ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 2 Issue 7 July 2020

Research Article

An Innovative Approach for Face Recognition Using Raspberry pi

Srihari K[1], Ramesh R[2], Udayakumar E[3] and Gaurav Dhiman[4]*

[1]*Associate Professor, Department of CSE, SNS College of Technology, Coimbatore, Tamilnadu, India*

[2]*Department of ECE, KIT-Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamilnadu, India*

[3]*Assistant Professor, Department of ECE, KIT-Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamilnadu, India*

[4]*Assistant Professor, Department of CSE, Government Bikram college of Commerce, Patiala, India*

***Corresponding Author:** Gaurav Dhiman, Assistant Professor, Department of CSE, Government Bikram college of Commerce, Patiala, India.

Received: June 11, 2020

Published: July 30, 2020

Abstract

The Biometrics is now a days trending security method used in the industries. The Face recognition is one way of applying biometrics, and Liveness detection is the add on security to the system which will help the security system to identify between the fake and the real identities. In this case the fake identities are photographs as printed media. And mobile or tablet as display devices. The entire system is developed on the Raspberry pi board because of its efficiency with powerful architecture and the portability.

Keywords: Face Recognition; Liveness Detection; Raspberry pi; Image Quality Assessment; Eigen Face Vector and Biometrics

Introduction

The Biometrics security is the most happening security system deployed now a days in the industries. But as the technologies upgrade or evolve, the attempts are made to have a malicious attempt to gain the access. In face recognition system the face of an authorized person is added in the database in the controlled and trusted atmosphere after the complete in person inspection. Once the person is added to the database, as per the algorithm the database is processed for the system. And then whenever the face of an authorized personal pops up in front of camera, the system will provide the access. But as its know the face of a person is available now a day all over the internet because of social media or any sharing system used. As the technologies evolve so is the quality of photos or the display devices. So, in order to avoid the malicious login attempt, the Liveness Detection is introduced. The Liveness Detection basically deals with either of the following methods: Spectrum analysis, motion, head pan and image quality assessment.

The Spectrum analysis goes with distribution of spectrum on the real and the fake faces as the distribution changes for each one of them. Its observed that the distribution for the fake identities are very linear in nature, as compared with the real face. The Head pan basically deals with the gait traits of a person which is believed to be unique for person to person. The next method is about the facial motions such as blinking of the eyes of pumping of the nose and lips corner movement. The last method as per our survey is the image quality assessment. Right now nature of the picture caught is contrasted and the reference picture for the data extraction, so to execute the liveness recognition with picture quality appraisal the framework needs a database. Presently, the Face acknowledgment framework, the face acknowledgment framework is generally utilized framework accessible in the market. As per the survey done the face recognition system can be broadly classified in any one of the following:

- Knowledge based method: In this method the face of the person is subjected to encode the knowledge of human face in the set of rules. But it is difficult to make appropriate established of instructions.
- Feature invariant method: In this method different procedures try to find invariant features of the face.
- Template matching method: This method of template based approaches compares the image with stored patterns and features. But limited to face that are frontal and un-occluded.
- Appearance based method: The appearance based approaches are known to use a training pattern. But storage requirement is very high.

From the above four methods discussion we can clearly see that each method has its own merits and demerits. So while developing the system one must work with the trade-offs as per the desired system. Now, the Raspberry pi, third and the final component of the system. This computer is a low cost highly portable. To operate this low cost computer called Raspberry pi, all it need is a display device to view the system software a pair of input devices connected via USB and a power supply. The Raspberry pi is launched in two models named as raspberry and it is expected to have the new version of the pi board in market soon. The software side the raspberry pi is developed for open- source distribution, as a effect the pi board runs on Debian based Raspbian and NOOBS. But the raspberry pi also supports third party software such as UBUNTU MATE. As raspberry pi works on open source distribution it is recommended to have a proper internet connectivity [1-21].

Related work

Liveness is the demonstration of separating the component space into living and non-living. Shams will attempt to present an enormous number of caricature biometrics into the framework. With the assistance of liveness identification, the presentation of a biometric framework will improve. It is a significant and testing issue which decides the reliability of biometric framework protection from caricaturing. In face acknowledgment, the typical assault strategies might be ordered into a few classes [22]. The characterization depends on what confirmation evidence is given to confront check framework, for example, a taken photograph, taken face photographs, recorded video, 3D face models with the capacities of squinting and lip moving, 3D face models with different articulations, etc. The Anti-parody issue ought to be all around explained before face acknowledgment frameworks could be broadly applied in our everyday life. An ongoing and nonintrusive strategy dependent on the dissemination speed of a solitary picture is proposed to address the issue of face parodying utilizing photos or recordings. Specifically, the distinction in surface properties between a live face and a phony one is effectively uncovered in the dispersion speed, we abuse anti-spoofing highlights by using the aggregate variety stream plot. All the more explicitly, characterizing the nearby examples of the dissemination speed, the purported neighborhood speed designs, as the highlights, which are contribution to the straight SVM classifier is proposed to decide if the given face is phony or not. One significant preferred position of the proposed strategy is that, rather than past methodologies, it precisely recognizes various vindictive assaults paying little heed to the mechanism of the picture, e.g. paper or screen.

In addition, the proposed strategy doesn't require a particular client activity. Exploratory outcomes on different informational collections show that the proposed technique is compelling for face liveness recognition. Biometrics alludes to advancements intended for the estimation and factual examination of individuals' physical and conduct qualities and has been broadly utilized in validation frameworks. These physical and social qualities incorporate facial highlights, fingerprints, hand geometry, ear cartilage geometry, retina and iris designs, voice waves, DNA, and marks. The innovation is chiefly utilized for recognizable proof and access control, or for distinguishing people that are under reconnaissance. In any case, there are vulnerabilities present in the accessible biometric frameworks. Face Recognition frameworks can be caricature by a personality cheat, particularly the ones dependent on face acknowledgment, where the hoodlum can get a photograph of a legitimate client from a critical separation, or even acquire it from the Internet. For case, rather than demonstrating one's own face to the biometric framework, an unapproved individual can wear a copy veil or show a photograph of an approved partner either imprinted on a piece paper, on a PC, or even on a mobile phone screen [22]. The Face liveness and camouflage location framework dispose of the odds of an individual to counterfeit his/her personalities.

Method of Implementation

Face recognition system

The Face Recognition algorithm used in this system is Eigenface vector algorithm. Eigenface algorithm needs less computational requirements and it execute faster because of which it ideal for raspberry pi. Because when it comes implementation on the raspberry pi, the resources such as memory and computational power is very limited. Eigenface comes under the appearance based model where the database is generated and then the information is passed through a training model to extract a set of features vector.

Liveness detection

The liveness Detection method used in this system is created on the image quality. The system is already incorporated with the face recognition system. So, this gives us the advantage of having the pre-formed databased which is used for the face recognition. From the above talked about strategies any strategy can be actualized to remove the data with respect to the nature of the picture for the evaluation of is liveness. While testing the liveness recognition we ran over the limit an incentive to be set for discovery between the genuine and the phony face, which can be effectively seen in the outcomes got. Liveliness detection used in Face recognition.

Implementation of face recognition and liveness detection on raspberry pi

The Raspberry pi codes are executed in the python language. The execution of the system is explained in the Experiment block. The proposed system raspberry pi is used for face recognition using Eigenface algorithm

Experiment performed

The Experiment was performed in the lab with Logitech web cam as the image acquisition device, Sony Xperia Z2 mobile device was used for the display media for attempting the login attempt, and the printed photographs were used as the printed media for the malicious login attempts. First, the dataset is created for the authorized person by executing the python file created for capturing the face and storing it dynamically. The system has been restricted to single face at a time to reduce the complexity and any false alarming. Next the model is trained as per the algorithm to create a covariance matrix which is further used for the face recognition. Now, as the system is ready for the detection and recognition. The image Quality Assessment is introduced in such a way that when the face is identified in the database, it is subjected to the liveness detection before approving the access.

As it is shown in the figure 1. Once the system is initialized, a photo is captured from the image acquisition device and face detection algorithm is used, then it is given to next block for the processing or else the captured photo is discarded. Once the face is detected, then the captured photo is subjected to the Face Recognition and Liveness Detection algorithm. On successful completion of which the authentic user is identified.

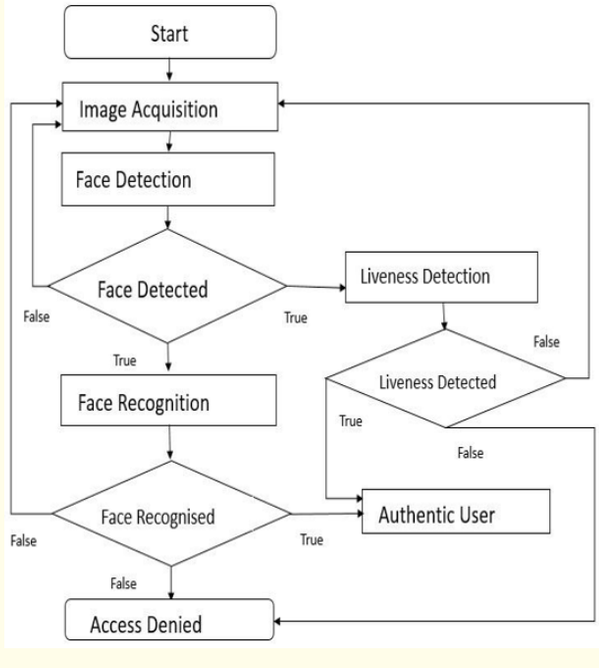

Figure 1: Flow chart of the system gives a brief idea about how the system works.

While implementing the face recognition system with eigenface algorithm the system has successfully created two folders for the database naming them as "POSITIVE" and "NEGETIVE". With the help of which it is possible to have the hierarchal level of clearance in the security system. With this facility the categories of persons coming in front of the system for the recognition can be classified into three classes:

1. First Class: This class contains the face of the persons which are authorized completely, this faces are registered in the positive faces folder which is named as "POSITIVE".
2. Second Class: This class contains the faces of the persons which can be tagged as black listed personals or restricted access. This provides the extra add-ons to the system.
3. Third Class: This class belongs to those persons who are not present in any of the database.

While implementing the system in Raspberry pi, the open source Database of AT&T lab was used to create a Negative folder. After observing the results for 10 persons the algorithm was tested for the printed media first and then the display media, Results of which are shown below.

Results and Discussion

The experiments are displayed in the figures and as it is clear from the results that the boundaries can be made clear for the Liveness Detection. And for the Face Recognition system screen shots of the output is shown. First the Obtained results for Liveness detection are as follows.

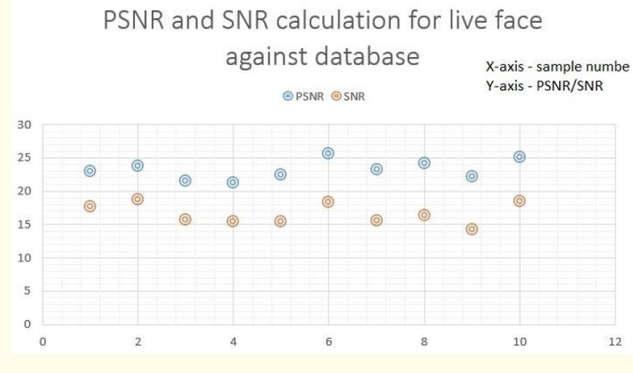

Figure 2: PSNR and SNR of live face against database.

In the figure 2 The PSNR and SNR of the live face is calculated with the reference images taken from the database.

The figure 3 shows the calculated values of PSNR and SNR of the printed media that is the photos with reference database.

Similarly figure 4 Shows the results obtained for calculating the PSNR and SNR values for the display media.

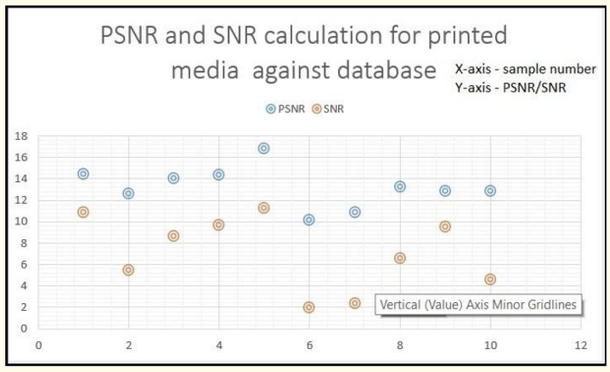

Figure 3: PSNR and SNR calculation for the Display media.

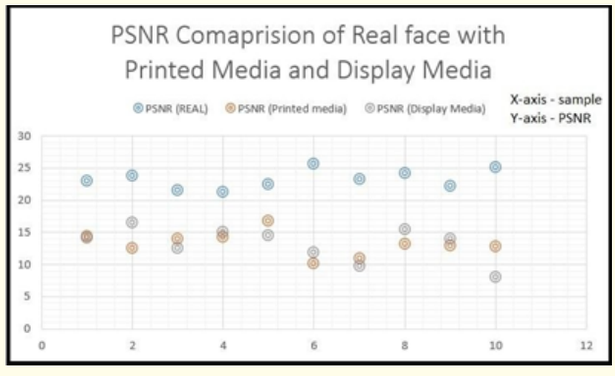

Figure 4: PSNR value comparison of the Real face with Printed media and the Display media

PSNR is used in Eigen vector selection and distance measures. After calculating the PSNR and SNR values for all the three attempts that is Real face, Printed media and the display media. The values were compared with each other for getting the clear difference between Real face and the fake attempt.

From the comparison obtained it is clearly visible that the values of the real face are clustered around the 20 to 25 units in the graph.

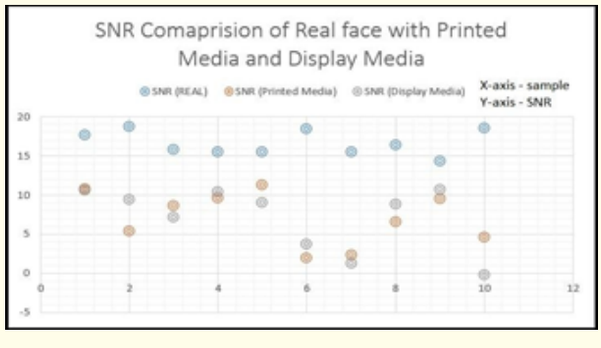

Figure 5: SNR comparison of Real face with the printed media and the display media.

The comparison method of the SNR is also similar to the PSNR method and the results shows that real face values are clearly clustered around 15 to 20 units. For all the figures from figure 2 to figure 5 X-axis displays sample quantity or the test subject displays the calculated PSNR or SNR value. Now, the results obtained for the Face Recognition system.

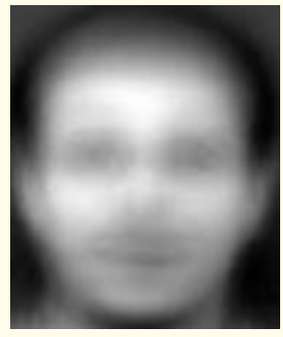

Figure 6: Mean face.

Figure 7: Positive faces.

Figure 8: Negative faces.

This are the three set of information generated by the algorithm which are then compared by the test sample to confirm the identity. Now, the screen shots taken from the output screen will give a jest information about hoe the output will be displayed. Raspberry pi is better when compared with PIC microcontroller for grater PSNR.

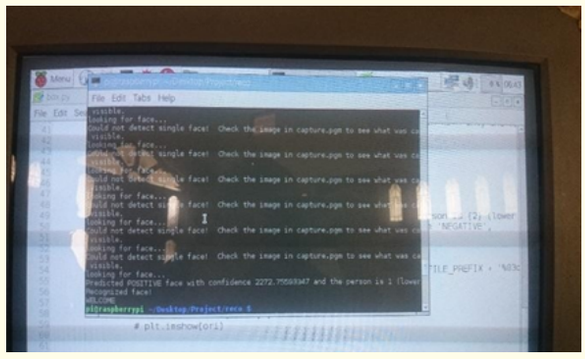

Figure 9: Display of output when face recognized.

Conclusion

This Paper are confined to the command window to reduce delay and to growth the swiftness of execution. As the scheme is in continuous loop so that once the face is recognized the process of recognition restarts, which increases the speed of overall execution. The complete system was tested on approx. 50 people. In which all of them were subjected to the custom database for the testing of Face Recognition. Then the 30 of them are were randomly selected for Liveness Detection, were their live faces were cross checked with spoof attempts either by printed media or by the display media.

Bibliography

1. Wonjun Kim., *et al.* "Face Liveness Detection from a Single Image via Diffusion Speed Model". *IEEE Trans on Image Processing* 24.8 (2015).

2. Klaus Kollreider., *et al.* "Real-Time Face Detection and Motion Analysis with Application in "Liveness" Assessment". *IEEE Transactions on Information Forensics and Security* 2.3 (2007).

3. Javier Galbally., *et al.* "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition". *IEEE Transactions on Image Processing* 23.2 (2014).

4. Diego Gragnaniello., *et al.* "An Investigation of Local Descriptors for Biometric Spoofing Detection". *IEEE Transactions on Information Forensics and Security* 10.4 (2015).

5. Z Akhtar., *et al.* "Biometric Liveness Detection: Challenges and Research Opportunities". *IEEE Security and Privacy* 13.5 (2015): 63-72.

6. SW Kim., *et al.* "Eigen directional bit-planes for robust face recognition". *IEEE Transactions on Consumer Electronics* 60.4 (2014).

7. C Liu. "The development trend of evaluating face-recognition technology". 2014 International Conference on Mechatronics and Control (ICMC), Jinzhou (2014): 1540-1544.

8. T Horiuchi and T Hada. "A complementary study for the evaluation of face recognition technology". 2013 47th International Carnahan Conference on Security Technology (ICCST) Medellin (2013): 1-5.

9. P Matthew and M Anderson. "Novel Categorisation Techniques for Liveness Detection". Next Generation Mobile Apps, Services and Technologies (NGMAST), Eighth International Conference (2014).

10. OV Komogortsev., *et al.* "Attack of Mechanical Replicas: Liveness Detection With Eye Movements". *IEEE Transactions on Information Forensics and Security* 10.4 (2015): 716-725.

11. C Gottschlich., *et al.* "Fingerprint liveness detection based on histograms of invariant gradients". *Biometrics* (2014).

12. S Tamilselvan., *et al.* "An Enhanced Face and Iris Recognition based New Generation Security System". Computing, Communications, and Cyber-Security, Lecture Notes in Networks and Systems (LNNS) series, Springer Nature 121.1 (2020): 845-855.

13. S Santhi., *et al.* "Design and Development of Smart Glucose Monitoring System". *International Journal of Pharma and Biosciences* 8.3 (2017): 631-638.

14. T Kanagaraj., *et al.* "Pressure Measurement by using ATMEGA 164 Microcontroller". *Advances in Natural and Applied Sciences, AENSI Journals* 10.13 (2016): 224-228.

15. P Vetrivelan., *et al.* "Design of Smart Surveillance Security System based on Wireless Sensor Network". *International Journal of Research Studies in Science, Engineering and Technology* 4.5 (2017): 23-26.

16. S Sivaganesan., *et al.* "Fingerprint based Watermarking using DWT and LSB Algorithm". *International Journal of Scientific Research in Multidisciplinary Studies* 5.10 (2019): 1-4.

17. Kishore Kumar., *et al.* "A Novel Multi-Angular LTP and MLDA Based Face Recognition Using Modified Feed Forward Neural Network". *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (2019).

18. S Santhi., *et al.* "Automatic Detection of Diabetic Retinopathy through Optic Disusing Morphological Methods". *Asian Journal of Pharmaceutical and Clinical Research* 10.4 (2017): 28-31.

19. Y Chen and W Zhang. "Iris Liveness Detection: A Survey". *2018 IEEE Fourth International Conference on Multimedia Big Data (BigMM), Xi'an* (2018): 1-7.

20. Balogh Zoltan., *et al.* "Motion Detection and Face Recognition using Raspberry Pi, as a Part of, the Internet of Things". *Acta Polytechnica Hungarica* 16 (2019): 167.

21. Arihant Kumar Jain., *et al.* "A Review of Face Recognition System Using Raspberry Pi in the Field of IoT". *Kalpa Publications in Engineering* 2 (2018): 7-14.

22. Piyush Devikar. "Face Liveness and Disguise Detection Using Raspberry Pi and OpenCV". *International Journal of Innovative Research in Computer and Communication Engineering* 5.1 (2017): 130-135.