Journal of Computer Science

Original Research Paper

An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients

Nico Surantha and Wingky R. Wicaksono

Department of Computer Science, BINUS Graduate Program – Master of Computer Science,
Bina Nusantara University, Jl. Kebon Jeruk Raya No 27, Jakarta 11480, Indonesia

Article history
Received: 13-02-2019
Revised: 25-05-2019
Accepted: 06-08-2019

Corresponding Author:
Nico Surantha
Department of Computer Science, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jl. Kebon Jeruk Raya No 27, Jakarta 11480, Indonesia
Email: nico.surantha@binus.ac.id

Abstract: This research aims to design and implement a home security system with human detection capability. Traditional home security systems, i.e., Closed-Circuit Television (CCTV) can only capture and record videos without the ability of giving warning feedback if there is any suspicious object. Therefore, an additional object detection and warning method is required. The proposed design is implemented using Raspberry Pi 3 and Arduino, that is connected by USB cable. The PIR sensor is installed on Arduino and webcam is mounted on Raspberry Pi 3. The Raspberry Pi 3 is used to process inputs from sensors and process images for human detection. PIR sensor detects the movement around the sensor to activate the webcam to capture a picture. Then, the object recognition is performed using Histogram of Oriented Gradients (HOG) and Support Vector Machine (SVM) to detect the suspicious object. If the suspicious object is detected, then the alarm is activated and sends an email to warn the house owner about the existence of the intruder. The results show that it takes on average 2 seconds for the proposed system to detect an intruder and that the system can successfully detect the intruder with accuracy of 90%.

Keywords: Smart Home, Histogram of Oriented Gradients, PIR Sensor, Internet of Things, Raspberry Pi

Introduction

House is a residential building, an asset, as well as a place to store wealth. Therefore, security becomes one of mandatory considerations in keeping the house from undesirable events or accidents (Eseosa and Promise, 2014). The traditional solution for house security is a Closed-Circuit Television (CCTV). CCTV is a device for monitoring the situation around an office area, house and building. CCTV is also useful for monitoring the situation around a house, both when the residents are at home and when they are not at home (Bangali and Shaligram, 2013). Despite the benefits, there are some problems related to the use of CCTV. Firstly, CCTV does not produce any notification and warning whenever it captures any suspicious object. Secondly, CCTV streams continuously to capture events that occur in the home environment even when there is no suspicious object or activity. Therefore, the streaming requires huge consumption of bandwidth and storage media due to the continuous video streaming and storing.

Internet of Things (IoT) is a network of interconnected electronic devices capable of sending data without interference or with minimal human intervention. This technology has been widely used for smart city application, personal health monitoring, manufacturing and smart lighting. Some researchers have developed security monitoring system based on IoT concept (Charadva *et al*., 2014; Chitnis *et al*., 2016). They utilize the capability of sensors, e.g., Passive Infrared (PIR) motion sensor, door open sensor, glass break detector to monitor the occurrence of any suspicious activity. The system is also equipped with feedback mechanism which warns the house owner if there is any intruder entering the house. In general, this technology offers better protection compared to the traditional CCTV.

In this paper, an IoT system for monitoring the presence of intruders in a house using the combination of motion detection and object recognition is proposed. The motion detection is performed using PIR sensor (Ansari *et al*., 2015; Chuimurkar and Bagdi, 2016; Raja *et al*., 2017) After the motion of object is detected, the web camera takes the picture of the suspicious spot. The system then performs object recognition by using Histogram of Oriented Gradient

Science Publications

(HOG) (Dalal and Triggs, 2005) and Supports Vector Machine (SVM) methods. Finally, the system is expected to recognize the appearance of an intruder and warn the house owner via alarm and send an email notification. The system is implemented on Raspberry Pi 3 and Arduino. The evaluation of the system includes the measurement of accuracy and delay of intruder recognition. The system is expected to recognize the intruder accurately in the shortest time. This paper is an extended version of our previous published conference proceeding (Surantha and Wicaksono, 2018). In this paper, the literature review and the explanation of HoG in detecting objects are extended. More experiments are also conducted to evaluate the performance of the system.

This paper is divided into five sections. Section II discusses previous works that have been done by researchers in this field. Section III describes the system design approach. Section IV presents performance evaluation results and discussion. Finally, section V outlines the conclusions of this research.

Related Work

There have been some previous studies on home security system. Tanwar *et al.* (2017) conducted a study entitled "An Advanced Internet of Thing based Security Alert System for Smart Home". It describes inexpensive home security systems using Infrared (PIR) and Raspberry Pi modules to minimize delays during e-mail alerts. Therefore, there are PIR sensors as motion detector and Raspberry Pi as its processing module.

Another research was conducted by Bangali and Shaligram (2013) entitled "Design and Implementation of Security Systems for Smart Home based on GSM technology". It proposed two methods for home security systems that are implemented into one application. The first system used a web camera used for capturing motion and objects, producing warning sounds and sending feedbacks to the user. The second method sent SMS using GSM-GPS Module (sim548c) and Atmega644p microcontroller, sensor, relay and buzzer.

The third study was conducted by Chuimurkar and Bagdi (2016) entitled "Smart Surveillance Security and Monitoring System Using Raspberry PI and PIR Sensor". It focused on the design and implementation of monitoring systems using Raspberry PI and PIR Sensors for mobile device. The system has the ability to detect smoke and human movement, providing precautions against potential crime and potential fire. The hardware used was Raspberry Pi (RPI) with OpenCV for handling image processing, alarm control and send captured photos to user email via WiFi8 Alarm system for the initial sign, the system will play the sound recording: "Intruder" or "smoke detected" when there is detection.

Al-qaness *et al.* (2016) conducted a study entitled "Device-Free Home Intruder Detection and Alarm System Using Wi-Fi Channel State Information". This study discusses the design of an intruder detection system and an alarm system using WiGarde by utilizing information from the Channel State (CSI) to detect intruders through a door or window. WiGarde extracts CSI amplitude information across MIMO antennas. This system is very good because it can avoid the occurrence of false alarms as it uses the bad stream elimination algorithm. Support Vector Machine (SVM) is used to classify human intrusion. The results of this study were compared to CSI-based intruder detection and RSSI-based intruder detection and good results were obtained.

The fifth study was conducted by Patidar *et al.* (2014) with the title "Real Time Vision Based Security System". This study discusses cheap security devices on the implementation side for detection of changes in the monitoring area. The tools used in this study are installed with linux and OpenCV. These tools were employed for image processing, GPU and GUI libraries. A webcam was used for area monitoring. The webcam is placed 2.5 m above the ground with a 30°C camera angle. Therefore, the webcam can get an effective distance of about 4 m. The study uses a change detection technique in the monitoring area with image acquisition stages, image segmentation and pre-processing image. If there are differences in the monitoring area, the calculation is done. The test was carried out by activating the system for 1 h 23 min and a detection rate of 86.11% was obtained. During this time, 72 movements were detected and 10 of them were 10 undetected movements. Overall, a detection rate above 86% at 5-6 frames/sec was obtained.

The sixth study was conducted by Parab and Amol Joglekar (2015) under the title "Implementation of Home Security System using GSM module and Microcontroller". This research discusses the design and implementation of a home security system using a GSM modem, where the power used was very low. In addition to using a GSM modem, magnets were also used with relays on doors and LEDs. So, when the door is opened, the yellow LED will turn to red. Then, the system will send an SMS to the owner.

From the literature review, there have been few researchers who focus on the IoT, home security system and motion detection. However, there has been no researcher specifically discussing IoT technology for home security with an additional ability to recognize intruders. In addition, there are several studies which did not present the results of accuracy obtained by the system. Therefore, in this research, the design is proposed to maximize the existing system and provide better feedback to users.

System Design Approach

Based on the problems faced, an IoT system with an additional capability of detecting and recognizing intruders using HOG and SVM methods is proposed (Dalal and Triggs, 2005; Satpathy *et al*., 2014). The system is implemented on Raspberry Pi 3 (Kumar and Reddy, 2016) and Arduino (Abdullah *et al*., 2016; Badamasi, 2014). The Raspberry Pi 3 is used because this board can process image processing with low power from computer and laptop. Arduino is used to integrate all the electronic devices in one environment. To detect the motion, the PIR sensor is utilized (Sahoo and Pati, 2017). In this section, the system design approach for the proposed home security system is discussed.

General System Design

In designing a system, the first step is to develop the architecture of the system. Firstly, the scenario of possible intruder entry and how the warning informs need to be considered. The possible intruder scenario can be seen in the “Arrival of Intruder” section in Fig. 1. In this research, we assume the intruder to enter the house from the front door. As the intruders arrive/enter, the PIR Sensor located near the front door detects the motion of the intruders. The PIR sensor reads every movement that passes through the detection range of the PIR sensor, i.e., approximately 4-7 m. In the process of motion detection, the system will read continuously until a movement is found.

If there is a movement, then the system will activate the camera. The generated images are then stored in the system directory. After the photo capture and storage process, the system will activate the function for human detection. In human detection, we use the HOG and SVM methods. Features of the photo are extracted using HOG and then a classification of features is performed by using SVM. SVM matches the features of the photos with features in the dataset. If human presence is detected in the photo, then the system will activate the buzzer as an alarm and send an email notification. If the-re is no human presence detected in the picture, then the system will re-read the movement or return to the initial process. The complete system workflow is shown in Fig. 2.

Hardware Design

This section outlines the hardware design. The hardware design includes the selection of electronics equipment and the integration of all of components. Figure 3 shows the hardware design for our security monitoring system. Meanwhile, the specifications of every component are presented in Table 1. The number in Fig. 3 corresponds to the order of component in Table 1. For processing module, we use Raspberry Pi 3 model B. This board is equipped with wireless LAN module for communication. Arduino is used to collect the signal from PIR sensor through jumper cable. Arduino is connected to Raspberry Pi via USB cable. To capture the picture, USB webcam is mounted to the Raspberry Pi 3 via USB cable. To release warning, buzzer module is connected to Raspberry Pi 3 through GPIO port. The Raspberry Pi 3 is also connected to the internet so that the system has the ability to send an email notification.

Table 1: Hardware specification

No	Name	Description
1	PIR Sensor	PIR Sensor for movement detection
2	Arduino	Arduino Uno
3	Camera	Using webcam camera USB 2.0 (Logitech c525) for take picture
4	Raspberry Pi 3	Using Raspberry Pi 3 Model B, ARM Cortex-A53 1.2 GHz, 1 GB RAM, 802.11n wireless LAN. In this Raspberry Pi 3 image processing has been installed (OpenCV)
5	Buzzer	Passive buzzer for alarm

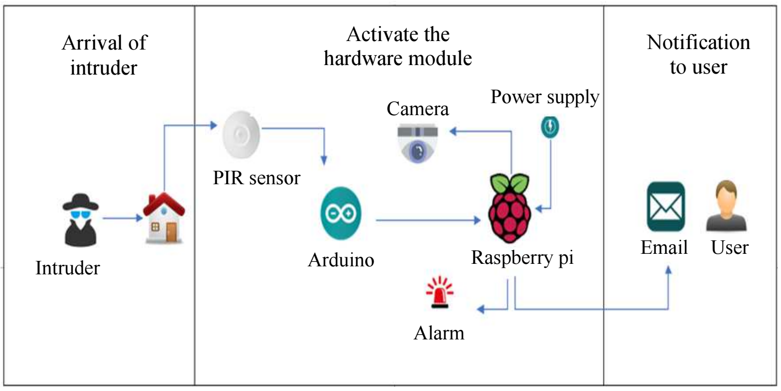


Fig. 1: Proposed system architecture

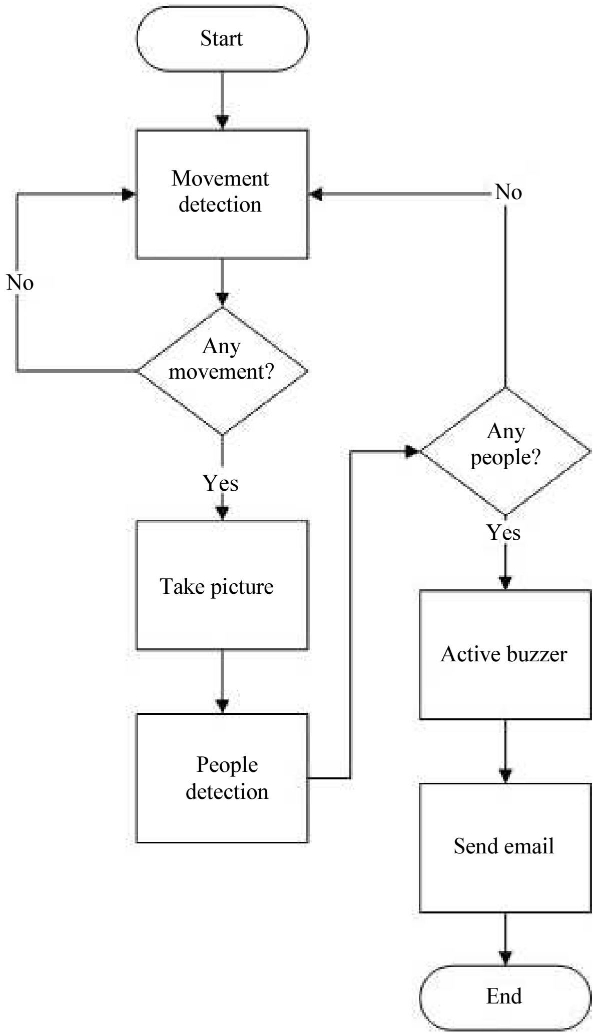


Fig. 2: System workflow

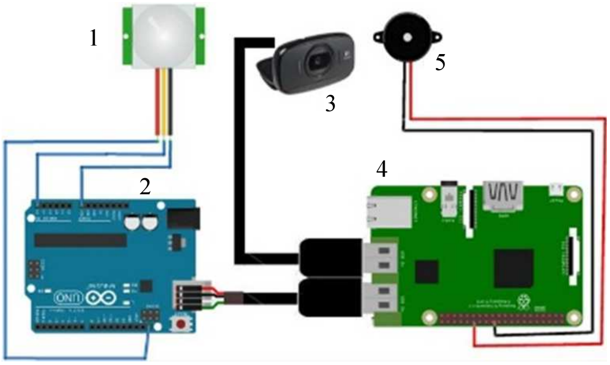


Fig. 3: Hardware architecture

Software Design

After the hardware design, software was then designed. Firstly, we create a use case diagram as shown in Fig. 4. The user starts activating the system in Rasp-berry Pi 3.

Algorithm : Motion Detection in Arduino

```
Declare :
Pin, pirState, val := 0,
Algorithm :
While val <> 1 do
If pin := HIGH
    If pirState := LOW
        val := 1
        pirState := HIGH
    Else
        IF pirState := HIGH
            val := 0
            pirState := LOW
End While
```

Listing *1*. Pseudo Code of Software in Arduino

Movement detection is handled by PIR Sensor and Arduino sends the true or false value to Raspberry Pi 3. Photo captured is triggered after Arduino sends the data. Raspberry Pi 3 controls the camera. Figure 5 shows the software architecture. This diagram shows the position or location of each application function on the hardware that will be installed and arranged from the application. HOG and SVM are also installed in Raspberry Pi 3. HOG is used to extract the features of human objects in the image. In the first step, the HOG method will convert RGB image (red, green, blue) to grayscale image. Then, gamma normalization will be done to calculate the result of the square root of each channel (red, green and blue channel). Then, the gradient value of each pixel will be calculated by dividing it into 8×8 cells. The next process is to determine the number of orientation bin that will be used in the histogram (spatial orientation binning). After that, the normalization process of block 16×16 is done to cells to overcome the lighting changes. In this process there are blocks that overlap due to their shifting cells. The final process is to calculate the HOG feature vector. The resulted HOG feature will be processed using the SVM method to determine whether the feature is a human feature or not. The full process of human detection can be seen in the Fig. 6.

System Setup

1. PIR Sensor on Arduino

Programming for motion detection using PIR sensor is performed on Arduino IDE application. The source code is then embedded into Arduino by connecting the Arduino with a computer using a USB cable and the programs are downloaded to Arduino.

2. Raspberry Pi 3

a. Raspbian Stretching. OpenCV and Python

The operating system used for Raspberry Pi 3 is Raspbian Stretch. This operating system can be downloaded on the official Raspberry site. This operating system operates on 32GB MicroSD. The type of MicroSD used is MicroSD Class 10 which is commonly used on Android smartphones. After Raspbian Strech is installed, the applications required on Raspberry Pi 3 are OpenCV and Python to run HOG and SVM. For the computer vision library, opencv 3.3.0, opencv_contrib and Python 3.0 is used in this research.

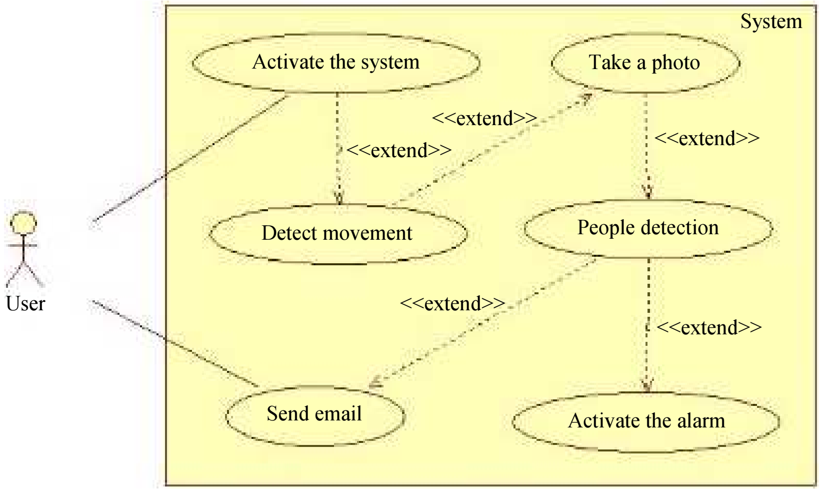


Fig. 4: Use case diagram

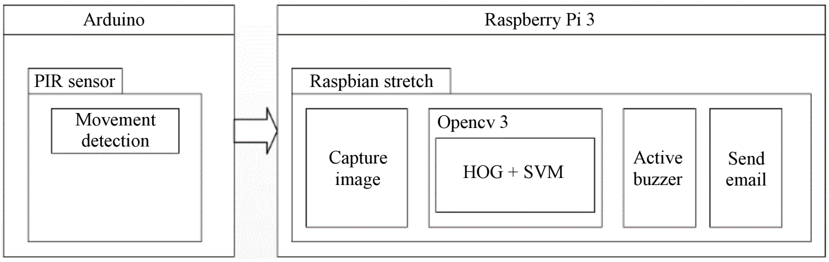


Fig. 5: Software architecture

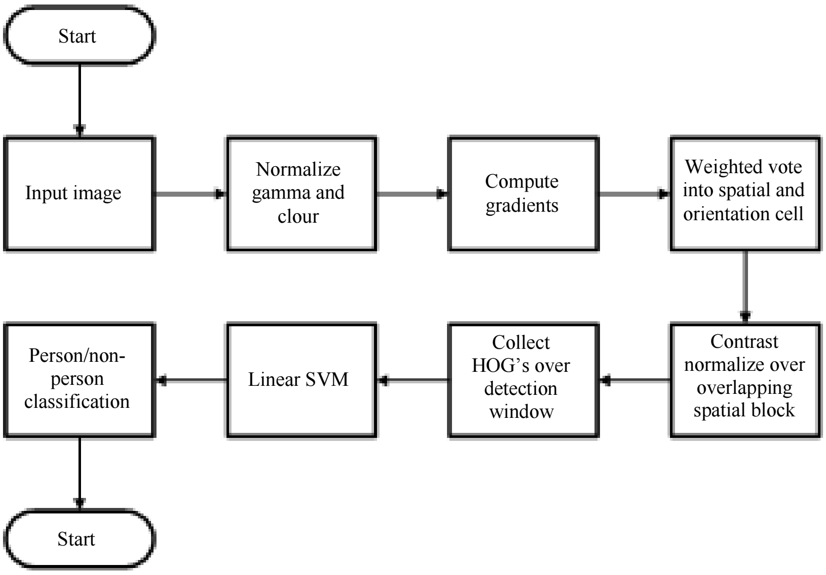

Start
Input image
Normalize gamma and clour
Compute gradients
Weighted vote into spatial and orientation cell
Contrast normalize over overlapping spatial block
Collect HOG's over detection window
Linear SVM
Person/non-person classification
Start

Fig. 6: Human detection process

b. Camera

The webcam camera function uses the fswebcam library. Then the .sh file is created with a program script. The resulting photo is 640×480 pixels and the FPS parameter 15. The purpose of the low-resolution setting is to perform the photo process quickly, i.e., less than 1 sec.

c. Alarm

The Alarm function on the Raspberry Pi 3 already supports the gpiozero pin interface. Therefore, the alarm can be used immediately.

d. E-mail

To send an email using SMTP, some configurations are conducted. In this study, two emails with the Gmail domain is utilized. The first e-mail address is rpiserverxxx@gmail.com, used as server initialization (from e-mail sender, from) and second e-mail address rpiserveryyy@gmail.com, used as the recipient. Then, the email as the sender and recipient's email are configured. The configuration is performed on the sender and recipient's gmail account in order to allow the less secure applications, therefore email can be sent automatically without any problem.

```
root=your_account@gmail.com
mailhub=smtp.gmail.com:587
FromLineOverride=YES
AuthUser=your_account@gmail.com
AuthPass=your_password
UseSTARTTLS=YES
UseTLS=YES
# Debug=Yes
```

Listing 3. Configuration in ssmpt.conf file.

Then the next step is to configure the /etc/smtp/ssmtp.conf file on the Raspberry Pi 3. Listing 3 shows the configuration in ssmtp.conf file.

e. Network

For networks, WiFi is used as media for internet connection. Static IP is used for IP configuration. These settings aim to facilitate connection and remote access to Raspberry Pi 3.

3. Training Dataset

Dataset training is not performed on the system. In this study using a dataset provided by OpenCV. The function is HOGDescriptor_getDefaultPeopleDetector().

Intruder Detection Using HoG

In this section, the intruder detection process using HoG is explained. From the results of the experiments that have been carried out according to the scenario, one photo was obtained. The photo is stored by the system in the temporary folder, namely directory /home/pi/Home Security/images. The photo can be seen in Fig. 7.

Then the extracted photo using HOG, with the first step is color normalization. At this stage, the original color photo is transformed into a grayscale one. The trick is to take all the pixels in the image then from the color of each pixel, information about the 3 basic colors, namely red, blue and green, is obtained. These three basic colors will be added, then divided by three so that the average values are added. This average value will be used to give color to the pixels of the image so that the color becomes grayscale. The three basic colors of a pixel will be set to the average value (via RGB function). The grayscale value can be obtained with the following equations:

$$f(x,y)=\frac{f_i^R(x,y)+f_i^G(x,y)+f_i^B(x,y)}{3}, \tag{1}$$

The photos that have been processed into grayscale can be seen in Fig. 8. After being converted to grayscale, then normalization is made from the grayscale photo. The results of photo normalization can be seen in Fig. 9.

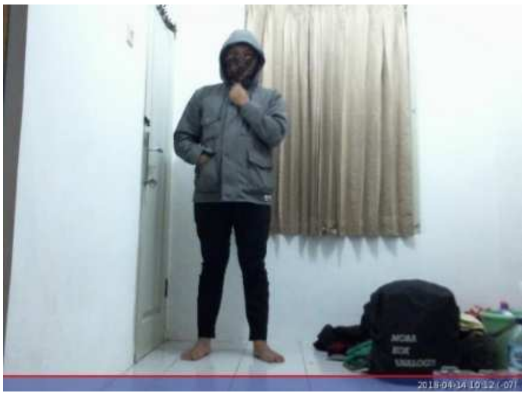


Fig. 7: Sample photo

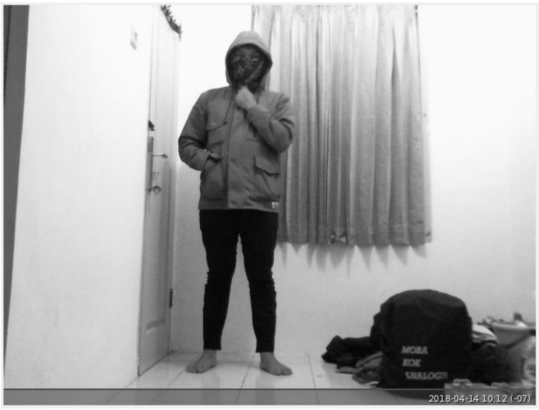


Fig. 8: Grayscale picture

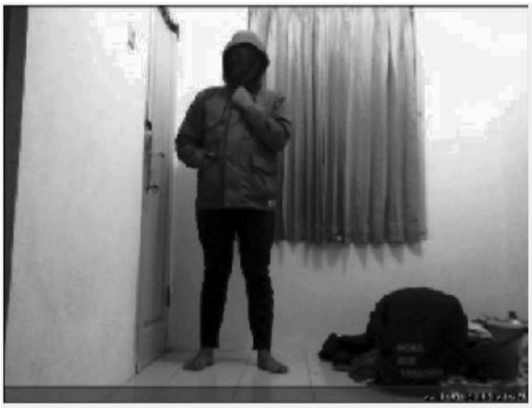


Fig. 9: Picture after being normalized

The next process is to calculate the gradient value. Gradient is the result of measuring changes in an intensity function and an image can be seen as a collection of several continuous intensity functions of the image. This process is used to obtain edges of objects in the image. The gradient of an image can be obtained by filtering with a 2-dimensional filter comprising vertical and horizontal filters. The commonly used method is 1-D centered with a matrix of $[-1, 0, 1]$.

Partial derivative formula for image functions (x, y):

1. $x-axis:\frac{\partial\rho}{\partial x}=\frac{f(x+h)-f(x-h)}{2h}$ (2)

2. $y-axis:\frac{\partial\rho}{\partial y}=\frac{f(y+h)-f(y-h)}{2h}$ (3)

The values of x and y are used to calculate the gradient:

1. Gradient Magnitude: $g=\sqrt{g^2x+g^2y}$ (4)

2. Gradient Direction: $\theta=arctan\frac{g_y}{g_x}$ (5)

The photos from the gradient calculation can be seen in Fig. 10. When the gradient computation process obtains different gradient values, it is necessary to group each cell into a larger group called block. After grouping into blocks, this block usually overlaps. In normalization, this block uses R-HOG square block geometry. This process is the final process of the HOG method that produces features. This process is carried out when the windows detector process is like in the process of calculating bin orientation. Windows detector size used is 64×128 which consists of 8×8 pixels. Calculating block normalization takes cell groups and normalizes the overall contrast response. This is done by accumulating the size of histogram from the cell group called block. The result is used to normalize each cell in a block, the following is a calculation of the histogram in the block:

1. L1 - $norm: v\rightarrow v/\left(\|v\|1+\varepsilon\right)$, (6)

2. L1 - $sqrt: \mathrm{v}\rightarrow\sqrt{\mathrm{v}/\left(\|v\|1+\varepsilon\right)}$, (7)

   that is the number to treat vector descriptor as an opportunity distribution.

3. L2 - $norm: \mathrm{v}\rightarrow\sqrt{\left(\|v\|\frac{2}{2}+\varepsilon^2\right)}$, (8)

4. L2 - Hys, L2 – *norm* followed by clipping and renormalization where is an un normalized vector

In this process, descriptors from all blocks are collected, which are R-HOG. The R-HOG is an overlapping grid used in classifiers. The R-HOG descriptor block uses square grid-shaped cells. R-HOG calculates the grid (which defines the number of cells in each block) of cell pixels which each contain bin. The description of the HOG of the image is visualized using a 9×1 normalization histogram at 8×8. In Fig. 11 it is seen that the dominant direction of the person's histogram is shaped, especially around the body and legs.

To check whether there are people or not in the window, SVM Classifier is used to separate classes of people and non-people or in this study, it is the detection of people in the SVM Classifier and classification algorithms that try to separate a hyperplan. Classification problems can be translated by finding a line (hyperlane) that separates the two classes. Feature HOG that has been processed is used as input from SVM learning. Feature HOG is changed to feature vector with size 4608×1. Feature vector size is generated from multiplication of block size (2×2 cells), number of bins 9 and number of blocks formed from photos. This feature vector is used as input for the SVM learning process. If the results in the SVM process can produce true values (there are people detected), the system will create a box (green box) that shows the position of the person in the image as shown by Fig. 12.

The system will then store the value of bounding boxes or true values in the previous process to the variable x1. The value of x1 will then be used as a filter where if the value of x1> = 1 then it means that the system detects people. If not, there are no people in the photo.

Then, the notification is sent to the email that has been configured. The screenshot of the email notification can be seen in Fig. 13. From this scenario, it produces a system log that shows the process of the application to process each of its functionalities. The system log can be seen in Fig. 14.

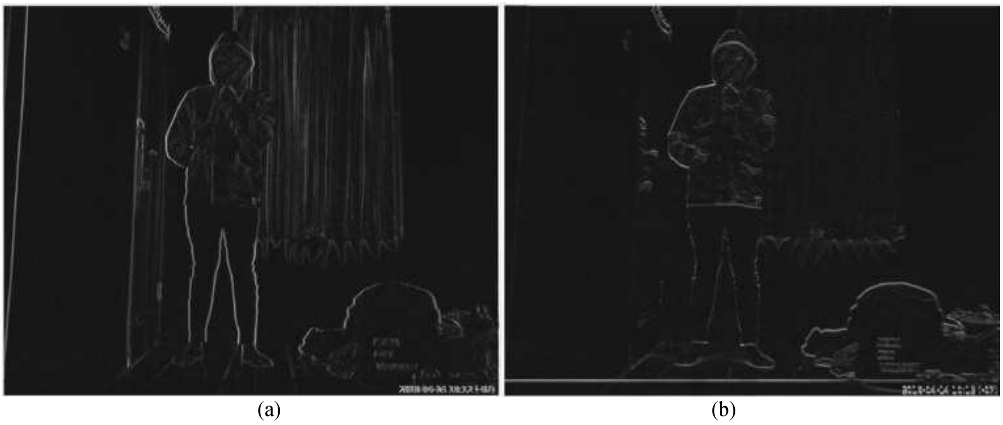


Fig. 10: Gradient Image (a) X-Gradient Image (b) Y-Gradient Image

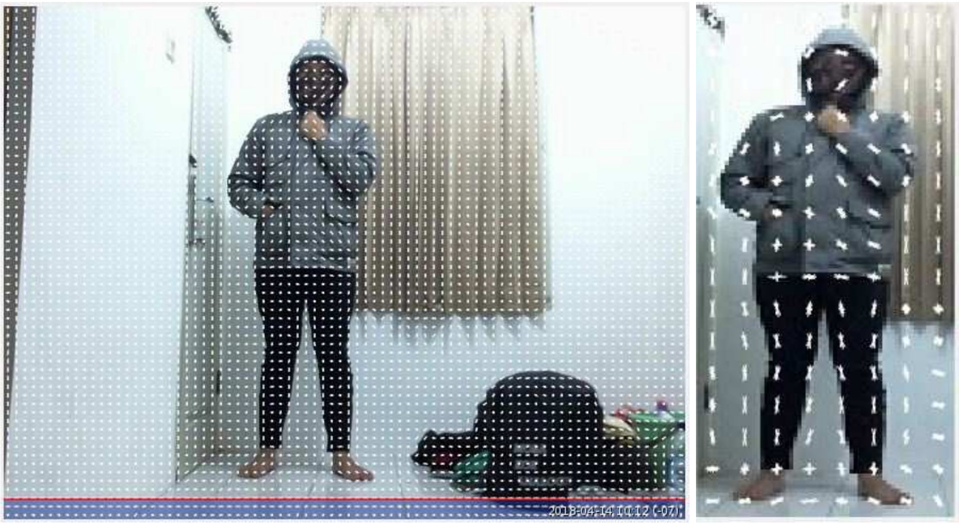


Fig. 11: Visualization of histogram of oriented gradients

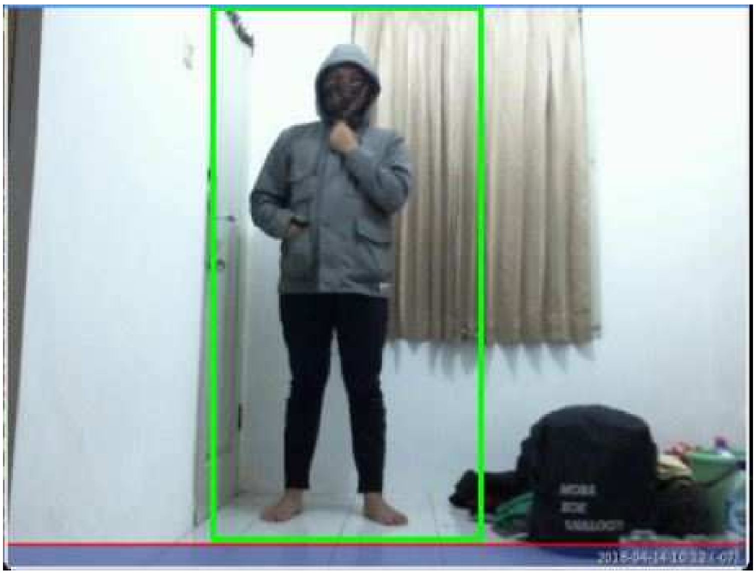
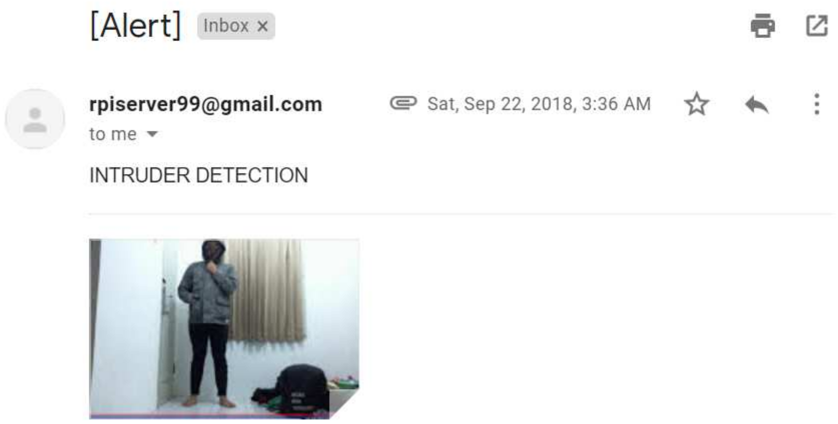


Fig. 12: Bounding boxes



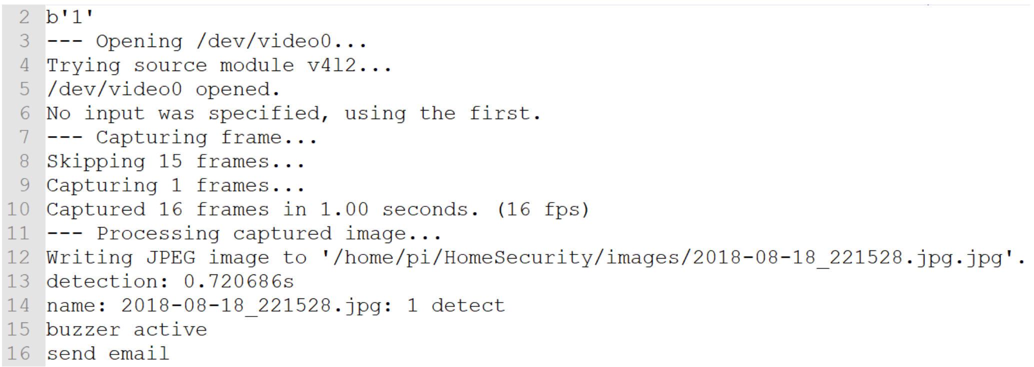
[Alert] Inbox ×

rpiserver99@gmail.com
to me

Sat, Sep 22, 2018, 3:36 AM

INTRUDER DETECTION

Fig. 13: Email notification



```
b'1'
--- Opening /dev/video0...
Trying source module v4l2...
/dev/video0 opened.
No input was specified, using the first.
--- Capturing frame...
Skipping 15 frames...
Capturing 1 frames...
Captured 16 frames in 1.00 seconds. (16 fps)
--- Processing captured image...
Writing JPEG image to '/home/pi/HomeSecurity/images/2018-08-18_221528.jpg.jpg'.
detection: 0.720686s
name: 2018-08-18_221528.jpg: 1 detect
buzzer active
send email
```

Fig. 14: System log

The captured image will be saved to the directory HomeSecurity/images/. After the system has finished analyzing, the photos that have been detected will then be moved to the directory HomeSecurity/images_detect and photos that cannot be detected will be moved to the directory HomeSecurity/images_fail.

Results and Discussion

This section discusses the implementation of IoT security monitoring system and the evaluation results. Firstly, we integrate and implement the designed system as shown in Fig. 15a to 15c. The figures show the connection between Arduino with PIR sensor, connection between Arduino and Raspberry Pi 3 and connection between Raspberry Pi 3 with buzzer and webcam, respectively.

Figure 16 shows the sketch of evaluation environment. The entrance access to this room is through 1 door and 1 window. The PIR sensor and camera are located in front the door as shown by Fig. 17. The scenario of the evaluation is described as follows:

- First, the system is activated and the intruder will open the door and enter the room
- The system will detect the movement of the intruder and take photos of the intruder
- The system will analyze the existence of intruder and activate the buzzer

Accuracy and Processing Time Evaluation

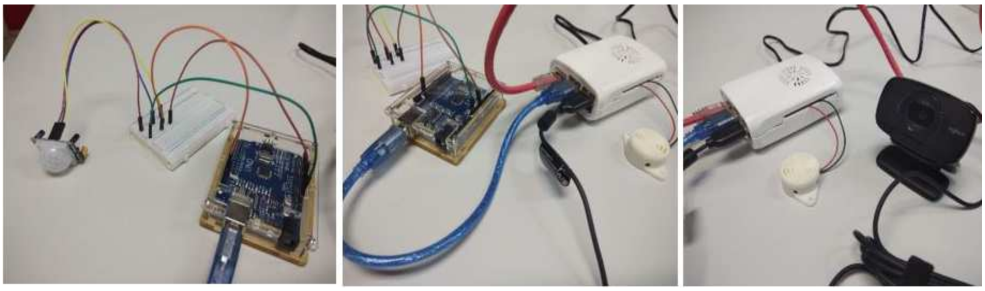
In this section, the accuracy of detection is described. The experiment used 2 objects, which are human (the true-event) and animal object (the false-event). The tests include checking from the start of the detection until the alarm is activated. For human detection, the input is in the form of humans from the beginning of detection until the alarm is activated and also testing from the beginning of detection until the alarm is activated to check whether the animal is detected or not.

This scenario is repeated for l00 times with various condition of intruders, e.g., carrying goods, half standing, facing sideways, half body, etc as shown in Fig. 18. There are two parameters measured in this evaluation. The first parameter is about the processing time of intruder detection. The second parameter is the accuracy of intruder detection.

Figure 19 shows the result of the processing time. The x-axis indicates the index of experiment (the total experiment is 100 times), while the y-axis indicates the measured time in seconds (s). Blue line indicates time to take pictures. It means the time started from the PIR sensor detects the movement until the photo is taken. Red line indicates time for human detection. It means the time started from taking the picture, system analyzes the picture, until the decision is made. The result shows that the average time to take the picture is 0.92 s, while the average time to detect the intruder is 0.99 s. Therefore, the total time from movement detection until the intruder image detection is 1.91 s. Based on the processing time measurement, the system can be considered capable of securing the house because it can detect the intruder within seconds.

Then, the accuracy of the human detection process is evaluated. The experiment produces 100 photos. From the photos, the existence of people on the photo is detected or in other words, the system is able to detect people or not from the photos. From the results of checking, 89 images were successfully detected (true-positive) and 11 other images could not be detected (false-negative). The time when the system successfully detects the intruder and when it does not successful in detecting the intruder is analyzed. The sample of image for true positive event can be seen in Fig. 20. In this sample, 1 person in that photo have a contrast colour with background, such as wall and door. Therefore, the system can detect the person in that photo easily. On the other hand, the sample image for true negative event can be seen in Fig. 21. From this image, the full human body cannot be recognized perfectly because the intruder is on the position of climbing the window.

For animal detection testing, the same scenario was used. The animal object was a cat and the number of tests performed was 30 times. Figure 22 shows a cat that was successfully photographed by the system. Figure 23 is the result of processing time. The x axis shows the trial index, while the y axis shows the time measured in seconds. The blue area shows the time to take pictures. This means that the starting time of the PIR sensor detects motion until the photo is taken. The red area indicates the time for animal detection. This indicates the time starting from taking pictures, analyzing images, to the final conclusion. The results show that the average time to take pictures is 1s, while the average time for detection is 1.35 s. Therefore, the total time from motion detection to animal detection is 2.35 s.



(a) (b) (c)

Fig. 15: (a) Arduino with PIR sensor (b) Arduino connected with Raspberry Pi 3 (c) Raspberry Pi 3 with buzzer and webcam

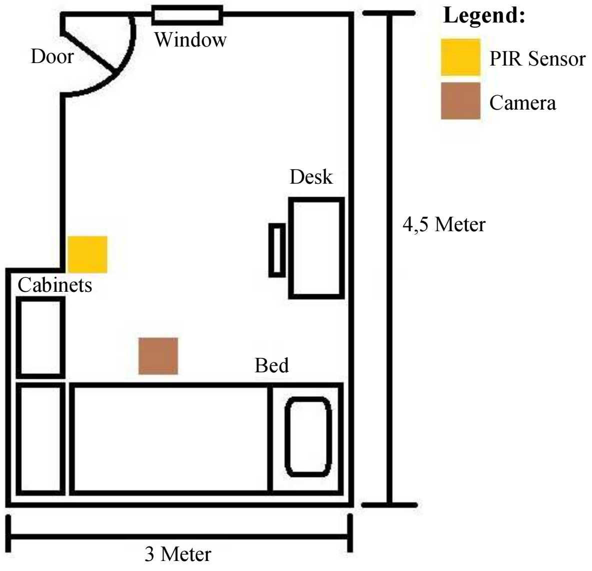


Fig. 16: Test environment

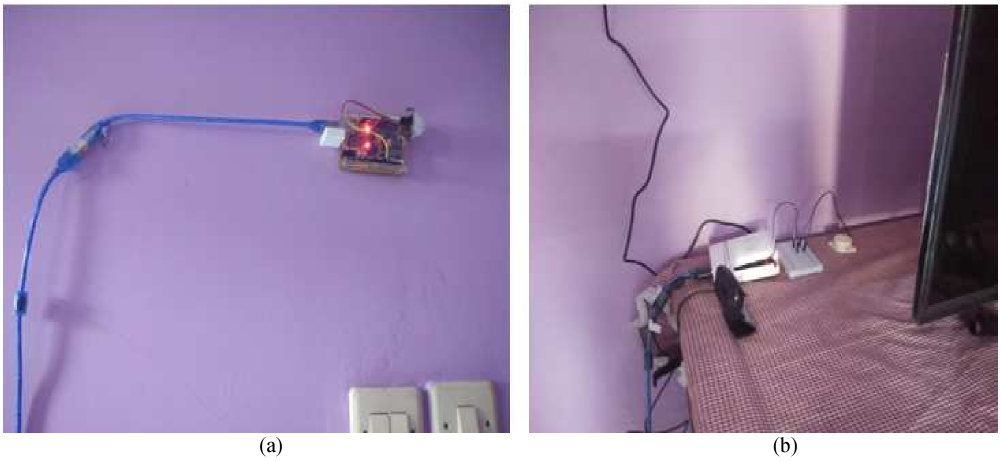


Fig. 17: Implementation in real environments, (a) installation of arduino and PIR sensors at the wall, (b) Installation of Raspberry Pi 3, cameras and buzzers above the table

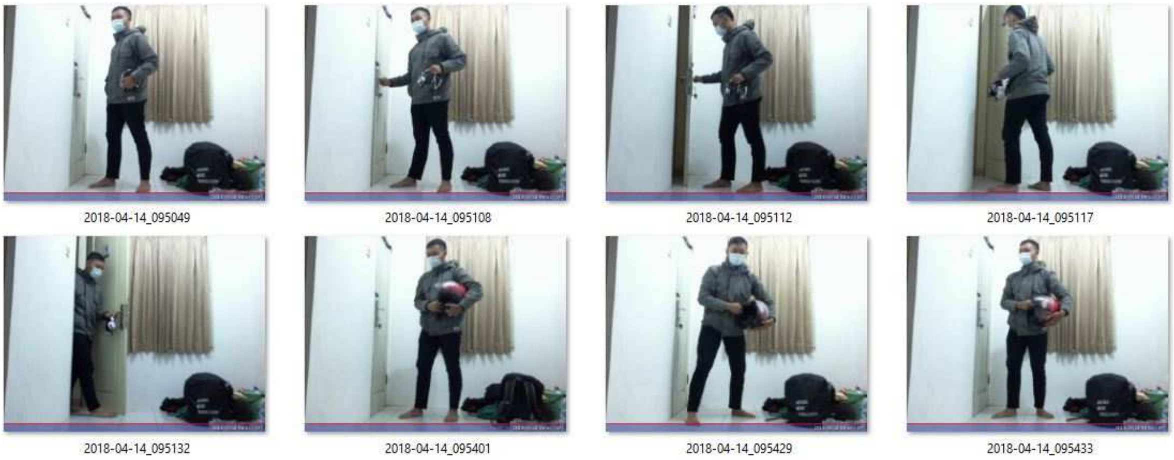


Fig. 18: Sample of captured image human

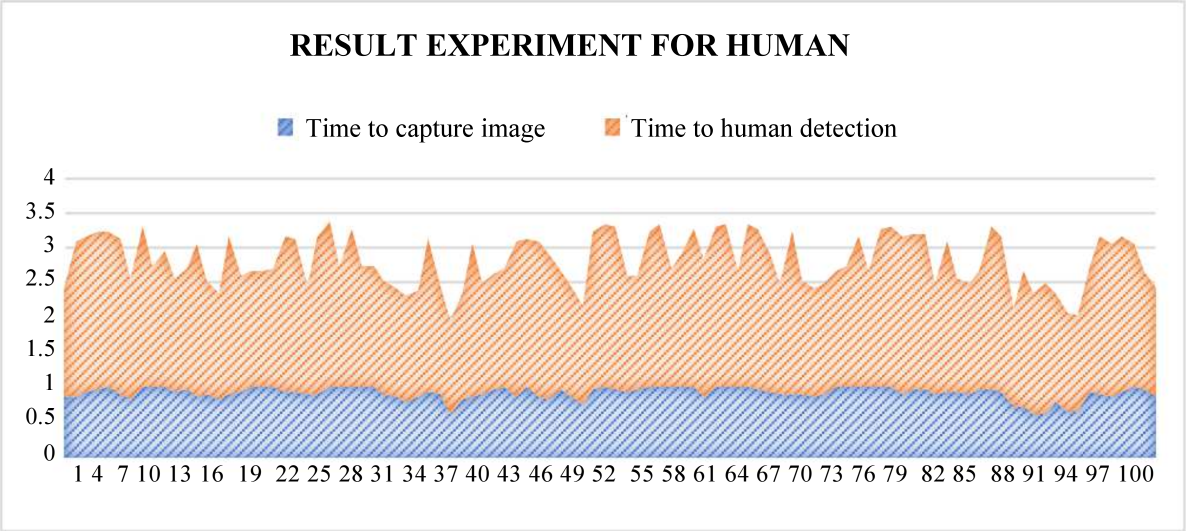


Fig. 19: Human detection time

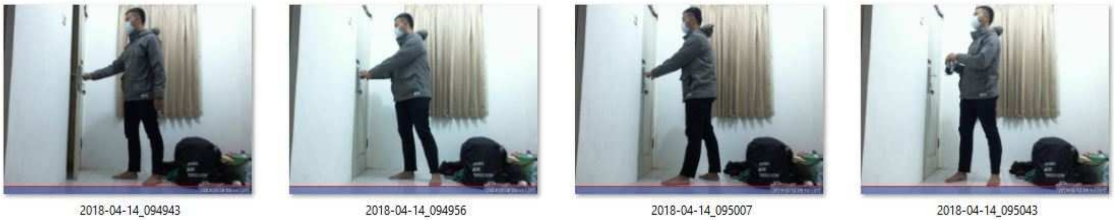


Fig. 20: Sample image of true positive event

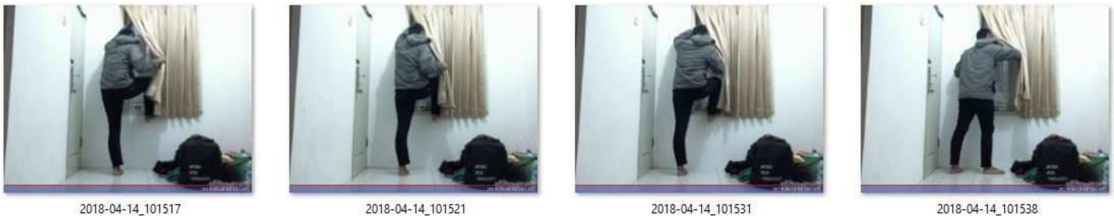


Fig. 21: Sample image of true negative event

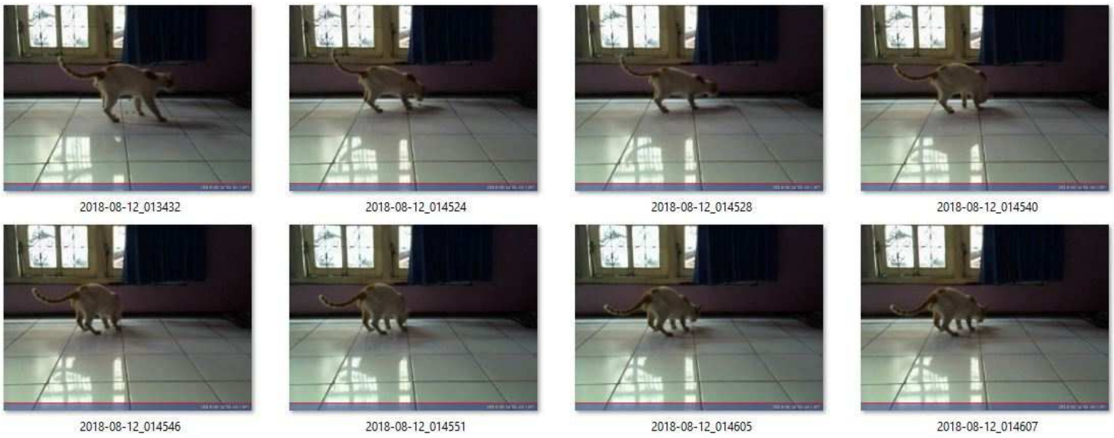


Fig. 22: Sample of captured image animal

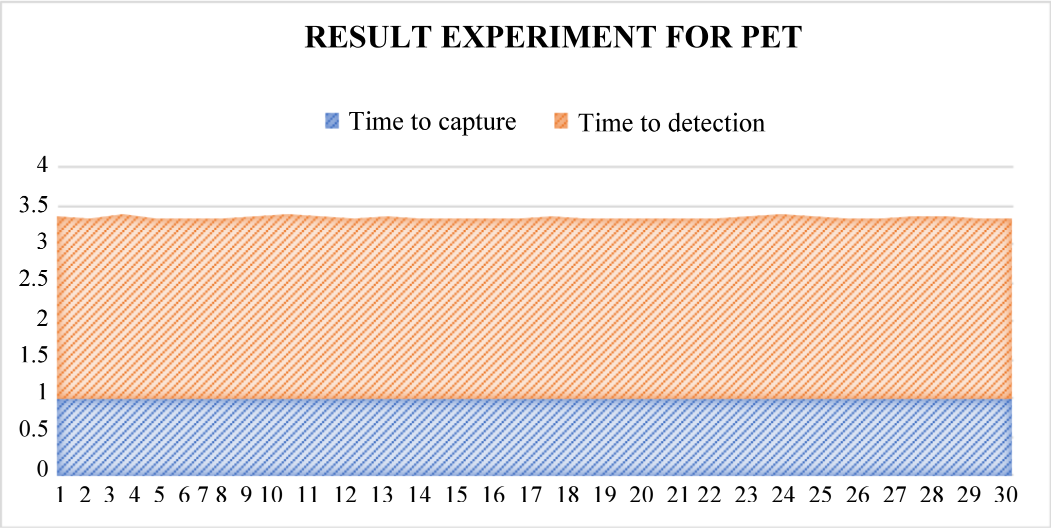


Fig. 23: Animal detection time

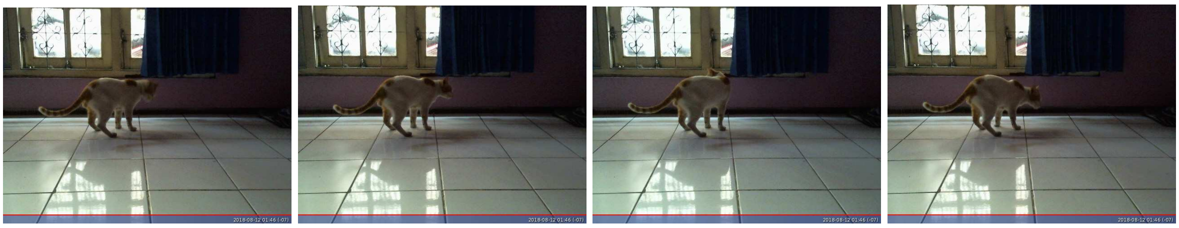


Fig. 24: Sample image of false negative event

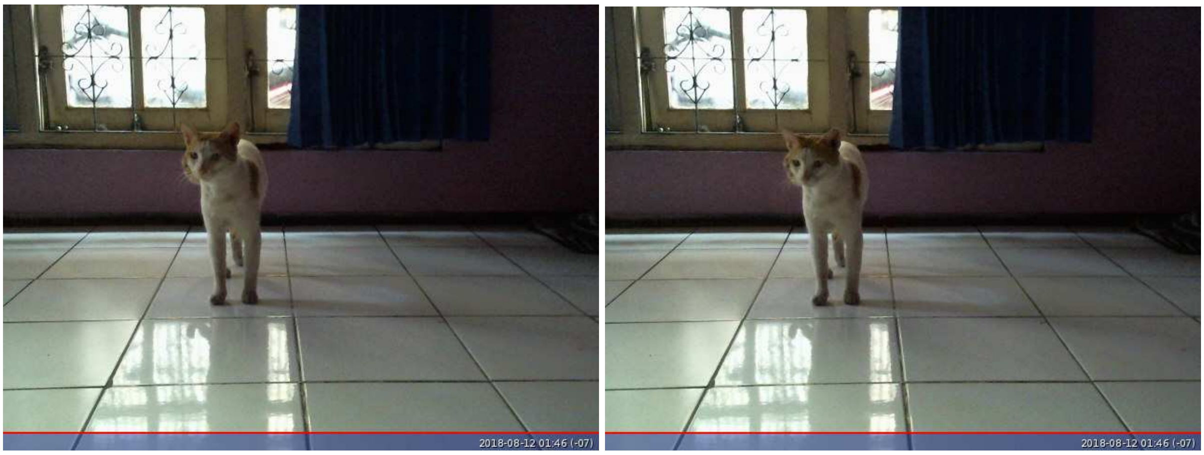


Fig. 25: Sample Image of False Positive Event

Table 2: Confusion matrix table

		Prediction	
Total sample = 130		Negative	Positive
Actual	Negative	TN = 28	FP = 2
	Positive	FN = 11	TP = 89
Accuracy: (TP+TN) / (TP+FP+FN+TN) = 0.9			

Table 3: Comparison result

No	Works	Method	Sensitivity	Time detection (second)	System accuracy
1	Patidar *et al*. (2014)	Change detection technique	-	-	86% (at 5-6 frames/second)
2	Our proposal	HOG + SVM	98%	1.9044	90%

Further, we analyze the sample of cat figure. It turns out that there are 2 false-positive results and 28 true-negative events. As shown in Fig. 24. In the true-negative event, the cat is not detected as a human. Therefore, it meets our expectation. The false-positive event is shown by Fig. 25. The cat in this figure is detected as a human because the shape and direction of the cat in the picture resembles a human, from the appearance of the head, body and 2 legs. Meanwhile, the long body of the cat and the tail do not appear in the figure.

From the results of the tests, the following results are obtained:

average time for human detection	: 1.91 s
average time for animal detection	: 2.35 s

It takes a little longer time for animal detection. It may happen due to the dark room and difficulty to estimate the edge in the picture of the cat.

From the data obtained, we have 100 photos for human intruder case and 30 photos of non-intruder case (animal object). To calculate accuracy, a confusion matrix is used, as shown by Table 2. The number of correctly detected photos is 117 photos. From the results of accuracy testing, the accuracy of the home security system using the HOG and SVM methods is 90% with the true positive rate (TPR) of 97.8% and the False Positive Rate (FPR) of 28.2%. The results outperform the works of Patidar *et al.* (2014) as shown by Table 3.

Therefore, it can be concluded that the system has achieved sufficient level of accuracy. It only takes around 2 sec for processing time, which is sufficient for the implementation. Therefore, it can be concluded that the system has achieved sufficient level of accuracy. It only takes around 2 sec for processing time, which is sufficient for the implementation.

Conclusion

This paper has proposed a security monitoring system based on IoT technology. The proposed system consists of Raspberry Pi 3, Arduino, PIR sensor, webcam and buzzer. The novelty of the system is the inclusion of human detection capability by HOG and SVM method and buzzer as method to warn the house owner. The simulation results show that the system can detect an intruder within seconds with accuracy of 90% with processing time around 2 seconds. Future research will explore other feature extraction and classification method to improve the accuracy of intruder detection.

Acknowledgement

The publication of this research is supported by Bina Nusantara University.

Author's Contributions

Nico Surantha: Idea of research, research advisor and paper author.

Wingky R. Wicaksono: Implementation, experiment and co-author.

Ethics

The authors agree with the publication of this manuscript, which does not contain ethical issues. All references are stated in the references section.

References

Abdullah, R., Z.I. Rizman, N.N.S.N. Dzulkefli, S.I. Ismail and R. Shafie *et al*., 2016. Design an automatic temperature control system for smart tudungsaji using Arduino microcontroller. ARPN J. Eng. Applied Sci., 11: 9578-9581.

Al-qaness, M.A.A., F. Li, X. Ma and G. Liu, 2016. Device-free home intruder detection and alarm system using Wi-Fi channel state information. Int. J. Future Comput. Commun., 5: 180-186. DOI: 10.18178/ijfcc.2016.5.4.468

Ansari, A.N., M. Sedky, N. Sharma and A. Tyagi, 2015. An internet of things approach for motion detection using Raspberry Pi. Proceedings of the International Conference on Intelligent Computing and Internet of Things, Jan. 17-18, IEEE Xplore Press, Harbin, China, pp: 131-134. DOI: 10.1109/ICAIOT.2015.7111554

Badamasi, Y.A., 2014. The working principle of an Arduino. Proceedings of the 11th International Conference on Electronics, Computer and Computation, Sept. 29-Oct. 1, IEEE Xplore Press, Abuja, Nigeria, pp: 1-4. DOI: 10.1109/ICECCO.2014.6997578

Bangali, J. and A. Shaligram, 2013. Design and implementation of security systems for smart home based on GSM technology. Int. J. Smart Home, 7: 201-208.

Charadva, M.J., R.V. Sejpal and N.P. Sarwade, 2014. A study of motion detection method for smart home system. Int. J. Innovat. Res. Adv. Eng., 1: 148-151.

Chitnis, S., N. Deshpande and A. Shaligram, 2016. An investigative study for smart home security: Issues, challenges and countermeasures. Wireless Sensor Netw., 8: 61-68. DOI: 10.4236/wsn.2016.84006

Chuimurkar, R.M. and V. Bagdi, 2016. Smart surveillance security monitoring system using Raspberry PI and PIR sensor. Int. J. Recent Trends Eng. Res., 2: 364-371.

Dalal, N. and B. Triggs, 2005. Histograms of oriented gradients for human detection. Proceedings of the Computer Society Conference on Computer Vision and Pattern Recognition, Jun. 20-25, IEEE Eplore Press, San Diego, CA, USA, pp: 886-893. DOI: 10.1109/CVPR.2005.177

Eseosa, O. and E. Promise, 2014. GSM based intelligent home security system for intrusion detection. Int. J. Eng. Technol., 4: 595-605.

Kumar, A.S. and P.R. Reddy, 2016. An internet of things approach for motion detection using raspberry-pi. J. Int. J. Adv. Technol. Innovat. Res., 8: 3622-3627.

Parab, A.S. and A. Joglekar, 2015. Implementation of home security system using GSM module and microcontroller. Int. J. Comput. Sci. Inform. Technol., 6: 2950-2953.

Patidar, S., A.P. Pandey, K. Ketan and G.R. Pareshkumar, 2014. Real time vision based security system. IOSR J. Electron. Commun. Eng., 9: 46-53. DOI: 10.9790/2834-09554653

Raja, M.A., G.R. Reddy and Ajitha, 2017. Design and implementation of security system for smart home. Proceedings of the International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, Feb. 16-18, IEEE Xplore Press, Chennai, India, pp: 1-4. DOI: 10.1109/ICAMMAET.2017.8186705

Sahoo, K.C. and U.C. Pati, 2017. IoT based intrusion detection system using PIR sensor. Proceedings of the 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, May 19-20, IEEE Xplore Press, Bangalore, India, pp: 1641-1645. DOI: 10.1109/RTEICT.2017.8256877

Satpathy, A., X. Jiang and H.L. Eng, 2014. Human detection by quadratic classification on subspace of extended histogram of gradients. IEEE Trans. Image Process., 23: 287-297. DOI: 10.1109/TIP.2013.2264677

Surantha, N. and W.R. Wicaksono, 2018. Design of smart home security system using object recognition and PIR sensor. Proc. Comput. Sci., 135: 465-472. DOI: 10.1016/j.procs.2018.08.198

Tanwar, S., P. Patel, K. Patel, S. Tyagi and N. Kumar *et al*., 2017. An advanced internet of thing based security alert system for smart home. Proceedings of the International Conference on Computer, Information and Telecommunication Systems, Jul. 21-23, IEEE Xplore Press, Dalian, China, pp: 25-29. DOI: 10.1109/CITS.2017.8035326