A Novel Detection of Fingerprint spoofing using Biometrics

MS. REPAKULA DURGA PRANUSHA[1], K. RAJESH[2] & MR. N.CHANDRASHEKHAR[3]

[1]M-Tech Dept of ECE Khammam Institute of Technology and Sciences, Khammam.

[2]Associate Professor Dept of ECE Khammam Institute of Technology and Sciences, Khammam.

[3]Associate Professor& HOD Dept of ECE Khammam Institute of Technology and Sciences, Khammam.

Abstract

In biometrics, Fingerprint is widely used in identification of individual's identity. Biometric recognition is leading technology for identification and security systems. Fingerprint has unique identification among all other biometric modalities. Use of the fingerprints as biometric characteristics is extensively used and developed for fingerprint recognition in forensic, civilian and commercial applications. This paper presents the brief data about fingerprint spoofing which encompasses misuse caused by the attackers. Fingerprint spoofing detection attributes to the investigation of the finger characteristics to ensure whether the finger is spoofed or live. The various spoofing types are explained and there detection techniques are introduced with three commonly used databases.

Keywords: - Biometrics, Fingerprint spoofing, Detection, databases.

1. INTRODUCTION

Biometrics technology is an automated recognition system which enables the authentication of individual based on biological and behavioral characteristics such as face ,iris ,gait ,voice ,fingerprints etc. Biometric methods are supposed to be a set of secure methods for identification and authentication of an individual as it has makeable advantages as compared with other methods. But at the same time biometric systems may be vulnerable to attacks, at each level such as biometric sensor level, data communication, database etc. These systems are not totally spoof proof. Recently, some studies summarized the possibility of spoofing recognition systems by artificial biometric samples such as fake fingerprints, artificial iris, facemask etc. Fingerprint Identification system is becoming a commonly used biometric technique with authentication, security, safety and many other vigilance system. Unlike other biometric traits such as iris, face, palm, etc., fingerprint identification is a most commonly used technique due to unique characteristics of fingerprint of every individual. This feature makes it most reliable and preferred method amongst other techniques [6].Due to its wide spread use, researchers have analyzed, the competitive attacks on the fingerprint identification systems including fingerprint "Impersonation". What is Impersonation?-It is a duplicate artificial fingerprint known as "Spoof artifacts" and is presented to a fingerprint sensor to fool the recognition system. Spoofing is a method of attacking biometric systems where artificial objects are presented to biometric ascription system that imitates biological and behavioral characteristics; the system is designed to measure. This paper focuses on Fingerprint Spoofing, its types and its identification techniques.

2. RELATED WORK

Existing system

Fake biometrics means by using the real images like iris images captured from a printed paper or fingerprint captured from a dummy finger of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first captures the original identities of the genuine user and then they make the fake sample for authentication. There is no such technology to provide security for fake users.

Proposed system

In the proposed method, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding livens assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. Here we are interfacing camera to ARM controller. The camera will capture face image of a person and send to controller. The controller will recognize the face and iris of the particular person from the image. The finger print module will take the finger print from the person and send to controller. The controller will recognize the finger print of particular person from the data base. If they are matched then it will display the data on display unit. Also here we added the RFID security system for more security. To demonstrate this we took an door locking application as an example. Also the card holder person details will be updated to PC through USB.

3. IMPLEMENTATION

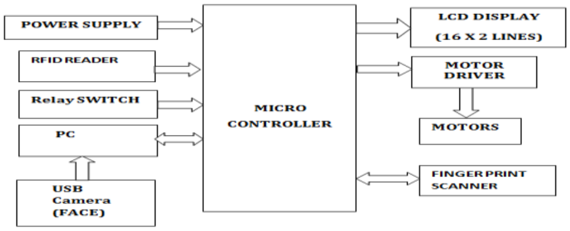


Fig:-1 BLOCK DIAGRAM

Power supply

The input to the circuit is applied from the regulated power supply. The a.c. input i.e., 230V from the mains supply is step down by the transformer to 12V and is fed to a rectifier. The output obtained from the rectifier is a pulsating d.c voltage. So in order to get a pure d.c voltage, the output voltage from the rectifier is fed to a filter to remove any a.c components present even after rectification. Now, this voltage is given to a voltage regulator to obtain a pure constant dc voltage.

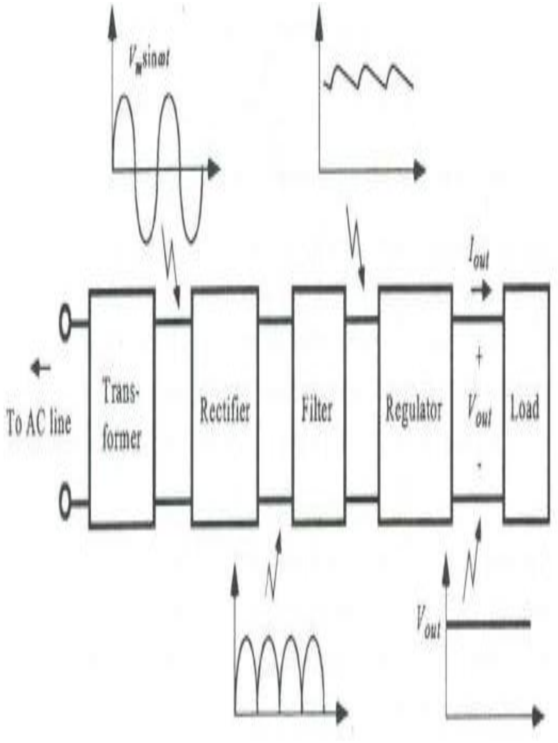


Fig 4.1components of power supply

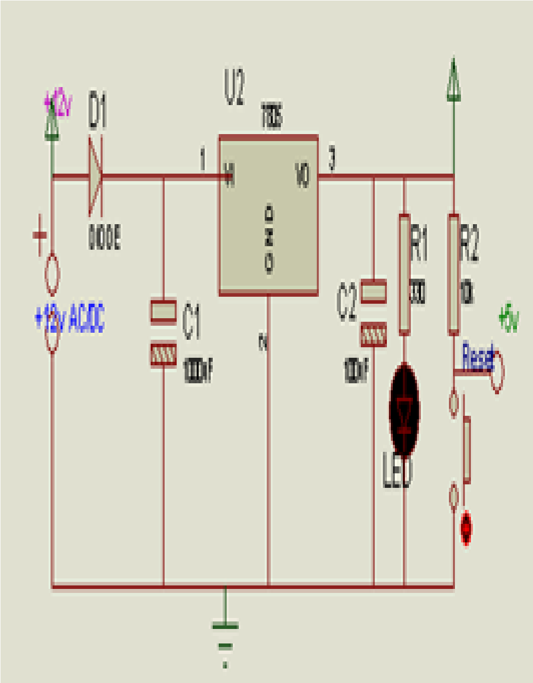
Transformer

Usually, DC voltages are required to operate various electronic equipment and these voltages are 5V, 9V or 12V. But these voltages cannot be obtained directly. Thus the a.c input available at the mains supply i.e., 230V is to be brought down to the required voltage level. This is done by a transformer. Thus, a step down transformer is employed to decrease the voltage to a required level. Rectifier

The output from the transformer is fed to the rectifier. It converts A.C. into pulsating D.C. The rectifier may be a half wave or a full wave rectifier. In this project, a bridge rectifier is used because of its merits like good stability and full wave rectification.

Filter

Capacitive filter is used in this project. It removes the ripples from the output of rectifier and smoothens the D.C. Output received from this filter is constant until the mains voltage and load is maintained constant. However, if either of the two is varied, D.C. voltage received at this point changes. Therefore a regulator is applied at the output stage. Voltage regulator:As the name itself implies, it regulates the input applied to it. A voltage regulator is an electrical regulator designed to automatically maintain a constant voltage level. In this project, power supply of 5V and 12V are required. In order to obtain these voltage levels, 7805 and 7812 voltage regulators are to be used. The first number 78 represents positive supply and the numbers 05, 12 represent the required output voltage levels



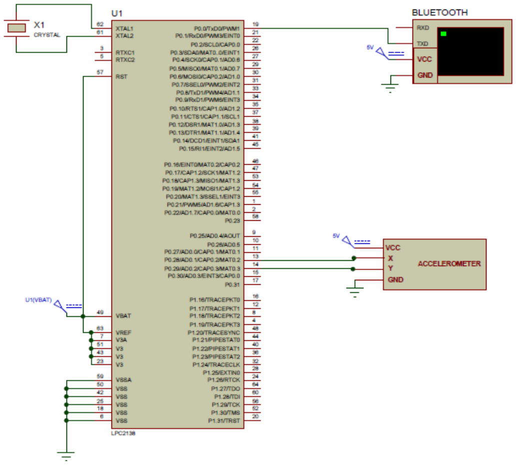
Bluetooth

The Bluetooth is communicated with serial communication. So the P0.0 and P0.1 pins are connected to Bluetooth module.

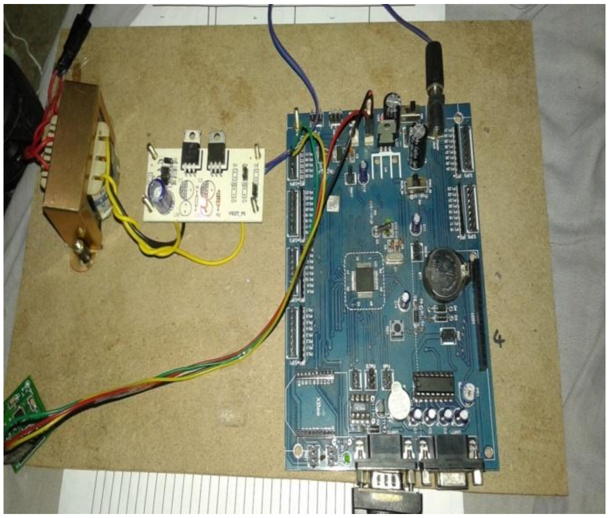
Accelerometer

The accelerometer is communicated with ADC communication. So the P0.29 and P0.30 pins are connected to accelerometer module.

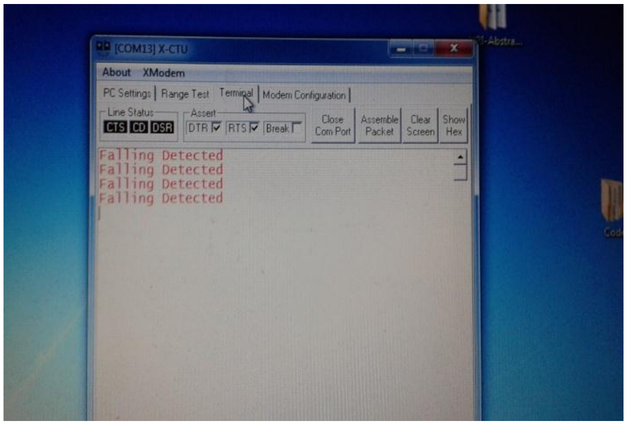
4. EXPERIMENTAL RESULTS



Proteus Simulation output

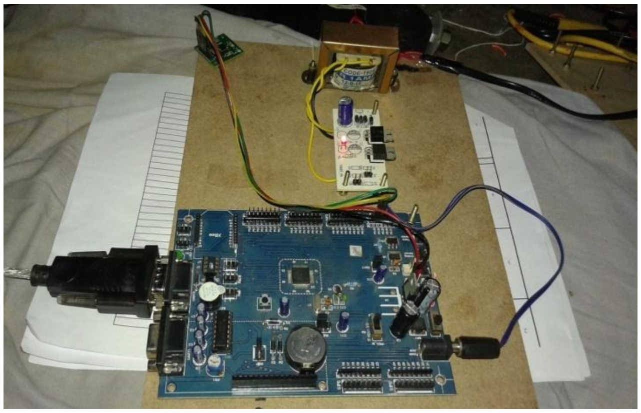


Final Kit



```
Falling Detected
Falling Detected
Falling Detected
Falling Detected
```

Processing Commands



Working Final Kit

5. CONCLUSION

Spoofing is a substantial challenge in fingerprint recognition systems. This paper has presented different spoofing techniques along with various state-of-the-art databases. Spoofing detection and its types are also been reviewed with corresponding databases. A fingerprint spoofing related algorithm needs a potent feature extractor which extracts the salient features from input images. A lot of algorithmic work is needs to be applied for fingerprint spoofing recognition system so as to derive generalized methods that are independent of specifications, requirements and results in increased spoofing recognition rate.

6. REFERENCES

[1] D. Maltoni, D. Maio, AK. Jain and S. Prabhakar, “Handbook of fingerprint recognition,” Springer Science and Business Media,2009.

[2] W. Zhao, R. Chellappa, PJ. Phillips and A. Rosenfeld, “Face recognition: A literature survey,” ACM Computing Surveys (CSUR) 35, no. 4: 399-458, 2003.

[3] S. Minaee, AA. Abdolrashidi, “Multispectral palmprint recognition using textural features,” IEEE Signal Processing in Medicine and Biology Symposium, 2014.

[4] S. Minaee, AA. Abdolrashidi, “Highly Accurate Multispectral Palmprint Recognition Using Statistical and Wavelet Features,” IEEE Signal Processing Workshop, 2015.

[5] KW. Bowyer, KP. Hollingsworth and PJ. Flynn, “A survey of iris biometrics research: 20082010,” Handbook of iris recognition. Springer London, 15-54, 2013.

[6] Emanuela M, Arun R, 2014. A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems ACM Comput. Surv.47, 2, Article A ,36 pages.

[7] Javier G,,Julian F,,Javier,,Raffaele C,2014,Fingerprint Anti-spoofing in Biometric Systems, Springer London.

[8] ManeeshS,July 2014Detection and Prevention of FingerprintAltering /Spoofing Based on Pores (Level-3) withthe Help ofMultimodal Biometrics,International Journal of Science and Research (IJSR).

[9] Annalisa F,Davide M ,2008,Fingerprint Synthesis and Spoof Detection,Springer London.

[10] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, “Determination of vitality from a noninvasive biomedical measurement for use in fingerprint scanners”, Pattern Recognition

Authors Profile

Ms. REPAKULA DURGA PRANUSHA pursuing M-Tech from department of embedded System at Khammam Institute of
Technology and Sciences, Khammam

K. Rajesh received M.Tech (Ph.D)degree and working as Associate Professor in ECE Dept ,Khammam Institute of Technology & Science, Ponnekal, Khammam, TS, India.His research area is fuzzy logic systems with VLSI and EMBEDDED SYSTEM. He has published 4 International Journal, 03 National Conference, 06 workshops & 4 FDP. He is having 9 years experience in teaching field and research domain fuzzy logic systems.

Mr. N. Chandra Shekhar completed his M-Tech with electronics and communication engineering. He has published more than five international journals. Currently he is a research Scholar in JNTU, Hyderabad and

Working as Associate Professor& Head of the department for ECE in Khammam Institute of Technology and Sciences, Khammam.