REVISTA VIRTUAL
Universidad Católica del Norte
CATÓLICA DEL NORTE Fundación Universitaria
Pioneros en educación virtual
http://revistavirtual.ucn.edu.co
No. 51 | Mayo-Agosto, 2017
ISSN-0124-5821 (en línea)

Cómo citar el artículo

González, C. & Salcedo, O. (2017). El acompañamiento educativo como estrategia de cercanía impulsadora del aprendizaje del estudiante. *Revista Virtual Universidad Católica del Norte, 51,* 175-193. Recuperado de http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/851/1369

Sistema de seguridad para locales comerciales mediante Raspberry Pi, cámara y sensor PIR*

Carlos Andrés González Godoy
Estudiante de Ingeniería de Sistemas, Universidad Distrital Francisco José de Caldas
Miembro del Grupo de Investigación "Internet Inteligente"
caagonzalezg@correo.udistrital.edu.co

Octavio José Salcedo Parra
Ingeniero de sistemas
Magíster en Economía
Magíster en Teleinformática
Doctor en Estudios Políticos
Doctor en Ingeniería Informática
Investigador Senior, Colciencias
Profesor de Planta, Universidad Distrital Francisco José de Caldas
Director del Grupo de Investigación "Internet Inteligente"
osalcedo@udistrital.edu.co

Recibido: 22 de septiembre de 2016.
Evaluado: 18 de mayo de 2017.
Aprobado: 24 de mayo de 2017.

Tipo de artículo: investigación científica y tecnológica.

* Este artículo es producto de un trabajo de investigación con el mismo título que fue llevado a cabo en la Universidad Distrital Francisco José de Caldas, en el proyecto de Ingeniería de Sistemas. Grupo de investigación: "Internet Inteligente" de Colciencias. En el trabajo participaron Carlos Andrés González Godoy y Octavio José Salcedo Parra, PhD. La investigación fue financiada por la Universidad Distrital Francisco José de Caldas. Fecha de inicio: 12 de febrero de 2016; fecha de finalización: 19 de agosto de 2016.

Resumen
Este artículo está enfocado en proveer un sistema para prevenir robos en locales comerciales, utilizando un ordenador de placa Raspberry Pi 2 modelo B, una cámara y un sensor de infrarrojos, los cuales permiten conocer si existe movimiento en la puerta del local comercial en periodos de 10 segundos. Esta información se envía por medio de un mensaje de correo electrónico, adjuntando la captura de la imagen; de esta manera, el propietario toma una decisión de acuerdo a la situación. Para la integración de este sistema es necesario el uso del sistema operativo Raspbian y configuración de un servidor de SMTP para el envío de la foto capturada al correo electrónico. El sistema garantiza la detección en un 90 % bajo los parámetros de distancia y grados del sensor respecto al sospechoso, pero es dependiente de la iluminación que se tenga para la captura de la imagen; de esta manera, es una alternativa de seguridad funcional.

Palabras clave
Cámara, Correo electrónico, Raspberry Pi, Sensor PIR.

Security System for Commercial Stores by Raspberry Pi, Camera, and PIR Sensor

This paper is focused on providing a system to prevent theft in stores, using a computer plate (Raspberry Pi Model B), a camera, and infrared sensor, which allow to know if there is movement in the door of the store in periods of 10 seconds. This information is sent through a message via e-mail, attaching the image capture; in this way, the owner makes a decision according to the situation. For the integration of this system, it is necessary to use the Raspbian operating system and configuration of an SMTP server for sending the photo captured to an email address. The system ensures detection by 90% under the parameters of distance and degree sensor from the suspect, but is dependent on the lighting that has to capture the image; in this way, it is an option in functional safety.

Keywords
Camera, Email, PIR Sensor, Raspberry Pi.

Système de sécurité pour les magasins par Raspberry Pi, la caméra et le capteur PIR

Cet article présente un système pour empêcher le vol dans les magasins, en utilisant une ordinateur Raspberry Pi 2 Modèle B, une caméra et un capteur infrarouge ; ce système nous permet de savoir s'il y a un mouvement à la porte des locaux commerciaux. Ces informations sont envoyées par un courrier électronique, avec la capture d'image ; De cette façon, le propriétaire prend une décision en fonction de la situation. Pour l'intégration de ce système, il est nécessaire d'utiliser la configuration Raspbian d'un serveur SMTP pour l'envoi de l'image dans un courrier électronique. Le système assure la détection de 90% selon des paramètres de degrés de distance et de capteur par rapport au suspect, mais son fonctionnement dépend de la lumière pour capturer l'image ; Il est donc une alternative en ce qui concerne la sécurité fonctionnelle.

Introducción

La seguridad es un aspecto a considerar por parte de los dueños de locales comerciales. Aunque se han establecido medidas entre las que se cuentan monitoreo de cámaras, alarmas y patrullajes de la Policía, estos últimos no han sido suficientes debido a que sus tiempos de operación son variables, circunstancia aprovechada por la delincuencia para cometer los robos en cuestión de minutos; además, la mayoría de estos locales no cuenta con sistemas de seguridad. Según un estudio publicado

en el diario *El Espectador* (2015), el aumento de los índices de robo de locales comerciales en la ciudad de Bogotá (Colombia) pasó a una cifra de 6.550 denuncias, siendo la localidad Antonio Nariño donde más aumentó debido a las zonas comerciales.

Con lo anterior, la mayoría de los dueños de estos establecimientos comerciales en la localidad Antonio Nariño no disponen del mecanismo para protegerse y tomar decisiones en tiempo real frente a eventualidades de esta naturaleza. Además, se presentan muchas fallas como falsas alarmas y los mencionados tiempos prolongados entre patrullajes, situaciones que generan inconformidad e impotencia.

La tecnología permanece en constante desarrollo y afronta problemas como el de la seguridad; así entonces, para el desarrollo del sistema que se presenta en este artículo se tomaron una placa Raspberry Pi, una cámara para ese dispositivo y un sensor PIR, elementos de costo reducidos y con altos beneficios al integrarse. Como se evidencia una dependencia frente a los tiempos de robo, se considera como estrategia generar notificaciones mediante el envío al correo electrónico del dueño del local comercial: con esto se dispondrá de una imagen de lo ocurrido en caso de que el sensor haya detectado movimiento en un periodo de 10 segundos; este se reinicia exista o no la detección, con el fin de que el dueño tome decisiones efectivas y el sistema continúe sus labores de monitoreo.

Planteamiento del problema

Aun cuando han surgido alternativas en materia de seguridad, aún no han sido suficientes teniendo en cuenta que los tiempos de robo son cada vez más cortos. Por ello, el presente proyecto está enfocado en dar un complemento de seguridad a los locales comerciales mediante el uso de tecnologías como la integración de la Raspberry Pi, un sensor de movimiento y una cámara que permitan reducir el riesgo de robo y tener toma de decisiones por parte de los dueños de los locales comerciales en caso de robo, generando así una nueva opción de seguridad.

Antecedentes

Rodarte, Gutiérrez y Pérez (2011) propusieron un sistema de seguridad de bajo costo con una red de sensores de movimiento PIR, enlazados por RF a un sistema de *hardware* libre Arduino, sirviendo este como interfaz. Aunque dicho proyecto versa sobre el robo en hogares, no se menciona en el mismo una forma de que el usuario conozca la vulnerabilidad de manera remota. En contraste, el proyecto que se explicita en este artículo utiliza un dispositivo más potente —la placa Raspberry Pi—, con la posibilidad de integrarle una cámara y procesar la captura de una imagen para ser enviada a través de correo electrónico; a nuestro juicio, esto resulta más práctico que la idea propuesta por los autores mencionados.

Zeki, Eldaw, Ibrahim, Haruna y Abdulkareem (2013) consideraron un sistema automático de control de seguridad interactivo, similar al propuesto en tanto captura una imagen del intruso; sin embargo, se enfoca en lugares de la vivienda, gestionado mediante un portal web. Frente a esta idea, el proyecto que se presenta aquí tiene como valor agregado el uso de un tiempo definido para dar como sospechosa a una persona que se encuentre dentro de la zona de detección, ya que está enfocado hacia los locales comerciales.

Sarthak, Vaibhav y Goyal (2014) exploraron en su artículo el uso de Raspberry Pi y envíos de mensajes de texto para domótica, generando control sobre la casa, en tanto al accionar un *switch,* se envía la alerta de uso de este a través de correo electrónico; pero no implementa algún sensor para darle cierta seguridad a este sistema. Adicionalmente, esta iniciativa pasa por alto el campo de los locales comerciales o negocios: utiliza un algoritmo realizado en el lenguaje de Python, aunque sí aborda el control de seguridad en las casas. El presente proyecto, a su turno, utiliza un sensor PIR que cubre un ángulo de 100 grados, de forma tal que no es necesario que el usuario esté en la ubicación para que funcione, motivo que lo hace apto para locales comerciales.

Amarilis, Rodríguez, Torres y Andrés (2014) construyeron una alarma de seguridad remota utilizando tecnología wifi, mediante la interconexión de minicomputadoras Raspberry Pi junto a un modelo cliente-servidor, donde el Raspberry Pi cliente transmitirá la señal usando un botón de pánico al servidor que cuenta con un indicador luminoso de encendido de alarma. A diferencia de dicha iniciativa, el presente proyecto hace uso de Ethernet para la capacidad de envío de las imágenes a través de correo electrónico; así, se hace posible ver lo que sucede en caso de que el sensor detecte una presencia sospechosa. Además, el sensor está en constante funcionamiento.

En su trabajo de grado, García (2014) describe un sistema de videovigilancia de bajo costo utilizando técnicas de procesamiento de imágenes para detectar posibles intrusos, de tal manera que hace posible seguir a una persona; además, hace uso de librerías de OPENC. Frente a este precedente, el presente proyecto tiene como valor agregado que no importa la cantidad de personas presentes sobre el sensor PIR, ya que si este detecta presencia comenzará a realizar un conteo de tiempo para capturar la imagen y enviarla a través de correo electrónico.

Wang (2011) propuso en su artículo una solución de control del sistema de seguridad usando el internet de las cosas, telecomunicaciones y otras tecnologías integradas, además de tener en cuenta otros aspectos como la humedad y el gas. La diferencia que marca el presente proyecto radica en que se centra en la seguridad de los locales comerciales en caso de intento de robo, sin tener que recurrir a tantos sensores; además, como se ha dicho, existe valor agregado en la captura y posterior envío de la imagen.

Behera et al. (2012) realizaron un sistema de vigilancia inteligente con un cierto número de cámaras para cubrir un área grande, permitiendo observar un número de videos de manera simultánea y seguir objetos en actividades sospechosas. En cambio, el presente proyecto es mucho más económico: solo es necesario usar una cámara y un sensor para dar seguridad a los exteriores de los locales comerciales y no es necesaria la presencia de los usuarios en la ubicación, debido a que envía capturas al correo electrónico.

Ikhankar, Ulabhaje, Dhadwe, Kuthe y Balpande (2015) crearon un robot junto a una Raspberry Pi para realizar un sistema de vigilancia en tiempo real, de esta manera utilizando la cámara para Raspberry Pi, tomando fotos en intervalos periódicos que se sobrescriben para que se vea como un flujo continuo de video. Frente a esta idea, el valor agregado de este proyecto está dado por no poseer dispositivos tan visibles como un robot y a la vez tan funcionales y prácticos, ya que el sensor tendrá un tiempo para dar como sospechoso a alguien y evitar falsas alarmas de robo.

Banerjee, Sethia, Mittal, Arora y Chauhan (2013) hablan de un sensor de movimiento seguro, mediante la introducción de una conexión por cable entre el Raspberry Pi y el sensor y utilizando una clave de cifrado enviado desde el teléfono móvil a través de Bluetooth. En comparación al trabajo mencionado, el presente proyecto utiliza el correo electrónico como mecanismo para observar que ocurre con una foto, dando un valor agregado el no tener que estar enviando confirmaciones y simplemente acceder para ver la captura en caso de que haya sospechoso y no estar revisando en todo momento lo que ocurre.

Abaya, Basa, Sy, Abad y Elmer (2014) en su estudio comentan acerca del sistema de vigilancia con capacidad de visión nocturna usando Raspberry Pi y OpenCV, diseñado para el interior de un almacén, siendo sus características la detección humana y de humo, mediante el software Open Source Computer Vision manejando el procesamiento de imágenes y una alarma. En discordancia, el presente proyecto tiene como valor agregado el uso de este en los exteriores de locales comerciales, de esta manera evitando que el ladrón ya se encuentre en el interior y enviando capturas de sospechosos a través de correo electrónico.

Takita et al. (2014) presentaron un sistema de cámaras para mejorar la seguridad en lugares públicos, basadas en un sistema llamado “Dairi”, el cual posibilita la unión de cámaras económicas mediante USB o LAN con el uso de una fuente de alimentación, al tiempo que proponen un concepto de privacidad. El valor agregado del presente proyecto frente a la idea mencionada es el uso del sensor PIR para la detección de sospechosos, así como el hecho de que no requiere monitorear constantemente la imagen proporcionada por las cámaras de seguridad.

Bar, Pande, Sandhu y Upadhyaya (2015) propusieron un método capaz de identificar la intrusión y enviar alertas a través de SMS: el objeto detectado es

seguido mediante una combinación de diferenciación de marco y el algoritmo de detección de características. En disparidad a la idea propuesta, el presente proyecto es menos complejo y más práctico, ya que solo la detección en la zona de detección hace posible enviar el mensaje adjuntando la imagen, y como valor agregado la persona tiene un tiempo muy corto para darla como sospechosa.

Menezes, Patchava y Gupta (2015) proporcionaron en su trabajo la detección de movimiento y sistema de seguimiento de la vigilancia, utilizando Raspberry Pi y SimpleCV para detectar objetos en movimiento en el área de vigilancia, sea en zonas residenciales, organizaciones gubernamentales, espacios comerciales, ambientes interiores y exteriores. Frente a la idea mencionada, el valor agregado del presente proyecto es el uso de un sensor PIR y un tiempo corto para dar como sospechoso a alguien y realizar la captura de la imagen para enviarla, evitando el tener que realizar un seguimiento constante.

Patchava et al. (2015) explican en su artículo el sistema Avanzado de Vigilancia de Raspberry Pi (ARS) bajo la misma idea de notificar al usuario cuando hay interferencia humana en el área de vigilancia; sin embargo, esta iniciativa usa la librería OpenCV analizando capturas de imagen para detectar movimiento. Aunque facilita la detección en la noche, no es posible que el usuario aprecie la imagen debido a que es enviada bajo el módulo GSM como un mensaje, característica que se tiene en cuenta en el presente sistema para evitar falsas alarmas a las autoridades.

Chandana, Jilani y Hussain (2015) generaron un sistema de monitoreo, el cual toma una imagen y la envía a correo electrónico utilizando el adaptador de Wi-Fi, enfatizando en los datos que brinda el sensor que son dados en tiempo real, contrario al presente sistema donde se destaca el periodo dado en el cual puede a ver movimiento para la posterior captura y toma de decisión por parte del usuario.

Vigneswari, Indhu, Narmatha, Sathinisha y Subashini (2015) propusieron un sistema de seguridad automatizado utilizando vigilancia, donde la persona una vez ingresa en el área a monitorear, los ventiladores y la luz se encienden y hace una captura de la imagen de la persona que ha ingresado, notificando al usuario con un mensaje, incluyendo el enlace para visualizar la imagen, por ello el presente sistema se decide utilizar el envío del correo con la imagen adjunta y eliminándola de la memoria SD, garantizando que no se sature la memoria y ocasione errores al guardar y enviar la imagen.

Sharma y Pavithra (2016), por su parte, mostraron un sistema de detección de movimiento que lo notifica mediante correo electrónico, y agregaron un servidor web en la Raspberry Pi para acceder remotamente al video en vivo desde un navegador. Así entonces, bajo este desarrollo el usuario debe saber cómo identificarse para ingresar a la plataforma, supervisar el monitoreo y observar al posible sospechoso. En contraste, el sistema que se presenta en este artículo

requiere ingresar al buzón de correo electrónico, considerando que se agrega un tiempo de diez segundos para notificar al usuario con la captura de la imagen.

Rani y Ramya (2016) proporcionaron un sistema más robusto aplicado a los cajeros automáticos: utilizan la misma dinámica de enviar capturas del sospechoso a través del GSM a la comisaria y banco correspondiente, los cuales toman decisiones para atrapar con mayor facilidad al sospechoso, y se procesan datos en tiempo real utilizando el sensor PIR. A diferencia de lo anterior, el sistema presentado aquí no contempla el envío de capturas continuas debido a que se tiene presente el tiempo de detección, aunque puede ser importante involucrar a futuro a las autoridades correspondientes.

Pingale, Khare y Thigale (2016) mostraron un sistema similar al del presente proyecto utilizando un sensor infrarrojo pasivo, una cámara y la placa Raspberry Pi, el cual permite detectar movimiento y obtener una imagen o notificación cuando ello sucede. Sin embargo, dicha iniciativa carece de estrategia alguna en materia de la detección, factor que sí se toma en cuenta en el presente sistema con periodos de diez segundos que son reiniciados cuando se envía notificación al correo electrónico, con el fin de minimizar tiempo y que la captura de la imagen sea útil para el usuario.

Propósito y fundamentación

El propósito de la investigación y su implementación es brindar a los dueños de los locales comerciales una alternativa de seguridad de bajo costo, eficaz en el tiempo de detección y de alerta al dueño, previniendo pérdidas económicas vitales para cualquier ciudadano por robo en su establecimiento.

Metodología

Para el desarrollo del proyecto se tuvo en cuenta la especificación del sistema: se utilizaron la Raspberry Pi 2 modelo B, la cámara CSI de 5 megapixeles con cable tipo *ribbon* y un sensor PIR HC-SR501. Se definió cómo se instalará el sistema operativo y se comunicará con el servidor de correo, con lo cual se compuso un diagrama de bloques para el uso del sistema:

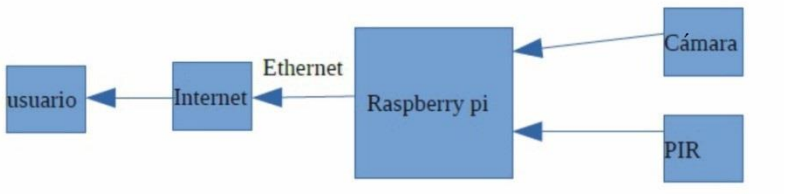

Figura 1. Diagrama de bloques del sistema. Fuente: elaboración propia.

En lo que atañe al *software*, la Raspberry Pi 2 modelo B soporta Linux; fue necesario instalar los controladores de la cámara y el sensor, así como el servidor SMTP, y crear una librería con Python para la captura y envío de la imagen con la cámara por correo electrónico.

En la implementación se realizó el montaje de los diferentes dispositivos y se crearon o probaron —en caso de venir instalados— los controladores para la lectura del sensor PIR y la cámara. Posteriormente, lo anterior se integró mediante una aplicación que "leería" el sensor y la cámara, capturaría la imagen y la enviaría por el servidor de correo electrónico. Finalmente, en la fase de puesta a punto se probó el sistema completo, verificando que se hubieren cumplido las pautas establecidas para el mismo al iniciarse el proyecto.

Especificación del sistema

La Raspberry Pi 2 modelo B utilizada para el proyecto dispone de las siguientes características: procesador de cuatro núcleos ARM Cortex-A7 CPU 900MHz, 1 GB de memoria RAM, 4 puertos USB, un puerto ethernet, interfaz para cámara (CSI), ranura para tarjetas micro SD, interfaz para *display* (DSI) y un puerto HDMI (figura 2).

Figura 2. Raspberry Pi modelo B. Fuente: elaboración propia.

La Raspberry Pi 2 soporta los sistemas operativos Raspbian, Arch Linux, Pidora y Minepeon. Para su instalación fue necesario descargar NOOBS —un instalador del sistema operativo para la Raspberry Pi— en otro equipo de cómputo, que posteriormente fue copiado a la tarjeta micro SD (previamente formateada); y luego se insertó la tarjeta en la ranura correspondiente de la la Raspberry Pi para completar el proceso. Además, se utilizó una cámara de 5 megapíxeles que soporta video en resolución 1080p (1920 x 1280 píxeles) a 30 cuadros por segundo, 720p (1280 x 720 píxeles) a 60 cuadros por segundo y VGA (640 x 480 píxeles) a 90 cuadros por segundo, conectada en el puerto CSI por medio de un cable de tipo *ribbon* (figura 3).

.

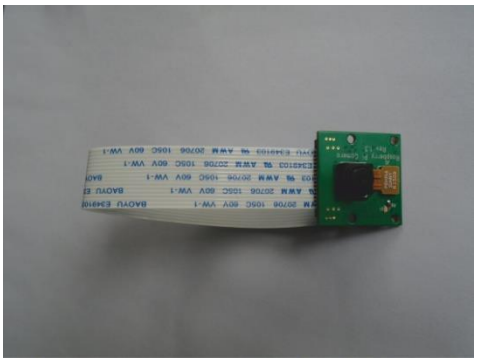

Figura 3. Cámara para Raspberry Pi. Fuente: elaboración propia.

A lo anterior se añadió el sensor PIR HC-SR501, el cual tiene un amplio rango de voltaje de alimentación 4,5 – 20VDC, tiempo de retardo de la señal de salida ajustable y un ángulo de 100° (figura 4).

Figura4. Sensor PIR HC-SR501.

Figura 4. Sensor PIR HC-SR501. Fuente: elaboración propia.

El sensor tiene dos modos de configuración. En el primero, el disparo no es repetido: el sensor se activa para el retardo de tiempo configurado y vuelve a su estado inicial, aun cuando la persona se encuentre frente al mismo. En el segundo, el disparo es repetido; el sensor se activa, pasa el retardo de tiempo configurado y, si la persona se mantiene, vuelve a activarse.

El área de detección comprende el espacio en forma semicircular enfrente del sensor, por lo que su ubicación debe coincidir con la zona de acceso que se quiere monitorear (figura 5).

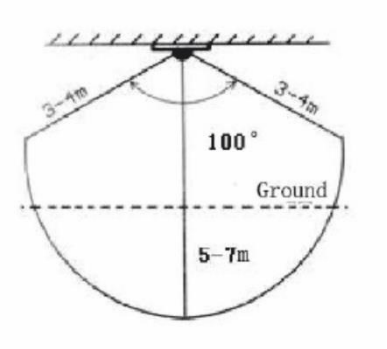

Figura 5. Área de detección. Fuente: Elecfreaks (2011).

De esta manera, cuando el sensor detecta una presencia, produce en su salida una señal alta de 3,3 VDC, por lo que no requiere circuitos de acondicionamiento de voltajes. Esto es, la conexión entre el sensor y la Raspberry Pi es directa.

Implementación del *hardware*

El sistema operativo utilizado en la Raspberry Pi para este proyecto fue una distribución de Linux basada en Debian, llamada Raspbian. Se optó por no emplear un entorno de escritorio para facilitar la labor de desarrollo de las aplicaciones de lectura y procesamiento de las señales recibidas por el sensor PIR y la cámara.

De modo específico, la instalación —que comenzó con la imagen de Linux en una tarjeta micro SD y el arranque del sistema en la Raspberry Pi— se realizó así: primero, se descargó una versión precompilada de la imagen (2016-02-26-raspian-jessie-lite.zip); luego, esta se descomprimió para obtener la imagen .img; después, se insertó la tarjeta micro SD en el computador y se abrió la consola de comandos; acto seguido, se digitó el comando $df –h para comprobar la partición de la tarjeta de memoria y se seleccionó la imagen, después de lo cual se verificó la instalación del sistema Raspbian (figura 6).

```
lithium@lithium:~/Descargas$ sudo dd bs=4M if=2016-02-26-raspbian-
jessie-lite.img of=/dev/sdb
[sudo] password for lithium:
324+1 registros leídos
324+1 registros escritos
1361051648 bytes (1,4 GB) copiados, 87,0635 s, 15,6 MB/s
lithium@lithium:~/Descargas$
```

Figura 6. Verificación de la instalación de Raspbian. Fuente: elaboración propia.

El control del sistema Raspbian se realizó desde un equipo de cómputo, utilizando un convertidor usb-serial y una aplicación llamada Screen; el convertidor para los voltajes 3,3 Vdc presentes en la Raspberry Pi 2 modelo B se conectó

disponiendo los cables TX, RX y *Ground* en los respectivos pines, como se ilustra en la figura 7.

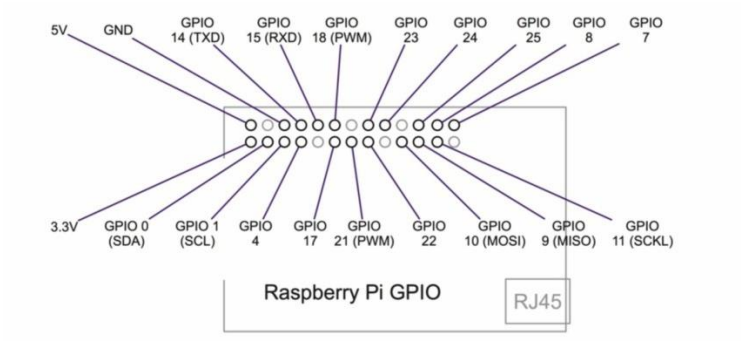

Figura 7. GPIO Raspberry Pi. Fuente: Ada Fruit (2015).

Después de lo anterior se encendió la Raspberry Pi y se conectó al *host*; posteriormente, se digitó el comando $sudo screen /dev/ttyUSB0 115200 en la terminal, por medio del cual inició el sistema y apareció la pantalla de identificación del mismo (usuario y contraseña por defecto: "pi" y "raspberry", respectivamente).


```
Raspbian GNU/Linux 8 raspberrypi ttyAMA0

raspberrypi login: pi
Password:
Last login: Fri Feb 26 01:30:13 UTC 2016 on ttyAMA0
Linux raspberrypi 4.1.18-v7+ #846 SMP Thu Feb 25 14:22:53 GMT 2016 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pi@raspberrypi:~$
```

Figura 8. Pantalla de identificación en la Raspberry Pi. Fuente: elaboración propia.

Las últimas versiones de Raspbian incluyen el controlador de la cámara, por lo cual no fue necesario instalarla; en lugar de ello, fue habilitada con el comando raspi-config como se observa en la figura 9.

Figura9. Habilitar Cámara Raspberry PI.

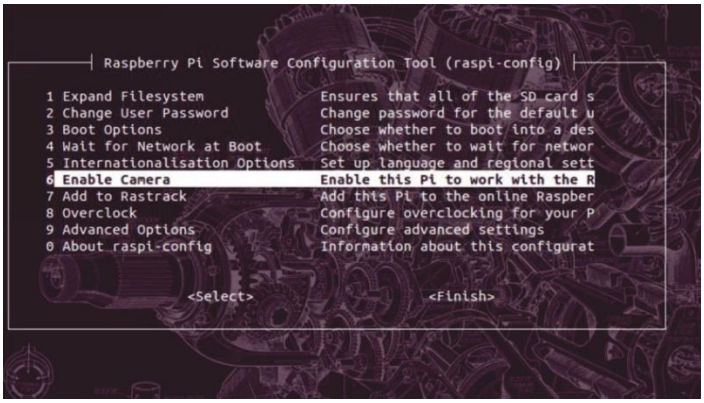

Figura 9. Habilitación de la cámara en la Raspberry Pi. Fuente: elaboración propia.

Implementación del *software*

Se utilizó Python como lenguaje de programación del algoritmo y se importaron las librerías *time* para manejo del tiempo, RPi.GPIO para controlar pines del Raspberry, smtplib para el uso del servidor email y Pi Camera para la operación de la cámara. Las figuras 10 y 11 muestran el código del algoritmo.


```
import smtplib
from email.MIMEMultipart import MIMEMultipart
from email.MIMEBase import MIMEBase
from email.MIMEText import MIMEText
from email import Encoders
import os
import RPi.GPIO as GPIO
import time
import picamera
import datetime
```

Figura 10. Librerías utilizadas en Python. Fuente: elaboración propia.

```
gmail_user = "RaspProyect@gmail.com"
gmail_pwd = "Rasp12berry"
Subject = "Intruso Detectado"
Message = "Se ha detectado un intruso, por favor ver imagen adjunta"
```

Figura 11. Parámetros del algoritmo. Fuente: elaboración propia.

Como se muestra en la figura 11, se inicializaron los parámetros del algoritmo para el correo electrónico Gmail, los cuales servirán para la posterior verificación: el usuario es "RaspProyect@gmail.com"; la contraseña, "Rasp12berry"; y el asunto, "Intruso detectado".

La salida del sensor PIR se conectó al GPIO4 de la Raspberry; además, se configuró *pull down* para asegurar el estado lógico bajo y que el sensor active la señal alta.

```
PIRSensor = 4
GPIO.setmode(GPIO.BCM)
GPIO.setup(PIRSensor, GPIO.IN, GPIO.PUD_DOWN)
```

Figura 12. Conexión del Sensor PIR en Python. Fuente: elaboración propia.

La figura 13 muestra las variables a tener en cuenta: el tiempo establecido de 10 segundos para activar el envío del mensaje; el tiempo que transcurre una vez hay detección; y los estados del sensor.

```
now = 0
Counter = 0
DetectTime = 10            #Tiempo de deteccion de 10 segundos
previous_state = False
current_state = False

#Inicializa y configura la camara
cam = picamera.PiCamera()
cam.vflip = True
```

Figura 13. Variables del Algoritmo en Python. Fuente: elaboración propia.

La figura 14 muestra la función get_file_name, la cual devuelve una cadena de texto con la fecha y hora del momento en que es llamada, y termina con la extensión .jpg. Esta cadena corresponde al nombre de la imagen y permite que este no se repita, a la vez que hace posible conocer el momento en que se capturó.

```
def get_file_name():
    return datetime.datetime.now().strftime("%Y-%m-%d_%H.%M.%S.jpg")
```

Figura 14. Función de Fecha para la imagen en Python. Fuente: elaboración propia.

La figura 15 muestra la función para el envío del mensaje de correo electrónico con la imagen adjunta. Para ello se utilizan extensiones multipropósito de correo de internet (MIME), las cuales son convenciones dirigidas al cambio a través de internet de un tipo de archivo; soportan texto, archivos adjuntos y cuerpo del mensaje.

```python
def mail(to, subject, text, attach):
   msg = MIMEMultipart()
   msg['From'] = gmail_user
   msg['To'] = to
   msg['Subject'] = subject
   msg.attach(MIMEText(text))
   part = MIMEBase('application', 'octet-stream')
   part.set_payload(open(attach, 'rb').read())
   Encoders.encode_base64(part)
      part.add_header('Content-Disposition',
            'attachment; filename="%s"' % os.path.basename(attach))
   msg.attach(part)
   mailServer = smtplib.SMTP("smtp.gmail.com", 587)
   mailServer.ehlo()
   mailServer.starttls()
   mailServer.ehlo()
   mailServer.login(gmail_user, gmail_pwd)
   mailServer.sendmail(gmail_user, to, msg.as_string())
   #mailServer.close()
   mailServer.quit()
```

Figura 15. Envío de Mensaje en Python. Fuente: elaboración propia.

Figura16. Main del Algoritmo en Python.

```python
while True:
    time.sleep(0.05)
    previous_state = current_state
    current_state = GPIO.input(PIRSensor)
    if current_state != previous_state:
      if current_state:
         Counter = Counter + 1
         print("Pulso detectado")
         print("Contador: %s" % (Counter))
         if Counter == 1:
            now = time.time()
    elif (time.time() > now + DetectTime):
      if Counter >= 3:
         print("Intruso Detectado")
         print("Tomando Imagen...")
         fileName = get_file_name()
         cam.capture(fileName)
         print("Enviando Imagen al correo....")
         mail(gmail_user, Subject, Message, fileName)
         print("Imagen enviada!")
         now = 0
         Counter = 0
         os.remove(fileName)
      else:
         now = 0
         Counter = 0
         print("Contador reiniciado")
```


Figura 16. *Main* del algoritmo en Python. Fuente: elaboración propia.

La figura anterior muestra un bucle infinito que estará en constante ejecución: cuando detecta un cambio en el estado del GPIO del sensor, aumenta el contador y toma el tiempo tras el primer pulso; una vez transcurren 10 segundos y hay más de tres detecciones, toma una fotografía del intruso y evoca la función de enviar la fotografía por correo electrónico; y finalmente elimina la fotografía de la memoria de la Raspberry Pi, y en caso de que pasados los 10 segundos haya menos de tres detecciones reinicia las variables y se ignoran las detecciones.

Para el arranque automático del algoritmo en Python Alarma.py se configuró un *script* para iniciarlo como un servicio de Linux al encender la Raspberry Pi 2 modelo B. Para ello, se digitó el comando sudo nano /lib/systemd/system/Alarma. Service; en el *script* se digitó execStart y la ruta del archivo de Python; después, se digitó el comando sudo systemdctl daemon enable Alarma.service, se reinició la Raspberry con el comando sudo reboot y se iniciaron las pruebas sin el uso de la terminal.

Para las pruebas se consideraron aspectos de distancia y grados del sensor respecto al sospechoso, y se incluyeron pruebas con y sin iluminación. Para lo mencionado se comprobó el funcionamiento del sistema conectando la fuente de energía con la Raspberry Pi 2 modelo B y el cable Ethernet: una vez se encendiera el led de la cámara se habría cargado todo el sistema y estaría listo para funcionar (figura 17).

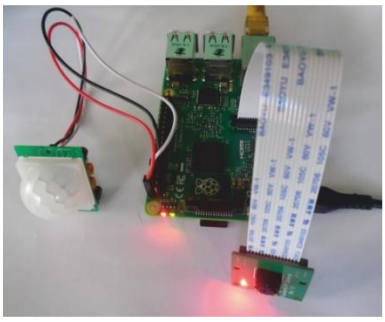

Figura 17. Sistema en funcionamiento. Fuente: elaboración propia.

Resultados

En la tabla 1 se muestran los diferentes valores dados para las pruebas en distancia, los grados del sensor respecto al sospechoso, la iluminación y la detección o ausencia de ella por parte del sistema, teniendo en cuenta el tiempo estipulado de diez segundos.

Tabla 1. Pruebas de detección

Distancia(cm)	Grados	Iluminación	Detección
20	0°	Sí	Sí
100	25°	Sí	Sí
100	25°	No	Sí
300	50°	Sí	No
300	15°	Sí	Sí
400	25°	Sí	Sí
450	15°	Sí	Sí
550	0°	No	Sí
600	0°	Sí	Sí
600	0°	Sí	No

Fuente: elaboración propia.

Lo anterior evidencia que si el intruso se encuentra al límite del área de detección (50°), o bien la distancia entre el sensor y el sospechoso es superior a seis metros, el sistema podría no detectarlo; mientras que, a pesar de no existir iluminación (la imagen capturada es totalmente oscura), la detección fue exitosa si la distancia entre el sensor y el intruso era inferior a 6 metros. La fecha y hora de captura de la imagen, el asunto, y el mensaje con la imagen del sospechoso se verificaron a través del correo electrónico, como se muestra en la figura 18.

Figura 18. Prueba del sistema y verificación por correo electrónico. Fuente: elaboración propia.

Discusión

A diferencia de lo expuesto en relación con el proyecto que se ha presentado aquí, algunos desarrollos paralelos en esta materia requieren que un personal monitoree la imagen de las cámaras (p. ej. en el trabajo de Behera et al. [2012] se implementa un sistema multicámara), mientras que otros involucran costos elevados para lograr los resultados esperados.

Mientras que en el trabajo de F. Abaya et al. (2014) la precisión para la detección fue 83,56 %, en este proyecto fue del 90 %; teniendo en cuenta que las pruebas fuera del área de detección no están incluidas, la exactitud osciló entre 50 y 100 %. En el presente proyecto, la exactitud asciende al 90 % bajo los parámetros mencionados en las pruebas. Además, el sistema de seguridad propuesto permite que no se sature la memoria con fotos, por cuanto estas se eliminan una vez enviadas al correo electrónico (estos aspectos no son mencionados en los trabajos relacionados en los trabajos tomados como antecedentes). Sin embargo, en caso de un corte de energía, la implementación de una batería adicional, así como la incorporación de una antena inalámbrica a la Raspberry Pi que evite el uso del cable Ethernet para la conexión a internet y para el envío de las detecciones por correo electrónico, serían complementos que responderían a situaciones de posible ocurrencia en la vida real.

Respecto a la imagen, la claridad en la captura en la noche sin iluminación del presente proyecto frente a los resultados de Menezes et al. (2015) es 0 % y 80 %,

respectivamente, sin tener en cuenta que el autor tiene la posibilidad de encender la luz una vez hay detección por parte del sistema utilizado. Por ello, el sistema realizado requiere de cierta iluminación para que al capturar la imagen el usuario pueda verla sin problemas; por tanto, añadir visión nocturna al proyecto eliminaría la dependencia de la iluminación (como puede ser el uso del *software* Open CV).

Los grados generados respecto del sensor al sospechoso variaron en el presente proyecto desde 0° hasta los 50° —límite del sensor—; mientras que Behera et al. (2012) muestran que el uso de ecuaciones para medir distancias entre objetos y personas permite que el área de detección corresponda a una zona específica, de tal manera que no se presenten errores (siempre y cuando las cámaras se ubiquen sobre el lugar a vigilar adecuadamente).

Se decidió establecer un tiempo de 10 segundos por cuanto los ladrones utilizan herramientas cada vez mejores para disminuir el ruido y el tiempo que toma el hurto (según lo consultado en *El Espectador* [2016], en la ciudad de Bogotá se realizan hurtos con llaves maestras y se arriba al lugar del delito en vehículos, con lo cual e reduce el tiempo); así entonces, el sistema propuesto podría generar con rapidez las notificaciones tanto al propietario de local comercial como a las autoridades respectivas (la información del local objeto del hurto, incluida su ubicación, podría adjuntarse al mensaje y a la imagen enviados por el sistema).

Conclusiones

El sistema de seguridad implementado es de bajo costo y accesible para los propietarios de los locales comerciales (solo deben contar con una dirección de correo electrónico), lo cual minimiza la dependencia del monitoreo y facilita su uso.

Las pruebas realizadas arrojaron un 90 % de éxito bajo los parámetros de distancia, grados respecto al sospechoso, iluminación y detección por parte del sistema. Aunque no se requiere iluminación para detectar al sospechoso, sí es necesaria para capturar la imagen. Entre los aspectos a tener en cuenta se encuentra la ubicación del sensor sobre la zona a monitorear: considerando que los valores de las pruebas variaron de 0° a 50° y los límites pueden ocasionar fallas en la detección, lo ideal sería ubicar el sensor en el centro de la zona, en tanto cubriría 100°. Las falsas alarmas, por su parte, pueden ocurrir con la presencia de un animal; empero, el hecho de que esto sea verificable mediante el correo electrónico agrega utilidad al sistema, a la vez que el tiempo de reacción de 10 segundos hace posible que se detecte a sospechosos potenciales y que el sistema cumpla con su función de monitoreo de forma constante.

A futuro, y como se mencionó anteriormente, el sistema puede complementarse con la adición de visión nocturna, en tanto eliminaría la dependencia de la iluminación para la captura de imágenes; y aún más, en el envío del correo

electrónico podrían describirse en detalle los datos del local comercial y su ubicación, con el fin de notificar a las autoridades.

Referencias

Abaya, W. F., Basa, J., Sy, M., Abad, A. C., & Dadios, E. P. (2014). Low cost smart security camera with night vision capability using Raspberry Pi and OpenCV. En *2014 International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)* (pp. 1–6). https://doi.org/10.1109/HNICEM.2014.7016253

Amarilis, E., Rodríguez, S., Torres, B. & Andrés, J. (2014). Activación de Alarmas Remotas mediante WIFI entre minicomputadoras Raspberry Pi [tesis de grado]. Guayaquil, Ecuador: Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica de Litoral.

Banerjee, S., Sethia, D., Mittal, T., Arora, U., & Chauhan, A. (2013). Secure Sensor Node with Raspberry Pi, Department of Electrical Engineering. *IEEE,* 26-30.

Bar, D., Pande, D., Sandhu, M. S., & Upadhyaya, V. (2015). Real-time security solution for automatic detection and tracking of intrusion. En *2015 Third International Conference on Image Information Processing (ICIIP)* (pp. 399–402). https://doi.org/10.1109/ICIIP.2015.7414804

Behera, K., Kharade, P., Yerva, S., Dhane, P., Jain, A. & Kutty, K. (2012). Multi-Camera Based Surveillance System. *IEEE,* 102-108.

Chandana, R., Jilani, K. & H Javeed. (2015). "Smart Surveillance System using Thing Speak and Raspberry Pi". *International Journal of Advanced Research in Computer and Communication Engineering, IJARCCE*, 214-218.

El Espectador (2016). Con llaves maestras hurtan cinco apartamentos en el sur de Bogotá. (2016). Recuperado de http://www.elespectador.com/noticias/bogota/llaves-maestras-hurtan-cinco-apartamentos-el-sur-de-bog-articulo-632097.

El Espectador. (2015). Aumentaron los índices de inseguridad en Bogotá. Recuperado de http://www.elespectador.com/noticias/bogota/aumentaron-los-indices-de-inseguridad-bogota-articulo-478939.

Ikhankar, R., Ulabhaje, S., Dhadwe, M., Kuthe, V. & Balpande, S. (2015). Pibot: The Raspberry Pi Controlled Multi-Environment Robot for Surveillance & Live Streaming. *IEEE,* 1402-1405.

Menezes, V., Patchava, V., & Gupta, M. S. D. (2015). Surveillance and monitoring system using Raspberry Pi and SimpleCV. En *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1276–1278). https://doi.org/10.1109/ICGCIoT.2015.7380661

Patchava, V., Shaik, H., Neelavarapu, R., Rao, M., Rohan, G. & Durga, B. (2015). Advanced Raspberry Pi Surveillance (ARS) System. *Proceedings of 2015 Global Conference on Communication Technologies, IEEE,* 860-862.

Pingale, S., Khare, G. & Thingale, S. (2016). Interactive motion detection security system using Raspberry Pi in IOT. *International Journal of Research in Computer Science and Information Technology (IJRCSIT)*, 137-139.

Rani, G. & Ramya, V. (2016). Efficient Camera Based Monitoring and Security System using Raspberry Pi, *International Journal of Innovative Technologies (IJIT),* 3677-3680.

Rodarte, J., Gutiérrez, J. & Pérez, R. (2011). Red de Detectores Pasivos Infrarrojos enlazado y por radiofrecuencia, como sistema de alarma de seguridad de bajo costo. *Revista Colombiana de tecnologías de Avanzada*, *2*(18), 42-45.

Sharma, G. & Pavithra (2016). An Efficient Security Alarm System Using Raspberry Pi and Internet of Things. *A National Level Conference and Technical Fest, (ISRASE).*

Takita, A., Ohta, N., Fujii, Y., Ueda, H., Yoshiura, N. & Maru, K. (2014). Security camera system for privacy protection and community safety. *IEEE.*

Vigneswari, P., Indhu, V., Narmatha, R., Sathinisha, A. & Subashini, M. (2015). Smart Surveillance System using Thing Speak and Raspberry Pi. *International Journal of Current Engineering and Technology, (IJCET),* 882-884.

Wang, Z. (2011). Design and Realization of Computer Network Security Perception Control. *IEEE,* 163-166.

Zeki, M., Eldaw, E., Ibrahim, A., Haruna, C. & Abdulkareem, S. (2013). Automatic Interactive Security Monitoring System*. ICRIIS'13*, 215-220.