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 HOME USING FACE RECOGNITIONAND LIVENESS DETECTION IN MACHINE LEARNING

Prof. Baliram Deshmukh
Professor , Computer EngineeringTrinity Academy of Engineering Pune, India

Khaladkar Hrushikesh
Student , Computer EngineeringTrinity Academy of Engineering Pune, India

Piske Madan
Student , Computer EngineeringTrinity Academy of Engineering Pune, India

Kolekar Vishal
Student , Computer EngineeringTrinity Academy of Engineering
Pune, India

Kurade Dipak
Student , Computer EngineeringTrinity Academy of Engineering Pune, India

***Abstract*—Ensuring the security of our lives and property is currently one of the biggest challenges facing Smart Locksystems. The use of bio-metric authentication of users attracts around the world due to their convenience and acceptance. Par- ticularly in offline settings where digital selfies and ID document facial photos are linked. In fact, comparisons of selfies with ids have also been used in some broader programs these days, such as automatic immigration control. The great difficulty of sucha process lies in limiting the differences between comparative facial images given their different origins. We propose a novel architecture for cross-domain matching problem based on deep features extracted by two well-referenced Convolutional Neural Networks (CNN). The results obtained from the data collected, called Face Data, with more than 93 percent accuracy, indicate the strength of the proposed face-to-face comparison problem and its inclusion in real time door lock security systems.**

***Index Terms*—Keywords: Convolutional Neural Networks (CNN), Smart door, Liveness detection automatic immigration control, Digital selfies, Face-to-face comparison problem.**

I. INTRODUCTION

Systems are becoming smarter as a result of the inte gration of artificial intelligence technology, and means to undermine those systems are also evolving at the same time.In particularly, it is not allowed to rely on a uni-modal system for reliable monitoring in security and surveillanceapplications. Security problems are given high priority becauseevery business owner strives to keep their homes, possessions,and workplaces as protected as they possibly could. In this way, the security does matter in everyday life. Unauthorized access by strangers is one of the main causes of securitybreach. The old door security systems made use of chains, keys & locks. However, the locks can be easily broken.The use of keys to unlock doors is not always effective since they may occasionally be used by the incorrect person, get stolen, or be copied. Then, during the learning algorithm, the single-mode system may rely on a biometrics to achieve authorization ensuring allowed access. Accuratelyidentifying the persons who want to access the entryway;however, uni-modal systems fail to achieve that benchmark. With the evolution of devices, the one thing which needsto be adapted is the pervasiveness and unobtrusive natureof acquiring biometric trait suggesting that the user should not be fatigued when requesting the authorization. Using complex features such as iris recognition and gait and signature requires users to perform certain tasks for authorization. Even with fingerprint authentication, you have to put your finger on the device to request access. Face mode is only available on security systems that match all settings. Other research is the only validation process that is flawed and can be misleading with evolutionary methods. Such as deep fakes, however, these methods are designed to fool the single-tier systems which does not comprehend to the diversified information.

II. LITERATURE SURVEY

Pan Gang et al[1] use real-time physical features to detect false images in face recognition using face mask.

This method uses only a wide-angle camera and does not require any different equipment to prevent negative attacks. Blinking is a physiological process of opening and closing the eyelids faster and more frequently per minute. The general camera captures fifteen frames per second giving 2 frames of the face used as evidence to prevent fraud attacks. Shooting 2 frames in a row is considered independent. HMM generates options from a finite state. The normal blink function uses HMM features to detect false positives. Anjos et al.planned how supported foreground or background motion correlation for checking physiological property of user. This methodology classified in motion detection. This methodologyworks on correlation between head rotation of user and its background. Authors use the correct action phrase to see the relationship. Optical flow is used to hunt out the direction of motion. This approach is easy method however need multiple frames to check physiological property, thus user ought to be co-operative. Face physiological property detection [3] has been planned to reinforce the dependability and security of face recognition system. The faux faces ar distinguished from the 000 ones exploitation totally different classification techniques. During this paper, we tend to proposeone image-based faux face detection methodology supported frequency and texture analyses for discriminating 2-D paper masks from the live faces.

For frequency analysis, we use the proposed [4] power spectrum-based method, which uses not only low frequency information but also information from high frequency domains. Also widely used is the binary model (LBP) [5]. In facial recognition, effective attack strategies can be divided into several categories. The idea of classification is to see what kind of evidence there is for facial evidence, such as stolen photos, stolen face photos, recorded videos, volunteer 3D face models, 3D face models that open and close their mouths, 3D face models with many features. language etc. [6]. The main purpose of this paper is to design and use a security door lock that supports RFID and GSM technology, which can be installed in smart buildings, secure offices and homes. The RFID reader reads the id range from passive tag and send to the microcontroller, if the id range is valid then microcontrollersend the SMS request to the documented person mobile range,for the primary countersign to open the door lock, if the personsend the countersign to the microcontroller, which may verify the passwords entered by the key board and received from documented mobile. If these 2 numbers match, the smart lock will be activated, otherwise the screw will be in position [7].

Initially, benchmarks were written as files and stored on the name server. The machine includes a camerato capture the pattern flow of user and sent for method choicesof the logic were compared and user where recognized. Initially, benchmarks were written as files and stored on the name server. Image method is used and information data input device identification is required for an additional level of security. Access system forms a vital important link during a terribly very security chain. The Fingerprint associated identification based security system given here is AN access system that enables exclusively authorized persons to access a restricted house.We used a security system that can unlock, identify and identify users, and open the door in real time to secure the door, supporting fingerprint, identification and door lock system [9]. They says perhaps the foremost very important application of correct personal identification is securing restricted access systems from ma- licious attacks. Among all the presently utilized biometrictechniques, fingerprint identification systems have receivedthe foremost attention due to the long history of fingerprints and their intensive use in forensics. This article addresses the challenge of choosing the best model for fingerprint matching, leading to the development of methods that meet the specific needs of performance and accuracy [10].

III. PROPOSED METHODOLOGY

The proposed work is carried out in different phases like im-age acquisition, feature extraction and classification as shown in Fig. 1.

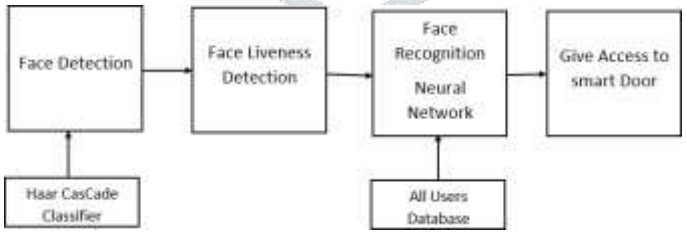


Fig. 1. Proposed System

Haar Cascade Classifier

The classifier is trained using a large number of both positive and negative images in the Haar Cascade technique, which is based on machine learning.

- Positive images - These pictures include the pictures that we want our classifier to be able to recognise.
- Negative images are pictures of everything else that don't include the thing we're trying to find.

In a detection window, a Haar-like feature takes into account adjacent rectangular sections at a certain point, adds the pixel

intensities in each sector, and then determines the difference between these sums. Subdivisions of an image are then cate- gorised using this distinction.

Algorithm

Step 1: First face is detected using haar Cascade classifier. Step 2: For face recognition first data set is created then it trained, using this dataset we recognized face.

Step 3: Then for face liveness detection we used face landmark detection database is used. In that dataset eye blinkis detected ,then we calculated aspect ratio of eye blink using eye blink value means if eye is opened what value we getand if eye is closed then what value get based that aspectratio value.

Step 4: In liveness detection three times aspect value is calculated.if eye is blinked means liveness is detected.

Step5: Then we created web application in that we checked camera live stream .finally we all merged based on camera output we face and liveness is detected .

System Architecture

that it will combine every LBP histogram for that image thenyou will get all the LBP histograms into one vector.

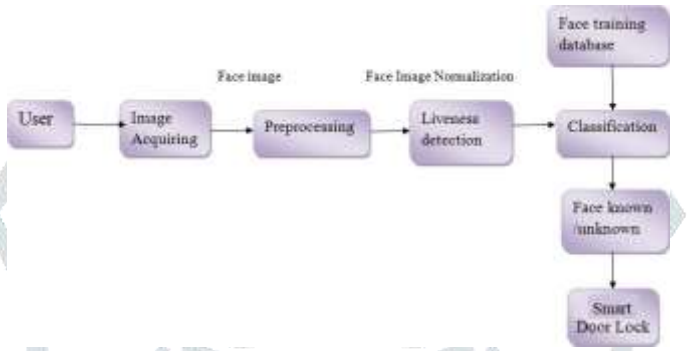


Fig. 2. System Architecture

Algorithm

Step 1: First face is detected using haar Cascade classifier. Step 2: For face recognition first data set is created then it trained, using this dataset we recognized face.

Step 3: Then for face liveness detection we used face landmark detection database is used. In that dataset eye blinkis detected, then we calculated aspect ratio of eye blink using eye blink value means if eye is opened what value we getand if eye is closed then what value get based that aspectratio value.

Step 4: In liveness detection three times aspect value is calculated if eye is blinked means liveness is detected.

Step5: Then we created web application in that we checked camera live stream finally we all merged based on camera output we face and liveness is detected.

Local Binary Patterns Histograms (LBPH)

LBP (Local Binary Pattern)

It determine the local features in the face. It operates utilising the simple LBP operator. A binary pattern code is created by comparing the values in a matrix that was initially 33 in sizeto the value of the centre pixel. By translating the binary code into a decimal one, the LBP code can be retrieved.

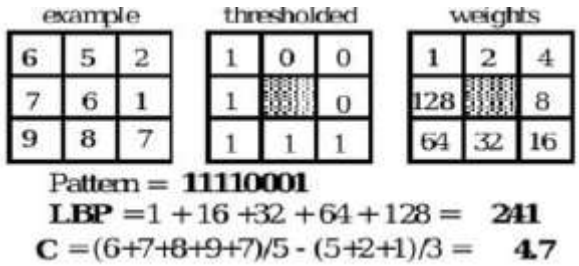


Fig. 3. Local Binary Pattern

A unique LBP code is assigned to every pixel in an image. The image will first be divided into numerous blocks. Then it will

start calculating the LBP histogram for each block after

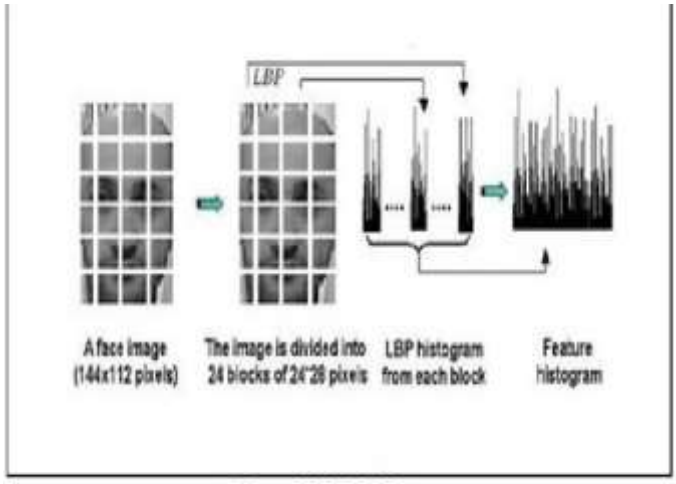


Figure 3-2-2: LBP Process

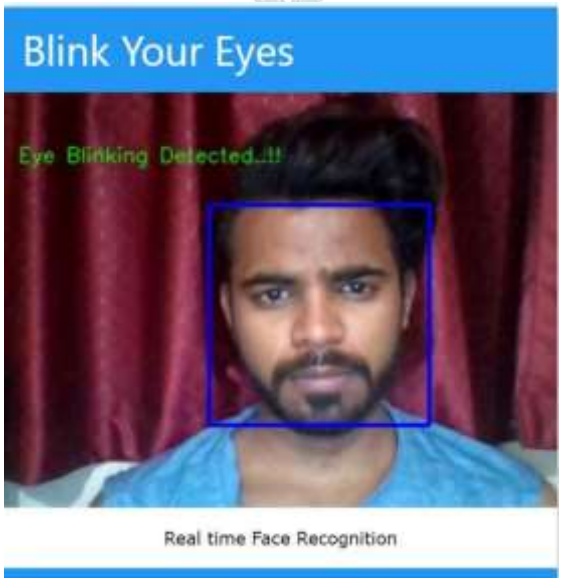
Fig. 4. LBP Process

- Capture an image then store it.
- The process will divide the image to several blocks.
- Histograms will be calculated for each block, then a histograms will be concentrated into a single vector.
- As a result, the facial recognition is represented by LBP and the shape of the face is obtained by concentrationof different local histograms.

Modules

- **Image Acquisition**: The camera will be interfaced tolocker which will be controlled by python interface.
- **Face Detection:** Facial landmarks can be used to detectface of person.
- **Face Recognition:** Neural Network can be trained torecognize faces.
- **Liveliness Detection:** Eye blink detection algorithm canbe used to detect liveliness
- **Access Control:** Finally access control is achieved basedon face liveliness Detection.

III. RESULTS



Eye Blink Detected 1

Access Granted 1

V. CONCLUSION

In this paper, we have proposed machine learning based face detection-recognition and liveness detection for smartdoor lock. In this paper user can access smart door lock by using face recognition & liveness technique. This face detecteddoor lock is much better than traditional door locks because it does not require any traditional key to unlock the locker. It is highly reliable system to ensure the security of our valuables.

VI. FUTURE WORK

1. The system must be implemented in embedded processors like raspberry pi.
2. Additional Securities can be used such as fingerprint recognition.
3. The System can be further extended to other banking services.

VII. APPLICATIONS

- It can be used as attendance system in school or college.
- Home security.
- ATM security

VIII. ACKNOWLEDGMNT

It gives us a great pleasure in presenting the report on Smarthome using face recognition and liveness detection using Machine Learning. We would like to express our special thanksof gratitude to our guide, Prof. B.B. Deshmukh, Computer Engineering Department, TAE (SPPU-PUNE) for giving us all the help and support we needed during course of the Paper writing work. We would like to thank Dr.Mukund Wagh, Head of Computer Engineering Department, TAE (SPPU- PUNE), Pune for giving us all the support and help. We would also like to thank Dr. Nilesh Uke, Principal, KJ's TrinityAcadamy of Engineering(TAE) (SPPU-PUNE) who motivatedus and created a healthy environment for us to learn in thebest possible way. We also thank all our staff members of our college for their support and guidance.

REFERENCES

[1]S. S. Sannakki, V. S. Rajpurohit, V. B. Nargund and P. Kulkarni, "Di- agnosis and classification of grape leaf diseases using neural networks", In: Fourth International Conference on Computing, Communications and Networking T echnologies (ICCCNT), pp.1-5, Tiruchengode, Tamil Nadu, 2013.
[2]Onkar Ghate, Gurunath Chavan, Krutika Dongare, Snehal Man- gale "BlueTech: A Bluetooth based Advertisement System for Mall",International Journal of Innovative Research in Computer and Communication Engineering,2017
[3]Christine Bauer and Christine Strauss "Reaching Consumers Individu- ally at the Right Place: A Literature Analysis of Location based Adver- tising on Mobile Devices ",Management Review Quarterly.66,2016

[4]T.Thiraviyam "ARTIFICIAL INTELLIGENCE MARKET-ING",International Journal of Recent Research Aspects,2018
[5]Daniel S´aez Trigueros "Face Recognition: From Traditional to Deep Learning Methods" ,arXiv,2018
[6]Tianyi Liu, Shuangsag Fang, Yuehui Zhao, Peng Wang, Jun Zhang "Im- plementation of Training Convolutional Neural Networks"arXiv,2016
[7]S. Muthuselvi and P. Prabhu "DIGITAL IMAGE PROCESSING TECH- NIQUES – A SURVEY" International Multidisciplinary Research Jour- nal,2016
[8]Erica Hokse "MOBILE LOCATION-BASED ADVERTISING",2016
[9]Srikar Appalaraju,Vineet Chaoji "Image similarity using Deep CNN and Curriculum Learning",arXiv,2017
[10]Manik Sharma, J Anuradha, H K Manne and G S C Kashyap "Facial detection using deep learning",IOP Conference Series: Materials Science and Engineering,2017
[11]Jinesh Mehta, Eshaan Ramnani, and Sanjay Singh "Face Detection and Tagging using Deep Learning",International Conference on Computer,
Communication, and Signal Processing (ICCCSP),2018
[12]Daniel Fleder and Kartik Hosanagar "Recommender Systems and their Impact on Sales Diversity",EC'07 - Proceedings of the Eighth Annual Conference on Electronic Commerce,2017
[13]Sumit Sidana "Recommendation systems for online advertis- ing",Computers and Society [cs.CY],2022