New Media Detection Technology Based on Big Data Network Intelligent Algorithm

Hui Xiao*

{*Corresponding author: 15926909490@163.com}

School of Big Data, Hubei Polytechnic University(teachers college), 435000, Huangshi, Hubei, China

Abstract. With the continuous development of new media information on the Internet, it has become a vital task to monitor the information spread in new media by using emerging artificial intelligence technologies, such as Big data and machine learning, in order to maintain network order. However, currently existing information feature detection models are mostly based on the characteristics of specific content itself. The challenges faced by this type of information feature detection model include high risk of overfitting, insufficient generalization ability, and failure to fully explore the deep correlation features inherent in media information. Based on this, this article first uses the BERT model to extract multi-level semantics from social media post text content, and then uses GNN technology to obtain the visual characteristics of the image. It can adopt the GCN algorithm for optimization to improve the performance of GNN, which is difficult to quickly converge when facing complex social network topologies. Finally, this paper constructs an illegal information detection model based on Big data network intelligent algorithm. Experiments show that, compared with the two baseline methods of SVM-TS (Support Vector Machine Model for Tabu Search) and EANN (Event Adverse Neural Networks), the illegal information intelligent detection model proposed in this paper shows higher accuracy in identifying false information, rumors, real events and unconfirmed events.

Keywords: New Media Technology, Intelligent Algorithms, Data Analysis, Detection Platform

1 Introduction

1.1 Background and Significance

In recent years, with the vigorous development of new media technology, fields such as audiovisual websites, mobile applications, short video platforms, internet television, and IPTV (Internet Protocol Television) intelligent terminals have also shown a vigorous growth trend. While the new media industry is thriving, there have also been some applications and smart terminals that violate national regulations on network audiovisual and network security management, spreading obscene pornography, bloody violence, and publishing false information [1-2]. In such an open and diverse

ICSETPSD 2023, November 17-18, Coimbatore, India
Copyright © 2024 EAI
DOI 10.4108/eai.17-11-2023.2342813

online space, various negative information is flooding the entire society, and people's trust in new media is decreasing. In order to create a positive network environment, identify false information and safeguard consumers' rights and interests, it can need to use Big data network intelligent algorithm technology to conduct in-depth filtering, personalized screening, real-time detection and accurate search of new media information [3].

1.2 Definition of Relevant Concepts

Intelligent algorithm technology refers to the combination of Big data, Natural language processing, machine learning, data mining, artificial intelligence technology and other technologies to conduct in-depth mining of the audience's use preferences, make the audience's interest points into a map, and then use Big data to conduct analysis, based on different individual behavior differences, to accurately match and recommend them. The operational logic of intelligent algorithm technology constructs a bidirectional selection mechanism between users and data. After the user's behavior of selecting content generates data, the system would rearrange and combine these data with a predetermined order, push the content similar to the user's selected content to the user again, record new data, continuously search for similarities, and gradually improve and perfect the existing data information, thereby enhancing the two-way interaction between the user and the data.

1.3 World Research Status

Social media has the characteristics of convenience, rapid dissemination, and low cost, making it a hot topic in current news consumption. But at the same time, it also provides convenience for criminals to embezzle others' privacy, spread junk and obscene information, manipulate political events, and guide public opinion on social media platforms [4-5]. The illegal information in social media has a serious adverse impact on people and society, and how to identify and timely block illegal information has become a major problem that needs to be solved urgently.

There is currently a lot of research on methods for detecting illegal information in social media. Pratiwi A R D implements SVM (Support Vector Machine) classification and Feature selection based on TF-IDF (Term Frequency – Inverse Document Frequency) weighting, and constructs an Indonesian rumor detection system. The research phase of the system includes the process of collecting data on Twitter social media, followed by preprocessing, including case folding, deletion of relevant webpage links, standardization, and deletion of stop words. Finally, he found that the system achieved good performance in testing scenarios using 10% of test data and single image features [6]. Kumar G uses an artificial neural network to identify malicious consumer nodes by evaluating the response of chat discussions/comments. Finally, the 'Protege' tool is used to demonstrate message exchange from untrusted nodes for upcoming large-scale indications. Finally, execute the expected method on the JAVA functional platform between Big data analysis and Hadoop [7]. On the detection method based on Communication studies, Vu D T proposed a propagation graph embedding method based on graph convolution network to learn the embedding vector, to represent the propagation mode and other characteristics of posts in the propagation process, and then used the full connected neural network to classify the learned embedding vector into different types of rumors. Finally, research has shown that this model can effectively extract and integrate useful features to detect propagation patterns [8]. To sum up, the methods developed by scholars have good results in the detection of illegal information in social media, but these methods are usually based on a single mode and belong to the deterministic classification function, which makes the model not flexible enough for the adaptability of imperfect observation data, and it is easy to cause over fitting problems in the model.

Therefore, this article extracts the textual and visual features of posts by processing multimodal information. Finally, based on Big data network intelligent algorithm, an illegal information detection model is constructed to detect illegal information in social media.

2 Multimodal Information Processing Based on Images, Text, and Audio

2.1 Feature Learning

Content based information analysis methods require extracting high-quality features from post content to detect illegal information, so the quality of the extracted features is largely related to whether the illegal information extraction task can proceed smoothly. Due to the fact that posts on social media are often multimodal, mainly including textual and visual information. Therefore, this section focuses on feature learning based on the above two forms of content representation.

2.2 Text learning Features

In text analysis and retrieval, text feature representation is a crucial task, which quantifies the feature words extracted from the text to express text information. In order to extract valuable information from massive amounts of text, it is necessary to first transform it into a processable structured form, as text is a highly complex data structure.

The BERT (Bidirectional Encoder Representations from Transformers) model is a language representation model, which is essentially the encoder part of the Transformer model [9-10]. This model is mainly used for automatic extraction of words and their combinations with specific meanings or relationships from language corpora. BERT's universal language model is to train a large number of unlabeled samples using huge data, huge models and huge computing overhead to obtain text containing rich semantic information. Due to its high accuracy and good generalization ability, this model has received widespread attention in recent years. When Natural language processing is carried out, the BERT model adopts the input mode of processing the word vector of the sentence, and based on the Statistical learning theory method, a Linear map is established for the relationship between the morphemes in the sentence and the meaning represented by each word. Compared to other words, after processing with the BERT model, the semantic information carried by paragraph vectors is more neutral in the entire sentence.

2.3 Visual Feature Learning

Deep learning is the main foundation of visual image feature learning, and deep neural networks can learn the visual features of images layer by layer. However, in many important applications, due to the data being indexed by irregular and non-Euclidean structures, explicit modeling using graphs or manifolds is required. In this situation, in order to apply deep learning technology to graph data, graph neural networks have emerged to meet practical needs [11-12].

The core idea of GNN (Graph Neural Network) is to capture and aggregate neighbor information to obtain the implicit embedding expression of the target node. Due to its good robustness, it is widely used in various practical scenarios. Among the various variant structures of GNN, Graph Convolutional Networks (GCNs) are the most widely used [13-14]. This model combines graph and pool, and uses graph convolution technology to analyze and process Big data such as images and videos, so as to obtain the semantic content hidden in them. The core operations of GCN involve convolution and pooling, while also being able to extract local features on the operating object. However, unlike this, the feature objects extracted by GCN are graph data [15-16]. The underlying operations of GCN cover neighbor aggregation and node updates, and the specific mathematical process is as follows:

$$R_n^{(0)} = s_n \tag{1}$$

$$u_n^{(i)} = f_{aggregate}^{(i)}(\{R_m^{(i-1)} | m \in M(n)\}) \tag{2}$$

$$R_n^{(i)} = f_{update}^{(i)}(R_n^{(i-1)}, u_n^{(i)}) \tag{3}$$

In the above formula, node n is the central node, and its initial feature representation is $\mathrm{s_n}, \mathrm{R_n^{(i)}}$ is the implicit representation of layer i node n, $\mathrm{u_n^{(i)}}$ is the aggregation of neighbor information of layer i n, and $\mathrm{f_{aggregate}^{(i)}}(\cdot)$ and $\mathrm{f_{update}^{(i)}}(\cdot)$ are the aggregation and update operations of layer i, respectively. The node update process is shown in Fig.ure 1:

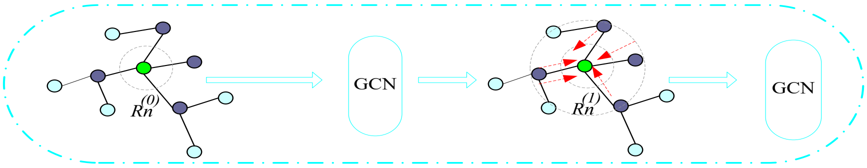

Fig. 1. Node update

3 Illegal Information Detection Based on Big Data Network Intelligent Algorithm

3.1 Building a Model Framework

Define the illegal information dataset as $\mathrm{A = \{A_1, A_2, \dots, A_k\}}$, where k represents the number of events in dataset A and $\mathrm{A_e}$ represents the e-th event in dataset A. $\mathrm{A_e = \{b_e, c_1^e, c_2^e, \dots, c_{t_e-1}^e, D_e\}}$ and $\mathrm{t_e}$ represent the number of related posts in event $\mathrm{A_e}$,

$\mathrm{c}_{\mathrm{j}}^{\mathrm{e}}$ represents the jth related post, and b_{e} represents the original post. Construct an illegal information dissemination map $\mathrm{D}_{\mathrm{e}} = \langle \mathrm{X}_{\mathrm{e}}, \mathrm{Y}_{\mathrm{e}} \rangle$ based on event A_{e}, where the node represents the social media account $\mathrm{X}_{\mathrm{e}} = \{\mathrm{X}_0^{\mathrm{e}}, \mathrm{X}_1^{\mathrm{e}}, \ldots, \mathrm{X}_{\mathrm{t_e}-1}^{\mathrm{e}}\}$; Edge represents the direction and direction of information dissemination, $\mathrm{Y}_{\mathrm{e}} = \{\mathrm{y}_{\mathrm{kt}}^{\mathrm{e}} | \mathrm{o}, \mathrm{p} = 0, \ldots \mathrm{t}_{\mathrm{e}} - 1\}$. For example, if the post $\mathrm{c}_1^{\mathrm{e}}$ forwards or comments on the post $\mathrm{c}_2^{\mathrm{e}}$, a directed edge, Y_{21}, is constructed from the post $\mathrm{X}_2^{\mathrm{e}}$ to the post $\mathrm{X}_1^{\mathrm{e}}$, representing the information dissemination from $\mathrm{X}_2^{\mathrm{e}}$ to $\mathrm{X}_1^{\mathrm{e}}$. So given a dataset A of illegal information with label θ_{e}, it can obtain the target classifier for illegal information detection:

$$f: A_e \to \theta_e / f: C \to \theta \tag{4}$$

The framework diagram for detecting illegal information is shown in Fig.ure 2:

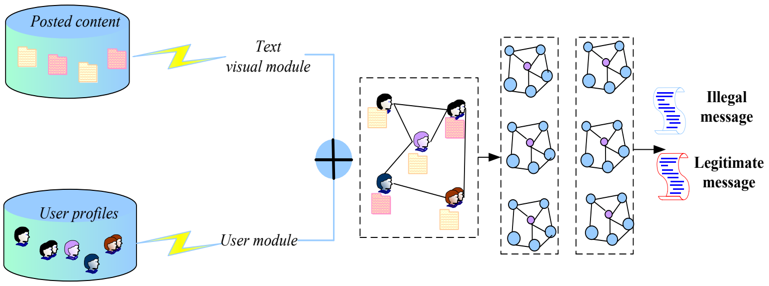

Fig. 2. Illegal information detection framework

3.2 Node Feature Embedding

Although the information disseminated on social networks has many characteristics, not every one of them can help us effectively detect illegal information, and different characteristics have different effects on the problem of illegal information detection [17-18]. Feature fusion is a commonly used method in feature enhancement, which complements each other by fusing two or more different features. Better feature fusion can provide supplementary information, reduce the Curse of dimensionality, and improve the accuracy of the whole decision-making process [19-20].

For the obtained text features and visual feature vectors, they should be concatenated with the user feature vectors. The concatenation process should correspond to the user and their published posts, ensuring that the social media account and personal information to which the user belongs can be integrated. The $\oplus$ concatenation method is used here. By overlaying two sets of vectors, the expression method of illegal information can be well learned, and ultimately fed into the model for training, thereby achieving higher detection accuracy.

4 Experimental Setup

4.1 Datasets

The dataset adopts public and real datasets used by mainstream methods: WEIBO and Twitter 16. The WEIBO dataset contains a large amount of text and photos, among which there are a total of 4721 events in the WEIBO dataset, 2512 are false events (Fake News: FN), and 2209 are real events (Real News: RN); The Twitter16 dataset contains 4 different tags, with a total of 812 events. Among the four tags, there are 231 "FR: False Rumors", 201 "NR: Non Rumors", 193 "UR: Unverified Rumors", and 187 "TR: True Rumors".

4.2 Parameter Settings

In order to verify the performance, the intelligent detection model proposed in this paper is compared with two advanced baseline models: SVM TS, which is a SVM Linear classifier based on heuristic rules to identify illegal information; And EANN, which uses adversarial networks to eliminate event specific feature representations from post features based on multimodal representations of extracted text and visual features, and learns the event invariant multimodal features of each post for illegal information detection. The experimental parameter settings are shown in Table 1:

Table 1. Experimental Parameter Settings

Type	Parameter	Value
BERT	Head	12
	Attention layer	12
	Hidden layer element	721
GCN	GCN hidden layer dimension	(50,　50)
	Batch size	50
	Dropout	0.5
	Learning rate	0.0005
	Weight attenuation coefficient	5e-2

4.3 Experimental Results

This article selects accuracy (ACC: Accuracy), precision (Pre.: Precision), recall (Rec.: Recall), and F1 value as the evaluation criteria for the intelligent detection model and baseline model proposed in this article. Experiment on a given dataset, whether WEIBO or Twitter 16, for all experimental models, it can iterate 50 epochs, Learning rate is 0.0005, and batch size is set to 50 for training.

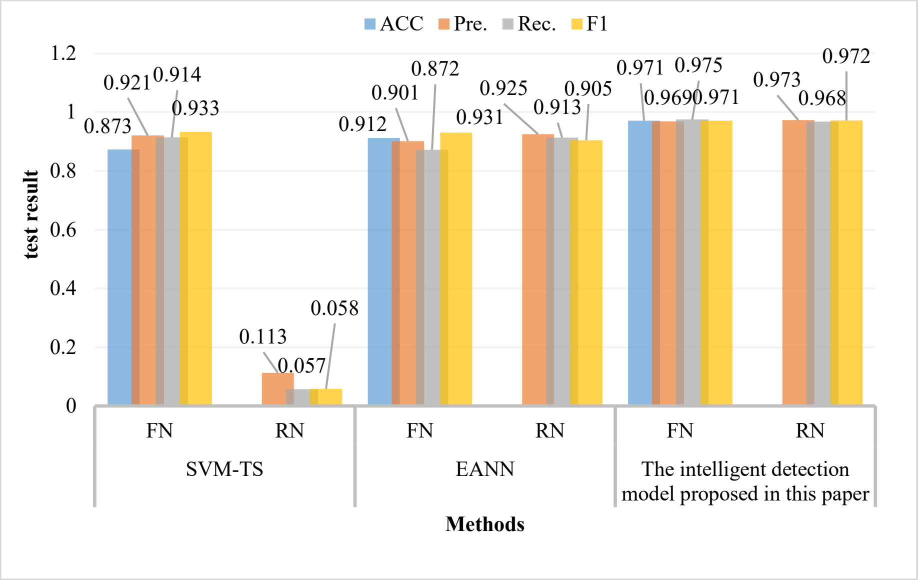

Fig. 3. Rumor detection results on the WEIBO data set

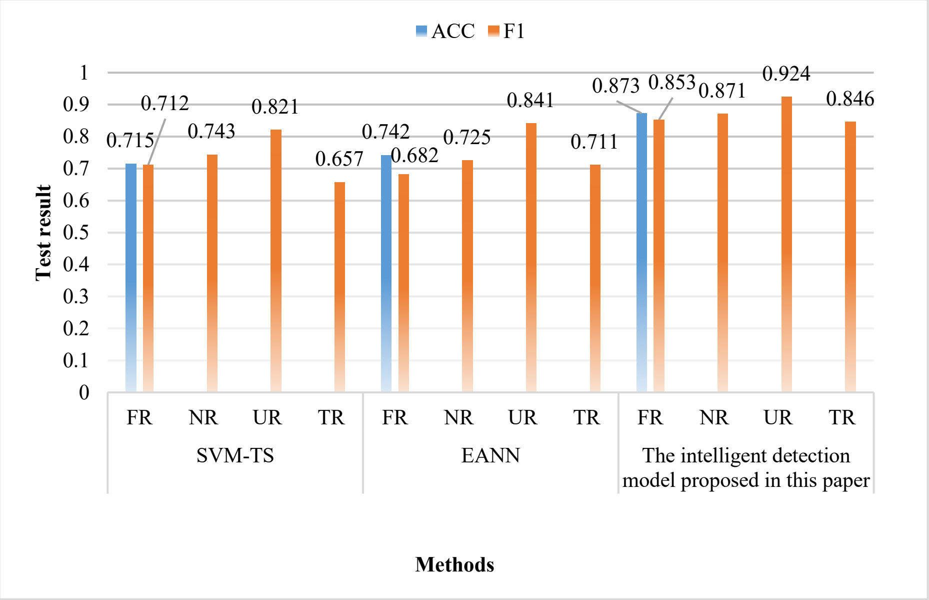

Fig. 4. False information detection results on the Twitter16 data set

Fig.ures 3 and 4 show the performance comparison of the intelligent detection model and two benchmark methods proposed in this paper in the WEIBO and Twitter16 datasets. By comparing the two baseline methods, it found that the EANN method outperforms the SVM-TS method in terms of performance.

The reason for this phenomenon is that the SVM-TS method only uses manually extracted text content, ignoring the structural features of false information during the propagation process, resulting in poor detection performance. EANN can learn advanced representation of false information through multimodal representation of posts.

Compared with traditional SVM-TS and EANN, the intelligent detection model for illegal information proposed in this paper has higher recognition accuracy. The research results show that the intelligent detection model proposed in this article has the ability to process graph/tree structures and learn higher-level representations, so it can effectively mine hidden information in information and play an important role in detecting false and illegal information. This proves that the intelligent detection model proposed in this article is efficient, advanced, and robust in detecting multimodal rumors on social media, and has higher prediction accuracy.

5 Conclusions

In the The Internet Age represented by new media, social network media is becoming more and more important in people's lives. At the same time, various security issues are also emerging, so improving the accuracy of new media technology in information detection is of great significance. This paper refers to the world literature, on the basis of in-depth research on the existing machine learning and deep learning technologies to detect false information, and in view of the fact that most of the existing false information detection methods are often based on single-mode classification functions, and the data is incomplete, which is prone to over fitting problems, this paper proposes an illegal information detection model based on Big data network intelligent algorithm. Finally, experiments show that the method proposed in this paper has good effectiveness, progressiveness and robustness in detecting multimodal online rumors on social media.

Acknowledgements

This work was supported by. Project Name: A study on the variations of Vocabulary, Semantics, and Grammar in Modern Chinese in the new Era (No.: 18xjr03R)

References

[1] Yu W , Huang X , Yuan Q ,et al.Information Security Field Event Detection Technology Based on SAtt-LSTM[J].Security and Communication Networks, 2021, 2021(3):1-8.

[2] Yuvaraj N , Srihari K , Dhiman G ,et al.Nature-Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking[J].Mathematical Problems in Engineering, 2021, 2021(Pt.8):1-12.

[3] Kadam N , Sharma S K .Social Media Fake Profile Detection Using Data Mining Technique[J].Journal of Advances in Information Technology, 2022,13(5):518-523.

[4] Candra A ,WELLA, Wicaksana A .Bidirectional Encoder Representations from

Transformers for Cyberbullying Text Detection in Indonesian Social Media[J].International journal of innovative computing, information and control, 2021,17(5):1599-1651.

[5] Kumar A R , Mohan P , Vignesh R .Chat Bot User Detection using Likes and Comments On Social Media[J].International Journal of Advanced Science and Technology, 2020, 29(7):8100-8107.

[6] Pratiwi A R D , Setiawan E .Implementation of Rumor Detection on Twitter Using the SVM Classification Method[J].2020,4(5):782-786.

[7] Kumar G , Rishiwal V .Malicious User Nodes Detection by Web Mining Based Artificial Intelligence Technique[J].International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 2020, 28(1):1-24.

[8] Vu D T , Jung J J .Rumor Detection by Propagation Embedding Based on Graph Convolutional Network[J].International Journal of Computational Intelligence Systems, 2021,14(1):1053-1065.

[9] Alami F , Alaoui S O E , Ennahnahi N .Contextual Semantic Embeddings based on Fine-tuned AraBERT Model forArabic Text Multi-class Categorization[J].Journal of King Saud University - Computer and Information Sciences, 2021,34(2):1-7.

[10] Lamsiyah S , Mahdaouy A E , Ouatik S E A ,et al.Unsupervised extractive multi-document summarization method based on transfer learning from BERT multi-task fine-tuning:[J].Journal of Information Science, 2023, 49(1):164-182.

[11] Li Y , Chen R , Zhang Y ,et al.Multi-Label Remote Sensing Image Scene Classification by Combining a Convolutional Neural Network and a Graph Neural Network[J].Remote Sensing, 2020, 12(23):1-17.

[12] B Y L A , B Y C A , B D Z A ,et al.MGRL: Graph neural network based inference in a Markov network with reinforcement learning for visual navigation - ScienceDirect[J].Neurocomputing, 2020, 421(Jan.15):140-150.

[13] Duan Y , Wang J , Ma H ,et al.Residual Convolutional Graph Neural Network with Subgraph Attention Pooling[J].Tsinghua Science and Technology, 2022, 27(4):653-663.

[14] Chen J , Lin G , Chen J ,et al.Towards efficient allocation of graph convolutional networks on hybrid computation-in-memory architecture[J].Science in China: Information Science (English), 2021, 64(6):108-121.

[15] Mansouri-Benssassi E , Ye J .Synch-Graph: Multisensory Emotion Recognition Through Neural Synchrony via Graph Convolutional Networks[J].Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(2):1351-1358.

[16] Taguchi H , Liu X , Murata T .Graph convolutional networks for graphs containing missing features[J].Future Generation Computer Systems, 2021, 117(5):155-168.

[17] Li D , Madden A .Cascade embedding model for knowledge graph inference and retrieval[J].Information Processing & Management, 2019, 55(6):102093.1-102093.15.

[18] Krlj B , Kralj J , Konc J ,et al.Deep node ranking for neuro-symbolic structural node embedding and classification[J].International Journal of Intelligent Systems, 2022, 37(1):914-943.

[19] Zhang J , Xu Q .Attention-Aware Heterogeneous Graph Neural Network[J].Big Data Mining and Analytics, 2021, 4(4):233-241.

[20] Mallick K , Bandyopadhyay S , Chakraborty S ,et al.Topo2Vec: A Novel Node Embedding Generation Based on Network Topology for Link Prediction[J].IEEE Transactions on Computational Social Systems, 2019, 6(6):1306-1317.