Associate prof. Dipankar Haldar, PhD
Serampore College University in India
e-mail: dipankarsmp@gmail.com
ORCID: 0000-0002-3970-8095

Justyna Gach
WSB University in Dąbrowa Górnicza
e-mail: gach.justyna1701@gmail.com
ORCID: 0009-0001-2651-0

DOI: 10.26410/SF_2/25/13

THE APPLICATION OF BIOMETRIC METHODS IN PERSONAL IDENTIFICATION

Abstract

Biometrics, a technique for identifying individuals based on their unique physical and behavioral characteristics, is finding growing use in a variety of fields, notably security systems. This article examines a variety of biometric approaches used in identification procedures, including fingerprint analysis, facial recognition, iris scanning, retina scanning, and voice and handwriting recognition. The operating principles and practical uses of these technologies, such as access control systems, border security, public monitoring, and law enforcement, are discussed. The study evaluates the performance of distinct biometric approaches, as well as their advantages and limits in identity verification. It also covers the difficulties in maintaining biometric databases and how they affect the accuracy and reliability of identification operations. Biometrics, owing to its precision and speed, is recognized as a vital instrument in crime prevention and national security. The study concludes by reflecting on the future of biometrics, the advancement of identifying technologies, and the issues that may arise when biometrics are increasingly implemented in international security systems and identity management.

Keywords

Biometrics, identification, security systems, dactyloscopy, national

Introduction

Identifying and safeguarding human identity has become crucial in the age of digital transformation, the increasing significance of information security, and the pervasive use of mobile and internet-based technologies. In this regard, biometrics – an interdisciplinary discipline that incorporates aspects of computer science, biology, mathematics, statistics, law, and ethics – is one of the fastest-growing sciences. The field of biometrics focuses on identifying and validating people using their distinct biological traits (such as fingerprints, iris patterns, or vascular structures) or behavioral traits (such as voice patterns, typing rhythm, or stride). Unlike traditional passwords, biometric techniques don't need the user to memorize them, which makes them very accurate and resistant to falsification. International standards provide a clear definition of biometrics. The International Organization for Standardization (ISO) defines biometrics as the "Automated recognition of individuals based on their physiological and/or behavioral characteristics"[1]. This implies it is based on who a person is or how they act, rather than what they own (e.g., an access card) or know (e.g., a password). Biometrics is now used in a variety of applications, including national security and military systems, e-banking, border control, healthcare, and ordinary consumer electronics like cellphones, laptops, and payment terminals. Its presence has become almost imperceptible while remaining important. Although biometrics as a scientific area just emerged in the nineteenth century, its origins go far deeper. Biometric features have been used for identification since ancient China, when merchants and authorities signed with their fingerprints. with medieval Persia, physical descriptions of prisoners were documented to aid with identification. In the late nineteenth century, British scientist Francis Galton, a cousin of Charles Darwin, showed the uniqueness of fingerprints and developed the first classification system for them, marking a watershed moment in the development of biometrics as a scientific approach. Around the same period, Alphonse Bertillon created an anthropometric system based on body measurements that was used by police agencies for many years[2]. The subsequent introduction of digital computers and algorithmic methodologies permitted the development of the first automated biometric systems, and the turn of the twentieth and twenty-first century witnessed a surge in the everyday usage of biometric technology[3].

Biometrics now plays an important part in the digital infrastructure of the information society, in addition to serving as an identifying system. However, as it grows in popularity, so does the number of legal, ethical, and societal problems. Biometric data is regarded highly sensitive since it is immutable and directly linked to an

1 A. K. Jain, A. Ross, K. Nandakumar, *Introduction to Biometrics*, Springer, 2011, p. 119.

2 National Research Council. *Biometric Recognition: Challenges and Opportunities*, p. 212.

3 J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, p. 198.

individual's identity; once hacked, it cannot be altered or canceled, unlike a password. Furthermore, some biometric technologies, such as face recognition in public places, pose severe concerns regarding surveillance limits, privacy rights, and civil liberties. According to Alessandro Acquisti, a top researcher in privacy and data ethics, "Biometrics are the most reliable identifiers that cannot be lost, forgotten, or changed. That's what makes it so strong and deadly"[4].

In response to these concerns, some governments and international organizations have enacted legislation to protect individual rights. The General Data Protection Regulation (GDPR), also known as the European Parliament and Council Regulation, is the most significant legal legislation controlling the processing of biometric data in Europe. According to GDPR, biometric data used to uniquely identify a natural person is classified as a special category of personal data that is generally prohibited from being processed unless specific legal grounds exist, such as explicit consent, public interest, employment necessity, or national security. GDPR also requires data controllers to follow principles such as data minimization (processing only what is necessary), implementing appropriate technical and organizational safeguards, and allowing individuals to exercise their rights, which include access to, correction, deletion, and objection to the processing of their data[5].

Biometrics, while technically sophisticated and full of potential, is not a neutral phenomenon; its advancement necessitates a constant balancing act between identification system efficiency and the safeguarding of basic human rights. The current user of biometric technology frequently unknowingly leaves traces of their identity not just online but also in databases whose security is critical to avoiding abuse. As a result, any introduction to biometrics must go beyond the technological and practical elements, taking into account the social, ethical, philosophical, and legal settings. Only then can we completely comprehend the importance of biometrics and its role in defining the future of human-technology interactions[6].

The current development of biometrics is bringing us closer to a scenario in which the distinction between physical and digital identity is becoming increasingly blurred. Access to services is increasingly granted using the distinctive aspects of our own bodies – our face, voice, eyes, or hands – rather than papers, passwords, or codes. In light of this shift, a fundamental issue arises: are we, as a society, ready for such a profound integration of our physical selves with technology? The solution is far from straightforward. On the one hand, biometrics provides great convenience, increases security, and lowers the chance of fraud. On the other hand, it requires complete faith in the organizations that collect and handle our data, as well as assurance that the methods used to identify us would not be used against us in the future.

4 S. Rane, Y. Wang, S. C. Draper and P. Ishwar, *Secure Biometrics: Concepts, Authentication Architectures and Challenges*, p. 326–339.

5 M. Faundez-Zanuy, J. Fierrez, M. A. Ferrer, M. Diaz, R. Tolosana and R. Plamondon, *Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health*, p. 87.

6 Ibid., p. 108.

Biometrics' future will be influenced not just by technology improvement, but also – and maybe more importantly – by public discussion, law, organizational ethics, and civic consciousness[7].

As a result, one of the most pressing tasks in the coming years will be not only the continued refinement of biometric algorithms, but also the development of what could be referred to as "technological ethics," as well as user education about their rights and the potential threats posed by the misuse of biometric data. Engineers and developers are not the only ones responsible for the future of this sector; legal experts, educators, sociologists, and philosophers are all involved and, most importantly, users must learn to evaluate the technology they use critically. In a world where "our body becomes our password," as many technological pundits now claim, we require a new level of awareness and alertness. Biometrics is more than just a technology; it is also a reflection of our societal values, attitudes toward privacy, and the extent to which we respect human dignity in the digital era[8].

In a larger sense, biometrics has become a symbol of the evolving interaction between humans and technology. Algorithms are increasingly processing our bodies, emotions, and movements, converting them into data that is then used to validate our identities. Rather of being recognized for our tales, words, or experiences, we are more identifiable by our appearance or behavior. This transition poses fundamental problems, such as whether technology allows us to express ourselves or reduces us to patterns and statistics. Are we still people creating our own identities, or are we becoming objects of incessant analysis? As biometric systems gain strength and popularity, we must determine whether we want a future based on trust and freedom or control and monitoring. That is why it is critical to create biometric technology in a way that preserves fundamental values such as privacy, dignity, and individual autonomy[9].

We must also remember that biometrics does not emerge in a vacuum; rather, it evolves within a social and political environment. Engineers, governments, companies, and individuals all have influence on how it is utilized. History has proven that even the most promising technology may be exploited if protections are not in place. This is why we need clear standards, more public knowledge, and open conversations about how biometric data is gathered and used. Biometrics is more than simply a technology; it holds significant power and responsibility. We must question ourselves whether we want a world in which biometrics make us safer and more empowered, or one in which they limit our freedom. In the end, how we utilize biometric technology will be a test–not only for science and law, but for society as a whole–to see if we can maintain our humanity in a more digital environment[10].

7 Ibid., p. 209

8 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed., p. 78.

9 J. Wayman, A. K. Jain, D. Maltoni and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, p. 48.

10 Ibid., p. 76

Types of methods

Biometric technologies are among the most advanced and successful methods for identifying and authenticating persons in both digital and physical systems. Unlike traditional security measures such as passwords or PIN codes, biometrics are based on the examination of individual qualities that are unique to each individual and exceedingly difficult to duplicate or fabricate. Biometric systems may use both physical and behavioral features, increasing their adaptability and extending their range of applications. In practice, a number of biometric approaches are used, each adapted to the unique demands of the company, desired security level, and ambient conditions.

These approaches are often divided into two categories: static techniques, which study permanent physical aspects, and dynamic techniques, which focus on human activities. Static biometric approaches provide greater accuracy and long-term consistency, whereas dynamic methods provide continuous identification verification throughout user activities. Regardless of the technology employed, the process entails collecting biometric data, processing it, extracting differentiating characteristics, and comparing the results to a stored reference template. Advanced artificial intelligence and machine learning algorithms offer more precise matching and lower false acceptance or rejection rates[11].

Biometric systems are utilized in both the public and private sectors, ranging from access control and transaction authorization to surveillance and national security identification. These technologies are increasingly often combined with mobile and cloud-based systems, making them acceptable for everyday applications while yet providing high levels of data security. However, deploying biometric technology raises legal and ethical concerns, notably around user privacy and accountability for any breaches. The system's ability to withstand spoofing assaults and other cybersecurity risks is a key consideration.

Biometrics' high efficacy originates from the difficulty of copying an individual's unique traits, which serve as a type of "access key." Well-designed systems may significantly lower the danger of illegal access while improving overall information and asset security. Different biometric approaches offer varied degrees of accuracy, reliability, and user ease, which is why hybrid systems that combine numerous techniques are frequently used. These combinations improve the system's resilience and flexibility to changing environmental circumstances[12].

In recent years, dramatic breakthroughs in digital technology and device downsizing have allowed biometrics to be applied on an unprecedented scale. Modern systems provide real-time user authentication, which is becoming increasingly crucial in light of rising cybersecurity risks and the need to secure sensitive data. It's also worth noting that the success of a biometric system is determined not only by the

11 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed., p. 211.
12 Ibid., p. 139.

underlying technology, but also by the quality of the input data, the environment in which it is gathered, and the security with which the biometric templates are maintained. Biometrics have enormous promise for automating security procedures and maintaining identities, but successful deployment necessitates appropriate infrastructure, user education, and compliance with data protection requirements.

These technologies provide a high level of security and accuracy by analyzing unique physical or behavioral characteristics that are difficult to forge, with ideal examples including the face, iris, fingerprint, hand geometry, voice, signature, and scent, while biometric methods use these features to reliably identify or authenticate individuals, finding wide application in security systems across both the private and public sectors.

Facial Recognition Technology: Principles, Applications, and Ethical Implications

The biometric approach of facial recognition includes studying the unique anatomical characteristics of the human face in order to identify or authenticate an individual. These systems process a face picture using cameras and powerful algorithms before comparing it to a database-stored template. These methods examine key traits such as eye distance, nose shape, jawline contour, and face proportions. Facial recognition may work in both static and dynamic situations (for example, passport images and real-time surveillance). The fact that this technology is contactless and user-friendly is one of its most significant advantages. This technology is utilized in cellphones, airports, access control systems, and city monitoring. Despite its great accuracy, facial recognition may face obstacles due to illumination, facial emotions, or partial face occlusion. Concerns have also been raised concerning privacy and the possibility for select organizations to misuse this technology. As a result, it is critical to appropriately control its usage and safeguard the security of users' biometric information. Facial recognition technology is continually advancing, and contemporary systems can recognize and analyze faces in crowds, from a distance, and from different perspectives. Artificial intelligence and machine learning are increasingly being utilized to increase accuracy and minimize identifying mistakes. In certain nations, similar technologies are also employed to fight crime and track down wanted persons. Facial recognition is used in the private sector to personalize services, such as in retail and marketing. This strategy is projected to become even more popular in the future, but there will also be an increase in demand for solutions that assure transparency and ethical use of technology[13].

Iris Pattern Recognition: Precision-Based Identification in High-Security Environments

Iris recognition is a very accurate and secure biometric identification technology. The iris, the colorful region of the eye that surrounds the pupil, has a distinct pattern that remains consistent throughout a person's lifetime. Even identical twins have varied

13 M. A. Turk, A. P. Pentland, *Eigenfaces for Recognition*, *Journal of Cognitive Neuroscience*, 1991, p. 71–86, available online: https://watermark.silverchair.com/jocn.1991.3.1.71.pdf [accessed: February 18, 2025].

iris patterns; therefore, this procedure is quite dependable. The method works by taking a high-resolution image of the eye with specialized cameras, frequently employing infrared light to emphasize the iris' complex intricacies. The collected pattern is then transformed to mathematical code and compared to data stored in a database. This approach has an extremely low mistake rate, both in terms of rejections and false acceptances. It is therefore often utilized in high-security settings including airports, military installations, and government buildings. Furthermore, iris scanning is quick, contactless, and user-friendly. The iris does not deteriorate or wear out with frequent use like fingerprints do. Additionally, the system is very resistant to efforts at deception, including the use of pictures or artificial eye replicas. However, the expense of implementation and the requirement for accurate imaging equipment are two of the difficulties. However, iris recognition is becoming more widely available because to technological developments, and it is being utilized more often in commercial applications such as payment systems and cellphones. All things considered, iris recognition is regarded as one of the most reliable biometric techniques now in use[14].

Fingerprint Analysis in Biometric Systems: Accessibility, Accuracy, and Challenges

One of the most popular and practical biometric identification techniques is fingerprint-based. Since each person has a distinct fingerprint pattern, this technology is extremely accurate and difficult to counterfeit. In order to authorize access, the fingerprint is scanned and compared to a previously saved template. Depending on the equipment, several technologies, such as optical or ultrasonic sensors, can be used for the scan. We frequently employ this technique to get entry to guarded facilities, unlock phones, and enter into bank accounts. It is quick and doesn't require password memory, which is convenient for a lot of people. It's not flawless, though; occasionally if a finger is damp, unclean, or damaged, the scanner won't be able to read the fingerprint. Security issues also arise since, unlike passwords, you cannot simply "reset" your fingerprint data if it is stolen. To increase security, this technique is frequently used in conjunction with other biometric technologies, such as facial recognition. Artificial intelligence is currently used by more sophisticated systems to improve accuracy and function better under various circumstances. However, the more biometric data we get, the more crucial it is to adequately preserve it, both legally and technically[15].

Hand Geometry-Based Identification: Mid-Security Biometric Solutions in Practice

The method which is related to biometric and use the geometry of a hand is the use of the biometrics of hand geometry. In Hand-geometry, the attributes are based on the shape, length and width of the finger and the ratio of different parts in the hand,

14 M. Goc, J. Moszczyński, *Polish Society of Criminology*, Warsaw, 2007, p. 36.

15 R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, *Biometric Identification Through Hand Geometry Measurements*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1188–1191, available online: https://ieeexplore.ieee.org/document/879796 [accessed: February 18, 2025].

as opposed to fingerprint patterns on papillary lines. This invention can tolerate minor skin injury, or dirt. Hand geometry-based systems are fast, user-friendly, and, in general, non-invasive. Handprint recognition system can be used in medium secure areas, access control of building or time attendance system also to the gym. During the enrollment, the user's hand is scanned once and saved in a system in the form of a pattern. For verification, the user presses his or her hand onto a dedicated scanner and the current image is compared to a reference image that had been previously stored. One of the benefits of the approach is that it suffers very low failure rate and it is also less costly to implement on the ground. Even when operating with a large number of users, these systems perform well. While it is true that hand geometry is not as singular as an iris or fingerprint, it is secure enough for most applications. The technology conveniently excels where speed and user comfort are concerned. This method's somewhat lesser accuracy when compared to more sophisticated biometric approaches is a disadvantage. Furthermore, hand geometry-based systems necessitate direct physical contact with the scanner, which in some circumstances may be deemed unsanitary. Hand geometry recognition is still a common and useful option for many businesses in spite of this[16].

Voice Biometric Authentication: Voiceprints, Vulnerabilities, and Technological Progress

Voice biometric identification is an authentication technique that uses an analysis of an individual's distinctive speech patterns. Pitch, tone, speed, accent, and timbre are some of the unique characteristics of the human voice that make it challenging to mimic. These characteristics are used by speech recognition software to generate a distinct voiceprint that is linked to a certain person. Voice registration and real-time voice comparison are usually the two steps in the procedure. Voice recognition makes contactless and easy authentication possible, in contrast to more conventional techniques like passwords or PIN numbers. Numerous applications use it, such as access control, customer service systems, cellphones, and telephone banking. Crucially, these systems may function in both passive and active modes, requiring the user to pronounce a certain word. Notwithstanding its benefits, this technology has drawbacks. Background noise, throat conditions, voice fatigue, and the speaker's emotional state can all have an impact on recognition accuracy. Anti-spoofing features are frequently included in contemporary systems due to worries about possible fraud involving voice recordings or artificial voices. However, thanks to developments in machine learning and artificial intelligence, speech biometrics is always getting better. It is a desirable identification approach, particularly in situations like distant identity verification where other biometric techniques are less useful[17].

16 A. Służewska, *Methods of Visualizing Fingerprint Traces on the Metal Surface of Cartridge Cases – a Brief Review*, *Problemy Kryminalistyki*, 2007, No. 257, Warsaw, 2007, p. 47.

17 M. Kulicki, V. Kwiatkowska-Wójcikiewicz, L. Stępka, *Forensic Science. Selected Issues of Criminal and Judicial Investigative Theory and Practice*, Toruń, 2009, p. 324–330.

Dynamic Signature Recognition: Behavioral Biometrics in Legal and Financial Contexts

Analyzing each person's signature's distinct features is the foundation of the biometric signature recognition technique. Biometric systems examine dynamic characteristics including pen pressure, writing speed, rhythm, and angle, in contrast to conventional handwritten signatures that are readily falsified. Biometric signatures are far more secure since these criteria are hard to copy. This approach makes use of specialized tools, such as digital pens or graphic tablets, that record intricate information while the sign is being made. Banks, government agencies, insurance providers, and other sectors requiring safe and trustworthy identification verification utilize signature recognition. Since many individuals are used to signing documents, this method's naturalness and social acceptance are among its main advantages; it doesn't feel invasive. Furthermore, it is simple to include a biometric signature into already-existing electronic documents. Nevertheless, this approach may be susceptible to changes in writing style brought on by stress, sickness, or exhaustion. As a result, biometric systems need to be calibrated correctly and have a margin of tolerance. Biometric signatures are becoming more and more popular as an addition to or substitute for conventional authentication techniques in spite of these drawbacks. These systems have two modes of operation: identification mode, which compares a signature to several templates in a database, and verification mode, which compares a signature to a stored template. Therefore, biometric signatures may be used to legally sign electronic documents and to verify identification. The increasing need for automated and secure identification systems is satisfied by this technology[18].

Olfactory Biometrics: Experimental Approaches to Human Scent-Based Identification

Based on each person's own fragrance, olfactory biometrics holds promise as an identifying technique. Each smell is distinct and is released by the human body as a result of sweat gland activity, skin bacteria, and other variables. Specialized tools, including chemical sensors, are needed to use this technology. These tools analyze and identify fragrance molecules in order to provide a biometric profile. This approach has drawbacks even though fragrance is hard to fake. The accuracy of identification can be impacted by a person's changing fragrance due to dietary changes, stress, medicine, and other environmental circumstances. Nevertheless, olfactory biometrics finds use in domains including environmental research, medical diagnostics, and security. As technology develops, it may become more popular and support other biometric techniques like fingerprint or face recognition. For this reason, despite the challenges associated with its use, olfactory biometrics could become an innovative tool in improving security and the accuracy of identification processes across various industries.

18 J. Gach, A. Tavares, *Fingerprinting as a Biometric Identification Tool: Methods and Applications in Modern Forensic Science*, *Security Forum*, 2024, No. 2.

Technical, Legal and Societal Challenges of Biometric Identification Systems

Biometrics is becoming a regular part of our daily lives – from unlocking phones, online banking, to airport security systems. It seems fast, convenient, safe, and modern. And to be fair, it does have a lot of advantages. But, as with most technology, things aren't always as perfect as they seem. Biometric sciences come with a number of serious downsides, many of which are overlooked or ignored. Before we fully embrace them, it's worth taking a closer look at the risks involved. Setting up a biometric system is expensive. You need hardware to scan faces, fingerprints, or irises, along with proper software and security infrastructure.

These technologies don't come cheap, which limits access for many institutions. It feels like this type of security is only for those who can afford it, creating a gap in availability and fairness. Biometrics doesn't work everywhere or in every condition. If it's dark, dirty, or if the equipment glitches – facial or fingerprint recognition might fail. In criminal investigations, it's even trickier[19]. Gathering high-quality biometric evidence at a crime scene isn't always possible. Rain, poor lighting, dust – and suddenly the entire system is useless. Skin damage, scars, illness, or just the natural aging process can make it hard for the system to recognize someone. And what about people without fingers, hands, or with facial deformities? For them, biometric tech simply doesn't apply. Sometimes, humans just don't fit the system. Additionally, biometrics isn't always as quick as claimed. Analysis in police or financial systems may take a while. The technology moves at its own speed and doesn't always live up to our expectations. The longer it takes to receive a result, the more complicated the case. Data leaks are one of the main issues. You can change your password if it is stolen. However, if someone manages to obtain your fingerprints or face information, you will be permanently affected. You cannot change your hands or face. Unfortunately, hackers may still affect even the most protected systems. Then there is the possibility of misidentification[20]. Not every technology is flawless. It's possible for a system to mistakenly identify someone, accusing an innocent person or allowing the wrong person to escape punishment. Errors like this can have major repercussions in high-stakes situations like courtrooms or airports. Another major warning sign is surveillance. Presumably for safety, facial recognition cameras are becoming more and more common in public areas, but sometimes without the knowledge or approval of the public. You may never be aware that you are being followed. That poses a serious risk to individual privacy. Speaking of permission, you frequently have no actual say in the matter. Do you want to utilize this service or app? Enter your biometric information. Do you not want to? You

19 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed, p.138.
20 Ibid., p 176.

can't access it then. What a waste of voluntary involvement. Furthermore, biometric technologies have the potential to discriminate. They don't give everyone the same recognition[21]. Elderly people, children, and those with darker skin are frequently mistaken. In the end, a purportedly impartial technology serves to strengthen already-existing societal injustices. Profiling can also be done with biometric data. Businesses may create thorough behavioral profiles by examining a person's gait, speech, and gadget usage. They can then sell this information to insurance companies or advertisements. It invades your personal life and goes beyond identification. The absence of control is another problem. You have no idea where your biometric information is kept, who may access it, or what happens to it once it is publicly available. The way these mechanisms' function lacks sufficient accountability and transparency. The psychological aspect cannot be disregarded either. Your behavior changes when you are aware that you are being watched all the time. You begin acting differently because the system "expects" it to, not because you want to. It produces a steady, silent pressure. Not to be overlooked are the technological malfunctions. Biometrics can malfunction or crash like any other technology. When it happens, you may lose access to your personal phone, bank accounts, and buildings. Convenience soon becomes a major issue. The public's lack of trust is also getting worse. Without knowing how biometric systems operate or how their data is secured, people feel compelled to use them. More openness and education are desperately needed; else, mistrust and fear will only increase[22].

The Future of Biometrics: Innovation, Regulation, and Digital Identity Transformation

In reality, no one can truly predict what the future of biometrics will look like; we can only speculate on possible outcomes. However, looking at the history of this field, the future appears to be both promising and crucial, especially as people become increasingly connected to the internet and digital systems with each passing day. Governments are also becoming more technology-friendly, with some administrative offices now accessible only through fingerprint or iris recognition. Initially, biometrics was associated solely with fingerprints or facial geometry, but as the science has evolved, identification is now also possible through scent or handwriting. Each of these methods is becoming increasingly advanced and complex.

Currently, researchers focus their work primarily on identification through voice tone, behavioral analysis, facial emotion recognition, and even the patterns of veins in the hands or on the body, as well as the way a person moves. These

21 R. R. Sokal and F. J. Rohlf, *Biometry: The Principles and Practice of Statistics in Biological Research*, 1973, p. 228.
22 Ibid., p. 312.

complex, multi-layered biometric systems not only allow for effective authentication but also enable the prediction of user behavior, which can be applied in areas such as cybersecurity, medicine, elderly care, and marketing. In biometric science, a key advantage is that the same principles can be applied across fields like forensics, psychology, and even healthcare. That is why I personally believe biometrics should be a more widely taught and understood area of knowledge. Unfortunately, with every mention of evolution or development, the word challenge inevitably follows. When it comes to biometrics, this challenge is closely tied to privacy protection and data security. The lesson here goes beyond passwords, PINs, or logins – it involves personal identifiers that, once exposed, can be exploited by criminals, with no option to delete or reset them. This means that security measures must be significantly more sophisticated, and the legal regulations governing the storage, processing, and sharing of data must become both standardized and stricter. This will require cooperation between technology developers, governments, and organizations focused on personal data protection, who must find a balance between innovation and responsibility[23]. Decentralized systems are already emerging–based on blockchain or zero-knowledge proof architectures – that allow identity verification without revealing full biometric data. These approaches could become the new standard in the future. Biometrics are somewhat like a swing – they can both increase and decrease the sense of security. On one hand, in authoritarian states such as North Korea, China, or Iran, biometrics are used to excessively monitor citizens, creating fear among people that they are under constant government surveillance, almost like machines. On the other hand, in democratic countries, biometrics help combat cybercrime. Therefore, building public trust through education, clear legislation, and choice will be essential–users should have real control over what data is collected and for what purpose[24]. In the long term, biometrics may cease to be merely a method of authentication and instead become an integral part of our digital identity–enabling not only access to services but also fostering personalized interactions with technology that increasingly understands our needs, emotions, and habits.

Summary

Biometrics has become an increasingly common part of modern life, offering fast, efficient, and personalized ways to verify identity through unique physical and behavioral traits. Whether it's unlocking a phone, accessing a bank account, or passing through airport security, biometric systems are designed to make life easier and more secure. However, this convenience comes with significant

23 J. Gach, A. Tavares, *Fingerprinting as a Biometric Identification Tool: Methods and Applications in Modern Forensic Science*, *Security Forum*, 2024, No. 2.

24 D. Krishna, F. A. Talukdar, and R. Laskar, *Study on Biometric Authentication Systems, Challenges and Future Trends: a Review*, p. 12.

challenges. The key concern is that biometric data is permanent – unlike passwords, you can't change your fingerprints or face. If such data is stolen or misused, the consequences can be long-lasting. Issues like lack of user consent, poor data transparency, and potential misuse by governments or corporations make it clear that biometrics is not just a technical tool, but also a social and ethical issue. Surveillance and discrimination are also major risks. Not all biometric systems treat users equally, and some can reinforce social biases. Public spaces monitored by facial recognition may improve security, but they also raise serious privacy concerns. Without strong legal protections and public understanding, we risk creating systems that control rather than protect. For this reason, the future of biometrics must be built not only on technological progress but also on responsibility, fairness, and transparency.

Governments must enforce strict data regulations, companies must prioritize user privacy, and individuals must be aware of their rights. Biometrics has the potential to support a safer and smarter world – but only if we ensure it works for people, not against them. Its true success will depend on how well we balance innovation with human dignity and democratic values.

Bibliography

Faundez-Zanuy, M., Fierrez, J., Ferrer, M. A., Diaz, M., Tolosana, R., & Plamondon, R. (n.d.). Handwriting biometrics: Applications and future trends in e-security and e-health.

Gach, J., & Tavares, A. (2024). Fingerprinting as a biometric identification tool: Methods and applications in modern forensic science. Security Forum, (2).

Goc, M., & Moszczyński, J. (2007). Polish Society of Criminology. Warsaw.

Jain, A. K., Ross, A., & Nandakumar, K. (n.d.). Introduction to biometrics.

Kolano, W., & Tavares, A. (2022). The role of Poland in ensuring European security. Security Forum, 6(1), 21–34.

Krishna, D., Talukdar, F. A., & Laskar, R. (n.d.). Study on biometric authentication systems, challenges and future trends: a review.

Kulicki, M., Kwiatkowska-Wójcikiewicz, V., & Stępka, L. (2009). Forensic science: Selected issues of criminal and judicial investigative theory and practice. Toruń.

National Research Council. (n.d.). Biometric recognition: Challenges and opportunities.

Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (n.d.). Secure biometrics: Concepts, authentication architectures and challenges.

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (n.d.). Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence. Available online: https://ieeexplore.ieee.org/document/879796 [Accessed: February 18, 2025].

Służewska, A. (2007). Methods of visualizing fingerprint traces on the metal surface of cartridge cases – a brief review. *Problemy Kryminalistyki*, (257). Warsaw.

Sokal, R. R., & Rohlf, F. J. (1973). Biometry: The principles and practice of statistics in biological research.

Sokal, R. R., & Rohlf, F. J. (n.d.). Introduction to biostatistics (2nd ed.).

Turk, M. A., & Pentland, A. P. (1991). Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1), 71–86. Available online: https://watermark.silverchair.com/jocn.1991.3.1.71.pdf [Accessed: February 18, 2025].

Wayman, J., Jain, A. K., Maltoni, D., & Maio, D. (n.d.). Biometric systems: Technology, design and performance evaluation.

About the Authors

Dipankar Haldar, PhD, Associate Professor of Serampore College University, India.

Justyna Gach, Vice-Chair of the Main Board of the International Scientific Association for Security "Save the World". Her academic interests focus on issues related to security systems, criminal forensics, and the role of technology in contemporary identification processes.