UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ESTADO DEL ARTE DE REGISTROS BIOMÉTRICOS ESTÁTICOS USADOS PARA AUTENTICAR LA IDENTIDAD DE UNA PERSONA

Trabajo de titulación previo a la obtención del

Título de Ingeniera de Sistemas

AUTORA: Alisson Estefanía Gutiérrez Yánez

TUTOR: José Luis Aguayo Morales

Quito – Ecuador

2022

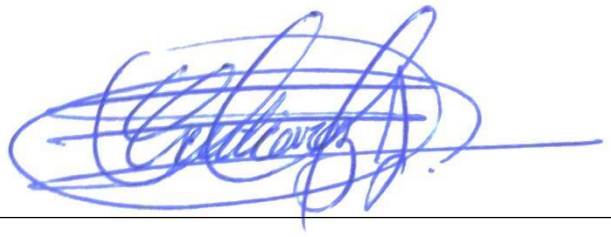
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN.

Yo, Alisson Estefanía Gutiérrez Yánez con documento de identificación N° 1726620261, manifiesto que:

Soy la autora y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 07 de marzo del año 2022.

Atentamente,



Alisson Estefanía Gutiérrez Yánez

1726620261

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA.

Yo, Alisson Estefanía Gutiérrez Yánez con documento de identificación N° 1726620261, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del Artículo Académico: "Estado Del Arte De Registros Biométricos Estáticos Usados Para Autenticar La Identidad De Una Persona", el cual ha sido desarrollado para optar por el título de: Ingeniera de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 07 de marzo del año 2022.

Atentamente,

Alisson Estefanía Gutiérrez Yánez

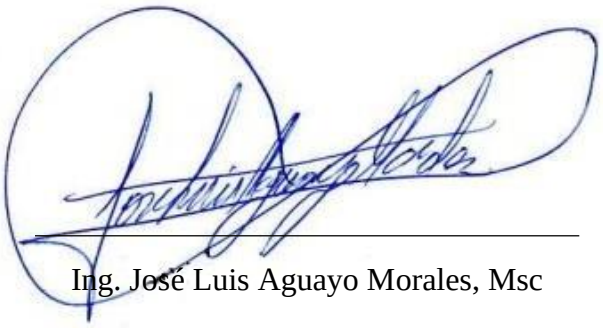
1726620261

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN.

Yo, José Luis Aguayo Morales con documento de identificación N° 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ESTADO DEL ARTE DE REGISTROS BIOMÉTRICOS ESTÁTICOS USADOS PARA AUTENTICAR LA IDENTIDAD DE UNA PERSONA, realizado por
Alisson Estefanía Gutiérrez Yánez, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 07 de marzo del año 2022.

Atentamente,



Ing. José Luis Aguayo Morales, Msc

1709562597

AGRADECIMIENTOS

Agradezco a mi madre bella por darme todo lo que siempre estuvo a su alcance, haciendo más allá de lo posible, por su esfuerzo al nunca darse por vencida para que yo tenga mi oportunidad de cumplir mi sueño, ser una profesional. Por cada uno de sus consejos “Estudia y prepárate, es la única manera de ser una mujer de bien y depender de ti misma siempre”. Como hija espero nunca defraudarle, que seas infinita madre mía.

A mi familia por brindarme al menos su apoyo moral, a mi padre y hermano por extenderme su mano cuando lo necesité.

Quiero agradecerme por no darme por vencida, por creer en mí, por no defraudar el esfuerzo de mi mami bella, por trabajar en ser incluso una mejor persona, por haber superado toda prueba que en su momento pensé que era lo peor, al ser como soy.

A mi tutor el Ing. Aguayo José Luis, tutor de mi tesis por dirigirme de la mejor manera en el desarrollo de mi trabajo de titulación, por su paciencia, experiencia, conocimiento y sobre todo por su calidad de persona que siempre ha sido. Una persona con la cuál no solo se puede conversar de temas académicos sino personales con risas y consejos.

A mis amigos los que forme en mi etapa universitaria y por cada uno de los recuerdos que me llevo de esta maravillosa etapa, ya que me enseñaron que cuando se escoge a los correctos te ayudan a superarte en el transcurso y no darte por vencido.

A la vida que me enseño apreciar y valorar lo simple, aquellas cosas que daba por hecho.

¡Finalmente, y no menos importante a Dios por sus promesas y su tiempo… es perfecto!

ESTADO DEL ARTE DE REGISTROS BIOMÉTRICOS ESTÁTICOS USADOS PARA AUTENTICAR LA IDENTIDAD DE UNA PERSONA.

STATE OF THE ART OF STATIC BIOMETRIC RECORDS USED TO AUTHENTICATE THE IDENTITY OF A PERSON.

Alisson Estefanía Gutiérrez Yánez [1], José Luis Aguayo Morales [2]

Resumen

El presente artículo académico investiga el estado del arte de registros biométricos estáticos usados para la autenticación de la identidad de la persona. En la actualidad los métodos de reconocimiento: facial, iris, nudillos, huellas dactilares y venas dactilares, centran su estudio en diferentes estrategias de segmentación para lograr una mayor precisión de coincidencia, lo que no es suficiente ante los crecientes desafíos de ataques que sufren cada uno de ellos. Es necesario investigar nuevos algoritmos que pretendan hacer sistemas de autenticación más robustos. Usando la metodología de mapeo sistemático y la revisión de la literatura se encontraron varias alternativas para el reconocimiento del individuo. La biometría ocular y dactilar son las más prometedoras por la aceptación del usuario, ya que son menos invasivas al momento de tomar la muestra, con un mejor comportamiento mejorando notablemente su resultado. La biometría de venas dactilares mostró mediante el QDA (Análisis de la discriminante cuadrática) un 98.7% de precisión y la biometría ocular reveló un 94% de efectividad.

Palabras Clave: Mapeo Sistemático, biométricos estáticos, algoritmos, autenticación.

Abstract

This academic paper investigates the state of the art of static biometric records used for the authentication of a person's identity. At present, recognition methods: facial, iris, knuckles, fingerprints and finger veins, focus their study on different segmentation strategies to achieve greater accuracy of coincidence, which is not enough in the face of the growing challenges of attacks suffered by each of them. New algorithms that aim to make authentication systems more robust need to be investigated. Using systematic mapping methodology and literature review, several alternatives for accurate person recognition were found. Ocular and fingerprint biometrics are the most promising due to user acceptance, since they are less invasive at the time of sampling, with a better behavior and significantly improved results. Finger vein biometrics showed 98.7% accuracy through QDA (Quadratic discriminant analysis) and ocular biometrics revealed 94% effectiveness.

Keywords: Systematic mapping, static biometrics, algorithms, authentication.

[1]Estudiante de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Egresado – Universidad Politécnica Salesiana – sede Quito – Campus Sur, Autor para correspondencia: agutierrezy@est.ups.edu.ec

[2]Ingeniero en Electrónica y Telecomunicaciones, Docente de la Carrera de Ingeniería de Sistemas – Universidad politécnica Salesiana – sede Quito – Campus Sur, Autor para correspondencia: jaguayo@ups.edu.ec

1. Introducción

Los registros biométricos estáticos son el resultado del procesamiento de los datos mediante métodos automáticos que analizan características del ADN (Ácido desoxirribonucleico) humano con el fin de autentificar a determinado individuo, centrando su estudio en la segmentación de características comunes y específicas, logrando una mayor precisión de coincidencia [1].

Los datos personales son procesados bajo principios como; el consentimiento, propósito definido, para brindar acceso al individuo que los posee y restricciones en la transferencia. Deberán tenerse en cuenta que al almacenar la información ninguna tercera persona pueda identificar a quien pertenece los datos utilizando medios razonables, por lo tanto, los datos perderían su característica de dato personal [2].

La verificación implica confirmar o denegar la identidad que una persona dice poseer. Por otro lado, cuando se trabaja en un modo de identificación, el sistema debe reconocer a esa persona si está registrada en una base de datos que guarda la identidad sus usuarios [3].

Este tipo de tecnologías biométricas aplicadas a la seguridad, resulta de vital importancia el evaluar previamente las ventajas e inconvenientes, así como tener en cuenta posibles sistemas o soluciones alternativas que puedan suponer una menor intrusión contra los interesados [1].

A continuación, se detalla el funcionamiento de cada uno de los registros biométricos estáticos usados para autenticar la identidad de la persona.

1.1. Reconocimiento Facial

La Biometría Facial comprende el análisis por medio de un algoritmo que codifica los modelos, formas y proporciones de sus rasgos, además de contornos faciales, estableciendo claves y niveles de seguridad, teniendo en cuenta: envejecimiento, cirugías plásticas, consumo de alguna sustancia (drogas, tabaco, alcohol) o el uso de cosméticos [4].

En la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula, convierte estas medidas en un código numérico [1], como se muestra en la Figura 1.

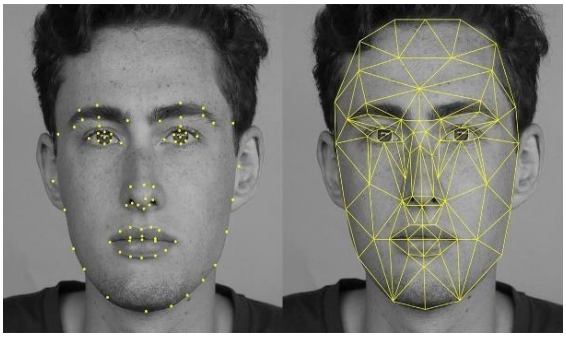
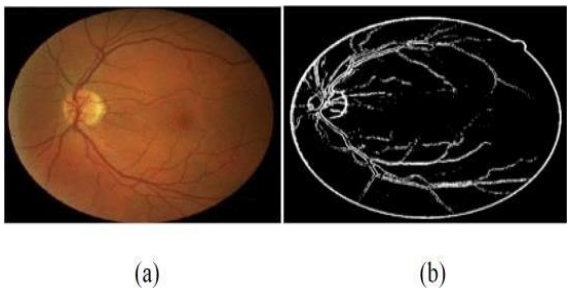


Figura 1. Reconocimiento Facial, claves y niveles de seguridad [1].

1.2. Reconocimiento del Iris

La Biometría del Iris comprende el análisis de la membrana circular, donde se aloja la pupila cuya dilatación y contracción sirven para verificar si la persona se encuentra viva o es real [5]. Es importante señalar que no existe ningún riesgo para la salud, ya que, al obtenerse la muestra mediante una cámara de infrarrojos, no hay peligro de que el ojo resulte dañado en el proceso [1].

El hecho de que el ojo humano derecho e izquierdo de cada persona sean diferentes, se puede afirmar que la biometría es segura, dado que no es fácil cambiar o replicar la vasculatura de la retina [6], detallando la imagen original vs. La segmentación de los vasos sanguíneos como se muestra en la Figura 2.



(a) (b)

Figura 2. (a) Imagen original (b) segmentación de vasos sanguíneos [6].

1.3. Reconocimiento de Nudillos basados en el dedo menor.

El patrón de nudillos es la única o principal fuente de información disponible para determinar actual y científicamente la identidad de los individuos en el campo forense; además, la biometría de nudillos basa su análisis en el estudio el dedo menor, los patrones de nudillos que se forman en la superficie donde se unen los huesos distales de falange y falange media [7].

Las imágenes dorsales identifican; la variación, longitud de los dedos, ancho de los dedos, uñas, pigmentación de la piel y la ubicación de los puntos DIP (interfalángico distal) en el nudillo menor y PIP (interfalángico proximal) en el nudillo mayor, este método plantea explotar cualquier característica anatómica de los dedos para segmentación robusta de los nudillos de los dedos menores [7], como se muestra en la Figura 3.

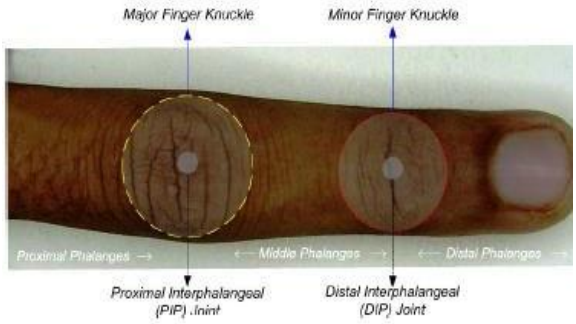


Figura 3. Biometría de Nudillos reconociendo patrones e identificando patrones PIP, DIP [7].

1.4. Reconocimiento de Huellas Dactilares

La Biometría Dactilar basa su análisis en la estructura de crestas y valles en las yemas de los dedos sobre la epidermis de cada individuo, así como las minucias, que son invariables en el tiempo [8].

Las minucias de los extractos de huellas dactilares son la terminación y la bifurcación, donde la terminación depende del punto final inmediato de una cresta [9], como se detalla en la Figura 4.

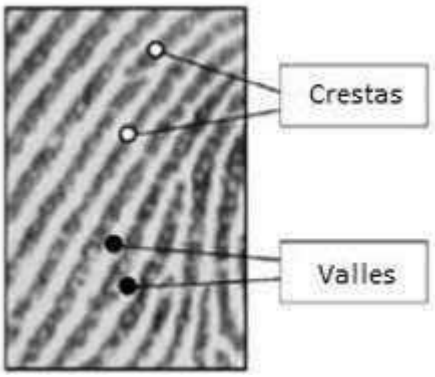


Figura 4. Diferencia entre cresta y Valle. [11]

Las huellas dactilares pueden ser planas o enrolladas. Una impresión plana captura solo una impresión del área central entre la yema del dedo y el primer nudillo, mientras que una impresión enrollada captura las crestas en ambos lados del dedo [10].

1.5. Reconocimiento de Venas Dactilares.

La Biometría de venas dactilares basa su análisis en colocar luz infrarroja para capturar la imagen de un dedo que contiene los patrones de las venas que este a su vez posee varios anchos y brillos que cambian temporalmente como resultado de las fluctuaciones en la cantidad de sangre en la vena, dependiendo de la temperatura y las condiciones físicas [10], detallando la imagen original vs. El patrón de venas extraídas como se muestra en la Figura 5.

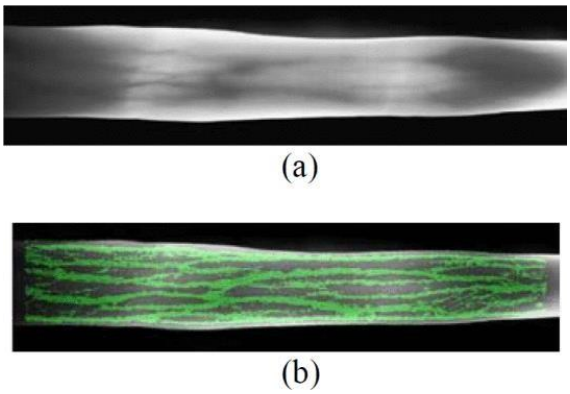


Figura 5. (a) Imagen original (b) patrón de venas extraídas [6].

A continuación, se detalla la metodología, fases y preguntas de investigación para el desarrollo del SMP (Mapeo Sistemático) y SLRP (Revisión de la literatura).

2. Métodos y Materiales

En la presente investigación se utiliza la *metodología prisma* para realizar el mapeo y revisión sistemática de la literatura existente. Contribuye al autor a identificar, reconocer y clasificar las técnicas de autenticación biométrica de la persona, teniendo en cuenta criterios de calidad y disminuyendo los sesgos de selección, dando respuesta a las preguntas de investigación planteadas [12].

Un sesgo falso de muestra legítima consiste en una amenaza, suplantación de identidad donde el individuo hace uso de artefactos producidos sintéticamente como: dedos gomosos, imagen de iris impresa, máscaras faciales [13].

La *metodología prisma* propone las siguientes fases: i) Formular las preguntas de PICOC, ii) Desarrollo de criterios de inclusión y exclusión, iii) Realizar la búsqueda bibliográfica detallada, iv) Citar los trabajos y realizar el resumen científico de la búsqueda.

A. Fase 1

El método PICOC es utilizado para la descripción de elementos de búsqueda de artículos relacionados con las diferentes técnicas de autenticación en la identificación de la persona, como se detalla en la Tabla I.

TABLA I
DESARROLLO DEL MÉTODO PICOC

Population (P): ¿Quién?	Registros biométricos estáticos.
Intervention (I): ¿Qué? ¿Cómo?	Técnicas de análisis que autentiquen la identidad de una persona.
Comparision (C): ¿Con qué comparar?	Estudios que presenten técnicas que verifican la identidad de la persona.
Outcomes (O): ¿Qué se busca conseguir o comparar?	Identificar los pros y contra de los distintos métodos existentes.
Context (C): ¿Qué tipo de organización y bajo qué circunstancias?	Revisar estudios existentes sobre los registros biométricos estáticos y las técnicas de autenticación de la persona.

B. Fase 2

Los criterios de selección para los estudios relevantes, fueron de inclusión y exclusión que se detallan a continuación:

- **Criterios de exclusión:** Se excluyeron todos los artículos académicos que no están escritos en el idioma inglés, que sean menor a cinco hojas de redacción, menores al año 2015 y los artículos que están relacionados con biométricos dinámicos.
- **Criterios de inclusión:** Se establecieron algunos criterios en los motores de búsqueda como: que el articulo académico se encuentre entre el año 2015 y 2021, términos propios del articulo académico (detallados en la fase III), investigaciones en desarrollo empírico con evidencia prometedora dentro del reconocimiento y autenticación biométrica.

C. Fase 3

Se definieron los términos necesarios para la creación de cadenas de búsqueda, además se utilizaron expresiones booleanas como "AND" u "OR": ("taxonomy biometric human") OR ("biometric security") OR ("fake biometric detection") OR ("biometric patters") OR ("Importance of begin unique from image quality") OR ("biometric") OR ("facial" AND "recognition") OR ("iris" AND "recognition") OR ("knuckle" AND "recognition") OR ("fingerprint" AND "recognition") OR ("finger vein" AND recognition"), como se detalla en la Tabla II.

TABLA II
TÉRMINOS PARA LA REALIZACIÓN DE LA BÚSQUEDA

Términos	Términos Semejantes
Recognition	Facial, iris, knuckle, fingerprint, finger vein.
Biometric security	Fake biometric detection, fake human traits.
Taxonomy biometric human	Biometric patters, Importance of identify human identity.

A. Fase 4

Estrategia de Búsqueda: Se aplicó la cadena de búsqueda en tres repositorios, siendo el primer filtro. "state of the art" AND "biometric human static" de los años del 2015 al 2021 obteniendo 2292, en el segundo filtro "fake biometric detection" con resultados del 543 y en el tercer filtro "biometric patters statics" AND "verifing human identities" con un resultado de 62 entre conferencias y revistas para un posterior estudio, como se detalla en la Tabla III.

TABLA III
CADENA DE BÚSQUEDA EN CADA REPOSITORIO

Repositorio	Cadena de Búsqueda	Tipo de Artículo	Filtro 1	Filtro 2	Filtro 3
IEEE	Título: "static biometric" AND "Recognition" OR "taxonomy biometric human" OR "biometric patters" AND "fake biometric detection" OR "verifying human identities" AND "state of the art"	Revistas y Conferencias	243	91	8
SCOPUS	Título: "static biometric" AND "Recognition" OR "taxonomy biometric human" OR "biometric patters" AND "fake biometric detection" OR "verifying human identities" AND "state of the art"	Revistas	870	56	17
Science Direct	Título: "static biometric" AND "Recognition" OR "taxonomy biometric human" OR "biometric patters" AND "fake biometric detection" OR "verifying human identities" AND "state of the art"	Revistas	1179	396	37
		TOTAL	2292	543	62

La investigación previa propone criterios para evaluar el rendimiento de la autenticación biométrica basado en [14], incluye el tiempo de formación del método,

requisitos computacionales, complejidad incluyendo 6 características universales como son la usabilidad, precisión, singularidad, desempeño, aceptación del usuario y robustez [15].

Preguntas de investigación: El objetivo principal es actualizar el estado del arte de los registros biométricos estáticos usados para autenticar la identidad de una persona, para lo cual se definen las preguntas de investigación para el Mapeo Sistemático (SMP#) y la Revisión de la literatura (SLRP#), las cuales se precisan a continuación:

- *SMP1: ¿Existe una taxonomía para el reconocimiento de los biométricos estáticos?*
- *SMP2: ¿Existe estudios al respecto en revistas o conferencias en los últimos seis años?*
- *SLRP1: ¿Qué técnicas/métodos se destacan dentro del reconocimiento de biométricos estáticos usados para autenticar la identidad de la persona?*
- *SLRP2: ¿Cuáles son los pros y contra de los métodos usados para la autenticación de la persona?*
- *SLRP3: ¿Qué medidas se utilizan en los métodos de autenticación biométrica?*
- *SLRP4: ¿Cuáles son los resultados documentados respecto a sesgos falsos de muestras legítimas con relación a los métodos fiables existentes para identificar una persona?*

A continuación, se detalla técnicas o métodos de artículos científicos, revistas indexadas que analizan cada uno de los registros biométricos estáticos enfocados en autenticar la identidad de la persona.

Revisión de la literatura

2.1 Algoritmo usado para el reconocimiento facial.

El estudio y la evaluación de las muestras realizadas a diferentes individuos, es de vital importancia, ya que es necesario reflejar vitalidad, grado de nitidez, niveles de color y luminancia. El obtener imágenes o videos es muy fácil, sin necesidad de atacar la BD (Base de Datos) que lo contiene, sino con el simple hecho que se pueden obtener en redes sociales es sencillo engañar un biométrico facial [15].

2.1.1 Modelo de distribución de puntos.

Según [16], propusieron lidiar con la variación que posee el reconocimiento facial en 2D, utilizaron vectores propios de pose y parámetros de pose para sintetizar imágenes corregidas. Los métodos propuestos lograron resultados de vanguardia, superando el modelo morfológico en 3D.

En enfoques como los ángulos de rotación de -45◦ a 45◦ arrojó como resultado una precisión de solo el 30%. Por lo tanto, este método tiene un nivel bajo de precisión, un nivel medio de usabilidad y un nivel bajo de seguridad sin privacidad, puesto que a pesar que la pose del usuario cambie, el perfil específico sigue existiendo.

2.1.2 Algoritmo evolutivo de partículas multiobjetivo.

En la actualidad, la cirugía plástica es un reto para los sistemas de reconocimiento, los cambios no lineales, son difíciles de predecir.

En [17], se propuso un algoritmo evolutivo el que se basa en partículas multiobjetivo que genera datos faciales no separados en niveles de granularidad, optimizando la información facial y haciendo coincidir con imágenes antes y después de la cirugía. Los resultados arrojan un mayor grado de precisión llegando al 90%. Por lo tanto, posee un nivel alto de precisión, con utilidad de nivel medio.

2.1.3 Sistema basado en piezas GMM.

Según [18], propusieron un sistema que basa su análisis en piezas GMM haciendo referencia a (Fragmentos Faciales) en el reconocimiento de rostros rotos, donde las imágenes de 64 × 80, en bloques de 8 × 8 con una superposición horizontal y vertical de 4 píxeles. Este proceso de evitar la superposición, conocido como teselación da como resultado 285 bloques. En su fase de prueba contra ataques de fuerza bruta muestra que, con la búsqueda de un solo bloque, este buscaría en un vector de 15 dimensiones con 285 puntos apropiados, dando como resultado que la búsqueda de múltiples bloques sea difícil de realizar y detectar en un 85%. Por lo tanto, el nivel de seguridad es medio alto.

2.2 Algoritmo usado para el reconocimiento del iris.

El diseño óptico de alta gama, simulando o robando una imagen del iris y su borde, en la actualidad implica un costo relativamente alto, pero es posible [15].

2.2.1 Modelo de protección bajo un iris sintético.

El método de protección [19], indica que las muestras de iris son generadas sintéticamente. La BD utilizada en este caso es CASIA-IrisV, contiene 7 imágenes en escala de grises de 320 x 280 bmp (Mapa de bits) de 1000 individuos reales.

La simulación de un iris falso consta de dos etapas, la primera generar un fondo de textura que representa la apariencia global del iris, la segunda es simular los surcos radiales y concéntricos.

Los resultados basados en IQA (Análisis de Calidad de imagen), muestran la capacidad del enfoque para adaptarse a un alto nivel de protección arrojando un 94% de efectividad.

2.2.2 Modelo de protección bajo ataque de suplantación.

El método de protección según [19], plantea que determinadas muestras reales-falsas tomadas de la base de datos ATVS.1, Analiza el Discriminante Cuadrático QDA ya que mostró ser mejor que el LDA (Análisis del Discriminante Lineal).

La base de datos ATVS.1 comprende 50 usuarios x 2 ojos x 4 imágenes x 2 sesiones, obteniendo un total de 800 iris falsos y sus correspondientes muestras reales, con iluminación infrarroja captura imágenes a escala de grises de 640 x 480 píxeles.

Los resultados arrojan el 97% para la correcta detección de vitalidad del iris, no solo superando el método de anti - spoofing en 10 veces su procesamiento.

2.2.3 Método Anti- Spoofing.

En [19], arroja un nuevo campo de investigación basando su estudio en un enfoque que es la “detección de vivacidad” con requisitos a seguir, esta técnica no puede ocasionar ningún daño al individuo, no debe requerir un contacto extremo con el mismo, su uso no debe ser complicado de entender, la interacción debe ser inmediata con el sensor y de costo no muy elevado.

La seguridad del método basa su cálculo en funciones IQ que minimiza su carga computacional, considerando implementaciones en Matlab de la discriminante lineal.

La imagen de entrada en escala de grises I de tamaño N × M se filtra con un núcleo gaussiano de paso bajo; dónde σ (sigma) es (σ = 0. 5 y el tamaño 3 x 3) con el fin de generar una versión suavizada I, la calidad entre las dos imágenes (I y I) se

calcula según la métrica IQA de referencia completa correspondiente.

Los resultados muestran que la vivacidad es capaz de clasificar en 97% en tiempo de ejecución, se midió en un estándar de 64 bits, no requiere segmentación y su procesamiento es 10 veces más rápido.

2.2.3.1 Técnicas basadas en Hardware.

Basa su funcionamiento en implantar algún dispositivo físico al sensor para la detección de rasgos particulares como "propiedades de reflexión específicas del ojo".

2.2.3.2 Técnicas basadas en Software.

Basa su funcionamiento el reconocimiento de rasgos falsos a partir de una muestra biométrica base y mas no del rango en sí.

Lo más deseable dentro de este método general, es combinar las dos técnicas, mientras que el hardware presenta un mayor rango de detección en sesgos falsos al contrario del software que es menos intrusivo en su implementación a su vez menos costoso ya que no requiere ningún dispositivo adicional.

2.3 Algoritmo usado para el reconocimiento de nudillos.

La decisión de salida de un clasificador multimodal de imágenes 2D con la entrada de puntuación coincide con un nivel más alto en [20] y proporciona mejores resultados porque realiza la fusión biométrica en el reconocimiento que se produce en diferentes etapas de emparejamiento y puntuaciones

tomando en cuenta las características extraídas en múltiples datos biométricos.

En la actualidad existe un artículo académico que basa su reconocimiento de patrones de nudillos internos basados en imágenes 3D con redes neuronales convolucionales, dónde las neuronas hacen referencia a campos receptivos [21].

Usa una capa de Softmax para el nivel de reconocimiento y clasificación con variantes como el número de neuronas de la capa conectada, los núcleos de convolución, algoritmos de optimización mostró como resultado el procesamiento de nudillos internos mediante tres grandes capas y una conectada el 96% de efectividad.

2.3.1 Patrones del Nudillo del dedo menor.

En [7], aplicado en la ciencia forense y la biometría humana, presenta un enfoque automatizado basando su estudio en la segmentación de la región de interés, reconocimiento de la imagen adaptándose a variaciones tomando en cuenta su BD que cuenta con muestras de niños entre los 4 y 7 años y adultos con más de 500 muestras.

Este modelo basado en la estabilidad y singularidad puede ser utilizado como evidencia en un tribunal de justicia, determinado científicamente la identidad del individuo en cuestión.

Los resultados muestran una mayor efectividad en niños mayores a 6 años, explorando coincidencias combinando estrategias lineales y no lineales con ayuda de puntuaciones para establecer coincidencia utilizando la combinación holística; donde:

- **Sc=** Emparejamiento.
- **Smajor y Smenor=** Puntuaciones coincidentes de las imágenes de nudillos mayores y menores.

$$s_c = \{(Smajor * \tau) + (Sminor * (1 - \tau))\} 1 * (1 + \frac{}{2 - Smajor})$$

Ecuación 1. Coincidencia utilizando combinación holística.

Demostrando que la fórmula anterior forma de los pliegues, las líneas de los nudillos menores y mayores son estables en distintos grupos de edad (59, 36, 37, 25, 6) años arrojando un 3.62% más de asertividad, son utilizados en la Republica China actualmente.

2.4 Algoritmo usado para el reconocimiento de huellas dactilares.

El recolectar huellas digitales no es nada complicado ya que, para obtener muestras, es necesario solo recolectarlas directamente de la superficie o con ayuda de gel de sílice, gelatina, playdoh y látex [15].

2.4.1 LivDet de suplantación de huellas dactilares.

Consta de un conjunto de huellas dactilares reales y falsas [19] capturadas por medio de un sensor óptico plano que consta de 3 partes: BiometrikaFX2000 con 569ppp (puntos por pulgada), Verificador de coincidencia cruzada 300CL con 500ppp e Identix DFR2100 con 686ppp, la base de datos contiene más de 18.000 muestras procedentes de más de 100 diferentes dedos.

El método presenta una combinación entre transpiración con características morfológicas (Análisis de la curvatura, cresta local, frecuencia y textura de multi resolución), seguidas de un protocolo de entrenamiento y pruebas (clasifica y califica).

Los resultados arrojan un 98.99% de aceptabilidad generalidad del método, que no es solo capaz de adaptarse a diferentes modalidades biométricas y ataques, pero

también funciona mejor que los métodos conocidos desde el estado de la técnica.

2.4.2 Algoritmo de Bresenham.

Basa su técnica en coordenadas de los puntos más cercanos a un determinado circulo, su centro es el origen polar, las coordenadas de los círculos concéntricos restantes se calculan luego de incrementos del radio especifico, donde la secuencia de pixeles hace referencia a un vector de características [8].

La comparación de los patrones de dos huellas se realiza a partir de la correlación espacial de vectores homólogos.

2.4.3 Técnicas basadas en características.

Esta técnica basa su comparación no a nivel de pixeles en una imagen sino mediante una rejilla que contiene pequeños que son alineadas para extraer características como la intensidad de los pixeles, orientación de crestas, numero de crestas y periodicidad [8].

El grosor de las crestas oscila entre 100 y 300μm (micrómetros), donde las heridas producidas por quemaduras superficiales, abrasiones, no afectan la estructura de la cresta ya que la piel se reconstruye dando lugar a la restauración del espacio perdido.

2.5 Algoritmo usado para el reconocimiento de venas dactilares.

Es utilizada actualmente a gran escala en Aadhar en India y el puerto de entrada a los Emiratos Árabes ya que ejerce gran impacto de tiempo real. El patrón vascular mencionado en [22], de los dedos usa información sobre las estructuras de vasos sanguíneos obteniendo grandes ventajas sobre otros sistemas como patrones únicos, alta tasa de verificación y difíciles de falsificar. Esta técnica enfrenta un gran desafío como el obtener la cantidad adecuada de luz para reflejar desde el dedo la vena.

El QDA basa su proceso en escala de grises y estos datos se envían a un vector en el cual se comparan los datos iniciales con

los nuevos, siendo casi imposible su vulnerabilidad [23].

2.5.1 Método de transmisión de Luz.

Este método consiste en penetrar la luz y la intensidad por medio del dedo entre el sensor y la cámara. Es necesario para obtener imágenes de buena calidad, presentando un efecto mínimo ante luces de fondo.

2.5.2 Método de Reflexión de Luz.

En este método el sensor de venas se coloca la fuente de luz infrarroja y la imagen obtenida es el contraste de las venas y otros tejidos mediante un sensor de imagen NIR. [24], como se muestra en la Figura 6.

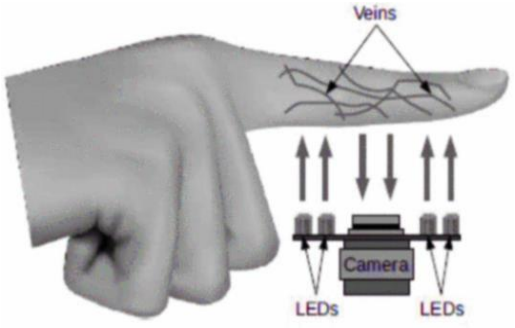


Figura 6. Método de reflexión de Luz. [24]

2.5.3 Método de penetración lateral.

En este método se coloca la luz en ambos lados del dedo con el sensor debajo del mismo, este tipo proporciona una mejor imagen en comparación al método de a los dos métodos antes mencionados.

Finalmente, se da respuesta a las preguntas de investigación planteadas en el SMP Y SLRP.

3. Resultados y Discusión

SMP1: ¿Existe una taxonomía para el reconocimiento de los biométricos estáticos?

La taxonomía permite tratar y clasificar los métodos de manera jerarquizada [25], mediante la autenticación de la persona en base a modelos biométricos; como son: facial, iris, nudillos, huellas dactilares y venas dactilares, como se muestra en la Tabla IV.

TABLA IV
ESQUEMA DE AUTENTICACIÓN BASADO EN BIOMETRÍA

Esquema	Autor
Reconocimiento facial	[15], [16], [17], [26], [27].
Reconocimiento de iris	[18], [28], [29], [30].
Reconocimiento de nudillos	[7], [31].
Reconocimiento de huellas dactilares	[8], [14], [18].
Reconocimiento de venas dactilares	[20], [32].

SMP2: ¿Existen estudios al respecto en revistas o conferencias en los últimos seis años?

Los estudios realizados y publicados en revistas/conferencias se distribuyen de los años 2015 al 2021 en el que se identifican los más importantes como se muestra en la Figura 7.

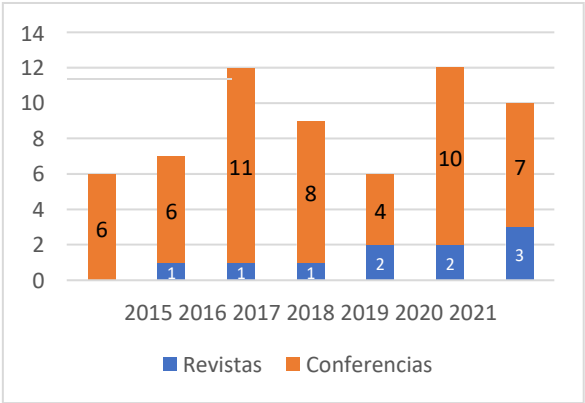


Figura 7. Distribución de estudios en los últimos seis años.

SLRP1: ¿Qué técnicas/métodos se destacan dentro del reconocimiento de biométricos estáticos usados para autenticar la identidad de la persona?

El identificar técnicas o métodos destacados dentro de la investigación ayuda a interpretar información de manera imparcial, como muestra la Tabla V.

TABLA V
MÉTODOS UTILIZADOS CON MAYOR IMPACTO

Esquema	Método
Reconocimiento facial	Modelo de distribución de puntos.
Reconocimiento de iris	Modelo de protección bajo un ataque de suplantación.
Reconocimiento de nudillos	Patrones de nudillos del dedo menor.
Reconocimiento de huellas dactilares	Técnicas basadas en características individuales.
Reconocimiento de venas dactilares	Método de reflexión de luz.

SLRP2: ¿Cuáles son los pros y contra de los métodos usados para la autenticación de la persona?

El identificar los pros y contra dentro de una investigación compara y define, puntos tanto positivos como negativos, como muestra la Tabla VI.

TABLA VI
Pros y contras de los métodos de autenticación.

	Ventajas	Desventajas
Reconocimiento facial	El algoritmo basa su modelo en Adaboost y SVM que ayuda a extraer los componentes de color que son determinados por el color de piel (esqueleto y geometría facial) destacando su simplicidad y requisito computacional económico [33]. Los videos faciales calculan el flujo sanguíneo Facial Blood Flow (FBI) con pequeño movimiento no dependiendo de rasgos faciales críticos [34].	El algoritmo muestra un menor rendimiento con imágenes de fondo complejo obteniendo detección del 87,46% [33]. El algoritmo por sí solo funciona con un rendimiento básico y ayudado de dos regiones faciales extra su rendimiento crece potencialmente [34].
Reconocimiento de iris	El algoritmo desarrolla una red de aprendizaje profundo YOLOv4, obtiene una mayor precisión de reconocimiento en intrusos y no requiere un proceso de segmentación del iris [35].	El algoritmo es un modelo para calcular la probabilidad y es aquí donde se obtiene un falso rechazo que conduce a problema de
Reconocimiento de nudillos	Este algoritmo presenta un modelo de individualidad basando su funcionalidad en patrones pre establecidos en dedos 3D de última generación en pixeles. [36].	
Reconocimiento de huellas dactilares	El algoritmo empareja dermatoglifos ilustrando la robustez de la huella dactilar frente alteraciones de la epidermis [37].	
Reconocimiento de venas dactilares	El algoritmo autentica a los usuarios el acceder a espacios con alta seguridad, siendo estable su capacidad de procesamiento sobre los atributos fisiológicos [38].	

	seguridad [35].
Reconocimiento de nudillos	El algoritmo no es útil en personas que sufren de artritis y artrosis ni en personas adultas, obteniendo resultados casi nulos en el reconocimiento del mismo [7].
Reconocimiento de huellas dactilares	El algoritmo puede ser engañado fácilmente si no hace uso de métodos anti - spoofing para garantizar la presencia real del dedo o escaneos profundos de la piel, además de generar cuellos de botella en el biométrico [39].
Reconocimiento de venas dactilares	El algoritmo exige mayor inversión y procesamiento para obtener imágenes estables por métodos discriminantes [40].

SLRP3: ¿Qué medidas se utilizan en los métodos de autenticación biométrica?

El establecer parámetros necesarios es importante, ya que sirve para medir el comportamiento a posteriori en determinadas tareas y evaluar el mismo, como lo muestra en la Tabla VII.

TABLA VII
Métrica de métodos Biométricos

	Usabilidad	Precisión	Singularidad	Desempeño	Robustez	Aceptabilidad	Seguridad
Reconocimiento facial	Baja	Baja	Medio	Alta	Alta	Baja	Media
Reconocimiento de iris	Media	baja	Alta	Alta	Alta	Nulo	Alta
Reconocimiento de nudillos	Media	Media	Media	Alta	Alta	Nulo	Nulo
Reconocimiento de huellas dactilares	Media	Alta	Alta	Alta	Media	Media	Baja
Reconocimiento de venas dactilares	Media	Baja	Alta	Baja	Media	Baja	Alta

SLRP4: ¿Cuáles son los resultados documentados respecto a sesgos falsos de muestras legítimas con relación a los métodos fiables existentes para identificar una persona?

El mapa de calor es una técnica que analiza el comportamiento de los usuarios con métricas establecidas en [15], divididos por la taxonomía del #SMP1 y técnicas detalladas en #SLRP1, con el fin de mostrar que método es fiable respecto en la detección de sesgos falsos de muestras legítimas, como se muestra en la figura 8.

Dónde el rango definido es bajo desde 0 a 40 (Rojo), medio desde 41 a 70 (Amarillo) y alto desde 71 a 100 (Verde).

RESULTADOS RESPECTO A LOS SESGOS FALSOS DE MUESTRAS LEGÍTIMAS.

	USABILIDAD	ACEPTACIÓN DEL USUARIO	SEGURIDAD	PRECISIÓN	SINGULARIDAD	DESEMPEÑO	ROBUSTEZ
RECONOCIMIENTO FACIAL							
Sistema basado en piezas GMM.	30	85	80	55	60	70	80
Modelo de distribución de puntos.	45	30	50	30	70	60	90
Algoritmo evolutivo de partículas multiobjetivo.	45	40	30	90	45	60	85
RECONOCIMIENTO DEL IRIS							
Modelo de protección bajo un iris sintético.	41	80	90	94	90	80	90
Modelo de protección bajo ataque de suplantación.	97	70	95	80	75	97	90
Método Anti- Spoofing.	80	90	90	87	97	95	75
RECONOCIMIENTO DE LOS NUDILLOS							
Patrones del Nudillo del dedo menor.	70	80	60	96	70	30	80
RECONOCIMIENTO DE HUELLAS DACTILARES							
LivDet de suplantación de huellas dactilares.	60	99,99	30	50	90	80	70
Técnicas basadas en características.	98,7	95	60	58	76	89	99
Algoritmo de Bresenham	80	93	10	71	99	70	60
RECONOCIMIENTO DE VENAS DACTILARES							
Método de transmisión de Luz.	60	96	80	43	96	30	45
Método de Reflexión de Luz .	70	95	90	65	86	10	60
Método de penetración lateral.	97	97	99	46	99	90	10

Figura 8. Mapa de calor de muestras legitimas. Elaborado por: Alisson Gutiérrez.

4. Conclusiones

La recopilación de artículos académicos sobre métodos estáticos usados para autenticar la identidad humana muestra varias alternativas con distinto grado de precisión mediante la extracción de rasgos únicos con la ayuda del comportamiento y el proceso asociado a la toma de la muestra.

La biometría facial mostró que necesita mejorar su rendimiento de verificación, ya que pueden dar falsos positivos al implementarla, depende de la simetría en la pose y la iluminación.
La biometría ocultar mostró que cuenta con menor aceptación por parte del usuario.
En la actualidad se desarrolla software robusto para la biometría ocular que procesa imágenes fuera del espectro visible con rangos más alto de reconocimiento y aceptación.
La biometría de los nudillos mostró mejor efectividad y menos falsos positivos en el reconocimiento de la persona al cambiar a técnicas 3D con procesamiento que usa inteligencia artificial.
La biometría dactilar mostró tener mayor aceptabilidad por parte del usuario porque es muy popular.
En la actualidad la biometría dactilar es utilizada para respaldar imágenes forenses por su efectividad para la identificación de personas.
La biometría de venas dactilares mostró ser más confiable en entornos de alta seguridad ya que basa su desarrollo en atributos fisiológicos y procesos de QDA con el 98.7% de precisión.
Los resultados documentados sobre los sesgos falsos de muestras legitimas muestran que todos los métodos son aceptados y usables por parte del usuario, pero presentan poca robustez para la identificación de la persona.

5. Trabajo Futuro

La literatura muestra varias alternativas para identificar una persona mediante el desarrollo de la biometría estática como son las venas dactilares u ocular siendo las más prometedoras, ya que por medio de sensores brindan la posibilidad de ser menos invasivos evitando la proximidad, mejorando el rendimiento del reconocimiento.

Hay que enfocarse en mejorar el reconocimiento de los patrones de las venas con métodos más efectivos y robustos frente a la intensidad luminosa para mejorar los resultados de autenticación biométricos futuros.

6. Referencias

[1] INCIBE, «Instituto Nacional de Ciberseguridad,» Tecnologías biométricas, 2020. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf.

[2] C. Jasserand, «Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data,» *European Data Protection Law Review,* vol. Volume 2 , nº https://edpl.lexxion.eu/article/EDPL/2016/3/6, pp. 297 - 311, 2016.

[3] Sistemas de Biometria, «Sistemas de Biometría,» IMPORTANCIA DE LOS SISTEMAS BIOMÉTRICOS, 10 Diciembre 2010. [En línea]. Available: https://sistemasbiometria.blogia.com/2010/121001-importancia-de-los-sistemas-biom-tricos.php.

[4] INTERPOL, «FACTORES EN LA IDENTIFICACIÓN FACIAL,» Reconocimiento Facial, Marzo 2020. [En línea]. Available: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial.

[5] Biometrics, «Biometrics,» Identificación biométrica a través del iris ocular, 2021. [En línea]. Available: https://biometrics-on.com/identificacion-biometrica-a-traves-

del-iris-ocular/#Por_que_resulta_apropiado_el_iris_en_la_identificacion_biometrica.

[6] K. Nivetha y D. Saraswady, «Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm,» *Segunda Conferencia Internacional sobre Electrónica y Sistemas de Comunicación (ICECS),* vol. 10, nº 1109, pp. 943-947, 2015.

[7] A. Kumar, «Importance of Being Unique From Finger Dorsal Patterns: Exploring Minor Finger Knuckle Patterns in Verifying Human Identities,» *IEEE,* vol. 9, nº IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, pp. 2-3, 2015.

[8] J. López, «Algoritmo para la identificación de personas basado en huellas dactilares.,» Departamento de Ingenierpia Electrónica, [En línea]. Available: https://upcommons.upc.edu/bitstream/handle/2099.1/8082/proyecto%20final%20de%20carrera.pdf?sequence=1. [Último acceso: 25 Abril 2021].

[9] K. Anil, J. Fellow y F. Jianjiang, «Latent Fingerprint Matching,» *IEEE Transactions on pattern analysis and machine intelligence,* vol. 33, nº 100, pp. 88-100, 2015.

[10] A. Kumar y Y. Zhou, «Human Identification Using finger images,» *", IEEE Transactions onimage processing,* vol. 21, nº 4, pp. 2228 - 2244, 2012.

[11] M. Hernandez, «Procesamiento dactilar usando Transformada de Fourier,» *Revista de Innovación Sistemática,* vol. 1, pp. 37-46, 2017.

[12] E. Linares-Espinós, V. Hernández, L. Domínguez-Escrig y S. Fernández-Pello, «Methodology of a systematic review,» *Science Direct,* vol. 42, nº 8, pp. 499 - 506, 2018.

[13] P. Pravallika y P. S, «SVM classification for fake biometric detection using image quality assessment: Application to iris, face and palm print,» *International Conference on Inventive Computation Technologies (ICICT),* vol. doi: 10.1109/INVENTIVE.2016.7823189., pp. 1-6, 2016.

[14] R. Kannavara y N. Bourbaki, «Una encuesta comparativa sobre iden-tcnicas de autenticacin de la ciudad basadas en redes neuronales,» *Biometrics:Teoría, métodos y aplicaciones , NV Boulgouris,* vol. 3, pp. 47-49, 2009.

[15] Z. Rui y Z. Yan, «A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification,» *IEEE,* nº 7, pp. 5994 - 6009, 2018.

[16] J. L. Alba y D. Gonzales, «Toward Pose-Invariant 2-D Face Recognition Through Point Distribution Models and Facial Symmetry,» *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol. 2, nº 3, pp. 413-420, 2007.

[17] S. Himanshu, . S. Bharadwaj y R. Singh, «Recognizing surgically altered face images using multiobjective evolutionary algorithm,» *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol. 8, nº 1, 2015.

[18] J. Galbally, C. McCool, J. Fierrez, S. Marcel y J. Ortega , «On the Vulnerability of Face Verification Systems to Hill-Climbing Attacks,» *Instituto de Investigaciones IDIAP,* p. 21, 2009.

[19] J. Galbally y S. Marcel, «Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint,and Face Recognition,» *IEEE TRANSACTIONS ON IMAGE PROCESSING,* vol. 23, nº 2, 2014.

[20] S. Sumathi y B. Rajalakshmi, «Survey Of Multimodal Biometric Using Ear And Finger

Knuckle Image,» *International Conference on Communication, Computing and Internet of Things (IC3IoT),* vol. 10, pp. 48 - 53, 2018.

[21] Y. Xue, M. Liu, M. Qiao y M. Xue, «Research on Inner Knuckle Pattern Recognition Method Based on Convolutional Neural Network,,» *IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC),* pp. 2510 -2514, 2021.

[22] R. Raghavendra, J. Surbiryala, B. Raja y C. Busch, «Novel finger vascular pattern imaging device for robust biometric verification,» *IEEE International Conference on Imaging Systems and Techniques (IST) Proceedings,* vol. 10, nº 2014.6958463., pp. 148-152, 2014.

[23] D. Akila, S. Jeyalaksshmi, R. Jayakarthik, S. Mathivilasini y G. Suseendran, «Biometric Authentication With Finger Vein Images Based On Quadrature Discriminant Analysis,» *2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM),* vol. doi: 10.1109/ICCAKM50778.2021.9357705, pp. 118 - 122, 2021.

[24] D. Akila, S. Jeyalaksshmi, R. Jayakarthik y S. Mathivilasini, «Biometric Authentication With Finger Vein Images Based On Quadrature Discriminant Analysis,» *International Conference on Computation, Automation and Knowledge Management (ICCAKM),* vol. doi: 10.1109/ICCAKM50778.2021.9357705., pp. 118-122, 2021.

[25] M. Amine Ferrag, L. Maglaras, A. Derhab y A. Amara Korba, «Taxonomy of Biometric-based Authentication Schemes for Mobile Computing Devices,» *3rd International Conference on Pattern Analysis and Intelligent Systems,* nº 10.1109, pp. 1-8, 2018.

[26] R. P. P. Prashant, R. Pramod y S. Sandhya, «A General Approach on Facial Feature Extraction and Face Attributes,» *3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS),* pp. 151-155, 2018.

[27] M. E. Trufasila y P. Anghelescu, «Biometric System based on Facial Recognition,» *11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI),* pp. 1-5, 2019.

[28] Y.-T. Hwang, F. de Chih-Peng y C.-S. Hsiao , «Iris Location and Recognition by Deep-Learning Networks Based Design for Biometric Authorization,» *IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech),* pp. 144-149, 2021.

[29] M. Luca, A. Ciobanu y T. Barbu , «Multimodal biometric authentication based on voice, face and iris,» *E-Health and Bioengineering Conference (EHB),* pp. 1-5, 2015.

[30] T. Jawale y S. Gandhe, «Human identilication using fusion of iris, signature and gait recognition,» *International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC),* pp. 282-287, 2016.

[31] . S. Karamchandani y N. Kudu, «Biometric identification system using fingerprint and knuckle as multimodality features,» *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* pp. 3279-3284, 2016.

[32] R. Garcia-Martin y R. Sanchez-Reillo, «Vein Biometric Recognition on a Smartphone,» *IEEE Access,* vol. 8, nº 10.1109, pp. 104801-104813, 2020.

[33] M. Chowdhury, J. Gao y R. Islam, «Fuzzy rule based approach for face and facial

feature extraction in biometric authentication,» *2016 International Conference on Image and Vision Computing New Zealand (IVCNZ),* nº doi: 10.1109/IVCNZ.2016.7804444., pp. 1-5, 2016.

[34] T. Pistola, A. Papadopoulos, N. Mitianoudis y V. Boulgouris, «Biometric Identification Using Facial Motion Amplification,» *IEEE International Conference on Image Processing (ICIP),* vol. doi: 10.1109/ICIP.2019.8803171., pp. 1695-1699, 2019.

[35] C. Hsiao, C. Fan y T. Hwang, «Iris Location and Recognition by Deep-Learning Networks Based Design for Biometric Authorization,» *IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech),* pp. 144-149, 2021.

[36] K. Cheng y A. Kumar, «Contactless Biometric Identification Using 3D Finger Knuckle Patterns,» *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 42, nº 8, pp. 1868-1883, 2020.

[37] H. Costa, O. Bellon, L. Silva y A. Bowden, «Towards biometric identification using 3D epidermal and dermal fingerprints,» *IEEE International Conference on Image Processing (ICIP),* pp. 3937-3942, 2016.

[38] D. Aklia, S. Jeyalaksshmi, R. Jayakarthik, S. Mathivilasini y G. Suseendran, «Biometric Authentication With Finger Vein Images Based On Quadrature Discriminant Analysis,» *2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM),* pp. 118-122, 2021.

[39] C. Jain, «Strengthening of Fingerprint Technology,» *International Conference on Computing, Power and Communication Technologies (GUCON),* pp. 721-726, 2018.

[40] D. Akila, S. Jeyalaksshmi, R. Jayakarthik y S. Mathivilasini, «Biometric Authentication With Finger Vein Images Based On Quadrature Discriminant Analysis,» *2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM),* pp. 118-123, 2021.

[41] A. Kumar y Y. Zhou, «Human identification using finger images,» *Transacciones IEEE acerca del procesamiento de imagenes,* vol. 21, pp. 2228 - 2244, 2012.

[42] D. Akila, S. Jeyalaksshmi, R. Jayakarthik, S. Mathivilasini y G. Suseendran, Artists, *Biometric Authentication With Finger Vein Images Based On Quadrature Discriminant Analysis.* [Art]. 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021.