VeinChain : Fingervein Authentication Using Blockchain

Thomas John
Dept. of Computer Science and Engineering
Rajagiri School of Engineering and Technology
Kochi, India

Saira Sunny George
Dept. of Computer Science and Engineering
Rajagiri School of Engineering and Technology
Kochi, India

Thomas Biju
Dept. of Computer Science and Engineering
Rajagiri School of Engineering and Technology
Kochi, India

Therese Joe
Dept. of Computer Science and Engineering
Rajagiri School of Engineering and Technology
Kochi, India

Ms. Amitha Mathew
Assistant Professor
Dept. of Computer Science and Engineering
Rajagiri School of Engineering and Technology
Kochi, India

***Abstract*—Biometric authentication systems have gained prominence as secure and efficient methods for identity verification. In this paper, we present a novel approach to finger vein authentication utilizing a portable near-infrared (NIR) imaging device integrated with blockchain technology for enhanced security and decentralization. The proposed system leverages a deep learning-based ResNet model to extract robust features from NIR-captured finger vein patterns, ensuring high accuracy and resilience against spoofing attacks. To further secure the authentication process, a blockchain network is employed to store cryptographic hashes of the vein pattern features, providing a tamper-proof and transparent ledger for authentication transactions. Experimental results demonstrate the system's high accuracy, scalability, and user privacy compliance. This integrated framework offers a secure, decentralized, and portable solution for biometric authentication, making it suitable for applications in financial services, healthcare, and secure access control.**

***Index Terms*—Biometric Authentication, Finger Vein Recognition, Near-Infrared Imaging, Blockchain, ResNet, Decentralized Security.**

I. Introduction

Biometric authentication has evolved as a crucial element in security systems due to its ability to provide unique and secure identity verification mechanisms. Traditional biometric systems, such as fingerprint and iris recognition, have proven effective but are susceptible to spoofing attacks and centralized data vulnerabilities. Finger vein recognition offers a secure alternative due to its internal feature structure, making it difficult to forge or replicate. With the rise of digital transactions and remote authentication, ensuring data security and user privacy has become paramount. Centralized authentication systems face risks such as hacking, unauthorized access, and data breaches, which can compromise user identities. Blockchain technology has emerged as a promising solution by providing decentralized and tamper-proof data storage, eliminating single points of failure. In this paper, we propose an advanced biometric authentication system that integrates a portable NIR imaging device with blockchain technology to enhance security, privacy, and decentralization. The portable NIR sensor enables convenient and high-quality image acquisition, while the deep learning-based ResNet model extracts meaningful vein features for authentication. The blockchain network further enhances security by storing cryptographic hashes of the vein patterns, ensuring the immutability and verifiability of authentication records. This approach not only mitigates the risks associated with traditional biometric authentication systems but also offers a scalable and efficient solution for secure identity verification in various applications.

II. Literature Survey

Biometric authentication has gained significant traction as a secure and reliable method for identity verification. Traditional biometric modalities such as fingerprint recognition, facial recognition, and iris scanning have been widely adopted; however, they are not without limitations. Fingerprint sensors are susceptible to spoofing through synthetic impressions, facial recognition can be deceived by high-resolution images or masks, and iris scanning, while more secure, requires expensive and intrusive hardware. These challenges have led to an increased interest in vein pattern recognition, a biometric modality that leverages the unique subcutaneous blood vessel structures of individuals.[1] Unlike fingerprints and facial features, vein patterns are internal to the body, making them inherently resistant to spoofing and environmental variations.

Vein Capturing Device Vein pattern recognition has emerged as a reliable biometric authentication method due to its resistance to forgery and environmental variations. This technology leverages the unique subcutaneous blood vessel structures of individuals, which remain stable over time. Near-Infrared (NIR) imaging is widely used for vein recognition as hemoglobin absorbs NIR light, making veins appear as dark patterns against the surrounding tissue.[1] For successful vein pattern extraction, the choice of imaging technique, camera type, and illumination circuit design plays a crucial role in ensuring high accuracy and reliability. The two primary imaging techniques for vein pattern recognition are light transmission and light reflection. In the light transmission method, NIR light passes through the finger, and a camera positioned on the opposite side captures the vein pattern. This technique provides higher contrast and better vein visibility, making it the preferred choice for this project.[2] On the other hand, the light reflection method involves capturing the light reflected from the surface of the skin, which is more susceptible to noise and external lighting conditions, leading to lower accuracy.[3] For imaging, cameras equipped with CCD or CMOS sensors are commonly used. While CMOS cameras are cost-effective and power-efficient, they have lower sensitivity to light variations, which can affect vein pattern clarity.[5] CCD cameras, in contrast, offer superior light sensitivity and produce clearer images, making them better suited for this application.[4] In this project, a modified CCD webcam is used, where the infrared filter has been removed to enhance its ability to capture vein patterns under NIR illumination. The NIR illumination circuit is a critical component in ensuring consistent and high-quality imaging. The design includes a 555 timer-based Pulse Width Modulation (PWM) circuit, which regulates the brightness of the NIR LEDs, ensuring optimal exposure in varying lighting conditions. Resistors and potentiometers control the LED current, preventing overexposure or underexposure.[1] The circuit was initially simulated in software, tested on a breadboard, and then fabricated onto a printed circuit board (PCB) for final integration into the system.

Finger Vein Recognition Based on ResNet Model Traditional machine learning approaches for vein recognition relied on handcrafted feature extraction methods such as Local Binary Patterns (LBP) and Gabor filters, but these techniques often suffered from sensitivity to noise, illumination variations, and inconsistent vein structures across different individuals. Recent advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have significantly improved the accuracy and robustness of vein recognition systems by learning hierarchical feature representations directly from raw images.[9] Residual Networks (ResNet) introduced skip connections, allowing deep networks to avoid vanishing gradients and learn more complex features. ResNet has been widely adopted in various biometric recognition tasks due to its ability to train very deep models without performance degradation.[6] In our project, ResNet was selected as the primary architecture for finger vein recognition due to its superior performance in feature extraction, robustness to variations in lighting conditions, and ability to generalize well even with limited training data. The skip connections in ResNet enable efficient gradient flow, reducing the risk of overfitting and improving convergence speed.[7] Other CNN architectures, such as deeply-fused CNNs and VGGNet, have been explored for finger vein recognition. Deeply-fused CNNs improve generalization by integrating features from multiple convolutional layers at different depths, enhancing vein pattern recognition.[8] However, while this approach provides robustness against noise and lighting variations, it lacks the efficiency and training stability of ResNet. VGGNet, on the other hand, utilizes a uniform kernel size across layers but suffers from high computational costs and the absence of skip connections, leading to vanishing gradient issues in deeper networks.[9] Compared to these architectures, ResNet demonstrates superior accuracy, stability, and computational efficiency, making it the optimal choice for our project.

Blockchain for Biometric Identity Management Traditional biometric identity systems rely on centralized databases, which pose significant security risks such as data breaches, unauthorized access, and single-point failures. To address these concerns, blockchain technology offers a decentralized and tamper-resistant solution for storing and managing biometric data securely.[10] In our project, blockchain plays a crucial role in enhancing the security and integrity of the vein-based authentication system by ensuring that biometric records are immutable and resistant to unauthorized modifications. Our system does not store raw vein images but instead extracts key feature representations from the vein patterns using a ResNet. These extracted features are then hashed and stored on the blockchain, ensuring that biometric data remains encrypted and unalterable. When a user attempts authentication, a new vein image is captured and processed through the CNN, generating a feature hash that is compared with the stored records on the blockchain. This eliminates the risks associated with centralized storage, as no single entity has control over the entire database, making it highly secure against attacks. Additionally, smart contracts are integrated into the system to automate the authentication process. When a user requests verification, the smart contract cross-checks the new hash with the stored data, allowing for a decentralized and trustless authentication mechanism. This ensures that the authentication process remains transparent and secure without the need for intermediaries. Furthermore, blockchain's inherent cryptographic protection ensures that even if a node is compromised, the integrity of biometric data remains intact, as any unauthorized modifications would be rejected by the consensus mechanism. By leveraging blockchain technology, our project ensures a decentralized, secure, and tamper-proof biometric authentication system. The integration of smart contracts and cryptographic hashing enhances security while eliminating the vulnerabilities associated with centralized databases.[11] Although the current implementation is optimized for a moderate number of nodes, future scalability concerns can be addressed by incorporating advanced consensus mechanisms such as Delegated Proof of Luck (DPoL), which offers improved efficiency in handling larger networks.[12]

III. Objectives and Scope

The primary objective of this research is to develop and evaluate a finger vein authentication system that integrates blockchain technology for enhanced security. The specific goals include:

1) Designing a portable NIR-based finger vein imaging system to capture high-quality vein patterns for biometric authentication.
2) Implementing a deep learning-based feature extraction approach using ResNet-50 to extract vein features for reliable authentication.
3) Developing a decentralized authentication framework utilizing blockchain technology to prevent identity fraud and unauthorized access.
4) Analyzing the performance of the authentication system under different similarity thresholds by computing confusion metrics such as accuracy, precision, recall, and F1-score.
5) Optimizing computational efficiency by evaluating authentication time and gas usage in blockchain transactions.

IV. Methodology

The proposed method presents a secure and non-tamperable finger vein authentication system by integrating a portable hardware-based NIR imaging device , deep learning-based feature extraction, and blockchain authentication.

A. *Hardware Development:*

The methodology for this project begins with hardware development, where a custom-designed near-infrared (NIR) imaging system is implemented. The imaging device consists of NIR LEDs (850nm–940nm) that illuminate the veins, a modified webcam configured for IR image capture, and a black-box enclosure to minimize external light interference. Correct finger positioning is ensured to achieve optimal imaging conditions.

Following image acquisition, the preprocessing stage is performed to enhance the visibility of finger vein patterns. This includes Region of Interest (ROI) extraction to focus on the vein structures, rotation alignment to correct standardization errors, resizing and normalization to maintain uniformity across samples, and contrast enhancement using CLAHE to improve local contrast without excessive enhancement. These preprocessing steps help ensure high-quality input data for feature extraction.

Following image acquisition, the preprocessing stage is performed to enhance the visibility of finger vein patterns. This includes Region of Interest (ROI) extraction to focus on the vein structures, rotation alignment to correct standardization errors, resizing and normalization to maintain uniformity across samples, and contrast enhancement using CLAHE to improve local contrast without excessive enhancement. These preprocessing steps help ensure high-quality input data for feature extraction.

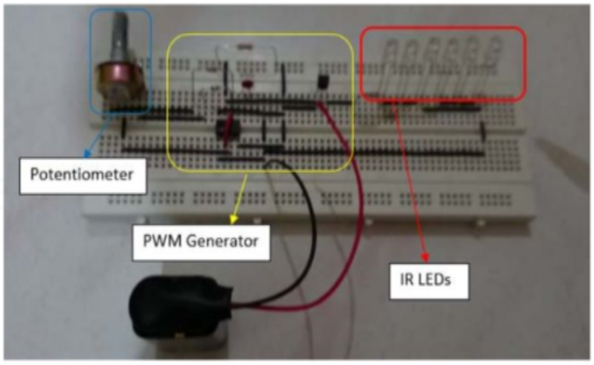

Fig. 1. *NIR LED Circuit Setup*

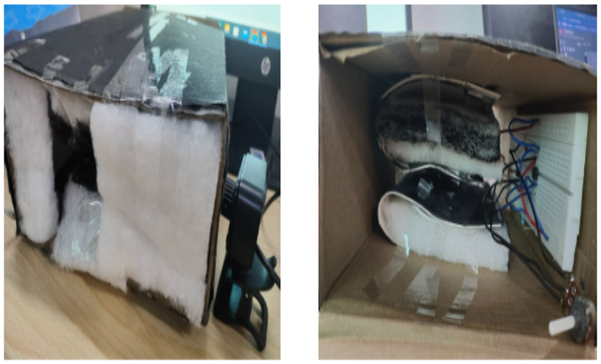

Fig. 2. *Blackbox hardware Setup*

B. *Feature Extraction Using ResNet-50 :*

A deep learning-based approach is employed for feature extraction using a ResNet-50 model. The model, pre-trained on ImageNet, is fine-tuned for finger vein recognition by replacing its default fully connected layer with a 128-dimensional embedding layer. This transformation consists of a dimensionality reduction step, non-linearity through ReLU activation, and batch normalization to maintain feature stability. The extracted feature vector effectively represents the vein pattern in a compact form, making it suitable for authentication.

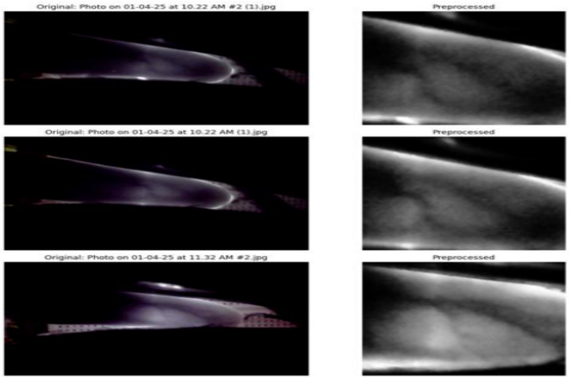
Original: Photo on 01-04-25 at 10.22 AM #2 (1).jpg
Preprocessed
Original: Photo on 01-04-25 at 10.22 AM (1).jpg
Preprocessed
Original: Photo on 01-04-25 at 11.32 AM #2.jpg
Preprocessed

Fig. 3. *Preprocessing using CLAHE*

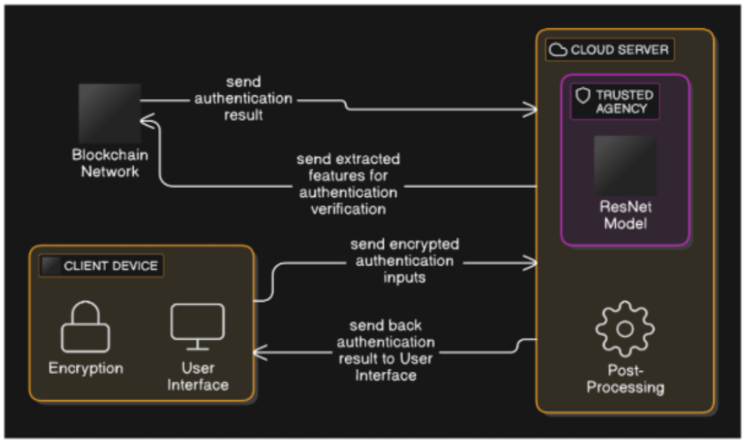
CLOUD SERVER
send authentication result
Blockchain Network
TRUSTED AGENCY
send extracted features for authentication verification
ResNet Model
CLIENT DEVICE
send encrypted authentication inputs
Encryption
User Interface
send back authentication result to User Interface
Post-Processing

Fig. 4. *Architecture Diagram*

C. *Secured Storage on Blockchain Technology:*

To ensure secure storage and decentralized verification, the extracted biometric feature vectors are stored on a private Ethereum blockchain. Smart contracts, implemented in Solidity, manage user enrollment and authentication by associating each user with a unique identifier and encrypted biometric template. The system employs AES encryption in CBC mode to encrypt feature vectors before storage, ensuring data privacy and protection against unauthorized access. Stored data is indexed by user IDs, with blockchain-based immutability preventing tampering.

D. *Frontend App:*

VeinChain, our finger vein authentication system provides a user-friendly interface for secure biometric authentication. It allows users to capture finger vein images using a NIR-based imaging device, submit them for processing, and receive authentication results in real-time. The website is designed with a clean and intuitive UI, featuring a login system, camera module, and authentication status display. It communicates with the backend (Flask) to handle image processing, feature extraction (ResNet-50), and blockchain-based verification, ensuring a secure and decentralized authentication process.

E. *Authentication Utilizing Cosine Similarity:*

User authentication is conducted using cosine similarity matching between newly acquired feature vectors and stored biometric templates. The query image undergoes the same preprocessing and feature extraction steps as during enrollment. The extracted feature vector is encrypted using AES encryption before storage. Upon retrieval, the stored biometric templates are decrypted, and cosine similarity is computed between the extracted feature vector and stored templates. If the similarity score exceeds a threshold of 90 percent, access is granted; otherwise, authentication is denied. This method ensures an optimal balance between security and usability while minimizing false acceptance rates.

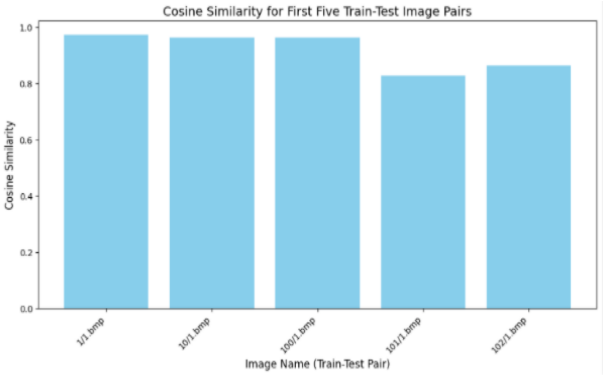

Fig. 5. *Cosine Similarity*

V. Results and Discussions

Performance Evaluation with Different Similarity Scores: Performance evaluation is conducted to assess the system's effectiveness using standard biometric verification metrics, including accuracy, precision, recall, Equal Error Rate (EER), and Receiver Operating Characteristic (ROC) curve analysis. These evaluations validate the system's reliability, ensuring its feasibility for real-world applications.

A. *Confusion Metrics for Similarity Score 90*

Metric	**Value**
True Positive (TP)	152
False Positive (FP)	13
False Negative (FN)	68
True Negative (TN)	207

TABLE I
Confusion Matrix Values for Similarity Score 90

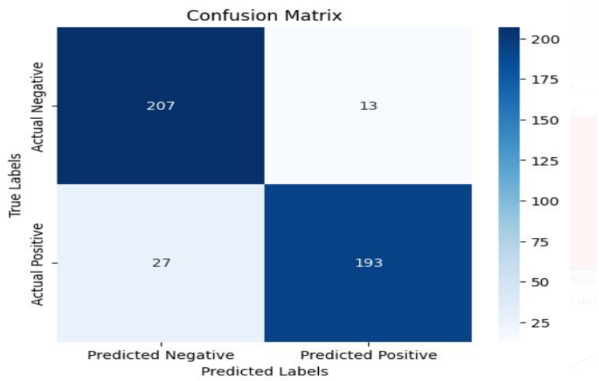

Fig. 6. Confusion Metrics for Similarity Score 90

B. *Confusion Metrics for Similarity Score 91*

Metric	**Value**
True Positive (TP)	137
False Positive (FP)	0
False Negative (FN)	83
True Negative (TN)	217

TABLE II
Confusion Matrix Values for Similarity Score 91

Metric	Value
Accuracy	80.45%
Precision	97.86%
Recall	62.27%
F1 Score	0.7611
False Positive Rate	1.36%
Avg Authentication Time	0.1169 sec
Avg Gas Used	101920.55

TABLE III
PERFORMANCE METRICS FOR SIMILARITY SCORE 91

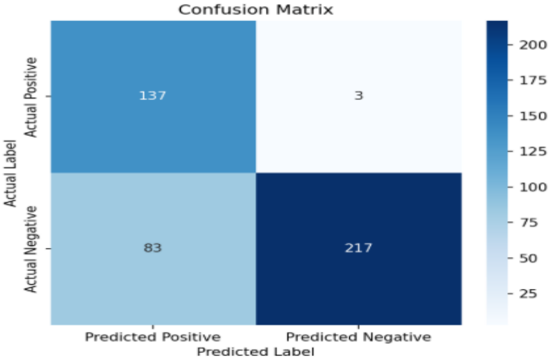

Fig. 7. Confusion Metrics for Similarity Score 91

C. Confusion Metrics for Similarity Score 92

Metric	Value
True Positive (TP)	117
False Positive (FP)	3
False Negative (FN)	103
True Negative (TN)	217

TABLE IV
CONFUSION MATRIX VALUES FOR SIMILARITY SCORE 92

Metric	Value
Accuracy	75.91%
Precision	97.5%
Recall	53.18%
F1 Score	0.6882
False Positive Rate	1.36%
Avg Authentication Time	0.1130 sec
Avg Gas Used	101920.10

TABLE V
PERFORMANCE METRICS FOR SIMILARITY SCORE 92

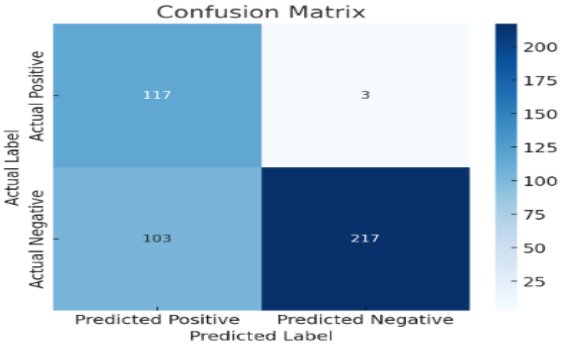

Fig. 8. Confusion Metrics for Similarity Score 92

D. Confusion Metrics for Similarity Score 89

Metric	Value
True Positive (TP)	167
False Positive (FP)	0
False Negative (FN)	53
True Negative (TN)	198

TABLE VI
CONFUSION MATRIX VALUES FOR SIMILARITY SCORE 89

Metric	Value
Accuracy	82.95%
Precision	88.36%
Recall	75.91%
F1 Score	81.66%
False Positive Rate	1.70%
Avg Authentication Time	0.0936 sec
Avg Gas Used	101921.25

TABLE VII
PERFORMANCE METRICS FOR SIMILARITY SCORE 89

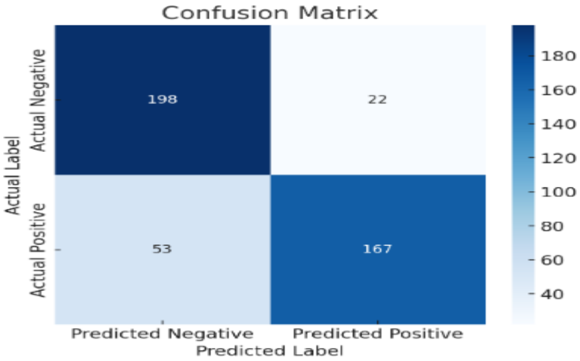

Fig. 9. Confusion Metrics for Similarity Score 89

The comparison of different similarity scores reveals that a similarity score of 90 provides the best balance between precision and recall, leading to optimal authentication performance. This suggests that 90 is the most effective threshold for ensuring reliable biometric verification while maintaining high accuracy.

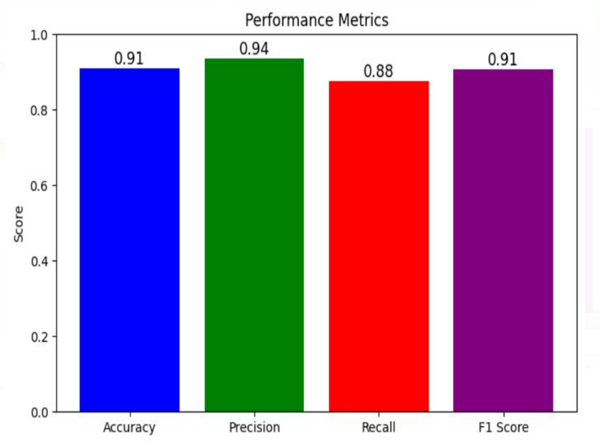

Fig. 10. Performance Metrics for Similarity Score 90

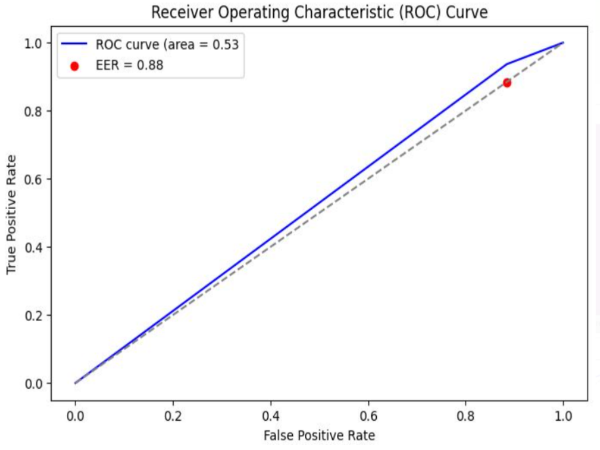

Fig. 11. ROC Curve for Cosine Similarity 90

VI. Conclusion

This paper presents an advanced and decentralized finger vein authentication system that integrates a portable NIR imaging device, deep learning-based feature extraction, and blockchain technology. Unlike conventional systems that rely on centralized databases, our approach eliminates single points of failure by leveraging a private Ethereum blockchain for secure and tamper-proof storage of biometric templates. The proposed methodology also improves feature extraction accuracy by fine-tuning a ResNet-50 model with a compact embedding layer, ensuring better recognition while reducing computational complexity. Additionally, the use of AES encryption for feature vector storage enhances data privacy, addressing a key limitation of many existing biometric authentication frameworks. Furthermore, the system achieves high security and usability by setting an optimal cosine similarity threshold, reducing false acceptance rates while maintaining robust performance. Future improvements will focus on real-time optimization, expanding the dataset for increased generalization, and exploring multi-modal biometrics for enhanced security and reliability in practical applications.

VII. References

[1]A. Syafeeza, L. Kwan, K. Syazana-Itqan, H. NA, W. Saad, and Z. Manap, “A low cost finger-vein capturing device,” 2006.

[2]Shaheed K, Liu H, Yang G, Qureshi I, Gou J, Yin Y. A systematic review of finger vein recognition techniques. Information. 2018 Aug 24;9(9):213.(Light trans)

[3]Zhang Z, Zhong F, Kang W. Study on reflection-based imaging finger vein recognition. IEEE Transactions on Information Forensics and Security. 2021 Jul 28;17:2298-310.(Light Reflection)

[4]Titrek F, Baykan ÖK. Finger vein recognition by combining anisotropic diffusion and a new feature extraction method. Traitement du Signal. 2020.(CCD)

[5]Huang Q, Hu K, Zhou P, Luo Y, Wu L. Design of finger vein capturing device based on ARM and CMOS array. In2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) 2018 May 25 (pp. 193-196). IEEE.(CMOS)

[6] W. Z. H. W. Zhibo Zhang, Guanghua Chen, “Finger vein recognition based on resnet with self-attention,” ResearchGate, 2023, available at: https://www.researchgate.net/publication/376948829 Finger Vein Recognition Based on ResNet with Self-Attention.

[7]Xu, Hong, et al. ”A novel deep learning finger vein segmentation algorithm for identification and recognition.” (2022).(Resnet2)

[8]Deeply Fused- Boucherit I, Zmirli MO, Hentabli H, Rosdi BA. Finger vein identification using deeply-fused Convolutional Neural Network. Journal of King Saud University-Computer and Information Sciences. 2022 Mar 1;34(3):646-56.(Deeply fused comparison)

[9]H. Al-Shazly, C. Linse, E. Barth, and T. Martinetz, “Finger vein recognition using deep learning and transfer learning,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 8, pp. 3226–3236, 2020.(CNN General)

[10] H. Garg and M. Dave, “Blockchain-based biometric identity management,” Journal of Blockchain Research and Applications, vol. 12, pp. 45–60, 2023.(Blockchain Base)

[11]Safety and Security- Barka E, Al Baqari M, Kerrache CA, Herrera-Tapia J. Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records. Journal of Sensor and Actuator Networks. 2022 Dec 13;11(4):85.(Security)

[12] H. Kim, W. Kim, Y. Kang, H. Kim, and H. Seo, “Post-quantum delegated proof of luck for blockchain consensus algorithm,” Applied Sciences, vol. 14, no. 18, p. 8394, 2024.(Future Scaling)