Detecting Fake Identities on Instagram by Using Machine Learning Algorithms

Mr B. Sujith Kumar[1], Smt D. Madhuri[2], Smt M.Prashanthi[3]
[1]*PG Scholar, Department of CSE, JNTUA College of Engineering Anantapur*
[2]*Assistant Professor (Contract), Department of CSE, JNTUA College of Engineering Anantapur*
[2]*Assistant Professor (Contract), Department of CSE, JNTUA College of Engineering Anantapur*

***Abstract*—Social media is one of the preferred communication platforms and has become a target for spammers and scammers. Instagram is a prominent Online Social Network platform for users. It has a lot of features for posting pictures, videos, and text. It created a wide range of communication all over the world. But it also harms people. It creates a way for attackers to steal personal data from individuals, spread rumors and fake news, defame someone's character, cyberbully, and misdirect people to fake websites. To prevent this type of attack there are a few methods that follow naive Bayes to detect those fake identities. The model can detect fake identities by using attributes like profile pictures, number of followers, number of followers, and the content that they use for chats. The existing methods consist of low accuracy rates, high complexity, and require skilled persons. Random forest has features like the ability to perform both regression and classification, searching for the best, and logistic algorithms have features like containing low bias, higher variance, and more collinearity. By combining these powerful algorithms, we can increase the accuracy rate, and decrease the complexity and there is no need for skilled persons to detect those fake identities. By this process, we can easily find an account that is genuine or fake with an accuracy rate of 91% which is more accurate than the previously existing methods that follow Navie bias algorithms.**

Index Terms: **Online Social Networks (OSNs), fake identities, machine learning algorithms, random forest algorithm, Naïve bias.**

I. INTRODUCTION

In the present day, OSNs have a lot of users [1]. The major advantage of OSNs is to be in contact with others and be communicative with each other. It created a vast platform for users to stay in contact and share valuable information on social networks. Because of this reason on day-by-day number of users is increasing rapidly [2].

Instagram is one of the main preferred online social media networks. It has a lot of features when compared to other social media networks. It creates a way for young talents, and content creators to show themselves on social media. Instagram provides a way of posting pictures, videos, and texts. Any new content creator can use Instagram better to grow in such a way of economic growth.

Instagram contains a huge number of accounts but many of them are fake identities. As a coin has both sides, Instagram also has a dark side of attackers and scammers [3]. Many people get an advantage from Instagram as well as affected by the same Instagram by losing their data like pictures, videos, and bank details when the user is misdirected to the wrong websites. They also got the ability to change the election results by using these misdirected websites [4]. An attacker/scammer creates an account on Instagram and uses that account for the wrong purpose. All these are becoming major problems for Instagram users.

Instagram is owned by META. Meta trying to detect those fake accounts/identities to prevent innocent people from cyberbullying, cyber-attacks, and many more. Detecting and reporting those accounts is a way of blocking those users for not interrupting other individuals. However, the detection of fake identities becoming a major task. It is mandatory to detect a fake account accurately. Many machine learning algorithms are used for this work but the accuracy rate is low, and the complexity of detection is high. Random forest and decision tree algorithms have a high potential of detecting a fake account on Instagram.

II. RELATED WORK

In [1] authors explained how social bots make money and fame on social media networks. Social bots are a computer program that controls online social network (OSN) accounts and mimic real users. Social bots are responsible for handling the accounts. Unfortunately, these social bots are slowly hand covered by the wrong hands so it is easy to misguide accounts to the wrong websites easy to steal personal data easy to spread faulty news.

The authors[2] proposed a survey on “Factors explaining users loyalty on social media based brand community”. Social media has an impact on brand promotion. It is the main root of trust-based relationships among people. It states the loyalty and trust of a customer towards the brand. But this is also misguided by attackers.

Ravneet Kaur and Sarbjeet Singh[3] mentioned that there are so many illegal activities that are going on with social networks. They categorized these abnormal activities as anomalies. To prevent these anomalies, they followed detection methods of behavior-based, structure-based, and spectral-based techniques. There are broadly three types of detection of anomalies. Namely “unsupervised, semi-supervised, supervised”.

Katharine Dommett and Sam Power [4] worked on how people use social media the advertise their political party during the elections in the UK. Political parties use Facebook for their advertising. In the UK parties are spending a lot of money on advertising. The election committee permitted transparent digital advertising but the parties spent lots of money only on advertising. It results in any new party or party with low funding not reaching out to people as much as other major party does. So here the problem arises of spending more money to reach out public and makes an immense impact on people regarding the single party which spent more money on advertising. Whereas other parties do not reach out to the people due to their less funding on Facebook advertising.

Author [5] explains that peer to peer-to-peer system is the most commonly used system architecture in social media. But here the problem is when a single system is affected by a fault system then it automatically affects the remaining systems. Thus, it acquires an entity called redundancy. By this, he stated that, if there is entity coordination among all systems then it is possible for cyber attacks.

The authors in paper [6] found the spreading of Astroturf in microblog streams. This means how the fake and artificial content is spreading on small blogs of information. It has a wide impact on people who blindly believe in online social networks. It also affects US political elections. So it is important to prevent these types of actions on social media networks by using techniques of mining, visualizing, mapping, classifying, and modeling.

III. METHODS

This section discusses the proposed task's implementation as well as the study's resources.

A. Dataset

The data set contains 120 records. The data set contains fields of profile pic (is yes-1, if no-0), full name in word tokens, ratio of numerical with full name, does username and name same(is yes-1, if no-0), description length, contains external URL (is yes-1, if no-0), account private(is yes-1, if no-0), number of posts, followers, following. Data is partitioned into test and train data sets. Information about the dataset, including the number of classes, class names, and dataset path, is provided in an Excel file.

B. Proposed method

The goal of this experiment is to detect whether an account on Instagram is fake or genuine by using machine learning algorithms. Several algorithms, including Decision tree, Random-forest, and logistic regression are applied to the detection of fake identity on Instagram. The Random-forest algorithm has the greatest result in predicting whether an account fake or genuine on Instagram.

C. Apply Algorithms

Many algorithms are used on cleaned data with a transparent and clear decision-making process.

1. Decision tree: Decision trees are transparent and can be visually represented, making it easy to choose a course of action.

2. Random forest: A well-known decision tree-based ensemble method that assigns importance to each feature.
3. Logistic regression: Logistic regression is significant because of its ability to provide probabilities and classify new data using continuous and discrete datasets.

Random Forest (RF)

Random forest is a notable ML pattern created by Leo Breiman and Adele Cutler. It faces the results of miscellaneous conclusion shrubs and mixes bureaucracy to follow a unique composition. It has enhanced notably taking everything in mind the evidence that it is foolproof and may be used to handle both accumulation and backslide issues.

Random Forests is a method of reducing variation by averaging many deep decision trees that have been trained on different parts of a single training set. This algorithm is utilized to forecast actions and results in a wide range of industries, including banking and e-commerce.

Random forests contain the three components in their architecture as shown in Fig.1 they are Training set, Testing set, and Prediction.

In the Training set, there are multiple boxes representing the training samples. These samples are used to train multiple Decision trees, which are shown as connected by arrows. Decision Trees area type of algorithm that will be used for regression and classification tasks.

The testing set section has a single box representing the testing data. This data is used to test the performance of the trained Decision trees. The testing data is connected by an arrow to the voting section.

projectionsfromeachDecisiontreearemergedtocreatea finalforecastduringthevotingstep.Forclassification problems, the Random Forest outcome is the class chosen by the majority of trees. The regression analysis returns the mean or average forecast of the specific tree.

The final output of the process is shown in the prediction section. This is where the final made by the Random Forest is displayed. Overall, this diagram visually represents how a Random Forest algorithm works. It shows how training data is used to train multiple Decision trees, how testing data is used to evaluate their performance, and how their predictions are combined to produce a final prediction.

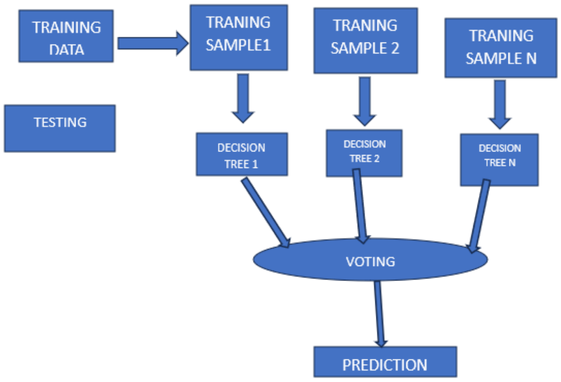

Fig 1: The architecture of random forest

Steps for detecting fake identities on Instagram using Random Forest

1. Collect the input data.

2. Preprocess the data to prepare it for analysis.

3. Divide the data into training and testing sets.

4. Import all necessary Random Forest modules.

5. Train the dataset using the Random Forest algorithm.

6. Validate the model using the test data and Random Forest.

7. Use various commands to make predictions with the trained model.

Decision Tree (DT)

A decision tree is a model that takes a flowchart-like structure to make predictions. It splits the data into branches and assigns out comes to the leaf nodes. Decision trees are used to creates imple models for classification and regression tasks.

The technique operates by continuously dividing the initial dataset into subsets depending on its values for attributes till an interruption requirement is reached, the highest level of the hierarchy or the minimal count of examples necessary to divide a node. This method determines the appropriate attribute to divide the data during training.

Logistic regression (LR)

The logistic algorithm is under a supervised learning technique. It predicts a categorical variable that is dependent by using an independent variable. The output of this is mostly discrete values like no, yes or true, false or 1,0. The probability lies between 0-1. It is mainly used for problems with classification.

IV. FLOW CHART

The following flowchart represents the workflow of the project. It gives a clear idea of the entire workflow of the project.

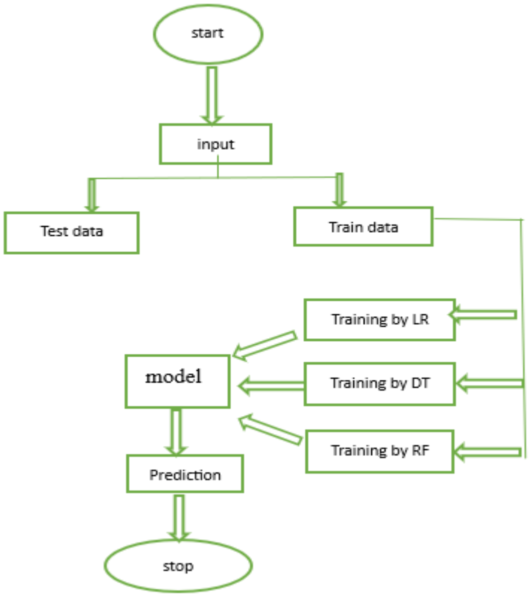

Fig 2: workflow flowchart of the project

V. RESULT AND DISCUSSIONS

In this work we have tested a total of 10 Instagram accounts among them five are fake and five are genuine. In this process the algorithms that we used to detect accounts fake/genuine Decision Trees, Logistic Regression algorithms, and Random Forest were used to predict whether an account was fake or genuine. The Random Forest performed much better than the other remaining algorithms. It is used to train specific classes, and after training, the system can predict the fake/genuine account.

Table 1: Algorithms prediction accuracy rate

	Random forest	Decision tree	Logistic regression
Fake 1	90.4306	89.4736	89.9521
Fake 2	90.4306	88.5167	89.9521
Fake 3	91.3875	88.5167	89.9521
Fake4	91.4075	89.4736	89.9521
Fake5	92.3875	90.2378	89.9521
Genuine 1	90.3829	89.4736	89.9521
Genuine2	91.3875	88.9952	89.9521
Genuine 3	90.9090	90.4306	89.9521
Genuine4	91.9090	89.4736	89.9521
Genuine5	90.3875	88.9952	89.9521

By following the above tabular values, the graph is generated for a better understanding of how the algorithms are performing for the model.

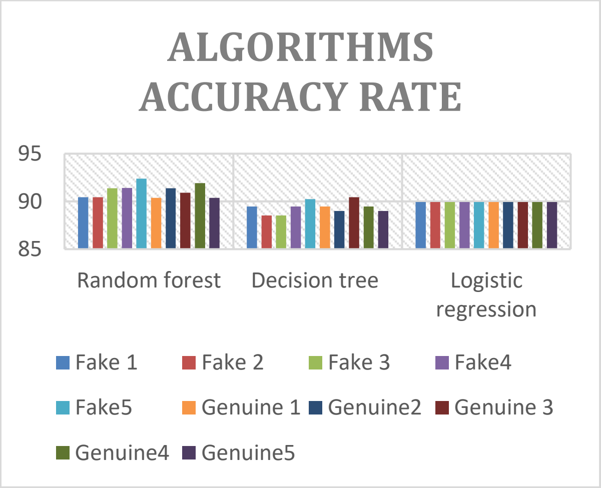

Fig 3: Comparing each algorithm's accuracy rate.

From the algorithms that we used random forest has the highest precision than other algorithms.

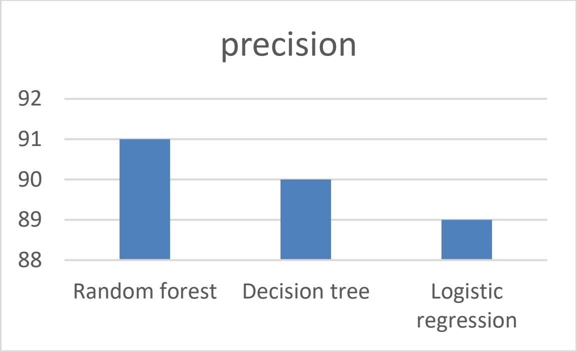

Fig 4: Precision of algorithms.

VII. CONCLUSION

This paper focused on detecting fake identities on a prominent online social media platform called Instagram with the highest accuracy rate. It used a few attributes like profile pic, full name word tokens, the ratio of characters in the name and full name, external URL, bio character length, name, and user name same or not, account private, number of followers, follows, and posts. By using the above-mentioned attributes, the system can predict whether an account is fake/genuine.

The future work for this project includes developing the model with a more powerful having much more accurate rate. The machine learning algorithms like Support vector machines the model could get more

REFERENCES

[1] Ildar Muslukhov, Yazan Boshmaf, Matei Ripeanu, Konstantin Beznosov, “The Social bot Network: When Bots Socialize for Fame and Money”,DOI:https://doi.org/10.1145/2076732.2076746

[2] Louis M. Potgieter, Rennie Naidoo, “Factors explaining user loyalty in a social media-based brand community”, South African Information Management, DOI::10.4102/slim.v19i1.744, February 2017.

[3] Katharine Dommett & Sam Power, “The Political Economy of Facebook Advertising: Election Spending, Regulation, and Targeting Online”, The Political Quarterly is published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing, DOI: https://doi.org/10.1111/1467-923X.12687, April 2019.

[4] Sarbjeet Singh, Ravneet Kaur, “ A survey of data mining and social network analysis based anomaly detection techniques”, Published on December 2015, DOI: https://doi.org/10.1016/j.eij.2015.11.004

[5] John R. Douceur “ The Sybil Attack” Microsoft Researcher, DOI: 10.1007/3-540-45748-8_24, March 2007.

[6] Michael Conover, Jacob Ratkiewicz, Bruno Gonçalves, Mark Meiss, Snehal Patil, Alessandro Flammini, Filippo Menczer “Truthy: Mapping the Spread of Astroturf in Microblog Streams”. DOI: https://doi.org/10.1145/1963192.1963301, May 2014.