JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Smart Surveillance System with Face Recognition and Threat Management

Naman Bhardwaj[1], Trupti Mate[2], V V R Teja[3], Rushikesh Biradar[4]

Department of E&TC, SKNCOE, SPPU, Pune

[1]namanbhardwaj2020@gmail.com, [2]trupti.mate_skncoe@sinhgad.edu,
[3]vvrteja313@gmail.com , [4]rushibiradar8@gmail.com

Abstract— **A smart surveillance system based on face recognition and motion detection was created and planned by us. When we became aware of the limitations of the conventional CCTV camera system, we saw an opportunity to revolutionise the security industry through the proper implementation of fully automated systems that are so secure and dependable that they can be used as a stand-alone security solution in locations where security is of the utmost importance. For this, we created a system with a number of cameras, a server, gate controllers, an android application, a database, and raspberry-Pi-based bots. This project uses python libraries like OpenCV and face recognition technology. After testing it out in a variety of situations, we discovered that it works practically perfectly.**

Keywords— **OpenCV, Face recognition, Motion detection, Security, Sever, Database.**

I. INTRODUCTION

In recent years, biometric technologies have gained increasing attention as a reliable method of enhancing security in a variety of settings. Among these technologies, face recognition has emerged as a particularly promising approach due to its non-invasive and user-friendly nature. As the world becomes more connected and reliant on digital systems, the demand for secure and efficient authentication methods continues to grow. Face recognition-based security systems offer a potential solution to this challenge by providing a secure, accurate, and convenient means of identifying individuals. However, despite its potential benefits, the development and implementation of face recognition-based security systems face a number of challenges, including privacy concerns, technical limitations, and ethical considerations. In this research paper, we will explore the current state of face recognition technology, its applications in security systems, and the various challenges and limitations facing its widespread adoption. We will also examine potential solutions and future directions for research and development in this field. By doing so, we aim to contribute to the ongoing discussion about the use of biometric technologies in society, and to help inform the development of more secure and ethical face recognition-based security systems.

II. LITERATURE SURVEY

Face recognition-based security systems have gained significant attention in recent years due to their potential to enhance security in various applications. In this literature survey, we highlight some of the recent advancements in this field. One of the most significant contributions to this area is the development of deep learning-based face recognition models. Taigman et al. (2014) introduced Deep Face, a deep learning model that achieved human-level performance in face verification tasks. Since then, various deep learning models, including Parkhi et al. (2015) and Nguyen et al. (2020), have been proposed for face recognition. Another important aspect of face recognition-based security systems is their ability to handle demographic variations such as age, gender, and ethnicity. Grother et al. (2019) studied the demographic effects on face recognition systems and provided valuable insights for developing more accurate and unbiased systems. However, Buolamwini and Gebru (2018) pointed out that current face recognition systems can still exhibit intersectional accuracy disparities, which can have significant consequences in real-world applications. Apart from the above-mentioned advancements, researchers have also explored various approaches to improve the performance of face recognition systems in challenging environments. Jaiswal and Sardana (2019) proposed an efficient approach for face recognition in low-light environments, which can have significant implications for surveillance applications. In conclusion, face recognition-based security systems have come a long way in recent years, with the development of deep learning models, research on demographic effects, and advancements in handling challenging environments. However, there is still a need for further research to address issues such as accuracy disparities and to improve the overall performance of these systems.

III. PROPOSED METHODOLOGY

A. Generalised Block Diagram:

There are seven surveillance units as follows:

Patrolling bot: It is a raspberry Pi based bot which is deployed in the premises for patrolling and has its own camera for the same.

Threat detection: It is a camera aimed at the entrance gate of the premises which is supposed to detect any motion occurring in it frame.

Access control: This is the unit responsible for recognizing faces of people trying to enter and exit the premises and then control the gate for the same.

Server: It contains all the main software that runs in order to make the system work and also is the main controlling or managing unit if the system.

Database: It is where we export and store all the important information such as Entry/Exit Logs, etc.

Application: It is the mobile application used to access and control the system.

Alarm: It is used to alert the residents and the authorities in an emergency.

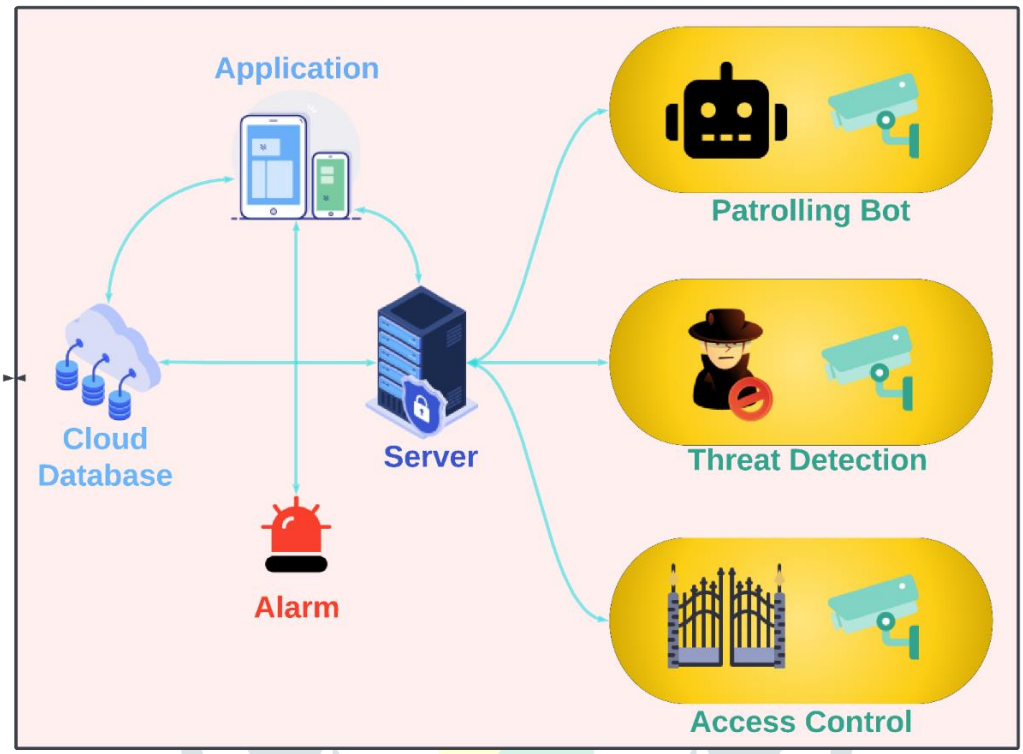

Fig.1 Block Diagram

B. WORKING:

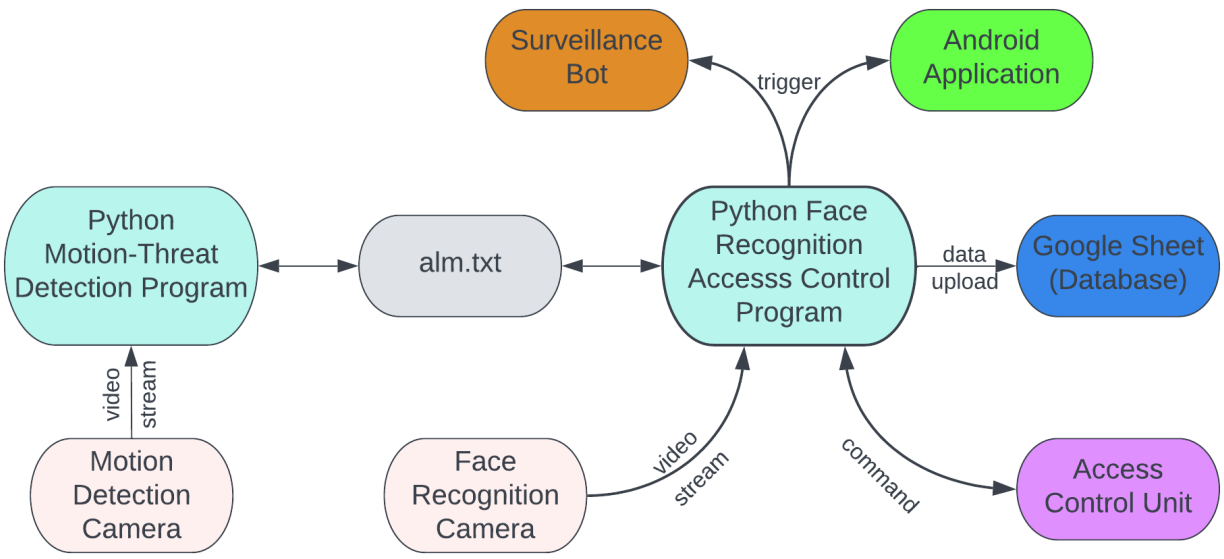

Fig.2 Hardware and software working setup

Here the Motion-Threat detection Python program and the Face Recognition Access Control Python Program are both located and running on the server. These programs are responsible for motion-Threat detection and access control respectively. These programs are responsible for controlling and managing various other elements. We achieve it by the following methods:
1. The motion-detection camera and the face-recognition camera both stream live video coverage to the server through the IP-Camera interface based on IP protocol.
2. These python programs also need to communicate with each other to allow for some basic features to run properly. We made it possible by using a text file located on the server with the name "alm.txt". The exact method will be explained in detail in the implementation section of the report.
3. The server uploads all the entry/exit log data, that it generates, to the database, which in this case is a google sheet. To do this the server makes use of the HTTPS Web Interface or protocol.
4. The server needs a way to trigger the mobile application and the surveillance bot to perform certain actions in certain situations.

C. WORKFLOW:

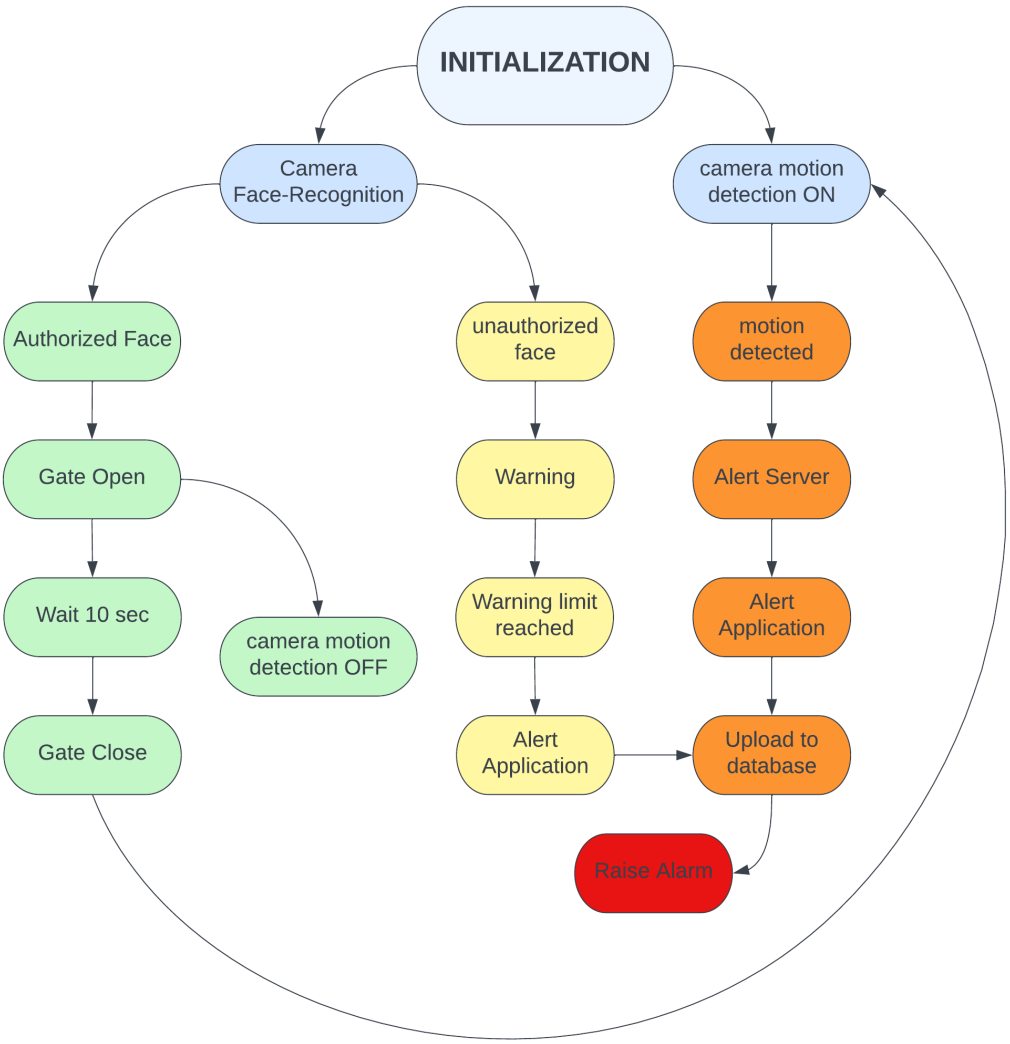

Fig.3 Workflow

As the system gets initialized the face recognition unit starts to detect faces. If the detected face is authorized, it opens the gate for a determined amount of time and also turns OFF the motion detection unit. After the mentioned time, the gate is closed and also the motion detection unit is turned back ON. But, if the detected face is unauthorized, the unit raises a warning to the person. After the limited warnings limit is reached, the unit alerts the application and then it uploads this information to the database. The motion detection unit, when turned ON, detects motion that occurs in its frame. If it detects any motion, it alerts the server and also the application and then upload this information to the database. When the app is triggered, it raises the alarm.

D. TESTING:

There are various scenarios for which our system needs to be tested. They are as follows**:**
Case 1:
Authorized person entering the premises:
Here we tested our access control unit to see how it works when an authorized person is trying to enter the premises.
As shown in the figure 123, the unit recognized the person and allowed them to enter the premises by opening the gate for them and also exported this information to the database.

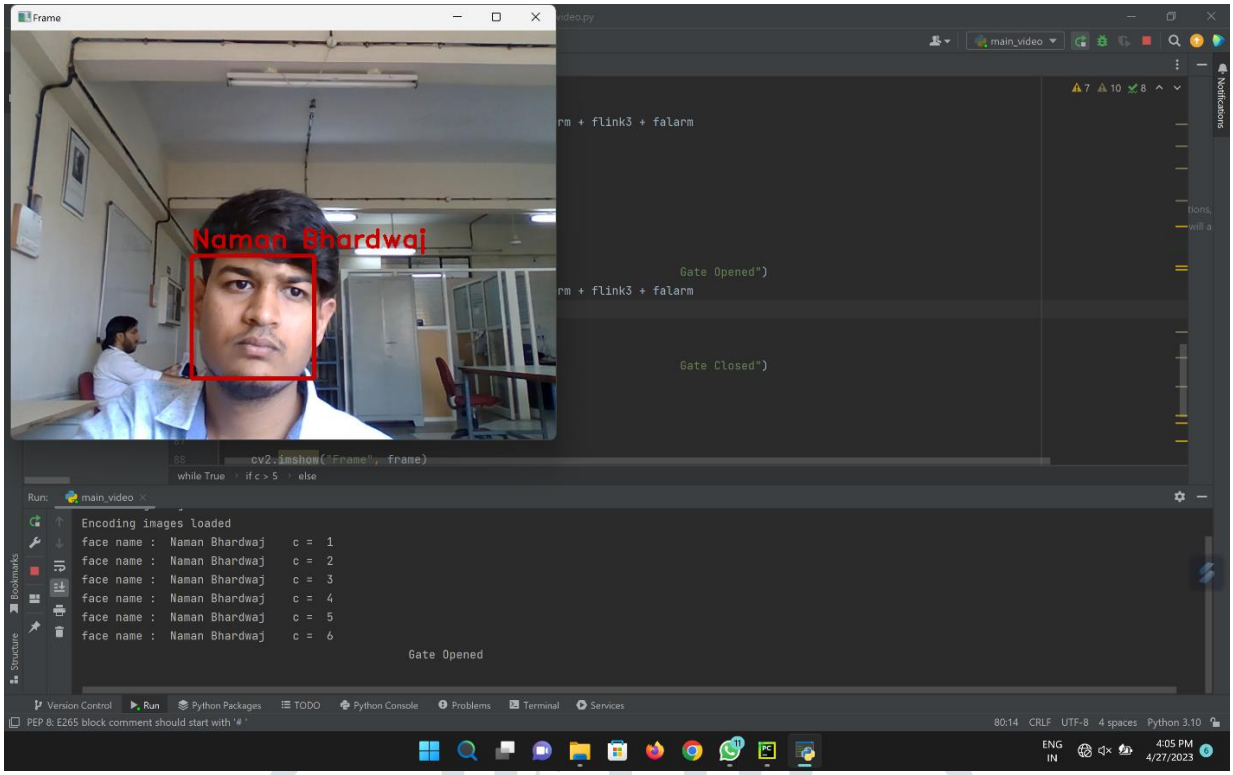

Fig.4 Simulation for Authorised person entering

Case 2:
Unauthorized person entering the premises:
Here we tested our access control unit to see how it works when an authorized person is trying to enter the premises**.** As shown in the figure 5.1.2, the unit is unable to recognize the person and denied them entry to the premises and triggered the warning. After the warning limit was reached the unit triggered the alarm and also exported this information to the database and triggered the application.

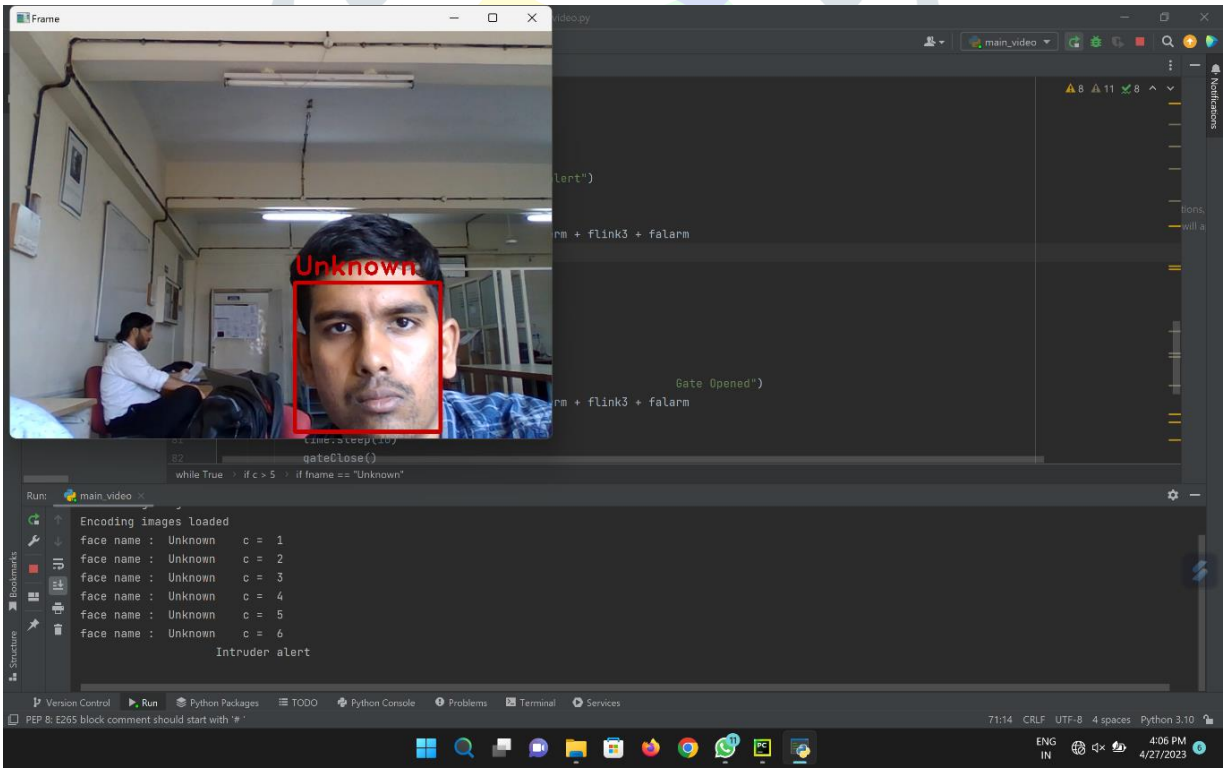

Fig.4 Simulation for unauthorised person entering

IV. Results and discussions

In this project there are main blocks that work together:

1.Face recognition program

2.Motion detection program

3.Database

4.Android application

5.Surveillance bot

6.Alarms

The face recognition software functions flawlessly. even though it does occasionally move a little slowly. The motion detecting program also functions flawlessly, but occasionally it falsely detects minute leaf movements and errant birds swooping into its field of view. Nevertheless, a few motion sensitivity changes seem to resolve the problem. The Google sheet we use as our database records all the information we provide to it via the server, and it also exports all the information to our Android application without any issues. However, one issue with it is that occasionally, for some reason unknown, it exports damaged data. While the Android app generally functions as intended, it occasionally crashes for unknown reasons. The security robot completes its task appropriately and arrives at the charging station when it is time. We are aware that there is currently a means to determine whether the bot's battery is fully charged; if this function had been included in the design, it would have been very beneficial. OpenCV is a highly powerful piece of software that we can use to accomplish a lot. But keep in mind that the software is quite power-hungry and hence uses a lot of processing resources.

V. Conclusions

We were able to design and create a smart access control security system with threat management that is very secure and dependable and can be used on security-sensitive sites like residential societies using OpenCV and numerous technologies like facial recognition and motion detection. Compared to a traditional security team, our solution is not only far more convenient and cost-effective, but also more reliable. Numerous system elements, including mobile applications, databases, servers, bots, entrance gates, and alarms, all function as intended without error and maintain residents' daily travel convenience.

Acknowledgment

It is a great pleasure to present the research paper on “Smart Surveillance System with Face Recognition and Threat Management”. We would like to convey our gratitude to our respected principal sir Dr. A.V. Deshpande, who have provided all the facilities to us. We would like to thanks our respected Head of Department Dr. S.K. Jagtap, Department of Electronics and Telecommunication for giving us support and suggestions during our project. With our deep sense of gratitude, we would like to thank our respected project guide Mrs. T.A. Mate and our respected project coordinator Mr. P.S. Kokare and Ms. M. M. Sonkhaskar (Department of Electronics and Telecommunication) for their guidance, support, valuable time and encouragement during the project. We also wish to thank all the teaching and non-teaching staff members of the Department of Electronic and Telecommunication Engineering for their valuable suggestions and support and co-operation during project.

References

[1] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L.” *DeepFace: Closing the gap to human-level performance in face verification*” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 1701-1708. (2014)

[2] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015)” *Deep face recognition*” British Machine Vision Conference, 1-12.

[3] Grother, P., Ngan, M., & Hanaoka, K.” *Face recognition vendor test (FRVT) part 3: Demographic effects*” National Institute of Standards and Technology (NIST) (2019)

[4] Buolamwini, J., & Gebru, T.” *Gender shades: Intersectional accuracy disparities in commercial gender classification*” Conference on Fairness, Accountability and Transparency, 77-91. (2018)

[5] Jaiswal, S., & Sardana, A. “*An efficient approach for face recognition in low-light environment*” International Journal of Computer Applications, 181(30), 36-42. (2019)