ISBN: 978-628-96613-1-6, ISSN: 2414-6390 Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.864

Video surveillance system using computer vision to improve the detection of suspicious behaviors in residences of Trujillo

Kevin M. Garcia Miranda, Bachelor[1]; Miguel A. Pairazaman Uriol, Bachelor[1]; Rolando J. Berrú Beltrán, Master[1]

[1]Universidad Privada del Norte, Perú, kgarciamir@gmail.com, angel.pairazaman@hotmail.com, rolando.berru@upn.edu.pe

Abstract- This research article aimed to determine the impact of a residential video surveillance system employing computer vision for the detection of suspicious behaviors in the province of Trujillo. The study was applied or technological in nature, with an experimental design, and the sample consisted of 12 residences in the city of Trujillo. Observation sheets were used as the primary instruments for data collection. The results showed that the implementation of the system reduced the detection time for suspicious behaviors by 20.83%, in addition to improving accuracy by 10.39% and both precision and sensitivity by 7.5%. It is concluded that the implementation of a video surveillance system integrating computer vision significantly enhances the efficiency of detecting suspicious behaviors, establishing itself as a reliable tool for residential security.

Keywords–surveillance system, computer vision, suspicious behavior, anomaly detection.

Sistema de videovigilancia empleando visión computacional para mejorar la detección de comportamientos sospechosos en residencias de Trujillo

Kevin M. Garcia Miranda, Bachiller[1]; Miguel A. Pairazaman Uriol, Bachiller[1]; Rolando J. Berrú Beltrán, Magister[1]

[1]Universidad Privada del Norte, Perú, kgarciamir@gmail.com, angel.pairazaman@hotmail.com, rolando.berru@upn.edu.pe

Resumen- El presente artículo de investigación se planteó como objetivo principal determinar la influencia de un sistema de videovigilancia residencial empleando visión computacional para la detección de comportamientos sospechosos en la provincia de Trujillo. El tipo de estudio fue aplicada o tecnológico con un diseño experimental, la muestra fue constituida por 12 residencias en la ciudad de Trujillo. Para la recolección de datos se emplearon fichas de observación como instrumentos principales. Entre los resultados obtenidos, se evidenció que la implementación del sistema permitió reducir el tiempo de detección de comportamientos sospechosos en un 20.83%, además de mejorar la exactitud en un 10.39% y la precisión y sensibilidad en un 7.5%. Se concluye que la implementación de un sistema de videovigilancia que integra visión computacional mejora la eficiencia en la detección de comportamientos sospechosos, constituyéndose en una herramienta confiable para la seguridad residencial.

Palabras clave- Sistema de videovigilancia, visión computacional, comportamientos sospechosos, detección de anomalías.

I. INTRODUCCIÓN

En los últimos años el campo de la visión artificial se ha extendido a diferentes aplicaciones del mundo real, demostrando su importancia en áreas como los negocios, la seguridad, el transporte y la vida cotidiana [1]. Uno de los desafíos que enfrenta y que se ha vuelto un área de investigación crítica, es la detección de eventos anormales [2]. En particular, los sistemas de videovigilancia han resaltado la necesidad de automatizar la identificación de comportamientos anormales, ya que, al trabajar con grandes volúmenes de videos, dependen tradicionalmente de operadores humanos para el análisis y la detección de anomalías, lo que resulta en un proceso ineficiente y costoso [3, 4].

Un problema recurrente en muchas zonas urbanas a nivel global es la seguridad ciudadana, donde los comportamientos sospechosos representan un factor importante para la prevención del delito. Según un informe del Ministerio del Interior de España, durante el primer trimestre de 2023, el 45,5% de los delitos catalogados como criminalidad convencional estuvieron relacionados a ataques del patrimonio. Además, los robos con fuerza en domicilios, establecimientos y otras instalaciones aumentaron un 6,2% respecto al mismo período del año anterior [5]. Ante esta situación, las medidas de seguridad, como el uso de alarmas y cámaras de videovigilancia, han aumentado en un 9%, demostrando su efectividad para disuadir robos y alertar rápidamente a las autoridades. A su vez, la integración de inteligencia artificial en las cámaras de videovigilancia ha cobrado relevancia al permitir no solo la detección de movimientos sospechosos, sino también la recopilación de evidencia, lo que fortalece estrategias de prevención y respuesta [6].

En Colombia, la Corporación Excelencia en la Justicia (CEJ) reportó que, durante el primer semestre del 2023, el país enfrentó un aumento significativo de delitos, destacando el robo a residencias, con un incremento del 13% en comparación con el mismo período de 2022, alcanzando un total de 17.529 casos, lo que equivale a un robo cada 15 minutos. Estos robos ocurren con mayor frecuencia durante las primeras horas del día, particularmente entre la medianoche y la 1 a.m., momentos críticos para la detección de comportamientos sospechosos. Asimismo, se registraron incrementos en delitos como hurtos de motocicletas, bicicletas y casos de extorsión, principalmente en horarios nocturnos y fines de semana. Este panorama evidencia la necesidad urgente de implementar sistemas de vigilancia inteligentes que permitan identificar patrones de comportamiento anómalo en tiempo real, reforzando la seguridad en franjas horarias y contextos vulnerables [7].

A nivel nacional, los datos de la encuesta realizada por Ipsos durante el primer trimestre de 2024 revelaron que el 63% de los peruanos perciben un aumento en la inseguridad en comparación al año 2023. Asimismo, el 31% expresó que no se siente seguro ni siquiera en su propio hogar. En este contexto, el 94% de los encuestados mostró un fuerte respaldo al uso de tecnologías avanzadas para la vigilancia, destacando su potencial en la prevención de delitos. Estas herramientas resultan clave para identificar comportamientos sospechosos, como el uso de gorras para ocultar la identidad o la portación de armas blancas, como cuchillos, en situaciones de riesgo, facilitando la intervención oportuna y la protección de las comunidades [8].

A nivel local, el informe técnico publicado por el Instituto Nacional de Estadísticas e Informática reveló que el 89.8% de las viviendas encuestadas en la ciudad de Trujillo perciben un alto nivel de inseguridad en los próximos doce meses. Además, el 13% de las viviendas en las principales ciudades con más de 20 mil habitantes fueron víctimas de robos o intentos de robo, representando un incremento del 1.2% respecto a 2023. El informe también identifica patrones recurrentes asociados a estos delitos, como la presencia de

personas que rondan los domicilios a horas inusuales y observan fijamente las viviendas, conductas que pueden ser indicadores tempranos de posibles actos delictivos [9]. Esta situación evidencia la necesidad de sistemas avanzados de videovigilancia que puedan detectar automáticamente este tipo de comportamientos sospechosos, mejorando la seguridad y prevención en áreas urbanas.

II. ANTECEDENTES

Los autores Miyahara y Nagayama, plantearon como objetivo mejorar la exactitud de detección de secuestros en base a las características de comportamientos en Japón. Para ello, analizaron los métodos de extracción de características Speeded-Up Robust Features (SURF) y Histogram of Oriented Gradients (HOG). En sus resultados demuestran que el sistema empleando HOG tuvo una tasa de exactitud del 81.1%, y con el método SURF la tasa fue del 75.5%, concluyendo que al implementar visión artificial usando el método HOG permitió al sistema automatizar la detección de casos de secuestros con una mayor tasa de exactitud [10].

Por otra parte, Yang y Yilmaz, tuvieron como objetivo el detectar anomalías, definidas como diferencias existentes entre el comportamiento de un individuo respecto a otro dentro de multitudes en Estados Unidos. Implementaron un modelo pre entrenado denominado YOLOv5x para la detección de objetos, la tarea de seguimiento de individuos se llevó a cabo con el algoritmo DeepSORT y para estimar el comportamiento atípico integraron la estimación de densidad de núcleo denominado KDE. Para los resultados trabajaron con dos conjuntos de datos, en el primer conjunto la detección obtuvo una precisión del 89% y una sensibilidad del 90%, mientras que en el segundo fue del 93% y 88% respectivamente. Con esto se demostró que el sistema integrando visión computacional presenta buenos valores de precisión con una clara eficacia en la detección de anomalías reales [11].

Del mismo modo, los autores Donia, El-Behaidy y Youssif, su trabajo se centró en proporcionar una solución innovadora que optimice la precisión para el reconocimiento de eventos agresivos impulsivos en Egipto. El enfoque se basa en el reconocimiento temprano de eventos mediante la extracción de características discriminativas espacio-temporales utilizando HOG y un flujo óptico denso. También, se emplearon técnicas avanzadas de reducción de complejidad, como el análisis de componentes principales (PCA) y el análisis discriminante lineal (LDA), para optimizar el rendimiento del sistema. Los resultados mostraron tasas de precisión superiores al 96% en la identificación de eventos violentos, reforzando la utilidad de estos métodos en sistemas de videovigilancia inteligentes [12].

Por último, Salazar, su estudio buscó determinar el impacto de un sistema automatizado basado en procesamiento digital de imágenes para el control de vigilancia de activos fijos en la empresa "NBA Consultores-Trujillo" en Perú, donde entre sus objetivos está reducir el tiempo. El sistema automatizado se trabajó en 5 etapas, siendo en la segunda donde se manejó el pre procesamiento de video, en dicha etapa se trabajó la transformación de imágenes a escala de grises, reduciendo así el volumen de datos, para luego aplicar el algoritmo de sustracción de imágenes. En sus resultados demostró una reducción del 86% en el tiempo de revisión de grabaciones, pasando de 30 horas a 4.32 horas. Sosteniendo la importancia de integrar visión computacional en los sistemas de videovigilancia para automatizar procesos [13].

III. OBJETIVOS

A. Objetivo General

Determinar la influencia de un sistema de videovigilancia residencial empleando visión computacional en la detección de comportamientos sospechosos en Trujillo en el año 2024.

B. Objetivos Específicos

- Establecer cómo influye un sistema de videovigilancia empleando visión computacional en el porcentaje de exactitud de detección de comportamientos sospechosos.
- Determinar cómo influye un sistema de videovigilancia empleando visión computacional en el porcentaje de precisión de detección de comportamientos sospechosos.
- Evaluar cómo influye un sistema de videovigilancia empleando visión computacional en el porcentaje de sensibilidad de detección de comportamientos sospechosos.
- Definir cómo influye un sistema de videovigilancia empleando visión computacional en el tiempo promedio de reconocimiento de comportamientos sospechosos.

IV. METODOLOGÍA

La investigación es de tipo aplicada con un diseño pre-experimental, mediante un análisis previo y posterior a la implementación de la solución con visión computacional. En esta investigación se trabajó con una muestra de 12 residencias, definidas como domicilios donde habitan personas o familias. La selección se llevó a cabo mediante un muestreo por conveniencia, esto debido a diversas limitaciones como la falta de accesibilidad a datos por restricciones de privacidad de los usuarios, la poca colaboración de la comunidad para participar en la investigación y los límites de presupuesto que evitaron realizar un análisis más extenso, complicando el desplazamiento y el alcance del equipo de investigación.

A. Diagnóstico Pre-test:

Para la detección de comportamientos sospechosos se establecieron 4 indicadores, estos fueron:

a) Porcentaje de exactitud de detección de comportamientos sospechosos.
b) Porcentaje de precisión de detección de comportamientos sospechosos.
c) Porcentaje de sensibilidad de detección de comportamientos sospechosos.
d) Tiempo promedio de reconocimiento de comportamientos sospechosos.

Se evaluó el desempeño del sistema de videovigilancia tradicional para la detección de comportamientos

sospechosos, considerando los indicadores de exactitud, precisión, sensibilidad y tiempo de reconocimiento. Para la recolección de datos específicos de cada indicador se utilizaron fichas de observación y para el cálculo se emplearon las siguientes fórmulas.

1. Indicador A: Porcentaje de exactitud de detección de comportamientos sospechosos (Ped)

$$\text{Ped} = \frac{VN+VP}{VN+FP+FN+VP} \times 100\% \quad (1)$$

VP: Verdaderos negativos
FP: Falsos positivos
VN: Verdaderos positivos
FN: Falsos negativos

2. Indicador B: Porcentaje de precisión de detección de comportamientos sospechosos (Ppd)

$$\text{Ppd} = \frac{VP}{FP+VP} \times 100\% \quad (2)$$

VP: Verdaderos negativos
FP: Falsos positivos
VN: Verdaderos positivos
FN: Falsos negativos

3. Indicador C: Porcentaje de sensibilidad de detección de comportamientos sospechosos (Psd)

$$\text{Psd} = \frac{VP}{VP+FN} \times 100\% \quad (3)$$

VP: Verdaderos negativos
FP: Falsos positivos
VN: Verdaderos positivos
FN: Falsos negativos

4. Tiempo promedio de reconocimiento de comportamientos sospechosos (Tpr)

$$\text{Tpr} = \frac{1}{n}\sum_{i=1}^{n}(Td_i - Tr_i) \quad (4)$$

Td: El tiempo en que se detectó el comportamiento
Tr: El tiempo real en que ocurre el comportamiento
n: Cantidad de grabaciones

B. *Desarrollo de Producto:*

Para el desarrollo e implementación del producto se tuvo un periodo de 3 meses. Se utilizó la metodología ágil de desarrollo de software Scrum, debido a que permite gestionar proyectos de manera flexible y adaptable. En la Tabla I se muestran las fases ejecutadas para el desarrollo del producto.

TABLA I
Fases para el desarrollo del producto

Fase	Descripción
1	Planificación • Conocer las necesidades de los usuarios. • Plantear los requerimientos del Producto. • Elaboración de prototipos del producto.
2	Desarrollo del Software • Diseñar y desarrollar un modelo de datos. • Examinar la comunicación entre los componentes del sistema. • Elaborar las interfaces diseñadas. • Realizar cada sprints para cada requerimiento.
3	Pruebas • Examinar y mejorar el sistema.
4	Implementación • Instalación y configuración del sistema

a. Fase 1: Planificación

Durante esta etapa se llevó a cabo la identificación y análisis de las principales necesidades de los usuarios relacionadas con comportamientos sospechosos frente a una residencia. Este proceso incluyó la recopilación de información a través de entrevistas realizadas a los participantes, quienes compartieron sus preocupaciones más relevantes en términos de seguridad y vigilancia. Por último, se establecieron los requerimientos del sistema en base a la información recolectada,se desarrollaron prototipos de las interfaces del sistema y se definieron los sprints, los cuales se pueden visualizar en las Fig. 1, 2, 3 y 4.

CÓDIGO	NOMBRE	NECESITO	FINALIDAD	PRIORIDAD	RIESGO
R01	Grabación	Poder captar segundos previos y posteriores al comportamiento sospechoso en formato MP4	Usar las grabaciones para un futuro análisis	Alta	Medio
R02	Almacenamiento	Almacenar videos en google drive	Visualizar las grabaciones de manera remota sin necesidad del sistema	Alta	Medio
R03	Detección Arma blanca	Identificar la presencia de armas blancas en video	Generar alertas en tiempo real para reforzar la detección de comportamientos sospechosos.	Alta	Alta
R04	Detección de Sujeto sospechoso	Identificar personas que permanezcan mirando al hogar del usuario por un tiempo prolongado.	Alertar sobre posibles comportamientos sospechosos para prevenir incidentes de seguridad.	Alta	Alta
R05	Detección Gorra	Identificar esta usando gorra y estan mirando a una zona durante un rango de horas de la noche.	Alertar sobre individuos que visten una gorra .	Alta	Alta
R06	Notificaciones	Notificar al usuario mediante correos electrónicos sobre un comportamiento sospechoso.	Informar en tiempo real sobre posibles riesgos o incidentes para tomar decisiones oportunas y reforzar la seguridad.	Alta	Medio
R07	Login Usuario	Ingresar al sistema	Visualizar todas las funcionalidades	Baja	Baja
R08	Diseño de Interfaz	Diseñar una interfaz intuitiva y accesible para la reproducción de videos	Ofrecer una experiencia de usuario fluida y eficiente en la visualización de grabaciones.	Baja	Baja
R09	Análisis de Video en Tiempo Real	Implementar análisis y procesamiento de secuencias de video en tiempo real.	Garantizar una detección precisa sin comprometer la velocidad ni la calidad del sistema.	Baja	Baja
R10	Reproducción de Video en la Interfaz	Implementar la reproducción de video dentro de una interfaz.	Visualización directa y efectiva.	Baja	Baja

Fig. 1 Requerimientos

En la Fig. 1 se puede observar una tabla con el código, nombre, la prioridad, riesgo,lo que el usuario necesita y la finalidad del requerimiento.

NOMBRE	RESPONSABLE	FECHA DE INCIO	FECHA FINAL	ESTADO
SPRINT 1		12/08/2024	20/08/2024	FINALIZADO
Diseño de Interfaz	KEVIN GARCIA	12/08/2024	15/08/2024	FINALIZADO
Login Usuario	MIGUEL PAIRAZAMAN	15/08/2024	18/08/2024	FINALIZADO
Reproducción de Video en la Interfaz	MIGUEL PAIRAZAMAN	18/08/2024	20/08/2024	FINALIZADO
SPRINT 2		20/08/2024	27/09/2024	FINALIZADO
Detección Arma blanca	KEVIN GARCIA	20/08/2024	02/09/2024	FINALIZADO
Detección de Sujeto sospechosa	KEVIN GARCIA	02/09/2024	16/09/2024	FINALIZADO
Grabación	MIGUEL PAIRAZAMAN	16/09/2024	23/09/2024	FINALIZADO
Almacenamiento	KEVIN GARCIA	23/09/2024	27/09/2024	FINALIZADO
SPRINT 3		27/09/2024	21/10/2024	FINALIZADO
Detección de Gorra	MIGUEL PAIRAZAMAN	27/09/2024	13/10/2024	FINALIZADO
Notificaciones	KEVIN GARCIA	13/10/2024	15/10/2024	FINALIZADO
Análisis de Video en Tiempo Real	MIGUEL PAIRAZAMAN	15/10/2024	21/10/2024	FINALIZADO

Fig. 2 Sprints del sistema

En la Fig. 2 se visualiza una tabla con todos los sprints en el cual se especifican los requerimientos, el responsable que lo realizó y las fechas límites.

Fig. 3 Mockup de la interfaz: Principal

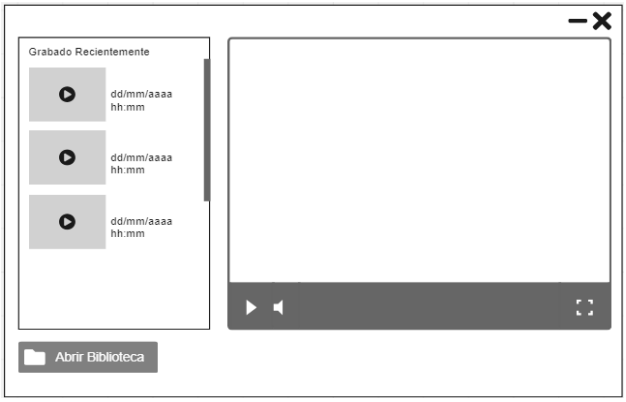

Fig. 4 Mockup de la interfaz: Grabaciones

En la Fig. 3 y Fig. 4 se aprecia el diseño preliminar de las interfaces de la pantalla principal y grabaciones, respectivamente, mostrando el aspecto visual y las funcionalidades esperadas.

b. Fase 2: Desarrollo del Software

Durante esta fase se inició el proceso de desarrollo del sistema. Se optó por utilizar YOLO V8 y MediaPipe para la detección de comportamientos extraños, debido a su precisión y eficiencia en el análisis en tiempo real.

Por otro lado, se realizó un diagrama de modelo de datos para estructurar los componentes del sistema y sus interacciones.

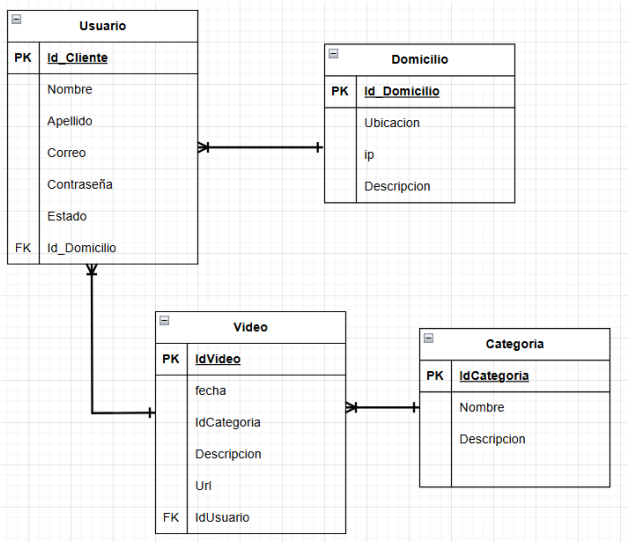

Fig. 5 Modelo de datos

En la Fig. 5 se observan todas las tablas necesarias para poder cumplir con el proceso de almacenamiento de las grabaciones de los comportamientos sospechosos detectados.

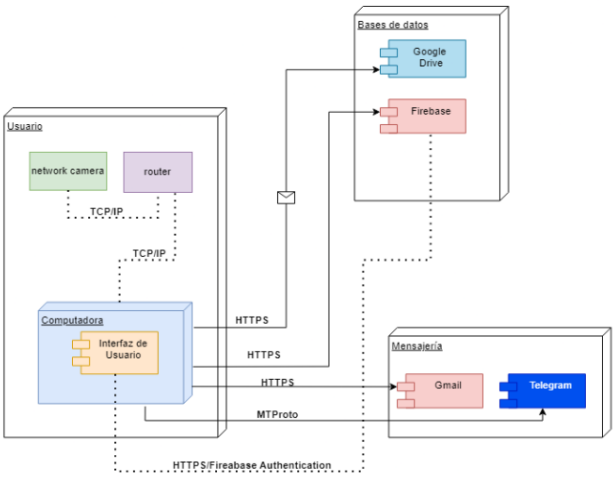

Fig. 6 Diagrama de Despliegue

En la Fig. 6 se observa un diagrama de despliegue, el cual muestra cómo el usuario, a través de una cámara de red y un router, se comunica con el sistema mediante protocolos como TCP/IP y HTTPS. El sistema se comunica con Firebase y Google Drive para el almacenamiento de datos, y utiliza servicios de mensajería como Gmail y Telegram para las notificaciones.

Teniendo claramente definida, a través del diagrama de despliegue, la infraestructura del sistema y cómo interactúan los diferentes componentes físicos y lógicos, se procedió a desarrollar todas las interfaces y los algoritmos necesarios para completar el sistema.

c. Fase 3: Pruebas

Durante esta etapa se procedió a probar cada sprint en un entorno simulado. Estas pruebas permitieron evaluar el funcionamiento de las funcionalidades desarrolladas, verificar la integración de los componentes y garantizar el correcto desempeño del sistema bajo condiciones controladas.

- Sprint 1:

Reproducción de video en la interfaz: Se trabajó toda la configuración necesaria para poder visualizar el video capturado por la cámara en tiempo real en la interfaz principal.

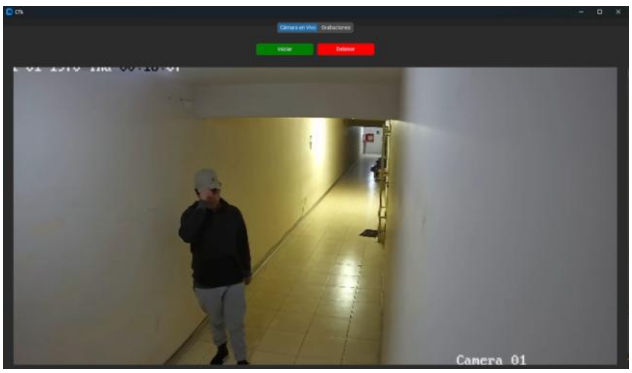

Fig. 7 Reproducción de video en la interfaz

En la Fig. 7 se evidencia una correcta integración y conectividad de la cámara de vigilancia con la interfaz principal.

- Sprint 2:

Detección de arma blanca: Se analizó el tipo de entrenamiento que se implementaría en YOLO v8, priorizando una respuesta inmediata en el reconocimiento y optimizando el consumo de recursos computacionales, dado que los dispositivos donde se ejecutaría el sistema presentaban limitaciones. Tras el análisis, se optó por la versión YOLO v8s debido a su balance entre velocidad y precisión. Además, se recopiló un conjunto de datos compuesto por 1541 imágenes de cuchillos para entrenar el modelo de manera efectiva.

Fig. 8 Detección de arma blanca

En la Fig. 8 se aprecia una escena de la detección de un arma blanca. Además, la confiabilidad de la detección es de 0.85, la cual puede llegar a variar dependiendo de la distancia de la cámara y el sujeto.

Detección de sujeto sospechoso: Se utilizó MediaPipe para realizar el seguimiento de poses humanas, obteniendo los puntos clave del cuerpo humano. Una vez integrada esta biblioteca al sistema, se enfocó específicamente en los puntos correspondientes a los ojos para calcular la posible trayectoria de la mirada del sujeto. Luego, para identificar un posible comportamiento sospechoso, se consideraron factores como la permanencia prolongada de la trayectoria de la mirada del individuo en una zona específica, como el hogar del usuario, durante un rango de horas de la noche que se clasificarían como inusuales o sospechosas.

Fig. 9 Detección mirada

En la Fig. 9 se observa una escena de la detección de mirada, esta se activa cuando el sujeto observa en dirección de una zona de la residencia por más de 10 segundos.

- Sprint 3:

Detección de gorro: Se añadieron 262 imágenes al modelo YOLO v8 para agregar la detección de gorros, reforzando la precisión en la identificación de

comportamientos sospechosos. Este nuevo criterio se sumó al algoritmo de detección de la trayectoria de la mirada y al análisis del rango horario, lo que permitió establecer de manera más confiable patrones de conducta potencialmente sospechosos.

Fig. 10 Detección de gorra

En la Fig. 10 se identifica una escena de la detección del uso de gorra, la cual complementa el análisis de comportamiento sospechoso de la detección de mirada.

d. Fase 4: Implementación

Durante esta prueba, se procedió a la instalación del sistema en todas las computadoras de los usuarios. Cada dispositivo fue configurado para adaptarse a las necesidades del entorno de cada usuario, realizando las modificaciones necesarias para garantizar un funcionamiento adecuado.

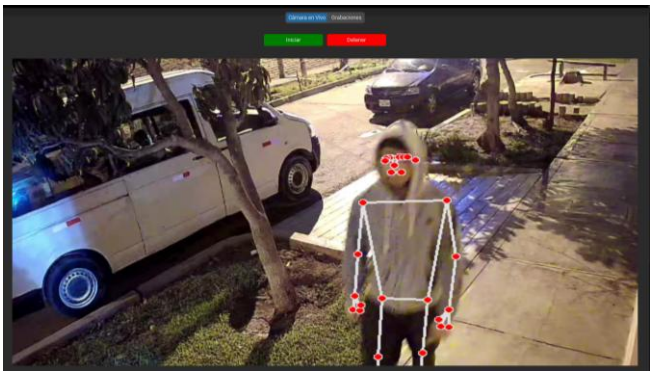
Fig. 11 Implementación del Sistema: Interfaz Principal

En la Fig. 11 se muestra la interfaz principal del sistema, donde se llevó a cabo la integración de la cámara de vigilancia junto con las modificaciones necesarias para que la detección de comportamientos sospechosos funcione correctamente.

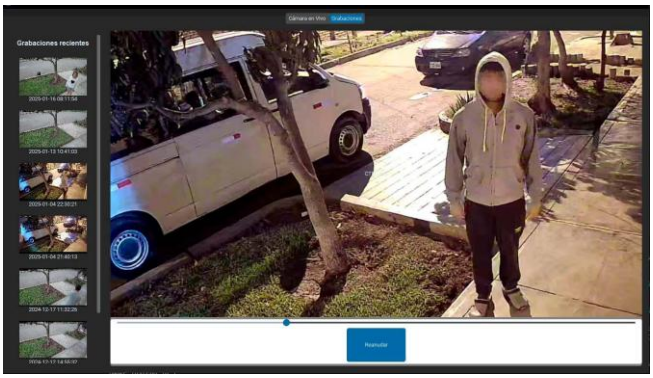

Fig. 12 Implementación del Sistema: Interfaz Grabaciones

En la Fig. 12 se evidencia la interfaz de grabaciones del sistema, donde el usuario puede visualizar todos los videos generados por el sistema. Cada grabación abarca los 30 segundos antes y 90 segundos después de la detección de un comportamiento sospechoso.

C. Diagnóstico Post-test:

Posteriormente a la implementación del sistema mostrado en la presente investigación, se volvieron a evaluar los mismos indicadores con los mismos instrumentos y ecuaciones (1), (2), (3) y (4) para contrastar los resultados con los datos obtenidos del diagnóstico pre-test y de esta manera definir la influencia de un sistema de videovigilancia empleando visión computacional en la detección de comportamientos sospechosos.

Además, de los datos recopilados del pre y post-test de cada uno de las residencias, se llevó a cabo la comprobación de las hipótesis estadísticas mediante la prueba t-student usando la herramienta XLSTAT.

V. RESULTADOS

En esta sección se presentan y analizan los valores obtenidos de los diagnósticos pre-test y post-test de cada indicador, junto con los datos de la prueba de hipótesis mediante t-student utilizando la herramienta XLSTAT con 11 grados de libertad y 0.05 de nivel de significancia.

A. Indicador A: Exactitud (Ped)

H0: El Porcentaje de Exactitud es el mismo después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

Ha: El Porcentaje de Exactitud es mayor después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

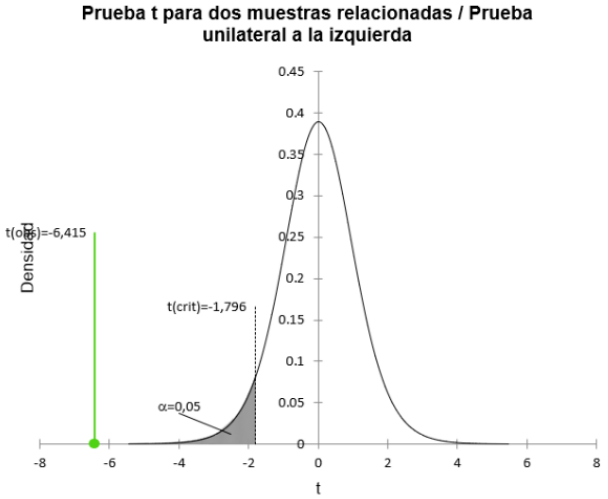

Fig. 13 Evaluación del área de aceptación o rechazo del porcentaje de Exactitud.

En la Fig. 13 se observa que el valor t(obs) = -6.415 es inferior al valor crítico t(crit) = -1.796, ubicándose en el intervalo de rechazo de la hipótesis nula y aceptando la hipótesis alterna como resultado.

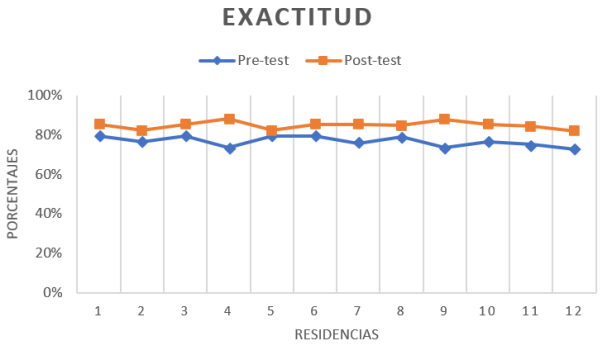

Fig. 14 Valores pre y post-test del Porcentaje de Exactitud

Según se observa en la Fig. 14, el porcentaje de Exactitud fue mayor después de haber implementado el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos en comparación al sistema tradicional con personas.

B. Indicador B: Precisión (Ppd)

H0: El Porcentaje de Precisión es el mismo después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

Ha: El Porcentaje de Precisión es mayor después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

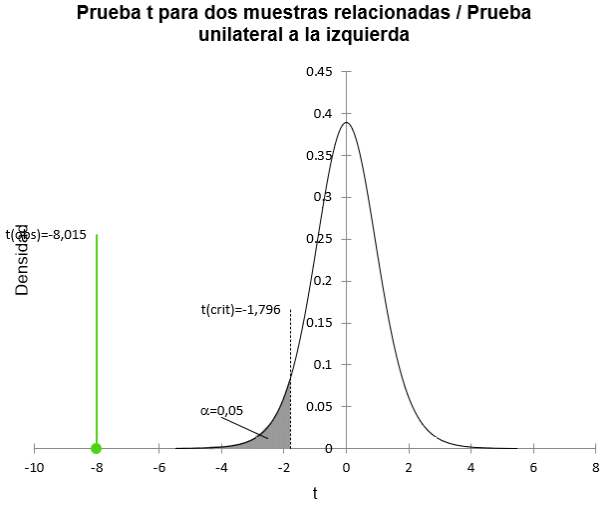

Fig. 15 Evaluación del área de aceptación o rechazo del porcentaje de Precisión

En la Fig. 15 se observa que el valor t(obs) = -8.015 es inferior al valor crítico t(crit) = -1.796, ubicándose en el intervalo de rechazo de la hipótesis nula y aceptando la hipótesis alterna como resultado.

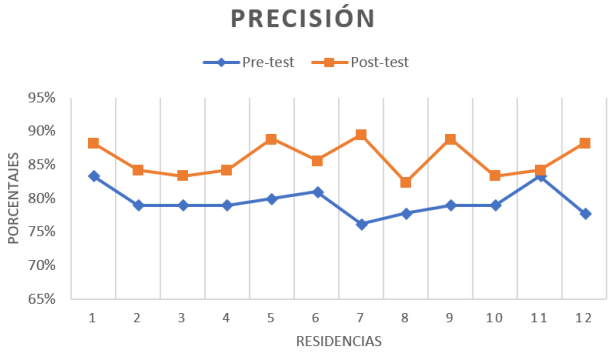

Fig. 16 Valores pre y post-test del Porcentaje de Precisión

Según se observa en la Fig. 16, el porcentaje de Precisión fue mayor después de haber implementado el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos en comparación al sistema tradicional con personas.

C. Indicador C: Sensibilidad (Psd)

H0: El Porcentaje de Sensibilidad es el mismo después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

Ha: El Porcentaje de Sensibilidad es mayor después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

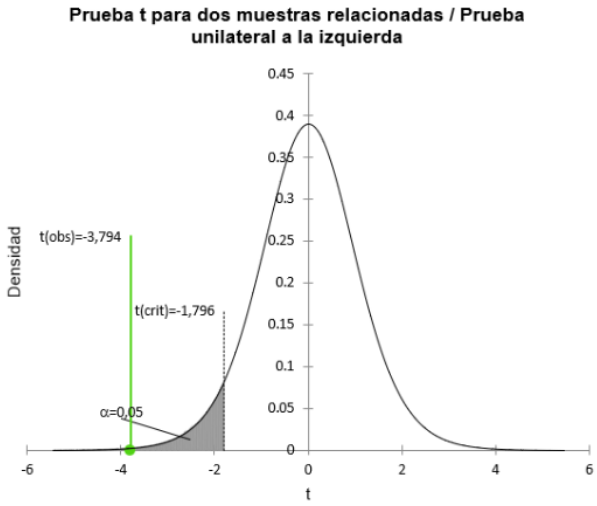

Fig. 17 Evaluación del área de aceptación o rechazo del porcentaje de Sensibilidad.

En la Fig. 17 se observa que el valor t(obs) = -3.794 es inferior al valor crítico t(crit) = -1.796, ubicándose en el intervalo de rechazo de la hipótesis nula y aceptando la hipótesis alterna como resultado.

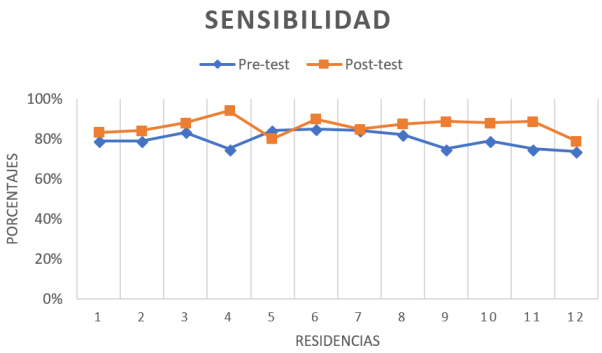

Fig. 18 Valores pre y post-test del Porcentaje de Sensibilidad

Según se observa en la Fig. 18, el porcentaje de Sensibilidad fue mayor después de haber implementado el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos en comparación al sistema tradicional con personas.

D. Indicador D: Tiempo de reconocimiento (Tpr)

H0: El Tiempo Promedio de Reconocimiento es el mismo después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

Ha: El Tiempo Promedio de Reconocimiento es menor después de emplear el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos.

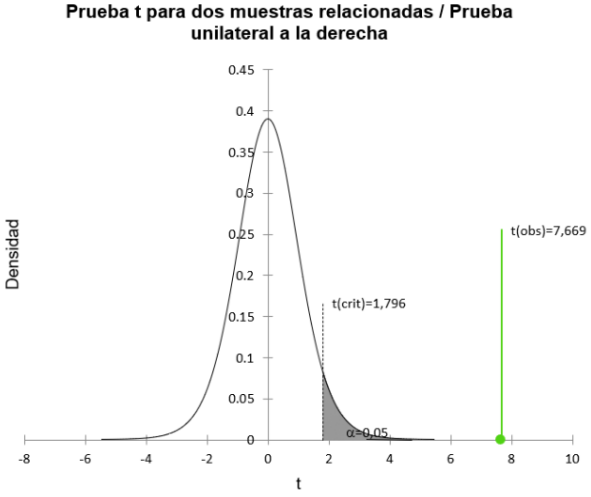

Fig. 19 Evaluación del área de aceptación o rechazo del tiempo promedio de reconocimiento.

En la Fig. 19 se observa que el valor t(obs) = 7.669 es superior al valor crítico t(crit) = 1.796, ubicándose en el intervalo de rechazo de la hipótesis nula y aceptando la hipótesis alterna como resultado.

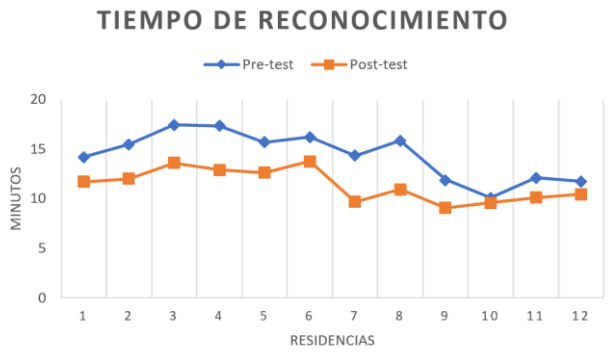

Fig. 20 Valores pre y post-test del Tiempo promedio de reconocimiento

Según se observa en la Fig. 20, el tiempo promedio de reconocimiento fue menor después de haber implementado el Sistema de videovigilancia con visión computacional para la detección de comportamientos sospechosos en comparación al sistema tradicional con personas.

De los gráficos mostrados en las Fig. 14, 15 y 16, se evidencia un aumento positivo en los porcentajes obtenidos de los indicadores a, b y c. En cuanto a la Fig. 18, muestra una reducción considerable en los minutos del indicador d. Estos resultados definen una influencia positiva del uso del sistema de videovigilancia empleando visión computacional. En la Tabla II se presenta un resumen de los promedios generales obtenidos del pre-test y post-test para cada indicador. Asimismo, se evidencia la diferencia entre estos valores.

TABLA II
Promedios generales de los resultados

Indicador		Pre-test	Post-test	(Post)-(Pre)	%
a	Ped	77%	85%	+8%	+10.39
b	Ppd	80%	86%	+6%	+7.5
c	Psd	80%	86%	+6%	+7.5
d	Tpr	14.35	11.36	-2.99	-20.83

VI. DISCUSIÓN

Los resultados presentados en la Tabla II, mostraron que el promedio de exactitud para la detección de comportamientos sospechosos obtenido del sistema de videovigilancia antes de implementar visión computacional fue del 77%; mientras que, después de la implementación tuvo un incremento relativo del 10.39% llegando a un promedio del 85%. En el artículo “An Intelligent Security Camera System for Kidnapping Detection”, los autores Miyahara y Nagayama luego de evaluar su sistema obtuvieron un promedio de 81.1% de exactitud [10], el cual fue menor al de esta investigación. Las diferencias en los promedios se pueden deber a que los autores Miyahara y Nagayama, en su cálculo, evaluaron 24 escenarios: 12 con comportamientos sospechosos y 12 con actividades normales. En contraste, la presente investigación trabajó con 10 escenarios simulados de comportamientos sospechosos y entre 20 a 22 escenarios reales recopilados por cada residencia de la muestra, lo cual se vio limitado por el tiempo disponible para la recopilación, pudiendo haber influido en el porcentaje de exactitud.

En la Tabla II se detallan resultados que muestran que el promedio de precisión en la detección de comportamientos sospechosos con el sistema de videovigilancia, antes de implementar visión computacional, fue del 80%. Posteriormente, tras la implementación, este promedio alcanzó un 86%, lo que presenta un incremento relativo del 7.5%. En contraste, los autores Donia, El-Behaidy y Youssif en el artículo "Impulsive Aggression Break, Based on Early Recognition Using Spatiotemporal Features" reportaron tasas de precisión superiores al 96% [11]. Esta diferencia se podría explicar debido al hecho de que los autores emplearon técnicas avanzadas de análisis de patrones dinámicos, como STPCA, que permite capturar variaciones espacio-temporales complejas, y HOG, que facilita la extracción precisa de características de bordes y formas. En esta investigación, sin embargo, se utilizó YOLOv8, basado en una arquitectura de redes neuronales convolucionales (CNN), siendo este eficiente en la detección en tiempo real de objetos generales que para analizar patrones dinámicos específicos. Esto último podría haber influido en el menor porcentaje de precisión en esta investigación.

De acuerdo con los datos registrados en la Tabla II, se observa que el promedio de sensibilidad en la detección de comportamientos sospechosos con el sistema de videovigilancia, antes de implementar visión computacional, fue del 80%. Tras la implementación, este promedio alcanzó un 86%, representando un incremento del 7.5%. En comparación, los autores Yang y Yilmaz en el artículo "Crowd Scene Anomaly Detection in Online Videos", obtuvieron un promedio de sensibilidad del 89% [12], un valor superior al obtenido en esta investigación. La razón de esta diferencia se puede deber a que los autores evaluaron su sistema utilizando el UCSD Anomaly Detection Dataset, un conjunto de datos robusto desarrollado por la Universidad de California en San Diego (UCSD), que identificaron un total de 6750 datos con anomalías. En cambio, la presente investigación evaluó el sistema con los datos recopilados de la muestra, que sumaron un total de 403 datos, lo cual pudo haber influido en el porcentaje promedio de sensibilidad obtenido. Frente

Según los datos de la Tabla II, el promedio del tiempo de reconocimiento con el sistema de videovigilancia, antes de incorporar visión computacional, fue de 14.35 segundos. Luego de la implementación el tiempo disminuyó a 11.36 segundos, equivalente a una reducción del 20.83%. Por otro lado, Salazar, en su investigación "Desarrollo de un Sistema Automatizado Basado en Procesamiento Digital de Imágenes para mejorar el proceso de control de vigilancia de Activos Fijos en la empresa NBA Consultores - Trujillo", alcanzó una reducción del 86% [13]. La diferencia se podría deber a que el autor en su análisis consideró al tiempo que un trabajador emplea en revisar la información del sistema para identificar un evento relevante, mientras que esta investigación se enfocó en medir el tiempo desde que ocurre un comportamiento sospechoso hasta su reconocimiento, influyendo en los resultados obtenidos respecto al tiempo.

VII. CONCLUSIONES

Se comprobó que la implementación de un sistema de videovigilancia residencial basado en visión computacional influyó positivamente la exactitud en la detección de comportamientos sospechosos. Antes de la implementación, el sistema obtuvo un promedio de exactitud del 77%, mientras que después de implementar el sistema con visión computacional, esta exactitud aumentó al 85%, lo que significó una mejora del 10.39%.

Se demostró que la implementación de un sistema de videovigilancia residencial basado en visión computacional influyó positivamente la precisión en la detección de comportamientos sospechosos. Antes de la implementación, el sistema obtuvo un promedio de precisión del 80%, mientras que después de implementar el sistema con visión computacional, esta precisión aumentó al 86%, lo que significó una mejora del 7.5%.

Se concluyó que la implementación de un sistema de videovigilancia residencial basado en visión computacional influyó positivamente la sensibilidad en la detección de comportamientos sospechosos. Antes de la implementación, el sistema obtuvo un promedio de sensibilidad del 80%, mientras que después de implementar el sistema con visión computacional, esta sensibilidad aumentó al 86%, lo que significó una mejora del 7.5%.

Se evidenció que la implementación de un sistema de videovigilancia residencial basado en visión computacional influye en la reducción del tiempo de detección de comportamientos sospechosos, donde se observó una disminución del 20.83% en el tiempo promedio de detección, pasando de una media de 14.35 segundos a 11.36 segundos.

TRABAJOS FUTUROS

Para investigaciones futuras que estén basados en el mismo tema de esta investigación, se hace las siguientes recomendaciones:

- Incorporar dispositivos con mayor potencia hardware, como una tarjeta de video o un procesador de alta gama. Esto permitirá analizar flujos de video con mayor detalle y procesar modelos más robustos, mejorando la detección de comportamientos complejos y aumentando la precisión en tiempo real.

- Ampliar los criterios de detección de comportamientos potencialmente sospechosos. Esto permitirá incorporar análisis complejos y contextualizados, como patrones grupales y diferentes posturas corporales específicas, por ejemplo, postura de cuclillas como postura como un comportamiento de una persona que deja un objeto dudoso en la puerta de la residencia.

- Ampliar la red de cámaras en una misma residencia para poder evaluar las diferentes perspectivas de una misma residencia y poder tener un análisis de comportamiento más completo, por ejemplo, realizar un seguimiento de una persona sospechosa desde el momento en que ingresa al perímetro hasta que interactúa con un área restringida o abandona el lugar.

AGRADECIMIENTO

Los autores agradecen a los usuarios que facilitaron sus viviendas y dispositivos, contribuyendo tanto a las pruebas del sistema como a la recolección de datos necesarios para el desarrollo de esta investigación.

REFERENCIAS

[1] International Business Machines Corporation. ¿Qué es la visión por computadora? [Internet]. IBM, corp; 27 de julio 2021 [citado 5 de enero de 2025] Disponible de: https://www.ibm.com/es-es/topics/computer-vision

[2] Yang Y, Fu Z, Naqvi SM. Abnormal event detection for video surveillance using an enhanced two-stream fusion method. Neurocomputing [Internet]. 2023 [citado 6 de enero de 2025]; 553 (126561). Disponible de: https://doi.org/10.1016/j.neucom.2023.126561

[3] Xu H, Li L, Fang M, Zhang F. Movement human actions recognition based on machine learning. Int J Onl Eng [Internet]. 2018 [citado 6 de enero de 2025]; 14 (04): 193-210. Disponible de: https://doi.org/10.3991/ijoe.v14i04.8513

[4] Choudry N, Abawajy J, Huda S, Rao I. A comprehensive survey of machine learning methods for surveillance videos anomaly detection. IEE Access [Internet]. 2023 ; 11: 114680 - 713. Disponible de: https://www.doi.org/10.1109/ACCESS.2023.3321800

[5] Gob.es. Balance de criminalidad, Primer trimestre 2023. España: Ministerio del Interior (ES); 2023. Disponible de: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Balance-de-Criminalidad-Primer-Trimestre-2023.pdf

[6] Seguridad AB. Estadísticas de Seguridad en España [Internet]. AB Seguridad. 27 de noviembre 2024 [citado 15 de diciembre de 2024] Disponible de: https://www.abseguridad.com/estadisticas-de-seguridad-en-espana/

[7] Muñoz C. Se agudiza la criminalidad en Colombia: cada día más de mil personas son víctimas de hurtos y/o extorsión [Internet]. Corporación Excelencia en la Justicia. 2023 [citado 15 de diciembre de 2024]. Disponible de: https://cej.org.co/destacados-home-page/se-agudiza-la-criminalidad-en-colombia-cada-dia-mas-de-mil-personas-son-victimas-de-hurtos-y-o-extorsion/

[8] Perú21. ESTUDIO DE OPINIÓN: Informe sobre Seguridad [Internet]. Ipsos.com. 2024 [citado el 10 de septiembre de 2024]. Disponible de: https://www.ipsos.com/sites/default/files/ct/news/documents/2024-03/Informe%20Encuesta%20%20Seguridad%20-%20Per%C3%BA21%20al%2023%20de%20febrero%202024.pdf

[9] Abad P, Gutiérrez C, Arias A. Estadísticas de Seguridad Ciudadana. Instituto Nacional de Estadistica e Informatica (PE); 2024. No.: 3 - Mayo 2024. Disponible de: https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_estadistica_seguridad_nov23_abr24.pdf

[10] Miyahara A, Nagayama I. An intelligent security camera system for kidnapping detection. Fujipress LTD [Internet]. 2013 [citado 6 de enero de 2025]; 17(5): 746-752. Disponible de: https://doi.org/10.20965/jaciii.2013.p0746

[11] Yang K, Yilmaz A. Crowd scene anomaly detection in online videos. ISPRS - Int Arch Photogramm Remote Sens Spat Inf Sci [Internet]. 2024 [citado 15 de septiembre de 2024]; XLVIII-2–2024:443–8. Disponible de: https://doi.org/10.5194/isprs-archives-XLVIII-2-2024-443-2024

[12] Donia M, El-Behaidy W, Youssif A. Impulsive Aggression Break, Based on Early Recognition Using Spatiotemporal Features. Big Data Cogn [Internet]. 2023 [citado 10 de enero de 2025]; 7(3):150. Disponible de: https://doi.org/10.3390/bdcc7030150

[13] Salazar Campos J. Desarrollo de un Sistema Automatizado Basado en Procesamiento Digital de Imágenes para mejorar el proceso de control de vigilancia de Activos Fijos en la empresa NBA Consultores - Trujillo [tesis maestria en Internet]. Perú: Universidad Nacional de Trujillo, 2019 [citado 20 de septiembre de 2024]. Disponible en: https://dspace.unitru.edu.pe/items/a80e3d1d-dc8b-422b-bc00-d4562fe35e61