# Intruder detection and recognition using different image processing techniques for a proactive surveillance

**Nelson C. Rodelas[1], Melvin A. Ballera[2]**
[1]Information and Communication Technology Department, University of the East, Manila, Philippines
[2]Research and Development Office, Technological Institute of the Philippines, Manila, Philippines

**Article Info**

***Article history:***

Received Jan 14, 2021
Revised Aug 31, 2021
Accepted Sep 7, 2021

***Keywords:***

AdaBoost
Deep learning algorithm
OpenCV
Proactive camera
Surveillance camera
Viola-Jones algorithm

## ABSTRACT

To innovate a proactive surveillance camera, there is a need for efficient face detection and recognition algorithm. The researchers used one of the Viola-Jones algorithm and used different image processing techniques to recognize intruders or not. The goal of the research is to recognize the fastest way on how the homeowners will be informed if an intruder or burglar enters their home using a proactive surveillance device. This device was programmed based on the different recognition algorithms and a criteria evaluation framework that could recognize intruders and burglars and the design used was developmental research to satisfy the research problem. The researchers used the Viola-Jones algorithm for face detection and five algorithms for face recognition. The criteria evaluation was used to identify the best face recognition algorithm and was tested in a real-world situation and captured a series of images camera and processed by proactive face detection and recognition. The result shows that the system can detect and recognize intruders and proactively send a notification to the homeowners via mobile application. It is concluded that the system can recognize the intruders and proactively notify the household members using the mobile applications and activate the alarm system of the house.

***Corresponding Author:***

Nelson C. Rodelas
Information and Communication Technology Department, University of the East
2219 C. M. Recto Avenue, Brgy. 404, Zone 41, Sampaloc, Manila, Philippines
Email: nelson.rodelas@ue.edu.ph

## 1. INTRODUCTION

In our modern world, the result of our capabilities can be greatly enhanced by computers. Technology is a vital aspect of the human condition [1]. From mobile phones with a lot of applications to supercomputers that act as servers of a massive amount of users, local area networks to cloud technologies, and a lot more. It is a fact that the world is dominated by technology on an extensive scale with an exponential rate of development because of curious minds that seek innovation. Digital image processing (DIP) is one of the breakthroughs in technology that focuses on processing digital signals. Because of the cheaper computers and dedicated hardware, most of the advanced technologies concerning images and their uses are now created with the use of DIP [2]. With this, images are digitized and can be stored in computer storage and other storage media [2], [3] for pre-processing of data and data mining [4]. Image processing can format and correct data, improve visual interpretation, and automatize target features and classifications [3].

Figure 1 shows the process of recognizing faces. The first process is to detect the face, then extract the different features of the face that make it unique and use it for recognition. Living in a new era where crimes are increasing, people want to secure their belongings at their homes. In that scenario, a person could have a system with advanced technological implementation for a person not to worry when they are far from their home [5]. One area of technology that could be used in that context is the field of computer vision using closed circuit television (CCTV) or surveillance camera. CCTV has two generations: a surveillance camera that has human intervention in evaluating images and a computer-based camera that can evaluate its images [6]. The latest generation of CCTV uses a digital system of surveillance that serves a wide range of requirements in terms of security however, some of them produce an insufficient image or video quality to support the detection of crimes. Also, the human factor is one of the major issues in using CCTV. It can be said that the existing CCTV system in the Philippines is reactive in terms of surveillance. It means that CCTV only uses it when the crime is already done. Another problem is that the criminals, being notorious, and do not mind CCTV, continuously commit a crime to satisfy their evil doings. The face of any individual may be caught in CCTV but its ability to identify is not always easy [7]. What is needed is a system that helps prevent future attacks of criminals [8]. Robbers are usually people who lurk around houses which they believe have a very weak security system. Weak security allows the robbers to enter the houses unnoticed by the people around them. Sometimes they do it to houses located in an environment where few people are visible so that they can enter unnoticed. With that said, some robbers do it by casually walking inside homes with open or unlocked doors while people think that he/she lives in that house.

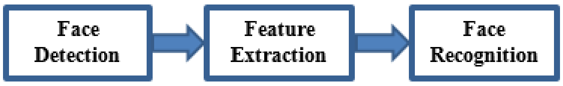


Figure 1. Face recognition process

The main focus of the research is to secure the house by detecting and recognizing intruders and burglars in real-time using the proposed prototype. It has an alarm system, mobile applications, and different image detection and recognition algorithm plus criteria evaluation to proactively produce results when intruders are recognized. To gather insights that would help this research, the researchers reviewed several recent studies and literature related to this study. The ideas gathered were used to evaluate what is the best methodology and tools that the proponent used to solve the problem.

The presence of a security system in households and establishments is important in the context of creating security systems [9]. Security system focuses on providing security when the homeowners are away from their home [5]. It was stated that short message service (SMS) could perform remote communication between homeowners and household devices. Mobile phones with short messaging service could be very useful when embedded in household security systems, where messages sent by security systems are immediately received by homeowners in the form of SMS. Many services offer alarm monitoring that allows homeowners to access their home security system via the internet [10]. It could check the status of the security system and view a live feed of surveillance cameras. Advanced systems even allow its users to configure security codes and activate or deactivate the security system by using web applications. But there is a more modern development in the home security system which is mobile devices and applications that offer portability. The use of mobile devices and a monitoring system offers a new way so that people could monitor the security of their belongings anytime and anywhere. Some prototypes use facial recognition in surveillance [11]. The manufacturers of the home security system have several ways for homeowners to monitor the security system of their home even when they are far away from their home [12]. Alarm systems nowadays could notify homeowners about the status of their security system by paging them. There is an available SMS communication home security system that monitors the house using sensors [5]. The researchers used a microcontroller and global system for mobiles (GSM) unit using a mobile phone to notify users when an intrusion occurs.

It is considered that the demand for home security using android based phones has created a system that secures the main entrance of the home and the car door lock [13]. The system also used Bluetooth technology to control the different appliances inside the house. It is also said that most of the algorithms for face recognition were developed to enhance images captured from different applications like military tactics, spacecraft, security purposes, and others [14]. They discussed the different face recognition algorithms and factors affecting face recognition. They said that the Eigenface algorithm was focused on the illumination of the image; the geometric based algorithm that was focused on perimeters, areas, and segments of image forms because of points located on it; template matching algorithm recognizes image using statistical treatment by converting images into numerical values with templates and eliminates variances. They said that expressions, occultation or hindrances in the captured image, poses or face angle, illumination or lightness and darkness of the image, and facial features were the basic factors in face recognition. Deep learning shows excellent performance in face recognition [15]. However, it needs a large number of interpreted training datasets. The researchers defined a deep learning algorithm as the enhanced algorithm of the machine learning algorithm that has more than three hidden layers to perform self-recognition of the image.

## 2. METHODOLOGY

The conceptual framework was designed after knowing the different gaps in developing a proactive surveillance camera. Different algorithms and criteria evaluation were considered to create the system. Figure 2 shows the conceptual framework of the research. The system captures images and performs detection of faces using the Viola-Jones Algorithm through the captured images. Once the system detects faces coming from the images, the detected faces are recognized using the five face recognition algorithms (eigenfaces, fisherfaces, local binary pattern, template matching, and deep learning) and match it to the database of faces. The system also performs the criteria evaluation to identify the best algorithm to be used in the system.

Different criteria were the following: illumination that measures the rate of recognition in terms of lighting condition of the captured picture; the facial angle-that measures the rate of recognition in terms of the angle of the detected face; the level of confidence of each algorithm in the process of recognition; the facial features or the changes of the feature of the captured face; and the time complexity or the time required in recognizing the detected face, it iterates until there are unmatched faces detected by the system. The server of the system has the capability of viewing the logs of intrusion and printing the list of captured intruders. It sends messages using SMS to the homeowners when there is no internet connection to notify that there is an intruder in the house and to open the mobile application to view the captured image of the intruder; The system automatically sends the captured picture to the through cloud technology when there is an internet connection. The mobile applications can view the captured picture of an intruder; the system has an automatic alarm system when an intruder is detected and the mobile application user has the privilege to turn off the alarm system.

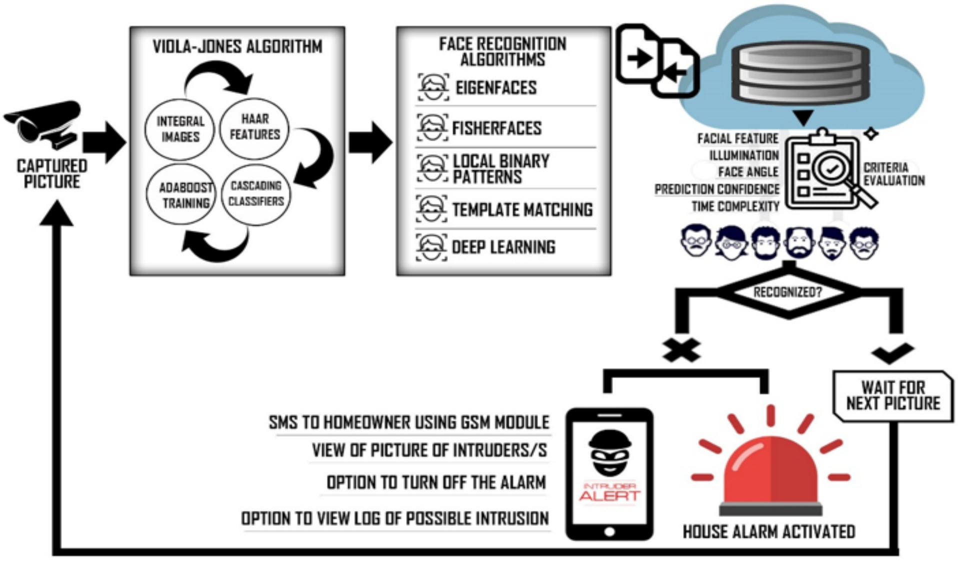


Figure 2. Conceptual paradigm

### 2.1. Research method

The researchers used developmental research. A developmental research method is defined as the study of design, development, and evaluation of products, programs, and processes that meet the criteria of effectiveness and consistency. The evaluation of the final product is implementation [16]. It facilitates the study of new tools, models, and procedures so that the researchers can anticipate the efficiency and effectiveness of the system. The researchers used an agile methodology that is used to develop products through iterations of the process. This methodology is effective specifically when the project can be divided into many small tasks, with lots of creativity, and must be developed to fit with the stakeholder's expectations.

### 2.2. Hardware devices

A raspberry pi (RPi) no infrared filter (NoIR) camera with a minimum of 8 megapixel (MP) quality was used to fetch the video feed and to process the video feed frame by frame. A camera without an infrared light filter could be used at night to vision to capture images even when it is dark with the aid of an infrared light-emitting diode (LED). The raspberry pi 3 is a circuit module that has the capabilities of a computer. It has universal serial bus (USB) ports and an ethernet port. This is responsible for conducting the comparing and sending of email to the homeowner containing the image of the suspected intruder inside the house. The infrared (IR) illuminator is the one responsible for allowing the raspberry pi camera to detect faces in dark places that allows the researchers to get better results and higher accuracy.

### 2.3. Software devices

The researchers used python, a high-level programming language to develop the face recognition program. It was integrated with the open-source computer vision (OpenCV) library [17]. OpenCV) is a library for computer vision that is free. It could be used in web development with the aid of different frameworks such as Django, Flask, and Pyramid. The pyramid framework was used in developing the web application that received and displayed the reports of intruders detected by the user. JQuery is a JavaScript library used in web applications to easily manipulate web page elements. MongoDB, a document-based database management system, serves as storage of data that is necessary for the functionality of the prototype. To connect the web page and the server, asynchronous JavaScript (AJAX), and xtensible markup language (XML) were used to send a POST request to the server in order to query if a fugitive is detected or not.

### 2.4. Algorithms

The face detection procedure was based on the features of the face (eyes, nose, and mouth) rather than its pixels because feature-based systems can be operated faster than pixel-based systems. It uses a Haar-like feature that performs the scalar product of the Haar-like templates and the captured image as seen in Figure 3. Given the pattern X of image A with the same size of N×N, it is defined by (1).

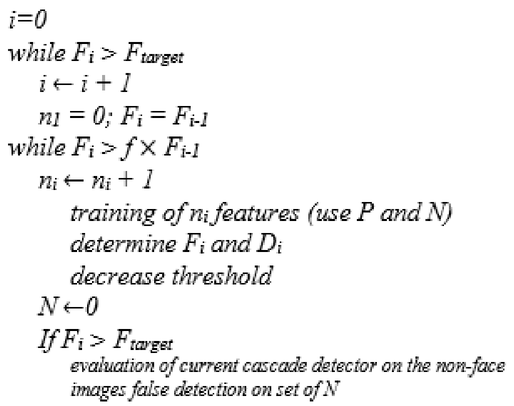
$$\sum_{1\leq i\leq N}\sum_{1\leq j\leq N} A(i,j)-1_{X(i,j)} \text{ is white}=\sum_{1\leq i\leq N}\sum_{1\leq j\leq N} A(i,j)-1_{X(i,j)} \text{ is black} \qquad (1)$$

The image should be normalized beforehand by its means and variance for the different lighting positions of the captured image [18]. The integral image can be computed using intermediate interpretation for the image that results in a training set of negative and positive images. It is being classified using AdaBoost classifiers [19] that boost the classification performance of a learning algorithm. The Ada-Boost algorithm combines all the weak classification functions and forms a stronger classifier and it approaches a training error of zero exponentially in the number of rounds of training [19], [20].

After performing the learning algorithm, the system trains cascade classifiers. The goal of detection and performance of the system in detecting face is dependent on the cascade design process. In building a cascade detector, the system selects the maximum acceptable false-positive layer (f), and the minimum acceptable detection rate per layer (d) [18], [19]. The system also selects Ftarget (overall false-positive rate) and initializes the false positive and the detection rate into one. Figure 3 shows the looping condition of the training algorithm of a cascade detector. The algorithm used sets of negative and positive examples in training in features using AdaBoost and evaluated current cascade classifiers to determine false positive rate cascade Fi and the detection rate Di [19].

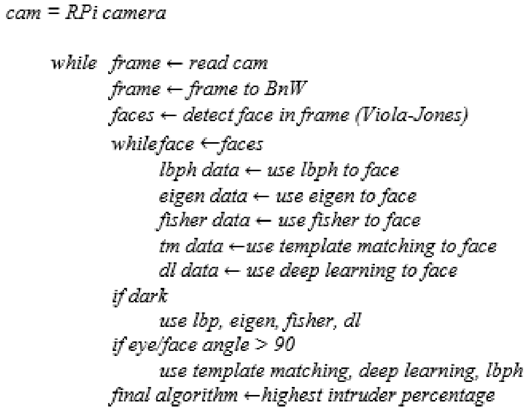
After the system detects any faces, the system will then recognize if the detected face is an intruder or not. Different algorithms were considered in intruder detection. The system used a template-based approach to face recognition that compares images with sets of templates from a database [21]. Sets of templates were constructed using different algorithm tools like principal component analysis (PCA) [22], [23] using eigenfaces algorithm, linear discriminant analysis (LDA) [24] using fisher faces algorithm, support vector machine (SVM) [25] using local binary pattern histogram, the template matching algorithm [26], and the deep learning algorithm [15]. The researchers created the criteria evaluation of the system to identify the appropriate and best face recognition algorithm to be used in intruder detection. This criteria evaluation is composed of illumination, face distance, time complexity, confidence level, and facial feature.

Figure 4 represents the pseudocode of the different criteria in the system. The raspberry pi (RPi) camera reads images and converts them into the frame then the frame will be converted into black and white form. The Viola-Jones algorithm will detect the face on the frame then it will be compared to the database of faces and performs the five algorithms for face recognition. The criteria evaluation will evaluate the illumination (dark), and perform local binary pattern algorithm (lbph), eigenface (eigen), fisher faces (fisher), and deep learning algorithm (dl). For the face angle, template matching, dl, and lbph will be evaluated. The algorithm with the highest percentage of intruder recognition will be displayed in the output. The camera captures an image that serves as an input for raspberry pi. The raspberry pi then prepares the image to be processed into the five algorithms. The five algorithms are local binary pattern histogram, fisher faces, eigenfaces, template matching, and deep learning.



```
i=0
while $F_i > F_{target}$
    $i \leftarrow i + 1$
    $n_1 = 0; F_i = F_{i-1}$
while $F_i > f \times F_{i-1}$
    $n_i \leftarrow n_i + 1$
        training of $n_i$ features (use P and N)
        determine $F_i$ and $D_i$
        decrease threshold
    $N \leftarrow 0$
    If $F_i > F_{target}$
        evaluation of current cascade detector on the non-face
        images false detection on set of N
```

Figure 3. Training algorithm for building cascade detector [19]



```
cam = RPi camera

    while  frame ← read cam
           frame ← frame to BnW
           faces ← detect face in frame (Viola-Jones)
           while face ← faces
                lbph data ← use lbph to face
                eigen data ← use eigen to face
                fisher data ← use fisher to face
                tm data ← use template matching to face
                dl data ← use deep learning to face
           if dark
                use lbp, eigen, fisher, dl
           if eye/face angle > 90
                use template matching, deep learning, lbph
           final algorithm ← highest intruder percentage
```

Figure 4. Pseudocode for criteria evaluation

## 3. RESULTS AND DISCUSSION

The main objective of the research is to innovate a proactive surveillance device that is used to detect and recognize intruders. This device uses different image processing techniques and criteria evaluation for accurate recognition of intruder/s. Specifically, the main objectives of the system are to identify the different image processing techniques that proactively seized images for surveillance, detect and recognize an intruder by different image processing techniques, create a framework that chooses an image processing technique as an algorithm to proactively perform surveillance and to monitor and notify the household owners and authorities using the mobile application once theft incidents happened.

Figure 5 shows the sample result of the system. The system was trained to detect and recognize faces on the captured images on the surveillance camera. A fifteen stage cascaded classifiers were trained and falsely eliminated 0.2% of the face patterns [27]. The system was expected to have a false alarm rate of 0.00215 or 4.1×10-33 and a hit rate of 0.99815 or 0.97. The system was trained by the captured pictures from the camera with a face training set of over 4,000 labeled faces with a base resolution of 24×24 pixels.

The system was tested in a real-world situation and captured a series of images using the serial camera and processed by proactive face detection and recognition. Using the different sub-algorithms and classifiers, the system can automatically detect faces or faces in a single frame. The color of the frame (box on the face) can be edited in the code. The system produced a frame or box on the detected face. The box contains two colors, a recognized face from the database represented by a green box and an intruder represented by a red box. This recognition is discussed in the next section.

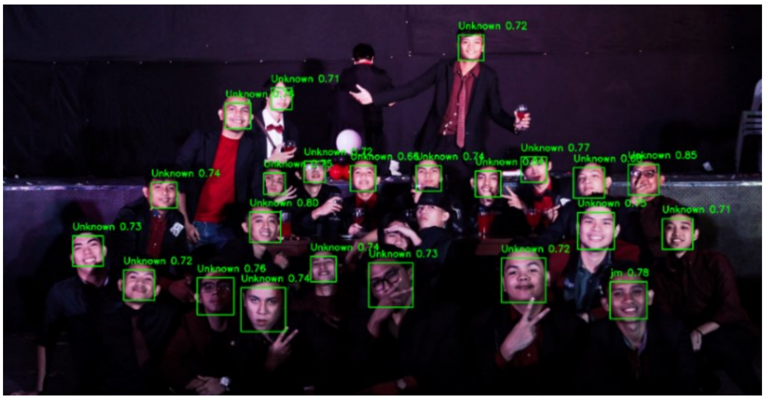


Figure 5. Sample face detection using Viola-Jones algorithm

### 3.1. Detection constraints

The main purpose of the system was to detect and to recognize intruder entry in the house in real-time and notify the owners and send a picture of the captured image. However, most of the intruders wore a bonnet, cap, or even cover his/her face especially if they know household surveillance cameras. The system considered this scenario by seeing the motion detection algorithm if the system did not detect any face. This algorithm was focused on each frame produced by the serial camera and compared them all to each other and analyzed if these frames have the same threshold. The pseudocode for motion detection was activated after searching for the face [7]. The surveillance camera was elevated to a distance of five to six meters from the entrance of the house to capture the frame. Once detected, the system then notified the owners and was asked to trigger the alarm button. After face detection, the system performed face recognition.

### 3.2. Face recognition results

This section discusses how the system performs a different algorithm for face recognition. The system performs five algorithms in face recognition, and each of these algorithms had a unique process in recognizing the detected image. The system used the OpenCV library in performing face recognition. OpenCV is a cross-platform library that focuses on the latest computer vision algorithms and real-time image processing. In terms of the database, the researchers created the data set by uploading pictures of five persons in five different poses, illuminations, and face angles for testing purposes. OpenCV created a comma-separated value (CSV) file of these twenty-five images since it is the simplest independent platform that can be used.

Table 1 shows the distribution of the percentage of the success rate of intruder recognition. These are the results of the testing for each algorithm and its success rate in recognizing intruders who entered the house using the dataset. The result shows that all of them had a high success rate. The lowest success rate performance was the template matching with a rate of 89.12%. The highest success rate performance was the deep learning algorithm with a rate of 97.32%.

Table 1. Image intruder success rate

| Algorithm | Success Rate |
|---|---|
| Eigenface | 92.96 |
| Fisherface | 93.84 |
| Local Binary Pattern | 93.08 |
| Template Matching | 89.12 |
| Deep Learning | 97.32 |

Figure 6 shows the graphical representation of the number of testing conducted using the system and the percentage rate of each algorithm in recognizing the homeowners or the faces that are saved in the database. The result shows that there is a lower percentage rate of detecting intruders on most of the algorithms. Figure 7 represents the graphical representation of intruder detection and recognition of different algorithms over its number of testing. It recognizes that there was an intruder in the house. The alarm system will then activate, and notification of homeowners and government authorities were notified. After the different image processing techniques were performed, the system performed criteria evaluation framework to recommend the best algorithm to send images to the system server and to mobile application.

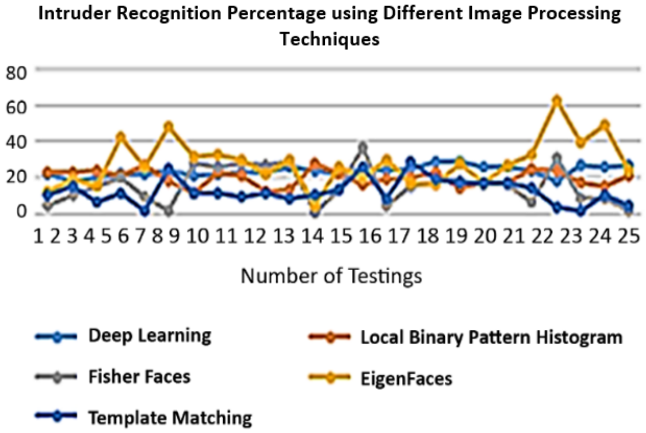


Figure 6. Detection and recognition of homeowners

Table 2 shows the results of the criteria evaluation testing conducted by each criterion. It shows that template matching and deep learning algorithms recognized the dataset in the criteria face angle, while template matching was the only algorithm unable to recognize the dataset. One of the reasons is that this algorithm only matches the dataset and the captured image [26]. Since the entire algorithm had its procedure in recognizing the image, it is evident that recognized images in their confidence level. Fisher face algorithm was more accurate when it comes to time complexity and the deep learning algorithm had a higher percentage of recognition in terms of facial features. These results were used to output the image on the mobile application for notification of intruders. The result was different when the system captured a picture of the detected intruder.

The result of the testing shows the process of choosing the right algorithm to be used in each scenario to proactively perform surveillance. It gave an accurate result of the image and the right output in notifying the homeowners whether the captured image is an intruder or not. The result also shows that deep learning algorithms can give higher percentage results in four out of five criteria evaluation.

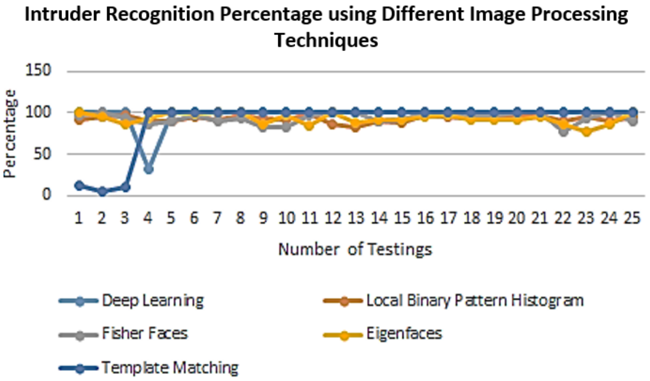


Figure 7. Detection and recognition of intruders

Table 2. Results of the success rate of intruder recognition with criteria evaluation

| Algorithm | Face Angle | Illumination | In %<br>Confidence Level | Time Complexity | Facial Feature |
|---|---|---|---|---|---|
| Eigenface | 14.29 | 97.10 | 74.29 | 77.14 | 82.86 |
| Fisherface | 20.00 | 74.29 | 80.00 | 94.29 | 14.29 |
| Local Binary Pattern | 11.43 | 65.71 | 71.43 | 18.00 | 7.00 |
| Template Matching | 54.29 | 17.14 | 77.14 | 25.71 | 88.57 |
| Deep Learning | 80.00 | 91.43 | 88.57 | 14.29 | 94.29 |

### 3.3. Hardware and software integration

The system was composed of hardware devices for monitoring and notification. These devices are raspberry pi, serial camera, IR, alarm, GSM module laptop or desktop for server and cellphone with mobile app software installed on it. A server can monitor and record events in real-time and save them to the database. The process of notification was dependent on the detected and recognized face of the system. It will not function when the recognized face is on the database. The notification will only function once the system detected and recognized the intruder. When the system detected, an intruder with real-time date and time, the system then automatically triggered the alarm system of the house and the mobile application user can only turn off the alarm. If the mobile data is not available, since it was activated using the internet, there was a notification using the SMS informing that intruder was entering the house.

The researchers also tested the performance of different physical components of the system to check the reliability of the devices such as the alarm system, SMS messaging of the GSM module, the range of the raspberry pi camera, and the cloud computing sending capabilities of the system. Ensuring the proper operations of the alarm system and proper communication to the raspberry pi is one of the purposes of testing the response time of the alarm system. The researchers tested the alarm response time by tabulating the delay time before the activation of the alarm system. The researchers tested 20 unrecognized images. Once the raspberry pi recognized an intruder, it sent enough electricity to activate the delay module and this delay module triggered the alarm device to be activated.

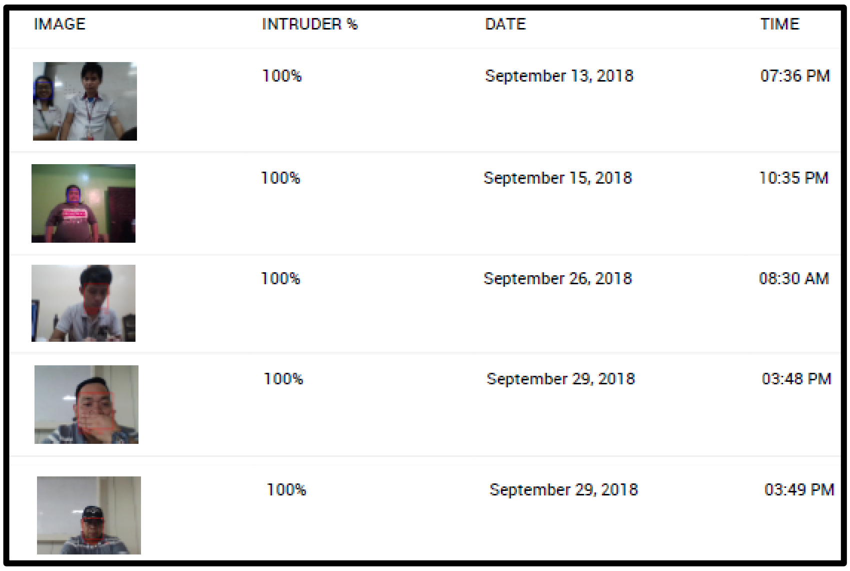
The average time recorded for the response time was 29.63 seconds. It can be said that the response time before the alarm system to be activated gives a faster reaction even if the system had many functionalities, performed algorithms, and criteria evaluation system. The system also has the capability of texting the homeowners and government authorities when the mobile application in the event that the mobile app is not connected to the internet. The researchers tested the time response of the GSM module by sending text messages to mobile application users. The GSM module was tested based on the elapsed time in sending the text message and receiving the message by the mobile app users. The alarm system and the GSM module were simultaneously activated and the SMS message was “An intruder has been detected in your house.” The researchers tested twenty unrecognized images to trigger the system that the image is an intruder. The researchers recorded the elapsed time in receiving the data from the system to the mobile phone using the mobile application.

### 3.4. Testing results

The researchers conducted twenty trials and tabulated the time response of text messages in seconds. The average response time is 34.76 seconds. It is important to identify the range of the raspberry pi serial camera in terms of its distance. The researchers tested and computed the average distance of the face image captured by this device. The researchers tested the camera with an initial distance of 4.5 inches and increased it by adding another 4.5 inches until it reached a point that the camera can no longer recognize the image. For an interval of 4.5 inches for each test, the researchers came up with a maximum distance/range of 94.49 inches or 2.4 meters. The system used cloud computing in sending the detected and recognized intruders into the house. Testing the average time response of the cloud in sending information was tested and tabulated. The researchers also tested the lapse time from notification of cloud technology to the mobile application. Again, the researchers used twenty unrecognized images. The system was connected to broadband because the raspberry pi needed an internet connection to connect to the mobile application. The sending capability of the system to its mobile application is dependent on the strength of the internet connection. The average response time of cloud technology is 14.27 seconds therefore, the researchers considered the strength of the internet connection.

The researchers made sure that all the features of the system, whether physical devices, server functionality, or mobile application are functioning and performing according to the flow of the system. The server of the system has the capability of providing the list of detected and recognized intruders. The report was composed of the image of the intruder, the rate or percentage of intrusion, and the date-time it was recognized. It can also be seen in the report that the system can detect and recognize intruders that wear a cap, or even the face is not fully seen.

Figure 8 shows the sample intrusion report of the system. The server of the system has the capability of providing the list of detected and recognized intruders. The report includes the image of the intruder, the rate or percentage of intrusion, and the date-time it was recognized. It can also be seen that the system can detect and recognize intruders that wear a cap or even the face is not fully seen.



| IMAGE | INTRUDER % | DATE | TIME |
|---|---|---|---|
| | 100% | September 13, 2018 | 07:36 PM |
| | 100% | September 15, 2018 | 10:35 PM |
| | 100% | September 26, 2018 | 08:30 AM |
| | 100% | September 29, 2018 | 03:48 PM |
| | 100% | September 29, 2018 | 03:49 PM |

Figure 8. Sample intrusion report

## 4. CONCLUSION

The real-time recognition and notification of household intruders is a system developed specifically for the use of homeowners. The software used different image processing techniques. Intruder notification, through a web-based mobile application, is reported by the server in real-time. Household owners could respond by identifying if the person detected is an intruder or not. If an intruder is detected or the user did not respond at a given time, the house alarm will be activated. It is, therefore, concluded that the five image processing techniques used by the researchers are evident in recognizing the image and identifying whether the picture captured by the system is an intruder or not. The different algorithms have unique characteristics that can be highlighted in the process of giving decisions if the captured picture can be identified as an intruder or not. It is also concluded that the deep learning algorithm is the best image processing technique that can be used in face recognition because it gives a higher percentage of performance results based on the criteria evaluation.

As much as there is one algorithm used in face detection and five algorithms in facial recognition, it is recommended to search for other algorithms that can be added to the system. Since each algorithm has its unique way of detecting and recognizing a face in an image, the researchers also recommend having a stress testing of the said system to ensure the accuracy of each algorithm in a given optimal solution in recommending the best algorithm to be used by the system. Different criteria evaluations used by the researchers were effective and produced an optimal solution, it is also recommended that the criteria evaluation can be enhanced and add more criteria that focus on a larger community. It is recommended also to present the system to government agencies and private companies for mass production of the system.

## ACKNOWLEDGEMENTS

The researchers would like to thank the University of the East Graduate Studies Information and Communication Department headed by the Chair, Dr. Dennis Gonzales who provided insight and expertise that greatly assisted the research, for sharing their pearls of wisdom with us during the course of this research. We also thank the panelists who are always willing to help in the improvement of this paper.

## REFERENCES

[1] V. Prashyanusorn, P. Prashyanusorn, S. Kaviya, Y. Fujii, and P. P. Yupapin, “The use of security cameras with privacy protecting ability,” *Procedia Engineering*, vol. 8, pp. 301-307, 2011, doi: 10.1016/j.proeng.2011.03.056.

[2] A. A. Aly, S. Bin Deris, and N. Zaki, “Research Review for Digital Image Segmentation Techniques,” *International Journal of Computer Science and Information Technology*, vol. 3, no. 5, pp. 99-106, 2011, doi: 10.5121/ijcsit.2011.3509.

[3] M. S. Alkoffash, S. Alqrainy, H. Muaidi, and M. Wedyan, “A novel approach for face recognition based on a multiple faces database,” *Journal of Software Engineering and Applications*, vol. 05, no. 12, pp. 1008-1012, 2012, doi: 10.4236/jsea.2012.512116.

[4] P. Kaur and K. Kaur, "Review of Different Existing Image Mining Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 518-524, 2014, doi: 10.18517/ijaseit.10.1.10227.

[5] S. Budijono, J. Andrianto and M. N. Noor, "Design and Implementation of Modular Home Security System with Short Messaging System," in *The European Physical Journal Conferences 68, 00025*, 2014, doi: 10.1051/epjconf/20146800025.

[6] R. Surette, "The Thinking Eye," *Policing: An International Journal,* vol. 28, no. 1, pp. pp. 152-173, 2005, doi: 10.1108/13639510510581039.

[7] H. Walker and A. Tough, "Facial Comparison from CCTV footage: The competence and confidence of the jury," *Science and Justice 55,* pp. 487-498, 2015, doi: 10.1016/j.scijus.2015.04.010.

[8] C. Sanderson, A. Bigdeli, T. Shan, S. Chen, E. Berglund, and B. C. Lovell, “Intelligent CCTV for Mass Transport Security: Challenges and opportunities for video and face processing,” *Series in Machine Perception and Artificial Intelligence*, pp. 557-573, 2009, doi: 10.1142/9789812834461_0030.

[9] B. Moshiri, A. M. Khalkhali, and H. R. Momeni, “Designing a home security system using sensor data fusion with DST and DSMT methods,” *2007 10th International Conference on Information Fusion*, 2007, doi: 10.1109/icif.2007.4408192.

[10] J. Yu, F. Kong, X. Cheng, R. Hao, and J. Fan, “Intrusion-resilient identity-based signature: Security definition and construction,” *Journal of Systems and Software*, vol. 85, no. 2, pp. 382-391, 2012, doi: 10.1016/j.jss.2011.08.034.

[11] J. R. Agustina and G. Clavell, "The Impact of CCTV on Fundamental Rights and Crime Prevention Strategies: The Case of the Catalan Control Commission of Video Surveillance Devices," *Computer Law and Security Review,* pp. 168-174, 2011, doi: 10.1016/j.clsr.2011.01.006.

[12] A. Elfasakhany, J. Hernández, J. C. García, M. Reyes, and F. Martell, “Design and development of a house-mobile security system,” *Engineering*, vol. 03, no. 12, pp. 1213-1224, 2011, doi: 10.4236/eng.2011.312151.

[13] S. Reza Khan and F. Sultana Dristy, “Android based security and Home Automation System,” *The International Journal of Ambient Systems and Applications*, vol. 3, no. 1, pp. 15-24, 2015, doi: 10.5121/ijasa.2014.3102.

[14] S. Banuchitra and K. Kungumaraj, “A comprehensive survey of content-based image retrieval techniques,” *International Journal of Engineering and Computer Science*, vol. 5, no. 8, pp. 17577-17584, 2016, doi: 10.18535/ijecs/v5i8.26.

[15] M. Yang, F. Li, L. Zhang, and Z. Zhang, “Deep learning algorithm with visual impression,” *Information Processing Letters*, vol. 136, pp. 1-4, 2018, doi: 10.1016/j.ipl.2018.03.004.

[16] R. C. Richey and J. D. Klein, “Developmental research methods: Creating knowledge from instructional design and development practice,” *Journal of Computing in Higher Education,* vol. 16, no. 2, pp. 23-38, 2005, doi: 10.1007/bf02961473.

[17] S. Li, “The application of face recognition based on opencv,” *Advanced Materials Research*, vol. 403-408, pp. 2350-2353, 2011, doi: 10.4028/www.scientific.net/amr.403-408.2350.

[18] Y.-Q. Wang, “An analysis of the viola-jones face detection algorithm,” *Image Processing On Line*, vol. 4, pp. 128-148, 2014, doi: 10.5201/ipol.2014.104.

[19] P. Viola and M. J. Jones, “Robust real-time face detection,” *International Journal of Computer Vision*, vol. 57, no. 2, pp. 137-154, 2004, doi: 10.1023/b:visi.0000013087.49260.fb.

[20] F. Faux and F. Luthon, “Theory of evidence for face detection and tracking,” *International Journal of Approximate Reasoning*, vol. 53, no. 5, pp. 728-746, 2012, doi: 10.1016/j.ijar.2012.02.002.

[21] J. Ni and R. Chellappa, “Evaluation of state-of-the-art algorithms for remote face recognition,” *2010 IEEE International Conference on Image Processing*, 2010, doi: 10.1109/icip.2010.5652608.

[22] M. Çarıkçı and F. Özen, “A face recognition system based on eigenfaces method,” *Procedia Technology*, vol. 1, pp. 118-123, 2012, doi: 10.1016/j.protcy.2012.02.023.

[23] A. De, A. Saha, and M. C. Pal, “A human facial expression recognition model based on Eigen Face Approach,” *Procedia Computer Science*, vol. 45, pp. 282-289, 2015, doi: 10.1016/j.procs.2015.03.142.

[24] R. Nka, “Face recognition based on principal component analysis and linear discriminant analysis,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 4, no. 8, pp. 7266-7274, 2015, doi: 10.15662/ijareeie.2015.0408046.

[25] L. Li, X. Feng, Z. Xia, X. Jiang, and A. Hadid, “Face spoofing detection with local binary pattern network,” *Journal of Visual Communication and Image Representation*, vol. 54, pp. 182-192, 2018, doi: 10.1016/j.jvcir.2018.05.009.

[26] K. Thakar, D. Kapadia, F. Natali, and J. Sarvaiya, “Implementation and analysis of template matching for image registration on devkit-8500d,” *Optik,* vol. 130, pp. 935-944, 2017, doi: j.ijleo.2016.11.057.

[27] G. Bradski, “Learning-based computer vision with Intel’s Open-Source Computer Vision Library,” *Understanding the Platform Requirements of Emerging Enterprise Solutions*, vol. 9, no. 2, 2005, doi: 10.1535/itj.0902.03.

## BIOGRAPHIES OF AUTHORS

**Dr. Nelson C. Rodelas** is one of the proud faculty member of the College of Engineering under the Computer Engineering Department of University of the East Caloocan at the same time a faculty member of the Graduate Studies in the ICT Department of University of the East Manila. He is a graduate of Doctor of Information Technology at University of the East Manila, a Master of Science in Engineering major in Computer Engineering at Polytechnic University of the Philippines and a Bachelor of Science in Computer Engineering at University of the East Caloocan. He is also a certified Board Passer in Licensure Examination for Teachers (LET) major in Mathematics. His publication and research areas include environmental research, waste management, data analytics and deep learning.

**Dr. Melvin A. Ballera** is a graduate and one of the pioneer of Doctor of Philosophy in Computer Science in the Philippines. He is one of the Director of Research and Development at the Technological Institute of the Philippines. His publication and research areas include natural language processing, deep learning, and data analytics.