

IoT Based Real-Time Face Recognition and Weapon Detection Door Lock System Using Raspberry Pi

Prof. P. R. Kulkarni¹, Ishwari Thakur², Ruchika Chaudhari³, Jagruti Pawar⁴, Punam Khairnar⁵
^{1,2,3,4,5}*Sandip Institute of Engineering and Management, Computer Engineering, Nashik*

Abstract - Nowadays the number of thefts and identity fraud has become a very serious problem & A weapon is any object that can do harm to another individual or group of individuals. In order to avoid these problems of thefts and identity fraud, a face recognition & weapon detection system must be established. Smart door lock security systems have become a necessity in daily life. Security systems prevent robbery in highly secure areas such as home environments with lesser power consumption and also more reliable standalone security devices for door lock systems as well as Intruder detection. Also, nowadays, privacy and security has become an important issue in our day-to-day life. Burglary and global attacks continue to escalate, so it is exigent to find Different solutions to ensure the safety of individuals. And, to ensure safety our daily life, a lot of research is going on in the field. Security matters to this day and that is why we are up with this project of Face recognition and weapon detection systems. We are developing this project using Raspberry-pi, where a person is allowed to enter the house only if his/her face is recognized by the proposed system and he does not carry any weapons with him. This system is more reliable and effective through the point of view of security. The scope of the proposed system is to develop a security access control application based on face recognition. The haar-like features is used for face detection and face recognition. In order to achieve a system with higher accuracy and effectiveness, we use Open CV libraries and python computer language. The Training and identification by the proposed system is done in embedded device known as Raspberry Pi.

Index Terms - Artificial Intelligence, Face Recognition, IoT, Open CV, Raspberry Pi, Security, Weapon detection.

I. INTRODUCTION

In these modern days, the world changes continuously by invention of new technologies. The continuous emerging need of smart devices has evolved the concept of connecting everyday object with existing

networks. Over the past few years, there have been quite a several choices in conventional technology and biometric technology to meet security needs. Some of the traditional technologies like ‘passcode, keys, ID cards’ has disadvantages like if the key or passcode is reveled then any unauthorized person can have access. While talking about security needs there is another issue that is now a days the number of thefts and frauds are increasing. Now a days security and privacy has become an important issue in our day-to-day life. One technology that is currently trending is “Smart Door Lock System”, this technology can protect our house or offices from unauthorized access, but it cannot prevent thefts and frauds, so we have proposed a system named “IoT Based Real Time Face Recognition and Weapon Detection System Using Neural Network”. This system will not only protect us from unauthorized access but also detect weapons and protect us from threats. This system consumes less power and provide more security from burglar detection and weapons.

II. PROPOSED SYSTEM

The traditional door lock system there are many drawbacks such as sometimes the owner of the house, loses their key in such cases, in such cases there are chances that any unauthorized person can enter forcefully. If the passcode or key gets reveled to intruders, then he can get unauthorized access to house. To tackle the above issues, we have proposed this system which will help us to detect the unauthorized user and also detect any weapon. We are developing this approach using Raspberry pi, where a person is allowed to enter the house only if his/her face is recognized by system and that person does not carry any weapon with him. Image of user will be capture through webcam, the image will be compared with the

image stored in database. After face detection if the person is authorized then weapon detection will be detected, if the person does not have any weapon door will open but if the person is unauthorized or contain any harmful weapon alarm will be generated and email will be sent to owner.

III SYSTEM DESIGN

The system uses camera at the door for face recognition as access control. Also, metal detector sensors are installed at the entry points to detect the weapon inside. Sensors are employed to detect human presence. A metal detector sensor is also used to give alert if any weapon nearby is detected. The system allows entry only if authorized person like owner or person registered on the database arrives. The person may be identified through valid proof of identity. It sends a message to the owner in case it does not recognize the person within 20 seconds and the owner can monitor the activities from the camera.

1. **Face Recognition:** It is a system capable of identifying and verifying a person from the stored database. It is use for security purpose. The database of the system consists of the images of the people who are permitted in the house. This database verifies and provides access to the authorized users. If the face is not recognized by the system, then an alert message is sent to the authorized user informing the detection of intruder.
2. **Weapon Detection:** It is a system which is capable of detecting objects or weapons underneath a person's cloth. This system is developed for the purpose of security. Weapon detection is the backbone of industrial applications also. The system must have the sensors to identify the attributes of the weapons so it could easily identify it. In the proposed system if any kind of weapon is detected then an alert message is sent to the authorized user. All sensor signals are checked, and status of the system is updated continuously. In case the burglar tries to break inside, siren is activated, and alert messages are redirected to the owner.

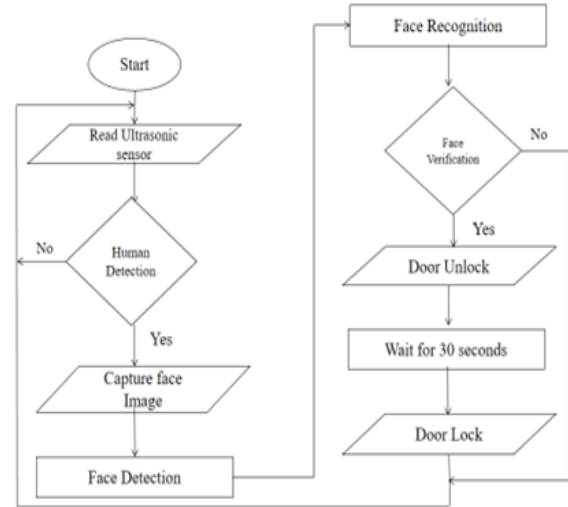


Fig. Flowchart of the system.

IV HARDWARE & SOFTWARE REQUIREMENT

System Necessity Hardware:

- R-pi 3B
- Pi-camera
- 8GB SD card
- LCD
- Servo motor
- Ultra-sonic sensor

Software:

1. Operating System: Windows XP and later versions
2. IDE: Web Based Interface.
3. Programming Language: Python.
4. Database: MySql, Oracle

Advantages:

- The software will be used for security purposes in organizations and in secured zones.
- The software stores the faces that are detected and may be used for future use as evidence.
- It grants a fast and efficient verification of an individual.
- It does not require spending additional money on its integration.
- Face recognition is used as a security tool for locking personal devices.
- Face recognition can help identify terrorists or the other criminals with the assistance of the face.

V. RESULT



Fig. Metal Detector Sensor

The system must have the metal detector sensors to identify the attributes of the weapons so it could easily identify it. In the proposed system if any kind of weapon is detected then an alert message is sent to the authorized user as well as the police.



Fig. Rpi model

In any IoT device needs at least one microcontroller device to function properly. In this system we use Raspberry Pi microcontroller for processing.



Fig. Facial Recognition Using Raspberry Pi

VI. CONCLUSION

In this proposed system we considered the problem and drawbacks of traditional door lock systems and tried to eliminate them by making a smart system. IoT

will help to control and monitor the system remotely. The use of face recognition is used for the purpose of access control and can detect the intruders. Also it helps in detecting the weapons concealed underneath the clothes of the intruder. Once the face is recognized then the Raspberry Pi helps in controlling the door access.

VII. ACKNOWLEDGMENT

The authors acknowledge the Management of Sandip Institute of Engineering and management, Nashik for providing high standard infrastructure and laboratory facilities to carry out this work.

REFERENCES

- [1] Anna Cinzia Squicciarini, Dan Lin, Smitha Sundareswaran Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites, in IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 1, 2015, pp. 193-206.
- [2] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, Privacy-aware image classification and search, in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 3544.
- [3] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, Personalized photograph rank ing and selection system, in Proc. Int. Conf. Multimedia, 2010, pp. 211220. Available: <http://doi.acm.org/10.1145/1873951.1873963>
- [4] K. Strater and H. Lipford, Strategies and struggles with privacy in an online social networking community, in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact, 2008, pp.111119
- [5] A. Acquisti and R. Gross, Imagined communities: Awareness,information sharing, and privacy on the facebook, in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006,pp. 3658.
- [6] R. Agrawal and R. Srikant, Fast algorithms for association rules in large databases, in Proc. 20th Int. Conf.
- [7] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing, in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357366.
- [8] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, Over-exposed?: Privacy

patterns and considerations in online and mobile photo sharing, in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357366.

IEEE International Conference on Intelligent Sustainable Systems, 2019.

- [9] M. Ames and M. Naaman, Why we tag: Motivations for annotation in mobile and online media, in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971980.
- [10] A. Besmer and H. Lipford, Tagged photos: Concerns, perceptions, and protections, in Proc. 27th Int.
- [11] J. Bonneau, J. Anderson, and G. Danezis, Prying data out of a social network, in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., 2009, pp.249254.
- [12] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu, and J.-L. Wu, Sheep dog: Group and tag recommendation for flickr photos by automatic search-based learning, in Proc. 16th ACM Int. Conf.
- [13] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, Connecting content to community in social media via image content, user tags and user communication, in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.12381241.
- [14] V. Schleswig-Holstein. Statistische erfassung zum internetverhalten jugendlicher und heranwachsender.
- [15] R. da Silva Torres and A. Falcao, Content-based image retrieval: Theory and applications, Revista de Informatica Teorica e Aplicada, vol. 2, no. 13, pp. 161185, 2006.
- [16] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, What does classifying more than 10,000 image categories tell us? in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp. 7184. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1888150.1888157>
- [17] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, Social circles: Tackling privacy in social networks, in Proc. Symp. Usable Privacy Security, 2008
- [18] Amit Deshwal, Mohnish Chandiramani, Umesh Jagtap, Prof. Amruta Surana, "SmartDoor Access using Facial Recognition" Volume: 3, Issue: 2, Jan-Feb 2019.1
- [19] Pallavi Raj et al., "Simulation and Performance Analysis of Feature Extraction and Matching Algorithms for Image Processing Applications",