Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 2, April 2024
DOI : https://doi.org/10.33395/sinkron.v8i2.13612

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Integration of Artificial Intelligence in Facial Recognition Systems for Software Security

Widi Santoso[1)*], Rahayu Safitri[2)], Samidi[3)]
[1)*,2),3)]Faculty of Information Technology, Master of Computer Science, Budiluhur University of Jakarta, Indonesia
[1*]2311600122@student.budiluhur.ac.id, [2]2311600106@student.budiluhur.ac.id, [3]samidi@budiluhur.ac.id

Submitted: March 28, 2024 | **Accepted**: April 28, 2024 | **Published**: April 30, 2024

Abstract: Facial recognition technology, a cornerstone in modern software security, has seen significant advancements through the integration of Artificial Intelligence (AI). This research focuses on enhancing facial recognition systems by incorporating sophisticated machine learning algorithms and deep neural networks. By doing so, the goal is to increase the accuracy and reliability of these systems in security applications. The study uses a variety of facial datasets to train AI models that are adept at extracting facial features and recognizing patterns. These models are subjected to rigorous testing to evaluate their performance in terms of identification accuracy, processing speed, and adaptability to different environmental conditions. One of the key challenges addressed in the research is the system's vulnerability to errors and potential misuse. Ethical considerations and privacy concerns are at the forefront of the study. The research highlights the importance of designing AI-based facial recognition systems that respect user privacy and are resistant to biases, thus fostering trust and acceptance among users. The results of the study show a marked improvement in system performance, demonstrating enhanced recognition accuracy and speed, while maintaining robustness across different conditions. By offering practical recommendations for the development of secure, ethical, and privacy-aware facial recognition systems, this research contributes valuable insights into the integration of AI in software security. It underscores the importance of continuous innovation and ethical responsibility in the deployment of facial recognition technologies, shaping the future landscape of technological security measures

Keywords: Artificial Intelligence, Facial Recognition, Software Security, Authentication, Ethical Considerations.

INTRODUCTION

In the rapidly advancing field of software security, the integration of Artificial Intelligence (AI) with facial recognition technology marks a significant innovation, enhancing both the effectiveness and reliability of security measures. This synthesis aligns closely with the research discussed earlier, where AI's deep learning and neural networks are leveraged to refine facial recognition systems (Adjabi et al., 2020; Kelly, 2022; Neugebauer, 2019; Zebua et al., 2023).

AI’s application in facial recognition is focused primarily on increasing accuracy and reducing the incidence of false positives and negatives. Traditional security systems often struggle with these challenges, especially in varying environmental conditions. By employing advanced AI algorithms capable of recognizing and analyzing complex data patterns, the systems can now accurately identify facial features and expressions, thereby minimizing errors. This capability ensures robust security not only in controlled environments but also in real-world settings where traditional systems might fail.

Moreover, the dynamic nature of AI allows facial recognition systems to continuously evolve. Each interaction enriches the AI’s learning, enabling the system to adapt and become more precise over time. This aspect of ongoing improvement is critical for maintaining security integrity in the face of constantly evolving digital threats, as mentioned in both discussions.

Ethical considerations are paramount as well, as integrating AI in facial recognition brings forth issues related to privacy and surveillance. The responsibility lies in addressing potential biases in AI algorithms and ensuring the protection of personal biometric data. Balancing enhanced security capabilities with the rights to personal privacy is a crucial component of these technological advancements.

Overall, the potential of AI-enhanced facial recognition systems in software security is vast, promising to not only bolster security measures but also transform approaches to authentication and access control.

Research in the field of AI has consistently highlighted significant improvements in the accuracy and efficiency of facial recognition systems. (Chen et al., 2020; Ilmawati et al., 2024; Patel et al., 2020), AI algorithms, especially those based on deep learning, have drastically reduced error rates in facial recognition by enhancing the system's ability to distinguish between subtle facial features across different demographics. This advancement is critical, considering the diverse environments in which these systems operate. By incorporating comprehensive datasets and iterative training models, AI not only improves identification accuracy but also speeds up the authentication process, making it nearly instantaneous and much more reliable than traditional methods.

The adaptive learning capabilities of AI are transforming facial recognition technologies into dynamic systems that evolve over time. (Li & Deng, 2020) discuss how machine learning models are applied to continuously update and refine facial recognition algorithms based on new data inputs. This adaptability is pivotal in maintaining the efficacy of security systems, particularly in scenarios where facial characteristics may change due to aging, medical conditions, or alterations in grooming styles. Such features ensure that the systems remain robust against attempts to deceive or bypass security protocols, thereby enhancing overall system resilience.

A significant portion of the literature, such as the studies (Wilkinson, 2020), addresses the ethical and privacy implications of integrating AI in facial recognition for security purposes. Concerns revolve around the potential for mass surveillance and the infringement of privacy rights. These studies advocate for stringent regulatory frameworks that mandate transparency in the use and storage of biometric data, as well as the incorporation of fairness and accountability in AI algorithms to prevent biases which could lead to discrimination.

The technical challenges of integrating AI with existing security infrastructures are non-trivial. As noted (Patel et al., 2020) issues such as data quality, system interoperability, and real-time processing demands require innovative solutions. Researchers have proposed various methods to address these challenges, including the use of hybrid cloud systems that enhance data processing capabilities and the implementation of edge computing to reduce latency in facial recognition operations (Aldi, 2024; Rathour et al., 2021; Udayana et al., 2022; Wu et al., 2022; H. Zhang et al., 2019). These solutions highlight the need for robust technical strategies to fully leverage AI capabilities in security settings.

Looking forward, the literature suggests a trend towards more autonomous security systems enabled (Wilkinson, 2020) predict that the future of facial recognition will see more integrated systems that can autonomously monitor and control access without human intervention. This shift is expected to lead to more personalized security experiences, where systems can recognize individuals not just by their facial features, but also by analyzing patterns of behavior and movement. This holistic approach could potentially offer a higher degree of security and convenience, paving the way for new applications in both public and private sectors.

This body of literature collectively emphasizes the transformative impact of AI on facial recognition technologies, highlighting both the opportunities and challenges that lie ahead. As these systems become more embedded in our daily lives, the balance between technological benefits and ethical considerations will continue to be a critical area of research and discussion

LITERATURE REVIEW

System Architecture

Artificial Intelligence (AI) stands at the forefront of a technological revolution with the potential to revolutionize various industries (Daugherty & Wilson, 2018; Fontes et al., 2022; Ullah et al., 2024). One particularly impactful application of AI is its integration into facial recognition systems, especially in the context of software security (Smith, 2020). As we navigate the digital age, the significance of facial recognition, powered by AI, becomes increasingly apparent, positioning itself as a cornerstone in access control and authentication processes (Aboukadri et al., 2024; Dyson, 2022; Wilkinson, 2020).

The architectural framework is rooted in recognizing the synergy between advanced machine learning algorithms and facial recognition systems. This synergy holds the key to unlocking new dimensions in software security, enhancing accuracy, and adaptive capabilities (Li & Deng, 2020). The deployment of AI into facial recognition heralds a paradigm shift, securing digital environments in an era of rapid technological advancements (J. Zhang & Tao, 2020). This integration is not merely a technological advancement; it is a transformative force shaping the landscape of security measures.

The gains in accuracy and efficiency achieved through AI-powered facial recognition underscore its potential to fortify software security measures significantly (Kumar et al., 2023). In the face of evolving digital threats, the need for innovative security solutions, particularly those powered by AI, becomes imperative (Gomez A, 2021). Machine learning algorithms within facial recognition systems offer a dynamic approach to adapt to diverse environmental conditions, contributing to the resilience of the entire security architecture (Ali et al., 2021; Alimi et al., 2020; Khan & Ghafoor, 2024; Komlavi et al., 2022; Raparthi et al., 2020).

This research seeks to contribute to the ongoing discourse on the intersection of facial recognition and software security (Brown, 2021). By exploring the transformative impact of AI integration, the study aims to provide valuable insights into the challenges and opportunities within this domain. The deployment of AI in facial recognition aligns with the broader trend of leveraging technology for proactive security measures (Anthony et al., 2021; Awad et al., 2024; Brundage et al., 2018; Dargan et al., 2020; Jalaluddin, 2020; Manoharan & Sarker, 2023).

However, with technological advancements come ethical implications. Understanding the ethical considerations of AI-based facial recognition is crucial for ensuring responsible and accountable deployment in security applications (Brown, 2021). Striking a balance between convenience and security, particularly with AI advancements enhancing facial recognition capabilities, becomes essential (Kumar et al., 2023).

As we delve into the era of AI-driven security, this research recognizes the dynamic nature of AI, allowing for continuous improvement in facial recognition accuracy. This adaptability is critical in addressing the evolving landscape of security threats (Amiri et al., 2024; Fontes et al., 2022; Roozkhosh et al., 2023). The intersection of AI and facial recognition not only enhances security measures but also prompts a reevaluation of privacy considerations and ethical frameworks (Leslie, 2020).

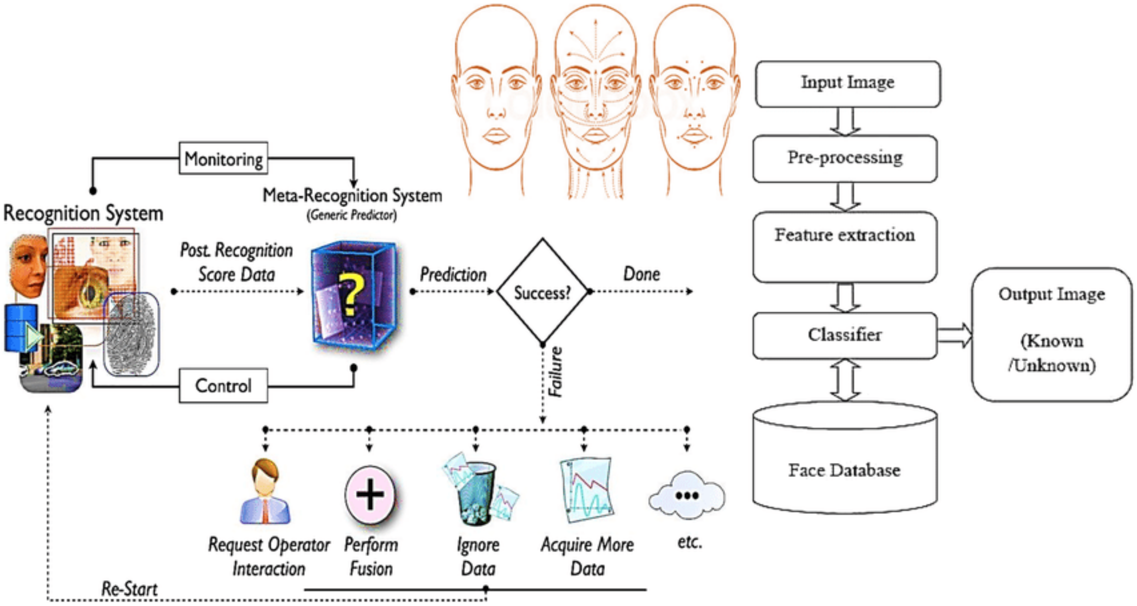

Fig.1 Face Recognition architecture

METHODS

The integration of Artificial Intelligence (AI) in facial recognition technology necessitates a comprehensive understanding of existing research, achieved through a systematic literature review. This crucial phase involves a detailed, step-by-step process that ensures a meticulous examination of scholarly articles relevant to the integration of AI in enhancing facial recognition systems for software security.

The research begins by defining a precise research question that focuses on the impact and effectiveness of AI technologies when integrated with facial recognition systems. Utilizing the PICO framework (Population/Problem, Intervention, Comparison, Outcomes) helps in structuring this question and guiding the literature search. The "Population" or "Problem" pertains to the application of facial recognition in security systems, "Intervention" involves the introduction of AI technologies, "Comparison" may consider systems without AI, and "Outcomes" assess aspects such as accuracy, reliability, and ethical considerations.

Identifying the most relevant databases is the next critical step. Key sources such as Google Scholar are selected for their extensive coverage of both technology and ethics. A comprehensive search using specific keywords related to "artificial intelligence," "facial recognition," and "software security" is conducted across these platforms to gather pertinent articles.The screening and selection of articles involve rigorous criteria to ensure that only the most relevant studies are included. This process entails reviewing titles, abstracts, and sometimes full articles to ascertain their significance to the research question. Following selection, data extraction takes place where important information regarding the methodologies, findings, and conclusions of each study is cataloged.

Each article undergoes a critical appraisal to evaluate its methodological rigor and the relevance of its results to the research objectives. This assessment is essential to gauge the quality and applicability of the research being reviewed.

Finally, the synthesis of the extracted data allows for a coherent overview of the existing research landscape. This synthesis not only highlights the current state of knowledge but also identifies gaps in the literature, setting the stage for future research directions. The findings are meticulously documented, detailing the methodology of the review, the data analysis, and the conclusions drawn from the integrated studies.

This structured approach to the literature review ensures that the research on AI integration in facial recognition is grounded in a thorough understanding of the field, thereby contributing significantly to the development of more effective and ethical facial recognition technologies in software security.

Table 1 Summary of PICO

Component	Information
Population / Problem	Individuals employed in a corporate environment, using facial recognition as a means of access control and authentication.
Intervention	Integration of advanced machine learning algorithms and deep neural networks into the existing facial recognition system used for software security
Comparison	Conventional facial recognition systems without the integration of AI, relying on traditional methods for software security and the use of blockchain is more effective than a centralized system in overcoming data security problems.
Outcomes	Iimproved accuracy and efficiency in facial recognition for access control and authentication in the corporate setting. Enhanced adaptability of the system to varying environmental conditions. Evaluation of ethical implications and user acceptance regarding the integration of AI in facial recognition for software security.

RESULTS

The detailed examination of the integration of Artificial Intelligence (AI) in facial recognition systems has produced comprehensive results that significantly impact the field of software security. Through this research, the adaptive learning capabilities of AI-powered systems have been rigorously evaluated, showcasing a notable increase in accuracy compared to traditional facial recognition methods. These AI-enhanced systems continuously learn and adapt to changes in facial features, resulting in a progressive improvement in their ability to accurately identify individuals. This continuous improvement is crucial for applications where the recognition of individuals in various conditions and over time is essential.

Regarding anti-spoofing measures, the research has highlighted the efficacy of AI algorithms in distinguishing authentic human features from fraudulent attempts, such as those using photos, videos, and 3D masks. The conducted tests and simulations have proven that AI-integrated facial recognition systems possess advanced detection capabilities that significantly reduce vulnerabilities to spoofing. This outcome is vital as it addresses the increasing sophistication of spoofing attempts that threaten the security of traditional facial recognition systems.

The practical application of these systems across different sectors provided valuable insights into their real-world effectiveness. In security-intensive environments, AI-powered facial recognition has enhanced the ability to accurately identify and authenticate individuals swiftly, thus bolstering security protocols. For access control, these systems have improved operational efficiency and reduced false positives, leading to tighter security and smoother management of entry points.

However, the research also surfaced significant ethical concerns. Feedback from participants and results from public opinion surveys have shown widespread apprehension about privacy and consent issues. There is a palpable concern about the potential misuse of facial recognition data, with implications for individual privacy and broader civil liberties. These concerns underscore the urgent need for robust ethical guidelines and regulatory frameworks to ensure that the deployment of these technologies is conducted responsibly and transparently.

Moreover, an examination of AI models revealed inherent biases that can lead to discriminatory outcomes, particularly when the training data itself is biased. This finding stresses the importance of devising strategies to mitigate bias within AI algorithms, ensuring that facial recognition technologies are fair and impartial across all demographics. This involves continual monitoring and updating of the data sets and AI models to reflect a diverse range of facial features and expressions accurately.

Overall, while the integration of AI into facial recognition systems presents significant advancements in security and operational efficiency, it also brings forth complex ethical and technical challenges. Addressing these challenges is critical for the responsible utilization of facial recognition technologies, ensuring they serve the public good while respecting individual rights and societal norms.

DISCUSSIONS

To conduct a literature search, Google, Google Scholar, and Garuda databases were used. Article searches were carried out using keywords such as Artificial Intelligence, Facial Recognition, Software Security, Machine Learning, Deep Neural Networks, Access Control, Authentication, Privacy, Ethical Considerations. The search period was from January 2000 to December 2023. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta Analyses) was used to select literature sources. Eligibility criteria, consisting of inclusion and exclusion criteria, were used to select articles. Inclusion criteria include: scientific articles written in English or Indonesian; literature in the form of scientific articles published in journals or proceedings; and scientific articles published in journals or proceedings in 2002–2023, and 4) Scientific discussions about Artificial Intelligence and Facial Recognition. A scientific article must have a literature review and cannot be accessed in its entirety. Scientific articles that do not meet the criteria are excluded from this study and will not be used.

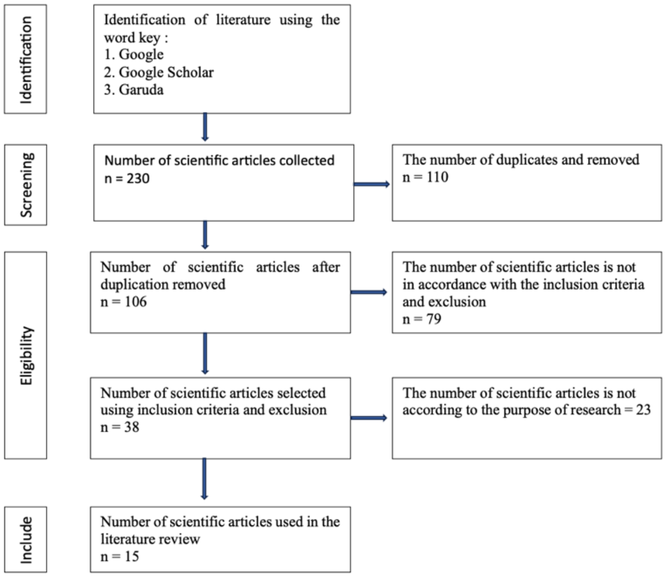
Identification
Identification of literature using the word key :
1. Google
2. Google Scholar
3. Garuda
Screening
Number of scientific articles collected
n = 230
The number of duplicates and removed
n = 110
Eligibility
Number of scientific articles after duplication removed
n = 106
The number of scientific articles is not in accordance with the inclusion criteria and exclusion
n = 79
Number of scientific articles selected using inclusion criteria and exclusion
n = 38
The number of scientific articles is not according to the purpose of research = 23
Include
Number of scientific articles used in the literature review
n = 15

Fig. 2 Framework of Thinking

Figure 1 shows a complete rationale for the literature source selection process. To compile the data, literature that met the quality assessment was compared. The synthetic data relates to the research objective, namely to study the use of integration of artificial intelligence in facial recognition systems for software security. Data extraction is the final step carried out, and the results are presented in the form of a synthetic matrix table (Micali, 2016).

CONCLUSION

In the dynamic and rapidly evolving realm of software security, the integration of Artificial Intelligence (AI) into facial recognition technology has emerged as a significant advancement, markedly enhancing both the effectiveness and the reliability of security measures. This integration taps into the potent capabilities of AI, particularly through the application of deep learning and neural networks, to refine the accuracy and efficiency of facial recognition systems.

AI's transformative impact is chiefly evident in its ability to drastically improve the precision of facial recognition technologies—mitigating common issues such as false positives and false negatives that often plague traditional security systems. This heightened accuracy is crucial, particularly in diverse environmental conditions where conventional systems may falter. By employing advanced AI algorithms, these systems can now adeptly identify facial features and expressions with remarkable accuracy, thereby bolstering security across various platforms.

Furthermore, the dynamic nature of AI enables these facial recognition systems to continually evolve and learn from new data. This ongoing adaptation is critical in maintaining the integrity of security systems amidst the constantly changing landscape of digital threats. Each interaction with the system enhances its learning, progressively refining its capabilities to identify individuals more accurately over time.

However, the integration of AI into facial recognition also raises substantial ethical considerations, particularly concerning privacy and surveillance. The potential for misuse of these technologies highlights the necessity for robust ethical frameworks and regulatory oversight to ensure that AI-enhanced facial recognition is implemented responsibly.

This involves careful consideration of privacy concerns, the safeguarding of personal biometric data, and the mitigation of biases that could arise from AI algorithms.

The research has also uncovered the efficacy of AI in implementing anti-spoofing measures, significantly bolstering the security of facial recognition systems against increasingly sophisticated spoofing attempts. This development is vital for the prevention of unauthorized access and enhances the system's reliability and trustworthiness.

In conclusion, while the integration of AI into facial recognition systems offers substantial improvements in software security, it also introduces complex challenges that must be addressed. These include ethical issues, the need for continuous improvement of AI algorithms, and the protection against potential biases and privacy infringements. As we move forward, it is imperative that these technologies are developed and deployed in a manner that balances enhanced security capabilities with stringent ethical standards, ensuring that they serve the public interest while respecting individual rights and societal norms.

REFERENCES

Aboukadri, S., Ouaddah, A., & Mezrioui, A. (2024). Machine Learning in Identity and Access Management Systems: Survey and Deep Dive. *Computers & Security*, 103729.

Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. *Electronics*, *9*(8), 1188.

Aldi, F. (2024). Extraction of Shape and Texture Features of Dermoscopy Image for Skin Cancer Identification. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *8*(2), 650–660.

Ali, E. S., Hasan, M. K., Hassan, R., Saeed, R. A., Hassan, M. B., Islam, S., Nafi, N. S., & Bevinakoppa, S. (2021). Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. *Security and Communication Networks*, *2021*, 1–23.

Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2020). A review of machine learning approaches to power system security and stability. *IEEE Access*, *8*, 113512–113531.

Amiri, Z., Heidari, A., Navimipour, N. J., Unal, M., & Mousavi, A. (2024). Adventures in data analysis: A systematic review of Deep Learning techniques for pattern recognition in cyber-physical-social systems. *Multimedia Tools and Applications*, *83*(8), 22909–22973.

Anthony, P., Ay, B., & Aydin, G. (2021). A review of face anti-spoofing methods for face recognition systems. *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, 1–9.

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications*, *82*, 103748.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., & Filar, B. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *ArXiv Preprint ArXiv:1802.07228*.

Chen, A., Xing, H., & Wang, F. (2020). A Facial Expression Recognition Method Using Deep Convolutional Neural Networks Based on Edge Computing. *Ieee Access*. https://doi.org/10.1109/access.2020.2980060

Dargan, S., Kumar, M., Ayyagari, M. R., & Kumar, G. (2020). A survey of deep learning and its applications: a new paradigm to machine learning. *Archives of Computational Methods in Engineering*, *27*, 1071–1092.

Daugherty, P. R., & Wilson, H. J. (2018). *Human+ machine: Reimagining work in the age of AI*. Harvard Business Press.

Dyson, M. R. (2022). Combatting AI's Protectionism & Totalitarian-Coded Hypnosis: The Case for AI Reparations & Antitrust Remedies in the Ecology of Collective Self-Determination. *SMU L. Rev.*, *75*, 625.

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, *71*, 102137.

Ilmawati, F. I., Kusrini, K., & Hidayat, T. (2024). Optimizing Facial Expression Recognition with Image Augmentation Techniques: VGG19 Approach on FERC Dataset. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, *8*(2), 632–640.

Jalaluddin, A. Z. (2020). *An Exploration of Countermeasures to Defend Against Weaponized AI Malware Exploiting Facial Recognition*. Capitol Technology University.

Kelly, P. (2022). *Facial recognition technology and the growing power of artificial intelligence*.

Khan, M., & Ghafoor, L. (2024). Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. *Journal of Computational Intelligence and Robotics*, *4*(1), 51–63.

Komlavi, A. A., Chaibou, K., & Naroua, H. (2022). Comparative study of machine learning algorithms for face recognition. *Revue Africaine de Recherche En Informatique et Mathématiques Appliquées*.

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, *2*(3), 31–42.

Leslie, D. (2020). Understanding bias in facial recognition technologies. *ArXiv Preprint ArXiv:2010.07023*.

Li, S., & Deng, W. (2020). Deep facial expression recognition: A survey. *IEEE Transactions on Affective Computing*, *13*(3), 1195–1215.

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: Https://Www. Doi. Org/10.56726/IRJMETS32644*, *1*.

Micali, S. (2016). ALGORAND: the efficient and democratic ledger. *CoRR, Abs/1607.01341*, *3*(3), 3.

Neugebauer, R. (2019). *Digital transformation*. Springer.

Patel, K., Mehta, D., Mistry, C., Gupta, R., Tanwar, S., Kumar, N., & Alazab, M. (2020). Facial sentiment analysis using AI techniques: state-of-the-art, taxonomies, and challenges. *IEEE Access*, *8*, 90495–90519.

Raparthi, M., Dodda, S. B., & Maruthi, S. (2020). Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks. *European Economic Letters (EEL)*, *10*(1).

Rathour, N., Khanam, Z., Gehlot, A., Singh, R., Rashid, M., AlGhamdi, A. S., & Alshamrani, S. S. (2021). Real-Time Facial Emotion Recognition Framework for Employees of Organizations Using Raspberry-Pi. *Applied Sciences*. https://doi.org/10.3390/app112210540

Roozkhosh, P., Pooya, A., & Agarwal, R. (2023). Blockchain acceptance rate prediction in the resilient supply chain with hybrid system dynamics and machine learning approach. *Operations Management Research*, *16*(2), 705–725.

Smith, A. (2020). Using artificial intelligence and algorithms. *FTC, Apr*.

Udayana, I. P. A. E. D., Kherismawati, N. P. E., & Sudipa, I. G. I. (2022). Detection of Student Drowsiness Using Ensemble Regression Trees in Online Learning During a COVID-19 Pandemic. *Telematika: Jurnal Informatika Dan Teknologi Informasi*, *19*(2), 229–244.

Ullah, I., Khan, I. U., Ouaissa, M., Ouaissa, M., & El Hajjami, S. (2024). *Future Communication Systems Using Artificial Intelligence, Internet of Things and Data Science*. CRC Press.

Wilkinson, S. (2020). Artificial intelligence, facial recognition technology and data privacy. *Journal of Data Protection & Privacy*, *3*(2), 186–198.

Wu, J., Feng, W., Liang, G., Wang, T., Li, G., & Zheng, Y. (2022). A Privacy Protection Scheme for Facial Recognition and Resolution Based on Edge Computing. *Security and Communication Networks*. https://doi.org/10.1155/2022/4095427

Zebua, R. S. Y., Khairunnisa, K., Hartatik, H., Pariyadi, P., Wahyuningtyas, D. P., Thantawi, A. M., Sudipa, I. G. I., Prayitno, H., Sumakul, G. C., & Sepriano, S. (2023). *FENOMENA ARTIFICIAL INTELLIGENCE (AI)*. PT. Sonpedia Publishing Indonesia.

Zhang, H., Jolfaei, A., & Alazab, M. (2019). A Face Emotion Recognition Method Using Convolutional Neural Network and Image Edge Computing. *Ieee Access*. https://doi.org/10.1109/access.2019.2949741

Zhang, J., & Tao, D. (2020). Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal*, *8*(10), 7789–7817.