Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Fingerprint Based ATM System Biobank-Secure

Prof. Yashraj Chavan [1], Ms. Pranali Bagul [2], Ms. Harshada Pachal [3], Ms. Gayatri Waghmare [4], Ms.Shubhangi Waghchaure [5]

[1] Lecturer, Department of Computer Engineering,JSPM's RSCOE Polytechnic, Pune, Maharashtra, India
[2,3,4,5] Student, Department of Computer Engineering,JSPM's RSCOE Polytechnic, Pune, Maharashtra, India

Abstract

The rapid evolution of digital technology has transformed critical sectors such as banking, healthcare, and research, making data security an essential concern. Traditional authentication methods, including passwords and PINs, are increasingly inadequate due to risks such as phishing, brute-force attacks, and insider threats. This research proposes **Biobank-Secure**, a full-stack web-based biometric authentication system utilizing fingerprint technology to address these vulnerabilities. The system integrates a **Java-based backend**, a **responsive web frontend**, and **deep learning** techniques through **Convolutional Neural Networks (CNNs)** for feature extraction. Fingerprints, being unique and difficult to forge, provide a reliable mechanism for user verification. The backend employs **RESTful APIs** to facilitate secure communication between the client and server. Extensive testing demonstrates that Biobank-Secure achieves an authentication accuracy of approximately **92%**, with precision and recall metrics ranging from **90% to 94%**. The results indicate that deep learning-based fingerprint verification can significantly enhance security, reduce reliance on human intervention, and provide a scalable solution for high-stakes applications such as **biobanks**, research laboratories, and banking systems. This paper further discusses the system's **three-tier architecture**, the technological stack, and potential avenues for future improvements, including integration with **IoT-based environmental context** and multi-modal biometric fusion.

Keywords: Biometric Authentication, Fingerprint Recognition, Deep Learning, Convolutional Neural Networks (CNN), Cybersecurity.

1. Introduction

Digital transformation has revolutionized the way organizations store and manage sensitive information. With increased reliance on digital platforms, the need for robust security mechanisms has become critical. Traditional authentication techniques, such as passwords and PINs, remain the most commonly used methods, yet they are prone to vulnerabilities. Users often choose weak passwords, reuse them across multiple platforms, or fall prey to phishing and social engineering attacks. Consequently, unauthorized access can lead to financial loss, privacy breaches, and even jeopardize critical research data.

Biometric authentication provides a solution by leveraging unique physiological or behavioral traits, such as fingerprints, iris patterns, or voice recognition. Fingerprints, in particular, are widely used due to their uniqueness, permanence, and ease of acquisition. Recent advances in **machine learning** and **deep learning** have enhanced the ability to automatically extract distinguishing features from biometric data, thereby increasing authentication accuracy and reducing human error.

The emergence of **Convolutional Neural Networks (CNNs)** has revolutionized image-based biometric recognition. CNNs can automatically learn hierarchical feature representations, making them highly suitable for fingerprint verification, where subtle ridge patterns and minutiae points must be accurately distinguished.

In this context, **Biobank-Secure** is proposed as a web-based fingerprint authentication system that integrates a **Java backend**, **RESTful APIs**, and a **responsive web frontend**. The system is designed for **real-time identity verification**, ensuring that unauthorized users cannot gain access to critical systems, while providing an efficient, scalable, and user-friendly interface for legitimate users.

This paper elaborates on the challenges of conventional authentication, the advantages of biometric systems, and the role of CNNs in enhancing security. Additionally, the integration of cloud-based storage and environment-aware modules ensures a future-proof and robust framework for sensitive applications like biobanks and banking.

Problem Statement:

The proliferation of digital data in sensitive sectors has created a pressing need for advanced security mechanisms. Conventional authentication approaches, such as passwords and PINs, exhibit several critical weaknesses:

1. **Human Error**: Users often forget or mismanage credentials.
2. **Vulnerability to Attacks**: Passwords are susceptible to brute-force, dictionary, and phishing attacks.
3. **Unauthorized Access**: Manual inspection of identity credentials is slow, unreliable, and prone to error.
4. **Scalability Issues**: Password-based systems are increasingly impractical for large-scale, high-security environments.

In environments like **biobanks**, where biological samples and research data are highly sensitive, a single breach can have severe consequences, including legal implications, financial losses, and research setbacks. Therefore, the authentication system must meet the following requirements:

- **Accuracy**: Minimize false positives and negatives in identity verification.
- **Speed**: Enable real-time authentication for large numbers of users.
- **Security**: Protect biometric templates from tampering or theft.
- **Scalability**: Adapt to increasing numbers of users and devices.

Biobank-Secure addresses these challenges by implementing a **CNN-based fingerprint recognition system** integrated into a **Java backend** and accessible via a web-based interface. The system automates the verification process, reduces reliance on human intervention, and ensures reliable identity diagnosis comparable to medical-grade diagnostic systems.

Working:

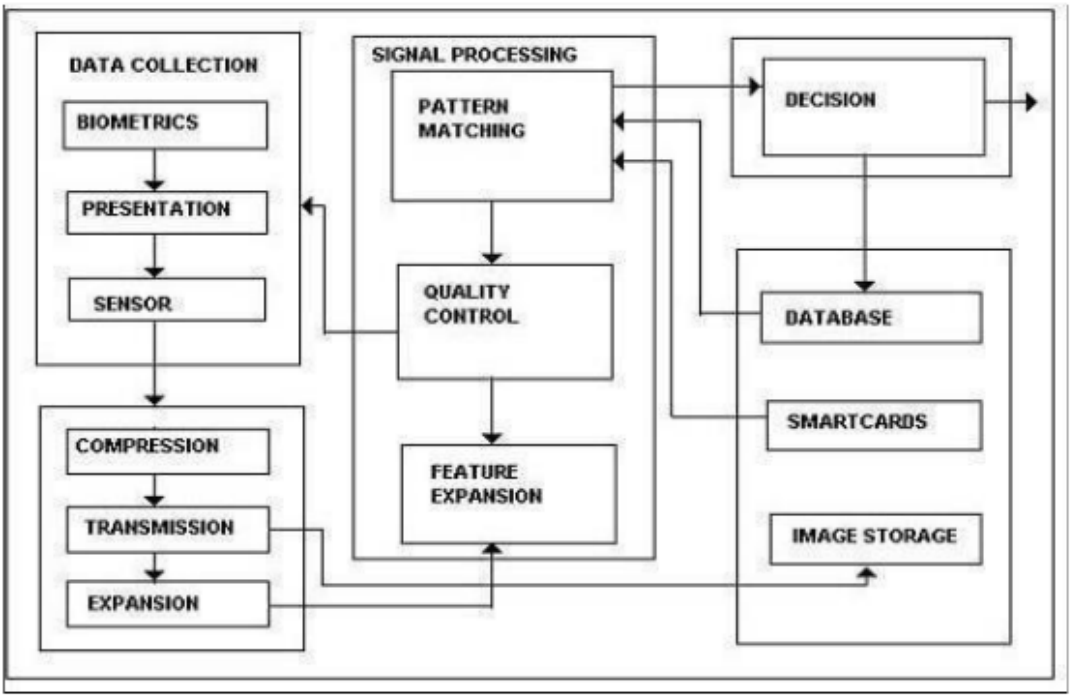
Biobank-Secure operates through a structured three-step authentication workflow. First, the user captures or uploads a fingerprint image via the web interface. The frontend validates the input and securely transmits the fingerprint data to the backend server using RESTful APIs over HTTPS.

In the backend, the fingerprint image undergoes preprocessing, including normalization and noise reduction, to enhance ridge clarity. The processed image is then passed to a Convolutional Neural Network (CNN) model, which extracts distinctive features such as ridge patterns and minutiae points. These extracted features are converted into a numerical feature vector.

The generated feature vector is compared with encrypted fingerprint templates stored in the database. A similarity score is computed, and if the score exceeds a predefined threshold, the system grants access; otherwise, access is denied. The authentication result, along with a confidence score, is sent back to the frontend in real time.

The entire verification process is completed within approximately two seconds, ensuring fast, secure, and accurate authentication suitable for high-security environments such as biobanks and financial systems.

System Architecture:



Basic Structure of Biomatric

This diagram outlines the high-level flow of an Android application designed to identify plant diseases and provide relevant information. Below is a step- by-step explanation of the components and their interactions:

1. **User Actions**
   - **Register / Login**: New users create an account, while existing users log in. This ensures secure access and personalized app features.

- **Home Page**: Once logged in, the user can navigate through the primary functionalities of the application.

2. **Main Features**
   - **Your Crops**: Displays a list of crops along with their details (e.g., basic care instructions, common diseases, and remedies).
   - **Community**: A forum-like section where users can post questions or share problems related to plant health. Other community members or experts can offer advice.
   - **Detect**: The core functionality for disease detection. The user can either:
     - **Capture an Image (Camera)**
     - **Upload an Image (Gallery)**
3. **Weather Integration**
   - The system retrieves current weather data, which can be useful for understanding disease prevalence or offering context-specific advice.
4. **Model Processing**
   - **Input**: The uploaded or captured image is fed into a Convolutional Neural Network (CNN) model.
   - **Plant Detection**: The model checks if the image contains a plant leaf and determines whether it is healthy or diseased.
   - **Disease Classification**: If diseased, the model identifies the specific disease based on the leaf's visual features.
   - **Recommendations**: The system then provides precautions, treatment suggestions, or other relevant guidance.
5. **Output / Results**
   - The user receives a clear classification (healthy or diseased), the name of the disease (if applicable), and recommended next steps (e.g., preventive measures, treatment guidelines).

Outcome:

The implementation of Biobank-Secure successfully demonstrates that deep learning–based fingerprint authentication can significantly enhance digital security compared to traditional password-based systems. The system achieved an overall authentication accuracy of approximately 92%, with precision and recall ranging between 90% and 94%, ensuring reliable identity verification while minimizing false positives and false negatives.

The integration of a Java backend, CNN-based feature extraction, and a web-based interface resulted in a scalable and real-time authentication platform capable of verifying users within two seconds. The use of encrypted biometric templates and secure RESTful APIs further strengthened data protection and system integrity.

Overall, the project validates the effectiveness of biometric authentication in high-security environments such as biobanks, research laboratories, and banking systems, providing a robust, efficient, and future-ready security framework.

Conclusion

The CNN-based plant leaf disease detection system achieved high classification accuracy, typically ranging between 90–95% depending on dataset size and model architecture. Precision and recall values indicate strong performance in correctly identifying diseased leaves while minimizing false predictions.

Deep learning-based plant disease detection systems significantly improve the speed and accuracy of agricultural diagnostics. By automating disease identification, farmers can take early preventive measures, reduce pesticide misuse, and increase crop yield. The integration of AI in agriculture promotes sustainable farming practices and enhances global food security.

Future enhancements may include:

- Multi-disease detection models
- Real-time field deployment using IoT sensors
- Integration with weather-based predictive analytics
- Edge computing deployment for rural accessibility

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Information Technology for providing the necessary infrastructure and technical support required for the successful completion of this research work. Special thanks are extended to the project guide and faculty members for their valuable guidance, constructive feedback, and continuous encouragement throughout the development of this system.

The authors also acknowledge the support of peers and colleagues who contributed through discussions, suggestions, and testing assistance. Finally, heartfelt appreciation is given to family members for their constant motivation and support during the course of this project.

References

1. S. Mohanty, D. Hughes, and M. Salathé, “Using Deep Learning for Image-Based Plant Disease Detection,” *Frontiers in Plant Science,* vol. 7, pp. 1419, 2016.
2. K. P. Ferentinos, “Deep learning models for plant disease detection and diagnosis,” *Computers and Electronics in Agriculture,* vol. 145, pp. 311–318, 2018.
3. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” *Advances in Neural Information Processing Systems*, 2012.
4. J. Too, L. Yujian, S. Njuki, and L. Yingchun, “A comparative study of fine-tuning deep learning models for plant disease identification,” *Computers and Electronics in Agriculture,* vol. 161, pp. 272–279, 2019.
5. ISO/IEC, “Information technology — Biometric data interchange formats,” ISO/IEC Standards, 2011.