JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Spam Review Detection Using Spam Filtering Algorithms

**Dand Shweta B.[1], Late Rohini B.[2]**

DBAT University, Department of CE, M.S.Bidve Engineering College, Latur, Maharashtra, India.[1]Asst. Professor, Department of CE, M.S.Bidve Engineering College, Latur, Maharashtra, India.[2]

***Abstract*: *Generally the people trust on product on the basis of that product reviews and rating. Reviews can affect an organization or profile of a brand. The corporation has to assess market reactions towards its goods. However, it is not straightforward to track and organize popular reviews. Many public views are hard to manually process in social media. A methodology is then required to categories positive or negative public assessments automatically. Online feedback will provide customers with an insight into the consistency, efficiency and advice of the product; this provides prospective buyers with a better understanding of the product. One such unrealized opportunity is the usability of web assessments from suppliers in order to fulfil client requirements by evaluating beneficial feedback. Good and negative reviews play a major role in assessing customer needs and in quicker collection of product input from consumers. Sentiment Analysis is a computer study that extracts contextual data from the text. In this study a vast number of online mobile telephone ratings are analyzed. We classify the text as positive and negative, but we also included feelings of frustration, expectation, disgust, apprehension, happiness, regret, surprise and confidence for spam review detection. This delimited grouping of feedback helps to holistically assess the product, allowing buyers to decide better.***

***Keywords*— *Machine Learning, Social Media, Text Mining, Text Classification, Sentiment Analysis, Online Reviews.***

## I. INTRODUCTION

Many businesses and software sectors store their data in Social networking creation provides the customer with an ability to share his or her views. That means the organization can't monitor the contents of the virtual universe now. Complaints in social media are submitted by customers who are not pleased by a company's services or goods. On the other hand, consumers are still optimistic for a commodity in the social media. This view could affect other potential clients, including positive or negative ones. Potential consumers can find out about a certain product before deciding to purchase goods.

An appraisal of the sentiment is expected to immediately decide whether the feeling is negative or positive. Feeling analyses are a subset of text mining that focuses in the text of a person's feeling, mood and attitude. The fundamental theory of sentiment analysis consists of categorizing the polarity of texts and determining whether they are positive or negative.Sentiment analyses are commonly used as rapid social network growth. For different places public opinion is becoming really critical. There have been some difficulties in collecting public examination.

Many product evaluation pages have recently been published on the Internet. It invites scientists to carry out a consumer review sentiment analysis.

## II. RELATED WORK

Dematis, E. Karapistoli and others[1], proposes an approach which integrates content and usage information to detect fake product reviews. The proposed model exploits both product reviews and reviewers' behavioral traits interlinked by specific spam indicators. In this paper, fine-grained burst pattern detection is employed to better examine reviews generated over "suspicious" time intervals. Reviewer's past reviewing history is also exploited to determine the reviewer's overall "authorship" reputation as an indicator of their recent reviews' authenticity level.

S. Zhou and others [2], adopts a big data analytical approach to investigate the impact of online customer reviews on customer agility and subsequently product performance. authors develop a singular value decomposition-based semantic keyword similarity method to quantify customer agility using large-scale customer review texts and product release notes. Using a mobile app data set with over 3 million online reviews, our empirical study finds that review volume has a curvilinear relationship with customer agility. Furthermore, customer agility has a curvilinear relationship with product performance. this study contributes to innovation literature by demonstrating the influence of firms' capability of utilizing online customer reviews and its impact on product performance. It also helps reconcile inconsistencies found in literature regarding the relationships among the three constructs.

C. Pandey and D. S. Rajpoot[3], Nowadays online reviews play an important role in customer's decision. Starting from buying a shirt from an e-commerce site to dining in a restaurant, online reviews has become a basis of selection. However, peoples are always in a hustle and bustle since they don't have time to pay attention to the intrinsic details of products and services, thus the dependency on online reviews have been hiked. Due to reliance on online reviews, some people and organizations pompously generate spam reviews in order to promote or demote the reputation of a person/product/organization. Thus, it is impossible to identify whether a review is a spam or a ham by the naked eye and it is also impractical to classify all the reviews manually. Therefore, a spiral cuckoo search based clustering method has been introduced to discover spam reviews. The proposed method uses the strength of cuckoo search and Fermat spiral to resolve the convergence issue of cuckoo search method. The efficiency of the proposed method has been tested on four spam datasets and one Twitter spammer dataset.

R. Narayan and others[4], Nowadays with the increasing popularity of Internet, online marketing is going to become more and more popular. This is because; a lot of products and services are easily available online. Hence, reviews about all these products and services are very important for customers as well as organizations. Unfortunately, driven by the will for profit or promotion, fraudsters used to produce fake reviews. These fake reviews written by fraudsters prevent customers and organizations reaching actual conclusions about the products. These fake reviews or review spam must be detected and eliminated so as to prevent deceptive potential customers. In this paper, we have applied supervised learning technique to detect review spam. The proposed work uses different set of features along with sentiment score to build models and their performance were evaluated using different classifiers.

R. Ghai and others[5], reference shows that a review processing method is proposed. Some parameters have been suggested to find the usefulness of reviews. These parameters show the variation of a particular review from other, thus increasing the probability of it being spam. This method introduced classifies the review as helpful or non-helpful depending on the score assigned to the review.

Ch. Xu and J. Zhang[6], paper shows that spam campaigns spotted in popular product review websites (e.g., amazon. com) have attracted mounting attention from both industry and academia, where a group of online posters are hired to collaboratively craft deceptive reviews for some target products. The goal is to manipulate perceived reputations of the targets for their best interests.Detailed The pair wise features are first explicitly utilized to detect group colluders in online product review spam campaigns, which can reveal collusions in spam campaigns from a more fine-grained perspective.

G. Fei, A. Mukherjee and others[7], reference shows that online product reviews have become an important source of user opinions. Due to profit or fame, imposters have been writing deceptive or fake reviews to promote and/or to demote some target products or services. Such imposters are called review spammers. In the past few years, several approaches have been proposed to deal with the problem. In this work, take a different approach, which exploits the burrstones nature of reviews to identify review spammers.

Viswanath, M. Ahmad Bashir and others[8], reference shows that users increasingly rely on crowd sourced information, such as reviews on Yelp and Amazon, and liked post sand ads on Facebook. This has lento market for black hat promotion techniques via fake (e.g., Sybil) and compromised accounts, and collusion networks. Existing approaches to detect such behavior relies mostly on supervised (or semi-supervised) learning over known (or hypothesized) attacks. They are unable to detect attacks missed by the operator while labeling, or when the attacker changes strategy.

H. Li and others[9], in paper online reviews have become an increasingly important resource for decision making and product designing. But reviews systems are often targeted by opinion spamming. Although fake review detection has been studied by researchers for years using supervised learning, ground truth of large scale datasets is still unavailable and most of existing approaches of supervised learning are based on pseudo fake reviews rather than real fake reviews. Working with Dianping1, the largest Chinese review hosting site, present the first reported work on fake review detection in Chinese with filtered reviews from Damping's fake review detection system.

**Challenges In Review Spam Detection**

- The fake reviews look like genuine reviews with a lot of similar keywords.
- Reviews are very subjective in nature and therefore can vary from a small paragraph to a long description.
- There are a number of review sites are available which provide space for writing reviews to reviewers, so it is very difficult to find out that reviewer has actual used the product and wrote the actual review or fake review

## III. PROPOSED METHODOLOGY

The first step is to identify and calculate spammer behavioral features in an unlabeled Amazon review dataset. This calculation is carried out on all dataset reviews based spam review detection using behavioral features method.

**System Architecture:**

The Fig.1 shows the proposed system architecture.

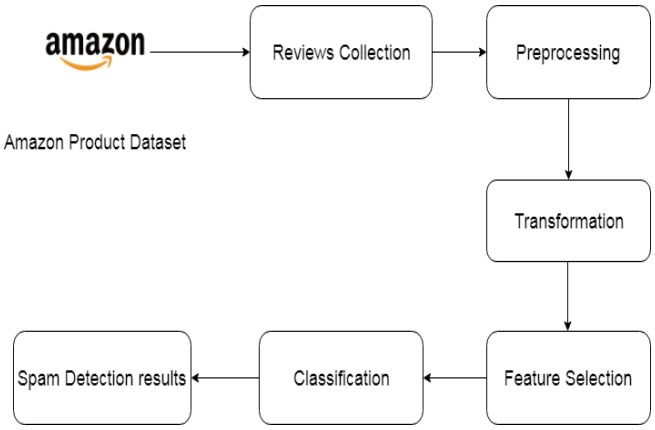


**Fig 1. System Architecture**

- SpamDup framework that is a novel network based approach which models review networks as heterogeneous information networks.
- A new weighting method for spam features is proposed to determine the relative importance of each feature and shows how effective each of features are in identifying spams from normal reviews.
- The SpamDup framework outperforms the state-of-the-art in terms of time complexity, which is heavily influenced by the number of features used to detect a spam review.

Our suggested framework's fundamental notion is to describe a given review dataset as a Heterogeneous Information Network (HIN) and transfer the challenge of spam detection into a classification task. In particular, a model review dataset in which reviews are linked together using various node kinds. The flowchart of the SpamDup framework is shown in Figure 1.

**Mathematical Modeling**

The mathematical model for Spam Detection is as-

S= {I, F, O}

where,

I = Set of inputs

The input consists of set of product reviews. It uses Amazon dataset.

F = Set of functions

F= {F1, F2, F3}

F1: Review Extraction

F2: Reviews processing

F3: Sentiment Analysis

F4: Semantic Analysis

F5: Spam Filtering

O: Spam Reviews

**Algorithm:**

**1. Sentiment Analysis Algorithm:**

Input: Text File (comment or review) T, The sentiment lexicon L.

Output: Smt = {P, Ng and} and strength S where P:

Positive, Ng: Negative, N: Neutral • Initialization: SumPos = SumNeg =0, where,

SumPos: accumulates the polarity of positive tokens tismt in T,

SumNeg: accumulates the polarity of negative tokens ti-smt in T,

Begin

1.For each ti∈ T do

2.Search for ti in L

3. If ti∈ Pos−list then

4. SumPos ← SumPos + ti−smt

5. Else ifti∈ Pos−list then

6. SumNeg ← SumNeg + ti−smt

7. End If

8. End For

9. If SumPos> |SumNeg| then

10. Smt = P

11. S=SumPos/(SumPos+SumNeg)

12. Else If SumPos< |SumNeg| then

13. Smt = Ng

14. S=SumNeg/(SumPos+SumNeg)

15. Else

16. Smt = N

17. S=SumPos/(SumPos+SumNeg)

18. End If End

**2. Latent Semantic Analysis Algorithm**

1) Step 1: Documents should be prepared in the following way:

• Exclude trivial words as well as low- frequency terms.

• Conflate terms with techniques like stemming or lemmatization.

2) Step 2: A term-frequency matrix (A) must be created that includes the occurrences of each term in each document.

3) Step 3: Singular Value Decomposition (SVD):

• Extract least-square principal components for two sets of variables: set of terms and set of documents.

• SVD products include the term eigenvectors U, the document eigenvectors V, and the diagonal matrix of singular values P.

4) Step 4: From these, factor loadings can be produced for terms UP and documents VP

**3. Netspam Algorithm**

following algorithm is taken from references no [11];

• Input: review–dataset, spam-feature-list, pre–labeledreviews
• Output: features importance (W), spamicity probability (Pr) • Process:
• Step 1: u, v: review, yu: spamicity probability of review u
• Step 2: f(xlu): initial probability of review u being spam
• Step 3: Pl: metapath based on feature l, L: features number
• Step 4: n: number of reviews connected to a review
• Step 5: mPl u: the level of spam certainty
• Step 6: mPl u, v: the metapath value
• Step 7: Prior Knowledge
• Step 8: if semi-supervised mode
• Step 9: if u ∈ pre−labeled−reviews
• Step 10: yu = label(u)
• Step 11: else
• Step 12: yu = 0
• Step 13: else unsupervised mode
• Step 14: yu = 1 LPL l=1 f(xlu)
• Step 15: Network Schema Definition
• Step 16: schema = defining schema based on spam feature-list
• Step 17: Metapath Definition and Creation
• Step 18: for pl ∈ schema
• Step 19: for u, v ∈ review−dataset
• Step 20: mpl u = |s × f(xlu)| s
• Step 21: mpl v = |s × f(xlv)| s
• Step 22: if mpl u = mpl v
• Step 23: mppl u, v = mpl u
• Step 24: else
• Step 25: mppl u, v = 0
• Step 26: Classification - Weight Calculation
• Step 27: for pl ∈ schemes
• Step 28: Wpl = Pn r=1Pn s=1 mp pl r,s × yr × ysP n r=1Pn s=1 mp pl r,s
• Step 29: Classification - Labeling
• Step 30: for u, v ∈ review−dataset
• Step 31: Pru,v = 1−QL pl=1 1−mppl u,v ×Wpl
• Step 32: Pru = avg (Pru,1, Pru, 2..., Pru, n)
• Step 33: return (W, Pr)

**Scope and Major Constraints**

- It identifies spam and spammers as well as different type of analysis on this topic.
- Written reviews also help service providers to enhance the quality of their products and services.
- It identifies the spam user using positive and negative reviews in online social media.
- This framework displays only trusted reviews to the users.

## RESULT AND DISCUSSION

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.0 backend database and Jdk 1.7. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

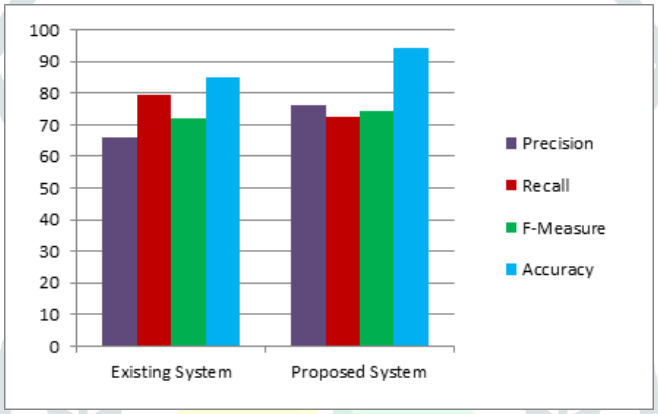


Fig 2.Performance Analysis between existing and proposed system

The proposed SpamDup framework time complexity is O(e^2 n). The SpamDup framework accuracy is 94.06% which is better than exiting Algorithm accuracy is 85.14% on using product dataset.

## CONCLUSION

Sentiment Analysis is a case study that looks at the feeling, mood, entropy or feelings of people. This paper addresses a basic issue of the study of feelings and the classification of feelings of polarity for spam review detection. Data was compiled from online product reviews of Amazon.com. A method known as the categorization of emotion polarity along with through explanations of each phase was proposed. These measures include pre-processing, pre-filtering, partitioning, data consistency. Functionality that include machine learning expertise. Much work has been done in opinion mining and consumer evaluation in the form of a study of documents, sentences, and features. Opinion Mining can become a most interesting field of study for potential preferences by using a number of found function expressions derived from the reviews. More novel and successful approaches need to be invented to address the existing difficulties of mining opinion and sentiment analysis.

## REFERENCES

[1] Dematis, E. Karapistoli, and A. Vakali, ‘‘Fake review detection via exploitation of spam indicators and reviewer behavior characteristics,’’ in Proc. Int. Conf. Current Trends Theory Pract. Inform. Cham, Switzerland: Edizioni Della Normale, 2018, pp. 581–595.

[2] S. Zhou, Z. Qiao, Q. Du, G. A. Wang, W. Fan, and X. Yan, ‘‘Measuring customer agility from online reviews using big data text analytics,’’ J. Manage. Inf. Syst., vol. 35, no. 2, pp. 510–539, Apr. 2018.

[3] C. Pandey and D. S. Rajpoot, ‘‘Spam review detection using spiral cuckoo search clustering method,’’ Evol. Intell., vol. 12, no. 2, pp. 147–164, Jun. 2019.

[4] R. Narayan, J. K. Rout, and S. K. Jena, ‘‘Review spam detection using opinion mining,’’ in Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Singapore: Springer, 2018, pp. 273–279.

[5] R. Ghai, S. Kumar, and A. C. Pandey, ‘‘Spam detection using rating and review processing method,’’ in Smart Innovations in Communication and Computational Sciences. Singapore: Springer, 2019, pp. 189–198.

[6] Ch. Xu and J. Zhang,” Combating product review spam campaigns via multiple heterogeneous pairwise features”, In SIAM International Conference on Data Mining, 2014.

[7] G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh, “Exploiting bustiness in reviews for review spammer detection”, In ICWSM, 2013.

[8] Viswanath, M. Ahmad Bashir, M. Crovella, S. Guah, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, “Towards detecting anomalous user behavior in online social networks”, In USENIX, 2014.

[9] H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao,” Spotting fake reviews via collective PU learning”, In ICDM, 2014.