Artificial Intelligence for Face Recognition in Security Systems: A Review of Algorithms and Challenges

El-Sayed M. El-kenawy, Anis Ben Ghorbal

School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain

Department of Mathematics and Statistics, Faculty of Science, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia.

Emails: sayed.elkenawy@polytechnic.bh; assghorbal@imamu.edu.sa

Abstract

FRT is acknowledged as one of the successful advancements of biometric applications in security, surveillance, health care and innovative solutions. More so, the past decade has seen improvements in deep learning, pre-trained Neural Network Convolutional Neural Networks (CNNs), and combining methods such as ensembles, which have highly improved the FRT's Accuracy and efficiency. Nonetheless, several issues remain – facial expression, illumination, demographic biases or adversarial and backdoor threats. Such limitations require new approaches and tools to enhance FRT's reliability and ethical use. The current review also presents ethical concerns and the social consequences of using FRT.

Keywords: Facial recognition technology; deep learning; neural networks; biases; adversarial attacks; ethics.

1. Introduction

Facial recognition technology (FRT) is widely taken as a revolutionary element in contemporary biometric applications, thus helping progress in numerous areas like security, monitoring, healthcare and smart city solutions. In the last decade, the incorporation of deep learning technologies, pre-trained Neural Networks (CNN) and an ensemble have contributed to increased Accuracy and efficiency. However, the field has the following ongoing issues: facial expression bias, illumination bias, demographic shift bias, and sensitivity to adversarial and backdoor attacks. These limitations signify the need to search for novel measures and mechanisms. The present study also highlights ethical considerations and consequences of FRT's use.

1. State-of-the-Art Algorithms and Techniques

FRT has received massive development using better algorithms and methodology in the recent past. Transfer learning is now the norm rather than the exception in contemporary FRT systems, allowing for pre-established models, for instance, DenseNet201, ResNet152V, and MobileNetV2, to minimize feature extraction and learning time on large databases. These models derive more stable and accurate algorithms for facial features that enhance the performance of recognition tasks in often changing illumination and occlusion. Predicting the features by applying multiple algorithms enhanced the performance of ensemble

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

models, such as weighted average and hybrid models. Facets like online learning allow systems to smoothly introduce fresh personnel and enhance existing templates while delivering flexibility in lively settings. These new developments, together with careful hyperparameter adjustment and data conditioning techniques, have proven to establish new standards for the effectiveness of FRT systems in terms of Accuracy and speed in responding to various real-life situations to ensure their effectiveness [1].

2. Bias and Security Vulnerabilities

Today, FRT suffers from key problems within the context of bias and security risks, rendering this technology untrustworthy. Expression bias, the differential recognition influence due to differences in the expression of the face, is a prevalent limitation in many of the standard datasets and algorithms. This is because demographic prejudices like age and race, gender or ethnicity gap in performance also intensify these problems, thus bringing out the question of equality in the table. In security, adversarial attacks, such as adversarial patches and digital manipulations, take advantage of the algorithm's vulnerability to mislead systems. More serious backdoor attacks like Facial Identity Backdoor Attacks (FIBA) involve poisoning samples of the victim during enrollment so that the attackers can masquerade past the systems using universal triggers. Such weaknesses call for strong countermeasures, including different datasets, amenable and equitable algorithmizing, and profound defense measures to enhance the FRT safeguard against misuse while protecting the rightful use [2].

3. Areas of Application and Its Effectiveness

The application of FRT has grown significantly across core infrastructure and essential applications by enhancing security, comfort and government procedures. In surveillance, FRT improves security for the general population by helping to recognize people in public areas and assisting the police in their investigation process. In particular, user authentication provides easy access to devices, workplaces, and financial transactions that replace traditional authentication methods due to the appearance of more efficient and secure biometrics. In public administration in smart cities, border control, and electronic voting, FRT is applied for identity management while solving organizational issues. Yet its attempt to integrate into these domains carries with it issues of privacy invasion, ethical violation, and the possibility of abuse. FRT has many advantages in the real world. However, its implementation must harmonize technology with people's rights and become an excellent benefit for people rather than harm them [3].

4. Audit Committee and Ethical and Governance Challenges

Facial recognition technology comprises one of the most significant ethical and governance risks as it is part and parcel of the recent societal shift that meshes with privacy and civil liberties. They capture and store pertinent biometric data, typically considered highly private. Therefore, the worries of overbearing surveillance and misuse come into place. Delays in adopting new technologies often earmark the current laws; it hampers the determination of aspects like security, consent and accountability. Also, using FRT in workplaces and other governmental and non-governmental organizations has raised several controversies regarding misuse and discrimination. To avoid such risks, there is a need for principled governance while using FRTs by considering transparency, fairness, and accountability. Through frameworks that set down legal standards and ethical norms as to the use of FRT, society will be able to fully realize the potential of FRT while maintaining social respect for civil liberties that bar this new technology [4].

5. **Future Directions and Open Problems**

The advancement of facial recognition technology (FRT) hinges on addressing unresolved challenges and pursuing innovative research directions. Enhancing datasets to include greater diversity in demographic representation, lighting conditions, and facial expressions can reduce biases and improve algorithmic fairness. Developing models with heightened robustness against adversarial attacks and backdoor vulnerabilities remains a critical priority to bolster security and trustworthiness. Research into interpretable and explainable FRT algorithms can promote transparency, fostering greater acceptance and accountability. Additionally, integrating privacy-preserving techniques, such as federated learning, can mitigate concerns regarding data security and unauthorized usage. These open problems present opportunities to refine FRT systems, ensuring their fairness, reliability, and ethical application in diverse real-world contexts.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

In this way, the review provides the basis for analyzing the state of FRT advancement, its constraints and possible future development. In so doing differentials, researchers and practitioners can effectively develop sound, fair, and socially appropriate facial recognition technology.

Literature Review

FRT has become an important aspect of security and other biometric applications in various industries affecting surveillance, authentication and smart city technologies. This literature review focuses on the progression of FRT and ways to address difficulties such as illumination, pose variation and expression bias learned through incorporating FRT with deep learning, ensemble models and transfer learning. There are a range of evaluated methods under review: pre-trained CNNs, novel recognition approaches, and resistance to adversarial and backdoor assaults. The rising ethical and privacy issues constitute a significant aspect of this venture to capture the social aspect of FRT. The applicability of state-of-the-art FRT for different use cases, current challenges, and prospects are discussed in this section, and a foundation for creating safe and ethical FRT systems is established.

As outlined in [5], Artificial Intelligence (AI) has become a pivotal driver of innovation in the video surveillance industry, with advancements in machine learning, deep learning, neural networks, natural language processing, and expert systems transforming traditional practices. The study focuses on the latest AI applications in camera surveillance, emphasizing how these technologies enhance the quality of security systems by addressing trends, overcoming challenges, and offering significant advantages through intelligent analytics and innovative system integration.

In the research presented in [6], a face recognition smart lock system is developed using the Yolo deep learning algorithm on a Jetson Nano board, addressing the need for improved speed and Accuracy in smart home security technologies. The proposed system collects multiple images of a new user within a short time, automatically transfers data to a server for training using an auto-labeling process, and employs methods such as running Yolo in the background, adjusting brightness with a built-in camera light, and maintaining an optimal distance range for face recognition. Users can operate the lock through face recognition or a developed Android application by verifying login credentials over the internet. Trained on thousands of images per user and tested under various conditions, the system achieved 99% accuracy and a recognition speed of 0.6 seconds under favorable lighting and distance conditions.

In the article denoted as [7], the rapid development of face recognition technology is highlighted alongside its promising future applications across various industries. The study provides an in-depth exploration of face recognition systems, detailing their core components, operational principles, and examples of algorithms while analyzing their respective strengths and limitations. Additionally, it addresses existing challenges in the technology and concludes with a forward-looking summary, emphasizing the need for further research to advance the field.

In the analysis conducted in [8], the effectiveness of deep learning models in advancing biometric recognition systems is comprehensively surveyed, covering over 150 significant studies. This research explores various biometric modalities, including face, fingerprint, iris, palmprint, ear, voice, signature, and gait recognition, highlighting the strengths and applications of deep learning in these areas. The study introduces widely used datasets and their characteristics, evaluates the performance of deep learning approaches on public benchmarks, and identifies key challenges and future research directions in biometric recognition systems.

As discussed in [9], face recognition (FR) technology has become integral across the security, healthcare, banking, and criminal identification sectors. This study comprehensively reviews state-of-the-art FR techniques, categorizing them into appearance-based and hybrid approaches. It examines challenges related to illumination, poses variation, facial expressions, occlusions, and aging, which significantly influence FR system performance. Additionally, the research offers a detailed classification of image- and video-based FR methods, emphasizing advancements in core processing steps and dataset handling. By analyzing existing solutions and identifying open problems, this survey is a valuable resource for further innovation in FR technology.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

The research presented in [10] highlights human face recognition as a rapidly advancing field, gaining significant attention from computer vision, machine learning, and artificial intelligence domains due to its progress and broad applications. This study reviews recent face recognition techniques, focusing on their performance across various datasets while addressing challenges such as illumination variability, pose differences, aging, cosmetics, occlusion, and background complexities. Emerging methods, including deep learning, sparse models, and fuzzy set theory, are analyzed alongside classical approaches. The study also explores major applications, current trends, and future directions, emphasizing the role of face recognition technologies in shaping the digital society.

In the article denoted as [11], the application of deep learning techniques to face recognition (FR) is explored through the deployment of five pre-trained Convolutional Neural Network (CNN) models: We have DenseNet201, ResNet152V2, MobileNetV2, SeResNeXt and Xception. Hence, the study proposes a new methodology of using a weighted average by grid search to improve the feature extraction and classification models. Data preprocessing, resizing, data augmentation, data normalization, and splitting are especially stressed as the crisis bars to enhance the reliability of the FR system. Consequently, systematic hyperparameter optimization is used in the context of network depth, learning rate, activation function, and optimization algorithms. The results from different datasets revealed that the proposed method outperforms the approaches in Recall, Precision, F1 score, Matthews correlation coefficient, and Accuracy for the comprehensive evaluation. With the experimental results of LFW dataset model consisting of the proposed model, generative model, model based on SVM classifier, least square regression model, CP beim, and PCA beim, the Accuracy of the proposed model emerges as 99.48%, which reflects that it is to a large extent effective for actual application in FR and superior to the previously proposed state of the arts sd.

The general performance of face recognition algorithms is thoroughly discussed in the publication, marked as [12]. In contrast, the more profound issues concerning face recognition algorithms' ability to cope with challenges emerging in real-life circumstances, which significantly distort the images on which these algorithms work, are assessed to be relatively weak despite high degrees of recognition. Some of the attack categories used in the study include physical presentation attacks, disguise/makeup attacks, digital adversarial attacks and morphing/tampering through GANs. Moreover, it deepens the examination of the influence of prejudice; it is disclosed that differences in age and gender directly correlate to the efficiency of algorithms. The above challenges are explained, and further research guidelines for strengthening and stabilizing face recognition models in real-world conditions are discussed.

As described in the paper [13], the major use of Face Recognition Systems (FRS) in security-sensitive operations such as surveillance and user verification makes it a helpful feature in current security systems. However, the authors show that this approach is vulnerable, especially to adversarial and backdoor attacks. Adversarial patch attacks and training data poisoning are disapproved due to their high consumption of time and energy and the need to manipulate privileged information, implying low stealth, universality level, and impracticality. Closing the above knowledge gaps, this research proposes a facial identity backdoor attack (FIBA) at the enrollment step. What is even worse, FIBA enables an attacker with a specific trigger to override FIBA universally by injecting a single poisoned example into the feature database. This method redraws the threat landscape to show a large-spread and low-profile means of challenging the dependability and integrity of FRS.

As discussed in section [14], this paper is concerned with face detection with voice and biometrics, where the distribution of age and gender have been highlighted. The method uses an input camera to take several shots of a person. Preprocessing involves using the Cascade Classification technique to develop human templates and recognize the face shapes successfully with the Doppel filter's guidance, saving them in a database with different Identifying Numbers. The verification process involves finding a correlation of templates stored in the database to enable automated attendance marking, especially in learning institutions. These results show the effectiveness of this technology in increasing security and efficiency by marking the attendance of employees to increase their attendance or students' presence. Evaluation is also made of the system's deployment in banks, thus facilitating access only to authorized individuals. New directions are identified as distancing methods for age and gender estimations from images and for suggesting better security measures based on new models.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

As is discussed in detail in section [15], Smart city application-based fog and cloud computing systems incorporating transfer learning for facial recognition (FR) systems were defined and analyzed in the study as [Google Scholar]. DCNN is used for feature extraction to handle occlusion, expression, illumination, and pose variation. The system aims at efficient and adaptive face recognition through online learning that allows the integration of new faces and better predictions. This recognition process includes Decision Tree (DT), K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) algorithm. When tested with 113 SDUMLA–HMT and CASIA datasets, the system performs better in all evaluated parameters with an accuracy of 99.06%, a precision of 99.12%, a recall of 99.07% and a specificity of 99.10% than other comparable algorithms.

The paper intended in [16] explores FRT regulation with an emphasis on the opportunity space for interest in public security and the concerns for privacy, civil liberties and ethics. The paper demonstrates tensions between state and corporate power and individual sovereignty over legal commonalities, critically assessing the existing international legal system and recognizing that legislation lacks coercive potential in human rights standards regulation. Instead, it seeks to articulate rational guidance on governance structures for FRT implementation by enhancing principles based on rights and ethics. The mentioned recommendations enhance the potential of FRT to help reinvent, as well as the risk it may bring about through the call for robust and changeable regulations.

As described in [17], this paper seeks to establish that facial expression bias is a significant security threat in face recognition scenarios. Nonetheless, the findings suggest that the methods explored herein remain sensitive to covariates, especially facial emotions. He further discusses biases present in popular face recognition databases and performs an analysis to understand the effect of these biases on the performance of face recognition systems. The experimental setting includes two face detectors, three recognition models, and three databases, which results in significant expression-related biases and their impact on algorithm performance. The research presented in the paper showed that all these aspects should be addressed through research conducted to improve the stability of face recognition systems and minimize these vulnerabilities.

In the work described in [18], facial expression bias is an important security threat to face identification systems. Some of the databases used in face recognition are assessed based on the severity of biases about expression, and algorithms study the effect. This study introduces an experimental setup between two face detectors, three recognition models, and three databases, clearing existing biases in current datasets and their impact on the performance of advanced methods. Such results should alert developers of methods to counter such biases with a call to future work that will enhance the reliability and Accuracy of face recognition systems.

The threats that adversarial and backdoor attacks pose to the effectiveness of FRS and the issues that make these attacks possible are explored using the publication specified as [19]. They propose a new attack called the Facial Identity Backdoor Attack (FIBA), which works at the enrollment stage rather than dealing with training data as most existing adversarial attacks do. An enrollment-stage backdoor attack is accomplished by a single poisoned example that forms a universal trigger, making it easier to circumvent FRS on a large scale. Focusing on the feature database instead of the training data, FIBA greatly extends the threat space and questions the viability, effectiveness and stealth of conventional attacks regarding scalability. The studies underscore that extensive countermeasures for such new risks are needed for FRS to mitigate the threats.

Below is a tabular form that captures all the papers reviewed in this literature review, aspects of focus, the contribution, and the evaluation criterion in Table 1. The studies considered cover a broad variety of topics, starting from recent improvements in AI-based surveillance cameras and smart locks and ending with face recognition systems problems, including expression bias, adversarial attacks, and backdoor attacks. Much thrust has been applied to analyzing contemporary algorithms, such as transfer learning, ensemble models, and computational intelligence, to enhance the Accuracy and efficiency of algorithms. There are also ethical and governance issues discussed, emphasizing what should be done to reduce risks and increase fairness in FRT use. The findings of these studies can serve as a solid groundwork for developing additional investigations about FRT systems that are secure, reliable, and ethical.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

Table 1: Summary of Literature Review

Reference	Focus Area	Key Contributions	Evaluation Metrics
[5]	AI in video surveillance systems	Examines advancements in AI-driven surveillance systems, highlighting improvements in security and efficiency. Explores innovative systems, analytical software, and the integration of technologies like deep learning and neural networks.	Emphasizes trends, challenges, and the impact on security system quality.
[6]	Smart lock system with face recognition	Develop a face recognition smart lock using Yolo on a Jetson Nano board. Features include auto-labeling, brightness adjustments, and Android app integration for authentication. Demonstrates improved speed and Accuracy in smart home security.	Achieved 99% accuracy with a recognition speed of 0.6 seconds under favorable conditions.
[7]	Applications of face recognition technology	Provides an in-depth review of face recognition systems, detailing components, principles, algorithms, and applications. Highlights challenges such as occlusion and expression bias while discussing future research directions.	There are no specific evaluation metrics, but it discusses broader applications and system efficiency.
[8]	Deep learning in biometric recognition	Surveys 150+ works on biometric recognition (face, iris, fingerprint, etc.) using deep learning. Discusses dataset characteristics, algorithm performance, and challenges.	Evaluate using benchmark datasets and identify open challenges in biometric recognition.
[9]	Advances in face recognition techniques	Reviews state-of-the-art FR methods, categorizing them into appearance-based and hybrid approaches. Highlights challenges like pose, illumination, occlusion, and expression biases.	Provides a detailed classification of image- and video-based FR methods.
[10]	Modern face recognition approaches	Reviews classical and modern FR techniques, focusing on performance across datasets. Explores deep learning, sparse	Analyzes challenges like age, gender, and background complexity in FR systems.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

		models, and fuzzy set theory. Discusses broader applications and societal impact.	
[11]	Deep learning and ensemble models for FR	Introduces a weighted average ensemble model using DenseNet201, ResNet152V2, MobileNetV2, and others. Employs hyperparameter tuning and robust preprocessing for improved Accuracy and efficiency.	Achieved 99.48% accuracy on the LFW dataset, outperforming other state-of-the-art methods.
[12]	Robustness of FR systems	Examines vulnerabilities like physical, digital, and adversarial attacks. Highlights biases in demographic factors and proposes future research directions to enhance FR model stability.	Discusses real-world robustness metrics without specific quantitative results.
[13]	Backdoor vulnerabilities in FRS	Proposes a novel attack (FIBA) at the enrollment stage, allowing attackers to bypass FRS with poisoned examples. Demonstrates the practical and stealthy nature of this threat.	Evaluates threat scalability, stealth, and universal trigger capabilities.
[14]	Face detection with voice and biometrics	Develops a system for automated attendance using face detection and Cascade Classification. Explores its application in education, workplaces, and banking to enhance security and efficiency.	Highlights effectiveness in marking attendance and improving punctuality but lacks quantitative evaluation.
[15]	Fog and cloud-based FR systems	Designs a FR system using transfer learning and computational intelligence. Handles challenges like occlusion, pose variation, and illumination. Compares Decision Tree, KNN, and SVM algorithms across datasets.	Achieved Accuracy of 99.06%, precision of 99.12%, recall of 99.07%, and specificity of 99.10% on SDUMLA-HMT, 113, and CASIA datasets.
[16]	Ethical and governance challenges in FRT	Explores privacy, ethics, and regulatory challenges. Critically examines international legal frameworks and proposes governance structures prioritizing human rights and ethical principles.	No quantitative metrics; focuses on legal and ethical recommendations.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

[17]	Facial Expression Bias in FR	Analyzes biases in popular FR datasets and their impact on recognition accuracy. Highlights vulnerabilities related to expression variation.	Evaluates impact using experimental frameworks with two face detectors, three recognition models, and three databases.
[18]	Impact of facial expressions on FR algorithms	Studies expression-related biases and their effect on algorithmic performance. Calls for improvements to enhance the reliability of FR systems.	It uses experimental setups to show biases in datasets and proposes areas for future research.
[19]	FR's vulnerabilities and practical threats	Investigates adversarial and backdoor threats to FRS, introducing a novel enrollment-stage attack (FIBA). Highlights scalability and stealth advantages over traditional attacks.	Analyzes threat effectiveness through the concept of universal triggers and poisoned examples.

The reviews discuss the constantly changing technology of facial recognition systems because of machine learning and deep learning development. Although much progress has been made regarding its Accuracy and robustness, ample problems exist, such as bias, security threats, and moral issues. These gaps provide the potential for innovation in algorithms, selection and compilation of datasets, and the formulation of suitable governance frameworks to manage the identified risks. Overcoming such limitations in future studies will promote the creation of more safe, fair, and sustainable FRT systems. The evidence sourced for this review presents a roadmap on how to enhance FRTs without compromising on the positive impacts of technology on society.

Discussion

This paper's last section discusses the literature review's central arguments based on the established FRT system's progress, hurdles, and repercussions. Analyzing innovation and impact, it formulates research priorities and principles of ethical application of FRT for creating safe, efficient and fair FRT systems.

1. FRT technological developments

Due to the adoption of deep learning, pre-trained CNN models, and ensemble learning, FRT has made significant progress. These technologies have improved the recognition process by increasing Accuracy and speed; otherwise, occlusions and variations in pose and illumination have posed problems. Applicable techniques, including transfer learning and hyperparameter tuning, have enabled the system to learn from various data sets with little computing power. However, real-time adaptation and scalability have not been fully solved, although the demands for these features are higher in applications like video surveillance and authentication [20], [21].

2. Addressing Bias in FRT

Expression, demographic, and illumination biases remain the core problems that FRT requires addressing. Findings indicate possible and probable performance differences concerning age, gender, and ethnicity; it is unethical and biased. These biases arise primarily due to biases in the dataset and constraints in the applied algorithms. To solve these problems, we must collect more diverse datasets, create new algorithms and

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

techniques that are fair to their subjects, and include interpretability methods into our machine learning models [22], [23].

3. Security Threats and Protection Techniques

FRT systems have increasing security threats, such as adversarial attacks, backdoor vulnerability, and enrollment stage attacks, such as FIBA. Such attacks target datasets, a feature database, or an algorithm with a possible consequence for system integrity. The central proposal is to decrease these vulnerabilities and provide stability for FRT systems by elaborating advanced defense strategies such as adversarial training, sanitization of the dataset, and proper management of a secure database [24], [25].

4. Macro Analysis of Ethical Considerations and Governance

The fast growth of FRT has raised concerns about privacy, surveillance, and citizenship freedom. There are no or limited clear legal guidelines or ethical practices to solve the problem of misuse of personal information, discrimination, and choice. Pending good governance models based on openness, responsibility, and the defense of people's rights. Public, private, and civil sector entities working together are crucial for decisions about innovation not to be made solely in the interest of technologists [26], [27].

5. Future Research Directions

However, for FRT systems to improve, future work needs to work on generating challenging datasets, building algorithms that can perform well under adversarial situations, and addressing real-time processing. There are ways to overcome data security issues, including federated learning. Therefore, examining explainable AI (XAI) in FRT improves trust and accountability in decision-making. These innovations will allow FRT systems to reach higher reliability and ethical fitness levels and create a sustainable path for safer incorporating FRT systems into society [28], [29].

This discussion underlines the importance of a multiple perspective on FRT development and the need for technical, ethical, and governance options. In this way, further development of FRT systems regarding existing drawbacks and potential future developments will positively impact society and reduce certain risks.

6. Conclusion

The biometric system has undergone a revolutionary change through facial recognition technology, enabling a new security, surveillance, and identity management era across varied sectors. The literature indicates significant advancement in utilizing machine learning and deep learning techniques, particularly convolutional neural networks (CNNs) and ensemble models, to improve Accuracy and keep efficiency rates within FRT. However, problems like dataset bias, vulnerabilities in security, and ethical issues remain hot challenges for the general adoption of FRT. The key to solving these challenges is ensuring the reliability and fairness of these systems in real-life applications.

The reviewed studies reflect the continuing existence of bias, including expression bias, demographic disparities, and environmental variability. These biases affect the efficacy of FRT systems, posing ethical questions about equity and inclusivity. Security threats, such as backdoor threats and adversarial attacks like Facial Identity Backdoor Attack (FIBA), warrant highly reliable defense mechanisms. Addressing adversarial training, database enhancement, and algorithmic fairness is the way forward in managing these risks for the credibility of FRT systems.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

Ethics and governance frameworks are central to the adoption of FRTs. A lack of sufficient regulations has led to increased concerns about privacy, surveillance, and even abuse of biometric data. Future policies must emphasize transparency, accountability, and protection of individual rights to ensure that technological advancements and societal values meet at a compromise. Finally, collaborative work is required amongst researchers, policymakers, and industry leaders to develop ethical standards and legal frameworks that guide the responsible use of FRT.

Future research must also tackle the current open problems in the literature, including diverse datasets, adversarial robustness, and real-time processing. Privacy-preserving techniques, like federated learning and XAI development in FRTs, could also increase trust and accountability. Achieving those goals will allow society to move towards a more secure, fair, and ethically aligned future with FRT systems and applications benefiting society, while harm might be potentially low. In this holistic approach, FRTs will maximize their entire capabilities responsibly and sustainably.

References

[1] L. Li, X. Mu, S. Li, and H. Peng, "A Review of Face Recognition Technology," *IEEE Access*, vol. 8, pp. 139110–139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[2] A. Fola-Rose, E. Solomon, K. Bryant, and A. Woubie, "A Systematic Review of Facial Recognition Methods: Advancements, Applications, and Ethical Dilemmas," *Proceedings - 2024 IEEE International Conference on Information Reuse and Integration for Data Science, IRI 2024*, pp. 314–319, 2024, doi: 10.1109/IRI62200.2024.00070.

[3] R. Sharma, V. K. Sharma, and A. Singh, "A Review Paper on Facial Recognition Techniques," *Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021*, pp. 617–621, 2021, doi: 10.1109/I-SMAC52330.2021.9640896.

[4] A. Tiwari, S. Manzoor, J. Sehgal, and A. Mishra, "A Comprehensive Review of Face Detection Technologies," *2nd IEEE International Conference on Advances in Information Technology, ICAIT 2024 - Proceedings*, 2024, doi: 10.1109/ICAIT61638.2024.10690719.

[5] B. Ivanova, K. Shoilekova, and R. Rusev, "Trends and Challenges in Surveillance - A Systematic Review of Camera Systems Implementing Artificial Intelligence," *Lecture Notes in Networks and Systems*, vol. 909 LNNS, pp. 103–112, 2024, doi: 10.1007/978-3-031-53549-9_11/FIGURES/3.

[6] T. N. Do, C. L. Le, and M. S. Nguyen, "IoT-Based Security with Facial Recognition Smart Lock System," *Proceedings - 2021 15th International Conference on Advanced Computing and Applications, ACOMP 2021*, pp. 181–185, 2021, doi: 10.1109/ACOMP53746.2021.00032.

[7] N. Jiang, "The Analysis and Application of Face Recognition Technology," *Proceedings - 2023 International Conference on Computers, Information Processing and Advanced Education, CIPAE 2023*, pp. 323–327, 2023, doi: 10.1109/CIPAE60493.2023.00069.

[8] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," *Artif Intell Rev*, vol. 56, no. 8, pp. 8647–8695, Aug. 2023, doi: 10.1007/S10462-022-10237-X/METRICS.

[9] H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, and F. Flammini, "A Comprehensive Review of Face Recognition Techniques, Trends, and Challenges," *IEEE Access*, vol. 12, pp. 107903–107926, 2024, doi: 10.1109/ACCESS.2024.3424933.

[10] W. Ali, W. Tian, S. U. Din, D. Iradukunda, and A. A. Khan, "Classical and modern face recognition approaches: a complete review," *Multimed Tools Appl*, vol. 80, no. 3, pp. 4825–4880, Jan. 2021, doi: 10.1007/S11042-020-09850-1/FIGURES/9.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

[11] J. Selvaganesan *et al.*, "Enhancing face recognition performance: a comprehensive evaluation of deep learning models and a novel ensemble approach with hyperparameter tuning," *Soft Comput*, vol. 28, no. 20, pp. 12399–12424, Oct. 2024, doi: 10.1007/S00500-024-09954-Y/METRICS.

[12] R. Singh, A. Agarwal, M. Singh, S. Nagpal, and M. Vatsa, "On the Robustness of Face Recognition Algorithms Against Attacks and Bias," *AAAI 2020 - 34th AAAI Conference on Artificial Intelligence*, pp. 13583–13589, Feb. 2020, doi: 10.1609/aaai.v34i09.7085.

[13] J. Chen *et al.*, "Rethinking the Vulnerabilities of Face Recognition Systems:From a Practical Perspective," May 2024, Accessed: Dec. 30, 2024. [Online]. Available: https://arxiv.org/abs/2405.12786v3

[14] M. Farhan Siddiqui, W. Ahmed Siddique, M. Ahmedh, and A. Khan Jumani, "Face Detection and Recognition System for Enhancing Security Measures Using Artificial Intelligence System," *Indian J Sci Technol*, vol. 13, no. 9, pp. 1057–1064, Mar. 2020, doi: 10.17485/IJST/2020/V013I09/149298.

[15] D. Salama Abdelminaamid, A. M. Almansori, M. Taha, and E. Badr, "A deep facial recognition system using computational intelligent algorithms," 2020, doi: 10.1371/journal.pone.0242269.

[16] X. Wang, Y. C. Wu, M. Zhou, and H. Fu, "Beyond surveillance: privacy, ethics, and regulations in face recognition technology," *Front Big Data*, vol. 7, p. 1337465, Jul. 2024, doi: 10.3389/FDATA.2024.1337465/BIBTEX.

[17] A. Peña, A. Morales, I. Serna, J. Fierrez, and A. Lapedriza, "Facial Expressions as a Vulnerability in Face Recognition," *Proceedings - International Conference on Image Processing, ICIP*, vol. 2021-September, pp. 2988–2992, Nov. 2020, doi: 10.1109/ICIP42928.2021.9506444.

[18] A. Peña, A. Morales, I. Serna, J. Fierrez, and A. Lapedriza, "Facial Expressions as a Vulnerability in Face Recognition," *Proceedings - International Conference on Image Processing, ICIP*, vol. 2021-September, pp. 2988–2992, Nov. 2020, doi: 10.1109/ICIP42928.2021.9506444.

[19] J. Chen *et al.*, "Rethinking the Vulnerabilities of Face Recognition Systems:From a Practical Perspective," May 2024, Accessed: Dec. 30, 2024. [Online]. Available: https://arxiv.org/abs/2405.12786v3

[20] H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, and F. Flammini, "A Comprehensive Review of Face Recognition Techniques, Trends, and Challenges," *IEEE Access*, vol. 12, pp. 107903–107926, 2024, doi: 10.1109/ACCESS.2024.3424933.

[21] M. Jha, A. Tiwari, M. Himansh, and V. M. Manikandan, "Face Recognition: Recent Advancements and Research Challenges," *2022 13th International Conference on Computing Communication and Networking Technologies, ICCCNT 2022*, 2022, doi: 10.1109/ICCCNT54827.2022.9984308.

[22] M. Hassaballah and S. Aly, "Face recognition: Challenges, achievements and future directions," *IET Computer Vision*, vol. 9, no. 4, pp. 614–626, Aug. 2015, doi: 10.1049/IET-CVI.2014.0084.

[23] D. Verma, K. Dhanda, M. Kumar, and M. Gulhane, "Facial Recognition Unlocking Potential Facing Challenges in Face and Gender Identification," *Proceedings of International Conference on Communication, Computer Sciences and Engineering, IC3SE 2024*, pp. 125–130, 2024, doi: 10.1109/IC3SE62002.2024.10592951.

[24] Mujiyanto, A. Setyanto, E. Utami, and K. Kusrini, "Facial Expression Recognition with Deep Learning and Attention Mechanisms: A Systematic Review," *Proceedings - International Conference on Informatics and Computational Sciences*, pp. 12–17, 2024, doi: 10.1109/ICICOS62600.2024.10636857.

[25] L. Li, X. Mu, S. Li, and H. Peng, "A Review of Face Recognition Technology," *IEEE Access*, vol. 8, pp. 139110–139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025

[26] M. K. Rusia and D. K. Singh, “A comprehensive survey on techniques to handle face identity threats: challenges and opportunities,” *Multimedia Tools and Applications 2022 82:2*, vol. 82, no. 2, pp. 1669–1748, Jun. 2022, doi: 10.1007/S11042-022-13248-6.

[27] H. Ghazouani, “Challenges and Emerging Trends for Machine Reading of the Mind from Facial Expressions,” *SN Comput Sci*, vol. 5, no. 1, pp. 1–31, Jan. 2024, doi: 10.1007/S42979-023-02447-Z/METRICS.

[28] K. Marwa and O. Kais, “Current Challenges of Facial Recognition using Deep Learning,” *2022 19th IEEE International Multi-Conference on Systems, Signals and Devices, SSD 2022*, pp. 1980–1986, 2022, doi: 10.1109/SSD54932.2022.9955857.

[29] Y. Wen, B. Liu, L. Song, J. Cao, and R. Xie, “Facial Recognition Technology and the Privacy Risks,” *Face De-identification: Safeguarding Identities in the Digital Era*, pp. 15–20, 2024, doi: 10.1007/978-3-031-58222-6_2.

DOI: https://doi.org/10.54216/MOR.030105
Received: November 20, 2024 Revised: December 18, 2024 Accepted: January 15, 2025