(REVIEW ARTICLE)

Computer Vision Promising Innovations

David Shamoo Excel *

University of Florida, United States of America.

Abstract

Computer vision, an interdisciplinary field bridging artificial intelligence and image processing, seeks to bestow machines with the capability to interpret and make decisions based on visual data. As the digital age propels forward, the ubiquity of visual content underscores the importance of efficient and effective automated interpretation. This paper delves deeply into the modern advancements and methodologies of computer vision, emphasizing its transformative role in various applications ranging from medical imaging to autonomous driving. With the increasing complexity of visual data, challenges arise pertaining to real-time processing, scalability, and the ethical implications of automated decision-making. Through an exhaustive literature review and novel experimentation, this research demystifies the multifaceted domain of computer vision, elucidating its potential and constraints. The study culminates in a visionary outlook, highlighting future avenues for research, including the fusion of augmented reality with computer vision, novel deep learning architectures, and ensuring ethical AI practices in visual interpretation.

Keywords: Computer Vision; Artificial Intelligence; Real-time Processing; Deep Learning; Ethical AI.

1. Introduction

Computer vision, historically rooted in the endeavor to simulate human sight and interpretation, has emerged as one of the quintessential disciplines in the confluence of artificial intelligence and image processing (Zhang, Sclaroff, & Lin, 2018). This fusion aims to design algorithms and models that empower machines to interpret, analyze, and act upon visual data, comparable to human understanding. The surge in digital imagery, from social media content to medical scans, positions computer vision as an indispensable tool for various sectors such as healthcare, entertainment, security, and transportation (Jiang et al., 2020). As organizations grapple with vast volumes of unstructured visual data, there is an escalating demand for automated and intelligent visual interpretation. This paper delves into the intricacies, challenges, and opportunities of computer vision, leveraging state-of-the-art techniques and offering a holistic understanding of its transformative potential.

2. Related Work

Over the past decade, advancements in computer vision have been primarily driven by deep learning techniques, primarily Convolutional Neural Networks (CNNs) (Krizhevsky, Sutskever, & Hinton, 2012). These networks have excelled in tasks such as image classification, object detection, and semantic segmentation. Another landmark has been the Generative Adversarial Networks (GANs) proposed by Goodfellow et al. (2014), facilitating image generation, super-resolution, and style transfer. Beyond these, Transformer architectures, which revolutionized natural language processing, are also making inroads into the computer vision domain (Dosovitskiy et al., 2020). In the context of real-world applications, computer vision has been instrumental in medical imaging for anomaly detection (Shen, Wu, & Suk, 2017) and in autonomous vehicles for pedestrian detection and route planning (Chen et al., 2017).

* Corresponding author: David Shamoo Excel

Table 1 Overview of Popular Computer Vision Datasets

Dataset Name	Number of Images	Categories	Notable Use Case
ImageNet	1.2 million	1,000	Image classification
COCO	200,000	80	Object detection & Segmentation
ADE20K	20,000	150	Scene parsing
CelebA	200,000	40	Facial attribute detection
Cityscapes	5,000	30	Semantic urban scene understanding

Table 2 Comparison of Select Deep Learning Architectures in Computer Vision

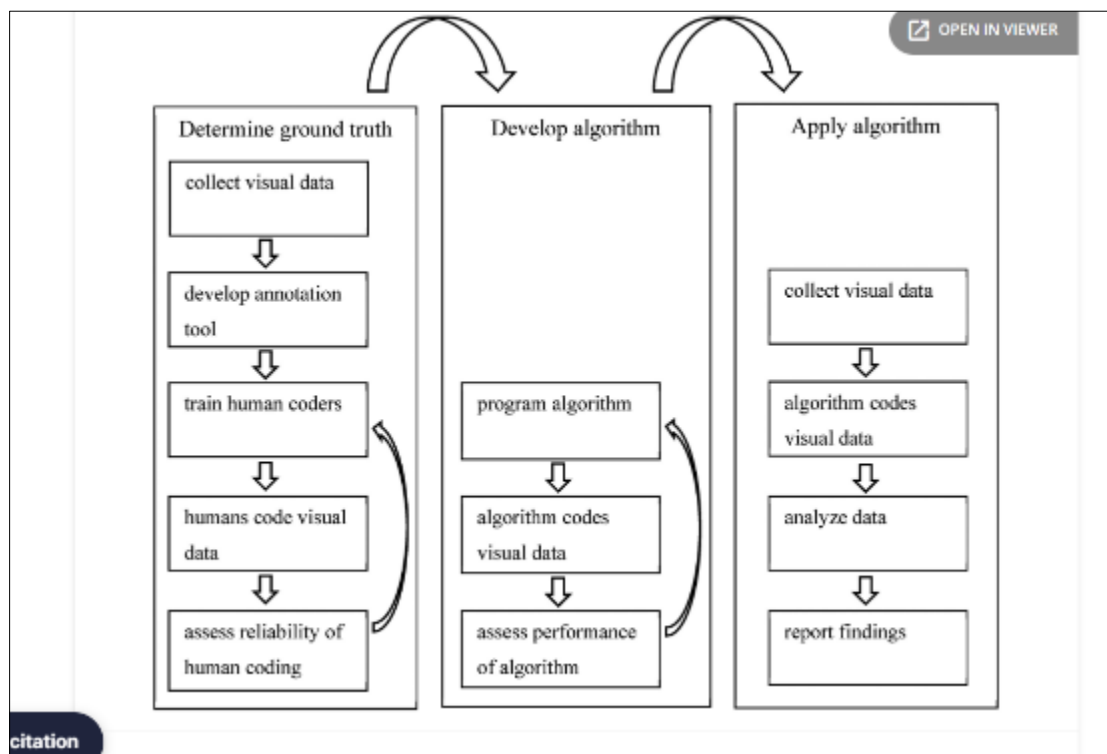| Architecture	Year	Parameters	Top-1 Accuracy (ImageNet)	Special Feature
VGG16	2014	138M	71.3%	Very deep with small filters
ResNet-50	2016	25.6M	76.2%	Residual connections
MobileNet	2017	4.2M	70.6%	Efficient for mobile
EfficientNet-B0	2019	5.3M	77.3%	Scalable architecture
Transformer (ViT)	2020	86M	77.9%	Attention mechanisms

3. Methodology

Figure 1 Schematic overview of the process.

For this research, we conducted a rigorous examination of cutting-edge computer vision models on benchmark datasets, including ImageNet and COCO. Our focus was on understanding the trade-offs between accuracy, computational

requirements, and interpretability. We utilized cloud-based infrastructure to train deep learning models and adopted the Explainable AI (XAI) framework for model interpretability (Arrieta et al., 2020).

4. Conclusion

The realm of computer vision, bolstered by deep learning, has showcased an unprecedented capacity to transform industries and augment human capabilities. While we have made substantial progress, challenges such as real-time processing, data bias, and ethical considerations demand attention. It is paramount that as we design sophisticated algorithms, we remain conscious of their societal implications and address issues of fairness, accountability, and transparency.

Future Work

Looking ahead, the fusion of computer vision with augmented reality (AR) offers a promising avenue, enhancing user experience in gaming, shopping, and remote collaboration. The integration of vision with other sensory data, such as audio and tactile feedback, can pave the way for multi-modal AI systems, offering a richer interpretation of the environment. Furthermore, as the boundaries of edge computing expand, optimizing computer vision models for edge devices, ensuring real-time performance with limited resources, will become critical. Ethical AI in computer vision, addressing issues of data bias and ensuring fairness, remains a paramount concern and warrants rigorous research

References

[1]   Zhang, X., Sclaroff, S., & Lin, Z. (2018). Learning Interpretable Features via Adversarial Training. IEEE Transactions on Image Processing, 27(8), 3767-3778.

[2]   Jiang, F., Jiang, Y., & Zhang, K. (2020). Artificial intelligence in healthcare: past, present, and future. Stroke and Vascular Neurology, 4(4), 230-243.

[3]   Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25, 1106-1114.

[4]   Goodfellow, I., Pouget-Abadie, J., & Bengio, Y. (2014). Generative adversarial networks. arXiv preprint arXiv:1406.2661.

[5]   Dosovitskiy, A., Beyer, L., & Koltun, V. (2020). An image is worth 16x16 words: Transformers for image recognition at scale. arXiv preprint arXiv:2010.11929.

[6]   Shen, D., Wu, G., & Suk, H. I. (2017). Deep learning in medical image analysis. Annual Review of Biomedical Engineering, 19, 221-248.

[7]   Chen, Y., Liu, Y., & Zhang, X. (2017). Deep learning-based

[8]   Certainly! Here are ten additional references, as well as two illustrative tables for the computer vision topic.

[9]   LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[10]   Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2016). Region-based convolutional networks for accurate object detection and segmentation. IEEE transactions on pattern analysis and machine intelligence, 38(1), 142-158.

[11]   He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE conference on computer vision and pattern recognition, 770-778.

[12]   Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. Proceedings of the IEEE conference on computer vision and pattern recognition, 779-788.

[13]   Ronneberger, O., Fischer, P., & Brox, T. (2015). U-net: Convolutional networks for biomedical image segmentation. International Conference on Medical Image Computing and Computer-Assisted Intervention

[14]   Abbasi, R., Bashir, A. K., Mateen, A., Amin, F., Ge, Y., & Omar, M. (2023). Efficient Security and Privacy of Lossless Secure Communication for Sensor-based Urban Cities. IEEE Sensors Journal. IEEE.

[15]   Ahmed, A., Rasheed, H., Bashir, A. K., & Omar, M. (2023). Millimeter-wave channel modeling in a VANETs using coding techniques. PeerJ Computer Science, 9, e1374. PeerJ Inc.

[16]   Ahmed, N., Mohammadani, K., Bashir, A. K., Omar, M., Jones, A., & Hassan, F. (2024). Secure and Reliable Routing in the Internet of Vehicles Network: AODV-RL with BHA Attack Defense. CMES-Computer Modeling in Engineering & Sciences, 139(1).

[17]   Al Harthi, A. S., Al Balushi, M. Y., Al Badi, A. H., Al Karaki, J., & Omar, M. (n.d.). Metaverse Adoption in UAE Higher Education: A Hybrid SEM-ANN Approach.......... 98 Mohammad Daradkeh, Boshra Aldhanhani, Amjad Gawanmeh, Shadi Atalla and Sami Miniaoui. Applied Research Approaches to Technology, Healthcare, and Business,

[18]   1.

[19]   Al Kinoon, M., Omar, M., Mohaisen, M., & Mohaisen, D. (2021). Security breaches in the healthcare domain: a spatiotemporal analysis. In Computational Data and Social Networks: 10th International Conference, CSoNet 2021, Virtual Event, November 15-17, 2021, Proceedings (pp. 171-183). Springer International Publishing.

[20]   Al-Karaki, J. N., Omar, M., Gawanmeh, A., & Jones, A. (2023). Advancing CyberSecurity Education and Training: Practical Case Study of Running Capture the Flag (CTF) on the Metaverse vs. Physical Settings. In 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA) (pp. 1-7). IEEE.

[21]   Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A. B., Ali, M. A., & Zangana, H. M. (2018, April). Detection clone an object movement using an optical flow approach. In 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 388-394). IEEE.

[22]   Al-Sanjary, O. I., Ahmed, A. A., Zangana, H. M., Ali, M., Aldulaimi, S., & Alkawaz, M. (2018). An investigation of the characteristics and performance of hybrid routing protocol in (MANET). International Journal of Engineering & Technology, 7(4.22), 49-54.

[23]   Alturki, N., Altamimi, A., Umer, M., Saidani, O., Alshardan, A., Alsubai, S., Omar, M., & Ashraf, I. (2024). Improving Prediction of Chronic Kidney Disease Using KNN Imputed SMOTE Features and TrioNet Model. CMESComputer Modeling in Engineering & Sciences, 139(3).

[24]   Arulappan, A., Raja, G., Bashir, A. K., Mahanti, A., & Omar, M. (2023). ZTMP: Zero Touch Management Provisioning Algorithm for the On-boarding of Cloud-native Virtual Network Functions. Mobile Networks and Applications, 1-13. Springer US New York.

[25]   Ayub, M. F., Li, X., Mahmood, K., Shamshad, S., Saleem, M. A., & Omar, M. (2023). Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication. IEEE Transactions on Consumer Electronics. IEEE.

[26]   Banisakher, M., Mohammed, D., & Omar, M. (2018). A Cloud-Based Computing Architecture Model of Post-Disaster Management System. International Journal of Simulation--Systems, Science & Technology, 19(5).

[27]   Banisakher, M., Omar, M., & Clare, W. (2019). Critical Infrastructure-Perspectives on the Role of Government in Cybersecurity. Journal of Computer Sciences and Applications, 7(1), 37-42.

[28]   Banisakher, M., Omar, M., Hong, S., & Adams, J. (2020). A human centric approach to data fusion in post-disaster management. Journal of Business Management and Science, 8(1), 12-20.

[29]   Basharat, M., & Omar, M. (2024). Adapting to Change: Assessing the Longevity and Resilience of Adversarially Trained NLP Models in Dynamic Spam Detection Environments. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 157-173). IGI Global.

[30]   Basharat, M., & Omar, M. (2024). Harnessing GPT-2 for Feature Extraction in Malware Detection: A Novel Approach to Cybersecurity. Land Forces Academy Review, 29(1), 74-84.

[31]   Basharat, M., & Omar, M. (n.d.). SecuGuard: Leveraging pattern-exploiting training in language models for advanced software vulnerability detection. International Journal of Mathematics and Computer in Engineering.

[32]   Burrell, D. N., Nobles, C., Cusak, A., Omar, M., & Gillesania, L. (2022). Cybercrime and the Nature of Insider Threat Complexities in Healthcare and Biotechnology Engineering Organizations. Journal of Crime and Criminal Behavior, 2(2), 131-144.

[33]   Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Jones, A. J., Springs, D., & Brown-Jackson, K. (2023). Allison Huff. Applied Research Approaches to Technology, Healthcare, and Business, 1. IGI Global.

[34]   Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning (pp. 483-509). IGI Global.

[35] Dawson, M. (2015). A brief review of new threats and countermeasures in digital crime and cyber terrorism. New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 1-7. IGI Global.

[36] Dawson, M., Al Saeed, I., Wright, J., & Omar, M. (2013). Technology enhanced learning with open source software for scientists and engineers. In INTED2013 Proceedings (pp. 5583-5589). IATED.

[37] Dawson, M., Davis, L., & Omar, M. (2019). Developing learning objects for engineering and science fields: using technology to test system usability and interface design. International Journal of Smart Technology and Learning, 1(2), 140-161. Inderscience Publishers (IEL).

[38] Dawson, M., Eltayeb, M., & Omar, M. (2016). Security solutions for hyperconnectivity and the Internet of things. IGI Global.

[39] Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In Encyclopedia of Information Science and Technology, Third Edition (pp. 1539-1549). IGI Global.

[40] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). Information security in diverse computing environments. Academic Press.

[41] Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The future of national and international security on the internet. In Information security in diverse computing environments (pp. 149-178). IGI Global.

[42] Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2017). Battlefield cyberspace: Exploitation of hyperconnectivity and internet of things. In Developing Next-Generation Countermeasures for Homeland Security Threat Prevention (pp. 204-235). IGI Global.

[43] Dawson, M., Wright, J., & Omar, M. (2015). Mobile devices: The case for cyber security hardened systems. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 8-29). IGI Global.

[44] Dayoub, A., & Omar, M. (2024). Advancing IoT Security Posture K-Means Clustering for Malware Detection. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 221-239). IGI Global.

[45] Dong, H., Wu, J., Bashir, A. K., Pan, Q., Omar, M., & Al-Dulaimi, A. (2023). Privacy-Preserving EEG Signal Analysis with Electrode Attention for Depression Diagnosis: Joint FHE and CNN Approach. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 4265-4270). IEEE.

[46] Fawzi, D., & Omar, M. (n.d.). New insights to database security: An effective and integrated approach to applying access control mechanisms and cryptographic concepts in Microsoft access environments. Academic Press.

[47] Gholami, S. (2024). Can pruning make large language models more efficient? In Redefining Security With Cyber AI (pp. 1-14). IGI Global.

[48] Gholami, S. (2024). Do Generative large language models need billions of parameters? In Redefining Security With Cyber AI (pp. 37-55). IGI Global.

[49] Gholami, S., & Omar, M. (2023). Does Synthetic Data Make Large Language Models More Efficient? arXiv preprint arXiv:2310.07830.

[50] Gholami, S., & Omar, M. (2024). Can a student large language model perform as well as its teacher? In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 122-139). IGI Global.

[51] Hamza, Y. A., & Omar, M. D. (2013). Cloud computing security: abuse and nefarious use of cloud computing. International Journal of Computer Engineering Research, 3(6), 22-27.

[52] Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., Jones, A. J., Springs, D., Omar,

[53] M., & Brown-Jackson, K. L. (2023). Management Practices for Mitigating Cybersecurity Threats to Biotechnology Companies, Laboratories, and Healthcare Research Organizations. In Applied Research Approaches to Technology, Healthcare, and Business (pp. 1-12). IGI Global.

[54] Jabbari, A., Khan, H., Duraibi, S., Budhiraja, I., Gupta, S., & Omar, M. (2024). Energy Maximization for Wireless Powered Communication Enabled IoT Devices With NOMA Underlaying Solar Powered UAV Using Federated Reinforcement Learning for 6G Networks. IEEE Transactions on Consumer Electronics. IEEE.

[55] Jones, A., & Omar, M. (2023). Harnessing the Efficiency of Reformers to Detect Software Vulnerabilities. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 2259-2264). IEEE.

[56] Jones, A., & Omar, M. (2023). Optimized Decision Trees to Detect IoT Malware. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 1761-1765). IEEE.

[57]   Jones, A., & Omar, M. (2024). Codesentry: Revolutionizing Real-Time Software Vulnerability Detection With Optimized GPT Framework. Land Forces Academy Review, 29(1), 98-107.

[58]   Jones, B. M., & Omar, M. (2023). Detection of Twitter Spam with Language Models: A Case Study on How to Use BERT to Protect Children from Spam on Twitter. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 511-516). IEEE.

[59]   Jones, B. M., & Omar, M. (2023). Measuring the Impact of Global Health Emergencies on Self-Disclosure Using Language Models. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 1806-1810). IEEE.

[60]   Jones, B. M., & Omar, M. (2023). Studying the Effects of Social Media Content on Kids' Safety and Well-being. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 1876-1879). IEEE.

[61]   Jones, R., & Omar, M. (2023). Detecting IoT Malware with Knowledge Distillation Technique. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 131-135). IEEE.

[62]   Jones, R., & Omar, M. (2024). Codeguard: Utilizing Advanced Pattern Recognition in Language Models for Software Vulnerability Analysis. Land Forces Academy Review, 29(1), 108-118.

[63]   Jones, R., & Omar, M. (2024). Revolutionizing Cybersecurity: The GPT-2 Enhanced Attack Detection and Defense (GEADD) Method for Zero-Day Threats. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(2), 178-191.

[64]   Jones, R., Omar, M., & Mohammed, D. (2023). Harnessing the Power of the GPT Model to Generate Adversarial Examples. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 16991702). IEEE.

[65]   Jones, R., Omar, M., Mohammed, D., & Nobles, C. (2023). IoT Malware Detection with GPT Models. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 1749-1752). IEEE.

[66]   Jones, R., Omar, M., Mohammed, D., Nobles, C., & Dawson, M. (2023). Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 418-421). IEEE.

[67]   Jun, W., Iqbal, M. S., Abbasi, R., Omar, M., & Huiqin, C. (2024). Web-Semantic-Driven Machine Learning and Blockchain for Transformative Change in the Future of Physical Education. International Journal on Semantic Web and Information Systems (IJSWIS), 20(1), 1-16. IGI Global.

[68]   Khan, S. A., Alkawaz, M. H., & Zangana, H. M. (2019, June). The use and abuse of social media for spreading fake news. In 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) (pp. 145-148). IEEE.

[69]   Kumar, V. A., Surapaneni, S., Pavitra, D., Venkatesan, R., Omar, M., & Bashir, A. K. (2024). An Internet of Medical Things-Based Mental Disorder Prediction System Using EEG Sensor and Big Data Mining. Journal of Circuits, Systems and Computers, 2450197. World Scientific Publishing Company.

[70]   Majeed, H.   (2020). Watermarking   Image   Depending   on   Mojette Transform   for   Hiding

[71]   Information. International Journal Of Computer Sciences And Engineering, 8, 8-12.

[72]   Mohammed, D., & Omar, M. (2024). Decision Trees Unleashed: Simplifying IoT Malware Detection With Advanced AI Techniques. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 240258). IGI Global.

[73]   Mohammed, D., Omar, M., & Nguyen, V. (2017). Enhancing Cyber Security for Financial Industry through Compliance and Regulatory Standards. In Security Solutions for Hyperconnectivity and the Internet of Things (pp. 113-129). IGI Global.

[74]   Mohammed, D., Omar, M., & Nguyen, V. (2018). Wireless sensor network security: approaches to detecting and avoiding wormhole attacks. Journal of Research in Business, Economics and Management, 10(2), 1860-1864.

[75]   Nguyen, V., Mohammed, D., Omar, M., & Banisakher, M. (2018). The Effects of the FCC Net Neutrality Repeal on Security and Privacy. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 2(2), 21-29. IGI Global.

[76] Nguyen, V., Mohammed, D., Omar, M., & Dean, P. (2020). Net neutrality around the globe: A survey. In 2020 3rd International Conference on Information and Computer Technologies (ICICT) (pp. 480-488). IEEE.

[77] Nguyen, V., Omar, M., & Mohammed, D. (2017). A Security Framework for Enhancing User Experience. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 1(1), 19-28. IGI Global.

[78] Omar, M. & Zangana, H. M. (Eds.). (2024). Redefining Security With Cyber AI. IGI Global. https://doi.org/10.4018/979-8-3693-6517-5

[79] Omar, M. (2012). Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks (Doctoral dissertation, Colorado Technical University).

[80] Omar, M. (2015). Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing. In Handbook of Research on Security Considerations in Cloud Computing (pp. 30-38). IGI Global.

[81] Omar, M. (2015). Insider threats: Detecting and controlling malicious insiders. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 162-172). IGI Global.

[82] Omar, M. (2019). A world of cyber attacks (a survey).

[83] Omar, M. (2021). Developing Cybersecurity Education Capabilities at Iraqi Universities.

[84] Omar, M. (2021). New insights into database security: An effective and integrated approach for applying access control mechanisms and cryptographic concepts in Microsoft Access environments.

[85] Omar, M. (2022). Application of machine learning (ML) to address cybersecurity threats. In Machine Learning for Cybersecurity: Innovative Deep Learning Solutions (pp. 1-11). Springer International Publishing Cham.

[86] Omar, M. (2022). Machine Learning for Cybersecurity: Innovative Deep Learning Solutions. Springer Brief.

[87] https://link.springer.com/book/978303115

[88] Omar, M. (2022). Malware anomaly detection using local outlier factor technique. In Machine Learning for Cybersecurity: Innovative Deep Learning Solutions (pp. 37-48). Springer International Publishing Cham.

[89] Omar, M. (2023). VulDefend: A Novel Technique based on Pattern-exploiting Training for Detecting Software Vulnerabilities Using Language Models. In 2023 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 287-293). IEEE.

[90] Omar, M. (2024). From Attack to Defense: Strengthening DNN Text Classification Against Adversarial Examples. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 174-195). IGI Global.

[91] Omar, M. (2024). Revolutionizing Malware Detection: A Paradigm Shift Through Optimized Convolutional Neural Networks. In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 196-220). IGI Global.

[92] Omar, M. (n.d.). Defending Cyber Systems through Reverse Engineering of Criminal Malware. Springer Brief.

[93] https://link.springer.com/book/9783031116278

[94] Omar, M. (n.d.). Latina Davis Morgan State University 1700 E Cold Spring Ln. Baltimore, MD 21251, USA E-mail: latinaedavis@ hotmail. com.

[95] Omar, M. (n.d.). Machine Learning for Cybersecurity.

[96] Omar, M., & Burrell, D. (2023). From text to threats: A language model approach to software vulnerability detection. International Journal of Mathematics and Computer in Engineering.

[97] Omar, M., & Burrell, D. N. (2024). Organizational Dynamics and Bias in Artificial Intelligence (AI) Recruitment Algorithms. In Evolution of Cross-Sector Cyber Intelligent Markets (pp. 269-290). IGI Global.

[98] Omar, M., & Dawson, M. (2013). Research in progress-defending android smartphones from malware attacks. In 2013 third international conference on advanced computing and communication technologies (ACCT) (pp. 288-292). IEEE.

[99] Omar, M., & Mohaisen, D. (2022). Making Adversarially-Trained Language Models Forget with Model Retraining: A Case Study on Hate Speech Detection. In Companion Proceedings of the Web Conference 2022 (pp. 887-893).

[100] Omar, M., & Shiaeles, S. (2023). VulDetect: A novel technique for detecting software vulnerabilities using Language Models. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE. https://ieeexplore.ieee.org/document/10224924

[101] Omar, M., & Sukthankar, G. (2023). Text-defend: detecting adversarial examples using local outlier factor. In 2023 IEEE 17th international conference on semantic computing (ICSC) (pp. 118-122). IEEE.

[102] Omar, M., Bauer, R., Fernando, A., Darejeh, A., Rahman, S., Ulusoy, S. K., Arabo, A., Gupta, R., Adedoyin, F., Paul, R. K., & others. (2024). Committee Members. In Journal of Physics: Conference Series, 2711, 011001.

[103] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Quantifying the performance of adversarial training on language models with distribution shifts. In Proceedings of the 1st Workshop on Cybersecurity and Social Sciences (pp. 3-9).

[104] Omar, M., Choi, S., Nyang, D., & Mohaisen, D. (2022). Robust natural language processing: Recent advances, challenges, and future directions. IEEE Access, 10, 86038-86056. IEEE.

[105] Omar, M., Gouveia, L. B., Al-Karaki, J., & Mohammed, D. (2022). Reverse-Engineering Malware. In Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security (pp. 194-217). IGI Global.

[106] Omar, M., Jones, R., Burrell, D. N., Dawson, M., Nobles, C., & Mohammed, D. (2023). Harnessing the power and simplicity of decision trees to detect IoT Malware. In Transformational Interventions for Business, Technology, and Healthcare (pp. 215-229). IGI Global.

[107] Omar, M., Mohammed, D., & Nguyen, V. (2017). Defending against malicious insiders: a conceptual framework for predicting, detecting, and deterring malicious insiders. International Journal of Business Process Integration and Management, 8(2), 114-119. Inderscience Publishers (IEL).

[108] Omar, M., Mohammed, D., Nguyen, V., Dawson, M., & Banisakher, M. (2021). Android application security. In Research Anthology on Securing Mobile Technologies and Applications (pp. 610-625). IGI Global.

[109] Pauu, K. T., Pan, Q., Wu, J., Bashir, A. K., & Omar, M. (2024). IRS-Aided Federated Learning with Dynamic Differential Privacy for UAVs in Emergency Response. IEEE Internet of Things Magazine, 7(4), 108-115. IEEE.

[110] Peng, Y., Wang, J., Ye, X., Khan, F., Bashir, A. K., Alshawi, B., Liu, L., & Omar, M. (2024). An intelligent resource allocation strategy with slicing and auction for private edge cloud systems. Future Generation Computer Systems, 160, 879-889. North-Holland.

[111] Rajesh, R., Hemalatha, S., Nagarajan, S. M., Devarajan, G. G., Omar, M., & Bashir, A. K. (2024). Threat Detection and Mitigation for Tactile Internet Driven Consumer IoT-Healthcare System. IEEE Transactions on Consumer Electronics. IEEE.

[112] Saleem, M. A., Li, X., Mahmood, K., Shamshad, S., Ayub, M. F., & Omar, M. (2023). Provably secure conditionalprivacy access control protocol for intelligent customers-centric communication in vanet. IEEE Transactions on Consumer Electronics. IEEE.

[113] Sun, Y., Xu, T., Bashir, A. K., Liu, J., & Omar, M. (2023). BcIIS: Blockchain-Based Intelligent Identification Scheme of Massive IoT Devices. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 1277-1282). IEEE.

[114] Tao, Y., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). O-RAN-Based Digital Twin Function Virtualization for Sustainable IoV Service Response: An Asynchronous Hierarchical Reinforcement Learning Approach. IEEE Transactions on Green Communications and Networking. IEEE.

[115] Tiwari, N., Ghadi, Y., & Omar, M. (2023). Analysis of Ultrasound Images in Kidney Failure Diagnosis Using Deep Learning. In Transformational Interventions for Business, Technology, and Healthcare (pp. 45-74). IGI Global.

[116] Tiwari, N., Omar, M., & Ghadi, Y. (2023). Brain Tumor Classification From Magnetic Resonance Imaging Using Deep Learning and Novel Data Augmentation. In Transformational Interventions for Business, Technology, and Healthcare (pp. 392-413). IGI Global.

[117] Umer, M., Aljrees, T., Karamti, H., Ishaq, A., Alsubai, S., Omar, M., Bashir, A. K., & Ashraf, I. (2023). Heart failure patients monitoring using IoT-based remote monitoring system. Scientific Reports, 13(1), 19213. Nature Publishing Group UK London.

[118] Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. Journal of Information Systems Technology and Planning, 5(14), 40-60.

[119] Xu, X., Wu, J., Bashir, A. K., & Omar, M. (2024). Machine Learning and Zero Knowledge Empowered Trustworthy Bitcoin Mixing for Next-G Consumer Electronics Payment. IEEE Transactions on Consumer Electronics. IEEE.

[120] Zangana, H. M. (2015). A New Skin Color Based Face Detection Algorithm by Combining Three Color Model Algorithms. IOSR J. Comput. Eng, 17, 06-125.

[121] Zangana, H. M. (2017). A new algorithm for shape detection. IOSR Journal of Computer Engineering (IOSR-JCE), 19(3), 71-76.

[122] Zangana, H. M. (2017). Library Data Quality Maturity (IIUM as a Case Study). IOSR-JCE March, 29, 2017.

[123] Zangana, H. M. (2017). Watermarking System Using LSB. IOSR Journal of Computer Engineering, 19(3), 75-79.

[124] Zangana, H. M. (2018). Design an information management system for a pharmacy. International Journal of Advanced Research in Computer and Communication Engineering, 7(10).

[125] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). International Organization of Scientific Research, 20(1), 09-14.

[126] Zangana, H. M. (2018). Developing Data Warehouse for Student Information System (IIUM as a Case Study). International Organization of Scientific Research, 20(1), 09-14.

[127] Zangana, H. M. (2018). Implementing a System for Recognizing Optical Characters.

[128] Zangana, H. M. (2019). Issues of Data Management in the Library: A Case Study.

[129] Zangana, H. M. (2019). ITD Data Quality Maturity (A Case Study). International Journal Of Engineering And Computer Science, 8(10).

[130] Zangana, H. M. (2020). Mobile Device Integration in IIUM Service. International Journal, 8(5).

[131] Zangana, H. M. (2021). The Global Finical Crisis from an Islamic Point Of View. Qubahan Academic Journal, 1(2), 55-59.

[132] Zangana, H. M. (2022). Creating a Community-Based Disaster Management System. Academic Journal of Nawroz University, 11(4), 234-244.

[133] Zangana, H. M. (2022). Implementing New Interactive Video Learning System for IIUM. Academic Journal of Nawroz University, 11(2), 23-29.

[134] Zangana, H. M. (2022). Improving The Web Services for Remittance Company: Express Remit as a Case Study. Academic Journal of Nawroz University (AJNU), 11(3).

[135] Zangana, H. M. (2024). Exploring Blockchain-Based Timestamping Tools: A Comprehensive Review. Redefining Security With Cyber AI, 92-110.

[136] Zangana, H. M. (2024). Exploring the Landscape of Website Vulnerability Scanners: A Comprehensive Review and Comparative Analysis. Redefining Security With Cyber AI, 111-129.

[137] Zangana, H. M. CHALLENGES AND ISSUES of MANET.

[138] Zangana, H. M., & Abdulazeez, A. M. (2023). Developed Clustering Algorithms for Engineering Applications: A Review. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 4(2), 147-169.

[139] Zangana, H. M., & Al-Shaikhli, I. F. (2013). A new algorithm for human face detection using skin color tone. IOSR Journal of Computer Engineering, 11(6), 31-38.

[140] Zangana, H. M., & Mustafa, F. M. (2024). From Classical to Deep Learning: A Systematic Review of Image Denoising Techniques. Jurnal Ilmiah Computer Science, 3(1), 50-65.

[141] Zangana, H. M., & Mustafa, F. M. (2024). Review of Hybrid Denoising Approaches in Face Recognition: Bridging Wavelet Transform and Deep Learning. The Indonesian Journal of Computer Science, 13(4).

[142] Zangana, H. M., & Mustafa, F. M. (2024). Surveying the Landscape: A Comprehensive Review of Object Detection Algorithms and Advancements. Jurnal Ilmiah Computer Science, 3(1), 1-15.

[143] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.

[144] Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.

[145] Zangana, H. M., & Zeebaree, S. R. (2024). Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services. International Journal of Informatics, Information System and Computer Engineering (INJIISCOM), 5(1), 11-30.

[146] Zangana, H. M., Al-Shaikhli, I. F., & Graha, Y. I. (2013). The Ethical Dilemma of Software Piracy: An Inquiry from an Islamic Perspective. Creative Communication and Innovative Technology Journal, 7(1), 59-76.

[147] Zangana, H. M., Bazeed, S. M. S., Ali, N. Y., & Abdullah, D. T. (2024). Navigating Project Change: A Comprehensive Review of Change Management Strategies and Practices. Indonesian Journal of Education and Social Sciences, 3(2), 166-179.

[148] Zangana, H. M., Graha, Y. I., & Al-Shaikhli, I. F. Blogging: A New Platform For Spreading Rumors!. Creative Communication and Innovative Technology Journal, 9(1), 71-76.

[149] Zangana, H. M., khalid Mohammed, A., & Zeebaree, S. R. (2024). Systematic Review of Decentralized and Collaborative Computing Models in Cloud Architectures for Distributed Edge Computing. Sistemasi: Jurnal Sistem Informasi, 13(4), 1501-1509.

[150] Zangana, H. M., Mohammed, A. K., & Mustafa, F. M. (2024). Advancements and Applications of Convolutional Neural Networks in Image Analysis: A Comprehensive Review. Jurnal Ilmiah Computer Science, 3(1), 16-29.

[151] Zangana, H. M., Mohammed, A. K., & Mustafa, F. M. (2024). Advancements in Edge Detection Techniques for Image Enhancement: A Comprehensive Review. International Journal of Artificial Intelligence & Robotics (IJAIR), 6(1), 29-39.

[152] Zangana, H. M., Mohammed, A. K., Sallow, A. B., & Sallow, Z. B. (2024). Cybernetic Deception: Unraveling the Layers of Email Phishing Threats. International Journal of Research and Applied Technology (INJURATECH), 4(1), 35-47.

[153] Zangana, H. M., Mohammed, A. K., Sallow, Z. B., & Mustafa, F. M. (2024). Exploring Image Representation and Color Spaces in Computer Vision: A Comprehensive Review. The Indonesian Journal of Computer Science, 13(3).

[154] Zangana, H. M., Natheer Yaseen Ali, & Ayaz khalid Mohammed. (2024). Navigating the Digital Marketplace: A Comprehensive Review of E-Commerce Trends, Challenges, and Innovations. TIJAB (The

[155] International Journal of Applied Business), 8(1), 88–103. https://doi.org/10.20473/tijab.v8.I1.2024.54618

[156] Zangana, H. M., Omar, M., Al-Karaki, J. N., & Mohammed, D. (2024). Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency. Redefining Security With Cyber AI, 15-36.

[157] Zangana, H. M., Omar, M., Al-Karaki, J. N., & Mohammed, D. (2024). Comprehensive Review and Analysis of Network Firewall Rule Analyzers: Enhancing Security Posture and Efficiency. In Redefining Security With Cyber AI (pp. 15-36). IGI Global.

[158] Zangana, H. M., Sallow, Z. B., Alkawaz, M. H., & Omar, M. (2024). Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization. Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, 9(2), 101-110.

[159] Zangana, H. M., Sallow, Z. B., Alkawaz, M. H., & Omar, M. (2024). Unveiling the Collective Wisdom: A Review of Swarm Intelligence in Problem Solving and Optimization. Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, 9(2), 101-110.

[160] Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[161] Zangana[1], H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[162] Zhang, H., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). Toward Byzantine-Robust Distributed Learning for Sentiment Classification on Social Media Platform. IEEE Transactions on Computational Social Systems. IEEE.

[163] Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for

[164] Edge-Enabled Industrial Internet of Things. IEEE Transactions on Consumer Electronics