significa que la secuencia es perfectamente aleatoria. Un valor P de 0 significa que la secuencia no es aleatoria. Si el valor $P \geq \alpha$, entonces se acepta la hipótesis nula (es decir, la secuencia parece aleatoria). Si $P < \alpha$, entonces la hipótesis nula es rechazada (es decir, la secuencia aparece no aleatoria). El nivel de significancia α se puede elegir para las pruebas. Normalmente se selecciona en el rango [0.001, 0.01]. α igual a 0.001 indica que una secuencia de 1000 es rechazada por la prueba si la secuencia no es

aleatoria. Para un valor P ≥ 0.001, la secuencia puede considerarse aleatoria. Para un valor P <0.001, una secuencia puede considerarse no aleatoria. α = 0.01 indica que uno de cada 100 es rechazado. Un valor P ≥ 0.01 muestra que la secuencia es aleatoria.

Propiedades de una secuencia aleatoria probada

Se han implementado las siguientes hipótesis con respecto a la secuencia binaria aleatoria que se probará:

1- Uniformidad: la ocurrencia de un 0 o un 1 es igualmente probable, es decir, la probabilidad de cada que ocurra un 1 es exactamente 1/2. El número esperado de ceros o unos es n / 2, donde n es la longitud de la secuencia.

2- Extensibilidad: cualquier prueba aplicable a una secuencia también se puede aplicar a una subsecuencia extraída aleatoriamente. Si una secuencia es aleatoria, cualquier subsecuencia extraída debe ser aleatoria. Por lo tanto, cualquier subsecuencia debe pasar cualquier prueba de aleatoriedad.

## 3.5 El caos en la criptografía.

La teoría del caos describe el comportamiento de un sistema dinámico no lineal determinista, que depende en gran medida de las condiciones iniciales. Un pequeño cambio en las condiciones iniciales conduce a grandes cambios en la evolución del sistema. Los sistemas caóticos revelan un aspecto aleatorio: son deterministas, pero su resultado parece un comportamiento aleatorio al que desconoce sus parámetros. En

los sistemas caóticos, la secuencia caótica se genera con una condición inicial. La secuencia se usa como una clave. La misma secuencia se usa para descifrado. El transmisor y el receptor deben tener exactamente la misma secuencia. La sincronización es primordial. Hay dos enfoques para modelar un criptosistema por caos: analógico y digital. El primero se basa en la sincronización de dos sistemas caóticos diseñados para la seguridad de la información en un entorno ruidoso. El segundo es independiente de la sincronización.

### 3.6 Sistemas criptográficos caóticos análogos

Se basan en la sincronización de dos sistemas caóticos diseñados para la seguridad de la información en un entorno ruidoso. Dos sistemas caóticos se pueden sincronizar por acoplamiento o uno puede conducir al otro. Una señal escalar o más se envía de un sistema a otro, o también de una tercera fuente externa. Hay varios tipos de sincronización debido a las diferentes definiciones matemáticas de sincronización: sincronización completa, sincronización de fase, sincronización impulsiva, sincronización proyectiva, sincronización generalizada, sincronización de retardo.

Los criptosistemas analógicos se clasifican de acuerdo con en cuatro generaciones.

La primera generación.

La primera generación de sistemas analógicos caóticos apareció en 1993, incluyendo el enmascaramiento de caos aditivo y la manipulación de desplazamiento caótica.

a) Enmascaramiento aditivo.

Su principio consiste en hacer una adición simple entre la señal de salida del transmisor (generador de caos) y la señal de información para enmascararla. El

principal inconveniente es que, si la sincronización no es exacta o si hay ruido aditivo del canal, no se puede extraer de la información útil. Por lo tanto, la máscara aditiva es muy sensible al ruido del canal y a la diferencia entre los parámetros del sistema de transmisión caótico y el de recepción. La transmisión de información usando este método es entonces no segura.

CSK (Chaotic Shift Keying) Los sistemas de comunicación modernos son esencialmente digitales y los sistemas analógicos basados en el caos, como el enmascaramiento caótico y la modulación caótica parametrizada, se están abandonando a favor de sistemas caóticos basados en métodos Shift Keying. Uno de los primeros sistemas de comunicación caótica es el CSK, que es una modulación digital basada en la sincronización en el nivel del receptor. Un transmisor CSK conmuta entre dos generadores de caos que representan los bits 0 y 1. Solo las señales binarias pueden ser encriptadas por este método. El receptor decide, a través de la correlación entre la señal recibida y una señal de referencia síncrona, qué generador se ha utilizado y, por lo tanto, el mensaje transmitido. La complejidad del CSK radica en el rendimiento reducido de la BER. La manipulación de desplazamiento caótica es robusta contra el ruido y la variación de los parámetros del sistema de emisión - recepción.

La segunda generación se conoce como modulación caótica. Hay dos métodos para modular la señal, el primero es la modulación de los parámetros caóticos, el segundo es la modulación caótica no autónoma. La modulación de los parámetros caóticos consiste en modular uno o más parámetros del generador caótico mediante el mensaje

de información, de modo que sus trayectorias cambien en diferentes atractores. El mensaje m (t) se usa para modular los parámetros del sistema caótico. Por este método, es posible enviar varias señales de modo que cada modula un parámetro del transmisor caótico. En el nivel del receptor, la recuperación de los parámetros modulados se puede basar en la estimación simultánea de estado / parámetro a través de un controlador adaptable. Para la modulación caótica no autónoma, el transmisor alterna entre diferentes trayectorias del mismo atractor caótico. La señal de información se inyecta en un generador caótico que actúa como un transmisor, con el fin de perturbar el atractor en el espacio de fase. También hablamos de modulación caótica cuando se utilizan técnicas de espectro expandido, multiplicando el mensaje enviado por el operador caótico.

La tercera generación

La tercera generación es la combinación de criptografía clásica y sincronización caótica. Este sistema de seguridad no está roto todavía. La clave de encriptación es generada por el sistema caótico y se utiliza para encriptar la información, el mensaje generado y(t) se reintroduce en el sistema de transmisión caótico, la dinámica caótica cambia continuamente. Luego, una señal de la función s(t) de las variables de estado del transmisor se transmite al receptor a través del canal público. Un espía que no conoce la clave secreta no puede extraer el mensaje p (t) de la señal transmitida. La señal recibida se usa para sincronizar entre el receptor y el transmisor. Se usa la sincronización adaptativa. La clave luego es reconstruida por el receptor, que finalmente puede decodificar el mensaje.

La cuarta generación.

La sincronización en las primeras 3 generaciones es continua. En esta sincronización, el ancho de banda de la señal de sincronización es comparable a la señal de información; lo que disminuye la eficiencia del uso del ancho de banda. Para la cuarta generación, se utiliza una nueva tecnología, llamada sincronización de impulso. Se basa en la introducción de un operador Dirac. El problema se convierte en un problema de estabilidad de un sistema de pulso. Este método es mucho más robusto para la compensación de parámetros que las otras tres generaciones.

Ventajas y desventajas del caos análogo

La ventaja de este caos analógico es cifrar y difundir el espectro de la señal al mismo tiempo y, por lo tanto, minimizar las herramientas utilizadas para realizar estas funciones. Además, es difícil aplicar la tecnología de aleatorización a una señal de propagación. Sin embargo, para implementar sistemas de comunicación prácticos asegurados por el caos, adolece de varios problemas:

Dificultad para determinar el tiempo de sincronización.

Problema de no linealidad del canal.

Dificultad para diferenciar entre señales pequeñas y ruido de transmisión. Los ruidos de sincronización deben ser más bajos que la señal. Si la relación señal / ruido es menor que el ruido del canal, las señales recuperadas no tendrán ningún significado.

Para establecer la comunicación, se necesitan al menos dos sistemas analógicos caóticos idénticos en dos ubicaciones remotas. Tales sistemas son difíciles de obtener por la divergencia tecnológica de los sistemas analógicos y la influencia de la variación de la temperatura del medio, además de los errores inevitables en los valores de los componentes del circuito de hardware que varían con el tiempo. Se prevé una solución

en este caso, que consiste en utilizar la sincronización adaptativa. Con base en las fallas ya mencionadas, criptoanálisis de algunos criptosistemas analógicos han roto la seguridad. Errores ineludibles en los valores de los componentes y la redundancia de la señal reducen el espacio clave y facilitan los ataques de texto claro.

## 3.7 Criptosistemas caóticos digitales

Los criptosistemas caóticos digitales están diseñados para computadoras digitales donde se implementan una o más secuencias caóticas. Se pueden clasificar en dos categorías principales: cifrado de flujo caótico y cifrado de bloques caótico.

### Cifrado de flujo caótico.

En el caso general, el mensaje se cifra bit a bit, utilizando un XOR aplicado a la salida de un generador de números pseudoaleatorio basado en una secuencia caótica. En comparación con los generadores de números pseudoaleatorios ordinarios, el caos es más simple y menos costoso de integrar. La salida del generador caótico es la clave del flujo que se utiliza para ocultar el mensaje mediante la aplicación de XOR. Otro caso es el cifrado de flujo utilizando el enfoque de sistema inverso. El cifrado se basa en la retroalimentación de texto cifrados anteriores.

### Cifrado caótico por bloques.

Los datos se cifran por bloque. La longitud del bloque depende del algoritmo utilizado.

Las propiedades de la transformación caótica y cómo implementarlo determinan el nivel de seguridad de dicho algoritmo. Varios algoritmos de cifrado de bloques caóticos propuestos en la bibliografía se basan en la estructura de Feistel. Las secuencias caóticas se usan luego para generar los flujos de claves o las tablas de sustitución (S-Box).

Aunque los algoritmos numéricos caóticos propuestos en la literatura no dependen de la sincronización y sus claves se basan esencialmente en las condiciones iniciales y los parámetros de control de las recurrencias caóticas, tienen ciertos defectos. De hecho, los atractores caóticos de algunos generadores caóticos contienen secuencias caóticas que muestran ventanas periódicas que no son adecuadas para la elección de parámetros y, por lo tanto, constituyen claves no robustas. Los sistemas caóticos funcionan en el mundo real; la transformación de enteros reales es necesaria. Este proceso conduce a una degradación del comportamiento caótico del generador y a un tiempo demasiado largo durante la ejecución.

# Capitulo 4. Esquema de conectividad multiusuario seguro.

El objetivo principal del sistema de comunicación propuesto en este documento es mantener la privacidad de la información médica del paciente, así como el acceso esta información en una ubicación remota por parte del médico autorizado en una red multiusuario. Las redes inalámbricas instaladas en el área médica que utilizan señales biomédicas tienen una gran contribución para mejorar la vida de los pacientes y brindan una mayor comodidad. Esta tecnología permite el monitoreo remoto para pacientes crónicos, la reducción del tiempo en el hospital para el paciente, ya que la vigilancia se puede hacer de forma remota.

El avance en la tecnología de sensores, junto con los avances en la tecnología de la información, exige seguridad en el manejo de la información (medicina segura). La gestión de estas nuevas tecnologías hace posible tener sensores en diferentes lugares para medir de forma remota las señales biomédicas inalámbricas, que se utilizan en muchas áreas [28]. Los esquemas de comunicación aplicados a la telemedicina usan Internet para la comunicación remota para pacientes y médicos. La privacidad de la información médica del paciente es de suma importancia.

En la técnica CDMA, varios transmisores comparten ancho de banda y envían información simultáneamente a través de un solo canal. Esta técnica utiliza la conversión de analógico a digital (ADC), tecnología de espectro ensanchado (SST) y una técnica de modulación digital, entre otras Bynary Phase Shift Keying (BPSK).

Primero, el mensaje original (entrada) se digitaliza. Luego, la frecuencia de la señal transmitida cambia de acuerdo con un patrón de código definido. Finalmente, solo los receptores cuya respuesta de frecuencia está programada con el mismo código pueden recuperar dicho mensaje simple. Los patrones de código definidos con sistemas caóticos hacen que el esquema propuesto sea robusto frente a ataques exhaustivos, ya que existen millones de códigos posibles.

Este trabajo propone un proceso para cifrar señales biomédicas de varios pacientes que envían información a diferentes médicos utilizando el mismo canal de comunicación. Para lograr compartir el canal y que los criptogramas no se corrompan por el ruido aditivo del canal, o por la interferencia de los otros usuarios, se propone un sistema de cifrado basado en los principios de CDMA, pero combinados con el uso de generadores caóticos. Esto resuelve el problema del uso de un solo canal de comunicación donde los criptogramas basados en la adición de la información con una señal caótica, se corrompen unos a otros al viajar por el canal, pues hay interferencia aditiva, por lo que resulta imposible descifrar la información original.

El esquema general para transmitir información médica se presenta en la Figura 4.1.

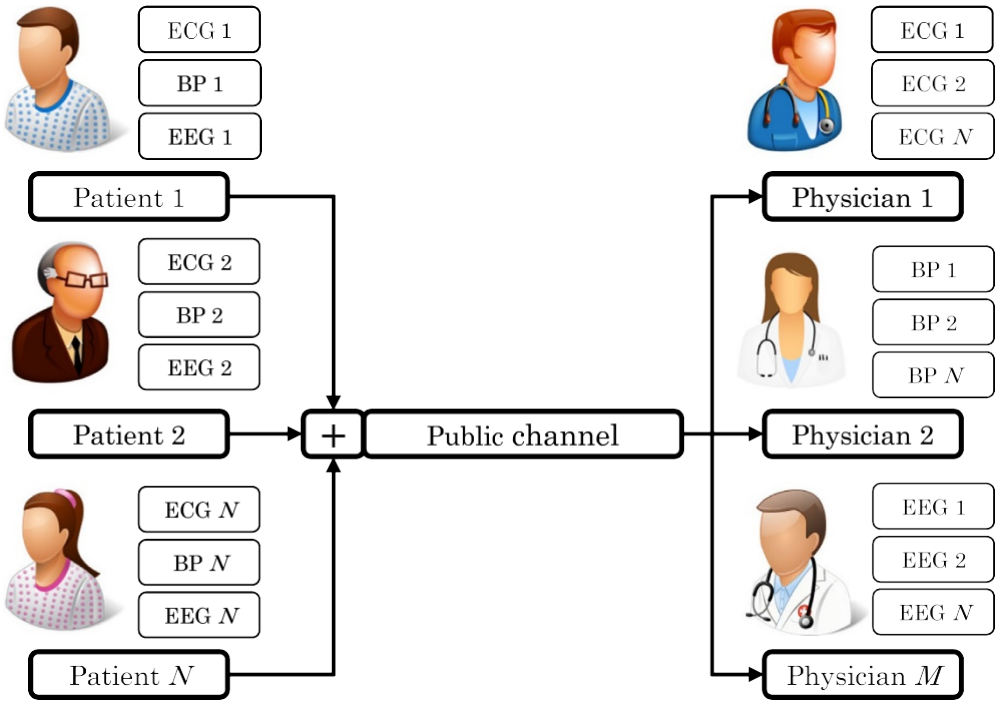



Figura 4. 1 Esquema propuesto para trasmisión segura de señales biomédicas.

El esquema consiste en N pacientes, que pueden tener varias condiciones médicas que deben ser monitoreadas por diferentes médicos especialistas. La información viaja a través de un canal público, en el que la información de los N pacientes puede enviarse simultáneamente en un canal de comunicación. En el otro lado del sistema de comunicación hay M especialistas que pueden atender a N pacientes.

Para proporcionar seguridad de la información, se propone un esquema de comunicación de red segura en la figura 4.2.

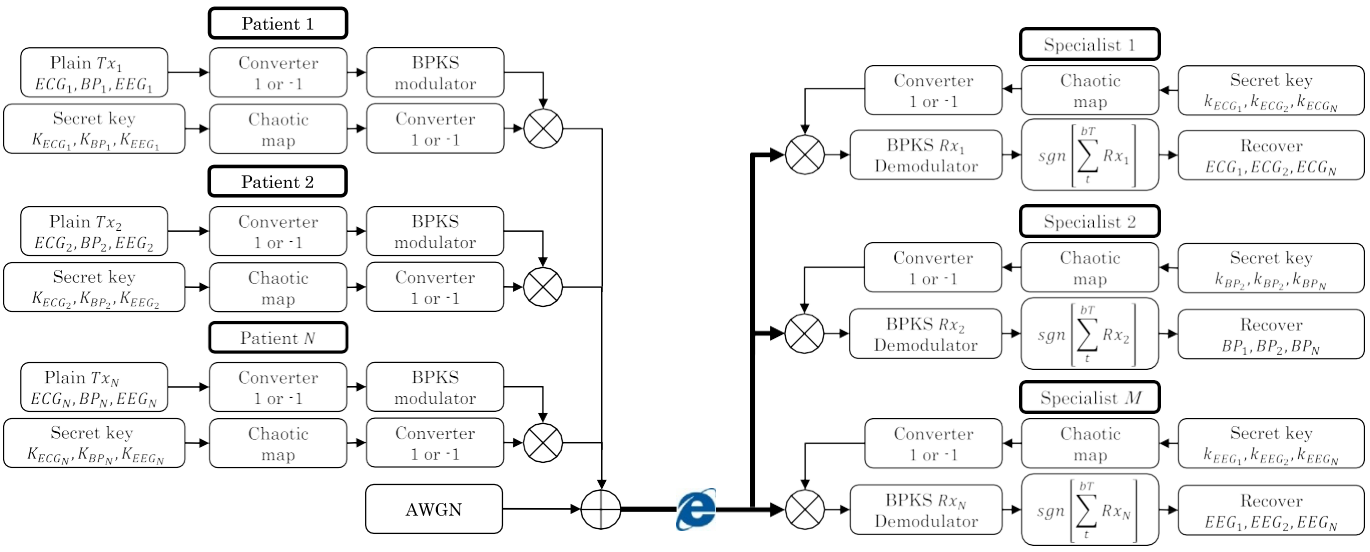



Figura 4.2 Diagrama a bloques del sistema propuesto.

Los pasos para el cifrado y la transmisión se describen a continuación:

1. El transmisor y el receptor comparten de forma segura la contraseña (clave secreta) en función de las condiciones iniciales y los parámetros de control del mapa caótico correspondiente. Cada usuario requiere una clave secreta para cada bioseñal.

2. Cada información analógica de los pacientes (señal simple) se adquiere mediante el uso de dispositivos sensores electrónicos, por ejemplo, medidor de presión arterial o un equipo de ECG portátil, que produzca la señal biomédica de un electrocardiograma. Una vez adquiridos, los datos de bioseñales de longitud L se digitalizan a 8 bits con frecuencia de muestreo Fs y se codifican en Non Return Zero (NRZ), e.i. 1 cuando el bit es "1" y -1 cuando el bit es "0".

Esta señal se define como P-NRZ binaria con longitud L × 8.

3. Una señal portadora para BPSK se genera en base a la señal del coseno con F Hz, amplitud A y C muestras por ciclo.

4. La señal P-NRZ se modula en BPSK. Se obtiene P-NRZ-BPSK, una señal de longitud L × 8 × C.

5. Se genera una señal caótica CS de longitud L × 8 × C con la clave secreta, donde cada valor caótico tiene una precisión decimal de 10-15 (por ejemplo, 1.123456789012345). Entonces, CS se amplifica 1000 veces con la operación del módulo 1 para mejorar la secuencia pseudoaleatoria (para aumentar la seguridad) como en [19] para producir ECS con la misma longitud que CS.

6. La señal caótica mejorada ECS se codificada a NRZ teniendo en cuenta la siguiente condición: Si ECS es mayor o igual a 0.5 entonces $ECS_{NRZ} = 1$, si es menor entonces $ECS_{NRZ} = -1$.

7. Las señales P-NRZ-BPSK y ECS-NRZ para cada bioseñal se multiplican para generar la señal de espectro ensanchado para todas las bioseñales del paciente requerido.

8. Todas las señales de espectro ensanchado de los N pacientes se suman y se combinan con el ruido gaussiano blanco aditivo (AWGN) para producir la señal cifrada transmitida TES sobre el canal compartido.

En el proceso de descifrado, cada M especialista puede recuperar las bioseñales específicas utilizando la clave secreta correspondiente y el mapa caótico. Los pasos para recuperar los bioseñales son:

1. La señal ECS-NRZ se genera, como el proceso de encriptación.

2. Se genera la misma señal portadora para BPSK, como el proceso de encriptación.

3. El ECS-NRZ de cada bioseñal correspondiente se multiplica con TES y se aplica la demodulación BPSK. El resultado es la señal DS demodulada con longitud L × 8 × C.

4. La señal sng es calculada para recuperar bioseñales, sng es la suma de todos los valores para cada "chip" de longitud C en DS. La señal de resultado sng es de longitud L × 8.

5. La siguiente condición se aplica para recuperar la bioseñal binaria: Si $sgn_j$ es mayor a 0 entonces $RBS_j = 1$, si es menor entonces $RBS_j = 0$.

donde RBS es la bioseñal binaria recuperada.

6. Finalmente, el bioseñal original se reconstruye haciendo la conversión digital analógica, segmentando el flujo a bloques de 8 bits.

Otros especialistas no podrán observar la información del paciente que no corresponda con sus especialidades, ni los intrusos pueden robar o dañar la información. De esta forma, se presenta un sistema de comunicación de red segura que puede monitorear la salud de diferentes pacientes con diferentes enfermedades y doctores con diferentes especialidades.

# Capítulo 5 Resultados.

Se han realizado simulaciones por computadora para implementar el esquema propuesto bajo el entorno MatLab R2014a en una computadora de escritorio con Intel (R) Xeon (R) CPU 2,16 GHz, 64 bits sistema operativo Windows 7 y RAM 16,0 GB. La aritmética doble punto flotante IEEE 754 se adopta para efectuar los cálculos de mapas caóticos y evitar la aparición de un ciclo de corto período y la degradación caótica. La eficacia de la encriptación se valida a través del análisis de claves, medidas estadísticas (BER, PSNR y MSE) y análisis de tiempo.

Tomando en consideración que la base de datos ATM de PhisioBank adquiere señales biológicas como electrocardiogramas (ECG) y señales de presión arterial (PA) con la misma frecuencia de muestreo, se han tomado los datos que en ella se proporcionan para efectuar la experimentación [29]. Las simulaciones se han realizado con el siguiente escenario: una red con 3 pacientes con diferentes sensores. El paciente 1 envía dos bioseñales (ECG1 y BP1), el paciente 2 envía una bioseña (ECG2) y el paciente 3 envía una bioseña (BP3). Todas las bioseñales tienen una duración de 10 s con una frecuencia de muestreo Fs = 100 Hz, que se describen de la siguiente manera (véase la Fig. 3):

1. Electrocardiograma (ECG1): registro "a05" de la base de datos "Apnea-ECG database (apnea-ecg)".

2. Presión sanguínea (BP1): registro "sshs07m" de la base de datos "Presión sanguínea en Dahl Rats (bpssrat)".

3. Electrocardiograma (ECG2): registro "b01" de la base de datos "Apnea-ECG database (apnea-ecg)".

4. Presión sanguínea (BP3): registro "ssbn13hs04" de la base de datos "Presión sanguínea en Dahl Rats (bpssrat)".

El esquema propuesto tiene flexibilidad sobre el mapa caótico que se implementará. Incluso cada paciente puede tener un mapa caótico particular, debido a que se han hecho simulaciones exitosas utilizando distintos mapas caóticos para generar las secuencias para realizar el cifrado. Los resultados que a continuación se presentan, se realizaron utilizando el mapa de Hénon [30]. Es un sistema dinámico bidimensional de tiempo discreto que toma un punto ($x_n$, $y_n$) en el plano y lo mapea a un nuevo punto de acuerdo con el siguiente conjunto de ecuaciones de diferencias:

$x_{n+1} = 1 – a(x_n)^2 + y_n$

$y_n + 1 = bx_n$

donde a y b son los dos parámetros de control y $x_0$ y y0 son las dos condiciones iniciales. La dinámica del mapa es caótica cuando a = 1.4, b = 0.3, $x_0 = 0$ e $y_0 = 0$.

## 5.1 Proceso de cifrado

El emisor y el receptor comparten las claves secretas asegurando que nadie más las conozca. Luego, las bioseñales que se muestran en la Figura 5.1 (valores en mV), se digitalizan a datos de 8 bits, como se muestra en la Figura 5.2 (se muestran los valores en decimal pero todos positivos).

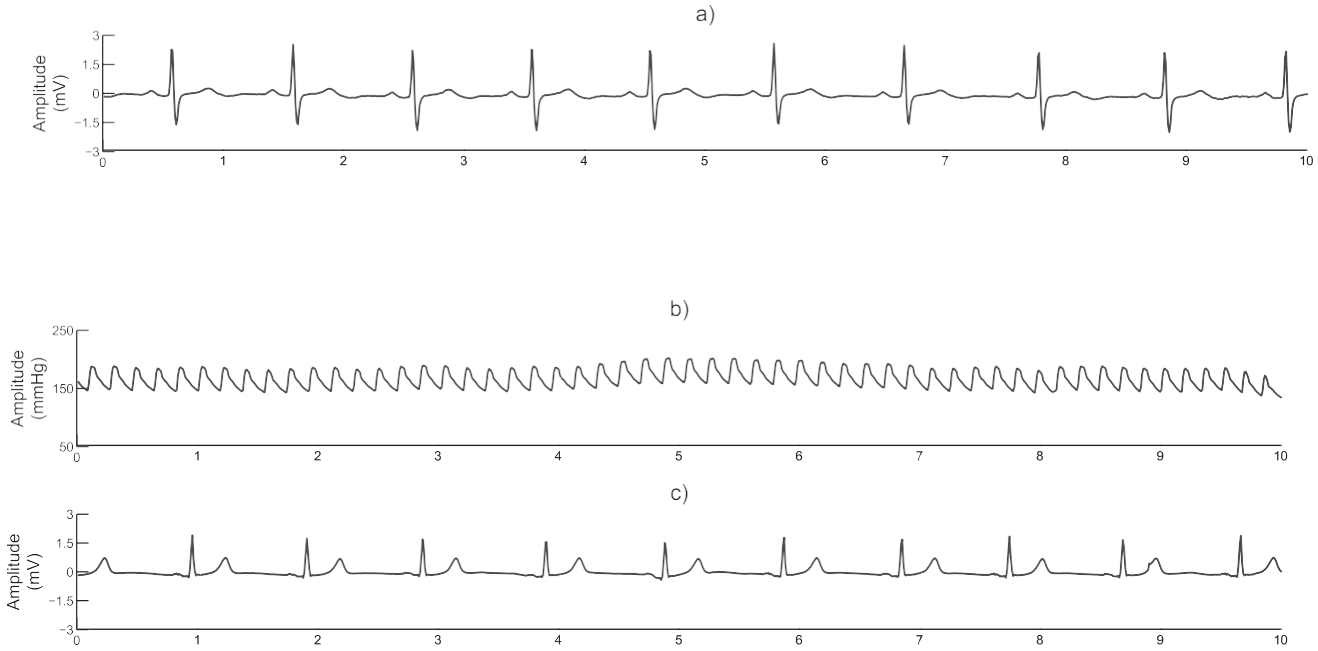
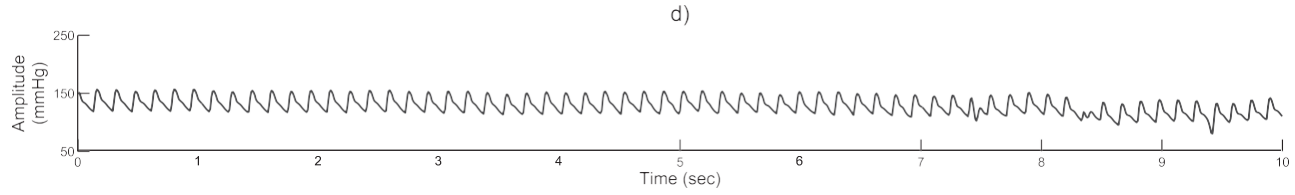



Figura 5.1 Señales biomédicas originales del PhysioBank ATM: (a) $ECG_1$, (b) $BP_1$, (c) $ECG_2$, and (d) $BP_3$.



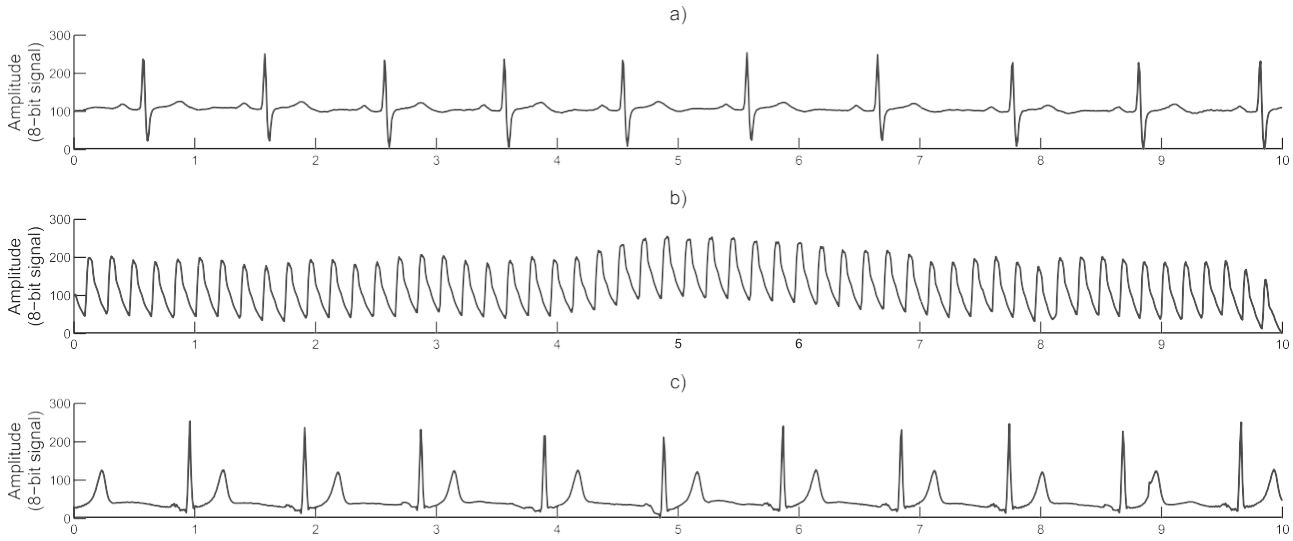
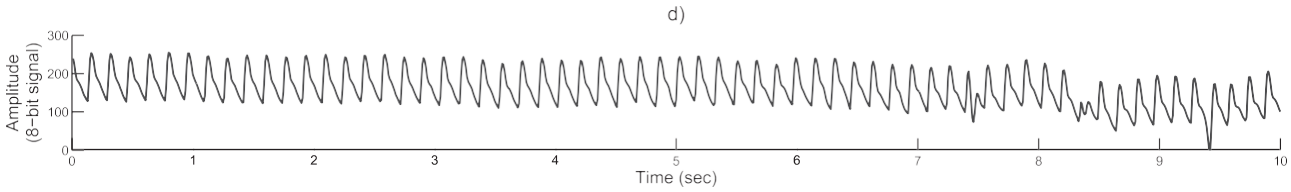



Figura 5.2 Bioseñales a 8 bits a) $ECG_1$, (b) $BP_1$, (c) $ECG_2$, and (d) $BP_3$.

Cada paciente y médico tendrá el mismo generador de caos (por ejemplo, el mapa de Hénon) con diferentes claves secretas (condiciones iniciales y parámetros de control del mapa caótico) para cada sensor de bioseñales en el paciente. Las claves secretas




utilizadas en la experimentación se describen en la Tabla 1, que se basan en las condiciones iniciales y los parámetros de control del mapa de Hénon para cada bioseñal de cada paciente.

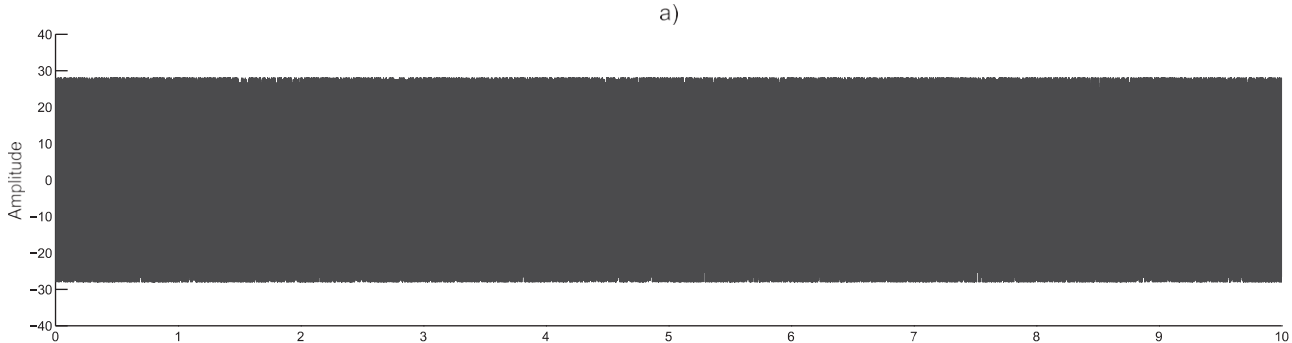
**Tabla 5.1**

Claves secretas del mapa de Hénon usado para el cifrado.

| | | $a$ | $b$ | $x_0$ | $y_0$ |
|---|---|---|---|---|---|
| Patient 1 | $K_{ECG_1}$ | 1.400123456789012 | 0.300123456789012 | 0.123456789012345 | 0.123456789012345 |
| | $K_{BP_1}$ | 1.400123456789013 | 0.300123456789013 | 0.123456789012346 | 0.123456789012346 |
| Patient 2 | $K_{ECG_2}$ | 1.400123456789014 | 0.300123456789014 | 0.123456789012347 | 0.123456789012347 |
| Patient 3 | $K_{BP_3}$ | 1.400123456789015 | 0.300123456789015 | 0.123456789012348 | 0.123456789012348 |

Para generar las codificaciones en BPSK de las señales P - NRZ se utiliza la función cosenoidal : w = 7 cos (3πt), con 50 muestras por ciclo. Los cuatro P - BPSK tienen una longitud de 400,000. Utilizando los mapas caóticos se generan 4 ECS-NRZ de longitud 400,000 usando las claves secretas de la Tabla 1. Las 4 señales de espectro expandido se generan por multiplicación de P - BPSK por ECS - NRZ. Finalmente, Todas las señales de especro expandido se suman y se le agrega el ruido gaussiano blanco aditivo (AWGN) para producir una señal equivalente a un criptograma compartido que se transmite a través de un único canal de comunicación.

En la Figura 5.3 se muestran en (a) la suma de las cuatro señales de espectro ensanchado (bioseñales encriptadas) se muestra con 10s. En (b) se muestra la señal transmitida con alto nivel de ruido.



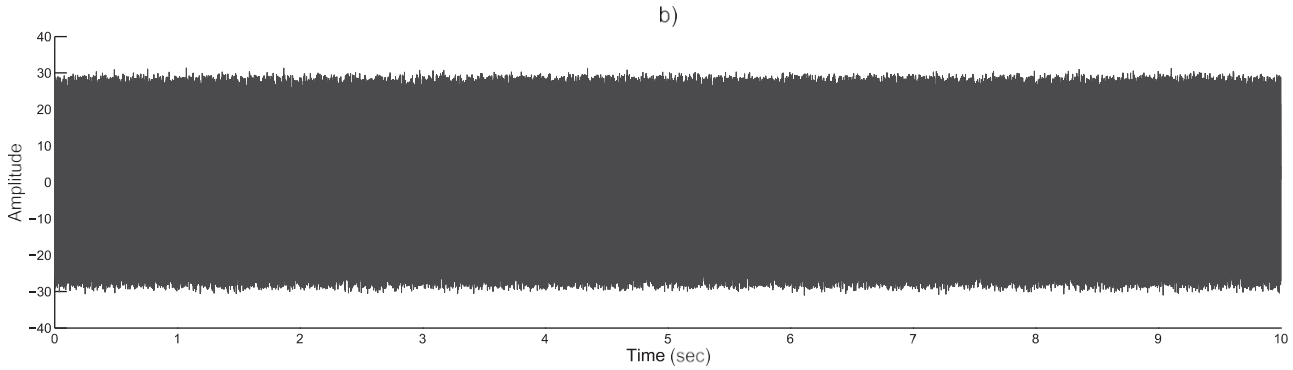
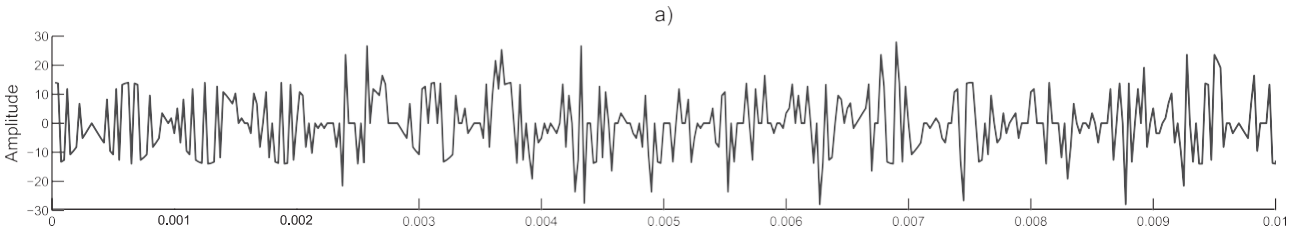



Figura 5.3

En la Figura 5.4 (a) y (b) presentan los primeros 10 milisegundos (ms) de señal encriptada sin ruido y la señal transmitida con ruido, respectivamente. En la Figura 5.4 (c) se muestra el ruido añadido a la señal encriptada, es decir, el error de la señal presentada en (a) y la presentada en (b). La señal transmitida es irreconocible visualmente para cualquier intruso o especialista incorrecto. Solo el especialista correcto con la clave secreta correspondiente puede recuperar las bioseñales requeridas.



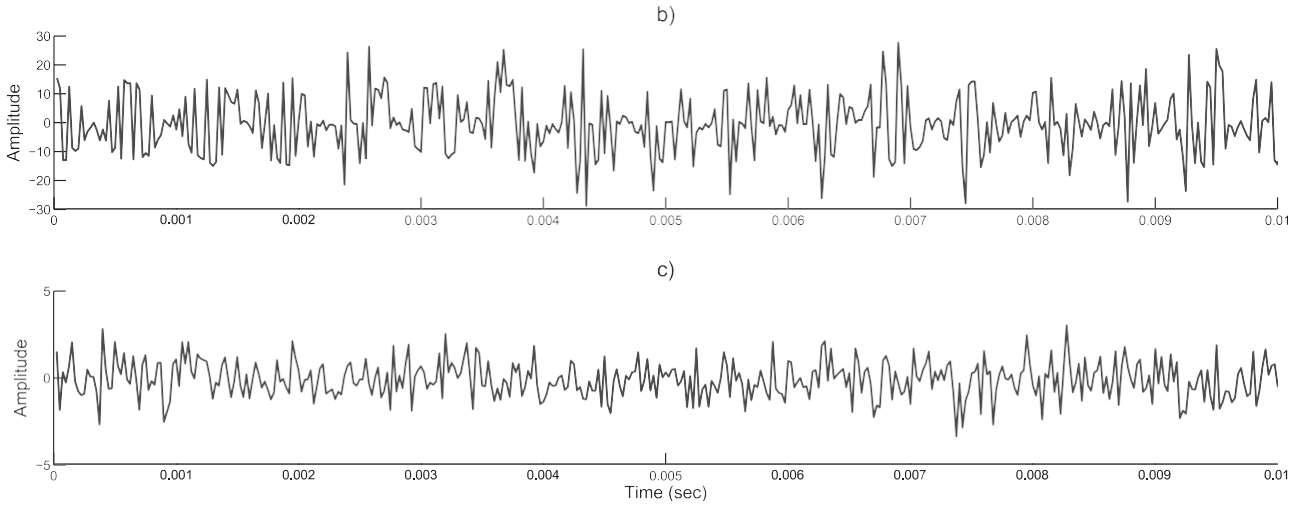



**Figura 5.4 Primeros 10 ms de la señales** (a) la suma de las bioseñales cifradas, (b) la suma de bioseñales mas ruido gausiano (señal transmitida) y (c) ruido agregado a la señal transmitida.

## 5.2 Proceso de descifrado

En el proceso de descifrado, el especialista correspondiente puede recuperar todas las bioseñales específicas solo si el mapa caótico y la clave secreta son los mismos del proceso de encriptación. En la Figura 5.5 la bioseñales de ECG1 del Paciente 1 y la bioseñal del BP3 del Paciente 3 son recuperadas correctamente por el especialista correspondiente. Sin embargo, la BP1 del paciente 1 y ECG2 del paciente 2 no se puede desencriptar con éxito, ya que las claves secretas correspondientes son incorrectas, como se puede ver en Tabla 2.

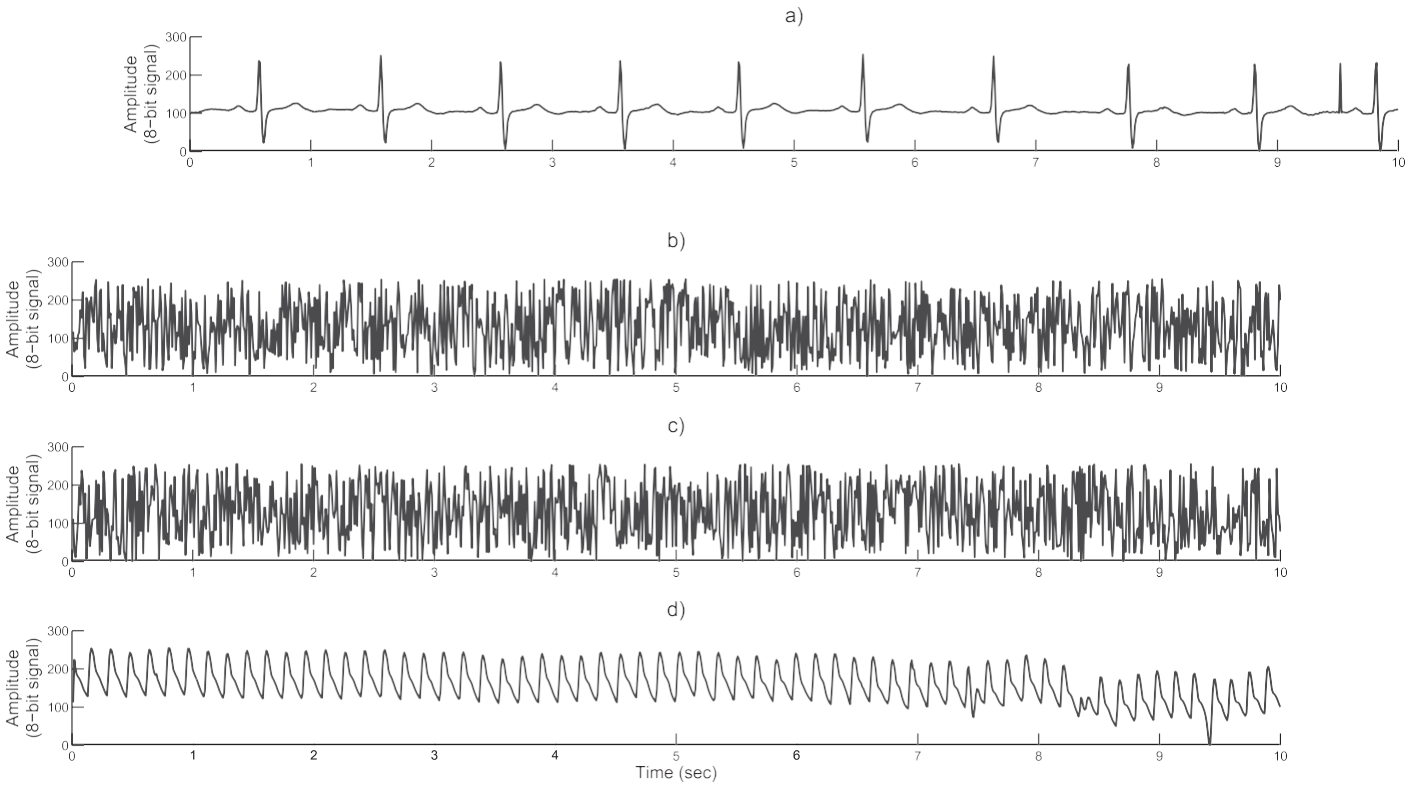



Figura 5.5 Señales a la salida del proceso de descifrado.

**Tabla 5.1**

Claves secretas del mapa de Hénon usado para el cifrado.

| | | $a$ | $b$ | $x_0$ | $y_0$ |
|---|---|---|---|---|---|
| Patient 1 | $K_{ECG_1}$ | 1.400123456789012 | 0.300123456789012 | 0.123456789012345 | 0.123456789012345 |
| | $K_{BP_1}$ | 1.400123456789013 | 0.300123456789014 | 0.123456789012346 | 0.123456789012346 |
| Patient 2 | $K_{ECG_2}$ | 1.400123456789015 | 0.300123456789014 | 0.123456789012347 | 0.123456789012347 |
| Patient 3 | $K_{BP_3}$ | 1.400123456789015 | 0.300123456789015 | 0.123456789012348 | 0.123456789012348 |

## 5.3 Análisis de calidad

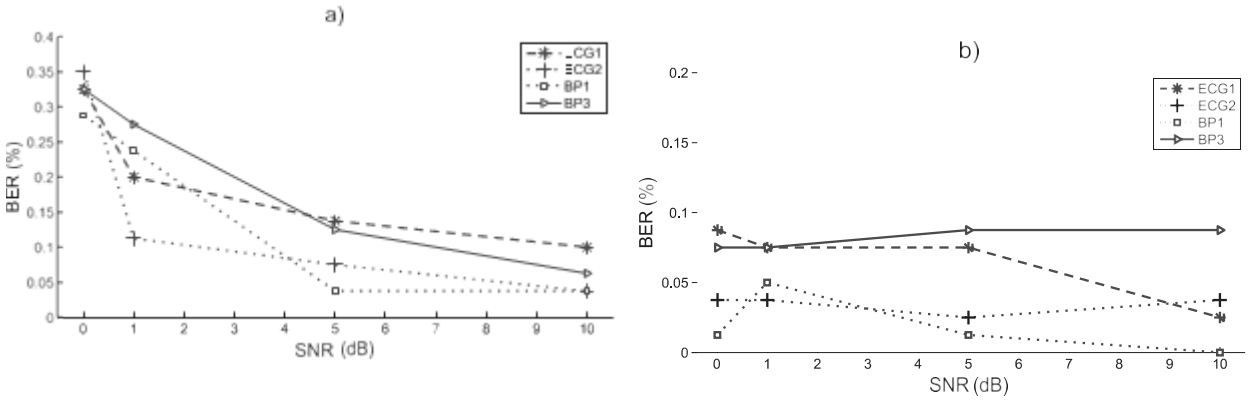
En esta subsección, la solidez frente al ruido y la calidad de las señales del esquema propuesto se presenta bajo varios escenarios utilizando niveles de energía por bit (Eb) de 1, 3, 5 y 7, y niveles de relación señal a ruido (SNR) de 0.01, 1, 5 y 10 que resultan

de agregar AWGN. Se calculan las métricas tales como la tasa de error de bit (BER), el error cuadrático medio (MSE) y la relación pico de señal a ruido (PSNR). Los resultados de la evaluación de calidad se determinan entre bioseñales simples (ECG1, BP1, ECG2, BP3) y las bioseñales recuperadas correspondientes.

Tasa de error de bit

En las comunicaciones digitales, la BER es el número de errores de bit dividido por el número total de bits transferidos durante algún intervalo de tiempo y se expresa como porcentaje. El número de errores de bit es la cantidad de bits de datos recuperados después de pasar a través del de canal de comunicación que han sido alterados por ruido, interferencia y errores de sincronización de bits.

En la simulación, las bioseñales simples y las bioseñales recuperadas se ordenan en un vector de 8000 bits. Los errores de bit se calculan y se obtiene el porcentaje. La Fig. 8 muestra los resultados de BER entre bioseñales simples y sus correspondientes bioseñales recuperadas (con la clave secreta correcta) en diferentes escenarios de AWNG y Eb.



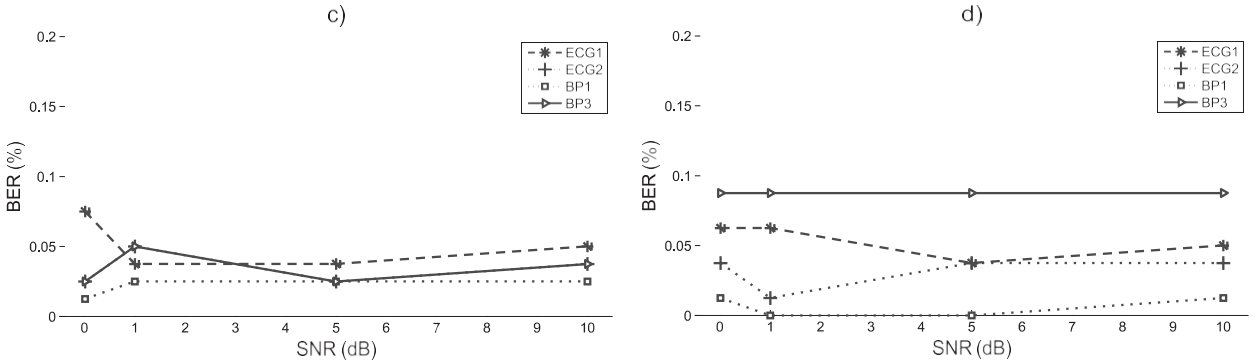



Figura 5.6 Resultados BER (a) Eb = 1, (b) Eb = 3, (c) Eb = 5, (d) Eb = 7.

El error máximo se presenta cuando SNR es 0.01 dB siendo el BER 0.35%; mientras más alto es el SNR, más bajo es el BER. A una SNR de 10 dB, los errores son mínimos. Si la SNR es mayor a 10 dB, tales errores permanecen constantes. Para los 8000 bits de cada bioseñal, el BER es muy pequeño con menos del 0.1% de bits perdidos cuando el Eb superior o igual a 3. Por lo tanto, el criptosistema propuesto es muy resistente al ruido.

Error cuadrático medio (MSE).

El MSE proporciona el error de reconstrucción con respecto al tamaño de la muestra. si ambas señales son iguales, entonces el MSE es cero. En la simulación, los datos de bioseñales originales y las bioseñales recuperadas se digitalizan a 8 bits, es decir, números enteros entre 0 y 255 con una longitud de 1000 datos. El MSE se muestra en la Figura 5.7 para diferentes niveles de Eb y SNR. El MSE de ECG1 es 30.49, 70.60, 17.01 y 16.74 para SNR 0.01, 1, 5 y 10, respectivamente. Cuando Eb es bajo, hay más bits perdidos en las señales recuperadas, pero cuando Eb es 3 o superior, el MSE es casi de 0. El MSE (con Eb de 3) de BP1 es 0.25, 1.02, 0 y 0 cuando el SNR es 0.01, 1,

5 y 10, respectivamente. En este sentido, el esquema propuesto es altamente resistente al ruido.

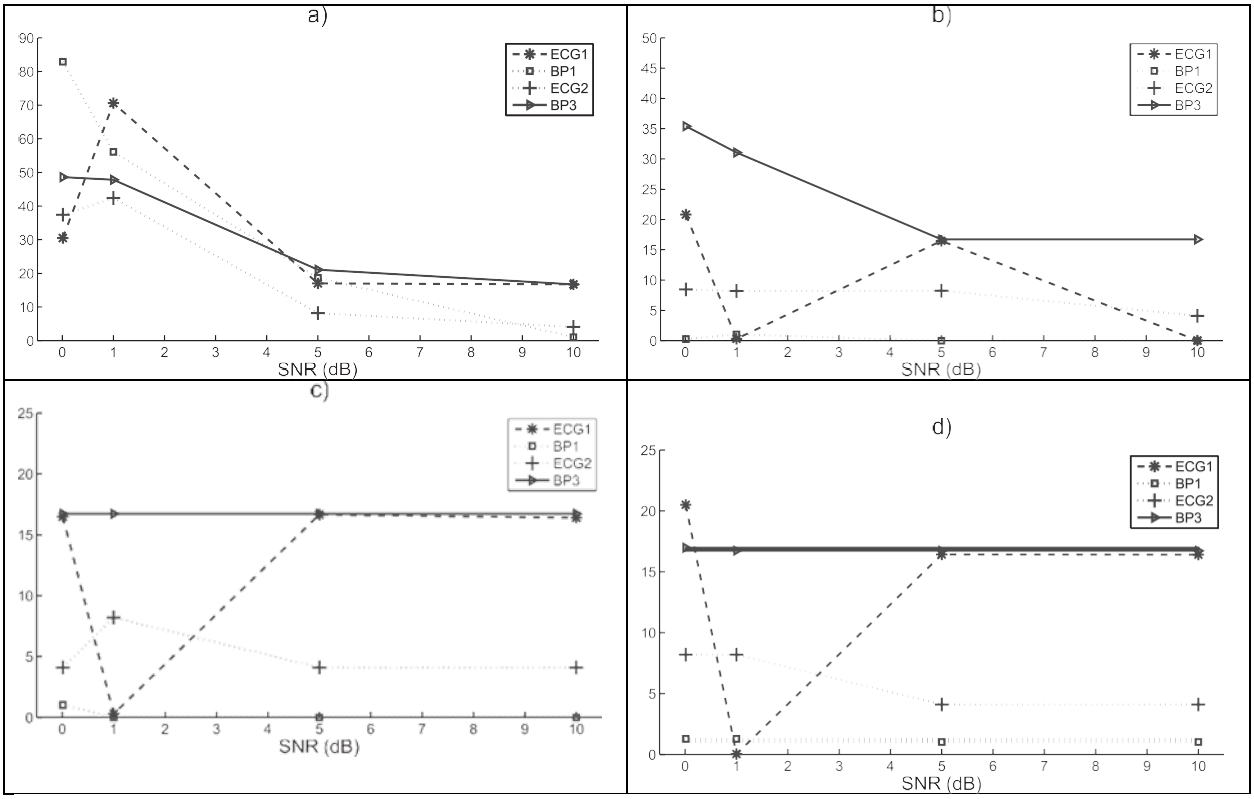



Figura 5.7 Resultados MSE: (a) MSE con Eb = 1, (b) MSE con Eb = 3, (c) MSE con Eb = 5, y (d) MSE con Eb = 7.

Relación Señal a Ruido Pico.

Determina la relación entre el valor máximo posible (potencia) de una señal y la potencia del ruido distorsionador que afecta la calidad de su representación. Se expresa en decibeles, se calcula con la siguiente formula:

$PSNR = 10 \log_{10} (255^2 / MSE)$.

Se expresa en decibeles. Se usa para calcular la relación pico señal a ruido entre dos señales, en este trabajo son los pares bioseñales originales y bioseñales recuperadas.

El PSNR es bajo cuando el MSE es muy alto, lo que significa que las señales son muy diferetes, en el caso contrario, si las señales son muy similares el MSE es muy bajo y por lo tanto el PSNR es muy alto. El PSNR entre bioseñales originales y bioseñales recuperadas se muestran en la Figura 5.8 para diferentes niveles de energía por bit y niveles de SNR. En los resultados de simulaciones, mientras mayor es el PSNR más alta es la similitud entre los señales originales y sus correspondientes señales recuperadas. Por ejemplo, para BP1 con Eb = 7, los resultados de PSNR son 17.05, 17.05, 18.02 y 18.02 dB cuando SNR 0.01, 1, 5 y 10 dB, respectivamente. Estos altos valores de PSNR indican que la señal simple BP1 y las correspondientes señales recuperadas se pueden recuperar con éxito después de aplicar diferentes niveles de distorsión sobre la señal transmitida encriptada TES.

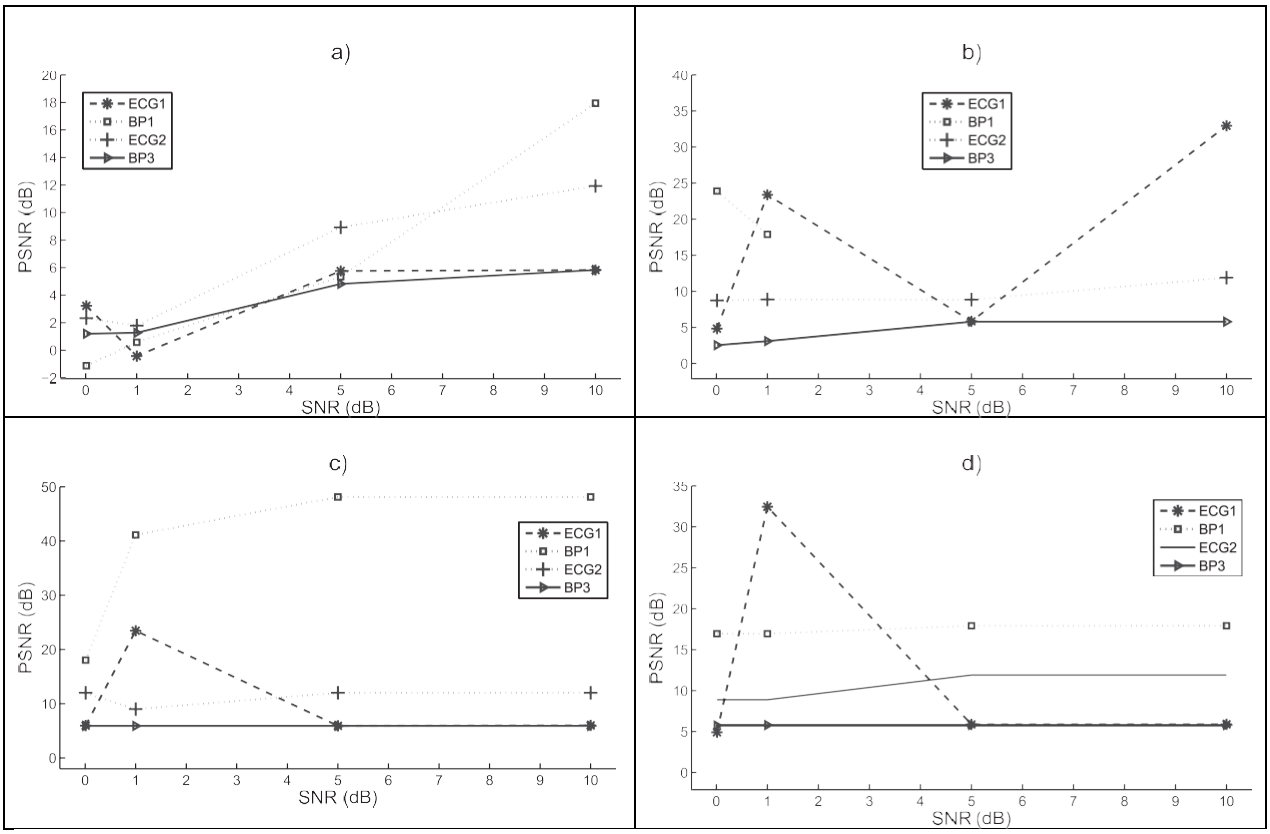


Figura 5.8 Resultados de PSNR: (a) PSNR con Eb = 1, (b) PSNR con Eb = 3, (c) PSNR con Eb = 5, y (d) PSNR con Eb = 7.

Análisis de las claves.

El espacio de clave secreta es un requisito de seguridad básica en cualquier criptosistema, ya que debe ser mayor de $2^{100}$ para resistir un ataque de búsqueda exhaustivo [31], donde todas las claves secretas posibles son probadas por un intruso que desea romper el criptosistema. Además, un algoritmo de encriptación eficiente debe ser muy sensible a un pequeño cambio en la clave secreta. El esquema de cifrado propuesto utiliza el mapa de Hénon, que tiene dos condiciones iniciales (x e y) y dos parámetros de control ( a y b) para cada paciente. Estos cuatro parámetros se definen como la clave $K \in x, y, a, b$. Todos ellos son variables con una precisión de 15 decimales ya que se utiliza el formato de punto flotante de doble precisión. Por lo tanto, el espacio total de la clave es $1015 + 1015 + 1015 + 1015 \approx 2199$ haciendo que el esquema propuesto sea resistente contra el ataque exhaustivo de búsqueda o el ataque de fuerza bruta considerando la potencide cálculo que actualmente tienen las computadoras.

La sensibilidad de clave (incluso a variaciones de nivel de bit) en criptosistemas basados en caos es una propiedad de seguridad básica para producir criptogramas no correlacionados cuando la misma bioseñal se cifra con dos claves secretas similares. En el proceso de descifrado, solo la misma clave secreta debe recuperar la bioseñal original correspondiente.

En el esquema propuesto, la sensibilidad clave en el proceso de encriptación se presenta visualmente en la Figura 5.5. Las bioseñales BP1 del Paciente 1 y ECG2 del Paciente 2 no se pueden recuperar con éxito, ya que las claves correspondientes son incorrectas incluso a nivel de bit (ver Tabla 2). Cuantitativamente, el BER, entre la bioseñal original de BP1 y la señal recuperada correspondiente, cuando se utiliza una clave ligeramente diferente en el proceso de descifrado es 0.5677, lo que significa que la señal recuperada es muy diferente a la original. Para la bioseñal ECG2 original y la recuperada con la clave errónea el BER es 0.6543, que resulta en una señal recuperada erróneamente. Por otro lado, la diferencia entre la bioseñal original ECG1 del paciente 1 y la bioseñales del BP3 del paciente 3 y las correspondientes (correctas) señales recuperadas es de 0.0001 y 0.0002, respectivamente. Además, solo la clave secreta correcta a nivel de bit puede recuperar alguna señal en el proceso de descifrado. Por lo tanto, el esquema propuesto es altamente sensible a la clave secreta.

Recientemente esquemas clásicos de cifrado basados en el caos para la información médica han sido propuestos en la literatura, donde solo se utilizan algoritmos de encriptación basados en el caos para encriptar datos biomédicos para proporcionar confidencialidad en una bioseñal particular. Por ejemplo, [19] usa el mapa logístico en una arquitectura de permutación y difusión para cifrar bioseñales como ECG, EEG y BP. Lin en [21] propuso un mecanismo de cifrado basado en un oscilador colpitts caótico para cifrar un EEG. Aunque los autores presentan una evaluación de seguridad, los resultados mostraron una baja eficiencia contra el ruido o el ataque de interferencia o no presentaron solidez contra el ruido. Por otro lado, se ha propuesto la técnica de

esteganografía para preservar la privacidad de las señales fisiológicas mediante el uso de códigos Hamming [32], transformada wavelet [33] o alineación de coeficientes [34]. Incluso, el cifrado basado en el caos clásico y la esteganografía se han propuesto en [35]. Algunos de ellos presentan análisis contra el ruido mediante el uso de ataques de ruido blancos gaussiano, pero con cierto grado de robustez. Además, estos esquemas transmiten una sola bioseñal encriptada.

En contraste con todos estos trabajos, el esquema propuesto transmite varias señales biomédicas seguras a la vez, donde varios pacientes (independientes) comparten solo un canal para comunicarse (sin sincronización entre partes). Además, por primera vez se presenta un algoritmo de encriptación de varias bioseñales simultáneamente, utilizando una combinación de técnicas de espectro esparcido y mapas caóticos discretos, con aplicación en la telemedicina segura, específicamente para una red de sensores BASN, además el esquema propuesto es altamente resistente contra el ruido o los ataques de interferencia.

# Capítulo 6. Conclusiones

En esta tesis doctoral, se propuso un nuevo esquema seguro de comunicaciones multiusuario para aplicaciones de telemedicina basado en la técnica de acceso múltiple por división de código. En la técnica CDMA, varios pacientes comparten ancho de banda y envían bioseñales de manera segura a través de un solo canal en un BANS, lo que optimiza el ancho de banda disponible y reduce el costo de implementación.

El esquema de seguridad usa cifrado caótico (especialmente con el mapa de Hénon) y modulación BPSK para proporcionar privacidad en bioseñales como electrocardiogramas y presión arterial en BASN. Cada bioseñal se cifró con una clave secreta basada en los parámetros de control y las condiciones iniciales del mapa de Hénon, que deben compartirse de forma segura entre las partes autorizadas mediante el uso de un protocolo de intercambio de claves seguro.

Los resultados de la simulación del análisis de calidad con BER inferior al 0.5% de bits perdidos, MSE muy bajo y alto PSNR entre bioseñales originales y bioseñales recuperadas, mostraron alta robustez contra el ruido cuando la energía por bit es 3 o mayor. Por otro lado, el esquema presenta un gran espacio clave y alta sensibilidad en la clave secreta, lo que lo hace seguro contra el ataque exhaustivo de búsqueda. En el proceso de descifrado, solo la clave secreta correcta puede recuperar la bioseñal específica.

Algunas desventajas del esquema propuesto es que está limitado a un muestreo de frecuencia bajo (100 Hz) lo que liita su uso a de bioseñales específicas ) de baja frecuencia). Otro es que requiere al menos 50 muestras por ciclo en la señal portadora para recuperar bioseñales con éxito.

En futuros trabajos, el esquema propuesto se probará en sistemas empotrados como microcontroladores de alto gamma o FPGA con detección de señal electrofisiológica en tiempo real. Además, es necesario realizar trabajos para una frecuencia de muestreo flexible. En seguridad, se determinará un análisis exhaustivo de seguridad para verificar su efectividad desde un punto de vista criptográfico como el análisis diferencial, el análisis estadístico, la sensibilidad de la clave secreta, la correlación, los histogramas, entre otros. Finalmente, cada paciente o médico puede tener su propio mapa caótico para aumentar la seguridad de la información y la resolución de ADC puede ser de 12 o 16 bits para aumentar la precisión de los datos.

# Bibliografía


[1] G. Shobha, R.R. Chittal, K. Kumar, Medical applications of wireless networks, in: 2nd International Conference on Systems and Networks Communications, 2007, pp. 1–6.

[2] M.H. Ibrahim, S. Kumari, A.K. Das, M. Wazid, V. Odelu, Secure anonymous mutual authentication for star two-tier wireless body area networks, Comput. Methods Prog. Biomed. 135 (2016) 37–50.

[3] D. Halperin, T. Heydt-Benjamin, K. Fu, T. Kohno, W. Maisel, Security and pri- vacy for implementable medical devices, Pervasive Comput. Mob. Ubiquitous Syst. 7 (2008) 30–33.

[4] A.B. Waluyo, I. Pek, X. Chen, W.S. Yeoh, SLIM: a secured lightweight interac- tive middleware for wireless body area network, in: 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2008, pp. 1821–1824.

[5] F. Xu, F. Qin, C.C. Tan, B. Wang, Q. Li, IMDGuard: securing implantable medical devices with the external wearable guardian, in: The 30th IEEE International Conference on Computer Communications, 2008, pp. 1862–1870.

[6] H. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, They can hear your heartbeats: non-invasive security for implanted medical devices, in: Conference of the ACM Special Interest Group on Data Communication, 2011, pp. 1–12.

[7] C.H. Lin, S.T. Young, T.S. Kuo, A remote data access architecture for home-monitoring health-care applications, Med. Eng. Phys. 29 (2007) 199–204.

[8] R. Abirami, K. Mahalakshmi, R. Ranjitha, S. Chevanthy, G. Vijayalakshmy, Bio-medical signal monitoring system for long distance secure wireless transmission, Int. J. Adv. Eng. Glob. Technol. 2 (2014) 511–516.

[9] Q.A. Kester, L. Nana, A.C. Pascu, S. Gire, J.M. Eghan, N.N. Quaynor, A security technique for authentication and security of medical images in health infor- mation systems, in: 15th International Conference on Computational Science and Its Applications, 2015, pp. 8–13.

[10] A.V. Diaconu, Circular inter–intra pixels bit-level permutation and chaos-based image encryption, Inf. Sci. 355 (2016) 314–327.

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

[12] V.G. Supriya, S.R. Manjunatha, Chaos based cancellable biometric template protection scheme-a proposal, Int. J. Eng. Sci. Inven. 3 (2014) 2319–6726.

[13] L. Gámez-Guzmán, C. Cruz-Hernández, R.M. López-Gutiérrez, E.E. García-Guer- rero, Synchronization of Chua's circuits with multi-scroll attractors: application to communication, Commun. Nonlinear Sci. 14 (2009) 2765–2775.

[14] M.I. Mihailescu, New enrollment scheme for biometric template using hash chaos-based cryptography, Proc. Eng. 69 (2014) 1459–1468.

[15] L. Cardoza-Avendaño, R.M. López-Gutiérrez, C. Cruz-Hernández, V. Spirine, R.A. Chávez-Pérez, A. Arellano-Delgado, Encrypted audio transmission via synchronized chaotic nd: YAG lasers, Revista Mexicana de Física 58 (2012) 472–480.

[16] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiér- rez, A robust embedded biometric authentication system based on fingerprint and chaotic encryption, Expert Syst. Appl. 42 (2015) 8198–8211.

[17] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiér- rez, O.R. Acosta Del Campo, A RGB image encryption algorithm based on total plain image characteristics and chaos, Signal Process. 109 (2015) 119–131.

[18] C. Fu, G.Y. Zhang, O. Bian, W.M. Lei, H.F. Ma, A novel medical image protection scheme using a 3-dimensional chaotic system, PLoS ONE 9 (2015) 1–25.

[19] M.A. Murillo-Escobar, L. Cardoza-Avendaño, R.M. López-Gutiérrez, C. Cruz-H- ernández, A double chaotic layer encryption algorithm for clinical signals in telemedicine, J. Med. Syst. 41 (2017) 1–17.

[20] G. Kenfack, A. Tiedeu, Chaos-based encryption of ECG signals: experimental results, J. Biomed. Sci. Eng. 7 (2014) 368–379.

[21] C.F. Lin, Chaotic visual cryptosystem using empirical mode decomposition al- gorithm for clinical EEG signals, J. Med. Syst. 40 (2016) 1–10.

[22] A. Pandey, B. Singh Saini, B. Singh, N. Sood, An integrated approach us- ing chaotic map & sample value difference method for electrocardiogram steganography and OFDM based secured patient information transmission, J. Med. Syst. 41 (2017) 1–20.

[23] T.L. Carroll, Chaos for low probability of detection communications, Chaos Soli- ton Fract. 103 (2017) 238–245.

[24] Z.B. Jemaa, S. Belghith, Chaotic time hopping based multiple access in BP- SK-UWB system, Signal Process. 120 (2016) 644–653.

[25] G. Kaddoum, F. Richardson, F. Gagnon, Design and analysis of a multi-carrier differential chaos shift keying communication system, IEEE Trans. Commun. 61 (2013) 3281–3291.

[26] R. Vali, S. Berber, S.K. Nguang, Analysis of chaos-based code tracking using chaotic correlation statistics, IEEE Trans. Circuits Syst. I 59 (2012) 796–805.

[27] N.X. Quyen, V.V. Yem, T.M. Hoang, A chaos-based secure direct-sequence/spread-spectrum communication system, Abstr. Appl. Anal. 10 (2013) 190–205.

[28] S. Ganesan, T. Aruldoss, A. Victoire, G. Vijayalakshmy, Real time estimation and detection of non- linearity in bio signals using wireless brain computer inter- face, Int. J. Bioinform. Res. Appl. 10 (2014) 190–205.

[29] Physionet, PhysioBank ATM, Online, available on: https://physionet.org/cgi-bin/ atm/ATM [visited on june 2017].

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

[31] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryp- tosystems, Int. J. Bifurcat. Chaos 16 (2006) 2129–2151.

[32] H.-J. Shiu, B.-S. Lin, C.-H. Huang, P.-Y. Chiang, C.-L. Lei, Preserving privacy of online digital physiological signals using blind and reversible steganography, Comput. Methods Prog. Biomed. 151 (2017) 159–170.

[33] C.A. Liji, K.P. Indiradevi, K.K.A. Babu, Integer-to-integer wavelet transform based ECG steganography for securing patient confidential information, Proc. Technol. 24 (2016) 1039–1047.

[34] C.Y. Yang, W.F. Wang, Effective electrocardiogram steganography based on co– efficient alignment, J. Med. Syst. 40 (2016) 1–15.

[35] G.M. Vengurlekar, S.K. Bhatia, ECG steganography based privacy protection of medical data utilizing chaos encryption, Int. J. Innov. Sci. Eng. Technol. 2 (2015) 818–822.