La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

Sistema de seguridad basado en un sistema embebido con cámara para día y noche con enlace IoT

Aldo-Francisco Muñoz-Vargas[1], Juan-Manuel Ramos-Arreguín✉, Saúl-Tovar Arriaga, Marco-Antonio Aceves-Fernandez, Jesus-Carlos Pedraza-Ortega

Universidad Autónoma de Querétaro, Facultad de Ingeniería
✉jsistdig@yahoo.com.mx, [1]aldomuoz98@gmail.com

Resumen

El desarrollo de sistemas de seguridad es muy útil y puede incluir dispositivos como cámaras infrarrojas y sistemas embebidos basados en microprocesadores y microcontroladores. Además, con el uso de sensores infrarrojos, se aumenta el tiempo de vigilancia, ya que estos pueden trabajar aún con la ausencia de luz. Una cámara de infrarrojos permite que la cámara siga captando imágenes incluso en condiciones de oscuridad, usando una lámpara de luz infrarroja. La integración que aquí se propone, lleva todos esos conceptos combinándolos con el internet de las cosas y una aplicación basada en Android, en la que una persona puede interactuar y revisar los datos generados por el sistema en cualquier momento mientras tenga una conexión a internet. El sistema operativo de la tarjeta Raspberry Pi se llama Raspberry Pi OS, la cual es una versión ligera de Linux. Así mismo, se propone una carcasa donde es montado el sistema completo, para contar con un prototipo funcional. La carcasa es un diseño propio y fue impresa en 3D, para ser montado en interiores, haciendo de este proyecto una opción potencial para aplicaciones de vigilancia. Se desarrollaron pruebas en condiciones de ausencia de luz, y los resultados fueron satisfactorios.

Palabras clave: Cámara infrarroja, cámara Pi, Raspberry Pi, Android, sensor de infrarrojos, Internet de las cosas (IoT).

Abstract

The development of security systems is especially useful and can include devices such as infrared cameras and embedded systems based on microprocessors and microcontrollers. In addition, with the use of infrared sensors, the monitoring time is increased since they can work even in the absence of light. An infrared camera allows the camera to continue to capture images even in dark conditions, using an infrared light lamp. The integration proposed here takes all these concepts, combining them with the Internet of Things and an Android-based application, in which a person can interact and review the data generated by the system at any time while having an Internet connection. The operating system of the Raspberry Pi board is called Raspberry Pi OS, which is a lightweight version of Linux. Likewise, a housing is proposed where the complete system is assembled, to have a functional prototype, with an own design and was printed in 3D, to be mounted indoors, making this project a potential option for surveillance applications. Tests were carried out in the absence of light, and the results were satisfactory.

Keywords: Infrared Camera, Pi camera, Raspberry Pi, Android, Infrared Sensor, Internet of Things (IoT).

1. Introducción

Desafortunadamente, México es conocido por tener un problema con todo tipo de inseguridad, hasta 2745 casos de robos a casa habitación por cada 100,000 personas ocurrieron en 2017 [1]. Específicamente, el robo de bienes materiales puede prevenirse, evitarse o frustrarse cuando se observa al presunto ladrón [2]. Sin embargo, si el robo ocurre de todos modos, tener un dispositivo que capturó evidencias del momento puede hacer la diferencia en el proceso de justicia.

Cada vez más aplicaciones han sido desarrolladas utilizando internet de las cosas, por lo que en este proyecto también se hace uso de esta tecnología, tomando ese concepto de comunicación que ha evolucionado de humano-humano, humano-cosa y finalmente entre cosas con cosas [3].

El sistema embebido *Raspberry Pi* fue ideado para cursos de programación de estudiantes, por lo que es económico. Este es un punto realmente importante para un sistema de seguridad que está destinado a funcionar durante largas horas haciendo probable su avería. Además, la cantidad de *IO* (Entradas y Salidas) es importante y hace que esta placa sea perfecta para este tipo de proyectos [4].

Algunas aplicaciones relacionadas con este desarrollo han utilizado sistemas embebidos como *Raspberry Pi* debido al bajo costo y las opciones versátiles como la cámara, las entradas y salidas digitales, y sus capacidades informáticas con un sistema *Linux* [5].

Asimismo, en 2017, utilizando los mismos elementos (*Raspberry Pi*, sensores infrarrojos y una cámara) se desarrolló un prototipo de sistema de vigilancia para detectar movimiento en la puerta de una tienda cada 10 segundos, enviando un correo electrónico en caso de movimiento con la imagen adjunta, haciendo saber al propietario de la situación [6].

En 2018 se desarrolló un sistema de seguridad basado en un sensor de contacto, un alambrado eléctrico, una alarma sonora, una cámara y una Raspberry Pi. Este consiste en el control de los elementos anteriores desde una aplicación en Android y en la cual es posible la visualización de forma remota del inmueble en vigilancia, dando así al usuario la oportunidad de tomar acciones y activar los elementos previamente mencionados si así lo considera, evitando o al menos retrasando la entrada de un posible delincuente [7].

En 2018, se continúa desarrollando sistemas de vigilancia basados en sistemas embebidos, como el trabajo de Jayakumar [8], donde se propone el desarrollo de un sistema de vigilancia usando una tarjeta Raspberry Pi y una cámara, que se basa en detección de movimiento de personas y detección de rostros, agregando seguimiento de la persona.

En 2019 se presentó un sistema de seguridad físico que utiliza internet de las cosas mediante una plataforma llamada *Zolertia Remote*, tratando de dar una alternativa al de vigilancia. Consta de tres secciones, una red de sensores inalámbrica, un servidor privado *MQTT* (*Message Queue Telemetry Transport*) y una aplicación *Android* [9].

En 2020 se llevó a cabo una aplicación similar a las anteriores en la que mediante una *Raspberry Pi* como servidor se controló un conjunto de cámaras a través de una aplicación en *Android*, este sistema fue desarrollado de modo que en caso de detección de cambio del entorno se tomarían imágenes o videos guardándose en la memoria de la *Raspberry* y enviando un correo de alerta o notificaciones en la aplicación móvil, siendo estos datos accesibles a través de la aplicación que consultaría los datos del servidor [10].

En el presente trabajo se propone un sistema de seguridad capaz de operar en condiciones de poca o nula iluminación mediante el uso de una cámara con capacidad para observar luz infrarroja y una lámpara que emita esta luz, este tipo de situación relacionado en variaciones de la iluminación no es muy tomado en cuenta en antecedentes consultados relacionados con sistemas basados en

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

Raspberry Pi, así como la accesibilidad de los datos desde cualquier punto. Por lo que resulta en un área de oportunidad en el desarrollo de sistemas de seguridad basados en Raspberry Pi y mediante el uso del concepto de IoT.

2. Materiales y metodología

En esta sección se describen algunos de los elementos de hardware y software utilizados para el funcionamiento de este prototipo, así como la metodología utilizada.

2.1 Materiales

Detectores de radiación infrarroja: Existen diversos tipos de detectores de esta radiación, uno de ellos son los detectores térmicos, estos absorben la radiación incidente, cambiando la temperatura del detector y permaneciendo en un estado de que tiende al equilibrio en función de los cambios de la radiación, tres de los más utilizados son: los bolómetros termopilas y detectores piroeléctricos. Para este caso se explorarán los detectores piroeléctricos. La figura 1 muestra una configuración de un detector piroeléctrico.

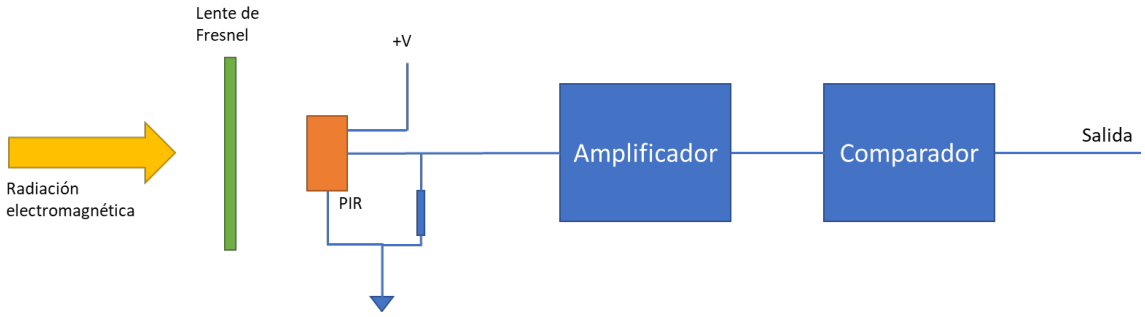


Figura 1. **Configuración típica de un detector piroeléctrico [11].**

Detectores piroeléctricos: Están hechos de un material que genera una carga eléctrica cuando se expone a la radiación infrarroja. Cuando la cantidad de radiación infrarroja cambia, también lo hace la carga, esto genera un voltaje que al ser amplificado puede tener diversas aplicaciones. En la figura 1 se observa un diagrama del funcionamiento de este detector. Suele utilizarse una lente de Fresnel la cual focaliza la radiación sobre el elemento primario, mientras el amplificador y comparador tratan la señal de modo que esta esta pueda a ser leída por un microcontrolador o sistema embebido [11]. A continuación, en la figura 2 se observa un Sensor Piroeléctrico Infrarrojo (*PIR*) el cual consta de lo descrito anteriormente.

Figura 2. Sensor Piroeléctrico Infrarrojo PIR [12] [13].

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

Cámaras y formación de imágenes: Una imagen se forma cuando una escena luminosa en 3D es proyectada sobre un plano 2D, las cámaras realizan este proceso; en una cámara cada punto de la escena se debe proyectar a un punto de la imagen dando así lugar a una imagen enfocada, lo anterior se muestra en la figura 3 [14].

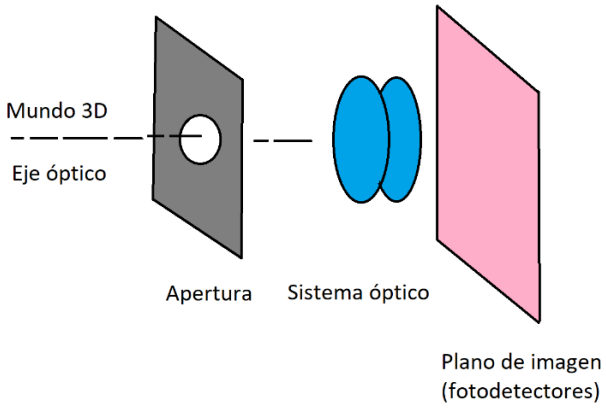


Figura 3. Modelo de cámara simplificado [14].

En el proceso de toma de imágenes, se hace uso de un proceso compuesto por captura y digitalización, donde una señal analógica es discretizada y enviada como señal digital a un ordenador. Este proceso se muestra en la figura 4 [14].

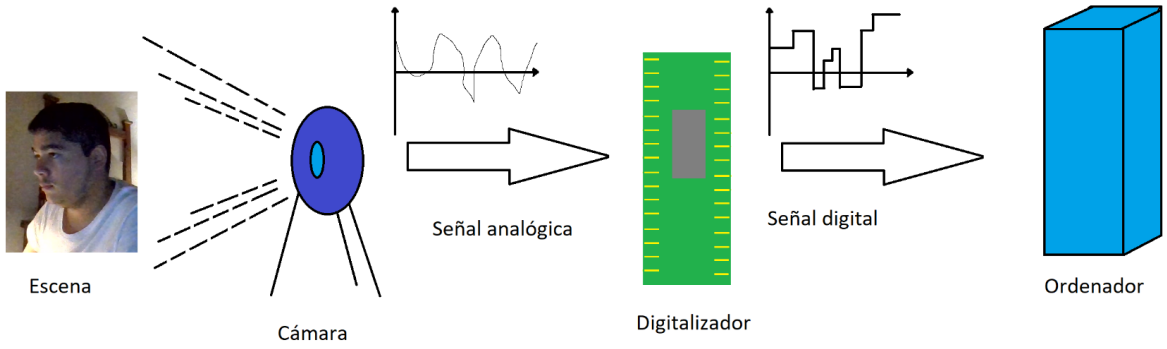


Figura 4. Proceso de captura y digitalización de imágenes [14].

Un dispositivo de captura determina los factores que tendrá la imagen final, tales como el tamaño de imagen, tamaño de pixel, el tipo de radiación que la cámara es capaz de captar, entre otras [14].

Dentro de un dispositivo de captura en el filtro de color existe un arreglo de sensores, el cual se denomina patrón de Bayer, donde el 50% de los sensores son verdes, el 25% son rojos y el otro 25% son azules. Esto se debe a que el ojo humano es más sensible al color verde que a los demás colores primarios. Esto se puede observar en la figura 5.

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

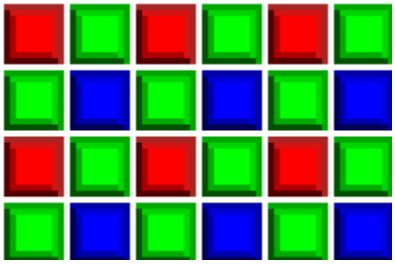


Figura 5. Distribución típica de un filtro de color [15].

La cámara NoIR utilizada en este prototipo, no posee un filtro infrarrojo haciendo posible que se detecte este tipo de luz [16]. En la figura 6 se observa una imagen tomada por la noche, usando solamente una lámpara infrarroja, y en la figura 7 se muestra la imagen tomada con iluminación artificial.

Figura 6. Imagen capturada por la cámara NoIR con iluminación infrarroja.

Figura 7. Imagen capturada por la cámara NoIR con luz visible.

2.2 Seguridad y conexiones con la nube.

Además de las enormes oportunidades que brinda *IoT*, existen varios problemas y preocupaciones relacionados con los sistemas integrados en términos de sus vulnerabilidades de red, estos problemas se pueden prevenir mediante técnicas de cifrado en las que un mensaje puede leerse con una firma especial. Estas técnicas son computacionalmente intensivas [17], de manera que, para evitar estos problemas de seguridad, se propone utilizar una nube de terceros para asignar todas esas cargas computacionales a otros, manteniendo al mismo tiempo almacenada y accesible la información recopilada por el sistema en cualquier momento y lugar.

Mega es un servicio en la nube que se propone para esta aplicación debido a la compatibilidad con Linux, en este servicio, los archivos se cifran antes de cargarlos y se descifran después de descargarlos utilizando una clave creada por el cliente, que se deriva de la contraseña. Utiliza un estándar de cifrado avanzado (*AES*), que es un algoritmo común para el cifrado de datos. Esto ofrece un buen nivel de seguridad con respecto a la información capturada por el sistema en caso de que alguien quiera robar o borrar el contenido. Es importante notar que existen varias vulnerabilidades sobre los datos que deja *Mega* mientras se usa en un navegador, afortunadamente, la aplicación para *Linux* no tiene ese problema [18] [19].

A continuación, en la tabla 1 se muestran los materiales que componen al sistema completo.

Tabla 1. Tabla de materiales.

Descripción	Cantidad
Raspberry Pi 3B+	1
NoIR Camera	1
PI Camera	1
5 V DC Power Supply	1
32 GB SD card	1
PIR sensor	1
Case	1

2.3 Metodología

La metodología seguida en el desarrollo e integración de este prototipo consta de las etapas mostradas en la figura 8 y descritas posteriormente.

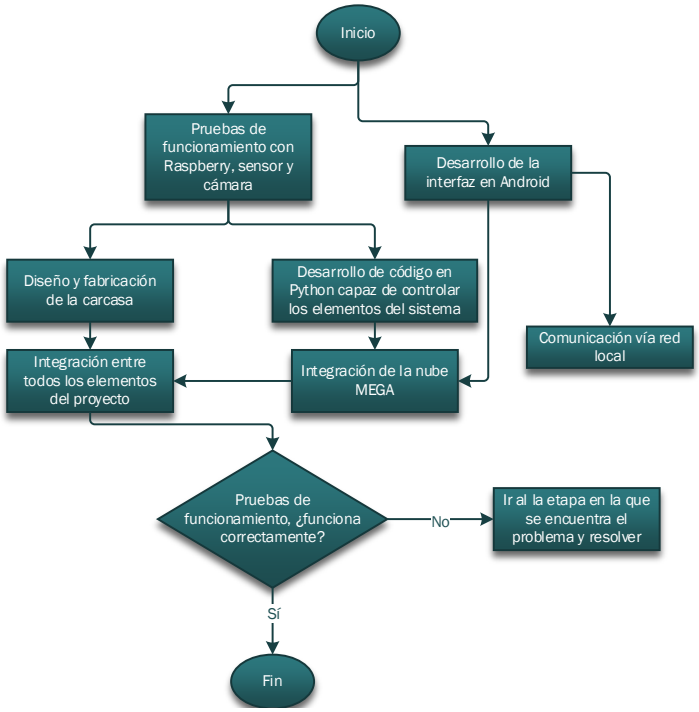


Figura 8. Diagrama de la metodología.

En la sección de pruebas de funcionamiento con Raspberry, sensor y cámara, se requiere implementar un algoritmo en una interfaz en Linux, desde la cual se pueden realizar pruebas del hardware como el sensor PIR, con la cámara.

Del mismo modo se requiere de una investigación sobre cómo conectar el sistema embebido, utilizando Python, con otros dispositivos a través de internet mediante conexiones locales, así como el desarrollo del código en Python que controlara todos los elementos. Por lo que esta tarea se observa en el recuadro de desarrollo de código en Python capaz de controlar los elementos del sistema.

En paralelo, se comenzó con el desarrollo de la interfaz en Android Studio. Esta interfaz móvil debe controlar a la Raspberry Pi, por lo que se requirió primero de una investigación de conexiones de red local en Android entre un teléfono y un sistema embebido como la Raspberry Pi. Una vez logrado esto se plantea el desarrollo de la interfaz en Android capaz de controlar el sistema de seguridad.

De igual forma, en paralelo, se trabaja en el diseño de una carcasa que se adapte a las necesidades del proyecto, para contener a los elementos del sistema y poder ajustar el ángulo de visión de la cámara.

En el trabajo con Internet de las Cosas, se usa la plataforma MEGA, para el almacenamiento de las fotos, debido a sus capacidades de integración con Linux y Android.

Finalmente, se elaboró la interconexión entre todos los elementos de hardware (Raspberry Pi, cámara, PIR y teléfono celular) a través de una interfaz en la que se puede controlar el algoritmo desarrollado en el sistema embebido mediante una aplicación en Android.

3. Resultados

En la figura 9, se puede observar el funcionamiento general del sistema de seguridad. La pieza central es la tarjeta Raspberry Pi, que tiene una comunicación continua con el dispositivo móvil. Este dispositivo se usa para configurar la manera de funcionar del sistema de seguridad. La nube MEGA se usa para almacenar las imágenes, y se permite la consulta de las imágenes capturadas desde cualquier lugar con una conexión a internet. Debe señalarse que por cuestiones de ahorro de almacenamiento tanto local como en la nube se decidió que, habiendo detectado movimiento, solo se capturaran imágenes en un intervalo que ronda los 3 segundos o menos. Como se observa en el diagrama, cada imagen registrada es nombrada con la fecha de captura para facilitar al usuario información sobre la misma.

3.1 Software.

Para este caso, existen varias formas de interactuar con el sistema, una de ellas consiste en el uso de sockets a través de un servidor y un cliente, donde el servidor puede recibir y responder a los mensajes del cliente en todo momento mientras están en la misma red. Se decidió usar el sistema embebido de la Raspberry Pi como servidor, mientras que el cliente, al ser cualquier tipo de dispositivo compatible con el uso de sockets, es la aplicación en Android Studio.

El uso de sockets permite ofrecer compatibilidad entre dispositivos, independientemente de su arquitectura. Por otro lado, el alcance de este software solo permite al usuario modificar parámetros del sistema de seguridad cuando se encuentra en la misma red, por lo que para monitorear remotamente se usa una carpeta en la nube, en la cual se recopilan todos los archivos (imágenes). Cuando se detecte movimiento, se almacenan las imágenes con su respectiva fecha y hora de captura.

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

En la figura 10 se muestra el menú de las imágenes capturadas. En el título de cada imagen se muestra la fecha y hora. En la figura 11 se muestran dos capturas de la aplicación en Android, donde una persona fue captada caminando frente al sistema mientras estaba funcionando.

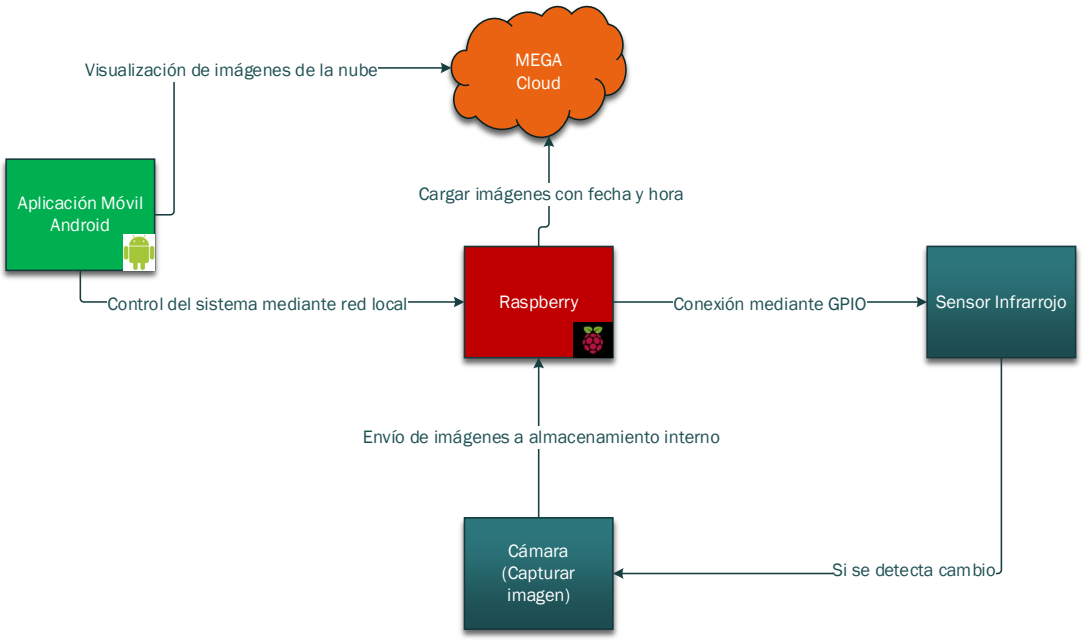


Figura 9. Funcionamiento general del sistema de seguridad.

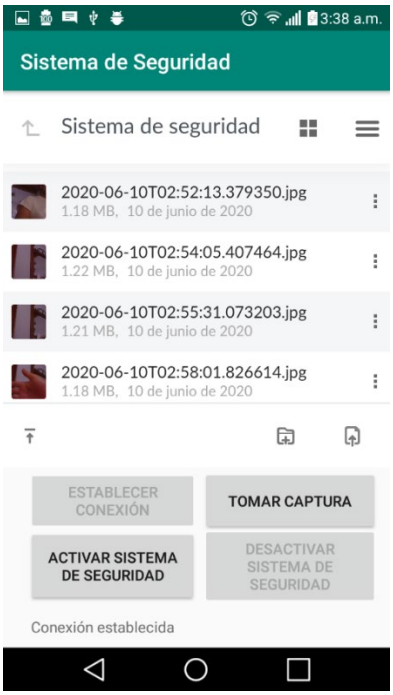
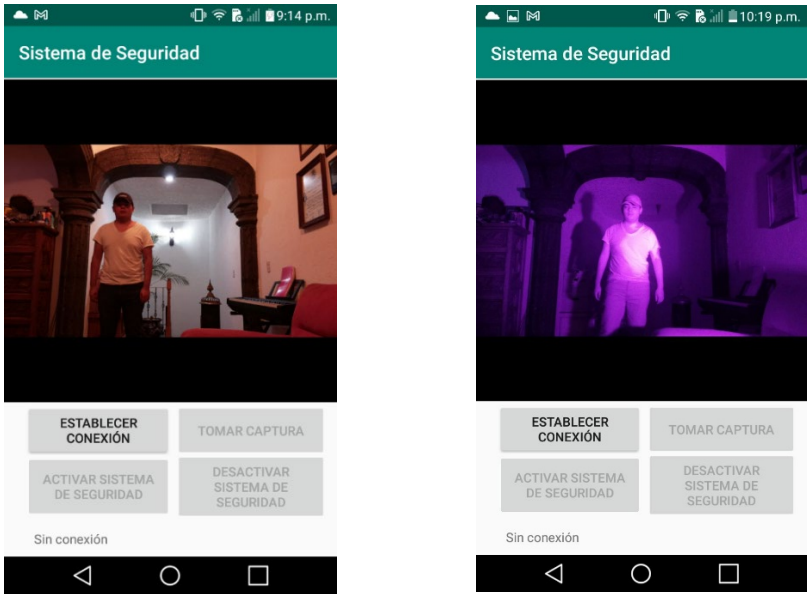


Figura 10. Aplicación móvil en funcionamiento.

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

1.1 Diseño de la carcasa.

En la figura 12 se presenta una vista del diseño de la carcasa usando software de CAD/CAM. Para el diseño se toma en cuenta los componentes que el sistema va a requerir, como son: el sistema embebido Raspberry Pi, cámara, sensor de presencia PIR, alimentación, principalmente. La figura 13 es el resultado de la impresión en 3D de la carcasa, con todos los componentes electrónicos instalados. Las dimensiones de la carcasa son 9.5 x 6.5 x 9.5 cm.



(a) (b)

Figura 11. Aplicación móvil en funcionamiento mostrando una imagen desde la nube. (a) Con luz artificial. (b) En ausencia de luz.

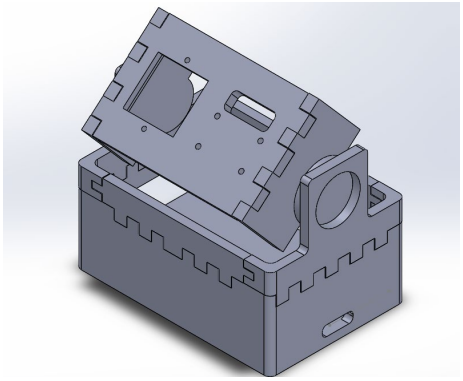


Figura 12. Modelo en 3D de la carcasa.

En la figura 14, se muestra una imagen donde el sistema captura a una persona pasando dentro del alcance del sistema de vigilancia. En este caso, la imagen se toma con luz visible. La figura 15 muestra el mismo caso, pero en esta ocasión, el lugar está a obscuras, por lo que se enciende la lámpara de infrarrojos.

La Mecatrónica en México, Enero 2021, Vol. 10, No. 1, páginas 35 – 46
Disponible en línea en www.mecamex.net/revistas/LMEM
ISSN: 2448-7031, Asociación Mexicana de Mecatrónica A.C

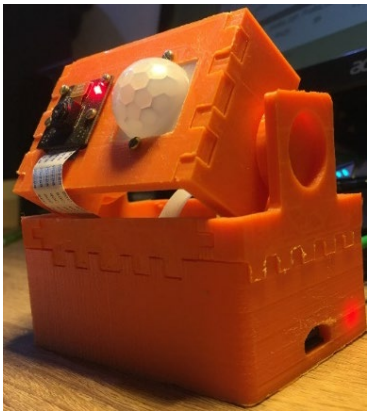


Figura 13. Carcasa impresa con los elementos de hardware.

Figura 14. Imagen en condiciones de luz visible.

Figura 15. Imagen en condiciones de luz infrarroja.

2. Conclusiones

Después de pruebas de funcionamiento del sistema se determinó que puede usarse como una medida de prevención al dejarse funcionando al salir del sitio donde este se encontrase, mandando este imágenes en caso de que alguien entrase en la zona donde este opera, sin embargo, también se

encontraron algunos problemas relacionados principalmente con imágenes capturadas por el sistema cuando nada sucedía en la imagen, la mayoría de ellas cercanas en tiempo al desencadenamiento de la señal de salida del sensor PIR debido al movimiento de alguien, pero también algunas otras totalmente aleatorias, por ello futuro trabajos principalmente desde el punto de vista de procesamiento de imágenes podrían ser sumamente útiles para un problema como este.

Por otro lado, la frecuencia con la que se capturan imágenes una vez que detectó movimiento podría mejorarse, afortunadamente, al estar este prototipo desarrollado en Python y en Linux, es sumamente accesible realizar cambios o implementar nuevas secciones en cuanto a código se refiere.

Referencias

[1] I. N. de E. y Geografía (INEGI), «Incidencia delictiva», *Encuestas en establecimientos. Especiales. Encuesta Nacional de Victimización de Empresas. ENVE, Encuestas en hogares. Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública. ENVIPE*, ene. 01, 2010. https://www.inegi.org.mx/temas/incidencia/ (accedido sep. 28, 2020).

[2] R. Macías Acosta, J. C. Macías Ponce, y M. Díaz Flores, «Programa para la Seguridad Nacional en México y su gasto aplicando sistemas de preferencias», *Rev. Venez. Gerenc.*, 2019, doi: 10.37960/revista.v24i2.31496.

[3] Lu Tan y Neng Wang, «Future internet: The Internet of Things», en *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, ago. 2010, vol. 5, pp. V5-376-V5-380, doi: 10.1109/ICACTE.2010.5579543.

[4] M. Richardson y S. Wallace, *Getting Started with Raspberry Pi*. O'Reilly Media, Inc., 2012.

[5] «Buy a Raspberry Pi 3 Model B – Raspberry Pi». https://www.raspberrypi.org/products/raspberry-pi-3-model-b/ (accedido oct. 01, 2020).

[6] C. A. G. Godoy y O. J. S. Parra, «Sistema de seguridad para locales comerciales mediante Raspberry Pi, cámara y sensor PIR», *Rev. Virtual Univ. Católica Norte*, vol. 0, n.º 51, Art. n.º 51, ago. 2017.

[7] J. S. Agressoth Cardona y S. Murillo Román, «Sistema de seguridad electrónico IOT contra intrusión para inmuebles, con estructura de control, mediante aplicación en Android», nov. 2018, Accedido: oct. 14, 2020. [En línea]. Disponible en: http://repository.udistrital.edu.co/handle/11349/22444.

[8] A. J. K. Jayakumar y S. Muthulakshmi, «Raspberry Pi-Based Surveillance System with IoT», en *Intelligent Embedded Systems*, Singapore, 2018, pp. 173-185, doi: 10.1007/978-981-10-8575-8_19.

[9] A. Cunalata y D. Alberto, «Desarrollo de un prototipo de sistema de seguridad contra intrusos utilizando protocolos de IoT sobre la plataforma Zolertia Remote», jul. 2019, Accedido: oct. 14, 2020. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/20318.

[10] J. Marín Rodríguez, «Desarrollo de un sistema de video vigilancia con servidor VPN Raspberry Pi y APP para móvil.», may 2020, Accedido: oct. 14, 2020. [En línea]. Disponible en: https://riunet.upv.es/handle/10251/143050.

[11] B. Fontal, *El espectro electromagnetico y sus aplicaciones*, vol. 1. Escuela Venezolana para la Enseñanza de la Química, 2005.

[12] «Artículo | Omniblug». http://www.omniblug.com/sensor-movimiento-pir-arduino.html (accedido oct. 23, 2020).

[13] M. Moghavvemi y Lu Chin Seng, «Pyroelectric infrared sensor for intruder detection», en *2004 IEEE Region 10 Conference TENCON 2004.*, nov. 2004, vol. D, pp. 656-659 Vol. 4, doi: 10.1109/TENCON.2004.1415018.

[14] García, Ginés, «Procesamiento Audiovisual», *ginés garcía mateos*, 2010. http://dis.um.es/profesores/ginesgm/pav.html (accedido oct. 23, 2020).

[15] Cambridge in Colour, «Compact vs. Digital SLR Cameras», 2020. https://www.cambridgeincolour.com/tutorials/compact-vs-digital-slr-cameras.htm (accedido nov. 01, 2020).

[16] «Camera Module - Raspberry Pi Documentation». https://www.raspberrypi.org/documentation/hardware/camera/ (accedido oct. 23, 2020).
[17] A. Ukil, J. Sen, y S. Koilakonda, «Embedded security for Internet of Things», en *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, mar. 2011, pp. 1-6, doi: 10.1109/NCETACS.2011.5751382.
[18] S. Thamburasa, S. Easwaramoorthy, K. Aravind, S. B. Bhushan, y U. Moorthy, «Digital forensic analysis of cloud storage data in IDrive and Mega cloud drive», en *2016 International Conference on Inventive Computation Technologies (ICICT)*, ago. 2016, vol. 3, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7830159.
[19] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, y K.-K. R. Choo, «Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices», *Aust. J. Forensic Sci.*, vol. 48, n.º 6, pp. 615-642, nov. 2016, doi: 10.1080/00450618.2015.1110620.

Autores

Aldo Francisco Muñoz Vargas. Estudiante de la carrera de Ingeniería en Automatización de la Facultad de Ingeniería de la Universidad Autónoma de Querétaro. Miembro del capítulo de honor Mu Psi - Eta Kappa Nu de la IEEE.

Juan Manuel Ramos Arreguín. Tiene Doctorado en Ciencias y Tecnología con Especialidad en Mecatrónica en el Centro de Ingeniería y Desarrollo Industrial. Con Maestría en Ingeniería Eléctrica con opción en Instrumentación y Sistemas Digitales en la Universidad de Guanajuato. La ingeniería en Comunicaciones y Electrónica en la Universidad de Guanajuato. Fue Presidente de la Asociación Mexicana de Mecatrónica en el periodo 2013 a 2016. Pertenece al SNI en nivel I. Cuenta con reconocimiento al perfil PRODEP. A partir de 2017 es Senior Member en el IEEE. Profesor de tiempo completo en la Universidad Autónoma de Querétaro, en la Facultad de Ingeniería.

Saúl Tovar Arriaga. Obtuvo su grado de Licenciatura en Ingenieria en Electrónica en el Instituto Tecnológico de Querétaro, su Maestria en Ciencias en Mecatrónica en la Universidad de Siegen, Alemania, y su Doctorado en Ciencias Biomédicas en la Universidad de Erlangen-Nuremberg, Alemania. Actualmente es profesor de tiempo completo e investigador en la Universidad Autónoma de Querétaro. Sus intereses de investigación incluyen robótica médica, diagnostico automatizado por imagen y visión por computadora.

Marco Antonio Aceves Fernández. El Dr. Marco Antonio Aceves Fernández es Ingeniero en Telemática por la Universidad de Colima en el año 2000, obtuvo su Maestría y su Doctorado en el área de Sistemas Inteligentes en la University of Liverpool, Reino Unido, éste último en el año 2005. Ha sido reconocido como miembro del Sistema Nacional de Investigadores (SNI) por parte del CONACyT de manera ininterrumpida desde el 2009. Es miembro Senior de la IEEE y Presidente honorario de la Asociación Mexicana de Software Embebido. Sus intereses incluyen Sistemas Inteligentes y Embebidos.

Jesús Carlos Pedraza Ortega. Realizó sus estudios de Maestría en la FIMEE, Universidad de Guanajuato. Obtuvo el Doctorado en Ingeniería Mecánica con especialidad en Robótica - Sistemas de Reconstrucción 3D en la University of Tsukuba en Japón, donde trabajó con el desarrollo de un sistema monocular de reconstrucción 3D utilizando. Como docente, ha impartido diferentes cursos en los tres niveles de estudios (Licenciatura, Maestría y Doctorado) desde 1997, actualmente en la Universidad Autónoma de Querétaro. Es Senior Member por la IEEE y es miembro de la Academia Mexicana de Ciencias. Sus líneas de investigación son sistemas de reconstrucción 3D, inteligencia artificial aplicada a sistemas de visión, entre otros.