IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 7.39 ⁙ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116122

NEURAL NETWORK APPROACH TO DETECT FAKE PROFILES ON SOCIAL NETWORKS

N. SREE DIVYA[1], GORIPARTHI PRASHANTH[2], MALGARI TEJASWINI REDDY[3], GOJE VAISHALI[4]

Assistant Professor, Department of IT, MGIT, Hyderabad, India[1]

UG Student, Department of Information Technology, MGIT, Hyderabad, India[2]

UG Student, Department of Information Technology, MGIT, Hyderabad, India[3]

UG Student, Department of Information Technology, MGIT, Hyderabad, India[4]

ABSTRACT: In the current age, the public activity of everybody has become related with online interpersonal organizations. These locales have rolled out an extraordinary improvement in the manner we seek after our public activity. Making companions and staying in touch with them and their updates has become more straightforward. In any case, with their fast development, numerous issues like phony profiles, online pantomime have likewise developed. There are no practical arrangements exist to control these issues. In this paper, I thought of a system with which the programmed ID of phony profiles is conceivable and is productive. This structure utilizes grouping strategies like Random Forest Classifier to order the profiles into phony or veritable classes. As this is a programmed location technique, it tends to be applied effectively by online informal communities that have a great many profiles whose profiles can't be inspected physically

Keywords: social media, Facebook, Random Forest Classifier, Classification, Framework, and Dataset

INTRODUCTION:

Social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people who have the same interests. These Online Social Networks (OSN) use web2.0 innovation, which permits clients to associate with one another. Person to person communication locales is developing quickly and fundamentally altering the manner in which individuals stay in touch with one another. The internet-based networks carry individuals with similar interests together which makes clients simpler to make new companions

HISTORY:

These social networking sites starting with http://www.sixdegrees.com in 1997 then came http://www.makeoutclub.com in 2000. Sixdegrees.com couldn't survive much and closed very soon but new sites like myspace, LinkedIn, Bebo became successful and Facebook was launched in 2004 and presently it is the largest social networking site in the world.

SOCIAL IMPACT:

Social networking platforms have turned into a fundamental piece of the present human existence — pretty much every individual is related with something like one of the web-based interpersonal interaction sites today. Subsequently, an immense group is generally dynamic on these stages; an enormous number of client commitment pulled in spammers and unauthentic clients on web-based person to person communication. To spread unauthentic messages like tales, disdain discourse, harassed message, and others, clients make a phony profile. Researchers proposed several techniques to limit this issue using machine-learning- and deep-learning-based models, but many fake accounts are still present. Be that as it may, for a decent long range interpersonal communication stage, these phony records are not satisfactory. This article sums up the new headway of person-to-person communication's phony record recognition, which assists the future specialist with building a powerful model to forestall and recognize counterfeit records on the web

Bot detection is the process of using various tools as well ways to identify bots in a collection. The complexity of this varies depending on the type of bot and the set of symbols it contains. The objective here is to decrease the quantity of bogus up-sides (bots are really human) and misalignments (people are truly bots).

DOI: 10.17148/IJARCCE.2022.116122

Fake Profile

A false profile is the representation of a person, organization or company that does not exist, on social media. These records are utilized to hide the character of the individual while sending oppressive or undermining messages, mimicking that person trying to harm their standing or to cause trouble or to mislead their loved ones by reaching the casualty profile to fool them into taking part in vindictive substance.

Internet bots

An internet (bot) is any automated software program that can repeatedly perform 5 different tasks. The use of bots on the web is so common that they currently make up 40% of all online traffic. The most well-known undertakings performed by these bots are business slithering, downloading, checking, and tagging

Machine learning

Machine reading is a method of automatic data analysis to build an analytical model. A branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

OBJECTIVE:

In today's online social networks there have been a lot of problems like fake profiles, online impersonation, etc. To date, no one has come up with a feasible solution to these problems. In this project, I intend to give a framework with which the automatic detection of fake profiles can be done so that the social life of people become secured and by using this automatic detection technique.

LITERATURE SURVEY:

Sarah Khaled et al. presented a new algorithm, SVM-NN, to provide efficient detection for fake Twitter accounts and bots, feature selection and dimension reduction techniques. This proposed algorithm (SVM-NN) uses less number of features, while still being able to correctly classify about 98% of the accounts of our training dataset [1].

Sreenivas Kumacham et al. proposed a machine learning model to predict the student placements using various Machine Learning algorithms that include J48, Naïve Bayes, etc., The model tries to obtain the results from various algorithms and these results are compared to predict the best algorithm for any given dataset.[2]

Y. Boshmaf, D. Logothetis, G. Siganos, J. Lería, J. Lorenzo, M. Ripeanu, K. Beznosov, proposed SENAD model identifies the Fake News spread and helps identify Fake accounts created to spread fake news. As part of working with Fake images, CredNN is the framework proposed, where a joint representation of forensic and emotional cues in fake images is learned via an ensemble of deep Convolutional Neural Networks fine-tuned on visual sentiment fake image datasets. Social Engagement-based News Authenticity Detection (SENAD) model [4]

Mohammed Basil Albayati, Ahmad Altamimi [2019] Proposed a model that uses a range of data mining techniques to detect false profiles. A set of supervised (ID3 decision tree, K-NN and SVM) and unsupervised (K-Means, K-Medoids) machine learning algorithms has been applied to 12 behavioural and non-behavioural discriminatory profile attributes. The results showed that ID3 had an accuracy rate of 97.76 % in the detection process.[6]

PROPOSED FRAME WORK:

OVERVIEW:

Each profile (or account) in a social network contains lots of information such as gender, no. of friends, no. of comments, education, work, etc. A portion of this data is private and some are public. Since private data isn't open in this way, we have utilized just the data that is public to decide the phony profiles in the interpersonal organization. Nonetheless, in the event that our proposed conspire is utilized by the person -to -person communication organizations itself, they can involve the confidential data of the profiles for location without abusing any security issues. We have thought about this data as highlights of a profile for the grouping of phony and genuine profiles. The steps that we have followed for the identification of fake profiles are as follows:

- First, all the features are selected on which the classification algorithm is applied. Legitimate consideration ought to be taken while picking elements, for example, includes that ought not be subject to different highlights and those highlights ought to be picked which can build the efficiency of the classification.
- After proper selection of attributes, the dataset of previously identified fake and real profiles are needed for the training purpose of the classification algorithm.

- The attributes selected in step 1 are needed to be extracted from the profiles (fake and genuine). For the person-to- person communication organizations which need to execute our plan don't have to follow the rejecting system, they can without much of a stretch concentrate the highlights from their information base. We applied to scrap off the profiles since no informal community dataset is accessible openly for the exploration motivation behind identifying the phony profiles.
- After this, the dataset of fake and real profiles is prepared.
- After the preparation of the training and the testing dataset, the training dataset is fed to the classification algorithm. It learns from the training algorithm and is expected to give correct class levels for the testing dataset.
- The levels from the testing dataset are removed and are left for determination by the trained classifier. The efficiency of the classifier is calculated by calculating the no. of correct predictions divided by total no. of predictions. We have used random forest classifier algorithm

Proposed framework:

Succession of cycles that should be followed for proceeds with location of phony profiles with dynamic gaining from the criticism of the outcome given by the order calculation. This framework can easily be implemented by social networking companies.

- The detection process starts with the selection of the profile that needs to be tested.
- After the selection of the profile, the suitable attributes (i.e., features) are selected on which the classification algorithm is implemented.
- The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier
- The classifier determines whether the profile is fake or genuine.
- The classifier may not be 100% accurate in classifying the profile so; the feedback of the result is given back to the classifier.
- This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles.

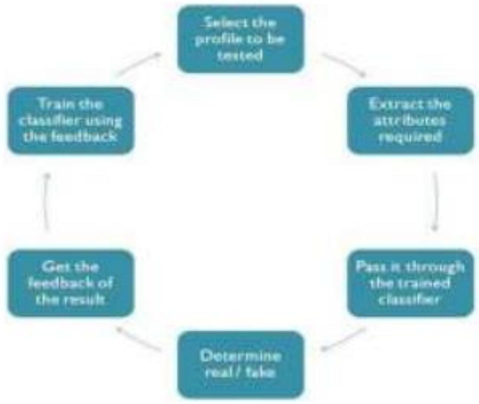

Select the profile to be tested
Extract the attributes required
Pass it through the trained classifier
Determine real / fake
Get the feedback of the result
Train the classifier using the feedback

Figure 1: Steps followed to determine that if a profile is fake

CLASSIFICATION:

Classification is the process of learning a target function f that maps each record, X consisting of a set of attributes to one of the predefined class labels, Y. A classification technique is an approach of building classification models from an input data set.

This technique uses a learning algorithm to identify a model that best fits the relationship between the attribute set and a class label of the training set. The general approach for building a classification model. The model produced by the learning calculation should both fit the info information accurately and accurately foresee the class marks of the test set with as high exactness as could be expected. The vital target of the learning calculation is to construct the model with great over-simplification capacity. The classifier that I have implemented for classifying the profiles is Random Forest and neural networks.

DOI: 10.17148/IJARCCE.2022.116122

Random Forest:

Random forest is a supervised learning algorithm that is used for both classifications as well as regression. But however, it is mainly used for classification problems. As we know that a forest is made up of trees and more trees mean more robust forests. Similarly, the random forest algorithm creates decision trees on data samples and then gets the prediction from each of them and finally selects the best solution by means of voting. It is an ensemble method that is better than a single decision tree because it reduces the over-fitting by averaging the result.

the working of the Random Forest algorithm with the help of following steps:

Step 1 − First, start with the selection of random samples from a given dataset.

Step 2 − Next, this algorithm will construct a decision tree for every sample. Then it will get the prediction result from every decision tree.

Step 3 − In this step, voting will be performed for every predicted result.

Step 4 − At last, select the most voted prediction result as the final prediction result

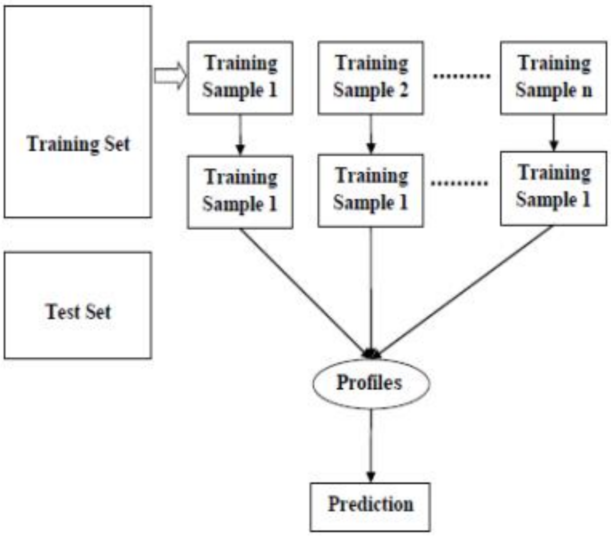


Figure 2: Working of Random Forest Algorithm

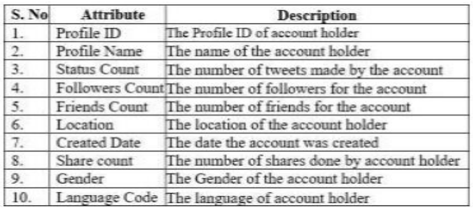
IMPLEMENTATION:

DATA SET:

We needed a dataset of fake and genuine profiles. Various attributes included in the dataset are a number of friends, followers, status count. Dataset is divided into training and testing data. Classification algorithms are trained using a training dataset and the testing dataset is used to determine the efficiency of the algorithm.

ATTRIBUTES CONSIDERED:

Attributes considered for fake profile identification and the description for each of the attributes is provided.



S. No	Attribute	Description
1.	Profile ID	The Profile ID of account holder
2.	Profile Name	The name of the account holder
3.	Status Count	The number of tweets made by the account
4.	Followers Count	The number of followers for the account
5.	Friends Count	The number of friends for the account
6.	Location	The location of the account holder
7.	Created Date	The date the account was created
8.	Share count	The number of shares done by account holder
9.	Gender	The Gender of the account holder
10.	Language Code	The language of account holder

Figure 3: Attributes Considered

Evaluation Parameters:

Efficiency/Accuracy = Number of predictions/Total

Number of Predictions Percent Error = (1-Accuracy)*100

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⵞ Impact Factor 7.39 ⵞ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116122

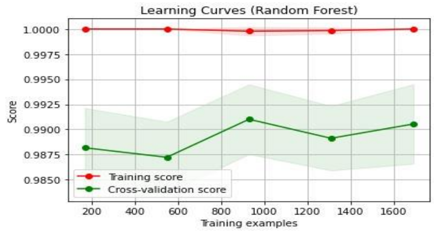
Confusion Matrix - Confusion Matrix is a technique for summarizing the performance of a classification algorithm. Calculating a confusion matrix can give you a better idea of what your classification model is getting right and what types of errors it is making.
TPR- True Positive Rate TPR=TP/(TP+FN)
FPR- False Positive Rate FPR=FP/(FP+TN)
TNR- True Negative Rate TNR=TN/(FP+TN)
FNR- False Negative Rate FNR=1-TPR
Recall- How many of the true positives were recalled (found),
i.e., how many of the correct hits were also found. Recall = TP / (TP+FN) Precision- Precision is how many of the returned hits were true positive i.e., how many of the found were correct hits.
Precision = TP / (TP + FP) F1 score- F1 score is a measure of a test's accuracy.
It considers both the precision p and the recall r of the test to compute the score.
ROC Curve- The Receiver Operating Characteristic is the plot of TPR versus FPR. ROC can be used to compare the performances of different classifiers.

Neural Networks:
A neural network is a network or circuit of neurons, or in a modern sense, an artificial neural network,
composed of artificial neurons or nodes. A neural network (NN), in the case of artificial neurons is an interconnected group of natural or artificial neurons that uses a mathematical model for information processing based on connectionsitic approach interconnected group of natural or artificial neurons that uses a mathematical model for information International Journal of Control and Automation

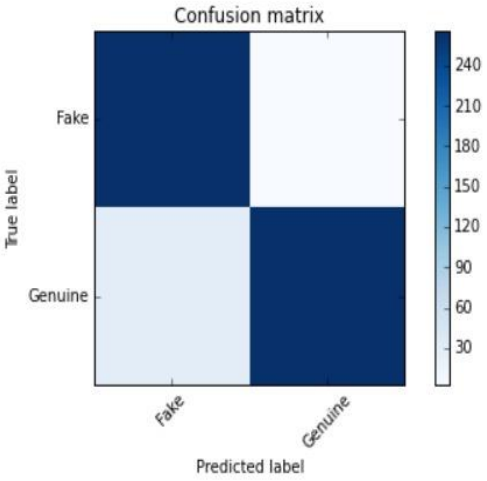
RESULTS:

RANDOM FOREST:

```
training datasets.......

The best classifier is:  RandomForestClassifier(n_estimators=40, oob_score=True)
[0.98817967 0.98345154 1.         0.99054374 0.98578199]
Estimated score: 0.98959 (+/- 0.00286)
```



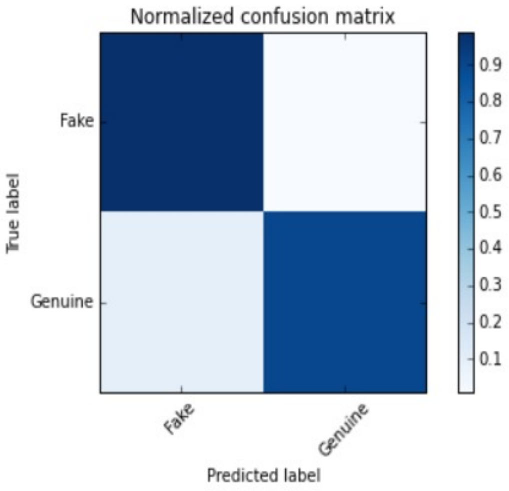
```
Confusion matrix, without normalization
[[265   3]
 [ 30 266]]
```

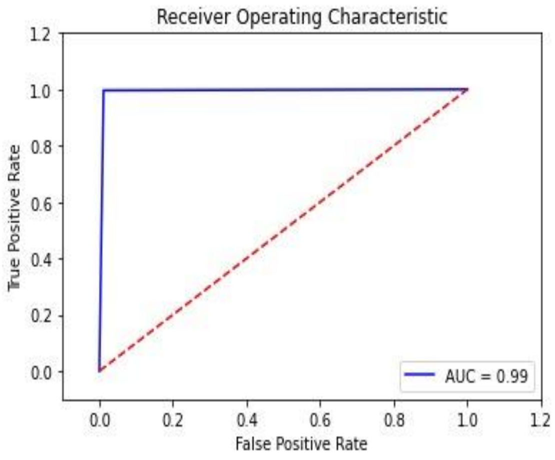


International Journal of Advanced Research in Computer and Communication Engineering

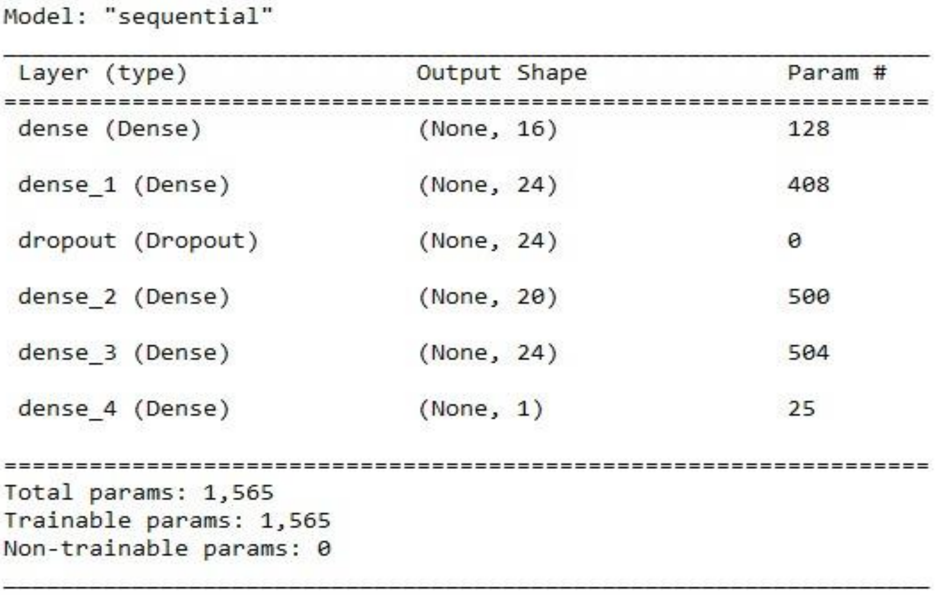
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116122

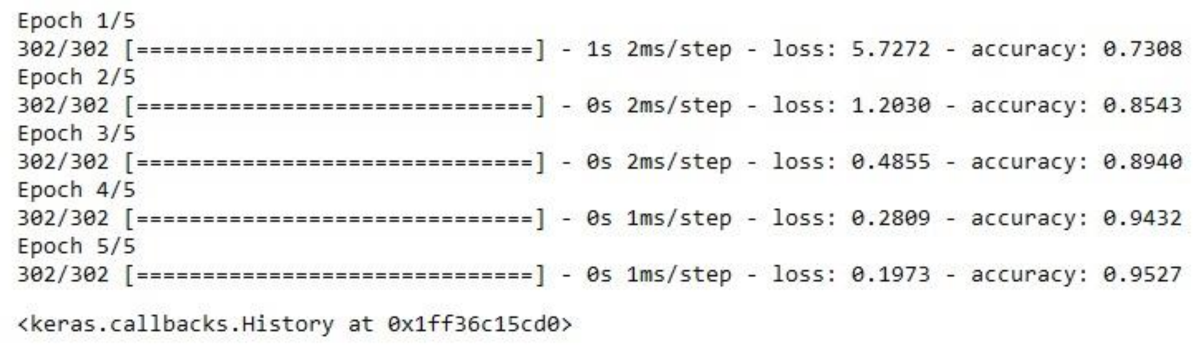




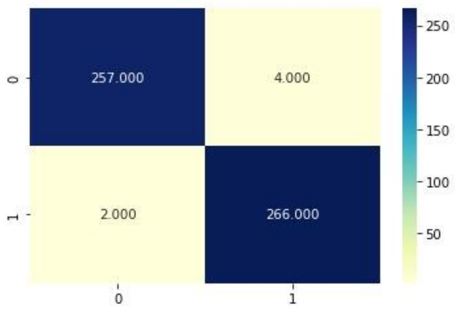
NEURAL NETWORKS:



```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 dense (Dense)               (None, 16)                128

 dense_1 (Dense)             (None, 24)                408

 dropout (Dropout)           (None, 24)                0

 dense_2 (Dense)             (None, 20)                500

 dense_3 (Dense)             (None, 24)                504

 dense_4 (Dense)             (None, 1)                 25

=================================================================
Total params: 1,565
Trainable params: 1,565
Non-trainable params: 0
_________________________________________________________________
```



```
Epoch 1/5
302/302 [==============================] - 1s 2ms/step - loss: 5.7272 - accuracy: 0.7308
Epoch 2/5
302/302 [==============================] - 0s 2ms/step - loss: 1.2030 - accuracy: 0.8543
Epoch 3/5
302/302 [==============================] - 0s 2ms/step - loss: 0.4855 - accuracy: 0.8940
Epoch 4/5
302/302 [==============================] - 0s 1ms/step - loss: 0.2809 - accuracy: 0.9432
Epoch 5/5
302/302 [==============================] - 0s 1ms/step - loss: 0.1973 - accuracy: 0.9527

<keras.callbacks.History at 0x1ff36c15cd0>
```



The efficiency of the Random Forest Classifier in classifying data is 98%

CONCLUSION:

We have given a framework using which we can identify fake profiles in any online social network by using Random Forest Classifier with a very high efficiency as high as around 95%. Fake profile Identification can be improved by applying NLP techniques and Neural Networks to process the posts and the profiles. In the future, we wish to classify profiles by taking profile pictures as one of the features.

REFERENCES:

1] S. Khaled, N. El-Tazi and H. M. O. Mokhtar, "Detecting Fake Accounts on Social Media," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 3672-3681.
[2] Rao, K. Sreenivasa, N. Swapna, and P. Praveen Kumar. "Educational data mining for student placement prediction using machine learning algorithms." Int. J. Eng. Technol. Sci 7.1.2 (2018): 43-46.
[3] Y. Boshmaf, D. Logothetis, G. Siganos, J. Lería, J. Lorenzo, M. Ripeanu, K. Beznosov, H. Halawa, "Íntegro: Leveraging victim prediction for robust fake account detection in large scale osns", Computers & Security, vol. 61, pp. 142-168, 2016.
[4] N. Singh, T. Sharma, A. Thakral and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, 2018, pp. 231-234.
[5] D. M. Freeman, "Detecting clusters of fake accounts in online social networks", 8th ACM Workshop on Artificial Intelligence and Security, pp. 91-101
[6] An Empirical Study for Detecting Fake Facebook Profiles Using Supervised Mining Techniques Mohammed Basil Albayati, Ahmad Altamimi 2019
[7] Using Machine Learning to Detect Fake Identities: Bots vs Humans 10.1109/ACCESS.2018.2796018, IEEE Access ESTÉE VAN DER WALT1 and JAN ELOFF1