IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205039 |

Secure Deposit Vault Locker Intruder Detection System

Vaishali Sandip Gavli[1]

Lecturer, Department of Computer Engineering, Matoshri Aasrabai Polytechnic, Eklahare, Nashik, Maharashtra, India[1]

ABSTRACT:This research focuses on the configuration and implementation of the intruder detection system for a bank locker. The conventional system used such as CCTV (closed-circuit television) only records continuous movements but is unable to detect and alert when suspicious activity is happening. Banks are often considered as most secure places. People trust banks with their money and it's the bank's responsibility to keep it safe. Therefore, many banks are now trying to increase the effectiveness of their security by investing in new technology. This security system is based on human detection. The camera installed in the bank locker room will capture every person entering the room. This data is given to the FaceNet which matches the input with the dataset for detecting whether the person is an intruder or not. In a traditional security system with CCTV, the suspicious activity and intruder has to be detected manually whereas, in this system, no manual interaction is required. This system is built to deter robberies or in the worst-case scenario, this system will be able to help law enforcement to solve the crime case by providing images and shreds of evidence. The data of people visiting a bank locker will be kept in an excel sheet which will be generated automatically after scanning by webcam. It makes it easy to keep a record of people visiting a bank locker. With access to the network, the excel sheet can be monitored remotely. With these much-secured lockers, its customers will be more confident. An effective intruder detection system will help enhance a bank's security.

KEYWORDS:Intruder Detection, One-Shot Embedding, Face Detection, Face Recognition, YOLO.

I. INTRODUCTION

We know that the banking industry is growing continuously this adds a higher risk of security to the banks. Thanks to the continuously growing and updating technology, because of this we can have better security systems to protect the banks. Regardless of that, the present world of threats and thieves attacking the banking industry is not reducing nor will it slow down anytime soon. As finance is one of the most important elements for living nowadays so many vulnerabilities are being discovered daily and exploits developed towards them mostly targeting financial institutions. Traditional methodologies like only CCTV cameras and thief detection cannot work anymore thus a need for revolutionary ideas and focus when it comes to the threats in the banking security industry. In most of the projects, the main focus is on just firewalls and burglar applications to carry out tasks with default setups to detect thieves and threats. Nowadays such methods in the present Cyber Security world can be easily manipulated. So banks continuously need to redefine their security management systems by continuous monitoring methods to be able to have a wider view and knowledge of threats they deal with on day to day basis.

Our project is basically based on AI (Artificial intelligence) and IoT (Internet of Things). The aim of our project is to make the banking process seamless for the customers. There in the hardware section, we just need a webcam. The concept of the project is that when a customer wants to withdraw or deposit money in his/her account then he has to just go through the face detection security patch for his/her withdrawals or deposits. Here the idea is that a webcam will be attached to the customer's locker, when the customer wants to withdraw/deposit money he has to detect his face for his/her actions. Here the respected bank will be having the facial data of the respected customer will be linked to the respected customer's bank ID. When any customer withdraws/deposits money his/her facial data will be matched with the facial data from the bank, if the data matches then the locker will be opened. if not then another try is given to the customer and if that also fails then the account will be frozen by the bank. The photo of the intruder will be captured by

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205039 |

the webcam and this photo along with an SMS and an email is sent to the bank, the customer, and to the nearest police station. This process of freezing the account and capturing photos and sending a notification will be done within seconds. This step will help to capture the intruder faster than ever.

II. RELATED WORK

In this system the sensors are used which are deployed in the environment, a Zigbee wireless sensor module and patrolling robot which will receive a signal from the sensor after detecting some unusual activity in the environment and will arrive at the location autonomously to take pictures. These pictures after compressing will be sent to the corresponding device as an alert. The various sensors used are constituted a mesh network [1].

The author has proposed to [2] design the architecture first before developing the whole system. This home security system is developed using a Raspberry Pi module and an infrared sensor. Infrared sensors record every moment within its range i.e. 5 to 7 meters. When the movement is detected the system activates the camera and records all movements. The resulting recording is then stored in the system. For human detection the author has used HOG and SVM methods, these two methods are installed in Raspberry Pi 3. For processing the module, Raspberry Pi 3 model B is used. The signal coming from the PIR sensor is collected by Arduino. Arduino and Raspberry Pi are connected to each other by USB cable. Arduino provides the environment for all electronic devices. It also provides the true or false values to Raspberry Pi 3 in order to notify when any movement is detected. The HOG method converts the RGB image to greyscale. To calculate the square root of three RGB channels (Red, Green, and Blue) the gamma normalization is used. The pixels of the image are divided into 8x8 cells to calculate the gradient value. The next step is to determine the number of orientation binsthat are used in the histogram. The normalization of 16x16 blocks is done. Then the HOG feature vector is calculated. The resulting HOG feature is then processed by the SVM method to determine the kind of feature i.e. if it is a human feature or not.

One of the operating systems used for Raspberry Pi is Raspbian Stretch, which can be downloaded fromthe official site of Raspberry. This system operates on MicroSD of class 10 which is ofsize 32GB. After installation of the operating system, to run HOG and SVM, Python and OpenCV are required. For computer vision, the author has used OpenCV 3.3.0, opencv_contrib, and Python 3.0. The library used for webcam camera functions is a webcam. To make the photo processing quick, the resolution of pictures is kept on low purposely. There's an alarm function in Raspberry Pi 3 which supports the gpiozero-pin interface. The author has sent an email using SMTP. The configuration of the sender's and receiver's email must be done. For an internet connection, Wi-Fi is used. For dataset training, the author has used a dataset provided by OpenCV [3].

The haar algorithm is used for comparing the image with the database. While comparing the image with the database, the image that matches the input gets the highest pixel value. Harr is a predefined software in which face detection is available. It is downloadable and can be calibrated according to use. The author has used 100x130 pixels as input for face detection. In haar algorithm, the distance between features of the image such as eyes, mouth, nose, etc. is calculated for future reference [4].

The aim is to design and implement a home security system with human detection capability. We know that our old security systems like CCTV (Closed Circuit Television) are able to capture only video recording and are of not any additional use. As a reason, an additional object detection and warning method is required. The hardware used is Raspberry Pi 3 and Arduino, which is connected by a USB cable. The PIR sensor is installed on Arduino and also a webcam is mounted on Raspberry Pi 3. PIR sensor detects the movement around its cover area if any human is detected then it activates the webcam to capture a picture. The Raspberry Pi 3 works as a processor to process inputs from sensors and process images for human detection. Histogram of Oriented Gradients (HOG) and Support

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205039 |

Vector Machine (SVM) are used for human recognition and to detect suspicious objects. The alarm is activated and an email is sent to warn the house owner about the existence of the intruder if any suspicious object is detected. When tested, the results show that on average 2 seconds is required for a proposed system to detect an intruder with approximately 90% accuracy rate [5].

This paper presents [6] a system for an enclosed area(basically a home or any closed room), based on IoT also supported by Digital Image Processing, to capture any Physical Intruder who breaks into the security system and alert the rightful person regarding the intrusion. The user uses the PIR motion sensor to detect any uneven activity, if any such kind of activity is detected then with the help of Arduino the webcam is turned ON and with the help of the Face Recognition System using Digital Image Processing, recognizes whether it is the rightful person or not. If it is an Intruder, then the webcam will start recording the activity of the Intruder and send a text message along with an email to the system/house owner alerting him/her/them about the intrusion. Hadoop distributed file system is used by the system to store primary data of the intrusion. In advance, a live feed link is sentto the user which is attached to the message/e-mail. Thinking about the power consumption this Intruder Detection System is energy efficientbecause the webcam will be turned on only when the motion sensor detects any suspicious activity and during the remaining time it'll be turned off.

This security system is a flee-standing intrusion detector. There is a [7] transmitter along with a portable receiver to alert the user/owner of the house that an intrusion has occurred within a fraction of a second. The necessary area of the house is covered and monitored by an infrared detector which activates the transmitter upon the detection of differences in infrared radiation levels, also it is associated with the presence of a high-temperature body in a surrounding equilibrated environment. If any such temperature change is detected then a radio signal is emitted by the transmitter which is received by the portable hand-held remote receiver. After receiving the signal the system senses an intrusion by the reception of suspicious changes in IR levels as sensed by an IR receiving diode. [8] Once the intrusion is detected, an SCR is triggered by the IR receiving diode which supplies electrical energy activating a transmitter and a timer. The transmitter gets deactivated only once when it is reset manually. Thefirst signal, which shows that an intrusion has been detected less than a previous period of time in the past in the monitored areas, is displayed on the receiver for that preselected period of time. After the initiation of the first signal, a second signal is generated to indicate that the intrusion took place at a time more than the preselected period of time in the past and that the probability of the intruder still being present less.

III. METHODOLOGY

The system Fig. 1 is designed using YOLO V3 Face detection, FaceNet, One-shot learning, and SMTP for communication. Consider a camera installed at the door of a bank locker. Customers and bank employees are coming into the locker area. The camera will feed the live video to the YOLO model. The FaceNet has an accuracy of 98.85% and YOLO face detection has a 78% accuracy. The system takes 0.3 seconds to detect the face and match it with the database.

3.1 Face Detection:

You Only Look Once (YOLO V3) is trained on the face dataset. It will detect the face in one go through each frame and make a bounding box over it. YOLO [10]is an object detection algorithm that is used to detect multiple objects in one frame. The idea of YOLO differs from other traditional systems in that bounding box prediction and class predictions are done simultaneously. The input image is first divided into an S × S grid. Next, N bounding boxes are made in every grid cell. Confidence is the probability that an object is present in the bounding box and is defined as:

$$C = \Pr(Object) * IOU$$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205039 |

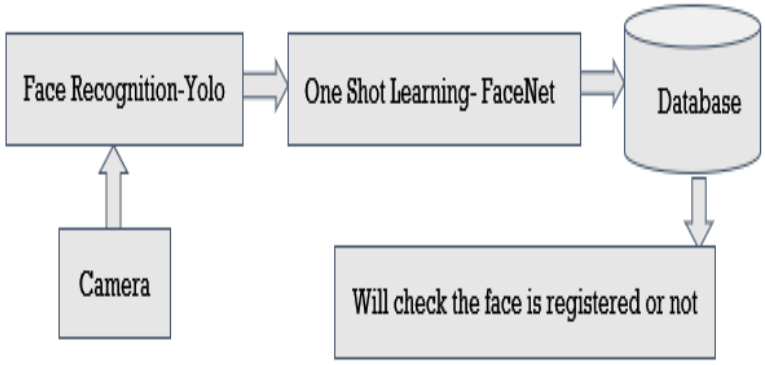

Fig. 1. System Architecture

IOU is an intersection over a union that ranges between 0 and 1. The overlapping area between the predicted box and ground truth is an intersection, and the union is the total area. According to the rule, the IOU should be near to 1, which means the predicted bounding box is near to the truth. YOLO will detect the face and create a bounding box, and we will get the x, y, height, and width of the box. This will be useful to crop the image and remove all background noise from the image. The same cropping method is used to create a database of all registered users' faces. The cropped image will be an input for FaceNet Model.

IV. EXPERIMENTAL RESULTS

4.1One-Shot Embedding

Before passing the image to the pre-trained model of FaceNet, the image is converted to an array. The array contains all the pixel values of the image (RGB). The mean and the standard deviation is calculated for the pixels, to standardize the image by using the below formula:

New pixel=(old pixel-mean)/standard deviation

Then those pixel is passed through the FaceNet model to get 128-bit face embedding. That 128-bit face embedding is a vector that contains all the features of the face detected by the pre-trained model of FaceNet. Similarly, for all images in the database 128 bit embedding is calculated using the same technique. In FaceNet architecture, the last layer is not an activation function. It is a fully connected layer that contains 128-bit embedding. It is called a Siamese Network.

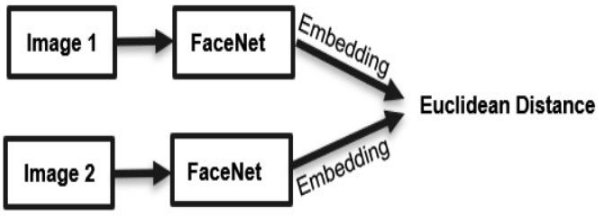

Fig. 2. FaceNet

In Fig. 2, two images are sent from FaceNet, which gives 128-bit embedding as output. Then Euclidean Distance is calculated for both embeddings that are called a degree of difference. This difference will decide whether both the images are of the same person or not. The threshold value is set to 7. If the degree of difference is less than 7, then both images are of the same person. If it's greater than 7, then both persons are different. In this way, face verification is done using One-shot learning.The benefit of one-shot learning is that there is no computation loss for training the whole model on the user dataset. We can easily add a new user to the database without training the model on it. Using one-shot learning, the system will work accurately even if the dataset has a single image of the user.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205039 |

4.2 Database and STMP

Once the face verification is done, the system will make an entry in the database i.e. in an Excel sheet. It will save the name of the user, time, and date of entry. If the user is not in the database, then the name of the user will be set to "ANONYMOUS". Also, the system will start the alarm bell and send a mail to the police, bank manager, security person, and all other stakeholders that there is an intruder in the locker area. It will send the intruder image as an attachment with the mail. For sending then mail, SMTP (Simple Mail Transfer Protocol) is used. It is a protocol that is used for sending electronic mail over the Internet. It is reliable and efficient.

V. CONCLUSION

In this paper, we have proposed a system using IoT and Machine Learning technology. For software, this system makes use of Python, NumPy, Yolo V3 model, FaceNet, and one-shot encoding. It uses a webcam in hardware. The system can detect the face of a person and then find it in a database. And it will update the excel sheet with the person's details and if the person is not found in the database, it will start the ring the alarm and will send alerts via mail. The system works very fast and efficiently. The drawback of the system is it detects one face at a time. The future scope of the research is, to detect multiple faces at a time and match them with a database. And also, to send the alert via SMS.

REFERENCES

[1] US4660024A - Dual technology intruder detection system - Google Patents

[2] NicoSurantha, Wingky R. Wicaksono, Design of Smart Home Security System using Object Recognition and PIR Sensor, Procedia Computer Science,Volume 135,2018,Pages 465-472,ISSN 1877-0509,

[3] Surantha, Nico&Wicaksono, Ridwan. (2019). An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients. Journal of Computer Science. 15. 1108-1122. 10.3844/jcssp.2019.1108.1122.

[4] Tanaya, K.Vadivukarasi, S.Krithiga "HOME SECURITY SYSTEM USING IOT" International Journal of Pure and Applied Mathematics Volume 119 No. 15 2018, pp.1863-1868

[5] More, P. R., &Gaikwad, S. Y. (2017). An Advanced Mechanism for Secure Data Sharing in Cloud Computing using Revocable Storage Identity Based Encryption. International Journal of Engineering Business Management, 1(1), 12-14.

[6] Surantha, Nico&Wicaksono, Ridwan. (2019). An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients. Journal of Computer Science. 15. 1108-1122. 10.3844/jcssp.2019.1108.1122.

[7] Kasar S., Kshirsagar V., Bokan S., Rathod N. (2020) Smart Physical Intruder Detection System for Highly Sensitive Area. In: Zhang YD., Mandal J., So-In C., Thakur N. (eds) Smart Trends in Computing and Communications. Smart Innovation, Systems and Technologies, vol 165. Springer, Singapore.

[8] US5854588A - Home security system for detecting an intrusion into a monitored area by an infrared detector - Google Patents

[9] Morea, M. P., &Sugandhib, R. (2021). A Review on Systematic Investigation of Leucocytes Identification and Classification Techniques for Microscopic Blood Smear.

[10] More, P., Ratre, S., Ligade, S., &Bhise, R. (2022, December). Design of an Efficient Approach for Performance Enhancement of COVID-19 Detection Using Auxiliary GoogLeNet by Using Chest CT Scan Images. In 2022 IEEE Bombay Section Signature Conference (IBSSC) (pp. 1-6). IEEE.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details