Image Quality Assessment for Fake Biometric Detection: Application To Face and Fingerprint Recognition

Prof.R.A.Jamadar[1], Shruti Ghorpade[2], Dhanashri Gund[3], Swapnada Kadam[4]

Information Technology Department, Savitribai Phule Pune University
AISSMS IOIT,Pune 01

Abstract- *Security is major concern for today's scenario. A high level industry uses passwords like thumb, face, voice, iris, etc. So many security systems are available. But not so reliable. So we have implemented two stage security system which is very precise and reliable. The system has two stages which is embedded system. Even if any stage is cracked falsely, unauthorized entry will be detected.Liveness detection methods are usually classified into two techniques. First is a Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself). and second is a Hardware-based techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure).The thumb samples are stored in the sensor If there is a fake samples which does not match with the stored samples (i.e.Face,Fingerprint) then the buzzer will beep continuously.*

Keywords- *PCB, AVR, Camera, PCA, Buzzer, LCD, etc.*

I. INTRODUCTION

Fake Biometric Detection Application is developed to ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protective measures. The objective of this system is to develop a system to enhance the security of biometric recognition framework, by providing a two stage security using finger print and face detection applications. To design and implement a system that provides double security against the fake biometric scanning of face or fingerprint using two stages for confirmation that the user who gets access to the system is authorized.

The system is divided into the following modules:

1) PC (JAVA)
2) Microcontroller- ATmegA16 from AVR
3) Buzzer- DC 5V
4) Fingerprint
5) Camera

The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric"). The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack") The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios; in addition to its very competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the proposed method presents some other very attractive features, all of them very desirable properties in a practical protection system.

II. SPECIFICATIONS OF THE SYSTEM

1. Fake Biometric Detection application offers to provide a double security to your system.

2. First the camera will capture the face and using USB it will be displayed on the LCD and transferred to the microcontroller and the buzzer will buzz if the face is unauthorized.

3. In the next stage the finger print of the user will be taken if the user is authorized and then further the user's fingerprint will be checked for confirmation.

III. PROPOSED WORK

System will have two stages which is used embedded system. Even if any stage is cracked falsely, unauthorized entry will be detected or the buzzer will beep. First stage will be face recognition. Authorized faces will saved in database. As anyone try to enter in vehicle, first he/she have to go through this stage. Whoever accesses this system, it will save profile of that person with date and time in database. If authorized face is recognized, system will check for iris. If iris test is passed then it will check face length, nose length, height and width of face, face color. If that person is authorized person then it go for next stage that is fingerprint test. User has to access fingerprint. Authorized fingers will be in database which is a sensor if matched it will give OK signal, else buzzer will beep continuously.

IV. ALGORITHM

- **PCA(Principle Component Analysis) Algorithm:**
  Look at the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images.

- **Eigen faces Algorithm:**

1. Calculate a set of weights based on the input image and the M Eigen faces by projecting the input image onto each of the Eigen faces.

2. Determine if the image is a face at all by checking to see if the image is sufficiently close to "face space."

3. If it is a face, classify the weight pattern as either a known person or as unknown.

4. (Optional) Update the Eigen faces and/or weight patterns

V. SYSTEM ARCHITECTURE DIAGRAM

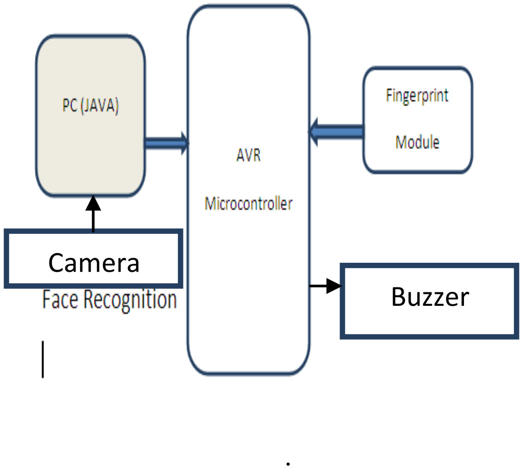

FIG.1. SYSTEM ARCHITECTURE DIAGRAM

fake biometric detection application offers to provide a double security to your system. the system use software and hardware part so this is embedded system. the authenticated face and fingerprints are stored in databases with the standard sensor. first the camera will capture the face and using usb it will be displayed on the lcd and transferred to the microcontroller and the buzzer will buzz if the face is unauthorized. in the next stage the finger print of the user will be taken if the user is authorized and then further the user's fingerprint will be checked for confirmation. if the fingerprint does not match with the stored database then the buzzer will beep continuously. so, if the first system will cracked falsely then the next stage will detected the unauthorized person automatically.

VI. CONCLUSION

Many frauds are happening with industries even if there is security. The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. This interest has lead to big advances in the field of security-enhancing technologies for biometric-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task.So its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose two of the most extended image-based biometric modalities have been considered in the experiments: fingerprints and 2D face. Second, evaluate the “multi-attack” dimension of the protection method. That is, its ability to detect not only spoofing attacks (such as other aliveness detection-specific Approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples.

ACKNOWLEDGMENT

This project is being executed by our group under the guidance of Prof Mr. R.A. Jamadar Sir. Also we are thankful to the lab assistant of the Computer lab in IT department and embedded lab in E&TC department of AISSMS IOIT,pune-01.

REFERENCES

A. For journal:

[1] R. Soundararajan and A. C. Bovik, “RRED indices: Reduced referenceentropic differencing for image quality assessment,” *IEEE Trans. ImageProcess.*, vol. 21, no. 2, pp. 517–526, Feb. 2012.

[2] M. G. Martini, C. T. Hewage, and B. Villarini, “Image quality assessment based on edge preservation,” *Signal Process., Image Commun.*, vol. 27, no. 8, pp. 875–882, 2012.

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” *Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.

[4] J. Zhu and N. Wang, “Image quality assessment by visual gradient similarity,” *IEEE Trans. Image Process.*, vol. 21, no. 3, pp. 919–933,Mar. 2012.

[5] Altered Fingerprints: Analysis and Detection Soweon Yoon, Student Member, IEEE, Jianjiang Feng, Member, IEEE, and Anil K. Jain, Fellow, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 34, NO. 3, MARCH 2012

B. For Book:

1.Basic for AVR microcontrollers – Nebojsa Matic.

2.Microcontroller Programming The Microchip AVR® -Julio Sanchez.

3. AVR Assembly Language for the Complete Begin -Michael A. Covington.

C. For Web sites:

1. http://en.wikipedia.org/wiki/Sevensegment_display
2. http://www.gsm-modem.de
3. http://www.datasheetsite.com/datasheet/MAX232
4. http://www.rentron.com/rf_remote_control.html
5. http://www.atmel.com/dyn/resources/prod_documents/doc0401.pdf