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

Trabajo terminal No. TT2025-1 IA-002

Alumnos: Castañon Hernández Valeria Jahzeel
Directores: Lauro Reyes Cocoletzi, 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 o analizar que sucede. Este trabajo propone un algoritmo 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 de intentos de allanamiento de morada a través del análisis de video proveniente de cámaras de videovigilancia. 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. Para abordar esta problemática, es esencial distinguir entre conductas delictivas y aquellas justificadas por la ley, como las visitas de cobradores o repartidores, en consonancia con el artículo 285 del Código Penal Federal [1].

El interés en mejorar la seguridad en el hogar y reducir la incidencia de delitos ha impulsado el desarrollo de este algoritmo, que tiene como objetivo alertar rápidamente a los propietarios sobre actividades inusuales o potencialmente peligrosas en el exterior de sus viviendas. Aunque se han propuesto diversos enfoques para abordar problemas similares, estos presentan limitaciones. Por ejemplo, un sistema de detección de caídas mediante una Máquina de Vectores Relevantes (RVM) logró una precisión del 89%, pero se limita a la detección de caídas y requiere un entorno controlado. Otro enfoque utilizó redes neuronales convolucionales (CNN) para detectar actividades sospechosas, con una precisión del 87.15% en pruebas, aunque su capacidad para generalizar a nuevas situaciones es limitada por la variabilidad de los escenarios de entrenamiento. Un tercer enfoque empleó Random Forest para analizar datos de sensores en entornos del internet de las cosas (IoT), alcanzando una alta precisión del 98.88%, pero está enfocado en actividades en interiores y requiere dispositivos específicos para la recolección de datos.

Este proyecto propone un algoritmo que pretende compararse con las metodologías antes

mencionadas al combinar la detección de actividades sospechosas con un enfoque más amplio y adaptable en diferentes escenarios, sin depender de dispositivos adicionales, por lo que potencialmente el proyecto es más versátil y eficaz en la prevención de delitos en el hogar.

Para lograr este objetivo, 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 se utilizará como entrada para una red neuronal, que será entrenada para reconocer y clasificar comportamientos potencialmente peligrosos.

2. Objetivo

Objetivo general

Desarrollar un algoritmo para detectar y clasificar a partir de visión computacional, patrones asociados a comportamientos sospechosos en videos de videovigilancia.

Objetivos específicos

1. Generar un conjunto de datos mediante la recolección de vídeos de diferentes fuentes (conjuntos de datos utilizados en trabajos relacionados y videos públicos de internet) .
2. Preprocesar de los videos recolectados mediante la aplicación de recortes, ajustes de iluminación o transformaciones geométricas.
3. Diseñar e implementar un algoritmo para la detección de las siguientes conductas: intentar abrir puertas o ventanas, saltar bardas, y permanecer de pie por un tiempo prolongado afuera de una casa.
4. Evaluar la precisión y efectividad del algoritmo mediante la comparación con trabajos similares y el uso de diversas métricas de evaluación (F1 score, matriz de confusión, gráficas, etc.).

3. Planteamiento del Problema

Según la revista digital El Economista, en 2023 la mayoría de los delitos en México registraron una baja significativa a nivel nacional; sin embargo, la gran mayoría de ellos siguen quedando impunes [3]. De acuerdo con el Observatorio Nacional Ciudadano, el delito de robo a casa habitación disminuyó alrededor del 16.20% entre 2022 y 2023 [4]. No obstante, encuestas del INEGI revelan que en México, de cada 100 delitos, solo 6.4 se denuncian, y de cada 100 delitos denunciados, solo 14 se resuelven [5]. 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. Esto evidencia que, aunque haya una disminución en la tasa de robos, la percepción de inseguridad sigue siendo alta debido a la baja tasa de resolución de casos y al aumento de

allanamientos en situaciones específicas.
En respuesta a esta problemática, se han propuesto diversos enfoques para la detección de comportamientos sospechosos a través del análisis de video, los cuales se plantean a continuación.
Un primer estudio implementó un sistema de detección de caídas utilizando una RVM, alcanzó una precisión del 89%, aunque su aplicación se limita a entornos controlados [6]. Otro trabajo utilizó CNN para clasificar actividades de vigilancia en sospechosas o normales, logró una precisión del 87.15%, pero su generalización es limitada debido a la variabilidad en los escenarios de entrenamiento [7]. Un tercer enfoque utilizó Random Forest en un entorno IoT asistido, alcanzando una alta precisión del 98.88%, aunque enfocado en actividades interiores y dependiente de múltiples sensores [8].
Dado que los métodos existentes presentan limitaciones en la detección precisa de intentos de allanamiento en entornos domésticos, este proyecto propone el desarrollo de un algoritmo avanzado que identifique patrones de movimiento asociados con intentos de allanamiento. Al integrar técnicas de aprendizaje automático, redes neuronales artificiales y análisis de datos, el algoritmo podrá detectar movimientos sospechosos y diferenciarlos de comportamientos cotidianos, como la llegada de un repartidor o un conocido, proporcionando una respuesta proactiva frente a posibles delitos y contribuyendo a mejorar la seguridad en el hogar.

4. Justificación

En la actualidad, estamos viviendo una época de rápidos cambios tecnológicos, donde la inteligencia artificial (IA) está cobrando un papel crucial en la vida cotidiana, en ámbitos como el estudio y el trabajo. Según un estudio realizado por Microsoft [6], alrededor del 56% de la generación Z (18-24 años) y el 43% de los millennials (25-44 años) ya utilizan y experimentan con la IA. Este creciente interés ha llevado a que aproximadamente el 50% de las empresas, según McKinsey [7], integren la IA en el desarrollo de sus productos y servicios. En este contexto, el presente proyecto adquiere relevancia.
A pesar de los avances tecnológicos en los sistemas de vigilancia doméstica, los delitos de allanamiento siguen ocurriendo con frecuencia [4]. Si bien muchas viviendas están equipadas con cámaras de seguridad, estas generalmente solo registran los eventos sin detectar ni analizar activamente lo que sucede. La detección de actividades sospechosas aún depende en gran medida de que los propietarios o terceros noten algo inusual, revisen las grabaciones, o reaccionen a las alarmas, lo que a menudo ocurre cuando el delito ya ha sido cometido. Esta respuesta tardía limita la eficacia de los sistemas de vigilancia actuales, dejando a los hogares vulnerables.
El desarrollo de un algoritmo capaz de detectar conductas sospechosas relacionadas con intentos de allanamiento, a través del análisis de posturas y movimientos, puede mejorar significativamente la seguridad al proporcionar una detección proactiva y reducir la

necesidad de supervisión constante. Además, este algoritmo puede extrapolarse a otros ámbitos, adaptándose para detectar diferentes tipos de comportamientos anómalos en diversos escenarios, lo que lo convierte en una herramienta versátil. Su integración en diferentes sistemas de seguridad podría realizarse con modificaciones mínimas, lo que incrementa su potencial de uso en la prevención de delitos y otros contextos de seguridad.

5. Productos o Resultados esperados

A continuación, se listarán los productos esperados de este trabajo:

1. Algoritmo capaz de detectar patrones de movimiento relacionados a intentos de allanamiento de morada
2. Conjunto de datos con videos de personas tratando de forzar puertas y/o ventanas, saltando bardas y quedándose paradas mucho tiempo
3. 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.

En la Figura 1 se presentan los componentes del proyecto:

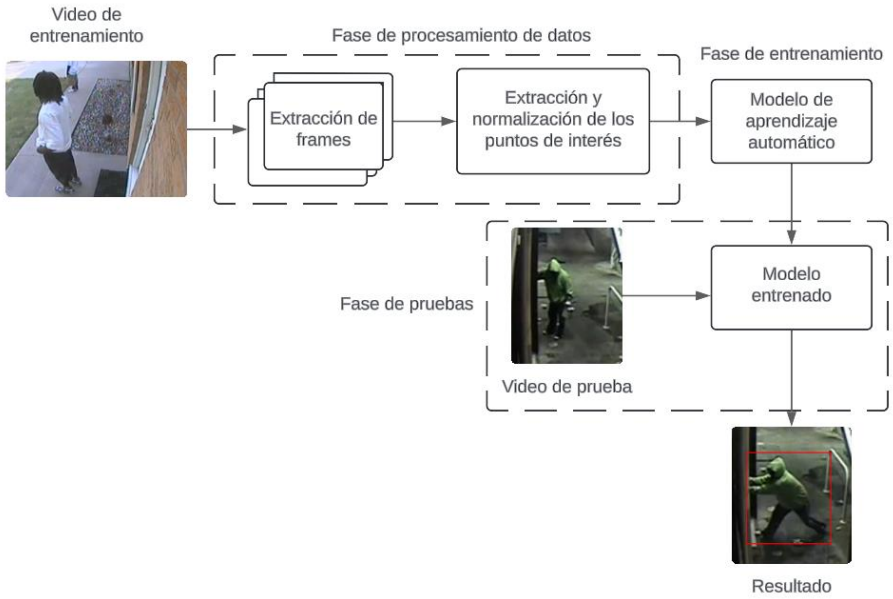


Figura 1. Diagrama de lo componentes que conforman el proyecto

6. Metodología

El desarrollo del proyecto se hará de la siguiente manera:

En la primera etapa, realizará búsqueda y recolección del conjunto de videos de entrenamiento que contienen actividades potencialmente sospechosas, como intentos de abrir

puertas, saltar cercas o permanecer de pie un tiempo prolongado. Estos videos se obtendrán de diversos conjuntos de datos utilizados en trabajos relacionados y videos públicos de internet.

En la segunda etapa, los videos se dividirán en frames para poder identificar los puntos de interés a través de algoritmos de visión por computadora, como MediaPipe, que permite localizar las posiciones de las articulaciones humanas (codos, rodillas, etc.) y rasgos faciales (ojos, nariz, boca, etc.). Estos puntos de interés se guardarán en una tabla para seguir con la siguiente etapa.

La tercera etapa hará la normalización de los puntos de interés para asegurar que variaciones en la escala, orientación o posición no afecten el análisis posterior.

Ya con los datos normalizados, la cuarta etapa consta de entrenar un modelo de aprendizaje, como una red neuronal, que aprende a identificar patrones en los puntos de interés asociados a comportamientos sospechosos.

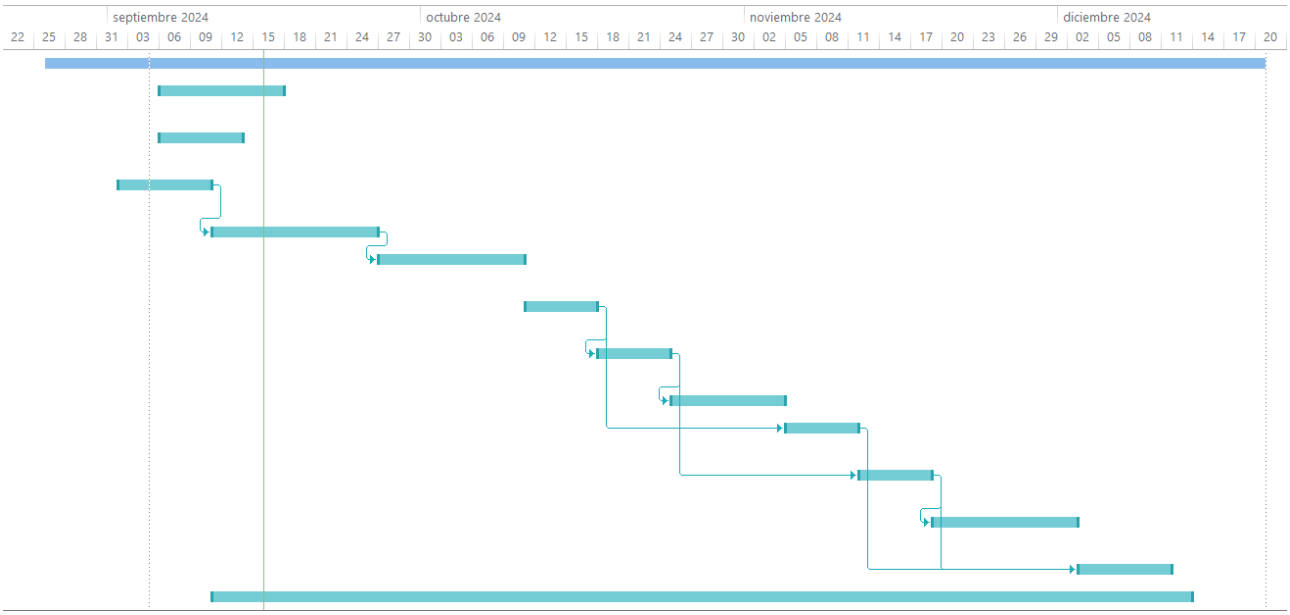
Para la quinta etapa, una vez que el modelo ha sido entrenado, se someterá a pruebas utilizando nuevos videos de prueba que no fueron utilizados en la fase de entrenamiento. Estos videos también se dividirán en frames y pasarán por el proceso de extracción y normalización de los puntos de interés.

Finalmente, la última etapa consiste en procesar nuevos videos y clasificar las acciones observadas. Si detecta comportamientos sospechosos basados en los patrones previamente aprendidos, los clasifica correctamente, una vez obtenidas las salidas se validarán los resultados mediante distintos métodos de evaluación como matrices de confusión, F1 score, precisión o graficas de entrenamiento y validación.

7. Cronograma

Nombre del alumno(a): Valeria Jahzeel Castañon Hernandez TT No. TT2025-1 IA-002
Título del TT: Algoritmo de detección de patrones de movimiento, para la identificación de allanamiento de morada usando visión computacional

Id	Nombre de tarea
1	Trabajo Terminal I
2	Búsqueda y revisión de antecedentes del proyecto
3	Invrestigación de tecnologias de vision computacional y aprendizaje máquina
4	Búsqueda de conjuntos de datos y videos públicos de internet
5	Selección de videos
6	Preprocesamiento del conjunto de datos generado
7	Diseño del módulo para la detección de puntos de interés
8	Diseño del módulo para la normalización de los resultados
9	Diseño del modelo de visión computacional
10	Implementacion del modulo para la deteccion de puntos de interés
11	Implementacion del módulo para la normalización de resultados
12	Pruebas y correcciones de los módulos implementados
13	Integración de los módulos desarrollados
14	Generación de documentación



8. Referencias

1. Código Penal Federal. (2024, 4 septiembre). Justia. https://mexico.justia.com/federales/codigos/codigo-penal-federal/
2. Google-Ai-Edge. (s. f.). mediapipe/docs/solutions/pose.md at master · google-ai-edge/mediapipe. GitHub. https://github.com/google-ai-edge/mediapipe/blob/master/docs/solutions/pose.md
3. El 2023 En México: a la baja la mayoría de los delitos, pero la alta impunidad subsiste. (2023, 28 diciembre). El Economista. https://www.eleconomista.com.mx/opinion/El-2023-en-Mexico-a-la-baja-la-mayoria-de-los-delitos-pero-la-alta-impunidad-subsiste-20231228-0113.html
4. Observatorio Interactivo de incidencia delictiva. Recuperado 28 de agosto de 2024, https://delitosmexico.onc.org.mx/tendencia?unit=folders&indicator=researchFoldersRate&group=month&crime=4200&state=0&domain=
5. De Estadística y Geografía, I. N. (s. f.). Incidencia delictiva. Recuperado 28 de agosto de 2024, de https://www.inegi.org.mx/temas/incidencia/
6. Shu, F., & Shu, J. (2021). An eight-camera fall detection system using human fall pattern recognition via machine learning by a low-cost android box. Scientific Reports, 11(1). https://doi.org/10.1038/s41598-021-81115-9
7. Amrutha, C., Jyotsna, C., & Amudha, J. (2020). Deep Learning Approach for Suspicious Activity Detection from Surveillance Video. IEEE. https://doi.org/10.1109/icimia48430.2020.9074920
8. Vallathan, G., John, A., Thirumalai, C., Mohan, S., Srivastava, G., & Lin, J. C. (2020). Suspicious activity detection using deep learning in secure assisted living IoT environments. The Journal Of Supercomputing, 77(4), 3242-3260. https://doi.org/10.1007/s11227-020-03387-8
9. El aumento de la adopción de la tecnología de Inteligencia Artificial (IA) genera expectación y pone de relieve la importancia de las conversaciones familiares sobre la seguridad online, según un nuevo estudio de Microsoft – Centro de noticias. (2024, 6 febrero). https://news.microsoft.com/es-es/2024/02/06/el-aumento-de-la-adopcion-de-la-tecnologia-de-inteligencia-artificial-ia-genera-expectacion-y-pone-de-relieve-la-importancia-de-las-conversaciones-familiares-sobre-la-seguridad-online-segun-un-nuev/
10. The state of AI in 2022—and a half decade in review. (2022, 6 diciembre). McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-nd-a-half-decade-in-review

9. 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 - vcastanonh2100@alumno.ipn.mx

Firma:_____

Lauro Reyes Cocoletzi, email - lreyesc@ipn.mx

Firma:_____

María del Rocío Ochoa Montiel, email - ma.rocio.ochoa@gmail.com

Firma: _____