ijrtsm

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"A REVIEW OF MULTIMODAL BIOMETRIC FUSION APPROACHES IN SECURE DIGITAL TRANSACTIONS"

Abhishek Solanki [1], Prof. O. P. Karada [2], Dr. Deepak Kumar Yadav [3]

[1] Research Scholar, Department of Computer Science & Engineering, Institute of Engineering and Technology, Madhya Pradesh, India

[2]Assistant Professor, Department of Computer Science & Engineering, Institute of Engineering and Technology, Madhya Pradesh, India

[3]Associate Professor, Department of Computer Science & Engineering, Institute of Engineering and Technology, Madhya Pradesh, India

ABSTRACT

The rapid growth of digital payment systems has increased the demand for authentication mechanisms that are both secure and user-friendly. Traditional methods such as passwords, PINs, and tokens are prone to theft, phishing, and replay attacks, making them inadequate for safeguarding financial transactions. Biometric authentication provides a more robust alternative by leveraging unique physiological and behavioral traits; however, unimodal systems often suffer from spoofing vulnerabilities, noisy data, and lack of universality. Multimodal biometric fusion—integrating two or more biometric modalities—addresses these challenges by enhancing accuracy, resilience, and spoof resistance. The emergence of machine learning and deep learning has further advanced this domain, enabling automated feature extraction, adaptive classification, and optimized fusion at sensor, feature, score, and decision levels. This review consolidates existing research on multimodal biometric fusion for secure digital payments, examining biometric modalities, fusion techniques, and ML/DL frameworks. Key issues such as spoofing, template protection, privacy regulations, and adversarial machine learning threats are discussed alongside real-world applications in mobile wallets, ATMs, and e-banking. Finally, the paper highlights research gaps and future directions, including lightweight edge-AI models, blockchain-enabled identity systems, continuous authentication, and explainable AI. The findings suggest that ML-driven multimodal biometrics offer a promising pathway toward secure and trustworthy digital payment ecosystems.

Key Words: *Multimodal biometrics; Biometric fusion; Machine learning; Deep learning; Digital payments; Secure authentication; Template protection; Spoof detection.*

I. INTRODUCTION

The growth of digital payment systems has transformed the global financial landscape by offering speed, convenience, and accessibility. However, these advantages come with heightened risks of fraud, identity theft, and cyberattacks [1], [2]. Traditional authentication methods such as passwords, PINs, and tokens suffer from limitations, including vulnerability to phishing, replay attacks, and the burden of memorization [3]. To overcome these challenges, biometric authentication has emerged as a reliable alternative by leveraging unique physiological and behavioral traits of individuals [4].

Biometric systems are broadly categorized into physiological modalities (e.g., fingerprint, iris, face, palm vein) and behavioral modalities (e.g., voice, signature, keystroke dynamics) [5]. These systems enhance security since biometric traits cannot be easily forgotten or shared. Yet, unimodal biometrics face significant drawbacks such as noisy data capture, intra-class variability, spoofing attempts, and lack of universality [6]. For example, fingerprints may be unreadable due to skin conditions, while facial recognition is often unreliable in poor lighting conditions [7]. Figure 1 showed the biometric multi-modal fusion.

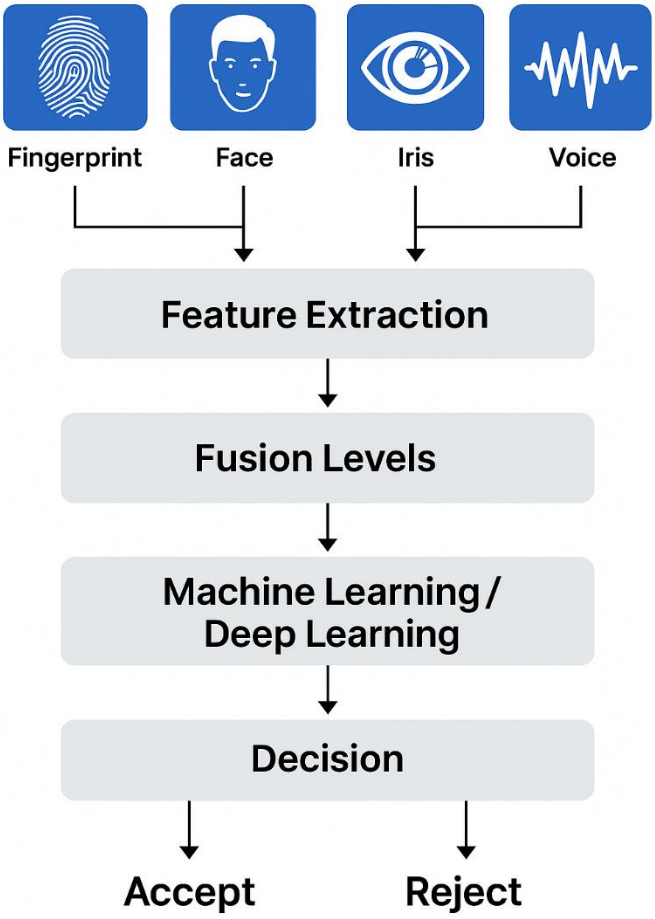

Figure 1 Overview of Multimodal Biometric Fusion

To address these issues, multimodal biometric fusion has gained importance, where multiple biometric traits are combined to increase accuracy, robustness, and resistance against spoofing [8]. Fusion can occur at various levels—sensor, feature, score, or decision—depending on the application and computational constraints [9]. The integration of machine learning (ML) and deep learning (DL) has further advanced multimodal systems by enabling automatic feature extraction, adaptive decision-making, and improved scalability [10], [11].

In the context of digital payments, multimodal biometric fusion ensures secure and seamless user authentication in mobile banking, e-wallets, and ATM systems [12]. Despite the benefits, challenges such as privacy protection, adversarial ML attacks, and resource limitations in mobile devices persist [13]. This review paper aims to (i) examine the role of multimodal biometric fusion in enhancing security of digital payments, (ii) highlight ML/DL-based fusion strategies, (iii) discuss performance evaluation and privacy concerns, and (iv) identify challenges and future research directions.

II. Fusion Techniques in Multimodal Biometrics

ISSN : 2455-9679
SJIF Impact Factor : 6.008

The effectiveness of multimodal biometric systems largely depends on the fusion strategy employed to combine information from multiple biometric sources. Fusion can occur at different levels, each with unique trade-offs in complexity, accuracy, and robustness [14]. Figure 2 showed the comparative analysis of fusion techniques.

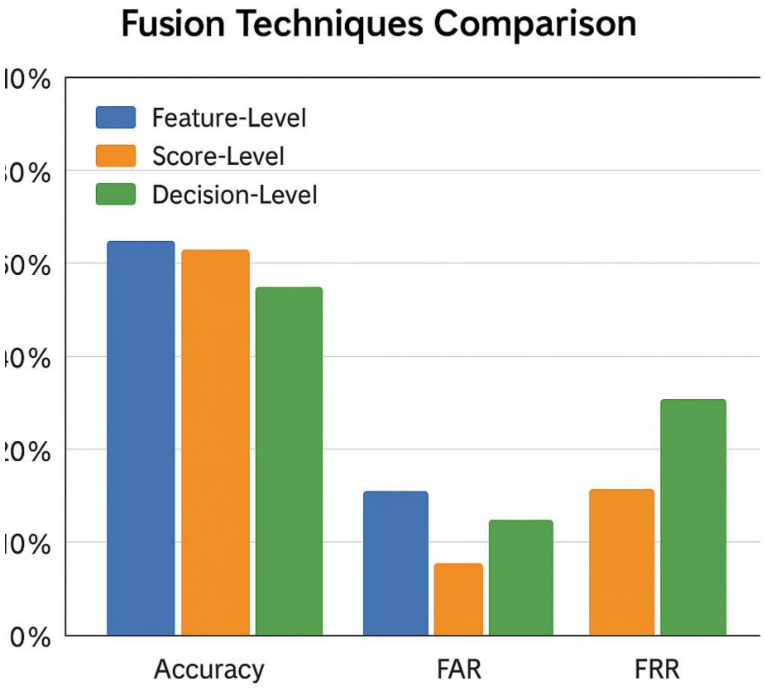

Figure 2 Comparison of fusion techniques.

2.1 Sensor-Level Fusion

At the earliest stage, raw data from multiple sensors (e.g., fingerprint image + iris scan) are combined before feature extraction. This approach requires sensors of compatible modalities and high-quality data acquisition, but it often results in high computational complexity and synchronization issues [15].

2.2 Feature-Level Fusion

Feature-level fusion combines feature vectors extracted from different modalities into a single representation. Machine learning methods such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Autoencoders are frequently applied to reduce dimensionality and remove redundancy [16]. Feature-level fusion provides rich discriminatory information but requires robust normalization methods to handle heterogeneity in feature scales.

2.3 Score-Level Fusion

In score-level fusion, the matching scores obtained from individual biometric systems are combined using methods such as sum, product, weighted average, logistic regression, or Support Vector Machines (SVM). This is the most widely adopted technique in real-world systems due to its balance between accuracy and computational efficiency [17].

2.4 Decision-Level Fusion

At this stage, the final recognition decisions (accept/reject) from different biometric systems are integrated using rules such as majority voting, AND/OR logic, or Bayesian decision theory [18]. Although simpler to implement, decision-level fusion generally provides lower accuracy compared to score- or feature-level fusion, as much of the discriminatory information is lost in earlier stages.

2.5 Machine Learning-Based Fusion

Recent advances in ML and DL have introduced adaptive fusion mechanisms that learn optimal weighting or non-linear combinations of modalities. Ensemble learning, Convolutional Neural Networks (CNNs), and Recurrent Neural

Networks (RNNs) have demonstrated superior performance compared to conventional statistical fusion [19]. These techniques enable dynamic fusion, where the system adapts to varying environmental or user conditions, making them especially suitable for digital payment environments that require fast and secure authentication.

In summary, score-level and feature-level fusion remain the most practical approaches in secure payment systems due to their balance of efficiency and accuracy, while ML-based adaptive methods represent the future direction of biometric fusion.

III. Biometric Modalities Used in Digital Payments

Biometric authentication relies on unique human traits that can be broadly divided into physiological and behavioral modalities. In digital payment systems, the choice of modality depends on a balance between accuracy, user convenience, cost, and spoof resistance [14].

3.1 Physiological Modalities

Fingerprint recognition is the most widely deployed modality in smartphones and ATMs due to its low cost and high accuracy. However, it may fail with worn, injured, or wet fingers, limiting universality.

Facial recognition has gained popularity in mobile payment applications such as Apple Pay and Alipay. It enables contactless authentication but is sensitive to illumination, pose variations, and spoofing via photographs or 3D masks [15].

Iris and retina recognition provide high accuracy and stability, as ocular features are difficult to forge. Despite this, their use in payment systems is limited by cost and user acceptance issues.

Palmprint and vein recognition offer strong anti-spoofing capability and are increasingly explored for high-security applications, though sensor integration in mobile devices remains challenging.

3.2 Behavioral Modalities

Voice recognition enables hands-free authentication and is integrated into smart assistants and banking apps. However, it is affected by background noise and vulnerable to replay or deepfake attacks.

Signature verification (both static and dynamic) continues to be relevant in financial systems where handwritten authorization is culturally accepted. Its reliability, however, decreases under stress or intentional distortion.

Keystroke dynamics and touchscreen behavior are emerging as unobtrusive modalities for mobile payment authentication, as they leverage existing hardware without requiring extra sensors.

3.3 Emerging Modalities

Recent studies explore electrocardiogram (ECG), electroencephalogram (EEG), and gait recognition as biometric traits for continuous and liveness-aware authentication. These modalities enhance resilience against spoofing but raise concerns regarding sensor cost and user acceptance [16].

3.4 Comparative Considerations

In the context of digital payments, fingerprint and face recognition dominate due to smartphone integration, while voice and touch dynamics serve as secondary or fallback modalities. High-security applications such as banking terminals may adopt iris or palm vein recognition. A combination of one physiological and one behavioral modality often yields optimal trade-offs between usability and security in multimodal systems [17].

IV. Machine Learning and Deep Learning in Biometric Fusion

Machine learning (ML) and deep learning (DL) have transformed the way multimodal biometric fusion is designed and deployed. Unlike traditional statistical methods, ML/DL approaches enable automatic feature extraction, adaptive classification, and robust fusion strategies, making them highly suitable for digital payment authentication where both speed and accuracy are critical [18].

4.1 Traditional Machine Learning Approaches

Conventional ML models such as Support Vector Machines (SVMs), k-Nearest Neighbors (kNN), Decision Trees, and Random Forests have been widely used for score- and feature-level fusion. These classifiers can handle heterogeneous

ISSN : 2455-9679
SJIF Impact Factor : 6.008

data by learning discriminative decision boundaries across multiple modalities. Ensemble methods, in particular, have shown effectiveness in reducing variance and improving robustness against noisy inputs [19].

4.2 Deep Learning-Based Fusion

With the rise of deep learning, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have become the backbone of modern multimodal biometric systems. CNNs are particularly effective for image-based modalities (e.g., face, fingerprint, iris), while RNNs handle sequential data such as voice and keystroke dynamics. Autoencoders and Generative Adversarial Networks (GANs) have also been explored for feature-level fusion, dimensionality reduction, and spoof detection [20].

4.3 Hybrid and Adaptive Fusion Models

Recent works propose hybrid models that combine ML classifiers with DL feature extractors to balance computational efficiency with accuracy. For example, CNN-extracted features from facial images can be fused with SVM-based classification of fingerprint scores, yielding high performance in mobile payment authentication. Adaptive fusion models further adjust the weight of each modality depending on environmental conditions (e.g., prioritizing fingerprint when face recognition fails under poor lighting).

4.4 Suitability for Digital Payments

In real-world payment systems, ML/DL-based fusion ensures low latency while maintaining high resistance to spoofing. Lightweight DL architectures and on-device inference are being increasingly optimized to operate efficiently on mobile and IoT devices. This makes ML-driven multimodal biometric systems practical for integration into e-wallets, contactless PoS systems, and ATM authentication frameworks.

V. Security and Privacy Concerns

While multimodal biometric fusion strengthens authentication in digital payments, it also introduces new security and privacy challenges.

5.1 Spoofing and Presentation Attacks

Biometric systems are vulnerable to spoofing, including fake fingerprints, 3D face masks, or replayed voice samples. Although multimodal systems reduce the likelihood of successful spoofing, adversaries may still exploit the weakest modality. Anti-spoofing techniques such as liveness detection, challenge–response protocols, and presentation attack detection (PAD) are increasingly integrated to mitigate these risks.

5.2 Template Security

Biometric templates, once compromised, cannot be revoked like passwords. Therefore, protecting stored templates in digital payment systems is critical. Techniques such as biometric cryptosystems, cancellable biometrics, and homomorphic encryption are being developed to ensure secure template storage and matching.

5.3 Privacy Regulations and Compliance

The use of biometrics raises privacy concerns, especially regarding data sharing, misuse, and surveillance. Regulatory frameworks such as GDPR (EU) and financial regulations (e.g., RBI guidelines in India) enforce strict rules for data collection, storage, and processing. Emerging solutions include federated learning and blockchain-based identity management, which reduce central storage risks while maintaining transparency.

5.4 Adversarial Machine Learning Threats

Recent research has shown that ML and DL-based biometric systems are susceptible to adversarial attacks, where imperceptible perturbations in input data cause misclassification. Continuous efforts are being made to develop robust models and adversarial defense strategies to ensure secure deployment in high-stakes applications such as payments [23].

VI. Applications in Secure Digital Payments

The integration of multimodal biometric fusion with machine learning has led to several practical applications in the digital payment's ecosystem. These applications aim to enhance transaction security, user convenience, and fraud resistance while maintaining compliance with financial regulations. Figure 3 showed the options used for secure digital payments.

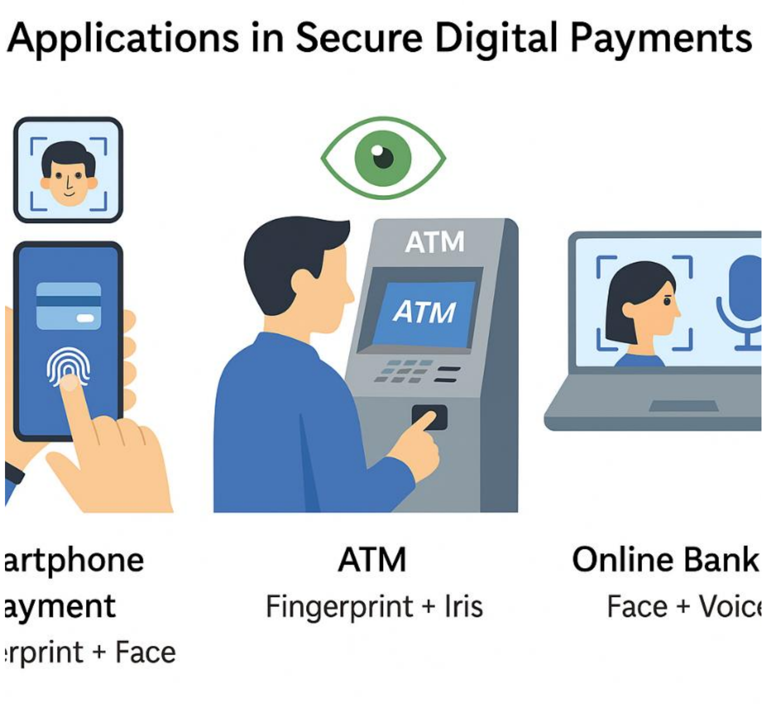

Figure 3 Applications in secure digital payments

6.1 Mobile Payment Authentication

Smartphones equipped with fingerprint sensors, front-facing cameras, and microphones enable seamless multimodal authentication for mobile wallets such as Google Pay, Apple Pay, and Paytm. Fusion of fingerprint and facial recognition provides robust verification, while voice or behavioral traits (e.g., touchscreen dynamics) serve as fallback mechanisms. Machine learning ensures low-latency recognition and adapts to real-world conditions such as variable lighting or background noise.

6.2 ATM and Point-of-Sale (PoS) Systems

Banks and retail systems are increasingly exploring multimodal biometric authentication at ATMs and PoS terminals. A common configuration combines fingerprint with face or iris recognition to secure cash withdrawals or high-value transactions. The use of decision-level or score-level fusion ensures that even if one modality fails due to poor capture conditions, the system can still authenticate users reliably.

6.3 E-Banking and Remote Verification

Remote banking applications integrate multimodal biometrics to prevent unauthorized access to accounts. Face recognition coupled with voice verification is commonly used during mobile logins or remote Know Your Customer (KYC) verification. In these contexts, machine learning-based liveness detection is crucial to counter replay or spoofing attacks.

6.4 Continuous and Context-Aware Authentication

Emerging digital payment systems employ continuous authentication, where behavioral modalities such as keystroke dynamics, gait, or touch patterns are continuously monitored alongside physiological traits. This ensures persistent verification during a payment session and reduces the risk of session hijacking.

6.5 High-Security Applications

For large financial institutions and critical infrastructures, multimodal fusion involving high-accuracy modalities such as iris, palm vein, or retina recognition is considered. These are combined with ML-driven adaptive fusion to deliver strong security against identity theft, especially in high-value transaction environments.

VII. Challenges and Research Gaps

Despite significant progress, the deployment of multimodal biometric fusion for secure digital payments faces several technical, operational, and ethical challenges.

7.1 Computational Complexity

Multimodal fusion often increases the computational burden, especially at the feature and score levels, where large volumes of data must be processed simultaneously. For mobile and IoT-based payment devices, implementing deep learning models in real-time without excessive power consumption remains a major barrier.

7.2 Interoperability and Standardization

Different banks, payment gateways, and mobile platforms employ heterogeneous biometric systems, making interoperability a persistent challenge. The absence of global standards for multimodal template storage and fusion protocols limits cross-platform adoption, particularly in international payment ecosystems.

7.3 Data Availability and Multimodal Datasets

Effective training of ML/DL fusion models requires large-scale multimodal biometric datasets representative of diverse demographics and real-world payment environments. However, public datasets are often limited to a single modality or lack realistic payment transaction scenarios, creating a gap between laboratory research and field deployment.

7.4 Balancing Security and User Convenience

While multimodal systems improve accuracy and spoof resistance, they may also reduce usability if multiple modalities are required for every transaction. Designing adaptive systems that selectively employ modalities based on risk levels (e.g., higher security for large transactions) remains an open research problem.

7.5 Privacy and Trust Issues

Even though encryption and cancellable biometrics offer protection, public trust in biometric payment systems is influenced by concerns about data misuse, surveillance, and lack of transparency. Robust frameworks for secure template management and explainable AI in decision-making are essential to improve acceptance.

7.6 Adversarial Machine Learning

The increasing reliance on ML/DL introduces vulnerability to adversarial attacks, where carefully perturbed inputs cause misclassification. Research into resilient architectures and real-time defense mechanisms against such attacks is still in its early stages, creating a significant gap for future exploration.

VIII. Future Research Directions

The future of multimodal biometric fusion in digital payments is shaped by advances in artificial intelligence, mobile hardware, and secure computing frameworks. Several key directions are likely to define upcoming research and deployment trends:

8.1 Lightweight and Edge-AI Models

To ensure real-time authentication on mobile devices, lightweight deep learning models such as MobileNet, SqueezeNet, and quantized CNNs should be further optimized. Edge-based AI will reduce dependence on cloud servers, lowering latency and preserving user privacy.

8.2 Blockchain-Enabled Identity Management

Integrating multimodal biometric authentication with blockchain-based identity platforms offers decentralized storage and tamper-resistant transaction logs. This can eliminate single points of failure in centralized systems and improve transparency in biometric usage.

8.3 Adaptive and Risk-Based Authentication

Future systems will likely incorporate context-aware and adaptive authentication, where modalities are selectively activated based on transaction value, user behavior, or environmental conditions. For instance, low-value payments may rely on a single modality, while high-value transfers trigger multimodal verification.

8.4 Continuous and Passive Authentication

Moving beyond one-time verification, continuous authentication through behavioral traits such as gait, keystroke, or touchscreen dynamics can enhance security. This approach ensures persistent monitoring against account hijacking without disrupting user experience.

8.5 Explainable and Trustworthy AI

As deep learning becomes central to biometric fusion, ensuring explainability and interpretability is essential. Explainable AI (XAI) methods will help regulators, financial institutions, and end-users trust ML-based decisions in payment systems.

8.6 Robustness Against Adversarial Attacks

Future research must also focus on developing resilient ML/DL architectures that can withstand adversarial manipulation. Defense strategies such as adversarial training, ensemble defenses, and robust feature representations will be crucial to safeguard payment authentication systems.

IX. Conclusion

The evolution of digital payment systems has created an urgent demand for authentication methods that are both highly secure and user-friendly. While traditional mechanisms such as passwords and PINs are increasingly vulnerable to fraud, biometric authentication offers a more reliable alternative. However, unimodal biometrics face challenges of spoofing, environmental sensitivity, and lack of universality, which limit their effectiveness in high-security financial environments.

This review has highlighted how multimodal biometric fusion, enhanced by machine learning and deep learning, addresses these shortcomings by combining complementary strengths of multiple modalities. Fusion at the sensor, feature, score, and decision levels enables systems to adapt to diverse conditions, while ML/DL approaches offer superior accuracy, adaptive weighting, and resilience against noise. In practical deployment, multimodal systems are already powering mobile wallets, ATM verification, and e-banking platforms, ensuring secure and convenient digital transactions.

At the same time, several challenges persist, including computational overhead, limited multimodal datasets, interoperability barriers, privacy concerns, and adversarial vulnerabilities. Addressing these issues requires continued research into lightweight models, blockchain-enabled identity systems, continuous authentication, and explainable AI frameworks.

In conclusion, ML-driven multimodal biometrics hold immense potential to serve as the cornerstone of secure digital payments. By balancing security, usability, and privacy, these systems can foster greater trust and accelerate the adoption of cashless economies worldwide.

:

REFERENCES

[1] A. Ozdemir and B. Gurses, “Digital payment systems and their impact on global finance,” Financ. Innov., vol. 7, pp. 1–15, 2021.

ISSN : 2455-9679
SJIF Impact Factor : 6.008

[2] S. Gupta and A. Arora, “Digital wallets and payment security: An Indian perspective,” J. Bank. Financ. Technol., vol. 6, no. 2, pp. 145–160, 2022.

[3] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York, NY, USA: Springer, 2007.

[4] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” Pattern Recognit. Lett., vol. 79, pp. 80–105, 2016.

[5] K. Nandakumar and A. Ross, “Multibiometric systems: Fusion strategies and applications,” Handbook of Statistics, vol. 29, pp. 263–294, 2020.

[6] S. Marcel, M. Nixon, and S. Li, Handbook of Biometric Anti-Spoofing. Cham, Switzerland: Springer, 2019.

[7] A. Rattani, R. Derakhshani, and A. Ross, “Selfie biometrics: Advances and challenges,” Comput. Vis. Image Underst., vol. 167, pp. 87–99, 2018.

[8] A. Ross and A. Jain, “Information fusion in biometrics,” Pattern Recognit. Lett., vol. 24, no. 13, pp. 2115–2125, 2003.

[9] N. Poh and J. Kittler, “A unified framework for biometric score fusion,” Pattern Anal. Appl., vol. 9, no. 4, pp. 464–478, 2006.

[10] A. K. Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics. New York, NY, USA: Springer, 2011.

[11] R. Sanchez-Reillo, “Biometric recognition for payment systems,” IEEE Consum. Electron. Mag., vol. 8, no. 6, pp. 49–54, 2019.

[12] A. Ross and R. Govindarajan, “Feature level fusion in biometric systems,” in Proc. Biometric Technology for Human Identification II, vol. 5779, SPIE, 2005, pp. 196–204.

[13] A. Jain and A. Ross, “Multibiometric systems,” Commun. ACM, vol. 47, no. 1, pp. 34–40, 2004.

[14] R. Shinde and S. Sonavane, “Multimodal biometric authentication using deep learning,” ICT Express, vol. 8, no. 2, pp. 178–183, 2022.

[15] F. Roli, J. Kittler, and T. Windeatt, “Multiple classifier systems in biometrics,” Pattern Recognit. Lett., vol. 33, no. 2, pp. 144–148, 2012.

[16] A. Raghavendra, K. Raja, and C. Busch, “Fingerprint and iris multimodal recognition using CNNs,” Pattern Recognit. Lett., vol. 91, pp. 87–94, 2017.

[17] A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template security,” EURASIP J. Adv. Signal Process., vol. 2008, no. 113, pp. 1–17, 2008.

[18] J. Yang, S. Li, and Y. Zhou, “Adversarial attacks and defenses in biometric recognition systems,” Neurocomputing, vol. 426, pp. 50–70, 2021.

[19] A. Ozdemir, B. Gurses, and S. Demir, “Cybersecurity issues in digital finance: A biometric perspective,” J. Inf. Secur. Appl., vol. 63, pp. 102–111, 2021.

[20] M. A. Ferrag, L. Maglaras, and A. Argyriou, “Secure and efficient biometric-based authentication for mobile payment systems,” Future Gener. Comput. Syst., vol. 102, pp. 104–118, 2020.