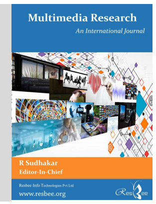
Vol. 9 Issue 2 April 2026

Multimedia Research

Received 4 February, Revised 26 March, Accepted 14 April



The Evolution of Biometric Authentication: Multimodal Fusion, Cancelable Templates, and Passive Liveness Detection in the Era of Deepfakes

Jouma Ali Al-Mohamad
Department of Computer and Mobile Communication Engineering
Faculty member at Al-Shahbaa Private University,
Faculty of Information Engineering, Aleppo, Syria.
jalmohamad@su.edu.sy

Abstract: Biometric authentication has undergone a paradigm shift from single-modal physical characteristics to sophisticated multimodal systems incorporating behavioral traits, continuous authentication, and advanced presentation attack detection. This evolution is driven by the increasing need for robust, adaptive, and user-centric identity verification mechanisms in digitally connected ecosystems. With global losses from identity fraud exceeding $50 billion in 2024 and deepfake incidents quadrupling between 2023 and 2024, the security community faces unprecedented challenges in verifying digital identity.These developments highlight the critical importance of integrating advanced detection and mitigation strategies into authentication pipelines. This article presents a comprehensive review of cutting-edge developments in biometric authentication, including optical scanning holography for cancellable templates achieving Equal Error Rates (EER) as low as 0.0035, wavelet scattering transforms combined with RSA encryption for speech protection, and passive liveness detection as the emerging gold standard for frictionless security. We analyze multimodal fusion architectures, tactical-grade wearable biometrics for extreme environments, and novel behavioral modalities such as in-air signatures verified through Siamese neural networks. The analysis further considers system scalability, interoperability, and real-time performance constraints in practical deployment scenarios. The paper concludes with future research directions addressing deepfake resilience, synthetic data augmentation, and privacy-preserving biometric systems. It also emphasizes the necessity of developing standardized frameworks and ethical guidelines to ensure trustworthy and responsible use of biometric technologies.

Keywords: Multimodal Biometrics; Cancelable Templates; Passive Liveness Detection; Presentation Attack Detection; Optical Scanning Holography; Wavelet Scattering Transform; Continuous Authentication; Behavioral Biometrics; Deepfake Detection; Template Protection; ISO/IEC 30107; Edge AI Biometrics.

Nomenclature

Abbreviation	Description
AROC	Area Under the Receiver Operating Characteristic Curve
AWGN	Additive White Gaussian Noise
BQAT	Biometric Quality Assessment Tool
CNN	Convolutional Neural Network
DOI	Digital Object Identifier
ECG	Electrocardiogram
EEG	Electroencephalography
EER	Equal Error Rate
EMD	Empirical Mode Decomposition
GAN	Generative Adversarial Network
IMU	Inertial Measurement Unit
ISO	International Organization for Standardization
LSTM	Long Short-Term Memory
MOSIP	Modular Open Source Identity Platform
OSH	Optical Scanning Holography
PAD	Presentation Attack Detection
PIN	Personal Identification Number
PPG	Photoplethysmography
RSA	Rivest–Shamir–Adleman (encryption algorithm)
SNR	Signal-to-Noise Ratio
TIMIT	Texas Instruments/Massachusetts Institute of Technology Speech Dataset
UX	User Experience
WST	Wavelet Scattering Transform

1. Introduction

The digital identity landscape of 2026 is characterized by a fundamental tension: the demand for seamless user experience clashes with the escalating sophistication of fraud attempts. This tension is further intensified by the rapid digitalization of services across finance, healthcare, and governance sectors, where identity verification is critical. Traditional knowledge-based authentication (passwords, PINs) and token-based methods have proven inadequate against modern threats, while biometrics offer the promise of authenticating "who you are" rather than "what you know" or "what you have" [2][15]. As a result, biometric systems are increasingly positioned as a cornerstone of next-generation identity infrastructures. However, the biometric landscape itself has grown increasingly complex. Emerging attack vectors and adversarial AI techniques continue to challenge the reliability of standalone biometric modalities. The proliferation of deepfakes, AI-generated synthetic identities, and sophisticated presentation attacks has rendered first-generation biometric systems vulnerable. These threats exploit both algorithmic weaknesses and gaps in sensor-level security, necessitating holistic system redesigns. A sobering statistic illustrates the urgency: global losses from identity fraud climbed over $50 billion in 2024, growing more than 20% year-over-year, while detected deepfakes quadrupled between 2023 and 2024 [3][5]. Such trends indicate that threat actors are leveraging scalable, automated tools to bypass conventional verification mechanisms. Simultaneously, user expectations have hardened: 72% of users abandon applications during onboarding if it requires too many steps, creating a UX-security paradox that demands innovative solutions [9]. Balancing minimal user friction with maximum security assurance has therefore become a central design challenge.

This review examines how the biometric authentication field is responding through three interconnected technological vectors: (1) multimodal fusion that combines multiple biometric traits for enhanced accuracy and spoof resistance, (2) cancelable biometrics and template protection schemes that safeguard irreplaceable biometric data, and (3) passive liveness detection that operates invisibly while maintaining robust security. Together, these vectors represent a shift toward more resilient, privacy-aware, and user-adaptive authentication ecosystems. Fig. 1 illustrates the rising trend of global identity fraud losses and deepfake incidents from 2020 to 2025.

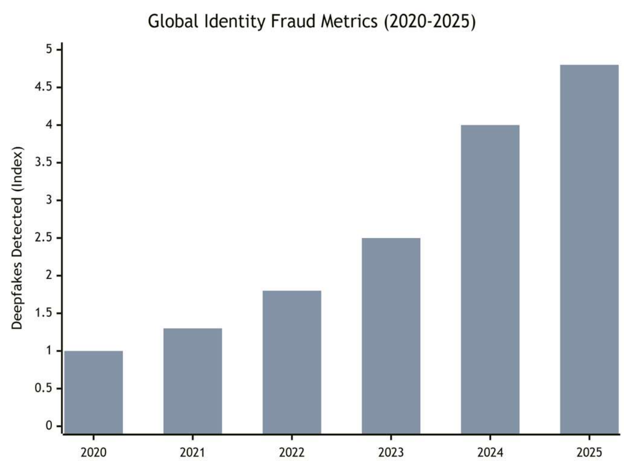


Fig. 1. *Global Identity Fraud Losses and Deepfake Growth (2020-2025)*

2. Theoretical Foundations: The Biometric System Architecture

A modern biometric authentication system comprises four essential subsystems, each presenting unique challenges and opportunities for innovation: These subsystems collectively define the operational pipeline of biometric systems and form the basis for subsequent advancements discussed in this paper.

1. **Sensor Subsystem:** Captures raw biometric data (fingerprint images, voice samples, facial video, etc.).
2. **Feature Extraction Subsystem:** Transforms raw data into mathematical representations (templates).
3. **Matching Subsystem:** Compares extracted templates against enrolled references.
4. **Decision Subsystem:** Applies threshold-based or probabilistic rules to accept/reject claims.

Professor Arun Ross of Michigan State University, in his keynote at MOSIP Connect 2026, emphasized critical considerations for robust system design: intra-user variations (how the same individual's biometrics change over time), inter-user similarities (overlap between different individuals' characteristics), noisy data acquisition, and non-universality (users whose biometrics are consistently poor quality) [2]. These factors necessitate sophisticated signal processing and machine learning approaches. These foundational challenges motivate the exploration of advanced biometric modalities and security mechanisms in the following sections. Fig. 2 illustrates the generic architecture of a biometric authentication system, including sensor, feature extraction, matching, and decision subsystems.

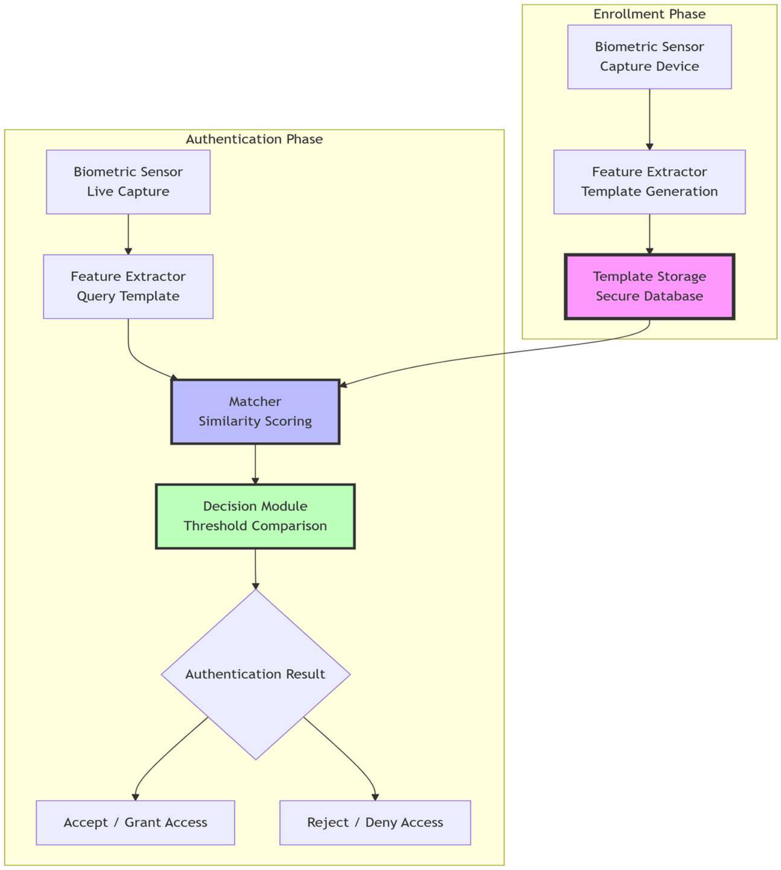


Fig. 2. *Generic Biometric Authentication System Architecture*

3. Emerging Biometric Modalities

3.1 Physiological Modalities: Beyond Fingerprints and Face

Traditional physiological biometrics (fingerprint, face, iris) have matured significantly, but new modalities and acquisition methods are expanding the field: These modalities enable more continuous, unobtrusive, and context-aware authentication systems.

3.1.1 Electrocardiogram (ECG) Biometrics

The heart's electrical activity, captured through wearable sensors, offers unique morphological characteristics (QRS complex, P-wave, T-wave patterns) that are highly individualistic and enable continuous verification [6]. However, motion artifacts and electrode position variability remain significant challenges for battlefield and athletic applications. Recent advances in AI-driven denoising and adaptive filtering are enhancing robustness [6].

3.1.2 Photoplethysmography (PPG):

Optical sensors measuring blood volume changes, commonly integrated into wristbands and smart rings, provide lightweight, energy-efficient biometric capture. Multi-wavelength PPG combined with accelerometer data has improved accuracy during physical exertion [6].

3.1.3 Electroencephalography (EEG)

Neural activity patterns captured through dry electrodes integrated into helmet systems offer indicators of both identity and cognitive state (fatigue, workload, stress). Susceptibility to motion-induced artifacts requires careful mechanical and electrical design [6].

3.2 Behavioral Modalities: The Dynamics of Identity

Behavioral biometrics capture how individuals perform actions, adding a temporal dimension that complicates forgery attempts: The temporal and dynamic nature of these modalities significantly increases resistance to spoofing and replay attacks. Fig. 3 illustrates the pipeline for in-air signature capture and verification, including motion acquisition, feature extraction, and classification stages.

3.2.1 In-Air Signatures

A novel contactless modality where users sign in three-dimensional space using fingertip tracking or depth sensing. Unlike static image-based signatures, in-air signatures contain temporal and dynamic motion patterns (velocity, acceleration, trajectory) that are more resilient to forgery [7]. A recent study using Bidirectional Siamese LSTM networks achieved 85% accuracy, 85% F1-score, and 91% recall with limited training data, demonstrating feasibility even in resource-constrained environments [7].

3.2.2 Gait Analysis

Walking patterns captured through inertial measurement units (IMUs) in wearable devices or vision systems enable continuous authentication. Tactical-grade IMUs with improved bias stability are particularly valuable for military applications where GPS may be denied [6].

3.2.3 Voice Dynamics

Beyond simple speaker recognition, modern systems analyze prosodic features, speaking style, and idiosyncratic pronunciation patterns. The wavelet scattering transform approach has demonstrated exceptional robustness, achieving 99.94% accuracy on the Chinese Mandarin Corpus even with car noise corruption [4].

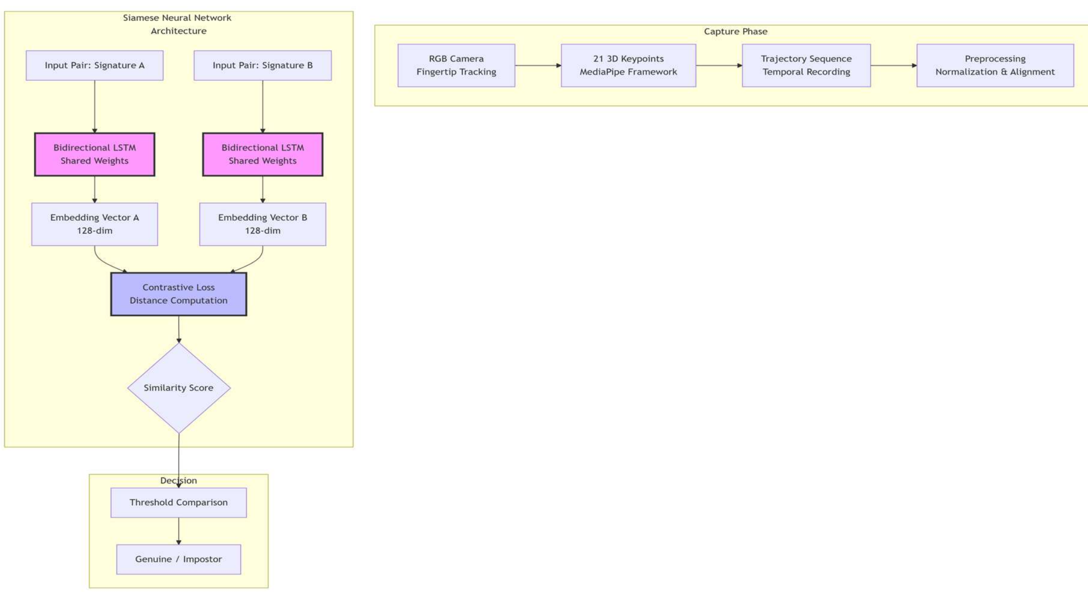


Fig. 3. *In-Air Signature Capture and Verification Pipeline*

4. Advanced Security Mechanisms

4.1 Cancelable Biometrics: Protecting Irreplaceable Data

Unlike passwords, biometric data cannot be changed if compromised. A stolen fingerprint or iris pattern is compromised forever. Cancelable biometrics addresses this fundamental vulnerability through intentional, repeatable distortions of biometric signals [14]. This approach ensures that compromised templates can be revoked and replaced without affecting the original biometric trait.

4.1.1 Optical Scanning Holography (OSH) for Cancelable Templates

A groundbreaking approach utilizes OSH to transform speech signals into 2-D matrices, which are then encrypted to create cancellable templates. This method ensures non-invertibility (original data cannot be reconstructed) and diversity (different applications receive different transformed versions). Evaluation metrics demonstrate exceptional performance: EER of 0.0035 and AROC of 0.9991, significantly outperforming existing approaches [1][4][12].

4.1.2 Wavelet Scattering Transform (WST) with RSA Encryption

A hybrid framework combines non-invertible wavelet scattering with RSA encryption for speech signal protection. WST introduces irreversibility, preventing reconstruction of original voice signals, while RSA provides robust cryptographic security. Results show remarkable resilience: 99.87% accuracy with EER of 0.0179 for AWGN on TIMIT dataset, and 99.94% accuracy with EER of 0.0062 for Chinese Mandarin Corpus [4][13].

4.1.3 Empirical Mode Decomposition (EMD)

Recent work has applied EMD with quaternion representations for IoT security, demonstrating effectiveness in resource-constrained environments [4]. Fig. 4 illustrates the framework for generating cancelable biometric templates through transformation and encryption of raw biometric data. Table 1 presents a comparative analysis of cancelable biometric techniques based on accuracy, EER, AROC, and dataset performance.

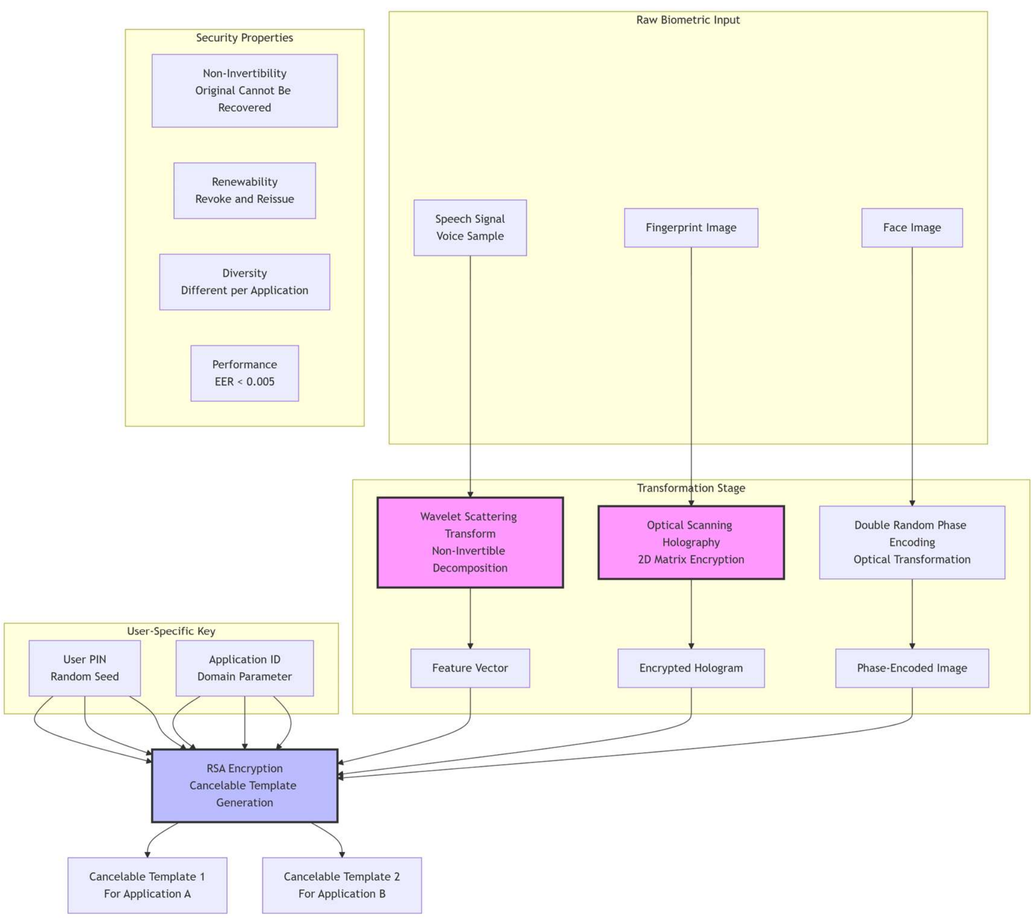


Fig. 4. *Cancelable Biometric Template Generation Framework*

Table 1. *Performance Comparison of Cancelable Biometric Techniques*

Technique	Modality	Dataset	Accuracy (%)	EER	AROC	Reference
Optical Scanning Holography	Speech	TIMIT	99.65	0.0035	0.9991	[1]
Wavelet Scattering + RSA	Speech	TIMIT (AWGN)	99.87	0.0179	0.982	[4]
Wavelet Scattering + RSA	Speech	Chinese Mandarin	99.94	0.0062	0.994	[4]
Double Random Phase Encoding	Multimodal	Custom	99.2	0.008	0.991	[1]
EMD + Quaternion	ECG	IoT-ECG	98.7	0.021	0.976	[4]

4.2 Presentation Attack Detection (PAD): Defeating Spoofing

Presentation attacks—using photos, videos, masks, or deepfakes to deceive biometric systems—represent the most direct threat to biometric security. The ISO/IEC 30107 standard provides a framework for evaluating PAD effectiveness [10][11]. The increasing realism of synthetic media has made PAD an essential component of modern biometric systems. Fig. 5 illustrates the comparison between passive and active liveness detection methods in terms of user interaction, security, and usability.

4.2.1 Passive Liveness Detection

The industry has shifted decisively toward passive liveness detection as the new gold standard. Unlike active methods requiring user actions ("blink now," "turn your head"), passive liveness operates invisibly during normal capture. Advanced AI algorithms analyze dozens of signals—3D depth, skin translucence, texture patterns, involuntary micro-movements, spectral reflectance—to confirm physical presence [9].
A real-world banking case demonstrated the impact: moving to passive liveness improved completion rates by 35%, achieving 95% onboarding success while maintaining robust security [9]. Kneron recently achieved perfect scores in independent ISO/IEC 30107-3 PAD testing, demonstrating resilience against a range of spoofing attempts [8].

4.2.2 Active Liveness (Legacy Approach)

While still used in some high-risk scenarios, active methods introduce significant friction and accessibility barriers. Users with disabilities may struggle with required movements, and pre-recorded video attacks can sometimes bypass these checks [10].

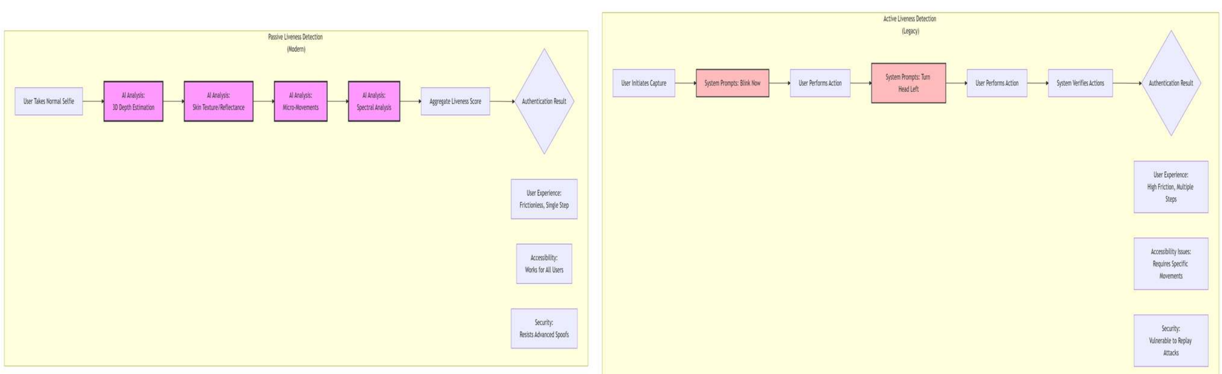


Fig. 5. *Passive vs. Active Liveness Detection Comparison*

5. Multimodal Fusion: Strength in Diversity

Single-modal biometric systems suffer from inherent limitations: noisy data, non-universality, spoof vulnerability, and performance degradation under varying conditions. Multimodal fusion addresses these limitations by combining multiple biometric sources [3][15]. This integration enhances robustness, accuracy, and resistance to spoofing attacks. Fig. 6 illustrates the different architectures for multimodal biometric fusion, including sensor-level, feature-level, score-level, and decision-level integration.

5.1 Fusion Architectures

- **Sensor-Level Fusion:** Combining raw data from multiple sensors before feature extraction. Example: merging fingerprint and finger vein images from a hybrid sensor.

- **Feature-Level Fusion:** Concatenating feature vectors extracted from different modalities. Challenges include dimensionality and incompatible feature formats.
- **Score-Level Fusion:** Combining matching scores from multiple classifiers. This is the most common approach due to its flexibility and relatively simple implementation.
- **Decision-Level Fusion:** Integrating final accept/reject decisions through voting or logical rules.

Each level offers distinct trade-offs in terms of complexity, flexibility, and performance.

5.2 Adaptive Multimodal Systems

Recent research emphasizes adaptive systems that dynamically select optimal fusion strategies based on context, quality assessment, and available modalities [3]. Synthetic data augmentation through GANs has emerged as a powerful technique for training robust multimodal systems when real paired data is scarce [3].

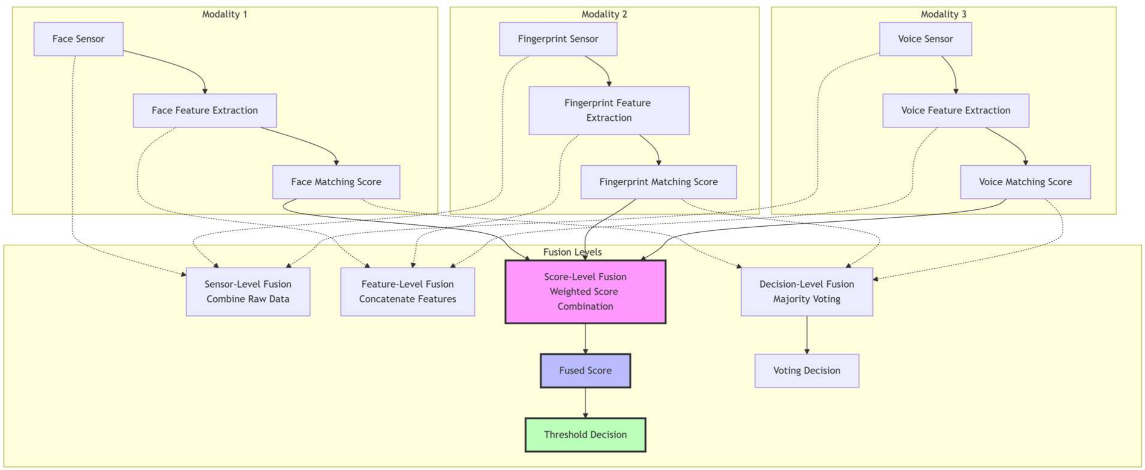


Fig. 6. *Multimodal Biometric Fusion Architectures*

6. Continuous Authentication: Beyond Point-in-Time Verification

Traditional biometric authentication performs a one-time check at login, leaving sessions vulnerable to hijacking. Continuous authentication addresses this gap by passively monitoring behavioral and physiological characteristics throughout a session [6]. This paradigm significantly reduces the risk of session hijacking and unauthorized access. Fig. 7 illustrates the architecture of a continuous authentication system, showing how behavioral and physiological data are monitored and analyzed in real time for ongoing user verification.

6.1 Modalities for Continuous Authentication

- **Keystroke Dynamics:** Typing rhythm, dwell time, and flight time provide distinctive patterns that can be continuously verified.
- **Mouse/Gesture Dynamics:** Movement trajectories, acceleration, and click patterns.
- **PPG/ECG from Wearables:** Heart signals enable continuous verification without active user participation [6].
- **Gait from IMUs:** Walking patterns can authenticate users continuously in mobile and tactical environments [6].

These modalities enable seamless and unobtrusive identity verification.

6.2 Edge AI for On-Device Processing

Continuous authentication generates vast amounts of data; transmitting raw biometrics to central servers raises privacy concerns and consumes bandwidth. Edge AI—performing authentication directly on user devices—has emerged as the preferred architecture. Modern systems leverage low-power neural accelerators to run inference continuously with minimal battery impact [8].

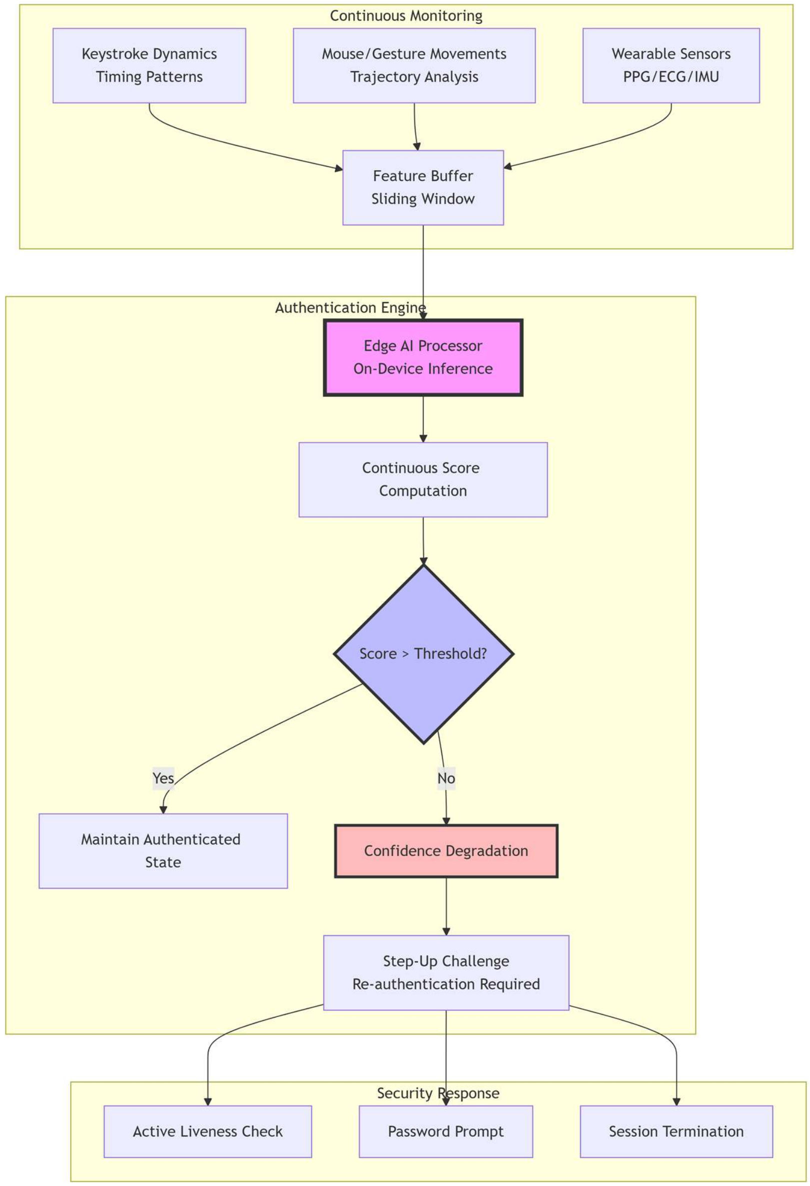


Fig. 7. *Continuous Authentication System Architecture*

7. Tactical-Grade Biometrics: Extreme Environment Authentication

Military and first responder applications impose unique requirements: operation under extreme temperatures, electromagnetic interference, high-gravity maneuvers, and physiological stress [6]. Fig. 8 illustrates a tactical-grade wearable biometric system integrating multiple sensors for reliable authentication in extreme environments.

7.1 Operational Challenges

- **Physiological Variability:** Fatigue, dehydration, and injury can alter biometric signatures, potentially increasing false rejection rates.
- **Environmental Noise:** Motion artifacts, equipment interference, and variable lighting degrade sensor performance.
- **Security Threats:** In hostile environments, biometric systems must resist physical tampering, electronic interception, and presentation attacks.

7.2 Multimodal Solutions for Tactical Environments

Tactical-grade wearables integrate multiple sensing modalities to maintain reliability under stress [6]:

- ECG sensors with AI-driven denoising for cardiac biometrics
- PPG with accelerometer fusion for motion artifact compensation
- EEG with dry electrodes in helmet systems for neural monitoring
- IMU-based gait analysis for continuous authentication in GPS-denied environments

Such multimodal integration ensures reliable authentication even under extreme conditions.

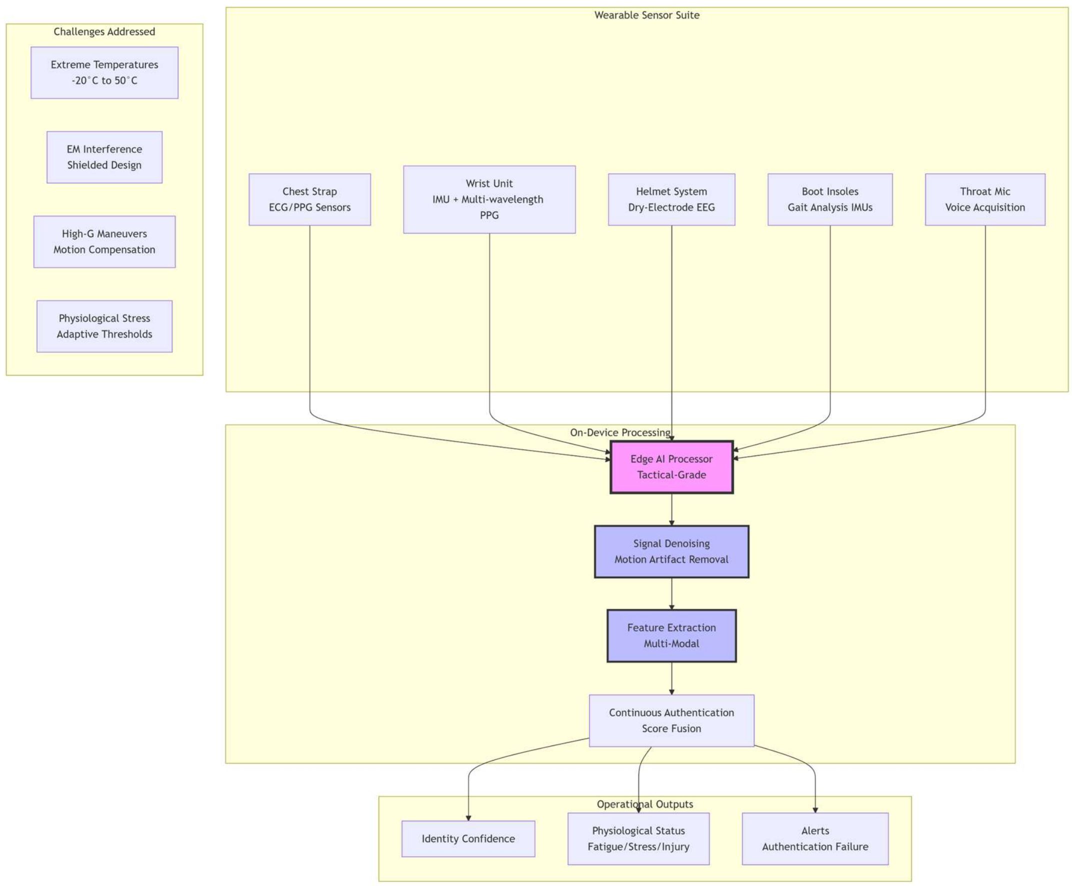


Fig. 8. *Tactical-Grade Wearable Biometric System*

8. Real-World Applications and Case Studies

8.1 Financial Services: Retail Biometrics at Scale

AuthID reported a 472% increase in biometric enrollments at a major global retailer over the past year, driven by renewed investment in identity capture, consent flows, and integration with loyalty systems [8]. This scale-up illustrates how large retailers are driving adoption beyond loss prevention into broader customer experience enhancement.

8.2 Government Digital Identity: Brazil's Gov.br

Brazil's Gov.br platform represents one of the largest digital identity deployments globally, using facial biometrics with passive liveness to authenticate citizens for thousands of services. The platform has enrolled approximately 170 million users, digitized 92% of federal services, and achieved billions in annual savings [9]. Officials credit success to frictionless UX combined with strong biometric security.

8.3 Dating Apps: Regulatory-Driven Adoption

Hinge has made face verification mandatory for new users in certain markets in response to UK and Australia age verification regulations. This illustrates how regulatory trends are shaping biometric deployment in consumer platforms [8].

8.4 Border Control: EU Entry/Exit System (EES)

The UK travel industry is urging the EU to grant operational flexibility for biometric border checks, citing concerns about throughput and queue management. This highlights the tension between security requirements and user experience in high-volume applications [8].
Table 2 presents real-world biometric deployments across sectors, highlighting modalities used, scale of implementation, and observed outcomes.

Table 2. *Real-World Biometric Deployments and Outcomes*

Application	Organization	Modality	Scale	Outcome	Reference
Retail Customer ID	Global Retailer (AuthID)	Face/Fingerprint	472% enrollment growth	Enhanced loyalty integration	[8]
National Digital ID	Brazil Gov.br	Face + Passive Liveness	170M users, 92% digitized	$Billions saved annually	[9]
Dating App Verification	Hinge	Face (Mandatory)	Multi-country rollout	Age compliance	[8]
Banking Onboarding	Anonymous Bank	Passive Liveness	95% completion rate	35% improvement	[9]
Military Authentication	NATO Research	Multimodal Wearables	Field trials	Enhanced readiness	[6]

9. Future Research Directions

9.1 Deepfake-Resistant Biometrics

As generative AI improves, biometric systems must evolve to detect increasingly sophisticated synthetic media. Research priorities include [3][5]: Future systems must integrate cross-modal verification and temporal consistency analysis to counter deepfake-based attacks.

- Analyzing physical consistency across video frames
- Detecting physiological signals (pulse, blood flow) in video
- Leveraging multi-spectral imaging beyond visible spectrum

9.2 Synthetic Data Augmentation

High-quality, diverse training data remains a bottleneck for biometric system development. Data scarcity is particularly critical in multimodal systems requiring synchronized datasets across modalities. GAN-generated synthetic biometrics offer a path to larger, more representative datasets while addressing privacy concerns [3]. Recent work demonstrates that synthetic data can effectively augment real datasets for training robust recognition systems [3].

9.3 Privacy-Preserving Biometrics

Beyond cancelable templates, emerging approaches include [1][4][14]: These techniques aim to reconcile strong authentication with stringent data protection regulations.

- Homomorphic encryption enabling matching on encrypted data
- Secure multiparty computation for distributed authentication
- Zero-knowledge proofs for age verification without identity disclosure

9.4 Standardization and Interoperability

The biometric community continues working toward common standards for [2][10]: Standardization is essential for ensuring interoperability, scalability, and regulatory compliance across systems.

- Presentation attack detection testing (ISO/IEC 30107)
- Biometric data quality assessment (BQAT/OpenBQ)
- Cross-platform template interoperability

Fig. 9 illustrates the future research roadmap for biometric authentication, highlighting key directions such as deepfake resilience, privacy-preserving methods, and synthetic data augmentation.

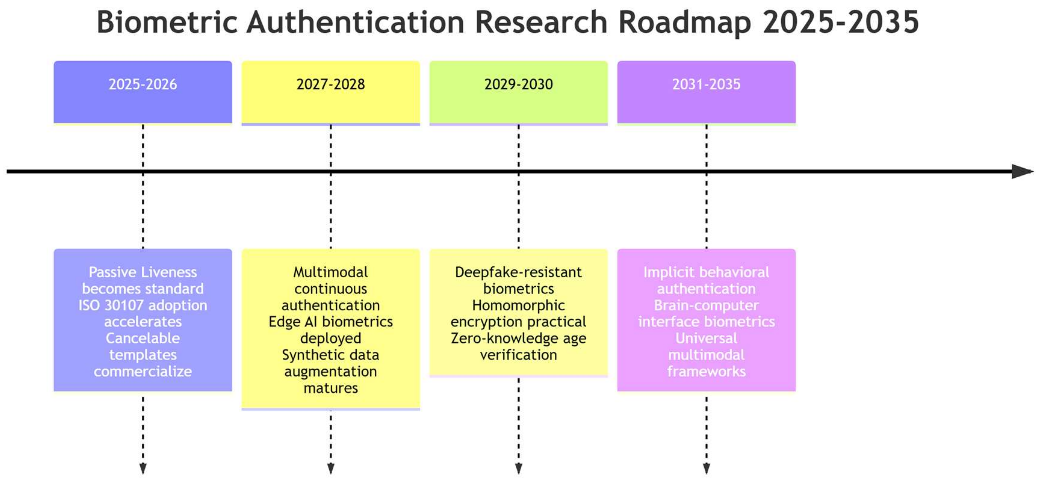


Fig. 9. *Future Research Roadmap for Biometric Authentication*

10. Conclusion and Recommendations

The field of biometric authentication stands at a critical inflection point. Rapid advancements in artificial intelligence and sensor technologies are redefining both capabilities and threat landscapes. The convergence of sophisticated threats (deepfakes, presentation attacks) with demanding user expectations (frictionless experience) has driven innovation across multiple fronts:

1. **Cancelable biometrics** have matured from academic concept to practical deployment, with optical scanning holography and wavelet scattering transforms achieving exceptional performance (EER < 0.005) while ensuring biometric data remains renewable and private [1][4].
2. **Passive liveness detection** has emerged as the new standard, eliminating user friction while maintaining robust security against spoofing attempts [9][10].
3. **Multimodal fusion**—particularly when enhanced with synthetic data augmentation—addresses the inherent limitations of single-modal systems [3].
4. **Continuous authentication** through wearable sensors and behavioral monitoring provides protection beyond point-in-time verification [6].
5. **Tactical-grade systems** demonstrate that biometrics can operate reliably under extreme conditions when properly engineered [6].

These advancements collectively indicate a shift toward intelligent, adaptive, and privacy-aware authentication ecosystems.

For organizations deploying biometric systems, the following recommendations are proposed:

- **Prioritize passive liveness** over active methods to maximize conversion rates [9]
- **Implement cancelable templates** to future-proof against data breaches [1][4]
- **Consider multimodal approaches** for high-security applications [3]
- **Adopt ISO/IEC 30107 testing** to validate PAD effectiveness [10]
- **Plan for continuous authentication** in high-risk sessions [6]

The next decade will witness further integration of biometrics into everyday life, from retail payments to national digital identity. Emerging paradigms such as decentralized identity and edge AI will further accelerate this integration. The challenge lies not in achieving high accuracy in controlled conditions—which current systems already demonstrate—but in maintaining that accuracy under real-world variability while preserving user privacy and resisting ever-more-sophisticated attacks.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] El-Shafai, W., El-Gazar, S., Salama, G.M., et al. (2026). Optical scanning holography for secure biometric access and modulation classification: a software-based approach. *Multimedia Tools and Applications*, 85, 138. https://doi.org/10.1007/s11042-025-15678-9

[2] Ross, A. (2026). Building robust biometric systems: intra-user variations, inter-user similarities, and presentation attacks. *MOSIP Connect 2026 Keynote*. https://mosip.org/connect2026

[3] Singh, L., Kumar, A., Golash, R. (2026). A review on advancing biometric authentication through integrating multimodal fusion with synthetic data augmentation for adaptive systems. *The European Physical Journal Plus*, 141(1), 45. https://doi.org/10.1140/epjp/s13360-026-01567-8

[4] El-Gazar, S., El-Shafai, W., El-Banby, G.M., et al. (2026). Securing biometric authentication: a hybrid approach with non-invertible wavelet scattering transform and RSA encryption for speech signal protection. *Multimedia Tools and Applications*, 85, 139. https://doi.org/10.1007/s11042-025-15679-8

[5] Miller, C. (2026). Emerging Payments Trends Report. *Javelin Strategy & Research*. https://javelinstrategy.com/research

[6] Greek, M., et al. (2026). Tactical-Grade Wearables and Authentication Biometrics. *Sensors*, 26(3), 759. https://doi.org/10.3390/s26030759

[7] Yilmaz, M.B., et al. (2026). Contactless biometric verification from in-air signatures using deep siamese networks. *Scientific Reports*, 16, 130. https://doi.org/10.1038/s41598-026-00123-5

[8] ID Tech Editorial Team. (2026, February 6). ID Tech Digest. *ID Tech*. https://idtech.com/news

[9] Ramos, R. (2026). 2026 Trends in biometrics and digital verification. *Identy.io*. https://identy.io/trends2026

[10] International Organization for Standardization. (2024). ISO/IEC 30107-3:2024 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. ISO.

[11] National Institute of Standards and Technology. (2025). NIST SP 800-63-4 Digital Identity Guidelines. https://doi.org/10.6028/NIST.SP.800-63-4

[12] Poon, T.C. (2007). *Optical scanning holography with MATLAB*. Springer, New York.

[13] Mallat, S. (2012). Group invariant scattering. *Communications on Pure and Applied Mathematics*, 65, 1331–1398. https://doi.org/10.1002/cpa.21413

[14] Patel, V.M., Ratha, N.K., Chellappa, R. (2015). Cancelable biometrics: a review. *IEEE Signal Processing Magazine*, 32, 54–65. https://doi.org/10.1109/MSP.2015.2434151

[15] Sahoo, S.K., Choubisa, T., Prasanna, S.R.M. (2012). Multimodal biometric person authentication: a review. *IETE Technical Review*, 29, 54–75. https://doi.org/10.4103/0256-4602.93139