DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELETRÓNICA Y TELECOMUNICACIONES

TEMA: COMPARACIÓN DE ESQUEMAS DE BIOMETRÍA CANCELABLE PARA AUTENTICACIÓN DEL IRIS.

AUTOR: GAVILEMA CABEZAS, ANDREA JOHANNA

DIRECTOR: ING. CARRERA, ENRIQUE VINICIO PhD

SANGOLQUÍ

2017

CERTIFICACIÓN

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"COMPARACIÓN DE ESQUEMAS DE BIOMETRÍA CANCELABLE PARA AUTENTICACIÓN DEL IRIS"*** realizado por la señorita ***ANDREA JOHANNA GAVILEMA*** CABEZAS, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditar y autorizar a la señorita ***ANDREA JOHANNA GAVILEMA CABEZAS*** para que lo sustente públicamente.

Sangolquí, 12 de mayo del 2017

ING. ENRIQUE VINICIO CARRERA ERAZO
DIRECTOR

AUTORÍA DE RESPONSABILIDAD

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, ***ANDREA JOHANNA GAVILEMA CABEZAS***, con cédula de identidad N° 1723783583 declaro que este trabajo de titulación ***"COMPARACIÓN DE ESQUEMAS DE BIOMETRÍA CANCELABLE PARA AUTENTICACIÓN DEL IRIS"*** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 12 de mayo del 2017

ANDREA JOHANNA GAVILEMA CABEZAS
C.C.: 1723783583

AUTORIZACIÓN

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, ***ANDREA JOHANNA GAVILEMA CABEZAS***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"COMPARACIÓN DE ESQUEMAS DE BIOMETRÍA CANCELABLE PARA AUTENTICACIÓN DEL IRIS"*** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 12 de mayo del 2017

ANDREA JOHANNA GAVILEMA CABEZAS
C.C.: 1723783583

DEDICATORIA

Para Lucy, Rafa, Alex, Sammy y Charles. En los momentos únicos e importantes de mi vida, ustedes siempre están presenten.

Andrea Johanna Gavilema Cabezas

AGRADECIMIENTO

Agradezco a Dios por ser tan bondadoso conmigo. Me ha bendecido con una familia realmente hermosa y unida. Ha puesto en mi vida a personas muy valiosas, que han sido participes de momentos maravillosos, que han dejado recuerdos invaluables en mi corazón.

Mamita gracias por ser mi ejemplo a seguir, tú y mi papi han sido mi apoyo incondicional. Sammy, Patty y Alex gracias por brindarme tantas alegrías y ser mis cómplices en muchas ocasiones.

Charles gracias por tu amor, paciencia, por ser mi complemento y no permitir que me rindiera en los momentos que pensaba que no lo podía conseguir.

De manera especial quiero dar las gracias a mi Director de tesis el Ing. Vinicio Carrera PhD, sin sus guías y apoyo no lo habría logrado. Gracias por su tiempo y amabilidad.

Andrea Johanna Gavilema Cabezas

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Los sistemas de biometría son una alternativa para realizar los procesos de autenticación e identificación de usuarios. Se basan en la utilización de un rasgo físico o de comportamiento, lo que genera ventajas en comparación a métodos tradicionales tales como claves o tarjetas de identificación. Sin embargo, se tienen inconvenientes en el momento que los rasgos biométricos se ven comprometidos. Para brindar seguridad y privacidad a los usuarios, se aplica una transformación en las plantillas biométricas generadas por los sistemas. Esta transformación se denomina biometría cancelable (CB). En este trabajo se presenta la implementación, evaluación y comparación de dos esquemas de biometría cancelable para reconocimiento y verificación del iris. Las técnicas que se consideraron para los esquemas fueron: Gray-Combo que hace referencia a una transformación no invertible y la asignación de un *token* a cada usuario. Por otra parte, se empleó la metodología Bin-Salt que es un enfoque *salting*, es decir utiliza un patrón artificial extra que se combina con las plantillas biométricas de los usuarios para producir su modificación. Los esquemas de biometría cancelable fueron evaluados considerando ocho criterios, que estimaban la robustez, el cumplimiento de las propiedades (rendimiento, irreversibilidad, diversidad e imposibilidad de vinculación) y a que ataque son más vulnerables los sistemas.

PALABRAS CLAVE:

- **BIOMETRÍA CANCELABLE**
- **RECONOCIMIENTO DEL IRIS**
- **GRAY-COMBO**
- **BIN-SALT**

ABSTRACT

Biometric systems are an alternative to perform the processes of authentication and identification of users. They are based on the use of a physical or behavioral trait, which generates advantages compared to traditional methods such as keys or identification cards. However, there are drawbacks at the moment that the biometric traits are compromised. To provide security and privacy to users, a transformation is applied to the biometric templates generated by the systems. This transformation is called cancelable biometrics (CB). This paper presents the implementation, evaluation and comparison of two cancelable biometrics schemes for recognition and verification of the iris. The techniques that were considered for the schemes were: Gray-Combo that refers to a non-invertible transformation and the assignment of a token to each user. On the other hand, the Bin-Salt methodology, which is a salting approach, uses an extra artificial pattern that is combined with the users' biometric templates to produce their modification. The cancelable biometrics schemes were evaluated considering eight criteria, which estimated the robustness, the compliance of the properties (yield, irreversibility, diversity and impossibility of linking) and to which attack systems are most vulnerable.

KEYWORDS:

- **CANCELABLE BIOMETRICS**
- **RECOGNITION IRIS**
- **GRAY-COMBO**
- **BIN-SALT**

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. Antecedentes

El Subcomité de Biometría del Consejo Nacional de Ciencia y Tecnología (NSTC) define a la biometría como un término que se emplea para detallar un atributo o un proceder, que se puede emplear para un sistema de identificación de personas. Los esquemas biométricos posibilitan la autenticación y reconocimiento de la identidad de una persona, haciendo uso de alguna de sus peculiaridades de comportamiento o rasgos físicos, únicos y propios de cada individuo. La autenticación o verificación consiste en comprobar quien dice ser tal persona. Por otra parte, los sistemas biométricos de igual forma realizan el proceso de reconocimiento o identificación, que se base en definir si la identidad de una persona pertenece a cierta base de datos.

Los sistemas de biometría constan de tres etapas: inscripción, almacenamiento y comparación. Durante la inscripción se extraen, procesa y modelan las características más significativas del rasgo seleccionado; las plantillas que por primera vez fueron procesadas tienen el nombre de plantillas originales o plantillas de referencia. En la segunda etapa estas plantillas se almacenan en una base de datos. Mientras que en la última fase, se extrae una nueva plantilla biométrica, que es llamada plantilla de consulta; la cual se compara con los datos ya almacenados. Si la comparación es exitosa, el usuario queda autentificado o identificado; de lo contrario, será rechazado por el sistema (Duró, 2001).

Para que los rasgos biométricos sean aptos para ser empleados en sistemas de biometría, además de ser características diferentes para cada individuo, deben ser permanentes e invariantes (Aguilera, 2012). Estas características generan ventajas en comparación con otros métodos de reconocimiento y verificación. Los rasgos no se pueden perder u olvidar, como

es el caso del uso de una contraseña. Asimismo la falsificación de rasgos biométricos es un proceso complejo, haciendo de la presencia del usuario un requisito indispensable para su identificación (Gayoso, 2014).

A pesar de sus ventajas, las plantillas biométricas manifiestan vulnerabilidad. En el caso de que un rasgo fisiológico se vea comprometidos no puede ser invalidado y reemplazado; ocasionando incertidumbre sobre la seguridad y privacidad de los sistemas biométricos. Se presenta a la biometría cancelable como una alternativa para brindar privacidad y protección a los datos biométricos.

Este método consiste en provocar una distorsión deliberada en la plantilla de referencia generando un biocódigo; empleando una función y/o clave, esté proceso debe ser no reversible; así se evitará vincular la identidad del usuario con el patrón generado por el rasgo seleccionado (Pillaj, 2010). La Organización Internacional de Normalización (ISO), en la norma ISO/IEC 24745 define cuatro propiedades que deben satisfacer los esquemas de biometría cancelable “revocabilidad/renovación, rendimiento, no irreversibilidad y diversidad o imposibilidad de vinculación”.

Dos tipos de biometría cancelable se distinguen, dependiendo de las propiedades de la función que se emplee para provocar la alteración en la plantilla de referencia, son: *salting* y función no invertible. En *salting*, la plantilla original se combina con otra platilla auxiliar para formar un biocódigo, que servirá de nueva referencia para el usuario. En contraste, el enfoque de función no invertible, utiliza solamente la información proporcionada por la plantilla original para provocar la distorsión y así producir el biocódigo (Jain A. K., 2008).

Entre los datos de esquemas biométricos, el patrón del iris es uno de los más prometedores en comparación con otros rasgos fisiológicos. Dúro (2001) menciona que de acuerdo a investigaciones desarrolladas por ingenieros y biólogos, el iris posee propiedades “morfológicas perfectamente circulares que presenta las propiedades matemáticas más individuales y únicas”. El patrón de cada individuo es utilizado para individualizar, autenticar o reconocer en los sistemas de identificación.

Dentro de los métodos de identificación no intrusivos el uso de sistemas biométricos es cada vez más frecuente, lo cual ha generado varias publicaciones a cerca de la seguridad y protección de plantillas biométricas de rasgos fisiológicos. Para los esquemas propuestos en la literatura, comúnmente se usa como medida de desempeño *False Acceptance Rate (FAR), False Reject Rate* (FRR), *Equal Error Rate* (EER), además estudian la seguridad estableciendo diversos escenarios de prueba. La valoración de técnicas o métodos de biometría cancelable es un campo amplio de investigación, puesto que no se ha establecido una metodología estándar hasta el momento (Belguechi R. C., 2011).

1.2. Justificación e Importancia

Contraseñas, número de identificación, tarjetas e identificadores de usuarios son empleados como métodos de autenticación; no obstante, tienen ciertas limitaciones, pues pueden ser robados o extraviados. Estos aspectos cuestionan su conveniencia al usarlos en aplicaciones para acceso a información restringida como, datos bancarios, médicos, o pagos con tarjeta de crédito, entre otras aplicaciones (García J. O., 2008).

Otro aspecto inquietante se genera frecuentemente cuando un usuario debe crear una clave, selecciona palabras o números que pueden ser descubiertos sin mucho esfuerzo. Por ejemplo, elijen su propio nombre, el de un familiar o de su mascota como contraseña de acceso. Se recomienda emplear diversas contraseñas para varias aplicaciones, modificarlas cada cierto tiempo, combinar letras y números, así como usar una contraseña larga; mientras más simple o sencilla sea la contraseña se tiene mayor probabilidad de que un ataque tenga éxito (García J. O., 2008).

Una técnica más precisa y fiable son los sistemas de biometría automatizados. Los rasgos físicos empleados en biometría son peculiares para cada persona, se dificulta su duplicidad (Ratha N. K., 2001). De esta forma se pretende que estos recursos sean asequibles únicamente por usuarios registrados en el sistema de biometría (García J. O., 2008).

La información que se adquiere de un rasgo biométrico, puede estar contenida en una gran cantidad de bytes, proporcionando una ventaja en comparación con una clave. La longitud de una contraseña es proporcional a la segura seguridad que proporciona, al igual que la dificultad de recordarla y tiempo para escribirla sin ningún error. El uso de biometría puede generar ventajas de seguridad, al igual que una contraseña extensa, con la sencillez de una clave corta (Ratha N. K., 2001).

Hoy en día la utilización de los modelos biométricos tiene gran demanda, puesto que es indispensable identificar a un usuario de algún sistema, ya sea para otorgarle algún privilegio o restricción, verificar su asistencia, entre otras aplicaciones. Así mismo, los sistemas de biometría facilitan la identificación de un persona que se ha inscrita varias veces, como es el caso de un individuo que tiene varios DNIs con algunas identidades; deducir este tipo de irregularidades es un proceso complejo, si se utilizan métodos diferentes a biometría. Un sistema biométrico previene y detecta, a un sujeto que desea registre más de una vez. Adicionalmente estos sistemas son empleados en aplicaciones de vigilancia, por ejemplo en seguridad pública o forense, proporcionando mayor agilidad en estos procesos además de ser una ayuda al personal de seguridad (García J. O., 2008).

No obstante, los sistemas de biometría que no son usados como una técnica de autenticación o reconocimiento supervisado; es decir aplicaciones a distancia pueden presentar cierta vulnerabilidad, que genera un peligro para los datos de los usuarios, pues los intrusos pueden tener la oportunidad de generar un ataque al sistema, antes de ser detectados; poniendo en amenaza la privacidad de información que se encuentran almacenada. Los sistemas de reconocimiento y autenticación establecidos en biometría a pesar de sus ventajas también se ven afectados, visto que varios rasgos biométricos pueden ser grabados sin el consentimiento del usuario. Por añadidura estas singularidades no pueden ser extraídas, pues son rasgos asociados de manera permanente al usuario (Ratha N. K., 2001).

La privacidad y seguridad de la información de los rasgos físicos es un constituyente fundamental para la aplicación de un sistema biométrico,

debería ser complicado o improbable para un intruso evadir la protección de un sistema; ya que es posible restablecer la información de una plantilla de almacenada, lo que conlleva a suplantación de identidad, además de poner en riegos la estabilidad de otros sistemas, donde se puede acceder con la información robada.

Varios enfoques en proponer protección y seguridad se han planteado, uno de ellos es el método de biometría cancelable (Hämmerle-Uhl, 2009). En estos esquemas la plantilla referencia creada a partir de un rasgo fisiológico, puede ser transformado en caso de que el rasgo se vea comprometido. Este procedimiento de protección de plantillas biométricas debe contar con propiedades que garanticen su robustez.

Los estudios con respecto a esquemas de biometría cancelable, se han centrado en plantear algoritmos para optimizar métricas para la identificación a través del iris, de los cuales se obtiene resultados apropiados. A pesar de ello, surgen nuevos campos de estudio, vinculados con seguridad y privacidad de los datos reservados. Es indispensable que los usuarios tengan la convicción de que las plantillas almacenadas no compromete su información personal, además la fianza del sistema es importante en caso de que exista algún tipo de ataque (Zamudio, 2010).

Examinar posibilidades de vulnerabilidad en los sistemas es fundamental, este trabajo estudia y evalúa cuantitativamente la robustez de un método de cada tipo de biometría cancelable empleando el patrón del iris. Hasta la fecha, este tema ha sido poco tratado en esta modalidad de biometría. Por esta razón, la estimación del cumplimiento de las propiedades de los sistemas, considerar un enfoque cuantitativo es un aporte significativo, pues facilita su comparación.

Se decidió evaluar sistemas de identificación del iris, ya que es un rasgo que dispone de preeminencias sobre otros identificadores biométricos, entre ellas esta su simple proceso de registración, debido a que no es necesario tener contacto físico con el usuario para obtener una imagen digital, se puede realizar considerando cierta distancia. Asimismo, por los estudios realizados,

se dice que el iris no sufre ningún prejuicio en estos métodos, por lo que sus porcentajes de aceptación son buenos.

1.3. Alcance

En este trabajo se evalúa dos esquemas de biometría cancelable para autentificación e identificación del iris. Utilizando las técnicas existentes se implementa los dos esquemas para autenticación y reconocimiento del iris, en la herramienta de *software* MATLAB y utilizando como referencia la base de datos CASIA_IrisV1, que contiene un total de 756 imágenes del iris de 108 personas. Esta base datos biométrica proporciona diversas muestras por usuario, lo que permite generar plantillas de referencia y plantillas de consulta.

Inicialmente se lleva a cabo un sistema de biometría sin ninguna variación, para tener una referencia de rendimiento. Se considera lo expuesto en (Masek, 2003), para los métodos de segmentación, normalización, codificación y cuantificación. Con el fin de obtener la alteración en las plantillas de referencia, se implementa dos funciones de transformación mencionadas en (Zuo, 2008), Gray-Combo y Bin-Salt. Gray-Combo refiere a una función no invertible, por consiguiente utiliza únicamente la información proporcionada por el iris del usuario para realizar la distorsión. Por otra parte, Bin-Salt emplea un patrón aleatorio para provocar la alteración y representa un método *salting*.

Las métricas consideradas para la evaluación de la robustez de los sistemas de biometría cancelable son los ocho factores planteados en (Belguechi R. C., 2012), donde sugiere una nueva metodología para la valoración de los métodos; se examinan las propiedades de: eficiencia o usabilidad, no invertibilidad y diversidad. El enfoque cuantitativo permite la clara comparación de los esquemas biométricos, de igual manera se verifica su privacidad y seguridad.

1.4. Objetivos

1.4.1. General

- Estudiar dos esquemas de biometría cancelable para la autenticación y reconocimiento de una persona, empleando el iris como rasgo fisiológico.

1.4.2. Específicos

- Analizar, elaborar y evaluar un sistema de biometría usando el iris, para su identificación y verificación.
- Examinar e implementar dos esquemas de biometría cancelable.
- Definir y valorar las propiedades de seguridad y privacidad de cada sistema implementado.
- Considerar los resultados obtenidos de la cuantificación de la robustez de los esquemas propuestos, para sugerir una alternativa fiable al usuario.

1.5. Estudio del estado del arte

Gracias al avance de la tecnología, esencialmente el procesamiento digital de señales, los sistemas biométricos se han puesto a disposición para la identificación de personas. El termino Biometría procese de dos vocablos griegos “bio” y “métrica” que quieren decir vida y medir. No obstante, el fundamento de los métodos aplicados en estos esquemas data de millones de años atrás, puesto que los seres humanos usaban los rasgos faciales para identificar personas conocidas o identificar a extraños. Así mismo, características como el tono de voz, forma de caminar, ayudaban a distinguir a los individuos (NSTC Subcommittee on Biometrics, 2006).

Más adelante, en la década de 1980, fue indispensable establecer un método de identificación de personas, debido al continuo incremento en la población. En Francia, se implantó un sistema para distinguir la identidad de

los presos, así sabrían que medida de justicia tomar si es un infractor constante. Alphonse Bertillon plantea un procedimiento haciendo uso de métricas fisiológicas, como por ejemplo la longitud de alguna extremidad, estatura, entre otras. Este acontecimiento da cabida al estudio y desarrollo de nuevos métodos, generando un campo denominado antropometría. Una nueva perspectiva fue presentada por Edward Henry, empleando huellas dactilares, que se usó en el departamento de policía en Bengala India (Zamudio, 2010).

La noción de valerse del iris como un rasgo biométrico fue manifestada por Leonard Flom y Aran Safir en 1985, definieron que dos irises no son idénticos. Más tarde, en el año 1987 proponen una de las primeras técnicas de reconocimiento del iris, sugiriendo diversas fases para su implementación. El sistema era un boceto que necesitaba la interacción de un operador, lo cual hacia al sistema semiautomático (United States Patente nº US4641349 A, 1987). El desarrollo de procedimientos biométricos automatizados se intensificó en la década de 1990. John Daugman en 1994, origina una patente exponiendo una forma automática para el reconocimiento del iris, describe diferentes partes del sistema funcional, que van desde la adquisición de la imagen, a la toma de decisión para la identificación (United States Patente nº 5,291,560, 1994). Otra perspectiva es publicada por Richard Wildes en 1997, empleando un mayor número de recursos computacionales (Kaur, 2014).

En la década de los 2000 el uso de sistemas biométricos se acrecentó para identificación de personas, se mostraba como una mejora y complemento a los métodos ya establecidos, como claves, identificaciones, entre otros (Kaur, 2014). No obstante, presenta ciertas vulnerabilidades, esta problemática fue presentada por Ratha, Connelle y Bole en el año 2001; donde se menciona diversos puntos de susceptibilidad, conjuntamente se incluye la definición de biometría cancelable (Ratha N. K., 2001).

En el 2008, Zuo, Ratha y Connell plantean cuatro técnicas para esquemas de biometría cancelable que se basan en sistemas de identificación de iris tradicionales. En los dos primeros métodos se emplea solo la información biométrica para provocar la distorsión en las plantillas de

referencias y de consulta, mientras en los otros dos métodos se emplean además información adicional (Zuo, 2008).

Surgen interrogantes sobre la privacidad de los datos biométricos que se encuentran almacenados y la eficiencia de los sistemas. Varios autores usan para la evaluación del rendimiento de sus sistemas fórmulas como EER o ROC. Para estudiar la seguridad establecen distintos escenarios de prueba. Belguechi, Cherrier y Rosenberger en 2012 plantean ocho métricas para evaluar la privacidad y seguridad de una técnica de biometría cancelable, a través de un enfoque cuantitativo (Belguechi R. C., 2012).

1.6. Descripción de capítulos del proyecto

En el capítulo 2 se menciona el fundamento teórico de biometría, dando una introducción a los sistemas de biometría. Se indican las técnicas desarrolladas para cada etapa de los sistemas de biometría (segmentación, normalización, codificación y comparación) para identificación y verificación del iris; así mismo se muestran las técnicas de biometría cancelable. Además se señalan los parámetros de evaluación de estos esquemas.

En el capítulo 3 se explica de manera detallada la metodología y técnicas que se emplearon para el sistema de biometría y los esquemas de biometría cancelable.

En el capítulo 4 se muestran y analizan los resultados obtenidos de las pruebas realizas para evaluar los sistemas desarrollados.

Finalmente, en el capítulo 5 se exponen las conclusiones y trabajos futuros.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Biometría

La fisonomía del rostro, ojos, huellas dactilares son algunas de las particularidades morfológicas que poseemos las personas, que nos permiten distinguirnos de otros seres humanos. El Subcomité del Consejo Nacional de Ciencia y Tecnología (NSTC) y las normas internacionales (ISO/IEC JTC1 SC37), estipulan que la palabra biometría se puede emplear como una propiedad o un procedimiento; es una propiedad fisiológica y anatómica, así como de conducta que se pueden medir. Biometría también se entiende como un procedimiento automatizado para la identificación de una persona (NSTC Subcommittee on Biometrics, 2006).

2.2. Rasgos biométricos

Una característica biométrica puede ser de conducta o biológica. Un rasgo biométrico de comportamiento se asimila o se consigue con el tiempo. Un ejemplo de ello es la manera en la que pulsamos las teclas. Desde otra perspectiva están las características fisiológicas o anatómicas. Huellas dactilares son tomadas como rasgos biométricos fisiológicos. Para el uso de una particularidad en un sistema biométrico se consideran ciertas propiedades que deben cumplir (Maltoni, 2009):

- **Universalidad:** Está presente en todos los individuos.
- **Unicidad:** Cada persona tiene peculiaridades biométricas que las distingue de los demás.
- **Permanencia:** El tiempo no debe influir en el rasgo biométrico.
- **Mensurabilidad:** Las características del rasgo se debería poder medir.
- **Aceptabilidad:** Tiene un alto grado de aceptación entre los usuarios.

- **Rendimiento:** Permite distinguir a las personas, considerando una baja tasa de error.
- **Evitabilidad:** Rechazo a ser evadido o engañado.

2.2.1 Anatomía del órgano de la visión

El órgano de la visión tiene como objetivo interpretar los cambios electromagnéticos de la luz en una específica clase de impulsos nervosos que se transfieren al cerebro. El globo ocular y el nervio óptico constituyen este órgano. El globo ocular es comúnmente llamado ojo, su forma es esférica, está constituido por tres revestimientos. La esclerótica es la cubierta externa, su cometido es brindar protección. En la membrana media se encuentra la úvea, que contiene a la coroides, el cuerpo circular y el iris. Finalmente está la retina en la parte más interna del ojo; es perceptible a la luz (Tomé G., 2008). En la figura 1, se muestra la estructura del globo ocular.

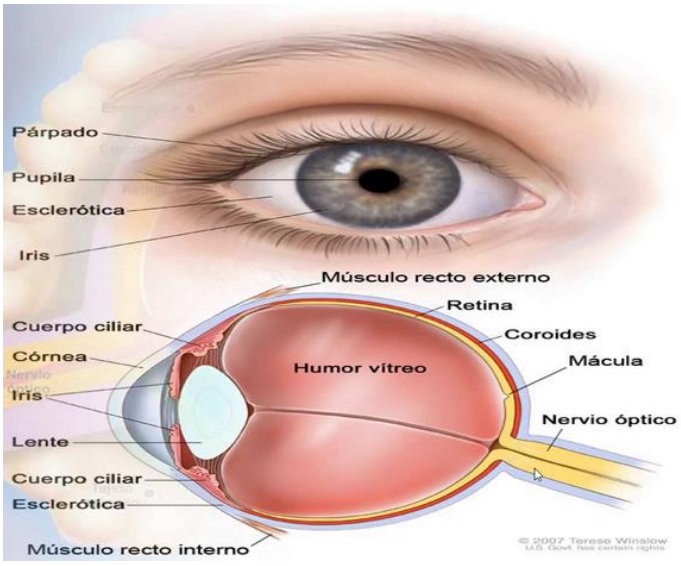

Figura 1. Estructura del globo ocular

Fuente: Terese Winslow © 2007

2.2.2 Iris

En el periodo de gestación, el iris del feto se desarrolla dentro del vientre materno comprimido a la membrana del tejido; el iris toma patrones

singulares, provocados por degradación al terminar la etapa prenatal. Las peculiaridades de los patrones que presenta el iris no están genéticamente ligados, lo contrario sucede con coloración y estructura (Vega, 2011).

El iris tiene una estructura en capas. La primera capa opaca la luz, tiene color negro violáceo. La capa posterior está conformada por músculos de dilatación, que facilitan las acciones de expansión y disminución; también está presente el esfínter. El siguiente estrato se encuentra unido a tejidos que está compuesto de melanocitos y colágeno. La capa exterior es más colorida y es más densa en comparación con las demás capas; mientras mayor sea la pigmentación en esta capa, la persona tendrá un iris más oscuro; en escasa pigmentación el iris tomará una coloración azul, producida por la coloración de la primera capa (Ganorkar, 2007). El iris ajusta el tamaño de la pupila para permitir que cierta cantidad de luz ingrese al ojo (Vega, 2011).

Según especialistas, el iris es catalogado como una característica biométrica con propiedades morfológicas únicas e individuales (Duró, 2001). Es un rasgo fisiológico que se encuentra alrededor de la pupila y está rodeado por la esclerótica. Se estima que el iris mantiene su estructura y propiedades constantes la mayor parte de la vida del ser humano. Cada persona posee diferentes patrones de iris. Asimismo se dice que el iris derecho e izquierdo de una persona son diferentes (Bowyer, 2008).

2.3. Sistemas de biometría

Un sistema biométrico permite la verificación e identificación de una persona, aplicando técnicas automáticas. Fiabilidad, aceptabilidad y desempeño son propiedades que deben cumplir. Con la fiabilidad se garantiza que es complicado engañar al sistema. De igual modo, su uso deberá ser sencillo e inspirar convicción en los usuarios, esto se refleja en la aceptabilidad que tiene el sistema. Otros requerimientos significativos son la precisión y el tiempo que se demora en el proceso de identificación, con ello se podría definir su desempeño (Hernández, 2009).

La autenticación en base a biometría utiliza técnicas capaces de adquirir, pre-procesar, extraer particularidades, codificar, cuantificar, comparar

determinado rasgo de un sujeto. Lo cual constituye una alternativa al uso de contraseñas, identificaciones u otro método identificación que pueden ser robados, transferidos, copiados o descifrados por personas ajenas al sistema.

Los esquemas automatizados de reconocimiento biométricos están conformados por diversas etapas que varían según el tipo de rasgo que se emplea. Principalmente se divide en dos secciones, la primera corresponde a la interfaz de usuario, el usuario interactúa exclusivamente con el sensor, que registrara su patrón biométrico. Mientras que en la segunda división se encuentran las herramientas de hardware o software que permiten el procesamiento del sistema (Tomé G., 2008). En la figura 2 se presentan los módulos que conforman un sistema de biometría.

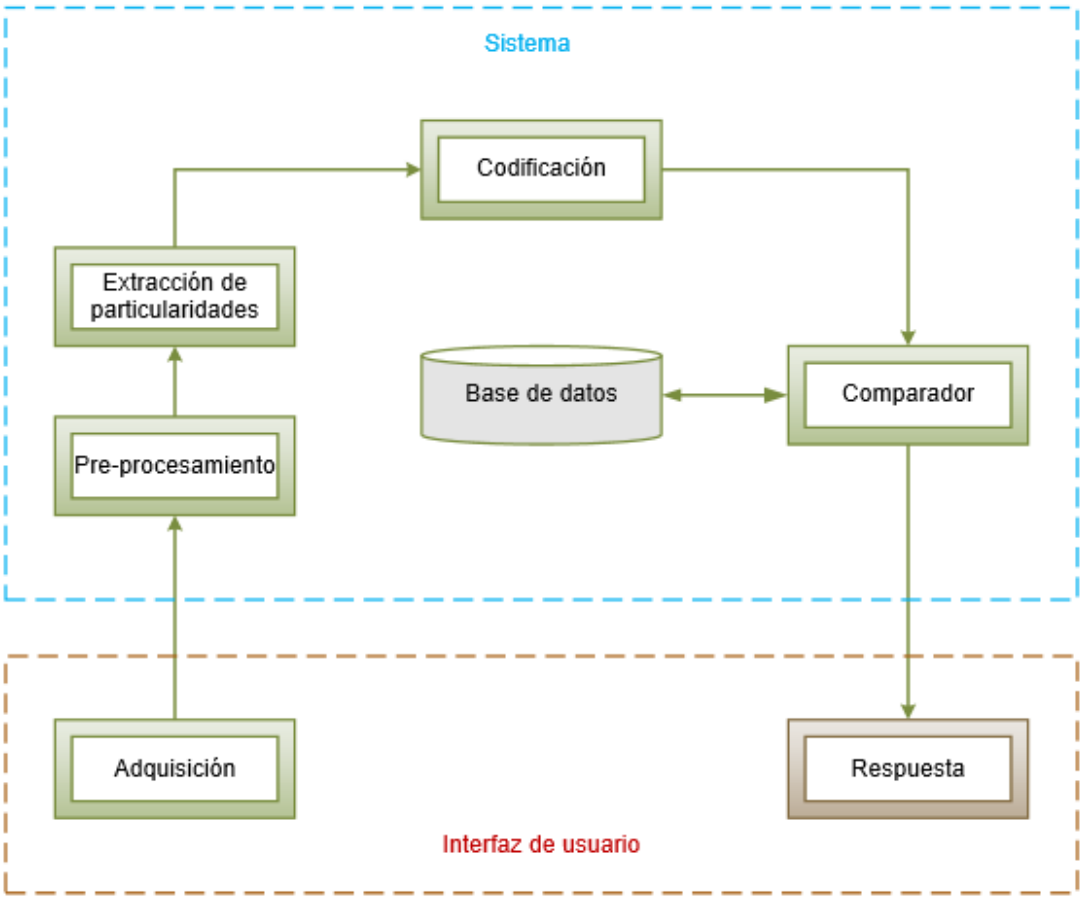

Figura 2. Esquema de componentes de un sistema biométrico

A continuación se mencionan algunas características de las etapas del sistema de identificación biométrico.

- **Adquisición de información:** Mediante un sensor se toman datos en formato digital. Esta sección es fundamental tener en consideración la cantidad y calidad de información adquirida, pues influyen en el desarrollo de las siguientes etapas.
- **Pre-procesamiento:** Para tener un buen rendimiento del sistema, a la información adquirida se la debe acondicionar en ciertas ocasiones, para excluir distorsiones provocadas al momento de su obtención.
- **Extracción de particularidades:** En esta etapa se extraen las singularidades, desechando la información que no servirá de referencias para el procedimiento de identificación.
- **Codificación:** Una modelo de plantilla se genera, codificando la información más discriminatoria.
- **Comparación de plantillas:** La comparación se realiza entre las plantillas que se encuentran almacenados en la base de datos del sistema y la plantilla generada de las características extraídas en las fases anteriores.

2.3.1. Sistema de biometría para reconocimiento del iris

El sistema de reconocimiento del iris consta de varias etapas, que van desde la adquisición de una imagen digital del iris, hasta la autenticación o reconocimiento de un usuario. Es necesario un pre-procesamiento de la imagen, extracción de particularidades, procesamiento y por último su comparación (Santos, 2008). Estas etapas fueron descritas en el capítulo anterior de manera general, es por eso que en esta sección se especifican para el reconocimiento del iris. Se observa en la figura 3 los módulos del esquema de biometría para reconocimiento del iris. Cabe señalar, que la etapa de extracción de particularidades se divide en segmentación y normalización.

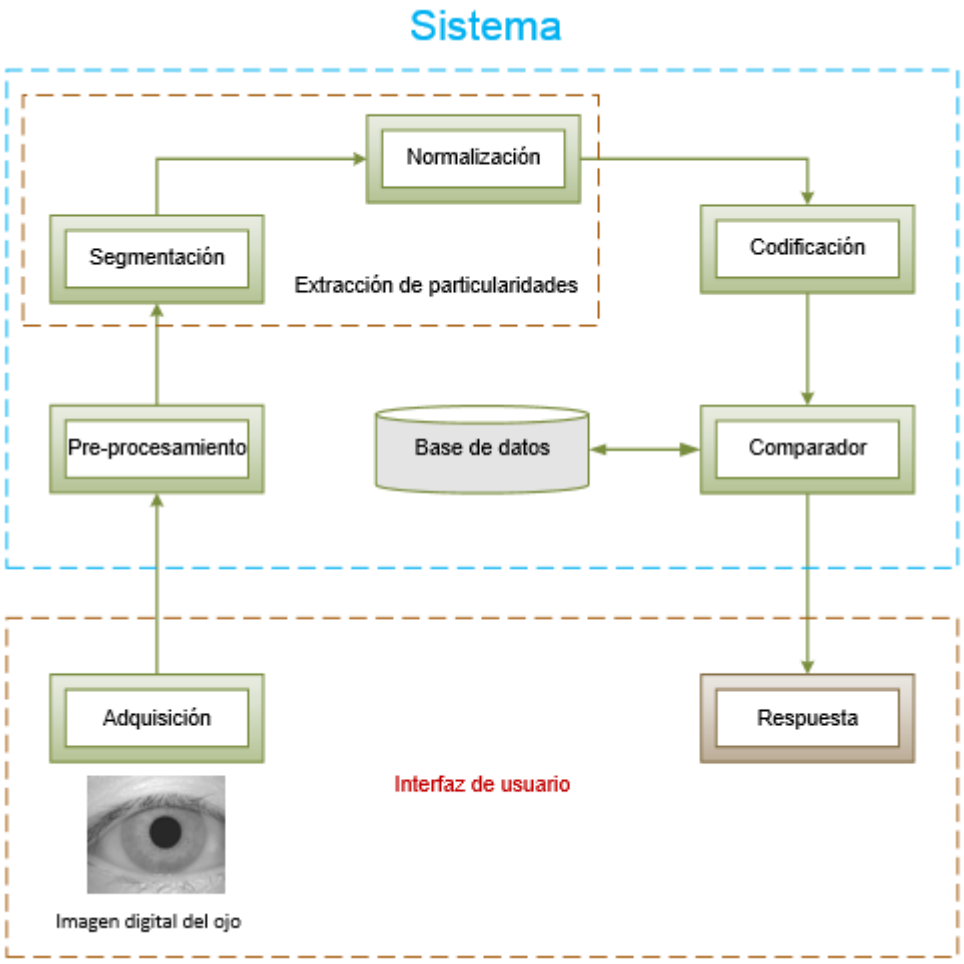

Figura 3. Etapas de un sistema biometría para reconocimiento del iris

2.3.1.1. Segmentación del iris

El proceso de segmentación del iris es fundamental para su identificación, visto que es donde se determina el área de imagen que será usada en las siguientes etapas del esquema (He, 2009). En esta etapa se busca localizar y aislar al iris, además de excluir la presencia de parpados y pestañas que pueden estar presentes en la región del iris. De la calidad de la imagen adquirida depende el óptimo proceso de segmentación (Masek, 2003).

Diversas técnicas de segmentación consideraban que el iris está delimitado por dos círculos, uno que borde con la esclerótica y el otro que limita con la pupila. No obstante, nuevos estudios señalan que el iris no es

absolutamente circular y sus bordes podrían no estar bien delimitados (Tomé G., 2008).

La transformada de Hough permite la identificación de patrones en una imagen digital (López, 2012). La noción fundamental es localizar curvas que permitan ser parametrizadas como polígonos, círculos y líneas. Es posible especificar analíticamente un fragmento de línea en diversas configuraciones (Duque, 2004).

En distintas propuestas de esquemas de reconocimiento del iris, la transformada de Hough circular ayuda a encontrar el radio y el punto céntrico de los círculos formados por el iris y la pupila. Para ello es necesario un pre-procesamiento, para establecer un mapa de contornos, calculando las primeras derivadas de las intensidades de la imagen adquirida del ojo; después se determinan los parámetros para definir un círculo, mediante la ecuación 2.1 (Masek, 2003).

$$x_c^2 + y_c^2 - r^2 = 0 \qquad (2.1)$$

El principio de la transformada de Hough circular, considera un punto de referencia, por el cual se trazan un número indefinido de rectas y círculos; al aplicar este algoritmo en una imagen, existe un decremento del número de rectas y círculos, debido a que las pendientes de las rectas, radios y centros de los círculos son restringidos por la conformación del espacio de la imagen (mapa de bordes).

Para la localización de los círculos, se tiene como referencia todos los posibles puntos céntricos, para ello se consideran los puntos blancos presentes en la imagen, de los cuales se trazan una circunferencia, considerando el rango de los radios determinados, así mismo se genera un vector donde se guardan los puntos céntricos, radios y la cantidad de puntos blancos de la imagen que concordaron con la localización del circulo trazado. Después de corroborar por completo el rango de radios, se destacan los puntos máximos, los cuales manifiestan una aproximación del círculo buscado (Rabie, 2008).

El parpado superior e inferior se pueden representar como líneas, la transformada de Hough lineal es usada para su localización. Se estable un valor de umbral para distinguir que región pertenece al parpado, de igual manera, las líneas antes establecidas, deben estar fuera del área de la pupila (Masek, 2003).

2.3.1.2. Normalización del iris

Una vez finalizado el proceso de segmentación del iris, se lleva a cabo la etapa de normalización. Normalización se entiende como homogeneizar la sección segmentada del ojo; la posición y tamaño de la pupila no son constantes en las imágenes adquiridas, estos y otros factores alteran el tamaño del iris, es por eso que es imprescindible esta fase, permitiendo así su comparación (Rabie, 2008). En el proceso de normalización se obtendrán imágenes de iris con iguales medidas; las imágenes de un mismo iris poseerán semejantes propiedades espaciales (Cruz, 2006).

Daugman propuso el modelo uniforme "*rubber sheet*", en el cual a todos los puntos del iris (x, y) se les atribuye dos coordenadas (r, θ), el ángulo θ tiene un rango $[0, 2\pi]$, el radio r tiene valor de 1 o 0. La ecuación 2.2 representa a la imagen del iris en coordenadas polares no concéntricas $I(r, \theta)$; con los puntos que conforma el límite interior y exterior del iris, se hallan combinaciones lineales, que se representan con $x(r, \theta)$ y $y(r, \theta)$ (Cruz, 2006).

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \tag{2.2}$$

Considerando las coordenadas de límite entre la pupila y el iris $(x_P, y_P, x_{I,}, x_I)$ se tiene:

$$x(r, \theta) = (1 - r)x_p(\theta) + rx_l(\theta) \tag{2.3}$$

$$y(r, \theta) = (1 - r)y_p(\theta) + ry_l(\theta) \tag{2.4}$$

La expansión de la pupila, así como el inconstante tamaño de la imagen se consideran en este método de normalización (Tomé G., 2008).

2.3.1.3. Codificación del iris

En vista que se ha concluido el proceso de segmentación y normalización, es factible codificar la información biométrica, que permitirá reconocer o autentificar a un sujeto. Previamente se señalaba que los patrones del iris lo hacen particular para distinguirlo, la codificación es donde se expone la caracterización de la textura del iris (Rabie, 2008). Teniendo como resultado una plantilla, que contiene la mayor cantidad de información distintiva del iris (Tomé G., 2008).

Un filtro de Gabor de una dimensión se establece al multiplicar un coseno que representa el término par y seno es la parte impar, de una onda con una ventana gaussiana. Los filtros Gabor facilitan la representación tanto en espacio como en frecuencia. Una señal se descompone al usar un par de cuadraturas de filtros se Gabor, la modulación de un coseno con una gaussiana generan la parte real, conocida también como simetría par, mientras que la modulación de un seno con una gaussiana proporcionan parte imaginaria entendida como parte simétrica impar (Masek, 2003).

Daugman utiliza los filtros de Gabor de dos dimensiones para codificar las características de la textura del iris. En este método la salida de los filtros de Gabor se demodula, compactando así los datos. Para lo cual se cuantifica la información, fijando cuatro niveles como referencia, que corresponden a los cuadrantes del plano complejo. Dos bits de la plantilla biométrica resultante hacen referencia a cada píxel normalizado del iris (Tomé G., 2008).

2.3.1.4. Comparación

Dado que las particularidades del iris se extraído, se las comparará con los patrones o plantillas antes almacenadas en la base de datos del sistema. Es fundamental señalar que no es una comparación binaria, se trata de obtener un porcentaje de semejanza, pues debido a disparidad de las plantillas correspondientes del mismo iris, pueden se provocada por una alteración en el proceso de captura de las imágenes. Es por eso que se estable un umbral de tolerancia, para realizar la etapa de comparación (Marín, 2009). Distintas

técnicas de comparación se han planteado, en los cuales se consideran algunas etapas, primero se busca alinear los patrones que se van a comparar, luego se extraen sus características, para evaluar su similitud y así obtener una decisión de reconocimiento (Tomé G., 2008).

La distancia de Hamming (HD) establece la suma de bits distintos de dos plantillas X e Y. Es la suma de la OR-exclusiva (XOR) de las dos plantillas, como se muestra en la ecuación 2.5. Donde N es el número de todos los bits de la plantilla del iris (Tomé G., 2008).

$$HD = \frac{1}{N}\sum_{i=1}^{N} X_j(XOR)Y_j \tag{2.5}$$

La HD de dos plantillas biométricas del mismo iris será cercana a 0, pues los bits son semejantes, es decir los patrones son en gran medida correlacionados. Por otra parte, si los bits de dos plantillas son todos independientes, la HD tendera a $0{,}5$, ya que la mitad de bits concuerdan y los otros estarán en desacuerdo, es el caso de comparar patrones de distintas personas (Tomé G., 2008).

2.3.2. Modalidad de funcionamiento

Un sistema biométrico puede emplearse de dos maneras: verificación o autenticación y reconocimiento o identificación (Jain A. K., 2004). El proceso de registro de usuarios tanto para verificación e identificación se realizan de la misma forma. Consiste en extraer las singularidades de una persona en una plantilla biométrica, así como guardarlas. En la figura 4 se distinguen las etapas para inscribir a un usuario.

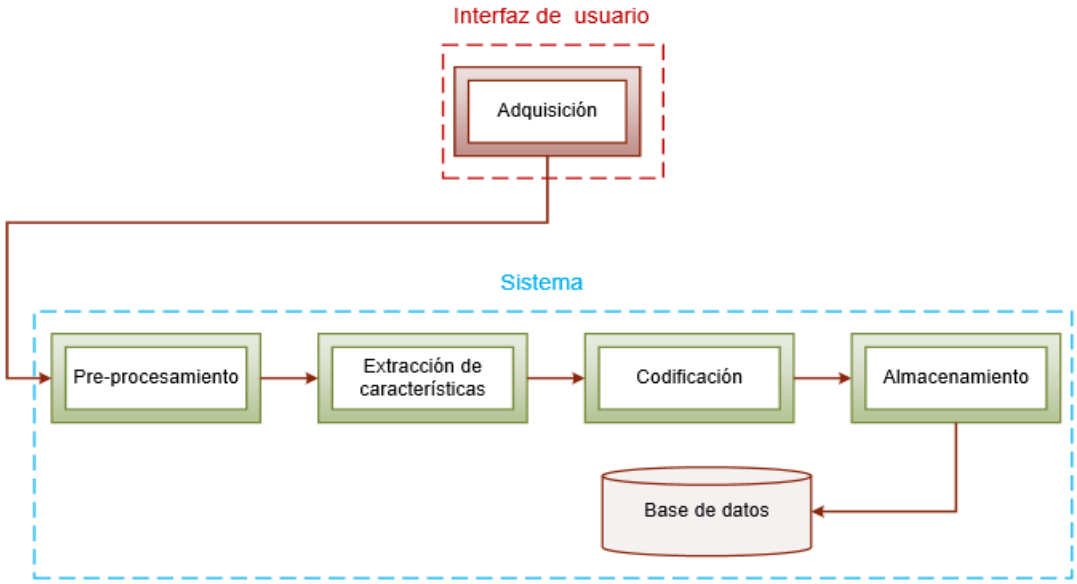

Figura 4. Esquema de etapas de inscripción de usuarios

En el procedimiento de inscripción o registro, los usuarios únicamente participan en la fase de adquisición; en la cual proporcionan una muestra digital del rasgo biométrico. Para producir una plantilla biométrica de las particularidades de cada sujeto perteneciente al sistema, se completan las etapas de pre-procesamiento, extracción y codificación. En la fase de almacenamiento el sistema designa automáticamente un ID o número de identificación; así mismo, establecen privilegio o restricciones dependiendo de cada usuario.

- **Verificación o autenticación:**

Se ratifica la identidad de un individuo; mediante de comparación de plantilla de consulta con las plantillas de referencia almacenas en la base de datos (Yanushkevich, 2009). El reconocimiento positivo emplea particularmente el proceso de verificación, ya que permite prevenir que una misma identidad sea usada por diferentes personas; (Wayman, 2001). La figura 5 indica el proceso de verificación de usuarios.

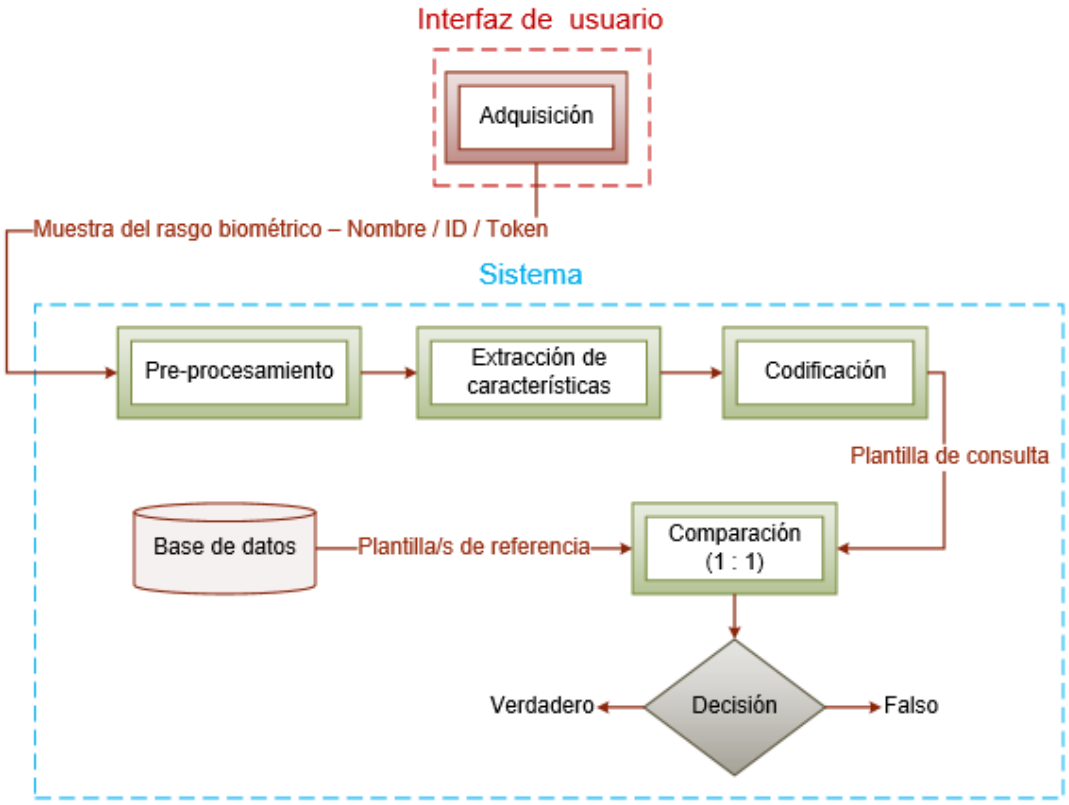

Figura 5. Procedimiento de verificación de identidad de un usuario

Si un sujeto pretende ser autenticado por el sistema de biometría, a más de proporcionar una muestra digital del rasgo biométrico; debe proveer cierta información, que haga alusión de la identidad del usuario que dice ser. Como por ejemplo, un nombre, un número de identificación (ID), o una tarjeta inteligente (token). Se efectúa una comparación uno a uno, para establecer si el sujeto es el usuario o no (Yanushkevich, 2009).

- **Identificación o reconocimiento:**

En el procedimiento de identificación, el sistema biométrico distingue a un sujeto; a través, de la comparación con todas las plantillas almacenas de los usuarios registrados en el sistema (Yanushkevich, 2009). El reconocimiento negativo se fundamenta en el procedimiento de identificación, así un individuo no puede usar varias identidades (Wayman, 2001). Las etapas del modo de identificación se muestran en la figura 6.

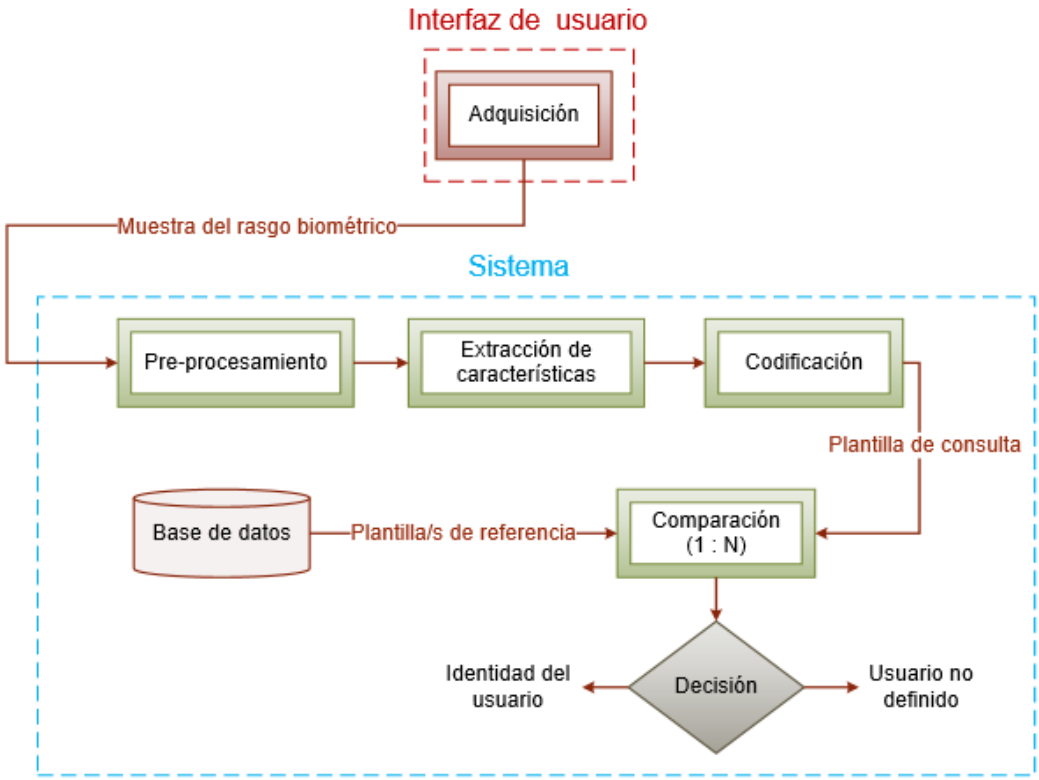

Figura 6. Procedimiento de identificación de un usuario

Los sistemas de biometría en modo de verificación efectúan una comparación de uno a mucho (N representa el número de usuarios registrados en el sistema), para determinar la identidad del sujeto que pretende ser reconocidos como usuario de sistemas (Yanushkevich, 2009). Este proceso demanda de un alto coste computacional, en comparación con el procedimiento de autenticación (Aguilera, 2012).

2.4. Evaluación del rendimiento de sistemas de biometría

En la práctica dos plantillas biométricas del mismo rasgo de un sujeto, no son estrictamente idénticas; esto se debe comúnmente al uso inadecuado del sensor para la adquisición de datos. En consecuencia, el rendimiento del sistema se ve afectado. Un sistema biométrico realiza la comparación de la plantilla biométrica que se desea identificar o verificar, con las plantillas guardadas, en base al cómputo de su semejanza se determina una puntuación, calificación o *score*. El sistema de biometría distinguirá la identidad de una persona, en el momento en que se obtenga una mayor

calificación, es decir cuando la similitud de las plantillas sea mayor (Tomé G., 2008).

En la evaluación del rendimiento del sistema se contemplan dos tipos de identidades: genuinos e impostores. Para distinguirlos se impone un umbral; un usuario se define como genuino, cuando la puntuación obtenida en la comparación, es mayor que el umbral; caso contrario será definido como impostor. Dos tipos de errores se originan en base a la determinación que tome el sistema (Aguilera, 2012):

- **Falso rechazo** (FR, *False Reject*): este error se produce, en el caso de que, dos plantillas biométricas correspondientes a un mismo usuario obtengan una calificación menor al umbral establecido. Es decir, el sistema establece a un usuario genuino como impostor.
- **Falsa aceptación** (FA, *False Acceptance*): cuando la comparación de dos plantillas biométricas, generadas a partir de diversos usuarios, consiguen una calificación mayor al umbral establecido; se dice que se generó un error de falsa aceptación. En otras palabras, el sistema determino como usuario genuino a un impostor.

2.5. Parámetros para la evaluación del proceso de reconocimiento

La evaluación del sistema varía, dependiendo del modo de funcionamiento del sistema. En el modo de autenticación se distinguen dos clases de errores que se pueden generar; estos error describen la reiteración con la que se ocasionan los inconvenientes de FA y FR (Aguilera, 2012).

- **La tasa de falsa aceptación** (FAR, False Acceptance Rate): Porcentaje de ocasiones que se asumen a un intruso como usuario genuino del sistema (Ávila, 2012).
- **La tasa de faso rechazo** (FRR, *False Rejection Rate*): Porcentaje de ocasiones que se rechaza a un usuario genuino del sistema (Ávila, 2012).

La figura 7 muestra las densidades de probabilidad de calificación de usuarios genuinos e impostores, donde se señalan la FAR y FRR. La FAR es la sección inferior de la distribución de la calificación de impostores que esta

sobre el umbral seleccionado. Por otro lado, la FRR es el sector inferior de la distribución de usuarios genuinos que no supera al umbral fijado (Tomé G., 2008).

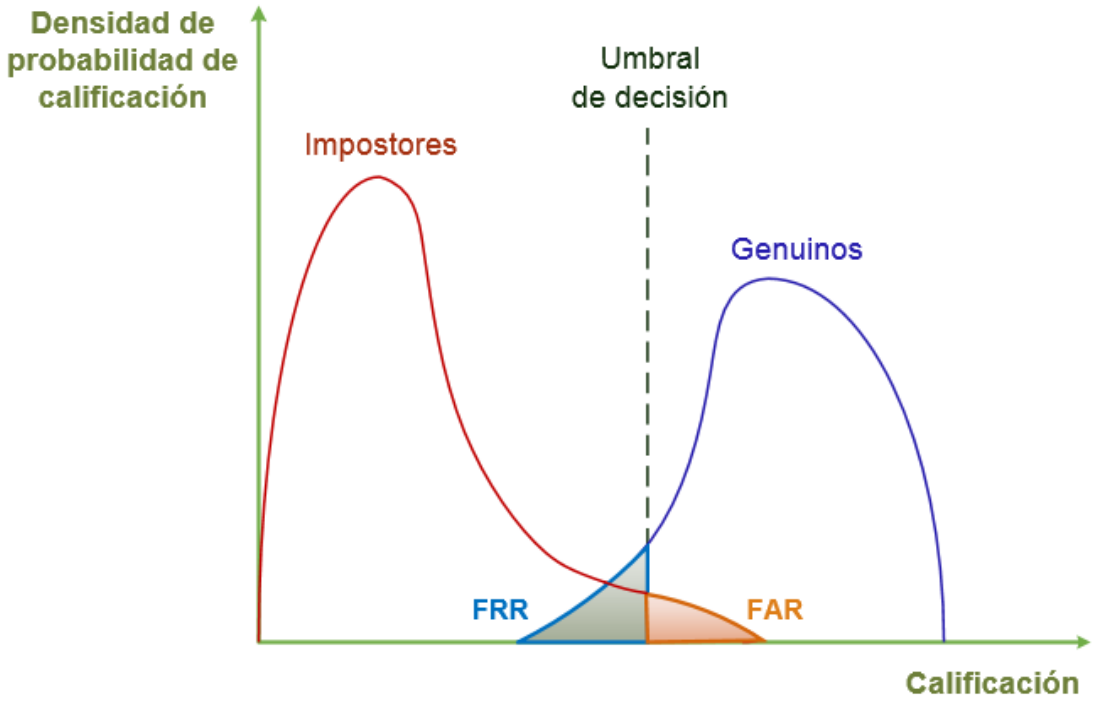

Figura 7. Densidad de probabilidad de calificación de genuinos e impostores

La FAR y FRR son parámetros inversamente proporcionales, que varían dependiendo del valor que tome el umbral de decisión (Tomé G., 2008). La FRR incrementa, conforme el valor del umbral de decisión aumente; mientras que, la FAR disminuye (Aguilera, 2012). Se considera al sistema muy permisivo, en el momento que se validan datos erróneos; es decir se determinan como usuarios genuinos a impostores, en este caso, el valor del umbral de decisión tendrá un valor bajo. Dando como resultado un porcentaje alto de la FAR y bajo de la FRR. Lo contrario sucede al designar un valor alto al umbral, en este caso se define al sistema como muy restrictivo (Tomé G., 2008).

Otra métrica es la tasa de igual error (EER, *Equal Error Rate*), es una relación entre la FAR y la FRR, se representa como el punto de cruce entre la curva FA y FR. El valor de la EER es proporcional a la zona de solapamiento de las curvas, es decir si la ERR es menor, la región de solapamiento es

menor y viceversa. La EER no necesariamente determina el umbral para el desarrollo del esquema (Tomé G., 2008).

La figura 8 señalan dos ejemplos de EER, la primera imagen corresponde a una EER con valor diferente al umbral de decisión; mientras que en el segundo gráfico, el umbral fijado y la EER tienen el mismo valor, en este caso FAR y FRR son iguales. La curva FA describe la distribución de probabilidad de calificación de un impostor, por otra parte, la curva FR indica la distribución complementaria de probabilidad de calificación de usuarios genuinos (Tomé G., 2008).

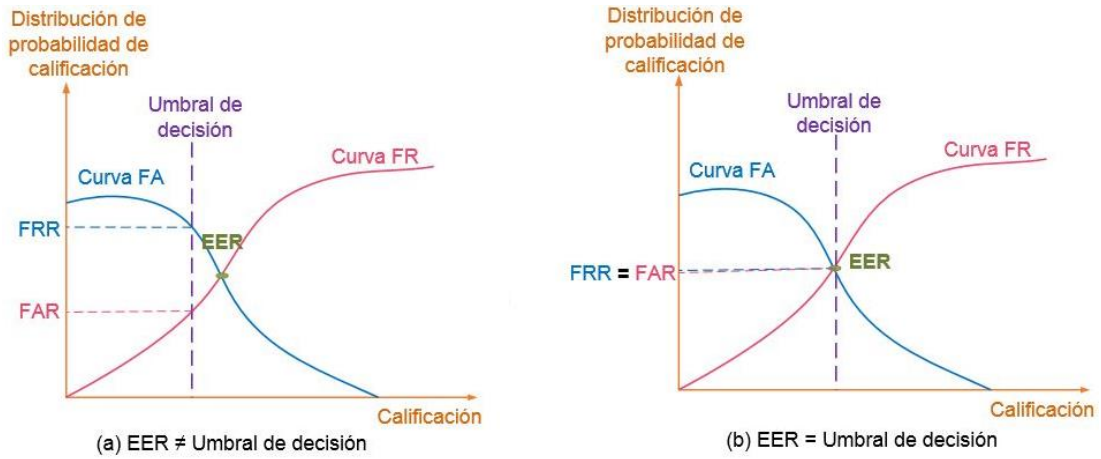

Figura 8. Distribución de probabilidad de impostores y usuarios genuinos

A través del uso de la curva característica operativa del receptor (ROC, *Receiver Operating Characteristic*) se establece una referencia del punto de trabajo; se constata la discriminación del sistema, analizando la sensibilidad respecto a especificidad para un rango de puntuaciones, previamente obtenidas. La gráfica de la curva ROC en el eje de las ordenadas se manifiesta la sensibilidad. Así mismo, en el eje de las abscisas se representa $(1 - Especificidad)$ (Alonso, 2002).

La ecuación 2.6 indica como determinar la sensibilidad. Donde se considera un umbral de decisión, el número de verdaderos positivos (VP) representa al número de comparaciones de un usuario genuino con puntuación mayor al umbral. Falsos negativos (FN) indica el número de comparaciones de un usuario genuino con puntuación menor al umbral (Alonso, 2002).

$$Sensibilidad = \frac{VP}{VP+FN} \quad (2.6)$$

La ecuación 2.7 muestra el cálculo de $(1 - Especificidad)$; en la cual, el número de falsos positivos (FP) señala al número de comparaciones de un impostor con puntuación mayor al umbral. Verdaderos negativos (VN) indican el número de comparaciones de un impostor con puntuación menor al umbral (Alonso, 2002).

$$1 - Especificidad = \frac{FP}{FP+VN} \quad (2.7)$$

En la figura 9 se observa la curva ROE de un sistema considerando tres umbrales; para determinar cuál es la mejor opción, se contempla en área bajo la curva ROC. La curva del sistema que considera el umbral 1 es preferible, pues le corresponde la mayor área, lo que quiere decir que exista mayor probabilidad de que un usuario sea definido como genuino (Abraira, 2011).

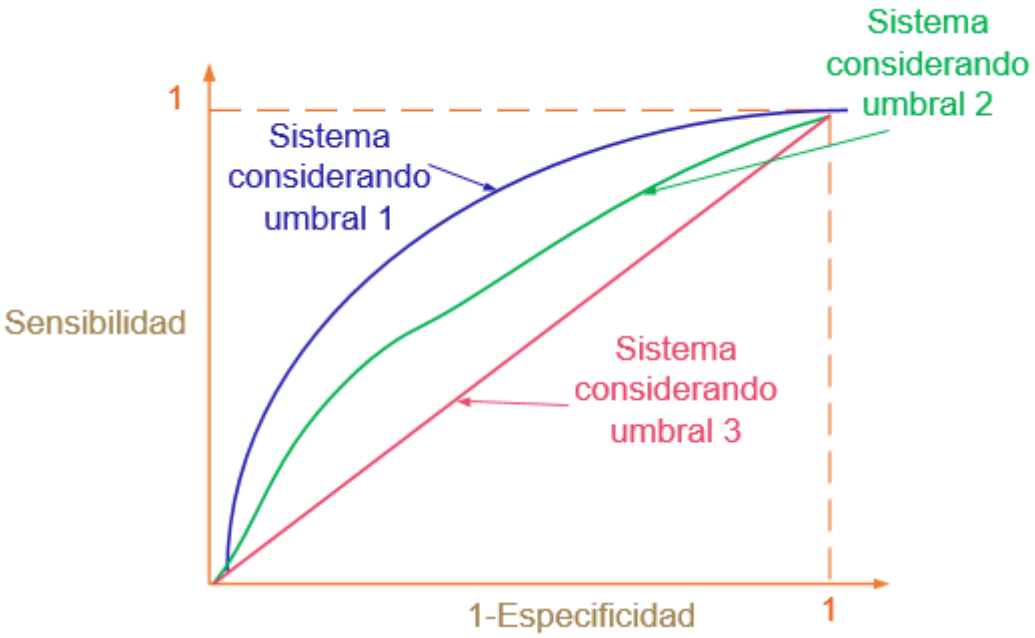

Figura 9. Curva ROE

Con la curva de detección de error de compensación (DET, *Detection Error Tradeoff*) se obtiene una sola curva que representa un error en comparación al otro error, en la gráfica los ejes se normalizan. La curva DET permite una mejor apreciación del funcionamiento del sistema (Aguilera, 2012). En la figura 10 se muestra la curva DET; donde se distingue la curva DET de dos sistemas,

cada uno con un valor diferente de umbral de decisión, se considera mejor al sistema que más se acerque al origen (sistema considerando umbral 1), lo que representa un porcentaje de errores FA y FR inferior.

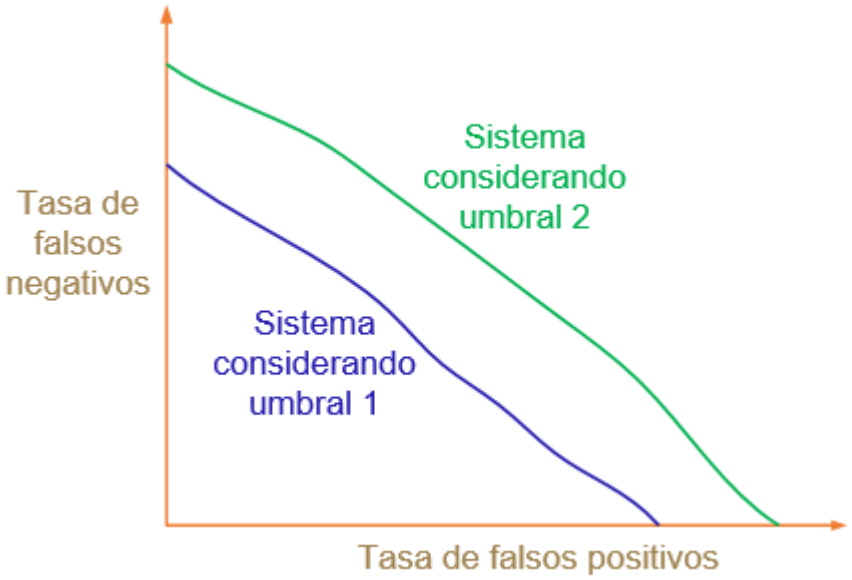

Figura 10. Curva DET

2.6. Biometría cancelable

En el caso de que un rasgo biométrico se vea comprometido, por robo de las plantillas almacenas en la base de datos o porque fue grabado sin consentimiento de su portador. Se ha planteado a la biometría cancelable (CB) como una solución ya que el rasgo biométrico no se puede intercambiar (Ratha N. K., 2001). CB representa una alteración deliberada en la plantilla original o de referencia que se obtiene al procesar las particularidades de un rasgo biométrico, permitiendo así realizar la comparación de las plantillas biométricas en el dominio de la función que se usó para lograr la alteración (Bringer, 2008). Esta transformación brinda privacidad a sistemas de biometría, pues debería ser improbable restablecer la plantilla biométrica original después de la alteración provocada (Ratha N. C., 2006).

Al aplicar la modificación, las características de individualidad no deberían disminuir, es decir no debe aumentar la FAR, en tanto restringir la FRR siendo el sistema flexible. La correlación de diversas transformaciones de la plantilla no deberá permitir la posibilidad de vinculación con la plantilla de referencia. Si la plantilla modificada se ve comprometida los parámetros de la alteración se sustituyen para generar una nueva plantilla (Rathgeb C. U., 2011). CB debe cumplir con cuatro propiedades (Teoh, 2007):

- **Diversidad:** La plantilla alterada no se puede emplear en más de una aplicación.
- **Reutilización:** En caso de que la plantilla modificada se vea comprometida, se debería anular y producir otra transformación.
- **Invertibilidad:** Los datos biométricos originales no se pueden recuperar.
- **Rendimiento:** El rendimiento de identificación del sistema no debe ser afectado.

En la figura 11 se observa el proceso de inscripción e identificación de un sistema de CB. Una función de transformación se aplica en la plantilla de referencia, para provocar la distorsión además de usar la función se podría considerar una clave. En la base de datos del sistema solo se almacena la plantilla transformada. Por otra parte, en el proceso de identificación se modifica a la plantilla que desea ser identificada, tomando en cuenta la función de transformación y si es el caso la clave. La comparación se realiza entre la plantilla transformada de referencia y la plantilla transformada de consulta, es decir en dominio de la función de trasformación (Jain A. K., 2008).

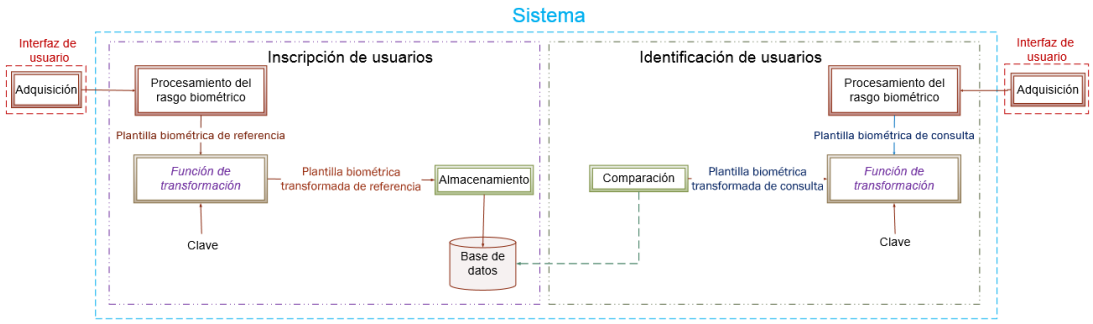

Figura 11. Inscripción e identificación de un sistema de biometría cancelable

2.6.1. Tipos de esquemas de biometría cancelable

Fundamentalmente, la biometría cancelable efectúa una alteración de los patrones biométricos, previo a su comparación. Existen diversos métodos para provocar la distorsión de las plantillas, dependiendo de sus parámetros, se pueden clasificar los esquemas de CB en: transformación no invertible y biometría *salting* (Rathgeb C. U., 2011).

2.6.1.1. Transformación no invertible

Una vez obtenida la plantilla biométrica original $\mathcal{T}$ se distorsiona utilizando una función de transformación no invertible $\mathcal{F}$. La función empleada tiene como características: unidireccional, sencilla de calcular y compleja de invertir. Un token o clave $\mathcal{K}$ establece los parámetros de la función de transformación; un usuario para ser autenticado debe presentar la clave que se le fue asignada (Jain A. K., 2008). En la figura 12 se observa el proceso de registro y verificación de un sistema de CB con enfoque de transformación no invertible.

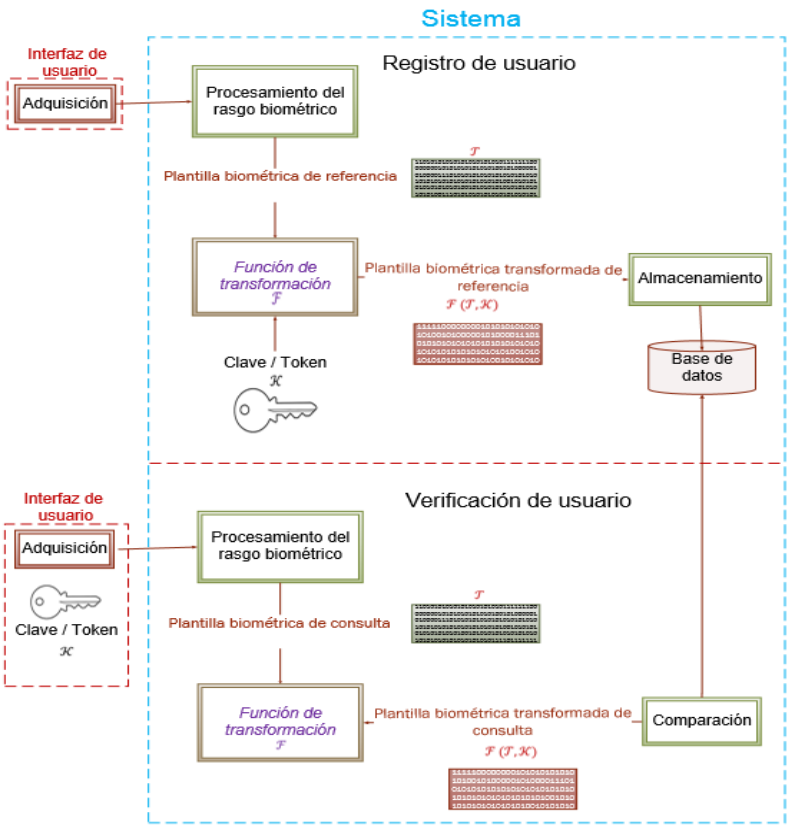

Figura 12.Sistema de CB con enfoque de transformación no invertible

Los parámetros de la función de transformación son modificables para general plantillas actualizables (Rathgeb C. U., 2011). Si el token o la plantilla biométrica modificada de referencia son interceptadas por intrusos al sistema, es un proceso complejo restaurar la información de la plantilla biométrica de referencia original. Lo que genera una mayor seguridad en los sistemas de biometría (Jain A. K., 2008).

Es fundamental que la función no invertible usada debe conservar la propiedad de búsqueda de similitudes entre plantillas que el sistema de biometría original; en los sistemas de BC, las particularidad de un usuario deben poseer una alta similitud. Mientras, que si las comparamos con las características de otro usuario deben ser bastante distintas (Jain A. K., 2008). A pesar de las ventajas que presenta la transformación no invertible, se presenta una disminución en la precisión del sistema; esto se debe, a la reducción de la información útil; asimismo la alineación de las plantillas, influye en su comparación (Rathgeb C. U., 2012).

2.6.1.2. Biometría salting

Las funciones $\mathcal{F}$ que se emplean en el enfoque *salting* o *biohashing*, usan diferentes claves o *secret seed* $\mathcal{K}$. La seguridad de este tipo de esquema se logra manteniendo en secreto los parámetros de la transformación. Para cada aplicación se emplea diferentes *secret seed* (Rathgeb C. U., 2011); que está constituida por bits aleatorios que se combinan con la información útil del rasgo biométrico (Kong, 2006).

Se pueden producir diversas plantillas de referencia transformadas del mismo usuario, lo que proporciona la propiedad de diversidad al sistema; ya que se emplea un clave para cada aplicación. La función de transformación es la misma para todas las aplicaciones. Por tal motivo debe garantizar que el rendimiento del sistema se mantenga. Si una plantilla biométrica de referencia modificada es interceptada por un intruso del sistema, esta debe poder ser revocada y reemplazada sin ninguna dificultad (Jain A. K., 2008).

Los sistema que usan funciones salting generan preocupación, debido al uso de una *secret seed* para todos los usuarios en una determinada

aplicación, pues disminuye la seguridad del sistema (Jin, 2010). En la figura 13 se expone en proceso de inscripción en un sistema de CB con enfoque *salting.* Donde, N representa el número de aplicaciones, que conforman el sistema.

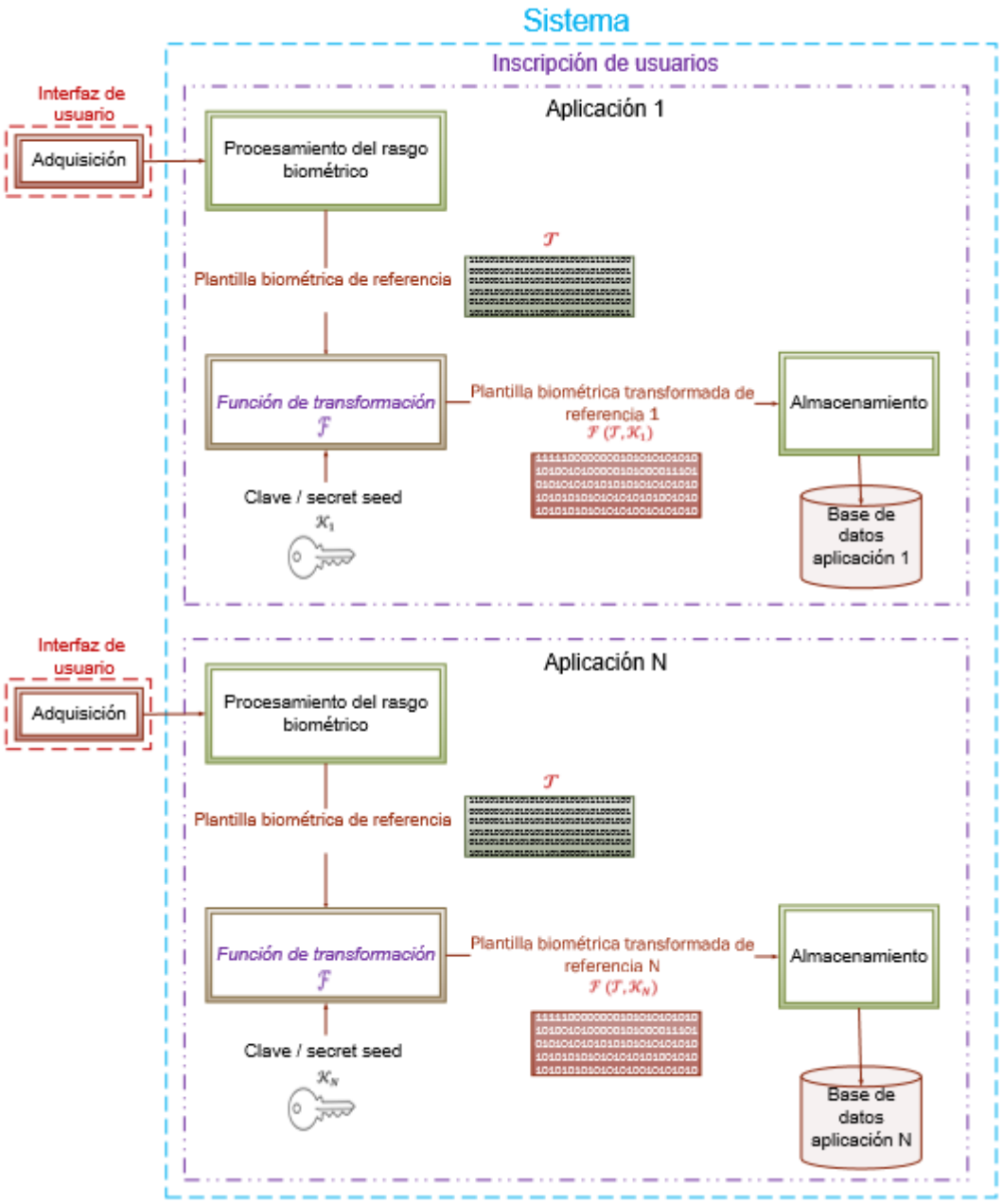

Figura 13. Proceso de registro en un sistema de CB con enfoque *salting*

2.6.2. Evaluación de esquemas de biometría cancelable

En diversos estudios de sistemas de CB, los autores generan resultados experimentales, generados a partir de la evaluación del rendimiento, así mismo el análisis de la seguridad, suponiendo puntos débiles de cada proceso que conforma al sistema y considerado algunos ataques que podría afectar a los esquemas. No existe hasta el momento un estándar para ponderar la privacidad de un sistema biométrico basado transformación cancelable (Belguechi R. C., 2012).

En (Belguechi R. C., 2012) se plantea un método para evaluar estos esquemas, fundamentando en estudios previos; en el cual se manifiestan diversos ataques considerando el punto de vista de un impostor o intruso, permitiendo así verificar el cumplimento de las propiedades de biometría cancelable. Además se definen ciertas ponderaciones que integran este estudio de seguridad y privacidad.

Para realizar el análisis de los esquemas de CB se considera a un usuario z, de cual se genera una plantilla biométrica de referencia $\mathcal{T}_z$, después de pasar por las etapas de adquisición, pre-procesamiento, extracción de peculiaridades y codificación. Además, se aplica una función $\mathcal{F}$, produciendo así un biocódigo o plantilla transformada de referencia $\mathcal{F}(\mathcal{T}_z,\ \mathcal{K}_z)$. Un conjunto de parámetros de conversión K_z también es usando. Si el usuario z desea ser verificado o reconocido por el sistema, se debe extraer una plantilla biométrica de consulta $\mathcal{F}(\mathcal{T}_z',\ \mathcal{K}_z)$. Se fija un umbral ϵ para realizar la comparación entre la plantilla de consulta y la plantilla de referencia de usuario z. El cual sirve como referencia para tomar la decisión de la comparación. Al no ser la $\mathcal{F}(\mathcal{T}_z,\ \mathcal{K}_z)$ exactamente igual a la $\mathcal{F}(\mathcal{T}_z',\ \mathcal{K}_z)$, se calcula una función de comparación o *match* $\mathcal{M}_T$, que se compara con ϵ, para que el usuario z sea aceptado o rechazado por el sistema (Belguechi R. C., 2012).

En la norma ISO/IEC 24745 se puntualizan las propiedades de seguridad de un esquema biométrico cancelable debe poseer:

- **Rendimiento:**

En biométrica, dos términos hacen referencia al error: la FRR y la FAR. Al utilizar CB estimamos los términos mencionados, con los parámetros de transformación que se utilizaron con se constata en las ecuaciones 2.8 y 2.9. Donde se calcula la similitud entre $\mathcal{F}(\mathcal{T}_z, K_z)$ y $\mathcal{F}(\mathcal{T}_z', K_z)$, plantillas correspondientes al usuario z. Si el resultado es mayor que ϵ se obtiene la tasa de falso de rechazo del sistema de CB FRR_T. Por otra parte, se compara la plantilla biométrica transformada de consulta $\mathcal{F}(\mathcal{T}_x', K_x)$ del sujeto x, con la $\mathcal{F}(\mathcal{T}_z, K_z)$ del usuario z, si el valor obtenido deber ser menor o igual ϵ, se determina la tasa de falsa aceptación del sistema de CB FAR_T,

$$FRR_T(\epsilon) = P\big(\mathcal{M}_T\big(\mathcal{F}(\mathcal{T}_z', K_z),\ \mathcal{F}(\mathcal{T}_z, K_z)\big) > \epsilon\big) \tag{2.8}$$

$$FAR_T(\epsilon) = P\big(\mathcal{M}_T\big(\mathcal{F}(\mathcal{T}_x', K_x),\ \mathcal{F}(\mathcal{T}_z, K_z)\big) \leq \epsilon\big) \tag{2.9}$$

- **Revocación o revocabilidad:**

Si se transforma la plantilla biométrica del usuario z, se genera un biocódigo $\mathcal{F}(\mathcal{T}_z, K_z^1)$ considerando los parámetros K_z^1, en el caso de que la información del rasgo biométrico o los parámetros de transformación se vean comprometidos, debe ser factible revocar el biocódigo y producir uno nuevo $\mathcal{F}(\mathcal{T}_z, K_z^2)$. La revocabilidad es ejecutable gracias a que solo se almacenan biocódigos de referencia.

- **Irreversibilidad o no invertibilidad:**

Un impostor pretende ser autenticado o reconocido, proporcionando diferentes datos. El éxito de este tipo de ataque se puede estimar con la ecuación 2.10, en la cual, se estima la probabilidad un ataque exitoso FAR_A . El biocódigo X_x, es creado por el impostor considerando la mayor cantidad de datos auténticos asequibles. La decisión se toma considerando ϵ.

$$FAR_A(\epsilon) = P\big(\mathcal{M}_T\big(X_x,\ \mathcal{F}(\mathcal{T}_z, K_z)\big) \leq \epsilon\big) \tag{2.10}$$

- **Imposibilidad de vinculación o diversidad:**

Es imprescindible no poder asociar a un usuario basándose en los datos de $\mathcal{F}(\mathcal{T}_z, K_z)$, previniendo así ataques de vinculación. Para un usuario z, debe ser

posible generar un conjunto Q de biocódigos $\mathcal{T}_z = \{\mathcal{F}(\mathcal{T}_z, K_z^1), \ldots, \mathcal{F}(\mathcal{T}_z, K_z^Q)\}$ que puedan ser revocados.

Con el propósito de calcular la robustez de un sistema de CB, que dispone de una base de datos con múltiples muestras biométricas transformadas pertenecientes a cada usuario. Un umbral de decisión ∈ se establece como referencia, para calcular ocho criterios A_i, que cuantifican el cumplimiento de las propiedades antes mencionadas (Belguechi R. C., 2012).

La evaluación de la privacidad y seguridad de un esquema de CB contempla las dos modalidades de funcionamiento de la biometría, en las cuales se planteando distintos escenarios de ataques. La autentificación se analiza, suponiendo que un intruso o impostor pretende suplantar a un usuario genuino específico. Por otra parte, para examinar la identificación, el impostor pretende hacerse pasar por uno de los usuarios registrado en el sistema (Belguechi R. C., 2012).

2.6.2.1. Autentificación o verificación

2.6.2.1.1. Rendimiento (A_1)

El rendimiento o eficiencia de un sistema de CB se puede determinar empleando la ecuación 2.11, la cual es una relación entre la FAR y FRR del sistema de CB $(FAR_T,\ FRR_T)$ y la FAR y FRR del sistema de biometría sin ninguna transformación $(FAR,\ FRR)$. Sí el resultado de esta expresión es igual a uno, indica que el rendimiento del esquema de CB no tiene ningún error; por otra parte, sí obtiene como resultado un valor negativo denota un deterioro del rendimiento; lo contrario sucede al conseguir un valor positivo, el rendimiento incrementa (Belguechi R. C., 2012).

$$A_1 = 1 - \frac{FAR_T,\ FRR_T}{FAR,\ FRR} \qquad (2.11)$$

2.6.2.1.2. Irreversibilidad (A_2 a A_5)

Para evaluar la propiedad de irreversibilidad o no invertibilidad se suponen cuatro escenarios de ataques. En los cuales, se producen varios intentos falsos de verificación por parte de intrusos o impostores (Belguechi R. C., 2012).

- **Ataque de cero esfuerzo (A_2):**

Un impostor x provee un rasgo biométrico $\mathcal{T}_x'$ y parámetros K_x para ser verificado como el usuario z: $\mathcal{F}(\mathcal{T}_x', K_x) = \mathcal{F}(\mathcal{T}_z, K_z)$.

- **Ataque de fuerza bruta (A_3):**

Un impostor genera valores aleatorios X_x para ser autenticado como el usuario z: $X_x = \mathcal{F}(\mathcal{T}_z, K_z)$.

- **Ataque de token robado (A_4):**

Un impostor ha conseguido el token K_z del usuario z e intenta distintos valores aleatorios $\mathcal{T}_x'$ para ser verificado: $\mathcal{F}(\mathcal{T}_x', K_z) = \mathcal{F}(\mathcal{T}_z, K_z)$.

- **Ataque de robo de características biométricas (A_5):**

Un impostor conoce la información biométrica original $\mathcal{T}_z$ y busca ser autentificado probando varios valores aleatorios de K_x: $\mathcal{F}(\mathcal{T}_z, K_x) = \mathcal{F}(\mathcal{T}_z, K_z)$.

La FAR es un parámetro significativo, para calcular la eficiencia de los cuatro ataques antes descritos. La ponderación de cada ataque $A_i, i = 2, \dots, 5$, facilita su clasificación además muestra el riesgo de que un impostor sea verificado como un usuario genuino del sistema (Belguechi R. C., 2012).

2.6.2.1.3. Diversidad o imposibilidad de vinculación (A_6 a A_8)

Como ya se ha indicado un esquema de CB debe ser capaz de producir diferentes biocódigos para cada aplicación de un usuarios (Belguechi R. C., 2012).

- **Información mutua de biocódigos:**

Para calcular la propiedad de diversidad, se determina el máximo valor de la información mutua de los biocódigos generados de cada usuario. Para la ponderación de A_6 se calcula de media de los valores máximos de información mutua de todos los usuarios.

La información mutua se entiende como el número de bits promedio para representar una plantilla X, menos el número promedio de bits necesarios para especificar una plantilla X después de conocer la una plantilla Y. Es decir, la información mutua de dos biocódigos determina la disminución de la incertidumbre (entropía) de un biocódigo X, considerando los valores de otro biocódigo Y.

La ecuación 2.12 se utiliza para calcular la información mutua de X e Y. P señala la estimación de la probabilidad de ocurrencia.

$$I(X,Y) = H(X) + H(X) - H(X,Y) = \sum_x \sum_y P(x,y) \log\left(\frac{P(x,y)}{P(x)P(y)}\right) \qquad (2.12)$$

Para la ponderación de A_6 se utiliza el valor medio de todos los usuarios del valor máximo de información mutua, como se observa en la ecuación 2.13, en la cual, $\mathcal{T}_z$ representa el biocódigo almacenado en la base de datos del usuario z, $\mathcal{T}_z'$ indica la consulta j-ésima de la base de datos del usuario z, N es el número de usuarios en la base de datos, M denota el número de biocódigos generados para cada usuario (Belguechi R. C., 2012).

$$A_6 = \frac{1}{N} \sum_Z \sum_{j=1}^{M} max\left(I\left(\mathcal{F}(\mathcal{T}_z, K_z), \mathcal{F}\left(\mathcal{T}_z^{\,j}, K_z\right)\right)\right) \qquad (2.13)$$

- **Ataque de escucha:**

Un impostor intercepta información de diferentes biocódigos originados de un mismo usuario y origina una plantilla por predicción, este ataque se evalúa, mediante el siguiente proceso: primero se produce Q biocódigos para el usuario z $\left\{\mathcal{F}(\mathcal{T}_z, K_z^1), \ldots, \mathcal{F}\left(\mathcal{T}_z, K_z^Q\right)\right\}$ Segundo, se realiza una estimación de posibles valores de biocódigo. Por último, se calcula la FAR de sistemas considerando $A_7 \rightarrow Q = 3$ y $A_8 \rightarrow Q = 11$.

2.6.2.2. Identificación o reconocimiento

Para evaluar los sistemas de CB en el proceso de identificación, se consideran los ocho parámetros planteados para la verificación. Con la

diferencia de que el impostor o intruso intenta hacerse pasar por todos los usuarios registrados en el sistema para ser identificado como uno de ellos (Belguechi R. C., 2012).

CAPÍTULO 3

METODOLOGÍA E IMPLEMENTACIÓN

3.1. Metodología

Se expone la metodología concerniente al diseño de los sistemas de biometría cancelable para autenticación y reconocimiento del iris, se mencionan las técnicas o algoritmos que se han utilizado en cada proceso mencionado en el capítulo anterior. En primer lugar, se puso en funcionamiento un sistema de biometría, teniendo así una referencia del rendimiento. Se ha empleado la herramienta de *software* MATLAB, para cumplir este objetivo.

3.1.1. Sistema de biometría

La implementación de este esquema es la base para el desarrollo de los dos sistemas de CB que se van a evaluar. Las etapas de segmentación, normalización, codificación y comparación, son idénticas para los dos esquemas que se van a comparar, la diferencia radica en la técnica que se empleó para generar CB. A continuación se especifican cada uno de los métodos empleados.

3.1.1.1. Adquisición

El reconocimiento y autenticación del iris, requiere de una imagen digital del ojo, de donde se extraerán y codificarán las particularidades del patrón iris, que podrán ser comparadas con las plantillas pre-registradas en el sistema. Existen diversas bases de datos de imágenes digitales del ojo. Que pueden utilizarse, permitiendo así el desarrollo e implementación de un esquema.

La Academia China de Ciencias – Instituto de Automatización (CASIA) ponen a la disposición de investigaciones, diversas bases de datos libres del iris. Se utilizó la base datos CASIA versión 1.0 (CASIA_IrisV1), que consta de 756 imágenes de ojos en escala de grises. Se distinguen 108 ojos o clases,

con 7 imágenes de cada clase, que se capturaron en dos sesiones, con un mes de paréntesis.

Todas las imágenes tienen formato BMP con resolución de (320 x 280). Las imágenes son procedentes de personas de origen asiático, teniendo como particularidades pestañas oscuras, además el iris muy pigmentado. Para la captura se las imágenes se empleó técnicas especializadas de óptica digital. Debido a las condiciones se utilizó luz infrarroja, con la cual las propiedades de la región del iris son a gran medida distinguibles, conjuntamente se tienen contraste entre el área de la pupila, del iris y esclerótica (CASIA 2003).

3.1.1.2. Segmentación

Al contar con la imagen digital del ojo, se inicia la segmentación automática de la región del iris, asimismo se realiza el aislando de las regiones ocluidas por parpados y pestañas. En figura 14 se indican de manera general las etapas del proceso de segmentación.

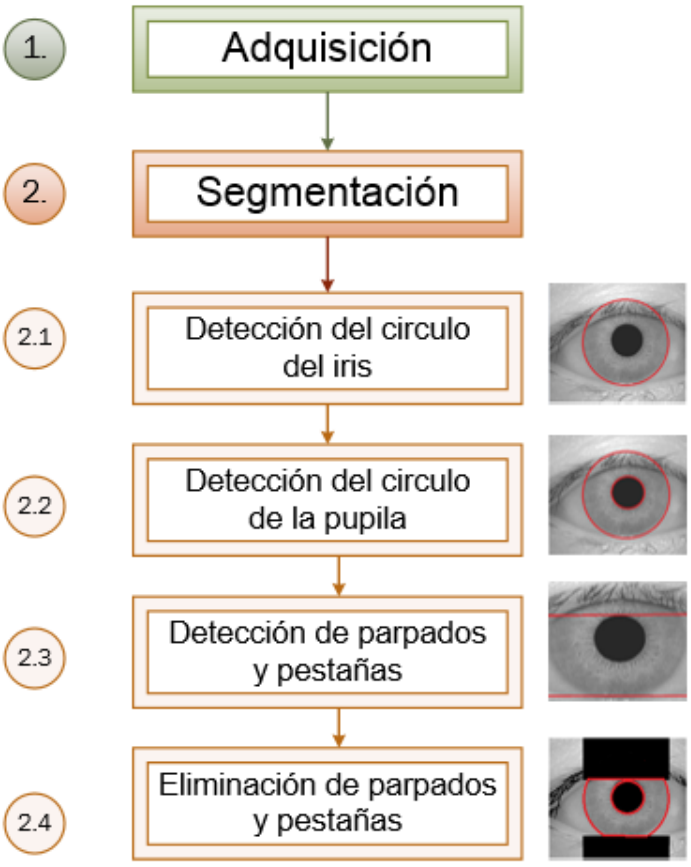

Figura 14. Etapas del proceso de segmentación del iris

El algoritmo de Canny se utilizó para detectar los bordes presentes en la imagen, para luego identificar los círculos del iris y de la pupila. La transformada de Hough circular se empleó para determinar los parámetros de cada círculo. Para la detección de parpados y pestañas, primero se obtuvieron los bordes del parpado superior e inferior usando el algoritmo de Canny. La transformada de Hough lineal es usada para su localización. Por último se eliminan estas regiones detectadas utilizando filtros.

3.1.1.2.1. Detección del círculo del iris - esclerótica

Para la detección del círculo formado entre el iris y la esclerótica, se inició localizando el mapa de bordes del iris aplicando el algoritmo de Canny. Este proceso se divide en tres fases. En la primera fase se obtiene la ponderación del gradiente, teniendo como resultado su magnitud y orientación. En el caso del límite del iris con la esclerótica, se usa dirección vertical para el gradiente de parcialidad. Las imágenes resultantes de la magnitud y orientación de los gradientes, se modifican para mejorar su contraste en las zonas oscuras.

En la segunda fase consiste en supresión no máxima, donde se reduce el grosor de los bordes, de las imágenes modificadas anteriormente. Posteriormente, se realiza una umbralización de histéresis, para determinar los pixeles que conforman los bordes definitivos y cuales el fondo de la imagen. La transformada de Hough se utilizó en el mapa de bordes para localizar el círculo que limita a la esclerótica con el iris, al concluir este proceso se obtiene las coordenadas del centro (x, y) y el radio r del círculo del iris. Se estableció un rango de valores del radio del círculo del iris, para filtrar la cantidad de resultados, considerando la base de datos de CASIA_IrisV1, el rango del radio del iris va de 80 a 130 pixeles (Daugman J. , 2003).

En la figura 15 se expone los resultados de cada etapa para lograr la detección del mapa de bordes del iris, empleando el algoritmo de Canny, además se indica a la imagen del ojo, en la cual se señala el círculo entre la esclerótica e iris, después de aplicar la transformada de Hough circular.

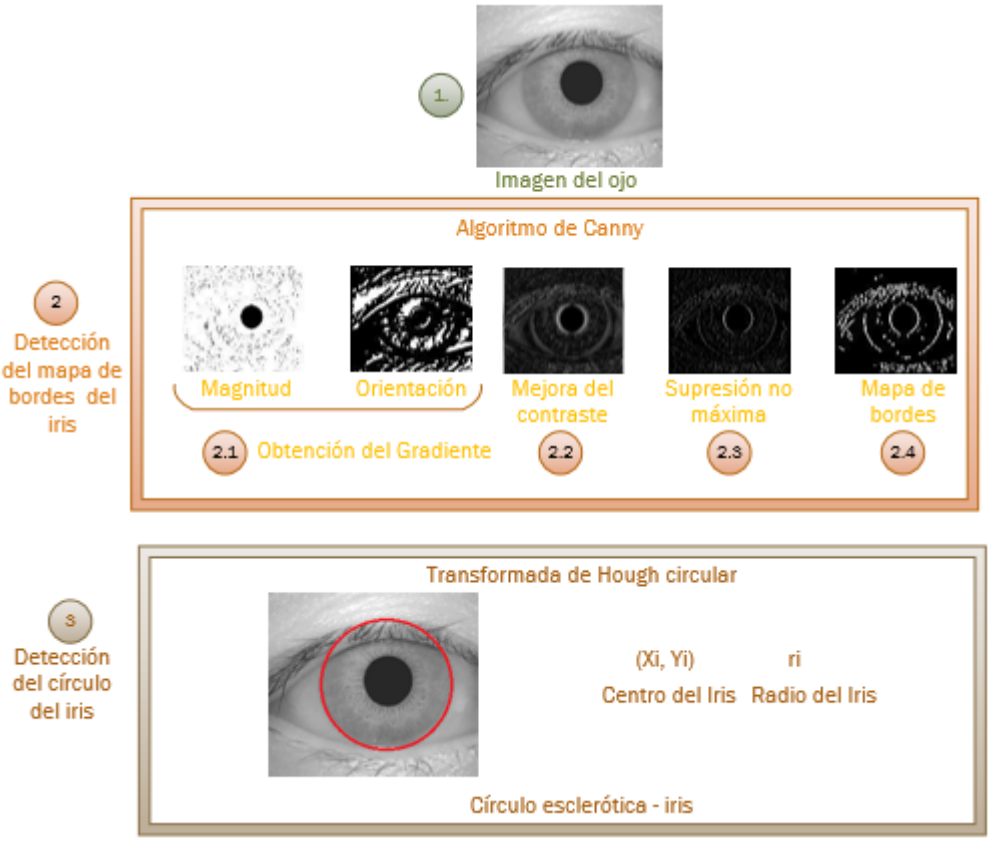

Figura 15. Detección del circo del iris - esclerótica

3.1.1.2.2. Detección del círculo de la pupila

Considerando que el círculo entre la esclerótica e iris ya fue localizado, la obtención del mapa de borde de la pupila se efectúa solo en esta área. Es decir no se considera la imagen completa del ojo, pues se conoce que la pupila está ubicada dentro del iris. De igual manera, el algoritmo de Canny se emplea para detectar los bordes de la pupila e iris.

En la etapa de ponderación de la magnitud y orientación, se calcularon gradientes con dirección horizontal y vertical. Asimismo se modificaron las imágenes resultantes, a fin de lograr un mejor contraste en las zonas oscuras. Seguidamente se disminuye el grosor de los bordes con la técnica de supresión no máxima. Para finalizar la detección de los bordes de la pupila se ejecuta una umbralización de histéresis.

En el mapa de contornos detectado de la pupila, se aplica la transformada de Hough obtiene las coordenadas del centro (x, y) y el radio r del círculo de

la pupila. El rango del radio tiene valores entre 20 y 50 píxeles considerando la base de datos de CASIA_IrisV1 (Masek, 2003). La detección del círculo entre el iris y la pupila en la imagen del ojo se muestra en la figura 16.

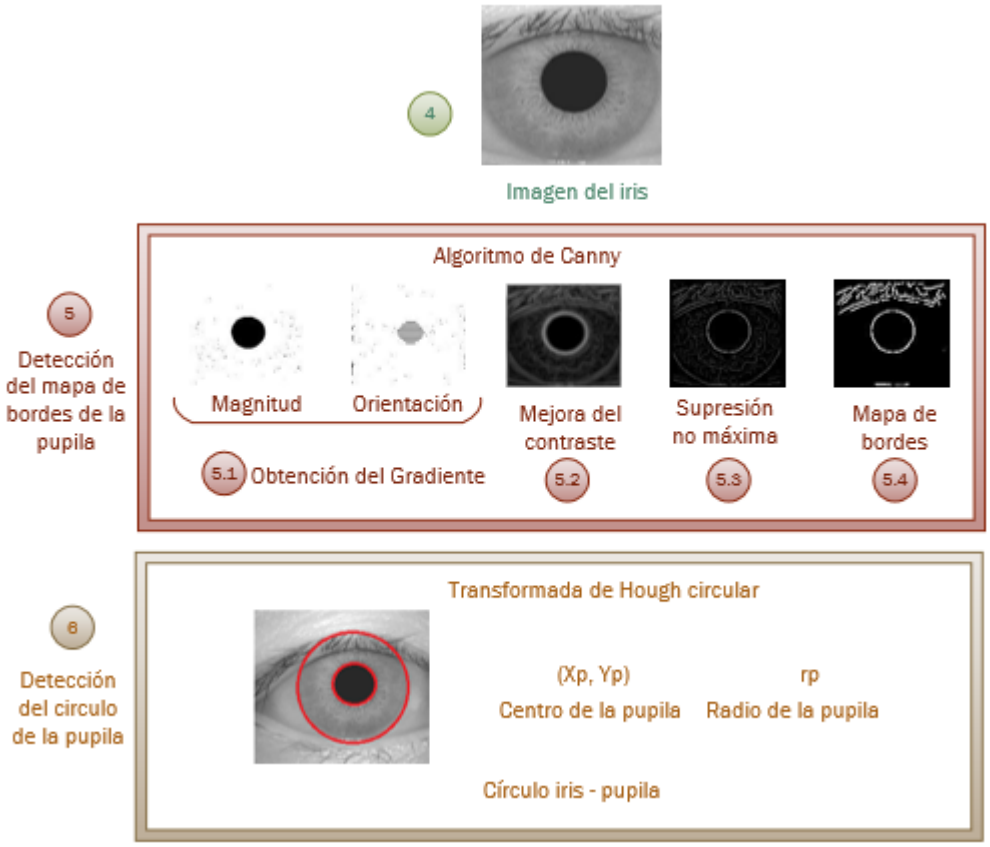

Figura 16. Detección del círculo de la pupila

3.1.1.2.3. Detección de parpados y pestañas

Al igual que en la detección de los bordes del iris y pupila, se obtiene la ponderación de la magnitud y orientación del gradiente con dirección horizontal. Para luego mejorar el contraste de las imágenes resultantes, además se utiliza la técnica de supresión máxima para la disminución el grosor de los bordes de la imagen. Por último se aplica la técnica de umbralización de histéresis, para extraer el mapa de bordes del parpa superior e inferior.

Se emplea la transformada de Hough lineal, para ubicar dos líneas horizontales, tanto en el parpado superior como inferior. Con la primera línea se ajusta al parpado, la según línea horizontal se cruza con la primera línea permitiendo así aislar la mayor cantidad del parpado. Al finalizar esta etapa se

obtienen las coordenadas polares de la línea superior e inferior que delimitan la presencia de los parpados en la región del iris. En la figura 17 se observa la detección de los parpados y pestañas en la región del iris.

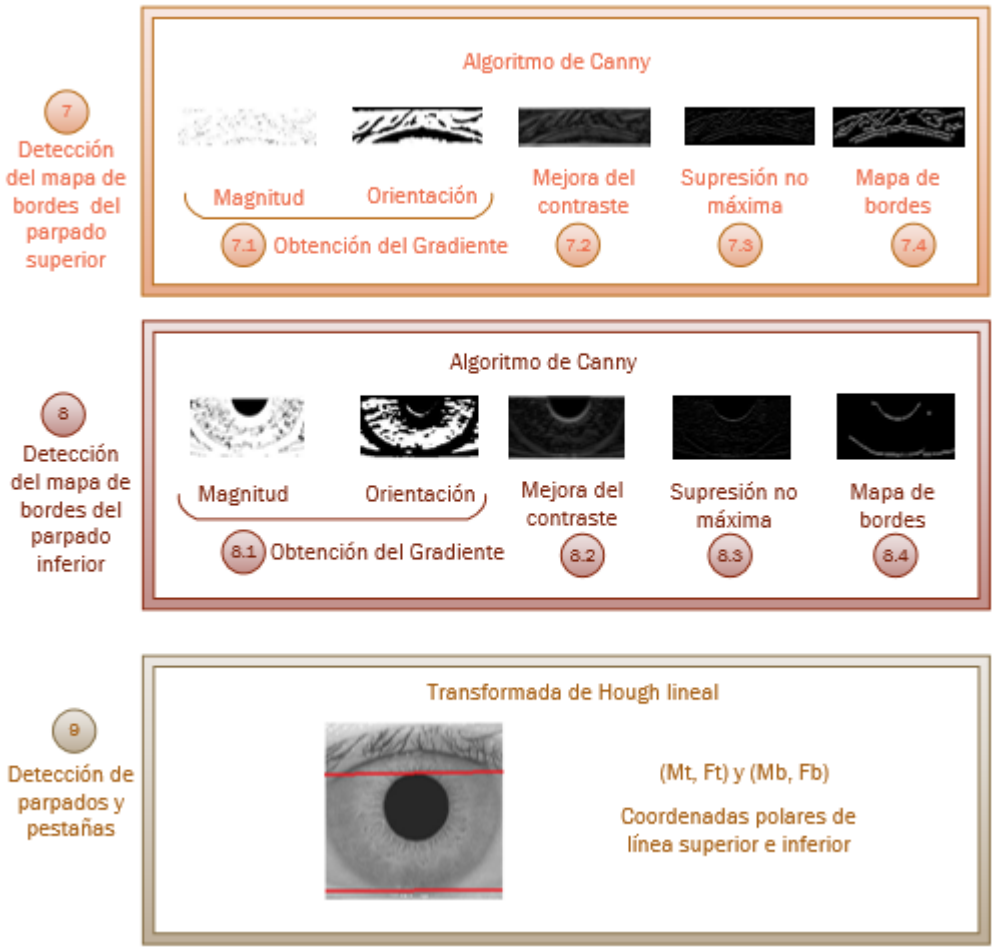

Figura 17. Detección de parpados y pestañas

3.1.1.2.4. Eliminación de los parpados y pestañas

Por último, las pestañas son aisladas mediante la aplicación de filtros; las pestañas se consideran como la parte más oscura de la imagen del ojo, por lo tanto se estable un umbral para su exclusión. Los segmentos de parpados y pestañas aislados, son relacionados con ruido, ya que no son consideradas para crear la plantilla del patrón del iris; el valor de sus intensidades se almacenara en una matriz denominada mascara de ruidos, que tiene las mismas dimensiones que la plantilla del iris. En la figura 18, se muestra el

resultado de la segmentación del iris además de la exclusión de parpados y pestañas.

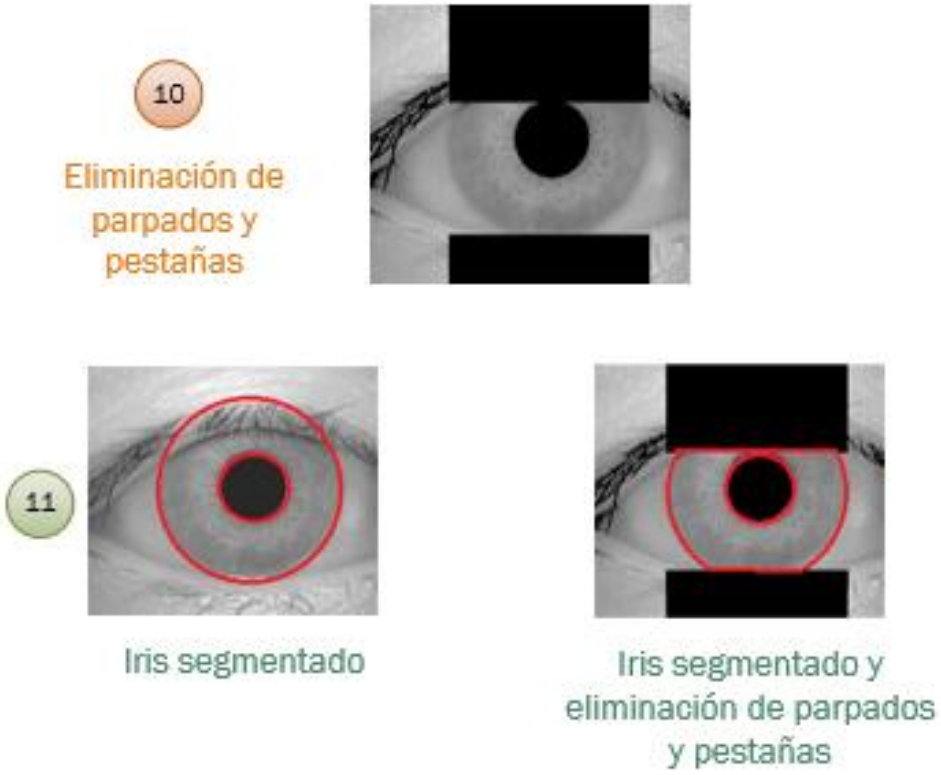

Figura 18. Segmentación del iris y eliminación de parpados y pestañas

3.1.1.3. Normalización

Para la etapa de normalización de la región del iris se emplea el método propuesto por Dougman, que consiste en codificar la región circular segmentada del iris, considerando las coordenadas del centro el iris y la pupila no son las mismas. Se establece como punto de referencia el centro de la pupila (Masek, 2003). En la figura 19 se indica un ejemplo de la ubicación del centro de la pupila e iris, los cuales no coinciden. Los puntos céntricos del círculo de la pupila y del iris se determinaron en la etapa de segmentación.

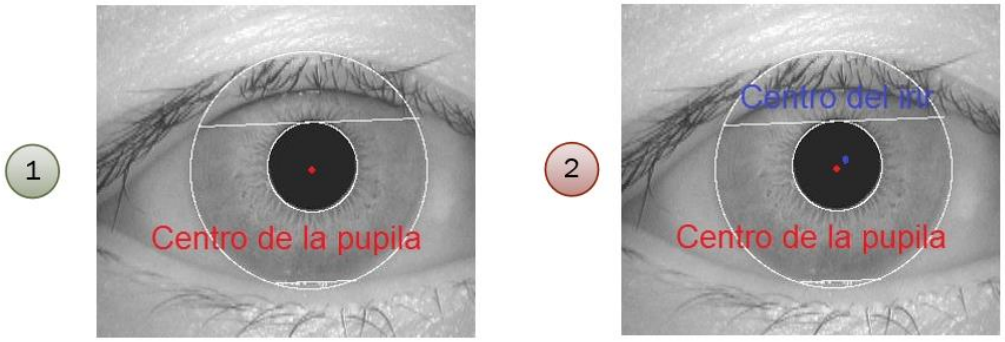

Figura 19. Ubicación del centro de la pupila e iris

Es elemental estimar el desplazamiento del centro de la pupila en relación con el centro del iris (o_x, o_y), para determinar los vectores radiales que pasan alrededor de la pupila al extremo del iris. En cada vector elegido se define un número de puntos de datos, que se denominan resolución radial angular r', por otra parte, la resolución angular θ se especifica como el número de vectores radiales (Masek, 2003). En la figura 20, se expone el proceso de normalización. Donde se identifican, los términos antes mencionados.

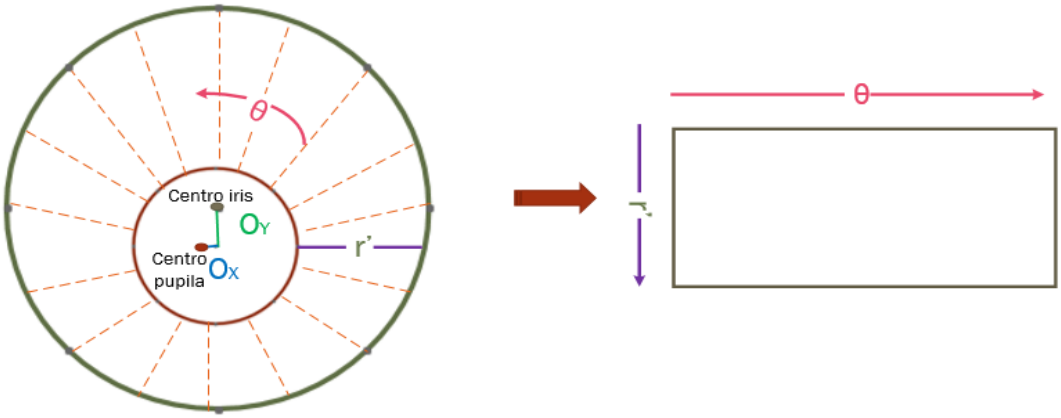

Figura 20. Proceso de normalización por método de Daugman

Se utilizó la ecuación 4.1 para modificar la escala de puntos en función del ángulo alrededor del círculo, en la cual se considera que $\alpha = o_x^2 + o_y^2$ y $\beta = \cos\left(\pi - \tan^{-1}\left(\frac{o_y}{o_x}\right) - \theta\right)$; el traslado del punto céntrico de la pupila con respecto al punto céntrico del iris está dado por o_x, o_y, la separación entre los bordes de la pupila y el iris en un ángulo θ alrededor de la zona, se denota por r' y el radio del iris es r_I (Masek, 2003).

$$r' = \sqrt{\alpha}\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_I^2} \quad (4.1)$$

Sin considerar la dimensión del radio obtenido en un ángulo, se seleccionan un número constante de datos radiales. Un ejemplo de ubicación de puntos de datos en la región del iris se observa en la figura 21.

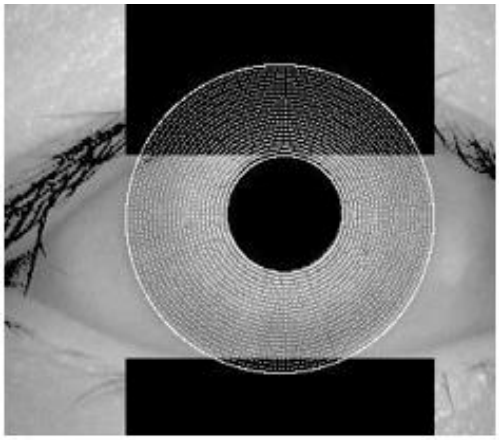

Figura 21. Ubicación de cada punto de datos de la región del iris

A continuación, los puntos en las coordenadas cartesianas se pasan a coordenadas con respecto al radio y ángulo, obteniendo así una matriz de dos dimensiones, horizontalmente se representa la resolución angular y verticalmente se refiere la resolución radial. Las pestañas y parpados detectados en la etapa de segmentación se normalizan en otra matriz, eludiendo la afectación de estos datos, también la información del borde de la pupila e iris son excluidos (Masek, 2003). El resultado de la normalización de la región de iris se muestra en la figura 22.

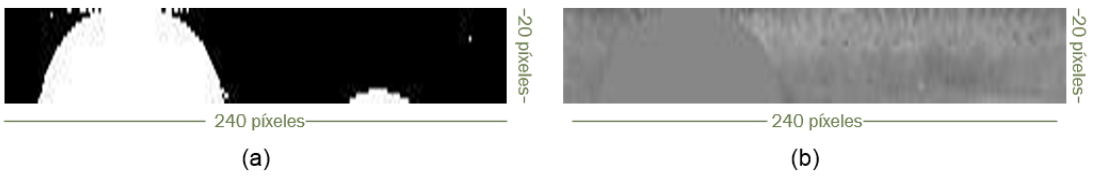

Figura 22. Resultado del proceso de normalización. (a) Regiones de ruido. (b) Región útil del iris

Según recomendaciones de trabajos previos se determina que la resolución radial constará de 20 segmentos, pues el valor que arroja mejores resultados en la etapa de comparación, para la base de datos la medida ideal

de la resolución angular se establece de 240 píxeles. Por lo tanto las medidas de las matrices serán de (20 x 240 píxeles) (Valencia M., 2014).

3.1.1.4. Codificación

El proceso de codificación consiste en la obtención de una plantilla de bits que refiere a cada imagen del iris; se considera la matriz de dos dimensiones resultante de la etapa anterior, en la cual un anillo del área del iris se manifiesta en una fila del arreglo. Visto que se tiene una máxima independencia de patrones en dirección angular (Kulkarni, 2012), En la figura 23 se observa la descomposición de la imagen normalizada del iris y las regiones de ruido en señales unidireccionales.

Figura 23. Descomposición de la imagen en señales unidireccionales. (a) Iris normalizado. (b) zonas de ruido

En esta etapa cada fila se considera como un arreglo de una dimensión, se emplea un filtro Log-Gabor igualmente de una dimensión, que permite trabajar en espacio y frecuencia, para efectuar la convolución entre ellos. Cuatro niveles son considerados para la ponderación en fase de la respuesta al aplicar el filtro, como se observa en la figura 24.

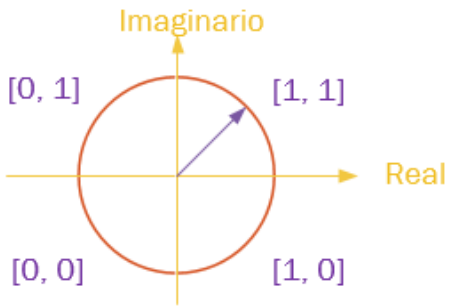

Figura 24. Codificación de fase

Dos bits de datos se generan por cada fasor. Para disminuir bits discordantes, se establece que entre cuadrantes solo se modifica un bit, teniendo un código de color gris después de la cuantificación de fase. De igual forma una plantilla de bit es creada a partir de la máscara de ruido (Masek, 2003).

3.1.1.5. Almacenamiento

Para llevar a cabo este procedimiento de almacenamiento en la base de datos del sistema de biometría, se tomó en consideración el número de la clase a la que pertenece cada imagen, este parámetro fija el número de usuario o ID. CASIA_IrisV1, proporciona 7 imágenes del ojo de 108 personas. Se consideraron 4 y 5 imágenes para generar las plantillas de referencia que se almacenan en dos bases de datos. Dejando 3 y 2 imágenes para realizar pruebas de autenticación y reconocimiento respectivamente.

3.1.1.6. Comparación

Para establecer la coincidencia entre dos plantillas se empleó el cálculo de la Distancia de Hamming (HD), pues así se realiza una comparación bit a bit además se ocupan ciertos bits de la máscara de ruido, específicamente los bits con valor de 0 en las máscaras de ruido de las dos plantillas de iris. La ecuación 4.2 indica cómo se obtuvo la HD, en la cual dos plantillas X_j y Y_j se comparan bit a bit, las máscaras de ruido referentes de cada iris se representan por Xn_j y Yn_j, además el total de bits que refieren a cada plantilla se denota como N (Masek, 2003).

$$HD = \frac{\sum_{j=1}^{N} X_i(XOR)Y_j(AND)Xn'_j(AND)Yn'_j}{N-\sum_{k=1}^{N} Xn_k(OR)Yn_k} \tag{4.2}$$

Algunas diferencias se presentan al comparar dos plantillas procedentes del mismo iris, pues el proceso de normalización no es exacto por presencia de ruido no detectado, el valor de la HD intra-clase será distinto de 0. Así mismo se presentan errores de alineación provocados por discrepancia de

rotación en la etapa de normalización, esto se contrarresta desplazando los bits en dirección horizontal de una plantilla, obteniendo un valor de la HD para cada desplazamiento, el valor más bajo se considera la mejor coincidencia entre las dos plantillas (Masek, 2003).

El desplazamiento corresponde a la rotación del patrón del iris en un ángulo dado por la resolución angular, se estableció un valor de 180 para la resolución angular, donde cada desplazamiento representa la rotación de 2 grados en el área del iris (Sanderson, 2000).

El total de bits desplazados se define por el doble del número de filtros usados, puesto que un filtro produce 2 bits de datos por cada pixel del área que se normalizó. Al utilizar solo un filtro en la etapa de codificación, se realizaron dos rotaciones, cada rotación implica un desplazamiento a la derecha y otro a la izquierda, trasladando 2 bits por cada rotación (Valencia M., 2014).

3.1.1.6.1. Parámetros de búsqueda de coincidencias

Para efectuar la búsqueda de coincidencias entre una plantilla de consulta y las plantillas de referencia almacenas en la base de datos del sistema, se fija un umbral, que es comprado con el valor obtenido del cálculo de la HD entre dos plantillas. Además se evalúan tres parámetros, para tener una mejor distinción entre las plantillas:

- Contador
- Promedio HD
- Valor mínimo HD

Las posibles de combinaciones de estos parámetros para la búsqueda de coincidencias son:

- Contador y promedio HD
- Contador y valor mínimo HD
- Promedio HD y valor mínimo HD
- Contador, promedio HD y valor mínimo HD

3.1.1.6.2. Búsqueda de coincidencias en el proceso de Identificación

En el procedimiento de identificación, se procesa una imagen generando así una plantilla codificada del iris, a la que se llamará plantilla de consulta, seguidamente se realiza la comparación de la plantilla con cada usuario registrado, es decir se compara la plantilla de consulta con las plantillas almacenas por ID (plantillas de referencia).

A continuación se detallan el método de obtención de los parámetros para la búsqueda coincidencias en el proceso de identificación. Previamente se fijado un valor para el umbral.

- **Contador**

Para evaluar el parámetro contador, se ha fijado un valor inicial que varía dependiendo del número de plantillas de referencia que se tenga almacenas por usuarios. Es decir, sí tengo 4 plantillas de referencias el rango de posibles valores que podría tener el contador como valor inicial es de 1 a 4. En el caso de disponer de 5 plantillas el rango sería de 1 a 5.

La plantilla de consulta se compara con todas las plantillas de referencia almacenas, de los cuales se obtiene un total de número de comparaciones que cumplen la condición. Sí como resultado de la HD de dos plantillas se obtiene un valor menor o igual al umbral el contador sumará 1.

Para tomar la decisión se considera el número de comparaciones que cumplen con la decisión, debe ser mayor o igual al valor fijado de inicialización del contador.

- **Promedio HD**

Se realiza el cálculo de la HD entre la plantilla de consulta y las plantillas de referencias de cada ID guardado en la base de datos del sistema. El promedio se calcula para todos los IDs, sin considerar si el valor obtenido de la HD es menor o igual al umbral fijado.

El menor valor de promedio es almacenado y se lo compara con el valor del umbral para tomar la decisión. Sí el menor promedio es menor o igual al valor fijado para el umbral, el usuario es identificado.

- **Valor mínimo HD**

Con la estimación de la HD de la plantilla de consulta y las cuatro o cinco plantillas de referencia almacenadas, se calcula el mínimo valor de la HD de todos los IDs guardados, sin considerar si este valor es menor o igual al umbral establecido previamente.

Para luego ser comparados con el valor del umbral y así tomar la decisión. El sujeto es identificado, sí el menor valor mínimo HD es menor o igual al umbral.

- **Promedio HD y valor mínimo HD**

La plantilla de consulta se compara con las plantillas de referencia almacenas en la base de datos del sistema. El promedio HD y mínimo valor HD se estiman para cada ID, sin considerar si los valores obtenidos de las HD son menores o iguales al umbral fijado.

Una vez calculado el valor mínimo HD y promedio HD por cada ID registrado, se determina el menor valor mínimo HD y el menor promedio HD. El sujeto es identificado sí el menor promedio y valor mínimo de la HD son menores o iguales al umbral.

- **Contador y valor mínimo HD o contador y promedio HD**

Adicional de fijar un valor para el umbral, se establece un valor inicial del contador. Sí como resultado de la HD de dos plantillas se obtiene un valor menor o igual a umbral el contador o número de comparaciones que cumplen con la condición sumará 1.

Al concluir las comparaciones entre la plantilla de consulta y las cuatro o cinco plantillas de referencia almacenadas con el mismo ID se estima el promedio o el valor mínimo del cálculo de la HD. El promedio HD y mínimo valor HD se estiman sin considerar si el valor obtenido de la HD es menor o igual al umbral fijado.

La decisión no es tomada hasta que la comparación se haga con toda la base de datos, con cada usuario registrado se determina el valor de contador y promedio o valor mínimo HD, para seleccionar el mayor valor del contador y

menor promedio o valor mínimo de la HD. Sí el menor promedio o valor mínimo de la HD es menor o igual al umbral la plantilla de consulta pertenece a ese ID.

- **Contador, promedio HD y valor mínimo HD**

Se determina la HD de la plantilla de consulta con las plantillas de referencias, sí la respuesta es menor o igual a umbral el contador sumará 1. El valor inicial del contador se ha fijado previamente con el valor del umbral.

Una vez concluidas las comparaciones entre la plantilla de consulta y las plantillas de referencia almacenadas con el mismo ID se estima el promedio, el valor mínimo HD y valor de contador.

Se selecciona el menor promedio HD, menor valor mínimo y mayor contador para tomar la decisión, el menor promedio y valor mínimo de la HD deben ser menor o igual al umbral fijado, para que el sujeto sea identificado. Además, el contador deber ser mayor o igual al valor de inicialización.

En la figura 25 se muestran las etapas del proceso de identificación considerando cuatro plantillas de referencias por usuario. Primero se adquiere la imagen del ojo, para pre-procesar y codificar el iris, obteniendo así la plantilla y máscara de consulta.

En el tercer punto se hace la comparación de la plantilla y máscara de consulta con las plantillas y máscaras de referencia del ID 1, para establecer el valor de contador y promedio de la HD; este procedimiento se repite para los N IDs registrados en el sistema.

Al concluir la comparación con todas las plantillas y máscaras de la base de datos, se determinan los valores de los parámetros de búsqueda de coincidencias, ya sea combinado o por separado (contador, valor mínimo HD y promedio HD). Por último, se evalúa el menor valor del promedio, valor mínimo de la HD y mayor contador.

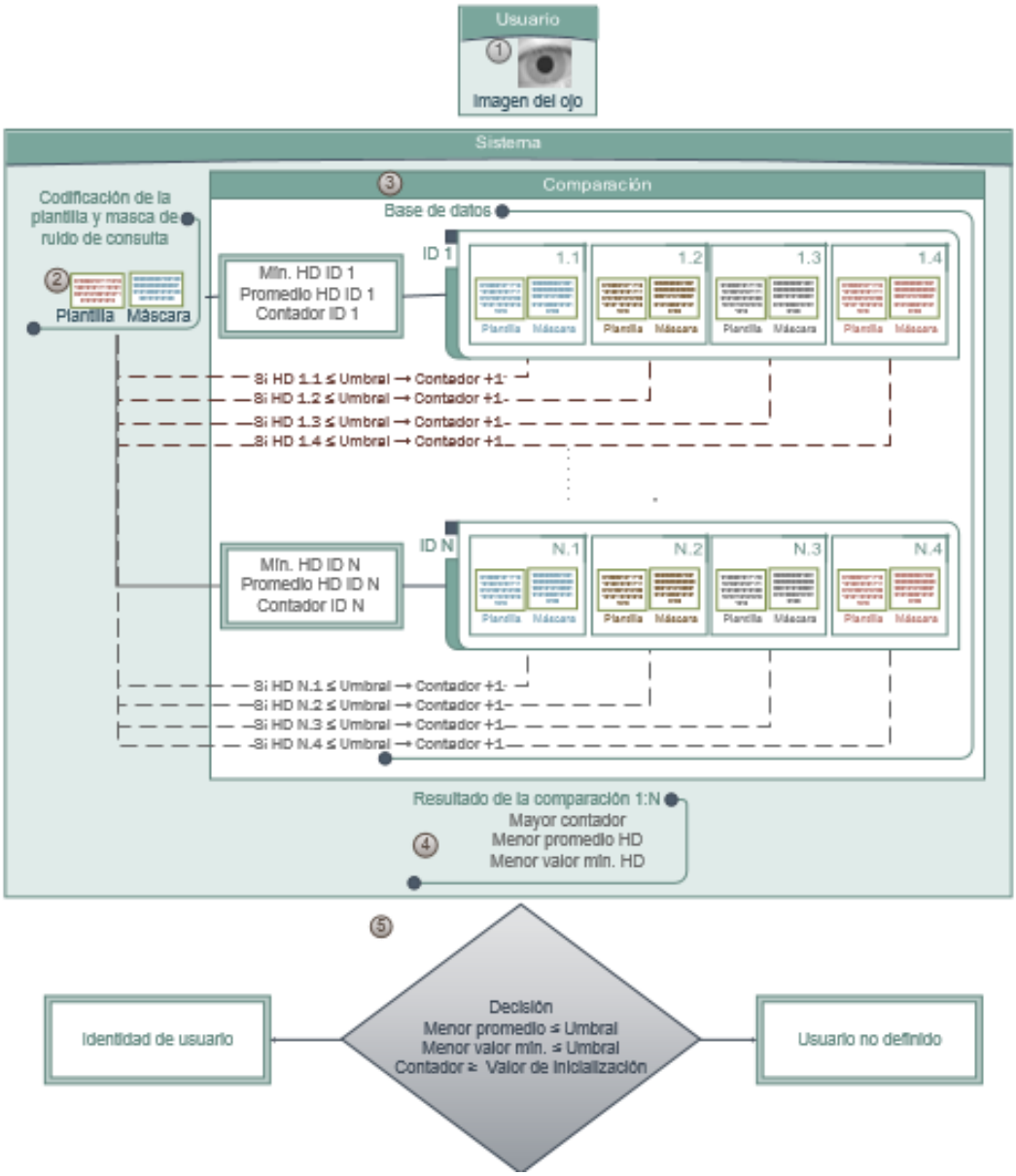

Figura 25. Etapas del proceso de reconocimiento

3.1.1.6.3. Búsqueda de coincidencias en el proceso de autenticación

En el proceso de autenticación, el usuario a más de proporcionar una imagen digital de ojo debe proveer su ID. Primero se constata de que el ID se encuentre registrado, posteriormente con esa información entregada se realizar la comparación de la plantilla y máscara codificada del usuario con las plantillas y máscaras almacenadas en la base de datos, correspondientes al ID otorgado por el usuario.

Al igual que en el proceso de identificación se ha establecido un valor para el umbral. Se especifican el procedimiento de obtención de los parámetros para la búsqueda coincidencias en el método de verificación a continuación.

- **Contador**

Para evaluar el contador es necesario fijar un valor de inicialización con anticipación. La plantilla de consulta se compara con las 4 o 5 plantillas de referencia almacenas, correspondientes al ID con el que se pretende autentificar. Sí como resultado de la HD de dos plantillas se obtiene un valor menor o igual al umbral el contador sumará 1. Obteniendo un total de número de comparaciones que cumplen la condición. El sujeto es verificado si el contador es mayor o igual al valor fijado de inicialización del contador.

- **Promedio HD**

Se determina la HD entre la plantilla de consulta y las plantillas de referencias del ID con el que se quiere autentificar. El promedio se obtiene sin considerar si el valor obtenido de la HD es menor o igual al umbral. El sujeto es verificado sí el valor del promedio es menor o igual al valor fijado para el umbral.

- **Valor mínimo HD**

La plantilla de consulta y las cuatro o cinco plantillas de referencia almacenadas del ID con el que se quiere verificar, se comparan para calcular el mínimo valor de la HD. Sí el menor valor mínimo HD es menor o igual al umbral, es autentificado como usuario del sistema.

- **Promedio HD y valor mínimo HD**

La plantilla de consulta se compara con las plantillas de referencia almacenas. El promedio HD y mínimo valor HD se estiman sin considerar si el valor obtenido de la HD es menor o igual al umbral fijado. El sujeto es identificado sí el promedio y valor mínimo de la HD son menores o iguales al umbral.

- **Contador y valor mínimo HD o contador y promedio HD**

El usuario será aceptado si el promedio o valor mínimo de la HD de las plantillas almacenadas es menor o igual al umbral determinado.

Adicionalmente el total de comparaciones entre el usuario y la base de datos que son menores o iguales al umbral, debe ser mayor o igual al valor de inicialización de contador.

- **Contador, promedio HD y valor mínimo HD**

Se realiza la comparación entre la plantilla de consulta y las cuatro o cinco plantillas de referencia almacenadas del ID con el que se desea verificar, sí como resultado de la HD se obtiene un valor menor o igual a umbral el contador sumará 1.

Se calcula el promedio y el valor mínimo del cálculo de la HD sin considerar si el valor obtenido de la HD es menor o igual al umbral fijado. El sujeto será verificado como usuario del sistema sí el promedio HD y valor mínimo HD son menores o iguales al umbral. Conjuntamente el contador debe ser mayor o igual al valor inicial fijado.

En la figura 26 se observa la metodología de verificación estimando cuatro plantillas de referencias alacenas en la base de datos. Para iniciar este proceso el sujeto que desee ser verificado como usuario del sistema debe proveer una imagen del ojo, que será pre-procesada, obteniendo así la plantilla y máscara de consulta. Así mismo, el sujeto debe proporcionar un ID, el cual es verificado por el sistema.

Como siguiente paso se realiza la comparación de la plantilla y máscara de consulta con las plantillas y máscaras de referencia, para establecer el valor de contador, promedio de la HD y valor mínimo HD. Por último, se evalúa el valor del promedio, valor mínimo de la HD y mayor contador.

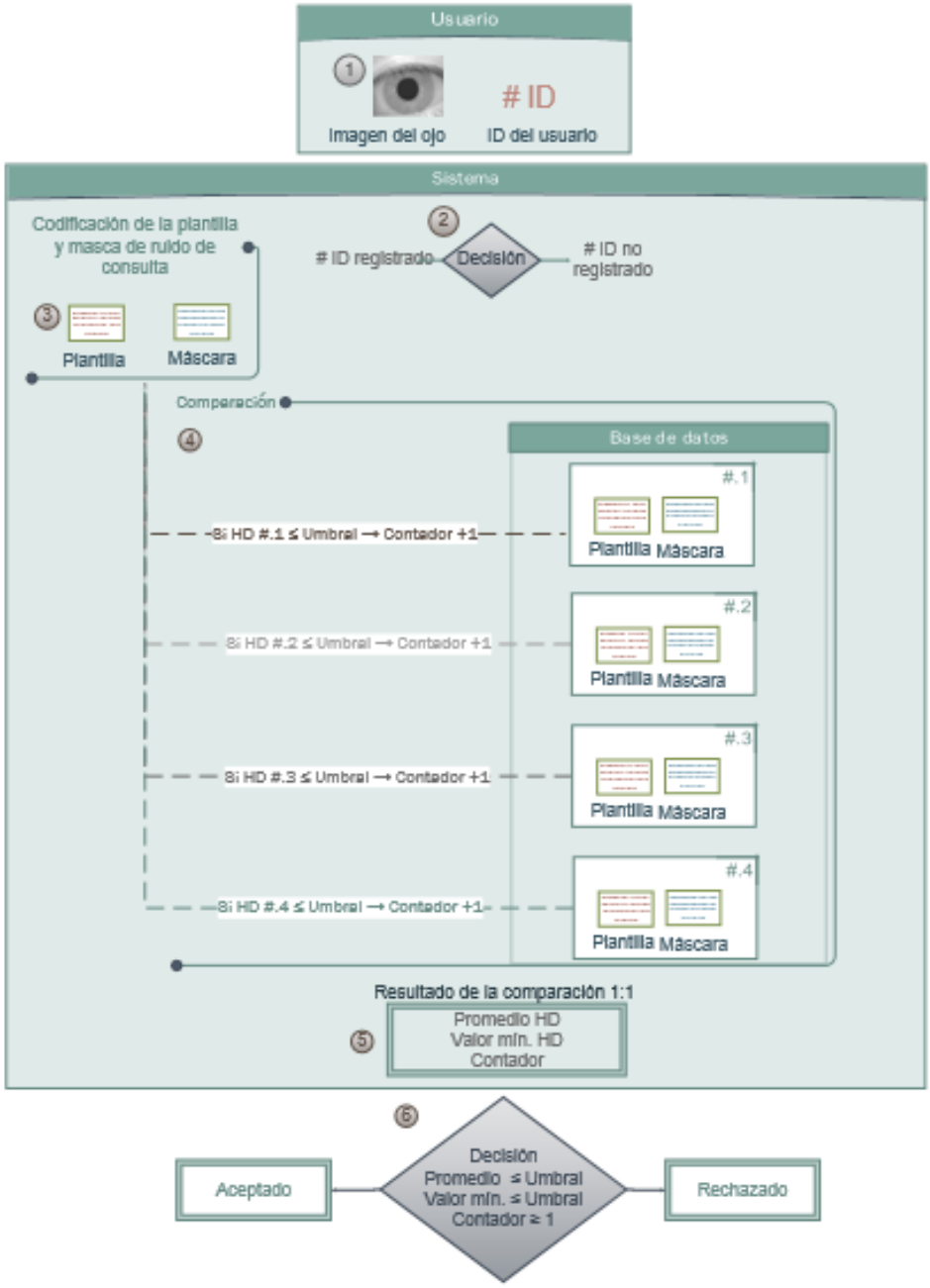

Figura 26. Etapas del proceso de autenticación

3.1.2. Sistema de biometría cancelable para reconocimiento del iris

Fundamentalmente, la biometría cancelable efectúa una alteración de los patrones biométricos, previo a su comparación. Para provocar una distorsión en el patrón del iris, se implementaron dos metodologías: Gray-Combo y Bin-Salt. Se desarrolló una función de transformación, un conjunto de parámetros

de transformación o patrón extra; para obtener los esquemas de biometría cancelable.

3.1.2.1. Gray-Combo

Gray-Combo es una técnica de enfoque de transformación no invertible. Una vez cumplidas las etapas de segmentación y normalización del iris, se obtiene la imagen del iris y máscara de ruido sin envolver, de dimensiones (20 x 480) pixeles cada una. En base a lo propuesto en (Zuo, 2008) se realiza la implementación de un esquema de CB, en el cual se desplazan y combinan de las filas de las imágenes del iris y máscara de ruido previamente obtenidas.

3.1.2.1.1. Parámetros de distorsión

El conjunto de parámetros de transformación es una matriz de dimensiones (20 x 13) conformada por números aleatorios en el rango de -20 a 20. La matriz que contiene el conjunto de parámetros se puede guardar en un dispositivo de almacenamiento (token). La función de transformación estima el valor de treinta posiciones de la matriz como parámetros. En la figura 27 se indica un ejemplo de token, en el cual se señal los valores que serán empleados para la modificación de la imagen normalizada del iris. Se distinguen los parámetros de desplazamiento, estos valores denotan las posiciones que recorrerá cada fila. Así mismo los parámetros de adición, muestran las filas que se suman entre sí.

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	9	-18	8	1	11	-16	2	8	9	19	12	18	-13
2	8	-17	6	-17	-4	5	-8	-8	19	2	3	-2	19
3	12	12	1	-4	-9	-15	-14	1	10	7	-2	-18	-10
4	-9	18	16	-16	-19	-15	5	14	18	-19	-10	15	17
5	8	8	11	-16	7	-16	20	4	15	13	10	5	-11
6	2	-15	-5	12	-3	-15	-14	-7	10	10	-11	-6	-5
7	-4	9	-12	-9	-2	-14	-10	-8	10	-16	-18	20	-17
8	-18	-16	-17	4	5	-12	-4	-2	-16	1	11	-11	6
9	-2	2	1	1	-4	-4	-1	-5	5	8	7	6	-13
10	-7	6	-12	-3	-8	-8	8	-6	-2	2	9	4	-19
11	4	-7	-5	-8	1	-7	5	8	-7	7	-8	3	5
12	10	6	2	11	8	-10	20	10	-16	-3	-3	-15	-6
13	-16	10	-11	-3	-15	16	-4	-3	13	-13	-4	-19	7
14	-15	3	6	6	-15	8	5	-3	-13	-10	13	-3	-5
15	2	10	-1	-16	-17	5	-14	-15	-14	-20	-7	7	5
16	-1	-11	-14	18	-20	12	-5	-19	7	17	13	13	-20
17	16	10	12	-13	-3	4	-14	-9	16	6	12	20	17
18	12	19	-16	-10	6	2	11	-7	1	18	14	3	12
19	10	15	-8	12	9	14	15	6	8	-14	0	17	10
20	-18	-17	-11	-1	1	8	-6	19	-14	17	6	3	13

Parámetros de adición

Parámetros de desplazamiento

Figura 27. Parámetros de transformación para la función Gray-Combo

3.1.2.1.2. Función de distorsión

Primero se realiza el desplazamiento circular de las filas de la platilla y máscara de ruido en dirección horizontal, con la ayuda de parte de los parámetros transformación; los valores negativos provocan traslados hacia la izquierda. Por otra parte la rotación hacia la derecha genera valores positivos, como se puede observar en la figura 28.

Figura 28. Desplazamiento de filas

A continuación se eligen las filas que se van a unir; la selección de las filas se realiza de igual forma por los parámetros fijados en el token. Un operador de adicción se emplea para combinar dos filas; las filas solo son usadas una vez en este proceso, como se contempla en la figura 29.

Figura 29. Adición de filas

3.1.2.2. Bin-Salt

Bin-Salt es una metodología de enfoque salting. En (Zuo, 2008) se plantea así mismo, la técnica de Bin-Salt para generar plantillas de CB. Después de cumplir las fases de segmentación, normalización y codificación del iris, extrayendo una plantilla del iris y máscara de ruido de (20 x 480) bits cada una, este método realiza la mezcla del código del patrón del iris original con un patrón extra de las mismas dimensiones.

3.1.2.2.1. Plantilla extra

La plantilla adicional se genera a través de una distribución uniforme, conformada por unos y ceros, de dimensiones (20 x 480) bits, como se exponen en la figura 30. Este patrón extra puede ser tomado como clave o token. Esta clave permite que el biocódigo obtenido después del proceso de combinación no sea inundado con la información de la plantilla extra.

Figura 30. Plantilla ruido aleatorio

3.1.2.2.2. Función de distorsión

Este método mezcla el código del patrón del iris original con un patrón extra, para ello se emplea la función XOR; que es una función no invertible. Pues si por ejemplo si se tiene 0, no se tiene la certeza si es el resultado de $1\ XOR\ 1$ o $0\ XOR\ 0$. En la figura 31 se indica el procedimiento para la obtención de biocódigos usando la técnica Bin-Salt.

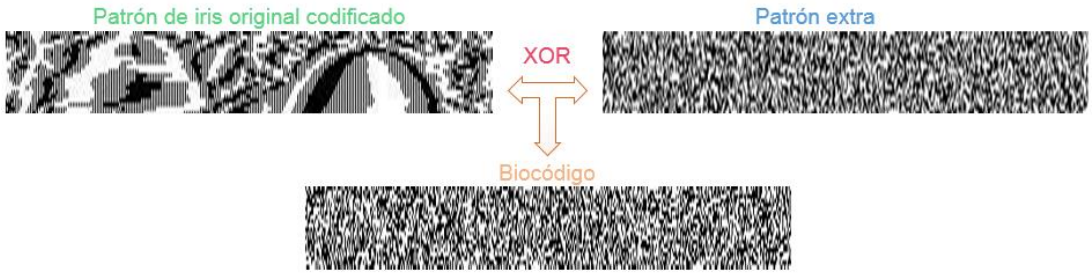

Figura 31. Procedimiento para generar biocódigos empleando transformación Bin-Salt

CAPÍTULO 4

RESULTADOS Y ANÁLISIS

4.1. Resultados experimentales

En (Belguechi R. C., 2012) se realiza el análisis de la seguridad y privacidad, además de la verificación del cumplimiento de las propiedades de los esquemas desarrollados para CB. Se dispuso de la base datos CASIA_IrisV1, con 7 imágenes pertenecientes a 108 sujetos, que permitieron generar plantillas del patrón del iris de los usuarios registrados; por otra parte, con la base de datos CASIA-IrisV3, se simularon a 103 intrusos; con los que se realizaron pruebas para determinar la robustez de los sistemas.

Se fijó un punto de operación o umbral de decisión ϵ, como referencia, además se establecieron tres parámetros para la búsqueda de coincidencias (promedio HD, mínimo valor HD y contador) en el sistema de biometría sin ninguna distorsión en las plantillas obtenidas de cada individuo registrado; así se pudo calcular ocho criterios A_i, que cuantifican el cumplimiento de las propiedades y la robustez de los esquemas de biometría cancelable.

4.1.1. Punto de operación y parámetros de búsqueda de coincidencias

Los sistemas de biometría con el fin de proporcionar mayor seguridad, pretenden obtener un valor bajo de la FAR, en lugar de EER. El valor definido para la FAR depende del nivel de seguridad requerido por la aplicación del sistema de biometría (Mayoue, 2007). La FAR define el umbral o punto de operación ϵ; que es un parámetro de referencia, que se compara con el resultado del cálculo de la HD entre dos plantillas biométricas, para decidir si un sujeto es aceptado o rechazado por el sistema.

Para seleccionar el valor de ϵ y los parámetros de búsqueda de coincidencia, se evalúa al sistema de biometría en un rango de 0.35 a 0.45. En primer lugar se estima la FAR y FRR del sistema de biometría, planteando las opciones de autenticación e identificación de los usuarios registrados en

el sistema, se hace una distinción en los parámetros de búsqueda de coincidencia.

4.1.1.1. Punto de operación y parámetros de búsqueda de coincidencias del proceso de autenticación

En el procedimiento de autenticación se obtiene la FRR realizando la comparación de las plantillas biométricas de consulta de cada usuario registrado con sus correspondientes plantillas de referencia almacenas en la base de datos del sistema. Por otra parte, para calcular la FAR se hace la comparación de las plantilla de consulta de los usuarios inscritos con de las plantillas de referencia almacenas, excepto con las plantillas correspondientes al mismo usuario. Es decir, se genera varios intentos falsos de verificación.

En la tabla 1, se muestran los valores resultantes del porcentaje la FAR y FRR del proceso de autenticación, considerando 4 plantillas de referencias, se hace una distinción entre el cálculo del promedio HD, valor mínimo y la combinación de estos dos parámetros.

Tabla 1:
Evaluación del promedio HD, valor mínimo HD y su combinación en el proceso de autenticación con 4 plantillas de referencia

ϵ	Valor mínimo HD		Promedio HD		Valor mínimo y promedio HD	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	13,888	0	18,209	0	18,209	0
0,36	9,753	0	16,049	0	16,049	0
0,37	7,168	2,974	12,654	0	12,654	0
0,38	6,805	5,515	12,037	0	12,037	0
0,39	5,322	8,072	11,111	0	11,111	0
0,40	5,292	10,695	8,641	0,592	8,641	0,308
0,41	3,473	59,731	7,716	1,604	7,716	0,308
0,42	2,974	79,818	5,246	7,273	5,246	3,395

0,43	2,063	93,951	3,395	17,901	3,395	15,432
0,44	1,963	99,721	2,777	53,395	2,777	48,765
0,45	1,240	100	1,543	93,827	1,543	88,272

Los porcentajes de la FAR y FRR de la evaluación del contador en el proceso de autenticación, considerando 4 plantillas de referencia, se muestran en la tabla 2.

Tabla 2:
Evaluación del contador en el proceso de autenticación con 4 plantillas de referencia

	Contador							
ϵ	**1**		**2**		**3**		**4**	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	10,80	0,61	16,04	0,61	22,53	0	42,59	0
0,36	8,95	2,16	13,88	1,85	18,82	0,30	35,80	0
0,37	6,48	2,85	10,80	2,68	17,59	1,23	29,01	0,30
0,38	5,55	3,02	9,87	4,52	14,19	3,31	25,30	0,61
0,39	4,63	3,52	8,95	6,92	13,88	5,34	22,22	1,64
0,4	4,01	5,69	6,48	7,32	12,03	9,65	18,82	3,21
0,41	3,08	7,62	6,17	8,24	10,80	11,28	15,43	7,24
0,42	2,46	8,35	4,32	8,53	8,64	13,74	12,96	10,39
0,43	1,85	8,76	3,39	9,28	8,33	15,17	10,49	13,32
0,44	1,23	9,60	3,08	12,76	5,86	17,98	7,40	19,33
0,45	0,61	12,28	1,54	15,85	4,01	20,53	6,48	25,93

En la tabla 3, se muestran los valores resultantes del porcentaje la FAR y FRR del proceso de autenticación, considerando 4 plantillas de referencias almacenas en la base de datos del sistema por usuario registrado. Además se hace una distinción entre el cálculo del promedio HD, valor mínimo y el valor de inicialización del contador.

Tabla 3:

Evaluación del contador y promedio o valor mínimo HD en el proceso de autenticación con 4 plantillas de referencia

Contador y promedio HD								
ϵ	1		2		3		4	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	14,81	0	15,43	0	19,13	0	30,86	0
0,36	12,65	0	13,58	0	16,04	0	25,92	0
0,37	10,80	0	10,80	0	14,81	0	21,60	0
0,38	10,18	0	10,49	0	11,72	0	18,82	0
0,39	9,25	0	9,56	0	11,72	0	16,97	0
0,4	7,09	0,30	7,09	0,30	10,72	0	15,74	0
0,41	6,17	0,30	6,48	0,30	9,25	2,16	13,27	0
0,42	3,70	3,39	4,01	3,39	7,09	7,71	11,42	0,61
0,43	2,16	11,72	2,46	11,42	6,79	7,71	8,95	3,08
0,44	1,85	33,64	2,16	33,33	4,63	25,61	5,86	11,42
0,45	1,23	62,34	1,54	62,03	2,77	55,55	4,93	33,95
Contador y valor mínimo HD								
ϵ	1		2		3		4	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	10,80	0	16,04	0	22,53	0	42,59	0
0,36	8,95	0	13,88	0	18,82	0	35,80	0
0,37	6,48	0,92	10,80	0	17,59	0	29,01	0
0,38	5,55	1,85	9,87	0,30	14,19	0	25,30	0
0,39	4,63	2,77	8,95	0,30	13,88	0	22,22	0
0,4	4,01	7,40	6,48	0,61	12,03	0	18,82	0
0,41	3,08	21,60	6,17	3,08	10,80	0	15,43	0
0,42	2,46	50,61	4,32	14,50	8,64	4,01	12,96	0,61
0,43	1,85	85,80	3,39	39,19	8,33	13,88	10,49	4,01
0,44	1,23	99,38	3,08	79,32	5,86	44,13	7,40	17,28
0,45	0,61	100	1,54	99,69	4,01	86,11	6,48	52,1

La evaluación de la combinación de los tres parámetros de búsqueda de coincidencias, considerando 4 plantillas de referencias en el proceso de verificación se indica en la tabla 4.

Tabla 4:
Evaluación del promedio HD, valor mínimo HD y contador en el proceso de autenticación con 4 plantillas de referencia

Contador, valor mínimo y promedio HD								
ϵ	**1**		**2**		**3**		**4**	
	FAR	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**
0,35	18,20	0	18,82	0	23,45	0	43,21	0
0,36	16,04	0	15,74	0	18,82	0	36,42	0
0,37	12,65	0	12,65	0	17,59	0	29,63	0
0,38	12,03	0	12,34	0	14,19	0	25,92	0
0,39	11,11	0	11,42	0	13,88	0	22,84	0
0,4	8,64	0,19	8,64	0,30	12,03	0	19,44	0
0,41	7,71	0, 19	8,02	0,30	12,65	0	16,04	0
0,42	5,24	1,53	5,55	4,01	8,64	2,46	13,58	0,61
0,43	3,39	5,36	3,70	16,04	8,33	11,72	11,11	4,01
0,44	2,77	35,14	3,08	49,69	5,86	40,12	8,33	52,16
0,45	1,54	60,47	1,85	89,50	4,01	83,33	7,40	17,28

Analizando los valores de las tablas 1, 2, 3 y 4, se optó por considerar la combinación del contador con promedio o el valor mínimo de la HD, en base a los valores obtenidos de la FAR y la FRR, visto que fueron los más bajos, respecto a estimarlos por separado o en otras combinaciones. El valor de inicialización del contador se establece en 1. Se grafica la FAR y la FRR, en donde se distinguen la EER; como se observa en la figura 32. La EER se ubica cerca del umbral igual a 0.42 para el caso de considerar el promedio HD. Considerando el valor mínimo la EER se sitúa en el umbral igual a 0.39.

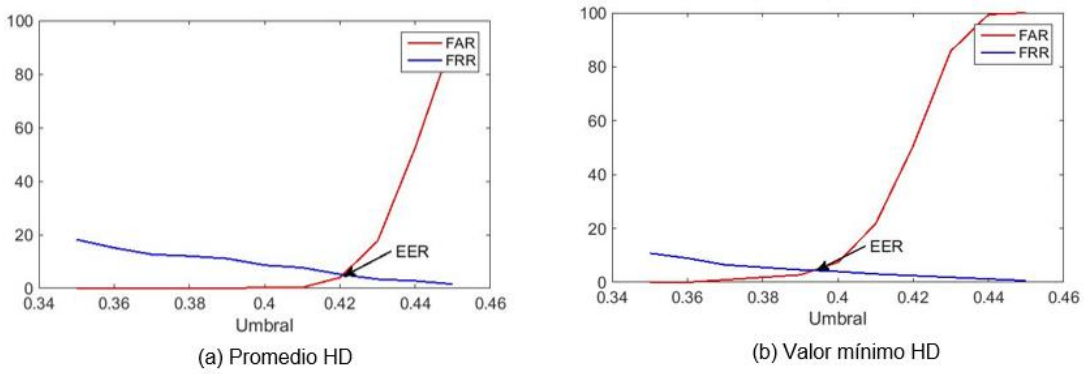

Figura 32. Distribución de la FAR y FRR del proceso de autenticación con 4 plantillas de referencia

Del mismo modo, se determinaron los valores del porcentaje la FAR y FRR del proceso de autenticación con 5 plantillas de referencia. Se hace un discernimiento de la estimación del promedio HD, valor mínimo HD y su combinación. Los resultados se indican en la tabla 5.

Tabla 5:
Evaluación del promedio HD, valor mínimo HD y su combinación en el proceso de autenticación con 5 plantillas de referencia

ϵ	Valor mínimo HD		Promedio HD		Valor mínimo y promedio HD	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	11,173	0	18,854	0	18,854	0
0,36	9,723	0	17,936	0	17,936	0
0,37	7,891	0,935	17,647	0	17,647	0
0,38	5,935	2,845	15,745	0	15,745	0
0,39	5,029	3,954	13,897	0	13,897	0
0,40	4,963	11,111	10,723	0	10,723	0
0,41	3,527	29,749	9,785	0	9,785	0
0,42	2,473	73,552	6,832	4,167	6,832	2,778
0,43	2,165	96,824	5,271	19,237	5,271	12,037
0,44	1,348	99,358	2,743	78,358	2,743	41,667
0,45	0.924	100	2,056	92,130	2,056	85

En la tabla 6, se muestran los porcentajes de la FAR y FRR de la evaluación del contador en el proceso de autenticación, con 5 plantillas de referencia almacenadas por cada usuario registrado en el sistema.

Tabla 6:
Evaluación del contador en el proceso de autenticación con 5 plantillas de referencia

ϵ	Contador									
	1		2		3		4		5	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	8,7	0,9	16,2	0,4	20,3	0,4	29,1	0,4	48,1	0,3
0,36	7,8	1,8	13,4	2,3	18,5	1,8	23,1	1,3	42,1	0,6
0,37	5,5	2,3	10,6	4,1	15,2	2,9	20,3	1,9	32,4	1,4
0,38	4,6	2,6	9,2	5,9	13,4	3,9	17,1	3,9	28,7	2,4
0,39	4,1	3,9	7,4	7,9	12,9	5,9	16,2	4,5	25,4	4,3
0,40	3,7	4,8	5,5	8,8	9,7	6,4	12,9	6,0	22,2	9,8
0,41	2,7	5,9	4,6	9,4	8,3	7,8	11,1	8,9	18,0	11,7
0,42	1,8	6,0	3,7	11,2	4,6	9,2	9,2	13,2	15,2	12,5
0,43	1,3	8,2	2,7	12,5	3,7	10,3	9,2	16,6	12,5	19,7
0,44	0,9	13,5	1,8	15,2	3,2	12,9	6,0	19,9	10,1	26,7
0,45	0	15,9	0,9	23,6	1,8	28,5	3,7	47,6	8,3	51,1

En la tabla 7, se muestran los valores resultantes del porcentaje la FAR y FRR del proceso de autenticación, considerando 5 plantillas de referencias. Se hace una distinción entre el cálculo del promedio HD, valor mínimo y el valor de inicialización del contador.

Tabla 7:

Evaluación del contador y promedio o valor mínimo HD en el proceso de autenticación con 5 plantillas de referencia

Contador y promedio HD

ϵ	1		2		3		4		5	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	19,4	0	19,9	0	21,7	0	29,1	0	48,1	0
0,36	16,6	0	17,5	0	18,5	0	23,1	0	42,1	0
0,37	16,2	0	16,2	0	16,6	0	20,3	0	32,4	0
0,38	13,4	0	13,4	0	15,2	0	16,6	0	28,7	0
0,39	10,1	0	10,6	0	13,4	0	16,2	0	25,4	0
0,40	6,4	0	6,4	0	9,7	0	12,963	0	22,2	0
0,41	5,5	0	5,5	0	8,3	0	11,1	0	18,0	0
0,42	4,6	3,7	4,6	3,7	5,0	3,2	9,2	1,3	15,2	0
0,43	2,7	15,2	3,7	15,2	3,7	12,5	9,2	6,9	12,5	2,3
0,44	1,8	46,7	1,8	46,7	3,2	43,5	6,0	28,7	10,1	13,4
0,45	1,8	89,8	1,8	89,8	1,8	86,5	3,7	71,7	8,3	41,2

Contador y valor mínimo HD

ϵ	1		2		3		4		5	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**
0,35	8,7	0	16,2	0	20,3	0	29,1	0	48,1	0
0,36	7,8	0	13,4	0	18,5	0	23,1	0	42,1	0
0,37	5,5	0,4	10,6	0	15,2	0	20,3	0	32,4	0
0,38	4,6	1,8	9,2	0,4	13,4	0	16,6	0	28,7	0
0,39	4,1	2,7	7,4	0,4	12,9	0	16,2	0	25,4	0
0,40	3,7	10,1	5,5	0,9	9,7	0	12,9	0	22,2	0
0,41	2,7	25,9	4,6	5,0	8,3	0	11,1	0	18,0	0
0,42	1,8	52,3	3,7	18,0	4,6	4,6	9,2	1,3	15,2	0
0,43	1,3	86,5	2,7	44,9	3,7	18,9	9,2	6,9	12,5	2,3
0,44	0,9	99,5	1,8	83,7	3,2	55,5	6,0	29,6	10,1	13,4
0,45	0	100	0,9	99,5	1,8	93,9	3,7	72,2	8,3	41,2

En la tabla 8 se indica la estimación de la FAR y FRR de la combinación de los tres parámetros de búsqueda de coincidencias, considerando 5 plantillas de referencias en el proceso de verificación.

Tabla 8:
Evaluación del promedio HD, valor mínimo HD y contador en el proceso de autenticación con 5 plantillas de referencia

Contador, valor mínimo y promedio HD										
	1		**2**		**3**		**4**		**5**	
ϵ	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	18,8	0	19,1	0	25,3	0	31,9	0	51,6	0
0,36	17,9	0	18,4	0	20,9	0	22,5	0	48,3	0
0,37	17,6	0	18,1	0	18,3	0	20,2	0	42, 7	0
0,38	15,7	0	16,4	0	17,6	0	19,2	0	37,6	0
0,39	13,8	0	14,4	0	15,2	0	17,5	0	35,1	0
0,40	10,7	0	13,4	0	13,9	0	15,1	0	30,2	0
0,41	9,7	0	10,1	0	12,6	0	13,3	0	20,1	0
0,42	6,8	2,7	8,6	2,7	10,2	2,3	12,9	1,3	18,1	0
0,43	5,2	10,6	7,4	12,5	9,6	11,1	10,5	5,5	15,4	1,3
0,44	2,7	39,8	5,1	40,2	7,3	41,2	9,1	26,3	13,9	11,1
0,45	2,0	83,3	3,3	84,7	5,7	84,2	6,6	68,5	10,2	37,1

Teniendo en cuenta los valores obtenidos en las tablas 5, 6, 7 y 8 se ha optado por considerar la combinación del contador con promedio o el valor mínimo de la HD, estableciendo el valor inicial del contador en 1. Los porcentajes obtenidos de la FAR y la FRR fueron los más bajos, respecto a evaluarlos por separado o en otras combinaciones. En la figura 33 se muestran graficados la FAR y FRR, donde se señala la EER del sistema. Se puede observar que la ERR se posiciona próxima al umbral de 0.42 estimando el promedio HD. Por otra parte, al considerar el valor mínimo HD la ERR se localiza cercana al umbral de 0.39 al igual que en la figura 32.

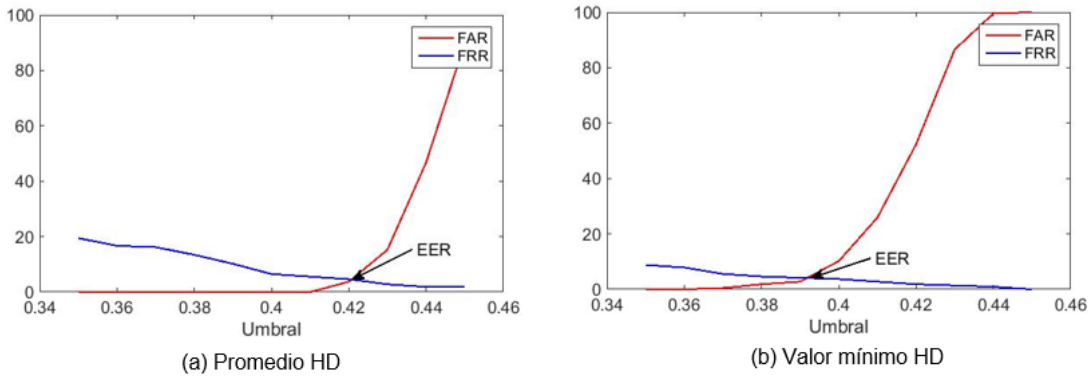

Figura 33. Distribución de la FAR y FRR del proceso de autenticación con 5 plantillas de referencia

Lo que se busca es obtener una FAR del 0%, es decir ningún intruso o impostor verificado como usuario, además de tener una FRR baja. Observando los valores de las tablas 3 y 7, correspondientes al proceso de autenticación, donde se estima el contador y promedio HD o valor mínimo HD en los sistemas de biometría sin ninguna modificación en las plantillas, los valores del umbral que cumplen estas condiciones son 0.36, 0.39 y 0.41.

Para fijar el punto de operación en el método de verificación, se estima el porcentaje de la FRR y FAR de los esquemas de CB con estos valores, contemplando las dos técnicas de búsqueda de coincidencias. En la tabla 9 se indican los resultados de los sistemas con la transformación Gray-Combo.

Tabla 9:
Evaluación del proceso de autenticación en los sistemas con Gray-Combo

	Gray-Combo							
	Almacenando 4 plantillas				Almacenando 5 plantillas			
ϵ	Promedio HD		Valor mínimo HD		Promedio HD		Valor mínimo HD	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0.36	15.123	0	7.407	0	17.592	0	6.944	0
0.39	9.876	0	3.703	2.160	7.870	0	3.703	1.851
0.41	7.407	0.617	2.469	8.641	5.555	0.462	2.777	10.185

En la tabla 10 se muestran los resultados de los sistemas con la transformación Bin-Salt, de igual manera se consideran las dos metodologías para la búsqueda de coincidencias.

Tabla 10:

Evaluación del proceso de autenticación en los sistemas con Bin-Salt

Bin-Salt								
ϵ	Almacenando 4 plantillas				Almacenando 5 plantillas			
	Promedio HD		Valor mínimo HD		Promedio HD		Valor mínimo HD	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0.36	33.641	0	17.592	0	38.888	0	14.084	0
0.39	24.074	0	10.185	0.925	24.074	0	6.944	0.925
0.41	16.049	0	8.024	4.012	14.814	0	6.018	6.481

Analizando los datos obtenidos en las tablas 10 y 11, que se refieren a la evaluación de los esquemas de CB en el proceso se autenticación, se han fijado el valor de umbral de 0.39 estimando el promedio HD, para la verificación de usuarios. Por otra parte, considerando el valor mínimo HD se determinó un valor de umbral del 0.36 para la autenticación.

4.1.1.2. Punto de operación y parámetros de búsqueda de coincidencias del proceso de identificación

Conjuntamente se realiza la evaluación del sistema biometría con el método de identificación. Para ello, se estimó la FRR y FAR de las comparaciones de las plantillas de consulta de todos los usuarios, con cada una de las plantillas de referencia almacenas en la base de datos del sistema, para ser reconocidos.

La FRR se evalúa cuando las plantillas de referencias de los usuarios inscritos no son identificadas o reconocidas por sistema. Por otra parte, sí las plantillas de referencias de los usuarios son reconocidos con un diferente ID al que les corresponde se calcula la FAR; esta plantillas se consideran

falsamente aceptadas, pues no todos los usuarios cuentan con el mismo acceso a información o privilegios.

En la tabla 11 se exponen los resultados de la estimación de la FAR y FRR con 4 plantillas de referencia almacenas por usuario registrado en el sistema. Se realiza una diferenciación en la estimación del promedio HD, valor mínimo y su combinación.

Tabla 11:
Evaluación del promedio HD, valor mínimo HD y su combinación en el proceso de identificación con 4 plantillas de referencia

ϵ	**Valor mínimo HD**		**Promedio HD**		**Valor mínimo y promedio HD**	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	17,237	0	23,945	0	23,945	0
0,36	12,873	0	19,862	0	19,862	0
0,37	9,241	1,934	15,923	0	15,923	0
0,38	6,823	2,936	13,952	0	13,952	0
0,39	6,129	3,172	12,634	0	12,634	0
0,40	4,929	4,444	10,885	0	10,885	0
0,41	3,962	5,823	8,924	0	8,924	0
0,42	1,963	5,945	7,023	1,837	7,023	0,617
0,43	1,273	7,734	5,938	3,912	5,938	1,543
0,44	0,942	8,349	1,935	4,824	1,935	2,778
0,45	0,716	10,37	1,066	5,024	1,066	2,778

En la tabla 12 se exponen los porcentajes de la FAR y FRR de la evaluación del contador en el proceso de identificación, considerando 4 plantillas de referencia almacenas en la base de datos del sistema de biometría, para ello se varia su valor inicial.

Tabla 12:

Evaluación del contador en el proceso de identificación con 4 plantillas de referencia

ϵ	Contador							
	1		2		3		4	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	3,02	5,85	4,18	6,91	6,04	7,19	15,42	0
0,36	2,529	5,55	3,95	5,85	5,88	6,32	11,63	0
0,37	1,984	4,16	2,32	4,26	5,02	5,39	8,92	0,30
0,38	1,362	4,08	2,03	4,52	4,87	3,08	3,84	0,61
0,39	0, 835	3, 03	1,62	3,92	2,95	2,54	2,42	1,64
0,4	0,671	3, 07	1,11	7,32	1,48	3,65	1,03	3,21
0,41	0,294	4,66	0,82	8,24	0,92	12,21	0,99	7,24
0,42	0	4, 96	0,52	10,53	0,64	13,93	0,64	10,39
0,43	0	5, 925	0,22	13,98	0,33	15,17	0,23	13,32
0,44	0	25, 96	0	21,76	0,16	19,68	0,08	19,33
0,45	0	31, 77	0	45,85	0	29,53	0	25,93

En la tabla 13, se presentan los valores resultantes del porcentaje la FAR y FRR del proceso de reconocimiento, considerando 4 plantillas de referencias. Se hace una distinción entre el cálculo del promedio HD, valor mínimo y el valor de inicialización del contador.

Tabla 13:

Evaluación del contador y promedio o valor mínimo HD en el proceso de identificación con 4 plantillas de referencia

ϵ	Contador y promedio HD							
	1		2		3		4	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	18,20	0	18,82	0	23,45	0	42,59	0
0,36	14,814	0	15,74	0	18,82	0	35,80	0

0,37	12,96	0	12,96	0	17,59	0	28,70	0
0,38	15,12	0	12,34	0	14,19	0	25,30	0
0,39	11,11	0	11,42	0	13,88	0	22,22	0
0,40	8,64	0	8,64	0	12,03	0	19,13	0
0,41	7,71	0	8,02	0	10,80	0	15,12	0
0,42	4,93	0,61	5,24	0,61	8,33	0,30	12,65	0
0,43	2,46	1,54	2,77	1,54	6,79	1,54	9,87	0,61
0,44	0,92	2,77	1,23	2,77	3,39	2,46	5,86	1,85
0,45	0,61	4,01	0,61	1,54	1,23	4,01	2,46	4,32

Contador y valor mínimo HD

ϵ	**1**		**2**		**3**		**4**	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	10,80	0	16,04	0	22,63	0	42,28	0
0,36	8,951	0	13,88	0	18,82	0	35,80	0
0,37	5,86	0,92	10,80	0	17,28	0	29,01	0
0,38	4,93	0,92	9,87	0	14,19	0	25,61	0
0,39	4,32	0,92	8,95	0	13,88	0	22,22	0
0,40	3,39	0,92	6,48	0	12,03	0	18,51	0
0,41	1,23	2,16	5,24	0,92	10,80	0	15,43	0
0,42	0,61	2,77	2,77	1,54	8,33	0,30	12,65	0,31
0,43	0	3,70	1,54	2,77	6,79	1,54	9,87	0,61
0,44	0	3,39	0,92	3,08	3,70	2,46	5,86	1,85
0,45	0	3,70	0	4,01	0,92	4,32	2,46	4,32

En la tabla 14 se expone la estimación de la combinación de los tres parámetros de búsqueda de coincidencias, considerando 4 plantillas de referencias en el proceso de reconocimiento.

Tabla 14:

Evaluación del promedio HD, valor mínimo HD y contador en el proceso de identificación con 4 plantillas de referencia

Contador, valor mínimo y promedio HD								
ϵ	1		2		3		4	
	FAR	FARR	FAR	FARR	FAR	FARR	FAR	FARR
0,35	17,901	0	18,519	0	23,457	0	42,593	0
0,36	14,815	0	15,432	0	18,827	0	35,802	0
0,37	12,654	0	12,654	0	17,593	0	29,012	0
0,38	11,420	0	12,346	0	14,198	0	25,309	0
0,39	10,802	0	11,420	0	13,889	0	22,222	0
0,40	9,642	0	10,582	0	12,037	0	18,827	0
0,41	7,716	0,218	9,025	0	11,111	0	15,123	0
0,42	5,247	0,617	5,247	0,617	9,642	0	12,346	0,309
0,43	2,419	1,543	2,778	1,543	6,790	1,543	9,877	0,617
0,44	1,296	2,778	1,235	2,778	3,704	2,778	5,556	1,852
0,45	1,839	3,704	0	3,704	1,235	4,012	2,469	4,012

Revisando los valores de las tablas 11, 12, 13 y 14 se optó por considerar la combinación del contador con promedio o el valor mínimo de la HD y se estableció el valor de inicialización del contador igual a 1, en base a los valores obtenidos de la FAR y la FRR, ya que fueron los más bajos, respecto a estimarlos por separado o en otras combinaciones. Los valores de la FAR y la FRR se grafican en la figura 34, donde se indica la EER. La EER se localiza cerca del umbral igual a 0.43 para el caso de considerar el promedio HD. Estimando el valor mínimo la EER se sitúa próxima al umbral igual a 0.41.

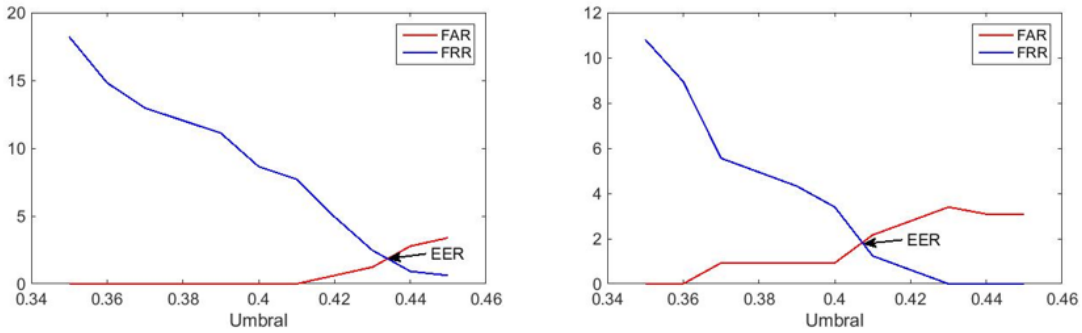

Figura 34. Distribución de la FAR y FRR del proceso de identificación con 4 plantillas de referencia

El porcentaje la FAR y FRR del proceso de reconocimiento almacenando 5 plantillas de referencia por usuario se muestra en la tabla 15, se estima el cálculo del promedio HD, valor mínimo y su combinación.

Tabla 15:
Evaluación del promedio HD, valor mínimo HD y su combinación en el proceso de identificación con 5 plantillas de referencia

ϵ	Valor mínimo HD		Promedio HD		Valor mínimo y promedio HD	
	FRR	FAR	FRR	FAR	FRR	FAR
0,35	12,935	0	20,845	0	20,845	0
0,36	11,111	0	19,945	0	19,945	0
0,37	9,341	0,463	19,354	0	19,354	0
0,38	7,936	0,463	18,379	0	18,379	0
0,39	6,935	0,463	15,111	0	15,111	0
0,40	5,493	0,9259	13,863	0	13,863	0
0,41	5,071	1,8519	7,924	0	7,924	0
0,42	3,956	2,778	6,824	0,926	6,824	0,463
0,43	3,845	2,778	4,927	1,852	4,927	2,315
0,44	2,778	2,778	3,333	1,852	3,333	2,778
0,45	2,934	2,778	3,186	2,315	3,186	2,778

En la tabla 16, se muestran los porcentajes de la FAR y FRR de la evaluación del contador en el proceso de identificación, con 5 plantillas de referencia.

Tabla 16:
Evaluación del contador en el proceso de identificación con 5 plantillas de referencia

	Contador									
ϵ	**1**		**2**		**3**		**4**		**5**	
	FRR	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**
0,35	3,5	6,3	4,8	12,9	5,6	11,9	9,9	7,1	11,4	0
0,36	26	5,5	3,9	11,5	4,9	10,7	6,8	6,3	9,6	0
0,37	2,2	4,1	3,3	7,8	4,2	10,3	6,2	5,3	5,9	0,3
0,38	1,9	4,3	2,2	7,4	3,6	10,1	5,8	3,1	3,8	0,6
0,39	1,4	3,7	1,8	5,1	2,6	9,9	4,5	2,5	2,4	1,6
0,4	0,7	3,2	1,2	4,9	2,3	3,6	3,8	3,6	1,2	3,2
0,41	0,3	4,1	1,2	2,1	1,1	4,5	2,2	12,2	0,9	7,2
0,42	0	4,6	0,8	3,3	1,2	12,9	1,4	13,9	0,5	10,3
0,43	0	5,1	0,4	5,4	0,4	15,6	1,1	15,1	0,3	11,3
0,44	0	12,9	0	10,0	0	17,6	0,6	16,6	0,1	13,3
0,45	0	27,7	0	21,8	0	20,4	0	19,2	0	15,5

En la tabla 17, se exponen los valores resultantes del porcentaje la FAR y FRR del proceso de identificación, considerando 5 plantillas de referencias almacenas. Se evalúa el cálculo del promedio HD, valor mínimo y el valor de inicialización del contador.

Tabla 17:

Evaluación del contador y promedio o valor mínimo HD en el proceso de identificación con 5 plantillas de referencia

Contador y promedio HD

ϵ	1		2		3		4		5	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0,35	19,4	0	19,9	0	21,7	0	29,1	0	48,1	0
0,36	16,6	0	17,5	0	18,5	0	23,1	0	42,1	0
0,37	16,2	0	16,2	0	16,6	0	20,3	0	32,4	0
0,38	13,4	0	13,4	0	15,2	0	17,1	0	28,7	0
0,39	10,1	0	10,6	0	13,4	0	16,2	0	25,4	0
0,40	6,4	0	6,4	0	9,7	0	12,9	0	21,7	0
0,41	5,5	0	5,5	0	8,3	0	11,1	0	18,3	0
0,42	5,1	0,4	5,2	0,9	52	0,9	9,2	0	15,2	0
0,43	3,7	2,3	4,1	2,3	4,1	1,8	9,2	1,3	12,5	0,9
0,44	2,7	2,7	2,7	2,7	3,7	1,8	6,4	2,7	10,1	2,3
0,45	3,2	3,2	3,7	3,7	3,7	3,7	4,6	4,1	7,4	4,1

Contador y valor mínimo HD

ϵ	1		2		3		4		5	
	FRR	FAR	FRR	FAR	FRR	FRR	FAR	FRR	FAR	FRR
0,35	8,7	0	19,9	0	21,7	0	29,1	0	48,1	0
0,36	7,8	0	17,5	0	18,5	0	23,1	0	42,1	0
0,37	5,5	0,4	16,2	0	16,6	0	20,3	0	32,4	0
0,38	4,6	0,4	13,4	0	15,2	0	17,1	0	28,7	0
0,39	4,6	0,4	10,6	0	13,4	0	16,2	0	25,4	0
0,40	4,1	0,9	6,4	0	9,7	0	12,9	0	21,7	0
0,41	3,7	2,3	5,5	0	8,3	0	11,1	0	18,2	0
0,42	3,2	3,2	5,1	0,9	5,1	0,9	9,2	0	15,2	0
0,43	3,2	3,2	4,1	2,3	4,1	1,8	9,2	1,3	12,5	0,9
0,44	2,3	2,3	2,7	2,7	3,7	2,3	6,4	2,7	10,1	2,3
0,45	3,2	3,2	3,2	3,2	3,7	3,7	4,1	3,7	8,3	5,1

La valoración de la combinación de los tres parámetros de búsqueda de coincidencias, considerando 5 plantillas de referencias en el proceso de identificación se indica en la tabla 18.

Tabla 18:
Evaluación del promedio HD, valor mínimo HD y contador en el proceso de identificación con 5 plantillas de referencia

	Contador, valor mínimo y promedio HD									
ϵ	**1**		**2**		**3**		**4**		**5**	
	FAR	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**	**FAR**	**FRR**
0,35	18,9	0	19,9	0	21,7	0	28,7	0	47,6	0
0,36	18,3	0	17,5	0	18,5	0	23,1	0	42,1	0
0,37	17,5	0	16,2	0	16,6	0	20,3	0	32,4	0
0,38	16,9	0	14,4	0	15,2	0	16,6	0	28,2	0
0,39	15,6	0	13,6	0	13,4	0	16,2	0	26,8	0
0,40	11,5	0	11,2	0	12,7	0	12,9	0	22,2	0
0,41	10,6	0	10,5	0	11,3	0	12,1	0	68,9	0
0,42	9,9	0	4,6	0,4	4,6	0,4	9,2	0	14,8	0
0,43	5,8	2,3	1,8	2,3	2,3	1,8	7,8	1,3	11,5	0,9
0,44	2,8	2,7	0	2,7	1,3	2,3	3,7	2,7	7,8	2,3
0,45	1,6	3,2	0	3,2	0	3,2	0,4	3,70	3,2	4,6

Se optó por considerar la combinación del contador con promedio o el valor mínimo de la HD y se estableció el valor de inicialización del contador en 1, en base a los valores obtenidos de la FAR y la FRR, ya que fueron los más bajos, respecto a estimarlos por separado o en otras combinaciones. En la figura 35 se indican graficados los valores de la FAR y FRR, donde se establece la EER. Estimando el promedio HD se observa que la ERR se ubica en el umbral de 0.44, donde la FRR y FAR tienen en mismo valor. Por otra parte, al considerar el valor mínimo HD la ERR se sitúa en el umbral de 0.44, de igual manera la FRR y FAR tienen el mismo valor.

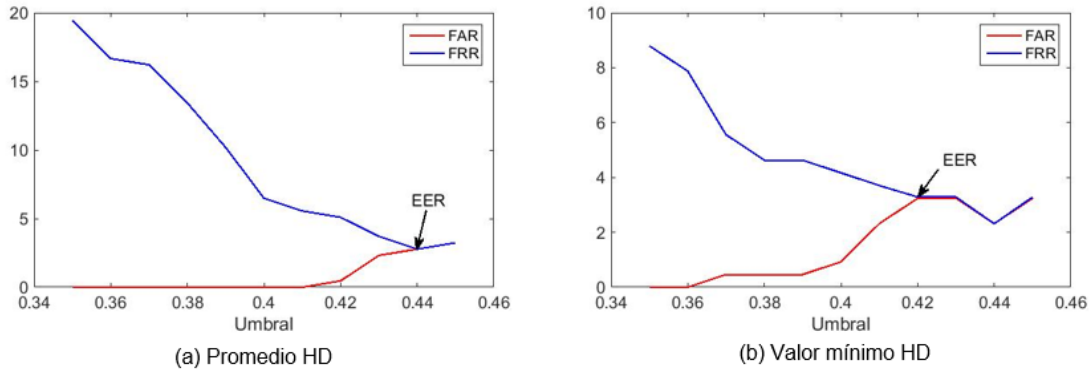

Figura 35. Distribución de la FAR y FRR del proceso de autenticación con 5 plantillas de referencia

Al igual que en el proceso de verificación lo que se pretende es obtener una FAR del 0%, y una valor mínimo en FRR. Se calcula el porcentaje de la FRR y FAR en los esquemas de CB con los valores del umbral que cumplen las condiciones. Fijándose en las tablas 5 y 6, los valores son 0.36, 0.39 y 0.41. En la tabla 19 se muestran los valores obtenido en los esquemas de CB con Gray-Combo en el proceso de identificación.

Tabla 19:
Evaluación del proceso de identificación en los sistemas con Gray-Combo

	Gray-Combo							
	Almacenando 4 plantillas				Almacenando 5 plantillas			
ϵ	Promedio HD		Valor mínimo HD		Promedio HD		Valor mínimo HD	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0.36	15.123	0	7.407	0	17.592	0	6.944	0
0.39	9.876	0	4.012	0.308	7.870	0	3.703	0
0.41	7.407	0	2.469	0.308	5.555	0	2.777	0.462

La tabla 20 expone los resultados de los sistemas con la transformación Bin-Salt en el procedimiento de reconocimiento.

Tabla 20:

Evaluación del proceso de autenticación en los sistemas con Bin-Salt

	Bin-Salt							
	Almacenando 4 plantillas				Almacenando 5 plantillas			
ϵ	Promedio HD		Valor mínimo HD		Promedio HD		Valor mínimo HD	
	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR
0.36	33.641	0	17.283	0	38.888	0	13.888	0
0.39	24.074	0	9.876	0	24.074	0	6.944	0
0.41	16.049	0	8.024	1.543	9.876	0	6.018	0.925

Considerando las tablas 19 y 20, se fija un umbral de 0.41 para el método de identificación de los sistemas de CB considerando el promedio HD para la comparación de las plantillas biométricas. Así como, un valor de 0.36 para la estimación del valor mínimo HD para reconocer a un usuario.

Los valores de umbral o punto de operación para cada proceso de los sistemas se establecen en la tabla 21. Se hace una distinción para las dos técnicas de búsqueda de coincidencias.

Tabla 21:

Valores del umbral de autenticación y reconocimiento de los esquemas de CB

	Autenticación		**Reconocimiento**	
	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.41	0.36

4.2. Evaluación de esquemas de biometría cancelable

Para el análisis de los sistemas de biometría cancelable se contempla las dos modalidades de funcionamiento de la biometría, autenticación o verificación y reconocimiento o identificación, en las cuales se planteando distintos escenarios de ataques, en los cuales intrusos o impostores son considerados.

4.2.1. Evaluación del proceso de autentificación

En el proceso de autenticación o verificación se evalúa a los sistemas, suponiendo que un intruso pretende suplantar a un usuario genuino específico.

4.2.1.1. Rendimiento (A_1)

Para establecer la verificación de la eficiencia de los sistemas se emplea la ecuación 5.1, con la cual se constata que el rendimiento de los sistemas no tenga un decremento. La tasa de falso rechazo del sistema de biometría original se representa por FRR, mientras que FRR_T refiere a la tasa de falso rechazo del esquema de CB. Se calcularon A_1 tanto para los esquemas de CB con Gray-Combo y Bin-Salt.

$$A_1 = 1 - \frac{FRR_T}{FRR} \qquad (5.1)$$

En la tabla 22, se indican los valores obtenidos de la FAR y FRR, en los sistemas de CB empleando el método de transformación Gray-Combo.

Tabla 22:
Porcentaje de FAR y FRR del sistema de biometría con Gray-Combo en el proceso de autenticación

Gray-Combo				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
FAR	0	0	0	0
FRR	9.876	7.407	7.870	6.944

Los valores de A_1 de los sistemas de CB con Gray-Combo se muestran en la tabla 23.

Tabla 23:
Valor de A_1 del esquema Gray-Combo en el proceso autenticación

Gray-Combo				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
A_1	0.111	0.172	-0.416	0.117

En la tabla 24, se indican los valores obtenidos en los sistemas de CB empleando el método de transformación Bin-Salt para el método de autenticación.

Tabla 24:
Porcentaje de FAR y FRR del sistema con Bin-Salt en el proceso de autenticación

Bin-Salt				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
FAR	0	0	0	0
FRR	16.049	17.592	14.814	14.084

Los valores de A_1 de los sistemas de CB con Bin-Salt se muestran en la tabla 25.

Tabla 25:

Valor de A_1 del esquema Bin-Salt para el proceso de autenticación

Bin-Salt				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
A_1	-0.444	-0.965	-1.666	-0.789

En el caso de que el rendimiento (A_1) sea negativo, se dice que la eficiencia del sistema disminuye al adicionar una función de transformación.

4.2.1.2. Irreversibilidad (A_2 a A_5)

Distintas imágenes de la base CASIA-IrisV3, se emplearon para generar biocódigos de consulta, que trataron de ser verificados como usuarios registrados en los sistemas; produciendo así varios intentos falsos de autenticación. Cuatro tipos de ataques se simularon, los cuales son detallados a continuación. La ponderación de la FAR de cada ataque, considerando el umbral o punto de operación fijados. Manifestando el riesgo de que un impostor sea verificado como un usuario genuino.

4.2.1.2.1. Ataque de cero esfuerzo (A_2):

En el primer escenario se considera a 103 impostores; cada impostor proporciona una imagen del ojo, en la cual se segmenta, normaliza y codifica el iris. Así mismo, provee un conjunto de parámetros de transformación, para ser verificado como cada uno de los 108 usuarios inscritos en los sistemas. Se generaron 11124 intentos de autenticación, los resultados obtenidos se observan en la tabla 26.

Tabla 26:
FAR de los esquemas de CB ante el ataque de cero esfuerzo en el proceso de autenticación

	A_2			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0	0	0	0
Bin-Salt	0	0	0	0

4.2.1.2.2. Ataque de fuerza bruta (A_3):

Se producen 10800 tentativas de verificación, originadas por 100 impostores, los cuales facilitan valores aleatorios aparentando ser biocódigos de los usuarios genuinos. En la tabla 27, se muestran los resultados de este tipo de ataque.

Tabla 27:
FAR de los esquemas de CB ante el ataque de fuerza bruta en el proceso de autenticación

	A_3			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0	0	0	0

Bin-Salt	0	0	0	0

4.2.1.2.3. Ataque de token robado (A_4):

En este contexto se simulan 11124 tentativas de autenticación para los esquemas de Gray-Combo; donde los 103 intrusos han conseguido el conjunto de parámetros de transformación (*token*) de todos usuarios. Así mismo, para los sistemas de Bin-Salt se generaron 11124 intentos de verificación, provocados por 103 intrusos y la platilla extra que se considera como *token*.

Los impostores para ser verificados, entrega una imagen del ojo, para segmentar, normalizar y codificar el iris, además en cada proceso de autenticación se proporciona la clave respectiva del usuario con el que se lo compara. Los valores obtenidos ante este ataque se indican la tabla 28.

Tabla 28:
FAR de los esquemas de CB ante el ataque de token robado en el proceso de autenticación

	A_4			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.003	0.003	0.004	0.004
Bin-Salt	0	0	0.004	0.004

4.2.1.2.4. Ataque de robo de características biométricas (A_5):

En este ataque los impostores conocen la información biométrica original de los usuarios registrados en los sistemas; probando diversos valores aleatorios de parámetros de transformación buscan ser autentificado. Se generaron 5400 tentativas de verificación, por cada usuario registrado en el sistema se realizaron 50 intentos de autentificación. En la tabla 29, se manifiestan los resultados que se obtuvieron ante este tipo de ataque.

Tabla 29:
FAR de los esquemas de CB ante el ataque de robo de características biométricas en el proceso de autenticación

	A_5			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.001	0	0.002	0
Bin-Salt	0	0	0	0

4.2.1.3. Diversidad o imposibilidad de vinculación (A_6 a A_8)

En esta sección se evalúa la diversidad de los esquemas de CB, pues deben ser capaces de producir diferentes biocódigos de un usuario para cada aplicación. De igual manera, se realizan pruebas para estimar la imposibilidad de vinculación de los biocódigos generados por los sistemas.

4.2.1.3.1. Información mutua de biocódigos (A_6)

Para calcular la propiedad de diversidad de los esquemas, se obtiene el máximo valor de la información mutua de las plantillas generadas por cada usuario. Para este cálculo se consideraron once aplicaciones y por cada aplicación se generaron 5 biocódigos por usuario. Para la ponderación de A_6 se estimó la media de los valores máximos de información mutua de todos los usuarios. En la tabla 30 se indican los valores de A_6 obtenido para los sistemas Gray-Combo y Bin-Salt. Para evaluar la diversidad de los esquemas no fue necesario hacer distinción en los parámetros de decisión, ya que los biocódigos almacenados son los mismos para tipo de sistema de CB.

Tabla 30:
Información mutua de los esquemas de CB en el proceso de autenticación

	A_6
Gray-Combo	0.09279
Bin-Salt	0

4.2.1.3.2. Ataque de escucha:

En el ataque de escucha diversos biocódigos procedentes de un mismo usuario del sistema, son interceptados por los impostores; para luego mediante predicción, originar una plantilla, que pretenden ser autentificada como usuario del sistema. De cada sujeto registrado en el sistema se genera cuatro plantillas impostoras, produciendo 432 ataques de escucha.

Así mismo, se produjeron 540 tentativas de verificación, al originar cinco plantillas impostoras.

El cálculo de A_7 y A_8 se diferencia en la cantidad de biocódigos que se usaron para la predicción de la plantilla de los impostores; en el caso de A_7 se usaron 3 biocódigos auténticos y para A_8 fueron 11 biocódigos genuinos.

4.2.1.3.2.1. Imposibilidad de vinculación con 3 biocódigos (A_7):

En la tabla 31 se señalan los valores de A_7 alcanzados para los sistemas Gray-Combo y Bin-Salt, A_7 representa la FAR ante los ataques de escucha. Donde se diferencias los resultados para las técnicas de comparación y el número de plantillas de referencia almacenas.

Tabla 31:
FAR de los esquemas de CB ante el ataque de escucha en el proceso de autenticación, considerando 3 biocódigos genuinos

	A_7			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.009	0.030	0.003	0.003
Bin-Salt	0	0	0	0

4.2.1.3.2.2. Imposibilidad de vinculación con 11 biocódigos (A_8):

De igual forma, para indicar los valores obtenidos en A_8 se calcula la FAR de los ataques de escuchas a los esquemas de CB. En los cuales, los impostores han interceptados 11 biocódigos de referencia de los usuarios registrados.

En la tabla 32 se muestran los valores A_8 alcanzados para los sistemas Gray-Combo y Bin-Salt, se hace una distinción entre las metodologías de comparación y el número de plantillas de referencia almacenas.

Tabla 32:
FAR de los esquemas de CB ante el ataque de escucha en el proceso de autenticación, considerando 11 biocódigos genuinos

	A_7			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.460	0.918	0.329	0
Bin-Salt	0	0	0	0

4.2.2. Evaluación del proceso de identificación

Para evaluar el proceso de identificación o reconocimiento, los impostores intentan hacerse pasar por todos los usuarios registrados en el sistema. Los parámetros planteados para el procedimiento de verificación, se consideran igualmente para la identificación. Las características de información mutua de los biocódigos (A_6) tienen los mismo valores tanto para autentificación como para reconocimiento.

4.2.2.1. Rendimiento (A_1)

Para estimar el rendimiento de los sistemas de CB evaluando el reconocimiento se maneja el mismo contexto que en el proceso de autenticación, con la diferencia del valor del umbral para la primera técnica de búsqueda de coincidencias (promedio HD). En la tabla 33, se indican los valores obtenidos de la FAR y FRR, en los sistemas de CB empleando el método de transformación Gray-Combo.

Tabla 33:
Porcentaje de FAR y FRR del sistema de biometría con Gray-Combo en el proceso de identificación

Gray-Combo				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
FAR	0	0	0	0
FRR	9.876	7.407	7.870	6.944

Los valores de A_1 de los sistemas de CB con Gray-Combo se muestran en la tabla 34. La ecuación 5.1 se empleó para su ponderación.

Tabla 34:
Valor de A_1 del esquema Gray-Combo en el proceso de identificación

Gray-Combo				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
A_1	0.040	0.172	0	0.117

En la tabla 35, se indican los valores obtenidos en los sistemas de CB empleando el método de transformación Bin-Salt, para el procedimiento de identificación.

Tabla 35:
Porcentaje de FAR y FRR del sistema con Bin-Salt en el proceso de identificación

Bin-Salt				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
FAR	0	0	0	0
FRR	16.049	17.592	9.876	13.888

La ecuación 5.1 se utilizó para el cálculo de A_1 en los sistemas de CB con Bin-Salt, los valores se muestran en la tabla 36, para el método de reconocimiento.

Tabla 36:
Valor de A_1 del esquema Bin-Salt para el proceso de autenticación

Bin-Salt				
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
A_1	-1.079	-0.931	-0.777	-1

En el caso de que el rendimiento (A_1) sea negativo, se dice que la eficiencia del sistema disminuye al adicionar una función de transformación.

4.2.2.2. Irreversibilidad (A_2 a A_5)

Al igual que el proceso de verificación se empleó la base CASIA-IrisV3, para producir varios intentos falsos de reconocimiento. Cuatro clases de ataques se simularon. Se calcula la FAR de cada ataque, teniendo en consideración los valores del punto de operación fijados y la técnica de comparación que se utilizó.

4.2.2.2.1. Ataque de cero esfuerzo (A_2):

Se produjeron 103 intentos de identificación, los impostores provee un conjunto de parámetros de transformación, además de la imagen de su ojo, para ser reconocido como uno de los 108 usuarios inscritos en cada uno de los sistemas. Los resultados obtenidos de la FAR en este tipo de ataque se observan en la tabla 37.

Tabla 37:
FAR de los esquemas de CB ante el ataque de cero esfuerzo en el proceso de identificación

	A_2			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
Gray-Combo	0	0	0	0
Bin-Salt	0	0	0	0

4.2.2.2.2. Ataque de fuerza bruta (A_3):

Se producen 108 tentativas de verificación, en los cuales los 100 impostores facilitan valores aleatorios aparentando ser biocódigos de los usuarios genuinos. Las plantillas generadas por los impostores se comparan con todos los usuarios del sistema. En la tabla 38 se muestran los resultados de la FAR ante este tipo de ataque.

Tabla 38:
FAR de los esquemas de CB ante el ataque de fuerza bruta en el proceso de identificación

	A_3			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
Gray-Combo	0	0	0	0
Bin-Salt	0	0	0	0

4.2.2.2.3. Ataque de token robado (A_4):

Para evaluar los sistemas de Gray-Combo, se produjeron 11124 intentos de identificación; donde los 103 intrusos ha conseguido el conjunto de parámetros de transformación (token) de los 108 usuarios registrados en los sistemas. Los impostores proporcionan una imagen del ojo para ser identificados, además en cada proceso de reconocimiento proveen la clave de uno de los usuarios.

Desde otra perspectiva, se generaron 103 tentativas de reconocimiento, para estimar esta clase de ataque en los sistemas de Bin-Salt. Los 103

intrusos usando la plantilla extra, pretenden ser identificados como usuarios del sistema. Los resultados obtenidos de la FAR ante este ataque se indican en la tabla 39.

Tabla 39:
FAR de los esquemas de CB ante el ataque de token robado en el proceso de identificación

	A_4			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
Gray-Combo	0.003	0.003	0.003	0.003
Bin-Salt	0	0	0.004	0.004

4.2.2.2.4. Ataque de robo de características biométricas (A_5)

En este ataque se consideran 5400 intentos de reconocimiento, generados por 50 valores aleatorios de parámetros de transformación proporcionados por los intrusos.

Estos parámetros se combinaron con 108 plantillas la información biométrica original de los usuarios registrados en los sistemas.

En la tabla 40 se observan los valores obtenidos de la FAR ante el ataque de robo de características biométricas.

Tabla 40:
FAR de los esquemas de CB ante el ataque de robo de características biométricas en el proceso de identificación

	A_5			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.41	0.36	0.41	0.36
Gray-Combo	0	0	0.010	0
Bin-Salt	0	0	0	0

4.2.2.3. Diversidad o imposibilidad de vinculación (A_6 a A_8)

Se evalúa las propiedades de diversidad o imposibilidad de vinculación, calculando la información mutua de los biocódigos de referencia generados. Además de los ataque de escucha, que mediante predicción se generan plantillas impostoras que pretenden ser reconocidas como plantillas de usuarios genuinos.

4.2.2.3.1. Información mutua de biocódigos:

Del mismo modo que se estimó la propiedad de diversidad en el proceso de autenticación, se obtienen los resultados para el procedimiento de reconocimiento. Los valores obtenidos se muestran en la tabla 41.

Tabla 41:
Información mutua de los esquemas de CB en el proceso de identificación

	A_6
Gray-Combo	0.09279
Bin-Salt	0

4.2.2.3.2. Ataque de escucha:

Diversos biocódigos provenientes de un mismo sujeto inscriptos en el sistema, son interceptados por los impostores. Para luego mediante predicción, producir una plantilla, que pretenden ser reconocida como usuario del sistema. La estimación de A_7 y A_8 son similares, con la diferencia de la cantidad de biocódigos de referencia usados para la predicción de la plantilla de los impostores; en el caso de A_7 se usaron 3 biocódigos auténticos y para A_8 fueron 11 biocódigos genuinos.

4.2.2.3.2.1. Imposibilidad de vinculación con 3 biocódigos (A_7):

Para evaluar A_7 se provocaron 432 tentativas de reconocimiento, considerando la base de dados con cuatro biocódigos de referencias almacenados por usuario, se originó una plantilla por predicción. Por otra parte, estimando cinco plantillas de referencia guardadas por usuario, se generaron 540 intentos de identificación.

En la tabla 42 se señalan los valores de la FAR obtenidos por los esquemas de CB ante el ataque de escuchas, con tres biocódigos de referencia para realizar la predicciones de las plantillas impostoras.

Tabla 42:
FAR de los esquemas de CB ante el ataque de escucha en el proceso de identificación, considerando 3 biocódigos genuinos

	A_7			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.053	0.030	0.044	0.029

Bin-Salt	0	0	0	0

4.2.2.3.2.2. Imposibilidad de vinculación con 11 biocódigos (A_8):

El número de falsos intentos de reconocimiento son los mismo que en A_7. Para los sistemas con cuatro plantillas de referencia almacenas fueron 432 intentos, mientras que para los esquemas con cinco plantillas guardadas se produjeron 540 tentativas de identificación.

Para indicar los valores obtenidos en A_8 se calcula la FAR del proceso de reconocimiento de las plantillas generadas por predicción a partir de once biocódigos genuinos. Estos valores se muestran en la tabla 43.

Tabla 43:
FAR de los esquemas de CB ante el ataque de escucha en el proceso de identificación, considerando 11 biocódigos genuinos

	A_7			
# de plantillas almacenadas	4		5	
Técnica de búsqueda de coincidencias	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
ϵ	0.39	0.36	0.39	0.36
Gray-Combo	0.812	0.918	0.696	0.916
Bin-Salt	0	0	0	0

4.3. Análisis de resultados

El sistema de biometría para el reconocimiento del iris, se evaluó contemplando los métodos de verificación y reconocimiento. Se plantearon dos técnicas para la búsqueda de coincidencias. Las variables que se consideran para la primera técnica fueron: umbral, contador y promedio HD.

Fijando un umbral de 0.39 para el procedimiento de autenticación considerando estos parámetros se alcanzó un 0% de la FAR y 11.111% de la FRR. Por otra parte para el proceso de identificación con un umbral de 0.41 se obtuvo 0% de la FAR y 7.716% de la FRR. Desde otra perspectiva se estiman los parámetros: umbral, contador y mínimo valor de la HD. Tanto para el proceso de autenticación e identificación se consiguió un 0% en la FAR y 8.950% en la FRR, con un valor de 0.36 para el umbral.

Los esquemas de CB han sido evaluados considerando ocho criterios, que a más de estimar su robustez, permitieron distinguir que ataque es el mayor impacto causa en la seguridad de los sistemas.

Para la ponderación de los criterios A_i $(2:8)$, se considera menos robusto el sistema si su valor se aproxima a 1. Es decir se prefieren los valores próximos a 0. En el caso de que el rendimiento (A_1) sea negativo, se dice que la eficiencia del sistema disminuye al adicionar una función de transformación; pues la FAR o/y la FRR incrementa en los esquemas de CB.

En la tabla 44 se presentan los valores obtenidos de los ocho criterios en el procedimiento de autenticación con la técnica de Gray-Combo, se hace una distinción del número de plantillas o biocódigos de referencia que se almacenos por usuario para realizar las comparaciones.

Tabla 44:
Resultado de la evaluación de los ocho criterios de los esquemas de BC con la técnica Gray-Combo para el proceso de autenticación

Metodología CB	**Gray-Combo**			
# plantillas almacenadas	4		5	
Técnica de comparación	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
A_1	0.11111	0.17241	-0.41674	0.11766
A_2	0.00008	0	0	0
A_3	0	0	0	0

A_4	0.00395	0.00386	0.00464	0.00413
A_5	0.00185	0	0.00240	0
A_6	0.09279	0.09279	0.09279	0.09279
A_7	0.00925	0.03009	0.00370	0.00370
A_8	0.46064	0.91898	0	0.32962

Al estimar la robustez de los esquemas de biometría cancelable con la metodología de transformación Gray-Combo para la autenticación del iris, se puede observar que se obtuvo un incremento en el rendimiento (A_1), pues los valores resultantes son mayor a cero.

Sin embargo, la primera técnica de búsqueda de coincidencias muestra un deterioro del rendimiento, al contemplar cinco biocódigos almacenados por usuario, debido al incremento de la FRR.

Analizando los demás criterios de evaluación, los esquemas con Gray-Combo, muestra mayor riesgo ente el ataque de escucha (A_8), donde se constata que la generación de biocódigos impostores validos incrementa al disponer de más plantillas genuinas. La segunda técnica de comparación fue la que mayor vulnerabilidad presento ante este ataque, con un valor de 0.91898.

Cabe recalcar, que se obtuvieron valores bajos en información mutua (A_6), donde se evaluó la propiedad de diversidad, esta medida indica la robustez en producir biocódigos de los sistemas de biometría cancelable.

Es indispensable para los esquemas garantizar esta propiedad, pues se debe impedir la vinculación de los usuarios con las plantillas almacenas, para brindar mayor privacidad y seguridad en los sistemas.

Analizando el procedimiento de verificación de igual forma se estimaron los ocho criterios con la técnica de Bin-Salt, haciendo una diferenciación en el número de biocódigos de referencia almacenados por usuario. En la tabla 45 se presentan los valores obtenidos.

Tabla 45:

Resultado de la evaluación de los ocho criterios de los esquemas de BC con la técnica Bin-Salt para el proceso de autenticación

Metodología CB	**Bin-Salt**			
# plantillas almacenadas	4		5	
Técnica de comparación	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
A_1	-1.1944	-0.96551	-1.66678	-0.78958
A_2	0	0	0	0
A_3	0	0	0	0
A_4	0	0	0.00359	0.00332
A_5	0	0	0	0
A_6	0	0	0	0
A_7	0	0	0	0
A_8	0	0	0	0

Con el primer criterio (A_1) se estima el rendimiento de los sistemas con Bin-Salt los valores obtenidos son negativos, es decir, existe degradación en el rendimiento. Esto se debe a que la FRR se incrementó. Pese a tener un decremento en el rendimiento, estos esquemas son inmunes a los diferentes tipos de ataques, para el proceso de autenticación. Además, se garantizó que los sistemas cumplen con la propiedad de diversidad, en vista que se alcanzó un valor de cero para A_6.

Desde otra perspectiva se analizó en procedimiento de identificación en los sistemas de CD. Los ocho criterios planteados para la verificación de usuarios, se consideran igualmente para la identificación. En la tabla 46 los valore conseguidos, que describen la robustez de los sistemas de biometría cancelable para el proceso de identificación aplicando la técnica Gray-Combo.

Tabla 46:
Resultado de la evaluación de los ocho criterios de los esquemas de BC con la técnica Gray-Combo para el proceso de identificación

Metodología CB	**Gray-Combo**			
# plantillas almacenadas	4		5	
Técnica de comparación	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
A_1	0.04004	0.17241	0	0.11766
A_2	0.00970	0.00970	0	0
A_3	0	0	0	0
A_4	0.51456	0.46601	0.00476	0.00440
A_5	0.010185	0	0.01037	0.00111
A_6	0.09279	0.09279	0.09279	0.09279
A_7	0.05324	0.03009	0.04444	0.02962
A_8	0.8125	0.91898	0.69629	0.91666

Tal como, en el proceso de autentificación, los esquemas con Gray-Combo muestran un incremento en el rendimiento (A_1), pues presenta valores positivos. Considerando los demás criterios, se debe mencionar que los valores resultantes para los ataques de robo de token (A_4) y escucha incrementaron (A_8) señalan vulnerabilidad de los sistemas ante esta clase de ataque. Los valores de la propiedad de diversidad A_6 son iguales, tanto para el procedimiento de verificación y reconocimiento.

Se destaca, que los esquemas con Gray-Combo presentan valores altos en los ataque de escucha A_8, siendo este ataque el que presenta mayor riesgo para los sistemas, al igual que en el procedimiento de verificación.

En la tabla 47 se presentan los valores obtenidos de los ocho criterios en el procedimiento de identificación con la técnica de Bin-Salt, se hace una

distinción del número plantillas o biocódigos de referencias que se almacenos por usuario para realizar las comparaciones.

Tabla 47:
Resultado de la evaluación de los ocho criterios de los esquemas de BC con la técnica Bin-Salt para el proceso de identificación

Metodología CB	**Bin-Salt**			
# plantillas almacenadas	4		5	
Técnica de comparación	Promedio HD	Valor mínimo HD	Promedio HD	Valor mínimo HD
A_1	-1.03991	-0.96551	-1.66678	-0.78958
A_2	0	0	0	0
A_3	0	0	0	0
A_4	0.39805	0.37864	0.00359	0.00332
A_5	0	0	0	0
A_6	0	0	0	0
A_7	0	0	0	0
A_8	0	0	0	0

El rendimiento (A_1) en el análisis de la metodología Bin-Salt disminuyó al igual que el proceso de verificación. Estimando los demás criterios, el valor obtenidos en el ataque de token robado A_4 incrementó, mostrando susceptibilidad de los sistemas ante ataques de robo de token.

CAPÍTULO 5

CONCLUSIONES Y TRABAJO FUTURO

5.1. Conclusiones

En este estudio se presenta la evaluación de dos técnicas de biometría cancelable. Se cuantificó la robustez de sus propiedades, mediante la valoración de ocho parámetros, permitiendo así su comparación. En primer lugar se implementó un sistema de biometría para reconocimiento de iris; para ello se tomó como referencia lo descrito por (Masek, 2003) y la base de datos CASIA.

La evaluación del sistema de biometría variando los parámetros de búsqueda de coincidencias y número de platillas de referencia almacenas por usuario ha demostrado que proporciona un proceso de autenticación y verificación fiable. El número de plantillas influye directamente en la discriminación. En el proceso de búsqueda de coincidencias los parámetros que alcanzaron un 0% en la FAR y el valor bajo de la FRR, considerando cinco plantillas de referencias fueron: umbral, contador y valor mínimo HD, con un 7.87% en la FRR en el proceso de autenticación y verificación con un umbral igual al 0.36. Los porcentajes conseguidos se encuentran dentro de los obtenidos por los sistemas que se citaron en el estado del arte.

Las técnicas de biometría cancelable Gray-Combo y Bin-Salt tienen como ventaja su fácil incorporación. Gray-Combo es un método que mediante los parámetros que se almacenan en un token realizan la transformación de información biométrica del iris (plantillas), el proceso de transformación implica el desplazamiento y combinación de filas de los usuarios. Para generar plantillas de biometría cancelable con Bin-Salt se mezcla el código del patrón del iris con una plantilla extra, la plantilla extra es una distribución uniforme, conformada por unos y ceros.

Con un umbral de decisión fijado en 0.36 y calculando contador y mínimo valor HD se consiguió la FRR con menor valor y 0% en la FAR. Gray-Combo señala un ligero decremento en la FRR en comparación con los valores

conseguidos por el sistema de biometría sin ninguna modificación en su funcionamiento, el porcentaje alcanzado fue de 0.69%. Lo contrario sucedió con la técnica de Bin-Salt, la FRR incremento a 14%.

La norma ISO/IEC 24745 señala las propiedades (revocabilidad o revocación, irreversibilidad o no invertibilidad, diversidad o imposibilidad de vinculación y rendimiento) que un esquema de biometría cancelable debe cumplir. Se calcularon ocho criterios, que permitieron cuantificar las propiedades de robustez, enfocándose en la privacidad de los esquemas.

Los resultados obtenidos indican que la técnica de Bin-Salt tiene un deterioro en el rendimiento. No obstante, los valores alcanzados ante los tipos de ataques planteados para la evaluación de los criterios, tanto para la verificación como para el reconocimiento del iris son bueno, pues se aproximan a cero. Por otra parte Gray-Combo presenta un aumento en el rendimiento del sistema, pero no garantiza el cumplimiento de las propiedades de imposibilidad de vinculación en el proceso de identificación, pues manifiesta susceptibilidad ante el ataque de escucha, entre mayor cantidad de información genuina obtenga un impostor será más factible para él generar biocódigos que sean reconocidos como usuarios del sistema.

La propiedad de diversidad se cumplió en las dos metodologías de biometría cancelable, impidiendo la vinculación de los usuarios con las plantillas de referencias almacenas, lo que brinda mayor seguridad y privacidad.

Al evaluar las propiedades, Bin-Salt muestra una mejora en la privacidad y seguridad del sistema de biometría del iris, siendo una alternativa fiable para su aplicación. Pese a que el rendimiento disminuyo (incremento la FRR), pues se prefiere que un usuario tenga proporcionar un mayor número de veces muestras del iris, a que impostores o intrusos tengan acceso al sistema (incremento en la FAR).

La privacidad de la información de los rasgos físicos que se almacenan en los sistemas de biometría tanto en el proceso de autenticación, como en el proceso de identificación es un constituyente fundamental para garantizar la seguridad y fiabilidad de los sistemas. Frente a esta necesidad, el método de

biometría cancelable presenta un enfoque de protección y seguridad de la información biométrica almacenada de cada usuario registrado en el sistema. El uso del iris como rasgo biométrico dispone de preeminencias (alta aceptación, universalidad, fácil registro, entre otras) sobre otros identificadores.

5.2. Trabajos futuros

A partir del estudio realizado, se propone como trabajo futuro implementar la etapa de adquisición para verificar el funcionamiento y factibilidad de la aplicación de las técnicas de biometría cancelable antes mencionadas considerando los diferentes parámetros fijados.

Hasta la fecha no existe un criterio generalizado para evaluar la robustez cuantitativamente de los algoritmos de biometría cancelable, por este motivo, se contempla la posibilidad de considerar nuevos de ataques, tales como: presentar en la etapa de adquisición un rasgo biométrico falso o algún dispositivo para intentar acceder al sistema (ataque directo). De igual manera, mediante software se podría manipular las diferentes etapas o modificar el umbral de decisión de los sistemas para que intruso sea reconocido o verificado (ataque indirecto).

Adicionalmente se podría plantear técnicas de predicción más complejas para la generación de plantillas falsas, empleando la información intersectada de las platillas genuinas, para así estimar la robustez de los sistemas ante un ataque de escucha.

REFERENCIAS

Abraira, V. (Mayo de 2011). *Curva ROC*. Obtenido de Material docente de la unidad de Bioestadística Clínica: http://www.hrc.es/bioest/roc_1.html

Aguilera, M. M. (2012). Reconocimiento biométrico basado en imágenes de huellas palmares. *Escuela Politécnica Superior*. Madrid: Universidad Autónoma de Madrid.

Alonso, E. D.-S. (2002). Análisis de las curvas receiver-operating characteristic: un método útil para evaluar procederes diagnósticos. *Revista Cubana de Endocrinologiá*, 169-76.

Ávila, C. S. (2012). *Aplicaciones de la Biometría a la Seguridad.* Universidad Politécnica de Madrid: Centro de Domótica Integral (CEDINT).

Belguechi, R. C. (2011). Evaluation of cancelable biometric systems: Application to finger-knuckle-prints. *Hand-Based Biometrics (ICHB), 2011 International Conference* (págs. 1-6). IEEE.

Belguechi, R. C. (2012). How to Evaluate Transformation Based Cancelable Biometric Systems. *NIST International Biometric Performance Testing Conference (IBPC).*

Bertolín, J. A. (2007). Análisis entorno a la tecnología biométrica para los sistemas electrónicos de identificación y autentificación. *Revista española de electrónica*, 52-67.

Biometrics, N. S. (7 de Agosto de 2006). *Biometrics History*. Obtenido de http://biometrics.gov/Documents/BioHistory.pdf

Bowyer, K. W. (2008). Image understanding for iris biometrics: A survey. En *Computer vision and image understanding* (págs. 281-307).

Bringer, J. C. (2008). The best of both worlds: Applying secure sketches to cancelable biometrics. *Science of Computer Programming, 74(1)*, (págs. 43-51).

Chinese Academy of Sciences- Institute of Automation. (2003). *Database of 756 Greyscale Eye Images*. Obtenido de http://www.sinobiometrics.com

Cruz, L. F. (2006). *Reconocimiento del Iris.* Trujillo, Perú: Tópicos Especiales en Procesamiento Gráfico, Universidad Nacional de Trujillo.

Daugman, J. (2003). *The importance of being random: statistical principles of iris recognition.* Pattern recognition, 36(2), 279-291.

Daugman, J. G. (1994). *United States Patente nº 5,291,560.*

Duque, J. P. (2004). Implementación de la transformada de Hough para la detección de líneas para un sistema de visión de bajo nivel. *Scientia et technica, 1(24)*, 79-84.

Duró, V. E. (2001). Evaluación de sistemas de reconocimiento biométrico. *Departamento de Electrónica y Automática*. Mataró: Escuela Universitaria Politécnica de Mataró.

Ganorkar, S. R. (2007). ris recognition: an emerging biometric technology. *n Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation* (págs. 91-96). World Scientific and Engineering Academy and Society (WSEAS).

García, J. O. (2008). *Biometría y seguridad.* Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

García, M. S. (2012). *Avances en el reconocimiento del iris: perspectivas y oportunidades en la investigación de algoritmos biométricos.* 267-276: Computación y sistemas, 16(3).

Gayoso, M. V. (2014). La transformada de Walsh-Hadamard y otros parámetros en la autentificación biométrica.

Hämmerle-Uhl, J. P. (2009). Cancelable iris biometrics using block re-mapping and image warping. *International Conference on Information Security* , (págs. 135-142). Springer Berlin Heidelberg.

He, Z. T. (2009). Toward accurate and fast iris segmentation for iris biometrics. *IEEE transactions on pattern analysis and machine intelligence, 31(9)*, 1670-1684.

Hernández, B. A. (2009). *Propuesta de estándar para el uso seguro de tecnologías biométricas.* Universidad Nacional Autónoma de México.

Hernandez, E. I. (2015). *Introducción a técnicas de reconocimiento de iris.* México: Facultad de Matemáticas, Universidad Autónoma de Yucatán.

Jain, A. K. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology, 14(1)*, 4-20.

Jain, A. K. (2008). Biometric template security . *EURASIP Journal on Advances in Signal Processing*, 113.

Jin, A. T. (2010). Cancelable biometrics. *Scholarpedia, 5(1)*, 9201.

Kaur, G. S. (2014). A review on biometric recognition. *nternational Journal of Bio-Science and Bio-Technology, 6(4)*, 69-76.

Kong, A. C. (2006). An analysis of BioHashing and its variants. *Pattern Recognition, 39(7)*, 1359-1368.

Kulkarni, S. B. (2012). A novel approach for iris encryption. *Technology*, 7.

Leonard Flom, A. S. (1987). *United States Patente nº US4641349 A.*

López, J. F. (2 de Noviembe de 2012). *Procesamiento Digital de Imágenes.* Obtenido de Transformada Hough: https://procesamientodigitalimagenes.wordpress.com/2012/11/02/transformada-hough/

Maltoni, D. M. (2009). *Handbook of fingerprint recognition.* Springer Science & Business Media.

Marín, M. R. (2009). Una mirada a la biometría. *Avances en Sistemas e Informática, 6(2)*, 29-38.

Masek, L. (2003). Recognition of human iris patterns for biometric identification. Australia: The University of Western Australia.

Mayoue, A. (2007). *Biosecure Tool: Performace Evaluation of a Biometric Verification System.* GET-INT, Ver, 1.

NSTC Subcommittee on Biometrics. (7 de August de 2006). *Biometrics.* Obtenido de http://biometrics.gov/Documents/BioHistory.pdf

Pillaj, J. K. (2010). Sectored Random Projections for Cancelable Iris Biometrics. *ICASSP*, 1838-1841.

Rabie, I. &. (2008). *Identificación de patrones biométricos del iris .* Quito: USFQ: Bachelor's thesis.

Ratha, N. C. (2006). Cancelable biometrics: A case study in fingerprints. *In 18th International Conference on Pattern Recognition (ICPR'06)* (págs. 370-373). IEEE.

Ratha, N. K. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 614-634.

Rathgeb, C. U. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security, 2011(1)*, 3.

Rathgeb, C. U. (2012). *ris biometrics: from segmentation to template security (Vol. 59).* Springer Science & Business Media.

Sanderson, S. &. (2000). *Authentication for secure environments based on iris scanning technology.*

Santos, A. D. (2008). *Nuevos Algoritmos y Ataques a Sistemas de Identificación Biométrica basados en Reconocimiento de Iris.*

Subcomité de Biometría del NSTC. (2011). *Biometría.* Obtenido de http://www.biometria.gov.ar/acerca-de-la-biometria/glosario/a-e.aspx

Teoh, A. B. (2007). Cancelable biometrics realization with multispace random projections. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(5)*, 1096-1106.

Tomé G., P. (2008). *Reconocimiento Automático de Patrones de Iris.* Universidad Autónoma de Madrid. Departamento de Ingeniería Informática.

Valencia M., J. F. (2014). Extracción de características del iris como mecanismo de identificación biométrica. *Revista Virtual Universidad Católica del Norte*, 182-196.

Vega, H. V. (2011). Reconocimiento del iris. *ECCIENCIA, 5(10)*, 40-46.

Virginia, E. D. (2001). Evaluación de Sistemas de Reconocimiento Biométrico. *Escuela Universitaria Politécnica de Mataró*.

Virginia, E. D. (2001). Evaluación de sistemas de reconocimiento biométrico. Barcelona.

Wayman, J. L. (2001). Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics, 1(01)*, 93-113.

Yanushkevich, S. N. (2009). Fundamentals of biometric system design: new course for electrical, computer, and software engineering students. *Bio-inspired Learning and Intelligent Systems for Security, 2009. BLISS'09* (págs. 3-8). IEEE.

Zamudio, L. M. (Diciembre de 2010). *Reconocimiento del iris como identificación biométrica utilizando el video.* Tijuana, B. C.: Centro de Investigación y Desarrollo de Tecnología Digital.

Zuo, J. R. (December de 2008). Cancelable iris biometric. *Pattern Recognition, 2008. ICPR 2008. 19th International Conference* (págs. 1-4). IEEE.