International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

FINGERPRINT SPOOFING DETECTION USING MACHINE LEARNING PFA

Sandhya k
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sandhyakmca2025@gmail.com

DR Dharamvir
HOD
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
dhiruniit@gmail.com

ABSTRACT

These methods employ texture analysis, detecting liveness (such as sweat and pulse), and advanced image processing along with to the ridge as well as valley to differentiate between real and artificial samples patterns. One technique that highlights the differences between artificial imitations and natural ridge structures is enhancing the contrast of fingerprint images. To applies contrast enhancement to the introductory fingerprint pictures. This technique is employed to identify phony fingerprints based on scanners. To determine whether the fingerprint used for authentication is authentic or fraudulent, fingerprint spoofing isrequired. The sensor that recognizes the ridges and valleys on a finger receives a fingerprint.After that, it recognizes the new fingerprint. to that fingerprint that was already there. In contrast, valleys are represented by the white spaces between the ridges, and ridges are represented by the dark lines. Using machine learning, fingerprint detection also identifies passive attacks. Additionally, it uses graphical analysis of both authentic and fraudulent fingerprint images to manage the data.

Keywords: biometrics, security, machine learning, fingerprint, liveness, detection, and antispoofing

INTRODUCTION

Furthermore, fingerprint recognition is crucial for detecting passive attacks and graphical analysis of fingerprint images to distinguish authentic users from fakesDespite their widespread use, fingerprint detection remains a significant challenge for research communities. The user was not given the option to log in directly via email, which would have solved significant issues like password forgetting. documents that have been proposed in the field of fingerprint biometrics, which has been expanding quickly and drawing interest from researchers in recent years [3]. No portfolios were added to the current fingerprint detection system.

The objective is to examine the various studies proposed in liveness fingerprint detection systems that able to classifies real fingerprint images and the fake one graphical analysis in spoof detection improves the system's accuracy even more. The system determines detection ratios of real versus fake fingerprints by analyzing sizable datasets of fingerprint samples, giving a numerical depiction of system performance. The combination of edge detection, database comparison, and ratio-based analysis guarantees that fingerprint recognition frameworks maintain high security and precision while being resistant to spoofing attempts.

LITERATURE SURVEY

fingerprint spoofing detection identifies a amount of shortcomings in the sites and systems that are currently in use to try to solve this problem. It can be challenging for users to engage with the system efficiently due to the current spoof detection platforms' frequent lack of sophisticated user-friendly features. main shortcomings noted, for instance comment section, which prohibits users from sharing feedback, reporting problems, or talking about issues pertaining to passive attack detection. The absence of interactive elements diminishes chances for ongoing enhancement and user involvement.

The login and authentication procedure is another issue with the current systems. Users frequently have trouble logging into the system, especially if they forget their login credentials. Users are forced to re-register whenever they experience login issues because current platforms lack convenient options like direct email login or a "forgot password" recovery feature. details are not well gathered, track user activity or confirm authenticity. users are left without adequate assistance when determining This not only deteriorates accessibility but also irritates users. Impression of the Finger Numerous studies on fingerprint framework identification have been instructed to use a phony fingerprint identification system. According to unique fingerprints, no two people in the universe will have exactly the same set of fingerprints on their fingers. Additionally, no two identical twins have the same fingerprints on the same finger. From the moment of our birth until the moment of our death, the impression of our fingers on our hands doesn't change.

EXISTING WORK

Existing fingerprint spoof of drawbacks despite their value. These systems lack sensitive content enablement, which allows users to upload content without any kind of restrictionor security verification, even though

they frequently include necessary modules such as a user module and a registration module. Concerns about data integrity and privacy are also raised by the lack of security measures for user-submitted spoofing results and uploaded data. The inability to upload images straight from external drives is another significant flaw that restricts the system's adaptability These systems lack sensitive content enablement, which allows users to upload content without any limitations or security verification, despite typically having necessary modules like a user module and a registration module.The absence of security safeguards for user-submitted spoofing results and uploaded data also raises privacyand data integrity concerns Another major issue that limits the systems is the inability to upload images directly from external drives flexibility. Additionally, because users do not receive any recommendations or customized guidance regarding spoofing detection, the systems are less user-friendly and effective at meeting specific needs.

DISADVANTAGES

- High Implementation Cost: Developing and maintaining safe detection of fingerprint spoofing
  systems requires a substantial financial outlay.
- Database Vulnerability: There are significant worries regarding data privacy because biometric databases are still vulnerable to hacking and illegal access.
- Time Consumption: The detection process frequently takes a long time before the user receives the results, which lowers system efficiency.
- Limited User Privacy: User privacy may be jeopardized by the tracking and storing of biometric information, such as fingerprints and facial photos.
- Manual Dependency: A lot of systems still need human intervention, which adds to the workload and limits automation.

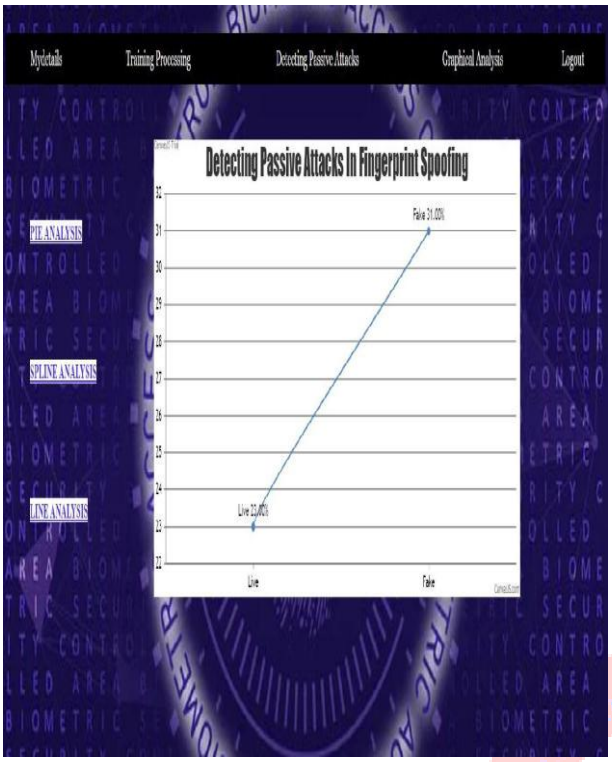
PROPOSED SYSTEM

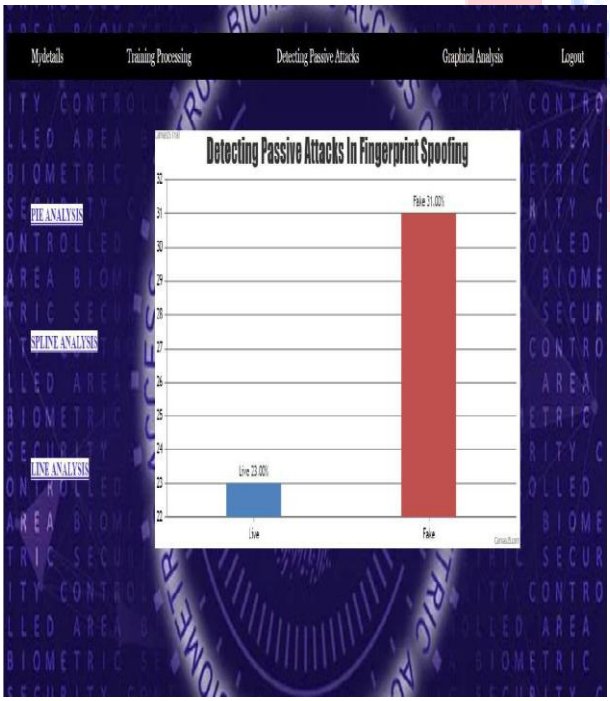
The main idea behind the current spoofing detection website is to improve security and dependability by addressing the shortcomings of previous systems through the introduction of novel techniques. The current system has made an effort to offer an enhanced structure by prioritizing user authentication prior to granting access, whereas earlier spoof detection frameworks had several shortcomings, including limited functionality and a lack of Security.

ADVANTAGES OF PROPOSED SYSTEM:

- Improved Security: Compared to current systems, fingerprint spoofing recognition offers more assurance and robust protection.
- User-Friendly Access: Spoof detection is widely available, straightforward, and easy to use.
- Quick and Convenient: Offers prompt responses, enhancing the user experience in general.
- Non-Transferability: To prevent unwanted use, fingerprint impressions cannot be shared or transferred digitally.
- Machine Learning Integration: Increases the accuracy of spoof detection by using sophisticated algorithms (like CNN).
- By automatically distinguishing between real and fake fingerprints, automated analysis minimizes manual labor.
- Data protection: Prevents unwanted access to biometric databases and guarantees enhanced privacy.

EXPERIMENTAL RESULTS





CONCLUSION

This paper's goal is to examine novel fingerprint recognition technologies and techniques for identifying passive fingerprint attacks. Biometric fingerprint systems are shielded from phony fingerprints, which can be created using a range of instruments and materials, by a method known as fingerprint spoofing detection.These recognition systems use physical fingerprints for computerized identification on the website. traits and depend on the behavioral and physiological characteristics of individuals. To find passive attacks in fingerprints, graphic analysis is utilized, which evaluates performance metrics like accuracy, precision, and recall. Spoofing detection makes it easier to tell if a fingerprint is a real or fake representation. Graphical analysis, which assessesperformance metrics like accuracy,precision, and recall, is 1 used to identify passive attacks in fingerprints. Determining whether a fingerprint is a real or fake representation is made easier with spoofing detection. The system analyzes the finger'sridges and valleys to determine authenticity by comparing a freshly scanned fingerprint with templates that have been stores.

REFERENCE

Text Book Reference:

1. Django for Beginners: Build websites with Python and Django.

2. Python Programming: An Introduction to Computer Science.

Web Reference

1. https://www.w3schools.com/python
2. https://pythonvisualization.github.io/folium/index.html
3. https://github.com/pythonvisualization/folium/blob/master/examples/plugin-Search.ipynb