AI and Biometrics: A New Era of Security Authentication

ARYA BRIJITH

IIPP Research Intern,

Asia University, Taiwan

(e-mail: arya.brijithk@gmail.com).

ABSTRACT The combination of AI with biometrics represents a substantial advancement in safe authentication, influencing several businesses. This synergy is used in many different fields, including automated face recognition, fraud detection, healthcare, airport security, the military, and the auto industry. However, there are significant moral and legal issues that go along with these commitments. Strong systems for informed consent and data protection are required due to the significant privacy issues. For a responsible deployment, it is also essential to address concerns of accuracy, prejudice, and discrimination. This article clarifies the use of AI in the field of security by exploring its applications, how ANN is integrated and the problems it brings followed by the future developments in the field.

KEYWORDS Artificial Intelligence (AI), biometrics, challenges, security.

I. INTRODUCTION

Biometrics are distinct bodily traits that can be recognized automatically, like fingerprints. It can be defined as a pattern recognition system, that can find uniquely identifying features among different individuals [4]. The Industrial Revolution's rapid urbanization boosted the demand for official identification procedures, which fueled a boom in the field of biometrics. Artificial intelligence (AI) is used in several biometric applications nowadays. *AI has been of paramount importance for increasing the performance of biometric systems to levels unseen with previous technology.*[1] Data is the greatest asset to almost every industry, therefore, AI tools use many datasets. The machine learns from past data and can make decisions. One main application is biometrics, where the machine can store information such as finger print, facial pattern etc. of the user and can apply the same for further investigations or applications. AI based biometric systems have numerous applications ranging from face detection for security purposes to healthcare industry. Though we adopt AI into various resources, we should realize that it can have some serious effect on not just the product but also its environment. We shall later discuss the issues and challenges faced by using AI in biometrics in this article.

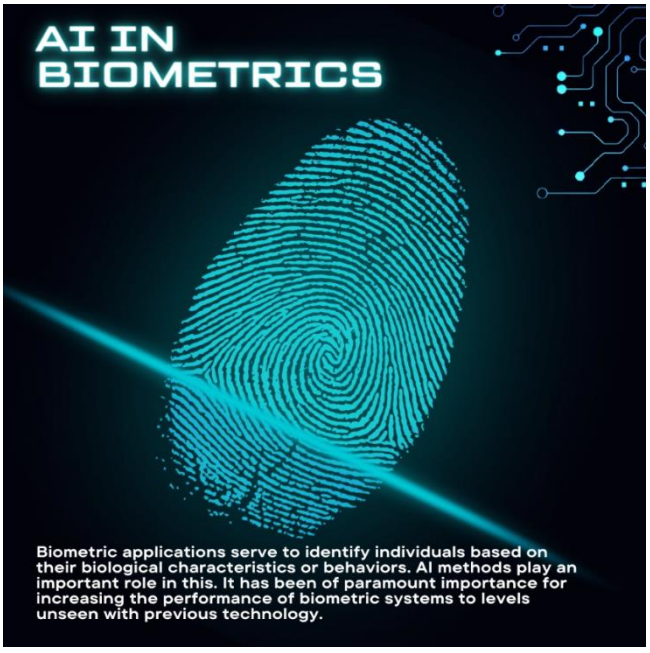

Figure 1: AI in biometrics

II. ABOUT BIOMETRICS

A technique known as biometrics measures and statistically analyses each person's distinctive physical and behavioral traits. The main uses of it are for identification and authentication.

Compared to conventional ways like passwords or PINs, biometrics offer a better position of security since they are specific to each individual and challenging to fabricate. Authentication is generally quick and more practical. Users no longer need to carry actual keys or cards or remember and maintain passwords. Also, it might help show that a certain person carried out a particular activity, lowering the probability of denial or rejection in the field of crime.

AI is used to extract distinctive characteristics from biometric data and compare them to templates that have been saved in a database. Deep learning techniques are very useful for this. By learning from big datasets and optimizing the matching process, algorithms can increase the accuracy of biometric systems which in turn helps to identify liveness in biometric authentication to thwart spoofing efforts (for example, using a photo for face recognition).
AI aids in the analysis and recognition of patterns in behavioral biometrics, such as mouse movement or keyboard dynamics. Better performance is made possible by the ability of AI-powered biometric systems to adapt and advance over time as they learn from fresh data.

III. HOW DOES ANN HELP?

Artificial neural networks (ANNs) are computer programs with biological influences that mimic how the human brain processes information. ANNs learn (or are taught) by experience rather than through programming, and they learn by identifying patterns and correlations in data.
It has revolutionized the way we think about biometrics. They act as vital detectives, searching through biometric information to find the most crucial information. As an example, ANNs can precisely identify key face traits in facial recognition, enabling very accurate identification. This is a game-changer, especially for jobs like point recognition where it is critical to correctly identify those complex crest patterns.
But ANNs go further than that. They excel at deciphering intricate relationships in biometric data. Consider attempting to determine how the way you type connects to who you are. The fact that there is not a straightforward relationship is where ANNs excel. They excel in literacy and making subtle connections that might not seem objectionable at first.
Further, ANNs are a great aid in processing large amounts of data. They can filter through everything and decide which corridor is most crucial, speeding up the process considerably. Think of it like simplifying a large library: ANNs enable us to locate the appropriate books—or in this case, data—more quickly.
Security is a major problem in biometrics, therefore ANNs are essential. They are taught to recognize real people's facial expressions. Thus, people can identify you in person rather than only in a print or movie. It is comparable to having a redundant subcaste of defense against fictitious efforts to fool the system.

They resemble the wizards of the biometric technology world as it puts in many hours behind the scenes to make sure that everything runs well. They play a significant role in extracting minute information and figuring out complex linkages in the data. They seem to have a sixth instinct for spotting possible issues or dishonest tactics. The precision and dependability of biometric systems are supported by ANNs, making them a crucial element in this cutting-edge sector.

IV. APPLICATIONS

AI in biometrics has a vast application. Some of those are as follows:

- **Automated Facial Recognition Systems:** Automated facial recognition systems are broadly comprised of four stages [2]-

1. Face detection - Uses cutting-edge algorithms to recognize human faces, repeatedly from CCTV images.
2. Face analysis -In this stage, extensive data collection takes place through in-depth analysis of facial characteristics, including 2- D and 3- D images.
3. Image-to-data conversion – In this stage, visual face data is converted into a digital format suitable for analysis using sophisticated mathematical formulae.
4. Comparison and matching- Lastly, Statistical analysis is used to compare the converted face data to a large database and discover implicit matches for fresh examination.

For determining approximative biometric matching, statistics has always been crucial. When a faceprint is compared against a large database of other faceprints, statistics are used to glean which “near matches” might be worth considering for further investigation and scrutiny.[3]

- **Fraud Detection and criminal investigation:** When there is no direct eyewitness testimony, digital facial photographs are rarely utilized alone. *However, in the absence of eyewitness accounts,*

CCTV footage may well be the only available data to bring a criminal to justice, especially in the context of a heinous crime where the use of automated biometric recognition is deemed proportional to the crime committed.[1] We know that fingerprint is unique for every human being. Even identical twins do not have similar finger prints. Thus, obtaining partial fingerprints from a crime scene is a crucial forensic science methodology. Large businesses were victims of violations of safety, which affected-mail addresses, private data and watchwords. On several occasions, cyber safety specialists have repeated that watchwords are largely susceptible to assaults, private data compromising, loan card data and social security figures. All this is why biometric logins contribute to cyber safety in a salutary way.[6]

- **Healthcare industry:** When people usually think about AI based face recognition and authentication, they assume it is only used by the police for investigations. Little do they know that AI in biometrics has a wider application. One such application is healthcare. Surprised? Do not be! Several tools have been developed to detect cancer cells and to retrieve personal information of the patient by use of their finger print. This not only helps with further information but can also help display the past data of the patient such as- if he/she is diabetic, have any genetic disorder, etc.
- **Airport Security:** We can all relate to how chaotic airport security can get. People gushing through the baggage lines, the security check and the boarding area is a common sight. The best way to reduce the chaos is by using AI tools for the security check. AI devices would already have your face registered (during the process of displaying your ID proof). Based on this, the passengers can bypass to the boarding area.
- **Military:** Every military in the world has a section dedicated to data and information security; in this area, biometrics find use in helping to protect trade secrets, thwart imposters, and facilitate information retrieval when necessary.[6] Military AI capabilities are being developed by several countries, and these capabilities may include employing AI to support independent systems. AI capabilities used by the service must be held responsible, especially when they are applied during military operations under the authority of a responsible mortal chain of command and control. A moral approach to the service's deployment of AI should precisely weigh the advantages and disadvantages while minimizing bias and accidents.
- **Automobile industry:** Cars with biometric capabilities are still being introduced in a variety of ways, and related new technologies are being developed. Autonomous cars may potentially offer a chance for forensic biometrics. Both the Mazda CX-60 SUV and the Mercedes-Benz C- Class sedan in India for 2022 were introduced with biometrics to access driver biographies that modify their seat operation, as well as a gently wider perpetration from Genesis. According to The India publish, the Mercedes C-Class in India would be equipped with a fingerprint scanner to provide access to a driver profile.

V. TABLES AND FIGURE

	TYPES	DESCRIPTION
	IRIS/RETINA	Analyses the distinctive patterns in the iris or retina of the eye.
	FINGERPRINT	Analyses the ridge and valley patterns on a person's fingertip to recognize their fingerprint.
	FACE RECOGNITION	Identifies people by examining their distinctive facial traits.
	VOICE RECOGNITION	Examines speech patterns, pitch, tone, and other vocal characteristics.
	BEHAVIOUR	Analyses distinctive behavioural patterns

Table 1: Types of biometrics

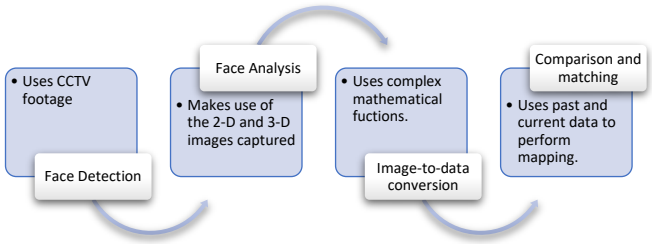

Table 2: **Stages of facial recognition systems**

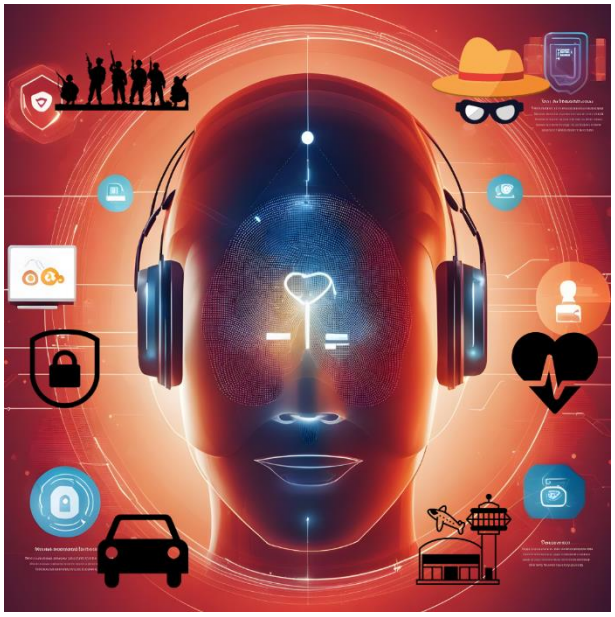

Figure 2: **Applications of AI**

VI. ISSUES AND CHALLENGES

- Privacy issue is one of the main concerns of AI biometrics. Biometrics and facial recognition use private, sensitive information that might disclose your identity, whereabouts, state of health, behaviour, and preferences. These data are open to theft, exploitation, and hacking by bad actors including rogue governments, hackers, and cybercriminals.
- Large databases of photographs, fingerprints, iris scans, speech patterns, and other biometric traits are needed for facial recognition and biometrics. In many cases, these data are gathered without your express awareness, consent, or control. The acquisition and consent of personal data is one of the primary dangers of utilizing AI for face recognition and biometrics. For instance, you could be recorded by security cameras, social networking sites, or internet businesses that employ biometrics and face recognition for authentication or analysis. This begs the question of whether you have the right to access, delete, or object to the processing of your data by third parties, as well as how it is stored, shared, and used by them.
- Biometric system integration with AI has advanced the field significantly, but it also comes with several difficulties. The topics of ethics and privacy are among the top issues. People naturally have concerns about the gathering and storage of biometric data since it is essentially private and sensitive. This data might potentially be misused or accessed by unauthorized parties, which is a real concern that requires cautious consideration. In this quickly developing industry, finding the ideal balance between technical advancement, and protecting individual privacy continues to be a major concern.
- The vulnerability to spoofing and presentation attacks in biometric authentication raises serious questions right away. With the development of technology, it is now possible to manufacture fake biometric data with terrifying precision. This includes deepfake films or even high-quality fingerprint copies that might fool biometric systems. To distinguish between genuine persons and fraudulent attempts, it becomes essential to deploy powerful AI-driven liveness detection tools. It resembles a dynamic arms race against spoofing techniques and necessitates ongoing study and invention.
- Imposters can completely control the addressed accounts or IoT bias, performing in ruinous damages consequentially, If the authentication information is stolen or compromised. For knowledge- grounded authentication, fakers can capture inputs by shoulder surfing and recording attacks, thermal attacks, and smirch attacks. For facial recognition, an adversary could conquer facial discovery through licit druggies' facial

prints. The point can be conquered by smirch attack and forged by deep literacy styles. The automated speaker verification grounded on the characteristics of voices is subject to renewal attacks.[7]

- Anti-discrimination regulations must be followed by biometric AI systems to help them from unfairly harming particular ethnical or ethnical groups.
- Another challenge that is yet to be overcome is that Twins can beat facial recognition.[6]
- For liberal democracies, there are several urgent ethical issues raised by the growing use of biometric facial recognition that must be considered. Particularly, the possible conflicts between security, on the one hand, and individual privacy, autonomy, and democratic accountability, on the other hand, are of concern. As in all polities, including many authoritarian ones, security and community safety are basic ideals in liberal democracies. Liberal democracies are dedicated to democracy, which entails democratic responsibility, as well as to the right to personal privacy and autonomy.[5]

VII. FUTURE DEVELOPMENTS

The combination of artificial intelligence and biometrics is ready to change security and authentication frameworks as we stand on the cusp of a new era of technology. Several significant changes are expected to impact this dynamic field's development in the future.

The multi-modal biometrics field is one of the most promising. This method incorporates a diverse range of biometric identifiers, including voice and iris recognition in addition to face and point recognition. Multi-modal biometrics improves security and delicacy by merging these several data inputs, building a strong authentication system that can fend off complex assaults. This convergence is a major step toward trustworthy identification methods that do not depend on just one type of verification.

Another significant development that is on the horizon is the development of uninterrupted authentication. Nonstop authentication uses continuous monitoring in place of the traditional one-time authentication approach to confirm drug users based on their behavioral characteristics. A faultless and mainly safe stoner experience is provided through real-time anatomization of keystroke mechanics, gait analysis, and other distinctive behaviors. This strategy not only improves security but also guarantees friendly interaction between people and the technologies they engage with.

Neural networks and deep learning algorithms are expected to be crucial in improving biometric recognition systems. These advanced models can adapt to and learn from large datasets, which improves performance in taxing scripts.

Ethics and bias reduction will be paramount as we set the course for the use of AI to biometrics. Sweats will be put into establishing trust and inclusion by enhancing justice, transparency, and equity in biometric algorithms. The application of AI to biometrics opens up a world of endless possibility and has the potential to revolutionize how we think about security and identification in the digital era. Utilizing the full potential of this disruptive technology will depend on striking a balance between innovation and appropriate use.

VIII CONCLUSION

Integrating biometric systems with AI techniques is one of several exciting research areas now being pursued. The combination of AI with biometrics represents a significant advancement in security authentication, having an impact across several sectors. Among the diligence serving from this confluence are automated face recognition, fraud discovery, healthcare, field security, military operations, and the machine assiduity. still, these developments raise important ethical and legal questions. It is pivotal to guard sequestration, therefore strong programs for informed concurrence and data protection are needed. A conscientious deployment also requires addressing enterprises like delicacy, prejudice, and demarcation. Collaboration amongst stakeholders is essential to establishing clear rules and regulations as the geography continues to change. This guarantees that the objectification of AI in biometrics preserves abecedarian ethical and legal morals while also enhancing security. The responsible embracement of this technology is crucial to unleashing its full eventuality while conserving individual rights and societal values.

References

[1] C. Berghoff, M. Neu and A. von Twickel, "The Interplay of AI and Biometrics: Challenges and Opportunities," in Computer, vol. 54, no. 9, pp. 80-85, Sept. 2021, doi: 10.1109/MC.2021.3084656.
[2] What Is Facial Recognition—Definition and Explanation, Feb. 2022, [online] Available: http://Kaspersky.com.
[3] R. Jafri and H. R. Arabnia, "A survey of face recognition techniques", *J. Inf. Process. Syst.*, vol. 5, no. 2, pp. 41-68.
[4] A. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14(1), 420 (2004)
[5] Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, 1-9.
[6] Iyer, A. P., Karthikeyan, J., Khan, R. H., & Binu, P. M. (2020). An analysis of artificial intelligence in biometrics—the next level of secu-rity. *J Crit Rev*, *7*(1), 571-576.
[7] Y. Liang, S. Samtani, B. Guo and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective," in *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128-9143, Sept. 2020, doi: 10.1109/JIOT.2020.3004077.
[8] De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021). Opportunities and challenges of using biometrics for business: Developing a research agenda. *Journal of Business Research*, *136*, 52-62.
[9] Agatonovic-Kustrin, S., & Beresford, R. (2000). Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. *Journal of pharmaceutical and biomedical analysis*, *22*(5), 717-727.

[10]Plageras, A. P., et al (2018). Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. Future Generation Computer Systems, 82, 349-357.
[11]Memos, V. A., et al. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. Future Generation Computer Systems, 83, 619-628.
[12]Yu, C., et al. (2018). Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools and Applications, 77(4), 4585-4608.