IJC
International Journal of Computer (IJC)
Peer-Reviewed International Journal
ISSN: 2307-4523
https://ijcjournal.org

Biometrics Solutions for Authentication Disability People: A survey

Khalid Mohammed Osman Saeed[a,*], Bashier Suliman Elbashier Ahmed[b]

a: Faculty of Computer Science and Information Technology, Omdurman Islamic University, Sudan
b: Institute for Research and Studies of the Islamic World, Omdurman Islamic University, Sudan
** Corresponding author: khalidmohosman@gmail.com | E-mail: bashiersuliman@gmail.com*

Accepted: 22 September 2026 | Published: 22 October 2026

Abstract

Biometric authentication systems have become an essential component of modern security applications due to their ability to provide reliable and user-friendly identity verification. Traditional authentication methods such as passwords and Personal Identification Numbers (PINs) are often difficult for people with disabilities to use effectively. As a result, researchers have explored biometric technologies that provide accessible, secure, and convenient authentication solutions for individuals with visual, hearing, speech, physical, and hand disabilities. This survey paper reviews various biometric authentication methods designed for people with disabilities, including iris recognition, sclera recognition, finger vein recognition, hand vein recognition, electrocardiogram (ECG), palmprint recognition, facial thermogram, retina scanning, and voice recognition. The paper discusses the strengths, limitations, security challenges, and usability considerations of these methods. Furthermore, the survey highlights current research gaps and future directions for developing inclusive and multimodal biometric systems that can improve accessibility and security for disabled users.

Keywords: Biometrics; Disability; Blind; deaf; Dumb; Iris; Retina; Palmprint; Facialthermogram

1. Introduction

Authentication systems are widely used in banking, healthcare, education, smart devices, and access control applications. Conventional authentication methods such as passwords, Personal Identification Numbers (PINs), and smart cards may present significant difficulties for people with disabilities. For example, visually impaired individuals may struggle with text-based authentication interfaces, while people with hand disabilities may face challenges when using fingerprint scanners or keyboards. Biometric authentication offers an effective alternative because it uses unique biological or behavioral characteristics to verify identity. Biometrics can improve both usability and security by eliminating the need to remember passwords or physically interact with complex interfaces.

People with disabilities require authentication systems that are accurate, accessible, reliable, and easy to use. Researchers have proposed several biometric approaches tailored to different disability categories. This survey paper explores these biometric methods, compares their advantages and disadvantages, and discusses the future of inclusive authentication systems.

The objectives of this survey are:

• To review biometric authentication methods for people with disabilities.

• To analyze the suitability of biometric techniques for different disability categories.

• To discuss current challenges and security concerns.

• To identify future research directions for accessible biometric systems for disabled people.

1.1. Overview of Biometrics

In this section biometrics, biometric authentication and biometrics identification will be defined.

The definition of biometrics [1] are the biological or physiological characteristics (fingerprints, facial structures, iris or retinal patterns, voice recognition, gait, etc.) measured and assessed for either identification or verification of an individual through comparison with a database of previously collected samples.

Biometric traits [2] are divided into two criteria, namely physiological biometrics and behavioral biometrics.

The physiological model is identifying by the shape of the body like a fingerprint, face recognition, iris recognition, hand geometry, palm print, and retina recognition. In the second model, behavioral biometric is the body that determines the behavior of the body. All these characteristics are keystroke dynamics, voice recognition, signature verification, and gait.

Another important concept in the biometrics field is biometric authentication which means a system that provides a trusted independent authentication and confirmation of the identity of parties individually. It is also a technical term that refers to metrics related to human's body characteristics and authentication implement used in computer science [2].

Biometric identification means an automated process of comparing a unique biometric parameter of a person with the entire database of available data, as a result of which a coincidence or difference between them is established.

1.2. Uses of Biometrics

There are three methods using for authentication users: knowledge-based (something a user knows), possession-based (something a user has), and biometric-based (something a user is). The first two approaches have been widely adopted in most information technology (IT) systems; however, they face many well-known challenges. The third approach, biometric-based authentication, which uses physiological and behavioural characteristics of a user, has gained popularity as a reliable solution [3].

One of the most important uses of biometrics is to facilitate digital identity for service delivery, but this use rises significantly with cash and voucher assistance (CVA). Identification by biometrics is typically viewed as more invasive than other means of identification, such as personal details like names and addresses, because of their immutability. By contrast, biometrics has also been promoted as a way to prevent identity theft because it is tied to a unique identifier [1].

Biometrics [4] enables diverse application scenarios which are either difficult or infeasible using more traditional methods, e.g. continuous authentication, forensics, and surveillance.

Biometric technologies and applications have come to play an essential role in society, e.g., for identity management, surveillance, access control, social and welfare management, and automatic border control, with these applications are being used either by billions of people.

Personal, commercial, and governmental identity management systems increasingly rely on biometric technologies, which enable reliable recognition of individuals based on highly distinctive characteristics of human beings, e.g. face or fingerprints. Applications ranging from personal device

access, border control, forensic investigations and law enforcement, national identification (ID) systems, and electors' registration benefit from the use of biometrics [5].

Authentication system [6] became a significant task for both of access control and securing user's private data. Human biometric characteristics such as voice, finger, iris scanning, face, signature and other features provide a dependable security level for both of the personal and the public use. Many biometric authentication systems have been approached for long time. Due to the uniqueness of human biometrics which played a master role in degrading imposters' attacks.

2. Biometrics solutions for authentication disability people

According to the world health organization, about 16% of the world's population lives with a disability, so this percentage is not a few and researchers try to find a method to authenticate disability people without problems.

Numbers of authentication methods and software application are created and proposed for disability authentication, some of these methods are success to solve the problem and some encounter difficulties and complexities.

Sometimes it is possible that some people with some disability may not register or authenticate himself, in that case multimodal biometrics is essential.

When design any biometric system the designer must consider the disability people and try to authenticate them using the new system, also must involve the disability people in biometric steps (image acquisition, image localization, image normalization, feature extraction, matching or verification).

There were some significant achievements on disability people authentication solutions in the past several years, to help them to authenticate without difficulties or problems. This section discusses these solutions.

2.1. Previous studies on authentication for blind and visually impaired individuals

Authentication systems play a vital role in ensuring the security and privacy of digital information. However, traditional authentication methods, such as passwords, PINs, and graphical patterns, are often designed for sighted users and can pose significant challenges for blind and visually impaired individuals. To address these limitations, researchers have explored alternative and accessible authentication methods, including Braille-based PIN entry, tactile or audio-based graphical passwords, and biometric solutions such as fingerprint recognition. According to information from the world health organization [7], the number of visually impaired people in the world is 285 million, 39 million are blind and 246 have low vision. In Sudan, as an example of the developing countries, about 0.7% of the total sudanese population is blind.

In 2018 Bhat et.al, proposed Abhigyaan device. In this world there are many people who are visually disabled. In our daily life our eyes play an important role in guiding us through all activities but what about the unfortunate people who are not able to use their vision, Abhigyaan is a low cost educational device that will help the visually impaired to gain knowledge with ease. Knowledge is the key to life, without knowledge it is difficult for a human to live life at par. It is very important to get the formal education to with stand the pressure of society [8].

A survey paper by YAN, 2019 [9] wrote "Non-contact biometric features such as face and iris are of additional benefit than contact-based biometrics such as fingerprint and hand geometry. In contrast, the UV of iris recognition is slightly lower than that of face recognition, as a small number of users may have visual impairment. But the UQ and PM of iris recognition are very high.

However, three main challenges still remain in non-contact biometric authentication systems: ability to handle unconstrained acquisition, robust and accurate matching and privacy enhancement without compromising security. For iris recognition, low resolution and image distortion will have a negative impact on recognition results, so a good hardware for iris data collection is necessary. In fact, iris recognition is rarely used in mobile devices. The AC of iris recognition is low. But on the other hand, iris data is difficult to be duplicated without user consent, which reduces the possibility of replay attack (spoofing attack) and has correspondingly higher security than other types of recognition.

In 2022, ShilpaTharani et al., in the paper “EYE-TM: an automatic teller machine for the visually impaired” there are three levels of security authentication which comes in handy for the visually impaired which can make them easily interact with the automatic teller machine (ATM) and help them in secured transactions. The first level of authentication includes the single user detection where only the single user is allowed to enter into the system. The next process involves fingerprint authentication which acts a biometric identity and matches with the account. The final step involved is the facial recognition system which again matches with the current identity of the user. The prerequisites are obtained from the user during the time of account creation. Thus, this ATM system aims in facilitating the visually impaired people in accessing their account without the help of any intruders and make their transactions more safe and secure [10].

In 2022, Jeba Sheela A et al., published a survey examining authentication and voice assistance technologies designed to support visually challenged individuals. The authors highlighted that, while sighted individuals can generally interact with their environment and digital systems without difficulty, visually impaired users often face significant challenges in accessing information and online services. The study emphasized that advances in assistive technologies have substantially improved opportunities for visually impaired people, particularly in the context of internet and website accessibility. The survey focused on the role of Automatic Speech Recognition (ASR) systems powered by artificial intelligence, noting that recent developments in deep learning have significantly enhanced speech recognition performance and the effectiveness of voice-based assistance. In addition, the authors reviewed various authentication approaches aimed at providing secure access to internet applications. Through a comprehensive analysis of existing research, the study concluded that the integration of advanced artificial intelligence (AI)-driven voice assistance and secure authentication mechanisms can greatly improve website accessibility, enabling visually impaired users to interact with online services more independently and efficiently, in a manner comparable to that of sighted users [11].

In October 2024, Iluno et al., developed a deep learning-based system aimed at enhancing human–computer interaction for visually impaired users in educational environments. The study was motivated by the recognition that, despite education being a fundamental right, individuals with visual impairments often face significant barriers in accessing equitable learning opportunities. The primary objective was to improve accessibility by integrating advanced deep learning technologies into an intuitive and user-friendly platform. The proposed system incorporated a biometric authentication mechanism based on facial recognition, providing students with secure and personalized access to educational resources. Using the YOLOv5 object detection framework, the system achieved reliable real-time identification of users, enabling efficient login procedures through facial biometrics. To further improve usability, an adaptive noise cancellation mechanism based on the Least Mean Squares (LMS) filter was implemented to reduce background noise and enhance speech recognition accuracy in noisy environments. The LMS filter continuously adapted to changing noise conditions, thereby improving voice intelligibility and interaction performance. Finally, the study integrated biometric identification, voice recognition,

and adaptive noise cancellation into a unified assistive system and evaluated its performance in real-world scenarios. The results demonstrated the system's effectiveness in providing a secure, accessible, and user-friendly solution for visually impaired learners. Consequently, the authors recommended its deployment in schools and colleges to enhance educational accessibility and improve the overall learning experience of students with visual impairments [12].

In August 2025, Md Mojibur et al. [13] highlighted the challenges faced by blind and visually impaired users when interacting with modern authentication systems. He noted that, despite the growing number of advanced authentication methods proposed in academic research, their suitability for blind and visually impaired individuals in terms of both accessibility and security remains uncertain. To address this issue, the researchers developed the Authentication Literature Evaluation for Security and Accessibility (ALESA) framework, which includes five accessibility criteria and eight security criteria for assessing authentication methods. Using this framework, they systematically evaluated 37 general-purpose authentication schemes and 13 schemes specifically designed for blind and visually impaired users. The findings revealed that many of these schemes suffer from limitations in both accessibility and security, including those specifically developed for this user group. The study also demonstrated that achieving a balance between usability and security remains a significant challenge, with many security vulnerabilities arising from accessibility barriers, particularly in screen reader-assisted environments. Consequently, the authors emphasized the need for researchers, developers, and policymakers to address these shortcomings and develop authentication solutions that are both secure and accessible for blind and visually impaired users.

In October 2025, Clara et al., introduced the ALIAS (Accessible Login and Identification Authentication System) project, which aims to develop barrier-free authentication solutions for blind and low-vision (BLV) users. The researchers emphasized that authentication is a fundamental component of information security; however, many existing authentication mechanisms remain inaccessible to individuals with visual impairments. Given the increasing reliance on digital services and the growing number of people affected by blindness worldwide, ensuring accessible and secure authentication has become a critical challenge. The ALIAS project addresses this issue by designing an inclusive authentication system grounded in cognitive ergonomics and user experience (UX) principles tailored specifically to the needs of BLV users. The study reviewed existing research on accessible authentication, identified current limitations and research gaps, and proposed a methodology for developing more inclusive solutions. As part of the project, the researchers planned to establish a comprehensive knowledge base on the digital practices, behaviors, and cognitive models of BLV users during authentication processes. This knowledge would guide the design and development of authentication prototypes, which would then be evaluated and refined through multiple iterative testing phases before the deployment of a final operational system. The project seeks to enhance both accessibility and security, enabling blind and low-vision users to interact with digital services more independently and effectively [14].

Prastyo and Setyanto conducted a study to evaluate the performance of the FaceNet and VGG16 deep learning models for facial recognition among visually impaired individuals. Recognizing that people with visual impairments may encounter difficulties during image acquisition, the researchers investigated how different face detection techniques influence recognition accuracy. The study compared two face detection methods, MTCNN and HaarCascade, using facial images collected from visually impaired participants under varying lighting conditions and facial expressions. The experimental results demonstrated that the effectiveness of face recognition systems depends heavily on the accuracy of the face detection stage. MTCNN achieved a higher face detection accuracy of 93.75% compared to 83.75% for HaarCascade. Furthermore, when facial images were correctly

detected using MTCNN, both FaceNet and VGG16 achieved a recognition accuracy of 100%. Based on these findings, the authors concluded that MTCNN is the preferred face detection approach for facial recognition applications involving visually impaired users and recommended combining it with either FaceNet or VGG16 to achieve highly reliable authentication performance [15].

In April 2026, Oommen and Sharma investigated the challenges that BLV individuals face when completing identity verification processes required to access government services and public benefits. The researchers argued that most contemporary identity verification systems are designed primarily around visual interaction, creating significant barriers for BLV users. Using a mixed-methods approach that combined an analysis of 219 Reddit discussions with semi-structured interviews involving 16 BLV participants, the study revealed widespread accessibility shortcomings in both digital and in-person verification procedures. The findings demonstrated that inaccessible verification systems do more than create inconvenience; they fundamentally alter how users achieve and maintain security, often reducing their independence and autonomy. The study also identified several factors that intensify exclusion from essential services, including repetitive verification requirements, inaccessible physical infrastructure, and frequent policy changes. Furthermore, participants expressed nuanced perspectives on artificial intelligence, recognizing its potential as a powerful accessibility tool while simultaneously expressing concerns about its increasing use in identity fraud and security-related threats. The authors concluded that future identity verification systems must balance accessibility, security, and user autonomy to ensure equitable access to critical public services for BLV individuals [16].

Previous studies on authentication for blind and visually impaired individuals indicate that no method has yet proven to be fully suitable and comfortable for these users.

2.1.1 Analysis of Biometric Authentication Methods for Blind and Visually Impaired People

The reviewed studies demonstrate a significant evolution in biometric authentication research for blind and visually impaired users, moving from technology-centered approaches toward user-centered and accessibility-focused solutions. While early studies primarily emphasized the technical performance of biometric systems, more recent research highlights the importance of balancing security, accessibility, usability, and user autonomy.

Evolution of Biometric Technologies

The work of N. K. Bhat et al. [8] focused on improving educational accessibility through the Abhigyaan device. Although the system was not primarily developed as a biometric authentication solution, it highlighted the importance of assistive technologies in enabling visually impaired individuals to interact independently with digital systems. This study established the foundation for later research that integrates accessibility with secure user identification.

Similarly, the survey by Yan [9] emphasized the advantages of non-contact biometric modalities such as facial and iris recognition. The study identified iris recognition as one of the most secure biometric methods due to its resistance to spoofing attacks and high uniqueness. However, it also acknowledged significant challenges, including image quality requirements, hardware limitations, and accessibility concerns for users with visual impairments. These findings suggest that although iris recognition offers strong security, practical deployment for visually impaired users remains challenging.

Multi-Modal Biometric Authentication

A notable advancement was presented by Shilpa Tharani et al. [10] through the EYE-TM system. Their approach combined three layers of authentication: single-user detection, fingerprint verification, and facial recognition. This multi-factor biometric architecture significantly strengthened security

while reducing the risk of unauthorized access. The system demonstrates that combining multiple biometric traits can provide higher reliability and security for visually impaired users during sensitive activities such as ATM transactions. However, the increased number of authentication steps may potentially affect usability and interaction speed.

Integration of Artificial Intelligence and Deep Learning

Recent studies have increasingly incorporated deep learning into biometric authentication. The work of Iluno et al. [12] represents a comprehensive approach that integrates facial biometrics, voice recognition, speech-to-text functionality, and adaptive noise cancellation. Unlike traditional authentication systems that focus solely on identity verification, this study combines authentication with assistive interaction technologies. The use of YOLOv5 for facial recognition and LMS filtering for noise reduction demonstrates how artificial intelligence can improve both authentication accuracy and user accessibility. This approach addresses a key challenge in biometric systems for visually impaired users: ensuring that authentication remains seamless within broader human-computer interactions.

Similarly, the study by Agung Budi Prastyo and Arief Setyanto focused on optimizing facial recognition performance. Their results demonstrated that the accuracy of biometric recognition is highly dependent on the quality of face detection. The superior performance of MTCNN compared with HaarCascade indicates that advanced deep-learning-based detection methods can significantly improve authentication reliability. Achieving 100% recognition accuracy with both FaceNet and VGG16 after successful face detection suggests that facial recognition has strong potential as an authentication method for visually impaired users, provided that environmental and image acquisition challenges are effectively addressed.

Accessibility and User-Centered Authentication

While many studies focus on technological performance, recent research has shifted attention toward accessibility challenges. The survey conducted by Akanda et al. [13] represents a critical evaluation of existing authentication methods through the ALESA framework. The study revealed that many authentication schemes fail to achieve an effective balance between accessibility and security. Importantly, it showed that accessibility barriers often create new security vulnerabilities, particularly when users rely on screen readers or external assistance. This finding suggests that high authentication accuracy alone is insufficient; systems must also be designed to accommodate the specific interaction needs of visually impaired users.

The ALIAS project proposed by Toussaint et al. [14] further advances this perspective by adopting cognitive ergonomics and user experience principles. Rather than concentrating solely on biometric algorithms, the project emphasizes understanding the cognitive behaviors and digital practices of blind and low-vision users. This user-centered methodology reflects a growing recognition that successful biometric systems must be designed around users' capabilities and experiences rather than requiring users to adapt to the technology.

Authentication Beyond Technical Performance

The study by Oommen and Sharma [16] expands the discussion beyond biometric accuracy to include social and policy implications. Their findings demonstrate that inaccessible identity verification processes can reduce user independence and limit access to essential government services. The study highlights that authentication systems influence not only security outcomes but also social inclusion and digital equality. Furthermore, participants expressed both optimism and concern regarding artificial intelligence, viewing it as a valuable accessibility aid while recognizing its potential role in identity fraud.

Role of Voice-Based Authentication and Assistance

The survey by Jeba Sheela et al. [11] highlights the importance of voice-based technologies in improving accessibility. Advances in ASR and deep learning have significantly enhanced the performance of voice assistants, allowing visually impaired users to access online services more independently. Although voice authentication alone may not provide the highest level of security compared with biometric modalities such as iris or facial recognition, its integration with other authentication methods can create more accessible and user-friendly systems.

2.1.2. Conclusion

Overall, the reviewed literature demonstrates substantial progress in biometric authentication for blind and visually impaired individuals. Facial recognition, fingerprint authentication, iris recognition, and voice-based technologies have shown considerable promise, particularly when enhanced by deep learning techniques. However, recent studies consistently indicate that authentication effectiveness should not be measured solely by recognition accuracy. Accessibility, independence, cognitive usability, and user trust are equally important factors. Future research should therefore focus on developing inclusive multi-modal biometric systems that integrate advanced security mechanisms with user-centered design principles to provide secure, accessible, and autonomous authentication experiences for blind and visually impaired users.

2.2. Previous studies on authentication for physical disability people

Ensuring secure and accessible authentication is essential for all users, yet traditional methods often overlook the needs of individuals with physical disabilities. Many common authentication techniques—such as typing passwords, entering PINs, or performing touch-based gestures—require fine motor skills or hand mobility that some users may find difficult or impossible to perform. In this section, previous studies have investigated alternative authentication solutions designed to reduce physical barriers.

In 2015 Qamar et.al, wrote paper entitled “Multi-sensory Gesture-Based Login Environment”, the traditional method of accessing a computer system by entering login credentials through a keyboard is difficult to practice in certain work environments. Examples of such environments are a surgical operation room or an industrial manufacturing facility where a subject is not able to access the keyboard due to fear of contamination or environmental hazards. Similar issues arise with physically challenged individuals who face difficulty in using a keyboard due to hand disability. A number of alternative accessibility methods have been developed such as finger print-based solutions used by mobile phones, face recognition for gaming via Kinect and tap pattern based login for touch screens. All of these solutions, however, cannot function efficiently in the above mentioned environments where both the face and the fingers are fully or partially covered by clothes, gloves or masks [17].

In October 2018, Fenner and Noteboom, [18] in their work about disability mentioned “the issue increases for persons with disabilities. Cognitive, physical, or multiple disabilities make identification of individuals difficult or impossible, thus increasing the need for a care giver or family member to verify the individual’s identity. People with disabilities may not have the capacity to remember a password or understand why it is necessary. For example, some individuals do not have the physical ability to interact with a biometric authentication system, due to a physical abnormality, accident, or birth-related issue ”.

Another idea by James et al., in 2020 wrote “different biometric authentication systems can present multiple problems to persons with different disabilities. A study involving both a control group and a disabled group found that speaker recognition was difficult for many people with

cognitive learning disabilities and for people with hand and arm disabilities because they had to press a button while speaking.

Many groups, including people with a physical or learning disability, people suffering from mental illness, the elderly, and people of minority race or minority religion, may become increasingly socially excluded as biometrics grows and expands. They can fall behind due to various reasons aversions to new technology, distrust of technology, or difficulties enrolling and verifying with biometric data. However, if biometric authentication becomes a requirement to receive government assistance, social services, and benefits, many of these groups will become even further disadvantaged" [19].

Nevertheless in February 2022 [20], Pintavirooj et al., proposed an eye-gaze control system for people with motor disabilities. The system consists of eye-tracking glasses, a depth camera to capture the geometry of the ambient space, a set of ultrasound and infrared sensors to detect an obstacle, a laptop placed on a flexible mount, and a safety switch to turn off the system in case of emergency.

Later in August 2022 the project by alzebali et al., it's aim to take advantage of today's technology to offer a helping hand to people with special needs. Therefore, the work suggests a control system as an android application in addition to a website for people with special needs. Many people with special needs have problems asking for or interpreting and recognizing their needs. Hence the idea of the application is designed to work on smart devices to help them communicate and identify their understanding way. Through the keyboard or speech translation. Artificial intelligence techniques have used to enrich the work and add useful and important features such as chatbot technology. In short, the project is to make life as easy as possible for people with physical disabilities and make them go about their lives without relying on others or waiting for help [21].

On February 2024, kamil and khalid, 2024 propose new method to authenticate disability people. Advanced eye-tracking technologies combined with artificial intelligence enable the execution of computer tasks using subtle eyelid movements. This technology allows for the elimination of traditional input devices such as keyboards and mice, and it also opens up better access to the digital world for people with disabilities.

Authorization by eyelid movement is a very attractive method for people with various diseases and disabilities. For people with mobility limitations, it can prove to be one of the most effective methods of authorization that require no effort and do not require wearing specialized equipment [22].

Pushpavalli et al., proposed a Secure Online Voting System aimed at improving the accessibility, security, and transparency of the electoral process. The study highlights the limitations of traditional voting systems, including restricted access for certain voter groups, security concerns, and a lack of transparency, all of which can negatively affect voter participation and public trust. To overcome these challenges, the proposed system utilizes advanced technologies that enable voters to cast their ballots remotely through internet-connected devices. This approach is particularly beneficial for Non-Resident Indians (NRIs) and individuals with physical disabilities. The system incorporates multiple security mechanisms, including biometric authentication, One-Time Password (OTP) verification, and real-time camera surveillance, to ensure voter authenticity while maintaining privacy. Furthermore, the integration of facial recognition and live monitoring enhances the integrity and transparency of the voting process, thereby increasing confidence in election outcomes. The study concludes that secure online voting platforms can play a significant role in promoting a more inclusive, reliable, and trustworthy democratic system in the era of digital transformation [23].

2.2.1. Analysis of Biometric Authentication Methods for Physical Disability People

The reviewed studies demonstrate the growing interest in developing accessible authentication and assistive technologies for people with disabilities. They collectively highlight the limitations of conventional authentication methods and propose alternative approaches that improve accessibility, security, and independence for users with diverse physical and cognitive impairments.

The study by Qamar et al. [17] introduced a multi-sensory gesture-based login environment as an alternative to traditional keyboard-based authentication. The authors identified situations where keyboards are impractical, such as surgical rooms, industrial facilities, and environments requiring protective equipment. The proposed solution is particularly relevant for individuals with hand disabilities who experience difficulties using standard input devices. A major contribution of this work is its recognition that common biometric methods such as fingerprint and facial recognition may fail when users wear gloves, masks, or protective clothing. However, the study primarily focuses on gesture-based interaction and does not fully address the diverse accessibility requirements of users with severe motor impairments.

Fenner and Noteboom [18], the challenges faced by people with disabilities in identity verification were explored. The study emphasized that cognitive, physical, and multiple disabilities can make authentication difficult or impossible without caregiver assistance. It highlighted the limitations of password-based systems for users with memory or cognitive impairments and pointed out that some individuals may be unable to interact with biometric systems because of physical abnormalities or injuries. This work provides valuable insight into the accessibility barriers present in traditional authentication systems and underscores the need for more inclusive solutions.

Similarly, Adegbengle et al. [19] examined the impact of biometric authentication on different disability groups. Their findings revealed that speaker recognition systems can be problematic for individuals with cognitive disabilities and those with hand or arm impairments due to operational requirements such as pressing buttons while speaking. The authors further argued that the widespread adoption of biometric technologies could unintentionally increase social exclusion among vulnerable populations, including people with disabilities, older adults, and individuals with limited technological literacy. The study contributes an important social perspective by emphasizing that authentication technologies must be designed to accommodate all users rather than creating additional barriers.

A significant advancement was presented by Pintavirooj et al. [20] through the development of an eye-gaze control system for individuals with motor disabilities. By combining eye-tracking glasses, depth cameras, obstacle-detection sensors, and emergency safety mechanisms, the system enables users to interact with digital environments without relying on physical movements. This approach demonstrates how eye-tracking technology can provide greater autonomy for individuals with severe mobility impairments. Nevertheless, the system requires specialized hardware, which may limit its affordability and widespread adoption.

In the same year, Alzebali et al. [21] proposed an Android application and web-based platform designed to support people with special needs in communication and daily activities. The integration of speech translation, virtual keyboards, and artificial intelligence techniques such as chatbots allows users to communicate more effectively and independently. The project focuses on improving quality of life and reducing dependence on caregivers. While the system successfully enhances communication accessibility, authentication and security aspects are not its primary focus.

More recently, Kamil and Khalid [22] proposed an innovative authentication method based on eyelid movements combined with artificial intelligence and eye-tracking technologies. The approach enables users to perform authentication tasks without keyboards, mice, or wearable equipment. This method is particularly beneficial for individuals with severe motor disabilities, as it requires minimal physical effort while maintaining usability. The study highlights the potential of eye-based biometrics

as a highly accessible authentication mechanism. However, further research is needed to evaluate its accuracy, security, and resistance to spoofing attacks in real-world scenarios.

Finally, Pushpavalli et al. extended the discussion of accessibility into the field of electronic voting by proposing a Secure Online Voting System. The system combines biometric authentication, OTP verification, facial recognition, and live camera monitoring to ensure secure and transparent remote voting. Its design specifically benefits individuals with physical disabilities by allowing them to vote from any location using internet-connected devices. The study demonstrates how biometric technologies can be integrated into public services to improve accessibility while maintaining security and trust. However, concerns related to privacy protection, cybersecurity threats, and technological accessibility remain important considerations for practical implementation.

2.2.2. Conclusion

Overall, the reviewed studies reveal a clear evolution from alternative authentication mechanisms toward more intelligent, inclusive, and user-centered solutions. Early research focused on overcoming the limitations of traditional keyboards and passwords, while recent studies increasingly utilize artificial intelligence, eye-tracking, and biometric technologies to support people with disabilities. Despite these advancements, several challenges remain, including usability across different disability categories, affordability of specialized hardware, privacy concerns, and the risk of social exclusion caused by inaccessible biometric systems. A common limitation across many studies is that they typically address a single disability category or rely on a specific biometric modality. Consequently, there remains a need for a unified authentication framework capable of supporting multiple disability groups, including visually impaired, deaf, speech-impaired, and physically disabled individuals. Future research should focus on developing adaptive multimodal biometric systems that offer high security, accessibility, and usability.

2.3. Previous studies on authentication for hand disability people

Traditional authentication methods, such as typing passwords, entering PINs, or using touch-based gestures, rely heavily on hand movement and fine motor control. This dependence creates significant challenges for individuals with hand disabilities, who may have limited mobility, reduced dexterity, or difficulty performing precise input actions. As a result, previous studies have explored alternative authentication techniques.

In 2016 Ali et al, mentioned “keystroke biometrics on smart phones, with touch screen and timing features, needs more research involving human factors, as human factors may skew findings. Their work focus on identifying several behavioral and physiological characteristics found in humans. Each is uniquely associated to an individual and categorically distinguishable. These factors can interfere with the authentication accuracy due to the variation in typing rhythm. Some of these causes identified are: fatigue, distraction, ethnic background, hand/finger dominance, gender and age, any accidental injuries, operations, physical disabilities or mental disabilities.

First, physiological characteristics, this includes a person’s physical attributes, such as finger/hand dominance, physical injuries and motor disabilities. These traits are considered to be the leading traits that can support high recognition or high false rejection rate, these are the physiological factors that can hinder or facilitate data capturing. For example, injuries and disabilities, such as a cut or dislocated finger, can produce quite different results in the keystroke rhythm dynamics. Consider a healthy individual who suddenly endures a cut on their thumb. When they type into their smart phone the pattern will be different than their template due to the cut” [24].

From different point of view in February 2016, Chathumal et al said “There are some applications for disabled people, but people who have disabilities in hands do not have a proper application to interact with new technologies. The aim of the project is to develop software that act as an intelligent controller to facilitate hand disabled people when interacting with a computer. Proposed intelligent solution is based on speech recognition, image processing and human computer interaction. The application is capable of moving mouse cursor with face detections, activities based on voice commands, provide user authentication by voice recognitions and give suggestions using facial emotions ” [25].

In the same context in February 2018 Alhayajneh et al., in the paper entitled “Biometric Authentication and Verification for Medical Cyber Physical Systems, Electronics”, wireless body area network (WBAN) is a network of wirelessly connected sensing and actuating devices. WBANs used for recording biometric information and administering medicationare classified as part of a Cyber Physical System (CPS). Disavantages of GG are not viable for mentally, requires controlled visually, and physically laboratory setting disabled individuals. Another disadvantage regarding the head-movement techniques are that the unique head-movements for human beings might not be functional for mentally or physically disabled individuals.

Hand wearable devices, including smart watches, are considered the most common forms of WBANs authentication systems with high accuracy rates. A second disadvantage of the hand wearable device authentication it requires hand movements for authentication, which might not be applicable for mentally or physically disabled individuals [26].

In contrast YAN, 2019, [9] mentioned hand disability in the paper “in recent years, fingerprint-based authentication systems have been widely accepted in both academia and industry. As a kind of biological feature commonly owned by human beings (except for a few persons with hand disabilities), fingerprints have enough inter-user differences and individual stability”.

Another study on the year 2023 by Brittany, about designing accessible computing device authentication for people with upper extremity impairment, as follows, computing device authentication, the process of proving one’s identity to a computing device (e.g., laptop, tablet, smart phone, etc.), is critical to protecting the sensitive data these devices contain. However, computing device authentication often makes assumptions about the user’s ability to perform complex tasks with their arms, hands, and fingers. For example, entering complex passwords, or accurately positioning a camera for facial recognition. This can create barriers for people with upper extremity impairment (UEI) who have reduced strength, accuracy, dexterity, speed, and/or range of motion in their shoulders, upper arms, forearms, hands, and/or fingers. The goal is to design new, more accessible computing device authentication for people with UEI [27].

Subsequently in May 2023 study by Morgan, that facial recognition and voice recognition are only used in situations where a patient’s “fingerprints aren't there because of accidents or disabilities or something.” The voice recognition we use only when the patient doesn’t have the fingerprints or doesn’t have their hands. We use fingerprints for more than half of the patients. We have been using face recognition alongside fingerprints to identify. This technology is very important. One technology could fail; if a face scanner fails then we need to look at the fingerprint and vice versa [28].

In light of previous studies, many attempts, solutions, and methods have been proposed for individuals with hand disabilities, but most biometric approaches were not highly distinctive. Therefore, there is a need for unique biometric traits that can be used for people with hand impairments.

2.3.1 Analysis of Biometric Authentication Methods for Hand Disability People

The literature review is centered on an important research problem: traditional authentication methods can become inaccessible when authentication depends on hand movement, fine motor control, or intact fingerprints. The studies you collected provide a useful foundation for proposing alternative biometric modalities for people with hand disabilities.

The literature shows three main problems:

- Behavioral authentication can be unstable. Keystroke dynamics depend on typing rhythm and can change because of injury, disability, fatigue, distraction, age, or other human factors.
- Many assistive authentication approaches still depend on physical interaction. Voice, head movement, wearable devices, or controlled positioning can themselves create accessibility barriers.
- Fingerprint authentication is not universally applicable. Individuals with hand injuries, missing fingers, or hand disabilities may have difficulty providing a usable fingerprint.

The 2023 work by Brittany is particularly relevant because it explicitly identifies the mismatch between conventional authentication requirements and the abilities of people with upper-extremity impairment.

The following table explain the previous studies for hand disability people.

Table 1. Previous studies for hand disability people

Study	Authentication/technology	Main contribution	Limitations
Ali/Patel et al. (2016)	Keystroke biometrics	Shows that typing behavior can vary because of physiological and human factors	Requires typing and fine motor interaction; injury or disability can change the user's biometric pattern
Chathumal/Samaraweera et al. (2016)	Speech, face detection, voice authentication	Provides hands-free interaction for people with hand disabilities	Voice/face approaches may not be suitable for every user or situation
Alhayajneh et al. (2018)	WBAN/biometric authentication	Investigates biometric authentication using body-connected sensing technologies	Wearable authentication can require physical interaction or controlled conditions
Yan (2019)	Fingerprint authentication	Highlights fingerprint stability and distinctiveness for most users	Fingerprints may be unavailable or difficult to capture for some people with hand disabilities
Brittany (2023)	Accessible device authentication	Explicitly addresses authentication barriers for people with upper-extremity impairment	Indicates the need for authentication designed around accessibility rather than adapting conventional input
Morgan (2023)	Fingerprint + facial/voice recognition	Describes multimodal identification when fingerprints are unavailable	Suggests the value of alternative or complementary biometrics rather than relying on one modality

2.3.2 Conclusion

The most important gap emerging from these studies is not simply that existing authentication methods have disadvantages. The deeper gap is that many solutions remain dependent on a particular physical or behavioral capability.

For example:

Password/PIN → requires manual input
Keystroke biometrics → requires consistent typing
Fingerprint → requires usable fingers/hand
Hand wearable → requires wearing/interacting with a device
Head movement → requires controlled head movement
Voice → requires reliable speech
Facial recognition → may require appropriate positioning and camera conditions

Therefore, an authentication system designed specifically for people with disabilities should consider the user's functional abilities when selecting the biometric modality.

2.4. Previous studies on authentication for deaf and dumb people

Systems that depend on voice commands, audio notifications, or spoken verification are inherently inaccessible to users who cannot hear or speak. Recognizing these limitations, previous research has investigated alternative authentication approaches designed specifically for this group.

In 2017 Sayeed et al., in their paper proposes a sign language interpretation system by a combination of data glove and photo plethysmograph sensor measurements collected concurrently from data glove. This system is tested on many numbers of trials by different subjects performing a set of particular shapes using the american sign language (American Sign Language (ASL)).

In the work a robust sign language system was developed for the usage of the disabled in the case of communication and common people also can use the security features. Data glove and helps in increasing the euclidean distance up to 10 times higher than the normal data glove usage in security. The simple euclidean distance calculations are found enough to establish the system without much complicated mathematical modeling or complex classifiers. This proves that this system can be readily implemented without much computational complexity [29].

Patel and Ambekar reported “in our day-to-day life, communication plays a crucial role to convey information from one person to another. It becomes very difficult for the people who are deaf and dumb to communicate with others. Sign language is the only way which connects them however not everyone is familiar with sign language. So there is need of translating sign language into text & speech. It is known as Sign Recognition. Sign language is a combination of body languages, hand gestures, and facial expressions. Among those, hand gestures is the most effective method hence the majority of research going is going on decoding the hand gestures” [30].

Subsequently, Morris et al. [31] stated “Artificial intelligence (AI) technologies have the potential to dramatically impact the lives of people with disabilities (PWD). People with accents, including accents due to disability (e.g.,“deaf accent”), also face challenges using current ASR tools, though it is possible to train personalized models for such groups. Speech disabilities such as disarthrya, as well as the use of speech-generating augmentative and alternative communication (AAC) devices, can also negatively impact ASR functionality. Further, people who are un able to speak at all (i.e., some people who are deaf, people with some forms of aphasia), may be locked out of using ASR technologies. Cognitive and intellectual disabilities are likely to impact the efficacy and utility of many aspects of text analysis systems”.

In September 2019 Effendy [32] discusses the problem of cerebral palsy as follows: cerebral palsy (CP) is a neurological condition that causes problems in body movement and muscle control that can inhibit the development of children’s speech. It can be classified into several types, based on the stiffness of the muscles that they suffer. This study offers a new technique for identifying the severity CP level of children based on their speech. This study utilizes the capabilities of the voice biometrics system (VBS) to authenticate people based on their voice. The Mel-frequency stochastic

model is also offered as a new approach in the feature extraction process. Because of the pattern of speech signals of children with CP which is irregular, then neuro fuzzy is chosen as a method in the speech classifier. Based on the experiment conducted to respondents, the accuracy of the technique is 87.5%. This result shows good performance of the new approach for realizing the research objective [32].

Sangeetha et al. [33] proposed a project that presents a machine learning–based system and integrates computer vision and speech processing techniques to enable intelligent sign language recognition and translation. Deaf and mute individuals primarily rely on sign language for communication; however, the majority of people are not familiar with it, leading to a significant communication gap. Existing solutions depend heavily on human interpreters or manual interpretation methods, which are often costly, time-consuming, error-prone, and unsuitable for real-time communication due to their limited availability. To address these challenges, the proposed system introduces a two-way communication framework that converts sign language gestures into text and speech for non-sign users, while also transforming voice or text input from normal users into sign language for hearing-impaired individuals. By leveraging machine learning algorithms, the system ensures real-time performance, improved accuracy, and cost-effectiveness. This approach reduces dependency on human interpreters and enhances accessibility, enabling seamless and inclusive communication between hearing and speech-impaired individuals and the general population [33].

Alabduallah et al. [34] reported that Sign language (SL) is an effective mode of communication, which uses visual–physical methods like hand signals, expressions, and body actions to communicate between the difficulty of hearing and the deaf community, produce opinions, and carry significant conversations. Sign language recognition (SLR), the procedure of automatically identifying and construing gestures of SL, has gotten considerable attention recently owing to its latent link to the lack of communication between the deaf and the hearing world. Hand gesture detection is its domain, in which computer vision (CV) and AI help deliver non-verbal communication between computers and humans by classifying the significant movements of the human hands. The emergence and constant growth of deep learning (DL) approaches have delivered motivation and momentum for evolving SLR. The main objective of the ISLRHP-HMOADL technique focused on hand pose recognition to improve the efficiency and accuracy of sign interpretation for hearing-impaired persons. Initially, the ISLRHP-HMOADL model performs image pre-processing using a wiener filter (WF) to enhance image quality by reducing noise. Furthermore, the fusion of three models, ResNeXt101, VGG19, and vision transformer (ViT), is employed for feature extraction to capture diverse and intricate spatial and contextual details from the images. The bidirectional gated recurrent unit (BiGRU) classifier is implemented for hand pose recognition. A comprehensive experimental study is accomplished under the ASL alphabet dataset to exhibit the improved performance of the ISLRHP-HMOADL model. The comparative results of the ISLRHP-HMOADL model illustrated a superior accuracy value of 99.57% over existing techniques [34].

Despite the availability of many traditional biometric authentication techniques such as fingerprint, facial recognition, and voice biometrics, some of these methods are unsuitable or have limited effectiveness when applied to individuals who are deaf and mute, especially when the system requires voice inputs or speech-based interactions.

2.4.1. Analysis of Biometric Authentication Methods for deaf and dumb

This section provides a critical, research-oriented analysis of the authentication methods considered for deaf and speech-impaired users, focusing on the contribution and limitations of each study.

Table 2. Previous methods for authentication deaf and dumb

Study	Main problem	Technology	Disability focus	Authentication focus
Qamar et al. (2015)	Keyboard limitations	Gesture-based login	Physical limitations	High
Noteboom (2018)	Authentication accessibility	Accessibility analysis	Multiple disabilities	High
James et al. (2020)	Biometric accessibility	Biometric systems	Multiple disabilities	High
Pintavirooj et al. (2022)	Physical interaction	Eye-gaze control	Motor disabilities	Partial
Alzebali et al. (2022)	Communication/independence	AI + mobile/web	Special needs	Low
Kamil & Khalid (2024)	Physical interaction	Eyelid + eye tracking + AI	Mobility limitations	High
Pushpavalli et al.	Voting accessibility/security	Biometrics + OTP + facial recognition	Physical disabilities	High

3. Discussion of The Results

The results of this study demonstrate that biometric authentication has considerable potential to improve the accessibility, security, and independence of people with disabilities. However, the analysis of previous studies indicates that the effectiveness of biometric authentication depends not only on the distinctiveness of the biometric trait but also on the user's functional abilities, the method of data acquisition, the accessibility of the interface, and the environmental conditions in which authentication takes place. Although several researchers have proposed alternative authentication techniques, no single method can be considered suitable for all disability categories. The findings therefore highlight the importance of developing inclusive authentication systems that adapt to the individual needs and abilities of users.

3.1. Accessibility Challenges in Existing Authentication Systems

One of the main findings is that conventional authentication methods frequently assume that users can perform specific physical, visual, auditory, or speech-related tasks. Passwords and personal identification numbers (PINs), for example, require users to interact with keyboards or touchscreens, while fingerprint authentication depends on the availability of usable fingers and the ability to position them correctly. Similarly, voice-based authentication requires users to produce recognizable speech, and visually dependent interfaces may create difficulties for blind and visually impaired individuals.

The reviewed literature demonstrates that these requirements can prevent some people with disabilities from completing authentication independently. Studies addressing physical and upper-extremity impairments emphasize the difficulties associated with typing, fine motor movements, and positioning devices. Research on blind and visually impaired users highlights the accessibility problems associated with visual instructions, image-based authentication, and systems that do not adequately support screen readers or alternative feedback mechanisms. Research concerning deaf and speech-impaired users also indicates that authentication methods relying exclusively on spoken commands or audio instructions may exclude users who cannot hear or produce speech.

These findings suggest that accessibility should be considered a fundamental design requirement rather than an additional feature introduced after system development. An authentication method may provide strong security for the general population while remaining unsuitable for particular users with disabilities. Consequently, evaluating biometric systems requires a broader perspective that includes accessibility, usability, independence, and security.

3.2. Findings Related to Blind and Visually Impaired Individuals

The reviewed studies reveal substantial progress in developing authentication and assistive technologies for blind and visually impaired individuals. Facial recognition, fingerprint authentication, iris recognition, voice assistance, and multimodal authentication have all been investigated as potential approaches to improving access to digital services.

The study by Yan (2019) highlights the potential advantages of non-contact biometric methods, particularly facial and iris recognition. These methods can reduce dependence on direct physical contact with a sensor. Nevertheless, their effectiveness may be affected by image quality, illumination, positioning, acquisition conditions, and hardware availability. The results therefore suggest that selecting a biometric modality based on its theoretical distinctiveness alone is insufficient; the system must also provide an accessible and reliable way for users to complete the acquisition process.

The EYE-TM system discussed by Shilpa Tharani et al. [10] combines user detection, fingerprint authentication, and facial recognition. This approach illustrates how multiple authentication stages can strengthen identity verification. However, introducing several stages may increase the time and effort required to authenticate. The findings indicate that multimodal authentication should be designed carefully to ensure that additional security does not create unnecessary accessibility barriers.

Research by Iluno and colleagues (2024) further demonstrates the potential of integrating facial recognition, speech-to-text functionality, voice commands, and noise cancellation into assistive systems. This integration illustrates that authentication can be combined with accessible interaction mechanisms to support more independent use. Similarly, Prastyo and Setyanto reported that MTCNN achieved a face-detection accuracy of 93.75%, compared with 83.75% for HaarCascade. They also reported 100% recognition accuracy for FaceNet and VGG16 when faces were successfully detected. These findings demonstrate the importance of the face-detection stage in determining the overall performance of a facial authentication pipeline. However, the reported recognition accuracy should not be interpreted as evidence of universal performance across all users and environmental conditions.

The ALESA framework discussed by Md Mojibur and colleagues (2025) provides an additional perspective by evaluating authentication methods according to accessibility and security criteria. Its findings indicate that authentication schemes can remain inaccessible or insecure even when they are specifically designed for blind and visually impaired users. The ALIAS project similarly emphasizes cognitive ergonomics and user experience as important elements of accessible authentication.

Taken together, these findings demonstrate that biometric recognition accuracy alone cannot guarantee successful authentication for blind and visually impaired individuals. Systems must provide accessible instructions, understandable feedback, reliable acquisition procedures, and alternatives when the primary method fails. The literature therefore supports the development of solutions that combine appropriate biometric modalities with accessible interaction design.

3.3. Findings Related to Individuals with Physical or Motor Disabilities

The analysis of studies addressing physical disabilities indicates that the primary challenge is reducing dependence on physical movements and conventional input devices. Authentication methods involving keyboards, touchscreens, fingerprint scanners, or wearable devices may be difficult for individuals with limited mobility or reduced motor control.

Qamar et al. (2015) explored a multisensory gesture-based login environment as an alternative to conventional keyboard-based authentication. Their work highlights the importance of considering situations in which users cannot easily access standard input devices. However, gesture-based methods may remain unsuitable for individuals who cannot perform the required movements consistently.

Pintavirooj et al. [20] investigated an eye-gaze control system that uses eye-tracking glasses, cameras, and additional sensors to support users with motor disabilities. Kamil and Khalid [22] also explored authentication based on eyelid movements and eye-tracking technologies. These approaches demonstrate the potential of eye-based interaction for reducing reliance on hand movements. Nevertheless, specialized hardware, calibration requirements, environmental conditions, and individual differences may affect their practical usability.

The reviewed literature also discusses AI-supported systems that allow interaction through alternative mechanisms. Although such systems may improve independence, their suitability depends on the particular abilities of each user. For example, an eye-based approach may be useful for a person who has limited limb mobility but may not be appropriate for someone who also has an eye-related impairment.

The results therefore suggest that authentication for individuals with physical disabilities should prioritize minimal physical effort, flexible interaction methods, and compatibility with assistive technologies. A system should not assume that all individuals within this category have the same functional abilities. Instead, it should support the selection of authentication methods according to each user's capabilities and preferences.

3.4. Findings Related to Individuals with Hand Disabilities

The reviewed literature reveals that hand disabilities create specific challenges for authentication methods that depend on fingerprints, typing behavior, hand movements, or wearable devices.

Ali et al. [24] highlighted how typing patterns can change because of injuries, fatigue, physical conditions, and other human factors. This finding is important because behavioral biometric systems may interpret changes in typing rhythm as evidence of an unauthorized user, even when the legitimate user is attempting to authenticate. Consequently, authentication methods based on keystroke dynamics may be unreliable for some individuals with hand impairments.

Chathumal and colleagues (2016) proposed a system combining speech recognition, image processing, and facial detection to facilitate computer interaction for people with hand disabilities. This approach illustrates the value of reducing dependence on manual input. However, speech-based authentication may not be suitable for users with speech impairments, and facial recognition may require appropriate camera positioning and acquisition conditions.

The reviewed work by Yan (2019) also indicates that fingerprint authentication, although distinctive and widely adopted, is not universally applicable to individuals with hand disabilities. Similarly, the study by Lewis [27] emphasizes that conventional authentication systems frequently assume that users possess sufficient strength, dexterity, accuracy, and range of motion to complete authentication tasks.

Banville's [28] findings further illustrate the practical value of combining fingerprint and facial recognition when one method is unavailable. This supports the broader observation that relying on a single biometric trait can create accessibility and reliability problems.

Overall, the findings indicate that authentication for individuals with hand disabilities requires alternatives that do not depend on intact fingerprints or precise hand movements. This provides a rationale for investigating biometric modalities that can be acquired without requiring substantial manual interaction. However, any proposed alternative must be experimentally evaluated to establish its distinctiveness, accessibility, reliability, and suitability for the intended users.

3.5. Findings Related to Deaf and Speech-Impaired Individuals

The reviewed literature indicates that authentication systems relying exclusively on voice commands, spoken verification, or audio instructions can create significant barriers for deaf and speech-impaired individuals. However, hearing impairment and speech impairment should not be treated as identical conditions: some deaf individuals can speak, while some individuals with speech impairments can hear normally. Authentication systems must therefore distinguish between hearing-related and speech-related accessibility requirements.

Sayeed et al. [29] investigated a sign-language-related system using data-glove and photoplethysmograph sensor measurements. The work demonstrates the potential of combining gesture information with physiological signals for recognizing user-specific patterns. However, wearable sensors and gesture-based approaches may introduce additional requirements for users who have limited hand mobility or difficulty wearing specialized devices.

Patel and Ambekar [30] examined sign-language recognition and translation to facilitate communication between deaf individuals and people unfamiliar with sign language. Similarly, later studies explored computer vision and deep-learning approaches to recognize sign-language gestures. The reported results demonstrate progress in gesture recognition and accessible communication. Nevertheless, sign-language recognition is not automatically equivalent to biometric authentication. Recognizing a gesture or interpreting a signed message does not, by itself, establish that the person performing it is the authorized user.

The reviewed research on speech recognition also indicates that speech-related technologies may perform poorly for some users with speech impairments, including individuals whose speech patterns differ from those represented in training data. This reinforces the need to avoid making speech a mandatory authentication requirement.

The overall findings suggest that deaf and speech-impaired users should be able to authenticate without depending on audio instructions or spoken responses. Alternative methods should provide visual, text-based, or other accessible feedback and should use an appropriate identity-verification mechanism. In addition, gesture-based authentication must be evaluated in terms of usability, security, and suitability for users with different levels of signing experience and hand mobility.

3.6. The Importance of Multimodal Biometric Authentication

A major finding across the reviewed studies is that no single biometric modality can reliably address the needs of every person with a disability. Fingerprint authentication may be unsuitable for some individuals with hand impairments, facial recognition may be affected by image acquisition conditions, voice recognition may exclude some speech-impaired users, and eye-based methods may be inappropriate for users with certain visual or ocular conditions.

Multimodal biometric authentication offers a possible way to address these limitations by combining two or more biometric traits. For example, a system may provide an alternative when the primary biometric modality cannot be acquired successfully. The reviewed EYE-TM system and the use of complementary fingerprint and facial recognition illustrate the potential advantages of combining authentication methods.

Nevertheless, multimodal authentication is not automatically more accessible or secure in every situation. Requiring users to complete multiple authentication procedures may increase complexity, acquisition time, equipment costs, and privacy risks. The system must therefore determine whether an additional biometric modality provides sufficient benefit to justify its use.

The findings support an adaptive approach in which the authentication method is selected according to the user's functional abilities and the requirements of the application. Such a system could offer alternative authentication paths rather than forcing every user to follow the same procedure. It should also provide a secure recovery mechanism when biometric acquisition fails.

This approach is particularly important for users with multiple disabilities, for whom a method designed for one disability category may introduce barriers associated with another. However, the reviewed literature does not establish that a single adaptive multimodal framework has already solved these challenges across all disability categories.

3.7. Implications for the Proposed Authentication Framework

The results of this study have several implications for the design of an inclusive biometric authentication framework.

The first implication is that biometric selection should be based on functional suitability rather than disability labels alone. Individuals with the same disability may have different abilities, preferences, and accessibility requirements. Therefore, the system should allow users to select suitable authentication methods and change them when necessary.

The second implication is that the framework should support alternative authentication paths. If the primary biometric method fails because of acquisition difficulties, environmental conditions, or changes in the user's physical condition, the user should have access to a secure alternative.

The third implication concerns accessibility throughout the authentication process. Accessibility must be incorporated into registration, biometric acquisition, verification, error handling, and recovery. Instructions and feedback should be available in appropriate formats, including audio, text, visual cues, or assistive-technology-compatible interfaces.

The fourth implication is that security and usability should be evaluated together. The framework should be assessed using measures such as recognition accuracy, false acceptance rate, false rejection rate, processing time, completion rate, user satisfaction, and the level of assistance required. Privacy protection and resistance to spoofing attacks should also be considered.

Finally, the framework should be evaluated with people representing different disability categories and levels of functional ability. Involving intended users in the design and testing process would help identify barriers that may not be apparent from a theoretical review alone.

3.8. Overall Discussion

In summary, the results demonstrate that biometric authentication offers promising opportunities to improve digital inclusion for people with disabilities, but important accessibility, usability, security, and implementation challenges remain. The reviewed literature shows that researchers have explored a variety of approaches, including facial and iris recognition, fingerprint authentication, voice technologies, eye tracking, eyelid movements, gestures, and multimodal biometric systems.

However, the effectiveness of these approaches depends on the relationship between the biometric modality and the user's functional abilities. The findings also demonstrate that high recognition accuracy does not necessarily guarantee an accessible or independent authentication experience. Factors such as acquisition requirements, hardware availability, environmental conditions, user preferences, privacy, and recovery procedures must also be considered.

The principal contribution of this study is its comparative perspective on authentication challenges across different disability categories and its identification of the need for a more comprehensive, disability-aware framework. Rather than assuming that one biometric method can serve all users, the findings support the investigation of adaptive authentication approaches that offer suitable alternatives according to individual requirements.

Since this study is based on a review and analysis of existing literature, the proposed implications should be interpreted as research directions rather than experimentally validated outcomes. Future work should implement and test the proposed framework with representative user groups, compare alternative biometric modalities, and measure both technical performance and user experience. Such evaluations would help determine whether an adaptive multimodal approach can provide secure, reliable, and accessible authentication for people with diverse disabilities.

4. Limitations of the Study

Despite its contributions to understanding biometric authentication for people with disabilities, this study has several limitations.

1. Limited Practical Implementation and Experimental Validation: This study is primarily based on a review and comparative analysis of existing literature. The proposed approaches have not been implemented and tested in a real-world environment. Therefore, their actual performance, reliability, usability, and effectiveness for people with different disabilities have not yet been experimentally verified.

2. Limited Availability of Research Across Disability Categories: The reviewed literature focuses mainly on specific disability categories or individual biometric authentication methods. Research addressing a comprehensive, unified authentication framework for people with different types of disabilities remains limited. Consequently, it is difficult to determine whether the proposed approaches can adequately meet the diverse needs of all users with disabilities.

3. Lack of Quantitative Evaluation and Comparative Performance Measurements: Since this study relies on qualitative literature analysis rather than original experimental data, it does not provide statistical evaluations or direct performance comparisons of the proposed biometric methods. Metrics such as recognition accuracy, false acceptance rate (FAR), false rejection rate (FRR), processing time, and user satisfaction have not been measured within this study. Further experimental research is therefore required to assess the performance, security, accessibility, and practical feasibility of the proposed approaches.

5. Conclusion

Overall, the reviewed literature establishes that conventional authentication technologies can create significant accessibility barriers for people with disabilities. Earlier research primarily attempted to replace keyboards and other physical input devices with gestures or alternative interaction mechanisms. Later studies increasingly explored eye-based, AI-supported, and biometric approaches. However, the literature remains largely fragmented, with individual studies focusing on particular disability groups, technologies, or application contexts. The reviewed studies therefore support the need for a comprehensive and disability-aware biometric authentication framework. Such a framework should consider not only biometric recognition accuracy but also accessibility, usability, independence, physical capability, enrollment requirements, and the interaction burden imposed on the user. Existing biometric authentication research for people with disabilities tends to focus on individual disability groups or individual authentication modalities, while limited research has investigated a unified, multimodal framework that systematically selects biometric modalities according to the functional capabilities and accessibility requirements of different disability categories.

References

[1] K. Holloway, R. Al Masri, and A. Abu Yahia, “Digital identity, biometrics and inclusion in humanitarian responses to refugee crises,” HPG Working Paper, Overseas Development Institute (ODI), London, U.K., Oct. 2021.

[2] B. M. Alsellami and P. D. Deshmukh, “The recent trends in biometric traits authentication based on Internet of Things (IoT),” in Proc. 2021 Int. Conf. Artif. Intell. Smart Syst. (ICAIS), 2021, doi: 10.1109/ICAIS50930.2021.9396007.

[3] R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, “Continuous multimodal biometric authentication schemes: A systematic review,” IEEE Access, vol. 9, pp. 34541–34557, 2021, doi: 10.1109/ACCESS.2021.3061589.

[4] M. Gomez-Barrero, P. Drozdowski, C. Rathgeb, J. Patino, M. Todisco, A. Nautsch, N. Damer, J. Priesnitz, N. Evans, and C. Busch, “Biometrics in the era of COVID-19: Challenges and opportunities,” IEEE Trans. Technol. Soc., vol. 3, no. 4, pp. 307–322, 2022, doi: 10.1109/TTS.2022.3203571.
[5] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig, and C. Busch, “Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection,” IEEE Access, vol. 9, pp. 139361–139378, 2021, doi: 10.1109/ACCESS.2021.3118830.
[6] S. A. Abdulrahman and B. Alhayani, “A comprehensive survey on the biometric systems based on physiological and behavioural characteristics,” Materials Today: Proceedings, vol. 80, pp. 2642–2646, 2023, doi: 10.1016/j.matpr.2021.07.005.
[7] World Health Organization (WHO), 2026. [Online]. Available: http://www.who.int/mediacentre/factsheets/fs282/en/
[8] N. K. Bhat, Y. B. Gajara, H. U. Rajgor, and S. P. Ambadekar, “ABHIGYAAN: Source of knowledge for visually impaired using vibrations,” Advances in Computational Sciences and Technology, vol. 11, no. 1, pp. 1–4, 2018.
[9] Z. Rui and Z. Yan, “A survey on biometric authentication: Toward secure and privacy-preserving identification,” IEEE Access, vol. 7, pp. 5994–6009, 2019, doi: 10.1109/ACCESS.2018.2889996.
[10] G. Lavanya, R. Rithika, P. S. Sanjana, and G. K. ShilpaTharani, “EYE-TM: An automatic teller machine for the visually impaired,” in Proc. Int. Conf. Comput., Commun., Electr. Biomed. Syst., 2022, pp. 503–507.
[11] J. S. A. Jeba Sheela, M. S. Meenakshi, N. S. Narmatha, and P. A. Pavithra, “Survey paper on authentication and voice assistance techniques to assist visually challenged people,” International Journal of Real-Time Applications and Computing Systems (IJORTACS).
[12] I. A. C. Iluno, O. C. Okeke, and I. Mgbeafuluike, “Development of a deep learning technology to improve human computer interaction for visually impaired,” International Journal of Real-Time Applications and Computing Systems (IJORTACS), vol. 3, no. 47, pp. 613–627, Oct. 2024. [Online]. Available: http://www.ijortacs.com
[13] M. M. R. Akanda, A. Lacy, and N. Saxena, “SoK: Inaccessible & insecure: An exposition of authentication challenges faced by blind and visually impaired users in state-of-the-art academic proposals,” in Proc. 34th USENIX Security Symp., Seattle, WA, USA, Aug. 2025.
[14] C. Toussaint, B. Chateau, P.-G. Gourio-Jewell, E. Bonnefoy, and N. Louveton, “Inclusive by design: Developing barrier-free authentication for blind and low vision users through the ALIAS project,” in Proc. ECCE 2025, Tallinn, Estonia, 2025, doi: 10.1145/3746175.3746210.
[15] A. B. Prastyo and A. Setyanto, “Analysis of FaceNet and VGG16 for blind face recognition with MTCNN and HaarCascade detection methods,” G-Tech: Jurnal Teknologi Terapan, vol. 9, no. 2, pp. 570–577, 2025.
[16] R. J. Oommen and T. Sharma, “Essential, yet overlooked: Identity verification barriers for blind and low vision people in government services,” arXiv preprint arXiv:2604.28166, Apr. 30, 2026, doi: 10.48550/arXiv.2604.28166.
[17] A. M. Qamar, A. Murad, M. A. Rahman, F. Ur Rehman, A. Ahmad, B. Sadiq, and S. M. Basalamah, “A multi-sensory gesture-based login environment,” in Proc. 23rd ACM Int. Conf. Multimedia (MM ’15), Brisbane, Australia, 2015, pp. 763–764, doi: 10.1145/2733373.2807987.
[18] C. R. Fenner and C. Noteboom, “How wearable technology will replace verbal authentication or passwords for universal secure authentication for healthcare,” in Proc. MWAIS, 2018.
[19] A. Adegbengle, U. Nzenwata, O. Rotimi, A. Oreoluwa, and A. James, “Ethics in biometrics authentication,” GSJ: Global Scientific Journal, vol. 8, no. 9, Sep. 2020.
[20] M. P. Paing, A. Juhong, and C. Pintavirooj, “Design and development of an assistive system based on eye tracking,” Feb. 2022.
[21] R. Aboalela, S. Sebaa, A. Almohamadi, R. Almohammadi, and G. Alzebali, “Hold My Hand application for disabilities,” International Journal on Cybernetics & Informatics (IJCI), vol. 11, no. 4, Aug. 2022.
[22] M. Kamil and S. Khalid, “Real-time Siamese neural network based algorithm for user recognition by their eye blinking,” 2024.
[23] K. Pushpavalli, D. Sathis Pandy, S. Tharun, and K. Sundaramoorthy, “Secure e-voting system with biometric authentication,” in Proc. Int. Conf. Comput. Sci. Commun. Eng. (ICCSCE 2025), Advances in Computer Science Research, vol. 124, 2025, doi: 10.2991/978-94-6463-858-5_275.
[24] M. L. Ali, G. Goldberg, J. Guzman, W. Huang, A. Manuele, and H. Patel, “Keystroke biometric authentication on short numeric input on mobile devices,” 2016, pp. 1–4.
[25] E. J. A. P. C. Chathumali, J. M. U. B. Jayasekera, D. C. Pinnawala, S. M. T. K. Samaraweera, and A. Gamage, “SPEECUR: Intelligent PC controller for hand disabled people using NLP and image processing,” Sri Lanka Institute of Information Technology, Sri Lanka, 2016.
[26] A. Alhayajneh, A. N. Baccarini, G. M. Weiss, T. Hayajneh, and A. Farajidavar, “Biometric authentication and verification for medical cyber physical systems,” Electronics, vol. 7, no. 12, Art. no. 436, 2018, doi: 10.3390/electronics7120436.

[27] B. Lewis, “Designing accessible computing device authentication for people with upper extremity impairment,” Ph.D. dissertation, Dept. Computer Science and Statistics, University of Rhode Island, Kingston, RI, USA, 2023, doi: 10.23860/diss-lewis-brittany-2023.
[28] M. C. Banville, “Am I who I say I am? The illusion of choice: Biometric identification in healthcare,” Ph.D. dissertation, Department of English, East Carolina University, Greenville, NC, USA, 2023.
[29] A. Samraj, N. Mehrdel, and S. Sayeed, “Sign language communication and authentication using sensor fusion of hand glove and photometric signals,” in Proc. 8th Int. Conf. Inf. Technol. (ICIT), 2017, pp. 1–7.
[30] U. Patel and A. G. Ambekar, “Recognition & translation of hand gesture for Indian sign language based on KNN & PNN classifier,” Advances in Computational Sciences and Technology, vol. 11, no. 1, pp. 19–24, 2018.
[31] A. Guo, E. Kamar, J. W. Vaughan, H. Wallach, and M. R. Morris, “Toward fairness in AI for people with disabilities: A research roadmap,” in Proc. ACM ASSETS 2019 Workshop on AI Fairness for People with Disabilities, USA, 2019, pp. 1–4.
[32] S. Nafisah and N. Effendy, “Voice biometric system: The identification of the severity of cerebral palsy using Mel-frequencies stochastics approach,” International Journal of Integrated Engineering, vol. 11, no. 3, 2019.
[33] D. Sangeetha, K. Dharani Dharan, A. C. Krishna, and C. Karthikeyan, “Speech and text conversion system for sign language using ML,” International Journal of Computer Technology and Electronics Communication (IJCTEC), vol. 9, no. 3, May–Jun. 2026, doi: 10.15680/IJCTECE.2026.0903003.
[34] B. Alabduallah, R. Al Dayil, A. Alkharashi, and A. A. Alneil, “Innovative hand pose based sign language recognition using hybrid metaheuristic optimization algorithms with deep learning model for hearing impaired persons,” Scientific Reports, vol. 15, Art. no. 9320, 2025, doi: 10.1038/s41598-025-93559-4.