Volume: 14 Issue: II Month of publication: February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77708

Palm-Based Bio-Metric Authentication Framework: Secure Contactless Payments

Abhijith K[1], Mrs. Divya P[2]
[1]MCA Scholar, [2]Assistant Professor, Department of MCA, Nehru College Of Engineering And Research Centre

***Abstract:** The increasing popularity of digital payment systems has raised concerns about the security of authentication, privacy, and trust. Traditional methods like passwords, personal identification numbers, and cards are still susceptible to fraud, theft, and usability issues. Biometric authentication has been identified as a potential substitute, with palm-based biometric systems, specifically palm vein biometric systems, offering improved security through contactless functionality and spoofing resistance. This paper introduces a trust-focused conceptual framework and system design for palm biometric payment systems, taking a system-level engineering approach that combines principles of biometric sensing, secure payment processing, and governance- focused adoption. The proposed conceptual framework for palm biometric payments organises the system as a multi-layered socio-technical system, including biometric sensing, authentication security, payment processing, and trust management. In contrast to purely algorithmic research, this study takes a system design approach, highlighting architectural choices, privacy- focused data management, and scalability needs that are essential for practical implementation. The analysis illustrates how palm biometric payment systems can effectively mitigate the major shortcomings of current digital payment authentication systems while meeting regulatory and ethical requirements. By connecting biometric engineering with system design and technology adoption needs, this research offers a holistic basis for future studies and the development of secure.*

***Keywords:** Bio-metric authentication, Bio-metric security, Contactless payment, Digital payments, Palm biometrics, Palm biometric authentication, Smart systems, System architecture.*

I. INTRODUCTION

The financial sector across the globe is experiencing a paradigm shift due to the rapid evolution of financial technology, mobile computing, cloud infrastructure, and artificial intelligence. Digital payment systems like mobile wallets, contactless cards, and online banking systems have become an essential part of the economic system. Although these technologies provide improved convenience and accessibility, they also pose serious security and privacy concerns. The traditional authentication systems, including passwords, PIN s, one-time passwords (OTPs), and physical cards, are inherently challenged by their dependence on remembered secrets or transferable tokens. These systems are susceptible to phishing, credential stuffing, skimming, shoulder surfing, and device theft. As Cybercrime evolves in sophistication, financial institutions are finding it increasingly hard to strike a balance between security and usability. Palm biometric authentication, especially palm vein biometric authentication, is a promising alternative. Palm veins are biometric characteristics that are not only unique to each individual but also reside inside the human body and are imaged using infrared technology, making them extremely difficult to counterfeit or manipulate at the surface level. Although pilot projects have shown the viability of palm- based payment systems in retail and transportation infrastructure, their adoption is still in its infancy. One of the most important drawbacks of existing research on palm biometric payment systems is that they are treated in a disjointed manner. Technical research on palm biometric payment systems tends to focus on accuracy and image processing, while behavioural research tends to concentrate on user acceptance and trust. There is a need for a system-level framework that encompasses biometric engineering, secure payment system design, and design principles for adoption. This paper aims to fill this void by proposing a conceptual framework and system design for palm biometric payment systems.

II. RELATED WORK AND BACKGROUND

A. Bio-Metric Authentication In Payment Systems

Biometric authentication systems use the unique physiological and behavioural features of individuals for identification. In payment systems, bio-metrics. improve security with less friction for users. Biometric characteristics that are resistant to spoofing attacks are those that are internal, such as veins, as opposed to external characteristics such as fingerprints or facial images, which can be copied using high- resolution images or molds. Palm vein bio-metrics. uses near-infrared (NIR) or infrared (IR) imaging to capture the subcutaneous vein patterns. Haemoglobin absorbs infrared light, which makes it possible to clearly view the vein patterns. Vein patterns are stable and less affected by the surface, making them ideal for secure authentication.

B. Palm Bio-Metrics: Technical Evolution

Early palm biometric systems were centred on palmprint texture analysis and line-based and texture- based feature extraction. More contemporary methods have incorporated palm vein imaging for enhanced robustness and anti-spoofing performance. Hybrid biometric systems that combine palmprint and palm vein features have shown enhanced recognition performance by exploiting complementary information. Recent advances in deep learning and computer vision have further improved biometric recognition performance. Vision transformers and convolution neural networks have been used for vein recognition, showing high accuracy even in the presence of varying illumination and user behaviour.

C. User Acceptance, Trust And Governance

However, technical performance is not a sufficient criterion for adoption. Palm biometric payment studies show that perceived usefulness, ease of use, and trust are important factors in influencing user intention, often overshadowing perceived risks when the system is perceived as secure and convenient. On a wider note, biometric systems are associated with privacy, surveillance, and data governance issues. Biometric media governance research highlights the significance of regulatory frameworks, transparency, and ethical handling of data to ensure public trust

III. PROBLEM STATEMENT AND RESEARCH GAP

Despite the technical maturity that palm biometric technologies have reached, their application in large- scale payment systems is still limited. The existing literature and applications demonstrate several structural and conceptual gaps that currently impede their widespread adoption and long-term viability.

The existing literature and applications tend to employ a fragmented system design paradigm, where separate system elements, such as biometric sensing, feature extraction algorithms, authentication modules, or payment processing modules, are designed and analysed in isolation. Although these studies and applications make significant technical contributions, they tend to neglect the analysis of these system elements in the context of a holistic, end-to-end payment system. This can result in scalability, maintainability, and overall system resilience issues in practical applications.

Another critical shortcoming is the lack of system-level integration of trust, security, and governance issues. The existing literature tends to focus primarily on biometric accuracy and performance analysis, while other issues, such as data governance frameworks, consent management, regulatory issues, and long-term protection of sensitive biometric data, are addressed to a much lesser extent.

Moreover, system-level frameworks that consider real-world deployment constraints are still limited. Real-world considerations like infrastructure variability, deployment and management expenses, compatibility with existing payment systems, and reliability in high-traffic or resource-scarce settings are still not well-represented. This leads to a continuous gap between experimental systems developed in a controlled environment and scalable systems that can support real-world smart payment systems.

Most existing works lack an interdisciplinary approach that relates engineering design with user adoption models, ethics, and sociology-technical aspects. Payment systems are inherently multidisciplinary, involving technology, human behaviour, and trust. A treatment of these aspects in separate domains restricts the ability of proposed solutions to gain widespread acceptance and usage.

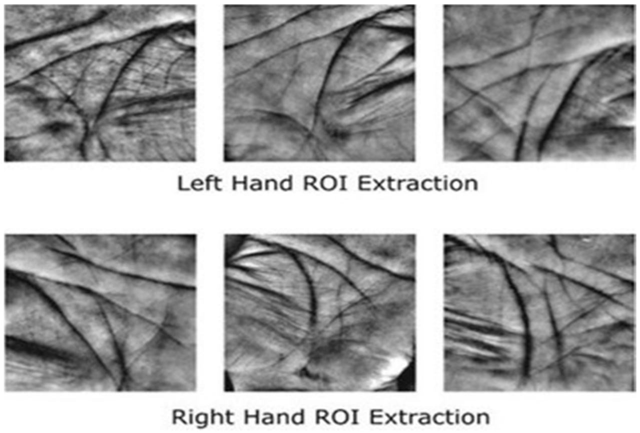
To overcome the above limitations, this paper presents a unified conceptual framework and system design for palm biometric payment systems. The proposed solution integrates biometric sensing, intelligent feature processing, secure payment authorisation, and governance aspects in a unified and extensible manner. By incorporating principles of applied computing with trust, usability, and adoption aspects, the proposed framework aims to facilitate secure, scalable, and user-friendly deployment of palm biometric payment systems in real-world smart settings.

IV. PROPOSED CONCEPTUAL FRAMEWORK

The proposed framework conceptualises palm biometric payment systems as a multi-layer sociology- technical system, comprising four interdependent layers.

A. Bio-Metric Sensing And Feature Layer

The biometric sensing and feature layer is tasked with the acquisition of high-quality palm images and the conversion of this data into a trustworthy biometric feature. Palm images are acquired through the use of infrared or near-infrared sensors, which allow the observation of both surface and subsurface vein patterns, as well as surface palm details. Prepossessing techniques such as noise removal, contrast adjustment, and geometric correction are employed to reduce the effects of lighting, hand placement, and environmental factors. Region-of-interest extraction is used to isolate the region of interest in the palm, ensuring proper alignment of the extracted features. Feature representation methods are used to encode both structural and textural information, while liveliness detection and subsurface imaging provide robust spoofing and presentation attack resistance.


Left Hand ROI Extraction

Right Hand ROI Extraction

Fig.1 Vein ROI Extraction

B. Authentication and Security Layer

The authentication and security component is tasked with the responsibility of authenticating the identity of the user and protecting the sensitive biometric data. The palm features are converted into secure biometric templates, which are encrypted using advanced cryptographic techniques before they are stored. Template protection techniques, such as cancellable biometrics. or secure hashing, are used to ensure that the raw biometric characteristics are not reversely reconstructed in case the data is breached. The storage of the data is also made secure using access-controlled databases and hardware-protected security modules. When authenticating, the encrypted templates are compared using secure comparison protocols to ensure that the biometric data is not revealed in plaintext.

C. Payment Processsing And Integration Layer

The payment processing and integration layer connects the biometric authentication subsystem with existing financial infrastructures, including banking networks, digital wallets, and third-party payment gateways. Once user identity is verified, this layer securely transmits transaction requests using standardized financial protocols and encrypted communication channels. Cloud-based architectures play a critical role in enabling scalability, fault tolerance, and high availability, allowing the system to handle large transaction volumes with minimal latency. Application programming interfaces (APIs) facilitate seamless interoperability with legacy payment platforms while supporting real-time transaction validation and settlement. By abstracting payment logic from biometric processing, this layer ensures flexibility, maintainability, and efficient integration within heterogeneous financial ecosystems.

D. User Trust And Governance Layer

The user trust and governance layer is concerned with ensuring that palm biometric payment systems are designed and function in a transparent, ethical, and legal manner. The layer implements privacy by design principles such as user consent management, purpose limitation, and data minimization. Legal compliance with data protection laws and biometric governance guidelines is also integrated into the system functionality through audit trails, access management, and policy enforcement. Transparency practices such as user disclosure and biometric data management further enhance user trust. The layer is important because it acknowledges the fact that biometric payment systems are not isolated systems but operate in a complex legal, cultural, and social environment and are therefore critical to user acceptance and sustainability.

V. SYSTEM ARCHITECTURE DESIGN

The architecture follows a layered approach in which each module performs a distinct function while interacting seamlessly with adjacent components. This modularity enhances maintainability, flexibility, and real-world deployability across heterogeneous smart environments.

A. Input And Acquisition Module

The input and acquisition module is tasked with acquiring palm biometric information in a contactless fashion through the use of infrared (IR) or near-infrared (NIR) sensors. The sensors are used to illuminate the palm, allowing for the observation of the internal vein structures as well as the external characteristics of the palm in a non-contact fashion. The module is intended to be robust to variations in the size of the hand, orientation, and distance from the sensor, allowing for easy user interaction. The real-time capture techniques used in the module are intended to facilitate rapid capture while also allowing for liveness detection via subsurface imaging.

B. Preprocessing And Feature Extraction Module

The preprocessing and feature extraction module is responsible for the conversion of raw palm images into biometric features that can be used for secure authentication. The preprocessing steps involve noise removal, contrast enhancement, geometric normalization, and alignment, which counteract the effects of lighting variations, motion blurs, and varying hand positions. Region-of-interest extraction identifies the regions of interest in palm images that hold stable biometric information. Sophisticated feature extraction algorithms represent the structural and textural information of palm veins or prints using compact numerical vectors. These feature vectors strike a balance between expressiveness and computational complexity, allowing for precise matching with minimal data size.

C. Authentication And Matching Module

The authentication and matching module is responsible for identity verification through the comparison of live biometric templates with reference templates stored securely. The process of matching involves the use of algorithms that calculate similarity scores based on predefined thresholds to establish the results of the authentication process. To ensure the security of the sensitive biometric data, the comparison process is carried out through encrypted or privacy-preserving schemes that prevent the templates from being revealed during the comparison process. The module is capable of handling one-to- one verification and one-to-many identification, depending on the system requirements. Through the balancing of accuracy and speed, this module allows for fast and accurate identity verification, which is central to the palm biometric payment system.

D. Transaction And Payment Module

The transaction and payment module directly interacts with financial infrastructure systems to process and authorize payments after successful biometric verification. The transaction and payment module interacts with financial infrastructure systems, payment wallets, or third-party payment services using standardized and secure communication protocols. The transaction request is encrypted and processed in real-time to ensure confidentiality and integrity of the payment process. Cloud deployment ensures low- latency processing, high availability, and dynamic scaling to handle peak transaction volumes. The transaction and payment module promotes interoperability with existing payment systems while facilitating seamless integration with smart commerce ecosystems.

E. Data Management Module

The data management module controls the secure storage, access, and management of biometric templates and transaction data. The biometric data is all encrypted and stored with controlled access to avoid misuse. The raw biometric images are deleted after the extraction process to avoid any privacy issues, while the biometric templates are stored only for authorized use.

The module provides data lifecycle management functions such as updates, revocation, and deletion of data in line with data privacy laws. Through the controlled retention of data and transparency, the module ensures long-term security and trust in the palm biometric payment system.

VI. SECURITY, PRIVACY, STANDARDS ALIGNMENT

The proposed palm biometric payment system is designed with clear adherence to international security and privacy standards, ensuring lawful, ethical, and trustworthy operation. Following the General Data Protection Regulation (GDPR), the proposed system follows privacy-by-design and privacy-by-default approaches, ensuring data minimization, purpose limitation, and user-controlled consent. The biometric data is processed only for authentication and payment authorization purposes, with well-defined procedures for enrollment, revocation, and erasure, thus ensuring data subject rights for informed consent and the right to be forgotten.

From the biometric protection point of view, the framework is compliant with ISO/IEC 24745, which requires the secure processing of biometric data through template protection, irreversibility, and unlinkability. The raw palm images are deleted after feature extraction, and only protected biometric templates are stored in encrypted form. Template revocability procedures ensure that compromised biometric references can be revoked and reissued without compromising the underlying physiological characteristics.

TABLE 1
RISKS AND MITIGATION STRATEGIES

THREATS / RISKS	MITIGAGTION STRATEGY
Exposure or leakage of biometric data	Biometric templates are stored exclusively in encrypted form, while raw palm images are permanently discarded immediately after feature extraction to reduce attack surface and data sensitivity
Permanent compromise of biometric identifiers	The system employs cancellable and revocable biometric templates, allowing compromised references to be invalidated and reissued without revealing the underlying physiological traits
Unauthorized secondary use of biometric information	Purpose limitation is enforced through strict access control mechanisms and comprehensive audit logging to ensure biometric data is used solely for authorized authentication purposes
Identity spoofing and replay attacks	Liveness detection mechanisms, secure biometric matching protocols, and encrypted communication channels are used to prevent impersonation and replay-based attacks
Lack of user trust and transparency	Explicit consent mechanisms are integrated into enrolment and authentication workflows, allowing users to control bio-metric registration, usage scope, and data deletion
Regulatory non-compliance	Governance policies, compliance monitoring, and automated policy enforcement are embedded at the system level to ensure continuous adherence to legal and biometric data protection requirements

VII. APPLICATIONS

Palm biometric payment systems offer a versatile and scalable solution that can be deployed across a wide range of real-world environments. By enabling secure, contactless, and identity-driven transactions, such systems align well with the requirements of modern smart infrastructures. In retail and e-commerce environments, palm biometric payments can significantly streamline checkout processes by eliminating the need for physical cards, mobile devices, or memorised credentials. Customers can complete transactions through a simple palm scan, reducing queue times and improving overall shopping experience. For merchants, this approach minimises fraud related to stolen cards or compromised credentials while supporting seamless integration with existing point-of-sale systems and digital payment platforms.

In public transportation systems, palm biometric authentication can enable ticket less travel and automated fare collection. Passengers can be authenticated at entry and exit points using palm scans, allowing fares to be calculated and charged automatically. This reduces congestion at ticket counters, enhances operational efficiency, and supports high-throughput environments such as metro stations and bus terminals.

In healthcare billing and administration, palm biometric payment systems can securely link patient identity with billing records and insurance information. This reduces administrative overhead, prevents identity-related billing errors, and ensures that payments and services are accurately attributed to the correct individual while maintaining privacy and compliance with healthcare data regulations

Within smart city services, palm biometric payments can support integrated access to public services such as utilities, government facilities, parking, and community programs. By functioning as a unified digital identity mechanism, the system enables secure and convenient access across multiple services, contributing to more efficient, inclusive, and user-centric smart city ecosystems.

VIII. ADVANTAGES & DISADVANTAGES

A. Advantages

1) High resistance to spoofing and forgery: palm biometric systems—particularly palm vein recognition—utilise internal physiological characteristics, which are inherently more secure than surface-level bio-metrics. Since vein patterns are located beneath the skin and captured using infrared imaging, they are extremely difficult to replicate using photographs, moulds, or synthetic artefacts. This significantly reduces the risk of spoofing attacks compared to fingerprint or facial recognition systems, which are increasingly vulnerable to deepfakes and replica-based fraud.

2) Contactless and hygiene authentication: palm biometric payment systems enable fully contactless authentication, requiring users only to hover their hand above a scanner. This feature gained prominence during and after the covid-19 pandemic, where hygiene and minimal physical contact became critical factors influencing technology adoption. Contactless interaction also reduces wear and tear on sensors, improving long-term system reliability.

3) Improved user convenience and transaction efficiency: by eliminating the need for passwords, pin s, or physical cards, palm biometric payments significantly reduce user effort and transaction time. Studies on user acceptance indicate that perceived ease of use and perceived usefulness strongly influence behavioural intention, making palm bio-metrics. Particularly attractive in high-frequency payment environments such as retail stores and public transportation systems.

4) Stability and consistency of biometric features: palm vein patterns exhibit long-term stability and are minimally affected by external factors such as minor injuries, skin dryness, dirt, or ageing. This stability contributes to consistent recognition performance across repeated transactions, reducing false rejection rates and improving overall system reliability.

5) Enhanced trust through strong security perception: acceptance studies demonstrate that users tend to prioritise trust and perceived security over perceived risk when evaluating biometric payment technologies. The invisibility and internal nature of palm vein data often create a stronger psychological perception of security, which positively influences adoption intention when privacy safeguards are clearly communicated.

6) Suitability for multi-domain deployment: palm biometric payment systems have been successfully piloted and deployed in retail, transportation, and access-controlled financial services, demonstrating their scalability. Integration with cloud-based payment infrastructures enables high availability and rapid transaction processing, making the technology suitable for smart cities and digital economies.

B. Disadvantages

1) High initial deployment and hardware costs: palm vein authentication requires *specialised infrared imaging sensors*, which are more expensive than conventional fingerprint scanners or cameras used for facial recognition. This increases initial infrastructure costs, particularly for small retailers or developing regions, potentially slowing widespread adoption.

2) Dependence on centralised data storage: many palm biometric payment implementations rely on *centralised cloud storage* for biometric templates. While this enables scalability, it also introduces single points of failure and increases exposure to large-scale data breaches if security mechanisms are insufficiently robust.

3) Limited public awareness and familiarity: compared to fingerprint or facial recognition, palm biometric payment systems are still relatively unfamiliar to the general public. Lack of awareness can result in hesitation or resistance during early adoption phases, particularly among users with low technological literacy or heightened privacy sensitivity.

4) Regulatory and ethical uncertainty: biometric regulations vary significantly across regions. In some jurisdictions, legal frameworks governing biometric data collection and processing remain underdeveloped or ambiguous. This regulatory uncertainty poses challenges for cross-border deployment and may limit adoption in regions with strict data protection laws.

5) Environmental and operational constraints: although more robust than external bio-metrics., palm vein systems may still be influenced by improper hand positioning, poor sensor calibration, or extreme environmental conditions. These factors require careful system design and user guidance.

IX. DISCUSSION

The proposed framework demonstrates that the successful realisation of palm biometric payment systems extends far beyond the development of highly accurate recognition algorithms. While biometric accuracy is a necessary foundation, it is not sufficient on its own to ensure real-world viability, scalability, or user acceptance. Instead, the findings of this study highlight the importance of system-level integration, trust- centric design, and robust governance mechanisms as equally critical determinants of success.

From a system perspective, palm biometric payment solutions must operate as cohesive end-to-end platforms rather than isolated technical components. Effective integration between biometric sensing, authentication, payment processing, and data management layers is essential to achieve low latency, reliability, and interoperability with existing financial and digital infrastructures. Fragmented designs that optimise individual modules without considering their interaction often fail to address deployment challenges encountered in high-traffic, real-world environments.

Trust emerges as a central theme in the adoption of biometric payment technologies. Users are more likely to accept palm-based payments when systems are transparent, predictable, and respectful of personal data. Trust-centric design therefore requires explicit consent mechanisms, clear communication of data usage policies, and user control over biometric enrolment and revocation. These elements directly influence perceived security and willingness to adopt the technology.

Finally, governance mechanisms play a decisive role in ensuring long-term sustainability. Compliance with security and privacy standards, ethical handling of biometric data, and continuous policy enforcement help mitigate risks related to misuse, surveillance, and regulatory violations. By embedding governance and accountability into the system architecture, the proposed framework supports not only technical robustness but also social legitimacy. Collectively, these insights reinforce the need for a holistic, interdisciplinary approach when designing palm biometric payment systems for practical deployment.

X. FUTURE RESEARCH DIRECTIONS

While the proposed palm biometric payment framework provides a comprehensive conceptual and architectural foundation, several avenues remain open for future research to strengthen its practical applicability and scientific contribution.

One important direction involves empirical validation through user studies and field trials. Large-scale pilot deployments in real-world environments such as campuses, transportation systems, or healthcare facilities would allow researchers to evaluate usability, transaction speed, error rates, and user acceptance. Incorporating qualitative feedback alongside quantitative performance metrics would provide deeper insight into trust formation, perceived privacy, and behavioural adoption factors.

Another promising area is the integration of palm biometric payment systems with decentralised identity (DID) infrastructures. Combining bio-metrics. with blockchain-based or self-sovereign identity models could enhance transparency, reduce reliance on centralised databases, and improve user control over identity credentials. Such integration may address long-standing concerns related to data ownership and single points of failure. Future research may also explore multi modal biometric fusion, combining palm bio-metrics. with complementary modalities such as finger vein, facial features, or behavioural traits. Multi modal approaches have the potential to improve authentication robustness, reduce false acceptance and rejection rates, and adapt to diverse operational conditions. Finally, advances in privacy-preserving biometric computation present significant opportunities. Techniques such as secure multiparty computation, homomorphic encryption, and federated learning could enable biometric matching and model training without exposing raw biometric data. Investigating these methods within palm-based payment systems would further strengthen privacy guarantees and regulatory compliance.

XI. CONCLUSION

This paper presented a comprehensive conceptual framework and modular system architecture for palm biometric payment systems, addressing both technical and sociology-organizational dimensions of deployment. By integrating biometric sensing and feature extraction, secure authentication mechanisms, payment processing infrastructure, and governance-oriented design principles, the proposed framework moves beyond algorithm-centric approaches toward a holistic system perspective.

The study emphasises that effective biometric payment solutions must balance recognition accuracy with system-level integration, trust, and regulatory compliance. Through a layered architectural design and explicit alignment with security and privacy standards, the framework demonstrates how palm bio-metrics. can be embedded into real-world payment ecosystems in a manner that is secure, scalable, and user-centric. Furthermore, by incorporating adoption-oriented considerations such as transparency, consent management, and ethical governance, the proposed approach addresses critical factors influencing long-term user acceptance.

Overall, this work provides a foundational reference for researchers and practitioners seeking to design, evaluate, and deploy next-generation biometric payment systems. The framework offers a flexible basis for future empirical validation and technological enhancement, supporting the continued evolution of palm biometric authentication as a viable component of smart financial and identity-driven systems.

REFERENCES

[1] Wang, C. H., Chen, W. R., Yen, J. J., Yang, X. S., & Siang, Y. S. (2026). Enhanced biometric authentication through integrated palm print and palm vein images. The Visual Computer, 42(1), Article

[2] Domingo, M. A. K. A., Bernadas, A. G. P., Maiquez, J. D. P., Ong, A. K. S., & Magana, M. C. (2025). Assessing the acceptance of palm biometric payment systems: An integration of the technology acceptance model and valence framework. Acta Psychologica, 259, 105426

[3] Yu, T., Teoh, A. P., Liao, J., & Wang, C. (2025). Show Your Palm to Pay: Are customers ready for palm print recognition technology in retail stores in China? International Journal of Human–Computer Interaction.

[4] Zhang, W., Zhang, H., & Deng, Z. (2025). Public attitude and media governance of biometric information dissemination in the era of digital intelligence. Scientific Reports, 15, 2419.

[5] Ke, L.-Y., Lin, Y.-C., & Hsia, C.-H. (2025). Finger vein recognition based on Vision Transformer with feature decoupling for online payment applications. IEEE Access, 13, 54636–54647.

[6] Wu, W., Elliott, S. J., Lin, S., Sun, S., & Tang, Y. (2020). Review of palm vein recognition. IET Biometrics, 9(1), 1–10.

[7] Kilian, V., Ally, N., Nombo, J., Abdalla, A. T., & Maiseli, B. (2020). Cost-effective and accurate palm vein recognition system based on multiframe super-resolution algorithms. IET Biometrics.

[8] Hemis, M., et al. (2025). Deep learning techniques for hand vein bio-metrics. Information Fusion.

[9] Kauba, C., Prommegger, B., & Uhl, A. (2019). Combined fully contactless finger and hand vein capturing device with a corresponding dataset. Sensors, 19(22), 5014.

[10] Wang, J.-G., Yau, W.-Y., Suwandy, A., & Sung, E. (2008). Person recognition by fusing palmprint and palm vein images based on “Laplacianpalm” representation. Pattern Recognition, 41(5), 1514–1527.

[11] Greitans, M., Pudzs, M., & Fuksis, R. (2010). Palm vein bio-metrics. based on infrared imaging and complex matched filtering. In Proceedings of the 12th ACM Workshop on Multimedia and Security (MM&Sec) (pp. 101–106). ACM.

[12] Piciucco, E., Maiorana, E., Campisi, P., & others. (2018). Palm vein recognition using a high dynamic range approach. IET Biometrics. Link:

[13] Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. Information Fusion, 103, 102144

[14] Schuiki, J., Linortner, M., Wimmer, G., & Uhl, A. (2022). Attack detection for finger and palm vein bio-metrics. by fusion of multiple recognition algorithms. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(4), 544–555.

[15] Aftab, A., et al. (2021). Hand-based multibiometric systems: State-of-the-art and future trends.