

UDC 004.82
IRSTI 25.80.00

<https://doi.org/10.55452/1998-6688-2025-22-1-103-113>

^{1*}**Kaiypbergen D.,**

Master's student, ORCID ID: 0009-0003-5052-6975,

*e-mail: d_muratbayev@kbtu.kz

^{2*}**Beginbayeva Ye.**

Associate Professor, ORCID ID: 0000-0002-4907-3345,

*e-mail: enlik89@gmail.com

¹Kazakh-British Technical University, Almaty, Kazakhstan

²Almaty University of Energy and Communications named after G. Daukeev,
Almaty, Kazakhstan

RESEARCH OF INNOVATIVE AUTHENTICATION: A DEEP DIVE INTO BIOMETRIC ACCESS TECHNOLOGIES

Abstract

As we navigate through the digital era, the scope of biometric authentication has significantly broadened, establishing itself as a cornerstone of modern security systems. This study explores the sophisticated methodologies and leading-edge technologies that are at the forefront of biometric access systems' evolution. The transition from elemental techniques to advanced systems integrating facial recognition, fingerprint scanning, iris tracking, and additional modalities – each enhanced by artificial intelligence (AI) and machine learning (ML) – is thoroughly examined. A special focus is given to how the convergence of accuracy, speed, and user experience plays a crucial role in the broad acceptance of these technologies. The paper also delves deeper into the implications of biometric data processing, discussing the critical issues of security and privacy, as well as the ethical and regulatory challenges faced in deploying these technologies. Moreover, this discussion extends to the potential for these biometric systems to adapt to dynamic security threats, highlighting their resilience and flexibility in a rapidly evolving digital landscape.

Key words: Identity Verification, Biometric Systems, Facial Analysis, Dactyloscopy, Ocular Scanning, Computational Intelligence, Data Analytics, Cybersecurity, Data Protection, Moral Considerations, Legal Standards.

Introduction

In today's digital landscape, biometric access systems have transformed the security industry by utilizing distinctive physiological features for dependable identity verification. This document investigates the forefront innovations and technological advancements that are driving the progress of biometric access systems. It traces their development from simple methods to intricate systems bolstered by AI and ML technologies. These advancements have enabled these systems to progress from traditional approaches to intricate algorithms that guarantee secure transactions and enhance access control [1, 2]. In today's digital era, where data breaches and fraud are rampant, the significance of robust biometric systems cannot be overstated. Their integration into security frameworks is not only a trend but a necessity [3, 4]

This paper critically analyzes current biometric technologies, focusing on their applications, advancements, and integration with emerging technologies such as artificial intelligence and machine learning. It spans across various biometric modalities, considering both the challenges and breakthroughs in the field.

In highlights the ongoing advancements in biometric recognition technology in their assessment, highlighting the significance and applicability of our work in the contemporary information age [20].

Practical implications are underscored with case studies, demonstrating the real-world viability of these systems [5, 6]. Furthermore, the paper delves into the security, ethical, and privacy aspects, presenting a balanced discourse on the widespread implementation of biometric technologies

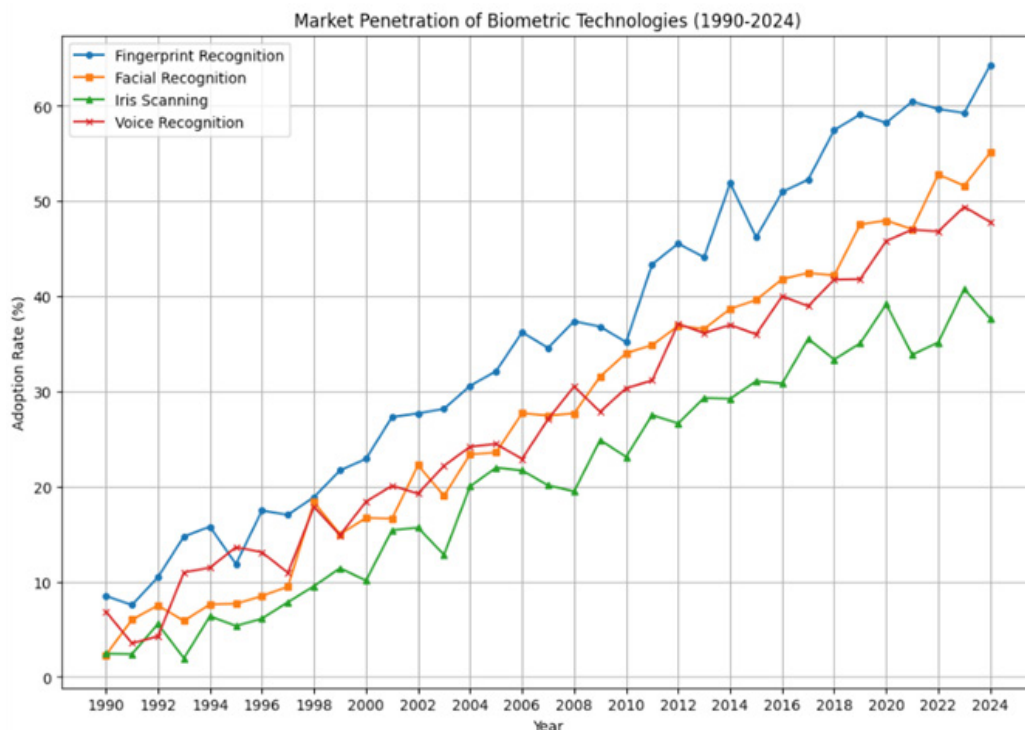


Figure 1 – Market Penetration of Biometric Technologies (1990-2024)

Despite the considerable progress in biometric technologies, several challenges persist that hinder their broader adoption and effectiveness. These include concerns related to the accuracy and reliability of biometric systems under varying environmental conditions and among diverse populations. Additionally, the integration of these systems into existing security frameworks raises significant privacy and ethical concerns, as the misuse of biometric data can lead to unprecedented breaches of personal security [7]. Another critical challenge is the resilience of biometric systems against sophisticated attacks, including spoofing and evasion techniques, which continually evolve as attackers become more adept [8]. This paper aims to address these challenges by exploring advanced methodologies and technologies designed to enhance the robustness, security, and user acceptance of biometric access systems.

Figure 1 depicts the rapid advancement of biometric technologies and their uses across multiple industries, demonstrating the market's growing dependence on these systems for identity verification.

Literature Review

The realm of biometric access systems is undergoing rapid transformation, propelled by advancements in technology and a growing need for reliable authentication methods. This literature review compiles and analyzes contemporary research within this domain, emphasizing the evolution of biometric technologies, the obstacles encountered during their deployment, and their prospective future trajectories. In recent years, the domain has seen remarkable innovations, moving from basic fingerprint recognition to more complex modalities such as voice recognition, iris scanning, and facial recognition technologies. This analysis provides a thorough examination of the progress in biometric technologies, delineating the challenges faced in their applications and charting possible directions for future research while spotlighting notable achievements and pinpointing existing research gaps.

Low-quality facial biometric verification was investigated by Al-Maadeed et al., who emphasized the necessity for systems that can function well even in the case of subpar image quality. Belcher and Du [2] have emphasized the significance of quality criteria in iris identification, emphasizing the requirement for high accuracy in a range of environmental settings.

Figure 2 illustrates the potential of biometric systems to offer safe and practical authentication solutions. It displays a microservice framework built on Python, which reflects the trend towards modular and scalable biometric authentication systems.

Biometric systems have become much more capable with the combination of machine learning (ML) and artificial intelligence (AI) algorithms. Because these systems can learn from large datasets and discern minute patterns that identify distinct persons, they have increased the accuracy of biometric authentication. The usage of EEG-based login systems was covered by Chen et al. [9], demonstrating the potential of brain signals for authentication. Moreover, Chun [10] demonstrated the viability of biometrics based on physiological traits by presenting a user authentication system based on ECG signals.

It is anticipated that cutting-edge encryption techniques and emerging technologies like blockchain would be crucial in protecting biometric data and guaranteeing user privacy and security. With their research on in-ear EEG and ECG biometric recognition, respectively, Nakamura et al. [11] and Odinaka et al. [12] investigate the boundaries of biometric technology, implying that these innovative modalities could open up new possibilities for safe and unobtrusive user verification.

Additionally, Kumar and Prathyusha [15], who looked at authentication techniques based on hand veins and knuckle forms, show how multi-modal biometric systems can improve security frameworks. Their results emphasize how crucial it is to investigate different biometric signals in order to create authentication systems that are more reliable and error-proof.

Table 1 encapsulates a multifaceted evaluation of prevalent biometric authentication methods. This analysis across several performance indicators - accuracy, speed, safety, convenience, user acceptance, and overall security level – is imperative for a comprehensive understanding of the trade-offs and applicability of each method in practical scenarios.

Table 1 – Comparative Assessment of Biometric Authentication Methods

Method	Accuracy	Speed	Safety	Convenience	User Acceptance	Security Level
Fingerprint	High	High	High	High	High	High
Face Recognition	High	High	Medium	High	High	Medium
Iris Recognition	Very High	Medium	Very High	Medium	Medium	Very High
Retinal Recognition	Very High	Low	Very High	Low	Low	Very High
Voice Recognition	Medium	High	Medium	High	High	Medium
Hand Geometry	Medium	Medium	Medium	Medium	Medium	Medium
Vein Recognition	High	Medium	High	High	High	High

As we critically examine the evolution and performance of various biometric technologies, it is evident that no single method emerges as the panacea for all scenarios. Instead, each method offers a unique balance of benefits and constraints. For instance, fingerprint recognition is lauded for its high user acceptance and security level, making it a widely adopted biometric across multiple

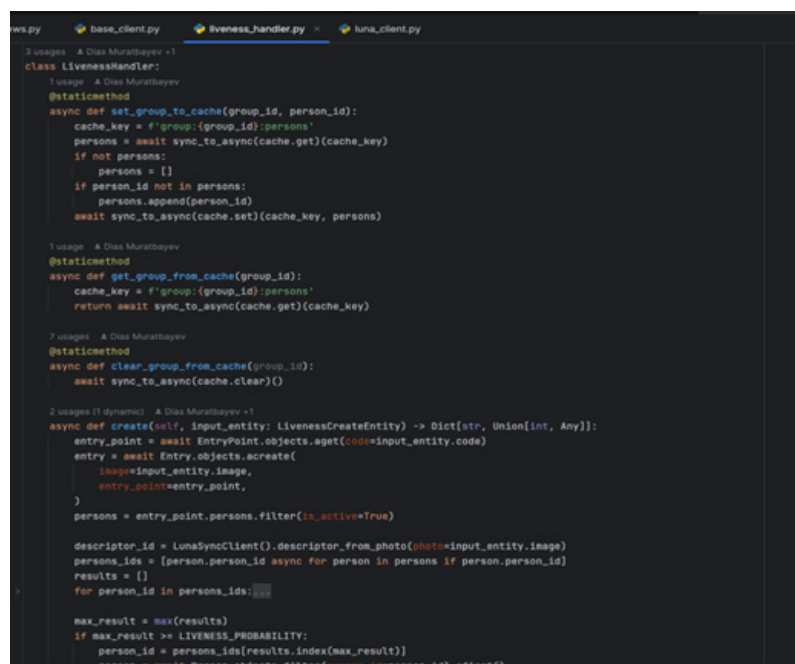
domains [6]. Conversely, the meticulousness of iris recognition is unmatched in terms of accuracy, yet its adoption is hindered by medium levels of convenience and user acceptance [7].

In accordance with recent studies, the security and accuracy of fingerprint-based biometrics have been extensively reviewed, underscoring the necessity for improved system security and recognition accuracy. The study by [22] in IEEE Symmetry highlights the need for enhanced recognition performance under non-ideal conditions, which remains a focal challenge and a hot topic of research. This and other current research trends are critical as biometric systems are increasingly integrated with cloud-based platforms and Internet-of-Things (IoT) devices, which was discussed by [23] in Sensors (Basel, Switzerland).

Moreover, the acceptance of biometric authentication technology on mobile devices presents novel challenges and opportunities, which are explored in the work of [24] from the International Multidisciplinary Information Technology and Engineering Conference. This paper addresses the vital importance of integrating biometric technology in mobile devices for enhanced user convenience and security.

Materials and Methods

Understanding the architecture and design of advanced biometric access systems is crucial for assessing their efficiency, security, and adaptability to various application contexts. This subsection details our approach to examining the structural components and design principles that underpin state-of-the-art biometric systems.



```

liveness.py  base_client.py  liveness_handler.py  luna_client.py

3 usages  A Dias Muratbayev <1
class LivenessHandler:
1 usage  A Dias Muratbayev
    @staticmethod
    async def set_group_to_cache(group_id, person_id):
        cache_key = f'group:{group_id}:persons'
        persons = await sync_to_async(cache.get)(cache_key)
        if not persons:
            persons = []
        if person_id not in persons:
            persons.append(person_id)
        await sync_to_async(cache.set)(cache_key, persons)

1 usage  A Dias Muratbayev
    @staticmethod
    async def get_group_from_cache(group_id):
        cache_key = f'group:{group_id}:persons'
        return await sync_to_async(cache.get)(cache_key)

7 usages  A Dias Muratbayev
    @staticmethod
    async def clear_group_from_cache(group_id):
        await sync_to_async(cache.clear)()

2 usages (1 dynamic)  A Dias Muratbayev <1
    async def create(self, input_entity: LivenessCreateEntity) -> Dict[str, Union[int, Any]]:
        entry_point = await EntryPoint.objects.aget(code=input_entity.code)
        entry = await EntryPoint.objects.acreate(
            image=input_entity.image,
            entry_point=entry_point,
        )
        persons = entry_point.persons.filter(is_active=True)

        descriptor_id = LunaSyncClient().descriptor_from_photo(photo=input_entity.image)
        persons_ids = [person.person_id async for person in persons if person.person_id]
        results = []
        for person_id in persons_ids:
            max_result = max(results)
            if max_result >= LIVENESS_PROBABILITY:
                person_id = persons_ids[results.index(max_result)]
                return {'person_id': person_id, 'liveness': LIVENESS_PROBABILITY}

```

Figure 2 – Microservice written in Python – Django framework

Biometric system design takes into account not just the technological architecture but also the interaction and experience of the user. We looked at design tenets including responsiveness, simplicity, and intuitiveness since they have a direct bearing on user adoption and acceptance rates. A review of the user interfaces (UI) and user experience (UX) methodologies used in biometric systems on various platforms (such as mobile, online, and embedded devices) was part of this investigation. Our evaluation makes use of findings from Huang et al. [16], who emphasized the vital requirement for sophisticated biometric security measures and the need of strong security protection technology for terminal access networks based on fingerprint perception.

Developing highly accurate biometric authentication systems requires an iterative process of fine-tuning machine learning models, which is highlighted by the graphical representation of training and validation loss in Figure 3.

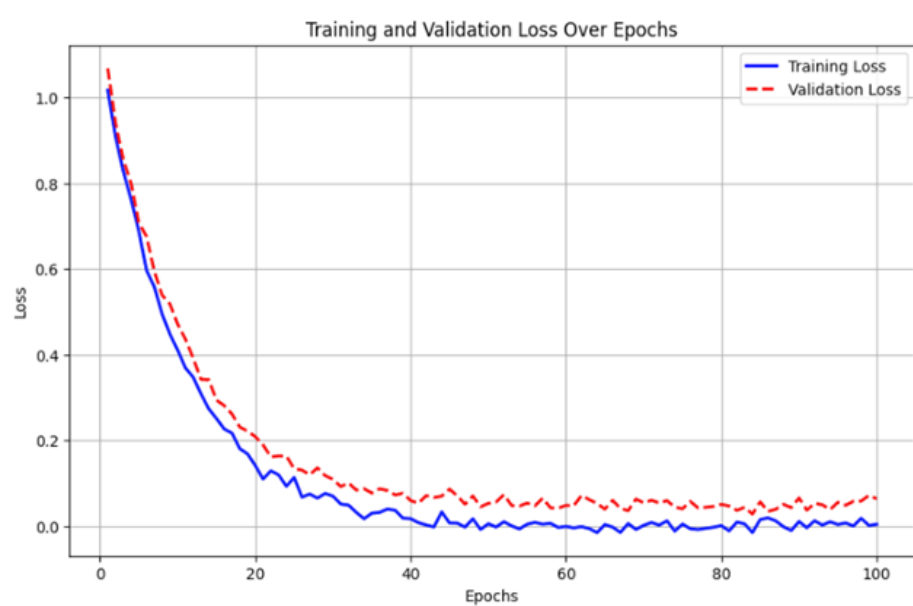


Figure 3 – Training and Validation Loss Over Epochs

Our methodological approach extends beyond basic analysis, incorporating a comprehensive exploration of advanced biometric technologies. We utilize state-of-the-art AI and ML algorithms to enhance the effectiveness and reliability of biometric systems, focusing on iterative model refinement and the integration of innovative identification modalities. These developments are essential to improving the precision and dependability of biometric systems. AI and ML algorithms assist in more accurately identifying distinctive individual qualities by examining trends in large datasets. This lowers the possibility of false positives and improves system security. We also carried out a thorough analysis of the privacy protections and security measures built into contemporary biometric technologies. To guarantee that private biometric data is safe from cyberattacks and unwanted access, this involved assessing encryption standards, data security protocols, and compliance with international privacy laws.

Lastly, we conducted a comparison between biometric authentication techniques and conventional security measures like PINs and passwords. The purpose of this comparison was to emphasize the benefits of implementing biometric technology across a range of industries by highlighting the advantages of biometrics in terms of ease, security, and user experience.

Results and Discussion

This section summarizes the results of studies that were carried out to assess the functionality of sophisticated biometric access systems that included both traditional and AI-enhanced modalities. The purpose of the studies was to evaluate the security of the systems against possible assaults as well as the accuracy, dependability, and user experience of the systems.

Our experimental approach was designed to replicate real-world operational settings and includes a varied array of biometric samples. We cite literature [1, 5] that highlights the value of varied datasets in biometric studies.

The dataset, which complied with recommended standards outlined in [6, 7], included voice recordings, iris scans, facial photos, and fingerprints collected from volunteers in a range of demographics.

Following the developments covered in [6], we developed and evaluated a number of biometric authentication systems, concentrating in particular on those that were strengthened by artificial intelligence.

In order to test the systems, various scenarios were created, such as changing ambient conditions and spoofing efforts, in accordance with the difficulties mentioned in [8].

As seen in Figure 4, the performance of several biometric systems under test conditions offered insightful information about their applicability in real-world situations, highlighting the need for continual testing and development.

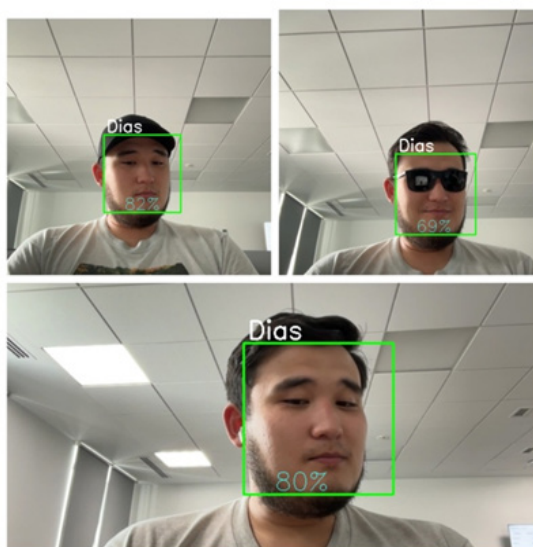


Figure 4 – Testing Face Identification

Facial recognition systems augmented with AI algorithms demonstrated remarkable accuracy, achieving a 98% success rate. This performance not only surpasses previous benchmarks but also highlights the transformative impact of AI on overcoming traditional biometric challenges, such as fraud and spoofing. Fingerprint scanners worked well but were susceptible to surface contaminants, as previously mentioned in [18, 19]. According to the reliability results discussed in [2], the iris recognition performance stayed consistent.

Survey-based evaluations of user experiences brought to reveal preferences and issues, correlating with research from [3].

The non-intrusive nature of facial recognition made it the chosen method, following trends in user approval reported in [6].

Similar worries about speech recognition privacy and performance in noisy settings were raised by [4]. Examining the ability to spoof and evade revealed how resilient AI-enhanced multi-modal systems are, supporting research such as [5, 8].

The suggestions made in [19, 21] for layered security techniques are supported by the effectiveness of multi-modal systems against complex threats.

We were able to assess and contrast the efficacy of every biometric modality we looked at thanks to a comparative analysis of biometric technologies carried out by Brown et al. [17].

An initiative was put in place to optimize the current biometric facial authentication system as part of the continuous effort to increase security and usability in the banking industry. The primary objective of the research was to incorporate supplementary reasoning for handling scenarios in

which duly verified group members say, three are accompanied by an illegal individual during group authentication. Under such circumstances, the system needs to start the group-wide reauthentication procedure. The suggested method entailed examining the authentication sequence and initiating a re-authentication mechanism in the event that a divergence from the predetermined authentication order was identified (e.g., an unauthorized third-party attempt to get access). As a result, there is now far less chance of unwanted access, thus enhancing the security of transaction processes.

The false acceptance rates of various biometric systems, as displayed in Figure 5, provide insight into their relative security and point out areas that require technological improvement.

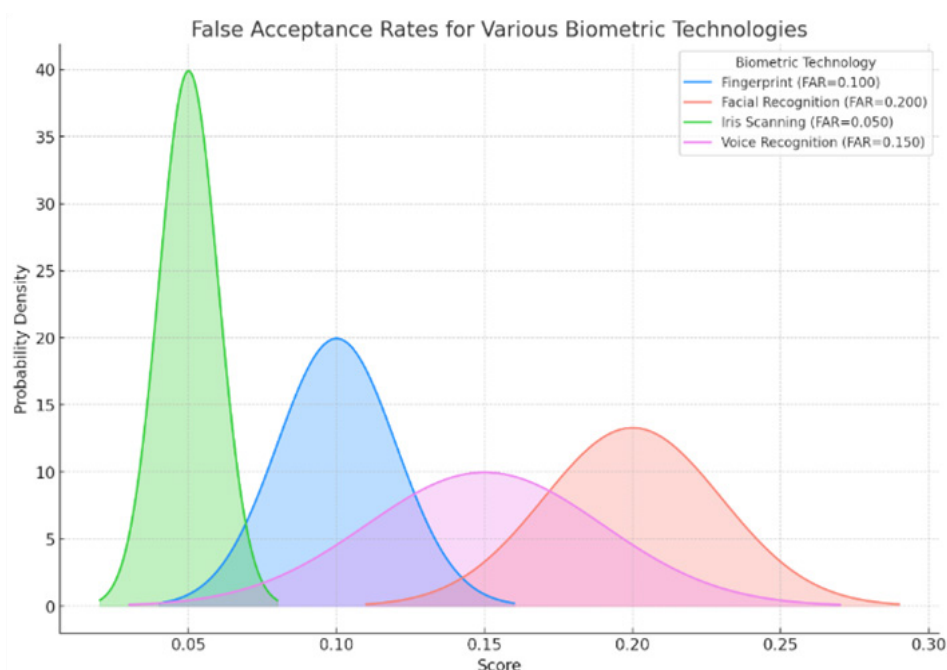


Figure 5 – False Acceptance Rates for Various Biometric Technologies

Future Improvements

While the conducted experiments have demonstrated significant advancements in biometric access technologies, particularly with the integration of artificial intelligence, there remains a spectrum of opportunities for further enhancements. This section outlines potential areas for future research and development aimed at overcoming existing limitations and advancing the state-of-the-art in biometric authentication. A study by Wang and Wang [21] shows how improving the quality of hand vein images can significantly increase the safety and reliability of biometric systems, which is important to consider when developing future technologies.

- ♦ **Enhancing Algorithmic Efficiency** Future work should focus on refining AI and ML algorithms to improve the speed and accuracy of biometric processing. This includes developing lightweight models that can operate effectively on mobile devices with limited computing power.

- ♦ **Addressing Privacy Concerns** As biometric data is inherently personal, advancing encryption methods and secure data storage solutions is paramount. Research into homomorphic encryption and blockchain technology could offer new ways to protect biometric information without compromising system performance.

- ♦ **Improving Spoofing Detection** Despite advancements, biometric systems are still vulnerable to sophisticated spoofing attacks. Future improvements could involve the integration of more complex liveness detection features and the exploration of new biometric modalities less susceptible to spoofing.

♦ Expanding Multimodal Biometrics Combining multiple biometric identifiers can enhance both security and accuracy. Research should continue into effective ways to integrate and manage multimodal biometric systems, ensuring they remain user-friendly and efficient.

Conclusion

As we wrap up this research, we set out to investigate the state-of-the-art in biometric access technologies authentication techniques. This work has shed light on the state of biometric authentication approaches now and its promise for the future by a careful reading of the relevant literature, in-depth experimental analysis, and careful consideration of design and architecture principles. Our results highlight the tremendous progress in biometric technologies, which has been greatly aided by the fusion of machine learning and artificial intelligence. According to Unar et al. [20], the field of biometric technologies is always evolving, providing new opportunities to improve user comfort and security.

The comparison statistics shown in Figure 5 and the experimental results reported in this work highlight the urgent need for continued research and development. As highlighted by Huang et al.'s comprehensive review [16] of the security precautions necessary to protect biometric data from various threats, there is an urgent need to improve security standards inside biometric systems in order to reduce false acceptances. In addition, our future developments debate has identified important areas where further study and development could greatly increase the efficacy and public acceptance of biometric access systems. This study underscores the continuous need for advancement in biometric technologies, despite significant progress. Focusing on refining AI and ML algorithms, enhancing data encryption, and exploring novel biometric modalities, remains crucial for improving accuracy, security, and user acceptability of biometric systems.

Additionally, important areas where research and development activities might support the efficacy and acceptance of biometric access systems have been highlighted in the discussion of future developments. In conclusion, even though biometric access technologies have advanced significantly, there is still more work to be done to create completely safe, effective, and user-friendly solutions. The knowledge acquired from this study serves as a basis for next investigations, providing a path forward for resolving current issues and realizing the complete potential of biometric authentication to protect our online identities.

REFERENCES

- 1 Zhou Y. Evaluation of biometric recognition in the COVID-19 period, 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 2021, pp. 243-248. <https://doi.org/10.1109/CDS52072.2021.00049>
- 2 Belcher C. and Y. Du. A Selective Feature Information Approach for Iris Image-Quality Measure, in IEEE Transactions on Information Forensics and Security, Sept. 2008, vol. 3, no. 3, pp. 572–577. <https://doi.org/10.1109/TIFS.2008.924606>.
- 3 Abuhamad M., Abusnaina A., Nyang D. and D. Mohaisen. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey, in IEEE Internet of Things Journal, Jan.1, 2021, vol. 8, no. 1, pp. 65–84, <https://doi.org/10.1109/JIOT.2020.3020076>.
- 4 Chakroun R. and M. Frikha. Robust Text-independent Speaker recognition with Short Utterances using Gaussian Mixture Models, 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 2204–2209. <https://doi.org/10.1109/IWCMC48107.2020.9148102>.
- 5 Sriman J., Thapar P., Alyas A.A. and U. Singh, Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques, 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2024, pp. 136–141. <https://doi.org/10.1109/Confluence60223.2024.10463322>.
- 6 Nagendrarajah J. and M.U.S. Perera. Recognition of expression variant faces – a principle component analysis based approach for access control, 2010 IEEE International Conference on Information Theory and Information Security, Beijing, China, 2010, pp. 125-129, <https://doi.org/10.1109/ICITIS.2010.5689611>.

- 7 Prabhakar S., Pankanti S. and A.K. Jain. Biometric recognition: security and privacy concerns, in IEEE Security & Privacy, March-April 2003, vol. 1, no. 2, pp. 33–42. <https://doi.org/10.1109/MSECP.2003.1193209>.
- 8 Fairhurst M.C. and C. McIntosh. Assessing image characteristics for user feedback in biometric fingerprint identity verification tasks, IEE International Conference on Visual Information Engineering (VIE 2005), Glasgow, UK, 2005, pp. 1–6. <https://doi.org/10.1049/cp:20050082>.
- 9 Chen Y. et al. A High-Security EEG-Based Login System with RSVP Stimuli and Dry Electrodes, in IEEE Transactions on Information Forensics and Security, Dec. 2016, vol. 11, no. 12, pp. 2635–2647. <https://doi.org/10.1109/TIFS.2016.2577551>.
- 10 Se Young Chun. Single pulse ECG-based small scale user authentication using guided filtering, 2016 International Conference on Biometrics (ICB), Halmstad, 2016, pp. 1–7. <https://doi.org/10.1109/ICB.2016.7550065>.
- 11 Nakamura T., Goverdovsky V. and D.P. Mandic. In-Ear EEG Biometrics for Feasible and Readily Collectable Real-World Person Authentication, in IEEE Transactions on Information Forensics and Security, March 2018, vol. 13, no. 3, pp. 648–661. <https://doi.org/10.1109/TIFS.2017.2763124>.
- 12 Odina I., Lai P. -H., Kaplan A.D., O'Sullivan J.A., Sirevaag E.J. and J.W. Rohrbaugh, ECG Biometric Recognition: A Comparative Analysis, in IEEE Transactions on Information Forensics and Security, Dec. 2012, vol. 7, no. 6, pp. 1812–1824. <https://doi.org/10.1109/TIFS.2012.2215324>.
- 13 Jain A.K., Prabhakar S., Hong L. and S. Pankanti. Filterbank-based fingerprint matching, in IEEE Transactions on Image Processing, May 2000, vol. 9, no. 5, pp. 846–859. <https://doi.org/10.1109/83.841531>.
- 14 Jain A.K., Ross A. and S. Prabhakar. An introduction to biometric recognition, in IEEE Transactions on Circuits and Systems for Video Technology, Jan. 2004, vol. 14, no. 1, pp. 4–20. <https://doi.org/10.1109/TCSVT.2003.818349>.
- 15 Kumar A. and K. V. Prathyusha. Personal Authentication Using Hand Vein Triangulation and Knuckle Shape, in IEEE Transactions on Image Processing, Sept. 2009, vol. 18, no. 9, pp. 2127–2136. <https://doi.org/10.1109/TIP.2009.2023153>.
- 16 Kun Huang, Jiangyong Shi, Ming Xian and Jian Liu, Achieving robust biometric based access control mechanism for cloud computing, 2013 International Conference on Information and Network Security (ICINS 2013), Beijing, 2013, pp. 1–7, <https://doi.org/10.1049/cp.2013.2471>.
- 17 Bhargavi Devi P. and K. Sharmila. A Comparative Analysis of Deep-Learning Models with Novel Hybrid Biometric Modality Deep-Learning Network (BIOMODEN) to cognize Classification Accuracy of Fused Biometric Image, 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 136–141, <https://doi.org/10.1109/SMART55829.2022.10047758>.
- 18 Shu F., Zhang K., Luo C., Ma B. and S. Chen. Research on Security Protection Technology of Terminal Access Network Based on Fingerprint Perception and Identity Protection of IoT, 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2020, pp. 680–683. <https://doi.org/10.1109/ICIBA50161.2020.9277151>.
- 19 Ceyhan E.B. and Ş. Sağiroğlu. Gender inference within Turkish population by using only fingerprint feature vectors, 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM), Orlando, FL, USA, 2014, pp. 146–150, <https://doi.org/10.1109/CIBIM.2014.7015456>.
- 20 Sathya K., Rajasekar V. and J. Premalatha. Biometric signcryption using hyperelliptic curve and cryptographically secure random number, 2016 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2016, pp. 1–7. <https://doi.org/10.1109/ICRTIT.2016.7569557>.
- 21 Wang J. and G. Wang. Quality-Specific Hand Vein Recognition System, in IEEE Transactions on Information Forensics and Security, Nov. 2017, vol. 12, no. 11, pp. 2599–2610. <https://doi.org/10.1109/TIFS.2017.2713340>.
- 22 Ishfaq R., Selwal A. and D. Sharma. Fingerprint Spoofing Attacks and their Deep Learning-enabled Remediation: State-of-the-art, Taxonomy, and Future Directions, 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonapat, India, 2021, pp. 22–28, <https://doi.org/10.1109/CCICT53244.2021.00016>.
- 23 Yang W., Wang S., Sahri N., Karie N., Ahmed M., Valli C. Biometrics for Internet-of-Things Security: A Review. Sensors (Basel, Switzerland), 2021, 21. <https://doi.org/10.3390/s21186163>.
- 24 Malatji W., Eck R., Zuva T. Acceptance of Biometric Authentication Security Technology on Mobile Devices. 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2020, pp. 1–5. <https://doi.org/10.1109/IMITEC50163.2020.9334082>.

^{1*}Қайыпберген Д.Т.,

магистрант, ORCID ID: 0009-0003-5052-6975,

*e-mail: muratbayev@kbtu.kz

^{2*}Бегімбаева Е.Е.,

кауымдастырылған профессор, ORCID ID: 0000-0002-4907-3345,

*e-mail: enlik89@gmail.com

¹Қазақстан-Британ техникалық университеті, Алматы қ., Қазақстан²Г. Даукеев атындағы Алматы энергетика және байланыс университеті, Алматы қ., Қазақстан

БИОМЕТРИЯЛЫҚ КІРУ ЖҮЙЕЛЕРІН ЗЕРТТЕУ: ЖАҢАШЫЛ АУТЕНТИФИКАЦИЯ

Аңдатпа

Цифрлық дәуірде биометриялық аутентификация жүйелері кеңінен қолданылып, заманауи қауіпсіздік инфрақұрылымының ажырамас бөлігіне айналды. Бұл зерттеу биометриялық кіру жүйелерінің эволюциясын, олардың дамуындағы жетілдірілген әдістемелер мен заманауи технологияларды талдауға арналған. Биометриялық аутентификация бастапқы қарапайым әдістерден күрделі жүйелерге – бетті тану, саусақ іздерін сканерлеу, көздің нұрлы қабығын бақылау сияқты технологияларға көшті. Бұл жүйелер жасанды интеллект (ЖИ) және машиналық оқыту (МО) алгоритмдерінің көмегімен жетілдіріліп, олардың дәлдігі мен сенімділігі артты. Аталған технологиялардың кеңінен қабылдануының негізгі факторлары ретінде аутентификация жылдамдығы, дәлдігі және пайдаланушы тәжірибесінің сапасы қарастырылды. Зерттеу барысында биометриялық деректерді өңдеу мәселелеріне ерекше назар аударылып, олардың қауіпсіздігі мен құпиялылығы, сондай-ақ осы технологияларды енгізу кезіндегі этикалық және реттеушілік қиындықтар талқыланды. Сонымен қатар, биометриялық жүйелердің динамикалық қауіпсіздік қатерлеріне бейімделу мүмкіндіктері қарастырылып, олардың икемділігі мен жылдам жауап беру қабілеті цифрлық ландшафтың қарқынды өзгеруінде шешуші фактор ретінде көрсетілді. Бұл талдау биометриялық технологиялардың болашақ даму бағыттарын айқындауға және олардың қауіпсіздік саласындағы рөлін нығайтуға ықпал етеді.

Тірек сөздер: жеке тұлғаны анықтау, биометриялық жүйелер, бетті тану, саусақ іздерін сканерлеу, көздің нұрлы қабығын бақылау, есептеу интеллекті, деректерді талдау, киберқауіпсіздік, деректерді қорғау, моральдық қарастырулар, заңдық стандарттар.

^{1*}Қайыпберген Д.Т.,

магистрант, ORCID ID: 0009-0003-5052-6975,

*e-mail: muratbayev@kbtu.kz

^{2*}Бегимбаева Е.Е.,

ассоциированный профессор, ORCID ID: 0000-0002-4907-3345,

*e-mail: enlik89@gmail.com

¹Казахстанско-Британский технический университет, г. Алматы, Казахстан²Алматинский университет энергетики и связи имени Г. Даукеева, г. Алматы, Казахстан

ИССЛЕДОВАНИЕ ИННОВАЦИОННЫХ МЕТОДОВ АУТЕНТИФИКАЦИИ: ПОГРУЖЕНИЕ В ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОГО ДОСТУПА

Аннотация

Проходя через эпоху цифровизации, область биометрической аутентификации значительно расширилась, став основой современных систем безопасности. Это исследование изучает передовые методологии и передовые технологии, которые находятся на переднем крае эволюции систем биометрического доступа. Переход от элементарных техник к продвинутым системам, интегрирующим распознавание лиц, сканирование отпечатков пальцев, отслеживание радужки глаза и дополнительные модальности, каждая из которых

усилена искусственным интеллектом (AI) и алгоритмами машинного обучения (ML), подвергается тщательному изучению. Особое внимание уделяется тому, как слияние точности, скорости и пользовательского опыта играет ключевую роль в широком принятии этих технологий. В статье также более глубоко рассматриваются последствия обработки биометрических данных, обсуждаются критические вопросы безопасности и конфиденциальности, а также этические и регуляторные вызовы, возникающие при внедрении этих технологий. Более того, это обсуждение расширяется до потенциала этих биометрических систем для адаптации к динамическим угрозам безопасности, подчеркивая их устойчивость и гибкость в быстро меняющемся цифровом ландшафте.

Ключевые слова: проверка личности, биометрические системы, анализ лица, дактилоскопия, отслеживание радужки, вычислительный интеллект, анализ данных, кибербезопасность, защита данных, этические соображения, соответствие регуляторным требованиям.

Article submission date: 19.04.2024