

Prediction of Fake Instagram Profiles Using Machine Learning

R.Subhashini^{1*}, R.Sethuraman², B. Keerthi Sambhitha³

¹Department of IT, Sathyabama Institute of Science and Technology, Chennai, India

^{2,3}Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India

*subhaagopi@gmail.com

ABSTRACT

The majority of people now use social networking sites as part of their everyday lives. Every day, a vast number of people build profiles on social networking sites and connect with others, regardless of their place or time. Users of social networking sites not only profit from them, but they also face security concerns about their personal details. To assess who is promoting threats in social networks, we must first identify the users' social network profiles. It is necessary to differentiate between genuine and false accounts on social media based on the classification. Detecting false accounts on social media has historically focused on a number of classification methods. However, it is possible to boost the accuracy of fake profile identification in social media. Machine learning and natural language processing (NLP) technologies are used in the proposed work to increase the percentage of fake profile prediction. The Support Vector Machine (SVM) and the Naive Bayes algorithm are the two algorithms used in classification provides better results.

Keywords

NLP, Machine Learning, Python.

Introduction

In recent years, social networking has grown in popularity on the internet, capturing large number users and trillions of time people spent on such platforms. Online social network (OSN) services include everything from social interaction-focused sites like Instagram and snapchat to mass communication platforms like Twitter and Google buzz, as well as social communication characteristics and current systems like flicker. Increasing security issues and preserving OSN privacy, on the other hand, remains a major bottleneck and viewed mission.

Literature Review

[1] Authors: Kai Shu, Suhang Wang, Huan liu- understanding user profiles on social media for fake detection.

Description: Because of the negative impact on individuals and culture, identifying fake news has become very relevant and is gaining growing attention. The efficiency of detecting fake news solely based on content is generally low, so it is suggested that user social engagements be introduced as auxiliary data to enhance fake news detection. As a result, a detailed understanding of the relationship between user accounts on social media and fake news is needed.

[2] Authors: Shalinda Adikari, Kaushik Dutta- Identifying fake profiles in LinkedIn.

Description: As companies increasingly rely on skilled social networks like LinkedIn (the largest of these), having one's profile noticed within the network is becoming more important. When the value of the network grows, so does the desire to use it for immoral purposes. Fake profiles have a negative impact on the network's overall trustworthiness, and they can cost a lot of time and effort to create a link based on false details.

[3] Authors: Jyoti Kaubiyal, Ankit Kumar Jain- A feature based approach to detect fake profiles in twitter.

Description: Social networking websites, especially Twitter and Facebook, have exploded in popularity in the last decade, attracting users worldwide. They've grown into a common source of information, attracting the attention of bad actors, such as cheaters. Fake accounts become more prevalent as the number of people using social media grows. These false and fake identities are heavily involved in malicious activities like spreading harassment, spreading disinformation, spamming, and falsely inflating the number of users in an app to encourage and manipulate public opinion. These false and fabricated identities are often used in fraudulent activities such as abuse, misinformation and depleting the percentage of users in an app to promote and influence public sentiments. To defend legitimate users from malicious intents, it's vital to identify these false identities.

[4] Authors: Yuval Elovici, Michael FIRE, Gilad Katz- Method for detecting spammers and fake profiles in social networks.

Description: A tool for protecting user privacy in an online social network by choosing negative examples of fake profiles and positive examples of legitimate profiles from the social network's database of current users. Then, for each chosen fake and legitimate profile, a predetermined collection of features is extracted by dividing the friends or followers of the chosen examples into communities and analysing the relationships of each node within and between the communities. Using supervised learning, classifiers that can detect other existing fake profiles based on their features are designed and trained.

Machine learning is a subfield of artificial intelligence concerned with development of algorithms that enable a computer to learn on its own from information and past experiences. Arthur Samuel was the first to coin the word "machine learning" in 1959. A Machine Learning system studies from previous data, builds prediction models, and predicts the outcome until new data is collected. The accuracy of expected performance is determined by the amount of data aids in the creation of a better model that accurately predicts the outcome.

Methodology

Supervised learning is a form of machine learning approach in which we train a machine learning system by feeding it sample labeled data and it then predicts output in order to train it, and it then predicts the output based on that data. We put the model to the test by giving it a sample dataset to see if it would predict accurate results. The aim of supervised learning is similar to when a student learns under the instruction of a teacher since it is dependent on supervision. Spam filtering is an example of supervised learning. There are two types of algorithms that can be used in supervised learning.

Unsupervised learning is a learning process in which a computer learns without assistance of a person. The algorithm is given a set of data that hasn't been labelled, categorised, and it is supposed to operate on it without supervision. Unsupervised learning tries to restructure input data into new features or a series of similar artefacts. Unsupervised learning should not have a fixed result. The machine tries to extract useful information from the massive amount of data it has access to.

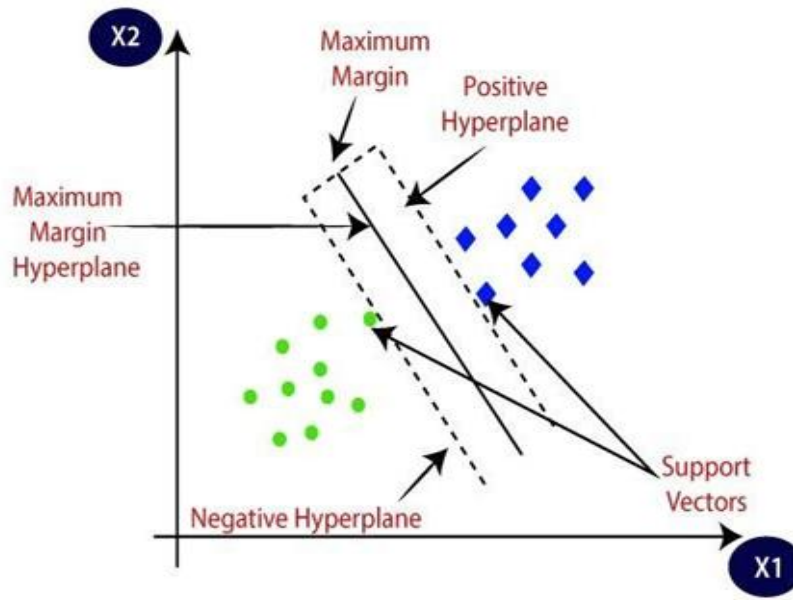


Figure 1:Tensorflow Architecture

Tensorflow can be used across a range of task but has a particular focus on training and inference of deep neural networks. Steps involved in implementing tensorflow use case: First it process the given dataset, that defines features and labels. We practice our model on the training data and try it tries to reduce error. Finally we test our trained model in test data as shown in fig.1 .Here aim is to achieve the highest possible accuracy by repeating the process to decrease the loss.

To assess who is promoting threats in social media, we must first identify the users' social media profiles. We may differentiate between genuine and false accounts on social media based on the classification. Detecting false accounts on social media has historically focused on a number of classification methods. We introduced a machine learning and natural language processing framework in this paper to identify untrustworthy users in online social networks. In addition, the SVM classifier algorithm has been introduced to boost the identification accuracy of fake profiles.

Encouragement for Classification and Regression problems, Vector Machine is one of the most commonly used Supervised Learning algorithms. However, it is mainly used for classification problems in Machine Learning. The SVM algorithm's aim is to find the best line or decision boundary for dividing n-dimensional space into classes so that new data points can be easily placed in the correct category. The best judgement boundary is known as a hyperplane. SVM selects the extreme points/vectors that aid in the formation of the hyperplane. The algorithm is known as a Support Vector Machine, and support vectors are the extreme cases. Consider the diagram below, which illustrates how two distinct groups are classified using a decision boundary or hyperplane.

The Naive Bayes algorithm calculates the likelihood that an entity with unique characteristics belongs to a particular crew or group. In a nutshell, it's a probabilistic classifier. Since it believes that the existence of a particular function is unrelated to the presence of other variables, the Naive Bayes algorithm is called "naive. "If we want to recognise fake profiles based on their time, date

of publication or tweets, language, and place, for example. Even if these characteristics are interdependent or related on the existence of other facets, I believe that they all lead to the probability of a false profile.

Tokenization is the process of decomposing a stream of text into tokens, which can be words, phrases, symbols, or other significant elements. The aim of tokenization is to look at the phrases that make up a sentence. After that, the token list is used as input for additional processing including parsing or textual knowledge mining. Both linguistics and computer science benefit from tokenization. Textual knowledge is nothing more than a string of characters at the most basic level. Stop phrases like 'and,' 'are,' and 'this,' for example, are commonly used. They don't seem to be useful for categorising records. As a consequence, they must be removed from the equation. On the other hand, creating a stop phrase record is challenging and inconsistent across textual sources. By reducing text awareness, this method also improves approach efficiency

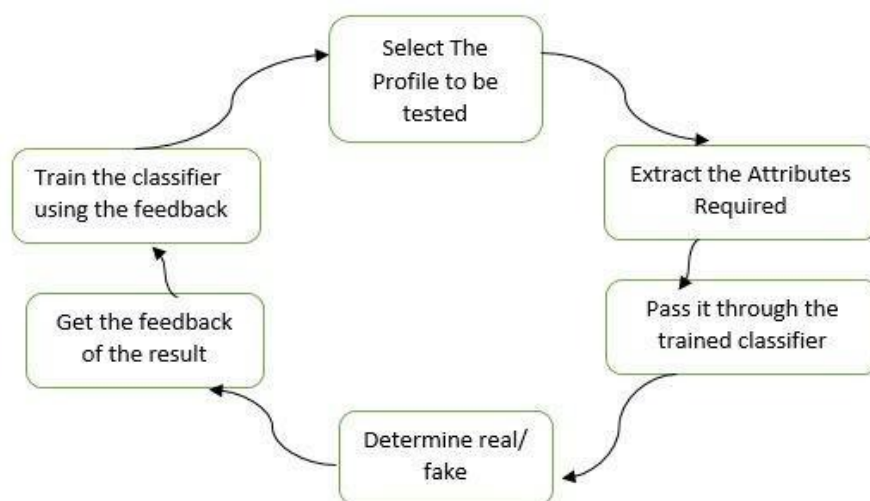


Figure 2:Principal component Analysis (PCA)

To collect the Dataset from Facebook profiles. Collecting data for training the ML model is the basic step in the machine learning pipeline. The predictions made by ML systems can only be as good as the data on which they have been trained. Following are some of the problems that can arise in data collection. inaccurate data. The collected data could be unrelated to the problem statement. Missing data. Sub-data could be missing. That could take the form of empty values in columns or missing images for some class of prediction. Data imbalance. Some classes or categories in the data may have a disproportionately high or low number of corresponding samples. As a result, they risk being under-represented in the model. Data bias. Depending on how the data, subjects and labels themselves are chosen, the model could propagate inherent biases on gender, politics, age or region, for example. Data bias is difficult to detect and remove.

Once the data is extracted from the twitter source as the datasets, this information has to be passed to the classifier. The classifier cleans the dataset by removing redundant data like stop words, emoticons in order to make sure that non textual content is identified and removed before

the analysis. Stemming can reduce indexing size by as much as 40% to 50%. The caller then alters the next frame of the test video to make it appear as if the car is in the area as a result of CNN's orders. The process is then replicated by uploading a new image to CNN. The inland distance (distance from the car to the centre line), yawning, and the distance travelled by the visual vehicle are all reported by the simulator. When the distance between the car and the ground reaches one metre, human interference is needed, and the car's re-positioning and repositioning are reset to fit the ground reality of the original video's corresponding frame.

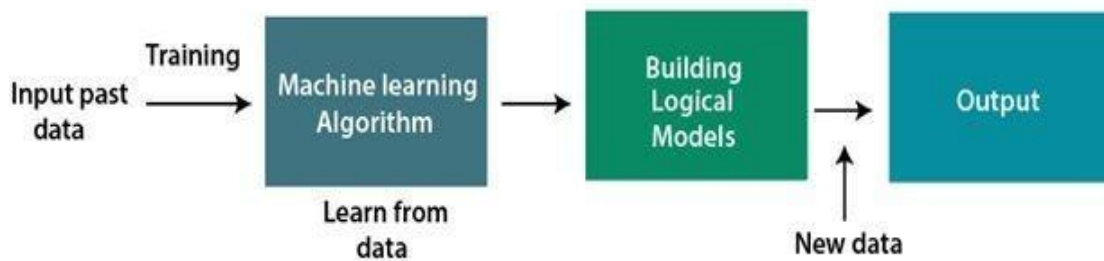


Figure 3:System Architecture

Results and Discussions

1. Training the Model

train														...	
	A	B	C	D	E	F	G	H	I	J	K	L	M		
486	0	0.27	1	0.27	1	0	0	0	0	16	24	1			
487	0	0.44	1	0	0	0	0	0	0	8	8	1			
488	0	0.44	1	0	0	0	0	0	2	34	22	1			
489	0	0.47	1	0	0	0	0	0	2	45	62	1			
490	0	0.33	1	0	0	0	0	0	0	49	0	1			
491	0	0	2	0	0	0	0	0	0	15	5	1			
492	0	0.25	1	0	0	0	0	0	0	62	403	1			
493	1	0.91	1	0	0	0	0	0	0	75	26	1			
494	0	0.44	1	0	0	0	0	0	0	10	0	1			
495	1	0.12	1	0	0	1	0	0	0	23	26	1			
496	0	0.2	1	0	0	0	0	0	0	22	11	1			
497	0	0.24	2	0	0	0	0	0	0	55	46	1			
498	0	0.27	1	0	0	0	0	0	0	16	0	1			
499	0	0.25	1	0	0	0	0	0	0	7	20	1			
500	0	0.28	1	0.24	0	0	0	0	0	64	0	1			
501	0	0.38	1	0	0	0	0	0	0	2	11	1			
502	0	0.37	2	0	0	0	0	0	0	12	30	1			
503	1	0.44	1	0	0	0	0	0	1	14	56	1			
504	0	0.47	1	0	0	0	0	0	0	24	22	1			
505	0	0	2	0	0	0	0	0	0	52	1	1			
506	0	0.44	1	0	0	0	0	0	1	16	27	1			
507	0	0.44	1	0	0	0	0	0	4	17	20	1			
508	0	0.57	2	0	0	0	0	0	0	50	49	1			
509	0	0.54	1	0	0	0	0	0	5	136	1029	1			
510	1	0.43	1	0	0	0	0	0	10	178	1417	1			
511	0	0.69	0	0	0	0	0	0	1	50	39	1			
512	1	0.38	1	0	0	0	0	0	2	207	2426	1			
513	0	0.36	1	0	0	0	0	1	0	178	820	1			
514	0	0	1	0	1	0	0	0	0	16	26	1			
515	0	0.14	1	0	0	0	0	0	0	49	2	1			
516	0	0.7	1	0.19	0	0	0	0	3	20	12	1			

Figure 4:Training at the beginning

In fig. 4, It starts training the model and we can see the training accuracy value. The loss values are higher in the beginning of training the model, which means the accuracy is lesser.



Figure 5: Loss/Accuracy measure

In fig. 5, the loss value is reduced which means the accuracy is increased after repeating the process.

2. Graph Visualization

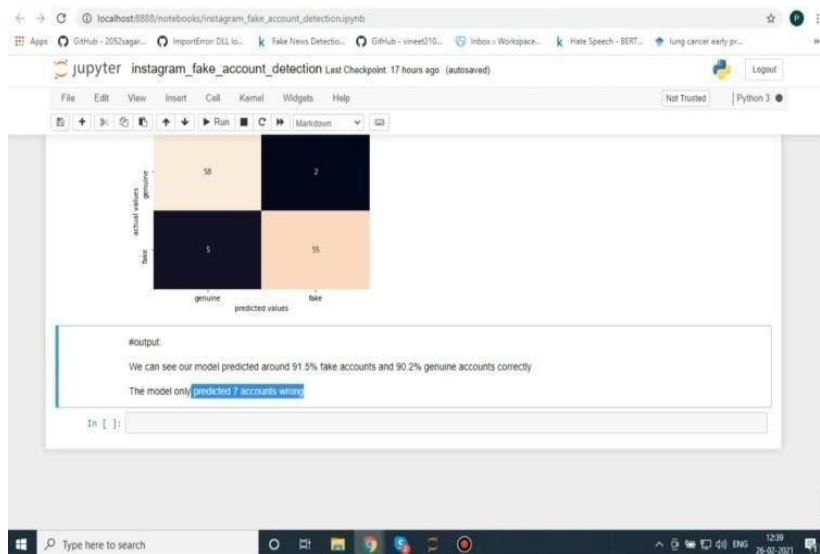


Figure 6: Tensorboard: TensorFlow’s visualization toolkit

The process is repeated till 30 epoch and finally the model gets trained and the model is stored in the following directory. After training we can visualize the graph using tensor board Fig.6 .The dataset is analysed using NLP preprocessing techniques, and machine learning algorithms such as SVM and Naive Bayes are used to identify the profiles.

To classify the fake profile or genuine profiles in Facebook.

3. Running the model through data set

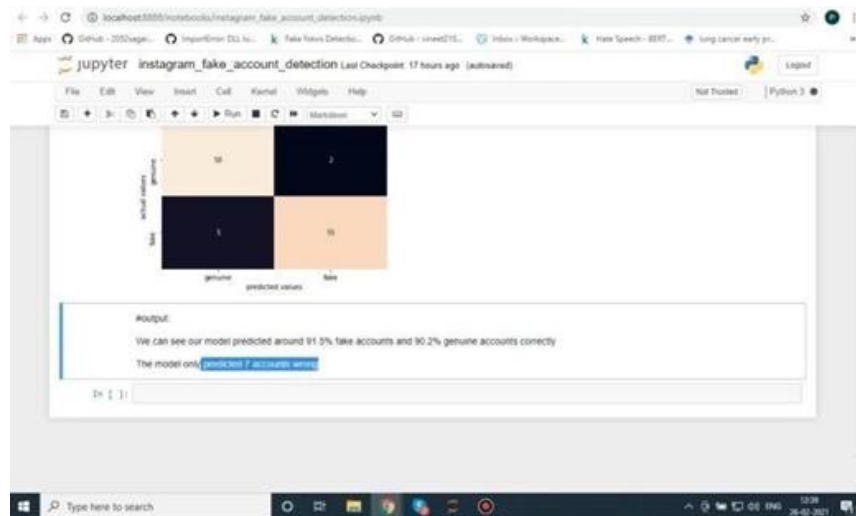


Figure 7:Running the model through data set

The trained network is used to generate steering commands from a single front-facing camera.

4. Running the model through live webcam feed

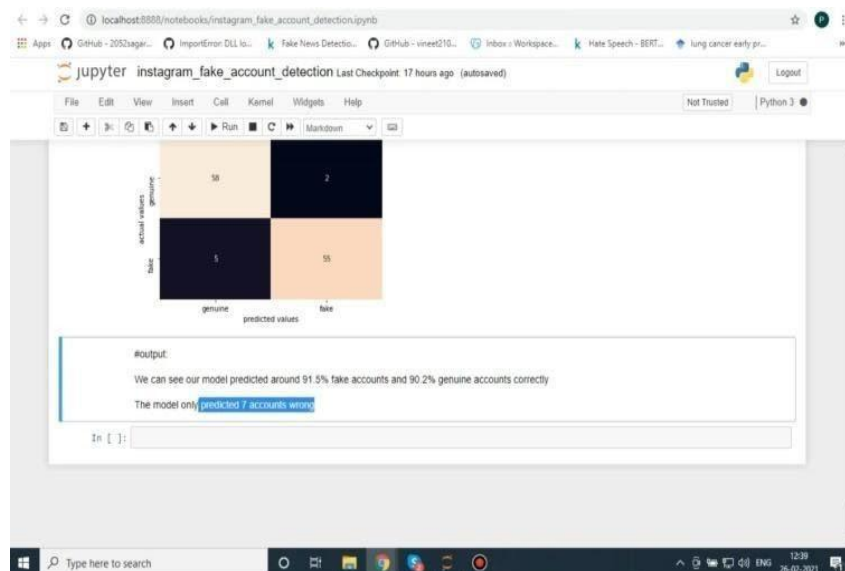


Figure 8:Running the model through live webcam feed

Conclusion

The proposed method uses Machine learning algorithms as well as natural language processing techniques for classification. The fake accounts on social networking sites are accurately classified and predicted using these techniques. The Instagram dataset is used to find fake profiles. To evaluate the dataset, NLP preprocessing techniques are used. In the present work, the detection accuracy rate was improved using ML algorithms.

References (APA 6th edition)

- [1] Romanov, Aleksei, Alexander Semenov, Oleksiy Mazhelis, and Jari Veijalainen. "Detection of fake profiles in social media-Literature review." In International Conference on Web Information Systems and Technologies, vol. 2, pp. 363-369. SCITEPRESS, 2018.
- [2] Adikari, Shalinda, and Kaushik Dutta. "Identifying fake profiles in linkedin." arXiv preprint arXiv:2006.01381 (2020).
- [3] Kaubiyal, Jyoti, and Ankit Kumar Jain. "A feature based approach to detect fake profiles in Twitter." In Proceedings of the 3rd International Conference on Big Data and Internet of Things, pp. 135-139. 2019.
- [4] Elovici, Yuval, F. I. R. E. Michael, and Gilad Katz. "Method for detecting spammers and fake profiles in social networks." U.S.
- [5] Patent 9,659,185, issued May 23, 2019
- [6] Elyusufi, Y. and Elyusufi, Z., 2019, October. Social networks fake profiles detection using machine learning algorithms. In The Proceedings of the Third International Conference on Smart City Applications (pp. 30-40). Springer, Cham.
- [7] Pavan, R., Kiriti, P., Keerthi Samhitha, B., Mana, S.C., Jose, J. 'A Novel Machine Learning-Based Ship Detection for Pre-annotated Ship Database' Lecture Notes in Electrical Engineering, 2021, 709, pp. 463–472.
- [8] Samhitha, B.K., Mana, S.C., Jose, J., Mohith, M., Siva Chandhrahasa Reddy, L. 'An efficient implementation of a method to detect sybil attacks in vehicular ad hoc networks using received signal strength indicator, 2019, International Journal of Innovative Technology and Exploring Engineering 9(1), pp. 2796-2800. 9(1), pp. 2796-2800