

Classification benchmarking of fake account datasets using machine learning models and feature selection strategies

Danilo Caivano², Mary Cerullo¹, Domenico Desiato^{2,*} and Giuseppe Polese¹

¹Department of Computer Science, University of Salerno, via Giovanni Paolo II n.132, 84084 Fisciano (SA), Italy

²Department of Computer Science, University of Bari Aldo Moro, via Edoardo Orabona n.4, 70125 Bari (BA), Italy

Abstract

Social network platforms are highly used for social interactions, and due to their increasing number of registered users, it is crucial to verify the authenticity of such accounts and the data they generate. In particular, the phenomenon of malicious accounts represents a crucial aspect that social network platforms have to deal with, and it is crucial to develop new methodologies and strategies to discriminate against malicious accounts automatically. To this end, data from social network platforms plays a crucial role in defining analytical activities devoted to fake account discrimination. In this proposal, we organized and cleaned fake account datasets collected by online sources and provided classification results obtained employing machine learning models and feature selection strategies. Moreover, we extend classification results by using a new proposed fake accounts dataset collected through data crawling activity. Experimental results produced by employing several machine learning models and feature selection techniques on the fake account datasets reveal discrimination improvements when feature selection strategies are exploited. Our proposal aims to support stakeholders, data analysts, and researchers by providing them with fake account datasets cleaned and organized for analytical activities, together with statistical classification results obtained using machine learning models and feature selection strategies.

Keywords

Data Analytics, Fake accounts, Machine Learning, Feature selection, Social networks

1. Introduction

Social networks have simplified how people communicate and exchange information globally. In particular, social interaction platforms such as Instagram, Twitter, Tumblr, etc., have improved the dynamics of human interaction, impacting the daily lives of their users and the entire society.


In social network platforms, it is crucial to monitor the popularity of a profile. In particular, the number of friends or followers significantly determines the profile's influence and reputation. Social network profiles with a large following are considered more influential and attractive to better-paid advertisements. A common practice of several social network users is to buy fake followers to appear more influential. Users are also stimulated by the meagre price (a few

AVI 2024: 17th International Conference on Advanced Visual Interfaces, 3–7 June 2024, Arenzano, Italy

*Corresponding author.

✉ danilo.caivano@uniba.it (D. Caivano); m.cerullo13@studenti.unisa.it (M. Cerullo); domenico.desiato@uniba.it (D. Desiato); gpolese@unisa.it (G. Polese)

ORCID 0000-0001-5719-7447 (D. Caivano); 0000-0002-6327-459X (D. Desiato); 0000-0002-8496-2658 (G. Polese)

 © 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

dollars for hundreds of fake followers) fake followers may be bought. Of course, such practice might be considered harmless if used to support individual vanity but dangerous if used to make an account more reliable and influential. For example, spammers can use fake followers to promote products, trends, and fashions by compromising the integrity of the social network platforms [1]. Moreover, phishing campaigns are commonly spread by exploiting fake accounts created ad-hoc with many followers and following to appear trustable, and in most cases, the users attracted by such numbers are defrauded [2].

Many anomalous accounts, such as Spammers, Bots, Cyborgs, and Trolls, are disseminated on social network platforms. In particular, spammers try to share malicious content or dangerous links. Bots produce accounts to simulate human behaviour, trying to perform typical human actions automatically. In contrast, Cyborgs are defined by humans and are not necessarily malicious.

In this proposal, we focus on the discrimination of fake accounts on social network platforms. In particular, we present an extensive empirical evaluation of fake account datasets available in online sources. In detail, we employ several machine learning models and evaluate their capabilities in terms of fake account discrimination. Further, we exploit different feature selection techniques to enhance models discrimination performances.

The general idea of our proposal is to offer stakeholders, data analysts, and researchers who work to define new methodologies for malicious account discrimination the possibility of quickly accessing fake account datasets that have been cleaned and organized for analytical activities. Moreover, we offer comparative results in terms of fake account discrimination. To this end, the usage of machine learning models is motivated by the fact that we want to provide a baseline for classification performances. In contrast, feature selection techniques are employed to improve the computed baseline. Moreover, we highlight the combinations of feature selection and model to adopt on the specific dataset to achieve the best classification results. Additionally, we extend our analysis by using a new fake account dataset collected by exploiting data crawling activity.

In summary, the main contributions of our proposal are i) fake account datasets collected by online sources cleaned and organized for analytical activities, ii) baseline and improved results of classification performances using machine learning models and feature selection techniques, and iii) a new fake account dataset collected through data crawling activity.

The remainder of the paper is organized as follows. Section 2 reports relevant works concerning fake account discrimination, whereas Section 3 presents our methodology. Section 4 shows results, and conclusions and future directions are provided in Section 5.

2. Related work

A key factor to be monitored for social network platforms is the identification of malicious accounts. The automatic collection of social network accounts has been addressed in [3]. In particular, the authors developed an ad-hoc web crawler to automatically collect and filter public Twitter accounts and organize the data in testing and training datasets. Moreover, a multi-layer perceptron neural network has been modelled and trained in over nine features characterizing a fake account. Another machine learning approach is provided in [4]. In

particular, the authors propose DeepProfile, which performs account classification through a dynamic CNN to train a learning model, which exploits a novel pooling layer to optimize the neural network performance in the training process. Moreover, In [5], content and metadata at the tweet level have been exploited for recognizing bots employing a deep neural network based on contextual long short-term memory (LSTM). In particular, this approach extrapolates contextual features from user metadata and uses the LSTM deep nets to process the tweet text, yielding a model capable of obtaining high classification accuracy with little data.

Statistical text analysis is exploited in a novel general framework to discover compromised accounts [6]. The framework relies on the consideration that an account's owner uses his/her profile in a way that is entirely different from the same account when it is hacked, enabling a syntactic analyzer to identify the features used by hackers (or spammers) when they compromise a genuine account. Thus, a language modelling algorithm is used to extrapolate the similarities between language models of genuine users and those of hackers/spammers to characterize hackers' features and use them in supervised machine learning approaches.

Further approaches devoted to fake account discrimination also considered feature engineering and/or selection issues [7, 8]. Nevertheless, most of the proposals, including a feature engineering process, rely on domain experts or include manual work for characterizing meaningful features that permit a classifier to work with high accuracy. For instance, in [9], the authors have enumerated the main characteristics to discriminate a fake account from a genuine one. In particular, by manually examining different types of accounts, they extracted a set of features to highlight the characteristics of malicious accounts. Moreover, they analyzed the liking behaviour of each account to build an automated mechanism to detect fake likes on Instagram. Furthermore, In [10], the authors propose a novel technique to discriminate real accounts on social networks from fake ones. Their technique exploits knowledge automatically extracted from big data to characterize typical patterns of fake accounts. Additionally, in [11], the authors extend the previous work by exploiting data correlations to develop a new feature engineering strategy to augment the social network account dataset with additional features, aiming to enhance the capability of existing machine learning strategies to discriminate fake accounts.

Compared to the fake account discrimination approaches described above, in this proposal, we release cleaned and organized fake account datasets collected from online sources for analytical activities. To this end, we exploit machine learning models and feature selection techniques to compute baseline and improved classification performance results. Finally, we extend our analysis by exploiting a new fake account dataset collected by data crawling activity.

In what follows, we introduce our methodology steps to compute classification results.

3. Methodology

This section presents our approach for computing data utility metrics over malicious account datasets. In particular, in the first phase of the approach, we employ machine learning models to classify malicious datasets and compute data utility metrics over them. Moreover, in the second step, we employ feature selection strategies over malicious account datasets to improve the discrimination performances of machine learning models.

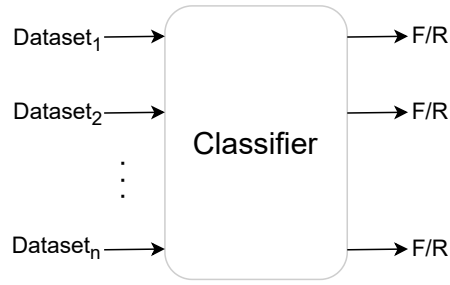


Figure 1: Classifier working on malicious accounts datasets.

The first phase of our approach (represented by Figure 1) is targeted to compute data utility metrics over malicious account datasets. In particular, we exploit machine learning models to compute classification metrics over each dataset in order to yield a first baseline that describes all datasets in terms of data utility.

The second phase of our approach (represented by Figure 2) is targeted to improve data utility metrics obtained in the previous step. In particular, we employ feature selection strategies over each dataset to improve the discrimination performances of machine learning models.

In what follows, we introduce malicious accounts datasets, machine learning models, feature selection strategies employed, and results obtained.

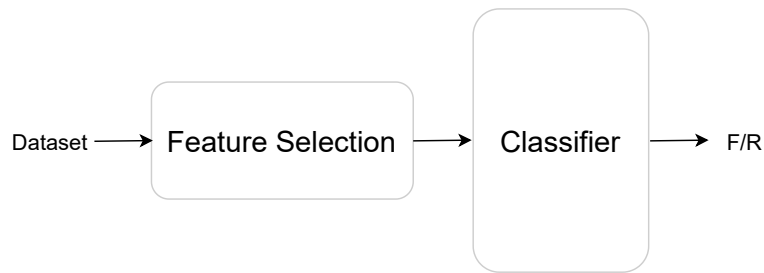


Figure 2: Features selection and classification.

4. Experimental Evaluation

In this section, we describe the datasets employed in our study and the data preparation techniques exploited to organize and clean them for data analytics activities. Next, we provide details concerning the machine learning models, feature selection strategies, and the proposed fake account dataset. Lastly, we present classification results achieved by using machine learning models and feature selection techniques over the collected datasets.

4.1. Data preparation and dataset descriptions

In this section, we describe the collected datasets and data preparation activities used to clean and organize them for data analysis activity. In particular, we collected ten different datasets, four related to Instagram accounts and six related to X (formerly Twitter) accounts. In what follows, we describe datasets and provide data sources.

- IG_1: The dataset consists of 1194 Instagram accounts, of which 994 real and 200 fake, and contains 10 features. The dataset source can be found at the following link: <https://github.com/Blacjar/instafake-dataset#fake-account-detection>
- IG_2: The dataset consists of 785 Instagram accounts, of which 93 real and 692 fake, and contains 13 features. The dataset source can be found at the following link: <https://www.kaggle.com/datasets/rezaunderfit/instagram-fake-and-real-accounts-dataset/data>
- IG_4: The dataset consists of 576 Instagram accounts, of which 288 real and 288 fake, and contains 12 features. The dataset source can be found at the following link: <https://www.kaggle.com/datasets/jasvindernotra/instagram-detecting-fake-accounts/data?select=instagram.csv>
- TW_3: The dataset consists of 2818 Twitter accounts, of which 1481 real and 1337 fake, and contains 34 features. The dataset source can be found at the following link: <https://www.kaggle.com/datasets/whoseaspects/genuinefake-user-profile-dataset/data>
- TW_7: The dataset consists of 9019 Twitter accounts, of which 5706 real and 3313 fake, and contains 16 features. The dataset source can be found in [12].

The datasets mentioned below can all be found at the following link: <https://botometer.osome.iu.edu/bot-repository/datasets.html>

- TW_8 (gilani2017): The dataset consists of 2503 Twitter accounts, of which 1413 real and 1090 fake, and contains 41 features.
- TW_9_LP (caverlee11): The dataset consists of 41499 Twitter accounts, of which 19276 real and 22223 fake, and contains 8 features.
- TW_9_M (midterm2018): The dataset consists of 50538 Twitter accounts, of which 8092 real and 42446 fake, and contains 18 features.
- TW_9_10: The dataset consists of 15,810 Twitter accounts, of which 7905 real and 7905 fake, and contains 43 features. In particular, the following dataset was obtained by concatenating multiple datasets, such as the verified-2019 and celebrity-2019 (real accounts), and the pronbots-2019, botwiki-2019, political-bots-2019, and vendor-purchased-2019 datasets (fake accounts).

Concerning data preparation activities, we replaced null values with zero and adopted an encoding strategy for non-numeric features to use machine learning models. In particular, the encoding strategy exploits a dictionary to map values of categorical columns into integers. This strategy allowed us to maintain the uniqueness of the tuples by avoiding altering the original data.

In the next section, we describe the machine learning models adopted and the parameters tuning used.

4.2. Adopted machine learning models and parameter tuning

This section describes the machine learning models employed in our study and the parameters tuning used for each model. In particular, we involved Decision Tree (DT) [13], K-Nearest Neighbors (KNN) [14], Logistic Regression (LR) [15], Gaussian Naïve Bayes (NB) [16], Random Forest (RF) [17] and Support Vector Classifier (SVC) [18] by considering their versions available in the Scikit-learn¹ python library. Moreover, for each model, we performed hyperparameter tuning using the GridSearchCV with 5-fold [18], aiming to identify the best combination of hyperparameters for the predictive models based on the accuracy scores. Details concerning machine learning models and parameters tuning are reported below. The decision tree (DT) model is a supervised learning model that, given a labelled dataset, recursively defines a tree structure where, at each level, local decisions are associated with a feature. After constructing the tree, each path from the root to a leaf node represents a classification pattern [13]. In detail, the hyperparameters utilized for the DT model are max_leaf_nodes in a range from 2 to 100 and [2, 3, 4] for min_samples_split. The k-Nearest Neighbor (KNN) algorithm is an instance-based technique that operates under the assumption that new instances are similar to those already provided with a class label. In this algorithm, all instances are treated as points in an n-dimensional space and are classified based on their similarity to other instances. In detail, the hyperparameters utilized for the KNN model are in the range of 1 to 25 for the n_neighbors param, ['uniform', 'distance'] for the weights param and [1, 2] for the p param. Logistic regression (LR) is a supervised learning approach capable of inferring a vector of weights whose elements are associated with each feature. In particular, a weight specifies the relevance of a feature with respect to the classification task [15]. In detail, the hyperparameters utilized for the LR model are 'l2' for penalty and [0.001, 0.01, 0.1, 1, 10, 100, 1000] for the C parameter. Gaussian Naïve Bayes (NB) is a supervised learning method based on the application of Bayes' theorem with the assumption of conditional independence between each pair of variables. In detail, the hyperparameters utilized for the NB model is the var_smoothing parameter ranging from 0 to -9. The random forest (RF) model is an approach based on the ensemble concept [19], i.e., exploiting a set of DTs to derive a global model that performs better than the single DTs composing the ensemble. In detail, the hyperparameters utilized for the RF model are bootstrap parameter set to true, [10, 20, 30, 100] for the max_depth, [2, 3] for the max_features, [3, 4, 5] for the min_samples_leaf parameter, [8, 10, 12] for min_samples_split, [10, 20, 30, 100] for n_estimators and finally, 'gini' or 'entropy' for the criterion. Support vector classification (SVC) is a model in which the training instances are classified separately in different points of a space and organized into separated groups. The SVC tries to achieve the optimal separation hyperplane by computing the most significant margins of separation between different classes [20]. In detail, the hyperparameters utilized for the SVC model are [0.1, 1, 10, 100, 1000] for the C parameter, [1, 0.1, 0.01, 0.001, 0.0001] for gamma and finally, and 'rbf' as kernel.

In the next section, we describe the feature selection strategies adopted and their settings.

¹<https://scikit-learn.org/>

4.3. Adopted feature selection strategies

This section describes the feature selection strategies employed and their settings. In particular, we involved Spearman's Correlation (SC) [21], Information Gain (IG) [22], Recursive Feature Elimination with Cross-Validation (RFECV) [23], Minimum Redundancy Maximum Relevance (MRMR) [24] and Principal Component Analysis (PCA) [21]. Feature selection strategies details are provided below. Spearman's Correlation [21] is a technique that measures the correlation between two variables. In particular, a positive value indicates that variables have a positive relationship, whereas a negative value indicates a negative relationship. Moreover, If the value is zero, no relationship between the two variables is defined. For this reason, variables with a higher absolute correlation value may be considered more relevant and retained. Information Gain [22] consists of a non-parametric entropy-based technique that measures the dependence between two variables. In particular, If such dependence is equal to zero, the two variables are independent, while a higher value indicates greater dependence. Selected features are those with the highest score, while discarded features are those with the score closest to zero. Recursive Feature Elimination with Cross-Validation (RFECV) [23] is a technique for extracting the most significant features by removing the weakest feature. The Logistic Regression estimator provides information on the importance of features. The best subset of features is then selected using the accuracy scores in combination with cross-validation. Minimum Redundancy Maximum Relevance (MRMR) [24] involves selecting features with the highest relevance and least redundancy through mutual information. In this case, the number of features to be selected is chosen based on the k returned by the RFECV method. Finally, Principal Component Analysis (PCA) [21] is a dimensionality reduction method that identifies principal components in the direction that preserves most of the variety in the original data. To this end, we use PCA by selecting a number of components that preserve the 95% of data variance considering all features.

In the next section, we provide details concerning the proposed fake accounts dataset.

4.4. Proposed fake accounts dataset

In this section, we describe the proposed fake accounts dataset. In particular, we collected the Proposed Dataset (PD) from Instagram's social platform. The dataset consists of 1937 accounts, divided into 944 real accounts and 993 fake accounts, and contains 11 features. In detail, we collected Instagram accounts by exploiting a data crawling technique implemented with an ad hoc script to extract the features needed. More specifically, fake accounts are purchased using the online service: <https://serviceiggrowthstar.it>, whereas real accounts are collected by involving real users and verified manually. All the above-described datasets are organized, cleaned and made accessible to the following GitHub repository: <https://github.com/Macerul/FakeAccountDatasets.git>. Additionally, we also provide in-depth statistics concerning additional metrics computed using machine learning models over each dataset, i.e., Precision, Recall, F1 and Accuracy, at the following link: https://github.com/Macerul/FakeAccountDatasets_Scores.git

In the next section, we describe experimental results achieved by employing machine learning models and feature selection techniques over each dataset.

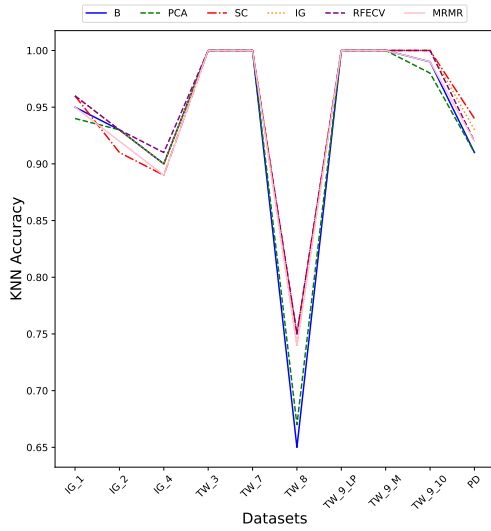


Figure 3: Accuracy results of KNN model over the collected fake account datasets.

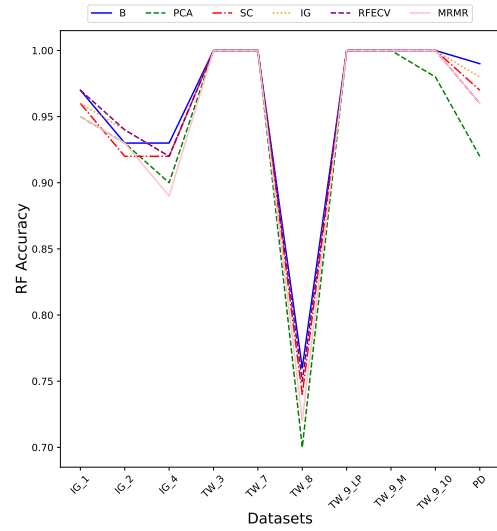


Figure 4: Accuracy results of RF model over the collected fake account datasets.

4.5. Results

In order to compute classification results, we run several experimental sessions in which different classification models are trained over the datasets described in Section 4.1. In particular, we discuss the performances achieved with the employed predictive models over each dataset and evaluate the feature selection strategies described in Section 4.3 regarding classification improvements. In detail, Figures 3 to 8 highlight results obtained by employing each classification model (x-axis) for each dataset (y-axis). Moreover, each figure presents results obtained by using only the model (B), Principal Component Analysis (PCA), Spearman's Correlation (SC), Information Gain (IG), Recursive Feature Elimination with Cross-Validation (RFECV), and Minimum Redundancy Maximum Relevance (MRMR) as feature selection strategies.

Figure 3 reports classification results achieved by employing the KNN model. In particular, it is possible to notice that classification results computed over the IG_1, IG_4, TW_8, TW_9_10 and PD datasets by exploiting SC, IG and RFEVC overcome the baseline results computed by using only the KNN model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over the TW_3, TW_7, TW_9_LP, and TW_9_M datasets, whereas the worst are obtained over the TW_8 dataset. In general, RFEVC is the feature selection strategy offering more improvements in terms of fake account discrimination when combined with the KNN model.

Figure 4 reports classification results achieved by employing the RF model. In particular, classification results computed over the IG_2 dataset by exploiting IG and RFEVC overcome the baseline results computed by using only the RF model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over the TW_3, TW_7, TW_9_LP, TW_9_M, and TW_9_10 datasets, whereas the

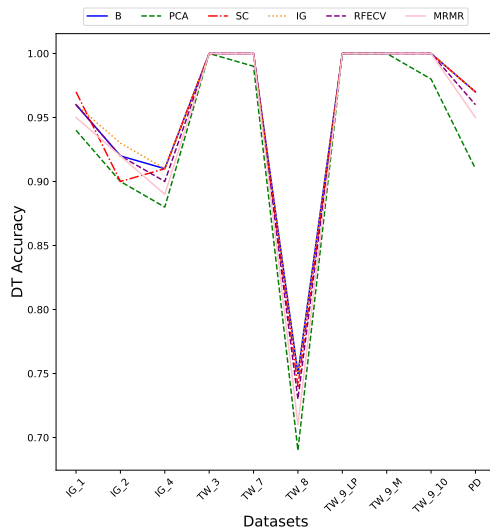


Figure 5: Accuracy results of DT model over the collected fake account datasets.

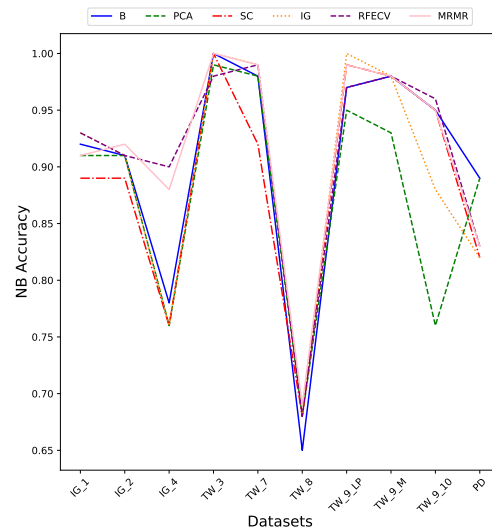


Figure 6: Accuracy results of NB model over the collected fake account datasets.

worst classification results are obtained over the TW_8 dataset. In general, RFEVC and IG are feature selection strategies offering more improvements in terms of fake account discrimination when combined with the RF model.

Figure 5 reports classification results achieved by employing the DT model. In particular, classification results computed over the IG_1 and IG_2 datasets by exploiting SC and IG overcome the baseline results computed by using only the DT model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over the TW_3, TW_7, TW_9_LP, TW_9_M, and TW_9_10 datasets, whereas the worst classification results are obtained over the TW_8 dataset. In general, SC and IG are feature selection strategies offering more improvements in terms of fake account discrimination when combined with the DT model.

Figure 6 reports classification results achieved by employing the NB model. In particular, it is possible to notice that classification results computed over the IG_1, IG_2, IG_4, TW_7, TW_8, TW_9, and TW_9_10 datasets by exploiting IG, RFECV, and MRMR overcome the baseline results computed by using only NB model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over the TW_3 and TW_9 datasets, whereas the worst are obtained over the TW_8 dataset. In general, IG and RFECV are feature selection strategies offering more improvements in terms of fake account discrimination when combined with the NB model.

Figure 7 reports classification results achieved by employing the SVC model. In particular, it is possible to notice that classification results computed over the IG_2, IG_4, and TW_8 datasets by exploiting MRMR and RFECV overcome the baseline results computed by using only the SVC model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over the TW_3, TW_7, TW_9_LP, TW_9_M, and

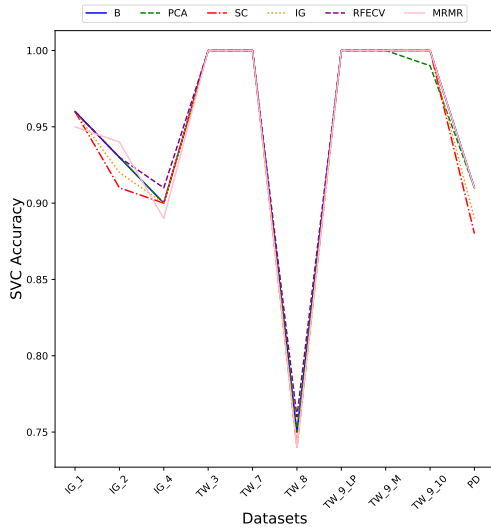


Figure 7: Accuracy results of SVC model over the collected fake account datasets.

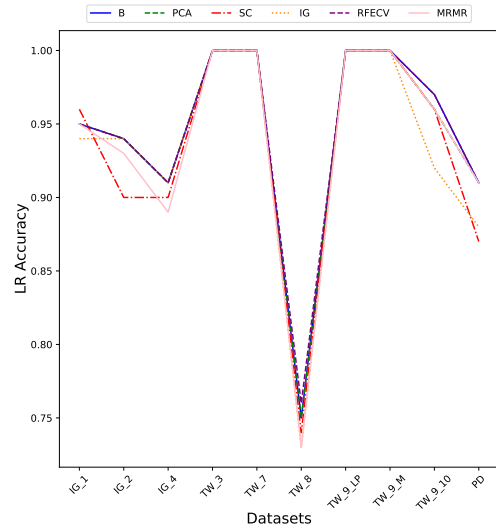


Figure 8: Accuracy results of LR model over the collected fake account datasets.

TW_9_10 datasets, whereas the worst classification results are obtained over the TW_8 dataset. In general, RFECV is the feature selection strategy offering more improvements in terms of fake account discrimination when combined with the SVC model.

Figure 8 reports classification results achieved by employing the LR model. In particular, it is possible to notice that classification results computed over the IG_1 and TW_8 datasets by exploiting SC and RFECV overcome the baseline results computed by using only the LR model, whereas those computed over the remaining datasets preserve the baseline. Moreover, the best classification results are obtained over TW_3, TW_7, TW_9_LP, and TW_9_M datasets, whereas the worst classification results are obtained over the TW_8 dataset. In general, RFECV is the feature selection strategy offering more improvements in terms of fake account discrimination when combined with the LR model.

In order to evaluate the number of selected features yielded by each feature selection technique over each collected dataset, we report in Figures 9 the obtained results. In particular, the x-axis represents the analyzed datasets, whereas the y-axis represents the amount of features selected for each dataset. Each line reported in Figure 9 represents the application of Spearman's Correlation (SC), Information Gain (IG), and Recursive Feature Elimination with Cross-Validation (RFECV) as feature selection strategies, respectively. We do not report results concerning Principal Component Analysis (PCA) and Minimum Redundancy Maximum Relevance (MRMR) since the PCA does not yield the number of selected features and MRMR yields the same number of features of RFECV (see Section 4.3). In general, as it is possible to see from Figure 9, the IG strategy selects the minimum number of features for almost all datasets, whereas RFECV yields the maximum one for all datasets except for the TW_3. Concerning SC, it overcomes RFECV results only over the TW_3 dataset and yields a number of features less than IG only over the IG_1, IG_4, and PD datasets.

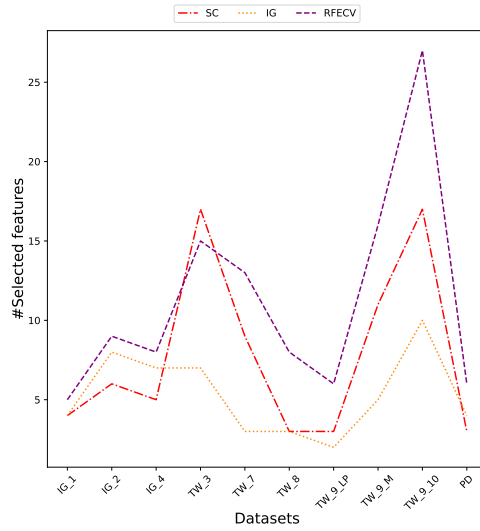


Figure 9: Number of selected features by each feature selection strategy w.r.t. analyzed datasets.

As illustrated in our results, feature selection strategies improve the classification results of machine learning models. In particular, the model that achieved the best results is the RF, whereas, for almost all models, RFECV is the feature selection strategy offering more improvements in fake account discrimination even if it selects a large number of features.

5. Conclusions

The increasingly widespread use of malicious accounts can compromise the trustability of social network platforms. In this context, the number of techniques for detecting fake accounts has grown proportionally to the number of new algorithms developed for harmful purposes, and it is necessary to collect and organize data associated with social network accounts to improve discrimination capacities. Under this view, we cleaned and organized fake account datasets from online sources for analytical activities. Evaluation results achieved over different machine learning models demonstrated that feature selection strategies improve classification performances. The main objective of our proposal is to support stakeholders, data analysts, and researchers by offering the possibility of quickly accessing fake account datasets together with machine learning classification results.

In the future, we would like to collect more data, including additional social network platforms, to improve the proposed analysis. Moreover, we would like to analyze the impact of the removed features of each feature selection strategy over training times and classification performances.

Acknowledgments

This Publication was produced with the co-funding of the European union - Next Generation EU:

NRRP Initiative, Mission 4, Component 2, Investment 1.3 – Partnerships extended to universities, research centers, companies and research D.D. MUR n. 341 del 5.03.2022 – Next Generation EU (PE0000014 - "Security and Rights In the CyberSpace - SERICS" - CUP: H93C22000620001).

References

- [1] C. Castillo, M. Mendoza, B. Poblete, Information credibility on twitter, in: Proceedings of the 20th international conference on World wide web, ACM, Hyderabad, India, 2011, pp. 675–684.
- [2] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science* 3 (2021) 563060.
- [3] C. Braker, S. Shiaeles, G. Bendiab, N. Savage, K. Limniotis, Botspot: Deep learning classification of bot accounts within twitter, in: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Springer, Petersburg, Russia, 2020, pp. 165–175.
- [4] P. Wanda, H. J. Jie, Deepprofile: Finding fake profile in online social network using dynamic cnn, *Journal of Information Security and Applications* 52 (2020) 102465.
- [5] S. Kudugunta, E. Ferrara, Deep neural networks for bot detection, *Information Sciences* 467 (2018) 312–322.
- [6] D. Seyler, L. L. and ChengXiang Zhai, Identifying compromised accounts on social media using statistical text analysis, *Computing Research Repository* abs/1804.07247 (2018) 1–8.
- [7] S. Kodati, P. R. Kumbala, S. Mekala, P. S. Murthy, P. C. S. Reddy, Detection of fake profiles on twitter using hybrid svm algorithm, in: *E3S Web of Conferences*, volume 309, EDP Sciences, Ternate, Indonesia, 2021, p. 01046.
- [8] K. K. Bharti, S. Pandey, Fake account detection in twitter using logistic regression with particle swarm optimization, *Soft Computing* 25 (2021) 11333–11345.
- [9] I. Sen, A. Aggarwal, S. Mian, S. Singh, P. Kumaraguru, A. Datta, Worth its weight in likes: Towards detecting fake likes on instagram, in: *Proceedings of the 10th ACM Conference on Web Science*, ACM, Amsterdam, Netherlands, 2018, pp. 205–209.
- [10] L. Caruccio, D. Desiato, G. Polese, Fake account identification in social networks, in: *2018 IEEE international conference on big data (big data)*, IEEE, 2018, pp. 5078–5085.
- [11] L. Caruccio, G. Cimino, S. Cirillo, D. Desiato, G. Polese, G. Tortora, Malicious account identification in social network platforms, *ACM Transactions on Internet Technology* 23 (2023) 1–25.
- [12] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi, Social fingerprinting: detection of spambot groups through dna-inspired behavioral modeling, *IEEE Transactions on Dependable and Secure Computing* 15 (2018) 561–576.
- [13] P. H. Swain, H. Hauska, The decision tree classifier: Design and potential, *IEEE Transactions on Geoscience Electronics* 15 (1977) 142–147.
- [14] O. Kramer, O. Kramer, K-nearest neighbors, *Dimensionality reduction with unsupervised nearest neighbors* (2013) 13–23.
- [15] F. O. Redelico, F. Traversaro, M. d. C. García, W. Silva, O. A. Rosso, M. Risk, Classification of normal and pre-ictal eeg signals using permutation entropies and a generalized linear model as a classifier, *Entropy* 19 (2017) 72.

- [16] S. Xu, Bayesian naïve bayes classifiers to text classification, *Journal of Information Science* 44 (2018) 48–59.
- [17] M. Pal, Random forest classifier for remote sensing classification, *International journal of remote sensing* 26 (2005) 217–222.
- [18] D. Kartini, D. T. Nugrahadi, A. Farmadi, et al., Hyperparameter tuning using gridsearchcv on the comparison of the activation function of the elm method to the classification of pneumonia in toddlers, in: *2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*, IEEE, Jakarta, Indonesia, 2021, pp. 390–395.
- [19] J. C.-W. Chan, D. Paelinckx, Evaluation of random forest and adaboost tree-based ensemble classification and spectral band selection for ecotope mapping using airborne hyperspectral imagery, *Remote Sensing of Environment* 112 (2008) 2999–3011.
- [20] S. S. Keerthi, S. K. Shevade, C. Bhattacharyya, K. R. Murthy, A fast iterative nearest point algorithm for support vector machine classifier design, *IEEE transactions on neural networks* 11 (2000) 124–136.
- [21] A. Homsî, J. Al-Nemri, N. Naimat, H. Kareem, M. Al-Fayoumi, M. Abu Snober, Detecting twitter fake accounts using machine learning and data reduction techniques, 2021, pp. 88–95. doi:10.5220/0010604300880095.
- [22] S. Lei, A feature selection method based on information gain and genetic algorithm, in: *2012 International Conference on Computer Science and Electronics Engineering*, volume 2, 2012, pp. 355–358. doi:10.1109/ICCSEE.2012.97.
- [23] A. Z. Mustaqim, S. Adi, Y. Pristyanto, Y. Astuti, The effect of recursive feature elimination with cross-validation (rfecv) feature selection algorithm toward classifier performance on credit card fraud detection, in: *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*, 2021, pp. 270–275. doi:10.1109/ICAICST53116.2021.9497842.
- [24] Y. Jiang, C. Li, mrmr-based feature selection for classification of cotton foreign matter using hyperspectral imaging, *Computers and Electronics in Agriculture* 119 (2015) 191–200. URL: <https://www.sciencedirect.com/science/article/pii/S0168169915003300>. doi:<https://doi.org/10.1016/j.compag.2015.10.017>.