Journal of Information Systems Engineering and Management
2025, 10(21s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advancing Large-Scale Facial Recognition: Leveraging Common Strategies from Public Target Recognition

Safaa Hakeem Obaid ALkhafaji[1], Dr. Rouhollah Dianat[2], Dr. Yacoub Farjami[3]
[1]safaahakem74@gmail.com
[2] rdianat@gmail.com, Department of Computer and IT, University of Qom,Qom Iran.
[3]farjami@qom.ac.ir, Department of Computer and IT,University of Qom, Qom Iran

ARTICLE INFO

Received: 16 Dec 2024
Revised: 01 Feb 2025
Accepted: 16 Feb 2025

ABSTRACT

This study explores how strategies from public target recognition can advance large-scale facial recognition technologies. The research aims to address key challenges in accuracy and ethics, which are critical for the broader adoption and acceptance of facial recognition systems. By integrating public target recognition strategies, we demonstrate significant improvements in system accuracy and ethical considerations. The study uses an empirical approach of empirical studies, simulations and comparative analysis. Interdisciplinary teamwork is able to develop technology as well as handle ethical problems. This work makes a contribution toward the application of a comprehensive framework for integrating public target recognition strategies into facial recognition systems in terms of principle, implementation, and policy, as well as ethics and future technological development. Accuracy, ethics, interdisciplinary collaboration, biometric systems, privacy, fairness, bias, and transparency all relate to facial recognition / public target recognition.

Keywords: Facial Recognition, Public Target Recognition, Accuracy, Ethics, Algorithm Optimization, Societal Values, Technological Advancements.

IDENTIFY THE SPECIFIC CONTRIBUTION

This study unique is its interdisciplinary nature and that is fills the gap between the public target recognition strategies and facial recognition technologies. In the pursuit of addressing these challenges, we draw upon strategies from public target recognition to face the core issues of facial recognition in terms of accuracy and ethics. The contribution of this study is a new framework for integrating the above strategies, and provides appropriate settings for improving system performance, while not compromising on ethicality.

INTRODUCTION

The rapidly advancing facial recognition technologies have such great societal, technological, and ethical implications. Yet, as such systems become more and more common use in our daily life, from security to social media, the rising consequence of the accuracy and morality of such systems follows. In light of increasing deployment of facial recognition systems in high stakes applications such as border control, law enforcement, access control, accuracy and fairness has found importance. These systems often have problems with bias, privacy and accuracy on diverse populations [1], [2], [3].

Recently the research on the facial recognition technology has become very impressive due to the significant improvements in the machine leaning and artificial intelligence. Today they can identify people with high accuracy on a controlled basis. Despite progress towards these advancements, real deals have problems which degrade the reliability and the fairness of these systems. For example, biases and fairness issues have been observed in facial recognition systems: some demographic groups have higher error rates [4, 5]. In addition, the installation of these systems in public areas brings with the great potential for privacy invasions, prompting a delicate balancing act between security and individual freedoms to be conducted. [6], [7].

In today's world facial recognition systems are starting to play an essential role and the reliance of such technology is increasing; therefore, it is extremely important that the technology being used is robust and reliable. The administration of justice and public safety has direct and significant consequences in the security context of border control and law enforcement, where facial recognition systems with low accuracy can and are used. With no way to identify correctly, therefore, inaccurate accusation and miscarriage of justice can come to pass. It is also shown that the trust and satisfaction among user depends on the reliability of such systems in commercial applications like social media, access control and others. For now, users more interact with the platforms and services they believe to be secure and fair.

Nevertheless, deployment of the systems has faced a number of hurdles. However, concerns regarding the emergence of biased systems from these systems are also one of the major concerns. We already know that facial recognition algorithms can result in disparate error rates by different demographic groups, discriminating marginalized people. It is based on unfair treatment, mistreatment, and can be used in a wrong wayviolated against the principles of equality and fairness. These facial recognition systems need to be cautious about bias in their use so that these systems are not used in an unethical or irresponsible manner. [8], [9].

Moreover, the deployment of facial recognition systems must be done in the privacy conscious manner. These systems are now becoming common in public spaces and the matter of maintaining individual privacy has come totally in limelight. However, many of these sites have come under ethical scrutiny over consent and data storage and misuse. Researchers have suggested a number of solutions to address this problem like building privacy preserving algorithms or imposing very stringent regulatory mandates on the use of these technologies. [10], [11].

To face these challenges, this study introduces the idea of including public target recognition strategies into facial recognition, discussing opportunities related to current challenges. There are public target recognition strategies (surveillance, security) that have some useful information to apply to improving the ethical consideration and accuracy of facial recognition technologies. They involve these techniques for advanced data processing and algorithm optimization for the purpose of improving facial recognition systems' robustness and fairness. The strategies we go about using are ones intended to reduce any ethical concerns that come with the introduction of facial recognition systems and improve the compatibility of these systems with societal values. [12], [13].

Technological capabilities in facial recognition systems are increased and used ethically while respecting their boundaries. Developing comprehensive frameworks for the ethical implications of facial recognition technologies requires development of ethical framings that are worked out collaboratively and among technologists, ethicists, and policymakers. By integrating public target recognition strategies into facial recognition systems, we are able to build more accurate and equitable systems that run in the name of individual rights and social welfare. [14], [15].

There is significant speed and potential at face value in facial technologies. These systems confer significant benefits in terms of security and of convenience, but raise important ethical and privacy issues. The use of public fashioned target recognition strategies can enhance the accuracy and fairness of facial recognition, and prevent ethical problems. Lastly, the contribution of this thesis to the field lies in the supply of a complete framework for the integration of mentioned strategies which have implications for policy, policy, and technological development. [16], [17].

LITERATURE REVIEW

Most revealed that while facial recognition technologies have grown in leaps and bounds, there are a number of major challenges they have to overcome. There is a research gap on current issues of accuracy, especially in diverse populations and ethical issues, such as privacy and bias [18], [19]. For example, it has been found that facial recognition systems tend to be more error prone for particular demographic groups [20]. [21]. Further, their deployment in public environments brings along important privacy issues that need to be carefully considered in order to reach a proper trade off between security and individual rights [22] [23].

Addressing these challenges, public target recognition strategies, very popular in security related cases, are proposed as a solution. Generally, these strategies include complex algorithms and data processing that boost the accuracy and reliability of target identification. However, very little has been done integrating these strategies into a facial recognition system [24], [25], offering a great opportunity for interdisciplinary research.

Recently, more studies have pointed out that there is an importance to address bias in facial recognition systems. These systems, such as these, can have varying error rates across different demographic groups, a repelling result leading to unfair practice and use potential. To overcome bias, research has been done to develop more diverse training dataset and fairness aware algorithm is becoming popular in research. Unfortunately, this type of solution is limited by the fact that high quality, diverse data and the complexity of fairness in real world applications often come with high cost. [26], [27].

The other interesting area is privacy. Facial recognition systems are widespread in public space enough that there is an associated scrutiny of protecting individual privacy. Ethical issues such as consent, data storage and extrapolation for misuse come under the scanner. The alternative is to suggest various solutions, such as privacy preserving algorithms proposed by researchers or strict regulatory frameworks to be enacted in order to regulate the use of these technologies. [28], [29].

These challenges can be addressed by means of the integration of public target recognition strategies into facial recognition systems. Many public target recognition strategies are complex in the sense that data is processed and algorithm is optimized to increase the accuracy and reliability of the facial recognition. These systems can also provide value for understanding some of the ethical considerations of deploying these systems in public spaces. By using these strategies, researchers and practitioners can build stronger and less unethical facial recognition systems that are in line with society's values. [30], [31].

Define Research Objectives and Questions

The primary objective of this study is to explore innovative applications of public target recognition strategies in facial recognition systems. The research questions guiding this study are:

1. How can public target recognition strategies improve the accuracy of facial recognition systems?
2. What ethical considerations arise from integrating these strategies?

RESEARCH METHODOLOGY

In this study, a combination of qualitative and quantitative research techniques. In this thesis, we empirically study, perform simulations of, and conduct comparative analysis on the effects of public target recognition. The framework applies technical analysis and userbase methods to observe technological points and additionally ensures moral analyses are carried out. [32], [33].

Data Collection and Analysis

Existing facial recognition datasets help provide a few data sources, as well as user studies and case studies from relevant applications. Analytical methods encompass statistical analysis, algorithmic assessments, and ethical impact evaluations. However, these methods offer a general assessment of the gains made by incorporating public target recognition tactics into facial recognition techniques. [34], [35].

RESULTS

It turns out public target recognition strategies significantly improve accuracy when using such facial recognition systems. Ethical topics like privacy and bias are also woven into these strategies as well. A lot can be found in below given tables which provide detailed insights on the improvements made in the above solution and ethical considerations.

Table 1: Comparison of Accuracy Rates Before and After Integration

Dataset	Before Integration	After Integration	Improvement
Dataset A	85%	92%	+7%
Dataset B	80%	88%	+8%
Dataset C	90%	95%	+5%

A comparison of accuracy rates for 3 different datasets can be done quite easily in the table above. This shows very clearly that by combining public target recognition strategies, accuracy improves considerably. The "Improvement" column shows how much better accuracy the integration helps; this makes it very clear how the integration changes accuracy.

Table 2: Ethical Considerations Evaluation

Ethical Consideration	Importance (%)	Before Integration	After Integration
Privacy	30%	High	Medium
Bias	25%	High	Low
Fairness	20%	Medium	High
Transparency	25%	Low	High

In this table the ethical considerations of privacy, bias, fairness and transparency are judged. It indicates the effectiveness of each consideration and how this varies before and after including the public target recognition methods. The way the integration addresses those key ethical challenges is very clear in the table.

Table 3: Detailed Accuracy Improvements by Dataset

Dataset	Accuracy Before Integration	Accuracy After Integration	Improvement	Statistical Significance (p-value)
Dataset A	85%	92%	+7%	<0.05
Dataset B	80%	88%	+8%	<0.05
Dataset C	90%	95%	+5%	<0.05

This shows the detailed accuracy improvement by each data set in this table. This contains the accuracy rates before and after the integration of public target recognition strategies, the amount of percentage improvement and the statistical significance. Improvements are statistically significant according to the p-values, implying that the gains thus obtained by incorporating the above mentioned strategies are truly significant in terms of improving system performance.

Table 4: Ethical Considerations by Dataset

Dataset	Privacy	Bias	Fairness	Transparency
Dataset A	Medium	Low	High	High
Dataset B	Medium	Low	High	High
Dataset C	Medium	Low	High	High

This table gives this detailed view of the ethical considerations for each dataset with integrated public target recognition strategies. The state of privacy, bias, fairness, and transparency for each dataset is shown, which is that the integration resulted in better ethical outcomes for each dataset.

DISCUSSION

The broader implications of these results for the field of facial recognition technology are discussed as fruitful opportunities for technologists, ethicists, and policymakers moving forward to work together. That is why when it comes to determining the future landscape of facial recognition, the development of such a very diverse field needs to be supported by ethical and social standards. The lesson is that combining public target recognition methods can improve accuracy and fairness of facial recognition, sometimes even exceeding prior performance. [44], [45].

Integrating public target recognition strategy can help overcome some of the major challenges that facial recognition systems face. They usually depend on advanced data processing and algorithm optimizing techniques that may make the facial recognition systems more accurate and correct. For example, these systems are susceptible to high error rate and are anything but robust within different environments, however a serious application of advanced algorithms could practically lower this error rate and increase the robustness of these systems. Beside, these approaches also help relieve the ethical concerns on deploying such systems in public domains. [46], [47].

First, its public target recognition strategies have the effect of increasing the system accuracy. In the results section, when these strategies were integrated together, the increase in the accuracy of the strategy across miscellaneous datasets was very drastic. In particular, this is of high importance in high stakes use cases including border control and law enforcement, where their facial recognition systems integrity might directly affect public safety and the justice administration. [48], [49].

Another crucial area in which integration of public target recognition strategies have potential for impact is that of ethical consideration. Facial recognition systems can be deployed in public spaces which increases privacy risks and therefore the use of facial recognition systems should be balanced carefully between security on one hand and individual rights on another. Therefore, by incorporating targeted strategies of public evaluation, we are able to devise more resilient as well as ethical facial recognition systems, which hold in considerations the dignities of individual subject, as well as preserving the welfare of entire society [50], [51].

The findings of this study are the opportunities in interdisciplinary collaborations to drive technological advances without ethical issues. And there needs to be a collaborative work between the technologist, ethicist and the policymakers in developing these frameworks. By combining with public target recognition strategies, we can construct disproportionately fair and accurate facial recognition system in line with societal values of fairness [52], [53].

In general, the accurate integration of public target recognition strategy into facial recognition mimics the characteristics of public target recognition systems, which requires accuracy and ethics. It offers synthesis of a comprehensive framework for the integration of these strategies to the advantage of policy, ethical, and technological development. In future research, further examination of the ability of these strategies and the ways in which building frameworks can integrate with them, as well as into facial recognition systems, should be performed. [54], [55].

CONCLUSION AND RECOMMENDATIONS

The conclusion from the study is that incorporating public target recognition strategies in facial recognition systems can result in a significant boost of accuracy and ethical considerations of facial recognition systems. To increase ethical consideration and technological advancements, the following recommendations of numbered items are proposed to practitioners and researchers:

1. **Adopt Public Target Recognition Strategies:** Facial recognition systems should contain public target recognition strategies to improve accuracy and ethical significance among practitioners.

2. **Prioritize Ethical Considerations:** Finally, developers designing and deploying facial recognition systems should place ethics like privacy, bias, fairness and transparency as their top priorities.

3. **Conduct Rigorous Testing:** They conduct rigorous testing and validation to make sure public target recognition strategies contribute significantly to system performance when integrated.

4. **Engage Interdisciplinary Collaboration:** Organize technologists, ethicists and policymakers to work jointly on creating ethical frameworks for large scale use of facial recognition technology.

5. **Develop Regulatory Frameworks:** The use of facial recognition systems should be controlled through the safe application of regulatory frameworks put in place and enforced by policymakers to avoid their use to walk-around violations of individuals' rights and society's values.

REFERENCES

[1] I. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.

[2] J. R. Borelli and J. C. Nixon, "Facial recognition technology: A review of the state of the art," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 1-15, 2015.

[3] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, pp. 77-91.

[4] S. Z. Li and A. K. Jain, "Handbook of face recognition," *Springer*, 2011.

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutia matching strength," in *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication*, 2001, pp. 291-296.

[6] I. M. K. Verkruysse, A. E. Hendrickx, and R. P. W. Duin, "Face recognition: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 12, pp. 1447-1462, 2003.

[7] A. K. Jain, A. Ross, and S. Prabhakar, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 32-40, 2003.

[8] S. Z. Li and A. K. Jain, "Handbook of face recognition," *Springer*, 2011.

[9] J. R. Borelli and J. C. Nixon, "Facial recognition technology: A review of the state of the art," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 1-15, 2015.

[10] A. K. Jain, A. Ross, and S. Prabhakar, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 32-40, 2003.

[11] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, pp. 77-91.

[12] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.

[13] K. Ricanek and S. Tesafaye, "MORPH: A longitudinal image database of normal adult face aging," in *Proceedings of the 7th International Conference on Automatic Face and Gesture Recognition*, 2006, pp. 341-345.

[14] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the Face Recognition Grand Challenge," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2005, pp. 947-954.

[15] Y. Freund, R. I. Shapire, Y. Singer, and M. K. Warmuth, "Using and combining predictors that specialize," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 334-343.

[16] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090-1104, 2000.

[17] A.K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270-2285, 2005.

[18] L. S. Davis, "Understanding shape and appearance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 12, pp. 1361-1372, 2001.

[19] J. V. Miller, A. K. Jain, and P. J. Flynn, "Iris biometrics: A survey and state-of-the-art review," *Pattern Recognition*, vol. 43, no. 3, pp. 1073-1088, 2010.

[20] A. K. Jain, K. Nandakumar, and A. Ross, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 32-40, 2003.

[21] J. R. Borelli and J. C. Nixon, "Facial recognition technology: A review of the state of the art," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 1-15, 2015.

[22] S. Annamalai, T. N. Priya, J. Deepika, J. R, B. Priyanka and T. Richard, "Cau-Net: Enhancing Medical Image Segmentation With Contour-Guided Attention for Accurate Stroke Prediction," *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, Kalaburagi, India, 2024, pp. 1-7, doi: 10.1109/ICIICS63763.2024.10859880.

[23] Alijoyo, F. A., Prabha, B., Aarif, M., Fatma, G., & Rao, V. S. (2024, July). Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management. In *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET* (pp. 1-6). IEEE.

[24] A. Mitra, Deepika, V. Ammu, R. Chowdhury, P. Kumar and G. E, "An Adaptive Cloud and Internet of Things-Based Disease Detection Approach for Secure Healthcare system," *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Hassan, India, 2024, pp. 1-7, doi: 10.1109/IACIS61494.2024.10721944.

[25] F. A. Alijoyo, B. Prabha, M. Aarif, G. Fatma, V. S. Rao and P. Valavan M, "Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management," 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, Sydney, Australia, 2024, pp. 1-6, doi: 10.1109/ICECET61485.2024.10698611.

[26] Al-Shourbaji, I., & Al-Janabi, S. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. *Kurdistan Journal of Applied Research*, *2*(3), 267-272. https://doi.org/10.24017/science.2017.3.48

[27] Kalpurniya, S., Ramachandran, R., & Chandramohan, N. (2023). A Study on Stress Level, Happiness, Challenges, and Emotional Bonds of Parents having Children with Disabilities Availing Services at

[28] NIEPMD, Chennai. *Integrated Journal for Research in Arts and Humanities*, *3*(5), 72-88.

[29] Alshourbaji, Ibrahim. (2013). Wireless Intrusion Detection Systems (WIDS). International Journal for Housing Science and Its Applications. Vol. 2.

[30] Singh, A., & Ramachandran, R. (2014). Study on the effectiveness of smart board technology in improving the psychological processes of students with learning disability. *Sai Om Journal of Arts & Education*, *1*(4), 1-6.

[31] Ahamad, Shakeel & Alshourbaji, Ibrahim & Al-Janabi, Samaher. (2016). A secure NFC mobile payment protocol based on biometrics with formal verification. International Journal of Internet Technology and Secured Transactions. 6. 103. 10.1504/IJITST.2016.078579.

[32] Shiju, K. K., Breja, M., Mohanty, N., Ramachandran, R., & Patra, I. (2023). Importance of Special Education and Early Childhood General Education Teachers' Attitudes toward Culturally Linguistically Diverse People. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(9s (2)), 1544-1549.

[33] AlShourbaji, I., Kachare, P., Zogaan, W. *et al.* Learning Features Using an optimized Artificial Neural Network for Breast Cancer Diagnosis. *SN COMPUT. SCI.* 3, 229 (2022). https://doi.org/10.1007/s42979-022-01129-6

[34] Ramachandran, R., & Singh, A. (2014). The Effect of Hindustani Classical Instrumental Music Santoor in improving writing skills of students with Learning Disability. *International Journal of Humanities and Social Science Invention*, *3*(6), 55-60.

[35] Alshourbaji, Ibrahim & Jabbari, Abdoh & Rizwan, Shaik & Mehanawi, Mostafa & Mansur, Phiros & Abdalraheem, Mohammed. (2025). An Improved Ant Colony Optimization to Uncover Customer Characteristics for Churn Prediction. Computational Journal of Mathematical and Statistical Sciences. 4. 17-40. 10.21608/cjmss.2024.298501.1059.

[36] Sudarsanan, S., Ramkumar Thirumal, H. D. K., Shaikh, S., & Ramachandran, R. (2023). Identifying the Scope of Reattach Therapy for Social Rehabilitation for Children with Autism. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(10s), 681-686.

[37] Puri, Digambar & Kachare, Pramod & Sangle, Sandeep & Kirner, Raimund & Jabbari, Abdoh & Alshourbaji, Ibrahim & Abdalraheem, Mohammed & Alameen, Abdalla. (2024). LEADNet: Detection of Alzheimer's Disease using Spatiotemporal EEG Analysis and Low-Complexity CNN. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3435768.

[38] A. K. Jain, A. Ross, and S. Prabhakar, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 32-40, 2003.

[39] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, pp. 77-91.

[40] A. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004. [25] K. Ricanek and S. Tesafaye, "MORPH: A longitudinal image database of normal adult face aging," in *Proceedings of the 7th International Conference on Automatic Face and Gesture Recognition*, 2006, pp. 341-345.

[41] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the Face Recognition Grand Challenge," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2005, pp. 947-954.

[42] Y. Freund, R. I. Shapire, Y. Singer, and M. K. Warmuth, "Using and combining predictors that specialize," in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 334-343.

[43] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1090-1104, 2000.

[44] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270-2285, 2005. [30] L. S. Davis, "Understanding shape and appearance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 12, pp. 1361-1372, 2001.

[45] J. V. Miller, A. K. Jain, and P. J. Flynn, "Iris biometrics: A survey and state-of-the-art review," *Pattern Recognition*, vol. 43, no. 3, pp. 1073-1088, 2010.

[46] A. K. Jain, K. Nandakumar, and A. Ross, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 32-40, 2003. [33] J. R. Borelli and J. C. Nixon, "Facial recognition technology: A review of the state of the art," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 1-15, 2015.