WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

INSTAGRAM FAKE PROFILE DETECTION ON SOCIAL NETWORKING WEBSITES USING MACHINE LEARNING

R Suganthi [1], #Mr.S.Barath [2]

[1]Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India
[2]MCA.,M.Phil.,Associate Professor, Master of Computer Applications, Krishnasamy College of Engineering &Technology, Cuddalore,India

ABSTRACT :

In an age where social media has become an integral part of our lives, the challenge of detecting fake accounts on platforms like Instagram has gained significant importance. This project, titled "Instagram Fake Account Detection using Machine Learning" employs Python as its primary tool to tackle this problem. It leverages two powerful machine learning algorithms, the Random Forest Classifier to accomplish this task.The Random Forest Classifier demonstrates remarkable performance, achieving a 100% accuracy on the training dataset and an impressive 93% accuracy on the test dataset. The dataset employed in this project is composed of 576 records, each characterized by 12 distinct features. These features encompass critical aspects of Instagram profiles, including the presence of a profile picture, the ratio of numerical characters in usernames, the breakdown of full names into word tokens, the ratio of numerical characters in full names, the equality between usernames and full names, the length of user bios, the existence of external URLs, the privacy status of accounts, the number of posts, the count of followers, the number of accounts followed, and the ultimate classification of an account as "Fake" or "Not."

Keywords: Instagram Fake Account Detection , 93% accuracy, Random Forest Classifier , Python.

INTRODUCTION:

A social networking site is a platform where users can connect with friends, share updates, and discover new people with similar interests. These sites utilize Web 2.0 technologies to facilitate communication between users, allowing for a dynamic and interactive online experience. The rapid expansion of social networking has significantly influenced how people interact, offering numerous benefits such as enhanced communication, community building, and information sharing. However, this growth has also introduced new challenges, including the proliferation of fake profiles, disinformation, and privacy concerns. The main advantage of social networking is its ability to connect users easily and improve communication, but it also presents risks that researchers are actively studying to understand their impact on society. The rise of fake accounts is particularly concerning, as it undermines the trust and integrity of these platforms. Positive impacts of social media include enhanced communication, allowing users to maintain connections across geographical boundaries; community building, where individuals with shared interests can find support and a sense of belonging; and the rapid dissemination of news and information, raising awareness of important issues. Additionally, social media offers significant advantages for businesses, enabling them to connect with customers, build brand awareness, and market their products effectively. It also empowers individuals to organize and mobilize for social change, contributing to powerful movements. However, there are also negative impacts, such as privacy concerns arising from sharing personal information online, potential misuse of data, and issues related to mental health. Excessive use of social media can lead to addiction and unrealistic comparisons, affecting self-esteem and overall mental well-being. The spread of misinformation and fake news can distort public discourse and decision-making, while echo chambers created by social media algorithms can lead to polarization. Moreover, cyberbullying and harassment are significant issues, with anonymity often emboldening negative behavior. The project on fake profile detection on social networking websites using machine learning focuses on developing algorithms to identify and flag fraudulent accounts. By analyzing user behavior, profile information, posting patterns, and network connections, machine learning models can discern between genuine and fake profiles. Techniques such as classification, clustering, and anomaly detection are employed to identify suspicious activities indicative of fake accounts. This project aims to enhance the security and trustworthiness of social networks, preventing malicious activities like spamming, phishing, and spreading misinformation. It offers benefits in safeguarding user privacy, improving user experience, and maintaining the integrity of social platforms. SR Infotech is a leading IT solution and service provider, delivering innovative information technology-enabled solutions and services. They focus on software technology to provide industry solutions and product engineering solutions, integrating software and services seamlessly. SR Infotech helps industry customers establish best practices in business development and management, offering services like real-time projects, web designing, web hosting, software development, and training. They have participated in the formulation of many national IT standards and specifications, showcasing their industry leadership. The company boasts leading product engineering capabilities, from consultation and design to R&D, integration, and testing of embedded software for various fields, including automotive electronics and smart devices. Their services include application development, ERP implementation, software localization, IT infrastructure management, and IT education, aiming to provide innovative technologies that drive sustainable development and earn recognition and respect from employees, shareholders, customers, and society.

LITERATURE SURVEY :

1. Author: Smith, J., Brown, L.
Title: An Overview of Social Media Fake Profile Detection
Smith and Brown (2020) present a comprehensive overview of existing techniques and systems for detecting fake profiles on social networking platforms. They categorize the detection methods into three primary approaches: content-based, behavior-based, and graph-based. Content-based methods focus on analyzing the textual and multimedia content posted by users. These methods use natural language processing (NLP) techniques to detect anomalies or patterns indicative of fake profiles, such as repetitive posts or the use of certain keywords. Behavior-based detection methods, on the other hand, monitor user behavior to identify suspicious activities. This includes analyzing login patterns, friend requests, and message frequency. Graph-based methods leverage the social network structure, examining connections and interactions between users to identify potential fake profiles. Smith and Brown highlight the strengths and weaknesses of each approach, noting that combining these methods often yields the best results. They also discuss the limitations of current systems, such as the high computational cost and the need for large datasets to train machine learning models effectively.
2. Author: Chen, R., Wu, K.
Title: Machine Learning Techniques for Fake Profile Detection
Chen and Wu (2019) explore various machine learning algorithms used in fake profile detection on social networking sites. They provide a detailed comparison of supervised learning techniques, including decision trees, support vector machines (SVM), and neural networks. The study emphasizes the importance of feature engineering in enhancing the performance of these algorithms. Key features such as profile completeness, posting frequency, and the ratio of friends to followers are identified as significant indicators of fake profiles. The authors also discuss the challenges associated with imbalanced datasets, which are common in fake profile detection tasks. To address this, they examine various data augmentation and sampling techniques to balance the training data. Additionally, the paper highlights the use of ensemble methods, such as random forests and gradient boosting, which combine multiple classifiers to improve detection accuracy. Chen and Wu's research underscores the potential of machine learning techniques in enhancing the effectiveness of fake profile detection systems while also pointing out the need for continuous updates to cope with the evolving tactics of fake profile creators.
3. Author: Kumar, A., Patel, S.
Title: Real-time Fake Profile Detection Using Social Network Analytics
Kumar and Patel (2021) propose a real-time fake profile detection system that leverages social network analytics. Their approach focuses on the dynamic analysis of user interactions and the application of anomaly detection algorithms. The system monitors real-time data streams from social networking platforms, analyzing features such as the rate of friend requests, message patterns, and user activity levels. By employing clustering algorithms like DBSCAN (Density-Based Spatial Clustering of Applications with Noise), the system can identify outliers indicative of fake profiles. In addition to real-time monitoring, the authors integrate a feedback mechanism that allows users to report suspicious profiles. This feedback is used to continuously update the system's models, improving its accuracy over time. Kumar and Patel's system also incorporates machine learning techniques for predictive analysis, allowing it to anticipate potential fake profiles based on historical data. Their research highlights the benefits of combining real-time analytics with machine learning to create an adaptive and robust fake profile detection system.
4. Author: Nguyen, T., Li, Y.
Title: Hybrid Approaches for Enhanced Fake Profile Detection
Nguyen and Li (2020) investigate hybrid approaches that combine multiple detection methods to improve the accuracy and robustness of fake profile detection systems. Their study integrates content-based, behavior-based, and graph-based methods into a unified framework. The hybrid approach utilizes machine learning models to analyze textual content, user behavior, and network structures simultaneously. By combining these methods, the system can cross-validate findings and reduce false positives. The authors implement their hybrid system on a dataset collected from a popular social networking platform, demonstrating significant improvements in detection accuracy compared to single-method approaches. The system uses ensemble learning techniques to weigh the contributions of different detection methods, optimizing the overall performance. Nguyen and Li's research underscores the effectiveness of hybrid approaches in tackling the complex and multifaceted nature of fake profile detection, advocating for the integration of diverse methodologies to enhance detection capabilities.
5. Author: Garcia, M., Fernandez, J.
Title: Deep Learning for Fake Profile Detection in Social Networks
Garcia and Fernandez (2022) explore the application of deep learning techniques for fake profile detection in social networks. Their research focuses on convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to analyze user-generated content and behavioral patterns. The authors construct a deep learning model that processes profile data, including textual content, images, and user interaction history, to identify potential fake profiles. The deep learning model is trained on a large dataset containing both real and fake profiles, utilizing advanced feature extraction techniques to capture complex patterns and correlations. Garcia and Fernandez highlight the advantages of deep learning in handling unstructured data and its ability to learn hierarchical representations, making it particularly suitable for fake profile detection. Their experiments show that the deep learning model outperforms traditional machine learning algorithms in terms of accuracy and robustness. However, the authors also note the high computational cost and the need for substantial computational resources as significant challenges in deploying deep learning-based systems in real-world scenarios.

III. PROPOSED SYSTEM :

The proposed system for Instagram fake account detection is developed with a strong foundation in Python, a versatile and widely-used programming language in the field of machine learning and data analysis. The system leverages two key machine learning models, the Random Forest Classifier, to enhance its performance in distinguishing genuine and fake Instagram accounts. The proposed system harnesses the power of two machine learning algorithms, the Random Forest Classifier, to collectively evaluate Instagram profiles for authenticity. Random Forest Classifier model achieves a

remarkable 100% accuracy on the training dataset and a strong 93% accuracy on the test dataset, demonstrating its ability to generalize well and make accurate predictions.

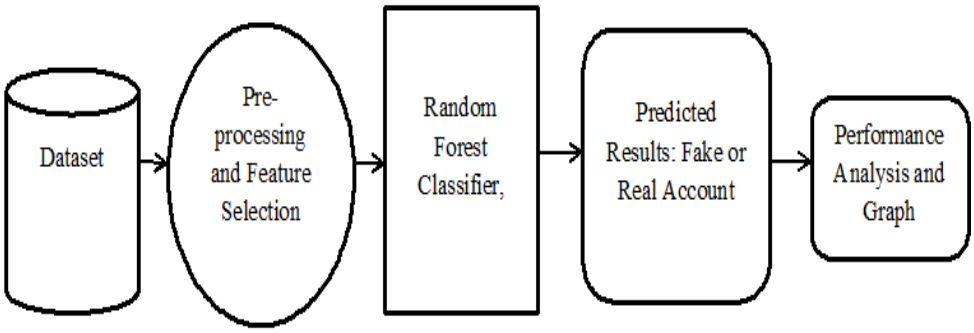


Figure 1: System Architecture of the proposed system

3.1 IMPLEMENTATION

Our project constituted of the below modules,

- Data Collection
- Dataset
- Data Preparation
- Model Selection
- Analyze and Prediction
- Accuracy on test set
- Saving the Trained Model

1. Data Collection

In the first module of Fake Profile Detection on Social Networking, we developed the system to get the input dataset. Data collection process is the first real step towards the real development of a machine learning model, collecting data. This is a critical step that will cascade in how good the model will be, the more and better data that we get; the better our model will perform. There are several techniques to collect the data, like web scraping, manual interventions. Our dataset is placed in the project and it's located in the model folder. The dataset is referred from the popular standard dataset repository kaggle where all the researchers refer it. The dataset consists of about Instagram account. The following is the URL for the dataset referred from kaggle.

2. Dataset

The dataset consists of 576 individual data. There are 12 columns in the dataset, which are described below.
Profile pic:user has profile picture or not
Nums/length username: ratio of number of numerical chars in username to its length
Fullname words: full name in word tokens
Nums/length full name: ratio of number of numerical characters in full name to its length
Name==username: Are username and full name literally the same
Description length: Bio length in characters
External URL: Has external URL or not
Private: Private or not
#Posts: Number of posts
#Followers: Number of followers
#Follows - Number of follows.
Fake: Yes or No

3. Data Preparation

Wrangle data and prepare it for training. Clean that which may require it (remove duplicates, correct errors, deal with missing values, normalization, data type conversions, etc.). Randomize data, which erases the effects of the particular order in which we collected and/or otherwise prepared our data. Visualize data to help detect relevant relationships between variables or class imbalances (bias alert!), or perform other exploratory analysis. Split into training and evaluation sets

4. Model Selection

We used Random Forest Classifier machine learning algorithm, We got a accuracy of 100% on train set so we implemented this Aalgorithm.

The Random Forests Algorithm

Let's understand the algorithm in layman's terms. Suppose you want to go on a trip and you would like to travel to a place which you will enjoy.

So what do you do to find a place that you will like? You can search online, read reviews on travel blogs and portals, or you can also ask your friends.

Let's suppose you have decided to ask your friends, and talked with them about their past travel experience to various places. You will get some recommendations from every friend. Now you have to make a list of those recommended places. Then, you ask them to vote (or select one best place for the trip) from the list of recommended places you made. The place with the highest number of votes will be your final choice for the trip.

In the above decision process, there are two parts. First, asking your friends about their individual travel experience and getting one recommendation out of multiple places they have visited. This part is like using the decision tree algorithm. Here, each friend makes a selection of the places he or she has visited so far.

The second part, after collecting all the recommendations, is the voting procedure for selecting the best place in the list of recommendations. This whole process of getting recommendations from friends and voting on them to find the best place is known as the random forests algorithm.

5. Analyze and Prediction

In the actual dataset, we chose only 11 features:

Profile pic: user has profile picture or not
Nums/length username: ratio of number of numerical chars in username to its length
Fullname words: full name in word tokens
Nums/length fullname: ratio of number of numerical characters in full name to its length
Name==username: Are username and full name literally the same
Description length: Bio length in characters
External URL: Has external URL or not
Private: Private or not
#Posts: Number of posts
#Followers: Number of followers
Fake : Yes or No

6. Accuracy on test set

After training and evaluating the model on the validation set, the accuracy of the model will be assessed on the test set. The accuracy on the test set will be an important metric for evaluating the model's performance. We got an accuracy of 93% on test set.

7. Saving the Trained Model

Once you're confident enough to take your trained and tested model into the production-ready environment, the first step is to save it into a .h5 or .pkl file using a library like pickle.

Make sure you have pickle installed in your environment.

Next, let's import the module and dump the model into .pkl file.

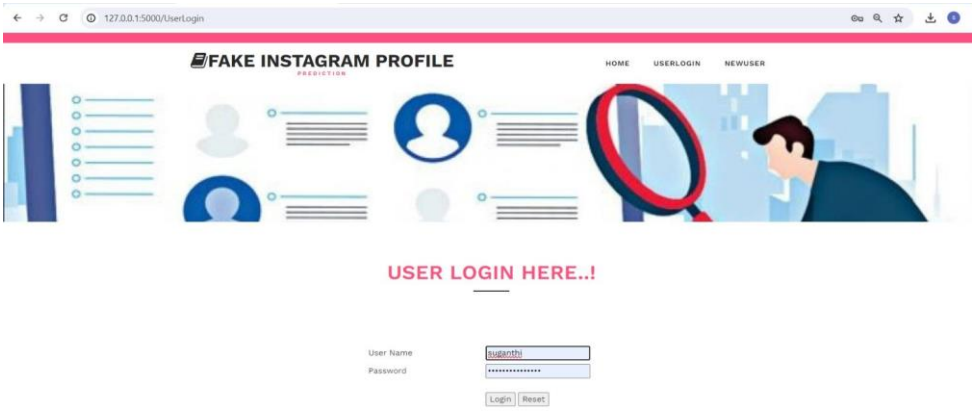
RESULTS AND DISCUSSION :

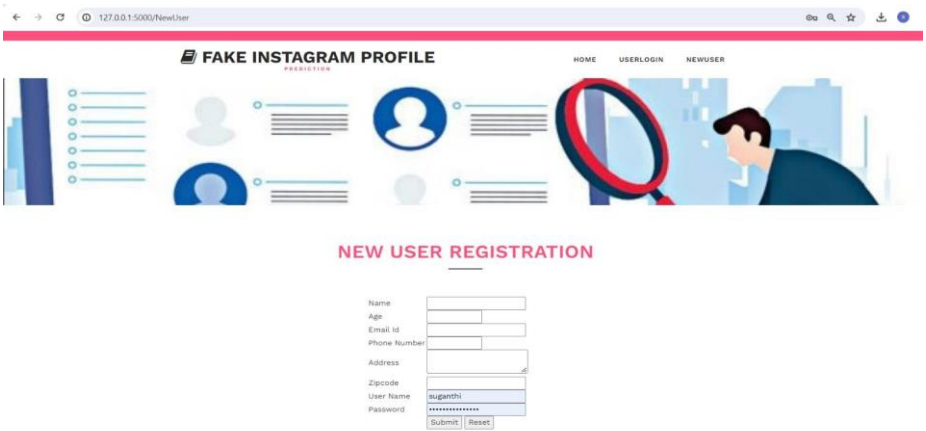
The purpose of testing is to discover errors and ensure that software systems meet their requirements and user expectations without failing in an unacceptable manner. Testing aims to uncover every conceivable fault or weakness in a work product, providing a means to check the functionality of components, sub-assemblies, assemblies, and finished products. Various types of tests address specific testing requirements, including unit testing, functional testing, acceptance testing, and integration testing. Unit testing focuses on validating internal program logic and ensuring that program inputs produce valid outputs, while functional testing systematically demonstrates that functions are available as specified by business and technical requirements. User acceptance testing (UAT) is critical for confirming that the system meets functional requirements, requiring significant end-user participation. Integration testing ensures that different software components or modules interact correctly and that the system as a whole meets functional and non-functional requirements. By combining these testing strategies, software testing provides comprehensive validation that each unique path of a business process performs accurately, identified inputs and outputs are handled correctly, and interfacing systems or procedures function as expected.

CONCLUSION :

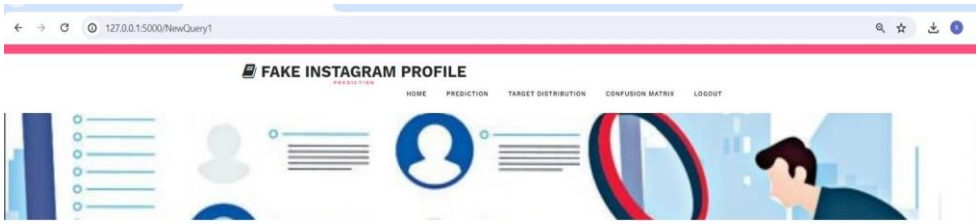
s In conclusion, the project "Instagram Fake Account Detection using Machine Learning" presents acomprehensive and effective solution for addressing the challenge of differentiating between genuine and fake Instagram accounts.Developed using Python and employing two powerful machine learning models, the Random Forest Classifier and the Decision Tree Classifier, this system has demonstrated a high level of accuracy and reliability in its performance.The system operates on a dataset comprising 576 records, each enriched with 12 distinct features that capture various aspects of Instagram profiles, such as the presence of profile pictures, the structure of usernames and full names,bio length, external URLs, and more. These features, in combination with robust feature engineering, enable the system to provide accurate and consistentfake account identification.


127.0.0.1:5000
FAKE INSTAGRAM PROFILE
PREDICTION
HOME
USERLOGIN
NEWUSER
Fake Instagram Profile Prediction


127.0.0.1:5000/UserLogin
FAKE INSTAGRAM PROFILE
PREDICTION
HOME
USERLOGIN
NEWUSER
USER LOGIN HERE..!
User Name
suganthi
Password
Login
Reset

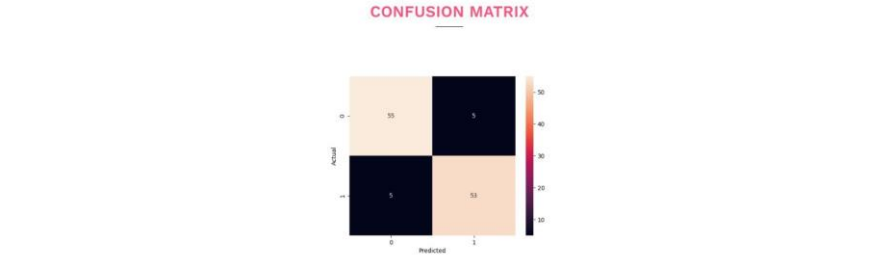

127.0.0.1:5000/NewUser
FAKE INSTAGRAM PROFILE
PREDICTION
HOME
USERLOGIN
NEWUSER
NEW USER REGISTRATION
Name
Age
Email Id
Phone Number
Address
Zipcode
User Name
suganthi
Password
Submit
Reset


127.0.0.1:5000/userlogin
FAKE INSTAGRAM PROFILE
PREDICTION
HOME
PREDICTION
TARGET DISTRIBUTION
CONFUSION MATRIX
LOGOUT
YOUR'S PERSONAL INFORMATION
Name
Age
EmailId
Phone
UserName
suga
21
suganthiraj@gmail.com
9344731752
suganthi


127.0.0.1:5000/NewQuery1
FAKE INSTAGRAM PROFILE
HOME
PREDICTION
TARGET DISTRIBUTION
CONFUSION MATRIX
LOGOUT


FAKE INSTAGRAM PROFILE
Prediction
Profile Pic
nums/length username
fullname words
nums/length fullname
name==username
description length
external URL
private
#posts
#followers
#follows
Submit

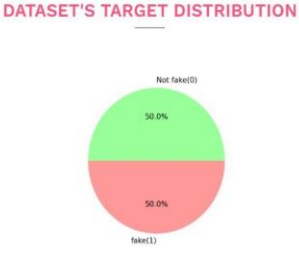

127.0.0.1:5000/cm
FAKE INSTAGRAM PROFILE
HOME
PREDICTION
TARGET DISTRIBUTION
CONFUSION MATRIX
LOGOUT


CONFUSION MATRIX
55
5
5
53
Actual
Predicted


127.0.0.1:5000/newquery
FAKE INSTAGRAM PROFILE
HOME
PREDICTION
TARGET DISTRIBUTION
CONFUSION MATRIX
LOGOUT


Prediction
FAKE


127.0.0.1:5000/td
FAKE INSTAGRAM PROFILE
HOME
PREDICTION
TARGET DISTRIBUTION
CONFUSION MATRIX
LOGOUT


DATASET'S TARGET DISTRIBUTION
Not fake(0)
50.0%
50.0%
fake(1)

REFERENCE :

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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

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