UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

TÍTULO DEL PROYECTO:

Implementación de control de accesos biométricos en aulas del Bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone (2020) P1

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR,

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

AUTORES:

Saldarriaga Amalla Abrahán Alexis

Zambrano Chalacama Jandry Javier

TUTOR

Ing. Nilo Walker Andrade Acosta, Mg. I.E.

EXTENSIÓN CHONE.

INGENIERÍA EN SISTEMAS.

CHONE - MANABÍ - ECUADOR

2022

CERTIFICACIÓN DEL TUTOR

Ing. Nilo Walker Andrade Acosta. Mg. I.E., docente de la Universidad Laica "Eloy Alfaro" de Manabí Extensión Chone, en calidad de tutor del trabajo de Titulación.

CERTIFICO:

Que el presente trabajo titulado "**Implementación de control de Accesos Biométricos en Aulas del Bloque B Planta Baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone"** ha sido exhaustivamente revisado en varias sesiones de trabajo, se encuentra listo para la revisión en Comisión Académica.

Las opiniones y conceptos vertidos en este trabajo son fruto de la perseverancia y originalidad de sus autoras: **Saldarriaga Amalla Abrahán Alexis y Zambrano Chalacama Jandry Javier,** siendo de su exclusiva responsabilidad.

Chone, abril del 2022

_____

Ing. Nilo Walker Andrade Acosta. Mg. I.E.

TUTOR

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN CHONE

DECLARACIÓN DE AUTORÍA

Quienes suscriben, **Saldarriaga Amalla Abrahán Alexis y Zambrano Chalacama Jandry Javier,** dejamos constancia que somos autores del presente trabajo bajo la modalidad de proyecto Integrador con el título: **"Implementación de control de Accesos Biométricos en Aulas del Bloque B Planta Baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone"**; y en virtud de aquello manifestamos la originalidad de la conceptualización del trabajo.

La responsabilidad de las opiniones, investigaciones, resultados, conclusiones y recomendaciones; así como la información obtenida en este trabajo de titulación, modalidad proyecto de investigación, es exclusiva responsabilidad de sus autores a excepción de las citas referenciales.

Para constancia de nuestra afirmación, firmamos en unidad de acto y criterio.

Chone, abril de 2022

_____	_____
Saldarriaga Amalla Abrahán Alexis	**Zambrano Chalacama Jandry Javier**

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN CHONE

APROBACION DEL TRIBUNAL

Los miembros del tribunal examinador aprueban el informe del trabajo de titulación con el título denominado **"Implementación de control de Accesos Biométricos en Aulas del Bloque B Planta Baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone"**; elaborado por los autores **Saldarriaga Amalla Abrahán Alexis y Zambrano Chalacama Jandry Javier,** de la carrera de Ingeniería en Sistemas.

Chone, abril del 2022

Lcda. Yenny Zambrano Villegas, Mg.
DECANA

Ing. Nilo Walker Andrade Acosta, Mg. IE.
TUTOR

MIEMBRO DEL TRIBUNAL

MIEMBRO DEL TRIBUNAL

SECRETARIA

DEDICATORIA

Dedicamos este trabajo a nuestros padres y cada una de aquellas personas, amigos, parientes, conocidos, que han estado al pie del cañón apoyándonos y dándonos fuerzas en cada etapa y proceso que hemos atravesado para lograr terminar con una de nuestras metas plasmada. Además de dedicarle este enorme esfuerzo a Dios por permitirnos continuar adelantes y no dejarnos derrumbar, igualmente dedicamos este proyecto a nosotros por el apoyo que nos tuvimos brindando mutuamente, dedicarle también este esfuerzo a nuestros compañeros que estuvieron alentándonos y dándonos aliento con su apoyo incondicional y a nuestro tutor que ha sido parte esencial para concluir el desarrollo de la Tesis.

Saldarriaga Amalla Abrahán Alexis

Zambrano Chalacama Jandry Javier

AGRADECIMIENTO

A Dios por ser quien ha estado a mi lado en todo momento, a mis padres, a mis hermanos, a mis tíos que desde un principio hasta el día de hoy siguen brindándome cariño y apoyo para culminar este proceso importante en mi vida.

También agradezco a todos los profesores por haber impartido sus conocimientos en especial al Ing. Nilo Andrade por su guía en todo el proceso de elaboración de tesis, a mis compañeros de aula de clases, amigos que me han apoyado, una y otra vez en este proceso de formación profesional.

Saldarriaga Amalla Abrahán Alexis

AGRADECIMIENTO

Agradezco primeramente a Dios por estar siempre a mi lado brindándome su mano y abrigándome con su manto día a día, a mis padres por ser pilares y parte fundamental en mi vida y en este proceso, a mi esposa por estar conmigo a pesar de las dificultades, a mi familia por su aliento continuo en cada etapa, a mis suegros que me apoyaron constantemente, a mis compañeros por ayudarme en cada momento de dificulta, agradezco a cada uno de ellos por los momento en los que me quise rendir y ellos no me lo permitieron.

Agradezco a cada uno de mis docentes por sus cátedras y amistad en cada salón que compartimos, en especial a mi amigo y tutor Ing. Nilo Andrade que con su guía ha permitido que este proceso de titulación sea una realidad.

Zambrano Chalacama Jandry Javier

RESUMEN

La biometría es un conjunto de técnicas de identificación basada en el reconocimiento de una característica física e intransferible de los individuos, la finalidad de este trabajo es usar esta tecnología para la implementación de un control de acceso biométricos en las aulas del Bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone, debido a que estas no constataban con un sistema de accesos controlado para evitar el ingreso de personal no autorizado, además de no contar con una seguridad total para poder proteger los equipos con los que estas cuentan; con esto cualquier persona podía ingresar o con poca o nula detección, lo cual permitían estar en peligro los equipamiento del salón así como las pertenencia de algún estudiante o docente, también consta el funcionamiento de la biometría y de los diferentes tipos de sistemas biométricos los cuales son de vital importancia actualmente.

Palabras claves: acceso, sistema, biométricos, control, seguridad, ingreso, personal.

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo busca el mejoramiento de la asistencia y la seguridad académica y administrativa del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone, de esta manera automatizar y poder obtener información para así generar reportes diarios de las aulas de clase en tiempo real, al no contar con un sistema de protección apropiado para la cautela de los equipamiento con los que estas cuentan a su vez, materiales y pertenencias dentro de los salones, por esta razón cualquiera podría ingresar, lo que conlleva a provocar inconvenientes como extraviarse las pertenencias que se encuentra dentro y por ende tener complejidad con quienes han ingresado sin autorización y sin ofrecer alerta para avisar el ingreso de intrusos.

La práctica de venir mejorando el acceso con escáner biométricos se hecho muy popular ya que a la hora de la investigación emos podido constatar que **antecediendo** a la Universidad Laica Eloy Alfaro de Manabí extensión Chone, varias instituciones han implementado el reconocimiento biométrico para poder controlar las asistencias de los docentes y estudiantes que ingresan a ciertas áreas de dichos establecimientos, el constante crecimiento tecnológico en el que nos encontramos inmersos el día de hoy nos obliga a adaptarnos a los cambios o correr el riesgo de quedar sumidos en la obsolescencia.

El estado actual de las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone son de forma típicas o clásicas de igual manera en la mayoría de los bloques y áreas de la Universidad, estas pueden ser accedidas

por cualquier persona beneficiaria a los estudios de tercer nivel o personal particular que tenga entrada a dicho establecimiento, de esta manera causan malestares y distracciones innecesaria, los cuales se han venido suscitando con anterioridad; estimando la **problemática** de cómo influiría la implementación de un control de acceso biométrico en el ingreso de las aulas.

Por esta razón el presente proyecto tuvo como **objetivos general** llevar a cabo la implementación de un control de acceso biométricos en aulas del Bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone; y así derivando como **objetivos específicos** realizar una búsqueda bibliográfica sistematizada de los controles o dispositivos de acceso biométrico; como segundo punto, Identificar los principales estándares a tomar en cuenta para el correcto funcionamiento del lector biométrico en el acceso controlado a las salones, en tercer lugar Determinar los parámetros técnicos de los sistemas de controlador biométrico y como último Instalar el verificador biométrico en las salas de catedra que sirva como base para su previa implementación.

Además, **ideando previamente** que los equipos de control de acceso biométrico sean compatibles con una variada forma de conexión con otros dispositivos, que el seleccionado un software para la adquisición de los datos, los sectores donde se implementaron cuentan con una estructura de redes y cableados, así se determinó que la implementación de control de acceso biométricos permitió proteger los recursos tecnológicos con lo cuales cuenta los diferentes salones de la planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone, y ayudó a

minimizar la inseguridad dentro de las aulas, por medio del monitoreo y el registro persistente para proteger los recursos de los maestros y alumnos dentro de las salas de catedra.

Sin embargo, se fundamentó la investigación teórica abordando los conceptos derivados de tres variantes como son: los sistemas biométricos, historia, importancia, características, identificación biométrica, etapas de un sistema de identificación biométrica y técnica de identificación biométrica, como segunda variable podemos constatar el control de acceso y tipo de controladores, bases de datos y tipos de base de datos; y como tercera variante los escáner de huella dactilar, tipo de escáner e implementación de escáner; a su vez se hizo referencia a la metodología que se aplicó en el presente proyecto de tesis, en el cual se usó los **métodos:** bibliográficos, de campo y el exploratorio para la conceptualización de las posiciones teóricas y conclusiones del mismos, además, se hizo una ficha de observación donde se llegó a un posterior análisis del siguiente estudio en él que se consigue conocer la carencia de seguridad y acceso controlado dentro de las aulas y entablar el puntos de vista para localizar los escáner para el control de acceso a las mismas; finalmente, se resaltó que de las variantes conseguidas del título del proyecto se han obtenido vasta información de distintas fuentes bibliográficas lo que es una sección importante del proyecto; en cuanto a la ficha de observación se hizo recolectar los datos necesarios para conocer los requerimientos y los puntos de vista para localizar los controles de acceso biométrico con esto se logró corregir los errores que presentaba ya sea por la seguridad o el ingreso de terceros.

1. Marco teórico conceptual

1.1. Sistemas biométricos

Según el Diccionario de la Real Academia Española, se define BIOMETRÍA como "Estudio mensurativo o estadístico de los fenómenos o procesos biológicos". Esta definición se hace más específica una vez que se usa el concepto de Biometría dentro del campo de la Identificación de individuos.

La Biometría consigue reconocer a una persona por medio de una imagen de su cara o por medio de la impresión de su huella dactilar, la función de identificación biométrica es algo innato en los organismos vivos, debido a que tienen la característica de reconocer a sus similares. (Ruiz Marín, Rodriguez Uribe, & Olivares Morales, 2009).

Según los autores (Madrigal González, Ramírez Madrigal, Hoyos Arbeláez, & Fernández, 2009) los sistemas biométricos se basan en las características físicas o morfológicas de las personas para así poder hacer algún tipo de reconocimiento, estas técnicas cada día son más confiables ya que estos sistemas se basan en características estables en el tiempo y tienen que cumplir condiciones de universalidad, unicidad, permanencia y cuantificación.

Los sistemas seguridad e identificación biométrica se aplican en diversos procesos por su alto nivel de confiabilidad y comodidad a la hora de autenticar individuos, esta tecnología tiene como base el reconocimiento de una característica física que sea única y que no pueda ser transferida de una persona a otra, como, por ejemplo: las

huellas dactilares, el reconocimiento facial, o el patrón venoso que se encuentran en los dedos.

Figura N° 1: Diferentes tipos de sistemas biométrico

Los sistemas biométricos según los autores, se fundamenta principalmente en el reconocimiento de cualidades únicas de cada ser vivo estos pueden ser las huellas dactilares, el iris de los ojos, los decibeles de las ondas de voz, etc. Los sistemas biométricos se han vuelto fundamentales en la actualidad al momento de bridar seguridad debido a su alto nivel de invulnerabilidad y su eficacia en detección de personas autorizadas y no autorizadas.

1.2. Historia de los sistemas biométricos

La biometría se remonta siglos atrás cuando los antiguos Egipcios median a las personas para identificarlas, esta forma de identificación se basaba en las medidas de algunas partes del cuerpo y sigue siendo utilizada desde entonces; la identificación con la huella dactilar se remonta a la antigua China, no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta, lo hacían como método para distinguir entre los niños y adolescentes. En Occidente, la identificación confiaba simplemente en la memoria fotográfica, hasta que Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló el sistema antropométrico en 1883; este era el primer sistema preciso, ampliamente utilizado para identificar a criminales y convirtió a la biométrica en un campo de estudio. Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema, principalmente problemas con métodos distintos de medidas y cambios de medida; después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar el mismo sistema visto en China cientos de años antes. (Miller, 2014)

1.3. Importancia de los sistemas biométricos

Los sistemas biométricos son importantes ya que desempeña un rol fundamental en los procesos de identificación la verificación de identidad sobre las que se basan las políticas de seguridad en los países los gobiernos se apoyan en estos sistemas para identificar a la población autenticando su identidad en los sistemas informáticos, también lo realizan para reforzar la seguridad publica en aeropuertos y ciudades y restringir acceso a sitio seguros en este caso tanto físico como virtuales. (Etchart, Luna, Leal, & Alvez , 2011).

Desde la antigüedad, el ser humano ha tratado de mantener el control del acceso a sitios, o a información que estima importante, ¡también se ha tratado continuamente de detectar a los individuos que nos rodean o que pertenecen a nuestro mismo clan; los sobres lacrados con el sello real, el razonamiento de un santo y seña, la implementación de una vestimenta específica, la posesión de una llave o de una clave permitieron a partir de continuamente la entrada a sitios restringidos. En la sociedad digital, se han sustituido los objetos de antaño por contraseñas, números PIN, certificados digitales, firmas digitales y tarjetas inteligentes; no obstante, dichos objetos o datos tienen la posibilidad de ser robados, falsificados, filtrados o deducidos; lo cual nos lleva a pensar que para permitir autenticar a una persona, así sea para acceder a un espacio físico, para realizar una transacción bancaria o para hacer una compra se tienen que buscar procedimientos que no dependan de una "llave" definida, sino que nuestra persona sea la llave que le posibilite autenticarse (Ruiz & Mora, 2009).

1.4. Características de los sistemas biométricos

Para (Hidalgo Jacome, 2010) las características principales de los sistemas biométricos es la automatización ya que la mayoría de proceso se los lleva a cabo por medio de un ordenador, por otro lado, no todos los rasgos física de o conductuales de las personas pueden ser estimada como biométrica.

Las características básicas de un sistema biométricos deben cumplirse y expresarse mediante restricciones que deben ser satisfactorias, cada una de ellas básicamente apunta a la obtención de un sistema biométrico con utilidades prácticas, dentro de los sistemas biométricos existen restricciones como el desempeño, el cual se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, otra de las restricciones que se debe de tener en cuenta es la aceptabilidad esta indica el grado en que la personas pueden aceptar un sistema biométrico, y por ultimo encontramos la fiabilidad , la que indica que tan difícil es burlar el sistema.

1.5. Identificación biométrica

La autenticación biométrica, además exitosa como verificación, es el proceso por el cual se comparan los datos de las propiedades de una persona con la "plantilla" biométrica de dicha persona, con el objeto de establecer su similitud. Antes que nada, el modelo de alusión se almacena en una base de datos o en un componente seguro portátil, como una tarjeta inteligente. Después se comparan los datos almacenados con los datos biométricos del individuo para autenticarse.

Para (Gómez Vieites, 2011) en la actualidad existen diferentes métodos para la identificación de la humanidad y estas pueden ser agrupadas en:

- ✓ Algo de una persona, como una tarjeta.
- ✓ Algo que una persona sabe, como una contraseña un código pin de índole confidencial.
- ✓ Algo que una persona tiene como una huella o algo que a la persona hace como escribir o hablar.

El primer método la identificación es muy común mediante DNI o pasaporte, el segundo método requiere de la identidad un contacto con esto la entidad proporciona un numero de contrato o identificador que permita la autenticación en el sistema. El tercer método consiste en la forma automática de identificación basada en reconocimiento de una persona ya sea en bases a la huella dactilares o por medio de iris o cualquier característica q sea única pero que contenga toda la humanidad.

1.5.1. Características

- ✓ Si se trata de lectores de huella digital independientes, tiene la capacidad de almacenar información sobre las personas, mientras que uno no independiente, envía la información a la computadora y esta se encarga de guardar la información.
- ✓ Tienen un tiempo exploración, el cuál determina cuánto tarda en realizar la lectura de la huella digital, se mide en segundos y puede ser de hasta 1.2 s.
- ✓ Tienen un tiempo de verificación, el cuál determina cuánto tarda en procesar la información que recabe de la huella digital, este se encuentra en promedio, se mide en segundos y puede ser de hasta 1.5 s

- ✓ Algunos equipos independientes incluso pueden tener la opción de insertar una contraseña como medida de seguridad adicional.
- ✓ Los modelos con conector USB, se alimentan desde el puerto USB de la computadora, mientras que otros modelos tienen un conector DC o adaptador para enchufe doméstico.
- ✓ Tienen dos valores llamados porcentajes de aceptación y rechazo falsas, las cuáles determinan la fiabilidad del dispositivo, este se mide en % y puede ser muy bajo como ejemplo 0.001%.

1.5.2. Etapas en un sistema de identificación biométrica

Las técnicas de identificación biométrica resultan muy distintas, debido a que cualquier factor relevante de una persona es potencialmente utilizable como componente de identificación biométrica. No obstante, inclusive con la pluralidad de técnicas existentes, en el momento de desarrollar un sistema de identificación biométrica, se preserva un esquema plenamente sin dependencia de la técnica empleada.

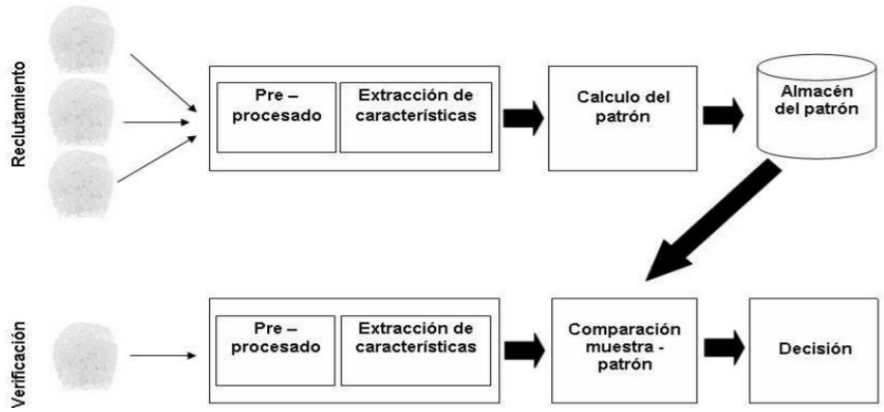


Figura N° 2: Etapas en un Sistema de Identificación Biométrica

a. **Reclutamiento:** En esta etapa, se toma una serie de muestras del cliente, y se procesan, para más adelante sustraer un jefe, el cual se almacenará y va a ser el grupo de datos que caracterizará a aquel cliente. Sise captura bastante más de una muestra, el jefe suele ser el resultado de una media de las propiedades logradas. Este proceso se hace de manera supervisada, o sea, hay una persona delegada de mantener el control de cómo se genera la captura de los datos, así como de afirmar la identidad de la persona que se está reclutando en el sistema. Además, se aprovecha esta etapa para enseñar al cliente cómo funciona el sistema y aclararle cada una de las dudas que pudiera tener.

b. **Implementación:** Cuando se tiene guardado el jefe del cliente, éste puede usar el sistema con normalidad, y sus propiedades son comparadas con el jefe guardado, determinando el triunfo o fracaso de dicha comparación. Como se observa en la Figura 2, todas las etapas mencionadas, está basada en una secuencia de bloques que realizan que las propiedades biológicas o de comportamiento del individuo acaben siendo un componente que lo identifique, estas etapas son:

- ✓ **Captura:** Se toman los datos biofísicos o de comportamiento del individuo; la toma de los datos es dependiente, claramente, de la técnica biométrica empleada, además tienen la posibilidad de hallar muchas variaciones una misma técnica biométrica. Ejemplificando, la huella dactilar podría ser obtenida por cámara de vídeo, ultrasonidos, impacto capacitivo sobre un semiconductor o investigación por láser. Esta etapa es primordial debido a que en ella está contenida la interfaz hombre máquina y el sensor para la captura de la

información biométrica, esto afecta de forma directa en el rendimiento del sistema biométrico debido a que un diseño pobre de la interfaz puede ser en una tasa alta de fallos al conseguir la información. Una forma de medir la eficiencia de esta etapa es con el error de compra (Tasa de error de compra, o FTA) el cual denota la cantidad de veces en la que el dispositivo de captura fracasa al obtener la característica biométrica.

- ✓ **Preprocesado:** En este bloque se adecuan los datos capturados para facilitar el procedimiento que tiene que hacer el siguiente bloque. Este bloque se delega, dependiendo de la técnica, de labores como: reconocer el principio de una oración y medir el sonido de fondo, binarizar y hacer una sustracción de bordes de la imagen, ubicar la muestra, rotarla y ampliarla o reducirla, para que esté entre los márgenes que reconoce el algoritmo siguiente, etc.
- ✓ **Extracción de Propiedades:** En esta etapa, los datos son procesados y un grupo de propiedades discriminatorias son extraídas para representar los aspectos medidos, estas propiedades conforman una plantilla, la cual es almacenada en una base de datos para su siguiente uso; por otro lado, en algunos casos, el desconocimiento sobre las propiedades que se tienen que sustraer, lleva a usar técnicas fundamentadas en Redes Neuronales, que, por medio de entrenamiento de las mismas, se tratan de adecuar a los resultados esperados.
- ✓ **Comparación:** Una vez extraídas las propiedades de la muestra capturada, se han de equiparar éstas con las anteriormente almacenadas, lo más relevante que se debe dejar claro una vez que se habla de este bloque, es que no

hablamos de una comparación binaria o de igualdad, sino que la alteración de las muestras, por diferencias en la captura o leve alteración de las propiedades de individuo, hacen que la comparación dé como consecuencia un puntaje ó posibilidad de afinidad. Por consiguiente, para establecer el triunfo o fracaso de la comparación, habrá que decidir un umbral (n) de tolerancia en dicha posibilidad. La comparación puede estar basada en todas las diferentes maneras que da la Teoría de Reconocimiento de Patrones, Métricas como la Distancia Euclídea, Distancia de Mahalanobis o Distancia de Hamming ó Estadísticas usando funcionalidades de repartición, clasificadores bayesianos, o técnicas fundamentadas en modelado de inconvenientes como Redes Neuronales, Modelos de Mezclas de Gausianas, etc. En el reclutamiento además se muestra un tipo de error conocido como error de reclutamiento (Tasa de error de reclutamiento, o FTE) el cual sugiere la cantidad de usuarios que no tienen la posibilidad de ser enrolados de manera correcta en el sistema biométrico.

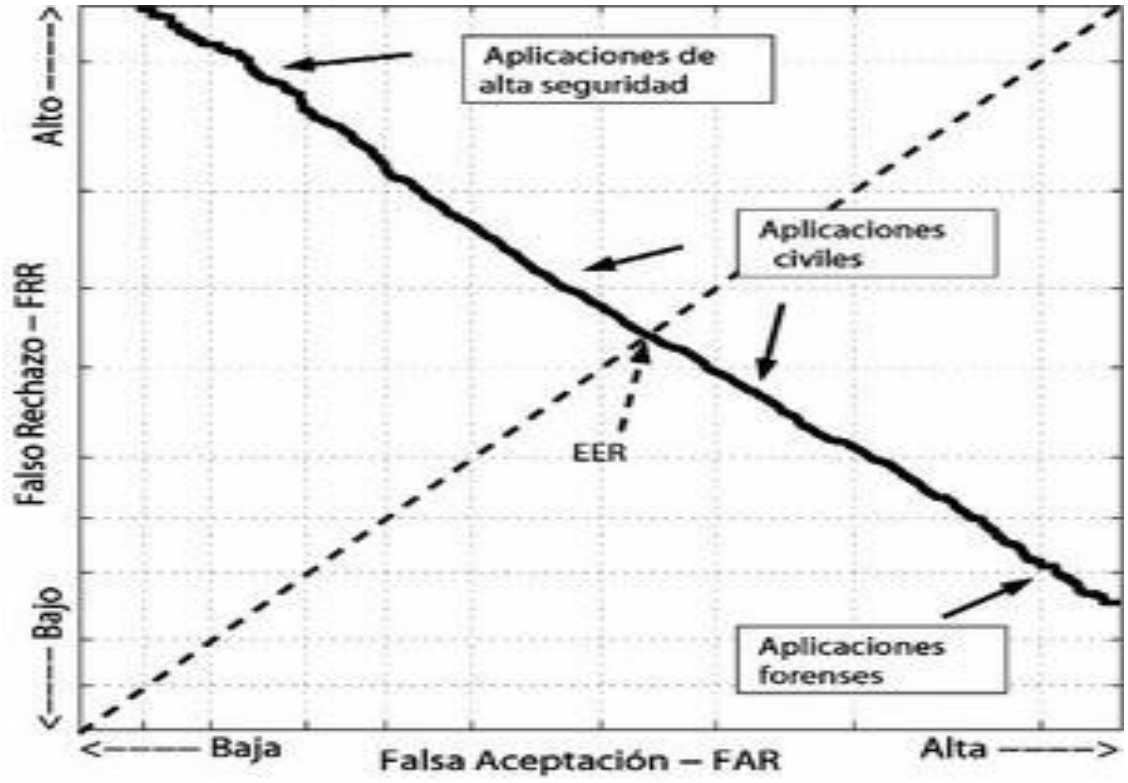


Figura N° 3: Rendimiento de un sistema biométrico resumido en un gráfico DET (La curva de rendimiento es calculadas usando los resultados de comparación del FaceG)

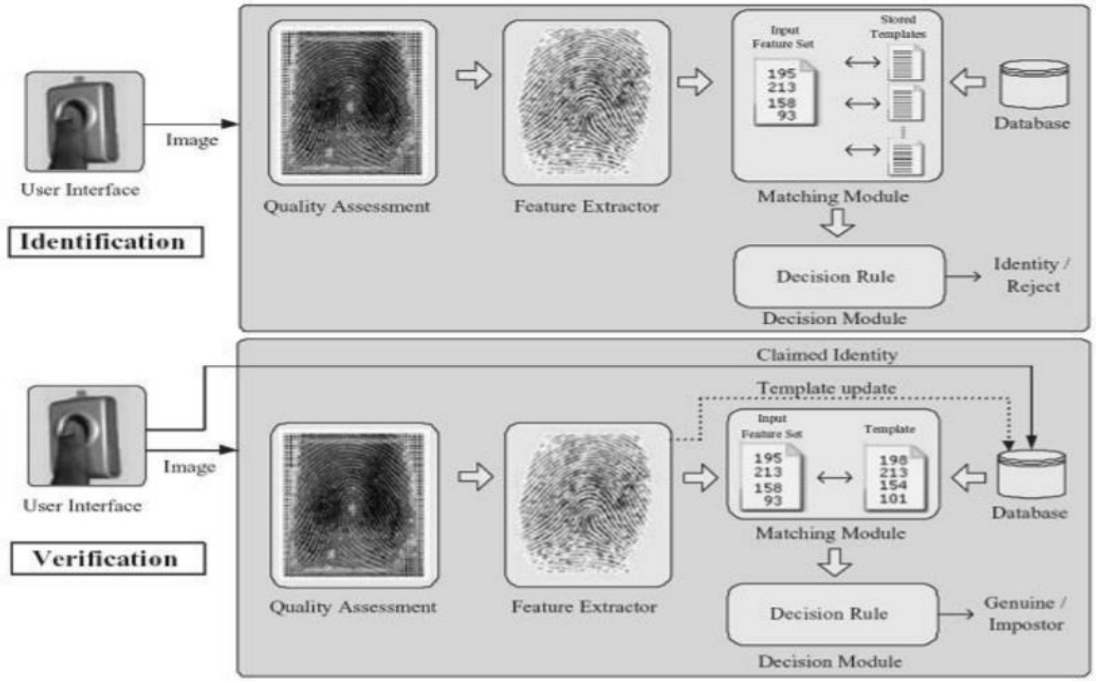


Figura N° 4: Reconocimiento (arriba) y Autenticación (abajo), diferencias entre las 2 fases

c. **Reconocimiento/Autenticación:** La identificación se puede realizar basándose en dos esquemas de funcionamiento del Sistema Biométrico:

- ✓ **Reconocimiento:** Se basa en identificar a un usuario dentro de todos los usuarios que ya se encuentran en el sistema. Por lo tanto, se comparan las características extraídas con los patrones de todos los usuarios reclutados por el sistema, este esquema de funcionamiento, necesario para muchas aplicaciones, tiene como inconvenientes la necesidad de una Base de Datos de patrones y la existencia de una red de comunicaciones, siempre on-line, que comunique los puestos de identificación con la Base de Datos. El resultado de la comparación puede ser: siempre positivo, es decir, se identifica siempre con el usuario que ha dado una probabilidad más alta, o puede indicar rechazos, si el usuario con la mayor probabilidad no supera un determinado umbral.
- ✓ **Autenticación:** también llamado sencillamente verificación, en este esquema de funcionamiento, el usuario, al que se le toman sus características biométricas, también comunica su identidad. El sistema se encarga, entonces, de comparar las características extraídas, con el patrón del usuario indicado. Si la comparación supera un determinado umbral de similitud, se considera que el usuario es el indicado, rechazando la comparación en caso contrario. El patrón del usuario puede estar almacenado en una Base de Datos, tal y como se hace en los sistemas de Reconocimiento, o, si el patrón es suficientemente pequeño, en un sistema portátil de información como puede ser una tarjeta. En este último caso no son necesarias ni la Base de Datos ni la red de comunicaciones de los sistemas de Reconocimiento.

Como se puede ver claramente en la figura 4 que la principal diferencia entre los esquemas se encuentra en el módulo de coincidencias o matching module ya que en este módulo se procesan las coincidencias entre las características.

d. Medición del rendimiento: Uno de los aspectos más importantes para el funcionamiento de un sistema biométrico es su rendimiento, este se puede resumir utilizando medidas de un solo valor como la tasa de error igual (Equal Error Rate, o EER) y el valor d-prima (D-prime value, o d'). El primero se refiere a un punto en el DET donde el FAR es igual al FRR, un valor bajo en el ERR indica un mejor rendimiento. El valor d-prima, mide la separación entre las medias de las distribuciones de probabilidad del genuino y el impostor en unidades de desviación estándar, este se define como:

$$d' = \frac{\sqrt{2}\left|\mu_{genuino} - \mu_{impostor}\right|}{\sqrt{\sigma^2_{genuino} + \sigma^2_{impostor}}}$$

Donde μ's y σ's son las medias y las desviaciones estándar, respectivamente, de las distribuciones del genuino y del impostor, un valor d-prime alto indica un mejor rendimiento del sistema biométrico.

1.5.3. Técnicas de identificación biométrica

En los últimos años la biometría ha crecido a partir de utilizar sencillamente la huella dactilar, a utilizar varios procedimientos diversos teniendo presente numerosas medidas físicas y de comportamiento, tales como el andar, el tipeo o la voz; tal es de esta forma, que el reconocimiento por biometrías pertenece a los problemas mundialmente más investigados en la actualidad; los resultados de estas

investigaciones permitieron conseguir nuevos descubrimientos acerca corporal humano y los patrones conductuales para expandir la lista de aspectos o propiedades que son útiles para la identificación, e inclusive el uso combinado de dichos aspectos. Por ejemplo, actuales descubrimientos han demostrado la probabilidad de utilizar la impresión de las orejas, ondas cerebrales, latidos del corazón y ADN como base para verificar la identidad. Las aplicaciones de la biometría además han incrementado a partir de sólo identificación de los organismos vivos hasta complejos sistemas de estabilidad.

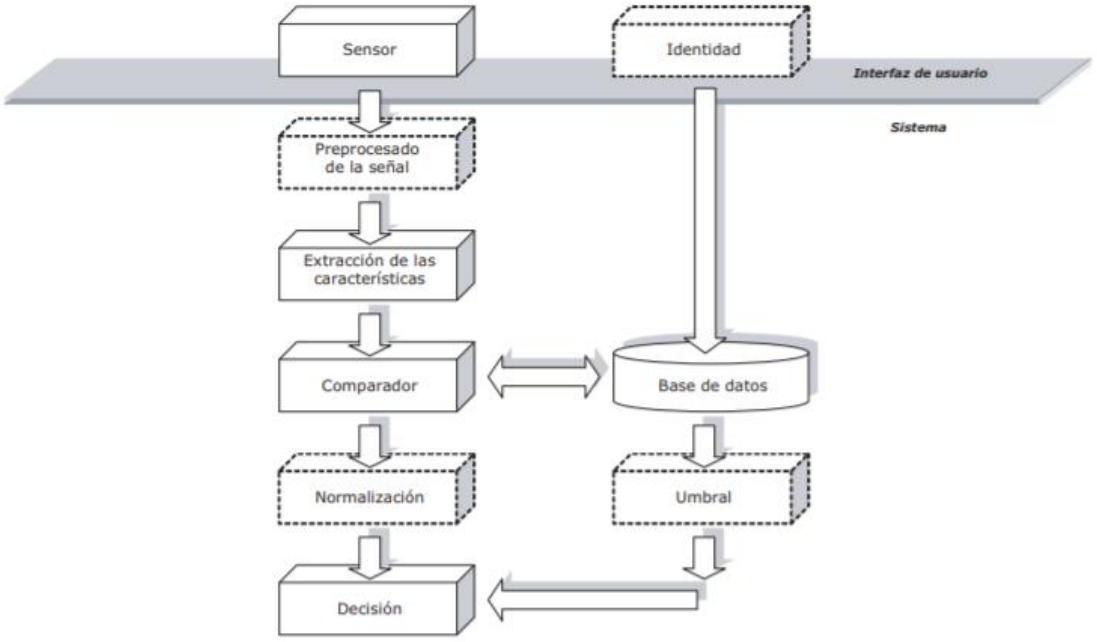


Figura N° 5: Esquema de funcionamiento de un sistema de reconocimiento biométrico

Según el autor (Escobar, 2010) en la actualidad debido a los avances de la tecnología se encuentra diferentes productos biométricos que permiten reconocer al ser humano de una manera fácil y segura como lo son:

1.5.3.1. Reconocimiento facial o de rostro.

Menciona (Hernández, 2010) que, a lo largo de los últimos años, el reconocimiento del rostro se convirtió en uno de las aplicaciones más estudiadas en campos como la biometría, el procesado de imagen o el reconocimiento de patrones. Una de las causas que ha llevado a este incremento son las necesidades cada vez más grandes de aplicaciones de estabilidad y vigilancia usadas en diferentes entornos.

El rostro es uno de los más importantes focos de atención en nuestras propias relaciones sociales diarias, centramos nuestra atención visual en las propiedades y expresiones faciales. Somos capaces de reconocer centenares de rostros, incluyendo el de esas personas que no hemos observado a lo largo de cualquier tiempo, realizando esta labor en una parte de segundo

El reconocimiento de rostro es menos exacto que el análisis de huellas dactilares debido a que este método no es un método invasivo. Estos métodos clasifican la apariencia humana y miden los puntos nodales del rostro, este análisis tridimensional en la cara descarta algunos inconvenientes que se presenta en un reconocimiento bidimensional, en la actualidad hay muchos códigos fuentes desarrollados que permiten realizar el análisis facial de una manera fácil hasta con implementos de redes sociales.

La forma de hacer el estudio de los datos, los algoritmos de reconocimiento de la cara se ordenan en dos grupos: procedimientos basados en propiedades y procedimientos basados en el aspecto.

- ✓ **Los procedimientos basados en propiedades**, hacen la exploración de las características y la geometría de la cara, como por ejemplo zonas, distancias y ángulos entre los recursos de la cara.
- ✓ **Los procedimientos basados en aspecto**, conocidos además como procedimientos holísticos, piensan en el rostro como un todo y hacen un estudio universal usando herramientas estadísticas. Dichos procedimientos buscan un nuevo subespacio de menor magnitud para proyectar los rostros.

El reconocimiento de individuos por medio del rostro se hace un estudio de la composición general, la manera y las proporciones de la cara. Las propiedades extraídas en el reconocimiento del rostro son habitualmente las distancias entre los diversos órganos como ojos, nariz y boca, la zona de todos ellos, el ángulo conformado entre órganos (Granda Carrillo, 2013).

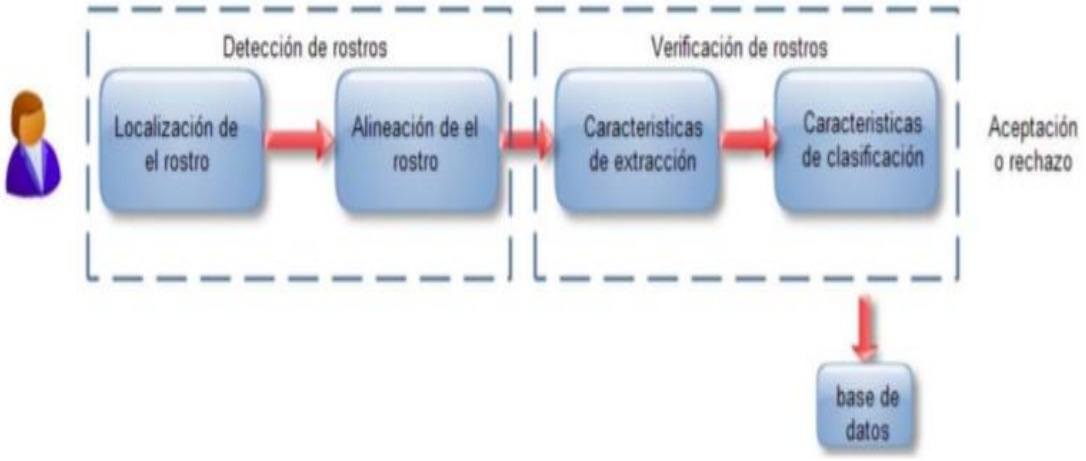


Figura N° 6: Etapas de reconocimiento facial

1.5.3.2. Reconocimiento de firmas.

Esta biometría es menos problemática debido a que es más difundida en el mundo, más económica al implementa. Estos sistemas de este tipo necesitan de una tableta que le permita la escritura conectada al computador, esta escanea la firman y analizan la misma desde dos puntos de vista los cuales son la firma en sí y el modo en que se efectúa. Los datos almacenados deben de incluir velocidad, precisión, dirección, largo de trazado, y el área donde el lápiz se levanta, el único inconveniente de este método es que una persona nunca firma de manera idéntica dos veces.

Dice (Granda Carrillo, 2013) que la firma manuscrita dentro del reconocimiento biométrico, es la más usada en el planeta como medio de autentificación, teniendo asentimiento legal, según se avanza la tecnología se vio el desarrollo de la misma, de pasar de firmar sobre el papel a hacer la firma sobre una tableta digitalizadora y ahora el desarrollo de la firma 3D por medio de gestos, con un dispositivo que cuente con los sensores necesarios para la compra de los datos, que definen la conducta del individuo y que faciliten su reconocimiento.

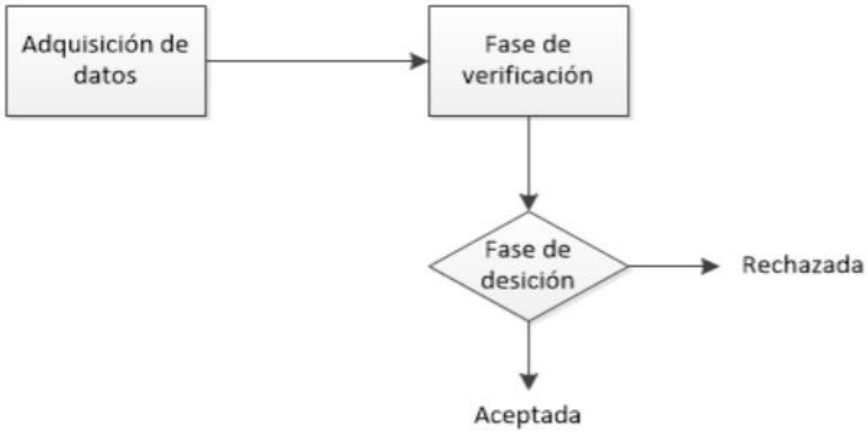


Figura N° 7: Etapas de reconocimiento de firma

(Mendaza Ormaza, Hurtado, Sánchez Reillo, Valverde Albacete, & Peláez Moreno, 2010) afirman que dada una firma que forma parte del usuario, una elección se toma sobre si esa firma fue elaborada por aquel usuario, una firma genuina, o fue desarrollada por otro cliente, una firma falsificada. Típicamente, las firmas falsificadas se ordenan en tres conjuntos:

- ✓ **Las falsificaciones aleatorias** se hacen sin ningún entendimiento sobre las firmas del cliente o de su nombre.
- ✓ **Las falsificaciones básicas** se hacen sabiendo el nombre del cliente sin embargo sin ningún entendimiento sobre su firma.
- ✓ **Las falsificaciones expertas** se hacen con un entendimiento completo sobre el nombre y la firma del cliente.

1.5.3.3. Mapa de la retina del ojo.

Esta mide el patrón de venas en el fondo del ojo, y esta se obtiene por medio de una proyección de una luz infrarroja a través de la pupila, este sistema no es muy fiable debido a que se ha comprobado que es apto a cambios producido por irritación ocular.

Dice (Villalobos Castaldi , 2011) que el patrón que conforman las venas que permanecen por abajo del área de la retina es un patrón estable y exclusivo; por consiguiente, es un procedimiento biométrico confiable. Utilizando método ópticos semejantes a los de un retinoscopio, tienen la posibilidad de obtener imágenes digitales del patrón de la retina de un sujeto por medio de la proyección de tenue haz de luz hacia el ojo. Para captar la imagen fundamental para el reconocimiento, es preciso que el individuo a detectar mire fijamente y bastante de cerca un dispositivo y mantenga su vista fija en un punto definido, pese a su fiabilidad, en muchas situaciones no se puede hacer que los sujetos a detectar cumplan con el método, además, de que necesitan de un equipo demasiado costoso.

Figura N° 8: Obtención de mapeo venosa en la retina del ojo con escáner biométrico

1.5.3.4. Patrón del iris

Este sistema es uno de los confiables ya que el iris posee alrededor de 266 puntos únicos mientras que la mayoría de los sistemas biométricos ostentan un alrededor de 13 a 60 características distinta, en este sistema se obtiene un mejor resultado debido a que cada ojo es único y permanece estable con el paso del tiempo.

(Tomé González, 2008) define que el reconocimiento de iris como uno de los medios más exactos y fiables; esto ha provocado un enorme interés en los últimos años gracias a sus aplicaciones en el campo de estabilidad y a su uso.

El iris humano se basa en un anillo ubicado entre la pupila y la esclera, el cual tiene enorme proporción de característica bastante estricta como bastoncillo, corona, pliegues, etcétera; estas propiedades visibles que se identifican como textura del iris, son únicas y propias de cada persona.

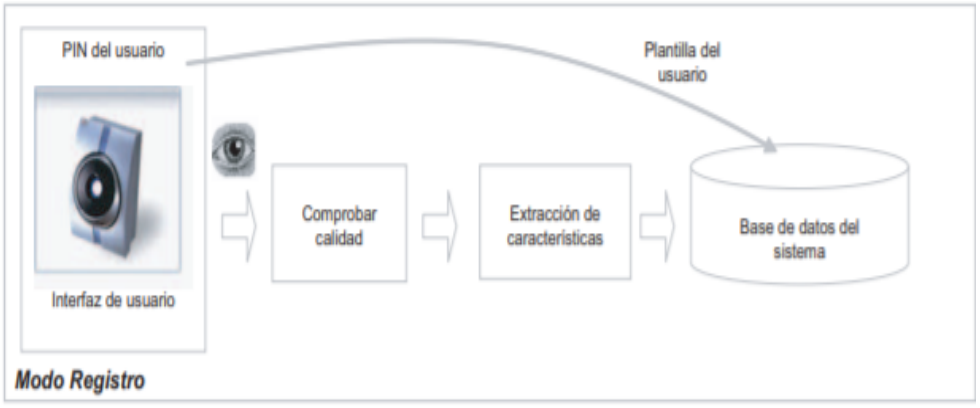


Figura N° 9: Esquema de funcionalidad del modo registro

Aunque la coloración y la composición del iris permanecen genéticamente ligadas, los detalles de los patrones no lo permanecen, el iris se realiza a lo largo del aumento prenatal con un preciso proceso de formación y plegado de la membrana

del tejido fino, y es ya en la juventud una vez que al final se estabiliza la pigmentación y la medida de la pupila; se estima que la iris de las personas son únicos y estructuralmente diversos, lo cual le posibilita que sea usado para fines de reconocimiento.

1.5.3.5. Reconocimiento de la voz

El análisis de la vos se considera que es uno de los sistemas biométricos eficaz, debido a que se ha comprobado de que cada persona contiene patrones únicos en su palabra, este sistema funciona la digitalización de palabras de una persona ya que toda persona en sus palabras se encuentra en segmentos y de ellos se obtiene 3 o 4 tonos dominantes y son capturado de en forma digital y se almacenan en una tabla.

Mencionan (García Cueva & Yunga Ochoa, 2010) que la biometría de voz es un sistema que posibilita detectar y autenticar la identidad de un sujeto por medio del reconocimiento de los patrones de su voz; en otras palabras, viable ya que el artefacto vocal de cada ser humano es exclusivo. Los aspectos físicos, tanto fonéticos como morfológicos, son particulares a cada individuo, lo cual los convierte en inmunes a imitaciones. Esta característica da a la tecnología virtud sobre otros sistemas de identificación, como la introducción de un PIN.

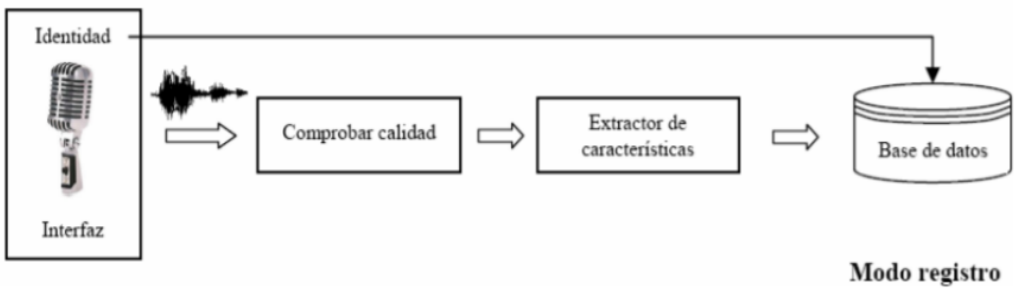


Figura N° 10: Estructura de un Sistema de Reconocimiento Biométrico en modo Registro

Refieren (Carrasco, Portugal, & Peralta, 2006) que los sistemas de reconocimiento de voz tienen dos módulos primordiales:

- ✓ **La sustracción de propiedades** es el proceso por el que extraemos una pequeña proporción de datos de la señal de voz que podría ser utilizada para representar a cada individuo.
- ✓ **La comparación de propiedades** implica el proceso de detectar a el individuo desconocida comparando las propiedades extraídas de su voz, con las anteriormente conseguidas, correspondientes a los individuos conocidas por sistema.

1.5.3.6. Reconocimiento de huellas dactilares

Esta es la técnica más antigua y por ende la muy utilizada a nivel mundial ya que las huellas dactilares son únicas y no cambia a lo largo de la vida, esta huella esta normalmente conformadas por una serie de líneas oscura que presentan la cresta y una serie de espacios blancos que presentan los valles, esta identificación funciona a través de la ubicación y dirección de la terminación de la cresta, bifurcaciones, deltas balles y cresta.

(García Donday, 2014) dice que las crestas dactilares de los dedos y las palmas de manos y pies se componen en el séptimo mes de gestación y están invariantes durante toda la vida. Esto hace de las huellas dactilares un rasgo biométrico bastante llamativo para sistemas de reconocimiento. Su elevado nivel de asentimiento provoca que su uso se encuentre bastante extendido en aplicaciones comerciales, sin embargo, además en el campo forense, en el cual hablamos de detectar criminales que dejan sus huellas en la escena de un crimen, la unicidad de las huellas dactilares está plenamente asumida a pesar de ser un hecho concebido desde datos empíricos

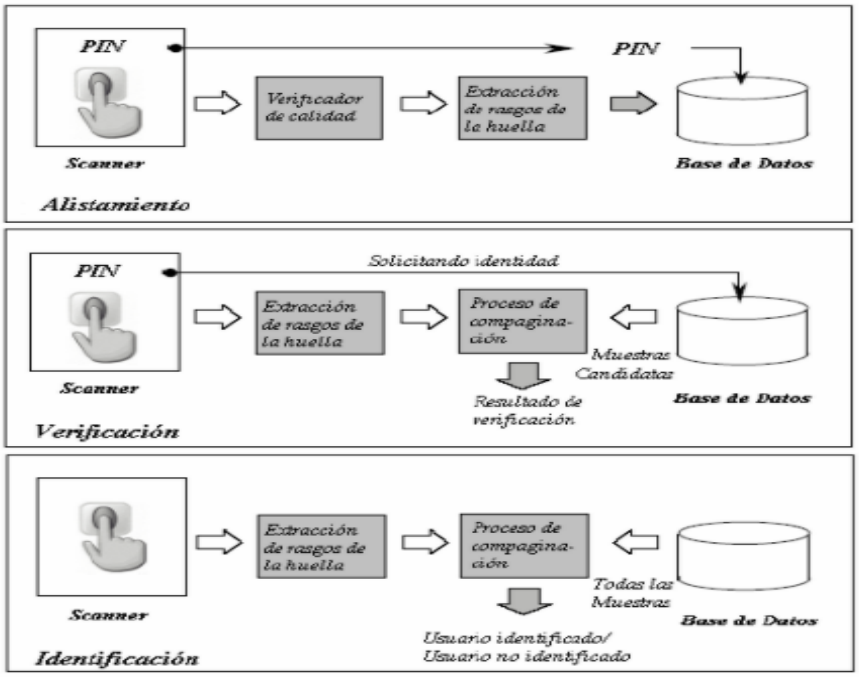


Figura N° 11: Esquema de un reconocimiento de huellas dactilares

1.5.3.7. Geografía de la mano.

Las características biométricas de manos se refieren usualmente a medidas geométricas tales como: longitud, anchura y altura de la mano y dedos. El número

de características obtenidas varía en los distintos trabajos. Por ejemplo, se obtienen 17 medidas de la mano referentes a la longitud de los dedos, anchuras y alturas; estas medidas son relativas a puntos predeterminados en la imagen mediante un conjunto de pivotes, se extraen 16 medidas de forma similar mediante unos ejes prefijados. Así se analizan los puntos de intersección de los dedos y mano con esos ejes para obtener las características de longitud y anchura, se utiliza un sistema con 30 características, donde han añadido otras medidas como por ejemplo la desviación de los dedos.

Como se ha mencionado antes, en todos estos trabajos se requiere un posicionamiento específico de la mano para obtener características invariantes. En este sentid se puede decir que la posición de la mano está referida a un sistema de referencia universal.

Por otra parte, se definen nuevas invariantes, como ángulos de apertura de la mano, posiciones de los extremos, y plantillas basadas en la disposición natural de la mano, que no están presentes en otros sistemas, estas son definidas al considerar un sistema de referencia propio inherente para cada mano en vez de una estrategia de sistema de coordenadas universal. Consecuentemente, todas las medidas son referenciadas sobre cada sistema propio, esperando una invarianza en la imagen para todos los registros de un mismo individuo, esto hace que no sea necesario delimitar la mano por medio de pivotes ni obligar al usuario a adoptar un posicionamiento determinado; el único requisito exigible es que el usuario extienda

su mano de modo natural antes de tomar una muestra. Esto implica que el prototipo desarrollado sea flexible, fácil de mantener y fácil de utilizar.

Para obtener estos datos es necesario un procesamiento de la imagen más complejo de detección de las articulaciones y segmentación de cada dedo, que se describirá en el siguiente apartado, de este modo se obtienen un total de 70 medidas geométricas sobre una colocación libre de la mano basándose en medidas físicas longitudes, anchuras de dedos y falanges etc; y en datos referentes a la posición natural de la mano posiciones, plantillas de borde, etc. Además, se obtienen medidas de la mano derecha e izquierda, por lo que se tienen el doble de datos e incluso se pueden estudiar la correlación existente entre ambas manos de un individuo, ya que como se sabe no existe simetría exacta entre el lado izquierdo y el derecho del cuerpo humano.

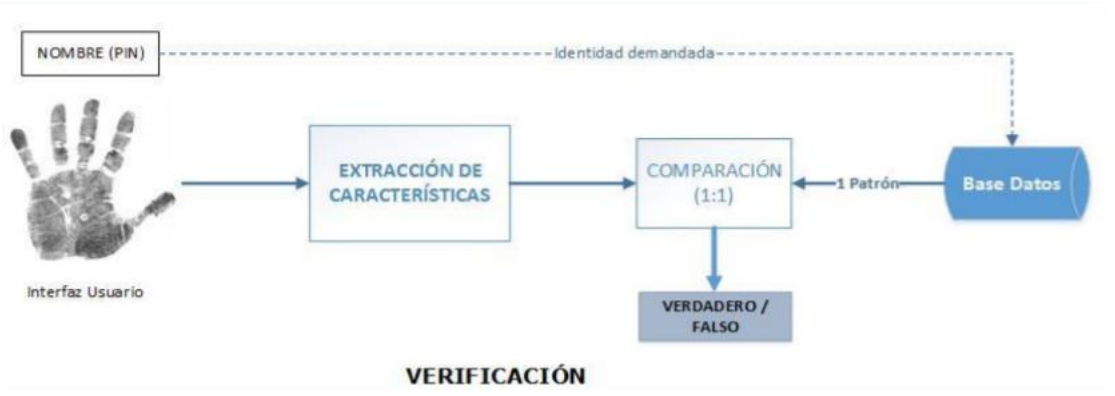


Figura N° 12: Esquema de verificación de un usuario por medio de un escáner de mano

1.6. Control de accesos

Mencionan (Romero Aguirre & Oviedo Chima, 2020) que los controles de acceso son la capacidad de permitir o denegar la utilización de un recurso físico o áreas

restringidas según rango del visitantes o virtual acceso a información a personas o entidades en especial; para ofrecer claridad al plan, se desea llevar a cabo un control de ingreso físico que está con base en el control de ingreso y salida en inmuebles, edificios, cuartos o superficies concretas sólo a personas autorizadas.

También (Vega Briceño, 2021) dice que la limitación al acceso se refiere a admitir ciertos acceso a nuestro recursos pero hasta un cierto punto, además se halla la revocación del acceso, el cual evita otorgar una parte de acceso a un recurso este se lo pueda quitar nuevamente; actualmente estos sistemas de controles de acceso se lo encuentran en múltiples formas para diversas aplicaciones.

1.6.1. Tipos de controladores

Para (Consentino, 2014) en la actualidad dentro del mercado existen tres tipos de controladores los cuales se manejan según el tamaño que tenga el sistema de control esperado.

a. Controladores autónomos simple.

Este tipo de controladores son los más recomendado para ser utilizado en el sistema de muy pocas puertas ya que consta con las características tales como poseen incorporados el lector de huella, reciben en forma local de tarjetas o teclado de programación, no almacenan eventos ni tampoco poseen comunicación a una instancia superior.

b. Controladores de sistemas distribuidos de muchos accesos

Este tipo de controladores son de acceso múltiples trabajan mediante barios controladores, y siguiendo una topología lógica donde cada uno de los

controladores se comunica mediante el centro del control en la mayoría de los sistemas funciona con servidores de sistema, por medio de estos controladores se guarda una armoniosa relación entre la cantidad de las puertas con el dispositivo lector que administra con capacidad de memoria y cantidad de entrada y salida que poseen

c. Controladores mixtos

Estos controladores tienen una característica intermedia entre los controladores anteriores, ya que por un lado poseen capacidad de programar, admiten bandas horarias y se comunican con un centro de control, a través de esta capacidad facilita el manejo de sistema intermedios y no se debe generar inconsistencia.

1.7. Base de datos

Concreta (Cruz Chávez, 2011) que una base de datos es una recopilación de archivos involucrados que posibilita el desempeño de la información de alguna compañía, todos estos archivos podrían ser observado como una recolección de registros y cada uno de estos registro está compuesto de una recolección de campos; los campos de cada registro posibilitan llevar información de cualquier atributo de una entidad de todo el mundo, un documento de una base de datos podría ser pensado como una tabla en la que poseemos renglones y columnas, cada renglón correspondiendo a un registro del documento y cada columna correspondiendo a un campo.

(Gutiérrez Díaz, 2005) menciona que una base de datos almacenados y organizados de manera que un programa del ordenador logre seleccionarlos velozmente y capaces de ser: recobrados, actualizados, insertados y borrados.

1.7.1. Tipos de bases de datos

a. Conforme con la flexibilidad de modificación

La primera categorización de bases de datos es dependiente de la forma en la que se catalogan los datos.

- ✓ **Bases de datos fijas**

Permanecen diseñadas para la lectura de datos, en otros términos, únicamente almacenan y registran los datos; después tienen la posibilidad de examinar para entender su comportamiento en todo el tiempo. Son en especial usadas para llevar a cabo proyecciones estadísticas y orientar procesos de tomas de elecciones en el campo empresarial.

- ✓ **Bases de datos dinámicas**

Son, por otro lado, modificables con el paso del tiempo. De esta forma, los datos tienen la posibilidad de actualizarse, editarse y eliminarse.

b. De acuerdo con el contenido

La segunda categorización de bases de datos es dependiente de la prioridad del contenido a examinar.

- ✓ **Bases de datos bibliográficas**

Son registros que ayudan a clasificar diversos campos de datos. Principalmente, estos campos tienen la posibilidad de consultar de modo separado o grupo, un claro

ejemplo podría ser los datos sobre un libro: creador, año de publicación, editorial, etcétera.

- ✓ **Bases de datos de escrito completo**

Son en especial útiles, pues permiten buscar términos específicos, palabras claves y las múltiples posibilidades de una base de datos bibliográfica, además de consultar el escrito entero guardado. Son correctas para trabajos académicos y de indagación.

- ✓ **Directorios**

Son Bases de Datos utilizadas por la mayor parte de la población casi a diario sin advertir, un caso muestra claro podría ser la agenda de contactos de nuestros propios teléfonos móviles, donde se almacena muchedumbre de información como:

- ❖ **Nombres y direcciones.**
- ❖ **Número telefónico y direcciones de email.**
- ❖ **Datos de facturación, códigos postales.**

c. Según los modelos de bases de datos

Se caracteriza por los diferentes modelos de gestión de datos, una de las enormes ventajas de estas Bases de Datos es que permiten la utilización de sistemas eficientes de Bases de Datos basados en algoritmos.

- ✓ **Bases de datos jerárquicas**

Almacenan la información en una composición jerárquica o con un orden de trascendencia, de esta forma, los datos se organizan en una figura parecida a un

árbol invertido con segmentos conocidos como nodos y ramas, que tienen dentro información de interés; dichos tienen la posibilidad de ser de 3 categorías:

- **Padre**
- **Hijo**
- **Raíz**

En medio de las primordiales propiedades de uno de los tipos de bases de datos más utilizadas se hallan las próximas:

- Se puede compartir la entrada y la información con diversos usuarios.
- Los datos son independientes.
- Es difícil modificarla, pues es una composición dura.
- Se requiere enorme entendimiento de las unidades de información.
- Los nodos lejanos de la raíz son de difícil ingreso, por lo cual hace falta tiempo.

✓ **Bases de datos de red**

Son una alteración de la anterior, su primordial diferencia radica en la estructura del nodo, debido a que en este modelo tienen la posibilidad de tener diversos padres; entre sus primordiales contras es que es complicado modificarlas y adaptarlas al tener una composición compleja.

✓ **Bases de datos transaccionales**

Son las encargadas de mandar y recibir datos a enorme rapidez, es raro que los usuarios “normales” las usen, pues permanecen dirigidas a ciertos sectores como los sistemas bancarios, en los cuales ejemplificando se registran operaciones inmediatas entre cuentas con los que corresponden datos de dichas operaciones.

✓ **Bases de datos relacionales**

Son, actualmente, uno de los tipos de bases de datos más usados, el lenguaje predominante en ellas es el Structured Query Language, más reconocido como SQL.

Los datos se almacenan en registros organizados en tablas, por lo cual tienen la posibilidad de asociar y cruzar los recursos con facilidad, es una base de datos aconsejable si los datos poseen un margen de error nulo y no requieren modificaciones sucesivas. Sus primordiales propiedades son:

- Pueden ser usadas por cualquier cliente.
- Su administración es simple.
- Se puede entrar inmediatamente a los datos.
- Garantiza la total consistencia de los datos, sin probabilidad de error.

✓ **Bases de datos deductivas o lógicas**

Se aplican principalmente en buscadores, aunque tienen la posibilidad de utilizarse de otras posibilidades; con ellas tienen la posibilidad de guardar los datos y consultarlos por medio de búsquedas sujetas a normas y reglas anteriormente establecidas; sus primordiales propiedades son:

- Permiten manifestar consultas por medio de normas lógicas.
- Soportan conjuntos de datos complicados.
- Se puede deducir información por medio de datos almacenados.
- Utilizan fórmulas matemáticas o algoritmos lógicos.

✓ **Bases de datos multidimensionales**

Se aplican para funcionalidades específicas, lo cual las separa de las bases de datos relacionales únicamente se aprecia a grado conceptual, pues en las

multidimensionales los campos o atributos de una tabla tienen la posibilidad de ser de 2 tipos:

- Pueden representar magnitudes en una tabla de datos.
- Pueden representar las métricas que se pretenden obtener.

Algunas de sus primordiales propiedades son:

- No emplean ni una jerarquía.
- Facilitan la averiguación y la modificación siguiente.
- Usan un lugar menor de almacenamiento.
- Tienen ingreso a enormes porciones de información.

✓ **Bases de datos orientadas a objetos**

Son de las más modernas, en especial por su enorme capacidad y potencia, una de sus primordiales propiedades es que en ellas no se guarda información descriptiva sobre el objeto, debido a que se almacena por completo al mismo, cada objeto tiene propiedades propias que le permiten marcar la diferencia de otros semejantes. Sus ventajas son claras:

- Admiten más proporción de contenido.
- Permiten que el cliente tenga más información de primera mano.

✓ **Bases de datos documentales**

Usan documentos, como la composición de almacenamiento y consulta de datos, estos se conforman por diversos registros y datos y se construyen con lenguaje NoSQL, lo cual les da muchas ventajas técnicas y de flexibilidad.

Con estas bases de datos se puede manejar gigantes volúmenes de información en cortos períodos de tiempo, sus variadas funcionalidades y módulos adaptables a

varios mecanismos de consulta les transforman en uno de las Bases de Datos más usadas por los programadores.

2. Ejecución de trabajo

2.1. Introducción

En este punto se da la explicación del proceso de implementación de un control de acceso biométrico en las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone, previa su implementación se creyó correcto ejercer dos técnica de observación y la bibliográfica para así establecer, visualizar el lugar correcto de instalación y poder esclarecer las problemáticas que en estas se vienen suscitando, a su vez poder obtener una amplia lista de información con el cual llevamos a cabo el proyecto.

A la hora de seleccionar entre todos los sistemas de biométrico que existen en el mercado, se decidió por un sistema detector de huella dactilar, esta decisión fue hecha al ver que esta cuenta con un mayor grado de éxito para la identificación de personas, la efectividad que este tiene ya sea en la seguridad y su margen de error mínimo con la cual cuenta, esta certeza se debe a que en el mundo no existen dos huellas iguales ya que estas son un código de barra único que todo ser humano tiene y cada uno posee uno distinto.

Se aplicará este tipo de dispositivos biométricos con la intención de resguardar la integridad de los salones, de esta manera poder obtener un mejor aprendizaje y así cuidar y proteger las pertenecías.

2.2. Huella dactilar

La huella es la impresión moldeada o visible que genera el contacto de las crestas capilares de un dedo de la mano, principalmente se utiliza el dedo índice o pulgar; tienen propiedades únicas denominadas minucias, las cuales son aspectos donde los bordes terminan o se separan.

Esta complexión es exclusiva para cada individuo y una vez determinada en la semana 19 de gestación, permanece inalterada toda la vida, por esta razón el dibujo de la huella dio lugar a la dactiloscopia, sistema científico de identificación por medio de la comparación de las huellas digitales; su carácter científico no es exagerado, debido a que la dactiloscopia se fundamenta en las leyes científicas de la perennidad y la inmutabilidad, y está respaldada además por la probabilidad matemática (Juanes, 2018).

Confirman (Rojas Portilla & Suárez Rueda, 2018) que se obtienen por medio de la obtención directa de la huella dactilar al situar el dedo sobre el área sensible del sensor electrónico, el método de la conversión de la huella capturada en una imagen digital es dependiente de los principios físicos de manejo del sensor usado. Entre los sensores, los más empleados son los sensores ópticos, dichos se fundamentan en la meditación de la luz sobre la yema del dedo, los sensores basados en fibra óptica, los electroópticos y los sensores sin contacto.

2.2.1. Composición de una huella dactilar

También definen (Rojas Portilla & Suárez Rueda, 2018)a huella dactilar tiene unas propiedades morfológicas particulares que permiten la definición de patrones en el

momento de la lectura en respectivos dispositivos, estas propiedades conforman la huella: crestas papilares y surcos o valles interpapilares que se ubican en la dermis, construyendo una secuencia de dibujos en la falange de los dedos de las manos que definen particularidades como un núcleo o numerosas deltas

Abrupta terminal	**Cresta de trazado más o menos horizontal que leída de izquierda a derecha, termina.**
Abrupta superior	Cresta de trazado más o menos vertical que acaba por su parte superior.
Abrupta inferior	Cresta de trazado más o menos vertical que acaba por su parte inferior.
Bifurcación	Cresta que proviniendo del lado izquierdo del dibujo papilar se desdobla en dos que siguen paralelas un trecho más o menos largo.
Convergencia	De igual forma que la bifurcación, aunque de orientación opuesta. Constituida por dos crestas paralelas que se fusionan formando una sola.
Fusión superior	Dos crestas paralelas, más o menos verticales, que proviniendo de la zona inferior del dactilograma se fusionan formando una sola.
Fusión inferior	Una cresta más o menos vertical, que proviniendo de la zona inferior del dactilograma se desdobla en dos que siguen paralelas un trecho más o menos largo.
Desviación	Dos crestas procedentes de lados opuestos del dactilograma que en el punto de encuentro se desvían y acaban.
Empalme	Cresta que corta que enlaza otras dos, más largas y paralelas.
Cuña	Formado por tres crestas abruptas, una de las cuales termina en el inicio del surco interpapilar formado por las otras dos de sentido opuesto.
Fragmento	Cresta de extremos abruptos y longitud variable y que no supere dos cuadrículas.

Interrupción	Discontinuidad de una cresta que no supere dos casillas.
Ojal	Espacio interpapilar elíptico formado por las dos ramas de una cresta bifurcada que vuelven a fusionarse por convergencia.
Punto	Pequeño fragmento de cresta tan corto como ancho.
Secante	Constituida por dos crestas que se cortan en forma de “aspa”.
Vuelta insólita	Cresta que, cambiando progresivamente de dirección, se curva como en cayado prolongándose incluso en sentido opuesto al de la principal, sin que llegue a constituir centro nuclea.
Otras morfologías	Resto de variantes morfológicas no contenidas en los apartados anteriores.

Tabla N° 1: Morfología de los puntos característicos en dactilogramas

Figura N° 13: Punto de característicos de la huella dactilar

2.2.2. Biometría dactilar

La biometría dactilar hace referencia al proceso de identificación de una persona por medio de sus huellas digitales; para que las medidas aporten utilidad, los datos biométricos tienen que ser únicos, permanentes y coleccionables, de esta forma, la

información se puede equiparar con una base de datos o contraponer con un registro para comprobar la identidad de una persona.

La biometría dactilar da varios beneficios, sin embargo, entre los más relevantes permanecen la estabilidad y la exactitud que asegura, debido a que un escáner de huellas dactilares te posibilita obtener cerca de 30 aspectos específicos de las huellas en un solo escaneo debido a que no hay 2 personas que compartan bastante más de 8 aspectos peculiares, lo cual convierte a este procedimiento en una forma de validación biométrica bastante fiable, además de ser simple y veloz.

2.2.2.1. Obtención de la huella dactilar

(Aguilar, Sánchez, Toscano, Nakano, & Pérez, 2008) confirman que una vez que se usa un sensor óptico, es casi imposible de que la huella dactilar de una misma persona proporcione exactamente la misma información una vez que se escanea constantemente, esta alteración podría ser causada por diferentes componentes, el sencillo hecho de no poner el dedo en la misma postura causa que la información capturada sea variable, o sea, en algunos casos habrá más información que en otras, aunque se trate del mismo dedo capturado, esta información que no es constante está en los extremos del dedo, debido a que la parte central casi continuamente se sitúa con una determinada presión y por consiguiente, la información se captura de manera correcta.

Para evadir probables errores en el reconocimiento, dicha información en los extremos va a ser eliminada, para lograr garantizar que sólo la información central sea procesada al instante de la sustracción de minucias, en caso de que esta

distorsión no fuera eliminada, el algoritmo podría identificar erróneas minucias; por lo consiguiente, la imagen ha sido recortada en un 10% en todos sus lados considerando que esto no quita información fundamental de la huella dactilar por lo dicho antes.

- **Aclaración**

El propósito de un algoritmo de aclaración es mejorar la claridad de la composición de los bordes en las zonas recuperables y marcar las zonas no-recuperables con demasiado sonido para un siguiente procesamiento, la mayor parte de las técnicas existentes permanecen fundamentadas en la utilización de filtros contextuales cuyos límites están sujetas a la frecuencia y orientación de los bordes locales; estos incluyen continuidad y regularidad de los bordes. Gracias a estas características de la imagen de la huella dactilar las zonas borrosas e interrumpidas tienen la posibilidad de ser recuperadas utilizando información contextual de los vecinos de alrededor. Los filtros tienen la posibilidad de ser definidos en el dominio de Fourier o en el dominio espacial, este aumenta el contraste en una dirección perpendicular a los bordes a medida que ejecuta un alisamiento en la dirección de los bordes. Los filtros de Gabor poseen una propiedad fundamental que se basa en una óptima resolución de frecuencia, las funcionalidades necesarias de conforman una representación bastante intuitiva de las imágenes de la huella dactilar debido a que capturan la periodicidad.

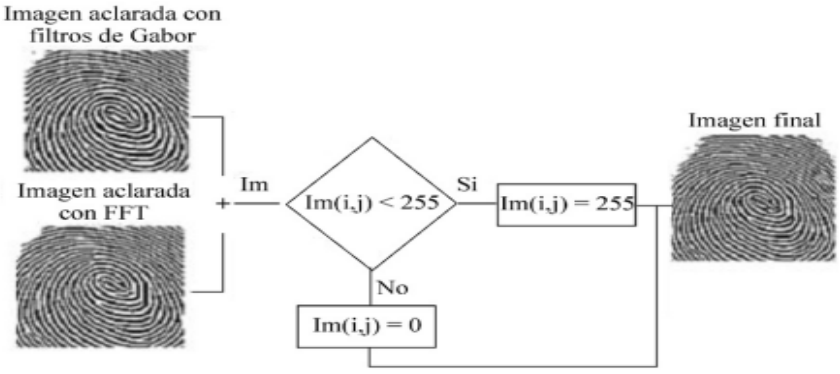


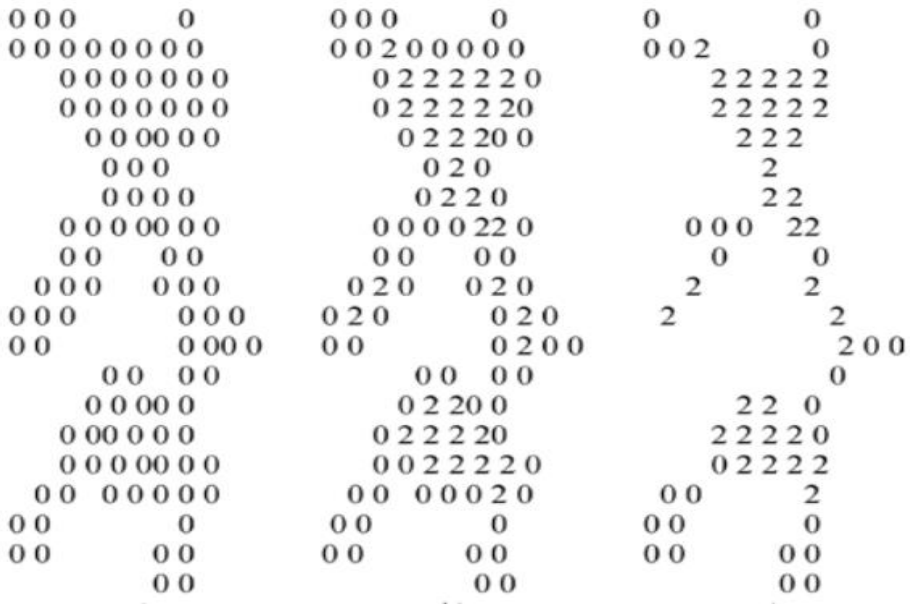
Figura N° 14: Fase de combinación

A poder realizar el proceso de aclaración de Gabor y unirlo con el proceso de aclaración el resultado final será una imagen más nítida y con menos margen de error, ya que en las zonas recuperables será menor.

- **Adelgazamiento**

  Antecedente de la fase de sustracción de minucias, se hace un proceso de adelgazamiento, o sea, se aplica un algoritmo que entrega como consecuencia una imagen con bordes de un píxel de grosor, a partir del proceso de aclaración la imagen es binarizada, o sea, está formada de ceros y unos, donde un “1” significa un píxel blanco y un “0” significa un píxel negro. Un píxel 0 (x,y) es interno, si sus 4 colindantes (x+1,y), (x-1,y), (x,y+1) y (x,y-1) son además 0, un píxel 0 es límite, si no es interno y sólo uno de sus 8 vecinos es 1, un píxel se estima de conexión si al ser eliminado se interrumpe una línea. El algoritmo se basa en descubrir píxeles internos en nuestra imagen y Luego remover los píxeles límite; este proceso es llevado a cabo hasta no descubrir más píxeles internos, posteriormente, se explica con más detalle este proceso.

El primer paso de este algoritmo se apoya en descubrir el total de píxeles internos que hay en nuestra imagen, luego, se eliminan todos los píxeles que son límite, teniendo presente que no se intente un píxel de conexión, este proceso se repite hasta que no existan más píxeles internos, el segundo paso se apoya en hacer una modificación al algoritmo, estos cambios se basan en hallar píxeles internos solamente con 3 vecinos y Luego se eliminan los píxeles límite, como tercera parte la fase de adelgazamiento se apoya en hacer nuevamente una modificación al algoritmo que se apoya en remover píxeles internos; la supresión de un píxel interno se hace una vez que no es viable borrar un píxel límite empero hay todavía píxeles internos.



Fase de inicio *Fase de pixeles internos* *Fase de eliminación de pixeles limites*

Figura N° 15: Fases de adelgazamiento

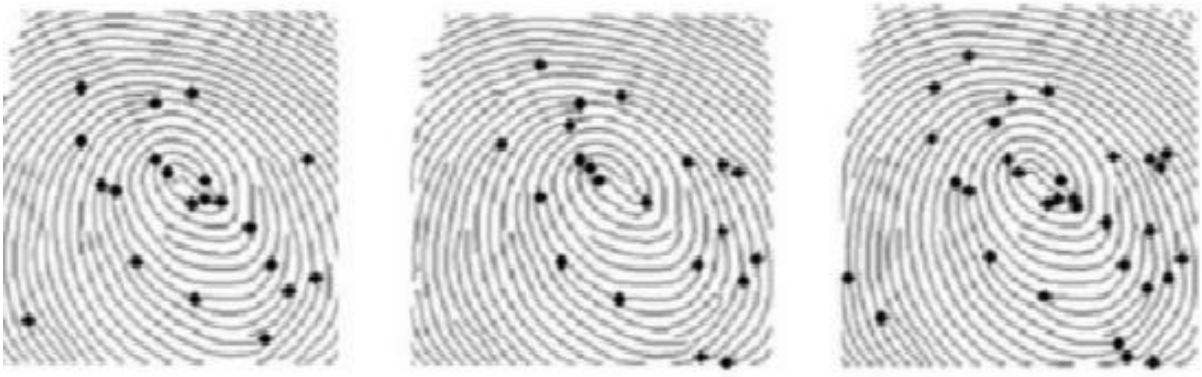
El último paso se basa en remover píxeles internos que poseen sólo 2 vecinos y teniendo cuidado de que no se intente un píxel de conexión.

Fase de adelgazamiento *Huella real adelgazada*

Figura N° 16: Fases de adelgazamiento final

- **Extracción de minucias**

Desde el proceso de adelgazamiento, la imagen está lista para aplicarle el algoritmo de detección de minucias, este algoritmo se basa en calcular el número de píxeles que cruzan el píxel central; es una sucesión ordenada de píxeles que definen el bloque de 8 vecinos del píxel central. Este proceso se hace sobre toda la imagen binaria implementando ventanas de 3x3, en la figura 17 se muestran las minucias localizadas.



Minucias con el método de Gabor | Minucias con el método de FFT | Minucias en combinación de ambos

Figura N° 17: Extracción de minucias

Implementando únicamente filtros de Gabor para poner en claro la imagen, 22 minucias fueron encontradas, una vez que se aplicó únicamente FFT a la imagen, 21 minucias fueron encontradas; pero una vez que se aplicó la mezcla, 32 minucias fueron localizadas; por esta razón se indica combinar ambas fases de aclaración y así evadir que varias minucias sean eliminadas a lo largo del proceso.

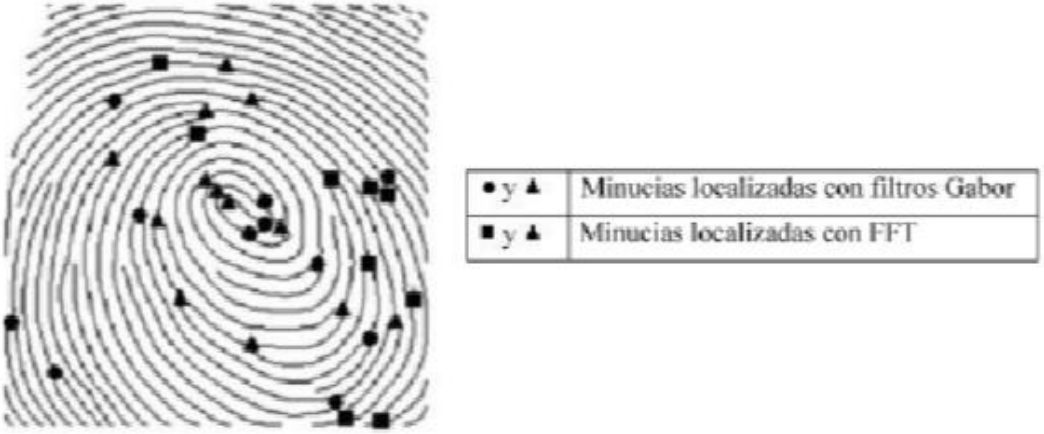


Figura N° 18: Imagen como resultado final de la obtención de minucias

- **Etapa de Reconocimiento**

El reconocimiento se hace con tres relevantes propiedades como lo son las coordenadas, la distancia y el ángulo, se utilizan estas propiedades para lograr tener el mínimo error viable en el reconocimiento, de esta forma, la información que se almacena de la huella dactilar se apoya en una matriz de tamaño 4x500. La matriz está formada de 500 vectores y cada vector de 4 valores que consisten de ambas coordenadas de la primera minucia, la distancia a la siguiente minucia y el ángulo de la primera minucia con respecto al eje Y; por consiguiente, la magnitud total de nuestra matriz almacenada es de 1000x500 ósea 5 huellas por persona y 50 personas diferentes.

El proceso de reconocimiento es llevado a cabo de la siguiente forma la imagen de acceso se convierte en una matriz de 4x500 y esta matriz es comparada con todas las almacenadas en la base de datos; primero, se encuentran los vectores con distancia equivalentes y se toman sólo los que poseen el mismo ángulo, luego, se descartan los vectores que poseen coordenadas bastante diferentes y así tenemos la posibilidad de garantizar un mejor reconocimiento, luego de algunas pruebas, escogió que las coordenadas tienen la posibilidad de alterar en un radio de 10 píxeles; con un umbral más grande de 15 se recibe un óptimo reconocimiento, o sea, que una imagen de ingreso va a ser conocida sólo una vez que su matriz contenga bastante más de 15 vectores equivalentes a alguna de las imágenes almacenadas en nuestra base de datos.

La imagen de ingreso es transformada en una matriz de 4x500 y luego es comparada con cada una de las matrices almacenadas, si en una matriz almacenada hay bastante más de 15 vectores equivalentes a los de acceso, la imagen es conocida.

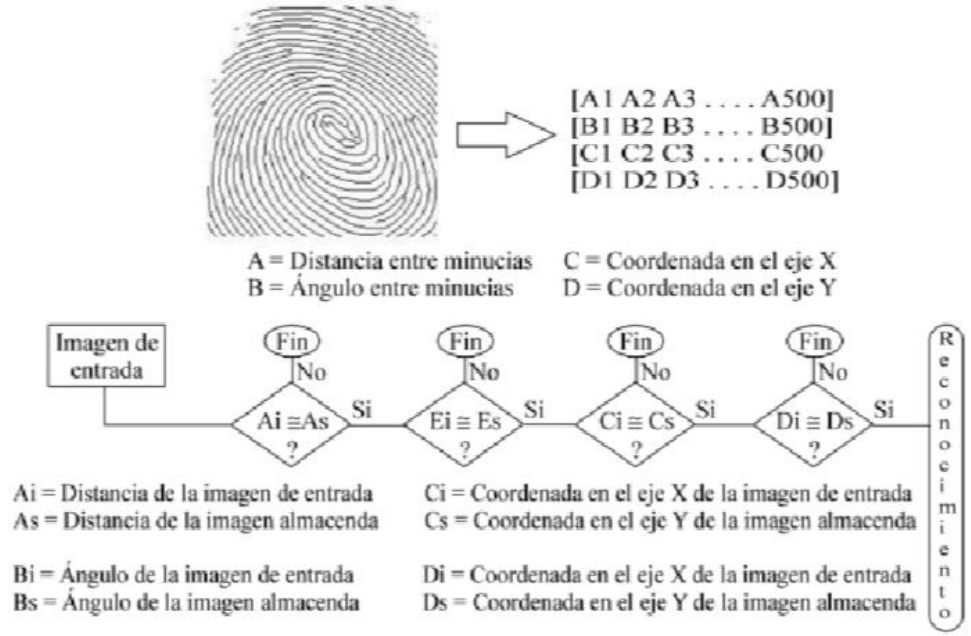


Figura N° 19: Proceso de reconocimiento

2.3. Implementación

2.3.1. Tipos de lectores biométricos de huella

	Modelo	Característica	especificaciones	Costo
		❖ Diseño compacto, ideal para instalar en marcos de puerta o espacios reducidos. ❖ Excelente costo/beneficio ❖ Incorpora lector 125 kHz EM. ❖ Dispositivo robusto de fácil instalación y configuración	❖ Capacidad de Huellas **1,000** ❖ Capacidad de Registros **50,000** ❖ Comunicaciones **TCP/IP, RS485, Mini USB** ❖ Entrada/Salida **Wiegand 26**	

	**Anviz T5**	❖ Capacidad para hasta 1,000 huellas y 50000 registros ❖ Procesador de alta velocidad. ❖ Comunicaciones RS485, Wiegand 26, USB y TCP/IP ❖ Salida de relevador de contacto seco, sensor de puerta abierta y entrada de botón de salida ❖ Software Anviz Crosschex integrado. **Aplicación Anviz Cloud no disponible para Latinoamérica** ❖ **Fuente de alimentación no incluida**	❖ Modo de identificación **Huella, Tarjeta, Huella + Tarjeta** ❖ Software **Anviz Crosschex Lite (Integrado). Aplicación Anviz Cloud no disponible para México.** ❖ CPU **CPU de alta velocidad de 32 bits** ❖ Sensor **AFOS** ❖ Área de escaneo de **huella 22 x 18 mm** ❖ Resolución **500 dpi** ❖ Lector RFID **Estándar EM 125 kHz** ❖ Dimensiones (Ancho x Alto x Profundidad) **50x124x34.5mm (1.97x4.9x1.36")** ❖ Temperatura **-30°C a 60°C** ❖ Alimentación **12 V DC** ❖ Modelos **Con lector RFID 13.56 Mhz (I06388) o lector RFID 125 kHz EM (I06389)**	**$ 150,^{00}**
		❖ El nuevo procesador de 1 Ghz basado en Linux garantiza un tiempo de comparación de 1:3000 inferior a 0,5 segundos ❖ La función WiFi garantiza el encendido para trabajar y realizar la instalación flexible del dispositivo. ❖ El sensor activo táctil garantiza una respuesta rápida para cada detección	❖ Capacidad Huellas 3.000, Tarjetas 3.000, Registros 50.000. ❖ Interfaz de comunicación TCP/IP, RS485, Mini USB, (Opcional) Wi-Fi ❖ Modos de Identificación Huella, Contraseña, Tarjeta (EM opcional, Módulo Mifare) ❖ Distancia de lectura de tarjeta 1~5cm (125kHz), >2CM (13,56MHz)	

	**Anviz EP30**	y ahorra el consumo total de energía del dispositivo. ❖ La pantalla LCD colorida garantiza la mejor interacción y experiencia de usuario y también puede proporcionar notificaciones claras a los usuarios. ❖ El gran teclado físico garantiza las mejores experiencias de usuario y es fácil de usar para todas las personas en todo el mundo. ❖ El servidor web garantiza la conexión fácil y rápida y la autogestión del dispositivo.	❖ Salida Wiegand, Salida Relé, Sensor de Puerta, Botón de Salida, Timbre de Puerta ❖ Velocidad de Identificación < 0,5s ❖ Tarjeta RFID (Opcional) EM, (Opcional) Mifare ❖ Temperatura de Funcionamiento -25°C~70°C ❖ Humedad De 10% a 90% ❖ Alimentación DC12V ❖ WebServer Sí	**$ 145,21**
		❖ Protección IP65, Resistente y de Mayor Durabilidad. ❖ Cubierta Métalica Anti-Vandalismo para Instalación en Exteriores. ❖ Rápido y Preciso Algoritmo de Huella Digital. ❖ Capacidad para 1,500 Huellas 10,000 Tarjetas y 100,000 Registros. ❖ Fácil Instalación y Conectividad. ❖ Entrada y Salida Wiegand.	❖ Capacidad de Eventos 100.000 ❖ Capacidad de Tarjetas 10.000 ❖ Comunicación RS485, TCP/IP, USB-Host ❖ Interfaz de Control de Acceso Cerradura Eléctrica, Sensor de Puerta, Botón de Salida, Salida de Alarma ❖ Wiegand Entrada y Salida	

	**Zkteco Ma300**	❖ Interfaz TCP/IP y RS485. ❖ Avanzadas Funciones de Control de Acceso. ❖ Interfaz TCP/IP y RS485. ❖ Lector de Huellas Digitales y Tarjetas RFID para Verificación Combinada.	❖ Funciones Opcionales MIFARE ❖ Funciones Estándar Acceso por Horarios, Anti-passback, Teclado externo USB ❖ Fuente de Alimentación 12V DC ❖ Índice de Protección IP65 ❖ Temperatura de Operación 10°C a 60°C ❖ Humedad de Operación 10% - 90% ❖ Dimensiones 73 x 148 x 34.5 mm ❖ Plataforma de Hardware ZEM720 ❖ Versión de Algoritmo ZKFinger VX10.0	**$ 120,^{00}**
	**ZKTeco LX50**	❖ Terminal Biométrica de Huella Digital ❖ Pantalla TFT Color de 2.8 Pulgadas ❖ Capacidad de 500 huellas ❖ Capacidad de 50,000 registros de checadas ❖ Comunicación USB-Host/Cliente	❖ Versión de Algoritmo ZKFinger VX 10.0 ❖ Capacidad e Usuarios 500 ❖ Capacidad de Huellas 500 ❖ Capacidad de Eventos 50.000 ❖ Comunicación USB-Host/Cliente ❖ Funciones Estándar Timbre Programado, SSR, ID de 9 Dígitos,	**$100,^{00}**

			❖ Entrada T9, Múltiples idiomas Timbre Programado, SSR, ID de 9 Dígitos, Entrada T9, Múltiples idiomas ❖ Dimensiones 180 x 132 x 32 mm	
	**ZKTeco F18 MF**	❖ Pantalla a color ❖ Fácil Instalación y conectividad ❖ Diseño delgado y elegante ❖ Características completas de Control de Acceso ❖ Nueva plataforma ❖ Nuevo firmware	❖ Pantalla a color TFT-LCD de 2.4 pulgadas ❖ Capacidad de Huellas Digitales 3.000 Plantillas ❖ Capacidad de Tarjetas 5.000 (Opcional) ID/ MIFARE/ HID ❖ Capacidad de Eventos 30.000 ❖ ZK Optical Sensor ❖ Versión de Algoritmo ZK Finger V9.0&10.0 ❖ Comunicación TCP/IP, RS232/485, USB-Host ❖ Interfaz de Control de Acceso Cerradura Eléctrica, Sensor de Puerta, Botón de Salida, Alarma, Timbre ❖ Wiegand Entrada, Salida y SRB ❖ Funciones Estándar Horario de Verano, Consulta de Registros, Anti-Passback, Lector de Huella Digital Externo	**$ 255,^{00}**

			por RS485, Impresora (Opcional) ❖ Fuente de Alimentación 12V DC, 3A ❖ Temperatura de Operación 0°C hasta 45°C ❖ Humedad de Operación 20% hasta 80% ❖ Dimensiones 80 x 183 x 42 mm	

Tabla N° 2: Tipo de controles de acceso

2.3.2. Controlador seleccionado

Después de observar y analizar los tipos de controladores de acceso que creímos conveniente, emos estimado que el controlador **Zkteco Ma300** que resulta ser mas factible ya sea por sus características o las especificaciones y por su costo; además lo mas importante sus funciones ya que este permite albergar una gran cantidad de huella, de tarjeta y la gran cantidad de eventos que este tiene, son de gran utilidad para lo operacionalización a realizar en este proyecto.

Figura N° 20: Controlador Zkteco Ma300

MA300 es un innovador lector biométrico de huella digital para aplicaciones de control de ingreso el cual adopta el avanzado algoritmo de ZK para dar fiabilidad, exactitud y inmediata rapidez de verificación, su cubierta metálica y custodia IP65 lo elaboran resistente al agua, polvo y males externos; el MA300 da flexibilidad para ser instalado de forma autónoma o con paneles de control de ingreso que toleren formato Wiegand de 26 bits; los usuarios podrían ser registrados por medio de una tarjeta de administrador una vez que el dispositivo funciona en modo autosuficiente. Cuenta con interfaz TCP/IP y RS485 para una simple conexión y escalabilidad, este dispositivo va a regular las entradas y salidas a las distintas aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone, además de obtener una mayor seguridad en las mismas, a pesar de que existen otros

dispositivos de acceso de menor valor, pero contaban con menor capacidades y eran de menor calidad.

2.3.3. Metodología de implementación

2.3.3.1. Método bibliográfico

Mediante la obtención bibliográfica se pudo obtener una basta información la cual esta relacionada con el proyecto esta fue de gran ayuda ya que permitió la resolución del mismo.

2.3.3.2. Ficha de observación

Mediante la observación se pudo determinar el área donde se implementará el sistema de control de acceso biométrico, además se analizó las falencias y problemáticas que mantienen las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí.

Área de observación donde el equipo se implementará	
ASPECTOS	**OBSERVACIONES**
Área en el cual se implementará el sistema biométrico.	Se implementará en las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión.
Falencias que presentan las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión.	Estas se encuentran de una forma común o que se utilizaban anteriormente, las puertas de

	madera y los cerrojos que estas tienen ya son prácticamente inseguros.
Como llevaban el control de acceso a las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión anteriormente.	Este se realizaba de manera clásica o en papel donde se determinaba un horario y el docente y la hora que este impartía su clase, pero existen espacios en blanco donde son utilizados por tercero y tienen acceso sin supervisión o conocimiento alguno de su presencia en el lugar
Identificar el sector estratégico para la ubicación del dispositivo biométrico	El dispositivo de control de acceso ira a un costado de la puerta incorporado a la pared.
Funcionamiento del dispositivo de control de acceso a las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí	Este fue un éxito ya que su funcionamiento, comunicación entre switch y el computador a la base de dato resulta ser optima y su control de acceso solo permite personal autorizado

Tabla N° 3: Modelo de la ficha de observación aplicada

2.4. Aplicación propuesta

2.4.1. Estructura propuesta del sistema de control de acceso biométrico

El sistema de control de acceso ya viene incorporado con un case metálico el cual le ayuda a soportar el clima como lo son la lluvia, el polvo, el viento, etc. Este sistema de control de acceso biométrico será ilustrado en la siguiente figura.

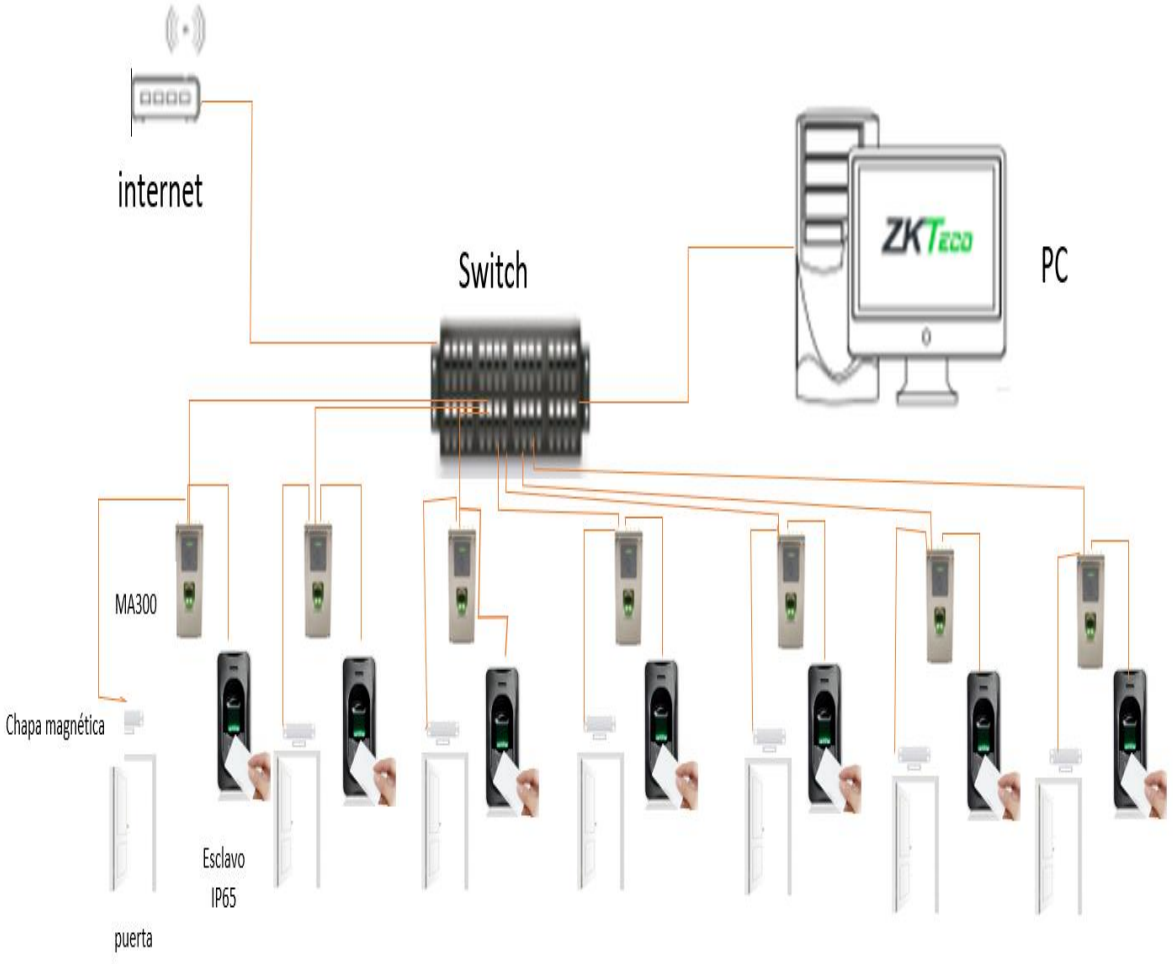


Figura N° 21: Diagrama de instalación

2.4.2. Proceso de instalación de las puertas de acceso biométrico Zkteco Ma300.

1) Se instalará el control de acceso biométrico Zkteco Ma300 postrado a la pared, a un costado de la puerta de manera que esta quede fijada y asegurada de manera segura.

Figura N° 22: Instalador biométrico postrado en la pared

2) Se instalará una puerta personaliza de vidrio templado con logos de la institución para dar un mejor relieve y contraste, aparte constará con un soporte metálico y una agarradera de igual manera.

Figura N° 23: Puerta de vidrio templado con agarradera y soporte metálicos

3) Instalación de canaletas las cuales ayudaran a ocultar el cableado que conectara el switch y el computador.

Figura N° 24: Canaleta de recubrimiento para los cables de conectores a el computador y el switch

4) Ya configurado el control de acceso y el computador se comprobó el funcionamiento total del sistema, sin olvidar la conexión a internet por medio de wifi.

Figura N° 25: Supervisión y control del sistema biométrico desde el computador

2.5. Diseño de la propuesta

Figura N° 26: Esquema de infraestructura

3. Conclusiones y recomendaciones

3.1. Conclusiones generales

Las variantes que se mostró en el proyecto, apoyo al progreso de las posiciones teóricas, de estas se obtuvieron subvariables que permitió la indagación de diferentes fuentes bibliográficas fundamentadas en la implementación y utilización de un sistema de control de acceso biométrico, las variantes que se separaron son Tecnología de la Información y Comunicación y Sistema Biométrico. Este sistema de control de acceso biométrico en ayuda de la Tecnología de la Información y Comunicación permitió el óptimo manejo ingreso a las aulas del bloque Bplanta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone, además de permitir una mejor seguridad en la misma.

Por medio de un diagnóstico usando instrumento de recolección de datos como la ficha de observación, se permitió decidir los requerimientos que las aulas del bloque B planta baja requieren como materiales a usar y conocer los puntos de vista donde se implementara el sistema de control de acceso, constatando de manera exacta el lugar donde se instalara el controlador biométrico.

El diseño del sistema de control de acceso biométrico en las aulas del bloque B planta baja de la Universidad Laica Eloy Alfaro de Manabí extensión Chone ha sido de mucha ayuda, debido a que permitió tener una visión relacionando los elementos de la seguridad y el control anterior a su instalación, este diseño además de que fue útil como base para enseñar los resultados pasados, además ayudo a enseñar los

errores que este tuvo, como un control de acceso a las aulas y la seguridad de las mismas.

3.2. Recomendaciones

Se recomienda que para conocer la profundidad sobre determinados campos de estudios, se debería realizar una investigación sistemática partiendo de las variaciones que el proyecto presente, para eso; en la investigación bibliográfica se debería conocer cuáles son las variantes que muestra el proyecto, una vez definidas, se debería descomponer todas ellas para establecer las subvariables, y poder crear una indagación sistemática correcta; además de que la utilización de las TIC en un sistema de control de acceso biométrico da un enorme desempeño óptimo por lo cual ayuda a mejorar la seguridad y control de acceso en las aulas.

Si es necesario realizar una instalación de control de acceso biométrico, la utilización de una herramienta de recolección de datos como lo es la ficha de observación va a ser importante para el desarrollo del mismo; la ficha de observación debería estar enfocada en el sector en el que se laborará, esto dejará conocer los aspectos que muestran ciertas falencias, tal cual ayudará al progreso de la instalación de un sistema de control de acceso biométrico.

Por último se recomienda que para lograr conocer el resultado final que va a tener la implementación del sistema de control de acceso biométrico se necesita diseñar un esquema del área en el cual se realizará dicho trabajo, esto dejará conocer con más visión los elementos que el sistema va a contener, este bosquejo ayuda al progreso proporcionando apoyo a lo largo del proceso de la instalación previniendo

cualquier error a lo largo de la preparación, ayudando a saber en dónde permanecen el controlador, la red de cableado de interacción que esta tienen con el Smith y el computador, etc.

4. Bibliografía

Aguilar, G., Sánchez, G., Toscano, K., Nakano, M., & Pérez, H. (2008). *Reconocimiento de huellas dactilares usando características locales.* Mexico: Instituto Politécnico Nacional.

Carrasco, M., Portugal, R., & Peralta, B. (2006). *Reconocimiento biométrico de audio y rostro: Un sistema viable de identificación* . Santiago de Chile, Chile: Pontificia Universidad Católica de Chile.

Consentino, L. (2014). Control de Accesos Unidades de Control o Controladores. *RNDS*, 1-4.

Cruz Chávez, M. A. (2011). *Base de datos, conceptos y sus características.* Cuernavaca, Morelos, Mexico: Universidad Autónoma del Estado de Morelos.

De Antón y Barberá, F. (2011). *Reflexión acerca de las minutiae vs punto caracteristicos e incidencia en su aplicación lofoscópica práctica.* Gaceta internacional de ciencias forences.

Escobar, J. A. (2010). Sistema de Seguridad Basado en Biometria . *Sciencia Et Techinica*, 6.

Española, D. d. (2021). *Real Academia Española*. Obtenido de https://dle.rae.es/biometr%C3%ADa?m=form

Espinoza Olguín, D. E., & Jorquera Guillen, P. I. (2015). *Reconocimiento Facia.* Valparaíso, Chile: PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO.

Etchart, G., Luna, L., Leal, C., & Alvez , M. (2011). *Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales* . Concepción del Uruguay, Entre Ríos, Argentina: Universidad Nacional de Entre Ríos.

García Cueva, M. A., & Yunga Ochoa, J. R. (2010). *Sistema Biométrico de Reconocimiento de Voz para el registro de asistencia del Personal en el Centro de Investigaciones (CATER).* Loja-Ecuador: Universidad Nacional de Loja.

García Donday, F. (2014). *Mejora de los algoritmos de reconocimiento de huellas dactilares en entorno forenses.* Madrid, España: Universidad Autonoma de Madrid.

Garcias, F., & Hidalgo, H. (2017). *Implementación del sistema biometrico para el control de asistencia admnistrativa de la Universidad Privada de Pucallp S:A:C2017.* Peru: Universidad Privada de Pucallpa. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/3430/VargasGarciaCristianGerman2016.pdf;jsessionid=529E4CB08A499732B3045C9525A784DE?sequence=1

Gómez Vieites, Á. (2011). *Seguridad en Equipos Informáticos (MF0486_3).* España: Grupo Editorial RA-MA.

Gonzáles, J. C., Contreras, W., Yañez, C., & Próc, L. (2009). Tecnologías biométricas aplicadas a la seguridad en las organizaciones. *Revista de Ingeniería en Sistemas e informática,* 1-12.

Granda Carrillo, M. A. (2013). *Sistema de reconocimiento Bioimétrico mediante firma manuscrito on-line 3D.* Madrid, España: Universidad Carlos III de Madrid.

Gutiérrez Díaz, A. (2005). *Bases de datos.* Ciudad de México, México: Centro Cultural Itaca S.C.

Hernández, R. G. (2010). *Estudio de técnicas de reconocimiento facial.* Barcelona, España: Universidad Politécnica de Cataluña .

Hidalgo Jacome, V. A. (2010). *Implementación de un sistema de autenticación, biometrica basado en huella digitales.* Riobamba: Escuela Superior Politecnica de Chimborazo.

Juanes, G. (2018). *Huellas dactilares.* mexico.

Madrigal González, C. A., Ramírez Madrigal, J. L., Hoyos Arbeláez, J. C., & Fernández, D. S. (2009). Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares. *Facultad de Ingeniería Universidad de Antoquia*, 21 - 32.

Mendaza Ormaza, A., Hurtado, O., Sánchez Reillo, R., Valverde Albacete, F., & Peláez Moreno, C. (2010). *Estudio de un sistema de reconocimiento biométrico mediante firma manuscrita online basado en SVM usando Análisis Formal de Conceptos.* Madri, España: Universidad Carlos III de Madrid.

Menendez, H., & Muñoz, C. (noviembre de 2016). *Sistema biométrico para automatizar el registro de asistencia docente en la Unidad Educativa ITSI Del Cantón Chone.* Calceta: Escuela Superior Politécnica Agropecuaria De Manabí Manuel Félix López (Tesis). Obtenido de http://repositorio.espam.edu.ec/bitstream/42000/318/1/TC96.pdf

Montaña Duque, D. F. (2017). *Sistema de identificación mediante huella digital para el control de acceso a la Universidad Libre Sede Bosque Popular simulado en un entorno web.* BOGOTÁ D.C.: Universidad Libre Sede Bosque Popular.

Ortiz, D. (2019). Capacitación & Excelencia. *Ciencia Digital*, 2 - 6. Obtenido de https://cienciadigital.org/revistacienciadigital2/index.php/CienciaDigital/article/view/598

Rojas Portilla, A., & Suárez Rueda, J. (2018). La huella dactilar como mecanismo de identificación biométrica para la no portabilidad de documentos de identidad. 38-45.

Romero Aguirre, E., & Oviedo Chima, I. D. (2020). *SISTEMA DE CONTROL BIOMETRICO PARA EL ACCESO DE ESTUDIANTES AL PLANTEL Y A LOS LABORATORIOS INTERNOS DE LA INSTITUCIÓN EDUCATIVA EL NACIONAL*. Monteria Córdoba: Universisdad de Córdoba.

Ruiz Marín, M., Rodriguez Uribe, J., & Olivares Morales, J. (abril de 2009). Una mirada a la biometria. *Revista Avances en Sistemas e Informática*, 29-38.

Ruiz, M., & Mora, J. (2009). Una mirada a la biometria A glance to the biometric. *Avances en sistema e informaticas*, 29-38.

Sánchez, F., Urribarri, D., & Castro, S. (2019). *Técnicas biométricas: análisis de las técnicas actuales y nuevas tendencias.* Comodoro Rivadavia, Argentina: Universidad Nacional de la Patagonia San Juan Bosco.

Tomé González, P. (2008). *Reconocimiento automático de patrones de iris.* Madrid, España: Universidad Autónama de Madrid.

Vargas Vergara, Z. V. (2013). *Sistema de control de acceso y monitoreo con la tegnología RFID para el departamento de sistema de la Universidad Politécnica Salesiana sede Guayaquil.* Guayaquil, Ecuador: Universidad Politécnica Salesiana.

Vargas, C. (2016). *Diseño e implementación de un prototipo para el control de acceso en la sede de ingenería de laUniversidad Distrital Francisco José de Caldas mediante el uso de torneques controlados por carnet con tecnologia NFC y lector biometríco de huella dactilar.* Bogotá: Universidad Distrital Francisco José de Caldas. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/3430/VargasGarciaCristianGerman2016.pdf;jsessionid=529E4CB08A499732B3045C9525A784DE?sequence=1

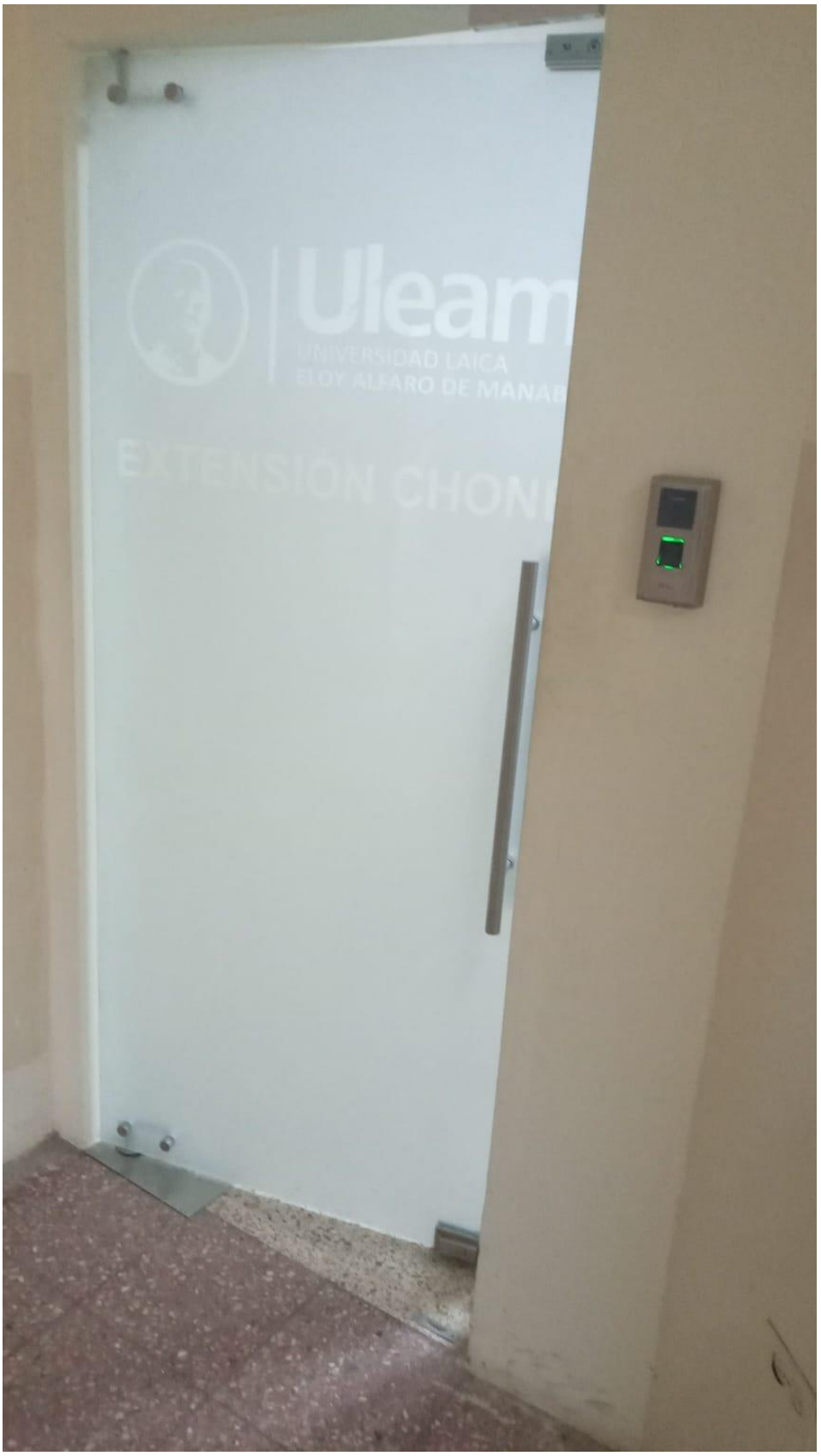
Vázquez López , M. Á. (2014). *Sistema de reconocimiento facial mediante técnicas de visión tridimensional.* Guanajuato: Centro de investigaciones en optica, A.C.

Vega Briceño, E. (2021). *Seguridad de la información.* 3Ciencias.

Villalobos Castaldi , F. M. (2011). *Uso de la red vascular de la retina como medio Biométrico de identificación.* Ciudad de México, México: Instituto Politécnico Nacional.

Yamith, V., & Mario, V. (2012). *Desarrollo del sistema control biométrico de docentes de la Universidad Central del Ecuador.* Quito: Universidad Central del Ecuador. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/220/1/T-UCE-0011-10.pdf

5. Anexo


Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANAB
EXTENSION CHON