A Systematic Review of Facial Recognition Methods: Advancements, Applications, and Ethical Dilemmas

Asante Fola-Rose
Department of Computer Science
Virginia State University
Petersburg, VA
folarosea@gmail.com

Enoch Solomon
Department of Computer Science
Virginia State University
Petersburg, VA
esolomon@vsu.edu

Keshawn Bryant
Department of Computer Science
Virginia State University
Stafford, VA
keshawnbbbryant@gmail.com

Abraham Woubie
Silo AI
Helsinki, Finland
abraham.zewoudie@silo.ai

***Abstract*—This paper provides an in-depth analysis of facial recognition systems, its advancements, applications, and the ethical dilemmas it presents in today's digital era. It examines the latest developments in facial recognition, including techniques, essential libraries, datasets, and ongoing research to enhance system robustness and expand application areas. The advantages of facial recognition, especially in security enhancement, are discussed, along with the controversies and concerns it raises, including privacy intrusion, bias, discrimination, and the potential for ubiquitous surveillance. The paper underscores the pressing need for comprehensive regulation and responsible use of this system. The emergence of AI-generated faces and their increasing realism present new challenges, particularly for identity verification processes. The societal implications of these developments, both beneficial and risky, are explored, including the threats associated with deepfakes and misinformation. The paper also discusses the potential applications of facial recognition in healthcare, education, and retail, while addressing the privacy issues that its use in these sectors may raise. It further delves into the key issues related to facial recognition, such as lack of transparency and consent, mass surveillance, racial bias and discrimination, data breaches, and accuracy issues. Looking ahead, the paper emphasizes the need to address ethical and privacy issues as the systems evolve, the importance of implementing robust regulations, ensuring transparency in data collection and use, and the continuous monitoring of the societal impact of these systems.**

I. Introduction

Facial recognition systems, at its core, is an automated process that identifies and verifies individuals by analyzing distinct facial features. It leverages sophisticated algorithms and machine learning to discern intricate patterns and match them against a database of known individuals or facial templates. This system has rapidly ascended to a pivotal role across various sectors of our society, redefining security, accessibility, and efficiency. This paper will explore the intricacies of facial recognition systems, This paper also shows the evolution to its present-day self with its invaluable use in law enforcement agencies this is just one example, but the rise of facial recognition technologies in different companies and agencies can pose some ethical dilemmas, deeper in this paper we will take a look behind the curtain of Facial recognition and delves into the ethical dilemmas within this method, with topics like racial bias and discrimination. In addition to that, this paper also shows its profound role in shaping our future. It will delve into its diverse applications, highlighting its paramount significance in various sectors. An essential emphasis is on integrating facial recognition systems into the detection of deepfake images to address the issue effectively [1]–[8]. Employing capabilities such as the suggested method, proposed by Sun, Y., Wang, X., & Tang, X. [9], to learn high-level features revealing identities for face verification involves leveraging the feature extraction hierarchy of deep ConvNets. These features are amalgamated from mid-level features across various scales, facilitating the detection of AI-generated faces.

II. State of The Art of Facial Recognition

A. Unveiling Facial Recognition

Facial recognition, a swiftly advancing bio-metric technique, is gaining traction in diverse fields, from fortifying security systems to authenticating users. The latest breakthroughs in deep learning have substantially enhanced the precision and resilience of facial recognition system [10].

B. Facial Recognition Techniques

Convolutional Neural Networks (CNNs): CNNs have revolutionized the precision of facial recognition systems. Networks such as VGGFace [11] and FaceNet [12] exhibit supe-

2835-5776/24/$31.00 ©2024 IEEE
DOI 10.1109/IRI62200.2024.00070

rior performance by adeptly identifying and leveraging facial characteristics.

- **VGGFace**:
  - **Dataset**: VGGFace was trained on a dataset with 2.6 million images of 2,622 identities.
  - **Performance**: Achieved 97.27% accuracy on the Labeled Faces in the Wild (LFW) benchmark dataset [11].
- **FaceNet**:
  - **Dataset**: FaceNet was trained on a dataset with 200 million images of 8 million identities.
  - **Performance**: Achieved 99.63% accuracy on the LFW dataset and 95.12% on the YouTube Faces DB (YTF) [12].

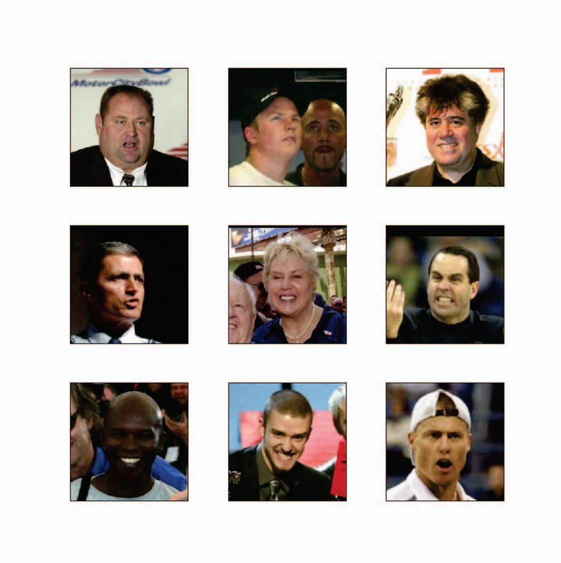

Fig. 1. Sample- Labeled Faces in the Wild [13]

3D Facial Recognition: Conventional 2D facial recognition grapples with changes in lighting and pose. 3D facial recognition, which incorporates depth data, provides a potential solution. Microsoft's Azure Kinect, with its depth-sensing capabilities, showcases the possibilities of 3D techniques. In a recent evaluation, 3D facial recognition systems using Azure Kinect demonstrated significant improvements, achieving an average accuracy of 98.3% in controlled environments [14].

C. Essential Libraries and Datasets

Key libraries for facial recognition research encompass OpenCV, Dlib, and TensorFlow. OpenCV is an indispensable resource for image processing and computer vision, playing a pivotal role in facial recognition applications. Dlib offers capabilities for facial landmark detection and recognition, while TensorFlow facilitates the deployment of deep learning models. Datasets like Labeled Faces in the Wild (LFW), CelebA, and MS-Celeb-1M are crucial for training and assessing facial recognition algorithms.

D. Deep Learning Methods in Facial Recognition

It's essential to delve into various deep learning methods utilized in the field to provide a deeper understanding of facial recognition methods. These methods include:

TABLE I
FUTURE DIRECTIONS IN FACIAL RECOGNITION

Neural Network Architecture	Use Cases	Specifications
Convolutional Neural Networks	Image classification, Object detection	Input layer, Convolutional layers, Pooling layers, Fully connected layers, Output layers
Recurrent Neural Networks	Speech and audio processing	Input layer, Recurrent layers, Output Layers
Generative Adversarial Networks	Image enhancement, Text to image synthesis	Generator, Discriminator, Adversarial loss
Siamese Networks	Face Verification, Plagiarism Detection	Twin networks, Shared weights
Capsule Networks	3D Shape recognition, Object Recognition	Capsules, Dynamic routing

1) Convolutional Neural Networks (CNNs): CNNs are particularly effective for analyzing visual imagery by utilizing convolutional layers, pooling layers, and fully connected layers to extract and learn spatial hierarchies of features from input images. CNNs typically achieve high accuracy in static image-based facial recognition, making them the most widely used method in this field. For example, state-of-the-art CNN architectures can achieve accuracy rates exceeding 99.8% on benchmark datasets like LFW (Labeled Faces in the Wild) [15].

2) Recurrent Neural Networks (RNNs): RNNs are designed for sequence prediction problems and are suitable for tasks involving time-series data or sequences of images. They are beneficial for video-based facial recognition and facial expression recognition. However, for static images, RNNs are generally outperformed by CNNs. RNN-based models can achieve around 95% accuracy in video-based facial recognition tasks [15].

3) Generative Adversarial Networks (GANs): GANs consist of a generator and a discriminator trained simultaneously through adversarial processes. They are excellent for data augmentation, generating diverse and realistic facial images, and enhancing training datasets. GAN-augmented CNNs can achieve higher robustness and accuracy, improving performance by 1-2% in some cases compared to non-augmented models [15].

4) Siamese Networks: Siamese networks are effective for face verification and one-shot learning tasks, capable of learning from a few examples. They use twin network architecture and contrastive loss to determine the similarity between input pairs. Siamese networks are ideal for verification scenarios, achieving accuracy rates above 95% for tasks like face verification on datasets such as the AT&T database [15].

5) Capsule Networks: Capsule networks preserve spatial hierarchies and pose information, improving robustness to transformations. They use dynamic routing algorithms to maintain the pose and spatial orientation of features. Capsule networks offer promising improvements in handling variations in pose and occlusion, with early research showing accuracy improvements of up to 2-3% over traditional CNNs in certain conditions [15].

6) Summary: In summary, CNNs remain the most effective and widely used method for static image-based facial recognition due to their high accuracy and established frameworks. RNNs add value in sequence-based applications, such as video facial recognition, while GANs enhance data augmentation capabilities. Siamese networks are ideal for verification tasks, and capsule networks offer potential improvements in handling spatial hierarchies and transformations. The choice of method depends on the specific requirements of the facial recognition task, the nature of the data, and available computational resources.

III. Benefits and Advantages of Facial Recognition Methods

Facial recognition methods offer several significant benefits and advantages, particularly in the realm of security. One of the primary security advantages is the uniqueness and permanence of facial features. Unlike passwords or lock combinations, which can be stolen or compromised, an individual's face provides a secure and reliable means of authentication. This makes facial recognition an effective tool for securing personal devices, such as smartphones, as it reduces the risk of unauthorized access.

Facial recognition also has assisted in locating missing persons. By integrating this method into cameras in public spaces, such as cities and stores, it becomes possible to track and find missing individuals more effectively. This widespread deployment can provide valuable assistance in search and rescue operations, potentially reuniting missing persons with their families more quickly.

Moreover, the facial recognition system has become an integral part of airport security worldwide. Bio-metric passports equipped with facial recognition capabilities expedite security procedures while enhancing overall safety. Despite privacy concerns, airports have demonstrated that facial recognition can bolster security while optimizing operations.

In the United Kingdom, a facial recognition system is being used to combat gambling addiction. By tracking the movements of registered gambling addicts within establishments, this system can promptly alert staff for intervention, streamlining effective self-exclusion procedures.

Overall, the application of facial recognition methods in security and public safety highlights its potential to offer robust protection and support in various scenarios. As the system continues to advance, its benefits are likely to expand, further enhancing its utility and effectiveness.

IV. Privacy Concerns and Misuse of Facial Recognition Systems

Facial recognition has become increasingly prevalent, offering both remarkable capabilities and significant risks. Its adoption spans various applications, from unlocking phones and enhancing security to tagging friends in social media photos and identifying individuals in public events. However, the rise of these systems brings forth a myriad of ethical and privacy concerns that must be carefully addressed.

A. Privacy Intrusion and Lack of Consent

The unregulated use of facial recognition systems intrudes upon individual privacy. Surveillance cameras capture faces without consent, raising ethical concerns. Unauthorized access to sensitive information, such as purchasing history or credit reports, can result from unauthorized deployment. Transparency and informed consent are crucial to mitigating these risks. The system's extensive deployment raises ethical concerns, emphasizing the need for ethical guidelines and regulatory frameworks [16].

B. Mass Surveillance and Surveillance State Concerns

The ubiquitous presence of facial recognition systems in public spaces, including streets and shopping centers, fosters a pervasive sense of surveillance. The ability to track public movements on a large scale can infringe upon democratic rights, eroding personal privacy and freedom. Instances of police requesting Ring camera footage during protests underscore the potential misuse of surveillance technology. Widespread adoption by government entities raises fundamental questions about civil liberties and the potential for unwarranted surveillance of citizens, potentially stifling dissent and curtailing freedom of expression.

C. Racial Bias and Discrimination

TABLE II
Mean and Median Face Quality Scores [17]

Race	**Training Set**		**Test Set**	
	Mean	**Median**	**Mean**	**Median**
African	71.59	73.66	70.10	72.33
Asian	66.59	69.74	67.50	69.18
Caucasian	69.26	71.26	67.92	69.62
Indian	68.73	71.69	69.33	71.36

Facial recognition algorithms have exhibited racial, gender, and age biases, leading to discriminatory outcomes. Extensive studies have revealed that these algorithms tend to exhibit lower accuracy rates in identifying individuals with darker skin tones, females, and older individuals [17]. As demonstrated in Table II, the mean and median face quality scores vary across different racial groups, which may contribute to the observed biases in facial recognition technology. This racial and gender bias has alarming implications, including the potential for racial profiling and gender discrimination. Ethical guidelines and regulatory frameworks are essential to protect individual rights and ensure the fair and accountable use of the technology.

D. Data Breaches and Privacy Infringement

Storing facial recognition data poses significant risks. Data breaches could expose sensitive information, compromising individuals' privacy. The consequences of such breaches extend beyond financial implications, as they can result in identity theft and the misuse of biometric information. Robust security measures are necessary to safeguard against unauthorized access and protect personal data [18].

E. Accuracy and Misidentification

Facial recognition systems are not infallible. False positives and misidentifications can have severe consequences, especially in law enforcement or security contexts. Ensuring high accuracy and minimizing errors is crucial to prevent wrongful accusations and potential harm to individuals.

F. State-Level Regulation

While the federal government remains at a standstill regarding comprehensive privacy laws, state legislators are taking matters into their own hands:

- Illinois Law: Illinois has been at the forefront by allowing a private right of action for violations related to facial recognition and biometric data use.
- Other States: Several other states are also exercising their regulatory power. For instance, New York City police have used facial recognition from thousands of cameras to identify individuals since 2017.

G. Patchwork of U.S. Law

At the federal level, there is no comprehensive law specifically regulating facial recognition systems. Instead, U.S. law's addressing this system remains a patchwork:

- Bio-metric Legislation: Three states—Illinois, Washington, and Texas—have passed bio-metric legislation, but the Washington statute does not specifically encompass facial recognition [19].
- Proposed Bills: While there is no federal law yet, numerous bills have been proposed to address facial recognition.

In summary, the states are leading the way in regulating facial recognition, emphasizing the importance of clear guidelines on data collection, storage, and usage. As technology evolves, finding the right balance between innovation and privacy protection remains a critical challenge.

V. The Future and Diverse Application of Facial Recognition Methods

As we look towards the future, the role of facial recognition methods is set to expand even further. The integration of AI and machine learning will continue to enhance the accuracy and efficiency of facial recognition systems. However, as technology advances, so too do the ethical and privacy concerns. It is crucial that as we embrace the benefits of facial recognition, we also address these challenges head-on. This includes implementing robust regulations, ensuring transparency in data collection and usage, and continuously monitoring the impact of these systems on our society.

Furthermore, facial recognition methods is poised to find utility in diverse sectors such as law enforcement, border control, healthcare, education, and retail. Its potential applications are vast and transformative. For instance, facial recognition systems can revolutionize patient identification in the healthcare sector, ensuring the right treatment is administered to the right person. Additionally, its application in emotion recognition provides valuable insights for mental health treatment. In education, facial recognition can facilitate attendance tracking and exam proctoring, ensuring fairness and integrity. Similarly, retailers can utilize facial recognition for personalized advertising and to prevent shoplifting. However, concerns regarding consumer privacy and consent must be addressed, particularly in highlighting the usage of facial recognition methods in deepfake image detection [20], [21].

A. AI-Generated Faces: Opportunities and Threats to Identity Verification

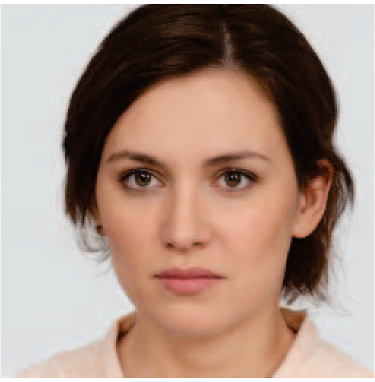

Fig. 2. AI generated women from generated.photos [22]

Advancements in AI have led to the creation of increasingly realistic AI-generated faces, presenting both opportunities and significant challenges. Our study at Virginia State University found that the Facial Recognition System with Deep Learning we developed could only correctly identify AI-generated images 61% of the time. This poses a considerable threat, as AI-generated faces can be used maliciously, creating fake images of public figures in compromising situations and potentially bypassing facial recognition systems to facilitate fraudulent activities. It is suggested that deepfake detection by deep Learning Methods can be done via a cross-modal integration utilizing, Fake Audio detection, Fake Image detection, Fake Hybrid multimedia detection, and Fake video detection [23], [24].

The rapid development of AI systems makes it challenging to fully understand and counteract the potential for malicious actions posed by AI-generated images. As we continue to navigate the future of facial recognition, it is essential to consider these threats and work towards mitigating them. Developing advanced detection techniques to identify AI-generated faces and prevent their misuse is crucial to maintaining the integrity of identity verification processes and ensuring security in various applications [25].

B. Impact of AI-Generated Faces on Society

The increasing use of AI-generated faces can have profound implications for society. While they can be utilized positively in areas such as entertainment and advertising, they also present risks like deepfakes and misinformation. Understanding these implications is crucial for developing appropriate responses and safeguards. In recent years, the rise of deepfake technology has introduced new challenges to various domains, including finance [7], [32]–[35]. A notable case involved a finance worker at a multinational firm unwittingly transferring a staggering $25 million to fraudsters posing as colleagues during a video conference call. The perpetrators skillfully manipulated deepfake technology to impersonate the company's chief financial officer (CFO) and other staff members [26].

C. The Deep Fake Scam

Setup: The unsuspecting finance worker participated in a video call, believing it involved several colleagues. However, unbeknownst to them, all the participants were deepfake recreations. The fraudsters expertly mimicked the appearance and voices of real employees.

Deception: The deep fake CFO instructed the worker to carry out a secret transaction. Despite initial suspicions, the worker was convinced by the seemingly authentic interactions with other attendees.

Costly Outcome: The worker remitted a total of $25 million to multiple bank accounts, falling victim to the elaborate ruse. The scam was only discovered later when the employee cross-checked with the corporation's head office [27].

D. Understanding Facial Recognition and Deep Learning Solutions to the Deepfake issue

Recent events have highlighted the pressing need for advanced facial recognition systems. These systems should be capable of differentiating between real individuals and those impersonating others using deepfake technology. Current methods, unfortunately, are not well-suited to counter such complex attacks. Another research method was able to detect deepfake images only 36.79% of the time [24]. The enhancement and utilization of facial recognition methods is a key step forward. Even in situations where their use might not seem necessary, these improved systems can offer an additional layer of security. This can help prevent fraudulent activities and scams. On another front, the creation of AI-powered tools to specifically identify deepfakes is of utmost importance. These tools, powered by deep machine learning, should be designed to pick up on minor details such as micro-expressions and inconsistencies. This will aid in the detection of fraudulent individuals. In essence, the combination of improved facial recognition and deep learning solutions can provide a robust defense against the increasing threat of deep fake impersonation [28]. It is a necessity to utilize the technology we have to be able to combat deepfake images to protect the welfare of the public.

VI. Consolidated Future Directions in Facial Recognition

TABLE III
FUTURE DIRECTIONS IN FACIAL RECOGNITION

Area	**Key Focus**
Robustness	Ethical concerns, Application domains
Integration	Accuracy with voice/Fingerprint ID
Design	Bias, explainable AI for acceptance
Practices	Collaboration, Public education
Learning	Adaptation to threats like deep fakes
Collaboration	Human-machine decision-making synergy
Cultural	Global deployment, Cultural nuances
Security	Defense against adversarial attacks
Participation	Public input in Facial Recognition Tech

Present research in facial recognition is geared towards enhancing system robustness, addressing ethical concerns, broadening application domains, and integrating with other biometric modalities. The evolution of facial recognition methods is intertwined with emerging technologies like edge computing and blockchain, which are gaining attention for their potential to boost speed, efficiency, and address data privacy and security issues [29].

The progression towards cross-modal integration, merging facial recognition with other forms of identification such as voice or fingerprint, augments accuracy and robustness in varied scenarios. [30]. Concurrently, the focus on human-centric design and explainable AI models is paramount to address algorithmic bias and deep learning opacity, ensuring widespread acceptance [31].

With the global prevalence of facial recognition, establishing standardized practices and fostering collaboration among stakeholders, including researchers, industry experts, policymakers, and advocacy groups, is crucial for responsible and ethical technology usage. Additionally, public awareness and education on facial recognition capabilities, limitations, and risks are vital considering the ethical implications.

Research is also directed towards adaptive learning mechanisms for continuous improvement, particularly in changing conditions and emerging threats like deep fake detection. The integration of facial recognition systems with human decision-making processes emphasizes the collaboration between humans and machines, leveraging the strengths of both.

Cross-cultural considerations are essential when deploying facial recognition globally, as cultural nuances significantly impact acceptance and effectiveness. Ensuring robustness against adversarial attacks and understanding the long-term social and economic impacts of facial recognition adoption are also critical areas of focus.

Lastly, promoting public participation in decision-making processes related to facial recognition technology is crucial for transparency. Research should investigate mechanisms for public input, impact assessments, and avenues for discourse [36].

VII. Conclusion

Facial recognition systems, a revolutionary development, has permeated numerous sectors such as healthcare, education, and retail, transforming their operations. Yet, its ubiquitous deployment has sparked intense debates around ethical implications. Concerns encompassing transparency, consent, mass surveillance, racial bias, discrimination, data security, and accuracy are at the forefront of these discussions.

Regulatory oversight is paramount in this context. It is incumbent upon authorities at all levels to devise regulations that ensure the responsible use of facial recognition technology. Such regulations should effectively address the ethical dilemmas and strike a balance between fostering technological progress and safeguarding privacy rights.

The emergence of deepfake technology underscores the necessity for sophisticated facial recognition systems and AI tools capable of detecting and mitigating such threats. This is especially critical in sectors like finance where identity verification is of utmost importance.

To sum up, as we chart the course for the future of facial recognition technology, insights gleaned from these experiences will inform the creation of robust, ethical, and effective systems.

References

[1] Solomon, E., Woubie, A. & Cios, K. UFace: An Unsupervised Deep Learning Face Verification System. *Electronics*. **11**, 3909 (2022)

[2] Solomon, E., Woubie, A. & Emiru, E. Unsupervised Deep Learning Image Verification Method. *ArXiv Preprint ArXiv:2312.14395*. (2023)

[3] Solomon, E., Woubie, A. & Emiru, E. Autoencoder Based Face Verification System. *ArXiv Preprint ArXiv:2312.14301*. (2023)

[4] Solomon, E., Woubie, A. & Emiru, E. Deep Learning Based Face Recognition Method using Siamese Network. *ArXiv Preprint ArXiv:2312.14001*. (2023)

[5] Solomon, E., Woubie, A. & Emiru, E. Self-supervised Deep Learning Based End-to-End Face Verification Method using Siamese Network. *2023 IEEE International Conference On Service Operations And Logistics, And Informatics (SOLI)*. pp. 1-6 (2023)

[6] Solomon, E., Woubie, A. & Emiru, E. Nearest Neighbor Based Unsupervised Deep Learning Image Recognition Method. *2023 International Conference On Modeling, Simulation & Intelligent Computing (MoSICom)*. pp. 592-596 (2023)

[7] Solomon, E. Face Anti-Spoofing and Deep Learning Based Unsupervised Image Recognition Systems. (2023)

[8] Woubie, A., Solomon, E. & Attieh, J. Maintaining Privacy in Face Recognition using Federated Learning Method. *IEEE Access*. (2024)

[9] Yi Sun, Xiaogang Wang, and Xiaoou Tang. Deep Learning Face Representation from Predicting 10,000 Classes. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pages 1891–1898, September 2014. doi: 10.1109/CVPR.2014.244.

[10] LeCun, Y., Bengio, Y. & Hinton, G. Deep learning. *Nature*. **521**, 436-444 (2015)

[11] Parkhi, O., Vedaldi, A. & Zisserman, A. Deep face recognition. *BMVC 2015-Proceedings Of The British Machine Vision Conference 2015*. (2015)

[12] Schroff, F., Kalenichenko, D. & Philbin, J. Facenet: A unified embedding for face recognition and clustering. *Proceedings Of The IEEE Conference On Computer Vision And Pattern Recognition*. pp. 815-823 (2015)

[13] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, ”Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments,” University of Massachusetts, Amherst, 2007. [Online]. Available: https://www.tensorflow.org/datasets/catalog/lfw.

[14] Albert, J., Owolabi, V., Gebel, A., Brahms, C., Granacher, U. & Arnrich, B. Evaluation of the pose tracking performance of the azure kinect and kinect v2 for gait analysis in comparison with a gold standard: A pilot study. *Sensors*. **20**, 5104 (2020)

[15] K. Choudhary, B. DeCost, C. Chen, A. Jain, F. Tavazza, R. Cohn, C. W. Park, A. Choudhary, A. Agrawal, S. J. L. Billinge, E. Holm, S. P. Ong, C. Wolverton, Recent advances and applications of deep learning methods in materials science.

[16] Ruhrmann, H. Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement. (Center for Information Technology Research in the Interest of Society . . . ,2019)

[17] Manideep Kolla and Aravinth Savadamuthu. The Impact of Racial Distribution in Training Data on Face Recognition Bias: A Closer Look. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) Workshops*, pages 313–322, January 2023

[18] Buolamwini, J. & Gebru, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. *Conference On Fairness, Accountability And Transparency*. pp. 77-91 (2018)

[19] Yew, R. & Xiang, A. Regulating facial processing technologies: Tensions between legal and technical considerations in the application of Illinois BIPA. *Proceedings Of The 2022 ACM Conference On Fairness, Accountability, And Transparency*. pp. 1017-1027 (2022)

[20] ACLU The Dawn of Robot Surveillance. (2019), https://www.aclu.org/report/dawn-robot-surveillance/

[21] Meruyert Serik, Nassipzhan Duisegaliyeva, and Danara Tleumagambetova. Creating a Proctoring System Using Neural Network in the Educational Process. In: Proceedings of the 2023 7th International Conference on Advances in Artificial Intelligence, 2023, pp. 98–105.

[22] ”Female with brown eyes and joyful expression,” Generated Photos. [Online]. Available: https://generated.photos/faces/brown-eyes/joy/female.

[23] Poredi, N., Sudarsan, M., Solomon, E., Nagothu, D. & Chen, Y. Generative adversarial networks-based AI-generated imagery authentication using frequency domain analysis. *Disruptive Technologies In Information Sciences VIII*. **13058** pp. 376-390 (2024)

[24] Arash Heidari, Nima Jafari Navimipour, Hasan Dag, and Mehmet Unal. “Deepfake detection using deep learning methods: A systematic and comprehensive review.”

[25] Forum, W. What cybersecurity threats does generative AI expose us to?. (2023), https://www.weforum.org/agenda/2023/06/what-cybersecurity-threats-are-posed-by-generative-ai/

[26] Manheim, K. & Kaplan, L. Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech.*. **21** pp. 106 (2019)

[27] Ghazi-Tehrani, A. & Pontell, H. Phishing evolves: Analyzing the enduring cybercrime. *The New Technology Of Financial Crime*. pp. 35-61 (2022)

[28] Ali, W., Tian, W., Din, S., Iradukunda, D. & Khan, A. Classical and modern face recognition approaches: a complete review. *Multimedia Tools And Applications*. **80** pp. 4825-4880 (2021)

[29] Jha, M., Tiwari, A., Himansh, M. & Manikandan, V. Face Recognition: Recent Advancements and Research Challenges. *2022 13th International Conference On Computing Communication And Networking Technologies (ICCCNT)*. pp. 1-6 (2022)

[30] Rahul Sharma and Shrikanth Narayanan. ”Audio-visual activity guided cross-modal identity association for active speaker detection.” IEEE Open Journal of Signal Processing, vol. 4, 2023, pp. 225–232.

[31] Jordan Richard Schoenherr et al. ”Designing AI using a human-centered approach: Explainability and accuracy toward trustworthiness.” IEEE Transactions on Technology and Society, vol. 4, no. 1, 2023, pp. 9–23.

[32] Solomon, E. & Cios, K. FASS: Face anti-spoofing system using image quality features and deep learning. *Electronics*. **12**, 2199 (2023)

[33] Solomon, E. & Cios, K. HDLHC: Hybrid Face Anti-Spoofing Method Concatenating Deep Learning and Hand-Crafted Features. *2023 IEEE 6th International Conference On Electronic Information And Communication Technology (ICEICT)*. pp. 470-474 (2023)

[34] Woubie, A., Solomon, E. & Emiru, E. Image Clustering using Restricted Boltzman Machine. *ArXiv Preprint ArXiv:2312.13845*. (2023)

[35] Solomon, E. & Woubie, A. Federated Learning Method for Preserving Privacy in Face Recognition System. *ArXiv Preprint ArXiv:2403.05344*. (2024)

[36] Muhammad Ade Kurnia Harahap et al. ”The Role of Information Technology in Improving Urban Governance.” Jurnal Minfo Polgan, vol. 12, no. 1, 2023, pp. 371–379.