ETHIOPIAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 06, June-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

PROSPECTS FOR THE DEVELOPMENT OF BIOMETRIC TECHNOLOGIES

Radjabov Sobirjon Sattorovich
DSc, Head of the Laboratory,
Institute of Fundamental and Applied Research
at the National Research University
"Tashkent Institute of Irrigation and Agricultural
Mechanization Engineers
Abdullaeva Barno Mo'ydinjon kizi
Junior Research Fellow,Namangan state university

Introduction. In recent years, biometric technologies have been rapidly advancing, which is explained by the expansion of their application areas. The reason for this is that human biometric characteristics are convenient, unique, and nearly impossible to forge, forget, lose, or transfer to someone else. According to data from Mordor Intelligence, an international consulting company, by the end of 2024, the global market size for biometric systems is expected to reach 51.15billionUSD.

With the growing demand for these technologies, the requirements for the accuracy (and in some cases, the speed) of identification are also increasing. From this perspective, in our opinion, the most promising directions for the development of biometric technologies are as follows:

Implementation of new biometric technologies;

Development and improvement of identification methods and algorithms;

Integration of multiple biometric technologies (multibiometrics).

These directions aim to enhance the reliability, efficiency, and versatility of biometric systems, addressing the increasing demands for secure and accurate identification solutions.

1. Implementation of New Biometric Technologies.

For several decades, the capabilities of biometric technologies were limited, with fingerprint-based technology being the most popular and widely used. However, in the last decade, advancements in computing and sensor technologies have significantly expanded the use of other biometric parameters such as gait, gestures, ear shape, scent, and more.

One example of this expansion is the use of gait for identification [1]. In video recordings, a person's face is often obscured or difficult to see due to factors such as insufficient lighting, headwear, masks, makeup, and other elements. In such cases, gait can be used for identification. Research shows that gait is a unique parameter that is difficult to forge and can be compared in reliability to fingerprint or iris scanning. Unlike traditional biometric parameters, gait can be observed from a distance and without direct contact. However, several factors can alter the visual appearance of gait, such as high heels, uncomfortable footwear, carrying heavy objects, clothing that conceals body parts or restricts movement, and walking speed.

Additionally, factors like camera angle, lighting, and camera parameters can affect the accuracy of identification. Thus, gait-based identification remains a unique and complex challenge. Despite advancements in modern computer vision methods, the quality and reliability of this method are still lower compared to facial recognition.

One of the latest achievements in the field of biometrics is the technology of creating and analyzing thermograms [2]. Scientists have discovered that using infrared cameras, it is possible to capture unique images of objects located beneath the skin's surface. The varying density of bones, fat tissues, and blood vessels is strictly individual, forming a thermographic image of the user's face. A facial thermogram is unique, enabling reliable differentiation even between identical twins.

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 06, June-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

Additional advantages of this approach include its resistance to any cosmetic changes, such as plastic surgery or makeup, and the confidentiality of the registration process.

Keyboard Dynamics or Keystroke Biometrics. Keyboard dynamics, also known as keystroke biometrics, analyzes the way a user types specific phrases or patterns [3]. There are two main types of keystroke recognition:

Authentication for Access; Used to authenticate users when accessing computational resources.

Activity Monitoring; Used to monitor user activity after access is granted. If another person is detected using the system, it can be automatically locked.

Research has shown that typing rhythm is an individual characteristic of a user, making it suitable for identification and authentication. The rhythm is measured by evaluating the time intervals between keystrokes and the duration of key presses. While the second method is considered more effective, the best results are achieved by combining both approaches. A unique advantage of this method is its cost-effectiveness, as it requires no additional hardware beyond a keyboard. However, this technology is still in development, and its reliability is difficult to assess, especially given the high demands placed on security systems.

Ear Shape Analysis. Ear shape analysis is one of the newest approaches in biometric identification (Figure 1) [3].

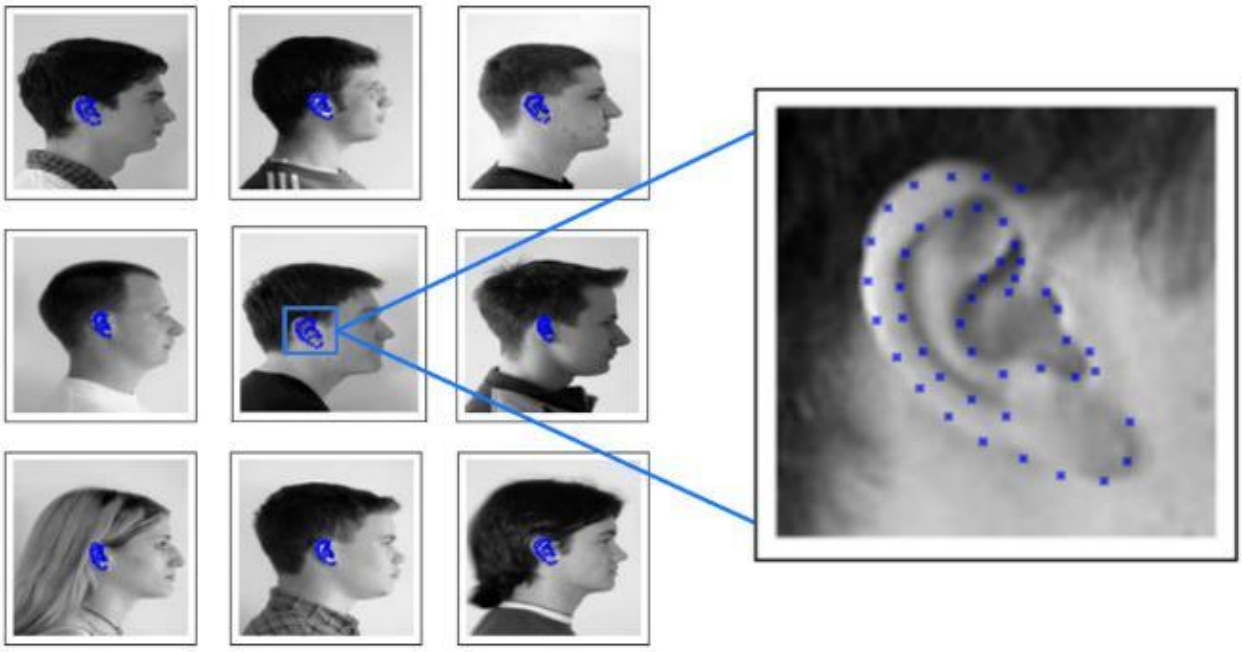

Figure-1.Ear shape analysis

Even an inexpensive webcam can provide reliable samples for comparison and identification. However, factors such as hair and accessories can reduce the system's efficiency. Additionally, external lighting and the position of the face relative to the camera can also affect the results.

Summary:

Keyboard Dynamics;

A cost-effective biometric method that analyzes typing patterns for identification and authentication. It is still under development and faces challenges in meeting high security standards.

Ear Shape Analysis; A novel biometric approach that uses ear shape for identification. While simple and cost-effective, it can be affected by external factors like hair, accessories, lighting, and camera angles.

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 06, June-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

Both methods represent innovative directions in biometric technology, but further research and development are needed to enhance their reliability and applicability in real-world scenarios.

2. Development and Improvement of Identification Methods and Algorithms.

In recent years, deep learning methods based on training neural networks have demonstrated the most effective results in solving problems related to biometric identification. Neural networks can extract highly abstract features, which are crucial for accurate recognition. This enables high performance in tasks such as video and image classification, image segmentation, object detection, visual tracking, and more.

However, despite the achievements of deep learning, in certain tasks such as gait recognition, shallow models still outperform neural networks for some specific datasets. At the same time, none of the existing approaches have yet achieved acceptable accuracy in all scenarios.

Recently, researchers at MIT introduced a new neural network architecture called Kolmogorov-Arnold Networks (KAN) [4], which serves as an alternative to multi-layer neural networks (MLPs). This architecture shifts activations to the "edges" of the network, distinguishing it from traditional neural network approaches.

According to the developers, this new type of neural network offers several advantages. Unlike MLPs, KAN can process new information without forgetting old data, allowing the model to remain relevant without the need for frequent retraining. Additionally, KAN stands out for its high accuracy and interpretability, surpassing MLPs in these aspects. This innovative architecture not only performs slightly better but also provides entirely new opportunities for solving complex dynamic problems.

KAN offers faster scaling capabilities for neurons compared to MLPs. However, there are some challenges—training KAN requires significant computational power and/or more time. Nevertheless, this is not an insurmountable obstacle, as traditional MLPs have also been continuously optimized and improved throughout their application history.

Thus, KAN represents a promising direction in the development of neural network technologies. This approach has the potential to significantly enhance the efficiency of solving complex tasks in the field of artificial intelligence, particularly in biometric identification.

Key Points:

Deep Learning; Neural networks, especially deep learning models, have shown remarkable success in biometric identification tasks due to their ability to extract abstract features.

Limitations of Deep Learning; In some cases, such as gait recognition, shallow models still outperform deep neural networks.

Kolmogorov-Arnold Networks (KAN): A novel neural network architecture introduced by MIT researchers, offering advantages such as better interpretability, high accuracy, and the ability to retain old data while processing new information.

Challenges: Training KAN requires significant computational resources and time, but these challenges are not insurmountable.

Future Potential; KAN is a promising direction that could revolutionize neural network technologies and improve the efficiency of solving complex tasks, including biometric identification.

This innovative approach could pave the way for more advanced and reliable biometric systems in the future.

Key Aspects of Multibiometric Integration.

eISSN: 2349-5715 pISSN: 2349-5707
Volume: 12, Issue 06, June-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

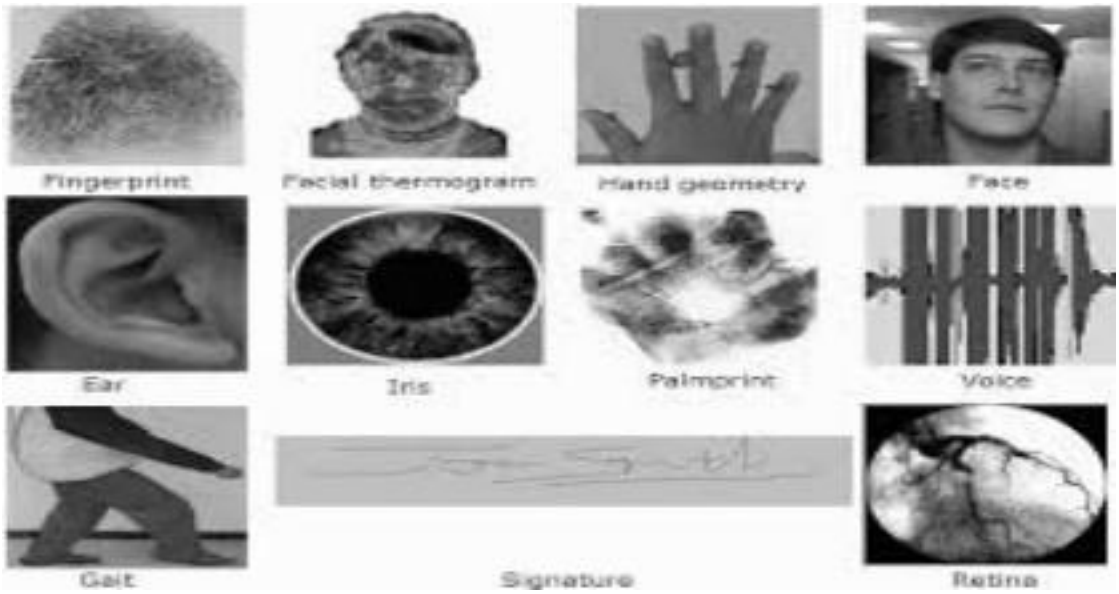

Figure-2. Multibiometric Integration

Sensor-Level Fusion:

Data from multiple biometric sensors (e.g., fingerprint scanner, facial recognition camera, voice recorder) are combined at the raw data level.

This approach leverages the strengths of each sensor to create a more comprehensive dataset.

Feature-Level Fusion. Features extracted from different biometric traits (e.g., fingerprint patterns, facial landmarks, voice frequencies) are combined.

This method enhances the uniqueness of the biometric profile by integrating diverse characteristics.

Decision-Level Fusion. Decisions from individual biometric systems (e.g., fingerprint match, facial match) are combined to make a final identification decision.

This approach ensures higher accuracy by cross-verifying results from multiple sources.

Conclusion. In conclusion, biometric identification is unparalleled in providing accurate, reliable, and irrefutable results for verification processes. In the near future, traditional methods like passwords and PIN codes are expected to be entirely replaced by new, more secure authorization and authentication methods based on biometric data. This shift will not only enhance security but also improve the user experience by making the identification process more convenient and faster. Biometric technologies are already widely used in various sectors, including banking, healthcare, national security, and information technology.

Furthermore, biometric identification is driving the development of new security standards and drawing attention to ethical and privacy concerns. The continuous improvement of technologies and methodologies in this field is helping to create more secure, reliable, and user-friendly identification systems that meet the demands of the modern world and the future.

In summary, biometric identification methods represent a promising direction of development that is expected to fundamentally transform approaches to data protection and security across various aspects of life.

References:

1. Йхапате М., Йхапате А.К. Идентификация человека по походке: Система, основанная на походке. – М.: Sciencia Scripts, 2023. – 64 с.

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 12, Issue 06, June-2025 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

2. Naziyra, Torebaeva. "FOYDALANUVCHILARNI BIOMETRIK IDENTIFIKATSIYALASH VA AUTENTIFIKATSIYALASH." Scientific Impulse 1.10 (2023): 2041-2044.
3. Nath A., Mondal T. Issues and challenges in two factor authentication algorithms //International Journal of Latest Trends in Engineering and Technology (IJLTET). – 2016. – Т. 6. – С. 318-327.
4. Ilgizarovna, Zakirova Rufina. "TWO-FACTOR BIOMETRIC AUTHENTICATION SYSTEM." ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ 46.5 (2024): 150-162.
5. Jiang, Changsong, et al. “Two-factor authenticated key exchange from biometrics with low entropy rates” IEEE Transactions on Information Forensics and Security (2024).
6. Jiang, Mingming, et al. “Biometric-based two-factor authentication scheme under database leakage” Theoretical Computer Science 1000 (2024): 114552.