

Identity Verification Processes with Voice Biometrics and Artificial Intelligence

Zeynep Örpek^{1*}, Büşra Tural² and Samet Özmen³

^{1*} Vakıf Katılım, Research & Development Center, Istanbul, Türkiye (zeynep.orpek@vakifkatilim.com.tr) (ORCID: 0000-0001-7130-9118)

² Vakıf Katılım, Research & Development Center, Istanbul, Türkiye (busra.tural@vakifkatilim.com.tr) (ORCID: 0000-0003-3645-8761)

³ Vakıf Katılım, Research & Development Center, Istanbul Türkiye (samet.ozmen@vakifkatilim.com.tr) (ORCID: 0000-0002-8398-3107)

Abstract – Biometrics refers to the measurable physical and behavioral characteristics of every living creature. These characteristics represent the unique biological characteristics of individuals. The identities of living things can be determined by analyzing various types of biological data such as fingerprints, faces, eyes, voices, and vascular patterns. Identification from biometric features is used in almost every field today. Voice biometrics performs identity verification by analyzing individuals' speech patterns. Today, voice identification is used as an alternative or verification step in many areas. However, with the spread, the protection of personal data and fraud has gained great importance. In particular, ensuring the confidentiality and security of biometric data is of critical importance for the healthy management of personal data and creating a secure environment. In this context, there are laws and standards determined by the regulatory and supervisory boards of the states. With the development of artificial intelligence technology in recent years, a new threat has emerged regarding the forgery of biometric data. Artificial intelligence algorithms could make it possible to forge biometric data, which could lead to increased fraud. Therefore, the development and implementation of security solutions for the security of biometric data has become an important necessity. In this article, studies on biometric features, especially voice biometrics, and their use with artificial intelligence technology will be discussed.

Keywords – Biometrics, Voice Biometrics, Identity Verification Process, Artificial Intelligence, Voice Recognition

Citation: Örpek, Z. et.al., (2024). Identity Verification Processes with Voice Biometrics and Artificial Intelligence. International Journal of Multidisciplinary Studies and Innovative Technologies, 8(1): 1-4.

I. INTRODUCTION

Technological developments have gained great momentum as traditional identity verification methods have been replaced by the use of biometric data. While traditional methods use knowledge-based identity verification systems such as passwords or PINs, biometric data is based on physical or behavioral characteristics of the human body. This biometric data includes physical features such as fingerprints, retina scans, and facial recognition, as well as voice biometrics.

In particular, voice biometrics offers a more reliable and user-friendly alternative to traditional methods in identity verification processes. Voice is one of the most distinctive biometric characteristics of the human body, and a person's speaking style, tone, emphasis, and other vocal characteristics, like other biometric data, constitute a person's unique identity. Each individual's voice has unique and variable characteristics. Voice characteristics such as speaking style, stress, and intonation can be used to identify a person. Voice biometrics builds on these unique characteristics, strengthening the identity verification process and reducing the risk of unauthorized access. Voice biometrics stands out as a method that strengthens identity verification processes based on the unique voice characteristics of each individual.

However, to use voice biometrics effectively, the integration of advanced technologies such as artificial intelligence is required. In addition to voice biometrics, artificial intelligence

further improves identity verification processes by demonstrating a performance that exceeds human ability in voice analysis and recognition. By learning from large data sets, artificial intelligence algorithms can identify complex voice characteristics and distinguish between individuals. Additionally, artificial intelligence-based systems get smarter over time and therefore produce more accurate results.

Artificial intelligence is capable of identifying voice characteristics and distinguishing individuals by learning from large data sets. In addition, artificial intelligence models that improve over time are becoming more effective in detecting and preventing fraud attempts. In this way, voice biometrics and artificial intelligence come together, making identity verification processes more secure and effective.

Voice biometrics and artificial intelligence are transforming identity verification processes in many areas, from financial institutions to the healthcare industry, from cybersecurity to the travel industry. These technologies offer an easier, faster, and more secure way to verify users' identities. However, with the adoption of these innovations, it is necessary to be careful about issues such as data privacy and security. In this article, the role and importance of voice biometrics and artificial intelligence technologies in identity verification processes will be examined in more detail and an in-depth analysis will be presented on the effects of these technologies in the field of security.

Biometric data are unique and measurable characteristics of people that are used to identify and distinguish individuals. Biometrics refers to a set of technologies that create powerful systems using human physiological or behavioral characteristics to meet individuals' secure authentication and access control needs. Through the use of biometric features such as fingerprints, iris patterns, facial features, voice characteristics, and DNA, individuals can be identified reliably and securely; This offers an alternative to traditional authentication methods such as passwords, personal identification numbers (PINs), or smart cards. [1]. Application areas of this technology include various fields such as security systems, forensic science, healthcare, online banking, and customer service. [2]. With the rapid advancement of information and communication technology, the an increasing demand for biometric technologies for various applications. It should also be noted that there are many studies in this field in the literature.

In the literature, biometrics are generally divided into two main categories: physiological biometrics and behavioral biometrics. [3]. The human voice falls into the category of behavioral biometrics and creates a voice that is unique and distinctive to individuals in terms of characteristics such as frequency, loudness, timbre, accent, rhythm, or tone. These vocal characteristics are determined by a combination of vocal components and behavioral patterns and vary for each individual. Thanks to these features, voice can be used as an effective biometric feature in authentication systems. [4].

Glowacki and Piotrowski propose a new architecture for voice authentication, enabling voice authentication using the data hiding technique [5]. A study on users of Google's wearable glasses found that by combining touch behaviors, it could achieve excellent accuracy in user authentication. Similarly, Panda has developed an algorithm that allows voice identity by analyzing voice in various environmental conditions, and such advancements increase the reliability of voice identity. [6].

In the work of Fairhurst, Li, and Da Costa-Abreu, in voice trial integrated online banking systems, a pre-edited voice of information is used for storage on the server and subsequent access. When the customer wants to perform a new transaction, it is checked whether the voice in the system matches and the process continues[7].

With their study, Can and his colleagues emphasize the importance of voice identity systems for the comfort and security of users and reveal the latest developments in the field of voice biometrics by examining single-model and multi-model systems in terms of security. It also provides a comprehensive assessment of the reliability and scope of use of this technology by addressing security attacks against voice identity systems [8].

Artificial intelligence (AI) is a set of highly transformative technologies that are currently revolutionizing various industries. The evolution of identity measures from traditional passwords and cryptographic keys to advanced authentication techniques has provided accessible, secure, and more reliable data protection tools. Therefore, it is clear that there is a growing interest in integrating artificial intelligence into biometrics and IoT to improve the overall security posture and protect data privacy [9].

Jahangir and his colleagues have conducted a comprehensive review and research of detailed descriptions with artificial intelligence techniques, and have shown that

back-learning techniques provide high-level representation with various layers of neural networks to extract distinguishing features from raw speech data and represent features from low-level to high-level pyramids[10]. Different machine classifiers such as decision tree, support vector machine, and Gaussian Mixture Model are combined to separate the features developed from the speaker's utterances into high-level parsing of the speech [11].

In his work, Chandran proposes a conceptual model for implementing an AI voice identity system integrated with blockchain technology, based on a limited and targeted narrative review of the existing literature on blockchain and AI voice identity[12].

Balaji and his colleagues carried out a study that aims to increase security measures and complement user comfort by proposing to move from password-based identity to voice-based identity using voice recognition software and machine learning. As a result, this study predicts that higher security and effectiveness can be achieved with the use of voice-based identity scheme methods compared to traditional password-based identity consistent systems [13].

Jain et al., in their study examining the advances made in the field of biometric recognition over the last 50 years, emphasized that unlocking the full potential of biometric data will not only lead to widespread adoption of this promising technology but also wider user acceptance and societal impact [14].

II. VOICE BIOMETRICS AND THE ROLE OF IN IDENTITY VERIFICATION PROCESSES

Voice biometrics is a biometric technology that provides identity verification or identification using a person's speech pattern. Voice biometrics recognizes a person by analyzing the characteristics of their sound waves. The characteristics of people's sound waves include factors such as frequency, intensity, tone, emphasis, and speaking rate. These characteristics of a person's speech form a unique biometric signature. This unique biometric signature stands out as an effective method for identity verification processes with biometric recognition. These processes generally identify the relevant person by comparing voice recordings in a previously created reference database to determine the identity of the user.

Biometric identification is considered more secure than traditional identity verification methods. Because biological or behavioral characteristics can hardly be copied and imitated. However, some concerns regarding the use of these systems raise controversy, especially around privacy and security issues.

The use of biometric data is limited and protected by official authorities or legal and regulatory institutions. In Turkey, biometric data is designated as special personal data in the KVKK (Personal Data Protection Law) and is protected by this law. Biometric data, which is considered as special personal data by KVKK, has not been comprehensively defined [15]. According to the General Data Protection Regulation (GDPR) of the European Union, biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data." [16].

It is of critical importance to pay attention to the following points for the secure storage and use of biometric data, ensuring the security and confidentiality of individuals' biometric data.

1. **Privacy and Security:** Biometric data is personal and sensitive. Therefore, privacy and security standards must be strictly applied when processing and using this data. The requirements set by official authorities, legal and regulatory institutions must be complied with and action must be taken within this framework.
2. **Approval and Traceability:** During the processing and use of biometric data, the data owner must be informed and consent must be obtained. Data owners must be able to access and track information such as who and when the data is shared.
3. **Accuracy and Success:** The success of the identity verification system developed when authenticating through biometric data is very important. The developed system must verify and prove its success with various metrics.
4. **Data Storage:** Secure storage of biometric data is critical. Rules may be set by official authorities for data retention conditions and these rules must be followed.

III. ARTIFICIAL INTELLIGENCE AND THE ROLE OF IN IDENTITY VERIFICATION PROCESSES

Artificial intelligence plays an increasingly important role in identity verification processes with the development and spread of technology. While identity verification allows people to prove their identity and carry out authorized transactions, artificial intelligence has the potential to make this process more reliable, efficient, and user-friendly. Artificial intelligence can be used in a wide range of areas, from analysis of biometric data to recognition of behavioral features and fraud detection.

Artificial intelligence plays an important role in the analysis of biometric data used in biometric recognition processes. Deep learning algorithms are used to detect and match biometric features such as facial recognition or fingerprint recognition. In this way, the identity verification process becomes faster and more accurate. A commonly used algorithm in facial recognition systems is known as Convolutional Neural Networks (CNN). This algorithm is used to identify complex structures and features of facial images. In the face recognition process, CNN identifies different features on the face (eyes, nose, mouth, etc.) and recognizes a person based on combinations of these features. CNN takes facial images as input and performs filtering and feature extraction in successive layers. These procedures determine identity by highlighting important features in various parts of the face. Minutiae-based algorithms are generally used in fingerprint recognition systems. These algorithms work on unique points in fingerprints. In fingerprint images, dots are generally found in certain patterns such as tips, branches, and junctions. Minutiae-based algorithms are used to identify these points and uniquely represent each fingerprint. Then, the identity verification or identification process is carried out by matching these points between different fingerprints.

IV. THE COLLABORATION OF VOICE BIOMETRICS AND ARTIFICIAL INTELLIGENCE IN IDENTITY VERIFICATION PROCESSES

The combination of voice biometrics and artificial intelligence in identity verification processes is used to make voice-based identity verification systems, one of the biometric data, more effective and reliable. This process is based on analyzing voice samples and using them to verify the identity of individuals.

Artificial intelligence plays an important role in analyzing and processing data used in voice biometrics systems. Deep learning and machine learning algorithms are used to verify people's identities by extracting complex features and patterns from voice samples. Artificial neural network models such as CNN, Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) are used in the analysis of voice samples and the identity verification process.

Artificial intelligence has great potential for fraud detection in voice biometrics systems. It is possible to detect fake or manipulated voice samples through real-time analysis of voice recordings. In this way, security can be further increased during the identity verification process.

Voice fraud is not limited to just editing or manipulating an audio recording. It is also possible to create completely artificial sounds with sound synthesis technologies. It can be used to imitate a person's voice or have certain texts read in a specific person's voice. These artificial sounds can appear very realistic when mixed with real sounds and can be difficult to recognize by the human ear. Therefore, checking the accuracy and reliability of audio recordings is extremely important, especially when considering legal or security concerns. Various methods and algorithms can be used to detect the fraud of voice recordings. For example, techniques such as audio spectrum analysis, deep learning algorithms, mathematical operations on the audio signal, and verification of the source of the audio are used to verify the authenticity of audio recordings. The combination of these techniques can provide a more effective and reliable detection process and help identify fake sounds.

The use of artificial intelligence in identity verification processes with voice biometrics has advantages and disadvantages that require detailed analysis. Evaluating these is extremely important to develop strong and successful applications.

Advantages:

- **Accuracy:** Artificial intelligence algorithms can provide high accuracy in identity verification processes with voice biometrics. This enables reliable identity verification by recognizing individuals' unique voice characteristics.
- **Speed and Efficiency:** Artificial intelligence-based voice biometrics systems can perform identity verification quickly and efficiently. This improves user experience and makes processes more efficient.

Disadvantages:

- **Security Concerns:** AI-based systems can potentially be fooled or circumvented by fake voices. This can create security concerns and undermine the reliability of systems.
- **Data Privacy Risks:** The confidentiality of the data used in identity verification processes with voice biometrics is important. However, this data processed and stored by artificial intelligence may pose privacy risks and become accessible to malicious individuals.

- **Technological Dependency:** The use of artificial intelligence-based systems may increase dependence on technology. This can cause identity verification processes to be impacted and become dysfunctional if systems are disrupted.

V. RESULTS

With the development of technology, significant advances have been made in artificial intelligence-based voice biometrics and identity verification processes. Thanks to artificial intelligence, the recognition and analysis of voices have now become more effective and precise. However, with these advances, artificial intelligence technology as well as artificial voice production have also raised potential concerns. Artificial intelligence-based voice recognition systems are successfully used in identity verification processes by analyzing voice features. However, technologies such as artificial sound production should also be taken into account in this process. New algorithms and techniques are being developed to accurately detect artificial sounds.

As a result, given the important role that artificial intelligence technology plays in voice biometrics and identity verification processes, future systems need to be carefully managed and developed in preparation for privacy concerns. In this way, in addition to the benefits that will be gained with the advancement of technology, potential risks that may arise can be minimized.

VI. CONCLUSION AND DISCUSSION

Artificial intelligence-based voice recognition systems are successfully used in identity processes by analyzing voice characteristics. However, technologies such as artificial sound production should also be taken into account in this process. New algorithms and techniques are being developed to accurately detect artificial sounds. This is an important step to increase the reliability of artificial intelligence-based voice recognition systems in identity processes. Considering technologies such as artificial voice generation is a critical requirement to minimize fraud and security vulnerabilities. Therefore, research in the field of voice biometrics needs to focus on developing more sensitive and reliable solutions against potential risks such as artificial voice production.

ACKNOWLEDGMENT

This study was carried out thanks to the working opportunity and infrastructure support provided by Vakıf Katılım R&D Center. These important contributions of Vakıf Katılım R&D Center played a critical role in the successful completion of the research. On this occasion, we would like to express our sincere gratitude to Vakıf Katılım R&D Center for their support.

REFERENCES

- [1] A. I. B. A. B. E. & S. K. Awad, "AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications," pp. 103748,82, 2024.
- [2] A. Goode, "Biometrics for banking: best practices and barriers to adoption. Biometric Technology Today," pp. 5-7, 2018(10).
- [3] S. & K. M. Dargan, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications," pp. 143, 113114., 2020.

- [4] N. A. A. & K. R. A. Singh, "Voice biometric: A technology for voice based authentication. Advanced Science, Engineering and Medicine," pp. 10(7-8), 754-759, 2018.
- [5] M. & P. Z. Glowacki, "Architecture of the integrated system for voice identity distribution. In 2012 19th International Conference on Microwaves, Radar & Wireless Communications," *IEEE*, vol. Vol. 2, pp. 542-545, 2012, May.
- [6] S. Panda, "Intelligent Voice-Based Authentication System. Proceedings of Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)," *IEEE, Palladam*, pp. 757-760, 12-14 December 2019.
- [7] M. L. C. & D. C. M. Fairhurst, "Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data," *IET Biometrics*, vol. 6(6), pp. 369-378, 2017.
- [8] Z. & A. E. Can, "A review of recent machine learning approaches for voice authentication systems, Journal of Information and Communication Technologies," pp. 5(1), 95-113, 2023.
- [9] B. D. S. S. F. N. E. C. P. X. P. I. S. . . & G. A. A. Kaur, "Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet of Things," p. 100780, 2023.
- [10] R. T. Y. W. N. H. F. M. G. A. -G. M. A. & A. I. Jahangir, "Speaker identification through artificial intelligence techniques: A comprehensive review and research challenges. Expert Systems with Applications," pp. 171, 114591, 2021.
- [11] N. N. T. N. Q. & L. Y. An, "Deep CNNs with self-attention for speaker identification," *IEEE*, pp. 7, 85327-85337., 2019.
- [12] D. R. Chandran, "Use of AI voice authentication technology instead of traditional keypads in security devices. Journal of Computer and Communications," pp. 10(6), 11-21, 2022.
- [13] S. S. M. J. N. K. & R. A. S. S. S. Balaji, "AI Based Voice Recognition," *EasyChair*, p. No. 12796), 2024.
- [14] A. K. N. K. & R. A. Jain, "50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern recognition letters," pp. 79, 80-105, 2016.
- [15] [Online]. Available: <https://www.kvkk.gov.tr/>.
- [16] [Online]. Available: <https://gdpr-info.eu/>.