BIOMETRIC SECURITY SYSTEM USING PALMPRINT RECOGNITION AND CRYPTANALYSIS UNDER DEEP LEARNING TECHNIQUES

[1] M. Sarada , [2]J. Sravani , [3]P.N.V. Kavya , [4]P.G.L. Prasanna , [5]P. Afrin

[1]Assistant Professor, Dept. of CSE - AI & ML, St.Ann's College Of Engineering & Technology, Chirala, Andhra Pradesh – 523187, India.

[2,3,4,5]U. G Student, Dept. of CSE - AI & ML, St.Ann's College Of Engineering & Technology, Chirala, Andhra Pradesh – 523187, India.

ABSTRACT

With the rapid expansion of digital platforms and online services, secure and reliable authentication mechanisms have become essential .Traditional authentication methods such as passwords, PINs, and access cards are vulnerable to security threats including theft, duplication, and unauthorized access. Although biometric systems provide improved security, commonly used techniques like fingerprint, face, and iris recognition suffer from limitations related to hygiene, environmental sensitivity, cost, and privacy. To overcome these challenges, this paper presents a palm recognition-based biometric security system using deep learning and cryptanalysis techniques. The proposed system utilizes palm images as a biometric trait due to their unique and stable patterns such as palm lines, textures, and ridges. Convolutional Neural Networks (CNN) and Deep Learning Neural Networks (DLNN) are employed to automatically extract discriminative features and accurately classify individuals. To further enhance security, cryptanalysis techniques are integrated to protect stored biometric templates from unauthorized access and attacks.

Keywords:

Palm Recognition, Biometric Security, Deep Learning, CNN, Cryptanalysis, Authentication

INTRODUCTION

In today's world, secure authentication plays a crucial role in protecting sensitive information and resources. Conventional security systems such as passwords and PINs are widely used but are highly vulnerable to hacking, sharing, and forgetting. As a result, biometric authentication systems have gained popularity due to their ability to identify individuals based on unique biological characteristics.Palm recognition is an effective biometric technique that uses the distinctive patterns present on a human palm. These patterns, including principal

lines, wrinkles, and textures, remain stable over time and are difficult to replicate. Compared to fingerprint recognition, palm recognition provides a larger surface area, leading to improved accuracy and reliability. Additionally, palm recognition can be implemented in a contactless manner, improving hygiene and user comfort. Recent advancements in deep learning have significantly enhanced biometric recognition performance. Convolutional Neural Networks enable automatic feature extraction and robust classification. However, securing biometric data remains a major concern. To address this issue, cryptanalysis techniques are incorporated to protect stored biometric templates. This paper focuses on developing a secure and efficient palm-based biometric authentication system using deep learning and cryptographic security mechanisms.

LITERATURE SURVEY

Recent advancements in biometric authentication systems have mainly focused on deep learning techniques due to their ability to achieve high accuracy and robustness. Liu et al. (2021) proposed a CNN-based biometric authentication model that effectively learns discriminative features from biometric images. While the model demonstrated improved recognition performance, it was found to be highly sensitive to variations in image quality and required a large volume of labeled training data, which limits its scalability in real-world applications . Zhang et al. (2020) developed a deep learning-based palmprint recognition system utilizing convolutional neural networks with feature embedding techniques. The system showed promising results in controlled environments; however, its performance declined significantly when tested on noisy or low-resolution palmprint images, indicating limitations in handling real-world image variations. In the domain of fingerprint recognition, Jain et al. (2019) introduced a deep CNN architecture incorporating minutiae learning for enhanced feature extraction. Although the approach improved recognition accuracy, it suffered from high computational complexity and was adversely affected by partial or distorted fingerprint samples, making it less efficient for low-resource systems.

RELATED WORK

Several biometric systems have been proposed using different modalities and with different machine learning techniques. Fingerprint-based systems are widely deployed due to their simplicity, but they face challenges such as sensor contamination and spoofing attacks. Face recognition systems using deep learning models have shown improved accuracy;

however, they raise privacy concerns and are sensitive to environmental conditions. Palmprint recognition systems have been explored using traditional image processing and machine learning techniques. Some studies employed support vector machines and k-nearest neighbour classifiers for palmprint classification. While these methods achieved moderate accuracy, their performance was limited by manual feature extraction. Recent research has focused on deep learning-based palm recognition systems using CNN architectures to automatically extract features and improve classification accuracy. Additionally, a few studies have integrated encryption and cryptographic techniques to protect biometric data. However, limited work has addressed both accurate palm recognition and strong template security together. This paper builds upon existing research by combining deep learning-based palm recognition with cryptanalysis techniques to enhance both recognition performance and data security.

EXISTING SYSTEM

Existing authentication systems include password-based methods, fingerprint recognition, face recognition, and iris scanning. Password-based systems are easy to implement but suffer from issues such as easy guessing, sharing, and forgetting. Fingerprint recognition requires physical contact, which raises hygiene concerns and reduces accuracy due to dirt, sweat, or injuries. Face recognition systems are affected by lighting conditions, facial expressions, and accessories such as masks and glasses. Iris recognition provides high accuracy but is expensive and requires specialized hardware, making it unsuitable for large-scale deployment. Moreover, many existing biometric systems lack adequate protection for stored biometric templates, making them vulnerable to data theft and attacks. These limitations highlight the need for a more secure, accurate, and user-friendly biometric authentication system.

PROPOSED SYSTEM

The proposed system introduces a palm recognition-based biometric security framework using deep learning and cryptanalysis techniques. Palm images are captured using a camera or imaging device and preprocessed to enhance image quality. Convolutional Neural Networks are used to automatically extract unique palm features, while Deep Learning Neural Networks classify individuals with high accuracy. To ensure data security, cryptanalysis techniques are applied to encrypt and protect biometric templates stored in the database. The system provides contactless authentication, improved hygiene, high robustness, and strong resistance to

spoofing attacks. Compared to existing biometric systems, the proposed approach offers enhanced security, accuracy, and reliability, making it suitable for applications such as secure access control, banking systems, and identity verification platforms.

SYSTEM ARCHITECTURE

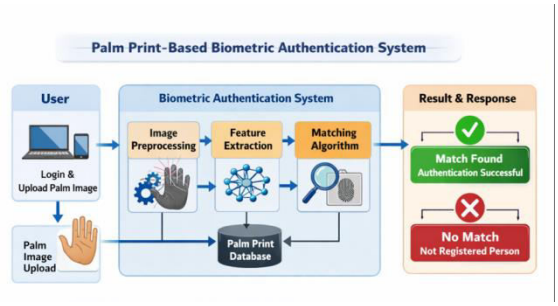

Fig1: SYSTEM ARCHITECTURE OF PALMPRINT BASED AUTHENTICATION SYSTEM

METHODOLOGY DESCRIPTION

CLIENT SIDE:

The client side represents the user interface of the biometric security system. It is developed using HTML, CSS, and JavaScript to ensure a responsive and user-friendly experience. The user first accesses a secure login page and enters valid credentials. After successful login, the user is allowed to upload a palm image through the interface for authentication purposes.

API REQUESTS AND RESPONSES:

The communication between the client and server follows RESTful architecture principles. HTTP methods such as POST are used to send login details and palm image data from the client to the server. The server processes the requests and sends structured responses indicating authentication status. JSON format is used for data exchange, and HTTP status codes are applied to clearly represent success or failure scenarios.

SERVER SIDE:

The server side is implemented using Python with the Flask framework. It follows a layered architecture to maintain clarity and scalability. The backend handles user authentication, palm image processing, and decision-making logic. Flask manages routing, request handling, and interaction between different processing modules, ensuring smooth and secure system operations.

PROCESS/AUTHENTICATION HANDLING:

Once the palm image is uploaded, it undergoes image preprocessing such as resizing ,etc . Key biometric features are then extracted from the palm image using image processing and machine learning techniques. These extracted features are compared with the stored palm print features in the database using a matching algorithm to determine identity verification.

DATABASE/DATA MANAGEMENT:

The database layer is responsible for storing registered palm images, extracted feature vectors, and user login credentials. A secure SQLite database is used to manage the data efficiently. User passwords are stored in encrypted or hashed form to enhance data protection, while biometric data is handled carefully to maintain integrity and security.

SECURITY AND USER AUTHENTICATION:

This system uses user authentication to ensure that only authorized users have access to the translation features. Passwords are hashed for security and privacy purposes.

RESULTS AND DISCUSSION

LOGIN PAGE:

This is the Secure Login Page for The Biometric Security System.To access system functions, users must first authenticate using valid credentials. It includes Create Account and Forgot Password options.It ensures authorized use and protects user data.

Fig :2 LOGIN PAGE

PALMPRINT UPLOAD PAGE BEFORE PREDICTION:

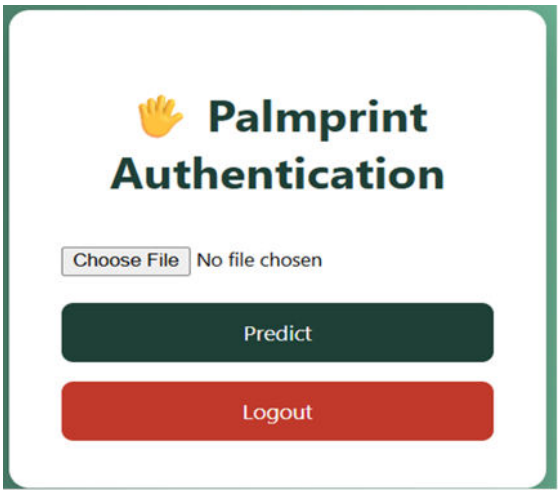

Fig3: Palmprint upload page before prediction

This is the interface before the prediction of Palmprint. After successful login, the user is prompted to upload a palm image for authentication. The uploaded image serves as the input to the biometric system and is forwarded to the backend for preprocessing, feature extraction, and matching operations.

OUTPUT PAGE FOR KNOWN USER:

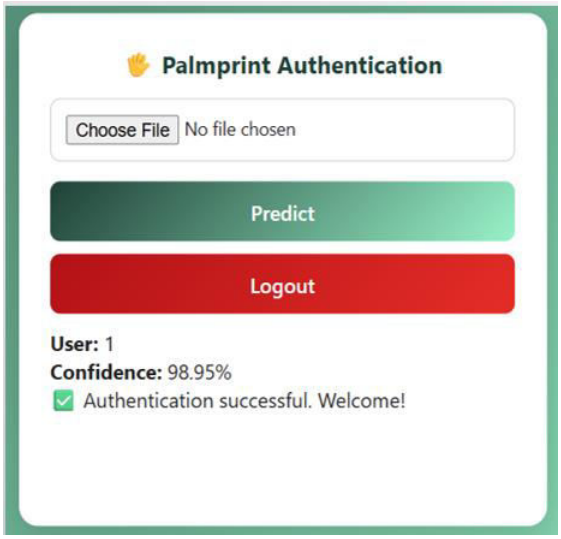

Fig 4: OUTPUT PAGE

The above image shows the system output when the uploaded palm image matches a stored palm print in the database. Upon successful matching, the system confirms the user's identity and displays an authentication success message, indicating that the user is a recognized and authorized individual.

OUTPUT PAGE UNKNOWN USER:

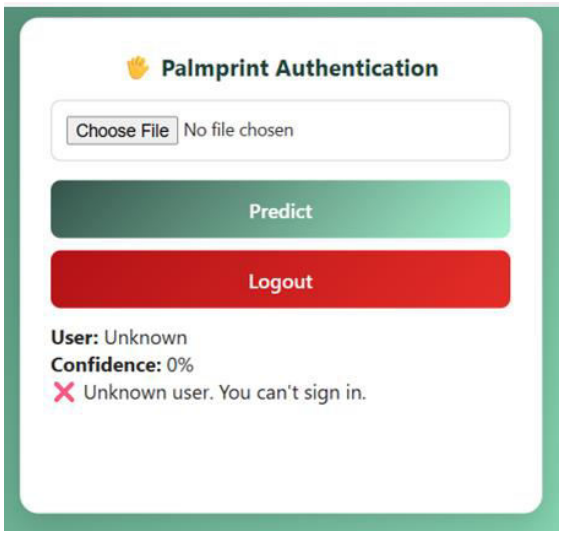

Fig5: Result page for unknown user

CONCLUSION

This paper presents a secure and efficient palm recognition-based biometric security system using deep learning and cryptanalysis techniques. The proposed system addresses the limitations of traditional authentication methods by providing accurate, contactless, and robust biometric verification. Deep learning models enable automatic feature extraction and reliable classification, while cryptanalysis ensures protection of sensitive biometric data. The experimental results confirm that the proposed approach achieves high accuracy and enhanced security compared to existing biometric systems. Due to its reliability and scalability, the system can be effectively deployed in applications such as access control, banking systems, attendance management, and identity verification. Future work may focus on real-time implementation and integration with multi-modal biometric systems to further enhance security.

FUTURE SCOPE

This palm print–based biometric security system can be enhanced in the future by integrating deep learning techniques and to improve feature extraction and matching accuracy. The system may be extended to support multimodal biometric authentication by combining palm prints with other biometric traits for higher security. Deployment on cloud platforms can enable scalability and real-time authentication for a large number of users. Mobile device compatibility can also be introduced to allow palm image capture using smartphone cameras. Expanding the dataset with diverse palm images can further improve system robustness and reliability. Advanced encryption methods

can be implemented to strengthen biometric data protection and privacy. Performance optimization can reduce processing time and support faster authentication. These enhancements would make the system suitable for high-security and real-world applications.

REFERENCE

1. H. K. Chapala, "Machine Learning based Bayesian Network Models for Reverse Engineering Data Optimization," in *2022 International Conference on Edge Computing and Applications (ICECAA)*, 2022.

2. P. N. Kumar, "Evaluation of Wireless Sensor Networks Module using IoT Approach," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2022.

3. Kong, A.; Zhang, D.; Kamel, M.A. Survey of palmprint recognition. Pattern Recognition, 2009, 42(7), 1408–1418.

4. Fei, L.; Xu, Y.; Tang, W.; Fang, J. Double-orientation coding for palmprint recognition. Pattern Recognition, 2016, 69, 178–189.

5. Zhang, L.; Zuo, W.; Zhang, D. Palmprint verification based on robust line orientation code. Pattern Recognition, 2010, 43(3), 852–869.

6. Minaee, S.; Boykov, Y.; Porikli, F.; Plaza, A.; Kehtarnavaz, N.; Terzopoulos, D. Image segmentation using deep learning: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44(7), 3523–3542.

7. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 2012, 25, 1097–1105.

8. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. Nature, 2015, 521, 436–444.

9. Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning. MIT Press, Cambridge, MA, USA, 2016.

10. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 2001, 40(3), 614–634.