IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Palmprint Recognition Systems For Secure Payment

A Review of Deep Learning Architectures, Operational Efficiency, and Regulatory Compliance

Anurag Zete, Dnyanesh Patil, Chaitanya Kolhe, Pradip Yadav, Dr. Md. Abdul Wassay

Student, Student, Student, Student, Asst. Professor

Sandip Institute of Technology and Research Centre, Nashik, Maharashtra

Abstract

The integration of advanced biometrics is critical for the evolving global financial technology (FinTech) sector, which requires fast, secure, and contactless authentication. This review analyzes the deployment of palmprint recognition systems for secure payment, a modality projected for significant market expansion (CAGR of 26.10%) due to its high feature density, permanence, and non-contact nature. The paper details state-of-the-art deep learning architectures, such as the hybrid Vision Transformer (ViT) and Convolutional Neural Network (CNN) fusion utilized in the Palm-ID system, which achieves high accuracy (TAR of 98.06% at FAR=0.01%) and superior operational efficiency, including template sizes compressed to 516 bytes and sub-millisecond 1:N search times[1]. Crucially, the review examines the robust security framework required for financial adoption, including Presentation Attack Detection (PAD) and the implementation of cancelable biometrics for template protection to ensure revocability. Finally, it addresses the mandatory compliance with international data privacy regulations, such as GDPR and CCPA [2], affirming that optimized palmprint recognition is technologically ready and strategically positioned to secure the next generation of frictionless retail payment systems[3].

Index/Key Terms : Palmprint Recognition, Secure Payment Systems, Deep Learning (DL), Vision Transformer (ViT), Convolutional Neural Network (CNN), Contactless Biometrics, Template Protection, Cancelable Biometrics, Presentation Attack Detection (PAD), GDPR, CCPA

1. Introduction: The Mandate for Secure, Contactless FinTech Authentication

1.1 The Evolution of Biometric Authentication in Financial Transactions

The global financial technology (FinTech) sector is undergoing a profound transformation driven by the escalating demand for digital and contactless payment solutions. The market for palmprint payment systems is projected for robust expansion, growing from USD 68.4 million in 2024 to an estimated USD 662.6 million by 2034, reflecting a Compound Annual Growth Rate (CAGR) of 26.10%.[4] Similarly, the broader 'Pay by Palm' market is projected to reach USD 2,594 million by 2035, accelerating at a CAGR of 19.2%[3]. This growth is fundamentally propelled by technological advancements in biometrics, the necessity for strong, secure authentication, and the retail sector’s pursuit of seamless, frictionless customer experiences[1], [3].

A primary challenge confronting FinTech innovation is the critical necessity to balance transaction speed with high assurance security levels. Commercial success requires rapid authentication, ideally completed in sub-second time frames[2]. Traditional payment methods, reliant on cash, cards, or PINs, are susceptible to fraud and often introduce transactional friction. The increasing instances of identity fraud and cybersecurity threats have accelerated the demand for non-replicable biometric solutions.[2] Biometric systems aim to provide a signal that accurately represents a human trait for recognition[5]. Within this context, palmprint recognition has emerged as a key modality, providing a robust, non-invasive alternative to established methods such as fingerprint and facial recognition.

1.2 Defining the Core Requirements for Biometric Payment Systems

For a biometric solution to achieve widespread adoption within secure payment systems, it must satisfy stringent operational and security criteria.

First, the requirement for **Accuracy and Robustness** demands near-perfect recognition rates. Biometric systems must reliably maintain high True Acceptance Rates (TAR), often exceeding 99%, even at extremely low False Acceptance Rates (FARs), such as 0.01%[3], [6]. This performance must be preserved in unconstrained, real-world conditions characterized by variable lighting, low resolution (common with smartphone capture), and significant pose variation—challenges inherent to contactless imaging.

Second, **Latency and Throughput** are paramount for retail environments. A positive user experience requires authentication to be executed in sub-second time frames[2], [5]. This necessitates high system throughput, particularly for large-scale identification scenarios, known as 1:N searches, which involve matching a user against an entire database efficiently[7].

Third, the factors of **Hygiene and User Experience** have been significantly redefined by recent public health concerns. The contactless nature of palmprint interaction—where the user simply hovers their hand over a sensor—provides a crucial advantage over modalities that require physical contact, such as fingerprint readers[8]. This addresses public health concerns and facilitates higher customer adoption in sensitive environments like hospitals and food-serving areas[7].

Finally, **Data Security and Privacy** are non-negotiable. Compliance with international regulations, including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [9], [10], is mandatory. Furthermore, the implementation of non-invertible and revocable templates is essential to mitigate the risk posed by compromised biometric data, which cannot otherwise be re-issued if breached.[11]

1.3 Structure and Scope of the Review

This review provides a rigorous analysis of the current landscape of palmprint recognition for payment systems. It leverages a state-of-the-art framework, the Palm-ID system [8], as a technical benchmark, detailing its deep learning architectural innovations and efficiency optimizations. The report then evaluates this technology against competitive biometric modalities, explores critical security protocols such as Presentation Attack Detection (PAD) and template protection, and culminates with a discussion of the regulatory landscape and the practicalities of commercial deployment, exemplified by systems such as Amazon One[11].

2. Comparative Analysis of Biometric Modalities and Palmprint Advantages

2.1 Technical and Operational Comparison of Biometrics

Biometric modalities traditionally deployed in payment and access control include facial recognition, fingerprint recognition, and, increasingly, palm recognition[9]. Each presents distinct trade-offs regarding security and usability. Facial recognition is contactless, but its performance can be compromised by factors such as lighting conditions, low image quality, and occlusions like masks[12]. Fingerprint recognition is highly accurate and widely adopted but fundamentally requires physical contact, raising hygiene concerns, particularly in high-throughput public settings[8], [10].

Palm recognition, encompassing both surface palm print and subsurface palm vein patterns, offers a compelling solution by integrating the high discriminability of friction ridge biometrics with the non-contact

requirement of modern transactions[13]. The biological richness of the hand provides a robust platform for identification. A palm print contains a significantly larger feature space—approximately ten times more unique features than a single fingerprint[13]. This inherently high feature density translates directly into superior uniqueness and stability, forming a strong technical foundation for achieving exceptionally high accuracy and reliability in financial authentication systems[3].

2.2 The Non-Contact and Unconstrained Superiority of Palm Recognition

The contactless nature of palm recognition represents a powerful strategic differentiator, particularly for large-scale consumer applications[14]. The operation is non-invasive and user-friendly, requiring only that the user quickly hovers their hand over the scanner[8]. This non-contact interaction directly minimizes the transmission of germs, enhancing safety in retail, hospital, and food-serving environments, and consequently accelerating customer adoption[3], [14].

Furthermore, palm recognition exhibits greater operational stability and versatility compared to other biometrics. Palm prints are generally less vulnerable to external factors such as dirt, wear, cuts, or scars that often degrade the quality of fingerprint capture[6]. Unlike face recognition, palm scanning is not hindered by obstructions such as glasses or masks, ensuring efficient and accurate information capture in diverse settings[15]. Palm biometrics benefits from providing a large surface area for recognition, which allows for highly distinctive and accurate verification and identification processes[10].

2.3 Palm Print vs. Palm Vein: Multimodal Synergy

The technology is broadly categorized into two main sensing methods: palm print recognition and palm vein recognition. **Palm print recognition** utilizes high-resolution visible light cameras or scanners to map the two-dimensional surface patterns, including creases, lines, and wrinkles[16]. This approach, particularly when leveraging consumer-grade devices like smartphone cameras, is emphasized in systems like Palm-ID due to its cost-effectiveness and ease of integration into existing applications[13], [17].

Conversely, **Palm Vein Recognition** scans the vascular structure beneath the skin using Near-Infrared (NIR) light. The hemoglobin in the veins absorbs the NIR light, generating a unique, detailed map of the subsurface vein structure[14]. Because this modality relies on internal, subsurface biological traits, it is intrinsically tamper-resistant and virtually impossible to replicate using surface artifacts.[16] This intrinsic security advantage is why palm vein technology is favored in high-security environments, such as banking and healthcare[18].

Commercial deployment often acknowledges the strengths of combining these methods. Many systems, including those by Armatura and Fujitsu, employ a **multimodal approach**, fusing information derived from both the visible spectrum (surface print) and the infrared spectrum (vein structure)[14]. This hybrid strategy enhances both the overall recognition accuracy and the system's resistance to presentation attacks, offering a higher security level than relying on either trait alone[15].

3. State-of-the-Art Deep Learning for Palmprint Recognition

3.1 The Contactless Recognition Pipeline

The efficacy of modern contactless palmprint recognition hinges on a sophisticated, multi-stage processing pipeline. This process begins with image acquisition, often via unconstrained mobile capture, followed by precise Region of Interest (ROI) extraction, image enhancement, feature extraction, and finally, matching[19].

The primary technical hurdle in contactless recognition is managing the high intra-class variability introduced during image capture. Contactless methods must contend with six degrees of freedom (DOF) between the user's palm and the capture device, leading to issues like extreme perspective distortions, rotation, and non-linear scale changes[17]. State-of-the-art systems address this by implementing robust preprocessing techniques. This includes utilizing deep learning models, such as a ResNet-50 based keypoint detection module, to locate key points around the palmar boundary. These key points facilitate a non-linear homography transformation and precise alignment, often involving a Spatial Transformer Network (STN) parametrized by

a thin-plate-spline (TPS), thereby ensuring the extracted 224 times 224 ROI is consistently aligned for downstream feature extraction[17].

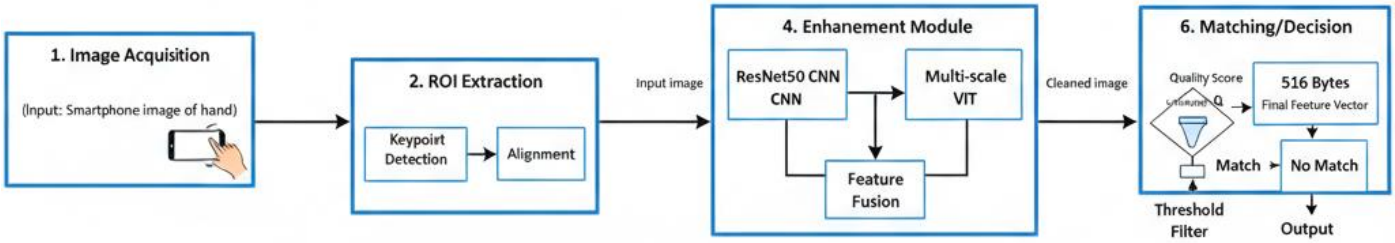

Figure 1: Comprehensive pipeline for contactless palmprint recognition, detailing the sequence from Keypoint Detection, non-linear ROI Extraction, Learned Enhancement, to Hybrid Feature Extraction (ViT-CNN fusion), Dimensionality Reduction, and final Matching.

3.2 Hybrid Deep Learning Architecture (Case Study: Palm-ID

Advancements in recognition accuracy have been achieved by moving beyond reliance on a single deep neural network architecture. The Palm-ID framework exemplifies this trend by employing a **multimodal embedding fusion** of a Vision Transformer (ViT) and a Convolutional Neural Network (CNN), specifically ResNet50[14]. This integration is based on the premise that CNNs and ViTs encode different yet complementary features for biometrics. The ResNet50 component is adept at capturing local, texture-based features, while the ViT component excels at aggregating global contextual information, thereby improving the overall robustness of the system[13], [14].

A critical architectural innovation is the use of **Multi-Scale Feature Capture** within the ViT. Because the stand-off distance during mobile capture is variable, leading to differences in image scale and resolution across databases, capturing features at diverse scales is vital for developing a robust system[1]. The ViT architecture incorporates multi-resolution patches (e.g., 16\times16 and 32\times32) as input features. This fusion of multi-scale local features yields a measurable improvement in recognition performance compared to using a single patch size, underscoring its necessity for unconstrained environments[15].

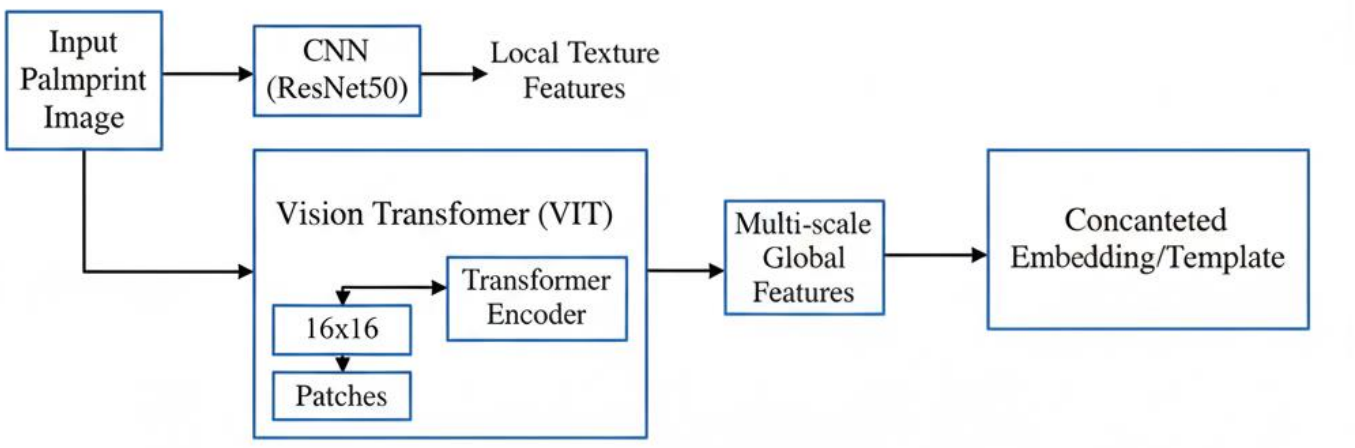

Figure 2: Conceptual diagram of the hybrid deep learning architecture, illustrating the fusion of complementary features extracted by the Convolutional Neural Network (CNN) and the Vision Transformer (ViT) using multi-scale input patches.

Moreover, the system incorporates a learned preprocessing step: a novel **Enhancement Module**. Given the common occurrence of low contrast, noise, occlusion, and surface markings (such as tattoos or handwriting) in unconstrained images, a SqueezeUNet architecture is trained using domain-specific augmentations to recover the original high-quality image[13]. This module is explicitly trained to suppress degradation while emphasizing the prominence of principal lines in the palmprint. The ablation analysis confirms that the

inclusion of this learned enhancement model is pivotal for boosting performance, particularly on challenging, lower-quality, time-separated datasets[17].

3.3 Performance Benchmarking in Operational Environments

The true measure of a payment biometric system lies in its proven performance across diverse, real-world conditions, including cross-sensor and longitudinal (time-separated) evaluations.

The Palm-ID system was evaluated against challenging protocols, including datasets separated by up to 13 months, simulating the long-term, time-separated nature of real-world identity management.[7] In verification (1:1) scenarios, the system demonstrated state-of-the-art results, achieving a True Acceptance Rate (TAR) of 98.06% at a False Acceptance Rate (FAR) of 0.01% on the demanding, time-separated APDB-2-3 dataset (collected seven months apart). This performance significantly surpassed other academic and commercial methods compared in the study[14].

For high-throughput 1:N search scenarios, the model exhibited superior identification performance. In closed-set identification tests, Palm-ID achieved an average Rank-1 Retrieval Rate of 98.24%, confirming its ability to accurately locate the correct identity immediately in a large gallery[18]. In open-set identification, the model dramatically reduced error rates. Compared to baseline methods, the False Negative Identification Rate (FNIR) at FPIR=1% was significantly lower, averaging 4.42% across all test sets, highlighting the system's enhanced ability to manage challenging operational conditions and prevent false rejections[15].

4. System Efficiency, Mobile Deployment, and Economic Feasibility

4.1 Optimization for Edge Computing and Low Latency

The successful deployment of biometrics in payment systems is highly dependent on meeting stringent latency requirements. Commercial systems like Amazon One emphasize sub-second authentication to ensure a frictionless user experience[20]. Achieving this speed requires optimizing feature extraction, template size, and search efficiency for edge devices.

The Palm-ID system is designed as an end-to-end mobile solution, with the entire recognition pipeline, including capture, feature extraction, and matching, embedded within a smartphone, enhancing both privacy and reducing communication latency[16]. The model achieves rapid template extraction in just 18ms[3], [17]. Crucially, the system demonstrates exceptional efficiency in large-scale identification: utilizing efficient threading on a standard server CPU, it performs a 1:10,000 gallery comparison in only 0.33ms[3], [13]. This sub-millisecond search capability confirms the system's readiness for large-scale retail identification systems that require near-instantaneous search results[1], [16], [20].

4.2 Template Compression and Dimensionality Reduction

A significant challenge in deep learning biometrics is the need for small, rapidly searchable templates despite the feature-richness of palmprints. High-dimensional feature vectors, such as the 768-dimensional embeddings generated by the ViT-CNN fusion, can lead to templates sized at 3080 bytes[16]. The resolution to this is found in aggressive template optimization.

The system employs a learned, non-linear dimensionality reduction model (DeepMDS++)[19]. This model compresses the individual ViT and ResNet embeddings from 384 dimensions to 256 dimensions each, resulting in a concatenated template size of 512 dimensions. This process reduces the template storage size by approximately four times while maintaining high recognition accuracy, averaging a TAR of 96.97%[5]. This template optimization is vital for minimizing storage costs and maximizing search speed in mobile and cloud environments[5].

Further optimization is achieved through data compression by converting the feature precision from a 32-bit float (4 bytes) to an 8-bit unsigned integer (1 byte). This compression scheme, which stores the resulting template efficiently in **516 bytes** (plus 4 metadata bytes), is demonstrated to have a negligible impact on accuracy, confirming the viability of deploying highly accurate palm recognition on constrained embedded devices[4].

Table 1 provides a quantitative comparison, highlighting the Palm-ID system's optimal balance of accuracy and speed achieved through template optimization.

Metric/Model	Technology/Fusion	Accuracy (TAR @ 0.01% FAR)	Template Size (Bytes)	Extraction Latency (ms)	1:10K Search Latency (ms)
Palm-ID (Proposed) [7]	CNN+ViT Multi-scale	High (Avg. 96.97% / 98.06% APDB-2-3)	516	18.0	0.33
Godbole et al. [7]	CNN	High (Avg. 95.94%)	3080	9.08	0.84
Armatura SDK (Commercial) [7]	Undisclosed	Competitive (97.78% APDB-2-3)	544	<60	<10

Table 1: Comparative Performance and Efficiency of SOTA Contactless Palmprint Recognition Systems

4.3 Economic Justification and Retail ROI

The financial viability of palmprint payment systems rests on the analysis of Return on Investment (ROI), driven primarily by risk mitigation. While specialized biometric terminals must be integrated with existing Point-of-Sale (POS) infrastructure, the main economic justification for financial institutions to invest in high-security biometrics is the potential to "significantly reduce (perhaps eliminate) fraud and theft" associated with transactions[21], [22].

The deployment of tamper-resistant, highly accurate biometrics is perceived as outweighing the incremental hardware costs. Consequently, financial entities (like Visa and Mastercard) are incentivized to drive adoption, sometimes by absorbing the system costs rather than passing them entirely to the merchant[2]. This cost absorption shifts the economic burden from retail adoption friction to financial risk mitigation, ensuring that the retail segment remains the largest and fastest-growing application area for palmprint payment systems[1].

5. Advanced Security and Regulatory Compliance

5.1 Presentation Attack Detection (PAD) and Liveness

All biometric payment systems are vulnerable to Presentation Attacks (PA), where fraudulent artifacts such as photos or casts are presented to the sensor[22]. To counter this, modern systems integrate robust Presentation Attack Detection (PAD) algorithms, often referred to as liveness detection, which typically run in the background during the capture process[5], [21].

Systems utilizing the palm vein modality possess a superior defense against spoofing. Since palm vein recognition requires Near-Infrared (NIR) imaging to detect subsurface, internal biological traits, replicating a live, functioning vein pattern with a surface artifact is exceptionally difficult[2], [22]. Research demonstrates that dedicated anti-spoofing algorithms that analyze image noise residuals derived from the acquired image can effectively detect presentation attacks in palm-vein sensors, achieving near-perfect classification error rates in controlled studies[6].

For visible-spectrum palmprint systems, security is enhanced through feature-level defenses. One approach involves using the L2 norm of the deep learning feature embedding as a highly effective, learned metric for image quality[3], [4]. This metric correlates strongly with image quality factors such as blurriness, contrast, and occlusion. By establishing a quality threshold, the system gains the flexibility to reject low-quality images that are often associated with sophisticated presentation attacks or simple artifacts, acting as an implicit security filter[15].

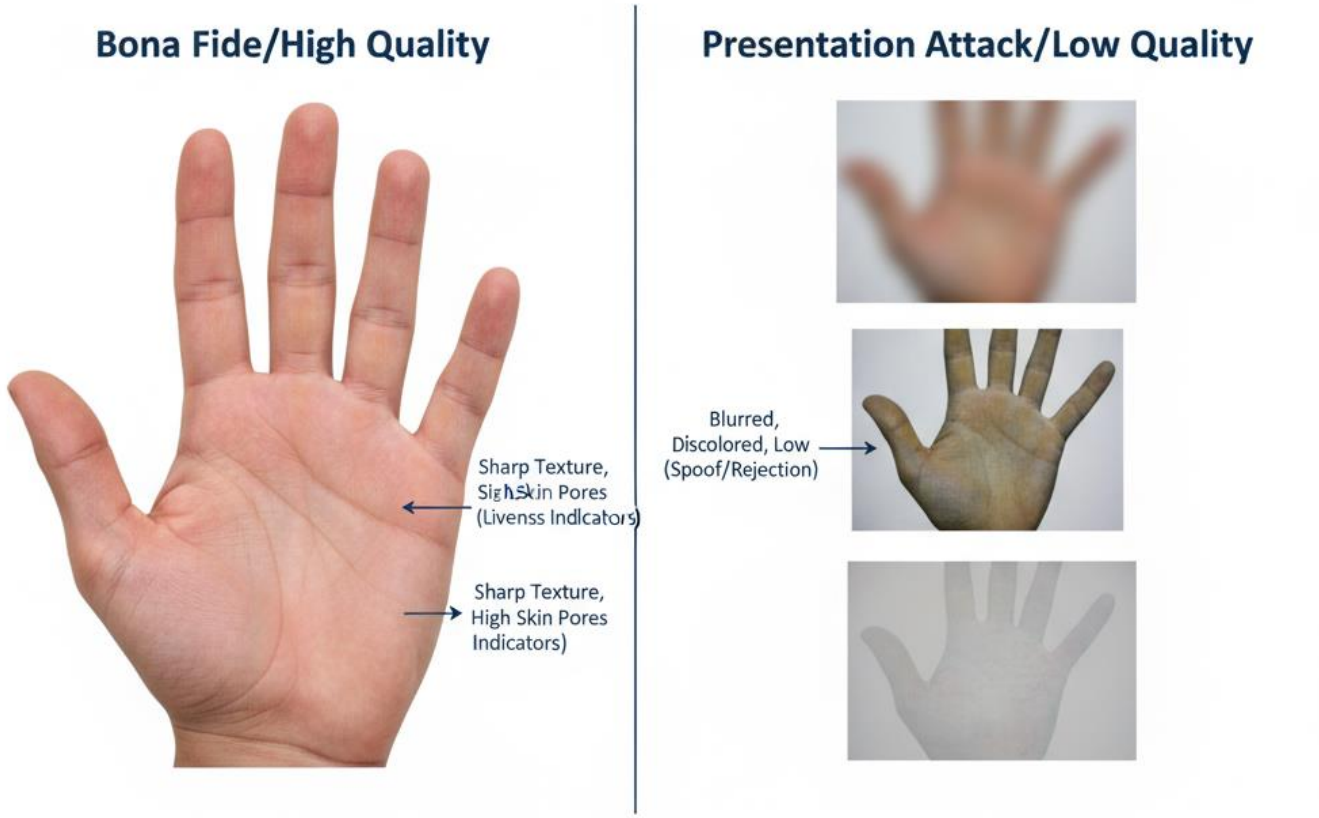

Figure 3: Comparative visualization of high-quality (bona fide) palm captures versus low-quality or potential Presentation Attack (PA) samples, illustrating the role of the learned quality metric for robust anti-spoofing defense.

5.2 Biometric Template Protection and Revocability

The inherent permanence of biometrics necessitates that raw biometric data never be stored, as a compromised raw template cannot be revoked[23]. Therefore, robust template protection schemes that satisfy criteria for high security, unlinkability (preventing cross-database correlation), and revocability (the ability to re-issue a new template upon compromise) are mandatory for secure payment systems[23].

Cancelable Biometrics represents the preferred template protection paradigm. This involves irreversibly and intentionally transforming the original biometric features into a non-invertible template[6]. Techniques combining randomized cuckoo hashing and minHash have been proposed for palmprint systems to resist unlinkability attacks, demonstrate large re-issuance capability, and still maintain high recognition performance[6]. Furthermore, research into using **Homomorphic Encryption (HE)** is underway to secure template processing, allowing feature comparison to occur on encrypted data, which is crucial for systems that rely on cloud-based storage for templates[23].

5.3 Regulatory Frameworks (GDPR, CCPA)

The legal status of biometrics as highly sensitive personal data is a major market driver for robust security implementation. Both the European Union's GDPR and the California Consumer Privacy Act (CCPA) classify biometric information within their broad definitions of "personal information" subject to stringent protection[2].

This regulatory environment mandates transparent data handling practices and ensures that the user maintains complete control over their digital biometric identity[2]. Commercially deployed systems, such as Amazon One, demonstrate compliance by explicitly allowing users to manage their data, connect or disconnect from participating businesses, and delete their biometric signature entirely at any time[2]. Robust template protection is therefore not merely a technical consideration but a necessary step for regulatory compliance and ensuring public trust.

Furthermore, integration into the financial ecosystem requires adherence to global payment security standards. Any entity that stores, processes, or transmits cardholder data—including third-party agents (TPAs) deploying biometric POS devices—must comply with the **Payment Card Industry Data Security Standard (PCI DSS)**[4], [22].

5.4 International Standards for Interoperability

To ensure market integration and maximum stakeholder interoperability, biometric systems must conform to international data format standards. The **ISO/IEC 19794** series defines these standards for biometric data exchange and storage[6]. ISO/IEC 19794-1 provides the common biometric record format framework, which is necessary for government and civilian biometric implementation[2].

In addition, digital identity assurance levels are guided by the **NIST SP 800-63 Digital Identity Guidelines**[3], [4]. Secure payment systems require high confidence authentication levels (AAL 2 or 3). The use of advanced, tamper-resistant biometrics like palm recognition provides the necessary technical foundation to meet these high assurance level requirements, confirming the user's control over the authenticator bound to their account[2], [5].

6. Commercial Deployment, Market Trends, and Future Directions

6.1 Current Commercial Landscape (Amazon One and Global Players)

Palmprint recognition systems have successfully transitioned from laboratory research to definitive commercial deployment, primarily driven by major global enterprises. The most prominent example is **Amazon One**, which has fully rolled out its palm-scanning payment system across all Whole Foods stores in the United States[1]. Amazon One uses the palm for payment, check-in, and digital authentication, processing over 1 million biometric authentications monthly[1]. The system relies on secure, encrypted storage in the AWS cloud[3].

Industry support further validates the technology's trajectory. Global payment networks, including Visa and Mastercard, along with major technology players like Tencent and Fujitsu, are actively supporting or deploying palm-based payment systems[15], [19]. This broad acceptance is facilitated by the availability of robust SDKs and APIs, enabling the seamless integration of palm scanners into existing payment and identity verification systems without requiring businesses to completely replace their infrastructure[19].

Modality	Feature Density/Security	Contact Requirement	Hygiene/User Experience	Primary PAD Countermeasure	Key Regulatory Challenge
Palmprint	Very High (10x Fingerprint)	Contactless	High	Multimodal Fusion (Vein/NIR)	Template Revocability (GDPR/CCPA)
Fingerprint	High	Contact Required	Low (Hygiene Risk)	Liveness Detection (Capacitive/Optical)	Standardization & Storage (ISO 19794-2) [
Face	High (External features)	Contactless	Medium/High	Liveness (3D/Infrared Depth)	Demographic Bias/Privacy Concerns
Palm Vein	Extremely High (Subsurface)	Contactless	High	Intrinsic (NIR capture)	Cost/Specialized Sensor Requirement

Table 2: Strategic Comparison of Biometric Modalities for Secure Payment

6.2 Identified Challenges and Future Research

Despite the demonstrated technical successes, continued research is essential to address practical limitations for mass deployment.

One persistent area of study is **long-term robustness and stability**. While palm biometrics are inherently stable throughout a person's lifetime , the performance must be continuously verified across extended longitudinal evaluations. Furthermore, the potential for certain short-term physiological factors, such as high fevers or significant skin conditions, to temporarily interfere with accurate verification must be fully mitigated.

Another key challenge is ensuring **cross-sensor and cross-domain interoperability**. The variations introduced by different capture devices (e.g., various smartphone models or proprietary scanners) in unconstrained environments necessitate further algorithm development to maintain high matching accuracy regardless of the acquisition source.

Future directions are focusing on leveraging the most advanced deep learning techniques. Continued exploration of advanced transformer-based models and the integration of multi-spectral fusion (combining visible light and NIR) are expected to yield further improvements in both anti-spoofing reliability and recognition accuracy, driving high-security standards.

6.3 Conclusion and Outlook

The review confirms that palmprint recognition systems are technologically mature and highly optimized for secure payment applications. The convergence of the biological advantage of high feature density and the strategic benefit of non-contact interaction, coupled with the technical breakthrough of efficient deep learning architectures (ViT-CNN fusion and template compression to 516 bytes with sub-millisecond search times), has successfully overcome previous barriers regarding accuracy and speed.

The success of large-scale commercial implementations like Amazon One demonstrates that the modality is ready for mass consumer adoption. However, continued success in the financial sector is inextricably linked to maintaining stringent compliance with evolving privacy regulations (GDPR and CCPA) through robust template protection schemes that guarantee revocability and unlinkability. By prioritizing advanced Presentation Attack Detection and adhering to regulatory mandates for user control, palmprint systems are strategically positioned to become the dominant technology for the next generation of frictionless, secure retail payment.

7. References

[1] S. A. Grosz, A. Godbole, and A. K. Jain, “Mobile Contactless Palmprint Recognition: Use of Multiscale, Multimodel Embeddings,” *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 8428–8440, 2024, doi: 10.1109/TIFS.2024.3413631.

[2] P. Mishra and M. P. S. Chawla, “A Fast Biometric Fingerprint Payment System,” vol. 2, no. 3.

[3] T. Min-Jen and C. Cheng-Tao, “Convolutional Neural Network for Detecting Deepfake Palmprint Images,” *IEEE Access*, vol. 12, pp. 103405–103418, 2024, doi: 10.1109/ACCESS.2024.3433497.

[4] “fin_irjmets1680531476,” *Int. Res. J. Mod. Eng. Technol. Sci.*.

[5] S. Iqbal *et al.*, “A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication Factor,” *IEEE Access*, vol. 8, pp. 177405–177423, 2020, doi: 10.1109/ACCESS.2020.3025429.

[6] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, “Touch of Privacy: A Homomorphic Encryption-Powered Deep Learning Framework for Fingerprint Authentication,” *IEEE Access*, vol. 13, pp. 59057–59073, 2025, doi: 10.1109/ACCESS.2025.3555311.

[7] J. Lou, J. zou, and B. Wang, “Palm Vein Recognition via Multi-task Loss Function and Attention Layer,” Nov. 11, 2022, *arXiv*: arXiv:2211.05970. doi: 10.48550/arXiv.2211.05970.

[8] T. Brisley, A. Gandhi, and J. Magen, “Context-Aware Palmprint Recognition via a Relative Similarity Metric,” Apr. 15, 2025, *arXiv*: arXiv:2504.11306. doi: 10.48550/arXiv.2504.11306.

[9] P. Chen *et al.*, “Design of Low-Cost Personal Identification System That Uses Combined Palm Vein and Palmprint Biometric Features,” *IEEE Access*, vol. 7, pp. 15922–15931, 2019, doi: 10.1109/ACCESS.2019.2894393.

[10] N. Zhang and M. Xi, "A high-efficiency palmprint recognition model integrating ROI and Gabor filtering," *PLOS One*, vol. 20, no. 6, p. e0323373, Jun. 2025, doi: 10.1371/journal.pone.0323373.

[11] Y. Zhang, L. Zhang, X. Liu, S. Zhao, Y. Shen, and Y. Yang, "Pay By Showing Your Palm: A Study of Palmprint Verification on Mobile Platforms," in *2019 IEEE International Conference on Multimedia and Expo (ICME)*, Jul. 2019, pp. 862–867. doi: 10.1109/ICME.2019.00153.

[12] C. Gao, Z. Yang, W. Jia, L. Leng, B. Zhang, and A. B. J. Teoh, "Deep Learning in Palmprint Recognition-A Comprehensive Survey," Jan. 02, 2025, *arXiv*: arXiv:2501.01166. doi: 10.48550/arXiv.2501.01166.

[13] N. Li *et al.*, "Chinese Face Dataset for Face Recognition in an Uncontrolled Classroom Environment," *IEEE Access*, vol. 11, pp. 86963–86976, 2023, doi: 10.1109/ACCESS.2023.3302919.

[14] W. K. Zhang and M. J. Kang, "Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers," *IEEE Access*, vol. 7, pp. 154360–154374, 2019, doi: 10.1109/ACCESS.2019.2927705.

[15] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, "Secure Authentication Protocol for Mobile Payment," *Tsinghua Sci. Technol.*, vol. 23, no. 5, pp. 610–620, Oct. 2018, doi: 10.26599/TST.2018.9010031.

[16] B. Mróz-Gorgoń, W. Wodo, A. Andrych, K. Caban-Piaskowska, and C. Kozyra, "Biometrics Innovation and Payment Sector Perception," *Sustainability*, vol. 14, no. 15, Art. no. 15, Jan. 2022, doi: 10.3390/su14159424.

[17] Z. Huang, J. Zhang, and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 6, pp. 7917–7932, Jun. 2023, doi: 10.1109/TPAMI.2022.3217882.

[18] M. Zhang, R. Liu, D. Deguchi, and H. Murase, "Masked Face Recognition With Mask Transfer and Self-Attention Under the COVID-19 Pandemic," *IEEE Access*, vol. 10, pp. 20527–20538, 2022, doi: 10.1109/ACCESS.2022.3150345.

[19] W. Yang, J. Hu, S. Wang, J. Yang, and L. Shu, "Biometrics for securing mobile payments: Benefits, challenges and solutions," in *2013 6th International Congress on Image and Signal Processing (CISP)*, Dec. 2013, pp. 1699–1704. doi: 10.1109/CISP.2013.6743950.

[20] B. Mróz-Gorgoń, W. Wodo, A. Andrych, K. Caban-Piaskowska, and C. Kozyra, "Biometrics Innovation and Payment Sector Perception," *Sustainability*, vol. 14, no. 15, Art. no. 15, Jan. 2022, doi: 10.3390/su14159424.

[21] P. Mishra and M. P. S. Chawla, "A Fast Biometric Fingerprint Payment System," vol. 2, no. 3.

[22] Z. Li, X. Liang, D. Fan, J. Li, W. Jia, and D. Zhang, "Touchless Palmprint Recognition based on 3D Gabor Template and Block Feature Refinement," Dec. 12, 2021, *arXiv*: arXiv:2103.02167. doi: 10.48550/arXiv.2103.02167.

[23] S. Iqbal *et al.*, "A Novel Mobile Wallet Model for Elderly Using Fingerprint as Authentication Factor," *IEEE Access*, vol. 8, pp. 177405–177423, 2020, doi: 10.1109/ACCESS.2020.3025429.