IDENTITY, BIOMETRICS, AND SECURITY OF BIOMETRIC SYSTEMS

Flutra Grabovci
Independent researcher, Republic of Kosovo, fluturagrabovci1@outlook.com
ORCID ID: 0009-0002-2468-2483
Senat Saliu
Independent researcher, Republic of North Macedonia, senat.s@hotmail.com
ORCID ID: 0000-0002-8396-9444

Abstract: This study addresses the concept of identity and the use of biometric methods for the unique recognition of individuals. Identity is based on physical, biographical, and legal features that make each person distinguishable. Biometrics uses physiological characteristics, such as the face, fingerprints, iris, retina, and DNA, as well as behavioral characteristics, such as speech, gait, and signature, to verify identity and prevent fraud. Modern biometric systems can combine multiple modalities to enhance accuracy and performance, leveraging sensors and digital analysis. The use of biometrics provides non-invasive solutions, especially in public environments and remote communication. However, the success of these systems is accompanied by challenges related to privacy, data protection, and user acceptance. This study emphasizes the importance of selecting appropriate biometric features and integrating various technologies for secure and effective identification.
Keywords: identification, biometrics, biometric characteristics.

1. INTRODUCTION

Since the beginning of human civilization, various methods have been used to recognize and identify individuals for purposes such as conducting transactions, verifying authorship of documents, and identifying persons. These methods included fingerprints and palm prints, body measurements, marking, and other forms of identification.

The human body carries information that can be used for identification from birth. With the development of technology, the need for more secure and accurate identification methods has increased, leading to the development of biometric identification. Biometrics represents a group of automated methods for uniquely identifying individuals based on their physical and behavioral characteristics.

Biometric characteristics are mainly divided into physiological and behavioral characteristics. Physiological biometrics includes fingerprints and handprints, DNA, facial features, and eye scanning, while behavioral biometrics relates to speech, voice, movement, handwriting, and signatures.

The aim of this paper is to emphasize the importance of identifying and differentiating individuals, as well as to examine the reliability, accuracy, and potential errors of biometric systems. In this context, biometrics provides a more secure alternative to passwords, which can be lost, forgotten, or misused, by enabling individuals to be identified through their unique characteristics.

2. IDENTITY AND IDENTIFICATION

The concept of identity refers to the subject that defines itself in relation to the object, that is, in relation to all others who surround it or to whom it can refer (Penda & Ivor, 2005, 1-2) Every individual possesses traits that make them unique, recognizable, and unrepeatable. Identity is established on the basis of certain identifying characteristics (Jain et al., 2021). Sometimes an individual's features are obvious, making identity easy to establish. However, often objects of the same type are similar and cannot be distinguished without applying certain methods, which detect details that are then used in the identification process to differentiate the objects. Identity represents the totality of immutable features that constitute a particular person or object, by which that person or object can be distinguished from all others. This set of traits, or individual characteristics, represents individuality (Radmilović Ž., 2009, 3-4).

Based on specific identifying characteristics, the identity of an unknown individual can be established by comparison with a previously known person; this process is referred to as personal identification. Since every person, animal, or object is unique and distinguishable, identification involves comparing specific characteristics to determine similarities or differences. For these characteristics to be suitable for identification, they should meet several basic requirements: universality, uniqueness, permanence, measurability, and ease of collection and use.

The determination and verification of a person's identity involve both physical and legal characteristics. Physical characteristics refer to factual features, while legal characteristics include information established by law, such as first name, surname, nationality, and residence (Radmilović, 2009, pp. 3–4).

A person's identity can be divided into personal, biographical, and biometric identity. Personal identity includes information acquired at birth, biographical identity develops throughout life and is reflected in official records, while

biometric identity is based on unique physical or behavioral characteristics, such as palmprints, facial features, and DNA (Dimić, 2016).

3. BIOMETRICS

Biometrics derives from the Greek words bios (life) and metron (measurement). It represents a group of automated methods for the unique identification of individuals based on one or more of their physical and behavioral characteristics. Biometrics has become an important field for numerous authentication and identification applications in civil and forensic domains (Boubchir & Daachi, 2021).

As an identification technique, biometrics has been known since ancient times, albeit in a slightly different way. The ancient Egyptians conducted various body measurements for identification purposes, in Babylon fingerprints on clay tablets were used for business transactions, and in China merchants used ink and paper to make palm and foot prints to distinguish small children (Boban & Perišić, 2015).

The first anthropometric system, later called the Bertillon system, was developed by the French police officer and scientist Alphonse Bertillon. The system was widely used for identifying criminals and offenders and was based on precise measurements of body dimensions, the length and width of the head, as well as recording personal features such as tattoos, scars, and body deformities. The Bertillon system was used until problems arose related to inconsistent measurement procedures, insufficient measurement accuracy, and the significant variability of the human body over the years. While the system helped narrow down the number of suspects, it did not provide exact results (Boban & Perišić, 2015).

The development of technology has also increased the need for more secure methods of personal identification, making biometric methods significantly more complex and accurate.

Biometric identification refers to technologies that measure and analyze a person's physical and behavioral characteristics. Although it is primarily used for identification purposes, it is also applied in other areas, such as recognizing a user's speech to enable faster typing. Biometrics combines the use of specialized devices that monitor specific physical or behavioral traits with software that analyzes the collected information.

The fundamental elements of biometrics are sampling, that is, converting an analog signal into a digital one, and artificial intelligence. The obtained information is processed by a computer, artificial intelligence is created, the computer recognizes patterns, and the computer's learning system is compared to the human brain. The goal is to use the computer as an intermediary in sampling, while the software package decides what to do with the digitized samples. This encompasses the entire process of digitization, pattern recognition, and artificial intelligence, all with the aim of improving the computer's learning process so that it can independently store and use the samples (CARNet CERT & LS&S, 2006).

4. BIOMETRIC CHARACTERISTICS

The fundamental feature of any biometric system is precisely which biometric characteristics it uses to operate. One of the synonyms often used for biometric characteristics is a biometric modality. The choice of which biometric characteristic or characteristics a biometric system will use depends on many factors. First and foremost, it is important to consider the level of security desired, then the applicability of such characteristics in the required circumstances, as well as the cost and availability of acquisition devices. Every designer of biometric systems must take into account the specificities of individual biometric characteristics and have appropriate evaluation methods for selecting the most suitable ones for their system. Seven factors of biometric characteristics have been defined to determine their suitability for a particular biometric system: universality, uniqueness, permanence, measurability, performance, acceptability, and resistance to circumvention (Cascone et al., 2023).

None of the biometric characteristics or traits can fully satisfy all the aforementioned factors. When developing a biometric system, these factors must be taken into account, and an appropriate balance must be struck between the capabilities offered by specific characteristics.

Biometric characteristics can be divided into two main groups: physiological and behavioral (Abdulrahman & Alhayani, 2023).

The physiological group of biometric characteristics is primarily based on human anatomy and includes features that develop during the fetal stage, such as the hands, fingerprints, and facial structure. The uniqueness of these characteristics is influenced by both genetic factors and prenatal developmental conditions. Studies of identical twins have shown that, despite their high genetic similarity, their fingerprints are not identical. A study comparing the fingerprints of 94 pairs of identical twins found that their fingerprints were more similar than those of unrelated individuals, but they remained distinguishable. This indicates that fingerprint formation is influenced not only by genetics but also by various prenatal developmental factors. Physiological biometric characteristics have been

studied since the early development of biometrics as a science and include several distinctive characteristics (Alrawili et al., 2023).

The face represents a human characteristic that people most often use for recognition. The structure of the face is primarily defined by the shape of the human cranium, as well as by skin texture and pigmentation. There are various face recognition algorithms that use many facial features, such as the distances between different parts of the face, the shape of the head, and the shape of individual facial components. It is very important that algorithms using the face as a basis for recognition rely on facial features that are not prone to change. For this reason, skin color, facial hair, moles, warts, and other potentially temporary facial features are not used.

The ear is becoming increasingly popular as a means of identification. Since the ear is significantly simpler than the face, primarily in shape and secondly in its more uniform color distribution, the load on the biometric system can be much lower, and performance can be better. Additionally, it can be very useful in situations where a person is photographed in profile and face recognition algorithms are not particularly successful. In such cases, the ear is generally available for acquisition.

The fingerprint is the most commonly used biometric characteristic in biometric systems. It is characterized by a high degree of uniqueness, and high accuracy has been achieved in comparison algorithms. A fingerprint is essentially the impression left by the friction ridges of a human finger. The friction ridges are raised layers of the epidermis. Connected ridges form the pattern of a person's finger. These ridges serve to enhance the sense of touch as the finger moves over uneven surfaces by sending signals to the nerves in the finger. Fingerprint comparison is mainly based on the shapes of the friction ridges, with particular attention paid to interruptions or bifurcations in the ridges. Fingerprint acquisition is a relatively simple and minimally invasive process. Initially, it was done by having a person dip their finger in ink and then leave an impression on paper, whereas today advanced optical and capacitive scanners are used to digitize the sample.

Hand geometry refers primarily to the dimensions of the human hand. It takes into account the width of the hand, the length of the fingers, the distance from the base of the hand to the tips of the fingers, and so on. This method is characterized by very easy use, as the hand imprint is simple to capture. High accuracy can be achieved while maintaining good system performance, primarily due to the fact that not too many details are used in the sample comparison process.

The iris is currently one of the most reliable methods in biometric identification and verification. It achieves high accuracy while remaining minimally invasive, as it is possible to capture an image of the iris from a certain distance. The method does not require direct contact with the sensor and uses a relatively simple CCD (Charge Coupled Device) camera, which allows recording in the form of an electrical signal stored with the help of an array of semiconductors.

The retina represents a characteristic that has demonstrated exceptional accuracy and, as such, has found its greatest application in military and security systems. Unfortunately, it is highly invasive, as it requires the subject to place their eye on a sensor and focus it in a specific position for acquisition to take place.

DNA, or deoxyribonucleic acid, is the fundamental material of inheritance, responsible for transmitting traits from parents to offspring. It is located within the cell nucleus in structural units called chromosomes. Biometric identification based on DNA is considered unmatched and indisputable, except in the case of identical twins. The acquisition method is highly invasive and involves collecting biological material containing DNA, such as a buccal swab or a blood sample.

Emerging technologies are becoming increasingly common in the field of physiological biometric characteristics. As a very popular area, biometrics continually generates new ideas for the application of novel biometric traits. Some of these innovations include using a person's scent, pulse rate, specific vein patterns, and even, in the Japanese automotive industry, the concept of using a driver's seat imprint for identification (Blagdon, 2011), which enables automatic adjustment of vehicle settings according to the driver's preferences.

Behavioral biometrics does not primarily rely on anatomical features but on how individuals behave and interact with a biometric system. It involves verifying or identifying individuals by comparing their behavioral patterns with those stored in a database. Since human behavior is complex and influenced by various factors, behavioral biometrics can be more difficult to analyze and generally less stable than physiological biometrics. Behavioral patterns develop over time and are influenced by factors such as human development, environment, language, and lifestyle. However, anatomical characteristics can also affect behavior, making it difficult to completely separate physiological and behavioral influences (Revett, 2008). Behavioral biometrics has significant potential in remote and digital communication, where it can help verify a person's identity without direct contact. This is particularly relevant in text-based communication, where identity can be difficult to confirm. Behavioral characteristics such as typing dynamics, mouse usage, and sentence construction can therefore be analyzed to support identity verification.

Behavioral biometrics represents an important research area and includes various characteristics used for recognition purposes (Yampolskiy & Govindaraju, 2009).

Voice or speech is a subject of great interest to researchers and is one of the earliest behavioral modalities studied in research. This modality is characterized by a simple acquisition method and can be used without the subject's consent, through eavesdropping equipment. It is often employed in criminal investigations as part of digital forensics. Physiological features, such as the anatomy of the vocal cords and the respiratory system, play a significant role in this modality. Voice recognition algorithms are among the most accurate of the behavioral characteristic algorithms and approach the precision of some algorithms based on physiological characteristics. They have particular application as part of multimodal systems, most often in combination with fingerprints or other physiological modalities. Voice recognition can be either text-dependent or text-independent. Text-dependent systems achieve higher accuracy but are more invasive, requiring the subject to repeat the same phrase during both enrollment and later verification or identification.

Gait is the most studied biometric characteristic based on the motor abilities of the human body. It is researched in many fields, ranging from medicine to robotics and computer science. Particular interest arises in medical sciences, as it is primarily used to find ways to compensate for disabilities and to develop prosthetic devices. Gait-based recognition is a relatively young discipline but highly interesting. It involves using video cameras or body-mounted sensors to record a person's gait, and the resulting recordings are then used to create a unique gait pattern. The effectiveness of gait-based biometric systems is promising and provides a solid foundation for further research and improvement.

Signature has historically been used predominantly as a means of confirming a person's identity. A person's signature served as proof of agreement with the content of a document. Even today, in judicial systems, a signature represents a legally valid confirmation of identity. Even before the advent of computer systems, various techniques were developed to verify the authenticity of a signature. These techniques were based on the dynamics of writing movements, characteristic pen lifts, pressure intensity on the paper, letter shapes, and more. With the introduction of computer systems, it became possible to convert paper signatures into digital form through scanning, leading to the development of various signature verification algorithms. Initially, these algorithms were based on previously used techniques, simply adapted into a machine-readable format. Signature recognition algorithms can operate online or offline. Online recognition involves real-time verification based on the impression a user provides on a specialized device, such as a graphics tablet. These algorithms can capture dynamic signature characteristics, such as line-drawing speed and pen pressure. Offline algorithms, on the other hand, work primarily with scanned signatures and cannot assess dynamic characteristics; instead, they rely mainly on letter shapes, height, and other static features.

Blinking is a modality that is gradually gaining interest. So far, there has not been much progress in its use, but it is considered to have solid potential. It is used by having the user attempt to follow an external stimulus with blinking, such as a piece of music. Measurements can include the time between blinks, the duration of individual blinks, and the number of blinks in a sequence.

Dynamic facial movements involve the activity of a user's face during the period of authentication or recognition. There have been attempts to utilize the specific characteristics of a person's smile. Additionally, some attention has been given to the behavior of pores on human skin during certain facial movements. The basic idea behind these methods is that facial muscles produce characteristic movements that a camera can capture, which can then be used for comparison and recognition.

Lip movements are based on a model-based approach, where a model is generated from the dynamics of lip movements and later used for comparison. A key aspect is the segmentation of the lips from a video recording, which serves as the basis for recognition. The features used in creating the model include the dynamics of mouth opening and closing, as well as certain physiological characteristics such as the width, thickness, or shape of the lips.

Credit card usage is primarily used in banking systems as a specific part of monitoring systems aimed at fraud prevention. Data mining techniques are generally employed, taking into account a wide range of factors, including the location of spending, spending patterns, the type of goods, or the retail outlet where purchases are made. The main purpose is to verify the identity of the user of the credit card and to prevent misuse.

Behavioral modalities arising from human-computer interaction are increasingly characterized by the emergence of new modalities that develop alongside advances in devices used to control computer systems. Some of the most frequently mentioned include typing dynamics, mouse usage dynamics, command word usage patterns, programming style, specific interaction with graphical user interfaces, generated network traffic, and many others. The development of interaction devices almost immediately inspires ideas for using these devices as acquisition tools for various recognition techniques. One example is the touchscreen interaction style, enabled by the advent of a new generation of touch-sensitive screens.

Emerging behavioral modalities are closely linked to advances in technology and sensors. As motor vehicles become equipped with an increasing number of sensors, one newly proposed modality is driving style. Additionally, modalities related to the specific use of software are becoming increasingly popular, such as email behavior, which monitors a range of factors related to how a user interacts with email. Similarly, there is web behavior. Recently, particular attention has been given to various games and the ability to identify players based on their in-game behavior. This modality is often referred to as game strategy and pertains both to a person's behavior in virtual game environments and in different social games, where strategies and playing styles—such as in poker—are frequently discussed (Milovanović, 2013)

5. MULTIMODAL BIOMETRICS

Multimodal biometrics is an advanced approach to identity verification and access control that combines multiple biometric modalities, such as fingerprints, facial features, iris patterns, and voice. By using several biometric characteristics instead of relying on a single trait, it improves accuracy, reliability, robustness, and security while reducing the limitations of unimodal systems (Bufer, 2023; Friedman, Hastie, & Tibshirani, 2000).

The main advantages of multimodal biometrics include improved identification accuracy, reduced False Acceptance Rates (FAR) and False Rejection Rates (FRR), and greater resistance to spoofing and unauthorized access. It also performs better in challenging conditions where one biometric modality may be affected by environmental or physical factors. However, its implementation requires sophisticated fusion algorithms, reliable data from each modality, interoperability and standardization, as well as strong privacy and data protection measures (Fang, Wang, & He, 2020, p. 752; Bachman, 1967, p. 45).

Multimodal biometric systems are applied in various fields, including access control, law enforcement, forensic investigations, border control, and healthcare. They enable more reliable identification by combining different biometric characteristics, such as fingerprints, facial recognition, and iris recognition. Current research focuses on improving fusion algorithms, integrating new modalities such as gait, ear shape, and behavioral biometrics, and applying machine learning and deep learning to enhance system performance and adaptability (Levenson, He, Chen, & Fang, 2021, p. 5; Hastie, Tibshirani, & Friedman, 2009, p. 350).

6. RELIABILITY AND ACCURACY OF BIOMETRIC SYSTEMS

With the development of technology, the need for safer environments and reliable systems for protecting people and property has increased. Traditional authentication methods, such as passwords, PINs, keys, and cards, have limitations because they can be lost, forgotten, shared, or copied. Consequently, biometrics is increasingly used as a more secure and reliable method of identity verification. However, biometric systems also have limitations, making reliability an important factor in evaluating their performance (Ćosić, 2015).

The accuracy of biometric identification systems depends on the type and quality of collected data, the equipment used, and the conditions under which biometric samples are obtained. No biometric system is completely accurate because biometric characteristics may vary depending on the time and conditions of data collection. Therefore, system performance must be evaluated by considering the accuracy of matching and the quality of input data (Paunović & Starčević, 2013).

Two major errors may occur in biometric systems: False Acceptance Rate (FAR) and False Rejection Rate (FRR). False acceptance occurs when an unauthorized person is incorrectly accepted as a legitimate user, while false rejection occurs when an authorized user is incorrectly denied access. FAR and FRR depend on the system's security threshold and represent a trade-off between security and usability. Increasing security requirements may reduce false acceptance but simultaneously increase false rejection (Paunović & Starčević, 2013).

In addition to these errors, biometric systems face other limitations, including high equipment costs, insufficient practical testing, varying system reliability, and privacy concerns related to the collection and storage of biometric data. Therefore, before implementing a biometric identification system, its reliability, accuracy, performance, limitations, and privacy implications should be carefully evaluated (Paunović & Starčević, 2013).

7. PRIVACY PROTECTION

Privacy is the ability to live independently and control access to personal data. As biometric systems are increasingly used in medicine, finance, insurance, forensics, and personal documents such as passports, privacy protection has become an important concern.

Biometrics raises three main privacy concerns. First, biometric characteristics are biological and may reveal additional personal or medical information that could lead to discrimination. Second, some biometric methods can enable unwanted identification, even of individuals using pseudonyms. Third, biometric characteristics are not secret

and may be collected without a person's knowledge, limiting anonymity (Prabhakar, Pankanti, & Jain, 2003). Therefore, biometric data should be collected for clearly defined purposes and used only for those purposes.
Various security measures have been developed to protect biometric data, including cancelable biometrics, renewability, and crypto-biometrics. Cancelable biometrics transforms biometric templates into an unusable form to protect them after theft. Crypto-biometrics uses cryptographic algorithms for encryption and decryption and can reduce the need to store biometric images or templates while supporting greater privacy. However, it may have lower accuracy and remain vulnerable to attacks on biometric templates or communication channels (Konjevod, 2016).

8. CONCLUSION

Identity represents a set of unique characteristics that make each individual distinguishable from others. The identification process is based on the comparison of these traits, which must be universal, measurable, stable, and difficult to imitate. With technological advancement, traditional identification methods have been supplemented and often replaced by biometric systems, which rely on physical and behavioral characteristics. Biometrics offers significant advantages due to its accuracy, security, and resistance to fraud, but it also carries challenges, such as invasiveness in some techniques, sensitivity to behavioral changes, and the need for specialized equipment.
Physiological characteristics (such as fingerprints, face, retina, iris, DNA) are more stable and accurate, whereas behavioral characteristics (such as writing style, speech, gait) can change over time and are influenced by many factors. Nevertheless, both groups form the foundation for the modern development of security and authentication systems. Multimodal biometric systems offer higher accuracy and security by combining multiple methods to prevent fraud and ensure reliable verification. However, every biometric system has limitations, and its reliability, accuracy, and suitability for specific purposes must be carefully evaluated.
Institutions using biometrics must implement clear protocols for the protection of biometric data, employing strong encryption algorithms and secure data storage. Methods requiring direct contact or the collection of biological samples (e.g., DNA, retina) should be used only in critical cases, such as criminal investigations or national security.
The use of multimodal biometric systems is essential for accurate and reliable identification, especially in digital communication and remote transactions. By combining different biometric traits, security is enhanced, and the risk of fraud is reduced. The traits must be universal, individual, stable, and measurable, while data collection should respect privacy and individual rights. Investment in development and innovation, particularly in new modalities and behavioral identification, helps improve existing systems and increase security.

REFERENCES

Alrawili, R., AlQahtani, A. A., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers & Electrical Engineering, 119, 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Altaras Penda, I. (2005). Identity as a personal issue. Revija za sociologiju, 36 (1-2). https://hrcak.srce.hr/13684

Bachman, J. G. (1967). University of Michigan. Survey Research Center and youth in transition. Ann Harbor Institute for Social Research, 1.

Blagdon, J. (2011). Japanese biometrics engineer wants us to sit to authenticate. The Verge. Retrieved March 12, 2012, from http://www.theverge.com/2011/12/23/2657191/biometrics-seat-pressureauthentication

Boban, M., & Perišić, M. (2015). Biometrics in the system of security, protection, and monitoring of information systems. In D. Zlatović (Ed.), Proceedings of the Polytechnic of Šibenik. Šibenik: Polytechnic of Šibenik. http://hrcak.srce.hr/142285

Boubchir, L., & Daachi, B. (2021). Recent advances in biometrics and its applications. Electronics, 10(9), 1097. https://doi.org/10.3390/electronics10091097

Cascone, L., Gao, Z., & Nappi, M. (2023). Biometrics for Industry 4.0: A survey of recent applications. Journal of Ambient Intelligence and Humanized Computing, 14, 11239–11261. https://doi.org/10.1007/s12652-023-04632-7

Ćosić, Z. (2015). Method for evaluating the reliability of biometric systems (Doctoral dissertation). Faculty of Organization and Informatics, University of Zagreb. https://urn.nsk.hr/urn:nbn:hr:211:269147

Dimić, M. (2016). Biometric identification systems (Undergraduate thesis). Faculty of Philosophy, University of Osijek. https://zir.nsk.hr/islandora/object/ffos:2344

Fang, Y., Wang, H., & He, W. (2020). A statistical roadmap for journey from real-world data to real-world evidence. Therapeutic Innovation & Regulatory Science, 54, 749–757.

Friedman, J., Hastie, T., & Tibshirani, R. (2000). Additive logistic regression: A statistical view of boosting (with discussion and a rejoinder by the authors). Annals of Statistics, 28, 337–407.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). Boosting and additive trees. In The elements of statistical learning: Data mining, inference, and prediction (pp. 337–387).

Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. arXiv. https://arxiv.org/abs/2105.06625

Konjevod, M. (2016). Biometrics and privacy protection (Undergraduate thesis). Faculty of Philosophy, University of Osijek. https://urn.nsk.hr/urn:nbn:hr:142:787558

Lee, H., Hong, S., & Kim, E. (2009). An efficient gait recognition with backpack removal. EURASIP Journal on Advances in Signal Processing, Article 46.

Levenson, M., He, W., Chen, J., & Fang, Y., et al. (2021). Biostatistical considerations when using RWD and RWE in clinical studies for regulatory purposes: A landscape assessment. Statistical Biopharmaceutical Research, 1–11.

Milovanović, M. M. (2013). Application of CBIR techniques in biometric identification of people based on gait (Doctoral dissertation). Belgrade.

Oloyede, M. O., & Hancke, G. P. (2016). Unimodal and multimodal biometric sensing systems: A review. IEEE Access, 4. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7580649

Paunović, S., & Starčević, D. (2013). Biometric systems for determining identity. Proceedings of the International Conference and Exhibition: XXVIII Scientific-Professional Conference InfoTech 2013, Aranđelovac, June 12–13, 2013. Belgrade: JURIT. http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/081.pdf

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. IEEE Security & Privacy. http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf

Radmilović, Ž. (2009). Biometric identification. Policija i sigurnost, 17(3-4). https://hrcak.srce.hr/79284

Revett, K. (2008). Behavioral biometrics: A remote access approach (1st ed.). West Sussex, UK: Wiley Publishing.

Yampolskiy, R. V., & Govindaraju, V. (2009). Taxonomy of behavioral biometrics. In L. Wang, X. Geng, L. Wang, & X. Geng (Eds.), Behavioral biometrics for human identification: Intelligent applications.

Wolie Bufer. (2023). Multimodal biometrics: Strengthening security through fusion of unique traits. Journal of Biometrics & Biostatistics, 14(3). https://www.hilarispublisher.com/open-access/multimodal-biometrics-strengthening-security-through-fusion-of-unique-traits-100124.html?utm