Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 9, September : 2025

Intelligent Fingerprint Liveness Detection Using Machine Learning Techniques

Dr.A.SATYANARAYANA
drsatyanarayanaakella_cse@siddhartha.co.in
Department of Computer Science Engineering,
siddhartha institute of engineering and technology, Hyderabad, india

Mr. K.RAVI NAIK
ravinaik_cse@siddhartha.co.in
Department of Computer Science Engineering,
siddhartha institute of engineering and technology, Hyderabad, india

Abstract

Fingerprint recognition systems are widely used for secure access control, yet they are vulnerable to spoofing attacks using fake fingerprints made from materials such as silicone, gelatin, or3d-printed replicas. This project focuses on developing an advanced fingerprint liveliness detection system to distinguish between genuine and spoofed fingerprints. The proposed system leverages a combination of physiological and behavioral characteristics to assess fingerprint liveliness. Key methods include analyzing perspiration patterns, skin elasticity, and micro-vibrations in response to touch. Additionally, a machine learning model is trained on data from a diverse set of real and artificial fingerprints to enhance accuracy and reduce false positives. To~ implement this system, a high-resolution fingerprints canner captures detailed fingerprint images and biometric signals. Features are extracted using image processing techniques, and the model evaluates these features to determine liveliness. The system ensures high usability and minimal latency, making it suitable for integration into existing biometric authentication systems. By enhancing security against spoofing attacks, this project addresses a critical challenge in biometric authentication, paving the way for more robust and reliable fingerprint-based security solutions.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 9, September : 2025

Keywords — Liveness detection, fingerprint spoofing, ATM security, pores and ridges, biometric authentication.

I. INTRODUCTION

Fingerprint recognition is widely used for secure authentication due to its convenience and uniqueness. However, the vulnerability of these systems to spoofing attacks, where artificial fingerprints made of materials like silicone or gelatin can bypass security, poses a significant threat. This undermines the trust and reliability of biometric systems in critical applications such as banking, access control, and personal device security. The motivation for this project stems from the need to address these vulnerabilities by developing a robust liveliness detection system. By ensuring only genuine fingerprints are recognized, this project aims to enhance security, protect sensitive information, and foster trust in biometric technologies. Devices and providing a more natural and intuitive interaction, Air Canvas aims to expand the possibilities of digital content and create a more inclusive digital landscape. Traditional fingerprint recognition systems, whilewidelyusedforauthenticationandsecurity, arevulnerableto spoofing attacks using artificial replicas made from materials like silicone, latex, or 3D-printed molds. These attacks exploit the inability of basic fingerprint scanners to distinguish between live (genuine) and fake (spoofed) fingerprints, posing significant security threats in sensitive applications such as banking, access control, and personal devices.

The primary problem is the lack of robust liveliness detection mechanisms that can reliably differentiate live fingerprints from spoofed ones without compromising user experience or increasing authentication latency. Current systems often either fail to detect sophisticated spoofing attempts or yield a high rate of false positives, which can lead to inefficiencies and loss of trust in biometric systems.

This project aims to address these challenges by developing an advanced fingerprint liveliness detection system that integrates physiological and behavioral biometric analysis with machine learning to enhance the accuracy and reliability of authentication processes.

II. BACKGROUNDSTUDY

Fingerprints are widely used in daily life for more than100 years due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. A large number of approaches to fingerprint matching and various algorithm and methods are behind their matching procedure, Fingerprint based security systems are implemented for secure access at various levels. Level-3featuresareoftendefinedasthedimensionalattributesof the ridges and include sweat pores, ridge contours, and ridge edge features, all of which provide quantitative data supporting more accurate and robust finger print recognition. Severalpore based methods were proposed for liveness detection. The procedures include extraction of the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using convolution [1] [2]; usage of adaptive pore model APM, time series detection of perspiration and pores location [3] [4];techniques to identify fingers with a dry skin and sweaty fingers and to determine the system performance of the sensor, i.e., to distinguish false acceptance rate and the false rejection rate [5].In their work, Peter Johnson and Stephanie Shockers, used pore centers as features and are identified by searching the ridge segments for local maxima in gray level, satisfying certain threshold criteria. The extracted features are classifieds live or fake using a support vector machine (SVM) classifier with radial basis function (RBF) kernel [6].

III. PROPOSED SYSTEM

The proposed fingerprint liveliness detection system introduces a comprehensive approach to biometric security by integrating multiple advanced technologies. It features multi-modal detection, combining thermal imaging, sweat pattern analysis, capacitive sensing, and image-based features to achieve high accuracy in detecting spoofed fingerprints. This approach strengthens resistance against sophisticated spoofing attempts. Additionally, machine learning integration leverages deep learning models, specifically Convolution Neural Networks (CNNs), to automate feature extraction and real-time classification, allowing the system to adapt to emerging spoofing techniques effectively. The system is optimized for real-time performance, ensuring minimal latency and seamless user experiences during authentication processes. Furthermore, it incorporates environmental robustness, adjusting its detection

mechanisms to maintain reliable performance across diverse environmental conditions.

A. Capacitance Formation:

The sensor consists of an array of tiny capacitors, each with two conductive plates: one embedded in the sensor and the other formed byte user's finger. When a finger touches the sensor, the ridges of the fingerprint come in close contact with the sensor, altering the capacitance values at specific points.

B. Fingerprint Imaging:

The ridges increase capacitance due to closer proximity, while the valleys (air gaps) reduce capacitance. The sensor captures these variations in capacitance to create a high-resolution image of the fingerprint pattern.

IV. RESULTS AND DISCUSSION

Detecting Liveliness of Fingerprint

To ensure that the fingerprint is from a living person (not areplica or fake), the capacitive sensor can employ liveness detection through the following methods:

Skin Properties Detection:

Dielectric Properties: Human skin has unique dielectricproperties that influence the capacitive response differently compared to synthetic materials like silicone or gel.The sensor can detect inconsistencies in the material's capacitance that indicate it is not real skin.

Electrical Impedance:

Live skin has an electrical impedance due to its natural moisture and electrolyte content, which affects the capacitance signal. Fake fingerprints made of plastic or rubber lack this electrical impedance, making them distinguishable.

Perspiration Measurement:

Live skin naturally emits moisture (sweat), which subtly affects the capacitive readings over time. The absence of such changes in capacitance signals can indicate a fake fingerprint.

Dynamic Signal Analysis:

The sensor may detect subtle changes caused by blood flow and pressure changes in live fingers when pressing against the sensor. Fake fingerprints are static and fail to show such variations.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 9, September : 2025

Multilayer Analysis:

Advanced capacitive sensors can penetrate slightly below the outer layer of the skin to detect sub dermal structures like issue or blood vessels, ensuring it's not just a surface replica.

V. USECASEDIAGRAM

Actors:

H. User–Interacts with the system by placing their finger for authentication.

I. System – The capacitive finger print sensor system that processes and verifies the fingerprint

Use Cases:

J. Place Finger

The user places their finger on the capacitive sensor. The system starts data collection.

K. Capture Fingerprint

The sensor captures the finger print ridges and valleys through capacitance data.

L. Process Fingerprint

The system converts capacitance data in to a finger print image.

M. Detect Liveness

The system analyzes dielectric properties, electrical impedance, and perspiration to determine if the finger is live.

N. Verify Finger print

The system compares the fingerprint against stored templates. Verifies liveness and authenticity.

O. Grant/Deny Access

If the finger print and liveness pass verification, access is granted. Otherwise, access is denied.

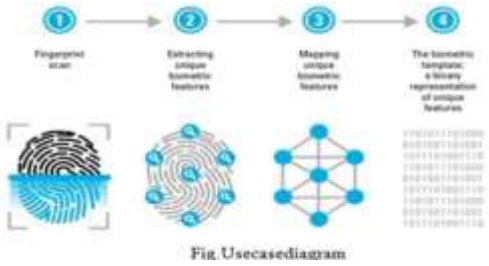
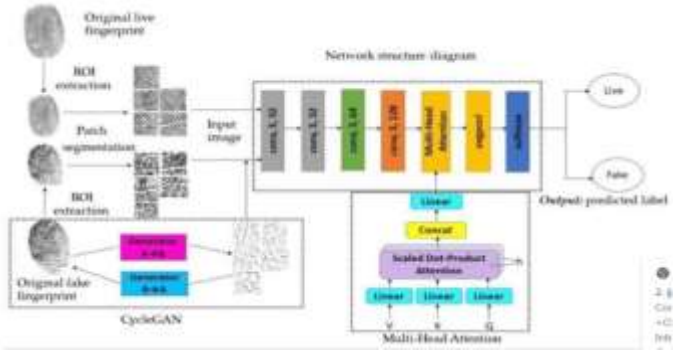


Fig Usecasediagram

ACTIVITYDIAGRAM



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 9, September : 2025

VI. INTERFACE REQUIREMENTS

System Requirements Hardware

Hard Disk: 500 GB. RAM: 8 GB.

Processor: Intel Core i5, AMD Ryzen 5, or equivalent Sensor: R502 Sensor

Software Requirements

Operating System : Windows 10 or higher

Python Environment:Python3.7 or higher required.

Dependencies and Libraries: OpenCV, Mediapipe, NumPy

Performance Requirements

The performance requirements for the proposed fingerprint

Liveliness detection system ensure efficient ,accurate, and reliable operation in real-world applications. The system must provide real-time detection, completing the liveliness check within to avoid deys during finger print authentication. It should achieve an accuracy level with atrue positive rate(TPR) of atleast 99%and a false positive rate (FPR) of no more than 1%, ensuring robust differentiation between live and spoofed fingerprints. In high- demand scenarios, the system must process 100 milliseconds or less least 10 fingerprint scans per second to handle multiple at le users simultaneously without performance degradation.

VII. OUTPUT SCREEN

VIII. ACKNOWLEDGEMENT

Our colleagues are genuinely appreciative to that multitude of individuals who have been providing us with any sort of help with the creation of this task report. We would there fore, create a large portion of the open door by communicating our sincerest gratitude to every one of my resources whoselessons gave us theoretical arrangement and lucidity of

understanding, which eventually made our occupation all the simpler. Credit likewise goes to every one of my companions whose support kept us in great stead. Their constant help has given me the strength and certainty to finish the undertaking with no trouble.

IX. CONCLUSION

The fingerprint enrollment and verification system has been successfully implemented, offering a reliable biometric authenticationsolutionusingtheR502/R503 fingerprintsensor.It efficiently handles fingerprint enrollment by capturing and storing templates with unique IDs, allowing users to enroll multiple fingerprints. Upon verification, the system compares the scanned fingerprint with stored templates and triggers a relay if a match is found, providing real-time feedback through LEDs and the Serial Monitor. The system also includes error handling for invalid fingerprints, feedback to guide users through the enrollment and verification process. The system's performance is reliable, with accurate fingerprint recognition and effective error handling, making it suitable for applications such as security systems, automated access control, and personal authentication. This solution meets the project objectives and can be further enhanced with features like liveliness detection or integration with cloud storage for improved security and scalability.

The fingerprint authentication system has been successfully developed and implemented, providing a secure and efficient methodofbiometricverificationusingtheR502/R503fingerprint sensor. The system enables users to enroll fingerprints with unique IDs, storing them in the sensor's memory for future reference. During the verification process, it accurately compares a scanned fingerprint with the stored templates, offering immediate feedback via LEDs and the Serial Monitor. A relay is triggered upon successful fingerprint verification, allowing the control of external devices such as locks or gates. The system is equipped with robust error handling mechanisms, addressing issues like invalid fingerprints, communication failures, and storage limitations, ensuring mooth operation.The user interface is intuitive, offering clear instructions

through the Serial Monitor, and LED indicators provide additional visual cues for the user. communication failures, and exceeding the sensor's storage capacity. The relay control feature works seamlessly, allowing external devices like locks or gates to be controlled based on system.

X. REFERENCES

[1]Neha Kesharwani,S.P.Ugale "Fingerprint RecognitionUsing Level3Features",InternationalJournalofAdvancedResearchin Computer and Communication Engineering Vol. 3, Issue 6 June 2014.

[2] Marcus de Assis Angeloni, Aparecido Nilceu,"Improving the Ridge Based Fingerprint Recognition Method Using SweatPores", UNESP - Univ EstadualPaulista Bauru, S˜ao Paulo, Brazil.

[3] S.Memon, Member, IEEE, N. Manivannan, Member, IEEE, W.

Balachandran Fellow, IEEE "Active Pore Detection for Liveliness in Fingerprint Identification System", November 22- 24, 2011

[4] Sujan T. V. Parthasaradhi,B.S., Reza Derakshani, M.S., Lawrence A. Hornak, , Stephanie A. C.Schuckers, "Time-SeriesDetectionofPerspirationasaLivelinessTestinFingerprint Devices",2012.

[5]E.J.BusselaaR,"Improvedporesdetectionin fingerprints by applying ring led's (525 nm)", Optica Vol.XL,No.4,2010.

[6]PeterJohnsonandStephanieSchuckers "Fingerprint Pore Characteristics For Liveliness Detection", Clarkson University Potsdam, NY 13699, U.S.A.

[7] Maurício pamplonasegundo, rubisley de paulalemes, "pore-based ridge reconstruction for fingerprint recognition" FederalUniversityOf Bahia, Brazil.

[8] QijunZhao,DavidZhang,LeiZhang,Nan Luo ,"Adaptive Fingerprint Pore Modeling And Extraction", 2010 Elsevier Ltd, 2010.02.016.

[9] Qijun Zhao, Lei Zhang, David Zhang, and Nan Luo, "Direct Pore Matching for Fingerprint Recognition , Springer-Verlag Berlin Heidelberg 2009.

[10]MahakArora1,VeenuSharma21,2ECE Department, KITM, Kurukshetra, Haryana India "Fingerprint Identification Using Fusion of Pores and Minutiae Extraction at Different Resolutions"

[11] David Asatryan, Grigor Sazhumyan "Segmentation Based Fingerprint Pore Extraction Method", International Journal