

Ensemble-Based Machine Learning Approach for Detecting Arabic Fake News on Twitter

Saadi Mohammed Saadi^{1*}, Waleed Al-Jawher²

¹ Iraqi Commission for Computers and Informatics / Informatics Institute of Postgraduate Studies, Baghdad 10001, Iraq

² Department of Electronic and Communication, Uruk University, Baghdad 10001, Iraq

Corresponding Author Email: phd202130692@iips.edu.iq

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ria.380103>

ABSTRACT

Received: 5 September 2023

Revised: 1 November 2023

Accepted: 9 November 2023

Available online: 29 February 2024

Keywords:

fake news, Support Vector Machine (SVM), social media, gradient boosting, ensemble methods

The rise of social media platforms has led to a significant increase in the spread of false or misleading information, which has become a major issue of concern. Twitter faces the difficult task of identifying and reducing the spread of 'fake news', which refers to material that is erroneously or intentionally spread. This type of content frequently includes false information, biased information, and data that is provided without considering its full context. The swift and comprehensive proliferation of platforms such as Twitter worsens the problem by enabling the widespread and rapid dissemination of unverified content, often leading to its viral dissemination and contributing to the propagation of falsehoods. This paper presents a specialized machine learning approach that utilizes an ensemble-based strategy to identify and classify false information on the social media platform Twitter. This approach utilizes the combined power of various classifiers, such as Support Vector Machines (SVM), k-Nearest Neighbors (KNN), and Gradient Boosting (GBoost), to create a strong prediction model by combining multiple weaker learners. Every classifier undergoes rigorous training using a specific set of variables, including text content, user profile information, and tweet metadata. This enables a thorough analysis to identify fake news. Within the proposed system, following separate training, the classifiers generate predictions that are then merged. A neural network is utilized to combine the outputs of all classifiers, resulting in a definitive prediction. This approach tackles the drawbacks of overfitting and improves the capacity of the model to apply to new data, resulting in a higher level of accuracy for the machine learning model. The empirical assessments conducted on a dataset that is freely accessible, containing both genuine and counterfeit tweets, show that the ensemble model performs much better than the individual base classifiers and traditional machine learning models. The proposed method attained an accuracy of 0.963, along with an Area Under the Curve (AUC) of 0.964, surpassing the precision, recall, and F1 scores of its individual classifiers. The results confirm the efficacy of the ensemble machine learning architecture as a dependable method for identifying false information in Arabic on Twitter. This has implications for wider usage on different social media platforms.

1. INTRODUCTION

Fake news spreads differently on social media. Traditional News starts with well-established media businesses with fact-checking and editorial standards. Unlike social media, where anybody can publish, these institutions are limited, making it easier to regulate and manage news accuracy. Millions of users create diverse content, making management and accuracy difficult. Additionally, speed and reach in the second difference. Traditional news takes longer to propagate since it's edited and validated. Fake news spreads quickly on social media. The rapid spread of viral disinformation makes it impossible to control. Control and verification are the third difference. Traditional media are responsible for accuracy. Social media users must verify without a central process. The fourth difference is user involvement and accessibility. Traditional news consumption is passive, with few outlets. User interaction is possible on social media. Creating, sharing,

and commenting on content makes the environment more interactive. NLP and ML are needed to recognize social media fake news automatically. Due to controlled environments, traditional news sources need less automated systems [1]. For fake news, word disambiguation, sentiment analysis, and spam detection, NLP and ML classify and organize text. These technologies are essential because of social media's global reach and enormous text data. Traditional media is controlled and accountable, but social media is user-driven. This change greatly affects fake news identification and management [2-5]. Due to social media's broad use, fake news detection (FND) is crucial in the digital era. An enlarged view of fake news' financial, political, and social effects: Financial markets can be impacted by fake news. Irrational investor behavior can cause market collapses due to misinformation about a company, economic policy, or market conditions. False information affects customer behavior, harming businesses and economies. Fake product or service news can damage a

company's reputation or increase its value. Economic effects: Fake news can damage financial institutions and markets, causing long-term economic damage. Political Effects: Fake news may swing elections by influencing voter behavior. Polarization of Society: False political information can deepen social differences and foster mistrust and enmity amongst political groupings. Fake news weakens democratic societies by undermining public trust in democratic institutions and procedures. Public Health: Misinformation about COVID-19, immunization, and medical therapies can harm public health. Social Harmony: Fake news can cause hatred, violence, and misunderstanding between communities, causing conflict. Media and Information Credibility: Fake news undermines reputable news sources and the public's ability to tell the truth from fiction [6, 7]. These detrimental effects can be mitigated by effectively detecting bogus news. FND methods detect and stop misleading information before it harms [8]. Due to its complexity, this work requires technology solutions and collaboration between governments, social media platforms, news organizations, and the public. The goal is to develop an informed and discriminating online community that can reject misinformation. Research and advancement in fake news identification are crucial. Fake news affects financial markets, among other things [9], Rumors can destabilize markets. Foolish reactions to fake news are becoming more widespread as consumers decide based on knowledge [10, 11].

Countering erroneous information has led to the development of fact-checking websites and computational methods. However, these remedies have limitations. Methods of Computing: These technologies identify fake news by analyzing article wording. They may look for writing style, phrase building, and word choice patterns associated with misinformation. Contextual Limitations: Computational methods may misinterpret data context, resulting in inaccuracies. Misinformers' Change: Fake news producers may change their methods to escape detection by these technologies. Implementation Complexity: Developing effective algorithms for altering data is challenging and resource-intensive [12]. Verification websites like PolitiFact and Snopes: These websites manually verify claims, particularly those viral on social media or in the media. Rich in Resources: Fact-checking is laborious and requires skilled human fact-checkers, making it hard to keep up with the huge amount of content published daily. Scope Limit: While some fact-checking groups focus on politics, they may ignore other fields with frequent erroneous information. Fact-checking takes time; thus incorrect information can spread before being challenged. Public Perception and Faith: In politically sensitive situations, fact-checkers' prejudice may affect public faith. Some solutions combine human and machine fact-checking. These have issues too: Integrating automated and human verification processes efficiently is tough. Balancing Scalability and Accuracy: Automation is scalable, but precision and dependability are challenging to guarantee. In conclusion, fact-checking websites and computational detection methods are useful tools in fighting fake news, but they are not perfect. They struggle with scope, intricacy, domain limits, and public opinion. This highlights the need for continual innovation and progress in false news detection methods and larger public education and media literacy efforts [13].

NLP and ML are employed in fake news identification because they can process and evaluate massive amounts of data, including unstructured Web data. This article discusses

these methods, their shortcomings, and how new ways can enhance them: Common NLP/ML Fake News Detection Methods: NLP systems detect false news language in article text. This may include reviewing writing style, word choice, and sentence structure. Analysis of sentiment the emotional tone of an item can indicate bias or deception [14]. The distribution of linguistic elements in fake and authentic news can show misleading patterns [15]. It analyzes how fake news spreads across networks and assesses it as true or false. It examines textual features and theoretical replies to determine deceit. Most research focuses on detecting and classifying fake news on Facebook and Twitter [16]. Text and metadata information are used to train ML models to categorize news as real or false. Modern NLP and ML Techniques' Limitations: Automated systems can misidentify subtle fake news due to context and nuance issues. Fake news spreaders can adapt to avoid detection by these methods. While some models perform well in their trained area, they may not generalize well. The quality and diversity of training data determine ML model performance. Biased or inadequate training data can affect model performance. Improvements New Methods: Advanced NLP techniques may help understand news context and intricacy. Creating models that work across domains and fake news kinds. Including Network Dynamics: Consider how information moves across networks to verify news beyond textual analysis. Using NLP and ML with human verification or other data sources to improve accuracy. Developing systems that can adapt to misleading methods.

In conclusion, NLP and ML have improved fake news identification, although they have limits. These include difficulties with nuanced and contextually rich data, domain generalization, and the need for large, unbiased training datasets [12, 17, 18]. New methods improve analysis and include more data and methods to address these issues. This methodological growth underscores the dynamic and difficult nature of fighting fake news online.

The following are the important contributions made in this work:

This work presents an efficient model for detecting Arabic fake news content using multiple base classifiers, utilizing an ensemble to aggregate outputs for final prediction.

Because of the platform's complexity, noise, bias, and dynamic nature, traditional Twitter false news detection tools, such as rule-based systems and machine learning techniques, may suffer.

The study addresses the growing incidence of fake news on social media, focusing on Arabic. It provides an ensemble-based machine-learning strategy for detecting bogus news on Twitter, incorporating multiple classifiers trained on diverse variables. This approach improves the performance and robustness of fake news detection. With this arrangement, the paper is now: Section 2 explores Related works, while Section 3 describes the proposed method used in developing the classification model. Section 4 describes the results and discussion of the proposed method, and Section 5 concludes the study.

2. RELATED WORK

Recent research has looked into the prevalence of false news on social media and presented methods for spotting it; how to make a prediction includes preparing a deceptive article [19]. FND methods vary based on target data and ML, considering

main tweets or posts, discussions, replies, and comments in news items [20]. The study found that English fake news identification has the most studies, whereas Arabic false news detection is still restricted [21]. The authors created a model that reduces false alarm rates by identifying and classifying social media fake news using entropy-based feature selection and Min-Max Normalization. Give these technical words a brief explanation:

Selection of Features Based on Entropy: This approach finds task-relevant features by using entropy. Features that provide information or decrease ambiguity are preferred. When certain textual or metadata features may point to lies, this method is helpful in detecting fake news. Values of dataset features are mapped via Min-Max Normalization to a standard scale, often from 0 to 1. The $(\text{value} - \text{min}) / (\text{max} - \text{min})$ transformation is applied, where min and max represent the minimum and maximum values of the feature. Every characteristic contributes equally to the analysis in machine learning models to guarantee that no factor influences the output in a disproportionate way [22]. The authors created a system for detecting false news items that use neural architectures such as CNN and Bi-GRUs, with a focus on longer text pieces. Evaluated the method on three publicly available datasets, and one the authors constructed regarding Accuracy, Precision, recall, and macro F1 score, Fake Flow exceeded baseline models, with Long prior model marginally outperforming it. The successive outcomes are 0.96, 0.93, 0.97, and 0.96 for the macro F1 score. The publication's authors [23] developed a machine-learning model to detect fake news, outperforming existing algorithms by 4.8% and achieving an accuracy of 81.7% when integrated into Facebook Messenger chatbots. Ahmed et al. [24] used machine-learning models to extract linguistic features from textual articles, achieving the highest accuracy (92%) with SVM and logistic regression. However, accuracy decreased as n-grams increased, affecting classification models. Qawasmeh et al. [25] used deep learning models to detect fake news on the FNC-1 English dataset, obtaining 85.3% and 82.9% accuracy despite Arabic FND being younger than English FND. Mahlous and Al-Laith [26], Conventional machine learning techniques were applied to identify fake news tweets about COVID-19 in this investigation. They reduced seven million Arabic tweets to just 5.5 million using preprocessing techniques. They developed a false news annotation system using feature extraction techniques and six machine learning classifiers. Using Logistic Regression, their model generated an F1 core of 93.3%. Jardaneh et al. [27] employed sentiment analysis, content-related and user-related variables, and algorithms from Random Forest, Decision Tree, AdaBoost, and Logistic Regression to detect bogus Arabic news with an accuracy of 76%. Najadat et al. [28] suggested AFND-LSTM and AFND-CNN-LSTM as deep learning models for their Arabic false news detection approach. They compare 422 assertions and 3,042 articles using data from the Syrian war and Middle Eastern political concerns. The results reveal that AFND-CNN-LSTM performs 70% better than AFND-LSTM. Alkhair et al. [29] investigated fake news items in the Middle East using YouTube answers and comments. To establish a new Arab corpus for false news research, they collected 4079 comments from three Arab celebrities and cleansed the data. They employed machine learning classifiers like Multinomial Naive Bayes, Support Vector Machines, and Decision Trees to examine the likelihood that rumors and facts are related. SVM classifier achieves a 95.35% accuracy rate. To identify fake

news in Arabic tweets, Thaher et al. [30] created a hybrid artificial intelligence model. To determine which text vectorization model was the most effective, they tested a variety of machine-learning algorithms. The T.F. model outperformed the L.R. classifier with an accuracy of 0.82 and an F1 score of 0.8042. Finally, the authors of the paper [31] suggested using social media comments to identify bogus news. They processed an Arabic news dataset using Rapid Miner and Python preprocessing methods. We employed Decision Tree, Naive Bayes, SVM, and K-NN as our four machine learning classifiers. In Rapid Miner, the N.B. classifier has an accuracy rate of 87.18%. Fake news is intentionally manufactured, fact-checked, and verified as misinformation to deceive consumers. It is made to mislead readers and contains verified information. Researchers refer to publications that purposely publish hoaxes, propaganda, and other false material and propagate on social media as fake news. It can use three broad categories to classify it [32].

1. Articles with entirely false news that the author created.
2. Write Satirical news with the audience's enjoyment in mind.
3. articles that are inaccurately written and contain some true news. Specifically created to advance a cause or sway opinion [33]. Rubin and his team discuss three types of false news, each representing inaccurate or misleading reporting [34].

3. PROPOSED METHOD

The following learning algorithms are part of the primary block diagram for the proposed approach. Figure 1 depicts the proposed ensemble method and our suggested technique for assessing the effectiveness of false news detection classifiers.

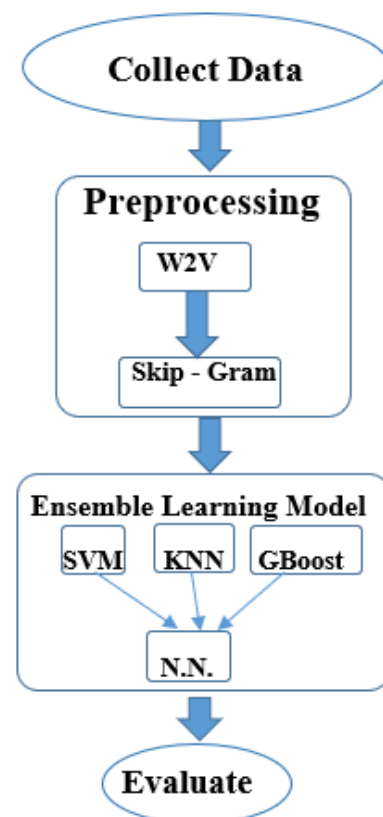


Figure 1. Proposed ensemble method

3.1 Data collection

Compile a dataset of Arabic tweets categorized as either true or fraudulent news. Use various sources to ensure the dataset is broad and covers various topics.

3.2 Preprocessing

In this paper, the proposed method for preprocessing the dataset is done in several phases to ensure that the original text, which includes noise and numerous undesired features, was cleaned in multiple stages, as shown in Table 1:

- 1- D0, the original dataset
- 2- D1, the first clean data, which comprises Remove Stop Words, Remove Noise, Normalize, and Punctuations, will improve the accuracy of the proposed approach to discern between true and fake news.
- 3- D2, the new data that resulted from the second cleaning stage by applying Root steaming techniques to reduce the data set size for significantly faster learning.
- 4- D3, the final cleaning stage known as light steaming, is a little reduction for the dimensionality of the data set to speed up the procedure. The suggested model will include all the above data sets and compare the results to determine the best.

Table 1. Multi-stage preprocessing of Twitter news from a data set

Data Name	Data Set
D0	قبل ظهور وباء فيروس كورونا، تنبأت بعض الأعمال الفنية بظهور "أوبئة مشابهة ووضع مصير العالم في خطر، أشهرها فيلم Contagion " عام 2011 .
D1	قبل ظهور وباء تنبأت بعض الاعمال الفنية بظهور اوبئه مشابهه ووضع مصير العالم اشهرها فيلم عام
D2	قبل ظهر وبء تنب بعض عمل فنه ظهر وبء تنبه وضع صير علم شهر يلم عام
D3	قبل ظهور باء تنب بعض اعمال فنيه بظهور اوبئه مشابهه ضع مصير عالم اشهر فيلم عام

3.3 Feature extraction

This study uses machine learning to convert textual expressions into vector expressions for mathematical operations in Natural Language Processing (NLP) studies. It extracts word-to-vector and Skip-Gram features from preprocessed data using semantically superior Word2Vec. One well-liked NLP feature extraction technique is Word2Vec. Vector word embedding is taught to Word2Vec models. Vectors represent word associations and semantic meanings. Large text datasets are used to train Word2Vec models. Words are predicted by the algorithms based on their context or the other way around. Word2Vec makes use of Skip-Gram and CBOW architectures. CBOW: Uses context words to predict the target word. Skip-Gram anticipates context terms for target words. After training, a high-dimensional vector (of several hundred dimensions) is assigned to each corpus word. In this space, words with similar meanings have close vectors. Word2Vec is trained to vectorize any text. These vectors can be used in sentiment analysis, topic modeling, and other NLP applications; Word2Vec is the recommended technique. Word2Vec is superior to bag-of-words models for meaning-based tasks because it captures semantic relationships between words. In contrast to one-hot encoding, Word2Vec represents

densely, reducing computing overhead. Unlike previous methods, Word2Vec can capture word meanings in various contexts. Word2Vec models learned on one dataset can be applied to another for transfer learning. Word embedding from Word2Vec can be tailored to suit NLP workloads.

3.4 Model for ensemble learning

A machine learning technique known as ensemble learning teaches weak learners to work together to solve problems for better outcomes. There are three types: Bagging, Boosting, and stacking. Bagging focuses on producing models with lower variance, whereas stacking and boosting strive to create robust models with low bias and variation. This research uses the stacking ensemble method to combine multiple models, such as KNN, G.B., and SVM, to produce a single precise model. Trained the proposed ensemble mode to forecast previously trained models' performance and sent classification information to stacking-based ensemble learners. This section presents an overview of the algorithms employed in the ensemble learning models discussed in this study.

A. Nearest Neighbors (KNN): KNN is a non-parametric, instance-based, supervised machine learning technique for classification and regression applications. KNN generates recommendations based on data points closest to the input data point [35].

B. Gradient Boosting: Machine learning techniques like ensemble learning combine weaker models to create a more potent predictive model. This process involves training base learners, calculating residuals, and combining predictions. A learning rate parameter regulates the contribution of each model to avoid overfitting. Methods such as subsampling and depth control are employed.

C. Support Vector Machine: A binary classification model called the Support Vector Machine (SVM) uses feature sets to predict a hyperplane that categorizes data points. The mathematically defined cost function of the model seeks to locate the plane that best divides the data points of two classes by the most significant margin [36].

The goal of the SVM model, which consists of sigmoid, kernel, Gaussian, and basic linear SVM models, is to locate the plane that divides data points of two classes with the most significant margin in an N-dimensional space. According to the sequential Eqs. (1), (2), and (3) [6].

$$J(\theta) = \frac{1}{2} \sum_{k=1}^n \theta_j^2, \quad (1)$$

such that

$$\theta^k X^{(n)} \geq 1, y^{(n)} = 1, \quad (2)$$

$$\theta^k X^{(n)} \leq -1, y^{(n)} = 0, \quad (3)$$

3.5 Building the model

This study proposes stacking SVM, KNN, and GBoost to train multiple classifiers using extracted features. This study develops an ensemble-based stacking prediction model to categorize text pieces as true or fake news. Researchers developed an ensemble stacking learning algorithm (ESLA) using numerous fundamental categorization models. The design uses k-nearest Neighbors, SVM, and Gradient Boosting.

ESLA stacks forecasts for better accuracy, making it unique. A trained meta-model, Ensemble Decision, predicts news article integrity using base model predictions from KNN, SVM, or GBoost for strategic ensemble learning model stacking. Using The strengths of each method improves model performance. When dimensions surpass samples, SVM excels—kernel functions model complex non-linear relationships. Good separation makes SVM robust. SVM ensemble prediction excels in binary categorization. It defines ensemble decision bounds. K-Nearest Neighbors solves basic categorization problems. Data distribution is not assumed, which is important in real-world situations where data may not follow theoretical assumptions. KNN provides more natural, distant ensemble decision-making. It finds local patterns other models overlook. Choose Gradient Boosting for binary, definite, and numerical data. It fits well even when overfitted. Flexibility comes from optimizing any differentiable loss function. GBoost enhances ensembles incrementally. Learn from model errors to improve the ensemble. Every model approaches the issue differently. KNN finds local patterns, SVM defines boundaries, and GBoost enhances predictions. Stacked model predictions produce a final model. Our diverse base models give the final model complete characterizations that capture different data aspects. Combine these models to reduce ensemble bias and variation. Some models’ pros outweigh the cons. Trained the suggested ensemble mode to predict model performance and offered stacking-based ensemble learners classification information.

3.6 Evaluation

Performance evaluation methodologies have long been used in categorization and have become standard performance evaluation measures in related fields. The metrics include accuracy, sensitivity, and specificity, and the equations are as follows [37]:

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (4)$$

The true positive rate (T.P.) and false positive rate (F.P.) greatly influenced the recall or sensitivity of positive instances.

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad (5)$$

The following equation computes the accuracy, the percentage of accurate predictions, and the false-negative rate (F.N.), which stands for the false-negative rate.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (6)$$

The term “T.N.” denotes true negative, while “sensitivity” refers to the level of positive records that yield the correct result for every positive record.

$$\text{Sensitivity} = \text{TP} / (\text{TP} + \text{FN}) \quad (7)$$

Particularity refers to the accuracy of accurately arranging positive records out of every single positive record.

$$\text{Specificity} = \text{TN} / (\text{TN} + \text{FP}) \quad (8)$$

The F-measure tool processes a few normal data recovery accuracy and reviews measurements.

$$F = 2 * \text{precision} * \text{recall} / (\text{precision} + \text{recall}) \quad (9)$$

True positive and negative (T.P.) and false positive (F.P.) are used for accurate classification, while false negative and F.N. are used for inaccurate classification. The accuracy of a test depends on its ability to accurately distinguish between fake and real news instances, with sensitivity referring to sensitivity and specificity to specificity. The study calculates prediction accuracy using various classifiers and models, with the suggested Stack model showing high training, testing, sensitivity, and specificity values. Regarding results, the ESLA algorithm performed better than other single classifiers. Table 2 illustrates the performance indicators for the proposed model.

Table 2. The result of the proposed model performance

Type of Model	AUC	CA	F1	Precision	Recall
Stack Ensemble Model	0.964	0.963	0.963	0.963	0.963
KNN	0.935	0.864	0.864	0.866	0.864
Gradient Boosting	0.785	0.785	0.733	0.735	0.732
SVM	0.799	0.799	0.707	0.709	0.709

4. RESULTS AND DISCUSSION

The paper compares the proposed method with previous works, comparing Fake News Detection Models using ML and DL-related works, as shown in Table 3. Which represents a summary of the methods used and the type of model, whether it was machine learning or deep learning, in addition to the language used in the social media data set, which was represented by detecting false or real news, whether it was English or Arabic, where we noticed that the proposed method had the best performance when compared to previous methods. It was adopted to expose fake news in Twitter tweets. Languages used in social media datasets have distinct linguistic characteristics, cultural contexts, and colloquial usage patterns that can significantly impact the identification of false news. ML false news detection systems were investigated using Arabic and English datasets. Every language has a unique lexicon, syntax, and grammar. The efficiency of ML or DL models may depend on how well they comprehend these unique characteristics. English-trained computers may find Arabic’s rich morphology and intricate phrase patterns challenging. Language-specific word and phrase contexts differ significantly. Fake news detectors must understand slang and cultural variances. In one language, a scathing or humorous remark could be taken seriously in another, impacting the identification of fake news. Annotated, high-quality datasets are necessary for efficient model training. The lack of datasets in certain languages makes it difficult to create models. Certain models better process certain languages. Because word order is flexible, word order models might perform better in English than in Arabic. After training and testing the data summarized in Table 3, the result performance that displays the measurement performance of each algorithm; here in this paper, note that when implementing the three algorithms (KNN, GBoost, and SVM) separately, the results are as follows (0.935, 0.785, and 0.799), and after applying the proposed method using a stacking model consisting of several rules- predict machine learning models using stacking method.

When we work, we use the trained base models to make predictions about the validation set. Used in these features in These predictions as the meta-model. Then, we train the model using the three algorithms as inputs to the model) The proposed model learns to combine the predictions of the base models and produces the final prediction for the ensemble. The performance value of the stacked set model using appropriate metrics on the validation set. Refine the hyper parameters of the baseline models, the meta-model, and any other parameters that affect group performance.

While applying the proposed method, the results were better, as the accuracy reached 0.963, which is a better result than it was previously when implementing the separate algorithms, which is the same value in F1, Recall, and Precision, in addition to the AUC equal to 0.964, which is higher when compared to the AUC value of the three algorithms. The KNN algorithm achieved the same performance for each F1 Recall, equal to 0.864; therefore, the distribution of the remaining

results follows the same pattern as accuracy. At the same time, precision was equal to 0.866, and AUC was equal to 0.935. For the GBoosting algorithm, the performance for each of F1, Recall, and Precision was (0.735, 0.733, 0.733), while the accuracy was equal to 0.732 and the AUC equal to 0.785. Finally, when implementing the SVM algorithm, the results were represented by the same performance for each Precision, Recall, and accuracy, equal to 0.709. At the same time, F1 was equal to 0.707, and AUC was equal to 0.799. High recall and precision indicate that the stack ensemble model is good at recognizing bogus news and mislabeling authentic material. Equal values across these variables suggest balanced classification performance. Shows that combining models improves fake news detection accuracy and dependability. A diverse methodology can better capture fake news' complexity and nuances.

Table 3 illustrates Compares Works on F.N. Detection using ML and DL.

Table 3. Compares works on F.N. detection using ML and DL

Ref.	Language Applied	Type of Learning	Dataset	Method Applied	Classifiers	Success ML	Best Performance for (Acc, Precision, Recall, and F1)
[21]	English	Machine Learning	5,800 tweets	The study offers a model for predicting the appearance of fake news.	SVM, Random Forest, and RNN	Random Forest	81.9% (Accuracy)
[22]	English	Deep Learning	Three different datasets: The authors used two available datasets (700 and 500) and constructed a third. The study employs three datasets, including 15,500 posts from Fake News Net and 230 Facebook posts, to analyze fake news.	The Fake Flow technique simulates the flow of expressive information in the news to identify fake news.	Bi-GRUs, or bidirectional gated recurrent units, and CNN	CNN	0.96(Accuracy)
[23]	English	Machine Learning	For Facebook, (12,600) FN _s pieces from Kaggle.com and (12,600) real articles.	A Facebook Messenger chatbot is using the proposed machine-learning technique, which tries to identify bogus news.	The work focuses on crowdsourcing with a content-based approach, social signal-based logistic regression, and HC-CB-4 crowdsourcing with harmonic Boolean labels.	HC-CB-4	81.7%(Accuracy)
[24]	English	Machine Learning	The FNC-1 dataset includes 1683 articles on train bodies and 49972 headlines on train stances.	The paper presented an n-gram analysis and multiple feature extraction methods-based FND algorithm.	ML techniques used for detection include KNN, SVM, L.R., LSVM, D.T., and stochastic gradient descent (SGD).	LSVM + LR	92%(Accuracy)
[25]	English	Machine Learning	Seventy million Arabic tweets (COVID-19)	The idea calls for using powerful ML techniques to detect FN _s automatically.	The bidirectional LSTM concatenated and Multihued LSTM models are separate in machine learning.	Bidirectional LSTM concatenated Model	85.3% accuracy performance.
[26]	Arabic	Deep learning	The text includes one thousand eight hundred sixty-two tweets relating to the Syrian situation.	The model's suggested COVID-19 false news classification algorithm is for Arabic-language sources.	N.B., L.R., SVM, MLP, R.F., and XGB) were applied to improve model performance.	The L.R. classifier employs n-gram-level Term Frequency-Inverse Document Frequency (TF-IDF).	87.8%
[27]	Arabic	Machine Learning	The study utilized a dataset of 422 claims and 3,042 articles to analyze the Syrian war and political issues in the Middle East.	The objective is to create a binary classifier that can categorize a tweet as 'untrustworthy' or 'trusted' while providing a probability estimate.	The study utilizes R.F., D.T., L.R., and AdaBoost algorithms for sentiment analysis.	Random Forest AdaBoost	76.%, 77%
[28]	Arabic	Deep Learning	gathered the data from 4079 comments on YouTube.	The study suggests a technique for identifying false news in Arabic by applying multiple deep-learning models.	- M 1 AFND-LSTM. - M 2 AFND-CNN-LSTM	M 2 AFND-CNN-LSTM	70.5%
[29]	Arabic	Machine Learning	1862 Arabic Twitter	Used Arabic comments on YouTube to investigate fake news publications in the Middle East.	MNB, DT, and SVM	SVM	95.35%
[30]	Arabic	Machine Learning		The study proposes using NLP, ML, and Harris Hawks Optimizer as feature selection	This model employs KNN, R.F., SVM, NB, L.R., LDA, D.T., and XGboost algorithms.	L.R. classifier performed the best	82% (Accuracy)

[31]	Arabic	Machine Learning	Create their dataset.	techniques for detecting false news in Arabic tweets. The paper suggests a method for spotting Arabic fake news by utilizing text mining to analyze comments on social media news.	KNN, DT, SVM, and NB.	SVM	87.18%
Proposed model	Arabic	Ensemble-based Machine Learning	2500 Arabic Tweets	This paper proposes a Stack Ensemble Model for Twitter fake news detection, combining multiple base classifiers to generate final predictions by aggregating outputs.	Stack ensemble model KNN, GBoost, and SVM	Stack ensemble model	0.963

5. CONCLUSIONS

In-depth subject knowledge and the capacity to identify linguistic discrepancies are prerequisites for manually assessing news. Social media is a source of fake news. The method proposed in this paper is used in real life. These platforms can automatically identify false information by utilizing machine learning algorithms. This aids in quickly identifying and removing misinformation. These algorithms allow internet news aggregators to assess an article's dependability before posting. Users are guaranteed accurate information as a result. Human fact-checkers in fact-checking organizations benefit from models. Programs can identify fake news using vast amounts of data. For these businesses, this increases scalability and efficiency. These models assist governments in keeping an eye on and reining in bogus news that compromises policy, health, and security. Accurate information is needed in public health emergencies; these algorithms can swiftly spot and remove misinformation. Educators can use these models to teach disinformation and media literacy. They also assist in spotting deceptive patterns and outcomes. More significant advantage: In this study, we investigated using machine learning models and a stacked ensemble to identify fake news items. The data we used in our study came from Twitter tweets and contained news pieces from multiple categories to capture the majority of news instead of neatly classifying political news. This strategy aims to identify linguistic traits that set true news apart from false information. Retrieved various textual features from the articles using the Word2Vec Skip-Gram method, then updated the models with these chosen attributes. They were trained and parameterized to guarantee that the learning models performed at their best. Some models have attained a better degree of accuracy in comparison to others. This study examined various performance measures for each method of machining. Using graph theory and deep learning techniques, the group learners—outperforming the individual learners by 0.963 points on all performance measures—could identify the primary sources disseminating false information. Detecting bogus news in videos in real time is another possible future strategy.

ACKNOWLEDGMENTS

The authors would like to thank the Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics (<https://iips.edu.iq/>), Baghdad-Iraq, for its support in the present work.

REFERENCES

- [1] Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H., Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3): 554-559. <https://doi.org/10.1073/pnas.1517441113>
- [2] Sebök, M., Kacsuk, Z., Máté, Á. (2022). The (real) need for a human touch: Testing a human-machine hybrid topic classification workflow on a New York Times corpus. *Quality & Quantity*, 56: 3621-3643. <https://doi.org/10.1007/s11135-021-01287-4>
- [3] Jin, Z., Cao, J., Guo, H., Zhang, Y., Wang, Y., Luo, J. (2017). Detection and analysis of 2016 us presidential election-related rumors on Twitter. In *International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation*, Washington, DC, USA, pp. 14-24. <https://doi.org/10.48550/arXiv.1701.06250>
- [4] Alazab, M., Awajan, A., Mesleh, A., Abraham, A., Jatana, V., Alhyari, S. (2020). COVID-19 Prediction and detection using deep learning. *International Journal of Computer Information Systems and Industrial Management Applications*, 12: 168-181. https://doi.org/10.1007/978-3-319-60240-0_2
- [5] Mahlous, A., Laith, A. (2021). Fake news detection in Arabic tweets during the COVID-19 pandemic. *International Journal of Advanced Computer Science and Applications*, 12(6): 778-788.
- [6] Ahmad, I., Yousaf, S., Ahmad, M. (2020). Fake news detection using machine learning ensemble methods. *Complexity*, 8885861: 1-11. <https://doi.org/10.1155/2020/8885861>
- [7] Khan, T., Michalas, A., Akhunzada, A. (2021). Fake news outbreak 2021: Can we stop the viral spread. *Journal of Network and Computer Applications*, 190: 103112. <https://doi.org/10.1016/j.jnca.2021.103112>
- [8] Al-Yahya, M., Al-Khalifa, H., Al-Baity, H., AlSaeed, D., Essam, A. (2021). Arabic Fake news detection: Comparative study of neural networks and transformer-based approaches. *Complexity*, 5516945: 1-10. <https://doi.org/10.1155/2021/5516945>
- [9] Kogan, S., Moskowitz, T.J., Niessner, M. (2019). Fake news: Evidence from financial markets. <https://ssrn.com/abstract=3237763>
- [10] Robb, A. (2017). Anatomy of a fake news scandal. *Rolling Stone*, 1301: 28-33.
- [11] Soll, J. (2016). The long and brutal history of fake news. *Politico Magazine*, 18(12): 2016.
- [12] Rubin, V.L., Chen, Y., Conroy, N.K. (2015). Automatic deception detection: Methods for finding fake news.

- Proceedings of the Association for Information Science and Technology, 52(1): 1-4. <https://doi.org/10.1002/pr2.2015.145052010082>
- [13] Kanchana, M., Kumar, V.M., Anish, T.P., Gopirajan, P. (2023). Deep fake BERT: Efficient online fake news detection system. In Proceedings of the 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, pp. 1-6. <https://doi.org/10.1109/ICNWC57852.2023.10127560>
- [14] Shu, K., Sliva, A., Wang, S., Tang, J., Liu, H. (2017). Fake news detection on social media: A data mining perspective. ACM SIGKDD Explorations Newsletter, 19(1): 22-36. <https://doi.org/10.1145/3137597.3137600>
- [15] Roy, S., Aral, S. (2018). The spread of true and false news online. Science, 359(6380): 1146-1151.
- [16] Allcott, H., Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2): 211-236. <https://doi.org/10.1257/jep.31.2.211>
- [17] Rubin, V.L., Conroy, N., Chen, Y., Cornwell, S. (2016). Fake news or truth? Using satirical cues to detect potentially misleading news. In Proceedings of the Second Workshop on Computational Approaches to Deception Detection, San Diego, CA, USA, pp. 7-17.
- [18] Jwa, H., Oh, D., Park, K., Kang, J.M., Lim, H. (2019). exBAKE: Automatic fake news detection model based on bidirectional encoder representations from transformers (BERT). Applied Sciences, 9(19): 4062. <https://doi.org/10.3390/app9194062>
- [19] Wotaiji, T.A., Dhannoon, B.N. (2023). An effective hybrid deep neural network for Arabic fake news detection. Baghdad Science Journal, 20(4): 1392. <https://doi.org/10.21123/bsj.2023.7427>
- [20] Veysel, A.P.B., Thai, M.T., Nguyen, T.H., Dou, D. (2019). Rumor detection in social networks via deep contextual modeling. In Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, Canada, pp. 113-120. <https://doi.org/10.1145/3341161.3342896>
- [21] Akinyemi, B., Adewusi, O., Oyebade, A. (2020). An improved classification model for fake news detection in social media. International Journal of Information Technology and Computer Science, 2020(1): 34-43. <https://doi.org/10.5815/ijitcs.2020.01.05>
- [22] Ghanem, B., Ponzetto, S.P., Rosso, P., Rangel, F. (2021). Fake-Flow: Fake news detection by modeling the flow of affective information. <http://arxiv.org/abs/2101.09810>
- [23] Della Vedova, M.L., Tacchini, E., Moret, S., Ballarin, G., DiPierro, M., De Alfaro, L. (2018). Automatic online fake news detection combining content and social signals. In Conference of Open Innovation Association, FRUCT. Jyväskylä, Finland, pp. 272-279. <https://doi.org/10.23919/FRUCT.2018.8468301>
- [24] Ahmed, H., Traore, I., Saad, S. (2017). Detection of online fake news using n-gram analysis and machine learning techniques. In Proceedings of the International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, Vancouver, BC, Canada, pp. 127-138. https://doi.org/10.1007/978-3-319-69155-8_9
- [25] Qawasmeh, E., Tawalbeh, M., Abdullah, M. (2019). Automatic identification of fake news using deep learning. In 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), Granada, Spain, pp. 383-388. <https://doi.org/10.1109/SNAMS.2019.8931873>
- [26] Mahlous, A.R., Al-Laith, A. (2021). Fake news detection in Arabic tweets during the COVID-19 pandemic. International Journal of Advanced Computer Science and Applications, 12(6): 778-788.
- [27] Jardaneh, G., Abdelhaq, H., Buzz, M., Johnson, D. (2019). Classifying Arabic tweets based on credibility using content and user features. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, pp. 596-601. <https://doi.org/10.1109/JEEIT.2019.8717386>
- [28] Najadat, H., Tawalbeh, M., Awawdeh, R. (2022). Fake news detection for Arabic headlines-articles news data using deep learning. International Journal of Electrical and Computer Engineering, 12(4): 3951-3959. <https://doi.org/10.11591/ijece.v12i4.pp3951-3959>
- [29] Alkhair, M., Meftouh, K., Smaïli, K., Othman, N. (2019). An Arabic corpus of fake news: Collection, analysis, and classification. In International Conference on Arabic Language Processing, Nancy, France, pp. 292-302. https://doi.org/10.1007/978-3-030-32959-4_21
- [30] Thaher, T., Saheb, M., Turabieh, H., Chantar, H.J.S. (2021). Intelligent detection of false information in Arabic tweets utilizing hybrid Harris hawks based feature selection and machine learning models. Symmetry, 13(4): 556. <https://doi.org/10.3390/sym13040556>
- [31] Alanazi, S.S., Khan, M.B. (2020). Arabic fake news detection in social media using readers' comments: Text mining techniques in action. International Journal of Computer Science and Network Security, 20(9): 29-35.
- [32] Ananth, S. (2019). Fake news detection using convolution neural network in deep learning. International Journal of Innovative Research in Computer and Communication Engineering, 7(1): 49-63.
- [33] Schow, A. (2017). The 4 types of 'fake news'. Observer. <http://observer.com/2017/01/fake-news-russia-hacking-clinton-loss>
- [34] Rubin, V.L., Chen, Y., Conroy, N.K. (2015). Deception detection for news: Three types of fakes. Proceedings of the Association for Information Science and Technology, 52(1): 1-4. <https://doi.org/10.1002/pr2.2015.145052010083>
- [35] Al-Saif, H., Al-Dossari, H. (2018). Detecting and classifying crimes from Arabic Twitter posts using text mining techniques. International Journal of Advanced Computer Science and Applications, 9(10): 377-387.
- [36] Hussain, M.G., Hasan, M.R., Rahman, M., Protim, J., Al Hasan, S. (2020). Detection of Bangla fake news using MNB and SVM classifier. In 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, pp. 81-85. <https://doi.org/10.1109/iCCECE49321.2020.9231167>
- [37] Sarnovský, M., Maslej-Krešňáková, V., Hrabovská, N. (2020). Annotated dataset for the fake news classification in Slovak language. In 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, pp. 574-579. <https://doi.org/10.1109/ICETA51985.2020.9379254>