WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# DETECTING FAKE PROFILES ON SOCIAL NETWORKING WEBSITES USING MACHINE LEARNING

***[1]Logapriya V [2]Anita Sofia V S***

[1]Student, Department of Computer Applications (PG), PSG College of Arts and Science, Coimbatore.
[2]Associate Professor, Department of Computer Applications (PG), PSG College of Arts and Science, Coimbatore.

**ABSTRACT**

Social media is a vital part of everyday life, since most people use it on a regular basis across a range of platforms. These platforms have many advantages, but they also have certain disadvantages, such as security threats involving personal data. Identifying possible dangers on social media, which necessitates differentiating between authentic and fraudulent profiles, is one of the main issues in maintaining security. Several conventional techniques have been used to identify fake social media profiles, however they frequently fall short in terms of precision and effectiveness. Security issues persist because many platforms still have trouble identifying fake accounts. By using high-gradient boosting algorithms and timestamp data types, this study seeks to improve the detection accuracy of fake accounts. This study investigates several advanced machine learning models to enhance detection capabilities by examining the interaction between several machine learning approaches and multi-feature time series data. In order to provide a more safe and trustworthy social media environment, the suggested method aims to maximise the accuracy of detecting fake accounts.

**Keywords:** Fake Profile Detection, accuracy, Machine Learning Algorithm, Random Forest Classifer, Real Account or Fake Account.

## 1. INTRODUCTION

The challenges of identifying fake accounts on social media sites like Instagram has grown crucial in a time when social media has become a vital part of our lives. To address this issue, the project "Instagram Fake Account Detection using Machine Learning" uses Python as its main tool. To accomplish this, it makes use of the Random Forest Classifier, an effective machine learning technique. The Random Forest Classifier performs very effectively, achieving 100% accuracy on the trained data and an astounding 93% accuracy on the test data. There are 576 records in the dataset used for this research, and each record has 12 unique attributes. These attributes incorporate key components of Instagram profiles, such as the nearness of a profile picture, the extent of numeric characters in usernames, the breakdown of full names into word tokens, the extent of numeric characters in full names, the uniformity of full names and usernames, the length of client bios, the nearness of outside URLs, the protection status of accounts, the amount of posts, the number of adherents, the number of accounts taken after, and the last assignment of an account as "Fake" or "Real". This project aims to offer a reliable and effective method for identifying fake Instagram accounts by utilising Python's capabilities and these cutting-edge machine learning models. By doing this, it helps to maintain both the platform's integrity and its users' security.

## 2. LITERATURE SURVEY

Nguyen and Li (2020) provide a hybrid machine learning-based fake profile detection system that blends graph-based, behavior-based, and content-based techniques. The method increases accuracy and decreases false positives by examining network topologies, user behaviour, and text content collectively. Their ensemble learning methodology surpasses single-method solutions when tested on a social media dataset, proving the efficacy of hybrid detection methodologies.

Using social network analytics, Kumar and Patel (2021) provide a real-time approach for detecting false profiles. It analyses user interactions, including friend requests and activity levels, using anomaly detection and clustering techniques like DBSCAN. Accurate detection is improved via machine learning-based predictive analysis, real-time monitoring, and a user feedback system. Their study highlights the benefits of combining machine learning with real-time analytics to produce a trustworthy detection system.

In their analysis of phoney profile detection techniques, Smith and Brown (2020) divide them into three categories: content-based, behavior-based, and graph-based. Graph-based techniques examine social network architecture, behavior-based techniques monitor user activity patterns, and content-based techniques utilise natural language processing (NLP) to identify irregularities in posts. They point out the advantages and disadvantages of each strategy, pointing out that hybrid approaches produce superior outcomes but demand a lot of processing power and big data sets.

## 3. PROPOSED SYSTEM

A Python-based Instagram fake profile detection system uses the Random Forest Classifier for accurate classification. Leveraging Python's machine learning libraries, it analyzes 576 profiles with 12 features to distinguish real and fake accounts. The model enhances accuracy, integrates feature engineering, and improves efficiency, ensuring a safer Instagram platform.

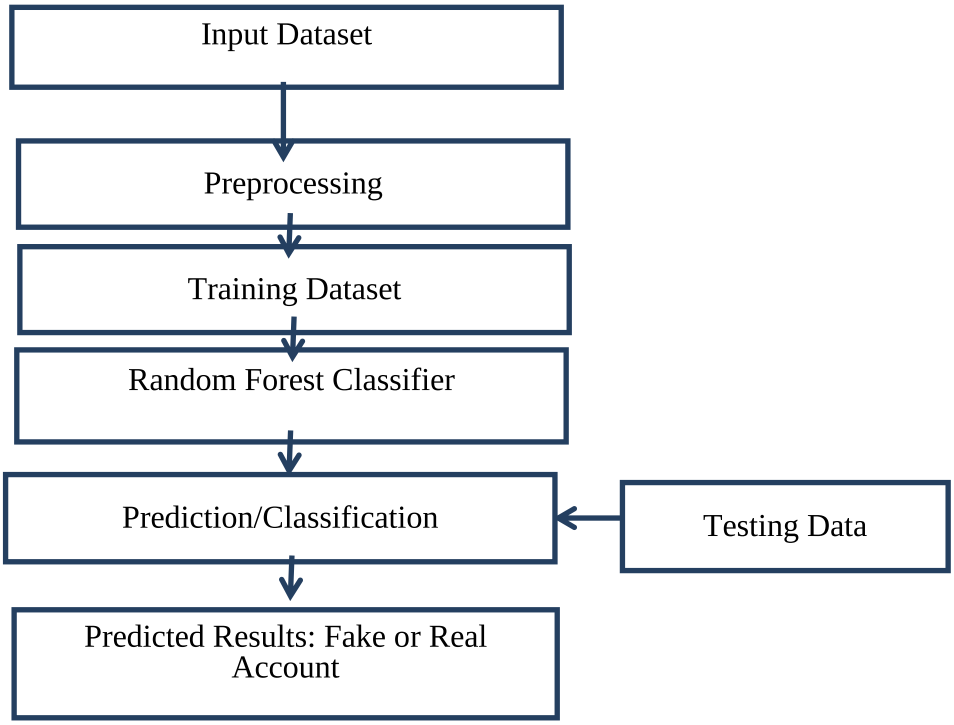

**Fig 1: System Flow Diagram of the proposed system**

## 4. IMPLEMENTATION

### *Data Collection*

A key component of machine learning, data gathering is the subject of the first module of Fake Profile Detection. Methods such as web scraping and physical interventions are used to gather data. The dataset is stored in the project file for processing. It originates from the popular Kaggle research database. Information from Instagram accounts is part of the study's dataset.

### *Dataset*

There are 576 distinct information elements in the dataset. Profile picture, Username length, Fullname words, fullname length, Name==username, Description length, External URL, Private, Posts, Followers, Follows, Fake are the 12 columns that make up the dataset.

### *Data Preparation*

Addressing missing information, eliminating replicas, fixing mistakes, normalizing, and converting types of information are all included in data cleaning. Remove order effects to guarantee learning that is impartial. It depicts Conduct exploratory analysis, identify class imbalances, and identify correlations. Additionally, it separates data for model construction into instruction and evaluation groups.

### *Model Selection*

The machine learning algorithm Random Forest Classifier was implemented after achieving 100% accuracy on the training set.

### *Analyze and Predict*

Only 11 features were selected from the original dataset: Profile picture, Username length, Fullname words, fullname length, Name==username, Description length, External URL, Private, Posts, Followers, Fake

### *Accuracy on test set*

The accuracy of the model is evaluated on the test set after training and validation. The significant performance indicator, test accuracy, is 93%.

### *Saving the Trained Model:*

Once the model has been trained and tested, use Pickle to save it as a.pkl file. After installing Pickle if necessary, import the model and dump it into a.pkl file for distribution.

## 5. RESULTS AND DISCUSSION

Detecting mistakes and ensuring that software systems fulfil user expectations and requirements without experiencing unacceptable failures are the goals of testing. Testing looks for every possible defect or weakness in an output to ensure that parts, sub-assemblies, assemblies, and finished products all operate as intended. Unit testing, functional testing, acceptance testing, and integration testing are some of the test kinds that handle particular testing requirements. A unit test focuses on confirming basic algorithmic logic and ensuring that application inputs produce valid results, whereas testing for functionality systematically demonstrates that functionalities are available as stated by company and needs for technology. User acceptability test, which necessitates substantial end-user participation, is essential for verifying that the system satisfies functional requirements. Integration testing ensures that different software modules or components interact correctly and that the process entire meets all of its requirements. Combining these testing techniques results in software testing that offers thorough confirmation that all distinct business process paths operate as intended, that recognised inputs and outputs are managed appropriately, and that interacting systems or processes operate as intended.

## 6. CONCLUSION

The "Instagram Fake Account Detection using Machine Learning" project offers a practical way to differentiate between real and fake profiles. It was created in Python using the Random Forest Classifier and uses a dataset of 576 profiles with 12 important attributes to achieve a 93% test accuracy. While reducing false positives, robust feature engineering, algorithm diversity, and adaptability improve detection accuracy. This method effectively detects fake accounts, enhancing Instagram's security and credibility.

## 7. SCOPE FOR FUTURE ENHANCEMENTS

Future efforts for Instagram Fake Profile Detection using Machine Learning will involve enhanced feature creation to adjust to emerging dangers and ongoing training of models with frequent retrain. Emotion and time analysis are examples of modern analysis of behavior that can improve individual identity verification. The methodology will be enhanced even more by integrating comprehensive analysis of information to identify fakes, edited visuals, and misleading material. Finding synchronized unauthentic activity can be aided by the analysis of trends in interaction. Faster reaction to risks will be made possible by continuous tracking abilities, reliability and confidentiality of users can be managed with information-preserving strategies like supervised learning. Higher analyses can be obtained through API interaction with Instagram, and performance enhancements will guarantee that the software can manage growing information quantities. Furthermore, the public's understanding can be increased through educational programs, and in order to reduce inequalities and comply with privacy laws, legal as well as ethical requirements must be given top priority.

## 8. REFERENCES

[1] Buket Erşahin, Özlem Aktaş, D. Kılınç and C. Akyol, "Twitter fake account detection," 2017International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 2017.

[2] Georgios Kontaxis, I. Polakis, S. Ioannidis and E. P. Markatos, "Detecting social network profilecloning,"2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Seattle, WA, USA, 2011, pp. 295-300, doi: 10.1109/PERCOMW.2011.5766886.

[3] Monther Aldwairi, and Ali Alwahedi, “Detecting Fake News in Social Media Networks”, Procedia Computer Science, Volume 141, 2018, Pages 215-222; ttps://doi.org/10.1016/j.procs.2018.10.171.

[4] E. Karunakar, V. D. R. Pavani, T. N. I. Priya, M. V. Sri, and K. Tiruvalluru, “Ensemble fake profile detection using machine learning (ML),” J. Inf. Comput. Sci., vol. 10, pp. 1071–1077, 2020.

[5] P. Wanda and H. J. Jie, “Deep profile: utilising dynamic search to identify phoney profiles in online social networks CNN” J. Inf. Secur. Appl., vol. 52, pp. 1–13, 2020.

[6] P. K. Roy, J. P. Singh, and S. Banerjee, “Deep learning to filter SMS spam,” Future Gener. Comput. Syst.,vol. 102, pp. 524–533, 2020.

[7] R. Kaur, S. Singh, and H. Kumar, “A modern overview of several countermeasures for the riseof spam and compromised accounts in online social networks,” J. Netw. Comput. Appl., vol. 112, pp. 53–88, 2018.
[8] G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty,“Automatically dismantling online dating fraud,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1128–1137, 2020.
[9] M. U. S. Khan, M. Ali, A. Abbas, S. U. Khan, and A. Y. Zomaya, “Segregating spammers andunsolicited bloggers from genuine experts on twitter,” IEEE Trans. Dependable Secure Comput., vol. 15, no. 4, pp. 551–560,Jul./Aug. 2018.
[10] V. Balakrishnan, S. Khan, and H. R. Arabnia, “Improving cyberbullying detection using twitterusers’psychological features and machine learning,” Comput. Secur., vol. 90, 2020, Art. no. 101710.