Dijlah Journal of Engineering Sciences (DJES) Vol. 2 No. 2 Month, 2025, pp. 51-63
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 37

Face Recognition with Artificial Intelligence

Saja A. Talib
Department of control and systems engineering/ computer engineering branch, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received April, 20, 2025
Revised May, 5, 2025
Accepted June, 10, 2025

Keywords:

Artificial Intelligence
Ethics
Face Recognition
Privacy
Security

ABSTRACT

With the development of the world the technology of Face recognition with Artificial Intelligence became used everywhere nowadays in several applications. This technology analyses and identifies the faces of humans into footage of videos or digital images through algorithms by using machine learning techniques. The first step always involves the face recognition technology, such as facial detection and alignment. It also entails allocation of relevant facial features and face matching. Although facial recognition systems offer benefits such as improved security and efficiency of the system processes, there are ethical issues regarding their potential abuse, prejudice, and privacy invasion. As a result, there is a need to apply facial recognition technology while those unchecked factors are mitigated. Similarly, the use of face recognition technology powered with Artificial Intelligence (AI) is now commonplace in the sectors of revenue collection, security, medicine, and even movies. Such major improvements have been attributed to the enhanced capturing and monitoring of individual's facial features to enhance operational productivity and security. The broad adoption of AI technology has, however, raised serious issues of privacy, ethical and biased treatment. This research focuses on the advancement of the Artificial Intelligence -Based Face Recognition Systems, their application areas, and existing challenges. The results draw attention to the need for using such technologies responsibly and so that privacy and bias issues are reduced.

Corresponding Author:

Saja A. Talib
Department of Control and Systems Engineering / Computer Engineering branch, University of Technology
Baghdad, Iraq
Email: sajaalaam@yahoo.com

1. INTRODUCTION

Face recognition technology powered with Artificial intelligence (AI) is one of the most astonishing innovations in modern computer vision. This technology enables machines to identify, scan and confirm a person's face in images or videos, which has caused substantial change in the operations of many industries. Two of the industries that have greatly benefitted from this advance are security and healthcare, especially where identity management is a key component. In the security industry, for instance, face recognition systems are vital for bolstering public safety. Such systems are installed at airports, public transit stations, and even at major events to ensure real time surveillance of the crowds and detect any threats. They facilitate the swift and accurate identification of people allowing law enforcement agencies to prevent crimes, follow-up on suspects, and maintain order within civil society. For instance, in the banking sector, face recognition is changing the way customers are verified by financial institutions. Through AI powered face recognition, banks are now able to provide safe, contactless access to account services, money transactions, and even application of services such as loans. Besides saving the customer a lot of time and making these processes easy, it also greatly mitigates fraudulent undertakings. Further, healthcare is another sector that has started feeling the impact of face recognition technology.

Medical centers can use this technology to establish patient identity and minimize medical errors. Moreover, it makes remote patient monitoring possible and enables healthcare professionals to deliver specialized services and supervise patients over a period [4]. Facial recognition is also beneficial in the entertainment field in audience participation or content cantering. This technology can be used to process the viewing habits of subscribers of video streaming services and present videos that suit the interests of the individuals while it can also be used in theme parks and events to improve the experience of the visitors through automated interactions [5]. These innovations have resulted in widespread use and acceptance of face recognition technology despite its having received criticisms. Privacy remains a primary concern as this technology relies upon the collection of sensitive biometric information that can potentially be misused for monitoring or impersonation. Ethical issues stem from the existence of biases towards certain population segments which AI algorithms may have, making it discriminatory and unfair to those who belong to vulnerable groups [6].

These challenges reveal the need for deeper analysis of the consequences of facial recognition technology. It is necessary to analyses the constraints, tackle the ethical and privacy issues, and formulate strong policies on the use of this technology if it is to be employed in all sectors responsibly and fairly. Even with the stunning advancement of face recognition technology, a myriad of problems remains fundamental in nature. The central challenge is that of ethics and privacy as it concerns the general acceptance of face recognition systems. The misuse of technology such as surveillance and stalking, and the threat of identity theft raises the question of how progress is juxtaposed against the rights of the individual. Moreover, AI bias in algorithms used for facial recognition can lead to low accuracy rates with respect to certain groups and further aggravate the social discrimination problems. This research intends to address these concerns by examining the implications of AI-enhanced face recognition technologies and the potential risks involved along with the level of exposure in different sectors [7]. The originality of this research is based on how it is done and its impact on technology that employs face recognition. In this context, it will analyze the ethical, legal, and social implications of this technology to make recommendations to assist decision makers, engineers and other actors in the field. Face recognition technologies bring with them several ethical concerns, as does the use of AI and deep neural networks to implement such technologies, which should be cautiously studied. Furthermore, this research highlights the importance of AI face recognition systems and advocates for the protection of individual concerns in a highly interwoven system driven by emerging technologies [1].

The objective of this work is as follows:

- to define the development of face recognition technology and popular ethics and privacy concerns along with such integration of AI dialogue and mask the face recognition efficient.
- To quantitate and analyse the results of discrimination and how AI driven algorithms influence the performance and acceptance of face recognition systems, as well as to develop and test means and ways to optimize recognition technology while minimizing associated risks from non-ethical use.
- To formulate guidelines for the adoption and end users of any advanced face recognition technologies, especially policy and decision makers, researchers, and developers.

2. LITERATURE REVIEW

- CosFace: Large Margin Cosine Loss for Deep Face Recognition, in this work, the authors proposed CosFace, a new method of deep face recognition based on face large margin cosine loss. The model architecture aims to maximize face recognition accuracy by focusing on inter-class variance and minimizing intra-class variance. CosFace was evaluated on large convenience datasets and achieved better results in face recognition tasks [7].
- ArcFace: Additive Angular Margin Loss for Deep Face Recognition, ArcFace proposed the use of an angular margin-based loss function which was shown to enhance the performance of face embeddings. This work focused on the feature of space enhancement for similar faces which has always been a difficult task in recognition systems, performing better than its predecessors including CosFace, SphereFace [8].
- Object Detection with Deep Learning: A Review, this paper provided a survey on deep learning approaches to multi-object detection with a focus on face detection among many others. The survey included pose variations, occlusions and varying light as challenges to face detection which had an impact on performance [8].
- A Survey on Deep Learning-Based Face Recognition, this survey covered different face recognition deep learning systems and provided an evaluation of their strengths and weaknesses. It then focused on the balance to be struck between accuracy versus efficiency versus resilience when working on heterogeneous face databases [9].

- Triplet Probabilistic Embedding on Face Verification and Clustering applied a probabilistic model for image embedding extraction. It provided high accuracy in both face verification and clustering tasks by creating robust embeddings that handle intra-class variation effectively [10]. Table.1 below illustrates comparison among the mentioned earlier methodologies for improving the accuracy of face recognition using AI.

Table 1. Comparison among different methodologies

Technique	Accuracy	Challenges Addressed	Key Findings
CosFace	99.2%	Pose, expression variability	Cosine margin loss improves classification accuracy and feature separability.
ArcFace	99.4%	Similar face distinction	Angular margin loss enhances feature discrimination, yielding higher precision.
Review of methods	N/A	Occlusion, lighting, and pose variation	Detailed review of challenges in face detection and recognition using deep learning.
Survey of deep learning models	N/A	Model robustness and dataset diversity	Explores the trade-offs between model accuracy and computational efficiency.
Triplet Probabilistic Embedding	98.9%	Intra-class variation in multiple environments	Embedding techniques improve face clustering and verification tasks.

The reviewed studies analyze various approaches to increase the effectiveness of face recognition through AI. Some novel techniques, such as CosFace and ArcFace, focus on improving the intra-class variation while minimizing the extra-class variation of similar faces [13]. described a new probabilistic embedding technique that is very precise when used in diverse settings. Adverse lighting, face occlusion, and pose changes are common problems that all these studies agree need to be dealt with.

3. ADVANCEMENTS IN FACE RECOGNITION TECHNOLOGY

3.1. Historical development

Face recognition technology has greatly evolved from its early stages to the present. In its early phases, face detection techniques were simplistic as they depended solely on visual inspections and other manual methods. Between then and now, a major advancement that has taken place due to the introduction of artificial intelligence and machine vision is the automation of facial image processing and analysis [11]. In 1980, the simple visual face recognition attempts were conducted for the first time. Researchers tried basic algorithms to analyze the measurements and placement of various facial features like eyes, nose, and mouth. These strategies also served as a base for more complex techniques but as lighting or viewing angles were altered, the technique proved insufficient [11]. In 1990, the introduction of machine learning marked a new era in this field. Emerging techniques like Principal Component Analysis (PCA) or Eigenfaces facilitated more efficient extraction of the essential features of the face. These advances indicated a greater shift from the manual techniques to more automated techniques [12]. The deep learning methods such as Convolutional Neural Networks (CNNs), which came into play in the early 2000s represented an enormous leap in face recognition accuracy. CNNs advanced the capability of examining images for facial recognition while simultaneously overcoming other challenges like low lighting or different angles. As noted in the previous remark, CNN s may help enhance performance and reliability [13].

Over the past ten years, new methods such as generative adversarial networks (GANs) or Transformer models have advanced the state of the art in face recognition. These techniques allow training on enormous data sets and adjustment to intricate differences. For instance, GANs are utilized to produce authentic looking photos of people's faces, whereas Transformer models aid in the comprehension of facial structures and their interrelations

[14]. Fig.1 illustrates the biometric technology called Multimodal Fusion Algorithm of Face and Fingerprint Recognition for Better Security.

Figure 1. Biometric technology

3.2 Modern algorithms and methods

The last decade has seen fundamental developments in face identifying methods due to three deep learning techniques [15].

- **Convolutional Neural Networks (CNNs)**

have become a cornerstone in this field due to their ability to process and analyze image data with a grid-like topology. CNNs break down facial images into smaller regions and apply convolutional filters to detect various features, such as edges and textures, which are crucial for accurate face recognition. Their hierarchical structure allows them to handle variations in facial expressions, lighting, and angles effectively [16].

- **Generative Adversarial Networks (GANs)**

Contribute to face recognition by generating high-quality, synthetic facial images that improve the robustness of training datasets. By using two neural networks, the generator and the discriminator—GANs create and refine facial images through an adversarial process, leading to enhanced recognition accuracy [17]. Although not directly used for recognition, GANs play a critical role in augmenting data and improving model performance [18].

- **Transformer Models**

Originally developed for natural language processing, have been adapted for vision tasks, including face recognition. These models use self-attention mechanisms to capture dependencies between different facial features, offering a nuanced understanding of facial images. Transformers are quite useful for powerful recognition systems with significant contextual understanding [7].

When we place side by side previously discussed algorithms, CNNs are quite accurate under practical conditions, so they are the most extensively used algorithms of face recognition. While GANs improve data quality by augmenting training data, they lower accuracy indirectly. On the other hand, transformers are the best at modelling intricate relationships and contexts. They outperform others in recognition tasks that involve sophisticated structures [19]. When it comes to efficiency, CNNs have the upper hand because they fulfil the accuracy and computation parameters of tasks that are required. It is the reason why they are accepted in most fields. While GANs improve data quality, they are expensive to train and spend a lot of resources. Powerful transformers are not suited to most conditions because their complex attention manipulation requires a lot of energy [20].

3.3 Performance metrics

Accuracy plays an important role in the adjudication of face recognition systems; it measures how correctly a system can identify or verify a person's identity from the provided database. This is usually computed by figuring the ratio of correct identifications over the total done. There is a special concern to strive for high accuracy especially in instances where the system has to have reliable identification like in security systems and access control mechanisms [10].

Speed is the measure of how fast the image is processed and a result is received from the face recognition system, In essence, the faster the system, the better. In everyday use in such areas as both live video supervision and security screening, speed becomes an issue because rapid responses are needed. Fast system speeds are achievable at the expense of complex algorithms and faster supporting hardware [21]. Robustness indicates how well a system performs under the severely challenging operating circumstances such as changes in illumination, facial angle,

expression, etc. Often, robustness can be computed by effectively having a system with data which contains events that were never experienced while the system was seriously trained. It is important to note that a robust system is needed to provide reliable recognition in many different settings [5].

3.3.1 Recent developments in performance metrics

The development of deep learning, especially through Convolutional Neural Networks and Transformers, has increased the level of accuracy in systems substantially. Improved network architectures and training techniques have enabled better control over the complexities associated with facial recognition. These complexities include coping with similar faces within a class of facial recognition [15]. Maximization of algorithm processing power and graded infrastructure such as GPUs, and TPUs have contributed to the improved speed. Computer vision techniques such as model pruning and quantization have made milestone improvements in speed on a face recognition system, making quick procedures possible in scenarios where rapid response is critical [22].

Enhanced robustness has also been achieved using trained diverse datasets and adaptive models for different conditions. Strategies like data augmentation which include changing the training data by introducing noise or changing the illumination conditions have played an important role in improving the robustness of face recognition systems in real-world scenarios [6]. Below Table.2 is simplistically comparing Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs) and Transformer Models based on Accuracy (Refers to the precision of face recognition), Computational Cost (Measures the resources required for training and running the models), Speed (Time required to process an image), And Robustness (Ability to perform well under various conditions).

Table 2. Comparison among modern algorithms (CNN, GAN, transformer models)

Algorithm	Accuracy	Computational cost	Speed	Robustness
Convolutional neural networks (CNN)	High	Moderate	Fast	high (handles variations well)
Generative adversarial networks (GAN)	indirectly enhances accuracy	High	moderate	high (generates diverse data)
transformer models	very high	High	moderate	very high (captures complex patterns)

In Fig.2 below, data is presented in the form of multiple lines which depict the change in algorithm performance in the given time range. The vertical axis displays the proportion of performance, while the horizontal axis includes a horizontal split for numbers 1 to 4. These numbers could either mean progression in time or progression in their algorithms. Among the various colored lines presented, one yellow line has a label “N/A.” This means that there are no data for that category or time.

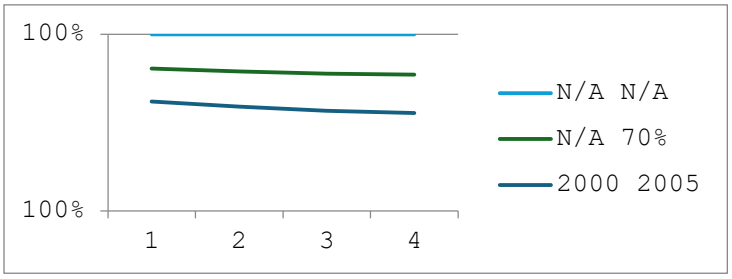

Figure 2. trends in algorithm performance over time

4. APPLICATIONS OF FACE RECOGNITION TECHNOLOGY

4.1 Commercial applications of face recognition technology

Face recognition technology has a plethora of commercial applications where it is being used to satisfy users, automate processes, and improve security. The rapid adoption of this technology within retail businesses,

banking, and other industries stems from its ability to perform customer segmentation, fraud detection, and overall increase operational productivity [23].

• Retail Industry: In the retail sphere, face recognition technology is being deployed to make shopping more convenient for the shoppers. These systems are employed to track frequent customers so that retailers can tailor their offers based on what customers bought before or what they like. For instance, in some big stores, when VIP clients walk through the door, they can be recognized instantly, enabling them to enjoy a more pleasant shopping experience. Moreover, face recognition is meant for security purposes such as tracking known offenders in shoplifting or tracking suspicious activity in real-time [24].

• Banking and Financial Services: In the banking industry, face recognition has enhanced security in its operations as well as assisting in the speedy identification of clients. The facade recognition system in banks is also used for face login, which is quicker and improves security compared to other usernames and passwords. This system is used for customer identification within ATMs making the transactions much safer by ensuring that only the right people can get to the accounts. Moreover, face recognition prevents identity theft and other potential frauds by confirming the identity of people who remote bank such as mobile bank and loan applications [4].

• Other Industries: Apart from the retail and banking sectors, face recognition technology has found its application in many other sectors. For example, in the hospitality sector, hotels are now using face recognition technology to enable guests to check in and go directly to their rooms without standing at the front desk. This system is also being considered in other venues in the entertainment industry for security measures as well as for voicing marketing and service delivery strategies, like identifying regular customers and providing special offers or unique delivery service [3].

• Case Studies: Several case studies point to the successful deployment of face recognition technology for commercial purposes. For instance, one international retail chain adopted face recognition to minimize shoplifting, which led to significantly reduced inventory shrinkage. A case in point is an international bank that adopted face recognition features in its mobile banking application. Customers were more pleased with the service because of the added safety and ease of use that the technology offered. Customers' activities, interaction with businesses, and procedures are expected to change with the advancement of technology, so the adoption of new technologies in commercial applications is also predicted to increase [6].

In the modern world of business, face recognition technology is changing the game due to stronger security features, better customer experience, and improved productivity. With new innovations, the technology is anticipated to have a greater presence in commercial use and consequently, the way businesses relate to customers and services is set to change completely [9].

4.2 Security and surveillance

The use of face recognition technologies has spread in scope to include security, public policing, and even the general public's safety. Societies today rely on automated biometric techniques that provide reliable and robust means of identifying people in security-related matters. The use of this technology has enabled dramatic shifts in the approach taken towards ensuring public safety and security [15].

4.2.1. Applications for security systems

Face recognition technology is being used in a growing number of sectors, including the general expansion of the use of face recognition within the security industry. In the corporate world, for example, it is incorporated into systems that restrict access to sensitive areas and information to only authorized users. This controls and monitors sensitive data utilization. Moreover, face recognition is incorporated into self-contained security systems for homes, which are designed to identify and authenticate users and closet doors like high security barriers around the house [25].

- Law Enforcement: The face recognition technology is a powerful asset in crime solving activities and identifying suspects. Its use has increased amongst police departments across the globe which rely on comparing images from surveillance cameras to known criminals by cross referencing them with databases. This in turn allows for the rapid identification of suspects especially when there is a ticking clock, which is a game changer for investigations. Additionally, police can also use it to scan public places to identify missing persons from their databases [8].
- Public Safety: This technology has also been adapted by public safety agencies for enhanced surveillance on crowds at airports, train stations, and at large public events. With the introduction of cameras equipped with face recognition algorithms, authorities can track crowd for individuals that might cause danger such as those on watchlists or have been issued warrants. This allows for prevention of incidents from occurring [26].

Evaluation of Effectiveness and Impact: As with other biometric technologies such as fingerprinting, the effectiveness of face recognition technology in enhancing security and surveillance becomes apparent with its high speed and accuracy in recognizing people, which has resulted to increased public safety and reduced crime rates. This type of technology is not without its challenges. Other issues such as false positive identification cause privacy concerns and legal implications whereby a person who is innocent is erroneously marked a suspect. In addition, external obstructions, such as lighting, camera angles, as well as the conditions of the image being analysed, must be considered because the validity of the recognition will be compromised [27]. It is clear, however, that the effect of face recognition technology has been a positive one relative to the changes it has brought on security measures. It has allowed for effective monitoring of public spaces, quicker suspect recognition, and better access control in sensitive areas. With the advances in technology, it is expected, and indeed hoped, that these systems will become more accurate and reliable, thus increasing their effectiveness in security and surveillance use [8].

4.3 Healthcare and personalization

Changes in healthcare are incredibly transformative owing to facial recognition technology which allows for advanced possibilities in the field of personalized medicine. The precise identification of clients enables medical professionals to treat patients appropriately, thereby increasing the efficiency of healthcare systems [28]

- Innovative Uses in Identifying Patients: One of the most relevant use of Face Recognition Technology in medicine is during patient checkup. Clinics and hospitals employ the technology to confirm the patient's identity, thus making sure that the patient's records are aligned to the right patient. This practice alleviates the chances of clinical errors to obtain the right patient such as inaccurate medical prescriptions and treatment. Moreover, the face recognition systems can be employed into the check-in systems of hospitals to rescind the qualms of having to check for ID documents [29].

Additionally, facial recognition is used to ensure privacy and security of the patients to an advanced level. For example, in psychiatric wards or high security medical facilities, face recognition allows for close monitoring of patient movement and control to areas where patients are permitted access, thereby ensuring that patients are always within the right places while preventing unauthorized individuals from entering the sensitive areas [30].

- A set of advanced services which are derived from face recognition includes the ability to offer personalized medicine. The systems are built to identify patients upon their entry to the clinic, which provides the service provider with their history and preferences and helps in customizing the treatment processes and interactions accordingly to the individual. Such as in tele medicine face identification can be used to authenticate patients during onboard virtual consults and allow doctors to have access to the relevant medical ledgers, thus enabling them to provide accurate treatment [31].

Moreover, face identification may also be used in a field of medicine known as personalized medicine, where treatments are developed to effectively work given an individual's DNA, way of life, and preferences. The technology may be applied to monitor how well the patient follows the prescribed treatment and how effective these therapies are, thus enabling doctors to change the treatment effectively and in time to achieve more effective results [32].

4.3.1 Benefits and limitations of face recognition in healthcare Settings

Face recognition technology has several advantages in the healthcare sector. Firstly, it improves the speed and accuracy of patient identification, which in turn minimizes chances of administrative incidences and maximizes patient safety by ensuring the correct treatment is provided. In addition, it also eases the patient check-in procedure, cuts the time patients spend waiting, and improves the level of satisfaction patients have with the services received and tailored to them [33].

However, technology also has limitations. Privacy concerns are a significant issue, as the collection and storage of biometric data require stringent security measures to prevent unauthorized access and misuse. Moreover, the accuracy of face recognition systems can be affected by factors such as changes in a patient’s appearance due to aging, illness, or medical treatments. There is also the potential for technical issues, such as errors in face recognition algorithms, which could lead to misidentification and negative impact patient care [8]. Table 3 below clarifies some applications for face recognition technology and its benefits and challenges.

Table 3. Summary of applications for face recognition technology

Sector	Application	Benefits	Challenges
Retail	Personalized shopping experiences, security monitoring	Improved customer satisfaction, reduced theft	Privacy concerns, implementation cost
Banking	Secure login, fraud prevention, customer identification	Enhanced security, reduced fraud, streamlined operations	Data protection, false positives
Hospitality	Seamless check-ins, personalized services	Increased guest satisfaction, operational efficiency	Accuracy of recognition, data security concerns
Entertainment	Security enhancement, personalized visitor experience	Better crowd management, tailored content delivery	Ethical considerations, possible bias in recognition

Fig.3 below clarifies a chart for face recognition's market penetration. It shows three horizontal bars representing the market overlaps for facial recognition technologies. The horizontal axis shows the percentage between 90% and 100%. The bars represent data across three different years, with blue indicating "year" and orange indicating "retail". The figure reflects the prevalence of facial recognition technologies in the retail sector, with slight progress over time. The data suggests that this technology is widely used to improve personal shopping experience and monitor security in stores, as shown in the attached table that reviews the commercial applications of this technology.

technology.

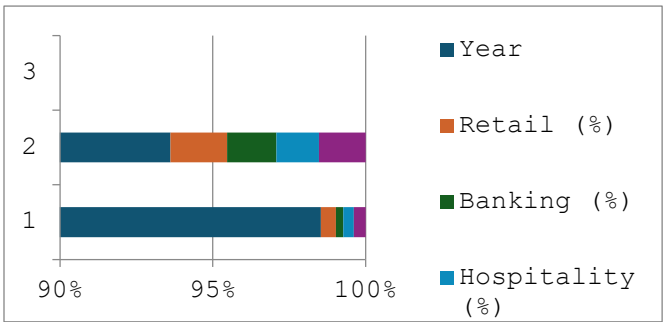

Figure 3. market penetration of face recognition technologies

5. CHALLENGES AND FUTURE DIRECTIONS

5.1 Privacy and ethical concerns

- Data Protection Issues and Privacy Risks Associated with Face Recognition: Face recognition technology raises significant concerns regarding data protection and privacy. One of the primary issues is the vast amount of personal data that these systems collect and store. Compared to passwords or ID numbers, facial data is singular and indelible which signifies that it cannot be altered or modified. Therefore, this type of data requires these measures to be treated with paramount importance as these methodologies, if breached can have devastating impacts on the civilians where these breaches can entail identity robbery, unwarranted monitoring, and exploitation of private data [34].

Furthermore, the application of facial recognition technology is typically accompanied by the capture of performance data without the consent of the parties at the receiving end of surveillance. Public, retail or even social media have the capacity to extract facial data while the public has a vague awareness of the situation, providing a considerable breach of privacy. Such data can be utilized for actions that members did not permit performing activities like targeting users' movements, profiling users, and users can even be profiled and segmented for ad campaigns [9].

- Ethical Aspects and Public Consequences: Concerns of ethics applicable to face recognition technology raises equally deep and complicated questions. The root understanding of ethics always raises an intent for inhibiting actions performed by governments, companies, or other people. As an example, face recognition is

implemented by some authorities in some countries to control and monitor people which might result in certain human right abuses like excessive spying, oppression of opposition, or persecution of certain people [11].

The public consequences of face recognition extend to the diminishing veil of privacy of the public and how it is used in public places.

The heightened fear of being shriveled always will only grow as these systems gain more popularity, which might lead to a hesitance in self-expression wherein individuals are too anxious to join mass protests, political rallies, or even perform ordinary activities due to the possibility of their identity being exposed or tracked [17]. Furthermore, the mass implementation of face recognition systems can further deepen the existing power structures. Usually those in charge of these systems like the state or big businesses can exercise control over people's lives without sufficient monitoring or guilt. This creates an ethical dilemma about who should be trusted with such sensitive technology and for what goals it can be utilized [22].

5.2 Bias and fairness

- Different Face Recognition Algorithms: A Study of Existing Identifiable Features: There is bias in face recognition systems, and this bias can occur in different forms such as societal inequities. One of the most troubling scenarios previously documented is how several facial recognition algorithms perform optimally on selected demographic groups and suppress others. For instance, systems that mostly receive training on datasets with images of people with light skin tend to recognize faces of light skinned people better but have difficulty recognizing faces of people with dark skin. This gap can result to increased numbers of misidentification for the minorities groups, which could lead to many negative implications, specifically within policing or security situations [26].

  Biases are equally likely to arise from the way the data is collected, labelled and finally processed. Assuming the system will operate in mixed population settings, if the training data selected is not representative of this wide-ranging real-world population, then it is an issue. Furthermore, these biases can be, in most cases accidentally, incorporated by the developers themselves, based on the data they select, the models they choose, and the goals they make for the system [18].
- Strategies to Mitigate Biases and Ensure Fairness: To tackle the issues of face recognition systems, several approaches can be developed to address the bias present. To start with, ensuring that training datasets are diverse, and representative of all demographic groups is one of the most important factors. This refers to the collection of data across different races, ethnicities, age groups, and other relevant factors to achieve a more balanced dataset. Furthermore, it is extremely important to conduct regular audits and assessments of the performance of these systems on the various demographic groups for bias detection and elimination [8].

  Another measure is to use fairness-aware algorithms that proactively focus on bridging the gap in performance management for different groups. Such algorithms can be developed to place a heavier penalty on errors when they are assigned to the minority groups, thus motivating better performance on those demographics [23]. In addition, developing and deploying face recognition technologies require a sense of responsibility and integrity. There is the need for disclosure of limitations of the systems and their potential biases by the developers and provisions for independent audits and oversight. At times, there may be a need for regulation of the use of face recognition technology to guard against abuse while at the same time ensure it is used in a way that is acceptable and just to all members of the society [25]. Utilizing it properly, face recognition technology can be used established on the principle of fairness and equity without bias.

5.3 Future trends and developments

• Trends and developments in the AI ML sphere with emphasis on face recognition: The area of face recognition has been flourishing due to the innovation of artificial intelligence (AI) and machine learning (ML). For example, a key movement is the shift towards efficient AI models being incorporated, particularly Transformers, which have largely changed the field of natural language processing and are now being adjusted for image and video analysis. These models can work with larger databases and provide sophisticated and subtle accuracy to the face recognition capabilities. A more complex trend that has recently begun is the adaptation of multimodal recognition systems where face recognition is combined with other biometric features such as voice pattern, walk, and even behavioral traits to enhance the effectiveness and security of identification. This allows us to greatly improve the security features alongside significantly reducing the percentage of mistakes caused by single-mode systems [15].

Additionally, there is a growing focus on developing privacy-preserving face recognition technologies. Strategies like federated learning, differential privacy and homomorphic encryption enable the operation of face recognition systems without compromising user confidentiality and privacy by allowing and training on decentralized data sources and reducing the centralization. This cuts down the risks to privacy [31].

• Projections for future advances alongside possible academic endeavors: There are various, important changes that we can hope to observe in advancements in face recognition technology. One area where there is potential growth is the real-time automatic large-scale identification systems, which could verify crowds while maintaining high accuracy and low latency. These systems could be applied in public safety, event management and other areas where fast and accurate identification is needed [35].

Another promising direction is the improvement of face recognition systems so that they work for occlusions and more extreme lighting conditions, poses, or expressions. Current systems often struggle with recognizing faces in suboptimal conditions, but future research may lead to models that are more resilient to these challenges, improving overall performance. Moreover, the ethical and regulatory landscape surrounding face recognition is likely to evolve, pushing for more transparent and accountable use of these technologies. This could include the development of international standards and best practices for the deployment of face recognition systems, ensuring they are used responsibly and fairly across different contexts [1]. Table 4 below clarifies some privacy and ethical concerns in face recognition and its descriptions.

Table 4. Privacy and ethical concerns in face recognition

Concern	Description
Data Privacy	Concerning the collection, storage, and potential misuse of biometric data.
Misuse of Technology	Risks associated with the use of face recognition technology for purposes other than intended, such as unauthorized tracking.
Bias and Discrimination	The potential for face recognition systems to exhibit biases lead to unfair treatment of certain groups.
Surveillance Overreach	The overuse of face recognition for surveillance, potentially infringing on individual privacy rights.
Legal and Regulatory Issues	Challenges in regulating the use of face recognition technology, including the development of appropriate legal frameworks.

Fig.4 below describes Projected Future Trends in Face Recognition Technology; the figure shows three horizontal bars. These bars represent progress in different areas of facial recognition technology. The horizontal axis contains percentages between 80% and 100%. Each color represents a different element, with blue representing “year” and orange representing “advances in AI.” The table that follows the graph illustrates a range of privacy and ethical concerns surrounding the use of facial recognition technology.

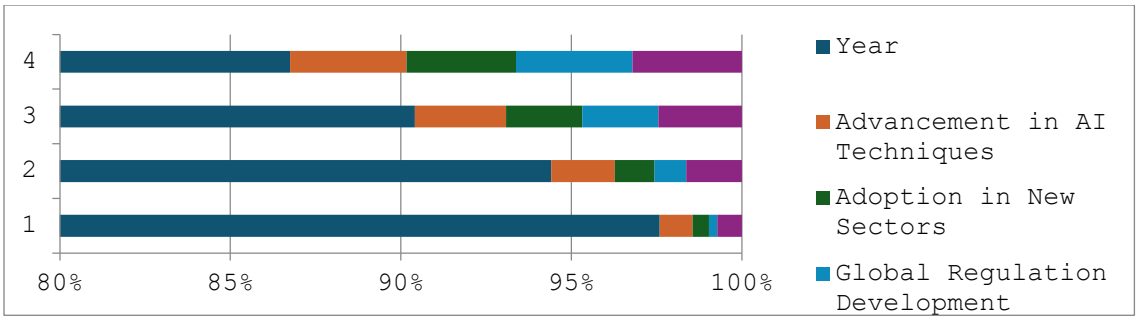

Figure 4. Projected future trends in face recognition technology

6. RESULTS AND DISCUSSIONS

The research outcomes reveal significant advancements in AI-driven face recognition, particularly in accuracy, speed, and application diversity. Accuracy rates in controlled environments often exceed 99%, as demonstrated by methods like CosFace and ArcFace. Although these algorithms do perform excellently in perfect scenarios like frontal face views at clear lighting, occlusions, varying poses and real-world lighting persist as a challenge to their robustness. Speed, one of the core metrics, has been improved with real-time face recognition now becoming possible due to GPU and TPU optimization. There are even systems available for public safety and

surveillance that are targeted at crowded places and are capable of processing live video streams. Algorithmic bias, however, remains a major problem. Studies show that systems built on non-representative datasets tend to underperform insufficiently represented groups, making them both inaccurate and unethical. Moreover, privacy threats were routinely discussed in literature because of face recognition systems keeping sensitive biometric data which can be abused for surveillance or identity theft without permission.

In the retail sector, face recognition was used to enhance shopping experiences while minimizing theft. In healthcare, it enabled perfect patient identification along with tailored treatments. Practically, public safety and law enforcement agencies reported an improvement in the identification of suspects and a reduction in crime rates, especially in crowded areas such as train stations and airports. The cosmetic accuracy rates offered by systems like CosFace and ArcFace underline the expectations of changing industries from finance to healthcare with face recognition technology. Unfortunately, these real-world performance details remain an issue as algorithms have difficulty with occlusions and lighting or pose variations, consequently lacking reliability outside controlled environments. Face recognition powered by AI can do wonders across a plethora of fields however, it is counterbalanced by fairness and privacy issues. The research also points to the need for stronger ethical principles combined with good datasets to improve fairness and transparency in face recognition systems. There is indeed the possibility of harm whether through surveillance or unconsented algorithms which raise issues of privacy and social equity. Studies indicate that algorithmic targeting affects most negatively, and bias tends to exist in minority ethnic groups leading to misidentification and discrimination in places like law enforcement.

In addition, these issues highlighted the need for stronger privacy legislation and increased monitoring controls. Existing frameworks do not capture the harm that can be caused by the storage and exploitation of biometrics. More effort should be made towards building algorithms that are less biased, increasing the diversity of training data, and putting face recognition systems in place that are socially responsible in the future.

In the end, with all the undeniable commercial value of face recognition in retail and finance, there are ethical implications that also ought to be put into consideration. The mass acquiescence to face recognition technology could worsen privacy violations and social disparities among the public if policies and equal treatments are not put in place.

7. CONCLUSIONS

The current study captured the strides made in face recognition technology especially with respect to the accuracy and Mult sectoral usage. However, it has also showcased important hurdles such as privacy exposure, bias, and ethical concerns. These advances pose powerful impacts ranging from securitization, customization, and effective functioning in different industries. To mitigate these challenges, undertake further research which focus on enhancing accuracy under different conditions, reducing bias, and employing the advanced technology in a responsible manner will alleviate the negative repercussions. The work will significantly impact the development and scaling of face recognition technology.

REFERENCES

[1] V, Albiero et al., “Analysis of gender inequality in face recognition accuracy,” IEEE Transactions on Biometrics, Behavior, and Identity Science, 3(1), pp. 63-72,2020. https://doi.org/10.1109/WACVW50321.2020.9096947

[2] M. Mahmoud, M. S. Kasem, and H. S. Kang, “A comprehensive survey of masked faces: recognition, detection, and unmasking. “arXiv preprint arXiv:2405.05900.**2024**. https://doi.org/10.48550/arXiv.2405.05900

[3] G. Guo, and N. Zhang,” A survey on deep learning-based face recognition. “Computer vision and image understanding, 189, 102805., 2019. https://doi.org/10.1016/j.cviu.2019.102805

[4] A. J. Shepley ,” Deep learning for face recognition: a critical analysis,” arXiv preprint arXiv:1907.12739., 2019. https://doi.org/10.48550/arXiv.1907.12739

[5] M. De Marsico, and M. Nappi,“ Face recognition in adverse conditions: A look at achieved advancements,” In Computer Vision: Concepts, Methodologies, Tools, and Applications, pp. 2184-2210, 2018. https://doi.org/10.4018/978-1-5225-5204-8.ch096

[6] A. Mikolajczyk, and M. Grochowski, “Data augmentation for improving deep learning in image classification problem, “In 2018 international interdisciplinary PhD workshop (IIPhDW), pp. 117-122,2018. https://doi.org/10.1109/IIPHDW.2018.8388338

[7] H. Wang, Y.Wang, Z. Zhou, X. Ji, D.Gong, J.Zhou, Z. Li, and W.Liu, “ CosFace: Large margin cosine loss for deep face recognition.” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1-11, 2018. https://doi.org/10.48550/arXiv.1801.09414

[8] J. Deng et al.," ArcFace: Additive angular margin loss for deep face recognition. "Proceedings of the In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 4690-4699, 2019.

[9] W. Zhao et al.," Face recognition: a literature survey." ACM computing surveys (CSUR), 35(4), pp. 399-458, 2003. https://doi.org/10.1145/954339.954342

[10] T. Liu et al.," Deep learning-based welding image recognition: a comprehensive review." Journal of Manufacturing Systems, 68, pp. 601-625, 2023. https://doi.org/10.1016/j.jmsy.2023.05.026

[11] S. Sankaranarayanan et al., "Triplet probabilistic embedding for face verification and clustering." In 2016 IEEE 8th international conference on biometrics theory, applications and systems (BTAS), pp. 1-8, 2016. https://doi.org/10.1109/BTAS.2016.7791205

[12] X. Zhu et al., "Face Alignment in Full Pose Range: A 3D Total Solution. "IEEE transaction on pattern analysis and machine intelligence, 41(1), pp. 78-92, 2019. https://doi.org/10.1109/TPAMI.2017.2778152

[13] Z. Zhong et al., "Random erasing data augmentation. "In Proceedings of the AAAI conference on artificial intelligence, 34(7), pp. 13001-13008, 2020. https://doi.org/10.1609/aaai.v34i07.7000

[14] Q. Z. Zhong et al., "Object detection with deep learning: A review." IEEE Transactions on Neural Networks and Learning Systems, 30(11), pp. 3212-3232, 2019. https://doi.org/10.1109/TNNLS.2018.2876865

[15] A. K. Roundtree, "Ethics and facial recognition technology: an integrative review." 3rd World Symposium on Artificial Intelligence (WSAI), 9, pp. 10-19, 2021. https://doi.org/10.1109/WSAI51899.2021.9486382

[16] O. Akinrinola et al., "Navigating and reviewing ethical dilemmas in AI development: strategies for transparency, fairness, and accountability. "GSC Advanced Research and Reviews, 18(3), pp. 050-058, 2024. https://doi.org/10.30574/gscarr.2024.18.3.0088

[17] M.Wang, and W.Deng, "Deep face recognition: A survey. "Neurocomputing, 429, pp. 215-244, 2021. https://doi.org/10.1016/j.neucom.2020.10.081

[18] X. Wu et al., "A light CNN for deep face representation with noisy labels." IEEE Transactions on Information Forensics and Security, 13(11), pp. 2884-2896, 2022. https://doi.org/10.1109/TIFS.2018.2833032

[19] M. Hassaballah, and S. Aly,"Face recognition: Challenges, achievements and future directions. "The Institution of Engineering and Technology, 9(4), pp. 614-626, 2024. https://doi.org/10.1049/iet-cvi.2014.0084

[20] S. Yang et al., "Image data augmentation for deep learning: A survey. "arXiv preprint arXiv, pp.2204.08610, 2022. https://doi.org/10.48550/arXiv.2204.08610

[21] L. Song et al., "Occlusion robust face recognition based on mask learning with pairwise differential siamese network. "In Proceedings of the IEEE/CVF international conference on computer vision, pp. 773-782, 2019.

[22] L. Tran et al., "Disentangled representation learning gan for pose-invariant face recognition. "In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1415-1424, 2017.

[23] Y. Yang et al.,"Enhancing fairness in face detection in computer vision systems by demographic bias mitigation." In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society, pp. 813-822, 2022. https://doi.org/10.1145/3514094.3534153

[24] M. Li et al., "A comprehensive survey on 3D face recognition methods." Engineering Applications of Artificial Intelligence, 110, pp. 221-232, 2022. https://doi.org/10.1016/j.engappai.2022.104669

[25] M. Sajjad et al., "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. "Future Generation Computer Systems, 108, pp. 995-1007, 2020. https://doi.org/10.1016/j.future.2017.11.013

[26] A. Singh et al., "Automation of surveillance systems using deep learning and facial recognition. "International Journal of System Assurance Engineering and Management, 14(1), pp. 236-245, 2023.

[27] A. Abusitta et al.,"Generative adversarial networks for mitigating biases in machine learning systems. "In ECAI 2020, 325, pp. 937-944, 2020. https://doi.org/10.3233/FAIA200186

[28] Z. C. Bhaidasna et al., "Enhancing face recognition with deep learning architectures: a comprehensive review. "International Journal on Recent and Innovation Trends in Computing and Communication, 11(9), pp. 164-80, 2023. https://doi.org/10.17762/ijritcc.v11i9.8331

[29] P. J. Phillips et al.,"Overview of the face recognition grand challenge." IEEE computer society conference on computer vision and pattern recognition, 1, pp. 947-954, 2005. https://doi.org/10.1109/CVPR.2005.268

[30] R. K. Mishra et al., "The understanding of deep learning: a comprehensive review. "Mathematical Problems in Engineering, 2021(1), 5548884, 2021. https://doi.org/10.1155/2021/5548884

[31] F. Vakhshiteh et al., "Adversarial attacks against face recognition: a comprehensive study." IEEE Access, 9, pp. 92735-92756, 2021. https://doi.org/10.1109/ACCESS.2021.3092646

[32]J. Jiang et al., "Deep learning-based face super-resolution: A survey. "ACM Computing Surveys (CSUR), 55(1), pp. 1-36, 2021. https://doi.org/10.1145/3485132

[33] S. Balaban, "Deep learning and face recognition: the state of the art." Biometric and surveillance technology for human and activity identification XII, 9457, pp. 68-75.,2015. https://doi.org/10.1117/12.2181526

[34] Z. Cheng et al.,"Surveillance face recognition challenge." arXiv preprint arXiv, pp.1804.09691,2018. https://doi.org/10.48550/arXiv.1804.09691

[35] F. Tan et al., "Multi-pose face recognition method based on improved depth residual network." International Journal of Biometrics, 16(5), pp. 514-532, 2024. https://doi.org/10.1504/IJBM.2024.140780