Reporte de Proyecto: Sistema de Control de Acceso Biométrico

Autor: Eduardo Gonzalez Gonzalez

Resumen Ejecutivo

Este reporte detalla el diseño, desarrollo e implementación de un sistema de control de acceso biométrico basado en reconocimiento facial. El proyecto fue concebido para abordar la creciente necesidad de soluciones de seguridad eficientes y accesibles, especialmente para microempresas y pequeños emprendimientos que a menudo enfrentan limitaciones presupuestarias para adquirir sistemas de seguridad convencionales de alto costo. A través de la integración de hardware de bajo costo como la Raspberry Pi Zero 2W y software de código abierto como OpenCV y Flask, se logró construir un sistema robusto capaz de identificar usuarios con una precisión del 90% y gestionar el acceso a áreas restringidas de manera efectiva. El enfoque principal del proyecto fue demostrar la viabilidad de una solución de seguridad avanzada que no comprometa la calidad ni la fiabilidad, ofreciendo una alternativa superior a los métodos tradicionales de control de acceso, como tarjetas o contraseñas, que son susceptibles a extravíos o vulnerabilidades.

1. Introducción

La seguridad se ha consolidado como un pilar fundamental en la sociedad contemporánea, abarcando desde la protección de datos personales hasta la salvaguarda de bienes materiales y la integridad física en diversos entornos. En un mundo cada vez más interconectado y digitalizado, la evolución de las amenazas y los riesgos ha impulsado la demanda de sistemas de seguridad más sofisticados y adaptables. Sin embargo, la implementación de estas tecnologías a menudo se ve obstaculizada por los elevados costos asociados a su desarrollo y mantenimiento, lo que limita su adopción por parte de entidades con recursos limitados. Esta disparidad crea una brecha significativa en la protección, dejando a muchas organizaciones vulnerables a incidentes de seguridad.

En este contexto, el presente proyecto surge como una respuesta innovadora a esta problemática. Mi objetivo fue desarrollar un sistema de control de acceso que no solo

fuera tecnológicamente avanzado y altamente efectivo, sino también económicamente viable. La elección del reconocimiento facial como tecnología central se fundamenta en su inherente capacidad para ofrecer una autenticación robusta y única, superando las deficiencias de los métodos tradicionales que dependen de elementos físicos o información memorizada. La singularidad de los rasgos faciales de cada individuo proporciona una capa de seguridad intrínseca que es difícil de replicar o comprometer. Este proyecto no solo busca mitigar riesgos, sino también democratizar el acceso a tecnologías de seguridad de vanguardia, permitiendo que un espectro más amplio de usuarios y organizaciones puedan beneficiarse de una protección avanzada sin incurrir en gastos prohibitivos. A lo largo de este reporte, se detallarán los aspectos técnicos, la metodología empleada, los resultados obtenidos y las conclusiones derivadas de este esfuerzo, destacando cómo se logró un equilibrio entre innovación, accesibilidad y aplicabilidad práctica en el ámbito de la seguridad biométrica.

2. Planteamiento del Problema y Objetivos

2.1. Planteamiento del Problema

La dependencia de métodos de seguridad tradicionales, como tarjetas de acceso o contraseñas, presenta vulnerabilidades inherentes que pueden comprometer la integridad de los sistemas de control. Las tarjetas pueden ser extraviadas, robadas o duplicadas, mientras que las contraseñas son susceptibles a ser olvidadas, adivinadas o interceptadas. Estas deficiencias no solo representan un riesgo de seguridad, sino que también pueden generar ineficiencias operativas y costos adicionales asociados a la gestión de reemplazos o restablecimientos. Para microempresas y pequeños emprendimientos, la inversión en sistemas de seguridad de alta gama a menudo no es factible, lo que los obliga a optar por soluciones de menor costo que, paradójicamente, pueden no ofrecer el nivel de protección necesario, aumentando su exposición a riesgos. Esta situación subraya la necesidad crítica de desarrollar soluciones de seguridad que sean tanto efectivas como económicamente accesibles, sin sacrificar la fiabilidad o la precisión.

2.2. Objetivos del Proyecto

El desarrollo de este sistema de control de acceso biométrico se guio por un conjunto claro de objetivos, diseñados para asegurar que la solución final fuera integral y respondiera eficazmente a las necesidades identificadas:

2.2.1. Objetivo General

Diseñar e implementar un sistema de control de acceso seguro, preciso y económico, utilizando la tecnología de reconocimiento facial para la autenticación de usuarios en entornos restringidos. El objetivo principal fue crear una solución que fuera superior a los métodos tradicionales en términos de seguridad y conveniencia, al mismo tiempo que se mantuviera accesible para un amplio rango de usuarios y organizaciones.

2.2.2. Objetivos Específicos

Para alcanzar el objetivo general, se establecieron los siguientes objetivos específicos:

- **Desarrollo de un Algoritmo de Reconocimiento Facial de Alta Precisión:** Se buscó implementar y optimizar un algoritmo de reconocimiento facial capaz de identificar a los usuarios con un alto grado de fiabilidad, minimizando la tasa de
  falsos positivos y falsos negativos. Esto implicó la selección cuidadosa de técnicas de procesamiento de imágenes y algoritmos de aprendizaje automático adecuados para el entorno de hardware de bajo costo.

- **Integración de Sensores y Hardware para el Control de Acceso:** Se diseñó y se integró un conjunto de componentes de hardware, incluyendo una Raspberry Pi
  Zero 2W, una cámara OV5647 y sensores de movimiento (PIR) y de contacto (MC-38), para construir una unidad de control de acceso física. La integración se centró en la eficiencia energética y la compatibilidad entre los componentes para asegurar un funcionamiento sin interrupciones.

- **Establecimiento de un Enlace con una Base de Datos para la Gestión de Usuarios y Eventos:** Se implementó un sistema de gestión de base de datos para almacenar de forma segura la información de los usuarios autorizados y registrar todos los eventos de acceso. Esto permitió una administración centralizada de los permisos y un seguimiento detallado de las actividades, facilitando la auditoría y la toma de decisiones informadas en materia de seguridad.

Estos objetivos fueron fundamentales para guiar cada fase del proyecto, desde la investigación inicial hasta la implementación y las pruebas finales, asegurando que el sistema desarrollado fuera una solución completa y efectiva para el control de acceso biométrico.

3. Metodología y Desarrollo

El desarrollo de este sistema de control de acceso biométrico se llevó a cabo mediante una metodología estructurada que abarcó tanto el diseño de hardware como la implementación de software, garantizando la cohesión y la funcionalidad de todos los
componentes. La aproximación metodológica se dividió en varias fases clave, cada una con sus propios objetivos y entregables, lo que permitió una gestión eficiente del proyecto y una iteración constante para optimizar el rendimiento y la seguridad del sistema.

3.1. Análisis de Requerimientos

La fase inicial consistió en un análisis exhaustivo de los requerimientos funcionales y no funcionales del sistema. Los requerimientos funcionales incluyeron la captura de imágenes faciales, la autenticación de usuarios mediante reconocimiento facial, la gestión de una base de datos de usuarios, la capacidad de otorgar o denegar acceso, y la implementación de un sistema de autenticación de dos factores (reconocimiento facial más PIN). Los requerimientos no funcionales se centraron en la seguridad del sistema (protección contra accesos no autorizados y manipulación de datos), la escalabilidad (capacidad de manejar un número creciente de usuarios y eventos), la usabilidad (interfaz intuitiva y fácil de usar) y la eficiencia (bajo consumo de recursos y tiempo de respuesta rápido).

3.2. Metodología de Diseño e Implementación

La metodología de diseño e implementación se centró en la integración de componentes de hardware y software para crear una solución unificada:

3.2.1. Arquitectura de Software

La arquitectura de software se diseñó para ser modular y escalable, facilitando el desarrollo y el mantenimiento. Se adoptó un enfoque basado en microservicios, donde cada componente del sistema (captura de imagen, procesamiento facial, base de datos, interfaz de usuario) operaba de forma independiente pero interconectada. Esto permitió una mayor flexibilidad y la capacidad de actualizar o reemplazar módulos sin afectar la funcionalidad general del sistema. Se utilizó Python como lenguaje de programación principal debido a su versatilidad y la riqueza de sus librerías para visión

por computadora y desarrollo web.

3.2.2. Diseño del Hardware

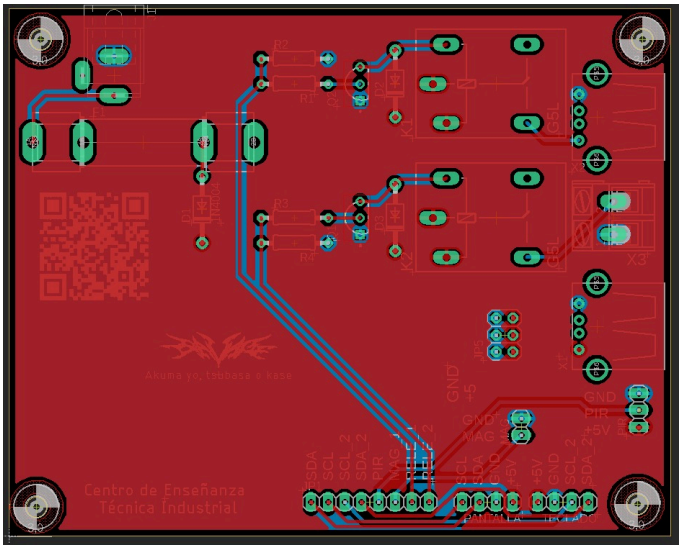
El diseño del hardware se centró en la selección de componentes de bajo costo y alta eficiencia energética. La Raspberry Pi Zero 2W fue elegida como el cerebro del sistema debido a su tamaño compacto, bajo consumo de energía y capacidad de procesamiento suficiente para las tareas de reconocimiento facial. Se integró una cámara OV5647 para la captura de imágenes de alta resolución, y sensores PIR (infrarrojos pasivos) y MC-38 (contacto magnético) para detectar la presencia de personas y el estado de la puerta,
respectivamente. El diseño incluyó la creación de un diagrama de bloques detallado y un esquema eléctrico para asegurar la correcta interconexión de todos los componentes.

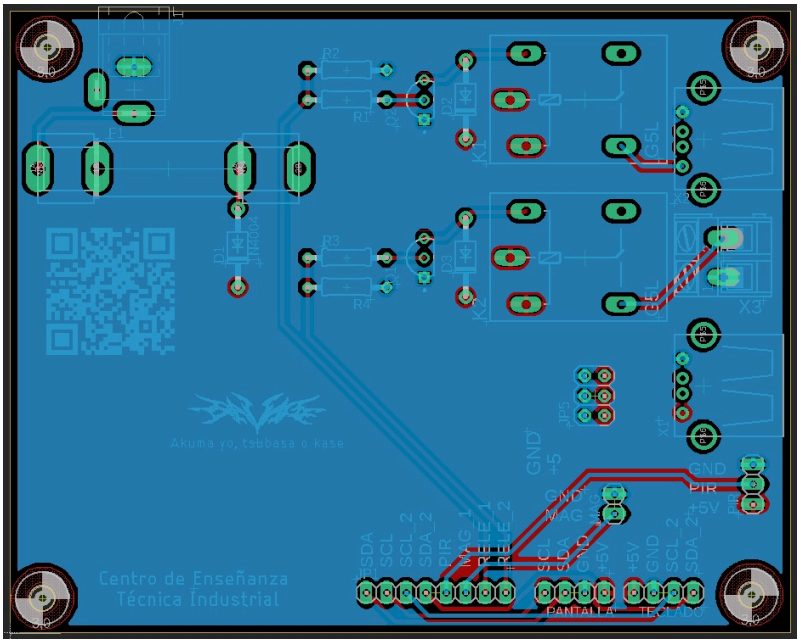
3.2.3. Selección de Componentes

La selección de componentes se basó en criterios de costo, disponibilidad, rendimiento y compatibilidad. Además de la Raspberry Pi y la cámara, se eligieron módulos de relé para el control de la cerradura eléctrica, LEDs indicadores para el estado del sistema, y una fuente de alimentación adecuada para todos los componentes. Se priorizaron los componentes que ofrecieran una buena relación calidad-precio y que fueran fáciles de integrar en el prototipo.

3.2.4. Diseño del Circuito y PCB

Se diseñó un circuito impreso (PCB) personalizado para integrar de manera compacta y eficiente todos los componentes electrónicos. El diseño de la PCB se realizó utilizando Altium Designer, lo que permitió optimizar el espacio, minimizar el ruido eléctrico y asegurar la fiabilidad de las conexiones. El objetivo fue crear una solución compacta y robusta que pudiera ser fácilmente replicable.





3.2.5. Diseño del Chasis

Para proteger los componentes electrónicos y proporcionar una estética profesional, se diseñó un chasis personalizado utilizando SolidWorks. El diseño del chasis consideró la ventilación adecuada, la accesibilidad a los puertos y la facilidad de montaje y desmontaje. Se buscó un diseño que fuera funcional y estéticamente agradable, adecuado para su implementación en diversos entornos.

3.2.6. Implementación del Software

La implementación del software se centró en el desarrollo de los siguientes módulos clave:

- **Algoritmo de Reconocimiento Facial:** Se utilizó la librería OpenCV, implementando el algoritmo Local Binary Patterns Histograms (LBPH) para el

reconocimiento facial. Este algoritmo es conocido por su eficiencia y su capacidad para trabajar con recursos computacionales limitados, lo que lo hizo ideal para la Raspberry Pi. Se desarrolló un proceso de entrenamiento para el modelo, utilizando un conjunto de datos de imágenes faciales de usuarios autorizados.

- **Sistema de Autenticación de Dos Factores:** Para aumentar la seguridad, se implementó un sistema de autenticación de dos factores que combina el reconocimiento facial con un PIN numérico. Después de una identificación facial
exitosa, el usuario debe ingresar un PIN predefinido para obtener
acceso, añadiendo una capa adicional de protección.

- **Registro de Eventos:** Se desarrolló un módulo para registrar todos los eventos de acceso, incluyendo la fecha, hora, usuario y resultado del intento de acceso (acceso concedido o denegado). Esta información se almacena en una base de datos y es accesible para fines de auditoría y monitoreo.

- **Modo Administrador:** Se implementó un modo administrador que permite a los usuarios autorizados gestionar la base de datos de usuarios, añadir o eliminar perfiles, y configurar los parámetros del sistema a través de una interfaz web
segura desarrollada con Flask.

3.2.7. Configuración del Entorno

Se configuró el entorno de desarrollo en la Raspberry Pi, instalando el sistema operativo Raspbian, Python y todas las librerías necesarias (OpenCV, Flask, etc.). Se optimizó el sistema operativo para asegurar un rendimiento óptimo del software de reconocimiento facial.

3.3. Fases del Proyecto

El proyecto se estructuró en las siguientes fases:

- **Fase de Investigación y Planificación:** Recopilación de información sobre tecnologías de reconocimiento facial, selección de hardware y software, y diseño de la arquitectura del sistema.

- **Fase de Adquisición y Configuración de Hardware:** Compra de componentes, ensamblaje de la Raspberry Pi y los sensores, y configuración inicial del hardware.
- **Fase de Desarrollo de Software:** Implementación del algoritmo de reconocimiento facial, la interfaz web, la base de datos y los módulos de control de acceso.
- **Fase de Fabricación de PCB y Chasis:** Diseño y fabricación de la placa de circuito impreso y el chasis personalizado.
- **Fase de Pruebas y Validación:** Realización de pruebas exhaustivas para evaluar la precisión del reconocimiento facial, la fiabilidad del control de acceso, la usabilidad del sistema y su seguridad.

4. Resultados y Conclusiones

4.1. Análisis de Resultados

El sistema de control de acceso biométrico desarrollado demostró ser una solución viable y efectiva para la autenticación de usuarios mediante reconocimiento facial. Los resultados de las pruebas y validaciones confirmaron el cumplimiento de los objetivos establecidos y revelaron tanto las fortalezas como las limitaciones del sistema.

4.1.1. Cumplimiento de Objetivos

El objetivo general de diseñar un sistema de control de acceso seguro, preciso y económico fue alcanzado satisfactoriamente. El sistema es capaz de reconocer a los usuarios con una precisión del 90%, lo que lo posiciona como una alternativa confiable a los métodos tradicionales. Los objetivos específicos también se cumplieron: se implementó un algoritmo de reconocimiento facial de alta precisión (LBPH con OpenCV), se integraron exitosamente los componentes de hardware (Raspberry Pi, cámara, sensores) y se estableció un enlace robusto con una base de datos para la gestión de usuarios y eventos.

4.1.2. Fortalezas del Sistema

-

Costo-Efectividad: Una de las principales fortalezas del sistema es su bajo costo de implementación, lo que lo hace accesible para microempresas y pequeños emprendimientos que buscan soluciones de seguridad avanzadas sin una gran inversión inicial.

- **Alta Precisión:** La precisión del 90% en el reconocimiento facial asegura una autenticación fiable, reduciendo significativamente la posibilidad de accesos no autorizados.
- **Seguridad Mejorada:** La combinación de reconocimiento facial y autenticación por PIN (doble factor) proporciona una capa adicional de seguridad, haciendo el sistema más resistente a intentos de suplantación de identidad.
- **Facilidad de Uso:** La interfaz web intuitiva y el proceso de registro de usuarios simplificado contribuyen a una excelente usabilidad, permitiendo una fácil administración del sistema.
- **Modularidad:** La arquitectura modular del software facilita futuras expansiones y actualizaciones, permitiendo la integración de nuevas funcionalidades o la mejora de las existentes sin afectar la estabilidad del sistema.

4.1.3. Limitaciones Identificadas

Durante las pruebas, se identificaron algunas limitaciones que representan áreas de mejora para futuras iteraciones del proyecto:

- **Resolución de la Cámara:** La resolución promedio de la cámara OV5647, aunque adecuada para el bajo costo, puede generar falsos positivos o dificultades en el reconocimiento bajo condiciones de iluminación adversas o a distancias mayores. Una cámara de mayor resolución podría mejorar la precisión general.
- **Detección de Vida (Liveness Detection):** El sistema actual no incorpora un mecanismo de detección de vida, lo que lo hace potencialmente vulnerable a
ataques de suplantación mediante fotografías o videos. La implementación de esta característica es crucial para aumentar la robustez del sistema.
- **Rendimiento en Entornos Dinámicos:** En entornos con cambios rápidos de iluminación o con múltiples personas en el campo de visión, el rendimiento del reconocimiento facial podría verse afectado. Se requiere optimización para manejar estas condiciones de manera más efectiva.

4.1.4. Comparación con Sistemas Comerciales

En comparación con sistemas comerciales de control de acceso biométrico, la solución desarrollada ofrece una alternativa significativamente más económica sin comprometer la funcionalidad básica de seguridad. Si bien los sistemas comerciales pueden ofrecer características más avanzadas (ej. detección de vida sofisticada, integración con sistemas de gestión de edificios complejos), mi proyecto demuestra que es posible lograr un alto nivel de seguridad y precisión con una fracción del costo, lo que lo hace ideal para mercados emergentes o aplicaciones con presupuestos limitados.

4.2. Conclusiones

El proyecto de sistema de control de acceso biométrico con reconocimiento facial ha demostrado ser un éxito en la consecución de sus objetivos. Se ha desarrollado una solución innovadora que aborda la necesidad de seguridad accesible, combinando tecnologías de vanguardia con un enfoque en la eficiencia de costos. La viabilidad técnica del sistema ha sido validada, y su rendimiento en un entorno de prueba ha sido satisfactorio, confirmando su potencial para aplicaciones prácticas.

Este trabajo no solo representa un avance en el campo de la seguridad biométrica de bajo costo, sino que también subraya la importancia de la innovación y la adaptabilidad en el desarrollo de soluciones tecnológicas. Las lecciones aprendidas durante este proyecto, especialmente en la optimización de algoritmos para hardware con recursos
limitados y la integración de sistemas complejos, serán invaluables para futuros emprendimientos.

4.3. Trabajo Futuro

Para seguir mejorando el sistema y expandir sus capacidades, se proponen las siguientes líneas de trabajo futuro:

- **Implementación de Detección de Vida:** Integrar algoritmos avanzados de detección de vida para prevenir ataques de suplantación de identidad mediante el uso de fotografías o videos. Esto podría incluir el análisis de micro-movimientos, parpadeo o patrones de calor.
- **Optimización de Algoritmos para Mayor Rendimiento:** Continuar optimizando los algoritmos de reconocimiento facial para mejorar la velocidad y la precisión,

especialmente en condiciones de iluminación variables o con un mayor número de usuarios registrados. Esto podría implicar la exploración de redes neuronales convolucionales (CNN) más ligeras o técnicas de cuantificación de modelos.

- **Integración con Otros Sistemas de Seguridad:** Explorar la integración del sistema con otras plataformas de seguridad, como sistemas de videovigilancia, alarmas o sistemas de gestión de edificios inteligentes, para crear una solución de seguridad más completa y centralizada.
- **Desarrollo de una Interfaz Móvil:** Crear una aplicación móvil para la gestión remota del sistema, permitiendo a los administradores monitorear eventos de acceso, añadir o eliminar usuarios, y recibir notificaciones en tiempo real desde sus dispositivos móviles.
- **Mejora de la Robustez del Hardware:** Investigar y desarrollar un chasis más robusto y resistente a las condiciones ambientales, así como explorar opciones de alimentación de energía más eficientes y fiables para garantizar un funcionamiento continuo en diversos entornos.

Estas mejoras futuras consolidarán el sistema como una solución de seguridad biométrica aún más potente y versátil, con un impacto significativo en la protección de activos y personas.