# Sistema de seguridad de reconocimiento facial para identificar a miembros de una comunidad en un entorno controlado

## Trabajo Terminal No. 2023-A02

*Alumnos: *Godinez Morales Mario Sebastian, *Gonzalez Riveron Diego Raul*

*Directores: Dr. Ramírez Romero Tonahtiu Arturo*

*mgodinez1800@alumno.ipn.mx, dgonzalezr1603@alumno.ipn.mx*

**Resumen –** Se propone desarrollar un sistema que clasifique los rostros de las personas obtenidos por medio de cámaras e identifique aquellas personas que pertenecen a la comunidad de un entorno controlado de las que son externas. Haciendo uso de OpenCV Haar Cascade para la detección de rostros, reconocimiento de patrones y el lenguaje de programación Python.

**Palabras clave** –Reconocimiento de patrones, Análisis de video en tiempo real, Seguridad Biométrica, Machine Learning.

### 1. Introducción

El reconocimiento facial nos permite de alguna manera identificar la identidad de una persona por medio de su cara o rostro, también es una categoría de seguridad biométrica debido a que se utiliza el rostro humano como clave de seguridad. [1]Actualmente los sistemas de reconocimiento facial han estado creciendo constantemente debido a que tienen una gran variedad de aplicaciones, algunas de ellas son:

- Método de identificación al momento de hacer un pago
- Desbloqueo de dispositivos
- Sistemas de seguridad en diferentes organizaciones
- Detectar síntomas de enfermedades por medio del rostro
- Facilitar la búsqueda de personas desaparecidas
- Reducir delitos en comercios

A grandes rasgos el funcionamiento de un sistema de reconocimiento facial se compone de las siguientes partes[1]:

1- Reconocimiento facial: La cámara detecta y fija un rostro

2- Análisis facial: Se captura y se analiza la imagen del rostro, puede ser una imagen 2D o 3D, algunos factores que se toman en cuenta para el análisis facial son: distancia entre ojos, profundidad de las cuencas en los ojos, distancia entre frente y mentón, contorno de los labios, entre otros.

3- Conversión de la imagen a datos: Partiendo de la imagen obtenida se hace una transformación a un conjunto de datos digitales basados en los rasgos faciales de la persona, posteriormente después de manipularlos

matemáticamente se obtiene un código numérico que se denomina huella facial. Dicha huella facial es única para cada persona al igual que la huella dactilar.

4- Búsqueda de una coincidencia: La huella facial obtenida se compara en una base de datos que contiene rostros conocidos para decidir si se reconoce a la persona o no.

El reconocimiento facial de todas las medidas biométricas que se tienen se considera el más natural debido a que se reconoce a una persona por medio de su cara sin mirar sus huellas dactilares o sus iris [2].

**Estado del arte**

Los trabajos similares que se han realizado son los siguientes:

**Tabla 1**.Tabla de sistemas similares al que se propone.

| Nombre | Biometria | Extracción de patrones | Verificación e Identificación | Recopilación discreta de datos | Base de datos |
|---|---|---|---|---|---|
| Sistema de seguridad para identificar a miembros de una comunidad en un entorno controlado | Cumple | Cumple | Cumple | Cumple | Cumple |
| Sistema de seguridad biométrico en base de las venas del dedo[3] | Cumple | Cumple | Cumple | No cumple | Cumple |
| Sistema de biometría de huellas dactilares para la seguridad del hogar[4] | Cumple | No cumple | Cumple | No cumple | Cumple |

| | | | | | |
|---|---|---|---|---|---|
| Diseño e implementación acceso biométrico<br><br>Sistema de control mediante huella dactilar para acceso restringido[5] | Cumple | No cumple | Cumple | No cumple | Cumple |
| Estado del arte de la seguridad en sistemas biométricos[6]. | Cumple | No cumple | Cumple | No cumple | Cumple |

## 2. Objetivos

Objetivo general

- Desarrollar un sistema que sea capaz de identificar a personas que pertenecen a una comunidad en un entorno controlado.

Objetivos específicos

- Implementar el módulo para detección de rostros.
- Desarrollar un algoritmo para la extracción de patrones en un rostro.
- Desarrollar el módulo para clasificar los rostros.
- Medir la eficiencia del clasificador de rostros.
- Implementar el entrenamiento del sistema para obtener el conjunto de datos de los rostros.

## 3. Justificación

Analizando la problemática que se tiene en cuestión de seguridad, cuando una persona ajena a una comunidad ingresa a una institución, se ve comprometida la seguridad de dicha comunidad debido a que la persona podría robar cosas, información o atentar contra algún o algunos miembros de dicha comunidad. Es por ello que se busca crear un sistema que sea capaz de identificar el ingreso de las personas por medio de reconocimiento facial y tener un control de los accesos de los miembros que pertenecen a la comunidad de un entorno controlado.

## 4. Productos y resultados esperados

El producto que se espera obtener es un sistema de cómputo (esto debido a que se requiere procesar video en tiempo real, procesamiento de imágenes y validar si una persona pertenece a una comunidad), que por medio del reconocimiento facial y reconocimiento de patrones, cuando una persona pase por los accesos en el entorno controlado, el sistema haga lo siguiente: si la persona entra por primera vez y el sistema no tiene algún antecedente de ella, se identificará como externa y se notificará de manera discreta con la foto del rostro de la persona a la persona encargada. Si la persona ya tiene antecedentes en el sistema i.e no es primera vez que ingresa por los accesos, entonces el sistema identificará a la persona como miembro de la comunidad, si la persona rara vez ingresa al entorno, entonces el sistema la identificará como sospechosa y alertará a la persona encargada con la foto de dicha persona.

Se analizan los rostros sin cubrebocas debido a que la tendencia actualmente tiende hacia el retiro de cubrebocas en espacios públicos.

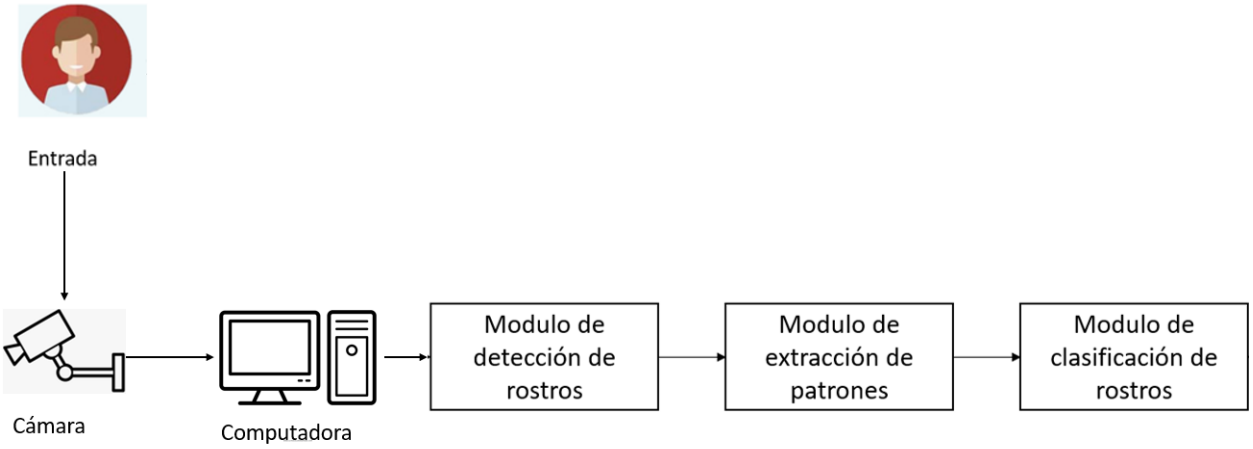



Figura 1. Arquitectura del sistema

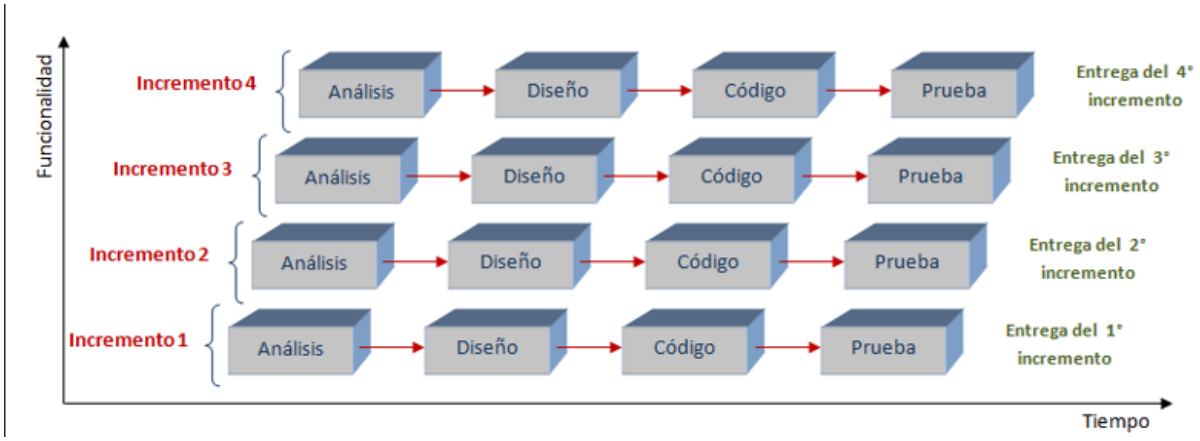
La arquitectura del sistema será cliente servidor debido a que cuando se detecte un rostro por medio de la cámara (cliente), la imagen se enviará a la computadora para su procesamiento (servidor) para finalmente obtener un resultado..

## 5. Metodología

Incremental

En esta metodología se descompone un proyecto en una sucesión de agregados llamados incrementos, cada agregado compone una funcionalidad parcial del producto final, con cada iteración que se realice se hace la entrega de un componente de trabajo[7].

Una vez que se tiene dividido el proyecto en módulos, el desarrollo incremental se lleva a cabo en pasos de tal manera que se abarca el análisis, diseño, implementación, realización de pruebas y mantenimiento. La funcionalidad que se desarrolla en cada etapa se agrega a la funcionalidad que se realizó anteriormente, este proceso se repite hasta que el software esté completamente desarrollado[8].




Elegimos esta metodología debido a que vamos a dividir el proyecto en varios módulos que estarán compuestos de incrementos lo cual nos va a permitir agregar funcionalidades de manera parcial con la ventaja de analizar cada incremento y verificar su funcionamiento, en caso de que tener fallos se corrigen al momento de tal manera que el avance es seguro, se realizará cada incremento hasta lograr el producto final.

**6. Cronograma**

**Nombre del alumno: Godinez Morales Mario Sebastian** **TT No.: ____-____**

**Título del TT: Sistema de seguridad empleando reconocimiento facial dentro de la ESCOM**

| Actividad | AGO | SEP | OCT | NOV | DIC | ENE | FEB | MAR | ABR | MAY | JUN |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Análisis de requerimientos. | | | | | | | | | | | |
| Análisis de riesgos. | | | | | | | | | | | |
| Incremento 1: Desarrollo del algoritmo para la extracción de patrones en los rostros. | | | | | | | | | | | |
| Incremento 2: Corrección del algoritmo para la extracción de patrones en los rostros. | | | | | | | | | | | |
| Diseño de la base de datos. | | | | | | | | | | | |
| Recopilación de Dataset de prueba | | | | | | | | | | | |
| Evaluacion TT1. | | | | | | | | | | | |
| Conectar los módulos del sistema | | | | | | | | | | | |
| Incremento 1: Pruebas del sistema. | | | | | | | | | | | |
| Incremento 2: Reingeniería del sistema. | | | | | | | | | | | |
| Evaluación TT II. | | | | | | | | | | | |
| Generación del Reporte Técnico. | | | | | | | | | | | |

**Nombre del alumno: Gonzalez Riveron Diego Raul** **TT No.: ____-____**

**Título del TT: Sistema de seguridad empleando reconocimiento facial dentro de la ESCOM**

| Actividad | AGO | SEP | OCT | NOV | DIC | ENE | FEB | MAR | ABR | MAY | JUN |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Análisis de requerimientos. | | | | | | | | | | | |
| Análisis de riesgos. | | | | | | | | | | | |
| Incremento 1: Implementación del algoritmo para extraer patrones de los rostros. | | | | | | | | | | | |
| Análisis de tráfico contra tiempo de procesamiento. | | | | | | | | | | | |
| Incremento 2: Desarrollo del módulo para clasificar rostros. | | | | | | | | | | | |
| Creación de la base de datos. | | | | | | | | | | | |
| Evaluacion TT1. | | | | | | | | | | | |
| Incremento 1: Pruebas del sistema. | | | | | | | | | | | |
| Incremento 2: Reingeniería del sistema. | | | | | | | | | | | |
| Evaluación TT II. | | | | | | | | | | | |
| Generación del Reporte Técnico. | | | | | | | | | | | |

## 7. Referencias


[1]latam.kaspersky.com. 2022. *Reconocimiento facial: definición y explicación*. [online] Available at: <https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition> [Accessed 25 May 2022].

[2]J. A. Cadena Moreano, R. H. Montaluisa Pulloquinga, G. A. Flores Lagla, J. C. Chancúsig Chisag, y O. A. Guaypatín Pico, «Reconocimiento facial con base en imágenes», *bol.redipe*, vol. 6, n.º 5, pp. 143–151, mayo 2017.

[3]Anand, J., Flora, T. A., & Philip, A. S. (2013). Finger-vein based biometric security system. International Journal of Research in Engineering and Technology eISSN, 2(12), 197-200.

[4]Siswanto, A., Katuk, N., & Ku-Mahamud, K. R. (2016). Biometric fingerprint architecture for home security systems.

[5]El-Sisi, A. (2011). Design and implementation of biometric access control system using fingerprint for restricted area based on gabor filter. Int. Arab J. Inf. Technol., 8(4), 355-363.

[6]Giraldo Giraldo, A., & Gómez Ramírez, D. P. (2017). Estado del arte de la seguridad en sistemas biométricos.

[7]Flores Moreno, D. E., & Villacís Flores, S. A. (2018). Implementación de un sistema de seguridad biométrica para la unidad de innovación tecnológica de la Universidad de las Américas.

[8]N. T, "What is the Incremental Development Model? Characteristics, Use, Types, Advantages & Disadvantages - Binary Terms", Binary Terms, 2022. [Online]. Available: https://binaryterms.com/incremental-development-model.html. [Accessed: 27- Apr- 2022].

[9]I. Model, "Incremental Model | What is an Incremental Model with Examples?", EDUCBA, 2022. [Online]. Available: https://www.educba.com/incremental-model/. [Accessed: 27- Apr- 2022].

## 8. Alumnos y directores

*Godinez Morales Mario Sebastian*. – alumno de la carrera de Ing. En Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2019630034, tel 5537307511, email mario_mg099@hotmail.com

Firma: 

*Gonzalez Riveron Diego Raul*. – alumno de la carrera de Ing. En Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 2019630011, tel. 5634901689, email dementordgr@gmail.com.

Firma: 

*Dr. Ramírez Romero Tonahtiu Arturo. – Doctor en ingeniería de sistemas, profesor investigador en ingeniería y posgrado. Áreas de interés: Inteligencia artificial, bases de datos, desarrollo de sistemas web y sistemas complejos. Publicaciones en congresos nacionales e internacionales, así como en revistas científicas arbitradas. Departamento de Ciencias e Ingeniería de la Computación, Escuela Superior de Cómputo, Tel. 57296000, ext. 52052. email: tonahtiu@yahoo.com*