

Universidad Autónoma de Baja California



Facultad de Ingeniería, Arquitectura
y Diseño - Campus Ensenada



Maestría y Doctorado en Ciencias e Ingeniería

Seguridad en un Sistema Biométrico Basado en Huellas Dactilares Aplicando Caos

TESIS

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

DOCTOR EN CIENCIAS

Presenta

Fausto Abundiz Pérez

Ensenada, Baja California, Agosto de 2016.

Universidad Autónoma de Baja California
Facultad de Ingeniería, Arquitectura y Diseño - Campus Ensenada

**Seguridad en un Sistema Biométrico Basado en Huellas
Dactilares Aplicando Caos**

TESIS

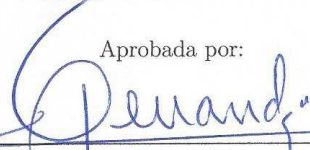
que para cubrir parcialmente los requisitos necesarios para obtener el grado de

DOCTOR EN CIENCIAS

Presenta:

Fausto Abundiz Pérez

Aprobada por:



Dr. César Cruz Hernández
Director de Tesis



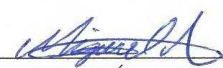
Dra. Rosa Martha López Gutiérrez
Miembro del Comité



Dra. Liliana Cardoza Avendaño
Miembro del Comité



Dr. Adrian Arellano Delgado
Miembro del Comité



Dr. Miguel Ángel Murillo Escobar
Miembro del Comité

Ensenada, Baja California, Agosto de 2016.

Universidad Autónoma de Baja California

Facultad de Ingeniería, Arquitectura y Diseño - Campus Ensenada

Seguridad en un Sistema Biométrico Basado en Huellas Dactilares Aplicando Caos

TESIS

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

DOCTOR EN CIENCIAS

Presenta:

Fausto Abundiz Pérez

Aprobada por:

Dr. César Cruz Hernández
Director de Tesis

Dra. Rosa Martha López Gutiérrez
Miembro del Comité

Dra. Liliana Cardoza Avendaño
Miembro del Comité

Dr. Adrian Arellano Delgado
Miembro del Comité

Dr. Miguel Ángel Murillo Escobar
Miembro del Comité

Ensenada, Baja California, Agosto de 2016.

Resumen de la tesis de **Fausto Abundiz Pérez**, presentada como requisito parcial para la obtención del grado de DOCTOR EN CIENCIAS del programa de Maestría y Doctorado en Ciencias e Ingeniería (MyDCI) de la UABC. Ensenada, Baja California, México. Agosto de 2016.

Seguridad en un Sistema Biométrico Basado en Huellas Dactilares Aplicando Caos

Resumen aprobado por:

Dr. César Cruz Hernández
Director de Tesis

El presente trabajo de tesis versa sobre la implementación de encriptado de imagen de huella dactilar y minucias, así como también función de transformación de minucias con el objetivo de brindarle seguridad a la información biométrica para su empleo en los sistemas de control de accesos. El interés de implementar un encriptado y modificación caótico a la información biométrica (en nuestro caso particular, huella dactilar) en los sistemas de control de accesos, radica en proporcionar una posible solución al problema de seguridad en algunas líneas de comunicación de los sistemas de control de accesos. Para realizar el encriptado y modificación de la información biométrica se recurre al sistema caótico del mapa generalizado de Hénon y el mapa de Rössler que presenta un comportamiento hipercaótico brindando así una mayor seguridad al encriptado y modificación. Como resultado final del trabajo de tesis se obtuvo un cifrado caótico satisfactorio, y una modificación de minucias aceptable en este tipo de sistemas.

Palabras clave: Encriptado, Caótico, Patrones cancelables, Biometría, control de acceso, huellas dactilares.

Dedicatoria

A mi madre Laureana Pérez Leonidez, a mi padre Cleofas Abundis Tecorral, a mi hermano Eduardo Abundiz Pérez y a mi hermana Auria Abundis Pérez, quienes con su apoyo, comprensión, consejos y cariños, que me brindaron, provocaron en mí el entusiasmo de culminar el presente trabajo de tesis. Por dicho motivo les dedico este trabajo.

Agradecimientos

Quiero expresar mi agradecimiento:

- A mi familia, Laureana Pérez Leonidez, Cleofas Abundis Tecorral, Eduardo Abundiz Pérez y Auria Abundis Pérez, quienes en el transcurso de mi vida, siempre me apoyan, aconsejan, educan, asesoran y me alientan a superarme cada día más. Por ese motivo los quiero mucho ya que ustedes son la parte más importante de mi vida.
- Al Dr. César Cruz Hernández quien día con día me asesoro y motivo de manera paciente en cada uno de los procesos realizados para culminar el presente trabajo. Además de ello me alentó a proseguir con mis estudios académicos, lo cual, le agradezco sinceramente.
- A mi comité de tesis, quienes con su apoyo, guía, sugerencias, confianza y amistad me motivaron a culminar mis estudios del grado de Doctor en Ciencias.
- Al Consejo Nacional de Ciencia y Tecnología (CONACyT), quienes me proporcionaron una beca, la cual, fue un gran apoyo económico para realizar mis estudios de posgrados en la Facultad de Ingeniería Campus Ensenada de la Universidad Autónoma de Baja California (UABC).
- Y a todos mis amigos, que me alentaron a proseguir con mis estudios de posgrado sinceramente muchas gracias por su apoyo.

Contenido

1. Introducción	1
1.1. Motivación	1
1.2. Problema de estudio	2
1.3. Objetivos	5
1.3.1. Objetivo General	5
1.3.2. Objetivos específicos	5
1.4. Propuesta de solución	6
1.5. Organización del manuscrito de tesis	7
2. Sistemas biométricos	8
2.1. Introducción	8
2.2. Antecedentes históricos	8
2.3. Identificadores biométricos	9
2.4. Clasificación del sistema biométrico	11
2.5. Estructura de un sistema biométrico	12
2.6. Aplicaciones de los sistemas biométricos	14
2.7. conclusiones	15
3. Caos determinístico	16
3.1. Introducción	16
3.2. Antecedentes históricos	17
3.3. Sistemas caóticos	19
3.4. Aplicaciones de la teoría del caos	24
3.5. conclusión	24
4. Sistemas biométricos de huellas dactilares	25
4.1. Introducción	25
4.2. Huella dactilar	25
4.2.1. Minucias	27
4.2.2. Clasificación de huellas	29
4.3. Comparación de huellas	30
4.4. Estructura de un sistema biométrico de huellas dactilares	31
4.5. Puntos vulnerables	33
4.6. Conclusiones	36

5. Alternativa de encriptado de imagen con mapeo de Rössler	37
5.1. Introducción	37
5.2. Metodología de encriptado y desencriptado	38
5.2.1. Proceso de encriptado	38
5.2.2. Proceso de desencriptado	40
5.3. Resultados experimentales	41
5.3.1. Etapas del proceso de encriptado y desencriptado	41
5.3.2. Análisis de seguridad	42
5.4. Conclusiones	48
6. Solución propuesta	49
6.1. Introducción	49
6.2. Alternativa de encriptado de minucias	49
6.2.1. Formula de Herón	49
6.2.2. Mapa hiper-caótico Generalizado de Hénon	50
6.2.3. Procedimiento de encriptado/desencriptado	51
6.3. Alternativa de modificación de minucias	53
6.3.1. Puntos Singulares	53
6.3.2. Modificación de minucias	54
6.4. Ubicación de encriptado y modificación de minucias	56
6.4.1. Ubicación del encriptado de minucias	56
6.4.2. Ubicación de la modificación de minucias	57
6.5. conclusiones	58
7. Pruebas y resultados	59
7.1. Introducción	59
7.2. Verificación de un usuario	59
7.2.1. Definición de verificación de un usuario	60
7.2.2. Comparación por medio de minucias	60
7.3. Verificación aplicando solo encriptado	63
7.3.1. Verificación aplicando solo modificación	66
7.4. conclusiones	69
8. Conclusiones y trabajos futuros	71
8.1. Conclusiones generales	71
8.2. Trabajos futuros	72
A. Programa final de modificación de minucias	73
A.1. Programa de registro	73
A.2. Programa de verificación de usuarios	75
B. Programa final de encriptado de minucias	79
B.1. Programa de registro	79
B.2. Programa de verificación de usuarios	80

Lista de Figuras

1.1.	Sistemas de Control de Acceso	3
1.2.	Sistemas de Control de Acceso Biométricos	4
1.3.	Sistemas de Control de Acceso con encriptado	5
1.4.	Proceso general de propuesta para cifrado de imagen de huella dactilar.	6
1.5.	Proceso general de propuesta para cifrado de minucias.	7
1.6.	Proceso general de propuesta para generar plantillas cancelables.	7
2.1.	Ejemplos de características biométricas	10
2.2.	Diagrama a bloques de la etapa de inscripción en los sistemas biométricos.	13
2.3.	Aplicaciones de acceso electrónico que utilizan sistemas biométricos.	15
3.1.	Atractor de Lorenz	18
3.2.	Osilaciones no periódicas de Rössler.	21
3.3.	Osilaciones no periódicas de Lorenz.	21
3.4.	Sensibilidad a las condiciones iniciales de Rössler.	22
3.5.	Sensibilidad a las condiciones iniciales de Lorenz.	22
3.6.	Atractores extraños proyectados en el espacio tridimensional.	23
3.7.	Curva de Koch	24
4.1.	Lector de huellas dactilares Digital Persona U.are.U 4500.	27
4.2.	Ilustración de las características relevantes en una huella; a) valles y crestas, b) minucias.	28
4.3.	Tipo de minucias que existen en una huella dactilar.	28
4.4.	Representación de minucias. Esta imagen pertenece a la referencia [MMJP03].	28
4.5.	Clases más comunes del esquema de Galton-Henry.	29
4.6.	Diagrama a bloques de la etapa de inscripción en los sistemas biométricos.	32
4.7.	Diagrama a bloques de la etapa de verificación en los sistemas biométricos.	33
4.8.	Diagrama a bloques de la etapa de identificación en los sistemas biométricos.	33
4.9.	Puntos vulnerables de ataques en los sistemas biométricos.	34
5.1.	Diagrama a bloques de los procesos de encriptado y desencriptado de una imagen.	38
5.2.	Imagen que muestra los resultados obtenidos de las etapas de permutación, difusión, permutación inversa y difusión inversa, cuando se introduce una imagen a las etapas y se utiliza la llave correcta para que se realicen los procesos inversos correctamente.	42
5.3.	Imagen que muestra los resultados obtenidos si no se omite ninguna etapa del proceso de encriptado y desencriptado.	43

5.4.	Imagen que muestra los resultados obtenidos si se omite la etapa de permutación o permutación inversa.	43
5.5.	Imagen que presenta los resultados del encriptado con y sin la etapa de permutación, utilizando la llave (0.1, 0.1, 0.1).	44
5.6.	Gráficas de las correlaciones horizontal, vertical y diagonal de la imagen original (I_o), imagen cifrada sin permutación (I_c) e imagen cifrada con permutación (I_c), utilizando la llave (0.1, 0.1, 0.1)	45
5.7.	Imagen que demuestra la sensibilidad de la llave en el algoritmo criptográfico el cual puede considerar la etapa de permutación u omitirla. La llave que se utiliza para el encriptado es (0,1, 0,1, 0,1) y la llave que se utiliza para el desencriptado es (0,100000000001, 0,1, 0,1)	47
6.1.	3D Mapa hiper-caótico generalizado de Hénon	51
6.2.	Diagrama de encriptado	51
6.3.	Puntos singulares core y delta.	54
6.4.	Punto de referencia (core).	54
6.5.	Distancias entre el punto de referencia y minucias.	55
6.6.	Minucias originales, modificadas y punto de referencia.	56
6.7.	Ubicación de encriptado en el registro.	56
6.8.	Ubicación de desencriptado en la verificación.	57
6.9.	Ubicación de modificador en el registro.	57
6.10.	Ubicación de modificador en la verificación.	58
7.1.	Diagrama ilustrativo de la verificación	60
7.2.	Comparación de dos conjuntos de minucias	61
7.3.	Primeras 16 imágenes de huellas dactilares de la base de datos FVC2002.	62
7.4.	Huella dactilar 101_1 de la base de datos FVC2002.	64
7.5.	Huella dactilar 101_8 de la base de datos FVC2002.	67
7.6.	Minucias de Huella dactilar 101_8	67
7.7.	Minucias de Huella dactilar 101_8	68
7.8.	Minucias modificadas y originales de la Huella dactilar 101_8	68
A.1.	Ventana del programa al iniciar el proceso de registro.	74
A.2.	Ventana que se despliega al pulsar el botón “Leer imagen”.	74
A.3.	Ventana que despliega la imagen de la huella selecciona y sus minucias.	74
A.4.	Ventana de guardado de archivo “.mat”.	75
A.5.	Ventana del programa de registro al finalizar el proceso.	75
A.6.	Ventana del programa al iniciar el proceso de verificación.	76
A.7.	Ventana del programa al presionar “Leer imagen”.	76
A.8.	Ventana del programa mostrando la huella dactilar seleccionada.	77
A.9.	Ventana de extracción de cacarterísticas	77
A.10.	Ventana del programa al presionar “comparar”.	77
A.11.	Ventana del programa que ilustra cuando un usuario es aceptado.	78
B.1.	Ventana del programa al iniciar el proceso de registro.	80
B.2.	Ventana que despliega la imagen de la huella selecciona y sus minucias.	80

B.3.	Ventana del programa al iniciar el proceso de registro.	81
B.4.	Ventana que despliega la imagen de la huella selecciona y sus minucias.	81
B.5.	Ventana del programa que ilustra cuando un usuario es aceptado.	81

Lista de Tablas

2.1. Aplicaciones forenses, gubernamentales y comerciales de sistemas biométricos basados en huellas dactilares.	14
4.1. Comparación entre identificadores biométricos. La información está simbolizada como: Alto (A), Medio (M) o Bajo (B).	26
5.1. Coeficientes de correlación entre dos píxeles de la imagen	45
7.1. Resultados de la comparación de huellas	63
7.2. Algunas comparación de huellas distintas	63
7.3. Primeras 14 minucias de la figura 7.4	64
7.4. Primeras 14 minucias cifradas, de la figura 7.4	65
7.5. Resultados de la comparación de huellas	65
7.6. Comparación despues del encriptado	66
7.7. Resultados de la comparación de huellas modificadas	69
7.8. Comparación de huellas modificadas distintas	69

Capítulo 1

Introducción

1.1. Motivación

Observando los grandes avances que se han obtenido hoy en día en las tecnologías de la comunicación nos podremos dar cuenta que existen diversas formas en las cuales podremos tener una comunicación a distancia, las cuales, pueden ser de carácter personal o laboral, por ejemplo tener una vídeo conferencia con asuntos empresariales para negociar un contrato. Por lo tanto, no es de extrañarse que actualmente diversas operaciones o actividades se realicen en redes de comunicación, por ejemplo las operaciones bancarias que se pueden realizar en portales de internet (banca en línea, Supernet, etc), realizar compras en línea (Mercadolibre, Ebay, Amazon, etc), acceder a foros de internet, tener acceso a un área restringida solo para miembros registrados, entre otras. Por tanto, es común que al utilizar las actividades antes mencionadas emergerán interrogantes sobre la seguridad e integridad de la información proporcionada para tener acceso a estas actividades. Algunas interrogantes que pueden surgir son: ¿Es seguro realizar esta actividad?, ¿Es confiable?, ¿Alguien podría suplantarme para realizar esta actividad u operación?, ¿Mi información puede ser utilizada en otra operación?, etc.

Por motivos de mitigar la desconfianza que podrían generar las interrogantes antes mencionadas, se comenzaron a desarrollar sistemas que automáticamente realizaran un reconocimiento, esto con el fin de brindarles mayor confianza a los usuarios de los servicios mencionados. Uno de los sistemas de reconocimiento automatizado que es más implementados hoy en día son los que utilizan información **biométrica** para reconocer a un individuo.

El tema de los sistemas biométricos ha tomado un gran interés en los recientes años, por tanto no es de sorprenderse encontrar en la literatura diversos artículos referente al tema, algunos ejemplos son las referencias [DMRK14], [KAS⁺15], [COTG14], [dLGALARA03], [Clo10], [Amb02]. También se pueden encontrar libros dedicados a un sistema biométrico o ha identificadores biométricos, ver por ejemplo las referencias [JbP98], [MMJP03], [LJ09], [Vac07], [Dal14], [Zha04], [DM04], [Bol04], [Bol03].

Actualmente existen diversos estudios realizados con respecto al tema de la biometría, algunos estudios son para que el sistema realice rápidamente su trabajo de reconocimiento, por ejemplo la detección de puntos singulares en las huellas, facilita su organización en la base de datos lo que ayuda al proceso de reconocimiento al cotejar las huellas eficientemente, ver las referencias [BKMM13], [HmLH07], [WYY11]. También existen estudios realizados para mejorar la comparación de las huellas dactilares, ejemplo ver la referencia [JC08], otro aspecto de estudio es la seguridad en los sistemas biométricos, ver por ejemplo las referencias [Rob07], [MDFGOG11], [FZ06]. Por tanto, Motivados con la idea de contribuir en una alternativa para mantener la integridad y seguridad de la información biométrica utilizada en los sistemas biométricos de huellas dactilares, en este trabajo de tesis se presenta las alternativas de *modificación de minucias*, *encriptado de minucias* y *encriptado de imagen de huella dactilar*, utilizando un sistema hiper-caótico.

1.2. Problema de estudio

Existe una gran importancia en la seguridad de la información, que se transmite por una línea de comunicación entre un emisor y receptor, por lo tanto, se han desarrollado técnicas para mitigar el riesgo de exposición de la información, una de estas es el encriptado de información, esta técnica consiste en *modificar la información*, de tal manera que sea irreconocible a menos que se cuente con la clave correcta para realizar el proceso inverso, con lo cual se obtiene la información antes de su modificación siendo esta nuevamente legible.

La milicia fue uno de los primeros en considerar la importancia de la confidencialidad de la información que se transmite en una línea de comunicación, debido a las repercusiones que podría traer la exposición de dicha información en un campo de batalla. Pero en la actualidad, debido a las diversas actividades que se realizan de forma remota auxiliándose de una red de comunicación, es de interés público proporcionarle seguridad a la línea de comunicación que se utilizan. Actualmente también se debe de considerar la seguridad en la información almacenada en un área segura, la cual, puede ser una base de datos o un archivo en un edificio, etc. En la mayoría de las ocasiones se desea tener control al acceso a esta información para brindarle seguridad.

Actualmente existen sistemas que restringen el acceso a un servicio, información o pertenencia de un individuo, estos sistemas de control de acceso pueden ser utilizados de forma virtual o física. Algunos ejemplos donde estos sistemas se implementa de forma virtual son: control de acceso a cuentas de correo electrónico, sistemas operativos de computadoras personales, cuentas de foros en internet, servicios bancarios en Internet, entre otros servicios que se realizan en Internet. Ejemplos donde se implementan físicamente son: accesos a laboratorios privados, acceso a edificios gubernamentales, accesos a áreas restringidas en un banco, acceso a instalaciones militares, etc.

La función de un sistema de control de acceso es prácticamente no permitir el acceso o

utilización de algún servicio, condicionando el acceso solo si se presenta la llave correcta, la cual, puede ser una tarjeta magnética, clave numérica, llave física, entre otras. Esto se ilustra en la figura 1.1, sin embargo existe un inconveniente al utilizar las llaves antes mencionadas, el cual es, la facilidad que se tiene para extraviarlas, situación que se presenta en pocas ocasiones al utilizar un identificador biométrico esto es debido a que solo se puede perder el identificador en un accidente físico que sufra la persona, debido a esta propiedad en la actualidad es común encontrarnos con sistemas de control de acceso que utilicen un identificador biométrico como llave para disponer de algún servicio, pero la dificultad de perder el identificador biométrico no es la única ventaja que se tiene al utilizarlos, también poseen otras características que benefician el control de acceso, en el capítulo 2 se mencionarán brevemente las características que poseen los identificadores biométricos.

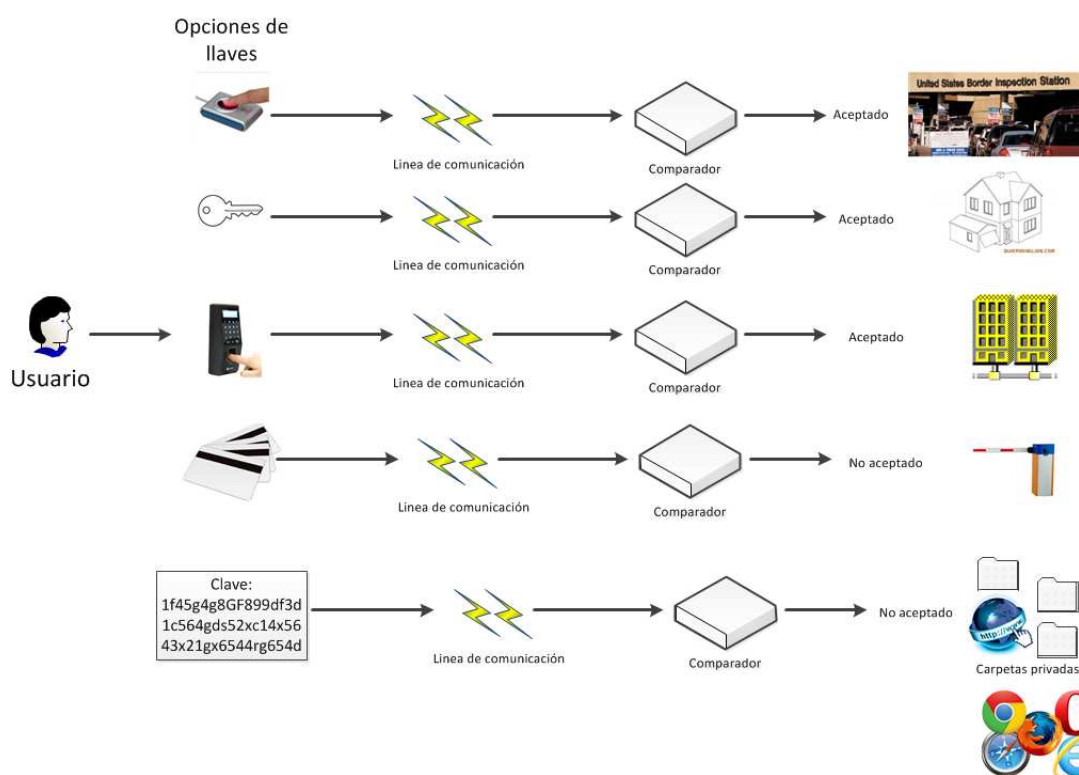


Figura 1.1: Sistemas de Control de Acceso

En la actualidad existen diversos sistemas biométricos de control de acceso, en la figura 1.2 se pueden ver algunos ejemplos, los cuales, pueden estar implementados en un solo dispositivo que realiza todas las etapas del sistema biométrico para reconocer a un individuo, o bien el sistema puede ser compuesto por varios dispositivos distribuidos de manera remota, por ejemplo, una casa puede tener instalada una cerradura electrónica que funcione en combinación con un equipo de identificación biométrica que utilice la huella dactilar para permitir el acceso, en este caso el equipo biométrico contendría todas las etapas requeridas de un sistema de identificación de huellas dactilares. Por otro lado, si hablamos de una

institución en donde se requiere controlar el acceso a diferentes instalaciones del lugar, se requerirá una terminal biométrica para cada una de las instalaciones que requiera controlar el acceso, por tanto se requiere que el sistema biométrico quede distribuido de tal forma que todos los dispositivos biométricos tengan acceso a la información biométrica de los usuarios registrados es decir se debe de considerar una base de datos en común para todos los equipos de identificación biométrica.

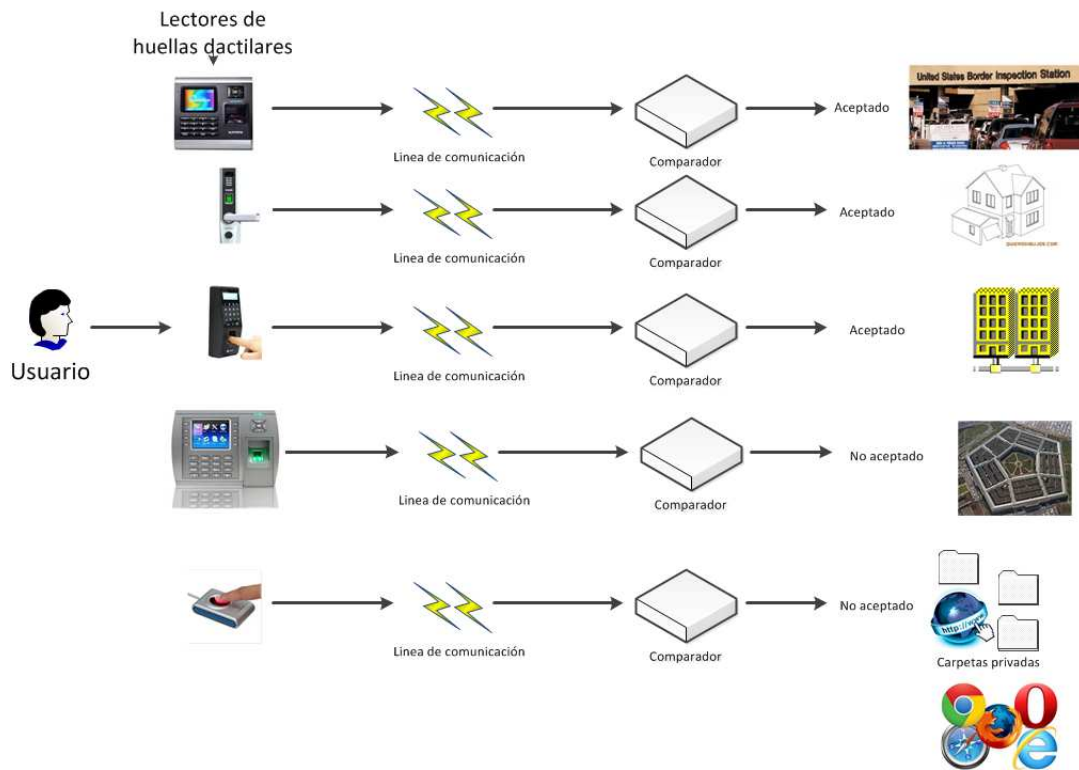


Figura 1.2: Sistemas de Control de Acceso Biométricos

En el escenario planteado anteriormente se puede comprender que la distancia existente entre los elementos que componen un sistema biométrico, pueden contribuir al riesgo de ser expuestos a un ataque en sus líneas de comunicación, por ejemplo, las líneas que conectan la base de datos y las diversas terminales biométricas. La finalidad de los ataques pueden ser para interrumpir la comunicación del sistema biométrico impidiendo el correcto funcionamiento del sistema o el ataque podría consistir en adquirir la información biométrica con la finalidad de utilizarla de manera fraudulenta en el mismo sistema biométrico u otros sistema biométrico que utilice el mismo identificador. Por tal motivo, se considero la necesidad de brindarle protección a la información que se transmite en estas líneas de comunicación, por ejemplo ver la figura 1.3. Algunas medidas que podrían ser utilizadas para mitigar el riesgo a la seguridad del biométrico son el encriptado, generar patrones cancelables, utilizar detección de vida, utilizar sistemas multi-biométricos, entre otros.

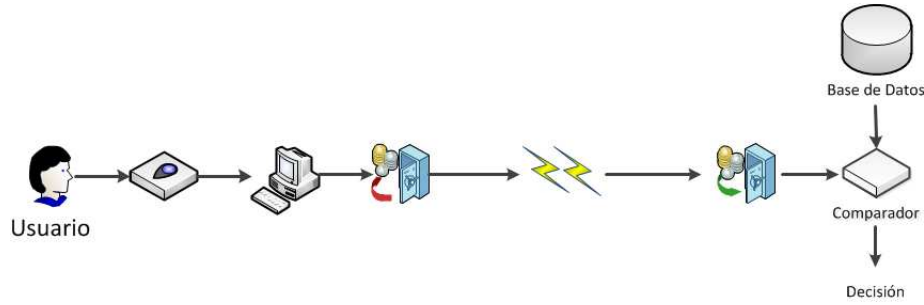


Figura 1.3: Sistemas de Control de Acceso con encriptado

Los sistemas biométricos de control de acceso que se encuentran actualmente en el mercado proporcionan seguridad a la información biométrica utilizando software que utilizan algoritmos de cifrado e integridad, como son el AES y SHA-2 respectivamente. Sin embargo, los algoritmos de cifrado que se utilizan en periodos de tiempo muy extensos, hace que el algoritmo sea analizado durante más tiempo, siendo el propósito de este análisis encontrar alguna forma para decifrar el contenido de la información oculta, y mientras mas tiempo se realice el criptoanálisis se incrementa la posibilidad de quebrantar la seguridad del algoritmo de cifrado.

Al considerar lo mencionado en el párrafo anterior se puede comprender que hacer uso de algoritmos de cifrado convencionales en los sistemas biométricos, represente una posible desventaja en la seguridad de la información biométrica protegida, debido a que estos algoritmos tienen bastante tiempo siendo utilizados. Por tal motivo varios investigadores comenzaron a desarrollar trabajos de investigación enfocados a la seguridad de la información biométrica, uno de los tópicos de investigación son nuevos métodos de cifrado, algunos de estos trabajos se pueden consultar en las referencias [BW12], [KZA11], [HL13], [SHX08], [Liu12]. Otro de los tópicos de estudio es producir plantillas cancelables de la información biométrica, algunos de estos trabajos se pueden consultar en las referencias [LK10], [AHW11], [LCTL07], [YJK09], [XW10], [AH11], , [RCBC06].

1.3. Objetivos

1.3.1. Objetivo General

Utilizar un sistema hiper-caótico para brindarle seguridad a un sistema biométrico de huella dactilar.

1.3.2. Objetivos específicos

- Abordar el problema de verificación de un usuario para el control de acceso
- Seleccionar un sistema caótico para realizar la modificación de minucias.

- Seleccionar un sistema caótico para realizar el cifrado de minucias.
- Seleccionar un sistema caótico para realizar el cifrado de imagen.
- Diseñar un esquema para generar una plantilla cancelable, empleando el sistema caótico seleccionado.
- Diseñar un esquema de cifrado de imagen de huella dactilar utilizando el sistema caótico seleccionado.
- Diseñar un esquema de cifrado de minucias utilizando el sistema caótico seleccionado.
- Probar la plantilla cancelable en un sistema de verificación biométrica.
- Probar y examinar la seguridad del cifrado de imagen de huella dactilar.
- Probar el cifrado de minucias en un sistema de verificación biométrica.

1.4. Propuesta de solución

El trabajo de tesis versa principalmente en el tema de mejorar la seguridad en un sistema biométrico de huella dactilar, protegiendo la información biométrica. Por tal motivo, en el trabajo se proponen tres alternativas de protección de la información biométrica.

La primer propuesta es el cifrado de imagen de la huella dactilar utilizando un sistema hiper-caótico, el objetivo de este proceso es transformar los datos de la imagen para que no sea visible la información biométrica de la huella dactilar, por tanto, aun cuando la imagen sea expuesta ésta no revele ninguna información, con estos se pretende brindarle protección en su almacenamiento y durante su envío. Pero cuando se requiera tener acceso a la información solo se necesita realiza el descifrado. En la figura 1.4 se ilustra esta propuesta.



Figura 1.4: Proceso general de propuesta para cifrado de imagen de huella dactilar.

La segunda propuesta es el cifrado de minucias utilizando un sistema hiper-caótico, el objetivo de este proceso es transformar las características extraídas de la huella dactilar, es decir, cambiar los datos de las minucias, brindando así protección a la información del identificador biométrico mientras se transmite en una línea de comunicación insegura y durante su almacenamiento. Cifrar las minucias representa una ventaja en la seguridad del sistema biométrico debido a que si es expuesta esta no revelara ninguna información de las minucias reales, es decir el criptograma mantendrá la información oculta. En la figura 1.5 se ilustra

esta propuesta.

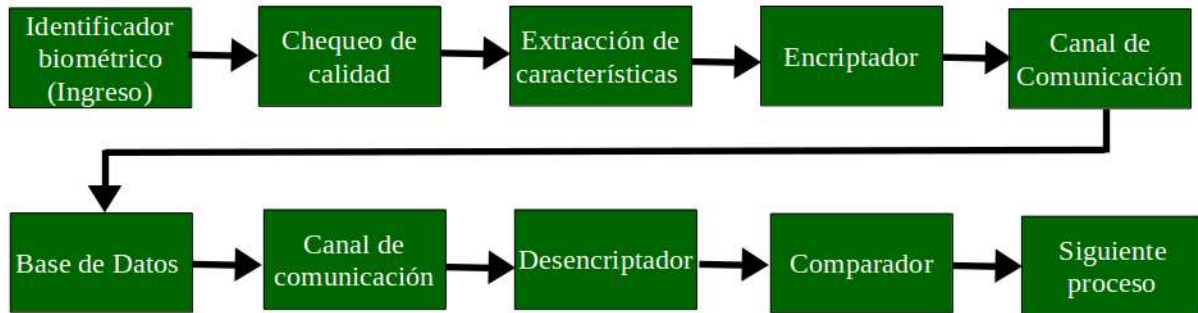


Figura 1.5: Proceso general de propuesta para cifrado de minucias.

La tercer propuesta es un proceso para generar plantillas cancelables utilizando un sistema hiper-caótico, es decir, realizar modificaciones de minucias. El objetivo es brindarle seguridad a la información del identificador biométrico que se transmite en una línea de comunicación insegura o se encuentre almacenada en una base de datos, debido a que si las minucias son expuestas estas pueden ser utilizadas fraudulentamente en cualquier sistema biométrico en donde se empleó este identificador. Generar plantillas cancelables permite que si la información es expuesta pueda ser borrada y remplazada con una nueva minucia modificada, lo que impedirá su utilización fraudulenta en cualquier sistema biométrico. En la figura 1.6 se ilustra esta propuesta.

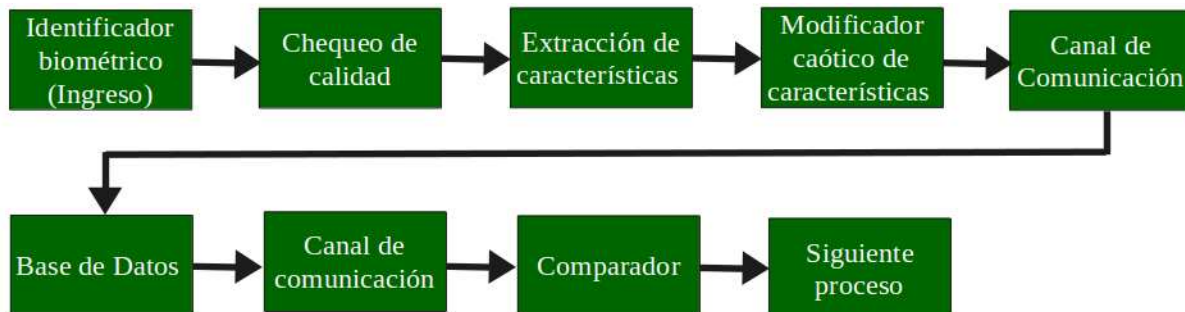


Figura 1.6: Proceso general de propuesta para generar plantillas cancelables.

1.5. Organización del manuscrito de tesis

Capítulo 2

Sistemas biométricos

2.1. Introducción

Este capítulo tiene el propósito de instruir al lector de este trabajo de tesis, en el tema de los sistemas biométricos de una manera breve y concisa, pero lo suficientemente adecuada para que el lector obtenga la información requerida para comprender el tópico. Esto con el objetivo que el lector comprenda la participación y el alcance del trabajo de tesis desarrollado en beneficio de la seguridad de los sistemas biométricos de huella dactilar.

2.2. Antecedentes históricos

La identificación biométrica es un tema que en la actualidad ha tomado una gran importancia en cuestiones de sistemas de seguridad, sin embargo la gran mayoría de la gente ignora que la identificación por medio de una característica biométrica tiene usándose durante mucho por los seres humanos, por ejemplo, se puede comprender de una manera sencilla, cuando reconocemos a una persona que pasa por la calle solo observando su rostro o escuchando su voz, se podría considerar como un reconocimiento biométrico esto aun cuando lo hacemos de manera inconsciente. También existe evidencia de artefactos arqueológicos de que nuestros antepasados reconocieron la individualidad de la huella dactilar, ver referencia [Moe71].

A mediados de 1800 fue una época importante en la identificación biométrica que utiliza las características de las huellas dactilares, debido a los estudios realizados en esta época se establecieron dos principios, que aun se cumplen: no existen huellas dactilares que en los patrones de crestas sean iguales cuando son de distintos dedos y los patrones de las crestas de las huellas dactilares son constantes en el periodo de vida de una persona. Ver referencia [JbP98].

En 1860, el telégrafo fue uno de los medios de comunicación más populares en el mundo, por tanto existieron diversas personas que ejercieron la profesión de telegrafista y mientras ganaban experiencia comenzaron a desarrollar una característica única en el ritmo en teclear

el mensajes. En la Primera Guerra Mundial, los franceses entrenaron a sus operadores de radio para que reconocieran a telegrafistas enemigos que enviaran mensajes en clave Morse identificándolos por su forma de teclear el mensaje, este método de identificación también se utilizó en la Segunda Guerra Mundial en las labores de inteligencia, al cual se le conoció como “fist of the sendel”.

Otro aspecto de importancia en la identificación haciendo uso de la biometría aconteció en 1882 cuando Alphonse Bertillon Jefe de la División de Identificación Criminal del Departamento de Policía de París, desarrolló e implementó la idea de un sistema de identificación de criminales por medio de una serie de mediciones del cuerpo humano. Pero esta idea fue siendo sustituida debido a que se comenzó a ver que utilizar las características de la huella era más confiable que utilizar las medidas del cuerpo humano.

Las técnicas de identificación biométrica que se utilizaban en los años de 1800 eran de forma manual, es decir, una persona tenía que realizar una inspección minuciosa de las características intrínsecas del identificador biométrico, para reconocer a un individuo, por tal motivo, se comenzaron a desarrollar métodos que incrementaran la eficiencia del proceso de reconocimiento, haciendo la búsqueda mas organizada y rápida. La demanda del reconocimiento de individuos por medio de un identificador biométrico comenzó a incrementar. En años posteriores en el tema de la huella dactilar se comenzó a considerar la tecnología de la época para adquirir la lectura del identificador por medio de un dispositivo electrónico, e implementar el reconocimiento automático por medio de procesos computacionales, dando como resultado el ***sistema de reconocimiento automático de huellas*** (AFIS, por sus siglas en inglés Automatic Fingerprint Identification Systems). Para mayor información el lector consultar la referencia [LJ09].

En los años 90's dispositivos económicos, así como eficientes de captura de imágenes de huellas dactilares fueron introducidos en el mercado, este factor ayudo a la aceptación y expansión del reconocimiento biométrico. En la actualidad el reconocimiento biométrico de huella dactilar tiene diversas aplicaciones, esto se debe a lo confiable que resulta la identificación utilizando este método.

2.3. Identificadores biométricos

Un ***identificador biométrico*** es la característica biológica de una persona, que permite su identificación. Actualmente los identificadores biométricos que se utilizan, están clasificados en dos grupos: ***los identificadores físicos*** y ***los identificadores conductuales***, los cuales describimos a continuación:

Identificadores físicos. Estos identificadores biométricos como su nombre lo dice, son partes físicas del cuerpo humano, utilizados para la identificación de una persona, ejemplos

de estos identificadores son: huellas dactilares, geometría de la mano, iris, termografía facial y cornea.

Identificadores conductuales. Estos identificadores biométricos son características que describen una conducta propia de un individuo, como ejemplo se pueden mencionar los siguientes: forma de teclear, reconocimiento de voz y forma de caminar.

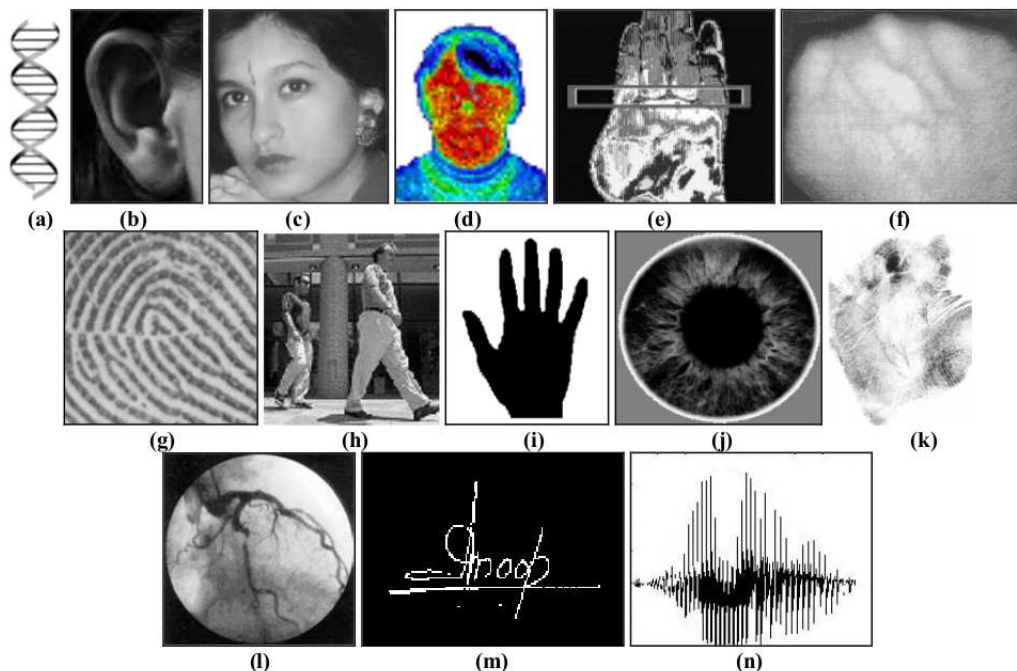


Figura 2.1: Ejemplos de características biométricas: a) ADN, b) Oreja, c) Rostro, d) Termografía facial, e) Termografía de mano, f) venas de la mano, g) huella dactilar, h) Forma de caminar, i) geometría de la mano, j) iris, k) huella de la palma de la mano, l) retina, m) firma y n) voz. Imagen obtenida de la referencia [JbP98]

En la figura 2.1 se muestran algunos identificadores biométricos que se utilizan en la actualidad para el reconocimiento de personas. Aún cuando existen diversos rasgos de conductas o partes físicas en una persona, no todos pueden ser considerados identificadores biométricos, para que sean considerados deben reunir las siguientes propiedades:

Universalidad. Esto se refiere a que todas las personas cuenten con esta característica.

Única. Esto se refiere a que debe ser único para cada persona y que no puede ser igual a otra.

Permanente. Esto se refiere a que la característica debe ser suficientemente invariante en un período largo de tiempo.

Cuantificación. Esto se refiere a que la característica biométrica pueda ser medida cuantitativamente.

Desempeño. Esto se refiere a la velocidad y precisión alcanzable para el reconocimiento, así como el funcionamiento, los factores ambientales que afectan a la precisión como a la velocidad.

Aceptabilidad. Esto se refiere a que tanto se acepta la implementación del identificador biométrico en la sociedad.

Fiabilidad. Este parámetro se refiere a la facilidad de engañar al sistema implementando el identificador biométrico.

Si el lector desea profundizar más en esta información, puede consultar por ejemplo las referencias [MMJP03], [LJ09], [DM04] y [Dal14].//

Nota: Uno de los identificadores biométricos que cumple satisfactoriamente con los atributos mencionados y el cual, es muy utilizado actualmente en los sistemas biométricos, es ***la huella dactilar***. Debido a esto, se tomó la decisión de utilizar este identificador en el proyecto de tesis.

2.4. Clasificación del sistema biométrico

En general, un sistema biométrico es un sistema de reconocimiento de patrones, el cual, determina la autenticidad de una característica fisiológica o conductual, llamada identificador biométrico de un individuo, con el propósito de usarlo para su posterior reconocimiento del individuo. Dependiendo de la aplicación de un sistema biométrico, puede llamarse ***sistema de identificación*** o ***sistema de verificación***, para mayor información el lector interesado consulte la referencia [JbP98]:

Sistema de Identificación. Es un sistema que reconoce a un individuo realizando comparaciones con la muestra (o patrón) biométrica de entrada al sistema biométrico, versus las muestras previas almacenadas en la base de datos. Esto con el motivo de establecer la *identidad del individuo* que previamente se registró en la base de datos. En estos sistemas se establece la identidad del individuo sin necesidad de afirmar una identidad. Se podría decir que la pregunta que se realiza en este sistema es ***¿quién soy yo?***.

Sistema de Verificación. Es un sistema que autentifica la identidad de una persona al comparar la muestra (o patrón) biométrica de ingreso al sistema biométrico, versus la muestra del individuo que previamente fue almacenada en la base de datos del sistema. En este sistema se acepta o rechaza al sujeto que se presenta afirmando una identidad. Se podría decir que la pregunta que se realiza en este sistema es ***¿soy yo quién afirmo ser?***.

La clasificación anterior de los sistemas biométricos no es la única, los sistemas biométricos también se pueden clasificar de acuerdo a los siguientes atributos:

- Sistema en línea o fuera de línea.
- Reconocimiento positivo o negativo.
- Cooperativo o no cooperativo.
- Modo de utilización consciente o inconsciente.
- Utilización habitual o no habitual.
- Supervisado o no supervisado.
- Ambiente controlado o no controlado.
- Aplicación pública o privada.
- Abierto o cerrado.

Las aplicaciones comerciales de los sistemas biométricos tienen popularmente los siguientes atributos: son cooperativos, se utilizan conscientemente, se utilizan habitualmente, de registro atendido, reconocimiento no atendido y ambiente no controlado. Si el lector desea mayor información puede consultar el libro de la referencia [LJ09] de las páginas 4 a la 7.

Actualmente en el mercado hay diversas empresas que hacen uso de identificadores biométricos para la identificación o verificación automatizada de individuos, algunas de estas empresas son: ActivCard, AuthenTec, BIO-Key, Biometric Security Card, Bioscrypt, DigitalPersona, Fujitsu, Identix, Indivos, NEC, NITGen, Precise Biometrics, SecuGen, Sony, ST Microelectronics, Toshiba y Ultra-Scan.

2.5. Estructura de un sistema biométrico

En la actualidad existen una gran cantidad de dispositivos electrónicos de reconocimiento automático que utilizan la tecnología más reciente implementando un sistema biométrico. En la figura 2.2 se muestra un sistema general de identificación biométrica en esta figura se puede observar que en general un sistema biométrico esta constituido por 5 sub-sistemas, siendo estos los siguientes:

Recopilación de información: Este sub-sistema es el encargado de obtener por medio de un sensor la muestra del identificador biométrico para su posterior procesamiento.

Transmisión: Este sub-sistema es el encargado de transmitir el identificador biométrico, considerando una compresión y re-expansion de la información.

Procesamiento de señal: Este sub-sistema es el encargado de verificar la calidad de la muestra obtenida, extraer las características de la muestra biométrica, así como también realizar la comparación de las características biométricas presentadas versus las características almacenadas en la base de datos.

Almacenamiento: Este sub-sistema es el encargado de conservar la información del usuario del sistema biométrico, por ejemplo, la plantilla biométrica, una imagen del identificador biométrico, etc.

Decisión: Este sub-sistema es el encargado de tomar la decisión de aceptar o rechazar el reconocimiento de usuario.

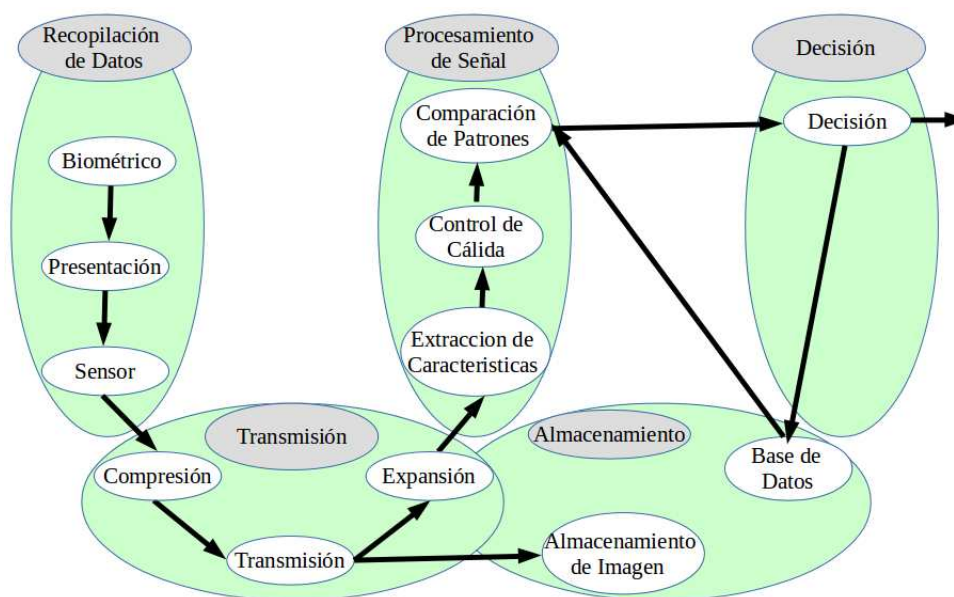


Figura 2.2: Diagrama a bloques de la etapa de inscripción en los sistemas biométricos.

La estructura general de un sistema biométrico está diseñada en base a cuatro módulos principales, que se describen a continuación:

Modulo del sensor. La función de este modulo es capturar el identificador biométrico de un individuo por medio de un dispositivo electrónico.

Modulo de extracción de características. La función de este modulo es procesar los datos del identificador biométrico, para obtener un conjunto de datos más representativos del identificador biométrico.

Modulo de comparación. La función de este modulo es comparar el conjunto de características de entrada al sistema biométrico, versus el conjunto de características almacenadas previamente en la base de datos.

Modulo de base de datos. La función de este modulo es almacenar los datos del identificador biométrico adquiridos en el proceso de registro.

2.6. Aplicaciones de los sistemas biométricos

Los sistemas biométricos tienen diversas aplicaciones pero en esta sección se mencionan algunas basadas en huellas dactilares, siendo esta tecnología comúnmente asociada al *reconocimiento forense*, *identificación de criminales* y *sistemas de seguridad en prisiones*. Sin embargo, existen otras aplicaciones de los sistemas biométricos (ver tabla 2.1 y figura 2.3), los cuales, se pueden clasificar en dos grandes grupos:

1. Aplicaciones de control de acceso de algún servicio como cuentas de correos en internet, banca electrónica y comercio electrónico.
2. Aplicaciones de control de registros; por ejemplo, control de registros médicos y control de registros de emigración.

Para mayor información remitimos al lector interesado consultar la referencia [LJ09].

Forense	Gubernamentales	Comerciales
Identificación de cadáveres	Tarjeta de ID nacional	Inicio de sesión red
Investigación criminal	Correccionales	Seguridad de datos electrónicos
Identificación de terroristas	Licencia de manejo	Acceso en internet
Búsqueda de niños	Seguridad social	ATM, tarjetas de crédito
Entre otros	Control de fronteras	Control de acceso físico
	Control de pasaporte	Teléfonos celulares
	Entre otros	Control de registros médicos
		Entre otros

Tabla 2.1: Aplicaciones forenses, gubernamentales y comerciales de sistemas biométricos basados en huellas dactilares.



Figura 2.3: Aplicaciones de acceso electrónico que utilizan sistemas biométricos.

2.7. conclusiones

Actualmente los sistemas biométricos están siendo utilizados en diversos servicios, por tanto, la integridad y seguridad de estos sistema debe de ir en aumento, con el propósito que el sistema conserve la confianza de los usuarios que utilicen el servicio. Esto indica que la contribución de este trabajo de tesis proporciona un alternativa útil que pueda ser considerada en estos temas.

Capítulo 3

Caos determinístico

3.1. Introducción

En la actualidad el tema de **caos** genera una tremenda fascinación, en los diferentes campos de estudios. Comúnmente cuando se pronuncia la palabra caos en una conversación lo primero en la mente es desorden, confusión, desastre, etc. Esto puede provocar curiosidad y controversia entre los individuos involucrados en la conversación, debido a la diversidad de interpretación de la palabra **caos** en las diferentes ramas de estudio, es decir, su significado puede ser distinto para los matemáticos, físicos, filósofos, médicos, economistas, ingenieros, etc. Pero; ¿qué significado tiene la palabra **caos** en este trabajo de tesis realmente?, debido a esta pregunta se decidió escribir este capítulo, para mencionar algunos aspectos de importancia respecto a este concepto, para brindarle al lector la suficiente información con el objetivo que el lector se familiarice con el tema.

Para contestar la pregunta formulada en el párrafo anterior, primero se dará la definición que proporciona el *Diccionario de la Lengua Española* (Real Academia Española, ver referencia [Esp92]) esta definición es la siguiente:

“Del latín **Chaos** y este del griego $\chi\alpha\omicron\varsigma$, abertura. Estado amorfo e indefinido que se supone anterior a la constitución del cosmos. También, admitido como confusión, desorden”.

Sin embargo, como se mencionó esta palabra puede tener diferente significado según sea el campo de estudio. Por tanto, se decidió buscar una definición más apegada a los campos de la física y matemáticas. En la tesis “El caos y la caracterización de series de tiempo a través de técnicas de la dinámica no lineal” [Esp04], se encuentran las siguientes definiciones:

“**Caos**. En mecánica y matemáticas, es un comportamiento de algunos sistemas dinámicos gobernados por leyes determinísticas, el cual, manifiesta un comportamiento aparentemente azaroso y resulta impredecible a largo tiempo. Por tanto, un nombre más preciso sería **caos determinístico** ...”

“***Caos***. Comportamiento estocástico que ocurre en un sistema determinista.”

Como puede verse en las dos últimas definiciones, se menciona que el **caos** tiene un comportamiento estocástico, sin embargo se presenta en un sistema determinista, estas dos cuestiones ha provocado mucha polémica entre los físicos y matemáticos, debido a que en un sistema determinista su comportamiento puede predecirse y repetirse, bajo las mismas condiciones, mientras que en un sistema estocástico esto no es posible (véase la referencia [Sar07]).

En esta tesis, cuando se mencione sistema caótico, se refiere a que el sistema tiene un comportamiento complejo, que aparenta un total desorden, sin embargo este comportamiento se puede predecir bajo ciertas condiciones y en periodos breves de tiempo.

3.2. Antecedentes históricos

A mediados de 1600 cuando Newton desarrollo las ecuaciones diferenciales descubrió sus leyes de movimiento y de gravitación universal, las cuales posteriormente utilizo para explicar las leyes de Kepler de movimiento planetario, específicamente el problema de dos cuerpos. Posteriormente varios investigadores pretendieron utilizar el método de análisis de Newton en el problema de los tres cuerpos, sin tener resultados. En 1887 el **Rey Oscar** II de Suecia ofreció un premio a quien pudiera determinar si el sistema solar era estable, para poder contestar a esta interrogante primero había que resolver el problema de los tres cuerpos, desafortunadamente nadie pudo hacerlo. Sin embargo, el ganador fue **Jules Henri Poincaré** por sus aportaciones a los estudios de la dinámica de los sistemas complejos, siendo este investigador uno de los primeros en percatarse del fenómeno que ahora llamamos **caos**. Poincaré publicó un trabajo en el que concluyó problema de los tres cuerpos no tiene una solución general mediante las ecuaciones de la mecánica clásica y que un sistema de tres cuerpos es extremadamente dependiente de sus condiciones iniciales. Sin embargo, el trabajo de Poincaré contenía errores, debido a esto, su edición fue sacada de circulación. Las contribuciones que escribió Poincaré referente al tema de caos, fueron olvidados con el pasar del tiempo.

Con la llegada de las súper computadoras también llegó un redescubrimiento del **caos**, el cual, fue hecho por el meteorólogo y matemático estadounidense **Edward N. Lorenz**, considerado por muchos como el descubridor del caos. En 1963 Edward N. Lorenz comenzó a trabajar en unas ecuaciones diferenciales que permitieran predecir el clima. Sin embargo, las ecuaciones que describían el comportamiento del clima requerían el cálculo de miles de operaciones debido a esto, Lorenz se dio a la tarea de simplificar al máximo su sistema de ecuaciones. Esto lo realizó descartando variables que consideró de menor relevancia en el sistema de ecuaciones para predecir el clima, al final, su sistema de ecuaciones consideraba solamente tres variables, **la dirección de los vientos, la presión del aire y la temperatura**, actualmente a este sistema de ecuaciones se les conoce como **ecuaciones de Lorenz**.

Al terminar de plantear sus ecuaciones, Lorenz se auxilió de las computadoras para obser-

var el comportamiento dinámico de su sistema de ecuaciones. Después, el pretendió verificar unos resultados obtenidos durante estas pruebas en computadora pero para ahorrarse tiempo decidió comenzar a la mitad de una de sus pruebas, así que tomó una de las hojas de resultados que había obtenido anteriormente e introdujo estos resultados a la computadora. Debido a que las computadoras en su tiempo eran muy ruidosas y lentas Lorenz decidió salir de su laboratorio, al cabo de una hora decidió volver a checar los resultados de su prueba, se encontró con resultados totalmente distintos a los que había obtenido anteriormente, desconcertado comenzó a verificar si tenía un error en su programa o equipo de computo, pero no encontró nada. Después, habiendo reflexionado se dio cuenta de que al introducir los datos para ahorrar tiempo, él discriminó algunos dígitos y al hacer ésto, los resultados cambiaron. Debido a esto, pudo observar que con cada iteración de sus ecuaciones, el error se iba magnificando, por consiguiente su sistema de ecuaciones tenía un comportamiento que era *sensible a las condiciones iniciales* y gráficamente la trayectoria de este sistema de ecuaciones presentaba un atractor extraño (ver figura 3.1). Con esto Lorenz concluyó que la predicción del clima a largo plazo estaba destinada al fracaso, debido a que cualquier pequeña alteración en el ambiente puede alterar los resultados.

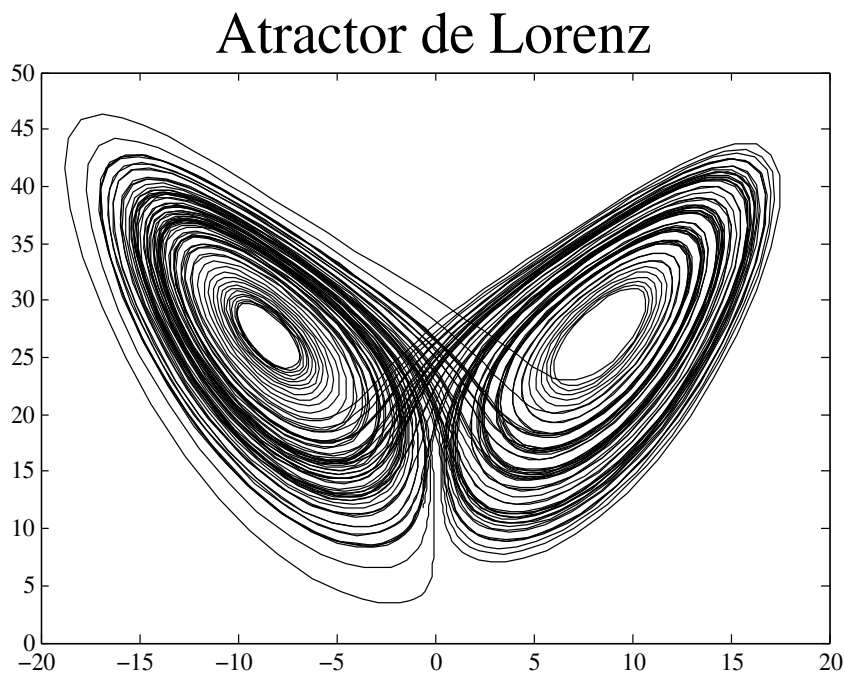


Figura 3.1: Imagen que resulta de graficar una variable con respecto a otra de las ecuaciones de Lorenz conocida como atractor de Lorenz.

En la década de 1970 muchos investigadores interesados en el tema del caos se encontraron con ecuaciones que presentaba un comportamiento caótico, entre las ecuaciones más conocidas están las ecuaciones de Rössler, Logístico y Hénon. Hoy en día, se sabe que el comportamiento caótico está presente en un gran número de sistemas en ingeniería y en la naturaleza.

3.3. Sistemas caóticos

En la ciencia de la física existe una rama que estudia el comportamiento evolutivo en el tiempo de los sistemas físicos, la cual se conoce como dinámica. Para comprender el comportamiento de un sistema dinámico, un aspecto importante que se debe considerar es si está clasificado como lineal o no-lineal, ya que esto permite comprender ciertas características importantes del sistema. a continuación se menciona esta clasificación:

Sistemas lineales. Un sistema lineal es aquel que está formado por un conjunto de ecuaciones lineales (las cuales, pueden ser diferenciales o discretas) que podrían describir el comportamiento de alguna variable física, estas ecuaciones son un planteamiento de igualdad que involucran operaciones de sumas, restas, etc. De una o más variables a la primera potencia. La mayor características de los sistemas lineales es que cumplen con el principio de proporcionalidad y superposición véase [Sar07]. A continuación se muestra un ejemplo de este tipo de sistemas.

$$\begin{aligned} 3\frac{dx_1}{dt} + 2\frac{dx_2}{dt} + \frac{dx_3}{dt} &= 1 \\ 2\frac{dx_1}{dt} + 2\frac{dx_2}{dt} + 4\frac{dx_3}{dt} &= -2 \\ -\frac{dx_1}{dt} + \frac{dx_2}{dt} - \frac{dx_3}{dt} &= 0 \end{aligned}$$

Sistemas no lineales. Un sistema no lineal es aquel que está formado por un conjunto de ecuaciones no lineales (los cuales, pueden ser diferenciales o discretas) que podrían describir el comportamiento dinámico de un variables física, estas ecuaciones son un planteamiento de igualdad que involucran operaciones de suma, resta, multiplicación, etc. De una o más variables a la segunda potencia o a una potencia mayor. La diferencia más notable con respecto a los sistemas lineales es que estos sistemas no cumplen el principio de proporcionalidad y superposición. A continuación se muestra un ejemplo de este tipo de sistemas.

$$\begin{aligned} 3\frac{d^2x_1^4}{dt} + \frac{d^3x_2^6}{dt} + \frac{dx_3^3}{dt} &= 1 \\ 2\frac{dx_1^3}{dt} + 2\frac{dx_2}{dt}x_1^3 + 4\frac{d^3x_3^5}{dt} &= -4 \\ -\frac{d^3x_1}{dt} + x_3^3\frac{d^2x_2^5}{dt} - \frac{d^2x_3}{dt} &= 5 \end{aligned}$$

La región del espacio de estados hacia la cual convergen todas las trayectorias posibles de un sistema dinámico, se llama **atractor**. El comportamiento dinámico de un sistema no lineal puede ser estable, inestable, periódico, caótico, etc. Si el comportamiento del sistema

es estable, sus trayectorias convergen a un punto de equilibrio, si es periódico sus trayectorias convergen a un ciclo límite, ahora si su comportamiento es inestable las trayectorias del sistema escapan a infinito (es decir, no hay una región de atracción) en otras palabras, no existe atractor. Si el comportamiento del sistema es caótico, este presenta un peculiar comportamiento en sus trayectorias, por un lado el sistema exhibe un atractor por el cual, el sistema se ve atraído, pero a su vez escapa de esta zona de atracción, debido a esto su trayectoria forma una imagen de una geometría complicada y con dimensión fractal, siendo esta la razón por la que el atractor de un sistema caótico se le llama ***atractor extraño***.

Un parámetro que nos indica la dependencia de las condiciones iniciales de un sistema caótico son ***los exponentes de Lyapunov***, los cuales, proporcionan información de la divergencia de las trayectorias de un sistema para condiciones iniciales cercanas. Un exponente de Lyapunov positivo, es necesario para indicar la presencia de caos en un sistema dinámico, debido a esto, los exponentes de Lyapunov positivos son utilizados para determinar la complejidad de un sistema caótico (ver por ejemplo [MdlN00]). Los exponentes de Lyapunov son proporcionales al orden del sistema dinámico, es decir, para un sistema de orden N , tendrá N exponentes de Lyapunov.

Se podría decir que los sistemas dinámicos que presentan caos reúnen las siguientes propiedades:

- Son sistemas modelados con ecuaciones diferenciales o en diferencias **no lineales**. A continuación se presentan dos ejemplos, uno en tiempo continuo (Sistema de Lorenz) y otro en tiempo discreto (Mapeo de Rössler):

Mapeo de Rössler

$$\begin{cases} x_1(k+1) = \alpha x_1(k)(1 - x_1(k)) - \beta(x_3(k) + \gamma)(1 - 2x_2(k)), \\ x_2(k+1) = \delta x_2(k)(1 - x_2(k)) + \varsigma x_3(k), \\ x_3(k+1) = \eta((x_3(k) + \gamma)(1 - 2x_2(k)) - 1)(1 - \theta x_1(k)), \end{cases} \quad (3.1)$$

Sistema de Lorenz

$$\begin{cases} \frac{dx}{dt} = \sigma(y(t) - x(t)), \\ \frac{dy}{dt} = rx(t) - y(t) - x(t)z(t), \\ \frac{dz}{dt} = x(t)y(t) - bz(t), \end{cases} \quad (3.2)$$

- Presentan **oscilaciones no periódicas**, ver figuras 3.2 y 3.3 donde se ilustran para el mapeo de Rössler y el sistema de Lorenz, respectivamente.

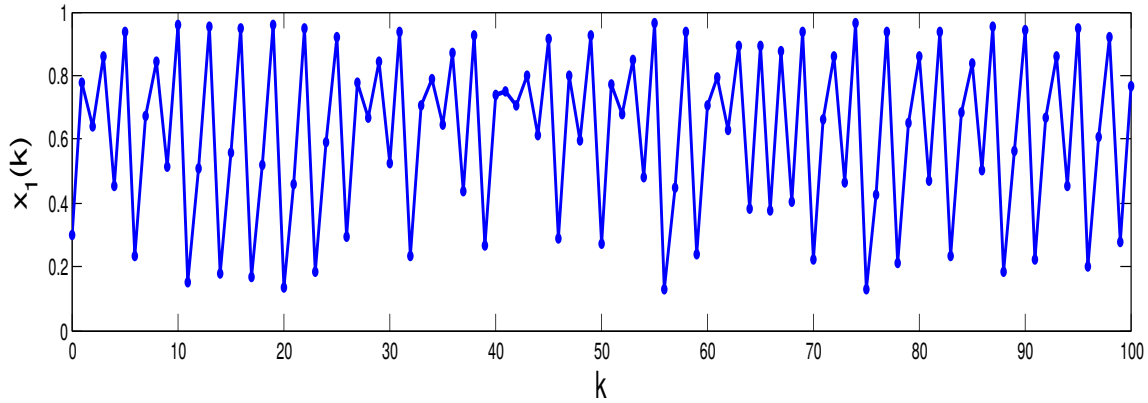


Figura 3.2: Oscilaciones no periódicas de la variable $x_1(k)$ versus el número de iteraciones k de las ecuaciones de Rössler con condiciones iniciales $x(0) = (0.3, 0, 0.05)$ y valores de parámetros $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$ y con $k = 100$ iteraciones.

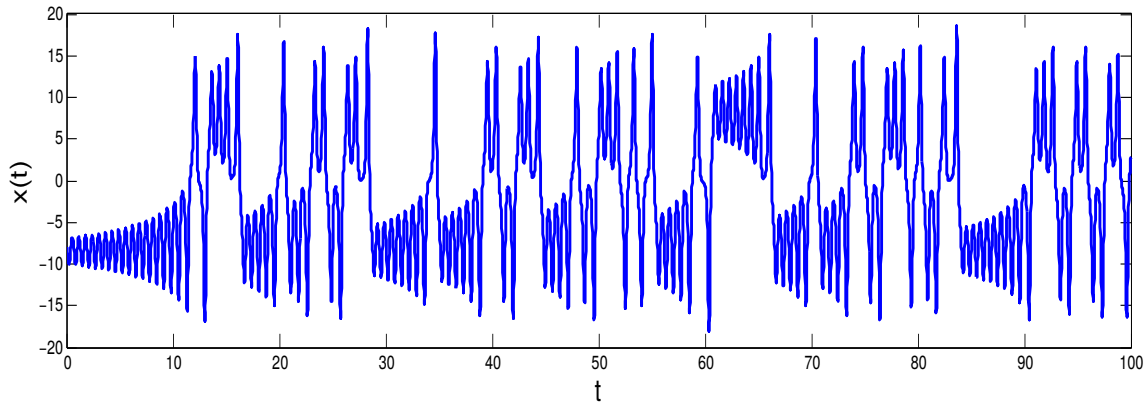


Figura 3.3: Oscilaciones no periódicas de la variable $x(t)$ versus el tiempo t de las ecuaciones de Lorenz con condiciones iniciales $(-8, -8, 24)$ y valores de parámetros $\sigma = 10$, $r = 28$ y $b = \frac{8}{3}$.

- Presentan **sensibilidad a condiciones iniciales**, ver figuras 3.4 y 3.5 para el mapeo de Rössler y el sistema de Lorenz, respectivamente. Nótese la cercanía de las condiciones iniciales que dan origen a dos trayectorias completamente distintas y en un breve lapso de tiempo.

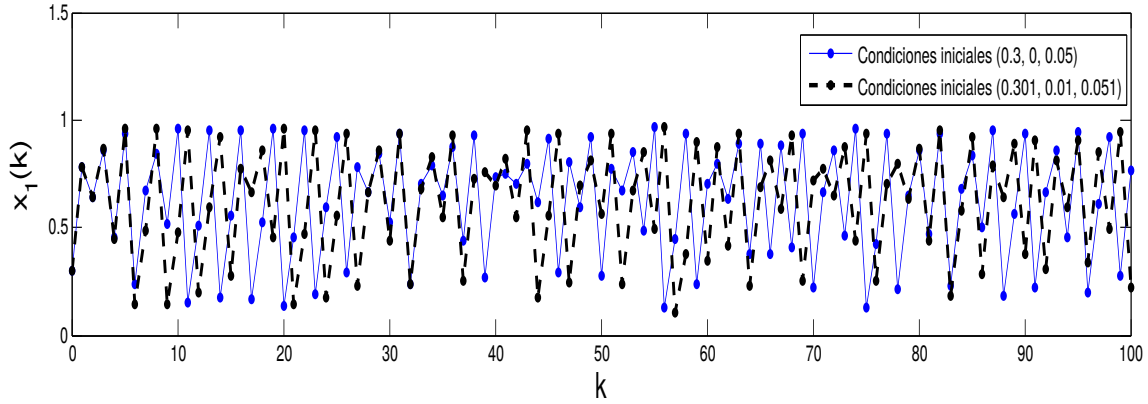


Figura 3.4: Ilustración de la sensibilidad a condiciones iniciales de la variable $x_1(k)$ de las ecuaciones de Rössler con valores de parámetros $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$.

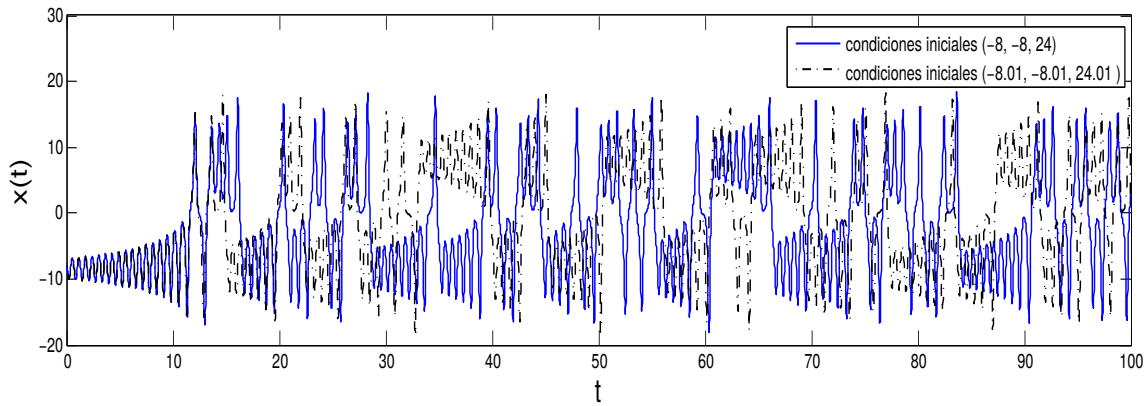


Figura 3.5: Ilustración de la sensibilidad a condiciones iniciales de la variable $x(t)$ de las ecuaciones de Lorenz con valores de parámetros $\sigma = 10$, $r = 28$ y $b = \frac{8}{3}$.

- Generan **atractores extraños** (no son puntos de equilibrio ni ciclos límites), ver figura 3.6.

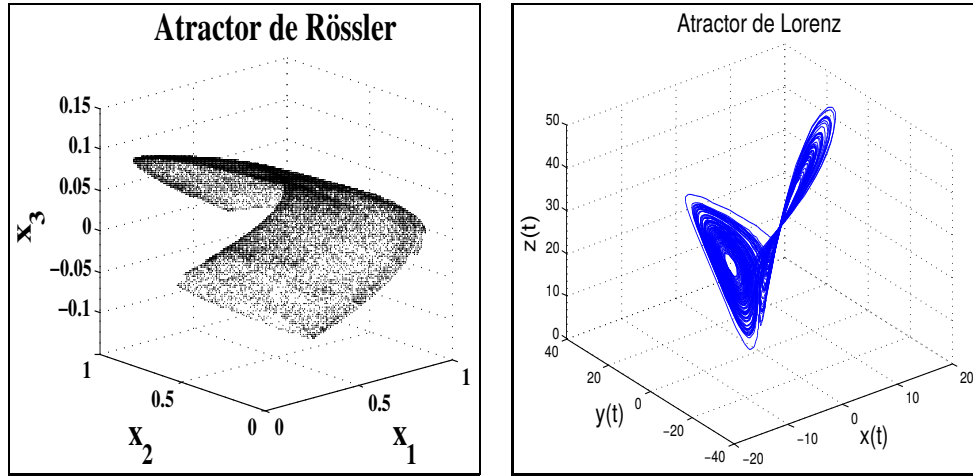


Figura 3.6: Atractores extraños proyectados en el espacio tridimensional.

- Tienen un **exponente de Lyapunov positivo**, los exponentes de Lyapunov para el mapeo de Rössler con los siguientes parametros $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\varsigma = 0.2$, $\eta = 0.1$, $\theta = 1.9$ y condiciones iniciales $(1, 0, 0)$ son: $(\lambda_1=0.313879, \lambda_2=0.019228, \lambda_3=-0.010713)$. Los exponentes de Lyapunov para el sistema de Lorenz con valores de parametros $\sigma = 16$, $r = 40$, $b = 4$ y condiciones iniciales $(0, 1, 0)$ son: $(\lambda_1=1.315952, \lambda_2=0.0, \lambda_3=-22.338674)$. Las expresiones matemáticas para determinar los exponentes de Lyapunov en tiempo discreto y continuo, son por ejemplo como siguen.

$$\left\{ \lambda_i = \frac{1}{KT} \sum_{K=1}^{K-1} \ln \left\| \delta x_i^{(k)} \right\| \quad i = 1, \dots, n \right. \quad (3.3)$$

Ecuación 3.3: Expresión matemática para determinar los exponentes de Lyapunov en tiempo discreto, en donde: λ_i es el i -ésimo exponente de Lyapunov, T es el tiempo entre muestras, x_i es la i -ésima componente de x y δx es la desviación en la trayectoria de dos condiciones iniciales arbitrariamente cercanas. Información obtenida de la referencia [CLG01].

$$\left\{ \lambda = \frac{1}{t} \ln \frac{d(t)}{d_0} \right. \quad (3.4)$$

Ecuación 3.4: Expresión matemática para determinar el exponente de Lyapunov en tiempo continuo, en donde: λ es el exponente de Lyapunov, t es el tiempo entre muestras, d_0 es la separación en el tiempo $t = 0$ de dos trayectorias caóticas cercanas y $d(t)$ es la separación de las trayectorias debido a la divergencia de las trayectorias en el tiempo. Información obtenida de la referencia [Hil00].

- El atractor tiene una **dimensión fractal**. Por ejemplo, ver figura 3.7 donde se ilustra la generación de una figura fractal, es decir, su dimensión no es un número entero, así que los sistemas caóticos su dimensión es un número fraccional.

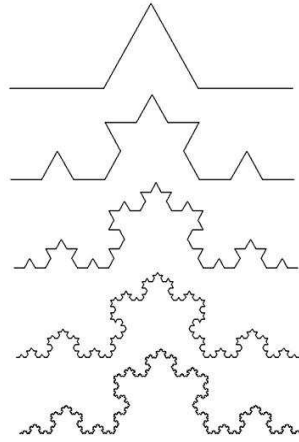


Figura 3.7: Curva de Koch obtenida de la página Web http://labellateoria.blogspot.com/2010_06_01_archive.html

3.4. Aplicaciones de la teoría del caos

La teoría del caos ha tomado gran popularidad por este motivo se realizan investigaciones en diferentes campos de estudios. Por ejemplo, en física se podría estudiar la caída de una hoja, en la biología se podría estudiar el comportamiento de crecimiento de una población y su evolución en el tiempo, en la medicina se podría estudiar la frecuencia cardiaca ejemplo de esto se puede ver en la referencia [CLG01], en la música los tonos que pueden producirse por medio de un sistema caótico ver referencia [Ort00], en la economía se podría estudiar el desarrollo económico de un país, para poder obtener una predicción de su comportamiento futuro. En meteorología se puede nombrar el caso más conocido de la teoría del caos, el cual, es el de Lorenz quien trabajó en unas ecuaciones con las que pretendía predecir el clima. En ingeniería existen reportado muchos estudios donde utilizan sistemas caóticos, por ejemplo podremos mencionar el estudio de encriptado realizado en este trabajo de tesis enfocándose en las comunicaciones seguras de un sistema biométrico.

3.5. conclusión

Actualmente se han desarrollado diversos estudios aplicando caos esto probablemente se deba a las propiedades que tienen los sistemas caóticos. Y por este motivo en este trabajo de tesis se presentan algunas propuestas donde se aplican los sistemas caóticos para brindarle seguridad a un sistema biométrico considerando las propiedades intrínsecas del caos.

Capítulo 4

Sistemas biométricos de huellas dactilares

4.1. Introducción

Uno de los sistemas biométricos más conocido e implementado en dispositivos electrónicos, es el que utiliza la **huella dactilar**, esto posiblemente se deba al entorno amigable que se tiene para poder utilizarlo, es decir, el usuario solo requiere presentar su dedo en un sensor de huellas dactilares para obtener una muestra del identificador que se utilizara para el reconocimiento. Por este motivo, se decidió escribir el presente capítulo con el objetivo que el lector de la tesis tenga una comprensión mas detallada del alcance del trabajo presentado.

4.2. Huella dactilar

Existen una gran variedad de rasgos biométricos, los cuales están siendo utilizados en diferentes aplicaciones de reconocimiento de individuos. La huella dactilar es uno de los más utilizados debido a la buena ponderación cualitativa en sus atributos que cumple satisfactoriamente con lo requerido para ser considerado un identificador biométrico, en la tabla 4.1 se puede apreciar claramente.

La representación de la epidermis de la punta del dedo es conocida como huella dactilar, esta es producida por el sudor y grasas producidas por la piel, cuando un dedo es presentado contra una superficie. Una de las primeras formas de capturar la huella fue por medio de tinta, la imagen que se produce con esta técnica forma patrones de líneas de color negro conocidas como crestas y líneas blancas nombradas valles. Lo ancho de las crestas varia de 100 a 300 μm , el periodo entre un ciclo de crestas/valles es de 500 μm . Las quemaduras, cortes, desgastes o heridas, no afectan la estructura interna que se encuentra debajo de la epidermis, lo que permite la recuperación del patrón original cuando la nueva piel crece.

En la referencia [JCD06], Anil Jain, Yi Chen y Meltem Demirkus mencionan que la huella dactilar contiene varios rasgos importantes que permiten su identificación, los cuales,

se pueden clasificar en tres categorías que se pueden nombrar como niveles:

Nivel 1 (patrones): En este nivel se consideran macro-detalles como el flujo de las crestas que permiten observar patrones que forman las crestas en la huella (arco, bucle, espiral, núcleo, etc). Los patrones que se pueden observar en la huella beneficia mucho en la automatización de la identificación de la huella debido a que por medio de ellas se pueden categorizar las huellas realizando una clasificación para agilizar el proceso de búsqueda en grandes base de datos permitiendo una comparación eficiente y rápida.

Nivel 2 (puntos característicos): En este nivel se consideran regiones específicas que forman las crestas, las cuales, se conocen como características de Galton o puntos característicos (minucias), tales como las bifurcaciones y terminaciones. Las minucias que se pueden observar en la huella dactilar permiten la identificación de las huellas de forma automatizada.

Nivel 3 (forma de poros y crestas): En este nivel se consideran las características de las crestas que no se tomaron en cuenta en los niveles anteriores, por ejemplo, la dimensión de lo ancho de la cresta, su forma, los poros que contiene, los cortes de la cresta, la separación de poros, entre otros detalles. Estas características también son permanentes y únicas, las cuales, pueden aportar información relevante para la identificación.

Identificador Biométrico	Universalidad	Única	Permanente	Cuantificación	Desempeño	Aceptabilidad	Fiabilidad
Huella Dactilar	M	A	A	M	A	M	M
Retina	A	A	M	B	A	B	B
Iris	A	A	A	M	A	B	B
Voz	M	B	B	M	B	A	A
Termografía Facial	A	A	B	A	M	A	B
Geometría de la Mano	M	M	M	A	M	M	M
Firma	B	B	B	A	B	A	A

Tabla 4.1: Comparación entre identificadores biométricos. La información está simbolizada como: Alto (A), Medio (M) o Bajo (B).

Las imágenes utilizadas para los sistemas biométricos basados en huellas dactilares, deben cumplir con algunos *parámetros*, algunos de éstos son: *resolución*, *área*, *número de píxeles*, *contraste* y *distorsión geométrica*. Estos parámetros dependen del dispositivo de captura, la imagen puede tener un rango del valor de sus parámetros. Comúnmente, los píxeles son de valores de 8 bits, los cuales, dan un rango de intensidad de 0 a 255. La resolución de la imagen es el número de píxeles por unidad de longitud, en las imágenes de

huellas dactilares su rango es de 250 puntos por pulgada (100 puntos por centímetro) a 625 puntos por pulgada (250 puntos por centímetro). Siendo un estándar común la resolución de 500 puntos por pulgada (200 puntos por centímetro). El área de la imagen es de 0.5 pulgadas cuadradas (1.27 centímetros cuadrados) a 1.25 pulgadas cuadradas (3.175 centímetros cuadrados), siendo comúnmente el estándar de 1 pulgada cuadrada (2.54 centímetros cuadrados). Para mayor información consultar las referencias [Dav03b] y [Dav03a].

Dependiendo del proceso de adquisición, una imagen de huella dactilar puede clasificarse como “*off-line*” o “*live-scan*”. Una huella clasificada como *off-line* indica que la imagen fue obtenida al manchar las puntas de los dedos con tinta para posteriormente plasmar la huella sobre un papel, que se escaneara para obtener una imagen digital de la huella. Una huella clasificada como *live-scan* indica que la imagen fue obtenida directamente de un lector de huellas dactilares, el cual, genera una imagen digital de la huella.



Figura 4.1: Lector de huellas dactilares Digital Persona U.are.U 4500.

Nota: El lector que se utilizó para adquirir las imágenes de las huellas dactilares en este trabajo de tesis, fue el lector de huellas de la compañía Digital Persona U.are.U 4500, es un lector de 8 bits que genera una imagen de dimensión de 355×390 pixeles, ver figura 4.1.

4.2.1. Minucias

Cuando la huella dactilar es capturada de un lector biométrico esta es representada como una imagen en donde se pueden observar regiones oscuras o claras, las regiones que forma una línea de color oscuro se llaman *crestas* y las regiones que forma una línea de color claro se llaman *valles* (ver figura 4.2 a). Observando las líneas oscuras se puede notar trayectorias particulares que forman pequeños detalles característicos, los cuales, se conocen como *minucias* (ver figura 4.2 b).

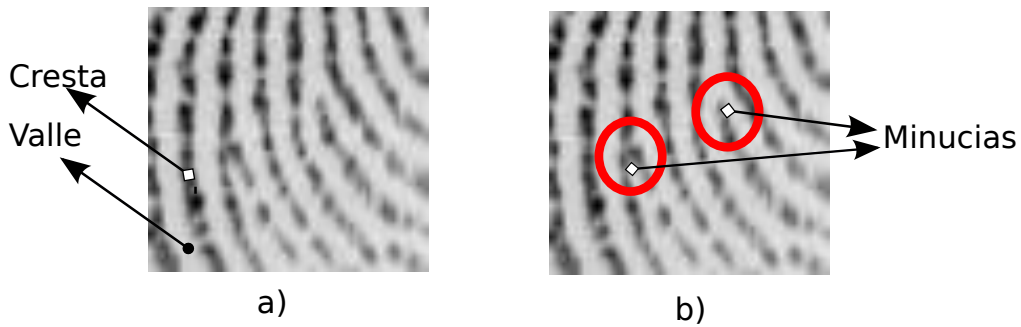


Figura 4.2: Ilustración de las características relevantes en una huella; a) valles y crestas, b) minucias.

En la imagen de la huella se pueden encontrar diferentes tipos de minucia, ver la figura 4.3. Pero no todas las minucias se consideran en un sistema biométrico automatizado, comúnmente un sistema biométrico solo extrae información de las minucias Terminación y Bifurcación.

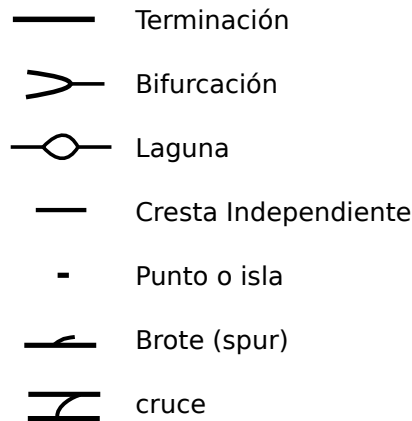


Figura 4.3: Tipo de minucias que existen en una huella dactilar.

Para poder identificar las minucias contenidas en una imagen de huella dactilar estas son representadas como: $m = \{x, y, \theta\}$, donde m representa la minucia, “ x ” y “ y ” la coordenada en la imagen y θ la dirección de la minucia considerando las líneas formadas por la cresta. Ver la figura 4.4.

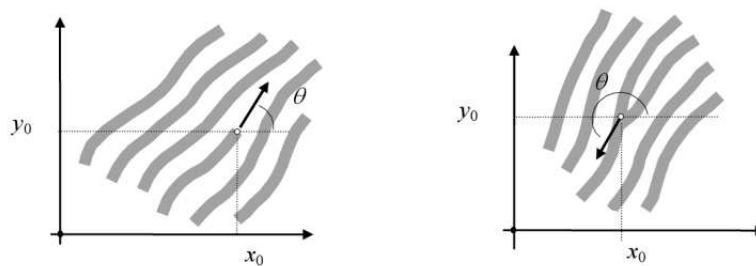


Figura 4.4: Representación de minucias. Esta imagen pertenece a la referencia [MMJP03].

4.2.2. Clasificación de huellas

Los sistemas biométricos para poder reconocer a una persona deben comparar una huella que se ingresa al sistema versus una huella que se encuentra almacenada en una base de datos, la cual, puede ser muy extensa lo que limita el tiempo de respuesta del sistema biométrico, debido a este motivo existen algunas medidas de clasificación para aumentar la velocidad en el proceso de reconocimiento, por ejemplo, las muestras de las huellas pueden ser almacenadas con alguna información del usuario (nombre, edad, país, sexo, etc.) que limite la búsqueda en la base de datos, sin embargo, en algunas ocasiones no es posible tener acceso a esta información por el tipo de aplicación del sistema biométrico como es el reconocimiento de criminales, reconocimiento forense, etc. En estos casos lo recomendable es utilizar las características intrínsecas de la muestra del identificador biométrico para realizar división de la base de datos en secciones que contenga una clase de huella dactilar.

Comúnmente la comparación de huellas se basa en las características locales como es las minucias, mientras que generalmente la clasificación de huellas se basa en las características globales, tales como la estructura global de las crestas o los puntos singulares bucles y deltas de la huella. En 1823, Johannes Evangelista Purkinje fue el primero en proponer una clasificación de huellas dactilares, quien clasifico las huellas en nueve categorías acorde a sus características globales de la huella, las cuales fueron: curva transversal, estría longitudinal central, raya oblicua, bucle oblicuo, espiral almendra, espiral espiral, elipse, círculo y doble espiral. Posteriormente, Francis Galton profundizo en los estudios de clasificación de huellas dactilares, él propuso tres clases principales (arco, bucle y espiral) que posteriormente dividió en sub-clases. Diez años después Edward Henry mejoro la clasificacion de Galton al aumentar el numero de clases, ha este esquema de clasificacion se le nombro Galton-Henry. En la figura 4.5 se muestran las cinco clases mas comunes del esquema de Galton-Henry; arco, arco tentado, bucle izquierdo, bucle derecho y espiral.

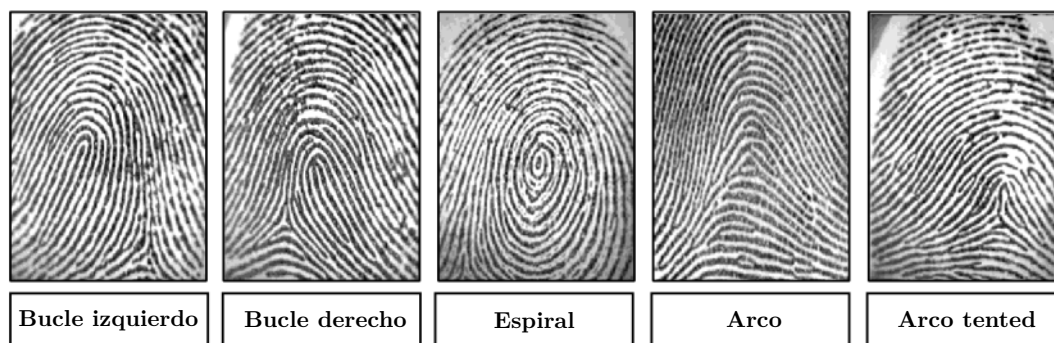


Figura 4.5: Clases más comunes del esquema de Galton-Henry; Bucle izquierdo, Bucle derecho, Espiral, Arco y Arco tentado. Esta imagen pertenece a la referencia [MMJP03].

4.3. Comparación de huellas

Los algoritmos que cotejan huellas dactilares comparan dos huellas y retornan un grado de similitud que comúnmente esta entre los valores de 0 y 1. Sin perdida de generalidad, de aquí en adelante se nombrará a las características de las huella obtenida en el registro como plantilla (T, por Template en ingles) y las características de la huella que se obtienen en la etapa de verificación/ identificación se nombrará entrada (I, por Input en ingles).

Los algoritmos de extracción de características son similares en ambos problemas identificación y verificación. Las comparación de huellas dactilares presentan algunos problemas comunes en las técnicas implementadas, debido a que esta asociado a la etapa de captura de la imagen, el problema más común es debido a la gran variabilidad de las impresiones de la huella dactilar. Los principales factores responsables de la variación son:

Desplazamiento: considerando que el área de captura es limitado, en algunas ocasiones el usuario pondrá su huella dactilar en diferentes posición sin percatarse de ello, lo que provocara imágenes con huellas dactilares desplazadas, en diferentes áreas.

Rotación: similar al desplazamiento, la imagen capturada de la huella también puede ser capturada con un desplazamiento rotacional lo que provocara que la imagen de la huella este rotada una cantidad de grados.

Solapamiento parcial: en algunas ocasiones los usuarios no ponen la huella completa en el área de captura, es decir, el lector de huellas captura una cantidad menor al adecuado, lo que provoca que las muestras a comparar tengan menor área de captura en común.

Distorsión no lineal: considerando que la huella tiene una forma tridimensional y que el lector tiene que transformar esta información en bidimensional. Durante el proceso de captura de información se presentan distorsiones difíciles de controlar debido a la elasticidad de la piel.

Condiciones de la piel: las características de la huella son captadas por el sensor cuando un dedo es presionado sobre la superficie del sensor, pero cuando una imagen es captada esta puede ser influenciada por la presión, suciedad de la piel, sudor, cicatrices, hongos en la piel, etc. Lo que provoca que una imagen captada cambie en cada una de las ocasiones que se presente al lector.

Ruido: el sensor de huellas al captar la imagen también puede captar otros aspectos como por ejemplo la grasa que se acumula en cada captura de huella, lo cual, puede introducir ruido. También se puede introducir ruido debido a fallas en el protocolo de comunicación, entre otros aspectos.

En la actualidad existen diversas implementaciones para el reconocimiento de individuos por medio de sus huellas dactilares, algunos son para cuestiones de índole legal como es el reconocimiento forense, la identificación de criminales, entre otros. También existen muchas otras aplicaciones de uso comercial para cualquier publico, por ejemplo: control de acceso

en una casa ó identificación y control de horario laboral de personal en empresas, entre otros. Debido a la amplia utilización de sistemas de reconocimiento automático de personas por medio de huellas dactilares existen y se investigan varios algoritmos de comparación de huellas dactilares. En el tema de comparación de huellas dactilares, existen tres técnicas principales, las cuales son:

Técnica de comparación basada en correlación: en esta técnica dos imágenes se superponen y se calcula la correlación de los píxeles considerando diferentes traslaciones y rotaciones de las dos imágenes para obtener la máxima similitud.

Técnica de comparación basada en patrones de las crestas: debido a que es difícil la extracción de minucias en imágenes de baja calidad existen técnicas de comparación que se enfocan en otros atributos característicos de las crestas que son más fáciles de apreciar, aun cuando la imagen sea de baja calidad, como por ejemplo: la orientación local de las crestas, la frecuencia de separación entre crestas, el patrón de continuidad de las crestas o la información de la textura de las crestas. Las técnicas de comparación de correlación o minucias pueden ser consideradas como una sub-categoría de comparación basada en patrones de las crestas, debido a que se enfocan en características específicas de los patrones encontradas en las huellas.

Técnica de comparación basada en minucias: este método de comparación es el más utilizado y estudiado. También, es la metodología que utilizan los expertos para realizar la comparación de dos huellas de forma manual. En esta técnica primeramente la imagen de la huella dactilar es representada en características específicas extraídas de acuerdo a los patrones que se presenta en la huella, las cuales, se conocen como minucias. Básicamente, la comparación consiste en alinear lo más óptimamente posible los dos conjunto de minucias generados por la huella de registro y la de ingreso, posteriormente se realiza la correspondencia entre el mayor número de pares de minucias.

4.4. Estructura de un sistema biométrico de huellas dactilares

La estructura de los sistemas biométricos que basan su decisión en la comparación de características de la huella dactilar, se encuentran compuestas fundamentalmente por dos etapas, las cuales, están constituidas principalmente por los cuatro módulos mencionados en la sección 2.5.

Etapas de enrolamiento: La etapa de enrolamiento o inscripción en un sistema biométrico, es la etapa en la que se registra al usuario en la base de datos para tener autorización a un servicio. Para el proceso de enrolamiento en un sistema biométrico, se requieren principalmente realizar cuatro pasos: el primero, es la adquisición de la muestra del identificador biométrico, en este paso se adquiere una imagen de la huella por medio de

un sensor, el segundo es el chequeo de calidad o preproceso de la muestra, en este paso, la imagen adquirida pasa por algunos procesos para checar la calidad de la imagen y realizar algunos procesos para mejorar la muestra, el tercero es la extracción de características del identificador biométrico, en este proceso se extraen los patrones (o plantillas) de la huella, el cuarto es el almacenamiento de la muestra en una base de datos. Esto se puede entender mejor observando la figura 4.6.

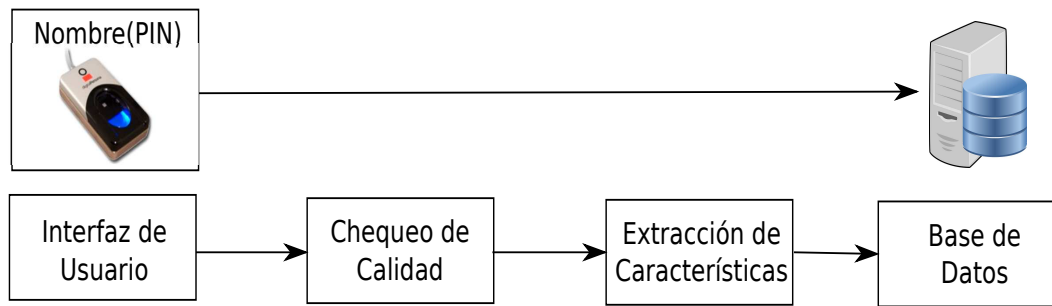


Figura 4.6: Diagrama a bloques de la etapa de inscripción en los sistemas biométricos.

Etapas de identificación o verificación: La etapa de verificación o identificación es la etapa en la que se realiza una comparación de la muestra de entrada al sistema biométrico versus la muestra almacenada en la base de datos, para determinar si la persona solicitante del servicio está inscrita en el sistema biométrico. Para el proceso de identificación o verificación en un sistema biométrico se requiere principalmente realizar cuatro pasos: el primero es la adquisición de la muestra del identificador biométrico, en este paso se adquiere una imagen de la huella por medio de un sensor, el segundo es la extracción de características del identificador biométrico en este proceso se extraen los patrones de la huella, el tercero es la comparación de la muestra de entrada versus la muestra almacenada en la base de datos, esta comparación tiene una pequeña diferencia dependiendo de su aplicación. Por ejemplo, si el sistema es para la verificación de usuarios, la comparación solamente se realiza con una huella en específico de la base de datos (ver figura 4.7), mientras que si el sistema es para la identificación de usuarios, la comparación se realiza con N huellas de la base de datos (ver figura 4.8). El cuarto paso es la toma de decisión del sistema, el cual, basa su respuesta dependiendo del resultado de la comparación.

Para mayor información el lector puede consultar por ejemplo las siguientes referencias [JRP04] y [Dav03a].

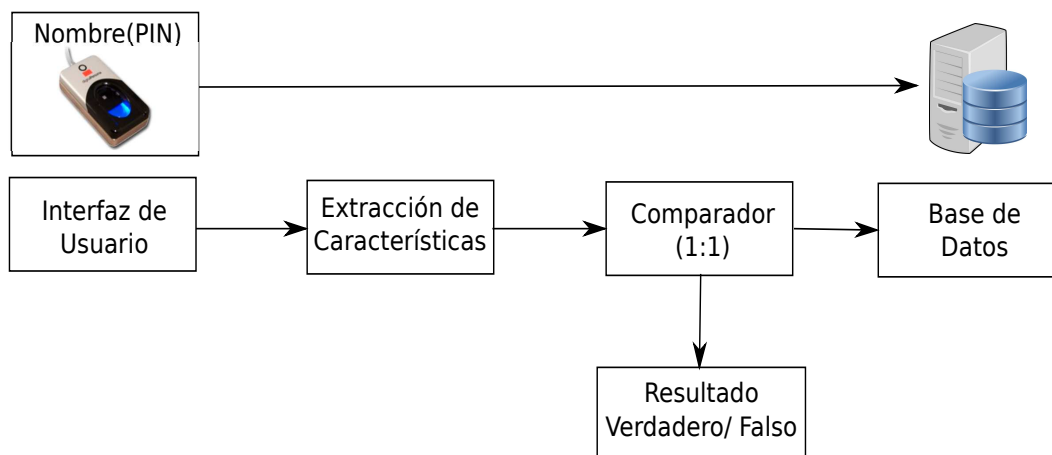


Figura 4.7: Diagrama a bloques de la etapa de verificación en los sistemas biométricos.

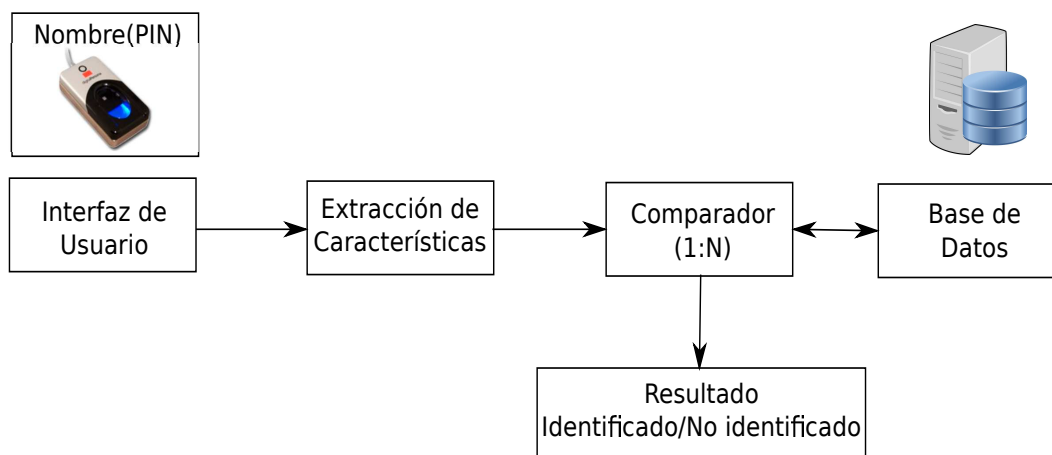


Figura 4.8: Diagrama a bloques de la etapa de identificación en los sistemas biométricos.

4.5. Puntos vulnerables

Físicamente los procesos que realizan las dos etapas de los sistemas biométricos se encuentran distribuidas en diferentes dispositivos. Además, por lo general, los procesos de la etapa de registro se encuentra en áreas controladas, las cuales, son protegidas físicamente esto hace que sean menos propensas a algún ataque. Sin embargo, la etapa de verificación o identificación según sea la aplicación del sistema biométrico, no cuenta con esta seguridad por lo que, deja vulnerable los procesos que se realizan en esta etapa, los cuales, son propensos a posibles ataques. En la figura 4.9 se muestran los puntos de posibles ataques que pueden sufrir los sistemas biométricos basados en huellas dactilares y mayormente enfocados en la etapa de verificación/identificación.

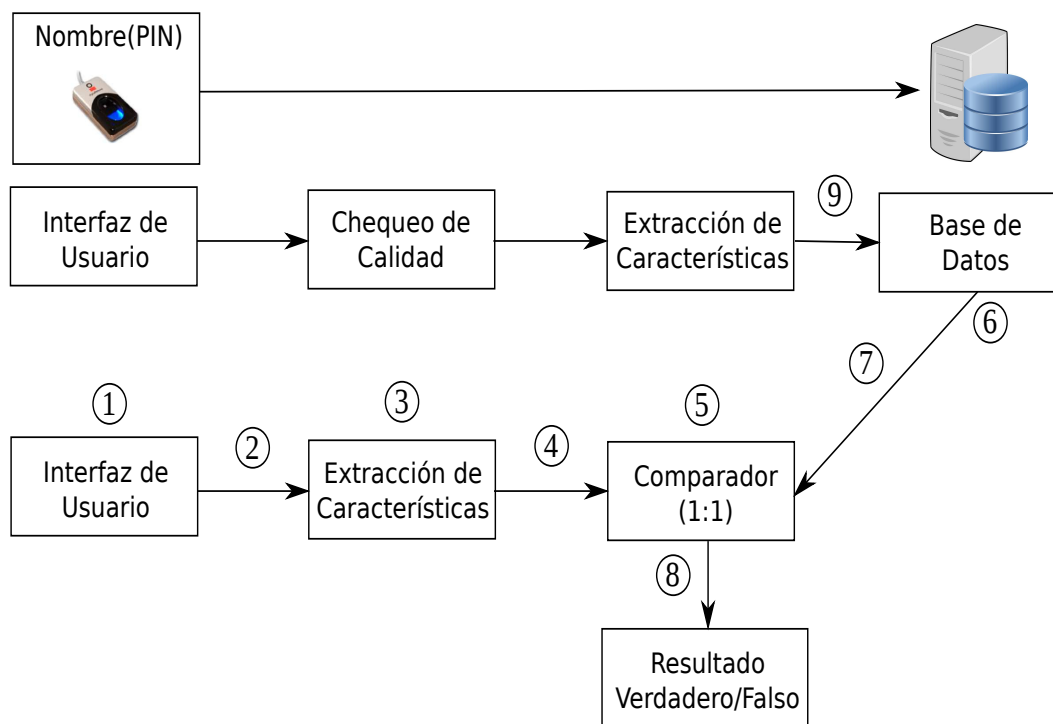


Figura 4.9: Puntos vulnerables de ataques en los sistemas biométricos de huellas dactilares.

Como se observa en la figura 4.9, se muestran numerados los puntos vulnerables de ataques que podrían sufrir los sistemas biométricos, a continuación se mencionarán de manera breve en que consiste cada uno de estos ataques.

① Ataque al elemento de censado (escáner)

Este tipo de ataque puede referirse a un ataque físico en contra del escáner de la huella dactilar. A continuación se mencionarán tres ejemplos de este tipo de ataque: Primer ejemplo, el escáner o su superficie pueden ser físicamente destruidas, esto con la intención de que ningún usuario pueda utilizar el sistema biométrico. Segundo ejemplo, al escáner se le puede presentar una falsa huella, esto se refiere a copias o impresiones sobre papel de la imagen de la huella, polímeros con la forma de la huella en tercera dimensión, moldes de polímeros gelatinosos, entre otros. Tercer ejemplo, una imagen digitalizada puede ser introducida entre el escáner y el circuito al que se encuentra conectado el escáner (convertidor A/D, microprocesador, etc.).

② Ataque al canal de comunicación entre los módulos del escáner y la extracción de características

En este tipo de ataque por lo general, se interrumpe la línea de comunicación para obtener una imagen de la huella dactilar, la cual, puede utilizarse en un tiempo posterior para pasar por alto el proceso de la adquisición de la huella por medio del escáner.

③ Ataque al modulo de extracción de características

Este tipo de ataque se realizan por un programa malicioso (troyano), el cual, simula

realizar el proceso de extracción para pasar por alto el verdadero proceso de extracción, para así, poder introducir características artificiales de la huella, las cuales, son generadas por el programa malicioso y siendo estas características las que se envían al modulo de comparación.

④ **Ataque al canal de comunicación entre los módulos de extracción de características y comparación**

En este tipo de ataque se interceptan el canal de comunicación para adquirir las características extraídas de las huellas de un usuario registrado en la base de datos. El motivo de este ataque es utilizar estas características en un tiempo futuro para pasar por alto los módulos del escáner y el de extracción de características.

⑤ **Ataque al modulo de comparación**

Este tipo de ataque se realiza por un programa malicioso (troyano), el cual, simula realizar el proceso de comparación para pasar por alto el verdadero proceso de comparación, para así, poder introducir el resultado de un punto de comparación generado artificialmente, esto podría contribuir a que un usuario registrado tenga un caso de falso rechazo o que una persona no registrada tenga un caso de falsa aceptación.

⑥ **Ataque a la base de datos**

Este tipo de ataque se realiza por un programa malicioso (troyano), el cual, simula el registro de datos en la de base de datos, para así, poder suministrar datos falsamente almacenados, los cuales, son generados artificialmente por el programa malicioso, estos datos pueden ser una plantilla registrada, el nombre del usuario, privilegios de acceso, entre otros. Este tipo de ataques puede ser realizado durante el tiempo que se efectúa la etapa de inscripción, durante el tiempo que se efectúa la etapa de verificación/identificación o podría efectuarse en la base de datos en cualquier momento.

⑦ **Ataque al canal de comunicación entre la base de datos y el modulo de comparación**

El canal de comunicación entre la base de datos y el modulo de comparación puede ser fisgoneado para robar la información grabada en la base de datos, la cual, se envía a través de este canal, esto con el motivo de utilizarla en un tiempo futuro.

⑧ **Ataque al canal de comunicación del modulo de comparación y la aplicación que requiere la verificación/identificación**

El canal de comunicación entre el modulo de comparación y la aplicación que requiere la verificación/identificación puede ser fisgoneada con el propósito de tener acceso a la respuesta resultante del modulo de comparación, esto con motivo de utilizar esta información obtenida en un tiempo futuro.

⑨ **Ataque al canal de comunicación del modulo de extracción de características de la etapa de enrolamiento y la base de datos**

Este canal de comunicación es propenso a ser interceptado para fisgonear, con el propósito de tener acceso a las características extraídas en el modulo anterior, con motivo de almacenarlas y poder hacer uso de estas características en un tiempo futuro.

Se puede notar que los ataques ②, ④, ⑦, ⑧ y ⑨, se podrían clasificar en el mismo tipo de ataque, debido a que estos ataques se realizan a los canales de comunicación de los sistemas biométricos, a los que nos podemos referir como ***ataques de reproducción***. También se puede notar que los ataques ①, ③, ⑤ y ⑥, son ataques que se realizan en alguno de los módulos del sistema biométrico, los cuales, comúnmente se realizan con **programas troyanos**.

Debido a la existencia de estos ataques a puntos vulnerables de los sistemas biométricos, se pueden implementar algunas acciones de protección para mitigar el riesgo de sufrir daños generados por ellos, entre estas acciones se utilizan las siguientes: datos aleatorios, retención de datos, detección en vivo, biometría múltiple, autenticación multifactor, criptografía, firmas digitales, limpieza de la red y seguridad física. Para mayor información consultar las referencias [Dav03a], [JA07], [Mar], [Orm10], [Ani08b] y [Ani08a].

4.6. Conclusiones

En la actualidad es muy común encontrar diversas aplicaciones donde se implementan los sistemas biométricos de huella dactilar, los cuales, son considerados muy seguros, sin embargo como se puede observar en este capítulo los sistemas biométricos no son 100 % seguros ó perfectos, por ese motivo existen varias investigaciones que están siendo realizadas por investigadores para mejorar algún aspecto del sistema biométrico, por ejemplo: mejorar la calidad de la imagen, mejorar o agilizar el proceso de extracción de características, mejorar o agilizar el proceso de comparación, mejorar el almacenamiento, entre otros. En este trabajo de tesis nosotros pretendemos aportar en el mejoramiento de la seguridad de los sistemas biométricos.

Capítulo 5

Alternativa de encriptado de imagen con mapeo de Rössler

5.1. Introducción

Desde hace siglos la integridad y seguridad, de la información transmitida entre dos individuos que desean intercambiar información de forma confidencial, ha tenido una gran importancia, por tal motivo, durante el transcurso de la historia se desarrollaron varias técnicas de cifrado para ocultar la información transmitida. Históricamente la mayoría de las técnicas de encriptado se desarrollaron por cuestiones bélicas, algunos ejemplos se reportan en las referencias

En la actualidad es común utilizar sistemas que controlen el acceso a un medio físico o virtual, como son los sistemas operativos de las computadoras, las cuentas de correos electrónicos, base de datos, edificios gubernamentales, cruce de fronteras, entre otros. Para controlar el acceso muchos de estos sistemas utilizan tarjetas magnéticas, llaves físicas, claves, identificadores biométricos, etc. Hoy en día los sistemas biométricos son uno de los sistemas más utilizados para controlar el acceso y varios de estos sistemas cifran la información del identificador biométrico para brindarle seguridad, por tal motivo, varios investigadores han realizado estudios para implementar algoritmos criptográficos en los sistemas biométricos, por ejemplo, ver la referencias [MCP⁺06] y [VTM08]. En varios trabajos de investigación, el cifrado que se propone es sobre los patrones extraídos de la imagen del identificador biométrico y en otros, el cifrado es sobre la imagen del identificador biométrico.

Relacionado al tópico de cifrado de imágenes, existen varios trabajos que reportan nuevas alternativas de cifrado, donde algunas proponen utilizar las propiedades intrínsecas de las secuencias de ADN, mientras que otros proponen beneficiarse de las propiedades pseudo-aleatorias que ofrecen los sistemas caóticos, algunos de estas investigaciones se presentan en las referencias [LWkkkkkkkk12], [Ye10] y [ZGW10]. En el presente trabajo se presenta una alternativa de cifrado de la imagen de una huella dactilar, utilizando un sistema caótico para ocultar la información de la imagen.

5.2. Metodología de encriptado y desencriptado

Si se revisa la literatura de comunicaciones seguras se encontrará un gran número de metodologías para realizar el cifrado de información, por tal motivo, se considera de gran importancia describir cual es la metodología seguida en el presente trabajo. El proceso de encriptado esta constituido por dos etapas importantes, la etapa de difuminación y la etapa de permutación, por otra parte, el proceso de descencriptado esta constituido por las inversas de las etapas anteriores, es decir, la etapa de permutación inversa y la etapa de difuminación inversa, esto se puede entender mejor observando la figura 5.1.

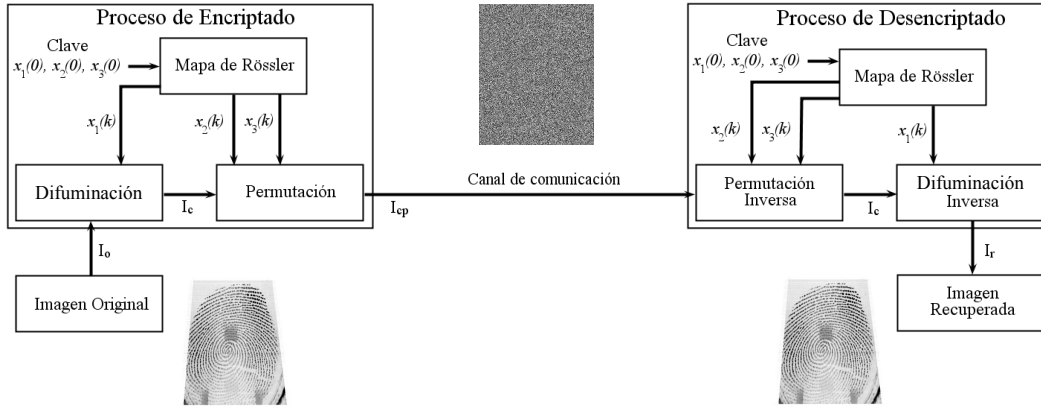


Figura 5.1: Diagrama a bloques de los procesos de encriptado y desencriptado de una imagen.

5.2.1. Proceso de encriptado

Para la realización de la etapa de encriptado se requieren las etapas de difuminación y permutación, las cuales, utilizan el mismo mapa hipercaótico de Rössler en sus procesos. El mapa hipercaótico se utiliza para generar una secuencia de número pseudoaleatorios, los cuales, se utilizan en las etapas antes mencionadas. Para explicar de mejor manera en que consisten cada una de estas etapas, se mencionarán por separado los pasos que se requieren seguir para realizar la difuminación y la permutación.

Etapa de difuminación

Paso 1: Tomar lectura de la imagen de la huella dactilar para generar una variable que el programa pueda manipular para realizar el cifrado, la cual, en este documento será representada por la variable $I_o(i, j)$, donde $i = 1, 2, \dots, n$ y $j = 1, 2, \dots, m$, por tanto, ésta representa una matriz de $n \times m$, donde n es el número de renglones y m es el número de columnas.

Paso 2: Construir un matriz de tamaño $n \times m$, que contenga los datos resultantes del estado hipercaótico $x_1(k)$ del mapeo de Rössler ver (3.1), donde $k = 1, \dots, N$, y $N = n \times m$,

esta matriz será nombrada como matriz de estado caótico y será representada por la variable $M_c(i, j)$.

Paso 3 Utilizando la matriz de estado caótico obtenida anteriormente, se generará una nueva matriz que sólo contengan valores dentro del conjunto $\{a \in \mathbb{N} : 0 \leq a < 256\}$. Esta matriz se utilizarán para difuminar la imagen. Para lograr esto primero se debe de tener en cuenta que $M_c(i, j) \in \mathbb{R}$, así como también que el valor de sus elementos se encuentra entre el rango de 0 a 1, por tanto, se tiene que realizar un mapeo del conjunto de los números reales ($\mathbb{R}$) obtenidos del mapeo hipercaótico de Rössler a un conjunto de números enteros ($\mathbb{Z}$) positivos correspondientes al conjunto $\{a \in \mathbb{N} : 0 \leq a < 256\}$, para lo cual, se utilizan las siguientes expresiones:

$$M_{cc} = (\{M_c(i, j) : (|M_c(i, j)| \times 100000) \in \mathbb{N}\} \bmod 256).$$

Paso 4: Sumar los elementos de la matriz $M_{cc}(i, j)$ con los elementos de la matriz imagen $I_o(i, j)$ aplicando el modulo 256, esto para garantizar solamente valores dentro del conjunto $\{a \in \mathbb{N} : 0 \leq a < 256\}$. Con este proceso se obtendrá una nueva matriz que será nombrada como matriz de imagen difuminada y será representada por $I_c(i, j)$.

Etapas de permutación

Paso 1: Leer imagen para realizarle el proceso de permutación de posiciones de píxeles. Esta variable es representada por $I_{in}(i, j)$, pero esta imagen es la obtenida en el proceso anterior, por tanto, $I_{in}(i, j) = I_c(i, j)$.

Paso 2: Generar un vector para las posiciones de los renglones y un vector para las posiciones de las columnas, los cuales, serán representados por las variables $Vren = [1 \ 2 \ 3 \ 4 \ \dots \ n]$ y $Vcol = [1 \ 2 \ 3 \ 4 \ \dots \ m]$

Paso 3: Generar dos vectores que contenga los datos resultantes de los estados caóticos x_2 y x_3 del mapeo de Rössler ver (3.1), éstos serán nombrados como vector caótico de renglones y vector caótico de columnas, los cuales, serán representados por las variables $X_c(k_1) = [x_2(0) \ x_2(1) \ \dots \ x_2(N)]$ y $X_r(k_1) = [x_3(0) \ x_3(1) \ \dots \ x_3(N)]$. Donde $k_1 = 1, 2, 3, \dots, N$ y $N > (21m)$

Paso 4: Generar dos vectores con secuencias pseudoaleatorias de las posiciones de los renglones y columnas de la imagen. Considerando que $X_r, X_c \in R$, así como también que el valor de sus elementos son menores a los valores de los elementos de los vectores $Vren$ y $Vcol$, se realiza un mapeo del conjunto de los números reales ($\mathbb{R}$) obtenidos del mapeo hipercaótico de Rössler a un conjunto de números enteros ($\mathbb{Z}$) positivos correspondientes a las posiciones de los renglones y columnas, para lo cual, se utilizan las siguientes expresiones:

$$Sren = (\{X_r : (|X_r| \times 100000) \in N\} \bmod n) + 1,$$

$$Scol = (\{X_c : (|X_c| \times 100000) \in N\} \bmod m) + 1.$$

Posteriormente utilizando los vectores $Vren$, $Vcol$, $Sren$ y $Scol$ se generarán dos vectores que contengan secuencias pseudoaleatorias de las posiciones de las columnas y renglones, para lo cual, se utilizará el siguiente algoritmo:

Algorithm 1 Genera secuencia aleatoria de posiciones.

Require: Solicitar variables $N = 21m$, $Scao(k_1) = Sren(k_1)$, $Vp(l) = Vren(i)$ y $N_2 = n$ para generar secuencia pseudoaleatoria de las posiciones de los renglones o $Scao(k_1) = Scol(k_1)$, $Vp(l) = Vcol(j)$ y $N_2 = m$ para generar secuencia pseudoaleatoria de las posiciones de las columnas.

Ensure: $Vsap$ Vector de secuencia aleatoria de posiciones.

```

1:  $p = 1$ ;  $a = 1$ ;  $b = N/21$ ;
2: while  $a \neq 0$  do
3:   if  $Scao(b)$  es igual a  $Vp(Scao(b))$  then
4:      $Vsap(p) = Scao(b)$ 
5:      $Vp(Scao(b)) = 0$ ;  $p = p + 1$ 
6:   end if
7:    $b = b + 1$ 
8:   if la suma de todos los elementos de  $Vp$  es igual a 0 then
9:      $a = 0$ 
10:  end if
11:  if  $b$  es igual a  $N$  then
12:     $b = 1$ 
13:     $Scao = ((Scao + 1) \bmod N_2) + 1$ 
14:  end if
15: end while
16: return  $Vsap$ 

```

Paso 5: Utilizando los vectores de las secuencias aleatorias de las posiciones de las columnas y renglones, los cuales estarán representados por las variables $Vsap_c$ y $Vsap_r$ respectivamente, se permutaran las posiciones de los pixeles de la imagen de la siguiente manera

$$I_{cp}(i, j) = I_{in}(Vsap_r(i), Vsap_c(j)).$$

5.2.2. Proceso de descriptado

Para la realización del proceso de descriptado se requieren de la etapa de permutación inversa y la etapa de difuminación inversa, las cuales, utilizan el mismo mapa hipercaótico que se utilizó en el proceso de encriptado, utilizando las mismas condiciones iniciales. A continuación se mencionará en que consiste cada una de las etapas mencionadas.

Etapa de permutación inversa

Los pasos que se deben seguir para realizar la permutación inversa son similares a los realizados en la etapa de permutación, pero en ésta ocasión $I_{in}(i, j) = I_{cp}(i, j)$ y la principal

diferencia del proceso radica en el paso 5. Para realizar la permutación inversa igualmente se utilizan los vectores de las secuencias pseudoaleatorias de las posiciones de las columnas ($Vsap_c$) y renglones ($Vsap_r$), pero para realizar la permutacion se utiliza la siguiente expresión

$$I_c(i, j) = I_{in}(Vsap_r(i), Vsap_c(j)).$$

Etapas de difuminación inversa

Los pasos que se deben de seguir para realizar el proceso de difusión inversa son similares a los presentados en la etapa de difuminación, la diferencia radica en el paso 4 de dicho proceso. Para realizar la difuminación inversa igualmente se utilizan las matrices $M_{cc}(i, j)$ y $I_c(i, j)$, pero en ésta ocasión la operacion que se realiza es la siguiente:

$$I_r(i, j) = (I_c(i, j) - M_{cc}(i, j)) \bmod 256$$

, igualmente el $\bmod 256$ es para garantizar que los valores resultantes de esta operación estén dentro del conjunto $\{a \in \mathbb{N} : 0 \leq a < 256\}$. Con éste proceso se obtendrá una nueva matriz que contendrá los datos recuperados de la imagen ocultada previamente en la etapa de encriptado, es decir, la matriz obtenida corresponde a la imagen recupera y será denotada por la variable I_r .

5.3. Resultados experimentales

En esta sección se presentan los resultados obtenidos de programas realizados en MatLab versión 2008a, los cuales realizan los procedimientos mencionados en la sección 5.2. Los resultados se presentan en dos subsecciones, en la primera subsección se presentan los resultados obtenidos si se aplican las etapas de encriptado, desencriptado, permutación, difusión, permutación inversa y difusión inversa. En la segunda subsección se presentan los resultado obtenidos del análisis de seguridad del encriptado.

5.3.1. Etapas del proceso de encriptado y desencriptado

Para observar de mejor manera que es lo que realizan las etapas de permutación y difusión, así como las etapas de sus inversas, en la figura 5.2 se presentan los resultados que se obtendrían si se ingresa una imagen a estas etapas, en esta ocasión se ingresa la misma imagen en ambas etapas, es decir se aíslan las etapas y se ingresa la imagen de la huella dactilar, esto proporciona una idea más clara de lo que realizan estas etapas.

En la figura 5.3 se presenta el resultado del proceso de encriptado y desencriptado, sin omitir ninguna de las etapas que se realizan en cada uno de los procesos. ¿ Pero qué pasaría si se omite alguno de las etapas? si se omite alguna de las dos etapas que se realizan en el proceso de encriptado o desencriptado no se podría recuperar la imagen, para demostrar este hecho se presenta en la figura 5.4 los resultados si se omite la etapa de permutación o permutación inversa en el proceso de encriptado o desencriptado según sea el caso.

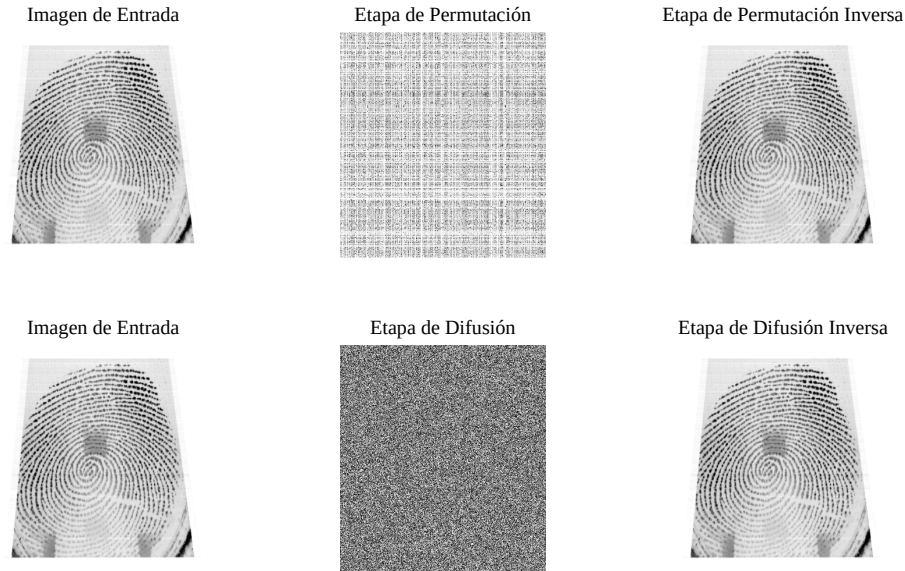


Figura 5.2: Imagen que muestra los resultados obtenidos de las etapas de permutación, difusión, permutación inversa y difusión inversa, cuando se introduce una imagen a las etapas y se utiliza la llave correcta para que se realicen los procesos inversos correctamente.

5.3.2. Análisis de seguridad

Para evaluar la eficiencia del criptograma generado por un algoritmo criptográfico, este debe de ser analizado considerando los diferentes tipos de ataques que se le pueden realizar a los criptogramas, algunos de estos ataques son: el ataque exhaustivo, el ataque estadístico, el ataque diferencial, entre otros. A continuación se presentan los resultados obtenidos del análisis de algunos ataques. También se debe hacer notar que si se observa la figura 5.2 se puede pensar que la la imagen podría ser considerada encriptada utilizando solamente la etapa de difusión, es decir se podría considerar un esquema de cifrado que omita la etapa de permutación y permutación inversa, por tal motivo los resultados que se presentan son considerando dos casos, el primero es cuando en el proceso de encriptado solo se utiliza la etapa de difusión y el segundo cuando en el proceso de encriptado se utiliza la etapa de difusión y permutación.

Resistencia ante ataques estadísticos

El primer análisis que se presenta es ante ataques estadísticos, los cuales, consisten en realizar análisis estadísticos de las propiedades de la imagen como son la distribución de los niveles de intensidad de la imagen y la correlación que existe entre los pixeles de la imagen. El histograma de la imagen es un buen medio para observar la distribución de los niveles de intensidad, una imagen a color tiene 3 histogramas uno para cada uno de los colores primarios, y las imágenes en escala de grises tienen solamente un histograma, el cual, corresponde

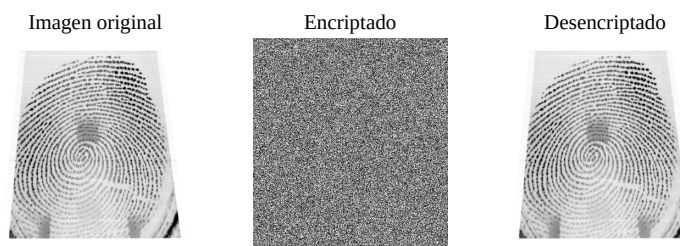


Figura 5.3: Imagen que muestra los resultados obtenidos si no se omite ninguna etapa del proceso de encriptado y desencriptado.

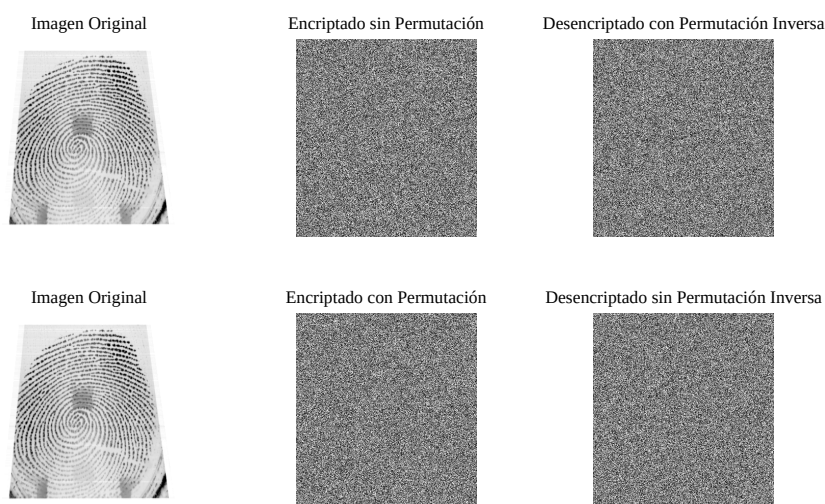


Figura 5.4: Imagen que muestra los resultados obtenidos si se omite la etapa de permutación o permutación inversa.

a los niveles en escala de grises.

Análisis del histograma de la imagen

Los algoritmos criptográficos deben proporcionar una distribución uniforme de los valores de grises en el histograma para poder brindar una fortaleza adecuada ante un ataque de análisis estadístico. En la figura 5.5 se ilustran los histogramas de la imagen antes y después del cifrado, considerando que el encriptado se realiza con o sin la etapa de encriptado, en la figura 5.5 se puede observar que la distribución de los valores de grises para la imagen original se encuentran concentrados en algunos valores de gris, mientras que en los histogramas de las imágenes cifradas se puede observar que la distribución de los valores de gris es casi uniforme.

También en la figura 5.5 se puede observar que los histogramas de las imágenes cifradas son los mismo esto se debe a que el proceso de permutación solo modifica las posiciones de los pixeles contenidos en la imagen y no modifica los valores de los pixeles, por tanto no modifica la distribución de los niveles de intensidad de la imagen cifrada.

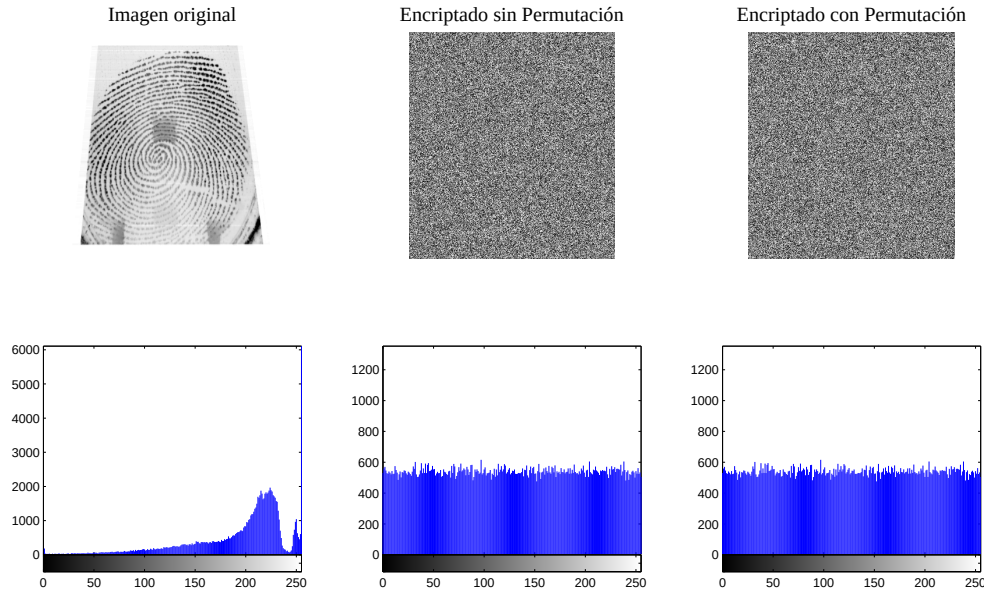


Figura 5.5: Imagen que presenta los resultados del encriptado con y sin la etapa de permutación, utilizando la llave (0.1, 0.1, 0.1).

Análisis de la correlación entre los pixeles de la imagen.

Comúnmente existe una alta correlación entre los pixeles adyacente de una imagen, por tal motivo, los algoritmos criptográficos deben de reducir esta correlación entre pixeles adyacentes, para poder brindar una fortaleza adecuada ante los ataque estadísticos. En la figura 5.6, se muestran los resultados gráficos de la correlación horizontal, vertical y diagonal de los pixeles adyacentes de las imágenes original, encriptada con y sin permutación, esto para observar la diferencia entre ellos.

Posteriormente en la tabla 5.1 se presentan los resultados numéricos de las correlaciones obtenidas de la imagen original, encriptada sin y con permutación, estos resultados fueron obtenidos utilizando las siguientes formulas:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad E(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (5.1)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \quad D(y) = \frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2 \quad (5.2)$$

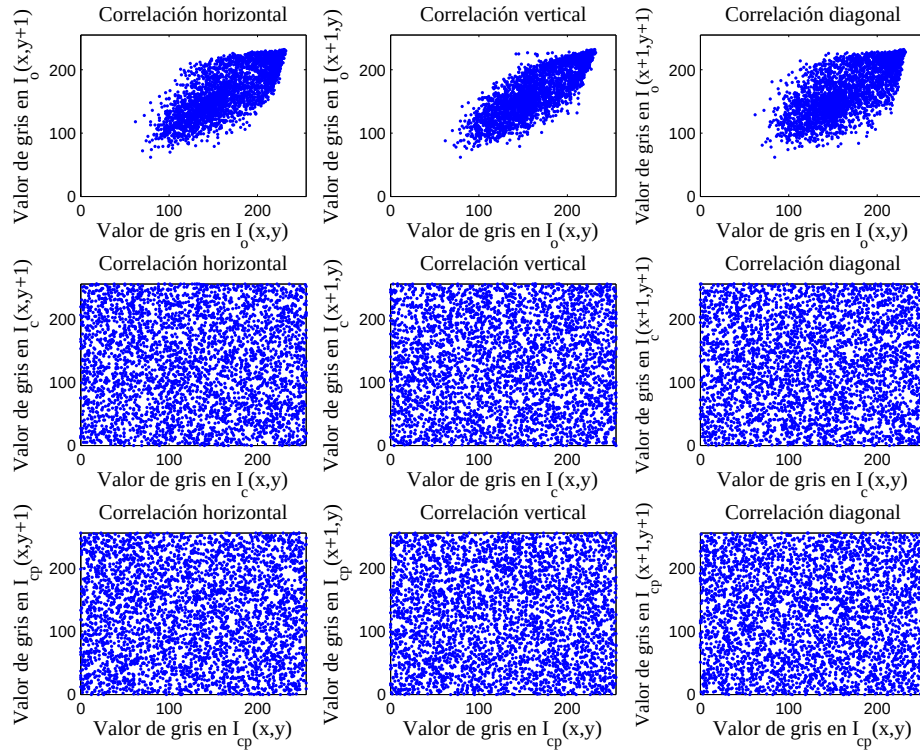


Figura 5.6: Gráficas de las correlaciones horizontal, vertical y diagonal de la imagen original (I_o), imagen cifrada sin permutación (I_c) e imagen cifrada con permutación (I_{cp}), utilizando la llave (0.1, 0.1, 0.1)

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (5.3)$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad (5.4)$$

Donde x e y son los valores de gris de dos píxeles que se encuentran adyacente en la imagen, $cov(x, y)$ es la covarianza, D es la varianza y E es la media.

Imagen	Correlación horizontal	Correlación vertical	Correlación diagonal
Original	0.8180	0.8670	0.8184
Encriptado sin permutacion	-0.0218	0.0169	-0.0219
Encriptado con permutacion	-0.0125	0.0033	-0.0125

Tabla 5.1: Coeficientes de correlación entre dos píxeles de la imagen

Observando los resultados presentados en la figura 5.6 se puede notar que para las gráficas de correlación correspondientes a la imagen original de la huella existe una concentración

de puntos, lo cual, indica que existe una correlación entre los píxeles de la imagen, sin embargo para las gráficas de correlación correspondientes a las imágenes encriptadas con y sin permutación, se puede notar que no se presenta una concentración de puntos en la gráfica, si no por el contrario existe una gran distribución de los puntos sobre todo el área de la gráfica, lo cual, indica una correlación muy baja entre los píxeles de las imágenes cifradas. Para los resultados numéricos presentados en la tabla 5.1 se debe considerar que para valores cercanos a ± 1 indica una alta correlación y para valores cercanos a 0 indica una baja correlación. En la tabla 5.1 se puede observar que para la imagen original los resultados numéricos de la correlación son aproximadamente 0.8 siendo este valor cercano a 1, por tanto, este valor es un indicador de una alta correlación entre los píxeles de la imagen, por otra parte para la imagen encriptada sin permutación los resultados numéricos son cercanos a cero, lo cual, indica una baja correlación, por ultimo los resultados numéricos de la imagen encriptada con permutación son valores cercanos a cero, por tanto su correlación es baja. Por lo tanto, observando los resultados numéricos y gráficos se puede concluir que la imagen cifrada cumple satisfactoriamente con el propósito de reducir la correlación entre los píxeles de la imagen, siendo esta una característica que debe cumplir un criptograma resistente ante ataques estadísticos.

Resistencia ante ataques exhaustivos

El segundo análisis que se presenta es ante ataques exhaustivos o también conocido como ataque de fuerza bruta, el cual consiste en probar todas las posibles llaves hasta encontrar una llave con la cual se pueda recuperar el mensaje original, por tanto este tipo de ataque está relacionado con la llave, por tal motivo para comprobar la eficiencia de la llave en el esquema criptográfico se realizaran el análisis del espacio de llaves y el análisis de sensibilidad de la llave.

Análisis del espacio de llave

Para considerar que el espacio de una llave es adecuada para resistir un ataque de fuerza bruta este espacio debe ser superior a $2^{100} = 1,2677 \times 10^{30}$. En el esquema de encriptado presentado en este documento. La llave que se utiliza en el esquema de encriptado esta constituida por las condiciones iniciales del sistema hipercaótico de Rössler, independientemente si se considera la etapa de permutación o no. Por tanto, si se considera una precisión de 10^{-12} , el esquema de encriptado proporcionara un espacio de llave de $10^{12} \times 10^{12} \times 10^{12} = 10^{36}$, por tanto, se puede concluir que el espacio de llave es adecuado para soportar un ataque exhaustivo.

Análisis de la sensibilidad de la llave.

El esquema criptográfico deberá ser muy sensible ante pequeñas variaciones de la llave para brindar una adecuada resistencia ante un ataque exhaustivo. Los sistemas caóticos tienen la característica de ser sensibles a las condiciones iniciales, es decir, los sistemas caóticos

tienen comportamientos dinámicos distintos cuando las condiciones iniciales tienen una pequeña variación, por tal motivo esta propiedad del sistema caótico brinda una muy buena sensibilidad a la llave. Esta propiedad puede demostrarse fácilmente, por ejemplo, considérese las imágenes de la huella dactilar ilustrada en la figura 5.3, en la cual, las imágenes fueron cifradas con la llave (0,1, 0,1, 0,1) y para recuperar la imagen original se requirió de la misma llave, ahora considérese que en la etapa de encriptado se varía ligeramente la llave de encriptado, es decir para este caso el descryptado se realiza con la llave (0,1, 0,1, 0,100000000001). En la figura 5.7 se puede observar que la imagen encriptada y la imagen descryptada son totalmente distintas, esto se debe a que se utilizaron dos llaves distintas en el proceso de encriptado y descryptado, aun cuando sean muy similares no se puede recuperar la imagen encriptada.

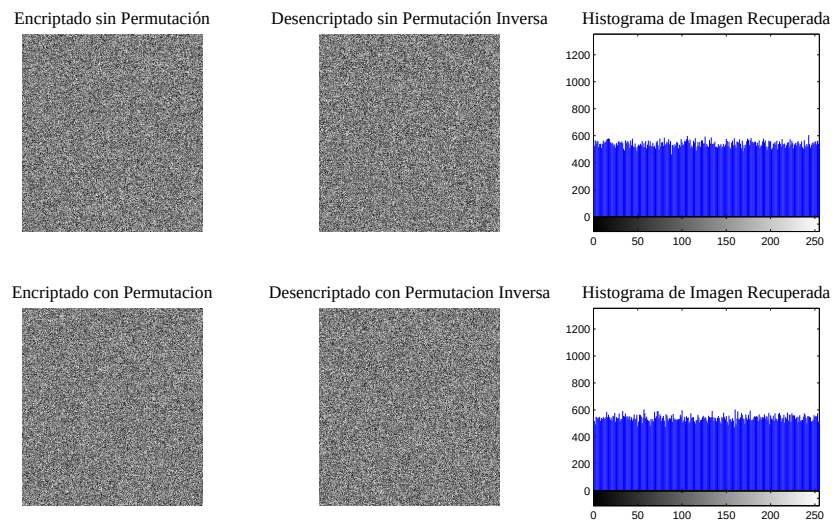


Figura 5.7: Imagen que demuestra la sensibilidad de la llave en el algoritmo criptográfico el cual puede considerar la etapa de permutación u omitirla. La llave que se utiliza para el encriptado es (0,1, 0,1, 0,1) y la llave que se utiliza para el descryptado es (0,100000000001, 0,1, 0,1)

Resistencia ante el ataque diferencial

El tercer análisis que se presenta es ante el ataque diferencial, el cual, consiste en realizar un pequeño cambio en el valor de los pixeles de la imagen original, para posteriormente aplicarles el algoritmo criptográfico a la imagen original antes y después del cambio, una vez teniendo los criptogramas se realiza una comparación por medio de los dos criptogramas para buscar similitudes entre la imagen original y la imagen encriptada. Existen dos parámetros que utilizan los investigadores para examinar la resistencia del encriptado ante el ataque diferencial, los cuales son el NPCR (Number of Pixels Change Rate) y el UACI (Unified Average Changing Intensity), para calcular los valores de estos parámetros se utilizaron las siguientes formulas:

$$C(i, j) = \begin{cases} 0 & \text{if } T_1(i, j) = T_2(i, j) \\ 1 & \text{if } T_1(i, j) \neq T_2(i, j) \end{cases} \quad (5.5)$$

$$NPCR = \frac{\sum_i^M \sum_j^N C(i, j)}{M \times N} \times 100 \% \quad (5.6)$$

$$UACI = \frac{\sum_i^M \sum_j^N |T_1(i, j) - T_2(i, j)|}{255 \times M \times N} \times 100 \% \quad (5.7)$$

donde M y N es lo alto y lo ancho de la imagen, $T_1(i, j)$ y $T_2(i, j)$ son los valores de grises del pixel en la localización (i, j) de las imágenes a comparar, T_1 para la imagen 1 y T_2 para la imagen 2. Para realizar el análisis se consideró como imagen original la huella dactilar mostrada en la figura 5.4, posteriormente se cambiaron los valores de los pixeles de la imagen en una unidad, es decir si un valor 127 del pixel de la imagen original es cambiado por el valor 128. Posteriormente se aplicó el encriptado a la imagen antes y después de cambiar los valores de sus pixeles, por tanto se obtuvieron dos criptogramas. Ahora considerando las variables presentadas en las ecuaciones anteriores, los valores de gris para el criptograma obtenido de la imagen original antes de realizar un cambio son representados por $T_1(i, j)$ y los valores de gris para el criptograma obtenido después de realizar el cambio son representados por $T_2(i, j)$. Para el caso cuando el proceso de encriptado omite la etapa de permutación los resultados que se obtienen son $NPCR_c = 100 \%$ y $UACI_c = 1.2489 \%$, ahora si el proceso de encriptado no omite ninguna etapa los resultados son $NPCR_{cp} = 100 \%$ y $UACI_{cp} = 1.2489 \%$. Esto indica que el esquema criptográfico es resistente ante un ataque diferencial.

5.4. Conclusiones

- Observando los resultados presentados en el análisis de seguridad, se puede considerar que el encriptado realizado con el mapeo de Rössler es satisfactorio. Otro aspecto que se debe mencionar es que observando los resultado obtenidos se puede considerar que el proceso de encriptado es satisfactorio aun cuando se omite la etapa de permutación, sin embargo, siempre es recomendable incluir esta etapa, esto es debido a que aun cuando los resultados de los análisis son muy similares, incluir la etapa de permutación disminuye la correlación de los pixeles contenidos en la imagen, lo cual beneficia en la resistencia del esquema de encriptado ante ataques estadísticos.
- El espacio de llaves puede ser ampliado si se consideran dos sistemas de Rössler uno para la etapa de difusión y otro para la etapa de permutación, debido a que la llave esta constituida por las condiciones iniciales las cuales tendría una precisión de 10^{-12} , esto proporcionaría un espacio de llaves de 10^{72} .

Capítulo 6

Solución propuesta

6.1. Introducción

En la presente tesis se pretende contribuir en la seguridad de los sistemas biométricos de control de acceso basados en huella dactilar, por tal motivo, el presente capítulo se centrará en proporcionar la información respecto a las alternativas propuestas para contribuir a esta labor. Lo primero que se presentará es la alternativa de encriptado de minucias utilizando un mapa hiper-caótico en conjunto con la formula de Herón (utilizada para calcular el área de un triangulo) para brindarle seguridad a la información en su traslado a la base de datos y durante el tiempo de almacenamiento. Lo segundo que se presentará será una alternativa para modificar la información de las minucias utilizando un mapa hiper-caótico permitiendo conservar su propiedad de comparación y distinción pero sin revelar información de las minucias originales. Posteriormente se presentará el lugar donde se localizará cada uno de estos procesos en un sistema biométrico de control de acceso basados en huellas dactilares.

6.2. Alternativa de encriptado de minucias

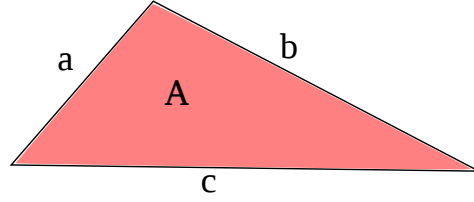
En el presente trabajo se presenta una alternativa de encriptado que utiliza la formula de Herón y un mapa hiper-caótico para ocultar la información, por tal motivo, primeramente se proporcionará una breve información al respecto.

6.2.1. Formula de Herón

Herón fue un matemático de Alejandría que fue reconocido como uno de los mayores inventores de la antigüedad, creó múltiples dispositivos utilizando su ingenio, por ejemplo: la dioptra y el odómetro. Una de las aportación más reconocidas de Herón es su fórmula para calcular el área de un triangulo conociendo solamente sus lados. A continuación se presenta la expresión matemática:

$$A = \sqrt{p(p-a)(p-b)(p-c)}$$

$$p = \frac{a+b+c}{2}$$



Donde p es el semi-perímetro, a , b y c son los lados del triángulo y A es el área del triángulo. Si el lector requiere indagar más sobre este tema puede consultar la referencia [Pér13] donde se presenta una comprobación utilizando el teorema de pitágoras en la página 211.

6.2.2. Mapa hiper-caótico Generalizado de Hénon

En la actualidad existen gran cantidad de información con respecto a los sistemas caóticos, pero cuando se mencionan comúnmente se refiere a un sistema dinámico que entre otros aspectos presenta un comportamiento aparentemente azaroso. Una manera de analizar la estabilidad de un sistema, es por medio de los exponentes de Lyapunov, los cuales, permiten interpretar las bifurcaciones y transiciones caóticas. Un sistema dinámico con un comportamiento hiper-caótico, presenta dos exponentes de Lyapunov positivo. El sistema hiper-caótico que se utilizará en este proceso de encriptado será el 3D mapa hiper-caótico generalizado de Hénon [], el cual se presenta a continuación:

$$\begin{aligned} x_1(k+1) &= -\beta x_2(k) \\ x_2(k+1) &= 1 + x_3(k) - \alpha x_2^2(k) \\ x_3(k+1) &= x_1(k) + \beta x_2(k) \end{aligned} \tag{6.1}$$

Donde x_1 , x_2 y x_3 son los estados del mapa de Hénon, α y β son los parámetros de control del mapa hiper-caótico.

El 3D mapa hiper-caótico generalizado de Hénon presenta un comportamiento hiper-caótico cuando se tiene los siguientes valores de parámetros $\alpha = 1,07$, $\beta = 0,3$ y las siguientes condiciones iniciales $x_1(0) = 0$, $x_2 = 0$ y $x_3 = 0$, en la figura 6.1, se muestra el atractor.

Mapa Generalizado de Hénon

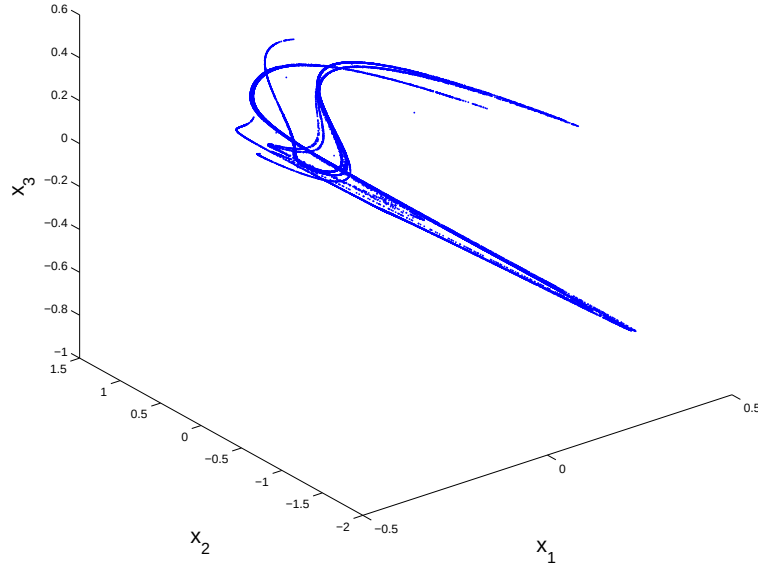


Figura 6.1: 3D Mapa hiper-caótico generalizado de Hénon

6.2.3. Procedimiento de encriptado/desencriptado

En el procedimiento de encriptado se utilizará el sistema hiper-caótico del mapa de Hénon generalizado como un generador de números Pseudo-aleatorios. El proceso general se muestra en la siguiente figura.

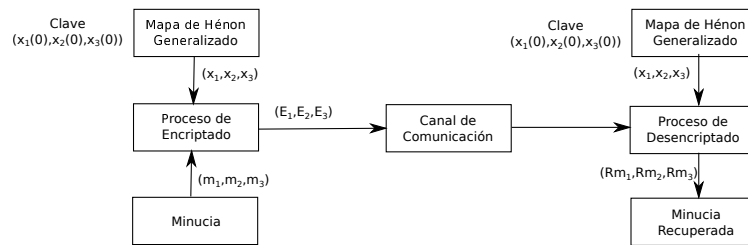


Figura 6.2: Diagrama de encriptado utilizando mapa de Hénon generalizado

En el procedimiento de encriptado se utiliza las condiciones iniciales como clave, pero el usuario introducirá una clave alfanumérica, y para generar las condiciones iniciales del sistema se realizará el siguiente procedimiento.

Paso 1: La clave alfanumérica estará constituida por 6 caracteres que pueden ser letras minúscula, mayúsculas o números. Por ejemplo: “Cifra9”, “4Hide8”.

Paso 2: Convertir los caracteres a valores numéricos considerando el código ASCII. Por ejemplo: Considérese “4Hide8”, sus caracteres será 4=52, H=72, i=105, d=100, e=101 y 8=56.

Paso 3: Considerando como posición 1 el carácter del lado izquierdo, se dividirán los valores de la posiciones impares entre 1000 y las posiciones pares entre 1000000, posteriormente sumar los valores contiguos para formar las condiciones iniciales. Por ejemplo: “4Hide8” será “52,72,105,100,101,56”, posteriormente realizando las operaciones indicadas

$$\frac{52}{1000}, \frac{72}{1000000}, \frac{105}{1000}, \frac{100}{1000000}, \frac{101}{1000}, \frac{56}{1000000}$$

Entonces las condiciones iniciales quedaran de la siguiente manera

$$x_1(0) = (52 \times 10^{-3}) + (72 \times 10^{-6}) = 0,052072$$

$$x_2(0) = (105 \times 10^{-3}) + (100 \times 10^{-6}) = 0,105100$$

$$x_3(0) = (101 \times 10^{-3}) + (56 \times 10^{-6}) = 0,101056$$

Para realizar el procedimiento del cifrado se realizaran los siguientes pasos:

Paso 1: Teniendo en cuenta que cada minucia esta compuesta por su componente en x , y y un ángulo ($m = \{m_x, m_y, m_\theta\}$), se obtendrá tres conjuntos de valores de los estados x_1, x_2, x_3 , iterando el mapa de Hénon generalizado, para cada uno de los componentes de la minucia, es decir (m_x, m_y, m_θ) , se obtendrá.

$$x_1(k), x_2(k), x_3(k), x_1(k+1), x_2(k+1), x_3(k+1), x_1(k+2), x_2(k+2), x_3(k+2)$$

Paso 2: Considerando que los valores de $x_1, x_2, x_3 \in \mathbb{R}$, se encuentran aproximadamente entre el rango -1.5 a 1.5, por conveniencia se realizará un mapeo del conjunto de números reales ($\mathbb{R}$) obtenidos del mapa hiper-caótico de Hénon a un conjunto de números enteros positivos ($\mathbb{Z}^+$) correspondiente al conjunto $\{x_n \in \mathbb{N} : 1 \leq x_n < (30) + 1\}$, por tanto se utilizará la siguiente expresión:

$$x_n = ((\{x_n \in \mathbb{N} : (|x_n| \times 10^8) \in \mathbb{N}) \bmod 30) + 1$$

Paso 3: Asignar los valores para las variables a , b y c , de la formula de Herón, para los componentes de la minucia de la siguiente manera

$$\begin{array}{lll} m_x & a_x = x_1(k) & b_x = x_2(k) & c_x = x_3(k) + x_1(0) \\ m_y & a_y = x_1(k+1) & b_y = x_2(k+1) & c_y = x_3(k+1) + x_2(0) \\ m_\theta & a_\theta = x_1(k+2) & b_\theta = x_2(k+2) & c_\theta = x_3(k+2) + x_3(0) \end{array}$$

Paso 4: Calcular el cuadrado del área (A) y el semi-perímetro (p) utilizando los datos

$$A^2 = p(p-a)(p-b)(p-c)$$

anteriores.

$$p = \frac{a+b+c}{2}$$

$$\begin{array}{lcl}
m_x & E_x = & \frac{m_x \times A_x^2}{p_x} \\
\text{Entonces tenemos} & m_y & E_y = \frac{m_y \times A_y^2}{p_y} \\
& m_\theta & \frac{m_\theta \times A_\theta^2}{p_\theta} \}
\end{array}$$

Por lo tanto el criptograma será $E = \{E_x, E_y, E_\theta\}$.

Para realizar el proceso de descifrado se realizan los siguientes pasos:

Paso 1: Realizar el mismo procedimiento del paso 1 y 2 del proceso de cifrado.

Paso 2: Asignar los valores para las variables a, b, c, p y A , de la formula de Herón, para los componentes de la minucia de la siguiente manera

$$\begin{array}{lllll}
m_x & a_x = x_1(k) & b_x = x_2(k) & c_x = x_3(k) + x_1(0) & A^2 = p(p-a)(p-b)(p-c) \\
m_y & a_y = x_1(k+1) & b_y = x_2(k+1) & c_y = x_3(k+1) + x_2(0) & \\
m_\theta & a_\theta = x_1(k+2) & b_\theta = x_2(k+2) & c_\theta = x_3(k+2) + x_3(0) & p = \frac{a+b+c}{2}
\end{array}$$

Paso 3: Considerando los datos de las variable encriptada $E = \{E_x, E_y, E_\theta\}$ y con los datos del paso anterior calcular los valores recuperados de las minucias $Rm = \{Rm_x, Rm_y, Rm_\theta\}$ utilizando las siguientes expresiones.

$$\begin{array}{l}
Rm_x = \frac{E_x \times p_x}{A_x^2} \\
Rm_y = \frac{E_y \times p_y}{A_y^2} \\
Rm_\theta = \frac{E_\theta \times p_\theta}{A_\theta^2}
\end{array}$$

6.3. Alternativa de modificación de minucias

En la presente sub-sección del trabajo se presenta una alternativa de modificación de minucias, la cual, utiliza un mapa hiper-caótico como para modificar los datos biométricos, por tal motivo, primeramente se proporcionará una breve información al respecto.

6.3.1. Puntos Singulares

Uno de los aspectos importantes en el tema de la información de una huella dactilar son sus puntos, los cuales, permiten tener puntos de referencias para estimar la posición relativa de las minucias, con respecto a estos puntos singulares. Existen dos tipos de puntos singulares uno es llamado punto núcleo (core) y el otro punto delta, un ejemplo se muestran en la imagen siguiente.

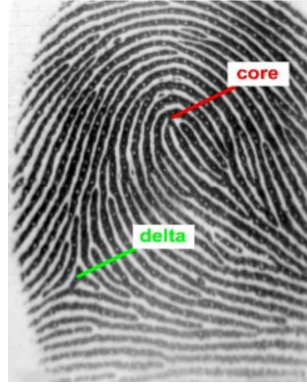


Figura 6.3: Puntos singulares core y delta.

En este trabajo de tesis para realizar la modificación de la minucia será requerido un punto de referencia por este motivo se considerará el punto singular que se encuentre en la parte superior, a este punto se le nombrará punto núcleo.

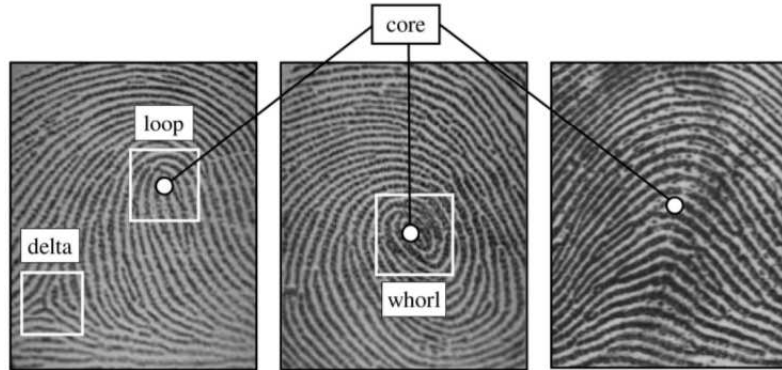


Figura 6.4: Punto de referencia (core)

6.3.2. Modificación de minucias

El procedimiento para realizar la modificación de las minucias de una huella dactilar se efectuará con los siguientes pasos.

Paso 1: Considerando una huella plasmada en forma vertical se tomara un punto de referencia (*core*), el cual sera la coordenada ($P = \{p_x, p_y\}$) de la singularidad que se encuentre en la parte superior de la imagen de la huella dactilar ver 6.4.

Paso 2: Teniendo en cuenta el punto de referencia $P = \{p_x, p_y\}$ y cada minucia $m_i = \{m_{x_i}, m_{y_i}, m_{\theta_i}\}$, se determinará la distancia d_i entre ambos.

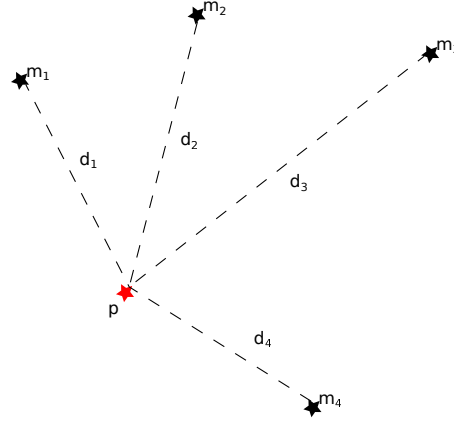


Figura 6.5: Distancias entre el punto de referencia y minucias.

Paso 3: Obtener valores enteros positivos a partir de la distancia d_i obtenida anteriormente, $d_i \in \mathbb{R} \rightarrow D_i = (d_i \in \mathbb{Z})$.

Paso 4: Determinar las condiciones iniciales que se utilizaran en el mapa de Rössler (expresión 3.4) para obtener los valores requeridos para modificar las minucias, esto se realizará considerando una *clave* = (x_1, x_2) y el valor $x_3 = \left\{ \frac{D_i}{10000} \right\}$ es decir: *Condiciones iniciales* = $\{clave, D_i\} = \{x_1, x_2, x_3\}$, donde D_i cambiará de valor dependiendo de la distancia entre el punto de referencia y la minucia, e i representa la i -ésima minucia.

Paso 5 : Obtener los valores para modificar las minucias. Realizar 200 iteraciones del mapa de Rössler considerando las condiciones iniciales que anteriormente se determinaron. Los valores de los estados caóticos obtenidos se utilizaran para modificar las minucias. Por lo tanto,

$$Dx = (\{x_1 \in \mathbb{N} : (x_1 \times 10^8) \in \mathbb{N}\}) \bmod 50$$

$$Dy = (\{x_2 \in \mathbb{N} : (x_2 \times 10^8) \in \mathbb{N}\}) \bmod 50$$

$$D\theta = (\{x_3 \in \mathbb{R} : (x_3 \times 10^8) \in \mathbb{R}\}) \bmod 2\pi$$

Paso 6: Modificar las minucias utilizando los valores previamente obtenidos con las siguientes expresiones $Mm_x = Dx + m_x$, $Mm_y = Dy + m_y$ y $Mm_\theta = D\theta + m_\theta$.

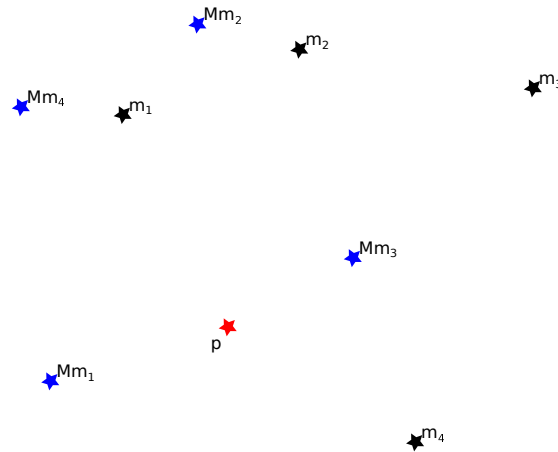


Figura 6.6: Minucias originales (negro), minucias modificadas (azul) y punto de referencia (rojo).

Nota: Considerando que la distancia entre las minucias y el punto de referencia no cambia significativamente permite tener la misma modificación para las datos si se trata de la imagen de la misma huella dactilar y es diferente para imágenes de diferentes huellas dactilares.

6.4. Ubicación de encriptado y modificación de minucias

6.4.1. Ubicación del encriptado de minucias

Considerando la estructura de los sistemas biométricos basado en huellas dactilares se consideró que en la etapa de enrolamiento (registro), el encriptado caótico se localizará después de la extracción de minucias, posteriormente los datos cifrados se enviará a la base de datos como se muestra en la figura 6.7. El cifrado proporcionará confidencialidad a la información, evitando su exposición ante algunos posibles ataques de espionaje realizados en la línea de comunicación entre la etapa de encriptado y la base de datos.

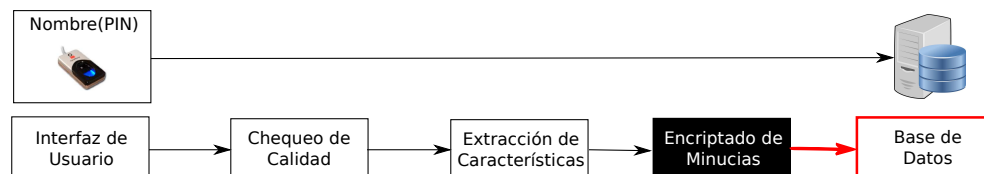


Figura 6.7: Ubicación del encriptado en la etapa del registro.

La etapa del desencriptado se localizará en la salida de la línea de información proveniente de la base de datos a la parte de verificación, esto para descifrar la información antes de su comparación. Lo anterior se ilustra en el diagrama que se muestra en la figura 6.8.

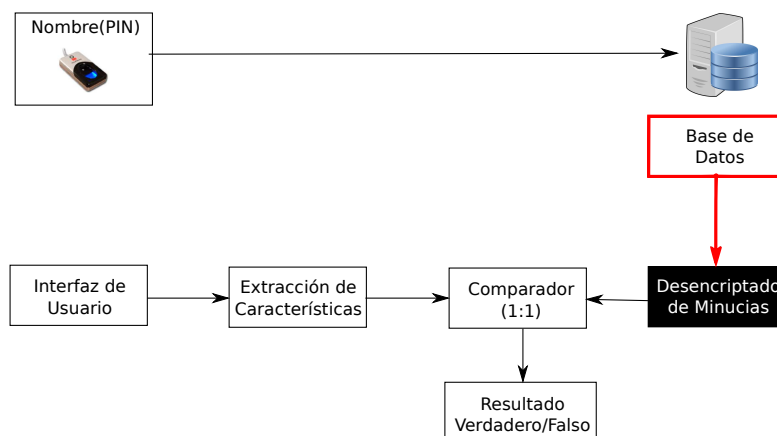


Figura 6.8: Ubicación de descriptado en la etapa de verificación.

6.4.2. Ubicación de la modificación de minucias

En la etapa de enrolamiento (registro) del sistemas biométricos basado en huellas dactilares la ubicación de la modificación de minucias se localizará después de la extracción de minucias, posteriormente los datos modificados se enviará a la base de datos como se muestra en la figura 6.9. La modificación proporcionará confidencialidad a la información de las minucias extraídas, evitando su exposición ante algunos posibles ataques de espionaje realizados en la línea de comunicación entre la modificación y la base de datos.

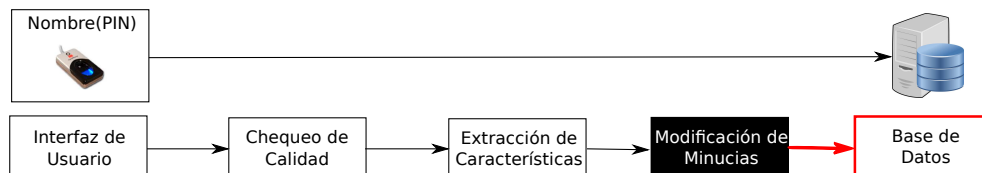


Figura 6.9: Ubicación del modificador de minucias en la etapa de registro

En la etapa de verificación del sistemas biométricos basado en huellas dactilares la ubicación de la modificación de minucias se localizará después de la extracción de minucias, posteriormente los datos modificados se enviará al modulo de comparación. Lo anterior se ilustra en el diagrama de la figura 6.10.

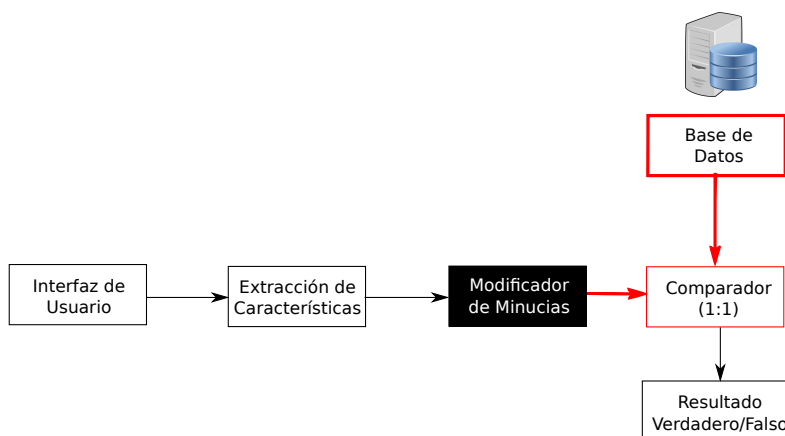


Figura 6.10: Ubicación del modificador de minucias en la etapa de verificación.

En las figuras anteriores se pueden observar cuadros de color negro, los cuales son las etapas que se agregan (encriptado, desencriptado o modificador de minucias) al sistema biométrico, también se observan flechas y recuadros de color rojo, las cuales, simbolizan las líneas de transmisión protegidas ante los posibles ataques de espionaje que se realicen para adquirir la información biométrica. También se puede observar, que la protección de los datos es durante su envío así como además durante el tiempo que se encuentre en la base de datos, esto se debe a que la información estará encriptada o modificada durante su almacenamiento dándole así una seguridad extra a la información.

6.5. conclusiones

Observando los procesos mostrados en este capítulo se puede llegar a entender que el utilizar los sistemas caóticos como herramientas para realizar encriptado o modificación de minucias es relativamente sencillo pero con grandes beneficios en ser altamente sensibles en su modificación dependiendo de la clave que se utilice debido a que los datos que se utilizan para modificar o cifrar son estados caóticos, los cuales, tienen la propiedad de presentar un comportamiento dinámico aparentemente pseudo-aleatorio.

Capítulo 7

Pruebas y resultados

7.1. Introducción

Esté capítulo está dedicado a presentar los resultados y pruebas realizadas, obtenidos durante la elaboración del trabajo de tesis, con el motivo que los lectores observen la contribución del trabajo de tesis en la seguridad de la información biométrica, en este caso proporcionándole seguridad a las minucias extradas de una huella dactilar. Los resultados del capítulo se encuentra dividido principalmente en dos métodos de protección, los cuales, son el encriptado de minucias y la modificación de minucias.

En los sistemas biométricos existen dos modalidades para confirmar la identidad de un usuario (ver la sección 4.4), en la presente capítulo sólo se considera la modalidad de verificación de usuarios, en donde la comparación se realiza de uno versus uno. Por tanto, antes de presentar los resultados se proporcionará una breve introducción de un sistema de verificación de huellas dactilares, con el objetivo que el lector tenga una mejor comprensión de los resultados que se presentaran.

7.2. Verificación de un usuario

Uno de los aspectos que se abordó en le presente trabajo de tesis es la verificación de usuarios en el control de accesos, el cual, es uno de los problemas que comúnmente atienden los sistemas biométricos. Por tal motivo, se presentan algunos pruebas de verificación de usuarios utilizando el proceso de comparación de minucias reportado por Joshua Abraham en la referencia [AGK11] , titulado “Fingerprint Matching using A Hybrid Shape and Orientation Descriptor”, el cual se puede acceder al documento en la pagina de Mathworks donde también se puede encontrar un programa desarrollado por el autor (<https://www.mathworks.com/matlabcentral/fileexchange/29280-fingerprint-matching- algorithm-using-shape-context-and-orientation-descriptors>, revisado 6-Agosto-2016)

7.2.1. Definición de verificación de un usuario

La **verificación de un usuario** por medio de su huella dactilar es uno de los problemas que atiende un sistema biométrico de control de acceso, pero esto que significa?, en este trabajo de tesis si un sistema biométrico verifica y confirma la existencia del registro de un individuo, el cual, con anterioridad se enrolo en la base de datos del sistema, se dirá que se realiza la verificación de un usuario, es decir la pregunta que se resuelve es “*el usuario es quien dice ser?*”. Algunas situaciones en donde se presenta este método de confirmación de identidad son: **el acceso a una cuenta de operaciones empresarial, el acceso al correo electrónico, el acceso a una cuenta bancaria**, etc. En las situaciones mencionadas, el acceso al servicio es permitido solamente a la persona quien tiene la autorización para hacer uso de el. Es decir, si una persona ajena al registro pretende solicitar acceso algún servicio, en donde no esta autorizado, está será rechazada por el sistema biométrico.

Para una mayor comprensión el lector puede observar en la figura 7.1, la verificación de un usuario (Bob).

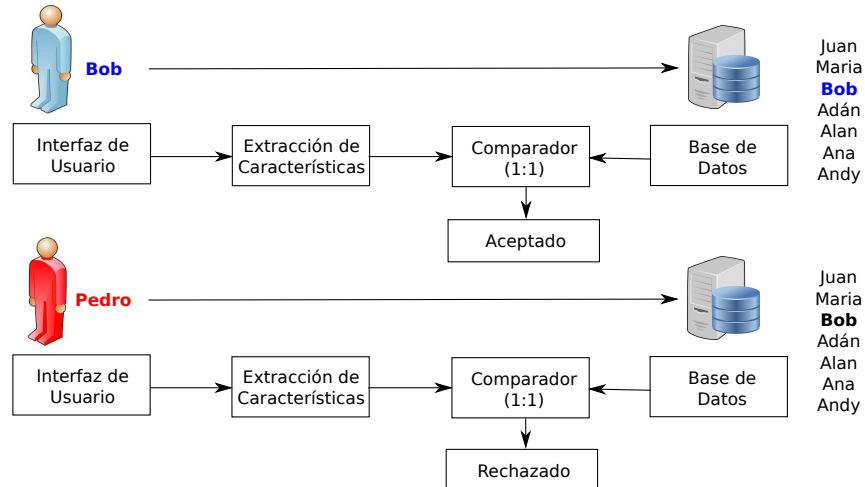


Figura 7.1: Diagrama esquemático que ilustra la verificación del registro de un usuario.

7.2.2. Comparación por medio de minucias

Una de las etapas principales en un sistema biométrico es la comparación y uno de los métodos más utilizados en huellas dactilares es la basada en minucias, siendo estas detalles particulares para cada individuo, y se describen como $m_i = \{x, y, \theta\}$ (ver). El objetivo principal de la comparación basada en minucias es realizar un cotejo uno a uno de emparejamiento de un conjunto de minucias previamente registradas versus el conjunto de minucias de ingreso al sistema biométrico de huellas dactilares. Por ejemplo:

$$A = \{m_{A_1}, m_{A_2}, \dots, m_{A_p}\} \text{ donde } m_{A_i} = \{x_{A_i}, y_{A_i}, \theta_{A_i}\} \text{ y } 1 \leq i \leq p.$$

$B = \{m_{B_1}, m_{B_2}, \dots, m_{B_p}\}$ donde $m_{B_j} = \{x_{B_j}, y_{B_j}, \theta_{B_j}\}$ y $1 \leq j \leq q$.

Donde p y q son el numero de minucias contenidas en un conjunto, A y B son el conjunto de minucias registrada y de ingreso respectivamente. Considerando que los conjuntos anteriores son producidos por detalles particulares auténticos de una huella dactilar, se puede realizar una métrica de similitud, comúnmente llamada “*similarity score*”. Un método para determinar esta similitud esta reportada en [LA06], se define como:

$$\text{sim}(A, B) = \frac{n_M^2}{n_A n_B}$$

Donde n_M es el número de pares coincidentes de minucias cotejadas, y n_A , n_B son el número de minucias de las regiones escaneadas de las huellas dactilares registrada y de ingreso respectivamente. Para una mejor comprensión ver figura 7.2.

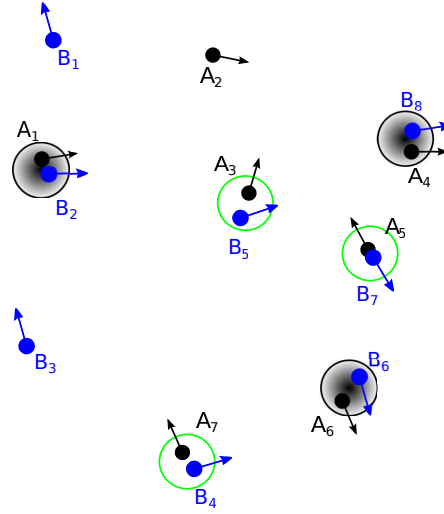


Figura 7.2: Comparación de dos conjuntos de minucias; con minucias similares dentro círculo negro ($n_M = 3$), conjunto A de color negro ($n_A = 7$), conjunto B de color azul ($n_B = 8$) y minucias con aparente similitud dentro del círculo verde.

En la literatura se pueden encontrar diversas formas para determinar la similitud de una huella dactilar, por ejemplo para realizar un cotejo adecuado de minucias en la referencia [AGK11], Joshua Abraham, Paul Kwan y Junbin Gao proponen un método de comparación que mejora los resultados obtenidos en la comparacion de minucias. En donde presentan el siguiente contador de similitud:

$$\text{sim}(A, B) = \frac{n_M (\sum_{(i,j)} \text{sim}_\delta(m_{A_i}, m_{B_j})) \cdot (\sqrt{S_{max}})}{n_A n_B} - \nu D_{SC}^{**} \quad (7.1)$$

$$S_{max} = \text{argmax}_{(i,j)} S^*(m_{A_i}, m_{B_j}, I(A_i, B_j)) \quad (7.2)$$

Donde $S^*(m_{A_i}, m_{B_j}, I(A_i, B_j))$ es el descriptor de medida de similitud basada en la orientación, D_{SC}^{**} es el estado de la medida de similitud en la distancia, ν es un parámetro ajustable

en $[0, 1]$, i y j son los índices de las minucias de las huellas dactilares A y B, respectivamente. $sim_{\delta}(m_{A_i}, m_{B_j})$ es el contador de minucias vecinas similares del par de minucias comparadas.

Nota: En la referencia [Lod13] se menciona que se puede realizar un ajuste de calidad basado en la cantidad de minucias contenidas en un conjunto, obteniendo así cinco posibilidades: Excelente ($m \geq 90$), muy buenos ($90 \geq m \geq 70$), bueno ($70 \geq m \geq 50$), justo, ($50 \geq m \geq 30$), pobre ($30 \geq m \geq 10$), y el valor "no ajustado" ($m \geq 0$). Esto se debe principalmente porque entre más minucias se tengan existirá mayor información que se pueda cotejar mejorando así el resultado.

En el presente trabajo de tesis las imágenes de la huella dactilares utilizadas para realizar las pruebas fueron obtenidas del lector de huellas dactilares y otras de la base de datos FVC2001. El lector puede consultar la base de datos entrando a la siguiente pagina <http://bias.csr.unibo.it/fvc2002/download.asp>. En la figura 7.3 se presentan las primeras 16 imágenes de la base de datos, esta base de datos esta constituida con 80 imágenes de huellas dactilar, sin embargo, son huellas de 10 dedos distintos, es decir las primeras 8 imágenes pertenecen al mismo dedo, las siguientes 8 a otro y así sucesivamente.

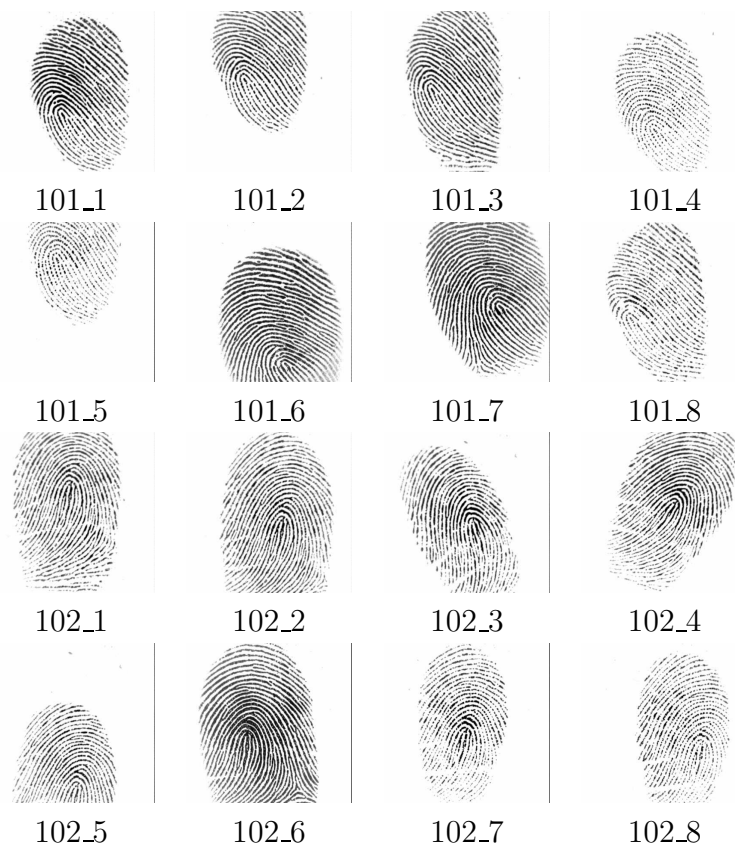


Figura 7.3: Primeras 16 imágenes de huellas dactilares de la base de datos FVC2002.

También a continuación se presentan algunas tablas con las comparaciones de huellas sin realizar el encriptado o la modificación de minucias.

muestra	1	2	3	4	5	6	7	8
101_1	4.4589	3.2334	2.3425	3.6594	4.3216	1.6450	1.3767	2.8751
102_1	3.7082	2.5504	2.5055	1.9440	3.4723	2.3772	2.4421	2.5672

Tabla 7.1: Resultados de la comparación del mismo dedo de las primeras 16 huellas de la base de datos FVC2002.

En la tabla 7.1 se puede observar que la mayoría de los valores del parámetro similitud ($sim(A, B)$), son mayores a 1, por tanto se puede considerar un umbral de discriminación donde el resultado de la comparación mayor a 1 indique, que las minucias cotejadas pertenecen a la misma huella.

	101_1	102_1	103_1	104_1	105_1	106_1	107_1	108_1	109_1	110_1
101_1	4.4589	0.1452	0.2293	0.1673	0.3616	0.1663	0.2365	0.3246	0.2121	0.2293
102_1	0.1452	3.7082	0.1009	0.1444	0.4849	0.0991	0.0776	0.2019	0.4137	0.1194

Tabla 7.2: Resultados de la comparación de algunas huellas distintas de la base de datos FVC2002.

En la tabla 7.1 se puede observar que la huellas distintas presentan valores del parámetro similitud ($sim(A, B)$) menores a 1.

7.3. Verificación aplicando solo encriptado

En esta subsección se presentaran los resultados del proceso de encriptado, así como, también los resultados obtenidos en el sistema biométrico después de implementar el procedimiento de encriptado y desencriptado. Para realizar las pruebas de encriptado se utilizaron las imágenes de la base de datos FVC2002 y se considero el esquema del sistema biométrico mostrado en la subsección 6.4.1, en donde se presenta la ubicación de la etapa de encriptado y desencriptado.

Para presentar, los resultados del encriptado se considerará un caso de cifrado de minucias como ejemplo y posteriormente se mostraran en una tabla los resultados obtenidos de la verificación de usuarios después de implementar el encriptado. En la figura 7.4 se presenta una huella dactilar, a la cual, se le extraen las minucias para posteriormente cifrarla por medio del procedimiento mostrado en la subsección 6.2.



Figura 7.4: Huella dactilar 101_1 de la base de datos FVC2002.

En la tabla 7.3 se presenta solamente 14 de las minucias extraídas de la imagen de la huella dactilar mostrada en la figura 7.4, sin embargo el número total de minucias extraídas son 25.

m_i	m_{x_i}	m_{y_i}	m_{θ_i}
m_1	216	46	0.5030
m_2	190	49	3.5827
m_3	146	64	3.2684
m_4	247	80	0.7002
m_5	173	86	0.3666
m_6	302	93	0.8372
m_7	176	127	0.2761
m_8	227	131	0.5634
m_9	164	135	3.3159
m_{10}	117	140	5.7642
m_{12}	216	169	0.7320
m_{13}	256	170	3.8934
m_{14}	196	181	3.7386

Tabla 7.3: Primeras 14 minucias de la figura 7.4.

En la tabla 7.4 se presenta las primeras 13 minucias encriptadas , que fueron estraidas de la imagen de la huella dactilar mostrada en la figura 7.4. Estas fueron cifradas utilizando la metodología mostrada en la subsección 6.2.

m_i	m_{x_i}	m_{y_i}	m_{θ_i}
m_1	0.0024	0.0290	0.0115
m_2	-0.2678	-0.7977	0.0035
m_3	0.1967	-0.1307	0.0021
m_4	-2.0140	1.6652	-0.0066
m_5	0.0804	-0.0626	0.0000
m_6	-0.4896	0.0054	0.0043
m_7	-0.3997	-0.2639	0.0011
m_8	0.0096	-1.4992	-0.0045
m_9	-4.7099	0.0602	-0.0209
m_{10}	2.2841	-2.2150	0.0031
m_{11}	-2.3211	1.5320	0.0012
m_{12}	-0.3797	-0.2114	0.0180
m_{13}	-2.6862	0.8876	-0.0236
m_{14}	0.1176	2.9673	-0.0007

Tabla 7.4: Primeras 14 minucias cifradas, de la figura 7.4. Todos estos valores deben ser multiplicados por un factor de 10^5 , es decir, $0,0024 \times 10^5$

Observando los resultados mostrados en las tabla 7.3 y 7.4, se puede ver claramente que los valores originales de las minucias son totalmente diferentes después del encriptado.

Nota: En el presente trabajo de tesis se utilizo la medida de similitud de la ecuación 7.1. Entonces en esta subsección se selecciono un umbral de 1, es decir, $\text{sim}(A, B) > 1$ corresponden a dos conjuntos de minucias pertenecientes a la misma huella dactilar.

En la tabla 7.5, se presentan los resultados de la comparación de la huella registrada y sus muestras extras, con el objetivo de observar si el encriptado no afecta la comparación de las minucias.

muestra	1	2	3	4	5	6	7	8
101_1	4.4589	3.2334	2.3425	3.6594	4.3216	1.6450	1.3767	2.8751
102_1	3.7082	2.5504	2.5055	1.9440	3.4723	2.3772	2.4421	2.5672
103_1	4.1189	2.2252	1.3966	3.6107	1.2668	1.4442	1.7982	1.6040
104_1	3.4573	1.7639	2.1718	0.8582	1.9839	1.0572	1.4192	2.1956
105_1	3.7595	2.2771	2.4038	1.1745	1.6055	2.3666	2.7182	1.5396
106_1	3.5597	2.1883	1.1935	1.5831	1.6487	1.7689	1.8549	1.7781
107_1	4.2253	2.1553	1.7540	1.9131	1.5363	1.6995	1.6508	1.5793
108_1	3.4630	1.3439	1.8809	1.3558	1.0391	1.0136	1.0704	1.4466
109_1	4.4272	1.7339	2.3407	1.8610	1.2915	1.5883	2.1905	2.0685
110_1	3.9547	2.0832	1.8128	1.2051	1.2208	2.3923	0.9253	1.6494

Tabla 7.5: Resultados de la comparación del mismo dedo de las primeras 16 huellas de la base de datos FVC2002.

En la tabla 7.5 se puede observar que los resultados de la comparación, son prácticamente

los mismo obtenidos antes de aplicar el cifrado de minucias, es decir, el cifrado no afecta a las operación del sistema biométrico.

	101_1	102_1	103_1	104_1	105_1	106_1	107_1	108_1	109_1	110_1
101_1	4.4589	0.1452	0.2293	0.1673	0.3616	0.1663	0.2365	0.3246	0.2121	0.2293
102_1	0.1452	3.7082	0.1009	0.1444	0.4849	0.0991	0.0776	0.2019	0.4137	0.1194
103_1	0.2293	0.1009	4.1189	0.2667	0.1400	0.2530	0.3581	0.0547	0.1605	0.2520
104_1	0.1673	0.1444	0.2667	3.4573	0.1330	0.0369	0.0443	0.1487	0.1783	0.0741
105_1	0.3616	0.4849	0.1400	0.1330	3.7595	0.1114	0.2294	0.1556	0.1969	0.0879
106_1	0.1663	0.0991	0.2530	0.0369	0.1114	3.5597	0.1500	0.0647	0.0964	0.3167
107_1	0.2365	0.0776	0.3581	0.0443	0.2294	0.1500	4.2253	0.1385	0.1336	0.4284
108_1	0.3246	0.2019	0.0547	0.1487	0.1556	0.0647	0.1385	3.4630	0.1803	0.0781
109_1	0.2121	0.4137	0.1605	0.1783	0.1969	0.0964	0.1336	0.1803	4.4272	0.1136
110_1	0.2293	0.1194	0.2520	0.0741	0.0879	0.3167	0.4284	0.0781	0.1136	3.9547

Tabla 7.6: Resultados de la comparación después de aplicar el encriptado y desencriptado, a las huellas de la base de datos FVC2002.

En la tabla 7.6, se presentan los resultados de la comparación de la huella registradas versus las huellas de dedos distintos, en la cual, se puede observa una ves más que el cifrado no afecta a las funciones del sistema biométrico.

7.3.1. Verificación aplicando solo modificación

En esta subsección se presentaran los resultados del proceso de modificación de minucias, así como, también los resultados obtenidos en el sistema biométrico después de implementar el procedimiento de modificación. Para realizar las pruebas de modificación se utilizaron las imágenes de la base de datos FVC2002 y se considero el esquema del sistema biométrico mostrado en la subsección 6.4.2, en donde se presenta la ubicación de la modulo de modificación de minucias tanto en la etapa de registro como en la etapa de verificación.

Para presentar, los resultados de la modificación se considerará un caso de una imagen de huella dactilar que se le extraen sus características, es decir, sus minucias para posteriormente modificar sus valores esto a modo de ejemplo y posteriormente se mostraran en una tabla los resultados obtenidos de la verificación de usuarios después de implementar la modificación. En la figura 7.5 se presenta la huella dactilar que se usa como muestra de la modificacion de minucias.



Figura 7.5: Huella dactilar 101_8 de la base de datos FVC2002.

En esta ocasión solo presentaremos imágenes para ilustrar la modificación debido a que se considera más fácil de comprender que sucede viendo la imagen que observando los datos numéricos. En la figura 7.6 se presentan las minucias extraídas, presentadas en la imagen como puntos de color rojo con excepción de una minucia que esta de color verde y el punto de referencia que esta representado por un punto azul.

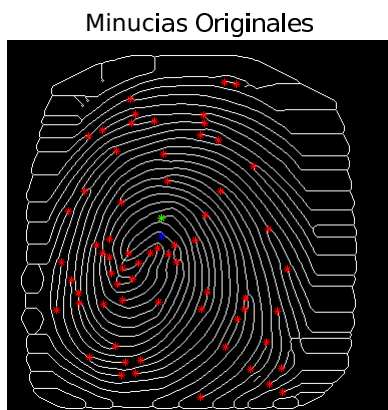


Figura 7.6: Minucias de Huella dactilar 101_8; minucias (rojo y verde), punto de referencia (azul).

En la figura 7.7 se presentan las minucias modificadas utilizando el procedimiento mostrado en la sección 6.4.2, utilizando una clave $(0.1, 0.1)$, con lo que se obtiene los resultados presentados en la imagen, la cual ilustra como puntos de color amarillo con excepción de una minucia que esta de color verde y el punto de referencia que esta representado por un punto azul.



Figura 7.7: Minucias de Huella dactilar 101_8; minucias (amarillo y verde), punto de referencia (azul).

Con el objetivo que el lector observe mas claramente como afecto la modificación a las minucias en la figura 7.8 se presentan sobrepuestas las minucias modificadas y originales, los colores siguen representado la misma información de las minucias que las figuras anteriores, pero en esta ocasión la minucias de color verde mostrada en la imagen nos muestra como la modificación de minucias las reubica a una posición distinta.

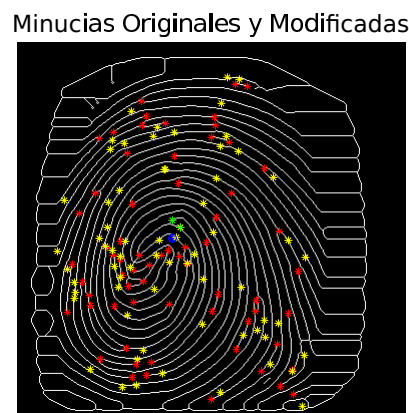


Figura 7.8: Minucias modificadas de la Huella dactilar 101_8; minucias originales (rojo y verde), minucias modificadas (amarillo y verde), puntos de referencia (azul).

Nota: En el presente trabajo de tesis se utilizo la medida de similitud de la ecuación 7.1. Entonces en esta subsección se selecciono un umbral de 0.22, es decir, $sim(A, B) > 0,22$ corresponden a dos conjuntos de minucias pertenecientes a la misma huella dactilar.

En la tabla 7.7, se presentan los resultados de la comparación de la huella registrada y sus muestras extras, con el objetivo de observar si el encriptado no afecta la comparación de las minucias.

muestra	1	2	3	4	5	6	7	8
101_1	4.4589	0.6340	0.9290	0.7940	0.1787	0.5033	0.6791	1.6078
102_1	3.7082	0.4072	0.9802	0.7755	1.6874	0.1968	0.4844	1.6186
103_1	4.1189	0.2697	0.1740	0.1730	0.4573	0.2958	0.6135	0.4595
104_1	3.4573	0.1651	0.3263	0.6534	0.1282	0.1664	0.9635	0.1964
105_1	3.7595	0.9362	1.1974	0.6401	0.1456	0.2179	0.0419	0.5919
106_1	3.5597	0.8438	0.0510	0.0541	0.0458	0.1606	0.0537	0.1439
107_1	4.2253	0.5873	0.9314	0.4863	0.7646	0.1776	0.1107	0.2729
108_1	3.4630	0.2144	1.1238	0.7260	0.2907	0.1499	0.1205	0.4848
109_1	4.4272	0.1554	0.9661	0.4158	0.3666	0.3267	0.3933	0.7610
110_1	3.9547	1.3837	1.4595	0.2805	0.2114	0.1136	0.4888	0.3942

Tabla 7.7: Resultados de la comparación del mismo dedo de las huellas de la base de datos FVC2002, pero aplicándole la modificación utilizando la clave (0.1,0.1)

Como se puede observar en la tabla 7.7, si se escoge un umbral de discriminación de 0.22 ($\text{sim}(A, B) > 0.22$), existen algunas comparaciones que podrían ser rechazados erróneamente, por ejemplo la mayoría de las muestras del 106_x, pero esto es debido a que las muestras presentan una gran diferencia en orientación o no se miran claramente, lo cual afecta a la medición pero si las muestras son adecuadas, la comparación correctamente puede realizarse.

	101_1	102_1	103_1	104_1	105_1	106_1	107_1	108_1	109_1	110_1
101_1	4.4589	0.0562	0.0627	0.0670	0.2956	0.0222	0.1634	0.0666	0.0777	0.1157
102_1	0.0562	3.7082	0.0369	0.0459	0.2200	0.0551	0.0852	0.0222	0.0819	0.0613
103_1	0.0627	0.0369	4.1189	0.0263	0.0808	0.0722	0.0694	0.0214	0.0409	0.0857
104_1	0.0670	0.0459	0.0263	3.4573	0.0822	0.0677	0.0392	0.0544	0.0535	0.0377
105_1	0.2956	0.2200	0.0808	0.0822	3.7595	0.0894	0.0809	0.0428	0.0668	0.0505
106_1	0.0222	0.0551	0.0722	0.0677	0.0894	3.5597	0.0614	0.0554	0.0564	0.0718
107_1	0.1634	0.0852	0.0694	0.0392	0.0809	0.0614	4.2253	0.0281	0.0413	0.0752
108_1	0.0666	0.0222	0.0214	0.0544	0.0428	0.0554	0.0281	3.4630	0.0989	0.0934
109_1	0.0777	0.0819	0.0409	0.0535	0.0668	0.0564	0.0413	0.0989	4.4272	0.0423
110_1	0.1157	0.0613	0.0857	0.0377	0.0505	0.0718	0.0752	0.0934	0.0423	3.9547

Tabla 7.8: Resultados de la comparación de las huellas distintas de la base de datos FVC2002, pero modificadas con clave (0.1,0.1)

En la tabla 7.8, se presentan los resultados de la comparación de la huella registradas versus las huellas de dedos distintos, en la cual, se puede observa, que son muy pocas las muestras que pueden ser aceptadas erróneamente, por ejemplo: 101_1 vs 105_1, 102_1 vs 105_1, etc.

7.4. conclusiones

Después de observar los resultados se puede comprender que en la etapa de encriptado no existe problema al implementarlo, sin embargo todavía faltan realizarle pruebas de seguridad al criptograma para garantizar su efectividad. También en la parte de modificación se pudo

observar que la calidad de la imagen captura afecta en gran medida al resultado de la modificación que a su vez afecta en la etapa de comparación aumentando los falsos rechazos, pero aun con este inconveniente los resultados son favorables al implementarlo en un sistema biométrico.

Capítulo 8

Conclusiones y trabajos futuros

8.1. Conclusiones generales

El presente trabajo de tesis proporciona una contribución más a las comunicaciones seguras, en esta ocasión, se atendió la problemática de la seguridad en algunas líneas de comunicación de un sistema biométrico de control de accesos basado en huellas dactilares. Consideración un escenario, en el cual, la etapa de registro, la etapa de almacenamiento (base de datos) y la etapa de verificación se encuentran separadas en sitios remotos. También, se omitieron algunos procesos debido a que su implementación en el programa de MatLab no fueron posibles debido a la incompatibilidad con nuestra versión de programa y las librerías del lector de huellas.

- Se observó que considerando las ecuaciones de Rössler y Hénon se puede presentar dinámicas hipercaóticas, las cuales, fueron benéficas para el propósito de cifrar y modificar la información de las características biométricas con dicha dinámica. Esto se debe al hecho, que la dinámica hipercaótica proporciona un medio de obtención de valores aparentemente azarosos que para nuestros propósitos son los más adecuados.
- La comparación, que se presentó en el trabajo de tesis, proporcionó buenos resultados al identificar las huellas dactilares, sin embargo estos resultados podrían mejorarse tomando en consideración que las muestras adquiridas por el lector deben pasar por una etapa que verifique la calidad de la imagen para disminuir muestras que no puedan ser identificadas correctamente.
- El encriptado y desencriptado de minucias de las huellas dactilares por medio de un programa implementado en MatLab, proporcionó buenos resultados. El cifrado y descifrado no afectó al proceso de comparación, siendo este hecho de gran importancia debido que esto nos indica que el cifrado presentado en esta tesis podría no afectar a los procesos que se realizan los sistemas biométricos convencionales.
- La modificación de minucias de las huellas dactilares por medio de un programa implementado en MatLab, proporcionó resultados favorables, sin embargo no fueron 100 % satisfactorios, pero esto pueden ser mejorados si se toman en consideración que las

muestras sean de calidades similares, es decir, con la menor cantidad de ruido o distorsión. La modificación aun cuando afecto el proceso de comparación, sigue siendo factible su implementación en un sistema biométrico de control de acceso, esto considerando que los problemas que se presentaron en la comparación también los presentan los sistemas implementados comercialmente, es decir, en el tema de los sistemas biométricos la disminución de falsos rechazo o falsas aceptaciones es todavia un tema abierto para su solución.

8.2. Trabajos futuros

Las actividades futuras que podrían realizarse con respecto al tema principal del trabajo realizado en la tesis serían las siguientes:

- Realizar una investigación con respecto a los falsos rechazos y las falsas aceptaciones, Aplicando la modificación de minucias presentada en la tesis.
- En esta ocasión se realizó el encriptado de minucias e imagen, en el cifrado de imagen ya se realizaron algunas pruebas para comprobar su efectividad, por tanto, un proceso similar puede ser realizado en el cifrado de minucias para corroborar su efectividad, también realizar una comparación con los métodos existentes de encriptado de minucias.
- Realizar un escrito con los resultados obtenidos del encriptado y modificación de minucias con miras de ser publicado.
- Realizar investigaciones con respecto a los ataques que sufren los sistemas biométricos comerciales. Pero en esta ocasión utilizando los encriptados y la modificación propuestas en la tesis, para analizar su efectividad a los posibles ataques que pueda sufrir.
- Implementar los programas de encriptado y modificación de minucias en otra plataforma de programación como Visual C++, Java, etc. Con el objetivo de llevar a cabo la implementación del encriptado y modificación de minucias caótico en un sistema biométrico comercial.

Anexo A

Programa final de modificación de minucias

A continuación se mostrarán dos programas que se desarrollaron con un entorno gráfico para simular las etapas de registro y verificación de un sistema biométrico de control de acceso basado en huellas dactilares. La realización de los programas se decidió después de observar los resultados obtenidos de las pruebas presentadas en el capítulo 7, en las cuales, se puede observar el proceso de modificación es viable para ser utilizado en un sistema biométrico, sin generar algún problema al resultado de la comparación de minucias.

A.1. Programa de registro

El objetivo del programa de registro es crear un archivo “.mat” que contendrá la información de la minucia modificada, la cual es requerida para realizar la comparación en el programa de verificación. En la figura A.1 se muestra la ventana con la que se inicia el programa, en la cual, se pueden observar tres botones, con el primer botón se obtiene la imagen del usuario que pretende ser registrado, lo que ocurre al presionar el botón es que se despliega una ventana en donde se muestran las imágenes de las huellas de las personas que se registraran, posteriormente de seleccionar una huella, ésta se mostrará en alguna sección de la ventana de registro, con el segundo botón el programa realizará el proceso de extracción de características distintivas de la huella dactilar, es decir, las minucias y el punto de referencia, una vez concluido este proceso se desplegará una imagen que muestre esta información, el tercer botón realiza el proceso de modificación de minucias presentado en el sección 6.4.2, al concluir la modificación se desplegará una ventana que solicitara indicar la carpeta y el nombre con el que se guardará las minucias modificadas y después se mostrará una imagen de las minucias originales y junto con las modificadas.



Figura A.1: Ventana del programa al iniciar el proceso de registro.

El motivo de que la imagen de la huella se obtenga de una carpeta en donde previamente se almacenó después de adquirirla del lector, en lugar de adquirirla directamente del lector de huellas dactilares, es debido a que no fue posible utilizar el lector de huellas dactilares directamente con el programa de MatLab, por tal motivo al momento de presionar el botón de “*Leer imagen*” se despliega la ventana que se muestra en la figura A.2.



Figura A.2: Ventana que se despliega al pulsar el botón “Leer imagen”.

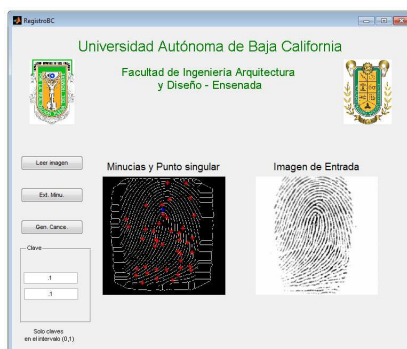


Figura A.3: Ventana que despliega la imagen de la huella selecciona y sus minucias.

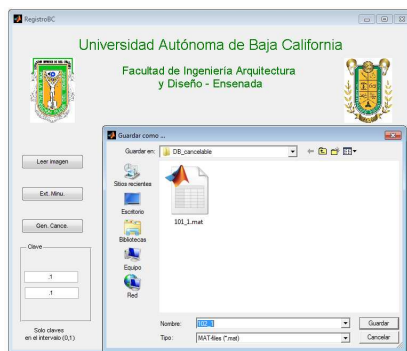


Figura A.4: Ventana de guardado de archivo “.mat”.

En la figura A.5 muestra la ventana que se despliega al finalizar el proceso de modificación para posteriormente mostrar las minucias modificadas ver la siguiente figura.

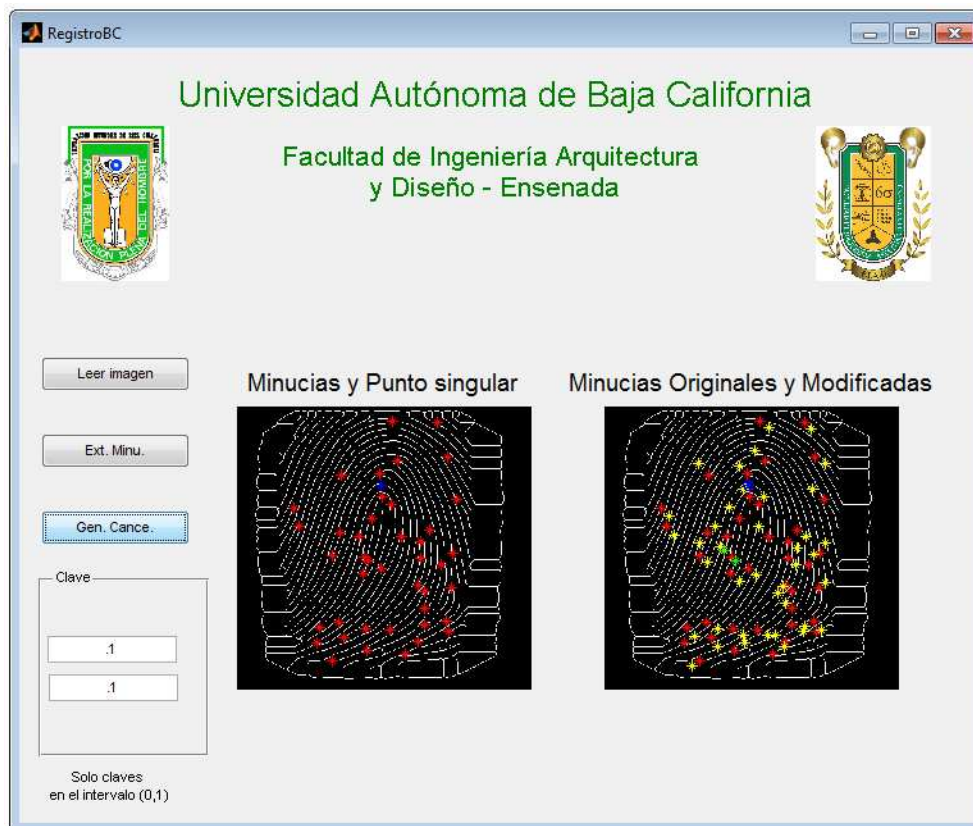


Figura A.5: Ventana del programa de registro al finalizar el proceso.

A.2. Programa de verificación de usuarios

El objetivo del programa de verificación es corroborar si el registro de un usuario existe, es decir, el programa realizará una comparación entre la información de la minucia modifi-

cada en la base de datos y la que ingresa el usuario. En la figura A.6 se muestra la ventana con la que se inicia el programa, en la cual, se pueden observar tres botones, con el primer botón “Leer imagen”, se obtiene la imagen de la huella dactilar del usuario que pretende ser reconocido por el sistema biométrico, al presionar este botón se despliega una ventana en donde se muestran las imágenes de las huellas que pretenden ser reconocidas por el programa, posteriormente de seleccionar una huella, ésta se mostrará en alguna sección de la ventana, con el segundo botón el programa realizará el proceso de extracción de características distintivas de la huella dactilar, es decir, las minucias y el punto de referencia. El tercer botón realiza el proceso de modificación de la minucia de ingreso y la comparación de la minucias guardada en la base de datos, este proceso de modificación es presentado en el sección 6.4.2, al concluir la modificación se desplegará en la ventana una leyenda que informara si fue aceptado o rechazado por el sistema biométrico ventana.

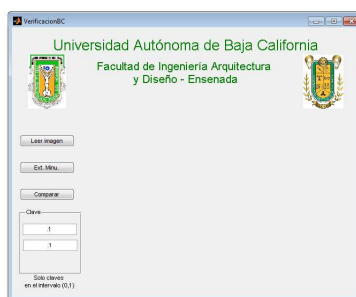


Figura A.6: Ventana del programa al iniciar el proceso de verificación.



Figura A.7: Ventana del programa al presionar “Leer imagen”.



Figura A.8: Ventana del programa mostrando la huella dactilar seleccionada.

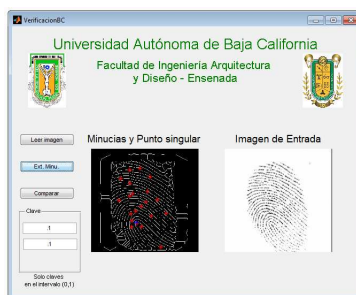


Figura A.9: Ventana del programa mostrando los resultados después de presionar el botón de extracción de características.

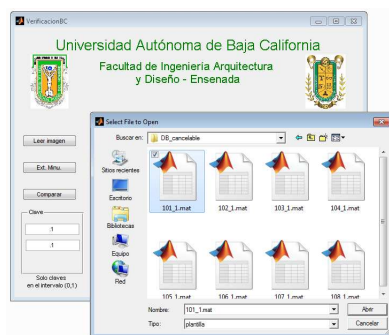


Figura A.10: Ventana del programa al presionar “comparar”.



Figura A.11: Ventana del programa que ilustra cuando un usuario es aceptado.

Anexo B

Programa final de encriptado de minucias

A continuación se mostrarán dos programas que se desarrollaron con un entorno gráfico para simular las etapas de registro y verificación de un sistema biométrico de control de acceso basado en huellas dactilares. La realización de los programas se decidió después de observar los resultados obtenidos de las pruebas presentadas en el capítulo 7, en las cuales, se puede observar que el proceso de encriptado es viable para ser utilizado en un sistema biométrico, sin generar algún problema al resultado de la comparación de minucias.

B.1. Programa de registro

El objetivo del programa de registro es crear un archivo “.mat” que contendrá la información de la minucia encriptada, la cual es requerida para realizar la comparación en el programa de verificación. En la figura B.1 se muestra la ventana con la que se inicia el programa, en la cual, se pueden observar tres botones, con el primer botón se obtiene la imagen del usuario que pretende ser registrado, lo que ocurre al presionar el botón es que se despliega una ventana en donde se muestran las imágenes de las huellas de las personas que se registraran, posteriormente de seleccionar una huella, ésta se mostrará en alguna sección de la ventana de registro, con el segundo botón el programa realizará el proceso de extracción de características distintivas de la huella dactilar, es decir, las minucias y el punto de referencia, una vez concluido este proceso se desplegará una imagen que muestre esta información, el tercer botón realiza el proceso de encriptado de minucias presentado en la sección 6.4.1, al concluir la modificación se desplegará una ventana que solicitara indicar la carpeta y el nombre con el que se guardará las minucias modificadas y después se mostrará una imagen de las minucias originales y junto con las modificadas.



Figura B.1: Ventana del programa al iniciar el proceso de registro.

En la siguiente figura se muestra la imagen seleccionada y sus minucias correspondientes. El ultimo botón esta asignado para realizar el proceso de encriptado al concluir el programa le solicitara guardar las minucias cifradas.

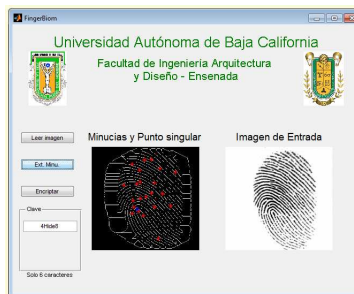


Figura B.2: Ventana que despliega la imagen de la huella selecciona y sus minucias.

B.2. Programa de verificación de usuarios

El objetivo del programa de verificación es corroborar si el registro de un usuario existe, es decir, el programa realizará una comparación entre la información descriptada de la minucia que se encuentra en la base de datos y la que ingresa el usuario. En la figura B.3 se muestra la ventana con la que se inicia el programa, en la cual, se pueden observar tres botones, con el primer botón "Leer imagen", se obtiene la imagen de la huella dactilar del usuario que pretende ser reconocido por el sistema biométrico, al presionar este botón se despliega una ventana en donde se muestran las imágenes de las huellas que pretenden ser reconocidas por el programa, posteriormente de seleccionar una huella, ésta se mostrará en alguna sección de la ventana, con el segundo botón el programa realizará el proceso de extracción de características distintivas de la huella dactilar, es decir, las minucias y el punto de referencia. El tercero botón realiza el proceso de comparación pero previamente realiza el descriptado de minucias almacenada en la base de datos. Al concluir el descriptado y la comparación se desplegará en la ventana una leyenda que informara si fue aceptado o rechazado por el sistema biométrico ventana.



Figura B.3: Ventana del programa al iniciar el proceso de registro.

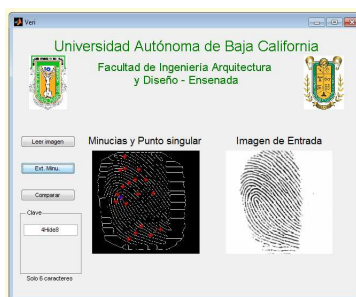


Figura B.4: Ventana que despliega la imagen de la huella selecciona y sus minucias.



Figura B.5: Ventana del programa que ilustra cuando un usuario es aceptado.

Bibliografía

- [AGK11] Joshua Abraham, Junbin Gao, and Paul Kwan. *Fingerprint matching using a hybrid shape and orientation descriptor*. INTECH Open Access Publisher, 2011.
- [AH11] T. Ahmad and Fengling Han. Cartesian and polar transformation-based cancelable fingerprint template. In *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, pages 373–378, Nov 2011.
- [AHW11] Tohari Ahmad, Jiankun Hu, and Song Wang. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition*, 44(10–11):2555 – 2564, 2011. Semi-Supervised Learning for Visual Content Analysis and Understanding.
- [Amb02] Parvathi Ambalakat. Secure authentication using biometric methods. *Information Security Technical Report*, 7(3):30 – 40, 2002.
- [Ani08a] K. Jain Anil. Biometric recognition: A new paradigm for security. Website, 2008. http://biometrics.cse.msu.edu/Presentations/AnilJain_BiometricsParadigm_Illinois_Oct07.pdf.
- [Ani08b] K. Jain Anil. Biometric system security. Website, 2008. http://biometrics.cse.msu.edu/Presentations/AnilJain_BiometricsSecurity_Japan_Jan06.pdf.
- [BKKM13] G.A. Bahgat, A.H. Khalil, N.S. Abdel Kader, and S. Mashali. Fast and accurate algorithm for core point detection in fingerprint images. *Egyptian Informatics Journal*, 14(1):15 – 25, 2013.
- [Bol03] Ruud Bolle. *Biometrics*. Rsa Press, 2003.
- [Bol04] Ruud Bolle. *Guide to biometrics*. springer, 2004.
- [BW12] G. Bhatnagar and Q.M.J. Wu. Chaos-based security solution for fingerprint data during communication and transmission. *Instrumentation and Measurement, IEEE Transactions on*, 61(4):876–887, April 2012.

- [CLG01] César Contreras Faz Marco V. José Claudia Lerma G., Daniel Olivares C. Sistema de análisis no lineal de la variabilidad de la frecuencia cardiaca. ELECTRO 2001, Instituto Tecnológico de Chihuahua, 2001. http://www.cnd.mcgill.ca/pdf_files/ELECTRO2001.pdf.
- [Clo10] Richard Clodfelter. Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3):181 – 188, 2010. New Technologies and Retailing: Trends and Directions.
- [COTG14] Y.J. Chin, T.S. Ong, A.B.J. Teoh, and K.O.M. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, 18(0):161 – 174, 2014.
- [Dal14] H.M. Daluz. *Fundamentals of Fingerprint Analysis*. CRC Press, 2014.
- [Dav03a] Dario Maio Anil K. Jain Salil Prabhakar Davide, Maltoni. *Handbook of Fingerprint Recognition*. springer, 2003.
- [Dav03b] Maltoni Dario Maio Anil K. Jain Salil Prabhakar Davide. *Handbook of Fingerprint Recognition*. springer, 2003.
- [Día95] J.C.G. Díaz. *Criptografía: Historia De La Escritura Cifrada*. sin colección. Editorial Complutense, 1995.
- [dLGALARA03] Rodrigo de Luis-García, Carlos Alberola-López, Otman Aghzout, and Juan Ruiz-Alzola. Biometric identification systems. *Signal Processing*, 83(12):2539 – 2557, 2003.
- [DM04] Anil K. Jain Davide Maltoni. *Biometric authentication*. springer, 2004.
- [DMRK14] Shah Faisal Darwaish, Esmiralda Moradian, Tirdad Rahmani, and Martin Knauer. Biometric identification on android smartphones. *Procedia Computer Science*, 35(0):832 – 841, 2014.
- [Esp92] Real Academia Española. *Diccionario de la lengua española / Real Academia Española*. Talleres Graficos de la Editorial Espasa-cape S.A., 1992.
- [Esp04] Adriana Elisa Espinosa. *El caos y la caracterización de series de tiempo a través de técnicas de la dinámica No-Lineal*. PhD thesis, Universidad Nacional Autónoma de México, 2004.
- [FZ06] M. Faundez-Zanuy. Biometric security technology. *Aerospace and Electronic Systems Magazine, IEEE*, 21(6):15–26, June 2006.
- [Hil00] Robert C. Hilborn. *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*. Oxford University Press, 2000.

- [HL13] Hung-I Hsiao and Junghsi Lee. A novel fingerprint image encryption algorithm based on chaos using apfm nonlinear adaptive filter. In *Consumer Electronics (ISCE), 2013 IEEE 17th International Symposium on*, pages 95–96, June 2013.
- [HmLH07] Ching-Yu Huang, Li min Liu, and D.C. Douglas Hung. Fingerprint analysis and singular point detection. *Pattern Recognition Letters*, 28(15):1937 – 1945, 2007.
- [JA07] Teresa Areitio Javier Areitio. Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación, Mayo 2007. <http://www.scribd.com/doc/13156295/Biometricos>.
- [JbP98] Anil Jain, Ruud bolle, and Sharath Pankanti. *Biometrics Personal identification in Networked Society*. springer, Agosto 1998.
- [JC08] RichardM. Jiang and Danny Crookes. Fpga-based minutia matching for biometric fingerprint image database retrieval. *Journal of Real-Time Image Processing*, 3(3):177–182, 2008.
- [JCD06] A. Jain, Yi Chen, and M. Demirkus. Pores and ridges: Fingerprint matching using level 3 features. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, volume 4, pages 477–480, 2006.
- [JRP04] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14(1):4–20, January 2004.
- [KAS⁺15] Salman H. Khan, M. Ali Akbar, Farrukh Shahzad, Mudassar Farooq, and Zeashan Khan. Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, 48(2):458 – 472, 2015.
- [KZA11] Muhammad Khurram Khan, Jiashu Zhang, and Khaled Alghathbar. Challenge-response-based biometric image scrambling for secure personal identification. *Future Generation Computer Systems*, 27(4):411 – 418, 2011.
- [LA06] Xuefeng Liang and Tetsuo Asano. Fingerprint matching using minutia polygons. In *18th International Conference on Pattern Recognition (ICPR’06)*, volume 1, pages 1046–1049. IEEE, 2006.
- [LCTL07] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, and Sangyoun Lee. Alignment-free cancelable fingerprint templates based on local minutiae information. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 37(4):980–992, Aug 2007.

- [Liu12] Rui Liu. Chaos-based fingerprint images encryption using symmetric cryptography. In *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, pages 2153–2156, May 2012.
- [LJ09] S.Z. Li and A.K. Jain. *Encyclopedia of Biometrics: I - Z*. Number v. 1 in Encyclopedia of Biometrics. Springer, 2009.
- [LK10] Chulhan Lee and Jaihie Kim. Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications*, 33(3):236 – 246, 2010. Recent Advances and Future Directions in Biometrics Personal Identification.
- [Lod13] Dana Lodrová. Security of biometric systems. *Information Sciences and Technologies*, 5(3):13, 2013.
- [LWkkkkkkkk12] Hongjun Liu, Xingyuan Wang, and Abdurahman kadir kadir kadir kadir kadir kadir kadir kadir. Image encryption using dna complementary rule and chaotic maps. *Applied Soft Computing*, 12(5):1457–1466, 2012.
- [Mar] Sergio Osuna Silvestre Marcos, Faúndez Zanuy. Experimentos sobre la vulnerabilidad de sistemas biométricos. http://www.shsconsultores.es/jornadas/0203_-_experimentos_sobre_la_vulnerabilidad_de_sistemas_biometricos.pdf.
- [MCP⁺06] Daesung Moon, Yongwha Chung, Sung Bum Pan, Kiyoun Moon, and Kyo Il Chung. An efficient selective encryption of fingerprint images for embedded processors. *ETRI Journal*, 28(4):444–452, August 2006.
- [MDFGOG11] Marcos Martinez-Diaz, Julian Fierrez, Javier Galbally, and Javier Ortega-Garcia. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12):1643 – 1651, 2011.
- [MdlN00] Lorenzo Gonzales Maria de las Nieves. *Influencia del Ruido Gaussiano Correlacionado en la Sincronizacion de Sistemas Caóticos*. PhD thesis, Universidad de Santiago de Compostela, 2000.
- [MMJP03] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. springer, 2003.
- [Moe71] A.A. Moenssens. *Fingerprint Techniques*. Inbau law enforcement series. Chilton Book Company, 1971.
- [Orm10] Lic. Jorge Ormachea. Seguridad en los sistemas biometricos. Website, Martes 01-Junio-2010. http://rosalesuriona.com/spip.php?article114&debut_articles=260.
- [Ort00] Juan Antonio Pérez Ortiz. *Música fractal: El sonido del caos*, 2000.

- [Pér13] M.A. Pérez. *UNA HISTORIA DE LAS MATEMÁTICAS: RETOS Y CONQUISTAS A TRAVÉS DE SUS PERSONAJES*:. 2013.
- [RCBC06] N. Ratha, J. Connell, R.M. Bolle, and S. Chikkerur. Cancelable biometrics: A case study in fingerprints. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, volume 4, pages 370–373, 2006.
- [Rob07] Chris Roberts. Biometric attack vectors and defences. *Computers & Security*, 26(1):14 – 25, 2007.
- [Sar07] Armando Fernández Sarasola. *Control de los Sistemas Continuos*. Textos universitarios ediuno, 2007.
- [SHX08] Zhao Song, Li Hengjian, and Yan Xu. A secure and efficient fingerprint images encryption scheme. In *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, pages 2803–2808, Nov 2008.
- [Vac07] J.R. Vacca. *Biometric Technologies and Verification Systems*. Elsevier Science, 2007.
- [VTM08] Juan M. Vilardy, Cesar O. Torres, and Lorenzo Mattos. Fingerprint encryption using fractional fourier transform. *5th. European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2008)*, 2008.
- [Web05] K.W. Webb. Biometric security solutions. *Security Privacy, IEEE*, 3(5):7–7, Sept 2005.
- [WYY11] Dawei Weng, Yilong Yin, and Dong Yang. Singular points detection based on multi-resolution in fingerprint images. *Neurocomputing*, 74(17):3376 – 3388, 2011.
- [XW10] Dacheng Xu and Xiaotao Wang. A scheme for cancelable fingerprint fuzzy vault based on chaotic sequence. In *Mechatronics and Automation (ICMA), 2010 International Conference on*, pages 329–332, Aug 2010.
- [Ye10] Guodong Ye. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, 31(5):347–354, 2010.
- [YJK09] Huijuan Yang, Xudong Jiang, and A.C. Kot. Generating secure cancelable fingerprint templates using local and global features. In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 645–649, Aug 2009.
- [ZGW10] Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using dna addition combining with chaotic maps. *Mathematical and Computer Modelling*, 52(11-12):202–2035, 2010.
- [Zha04] David D. Zhang. *Palmprint authentication*. kluwer Academic, 2004.