APLICACIÓN DE INTELIGENCIA ARTIFICIAL COMO ESTRATEGIA PARA LA DISMINUCIÓN DEL NIVEL DE RIESGO EN SEGURIDAD RESIDENCIAL EN EL SECTOR DE BOCAGRANDE (CARTAGENA DE INDIAS)

Presentado por:

HUGO ALBERTO PELÁEZ RAMOS

UNIVERSIDAD SAN BUENAVENTURA DE CARTAGENA
CONVENIO UNIVERSIDAD MILITAR NUEVA GRANADA BOGOTÁ
ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD
CARTAGENA DE INDIAS
2019

APLICACIÓN DE INTELIGENCIA ARTIFICIAL COMO ESTRATEGIA PARA LA DISMINUCIÓN DEL NIVEL DE RIESGO EN SEGURIDAD RESIDENCIAL EN EL SECTOR DE BOCAGRANDE (CARTAGENA DE INDIAS)

Presentado por:

HUGO ALBERTO PELÁEZ RAMOS

Ensayo como requisito para optar al título de:
Especialista en Administración de la Seguridad

Tutor temático
JAVIER VILLARREAL

Tutor metodológico
FRANCISCO JAVIER MAZA AVILA

UNIVERSIDAD SAN BUENAVENTURA DE CARTAGENA
CONVENIO UNIVERSIDAD MILITAR NUEVA GRANADA BOGOTÁ
ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD
CARTAGENA DE INDIAS
2019

RESUMEN

La vigilancia privada cuenta con seguridad física y electrónica complementándose y generando cada vez más una prestación del servicio que coadyuve a mitigar riesgos potenciales, particularmente en zonas residenciales; estas prestaciones de servicios de seguridad podrían ser optimizados con el empleo de la inteligencia artificial, particularmente en análisis biométrico en el reconocimiento facial y el reconocimiento de matrículas de vehículos.

PALABRAS CLAVE: *Biometría, inteligencia artificial, reconocimiento.*

ABSTRACT

Private surveillance has physical and electronic security complementing each other and generating more and more a service provision that helps mitigate potential risks, particularly in residential areas. These security services could be optimized with the use of artificial intelligence, particularly in biometric analysis for facial recognition, and vehicles license plate recognition.

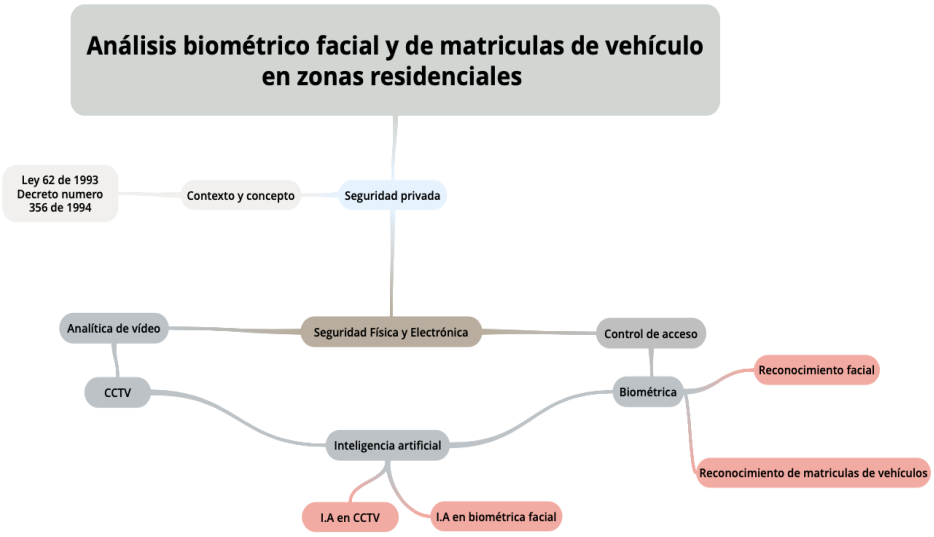
KEYWORDS: *Biometrics, artificial intelligence, recognition.*

INTRODUCCIÓN

La vigilancia privada se ha extendido a nivel global como una respuesta a la necesidad humana de protección, la cual cada vez se ve más vulnerada por los múltiples factores de riesgo generados por contextos inseguros, y que ha llevado a multiplicar esfuerzos en mejoras en sistemas físicos que faciliten y aseguren el bienestar de las comunidades. Las zonas residenciales han sido uno de los sectores que ha demandado este tipo de servicios de vigilancia privada, en donde se prestan servicios por medio de guardas de seguridad, sistemas como alarmas, cámaras de video y control de acceso; lo anterior, como una respuesta social ante el aumento de la inseguridad y la violencia urbana que ha llevado a que se modifique la forma y estructura de hábitat en espacios más cerrados y controlados, generando percepción de mayor seguridad en los habitantes.

Por tanto, las empresas de vigilancia para estar en la vanguardia dando respuestas efectivas ante estas demandas, debe generar nuevos sistemas con mayor tecnología que permita también la reducción de costos en los servicios ofertados, sin que estos disminuyan su calidad, sino que esta incremente; tal es el caso, de la implementación de inteligencia artificial en la detección de movimiento por medio de analítica de video que vigilen zonas internas y perimetrales de conjuntos residenciales. Adicionalmente un control de acceso facilitado por biométrica facial.

Figura 1. Análisis biométrico facial y de matrículas de vehículos en zonas residenciales



Fuente: Elaboración propia

1. CONTEXTO Y CONCEPTO DE VIGILANCIA PRIVADA

En Colombia, el surgimiento de la vigilancia y seguridad privada emerge como una necesidad ante las múltiples secuelas ocasionadas por la violencia que azotaba toda la población, la cual ha sido perpetrada por guerrillas, paramilitarismo, narcotraficantes y bandas criminales organizadas, lo que llevo a que se emplearan servicios privados que garantizaran la seguridad individual (Stella & Mendez, 2014; Dammert, 2017). La implementación de este tipo de seguridad se evidenció como una necesidad ante el poco alcance de las fuerzas policiales y militares del país, ya que, la demanda de seguridad empezó a aumentar y se tuvo que recurrir a servicios especializados en materia de seguridad.

Relacionado con la normatividad del contexto la Ley 62 de 1993 da origen a la Superintendencia de Vigilancia y Seguridad Privada, y, bajo una aprobación de disposición general como quedo plasmado en el Decreto numero 356 de 1994 por el cual se expide el estatuto de vigilancia y seguridad privada, teniendo por objeto regular la prestación de dichos servicios. Por consiguiente, se constituye la prestación de servicios privados atendiendo a las deficiencias del Estado en proveer seguridad, no logrando dar alcance a las múltiples vicisitudes que se presentan relacionadas con la seguridad, tal como sucede en el sector gubernamental, energético, minero, de hidrocarburos, entre otros. Algunos datos que podrían respaldar la alta demanda en estos servicios, son algunas estadísticas otorgadas por la Pérez, de la Federación Colombiana de Empresas de Vigilancia y Seguridad Privada (2018), y es que, para el año 2016 el incremento del 4,3% en cuanto a sus ingresos anuales.

Algunos autores, entre ellos Caonero, Godnik, Fernández, Bustamante & Natenzon (2011), en el informe del Centro Regional de las Naciones Unidas para la Paz, el Desarme y el Desarrollo en América Latina y el Caribe (UNLIREC) definieron la seguridad privada como:

> "(…) *La seguridad privada es un término utilizado para describir una amplia gama de servicios relacionados con la seguridad y proporcionados por entidades privadas con fines de lucro. Éstos pueden incluir, entre otros los siguientes: vigilantes y guardias (armados y no armados), patrullas, escoltas, servicios de vehículos blindados, transporte de valores y mercancías, servicios de inteligencia, perros entrenados, vigilancia electrónica, investigaciones, protección de los activos*

> *físicos, blindaje de edificios, protección de obras e infraestructura, protección anti-secuestro, capacitación en seguridad y autoprotección, ventas de armas y capacitación, así como la intermediación de estos servicios*" (p. 220).

2. SEGURIDAD FÍSICA Y ELECTRÓNICA

La seguridad física hace referencia al análisis de riesgos, amenazas y vulnerabilidades tanto de personas como en infraestructura y como partir de ello se pueden tomar medidas tanto preventivas como reactivas que permita la protección.

Entre los elementos constitutivos de la seguridad física se pueden encontrar:

- Guardas de seguridad, supervisores, supervisores motorizados
- Comunicación por radio, teléfonos y avanteles
- Control de rondas electrónicas, informes consignados en minutas y relojes de marcación (Montejo, 2013)

Para poder potencializar la seguridad física, se requiere tanto de tecnología como de potencial humano capacitado para atender a estas demandas del contexto; esto ha llevado a que las empresas dedicadas a la prestación de servicios de vigilancia privada empleen tecnologías que faciliten la detección de riesgos potenciales y que estos puedan ser reducidos significativamente; entre estas tecnologías se encuentran las cámaras de video (Martínez, 2010, citado en Paladines & Villavicencio, 2013).

La seguridad privada debe multiplicar sus esfuerzos implementando seguridad electrónica que permita reforzar la seguridad física, ya que este no da alcance ante la protección de los múltiples riesgos a los que se está expuesta la comunidad en general.

Tal como lo menciona Pinzón (2018), tomando como base lo mencionado en Security Fair Colombia:

> "(…) *Facilita la prevención y la protección de los ambientes tanto en edificaciones públicas como privadas, residenciales, áreas críticas, sitios estratégicos, ciudades y fronteras. Dura*
>
> *nte mucho tiempo, la seguridad se manejó esencialmente con vigilantes y una que otra ayuda, como alarma, sensores, y cámaras fijas que solo tomaban un punto de las instalaciones, debido a esto nace la necesidad de mejorar bajo las estructuras*

> *electrónicas, es por ello que se crea la necesidad de implementar estos modelos de seguridad electrónica*" (2018, p.10)

3. ANALÍTICA DE VIDEO

De acuerdo con lo evidenciado por Roca (2016) en la feria de seguridad electrónica, dejo plasmado por medio de una entrada de blog que:

> "(…) *En las empresas e instituciones la seguridad electrónica se basa en el uso de tecnologías de última generación, lo que incluye sistemas CCTV (circuitos cerrados de televisión), controles de acceso y presencia, sistemas de intrusión, control de activos y control de acceso gestionado, centros de control de alarmas, etc.*" (Chillida, 2018)

La industria de seguridad suele emplear Circuito Cerrado de Televisión (CCTV), hoy día Sistemas de Video Vigilancia, para control de acceso, lo cual facilite la labor de preservar la seguridad del sitio de donde se tenga custodia. Este CCTV ha sido definido como: "Un sistema de transmisión y visualización de imágenes en movimiento que solo puede ser visualizado por un grupo limitado de personas, a diferencia de la televisión abierta o pública" (Martí, 2013).

Los CCTV cuentan con tecnología que permite que la transmisión de las imágenes se haga por medio de redes bien puede ser de cableado, de fibra óptica o en wifi; estos sistemas pueden contar con múltiples cámaras interconectadas a monitores o televisores que permiten reproducir imágenes de actividad física bien sea, en tiempo real o grabadas, de áreas e instalaciones que deben ser supervisadas.

La composición de estos CCTV puede ser desde uno básico a uno más complejo y tecnológico, compuestos por cámaras de grabación, multimatrices distribuidas, servidores IP, transmisores y grabadores digitales; estas cámaras se encuentran debidamente conectadas a un secuenciador conectado a un monitor y la información podría ser almacenada en tiempo real en medios analógicos o digitales. (Chica, 2015; Fillipo, Olarte & Cañón. 2009).

No basta con tener equipos tecnológicos que faciliten la identificación de riesgos inminentes, será necesario también personal entrenado en atender a las situaciones que se

generen en el momento y que requieran ser atendidas de forma urgente, generando así una disminución en los múltiples riesgos que puedan presentarse.

La analítica de vídeo es un software que permite captar imágenes y procesarlas en datos; este, cuenta con variadas formas de aplicabilidad en lo que respecta a seguridad, ttal como lo relaciona TAS (2018) (Tecnología Acceso y Seguridad, 2018):

- Captura de imágenes faciales
- Reconocimiento facial
- Reconocimiento de placas (matrículas)
- Reconocimiento de contenedores, trenes, vagones.
- Monitoreo de tráfico
- Detección de hurto en el punto de venta
- Análisis de perímetro e intrusión
- Detección de objetos desatendidos
- Seguimiento de objetos

4. CONTROL DE ACCESO

Otra de las funciones principales en las zonas residenciales es el control de acceso tanto vehicular como peatonal y dicho control en la mayoría de estas zonas se realiza con capital humano que en ocasiones tiende a rotar con mucha frecuencia, dificultando así una labor más óptima y eficaz que en múltiples ocasiones podría llevar a generar molestias en los habitantes. En algunos conjuntos cerrados se ha propendido por disminuir esas incidencias de la rotación de personal sobre el control de acceso, haciendo uso de tecnologías que faciliten la labor, como la biométrica dactilar, lector de tarjetas o chips para acceso vehicular o reconocimiento de placas de los vehículos.

5. INTELIGENCIA ARTIFICIAL

Tal como se ha explicado en apartados anteriores, la necesidad de crear espacios seguros para las poblaciones ha llevado a que se implementen sistemas avanzados y con tecnología de punta para mitigar riesgos. Gracias a la innovación en tecnologías de nueva generación, es que se puede implementar sistemas más sofisticados en la seguridad de las zonas residenciales y para ello la inteligencia artificial cuenta con grandes aportes que cada vez

estén mas sistematizados los procesos a menor costo y con mayor optimización en los resultados. Una de estas tecnologías corresponde a los aportes dados por la inteligencia artificial; para ello se definirá en primera instancia este concepto y su aplicabilidad en el contexto.

La inteligencia artificial es el estudio de la conducta inteligente, el cual hace un uso del funcionamiento de la mente humana y lo pone en uso de la tecnología.

Para poder entender mejor esta analogía entre la inteligencia artificial y la mente humana se revisa una analogía que ha existido entre la mente humana y los computadores:

La mente y el cerebro de los humanos ha sido comparado con teorías computacionales, ya que nuestros sistema funciona con canales de entrada (hardware) y canales de procesamiento y salida (software); estos canales de entrada corresponden a los órganos sensoriales lo que a los computadores sería todos los elementos físicos que componen un sistema de cómputo (pantalla, CPU, teclado, mousse, etc); entre tanto, los canales de procesamiento correspondería a los diferentes lóbulos del cerebro (frontal, parietal, temporal y occipital). Los lóbulos del cerebro son los encargados de procesar la información que proviene del exterior, los cuales son captados por los órganos sensoriales. La analogía con sistemas de cómputo podría evidenciarse en que los computadores cuentan con un "*Front end processor*" (FEP), procesadores de la información sensorial.

Martinez & Fornaguera proponen el siguiente ejemplo para entender mejor lo anteriormente descrito:

> "(…) *Un computador es incapaz de interpretar directamente la información que recibe una cámara de televisión. Sin embargo, con una tarjeta digitalizadora se puede convertir la luz de una imagen en una matriz de puntos con valores correspondientes a brillo, color, intensidad. De esta forma se puede formar una "imagen" digitalizada que directamente no tiene ningún sentido para el computador. Lo lóbulos occipital y temporal actúan como estos pre-procesadores que convierten la información directa de los sentidos en información interpretable y analizable para el lóbulo frontal de la corteza, sitio, donde se presume se genera la representación de la realidad del momento*" (1998, p. 44).

De acuerdo con Sanabria & Archila (2011), el uso de esta inteligencia artificial ha sido empleado en vigilancia/ seguridad así como en identificación biométrica para el

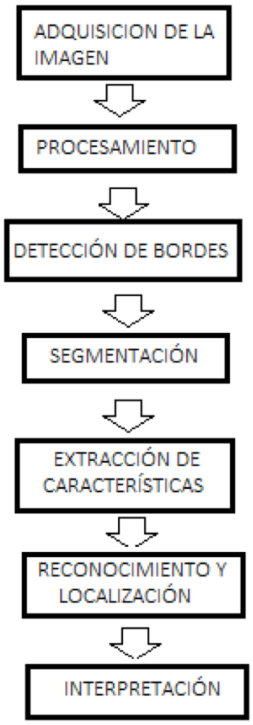
control de acceso, como lo puede ser: huellas dactilares patrón de iris y de voz, patrón de marcha y características faciales; estas dos últimas que serán explicadas posteriormente con más detalle y precisión respecto a su aplicabilidad en seguridad.

5.1. Visión artificial

La empleabilidad de la visión artificial en el ámbito de la seguridad ha generado en los últimos años múltiples avances que permiten que haya mejoras en la prestación de los servicios, reduciendo los niveles de riesgo que puedan presentarse en contextos residenciales, dando respuesta a las exigencias realizadas por clientes, en donde el interese se encuentra en la vigilancia de espacios controlados y como labor fundamental, el control de acceso.

Esta forma de inteligencia artificial ha permitido que se realice reconocimiento facial desde el análisis biométrico de las características morfológicas de cada persona que desea acceder a sitios especificaos que cuentan con vigilancia y por ello, uno de los órganos mas sensibles ante los estímulos del externos y que generar gran cantidad de información para procesar, es la vista; desde la inteligencia artificial ésta, inspira la creación de cámaras de video, ya que la retina se comporta como una cámara fotográfica o de video. El funcionamiento de estos equipos permiten identificar características de color, movimiento y distribuciones de punto a punto. A continuación, se describe el procedimiento de la ejecución de la visión artificial, según Alvear, Farinango, Navarrete, Rosero, Noguera y Cuzme (2016):

Figura 2. Procedimiento de la ejecución de la visión artificial



Fuente: Alvear, Farinango, Navarrete, Rosero, Noguera y Cuzme (2016)

En la fase de adquisición la imagen es captada y se digitaliza; en el procesamiento se identifican características permitiendo eliminar partes que no son relevantes; en cuanto a la detección de bordes, se discrimina el fondo y la imagen principal separando los objetos de interés; posteriormente se realiza una segmentación de la imagen en donde se puede seleccionar los pixeles de acuerdo a los valores RGB (por sus siglas en inglés, red, Green, blue, los cuales corresponden a los colores primarios y que de allí deriva toda la gama de colores); `por último, se hace un reconocimiento por 3D y a partir de una triangulación, se puede seleccionar la imagen y que esta pueda ser interpretada.

6. IDENTIFICACIÓN BIOMÉTRICA

Desde el 9-11 (atentado a las Torres gemelas el 11 septiembre de 2001), los sistemas de análisis biométrico han aumentado considerablemente como una propuesta que ayude a mitigar los riesgos, específicamente en los cuerpos de seguridad aplicándolo en: control de

acceso lógico y físico, investigación forense, seguridad informática protección contra el fraude de identidad y prevención o detección del terrorismo. (Xiao, 2007)

Los sistemas de reconocimiento biométrico emplean la inteligencia artificial y funciona como un sistema autónomo que permite identificar características de personas ya sea por su morfología o por su comportamiento. Entre esta variable, se reconocen lo autentificadores, en los que se encuentran las huellas dactilares, la geometría de la mano, la cara, termograma facial, el iris, la retina, la voz, entre otros. Estas características al ser biológicas son estables y duraderas, pero se debe tener en cuenta los siguientes aspectos para que dicha característica pueda ser considerada válida para efectos del uso de inteligencia artificial sobre esta (Jain & Ross, 2008, p.15)

- Universalidad: todo individuo que acceda a la aplicación debe poseer el rasgo.
- Singularidad: el rasgo dado debe ser lo suficientemente diferente entre los individuos que comprenden la población .
- Permanencia: el rasgo biométrico de un individuo debe ser lo suficientemente invariable durante un período de tiempo con respecto al algoritmo de correspondencia. Un rasgo que cambia significativamente con el tiempo no es un biométrico útil.
- Medibilidad: debería ser posible adquirir y digitalizar el rasgo biométrico utilizando dispositivos adecuados que no causen inconvenientes indebidos al individuo. Además, los datos sin procesar adquiridos deben ser susceptibles de procesamiento para extraer conjuntos de características representativos.
- Rendimiento: la precisión del reconocimiento y los recursos necesarios para lograr esa precisión deben cumplir con las restricciones impuestas por la aplicación.
- Aceptabilidad: las personas de la población objetivo que utilizarán la aplicación deben estar dispuestas a presentar su rasgo biométrico al sistema.
- Circunvención: se refiere a la facilidad con que se puede imitar el rasgo de un individuo utilizando artefactos (por ejemplo, dedos falsos), en el caso de rasgos físicos y mimetismo, en el caso de los rasgos de comportamiento.

La identificación biométrica ha tenido un gran alcance de madurez, reflejado en la múltiple empleabilidad de estos sistemas, que ya no son solo empleados en espacios controlados, sino que han ganado campo en el uso cotidiano tal como en los celulares y

computadores. Esta amplia gama de aplicación, se debe a los avances que se han realizado gracias a la tecnificación y mejoras en sus diseños.

Específicamente en el campo de la seguridad ha sido parte fundamental en el control de acceso, en donde se emplea con mayor frecuencia las huellas dactilares, pues este tipo de reconocimiento ha mostrado ser altamente efectivo. Cabe resaltar que para efectos de la biometría en seguridad se debe establecer si lo que se busca es identificar o autenticar, pues el primero tendrá funciones de rastreo de comportamientos que podrían resultar amenazantes, en tanto la autenticación facilitaría el control de acceso al sitio que se custodia; ante tal evento, se podría pensar que en la zona residencial en Bocagrande, se propendería por identificar y así lograr mitigar los riesgos asociados a violencia.

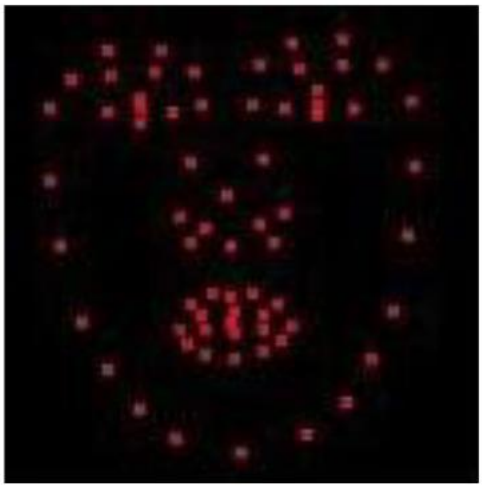
6.1. Reconocimiento facial

Uno de los modelos más avanzados en cuanto a inteligencia artificial supone, es el reconocimiento facial y de esta misma forma, ha sido el sistema más antiguo con el que cuentan los seres humanos para hacer el reconocimiento de otro. Partiendo de este hecho, se podría pensar que, este reconocimiento facial podría tener una alta capacidad de responder a verificación de identidad. El reconocimiento facial, según Cortés, Medina & Muriel (2010) permite:

> "(…) *clasificar la apariencia de la persona e intenta medir algunos puntos nodales del rostro como la distancia entre los ojos, el ancho de la nariz, la distancia del ojo a la boca, o la longitud de la línea de la mandíbula*" (p.99).

Al ser este un sistema de reconocimiento tridimensional, permite que se haga el reconocimiento de puntos estratégicos en el rostro que, como se cita anteriormente, perímete medir diferentes dimensiones; para ello, Gualdrón, Duque y Chacón (2013) realizan una ubicación de puntos en el rostro por medio del Active Shape Model (ASM), el cual es un modelo paramétrico que genera patrones y características que se pretendan determinar; el siguiente gráfico corresponde a un ejemplo de cómo se emplea el ASM:

Figura 3. Ejemplo del uso del ASM



Fuente: Gualdrón, Duque y Chacón (2013)

En la Feria Internacional de Seguridad (ESS), llevada a cabo en el 2018, se realizó exposición de cámaras que incluyen inteligencia artificial y que esta permite que se haga reconocimiento facial el cual contempla una base de datos en las que se almacena los rostros de las personas que accedan a algún espacio vigilado, y cada que algún sujeto este frente a la cámara, ésta la comparara y la asociara a alguna ya almacenada. Algunas especificaciones dadas por Martínez (2018) relacionadas con el proceso de este análisis biométrico permite que:

> "(…) *Las caras que no estén en la base de datos son captadas y reportadas como extraños y esta información es considerada como meta data en donde relaciona género, edad, si tiene gafas o montura facial; es decir, si tiene cubierto el rostro. Cuando el rostro captado se encuentra en la base de datos, la cámara reporta un porcentaje de coincidencia. Adicionalmente, este tipo de cámaras incluso reportan un mapa de calor identificando los espacios con mayor presencia de personas y los de menos asistencia*"

6.2. Reconocimiento de matrículas de vehículos

Otro sistema de control de acceso es el reconocimiento de las matrículas de los vehículos y este, también se realiza a través de la inteligencia artificial en el cual hace búsqueda de patrones, que en este caso sería la placa de un vehículo, funcionando de forma similar al reconocimiento facial, en donde hay una adquisición de la imagen, un

procesamiento para luego realizar un reconocimiento y así facilitar el ingreso o salida del vehículo, una vez esta haya sido debidamente reconocido por la cámara que cuenta con el sistema de inteligencia artificial. Según Navacerrada (2018), el sistema de reconocimiento de matrículas permite realizar diversos reconocimientos, entre los cuales se encuentra:

- Irregularidades o fraude en estaciones de servicio: Una estación de servicio en la que registre todos aquellos coches o clientes que abandonan la estación sin el pago correspondiente.
- Cruce de fronteras, control y seguridad.
- Control de acceso a aparcamientos.
- Sistemas de detección de irregularidades, fraude o mala conducción en carreteras
- Sistemas de control de velocidad de vehículos en carretera
- • Sistemas de control de velocidad media de vehículos
- Control de acceso a zonas restringidas. Calles peatonales, aeropuertos, zonas prohibidas, etc.
- Control de irregularidades en coches mediante Inspección técnica de vehiculas (ITV): Coches que más contaminan, coches en mal estado, ...
- Sistema de control de asistencia al trabajo, escuela, etc.

El sistema de reconocimiento de matrículas o también denominado ANPR (Automatic number plate recognition en inglés), es un sistema que facilita la vigilancia, haciendo uso de software empleando cámaras de reconocimiento óptico y con caracteres que permiten escanear imágenes. Se considera que este sistema puede escanear matriculas en un rango de 5 a 50 metros de acuerdo al modelo de la cámara que se use para el reconocimiento, así como de la velocidad al que circule el vehículo (Rodríguez, Vera &Vintimilla, 2012)

CONCLUSIONES

Cobra importancia en el desarrollo de este documento, el profundizar en el reconocimiento facial y el reconocimiento automatizado de matrículas de vehículos, ya que se desea documentar la importancia de pasar de contar con seguridad física a un sistema de vigilancia análogo y que esto permita que la seguridad privada se mantenga vigente y a la vanguardia, dando respuesta a las vicisitudes del contexto. Relacionado con la aplicabilidad de este modelo de inteligencia artificial aplicada a la analítica de video, reconocimiento

facial y matrículas de los vehículos, el cual facilite el control de acceso a zonas residenciales en donde, suele suceder que la rotación de personal es elevada y en ocasiones la presencia de un nuevo guarda de seguridad no permite que el acceso a la residencia sea cómoda o confiable.

El reconocimiento de matrículas haciendo uso de inteligencia artificial, se hace necesario en lugares en donde el acceso se realiza principalmente desde los parqueaderos, tal como podría ocurrir en el sector Residencial de Bocagrande; esto, permitiría minimizar los riesgos asociados al ingreso de personal no autorizado y que ello conlleve la comisión de hurtos a las viviendas de dicho sector.

Adicionalmente, el sistema de reconocimiento facial agudizaría el control de acceso evitando que la rotación de personal de vigilancia (que suele ocurrir con frecuencia), lo que por lo general suscita a dificultades en reconocer las personas que habitan usualmente estas zonas residenciales, y aún más difícil, el tener un control de los vehículos que suelen ingresar al sector. La implementación de sistemas que cuenten con inteligencia artificial permitiría la reducción de costos en seguridad física y la disminución de riesgos asociados a hurto o violencia.

REFERENCIAS

Alvear, V., Farinango, H., Navarrete, I., Rosero, P., Noguera, J., Cume, F. Y Peluffo, D. (2016). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura**.** *International Conference on Information Systems and Computer Science***.** Universidad Técnica del Norte. Ibarra, Ecuador.

Caonero, F., Godnick, W., Fernández, S., Bustamante, J. y Natenzon, S. (2011). Control y Regulación de las Empresas de Seguridad Privada en América Latina y el Caribe: un análisis comparativo. *Centro Regional de las Naciones Unidas para la Paz, el Desarme y el Desarrollo en América Latina y el Caribe (UNLIREC).* Perú, 187-266. Recuperado de : https://www.google.com/search?client=safari&rls=en&q=Control+y+Regulaci%C3%B3n+de+las+Empresas+de+Seguridad+Privada+en+Am%C3%A9rica+Latina+y+el+Caribe:+un+an%C3%A1lisis+comparativo&ie=UTF-8&oe=UTF-8

Chica, W. (2015). Diseño de un sistema de videovigilancia mediante un circuito cerrado te televisión, monitoreo remoto, notificación de eventualidades mediante SMS, utilizando el sistema GNOKII para la empresa Punotent S.A. (Tesis de pregrado). Escuela Politécnica Nacional. Quito, Ecuador.

Chillida, J. (2018) . ¿Qué es la seguridad electrónica? Consultado el 1 de octubre de 2018. Disponible en <http://www.informeticplus.com/que-es-la-seguridad- electrónica.

Cortés, j., Medina, A. Y Muriel, F. (2010). Sistemas de seguridad basados en biometría. *Scientia Et Technica.* 17 (46), 98-102. Recuperado en: http://www.redalyc.org/articulo.oa?id=84920977016

Dammert, L. (2007). Seguridad pública en América Latina. ¿qué pueden hacer los gobiernos locales?. *Nueva sociedad,* 212, 67-81. Recuperado de: https://www.researchgate.net/publication/320164031

Decreto (Ley) 356 de 1994. Congreso Nacional de la Republica de Colombia. Consultada el 29 de octubre de 2019.

Fillipo, V., Olarte, W. Y Cañón, B. (2009). Fundamentos de diseño para un circuito cerrado de televisión. *Scientia et Technica* . 42 (1), 46-50.

Gualdrón, O., Duque, O. Y Chacón, M. (2013). Diseño de un sistema de reconocimiento de rostros mediante la hibridación de técnicas de reconocimiento de patrones, visión artificial e ia, enfocado a la seguridad e interacción robótica social. 6 (1), 16-28 . Recuperado de: https://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/3

Jain, A., Flynn, P., & Ross, A. A. (2007). *Handbook of biometric.* New York: Springer Science & Business Media.

Ley 62 de 1993. Congreso Nacional de la República de Colombia. Consultada el 29 de octubre de 2019.

Martí, S. (2013). Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia (Tesis de pregrado.). Universidad Politécnica de Valencia. Valencia, España.

Martínez, A. Y Fornaguera, A. (1998). Analogía computacional del cerebro y la mente. *Revista médica del hospital Nacional de niños.* 33 (1), 1-16.. Costa Rica.

Martínez, J. (2018). La inteligencia artificial como herramienta innovadora en la video analítica . (Tesis de especialización). Universidad militar Nueva Granda, Bogotá, Colombia.

Montejo, J. (2013). Importancia de la seguridad física en Colombia como mecanismo de seguridad en el sector privado (Tesis de especialización). Universidad Militar Nueva Granada. Bogotá, Colombia.

Navacerrada, J. (2018). Sistema de detección de matrículas con Open CV . (Tesis de maestría) Universidad Politécnica de Madrid. Madrid, España.

Paladines, G. y Villavicencio, J. (2013). Implementación de equipos de monitoreo y seguridad basado en cámaras IP en el almacén Lindón García representaciones del cantón Tosagua (Tesis de pregrado). Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López. Calceta.

Perez, C. (2018). El sector de seguridad y vigilancia privada: Evolución reciente y principales retos laborales, regulatorios y de supervisión. Fedeseguridad. Bogotá, Colombia.

Pinzón, J. (2018). Seguridad electrónica: apoyo en el sector residencial como elemento material probatorio en la materialización de los riesgos (Tesis de especialización). Universidad Militar nueva Granada. Bogotá, Colombia.

Rodríguez, H., Vera, R. Y Vintimilla, B. Detección y extracción de placas de vehículos en señales de vídeo. Revista tecnológica ESPOL. 25 (1), 1-11.

Sanabria, J. Y Archila, J. (2011). Detección y análisis de movimiento usando visión artificial. Scientia et Technica. 49, 180-188. Recuperado de http://revistas.utp.edu.co/index.php/revistaciencia/article/view/1513

Stella, M. y Mendez, B. (2013). Colombia: Vigilancia, seguridad privada y manejo de armas 1994 -2013. Secretaría de Gobierno de Bogotá. Bogotá, Colombia, 241-275. Recuperado de: https://www.lamjol.info/index.php/RPSP/article/view/1576

Tecnología, Acceso & Seguridad. (2018). Video Analítica. Guatemala. Tomado de http://www.tas-seguridad.com/video-analitica/

Xiao, Q. (2007). Biometrics—Technology, Application, Challenge, and Computational Intelligence Solutions. IEEE Computational intelligence magazine. 5-25, Canadá. Recuperado de:

https://www.researchgate.net/publication/3455537_Technology_review_-_Biometrics-Technology_Application_Challenge_and_Computational_Intelligence_Solutions?enrichId=rgreq-6e1129300a95540eec922caca9dca43a-XXX&enrichSource=Y292ZXJQYWdlOzM0NTU1Mzc7QVM6Mzk2MDc0OTIyNTk0MzA2QDE0NzE0NDMwMjg1NDk%3D&el=1_x_2&_esc=publicationCoverPdf