UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

CENTRO DE IDENTIFICACIÓN Y SEGURIDAD DIGITAL

FACULTAD 1.

Modelo para la protección de plantillas de minucias de huellas dactilares

Ing. Ramón Santana Fernández

Habana, 2016

UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

CENTRO DE IDENTIFICACIÓN Y SEGURIDAD DIGITAL

FACULTAD 1.

Modelo para la protección de plantillas de minucias de huellas dactilares

AUTOR: Ing. Ramón Santana Fernández

TUTORES: Dr. Yanio Hernández Heredia

Dra. Vivian Estrada Sentí

Habana, 2016

Frase

Vive hoy lo que otros sueñan con vivir en el futuro.
Pablo Coelho

Agradecimientos

A mis padres por su incondicional amor y paciencia, aun en los momentos en los que no les he dejado fácil el trabajo de ser padres.

A mi hermano por su apoyo y comprensión, por ser incondicional y empujarme hacia adelante cuando yo no sé si puedo continuar.

A Allitsac por cada detalle, por llegar en el momento en que menos lo esperaba y regalarme su sonrisa.

A mis tutores Vivian y Yanio, a los doctores del PEFCI y en especial al Dr. Juan Pedro Febles por cada corrección, cada palabra de aliento y por la confianza depositada.

A mis amigos Darién y Lisset por todo el apoyo que me han brindado sobre todo en los tiempos difíciles.

A mis amigos y compañeros de trabajo Machado y Osay por todo el apoyo que me han brindado.

A mis compañeros de investigación y en especial a Anais y Yaicel que han estado ahí para mí en cada momento.

Dedicatoria

A las personas más importantes en mi vida…

SÍNTESIS

En la arquitectura general de un sistema biométrico han sido detectadas ocho vulnerabilidades que comprometen el proceso de autenticación de personas. De ellas seis vulnerabilidades permiten la obtención de la plantilla de minucias en texto claro. Para mitigar estas vulnerabilidades han sido propuestos varios modelos de protección de plantillas de minucias sin embargo, varias vulnerabilidades en la seguridad criptográfica de estos modelos facilitan la obtención de los datos biométricos en texto claro. Con el propósito de aumentar la seguridad criptográfica y facilitar la revocabilidad se propone en la presente investigación un modelo de protección de plantillas de minucias de huellas dactilares. El modelo tiene como objetivo realizar la protección de plantillas de minucias de huellas dactilares basado en estructuras locales y métodos criptográficos de forma tal que aumente la seguridad criptográfica y facilite la revocabilidad de los datos biométricos utilizados para el reconocimiento de personas. Como principales resultados se obtiene un modelo de protección de plantillas de minucias de huellas dactilares que permite la comparación de plantillas en el dominio protegido y facilita la revocabilidad de plantillas canceladas, utilizando estructuras de minucias para aumentar la seguridad del proceso de reconocimiento de personas mediante huellas dactilares. La estructura de minucias denominada estructura compleja y el método de comparación constituyen aportes prácticos de la investigación.

Índice

Índice

INTRODUCCIÓN

La utilización de identificadores biométricos para controlar el acceso a recursos protegidos eleva, de manera considerable, la seguridad del proceso de autenticación. La principal razón reside en que son características físicas o conductuales inherentes a un individuo, las cuales son más difíciles de robar, perder o adivinar que los identificadores tradicionales. La huella dactilar es considerada el identificador biométrico más utilizado para realizar el reconocimiento de personas. Esto se debe principalmente a que el proceso de adquisición del rasgo biométrico es poco invasivo [1].

La biometría es la medición de datos biológicos [2]. El término biometría es comúnmente utilizado para referirse al reconocimiento de una persona mediante características físicas como la huella dactilar, el rostro, el iris o de comportamiento como la firma y la forma de caminar [3], [4]. En la actualidad la biometría cuenta con un gran campo de aplicación en sistemas criminales, gubernamentales y comerciales ganando gran aceptación como uno de los métodos más efectivos para la autenticación de personas en una amplia gama de aplicaciones informáticas [5].

Un sistema biométrico es esencialmente un sistema de reconocimiento de patrones que opera a partir de la adquisición de datos biométricos de un individuo, extrae un conjunto de características de los datos capturados y las compara con las almacenadas [2]. En dependencia del contexto puede ser utilizado para realizar verificación o identificación biométrica. El proceso de verificación valida la identidad de un individuo al comparar la muestra obtenida con la que se encuentra almacenada en la base de datos. El proceso de

identificación compara la muestra dactilar adquirida con todas las almacenadas en la base de datos. Este proceso es un componente crítico en la aplicación del reconocimiento negativo, el cual evita que una persona pueda tener múltiples identidades.

La utilización de identificadores biométricos para la autenticación de personas en sectores civiles y gubernamentales como instrumento de seguridad a través de redes públicas o privadas, ha generado mayor preocupación por la seguridad de los datos biométricos. Análisis realizados por diversos autores [2], [6]–[8] han detectado ocho puntos de vulnerabilidad en la arquitectura general de un sistema biométrico mediante los cuales es posible obtener el rasgo biométrico, como se muestra en la figura 1.

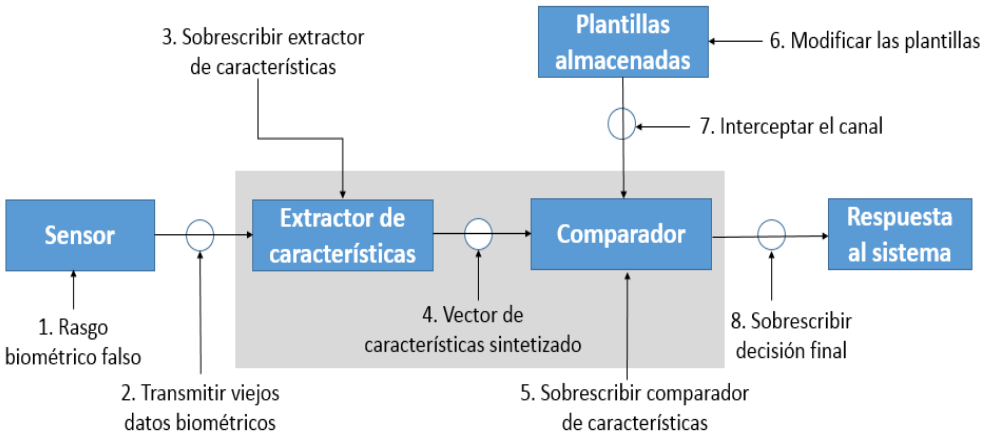


Figura 1: Principales puntos de vulnerabilidad en un sistema biométrico Adaptado [9]

Los puntos de vulnerabilidad en la arquitectura general de un sistema automático de identificación mediante huellas dactilares, que resultan de interés para esta investigación, son aquellos mediante los cuales es posible la obtención de los datos biométricos de forma parcial o total. Estos son:

1. el extractor de características
2. el canal de comunicación entre el extractor y el comparador

3. el comparador de características
4. el canal de comunicación del comparador con la base de datos biométrica
5. la base de datos biométrica

La necesidad de proteger los datos biométricos en estos puntos de vulnerabilidad reside en que la huella dactilar es única para toda la vida y no puede ser cancelada o cambiada como una contraseña personal. La obtención por parte de un atacante de las minucias pertenecientes a una huella dactilar representa la pérdida del identificador para toda la vida. Esto se debe a que al filtrarse parcial o totalmente una plantilla de minucias, se puede realizar la reconstrucción de la huella dactilar correspondiente, obteniéndose una impresión como se propone en [5].

La manera más sencilla de proteger los datos biométricos almacenados sería utilizando la criptografía clásica [7], [10] sin embargo, las propiedades de las funciones utilizadas por estos métodos dificultan el proceso de comparación de minucias en un dominio protegido. Esto se debe principalmente a que pequeños cambios en el conjunto de datos a cifrar provocan grandes cambios en el conjunto de datos cifrados. Las muestras de huellas dactilares cambian debido a varios factores como la traslación, la rotación, la superposición parcial y la deformación lineal que experimenta el dedo al hacer contacto con una superficie.

La principal deficiencia de la utilización de métodos criptográficos clásicos como *Advanced Encryption Standard* (AES), *Data Encryption Standard* (DES), entre otros, para la protección de datos biométricos reside en la pérdida del rendimiento biométrico durante el proceso de comparación de plantillas de minucias en el dominio protegido. Por esta razón es necesario decodificar el

conjunto de datos biométricos antes de realizar el proceso de comparación de características. Durante este instante las características biométricas se encuentran en texto claro. Diferentes ataques mediante virus troyanos o mal funcionamiento de hardware durante el proceso de comparación son algunos de los factores que permiten la obtención de las minucias durante el proceso de comparación. Para proteger los datos biométricos durante el proceso de autenticación de personas se describe en la bibliografía la utilización de la criptografía biométrica.

Varios enfoques han sido propuestos para realizar la protección de plantillas de minucias de huellas dactilares, clasificándose en dos grandes grupos:

1. Cripto-sistemas biométricos

   Han sido definido por varios autores [7], [11], [12] como una construcción criptográfica donde se bloquean un conjunto de datos a partir de una llave. Para desbloquear este conjunto de datos otro usuario necesita un conjunto de datos de prueba lo suficientemente cercano al original como para liberar la llave y el conjunto de datos originales.
2. Las transformaciones cancelables o no invertibles

   Han sido definidas [13] como una distorsión de la señal biométrica provocada por una función de un solo sentido.

Los primeros modelos elaborados para la protección de los datos biométricos (modelos pioneros), los cuales constituyen la base criptográfica de los modelos propuestos en la actualidad, son:

1. Hash biométrico
2. Bóveda difusa

3. Plantillas cancelables

Estos modelos tienen como objetivo enmascarar los datos biométricos originales transformándolos mediante el uso de diferentes métodos y funciones matemáticas. Para garantizar la seguridad de los datos, el proceso de comparación se realiza en el dominio protegido o transformado. Debido a las variaciones presentadas por los datos biométricos, se hace necesario realizar la alineación de las plantillas de minucias.

El rendimiento biométrico, expresado en tasas de falso rechazo, falso aceptado, genuinos aceptados, genuinos rechazados y tasas de error relativo, son métricas importantes para el correcto funcionamiento del sistema. Para no afectar el rendimiento biométrico varios enfoques han sido propuestos con el objetivo de mitigar las dificultades impuestas por el proceso de alineación. Cada uno de estos modelos tiene sus ventajas y limitaciones en cuanto a la seguridad de la plantilla, costo computacional, requerimientos de almacenamiento, aplicabilidad y tipo de representación biométrica utilizada.

Estudios realizados por varios autores sobre la seguridad criptográfica de los modelos pioneros [9], [14], [15] han señalado diferentes vulnerabilidades mediante las cuales es posible obtener los datos en texto claro a partir de las plantillas protegidas. Por ello no se encuentran listos para ser desplegados en un sistema automático de identificación de personas mediante huellas dactilares en un ambiente real [7].

Basado en el estudio realizado se identificaron un conjunto de limitaciones y/o deficiencias entre las que se pueden destacar las siguientes:

1. Los modelos de protección de plantillas de minucias de huellas dactilares presentan vulnerabilidades que permiten la obtención de los datos originales a partir de los datos cifrados.
2. Los modelos de alineamiento propuestos se basan en la selección de una característica biométrica que puede estar o no presente, que puede ser mal seleccionada o son costosos computacionalmente.
3. La propiedad de revocabilidad en los modelos propuestos no es sencilla de realizar, lo que provoca que sea compleja la utilización de estos métodos en el proceso de identificación biométrica.
4. Aun cuando han sido mitigadas algunas de las vulnerabilidades del modelo de protección bóveda difusa, existen problemas conceptuales en la definición del modelo en sí, que no aseguran el cumplimiento del principio de seguridad criptográfica.
5. Los métodos empleados para la comparación de plantillas de minucias en el dominio cifrado se basan en la distancia euclidiana o en la verificación de que un elemento del conjunto de prueba aparezca en el conjunto de muestra, lo que disminuye el rendimiento biométrico.
6. En [7] se plantea que los modelos propuestos no se encuentran listos para ser utilizados en la protección de plantillas de minucias de huellas dactilares en ambientes reales.
7. En [16] se plantea que el modelo de bóveda difusa no ofrece seguridad criptográfica mientras sea utilizado para proteger los datos pertenecientes a un solo identificador biométrico.

Basado en el estudio realizado se identificó el siguiente problema de investigación:

¿Cómo aumentar la seguridad criptográfica y facilitar la revocabilidad de los datos biométricos utilizados para el reconocimiento de personas mediante huellas dactilares?

Objeto de estudio: los procesos de seguridad criptográfica y el reconocimiento de personas mediante huellas dactilares.

Campo de acción: los modelos de protección de plantillas de minucias de huellas dactilares basados en estructuras de minucias.

Como **objetivo general** de la investigación se plantea:

Desarrollar un modelo de protección de plantillas de minucias de huellas dactilares, basado en estructuras locales y métodos criptográficos, que aumente la seguridad criptográfica y facilite la revocabilidad de los datos biométricos utilizados para el reconocimiento de personas.

Objetivos específicos:

1. Elaborar el marco teórico de la investigación a través de la extracción y recopilación de información asociada al problema de la investigación para conocer las fortalezas y debilidades de los modelos de protección de plantillas de minucias existentes.
2. Proponer un método para la comparación de plantillas de minucias en el dominio protegido que permita el análisis global y local de la información protegida.
3. Diseñar un modelo de protección de plantillas de minucias de huellas dactilares para aumentar la seguridad criptográfica del proceso de reconocimiento de personas mediante huellas dactilares.

4. Validar el modelo propuesto utilizando bases de datos internacionales para corroborar la hipótesis de la investigación.

Derivado de la construcción del marco teórico de la investigación y según lo expuesto, se formula la siguiente **hipótesis** de la investigación:

El desarrollo de un modelo de protección de plantillas de minucias de huellas dactilares, basado en estructuras locales y métodos criptográficos, aumenta la seguridad criptográfica y facilita la revocabilidad de los datos biométricos utilizados para el reconocimiento de personas.

Entre los métodos científicos utilizados en la investigación se encuentran:

Métodos teóricos: el método **hipotético-deductivo** para la formulación de la hipótesis de la investigación y presentar nuevas líneas de trabajo afines que tributen al desarrollo de la investigación. El método **histórico-lógico** para el estudio de trabajos anteriores y afines con el problema planteado. El método **analítico-sintético** para desglosar el problema principal en pequeños problemas de investigación, facilitando profundizar en el conocimiento existente sobre el tema sintetizándolo en la solución final. El método **modelación** para el desarrollo del modelo de protección de plantillas de minucias.

Métodos empíricos: el método **análisis documental** para la revisión de la bibliografía especializada en el transcurso de la investigación. El método **experimental** para la comprobación del modelo propuesto.

Principales aportes

La novedad científica del trabajo se expresa en los siguientes aportes teóricos y prácticos:

Aporte teórico

- La fundamentación y sistematización de un modelo para la protección de plantillas de minucias que permita la comparación de plantillas de minucias en el dominio protegido y facilita la revocabilidad de plantillas canceladas utilizando estructuras locales de minucias para aumentar la seguridad del proceso de reconocimiento de personas mediante huellas dactilares en sistemas automatizados de identificación de personas.

Aporte práctico

- Estructura de minucias para la representación y extracción de características identificativas, invariantes a rotación y traslación.
- Un módulo para realizar la protección y comparación de plantillas de minucias que puede ser utilizado en un sistema automático de identificación mediante huellas dactilares. Este módulo incluye un algoritmo de cifrado y un algoritmo de comparación de plantillas cifradas.

La tesis está estructurada en: introducción, tres capítulos, conclusiones, recomendaciones, bibliografía y un cuerpo de anexos.

En el capítulo 1 se presentan los fundamentos teóricos de la investigación, se realiza un análisis de los principales modelos utilizados para la protección de plantillas biométricas resaltando sus vulnerabilidades, principales debilidades y fortalezas.

En el capítulo 2 se realiza un análisis documental de los modelos híbridos, se describen los componentes fundamentales del modelo de protección de plantillas de minucias propuesto y su funcionamiento, detallando las estructuras

de minucias y funciones utilizadas para la protección del conjunto de datos biométricos.

En el capítulo 3 se presentan los resultados obtenidos durante el proceso investigativo, las indicaciones metodológicas para la implementación del modelo, el diseño de los experimentos así como los resultados de la implementación del modelo y la comparación con los resultados de los modelos existentes a nivel mundial.

Capítulo I: Marco teórico referencial sobre los modelos de protección de plantillas de minucias de huellas dactilares

Capítulo I: Marco teórico referencial sobre los modelos de protección de plantillas de minucias de huellas dactilares

En el presente capítulo se realiza el análisis del marco teórico referencial de la investigación. Se exponen los principales conceptos asociados al dominio del problema planteado y se formaliza la descripción de los principios fundamentales a tener en cuenta para la protección de los datos biométricos.

1.1 Elementos asociados al dominio del problema

La biometría (del griego bios vida y metrón medida) consiste en desarrollar métodos automatizados que analizan determinadas características humanas para identificar o verificar la identidad de personas, usando técnicas de reconocimiento de patrones. Estas características son difíciles de perder, transferir u olvidar y pueden ser físicas o de comportamiento. Las huellas dactilares, la retina, el iris, los patrones faciales o la geometría de la palma de la mano, representan ejemplos de características físicas, mientras que las del comportamiento pueden incluir la firma, la forma de caminar y la forma de teclear [1].

Los sistemas biométricos aportan una solución efectiva al problema de la identificación. No obstante, cada característica biométrica es diferente, y no siempre todas son adecuadas en las distintas aplicaciones. Al diseñar un sistema biométrico se evalúan diversos parámetros, como el poder distintivo de la característica biométrica que se emplee y la facilidad que se tenga para su uso, entre otros, que determinan su utilidad en las aplicaciones reales [17].

Capítulo I

La identificación de personas mediante características físicas o conductuales, únicas persistentes e invariantes en el tiempo, constituye el campo de investigación del reconocimiento biométrico [1], [18]. La identificación de personas mediante huellas dactilares [1] se realiza utilizando la orientación y localización de las bifurcaciones y terminaciones presentes en las crestas, denominadas minucias.

- **Huellas dactilares**

En [1] se definen las huellas dactilares como un rasgo biométrico compuesto por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos inter-papilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene un aceite el cual es retenido en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo, produciendo el facsímil o negativo de la huella.

- **Minucia.**

En [1] se define una minucia como varias maneras en las que las crestas son descontinuadas. Constituye la característica más utilizada en el reconocimiento de personas mediante huellas dactilares. Está constituida por un par de coordenadas (x, y), un ángulo (σ) formado por la orientación de la cresta en relación con el eje x y el tipo de minucia (bifurcación o terminación).

- **Plantillas de minucias**

En [19] se definen las plantillas de minucias como los datos que representan la medida del identificador biométrico luego de ser enrolado en el sistema y que

será utilizado en el proceso de verificación de identidad para comparar con diferentes plantillas biométricas de prueba.

1.2 Protección de plantillas de minucias

El término criptografía se define en [20] como el estudio de las técnicas matemáticas relacionadas a aspectos de seguridad de la información tales como: confidencialidad, integridad de los datos, autenticación y origen de los datos.

La protección de plantillas de minucias de huellas dactilares se define en [1], [21] conceptualmente como la transformación de los datos en texto claro a otro espacio de representación utilizando una transformación no invertible.

El objetivo principal de este proceso consiste en proteger los datos biométricos de manera tal que sea complejo computacionalmente obtener el conjunto de datos originales a partir de los datos protegidos. Como parte de este conjunto de técnicas se debe tener en cuenta que el proceso de comparación debe realizarse en el dominio protegido degradando lo menos posible el rendimiento biométrico del sistema.

Las principales problemáticas en este campo de estudio, que serán abordadas en la presente investigación, son:

1. La alineación de las plantillas de minucias antes de realizar el proceso de comparación, sin filtrar información concerniente a las minucias.
2. Las brechas de seguridad encontradas en los métodos bóveda difusa, plantillas cancelables y hash biométrico, los cuales constituyen las bases criptográficas de los modelos de protección de plantillas de minucias en la actualidad.

3. Los algoritmos de comparación revisados en la bibliografía realizan el análisis local de los datos en el mejor de los casos, dejando información que puede mejorar las tasas de error obtenidas en este proceso.

1.2.1 Características fundamentales de los modelos de protección de plantillas de minucias.

Para la formulación de un modelo de protección de plantillas de minucias [7] se han definido tres principios fundamentales:

1. Seguridad criptográfica: consiste en la dificultad computacional de obtener el conjunto de datos biométricos originales a partir del conjunto de datos biométricos protegidos.
2. Revocabilidad: consiste en la posibilidad de obtener múltiples plantillas biométricas seguras a partir de los mismos datos biométricos originales.
3. Rendimiento biométrico: Consiste en la capacidad del modelo de mantener el rendimiento del proceso de reconocimiento en términos de tasas de falsos aceptados y tasas de falsos rechazos.

La presente investigación se enmarca en aumentar la seguridad criptográfica de los datos biométricos y facilitar la revocabilidad de los datos protegidos. La propiedad de ser no invertible el proceso de cifrado y la selección de características identificativas, invariantes a rotación y traslación, son dos características de impacto en la investigación. La propiedad de ser no invertible el proceso de cifrado garantiza altos niveles de seguridad. La selección de características identificativas invariantes a rotación y traslación, resistentes a la deformación no lineal y a la superposición parcial constituye una ventaja para el proceso de comparación de características en el dominio cifrado. La selección

de estas características permite además el cifrado de toda la información, al eliminar la necesidad de almacenar datos de ayuda.

Los modelos de protección de plantillas de minucias propuestos en la bibliografía realizan el cifrado de los datos biométricos de tres formas posibles:

1. Cifrando directamente el conjunto desordenado de minucias.
2. Cifrando el conjunto de características biométricas desordenadas derivadas del conjunto de características originales.
3. Cifrando un vector de longitud fija derivado de las características originales.

Para los casos de los conjuntos desordenados han sido propuestos diferentes modelos de protección entre los que se encuentran la bóveda difusa y las plantillas cancelables. El caso del vector de longitud fija puede ser asegurado utilizando los modelos hash biométrico y compromiso difuso.

Los modelos de protección de plantillas biométricas, han sido clasificados por varios autores [22]–[26] según su funcionamiento en: cripto-sistemas biométricos y transformación de plantillas no invertibles como se muestra en la figura 1.1.

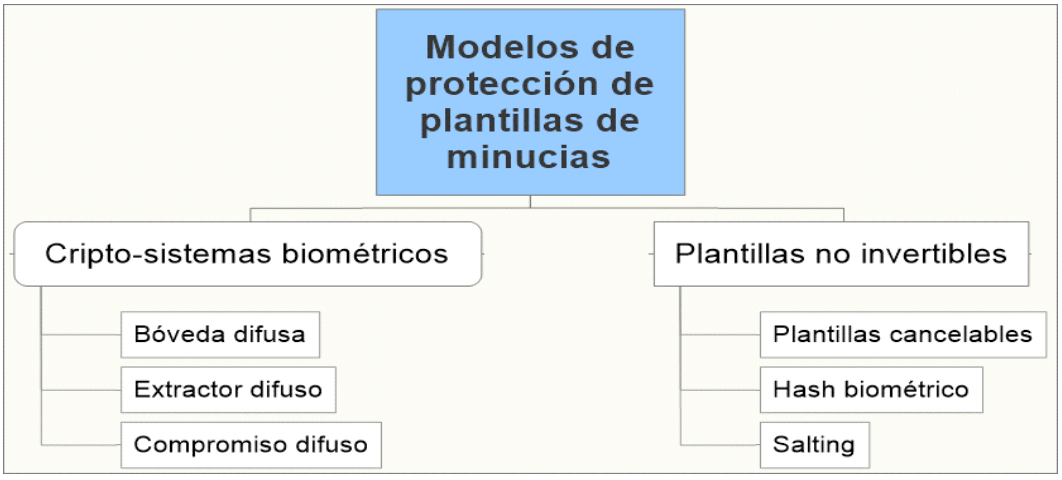


Figura 1.1: Clasificación de los modelos de protección de plantillas de minucias.

1. Cripto-sistemas biométricos: se genera un esquema seguro junto a una llave asociada, a partir de la plantilla biométrica original. Estos datos son almacenados en lugar de la plantilla biométrica original. Al realizar el proceso de verificación o identificación es posible comparar ambos esquemas seguros y determinar por su grado de similitud si pertenecen a una misma persona. Este mecanismo no solo cifra la plantilla biométrica, sino que también facilita la administración de las llaves.
2. Plantillas no invertibles: transforma una plantilla biométrica utilizando una llave específica. Para ello son utilizadas funciones no invertibles, garantizando de esta manera la seguridad criptográfica. El proceso de comparación es realizado en el dominio protegido, de esta manera disminuyen las posibilidades de filtrar información sensible.

En la presente investigación se analizaran los modelos de bóveda difusa, extractor difuso, plantillas cancelables y hash biométrico debido a que fueron formulados específicamente para la protección de datos biométricos de huellas dactilares.

1.3 Modelos de protección de plantillas de minucias

Los modelos de protección de plantillas de minucias [27] basan su funcionamiento en la transformación de los datos, el enmascaramiento de los datos originales o la combinación de ambos [7]. En el caso de los cripto-sistemas biométricos se han desarrollado dos enfoques principales, modelos de generación de llaves criptográficas y los modelos de asociación de llaves. El principal objetivo en ambos casos es disminuir las probabilidades de obtener parcial o totalmente las plantillas de minucias en ataques realizados a sistemas

automatizados de identificación mediante huellas dactilares al mismo tiempo que se facilita la comparación en el dominio protegido.

Los modelos que se resumen a continuación constituyen la base criptográfica del proceso de protección de plantillas de minucias de huellas dactilares.

1.3.1 Modelo de bóveda difusa

Este modelo es una construcción criptográfica basada en el compromiso difuso propuesto en [28], es un cripto-sistema biométrico diseñado para realizar el cifrado de conjuntos desordenados. El modelo de bóveda difusa descrito por primera vez en [11] fue concebido como una forma de cifrado tolerante a errores. El método de codificación y decodificación se basa en el problema descrito en [11]. A continuación se enuncia de manera breve el problema:

Alice desea cifrar con un secreto *k* en un conjunto A de elementos que pertenece a un universo público U, para ello selecciona un polinomio *p* de manera tal que pueda ser evaluado cada elemento de *k* como los coeficientes de *p* obteniendo el conjunto cifrado c. Adicionalmente crea un conjunto de elementos basura b y los mezcla con el conjunto cifrado c.

Para obtener el secreto k se utiliza un conjunto de elementos B, se realiza la interpolación polinomial de los elementos cifrados y el conjunto B. De esta manera si ambos conjuntos de elementos se superponen entonces puede ser recuperado el secreto k y los elementos protegidos. Para acercar el resultado de la interpolación polinomial a los datos originales se utiliza un código de corrección de errores. En la bibliografía se observa que el más utilizado es el propuesto por Red-Solomon [29]. Como resultado es posible reconstruir p y k de manera exacta.

El modelo propuesto en [11] está compuesto por dos métodos. Un método de codificación y un método de decodificación de la bóveda difusa como se muestra un la figura 1.2.

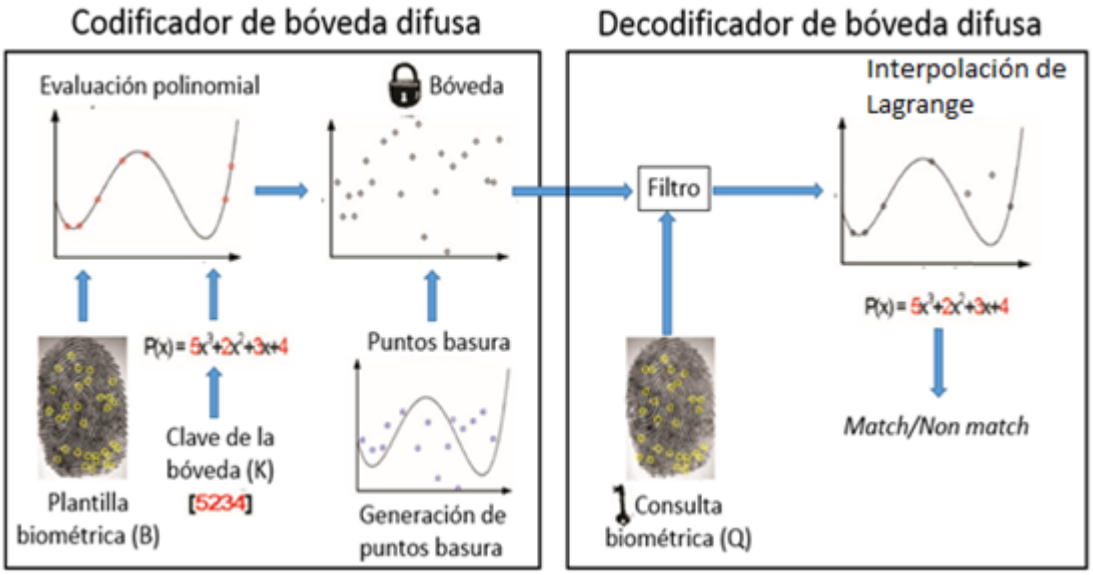


Figura 1.2: esquema de codificación y decodificación del método bóveda difusa.

El procedimiento realizado para codificar los datos biométricos [11] es crear una palabra de código Reed-Solomon generalizada que representa el secreto *κ* (junto al polinomio correspondiente *p* donde *k* representa los coeficientes del polinomio). Se evalúan las coordenadas *x* correspondientes al conjunto de datos originales *A* en *p* ← *k*. Para ocultar el resultado de esta operación se genera un conjunto de puntos basura o puntos de burla de la forma (*x, y*) y se mezclan aleatoriamente. Como premisa en la generación de los puntos basura se tiene que, deben ser seleccionados de manera tal que no se intercepten en el conjunto *A* ni en el polinomio *p*.

El procedimiento para decodificar los datos contenidos en la bóveda difusa tiene como entrada el conjunto de muestra *B* junto a la bóveda *Va* y consiste en determinar la palabra de código que codifica el secreto *k*. Se realiza k' ← p

(procedimiento inverso al cifrado) para denotar la conversión de un polinomio a lo sumo de grado k en el secreto f^k. Se denota $(x_i, y_i) \xleftarrow{(b_i, o)} R$ como la proyección del conjunto cifrado *R* en la coordenada *x* (b_i). Si se encuentra un par (b_i, y) que pertenece al conjunto *R* para cualquier valor de *y,* entonces (b_i, y) = (*x, y*), sino es asignado *null* al punto (*x, y*). De ser exitoso este proceso se obtiene como resultado el secreto *k'* el cual debe ser igual al original si el conjunto de prueba *B* es parecido al conjunto original *A*.

La seguridad criptográfica de este modelo según varios autores [9], [16], [30]–[32] está basada en la dificultad computacional de resolver el problema de la reconstrucción del polinomio y en la cantidad de puntos basura que sean añadidos para enmascarar los puntos originales. A este modelo es posible realizarle varios de ataques expuestos en [9], [16], [33] y que serán analizados en el epígrafe 1.5.

Otros enfoques del modelo de bóveda difusa han sido propuestos para diferentes aplicaciones en específico [34] o para añadir el proceso de alineación de los datos biométricos [12], [35]–[37]. Los principales cambios realizados al modelo original están en la utilización de un polinomio de grado mayor para la generación de los puntos basura, la inclusión de estructuras topológicas, la selección de un punto focal, del punto de máxima curvatura y el cálculo de un hash geométrico para realizar el proceso de alienación.

1.3.2 Modelo extractor difuso.

El modelo denominado extractor difuso es una construcción criptográfica que habilita dos entradas y realiza la comparación en el dominio protegido. Varios autores [38], [39] explican en detalles el proceso y el objetivo principal de este

modelo. La idea principal del modelo de cifrado es generar una llave criptográfica partiendo de un conjunto de datos de ayuda para garantizar una autenticación segura y confiable.

El modelo extractor difuso se separa en dos procesos, la generación del esquema seguro y el extractor difuso en sí. La generación del esquema seguro está compuesta por dos procedimientos denominados generación del esquema y recuperación. La generación de estos procedimientos se realiza a partir de un espacio M con una función de distancia dis bajo dos propiedades esenciales:

- La generación del esquema toma como entrada $w \in M$ y como salida brinda una cadena de bits representada como s.
- El procedimiento de recuperación toma como entrada un elemento $i \in M$ y la cadena de caracteres, además si $dis(w, i) \leq t$ entonces $recuperación\big(i, esquema\ seguro(w)\big) = w$.

El segundo proceso, extractor difuso, es definido como un par de procedimientos aleatorios denominados generación (g) y reproducción (r). En este proceso se cumplen dos propiedades esenciales:

- El procedimiento de generación recibe como entrada una contraseña (w) y extrae una cadena de bits b junto a una cadena de ayuda d.
- El procedimiento de reproducción recibe como entrada un elemento de la contraseña o palabra clave $(i \in M)$ y una cadena de bits d. Este procedimiento verifica si $dis(w, i) \leq t$, siendo t el umbral definido, y si (b, d) fueron generados por el procedimiento de generación mediante el uso de la palabra clave w.

La eficiencia de este modelo puede ser medida por el tiempo de ejecución de los procedimientos de generación y recuperación. Si ambos son realizados en tiempo polinómico puede decirse que es un esquema eficiente. El propósito fundamental de este modelo es realizar el cifrado de datos biométricos de huellas dactilares, pero también puede ser utilizado en otros tipos de datos biométricos como el iris o el rostro.

Inicialmente el modelo extractor difuso fue diseñado para la generación de llaves de cifrado y no abordaba directamente la privacidad de las plantillas de minucias. Este modelo almacena un conjunto de datos de ayuda para realizar la reconstrucción de la plantilla de minucias original. En [40] se destaca que al conocerse el esquema seguro es posible obtenerse parcialmente la plantilla de minucias. Este esquema solo es aplicable al proceso de verificación de identidad y no al proceso de identificación debido a que cada usuario tiene un esquema de seguridad en específico.

1.3.3 Modelo de plantillas cancelables

Este modelo consiste en una intencionada y repetida distorsión de la señal biométrica basada en una transformación [13]. La transformación tiene como propiedad fundamental que no es posible invertir los datos. Este tipo de transformación puede ser aplicada tanto en el dominio de la señal como a las características extraídas del rasgo biométrico. Las transformaciones en el dominio de la señal se realizan directamente en la imagen como se muestra en la figura 1.3.

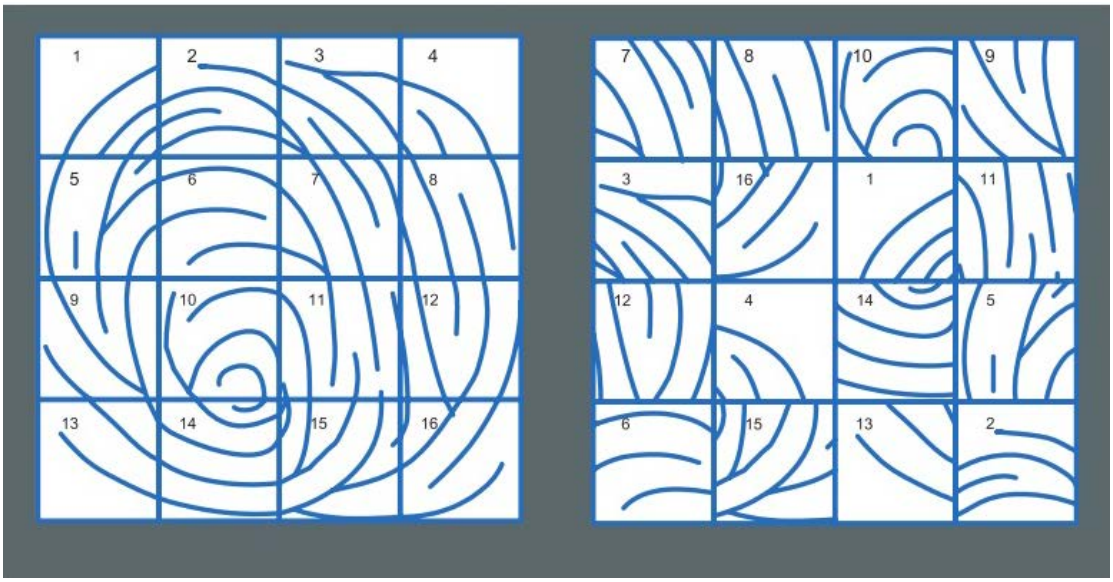


Figura 1.3: Transformaciones no invertibles aplicadas a la imagen. Tomado de [13]

Las transformaciones realizadas a las características extraídas del rasgo biométrico se realizan sobre las plantillas biométricas (plantillas de minucias en el dominio de la investigación) y tienen la forma:

$$S = \{(x_i, y_i, \sigma_i), i = 1 \dots, M\}.$$

Donde S representa la plantilla cifrada, x_i, y_i, σ_i representan las coordenadas y el ángulo de cada minucia perteneciente a la plantilla en texto claro y M representa la cantidad de minucias en la plantilla en texto claro.

El procedimiento para realizar la transformación propuesto en [13] consiste en el mapeo de *S* en *S'* de manera tal que no pueda ser recuperado *S* a partir de *S'*. La función utilizada para mapear las características biométricas tiene la propiedad de uno a muchos y pueden ser utilizadas varias funciones para realizar la transformación de las componentes de una minucia (x, y, σ).

En [41]–[45] se describen otros enfoques del modelo plantillas cancelables para la protección de plantillas de minucias de huellas dactilares. En esto enfoques

se realiza el análisis en el dominio de las características extraídas y no en el dominio de la señal. Para el cifrado de las características se utiliza una función de un solo sentido o función no invertible con la propiedad de uno a muchos.

Un hecho importante a destacar en estos enfoques es que se describen 3 tipos de transformaciones para realizar el cifrado de los datos, las transformaciones cartesianas, polares y funcionales. La transformación cartesiana mapea las minucias en coordenadas rectangulares utilizando como referencia uno de los puntos singulares, orienta el eje x en la misma dirección que la singularidad y divide el área rectangular en celdas o sub áreas de tamaño fijo. Esta transformación consiste en el cambio de celda de las minucias y pueden realizarse rotaciones en múltiplos de 90 grados después de transformada. El mapeo de las celdas se realiza a partir de una matriz de mapeo *M* por lo que el proceso puede denotarse como *C'* = *CM*, donde *C'* es el conjunto transformado y *C* es el conjunto original.

La transformación radial o polar consiste en el mapeo de las minucias originales en el espacio de coordenadas polares con referencia a la singularidad núcleo. Para realizar el mapeo de las minucias se divide el espacio en sectores polares y se cambian las minucias de sector para alterar las componentes de cada minucia (coordenadas (x, y) y ángulo σ). El mapeo es realizado teniendo en cuenta la llave de traslación $1 \times LS$ donde L es la cantidad de niveles y S representa el ángulo. La función de transformación puede describirse como

$$C' = C + M. \quad (1.1)$$

La transformación funcional consiste en la evaluación de las minucias en una función paramétrica, suavizada localmente pero no globalmente, que se rige por una clave. La función tiene 3 restricciones que a continuación se detallan:

1. La transformación debe ser suavizada localmente. Esto asegura que pequeños cambios en la posición de las minucias antes de realizar la transformación conduzca a pequeños cambios en la posición de los datos transformados.
2. La transformación no debe ser suavizada globalmente. Esto asegura que los datos originales y transformados no estén altamente correlacionados, para asegurar la seguridad criptográfica del modelo.
3. La transformación de los datos debe garantizar que la distancia entre los datos originales y los transformados sea mayor que la aceptada por el algoritmo de comparación.

El proceso de codificación utilizando plantillas cancelables es realizado en cada autenticación y en cada enrolamiento en el sistema biométrico. Si una plantilla protegida es comprometida es posible cambiar la función de transformación para generar una nueva plantilla a partir de los datos biométricos del usuario. De esta manera, aunque se conozca la plantilla protegida y la función de transformación, los datos biométricos originales no pueden ser recuperados. En la figura 1.4 se representan los tres tipos de transformaciones.

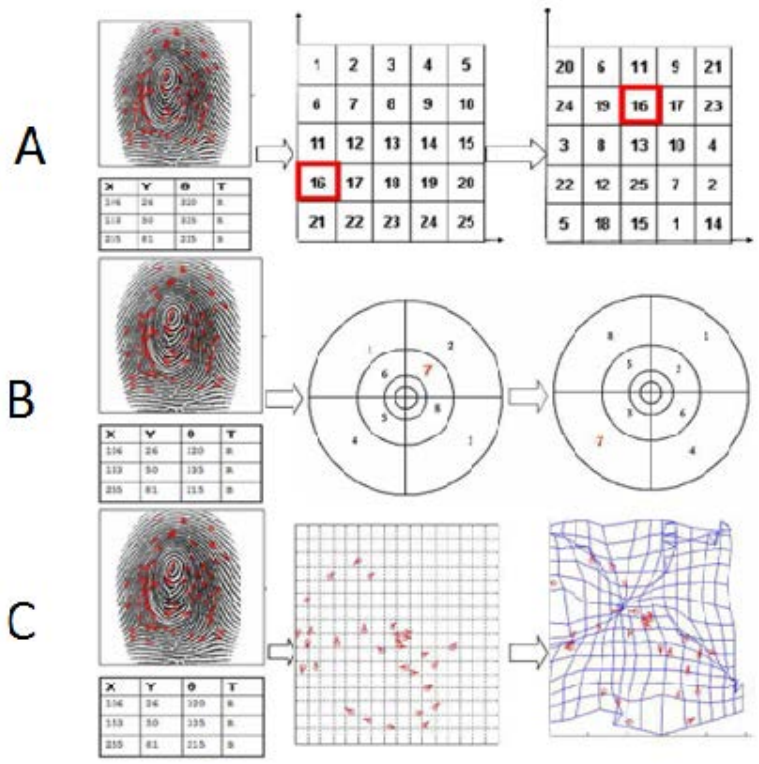


Figura 1.4: métodos de transformación cartesiana (A), polares (B) y funcionales (C). Tomado de [41]***.***

Otros enfoques de este modelo han sido propuestos para mejorar el proceso de alineación de las plantillas protegidas. En [43] se describe un enfoque libre de alineación en el cual se extraen un conjunto de características identificativas que provienen de las minucias, invariantes a rotación y traslación. Para proteger los datos se utiliza una transformación no invertible de tipo funcional. En [44] se describe el proceso de cifrado utilizando una transformación no invertible del tipo cartesiana. El proceso de alineación en este enfoque se realiza extendiendo el método de alineación mediante la selección de una minucia de referencia. En este caso particular se seleccionan una a una las minucias como referencia y se conforma un vector binario con las relaciones entre la minucia de referencia y las demás. En [46] se describe otro enfoque del método plantillas cancelables

libre de alineación. La transformación seleccionada para el cifrado de los datos es la transformación cartesiana. En este caso se realiza el cifrado de un conjunto de características identificativas extraídas de las minucias, invariantes a rotación y traslación propuestas en [47].

El modelo de plantillas cancelables y los enfoques analizados presentan como principal problema que basan la alineación en la selección de una característica que puede o no estar presente o puede ser mal seleccionada. Esto conllevaría a una pérdida significativa del rendimiento biométrico.

1.3.4 Modelo hash biométrico

Este modelo consiste en la representación y transformación de un conjunto de datos extraídos de las minucias a partir de un punto de referencia, utilizando la técnica de extracción propuesta en [48]. Este modelo es aplicado exclusivamente a características de textura de la huella dactilar y consta de un método de representación y un método de filtrado. El método de representación de la información utilizado es denominado *FingerCode* el cual consta de 3 pasos fundamentales:

1. Determinar el marco de referencia en la imagen de la huella dactilar.
2. Filtrar la imagen en 8 direcciones diferentes utilizando el banco de filtros de Gabor.
3. Calcular la desviación estándar de los valores de grises en sectores alrededor del punto de referencia.

El filtrado de las características genera un conjunto de discos que contienen la información a ser filtrada para formar un vector de características de longitud fija que representa el hash biométrico de la huella dactilar bajo análisis. El cálculo

de la desviación estándar en estos filtros define los componentes del vector de características de longitud fija. En [49] se describe un enfoque de este método mediante el cual se descompone el modelo en dos componentes, en una transformación integral, invariable y discriminativa de los datos de huellas dactilares con un moderado grado de tolerancia y en la discretización de los datos a través de un producto interno de números aleatorios y datos del usuario. En este enfoque se utiliza el *framework* de transformación de Fourier-Mellin que contiene un conjunto de mejoras en el procesamiento de la imagen. Entre ellas se pueden mencionar la preservación de bordes locales y la reducción de ruido. En vez de utilizar el banco de filtros de Gabor se utiliza la transformada de Fourier para calcular los discos que representan los niveles de grises.

En [50] se describe otro enfoque del modelo de protección denominado hash biométrico. El principal aporte, en relación con descrito en [49], es la eliminación de la dependencia del núcleo de la huella dactilar como punto de referencia. En este caso se representa cada minucia por su *FingerCode* y para realizar la protección de cada *FingerCode* se realiza el proceso de formación del hash biométrico.

En [50] se utilizan los filtros de Gabor para filtrar la región de interés y a diferencia del método original esta no se normaliza. En la figura 1.5 se representa el proceso de obtención del hash biométrico.

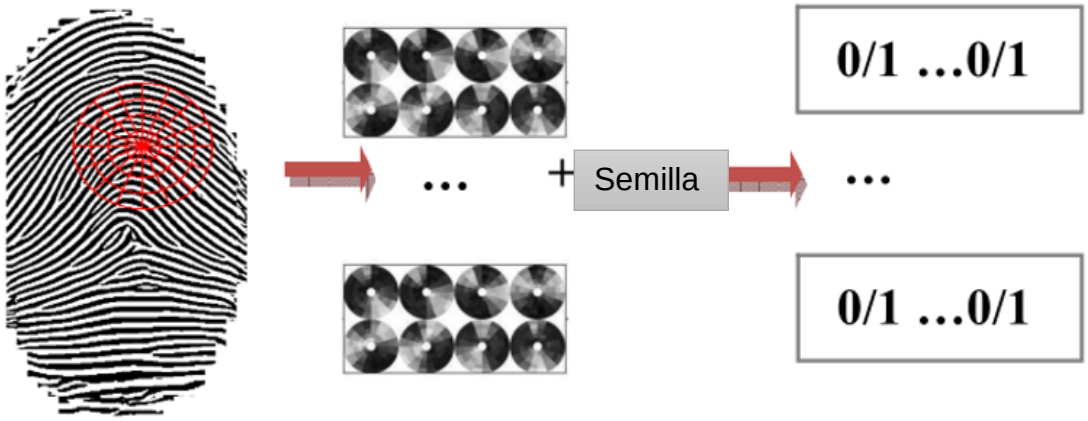


Figura 1.5: representación del hash biométrico. Adaptado de [50]

En [51] se describe otro enfoque para la obtención del hash biométrico. En este trabajo se proponen dos descriptores, un descriptor basado en textura para capturar el patrón de flujo de crestas y otro descriptor basado en minucias para la relación de cada minucia con su vecindad. La extracción de características se realiza de manera similar a lo propuesto por [50], la variación reside en la utilización de la estructura k-vecindades (*K-Plet*) con centro en la minucia en análisis para el descriptor basado en minucia. Este permite la representación local de la información entre minucias y es seleccionado para verificar si la comparación del descriptor basado en textura es consistente a nivel global. Para minimizar el impacto de los cambios en las minucias que conforman la estructura *K-Plet* se realiza la comparación de las estructuras utilizando una técnica de alineación propuesta.

Para realizar el proceso de selección de minucias válidas, el autor de este modelo propone tener en cuenta que la minucia esté circundante al área de interés. Para validar cada minucia se define que, la minucia se encuentre en el límite de la imagen y cada sector se encuentre representado por valles y crestas

alternativamente. El proceso de protección comienza con la representación del *MinuCode* de cada minucia seleccionada como válida, se normaliza cada *MinuCode* en el rango [-1, 1], se genera una matriz aleatoria *M* y se aplica el método de Graham-Smith para convertir la matriz en conjuntos orto normales. Luego se realiza la proyección de cada *MinuCode* en la matriz, se binariza el resultado, se eliminan los *MinuCode* y se almacenan los *BioCode.*

A todos los enfoques analizados del modelo hash biométrico resumidos en el anexo 2 se le pueden realizar un conjunto de ataques que serán expuestos en el epígrafe 1.5 mediante los cuales es posible obtener las plantillas de minucias en texto plano.

Los modelos de protección de plantillas de minucias de huellas dactilares analizados en este epígrafe realizan la protección de los datos biométricos mediante la transformación de los datos utilizando diferentes estrategias matemáticas. En los casos de la bóveda difusa y las plantillas cancelabes, especificamente la transformación funcional, realizan la transformación de los datos utilizando una función de transformación y una llave. La salida de estos modelos es un vector de características transformado de longitud variable. Como principal ventaja se tiene que teóricamente estas transformaciones son no invertibles sin embargo, como se describe en el acápite 1.5 existen vulerabilidades en la fundamentación teórica de ambos modelos que permiten la obtención de las minucias en texto claro.

En el caso del extractor difuso es un modelo de generación de llaves biométricas que permite realizar el cifrado de las características. La salida de este modelo es un vector de características de longitud variable. Este modelo de cifrado

constituye el punto de partida para la formulación de ataques a la bóveda difusa y a las plantillas cancelables.

El hash biométrico realiza la transformación basado en las características de textura de la huella dactilar. Este modelo de protección utiliza una llave de cifrado para combinar con las características extraídas y obtener el texto cifrado. La salida de este es una cadena binaria de tamaño fijo que caracteriza la huella dactilar.

La revocabilidad en todos los modelos es difícil de alcanzar según varios autores [7], [16], [41], [50], [52]. En los modelos de plantillas cancelables y bóveda difusa se plantea la necesidad de cambiar la función de cifrado. En los modelos extractor difuso y hash biométrico se plantea la necesidad de cambiar la llave de cifrado. Como principal deficiencia detectada en la bibliografía consultada es que no se hace referencia, en ninguno de los modelos, al proceso de generación de llaves utilizado, ni al procedimiento a seguir para cambiar la función de cifrado, solo se menciona que es necesario realizarlo.

1.4 Alineación de plantillas de minucias de huellas dactilares

El proceso de alineación de plantillas de minucias es considerado un reto [22], [53] debido principalmente a que no se cuenta con las características originales. La comparación en el dominio cifrado se realiza con datos transformados por un método de cifrado. La dificultad reside en el cambio que se produce en la posición y el ángulo de las minucias que, al no tener la plantilla original, es difícil detectar cuáles minucias coinciden y cuáles se adicionan en el proceso de captura de la huella dactilar.

Para realizar la alineación de plantillas de minucias, antes de realizar el cifrado, se han propuesto varios métodos entre los que se destacan:

- la detección de las singularidades de la huella dactilar [1].
- la detección de un punto focal [22].
- la selección de una minucia de referencia [44].
- el cálculo del punto iterativo más cercano [36], [53], [54].
- la formación de estructuras topológicas [35], [37], [47].

Los métodos anteriormente señalados realizan el proceso de alineación sin embargo, presentan un conjunto de limitaciones que afectan el rendimiento biométrico de los modelos de protección de plantilla de minucias que lo utilizan. La ausencia de las singularidades (núcleo y delta) en imágenes de huellas dactilares imposibilita la utilización del modelo de alineación utilizando las singularidades de la huella dactilar.

Durante el proceso de selección del punto focal o la minucia de referencia la ocurrencia de un mínimo cambio o error conlleva a una errónea selección y por consiguiente a una pérdida significativa en el rendimiento biométrico. La inclusión o eliminación de minucias durante el proceso de captura y extracción provocan inestabilidad en las estructuras topológicas que se forman para la alineación, además, el almacenamiento de algunas estructuras como datos de ayuda para el proceso de alineación puede ser utilizado para correlacionar dos plantillas de minucias.

Algunos enfoques de modelos de protección utilizan un conjunto de características extraídas de las estructuras topológicas para realizar el proceso de cifrado libre de alineación. En este caso persiste el problema del cambio de

las minucias entre dos extracciones de un mismo rasgo biométrico, lo que degrada el rendimiento biométrico.

1.5 Principales ataques a modelos de protección de plantillas de minucias de huellas dactilares.

La seguridad criptográfica de los modelos para la protección de plantillas de minucias de huellas dactilares es un aspecto clave a tener en cuenta. En la arquitectura general de un sistema de identificación de personas mediante huellas dactilares han sido detectados ocho puntos mediante las cuales es posible realizar ataques y comprometer el correcto funcionamiento del sistema. Entre estos puntos principales de vulnerabilidad se encuentran [18], [55]:

- la reescritura de los módulos de extracción y comparación de características.
- la manipulación directa de las plantillas en la base de datos.

Estos dos ejemplos podrían facilitar la obtención de las características originales o la inserción de plantillas de minucias falsas en el sistema.

Los modelos de protección de plantillas de minucias realizan el cifrado de los datos para garantizar su seguridad criptográfica sin embargo, varios ataques han sido propuestos [9], [14]–[16], [18], [56]–[58] para obtener, de manera total o parcial, las minucias en texto claro.

Existen más ataques que afectan el buen funcionamiento de un sistema de autenticación biométrica [59] sin embargo, la presente investigación se centra en los ataques realizados a las plantillas protegidas para obtener las minucias en texto claro o burlar la seguridad del sistema. La razón principal reside en que las plantillas de minucias en texto claro no son revocables y una vez

comprometida su seguridad conllevan a la pérdida del identificador biométrico. Los principales ataques se muestran en la figura del anexo 1 y son:

1. Ataque vía multiplicidad de valores: ataque de correlación y ataque de comparación cruzada.
2. Ataque por inversión de llave encubierta.
3. Ataque de sustitución mezclada.
4. Ataque de fuerza bruta: Ataque de falso aceptado.
5. Ataque de enmascaramiento.
6. Ataque de pre-imagen al hash biométrico.

Los ataques vía multiplicidad de valores definidos en [9] consisten en la recopilación de varias plantillas por parte del atacante con el objetivo de compararlas y obtener las características que se mantienen constantes (Minucias reales). En el peor de los casos, utilizando esta técnica, es posible obtener la plantilla real X y la clave K. Al obtener dos o más plantillas de minucias protegidas utilizando el modelo de bóveda difusa y generada a partir del mismo rasgo biométrico, con llaves de encriptación iguales o diferentes, el atacante puede correlacionar los datos biométricos y obtener parcial o totalmente las minucias originales [16].

Existe la probabilidad de que el atacante obtenga algunos puntos basura como reales. Esto se debe a que algunos puntos basura pueden coincidir con los reales a pesar de ser generados de manera aleatoria. En [60] se describe el proceso de correlación de plantillas de minucias y se concluye que, es posible obtener los datos originales en un 59% de los datos analizados.

En el caso del modelo de plantillas cancelables en [14] se detalla un proceso para obtener las características originales a partir de dos o más plantillas protegidas mediante este tipo de ataque. Debido a la propiedad uno a muchos que presentan las funciones de cifrado, es posible encontrar varias soluciones inversas por cada minucia a partir de una plantilla cifrada.

Todas las soluciones posibles pueden ser tratadas como valor difuso, tomando algunas características como puntos basuras y otras como puntos originales. De esta manera si el atacante obtiene otra plantilla cifrada a partir de la misma plantilla original puede obtener las minucias reales realizando el ataque vía multiplicidad de valores al comparar ambas plantillas. Cuando se obtiene una sola solución pueden revelarse el 90.2 por ciento de los datos originales.

Los ataques de comparación cruzada y de correlación son tipos específicos de los ataques vía multiplicidad de valores realizados al modelo de bóveda difusa y de plantillas cancelables. Los ataques de comparación cruzada pueden realizarse teniendo como mínimo dos plantillas protegidas. Este tipo de ataque se utiliza en primer lugar para conocer si dos plantillas protegidas pertenecen al mismo rasgo biométrico y en segundo lugar para obtener tanto las características originales como la llave o polinomio de cifrado, o alguna de estas dos. Esta última es la más eficiente debido a que puede desbloquear una bóveda con otra, obteniendo las características originales y la llave de cifrado. En el caso de saber si dos plantillas pertenecen al mismo rasgo puede realizarse solo con los datos de ayuda almacenados para el proceso de alineación.

Los ataques de correlación [16] consisten en obtener el conjunto de pares de puntos presentes en ambas plantillas que comparan entre sí. Para ello se

auxilian de una función de medición de distancia entre dos puntos que son considerados puntos que comparan entre sí, buscan puntos que sean vecinos a estos y compartan esta medida.

El cálculo de una medida de distancia razonable o apropiada es una premisa necesaria para el éxito de esta técnica y se describe en detalle en [16]. Una vez lograda la decodificación de los puntos genuinos, que interpolados dan como resultado el polinomio y las características originales, se termina el ataque de manera satisfactoria. Los ataques de correlación y comparación cruzadas pueden realizarse en conjunto. Un ejemplo de ello es el ataque a dos bases de datos que contengan usuarios en común para obtener las plantillas protegidas de ambos y a partir de ellas los datos en texto claro.

Los ataques por repetición de llave encubierta [9], [61] tienen como objetivo obtener una llave de encriptación válida. El modelo de bóveda difusa propone la liberación de la clave de cifrado en cada intento de comparación que sea positivo, lo que constituye una vulnerabilidad explotada por este tipo de ataque. En este caso el atacante puede decodificar la plantilla protegida y obtener los datos biométricos originales o codificar un conjunto de datos biométricos.

Los ataques de sustitución mezclada [9] se realizan mediante la alteración del registro biométrico con o sin conocimiento de los datos biométricos almacenados en la plantilla protegida. Este tipo de ataque niega el servicio de autenticación al usuario genuino mientras asegura la autenticación del impostor. Otro enfoque describe la combinación de los datos biométricos del atacante con los del usuario genuino. Este enfoque es conocido como mezcla interna y es mucho más difícil de detectar debido a que no provoca la denegación del servicio de autenticación.

Los ataques de fuerza bruta se realizan mediante la generación de todas las posibles combinaciones de muestras para revelar la auténtica. En [16] se implementaron varios enfoques del método de protección bóveda difusa para realizar ataques de fuerza bruta. El ataque de fuerza bruta clásico se realiza enviando al sistema una bóveda *V* que contiene un conjunto de puntos y un polinomio *p* de grado *k* generados aleatoriamente. El ataque termina cuando se satisface el criterio establecido para encontrar el polinomio correcto. El criterio utilizado consiste en comprobar cuántos puntos pertenecientes a la bóveda *V* son interpolados de manera correcta en cada intento de autenticación.

El ataque de falso aceptado es una mejora del ataque de fuerza bruta. Este ataque se realiza utilizando una base de datos de plantillas de minucias y una bóveda difusa que haya sido interceptada. Se realiza la interpolación de cada muestra en la base de datos y se comparan los resultados hasta satisfacer el criterio para encontrar el polinomio correcto descrito anteriormente. Este tipo de ataque requiere mucho más esfuerzo y se estima que la probabilidad de encontrar el polinomio correcto es de $1-(1-\epsilon)^n$. De conocerse el valor de la tasa de falso aceptado ϵ es posible realizar este ataque de una manera más sencilla.

El ataque de imagen previa descrito en [57] se realiza al modelo de hash biométrico. El objetivo principal es utilizar un algoritmo genético para obtener un aproximado de los estados intermedios *FingerCode* y *BioCode*, en la generación del hash biométrico. Para ello se describe como genotipo al candidato a *FingerCode* descrito como un vector de dimensión *m*.

Como población se escoge un conjunto de candidatos (10 000 en la investigación de referencia) caracterizados por su genotipo. Se describe una función de aptitud para cuantificar la aptitud de un individuo con su medio ambiente, teniendo en cuenta su genotipo. Por último, se describe un operador de genotipos para definir alteraciones en el genotipo utilizando tres operadores: mutación, selección y cruzamiento. Con este tipo de ataque es posible obtener una plantilla similar a la plantilla original bajo condiciones reales.

Los ataques descritos en la bibliografía para los modelos de protección de plantillas de minucias de huellas dactilares muestran que el requisito de seguridad criptográfica no se cumple debidamente. La obtención de las plantillas de minucias en texto claro constituye un riesgo para la seguridad de la información protegida biométricamente. En la tabla 1.1 se resumen los modelos y los ataques por los cuales son afectados.

Tabla1.1: Resumen de los ataques que afectan a cada modelo de protección.

Ataques	Bóveda difusa	Plantillas cancelables	Hash biométrico
Multiplicidad de valores	X	X	
Correlación	X	X	
Fuerza bruta	X	X	
Sustitución mezclada	X		
Imagen previa			X
Enmascaramiento	X	X	X
Repetición de llave encubierta	X	X	

1.6 Principales problemas y desafíos.

Entre los principales problemas y desafíos descritos por diferentes autores se encuentran la protección de los datos biométricos sin degradar el rendimiento del proceso de reconocimiento [10]. Los sistemas criptográficos clásicos (RSA, AES, entre otros) utilizan un conjunto de funciones que no son sensibles al cambio en los datos a cifrar. Un pequeño cambio en los datos de entrada provoca grandes cambios en los datos cifrados resultantes [10], [62]. En cada intento de autenticación, es necesario:

1. Descifrar las plantillas de minucias.
2. Realizar la comparación en texto plano.
3. Eliminar las plantillas en texto plano de la memoria.

Durante el proceso de autenticación las plantillas de minucias quedan expuestas a ataques. Esto constituye una vulnerabilidad debido a que pueden ser obtenidas utilizando un virus troyano o accediendo directamente a la memoria en este momento. Las variaciones intra-usuario que presenta las muestras dactilares traen como consecuencia que de 100 minucias que contiene una plantilla solo se correspondan satisfactoriamente de 12 a 15 minucias [1] con otra muestra del mismo identificador biométrico. Estas variaciones dificultan el proceso de reconocimiento en el dominio cifrado.

Conclusiones parciales

- El análisis de los modelos criptográficos de protección de plantillas de minucias de huellas dactilares posibilitó la detección de un conjunto de

vulnerabilidades que disminuyen la seguridad criptográfica de los datos protegidos.

- La caracterización del proceso de protección de plantillas de minucias facilitó la identificación de los principios fundamentales que debe cumplir cualquier modelo de protección de plantillas de minucias así como el estado actual del cumplimiento de cada uno de estos principios.
- El análisis de los métodos de alineación de plantillas de minucias que son utilizados en el proceso de protección permitió la selección de una estrategia libre de alineación mediante estructuras de minucias.
- La identificación de los ataques a los modelos de protección de plantillas de minucias de huellas dactilares proporcionó los elementos necesarios para la identificación de vulnerabilidades críticas en los modelos criptográficos actuales.

Capítulo II: Modelo para la protección de plantillas de minucias de huellas dactilares.

Capítulo II - Modelo para la protección de plantillas de minucias de huellas dactilares.

En el presente capítulo se analizan los modelos para la protección de plantillas de minucias de huellas dactilares que extraen un conjunto de características identificativas provenientes de las minucias y realizan el cifrado de los datos. Se propone un modelo para la protección de plantilla de minucias y una estructura para realizar la protección. Como parte de la investigación se desarrollan tres métodos: un método de representación y extracción de características identificativas, un método de cifrado de características identificativas y un método de comparación de características identificativas. El modelo de protección y el método de representación y extracción de características constituyen los principales aportes de la investigación.

2.1 Diagnóstico sobre la situación que presentan los modelos que realizan la protección de plantillas de minucias de huellas dactilares.

En la actualidad existen varias implementaciones de los modelos de protección de plantilla de minucias de huellas dactilares para un sistema automatizado de identificación de personas. Estos modelos están destinados a la investigación y se han implementado con el objetivo de realizar experimentaciones. Esto se debe a la afirmación realizada en [7], donde se asegura que aún no están listos para ser desplegados en un ambiente real. Las principales causas son las vulnerabilidades descritas en la bibliografía que comprometen la seguridad criptográfica de los modelos, la dificultad en varios casos de realizar la revocabilidad y la afectación del rendimiento biométrico durante el proceso de autenticación.

La mayoría de los sistemas de identificación mediante huellas dactilares en la actualidad realizan el proceso de reconocimiento en texto claro lo cual constituye una vulnerabilidad. Los sistemas que realizan la protección de los datos biométricos utilizan esquemas criptográficos clásicos y realizan el proceso de comparación bajo condiciones seguras y en ambientes controlados.

2.1.1 Modelos híbridos que realizan la protección de plantillas de minucias mediante estructuras topológicas.

Como parte de la investigación se realizó el análisis de la literatura especializada para identificar y analizar modelos para la protección de plantillas de minucias de huellas dactilares. Se efectuó un análisis comparativo para detectar insuficiencias y verificar en qué medida los modelos cubren aspectos relevantes sobre la protección de plantillas de minucias.

Para la comparación de plantillas de minucias protegidas fueron definidos un conjunto de atributos (o aspectos importantes a considerar) identificados en la literatura y ratificados por expertos. Los atributos son:

1. Alineación de plantillas de minucias.
2. Comparación en el dominio protegido.
3. Análisis global y local de la información contenida en las plantillas protegidas.

El estudio evidenció la necesidad de una herramienta que cumpla los requisitos de seguridad criptográfica, revocabilidad y rendimiento propuesto por varios investigadores destacados de dicha área del conocimiento. Existen dificultades para elegir y aplicar un modelo de protección, pues no se encuentran en la bibliografía métodos de comparación robustos que realicen el análisis de la

información de manera local y global. Otra limitación de los modelos pioneros es que no fueron consideradas las variaciones a las que está sujeta la toma de una huella dactilar.

Los modelos de protección de plantillas de minucias de huellas dactilares se clasifican en dos grupos, **los dependientes de un método para la alineación de los datos y los libres de alineación**. Los modelos que incluyen métodos de alienación [35], [36], [54] almacenan un conjunto de datos denominados datos de ayuda; esto constituye una vulnerabilidad debido a que quedan datos sin cifrar que pueden ser utilizados para realizar ataques de correlación. Los modelos libres de alineación realizan el cifrado de un conjunto de características provenientes de las minucias, invariantes a rotación, traslación y resistentes a deformación no lineal, cifrando toda la información disponible. La seguridad criptográfica en los modelos libres de alineación es mayor debido a que no dejan información sin cifrar. De esta manera resulta más complejo correlacionar diferentes plantillas de minucias protegidas pertenecientes al mismo rasgo biométrico. Por ello se decide realizar un estudio del estado del arte de los métodos de representación y extracción de características identificativas provenientes de las minucias.

Para realizar la representación y extracción de características invariantes a rotación y traslación, provenientes de las minucias, en [35] se proponen tres estructuras topológicas. De cada una de ellas se extrae un conjunto de datos provenientes de las minucias para realizar el proceso de cifrado utilizando los modelos de bóveda difusa, plantillas cancelables o hash biométrico. Estos modelos son los denominados modelos híbridos de protección de plantillas de minucias.

En [63] se describe un modelo de cifrado hibrido compuesto por un método de representación de la información contenida en las minucias y una transformación cartesiana. Para ello se extraen un conjunto de características identificativas provenientes de las minucias, invariantes a rotación, traslación y resistentes a deformación no lineal las cuales serán cifradas. El proceso de extracción comienza con la selección de tres minucias de la plantilla de minucias, a continuación, se forma un círculo donde las minucias se encuentran en el borde, se calcula el circuncentro de la tripleta y los ángulos formados entre cada vértice del triángulo y el circuncentro. El proceso de cifrado de las características identificativas consiste en el almacenamiento como se muestra en la figura 2.1 de:

1. las coordenadas del circuncentro $(x';y')$,
2. el ángulo mayor φ_{12}y su vecino o ángulo adyacente φ_{23}
3. los ángulos $\phi_1,\ \phi_2,\phi_3$
4. el tipo δ.

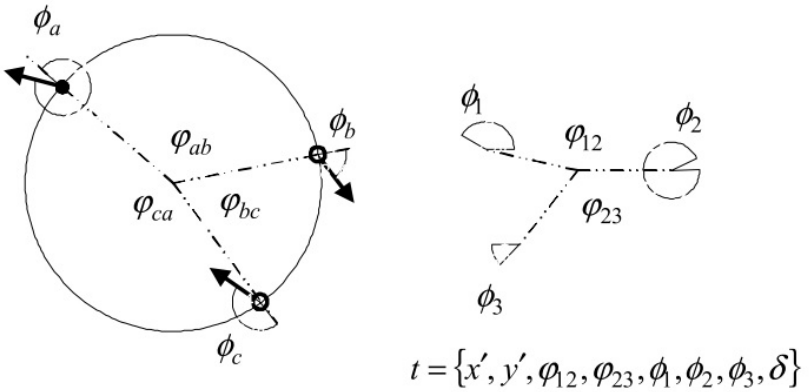


Figura 2.1: extracción de características identificativas a partir del centro. Tomado de [63]

Este modelo hereda las vulnerabilidades encontradas en el modelo de protección plantillas cancelables. La revocabilidad del modelo no queda

explicada de manera explícita al ser utilizada una transformación cartesiana para codificar los datos.

En [64] se describe un modelo de cifrado híbrido para datos biométricos de huellas dactilares. Este modelo está compuesto por una característica compleja, invariante a rotación y traslación y una variante de bóveda difusa. La característica propuesta en [64] se define como la relación entre dos minucias expresadas por la longitud de la recta que las separa, la diferencia de orientación de los ángulos de cada minucia y el ángulo formado por rectas paralelas a la dirección de las minucias.

Las relaciones entre minucias se determinan utilizando estructuras de n vecindades más cercanas, con n = 4. Se forma un vector de 4 dimensiones, invariante a rotación y traslación que es cifrado con el modelo de bóveda difusa y comparada por el algoritmo de comprobación de estructura jerárquica (HSC) propuesto en esta misma investigación.

Este modelo híbrido hereda las vulnerabilidades encontradas en el modelo de protección bóveda difusa. La revocabilidad del modelo recae en el cambio de la función de cifrado y el rendimiento, similar al rendimiento del modelo original. Al obtener las características transformadas es posible generar nuevas plantillas a partir de ella debido a que las características identificativas provenientes de las minucias comparten la propiedad de invariabilidad.

Otro modelo híbrido de protección planteado en [47] formula un método de representación y extracción de características identificativas a partir de tripletas de minucias de huellas dactilares. El proceso consta de 4 pasos:

1. Formulación de vecindades de minucias

2. Descomposición de las vecindades.
3. Extracción de características invariantes.
4. Protección de las plantillas.

La formulación de vecindades de minucias se realiza mediante la selección de las 3 minucias más cercanas (medida por la distancia euclidiana) a la minucia *m* que está siendo analizada. El proceso de descomposición de vecindades consiste en la formación de 4 tripletas de minucias, 3 formadas mediante la unión de la minucia *m* y dos vecindades y una formada por sus vecindades como se muestra en la figura 2.2:

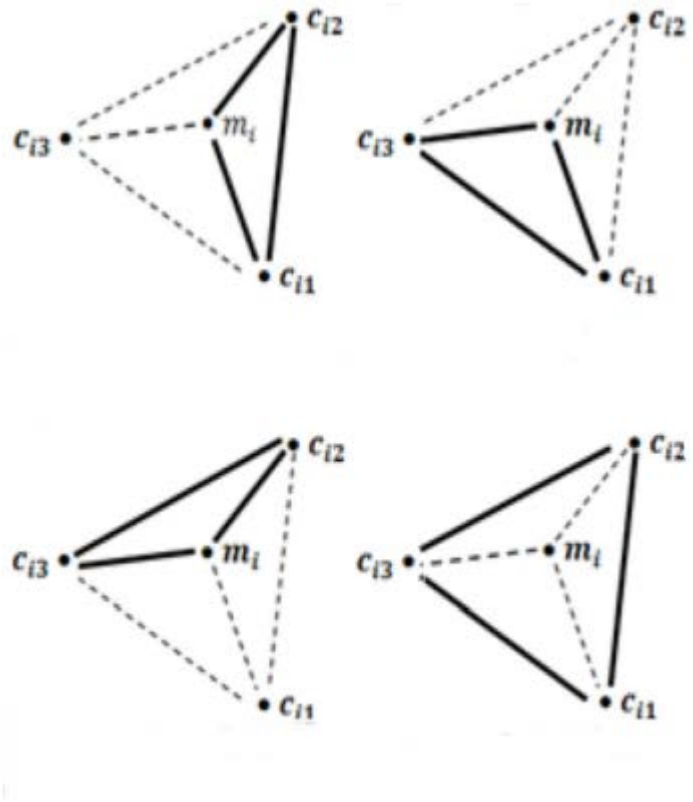


Figura 2.2: Estructuras triangulares de minucias. Tomado de [47]

En el proceso de extracción de características invariantes se extrae de cada tripleta la longitud de los lados, la amplitud de los ángulos internos y se calcula la diferencia entre las dos minucias adyacentes a cada lado. Con estas

características se forma el vector característico para realizar la codificación. El proceso de protección se realiza utilizando el esquema de hash biométrico propuesto en [8].

En [46] se describe un modelo hibrido de cifrado que utiliza un esquema de representación y extracción de características identificativas provenientes de las minucias y el modelo de plantillas cancelables. El proceso de comparación se realiza mediante el cotejo de todos los vectores de 9 dimensiones protegidos. Al modelo le han sido encontradas un conjunto de vulnerabilidades expuestas en [65]. La realización de ataques a estas vulnerabilidades permite la obtención de los datos originales a partir de los datos protegidos.

En [66] se describe un modelo híbrido de protección de plantillas de minucias. Este modelo propone un método de representación y extracción de características identificativas basado en la triangulación de Delaunay denominado cuadrángulo de Delaunay. En este enfoque se genera el diagrama de Voronoi asociado a una plantilla de minucias y se unen los centros de cada par de minucias vecinas para crear la red de Delaunay. Para formar los cuadrángulos de Delaunay se seleccionan dos triángulos que compartan un mismo lado.

Este enfoque registra la información local de las estructuras topológicas formadas y contiene un lado y un ángulo más que lo registrado en la triangulación de Delaunay. De esta manera se evita el registro de información global de la plantilla de minucias. Como principal ventaja sobre la triangulación de Delaunay este enfoque alcanza mayor robustez en cuanto a variación por distorsión no

lineal. Las características invariantes que son seleccionadas en este método son:

1. La longitud de los lados.
2. Los ángulos formados entre una la dirección de cada minucia y el lado correspondiente a su vecina en dirección a las manecillas del reloj.
3. Los ángulos entre dos lados.
4. El tipo de cada minucia.

Cada vector extraído de un cuadrángulo de Delaunay es cuantizado en una cadena binaria corta y luego son concatenadas todas las cadenas en un único vector característico de longitud fija. Para aumentar la discriminatividad de esta estructura se obtiene una característica adicional de cada cuadrángulo de Delaunay. Este modelo híbrido de protección tiene todas las vulnerabilidades y limitaciones planteadas en el modelo de protección plantillas cancelables. La necesidad de registrar un punto central o punto de referencia es otra limitación que afecta el rendimiento del sistema.

En [67] se describe un método de representación y extracción de la información contenida en las plantillas de minucias, invariante a rotación y traslación denominada concha de minucias. El método propuesto consta de tres etapas:

1. La extracción de los puntos singulares núcleo y delta.
2. El cálculo de la distancia de cada minucia a las singularidades.
3. La construcción de la concha de minucias.

El cálculo de la distancia de cada minucia a las singularidades se realiza utilizando distancia euclidiana y la construcción de la concha*/curva* de minucias consiste en la construcción de triángulos rectos donde las distancias calculadas

son la hipotenusa del triángulo. Para construir el primer triángulo se genera aleatoriamente la distancia inicial d_0, esta constituye la llave privada de cada usuario.

Este método de representación tiene como principal dificultad en su formación la ausencia de puntos singulares en la clase arco y en algunas tomas de huellas dactilares. Este método no realiza cifrado alguno de las características extraídas de las minucias, almacenando la estructura y comparándola con cada estructura calculada en el proceso de autenticación. Este método no contempla el proceso de revocabilidad lo que constituye una limitación.

Los modelos y métodos de representación analizados en la bibliografía realizan la extracción de la información identificativa de las minucias y preparan los datos para el proceso de cifrado teniendo en cuenta la distorsión no lineal, la rotación y la traslación de los datos. Los esfuerzos en cada enfoque están destinados a resolver el problema de la alineación de las plantillas de las minucias y a aumentar la fortaleza del método en cuanto al cambio de minucias por inserción o eliminación en un conjunto con respecto al otro.

Como resultado del análisis realizado, se detectaron insuficiencias que atentan contra la seguridad criptográfica, la revocabilidad y el rendimiento de los modelos de protección de plantillas de minucias. Estas insuficiencias o limitaciones se presentan a continuación:

1. Los modelos híbridos heredan las vulnerabilidades de los modelos pioneros debido a que solo realizan una transformación inicial de los datos que no es revocable.

2. No se evidencia un enfoque que prediga, con cierto nivel de certeza, cuando una minucia que forma una estructura topológica.
3. La revocabilidad de las plantillas protegidas resulta compleja de lograr, en la mayoría de los casos es necesario cambiar la función de cifrado. Algunos de ellos no contemplan el proceso de revocabilidad lo que constituye una limitación.
4. Algunos modelos propuestos como modelos de cifrado son solo métodos de representación de la información contenida en las plantillas de minucias que carecen de revocabilidad.
5. La realización de ataques a vulnerabilidades en los modelos analizados permite la obtención de los datos originales a partir de los datos protegidos.
6. Algunos modelos presentan limitaciones en cuanto al campo de aplicación.

En la presente investigación se abordan estos inconvenientes para atenuarlos mediante el modelo propuesto. Las vulnerabilidades de los modelos híbridos se eliminan al utilizar una función de un solo sentido sin las restricciones que propone el modelo de plantillas cancelables y sin almacenar información en texto claro para el proceso de alineación. Se utiliza un enfoque de predicción a través de la extracción de los ángulos centrales en el componente método de representación y extracción de características y el cálculo de la probabilidad de ocurrencia en el componente método de comparación de características identificativas.

La revocabilidad de las plantillas protegidas se facilita al presentar un esquema de generación de llaves de cifrado y construir la función de cifrado a partir de él.

El modelo que se propone a continuación contiene dos etapas, una etapa de representación y extracción de características identificativas y una etapa de cifrado. Mediante estas etapas se selecciona un conjunto de características identificativas, invariantes a rotación y traslación y se transforman los datos utilizando una función. A continuación se presenta el modelo conceptual para la protección de plantillas de minucias de huellas dactilares que se elabora en la investigación para atenuar las insuficiencias encontradas en el diagnóstico bibliográfico realizado.

2.2 Modelo conceptual para la protección de plantillas de minucias de huellas dactilares

El término modelo proviene del italiano “modelo” que se refiere a la representación de algo que se debe seguir o imitar. Un modelo permite una comprensión más plena del objeto de estudio para resolver un problema y representarlo de alguna forma [68].

A continuación, se presenta el modelo teórico propuesto teniendo en cuenta sus principios, cualidades y componentes.

El objetivo del modelo es representar y transformar la información contenida en las plantillas de minucias de forma tal que sea complejo computacionalmente obtener la plantilla de minucias original a partir de los datos transformados y así contribuir a la autenticación segura de personas mediante huellas dactilares. Se integran los principales fundamentos teóricos establecidos en el capítulo 1 con las características, estado actual y desarrollo de la criptografía biométrica. El autor desarrolla un modelo que contribuye a aumentar la seguridad criptográfica

y facilitar la revocabilidad de los datos biométricos lo cual constituye una solución al problema de investigación identificado.

2.2.1 Principios, cualidades y componentes para el desarrollo del modelo de protección de plantillas de minucias de huellas dactilares.

Los **principios** que sustentan la construcción del modelo propuesto para la protección de plantillas de minucias de huellas dactilares son:

1. La **seguridad criptográfica** para certificar que las plantillas protegidas que sean obtenidas por un atacante no revelen información original y garantizar la seguridad de los datos biométricos.
2. La **revocabilidad** para permitir obtener más de una plantilla segura a partir de los mismos datos biométricos.
3. El **rendimiento biométrico** el cual es necesario para obtener resultados certeros en el proceso de autenticación biométrica.
4. La **interoperabilidad** para garantizar el uso de plantillas de minucias de otros sistemas automáticos de identificación de personas mediante huellas dactilares.
5. La **flexibilidad** lograda a partir de la selección de métodos de generación automática de llaves para el cifrado.

Las **cualidades** del modelo propuesto para la protección de plantillas de minucias de huellas dactilares son:

1. **Un nivel de protección de los datos compuesto:** que brinda al realizarse la representación y extracción de características identificativas provenientes de las minucias y cifrarse utilizando una función de transformación.

2. **El enfoque sistémico**: se evidencia a través de las interacciones del conjunto de componentes que brindan seguridad al proceso de reconocimiento biométrico.
3. **La amplitud**: brinda la capacidad de emplearse con diferentes enfoques en un sistema automatizado de identificación de huellas dactilares.
4. La **no invertibilidad** para asegurar que las plantillas solo puedan ser transformadas en un solo sentido, lo que disminuye las vulnerabilidades.
5. La **independencia funcional** del modelo lo que contribuye a su reutilización e implementación en cualquier sistema automatizado de identificación mediante huellas dactilares.

Las principales **componentes** del modelo son:

1. Componente: Método de representación y extracción de características identificativas.
2. Componente: Método de cifrado de características identificativas.
3. Componente: Método de comparación de características identificativas.

En la figura 2.3 se muestra la interrelación entre cada uno de estos componentes. En el epígrafe 2.3 se describe el funcionamiento de cada componente en el proceso de cifrado de las características identificativas de las huellas dactilares.

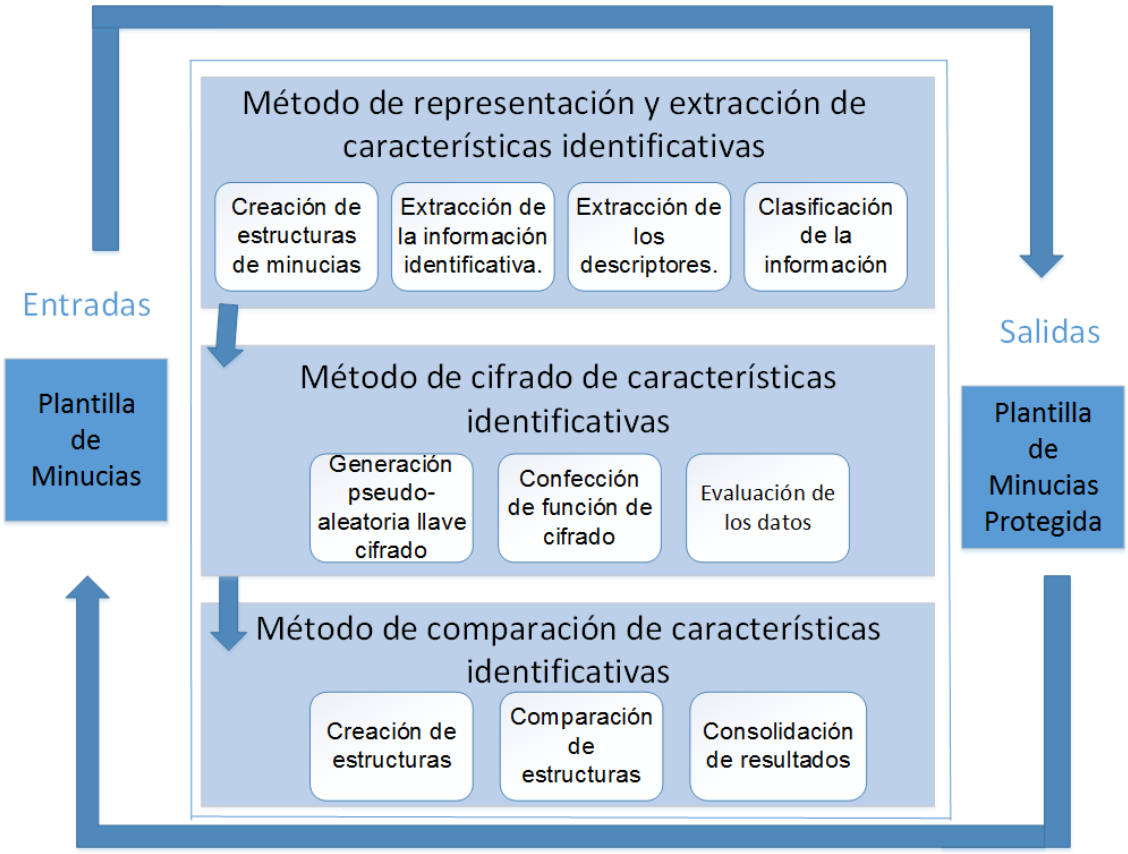


Figura 2.3: Representación del modelo propuesto.

2.3 Estructura del modelo de protección de plantillas de minucias de huellas dactilares.

En la presente investigación se propone un modelo para proteger los datos biométricos contenidos en las plantillas de minucias de huellas dactilares compuesto por un nivel de seguridad. Como entradas del modelo se tienen las plantillas de minucias en texto claro y como salidas las plantillas de minucias en el dominio protegido. El modelo contempla el nivel de seguridad dividido en:

a) **Transformación de los datos:** consiste en la transformación de la información contenida en las plantillas de minucias. Las minucias y su interacción con las vecindades son representadas utilizando el método de representación y extracción de información identificativa a partir de las

minucias. la información extraída es invariante a rotación y traslación y resistente a deformación no lineal y a superposición parcial.

b) **Cifrado de los datos:** consiste en la evaluación de las características extraídas en una función invertible. Esta función es un polinomio elaborado a partir de la generación de una llave de cifrado utilizando un método de generación de llaves específico.

El modelo contempla la inclusión o adaptación de un método de comparación de características. Este método tiene en cuenta:

- las variaciones intra-usuario que presentan las huellas dactilares
- la detección, con un cierto nivel de certeza, de las características que son genuinas y las agregadas por cambios en los datos de entrada.

Componentes del modelo propuesto:

El **componente de representación y extracción de características identificativas** realiza la representación de la información contenida en las plantillas de minucias a través de la estructura compleja la cual constituye un aporte de la investigación. Este componente recibe como entrada la plantilla de minucias en texto claro y retorna un conjunto de características transformadas, derivadas de las minucias que permiten identificar a una persona.

El **componente de cifrado de características identificativas** realiza la codificación de las características y habilita la revocabilidad de las plantillas protegidas. Este componente recibe como entrada las características transformadas y retorna las características codificadas.

El **componente de comparación de características identificativas** realiza el cálculo del índice de similitud entre dos plantillas protegidas. El componente

toma como entrada dos conjuntos de características cifradas o plantillas protegidas y realiza la comparación en dos niveles. El primer nivel consiste en la comparación de las estructuras primarias y retorna el índice de similitud entre ellas. El segundo nivel consiste en la comparación de las estructuras secundarias, retornando el índice de similitud entre ellas. Finalmente se realiza la consolidación de los datos resultantes de ambas etapas de manera local y global.

En el epígrafe 2.4 se explica con mayor grado de detalles estos componentes, a través de la descripción de una instancia del modelo. En la figura 2.4 se representa el proceso de cifrado con todos los componentes del modelo incluidos.

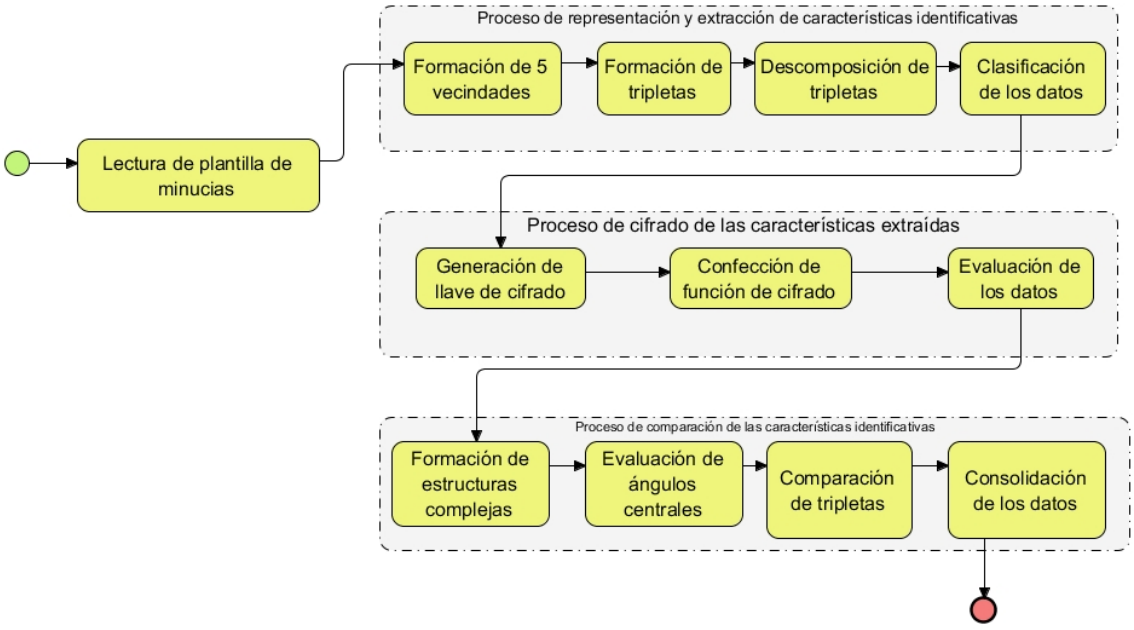


Figura 2.4: Representación del proceso de protección de plantillas de minucias utilizando el modelo propuesto.

2.3.1 Componente método de representación y extracción de características identificativas.

Un método de representación de la información contenida en las minucias consiste en el análisis y transformación de la información de una minucia (x, y, σ, t). Como propiedad esencial de la transformación se define que las características resultantes deben ser lo suficientemente discriminativas como para identificar a una persona. El componente de representación y extracción de características identificativas a partir de las minucias que se elabora como parte del modelo debe cumplir las siguientes restricciones:

1. Invariante a rotación.
2. Invariante a traslación.
3. Resistente a la deformación no lineal.
4. Resistente a la superposición parcial.
5. La transformación debe ser irreversible.
6. Independiente de las características extraídas.

El autor utiliza la estructura compleja [69] debido a que aporta información local y global de la huella dactilar, que resulta importante utilizar durante el proceso de comparación. Una estructura compleja se caracteriza por la unión de dos estructuras de minucias ampliamente estudiadas en la bibliografía:

1. la estructura de n vecindades más cercanas.
2. las tripletas de minucias.

La estructura n vecindades más cercanas es utilizada por el método de representación y extracción de características identificativas para caracterizar la huella dactilar de manera global, estableciendo las relaciones entre las n

minucias más cercanas a una minucia de referencia. Durante la comparación de estructuras identificativas se utiliza la estructura de n vecindades más cercanas para obtener la relación existente entre las minucias, permitiendo detectar que minucias pertenecen al conjunto original (conjunto de muestra).

La estructura tripletas de minucias es utilizada para realizar el análisis local de la huella dactilar. A través de ella se realiza la descripción de la relación que se establece entre tres minucias pertenecientes a la estructura compleja. De cada tripleta se extrae un conjunto de información que caracteriza e identifica localmente a la estructura. Esta información identificativa, transformada inicialmente, es utilizada como datos de entrada en el método de cifrado. El método de representación y extracción de la información es considerado un nivel de transformación.

De manera general este componente del modelo está integrada por:

1. Creación de estructuras de minucias.
2. Extracción de la información identificativa.
3. Extracción de los descriptores.
4. Clasificación de la información transformada.

2.3.2 Componente método de cifrado de características identificativas.

Como segunda componente del modelo se propone un método de cifrado de características identificativas extraídas en el componente anterior. Para ello se propone realizar:

1. Generación pseudo-aleatoria de la llave de cifrado.
2. Confección de la función de cifrado.
3. Evaluación de los datos en la función.

Debido a la gran variabilidad intra e inter usuario que presentan las huellas dactilares se realiza el cifrado utilizando un polinomio como función de cifrado. Para la construcción del polinomio se tiene en cuenta:

1. El resultado de la comparación del conjunto de características x y el conjunto de características transformadas $f_{(x)}$ no puede ser mayor que el umbral de similitud u.

$$C\left(f_{(x)}, x\right) > u \qquad (2.1)$$

2. Como característica de seguridad el polinomio debe ser de grado n > 3.
3. Al menos dos de los términos del polinomio deben ser negativos.
4. Varias plantillas protegidas generadas a partir del mismo conjunto de datos biométricos no pueden dar positivo ante una comparación.

De esta manera se garantiza que la transformación de los datos sea irreversible mientras se almacene solamente los datos transformados y que no puedan ser correlacionados mediante un ataque de multiplicidad de valores.

2.3.3 Componente método de comparación de características identificativas.

Con el objetivo de realizar el reconocimiento biométrico en el dominio protegido se desarrolla un método para la comparación de características identificativas. El método utilizado para la comparación de plantillas de minucias protegidas puede ser diseñado específicamente para realizar este proceso a partir de las características extraídas o puede ser adaptado para realizar la comparación a partir de un método existente.

El componente de comparación de plantillas protegidas en el dominio protegido se descompone en:

1. Creación de las estructuras protegidas.
2. Comparación de las estructuras protegidas.
    a. Cálculo de la similitud de ángulos centrales
    b. Comparación a nivel local.
    c. Comparación a nivel global.
3. Consolidación de los resultados.

Como premisas para la construcción de un componente de comparación de plantillas protegidas utilizando este modelo se define que:

1. Las estructuras sean tratadas como minucias a los efectos de la comparación, analizando el índice de similitud entre dos estructuras.
2. El análisis de la información contenida en las estructuras debe realizarse de manera local y global.
3. Se posibilite la obtención de cuáles datos coinciden en la plantilla original y cuáles son introducidos por las variaciones intra-usuario.
4. La consolidación de los datos debe reflejar el análisis global y local, aportando mayor énfasis en el análisis local.

Además de ello se realiza el cálculo de la similitud entre estructuras compleja basado en umbrales de decisión para obtener mayor precisión en el proceso de comparación a nivel global. En dependencia de las estructuras complejas seleccionadas para realizar la representación y extracción de información identificativa proveniente de las minucias se establece un umbral de similitud por característica seleccionada. Esto permite la discriminación de los datos a nivel local y global, aumentando la exactitud del método de comparación.

2.4 Instancia del modelo para la protección de plantillas de minucias de huellas dactilares

Para implementar el modelo de protección de plantillas de minucias de huellas dactilares se realiza una instancia con métodos propuestos por el autor. Para la representación y extracción de la información proveniente de las minucias se emplea una estructura compleja, la cual constituye un aporte de la presente investigación. La información resultante del método de representación y extracción es invariante a rotación y traslación, resistente a la deformación no lineal y a la superposición parcial. Para realizar la comparación de las plantillas protegidas se diseña un método de comparación el cual constituye otro aporte de la investigación. Para realizar el cifrado de las características se selecciona un método para la generación pseudo-aleatoria de números enteros a partir de una semilla y se utiliza un polinomio de grado n. A continuación se describen los componentes y métodos propuestos como instancia del modelo.

2.4.1 Componente método de representación y extracción de características identificativas.

El método desarrollado para la representación y extracción de las características identificativas a partir de las minucias utiliza la estructura compleja como estructura de minucias. El método consta de 3 algoritmos:

1. Algoritmo para la formación de estructuras complejas de minucias.
    a. Formación de la estructura 5 vecindades más cercanas a una minucia.
    b. Extracción de las tripletas que pueden formarse utilizando el centro y las minucias vecinas de la estructura.

2. Algoritmo para la extracción de características invariantes a rotación y traslación provenientes de las tripletas.

3. Algoritmo para la clasificación de las características extraídas.

El proceso de representación y extracción de características identificativas [69] se muestra en el anexo 3. Para la formación de la primera estructura de minucias perteneciente a la estructura compleja se selecciona 5 vecindades como la cantidad apropiada para la estructura n vecindades de minucias, debido a que, en el análisis y revisión de la bibliografía es la cantidad de minucias que mayor utilización tiene y la de mejores resultados [70], [71]. Para obtener resultados propios se realizó un experimento en el que se compararon las estructuras complejas con diferentes cantidades de vecindades de minucias. Los resultados obtenidos se muestran en la tabla 2.1:

Tabla 2.1: resultado comparativo de las estructuras de minucias.

Cantidad de vecindades	Tasas de falso aceptado	Tasas de falso rechazo	Índice de similitud
4	0.029	0.034	3.30 %
5	0.020	0.021	3.30 %
6	0.025	0.027	3.30 %
7	0.030	0.033	3.30 %

El algoritmo para la formación de estructuras complejas comienza con la selección de un punto central $A(x, y)$ dentro del conjunto de minucias $E(x, y, \alpha, t)$ donde (x, y) representan las coordenadas en el espacio cartesiano, α representa el ángulo de la minucia y t el tipo de minucia, utilizado en la ecuación 2.2 que se representa a continuación.

$$\sum_{i=0}^{n} \frac{x_i}{n}; \sum_{i=0}^{n} \frac{y_i}{n} \qquad (2.2)$$

La selección de este punto central permite establecer un orden en la creación de las estructuras de minucias y tiene como objetivo disminuir el tiempo y costo computacional durante el proceso de comparación. Este punto central o centroide calcula el centro de la colección de minucias. Partiendo del punto $A(x, y)$ se busca la minucia $Z(x, y)$ más cercana a él utilizando la función de distancia:

$$\lambda = min_{z_i \in E}\, d(A, Z_i) \qquad (2.3)$$

Donde i toma valores de $0\ a\ n$, siendo n la cantidad de minucias y d la distancia euclidiana entre dos puntos (minucias). Finalmente se ordenan las minucias en contra de las manecillas del reloj.

Para la formación de las 5 vecindades más cercanas se toma como centro la minucia z_0 obtenida de (2.3) y se calculan las 5 vecindades más cercanas V utilizando la función 2.4.

$$\lambda = min_{z_i \in E}\, d(z_0, z_i) \text{ con } z_0 \neq Z_i \qquad (2.4)$$

Donde λ representa la mínima distancia entre una minucia z_i y la minucia central z_0. Una vez obtenidas las 5 vecindades más cercanas, a partir de la minucia central, se calcula el ángulo que forma cada vecindad en relación con el centro. Este ángulo se calcula con respecto al eje x y es de vital importancia durante el proceso de comparación para calcular la probabilidad de que una tripleta esté formada o no a partir de minucias válidas. Esto permite conocer si una tripleta está formada por minucias que coinciden con el conjunto original, lo que mejora el rendimiento biométrico.

La descomposición en tripletas de minucias se realiza a partir de la formación de todas las tripletas posibles dado una estructura de 5 vecindades más cercanas. Para describir el tipo de dato que contiene cada tripleta y la relación entre las minucias se adiciona un descriptor a cada tripleta denominado primario o secundario:

1. Primario: Cuando uno de sus vértices coincide con la minucia central.
2. Secundario: Cuando ninguno de sus vértices coincide con la minucia central.

Posteriormente se realiza el proceso de selección de tripletas de calidad el cual consiste en la eliminación de tripletas donde la suma de dos de sus ángulos sea mayor que 150 grados. Esto se debe a que se ha observado que la formación de este tipo de tripletas es menor en plantillas de minucias que pertenecen a un mismo rasgo biométrico. La estructura compleja queda como se muestra en la figura 2.5

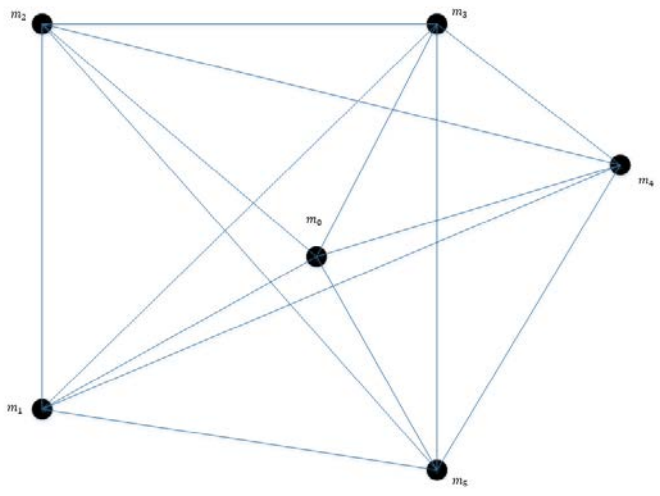


Figura 2.7: Estructura compleja.

De cada tripleta se extraen las características identificativas como se muestra en la figura 2.6.

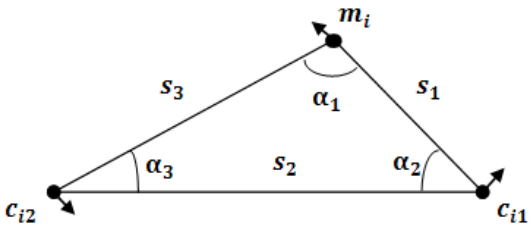


Figura 2.6: Extracción de características identificativas de las tripletas de minucias.

Tomado de [47]***.***

Existen una variedad de características identificativas que pueden ser extraídas de las tripletas de minucias entre las que se encuentran:

1. Forma del triángulo.
2. El tipo de triangulo.
3. La mediana del triángulo.
4. El lado de mayor longitud del triángulo.
5. La posición y la orientación de la minucia con respecto a sus vecindades.
6. Los ángulos formados entre la dirección de cada minucia y el lado correspondiente a su vecina en dirección a las manecillas del reloj.
7. La longitud de los lados del triángulo.
8. La amplitud de los ángulos internos del triángulo.
9. La diferencia entre dos ángulos adyacentes a un lado.

En la presente investigación se seleccionan las características:

1. Longitud de los lados del triángulo.
2. Amplitud de los ángulos internos del triángulo.
3. Diferencia entre dos ángulos adyacentes a un lado.

Esta selección se debe a que son utilizadas con éxito en varios modelos de protección libres de alineación [47]. Para la extracción de las características

identificativas invariantes a rotación y traslación como se muestra en la figura 2.6 se utiliza el teorema del coseno, quedando el vector de características de la siguiente forma $S_1, S_2, S_3; \alpha_1, \alpha_2, \alpha_3; \Delta\sigma_1, \Delta\sigma_2, \Delta\sigma_3$.

La longitud de los lados se representan como S_1, S_2, S_3, los ángulos internos son representados como $\alpha_1, \alpha_2, \alpha_3$, la diferencia de los ángulos de las minucias adyacentes a un lado representada como $\Delta\sigma_1, \Delta\sigma_2, \Delta\sigma_3$ y se calcula mediante la expresión 2.5.

$$\Delta\sigma_1 = \mathrm{dif}(\mathrm{angulo}c_{i2}, anguloc_{i1}) \qquad (2.5)$$

Este proceso se realiza a todas las minucias presentes en la plantilla de minucias en texto claro, quedando la misma cantidad de minucias que de estructuras complejas.

2.4.2 Componente método de cifrado de características identificativas

El proceso de cifrado de características identificativas transforma las características extraídas al evaluar todos los datos utilizando una función matemática. El proceso de cifrado de características identificativas se divide en:

1. Generación de la clave de cifrado.
2. Formación de la función de cifrado.
3. Evaluación de los datos.

El proceso de generación de la clave de cifrado consiste en la generación de un conjunto de números pseudo-aleatorios que conformarán la llave de cifrado. En la presente investigación y con fines experimentales se propone utilizar el esquema de generación de números pseudo-aleatorios utilizando el método de

generación congruencial lineal [72] debido a que es ampliamente utilizado con fines de simulación. Para ello se recurrir a la expresión 2.6:

$$x_n = (ax_{n-1} + c)r \quad (2.6)$$

Donde $a\ y\ c$ son dos números primos pequeños que constituyen el multiplicador y el aditivo, x_{n-1} es el resultado de la operación anterior a excepción del primer número generado donde se sustituye x_{n-1} por x_0 y r es el resultado de la operación $a\ mod\ c$. La generación de la llave criptográfica da como resultado los coeficientes para la construcción de un polinomio p de grado n el cual es utilizado para evaluar los datos biométricos.

El proceso de cifrado de las características identificativas consiste en la evaluación de todas las características identificativas en el polinomio elaborado a partir de la llave. En este proceso se realiza la evaluación inicialmente de los 5 ángulos centrales, posteriormente se evalúan las características provenientes de las tripletas primarias y finalmente de las tripletas secundarias como se muestra en el anexo 4.

Como salida de este proceso se tiene una cadena de números enteros que representan las características identificativas provenientes de las minucias. Estas características son utilizadas por el método de comparación para reconstruir las estructuras y calcular el índice de similitud existente entre dos plantillas protegidas. Para almacenar estas características en la plantilla protegida se utiliza una estructura que delimita cuáles son los datos pertenecientes a los ángulos centrales, tripletas primarias y tripletas secundarias. La forma para el almacenamiento de la plantilla se presenta en la tabla 2.2:

Tabla 2.2 Almacenamiento de los datos en la plantilla protegida

Formato de la plantilla	Valores
Ángulos centrales	5 unidades (cada uno es un entero de 32 bits)
Cantidad de tripletas primarias	Entero 32 bits
Tripletas primarias	19 unidades (cada uno contiene los datos asociados a una tripleta)
Cantidad de tripletas secundarias	Entero de 32 bits
Tripletas secundarias	5 unidades (cada uno contiene los datos asociados a una tripleta)

El almacenamiento de estas características obedece al mismo orden de conformación del vector de características. De esta manera durante el proceso de comparación se extraen los ángulos centrales, las características identificativas con descriptor primario y las características identificativas con descriptor secundario. La propuesta de este tipo de almacenamiento está basada en el almacenamiento de las plantillas de minucias en texto claro [19].

2.4.3 Componente método de comparación de características identificativas.

La comparación de características identificativas, en la presente investigación, se refiere al proceso mediante el cual se calcula el índice de similitud entre dos plantillas de minucias en el dominio protegido. Se describe en este acápite un

método de comparación de características identificativas para comprobar la aplicabilidad del método de comparación.

Para realizar la comparación de características identificativas en el dominio protegido se define como pre condición que ambas plantillas se encuentren transformadas. Para hacer uso de los descriptores, primario y secundario, definidos en el método de representación y extracción de características identificativas se desarrolla el proceso de comparación de plantillas protegidas mediante:

1. Algoritmo para la creación de estructuras protegidas.
2. Algoritmo para la comparación de estructuras protegidas.
    a. Cálculo de la probabilidad de ocurrencia.
    b. Comparación de estructuras primarias.
    c. Comparación de estructuras secundarias.
3. Algoritmo para la consolidación de los resultados.

El proceso de comparación se realiza, de manera general, como se muestra en el anexo 5. El proceso de comparación de estructuras complejas se inicia con la extracción de los datos identificativos almacenados en la plantilla protegida. La lectura arbitraria de los datos permite la conformación de las estructuras complejas. Las primeras 15 tripletas leídas pertenecen a las tripletas primarias y las demás son las tripletas secundarias.

El método de comparación de estructuras se divide en tres algoritmos.

a) El algoritmo para el cálculo de la probabilidad de ocurrencia consiste en la comparación de los ángulos centrales de las estructuras complejas. Este algoritmo utiliza un umbral de rotación (Ur) para representar la

máxima rotación permitida que pueden experimentar las minucias en cada muestra. Como objetivo se persigue conocer qué tripletas de minucias presentes en el conjunto de muestra fueron formadas a partir de minucias que no estaban en el conjunto de minucias de la plantilla de prueba.

b) El algoritmo de comparación de estructuras complejas (primarias y secundarias) define el descriptor desfasamiento (d), el cual constituye la diferencia, en pixeles, entre la longitud de los lados de cada tripleta. El descriptor grados de libertad (gl) se define como la diferencia entre dos ángulos a comparar y se encuentra asociado a los ángulos internos (gli) y la diferencia de los ángulos de dos minucias adyacentes a un lado (gld). Ambos descriptores actúan como umbrales para calcular el índice de similitud entre dos estructuras como se muestra en la figura 2.7.

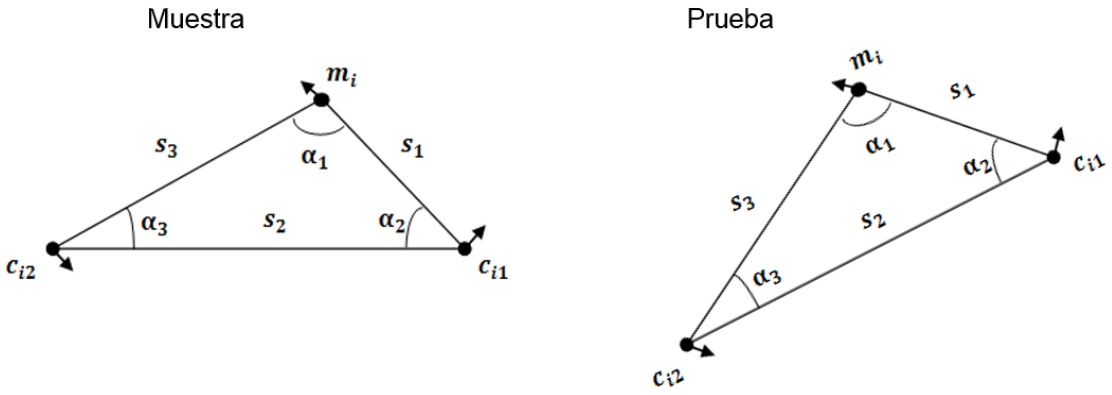


Figura 2.7: Comparación de tripletas primarias. Tomado de [47]**.**

La comparación de los descriptores consiste en hallar el módulo de la resta de los valores de cada uno de ellos como se muestra en las expresiones 2.7, 2.8, 2.9.

$$d = \left| d_{muestra} - d_{prueba} \right| \qquad (2.7)$$

$$gli = \left|gli_{muestra} - gli_{prueba}\right| \qquad (2.8)$$

$$gld = \left|gld_{muestra} - gld_{prueba}\right| \qquad (2.9)$$

La comparación de estructuras con mayor probabilidad de ocurrencia se realiza mediante la comparación de las tripletas de primer orden y las tripletas de segundo orden de cada estructura compleja. Las tripletas que no dan un resultado positivo se comparan sin tener en cuenta si son primarias o secundarias. El cálculo de similitud entre las estructuras complejas se realiza utilizando la expresión 2.10:

$$I = \left(\frac{P}{P_t} \times 0.6\right) + \left(\frac{S}{S_t} \times 0.4\right) \quad (2.10)$$

Donde P representa la cantidad de tripletas primarias que se comparan positivamente, P_t la cantidad de tripletas primarias en total, S la cantidad de tripletas secundarias que comparan positivamente y S_t la cantidad de tripletas secundarias total.

c) El algoritmo de consolidación de los datos consiste en calcular el índice de similitud general que tienen las estructuras complejas que comparan de manera global. Para conocer si una plantilla de prueba y una plantilla de muestra en el dominio protegido pertenecen a una misma persona se calcula el índice de similitud i entre ambas a partir de la expresión 2.11:

$$i = (m/n) \times 100 \qquad (2.11)$$

Donde *m* representa la cantidad de estructuras complejas que aparecen en ambas plantillas y *n* el total de estructuras complejas.

La utilización de la estructura compleja mejora la tolerancia a cambios en los conjuntos de minucias de prueba y de muestra. La eliminación o reemplazo de una minucia en el conjunto de prueba con respecto al conjunto de muestra afecta en menor medida que lo propuesto en [47] debido a que se introduce el cálculo del ángulo central, los descriptores de las tripletas y la cantidad de información que es utilizada en el método propuesto es mayor.

El modelo desarrollado contiene los componentes y relaciones entre los diferentes elementos que conforman el proceso de protección de plantillas de minucias de huellas dactilares, lo que aumenta la seguridad criptográfica y facilita la revocabilidad de los datos. Esto disminuye las probabilidades de realizar ataques para obtener los datos biométricos en texto claro pues es libre de alineación y solo almacena los datos cifrados. Esto tiene un impacto sobre la seguridad debido a que los datos de ayuda almacenados por los modelos analizados pueden ser correlacionados mediante ataques de multiplicidad de valores.

Conclusiones parciales del capítulo.

Una vez realizado el diagnóstico inicial y fundamentado el modelo de protección se concluye lo siguiente:

- Como resultado del análisis comparativo realizado se detectaron insuficiencias que limitan la seguridad criptográfica de estos modelos y su capacidad para realizar la revocabilidad de las plantillas canceladas.

- La conceptualización del modelo de protección de plantillas de minucias planteó los elementos teóricos necesarios para mitigar las insuficiencias detectadas en los modelos analizados.

- Mediante la integración de experiencias positivas respecto al análisis comparativo realizado, fueron definidos los constructos que sustentan el diseño del modelo propuesto.

- La elaboración de la estructura compleja, como base para la representación y extracción de características identificativas, permitió la obtención de características invariantes a rotación y traslación y la eliminación de algunas insuficiencias detectadas en el estudio diagnóstico realizado.

- La construcción de un modelo práctico como instancia del modelo teórico permitió sentar las bases para la validación de la hipótesis de la investigación.

Capítulo III: Validación del modelo para la protección de plantillas de minucias de huellas dactilares.

Capítulo III: Validación del modelo para la protección de plantillas de minucias de huellas dactilares.

En el presente capítulo se formulan las indicaciones metodológicas para la implementación del modelo y se describen los experimentos realizados para validar el modelo propuesto en la presente investigación. Se realiza un análisis comparativo con los resultados obtenidos de la medición de la seguridad criptográfica y la revocabilidad en los modelos pioneros y el modelo propuesto.

3.1 Instrumentación del modelo.

Para la implementación del modelo, en sistemas automáticos de identificación mediante huellas dactilares, se definen las siguientes acciones:

1. **Modificación del módulo de extracción**: se adiciona el proceso de representación y extracción de características identificativas y el cifrado de las características luego de extraídas las minucias. Se reemplaza la forma de crear la plantilla de minucias para adaptarla a las nuevas condiciones de una plantilla cifrada.
2. **Estimación de umbrales:** se estiman los umbrales a utilizar en el método de comparación. Para ello se tiene en cuenta la calidad de las muestras obtenidas y del sensor utilizado en el sistema automático de identificación mediante huellas dactilares donde se implemente. Para ello se propone utilizar el protocolo de pruebas utilizado en la investigación.
3. **Comparación de plantillas:** se aplica el método de comparación de plantillas en el dominio protegido el cual reemplaza o adapta el método de comparación utilizado por el sistema automático de identificación de huellas dactilares en texto claro para comparar características protegidas.

4. **Seguridad criptográfica**: la generación de llaves de cifrado se realiza utilizando un método de generación de llaves robusto. La función de cifrado tiene tantos términos como seguridad sea necesaria. Las llaves de cifrado se almacenaran utilizando un contenedor de llaves seguro de los que han sido propuestos en la bibliografía para almacenar las llaves de los cripto-sistemas clásicos. Este proceso es indispensable para lograr buenos resultados en términos de seguridad y protección de la información.
5. **Revocabilidad de los datos:** se cancelan las plantillas comprometidas y se genera una nueva llave de cifrado para realizar el proceso de cifrado a partir de los mismos rasgos biométricos. En dependencia del contexto se debe cifrar la base de datos en su totalidad o las nuevas plantillas cifradas que han sido generadas. Este proceso es indispensable para la generación de nuevas plantillas biométricas protegidas y permite la utilización del mismos rasgo biométrico una vez que ha sido robado.

Para la realización de experimentos aplicando el modelo propuesto se utilizó el kit de desarrollo de software (SDK) provisto por la empresa de desarrollo biométrico Innovatrics. Se escoge la utilización de este SDK debido a que esta empresa es considerada líder en el mundo en el tema de reconocimiento biométrico y ha obtenido varios premios en las competencias de verificación de huellas dactilares (FVC). El SDK fue utilizado para realizar el proceso de extracción de minucias de huellas dactilares, las cuales constituyen la entrada del modelo. Adicionalmente se utilizaron plantillas de minucias provistas por el Centro de Aplicaciones y Tecnologías de Avanzada (CENATAV), las cuáles

fueron extraídas con el extractor de *neurotecnology*. Este proceso se realizó aplicando el ciclo de vida en espiral que plantea la ingeniería de software.

Durante cada fase de desarrollo se realizaron experimentaciones para depurar y construir las bases teóricas de cada componente del modelo. Las comparaciones de los resultados obtenidos en cada experimento realizado modificaron las concepciones teóricas del modelo para mejorar los resultados.

Para comparar los resultados obtenidos por otros trabajos recientes se utilizaron los mismos datos que fueron usados para validar la hipótesis de la tesis doctoral *Cryptanalysis of the Fuzzy Vault for Fingerprints: Vulnerabilities and Countermeasures Dissertation* [16]. Estos datos fueron procesados y comparados manualmente y con ellos se obtuvieron resultados favorables en la investigación.

3.2 Validación del modelo propuesto

Los modelos de protección de plantillas de minucias de huellas dactilares deben garantizar la seguridad de los datos protegidos ante diferentes tipos de ataques. La revocabilidad de las plantillas protegidas por su parte debe garantizar que sea posible generar más de una plantilla protegida a partir del mismo rasgo biométrico y que no sea posible correlacionar dos plantillas para obtener los datos biométricos originales.

La validación de la seguridad criptográfica y la revocabilidad del modelo propuesto se realizan de la misma manera en la que fueron validados los modelos pioneros. Inicialmente se analiza de la seguridad criptográfica de los modelos pioneros y del modelo propuesto basado en la realización de varios ataques que se presentan a continuación:

1. Seguridad criptográfica.
2. Ataque de fuerza bruta.
3. Ataque de correlación.
4. Ataque de imagen previa.

Un resumen de las acciones del proceso de validación se muestra en la figura 3.1.

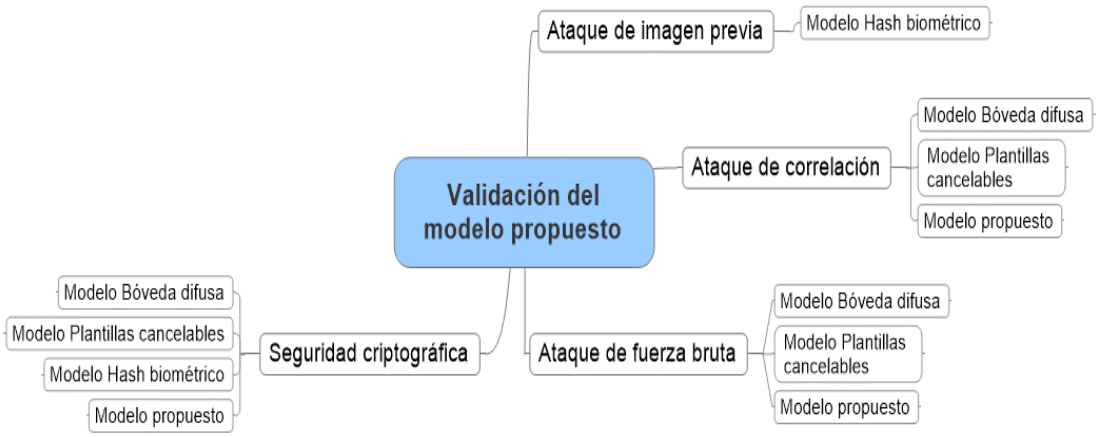


Figura 3.1: Proceso de validación del modelo propuesto. Fuente de elaboración propia.

3.2.1 Análisis de la seguridad criptográfica

El análisis de la seguridad criptográfica del modelo se realiza mediante el cálculo de los bits de fortaleza que presenta. Para realizar el cálculo se analiza la cantidad N de minucias que deben coincidir respecto al total de minucias m para romper la transformación. Este es un aspecto importante debido a que expresa la seguridad criptográfica que provee el modelo a los datos protegidos.

- **Bóveda difusa**

Los autores de este modelo de protección proponen que el método tiene un nivel de seguridad de 85 bits para un sistema con fuerte entropía personal. Para validar este nivel de seguridad se basan en que: para desbloquear una bóveda

difusa es necesario responder correctamente 29 preguntas de las 32 que fueron aseguradas originalmente. Esto en términos biométricos sería que de 32 minucias que estén en el conjunto original 29 tienen que comparar positivamente con el conjunto de muestra, lo que representa un 90.6 por ciento de las características originales.

Teniendo en cuenta que este modelo de protección es elaborado para aplicaciones que no contengan un alto número de usuarios se plantea que el problema principal lo constituye la cantidad de datos a comparar por el método de comparación. Esto provoca que la seguridad criptográfica del modelo sea variable, en dependencia de la cantidad de datos de comparación. Por ejemplo el peor de los casos sería encontrar una coincidencia de 1 en seis millones de registros. En este ejemplo la seguridad del método se calcula en 33 bits de fortaleza debido a que depende de la interpolación de un conjunto de características originales en la bóveda. Este problema se elimina en el modelo propuesto debido a que el proceso de comparación se define utilizando un método de comparación que analiza las características globales y locales de la huella dactilar.

- **Plantillas cancelables**

Los autores de este modelo de protección realizan un análisis de la seguridad de cada una de las transformaciones propuestas. El análisis que se toma como punto de comparación en la presente investigación es el realizado para las transformaciones funcionales debido a que son las más parecidas a la transformación propuesta por el autor. Para el análisis se tiene en cuenta que se

codifican 8 bits por minucia, la cantidad mínima de minucias a comparar de manera positiva es 15 y la cantidad total de minucias es 35.

En este análisis se asumen que las plantillas de minucias ya han sido alineadas, factor que mejora los resultados del modelo. En el modelo desarrollado en la presente investigación no es necesario asumir esto debido a que el modelo es invariante a rotación y traslación. Para calcular la fortaleza del método se utiliza la expresión 3.1:

$$p = 8m - \log_2 \binom{N}{m} \qquad (3.1)$$

Como resultado se obtiene que el método ofrece una seguridad de 66 bits. En la tabla 3.1 se muestran los resultados obtenidos con el modelo propuesto los cuales son superiores.

- **Hash biométrico**

Este modelo contiene diferencias significativas en cuanto a los modelos de bóveda difusa, plantillas cancelables y el modelo propuesto. La entrada de este modelo es la imagen de la huella dactilar, a partir de la cual se obtiene el hash biométrico. En el caso de la bóveda difusa, las plantillas cancelables y el modelo propuesto la entrada es la plantilla de minucias.

En el análisis realizado por los autores del modelo hash biométrico no se expone de manera textual la expresión utilizada para calcular la seguridad criptográfica, se analiza el modelo y se asegura que tiene 384 bits de seguridad. En comparación con el modelo propuesto la seguridad criptográfica es superior (354) sin embargo, el hash biométrico presenta vulnerabilidades que no ocurren en el modelo desarrollado en la presente investigación.

- **Modelo propuesto**

El aumento en la seguridad criptográfica del modelo propuesto se sustenta en el análisis comparativo de la seguridad de los modelos bóveda difusa, plantillas cancelables y hash biométrico. Para el cálculo de los bits de fortaleza se toma como punto de referencia la expresión 3.1. Para cada transformación se codifica como mínimo 32 bits de información en vez de 8 como se propone en las plantillas cancelables y en la bóveda difusa. La cantidad de estructuras complejas promedio es de 40 por plantilla y como mínimo deben comparar 12 estructuras complejas para obtener un índice de similitud que permita asegurar que ambas plantillas pertenecen a una misma persona.

Como resultado se obtiene que el modelo propuesto presenta 354 bits de fortaleza lo que se considera un nivel alto de seguridad en comparación con los modelos pioneros. Se debe destacar que la fortaleza está en correspondencia con la cantidad de bits que se codifican y la cantidad de estructuras complejas formadas. En el caso del modelo la cantidad de bits que se codifican es mayor. La cantidad de estructuras complejas y la cantidad de minucias que contiene la plantilla en texto claro es la misma sin embargo, la cantidad de información a codificar es mayor debido a que de una minucia solo se codifica las coordenadas (x, y) y el ángulo σ, mientras que de una estructura compleja se codifica toda la información extraída de las tripletas formadas entre las 5 vecindades más cercanas.

Ataque de Fuerza bruta

Este tipo de ataque consiste en adivinar un conjunto finito de características, suficientes para identificar a una persona. Por lo general, la dificultad de realizar

un ataque de fuerza bruta es expresada en cantidad de operaciones necesarias para realizar con éxito la reconstrucción de la plantilla biométrica. Para estimar la fortaleza del modelo propuesto se realiza el análisis teórico del ataque de fuerza bruta sobre los modelos bóveda difusa, plantillas cancelables y el modelo propuesto. Aunque estos aspectos fueron abordados en el epígrafe 3.2.2 vale la pena destacar que para realizar este ataque se envía una plantilla generada aleatoriamente y se evalúa el criterio de satisfacción.

El criterio de satisfacción consiste en comprobar cuántos elementos del conjunto de datos generados coinciden con los elementos del conjunto de datos protegidos. El ataque culmina cuando se satisface el criterio, lo cual indica que se ha roto la seguridad del modelo y obtenido un conjunto de datos con el cual es posible suplantar la identidad de una persona. A continuación se explica cómo se realiza este ataque en los modelos pioneros y en el modelo propuesto.

- **Bóveda difusa**

En [52] se realiza una implementación del modelo bóveda difusa y se calcula su seguridad criptográfica utilizando una clave de 144 bits, de ellos 128 son utilizados para el cifrado y 16 para el código de corrección de errores. Para ello calculan la combinación de la cantidad de elementos que son reales en la bóveda con la cantidad de combinaciones de los elementos como se muestra en la expresión 3.2:

$$C(elementos\ total, combinaciones\ del\ elemento) \quad (3.2)$$

Este ataque tiene como objetivo identificar los puntos genuinos y los puntos basura dentro de la bóveda para encontrar un polinomio de interpolación que permita obtener los datos originales. Para considerar exitoso un ataque de este

tipo en el modelo bóveda difusa, con 18 puntos originales y 200 puntos basura se estima necesario un promedio de 5.3×10^{10} intentos para encontrar los puntos originales.

- **Plantillas cancelables**

En el caso del modelo de plantillas cancelables se analiza solo las transformaciones funcionales debido a que son las más parecidas a la transformación propuesta por el autor. La cantidad mínima de minucias a comparar de manera positiva es 15 y la cantidad total de minucias es 35, lo que sustituido en la expresión 3.2 da como resultado aproximadamente 3×10^{9} intentos.

Analizando lo expresado en [13] sobre los métodos de comparación a utilizar se estima que la probabilidad de realizar un ataque de fuerza bruta exitosamente puede calcularse mediante la expresión 3.3:

$$G = \frac{N}{K \times d} \qquad (3.3)$$

Donde N representa la cantidad de minucias que tiene la plantilla, $K\ y\ d$ representan los valores posibles que pueden tomar las coordenadas y la orientación. La probabilidad se estima en 0.03125 % de obtener una plantilla que compare positivamente.

Para este modelo se diseñó un conjunto de ecuaciones para realizar un ataque de fuerza bruta por [14]. Este ataque consiste en la solución de un conjunto de ecuaciones para obtener las características originales. En él se demuestra que es posible obtener las características originales en un 90.2 % cuando tiene una sola solución y un 9.8% cuando tiene dos soluciones.

Estos resultados son alarmantes para la seguridad criptográfica del modelo debido a que se garantiza el acceso a cualquier sistema automático de identificación mediante huellas dactilares.

- **Modelo propuesto**

En el caso del ataque de fuerza bruta analizado por [52] en relación con el modelo propuesto se estima que en una plantilla de 18 estructuras protegidas:

1. Deben encontrarse al menos 6 elementos de una tripleta.
2. Deben encontrarse al menos 190 tripletas.

Para ello se calcula, utilizando la expresión 3.2, la combinación de $C(190,6)$, lo que resulta en $60334683255 \approx 6.0 \times 10^{10}$ probabilidades de encontrar una plantilla protegida que compare, teniendo en cuenta que se pueden repetir los elementos dentro de una tripleta.

En un caso ideal donde deban comparar todos los elementos de una tripleta y todas las tripletas formadas en las estructuras como se muestra a continuación:

1. Los 9 elementos de una tripleta
2. Las 342 tripletas formadas en las 18 estructuras.

Se calcula, utilizando la expresión 3.2, la combinación $C(342,9)$, lo que resulta en $158625578809472060 \approx 1.5 \times 10^{17}$. Este caso es el que más se adecúa al calculado en [52] por lo que en comparación es posible asegurar que la probabilidad de tener éxito en este tipo de ataque en comparación con el método propuesto es considerablemente menor. Esto se debe a que es mucho mayor la cantidad de elementos que hay que tener en cuenta para realizar la comparación en el modelo propuesto.

En relación al análisis realizado en las plantillas cancelables, el modelo propuesto tiene la misma cantidad de minucias que de estructuras complejas sin embargo, la estructura compleja contiene más información que una minucia. En este caso una estructura compleja está compuesta por 19 tripletas que a su vez se encuentran compuestas por los datos pertenecientes a los 3 ángulos internos, 3 variaciones de los ángulos adyacentes a un lado y 3 lados. Estos son los datos sobre los cuales se basa el método de comparación para establecer el índice de similitud entre dos plantillas protegidas.

Para calcular la probabilidad de obtener un conjunto de estructuras complejas que coincidan con el conjunto original se establece la expresión 3.4:

$$G = \frac{N}{ai \times da \times d} \qquad (3.4)$$

Donde N representa la cantidad de estructuras complejas, ai y da representan los valores posibles de los ángulos internos y la diferencia de ángulos adyacentes respectivamente, d representa los valores posibles de los lados.

Como resultado se obtiene una probabilidad de $0.4 \times 10^{-25}\%$ de realizar un ataque exitoso. De esta manera se puede afirmar que la probabilidad de obtener un rasgo utilizando este ataque es considerablemente menor.

En [16] se realiza un ataque de fuerza bruta, con el objetivo de determinar el conjunto de puntos reales dentro de la bóveda difusa denominado ataque de fuerza bruta ordinario. En este ataque el polinomio de interpolación es creado a partir del código de corrección de errores. Para determinar si se ha tenido éxito en el ataque se verifica que $h(f^*) = h(f)$. En el modelo propuesto no se utiliza el código de corrección de errores ni se almacena el polinomio característico

junto a los datos cifrados, razones por las cuales este ataque específicamente no es aplicable.

A continuación, se presenta la tabla comparativa 3.1 con los tipos de ataques realizados a los modelos pioneros de protección de plantillas de minucias de huellas dactilares y al modelo propuesto.

3.1 Tabla comparativa sobre la seguridad criptográfica de los modelos analizados

Aspectos	**Bóveda difusa**	**Plantillas cancelables**	**Hash biométrico**	**Modelo propuesto**
Seguridad criptográfica	85 bits	66 bits	384 bits	354 bits
Ataque de fuerza bruta (cant. de operaciones)	5.3×10^{10}	3×10^{9}	_	1.5×10^{17}
Ataque de fuerza bruta (probabilidad)	0.13625%	0.03125 %.	_	$0.4 * 10^{-25}$%.
Multiplicidad de valores	97.68 %	97.68%	_	_

- **Ataque de imagen previa.**

Este ataque es diseñado específicamente para el hash biométrico y consiste en encontrar un conjunto de datos identificativos aproximados que comparen en el dominio protegido. El hash biométrico no parte de la plantilla de minucias, este esquema parte de la técnica de extracción denominada *FingerCode*. Su principal vulnerabilidad reside en que las semillas utilizadas para la creación de los *BioCode* son almacenados juntos. En [57] se describe un ataque realizado al

modelo hash biométrico en el cual se obtienen los *BioCode* y de ellos los *FingerCode* asociados a la imagen de la huella dactilar. Para obtener los *FingerCode* se describen 5 etapas que a continuación se mencionan:

1. Genotipo.
2. Población.
3. Función de aptitud.
4. Operadores sobre el genotipo.
    a. Mutación
    b. Selección.
    c. Cruzamiento.
5. Criterio de parada.

Este ataque propone realizar una aproximación al FingerCode original a partir de la función de aptitud que representa la distancia real entre el *BioCode* generado y el original. Para ello son utilizados por los autores del ataque dos métodos:

1. Extracción de características de patrones binarios locales (ECPBL).
2. Método de Gabor.

Los resultados obtenidos en la aproximación del *FingerCode* a partir de la generación de un *BioCode* se muestran a continuación en la tabla 3.2:

Tabla 3.2: Valores de la aproximación entre el FingerCode real (FR) y el generado (FG).

Métodos para generar el FingerCode	**Dimensión**	**Valor promedio de la función de aptitud**	**Valor promedio de diferencia entre FG y FR**
ECPBL	152	5.5	6.5

Gabor	256	9.2	203.2

Este ataque no puede ser realizado al modelo de protección de plantillas de minucias que se propone en la presente investigación. Este ataque está diseñado para obtener los datos asociados al *FingerCode* y reconstruir el *BioCode*. El modelo elaborado en la presente investigación no contempla estas estructuras, ni realiza de manera similar el proceso de protección de datos.

3.2.2 Análisis de la revocabilidad del modelo propuesto.

Los datos pertenecientes a un identificador biométrico son únicos e invariantes para toda la vida. La obtención de estos mediante ataques informáticos realizados a un sistema automático de identificación mediante huellas dactilares trae como consecuencia la pérdida del identificador biométrico. Durante el proceso de protección de plantillas de minucias de huellas dactilares se agrega un factor de variabilidad para mitigar esta dificultad y permitir generar renovar las plantillas protegidas. Este factor de variabilidad es denominado revocabilidad, la cual consiste en la generación de varias plantillas protegidas a partir del mismo rasgo biométrico.

Para validar la revocabilidad del modelo propuesto se describen dos ataques propuestos en la bibliografía a los cuales son vulnerables los modelos de bóveda difusa y plantillas cancelables. Estos ataques se clasifican como parte de los ataques de multiplicidad de valores y son los **ataques de correlación** y de **comparación cruzada.**

Los ataques de correlación están dirigidos a obtener los datos biométricos en texto claro a partir de dos o más plantillas biométricas cifradas. Para ello se

establece una correlación entre las plantillas o utilizando el ataque de comparación cruzada para determinar si pertenecen ambas plantillas al mismo identificador biométrico.

Una vez establecido si dos plantillas protegidas fueron obtenidas a partir del mismo identificador biométrico, se comparan entre sí para detectar cuáles son los datos coinciden entre ellos y por lo tanto son considerados los datos originales.

En [16] se conceptualizan y describen dos escenarios en los cuales puede ser realizado el ataque de correlación. A continuación, se detallan los escenarios para correlacionar dos plantillas de minucias:

a. Un atacante ha obtenido dos plantillas protegidas V y W pero no conoce que ambas plantillas pertenecen al mismo identificador biométrico.
b. Un atacante ha obtenido dos plantillas protegidas V y W y conoce que ambas plantillas pertenecen al mismo identificador biométrico.

La definición de un ataque de correlación se describe a continuación:

Sean V y W dos bóvedas, cada punto $v \in V$ y $w \in W$ los cuales codifican una característica de la huella dactilar (la coordenada x) m y m' respectivamente. Asumiendo que exista una medida de distancia o similitud $d(m, m')$ es posible calcular el mapa de distancia de V x W mediante la expresión 3.5:

$$d: V \times W \to \mathbb{R} \geq 0, (v, w) \mapsto d(m, m') \qquad (3.5)$$

Considerando para cada bóveda que la expresión 3.6:

$$d_W(v) \coloneqq min_{w \in W} d(v, w) \qquad (3.6)$$

Donde d_W representa la mínima distancia de v a uno de los puntos en W. Este ataque está diseñado para desbloquear la bóveda utilizando otra bóveda que ha sido codificada utilizando el mismo rasgo biométrico y en el peor de los casos tiene un 97.68 % de efectividad.

En el caso del modelo plantillas cancelables los ataques de correlación se realizan de la misma manera. Al obtenerse una plantilla de minucias protegida utilizando este método es posible obtener la solución inversa para cada minucia. Debido a la propiedad de uno a muchos de las funciones de transformación se obtienen varias soluciones.

Una vez obtenidas las soluciones inversas se tratan como una bóveda difusa y se realiza la comparación cruzada para determinar que valores son los reales. Cuando se obtiene la segunda plantilla se realiza la comparación cruzada para correlacionar los puntos verdaderos, tratando cada solución como una bóveda difusa. Los resultados obtenidos coinciden con los de la bóveda difusa.

En el modelo que se propone en la presente investigación este ataque no aplica debido a que el proceso de transformación y cifrado de los datos biométricos se realiza de manera invertible y solo se almacena la imagen de la función o datos transformados. Una vez transformado $x \rightarrow X$ y evaluado en $f(x)$ no es posible realizar la reconstrucción del polinomio solo con los datos cifrados.

3.2.3 Análisis del rendimiento biométrico en el proceso de comparación de estructuras complejas

Para realizar la comparación de las estructuras complejas se utilizó el protocolo de pruebas propuesto en [1] y utilizado internacionalmente para comparar plantillas de minucias de huellas dactilares. El proceso de comparación se

realizó con el algoritmo elaborado en la presente investigación en el epígrafe 2.4.3.

Los experimentos que se describen a continuación fueron realizados utilizando el protocolo de pruebas descrito en [1] donde las tasas de falsos aceptados (FAR) y falsos rechazos (FRR) se calculan utilizando las expresiones 3.7 y 3.8 respectivamente.

$$\text{FAR} = \int_0^t p(s|H_1)ds \quad (3.7)$$

$$\text{FRR} = \int_0^1 p(s|H_0)ds \quad (3.8)$$

Los datos para realizar las pruebas se tomaron de las bases de datos internacionales identificadas como FVC2000, FVC2002 y FVC2004. Estas bases de datos son ampliamente utilizadas para probar el rendimiento de los métodos de comparación a nivel internacional por las investigaciones desarrolladas en el área del reconocimiento de personas mediante huellas dactilares. Cada base de datos contiene 80 imágenes de huellas dactilares tomadas con diferentes sensores como se detalla en las tablas A1, A2 y A3 que se encuentran en el anexo 6. Los datos están tipificados como se muestra a continuación:

Rasgo biométrico 101_1, lo que representa:

- 101 números que identifican el rasgo biométrico.
- 1 número que identifica la toma.

Para la representación de características identificativas se estudiaron las estructuras propuestas en [71], las cuales han sido utilizadas en trabajos similares y fueron analizadas en el epígrafe 2.1. La selección de la cantidad de minucias que contiene la estructura está basada en:

1. La revisión bibliográfica realizada.
2. El balance entre cantidad de datos para la comparación y el cifrado.
3. Experimentos realizados donde se varía la cantidad de datos y se analiza el rendimiento biométrico del método después de realizar la representación y extracción de características identificativas.

Teniendo en cuenta estos elementos se selecciona para la estructura de n vecindades las 5 minucias más cercanas a la minucia en análisis. Se selecciona las tripletas de minucias debido a que aportan información local de la huella dactilar, invariante a rotación y traslación; además ha sido utilizada con éxito en varios algoritmos de comparación, indexación y protección.

La estructura compleja descrita en el epígrafe 2.4.1 da como resultado 10 tripletas que incluyen la minucia central, denominadas tripletas primarias y 9 tripletas que no incluyen la minucia central, denominadas tripletas segundarias. De cada tripleta se extraen 9 características identificativas lo que da un total por estructura compleja de 171 características identificativas a comparar. Teniendo en cuenta que una plantilla de minucias promedio contiene 50 minucias y que se forma igual cantidad de estructuras complejas se decide utilizar n = 5 minucias para la estructura de n vecindades más cercanas.

La comparación de estas estructuras se realizó con todas las bases de datos descritas anteriormente, pero los resultados que se muestran son los de las bases de datos FVC 2000 DB1-B y FVC2000 DB2-B debido a que los datos publicados por otros autores utilizan estas mismas bases de datos. Esto nos permite comparar los resultados de la investigación realizada con resultados

publicados a nivel internacional. Los umbrales de similitud fueron definidos como:

- Umbral de similitud entre ángulos interiores 12 grados.
- Umbral de similitud entre diferencia de ángulos 10 grados.
- Umbral de similitud entre longitud de los lados 5 px.
- El umbral de similitud se obtuvo del proceso de prueba.

Los resultados obtenidos se muestran en la tabla 3.3.

Tabla 3.3 Tasas de falso rechazo, falso aceptado (FMR y FRR) e índice de similitud obtenidas con texto claro.

Base de datos	**Tasa de falsos aceptados**	**Tasa de falso rechazo**	**Índice de similitud umbral**
DB1-B	0.021519	0.0278481	3.30%
DB2-B	0.020886	0.0218354	3.30%

Adicionalmente se observaron los índices de similitud máximos y mínimos entre estructuras complejas. Los resultados se muestran a continuación en la tabla 3.4:

Tabla 3.4 Resultados límites del índice de coincidencia para estructuras que coinciden (TM) y para las que no coinciden (TNM).

Base de datos	**Mayor índice TM**	**Menor índice TM**	**Mayor índice**	**Menor índice TNM**
DB1-B	51. 63	1.24	7.08	0
DB2-B	49.69	1.00	6.46	0

Los resultados obtenidos indican que es posible identificar a una persona utilizando características identificativas obtenidas a partir de la estructura compleja. Una vez aplicado el método de cifrado se comprueba la afectación al rendimiento biométrico. Para el cálculo de los umbrales de similitud se evaluaron los umbrales en la función de cifrado y se realizó varias veces la prueba modificando los valores evaluados y observando los resultados. Los resultados se muestran a continuación en la tabla 3.5 y 3.6:

Tabla 3.5: Tasas de falso rechazo, falso aceptado (FMR y FRR) e índice de similitud obtenidas con texto cifrado.

Base de datos	Tasa de falso aceptado	Tasa de falso rechazo	Índice de similitud umbral
DB1-B	0.063422	0.0599387	3.30%
DB2-B	0.069967	0.0615228	3.30%

Tabla 3.6: Tasas de falso rechazo, falso aceptado (FMR y FRR) e índice de similitud obtenidas con texto cifrado.

Base de datos	Tasa de falso aceptado	Tasa de falso rechazo	Índice de similitud umbral
DB1-A	0.0975	0.03296	19.24%
DB2-A	0.0736	0.05194	19.24%

Adicionalmente se realizó la comprobación del rendimiento biométrico utilizando los mismos datos utilizados en [16]. Los valores obtenidos se muestran en la tabla 3.7. Este experimento tiene como particularidad que los datos coinciden en 10 minucias que aparecen en ambas plantillas.

Tabla 3.7: Resultados comparativos entre el aporte realizado a la bóveda difusa por [16]

y el modelo propuesto expresado en por ciento.

Modelos	**Tasa de falso aceptado**	**Tasa de genuino aceptado**
Bóveda difusa modificada	0.03	81.14
Modelo propuesto	0.04	79.65

Se debe destacar que el autor del aporte realizado a la bóveda difusa en 2012 asegura que mientras se realice el cifrado de una sola característica biométrica este método no será seguro. En comparación el modelo que se propone en la presente investigación no presenta las vulnerabilidades que aparecen en los modelos de bóveda difusa, plantillas cancelables y hash biométrico, aunque el rendimiento biométrico decae ligeramente en comparación con estos modelos.

Basado en el estudio realizado, se detectaron insuficiencias y/o limitaciones que atentan contra la seguridad criptográfica, la revocabilidad y el rendimiento de los modelos de protección de plantillas de minucias, las que fueron resumidas en el capítulo 2. A continuación se presenta la tabla 3.8 dónde se muestra un análisis comparativo que demuestra el grado de solución que logra el modelo propuesto como resultado de la presente investigación en comparación con los principales modelos existentes.

Tabla 3.8 Comparación del modelo propuesto con otros modelos de cifrado.

Modelos	Alineación	Comparación utilizando información local y global	Dificultad en realizar la revocabilidad	Vulnerabilidad ante ataques
Bóveda difusa	No	No	alta	Alta
Plantillas cancelables	No	No	alta	Alta
Hash biométrico	No	No	Media	Alta
Extractor difuso	No	No	Alta	Alta
Modelo propuesto	Si	Si	Baja	Muy baja

Conclusiones del capítulo.

Una vez realizado el análisis comparativo de la seguridad criptográfica y la revocabilidad de los modelos pioneros y el modelo propuesto en la presente investigación se concluye lo siguiente:

- El análisis teórico sobre la seguridad criptográfica del modelo propuesto en comparación con los modelos de protección de plantillas de minucias de huellas dactilares analizados permitió asegurar que el modelo desarrollado no es vulnerable a los ataques descritos en la bibliografía.
- El análisis de la propiedad de revocabilidad en los modelos pioneros en comparación con el modelo que se propone en la investigación mostró que se facilita la realización de la revocabilidad en el mismo y se eliminan las vulnerabilidades que se presentan en los modelos pioneros en cuanto a esta propiedad.
- Los resultados obtenidos del rendimiento biométrico haciendo uso de las estructuras complejas para transformar los datos, manteniendo el

valor identificativo de los mismos, muestran la factibilidad del uso de este tipo de estructura como método de obtención de datos invariantes a rotación y traslación, resistentes a la deformación no lineal.

Conclusiones generales

Los resultados obtenidos durante la presente investigación permiten concluir que:

- El análisis de los elementos teóricos y prácticos más actuales en el campo de la biometría, específicamente la protección de plantillas de minucias de huellas dactilares, permitió el diseño de un modelo de protección invariante a rotación, traslación y resistente a la deformación no lineal
- El uso de la estructura de minucias propuesta en la investigación permitió identificar cuáles datos son transformados a partir de minucias que coinciden en texto plano para mejorar el rendimiento del método de comparación.
- El análisis de la seguridad criptográfica y la revocabilidad de los modelos pioneros permitieron elaborar un modelo de protección libre de las vulnerabilidades descritas en la bibliografía que facilita el proceso de revocabilidad.
- La utilización de bases de datos internacionales para la validación del modelo propuesto permitió comparar los resultados obtenidos con resultados publicados y reconocidos a nivel internacional, mostrando un ligero decremento en el rendimiento biométrico del modelo propuesto pero con mayor seguridad criptográfica que los modelos pioneros.

Recomendaciones

- Extender el modelo para realizar la protección de otros identificadores biométricos como el iris y el rostro.
- Proponer un método para el cálculo de los umbrales de decisión mediante el análisis estadístico de la comparación de estructuras complejas en el dominio protegido.

REFERENCIAS BIBLIOGRÁFICAS

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. 2009, p. 506.

[2] N. Dahiya and C. Kant, “Biometrics Security Concerns,” in *Second International Conference on Advanced Computing & Communication Technologies Biometrics*, 2012, pp. 299–304.

[3] R. Lathwal and V. K. Saroha, “A Study on Biometric Technology and Access Control System : Network Security,” *Int. J. Comput. Sci. Eng.*, vol. 2, no. 7, pp. 31–35, 2014.

[4] N. Kamboj and A. K. Yadav, “Biometric System: Secure User Authentication,” *IJCSC*, vol. 6, no. 2, pp. 223–226, 2015.

[5] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, “Fingerprint Image Reconstruction from Standard Templates,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, 2007.

[6] M. Gobi and D. Kannan, “A Secured Public Key Cryptosystem for Biometric Encryption,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 184–191, 2014.

[7] A. K. Jain, K. Nandakumar, and A. Nagar, “Fingerprint Template Protection : From Theory to Practice,” *Secur. Priv. Biometrics*, pp. 187–214, 2013.

[8] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 1–17, 2008.

[9] W. J. Scheirer and T. E. Boult, “CRACKING FUZZY VAULTS AND BIOMETRIC ENCRYPTION,” in *Biometrics Symposium, 2007*, 2007, pp. 1–6.

[10] M. M. Roja and S. Sawarkar, “ElGamel Encryption for Biometric Database Protection,” *Int. J. Comput. Appl.*, vol. 68, no. 6, pp. 10–14, 2013.

[11] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” in *IEEE International Symposium on Information Theory*, 2002, p. 408.

[12] S. Lee, D. Moon, W. Y. Choi, and Y. Chung, “Analysis of Tradeoffs among Verification Accuracy , Memory Consumption , and Execution Time in the GH-based Fuzzy Fingerprint Vault,” in *International Conference on Security Technology Analysis*, 2008, pp. 73–78.

[13] R. M. Bolle, N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Syst. J.*, vol. 40, no. 3, 2001.

[14] F. Quan, S. Fei, C. Ann, and Z. Feifei, “Cracking Cancelable Fingerprint Template of Ratha,” in *2008 International Symposium on Computer Science and Computational Technology*, 2008, pp. 572–575.

[15] J. Merkle and B. Tams, “Security of the Improved Fuzzy Vault Scheme in the Presence of Record Multiplicity,” no. 0, pp. 1–40, 2013.

[16] B. B. Tams, “Cryptanalysis of the Fuzzy Vault for Fingerprints : Vulnerabilities and Countermeasures,” 2012.

[17] G. H. Sierra, “Métodos de representación y verificación del locutor con independencia del texto,” 2014.

[18] R. Kumar, “Vulnerability to Fingerprint Biometric Systems- An Overview,” *IJCSC*, vol. 5, no. 1, pp. 109–115, 2014.

[19] I. Standard, “INTERNATIONAL ISO / IEC,” vol. 2005, 2005.

[20] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *APPLIED CRYPTOGRAPHY*. 1996, pp. 1–794.

[21] V. Shoup, “A Proposal for an ISO Standard for Public Key Encryption (version 2 . 1),” 2001.

[22] K. Nandakumar, “A Fingerprint Cryptosystem Based on Minutiae Phase Spectrum,” in *WIFS 2010*, 2010, pp. 2–7.

[23] A. Nagar, K. Nandakumar, and A. K. Jain, “A hybrid biometric cryptosystem for securing fingerprint minutiae templates q,” *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 733–741, 2010.

[24] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, p. 3, 2011.

[25] J. Mwema, J. Mwema, M. Kimwele, and S. Kimani, “A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates,” *Int. J. Comput. Trends Technol.*, vol. 20, no. 1, 2015.

[26] T. Ignatenko and F. M. J. Willems, “Biometric Systems: Privacy and Secrecy Aspects,” *IEEE Trans. Inf. FORENSICS Secur.*, vol. 4, no. 4, pp. 956–973, 2009.

[27] R. S. Fernández, V. E. Sentí, and Y. H. Heredia, “Cryptographic schemes for minutiae template protection,” *Int. J. Innov. Appl. Stud.*, vol. 14, no. 4, pp. 997–1004, 2016.

[28] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.

[29] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, 1960.

[30] J. Merkle, M. Niesing, and M. Schwaiger, “Provable Security for the Fuzzy Fingerprint Vault,” in *The Fifth International Conference on Internet Monitoring and Protection*, 2010, pp. 65–73.

[31] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, “Secure Biometrics: Concepts, Authentication Architectures & Challenges,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, 2013.

[32] J. Hartloff, M. Bileschi, S. Tulyakov, J. Dobler, and A. Rudra, “Security analysis for fingerprint fuzzy vaults,” in in *Spie Defense, Security, and Sensing*, 2013.

[33] U. Uludag and A. K. Jain, “Attacks on Biometric Systems : A Case Study in Fingerprints,” in in *Electronic Imaging*, 2004, pp. 622–633.

[34] T. C. Clancy, N. Kiyavash, and D. J. Lin, “Secure smartcardbased fingerprint authentication,” in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, 2003, pp. 45–52.

[35] J. Jeffers and A. Arakala, “FINGERPRINT ALIGNMENT FOR A MINUTIAE-BASED FUZZY VAULT,” in *2007 Biometrics Symposium*, 2007.

[36] U. Uludag, “Securing Fingerprint Template : Fuzzy Vault with Helper Data,” in *2006 Conference on Computer Vision and Pattern Recognition Workshop*, 2006.

[37] J. Li, X. Yang, J. Tian, P. Shi, and P. Li, “Topological Structure-based Alignment for Fingerprint Fuzzy Vault,” in *19th International Conference on Pattern Recognition Pattern Recognition*, 2008, no. 1, pp. 6–9.

[38] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data,” *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[39] R. Canetti, L. Reyzin, and A. Smith, “Reusable Fuzzy Extractors for Low-Entropy Distributions,” pp. 1–27, 2016.

[40] Q. Li, M. Guo, and E.-C. Chang, “Fuzzy Extractors for Asymmetric Biometric Representations,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2008. CVPRW’08.*, 2008, pp. 1–6.

[41] N. Ratha, J. Connell, and R. M. Bolle, “Cancelable Biometrics : A Case Study in Fingerprints,” in *The 18th International Conference on Pattern Recognition (ICPR’06)*, 2006, pp. 18–21.

[42] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, 2007.

[43] H. Yang, X. Jiang, and A. C. Kot, “Generating Secure Cancelable Fingerprint Templates Using Local and Global Features,” in *2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 0–4.

[44] C. Lee and J. Kim, “Cancelable fingerprint templates using minutiae-based bit-strings,” *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 236–246, 2010.

[45] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, “Generating Registration-Free Cancelable Fingerprint Templates Based on Minutia Cylinder-Code Representation,” in *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013*, 2013, pp. 1–6.

[46] Z. Jin, B.-M. Goi, A. Teoh, and Y. H. Tay, “A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template,” *Secur. Commun. Networks*, vol. 7, no. 11, pp. 1691–1701, 2014.

[47] J. Zhe and A. T. Beng, “Fingerprint Template Protection with Minutia Vicinity Decomposition,” in *2011 International Joint Conference on Biometrics (IJCB),*, 2011, pp. 1–7.

[48] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “FingerCode: a filterbank for fingerprint representation and matching,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 1999, vol. 2, p. 8.

[49] A. Teoh, D. Ngo, C. Ling, and A. Goh, “Biohashing : two factor authentication featuring fingerprint data and tokenised random number,” *Pattern Recognit.*, vol. 37, pp. 2245–2255, 2004.

[50] R. Belguechi, C. Rosenberger, and S. A. Aoudia, “BioHashing for securing fingerprint minutiae templates,” in *2010 International Conference on Pattern Recognition*, 2010, pp. 1172–1175.

[51] R. Belguechi, E. Cherrier, C. Rosenberger, and S. Ait-aoudia, “Operational bio-hash to preserve privacy of fingerprint minutiae templates,” *IET Biometrics*, no. February, pp. 1–9, 2013.

[52] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy Vault for Fingerprints,” pp. 310–319, 2005.

[53] X. Zhang, Q. Feng, and K. He, “A New Blind Fingerprint Alignment Algorithm used in Biometric Encryption,” in *International Conference on Computer, Communications and Information Technology (CCIT 2014)*, 2014, vol. 1, no. Ccit, pp. 231–234.

[54] K. Nandakumar, A. K. Jain, and S. Pankanti, “Fingerprint-Based Fuzzy Vault : Implementation and Performance,” *IEEE Trans. Inf. FORENSICS Secur.*, vol. 2, no. 4, pp. 744–757, 2007.

[55] A. Jindal, D. Pal, N. Bhardwaj, and A. Panwar, “A Survey on Biometric Security Threats and Countermeasure,” vol. 2, no. 12, pp. 659–664, 2013.

[56] H. F. Security, *Hash function security : Cryptanalysis of the Very Smooth Hash and multicollisions in generalised iterated hash functions*. 2012.

[57] P. Lacharme, E. Cherrier, and C. Rosenberger, “Preimage Attack on BioHashing,” in *International Conference on Security and Cryptography*, 2014.

[58] A. Rozsa, “ATTACK ON MINUTIAE-BASED FINGERPRINT AUTHENTICATION SYSTEMS BY USING GENETIC ALGORITHM,” 2014.

[59] P. S. Prasad, “Vulnerabilities of Biometric System,” *Int. J. Sci. Eng. Res.*, vol. 4, no. 6, pp. 1126–1129, 2013.

[60] A. Kholmatov and B. Yanikoglu, “Realization of correlation attack against the fuzzy vault scheme,” in in *Electronic Imaging*, 2008, pp. 68190–68197.

[61] Y. C. Feng, M. Lim, and P. C. Yuen, “Masquerade attack on transform-based binary-template protection based on perceptron learning,” *Pattern Recognit.*, vol. 47, no. 9, pp. 3019–3033, 2014.

[62] U. Uludag, S. Member, S. Pankanti, and S. Member, “Biometric Cryptosystems : Issues and Challenges,” in *Proceedings of the IEEE*, 2004, vol. 92, no. 6, pp. 948–960.

[63] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, “Matching with Secure Fingerprint Templates using Non-invertible Transforms,” in *2008 Congress on Image and Signal Processing Matching*, 2008, pp. 29–33.

[64] K. Xi and J. Hu, “Biometric Mobile Template Protection : A Composite Feature based Fingerprint Fuzzy Vault,” in *IEEE International Conference on Communications*, 2009, pp. 1–5.

[65] K. Simoens, C. Chang, and B. Preneel, “Reversing Protected Minutiae Vicinities,” in *2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, 2010, pp. 1–8.

[66] W. Yang, J. Hu, and S. Wang, “A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1179–1192, 2014.

[67] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, “Fingerprint shell : Secure representation of fingerprint template q,” *Pattern Recognit. Lett.*, vol. 45, pp. 189–196, 2014.

[68] O. F. Díaz, “MIDAC: MODELO PARA EL DESARROLLO DE APLICACIONES COMPUESTAS BASADAS EN ARQUITECTURAS ORIENTADAS A SERVICIOS,” 2012.

[69] R. S. Fernández, A. A. M. Cento, and V. E. Sentí, “Extracción de características identificativas en plantillas de minucias mediante la estructura compleja,” *Rev. Cuba. Ciencias Informáticas*, vol. 9, no. 4, pp. 132–141, 2015.

[70] R. Cappelli, M. Ferrara, and D. Maltoni, “Minutia Cylinder-Code : A New Representation and Matching Technique for Fingerprint Recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, 2010.

[71] A. Arakala and J. Jeffers, “Minutiae-Based Structures for a Fuzzy Vault,” in *Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, 2006, pp. 1–6.

[72] R. C. Bu, *Simulación: un enfoque práctico*. Editorial Limusa, 1996.

[73] U. Uludag and A. K. Jain, “Attacks on Biometric Systems : A Case Study in Fingerprints,” in in Electronic Imaging, 2004, pp. 622–633.

[74] Y. Sutcu, H. T. Sencar, and N. Memon, “A Secure Biometric Authentication Scheme Based on Robust Hashing,” in Proceedings of the 7th workshop on Multimedia and security, 2005, pp. 111–116.

[75] S. Yang and I. Verbauwhede, “AUTOMATIC SECURE FINGERPRINT VERIFICATION SYSTEM BASED ON FUZZY VAULT SCHEME,” in IEEE International Conference on Acoustics, Speech, and Signal, 2005, pp. 3–6.

[76] E.-C. Chang, R. Shen, and F. W. Teo, “Finding the Original Point Set Hidden among Chaff,” in Proceedings of the 2006 ACM Symposium on Information, computer and communications security, 2006, pp. 182–188.

[77] H. Li and P. Liu, “An Identification System Combined with Fingerprint and Cryptography,” in First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS’06), 2006, pp. 4–7.

[78] T. E. Boult, W. J. Scheirer, and R. Woodworth, “Revocable Fingerprint Biotokens: Accuracy and Security Analysis,” in IEEE Conference on Computer Vision and Pattern Recognition, 2007, pp. 1–8.

[79] F. Farooq, R. M. Bolle, T. Jea, and N. Ratha, “Anonymous and Revocable Fingerprint Recognition,” in IEEE Conference on Computer Vision and Pattern Recognition, 2007, pp. 1–7.

[80] J. Feng, “Combining minutiae descriptors for fingerprint matching,” Pattern Recognit., vol. 41, pp. 342–352, 2008.

[81] J. Hu, “Mobile Fingerprint Template Protection : Progress and Open issues,” IEEE, 2008.

[82] S. Arabia, “Spiral Cube for Biometric Template Protection,” in Image and Signal Processing, 2012, pp. 235–244.

[83] R. Bais and K. K. Mehta, “Biometric Parameter Based Cryptographic Key Generation,” Int. J. Eng. Adv. Technol., vol. 1, no. 5, pp. 157–160, 2012.

[84] D. Bhagat, “Empirical Study of Technologies for Information Security,” IJEAR, vol. 2, no. 2, pp. 57–61, 2012.

[85] P. A. Kumari and G. J. Suma, “A NOVEL MULTIMODAL BIOMETRIC SCHEME FOR PERSONAL AUTHENTICATION,” Int. J. Res. Eng. Technol., vol. 2, no. 2, pp. 55–66, 2014.

[86] J. Sonar and S. O. Dahad, “A Review on Security of Fingerprint Template Using Fingerprint Mixing,” Int. J. Eng. Trends Technol., vol. 10, no. 8, pp. 402–407, 2014.

[87] R. Jain and C. Kant, “Attacks on Biometric Systems : An Overview,” Int. J. Adv. Sci. Res., vol. 01, no. 07, pp. 283–288, 2015.

[88] A. Juels, A. Juels, C. Drive, M. Wattenberg, and W. Street, “A Fuzzy Commitment Scheme,” 2015.

[89] M. Ghuge and K. Doke, “A Comprehensive Study on Various Visual cryptography Schemes with an Application,” Int. J. Emerg. Technol. Adv. Eng., vol. 4, no. 2, pp. 2–6, 2014.

[90] R. Wang, X. Yang, X. Liu, S. Zhou, P. Li, K. Cao, and J. Tian, “A Novel Fingerprint Template Protection Scheme Based on Distance Projection Coding,” in 2010 International Conference on Pattern Recognition, 2010, pp. 890–893.

[91] H. Xu and R. N. J. Veldhuis, “Spectral Minutiae Representations for Fingerprint Recognition,” in 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010, pp. 1–5.

[92] H. Xu and R. N. J. Veldhuis, “Binary Representations of Fingerprint Spectral Minutiae Features Complex Spectral Minutiae Represen- tation,” in 2010 International Conference on Pattern Recognition Binary, 2010, vol. 1, pp. 1–5.

[93] M. Mehta, H. Diwanji, and J. S. Shah, “A Genetic Based Non-Invertible Cryptographic Key Generation From Cancelable Biometric in MANET,” IJCTA, vol. 2, no. 6, pp. 3019–3022, 2011.

[94] L. Nanni, S. Brahnam, and A. Lumini, “Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system,” Electron. Lett., vol. 47, no. 15, 2011.

[95] B. Preneel, Modern Cryptology : An Overview, no. February. 2011, pp. 1–31.

[96] N. Radha and S. Karthikeyan, “AN EVALUATION OF F INGERPRINT SECURITY USING NONINVERTIBLE BIOHASH,” Int. J. Netw. Secur. Its Appl., vol. 3, no. 4, pp. 118–128, 2011.

[97] J. Tomas-buliart, A. Gomez-muro, M. Fernandez, and M. Soriano, “Use of Turbo Codes with Low-Rate Convolutional Constituent Codes in Fingerprinting Scenarios,” 2011.

[98] H. Wimberly and L. M. Liebrock, “Using Fingerprint Authentication to Reduce System Security : An Empirical Study,” in 2011 IEEE Symposium on Security and Privacy, 2011.

[99] M. Lafkih, P. Lacharme, C. Rosenberger, M. Mikram, S. Ghouzali, M. El Haziti, and D. Aboutajdine, “Vulnerabilities of fuzzy vault schemes using biometric data with traces,” in International Wireless Communications & Mobile Computing Conference, 2015.

[100] M. Blanton and M. Aliasgari, “Secure Computation of Biometric Matching,” Dep. Comput. Sci. Eng. Univ. Notre Dame, Tech. Rep, vol. 3, pp. 1–22, 2009.

[101] Y. Hani and B. Yahaya, “Fingerprint Biometrics Authentication on Smart Card,” in 2009 Second International Conference on Computer and Electrical Engineering, 2009, pp. 673–675.

[102] Z. Jin, A. J. Teoh, T. S. Ong, and C. Tee, “Secure Minutiae-Based Fingerprint Templates Using Random Triangle Hashing,” in in Visual Informatics: Bridging Research and Practice, 2009, pp. 521–531.

[103] A. P. K. Krishan, B. K. Sy, and A. Ramirez, “Parallel Secure Computation Scheme for Biometric Security and Privacy in Standard-Based BioAPI Framework,” no. Newton 2005, 2009.

[104] N. Lalithamani, “Towards Generating Irrevocable Key For Cryptography From Cancelable Fingerprints,” 2009.

[105] A. Nagar, A. K. Jain, and E. Lansing, “Biometric Template Transformation : A Security Analysis,” in in SPIE Electronic Imaging, 2010, pp. 75410–75410.

[106] A. Nagar, K. Nandakumar, and A. K. Jain, “A hybrid biometric cryptosystem for securing fingerprint minutiae templates q,” Pattern Recognit. Lett., vol. 31, no. 8, pp. 733–741, 2010.

[107] A. S. Rao and D. Albert, “Prospect of Implementation of Biometric Verification for Secure Credit Card Transactions,” Int. J. Electron. Electr. Eng., vol. 1, no. 4, pp. 291–294, 2013.

[108] M. Rathamani and P. Sivaprakasam, “Enhancing Cloud Data Security Using Dynamic Key Generation Algorithm,” Int. J. Adv. Sci. Tech. Res., vol. 6, no. 3, pp. 217–222, 2013.

[109] A. Ratle, “Availability Optimization for Series / Parallel Systems using Evolutionary Algorithm Availability Optimization for Series / Parallel Systems using Evolutionary Algorithm,” no. December, 2013.

[110] Y. Imamverdiyev, A. Jin, and J. Kim, “Expert Systems with Applications Biometric cryptosystem based on discretized fingerprint texture descriptors,” Expert Syst. Appl., vol. 40, no. 5, pp. 1888–1901, 2013.

[111] J. A. Siguenza, C. F. Tomas, and C. D. C. Madrid, “Hill-Climbing and Brute-Force Attacks on Biometric Systems : A Case Study in Match-on-Card Fingerprint Verification,” in IEEE Intl. Carnahan Conference on Security Technology, ICCST, 2006, no. October, pp. 151–159.

[112] A. Nagar, K. Nandakumar, and A. K. Jain, “Securing Fingerprint Template : Fuzzy Vault with Minutiae Descriptors,” in 19th International Conference on Pattern Recognition, 2008, pp. 2–5.

[113] G. Rajagopal and R. Palaniswamy, “Performance Evaluation of Multimodal Multifeature Authentication System Using K NN Classification,” vol. 2015, 2015.

[114] R. Belguechi, A. Hafiane, E. Cherrier, and C. Rosenberger, “Comparative Study on Texture Features for Fingerprint Recognition : Application to The BioHashing Template Protection Scheme,” J. Electron. Imaging, Soc. Photo-optical Instrum. Eng., 2016.

[115] T. K. Dang, Q. C. Truong, T. Thi, B. Le, and H. Truong, “Cancellable fuzzy vault with periodic transformation for biometric template protection,” IET Biometrics Res., no. JANUARY, 2016.

[116] R. S. Fernández, V. E. Sentí, and Y. H. Heredia, “Cryptographic schemes for minutiae template protection,” Int. J. Innov. Appl. Stud., vol. 14, no. 4, pp. 997–1004, 2016.

[117] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, and F. Scotti, “Privacy-Preserving Fingercode Authentication,” in Proceedings of the 12th ACM workshop on Multimedia and security, 2010, pp. 231–240.

[118] S. Li and A. C. . Kot, “PRIVACY PROTECTION OF FINGERPRINT DATABASE USING LOSSLESS DATA HIDING,” in IEEE International Conference on Multimedia and Expo (ICME), 2010, pp. 1293–1298.

[119] E. Liu, J. Liang, L. Pang, M. Xie, and J. Tian, “Author’s personal copy Minutiae and modified Biocode fusion for fingerprint-based key generation,” J. Netw. Comput. Appl., vol. 33, pp. 221–235, 2010.

[120] M. K. Saini, J. S. Saini, and S. Sharma, “Various Mathematical and Geometrical Models for Fingerprints : A Survey,” in Conf. on Advances in Signal Processing and Communication, 2013, pp. 12–15.

[121] K. H. Solanki, A. Sahayak, and V. V. Nagar, “A New Approach To Symmetric Key Generation Using Combination Of Biometrics Key And Cryptographic Key To Enhance Security Of Data,” Int. J. Eng. Res. Technol., vol. 2, no. 3, pp. 1–7, 2013.

[122] N. G. K. Thamaraiselvi, R. Priyadharshini, R. M. M. Hariharan, and B. Dhivya, “Feature Level Fusion of Multibiometrics to Provide Template Security,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 57–64, 2013.

[123] B. Vibert, C. Rosenberger, and A. Ninassi, “Security and Performance Evaluation Platform of Biometric Match On Card,” in International Conference on Mobile Applications and Security Management, 2013.

[124] S. Wang and J. Hu, “Design of alignment-free cancelable fi ngerprint templates via curtailed circular convolution,” Pattern Recognit., pp. 1–9, 2013.

[125] I. Engineering, “A Hybrid Approach for Image Data Security,” Int. J. Adv. Res. Electr. Electron. Instrum. Eng., vol. 3, no. 4, pp. 8484–8488, 2014.

[126] M. Inuma, “A relation between irreversibility and unlinkability for biometric template protection algorithms,” Josai Math. Monogr, vol. 7, pp. 55–65, 2014.

[127] I. Journal, R. Srivastava, and S. S. Thakur, “Performance Analysis of Fingerprint Based Biometric Authentication System using RSA,” Eng. Universe Sci. Res. Manag., vol. 6, no. 2, pp. 1–6, 2014.

[128] K. S. R. Krishna, G. Raghavendra, M. Shiva, P. S. Rao, K. S. Narayana, and K. V. Chowdary, “A Novel Approach for Non-Invertible Cryptographic Key Generation from Cancellable Fingerprint Template,” Int. J. Sci. Eng. Res., vol. 5, no. 6, pp. 1177–1183, 2014.

[129] W. Zhao and H. Zhang, “Secure Fingerprint Recognition Based on Frobenius Norm,” in 2012 International Conference on Computer Science and Electronics Engineering Secure, 2012, pp. 1–4.

[130] T. Ahmad, “SHARED SECRET-BASED KEY AND FINGERPRINT BINDING SCHEME,” KURSOR J., vol. 7, no. 1, pp. 11–18, 2013.

[131] S. Chandra, S. Paul, B. Saha, and S. Mitra, “Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network,” IOSR J. Comput. Eng., vol. 12, no. 1, pp. 16–22, 2013.

[132] S. Chiou, “Secure Method for Biometric-based Recognition with Integrated Cryptographic Functions,” Biomed Res. Int., pp. 1–20, 2013.

[133] M. David, “Privacy preserving biometrics using partially homomorphic encryption,” pp. 1–7, 2013.

[134] Z. Jiang, J. Zhao, J. Han, Z. Wang, S. Tang, J. Zhao, and W. Xi, “Wi-Fi Fingerprint Based Indoor Localization without Indoor Space Measurement,” in 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, 2013.

[135] Z. Jin, B. Goi, A. Teoh, and Y. H. Tay, “A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template,” in SECURITY AND COMMUNICATION NETWORKS, 2013.

[136] A. Juels, C. Drive, M. Wattenberg, and W. Street, “A Fuzzy Commitment Scheme,” pp. 1–21, 2013.

[137] H. Kang, Y. Hori, T. Katasahita, and M. Hagiwara, “The Implementation of Fuzzy Extractor is Not Hard to Do : An Approach Using PUF Data,” in SCIS 2013 The 30th Symposium on Cryptography and Information Security, 2013, pp. 1–7.

[138] C. Kant and A. Toky, “Biometrics Security Concerns,” IJITKM, vol. 7, no. 1, pp. 117–129, 2013.

[139] K. K. A. Ghany, A. E. Hassanien, N. I. Ghali, and A. C. Biometrics, “A Hybrid approach for biometric template security,” in 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2012, pp. 973–974.

[140] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, “Expert Systems with Applications An effective biometric cryptosystem combining fingerprints with error correction codes,” Expert Syst. Appl., vol. 39, no. 7, pp. 6562–6574, 2012.

[141] X. Li and D. Sun, “A Dual-Mode Fingerprint Fusion Encryption Method Based on Fuzzy Vault,” in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012, no. 60773015, pp. 208–215.

[142] X. Li and D. Sun, “A Dual-Mode Fingerprint Fusion Encryption Method Based on Fuzzy Vault,” in 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012, no. 60773015, pp. 208–215.

[143] X. Li, “Interoperable Protected Fingerprint Minutiae Templates,” 2012.

[144] M. M. Pravinchandra, “Performace Analysis of Encryption and Decryption using Genetic Based Cancelable Non-Invertible Fingerprint based Key in MANET,” in 2012 International Conference on Communication Systems and Network Technologies, 2012.

[145] B. R. Rao, E. V. V. K. Rao, S. V. R. Rao, and M. Rama, “Finger Print Parameter Based Cryptographic Key Generation,” Int. J. Eng. Res. Appl., vol. 2, no. 6, pp. 1598–1604, 2012.

[146] H. A. Salman, “Fuzzy Bio-Cryptography Key Generation,” in The 13th International Arab Conference on Information Technology, 2012, vol. 1, pp. 13–18.

[147] X. Shao, H. Xu, R. N. J. Veldhuis, and C. H. Slump, “A CONCATENATED CODING SCHEME FOR BIOMETRIC TEMPLATE PROTECTION,” in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 1865–1868.

[148] B. K. Sy and A. P. K. Krishnan, “Generation of Cryptographic Keys from Personal Biometrics : An Illustration Based on Fingerprints,” 2012.

[149] S. Salim and A. Biohashing, “International Journal of Computer Sciences Fingerprint Privacy Protection Techniques : A Comparative Study,” Int. J. Comput. Sci. Eng., vol. 2, no. 7, pp. 86–89, 2014.

[150] A. Sharma and N. Kumar, “Encryption of Text Using Fingerprints as Input to Various Algorithms,” vol. 3, no. 4, pp. 418–421, 2014.

[151] K. Sharma, “Fuzzy Vault Scheme using Multi-Features Bio Traits based on Polynomial Coefficients,” in 2nd International Conference on Computer and Intelligent Systems (ICCIS’2014) & 2nd International Conference of Electrical, Electronics, Instrumentation and Biomedical Engineering (ICEEIB’2014), 2014, no. 1999, pp. 2–6.

[152] A. Shukla, “Secure Transaction of Minutiae Data over Web,” Int. J. Sci. Res. Eng. Technol., vol. 2, no. 10, pp. 614–616, 2014.

[153] G. Morana, E. Tramontana, and D. Zito, “Detecting Attacks on Java Cards by Fingerprinting Applets,” in 2013 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2013.

[154] V. C. Ossai, I. C. Okoro, E. O. Alagbu, A. O. Agbonghae, and I. N. Okafor, “Enhancing E-Voting Systems By Leveraging Biometric Key Generation (Bkg),” Am. J. Eng. Res., vol. 2, no. 10, pp. 180–190, 2013.

[155] S. Biswas, N. K. Ratha, G. Aggarwal, and J. Connell, “Exploring Ridge Curvature for Fingerprint Indexing Exploring Ridge Curvature for Fingerprint Indexing,” in BTAS 2008. 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008., 2008, no. NOVEMBER, pp. 1–6.

[156] S. Chikkerur, N. K. Ratha, J. Connell, and R. M. Bolle, “Generating Registration-free Cancelable Fingerprint Templates,” in 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, no. NOVEMBER, pp. 1–6.

[157] S. Rane, W. Sun, and A. Vetro, “Secure Distortion Computation Among Untrusting Parties Using Homomorphic Encryption,” 2009.

[158] B. Yang and C. Busch, “Parameterized Geometric Alignment for Minutiae-Based Fingerprint Template Protection,” in IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, 2009, pp. 1–6.

[159] J. Malik and D. Girdhar, “Reference Threshold Calculation for Biometric Authentication,” Image, Graph. Signal Process., no. January, pp. 46–53, 2014.

[160] C. Mathew and A. Babu, “Secure Authentication Schemes 2,” Int. J. Res. Comput. Commun. Technol., pp. 53–56, 2014.

[161] A. S. Naik, S. M. Metagar, and P. D. Hasalkar, “A Survey on Secure Crypto-Biometric System using Blind Authentication Technique,” Int. J. Comput. Sci. Eng. Open, vol. 2, no. 5, pp. 93–97, 2014.

[162] P. Poongodi and P. Betty, “A Study on Biometric Template Protection Techniques,” Int. J. Eng. Trends Technol., vol. 7, no. 4, pp. 202–204, 2014.

[163] Y. Pruthi, H. Singh, and A. Verma, “A Comparative Study on Biometric Technology,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 1, pp. 993–996, 2014.

[164] K. P. Pulukuri, G. D. Rao, S. Kandala, and R. Nilaj, “SECURE FINGERPRINT USING MOSAICING,” IOSR J. Comput. Sci., vol. 2014, pp. 73–79, 2014.

[165] J. C. Bricout and P. M. A. Baker, “Leveraging online social networks for people with disabilities in emergency communications and recovery,” vol. 7, no. 1, pp. 59–74, 2010.

[166] A. M. P. Canuto, F. Pintro, A. F. Neto, and M. C. Fairhurst, “Enhancing Performance of Cancellable Fingerprint Biometrics using Classifier Ensembles,” in 2010 Eleventh Brazilian Symposium on Neural Networks, 2010, pp. 55–60.

[167] A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, “Cryptographic Key Generation from Multiple Biometric Modalities : Fusing Minutiae with Iris Feature,” Int. J. Comput. Appl., vol. 2, no. 6, pp. 16–26, 2010.

[168] N. Liu, “Research and Application of Fingerprint Recognition Based on MATLAB,” Open Autom. Control Syst. J., vol. 7, no. 2, pp. 1107–1111, 2015.

[169] R. G. Rittenhouse and J. A. Chaudhry, “A Survey of Alternative Authentication Methods,” in International Conference on Recent Advances in Computer Systems (RACS 2015), 2016, no. Racs 2015, pp. 179–182.

[170] M. K. Virdi, “Fingerprint Matching System for Spurious Minutiae,” J. Basic Appl. Eng. Res., vol. 1, no. 11, pp. 50–53, 2014.

[171] P. Sharma, M. Kapoor, and N. Dhillon, “Design of Biometric Authentication System using Three Basic Human Traits,” Int. J. Sci. Res., vol. 5, no. 1, pp. 1116–1120, 2016.

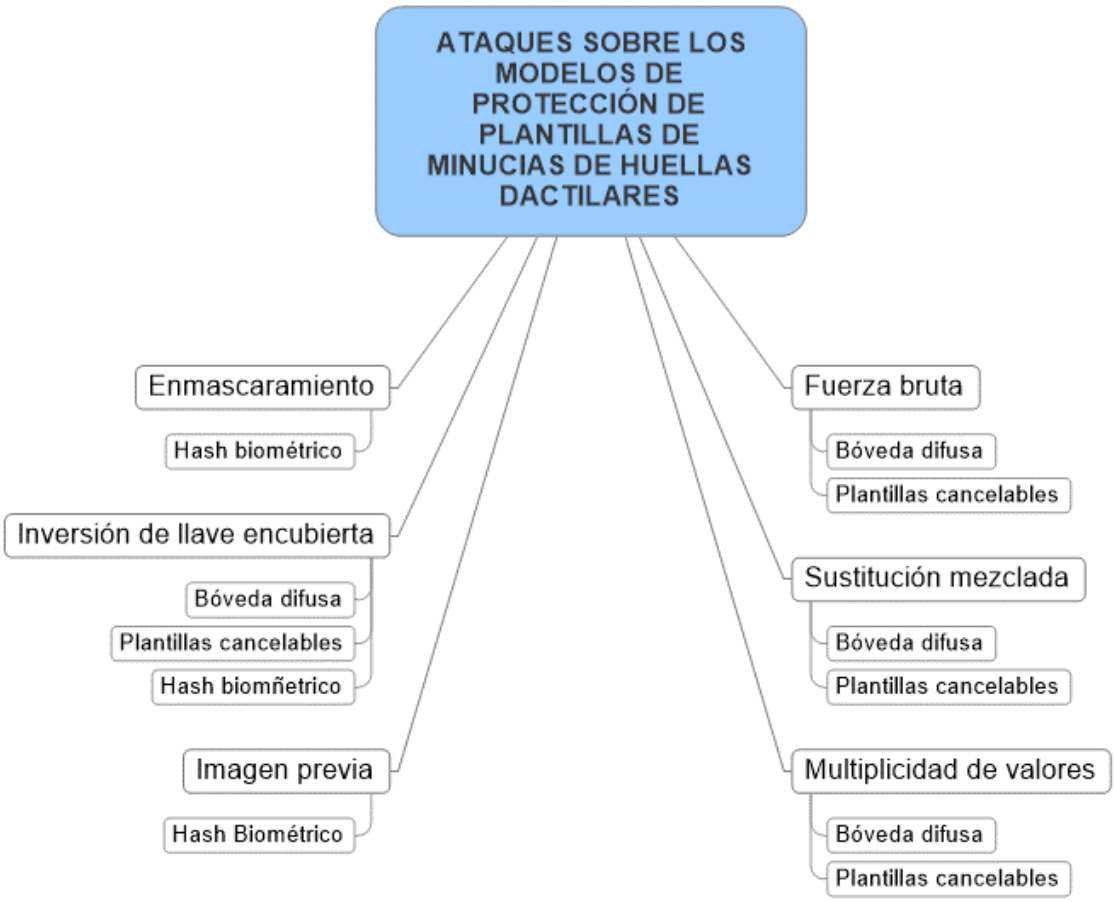
[172] R. S. Prasad and S. M. Nejres, “An Efficient Approach for Fingerprint Recognition,” Int. J. Eng. Innov. Res., vol. 4, no. 2, pp. 307–113, 2016.

[173] S. Narwal and D. Kaur, “Comparison between Minutiae Based and Pattern Based Algorithm of Fingerprint Image,” I.J. Inf. Eng. Electron. Bus., vol. 2, no. 3, pp. 23–29, 2016.

Cuerpo de Anexos

Anexos

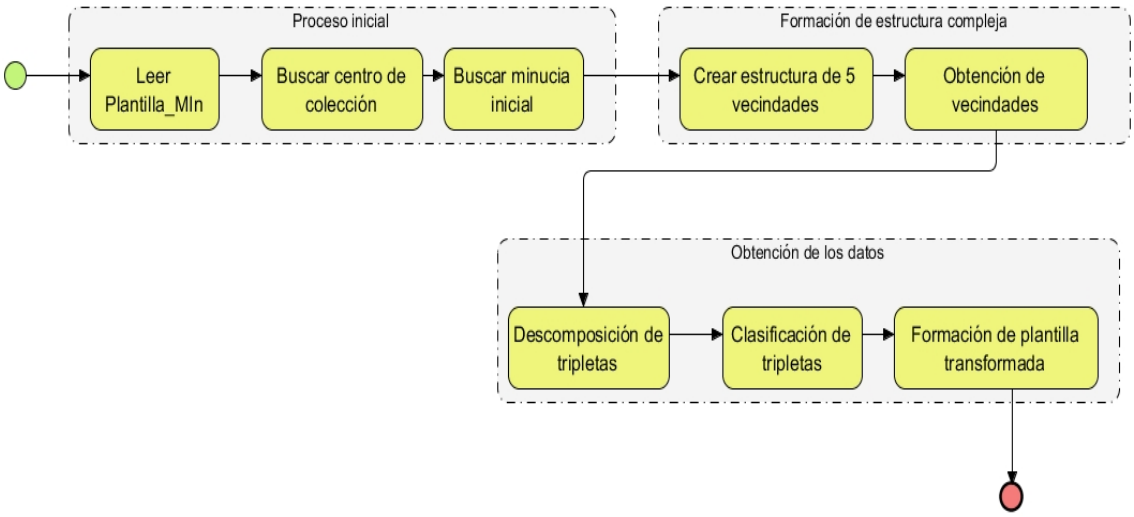
Anexo 1: Representación de los ataques a los modelos de protección de plantillas de minucias de huellas dactilares.



Anexo 2: Enfoques del modelo de protección de plantillas de minucias hash biométrico.

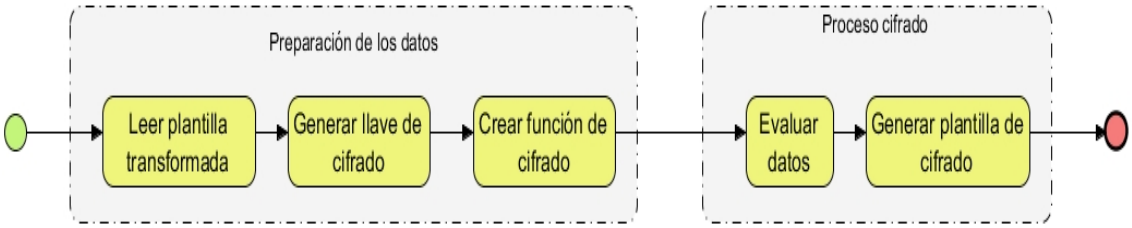
Enfoques del modelo de protección hash biométrico	Modificaciones	Desventajas
Jain, Prabhakar, Hong y Pankanti 1999	Modelo original	No contempla la alineación de los datos. Es dependiente del núcleo de la huella dactilar. Es posible obtener las características originales o un conjunto bastante cercano a las originales mediante la realización de ataques.
Teoh, Ngo, Ling y Goh, 2004	Mejoras en el procesamiento de la imagen.	No contempla la alineación de los datos. Es dependiente del núcleo de la huella dactilar. Es posible obtener las características originales o un conjunto bastante cercano a las originales mediante la realización de ataques.
Belguechi, Rosenberger y Aoudia, 2010	Se elimina la dependencia del núcleo, para la selección de los discos se utilizan las minucias	No contempla la alineación de los datos. Este enfoque es dependiente del proceso de extracción de minucias para formar el vector de longitud fija. Es posible obtener las características originales o un conjunto bastante cercano a las originales mediante la realización de ataques.
Belguechi, Cherrier, Rosenberger y Aoudia, 2013	Se adicionan dos descriptores, uno de textura y uno de minucias. Se utiliza la estructura de minucias n vecindades más cercanas.	Es posible obtener las características originales o un conjunto bastante cercano a las originales mediante la realización de ataques.

Anexo 3: Representación del proceso que ocurre en el componente de representación y extracción de información identificativa a partir de las plantillas de minucias.



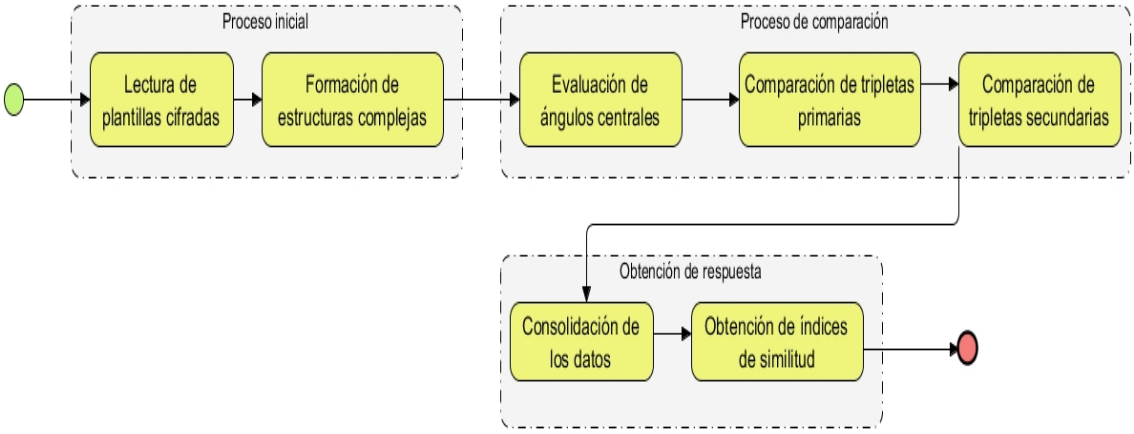
Este proceso tiene como entrada la plantilla de minucias en texto claro y como salida una plantilla que contiene las características extraídas de la estructura compleja.

Anexo 4: Representación del proceso que ocurre en el componente de cifrado de características identificativas.



Este proceso tiene como entrada la plantilla que contiene las características extraídas de la estructura compleja y como salida la plantilla cifrada.

Anexo 5: Representación del proceso que ocurre en el componente de comparación de características identificativas.



Este proceso tiene como entrada dos plantillas en texto cifrado y como salida el índice de similitud entre ambas plantillas.

Anexo 6: Composición de los datos en las bases de datos de prueba

Tabla A1 bases de datos de la FVC2000

Fvc-2000	Tipo de sensor	Imágenes Ancho x alto
DB1_B	Sensor óptico de bajo costo	300 x 300
DB2_B	Sensor capacitivo de bajo costo	256 x 364
DB3_B	Sensor óptico	448 x 478
DB4_B	Sintetizadas por SFinge	240 x 320

Tabla A2 bases de datos de la FVC2002

Fvc-2002	Tipo de sensor	Imágenes Ancho x alto
DB1_B	Sensor óptico	388 x 374
DB2_B	Sensor óptico	295 x 560
DB3_B	Sensor capacitivo	300 x 300
DB4_B	SFinge v2.51	288 x 384

Tabla 3.5 bases de datos de la FVC2004

Fvc-2004	Tipo de sensor	Imágenes Ancho x alto
DB1_B	Sensor óptico	640 x 480

DB2_B	Sensor óptico	328 x 364
DB3_B	Sensor térmico global	300 x 480
DB4_B	SFinge v3.0	288 x 384