AN INTERNATIONAL CONFERENCE ON
Humanities, Science & Research
At Asha Girls College, Panihar chack, Hisar (Haryana)
27-28th January, 2024

State-of-the-Art Techniques in AI for Biometric Recognition Systems

Dr. Amitabh Amaresh Halder, Assistant Professor , SSESA'S SCIENCE COLLEGE, Congress Nagar Nagpur, RTM Nagpur University, Nagpur, Email: amitabhhalder@gmail.com

Abstract

Biometric recognition systems have witnessed significant advancements with the integration of artificial intelligence (AI) techniques in recent years. This paper presents a comprehensive review of the state-of-the-art AI approaches employed in biometric recognition, focusing on their applications, methodologies, and performance evaluations. The study explores key AI technologies such as deep learning, convolutional neural networks (CNNs), and recurrent neural networks (RNNs), highlighting their effectiveness in enhancing biometric modalities including facial recognition, fingerprint identification, iris scanning, voice authentication, and gait analysis. Furthermore, the paper discusses challenges such as data privacy, security vulnerabilities, and ethical considerations associated with AI-powered biometric systems. Through a systematic analysis of current research trends, datasets, and evaluation metrics, this study aims to provide insights into the future directions and potential innovations in AI-driven biometric recognition systems, emphasizing their role in advancing security, accessibility, and user authentication technologies.

Keywords – Facial recognition, Fingerprint identification, Iris scanning, Voice authentication, Gait analysis

Introduction

In recent years, biometric recognition systems have become integral to a wide array of applications, from securing personal devices to enhancing border control and facilitating seamless user authentication. These systems leverage unique biological or behavioral characteristics of individuals, such as fingerprints, facial features, iris patterns, voiceprints, and gait dynamics, to establish identity with high accuracy and reliability. The integration of artificial intelligence (AI) techniques, particularly deep learning methodologies, has revolutionized the field by significantly enhancing the performance and scalability of biometric modalities.

AI-based approaches, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs), have enabled biometric systems to extract intricate features from raw data, thereby improving robustness against variations in environmental conditions and enhancing resistance to spoofing attacks. This paper provides a comprehensive review of the state-of-the-art AI techniques applied in biometric recognition systems. It explores their evolution, applications across different biometric modalities, methodologies employed, and performance evaluations.

Furthermore, the paper discusses the challenges and opportunities associated with AI-driven biometric systems, including issues related to data privacy, security vulnerabilities, and ethical considerations. By analyzing current research trends, datasets used for training and evaluation, and benchmarking metrics, this study aims to elucidate the advancements made and future directions in the field of AI for biometric recognition. Ultimately, understanding these advancements is crucial for harnessing the full potential of biometric technologies in enhancing security, accessibility, and user authentication in various domains.

Literature review

In order to safeguard user material, authentication methods are widely used in online services and mobile devices. In order to better manage information security, a number of tools and strategies have been created. Nonetheless, biometric technologies have come a long way in supporting some aspects of information security. Biometric authentication has been the subject of much research in recent years (Jain, Nandakumar & Ross, 2016; Jain, Ross & Prabhakar,

2004). Since biometric systems are not readily exploited, biometric user authentication is becoming more prevalent over time. This is due to the fact that in order for systems to be compromised, the persons attempting to do so must possess the same physiological factors as the real users. As a result, the systems are now more secure and less susceptible to attacks.

It needs no introduction that biometrics is a cutting-edge and abundantly fertile area of study. Biometric systems have been the subject of several surveys. A recent example of a survey that narrowly targets a certain modality or setting is the work of Connor and Ross (2018), who examined a gait-based biometric identification system. A number of gait recognition modalities and their characteristics have been examined.

In their comprehensive review of periocular biometrics, Kumari and Seeja (2019) draw on a wide range of current feature extraction techniques and matching systems. Additionally, the research highlights the many uses of periocular biometrics and their significance. Dargan and Kumar (2020) have conducted an extensive literature review on biometric recognition systems, including topics such as feature extraction techniques, classifiers, and datasets for both one- and multi-modal systems. Their primary goal is to educate the researcher on what to look for in a biometric system to make it more secure. Using a variety of modalities, Sundararajan and Woodard (2018) examined deep learning's application to biometric identification. Still, they draw the conclusion that deep learning methods have mostly been tested on facial biometrics and voice recognition.

In their study, Dinca and Hancke (2017) highlighted how multibiometric systems might help fulfil the growing need for authentication security. Two crucial areas of biometric systems—fusion techniques and security—are primarily addressed by their work. In their 2018 study, Rui and Yan provide a comprehensive overview of authentication methods that are both safe and privacy protective. The authors have primarily focused on two areas of biometric systems: liveness detection and privacy protection. Wearable biometrics is an emerging field that will need substantial investment from academics, adding to the growing body of work in the field of wearable technology and the Internet of Things.

A fascinating review by Sundararajan, Sarwat, and Pons (2019) compares the salient features of various modalities and draws attention to serious assaults on both conventional and wearable biometric systems within this framework. Having said that, the review covers the majority of biometric modalities, including physiological and behavioural features, and the manuscript's scope is rather wide. A more targeted and comprehensive evaluation of hand-based multibiometric systems is also lacking as the quantitative analysis is not included in several publications.

Big Data, machine learning, and robotics are some of the latest artificial intelligence technologies that have found use in healthcare risk detection, monitoring, and assessment (Hossen and Armoker, 2020; Dharani & Krishnan, 2021; Duan et al., 2022). The healthcare industry is highly dependent on medical data and analytics to improve processes and make medical service management easier. There has been an exponential growth in the quantity and variety of medical data collected in the last few years. People are increasingly using monitoring devices, such as health tracking apps and electronic health records (EHRs), in everyday situations when medical attention is not necessary. This data comes from a variety of sources, including medical imaging, research, and patients (Antoniou et al., 2018; Liu et al., 2020; Xie et al., 2020). When used to this setting, AI can collect data, analyse it, do dynamic analyses, and provide actionable medical intervention outcomes (Comito et al., 2020). In most cases, data storage and processing power are used to assist machine learning algorithms that carry out this role (Charan et al., 2018; Woo et al., 2021). By routinely observing medical data, for instance, patient behaviour patterns could be possible to build dependable forecasts. Therefore, AI has the potential to provide recommendations for medical interventions, therapeutic insights, and strategies to improve health outcomes across the board, including prescription

and usage of medications, early detection of illness, and treatment of existing conditions. Modern medical facilities are investigating the potential of artificial intelligence (AI) to reduce operational costs (Sqalli and Al-Thani, 2019; Zhou et al., 2020) and increase practice accuracy (Zhou et al., 2020; Mary et al., 2020). Artificial intelligence (AI) helps doctors and patients make better treatment choices by providing comprehensive information on available alternatives (Deng et al., 2019).

The integration of healthcare environments with an AI intervention supported only by machine learning is complex, and while this might lead to optimistic visions of AI's future in terms of its potential, it also means that AI will likely bring its fair share of problems. Problems with patient privacy that restrict data access, harm to patients from system errors, and the ethical, legal, and medical difficulties of using AI to make decisions about people's lives and health issues are some of the most prominent new risks and challenges (Aljaaf et al., 2015; Srivastava and Rossi, 2019; Madanan et al., 2021; Dwivedi et al., 2021; Liu et al., 2020; Shaban-Nejad et al., 2021).

Despite the problems with AI, it has many positive uses, one of the most significant being its ability to aid in healthcare preventive care, which helps people of all ages get and stay healthy. In the case of preventive health conditions like type 2 diabetes and high blood pressure, for instance, patients have been empowered to make evidence-based choices via the use of apps (Antoniou et al., 2018; Jaiman and Urovi, 2020; Samuel et al., 2022). According to Stamford et al. (2016), Siddiqui et al. (2018), and Kumar and Suresh (2019), a plethora of AI applications are necessary for the early detection and assessment of health information. Numerous fields make use of these AI applications for the purpose of making accurate, quick, and trustworthy diagnoses (Ribbens et al., 2019; Sasubilli et al., 2020; Jahan and Tripathi, 2021). In its most basic form, AI uses Big Data to do extensive comparison analysis, comparing a patient's information with digital photos and data from massive databases that include information about other patients in similar and comparable contexts (Charan et al., 2018; Somasundaram et al., 2020).

Objectives of the study

- To conduct a comprehensive review of the latest AI techniques, including deep learning methodologies such as CNNs, RNNs, and GANs, applied in biometric recognition systems.
- To explore the applications of AI-driven biometric recognition across various modalities such as facial recognition, fingerprint identification, iris scanning, voice authentication, and gait analysis.
- To analyze the methodologies and innovations in AI that have significantly contributed to improving the accuracy, robustness, and scalability of biometric systems.

Research methodology

This study employs a systematic review approach to investigate state-of-the-art techniques in artificial intelligence (AI) for biometric recognition systems. The research methodology involves several key steps. First, a comprehensive search strategy is implemented across relevant academic databases, including IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar, to identify peer-reviewed articles, conference papers, and technical reports published between 2010 and 2023. Keywords such as "AI," "deep learning," "biometric recognition," "facial recognition," "fingerprint identification," "iris scanning," "voice authentication," and "gait analysis" are used to ensure inclusivity of relevant literature.

Second, the identified studies are screened based on predefined inclusion criteria, which encompass relevance to AI techniques applied in biometric systems, clarity of methodology description, and use of empirical evaluations. Articles that meet the inclusion criteria undergo detailed examination for data extraction, focusing on AI methodologies employed, biometric

modalities studied, performance metrics reported, datasets utilized, and any comparative analyses with traditional approaches.

Discussion

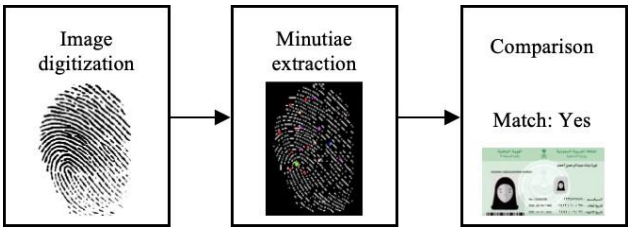

Figure1. Fingerprint authentication process: (1) image digitization, (2) minutiae extraction, and (3) comparison to the templates

The fingerprint authentication process involves several critical steps that collectively ensure reliable and secure user identification.

Image Digitization (Step 1): The process begins with the acquisition of a fingerprint image using a digital sensor. This image is then digitized into a high-resolution grayscale or binary format, capturing detailed ridge patterns and minutiae points essential for subsequent analysis.

Minutiae Extraction (Step 2): In this step, specialized algorithms are applied to extract minutiae points from the digitized fingerprint image. Minutiae points are key features such as ridge endings and bifurcations, which are unique to each fingerprint and serve as distinctive markers for identification. These algorithms use image processing techniques, including ridge thinning, ridge orientation estimation, and minutiae detection, to accurately locate and record these points.

Comparison to Templates (Step 3): Once minutiae extraction is complete, the extracted minutiae points are compared against stored templates in a database. Templates are pre-registered representations of minutiae configurations derived from previously enrolled fingerprints. During comparison, algorithms evaluate the similarity between the extracted minutiae points and the templates using mathematical algorithms such as Euclidean distance or correlation-based methods. A threshold is applied to determine if the fingerprint under consideration matches any of the stored templates.

System Reliability and Security: The effectiveness of the fingerprint authentication process relies heavily on the accuracy of minutiae extraction and the robustness of template matching algorithms. Advancements in AI and machine learning have enhanced these processes by improving feature extraction techniques and optimizing matching algorithms for speed and accuracy. Additionally, ensuring the security of stored templates and protecting against spoofing attacks (e.g., using fake fingerprints) remains a critical area of research and development in biometric authentication systems.

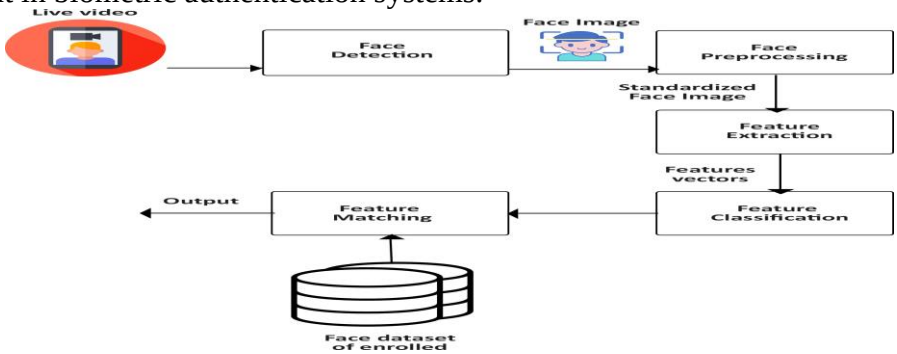

Figure 2. facial recognition structural steps: (1) facial detection, (2) feature extraction, and (3) facial recognition.

Facial recognition technology has evolved significantly, comprising distinct structural steps that enable accurate identification and verification of individuals:

Facial Detection (Step 1): The process begins with facial detection, where algorithms scan an image or video frame to locate and isolate human faces. This step involves techniques such as Viola-Jones method, Haar cascade classifiers, or deep learning-based approaches (e.g., using CNNs) to detect facial regions accurately amidst varying backgrounds, lighting conditions, and facial orientations.

Feature Extraction (Step 2): Once faces are detected, feature extraction techniques are applied to capture distinctive facial characteristics. These features include spatial arrangements of eyes, nose, mouth, and other facial landmarks, which are critical for generating a unique facial signature. Methods like Principal Component Analysis (PCA), Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), or deep learning architectures (like VGG, ResNet) are utilized to extract and represent these features robustly.

Facial Recognition (Step 3): In the final step, the extracted facial features are compared against a database of known individuals or templates. This comparison involves measuring the similarity between the extracted features and the stored templates using metrics such as Euclidean distance, cosine similarity, or neural network-based similarity scores. Advanced techniques may employ ensemble learning, fusion strategies, or deep metric learning to enhance recognition accuracy and mitigate challenges like pose variation, occlusions, and aging effects.

Technological Advancements: Recent advancements in deep learning, particularly with the advent of convolutional neural networks (CNNs) and generative adversarial networks (GANs), have significantly improved facial recognition accuracy and robustness. These techniques excel in handling complex data distributions and learning discriminative features directly from raw pixels, thereby overcoming limitations of traditional feature-based methods.

Conclusion

This study has explored the current landscape of artificial intelligence (AI) techniques applied in biometric recognition systems, emphasizing their evolution, applications, methodologies, and performance evaluations. Through a systematic review of literature and analysis of research trends, several key findings have emerged:

Firstly, AI, particularly deep learning methodologies such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs), has revolutionized biometric recognition by significantly enhancing accuracy, robustness, and scalability across various modalities including facial recognition, fingerprint identification, iris scanning, voice authentication, and gait analysis.

Secondly, the integration of AI in biometric systems has introduced new challenges, including concerns related to data privacy, security vulnerabilities, and ethical considerations. Addressing these challenges is crucial for ensuring the responsible development and deployment of AI-driven biometric technologies.

Thirdly, advancements in AI have facilitated the development of more sophisticated algorithms for feature extraction, pattern recognition, and similarity matching, thereby improving the overall performance of biometric systems in real-world scenarios.

Moreover, the study has identified gaps in current research, such as the need for standardized benchmark datasets, improved generalization capabilities across diverse demographics, and enhanced resistance against spoofing attacks.

In conclusion, while AI has significantly advanced biometric recognition systems, future research should focus on addressing the identified challenges and exploring novel AI techniques to further improve accuracy, security, and usability. By fostering interdisciplinary collaborations and adopting ethical guidelines, AI-driven biometric technologies can continue

to evolve, contributing to enhanced security measures, seamless user authentication, and broader societal applications.

References

- Otti, C. (2016). Comparison of biometric identification methods. In 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 339-344). IEEE.
- Sumalatha, A., & Rao, A. B. (2016). Novel method of system identification. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 2323-2328). IEEE.
- Ortega, M., Penedo, M. G., Rouco, J., Barreira, N., & Carreira, M. J. (2009). Retinal verification using a feature points-based biometric pattern. EURASIP Journal on Advances in Signal Processing, 2009, 1-13.
- Byron, C. D., Kiefer, A. M., Thomas, J., Patel, S., Jenkins, A., Fratino, A. L., & Anderson, T. (2021). The authentication and repatriation of a ceremonial tsantsa to its country of origin (Ecuador). Heritage Science, 9(1), 1-13.
- Borra, S. R., Reddy, G. J., & Reddy, E. S. (2016). A broad survey on fingerprint recognition systems. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1428-1434). IEEE.
- Peralta, D., Galar, M., Triguero, I., Paternain, D., García, S., Barrenechea, E., ... Herrera, F. (2015). A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. Information Sciences, 315, 67-87.
- Sharma, M. (2014). Fingerprint biometric system: A survey. International Journal of Computer Science & Engineering Technology (IJCSET), 5(7), 743-747.
- Delac, K., & Grgic, M. (2004). A survey of biometric recognition methods. In Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine (pp. 184-193). IEEE.
- Sugandi, B., Dewita, I., & Hudjajanto, R. P. (2019). Face recognition based on PCA and neural network. In 2019 2nd International Conference on Applied Engineering (ICAE) (pp. 1-5). IEEE.
- Anusha, P., Prasad, K. L., Kumar, G. R., Lydia, E. L., & Parvathy, V. S. (2020). Facial detection implementation using principal component analysis (PCA). Journal of Critical Reviews, 7(10), 1863-1872.