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 RECOGNITION LIVENESS DETECTION IN MACHINE LEARNING

**Asst Prof. Baliram Deshmukh [1], Madan Piske[2], Dipak Kurade[3], Vishal Kolekar[4] , Hrushikesh Khaladkar[5].**

[1,]Asst Prof Information Technology/Trinity Academy of Engineering, Pune/SPPU/India
[2,3,4,5,] Student Computer Engineering/Trinity Academy of Engineering, Pune/SPPU/India

**Abstract**

**Ensuring the security of our lives and property is currently one of the biggest challenges facing Smart Lock systems. The use of bio-metric authentication of users attracts around the world due to their convenience and acceptance. Particularly 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 such a 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.**

**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 integration 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 surveillance applications. Security problems are given high priority because every 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 security breach. The old door security systems made use of keys, locks and chains. 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 a single biometric feature may be accommodated by a uni-modal system during the shallow learning algorithm period, ensuring allowed access. Accurately identifying 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 needs to be adapted is the pervasiveness and unobtrusive nature of acquiring biometric trait suggesting that the user should not be fatigued when requesting the authorization. Using iris recognition, and complicated traits such as Gait and signature, require the user to perform some tasks which are specific to the authorization system. Even with fingerprint recognition one has to place the finger on the device to request the access. The face modality is the only trait which can be used for a security system that complies with ubiquitous characteristics. Another aspect which needs to be explored is the single-tier recognition system which results in false positives and can be spoofed with the 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

Gang Pan et al.[1] gift a spoofing against photograph in face recognition exploitation real time physiological ropertydetection exploitation spontaneous eye blinking. This methodology needs solely a generic camera no different hardware to avoid spoofing attack in nonintrusive manner. Eye blinking is physical method that in a flash opens and closes lids Again and once more in an exceedingly very minute. Generic camera captures fifteen frames per seconds, it provides 2 frames of faces that used as clue against spoofing attack. 2 captured frames in sequence ar thought-about as freelance. HMM produces options from finite state set. Typical blinking activity exploitation HMM feature finds spoofing attack. Anjos et al [2] planned how supported foreground or background motion correlation for checking physiological property of user. This methodology classified in motion detection. This methodology works on correlation between head rotation of user and its background. To go looking out correlation author uses fine grained motion direction. 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 are distinguished from the 000 ones exploitation totally different classification techniques. During this paper, we tend to propose one image-based faux face detection methodology supported frequency and texture analyses for discriminating 2-D paper masks from the live faces.

For the frequency analysis, we have got applied power spectrum primarily based methodology [4] that exploits not solely the low frequency info however conjointly the info residing among the high frequency regions. Moreover, wide used native Binary Pattern (LBP) [5]. In face recognition, the quality attack strategies may even be classified into many classes. The idea of classifying depends on what verification proof is give to face verification system, sort of a purloined picture, purloined face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with numerous expressions and so on [6]. The most goal of this paper is to vogue and implement a door lock security system supported RFID and GSM technology which could be organized in smart homes, secured 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 microcontroller send the SMS request to the documented person mobile range, for the primary countersign to open the door lock, if the person send the countersign to the microcontroller, which may verify the passwords entered by the key board and received from documented mobile. If these 2 passwords are matched the smart lock are opened otherwise it's going to be stay in bolted position[7].

Initially pattern flow unit of measurement collected as datasets and maintained in agent server. The machine includes a camera to capture the pattern flow of user and sent for method choices of the logic were compared and user where recognized. Additionally to the authentication of user there's another system to spot the user before that RFID little indefinite quantity checking is required. 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've implemented a lock security system supported fingerprint, identification ands technology containing door lockup system which might activate, proof and validate the user and unlock the door in real time for door lock secure[9]. They says perhaps the foremost very important application of correct personal identification is securing restricted access systems from malicious attacks. Among all the presently utilized biometric techniques, fingerprint identification systems have received the foremost attention due to the long history of fingerprints and their intensive use in forensics. This paper deals with the difficulty of selection of associate optimum formula for fingerprint matching thus on vogue a system that matches required specifications in performance and accuracy[10].

## III. PROPOSED METHODOLOGY

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

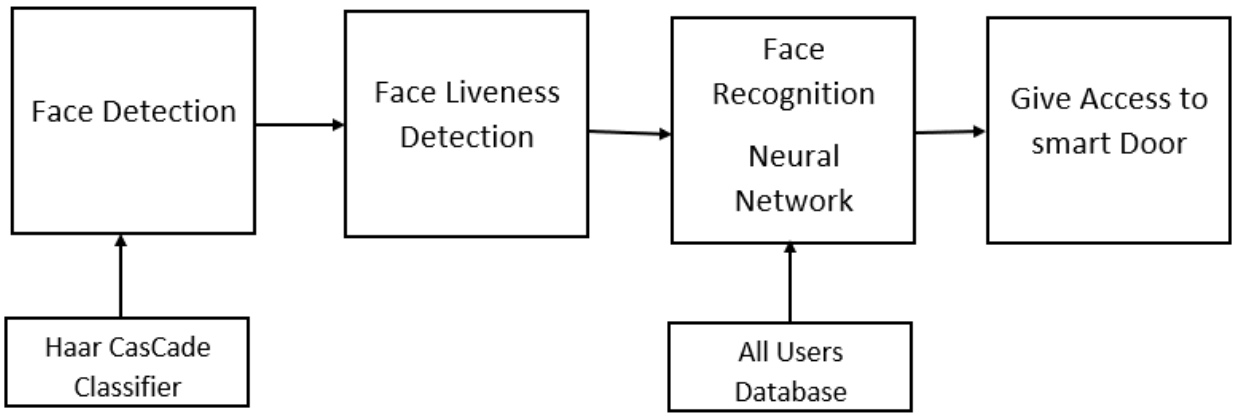


*Figure 1.Proposed System*

### 1.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 categorised using this distinction.

### 1.1Algorithm:

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 blink is detected ,then we calculated aspect ratio of eye blink using eye blink value means if eye is opened what value we get and if eye is closed then what value get based that aspect ratio 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 .

## 2.System Architecture:

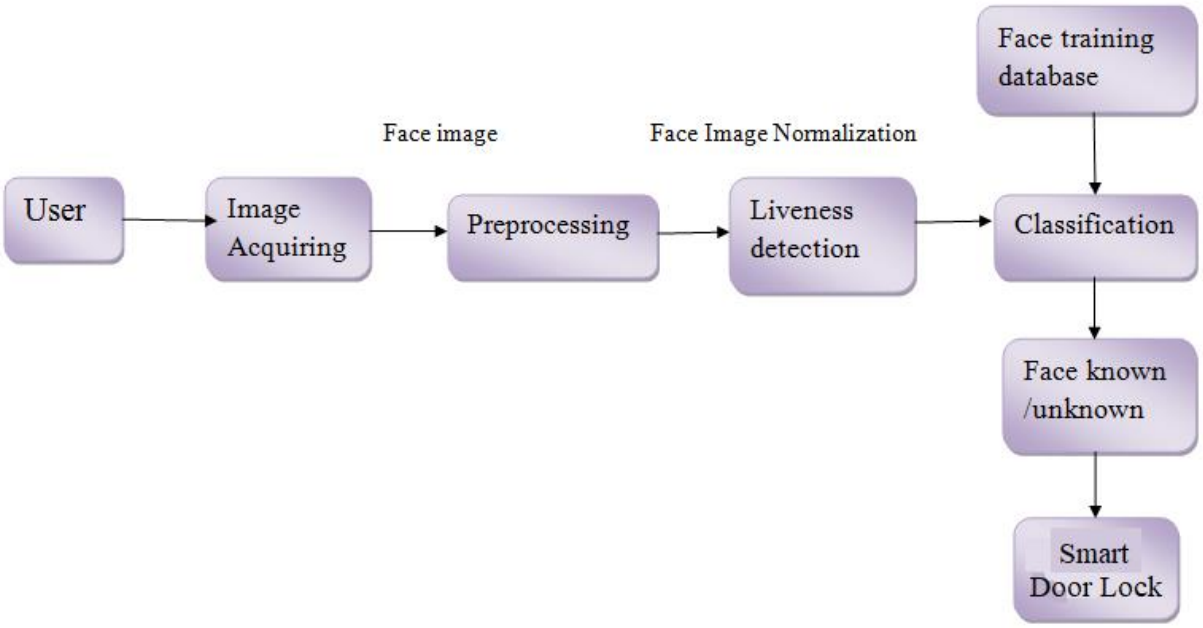


*Figure 2. System Architecture*

### 2.1Algorithm:

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 blink is detected ,then we calculated aspect ratio of eye blink using eye blink value means if eye is opened what value we get and if eye is closed then what value get based that aspect ratio 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 .

### 3.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 size to the value of the centre pixel. By translating the binary code into a decimal one, the LBP code can be retrieved.

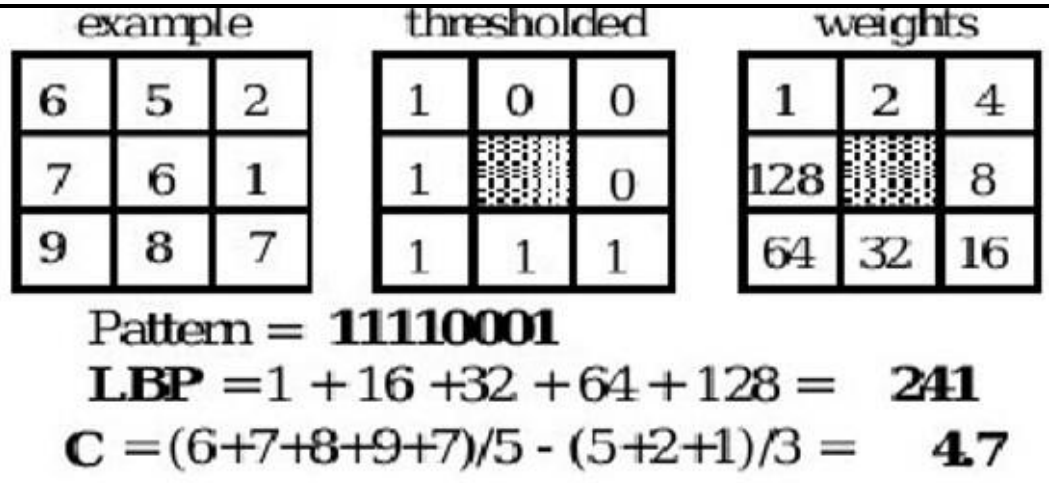


*Figure 3. Local Binary Pattern*

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

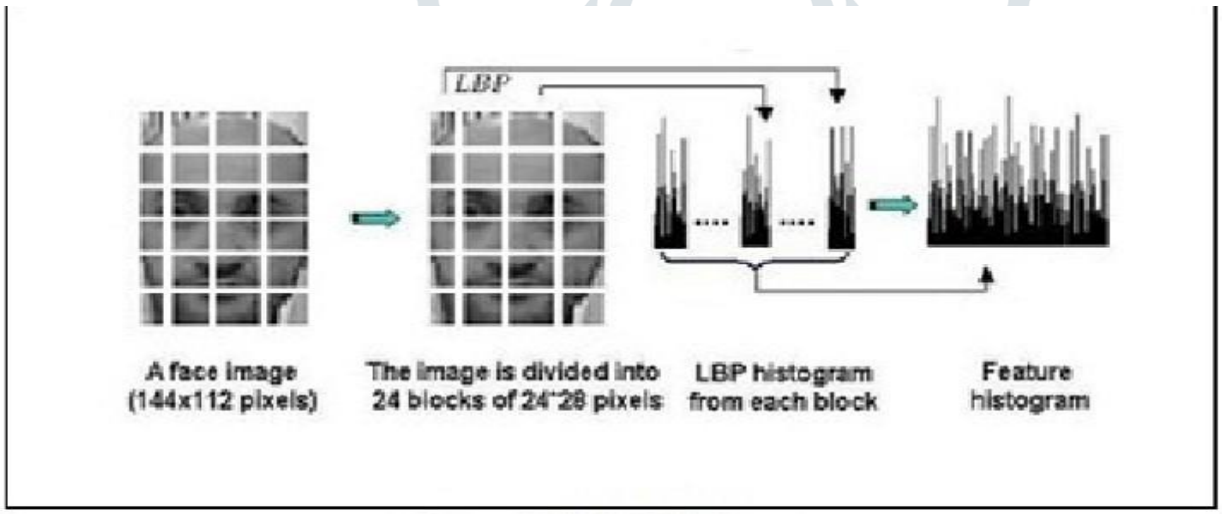


*Figure 4. LBP Process*

- 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 concentration of different local histograms.

**4.Modules:**

• **Image Acquisition**: The camera will be interfaced to locker which will be controlled by python interface.

• **Face Detection:** Facial landmarks can be used to detect face of person.

• **Face Recognition**: Neural Network can be trained to recognize faces.

• **Liveliness Detection:** Eye blink detection algorithm can be used to detect liveliness

• **Access Control**: Finally access control is achieved based on face liveliness Detection.

## IV. CONCLUSION

In this paper, we have proposed a machine learning based face detection-recognition and liveness detection for smart door lock. In this project user will use smart door lock by using face detection and liveness technique. This face detected door 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.

## ACKNOWLEDGMENT

It gives us a great pleasure in presenting the report on Smart home using face and livened detection using Machine Learning. We would like to express our special thanks of 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 B. Wagh, Head of Computer Engineering Department, TAE (SPPU-PUNE), Pune for giving us all the help and support. We would also like to thank Dr. Nilesh Uke, Principal, KJ's Trinity Acadamy of Engineering(TAE) (SPPU-PUNE) who motivated us and created a healthy environment for us to learn in the best 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, "Diagnosis and classification of grape leaf diseases using neural networks", In: Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp.1-5, Tiruchengode, Tamil Nadu, 2013.

[2] Onkar Ghate, Gurunath Chavan, Krutika Dongare, Snehal Mangale "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 Individually at the Right Place: A Literature Analysis of Location based Advertising on Mobile Devices ",Management Review Quarterly.66,2016

[4] T.Thiraviyam "ARTIFICIAL INTELLIGENCE MARKETING",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 "Implementation of Training Convolutional Neural Networks"arXiv,2016

[7] S. Muthuselvi and P. Prabhu "DIGITAL IMAGE PROCESSING TECHNIQUES – A SURVEY" International Multidisciplinary Research Journal,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 advertising",Computers and Society [cs.CY],2022