IJMLNCE JOURNAL

International Journal of Machine Learning and Networked Collaborative Engineering

Journal Homepage: http://www.mlnce.net/home/index.html

DOI: https://doi.org/10.30991/IJMLNCE.2018v02i03.004

Machine Learning Approach for User Account Identification with Unwanted Information and Data

[a]T.V.M.Sairam[*], [b]Abhishek Kumar

[a]*Research Scholar, Department of Computing Science &Engineering*

Vellore Institute of Technology. sairam.tadepalli1904@gmail.com

https://orcid.org/0000-0003-2292-6210

[b]*Assistant Professor,Department of Computer Science and Engineering,*

Aryabhatta College of Engg. & Research Center,abhishekkmr812@gmail.com

https://orcid.org/0000-0003-4161-508X

Abstract

Machine Learning used for many real time issues in many organizations and for the purpose of social media analytics machine learning models is used most prominently and to identify the genuine accounts and the information in the social media we are her with a new pattern of identification. In this pattern of model we are proposing some words which are hidden to identify the accounts with fake data and the some of the steps we are proposing will be help to identify the fake and unwanted accounts in Facebook in an efficient manner. Clustering in machine learning will be used and in prior to that we are proposing an efficient architecture and the process flow which can identify the fake and suspicious accounts in the social media. This article will be on machine learning implementations and will be working on OSN (online social networks). Our work will be more on Facebook which is maintaining more amount of accounts and identifying which are over ruling the rules of privacy and protection of the user content. Machine learning supervised models will be used for text classification and the image classification is performed by CNN of unsupervised learning and the explanation will be given in the implementation phase. There are large numbers of algorithms we can consider for machine learning implementations in the social networking and here we considered mainly on CNN because of having the feasibility of implementation in different rules and we can eliminate the features we don't need. Feature extraction is quite simple using CNN.

Keywords

Machine Learning, Social Media, Analytics, CNN, Supervised Learning, Unsupervised Learning.

1. Introduction

Consider a person is maintaining his personal information in social media and time to time he is updating his information and capturing the society sight on him. Suppose if the person has a sponsored

[*] Corresponding author
T.V.M.Sairam
Email: sairam.tadepalli1904@gmail.com

account in the platform, it is not an issue. Otherwise, it's a serious issue if the content is the adult and contains any pornography or nudity. To mention this words in the article is not a matter and the thing matters are spreading the adult content and maintaining the account which is against the rules of social media. Cyber threats are more nowadays and the teams which are appointed for the cybersecurity are being failed for a long time because of not identifying the correct pattern of these kinds of threats. In this article, we are highlighting the user accounts which are not following the hashtag concept of the social media. Facebook contains a hashtag dataset which is banned from using in the image tagging. In the text classification, we can identify this kind of things by using machine learning supervised model methods support vector machine model using the bag of words concept. Here we are extending the pattern and the workflow of the algorithm.

Big data is being created daily on social media, and the significant collection of data consists of images, and the tagging of images can be useful for identifying the accounts which are unauthorized [1]. As we are discussing social media, even Instagram and Twitter have the list of banned hashtags and the identification made easy by those firms for the fake and unwanted user profiles. But the users are more intelligent than the platform creators. They are identifying the new ways for the creation of the false and unwanted accounts with adult content for cyberbullying.

Cyberbullying is the process of stealing genuine information and saving those. Users will create a fake account exact to the original account and sell information for money. This content may be offensive in social media and the algorithm which the current versions are not tracking. Based on the information we collected in the past work done by various researchers we implemented our algorithm and the process flow and achieved success rate of 95% of the fake accounts using the CNN. Here this process is divided into two categories based on the primary requirement. First one is text classification. As discussed before we have the concept of banned keywords which should not be mentioned while tagging or posting. Second is images repetition in more than one account, and those pictures have to be identified in any other public website and have to conduct image classification using tensor flow library which is much used for such type problems. In the next section, we are explaining a few past operations or research done by few enthusiastic researchers and later with the proposed approach, next with architectural approach we are considering and finally concluding with explanation and references. We spoke lot about medical domains implementation in machine learning and deep learning and we don't know what to achieve in the medical domain using machine learning and deep learning. In this article we are discussing about the fake accounts detection in the Facebook as we can consider the same social networking as the platform for creating medical data in a large manner time to time. In this consideration we are focusing on the accounts which are posting the irrelevant information about the health care in the social media. Here we can get lot of pages, groups and the accounts which are sharing some health tips to the user and which are promoting their product which was not taken acceptance from the medical council. In those pages we can find the fake information on the health tips and we can consider those are the fake and unwanted accounts. Though they are real accounts but the rule here we are implementing is they are providing and projecting the fake information on the health standards.

Another situation we can remember through twitter tweets which are being poled fake votes in any hashtag competition. Whenever any hashtag is created as an event and consider some groups which are anti to that person related to hashtag then they will target to spread the fake and harmful information through fake accounts. For those kind of accounts they use abbreviation language to target the person in public. Consider a large group of people as conducting health camp in various cities and the other private hospital people may target them in the social media with fake information on that and try to spoil the camp. In those situations we are getting lot of information which is unwanted to be maintained in our servers.

CNN is the algorithms we are here mainly considered for the image classification. But also we can use for the text classification. **RULE** is the theory we are considering for the filtering of the accounts based on the keywords we are mentioning. Here we can consider some of the keywords like LOL, ROFL etc. Which widely used as the sarcastic words in the communication. We will group the combination of the words and list out the combination of those will work or not.

Support consider association rules in the data mining which will consider the group of rules which will take the user to the next level to understand the prediction model on which if the person purchases milk he tends to purchase diapers also. If the person purchased eggs then her tends to purchase bear. In this case we are considering the group of rules and the combinations and this could be the long process but it works. In the association rules are considering the probability of occurrence of the issue.

2. Literature Review

Many of the authors in the previous study mentioned few things related to the concepts in the social networking and few of the ideas we are going to explain here for better understanding of our theory.

Walt [2] explains the concept of identifying bots and human-managed accounts individually with his team member Jan and the idea is considering supervised learning for text classification using the bag of words for detecting spam messages in the report on the current trend topic on the internet [3]. They used Filtering [4][5] used for identifying accounts which are in the blacklist and comparing them with the current existing list of items.

Yongjun [6] Explains about their research regarding the content matching in the different social platforms related to the same user. Identification of the user is based on the shared content using the user-generated content (UGC) concept. Here they performed machine learning models based on the profiles access and the content displayed on the platform based on the individual user.

Ala M. Al-Zoubi [7] explains about the different identifying contents in the social media based on the spam profiles using support vector machines. Here they used whale optimization algorithm to identify the fake and spam accounts in the social media. Again here they focused on online social networks [2][3].

Julien Fontanarava* [8] explains the identification of the fake reviews in the online platforms. This will happen especially on Twitter on the trending topics. It might be a political or any personal all the illegal activities and the fake information will be passed in twitter. To identify those authors performed supervised learning classification model to analyze the fake reviews in the twitter especially.

Other researchers focused on different aspects of social media and in this article we are focusing on presenting you the basic ideas like fake accounts and unwanted accounts in Facebook based on the content published on their accounts and pages.

3. Proposed Approach:

3.1. Text Classification

There are most common banned text words in the privacy policy of the social networking. Here Facebook is the case. If we are identifying those words in the posts. There is a pattern we are following. The following algorithm will explain u in a clear manner.

```
START (HASHTAG,SPON,USERNAME)
{
Ht = hashtag is there or not (1/0)
Spon = Sponsored  account or not (1/0)
Username = username

HASHTAG [] = hashtag API query;

If (Ht == HASHTAG[])
        then
        username = blacklist[]
Else if
If( Ht.HASHTAG[] == true && spon == true)
        then
        username = truelist[]
Else
        username = blacklist[]
Print all the accounts
Create CSV file
END
}
```

The algorithm which we mentioned above is the sample, and the original type of algorithm will be different.

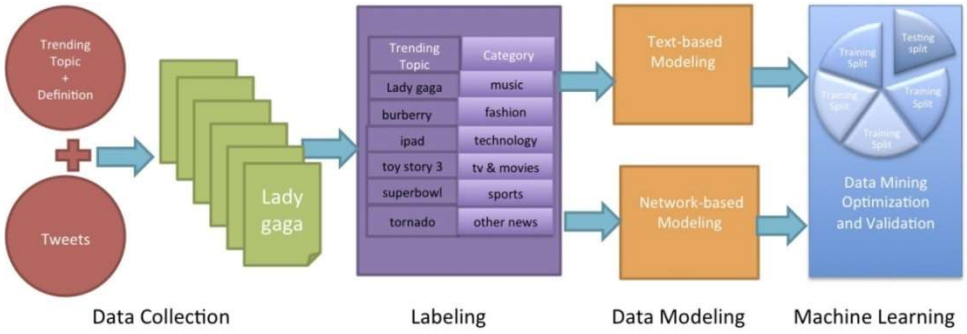

Figure 1 Text Classification Architecture

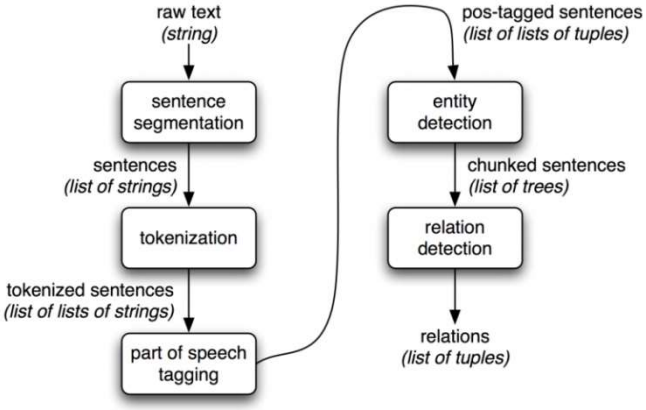

Figure 2 Tokenization in text classification

Text classification here done in two phases. One with normal NLP operation and other is tokenization. In this tokenization, we are separating the sentences into parts, and then we are matching the entity relations with the already existing entities. The chunks are separated and mapped to the test set data, and then we are identifying whether the account is genuine or not.

Figure 1 explains the NLP operation using machine learning model, and in that, we are considering sample tweets for example and then mapping them with the relevant user contents based on the natural language processing. Finally, we get the set based on the training and test set of the data. Based on that we need to perform tokenization, and then we have to implement the support vector machine model to identify the account trustworthiness. Whereas fig 2 explains the concept of tokenization.

In the text classification, we are using tokenizing to separate the text and the hashtag. Here we have some predefined hashtag words in the array, and we are correlating the array with the current words we identified. If the word is available in the array then send that account to block list otherwise that account is genuine.

3.2. Image classification

In the image classification, we are following the process of using tensor flow model for gathering information of images with the hashtag tagging and maintain them as a training set, and we need to analyze the same with the text data.

Fig 3 explains the concept of image classification in general and fig 4 explains the classification using sensor flow library

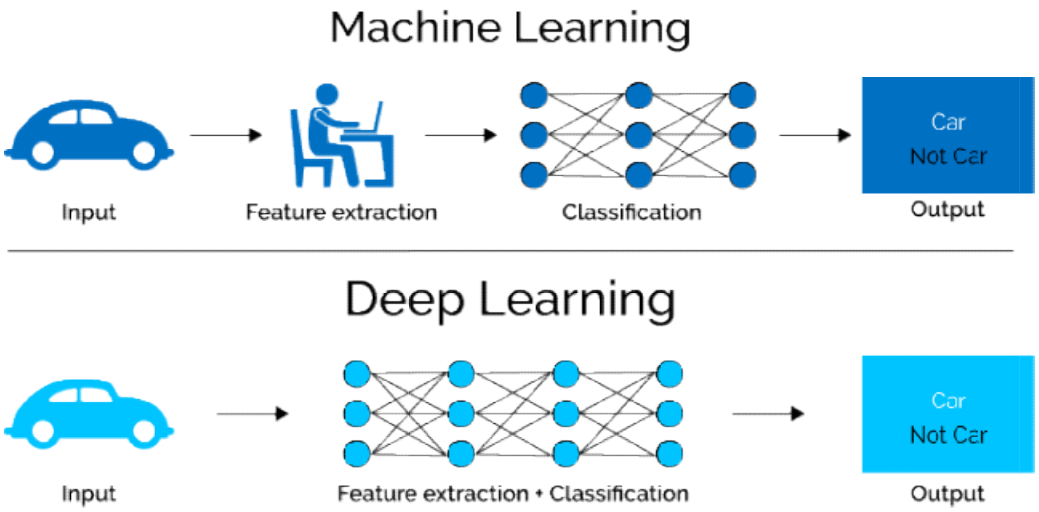

Figure 3 Image classification difference in Machine Learning and Deep Learning

In image classification the hidden layers will perform all the task and if the algorithm is considered then all the images which are collected as set will train the machine with the suitable method[9-10][16] and then there will be some combinations which the process which we are following has to consider while checking the account data. So that whenever the new account found with the same kind of inputs, then it must be regarded as the blacklist account and we have to block that permanently [13-14].

In this article, we contributed our time and ideology and considered this research would help social networking like facebook which is regarded as in this article to manage accounts in a right manner[17][15].

Figure 4 Image classification using sensor flow

In figure 5 we can show the concept of image classification using CNN. As we discussed previously, we can perform image classification using CNN. In CNN we are conducting more hidden layers and identifying the combinations of the rules are pose on the model. The sample architecture is mentioned below[14-15].

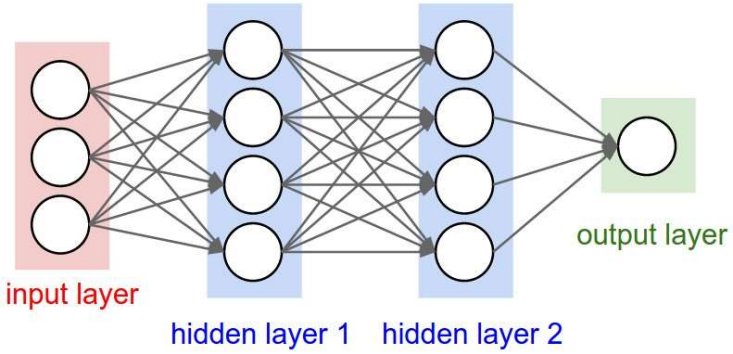

Figure 5: CNN implementation for image classification

```
START (HASHTAG,SPON,USERNAME,IMG)
{
Ht = hashtag is there or not (1/0)
Spon = Sponsored account or not (1/0)
Username = username

HASHTAG [] = hashtag API query;

If (Ht == HASHTAG[])
        then
        username = blacklist[]
Else if
If( Ht.HASHTAG[] == true && spon == true)
        then
        username = truelist[]
Else if
(ht.HASHTAG[] == true && spon == true && IMG.HASHTAG[] == true)
        then
        username = truelist[]
Else
        username = blacklist[]
Print all the accounts
Create CSV file
END
}
```

The above is the image classification algorithm model we are proposing and this is not precisely we present directly. Just for the sample, we present with sample notations.

Machine learning algorithms are more famous for implementation in prediction models, and here we are trying to implement the concept in social media analytics which is a major threat to the society and also for the people in the social media. These days kids are more frequently available in social media. Here kids mean teen. In this current situation, we are unable to stop them from using social media, but we can try to make that platform as a good for them with protecting them from unauthorized information. This kind of protection will be given using machine learning and deep learning models.

In the text classification, we are performing not with advanced models but with the basic idea of the machine learning models like support vector machines and the random forest methods. In these two cases, we found better and standard models implementation procedure and implemented text classification with these two. We may consider other machine learning models as well, but the case here is we need to perform text and image in the unsupervised learning methodology, and we have done that with CNN model which will be in different layer type implementation with layers 2 3 4 and those are the significant parts in the hidden layers. With this implementation, we found a better way to secure social media world with the teens.

4. Results and Output

Considering the work we have done, we would like to explain the worhttps://orcid.org/0000-0003-4161-508Xk with suitable outputs based on the algorithm we use.

4.1. Text Classification Results

We perform this with three algorithms. SVM, Random Forest, and CNB Classifier.

In SVM we consider the bag of words to match and identify the hashtag set. In the random forest, we would like to map the rules to determine the nature of account [8-13], in CNB we use WEKA tool for the classification of account.

The following table will explain the accuracy of each algorithm we consider

Table 1: Results of accuracy in Text Classification

Algorithm	**Tool**	**Accuracy**
SVM	Not Tool. Bag of Words	96%
CNB	WEKA	75%
Random Forest	NA	96%

Here if we observer we can find random forest and SVM will have equal accuracy rate compared to CNB classifier.

4.2. Image classification

We perform image classification based on the number of hidden layers we consider. In the first level, we find three hidden layers, second four layers and the final level we consider five hidden layers. And observe the accuracy of the identifying the fake and genuine account

Table 2: Image classification with CNN

CNN Implementation	3 Layers	75%
	4 Layers	80%
	5 Layers	85%

Here in this implementation based on the number of hidden layers we can get better accuracy. Based on increasing the rules, we get better accuracy.

5. Conclusion

The algorithm we are focusing in this architecture is having different levels to understand. In this method, Facebook is the main focus, and the thing here is we are analyzing facebook in tow levels. One is using text classification, and the other is image classification. In text classification, we are using support vector machine models which will develop the model based on the bag of words to identify the hashtag data. In the image classification, we are using CNN and sensor flow methods individually to identify the accuracy. And they performed equally. In the future implementation, we are focusing for more accuracy in identifying fake accounts and unwanted accounts.

References

[1] “Identifying image tags from Instagram hashtags using the HITS algorithm” Stamatios Giannoulakis, Nicolas Tsapatsoulis, IEEE 15th International conference, 2017. **DOI:** 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.29

[2] “Using Machine Learning to Detect Fake Identities: Bots Vs Humans” Van Der Waltt * IEEE Transaction,2017 DOI 10.1109/ACCESS.2018.2796018

[3] “A survey on classification algorithms for email spam filtering” S.K.Tuteja, Int. J. Eng.Sci.Vol-6 no:5,2016 DOI: 10.22266/ijies2018.0630.01

[4] “Fame for scale: Efficient detection of fake twitter followers", S.Cresci, Decision support system. Vol:80, 2015

DOI:10.1016/j.dss.2015.09.003

[5]"Suspended accounts in retrospect: An analysis of Twitter spam," K.Thomas* ACM SIGCOMM Conf. 2011

[6] "Matching user accounts based on user-generated content across social networks" Yongjun Li*, Future Generation Computer Systems, Elsevier, 2018 https://doi.org/10.1016/j.future.2018.01.041

[7] "Evolving Support Vector Machines using Whale Optimization Algorithm for spam profiles detection on online social networks in different lingual contexts" AlaM.Al-Zoubi * Knowledge-Based Systems, Elsevier, 2018-09-07

[8] O. Dekel, O. Shamir, and L. Xiao. Learning to classify with missing and corrupted features.Machine Learning, 81(2):149{178, 2010. DOI:https://doi.org/10.1007/s10994-009-5124-8

[9]A. Globerson and S. Roweis. Nightmare at test time: robust learning by feature deletion. In Proceedings of the 23rd International Conference on Machine Learning, pages 353{360.ACM, 2006.

[10]I. J. Goodfellow, D.Warde-Farley, M. Mirza, A. Courville, and Y. Bengio. Maxout networks. In Proceedings of the 30th International Conference on Machine Learning, pages 1319{1327. ACM, 2013.

[11]G. Hinton and R. Salakhutdinov. Reducing the dimensionality of data with neural networks.Science, 313(5786):504 { 507, 2006. DOI: 10.1126/science.1127647

[12]G. E. Hinton, S. Osindero, and Y. Teh. A fast learning algorithm for deep belief nets.Neural Computation, 18:1527{1554, 2006. https://doi.org/10.1162/neco.2006.18.7.1527

[13]K. Jarrett, K. Kavukcuoglu, M. Ranzato, and Y. LeCun. What is the best multi-stage architecture for object recognition In Proceedings of the International Conference on Computer Vision (ICCV'09)? IEEE, 2009.DOI: https://doi.org/10.1109/ICCV.2009.5459469

[14]A. Krizhevsky. Learning multiple layers of features from tiny images. Technical report, University of Toronto, 2009.

[15]A. Krizhevsky, I. Sutskever, and G. E. Hinton. Image net classification with deep convolution neural networks. In Advances in Neural Information Processing Systems 25, pages,1106{1114, 2012.

[16]Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D.Jackel. Backpropagation applied to handwritten zip code recognition. Neural Computation, 1(4):541{551, 1989. https://**doi**.org/10.1162/neco.1989.1.4.541

[17] Rawat K., Kumar A., Gautam A.K. (2014) Lower Bound on Naïve Bayes Classifier Accuracy in Case of Noisy Data. In: Babu B. et al. (eds) Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi DOI: https://10.1007/978-81-322-1602-5_68

Author's Biography

T.V.M.Sairam, Completed Bachelors in Computer Science and Engineering and Masters in Cloud Computing. Pursuing Ph.D. in Machine Learning from Vellore Institute of Technology. He was certified in Data Science from John Hopkins University, USA, and published various research articles in Scopus Journals and American indexed journals. His most research is on Machine Learning implementations in more real-time platforms like Social Networking and Working on Deep Learning implementation in Online Platforms and Social Media.

Abhishek Kumar has completed Masters in Computer Science and engineering from Government College, Ajmer, Rajasthan Technical University, Kota, India. He has been working as an Assistant Professor of Computer Science Department at Aryabhatt Engineering College and Research Centre, Ajmer and also visiting faculty for Government University MDS, Ajmer. He has total academic teaching experience of 7 years with many research publications in reputed National and International Journals like Springer, IEEE, Elsevier, Wiley, etc. He has authored four textbook and one edited book, currently working on Network Simulation with MATLAB with Wiley publication.

How to Cite

Kumar, A., & SAIRAM, T. (2018). Machine Learning Approach for User Accounts Identification with Unwanted Information and data. International Journal of Machine Learning and Networked Collaborative Engineering, 2(03), pp. 119-126. https://doi.org/10.30991/IJMLNCE.2018v02i03.004