International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 6 Issue 3, March 2025

A Biometric Revolution in the Age of Artificial Intelligence: Face Recognition Technology

Nitish Verma[1], Aniket Kumar[2], Mr. Ankit Sharma[3]
School of Computer Science and Engineering, Galgotias University[1]
School of Computer Science and Engineering, Galgotias University[2]
Assistant Professor, School of Computer Science and Engineering, Galgotias University[3]
Email: nitish.21scse1280031@galgotiasuniversity.edu.in[1],
aniket.21scse1330002@galgotiasuniversity.edu.in[2], sharma.ankit@galgotiasuniversity.edu.in[3]

Abstract: *This paper provides a comprehensive exploration of the underlying principles, real-world applications, existing limitations, and prospective advancements in face recognition technology, emphasizing the need for secure and ethical implementation in modern digital ecosystems. Face recognition technology has emerged as a transformative innovation in the field of biometric authentication, offering a reliable, efficient, and non-invasive method for personal identification and verification. By leveraging advancements in computer vision and deep learning, particularly Convolutional Neural Networks (CNNs), this technology enables the detection, extraction, and comparison of unique facial features from static images and real-time video streams. The facial recognition process typically involves key stages such as face detection, feature mapping, and encoding of facial landmarks into numerical embeddings, which are then matched against a pre-existing database for identification or verification purposes. Its applications span a broad range of domains, including surveillance, law enforcement, airport security, mobile device unlocking, and commercial services such as targeted advertising and customer analytics in retail environments. Despite these benefits, several challenges continue to hinder optimal performance, especially under variable lighting conditions, facial occlusions (e.g., glasses, masks), aging, and changes in expression. Furthermore, the widespread deployment of facial recognition systems has raised significant ethical and legal concerns related to data privacy, consent, and algorithmic fairness. Recent developments have aimed to address these issues through innovations like liveness detection to prevent spoofing, and multi-modal biometric systems that combine facial recognition with other biometric inputs such as iris or voice recognition. These advancements promise to enhance both the robustness and security of identity management systems. As research continues to evolve, balancing technological capability with ethical responsibility remains critical.*

Keywords: *Face Recognition, Technology, Biometric Authentication, Deep Learning, and Privacy Concerns.*

1. Introduction

Face recognition technology has emerged as a paramount innovation within the ambit of biometric authentication. It offers a paradigm shift from conventional security systems by enabling seamless, non-contact identification and verification of individuals through the analysis of distinctive facial features. This transformative technology leverages advanced methodologies in computer vision, machine learning, and, most significantly, deep learning to

interpret and classify human faces with remarkable precision and efficiency. As societal reliance on intelligent systems continues to deepen, face recognition has evolved from a niche innovation into a ubiquitous tool with far-reaching applications across national security, law enforcement, financial services, healthcare, and consumer technology ecosystems.

At its core, a facial recognition system functions through a meticulously sequenced process encompassing three primary stages: face detection, feature extraction, and pattern matching. Face detection constitutes the initial phase, wherein the system scans digital images or video streams to identify and localize human faces. Advanced algorithms, often based on Haar cascades or modern deep learning models such as YOLO (You Only Look Once) or MTCNN (Multi-task Cascaded Convolutional Neural Network), enable high-speed detection across varied environmental contexts. Subsequent to detection is the feature extraction phase, during which the system isolates and analyzes key facial landmarks—such as the interocular distance, nasal bridge curvature, cheekbone prominence, and jawline geometry. These features are algorithmically encoded into multidimensional vectors representing the unique facial signature of the individual. The final stage, pattern matching, involves comparing the extracted feature vectors with existing data stored in a reference database. Depending on the objective, the system may perform verification (one-to-one comparison) or identification (one-to-many comparison). This mathematical comparison yields a similarity score, which is then assessed against a predefined threshold to affirm or deny identity.

The advent of deep learning, particularly the utilization of Convolutional Neural Networks (CNNs), has profoundly elevated the accuracy and scalability of facial recognition systems. CNNs are uniquely equipped to handle image classification tasks, as they are capable of autonomously learning hierarchical features from raw pixel data through layers of convolution, pooling, and activation functions. Landmark models such as DeepFace (developed by Facebook) and FaceNet (by Google) have demonstrated that CNNs, when trained on large-scale datasets, can achieve near-human accuracy in face recognition tasks. These models not only extract discriminative features but also learn the optimal embedding spaces wherein facial similarity corresponds to Euclidean distance. As a result, contemporary CNN-based systems can effectively navigate the challenges of intra-class variations (same person with different expressions or lighting) and inter-class similarities (different individuals with similar appearances).

The versatility of facial recognition technology is evidenced by its widespread adoption across diverse domains. In the realm of national security and law enforcement, facial recognition is extensively deployed for surveillance, suspect identification, and border control. Law enforcement agencies utilize real-time facial analytics to monitor public spaces and detect persons of interest, thereby enhancing situational awareness and operational response. In consumer technology, particularly in smartphones and personal computing devices, facial recognition provides biometric access control, replacing traditional PINs and passwords. Apple's Face ID is a prominent example, utilizing infrared sensors and machine learning algorithms to authenticate users securely. In healthcare, facial biometrics are employed for patient identification, access control in restricted zones, and even for diagnostic purposes, such as detecting genetic disorders with facial manifestations. In the finance and e-commerce sectors, facial recognition is used to authorize transactions, combat identity fraud, and enable Know Your Customer (KYC) compliance with minimal user friction. Retail and marketing industries also employ advanced facial analytics to analyze customer demographics, track engagement, and deliver personalized advertisements, thereby transforming consumer interaction models.

Despite its technological prowess, face recognition systems are not impervious to operational challenges. Variability in illumination, facial expressions, occlusions such as eyeglasses or masks, and aging effects can substantially impair recognition accuracy. These challenges are often exacerbated in uncontrolled environments such as outdoor surveillance, where lighting and angles cannot be standardized. Moreover, pose variation—wherein the orientation of the face relative to the camera deviates from the frontal position—remains a significant hurdle. While CNNs demonstrate robustness in dealing with minor pose changes, extreme angles still result in degraded performance. The inclusion of diverse demographic data during training is essential to mitigate algorithmic bias, as models trained on homogenous datasets tend to exhibit disparate performance across age, gender, and ethnic groups. Thus, there is a pressing need for demographically balanced and ethically sourced datasets to ensure equitable system performance.

The integration of facial recognition technology into public and private spheres has ignited profound debates surrounding privacy, civil liberties, and algorithmic accountability. One of the central concerns is the unconsented collection and storage of facial data, often conducted surreptitiously through surveillance cameras or digital platforms. Such practices raise fundamental questions regarding informed consent, data ownership, and the right to anonymity in public spaces. In jurisdictions lacking comprehensive data protection frameworks, there

exists a tangible risk of state surveillance encroaching upon individual freedoms. Furthermore, the potential for misidentification, particularly among minority populations, poses a serious threat to justice and equity. Several high-profile cases have demonstrated that inaccuracies in facial recognition systems can lead to false arrests and legal consequences, thereby eroding public trust. Regulatory responses have varied globally. The European Union, through its General Data Protection Regulation (GDPR), mandates strict guidelines for biometric data processing, including transparency, consent, and data minimization. Meanwhile, some municipalities in the United States have imposed moratoriums on the use of facial recognition by law enforcement, citing civil rights concerns.

The future trajectory of facial recognition is closely intertwined with advances in multi-modal biometrics, anti-spoofing technologies, and federated learning. Multi-modal biometric systems aim to enhance robustness and reduce false positives by integrating multiple biometric modalities—such as facial, iris, and voice recognition—into a unified authentication framework. Liveness detection mechanisms are being incorporated to assess involuntary human traits like eye blinks, facial micro-movements, or thermal signatures in order to prevent spoofing attacks using photographs, videos, or 3D masks. Federated learning, along with on-device processing, offers a promising approach to address privacy concerns by enabling decentralized model training on user devices. This ensures that raw facial data never leaves the local environment, significantly reducing the risk of data breaches while preserving personalization. Additionally, explainable AI (XAI) is gaining momentum, as researchers work to develop models that provide intelligible justifications for recognition decisions, thereby enhancing trust and accountability.

The continuing evolution of facial recognition technology necessitates a delicate balance between technological innovation and ethical responsibility. While the potential benefits are manifold—from enhanced security to personalized user experiences—the deployment of such powerful tools must be guided by principles of fairness, transparency, and respect for human dignity. Policymakers, technologists, and civil society must collaborate to establish robust regulatory frameworks, promote algorithmic inclusivity, and ensure that face recognition systems are used in contexts that uphold democratic values. Public awareness and education are also essential to empower individuals to make informed decisions regarding their biometric data. Face recognition technology stands at the confluence of artificial intelligence, biometrics, and societal transformation. Its capacity to provide secure, rapid, and intuitive identification renders it a cornerstone of the modern digital infrastructure. Yet, as its influence permeates deeper into personal and public domains, it brings with it an array of ethical dilemmas and technical complexities that demand careful navigation. The trajectory of this technology will be shaped not merely by algorithmic breakthroughs, but by our collective commitment to responsible innovation. Only through interdisciplinary collaboration and ethical foresight can we ensure that facial recognition serves as an instrument of progress—enhancing safety, convenience, and inclusivity—without compromising the fundamental rights and freedoms of individuals.

2. Review of Literature

Face recognition technology has undergone remarkable evolution, transitioning from early geometric-based methods to advanced deep learning-driven systems. Initially, techniques like Eigenfaces and Fisherfaces were used, focusing on dimensionality reduction and linear models to extract key facial features. These methods were effective in controlled environments but struggled with variations in lighting, pose, and expression, which limited their practicality for real-world applications.

The introduction of Convolutional Neural Networks (CNNs) marked a significant breakthrough, offering a more robust and scalable approach. Modern models, such as DeepFace, VGG-Face, and FaceNet, leverage deep learning architectures that automatically learn facial features from raw image data, significantly improving the accuracy and performance of face recognition systems. These models excel in diverse conditions, such as varying lighting, expressions, and poses, making them far superior to earlier techniques.

Recent advancements have also explored the use of Generative Adversarial Networks (GANs) for data augmentation, which helps generate synthetic data to improve the generalization of face recognition models. Transfer learning has become another important technique, where pre-trained models are fine-tuned on smaller, task-specific datasets, enabling better performance even with limited data.

Despite these advancements, face recognition systems still face several challenges. Bias remains a significant issue, as many systems exhibit reduced accuracy for certain demographic groups, particularly based on race, age, or gender. This has raised ethical concerns about fairness and equity in automated decision-making. Additionally, the widespread deployment of face recognition for surveillance and security purposes has triggered privacy

concerns, especially regarding data collection and potential misuse.

The future of face recognition technology lies in addressing these challenges. Solutions such as multi-modal biometrics, which combine facial recognition with other identification methods like voice or fingerprints, promise to increase accuracy and security. Privacy-preserving techniques, such as federated learning, hold promise for enhancing user privacy by keeping data decentralized. Furthermore, the development of explainable AI (XAI) is expected to improve the transparency of these systems, allowing users to better understand the decision-making process and build greater trust in their use.

In summary, face recognition has made significant progress, but ongoing research is essential to tackle issues of bias, privacy, and fairness. Addressing these concerns will ensure the continued evolution and responsible deployment of face recognition technology in a wide range of applications. The evolution of face recognition technology has attracted scholarly attention across disciplines ranging from computer science to ethics and law. **Turk and Pentland (1991)** pioneered the development of the Eigenfaces method, establishing a foundational model for facial feature extraction using principal component analysis. Subsequently, **Belhumeur, Hespanha, and Kriegman (1997)** introduced the Fisherfaces method, enhancing recognition accuracy under varying lighting conditions. With the rise of deep learning, **Taigman et al. (2014)** advanced the field through DeepFace, demonstrating human-level performance by utilizing nine-layer deep neural networks. Similarly, **Schroff, Kalenichenko, and Philbin (2015)** developed FaceNet, which introduced triplet loss for learning a compact embedding space, revolutionizing face verification and clustering.

The application of **Convolutional Neural Networks (CNNs)** has been extensively explored by **Parkhi et al. (2015)**, whose VGG-Face model has been influential in real-world deployments. **Masi et al. (2018)** extended this line of work by addressing pose and illumination variations through data augmentation strategies. **Liu et al. (2017)** contributed to the understanding of large-scale face recognition with their SphereFace model, which introduced angular margin loss to improve classification boundaries.

In terms of environmental and demographic challenges, **Klare et al. (2012)** revealed racial and gender bias in facial recognition algorithms, a concern echoed by **Buolamwini and Gebru (2018)**, who demonstrated significant accuracy disparities in commercial systems across different demographic groups. **Grother, Ngan, and Hanaoka (2019)**, in a comprehensive study for the U.S. National Institute of Standards and Technology (NIST), quantified these disparities, urging the development of more inclusive training datasets.

Privacy and ethical concerns have been the subject of critical inquiry by scholars such as **Cavoukian (2009)**, who advocated for privacy by design, and **Zuboff (2019)**, whose seminal work on surveillance capitalism highlighted the commodification of biometric data. **Brunton and Nissenbaum (2015)** further contextualized the societal implications of facial surveillance within digital ethics frameworks. Meanwhile, **Wright and Kreissl (2014)** examined the expansion of facial recognition within public policing contexts, raising alarms over accountability and transparency.

From a regulatory perspective, **Tene and Polonetsky (2012)** discussed the inadequacies of existing privacy laws in addressing biometric data, advocating for technology-specific regulations. **Raji and Fried (2020)** highlighted the need for corporate governance and ethical auditing in the deployment of facial recognition systems. **Garvie, Bedoya, and Frankle (2016)** critically analyzed the unchecked use of face recognition by U.S. law enforcement agencies, identifying a lack of oversight and public consent.

In exploring technical innovations aimed at mitigating these concerns, **Chingovska, Anjos, and Marcel (2012)** introduced spoofing detection techniques, while **Li et al. (2018)** integrated depth-sensing and liveness detection to counter facial forgery attacks. The concept of federated learning for privacy-preserving model training was explored by **McMahan et al. (2017)**, offering a path forward for decentralized facial recognition without compromising user data.

3. Overview of Face Recognition Technology

3.1. Non-mandatory

The first important aspect of face recognition technology is that it is optional. Facial recognition can work without the subject's conscious involvement, in contrast to palm vein, iris, and retina recognition, which depend on the subject actively assisting the device in gathering the required biometric data. This means that the system can automatically capture and analyze facial images even when the individual is unaware of the process.

This non-mandatory aspect is crucial because it makes the technology less intrusive and less likely to be perceived as offensive. It also reduces the risk of individuals with malicious intent attempting to evade or manipulate the

system, as they may not even realize they are being identified. As a result, facial recognition is often more practical and easier to implement in various settings compared to more intrusive methods like fingerprint recognition.

3.2. Concurrency

Concurrency is a significant feature of facial recognition technology. It enables the rapid and simultaneous collection and identification of several faces in a single frame using cameras and other image or video acquisition systems. This capability offers substantial advantages over other biometric identification methods like fingerprint or palm print recognition. For example, face recognition systems can effectively evaluate the photos of several people in real-time in busy places like stadiums, train stations, and airport gates and exits. This ensures that the flow of people is not disrupted while still providing timely and accurate identification and verification of individuals.

3.3. Non-contact

Another advantage of facial recognition technology is that it doesn't require physical interaction. Unlike fingerprint identification, which relies on electronic pressure sensors to collect and compare fingerprints, facial recognition does not require any physical contact. This is particularly advantageous in health-sensitive environments like hospitals, where contact-based systems can facilitate the spread of diseases.

While other biometric methods, such as palm print and retina recognition, do not require substantial physical contact, they still necessitate the subject to be in close proximity to the acquisition device and to actively cooperate with the process. In contrast, facial recognition systems can capture and process facial information from a distance, without any physical interaction. This makes facial recognition a more hygienic and user-friendly option, as it can function effectively even when the subject is far away from the camera.

4. Application

4.1. Face tracking

The main purposes of face tracking technology are to follow suspects or find missing people. The accuracy of negative face identification has greatly increased with the development of 3D face recognition algorithms and systems. The technology receives photos of suspects or missing children and extracts dynamic picture information from a large volume of security video data. The system identifies and locks onto the most matching face information, allowing for continuous tracking. This enhanced capability makes it easier to locate and monitor individuals in real-time, even in crowded and complex environments.

Fig.1

4.2. Face retrieval

Businesses and educational institutions frequently employ facial recognition technology for sign-in and clock-in. To set up the system, the facial information of all staff members or students must first be input into the database. When it's time to check in, individuals simply need to approach the image collection equipment. After that, the algorithm records their face features and contrasts them with the information in the database. The check-in process is finished if the match is successful.

This technology is quick and easy to use, and it requires little collaboration from people. It is a common option for these applications as it is especially good at identifying static pictures. The ease of use and high accuracy contribute to its widespread adoption in both corporate and educational settings.

Fig.2

4.3. Face verification

Facial recognition technology is primarily used in customs stations and other security-sensitive locations to verify personnel information. When a person approaches the acquisition equipment, the face recognition system captures their facial information in real-time. The ID card and other original data kept in the database are then compared with this collected data. This procedure ensures that only authorized persons are given access by assisting in determining the veracity of the identification

information provided by the person being verified. The real-time and accurate nature of this technology makes it highly effective for security and identity verification purposes.

Fig.3

4.4. Disputes

Concern over the protection of personal information has grown significantly as a result of the quick development of face recognition technologies. As this technology becomes more commercialized, we are forced to reconsider the balance between personal privacy and security. However, it's important to acknowledge that, from a legal perspective, facial recognition technology and privacy issues often conflict.

According to Article 41 of the People's Republic of China's Cybersecurity Law, which went into effect in 2017, "network operators shall adhere to the principles of legality, legitimacy, and necessity when they collect and use personal information." They must publicly disclose the rules for collecting and using information, clearly indicate the purpose, method, and scope of collecting and using the information, and obtain the consent of the individuals whose information is being collected. Network operators shall not collect personal information irrelevant to the services they provide, nor shall they collect and use personal information in violation of the provisions of laws and administrative regulations or the agreements with users. They must also process the personal information they keep in accordance with the provisions of laws and administrative regulations and the agreements with users."

Compared to fingerprint recognition, facial recognition has a certain degree of concealment. It can be implemented without the cooperation or prior consent of the individual being identified. For example, students in a classroom might unknowingly have their facial expressions and behavior captured and analyzed by a facial recognition system to assess their concentration and attentiveness. This unauthorized collection and analysis of personal information can infringe on students' privacy and potentially impact their personal safety.

The asymmetry of information between the entities using facial recognition technology and the public is a significant concern. By utilizing their better information gathering and application skills, these organizations may freely employ facial recognition technology to take pictures of people's faces in public settings for a variety of uses. It is difficult to defend people against such actions, which could not be regarded as a violation of their privacy or public social rights.

In summary, while facial recognition technology offers numerous benefits, it also poses significant risks to personal privacy and public rights. Striking a balance between these concerns is crucial for ensuring that technology is used ethically and responsibly.

5. Debate on Face Recognition Technology

Many facets of society have begun to question the security and privacy protections of facial recognition technology as a result of their extensive use. "Human faces are open, but computers with the ability to record, store, and analyze face images at low cost, quickly, and in large volumes will eventually lead to a redefinition of the concepts of privacy, fairness, and trust," an article published in the British business journal The Economist in September 2017 said.

This emphasizes how big data systems and public surveillance systems that employ face recognition technology are vulnerable to misuse or monopolization by people or groups when the trend of big data openness picks up speed. This has sparked a discussion about the benefits and drawbacks of face recognition technology and raised public worries about personal privacy and security under the scrutiny of public surveillance systems.

On one hand, facial recognition offers significant benefits, such as enhancing security and efficiency in various settings. On the other hand, the potential for misuse and the erosion of privacy are serious concerns. The public is increasingly aware of the need for robust regulations and safeguards to ensure that the technology is used ethically and responsibly.

5.1. In favour

Supporters of facial recognition technology contend that this system may give the public very strong security with little loss of privacy, hence improving community security and enhancing "additional security" in different media disputes. They think the substantial security advantages outweigh any privacy compromise. Widespread use of this precise and efficient monitoring system can lower crime and be a vital tool for improving community safety and

people's quality of life. Furthermore, the public may receive an invaluable "additional sense of security" from this approach. Advocates point out that compared to manual monitoring techniques, the pervasive public surveillance system provides significantly more thorough security. They also highlight the system's added societal usefulness, including controlling the floating population, tracking down missing people, and tracking down suspects at large. Supporters of the system have differing opinions on privacy. Some people underestimate the harm that technology poses to privacy, or they deny that privacy problems even exist. Others agree that privacy might be an issue, but they come to the conclusion that the advantages of security exceed the costs of freedom and privacy. They defend their support for the system by claiming that a benefit trade-off study demonstrates that the security advantages outweigh the costs.

5.2. Objection

First of all, biological information is gathered for facial recognition, which is important for people. Relevant institutions or organizations must demonstrate the validity of this strategy prior to collection. Ordinary personal information, such as an address, phone number, email, account, and trail, must be gathered with the prior agreement of the individual being acquired due to its recognized nature, as per current laws and regulations. However, there may also be legal repercussions, including criminal repercussions, if the collecting party misuses, sells, or discloses the related information. Compared to broad personal information, biological data has a clearer personal orientation and is more significant to individuals. Why does the collection of biological data not need the agreement of the individual being collected? Furthermore, there is no legal culpability for unlawful collection or use, and there are no restrictions on the subject, goal, manner, extent, or process of collecting. If the government is in charge of the collection, it must be expressly permitted by law; otherwise, it cannot be carried out, and the government has no jurisdiction to gather the biometric information of regular people for security purposes. Individuals' biological data must be gathered with their express agreement, whether it is being collected by businesses or other organizations; collecting personal information about people without consent is prohibited.

Second, using face recognition in the subway as an example, it has the least amount of reason and must be adopted after public engagement and a hearing procedure since it concerns significant personal rights and interests of the public. A few years ago, the Beijing metro rate adjustment process underwent rigorous hearing processes and extensively solicited public feedback. How can we decide to use face recognition technology—which includes more significant human rights and interests—without first consulting or holding a hearing if changing ticket pricing necessitates a lengthy consultation process? Is a few yuan RMB less significant than personal biological information? People are willing to jump into widespread face recognition without any evidence, and there are good reasons to question if this is the product of lobbying by pertinent interest groups or illicit interest transactions.

Thirdly, the use of face recognition technology is said to provide classification security; nevertheless, the issues with the standard itself remain unresolved. To classify people, what authority does a traffic management department have? On what law does it rest? Furthermore, what criteria will the relevant agencies use to categorize passengers, what information will be included by the criteria, who will be involved in the process of determining the criteria, and should the criteria be made public? Prior to the use of face recognition, shouldn't these issues be resolved? It should be made plain how rubbish is classified, as well as how humans are classified. How can we determine if internal standards are fair and lawful if relevant departments plan to implement them? How can one determine whether discrimination is illegal? How can one determine whether establishing standard content at will is problematic? How should interested parties file an appeal and make sure their rights are adequately addressed if they disagree with the classification criteria or believe that an incorrect classification violates their legal rights and interests? How can we make such a hasty choice to utilize face recognition for categorization and security inspection on a big scale in locations like subways before these issues are resolved? Lastly, there is insufficient data to demonstrate that facial recognition may increase subway traffic efficiency; even if this were true, the efficiency alone would not be sufficient to support complete deployment. Human recognition technology is being installed in the subway to increase traffic efficiency during periods of high passenger volume, according to officials at the rail transport command. Claims don't represent objective facts, which is the issue. How can we be sure that implementing this technology in the subway would increase traffic efficiency before doing thorough empirical research? I find it difficult to accept this conclusion given my experiences at hotels and the airport. We have cause to question whether the experts' assessment is accurate, even if they provide some support. The expert's judgment is likely to be flawed because this entails predicting and evaluating the unknown circumstance. For instance, several demographic

specialists have said clearly in the years preceding the second child policy's full implementation that China's population will rise significantly as a result of the policy's implementation. Everyone can see the true fertility rate since the second kid was born. Taking a step back, even though face recognition can increase efficiency, this alone does not provide a sufficient foundation for deployment. Don't use efficiency to deceive the people. When there is a high volume of passengers, the subway's efficiency can be maximized by avoiding the so-called security check. During peak or general periods, the present personnel inspection—particularly the personnel inspection among them—is insignificant. We truly fail to comprehend the practical purpose and relevance of such a personal examination, in addition to the waste of the tax dollars.

In addition to being against the use of facial recognition technology in subways, I am also against requiring individuals to submit to face recognition inspections at airports, hotels, and other locations for the reasons listed above, particularly in light of the possible hazards and adverse consequences. Businesses entice individuals to use facial recognition freely by offering tiny profits or simple, secure features. It is challenging to obtain meaningful user permission since the majority of the information is incomplete, making its usage illegal. The presumption of innocence premise is often used in contemporary criminal procedural law. This idea states that unless a person is proven guilty by a court, they are legally assumed innocent. But the presumption of guilt is the foundation of all existing security measures. Everyone must go through more rigorous security checks since it is assumed that everyone poses a risk to public safety.

6. Risk on Face Recognition System

The most common and contentious location for a face recognition system is a public area, and more discussion is still required to weigh the benefits and drawbacks of security and privacy. Public facial recognition systems currently face three major issues: inadequate public consultation and transparency; a lack of a clear and comprehensive legal framework governing the collection, use, and storage of biometric data, which can result in misuse and abuse of the technology and make the collection of biometric data by private organizations or government entities appear unlawful and violate individual rights, where public opinion and concerns are not adequately considered before deployment, and the lack of a transparent process for setting classification standards and security measures can lead to mistrust and resistance from the public, necessitating proper public hearings and consultations; and the potential for misuse and discrimination, including unauthorized access, data breaches, and improper use by authorities, which can violate the principle of equality and the fundamental right to inviolability of freedom, requiring robust mechanisms for appeal and remedy. Addressing these issues requires a multi-faceted approach, including the development of clear legal guidelines, increased public engagement, and the implementation of robust safeguards to protect individual privacy and prevent misuse.

6.1. Technical error

Because face recognition technology is still in its infancy, there is a chance that it could match incorrectly, which might result in police harassment of innocent people or make it impossible for building occupants to successfully navigate access control. Errors in the personal data gathered in the database, incorrect system user behavior, and the probabilistic nature of the matching process are the main causes of this problem rather than the duplication of human faces. While technical errors alone may not be a sufficient theoretical argument against the use of this system, they do highlight the high fault tolerance required for identity recognition systems. The potential negative consequences of system inaccuracy are difficult to fully evaluate, making it crucial to address these technical shortcomings to ensure the system's reliability and fairness.

6.2. Functional latent change

A phenomenon known as functional latent change occurs when a particular technology, which was once created to fulfill a certain goal, develops new and surprising uses. Such hidden functional changes may result from the misuse of technology or from the growth of its application space. Because of its great degree of flexibility, facial recognition technology is especially vulnerable to this phenomenon. There is a great deal of possibility for functional modification, and its use may readily extend beyond the initial purposes of location tracking and identification. For instance, the original design purpose of facial recognition technology was to manage criminal information and track fugitive suspects for public security departments. However, with advancements in big data technology and increased data transparency, the originally centralized facial recognition systems have evolved into interconnected distributed systems. These systems can now integrate data and allow users to collaborate on dynamic tasks, enabling them to achieve purposes that

were not initially intended. This expansion and repurposing of technology can lead to unexpected related problems, such as privacy violations, misuse, and discriminatory practices.

6.3. Privacy disclosure

Without adequate consultation and information gathering, it is very difficult to prevent violating the privacy of those being watched in public areas. We must give particular consideration to an individual's self-conscious privacy, which is the right to be free from outside interference and to make one's own decisions on one's private life, in addition to information and spatial privacy. These privacy rights, especially self-conscious privacy, are frequently violated by the existing face recognition technologies without any technological obstacles. Without the user's permission, the system may gather, examine, and share real-time data including mobility and consumption patterns as well as fixed data like age, employment, property status, and personal name. As monitoring accuracy and micro-expression psychoanalysis technology improve, future systems may even read sensitive information like personality, emotions, conversation content, potential diseases, and sexual orientation. Under comprehensive facial recognition monitoring in public places, individuals are effectively reduced to "information labels," similar to more conventional identifiers like barcodes and character passwords, with their faces acting as a component of a broader identity identification or authentication system. The entire human body becomes a little mobile database inside a bigger database as a result of this transition, and the human face becomes an information structure. Because of the possibility of functional advancements in identification technology, users of the technology can access the data in these "small databases" whenever they want and for free. Despite the fact that this information is intrinsically tied to the individual, the technology users have the right to utilize it, frequently without any beneficial effects on them. As a result, public monitoring systems deal with two privacy issues: they collect private information from individuals and risk database information leakage due to potential functional changes. Even if there isn't any proof that the security advantages of face recognition technology exceed the privacy risks to individuals, the technology's research and development will continue due to the ongoing expansion of its application areas. There will be more in-depth exploration of the conflict between security and privacy in facial recognition technologies.

7. Methodology

The methodology for face recognition involves a series of well-defined processes designed to accurately identify or verify individuals based on their facial features. It begins with image acquisition, where a digital image or video is captured using cameras or sensors. Face detection algorithms then locate the face(s) within the image, isolating them from other elements to ensure only relevant facial data is processed. Next, feature extraction captures unique facial characteristics such as facial landmarks, textures, and overall structure, often using advanced techniques like Convolutional Neural Networks (CNNs) for more robust and accurate results. The extracted features are compared to a database of known face data using similarity metrics like cosine similarity or Euclidean distance, leading to either identity verification or identification from the database. To enhance security and reduce false positives, post-processing techniques such as liveness detection and thresholding may be employed. Despite the integration of state-of-the-art technologies like deep learning, transfer learning, and generative models, challenges such as bias and privacy concerns remain. This methodology forms the backbone of modern face recognition technology, driving its application in areas like security, personal identification, and access control.

Convolutional Neural Networks

Convolutional Neural Networks (CNNs) have become the cornerstone of modern face recognition systems due to their ability to automatically learn hierarchical features from raw images. Designed to detect patterns and structures in images, CNNs use convolutional operations with filters that capture essential details like edges, textures, and facial landmarks, enabling them to process facial images with remarkable accuracy, even under varying conditions such as different lighting, angles, and facial expressions. In the context of face recognition, CNNs perform several crucial tasks: they detect and isolate faces within images or video streams, extract distinctive facial features, and represent these features as unique embeddings. These embeddings are then compared to stored face data for matching and identification. One of the key advantages of CNNs is their ability to automatically learn from data, eliminating the need for manual feature extraction and enhancing the system's performance. Models like FaceNet, VGG-Face, and DeepFace have demonstrated superior performance in both face verification and identification tasks. Despite challenges such as the need for large labeled datasets and high computational power, CNNs remain one of the most

powerful and widely used techniques in the field, driving advancements in security, surveillance, and other biometric applications.

8. Conclusion

At this point, the main importance is in freeing people from repetitive tasks, cutting costs, and increasing efficiency rather than replacing particular occupations or technologies. However, the accuracy and dependability of face recognition technology are still insufficient for some crucial fields. Face recognition accuracy and speed will increase with the development of pattern recognition, computer vision, image processing, and machine learning. Powerful databases and processors in the background, together with sophisticated front-end devices, will allow computer face recognition to outperform human recognition in terms of accuracy and speed. Face recognition technology will advance beyond identification recognition to include additional capabilities like assessing health, attractiveness, and age. In the near future, face recognition will become more prevalent in daily life and be widely used. For instance, in public places like subways, where large numbers of people flow in and out daily, face recognition can be used for security checks. However, the pursuit of security through face recognition should not lead to comprehensive repression and panic. The real concern is the potential for information abuse by public authorities, which could result in significant personal and familial consequences, including property loss, reputational damage, occupational setbacks, loss of freedom, health issues, or even loss of life. In order to control the use of facial recognition technology, the National People's Congress Standing Committee must do a fundamental legitimacy analysis and take into consideration starting legislative proceedings.

Acknowledgment

Colleagues and students from Galgotias University's Department of School of Computer Science and Engineering provided help for this study. We are really grateful for their devotion and hard work.

References

[1] Sun, Y., Wang, X., & Tang, X. (2014). *Deep learning face representation by joint identification-verification*. In Proceedings of the 27th IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1988-1995).IEEE.https://doi.org/10.1109/CVPR.2014.257

[2] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). *DeepFace: Closing the gap to human-level performance in face verification*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1701-1708). IEEE. https://doi.org/10.1109/CVPR.2014.220

[3] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). *Face recognition: A literature survey*. ACM Computing Surveys (CSUR), 35(4), 399-458. https://doi.org/10.1145/954339.954342

[4] Jain, A. K., & Li, S. Z. (2011). *Handbook of face recognition*. Springer Science & Business Media. https://doi.org/10.1007/978-0-387-77597-7

[5] Masi, I., Chen, Y., & Dantcheva, A. (2018). *Deep learning for face recognition: A critical review*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 40(9), 2312-2328. https://doi.org/10.1109/TPAMI.2017.2724477

[6] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). *Deep face recognition*. In Proceedings of the British Machine Vision Conference (BMVC) (pp. 1-12). https://doi.org/10.5244/C.29.41

[7] Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. In Proceedings of the 1st Conference on Fairness, Accountability and Transparency(pp.77-91).https://doi.org/10.1145/3287560.3287593

[8] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). *FaceNet: A unified embedding for face recognition and clustering*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 815-823).IEEE.https://doi.org/10.1109/CVPR.2015.7298682

[9] Singh, Harsh Pratap, et al. "AVATRY: Virtual Fitting Room Solution." 2024 2nd International Conference on Computer, Communication and Control (IC4). IEEE, 2024.

[10] Singh, Nagendra, et al. "Blockchain Cloud Computing: Comparative study on DDoS, MITM and SQL Injection Attack." 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML). IEEE, 2024.

[11] Singh, Harsh Pratap, et al. "Logistic Regression based Sentiment Analysis System: Rectify." 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML). IEEE, 2024.

[12] Naiyer, Vaseem, Jitendra Sheetlani, and Harsh Pratap Singh. "Software Quality Prediction Using Machine Learning Application." Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 2. Springer Singapore, 2020.

[13] Pasha, Shaik Imran, and Harsh Pratap Singh. "A Novel Model Proposal Using Association Rule Based Data

Mining Techniques for Indian Stock Market Analysis." Annals of the Romanian Society for Cell Biology (2021): 9394-9399.

[14] Md, Abdul Rasool, Harsh Pratap Singh, and K. Nagi Reddy. "Data Mining Approaches to Identify Spontaneous Homeopathic Syndrome Treatment." Annals of the Romanian Society for Cell Biology (2021): 3275-3286.

[15] Nguyen, H. D., & Duong, T. P. (2019). *A comprehensive review on facial recognition: Challenges and applications*. Journal of Visual Communication and Image Representation, 65, 102676. https://doi.org/10.1016/j.jvcir.2019.102676

[16] He, K., Zhang, X., Ren, S., & Sun, J. (2016). *Deep residual learning for image recognition*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 770-778). https://doi.org/10.1109/CVPR.2016.90.