ISSN: 0976-3031

*Available Online at http://www.recentscientific.com*

**CODEN: IJRSFP (USA)**

*International Journal of Recent Scientific Research*
*Vol. 14, Issue, 06 (A), pp. 2267-2271, June, 2023*

**International Journal of Recent Scientific Research**

**DOI: 10.24327/IJRSR**

## Research Article

# HYBRID SUPPORT VECTOR MACHINE ALGORITHM FOR TWITTER FAKE ACCOUNT DETECTION

**Simbahan KP, Enriquez JM, Agustin V, Dioses R and Regala R**

Department of Computer Science, Pamantasan ng Lungsod ng Maynila, Manila, Philippines

**DOI: http://dx.doi.org/10.24327/ijrsr.2023.1406.0683**

**ARTICLE INFO**

***Article History:***

Received 13th March, 2023
Received in revised form 11th April, 2023
Accepted 8th May, 2023
Published online 28th June, 2023

***Keywords:***

Data Preprocessing, Machine Learning, Support Vector Machine, Twitter Fake Account Detection.

**ABSTRACT**

This study addressed the issue of internet disinformation by examining the identification of fake Twitter accounts. To tackle the increase in fake accounts on Twitter, detecting technologies needed to be developed. However, Traditional SVM algorithms had limitations in noisy scenarios, underperformed with more features than training data samples, and required longer training times for large datasets. To overcome these limitations and improve accuracy in recognizing fake Twitter accounts, this thesis employed a Hybrid SVM algorithm incorporating Kendall Rank Correlation, PCA, and LLE. The proposed approach recommended a Hybrid SVM algorithm, combining approaches to enhance classification performance. It used Kendall Rank Correlation to capture data correlations, PCA to reduce dimensionality, and LLE to minimize computational complexity, lowering SVM training time. After extensive testing, the proposed Hybrid SVM model demonstrated exceptional performance, achieving an accuracy and precision rate of approximately 98%. Consistent recall performance enabled reliable identification of fake accounts. The findings highlighted the effectiveness of the suggested method in spotting fake accounts and emphasized the importance of feature selection and dimensionality reduction in improving classification performance. The study contributed to social media analytics and internet security by offering insights and suggestions to address the widespread problem of fake Twitter accounts.



## INTRODUCTION

Twitter, a widely popular social media platform launched in 2006, has gained immense popularity and boasts a substantial user base of approximately 290.5 million monthly users as of 2019, with projections indicating further growth to over 340 million users by 2024 (Dixon, 2022). However, the platform's increasing popularity has also led to the rapid increase of fake accounts, which pose significant challenges. These fraudulent accounts are often utilized as tools for eroding trust in social networks, engaging in mass theft of personal data, and orchestrating information injections, among other illicit activities (Pasieka, 2021). Consequently, the erosion of trust in Twitter's security and reliability has the potential to drive its users away from the platform.

In the realm of fake account detection, the Support Vector Machine (SVM) algorithm has emerged as a popular choice for classifying fake accounts across various social media platforms. SVM is a supervised machine learning method that analyzes data for classification and regression analysis, effectively sorting data into distinct categories. By outputting a map of sorted data with maximized margins between the two categories, SVM has found applications in text categorization, image classification, handwriting recognition, and numerous scientific domains.

Other machine learning algorithms were also been used by past studies. In the study of (Ersahin *et al*., 2017) they used Naïve Bayes Algorithm as a classification method for detecting fake accounts on Twitter. They preprocessed their dataset using a supervised discretization technique named Entropy Minimization Discretization (EMD) on numerical features analyzed by Naïve Bayes Algorithm. The study also stated that feature selection can also improve the results and it is intended to make a study on this area in a short time. The study produced an accuracy score of 90.9% after performing the discretization method with their control giving an accuracy score of 86.1%. In the study of (Alom *et al*., 2018) they used seven machine learning algorithms namely: kNearest Neighbor (k-NN), Decision Tree (DT), Naive Bayesian (NB), Random Forest (RF), Logistic Regression (LR), Support Vector Machine (SVM), and Extreme Gradient Boosting (XGBoost) to classify spam and legitimate users. The findings in their study is that Random Forest (RF) gives a better accuracy result of 91% compared to other algorithms. It should be noted that they did not use data preprocessing before conducting the experiment.

**Corresponding author:* **Simbahan KP**
Department of Computer Science, Pamantasan ng Lungsod ng Maynila, Manila, Philippines

Given these various studies and their results, this study focused on the SVM algorithm as a classification model to determine fake accounts on Twitter given that the results from the discussed studies show SVM performing better when data preprocessing is applied. However, SVM itself is not without limitations. Particularly, it encounters challenges when dealing with noisy data, datasets with a large number of features, and computationally complex calculations, often resulting in extensive processing time for training the algorithm. Past studies have indicated that SVM's performance tends to suffer in datasets with higher levels of noise, as well as when the number of features per data point exceeds the number of training data samples. Additionally, the algorithm's computational complexity can lead to prolonged training times, especially when confronted with intricate calculations (Patil, 2022).

Given the problems that are associated with SVM, this paper proposed the integration of a Hybrid Support Vector Machine Algorithm that incorporates various data preprocessing techniques. The program will specifically use dimension reduction methods like Principal Component Analysis (PCA) and Locally Linear Embedding (LLE), and feature selection methods like Kendall Rank Correlation. By combining these methods, SVM's performance has been improved overall while simultaneously addressing its drawbacks.

By implementing feature selection and dimension reduction techniques, the proposed Hybrid Support Vector Machine Algorithm overcame the limitations of SVM. With the utilization of Kendall Rank Correlation for feature selection, along with PCA and LLE for dimension reduction, it seeks to improve the classification accuracy and mitigate the impact of noise and high-dimensional datasets. The aim of the proposed combination of algorithms is to enhance the speed and accuracy of Twitter's fake account detection while also making a contribution to the field of social media platform security as a whole.

## METHODOLOGY

### *Requirement Gathering*

The datasets used in this study originated from (Cresci *et al*., 2017)'s research paper, which offers a thorough and painstakingly curated dataset extracted from Twitter using the Twitter API. This dataset was made publicly available with the explicit objective of facilitating further research in areas like the present research, by giving researchers a trustworthy and organized resource that allows for investigating various aspects of Twitter data.

**Table 1** Datasets used in this study

| DATASET | NUMBER OF USERS |
|---|---|
| Genuine accounts | 3,474 |
| Social spambots #2 | 3,457 |
| TOTAL: | 6,931 |

Table 1 shows the name of the datasets used in this study from (Cresci *et al*., 2017). The datasets combined will give 6,931 users. All data from both datasets are in the English language.

**Table 2** List of features used in this study from the datasets

| Features used in the study | Amount |
|---|---|
| statuses_count | 6,931 |
| followers_count | 6,931 |
| friends_count | 6,931 |
| favourites_count | 6,931 |
| listed_count | 6,931 |
| label_count | 6,931 |

Table 2 shows the list of features used in this study from the datasets of (Cresci *et al*., 2020). The given features represent a significant importance in determining fake accounts from genuine ones. To understand each feature more here is a detailed explanation:

**Statuses_count** - number of tweets a specific user tweeted from the creation of their account to the date the data is collected.

**Followers_count** - number of followers a specific user has from the creation of their account to the date the data is collected.

**Friends_count** - number of people a specific user is following from the creation of their account to the date the data is collected.

**Favourites_count** - number of tweets a specific user marked as favourite from the creation of their account to the date the data is collected.

**Listed_count** - number of lists a specific user is in or they created from the creation of their account to the date the data is collected.

**Label_count** - generated after combining both datasets wherein 0 is given to all users from the genuine accounts dataset and 1 for the users from the social spambot#2 dataset. Hence, 0 is genuine users and 1 is fake users.

### *Application of Kendall Rank Correlation*

The first method is the addition of a preprocessing technique, specifically, a feature selection model called Kendall Rank Correlation. This made it possible to evaluate how features and the target variable rank similarly in unseen data, assuring consistency with the correlation patterns in the training data.

### *Reduction of Feature Dimensionality with the Application of Principal Component Analysis*

The second method is the addition of a dimensionality reduction technique, specifically, Principal Component Analysis. This reduced the number of features while preserving essential information by identifying the most significant variations in the data.

### *Application of Locally Linear Embedding*

The third method is the addition of another dimensionality reduction technique, specifically, Locally Linear Embedding. This enabled an assessment of how features and the target variable rank similarly in unseen data, guaranteeing consistency with the correlation patterns identified in the training data. This helped reduce the dimensionality of the dataset, which in turn helped shorten training time. It also preserved the neighborhood structure and local correlations in the data.

### *Application of Support Vector Machine Algorithm*

The Support Vector Machine approach is utilized in this study as the machine learning algorithm to identify fake accounts from Twitter and to find a hyperplane that maximizes the separation margin between two classes.

### *Results Evaluation*

The proposed Hybrid SVM classifier is evaluated once trained. Its effectiveness is evaluated using the correlation matrix, to

describe the performance of the classification model. Terms used with a confusion matrix for binary classifiers are: True-positive (TP): n of accounts correctly identified as Fake. False-positive (FP): n of accounts incorrectly identified as Fake. True-negative (TN): n of accounts correctly identified as Real. False-negative (FN): n of accounts incorrectly identified as Real. These can be further used to find the following metrics to determine the effectiveness of each model:

**Precision:** The ratio of true positives to values that were accurately anticipated. It is defined in Eq.1, given as follows:

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad \textbf{(1)}$$

**Recall:** The proportion of real positives to all positives. It is defined in Eq2, given as follows:

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad \textbf{(2)}$$

**Accuracy:** Using the accuracy parameter, the accurate identification of accounts from the corpus is determined. It is defined in Eq.3, given as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad \textbf{(3)}$$

In addition to the previous metrics:

**Training Time:** By deducting the beginning time of the training process from the finish time, the training time can be computed. It is defined in Eq.4.

$$\boldsymbol{Training\ Time = End\ Time - Start\ Time} \quad (4)$$

## RESULTS

### *Performance Metrics*

**Table 3** 10 Instances of Performance Metrics Results

| | Existing SVM Algorithm | | | | Proposed Hybrid SVM Algorithm | | | |
|---|---|---|---|---|---|---|---|---|
| ***RUN*** | ***Accuracy*** | ***Precision*** | ***Recall*** | ***Training Time (sec)*** | ***Accuracy*** | ***Precision*** | ***Recall*** | ***Training Time (sec)*** |
| **1** | 0.946647 | 0.918424 | 0.976083 | 0.658975 | 0.982696 | 0.987897 | 0.976083 | 0.385986 |
| **2** | 0.946647 | 0.918424 | 0.976083 | 0.601003 | 0.982696 | 0.987897 | 0.976083 | 0.444988 |
| **3** | 0.946647 | 0.918424 | 0.976083 | 0.595984 | 0.981975 | 0.986404 | 0.976083 | 0.389200 |
| **4** | 0.946647 | 0.918424 | 0.976083 | 0.592984 | 0.981975 | 0.986404 | 0.976083 | 0.463008 |
| **5** | 0.946647 | 0.918424 | 0.976083 | 0.634983 | 0.981975 | 0.986404 | 0.976083 | 0.303991 |
| **6** | 0.946647 | 0.918424 | 0.976083 | 0.588963 | 0.981975 | 0.986404 | 0.976083 | 0.511006 |
| **7** | 0.946647 | 0.918424 | 0.976083 | 0.627978 | 0.981975 | 0.986404 | 0.976083 | 0.190995 |
| **8** | 0.946647 | 0.918424 | 0.976083 | 0.606988 | 0.981975 | 0.986404 | 0.976083 | 0.177996 |
| **9** | 0.946647 | 0.918424 | 0.976083 | 0.590967 | 0.981975 | 0.986404 | 0.976083 | 0.169018 |
| **10** | 0.946647 | 0.918424 | 0.976083 | 0.601020 | 0.982696 | 0.987897 | 0.976083 | 0.500988 |
| average | 0.946647 | 0.918424 | 0.976083 | 0.609926 | 0.982329 | 0.98713 | 0.976083 | 0.369957 |

Table 3 shows the performance metrics results of 10 instances of the existing Support Vector Machine Algorithm and the proposed Hybrid Support Vector Machine Algorithm. It offers significant positive differences in accuracy and precision. Averaging ten cases, the accuracy of the existing algorithm in determining fake accounts on Twitter is 94.66%. The proposed hybrid algorithm surpassed the accuracy results giving an average of 98.23% accuracy. Averaging ten instances, the precision of the existing algorithm gives an average of 91.84%, whereas the proposed hybrid algorithm gives an average of 98.71%. As for the recall results, it shows no difference in value and retains the 97.60% from the existing algorithm and the proposed hybrid algorithm. Lastly, the training time also shows significant positive differences where in 10 instances, the average training time of the current algorithm is 0.609 seconds while the proposed hybrid algorithm gives an average of 0.370 seconds.

### *Application of Kendall Rank Correlation Results*

The initial goal, is to use Kendall Rank Correlation, a feature selection technique, to examine statistical correlations and find relevant features in order to overcome the obstacles given by noisy datasets and potential misclassification. We conducted a performance metric comparison between the existing SVM method and an SVM algorithm preceded by the application of Kendall Rank Correlation. The results of this comparison are presented in Table 4

**Table 4** Comparison Table SVM vs SVM-KRC

| | Accuracy | Precision | Recall | Training Time |
|---|---|---|---|---|
| Existing SVM | 0.946647 | 0.918424 | 0.976083 | 0.611017 |
| SVM with Kendall Rank Correlation | 0.948810 | 0.922316 | 0.976083 | 0.608995 |

Table 4 shows the comparison of the performance metrics results of the existing SVM algorithm vs. SVM with Kendall Rank Correlation. The results show a minor increase in accuracy from 94.6% to 94.8% and precision from 91.8% to 92.2%. As for the recall results, both show the same result of 97.6%. The training time also shows a minor decrease compared to the existing algorithm.

### *Reduced Feature Dimensionality with Application of Principal Component Analysis*

The second objectives is to reduce feature dimensionality using Principal Component Analysis. The results of this comparison are presented in Table 5.

**Table 5** Comparison Table SVM vs SVM-KRC vs SVM-KRC-PCA

| | Accuracy | Precision | Recall | Training Time |
|---|---|---|---|---|
| Existing SVM | 0.946647 | 0.918424 | 0.976083 | 0.611017 |
| SVM with Kendall Rank Correlation | 0.948810 | 0.922316 | 0.976083 | 0.608995 |
| SVM with Kendall Rank Correlation and PCA | 0.950252 | 0.924929 | 0.976083 | 0.819013 |

Table 5 shows the comparison of the performance metrics results of the existing SVM algorithm vs SVM with Kendall Rank Correlation vs SVM with Kendall Rank Correlation and Principal Component Analysis. The results show a minor significant increase in accuracy and precision. As for the recall the results show no difference. The results of the training time however showed a significant increase from 0.611017 seconds (SVM), 0.608995 seconds (SVM-KRC) to 0.819013 seconds.

The increase in training time could be due to the additional computations that were involved because of the addition of PCA.

***Applying Locally Linear Embedding***

The third goal is to simplify the data so that it can be processed or trained more quickly. To accomplish this, the technique that is utilized is Locally Linear Embedding after initially reducing feature dimensionality using Principal Component Analysis. The results of this comparison are presented in Table 6.

**Table 6** Comparison Table SVM vs SVM-KRC vs SVM-KRC-PCA vs SVM-KRC-PCA-LLE

| | Accuracy | Precision | Recall | Training Time |
|---|---|---|---|---|
| Existing SVM | 0.946647 | 0.918424 | 0.976083 | 0.611017 |
| SVM with Kendall Rank Correlation | 0.948810 | 0.922316 | 0.976083 | 0.608995 |
| SVM with Kendall Rank Correlation and PCA | 0.950252 | 0.924929 | 0.976083 | 0.819013 |
| SVM with Kendall Rank Correlation, PCA, and LLE | 0.982696 | 0.987897 | 0.976083 | 0.215019 |

Table 6 shows the comparison of the performance metrics results of the existing SVM algorithm vs. SVM with Kendall Rank Correlation vs. SVM with Kendall Rank Correlation and Principal Component Analysis vs. SVM with Kendall Rank Correlation, Principal Component Analysis, and Locally Linear Embedding. The results show a significant increase in accuracy and precision. The recall still shows the same value compared to every algorithm used in this study. The training time shows a significant decrease from 0.819013 seconds (SVM-KRC-PCA) to 0.215019 seconds. This shows that the study is successful in simplifying the data to have a shorter training time without sacrificing any inaccuracy towards the results.

## DISCUSSION

The study produced a Hybrid Support Vector Machine Algorithm to determine fake accounts on Twitter, a popular social media platform. Using the datasets listed in this study, the hybrid algorithm outperformed the existing Support Vector Machine Algorithm in distinguishing fake accounts from authentic ones. When compared to the existing algorithm, the methods discussed in this study have demonstrated improved accuracy, precision, and training time scores while retaining recall scores from the original SVM. The results highlight the most significant results and conclusions from the study's implementation.

Based on the findings and limitations of this research, several recommendations are put forth to enhance and expand upon the existing work:

1. Increase Dataset Size: To further validate and generalize the findings, future studies should think about gathering larger datasets. Researchers can increase the reliability and validity of the results by increasing the dataset to provide a more thorough representation of the target population.
2. Augment Instance Numbers: It is advised to increase the number of instances employed in this study's performance metrics analysis. An evaluation of the precision and efficacy of the suggested solution would be more robust and reliable if there were more cases.
3. Incorporate Additional Features: Future research should investigate the incorporation of variables other than numerical attributes in order to increase the specificity of fake account categorization. The accuracy and precision of the classification model could be improved by using other elements such as textual, temporal, or network-based properties.
4. Explore Advanced Data Preprocessing Techniques: The efficiency of the fraudulent account detection system might be further optimized by researching different data preparation methods. In particular, investigating methods that place a higher priority on recall outcomes would be helpful in identifying a greater percentage of fake accounts while avoiding false negatives.

By incorporating these recommendations into future studies, researchers can enhance the accuracy, reliability, and applicability of fake account detection techniques on Twitter. This will contribute to the advancement of the field and provide valuable insights for addressing the ever-evolving challenge of identifying fake accounts on social media platforms.

## CONCLUSION

This study focused on improving the efficiency and accuracy of SVM through the application of specific techniques and objectives that can potentially lead to the development of a solution to optimize the algorithm. Given that three specific objectives are formulated in order to produce a better algorithm for future researchers, Twitter users, and personnel: When compared to the existing algorithm, the use of Kendall Rank Correlation as the feature selection model to tackle the problem of data noise by selecting significant features to avoid misclassification resulted in positive minor improvements. The use of Principal Component Analysis to reduce feature dimensionality resulted in significant improvements. Dimension reduction was found to be an important aspect in increasing the efficiency and accuracy of SVM. The use of Locally Linear Embedding as an additional dimension reduction technique has also been demonstrated to be an important contributor in significantly enhancing SVM's efficiency, accuracy, and training time. These techniques, applied to improve the SVM's accuracy in classifying fake Twitter accounts, provided a better hybrid algorithm.

## References

Dixon S. Number of Twitter users worldwide from 2019 to 2024; [online]. 2022 [cited 2022 December 14]; Available from https://www.statista.com/statistics/303681/twitter-users-worldwide/

Pasieka, N., Kulynych, M., Chupakhina, S., Romanyshync, Y., & Pasieka, M. (2021, September). Harmful Effects of Fake Social Media Accounts and Learning Platforms. In Proceedings of the 2021 International Conference on Machine Learning and Data Science (pp. 24-30). CEUR-WS.org.

Ersahin, B., Aktas, O., Kilinc, D., & Akyol, C. (2017, October). Twitter fake account detection. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 1-6). doi:10.1109/ubmk.2017.8093420.

Alom, Z., Carminati, B., & Ferrari, E. (2018). Detecting Spam Accounts on Twitter. In Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 1191-1198). IEEE. doi:10.1109/ASONAM.2018.850849.

Patil A. Disadvantages of SVM. OpenGenus IQ: Computing Expertise & Legacy; [online]. 2022. Available from https://iq.opengenus.org/disadvantages-of-svm/

Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race. In Proceedings of the 26th International Conference on World Wide Web Companion (WWW '17 Companion) (pp. 963-972). Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee.

**How to cite this article:**

Simbahan KP *et al*.2023, Hybrid Support Vector Machine Algorithm For Twitter Fake Account Detection. *Int J Recent Sci Res.* 14(06), pp. 2267-2271. DOI: http://dx.doi.org/10.24327/ijrsr.2023.1406.0683

*******