Detection of Fake Online Reviews using ML

Mallikarjuna S B ¹, Nithya H L²

¹, ²Department of Computer science and Engineering, BIET Davanagere.

Abstract: Online audits have incredible effect on the present business furthermore, trade. Basic leadership for acquisition of on the web items generally relies upon surveys given by the clients. Thus, shrewd people or gatherings attempt to control item surveys for their own advantages. This paper presents a few semi-supervised and supervised content mining models to recognize counterfeit online audits just as analyses the productivity of both procedures on dataset containing lodging surveys.

Keywords: Semi-supervised, Supervised and Counterfeit.

I. INTRODUCTION

With the hazardous development of data on the web, the web has turned into the best and goliath conveyed registering application today. Billions of site pages are shared by a large number of associations, colleges, scientists, and so forth. Web quest gives extraordinary usefulness to circulating, sharing, sorting out, and recovering the developing measure of data. Accordingly, web indexes have turned out to be increasingly significant and are utilized by a great many individuals to discover essential data. It has turned out to be significant for a website page, to be positioned high in the significant web indexes' outcomes. Accordingly numerous methods are proposed to impact positioning and improve the position of a page. A portion of these methods are legitimate and are called Search Engine Optimization (SEO) systems, yet some are not lawful or moral and attempt to hoodwink positioning calculations. They attempt to rank pages higher than they merit [2].

Web spam alludes to web content that get high position in internet searcher results in spite of uninformed worth. Spamming deceives clients, yet in addition forces existence cost to internet searcher crawlers and indexers. That is the reason crawlers attempt to recognize web spam pages to abstain from handling and ordering them.

The social Web and the expanding notoriety of web based life have prompted the spread of different sorts of substance produced legitimately by clients, the purported User Generated content (UGC). By methods for Web 2.0 innovations, it is workable for each person to diffuse substance via web-based networking media, nearly with no type of confided in outside control. This infers that there are no way to check, from the earlier, the dependability of the sources and the acceptability of the substance created [2].

Technologies are evolving quickly. Old advancements are ceaselessly being supplanted by new and modern ones. These new advancements are empowering individuals to have their work done proficiently. Such a development of innovation is online commercial centre. We can shop and reserve spot utilizing online sites. Nearly, everybody of us looks at reviews prior to acquiring a few items or services. Consequently, on the web audits have turned into an extraordinary wellspring of notoriety for the organizations. Likewise, they have enormous effect on ad also, advancement of items and services. With the spread of online commercial centre, counterfeit online surveys are getting to be incredible matter of concern. Individuals can make false surveys for advancement of their own items that damages the real clients. Additionally, aggressive organizations can attempt to harm every others notoriety by giving phony negative reviews [1].

Analysts have been learning about numerous methodologies for location of these phony online surveys. A few approaches are survey substance put together and some are based with respect to conduct of the client who is posting audits. Substance based investigation centres around what is composed on the survey where client conduct put together and some are based with respect to nation, ip-address, number of posts of the analyst and so forth. A large portion of the proposed methodologies are supervised grouping models. Hardly any analysts, likewise have worked with semi-supervised models. Semi-supervised techniques are being presented for absence of dependable marking of the surveys.

In this paper, we make some arrangement draws near for recognizing counterfeit online audits, some of which are semi-supervised what's more, others are regulated. For semi-supervised learning, we use Expectation-amplification calculation. Factual Gullible Bayes classifier and Support Vector Machines (SVM) are utilized as classifiers in our examination work to improve the execution of arrangement. We have for the most part centred around the substance of the survey-based methodologies. As highlight we have utilized word recurrence check, conclusion extremity and length of survey.
A. Objectives
An efficient platform is developed to detect the fake reviews generated by the user in online marketing by the supervised and semi-supervised study. The objective of proposed platform is as follows:

1) To develop reliable and efficient platform for necessary feature extraction from the raw text data.
2) To develop an efficient semi-supervised and supervised text mining techniques for detecting fake online reviews.
3) To do performance analysis of the proposed system.

B. Proposed System
Proposed work, focus on some classification approaches for detecting fake online reviews, some of which are semi-supervised and others are supervised. For semi-supervised learning, Expectation-maximization algorithm is used. Statistical Naive Bayes classifier and Support Vector Machines (SVM) are used as classifiers in our research work to improve the performance of classification. Main focused on the content of the review based approaches. As feature we have used word frequency count, sentiment polarity and length of review.

II. LITERATURE REVIEW
An In 2018, Pankaj Chaudhary, Abhimanyu Tyagi and Santosh Mishra presents article targets giving an examination of the fundamental survey and analyst driven highlights that have been proposed up to presently in the writing to identify phony audits, specifically from those methodologies that utilize directed AI procedures. These arrangements furnish by and large better outcomes as for simply solo approaches, which are regularly in view of diagram based techniques that think about social ties in audit locales. Moreover, this work proposes and assesses some extra new highlights that can be reasonable to order certified and phony audits. For this reason, a regulated classifier dependent on Random Forests have been actualized, by thinking about both surely understood and new highlights, and an enormous scale marked dataset from which every one of these highlights have been extricated.

In 2017, J. K. Rout, A. Dalmia and K.-K. R. Choo clarify how semi-administered learning strategies can be utilized to distinguish spam audits, before exhibiting its utility utilizing a dataset of lodging audits(reviews).

In 2016, Chengai Sun, Qiaolin Du and Gang Tian proposes a novel convolutional neural system model to coordinate the item related audit includes through an item word structure model. To lessen over fitting and high difference, a sacking mode is acquainted with pack the neural system model with two productive classifiers. Tests on the genuine Amazon survey dataset exhibit the viability of the proposed methodology.

In 2015, A. Heydari, M. A. Tavakoli, N. Salim, and Z. Heydari present research around deliberately breaking down and ordering models that recognize survey spam. Next, the examination continues to evaluate them as far as exactness and results. They find that reviews can be arranged into three gatherings that emphasis on techniques to identify spam surveys, singular spammers and gathering spam. Diverse identification methods have various qualities and shortcomings and in this manner support distinctive discovery settings.

In 2014, J. Li, M. Ott, C. Cardie and E. Hovy investigate summed up approaches for distinguishing online misleading assessment spam based on another highest quality level dataset, which is contained information from three distinct areas, every one of which contains three sorts of audits. They Proposed methodology which attempts to catch the general contrast of language utilization among beguiling and honest audits, which they expectation will support clients when settling on buy choices and survey entry administrators.

In 2012, J. Karimpour, A. A. Noroozi and S. Alizadeh propose another strategy to determine this downside by utilizing semi-administered figuring out how to consequently name the preparation information. To do this, they fuse Expectation-Maximization calculation that is a productive and a significant calculation of semi-regulated learning. Trials are completed on the genuine web spam information, which demonstrate the new technique, performs very well.

In 2012, S. Feng, R. Banerjee and Y. Choi made research on syntactic stylometry for double dealing identification, including a to some degree whimsical edge to earlier writing. More than four diverse datasets crossing from the item survey to the article space, they show that highlights driven from Setting Free Grammar (CFG) parse trees reliably improve the recognition execution more than a few baselines that are based just on shallow lexico-syntactic highlights.

In 2011, M. Ott, Y. Choi, C. Cardie and J. T. Hancock studied deceptive feeling spam—invented sentiments that have been purposely composed to sound valid. Incorporating work from brain research furthermore, computational semantics, they create furthermore, contrast three methodologies with distinguishing misleading feeling spam, and at last build up a classifier that is about 90% exact on our highest quality level feeling spam dataset.
In light of highlight investigation of our scholarly models, they furthermore make a few hypothetical commitments, including uncovering a relationship between misleading feelings and creative composing.

In 2010, E. P. Lim, V.-A. Nguyen, N. Jindal, B. Liu and H. W. Lauw distinguish clients creating spam surveys or then again survey spammers. They recognize a few trademark behaviours of audit spammers and model these practices so as to identify the spammers. Specifically, we look to demonstrate the accompanying practices. To begin with, spammers may target specific items or item bunches so as to boost their impact. Second, they will in general veer off from different commentators in their appraisals of items. They propose scoring techniques to quantify the level of spam for every analyst and apply them on an Amazon audit dataset. They at that point select a sub- set of exceptionally suspicious analysts for further examination by our client evaluators with the assistance of an electronic spammer evaluation programming uncommonly produced for client assessment experiments. They demonstrate that the identified spammers have more significant sway on appraisals contrasted and the unhelpful analysts.

In 2001, J. W. Pennebaker, M. E. Francis and R. J. Booth give a proficient and successful strategy for considering the different passionate, intellectual, and basic segments present in people's verbal and composed discourse tests, they initially built up a book examination application called Linguistic Inquiry and Word Count, or LIWC. The first LIWC application was created as a component of an exploratory investigation of language and divulgence. The program is intended to examine individual or numerous language records rapidly and effectively. Simultaneously, the program endeavours to be straightforward and adaptable in its activity, enabling the client to investigate word use in various manners.

III. SYSTEM DESIGN

System design thought as the application of theory of the systems for the development of the project. System design defines the architecture, data flow, use case, class, sequence and activity diagrams of the project development.

A. System Architecture

This architecture diagram illustrates how the system is built and is the basic construction of the software method. Creations of such structures and documentation of these structures is the main responsible of software architecture.

Fig. 1 Architecture Diagram.
B. Data Flow Diagram

Data flow diagram also referred as bubble graph. This diagram is useful for representing the system for all degree of constructions. The figure is differentiated into parts which show maximizing data path & practical aspect.

![Data Flow Diagram](image)

Fig. 2 Data Flow Diagram

The Fig. 2 is the dataflow diagram of proposed system. Firstly, we select customer reviews as datasets from commercial website where we get both genuine and fake reviews done for marketing. Then the dataset is undergoes preprocessing stage where null data, stop words and unnecessary data is removed and dataset is transformed into particular format we say CSV in this project. Next dataset in fed into feature selection process based on this feature classification is done by training classifier using these features.

IV. IMPLEMENTATION

A. Supervised

We employ two different supervised machine learning methods, namely Multinomial Naive Bayes and Support Vector Machine. Both these techniques require labeled data to build classifiers that annotate data as spam or non-spam. Manual labeling of data is very resource intensive, requires a lot of time and training and still the authenticity of the labeled data cannot be determined with certainty. This is one of the major drawbacks of the supervised learning methods and to mitigate the effects of these weaknesses we explore a semi supervised approach for spam detection based on a co-training algorithm.

```
Algorithm 1 Algorithm for detecting spam reviews using SVM
1: documentsList = input dataset
2: for i = 1 to 5 do
3:   training_data, testing_data = Split documentsList
4:   tokenize = CountVectorizer(training_data), fit_transform(training_data)
5:   tfidf = TfidfTransformer().fit_transform(tokenize)
6:   classifier = SGDClassifier().fit(tfidf)
7:   prediction = classifier.predict(testing_data)
8: end for
```

B. Semi Supervised

We use a semi supervised two view co-training algorithm to annotate the large set of unlabeled data from a small labeled data set. The motivation behind implementing this technique is that co-training algorithm takes advantage of the feature split when learning from labeled and unlabeled data. The feature sets we presented are independent of each other as review features are more focused on content and text of reviews. While reviewer features focus on friend count, rating deviation and review count of each reviewer. Another motivation is that manual labeling of data is labor intensive and resource consuming. Labeling even a small set of data set requires a lot of effort and still we are left with a large set of unlabeled data. Co training aims at utilizing this small set of labeled data to annotate the unlabeled reviews. Its approach is to incrementally build classifiers over each feature sets.
It is a two view algorithm, where the first view is to directly detect if the review is spam; the other view is to detect if the author of the review is spammer. The major steps of the algorithm are:

1) For each review it uses two views of feature sets. Review features ‘Fr’ and reviewer features ‘Fu’. ‘L’ is a small set of labeled reviews and ‘U’ is the large set of unlabeled reviews.

2) We learn two classifiers, $C_r$ based on review features and $C_u$ based on reviewer features.

3) $C_r$ labels reviews from $U$ based on $Fr$, $p$ positive and $n$ negative reviews are from $U$, $T_r$ reviews.

4) $C_u$ labels reviews from $U$ based on $Fu$, $p$ positive and $n$ negative reviews are from $U$, $T_u$ reviews.

5) Extract reviews $T_r$ reviews authored by $T_u$ reviews

6) Move $T_u$ reviews from $U$ to $L$.

C. Data Collection Process

The data set utilized by our project primarily comes from the Yelp website. It contains data in JSON format and the data which was of particular use to us contains the following entities: Review Object and User (Reviewer) Object. We have only considered data related to restaurants from yelp dataset ignoring the others. For this we parsed out records corresponding to restaurants only. The following steps were involved in the data collection process

1) Filter out all business objects in the business data file having the category “Restaurant” in the records

2) Filter out all the reviews having the filtered business IDs in them.

3) Filter out all user IDs from the review data file and use that to fetch details of every user from user data file who had reviewed at least one of the restaurants.

The figure 3 shows the dataset content which is in CSV file.

By combining the both supervised and semi supervised method, we introduce the feature set that we used for spam detection. Based on previous works, we selected a set of features that play a key role in determining whether a review is spam or not. This set of features is restricted by the information we could extract from the Yelp website. It can be divided into two categories:

As classifier, we have used Support Vector machines (SVM) and Naive Bayes (NB) classifier with co-training algorithm. Scikit Learn package of Python programming language provides sophisticated library of these classifiers. Hence for our research work, we have used Python with scikit-learn and numpy packages. We have tuned the parameters of the SVM for better results. For supervised classification, we have used Multinomial Naive Bayes and SVM classifiers. We know, Naive Bayes classifier can be implemented where conditional independence property is maintained. As, text comes randomly from user mind, we can’t know what the next line and word is going to be. Hence, Naive Bayes classifier is popularly used in text mining. It is probabilistic method hence it can be used both for classification and regression. It is also very fast to calculate.
V. PERFORMANCE ANALYSIS

We run the co training algorithm using two different classifiers based on Naive Bayes method and SVM and analyze the results obtained using each method. The results obtained from the co-training method are evaluated based on the evaluation metrics of precision, recall and F score.

\[
\text{Precision} = \frac{Sp \cap Sc}{Sp}, \\
\text{Recall} = \frac{Sp \cap Sc}{Sc}, \\
F = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
\]

where, Sc is the set of true review spams, Sp is the set of predicted review spams. The co-training algorithm is simple to implement and the only mathematical background required would be an understanding of the Naive Bayes algorithm and SVM algorithm. As we will observe through the results the co-training algorithm takes advantage of the feature split that is not considered by either Linear SVM or Multinomial Naive Bayes methods and produces superior results.

We evaluate the performance using Precision, Recall and F-Score. Fig 4 and 5 shows the result of MNB and SVM with different feature sets. We observe little variation in the performance of NB method as we increase feature sets, which indicates that the other features are dominated by our four best features. When we include only review features and exclude the reviewer features the F-Score drops the most in both NB and SVM method.

![Fig. 4 Performance Results of MNB method with feature set](image1)

![Fig. 5 Performance results of SVM method with feature set](image2)

Version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.
VI. RESULTS AND OUTPUT SCREENSHOTS

The results of supervised methods are shown in the graph in Figure 7.1. The machine learning method Multinomial Naïve Bayes (NB) performs significantly better as compared with the Linear SVM. We used 26900 reviews as training data set for NB and linear SVM method to build classifiers. We initially selected the four best features by implementing feature selection and observe that the Naive Bayes method clearly outperforms SVM. The four best features suggested by feature selection are Reviewer friend count, Reviewer review count, Bigram measures and Length of the review text.

![Figure 6 CSV dataset file is processing](Image)  
Fig. 6 CSV dataset file is processing

Figure 5 depict the processing of the proposed system after uploading the dataset which is in CSV file format.

![Figure 7 Predicted file is ready to download](Image)  
Fig. 7 Predicted file is ready to download

The figure 6 shows the GUI which shows the small window is pop-up in which we have a interface to download the review predicted file.

The predicted result file which is downloaded is shown in below figure 7 and 8. In fig 7 we have Review content, name, location, date and feature sets counts of particular reviews respectively.

![Figure 8 Part of Predicted Result along with some feature sets count](Image)  
Fig.8 Part of Predicted Result along with some feature sets count

In the below fig 8 we have predicted result which is in red color column and actual review is in green color column.
VII. CONCLUSION

Several semi-supervised and supervised text mining techniques are showed for detecting fake online reviews in this research. We have combined features from several research works to create a better feature set. Also we have tried some other classifier that was not used on the previous work. Thus, it has been able to increase the accuracy of previous semi-supervised techniques done. Here it is also found out that supervised Naive Bayes classifier gives the highest accuracy. This ensures that our dataset is labelled well as we know semi-supervised model works well when reliable labelling is not available.

In future, user behaviours can be combined with texts to construct a better model for classification. Advanced pre-processing tools for tokenization can be used to make the dataset more precise. Evaluation of the effectiveness of the proposed methodology can be done for a larger data set. This research work is being done only for English reviews. It can be done for Bangla and several other languages.

REFERENCES

[1] Pankag Chaudhary, Abhimanyu Tyagi and Santosh Mishra, “Fake Review Detection through Supervised Classification”, Conference on Recent Innovations in Emerging Technology & Science, April 6-7, 2018.

[2] J. K. Rout, A. Dalmia, and K.-K. R. Choo, “Revisiting semi-supervised learning for online deceptive review detection,” IEEE Access, Vol. 5, pp. 1319–1327, 2017.

[3] Chengai Sun, Qiaolin Du and Gang Tian, “Exploiting Product Related Review Features for Fake Review Detection,” Mathematical Problems in Engineering, 2016.

[4] A. Heydari, M. A. Tavakoli, N. Salim, and Z. Heydari, “Detection of review spam: a survey”, Expert Systems with Applications, vol. 42, no.7, pp. 3634–3642, 2015.

[5] J. Li, M. Ott, C. Cardie, and E. Hovy, “Towards a general rule for identifying deceptive opinion spam,” in Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (ACL), 2014.

[6] J. Karimpour, A. A. Noroozi, and S. Alizadeh, “Web spam detection by learning from small labeled samples,” International Journal of Computer Applications, vol. 50, no. 21, pp. 1–5, July 2012.

[7] S. Feng, R. Banerjee, and Y. Choi, “Syntactic stylometry for deception detection,” in Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics: Short Papers, Vol. 2, 2012.

[8] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, “Finding deceptive opinion spam by any stretch of the imagination,” in Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics-Human Language Technologies (ACL-HLT), vol. 1, pp. 309–319, Association for Computational Linguistics, Portland, Ore, USA, June 2011.

[9] E. P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, “Detecting product review spammers using rating behaviors,” in Proceedings of the 19th ACM International Conference on Information and Knowledge Management (CIKM), 2010.

[10] J. W. Pennebaker, M. E. Francis, and R. J. Booth, "Linguistic Inquiry and Word Count: Liwc," vol. 71, 2001.
