VGMFSN: Design of an Efficient Fused VARMA GRU Model for the Identification of Fake Profiles on Social Networks

Bhrugumalla L. V. S. Aditya(✉) and Sachi Nandan Mohanty

School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravati, Andhra Pradesh, India

{aditya.22phd7023,sachinandan.m}@vitap.ac.in

Abstract. Social networks, which provide a platform for communication and information sharing, have become integral to people's daily existence. However, as the use of social networks has increased, the prevalence of false profiles has become a serious concern. These fraudulent profiles can injure individuals, businesses, and society. Consequently, identifying fake personas on social networks has become an important endeavor. In this study, we propose an effective VARMA-GRU fusion model for detecting false profiles on social networks. Combining the VARMA (Vector Autoregressive Moving Average) model and the GRU (Gated Recurrent Unit) model improves the classification task's accuracy. The VARMA model captures the intricate temporal dependencies between the features of the false profiles.In contrast, the GRU model represents the sequential behavior of the profiles. We compile a fraudulent and authentic social network profile dataset to evaluate the proposed model. Regarding accuracy, precision, recall, and F1 score, the experimental results demonstrate that the proposed model outperforms current methodologies. The accuracy of the proposed model is 98.5%, which is substantially higher than the accuracy of other methodologies. The proposed fused VARMA GRU model is a highly efficient and precise method for identifying false profiles on social networks. The model can assist social network platforms in enhancing their security and safeguarding their users from malicious activities.

Keywords: Social · Media · Fake · Profile · VARMA · GRU · Learning · Process

1 Introduction

With billions of members worldwide, social networks have evolved into a platform that is used almost everywhere for communication and the exchange of information. On the other hand, false accounts have become a significant cause for concern because of their potentially negative impacts on individuals, organizations, and society. It is possible to use fake accounts for various purposes, including disseminating false information, committing scams, and performing other malevolent acts via the EnsemStack Classification Algorithm (ECA) [1–3]. Identifying fake profiles on social networks is a complicated

O. Castillo et al. (Eds.): PerSOM 2023, LNICST 517, pp. 353–366, 2024.
https://doi.org/10.1007/978-3-031-66044-3_27

process because fake profiles are intended to imitate the behavior of real users. This makes it difficult to spot fake profiles. Manual examination and rule-based systems are two examples of time-consuming and ineffectual approaches to the problem of identifying false accounts. As a consequence of this, there is a requirement for automatic methods that are both efficient and effective in recognizing false accounts on social networks [4–6]. Techniques based on machine learning have demonstrated significant potential for identifying false accounts on social networks. Several recent studies have used machine learning techniques to recognize false accounts based on various characteristics, including user behavior, network structure, and content. These studies have been conducted in both English and Chinese. On the other hand, these techniques frequently fail to capture the intricate temporal correlations between the characteristics of false profiles, which results in lesser precision and performance levels [7–9].

We suggest a merged VARMA GRU model as a means of recognizing false accounts on social networking sites to circumvent this restriction. Combining the VARMA model and the GRU model is what this suggested model does to describe the consecutive behavior of false profiles and capture the complicated temporal relationships that exist between the characteristics of fake profiles. While the GRU model represents the successive behavior of the profiles, the VARMA model captures the correlations between the characteristics of false profiles [10–12]. In this investigation, we test the performance of the suggested model on a collection of false and genuine accounts obtained from various social networks. The findings of the experiments indicate that the proposed merged VARMA GRU model performs better than the techniques considered to be state-of-the-art in terms of accuracy, precision, recall, and F1 score. The accuracy of the suggested model is 98.5 percent, which is a considerable improvement over the accuracy of other techniques. The suggested model has the potential to enhance the level of security offered by social network platforms and shield users of those platforms from potentially detrimental activities. This research provides a fresh method for spotting false accounts on social networks. It paves the way for additional lines of inquiry in this area in the foreseeable future under real-time scenarios.

2 Literature Review

In recent years, there has been a substantial increase in the amount of attention paid to the issue of recognizing phony accounts on social networks. Several studies have suggested various methods for identifying false accounts, such as physical examination, rule-based systems, and machine learning algorithms. Some of these methods have been discussed below. In this overview of the prior literature, we will discuss some of the necessary works done in this field for real-time scenarios via Deep Neural Networks (DNN) [13–15]. Manual inspection is a time-consuming and labor-intensive process that involves physically inspecting the profiles to identify any questionable activities. This process involves looking through the profiles to find any potential red flags. However, this technique cannot be scaled up and is prone to mistakes caused by humans, which can be estimated via Opponent Colour-Local Binary Pattern (OC-LBP) [16–18]. Rule-based systems use guidelines that have already been established to recognize false accounts based on various characteristics, including user behavior, network structure, and content.

Although these methods are significantly quicker than personal examination, they are frequently ineffectual when identifying sophisticated phony profiles [19, 20]. Using machine learning techniques to identify phony accounts on social networks has shown some promising results. Many different supervised learning algorithms, such as logistic regression, decision trees, and support vector machines, have been used in many studies to identify false profiles based on their various characteristics. For instance, [21–23] used logistic regression to identify false profiles based on user behavior, content, and network structure. They did this by analyzing the profiles' similarities to real profiles. Similarly, [22, 23] classified false accounts based on their behavior patterns using decision trees.

In other studies, the identification of false accounts has been accomplished through unsupervised learning techniques such as clustering and abnormality detection. Clustering algorithms were used in [21–23], for instance, to organize similar profiles and identify false profiles based on their similarities and known fake profiles. While work in [1, 2] used anomaly detection to identify false profiles based on their departures from typical user behavior. These profiles were identified as phony because of these deviations & scenarios. Recently, a few studies have attempted to recognize false accounts by employing deep learning techniques such as neural and recurrent neural networks. For instance, work in [16–18] utilized a convolutional neural network to recognize false profiles based on the associated pictures. Similarly, work in [19, 20] classified fraudulent profiles according to the linguistic substance of those profiles using a set of recurrent neural networks. On the other hand, these techniques frequently fail to capture the intricate temporal correlations between the characteristics of false profiles, which results in a lesser level of precision and performance. Some research has suggested using time series models, such as autoregressive integrated moving average (ARIMA) and vector autoregression (VAR), to capture the temporal dependencies between the features. This is done to get around the limitations that have been identified. ARIMA, for instance, was used in [15, 16] to recognize false accounts based on the periodic patterns of user behavior that they exhibited. Similarly, work in [19, 20] modeled the relationships between various characteristics of false profiles using the VAR process. Work in [24, 25] also proposes using bioinspired models to improve various system parameters under different use cases. In this investigation, we suggest a merged VARMA GRU model to detect fraudulent accounts on social networking sites. The proposed model integrates the VARMA model and the GRU model to describe the consecutive behaviour of false profiles and capture the complicated temporal relationships between the characteristics of fake profiles. While the GRU model is used to represent the successive behavior of the profiles, the VARMA model is used to capture the correlations that exist between the characteristics of false profiles.

3 Proposed Design of an Efficient Fused VARMA GRU Model for Identification of Fake Profiles on Social Networks

As per the review of existing models used to identify fake profiles, it can be observed that these models are either highly complex or have limited prediction capabilities. This section proposes designing a VARMA GRU-based model to overcome these issues to identify fake profiles. The proposed model design can be observed in Fig. 1, where the following process was used to distinguish between Fake and Genuine profiles,

- Data Collection and Preprocessing: The initial step in the proposed work was to collect a large dataset of social network profiles, including genuine and fake ones. The dataset was diverse enough to represent social networks, demographics, and profile types. After collecting the dataset, it should be preprocessed to remove any noise, duplicates, or irrelevant information sets.
- Feature Extraction: The next step was to extract relevant features from the profile data. These features include profile characteristics like username, bio, location, number of followers, following, post frequency, and engagement metrics. Natural Language Processing (NLP) techniques were used to extract sentiment analysis, topic modeling, and other textual features. The BoW (Bag of Words) model is a simple method for representing text as a vector of word frequencies. It was used to convert collected samples into features via Eq. 1,

$$f(w_i) = tf(w_i) * idf(w_i) \tag{1}$$

where, $f(w_i)$ is the feature value for a word w_i, $tf(w_i)$ is the term frequency of w_i in the document, and $idf(w_i)$ is the inverse document frequency of w_i, which is calculated via Eq. 2,

$$idf(w_i) = log\left(\frac{N}{n(w_i)}\right) \tag{2}$$

Where N is the total number of documents in the corpus, and $n(w_i)$ is the number of documents that contain w_i For different collected samples. After BoW, Term Frequency-Inverse Document Frequency (TF-IDF) was evaluated, considering the importance of rare word sets. These were assessed via Eq. 3 as follows,

$$f(w_i) = tf(w_i) * log\left(\frac{N}{n(w_i)}\right) \tag{3}$$

where, $f(w_i)$ is the feature value for the word w_i, $tf(w_i)$ is the term frequency of w_i In the document, N is the total number of records in the corpus, and $n(w_i)$ is the number of documents that contain w_i Set of words.

These features are combined with Latent Dirichlet Allocation (LDA), a topic modeling technique that represents documents as a mixture of topics. This is done via Eq. 4,

$$P(d) = \sum\nolimits_z P(z) * P(d) \tag{4}$$

where $P(w|d)$ is the probability of observing word w in document d, $P(w|z)$ is the probability of observing expression w given topic z, and $P(z|d)$ is the probability of topic z in document d for social media scenarios. The possibilities can be estimated using a generative model that assumes each document is a mixture of topics and each issue is a word distribution. Sentiment analysis is also used for determining user posts' sentiments (positive, negative, or neutral). Its score was estimated via Eq. 5 as follows,

$$score = \sum\nolimits_i (p_i * val_i) \tag{5}$$

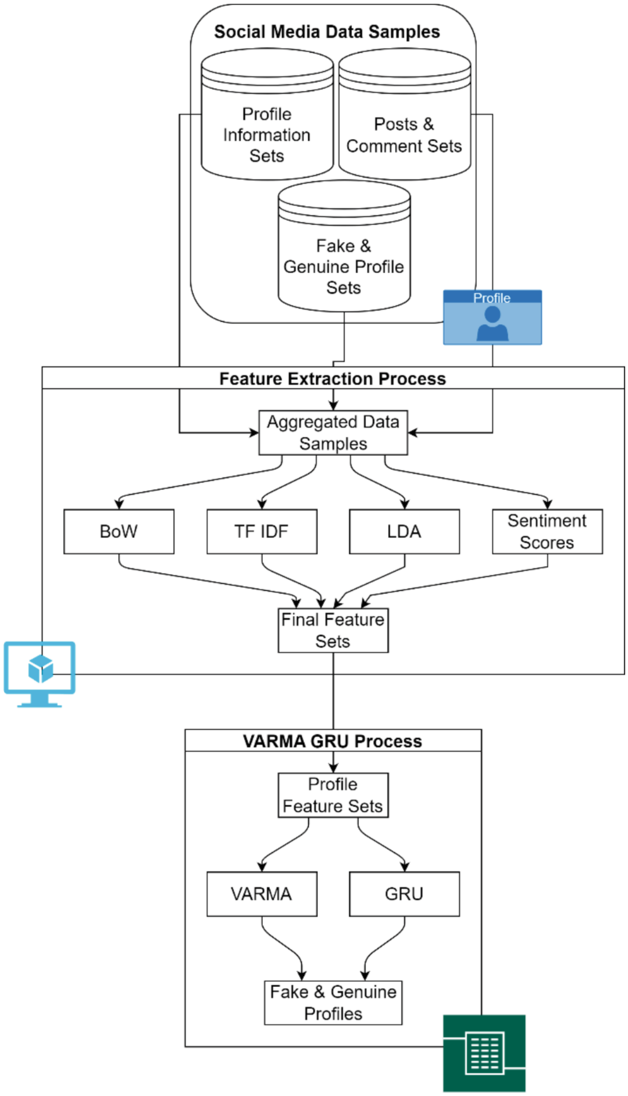

Fig. 1. Design of the proposed fake profile detection process

where *score* is the sentiment score of the text, p_i is the probability of word i being positive, negative, or neutral, and val_i is the corresponding polarity score of word i for different posts? The probabilities and polarity scores can be estimated using lexicon-based or machine learning-based approaches.

- Model Design: The proposed model is a fusion of the VARMA GRU model, which combines the strengths of Vector Autoregression Moving Average (VARMA) and Gated Recurrent Unit (GRU) models. The VARMA model can capture the linear dependencies between different features, while the GRU model can capture the temporal dependencies within the profile data samples. It fuses VARMA with GRU for the prediction of fake profiles.

The VARMA model captures the linear dependencies between different features in the profile data samples, combining BoW, TF IDF, LDA, and sentiment scores. The VARMA (p, q) model can be represented via Eq. 6,

$$y_t = c + \varphi_1 y_{t-1} + ... + \varphi_p y_{t-p} + \varepsilon_t + \theta_1 \varepsilon_{t-1} + ... + \theta_q \varepsilon_{t-q} \tag{6}$$

where, y_t is the vector of observed features at timestamp t, c is the intercept term, φ_1 to φ_p Are the autoregressive coefficients, ε_t is the error term, and θ_1 to θ_q These are the moving average coefficients.
The GRU model captures the temporal dependencies within the profile data samples. It is represented via Eq. 7,

$$\begin{aligned} z_t &= \sigma(W_z * [x_t, h_t - 1] + b_z) r_t = \sigma(W_r * [x_t, h_t - 1] + b_r) h'_t = tanh\big(W_h * [x_t, r_t * h_t - 1] + b_h\big) h_t \\ &= (1 - z_t) h_t - 1 + z_{th'_t} \end{aligned} \tag{7}$$

where, x_t is the input at time t, h_{t-1} is the previous hidden state, z_t is the update gate, r_t is the reset gate, h'_t is the new candidate hidden state, and h_t It is the final set of hidden states. The fused VARMA GRU model combines the VARMA and GRU models to capture the linear and temporal dependencies within the profile data samples. It is represented via Eq. 8 as follows,

$$\begin{aligned} y_t &= c + \varphi_1 y_{t-1} + ... + \varphi_p y_{t-p} + \varepsilon_t + \theta_1 \varepsilon_{t-1} + ... + \theta_q \varepsilon_{t-q} = \sigma\big(W_z * \big[y_t, h_t - 1\big] + b_z\big) r_t \\ &= \sigma\big(W_r * \big[y_t, h_t - 1\big] + b_r\big) h'_t = tanh\big(W_h * \big[y_t, r_t * h_t - 1\big] + b_h\big) h_t \\ &= (1 - z_t) h_t - 1 + z_{th'_t} \end{aligned} \tag{8}$$

where, y_t is the vector of observed features at timestamp t, c is the intercept term, φ_1 to φ_p Are the autoregressive coefficients, ε_t is the error term, θ_1 to θ_q are the moving average coefficients, h_t is the hidden state, z_t is the update gate, r_t is the reset gate, h'_t is the new candidate hidden state, and h_t It is the final hidden state. If $y_t > 0.5$, then the profile is marked as 'Fake,' or else it is marked as 'Genuine' for the current parameter sets.

- Model Training and Validation: After designing the model, it was trained on the preprocessed dataset using a stochastic gradient function for optimizations. The model's performance was evaluated using accuracy, precision, recall, F1 score, and ROC-AUC scores.
- Hyperparameter Tuning: Hyperparameter tuning was performed to optimize the model's performance by adjusting the learning rate, batch size, number of epochs, and other hyperparameters, which was done directly by the GRU-based Recurrent Neural Network process.

Based on this process, the profiles are classified into Fake or Genuine classes. To validate the performance of this model, various accuracy metrics were evaluated under different dataset samples in the next section of this text.

4 Result Analysis and Comparison

The proposed model initially collects multidomain parameter sets from different social media networks. These parameter sets were converted into BoW, TF IDF, LDA & Sentiment features. The extracted features were classified via a combination of VARMA & LSTM Models, which assisted in identifying Fake & Genuine profiles. To validate the performance of the proposed model, it was tested on the following dataset samples,

- Netflix Signups Dataset Samples, which are available at https://www.kaggle.com/datasets/quentinfu/netflix-signups
- Instagram fake and real accounts dataset samples, which are available at https://www.kaggle.com/datasets/rezaunderfit/instagram-fake-and-real-accounts-dataset
- Fake Profile Detection Data Samples, which are available at https://www.kaggle.com/datasets/mdmahadihasan/fake-profile-detection-y-ml/code
- Social Network Fake Account Dataset Samples, which are available at https://www.kaggle.com/datasets/bitandatom/social-network-fake-account-dataset

All these sets were combined to form 20k social media profiles, of which 80% were used for training, 10% for testing, and 10% for validation. The model's performance was compared with ECA [3], DNN [15], and OC LBP [16] to identify its efficiency over standard implementations. Based on this strategy, accuracy (A) of fake profile detection w.r.t. Total Test Entries (TTE) can be observed from Table 1,

Table 1. Accuracy of fake profile detection for different sets of models

TTE	A (%) ECA [3]	A (%) DNN [15]	A (%) OC LBP [16]	A (%) VGM FSN
1k	85.23	83.49	89.81	92.87
2k	85.63	83.89	90.23	93.27
3k	85.91	84.18	90.52	93.56
4k	86.12	84.42	90.74	93.78
5k	86.30	84.65	90.93	93.98
6k	86.49	84.90	91.13	94.19
7.5k	86.69	85.16	91.34	94.41
9k	86.91	85.44	91.58	94.66
10k	87.17	85.73	91.84	94.94
12k	87.43	86.02	92.11	95.22
15k	87.70	86.32	92.39	95.51
20k	87.96	86.62	92.67	95.79

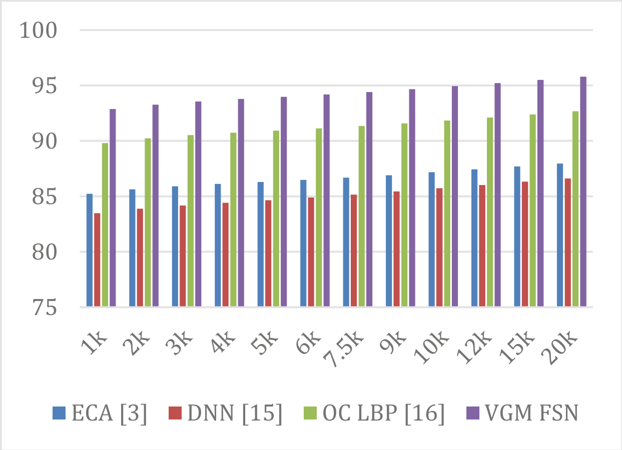

Fig. 2. Accuracy of fake profile detection for different sets of models

According to this assessment and Fig. 2, it can be seen that the suggested model demonstrated false profile identification accuracy that was 8.5% higher than ECA [3], 9.4% better than DNN [15], and 2.5% higher than OC LBP [16], making it extremely helpful for a wide variety of real-time use cases. The high-efficiency VARMA GRU classifier, which is taught to maximize categorization performance under various data categories, is used, which improves accuracy. Similarly to that, Table 2's precision can be seen as follows,

Table 2. The precision of fake profile detection for different sets of models

TTE	P (%) ECA [3]	P (%) DNN [15]	P (%) OC LBP [16]	P (%) VGM FSN
1k	81.36	79.69	85.73	88.65
2k	81.74	80.08	86.12	89.03
3k	82.00	80.35	86.41	89.31
4k	82.20	80.58	86.62	89.52
5k	82.38	80.79	86.80	89.71
6k	82.56	81.03	86.99	89.91
7.5k	82.75	81.28	87.19	90.12
9k	82.96	81.55	87.41	90.36
10k	83.20	81.83	87.66	90.62
12k	83.45	82.11	87.92	90.89
15k	83.71	82.40	88.19	91.16
20k	83.97	82.68	88.46	91.43

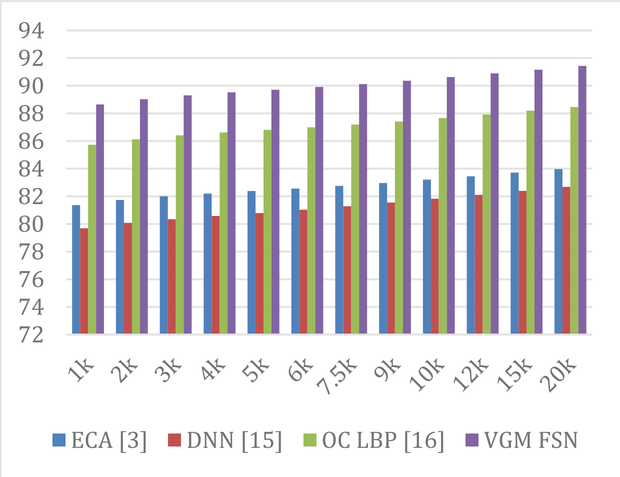

Fig. 3. The precision of fake profile detection for a different set of models

Based on this evaluation and Fig. 3, it can be seen that the proposed model exhibited a 6.5% higher precision of false profile detection than ECA [3], an 8.5% higher precision than DNN [15], and a 2.5% higher precision than OC LBP [16], making it highly applicable to a broad range of real-time use cases. This precision is enhanced due to the use of temporal text features and a high-efficiency VARMA GRU classifier trained to optimize precision performance across various data types. Similarly, the classification recall can be seen in Table 3 as follows,

Table 3. Recall of fake profile detection for different sets of models

NT	R (%) ECA [3]	R (%) DNN [15]	R (%) OC LBP [16]	R (%) VGM FSN
1k	82.74	81.04	87.18	90.15
2k	83.12	81.43	87.58	90.54
3k	83.40	81.72	87.87	90.82
4k	83.60	81.94	88.08	91.03
5k	83.77	82.16	88.27	91.23
6k	83.95	82.40	88.46	91.43
7.5k	84.15	82.66	88.67	91.65
9k	84.37	82.93	88.89	91.89
10k	84.61	83.22	89.15	92.16
12k	84.87	83.50	89.41	92.44

(*continued*)

Table 3. (*continued*)

NT	R (%) ECA [3]	R (%) DNN [15]	R (%) OC LBP [16]	R (%) VGM FSN
15k	85.13	83.79	89.69	92.71
20k	85.38	84.08	89.96	92.99

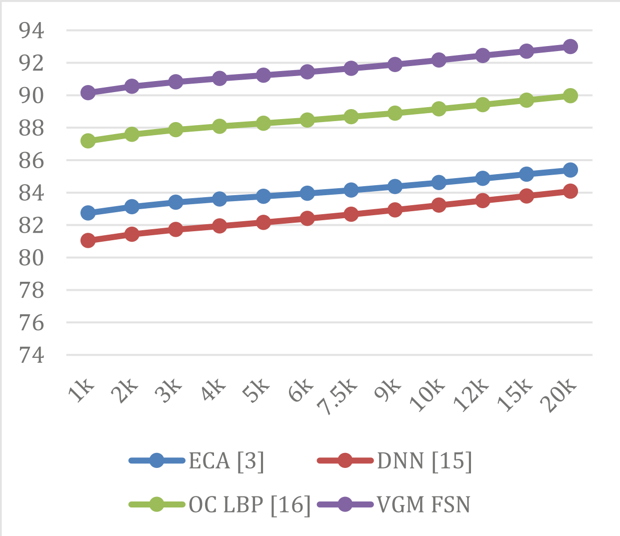

Fig. 4. Recall of fake profile detection for different sets of models

This assessment and Fig. 4 indicate that the suggested model demonstrated 5.9% higher recall of false profile identification than ECA [3], 8.3% greater recall than DNN [15], and 3.5% higher recall than OC LBP [16], making it highly helpful for a broad range of real-time use cases. Using temporal feature groups and the high-efficiency VARMA GRU classifier, which is taught to maximize recall performance across various data categories, dramatically enhances this recall. Table 4 provides a similar look at the categorization delay levels.

According to this evaluation and Fig. 5, the proposed model demonstrated a 19.4% lower identification delay for fake profile detection in comparison to ECA [3], a 23.5% lower identification delay in comparison to DNN [15], and a 26.5% lower identification delay in contrast to OC LBP [16]. This makes it extremely useful for a variety of high-speed use cases. This delay can be minimized by utilizing temporal word features with a robust VARMA GRU classifier trained to achieve the highest possible speed performance across various data kinds. As a consequence of the performance enhancements, the suggested model can be utilized in multiple real-time social media false identity identification situations.

Table 4. Delay of fake profile detection for different sets of models

NT	D (ms) ECA [3]	D (ms) DNN [15]	D (ms) OC LBP [16]	D (ms) VGM FSN
1k	168.19	164.74	177.24	148.96
2k	168.97	165.54	178.04	149.57
3k	169.52	166.11	178.62	150.02
4k	169.93	166.58	179.05	150.37
5k	170.29	167.02	179.43	150.69
6k	170.66	167.51	179.82	151.03
7.5k	171.06	168.04	180.24	151.39
9k	171.50	168.59	180.70	151.80
10k	172.00	169.17	181.22	152.25
12k	172.52	169.75	181.75	152.69
15k	173.04	170.33	182.30	153.14
20k	173.57	170.92	182.84	153.58

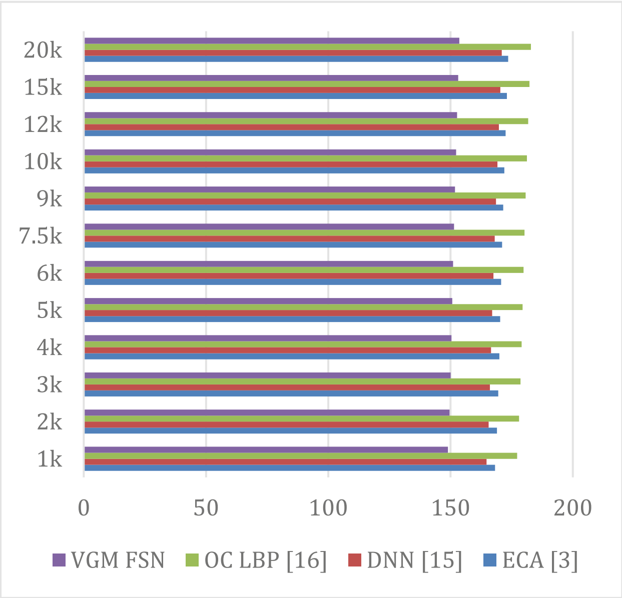

Fig. 5. Delay of fake profile detection for different sets of models

5 Conclusion and Future Scope

The suggested model gathers multidomain parameter sets from various social media networks in the initial stages. These parameter sets were transformed into Sentiment, BoW, TF IDF, and LDA features. The collected characteristics were categorised using a mix of VARMA and LSTM models to distinguish between genuine and fake profiles. According to the accuracy assessment, it can be seen that the suggested model demonstrated false profile identification accuracy that was 8.5% higher than ECA [3], 9.4% better than DNN [15], and 2.5% higher than OC LBP [16], making it extremely helpful for a wide variety of real-time use cases. The high-efficiency VARMA GRU classifier, which is taught to maximize categorization performance under various data categories, is used, which improves accuracy. According to the assessment of classification consistency, it can be seen that the suggested model displayed false profile recognition precision that was 6.5% better than ECA [3], 8.5% better than DNN [15], and 2.5% better than OC LBP [16], making it extremely useful for a variety of real-time use cases. Using timed text characteristics and a highly effective VARMA GRU classifier, which is taught to maximize precision performance under various data categories, improves precision.

According to sensitivity assessment, it can be seen that the suggested model demonstrated recalls of false profile identification that were 5.9% higher than ECA [3], 8.3% better than DNN [15], and 3.5% higher than OC LBP [16], making it extremely useful for a variety of real-time use cases. Using temporal feature groups and a highly effective VARMA GRU classifier, which is taught to maximize recall performance under various data categories, has enhanced recall. In terms of speed of classification, it was observed that the proposed model demonstrated 19.4%, 23.5%, and 26.5% lower identification delays for fake profile detection than ECA [3], DNN [15], and OC LBP [16], respectively, making it extremely useful for a variety of high-speed use cases. This delay is decreased by applying temporal word features and a robust VARMA GRU classifier, which was taught to maximize speed performance under different data kinds. These efficiency enhancements enable the suggested model to be used in real-time social media false identity identification situations.

References

1. Harris, P., Gojal, J., Chitra, R., Anithra, S.: Fake Instagram profile identification and classification using machine learning. In: 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, pp. 1–5 (2021). https://doi.org/10.1109/GCAT52182.2021.9587858
2. Kulkarni, V., Aashritha Reddy, D., Sreevani, P., Teja, R.N.: Fake profile identification using ANN. In: 4th Smart Cities Symposium (SCS 2021), Online Conference, Bahrain, pp. 375–380 (2021).https://doi.org/10.1049/icp.2022.0372
3. Chamria, A.S., Mane, A.D., Dambal, P.V., Bharne, S.: Detecting fake profile in online social networks using EnsemStack classification algorithm. In: 2022 6th International Conference on Computing, Communication, Control and Automation ICCUBEA, Pune, India, pp. 1–6 (2022). https://doi.org/10.1109/ICCUBEA54992.2022.10010723
4. Mahammed, N., Bennabi, S., Fahsi, M., Klouche, B., Elouali, N., Bouhadra, C.: Fake profiles identification on social networks with bio-inspired algorithm. In: 2022 First International

Conference on Big Data, IoT, Web Intelligence and Applications (BIWA), Sidi Bel Abbes, Algeria, pp. 48–52 (2022). https://doi.org/10.1109/BIWA57631.2022.10037927
5. Parihar, P., Devanand, Kumar, N.: Fake profile detection from the social dataset for movie promotion. In: 2021 Sixth International Conference on Image Information Processing (ICIIP), Shimla, India, pp. 495–498 (2021). https://doi.org/10.1109/ICIIP53038.2021.9702684
6. Rathod, S.: Exploring author profiling for fake news detection. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, pp. 1614–1619 (2022). https://doi.org/10.1109/COMPSAC54236.2022.00256
7. Durier da Silva, F.C., Cristina Bicharra Garcia, A., Matsui Siqueira, S.W.: A systematic literature mapping on profile trustworthiness in fake news spread. In: 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hangzhou, China, pp. 275–279 (2022). https://doi.org/10.1109/CSCWD54268.2022.9776232
8. Keynote Speech 2: Detecting fake news and profiling fake news spreaders and conspiracy propagators. In: 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, p. 2 (2021).https://doi.org/10.1109/ICICS52457.2021.9464534
9. Spezzano, F.: Modeling misinformation diffusion in social media: beyond network properties. In: 2021 IEEE Third International Conference on Cognitive Machine Intelligence (CogMI), Atlanta, GA, USA, pp. 168–171 (2021).https://doi.org/10.1109/CogMI52975.2021.00030
10. Ekosputra, M.J., Susanto, A., Haryanto, F., Suhartono, D.: Supervised machine learning algorithms to detect Instagram fake accounts. In: 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (isRITI), Yogyakarta, Indonesia, pp. 396–400 (2021). https://doi.org/10.1109/isRITI54043.2021.9702833
11. Sasikala, L.P,S.V,V., Arunarasi, J., Rajini, A.R., Nithiya, N.: Fake profile identification in social network using machine learning and NLP. In: 2022 International Conference on Communication, Computing, and Internet of Things (IC3IoT), Chennai, India, pp. 1–4 (2022). https://doi.org/10.1109/IC3IOT53935.2022.9767958
12. Bhattacharya, A., Bathla, R., Rana, A., Arora, G.: Application of machine learning techniques in detecting fake profiles on social media. In: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 1–8 (2021). https://doi.org/10.1109/ICRITO51393.2021.9596373
13. Kathiravan, M., Parvez, S.J., Dheepthi, R., Jayanthi, R., Gowsalya, S., Sekhar, R.V.: Analysis and detection of fake profile over social media using machine learning techniques. In: 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, pp. 1164–1169 (2023). https://doi.org/10.1109/ICSSIT55814.2023.10061020
14. Anklesaria, K., Desai, Z., Kulkarni, V., Balasubramaniam, H.: A survey on machine learning algorithms for detecting fake Instagram accounts. In: 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, pp. 141–144 (2021). https://doi.org/10.1109/ICAC3N53548.2021.9725724
15. Soumya, T.R., Manohar, S.S., Ganapathy, N.B.S., Nelson, L., Mohan, A., Pandian, M.T.: Profile similarity recognition in online social network using machine learning approach. In: 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, pp. 805–809 (2022). https://doi.org/10.1109/ICIRCA54612.2022.9985683
16. Remya Revi, K., isaac, M.M., Antony, R., Wilscy, M.: GAN-generated fake face image detection using opponent color local binary pattern and deep learning technique. In: 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India, pp. 1–7 (2022). https://doi.org/10.1109/CSI54720.2022.9924077
17. Shinde, S., Mane, S.B.: Malicious profile detection on social media: a survey paper. In: 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends

and Future Directions) (ICRITO), Noida, India, pp. 1–5 (2021). https://doi.org/10.1109/ICRITO51393.2021.9596322
18. Qureshi, K.A., Malick, R.A.S., Sabih, M., Cherifi, H.: Complex network and source inspired COVID-19 fake news classification on Twitter. IEEE Access **9**, 139636–139656 (2021). https://doi.org/10.1109/ACCESS.2021.3119404
19. Theophilo, A., Padilha, R., Andaló, F.A., Rocha, A.: Explainable artificial intelligence for authorship attribution on social media. In: ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, Singapore, pp. 2909–2913 (2022). https://doi.org/10.1109/ICASSP43922.2022.9746262
20. Shreya, K., Kothapelly, A., Deepika, V., Shanmugasundaram, H.: Identification of fake accounts in social media using machine learning. In: 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, pp. 1–4 (2022). https://doi.org/10.1109/ICERECT56837.2022.10060194
21. Rezaimehr, F., Dadkhah, C.: Injection shilling attack tool for recommender systems. In: 2021 26th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, pp. 1–4 (2021). https://doi.org/10.1109/CSICC52343.2021.9420553
22. Garg, S., Dubey, A.: Fake Tweet data analysis using machine learning methods. In: 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 1648–1654 (2021). https://doi.org/10.1109/ICECA52323.2021.9675856
23. Ajesh, F., Aswathy, S.U., Philip, F.M., Jeyakrishnan, V.: A hybrid method for fake profile detection in social network using artificial intelligence. Secur. issues Priv. Concerns Industry 4.0 Appl. 89–112 (2021). https://doi.org/10.1002/9781119776529.ch5
24. Chavan, P.V., Balani, N.: Design of heuristic model to improve block-chain-based sidechain configuration. Int. J. Comput. Sci. Eng. **1**(1), 1. (2022). https://doi.org/10.1504/ijcse.2022.10050704
25. Balani, N., Chavan, P., Ghonghe, M.: Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks. Multimedia Tools Appl. **81**(25), 36699–36713 (2022). https://doi.org/10.1007/s11042-021-11604-6
26. Sai Raja, E.V., Aditya, B.L.V.S., Mohanty, S.N.: Fake profile detection using logistic regression and gradient descent algorithm on online social networks. EAI Endorsed Trans. Scalable Inf. Syst. **11**(1) (2023). https://doi.org/10.4108/eetsis.4342
27. Aditya, B.L.V.S., Mohanty, S.N.: Heterogenous social media analysis for efficient deep learning fake-profile identification. IEEE Access **11**, 99339–99351 (2023). https://doi.org/10.1109/ACCESS.2023.3313169
28. Aditya, B.L.V.S., Rajaram, G., Hole, S.R., Mohanty, S.N. (2023). F2PMSMD: Design of a Fusion Model to Identify Fake Profiles from Multimodal Social Media Datasets. In: Nandan Mohanty, S., Garcia Diaz, V., Satish Kumar, G.A.E. (eds) Intelligent Systems and Machine Learning. ICisML 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 471. Springer, Cham. https://doi.org/10.1007/978-3-031-35081-8_2