INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Real time security surveillance using machine learning

G. Sumith Reddy
sumeethreddy888@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Devasani Aravind
devasaniaravind5@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

Vanama Mohith
saimohith.97@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

A. Sivajayaprakash
sivajayaprakash.a@ktr.srmuniv.ac.in
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

As we know security has become a major concern in modern society. It is achieved by surveillance which is capable of taking brisk actions. This paper presents a new system architecture which provides real-time surveillance where unauthenticated people are differentiated and provides the data flow and storage path. Recognition errors are narrowed as much as possible to make the system work efficiently. The proposed approach exploits the Viola-Jones method for face detection, the LBPH (Local Binary Pattern Histogram) algorithm as feature tracker. This combination of algorithms gives more accuracy and less processing time in the proposed design. User data is stored separately from the trained file to make the system more reliable. The proposed design can be integrated into any place which is concerned about security and prevents the security breaches before they occur.

Keywords— *Surveillance architecture, Local binary pattern histogram, Open CV, Viola-Jones*

1. INTRODUCTION

There is an immediate requirement for automated surveillance which detects unauthorized entity and alerts the administrator. Cameras are already installed across the world for surveillance but, they require the human resource to monitor. Monitoring, identifying and alerting is expected in the modern surveillance systems. In order to automate the existing surveillance system, sustainable architecture needs to be designed. This work provides system design for security surveillance in the real-time environment using facial recognition. Machine learning is the core domain of this system design. Machine Learning is a way to perform tasks without explicit coding, it uses mathematical principles and algorithms to build a model of sample data called training data using this it makes decisions or predictions. It can be used in computer vision for object detection, facial detection and also facial recognition. It does the complex task to extract information from an image and trains on the data to make predictions. Surveillance requires face detection and face recognition to determine the difference between an intruder and a registered entity. This is made possible using Viola Jones and Local Binary Pattern Histogram Algorithms of these both LBPH is a key algorithm which performs the task of facial recognition. Facial Recognition is used to identify a person from an image or video source it uses facial features to identify a person, the results may vary because of various parameters like illumination variation, low resolution, and occlusion. The results produced by facial recognition are a mostly probabilistic prediction based on known facial features provided by the system. The system is designed in such a way that the data provided for training and extracted feature after the training are secured. LBPH algorithm used in definite approach provides maximum accuracy and performance in facial recognition.

2. LITERATURE SURVEY

In Paul Viola, Michael Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features" paper author describes an approach for detection of a face in a given image. The algorithm searches for a face at different levels and discards the unwanted regions. It involves three key contributions, they are Integral image, Adaboost and Cascade. This algorithm is capable of detecting faces in an image at high rates.

Nicolas Delbiaggio, "A comparison of Facial Recognition's Algorithms" tests different facial recognition algorithms. All the algorithms are trained on the identic data set and their performance and accuracy are compared. It recommends pre-processing the dataset in order to improve recognition. This thesis also covers the whole face recognition process.

Johannes Kinzig, Christian von Harscher, "Benchmarking the LBPH Face Recognition Algorithm with OpenCV and Python" The performance limits of LBPH algorithm in combination with python and OpenCV is tested on varies

systems and described in this thesis. It also suggests that that LBPH Recognizer is suitable for real-time applications. The recognizer video stream is fluent and there were no delays in the stream.

Muhammad Naeen, Imran Qureshi, Faisal Azam, "Face Recognition Techniques and Approaches A Survey" discusses different approaches of facial recognition and provides the merits and demerits of different approaches. Holistic methods, feature-based methods, Model-based methods and Hybrid methods are few approaches discussed in this paper.

B.S.Manjunath, R.Chellappa, C.Von der Malsburg, "A Feature-Based Approach to Face Recognition" gives a detailed explanation about extracting features from pictures. Features of a human face include eyes, nose, mouth, ears etc. Features are represented using topological graphs and similar faces are identified using deterministic graph matching scheme.

Aftab Ahmed, Jiandong Guo, Fayaz Ali, Farha Deeba, Awais Ahmed, "LBPH Based Improved Face Recognition at Low Resolution" authors propose a system which operates at low resolution and can identify faces in various angles and positions.

Yogish Naik, "Detailed Survey of Different Face Recognition Approaches" provides an overview of facial recognition methodology and functions. The paper also suggests a few improvements considering the advantages and disadvantages of most recent facial recognition techniques.

Shervin Emami, Valentin Petrut Suciu, "Facial Recognition using OpenCV" created a sample application that provides insights into the facial features which are extracted. The application is developed using computer vision, OpenCV and.Net.

3. PROBLEM STATEMENT

The existing system has a post-investigation architecture where the intruder is identified after the event. The person's face needs to be cropped from the recorded video stream and searched in the database. It doesn't provide real-time surveillance where detection and recognition happen at the same time. Existing surveillance doesn't warn the security personnel with an alert message when the outbreak happens. So, continuous monitoring is required since a security breach is unpredictable. Human resource needs to be deployed for continuous monitoring. Moreover, existing systems don't provide 3 tier architecture. Considering the real-time problems and referring to the literature reviews we propose a system architecture that provides a solution to existing system problems.

4. ALGORITHMS

Viola-Jones and Local Binary Pattern Histogram algorithms are used in this paper. The accuracy and efficiency of the system can still be increased by using CNN (Convolution Neural Network).

4.1 Viola-Jones Algorithm

Viola-Jones algorithm is used to identify faces in a given image. The algorithm contains 4 components Haar features selection, Integral Image, Adaboost, and Cascade Classifier. A small fixed window traverser through the entire image and checks for Haar features in the window. Window region is discarded if haar features are not present in it.

4.2 Local Binary Pattern Histogram Algorithm

Local Binary Pattern Histogram uses a texture of an image for processing. It divides the picture into a small window. This algorithm considers 4 parameters radius, neighbor, grid X, and grid Y. All the pixels in the image are labeled according to the intensity of the picture. The local binary pattern is created based on central thresholds in the 3x3 matrix of pixels. Binaries are assigned to neighbour pixel based on threshold and concatenate these binaries in clockwise or anti clockwise and change the centre pixel intensity to the decimal value of concatenated binaries.

$$L(x_c,y_c)=\sum_{p=0}^{p-1} 2^p\, s(i_p - i_c)$$

$L(x_c, et_c)$ -→ new threshold at the central pixel, i_c --→ intensity at centre pixel, i_p -→ intensity at neighbour pixel. If the intensity of neighbour pixel is greater than the intensity of the centre pixel then set neighbour pixel to 1 else set 0.

$$s(z)=\begin{cases} 1 & if\ z \geq 0 \\ 0 & else \end{cases}$$

z represents $i_p - i_c$, if $i_p >= i_c$ then set to 1 else set to 0. We need to compare two histograms and return the one with the closest histogram. The Euclidean distance between histograms can be represented as

$$D = \sqrt{\sum_{i=1}^{n} (hist1i - hist2i)^2}$$

D -→ Distance (confidence). This formula is used by the algorithm to determine confidence and closest match to test image. If confidence is less than the algorithm is surer that it has found a match that is similar to the test image.

5. PROPOSED SYSTEM

The domain discussed in this paper is the fundamental pillar for modern day technological development. This system helps to find security breaches in real time. It uses a feature-based approach. This approach can also be replaced by a holistic or hybrid based on the requirement. The system consists of three main phases' detection, training, and recognition. Initially, images of persons are collected and labelled accordingly by an administrator and collected images are subjected to pre-processing i.e. detecting the face in the image using viola jones algorithm and converting it to grayscale because LBPH algorithm works on greyscale images. The details provided by the user is updated into the database by an administrator. The collected face datasets are stored in the local system. When it comes to security surveillance scope for error should be marginal. So, the choice of algorithm for the system also an important factor. LBPH algorithm provides more accuracy

compared to Eigenfaces and fisher faces. After the collection of datasets, the administrator trains the datasets using Local Binary Pattern Histogram [LBPH] algorithm. A .yml file is generated by an algorithm which contains facial details of the user, which can be used for facial recognition.

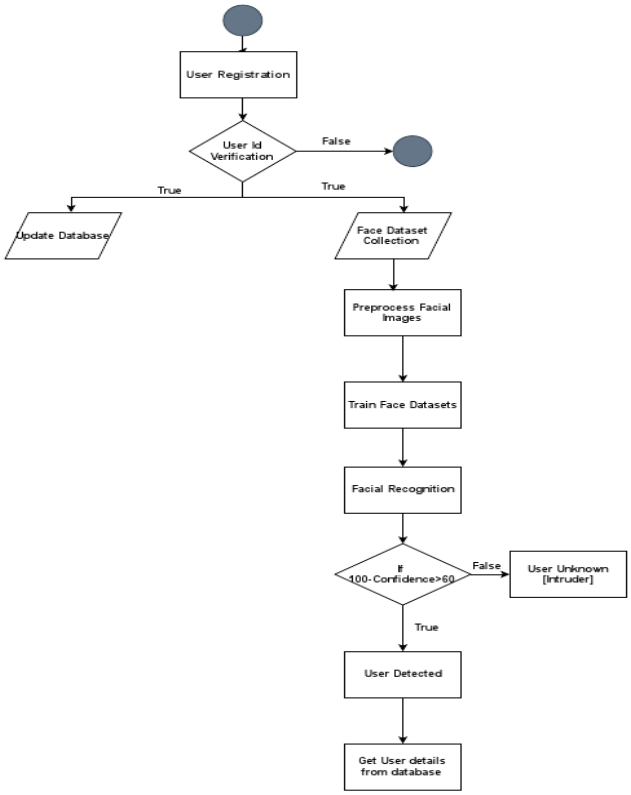

Fig. 1: Proposed system

The generated .yml file is stored in the central server which contains only user id. The corresponding name of the id is stored in the database so that even if the trained file falls into the wrong hands it cannot be used without the information which is stored in the database. Additional information such as job description, user background, criminal records, etc can also be stored. This system provides separate databases for restricted persons. This gives a warning to security when these persons try to gain access. The datasets can also be received from different sources. If a new dataset is to be added to the existing dataset, the model is trained only for the later images, since machined is trained on the previous image. The facial recognition runs in the monitoring room where the LBPH recognizer compares the raw feed against the features stored in trained file and displays authentication. The system can be integrated with GUI or webpage for making user-friendly in executing various operations. Furthermore, this system collects the time stamps of the user entering and leaving on a daily basis. This information is stored in a database and can be used later for knowing the amount of time the user spent inside. This can also be used to alert security if a user has not come out for a very long time predicting he might have some problem. But more importantly, it can be used by attendance management to know the amount of work hours spent.

6. MODULES IN ARCHITECTURE

6.1 Administration

In this module face dataset collection of users take place, it is the duty of the administrator to collect the data from the user and also to verify the documents presented by the user as proof to his identity. After verification, the administrator collects face datasets and updates user details in the database. By using this face datasets, the administrator trains a model, which can be used for recognition of the user. The trained model data is transferred to the operating system which has a face recognition program.

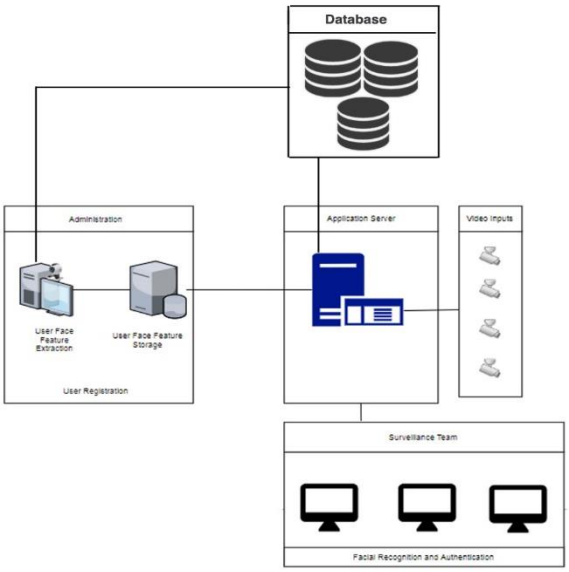

Fig. 2: Modules architecture

6.2 Database

There are two separate databases one of which is created to maintain an individual's data and time stamps of entering and exiting. The other database is external which contains criminal records of various individuals. If a certain individual has a criminal record and recognized the security would be alerted with his criminal record on the screen.

6.3 Application server

This is the place where the recognition program is executed to identify users and intruders. It receives a live feed from cameras and trained model from administrator using this recognition is performed. LBPH algorithm outcome is based on confidence so if 100-confidence>=60 then the user name is queried from a database and is labeled on the screen where the user is detected. If 100-confidence<=20 then it is labeled intruder.

6.4 Surveillance module

This module consists of an operator who monitors activities on the screen. Their duty is to alert the security team if an intruder enters the system and also to provide feedback to the development team if a wrong recognition or errors take place.

6.5 Video inputs

These are the sources from where video streams are received in real time. Video inputs can be from CCTV, Ip camera, etc.

7. CONCLUSION

Separately in the database from the training file so that information is not accessible to the public. Implementation simplicity, in-expensive computation, real-time nature and smart acquisition of facial images are some of the features of this system. This design helps to identify unauthorized users at a real time so that security breaches can be prevented. Face detection is always a challenge, especially face recognition under different lighting conditions, positions, and image depths. Good results are generated when faces gathered under reasonably varied illumination conditions, positions and angles are tested on this system. Our proposed surveillance system can

be implemented at offices, educational institutions, and different sensitive installations. Different facial positions and angles are also supported by the system. This system is flexible so that it can be changed based upon the requirement to perform different tasks. In addition, many intelligent algorithms can be included with this system to make it a more robust and error-free computer-based automatic system for surveillance.

8. REFERENCES

[1] In Paul Viola, Michael Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features", - Computer Vision and Pattern Recognition, 2001.

[2] Nicolas Delbiaggio, "A comparison of Facial Recognition's Algorithms",

[3] Johannes Kinzig, Christian von Harscher, "Benchmarking the LBPH Face Recognition Algorithm with OpenCV and Python",

[4] Muhammad Naeen, Imran Qureshi, Faisal Azam, "Face Recognition Techniques and Approaches A Survey", - Sci.Int.(Lahore),27(1),301-305,2015

[5] B.S.Manjunath, R.Chellappa, C.Von der Malsburg, "A Feature-Based Approach to Face Recognition", - Proceedings 1992 IEEE Computer Society Conference on Computer Vision and Pattern Recognition

[6] Aftab Ahmed, Jiandong Guo, Fayaz Ali, Farha Deeba, Awais Ahmed, "LBPH Based Improved Face Recognition at Low Resolution", - 2018 International Conference on Artificial Intelligence and Big Data.

[7] Yogish Naik, "Detailed Survey of Different Face Recognition Approaches", - IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1306 – 1313

[8] Shervin Emami, Valentin Petrut Suciu, "Facial Recognition using OpenCV", - Journal of Mobile, Embedded and Distributed Systems, vol. IV, no. 1, 2012.

