e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

Fake Account Detection on Instagram

Shwetha V Bhat, Niveditha Niranjan Jain

Assistant Professor, Department of MCA, Mangalore Institute of Technology & Engineering College, Moodabidri, Karnataka, India

PG Student, Department of MCA, Mangalore Institute of Technology & Engineering College, Moodabidri, Karnataka, India

ABSTRACT: The meteoric rise of social media has led to a proliferation of fake accounts, which can be used for illicit purpose like identity theft, phishing, and the propagation of misinformation. To deal with the matter of the surge in fake social media accounts, researchers have explored a several machine learning methods and algorithms to identify and detect these fraudulent profiles. These advanced analytical methods aim to differentiate genuine user accounts from those created for malicious purposes. This study's objective is to assess the efficacy of three wellknown machine learning algorithms. - Support Vector Machines (SVM), Logistic Regression, Random Forest - in identifying fake accounts. The proposed approach demonstrated significant improvements in detection accuracy, achieving over 90% precision and recall. The study analyzed user metadata, engagement patterns, and content similarity features to classify accounts as authentic or fake. Random Forest attained the maximum precision of up to 91.76% in a 2class (authentic vs fake) and 4-class (authentic, active fake, inactive fake, spammer) classification. The five key components were number of posts, followers, biography length, following, and link availability. Descriptive statistics revealed notable differences in user behavior between fake and authentic accounts. Leveraging machine learning and NLP techniques can substantially increase the false profile's accuracy identification compared to traditional methods. The findings highlight the efficacy of sophisticated algorithms for machine learning, particularly Random Forest, in detecting fake accounts with high precision by analyzing user metadata, engagement, and content features. This can help social networks and businesses mitigate the effect of fake accounts used for malicious purposes.

KEYWORDS: Machine Learning (ML), Support Vector Machine (SVM), Logistic regression

I.INTRODUCTION

The rampant proliferation of fake accounts on social media platforms, has become a pressing issue in recent times. These fake accounts can have serious negative impacts, including identity theft, phishing attacks, the dissemination of false or misleading information has become a growing concern in the digital age, and the manipulation of engagement metrics for brands and influencers. With estimates of over 1.7 billion fake accounts throughout social media networks, the necessity for robust and trustworthy detection techniques has grown more crucial and urgent.

Precise identification of fraudulent accounts is vital for preserving a trustworthy and secure digital atmosphere for social media users. However, manually identifying these accounts is a time-consuming and resource-intensive process that is not scalable for the sheer volume of fraudulent accounts on platforms such as Instagram has changed into a significant challenge. ML algorithms in this particular context can serve as a pivotal tool in bolstering detection capabilities and strengthening the overall security of social networks. Many ML algorithms have demonstrated encouraging outcomes in identifying and flagging fraudulent accounts on social media networks. SVM have been employed to classify and identify malicious applications on Facebook, attaining impressive accuracy levels in the process. Logistic regression, when integrated with techniques like median imputation and maximum probability approximation, has also demonstrated strong performance in detecting fake accounts on Instagram, with an accuracy rate of 90.8%.Random Forest, a ML algorithm, has grown to be among the most often used strategies in order to identify and identifying fake accounts on social media platforms., has achieved even higher accuracy rates of up to 92.5% when used with k-fold cross-validation.

Additionally, leveraging these algorithms can improve the identification of fake accounts by analyzing the quantity of fans and accounts followed. SVM techniques can indeed be valuable for feature extraction, selection, and data preparation in fake account detection. Logistic regression is also useful for assessing the profile completeness, presence of a bio, profile picture, account age, and verification status, as these can be indicative features for identifying fake accounts. Combining these approaches can enhance the robustness and precision of the detection mechanism.

The expected outcomes of this research include increased accuracy in fake account detection, reduced instances of fraudulent activities, and a combination of SVM techniques, logistic regression not only increases precision of fake account detection but also contributes to creating an online setting that is more secure for Instagram users. By implementing these machine learning algorithms, the research aims to offer a scalable and efficient resolution to the increasing issue of fake accounts on social media platforms.

II. RELATED WORK

The identification of fake accounts on Instagram, worked as significant challenge in recent years. Multiple studies have applied a range of ML techniques to recognise and categorize fraudulent accounts. One study, in particular, employed a image detection and NLP to detect fake accounts on Instagram, achieving high accuracy. Another study utilized Naive Bayes, Multilayer Perceptron, Naive Bayes, J48 Decision Tree to identify fake Instagram profiles.

Using ML techniques has demonstrated effective in detecting patterns and anomalies that indicate fake accounts. For instance, a study used SVM and neural networks to identify fake accounts on Twitter, achieving accuracy of 93.9%. Another study employed Random Forest, SVM to identify fake accounts on Instagram, using features such as user behavior, account attributes, and content trends. Additionally, studies have explored the usage of deep learning techniques, such as convolutional neural networks, to detect fake accounts on social media platforms. Detecting fake accounts on Insta is a task that requires integrating different machine learning methods and techniques. A study utilized logistic regression and a contemporary metaheuristic method to detect fake accounts on Twitter, achieving a precision of 86%. Another study proposed a fresh strategy to fake news and fake account detection in OSNs using user social engagement and visual content-centric models.

Detecting fake accounts on Instagram is difficult for maintaining the integrity and security of the platform. Fake accounts utilised to spread misinformation, engage in spamming activities, and compromise user data. Thus, creating efficient algorithms and methods for identifying fake accounts is vital to guaranteeing users' safety and security on social media platforms.

III.METHODOLOGY

The goal of the project is to develop a programme that recognises phoney Instagram accounts using ML algorithms. To ascertain the most accurate model for fraudulent account identification, the study will compare the execution of SVM, Random Forest, and Logistic Regression.

The primary steps in the methodology are:

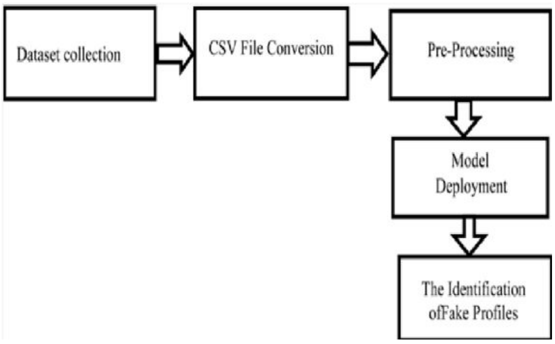


Fig 1. Data Flow Diagram

1. Data Collection

Gather user profile information, activity metrics, and social network features from Instagram, such as number of posts, followers, followings, engagement metrics, profile completeness, posting frequency, and account age. Manually label a of accounts as real or fake to create a training dataset.

2. Data Pre-processing

Clean the data by removing or correcting inaccuracies, engineer new features that help distinguish real from fake accounts, and normalize the data to ensure all features contribute equally.

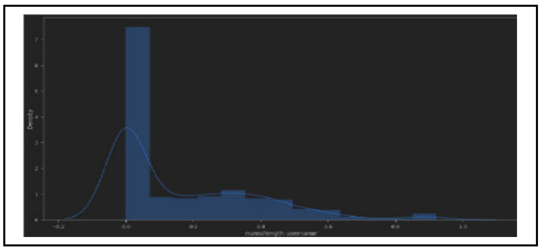


Fig 2. Data Analysis

3. Feature Selection

Correlation analysis is useful for locating and eliminate features that are redundant, and PCA able to be employed for minimise dimensionality while keeping the majority of variance.

4. Model Training

Train the Random Forest, SVM, Logistic Regression models using the Pre-processed data:

4.1 SVM: Find the optimal hyperplane that separates real and fake accounts with maximum margin using kernel tricks to handle non-linearity. Formula:

$$\min_{\mathbf{w},b} \frac{1}{2}\|\mathbf{w}\|^2 \quad \text{subject to} \quad y_i(\mathbf{w}\cdot\mathbf{x}_i + b) \geq 1 \quad \forall i$$

4.2 Logistic Regression: Estimate the probability of an account being fake using a sigmoid function and optimize the cost function via gradient descent. Formula:

$$P(y=1|\mathbf{x}) = \frac{1}{1+e^{-(\mathbf{w}\cdot\mathbf{x}+b)}}$$

4.3 Random Forest: Use an ensemble of decision trees trained on bootstrapped samples, aggregating predictions via majority voting. Formula:

$$\hat{f}(x) = \frac{1}{M}\sum_{m=1}^{M} h_m(x)$$

where $h_m(x)$ is the prediction of the m-th tree, and M is the total number of trees

5. Model Evaluation

- **Metrics:** AUC-ROC, Precision, Recall, Accuracy, F1-score
- **Cross-Validation:** Use k-fold cross-validation to evaluate the models' generalizability.
- **Confusion Matrix:** Analyze genuine negatives, erroneous positives, authentic positives, and artificial negatives

6. Comparison and Selection:

The research aims to develop an accurate and robust fake account detection system for Instagram by contrasting the performance metrics of algorithms and selecting the model for ultimate deployment with the best overall performance.

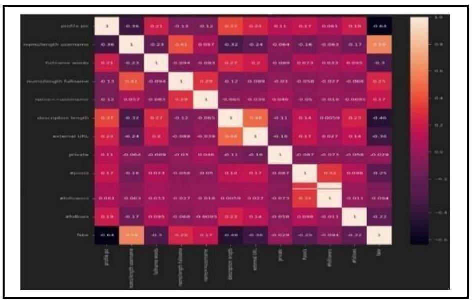


Fig 3. Comparison of Features

IV.PROPOSED WORK

This study aims to build a robust and effective machine learning-based approach for detecting fake accounts on Instagram, a popular social media platform. The researchers plan to leverage three powerful algorithms - logistic regression, random forest, SVM- to tackle this important challenge. The initial phase of this investigation process will be to collect a comprehensive dataset from Instagram, utilizing publicly available APIs and web scraping techniques. This dataset will form the foundation for the study, and the researchers will meticulously identify and label both fake and real accounts through a blend of manual inspection and classification based on various account attributes, such as profile information, following counts, and status counts.

With the dataset in hand, the researchers will then concentrate on the crucial task of feature engineering, which to be capable of improving performance, in choosing and altering the most relevant attributes of the models for machine learning. They will meticulously choose the most significant features from the gathered data, including account metadata, user activities, and posting behavior, to improve the precision of the models. These features will then be engineered to get meaningful patterns and traits that can successfully differentiate fake accounts from their legitimate counterparts. This feature engineering process is anticipated to be crucial for the success of ML models.

The proposed work will then implement and assess the performance of the 3 systems- to determine their effectiveness in detecting fake accounts on Instagram. The logistic regression model will be utilized to classify accounts as either fake or real based on the engineered features, while the random forest model will be utilised to determine intricate patterns within the information that can differentiate fake accounts from real ones. The SVM model, however, will utilize the engineered features and their relationships to classify the accounts.

These methods will help the researchers optimize the elevated parameters of each model and evaluate each model's capacity for generalisation, correspondingly.

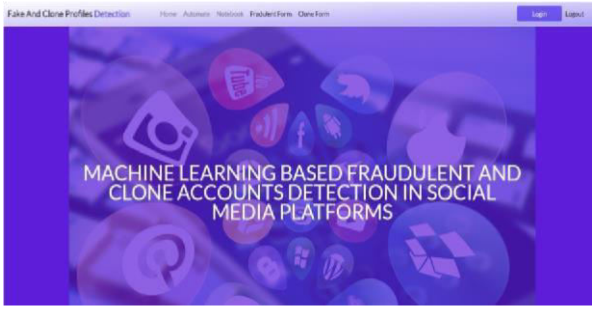
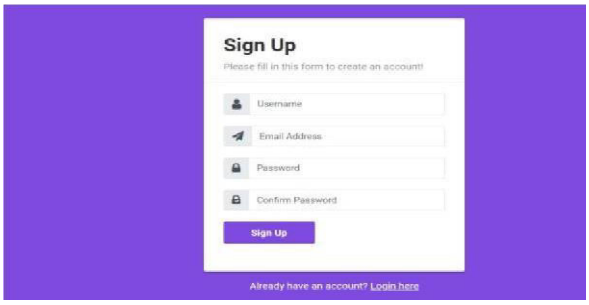

Fake And Clone Profiles Detection
Home
Admin
Notebook
Fradulent Form
Clone Form
Login
Logout
MACHINE LEARNING BASED FRAUDULENT AND CLONE ACCOUNTS DETECTION IN SOCIAL MEDIA PLATFORMS

Fig 4. Home Page


Sign Up

Please fill in this form to create an account!

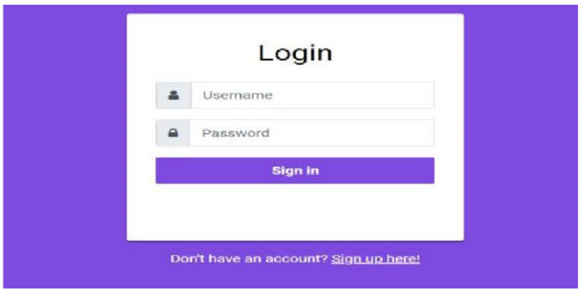
Already have an account? Login here

Fig 5. Sign Up Page

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707053 |



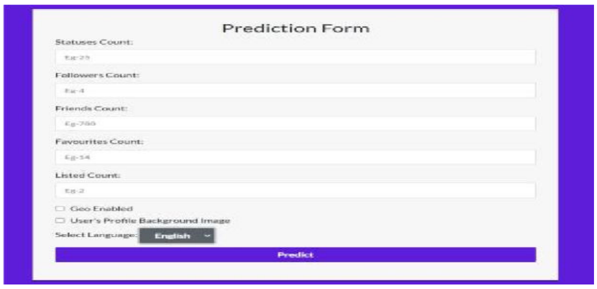
Login

Username

Password

Don't have an account? Sign up here!

Fig 6. Login Page



Prediction Form

Statuses Count: Eg-23

Followers Count: Eg-4

Friends Count: Eg-700

Favourites Count: Eg-14

Listed Count: Eg-2

□ Geo Enabled

□ User's Profile Background Image

Select Language: English

Fig 7. Prediction Page

V.CONCLUSION

On Instagram, machine learning methods such as Random Forest, Logistic Regression, SVM have demonstrated promise in spotting fraudulent accounts. These algorithms can classify accounts as real or fake according to several features such as user metadata, posting patterns, and engagement metrics. Research has demonstrated that the precision of several algorithms for ML in this task varies with these algorithms generally performing better in certain cases.

The choice of algorithm ultimately relies on the application's particular requirements moreover the calibre of the prepared data. Fake account detection on Instagram is a crucial task for maintaining the integrity of social network platforms and preventing cybercrimes like identity theft and phishing. With the usage of ML methods, fake accounts can be identified and removed, reducing the danger of these malicious activities. Furthermore, the identification of fake accounts has important ramifications for people, companies, and social network platforms. Social media companies may enhance user experience and lower the potential for cybercrimes through the integration of ML algorithms into their systems to more effectively detect and remove fraudulent accounts.

Future research in this area should focus on improving the scalability and efficacy of models for detecting fraudulent accounts. This can be gained by incorporating additional features, such as image recognition and NLP, and by developing more robust and adaptable algorithms. Incorporating cutting-edge machine learning methods, like Gradient Boosting Classifiers, can greatly improve social media networks' capacity to find and eliminate fake accounts, thereby fostering a more secure and safe online community. Overall, the research on fake account detection on Instagram using ML method has demonstrated encouraging outcomes, with the capacity to significantly affect social media networks' security and integrity. As the issue of fraudulent accounts keeps developing, the creation of increasingly complex and potent detection techniques will be essential to preserving these platforms' legitimacy and confidence.

REFERENCES

1. Meshram, P., Bhambulkar, R., Pokale, P., Kharbikar, K., and Awachat, A. "Automatic Detection of Fake Profile Using Machine Learning on Instagram." International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 8, 2021, pp. 1-6. DOI: 10.17577/IJERTV10IS080001.
2. Roy, P.K. and Chahar, S. "Fake Profile Detection on Social Networking Websites: A Comprehensive Review." IEEE Transactions on Artificial Intelligence, vol. 1, 2020, pp. 271-285. DOI: 10.1109/TAI.2020.3024181.
3. Van der Walt, E. and Eloff, J.H.P. "Using Machine Learning to Detect Fake Identities: Bots vs Humans." IEEE Access, vol. 6, 2018, pp. 65406549. DOI: 10.1109/ACCESS.2018.2806699.
4. Meshram, P., Bhambulkar, R., Pokale, P., Kharbikar, K., and Awachat, A. "Survey Paper on Automatic Detection of Fake Profile Using Machine Learning on Instagram." International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 8, 2021, pp. 1-6. DOI: 10.17577/IJERTV10IS080002.
5. Van der Walt, E. and Eloff, J.H.P. "Using Machine Learning to Detect Fake Identities: Bots vs Humans." IEEE Access, vol. 6, 2018, pp. 65406549. DOI: 10.1109/ACCESS.2018.2806699.
6. Tiwari, V. "Analysis and detection of fake profile over social media." 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 1191-1195. DOI: 0.1109/CCAA.2017.8230015.
7. Akyon, F.C. and Kalfaoglu, M.E. "Instagram Fake and Automated Account Detection." 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 1305-1309. DOI: 10.1109/ICCC47050.2019.9064292

8. Yadav, A., Kumari, R., and Sharma, R. "INSTAGRAM FAKE PROFILE DETECTION - A REVIEW." International Journal of Novel Research and Development, vol. 8, no. 7, 2023, pp. d17-d18. DOI: 10.55662/IJNRD.2307303.
9. Masood, F., Ammad, G., Almogren, A., Abbas, A., Khattak, H.A., Din, I.U., Guizani, M., and Zuair, M. "Spammer Detection and Fake User Identification on Social Networks." IEEE Access, vol. 8, 2020, pp. 213845-213867. DOI: 10.1109/ACCESS.2020.3040448.
10. Dey, A., Reddy, H., Dey, M., and Sinha, N. "Detection of Fake Accounts in Instagram Using Machine Learning." International Journal of Computer Science & Information Technology (IJCSIT), vol. 11, no. 5, 2019, pp. 83-92. DOI: 10.5121/ijcsit.2019.11507.
11. Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., and Tesconi, M. "The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race." Proceedings of the 26th International Conference on World Wide Web Companion, 2017, pp. 963-972. DOI: 10.1145/3041021.3055135.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com