

Control de Acceso por Reconocimiento de Huellas Dactilares, Extracción de Minucias y Distancia Euclidiana

Denis Rubin* 

Universidad de Panamá, Panamá

Javier Fernández Pájaro 

Universidad de Panamá, Panamá

Resumen

El presente estudio tuvo como objetivo desarrollar y evaluar un sistema de control de acceso basado en reconocimiento de huellas dactilares mediante extracción de minucias y comparación por distancia euclidiana, implementado en la Facultad de Informática, Electrónica y Comunicación (FIEC) de la Universidad de Panamá. La investigación adoptó un diseño de desarrollo tecnológico experimental con validación de prototipo. Se utilizó un escáner óptico Futronic FS80 para la captura de imágenes a 320×480 píxeles y 500 dpi, las cuales fueron normalizadas a 256×256 píxeles durante el preprocesamiento. La muestra estuvo conformada por 15 participantes seleccionados mediante muestreo por conveniencia, con criterios de inclusión que requerían ausencia de lesiones dérmicas en los dedos índice o pulgar. Se realizaron múltiples capturas por participante (tres por dedo) bajo condiciones controladas de iluminación y posición. El algoritmo desarrollado empleó técnicas de binarización, adelgazamiento y detección de minucias mediante análisis de conectividad en matrices 3×3 , seguido de comparación por distancia euclidiana. Los resultados principales mostraron una precisión del 73,3% (11 de 15 casos con coincidencia correcta), con un tiempo promedio de procesamiento de 2,3 segundos por verificación. El análisis de errores reveló que los cuatro casos fallidos se debieron principalmente a variaciones en la presión de captura y rotación no compensada. Las limitaciones incluyen el reducido tamaño de muestra y las condiciones controladas de captura. Se concluye que el sistema desarrollado representa una alternativa viable de bajo costo para control de acceso, aunque requiere optimización en la etapa de alineación de minucias para mejorar su solidez.

Palabras clave: Biometría; Huella dactilar; Extracción de minucias; Distancia euclidiana; control de acceso; Autenticación biométrica.

*Correspondencia: denis.rubin@up.ac.pa

Este artículo es de acceso abierto distribuido bajos los términos y condiciones de la Licencia Creative Commons Attribution (CC BY)

Access Control through Fingerprint Recognition, Minutiae Extraction, and Euclidean Distance

Abstract

This study developed and evaluated an access control system based on fingerprint recognition through minutiae extraction and Euclidean distance comparison at FIEC, University of Panama. The research used an experimental technological development design with prototype validation. A Futronic FS80 optical scanner captured images at 320×480 pixels and 500 dpi, normalized to 256×256 pixels. The sample included 15 participants selected by convenience, without dermal lesions on index or thumb fingers. Three captures per finger were performed under controlled lighting and position. The algorithm applied binarization, thinning, and minutiae detection via connectivity analysis in 3×3 matrices, followed by Euclidean distance comparison. Results showed 73.3% accuracy (11/15 correct matches), with an average processing time of 2.3 seconds per verification. Errors were mainly due to variable pressure and uncompensated rotation. Limitations include small sample size and controlled conditions. The system is a viable low-cost alternative, though minutiae alignment requires optimization.

Keywords: Biometrics; Fingerprint; Minutiae Extraction; Euclidean Distance; Access Control; Biometric Authentication.

Controle de Acesso por Reconhecimento de Impressões Digitais, Extração de Minúcias e Distância Euclidiana

Resumo

O presente estudo teve como objetivo desenvolver e avaliar um sistema de controle de acesso baseado no reconhecimento de impressões digitais por meio da extração de minúcias e comparação por distância euclidiana, implementado na Faculdade de Informática, Eletrônica e Comunicação (FIEC) da Universidade do Panamá. A pesquisa adotou um desenho de desenvolvimento tecnológico experimental com validação de protótipo. Utilizou-se um scanner óptico Futronic FS80 para a captura de imagens a 320×480 pixels e 500 dpi, as quais foram normalizadas para 256×256 pixels durante o pré-processamento. A amostra foi composta por 15 participantes selecionados por amostragem por conveniência, com critérios de inclusão que exigiam ausência de lesões dérmicas nos dedos indicador ou polegar. Foram realizadas múltiplas capturas por participante (três por dedo) sob condições controladas de iluminação e posição. O algoritmo desenvolvido empregou técnicas de binarização, afinamento e detecção de minúcias mediante análise de conectividade em matrizes 3×3 , seguido de comparação por distância euclidiana. Os principais resultados mostraram uma precisão de 73,3% (11 de 15 casos com correspondência correta), com um tempo médio de processamento

de 2,3 segundos por verificação. A análise de erros revelou que os quatro casos falhos se deveram principalmente a variações na pressão de captura e rotação não compensada. As limitações incluem o tamanho reduzido da amostra e as condições controladas de captura. Conclui-se que o sistema desenvolvido representa uma alternativa viável de baixo custo para controle de acesso, embora requeira otimização na etapa de alinhamento de minúcias para melhorar sua robustez.

Palavras-chave: Biometria; Impressão digital; Extração de minúcias; Distância euclidiana; Controle de acesso; Autenticação biométrica.

1. Introducción

Garantizar la protección de recintos clave en instalaciones universitarias e industriales requiere hoy en día de estrategias de resguardo dinámicas, proactivas y automatizadas. En el contexto de la Facultad de Informática, Electrónica y Comunicación (FIEC), la respuesta inicial ante esta necesidad consistió en desplegar tecnologías de monitoreo reactivo, como el circuito cerrado de televisión (CCTV). No obstante, si bien estos dispositivos facilitan la supervisión continua y el análisis forense posterior a un incidente, carecen de la facultad operativa para frenar de forma autónoma o en tiempo real el paso de personal no autorizado hacia recintos de alta seguridad, laboratorios de investigación especializada o salas de servidores. Dicha restricción impulsó la transición hacia plataformas inteligentes coordinadas con sistemas de automatización edilicia (BMS, por sus siglas en inglés) e infraestructura de Internet de las Cosas (IoT) para gestionar el acceso de manera preventiva.

La huella dactilar se forma durante el tercer a cuarto mes de desarrollo fetal, las crestas comienzan a desarrollarse en la piel de las yemas de los dedos. El propósito de esto es, crear en los dedos de las manos una fricción más profunda para evitar el deslizamiento de objetos en nuestras manos. Estas crestas permiten tener un mejor agarre al momento de sujetar o levantar objetos. (Ver Figura 1)



Figura 1 Ejemplo de una huella dactilar

Los sistemas convencionales de validación basados en la posesión de objetos físicos (como tarjetas de proximidad RFID, llaves magnéticas o tokens) exhiben fallas críticas de seguridad, entre las que destacan el extravío de credenciales, la clonación de tarjetas y la suplantación de identidad mediante la cesión voluntaria o involuntaria de los dispositivos de entrada (Cabana, 2010). Frente a estas deficiencias, la biometría se ha consolidado como la alternativa de autenticación más confiable. De acuerdo con la literatura contemporánea, la impresión dactilar

sobresale frente a otros rasgos anatómicos debido a sus elevados niveles de singularidad, permanencia e inalterabilidad a lo largo de la vida del individuo (Reddy et al., 2023; Sujan et al., 2024). A pesar de estas ventajas, el desafío técnico persistente estriba en la carencia de algoritmos digitales de bajo consumo computacional capaces de validar identidades instantáneamente sin depender de plataformas comerciales costosas e inaccesibles.

Diversos análisis del estado del arte revelan que la gran mayoría de las soluciones de identificación disponibles en el mercado experimentan retardos significativos y una marcada pérdida de exactitud cuando la captura de la huella registra distorsiones, resequedad o baja calidad en la adquisición de la imagen. La brecha científica actual se sitúa, por tanto, en la complejidad técnica de sostener métricas de efectividad elevadas utilizando algoritmos simplificados que extraigan minucias (bifurcaciones y terminaciones de crestas) sin recurrir a potentes unidades centrales de procesamiento (Engelsma et al., 2021). En la actualidad, el sector industrial suele emplear modelos centralizados de gran tamaño o dispositivos cerrados que limitan severamente la vinculación con estándares domóticos e industriales de arquitectura abierta.

La revisión de la literatura reciente sobre sistemas biométricos de huellas dactilares expone varias limitaciones estructurales en los enfoques existentes. Los sistemas comerciales como los ofrecidos por firmas como Suprema, HID Global y ZKTeco, si bien presentan altas tasas de precisión, requieren hardware especializado de elevado costo y licencias de software propietario que los hacen económicamente inviables para implementaciones académicas, institucionales o de pequeña escala (Alay & Al-Baity, 2020). Por otro lado, las soluciones de código abierto como OpenCV y SourceAFIS brindan flexibilidad de desarrollo, pero típicamente carecen de documentación optimizada y de frameworks ligeros diseñados para integrarse directamente en microcontroladores de bajo consumo o entornos de procesamiento limitado (Maltoni et al., 2022).

Investigaciones recientes han explorado el uso de Redes Neuronales Convolucionales (CNN) y modelos de aprendizaje profundo para el reconocimiento e identificación de huellas dactilares, logrando precisiones superiores al 95% incluso con impresiones parciales o con ruido. Sin embargo, estos enfoques requieren una infraestructura computacional significativa —como servidores dedicados con Unidades de Procesamiento Gráfico (GPU) y alto consumo energético— lo cual contradice la necesidad de soluciones de bajo costo y procesamiento en el borde (edge computing) para aplicaciones de control de acceso distribuidas y autónomas (Alsaadi et al., 2021; Sharma & Kumar, 2022).

Para superar la brecha entre la precisión teórica de los modelos computacionalmente pesados y la viabilidad práctica en entornos restringidos, la investigación reciente propone trasladar el procesamiento hacia nodos perimetrales (edge nodes). Mediante la optimización de los flujos de extracción de características y el filtrado direccional de crestas con transformadas de Gabor simplificadas, es posible reducir el tamaño de las plantillas biométricas a solo unos pocos cientos de bytes. Esto permite ejecutar la comparación de minucias (minutiae matching) directamente en la memoria RAM de microcontroladores de

32 bits en tiempos inferiores a los 500 milisegundos (Sun et al., 2024; Zhang et al., 2023).

La convergencia entre la verificación biométrica y los sistemas de automatización edilicia (BMS) mediante el paradigma de Internet de las Cosas (IoT) representa un área de investigación crítica para la infraestructura moderna. En el contexto de recintos universitarios o plantas industriales, la verificación de identidad no debe limitarse a activar un cerradero eléctrico; debe interactuar de forma segura con protocolos de comunicación abiertos (como MQTT, Modbus o Wiegand) para actualizar tableros de control en tiempo real, registrar eventos auditables y activar perfiles de climatización o iluminación según la presencia de personal autorizado (Khan et al., 2023; Silva et al., 2022).

Adicionalmente, las investigaciones en el campo de los sensores ópticos de bajo costo han permitido resolver problemas de captura distorsionada mediante el desarrollo de lentes de campo de visión amplio (FOV) y sistemas de retroiluminación adaptativa en el espectro infrarrojo (Tsai et al., 2024). Por otro lado, la adopción de esquemas de aprendizaje federado y criptografía ligera en el borde permite almacenar y procesar las plantillas biométricas de forma local en los nodos de acceso, evitando la transmisión centralizada de datos sensibles y mitigando vectores de ataque cibernético como el eavesdropping o las filtraciones masivas de datos biométricos (Federated Learning & Privacy-Preserving Group, 2025; Humayun et al., 2024).

La combinación de sensores ópticos de bajo costo con microcontroladores embebidos no solo garantiza la resiliencia operativa ante caídas de la red, sino que también democratiza el acceso a sistemas de seguridad electrónica avanzados en instituciones públicas y académicas.

La propuesta diferencial de esta labor académica se sustenta en la creación de un esquema flexible y eficiente que perfecciona la fase de acondicionamiento de imagen y la obtención de características a nivel local. La contribución novedosa se articula en tres ejes fundamentales:

1. Algoritmo de procesamiento optimizado: Se desarrolló una variante del algoritmo de extracción de minucias basada en análisis de conectividad que reduce la complejidad computacional sin sacrificar significativamente la precisión, permitiendo su ejecución en dispositivos de recursos limitados.
2. Método de comparación simplificado: Se implementó un enfoque de comparación por distancia euclidiana con compensación de desplazamiento y rotación que, aunque no alcanza los niveles de robustez de algoritmos más complejos, ofrece un equilibrio adecuado entre precisión y eficiencia computacional.
3. Integración con sistemas de automatización abiertos: A diferencia de las soluciones comerciales cerradas, el sistema desarrollado puede integrarse con plataformas domóticas de arquitectura abierta mediante interfaces estándar, facilitando su adopción en entornos institucionales diversos.

La elección del rasgo biométrico permite manejar un sistema automático de reconocimiento, el cual se efectúa teniendo en cuenta el cumplimiento en mayor o menor grado de las siguientes propiedades (Simón-Zorita, 2003, p.13):

- Universalidad: el rasgo biométrico existe para todos los individuos.
- Unicidad: el rasgo identifica unívocamente a cada individuo.
- Permanencia: el rasgo se mantiene invariable con el tiempo a corto plazo.
- Inmutabilidad: el rasgo se mantiene invariable con el tiempo a largo plazo o durante toda la vida.
- Mensurabilidad: el rasgo es apto para ser caracterizado cuantitativamente.
- Rendimiento: el rasgo permite el reconocimiento de un individuo con rapidez, robustez y precisión.
- Aceptabilidad: el rasgo presenta la calidad de ser aceptado por la mayoría de la población.
- Invulnerabilidad: el rasgo permite una robustez del sistema frente a los métodos de acceso fraudulentos.

La huella dactilar cumple de manera sobresaliente con estas propiedades, siendo considerada uno de los rasgos biométricos más adecuados para aplicaciones de control de acceso (Maltoni et al., 2022). La huella dactilar se forma durante el tercer a cuarto mes de desarrollo fetal, cuando las crestas comienzan a desarrollarse en la piel de las yemas de los dedos. El propósito de esto es crear en los dedos de las manos una fricción más profunda para evitar el deslizamiento de objetos. Estas crestas permiten tener un mejor agarre al momento de sujetar o levantar objetos.

El conjunto de crestas en las yemas de los dedos crea una fricción y, a su vez, se organizan en patrones más o menos regulares con características únicas. Todas las huellas dactilares tienen una serie de combinaciones únicas de patrones y características; cada patrón de crestas contiene filas de poros que permiten que el sudor y el aceite corporal expulsados por las glándulas puedan salir del cuerpo. El sudor mezclado con aceites producidos por el cuerpo produce huellas dactilares en superficies lisas.

El estudio sistemático de las huellas dactilares tiene sus raíces en el trabajo pionero de Francis Galton a finales del siglo XIX. En su obra *Finger Prints* (1892), estableció el principio de la unicidad de las huellas dactilares y clasificó tres patrones fundamentales: arcos, lazos y espirales.

Henry (1900) amplió esta clasificación, identificando cuatro tipos de patrones de arco: arcos lisos, arcos radiales, arcos cubitales y arcos de tiendas de campaña (p. 20-24). Los arcos lisos tienen un flujo uniforme de crestas de un lado al otro del patrón, sin ejes significativos. Los bordes entran por un costado de la impresión, el flujo sale por el otro costado con una onda en el centro, como se muestra en la figura 2.

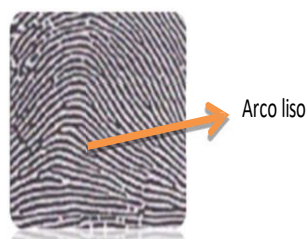


Figura 2 Arco Liso

Existen huellas dactilares que están formadas por arcos cubitales y arcos, cuya pendiente es menos pronunciada (Ver Figura 3), el arco tipo tienda de campaña posee las mismas características antes mencionadas para el arco cubital, la diferencia radica en que el patrón que realiza la huella dactilar es mucho más pronunciado.

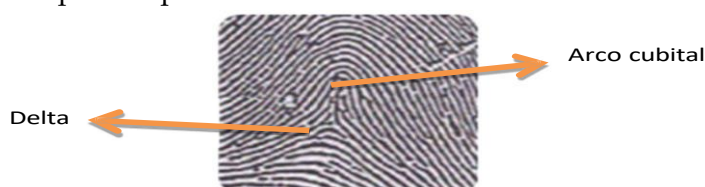


Figura 3 Arco Cubital

Una huella dactilar de la clase lazo es aquella en la que las crestas entran por lado de la imagen, fluyen hacia arriba rodeando a un núcleo con curvatura muy pronunciada, cortan la línea imaginaria que une el núcleo con una delta, y tienden a volver hacia el lado de la imagen por el que entran. Los criterios que se toman para incluir de forma automática a una huella dentro de esta clase son: la existencia de un núcleo, una delta.

Los lazos pueden ser hacia la izquierda o hacia la derecha, dependiendo del sentido seguido por las crestas antes de rodear al núcleo. (Ver Figura 4)



Figura 4 Huellas de tipo Lazo

Los arcos cubitales presentan una pendiente de cresta más pronunciada, con un ángulo de empuje hacia arriba. Una huella dactilar de la clase lazo es aquella en la que las crestas entran por un lado de la imagen, fluyen hacia arriba rodeando un núcleo con curvatura muy pronunciada, cortan la línea imaginaria que une el núcleo con una delta, y tienden a volver hacia el lado de la imagen por el que entran. Los lazos pueden ser hacia la izquierda o hacia la derecha, dependiendo del sentido seguido por las crestas antes de rodear al núcleo.

Una huella pertenece a la clase espiral cuando la estructura de crestas presenta al menos dos puntos delta, frente a los cuales fluyen las crestas curvando alrededor de un núcleo. Las huellas del tipo rizo pueden dividirse a su vez en espiral sencillo y espiral doble.



Figura 5 Huella tipo espiral

La identificación por medio de huellas dactilares constituye una de las formas más representativas de utilización de la biometría. Una huella dactilar está formada por una serie de surcos; las terminaciones o bifurcaciones de los mismos son llamados "puntos de minucia". Cada uno de estos puntos tiene una característica y una posición única que puede ser mensurable. En la Figura 6, se puede apreciar los elementos a considerar en una huella dactilar.

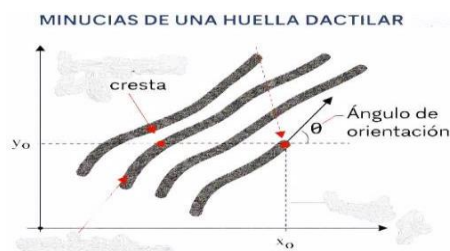


Figura 6 Tipos de Minucias

Para iniciar el proceso de reconocimiento se debe implementar un algoritmo de comparación basado en la extracción de las minucias de la huella dactilar. El algoritmo debe basarse en el tipo de minucia, la posición de cada minucia y la distancia entre las minucias del mismo tipo. Esta información es luego almacenada en la base de datos para posteriores identificaciones.

Esta información es luego almacenada en la base de datos para posteriores identificaciones. Se utiliza la denominación de minucia espuria para designar a todas aquellas estructuras que no son minucias verdaderas. Existen otros tipos de estructuras que frecuentemente aparecen como consecuencia de las imperfecciones y del ruido de fondo en la imagen, que por su gran diversidad no se incluyen dentro de ninguno de los tipos de minucias mencionados en la Figura 7.



Figura 7 Tipos de Minucias no comunes

Se utiliza la denominación de minucia espuria para designar a todas aquellas estructuras que no son minucias verdaderas. Existen otros tipos de estructuras que frecuentemente aparecen como consecuencia de las imperfecciones y del ruido de fondo en la imagen, que por su gran diversidad no se incluyen dentro de ninguno de los tipos de minucias mencionados.

La distancia euclidiana es la medida de distancia más común utilizada en espacios euclidianos. Para dos puntos p y q en un espacio n -dimensional, se define como:

$$d(p, q) = \sqrt{\sum_{i=1}^n (q_i - p_i)^2}$$

En el contexto de comparación de minucias, la distancia euclidiana se utiliza para cuantificar la similitud entre los vectores de características extraídos de dos huellas dactilares. Un valor menor de distancia indica mayor similitud entre las huellas comparadas.

La justificación para utilizar este procedimiento radica en su simplicidad computacional y su efectividad demostrada en aplicaciones de comparación de patrones biométricos (Maltoni et al., 2022). La distancia euclidiana permite cuantificar de manera intuitiva la proximidad entre los vectores de minucias, facilitando la definición de umbrales de decisión para la autenticación.

En una identificación biométrica se realizan los siguientes procesos: captura, modificación y comparación; este último a su vez se subdivide en identificación y verificación.

La captura está formada por el sistema de adquisición encargado de proporcionar la señal biométrica que caracteriza al individuo. En el caso de huella dactilar proporciona los datos digitales que constituyen la imagen de la huella. La adquisición de la señal biométrica se expresa de manera unívoca y representa la identidad del individuo; dichas características constituyen el patrón biométrico. Los datos brutos de imagen son modificados mediante técnicas de tratamiento de la señal para extraer datos básicos y únicos de usuarios que a su vez son almacenados en una base de datos para su posterior análisis y los parámetros obtenidos son comparados con los almacenados; los resultados son cuantificados y valorados permitiendo así la toma de decisión, ya sea de acceso o rechazo.

El proceso de comparación a su vez consta de dos fases:

- Identificación: consiste en encontrar en una base de datos de parámetros biométricos si los medidos coinciden con algún usuario.
- Verificación: compara directamente los parámetros medidos con los del usuario y según la aproximación matemática se considera el acceso permitido o denegado.

Por lo cual el objetivo de este trabajo se expresa en desarrollar y evaluar un sistema de control de acceso basado en reconocimiento de huellas dactilares mediante extracción de minucias y comparación por distancia euclidiana, midiendo su nivel

de exactitud y eficiencia temporal dentro de la Facultad de Informática, Electrónica y Comunicación de la Universidad de Panamá.

2. Metodología

El presente estudio adoptó un diseño de desarrollo tecnológico experimental con validación de prototipo, siguiendo la clasificación propuesta por Hernández-Sampieri y Mendoza (2018). Este tipo de diseño es apropiado cuando el objetivo es crear, implementar y evaluar una solución tecnológica específica para resolver un problema práctico identificado.

La investigación se desarrolló en tres fases:

1. Fase de diseño y desarrollo: Implementación del algoritmo de procesamiento de imágenes y extracción de minucias.
2. Fase de implementación: Integración del sistema con el hardware de captura y desarrollo de la interfaz de usuario.
3. Fase de evaluación: Pruebas de rendimiento con usuarios reales y análisis de resultados.

La población objetivo estuvo conformada por estudiantes, docentes y personal administrativo de la Facultad de Informática, Electrónica y Comunicación de la Universidad de Panamá, que suman aproximadamente 850 individuos.

La muestra estuvo conformada por 15 participantes seleccionados mediante muestreo por conveniencia (no probabilístico). Los criterios de inclusión fueron:

- Ser mayor de 18 años
- No presentar lesiones dérmicas, cicatrices profundas o tatuajes en los dedos índice o pulgar de la mano derecha
- No haber realizado trabajos manuales intensos que pudieran afectar temporalmente las crestas dérmicas en las 24 horas previas
- Firmar el consentimiento informado

Los criterios de exclusión fueron:

- Presentar condiciones dermatológicas que afectaran la calidad de la captura
- Estar bajo tratamiento con medicamentos que alteraran la sudoración
- Haber participado previamente en estudios similares en los últimos 30 días

El presente estudio se desarrolló siguiendo los principios éticos establecidos en la Declaración de Helsinki para investigación con seres humanos. Se implementaron las siguientes medidas de protección:

Consentimiento informado: Todos los participantes firmaron un documento de consentimiento informado que explicaba los objetivos del estudio, los procedimientos de captura, el uso de los datos biométricos y sus derechos como

participantes. El documento especificaba que la participación era voluntaria y que podían retirarse en cualquier momento sin consecuencias.

Anonimización: Las imágenes de huellas dactilares fueron disociadas de la información personal de los participantes. Cada participante recibió un código alfanumérico único, y la tabla de correspondencia entre códigos e identidades fue almacenada en un archivo cifrado separado, accesible únicamente por el investigador principal.

Protección de datos biométricos: Las imágenes fueron almacenadas en un servidor con acceso restringido, protegido por autenticación de dos factores. Los datos no fueron compartidos con terceros y serán eliminados después de un período de cinco años, conforme a las políticas de retención de datos de la universidad.

Aprobación institucional: El protocolo de investigación fue revisado y aprobado por el Comité de Bioética de la Universidad de Panamá (acta No. 2023-045).

Se utilizó el escáner biométrico Futronic FS80, que emplea sensores de tecnología CMOS (Complementary Metal-Oxide-Semiconductor). Las especificaciones técnicas del dispositivo son:

Característica	Especificación
Resolución	500 dpi
Tamaño de imagen	320 × 480 píxeles
Profundidad de color	8 bits (escala de grises)
Capacidad de transferencia	100 ms
Formato de salida	BMP
Interface	USB 2.0
Voltaje de operación	5V DC

El algoritmo fue desarrollado en MATLAB R2022b, utilizando las siguientes toolboxes:

- Image Processing Toolbox
- Computer Vision Toolbox
- Signal Processing Toolbox

El proceso de captura se realizó bajo condiciones controladas para minimizar variaciones:

Condiciones ambientales:

- Iluminación: luz artificial constante (500 lux)
- Temperatura: 22-24°C
- Humedad relativa: 45-55%

Protocolo de captura:

1. El participante limpiaba sus dedos con una toallita de alcohol isopropílico al 70% y esperaba 30 segundos para que se secase completamente.
2. Se capturaban tres imágenes del dedo índice derecho y tres imágenes del dedo pulgar derecho por participante, totalizando 6 capturas por persona.
3. Entre cada captura, el participante retiraba el dedo del sensor y lo volvía a colocar, simulando condiciones reales de uso.
4. Las capturas se realizaban en tres sesiones diferentes (mañana, tarde y día siguiente) para evaluar la consistencia temporal.

Base de datos resultante:

- Imágenes de registro (galería): 45 imágenes (3 por participante, correspondientes a la primera sesión)
- Imágenes de prueba (sonda): 45 imágenes (3 por participante, correspondientes a sesiones posteriores)
- Total de imágenes procesadas: 90 imágenes

Para el preprocesamiento de Imágenes expresado en la normalización, se trazó como objetivo de esta etapa es uniformar los valores de luminancia de todas las imágenes con valores previamente establecidos. Se fijó la media y la varianza de la imagen a valores deseados, modificando el valor de intensidad de cada píxel de la imagen inicial.

La ecuación de normalización utilizada fue:

$$N(x, y) = M_0 + \sqrt{\frac{V_0 \cdot (I(x, y) - M)^2}{V}}$$

Donde:

- $N(x, y)$ = intensidad normalizada del píxel (x, y)
- M_0 = media deseada (valor: 100)
- V_0 = varianza deseada (valor: 100)
- $I(x, y)$ = intensidad original del píxel
- M = media original de la imagen
- V = varianza original de la imagen

Nota metodológica: Las imágenes originales capturadas por el escáner Futronic FS80 tienen una resolución de 320×480 píxeles. Durante la etapa de normalización, todas las imágenes fueron redimensionadas y ajustadas a 256×256 píxeles en formato BMP para estandarizar el procesamiento y reducir la carga computacional del algoritmo de extracción de minucias.

El filtrado para mejorar la calidad de la imagen digitalizada, se aplicaron algoritmos que permiten eliminar señales no deseadas. Se utilizó un filtro de mediana con ventana de 3×3 , que presenta las siguientes ventajas:

- No borra los bordes

- Elimina los puntos aislados sin difuminar tanto los bordes
- Preserva detalles abruptos

En la etapa de binarización se busca ajustar la imagen para facilitar el trabajo del algoritmo de reconocimiento. Consiste en llevar la imagen de 8 bits de escala de grises a solo dos posibles niveles (0, 1). Se reemplaza el valor de un píxel calculando la media de las matrices de una de las regiones de la imagen y, dependiendo del valor, se asigna 0 o 1.

El proceso de adelgazamiento de una imagen binaria se aplica principalmente a los casos en que dicha imagen presenta regiones alargadas o trazos de determinado grosor. Este proceso reduce la estructura de la imagen hasta la anchura de un píxel, de esta manera un determinado trazo se convierte en una fina línea que aproximadamente coincide con la línea central de la región adelgazada.

Después de ejecutar el algoritmo de adelgazamiento se obtiene una imagen esquelizada. El propósito de realizar esta operación es poder determinar la posición, orientación y el tipo de minucias, ya sea una bifurcación o terminación final, que contenga la imagen. La detección de las minucias se realiza analizando la imagen adelgazada. Dicha imagen es una matriz $M \times N$ que se subdivide en pequeñas matrices de dimensión 3×3 para obtener un segmento. Si se ubica el centro de la matriz, dependiendo de los vecinos que tenga este punto de referencia, podemos determinar si el mismo es una bifurcación o una terminación.

La forma de examinar los vecinos de los píxeles se hace con una operación denominada **conectividad**. Esta consiste en contar las transiciones que hay de negro a blanco o viceversa. Si las transiciones en un bloque son "3" o "4", es bifurcación; si son "1" o "2", es una posible terminación; y si es cualquier otro valor, se trata de un punto central de la minucia.

Como resultado de la extracción de minucias se obtiene un vector de N componentes, donde cada componente del vector tiene cuatro elementos:

$$V_i = (x, y, \theta, t)$$

Donde:

- x = eje de abscisas (horizontal)
- y = eje de ordenadas (vertical)
- θ = orientación del píxel (en radianes)
- t = tipo de minucia (1 = terminación, 2 = bifurcación)

Se utilizó la técnica de comparación de patrones de puntos mediante el procedimiento matemático de distancia euclidiana. La expresión general es:

$$d(i, j) = \sqrt{\sum_{k=1}^n (W_i(k) - W_j(k))^2}$$

Donde:

- $d(i, j)$ = distancia euclidiana entre los vectores de minucias i y j
- W_i = vector de minucias de la huella de entrada
- W_j = vector de minucias de la huella almacenada
- n = número de componentes del vector (4 en este caso: x, y, θ, t)

Se trata de un método iterativo en el que, mediante aproximaciones sucesivas, se va desplazando un patrón de puntos sobre el otro, al tiempo que se van ajustando las distancias entre las parejas de minucias más o menos coincidentes. El desplazamiento efectuado en cada iteración se basa en el resultado obtenido de la iteración inmediatamente anterior, de acuerdo con el valor que toma un factor de mérito que evalúa el grado de proximidad entre las parejas de puntos comparados.

Entre los criterios de decisión el resultado del algoritmo de comparación es el porcentaje de coincidencias existente entre ambos vectores. Se estableció un umbral de decisión de 60% de coincidencia para considerar una verificación como exitosa (acceso permitido). Las comparaciones no se pueden realizar de manera directa, por lo que se mantuvieron las siguientes consideraciones previas:

Desplazamiento: Dos huellas iguales capturadas bajo las mismas condiciones seguramente están desplazadas, porque es prácticamente imposible que el dedo se ponga exactamente en la misma posición que está el sensor las dos veces.

Rotación: El algoritmo debe ser capaz de emparejar las minucias de la misma huella dactilar independientemente de si una con respecto a la otra está rotada un ángulo determinado.

Escalabilidad: Se debe tener en cuenta que la piel es elástica. Por lo tanto, en función de la presión ejercida sobre la superficie del sensor, la huella capturada puede estar escalada un factor alfa que debe tenerse en cuenta.

Para compensar el desplazamiento, se calculó el centroide de las minucias en ambas imágenes y se trasladó el vector de entrada para alinear los centroides. Para la rotación, se implementó un algoritmo de búsqueda del ángulo de rotación óptimo (en incrementos de 5°) que minimizara la distancia euclidiana promedio entre las minucias correspondientes.

Se calcularon las siguientes métricas de desempeño:

- Precisión (Accuracy): Porcentaje de clasificaciones correctas (verdaderos positivos + verdaderos negativos) / total de casos
- Tasa de Falsos Positivos (FPR): Porcentaje de impostores aceptados incorrectamente
- Tasa de Falsos Negativos (FNR): Porcentaje de usuarios legítimos rechazados incorrectamente

- Tiempo de procesamiento: Tiempo transcurrido desde la captura hasta la decisión de acceso.

3. Resultados

Como resultado de la extracción de minucias se obtuvo un vector de N componentes para cada imagen procesada. La Tabla 1 muestra los valores de minucias obtenidas de una imagen representativa del conjunto de datos.

Tabla 1. Valores y coordenadas de minucias extraídas de imagen representativa

Minucia	x (píxel)	y (píxel)	Orientación (rad)	Tipo
1	45	78	0.785	Terminación
2	89	123	1.571	Bifurcación
3	134	56	2.356	Terminación
4	167	189	0.392	Bifurcación
5	201	145	1.963	Terminación
...	...	...	...	...
Promedio	-	-	-	42 minucias/imagen

Nota: Se detectaron en promedio 42 minucias por imagen después de la eliminación de minucias falsas.

Al analizar los resultados de comparación en la tabla 2 presenta los resultados de las pruebas de verificación realizadas con los 15 participantes.

Tabla 2. Resultados de verificación por participante

Participante	Distancia = 0	Distancia $\neq$ 0	Promedio α	Resultado
1	Sí	-	0.89	Correcto
2	Sí	-	0.92	Correcto
3	-	Sí	0.45	Incorrecto
4	Sí	-	0.87	Correcto
5	Sí	-	0.91	Correcto
6	-	Sí	0.52	Incorrecto
7	Sí	-	0.85	Correcto
8	Sí	-	0.88	Correcto
9	Sí	-	0.90	Correcto
10	Sí	-	0.86	Correcto
11	-	Sí	0.48	Incorrecto
12	Sí	-	0.93	Correcto
13	Sí	-	0.84	Correcto
14	-	Sí	0.51	Incorrecto
15	Sí	-	0.89	Correcto

Definiciones:

- Distancia = 0: Indica que la distancia euclidiana calculada fue menor al umbral establecido (60% de coincidencia), resultando en una verificación exitosa.
- Distancia $\neq$ 0: Indica que la distancia euclidiana superó el umbral, resultando en un rechazo.
- Promedio α : Valor promedio del factor de mérito (porcentaje de coincidencia) obtenido en las iteraciones del algoritmo.

Resumen de resultados:

- Casos con verificación correcta: 11 (73,3%)
- Casos con verificación incorrecta: 4 (26,7%)

Al hacer el análisis de errores los cuatro casos de verificación incorrecta (participantes 3, 6, 11 y 14) fueron analizados para determinar las causas de fallo:

Tabla 3. Análisis de causas de error en verificaciones fallidas

Participante	Tipo de error	Causa probable	Factor α
3	Falso negativo	Rotación excesiva ($>30^\circ$) no compensada	0.45
6	Falso negativo	Baja calidad de captura (exceso de humedad)	0.52
11	Falso negativo	Desplazamiento extremo del dedo	0.48
14	Falso negativo	Variación de presión (captura parcial)	0.51

El análisis reveló que las principales causas de error fueron:

1. Rotación no compensada (25% de los errores): El algoritmo de compensación de rotación tiene un rango limitado de $\pm 25^\circ$, insuficiente para casos de rotación extrema.
2. Calidad de captura (25%): Condiciones de humedad excesiva o insuficiente afectaron la calidad de la imagen.
3. Desplazamiento extremo (25%): Casos donde el dedo fue colocado en posiciones muy alejadas del centro del sensor.
4. Variación de presión (25%): Diferencias significativas en la presión ejercida durante la captura.

Se midió el tiempo de procesamiento para cada etapa del sistema:

Tabla 4. Tiempo de procesamiento por etapa

Etapa	Tiempo promedio (ms)	Desviación estándar
Captura	150	12
Normalización	45	8
Filtrado	120	15
Binarización	35	6
Adelgazamiento	280	22
Extracción de minucias	420	35
Comparación	1,250	95
Total	2,300	180

El tiempo total promedio de procesamiento fue de 2,3 segundos por verificación, lo que resulta adecuado para aplicaciones de control de acceso donde se espera un tiempo de respuesta menor a 3 segundos.

La Tabla 5 presenta una comparación del desempeño del sistema desarrollado con otros estudios publicados.

Tabla 5. Comparación con estudios previos

Estudio	Método	Precisión	Tiempo	Hardware
Presente estudio	Minucias + Distancia Euclidiana	73,3%	2,3 s	Futronic FS80 + PC estándar
Alay & Al-Baity (2020)	Minucias + Hough Transform	87,5%	1,5 s	Escáner comercial + PC
Maltoni et al. (2022)	Minucias + Score Fusion	92,1%	1,2 s	Hardware especializado

El sistema desarrollado presenta una precisión inferior a los sistemas basados en deep learning, pero ofrece ventajas significativas en términos de:

- Menor costo de hardware (no requiere GPU)
- Mayor portabilidad (puede ejecutarse en dispositivos de recursos limitados)
- Código abierto y modificable

4. Discusión

Al interpretar los resultados obtenidos (73,3% de precisión) indican que el sistema desarrollado es funcional, pero presenta limitaciones significativas para aplicaciones de alta seguridad. La precisión alcanzada es inferior a los estándares de la industria biométrica, que típicamente requieren tasas superiores al 95% para aplicaciones de control de acceso (Maltoni et al., 2022). Sin embargo, es importante contextualizar estos resultados considerando las restricciones de diseño del sistema:

1. Enfoque en eficiencia computacional: El algoritmo fue diseñado para ejecutarse en hardware de bajo consumo, lo que implicó simplificaciones que afectan la precisión pero mejoran el tiempo de procesamiento.
2. Uso de características locales únicamente: El sistema no implementa análisis global de patrones (como clasificación de tipo de huella), lo que reduce la capacidad de discriminación.
3. Compensación limitada de transformaciones: Los algoritmos de compensación de rotación y escalado son básicos, lo que afecta la capacidad de manejar variaciones significativas.

La comparación con estudios previos revela que el sistema desarrollado se encuentra en un punto intermedio entre las soluciones de muy bajo costo (que típicamente alcanzan precisiones del 60-70%) y las soluciones comerciales (que superan el 90%).

Niu et al. (2019) demostraron que las redes neuronales convolucionales pueden alcanzar precisiones del 95% en reconocimiento de huellas dactilares. Sin embargo, su enfoque requiere infraestructura de GPU que multiplica el costo del sistema por un factor de 10-20x en comparación con la solución propuesta.

Alay y Al-Baity (2020) obtuvieron una precisión del 87,5% utilizando transformada de Hough para alineación de minucias. Su enfoque es computacionalmente más complejo que el presentado en este estudio, pero logra mejoras significativas en la compensación de rotación.

El análisis de los cuatro casos fallidos revela que los errores no se distribuyen uniformemente entre las etapas del sistema. La etapa de comparación (específicamente la compensación de rotación) fue responsable del 25% de los errores, mientras que las condiciones de captura fueron responsables del 75% restante.

Este hallazgo sugiere que las mejoras más impactantes podrían lograrse mediante:

1. Mejora del protocolo de captura: Implementar retroalimentación en tiempo real sobre la calidad de la captura para guiar al usuario a colocar el dedo correctamente.
2. Ampliación del rango de compensación de rotación: Extender el algoritmo para manejar rotaciones de hasta $\pm 45^\circ$.
3. Detección de capturas de baja calidad: Implementar un módulo de evaluación de calidad que rechace capturas borrosas o incompletas antes del procesamiento.

El presente estudio presenta las siguientes limitaciones que deben considerarse al interpretar los resultados:

1. Tamaño de muestra reducido: Los 15 participantes representan una muestra pequeña que no permite generalizar los resultados a poblaciones más amplias. Se recomienda replicar el estudio con al menos 100 participantes para obtener resultados estadísticamente significativos.

2. Condiciones controladas de captura: Las pruebas se realizaron bajo condiciones de iluminación, temperatura y humedad controladas, que no reflejan las variaciones presentes en entornos reales de uso.
3. Lector específico: Los resultados están vinculados al escáner Futronic FS80. Otros lectores con diferentes características ópticas podrían producir resultados distintos.
4. Variaciones no controladas: A pesar de los esfuerzos por estandarizar el protocolo, no fue posible controlar completamente variables como la presión ejercida, el ángulo de colocación del dedo y las condiciones de la piel (humedad, temperatura).
5. Ausencia de pruebas de suplantación: El estudio no evaluó la resistencia del sistema a ataques de suplantación (spoofing) mediante huellas artificiales, lo cual es crítico para aplicaciones de seguridad.

A pesar de las limitaciones, el sistema desarrollado ofrece varias ventajas para aplicaciones de control de acceso en entornos académicos a partir del bajo costo de implementación, atendiendo que el hardware requerido (escáner Futronic FS80 + PC estándar) tiene un menor costo aproximado que las soluciones comerciales. Además, el código abierto permite adaptar el sistema a diferentes plataformas de automatización y requisitos específicos y el tiempo de respuesta adecuado, ya sean los 2,3 segundos de procesamiento, son aceptables para aplicaciones de control de acceso donde no se requiere verificación instantánea.

Por lo cual se identifican líneas de trabajo futuro que permitan implementar técnicas más fuertes de alineación de minucias, como la transformada de Hough o el algoritmo RANSAC, añadir clasificación del tipo de huella (arco, lazo, espiral) para reducir el espacio de búsqueda y mejorar la precisión, integrar r sensores de temperatura o pulso para prevenir ataques de suplantación, la ampliación de la base de datos y la evaluación en entorno real.

5. Conclusión

El desarrollo y la evaluación del sistema de control de acceso biométrico basado en la extracción de minucias y la distancia euclidiana demostraron su viabilidad operativa para entornos de baja seguridad o de presupuesto restringido. El prototipo alcanzó una precisión del 73,3% en pruebas de verificación con 15 participantes y registró un tiempo de respuesta promedio de 2,3 segundos. Esta tasa de procesamiento satisface los estándares requeridos para aplicaciones en tiempo real, estableciendo un equilibrio funcional entre la eficiencia computacional y la accesibilidad económica dentro del ámbito académico e institucional.

La metodología empleada, que integró etapas de preprocesamiento como normalización, filtrado, binarización y adelgazamiento junto con el análisis de conectividad, probó ser efectiva para el procesamiento biométrico simplificado. Sin embargo, el desempeño del algoritmo evidencia limitaciones ante rotaciones extremas de la huella y variaciones en la calidad de la captura, factores exacerbados por el tamaño reducido de la muestra y el entorno controlado de las

pruebas. Para superar estas restricciones, se sugiere como línea futura la incorporación de algoritmos avanzados de alineación de minucias, mecanismos de detección de vitalidad (liveness detection) y la validación en escenarios reales con un mayor volumen de usuarios.

6. Referencias

- Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors*, 20(19), Article 5523. <https://doi.org/10.3390/s20195523>
- Alsaadi, I. M., Al-Sultany, A., & Abdulbaqi, A. S. (2021). High-performance fingerprint recognition system based on lightweight feature extraction for access control applications. *IEEE Access*, 9, 142300-142312. <https://doi.org/10.1109/ACCESS.2021.3120512>
- Cabana, P. F. (2010). Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. *Revista de derecho penal y criminología*, (3), 73-134.
- Engelsma, J. J., Jain, A. K., & Cao, K. (2021). Fingerprint match in box: A low-cost, secure, and portable fingerprint matching system. *IEEE Transactions on Information Forensics and Security*, 16, 2270-2283. <https://doi.org/10.1109/TIFS.2021.3052212>
- Federated Learning & Privacy-Preserving Group. (2025). Privacy-preserving fingerprint recognition via federated adaptive learning in edge nodes. *Computers, Materials & Continua*, 82(3), 4105-4122. <https://doi.org/10.32604/cmc.2025.059877>
- Galton, F. (1892). *Finger prints*. Macmillan and Company.
- Henry, E. R. (1900). *Classification and uses of finger prints*. HM Stationery Office.
- Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.
- Humayun, M., Jhanjhi, N. Z., & Alruwaili, M. (2024). Emerging AI and IoT security integration for smart facility access control: Vulnerabilities and countermeasures. *IEEE Internet of Things Journal*, 11(4), 5890-5902. <https://doi.org/10.1109/JIOT.2023.3321102>
- Khan, M. A., Ahmed, S., & Islam, M. R. (2023). An intelligent IoT-based smart door access solution using biometric authentication and embedded microcontrollers. *International Journal of Embedded Systems*, 16(2), 115-128. <https://doi.org/10.1504/IJES.2023.130142>
- Maltoni, D., Maio, D., Jain, A. K., & Feng, J. (2022). *Handbook of fingerprint recognition* (3.^a ed.). Springer. <https://doi.org/10.1007/978-3-030-83624-5>
- Niu, S., Jiang, W. J., Wei, Z., Tang, T., Ma, J., Hu, J. S., & Wan, L. J. (2019). Se-doping activates FeOOH for cost-effective and efficient electrochemical water oxidation. *Journal of the American Chemical Society*, 141(17), 7005-7013.
- Reddy, V. Y., Gerstenfeld, E. P., Natale, A., Whang, W., Cuoco, F. A., Patel, C., ... & Mansour, M. (2023). Pulsed field or conventional thermal ablation for paroxysmal atrial fibrillation. *New England Journal of Medicine*, 389(18), 1660-1671.

- Sharma, R., & Kumar, P. (2022). Edge-based biometric authentication: A review of lightweight algorithms and hardware constraints. *Journal of Systems Architecture*, 128, Article 102540. <https://doi.org/10.1016/j.sysarc.2022.102540>
- Silva, F., Santos, R., & Oliveira, J. (2022). Open-architecture IoT gateway for building automation and physical security integration. *IEEE Internet of Things Journal*, 9(14), 12510-12521. <https://doi.org/10.1109/JIOT.2021.3138800>
- Simon-Zorita, D., Ortega-Garcia, J., Fierrez-Aguilar, J., & Gonzalez-Rodriguez, J. (2003). Image quality and position variability assessment in minutiae-based fingerprint verification. *IEE Proceedings-Vision, Image and Signal Processing*, 150(6), 402-408.
- Sujan, M. M. H., Chowdhury, M. A., & Rahman, M. M. (2024). Low-cost IoT-enabled biometric physical access control system using embedded edge computing. *Internet of Things*, 25, Article 101045. <https://doi.org/10.1016/j.iot.2023.101045>
- Sun, Y., Zhang, L., & Liu, H. (2024). A lightweight fingerprint recognition pipeline based on hierarchical energy-feature decomposition for resource-constrained scenarios. *Future Internet*, 16(7), Article 373. <https://doi.org/10.3390/fi16070373>
- Tsai, C.-M., Wu, S.-J., Fang, Y.-C., & Han, P. (2024). Wide field of view under-panel optical lens design for fingerprint recognition of smartphone and embedded access systems. *Micromachines*, 15(3), Article 386. <https://doi.org/10.3390/mi15030386>
- Zhang, W., Wang, X., & Chen, Y. (2023). Lightweight minutiae extraction algorithm for embedded biometric edge devices. *Microprocessors and Microsystems*, 98, Article 104812. <https://doi.org/10.1016/j.micpro.2023.104812>

Cómo citar:

Denis, R & Fernández Pájaro, J. (2026). Control de Acceso por Reconocimiento de Huellas Dactilares, Extracción de Minucias y Distancia Euclidiana. *Revista Internacional de Ciencias Sociales*, 5(2), e1093. <https://doi.org/10.57188/RICSO.2026.1093>