A Proposed System for Security Surveillance to Detect Human Intrusion

Gaayan Verma, Madhurima Hooda, Saru Dhir

Abstract**:** ***Nowadays, Security is one of the, if not the biggest priority in places such as public speaking venues, restricted areas and all important places of any country. Moreover, military conflicts & terrorism has increased recently. Monitoring these areas is substantial, but currently, monitoring is dependent upon technology and manpower. Since there is always the potential of having a human error that may be caused due to several reasons, to counter this issue, this research paper proposed an application to reduce human error. The primary feature of this application is a surveillance system that detects the face of a human, identifies the personality and display their information to possibly prevent human intrusion..***

Keywords: Human intrusion, surveillance system, security surveillance and real time security surveillance, face detection, machine learning

I. INTRODUCTION

Originally, Security surveillance is considered to monitor an area by cameras which is usually connected to a storage and watched by security guards (humans). For personal uses like in homes, the cameras are connected to recording device which records all the activities. In case of any intrusion, an alarm is raised or a notification on the mobile phone is sent. Unfortunately, it has not solved the problem of preventing human intrusion. An existing system designed projected a design of a remote embedded intelligent security monitoring system based on the background modeling algorithm [1] which can detect and determine if intrusion is occurring or not in real-time. In this system, user can log in to an application and then check the specific camera which detected the intrusion. This gave the user to have a better understanding of the situation and a sense of safety as compared to the traditional closed-circuit television (CCTV) camera systems [12].

Even though many implementations of Security surveillance for human intrusion [9,16,17,18,19] are available but these lacks in trustworthiness to the user. Another proposed system applies deep learning which is gaining popularity.

In this system, Time data mining of short part from a live feed is collected by surveillance camera by processing arcs or lines on the object of interest [2], Deep learning and Support Vector Machine (SVM) to make the Security system accurate and reliable. Deep learning countenances computational models that contains several processing layers to learn exemplifications of data with various stages of abstraction [11.13]. Neural Network models are extensively cast-off for automatic cataloguing [14]. Support vector machines also known as SVMs are supervised learning models which are used to counter classification or regression challenges [10]. A big drawback of deep learning was that it requires heavy computational cost, which was a challenge. Some researchers proposed an algorithm that require low computation power and is fast enough so it can process low-resolution frames and it can distinguish between occurrence of distinct events such as overcrowding and can operate in low-resolution video without using any classification technique [3]. This was especially useful for ATMs (Automatic Teller Machines) as these machines have low hardware capability and are usually targeted by intruders.

The proposed system not only works on further increasing the security but it helps the user to identify and fetch full information about the intruder. This is principally worthwhile in public events. The threat can be suppressed at the time of entry itself, also in hospitals, this approach would be very useful for the safety of patients.

II. PROPOSED ALGORITHM

A. Flowchart

This proposed system is a Security Surveillance System Graphical User Interface which is developed on open-cv and utilizes number of python libraries. CascadeClassifier in Open-cv is used to capture the video. Classifiers are trained by using number of similar type of objects called positive objects that are reduced to similar size to recognize faces [4] and places a rectangle on the face.

Revised Manuscript Received on November 27, 2019.

***** Correspondence Author

Mr. Gaayan Verma, B.Tech in Information Technology from Amity School of Engineering & Technology, Amity University, Noida.

Dr. Madhurima Hooda, Assistant Professor in the Discipline of Information Technology at Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida.

Dr. Saru Dhir, Ph.D in CSE, M.Tech in CS and M.Sc., Software Engineering, Agile Development, Software Testing, Cyber Crime.

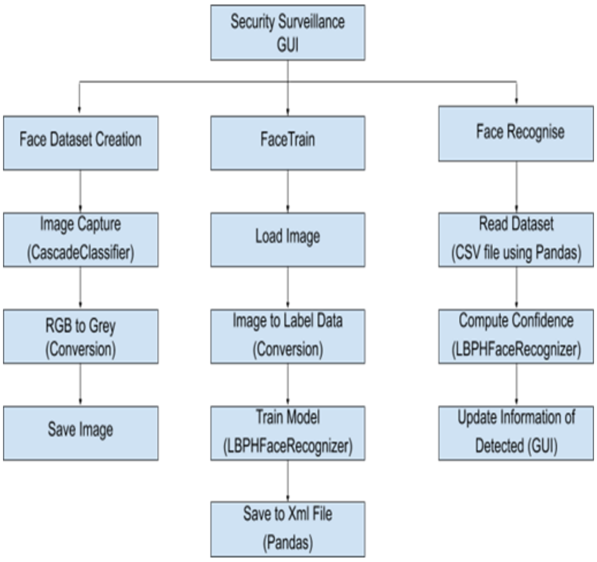

Security Surveillance GUI
Face Dataset Creation
FaceTrain
Face Recognise
Image Capture (CascadeClassifier)
Load Image
Read Dataset (CSV file using Pandas)
RGB to Grey (Conversion)
Image to Label Data (Conversion)
Compute Confidence (LBPHFaceRecognizer)
Save Image
Train Model (LBPHFaceRecognizer)
Update Information of Detected (GUI)
Save to Xml File (Pandas)

Fig. 1. Steps of face recognition of the proposed system

LBPHFaceRecognizer[2] gives a metric value which is known as confidence score. It tells how much the face is matched to faces present in dataset. (LBPH) Local Binary Patterns Histograms algorithm is originated from LBP which is very simple texture operator that marks the pixels of an image, This is done because all by thresholding the neighborhood of each pixel which combines with histograms to increase the accuracy and efficiency.

B. Real Time Security Survelliance

The interface of the projected application is very user-friendly which updates in real-time. It displays the information of the person identified by investigating the dataset and resets it to default as soon as real-time video feed is closed. It consists of three buttons namely:

1. FaceCapture- to start detecting the face. (*shown in figure 3*).

2. FaceTrain- to deal with the training of the model. (*shown in figure 4*).

3. RecogiseFace- to compare the detected face with the faces stored in the dataset.

(*shown in figure 2*).

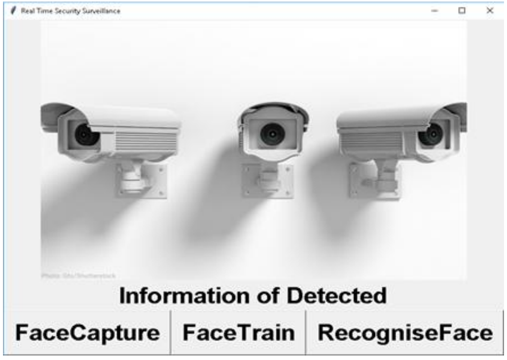


Fig. 2. Flowchart summarizing Graphical user interface of the proposed system.

C. FaceDataset Creation

When the 'Face Dataset' button is pressed the program captures 30 snap shots of all the faces detected in the video feed and saves them in greyscale. The use of grey is to increase the accuracy of the on face recognition [5] by removing the color element form the picture and focusing on the features of the face. The images saved are only the rectangle detected by CascadeClassifier. All the pictures are saved in the 'Dataset' folder which is used by the next function which is known as 'FaceTrain'.

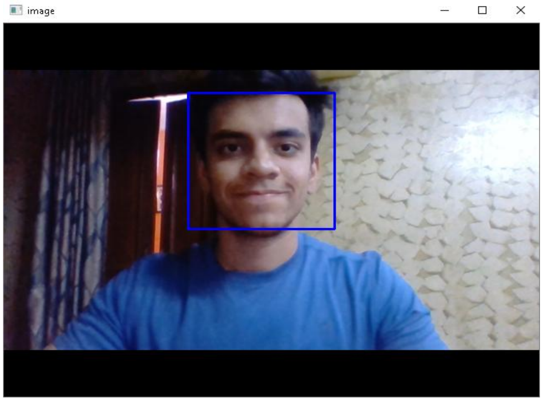
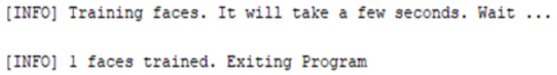


Fig. 3 (a). Face Capture feature of proposed system

D. FaceTrain

As the name says "faceTrain' deals with the training of the model. The main function of the model is to convert the GreyScale image into a numerical format (numpy array). It saves various kinds of information which are converted using CascadeClassifier such as threshold, reduced dimension in the form of a grid (usually 8x8), data which is the actual values of each pixel as a value which is used by the recognizer. All the information is saved in an XML file in the 'trainer' folder.



```
[INFO] Training faces. It will take a few seconds. Wait ...

[INFO] 1 faces trained. Exiting Program
```

E. FaceRecognise

The foundation of this function is LBPHFaceRecognizer which is used to determine how similar is the face in the live video feed to the face stored in the dataset. This is made possible by a 'confidence score', ConfidenceScore is a numeric value having a range of 0-100, It depicts the percentage of similarity the model has computed. The information of the detected face is displayed on the GUI. Also, the updates in real-time logs are also accessible in program feed.

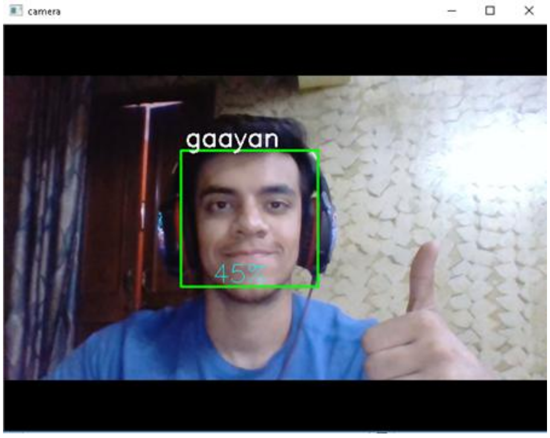


Fig. 3 (b). Face Recognition feature of proposed system

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

III. RESULTS AND DISCUSSIONS

This work has high potential as it can be implemented in many areas. For instance, implementation as a login authentication on a billing system resulting in preventing human intrusion providing convenience for the employee. Another example, in public meetings camera sensor modules can be used to identify and allow all the permitted guests to enter the premises and prevent lethal threats. This can also be used in a polling station at the time of voting allowing people who are citizens of the country and preventing false/ multiple votes. So, successfully integrating real-time face recognition [7] into a security system that identifies and displays information of the detected on the GUI has vital applications. If the identification of the person is not present in the dataset, an unknown label is set over the face which helps to determine the unknown threat. This work is very flexible in terms of adding information about the person and training the model. This concept would excel at a workplace where information of each employee is available and a database maintained for the same, also employee won't have to scan cards to enter the facility face scanners can be implemented near the doors which can scan the face, match the face with the database and open the door. This kind of technology is widely used in smartphones which gives users the convenience to crack in to the phone with just looking at the phone. The graph in figure 4 provides a visualization of number of features versus accuracy percentage of the implemented system. Figure 5 shows details of the person identfied. The details are fetched from the dataset.

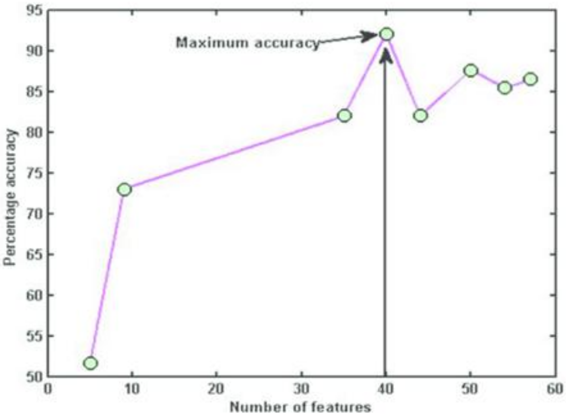
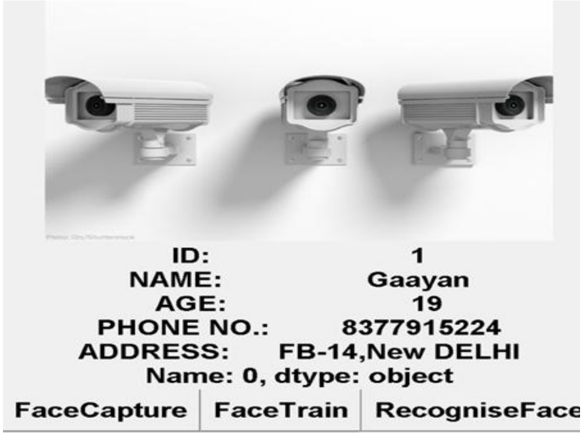


Fig 4: Graph showing number of features vs Percentage accuracy



ID: 1
NAME: Gaayan
AGE: 19
PHONE NO.: 8377915224
ADDRESS: FB-14,New DELHI
Name: 0, dtype: object

Fig 5: GUI displaying information of detected person

IV. CONCLUSION AND FUTURE WORK

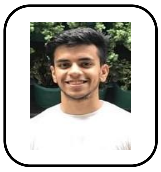
There is a lot of potential in the turf of image recognition and its various implementations. Face detection of relatively satisfactory accuracy can be achieved by adding sensors and high-resolution camera modules [8,9]. This concept is very user-friendly and reduces a lot of manpower which goes along with the current trend of automation, there is no chance for human error and it is very easy to add more features into the current system. Image recognition or machine learning [6,15] in general needs a lot of data to give viable results. This would be possible by implementing this project with the cloud which consists of an array of data that can be extracted and used to get better results. Also results with machine learning gets substantially better if it has provided with a huge amount of data.

REFERENCES

1. Landa, Jiang, Chu Jun, and Miao Jun. "Implementation of a remote real-time surveillance security system for intruder detection." 2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). IEEE, 2017.
2. Abhari, Abdolreza, Sepideh Banihashemi, and Jason Li. "Object Movement Detection by Real-Time Deep Learning for Security Surveillance Camera." 2017 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2017.
3. Rasmi, V. S., and K. R. Vinothini. "Real time unusual event detection using video surveillance system for enhancing security." 2015 Online International Conference on Green Engineering and Technologies (IC-GET). IEEE, 2015.
4. Yang, Jie, and Alexander H. Waibel. "A real-time face tracker." wacv. Vol. 94. 1996.
5. Sayem, Ibrahim Mohammad, and Mohammad Sanaullah Chowdhury. "Integrating Face Recognition Security System with the Internet of Things." 2018 International Conference on Machine Learning and Data Engineering (iCMLDE). IEEE, 2018.
6. P. J. Thilaga, B. A. Khan, A. A. Jones and N. K. Kumar, "Modern Face Recognition with Deep Learning," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp. 1947-1951.
7. Jobanputra, Mayank, et al. "Real-time face recognition in HD videos: Algorithms and framework." 2018 Annual IEEE International Systems Conference (SysCon). IEEE, 2018.
8. Cheong, Wee Lau, et al. "Building a computation savings real-time face detection and recognition system." 2010 2nd International Conference on Signal Processing Systems. Vol. 1. IEEE, 2010.
9. Das, Soubhik, and Manisha J. Nene. "A survey on types of machine learning techniques in intrusion prevention systems." 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 2017.
10. Kesavaraj, Gopalan, and Sreekumar Sukumaran. "A study on classification techniques in data mining." 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.
11. LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." nature 521.7553 (2015): 436.
12. Monika and Madhulika. “A perlustration of Human Apprehension and Behavior Accedence in surroundings” Journal of Multi Disciplinary Engineering & Technology (JMDET), vol. 8 no. 2, pp. 38-46, (2014).
13. Monika and Madhulika, “Detecting Human from Environment: Using AI for embellishing preprocessing step of Human Accedence”, International Journal of Computer Science and Technology (IJCSET), vol. 5 no. 4, pp. 76-80, (2015).
14. Monika and Madhulika "Performance Evaluation of Neural Network for Human Classification using Blob Dataset" Recent Patents on Computer Science, Bentham Science in press.
15. Chotwani, Priyal, Asmita Tiwari, and Madhurima Hooda. "Fraudulent Loan Prediction using Machine Learning Algorithms." Indian Journal of Public Health Research & Development 10.5 (2019): 845-850.
16. Saurabh Mishra, Madhurima Hooda, Saru Dhir and Alisha Sharma. iCop: A System for Mitigation of Felonious Encroachment Using GCM Push Notification, CSI-2015 50th Golden Jubilee Annual

Convention on “Digital Life”, 02nd – 05th December, 2015.
17. Madhurima, Madhulika. “Feature Based Object tracking in a video sequence using SIFT Approach”, National Conference on Emerging Technologies and Advancements in computing (NCETAC’10), Gurgaon (May 2010).
18. Hooda, Madhurima, Shashwat Pathak, and Babita Yadav. "Pervasive Security of Internet Enabled Host Services." 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE, 2017.
19. Madhurima, Madhulika. "Object tracking in a video sequence using Mean-Shift Based Approach: An Implementation using MATLAB7." IJCEM International Journal of Computational Engineering & Management 11 (2011).

AUTHORS PROFILE



Mr. Gaayan Verma is pursuing B.Tech in Information Technology from Amity School of Engineering & Technology, Amity University, Noida, Batch (2017-21). His area of interests are Machine Learning, Artificial Intelligence, Deep Learning and Data Science. He has published and presented research papers in several conferences of repute. He has filed a provisional patent titled “A system and method to analyse social credibility of a person”, Application Number E-101/71499/2019-DEL 201911032333” in the year 2019.

Dr. Madhurima Hooda is currently working as an Assistant Professor in the Discipline of Information Technology at Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida, India. She has approximately 14 years of Teaching and research experience. She has published many research papers in national and international journals and conferences of repute. She has published a book titled "Computer Networks" with Laxmi publications and contributed as an editor in global edition of the book "Absolute Java", Pearson Education. Her area of research is video object tracking, software testing, IoT, AJAX Applications and Machine learning. Her M.Tech work has been published as a book titled “Video Object Tracking” by LAP LAMBERT Academic Publishing GmbH & Co. KG, Germany. She has currently three patents and two copyrights on her name. She is an editor of Journal of Information Processing Systems (Scopus indexed). She is also a member of several professional bodies IETE, IFERP, IOAP and many more.

Dr. Saru Dhir has done her Ph.D in CSE, M.Tech in CS and M.Sc. She has more than 14 years of experience in teaching and research. Her research areas are: Software Engineering, Agile Development, Software Testing, Cyber crime. She has published many research papers in national and international journals and conferences of repute. She has completed Microsoft technology associate certification in DBA, C#, Networking and visual basic.

Retrieval Number: A10201191S19/2019©BEIESP
DOI: 10.35940/ijitee.A1020.1191S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication