UDC 57.087.1-027.45

HOW RELIABLE ARE MODERN BIOMETRIC SYSTEMS?

Gurskaya A. S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Likhtarovitch I. I. – Senior Lecturer at the Department of Foreign Languages

Annotation. This paper examines the reliability of contemporary biometric authentication systems by analysing performance indicators, error rates and security vulnerabilities. It highlights the balance between user convenience and strengthened access control, as well as the technical and ethical challenges of deployment. Fingerprint, facial and iris recognition are representative modalities illustrating the growing role of biometrics in digital security systems.

Keywords. biometric authentication, system reliability, false acceptance rate (FAR), false rejection rate (FRR), multimodal verification, data protection, vulnerability assessment.

***Introduction*.** The conceptual foundations of identification through inherent human traits extend back to the late nineteenth century, when fingerprint classification systems were first adopted for forensic purposes in criminal investigations. However, the digital transformation of biometric technologies accelerated markedly in the early 2000s, driven by exponential growth in computational capabilities, the emergence of high-resolution optical and capacitive sensors, and refinements in pattern-recognition algorithms [1]. A pivotal paradigm shift occurred around 2020, when artificial intelligence and deep learning architectures began enhancing feature extraction, liveness detection, and adaptive decision-making processes in real-time authentication scenarios. Convolutional neural networks now enable systems to detect subtle texture variations beyond visual perception, significantly reducing susceptibility to high-quality forgeries. This evolution allows algorithms to adapt to gradual changes in a user's biometric characteristics over time, maintaining accuracy without requiring frequent re-enrollment. Such adaptive learning ensures that the system remains resilient against natural aging processes while preserving the speed of verification [2]. Contemporary implementations now achieve near-human-level precision under controlled environmental conditions, with some commercial systems reporting accuracy rates exceeding 99.8% for fingerprint and iris modalities [3]. Consequently, biometrics has emerged as a disruptive force, reshaping conventional security models by enabling seamless, individualised verification experiences that transcend traditional knowledge– or possession-based credentials [1].

Main part. A primary strength of biometric systems lies in their capacity for robust identity confirmation. Unlike conventional password-based approaches or physical tokens, physiological and behavioural traits are inherently bound to the individual – they cannot be misplaced, forgotten, or casually transferred among users. Advanced algorithms process distinctive markers, such as ridge endings and bifurcations in fingerprints, geometric facial landmarks, or the complex vascular patterns of the iris, to authenticate individuals within milliseconds [3]. This functionality resembles a personalised, always-available security protocol, often surpassing traditional methods in both operational speed and user experience.

Modern biometric solutions are increasingly embedded in consumer electronics and enterprise environments. For instance:

1 Windows Hello leverages infrared facial mapping combined with liveness detection to enable passwordless device access.

2 Mobile banking applications employ AI-driven behavioural analysis to authorise transactions while detecting spoofing attempts.

3 Automated border control systems integrate e-passport data with real-time facial comparison to accelerate passenger processing without compromising security thresholds [1].

These implementations illustrate how biometrics streamlines routine verification tasks while maintaining adaptive, context-aware security policies. Organisations further utilise such frameworks for workforce management – automating attendance logs, restricting physical access to sensitive

infrastructure, and generating tamper-resistant audit records. The outcome is enhanced operational efficiency, reduced administrative overhead, and scalable security architecture capable of supporting thousands of simultaneous authentications.

From an end-user standpoint, biometric authentication offers tangible benefits: unlocking a smartphone via fingerprint sensor, approving a contactless payment with facial recognition, or accessing cloud-based services without memorising complex credential combinations (Figure 1). Personal experience confirms that enabling facial recognition on a personal device significantly reduces login friction while maintaining a strong security posture. Nevertheless, this convenience necessitates mindful usage practices. Biometric templates, once compromised through data breaches or insecure storage protocols, cannot be “reset” in the manner of traditional passwords – making transparent data-handling policies and robust encryption essential for long-term trust. Furthermore, the permanence of biometrical identifiers necessitates a higher standard of care compared to traditional credentials. Unlike a compromised password that can be changed instantly, a leaked biometric template remains a permanent vulnerability. Consequently, users should prioritize systems that employ template protection schemes, such as hashing or encryption, ensuring that raw biometric data is never stored in a reversible format. This approach mitigates the risk of identity theft even in the event of a server-side breach [4].

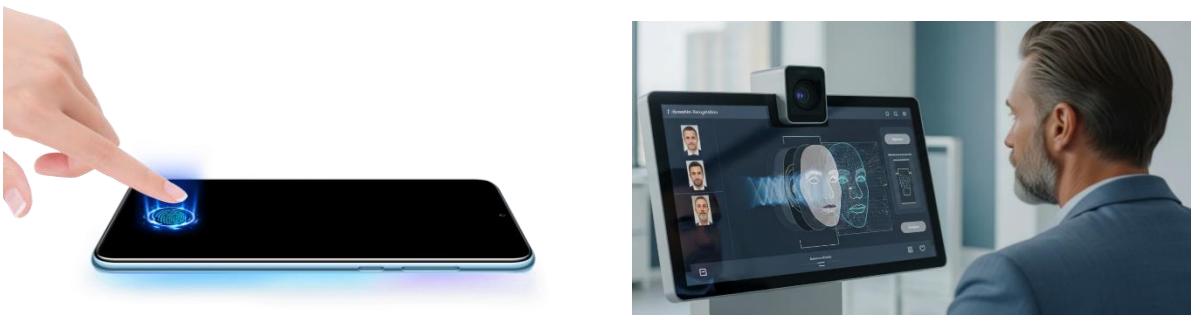

Figure 1 – Biometric authentication interfaces in consumer electronics: capacitive fingerprint sensor, infrared facial recognition camera, and near-infrared iris scanner

Contemporary users frequently incorporate such tools into daily digital routines. The appeal lies not merely in time savings, but in the capacity to maintain consistent security across multiple devices and services without cognitive overload. However, widespread adoption also raises important questions regarding dependency, privacy preservation, and the irreversible nature of biological data exposure.

Despite remarkable technological progress, biometric systems remain probabilistic rather than deterministic in their operation. Three categories of operational errors warrant sustained user awareness:

1 False Acceptance Rate (FAR): the statistical probability that an unauthorised individual is incorrectly granted system access – a critical metric for high-security applications.

2 False Rejection Rate (FRR): the likelihood that a legitimate user is erroneously denied entry, potentially causing frustration or operational delays.

3 Contextual Sensitivity: performance degradation attributable to environmental variables (e.g., low illumination, sensor contamination) or physiological changes (e.g., minor injuries, aging effects, temporary alterations in appearance).

FAR and FRR exibit an inverse relationship: lowering one inevitably raises the other. Administrators must therefore calibrate thresholds based on context – prioritising low FAR for high-security environments and low FRR for consumer-facing applications to balance protection with usability.

Two interrelated challenges merit particular attention in deployment planning:

1 Single-point dependency risk: Users may disable supplementary security layers (e.g., PIN codes, hardware tokens) when biometrics feels “sufficient”, inadvertently weakening overall protection through reduced defence-in-depth.

2 Data sovereignty and privacy: Biometric templates represent highly sensitive personal information. Inadequate encryption standards, centralised storage architectures, or unauthorised secondary usage can erode user trust and expose individuals to identity-related threats with potentially irreversible consequences [4].

To harness biometric technologies effectively while minimising associated risks, both individual users and institutional stakeholders should consider the following practices:

1 Implement multifactor authentication frameworks, combining biometric verification with a knowledge-based factor (e.g., PIN) or possession-based token to create layered security.

2 Verify data storage and processing protocols – prefer on-device template storage over cloud-based solutions where feasible, and ensure compliance with relevant data protection regulations.

3 Explore multimodal biometric systems that fuse multiple independent traits (e.g., face + voice + behavioural dynamics) to improve overall accuracy, resilience against spoofing, and accessibility for diverse user populations. For instance, combining facial recognition with voice analysis creates a higher barrier for attackers, as replicating multiple biological traits simultaneously is considerably more difficult than spoofing a single modality. This fusion also ensures continuity if one sensor fails or is obstructed, thereby enhancing overall system robustness. Such redundancy is particularly valuable in critical infrastructure where uninterrupted access verification is paramount [1].

4 Advocate for privacy-by-design principles during system procurement, development, and deployment phases, ensuring transparency, user consent, and algorithmic accountability [4].

Beyond core security applications, biometric technologies show expanding promise in healthcare monitoring (e.g., continuous patient verification), accessibility enhancements (e.g., hands-free control interfaces for users with motor impairments), and personalised user experiences – provided that ethical guidelines and human-centred design principles govern their implementation.

***Conclusion*.** Biometric authentication represents a significant advancement in digital security infrastructure, delivering enhanced convenience and strong identity assurance when properly configured and responsibly managed. However, its reliability remains context-dependent and not absolute: environmental conditions, sensor quality, algorithmic sophistication, and implementation practices all influence real-world performance.

Maximising benefits while mitigating risks requires a balanced, informed strategy: users must understand core error metrics, scrutinise data protection measures, and avoid treating biometrics as a standalone solution. The principal advantage – eliminating password fatigue and accelerating secure access – must be weighed against potential drawbacks, including environmental sensitivity, spoofing vulnerabilities, and the irreversible nature of biological data exposure.

As a guiding principle, biometric verification should function as a complementary layer within a comprehensive defence-in-depth security framework, not as a replacement for holistic protection protocols. Only through such cautious, ethically grounded adoption can individuals and organisations fully leverage biometric innovation while preserving control over personal information and maintaining long-term digital trust [2][4].

References

1. NIST. Face Recognition Vendor Test (FRVT) – Performance Metrics. [Electronic resource] / National Institute of Standards and Technology., 10.01.2025. – Mode of access: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt – Date of access: 22.02.2026.

2. History of biometric technology. [Electronic resource] / Wikipedia., 15.04.2025. – Mode of access: https://en.wikipedia.org/wiki/Biometrics – Date of access: 22.02.2026.

3. Jain, A. K., Nandakumar, K., & Ross, A. Biometric template security: challenges and solutions. [Electronic resource] / IEEE Computer Society., 2024. – Mode of access: https://www.computer.org/csdl/magazine/co – Date of access: 22.02.2026.

4. European Union Agency for Cybersecurity (ENISA). Biometric authentication: security and privacy considerations. [Electronic resource]., 2024. – Mode of access: https://www.enisa.europa.eu/publications/biometric-authentication – Date of access: 22.02.2026.