**Algoritmo de detección de patrones de movimiento, para la identificación de allanamiento de morada usando visión computacional**

***Trabajo terminal No. -- - - - - -***

*Alumnos: Castañon Hernández Valeria Jahzeel*

*Directores: Dr. Lauro Reyes Cocoletzi, Dra. Maria del Rocío Ochoa Montiel*

*e-mail:vcastanonh2100@alumno.ipn.mx*

**Resumen –** A pesar de los avances tecnológicos en los sistemas de vigilancia para el hogar, los delitos como el allanamiento de morada siguen ocurriendo con frecuencia. Aunque muchas viviendas están equipadas con cámaras de seguridad, estas suelen limitarse a registrar eventos, sin detectar que suceden. Este trabajo propone una aplicación que detecte patrones de movimiento asociados con intentos de allanamiento, utilizando una arquitectura de red neuronal existente ( Mediapipe) para obtener una estimación numérica de estos movimientos y posteriormente, introducirlos en un modelo de predicción de comportamientos sospechosos.

**Palabras clave** – Visión computacional, patrón de movimiento, red neuronal

## 1. Introducción

Este proyecto se centra en el desarrollo de un algoritmo para la detección a través del análisis de video proveniente de cámaras de videovigilancia, con un enfoque específico en la detección de intentos de allanamiento de morada. El allanamiento de morada se define como el intento de una persona o un grupo de personas de entrar o permanecer en una vivienda o local ajeno sin el consentimiento del ocupante. (bucar otras palabras oara untento)

Para abordar esta problemática, resulta esencial distinguir entre conductas delictivas y aquellas justificadas por la ley (visitas de cobradores o repartidores), en consonancia con el artículo 285 del Código Penal Federal [1]. (Relacionarlo o poner el ejemplo en casos coloquiales como cuando va un cobrador o repartidor ? en el planteamiento mejor)

El desarrollo de este algoritmo surge del interés en aumentar la seguridad en el hogar, así como en reducir la incidencia de estos delitos o, al menos, alertar de manera más rápida a los propietarios sobre actividades "inusuales" o "potencialmente peligrosas" que puedan estar ocurriendo en el exterior de su vivienda.

Con el fin de mejorar la seguridad en el hogar y ofrecer una respuesta más rápida ante posibles amenazas, el algoritmo utilizará tecnologías avanzadas como **Mediapipe** [2] para el procesamiento y análisis de los videos. Mediapipe permitirá la detección de puntos de referencia corporales en los videos, los cuales serán cruciales para identificar patrones de comportamiento sospechosos. Esta información, posteriormente, se utilizará como entrada para una red neuronal, que será entrenada para reconocer y clasificar comportamientos potencialmente peligrosos.

## Objetivo

**Objetivo general**

Desarrollar un algoritmo para detectar y clasificar a partir de videos, las siguientes conductas: intentar abrir puertas o ventanas, saltar bardas, y permanecer de pie por un tiempo prolongado afuera de una casa.

**Objetivos específicos**

1. Generar un conjunto de datos mediante la recolección de vídeos de diferentes fuentes(conjuntos de datos públicos y YouTube)
2. Preprocesar de los videos recolectados
3. Diseño e implementación de un algoritmo de visión por computadora para la detección de patrones de movimiento
4. Evaluación de la precisión y efectividad del algoritmo
5. **Planteamiento del Problema**

Según la revista digital *El Economista*, en 2023, [3] la mayoría de los delitos en México registraron una baja significativa a nivel nacional; sin embargo, la gran mayoría de ellos siguen quedando impunes. De acuerdo con el Observatorio Nacional Ciudadano, el delito de robo a casa habitación disminuyó alrededor del 16.20% entre 2022 y 2023. No obstante, encuestas realizadas por el INEGI revelan que, en México, de cada 100 delitos, solo 6.4 se denuncian, y de cada 100 delitos denunciados, solo 14 se resuelven.

Además, la incidencia de allanamientos tiende a aumentar durante las vacaciones, cuando las familias regresan a sus hogares y descubren puertas o ventanas rotas, o que les faltan pertenencias.

Este proyecto propone el desarrollo de algoritmo para identificar patrones de movimiento asociados con intentos de allanamiento. Al integrar algoritmos de aprendizaje máquina, redes neuronales artificiales y análisis de datos, el algoritmo podrá detectar movimientos sospechosos, proporcionando una respuesta proactiva frente a posibles delitos.

En la Tabla 1 se muestra una serie de documentos que realizan algo similar a lo que se ha planteado, de manera que se puede comparar cada uno de estos con el algoritmo propuesto:

|  |  |  |  |
| --- | --- | --- | --- |
| **Título del trabajo** | **Metodología** | **Conjunto de datos** | **Resultados** |
| An eight‑camera fall detection system using human fall pattern recognition via machine learning  by a low‑cost android box | Se implementó un Relevance Vector Machine (RVM) para la detección de caídas, utilizando HOG y PCA, seguido de un algoritmo de Viterbi para generar alertas en tiempo real. | El conjunto de datos fue creado por ellos mismos mediante el uso de muñecos para simular las caídas, se tiene 1 minuto de video estático en cada video para después tener la grabación de la caída durante y después de que sucedió. | El sistema alcanzó una precisión del 89% en detección humana y una precisión en el entrenamiento del 94% |
| Deep Learning Approach for Suspicious Activity  Detection from Surveillance Video | Se extraen fotogramas de videos de seguridad y se utilizan como entrada para una Red Neuronal Convolucional (CNN). Posteriormente se clasifican las actividades observadas en dos categorías: "sospechosa" o "normal". En caso de detectar una actividad sospechosa, el sistema envía una alerta a las autoridades correspondientes. | Se utilizó el conjunto de datos KTH para el entrenamiento de las conductas normales; el conjunto de datos CAVIAR, videos obtenidos de campus y videos de YouTube fueron utilizados para entrenar las conductas sospechosas, estas incluyen el uso de teléfono celular en el campus, peleas y desmayos. | La fase de entrenamiento alcanzó una precisión del 76% en las primeras 10 épocas. La precisión en la fase de pruebas es del 87.15%. |
| Suspicious activity detection using deep learning in secure  assisted living IoT environments | El sistema procesa imágenes con un clasificador basado en Random Forest para identificar actividades sospechosas. Según el resultado, se pueden activar alarmas, enviar SMS o realizar llamadas. | Se utilizó el conjunto de datos HHAR, contiene datos de acelerómetros y giroscopios de diferentes smartphones y smartwatches, recopilados mientras los usuarios realizaban actividades como caminar, sentarse o subir escaleras. | Se alcanzó una precisión máxima del 98.88%, los resultados mostraron una sensibilidad y especificidad que oscilaban entre el 95.5% y el 99.8%. |

Tabla 1. Trabajos relacionados y su comparación con el algoritmo a desarrollar

## Justificación

A pesar de los avances tecnológicos en sistemas de vigilancia para el hogar, los delitos de allanamiento siguen ocurriendo con regularidad. Aunque muchas casas están equipadas con cámaras de seguridad, estas generalmente solo registran los eventos, sin detectar/analizar activamente que sucedan. La detección de actividades sospechosas suele depender de que los propietarios o terceros noten algo inusual y revisen las grabaciones, momento en el cual el delito ya ha sido cometido. Esta reacción tardía reduce la eficacia de los sistemas de vigilancia actuales, dejando a los hogares vulnerables y a los propietarios sin una verdadera capacidad de respuesta ante situaciones de riesgo y es aquí donde la integración de la detección automática en los sistemas de vigilancia puede cambiar esta dinámica.

El impacto de este proyecto es significativo ya que el algoritmo propuesto (esto queda pendiente, hacer preguntas para ver mas o menos como lo puedo colocar) novedad, el algoritmo o cosas similares ¿para que?

Poner los beneficios de mi sistema

## Productos o Resultados esperados

En la Figura 1 se muestra la arquitectura para la creación del conjunto de datos que se usaron para entrenar el modelo:

Diagrama

Descripción generada automáticamente

Figura 1. Generación de la base de datos

(guardarla mejor para el reporte final)

En la Figura 2 se presenta los componentes del proyecto:

Diagrama

Descripción generada automáticamente

Figura 2. Diagrama de arquitectura del algoritmo

(hacer mas simple el diagrama)

Por último, se listarán los productos esperados de este trabajo:

1. Algoritmo capaz de detectar patrones de movimiento relacionados a intentos de allanamiento de morada
2. Reporte técnico que muestre el proceso de desarrollo del algoritmo y que compare los trabajos relacionados con el trabajo propuesto, explique el funcionamiento del algoritmo, así como el análisis de los resultados obtenidos y por último una conclusión en base a todo lo anterior.
3. Dataset….

## Metodología

La metodología que se siguió es un proceso incremental, en la Figura 3 se muestra de manera gráfica el proceso que se siguió para el desarrollo del proyecto, sin embargo, también se va a explicar un poco todo este proceso:

La primera etapa se dedica a la búsqueda y recolección de videos de diferentes conjuntos de datos y videos de YouTube, para que posteriormente en la segunda etapa se realice un preprocesamiento de estos videos, este preprocesamiento incluye el recorte, ajuste de iluminación, redimensionamiento y/o transformaciones geométricas para hacer más fácil el proceso de detección de puntos de referencia.

En la tercera época se empieza

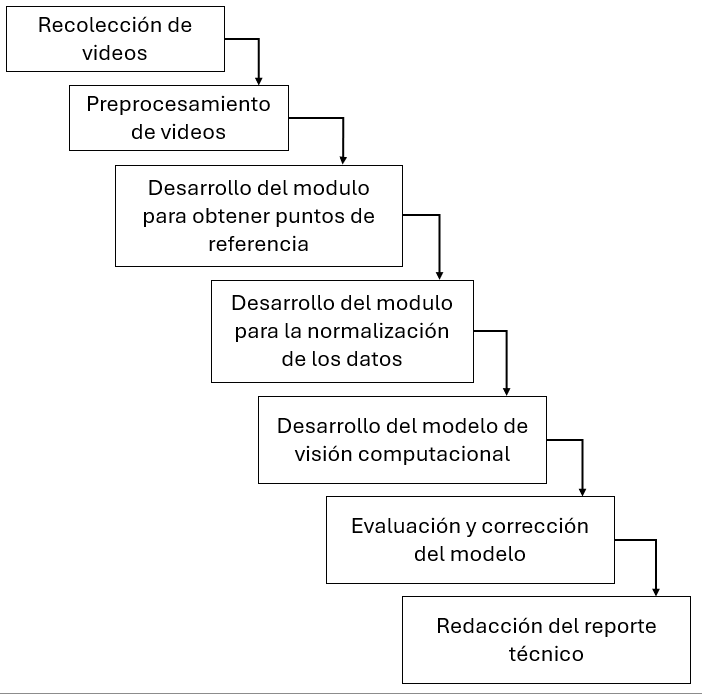


Figura 3. Metodología del proyecto

(todos los cuadros del mismo tamaño, en vez de imagen colocar una lista)

Se describirán las vías que facilitarán el desarrollo del proyecto. Se sugiere definir las metas intermedias a alcanzar y seguir algún estándar (por ejemplo, ISO9001), pero no se pondrá la descripción del estándar, sino su aplicación a la planeación del trabajo a realizar. Se mencionarán las técnicas y herramientas a emplear.

Esta sección no debe exceder un 20% del total, aproximadamente 0.8 páginas.

Esto nada mas es para que aprueben el proyecto, así que la metodologia es algo general

## Cronograma

Planear las etapas, actividades o tareas clave que demande el TT y estimar su tiempo de realización. Su elaboración debe apoyar la delimitación de los alcances del proyecto. Elaborar un cronograma por alumno. El tiempo considerado debe concluir normalmente en Mayo, los casos especiales se revisarán de manera individual. Al final de este documento se encuentra un ejemplo.

## Referencias

1. https://mexico.justia.com/federales/codigos/codigo-penal-federal/
2. https://github.com/google-ai-edge/mediapipe/blob/master/docs/solutions/pose.md

Diagrama

Descripción generada automáticamente

## Alumnos y Directores

*Valeria Jahzeel Castañón Hernández.* - Alumno de la carrera de Ingeniería en Inteligencia Artificial en la Unidad Profesional Interdisciplinaria de Ingeniería campus Tlaxcala (UPIIT), Boleta:2022710020, Tel. 2461168226, email [chj08378@gmail.com](mailto:chj08378@gmail.com)

### Firma:

*Lauro Reyes Cocoletzi* – Tel. 2461921666, email

Firma:

*Maria del Rocío Ochoa Montiel* – Tel. 2414147016, email

Firma:

# CRONOGRAMA Nombre del alumno(a): Título del TT:

TT No.:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Actividad | AGO | SEP | OCT | NOV | DIC | ENE | FEB | MAR | ABR | MAY | | JUN |
| Análisis y diseño del sistema |  |  |  |  |  |  |  |  |  |  | |  |
| Evaluación de TT I. |  |  |  |  |  |  |  |  |  |  | |  |
| Generación del código. |  |  |  |  |  |  |  |  |  |  | |  |
| Pruebas. |  |  |  |  |  |  |  |  |  |  | |  |
| Reingeniería. |  |  |  |  |  |  |  |  |  |  | |  |
| Generación del Manual de Usuario  y la Página web. |  |  |  |  |  |  |  |  |  |  | |  |
| Generación el Reporte Técnico. |  |  |  |  |  |  |  |  |  |  | |  |
| Presentar los resultados en  congresos. |  |  |  |  |  |  |  |  |  |  | |  |
| Evaluación de TT II. |  |  |  |  |  |  |  |  |  |  |  |  |