International Journal of Advance Research and Innovation
Vol. 11(2), Apr-Jun 2023, pp. 21-25
Doi: 10.51976/ijari.1122303

Article Info

Received: 15 Mar 2023 | Revised Submission: 23 May 2023 | Accepted: 30 May 2023 | Available Online: 15 Jun 2023

Fake Profile Detection on Dating Websites using Machine Learning

Adnan Khan and Ahmad Kamal***

ABSTRACT

Choosing a mate is an integral part of human life and the world has started looking for mates online whether through online dating platforms, matrimonial platforms, or any social media platforms. The online world gives ease to people in finding other interesting people but it also allows scammers to fake themselves on the platforms and do frauds. This paper focuses on online fraud happening on dating websites. In the research, efforts have been made to solve online dating scams by early detection of fake profiles in order to make people aware of the scammers. First, the data has been collected using crawler API and then the data has been processed. Afterward, machine learning techniques have been applied to train a model that can accurately predict whether a profile is fake or real. The classification models like random forest model, naive Bayes, support vector machine, and K- nearest neighbor have been used for this purpose Then the models are tested and their accuracies have been compared. The Random Forest with 94.89 % of accuracy, came out to be giving best results.

Keywords: *Fake Profile; Machine Learning; Dating Websites.*

1.0 Introduction

Online dating applications and websites are revolutionizing the culture of seeking a companion all over the world. According to a report by adjust.com in the year 2020, about 240 million people used online dating throughout the world. Fraud on dating websites is also increasing. Interpol had issued a warning to its 194 member countries against online dating scams. This is a federal crime where the victim is not only scammed but also goes through emotional trauma. In online dating scams, scammers create a fake profile posing as some other person or sometimes just giving fake information about them. The victims are usually the people looking for an emotional relationship and the scam starts when they start entrusting the scammer. The scammer manipulates them over time in order to gain their trust and ultimately, the scammers start begging for money or gather enough personal information about them to either blackmail them or steal their identity.

The only way to save a person from a scam is to know and get aware of the scam. In a more direct way, we could say that if we get to know which profilers are lying about themselves, it becomes easier for the other person to not get involved with them or at least be cautious about them. In this research, efforts have been done to solve online dating scams severe problems by classifying fake profilers using Machine Learning. The objective is to identify a fake profile just by having a little information about the profile like age, occupation, marital status, location, and ethnicity. In the paper, it is proposed to enhance the machine learning fake profile detection system so that scammers can be identified earlier on dating websites and users could become aware of the situation.

This paper is developed as follows. In the next section i.e. section 2, Literature review is discussed. Section 3 discusses the methodology; section 4 discusses the result and discussion and at last section 5 concludes the paper.

2.0 Literature review

There has been a ton of work done in the past for detecting fake profiles across various social media

**Corresponding author; M. Tech, Computational Mathematics, Jamia Millia Islamia, New Delhi, India (Email: adnankhan.cs@gmail.com)*
***Assistant Professor (Computer Science), Jamia Millia Islamia (A Central University) New Delhi, India*

websites including Facebook, Instagram, Tinder, LinkedIn, etc. One such work was done in 2020, where a dataset of legitimate and fake accounts was created. Then, to categorize fictitious users on the dataset, the acquired dataset was fed into the bagging classifier. According to the experimental findings, the suggested method outperforms existing algorithms and correctly categorizes over 98 percent of the accounts with a low error rate [1].

Fake profiles can be of many types, one such type is celebrity impersonator. Another work has been done on Instagram for specifically identifying impersonators. The objective was to detect fake profiles of celebrities and politicians figures by considering their profile characteristics, comments, likes, and age of reviews [2].

In another research, Instagram accounts profile information and activities of the users were taken as input for predictions and the results were shown. In the work, they took a small data set for about 1002 real profiles and about 200 fake profiles which were labeled by them manually. Apart from this they also took 700 real and 700 automated (bots) accounts the two datasets were used separately. The system used several Machine Learning algorithms including Naive Bayes, Logistic Regression, Support Vector Machines, and Neural Networks to find these accounts. Classification accuracy rates of 86% and 96% are found for the automated and fraudulent account detection datasets, respectively [3]. Meanwhile, in another study on the same platform, machine learning algorithms as well as natural language processing techniques were suggested. It was concluded that it is easy to identify fake accounts on social networking sites using these techniques. But they only used the Instagram dataset to find fake profiles in this article. NLP preprocessing methods are employed to examine the dataset. In this study, ML algorithms were used to increase the detection accuracy rate [4].

Another study used machine learning to improve predictions about spotting fake accounts based on users' posts and status updates on social networking sites. Both Twitter and Facebook had it done, and it had a 97 percent accuracy rate [5].

Twitter is said to be the most useful tool when it comes to misleading people on a mass level. In a study With the help of feature selection and dimension reduction approaches, an SVM-NN model is suggested to offer effective bot and false Twitter account detection. Approximately 98 percent of the accounts in our training dataset can be accurately classified by the suggested technique (SVM-NN), which employs less characteristics [6].

There is a detection technique that can identify fake and clone Twitter profiles. A collection of principles that may distinguish between false and real profiles are used to detect phony profiles. Similarity Measures and the C4.5 algorithm were used to detect clones, and a comparison was done to evaluate the effectiveness. The majority of the clones that were given into the algorithm were able to be detected using similarity measures, which performed better than C4.5 [7].

Fake profiles exist on every social media platform, the most famous employment and career oriented platform LinkedIn is not an exception. In a paper a methodology was proposed for detecting social network profile cloning.The tool's main goal was to find any data in a user's profile that may be used to specifically identify him.They used the technology to discover that user profiles frequently contain uncommon information that, when combined with a name, can uniquely identify a profile and thereby any duplicates that may already exist. There were no machine learning techniques applied. We discovered duplicate profiles in the same social network, which was LinkedIn, for 7% of the user profiles we evaluated.[8].

In that study, we define the bare minimum set of profile information required for spotting Fake LinkedIn profiles and provide a suitable data mining method for doing so. They showed that their approach can identify false profiles with 87 percent accuracy and 94 percent True Negative Rate even with sparse profile information, which is equivalent to the outcomes obtained using bigger data sets and more detailed profile information [9].

On social media websites which are specially built to find mates are most prone. The known dating website Tinder is also a platform for fake profiles. Users are unaware of how much personal information they may be broadcasting about themselves in this situation. Without encrypting the more private information of users and connections to other social media platforms, Tinder is making it simple for attackers to look at and compile a tonne of data to make assumptions and pursue its victims [10].

In another work for detecting bots on tinder, it was observed that the collected bots demonstrate that

they are more sophisticated than the bots examined on other social media platforms. Tinder bots have profiles that are incredibly difficult to tell from those of regular users. We investigate the behavior and profiles of these bots and present the traits that can be used in the development of a supervised learning strategy for bot detection [11].

On dating websites the most severe problem occurs as it is the hunting ground of a very particular type of scammers who intend to connect with legitimate users and lead them into emotional relationships to exploit them later. The research study conducted for automatic dismantling online dating fraud, where machine learning models were used along with deep learning and natural language processing. The system performs with 97% accuracy [12].

3.0 Methodology

In this paper, necessary preprocessing measures have been taken to transform the raw data into processed data. Then the machine learning models have been trained to make predictions. Then the performance of these models has been validated.

The data that we used in the paper was extracted from a dating website named Datingmore.com which let us extract the data and a sister website named scamdigger.com had the information of the fake profiles for Datingmore.com. Two different codes were used to extract the data from both websites using the library BeautifulSoup.

As a result, we had data to process with 17,937 rows and 11 columns(features) as ‘gender’, ‘age’, ‘location’, ‘status’, ‘username’, ‘ethnicity’, ‘occupation’, ‘description’, ‘images’, ‘site’, and ‘Fake’. Here ‘Fake’ column is our target column which we will be predicting. In the very first step of our preprocessing, we will delete the columns which are of no use. These four columns are [‘description’, ‘images’, ‘username’, and ‘site’]. There were a lot of values missing values for location, status, and age attributes. For all three attributes, the data points containing missing values were the same. So for the best interest of all, we decided to drop the data points containing missing values.

3.1 Age attribute

We had numeric values of age, but it would have been more helpful to have age in groups as age is scattered approximately from 0 to 80 if we could group certain age period profilers then it will be greatly beneficial when we feed this data into our machine learning model. So We grouped the age responses into 7 groups according to their age periods.

3.2 Gender, status, and ethnicity encoding

The ‘gender’ feature only contains two classes, ‘male’ and ‘female’. It was easily encoded as ‘0’ and ‘1’ using the sklearn feature encoder library available in python. It easily transformed the categorical data in the ‘status’ feature to describe the current relationship status of the profiler as ‘single’, ‘married’, ‘divorced’ and ‘separated’, and ‘-’ for reasons not mentioned. This is an important feature in terms of dating profiles. This profile status just like gender also got encoded using labels from 0 to 5 using the label encoder library from sklearn in python. The third is ‘ethnicity’, this is also a categorical feature that is converted to numerical data using encoding exactly as we converted the above features. It contained 19 unique values as different races which were labeled from ‘0’ to ‘18’ to feed to the machine learning model.

3.3 Location attribute

The best way to use this feature was to get geological coordinates from the address location which could be easily used in the machine learning model. The geocoder service of geopy was used to extract the longitudes and latitudes of all the locations in our set location features.

3.4 Occupation feature

The occupation feature was the most complicated of all as it had 4835 unique values and it would have been a mistake to categorize them and process the 4835 categorical values to the machine learning model. Not just this, the other problem was that we had these occupations in different languages like English, French, Spanish, and many others. Almost all the unique values were looked into and it was started to put keywords in groups(lists). For example ‘medical’ is the first list as shown above and we try to put every relatable keyword so that we could group all the relatable professions. This was done for about 46 different groups and a 2-D list was made for the same where the first element of each list works as both index and values. We finally encoded

these 46 categories from '0' to '45' using some techniques as above.

3.5 Balancing the data set

At this point there were all numerical values with a ready data set to process into the machine learning models and make predictions. Seven useful features as ['gender', 'status', 'ethnicity', 'occupation', 'lat', 'lon', 'age group'] to predict the target feature 'Fake' as '0' meaning not fake and '1' meaning the profile is fake.

The only problem that we have now is that we have an unbalanced data set containing more fake profiles than real ones. We have data with 10,974 real accounts and 2180 fake accounts. This problem was solved by using SMOTE(Synthetic Minority Oversampling Technique). Synthetic data created to balance it. It operates by choosing examples from the feature space that are close to one another, drawing a line between the examples, and then drawing a new sample at a position along the line.

Now it became a balanced data set with 10974 fake accounts and 10974 real accounts.

The dataset is all set to process in a machine-learning model. In the next section, we will discuss the result as feed and train different machine learning classification models and see the results.

4.0 Results and Discussions

In this section, different machine learning models that were implemented are discussed. 4 models have been trained and their performance has been evaluated. The data was divided for training and testing. 80% of the data was dedicated to training and 20 % to testing. The training data was fed to the different models. Lets here discuss the observation of all four models named the Random Forest model, K-Nearest Neighbor, and Naive Bayes Model [Fig][I][II][III][IV].

Table 1

Model	Accuracy	Precision	Recall	f1 score
Random Forest	94.92 %	0.9	0.959	0.94
K-Nearest Model	93.23%	0.913	0.954	0.933
Support Vector Machine	89.77%	0.863	0.943	0.901
Naive Bayes Model	75.40%	0.747	0.761	0.754

Figure 1: Confusion Matrix for Random Forest Model

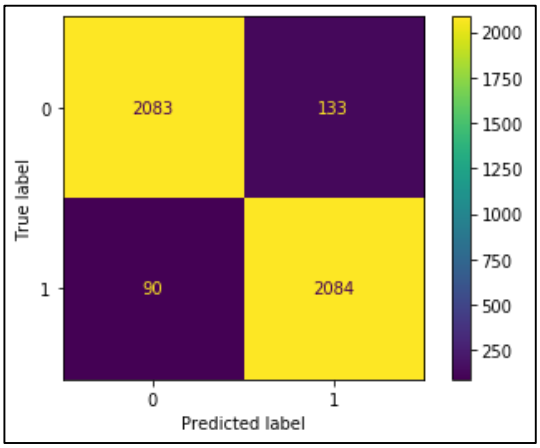


Figure 2: Confusion Matrix for K-Nearest Neighbour

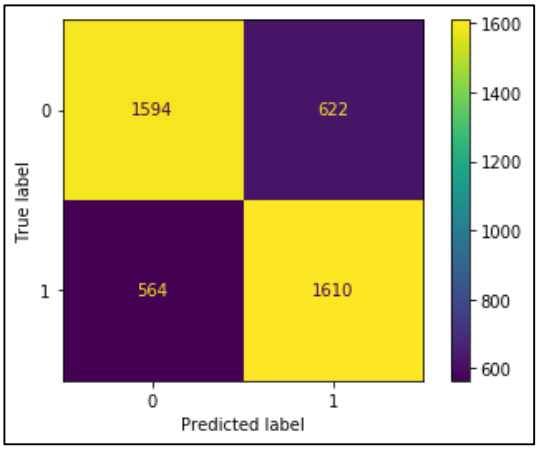


Figure 3: Confusion Matrix for Support Vector Machine

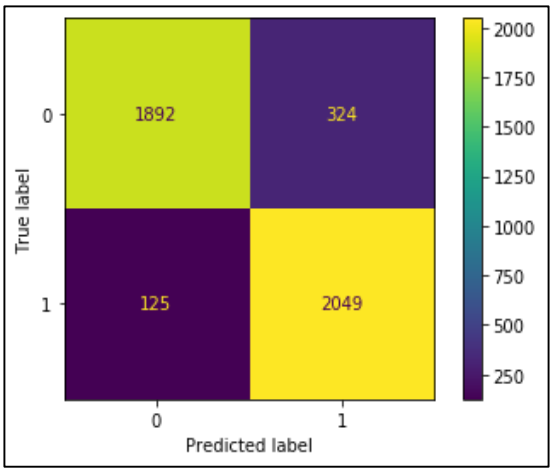
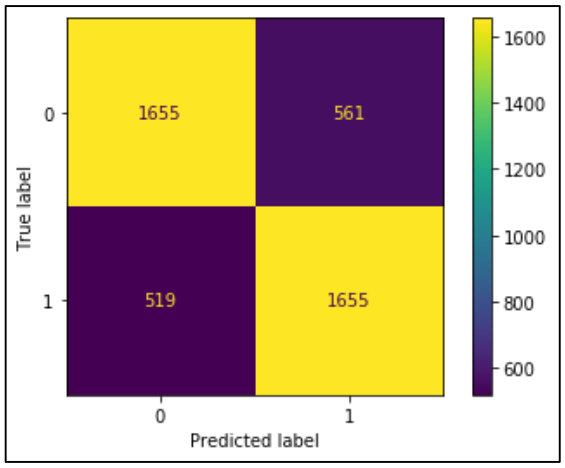


Figure 4: Confusion Matrix for Naive Bayes Model



5.0 Conclusion

This system helps to efficiently detect fake profiles so that scammers can be identified earlier in order to prevent fraud from happening. The main objective was to detect fake profiles using machine learning models. It was successfully experimented with several machine learning models to achieve the goal. All the models were validated through appropriate accuracy measures Precision, Recall, F1, and confusion metrics [Table 1]. The results were somehow satisfactory and the models were able to classify the fake and real profiles. The Random Forest model outperforms all the other models with an accuracy of 94.92 %[Fig 1].

References

[1] Sheikhi, Saeid. "An Efficient Method for Detection of Fake Accounts on the Instagram Platform." *Rev. d'Intelligence Artif.* 34, no. 4 (2020): 429-436.

[2] Zarei, Koosha, Reza Farahbakhsh, and Noel Crespi. "Typification of impersonated accounts on instagram." In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, pp. 1-6. IEEE, 2019.

[3] Akyon, Fatih Cagatay, and M. Esat Kalfaoglu. "Instagram fake and automated account detection." In *2019 Innovations in intelligent systems and applications conference (ASYU)*, pp. 1-7. IEEE, 2019.

[4] Saranya Shree, S., C. Subhiksha, and R. Subhashini. "Prediction of Fake Instagram Profiles Using Machine Learning." *Available at SSRN 3802584* (2021).

[5] Raturi, Rohit. "Machine learning implementation for identifying fake accounts in social networks." *International Journal of Pure and Applied Mathematics* 118, no. 20 (2018): 4785-4797.

[6] 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), 2018, pp. 3672-3681, doi: 10.1109/BigData.2018.8621913.

[7] Sowmya, P., and Madhumita Chatterjee. "Detection of fake and clone accounts in twitter using classification and distance measure algorithms." In *2020 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0067-0070. IEEE, 2020.

[8] Kontaxis, G., Polakis, I., Ioannidis, S., & Markatos, E. P. Detecting social network profile cloning. in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on. 2011. IEEE

[9] Adikari, Shalinda, and Kaushik Dutta. "Identifying fake profiles in linkedin." *arXiv preprint arXiv:2006.01381* (2020).

[10] Feltz, Margaret, and Ming Chow. "The security of tinder." *CsTufts Edu* (2015).

[11] Nazer, Tahora H., Fred Morstatter, Gareth Tyson, and Huan Liu. "A Close Look at Tinder Bots." (2017).

[12] Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128-1137.