Section A-Research paper
ISSN 2063-5346

FAKE FINGERPRINT DETECTION

[1]Dr.Siva Kumar.P
Professor & HOD
Information technology
Manakula Vinayagar Institute of Technology
Puducherry,India
Email. id: hodit@mvit.edu.in

[2]Madhumidha.B
Information Technology
Manakula Vinayagar Institute of Technology
Puducherry,India
Email. id: madhumidhait2019@mvit.edu.in

[3]Yazhini Sivasankari.B
Information Technology
Manakula Vinayagar Institute of Technology
Puducherry,India
Email.id:yazhinisivasankariit2019@mvit.edu.in

[4]Priyadharshini.M
Information Technology
Manakula Vinayagar Instiute of Technology
Puducherry,India
Email.id: priyadharhiniit2019@mvit.edu.in

Abstract: With the increase in technology, for the estimation and security biometric systems has created a various initiative. In this paper, we focused on various solutions that overcome the several kinds of issues faced by using hardware based fake fingerprint detection. In the existing scenario, to identify the spoofing of fake fingerprint, the system is trained with several kinds of images that represent the artificially moulded fingerprints also those images are compared with the real fingerprint images. This produces a low degree of complexity and gray scale levels in finger ridges and valleys. In our proposed scenario, we consider the features such as color, light transmission property fingerprint for features extraction. This efficient method discriminates the legitimate features from the artificially moulded fingerprints. Also, by using singular value decomposition method we can achieve more accurate detection of finger features. It is more robust to detect the fake features from the original features. From the experimental result, we can recognize the additional features such as color transmission and pressure features which are fake or real samples.

Keywords— Fingerprints, Feature Extraction, Biometric, spoofing.

I. INTRODUCTION

A wide range of people benefit from biometric technology in order to identify and examine people primarily on their physical and behavioral traits. Authentication via biometrics is the most secure option. Biometric features should be carefully adopted in accordance with specifications like universality, distinctiveness, performance, and collectability. Additionally, when designing a biometric system, the criteria for recognition, precision, and synchronization should be tackled.

A biometric authenticating mechanism makes use of characteristics that are specific to a person. IOT device manufacturers uses fingerprint readers to offer rapid and safe recognition. According to Fig. 1.1, biometric traits can be divided into two categories: physiological traits and behavioral traits.

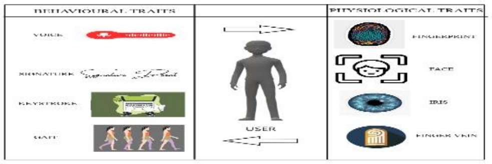

Fig 1.1 Common traits in biometric authentication systems.

II. RELATED WORK

The existing work mainly focuses on the fine feature extraction from the fingerprint and also in the performance of fingerprint recognition algorithms. The pore features have proven that it is useful for recognition of fingerprints and the minutiae and ridge patterns are achievable from low resolution images. To recover the pore information, we used an approached with the joint learning with super resolution and pore detection network. Here the use of framework called Super-Resolution Generative Adversarial Network (SRGAN) helps to reframe the low-resolution images to high-resolution images. And these high-resolution fingerprint samples are synthesized from the real low-resolution samples by the distinctive feature representation. From the deep fingerprint verifier, the extracted features are added to the subject for determining its uniqueness. Also, the reconstruction ridge and utilization of ridge patterns are added to make the best of feature extraction. In overall, the proposed method enhances the quality of fingerprint images and also resolves the recognition problem [2].

The other study, describes the security enhancement of the finger authentication system. Here, the use artificially moulded fingerprints and about the sensors which used in capturing of finger images were discussed. This study aims mainly spots the fake fingerprints samples with high degree of textures and the effect of normalization. The study focuses on min-max normalization to improve the performance of detecting fake fingerprint image samples with various state of sensors. To examine the effect of normalization, the Gray Level Co-occurrence Matrix (GLCM) images are evaluated along with K-Nearest Neighbor (KNN), Support Vector Machine (SVM) and Neural Network (NN). In this study the increased texture of the real fingerprint samples results was achieved [1].

According to the author's vision in this study, the field of biometric security has the greater advancement of fingerprint recognition system. Also, it plays a vital role in fingerprint authentication system in personally and also globally. Even though, the technology of biometric security is still admitted to spoofing attacks with fake samples of an individual's fingerprints. The sensors and spoof detectors are still attempting a major challenge with the artificial or spoofing materials. This paper proposes a method for fake fingerprint detection using feature descriptors [3].

III. PROBLEM STATEMENT

There is a need to develop a solution that can be broadly accepted and would result in improved security in biometric system. The system should be capable of analyzing the characteristics of artificially moulded fingerprints and real fingerprint. It should eliminate the access whenever the spoofing of fake fingerprint takes place and it must check the finger liveness when it is placed on the sensor. As a result, our goal is to create a model that shows the accuracy of the liveness detection of an individual's finger and identification of spoofing attacks.

IV. EXISTING SYSTEM

In the existing system, the biometric authentication system is trained with various images that represent the difference between real and fake fingerprints. The differences between these images are caught from the gray scale levels of finger ridges and valleys. Also, this system is only considered with the pre-process images and does not consider the liveness comparison. Here we consider two input samples such as real and fake sample features. The system requires one input image to maintain its generality and simplicity. We are capable to figure out the error sensitivity measures by using the whole reference image quality assessment. Colour, local artefacts, precision, illumination levels, and the amount of information that exists in both kinds of images and structures comprise the primary distinctions between real and false examples. For instance, it is more likely that the iris photographs that are taken from printed paper will be blurry or entirely out of focus. Face images which are captured from a mobile or any other devices will possibly under exposed. Additionally, photographs of fingerprints taken with a dummy finger show local acquisition artefacts like spots and patches. Additionally, when a synthetically portrayed image is included to a communication channel without first going via a feature extractor, it will typically lack some of the characteristics of natural images. So, this technique found a decrease in accuracy and security of the biometric authentication system.

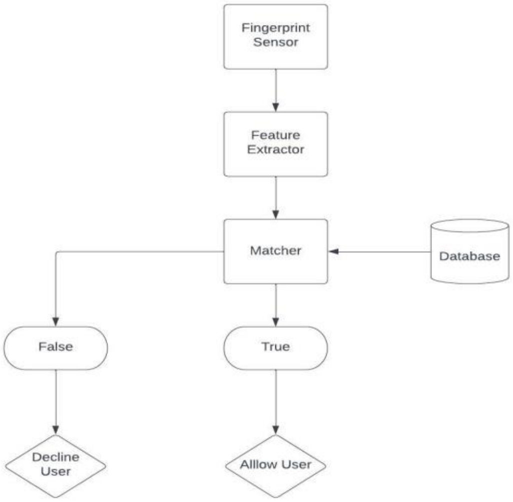

Fig 4.1 Existing Biometric System

V. OBJECTIVE OF THE PROJECT WORK

The basic goal is to decrease the spoofing attacks caused in biometric system and to improve the efficiency, accuracy and security biometric authentication.

VI. PROPOSED MODEL

By using many descriptors derived from various colour spaces and a print light detector to calculate low-position features, we are able to take advantage of the shared color-texture information from the luminance and chrominance channels. We test the effectiveness of several colour spaces and descriptors in communicating the inherent difference in colour texture between real fritters and imitation fritters. Using their pre-defined, thoroughly well-defined experimental assessment processes, we undertake extensive, grounded experimental analysis on the three most difficult and difficult spoofing fingerprints, ensuring the results' reproducibility and a fair comparison with the actual system.

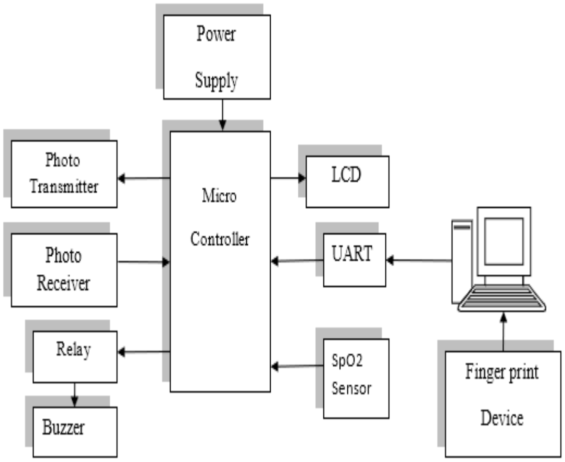

Fig 6.1 Proposed Work Flow

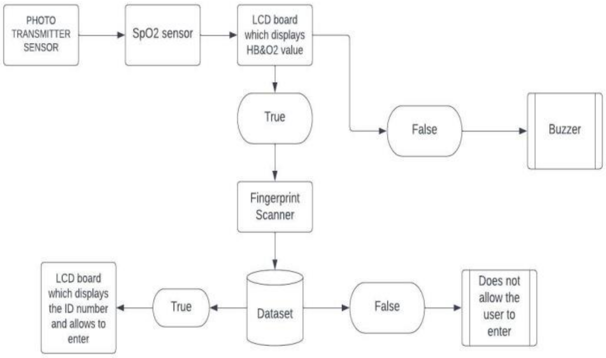
PHOTO TRANSMITTER SENSOR
SpO2 sensor
LCD board which displays HB&O2 value
True
False
Buzzer
Fingerprint Scanner
LCD board which displays the ID number and allows to enter
True
Dataset
False
Does not allow the user to enter

Fig 6.2 Proposed Architechture

Originally, the motor converts the Direct current of 120 volts into 12 volts, also the power rectifier converts that 12 volt into 5Volts and now every factor performs under 5 volts. The SpO2 detector senses the placed finger is belonging to mortal or artificially moulded by detecting the heartbeat rate and blood oxygen position and the color detector reads the point and stores it temporarily. The values similar as heartbeat rate, oxygen position and color detector and also the commands like" Finger Ok" or " Finger Not Ok" are displayed in the PCB panel 1 still, the command "Finger Not Ok" is displayed on the PCB panel and the Buzzer makes a sound to indicate the use of fake point, if the corresponding Values aren't satisfied still, the command "Finger OK" is displayed on PCB panel also the remaining factors are actuated for further processes, If the corresponding values are satisfied. Now the point scanner reads our point lively and compares with point which is stored temporarily. If this comparison isn't satisfied the command" ID not verified" will be displayed on the PCB panel 2. Or if this comparison is satisfied also the command "ID verified" will be displayed on the PCB panel 2. Also displays the delicacy percent of the matching finger.

VII. RESULT & DISCUSSION

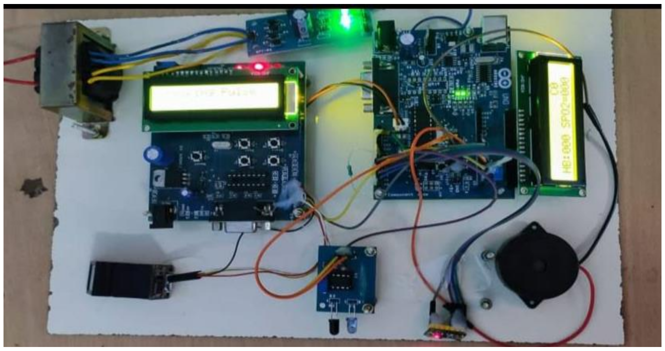

Fig 7.1 Proposed System Prototype

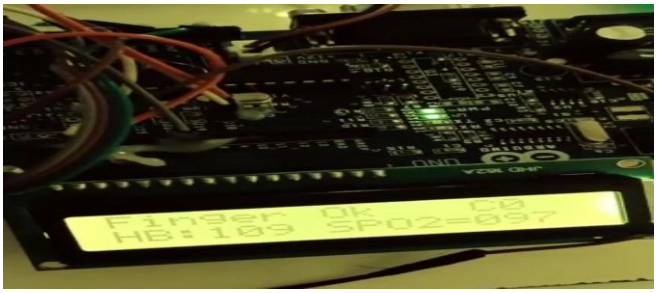

Fig 7.2 Finger Liveness Verification

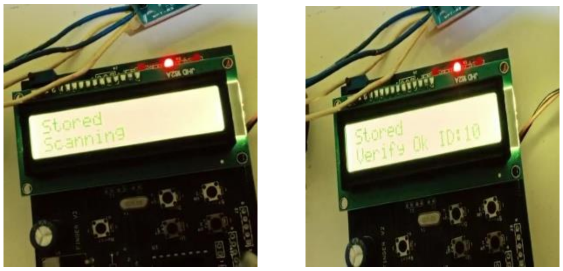

Fig 7.3 User Fingerprint Verification

VIII. CONCLUSION

The innovation of this project is to identify the illegal attempts of fake or artificially moulded fingerprints. The artificial fingers or fingerprints of an individual can be made with a material such as silicon, rubber, etc. We use sensors to detect those moulded fingerprints, even thin layers of the fingerprint patterns of an individual can be detected as expected and the accuracy of the system is high. From the experimental result, we can recognize the additional features such as color transmission and pressure feature which are real or fake samples. The proposed scenario is more of an accurate classification result due to the consideration of additional features. This system is highly secure from spoofing. An individual's artificial fingers or fingerprints.

IX. FUTURE SCOPE

When we come to large scale implementation of the project, this will be used in big organization for user entry purpose. And this will be very much useful for accessing the data or details of an individual which is stored in the internet.

For example, every people have unique Aadhar ID and those details are stored in a cloud or big database. If an individual wants to access the details of his or her specifications then he or she can access it by during their Aadhar number. But consider a scenario that the person missed or forgotten their Aadhar card or Aadhar number, in such case they have another way of accessing, that is with the help of Biometric authentication. As we know, during the time of Aadhar registration we also registered with our finger samples, with the use of this we can access our details within a short period of time and with advanced feature of fake fingerprint detection. This helps surely that, only the right person will access the details and there will be no possibilities of any fraudulent attempts.

Another example is with banking, usually we access our ATM with secret number or secret code and when this project comes to implementation, we can also access the ATM by Biometric authentication instead of secret code.

REFERENCES

[1] Safrira Nuraisha & Guruh Fajar Shidik , RK 2018, “Evaluation of Normalization in Fake Fingerprint Detection with Heterogeneous Sensor”, International Seminar on Application for Technology of Information and Communication (iSemantic),RK 2018 .

[2]Syeda Nyma Ferdous**,** “ Super-resolution Guided Pore Detection for Fingerprint Recognition”, 25th International Conference on Pattern Recognition (ICPR),UTC from IEEE Xplore, 2020.

[3]B.V.S Anusha,“End2End Fingerprint Spoof Detection using Patch Level Attention”, International Journal pf Innovative Technology and Exploring Engineering(IJITEE), 2020.

[4] Aggarwal, N & Agrawal, “First and second order statistics features for classification of magnetic resonance brain images”, Journal of Signal and Information Processing, vol.3, pp.146-153,RK 2012.

[5] Aly, “Survey on multiclass classification methods”, Neural Network, pp.1-9,M 2005.

[6] Antonelli, A, Cappelli, R, Maio, D &Maltoni, “Fake finger detection by skin distortion analysis”, IEEE Transactions on Information Forensics and Security, vol. 1, no.3, pp. 360-373,D 2006.

[7] Arastehfar, S, Pouyan, AA &Jalalian, “An enhanced median filter for removing noise from MR images”, Journal of Artificial Intelligence (AI) and Data Mining, vol.1,no.1,pp. 13-17,A 2013.

[8] Baldisserra, D, Franco, A, Maio, D &Maltoni, “Fake fingerprint detection by odor analysis”, In Advances in Biometrics , Springer Berlin Heidelberg, pp. 265-272,D 2005.

[9] Bao, L &Zeng,“Comparison and analysis of the selection mechanism in the artificial bee colony algorithm”, Proceedings of Ninth International Conference on Hybrid Intelligent Systems, vol. 1, pp. 411- 416, JC 2009.

[10] Belkin, M, Niyogi, P & Sindhwani, V, “Manifold regularization: A geometric framework for learning from labelled and unlabeled examples”, Journal of Machine Learning Research, vol.7, pp.2399– 2434,2006.

[11] Biel, L, Pettersson, O, Philipson,L&Wide,“ECG analysis: a new approach in human identification”, IEEE Transactions on Instrumentation and Measurement, vol.50, no.3, pp.808–812,P 2001.