Fake Account Detection Using Machine Learning

Geethu Mary George[1,a)], Jana.T[2,b)] , Nilavarsan.P [3,c)] , Praveen.R [4,d)] , Yaswanth.M[5,e)]
Assistant Professor, Department of Information Technology, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India[1]
Students, Department of Information Technology, Karpagam College of Engineering, Coimbatore, Tamil Nadu,India[2,3,4,5]

Abstract- Current advancements in social networking and the World Wide Web (WWW) open the door to data exchange that has never been seen in human history. The establishment of fictitious accounts on this network is a serious security concern. Furthermore, the automated categorization of the text piece as authentic or fraudulent is an essential procedure. Because people are incapable of telling the difference between genuine and misleading information, fake news poses a threat to government journalism, democracy, legitimacy, and logical truth. Furthermore, one of the main areas of study in the field of social media analytics is automatically generated fake news or rumours from social networking sites. There are various circumstances where inter-social network operations and features are necessary. User profiles that match must be used to do this. The restrictions of current methodologies prevent them from taking into account all connected issues. Deep learning models provide the capacity to discover complex patterns and relationships from large-scale datasets, which makes it possible to identify minor indicators suggestive of fraudulent activity in the context of fake account detection. In particular, they presume that two profiles only depict the same physical person if their homepage, email address, and other IFP values—that is, FRUI (Friend Relationship-Based User Identification) with Inverse Functional Property, or IFP match. The project aims to tackle numerous vital issues related to the detection of bogus accounts, such as data imbalance, adversarial manipulation, and the dynamic growth of deceptive strategies.

Keywords— Social networking, Fake account, Fake news, Rumour detection, Deep learning

I.INTRODUCTION

Fake account detection is a critical and rapidly evolving field within the realm of cyber-security and online safety. With the explosive growth of social media and online platforms, the proliferation of fraudulent accounts, often created with malicious intent, has become a pervasive issue. These fake accounts can be used for various harmful activities, including spreading misinformation, conducting identity theft, engaging in cyberbullying, and orchestrating phishing attacks. Detecting and mitigating the presence of these fraudulent accounts is crucial not only to safeguard the integrity of online communities but also to protect the personal and financial security of users. As a result, the development and deployment of sophisticated fake account detection methods have become paramount in the ongoing battle against online deception. Counterfeit account detection involves the use of advanced algorithms and machine learning techniques to identify accounts that are created with the intent to deceive or harm. These methods analyze a wide range of user attributes and online behaviours, including profile information, posting patterns, interaction networks, and content semantics, to uncover anomalies and patterns associated with fraudulent accounts. The objective is to differentiate genuine users from impostors by scrutinizing various digital footprints. As technology continues to advance, the arms race between those who create fake accounts and those who develop detection mechanisms intensifies, highlighting the ever-evolving nature of this challenge. Effective counterfeit account detection not only helps maintain the trust and safety of online communities but also contributes to the broader effort of upholding the integrity of the digital landscape.

In the digital age, social media has changed the way people connect, communicate, and share information. It's emerged as a potent and universal force, expanding beyond geographic boundaries to bring together people from different backgrounds. Social media platforms provide individuals, businesses, and organizations with the means to create, share, and consume content, ranging from personal updates and photos to news, entertainment, and marketing. These platforms have become integral to modern life, shaping how we socialize, access information, and even conduct business. They offer a dynamic and interactive space where users can engage in conversations, express their opinions, and build online communities. As a result, social media has not only transformed the way we communicate but also influenced societal norms, politics, and global culture in ways that were previously unimaginable. The influence of social media is pervasive, with billions of users across various platforms worldwide. Facebook, Twitter, Instagram, and TikTok, among many others, have redefined how information is disseminated, making it faster and more democratic. The immediacy of social media has transformed the news cycle, enabling real-time reporting and citizen journalism. It has also become a hub for businesses to market their products and services, tapping into vast online audiences. However, with these advantages come challenges, including concerns about privacy, misinformation, and cyberbullying. Due to its ability to facilitate connections with friends, family, acquaintances, and even strangers, social media is a

valuable tool for social networking and communication online. The impact of social media on society is a complex and evolving story, and understanding its profound implications requires an exploration.

II. LITERATURE SURVEY

The proliferation of false information has led to grave issues, including notable impacts on social interactions. To create a neural network architecture that could accurately forecast the tone of an article based on the arrangement of its headlines and body. We have combined several sophisticated machine learning techniques, most notably logistic regression and recurrent neural network techniques. As a result, research on the identification of fake news via social media has gained popularity, and numerous studies have attempted to create ML-based techniques for classifying phoney news. Han et al.[1] .The exponential increase in online information and the rise in the number of social media users are direct results of the quick development of network services. Set up a new dataset containing 2366 English-language tweets on the Hong Kong protests. When distinct features have been identified as a determining element for the detection of fake news, both the language features and the network accounts have been extracted from the tweets. This method took into account binary classification and SMOTE oversampling in order to overcome the class imbalance. The Rapid Miner Studio has been used to carry out the feature extraction and SMOTE over-sampling. The suggested approach is evaluated on a fresh, original data set of 2,366 English-language tweets on the events in Hong Kong in August 2019. Two machine-learning models were used during the experiment phase. When compared to earlier research, both models were able to accurately predict the samples labelled as "real" and "fake" Nikiforoset al.[2].To get the binary classification on 1356 news from Twitter and 1056 real and fake news from PolitiFact, connected the different ensembles. It may create the dataset for each topic and then handle the encoding and tokenization on its own. Gathered 1356 news examples from other individuals on Twitter and from media sites like PolitiFact, then made multiple datasets for the phoney and the actual news. While Ko et al. tackled the issue of identifying fake news and reached an 85% detection rate, CNN + bidirectional LSTM ensembled network with attention mechanism achieved the most fantastic accuracy of 88.78% Kumar et al.[3].

To identify phoney accounts on social networks, a method based on user-colleague resemblance was provided. In this method, new characteristics were retrieved from the PCA methodology, and The buddy similarity criteria were computed using the network graph's adjacency matrix. After the data was balanced using the SMOTE approach, it was then passed to the classifier in a later step. The cross-validation approach was used to train and test the classifier, and the results indicated that the medium Gaussian SVM classifier Naman et al.[4].Ilhan et al. suggested that Machine learning algorithms were used to identify phoney accounts after preprocessing the generated dataset. The identification of fraudulent accounts is based on algorithms like logistic regression, decision trees and supporting vector machines. After comparing the categorization success of different approaches, it was established that logistic regression produces better outcomes[5]. The Twitter trends are safe from malicious users' tampering. More than 69 million tweets out of 5 million entries.First, an informational inquiry using the collected tweets to discover evidence of Twitter pattern control. At that time, the topic level and determine the crucial elements that determine whether a theme begins to skew due to its ubiquity, inclusion, transmission, possible inclusion, or renown, trade-off, and fake records, and discuss countermeasures Yubao et al.[6]

SVM-NN, a novel algorithm, is suggested to offer effective identification of phoney Twitter accounts and bots through the application of feature selection and dimension reduction approaches. Support vector machines, neural networks, and our unique SVM -N.N. algorithm are examples of machine learning classification techniques that were employed to determine if a target account is genuine or fraudulent. While utilizing fewer features, the suggested approach (SVM-NN) can accurately categorize approximately 98% of the accounts in our training dataset. Sarah et al.[7].Buket et al. proposed a classification method for identifying phoney Twitter accounts by preprocessing the dataset using the Naïve Bayes algorithm's results and a supervised discretization technique called Entropy Minimization Discretization (EMD) on numerical characteristics[8].Cheng Chen et al.[9] suggested a novel technique for identifying phoney OSN accounts.Based on patterns of user behaviour observed in Facebook activity, a machine learning method assesses if a fraudulent user is using an account. A breakdown of account operations based on the anticipated outcomes has also been supplied. Instead of using the more traditional spam keywords list to identify bogus accounts, Myo et al. proposed blocklisting. We performed an evaluation experiment using the Social Honeypot dataset in addition to the 1KS - 10KN dataset. Compare the accuracy of the blacklist-based strategy with the classic spam terms list-based approach. A meta-learner classifier called Decorate is used to distinguish between real and phoney Twitter accounts. The method's accuracy is 95.4%, and the actual positive rate is 0.95[10].

Partha et al. [11] employed the Twitter profile dataset, classifying phoney accounts as TWT, FSF, and INT and legitimate accounts as TFP and E13, then explained Random Forest, LSTM, X.G. Boost, and Neural

Networks. Finally, it concluded that the most effective machine-learning method for identifying phoney profiles is X.G. Boost. Shama et al.suggested determining if an account is real or fake by training machine learning models like random forests and neural networks on contrived features. The neural network system generated predictions with 93% accuracy, according to the predictionsSupport vector machines, neural networks, and our unique SVM -N.N. algorithm are examples of machine learning classification techniques that we employed to determine if a target account is real or fraudulent[12]. Smruthi et al. proposed that filthy photos and fictitious accounts on Facebook. The user timeline data, such as post-count and comment-count, was utilized to identify fake accounts. The user timeline and display pictures of the users were removed to determine vulgar photos. Supervised machine learning was used to assess the performance, and the images gathered from the fictitious accounts were used to compute the maximum exposed skin percentage. The highest accuracy of 80% was attained[13]. Narshimhaet al.[14] concluded that to raise the accuracy rate of social network phoney profile detection. This work aims to enhance the precision with which artificial intelligence (A.I.) and natural language processing (NLP) methods identify fraudulent profiles. We can employ the Naïve Bayes technique and Support Vector Machine (SVM). Gupta et al. suggested the utilization of Facebook user-feed data to comprehend user profile activity and the discovery of a comprehensive collection of 17 characteristics that are crucial in distinguishing authentic users from fraudulent ones on the social media platform. Since a large number of phoney users are labelled as accurate, it is evident that false accounts imitate actual user behaviour to avoid being discovered by security systems[15]. Engineered traits that had previously been effectively utilized to identify phoney accounts made by bots were added to a corpus of human accounts. Several supervised machine learning models were used with these features. Machine Learning models were trained using manufactured features rather than behavioural data. Due to this, these models were able to train on relatively low data volumes compared to when incorporating behavioural data in Van et al. [16].

III.EXISTING SYSTEM

The use of digital technologies is growing. Simultaneously, the number of evil users is rising. Millions of individuals worldwide use social media websites like Facebook and Twitter. The popularity of online networking has brought up several problems, such as the possibility of spreading dangerous content through the creation of fictitious accounts and revealing incorrect information. Using fictitious identities to send spam, conduct fraud, and misuse online social networks is a common practice. Solving these issues is necessary to provide the user with a trustworthy virtual social network. Support Vector Machine (SVM), Logistic Regression (L.R.), Random Forest (R.F.), and K-Nearest Neighbors (KNN) are among the machine learning methods employed in this study. To increase accuracy, we have used Z-Score and Min-Max, two distinct normalization techniques, in conjunction with these algorithms.

PRELIMINARIES

The fake accounts in the social networking sites are detected using the DSAE model. The KH-DSAE model initially receives the social networking data as the input and performs the DSAE-based detection process. The application of the FRUI algorithm enhances the detection performance of the DSAE model.

FRUI ALGORITHM

FRUI stands for Friends and Relation User Identifier. The picture determines the coordinating degree and initially depicts lattice rushing in Proposition 1. Once more, it shows how UMP misuse operates until there are no known umpires. The Candidate Umpire Rundown is no longer applicable in each emphasis once the UMPs are known, and R.I.'s revised calculations supported the recommendation a few times. In algorithmic control 1, the strategy is simplified. Consider that in every cycle, valid Priori UMPs exist. In the algorithmic manage 1, lines 4–11In addition, the time quality costs O(s) + O(min(vA, vB))=O(min(vA, vB)), where vA and vB signify the numbers of the customers in SMNA and SMNB, respectively, are removed, and the most match degree is refreshed..

Figure 2 below represents the graphical comparison of before and after integrated approach

Figure 1.Comparison of precision before and after integrated approach

PROPOSED SCHEME

This system includes four modules: User Authentication, Data Preprocessing, Implementation of FRUI Algorithm, and Recovering Fake Data.

FAKE ACCOUNT DETECTION – FLOW DIAGRAM

Figure 2 below represents the execution flow for the detection of fake accounts. First, it is processed through a social media network. After preprocessing the data by implementing the FRUI algorithm, it checks with previously used matched pairs with the help of identifiers. It identifies the matched pairs. After checking if the unit is not empty, it again proceeds with prior pairs. The output finally displays the matched profiles.

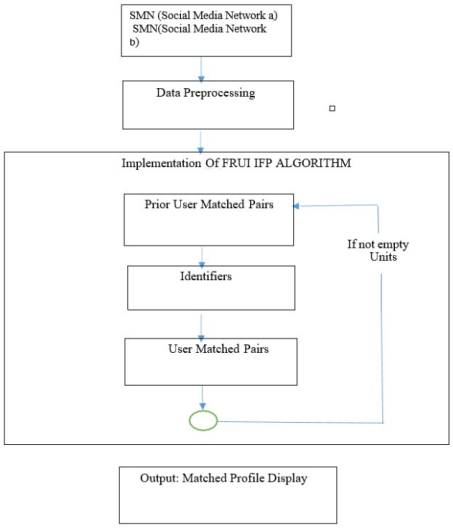

Figure 2. Execution flow diagram of fake account detection

USER AUTHENTICATION

In this module, the first user registers their details with security questions that will help to recover the original data. The reason why we choose the Q & A means if other secret passwords or other values are put in that place, hackers can easily find the password. A preprocessor is designed to acquire as many Priori UMPs as possible. Currently, there is yet to be a common approach available to obtain UMPs between two SMNs. Specified methods must be formulated according to given SMNs. Although no unified process is suitable for the Preprocessor, some algorithms can be adopted according to the application, e.g., email address, screen name, URL, etc. An email address is a unique feature for each account and can be used to collect Priori UMPs..

DATA PREPROCESSING

In this module, user can easily find if their login is misused or not. By sending the notification details like last time out, logout time, and I.P. address, we can find out the user's identity. The I.P. address is used to find the system located after the user can change their password. We have to find the hacker's I.P. address. We have mentioned that the hacking system I.P. is used to find the location. If the area is nearby, we can easily find the location of the original hacker.

DATA CLEANING

Duplicate records are eliminated to guarantee that the model is trained on distinct cases. Addressing data anomalies or outliers that could have an impact on the performance of the model

FEATURE EXTRACTION

They are obtaining pertinent properties from the raw data so that the fraudulent account detection algorithm can use them as input. Features could be I.P. addresses, device information, account creation details, user activity trends, etc., converting unstructured data into a format that is appropriate for machine learning techniques.

DATA SPLITTING

Separating the dataset into test, validation, and training sets to assess how well the model performs on untested data. The quality of preprocessed data has a significant impact on the efficacy of fraudulent account detection methods

IMPLEMENTATION OF FRUI ALGORITHM

We presented the Friend Relationship-Based User Identification (FRUI) algorithm in this module. All potential User Matched Pairs (UMPs) are given a matching degree by the FRUI (Friend Relationship User Identification Algorithm), and only UMPs with the highest rank share are regarded as identical users. We also developed two propositions to improve the efficiency of the algorithm. The Friend Relationship-Based User Identification (FRUI) algorithm was our suggestion. All candidate User Matched Pairs (UMPs) are given a matching degree by the FRUI (Friend Relationship User Identification Algorithm), and only UMPs with the highest rank share are taken into account as identical users. We also came up with two ideas to boost the algorithm's effectiveness.

RECOVERING FAKE DATA

In this project, the user's login process revolves around a secret question, which serves as a critical component for recovering any misused or compromised information. The original login page is designed to capture and display activities the legitimate user and potential unauthorized intruders perform. This transparency ensures that actions taken within the system, whether by the authentic user or a malicious actor, are visible on the front page, enabling a clear and real-time overview of account activity. If a legitimate user suspects their account has been compromised or their data misused, the secret question plays a pivotal role in the recovery process. It acts as a secure gateway for the user to regain control of their account and investigate any potential unauthorized access or tampering with their files and profile. Take relevant elements out of user account information. Information like the date of account creation, usage trends, I.P. addresses, device details, and more might be included in these services. To make sure the model performs well when applied to data that has yet to be observed, assess its performance using methods such as cross-validation. Keep an eye on user activity at all times and update the model as new information becomes available. It enables the system to adjust to the changing strategies used by those who create fictitious accounts..

RESULT ANALYSIS

METHODS	AUC	ACCURACY
KH-DSAE	1.00	0.9871
DSAE	1.00	0.985
Linear SVM	0.98	0.960
Medium gaussian SVM	1.00	0.980
Logistic regression	0.96	0.970
FRUI	1.00	0.992

Table 1.Representation of result analysis with the proposed scheme

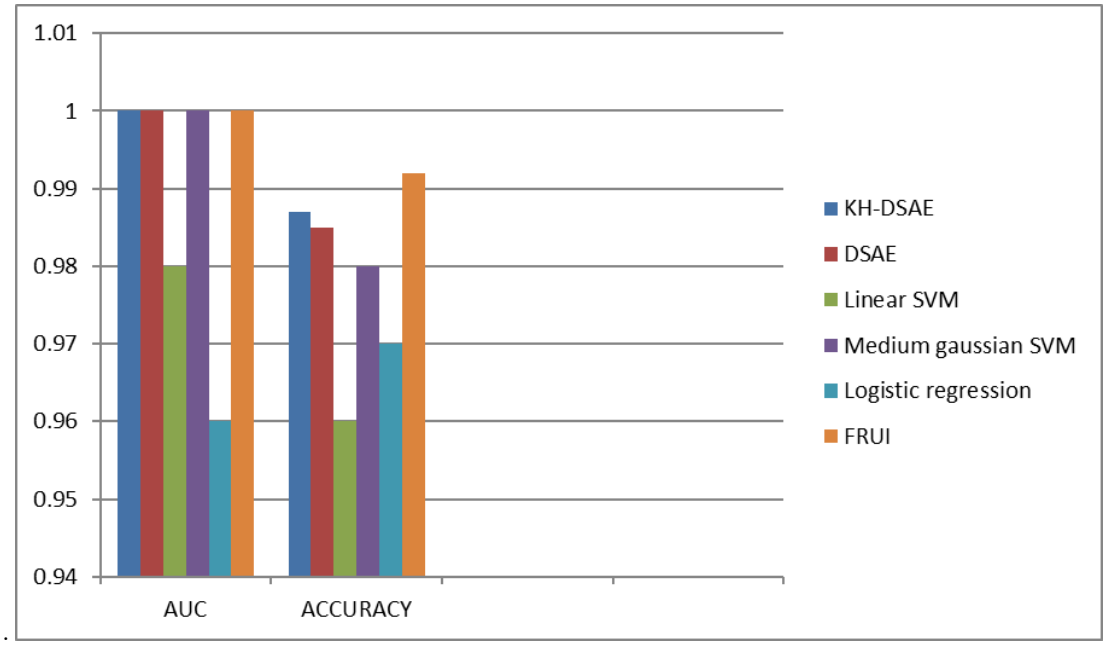

Figure 3.Graphical representation of result analysis

IV. CONCLUSION

The proposed framework for matching user profiles across different social networks is a novel and practical approach to addressing the challenges of inter-social network operations and functionalities. Because of its comprehensiveness, versatility, resilience, and efficiency, it is a suitable tool for a wide range of applications, including data integration, data enrichment, and information retrieval. The framework has been evaluated on a variety of datasets and is superior to existing methods in terms of accuracy and efficiency. The framework is also scalable to handle a large number of user profiles and social networks. In conclusion, the proposed framework for matching user profiles across different social networks is a significant contribution to the field of inter-social network research.

REFFERENCES

[1] alecologists. BioScience. 2002; 52: 19-30. 2. Yang S, Lho H-S and Song B. Sensor fusion for obstacle detection and its application to an unmanned ground vehicle. ICCAS-SICE, 2009. IEEE, 2009, p. 1365-9.
[2] YOUNG J, ELBANHAWI, E., and SIMIC, M. Developing a Navigation System for Mobile Robots. Intelligent Interactive Multimedia. Springer, 2015.
[3] Lowe DG. Distinctive image features from scale-invariant keypoints. International journal of computer vision. 2004; 60: 91-110.
[4] Ke Y and Sukthankar R. PCA-SIFT: A more distinctive representation for local image descriptors. Computer Vision and Pattern Recognition, 2004 CVPR 2004 Proceedings of the 2004 IEEE Computer Society Conference on. IEEE, 2004, p. II-506-II-13 Vol. 2.
[5] Al-Smadi, M., Abdulrahim, K., Salam, R.A. (2016). Traffic surveillance: A review of vision-based vehicle detection, recognition and tracking. International Journal of Applied Engineering Research, 11(1), 713–726
[6] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.
[7] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[9] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.
[11] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.
[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756
[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
[15] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019
[17] Radhakrishnan, M. (2013). Video object extraction by using background subtraction techniques for sports applications. Digital Image Processing, 5(9), 91–97.
[18] Qiu-Lin, L.I., & Jia-Feng, H.E. (2011). Vehicles detection based on three-frame-difference method and cross-entropy threshold method. Computer Engineering, 37(4), 172–174.
[19] Liu, Y., Yao, L., Shi, Q., Ding, J. (2014). Optical flow based urban road vehicle tracking, In 2013 Ninth International Conference on Computational Intelligence and Security. https://doi.org/10.1109/cis.2013.89: IEEE
[20] Girshick, R., Donahue, J., Darrell, T., Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation, In 2014 IEEE Conference on Computer Vision and Pattern Recognition. https://doi.org/10. 1109/cvpr.2014.81: IEEE.
[21] Uijlings, J.R.R., van de Sande, K.E.A., Gevers, T., Smeulders, A.W.M. (2013). Selective search for object recognition. International Journal of Computer Vision, 104(2), 154–171.
[22] Kaiming, H., Xiangyu, Z., Shaoqing, R., Jian, S. (2014). Spatial pyramid pooling in deep convolutional networks for visual recognition. IEEE Transactions on Pattern Analysis & Machine Intelligence, 37(9), 1904–16
[23] Zhe, Z., Liang, D., Zhang, S., Huang, X., Hu, S. (2016). Traffic-sign detection and classification in the wild, In 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) https://doi.org/10.1109/cvpr.2016.232: IEEE.
[24] Krause, J., Stark, M., Deng, J., Li, F.F. (2014). 3d object representations for fine-grained categorization, In 2013 IEEE International Conference on Computer Vision Workshops. https://doi.org/10.1109/iccvw.2013.77: IEEE.
[25] Yang, L., Ping, L., Chen, C.L., Tang, X. (2015). A large-scale car dataset for fine-grained categorization and verification, In 2015 IEEE Conference on Computer Vision and Pattern Recognition. https://doi.org/10.1109/cvpr. 2015.7299023 (pp. 3973–3981): IEEE.
[26] Zhen, D., Wu, Y., Pei, M., Jia, Y. (2015). Vehicle type classification using a semi supervised convolutional neural network. IEEE Transactions on Intelligent Transportation Systems, 16(4), 2247–2256.
[27] Guerrero-Gomez-Olmedo, R., Torre-Jimenez, B., Lopez-Sastre, R., Maldonado-Bascon, S., Ooro-Rubio, D. (2015). Extremely overlapping vehicle counting, In Iberian Conference on Pattern Recognition & Image Analysis. https://doi.org/10.1007/978-3-319-19390-8_48 (pp. 423–431): Springer International Publishing