UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Facultad de Ingeniería, Arquitectura y Diseño

Programa de Maestría y Doctorado en Ciencias e Ingeniería

ENCRIPTADO CAÓTICO EN SISTEMAS BIOMÉTRICOS

TESIS

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

DOCTOR EN CIENCIAS

presenta:

EVERARDO INZUNZA GONZÁLEZ

Director de tesis

DR. CÉSAR CRUZ HERNÁNDEZ

Ensenada, Baja California, México. Diciembre de 2012.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

Facultad de Ingeniería, Arquitectura y Diseño

ENCRIPTADO CAÓTICO EN SISTEMAS BIOMÉTRICOS

TESIS

que para obtener el grado de DOCTOR en CIENCIAS presenta:

EVERARDO INZUNZA GONZÁLEZ

Y aprobada por el siguiente comité:

Dr. César Cruz Hernández
Director del Comité

Dr. Enrique Efrén García Guerrero
Miembro del Comité

Dr. Oscar Roberto López Bonilla
Miembro del Comité

Dr. Didier López Mancilla
Miembro del Comité

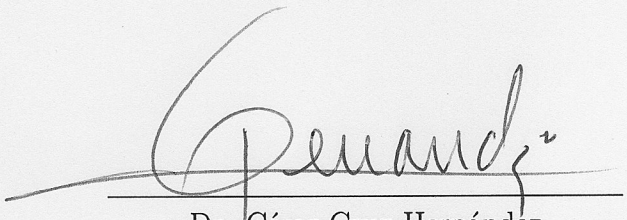
Dra. Rosa Martha López Gutiérrez
Miembro del Comité

Diciembre de 2012

RESUMEN de la tesis de **Everardo Inzunza González**, presentada como requisito parcial para obtener el grado de DOCTOR EN CIENCIAS en ELÉCTRICA con orientación en COMUNICACIONES, del programa de Maestría y Doctorado en Ciencias e Ingeniería de la UABC. Ensenada, B. C. México, Diciembre de 2012.

ENCRIPTADO CAÓTICO EN SISTEMAS BIOMÉTRICOS

Resumen aprobado por:



Dr. César Cruz Hernández

Director de Tesis

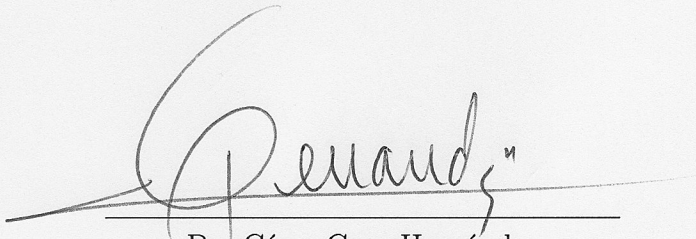
En este trabajo de tesis doctoral, se presenta el diseño e implementación de un sistema biométrico seguro que utiliza el encriptado caótico e hipercaótico, específicamente en un sistema de reconocimiento de rostros, el cual emplea el método *eigenface* y trabaja remotamente. Para el encriptado de las imágenes de rostros y patrones se utilizan los mapeos caóticos de Hénon, gato de Arnold, y los mapeos hipercaóticos de Chen y Rössler. Se propone un algoritmo sencillo de encriptado y dos algoritmos de doble encriptado, todos estos empleando un umbral de cuantización optimizado. Para evaluar la seguridad de los algoritmos propuestos para el encriptado hipercaótico, se les realiza un análisis contra distintos ataques a los criptogramas, por ejemplo, ataques de fuerza bruta, ataques estadísticos mediante el uso de histogramas, gráficas de dispersión entre pixeles adyacentes, las cuales permiten obtener sus coeficientes de correlación y entropía de la información, también se muestran resultados contra ataques diferenciales. Además, se realiza una comparación de los resultados de este análisis de seguridad con respecto a otros experimentos reportados recientemente en la literatura que utilizan distintos algoritmos de encriptado caótico. Las simulaciones y resultados experimentales, comprueban que el análisis de seguridad realizado a los algoritmos de encriptado propuestos en este trabajo de tesis doctoral, son fuertes contra los distintos tipos de ataques, por lo tanto son factibles de implementar en sistemas de identificación biométrica que requieran el uso de una red pública para la comunicación, tal como la internet. Por último, se presentan las interfaces gráficas de usuario del software desarrollado para el encriptado hipercaótico y para el reconocimiento de rostros.

Palabras clave: Encriptado caótico, análisis de seguridad, sistema biométrico, reconocimiento de rostros.

ABSTRACT of the thesis of **EVERARDO INZUNZA GONZÁLEZ**, presented as a partial requirement to obtain the degree of DOCTOR in ELECTRICAL SCIENCES, with major in COMMUNICATIONS, of the program of MSc and PhD in Sciences and Engineering of UABC. Ensenada, B. C., Mexico, December 2012.

CHAOTIC ENCRYPTION IN BIOMETRICS SYSTEMS

Abstract approved by:



Dr. César Cruz Hernández

Thesis supervisor

In this doctoral thesis, the design and implementation of a biometric system using chaotic and hyperchaotic encryption is presented, specifically in a face recognition system, which uses the *eigenface* method and works remotely. The Hénon chaotic map, Arnold's cat map, and the hyperchaotic mappings of Chen and Rössler are used for the encryption of the faces images and patterns. A single encryption algorithm and two double encryption algorithms are proposed, all these using a threshold of optimized quantization. To assess the security of the proposed algorithms for the hyperchaotic encryption, an analysis against various attacks on encryption, such as brute force attacks, statistical attacks using histograms, scattering graphs between adjacent pixels is performed, which allow to obtain the coefficients of correlation and information entropy, results against differential attacks are also shown. Furthermore, a comparison of the results of this security analysis with regard to other experiments reported recently in the literature using different chaotic encryption algorithms is performed. The simulations and experimental results verify that the security analysis performed to the encryption algorithms proposed in this PhD thesis are strong against the different types of attacks, therefore are feasible to implement in biometrics identification systems which require the use of a public network for communication, such as the internet. Finally, the graphical interfaces of the software's user developed for the hyperchaotic encryption and face recognition are presented.

Keywords: Chaotic encryption, security analysis, biometric system, face recognition.

A mi familia

Agradecimientos

*A **DIOS**, por darme cada día un respiro de vida, un soplo de inteligencia y una eternidad de bendiciones. Gracias Señor, por acordarse de mí y hacer este sueño una realidad.*

*Al **Dr. César Cruz Hernández**, por haberme dirigido en este camino tan complicado e interesante. Por toda su paciencia y por sus valiosos consejos que permitieron la culminación de este trabajo de investigación.*

*Al **Dr. Enrique Efrén García Guerrero**, por sus valiosos consejos y comentarios durante todo este proceso de formación doctoral y por su gran amistad. Muchas gracias Dr. García!*

*Al **Dr. Oscar Roberto López Bonilla**, por sus comentarios tan acertados en todas las presentaciones y revisiones de la tesis, que complementaron la formación doctoral.*

*Al **Dr. Didier López Mancilla**, por la atención prestada durante el desarrollo de este trabajo y por todos sus comentarios que permitieron mejorar este proyecto de tesis.*

*A la **Dra. Rosa Martha López Gutiérrez**, por el apoyo brindado y observaciones durante todo el transcurso de mi doctorado.*

*A la memoria de mi padre **José Alejandro Inzunza**, por darme la vida, por todos consejos que me dió en mi infancia y que marcaron mi vida por el buen camino!, gracias Papá!*

*A mi **Madre Santa Manuela González**, por darme la vida, por sus valiosos consejos y palabras tan bonitas que siempre me dice. Te quiero mucho mamá!!*

*A mis **hermanos(a), Leticia, Magdalena, Mirna, Martín y Alejandro**, por todos sus consejos y experiencia de vida que me han compartido. Los quiero mucho!*

*A mi esposa **Leticia Rodríguez Orozco**, por toda la paciencia y motivaciones que permitieron darme perseverancia para el desarrollo de este trabajo de tesis doctoral.*

*A la familia **Hernández González**, en especial a la memoria de mi Tío Fernando, que siempre me estuvo guiando por el buen camino.*

Al ***CONACyT****, a través del proyecto de grupos de investigación ref. 166654.*

Al ***CONACyT****, a través del proyecto número 119168.*

A nuestra alma mater: ***Universidad Autónoma de Baja California****, que tanto me ha dado en lo profesional y en lo académico.*

A la ***Facultad de Ingeniería, Arquitectura y Diseño****, la cual considero como mi segundo hogar.*

Al ***personal directivo de la FIAD****, por el apoyo brindado, en especial al Dr. Juan Iván Nieto.*

Al ***coordinador de posgrado****, Dr. Juan de Dios Sánchez, por sus asesorías administrativas.*

A la ***Dra. Eloísa García*** *por todos los tip's acerca de LaTeX y por su bonita amistad.*

A todos mis amigos de la UABC: ***Yolanda Baez, Pablo Rousseau, Jesús Olguín, Juracy Soares, Juan Miguel Hernández, Sergio Infante, Diego Tlapa, Dora Luz, Jorge Limón, Jesus Salinas, Julián Aguilar, Christian Navarro, Juan Pablo Torres****, quienes con su apoyo y confianza fue posible llegar a la meta... Muchas gracias compañeros!!*

A todos los ***profesores e investigadores*** *del MYDCI, que compartieron conmigo una parte de sus conocimientos durante los cursos de doctorado.*

A mis ***colegas profesores e investigadores de la FIAD****, por todos sus comentarios motivadores y sus buenos deseos.*

Al personal administrativo de la FIAD: ***Luisa, Sarita, Martha y Eliud****, por el apoyo brindado durante todos estos años, muchas gracias!*

A la ***Familia Rodríguez****, por su amistad y cariño que me han demostrado.*

A mis amigos de mi tierra natal: ***Arturo, Gerardo, Ricardo, Geovany, Rodrigo, Arcadio, Sinuhe, Francisco Jesús, Francisco Candelario, Yiyo, Fabián, Paúl.*** *Gracias amigos!*

Ensenada, B. C. México.
04 de Diciembre de 2012.

EVERARDO INZUNZA GONZÁLEZ

Tabla de Contenido

Página

Tabla de Contenido (Continuación)

Tabla de Contenido (Continuación)

Lista de figuras

Lista de figuras (Continuación)

Lista de figuras (Continuación)

Lista de tablas

Capítulo I

Introducción

El presente trabajo de tesis doctoral, se ha desarrollado con la finalidad de contribuír a la solución de problemas abiertos de sistemas de control de acceso que operan remotamente, empleando como clave de acceso un identificador biométrico, en áreas seguras, donde es necesario que el sistema asegure y reconozca realmente la identidad de las personas. Para garantizar la privacidad de información biométrica de los usuarios, la cual es enviada por una red pública, se propone aplicar el encriptado hipercaótico, en este caso específico a los sistemas de reconocimiento de rostros. En particular, para la tarea de identificación, se seleccionó el método eigenface (Turk y Pentland, 1991a,b), para el encriptado de la información confidencial se propone utilizar los mapeos caóticos de Hénon (Hénon, 1976) y Arnold (Isaeva *et al.*, 2006), así como los mapeos hipercaóticos de Chen (Chen, 2001) y Rössler (Itoh *et al.*, 2001), debido a que exhiben dinámicas extremadamente complejas. Se propone utilizar el algoritmo de encriptado y desencriptado caótico reportado por Muhammad y colaboradores en (Muhammad *et al.*, 2007b), el cual, es utilizado para encriptar plantillas de iris, sin embargo, en este trabajo de tesis, se hace una modificación a este algoritmo de encriptado para mejorar el nivel de seguridad de la información biométrica encriptada, esta mejora consiste en hacer una optimización al umbral de cuantización del encriptador hasta que se encuentre la mejor entropía de información. Además, se proponen dos algoritmos de doble encriptado hipercaótico empleando el mismo mapeo o con distintos mapeos y umbral de cuantización optimizado.

I.1 Motivación

Con la rápida evolución de las tecnologías asociadas a la información, nuestra sociedad está cada día más conectada electrónicamente. Labores que tradicionalmente eran realizadas por seres humanos, son gracias a las mejoras tecnológicas, realizadas por sistemas automatizados. Dentro de la amplia gama de posibles actividades que pueden automatizarse, aquella relacionada con la capacidad para establecer la identidad de los individuos ha cobrado importancia y como consecuencia directa, la biometría se ha transformado en un área emergente. Dado al gran avance de la computación y las redes de telecomunicaciones, cada vez es más importante comunicar a estos sistemas de reconocimiento biométrico, en una forma más segura, para garantizar con un alto nivel de seguridad la privacidad de la información biométrica de los usuarios, por tal motivo, se propone aprovechar las grandes ventajas de los sistemas caóticos para el encriptado de esta información confidencial.

I.2 Criptografía

La palabra **criptografía**, proviene del griego $\kappa\rho\upsilon\tau\tau\tau\acute{o}\varsigma$ *krypto* (oculto) y grafía (escribir), según la Real Academica Española *(RAE)* se define como el *arte de escribir con clave secreta o de un modo enigmático.* Es decir, la ciencia que se encarga de cifrar o descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera segura y que sólo pueden ser interpretados por las personas a quienes van dirigidos. Con más precisión, cuando se habla de esta área de conocimiento como ciencia, se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves. La

criptografía es la disciplina que trata de la transmisión y almacenamiento de datos de manera que no puedan ser comprendidos ni modificados por terceros. Los diferentes métodos de criptografía actualmente utilizados necesitan que dos personas que deseen comunicar información, intercambien de forma segura una o más claves; una vez que las claves han sido intercambiadas, los interlocutores pueden transferir información con un nivel de seguridad conocido (Menezes *et al.*, 1996). Pero esta forma de trabajar basa la seguridad de las transmisiones exclusivamente en la seguridad del intercambio de claves. La forma más segura de realizar este intercambio de claves es de manera presencial, pero ello no es posible en algunos de los casos, dado el múltiple número de interlocutores con los que se desea intercambiar información confidencial (bancos, tiendas en internet, colegas de trabajo en sedes distantes, etc.). De manera que el punto donde hay menor seguridad en el intercambio de información confidencial está en el proceso de intercambio y transmisión de las claves (Schneier, 1996). En la figura 1, se observa un esquema a bloques de la técnica criptográfica de clave privada o simétrica, en este caso el término simétrico se refiere a que se utiliza la misma clave para encriptar y desencriptar la información.

También existe el sistema criptográfico de clave asimétrica o de clave pública, debido a que la clave que se utiliza para encriptar la información es del conocimiento de todos los usuarios de la red y para poder desencriptar la información se utiliza una clave completamente distinta a la clave pública, la cual se le conoce como clave privada y solamente el destinatario autorizado debe conocer esta clave privada. El término asimétrico se refiere a que la clave de encriptamiento de la información es distinta a la clave de desencriptamiento (Menezes *et al.*, 1996; Schneier, 1996).

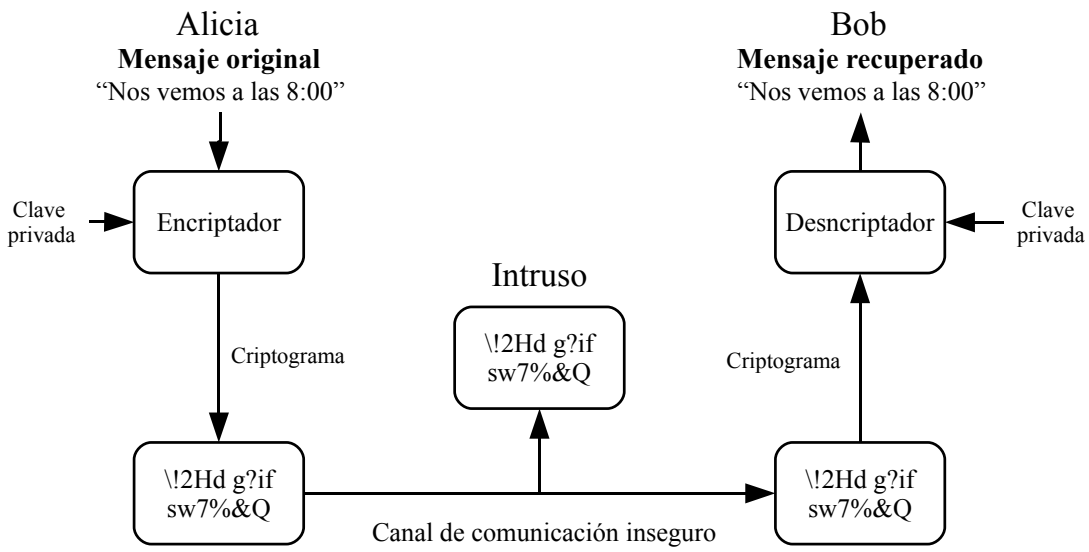


Figura 1: Esquema a bloques del sistema criptográfico de clave simétrica (Menezes *et al.*, 1996).

Con intención de incrementar la seguridad en los sistemas criptográficos, se ha propuesto aplicar el caos en el encriptado de la información confidencial, ver por ejemplo (Baptista, 1998; Giuseppe y Saverio, 1999; Jakimoski y Kocarev, 2001). En estos casos, ellos proponen encriptar mensajes de texto aplicando caos e hipercaos. En el trabajo reportado en (Li *et al.*, 2001) se propone una técnica para mejorar la seguridad del encriptado caótico. Recientemente se ha publicado el libro “Criptografía basada en caos” (Kocarev y Shiguo, 2011), ahí detallan aspectos relacionados con la teoría de caos, algoritmos y aplicaciones. Mencionan que la criptografía basada en caos es una nueva línea de investigación que une a dos campos, es decir, el caos (sistemas con dinámicas no lineales) y la criptografía (seguridad de datos en computación).

I.3 Planteamiento del problema

El presente trabajo de tesis doctoral, parte de un problema abierto en aplicaciones de control de acceso que operan remotamente, en el cual, para que una persona pueda ingresar a cierta área restringida, es necesario que sea un usuario que previamente haya sido dado de alta o registrado en el sistema de identificación biométrica. En este caso, el rostro es el identificador biométrico a registrar y reconocer por el sistema automático de identificación. Una vez que el usuario desea ingresar a esta área de acceso restringido, es necesario que se identifique con el sistema biométrico, en este caso la imagen de su rostro es su clave de acceso, esta imagen es digitalizada y enviada a través de una red pública a un servidor de cómputo en el que se encuentran registrados todos los usuarios. Si esta imagen del rostro coincide con alguna de las que se encuentran almacenadas, el sistema dará acceso al usuario, de lo contrario será denegado. La figura 2 muestra el esquema a bloques de este problema.

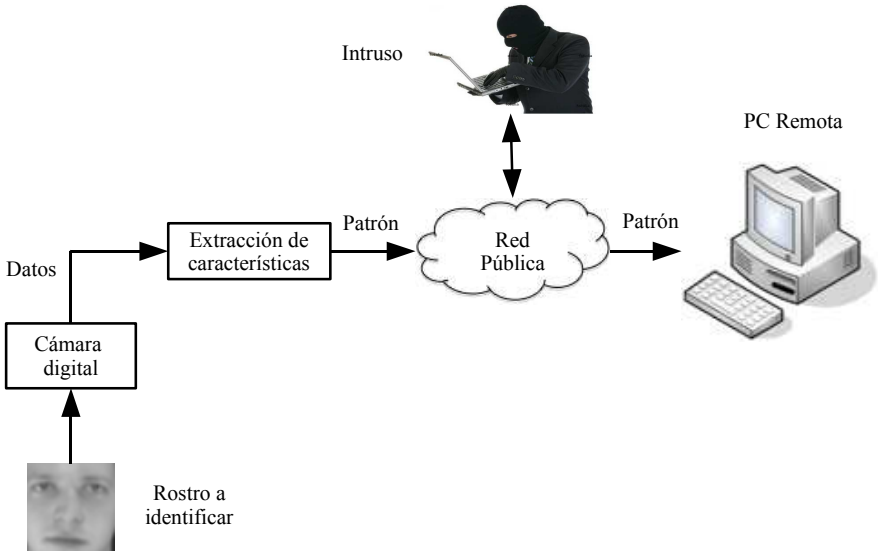


Figura 2: Planteamiento del problema.

Como se puede observar en la figura 2, la imagen del rostro que es captada por el sensor biométrico, en este caso es una cámara digital, es enviada a través de una red

pública, tal como la internet, esto hace vulnerable a que un intruso o atacante pueda obtener esta información y hacer mal uso de ella, por tal motivo, cuando es necesario enviar información confidencial de manera segura a la base de datos remota, esta debe ser enviada de forma encriptada.

I.3.1 Propuestas de solución

En la figura 3, se presenta el esquema general de la propuesta de solución a este problema. Las características especiales del caos, hacen de los mapeos caóticos excelentes candidatos para el encriptado de la información biométrica (Fu *et al.*, 2011; Kocarev y Shiguo, 2011; Fateri y Enayatifar, 2011; Muhammad *et al.*, 2007b), basados en el requerimiento clásico de Shannon de confusión y difusión (Shannon, 1949, 1948; Zhang *et al.*, 2004), por tal motivo se propone aplicar el caos para encriptar la información biométrica. Como se puede observar en la figura 3, se propone aplicar el encriptador hipercaótico justo antes de enviar la información por la red pública. En el receptor, lo primero que se hace es desencriptar la información, posteriormente se hace la extracción de características, luego se realiza la tarea de comparación de la información biométrica almacenada en la base de datos, para finalmente habilitar el dispositivo de aplicación, el cual depende del resultado de la comparación.

Propuesta de solución 1

La figura 4, presenta un esquema a bloques más detallado de la propuesta 1 de solución al problema planteado, se puede observar que en la parte del transmisor, se captura la imagen y luego se encripta empleando algún mapeo caótico/hipercaótico utilizando como clave de encriptado las condiciones iniciales del mapeo, posteriormente esta información encriptada (criptograma) se envía a través de una red pública, en este caso por internet. Del lado remoto, un servidor recibe el criptograma, y lo desencripta empleando el mismo mapeo y clave que se utilizaron en el transmisor, posteriormente se realiza la

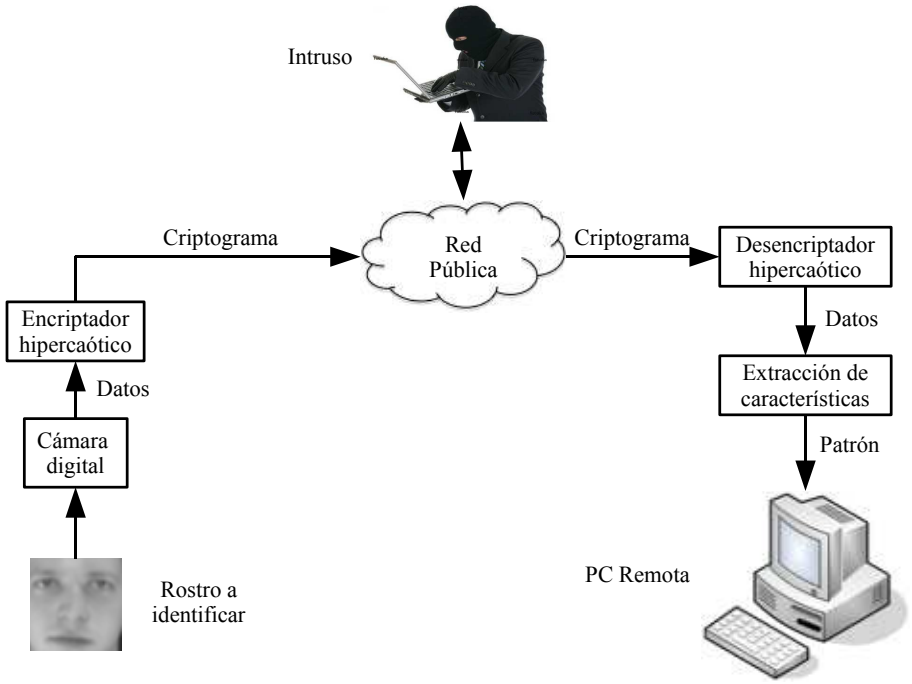


Figura 3: Esquema general de la propuesta de solución al problema planteado.

tarea de reconocimiento biométrico, es decir, se hace una extracción de características, se forma una plantilla con esta información, posteriormente se hace una comparación con las plantillas registradas en la base de datos, y en caso que coincida con alguna de las plantillas registradas previamente, el sistema dará acceso al usuario, de lo contrario será denegado su acceso.

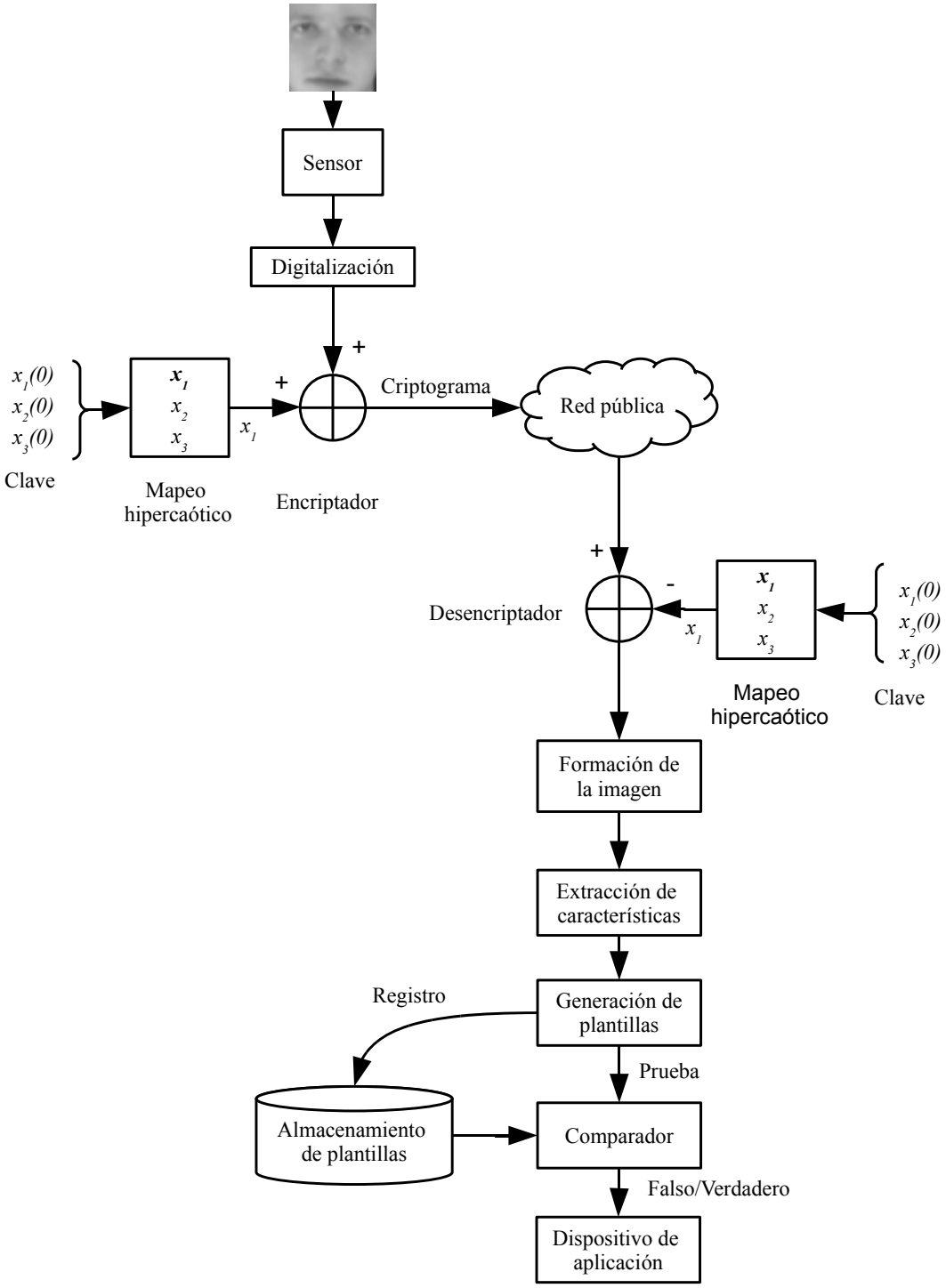


Figura 4: Esquema a bloques detallado de la propuesta 1 de solución al problema planteado.

Propuesta de solución 2

La figura 5, presenta un esquema a bloques detallado de la propuesta 2 de solución al problema planteado, en este caso se propone, que la extracción de características y formación de la plantilla se realicen en la parte del transmisor. Los demás procesos, quedan de la misma manera que se mostró en la figura 4. La ventaja de esta propuesta, es que agiliza el proceso de encriptado, ocupa menor cantidad de memoria para el almacenamiento, ahorra ancho de banda en la red de comunicación y el envío de la información es más rápido, debido a que la información de los patrones es mucho menor con respecto a la información de la imagen original.

En ambas propuestas, para la tarea de reconocimiento, se seleccionó el método ***eigenface*** (Turk y Pentland, 1991a,b), para el encriptado de la información confidencial se propone utilizar los mapeo caóticos de Hénon (Hénon, 1976) y gato de Arnold (Isaeva *et al.*, 2006), así como los mapeos hipercaóticos de Chen (Chen, 2001) y Rössler (Itoh *et al.*, 2001), debido a las dinámicas complejas que generan. Para la parte de encriptado y desencriptado caótico se utilizará el algoritmo reportado por (Muhammad *et al.*, 2007b), ya que presenta buen nivel de seguridad y es factible de implementarse fisicamente en computadoras y sistemas empotrados. Sin embargo, en este trabajo de tesis se realiza una mejora al umbral de cuantización, debido a que (Muhammad *et al.*, 2007b) proponen un umbral fijo de 0.5, pero de acuerdo a las simulaciones y experimentos realizados en este trabajo, se observó que no es el mejor umbral para alcanzar el nivel de seguridad más alto en el encriptado de la información, por tal motivo se realizó una optimización al valor del umbral de cuantización.

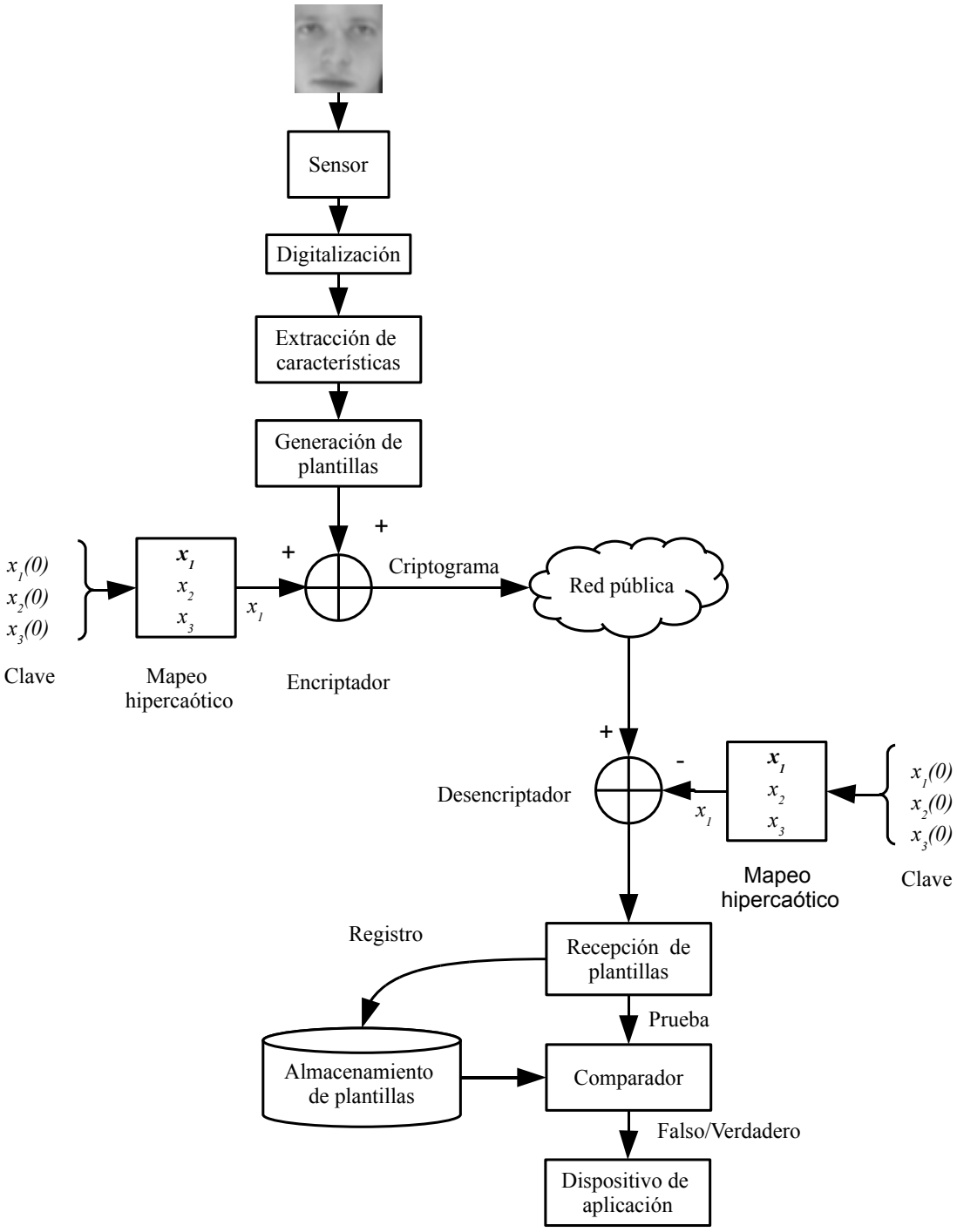


Figura 5: Esquema a bloques detallado de la propuesta 2 de solución al problema planteado.

I.4 Objetivos

Con la realización de la presente propuesta de tesis doctoral, se pretende alcanzar los siguientes objetivos:

Objetivo general:

Contribuir a la seguridad del encriptado de información confidencial para su empleo en los sistemas automáticos de identificación biométrica.

- **Objetivo particular 1:** *Encriptar información empleando sistemas con dinámicas caóticas e hipercaóticas.*
- **Objetivo particular 2:** *Aplicar el encriptado caótico en los sistemas automáticos de identificación biométrica para el control de acceso.*
- **Objetivo particular 3:** *Evaluar el nivel (o grado) de seguridad de la información biométrica encriptada.*

I.5 Organización del manuscrito

Este trabajo de tesis doctoral se organiza en siete capítulos y dos apéndices. En el **segundo capítulo**, se presenta una breve descripción de los sistemas caóticos, mapeos a utilizar y algunos trabajos relacionados al encriptado caótico. En el **tercer capítulo** se presenta una descripción de los sistemas biométricos y la técnica *eigenface* para la obtención de patrones, también se presentan los trabajos relacionados a esta investigación, primero se mencionan los trabajos relacionados con respecto al encriptado de información biométrica, luego se mencionan trabajos que involucran el encriptado caótico de imágenes. El **cuarto capítulo**, presenta la metodología de encriptado y desencriptado caótico, se propone un algoritmo de encriptado sencillo y dos algoritmos de doble encriptado caótico. En el **capítulo cinco**, se presentan las técnicas más comunes para realizar el análisis de seguridad a los algoritmos de encriptado propuestos en este trabajo de tesis, se consideran los ataques de fuerza bruta, análisis estadístico y ataques diferenciales. El **capítulo seis**, presenta los resultados experimentales obtenidos con el algoritmo de encriptado sencillo y los algoritmos de doble encriptado. También se hace un estudio comparativo de los resultados de esta tesis doctoral versus trabajos publicados recientemente en la literatura. Finalmente, en el **capítulo siete** se presentan las conclusiones generales, aportaciones y potenciales trabajos para desarrollar en un futuro. El **apéndice A**, presenta la interfaz gráfica del software encriptador caótico de imágenes, se muestra la pantalla principal del software desencriptador caótico de imágenes, se presenta la interfaz principal del software desarrollado para el reconocimiento de rostros humanos, se presenta el software desarrollado para encriptar patrones de rostros, por último se muestra el software desarrollado para desencriptar patrones de rostros. En el **apéndice B**, se presentan los productos de investigación derivados de este trabajo de tesis doctoral.

Capítulo II

Sistemas caóticos

II.1 Introducción

El **caos**, se define de acuerdo a la *RAE* como: *(1) Estado amorfo e indefinido que se supone anterior a la ordenación del cosmos. (2) Confusión, desorden. (3) Desde el punto de vista físico y matemático se considera como un comportamiento aparentemente errático e impredecible de algunos sistemas dinámicos, aunque su formulación matemática sea en principio determinista.* Por otra parte, (Li y Yorke, 1975) definen al caos como oscilaciones determinísticas. La teoría de caos, proporciona el significado para explicar los fenómenos de caos, controlar sistemas con dinámicas caóticas, del cual hacen uso de las propiedades del caos, especialmente su "aleatoriedad y ergodicidad", las cuales han demostrado ser adecuadas para el diseño de sistemas para protección de datos (Kocarev y Shiguo, 2011).

La primera aplicación para transmitir señales utilizando caos fue propuesta por (Pecora y Carroll, 1990), ellos mostraron que dos circuitos caóticos similares pueden sincronizar sus trayectorias, entonces el mensaje a ser enviado es enmascarado en una de las señales caóticas. Por el lado de la red, en el receptor, el mensaje es recuperado mediante un circuito sincronizado con el transmisor. Posteriomente, (Baptista, 1998), confirma que las oscilaciones caóticas que presentan un comportamiento aparentemente estocástico, caracterizado por un gran ancho de banda en el espectro de frecuencias, se pueden utilizar para encriptar información, con la finalidad de transmitir mensajes secretos en forma segura.

Recientemente, se han incrementado los esfuerzos en emplear caos en sistemas de comunicación, con la intención de mejorar algunas de sus características. El **caos** y la **criptografía** tienen algunas propiedades en común, la más relevante es la sensibilidad a pequeños cambios paramétricos y condiciones iniciales. Como se mencionó anteriormente, el caos se ha utilizado en el diseño de sistemas criptográficos, ver por ejemplo (Baptista, 1998; Giuseppe y Saverio, 1999; Kocarev y Shiguo, 2011). La característica común de los esquemas seguros de comunicación con base en caos, es que éstos, emplean una señal caótica para transmitir el mensaje confidencial. Es decir, mediante una modulación o algoritmo apropiado en el transmisor caótico, el mensaje confidencial se encripta y posteriormente se envía al receptor caótico a través de un canal o red pública, para finalmente ser desencriptado del lado remoto.

II.1.1 Dinámica caótica

Para poder clasificar el comportamiento de un sistema como ***caótico***, el mapeo debe tener las siguientes propiedades:

- Ser sensible a las condiciones iniciales.
- Su serie de tiempo debe estar acotada en amplitud.
- Las iteraciones de la serie son infinitas.
- La serie es oscilatoria aperiódicamente.
- La serie no converge.
- El sistema es no lineal.
- Proviene de un modelo determinístico.
- Debe ser transitivo.

- Sus atractores deben formar un conjunto denso en una región compacta del espacio de fase (presenta un atractor extraño).
- El atractor presenta dimensión fractal.
- Al menos tiene un exponente de Lyapunov positivo.

Debido a las propiedades de los sistemas caóticos mencionadas anteriormente, estos son atractivos para **criptografía caótica** (Kocarev y Shiguo, 2011). La sensibilidad a parámetros y condiciones iniciales, causa que las dinámicas del sistema cambien drásticamente aún cuando existe una muy ligera perturbación de los parámetros, esta propiedad se parece a un sistema criptográfico convencional. Mezclado o confusión es la tendencia del sistema a mezclar rápidamente pequeñas porciones del espacio de estado en una red compleja. Esas características pueden también hacer que la correlacionada información se convierta o desparrame por todo el espacio de fase, por lo tanto forman una base de datos encriptados caóticamente (Mao y Chen, 2004).

El espectro de Lyapunov está estrechamente relacionado con la dimensión fractal del atractor extraño asociado al modelo caótico. Kaplan y Yorke determinaron que la información de la dimensión d_f está relacionada al espectro de Lyapunov (Kaplan y Yorke, 1979) por la siguiente ecuación, reportada en (Wolf *et al.*, 1985):

$$d_f = j + \frac{\sum_{i=1}^{j} \lambda_i}{|\lambda_{j+1}|}, \tag{1}$$

donde j está definido por la condición:

$$\sum_{i=1}^{j} \lambda_i > 0 \quad o \quad \sum_{i=1}^{j+1} \lambda_i < 0. \tag{2}$$

II.2 Mapeos caóticos

II.2.1 Mapeo caótico de Hénon

Este mapeo de Hénon está compuesto por el siguiente sistema de ecuaciones en diferencias (Hénon, 1976):

$$x_1(k+1) = c - ax_1^2(k) + x_2(k),$$
$$x_2(k+1) = bx_1(k). \tag{3}$$

El mapeo de la ec. (3) exhibe dinámica caótica utilizando los siguientes parámetros y condiciones iniciales (Hénon, 1976): $a = 1.4$, $b = 0.3$, $c = 1$, $x_1(0) = 0.1$ y $x_2(0) = 0.15$.

Con este mapeo de Hénon se pueden generar señales caóticas en tiempo discreto, en la figura 6 se muestra el estado x_1 y x_2 en tiempo discreto generados con este mapeo y utilizando las condiciones iniciales y parámetros anteriores.
En la figura 7, se presenta el atractor caótico del mapeo de Hénon obtenido con la simulación numérica en Matlab, en este espacio se observa cierto confinamiento en la dinámica del mapeo, sin embargo el mapeo es caótico.

En la figura 8 se muestra el espectro de frecuencias de los estados x_1 y x_2 del mapeo de Hénon. Se puede observar que el estado x_1 contiene componentes espectrales de mayor potencia, también se observa que el espectro de frecuencias de las trayectorias es contínuo, por lo tanto son caóticas (Andrievskii y Fradkov, 2003).

El cálculo de los exponentes de Lyapunov que se presenta en los siguientes ejemplos, está basado en los trabajos realizados por (Wolf *et al.*, 1985; Briggs, 1990). La figura 9 muestra los exponentes de Lyapunov del mapeo de Hénon, en esta figura se puede observar que λ_1 tiene un valor aproximado a 0.41847, mientras que λ_2 tiene un valor

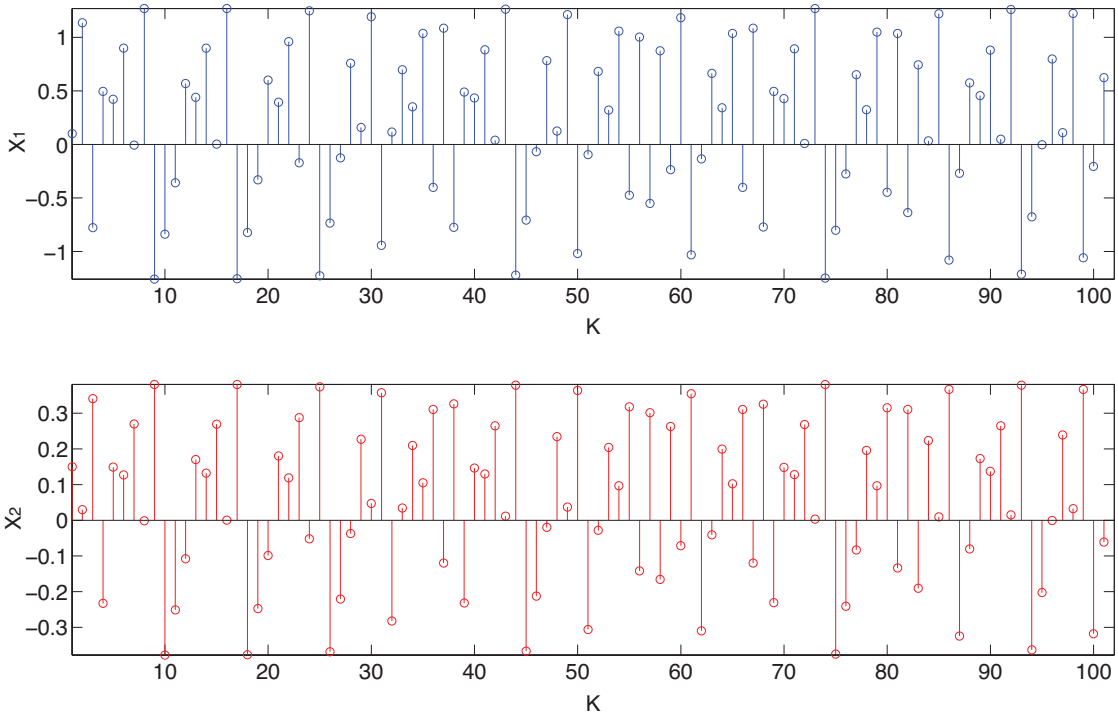


Figura 6: Señales caóticas en tiempo discreto obtenidas con el mapeo de Hénon.

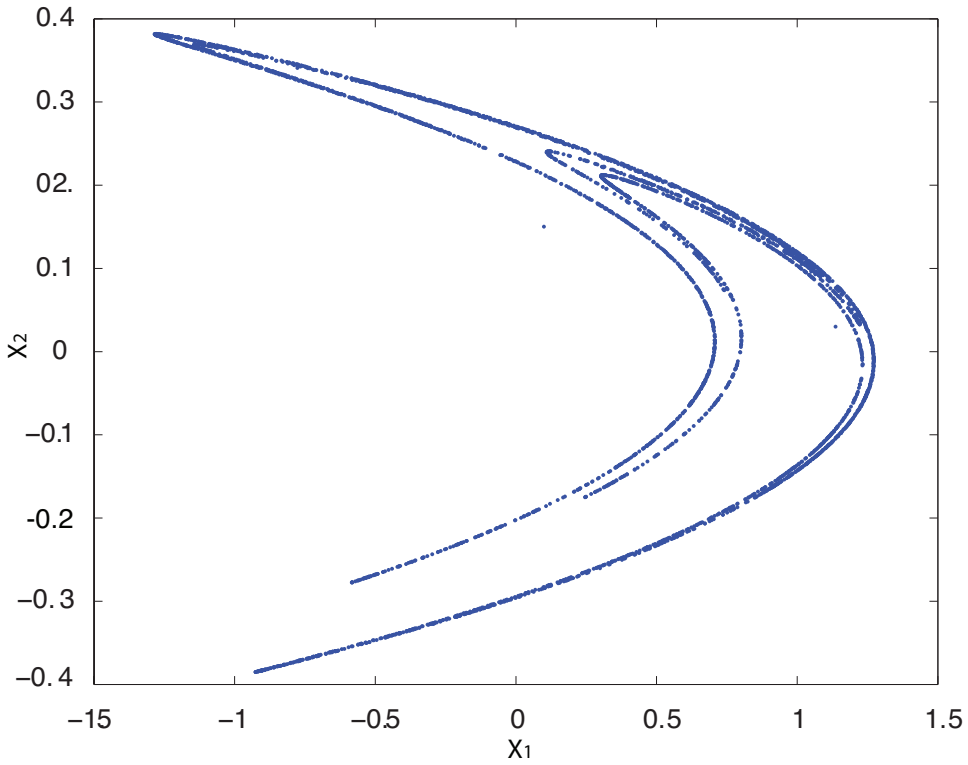


Figura 7: Atractor extraño del mapeo caótico de Hénon.

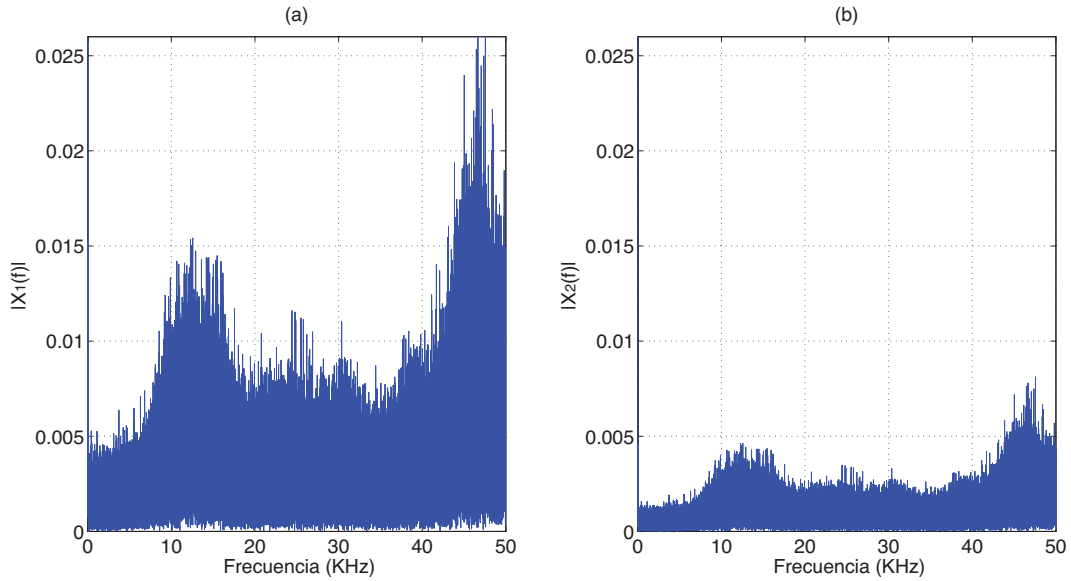


Figura 8: Espectro de frecuencias del mapeo caótico de Hénon. (a) Espectro del estado x_1, (b) Espectro del estado x_2.

negativo de -1.6224. Debido a que el mapeo de Hénon tiene al menos un exponente de Lyapunov positivo, se considera caótico (Banerjee y Verghese, 2001).

La figura 10 muestra una comparación de las curvas de autocorrelación del estado x_1 y x_2 del mapeo caótico de Hénon. Se puede observar, desde el punto de vista estadístico que los estados tienen buena complejidad, debido a que los coeficientes de autocorrelación son cercanos a cero.

La figura 11 muestra una comparación de las curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2 del mapeo caótico de Hénon, se observa que estos coeficientes de correlación son cercanos a cero, lo cual indica que no hay similitud entre los estados del mapeo de Hénon.

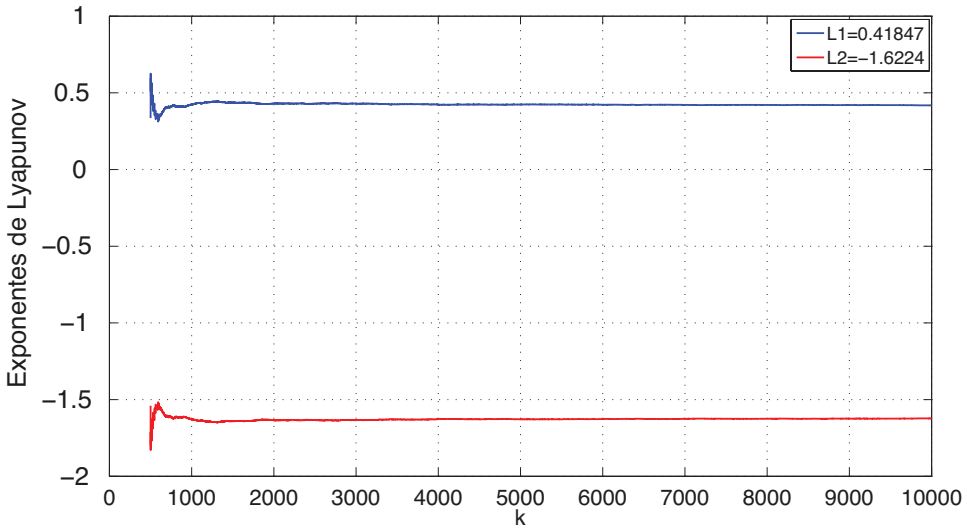


Figura 9: Exponentes de Lyapunov del mapeo de Hénon.

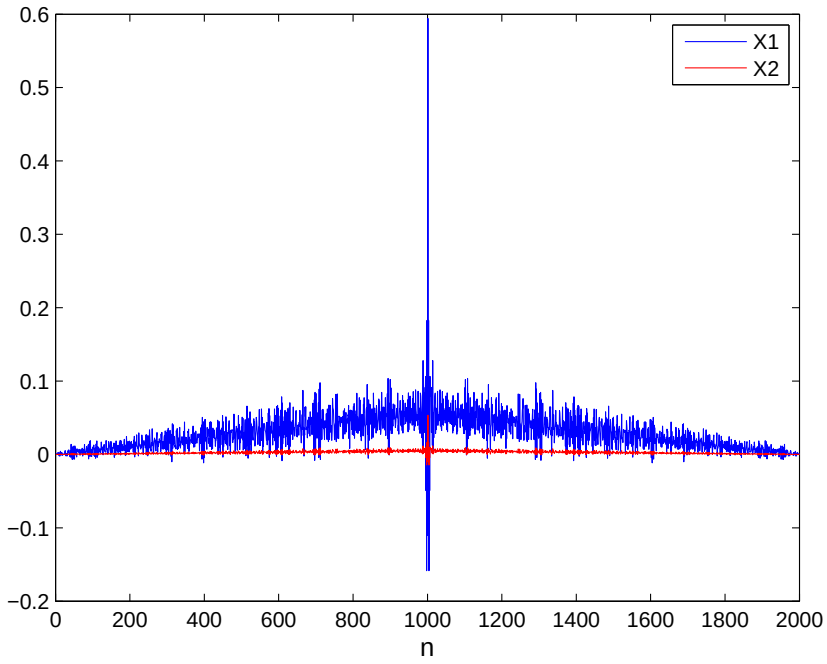


Figura 10: Comparación de las curvas de autocorrelación del estado x_1 y x_2 del mapeo caótico de Hénon.

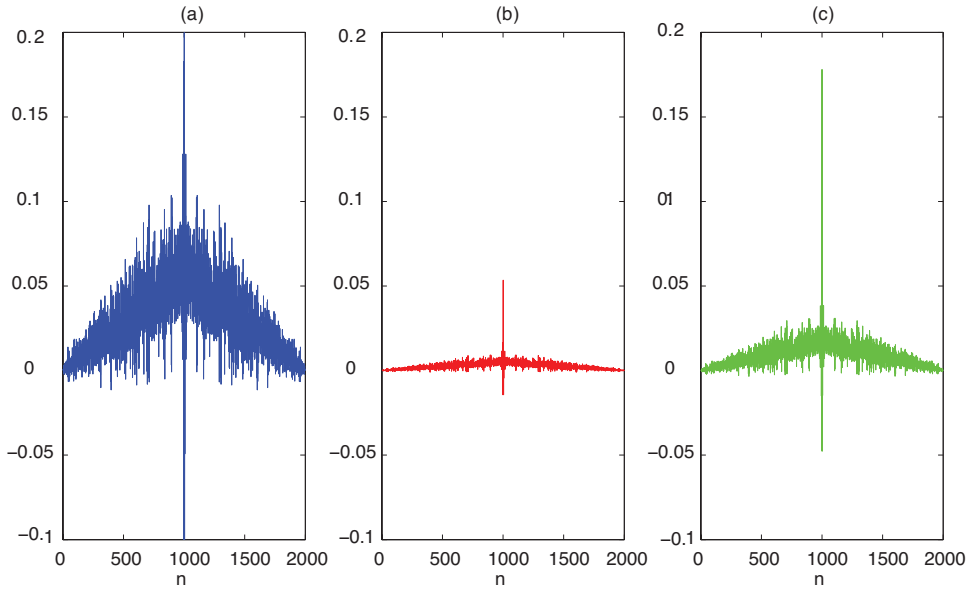


Figura 11: Curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2 del mapeo caótico de Hénon. (a) Autocorrelación estado x_1, (b) Autocorrelación estado x_2, (c) Correlación cruzada entre los estados x_1 y x_2.

Por otra parte, la figura 12 muestra el diagrama de bifurcación del mapeo caótico de Hénon con un barrido en el parámetro a, mientras que b se mantiene constante ($b = 0.3$), se puede observar que cuando el parámetro a está en el rango de $0 \leq a \leq 0.36$ el mapeo de Hénon presenta una dinámica periódica con una sóla frecuencia ó periodo 1, cuando el parámetro se encuentra en el rango de $0.36 \leq a \leq 0.90$ el mapeo de Hénon también presenta dinámica periódica, pero ahora con dos frecuencias ó periodo 2, cuando el parámetro se encuentra en el rango $0.90 \leq a \leq 1.02$ el mapeo presenta dinámica de periodo 4, cuando está en el rango $1.02 \leq a \leq 1.052$ el mapeo tiene dinámica periodo 8. El mapeo de Hénon presenta una dinámica caótica en los rangos $1.06 \leq a \leq 1.22$, $1.26 \leq a \leq 1.295$ y $1.31 \leq a \leq 1.425$, por otra parte, cuando el parámetro $a > 1.425$ el mapeo de Hénon se hace inestable, es decir se indetermina y tiende a infinito.

En la figura 13 se muestra el diagrama de bifurcación del mapeo caótico de Hénon con un barrido en el parámetro b, mientras que el parámero a se mantiene constante ($a = 1.4$), se puede observar que cuando el parámetro b se encuentra en $b = 0$, el

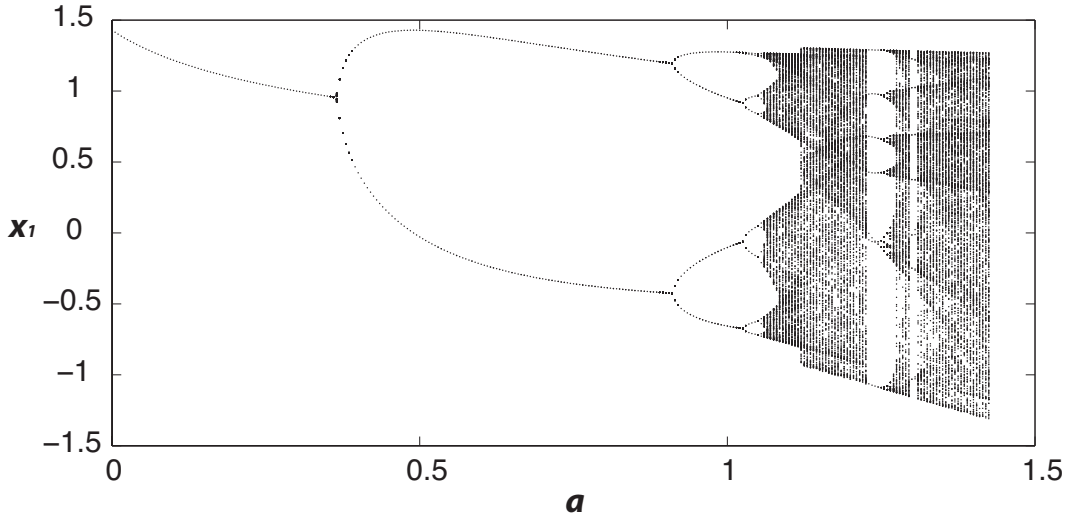


Figura 12: Diagrama de bifurcación del mapeo caótico de Hénon cuando se hace un barrido en el parámetro a, mientras que $b = 0.3$.

sistema presenta dinámica periodo 8, cuando está en el rango $0.03 \leq b \leq 0.035$ y $0.049 \leq b \leq 0.059$ se pueden observar algunos huecos, lo cual significa la ausencia de caos, por otro lado, el mapeo de Hénon presenta dinámica caótica cuando el parámetro se encuentra en el rango $0.0594 \leq b \leq 0.3132$, por último, cuando $b > 0.3131$ el mapeo de Hénon se hace inestable.

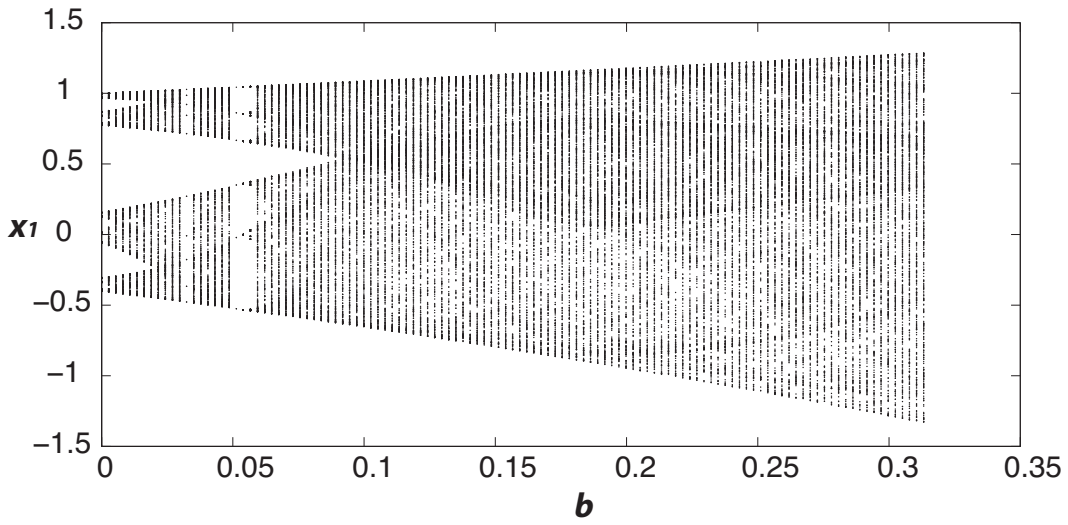


Figura 13: Diagrama de bifurcación del mapeo caótico de Hénon cuando se hace un barrido en el parámetro b, mientras que $a = 1.4$.

II.2.2 Mapeo hipercaótico de Chen

Este mapeo está descrito por el siguiente conjunto de ecuaciones en diferencias (Chen, 2001; Aguilar-Bustos y Cruz-Hernández, 2009):

$$\begin{aligned} x_1(k+1) &= 1 - a(x_1^2(k) + x_2^2(k)), \\ x_2(k+1) &= -2abx_1(k)x_2(k). \end{aligned} \tag{4}$$

Con $a = 1.95$ y $b = 1$, el mapeo de Chen exhibe una dinámica hipercaótica (Chen, 2001). En la figura 14 se muestra el par de señales caóticas en tiempo discreto generadas con este modelo y utilizando las siguientes condiciones iniciales: $x_1(0) = 0.025$ y $x_2(0) = 0.025$. En la figura 15, se presenta el atractor extraño del mapeo hipercaótico de Chen obtenido con la simulación numérica en Matlab, se puede observar que tiene muy buena dispersión en el plano de fase, lo cual es deseable en todo sistema caótico y por lo tanto cuando se aplica a un sistema criptográfico garantiza buen nivel de seguridad.

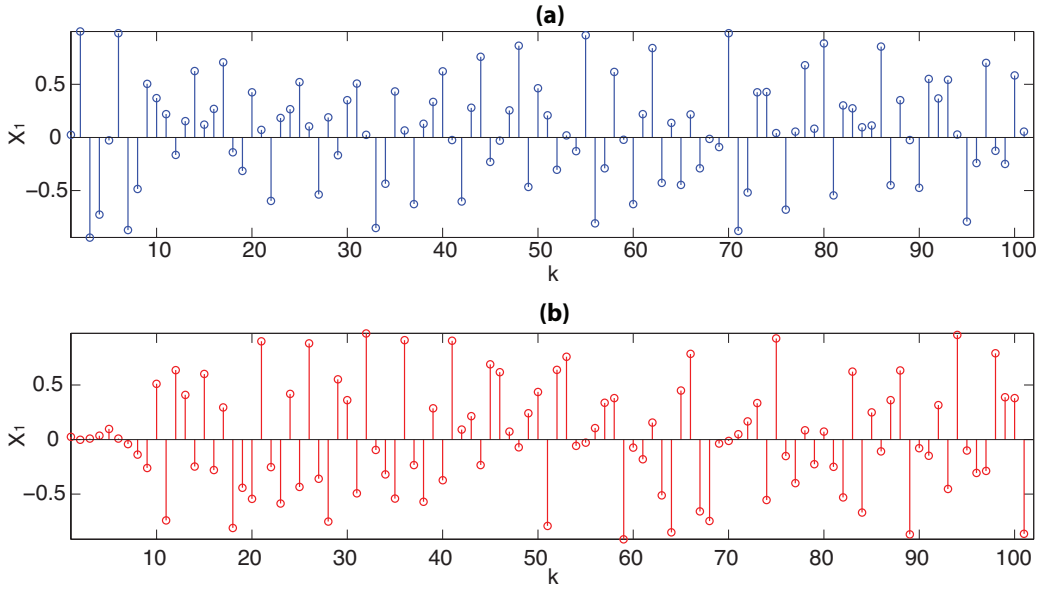


Figura 14: Señales en tiempo discreto obtenidas con el mapeo hipercaótico de Chen.

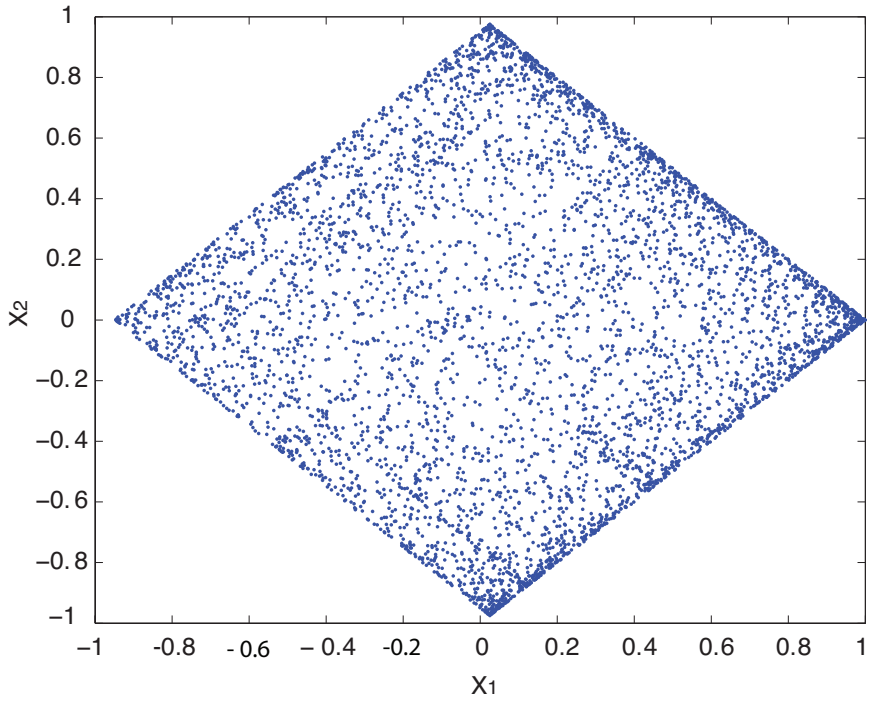


Figura 15: Atractor extraño del mapeo hipercaótico de Chen.

En la figura 16 se muestra el espectro de frecuencias de los estados x_1 y x_2 del mapeo hipercaótico de Chen. Se puede observar que ambos espectros contienen componentes espectrales muy similares en magnitud y frecuencia, además se observa que el espectro de frecuencias de las trayectorias es continuo, por lo tanto son hipercaóticas (Andrievskii y Fradkov, 2003).

La figura 17 muestra los exponentes de Lyapunov del mapeo hipercaótico de Chen calculados con el método reportado en (Wolf *et al.*, 1985; Briggs, 1990), se puede observar que $\lambda_1 = 0.44185$ y $\lambda_2 = 0.43275$, por lo tanto, debido a que los dos exponentes son positivos, el sistema de Chen es hipercaótico (Chen, 2001).

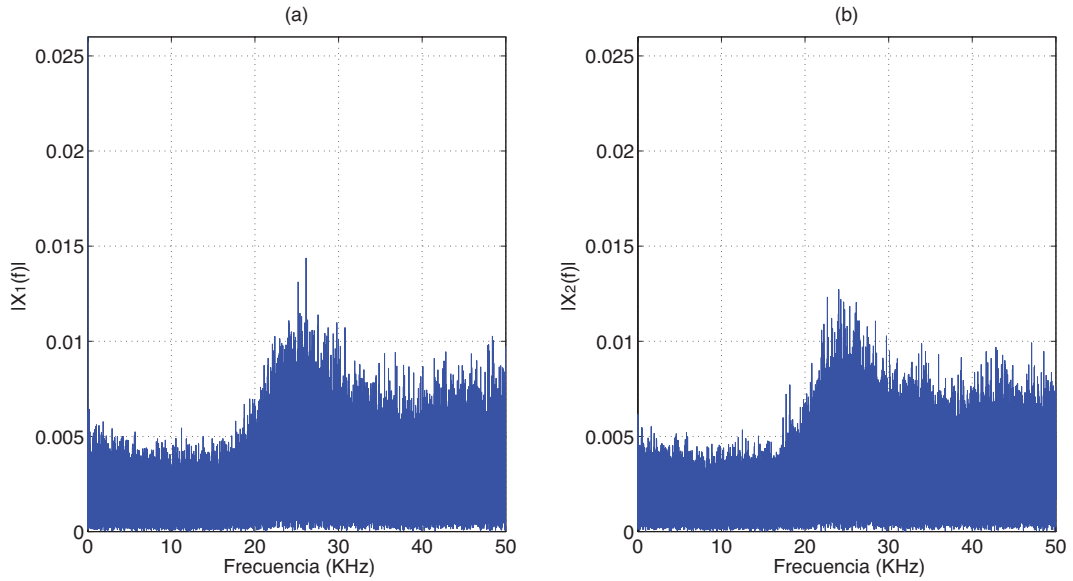


Figura 16: Espectro de frecuencias del mapeo hipercaótico de Chen. (a) Espectro del estado x_1, (b) Espectro del estado x_2.

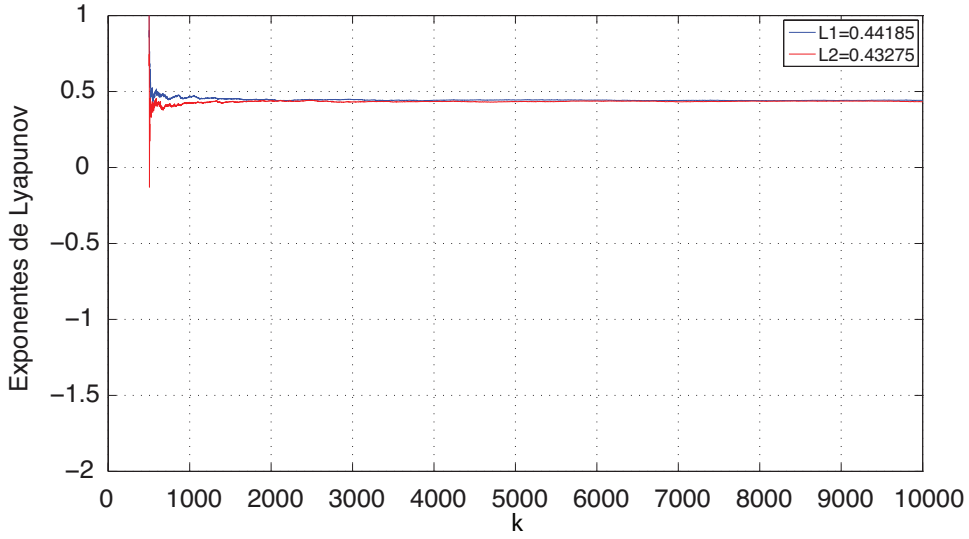


Figura 17: Exponentes de Lyapunov del mapeo hipercaótico de Chen.

La figura 18 muestra una comparación de las curvas de autocorrelación del estado x_1 y x_2 del mapeo hipercaótico de Chen, tal como se observa en la figura 18, los coeficientes de autocorrelación son muy cercanos a cero, lo que significa que no existe similitud entre los estados del mapeo de Chen, por lo tanto, estas secuencias hipercaóticas generadas por este mapeo presentan buenas propiedades estadísticas para utilizarse en aplicaciones de encriptado/desencriptado de información biométrica. Se puede observar que los estados x_1 y x_2 del mapeo de Chen tienen mayor complejidad con respecto a los estados x_1 y x_2 del mapeo de Hénon.

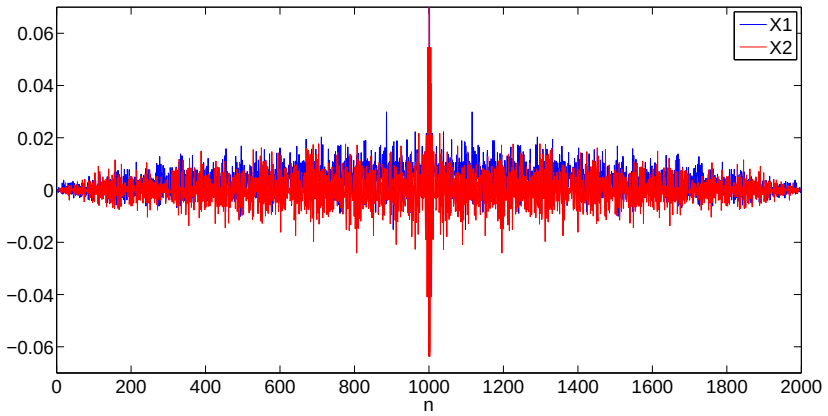


Figura 18: Comparación de las curvas de autocorrelación del estado x_1 y x_2 del mapeo hipercaótico de Chen.

La figura 19 muestra una comparación de las curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2 del mapeo hipercaótico de Chen, se puede observar que tanto los coeficientes de autocorrelación, así como los de correlación cruzada son muy cercanos a cero, por lo tanto, no existe similitud entre los estados del mapeo hipercaótico de Chen.

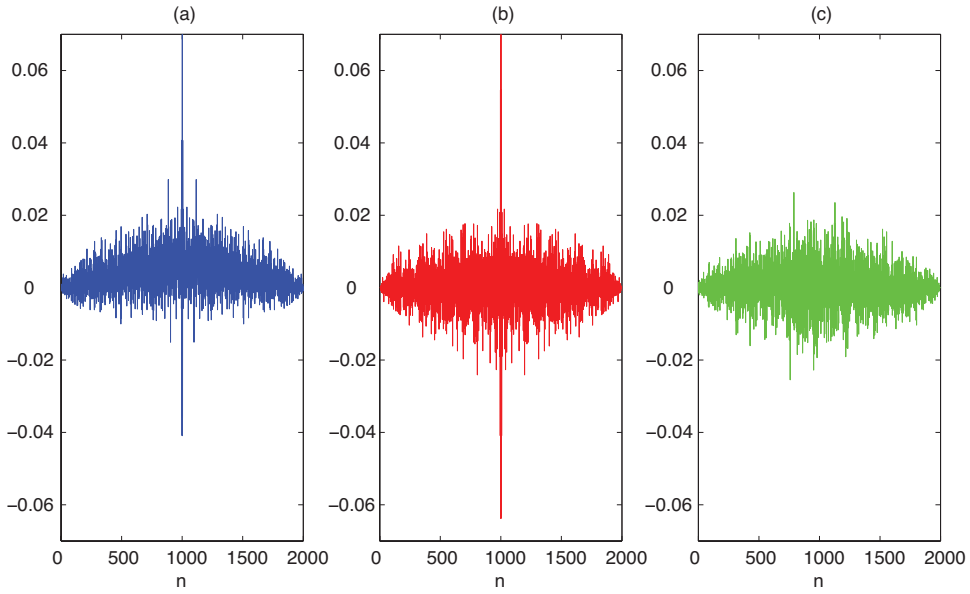


Figura 19: Curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2 del mapeo hipercaótico de Chen. (a) Autocorrelación estado x_1, (b) Autocorrelación estado x_2, (c) Correlación cruzada entre los estados x_1 y x_2.

En la figura 20 muestra el diagrama de bifurcación del mapeo hipercaótico de Chen con barrido en el parámetro a, mientras que el parámetro b se mantiene constante ($b = 1$), se observa que cuando el parámetro $a > 1.41$ el mapeo presenta dinámica hipercaótica, cuando el parámetro a está dentro del rango $0 < a < 1.41$ el mapeo de Chen presenta dinámicas de periodo 1, periodo 2, periodo 4 y periodo 8, tal como se muestra en la figura 20.

En la figura 21 se muestra el diagrama de bifurcación del mapeo hipercaótico de Chen con barrido en el parámetro b, mientras que el parámetro a se mantiene constante ($a = 1.95$), se observa que cuando el parámetro b está en el rango $0 - 0.605$ y $0.8 - 1.05$ el mapeo de Chen también presenta dinámica hipercaótica. Cuando el parámetro b está en el rango $0.605 \leq b \leq 0.8$ y $b > 1.05$ se observan unos huecos, los cuales indican la ausencia de caos.

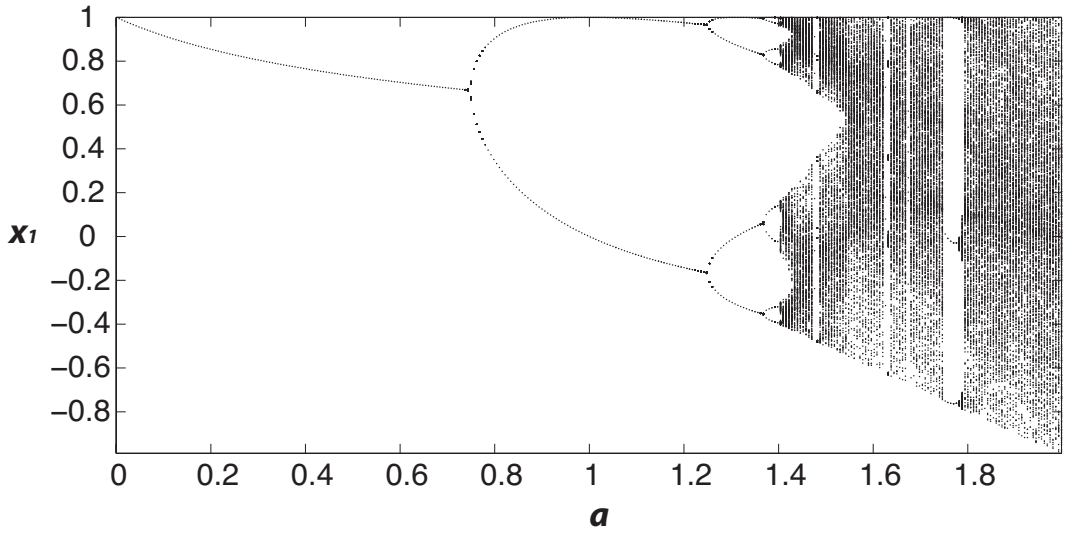


Figura 20: Diagrama de bifurcación del mapeo hipercaótico de Chen cuando se hace un barrido en el parámetro a, mientras que $b = 1$.

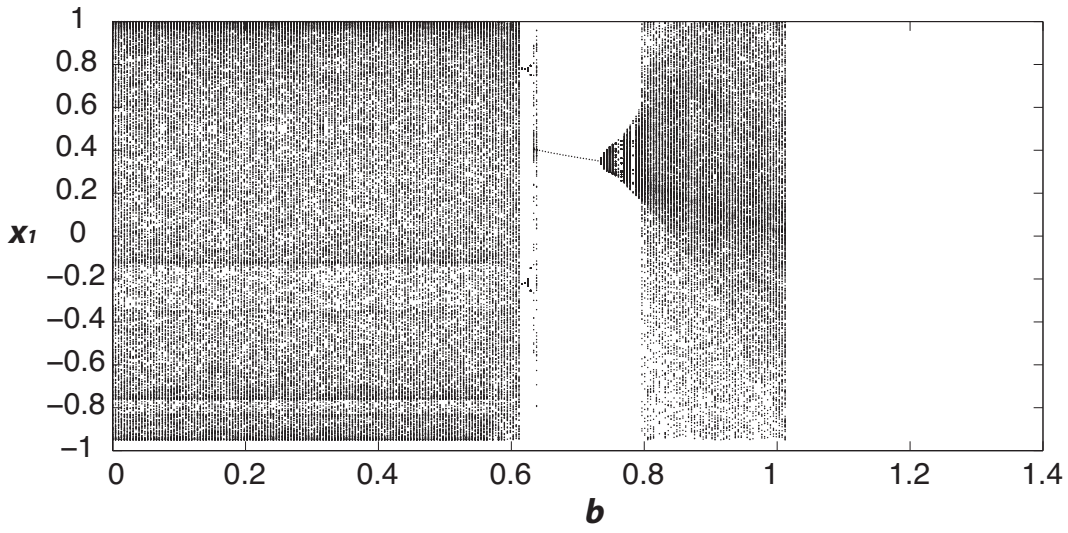


Figura 21: Diagrama de bifurcación del mapeo hipercaótico de Chen cuando se hace un barrido en el parámetro b, mientras que el parámetro $a = 1.95$.

II.2.3 Mapeo hipercaótico de Rössler

El mapeo hipercaótico de Rössler es modelado por las siguientes ecuaciones en diferencias (Itoh *et al.*, 2001; Aguilar-Bustos *et al.*, 2008):

$$\begin{aligned} x_1(k+1) &= \alpha x_1(k)(1-x_1(k)) - \beta(x_3+\gamma)(1-2x_2(k), \\ x_2(k+1) &= \delta x_2(k)(1-x_2(k)) + \zeta x_3(k), \\ x_3(k+1) &= \eta((x_3(k)+\gamma)(1-2x_2(k))-1)(1-\theta x_1(k)), \end{aligned} \tag{5}$$

con el conjunto de parámetros $\alpha = 0.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.2$, $\eta = 0.1$ y $\theta = 1.9$, el sistema (5) exhibe dinámicas hipercaóticas (Itoh *et al.*, 2001). En la figura 22, se muestran los tres estados hipercaóticos (x_1, x_2 y x_3) generados con este mapeo, las condiciones iniciales utilizadas son: $x_1(0) = 0.1$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$. En la figura 23, se presenta el atractor extraño producido por el mapeo de hipercaótico de Rössler y obtenido con una simulación numérica en Matlab, se observa que ocupa un espacio tri-dimensional en el diagrama de fase, lo cual es muy deseable en un modelo hipercaótico.

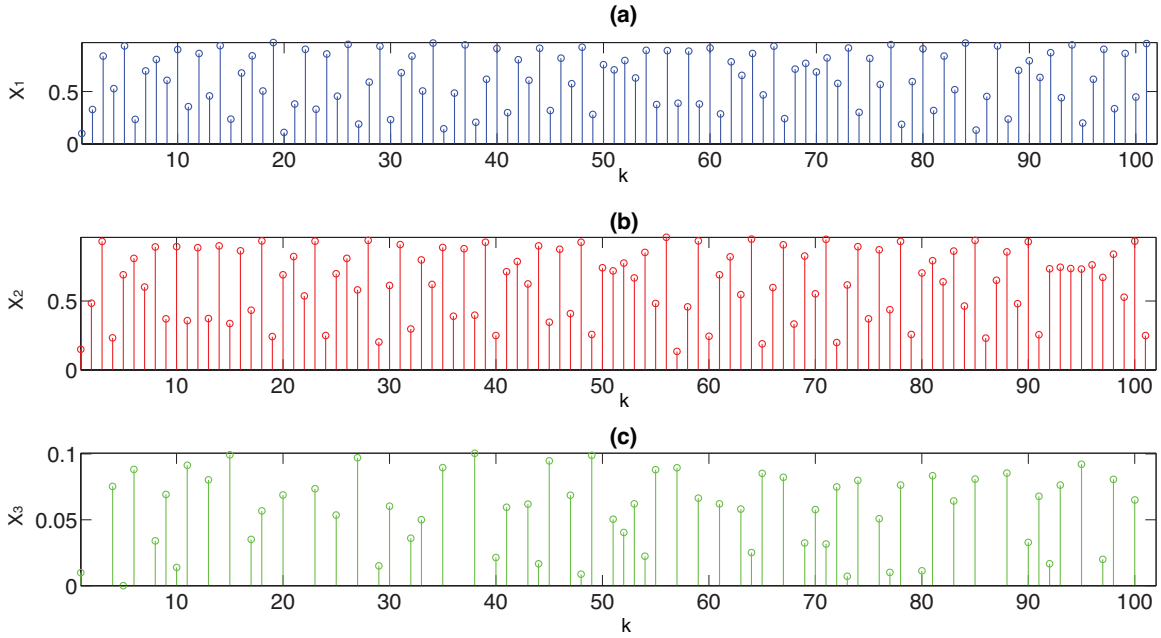


Figura 22: Señales en tiempo discreto obtenidas con el mapeo hipercaótico de Rössler. (a) Estado x_1, (b) estado x_2, (c) estado x_3.

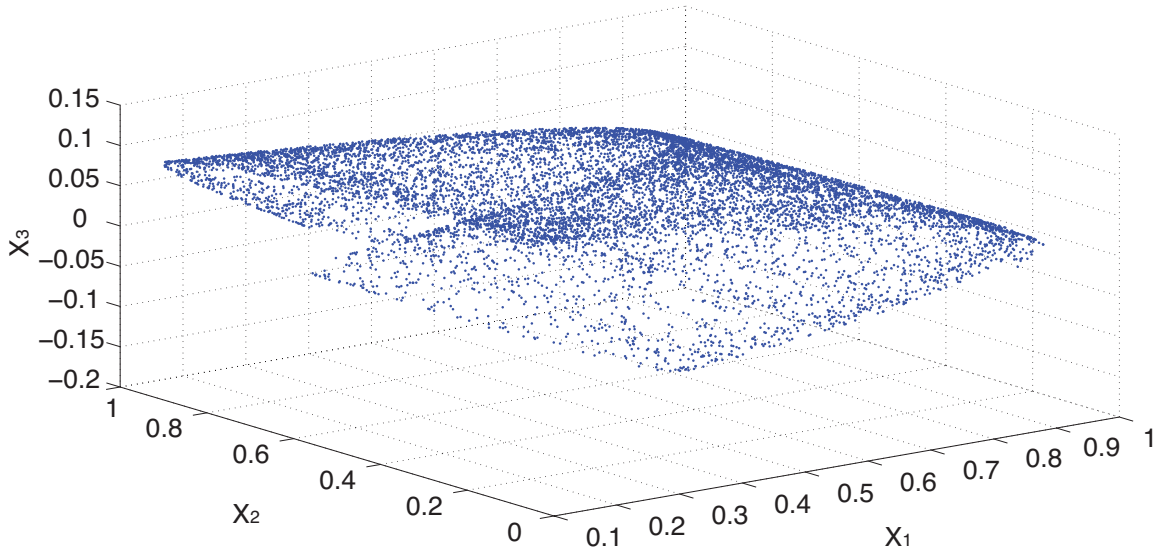


Figura 23: Atractor extraño del mapeo hipercaótico de Rössler.

En la figura 24 se muestra el espectro de frecuencias de los estados x_1, x_2 y x_3 del mapeo de hipercaótico de Rössler. Se puede observar que los estados x_1 y x_2 poseen componentes espectrales muy similares y se observa que predominan las frecuencias mayores a los 30 KHz, mientras que el estado x_3 contiene componentes espectrales de amplitud pequeña, también se observa que el espectro de frecuencias de las trayectorias es continuo, por lo tanto son hipercaóticas (Andrievskii y Fradkov, 2003).

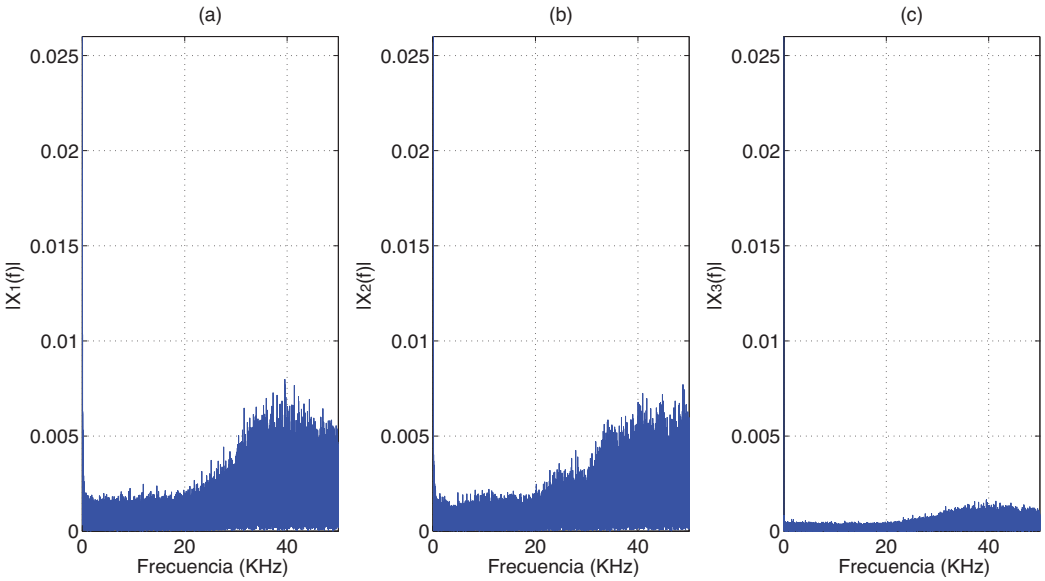


Figura 24: Espectro de frecuencias del mapeo hipercaótico de Rössler. (a) Espectro del estado x_1, (b) Espectro del estado x_2, (c) Espectro del estado x_3.

La figura 25 muestra los exponentes de Lyapunov del mapeo hipercaótico de Rössler obtenidos con el método reportado en (Wolf *et al.*, 1985; Briggs, 1990), en esta figura se puede observar que el exponente más positivo es λ_1 (color azul) y tiene un valor aproximado de 0.313879 y λ_2 (color verde) tiene un valor aproximado de 0.019228. Como el sistema tiene dos exponentes positivos, con esto se muestra que es hipercaótico (Itoh *et al.*, 2001). El tercer exponente de Lyapunov λ_3 (color rojo) es negativo y tiene un valor aproximado de -0.010713 . La figura 26 muestra un acercamiento a estos mismos exponentes.

Los mapeos hipercaóticos están teóricamente probados que tienen buena aleatoriedad, periodo infinito e impredicibilidad a largo plazo. Estos mapeos complejos usualmente están definidos como un sistema caracterizado con al menos dos exponentes de Lyapunov positivos, los cuales proveen formas de ondas más complejas que los mapeos caóticos sencillos. En consecuencia, estos mapeos hipercaóticos tienen las características de alta capacidad, alta seguridad y alta eficiencia (Cruz-Hernández y Martynyuk, 2010).

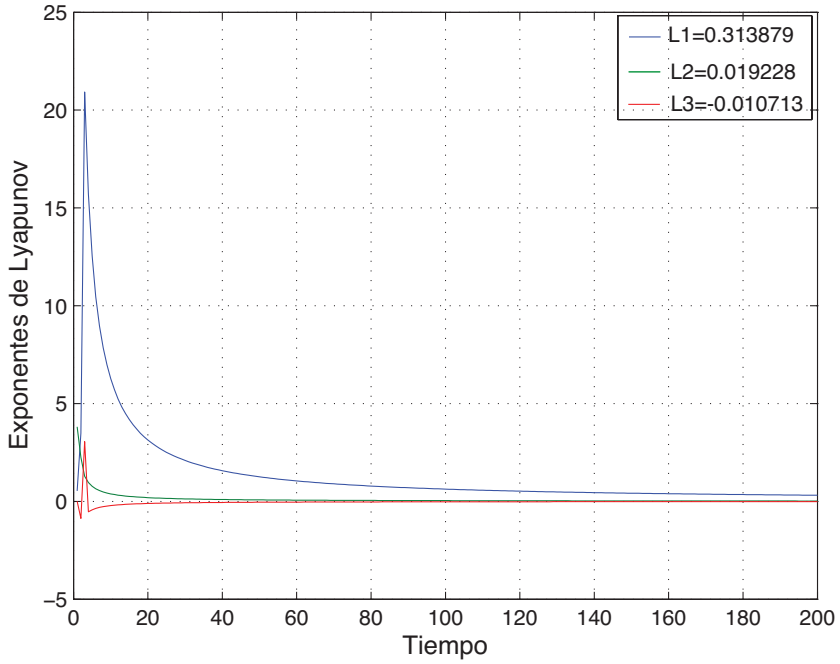


Figura 25: Exponentes de Lyapunov del mapeo hipercaótico de Rössler.

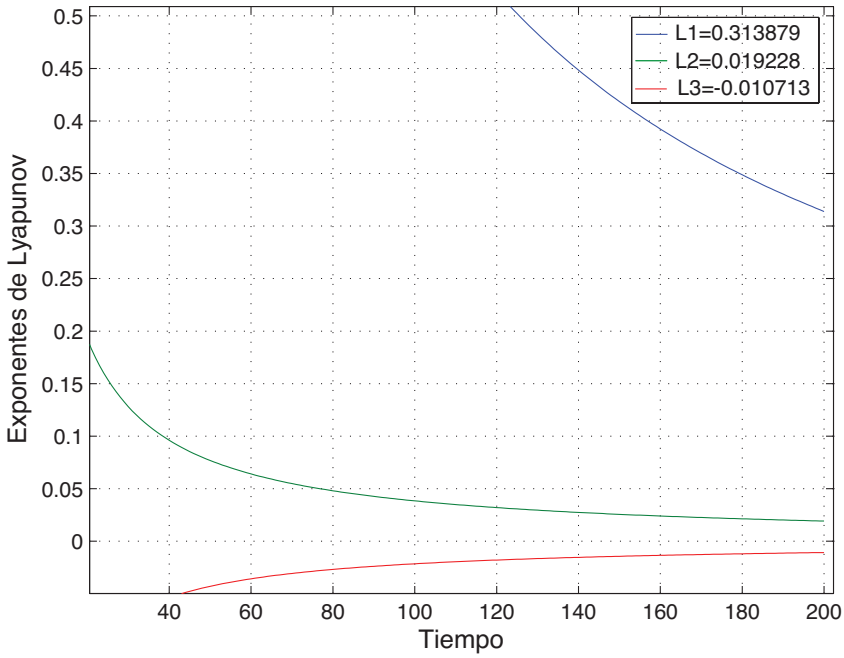


Figura 26: Acercamiento a los exponentes de Lyapunov del mapeo hipercaótico de Rössler.

La figura 27 muestra una comparación de las curvas de autocorrelación de los estados x_1, x_2 y x_3 del mapeo hipercaótico de Rössler. Se puede ver que los coeficientes de autocorrelación de los estados x_1, x_2 y x_3 son cercanos a cero, específicamente el correspondiente a x_3, sin embargo, x_1 y x_2 tienen un poco más de similitud entre ellos.

La figura 28 muestra una comparación de las curvas de correlación cruzada de los estados x_1 vs x_2, x_1 vs x_3 y x_2 vs x_3 del mapeo hipercaótico de Rössler, se puede observar que las combinaciones x_1 vs x_3 y x_2 vs x_3 son las que presentan la mejor correlación cruzada.

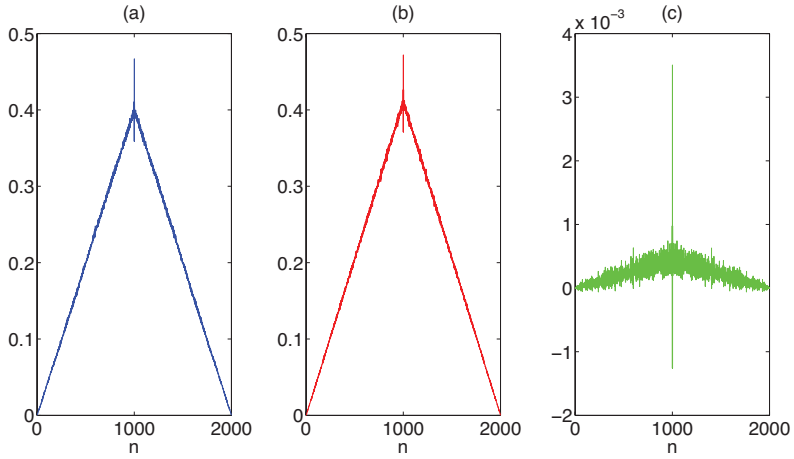


Figura 27: Comparación de las curvas de autocorrelación de los estados x_1, x_2 y x_3 del mapeo hipercaótico de Rössler.

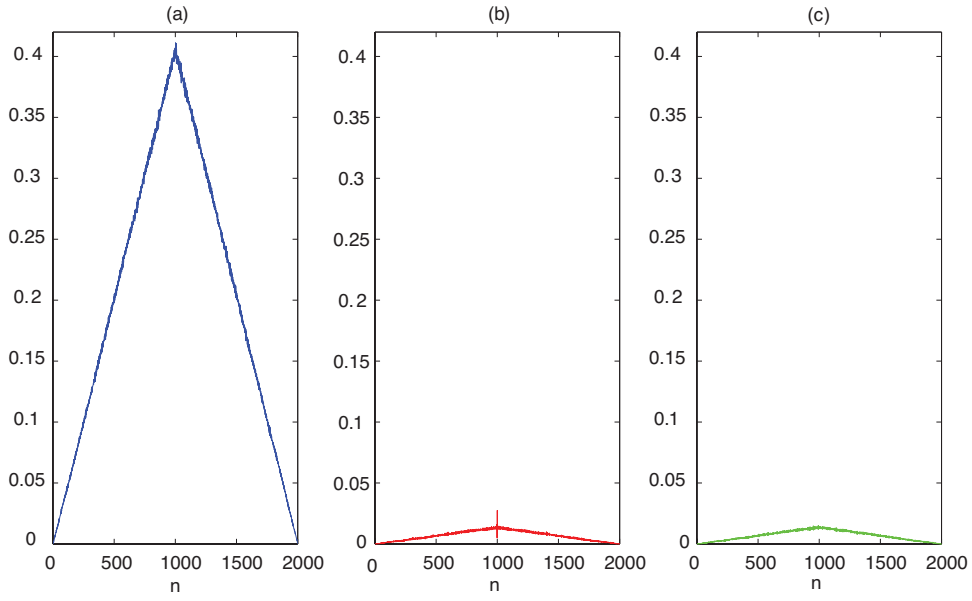


Figura 28: Comparación de las curvas de correlación cruzada de los estados x_1 vs x_2, x_1 vs x_3 y x_2 vs x_3 del mapeo hipercaótico de Rössler.

En la figura 29 se muestra el diagrama de bifurcación del mapeo hipercaótico de Rössler con barrido en el parámetro α, mientras que los demás parámetros se mantienen fijos con los valores indicados anteriormente, se observa que cuando el parámetro α está en el rango $3.5 \leq \alpha \leq 3.9$ el mapeo presenta dinámica hipercaótica, sin embargo, cuando el parámetro $\alpha > 3.90$, el mapeo de Rössler se hace inestable.

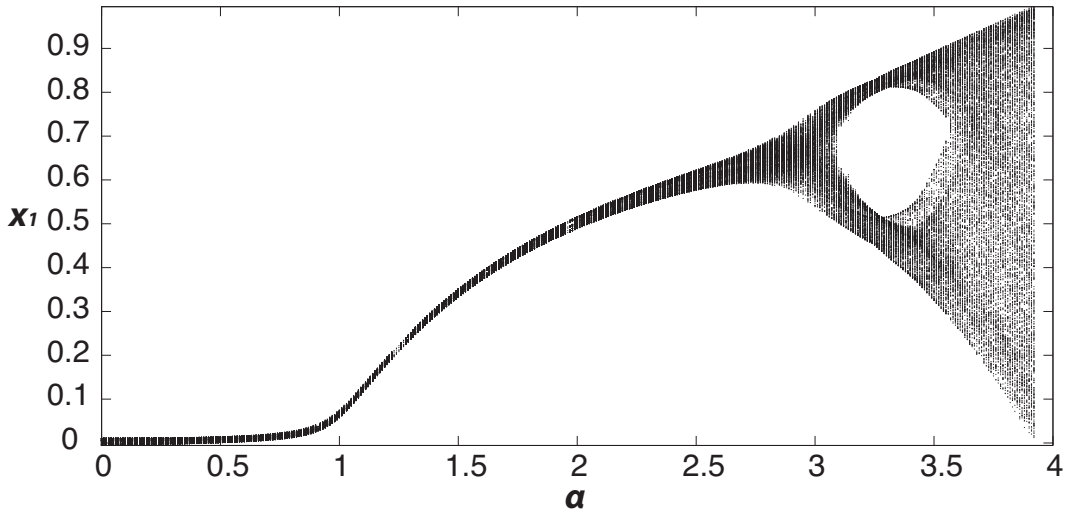


Figura 29: Diagrama de bifurcación del mapeo hipercaótico de Rössler cuando se hace un barrido en el parámetro α, mientras que los otros parámetros se mantienen fijos.

En la figura 30 se muestra el diagrama de bifurcación del mapeo hipercaótico de Rössler con barrido en el parámetro β (los demás parámetros se mantienen fijos), se observa que cuando el parámetro β está en el rango $0 \leq \beta \leq 0.12$ el mapeo presenta dinámica hipercaótica, cuando el parámetro $\beta > 0.12$ el mapeo se hace inestable.

En la figura 31 se muestra el diagrama de bifurcación del mapeo hipercaótico de Rössler con barrido en el parámetro θ (los demás parámetros se mantienen fijos), se observa que cuando el parámetro θ está en el rango $0 \leq \theta \leq 3.3$ el mapeo presenta dinámica hipercaótica, cuando el parámetro $\theta > 3.3$ el mapeo se hace inestable.

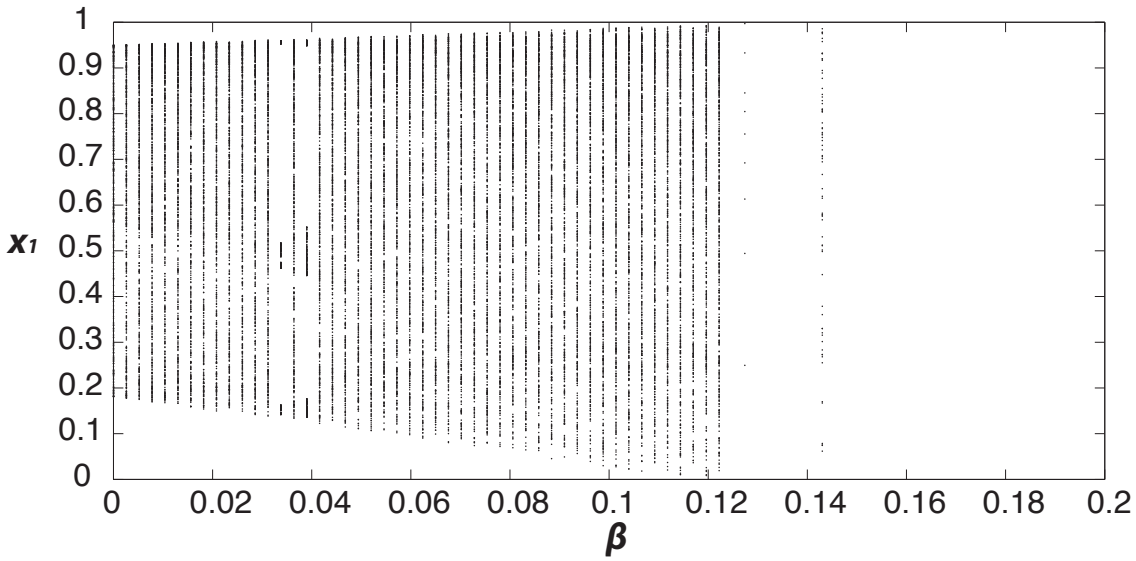


Figura 30: Diagrama de bifurcación del mapeo hipercaótico de Rössler cuando se hace un barrido en el parámetro β, los otros parámetros se mantienen fijos.

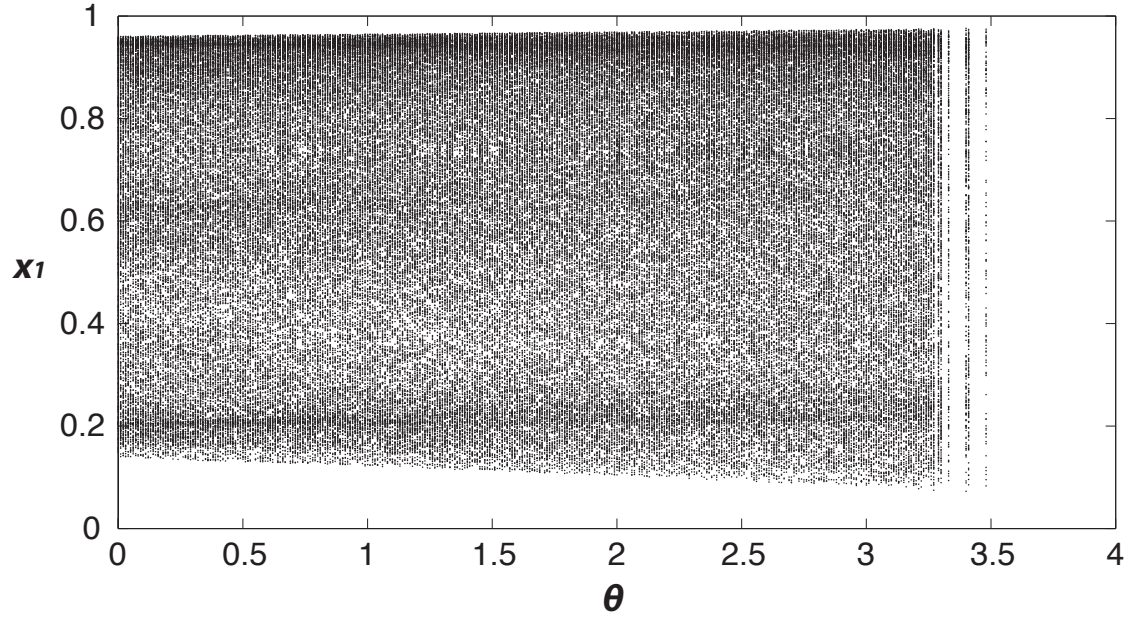


Figura 31: Diagrama de bifurcación del mapeo hipercaótico de Rössler cuando se hace un barrido en el parámetro θ, los otros parámetros se mantienen fijos.

II.2.4 Mapeo caótico del gato de Arnold

Este sistema está compuesto por dos ecuaciones en diferencias (Isaeva *et al.*, 2006):

$$p_{(n+1)} = p_n + q_n \ \ (mod\ N),$$
$$q_{(n+1)} = p_n + 2q_n \ \ (mod\ N). \tag{6}$$

Al sistema representado por la ec. (6), se le conoce como gato de Arnold, debido al uso de una imagen con la cara de un gato para explicaciones de ciertas acciones de este mapeo en artículos y libros de texto de Arnold (Arnold y Avez, 1968; Arnold, 1988). El mapeo de la ec. (6) es un sistema conservativo, es decir cualquier dominio en el plano (p, q), conserva su área bajo iteración. Es bien conocido que el mapeo (6) genera dinámicas caóticas en el sentido de la teoría hiperbólica de Smale y Anosov (Smale, 1967). Sus exponentes de Lyapunov son $\lambda_1 = 0.9624$ y $\lambda_2 = -0.9624$, el exponente mayor es positivo, por lo tanto se refleja la presencia de una sensibilidad exponencial con respecto a las condiciones iniciales, el cual es una de las principales características del caos (Isaeva *et al.*, 2006). La figura 32 muestra la dinámica en tiempo discreto de los estados x_1 y x_2 generadas por el mapeo del gato de Arnold, empleando las condiciones iniciales $x_1(0) = 0.1$ y $x_2(0) = 0.2$ y el parámetro $N = 1$. En la figura 33, se presenta el atractor extraño de este mismo mapeo, se puede observar que toda la dinámica se dispersa en todo el plano de fase, lo cual es muy deseable en todo sistema caótico, esto quiere decir que el mapeo gato de Arnold tiene una dinámica muy compleja, debido a la gran similitud con un sistema aleatorio, esta gran dispersión en el plano de fase, beneficia a un sistema criptográfico al proporcionar una mejor entropía de información o aleatoriedad a la información encriptada.

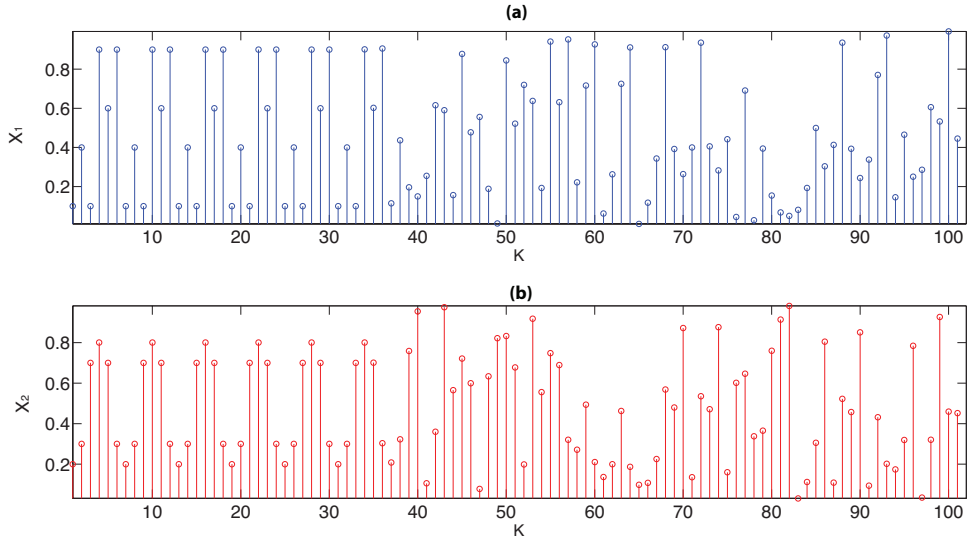


Figura 32: Señales caóticas en tiempo discreto obtenidas con el mapeo Gato de Arnold.

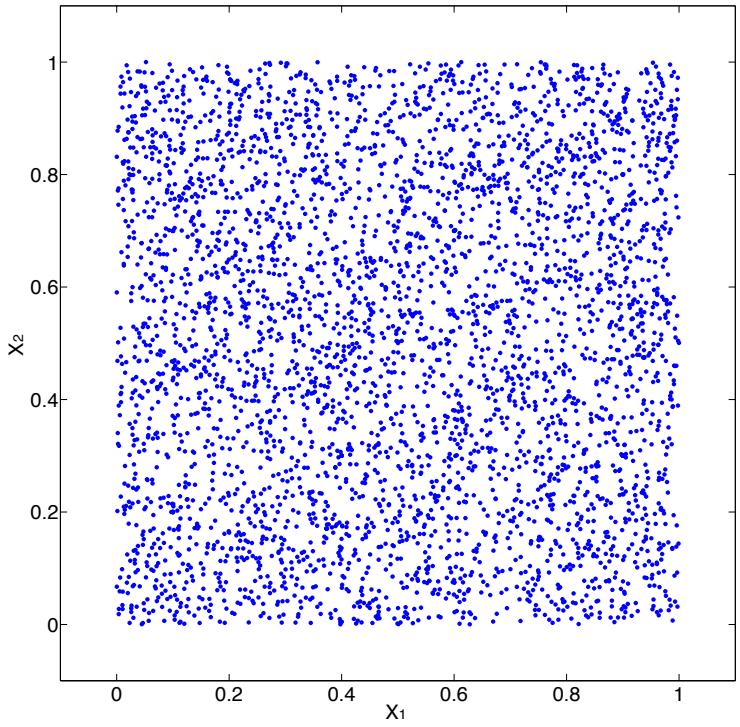


Figura 33: Atractor extraño del mapeo Gato de Arnold.

La figura 34 muestra el espectro en frecuencias del mapeo gato de Arnold, se observa que tiene una distribución uniforme en frecuencias con magnitudes similares, lo cual lo hace un buen mapeo para ser empleado en sistemas criptográficos. Además se puede observar que el espectro de frecuencias de las trayectorias es continuo, por lo tanto son caóticas (Andrievskii y Fradkov, 2003)

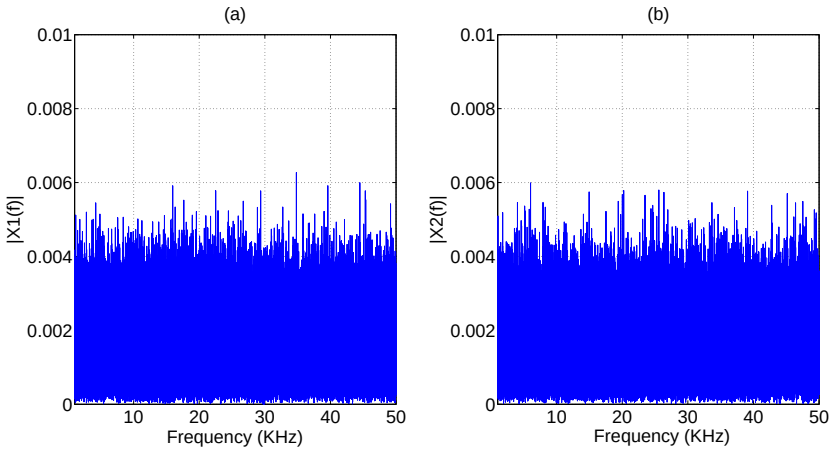


Figura 34: Espectro de frecuencias del mapeo gato de Arnold. (a) Espectro del estado x_1, (b) espectro del estado x_2.

La figura 35 muestra una comparación de las curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2, del mapeo gato de Arnold, se puede observar que tanto los coeficientes de autocorrelación como los de correlación cruzada están dentro del rango $0 - 0.26$.

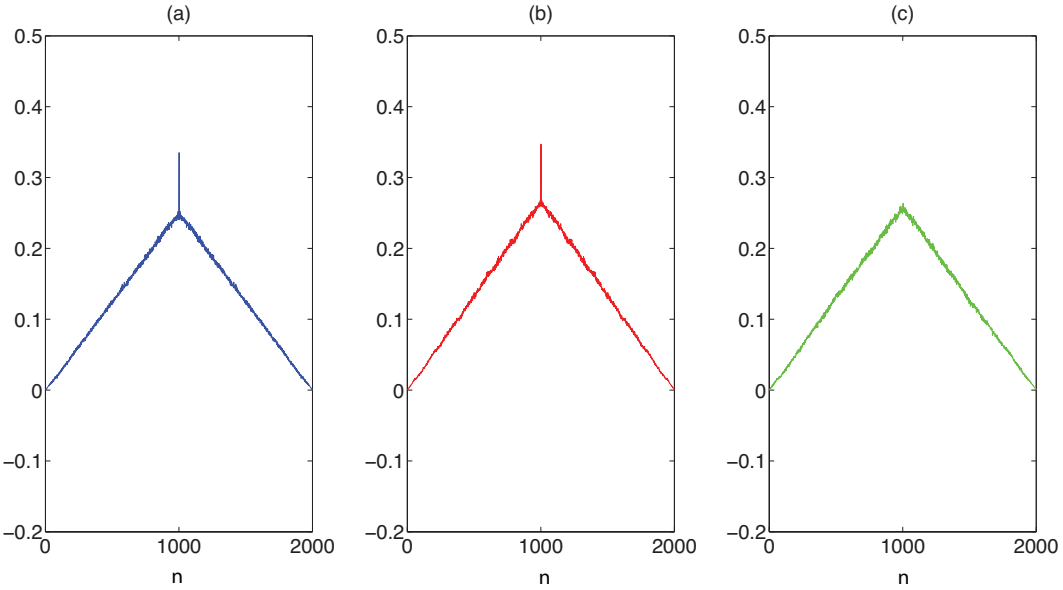


Figura 35: Curvas de autocorrelación y correlación cruzada de los estados x_1 y x_2 del mapeo gato de Arnold. (a) Autocorrelación estado x_1, (b) Autocorrelación estado x_2, (c) correlación cruzada entre los estados x_1 y x_2.

La figura 36 muestra el diagrama de bifurcación del mapeo caótico gato de Arnold con barrido en el parámetro N, se observa que cuando el parámetro está en el rango $1 \leq N \leq 40$ el mapeo presenta dinámica caótica, además se puede observar que conforme incrementa el valor de N, se incrementa directamente la cantidad de frecuencias, sin embargo, cuando el parámetro $N > 40$ el mapeo se hace inestable.

II.3 Revisión bibliográfica

II.3.1 Encriptado caótico

En la literatura actual, se reportan muchos trabajos sobre encriptado de imágenes empleando caos e hipercaos, por ejemplo en el año 2004, (Chen *et al.*, 2004) proponen un esquema de encriptado simétrico de imágenes basado en mapeo caótico de 3D, también llamado *3D cat map*, básicamente realizan una generalización del mapeo *cat map* de dos dimensiones a uno de 3D, para diseñar un esquema de encriptado seguro y que opere en

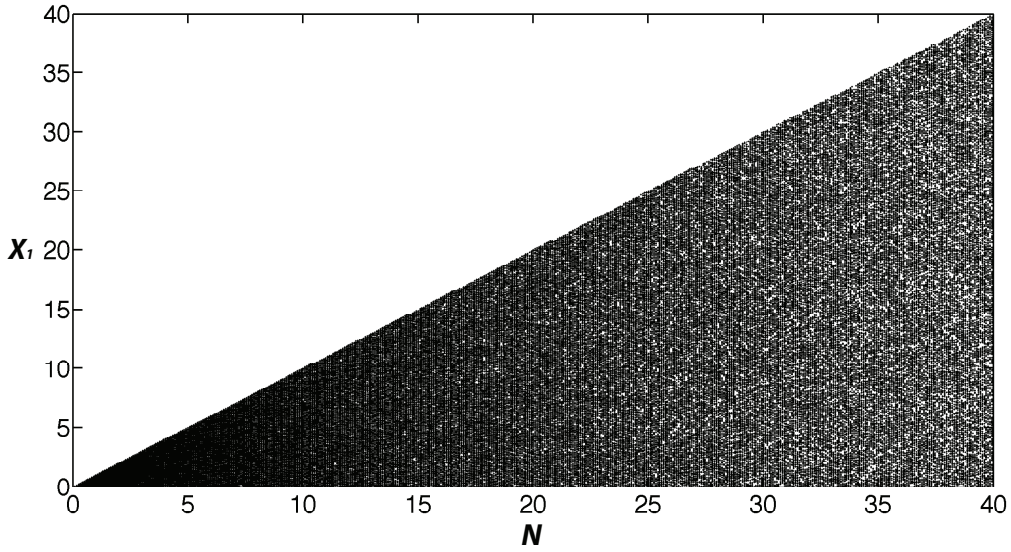


Figura 36: Diagrama de bifurcación del mapeo caótico gato de Arnold cuando se hace un barrido en el parámetro N.

tiempo real, este esquema emplea el mapeo cat 3D para revolver las posiciones y niveles de grises de los pixeles de la imagen original, y utilizan otro mapeo caótico para confundir la relación entre la imagen encriptada y la imagen original. Mediante resultados experimentales demuestran la alta seguridad y una velocidad rápida de encriptado del esquema que ellos proponen (Chen *et al.*, 2004). En el año 2005, (Zhang *et al.*, 2005), presentan una técnica de encriptado de imágenes basada en mapeos caóticos, mencionan que los métodos de encriptado convencional no pueden ser aplicados a imágenes, debido a la alta redundancia, correlación, estructura local y las características de amplitud - frecuencia de los pixeles. En ese artículo, ellos mejoran las propiedades en términos de confusión y difusión del mapeo caótico exponencial discreto, y diseñan un esquema clave para resistir ataques de tipo: estadístico, diferenciales y código de grises, sus resultados experimentales muestran que el esquema presentado es eficiente y muy seguro (Zhang *et al.*, 2005). Un año después, (Gao *et al.*, 2006) presentan un nuevo algoritmo caótico para el encriptado de imágenes, mencionan que los sistemas

criptográficos caóticos de una dimensión, tienen espacio de clave pequeño y seguridad débil, por tal motivo, proponen un nuevo algoritmo caótico no-lineal (NCA) el cual utiliza función potencia y tangente en vez de una función lineal, sus resultados experimentales demuestran que tienen la ventaja de un gran espacio de claves y alto nivel de seguridad, manteniendo al mismo tiempo una eficiencia aceptable (Gao *et al.*, 2006). En el año 2007, (Behnia *et al.*, 2007), proponen el trabajo, un esquema de encriptado caótico rápido basado en mapeo caótico no-lineal por segmentos (Behnia *et al.*, 2007). Posteriormente (Behnia *et al.*, 2008) reportaron el trabajo, un nuevo algoritmo para el encriptado de imágenes basado en la mezcla de mapeos caóticos, en este caso emplean criptografía de clave simétrica, utilizan el mapeo acoplado, el cual es mezclado con otro mapeo caótico uni-dimensional y es usado para el encriptado de imágenes con alto grado de seguridad, con una velocidad aceptable, los experimentos presentados aprueban la efectividad del método que proponen y la implementación del algoritmo, esta mezcla de mapeos caóticos tiene la ventaja de tener un gran espacio de claves y alto nivel de seguridad. En el año 2010,(Zhang *et al.*, 2010), presentan el artículo, encriptado de imágenes usando adición DNA en combinación con mapeos caóticos, con base en simulación de resultados experimentales y al análisis de seguridad que realizan, mencionan que es un buen encriptado y además puede resistir contra ataques: de fuerza bruta, estadísticos y diferenciales (Zhang *et al.*, 2010). En el año 2011, (Patidar *et al.*, 2011) proponen el trabajo, un esquema robusto y seguro para el encriptado caótico de imágenes basado en substitución y permutación pseudo aleatoria, evalúan la seguridad y desempeño del algoritmo mediante el uso de histogramas, coeficientes de correlación, entropía de la información, análisis de sensibilidad a la clave, análisis diferenciales, análisis de espacio de claves y análisis de tasa de encriptado/desencriptado, esos resultados sugieren que el algoritmo que proponen es robusto y seguro, y que puede ser utilizado para aplicaciones de comunicaciones seguras de imágenes y videos (Patidar *et al.*, 2011). En este

mismo año, (Fu *et al.*, 2011), presentan el trabajo, un esquema original de encriptado de imágenes digitales, basado en caos y en permutación a nivel de bit, los resultados que obtienen con los distintos tipos de análisis, son interesantes e indican que el nivel de seguridad del nuevo esquema es competitivo con los encriptadores de imágenes del tipo permutación - difusión, mientras que la complejidad computacional es mucho menor, por lo que el esquema que proponen es un buen candidato para aplicaciones que operan en tiempo real de comunicaciones seguras de imágenes (Fu *et al.*, 2011). En el año 2012, (Deng y Zhao, 2011) proponen el encriptado de imágenes con un solo canal a color basado en un sistema criptográfico de clave asimétrica, como resultado obtienen un sistema compacto y robusto, el cual permite que encripte los valores reales de los niveles de grises de los pixeles para ser transmitidos, desmuestran mediante resultados numéricos la viabilidad y efectividad del método que proponen (Deng y Zhao, 2011). En este mismo año, (Liu *et al.*, 2012), publican el trabajo doble encriptado de imagen utilizando la transformada de Arnold y transformada discreta fraccional angular, los parámetros de ambas transformadas sirven como claves adicionales para mejorar la seguridad, realizan algunas simulaciones numéricas para validar el esquema de encriptado (Liu *et al.*, 2012).

II.4 Conclusiones

En este capítulo se presentaron las principales características de los sistemas caóticos, las cuales son atractivas para los diseñadores de sistemas criptográficos. Se realizaron diferentes tipos de análisis a las señales caóticas que son generadas por los mapeos de Hénon, Chen, Rössler y gato de Arnold, con la intención de conocer la complejidad de estas dinámicas caóticas, los análisis realizados son: Espacio de fase (atractores), espectros de frecuencias, exponentes de Lyapunov, curvas de autocorrelación, correlación cruzada y diagramas de bifurcación. Además se presentó una revisión bibliográfica sobre trabajos relacionados a este tema de tesis, se pudo observar que existe gran diversidad de trabajos que emplean el encriptado caótico en imágenes digitales.

Capítulo III

Sistemas biométricos

III.1 Introducción

La palabra **biometría**, proviene del griego (βios => (vida), metro => (medir)), se refiere a dos campos de estudio y aplicaciones muy diferentes. El primero, es el más antiguo y se usa para estudios biológicos, tales como: la colección, síntesis, análisis y manejo de datos en biología. El segundo, se utiliza en sistemas que miden algún parámetro o variable física (Jain *et al.*, 2011). Por otra parte, según la *RAE*, el término **biométrico** se define como el *estudio mensurativo o estadístico de los fenómenos o procesos biológicos*. Sin embargo, en este trabajo de tesis, el significado de la palabra **biometría** ha sido empleado para incluír el estudio de los métodos automáticos de identificación de personas basados en características físicas o conductuales (Jain *et al.*, 2008). La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital. Los sistemas biométricos incluyen un dispositivo de captación para medir una o más características físicas o conductuales, que incluyen, huella digital, huella de la mano, geometría de la mano, rostro, iris, retina, oreja, voz, firma, forma de caminar, venas de la mano, olor y DNA, con esta información de cualquier persona se puede determinar o verificar su identidad. En algunas ocasiones, estas características también son referidas por diferentes términos, tales como: rasgos, indicadores, identificadores o modalidades (Jain *et al.*, 2011).

Características de los sistemas biométricos

- Garantiza con mucha seguridad la identidad de los usuarios.
- Evita el uso de password's difíciles de recordar.
- Evita el uso de tarjetas: magnéticas, inteligentes (ROM) y RFID (Radio Frequency Identification).
- Es intransferible.
- Difícil de reproducir, compartir y distribuir.
- Difícil falsificación.

En la figura 37, se muestran algunos identificadores biométricos. Los identificadores fisiológicos están relacionados con la forma de alguna parte del cuerpo, mientras que los identificadores conductuales están relacionadas con el comportamiento o conducta de las personas.

El proceso de autenticidad biométrica se refiere a la verificación de individuos con base en sus características fisiológicas ó conductuales. Este es más seguro que el proceso de autenticidad con base en el uso de *passwords* o claves secretas. Como las características biométricas no se pueden extraviar u olvidar, éstas son extremadamente difíciles de reproducir, compartir y distribuir. De este modo, la autenticidad con base en biometría es potencial candidata para remplazar a la autenticidad con base en passwords (Uludag *et al.*, 2001). En la figura 38, se muestra un diagrama a bloques de un sistema biométrico.

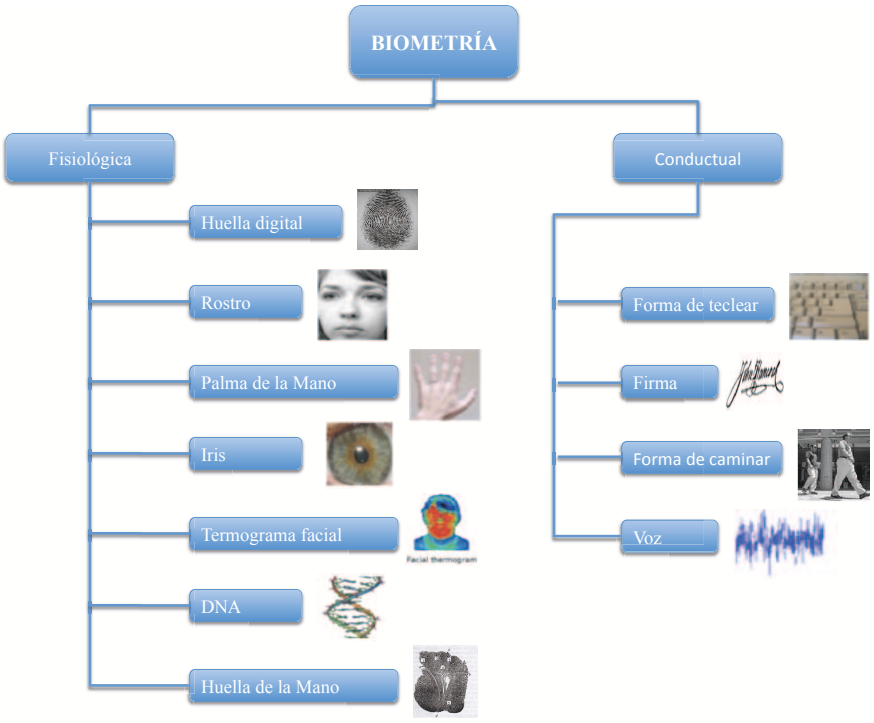


Figura 37: Ejemplo de algunos identificadores biométricos (Jain *et al.*, 2004, 2008).

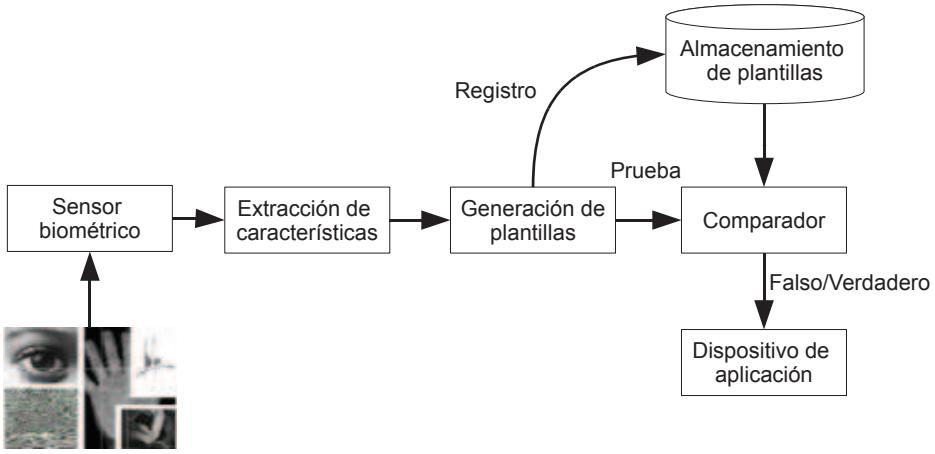


Figura 38: Diagrama a bloques de un sistema de identificación biométrico (Jain *et al.*, 2011).

III.2 Sistemas de reconocimiento de rostros

Un sistema de reconocimiento facial es una aplicación dirigida por computadora para identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales a partir de una imagen digital o un fotograma de una fuente de video. Una de las maneras de hacer esto es mediante la comparación de determinados rasgos faciales de la imagen facial y una base de datos (Zhang, 2000). Es utilizado principalmente en sistemas de seguridad para el reconocimiento de los usuarios. Consiste en un lector que define las características del rostro, y al solicitar acceso se verifica que coincidan las características del usuario con la base de datos. Los sistemas de reconocimiento de imágenes faciales tienen menor unicidad que los sistemas de reconocimiento basados en huellas dactilares y de iris, sin embargo, proporciona una forma de identificación más directa, amigable y es más aceptable comparado con otros sistemas de indentificación biométricos. Por lo tanto, la investigación sobre el reconocimiento del rostro se ha convertido en una de las partes más importantes en la biometría (Zhang, 2000).

III.2.1 Antecedentes

Desde 1960, se han hecho una gran cantidad de trabajos de investigación sobre reconocimiento del rostro, y se han obtenido muchos resultados fructíferos. Una de las razones, por la que los sistemas de reconocimiento de rostros han obtenido una amplia investigación, es que algunas aplicaciones prácticas se necesitan urgentemente. Por ejemplo los cajeros del banco, ocupan saber si realmente los usuarios correctos están utilizando su cuenta, o bien, si un policía trata de encontrar si el hombre de la foto es reincidente, también los oficiales de migración revisan si la persona que está cruzando la frontera internacional es el mismo que el que está en la foto del pasaporte. Asimismo,

en la vida cotidiana, un guardia de seguridad puede revisar si están autorizadas las personas que entran a una oficina o edificio todos los días (Zhang, 2000). Los sistemas de reconocimiento de la cara, contienen dos pasos clave, tal como se muestra en la figura 39, los cuales son: 1) detección y localización del rostro junto con la extracción de las características y 2) reconocimiento del rostro. El primer paso decide si la imagen de entrada o secuencia de imágenes incluye rostros, y si así lo es, obtiene la posición del rostro, luego segmenta cada rostro del fondo de la imagen. El segundo paso busca las características del rostro, las cuales distinguen a los individuos y dice quienes de las personas en la imagen es la persona autorizada o quien está en la base de datos (Zhang, 2000).

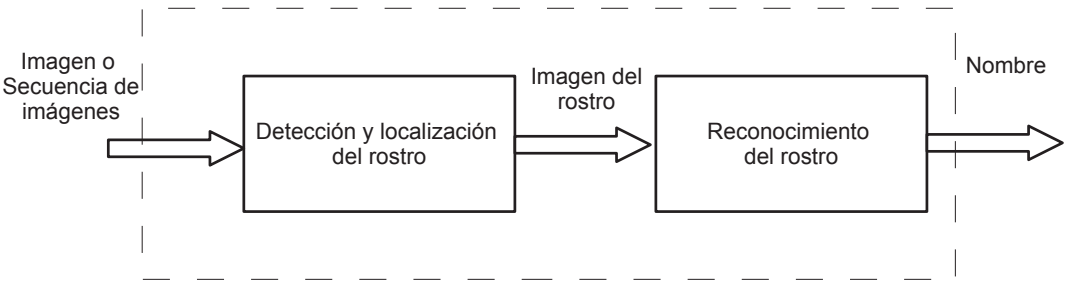


Figura 39: Diagrama de flujo del sistema de reconocimiento facial (Zhang, 2000).

Tanto la extracción de características como el reconocimiento facial pueden variar de acuerdo a las diferentes aplicaciones. Algunas veces, queremos saber si la persona que se presenta es realmente quien está registrada, tal como la persona que deposita en un banco, en este caso el proceso es llamado ***verificación*** del rostro. Mientras que en otras condiciones, si queremos saber quien es la persona que se presenta, por ejemplo en la entrada a una oficina y el sistema escanea su rostro y coincide con unas de las almacenadas en la base de datos, entonces lo reconoce y dice cual es su nombre, en otras palabras, a éste proceso se le llama de ***reconocimiento*** (Zhang, 2000). Si

las expresiones del rostro varían, su orientación y la edad, también se pueden tener grandes diferencias entre el rostro almacenado en la base de datos y el rostro que está siendo reconocido, por lo tanto será muy difícil extraer las características y reconocer tales rostros (Zhang, 2000). Algunos algoritmos populares de reconocimiento facial son: eigenface, fisherface, el modelo de Markov, y el neuronal (Zhang, 2000; Zhang *et al.*, 2004; Eleyan y Demirel, 2005, 2006).

III.3 Obtención de patrones

Las técnicas basadas en análisis de componentes principales (PCA) (Sirovich y Kirby, 1987; Kirby y Sirovich, 1990), típicamente incluyen dos etapas: **Entrenamiento** y **clasificación**. En la etapa de **entrenamiento**, se establece un subespacio de las muestras de entrenamiento utilizando PCA y estas imágenes de entrenamiento de los rostros son mapeadas a este subespacio para la clasificación ó reconocimiento. En la etapa de **clasificación**, la imagen del rostro de entrada es proyectada al mismo subespacio y clasificada por un apropiado clasificador. Para más detalles de éste método, ver por ejemplo (Zhang, 2000; Turk y Pentland, 1991a,b). La técnica para el reconocimiento de los rostros, involucra las siguientes operaciones de inicialización (Turk y Pentland, 1991a):

1. Capturar el conjunto inicial de imágenes de rostros (conjunto de entrenamiento).

2. Calcular los *eigenfaces* del conjunto de entrenamiento, manteniendo solamente M imágenes que corresponden los valores propios mayores (Los valores propios con valores cercanos a cero se desprecian). Estas M imágenes definen el subespacio.

3. Si la imagen de entrada es un rostro, se clasifican los pesos de los patrones como una persona conocida o desconocida.

4. Se pueden estar actualizando los *eigenfaces* y/o los pesos de los patrones (opcional).

III.3.1 Cálculo de *eigenfaces*

Un rostro humano se puede considerar como una muestra estocástica, y cada imagen de rostro es considerada como un vector con dimensión muy grande y cada pixel corresponde a una componente. Si todas las imágentes de los rostros se encuentran en el mismo subespecio del gran espacio dimensional, este subespacio es una buena representación de las imágenes de rostros, debido a que muestra las características comunes de los rostros. Así que la detección de rostros consiste en encontrar el subespacio.

Suponga, $A = [a_{ij}]_{rxc}$ como una imagen de rostro humano, donde r y c son el número de renglones y columnas de la imagen, respectivamente; a_{ij} es el valor de gris del pixel en el *i-ésimo* renglón y *j-ésima* columna. Re-arreglando a_{ij} y convirtiéndola a vector columna:

$$x^i = [a_{11}\ a_{21}\ ...\ a_{r1}\ a_{12}\ a_{22}\ ...\ a_{r2}\ ...\ a_{1c}\ a_{2c}\ ...\ a_{rc}]^T, \tag{7}$$

donde x^i es un vector de dimensión D, $D = r\ x\ c$. Luego las imágenes son centradas mediante la substracción de la imagen promedio a cada vector imagen.

$$\overline{x}^{\,i} = x^i - m, \tag{8}$$

donde m es el vector promedio de las imágenes de entrenamiento y está dado por

$$m = \frac{1}{M}\sum_{i=0}^{M-1} x^i. \tag{9}$$

Los vectores de la ec. (8) están combinados, lado por lado, para crear una matríz

de datos de tamaño $D \times M$, donde M es la cantidad de imágenes del conjunto de entrenamiento.

$$\overline{X} = \left\{ \overline{x}^1 \mid \overline{x}^2 \mid ... \mid \overline{x}^P \right\}, \tag{10}$$

la matríz de covarianza se puede calcular como

$$\Omega = \overline{X} \cdot \overline{X}^T. \tag{11}$$

Esta matríz de covarianza tine hasta d *eigenvectores* asociados con *eigenvalores* distintos a cero, asumiendo $d < D$.

Sean λ_1, λ_2, ... , λ_d ($\lambda_1 \geqslant \lambda_2, \geqslant ... \geqslant$, $\lambda_d > 0$) los *eigenvalores* y u_1, u_2 , ... , u_d sus correspondientes *eigenvectores* de la matríz de covarianza Ω. Así que, cada imagen de rostro humano, x^i, puede ser representada por una combinación lineal de *eigenvectores*. De acuerdo a la teoría del álgebra, sabemos que u_1, u_2 , ... , u_d pueden ser ortogonal uno del otro y vector unidad. Usualmente, $M < D$, se puede satisfacer debido a que D es mayor que la cantidad de usuarios. Entonces se deduce que $d < D$. En otras palabras, la imagen del rostro humano puede ser representada por pocos vectores base (d vectores) (Turk y Pentland, 1991a).

Algunos valores de λ_i, en d *eigenvalores* son muy pequeños, cuyo correspondientes *eigenvectores* contribuyen poco para representar las imágentes de los rostros de los usuarios, por lo tanto, pueden ser ignorados. Por lo tanto, los *eigenvectores* se ordenan en forma decreciente de acuerdo a los *eigenvalores* y seleccionamos los k mejores *eigenvectores* para representar a los usuarios (Turk y Pentland, 1991a).

A. Ordenando los *eigenvectores*

Los *eigenvectores* $u_i \in U$ se ordenan de acuerdo a sus correspondientes *eigenvalores* λ_i de mayor a menor. Solamente se mantienen los *eigenvectores* asociados con *eigenvalores* diferentes a cero. Esta matríz de *eigenvectores* se le llama *eigenspace* ó subespacio U, donde cada columna de U es un eigenvector

$$U = [\, u_1 \mid u_2 \mid \cdots \mid u_d \,]. \tag{12}$$

B. Proyectando las Imágenes de entrenamiento

Para proyectar las imágenes de entrenamiento, cada una de las imágenes centradas con la ec. (8) debe ser proyectada al subespacio, para esto se calcula el producto punto de la imagen con cada uno de los *eigenvectores* ordenados en ec. (12), como sigue,

$$\widetilde{x}^{\,i} = U^T \overline{x}^i. \tag{13}$$

Por lo tanto, el producto punto de la imagen y el primer *eigenvector* serán el primer valor del nuevo vector. El nuevo vector calculado con la ec. (13) de la imagen proyectada debe contener los mismos valores que *eigenvectores*.

C. Identificando las imágenes de prueba

Cada imagen de prueba es centrada mediante la substracción de la imagen promedio, luego es proyectada al mismo subespecio, definido por U, como sigue,

$$\overline{y}^{\,i} = y^i - m, \tag{14}$$

donde m es calculada utilizando la ec. (9), y $\overline{y}^{\,i}$ es la imagen de prueba centrada. Luego, se proyecta esta imagen centrada de acuerdo a,

$$\widetilde{y}^{\,i} = U^{T}\,\overline{y}^{\,i}. \tag{15}$$

La imagen de prueba proyectada ($\widetilde{y}^{\,i}$) se compara con cada imagen de entrenamiento proyectada y la imagen de entrenamiento que se encuentre más cercana a la imagen de prueba es usada para identificar la imagen de entrada (imágenes de prueba). Estas imágentes pueden ser comparadas utilizando cualquier métrica de similitud; la más común es la norma 2 (L_2) o distancia Euclidiana, de la siguiente manera,

$$\varepsilon^2 = \left\|\widetilde{y}^{\,i} - \widetilde{x}^{\,k}\right\|_2, \tag{16}$$

donde $\widetilde{x}^{\,k}$ es un vector que describe la k-ésima clase de rostro. Un rostro es clasificado como perteneciente a la clase k cuando el mínimo ε es menor a algún umbral escogido θ_ε. De lo contrario, la imagen del rostro se clasifica como "desconocido ".

III.4 Revisión bibliográfica

III.4.1 Encriptado de información biométrica

A la fecha, se han reportado distintas metodologías para proteger o encriptar la información biométrica, por ejemplo (Jain y Uludag, 2002), con la intención de proteger la información biométrica, utiliza la *esteganografía* para ocultar las minucias que se obtienen de una huella digital. Ahí proponen utilizar como imágenes de "cubiertas" (cover images) huellas digitales sintéticas, rostros, paisajes, etc. El método propuesto por (Jain y Uludag, 2002) consiste en generar marcas de agua basadas en modulación de amplitud, el cual es una extensión del método de marcas de agua de canal azul reportada en (Kutter *et al.*, 1997; Uludag *et al.*, 2001).

En el trabajo reportado por (Bremananth y Chitra, 2005) proponen un eficiente sistema criptográfico mediante el uso de autocorreladores, en este caso la información

biométrica que encripta son mensajes de texto y la cripto-clave la generan en función de los patrones de imágenes de iris de los usuarios. En la técnica que proponen (Bremananth y Chitra, 2005), las cararacterísticas del iris las extraen utilizando la transformada wavelet de multiresolución, ésta produce códigos de iris de 135 bits para cada persona y son utilizados para encriptar y desencriptar los mensajes (Bremananth y Chitra, 2005). Los autocorreladores son utilizados para rellamar los mensajes originales de los datos corrompidos parcialmente y producidos por el proceso de desencriptamiento. El método tiene la intención de resolver los problemas de administración y anulación de claves. Analizan los resultados en un sistema convencional de criptografía de iris (CIC) y en un sistema de criptografía de iris anti-rechazo (NRIC) (Bremananth y Chitra, 2005). Con una idea similar, (Chen y Chandran, 2007) también generan claves criptográficas, pero basada en información biométrica de los rostros. En el trabajo reportado por (Soutar *et al.*, 1999), emplean encriptado convencional y generan una bio-clave que se obtiene a partir de una huella digital y una clave k de N bits.

En el trabajo presentado por (Khan, 2006), el cual se titula implementación de seguridad en plantillas de un sistema remoto de autenticación biométrica, es un sistema criptográfico basado en caos para resolver la privacidad y seguridad de las plantillas biométricas en un sistema de autenticación biométrica que opera remotamente sobre una red. Las plantillas biométricas son encriptadas mediante un esquema de criptografía caótica y moduladas con una técnica de espectro esparcido caóticamente, los resultados experimentales que reportan, muestran que la seguridad, desempeño y exactitud del método presentado es alentador para la implementación práctica en ambientes reales.

Por otro lado, el trabajo reportado por (Han *et al.*, 2007), se titula "encriptado de imágenes de huellas digitales vía atractores caóticos de múltiples enrrollamientos", ellos proponen una técnica de encriptado caótico de imágenes de huellas digitales, las cuales son encriptadas vía una secuencia caótica de 2D obtenida de un atractor caótico de

múltiples enrrollamientos, validan la técnica de encriptado caótico con la transformada discreta de Fourier en 2D.

En el trabajo realizado por (Muhammad *et al.*, 2007b) quienes presentan el trabajo titulado transmisión de plantillas biométricas ocultas en base a contenido caótico seguro, mencionan que las técnicas de encriptamiento y ocultamiento de la información biométrica son utilizadas para mejorar la seguridad y privacidad en las plantillas de iris transmitidas. Las claves secretas son generadas por una imagen biométrica y es utilizada como el valor numérico de un parámetro y como condición incial del sistema caótico, por lo que en cada sesión de transacción tiene diferentes claves secretas para protegerse de los ataques. Se utilizan dos mapeos caóticos para el encriptado, para resolver el efecto de palabra de tamaño finito y para mejorar la resistencia del sistema contra ataques de fuerza bruta. El encriptado caótico se aplica a las plantillas del iris antes de ser ocultadas (esteganografía) dentro de las imágenes cover/host para hacerlas más seguras, luego las plantillas son escondidas (ocultadas) dentro de la imagen cubierta (cover), ellos mencionan que los resultados muestran que la seguridad, desempeño y precisión del esquema presentado son alentadores, en comparación con otros métodos encontrados en la literatura actual (Muhammad *et al.*, 2007b). Con una idea similar, (Muhammad *et al.*, 2007a) encriptan plantillas de huellas digitales empleando caos y las ocultan en señales de audio empleando esteganografía.

Por otra parte, en el trabajo reportado por (Jain *et al.*, 2008) utilizan una técnica de transformación de características para proteger la información biométrica, básicamente consiste en evaluar una función de transformación que depende de la extracción de caraterísticas de la información de la imagen biométrica y de una clave secreta. En este caso la información biométrica es una huella dactilar, pero puede ser cualquier otro identificador biométrico, por ejemplo: palma de la mano, iris, voz, retina, huella de la mano, termograma facial o el rostro.

Adicionalmente (Lu *et al.*, 2009) utilizan el encriptado biométrico en un sistema de reconocimiento de rostros para mejorar el desempeño en la privacidad de la información biométrica, ésta técnica se basa en el sistema HDS (Helper Data System) y en el sistema de encriptado biométrico basado en la modulación de índice de cuantización (QIM) para un escenario de auto-exclusión de reconocimiento de rostros (Linnartz y Tuyls, 2003; Buhan *et al.*, 2007). En este caso están utilizando criptografía convencional basada en funciones Hash y el sistema HDS (Lu *et al.*, 2009).

III.5 Conclusiones

En este capítulo se presentó una introducción a los sistemas de identificación biométrica, específicamente a los sistemas de reconocimiento de rostros. Se mostró una breve descripción del método *eigenface*, el cual fue motivado por la teoría de la información, que conduce a la idea de basar el reconocimiento de rostros en un pequeño conjunto de imágenes de razgos que mejor se aproximen al conjunto de imágenes de rostros, sin requerir que estas correspondan a nuestras nociones intuitivas de las partes y características faciales. Aunque no es una solución elegante al problema general de reconocimiento, el método *eigenface* proporciona una solución práctica que se ajusta bien al problema del reconocimiento del rostro. Este método es rápido, relativamente sencillo y ha sido demostrado que trabaja bien en un ambiente controlado.

Además se presentó una revisión bibliográfica sobre trabajos de investigación que emplean el encriptado de información en sistemas de reconocimiento biométrico. En este trabajo de tesis, se toma como base el algoritmo de encriptado reportado en (Muhammad *et al.*, 2007b), sin embargo, en este trabajo se hace una optimización del umbral del cuantización y además se proponen dos esquemas de doble encriptado hipercaótico, con la finalidad de incrementar el nivel de seguridad de la información biométrica encriptada.

Capítulo IV

Encriptado y desencriptado caótico

IV.1 Introducción

Debido a las propiedades del caos que se mencionaron en el capítulo II, se han propuesto muchos algoritmos de encriptado de imágenes basado en caos, ver por ejemplo (Kocarev y Shiguo, 2011; Fu *et al.*, 2011; Patidar *et al.*, 2011; Mao y Deng, 2011; Akhshani *et al.*, 2010; Zhang *et al.*, 2010; Liu *et al.*, 2009; Peng *et al.*, 2009; Gao y Chen, 2008; Behnia *et al.*, 2007, 2008; Muhammad *et al.*, 2007b; Gao *et al.*, 2006; Zhang *et al.*, 2005; Chen *et al.*, 2004; Mao y Chen, 2004). En este trabajo de tesis doctoral, se seleccionó el método reportado en (Muhammad *et al.*, 2007b), el cual fué empleado para encriptar plantillas de iris mediante el uso del mapeo generalizado de Hénon. Sin embargo, en esta investigación se utilizan los mapeos caóticos de Hénon, gato de Arnold, Logistic 1D y los mapeos hipercaóticos de Chen y Rössler para ser aplicado en un sistema de reconocimiento de rostros, de tal forma que se pueda encriptar imágenes de rostros y patrones de rostros, además se hizo una optimización en el umbral de cuantización para mejorar la entropía de la información y con esto alcanzar mejor nivel de seguridad. Se propone un algoritmo de encriptado sencillo y dos algoritmos de doble encriptado caótico.

IV.2 Propuesta de encriptado y desencriptado sencillo

IV.2.1 Algoritmo de encriptado sencillo

En la figura 40 se muestra el esquema de encriptado sencillo propuesto en este trabajo de tesis doctoral para encriptar las imágenes de rostros y patrones de rostros. Las entradas para este esquema son la imagen del rostro y las condiciones iniciales (como *clave* de encriptado) del mapeo hipercaótico. Posteriormente la imagen del rostro es digitalizada, para posteriormente realizarse la operación X-OR con la señal hipercaótica generada con el mapeo de Rössler (5), antes de realizar la operación X-OR, la señal hipercaótica también tiene que ser digitalizada, esto se hace utilizando el cuantizador, en este cuantizador se establece un umbral entre el valor mínimo y máximo de la amplitud de la señal caótica, por ejemplo si la señal caótica oscila entre 0 y 1, se puede establecer un umbral de 0.5. Cuando la amplitud de la señal hipercaótica es mayor o igual a 0.5, la salida del cuantizador es un nivel lógico alto, mientras que cuando la amplitud de la señal hipercaótica es menor a 0.5, la salida del cuantizador es un nivel lógico bajo. El resultado de la operación X-OR entre la imagen del rostro digitalizada y la señal hipercaótica en formato binario, también es una señal binaria, que recibe el nombre de criptograma y corresponde al rostro encriptado, el cual se envía a través de la red pública.

IV.2.2 Algoritmo de desencriptado sencillo

La figura 41 muestra el esquema de desencriptado sencillo propuesto en este trabajo para recuperar las imágenes de rostros en el receptor. Básicamente se sigue el proceso

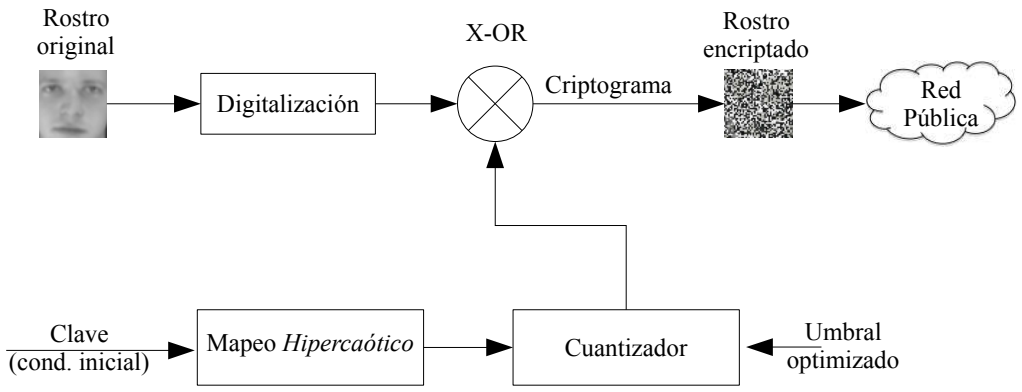


Figura 40: Esquema del encriptador hipercaótico.

inverso del encriptado, es decir, se recibe el criptograma y se introduce la clave que se empleó para el encriptado (las mismas condiciones iniciales). De igual forma, la señal hipercaótica generada se aplica a un cuantizador para que sea convertida a formato binario, el umbral del cuantizador tiene que ser el mismo que el que se utilizó para encriptar la imagen, posteriormente se aplica la operación X-OR entre el criptograma y señal hipercaótica binaria, el resultado de esta operación también es una cadena de bits, posteriormente estos bits se agrupan en 8 para formar los bytes que corresponden al nivel de gris de cada pixel, por último se reconstruye la imagen del rostro recuperado.

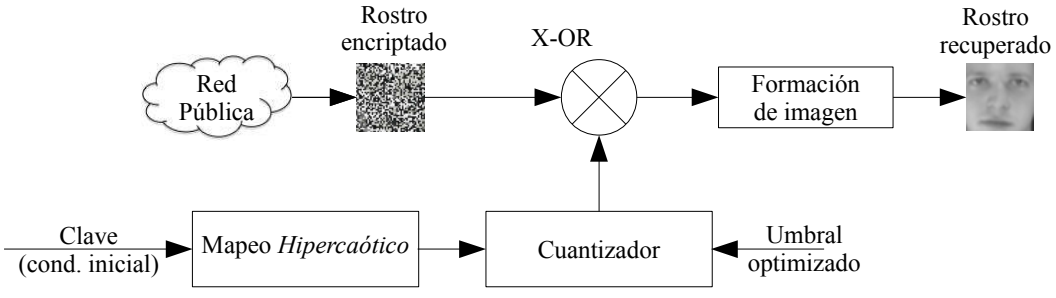


Figura 41: Esquema del desencriptador hipercaótico.

IV.3 Propuesta de doble encriptado y desencriptado

Recientemente se han reportado en la literatura algunos trabajos relacionados al doble encriptado de imágentes, ver por ejemplo (Shan *et al.*, 2012; Wang *et al.*, 2012; Zhong *et al.*, 2012; Aguilar-Bustos *et al.*, 2010), por tal motivo, en este trabajo de tesis, se propone emplear un doble encriptado, en un primer caso, el doble encriptado que se propone es empleando diferentes estados del mismo mapeo caótico. Posteriormente se propone que se utilicen diferentes estados de distintos mapeos caóticos, esto con la idea de obtener un encriptado mucho más seguro.

IV.3.1 Algoritmo de doble encriptado con el mismo mapeo.

La figura 42 muestra el esquema a bloques del algoritmo de doble encriptado caótico empleando el mismo mapeo. De manera similar al encriptado sencillo, las entradas de este algoritmo son la imagen a encriptar y la clave de encriptado, en este caso son las condiciones iniciales del mapeo caótico. Una vez inicializado el mapeo, se comienza a generar las señales caóticas y posteriormente son aplicadas (x_1 y x_2) a un cuantizador para ser convertidas a binario, posteriormente se realiza la operación XOR del estado x_1 en binario con la información digitalizada de la imagen a encriptar, luego, el resultado de este primer encriptado pasa por otro proceso de encriptado, pero ahora se realiza la operación XOR con el estado x_2 binario, el resultado de ese proceso es una imagen doblemente encriptada que posteriormente se envía por la red pública.

De manera general podemos decir que la imagen primero se encripta con el estado x_1 del mapeo caótico y posteriormente se encripta con el estado x_2, el resultado de esta operación de doble encriptado es enviado por la red pública.

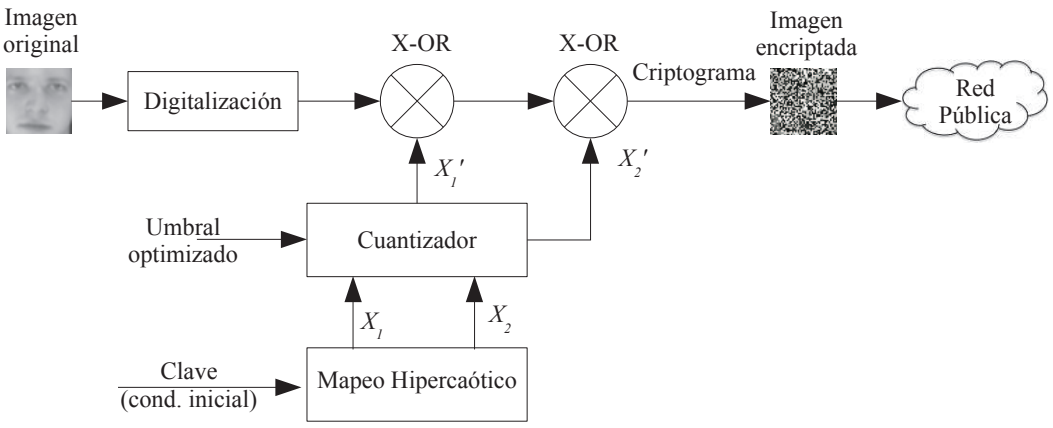


Figura 42: Esquema de doble encriptado hipercaótico empleando el mismo mapeo.

IV.3.2 Algoritmo de doble desencriptado con el mismo mapeo

La figura 43 muestra el esquema a bloques del algoritmo de doble desencriptado caótico empleando el mismo mapeo. Básicamente es el proceso inverso del doble encriptado con el mismo mapeo. Es decir, el criptograma recibido, primeramente se realiza un proceso de desencriptado con el estado x_2 binario del mapeo caótico y posteriormente se realiza el segundo proceso de desencriptado con el estado x_1 binario, después se forma la imagen recuperada.

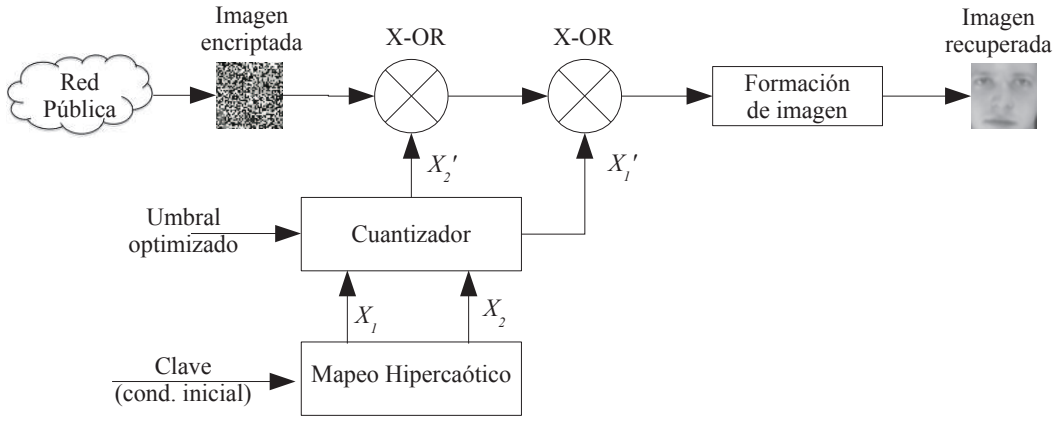


Figura 43: Esquema de doble desencriptado hipercaótico empleando el mismo mapeo.

IV.3.3 Algoritmo de doble encriptado con diferente mapeo

La figura 44 muestra el esquema a bloques del algoritmo de doble encriptado caótico empleando diferentes mapeos. Las entradas de este algoritmo son la imagen a encriptar y las dos claves de encriptado. Una vez inicializado los mapeos, comienzan a generar las secuencias caóticas, posteriormente el estado x_1 del primer mapeo pasa por un cuantizador, así como también el estado x_2 del segundo mapeo pasa por otro cuantizador. La imagen digitalizada primero se encripta empleando la operación XOR con el estado x_1 binario del primer mapeo caótico, luego se encripta con el estado x_2 binario del segundo mapeo caótico, el resultado de esta operación es la imagen doblemente encriptada con distinto mapeo, posteriormente es enviada por la red pública.

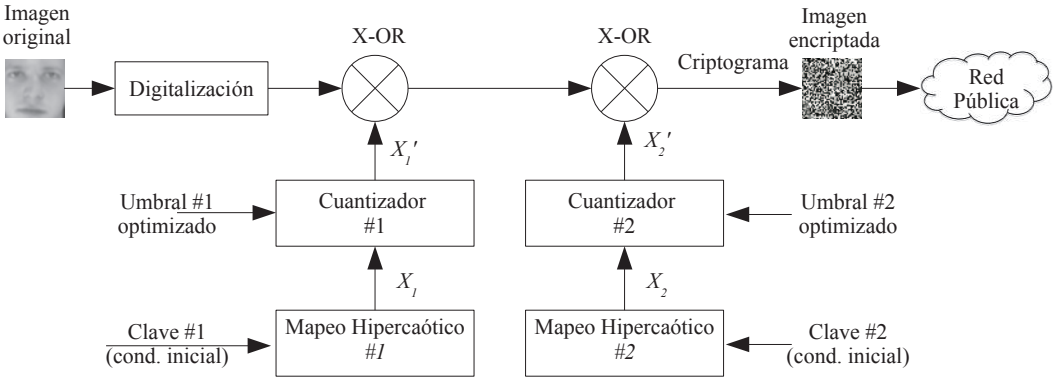


Figura 44: Esquema de doble encriptado hipercaótico empleando diferente mapeo.

IV.3.4 Algoritmo de doble desencriptado con diferente mapeo

La figura 45 muestra el esquema a bloques del algoritmo de doble desencriptado caótico empleando diferentes mapeos. Básicamente es el proceso inverso del doble encriptado con distinto mapeo. Es decir, el criptograma recibido, primeramente se realiza un proceso de desencriptado con el estado x_2 binario del segundo mapeo caótico y posteriormente se realiza el segundo proceso de desencriptado con el estado x_1 binario del

primer mapeo, después se forma la imagen recuperada.

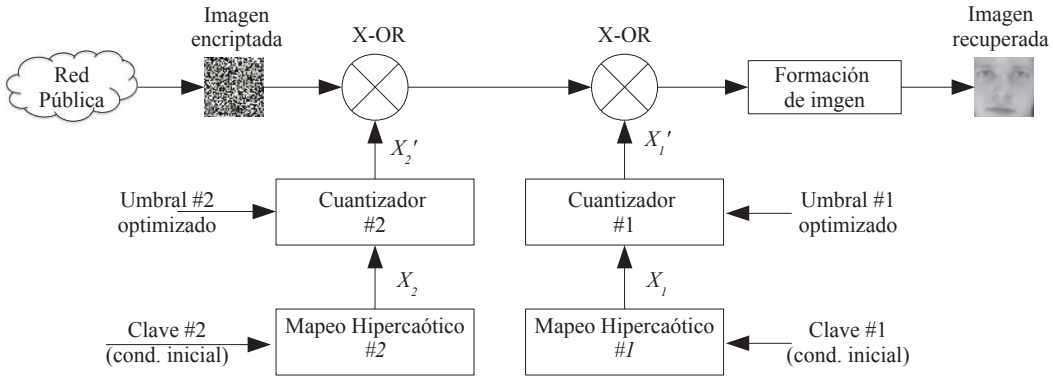


Figura 45: Esquema de doble desencriptado hipercaótico empleando diferente mapeo.

IV.4 Conclusiones

En este capítulo se propuso un algoritmo de encriptado caótico sencillo, de tal forma que el encriptado de rostros o patrones se puede realizar de una forma rápida. También se propusieron dos algoritmos de doble encriptado caótico, con la idea de incrementar el nivel de seguridad de la información biométrica. Los mapeos caóticos a utilizar son, Hénon, Chen, Rössler y gato de Arnold. El umbral del cuantizador se optimizó para obtener el mejor nivel de seguridad con cada uno de los mapeos. La ventaja del algoritmo sencillo es que se ejecuta un poco más rápido con respecto a los de doble encriptado. La ventaja de los algoritmos de doble encriptado es que tienen mayor nivel de seguridad y sobretodo el algoritmo que emplea distinto mapeo. El algoritmo de doble encriptado con diferente mapeo emplea dos claves de encriptado, debido a que cada mapeo tiene sus propias condiciones iniciales, esto le da un grado más de seguridad, al ser requeridas dos claves de encriptado/desencriptado.

Capítulo V

Análisis de seguridad

V.1 Introducción

La palabra **seguridad**, proviene del latín (securĭtas, -ātis), según la *RAE* se define como: (1) Cualidad de seguro. (2) Certeza - *conocimiento seguro y claro de algo.* (3) Fianza u obligación de indemnidad a favor de alguien, regularmente en materia de intereses. (4) *Dicho de un mecanismo que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.* En el trabajo reportado por (Behnia *et al.*, 2008), definen **seguridad** como una medida crucial de la calidad de un sistema criptográfico, mencionan que es la capacidad de resistir los ataques de intrusos o usuarios no autorizados para obtener conocimiento de la información sin encriptar (confidencial). La discusión de la seguridad para los sistemas criptográficos con valores discretos está basada en un modelo, el cual fué primeramente introducido por (Shannon, 1949, 1948), después fue extendido por otros autores, ver por ejemplo (Chen *et al.*, 2004; Behnia *et al.*, 2007; Gao y Chen, 2008; Liu *et al.*, 2009; Zhang *et al.*, 2010; Fu *et al.*, 2011; Patidar *et al.*, 2011; Mao y Deng, 2011; Liu *et al.*, 2012) .

V.2 Resistencia contra ataques de fuerza bruta

V.2.1 Análisis de espacio de claves secretas

El espacio de claves, es el númuero total de diferentes claves que pueden ser utilizadas en el procedimiento encriptado/desencriptado. Para que un sistema criptográfico sea

efectivo y seguro, el espacio de claves debe ser lo suficientemente grande para hacer inviable el ataque de fuerza bruta (Fu *et al.*, 2011). La clave del sistema criptográfico propuesto, está compuesto de dos partes: a) Las condiciones iniciales del mapeo, b) los parámetros de control del mismo mapeo. Si el espacio de clave de un algoritmo de encriptado es lo suficientemente grande, típicamente mayor a 128 bits, ya se considera seguro para la mayoría de las aplicaciones criptográficas en término de la velocidad de las computadoras actuales, por lo tanto, el ataque de fuerza bruta en tal algoritmo es inviable (Patidar *et al.*, 2011).

V.2.2 Análisis de sensibilidad

Esta prueba consiste en hacer un pequeña modificación a las condiciones iniciales y/o parámetros de un mapeo caótico y evaluar cuanto cambia la dinámica del mapeo, así como el efecto de la imagen encriptada. La extrema sensibilidad a la clave, es una característica esencial para cualquier buen sistema criptográfico, esta sensibilidad garantiza la seguridad del criptosistema contra ataques de fuerza bruta en cierta medida. La sensibilidad de un sistema criptográfico puede ser observada de dos maneras distintas: (a) la imagen encriptada producida por el criptosistema debe ser muy sensible a la clave secreta, es decir, si utilizamos claves ligeramente diferentes para encriptar la misma imagen original, entonces las dos imágenes encriptadas que se producen, deben ser completamente independientes (diferentes) una de la otra, en otras palabras, deben poseer una correlación insignificante, (b) la imagen encriptada, no puede ser desencriptada correctamente aunque exista una ligera diferencia entre las claves de encriptado y desencriptado (Patidar *et al.*, 2011).

V.3 Análisis estadístico

Es bien sabido que muchos sistemas criptográficos han sido analizados exitosamente con la ayuda del análisis estadístico y varios ataques estadísticos han sido creados para ello. Por lo tanto, un encriptador efectivo debe ser robusto contra cualquier ataque estadístico. Para probar la rubustez de los algoritmos de encriptado mediante análisis estadístico, comúnmente se utilizan histogramas, correlación de pixeles adyacentes y entropía de la información (Fu *et al.*, 2011).

V.3.1 Histograma estadístico

El concepto de **histograma**, según la *(RAE)*, es una representación gráfica de una distribución de frecuencias por medio de rectángulos, cuyas anchuras representan intervalos de la clasificación y cuyas alturas representan las correspondientes frecuencias. Desde el punto de vista de procesamiento de imágenes, el histograma de una imagen es una gráfica que muestra la cantidad de pixeles de cada valor de intensidad diferente encontrado en la imagen. Para una imagen de 8 bits en escala de grises, existen 256 niveles de intensidades diferentes (Patidar *et al.*, 2011). La distribución del histograma de la imagen encriptada es lo más importante. Mas específicamente, este debe ocultar la redundancia de la imagen original y no debería filtrarse alguna información de la imagen original (confidencial) o que exista una relación entre la imagen encriptada y la imagen original (Fu *et al.*, 2011). Por lo tanto, mientras más uniforme sea la distribución del histograma de la imagen encriptada, el algoritmo es más fuerte contra ataques de tipo estadístico.

V.3.2 Análisis de correlación de pixeles adyacentes

En 1949, Shannon propuso dos técnicas básicas para realizar el diseño de encriptadores (Shannon, 1949), **la difusión y confusión** y estas dos propiedades superiores pueden ser demostradas por una prueba en la correlación de pixeles adyacentes en la imagen encriptada (Chen *et al.*, 2004).

A partir de la imagen bajo análisis, ya sea la imagen original o el criptograma, se toman al menos mil pares de pixeles adyacentes (en dirección horizontal, vertical y diagonal) y se calcula su coeficiente de correlación (Chen *et al.*, 2004) respectivamente, mediante la ec. (17)

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{17}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{18}$$

donde $cov(x,y)$ es la covarianza, $D(x)$ es la varianza, x e y denotan los valores en la escala de grises de la imagen bajo análisis. Para este caso de computación numérica, se utilizó la ec. (19) y ec. (20):

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{19}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))) \tag{20}$$

donde $E(x)$ es el valor promedio de los niveles de gris de los pixeles. Para calcular los coeficientes de correlación, se sugiere seleccionar aleatoriamente al menos 1000 pares de pixeles (x_i, y_i) de la imagen sujeta para análisis (original o encriptada) y se genera la gráfica de dispersión con estas parejas de pixeles adyacentes, es decir se gráfica el pixel x_i *vs* y_i. Posteriormente se calculan sus correspondientes coeficientes de correlación (r_{xy}) utilizando la ec. (17).

V.3.3 Entropía de la información

En los trabajos reportados por (Shannon, 1949, 1948), se introdujeron los fundamentos matemáticos de la teoría de la información aplicada a la comunicación y almacenamiento de datos. La entropía de la información, es un criterio que muestra la aleatoriedad de los datos. También puede ser utilizada para evaluar la seguridad del encriptado (Mao y Deng, 2011).

Para calcular la entropía $H(s)$ (Behnia *et al.*, 2007, 2008; Akhshani *et al.*, 2010), de una fuente (s), se utiliza la ec. (21):

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \cdot Log_2(\frac{1}{P(s_i)})\ bits \tag{21}$$

donde $P(s_i)$ representa la probabilidad del simbolo s_i.

Para una fuente puramente aleatoria, que está emitiendo 2^N símbolos con la misma probabilidad, después de evaluar la ecuación (21), se tiene una entropía $H(s) = N$, en este caso, para imágenes con pixeles completamente aleatorios en la escala de grises de 8 bits, su entropía $H(s) = 8\ bits$. Cuando las imágenes de rostros sean encriptadas, idealmente su entropía debe ser 8. Cuando un sistema criptográfico emite símbolos (criptogramas) con entropía menor a 8, este encriptador tiene cierto grado de predicibilidad, por lo que su seguridad se pone en riesgo (Behnia *et al.*, 2008).

V.4 Ataques diferenciales

Para realizar el análisis contra ataques diferenciales (Chen *et al.*, 2004) y comprender las diferencias entre las imágenes encriptadas, se utilizan dos medidas comúnes, *NPCR* (Number of Pixels Change Rate) y *UACI* (Unified Average Changing Intensity). Estas medidas son utilizadas para probar la influencia del cambio de un pixel en toda la imagen encriptada.

V.4.1 Tasa de cambio de la cantidad de pixeles - Number of Pixels Change Rate ($NPCR$)

Mide el porcentaje de la cantidad de pixeles diferentes entre dos imágenes y se puede calcular utilizando la ec. (22) :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{22}$$

donde $D(i,j)$ es un arreglo binario:

$D(i,j) = 0$, si $C_1(i,j) = C_2(i,j)$,

$D(i,j) = 1$, cuando $C_1(i,j) \neq C_2(i,j)$,

C_1 y C_2 son imágenes encriptadas obtenidas con claves (condiciones iniciales) muy semejantes. W y H definen el tamaño de la imagen bajo análisis (Chen *et al.*, 2004; Peng *et al.*, 2009; Mao y Deng, 2011).

V.4.2 Intensidad de cambio promedio unificada - Unified Average Changing Intensity ($UACI$)

Mide la intensidad promedio de las diferencias entre las dos imágenes encriptadas C_1 y C_2, se calcula empleando la ec. (23):

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%. \tag{23}$$

donde C_1, C_2, W y H fueron definidas previamente (Chen *et al.*, 2004; Peng *et al.*, 2009; Mao y Deng, 2011).

V.5 Conclusiones

Es muy importante realizar el análisis de seguridad a los algoritmos de encriptado caótico, debido a que con este análisis conocemos qué tan robusto o fuerte es el algoritmo de encriptado contra los diferentes tipos de ataques y poder determinar si es posible que algún cripto-analista o intruso pudiese descifrar la información encriptada sin conocer la clave, o bien, si realiza algún análisis estadístico o diferencial a los criptogramas con las velocidades y capacidades de los equipos de cómputo actuales. De tal forma, que cuando los parámetros de seguridad se encuentran muy aproximados a su valor ideal, garantizan al diseñador del sistema criptográfico y a los usuarios de estos sistemas, de que prácticamente es inviable o imposible de romper o descifrar la información confidencial que manejan estos sistemas en ausencia de la clave de encriptado.

Capítulo VI

Resultados

VI.1 Introducción

En este capítulo se presentan los resultados del análisis de seguridad realizado al algoritmo de encriptado sencillo y a los algoritmos de doble encriptado. En la resistencia contra ataques de fuerza bruta se considera el análisis de espacio de claves secretas y el análisis de sensibilidad. Con respecto al análisis estadístico se considera el análisis de histogramas, correlación de pixeles adyacentes y la entropía de información. En lo que se refiere a los ataques diferenciales, se considera el cálculo de los parámetros $NPCR$ y $UACI$.

VI.2 Encriptado sencillo

La figura 46a) muestra la imagen de un rostro que se utilizó para realizar el análisis de seguridad al encriptado sencillo. Esta imagen se encuentra en formato BMP con escala de grises y es de 256×256 pixeles. En la figura 46b) se presenta su histograma correspondiente. La imagen de la figura 46a) se encriptó con el mapeo caótico de Hénon empleando la técnica de encriptado sencillo propuesta en el capítulo IV.2.1.

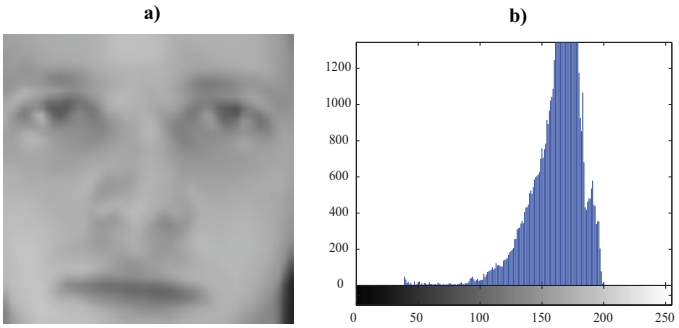


Figura 46: Imagen original y su correspondiente histograma. (a) Imagen original, (b) histograma de la imagen original.

VI.2.1 Resistencia contra ataques de fuerza bruta

Análisis de espacio de claves secretas

La clave del sistema criptográfico propuesto, está compuesto de dos partes: a) Las condiciones iniciales del mapeo, por ejemplo del mapeo de Hénon ($x_1(0)$, $x_2(0)$), b) los parámetros de control del mismo mapeo (a, b y c). De acuerdo al estándar IEEE para aritmética de punto flotante (IEEE, 2008), la presición computacional de los números de doble presición de 64 bits es de 1×10^{-16}, en este trabajo se probó numéricamente para saber hasta que valor (precisión) es sensible el mapeo hipercaótico de Hénon en las variaciones a las condiciones iniciales y parámetros, se encontró que cumple con el estándar IEEE, por lo tanto el espacio de claves es 1×10^{77}, en un sistema binario equivale a 2^{256}. Por tal motivo, el espacio de claves es lo suficientemente grande para resistir todos los tipos de ataques de fuerza bruta, superando los resultados reportados por (Fu *et al.*, 2011; Patidar *et al.*, 2011; Mao y Deng, 2011; Zhang *et al.*, 2010; Chen *et al.*, 2004).

Análisis de sensibilidad

Para hacer esta prueba de sensibilidad al mapeo de Hénon, solamente se hizo una pequeña modificación a la condición inicial del estado x_1, es decir, $x_1(0) = 0.1000000000000001$, el estado x_2 se mantuvo con el valor $x_2(0) = 0.15$, así como también los parámetros $a = 1.4$ $b = 0.3$ y $c = 1$. La figura 47a) muestra la imagen recuperada cuando existe una pequeña diferencia (1×10^{-15}) en la condición inicial $x_1(0)$, en este caso se pueda observar que prácticamente no se recupera informción valiosa. La figura 47b), presenta el histograma de la imagen recuperada cuando existe una diferencia en la condición inicial de $x_1(0)$. Debido a que el histograma de la imagen recuperada empleando condición inicial distinta a la correcta, tiene una distribución uniforme, indica que el algoritmo es muy sensible a variaciones en las condiciones iniciales y paramétricas. Esta sensibilidad a variaciones muy pequeñas son deseables en cualquier sistema criptográfico.

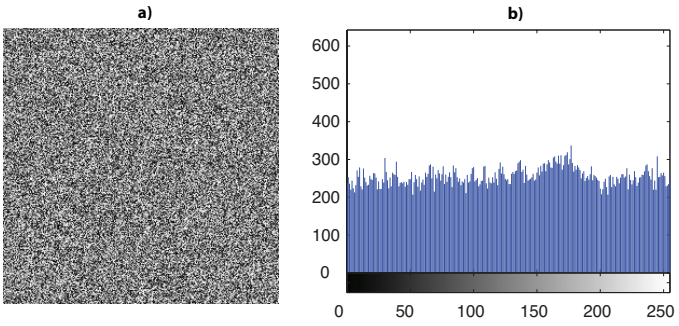


Figura 47: Prueba de sensibilidad a la clave secreta del mapeo de Hénon. (a) Imagen recuperada con un pequeño diferencial en $x_1(0) = 0.1000000000000001$, (b) histograma de la imagen recuperada con diferencia de $x_1(0) = 0.1000000000000001$.

VI.2.2 Análisis estadístico

Histograma estadístico

En la figura 48a) se presenta la imagen original del rostro y en la parte inferior se muestra su histograma correspondiente, esta imagen se encriptó con el mapeo caótico de Hénon empleando la técnica propuesta en el capítulo IV.2.1. En la parte superior de la figura 48b) se muestra la imagen encriptada (criptograma) empleando las condiciones iniciales como clave de encriptado: $x_1(0) = 0.10$, $x_2(0) = 0.15$, con un umbral de cuantización optimizado de 0.30. En la parte inferior de la figura 48b) se muestra el histograma correspondiente al criptograma, se puede observar que en el histograma de la imagen original 48a), la mayor cantidad de información se concentra entre los pixeles que se encuentran en la escala de grises entre 100 y 200, mientras que en el histograma de la figura 48b) (criptograma) la información se dispersó entre todas las tonalidades que están en el rango 0 a 255 de la escala de grises. Sin embargo, cerca de la escala de 150 se observan unos valles, lo cual no es muy deseado en un sistema criptográfico, pues representa una pequeña debilidad del sistema criptográfico desde el punto de vista estadístico. En la figura 48c) se muestra la imagen recuperada en el receptor y su correspondiente histograma, se puede observar que tanto la imagen recuperada como el histograma son iguales a la imagen original, por lo tanto se logró recuperar el 100% de la información.

De igual forma, la imagen de la figura 46a) se encriptó empleando la técnica de encriptado sencillo propuesta en el capítulo IV.2.1, pero ahora utilizando los mapeos caóticos Logistic 1D, gato de Arnold, y los mapeos hipercaóticos de Chen y Rössler. Se calcularon todos los parámetros de seguridad, los cuales se concentran en la tabla I, esto con la finalidad de hacer una comparación del encriptado sencillo y utilizando distintos mapeos caóticos e hipercaóticos. En la tabla I, se observa que el mejor resultado

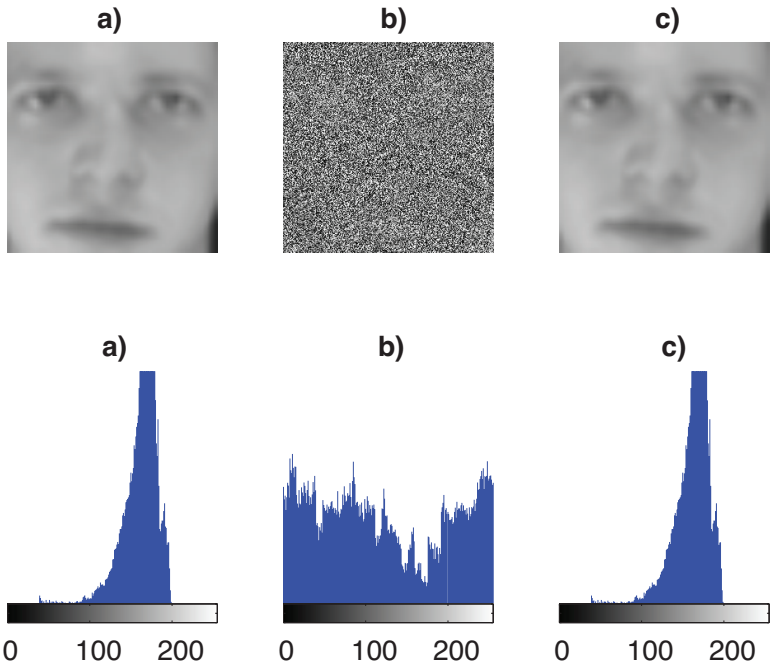


Figura 48: Parte superior: (a) Imagen Original, (b) criptograma obtenido con Hénon, (c) imagen recuperada. Parte inferior: (a) Histogramas de la imagen original, (b) histograma del criptograma, (c) histograma de la imagen recuperada.

de $NPCR$ lo presentan los mapeos de Hénon, Logistic 1D y Rössler. En cuanto al parámetro $UACI$, el mejor resultado lo tiene el hipercaótico de Rössler, en segundo término se encuentra el mapeo de Hénon. El mejor resultado de coeficiente de correlación horizontal lo presenta el mapeo Logistic 1D, posteriormente el hipercaótico de Chen. Mientras que el mejor coeficiente de correlación vertical lo tiene el hipercaótico de Rössler, le sigue el mapeo gato de Arnold. En cuanto al coeficiente de correlación en forma diagonal, el mejor valor lo tiene nuevamente el hipercaótico de Rössler, en segundo término se encuentra Hénon. En lo que se refiere a entropía de la información, el mapeo que presenta mejor aleatoriedad es el gato de Arnold, posteriormente se encuentra el mapeo Logistic 1D. Por último, el mapeo hipercaótico de Rössler es el que tiene mejor espacio de claves, esto es debido a que tiene la mayor cantidad de parámetros y condiciones iniciales, lo que permite incrementar exponencialmente el espacio de claves,

en este caso es de 2^{524}, en segundo lugar se encuentra el mapeo caótico de Hénon, con un espacio total de 2^{256}. En general podemos decir, que los 5 mapeos utilizados para el encriptado sencillo presentan buenos resultados en cuanto a nivel de seguridad se refiere. Sin embargo, la distribución de los histogramas de los criptogramas (ver parte inferior de la fig. 48b), no son completamente uniformes, lo que hace que tengan cierta debilidad en cuanto a los ataques del tipo estadístico. Por tal motivo, se propone aplicar un doble encriptado para mejorar la distribución de los histogramas y aumentar un poco la entropía de la información, esto con la finalidad de poder garantizar con mayor seguridad la privacidad de la información biométrica.

Tabla I: Comparación de resultados del encriptado sencillo entre distintos mapeos.

Parámetro		**Encriptado sencillo con un mapeo caótico**				
		Hénon	Logistic 1D	gato de Arnold	Chen	Rössler
Sensibilidad	Clave	SI	SI	SI	SI	SI
	Plaintext	SI	SI	SI	SI	SI
	NPCR(%)	100	100	99.51	99.99	100
	UACI(%)	39.40	37.39	33.88	33.25	42.09
Coefs. de correlación	Horizontal	-0.0207	-0.0023	-0.0105	0.0031	-0.0157
	Vertical	-0.0260	-0.0133	0.0047	0.0404	0.0002
	Diagonal	0.0032	0.0168	-0.0041	-0.0043	-0.0017
Entropía de la información		7.9195	7.9698	7.9969	7.9622	7.82
Espacio de clave		2^{256}	2^{106}	2^{156}	2^{212}	2^{524}

VI.3 Doble encriptado con el mismo mapeo

Los resultados presentados en esta sección para demostrar la eficiencia y seguridad del algoritmo de doble encriptado caótico con el mismo mapeo, aplicado al sistema de reconocimiento de rostros y propuesto en este trabajo, también emplea la imagen original mostrada en la figura 46a), con tamaño de 256×256 pixeles en escala de grises. La figura 46b) presenta el histograma correspondiente a la imagen original.

La imagen mostrada en la figura 46a) se encriptó utilizando mapeo hipercaótico de Rössler empleando la técnica propuesta en el capítulo IV.3.1, la cual consiste en doble encriptado empleando el mismo mapeo, en este caso específico se utilizaron los estados x_1 y x_2 del mapeo de Rössler, los umbrales optimizados para cuantizar los estados x_1 y x_2 son 0.59 y 0.57 respectivamente.

VI.3.1 Resistencia contra ataques de fuerza bruta

Análisis de espacio de claves secretas

Como se mencionó anteriormente, la clave del sistema criptográfico propuesto, está compuesto de dos partes: a) Las condiciones iniciales del mapeo, por ejemplo del hipercaótico de Rössler ($x_1(0)$, $x_2(0)$, $x_3(0)$), b) los parámetros de control del mismo mapeo (α, β, γ, δ, ζ, η y θ). De acuerdo al estándar IEEE para aritmética de punto flotante (IEEE, 2008), la presición computacional de los números de doble presición de 64 bits es de 1×10^{-16}, en este trabajo se probó numéricamente para saber hasta que valor (precisión) es sensible el mapeo hipercaótico de Rössler en las variaciones a las condiciones iniciales y parámetros, se encontró que cumple con el estándar IEEE, por lo tanto el espacio de claves es 1×10^{160}, en un sistema binario equivale a 2^{531}. Por tal motivo, el espacio de claves es lo suficientemente grande para resistir todos los tipos de ataques de fuerza bruta, superando los resultados reportados por (Fu *et al.*, 2011; Patidar *et al.*, 2011; Mao y Deng, 2011; Zhang *et al.*, 2010; Peng *et al.*, 2009; Chen *et al.*, 2004).

Análisis de sensibilidad

Los resultados experimentales también demuestran que el esquema de doble encriptado es muy sensible a claves secretas (condiciones iniciales y parámetros), para hacer esta prueba de sensibilidad, solamente se hizo una pequeña modificación a la condición inicial del estado x_1, es decir se hizo $x_1(0) = 0.1000000000000001$, los otros dos estados y parámetros mantuvieron los valores originales, osea, $x_2(0) = 0.15$, $x_3(0) = 0.01$, $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.2$, $\eta = 0.1$ y $\theta = 1.9$. La figura 49a) muestra la imagen recuperada cuando existe una pequeña diferencia (1×10^{-15}) en la condición inicial $x_1(0)$, en este caso se pueda observar que prácticamente no se recupera informción valiosa. La figura 49b), presenta el histograma de la imagen recuperada cuando existe una diferencia en la condición inicial $x_1(0)$. Debido a que el histograma de la imagen recuperada con condición inicial distinta a la correcta, tiene una distribución uniforme, indica que el algoritmo es muy sensible a variaciones en las condiciones iniciales y paramétricas.

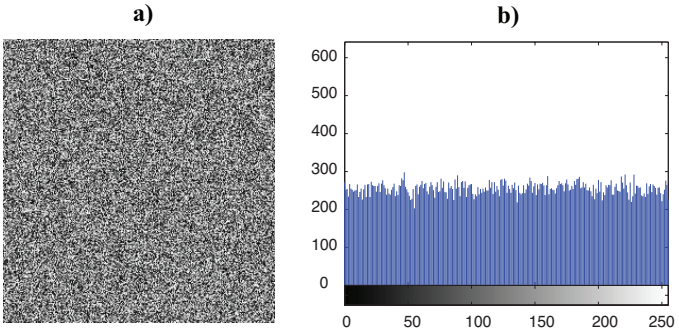


Figura 49: Prueba de sensibilidad a la clave secreta del mapeo de Rössler. (a) Imagen recuperada con un pequeño diferencial en $x_1(0) = 0.1000000000000001$, (b) histograma de la imagen recuperada con diferencia de $x_1(0) = 0.1000000000000001$.

VI.3.2 Análisis estadístico

Histograma estadístico

En la figura 50a) se presenta la imagen original del rostro y en la parte inferior se muestra su histograma correspondiente, esta imagen se encriptó con el mapeo hipercaótico de Rössler empleando la técnica propuesta en el capítulo IV.3.1. En la figura 50b) se muestra la imagen encriptada (criptograma) empleando las condiciones iniciales como clave de encriptado: $x_1(0) = 0.10$, $x_2(0) = 0.15$, $x_3(0) = 0.01$ y en la parte inferior de la figura 50b) se muestra el histograma correspondiente al criptograma. Se puede observar, que en el histograma de la imagen original 50a), la mayor cantidad de información se concentra entre los pixeles que se encuentran en la escala de grises entre 100 y 200, mientras que en el histograma de la figura 50b) (criptograma) la información se dispersó entre todas las tonalidades que están en el rango 0 a 255 de la escala de grises. Por lo tanto, podemos decir, que el sistema es robusto contra ataques de tipo estadístico. En la figura 50c) se muestra la imagen recuperada en el receptor y su correspondiente histograma, se puede observar que tanto la imagen recuperada como el histograma son iguales a la imagen original, por lo tanto se logró recuperar el 100% de la información.

Análisis de correlación de pixeles adyacentes

Se examinó la correlación entre dos pixeles adyacentes en forma horizontal, vertical y diagonal. Para hacer esto, se seleccionaron aleatoriamente 2025 pares de pixeles (x_i, y_i) de la imagen sujeta para análisis (original o encriptada) y se genera la gráfica de dispersión con estas parejas de pixeles adyacentes, es decir se grafica el pixel x_i vs y_i. Posteriormente se calculan sus correspondientes coeficientes de correlación (r_{xy}) utilizando la expresión (17).

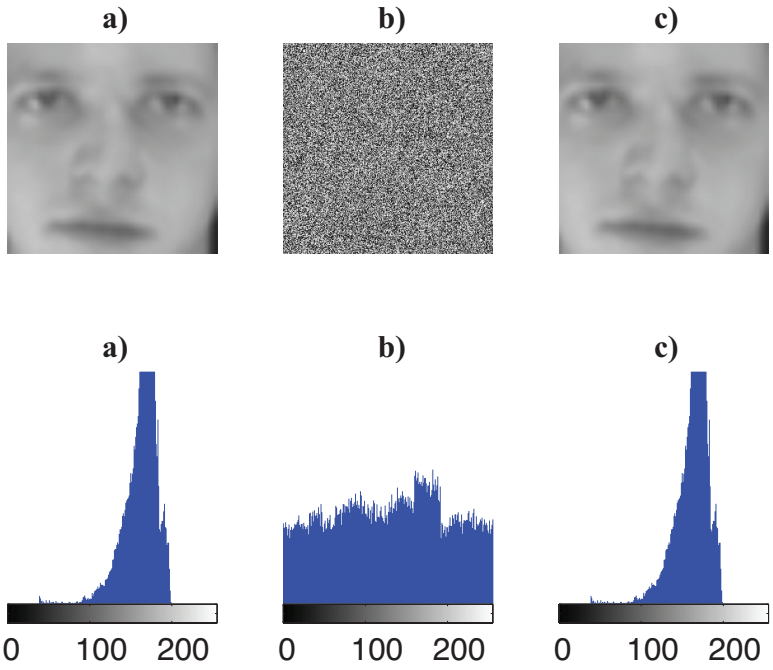


Figura 50: Parte superior: (a) Imagen Original, (b) criptograma obtenido con Rössler, (c) imagen recuperada. Parte inferior: (a) Histogramas de la imagen original, (b) histograma del criptograma, (c) histograma de la imagen recuperada.

La figura 51a), muestra la distribución de correlación de dos **pixeles adyacentes horizontales** de la imagen original (ver fig. 50a)). Utililizando la expresión (17) obtenemos el coeficiente de correlación de 0.9983. La figura 51b) muestra la distribución de correlación de dos pixeles adyacentes horizontales de la imagen encriptada (ver fig. 50b)), de igual forma, empleando la expresión (17) calculamos el coeficiente de correlación de 0.0387.

La figura 52a), muestra la distribución de correlación de dos **pixeles adyacentes verticales** de la imagen original, utililizando la expresión (17) obtenemos el coeficiente de correlación de 0.9972. La figura 52b) muestra la distribución de correlación de dos pixeles adyacentes verticales de la imagen encriptada, empleando la expresión (17) calculamos su coeficiente de correlación de -0.0118.

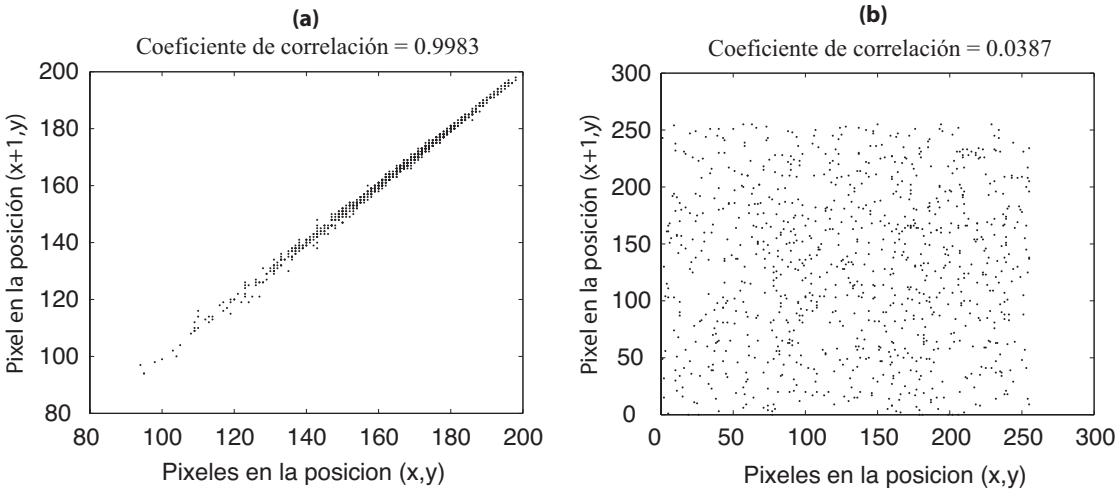


Figura 51: Correlación de dos pixeles adyacentes horizontales: (a) Imagen original, (b) imagen encriptada.

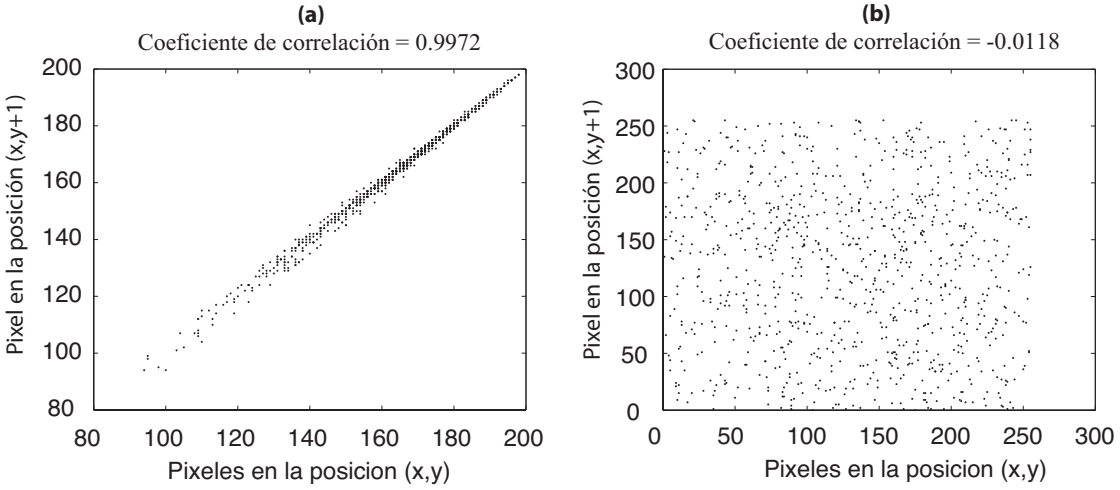


Figura 52: Correlación de dos pixeles adyacentes verticales: (a) Imagen original, (b) imagen encriptada.

La figura 53a), muestra la distribución de correlación de dos **pixeles adyacentes en forma diagonal** de la imagen original, utililizando la expresión (17) obtenemos el coeficiente de correlación de 0.9958. La figura 53b) muestra la distribución de correlación de dos pixeles adyacentes en forma diagonal de la imagen encriptada, empleando la expresión (17) calculamos su coeficiente de correlación de -0.0258.

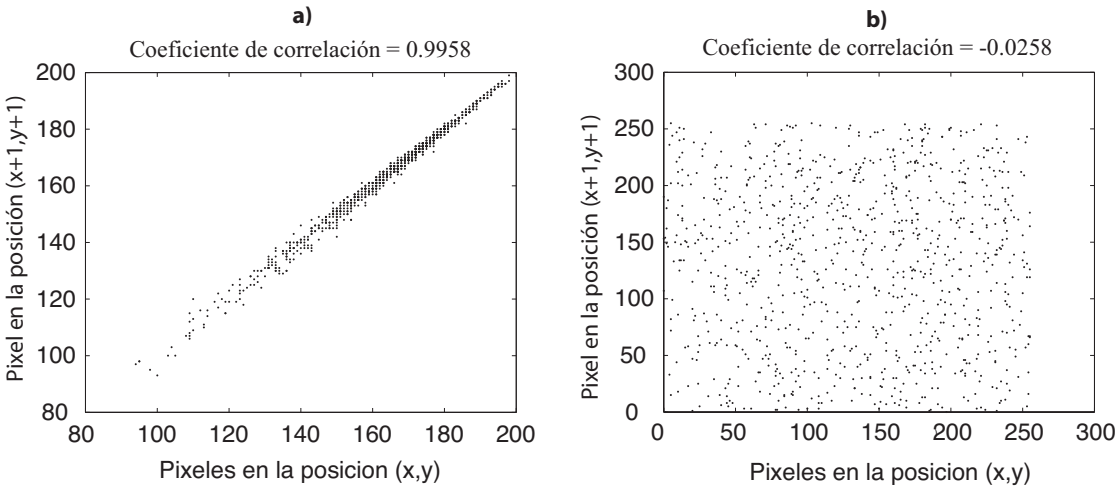


Figura 53: Correlación de dos pixeles adyacentes diagonales: (a) Imagen original, (b) imagen encriptada.

En resumen, cuando se utilizan las condiciones iniciales $x_1(0) = 0.10$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$ como clave de encriptado con el mapeo hipercaótico de Rössler, se obtienen los coeficientes de correlación de dos pixeles adyacentes de la imagen original del rostro y de su correspondiente imagen encriptada, tal como se puede observar en la tabla II. Por otra parte, si hacemos un pequeño cambio en la condición inicial $x_1(0)$, por ejemplo variando una centécima, es decir: $x_1(0) = 0.11$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$, se obtienen los coeficientes de correlación mostrados en la tabla III. Los coeficientes de correlación de la imagen encriptada mostrados en la tabla III, también indican que el hecho de haber modificado un centécima la condición inicial, estos pixeles tienen menos similitud, debido a que el coeficiente de correlación se aproxima más al valor ideal 0. Se

observa que los coeficientes de correlación horizontal y diagonal superan con un poco a los obtenidos en la tabla II. Con esta prueba experimental, se demuestra que los coeficientes de correlación son sensibles a variaciones en las condiciones iniciales ó clave secreta, sin embargo no se pone en riesgo la seguridad de la imagen encriptada, debido a que los coeficientes de correlación se mantienen cercano a cero.

Tabla II: Coeficientes de correlación de dos pixeles adyacentes de la imagen original del rostro y de su correspondiente imagen encriptada, a partir de $x_1(0) = 0.10$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$.

Pixeles	**Imagen original**	**Imagen encriptada**
Horizontal	0.9983	0.0387
Vertical	0.9972	-0.0118
Diagonal	0.9958	-0.0258

Tabla III: Coeficientes de correlación de dos pixeles adyacentes de la imagen original del rostro y de su correspondiente imagen encriptada, a partir de $x_1(0) = 0.11$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$.

Pixeles	**Imagen original**	**Imagen encriptada**
Horizontal	0.9983	0.0256
Vertical	0.9972	-0.0195
Diagonal	0.9958	-0.0134

Entropía de la información

Para evaluar la entropía de la información, del algoritmo de encriptado hipercaótico utilizado en este trabajo, se emplea la expresión (21), primero se calcula la probabilidad de ocurrencia de cada símbolo (pixel), esto con la ayuda del histograma del criptograma. Para el caso del criptograma obtenido con la clave de encriptado $x_1(0) = 0.10$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$, la entropía calculada es $H(s_i) = 7.9830$. Este es un buen resultado, debido a que se aproxima a su valor ideal de 8.

VI.3.3 Ataques diferenciales ($NPCR$ y $UACI$)

Para realizar el análisis contra **ataques diferenciales**, se utilizan claves muy similares para encriptar la imagen original del rostro, en este caso la primer clave de encriptado utilizada es $x_1(0) = 0.10$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$, con esta clave se obtiene el criptograma C_1, la siguiente clave es $x_1(0) = 0.10 + 1e^{-10}$, $x_2(0) = 0.15$ y $x_3(0) = 0.01$ y se obtiene el criptograma C_2. Empleando las expresiones (22) y (23), se obtienen $NPCR = 98.09\%$ y $UACI = 30.78\%$, estos resultados muestran que el algoritmo es fuerte contra ataques diferenciales, debido a que el NPCR es aproximado al valor ideal de 100%.

VI.3.4 Comparación de resultados con otros algoritmos de encriptado basados en caos

En esta sección, se comparan los resultados obtenidos en el análisis de la seguridad realizado en este trabajo de tesis cuando se emplea el esquema de doble encriptado con el mismo mapeo, con otros algoritmos de encriptado basados en caos que han sido reportados recientemente en la litereatura (Patidar *et al.*, 2011; Fu *et al.*, 2011; Zhang *et al.*, 2010; Peng *et al.*, 2009). Esta comparación es relativa, debido a que el tipo de información encriptada no es la misma, sin embargo, los resultados numéricos son muy semejantes y están en el mismo orden o escala, lo que implica todos presentan buenos niveles de seguridad. En la tabla IV, se muestra una comparación entre los distintos tipos de análisis de seguridad realizado recientemente en el encriptado de imágenes y que emplean caos. Las primeras dos columnas contiene los tipos de parámetros que se están utilizando para la comparación. La tercera columna de esta tabla, corrresponde algoritmo de doble encriptado con el mismo mapeo, propuesto en este trabajo de tesis para encriptar imágenes de rostros y contiene los resultados numéricos obtenidos en este

trabajo de investigación. La 4a, 5a, 6a y 7a columna corrresponden a los resultados reportados recientemente en la literatura empleando otros algoritmos de encriptado respectivamente (Patidar *et al.*, 2011; Fu *et al.*, 2011; Zhang *et al.*, 2010; Peng *et al.*, 2009). En la tabla IV, se puede observar que todos estos métodos tienen sensibilidad a la clave y al *plaintext* o imagen original. En cuanto a la comparación del $NPCR$, el resultado en este trabajo es de 98.09%, mientras que (Peng *et al.*, 2009) presenta el mejor resultado con un valor de 99.65%. Respecto al $UACI$, se observa que el mejor resultado lo presenta (Zhang *et al.*, 2010), en este trabajo se obtuvo el resultado con un valor de 30.78%. Por otra parte, haciendo una comparación de los coeficientes de correlación, el trabajo de (Peng *et al.*, 2009) supera a todos los algoritmos en la correlación de pixeles adyacentes en forma horizontal, reportan el valor de 0.0016, mientras que el resultado de este trabajo se obtiene un valor de -0.0020, siendo el segundo lugar de los mejores en cuanto a correlación de pixeles adyacentes en forma horizontal. En cambio, en este trabajo se obtuvo el mejor resultado en correlación de pixeles adyacentes en forma vertical, el valor obtenido es 0.0015. En cuanto a la correlación de pixeles adyacentes en forma diagonal, el mejor resultado lo reporta (Peng *et al.*, 2009) con un valor de 0.0025, mientras que en este trabajo se obtuvo un valor de 0.0064, siendo el tercer lugar. Por otra parte, el trabajo (Zhang *et al.*, 2010) reporta el mejor resultado de entropía de la información, en este caso obtuvieron una entropía igual a 7.9980, muy cercana a la ideal. En este trabajo se obtuvo una entropía de 7.9830. En cuanto al análisis de espacio de clave, el mapeo hipercaótico de Rössler empleado en éste trabajo tiene una sensibilidad de 2^{524}, el cual supera a todos los trabajos comparados en la tabla IV. Como se puede observar, algunos trabajos presentan excelentes resultados en cuanto a entropía de información, otros con respecto a espacio de claves, y otros en cuanto a coeficientes de correlación y sensibilidad. Sin embargo, a nuestro conocimiento, aún no existe un método que supere a todas las técnicas en todos los parámetros de seguridad.

Tabla IV: Comparación de resultados con otros algoritmos de encriptado basados en caos.

Parámetro		**Algoritmo de encriptado**				
		Inzunza, 2012	Vinod, 2011	Chong, 2011	Quiang, 2010	Peng, 2009
Sensibilidad	Clave	SI	SI	SI	SI	SI
	Plaintext	SI	SI	SI	SI	SI
	NPCR(%)	98.09	99.60	99.64	99.61	99.65
	UACI(%)	30.78	33.46	N/A	38	33.46
Coefs. de correlación	Horizontal	-0.0020	0.0028	-0.0254	0.0036	0.0016
	Vertical	0.0015	-0.0062	0.0119	0.0023	-0.0049
	Diagonal	0.0064	N/A	0.0341	0.0039	0.0025
Entropía de la información		7.9830	7.9963	7.9901	7.9980	7.9969
Espacio de clave		2^{524}	2^{161}	N/A	2^{239}	2^{314}
Modelo Caótico		Rössler	Standard	Arnold Cat	Logistic maps	CNN

VI.4 Doble encriptado con distinto mapeo

VI.4.1 Encriptado caótico de patrones de rostros

En la figura 54a) se presenta la imagen de un patrón de rostro y en la parte inferior se muestra su histograma correspondiente, a esta imagen se le aplicó doble encriptado con diferente mapeo, empleando la técnica propuesta en el capítulo IV.3.3, primeramente fue encriptada con el mapeo hipercaótico de Rössler y posteriormente con el mapeo hipercótico de Chen. El umbral optimizado para cuantizar el estado x_1 del mapeo de Rössler es de 0.59, mientras que el umbral optimizado para cuantizar el estado x_2 de Chen es de 0.14. En la figura 54b) se muestra la imagen doblemente encriptada (criptograma) con distinto mapeo, en este caso para el mapeo de Rössler se utilizaron las condiciones iniciales: $x_1(0) = 0.10$, $x_2(0) = 0.15$, $x_3(0) = 0.01$, mientras que para el mapeo de Chen se emplearon las siguientes condiciones iniciales: $x_1(0) = 0.025$ y $x_2(0) = 0.025$. En la parte inferior de la figura 54b) se muestra el histograma correspondiente al criptograma. Se puede observar, que en el histograma de la imagen original

54a), la mayor cantidad de información se concentra entre los pixeles que se encuentran en la escala de grises entre 0 y 100, la cual ilustra que es una imagen muy oscura, mientras que en el histograma de la figura 54b) del criptograma, la información se dispersó de manera uniforme entre todas las tonalidades, las cuales están en el rango 0 a 255 de la escala de grises. Por lo tanto, podemos decir, que el sistema es fuerte contra ataques de tipo estadístico. En la figura 54c) se muestra la imagen recuperada en el receptor y su correspondiente histograma, se puede observar que tanto la imagen recuperada como el histograma son iguales a la imagen original (a), por lo tanto se logró recuperar el 100% de la información.

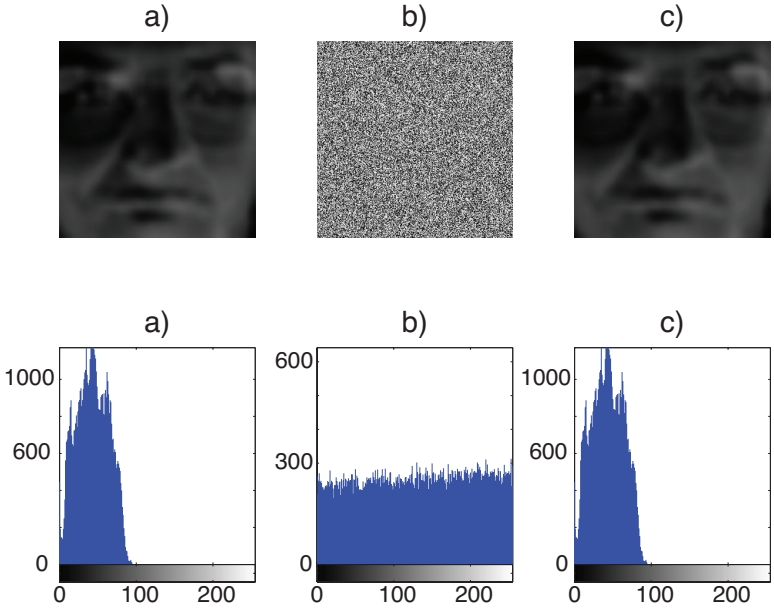


Figura 54: Parte superior: (a) Patrón original, (b) criptograma, (c) patrón recuperado. Parte inferior: (a) Histograma del patrón original, (b) histograma del criptograma, (c) histograma del patrón recuperado.

La tabla V, muestra una comparación de los parámetros de seguridad cuando se hace un doble encriptado a un patrón de rostro y se emplea distinto mapeo caótico. Se puede observar en esta tabla, que la combinación de mapeos Rössler - Hénon es la que presenta mejor $NPCR$ con un valor de 100%, de ahí le sigue la combinación Rössler - Chen, la

cual tien el valor $NPCR = 99.71\%$. En cuanto al parámetro $UACI$, la combinación Rössler - Hénon también presenta el mejor resultado, con un valor de $UACI = 36.59\%$, mientras que en segundo lugar se encuenta la combinación Rössler - Chen, con un valor de $UACI = 34.30\%$. Con respecto al coeficiente de correlación de pixeles horizontales, la combinación Chen - Arnold presentó el mejor resultado, con un valor de $r_{xy} = -0.0010$, en segundo lugar se encuentra la combinación Rössler - Hénon con $r_{xy} = -0.0021$. En lo que se refiere al coeficiente de correlación de pixeles verticales, la combinación Hénon - Arnold presenta el mejor resultado, con un valor de $r_{xy} = 0.0030$, le sigue la combinación Rössler - Chen con $r_{xy} = 0.0073$. Con respecto a la correlación de pixeles ordenados en forma diagonal, la combinación Hénon - Arnold obtiene el mejor resultado, con un valor de $r_{xy} = 0.0016$, en segundo término se encuentra la combinación Rössler - Hénon con $r_{xy} = -0.0017$. En lo que se refiere a espacio de claves, la combinación Rössler - Hénon también presenta el mejor resultado, con un total de posibles combinaciones de clave aproximadamente de 2^{780}, el segundo lugar lo tiene la combinación Rössler - Chen, con un valor de 2^{737}. Finalmente, en cuanto a la entropía de información, la combinación Chen - Arnold presentó el mejor resultado $H(s) = 7.9977$, en segundo lugar se encuentra la combinación Rössler - Arnold con $H(s) = 7.9974$. En general, todos los parámetros de seguridad que se presentan en la tabla V, son excelentes desde el punto de vista criptográfico y de análisis de la seguridad. Sin embargo, la combinación que presenta mayor robustez contra ataques diferenciales y de fuerza bruta es la combinación Rössler - Hénon. Por otra parte, haciendo una comparación, de los resultados mostrados en la tabla IV con respecto a la tabla V, se observa que en su gran mayoría de parámetros de seguridad son muy similares, excepto el parámetro de espacio de claves, en la tabla V presenta mejores resultados en la mayoría de las combinaciones, por lo tanto, el hecho de combinar mapeos, incrementa exponencialmente el espacio de claves y mejora un poco la entropía de información.

Tabla V: Comparación de resultados empleando doble encriptado caótico y distinto mapeo a un patrón de rostro (ver figura 54).

Parámetro		**Combinación de mapeos caóticos**				
		Rössler-Chen	Rössler-Arnold	Chen-Arnold	Hénon-Arnold	Rössler-Hénon
Sensibilidad	Clave	Yes	Yes	Yes	Yes	Yes
	Plaintext	Yes	Yes	Yes	Yes	Yes
	$NPCR(\%)$	99.71%	99.57%	99.60%	99.59%	100%
	$UACI(\%)$	34.30%	33.37%	33.45%	33.39%	36.59%
Coefs. de correlación	Horizontal	-0.0082	-0.0103	-0.0010	0.0054	-0.0021
	Vertical	0.0073	0.0098	-0.0124	0.0030	0.0151
	Diagonal	0.0089	-0.0067	0.0072	0.0016	-0.0017
Entropía de la información		7.9956	7.9974	7.9977	7.9972	7.9534
Espacio de clave		2^{737}	2^{681}	2^{368}	2^{411}	2^{780}

VI.5 Conclusiones

En este capítulo se presentaron los resultados del algoritmo de encriptado sencillo y los algoritmos de doble encriptado. La ventaja del algoritmo de encriptado sencillo es que se ejecuta más rápido y son más prácticos de implementar en aplicaciones que trabajan en tiempo real. Con respecto al análisis de seguridad de este encriptado, se obtuvieron buenos niveles en los parámetros de seguridad, lo cual garantizan la confidencialidad en el envío de la información biométrica a través de una red pública. Con respecto a los algoritmos de doble encriptado, aunque son un poco más lentos, también son factibles de implementar en sistemas que operan en tiempo real. Además, garantizan con mucha seguridad la privacidad de la información confidencial, pues de acuerdo al análisis de seguridad realizado, los parámetros de seguridad se encuentran muy cercanos a su valor ideal, también se observó que mientras más mapeos se utilicen para el encriptado y entre más estados y parámetros contengan estos mapeos, el nivel de seguridad se incrementa considerablemente.

Capítulo VII

Conclusiones generales

En este trabajo de tesis doctoral, se presentó la aplicación del encriptado hipercaótico a un sistema de reconocimiento de rostros que emplea la técnica *eigenface*. Se implementó en computadora un algoritmo de encriptado sencillo y dos algoritmos de doble encriptado. Se realizó un análisis de la seguridad al algoritmo encriptado hipercaótico aplicado a los sistemas de reconocimiento de rostros. Como resultado de la optimización del umbral de cuantización, se logró mejorar los niveles de seguridad de los algoritmos de encriptado propuestos. Para el encriptado de la información, se utilizaron los mapeos de Hénon, gato de Arnold, Logistic 1D, Chen y Rössler. Para evaluar la seguridad de los algoritmos de encriptado propuestos, se les hizo un análisis contra distintos tipos de ataques, por ejemplo, ataques de fuerza bruta (espacio de claves, sensibilidad a condiciones iniciales y parámetros), ataques estadísticos mediante el uso de histogramas y gráficas de dispersión entre pixeles adyacentes, coeficientes de correlación y entropía de la información, también se realizó un análisis contra ataques diferenciales. Se hizo una comparación de los resultados de este análisis de seguridad con respecto a otros experimentos reportados recientemente en la literatura que emplean distintos algoritmos de encriptado caótico. Este análisis de seguridad realizado, indica que los algoritmos de encriptado propuestos en este trabajo de tesis, tienen buenas propiedades deseables desde el punto de vista criptográfico y los resultados muestran que los algoritmos propuestos tienen un desempeño competitivo con respecto a otros algoritmos similares reportados en la literatura actual, ver por ejemplo (Patidar *et al.*, 2011; Fu *et al.*, 2011; Mao y Deng, 2011; Akhshani *et al.*, 2010; Zhang *et al.*, 2010; Behnia *et al.*, 2007, 2008; Chen

et al., 2004; Gao y Chen, 2008; Peng *et al.*, 2009; Rhouma *et al.*, 2009; Mazloom y Eftekhari-Moghadam, 2009; Liu *et al.*, 2009).

La ventaja del modelo hipercaótico utilizado para el doble encriptado (Rössler - Chen), es que tiene alta sensibilidad a las condiciones iniciales y por lo tanto, tiene un gran espacio de claves, que lo hace muy robusto contra ataques de fuerza bruta. Además, presentó muy buenas propiedades estadísticas, que lo hace resistir de forma efectiva contra ataques estadísticos. Los algoritmos propuestos también tienen alta sensibilidad para resistir ataques diferenciales. Por lo tanto, debido que los algoritmos desarrollados en este trabajo tienen un alto nivel de seguridad, se pueden sugerir para encriptar información confidencial de tipo biométrica y transmitirse en forma segura a través de una red pública, tal como la internet. Por último, se recomienda el uso de estos sistemas para el control de acceso en ciertas áreas restringidas, por ejemplo, resguardo de valores, en ciertos sistemas cibernéticos, tales como: banca electrónica, comercio electrónico, operaciones de crédito, sistemas operativos, redes de computadora, etc.

VII.1 Trabajos a futuro

Los algoritmos criptográficos tienen un tiempo de vida finito, siempre será necesario proponer nuevas metodologías cada vez más complejas y seguras para proteger la información confidencial, por lo tanto, quedan algunos problemas abiertos de investigación, que a continuación se enlistan:

- Aplicar el encriptado caótico en sistemas que utilicen otro método de reconocimiento de rostros, tales como: Máquinas de vectores de soporte (SVM), reconocimiento de rostros en 3D, redes neuronales, dual eigenspace, Fisher face, correlación, wavelet, etc.

- Aplicar el encriptado caótico en otros sistemas de identificación biométrica, por ejemplo: en reconocimiento de iris, retina, voz, huella de la mano, palma de la mano, termografía facial, huella digital, etc.
- Aplicar el encriptado caótico sistemas de identificación biométrica multimodales.
- Proponer nuevos algoritmos de encriptado que incrementen el nivel de seguridad de la información encriptada.
- Utilizar nuevos mapeos caóticos con mayor cantidad de estados y parámetros, esto con la finalidad de incrementar el nivel de seguridad del encriptado.
- Discretizar modelos caóticos de múltiples enrrollamientos para evaluar el nivel de la seguridad con estos sistemas caóticos.
- Discretizar modelos hipercaóticos con más de cuatro estados y evaluar el nivel de la seguridad del encriptado.
- Combinar criptografía basada en DNA y caótica, mediante el empleo de nuevos algoritmos de encriptado.
- Combinar criptografía caótica con criptografía cúantica y evaluar la seguridad.
- Implementar todos estos algoritmos de encriptado caótico empleando programación en cómputo paralelo, esto para agilizar el proceso de encriptado y desencriptado, además de incrementar el nivel de seguridad al aumentar la complejidad de las operaciones de difusión y confusión.

Bibliografía

Aguilar-Bustos, A. Y. y Cruz-Hernández, C. (2009). Synchronization of discrete-time hyperchaotic systems: An application in communications. *Chaos, Solitons and Fractals*, **41**: 1301–1310.

Aguilar-Bustos, A. Y., Cruz-Hernández, C., López-Gutiérrez, R. M., y Posadas-Castillo, C. (2008). Synchronization of different hyperchaotic maps for encryption. *Nonlinear Dynamics and Systems Theory*, **8**(3): 221–236.

Aguilar-Bustos, A. Y., Cruz-Hernández, C., López-Gutiérrez, R. M., Cuatle, E. T., y Posadas-Castillo, C. (2010). *Hyperchaotic Encryption for Secure E-Mail Communication*, capítulo Emergent Web Intelligence: Advanced Information Retrieval, páginas 471–486. Springer London.

Akhshani, A., S. Behnia, A. A., Hassan, H. A., y Hassan, Z. (2010). A novel scheme for image encryption based on 2D piecewise chaotic maps. *Optics Communications*, **283**: 3259–3266.

Andrievskii, B. R. y Fradkov, A. L. (2003). Control of chaos: Methods and applications. i. methods. *Automation and Remote Control*, **64**(5): 673–713.

Arnold, V. I. (1988). *Geometrical Methods in the Theory of Ordinary Differential Equations*, página 351. Springer-Verlag, Berlin, Alemania.

Arnold, V. I. y Avez, A. (1968). *Ergodic Problems of Classical Mechanics*, página 286. Benjamin, New York.

Banerjee, S. y Verghese, G. C. (2001). *Nonlinear Phenomena in Power Electronics: Attractors, Bifurcations, Chaos, and Nonlinear Control*. IEEE Press, primero edición.

Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A*, **240**: 50–54.

Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H., y Akhavand, A. (2007). A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. *Physics Letters A*, **366**: 391–396.

Behnia, S., Akhshani, A., Mahmodi, H., y Akhavand, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons and Fractals*, **35**: 408–419.

Bremananth, R. y Chitra, A. (2005). An efficient biometric cryptosystem using auto-correlators. *International Journal of Signal Processing*, **2**(3): 158–164.

Briggs, K. (1990). An improved method for estimating Lyapunov exponents of chaotic time series. *Physics Letters A*, **151**: 27–32.

Buhan, I., Doumen, J., Hartel, P., y Veldhuis, R. (2007). Constructing practical fuzzy extractors using qim. Tech. Rep. TR-CTIT-07-52 1-15p., Centre for telematics and information technology. University of Twente, Enschede.

Chen, B. y Chandran, V. (2007). Biometric based cryptographic key generation from faces. En *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications*, Glenelg, Australia.

Chen, G., Mao, Y., y Chui, C. K. (2004). A symmetric image encryption based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, **21**(3): 749–761.

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

Cruz-Hernández, C. y Martynyuk, A. A. (2010). *Advances in chaotic dynamics and applications, Series: Stability, Oscillations, and Optimization of Systems*, Vol. 4. Cambridge Scientific Publishers.

Deng, X. y Zhao, D. (2011). A single-channel color image encryption based on asymmetric crypto system. *Optics and Laser Technology*, **44**(2012): 136–140.

Eleyan, A. y Demirel, H. (2005). Face recognition system based on PCA and feedforward neural networks. En *Proceedings of Computational Intelligence and Bioinspired Systems*, páginas 935–942, Barcelona, España. Springer-Verlag.

Eleyan, A. y Demirel, H. (2006). PCA and LDA based face recognition using feedforward neural network classifier. En *Proceedings of Multimedia Content Representation, Classification and Security*, páginas 199–206, Istanbul, Turke. Springer-Verlag.

Fateri, S. y Enayatifar, R. (2011). A new method for image encryption via standard rules of CA and logistic map function. *International Journal of Physical Sciences*, **6**(12): 2921–2926.

Fu, C., bin Lin, B., sheng Miao, Y., Liu, X., y Chen, J.-J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics Communications*, **284**: 5415–5423.

Gao, H., Zhang, Y., Liang, S., y Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons and Fractals*, **29**(2): 393–399.

Gao, T. G. y Chen, Z. Q. (2008). A new image encryption algorithm based on hyperchaos. *Physics Letters A*, **372**(4): 394–400.

Giuseppe, G. y Saverio, M. (1999). A system theory approach for designing cryptosystems based on hyperchaos. *IEEE Trans. on Circuits and systems - I: Fundamental theory and applications*, **46**(9): 1135–1138.

Han, F., Hu, J., Yu, X., y Wang, Y. (2007). Fingerprint images encryption via multiscroll chaotic attractors. *Applied Mathematics and Computation*, **185**: 931–939.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, **50**(1): 69–77.

IEEE, C. S. (2008). IEEE standard for floating - point arithmetic. *IEEE std 754 - 2008*, páginas 1–58.

Isaeva, O. B., Yu, J. A., y Kuznetsov, S. P. (2006). Arnold's cat map dynamics in a system of couplep nonautonomous van der pol oscillator. *Physical Review E*, **74**(046207): 1–5.

Itoh, M., Yang, T., y Chua (2001). L.o. conditions for impulsive synchronization of chaotic and hyperchaotic systems. *International Journal of Bifurcation and Chaos*, **11**(2): 551–560.

Jain, A. K. y Uludag, U. (2002). Hiding fingerprint minutiae in images. En *Proc. of third workshop on automatic identification advanced technologies*.

Jain, A. K., Ross, A. A., y Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics*, **14**(1): 1–29.

Jain, A. K., Nandakumar, K., y Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, página 17.

Jain, A. K., Ross, A. A., y Nandakumar, K. (2011). *Introduction to biometrics*, página 311. Springer, New York.

Jakimoski, G. y Kocarev, L. (2001). Chaos cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans. on Circuits and systems - I: Fundamental theory and applications*, **48**(2): 163–169.

Kaplan, J. y Yorke, J. (1979). Chaotic behavior of multidimensional difference equations, in: Functional diferential equations and the approximation of fixed points. *Lecture notes in Mathematics*, **730**: 204–227.

Khan, M. K. (2006). Implementing templates security in remote biometric authentication systems. En *2006 International Conference on Computational Intelligence and Security (CIS' 2006)*, Vol. 2, páginas 1396–1400, Guangzhou, China. IEEE.

Kirby, M. y Sirovich, L. (1990). Application of the karhunen-loeve procedure for the

characterization of human faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **12**(1): 103–108.

Kocarev, L. y Shiguo, L. (2011). *Chaos - based cryptography, theory, algorithms and applications*, página 395. Springer-Verlag, first ed. edición.

Kutter, M., Jordan, F., y Bossen, F. (1997). igital signature of color images using amplitud modulation. En *Proc. SPIE EI.*, Vol. 3022, páginas 518–526, San Jose, CA, USA.

Li, S., Mou, X., y Yuanlong (2001). Improving security of a chaotic encryption approach. *Physics Letters A*, **290**(3-4): 127–133.

Li, T. Y. y Yorke, J. A. (1975). Period three implies chaos. *American Mathematical Monthly*, **82**(10): 985–992.

Linnartz, J. P. y Tuyls, P. (2003). New shielding functions to enhance privacy and prevent misure of biometric templates. En *Proc. Int. Conf. on Audio and Video based Biometric Person Authentication*, Berlin, Heidelberg. Springer-Verlag.

Liu, S., Sun, J., y Xu, Z. (2009). An improved image encryption algorithm based on chaotic system. *Journal of computers*, **4**(11): 1091–1100.

Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., Ahmad, M. A., Dai, J., y Liu, S. (2012). Double image encryption by using arnold transform and discrete fractional angular transform. *Optics and Lasers in Engineering*, **50**(2012): 248–255.

Lu, H., Martin, K., Bui, F., Plataniotis, K. N., y Hatzinakos, D. (2009). Face recognition with biometric encryption for privacy-enhancing self-exclusion. En *DSP 09 of the16th international conference on Digital signal processing*, New Jersey, USA.

Mao, Y. y Chen, G. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. *International Journal of Bifurcation and Chaos*, **14**(10): 3613–3624.

Mao, Y. y Deng, Z. (2011). A new image encryption algorithm of input-output feedback based on multi-chaotic system. *Applied Mechanics and Materials*, **40-41**: 924–929.

Mazloom, A. y Eftekhari-Moghadam, A. M. (2009). Color image encryption based on coupled nonlinear chaotic map. *Chaos, Solitons and Fractals*, **42**(2009): 1745–1754.

Menezes, A. J., Oorschot, P. C. V., y Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Muhammad, K. K., Ling, X., y Jiashu, Z. (2007a). *Robust hiding of fingerprint-biometric data into audio signals*, Vol. 4642, capítulo 5, páginas 702–712. Springer.

Muhammad, K. K., Zhang, J., y Tian, L. (2007b). Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Solitons and Fractals*, **32**: 1749–1759.

Patidar, V., Pareek, N. K., Purohit, G., y Sud, K. K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics Communications*, **284**(2011): 4331–4339.

Pecora, L. M. y Carroll, T. L. (1990). Synchronization in chaotic systems. *Phys. Rev. Lett.*, **64**: 821–824.

Peng, J., Zhang, D., y Liao, X. (2009). A digital image encryption algorithm based on hyper-chaotic cellular neural network. *Fundamenta Informaticae*, **90**: 269–282.

Rhouma, R., Meherzi, S., y Belghith, S. (2009). OCML-based colour image encryption. *Chaos, Solitons and Fractals*, **42**(2009): 1745–1754.

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc.

Shan, M., JieChan, ZhiZhong, y BengongHao (2012). Double image encryption based on discrete multiple-parameter fractional fourier transform and chaotic maps. *Optics Communications*, (http://dx.doi.org/10.1016/j.optcom.2012.06.023).

Shannon, C. E. (1948). Communication theory of security systems. *The Bell System Technical Journal*, **27**: 379–423, 623–656.

Shannon, C. E. (1949). Communication theory of secrecy system. *The Bell System Technical Journal*, **28**(4): 656–715.

Sirovich, L. y Kirby, M. (1987). A low-dimensional procedure for the characterization of human faces. *J. Optical Soc. Am. A*, **4**(3): 519–524.

Smale, S. (1967). Differentiable dynamical systems. *Bulletin of the American Mathematical Society*, **73**(1967): 747–817.

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., y Kumar, B. V. K. V. (1999). *Biometric Encryption*, capítulo 22. McGraw - Hill.

Turk, M. y Pentland, A. (1991a). Eigen face for recognition. *Journal of Cognitive Neuroscience*, **3**(1): 71–86.

Turk, M. y Pentland, A. (1991b). Face recognition using eigenfaces. En *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*, páginas 586–591.

Uludag, U., Gunsel, B., y Tekalp, A. M. (2001). Robust watermarking of busy images. En *Proc. SPIE EI.*, Vol. 4314, páginas 18–25.

Wang, Q., Guo, Q., y Zhou, J. (2012). Double image encryption based on linear blend operation and random phase encoding in fractional fourier domain. *Optics Communications*, (http://dx.doi.org/10.1016/j.optcom.2012.07.033).

Wolf, A., Swift, J. B., Swinney, H. L., y Vastano, J. A. (1985). Determining lyapunov exponents from a time series. *Physica D*, **16**: 285–317.

Zhang, B. L., Zhang, H. H., y Ge, S. S. (2004). Face recognition by applying wavelet subband representation and kernel associative memory. *IEEE Trans. Neural Networks*, **15**(1): 166–177.

Zhang, D. D. (2000). *Automated biometrics technologies and systems*. Kluwer Academic Publishers.

Zhang, L., Liao, X., y Wang, X. (2005). An image encryption approach based on chaotic maps. *Chaos, Solitons and Fractals*, **24**(2005): 759–765.

Zhang, Q., Guo, L., y Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, **52**(2010): 2028–2035.

Zhong, Z., Chang, J., Shan, M., y Hao, B. (2012). Double image encryption using double pixel scrambling and random phase encoding. *Optics Communications*, **285**(5): 584–588.

Apéndice A

Programas desarrollados

Desarrollo de software encriptador de imágenes

En la figura 55, se presenta como ejemplo de aplicación del algoritmo de encriptado caótico de imágenes, una interfaz gráfica desarrollada en Matlab, con este software, se puede capturar una imagen, en la configuración de encriptado, se puede seleccionar el mapeo caótico de Hénon, o bien los mapeos hipercaóticos de Chen y Rössler, luego se deben introducir las claves de encriptado y el umbral de cuantización. Posteriormente se puede encriptar la imagen, archivarla en el disco duro y enviarla por una red pública, tal como la internet.

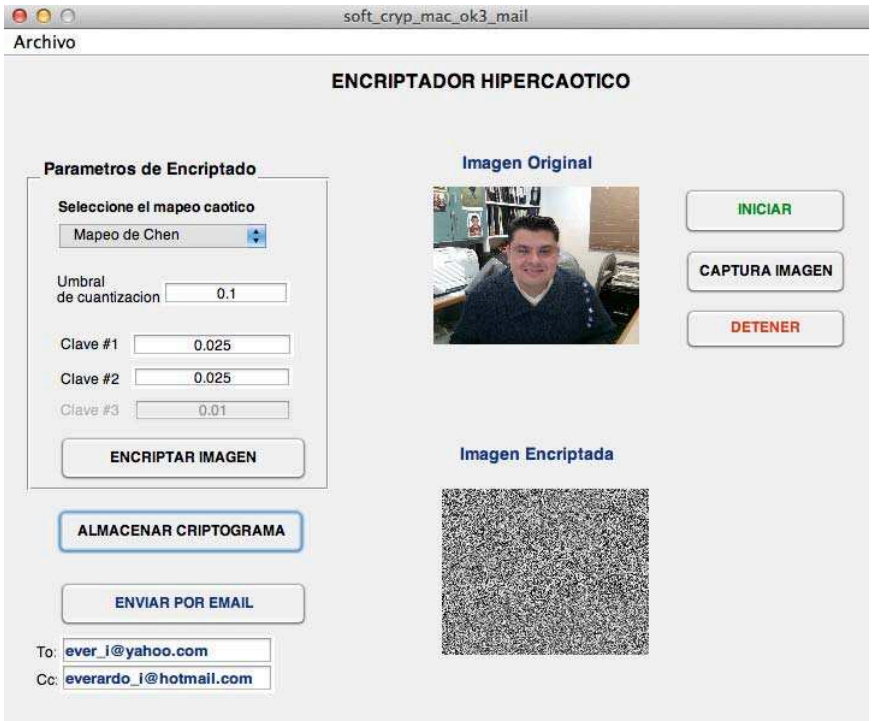


Figura 55: Software encriptador de imágenes.

Desarrollo de software desencriptador de imágenes

En la figura 56, se presenta como ejemplo de aplicación del algoritmo de desencriptado caótico de imágenes, una interfaz gráfica desarrollada en Matlab, con este software, se puede abrir un criptograma, en la configuración de desencriptado, se puede seleccionar el mapeo caótico de Hénon, o bien los mapeos hipercaóticos de Chen y Rössler, luego se debe introducir las claves de desencriptado y el umbral de cuantización. Posteriormente se puede desencriptar la imagen y archivarla en el disco duro de la computadora.

Figura 56: Software desencriptador de imágenes.

Desarrollo de software para reconocimiento de rostros

En la figura 57, se presenta como ejemplo de aplicación del algoritmo de reconocimiento de rostros, empleando el método *eigenfaces*, esta interfaz gráfica también está desarrollada en Matlab, con este software, se pueden registrar N usuarios en la base de datos, se introduce un umbrar como tolerancia para el algoritmo de reconocimiento, posteriormente se calculan los *eigenfaces*, luego el sistema ya está preparado para que lo usuarios soliciten su acceso, en caso de ser un usuario reconocido o registrado previamente, el sistema enviará un mensaje de bienvenida, de lo contrario, le avisará que no encontró información biométrica relacionada y denegará el acceso.

Figura 57: Software para el reconocimiento de rostros.

Desarrollo de software para encriptar patrones

En la figura 58, se presenta la interfaz gráfica principal, de un software desarrollado para encriptar patrones de rostros, con este software, se puede abrir la imagen de un patrón obtenido con el método *eigenface*, posteriormente se configura el encriptado mediante la selección del mapeo caótico de Hénon, o bien, los mapeos hipercaóticos de Chen y Rössler, luego se debe introducir las claves de encriptado y el umbral de cuantización. Posteriormente se puede encriptar el patrón, archivarla en el disco duro y enviarla por la red pública.

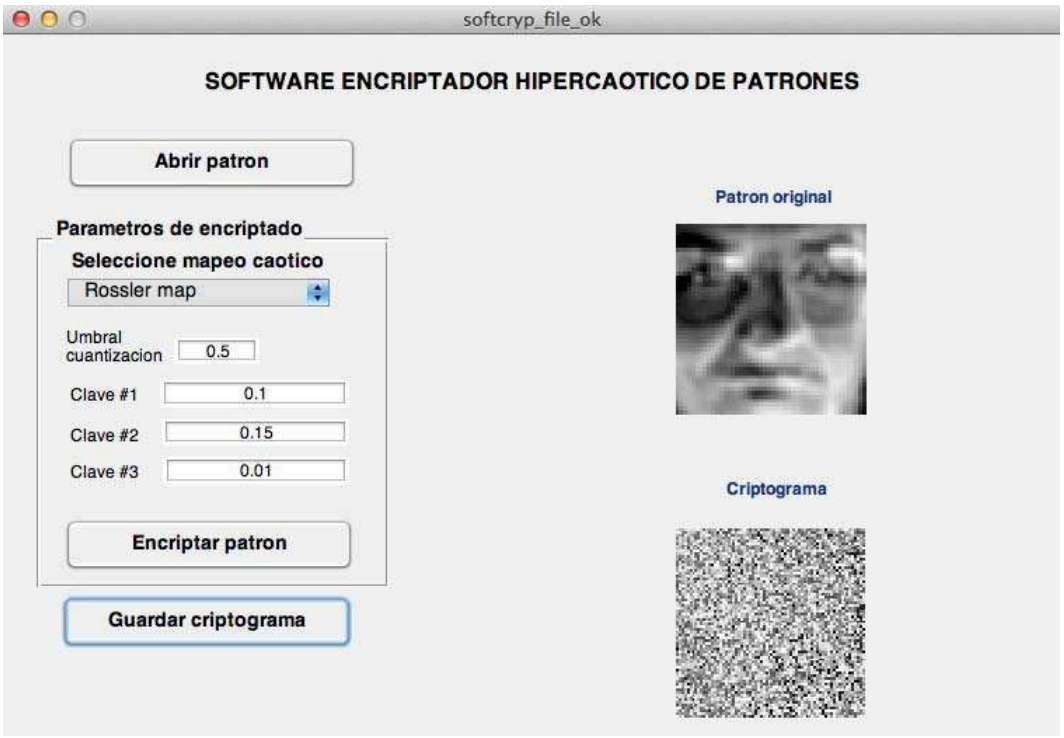


Figura 58: Software para el encriptado de patrones de rostros.

Desarrollo de software para desencriptar patrones

En la figura 59, se presenta la interfaz gráfica principal, del software desarrollado para desencriptar patrones de rostros, con este software, se puede abrir la imagen de un criptograma obtenido con el encriptado hipercaótico, posteriormente se configura el desencriptado mediante la selección del mapeo caótico de Hénon, o bien, los mapeos hipercaóticos de Chen y Rössler, luego se debe introducir las claves de desencriptado y el umbral de cuantización. Posteriormente se puede desencriptar el patrón, archivarlo en el disco duro y hacer la comparación para ver si es un usuario autorizado.

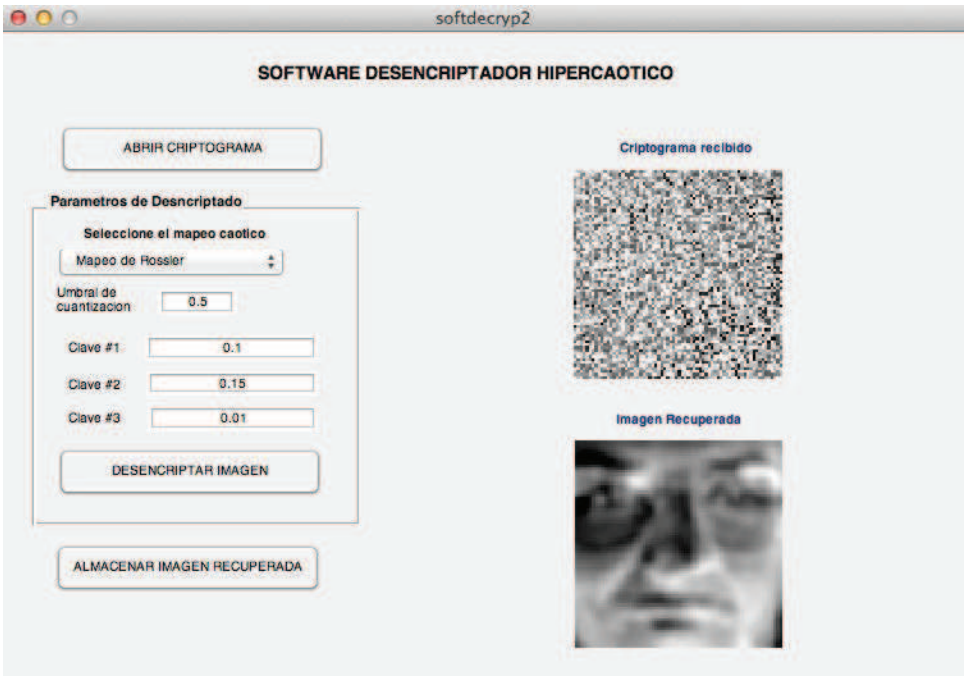


Figura 59: Software para el desencriptado de patrones de rostros.

Apéndice B

Publicaciones derivadas del trabajo de tesis doctoral

Publicaciones en revistas indizadas

E. Inzunza-González, C. Cruz-Hernández, 2013. *Double hyperchaotic encryption for security in biometric systems.* Nonlinear Dynamics and Systems Theory. Aceptado para ser publicado en el 13 (1) 2013.

E. Inzunza-González, C. Cruz-Hernández, H. Serrano-Guerrero, 2013. *Hyperchaotic encryption: An application in biometric systems based on face recognition.* Sometido en AEÜ - International Journal of Electronics and Communications.

E. Inzunza-González, C. Cruz-Hernández, R. M. López-Gutiérrez, E. E. García-Guerrero, L. Cardoza-Avendaño, H. Serrano-Guerreo. 2009. *Software to Encrypt Messages Using Public-Key Cryptography.* World Academy of Science, Engineering and Technology, 54:623-627.

H. Serrano-Guerrero, C. Cruz-Hernández, R. M. López-Gutiérrez, C. Posadas-Castillo, **E. Inzunza-González**. 2010. *Chaotic Synchronization in Star Coupled Networks of 3D CNNs and Its Application in Communications.* International Journal of Nonlinear Sciences and Numerical Simulation, 11(10):572-580.

C. Cruz-Hernández, **E. Inzunza-González**, R. M. López-Gutiérrez, H. Serrano-Guerrero, E. E.García-Guerrero. 2010. *Encrypted audio communication based on synchronized unified chaotic systems.* World Academy of Science, Engineering and Technology, 66:475-480.

R.M. López-Gutiérrez, E. Rodríguez-Orozco, C. Cruz-Hernández, **E. Inzunza-González**, C. Posadas-Castillo, E. E. García-Guerrero, L. Cardoza-Avendaño. 2009. *Secret Communications Using Synchronized Sixth-Order Chuas's Circuits.* World Academy of Science, Engineering and Technology, 54:608-613.

L. Cardoza-Avendaño, R. M. López-Gutiérrez, **E. Inzunza-González**, C. Cruz-Hernández, E. E. García-Guerrero, V. Spirin, H. Serrano. 2009. *Encrypter Information Software Using Chaotic Generators.* World Academy of Science, Engineering and Technology, 54:391-395.

Publicaciones en congresos internacionales

R. M. López-Gutiérrez, C. Cruz-Hernández, A. Aguilar-yañez, L. Cardoza-Avendaño, **E. Inzunza-González**. 2012. *Experimental network synchronization of Chua's circuits using plastic optical fiber: application to communications.* 12th Experimental Chaos and Complexity Conference. Pag. 56, Ann Arbor, Michigan, USA.

C. Cruz-Hernández, R. M. López-Gutiérrez, **E. Inzunza-González**, L. Cardoza-Avendaño. 2009. *Network synchronization of unified chaotic systems in master-slave coupling.* 3er International Conference on Complex Systems and Applications (ICCSA 2009). Pags. 56 - 60, Le, Havre, Normandy, France.

Publicaciones en congresos nacionales

O.R. Acosta Del Campo, E. E. García-Guerrero, C. Cruz-Hernández, **E. Inzunza-González**, R. M. López-Gutiérrez, L. Cardoza-Avendaño, A. Arellano Delgado. 2010. *Encriptado de información confidencial empleando hipercaos.* LIII Congreso Nacional de Física. Boca del Río, Veracruz, México.