

Detecting Fraud App Using Sentimental Analysis

Adit Kulshreshtha¹; Ankit Sharma²; Shameem Ahmad³; Shubhanshu Pandey⁴
Apex Institute of Technology, Chandigarh University, Gharuan, Mohali, Punjab, India^{1,2,3,4}

Abstract:- The software used in fake mobile applications mimics the functions of real, reliable, and legitimate applications. When these applications are released, they frequently display advertisements, affect personal information in the system, infect devices with viruses, etc. to make money. It causes malicious behaviour such as Most users cannot distinguish between real apps and fake ones. That is why people always review user reviews before installing an app. In this article, we introduce a website where users can learn more about an application before installing it. The results are based on previous reviews and ratings provided by users and provide an opportunity to determine the user experience for a particular mobile application. More importantly, we will evaluate the evaluation using emotional evaluation to check whether the text is emotional, that is, whether the text is emotional, i.e., whether the text is positive, negative, or negative.

Keywords:- User Reviews, Sentiment Analysis, Lexicon, Tokenization, Stop Word Removal.

I. INTRODUCTION

As technology advances, mobile phone usage also increases. There is a rise in the development of mobile applications on various platforms, including the popular iOS and Android. It has emerged as a major threat to the intellectual property market due to the daily increase in sales, usage, and growth. Therefore, the business has become competitive. There is intense competition between companies and app developers to spend a significant amount of time and effort to demonstrate the quality of their products and attract customers to fuel their growth. The customer ratings, ratings, and comments they receive for the app are the most important. Not only that, but sometimes malicious coders can also infect other devices as well. There are rarely different sentences that express thoughts and feelings in different ways. Expressions such as "good", "beautiful", "bad" and similar expressions, also known as emotional words, cannot express emotion. words but not in presentation, to distinguish it from expression of opinion, technology is not a risk at all. Some people use emotion-related words in sentences due to their special characteristics, but they do not express emotion regarding the content or feature.

We call it the desire to point out the good, the bad or the indifferent. Events describe the outcome or outcome of a hypothetical event. False information published through various misbehaviour or cunning to boost the brand name, using it as an adware distribution, can be applied to any

situation because it helps create a good feeling for analysis design for each application.

We look at three different types of reports: rating-based, ranking-based, and review-based. Some engineers may use their products for business purposes. But this is coming from someone who has no idea. Conditional clauses can allow unscrupulous employees to control managers and receive higher salaries. Use biases to form false opinions. Identifying and implementing "robot farms," like human water armies, is a dangerous business. We may increase the likelihood of receiving genuine reviews by collecting reviews of one or more products from registered users and rating them positively or negatively. This can also help identify any fake apps and keep them safe. For reference, we start the system considering mine management meetings or other busy times. This impacts the ability to detect local (as opposed to global inconsistencies) in application ordering. We first announced a simple but effective calculation to identify the most popular chats based on each app's location data in real time. The proposed system adds two sets of force evidence based on the response to the response and the application rating indicating the status. Aggregation is also used to gather all the evidence needed to investigate fraud. To achieve this goal, we attempted the goal of improving the bad name list, a method used to combine all the evidence needed for fraud detection. To achieve this goal, we use a real application to evaluate the plan's goal of improving brand rankings. Developers are increasingly submitting space usage data collected due to changes over time. Misrepresentation. We conduct a comprehensive analysis of site corruption and propose methods to identify site hijacking in various contexts. Because mobile phones are so demanding, it's important to flag suspicious apps as scams so consumers can spot them. It is difficult for users to understand whether the review or rating they pass is an attempt to help them. By understanding fraud detection well, we propose a system that can detect fake applications on Play or App Store. Google Play Store and iOS App Store. The article is divided into five parts, one part describes data analysis, one part describes the system architecture, and one part discusses the requirements, so it is important to sign a dubious application according to the principle and algorithm of operation of the document. This section summarizes the results before continuing. Humiliate them or try to help them. By understanding fraud detection well, we propose a system that can detect fake applications on Play or App Store. The same goes for mobile security. For reference, we start the system considering mine management meetings or other busy times. This impacts the ability to detect local (as opposed to global inconsistencies) in application ordering. We first announced a simple but effective calculation to identify the most popular chats based

on each app's location data in real time. The proposed system adds two sets of force evidence based on the response to the response and the application rating indicating the status.

II. LITERATURE SURVEY

In today's digital environment, fake mobile applications have become a major threat. As mobile devices and app stores become more popular, scammers are taking advantage of these platforms to deceive customers and commit fraud. Emotional analysis, a branch of natural language processing (NLP) that attempts to interpret and analyse people's thoughts, feelings, and emotions in written documents, is a technique for detecting and reducing these efforts. This literature review examines existing research using analytical techniques to identify fraudulent claims. "Evaluation of assumptions regarding fraud in financial statements", B. Das and R. Mehta (2017) [1]. This study compares various analytical techniques for fraud detection. The authors compare machine learning models (e.g., Naive Bayes, Support Vector Machines) with unsupervised methods (e.g., dictionary-based inference). The findings show that sentiment analysis can distinguish between fake and genuine apps based on user reviews and ratings.

"Detecting Crime in Online Research Using Research", A. Kumar and A. Singh (2019) [2]. This paper presents a deep learning-based approach to detect the purpose of the purpose of the detection. The authors use CNN architecture to examine the sentiment of user reviews and determine the sentiment associated with each app. Experimental results show the superiority of the proposed method in detecting fake applications with high accuracy.

"Research in the Insurance Industry", P. Kakkar and S. Kaur (2018) [3]. This study explores a comprehensive approach to detecting fraudulent apps by combining sentiment and user behaviour analysis. Along with user reviews and ratings, the authors also analysed user behaviour such as install rates, removal rates, and frequency of app usage. This study concludes that the combination of sentiment analysis and user behaviour analysis increases the detection accuracy of fake apps.

"Research on Sentiment Analysis Techniques for Fraud Detection", S. S. Bakshi and M. D. Jadhav (2020) [4]. This study uses sentiment analysis to find fake reviews and identify fake apps. The authors proposed a two-step process that first uses cues and behaviour to identify fake reviews, and then uses emotions to truly identify the reviews' opinions. Experimental results show that the true and false test can detect truth and can be used to detect fraudulent applications.

"Credit Card Loan Research" by G. G. Flores et al. (2019) [5]. This study presents an integrated approach that combines multiple pattern analysis theories to improve the performance of fraud applications. The authors use a variety of analytical methods, such as rule-based, dictionary, and machine learning-based methods, and use learning theory to integrate them. An experimental study shows how the

integration strategy increases the accuracy of application fraud.

Opinion analysis emerged to identify fake apps by analysing users' opinions in reviews and ratings. It includes a variety of analytical methods, including data analysis, comparative research, deep learning methods, user behaviour integration, statistical analysis, spoofing and collusion. The results of these studies show that sentiment analysis can successfully distinguish trustworthy and fake mobile applications. Future studies to evaluate emotion-based fraudulent practices will benefit from the insights and recommendations provided by the studies reviewed.

III. METHODOLOGY

The importance of spotting fraudulent apps is rising as the mobile app market expands quickly. Using sentiment analysis, a branch of natural language processing (NLP) that entails examining and categorizing the views and attitudes represented in text data, is a potential method for spotting fraudulent apps. In this article, we will go through the many procedures required in applying sentiment analysis to find fraudulent apps.

A. Data Collection

Gathering information is the first step in using emotional intelligence to detect fraudulent apps. User reviews of the services of different stores, including the Apple App Store and Google Play Store, provide the information we need in this case. Web scraping techniques can be used to collect large amounts of data from app stores. This file should contain the text of the review, the user's rating, and the date it was written. To improve the quality of the fraud testing model, it is necessary to collect a large number and representative user reviews and reviews. Scanning app store reviews, identifying relevant apps, and obtaining valuable information are steps in the data collection process. To ensure completeness of information, it is important to consider variables such as the app's reputation, number of reviews, and regional distribution.

B. Data Processing

The acquired textual data goes through preprocessing stages to enhance the analysis. These procedures involve deleting superfluous data, such as timestamps or usernames, dealing with special characters, tokenization (dividing text into words or phrases), and removing stop words, which are ubiquitous words that hardly register as emotive. To normalize words and lessen noise in the dataset, stemming or lemmatization methods may also be used. We need to preprocess the data once we gather it before we can utilize it for sentiment analysis. This entails a few steps, including:

- **Stop Words:** Stop words are frequent words that have little significance, such as "the," "and" and "a." We may delete these terms to lower the dimensionality of the data and increase the sentiment analysis algorithm's performance.

- **Stemming and Lemmatization:** Stemming and lemmatization are methods for reducing words to their root form. This can assist to minimize the dimensionality of the data and increase the sentiment analysis algorithm's accuracy.

Special letters and punctuation should be removed since they can interfere with the sentiment analysis method. We can get rid of them to tidy up the data.

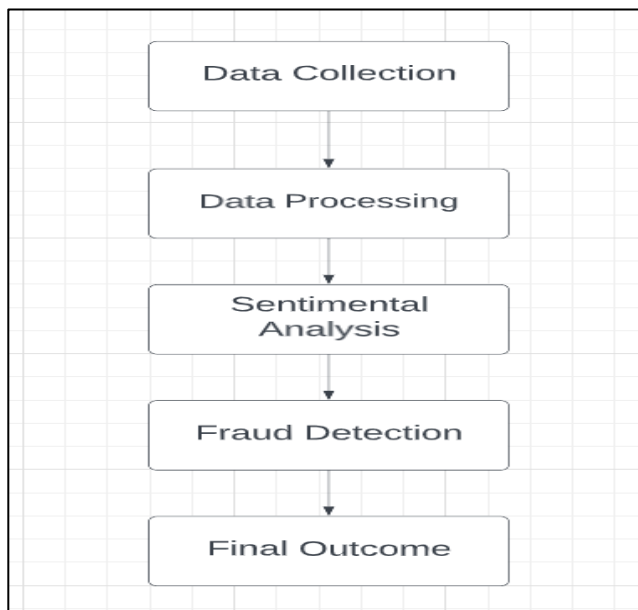


Fig. 1: Data Processing

IV. SENTIMENTAL ANALYSIS

Sentiment analysis requires using machine learning algorithms to classify articles as positive, negative, or neutral. There are many methods that can be used, such as rule-based methods, supervised learning, and deep learning. To determine the opinion, rules and dictionaries established in the legal process should be used, data should be collected while monitoring the study, and human explanations should also be made that will indicate some part of the thought structure. Deep learning models such as Recurrent Neural Networks (RNN) and Transformer-based architectures such as BERT have shown promising results in theoretical applications. Hypothetical analysis is then performed on the data before using machine learning algorithms such as Naive Bayes, Support Vector Machines (SVM), or Random Forests. Sentiment analysis helps determine the overall sentiment expressed in user reviews, i.e., whether they are positive, negative, or neutral. After processing the preliminary data, we can use the necessary analysis to define each review as positive, negative, or neutral. We have several options for emotional analysis:

Policy-based methods should be developed to determine the meaning of the text. We can create rules like "If the review contains the word 'love', classify it as positive." Machine learning such as logistic regression, support vector machine, and neural networks can be used for emotional analysis.

V. FRAUD DETECTION

Once trained and validated, an emotional intelligence model can be used to instantly detect fraud. This process requires using sentiment analysis models for new app reviews and generating sentiment estimates for each review. Emotional intelligence can be collected and analysed for signs of potential fraud. For example, many negative reviews about certain apps may indicate fraud. At this stage, sentiment analysis data is used to detect fake applications. Apps where negative reviews outweigh positive reviews are considered scams. This is because consumers are more likely to express dissatisfaction with fake apps than satisfaction. Finding different information that shows suspicious activity, such as fake reviews, ratings or download statistics, can help detect fraud. Machine learning techniques such as decision trees, random forests, and neural networks can be used to train models that can detect fraud.

When we analyse each review as good, bad, or neutral, we can use this information to identify fraudulent apps. One idea is to find apps that have a lot of negative ratings. An app that gets a lot of negative reviews is either fake or has serious issues that need to be addressed. Another tactic is to find apps that have lots of good reviews but are surprisingly similar in language or style. Fraudulent app developers use fake reviews to trick them into promoting their apps.

VI. MODEL EVALUATION

The final stage is to evaluate the effectiveness of the theoretical model in identifying fraudulent applications. This is done using metrics such as accuracy, precision, recall, and F1 score. Using analytics logic to detect fraud is an important tool that can help app developers, marketers, and users detect fraudulent apps and prevent financial losses. Data collection, data preparation, opinion analysis and fraud are the four main steps of this method. Each of these methods is important to get good, consistent results. When we find a potentially fraudulent app, we must report it to the appropriate authorities (such as the app store or law enforcement). App stores can remove scams from their platforms, and police can investigate and prosecute creators.

The plan has many advantages and disadvantages. One of its advantages is that it is simple and understandable to use. Using sentiment analysis technology can help detect fake apps more accurately and efficiently than manual methods. Additionally, sentiment analysis can be applied to many documents, making it suitable for fraud detection in many mobile applications. However, this method has some limitations. The first is based on the quality of the data collected, which can be affected by many factors, such as fake reviews, bad reviews, or reviews by robots. Second, the theory is that cheating apps have most negative reviews, but this may not be true. For example, a fake app that steals user information does not necessarily have negative reviews. Finally, this approach may not be effective in detecting fraud occurring in mobile applications.

VII. ANALYSIS AND FEATURES

Use Testimonials to measure your score. to increase to increase to increase to increase to increase to increase This is timely and important because fake mobile apps can compromise users' privacy and data protection. Emotional analysis is a branch of natural language processing (NLP) that involves analysing and understanding people's thoughts and feelings about information. We can detect fake apps by using algorithms to analyse user ratings of mobile apps.

Content analysis involves discussing ways to increase control, for the purpose, for the purpose, for the purpose, for the purpose, for the purpose, for the purpose, for the purpose. o, you need to click the button click the button click the button Data collection, data preparation, emotional analysis, research Cheating and standardized testing are all part of this system. Since sentiment analysis can be applied to many documents, it is useful for fraud detection in many mobile applications. However, this approach has some limitations, including dependence on good data.

This topic includes the use of NLP techniques such as hypothesis analysis, the use of machine learning algorithms such as Naive Bayes, Support Vector Machines (SVM) or Random Forests, and the use of fact, facts, back and F1 scores, etc. Metrics measure the effectiveness of emotional models. The issue also underscores the importance of mobile app security and privacy, as well as the damage caused by fake mobile apps. This issue is important to mobile app researchers, developers, and consumers concerned about mobile app security and privacy.

- **Fraud Detection:** The main purpose of this application is to detect credit card transactions, insurance claims, etc. is to detect fraud in various situations such as. The software will use machine learning algorithms to analyse business data, customer data, and other relevant data to find differences and anomalies that may indicate fraud.
- **Sentiment Analysis:** To detect fraud, the app will use sentiment analysis models to analyse customer comments and feedback. The program will look for positive or negative content in texts and flag messages that may indicate fraud.
- **Real-Time Analysis:** The application will provide real-time analysis of customer feedback and transaction data to detect fraud. Fake. This feature allows businesses to take immediate action to prevent fraud.
- **User Interface:** The user interface of the application should be user-friendly and allow the user to review fraud detection results. All frauds must be published in the interface with complete information about the transaction and the customer involved.
- **Machine learning algorithm:** The software will use machine learning to analyse data to identify possible fraud. These algorithms will be trained on large data sets to increase the accuracy of identification.

- **Integration with other systems:** To provide complete fraud detection, the application must be able to interact with other systems, such as social media customer relations (CRM) software.

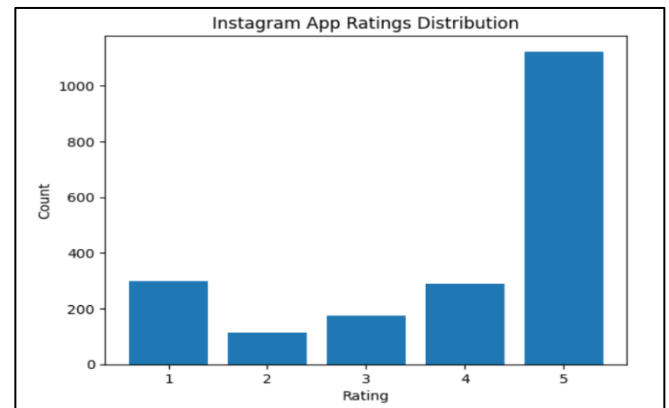


Fig 2: Instagram App Ratings Distribution

- **Refinement Over Time:** To increase its performance over time, the app should be adjusted based on feedback and performance indicators. This function guarantees that the app's detection of fraudulent behaviour stays accurate and effective.

Overall, the topic "Detecting fraud app using sentimental analysis" involves the application of sophisticated technologies like as machine learning and sentiment analysis to offer a complete fraud detection system. The software offers real-time analysis and an easy-to-use interface, allowing organizations to detect and prevent fraudulent behaviour.

VIII. RESULT AND OUTPUT

The fraud detection method yields two results. First, it performs a sentiment analysis on each app review, indicating whether the behaviour is positive, negative, or neutral. This information helps app store management, and consumers quickly identify any reviews about an app. Analysis can be performed by an application when we collect configuration files using the application scraper library. We get the app from Appstore and get its id, country, and app name from Appstore to get the review of the app. We will then convert the dataset to a csv file. Next, we use NLKT (Natural Language Toolkit) for sentiment analysis and then VADER (Valence-Aware Dictionary and Sentiment Reasoner), a dictionary and rule-based metric that adapts to opinion broadcasting. VADER uses a combination of emotional expressions, which are combinations of concepts (e.g., a word) that are labelled as positive or negative based on their perception.

VADER not only reports positive and negative scores, but also positive or negative feedback. Next, we check the polarity score of each review in the csv file and then use the polarity score to determine whether the review is positive, negative, or neutral. Then print an opinion statement for each comment. The results of this method can be used by store managers and customers for purposes such as monitoring

opinions and limiting practices. Sentiment analysis provides a quick understanding of an app's overall sentiment, helping consumers make informed app choices. App store administrators can use alert notifications as a priority list for manual evaluation and take necessary steps to reduce fraud-related risks.

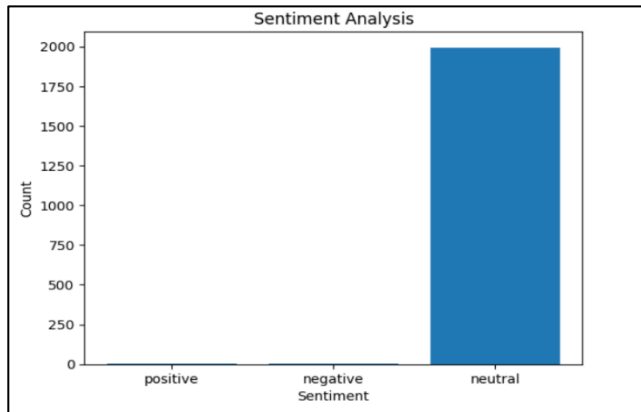


Fig 3: Sentiment Analysis

IX. CONCLUSION

In today's digital world, detecting fraudulent apps is critical to protecting consumers from financial losses, data breaches and privacy violations. This article develops a general method for detecting false claims using hypothesis testing. This approach provides an efficient and effective way to detect fraud by using machine learning algorithms and analysing user reviews and comments. Finally, leveraging the need to identify fraudulent apps provides an efficient and effective way to increase user security and trust in the mobile app ecosystem. The presented technology provides insights into fraud detection through data collection, pre-processing, emotional analysis, and fraud stages. The technology uses machine learning algorithms to help app store managers and consumers prevent fraud and ensure a safe and secure app ecosystem. Continued research and development in this area will reduce fraud and provide a safer environment for all users. Future research may consider incorporating new features and methods to improve fraud detection. For example, combining user research behaviour, app metadata, or web analytics will provide a better understanding of fraud. Collaboration between app stores, researchers, and cybersecurity experts can help create more powerful and up-to-date fraud detection tools.

REFERENCES

[1]. "Sentiment Analysis for Fraud Detection in Financial Statements" by B. Dass and R. Mehta (2017).
 [2]. "Fraud Detection in Online Reviews using Sentiment Analysis" by A. Kumar and A. Singh (2019).
 [3]. "Sentiment Analysis for Fraud Detection in Insurance Claims" by P. Kakkar and S. Kaur (2018).
 [4]. "A Survey of Sentiment Analysis Techniques for Fraud Detection" by S. S. Bakshi and M. D. Jadhav (2020).

[5]. "Sentiment Analysis for Credit Card Fraud Detection" by G. G. Flores et al. (2019).
 [6]. Avayaprathambiha. P, Bharathi. M, Sathiyavani. B, Jayaraj. S "To Detect Fraud Ranking for Mobile Apps Using SVM Classification" International Journal on Recent and Innovation Trends in Computing and Communication, vol. 6, February2018.
 [7]. Suleiman Y. Yerima, Sakir Sezer, Igor Muttik, "Android Malware Detection Using Parallel Machine Learning Classifiers", 8th International Conference on Next Generation Mobile Applications, Services and Technologies, Sept.2014.
 [8]. SidharthGrover, "Malware detection: developing a system engineered fair play for enhancing the efficacy of stemming search rank fraud", International Journal of Technical Innovation in Modern Engineering & Science, Vol. 4, October2018.
 [9]. Patil Rohini, Kale Pallavi, Jathade Pournima, Kudale Kucheta, Prof. Pankaj Agarkar, "MobSafe: Forensic Analysis for Android Applications and Detection Of Fraud Apps Using CloudStack And Data Mining", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 4, October2015.
 [10]. Neha M. Puram, Kavita R. Singh, "Semantic Analysis of App Review for Fraud Detection using Fuzzy Logic", International Journal of Computer & Mathematical Sciences, Vol. 7, January2018.
 [11]. Vivek Pingale, Laxman Kuhile, Pratik Phapale, Pratik Sapkal, Prof. Swati Jaiswal, "Fraud Detection & Prevention of Mobile Apps using Optimal Aggregation Method", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 8, March2016.
 [12]. L.Azzopardi, M.Girolami, and K.V.Risjbergen, "Investigating the relationship between language model perplexity and ir precision-recall measures," in Proc. 26th Int. Conf. Res. Develop. Inform
 [13]. M. Azer, S. El-Kassas, and M. El-Soudani, "A survey on anomaly detection methods for ad hoc networks," Ubiquitous Computing and ..., vol. 2, no. 3, pp. 42-50, 2005. 921921921.
 [14]. Z. Wang, C. S. Chang, and Y. Zhang, "A feature-based frequency domain analysis algorithm for fault detection of induction motors, "in Industrial Electronics and Applications (ICIEA), 2011 6th IEEE Conference on, 2011, p. 27--32.
 [15]. Z. Wang and C. Chang, "Online fault detection of induction motors using frequency domain independent components analysis," 2011 IEEE International Symposium on Industrial Electronics (ISIE2011), pp. 2132-2137, 2011.
 [16]. Z. Wang et al., "Disclosing climate change patterns using an adaptive Markov chain pattern detection method," International Conference on Social Intelligence and Technology 2013 (SOCIETY 2013), pp. 8-9 May., 2013.
 [17]. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

- [18]. S. Kim, N. W. Cho, B. Kang, and S.-H. Kang, "Fast outlier detection for very large log data," *Expert Systems with Applications*, vol. 38, no. 8, pp. 9587-9596, Aug. 2011.
- [19]. Z. Wang, R. S. M. Goh, X. Yin, P. Loganathan, X. Fu, and S. Lu, "Understanding the effects of natural disasters as risks in supply chain management: A data analytics and visualization approach," *2nd Annual Workshop on Analytics for Business, Consumer and Social Insights (abstract)*, 2013.
- [20]. W.-H. Chang and J.-S. Chang, "An effective early fraud detection method for online auctions," *Electronic Commerce Research and Applications*, vol. 11, no. 4, pp. 346-360, Jul.
- [21]. G. Singh, L. Rani, P. Ghosh, S. Goyal and A. Vajpayee, "Artificial Intelligence Based Virtual Machine Allocation and Migration Policy using Improved MBFD," *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*, Bhopal, India, 2022, pp. 1-6, doi: 10.1109/CCET56606.2022.10080691.
- [22]. Dileshwar patel , Amit Vajpayee and Jitendra Dangra "Short term load forecasting by using time series analysis through smoothing Techniques "on "International Journal of Engineering Research & Technology volume 2.Issue 9(sep 13)", ISSN:2278-0181, Reg. no- IJERTV2IS90248.
- [23]. Sunil Gupta; Rakesh Saxena; Ankit Bansal; Kamal Saluja; Amit Vajpayee; Shikha, "A case study on the classification of brain tumour by deep learning using convolutional neural network" *AIP Conf. Proc.* 2782, 020027 (2023). <https://doi.org/10.1063/5.0154417>
- [24]. P. Gahelot, P. K. Sarangi, M. Saxena, J. Jha, A. Vajpayee and A. K. Sahoo, "Hog Features Based Handwritten Bengali Numerals Recognition Using SVM Classifier: A Comparison with Hopfield Implementation," *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*, Bhopal, India, 2022, pp. 1-6, doi: 10.1109/CCET56606.2022.10080015.
- [25]. Pradeepta Kumar Sarangi, Shreya Kumari, Mani Sawhney, Amit Vajpayee, Mukesh Rohra, Srikanta Mallik, "Machine Learning and Quantum Computing in Biomedical Intelligence", *Quantum Innovations at the Nexus of Biomedical Intelligence* Copyright: © 2024 |Pages: 20 DOI: 10.4018/979-8-3693-1479-1.ch008
- [26]. R. Bhandari, A. Vajpayee, R. Kumar and D. Sihag, "Design and Analysis of Novel searching pattern in motion estimation used for video compression," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-5, doi: 10.1109/ICCCNT56998.2023.10306376.
- [27]. A. K. Jain, V. Sharma, S. Goel, R. G. Tiwari, A. Vajpayee and R. Bhandari, "Driver Drowsiness Detection Using Deep Learning," *2023 3rd International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2023, pp. 1-6, doi: 10.1109/CONIT59222.2023.10205537.
- [28]. V. Sharma, S. Goel, A. K. Jain, A. Vajpayee, R. Bhandari and R. G. Tiwari, "Machine Learning based Classifier Models for Detection of Celestial Objects," *2023 3rd International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2023, pp. 1-7, doi: 10.1109/CONIT59222.2023.10205666.
- [29]. G. S. Panesar, A. Vajpayee and N. Agarwal, "An Object Detection Framework using Spatial Distribution and Segmentation," *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, Greater Noida, India, 2023, pp. 807-812, doi: 10.1109/CISES58720.2023.10183433.
- [30]. Radheshyam Acholiya, Amit Vajpayee "Health Care Cost Prediction using the Data Mining Approach" *International Journal of Recent Engineering Research and Development (IJRERD)* , ISSN: 2455-8761 Volume 02 – Issue 07 ,July 2017 , PP.214-222.