Journal of Computer Technology and Applied Mathematics
Vol. 1, No. 1, 2024

Machine Learning-Based Facial Recognition for Financial Fraud Prevention

WANG, Yong [1*] ZHAN, Xiaoan [2] ZHAN, Tong [3] XU, Jiahao [4] BAI, Xinzhu [5]

[1] University of Aberdeen, UK
[2] New York University, USA
[3] Columbia University, USA
[4] University of Southern California, USA
[5] Tianjin University of Finance and Economics, China

**** WANG, Yong is the corresponding author, E-mail: fredi4jae@gmail.com***

Abstract: At present, face recognition theory and technology have achieved great success, and are widely used in key fields such as government, finance and military. Similar to other information systems, face recognition systems are also faced with various security problems, of which face spoofing (FS) is one of the most important security problems. The so-called face fraud refers to the attacker using printed photos, video playback and 3D masks and other attack methods to trick the face recognition system to make wrong judgments, so it is a key problem that the face recognition system must solve.This paper explores the application of machine learning face recognition technology in preventing financial fraud, aiming to provide effective fraud prevention solutions for the financial industry. It discusses the principles, methods, and practical cases of applying face recognition technology in various financial scenarios, such as transaction monitoring, identity verification, and payment security. The paper also delves into the challenges posed by face fraud forgery, highlighting the importance of adopting effective deep forgery detection technology. Additionally, it provides insights into machine learning face recognition models, their quantization methods, and the balance between recognition speed and precision. Finally, the paper emphasizes the significance of anti-deception technology in designing secure and reliable face recognition systems, focusing on sensor selection and algorithm optimization to enhance the system's resistance to deception attacks.

Keywords: Financial Fraud Prevention, Machine Learning Face Recognition, Deep Forgery Detection, Anti-deception Technology.

DOI: https://doi.org/10.5281/zenodo.11004115

1 Introduction

In recent years, the means and techniques of financial fraud have been renovated day by day, bringing serious security risks and economic losses to the financial system. Traditional fraud detection methods often face the problems of low detection accuracy and high false positive rate, and it is difficult to meet the needs of increasingly complex fraud forms and the rapid development of financial transactions. The emergence of machine learning face recognition technology has brought new hope for financial fraud prevention. [1] By utilizing machine learning algorithms and big data analysis, face recognition technology can accurately and quickly identify possible abnormal behavior in financial transactions, thereby helping financial institutions to detect and prevent potential fraud in a timely manner.

This paper will deeply discuss the application principles, methods and practical cases of machine learning face recognition technology in financial fraud prevention. We will analyze the specific applications of this technology in financial transaction monitoring, identity verification [2], payment security, etc., and explore its advantages and challenges in improving fraud detection accuracy and reducing risk costs. Through the research and practice of machine learning face recognition technology, we hope to provide an effective fraud prevention program for the financial industry and promote the safe, reliable and innovative development of financial services.

2 Related Word

2.1 Facial recognition technology

As a biometric technology, face recognition technology can automatically identify individual identities, reduce manual participation in the process, and meet the actual needs of customer identification such as the real name system of financial services accounts. At present, face recognition technology has been integrated into financial services, widely used in outlets, mobile banking, unit security and other fields, through face verification, face recognition, customer identification. [3] On the one hand, it replaces manual processing process, simplifies procedures

and improves efficiency; On the other hand, as an effective way of remote and contactless business identification, it has been widely used in smart finance, mobile finance and other scenarios.

1. Face verification to verify personal identity. Face verification is one of the applications of face recognition. Its principle is to compare the generated sample feature sequence with the template feature sequence of the stored user given by the user identification information [4](1:1 comparison) to confirm whether the user is the declared identity. Financial institutions confirm the real identity of business handlers through face verification, and meet regulatory requirements such as real names and real people for business handling.

(1) Counter service. According to the regulatory requirements such as the real-name account system, some bank branch counter services (such as opening personal RMB [5] settlement accounts) need to be checked online to check personal information such as name, ID number and photo. Some banking institutions have applied face recognition technology for automatic verification, reducing manual verification deviation and improving verification efficiency. [6] In addition, large cash withdrawal, account password unlocking and other businesses that need identity verification can also be applied to face recognition technology for face verification to confirm that it is handled by me.

(2) Intelligent service. Intelligent service equipment such as bank automated teller machines have widely applied face recognition technology to automatically identify customers. [7] Take face swipe deposit and withdrawal business as an example, after the customer enters the identity information, the self-service device immediately collects the customer's face information, and after the verification is successful, the corresponding bank card can be selected for deposit and withdrawal operation.

(3) Mobile financial services. Mobile financial clients such as mobile banking have widely used face recognition technology, mainly for the identification of remote operators to ensure that the relevant business operations are actual operations. [8] Such as large transfers, credit applications, equipment binding and other important businesses, in the business process are required to remotely collect and identify the operator's face information to verify the actual identity of the operator, and effectively protect the security of customers' account funds.

(4) System user authentication. Banking institutions in order to ensure the security management of important business systems, on the basis of traditional user names and passwords, increased the operator face recognition verification link to ensure that the actual operator is an effective system user, such as personal credit inquiry, credit management system, etc., to protect the security of all kinds of sensitive data of customers.

2. Face recognition, identification of personal identity. Face recognition, as another application scenario of face recognition, refers to the comparison of the generated sample feature sequence with all the stored template feature sequences within the specified range [9] (1: N comparison) to determine the user identity. Financial institutions mainly collect and identify face information to determine the identity information corresponding to face information to provide a basis for business management.

(1) Face payment. Directly use the face as the payment medium, collect, process and transmit the face data through special equipment, identify the identity of the customer, and then use its designated account to complete the payment. Such as "UnionPay brush face pay", the user through the "cloud flash pay" or mobile banking face verification, set the face payment password, open the face pay function, you can use the face pay in the offline store for payment. In addition, [10] Alipay "Dragonfly" and wechat Pay "frog" are also face payment products.

(2) Wisdom scene. Banking institutions actively expand the application scenarios of face recognition technology through the output of financial technology. For example, Agricultural Bank of China Yangzhou Branch combined with the campus security construction scene, the application of the "home school access" platform to provide smart campus services for schools, and realize the application of students' school gate gate gate temperature detection, face brushing electronic class cards outside the classroom and parental communication.

(3) Security management. Banking institutions have used face recognition technology in security facilities such as internal gate and ladder control, mainly for the identification of unit employees, strengthen internal staff management, and effectively control workplace security risks. [11] For example, some banking institutions have installed face recognition rolling mills in the office space to brush the face to measure temperature and enter the door to achieve daily management of employee attendance.

2.2 Face fraud forgery

The rapid development of deep forgery technology has brought new challenges to face fraud. Scammers can use machine learning to generate fake personas or use manipulated photos and videos to impersonate existing people to commit fraud. The following is the main content of face fraud forgery:

2.2.1 Principle of fraud

At the heart of how fraud occurs is the use of deep forgery techniques by fraudsters to generate fake personas, including photos and videos. These techniques can create highly realistic images and videos of faces, making fake identities appear almost indistinguishable from real ones. As technology continues to advance, these fake images and videos are becoming increasingly difficult to identify. [12-13] Fraudsters use these false identities to fake their real

identities to make fake video calls or image transmissions. They may pose as bank employees, friends, or other trusted figures to trick victims into making money transfers or revealing sensitive personal information. This kind of fraud exploits people's trust in facial recognition and video calls, making it even more confusing and deceptive. In this case, the victim is often unable to identify the false identity and thus vulnerable to fraud. Therefore, it is particularly important to strengthen the supervision and response measures on deep forgery technology, as well as improve the public's security awareness and prevention ability.

2.2.2 Fraud realization method

The main way the fraud is achieved is through deep forgery technology to create fake facial images and videos. This technique has a high degree of fidelity, allowing scammers to create identities that appear real. First, they can use deep faking technology to easily generate realistic facial images and videos that require no professional skills to operate easily. Second, scammers can use [14] pre-recorded videos or processed deep fake videos to show the victim through the phone's camera. The videos may have been pre-recorded or manipulated in real time to simulate a real video call, thereby convincing the victim that a real video call was taking place. In addition, scammers can also obtain real images and videos of others by intercepting data transmitted over the Internet or attacking servers. Once they have real images and videos, they can use deep forgery techniques to modify and forge them to create fake identities that look real. [15] This approach allows scammers to bypass traditional authentication methods, passing them off as the real thing and making it easier to commit fraud. Therefore, strengthening the supervision and preventive measures on deep forgery technology and increasing the security awareness of the public are crucial to preventing this type of fraud.

Therefore, in order to meet the challenges brought by face fraud forgery, an effective deep forgery detection technology must be adopted. These techniques identify deep fakes by analyzing artifacts in images and videos, thereby detecting the difference between real and fake. [16-18]Deep forgery detection techniques usually involve a variety of methods, including image quality analysis, facial feature detection, video stream detection, etc. Among them, image quality analysis can be used to detect abnormal pixels or traces in the image, so as to find the authenticity of the image; Facial feature detection focuses on the recognition of facial features in images to identify false faces. [19] Video stream detection focuses on the continuity and naturalness of video to detect abnormal phenomena in video. In addition, pattern recognition and classification algorithms based on machine learning are also widely used in deep forgery detection to improve the accuracy and efficiency of detection by training and learning a large amount of data. The application of these technologies will play an important role in the security of the financial sector, helping to protect the safety of customers' funds and personal privacy, and improving the overall security and stability of the financial system.

2.3 Machine learning face recognition model

At present, the most advanced face recognition model mainly determines the identity of a face image by the similarity of feature vectors [20]. The neural network for extracting feature vectors is called feature extraction network, which can convert a 3-channel true color face image into a feature vector. After extracting the feature vector of the image to be recognized through this feature, matching it with the feature vector in the face image library can determine the identity of the face image. Generally, L2 distance or cosine similarity is used to match the feature vector, and finally the identity of the image in the image library that is closest to the feature of the image to be recognized is taken as the output identity. The process of recognizing a face image by a face recognition model can be formalized as:

(1)

Where, x is the face image to be recognized, x; Is the face image in the gallery, and F(x) is the feature vector obtained after feature extraction of x by the face recognition model. *,* is the distance between two eigenvectors. The final identification is the one closest to the x feature in the gallery.

The traditional face recognition model quantization mapping method is to convert 32bit floating point numbers into 8bit integers, and the conversion process is divided into three ways:

1) Unsaturated mode: [21] Map the maximum value of positive and negative absolute values of floating point numbers in the model to the maximum and minimum value of integers.

2) Saturation method: First calculate the threshold of floating-point numbers in the model, and then map the positive and negative thresholds of floating-point numbers to the maximum and minimum values of integers.

3) Affine mode: Maps the maximum and minimum values of floating point numbers in the model to the maximum and minimum values of integers.

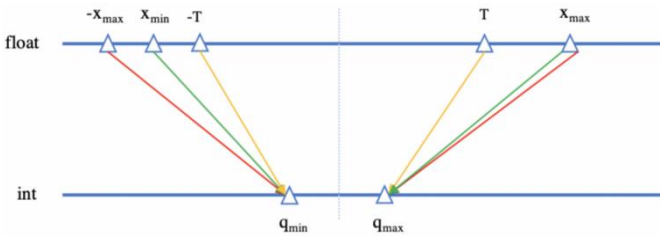

Figure 1 Red represents the unsaturated mode, yellow represents the saturated mode, and green represents the affine mode

When the traditional quantization method is used to

quantify the face recognition model, no matter what kind of mapping method, it will be affected by the outlier points and the uneven distribution of float parameters, resulting in increased recognition accuracy loss after quantization. As shown in Figure 2, the outlier points on the left make the quantization range larger, and the numerical points on the right after quantization become too dense, increasing the quantization loss.

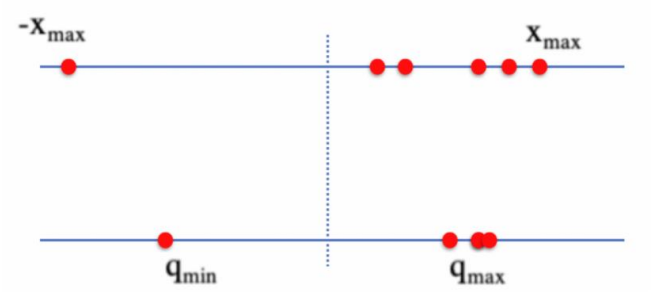

Figure 2 Quantified loss loss chart

In light of enhancing the swiftness and precision of FaceID facial recognition technology on mobile devices, quantization emerges as a pivotal strategy. Simply put, quantization involves substituting the original floating-point data with lower-bit data, effectively compressing the model. The central challenge lies in reducing the bit width of model data while upholding face recognition accuracy. Achieving a balance between recognition speed and precision entails considering numerous factors throughout the face recognition process.

In conclusion, the development of machine learning face recognition models has revolutionized the field of identity verification and fraud prevention. [23] These models rely on feature extraction networks to convert face images into feature vectors, which are then matched with vectors in a reference library to determine identity. Traditional quantization methods, aimed at compressing these models for efficient mobile deployment, face challenges. The conversion of 32-bit floating-point numbers to 8-bit integers through methods like unsaturated, saturation, or affine modes can lead to increased recognition accuracy loss due to outlier points and uneven parameter distribution.

To address these challenges, innovative quantization techniques are essential. By optimizing the bit width of model data while preserving accuracy, mobile facial recognition technologies like FaceID can achieve a balance between speed and precision. [24-25] This optimization is crucial for ensuring seamless and reliable user experiences in various applications, from financial transactions to security management.

Therefore, in building a secure and reliable face recognition system, anti-fraud technology is crucial. First, the choice of sensors is crucial to resist spoofing attacks by detecting features in the signal in real time. Secondly, algorithm optimization is also the key, such as mirror feature projection, depth feature fusion and other methods can improve the recognition accuracy and anti-attack ability of the system. Comprehensive consideration of the choice of sensors and algorithms can effectively improve the security and reliability of face recognition systems in real scenarios.

3 Methodology

3.1 Model overview

Due to the rapid development of computer science and electronic technology, face recognition is now becoming the second largest biometric authentication method in the world after fingerprints in terms of market share. More and more manufacturers are incorporating face recognition into their products, such as Apple's face recognition technology on mobile phones, and banks are using [26]eKYC solutions for the onboarding process.

The main purpose of face recognition research is to improve the performance of verification and recognition tasks, in the past, the research on the security vulnerabilities of face recognition systems is relatively small, until recent years, people began to pay attention to different types of face recognition attack techniques, including recognizing whether a face feature is from a living person or a photo.

Two attack methods used on face recognition systems:

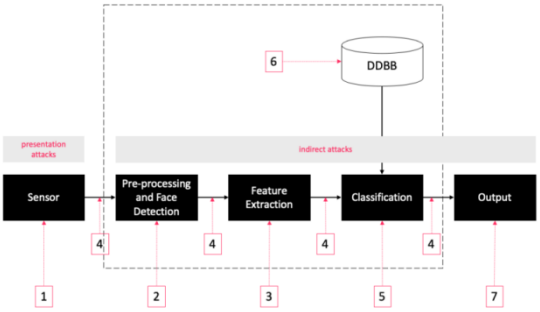

Figure 3 Face recognition system attack

As shown in Figure 3, there are seven modules and points that can be targeted as attacks, and they fall into two types: demonstrative attacks and indirect attacks.

Demonstration attack

The demonstration attack is carried out at the sensor level (1) without access to the system interior.

Demonstration attacks are related to pure biometric vulnerabilities, in which an intruder fraudulently accesses a biometric system using some kind of artifact, for example, a photo, mask, synthetic fingerprint or printed iris image, as well as attempts to mimic the behavior of a real user (e.g. gait, signature).

Since "biometrics are not secret," attackers are aware of the reality that a large amount of biometric data is

exposed, showing a person's face, eyes, voice, and behavior, so they can use this information resource to try to fool a face recognition system using the following example.

Attackers use photos of users to be impersonated.

1.They use user videos to imitate.

Hackers can build and use 3D [27] models of the attacked face, for example, ultra-realistic masks

We use anti-spoofing technology to prevent these attacks.

Indirect attack； Indirect attacks are performed on media such as databases, matching communication channels, etc. (2-7), in this type of attack, the attacker needs to access the inside of the system; Indirect attacks can be prevented through related techniques related to "classical" cybersecurity (rather than biometrics), so we won't discuss them in this article.

2.Mode of attack

Most of the latest facial biometrics systems are vulnerable if demonstrative attack detection is not implemented.

Usually, facial recognition systems can be fooled by presenting a photo, video or 3D mask of the target person to the camera, or by using makeup or plastic surgery, etc., however, due to the high exposure and low cost of high-resolution digital cameras, the use of photos and videos is the most common type of attack.

Photo attack: A photo of the attacked identity is displayed on the sensor of the facial recognition system.

Video attack: An attacker can play a legitimate user's video in any device that copies the video and then present it to a sensor/camera.

3D Mask attack: In this type of attack, the attacker builds a 3D reconstruction of the face and presents it to the sensor/camera.;Other attacks: Makeup, surgery

3.2 Fraud detection practice

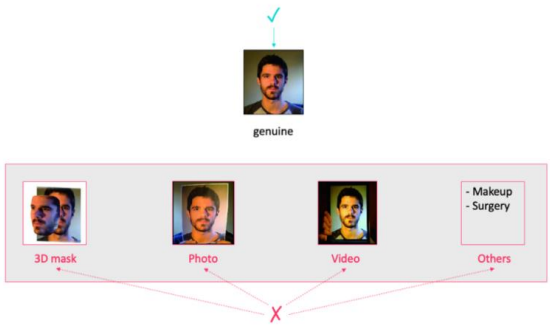

Figure 4 Anti-fraud architecture of face recognition system

The security of a face recognition system lies in its ability to resist spoofing attacks. In order to design a secure and reliable face recognition system in real scenes, anti-deception technology has become the first task. These techniques include a variety of aspects, from sensor selection to algorithm optimization.

First, the choice of sensor is crucial. We can use sensors to detect features in the signal in real time, such as signs of life through specialized hardware such as 3D cameras, or challenge response methods that require users to interact with the system in a specific way to detect demonstration attacks. In addition, recognizing facial expressions and head movements is also a common anti-deception method.

Secondly, the optimization of the algorithm is also crucial. The ability of face recognition system against deception attack can be improved by the techniques of mirror feature projection, deep feature fusion, image quality evaluation and deep learning. For example, specular feature projection can train SVM models by learning projections of real and fake data to detect simulated attacks. Deep feature fusion uses deep convolutional neural network to construct network structure, so as to effectively recognize face anti-deception data. The image quality evaluation evaluates the image quality by comparing the original image with the processed image. The deep learning method combines a pre-trained convolutional [29-30] neural network model and a local binary pattern descriptor to further improve the robustness of the system.

In summary, by choosing the right sensor and optimization algorithm, the face recognition system can improve its ability to resist deception attacks, so as to ensure the security and reliability in real scenarios.

4 Conclusion

With the popularity of FaceID face recognition technology in mobile phones, IoT and other devices, limited by energy consumption and device size, the computing performance and storage capacity of the hardware on the end is relatively weak, which brings new challenges to the face recognition on the end - the need for a smaller, faster and stronger model. In order to achieve faster and more accurate operation of FaceID face recognition technology on mobile terminals, quantification has become an important means. In simple terms, quantization is the process of replacing the original floating point data with lower bit data, which has reached the process of shrinking the model. The core challenge is how to reduce the bit width of the model data while ensuring the accuracy of face recognition. In order to solve the balance problem of face recognition speed and accuracy, it is necessary to consider many factors in the entire face recognition process, and then explain the benefits of face model quantization, the problems faced by the use of traditional quantization, Baidu FaceID face recognition model quantization technology/quantization benefits, and the support for different chips.

In conclusion, the integration of machine learning face recognition technology holds immense potential in bolstering fraud prevention measures within the financial sector. By leveraging advanced algorithms and big data analytics, financial institutions can swiftly detect and mitigate various forms of fraudulent activities, safeguarding both customer assets and personal information. Moreover, the advent of deep forgery detection techniques represents a critical step forward in addressing the evolving challenges posed by face fraud forgery. As these technologies continue to mature, they will play a pivotal role in enhancing the overall security and stability of financial systems, fostering trust and innovation in the digital era.

Acknowledgments

I would like to extend my sincere thanks to the authors of the cited literature and to the first authors, Lei H., Chen Z., Yang P., Shui Z., and Wang B. Their excellent work in the paper "Real-time Anomaly Target Detection and Recognition in Intelligent Surveillance Systems based on SLAM" provides valuable reference and inspiration for this research. Their in-depth exploration of real-time anomaly detection and recognition in intelligent surveillance systems based on SLAM lays a solid foundation for my research in this area. I sincerely thank them for their contributions and pay high tribute to their outstanding work. And would like to extend my sincere thanks to the authors of the cited literature and to the first author, Huang Zengyi, et al. Their remarkable work in the paper "Application of Machine Learning-Based K-Means Clustering for Financial Fraud Detection" provides valuable insights and methodologies for this research. Their application of machine learning-based K-Means clustering for financial fraud detection offers a significant contribution to the field. I sincerely appreciate their efforts and acknowledge the importance of their work in advancing the understanding and application of machine learning in fraud detection.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Author Contributions

Not applicable.

About the Authors

WANG, Yong

Information Technology, University of Aberdeen, Aberdeen, United Kingdom.

ZHAN, Xiaoan

Electrical Engineering, New York University, NY, USA.

ZHAN, Tong

Computer Science, Columbia University, NY, USA.

XU, Jiahao

Master of Science in Financial Engineering, University of Southern California, CA, USA.

BAI, Xinzhu

Tourism Management , Tianjin University of Finance and Economics, Tianjin, China.

References

[1] Lei, H., Chen, Z., Yang, P., Shui, Z., & Wang, B. (2024). Real-time Anomaly Target Detection and Recognition in Intelligent Surveillance Systems based on SLAM.

[2] Huang, Zengyi, et al. "Application of Machine Learning-Based K-Means Clustering for Financial Fraud Detection." Academic Journal of Science and Technology 10.1 (2024): 33-39.

[3] Xu, K., Zhou, H., Zheng, H., Zhu, M., & Xin, Q. (2024). Intelligent Classification and Personalized Recommendation of E-commerce Products Based on Machine Learning. arXiv preprint arXiv:2403.19345. (15 个)

[4] Zhou, H., Xu, K., Bao, Q., Lou, Y., & Qian, W. (2024). Application of Conversational Intelligent Reporting System Based on Artificial Intelligence and Large Language Models. Journal of Theory and Practice of Engineering Science, 4(03), 176-182.

[5] Li, L., Xu, K., Zhou, H., & Wang, Y. (2024). Independent Grouped Information Expert Model: A Personalized Recommendation Algorithm Based on Deep Learning.）

[6] Che, C., Lin, Q., Zhao, X., Huang, J., & Yu, L. (2023, September). Enhancing Multimodal Understanding with CLIP-Based Image-to-Text Transformation. In Proceedings of the 2023 6th International Conference on Big Data Technologies (pp. 414-418).

[7] Huang, Zengyi, et al. "Research on Generative Artificial Intelligence for Virtual Financial Robo-Advisor." Academic Journal of Science and Technology 10.1 (2024): 74-80.

[8] Wu, Jiang, et al. "Case Study of Next-Generation Artificial Intelligence in Medical Image Diagnosis Based on Cloud Computing." Journal of Theory and Practice of Engineering Science 4.02 (2024): 66-73.

[9] Zhu, Mingwei, et al. "Enhancing Collaborative Machine Learning for Security and Privacy in Federated Learning." Journal of Theory and Practice of Engineering Science 4.02 (2024): 74-82.

[10] Li, X., Zong, Y., Yu, L., Li, L., & Wang, C. (2024, February). OPTIMIZING USER EXPERIENCE DESIGN AND PROJECT MANAGEMENT PRACTICES IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE INNOVATION. In The 8th International scientific and practical conference “Priority areas of research in the scientific activity of teachers”(February 27–March 01, 2024) Zagreb, Croatia. International Science Group. 2024. 298 p. (p. 214).

[11] Zhu, Mengran, et al. "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach." Journal of Theory and Practice of Engineering Science 4.02 (2024): 23-30.

[12] Wu, Jiang, et al. "Case Study of Next-Generation Artificial Intelligence in Medical Image Diagnosis Based on Cloud Computing." Journal of Theory and Practice of Engineering Science 4.02 (2024): 66-73.

[13] Haowei, M. A., et al. "Employing Sisko non-Newtonian model to investigate the thermal behavior of blood flow in a stenosis artery: Effects of heat flux, different severities of stenosis, and different radii of the artery." Alexandria Engineering Journal 68 (2023): 291-300.

[14] Sun, Guolin, et al. "Revised reinforcement learning based on anchor graph hashing for autonomous cell activation in cloud-RANs." Future Generation Computer Systems 104 (2020): 60-73.

[15] Li, H., Wang, X., Feng, Y., Qi, Y., & Tian, J. (2024). Integration Methods and Advantages of Machine Learning with Cloud Data Warehouses. International Journal of Computer Science and Information Technology, 2(1), 348-358.

[16] Zhou, Y., Tan, K., Shen, X., & He, Z. (2024). A Protein Structure Prediction Approach Leveraging Transformer and CNN Integration. arXiv preprint arXiv:2402.19095.

[17] Ni, Chunhe, et al. "Enhancing Cloud-Based Large Language Model Processing with Elasticsearch and Transformer Models." arXiv preprint arXiv:2403.00807 (2024).

[18] He, Z., Shen, X., Zhou, Y., & Wang, Y. Application of K-means clustering based on artificial intelligence in gene statistics of biological information engineering.

[19] Wu, Y., Jin, Z., Shi, C., Liang, P., & Zhan, T. (2024). Research on the Application of Deep Learning-based BERT Model in Sentiment Analysis. arXiv preprint arXiv:2403.08217.

[20] Xu, Z., Gong, Y., Zhou, Y., Bao, Q., & Qian, W. (2024). Enhancing Kubernetes Automated Scheduling with Deep Learning and Reinforcement Techniques for Large-Scale Cloud Computing Optimization. arXiv preprint arXiv:2403.07905.

[21] Xu, X., Xu, Z., Ling, Z., Jin, Z., & Du, S. (2024). Comprehensive Implementation of TextCNN for Enhanced Collaboration between Natural Language Processing and System Recommendation. arXiv preprint arXiv:2403.09718.

[22] Shi, Peng, Yulin Cui, Kangming Xu, Mingmei Zhang, and Lianhong Ding. 2019. "Data Consistency Theory and Case Study for Scientific Big Data" Information 10, no. 4: 137. https://doi.org/10.3390/info10040137.

[23] Zhenghua Hu, Xianmei Wang, Kangming Xu, and Pu Dong. 2020. Real-time Target Tracking Based on PCANet-CSK Algorithm. In Proceedings of the 2019 3rd International Conference on Computer Science and Artificial Intelligence (CSAI '19). Association for Computing Machinery, New York, NY, USA, 343–346. https://doi.org/10.1145/3374587.3374607.

[24] Song, B., Xu, Y., & Wu, Y. (2024). ViTCN: Vision Transformer Contrastive Network For Reasoning. arXiv preprint arXiv:2403.09962.

[25] Wu, Binbin, et al. "Enterprise Digital Intelligent Remote Control System Based on Industrial Internet of Things." (2024).

[26] Pan, Y., Wu, B., Zheng, H., Zong, Y., & Wang, C. (2024, March). THE APPLICATION OF SOCIAL MEDIA SENTIMENT ANALYSIS BASED ON NATURAL LANGUAGE PROCESSING TO CHARITY. In The 11th International scientific and practical conference “Advanced technologies for the

implementation of educational initiatives"(March 19–22, 2024) Boston, USA. International Science Group. 2024. 254 p. (p. 216).

[27] K. Xu, X. Wang, Z. Hu and Z. Zhang, "3D Face Recognition Based on Twin Neural Network Combining Deep Map and Texture," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1665-1668, doi: 10.1109/ICCT46805.2019.8947113.

[28] Medication Recommendation System Based on Natural Language Processing for Patient Emotion Analysis. (2024). Academic Journal of Science and Technology, 10(1), 62-68. https://doi.org/10.54097/v160aa61

[29] Li, X., Zheng, H., Chen, J., Zong, Y., & Yu, L. (2024). User Interaction Interface Design and Innovation Based on Artificial Intelligence Technology. Journal of Theory and Practice of Engineering Science, 4(03), 1-8.

[30] Huang, Zengyi, et al. "Research on Generative Artificial Intelligence for Virtual Financial Robo-Advisor." Academic Journal of Science and Technology 10.1 (2024): 74-80.