DISEÑO Y DOCUMENTACION DEL HARDWARE

Andrea Tatiana Acuña Prada

.1096959406

Angie Alejandra Cadena Lizarazo

1005540911

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de Ciencias Naturales e Ingenierías

Ingeniería de Telecomunicaciones

INTRODUCCIÓN

El reconocimiento de iris es una tecnología biométrica que destaca por su alta precisión y fiabilidad. A diferencia de otras características biométricas como las huellas dactilares o el reconocimiento facial, el iris humano no cambia significativamente con el tiempo, lo que lo convierte en una excelente herramienta para sistemas de autenticación de identidad. Cada iris posee un patrón único formado por estructuras complejas que permiten una identificación altamente confiable incluso entre gemelos idénticos (Didácticas Electrónicas, s.f.). Esta característica ha impulsado su uso en escenarios que requieren altos niveles de seguridad, como aeropuertos, bancos, y centros de investigación.

A pesar de su potencial, la adopción comercial de esta tecnología se ha visto limitada por el alto costo de los equipos especializados. Por tanto, el presente documento plantea un diseño de hardware de bajo costo, centrado en el reconocimiento de iris, que aprovecha componentes accesibles y de fácil implementación sin sacrificar la calidad en la captación, procesamiento, autenticación y almacenamiento de los datos. Así mismo, se integra el marco legal colombiano en el tratamiento de datos biométricos para garantizar la ética y legalidad del sistema propuesto.

VISIÓN GENERAL DEL SISTEMA

El sistema se estructura en cuatro etapas principales, interconectadas para formar un flujo de procesamiento continuo y eficiente. Estas etapas son: captura de imágenes, procesamiento y preprocesamiento, autenticación y almacenamiento/comunicación. Cada una está pensada para cumplir un rol específico y alinearse con los principios de un sistema biométrico efectivo, es decir: unicidad, permanencia, colectabilidad, rendimiento, aceptabilidad y resistencia al fraude.

1. CAPTURA DE IMÁGENES (APLICADO AL IRIS) La calidad de la imagen capturada es fundamental, ya que afecta directamente la eficacia de los algoritmos de segmentación y comparación. Se requiere una imagen bien iluminada, enfocada y centrada del iris, que permita distinguir con claridad sus patrones característicos.

Para ello, se utilizan cámaras adaptadas para captar en el espectro infrarrojo cercano (NIR), lo que reduce el impacto de la luz visible y mejora el contraste de las estructuras internas del iris sin generar molestias para el usuario. El uso de módulos de cámaras USB modificadas o cámaras CSI como la Raspberry Pi Camera V2 permite lograr este objetivo con costos relativamente bajos.

Además, el sistema de iluminación con LEDs IR mejora la visibilidad del iris en ambientes de baja luz. Estos LEDs, controlados mediante pines GPIO, se colocan de forma que no generen reflejos especulares que interfieran con la imagen capturada.

Figura 1 Raspberri PI4 sistema para capturas de imágenes

2. PROCESAMIENTO Y PREPROCESAMIENTO (APLICADO AL IRIS)

   Tras la captura de la imagen, es necesario aplicar una serie de transformaciones que permitan extraer información relevante del iris y prepararla para la comparación. Este proceso incluye:

- **Segmentación**: Identificación del contorno del iris, excluyendo párpados y pestañas.
- **Normalización**: Transformación de la imagen circular del iris a una representación rectangular normalizada.
- **Extracción de características**: Aplicación de filtros (como Gabor) para obtener un vector característico.

Para ello, se recomienda el uso de bibliotecas como OpenCV, que ofrece herramientas robustas para el tratamiento de imágenes, y plataformas de bajo consumo como Raspberry Pi, que permiten la ejecución local del código sin necesidad de hardware externo costoso. En aplicaciones más exigentes, el Jetson Nano de NVIDIA permite el uso de redes neuronales convolucionales para una segmentación y extracción de características más precisas.

3. AUTENTICACIÓN (APLICADO AL IRIS)

   La autenticación es el núcleo del sistema. Implica comparar los vectores de características extraídas del iris con los almacenados previamente en una base de datos segura. La autenticación puede realizarse de forma binaria (aceptar/rechazar) o mediante una puntuación de similitud.

Existen dos enfoques principales:

- **Métodos Clásicos**: Como las transformadas de Gabor, que generan un código binario del iris que puede compararse rápidamente mediante operaciones lógicas XOR.
- **Aprendizaje profundo**: Uso de modelos entrenados con redes neuronales profundas para detectar coincidencias. Herramientas como TensorFlow y PyTorch permiten desarrollar clasificadores personalizados o reutilizar modelos preentrenados adaptados al reconocimiento de iris.

La elección depende del entorno: en sistemas de control de acceso rápido, los métodos clásicos son preferibles por su eficiencia. Para sistemas de vigilancia o investigación, el aprendizaje profundo ofrece mayor adaptabilidad.

4. ALMACENAMIENTO Y COMUNICACIÓN (APLICADO AL IRIS)

   El almacenamiento de datos biométricos requiere protección especial, dada su sensibilidad. Se propone una base de datos local para eliminar la dependencia de servidores remotos y evitar vulnerabilidades por exposición en redes públicas.

Se implementan medidas como:

- **Cifrado AES-256** para los vectores biométricos.
- **Controles de acceso** a nivel de sistema operativo.
- **Auditorías de acceso** para registrar intentos de uso indebido.

La comunicación puede establecerse mediante interfaces WiFi o BLE para conectarse con sistemas de autenticación centralizados, siempre manteniendo la protección de la información en tránsito mediante protocolos seguros como HTTPS o VPN.

DIAGRAMA DE BLOQUES DEL SISTEMA

Representa la arquitectura general del sistema de reconocimiento de iris, en la que cada bloque funcional está orientado al flujo secuencial desde la captura de datos hasta la validación biométrica:

1. Captura de imágenes (cámara IR)
2. Iluminación controlada (LEDs IR + GPIO)
3. Procesamiento (Raspberry Pi o Jetson Nano + OpenCV/TensorFlow)
4. Comparación y autenticación (modelo IA o transformada de Gabor)
5. Almacenamiento cifrado y comunicación segura (base de datos local + WiFi/BLE)

LISTA DE MATERIALES (AMPLIADA Y ARGUMENTADA)

Componente	**Opciones**	**Justificación Técnica**
Cámara	USB IR o Raspberry Pi V2	Permite capturar detalles del iris con buena resolución y sensibilidad al IR
Procesador	Raspberry Pi 4 / Jetson Nano	Ejecuta algoritmos de segmentación, extracción y clasificación en tiempo real
Iluminación	LEDs IR + resistencias + transistores	Mejora la visibilidad sin molestar al usuario y sin afectar la calidad de la imagen

Fuente de poder	Adaptador 5V 2-3A o baterías Li-Ion	Alimenta el sistema de forma estable, permitiendo portabilidad
Almacenamiento	microSD / SSD externo	Guarda datos biométricos con acceso rápido y seguro
Software	OpenCV, TensorFlow, PyTorch	Librerías de código abierto que permiten adaptabilidad y flexibilidad del sistema

INSTRUCCIONES DE ENSAMBLAJE (AMPLIADAS)

1. *Montaje de la cámara*: Fijarla a nivel de los ojos, asegurando estabilidad con soporte ajustable.
2. *Conexionado*: Conectar la cámara al procesador (CSI o USB) y verificar alimentación adecuada.
3. *Iluminación*: Instalar LEDs IR con su controlador (transistores, resistencias) y probar iluminación en condiciones oscuras.
4. *Configuración de sistema operativo*: Instalar Raspbian o Ubuntu, luego OpenCV y TensorFlow.
5. *Calibración de softwar*e: Ejecutar pruebas de captura, ajustar niveles de exposición y filtros para optimizar contraste del iris.
6. *Validación funcional*: Probar con múltiples usuarios para asegurar tasa de aceptación y rechazo adecuadas.

ETICA Y MARCO NORMATIVO EN COLOMBIA (AMPLIADO)

El uso de datos biométricos en Colombia está regulado por la Ley 1581 de 2012, que establece los principios para el tratamiento de datos personales, y por el Decreto 1377 de 2013, que reglamenta dicha ley. Los datos biométricos como el iris están clasificados como "datos sensibles", lo que implica:

- *Autorización previa y expresa* por parte del titular.
- *Finalidad claramente informada* antes de la recolección.
- *Prohibición de acceso a terceros no autorizados*.
- *Garantía del derecho de habeas data*: el titular puede conocer, actualizar y rectificar sus datos.

La Superintendencia de Industria y Comercio es la entidad encargada de vigilar y sancionar el uso indebido de estos datos. Cualquier implementación de sistemas de reconocimiento de iris

debe contemplar protocolos de consentimiento informado, almacenamiento cifrado y transparencia sobre el uso de la información.

CONCLUSIÓN

El sistema diseñado representa una solución viable para la autenticación biométrica mediante el reconocimiento de iris. La selección de componentes económicos, combinados con algoritmos avanzados de procesamiento y aprendizaje profundo, permite implementar soluciones escalables y adaptables a diferentes contextos. Además, el cumplimiento del marco normativo colombiano asegura que la recolección y tratamiento de datos se haga de forma ética y legal. Esto convierte al proyecto no solo en una propuesta técnicamente eficiente, sino también socialmente responsable y legalmente fundamentada.

BIBLIOGRAFÍA

1. Caicedo Marmolejo, R., & Chinchilla, F. (2012). *Sistema de identificación por reconocimiento de iris utilizando transformada de Gabor*. Universidad del Valle.
2. Ferrer Barrientos, A., & Rodríguez Gómez, M. (2013). *Desarrollo de un sistema biométrico embebido basado en Raspberry Pi*. Universidad Politécnica de Madrid.
3. García Maya, J., & Moreno Ruiz, A. (2014). *Reconocimiento biométrico utilizando aprendizaje profundo en hardware Jetson Nano*. Universidad Autónoma de Madrid.
4. Merino Barbancho, J. (2016). *Aplicación del deep learning al reconocimiento biométrico en sistemas de bajo costo*. Universidad de Málaga.
5. Orozco-Rosas, U., Sánchez-Pérez, G., & Lara-Alvarez, C. (2012). *Evaluación de métodos de reconocimiento de iris en condiciones no controladas*. Revista Iberoamericana de Inteligencia Artificial, 15(49), 34-42.
6. Valencia Murillo, J. D., & Cruz Ardila, M. (2014). *Implementación de técnicas de procesamiento digital para biometría de iris*. Universidad Distrital Francisco José de Caldas.
7. Yonekura Baeza, J. (2014). *Diseño de sistemas biométricos multimodales y su aplicación en seguridad electrónica*. Pontificia Universidad Católica del Perú.
8. Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.
9. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2013). *Decreto 1377 de 2013. Reglamenta la Ley 1581 de 2012*.