

## Article

# Fake User Detection Based on Multi-Model Joint Representation

Jun Li <sup>1,\*</sup>, Wentao Jiang <sup>1</sup>, Jianyi Zhang <sup>2</sup>, Yanhua Shao <sup>3</sup> and Wei Zhu <sup>1</sup>

<sup>1</sup> School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China; 2023020963@bistu.edu.cn (W.J.); 2023020996@bistu.edu.cn (W.Z.)

<sup>2</sup> School of Computing and Informatics, University of Louisiana at Lafayette, Lafayette, LA 70504, USA; jianyi.zhang@louisiana.edu

<sup>3</sup> National Computer System Engineering Research Institute of China, Beijing 100083, China; shaoyanhua@ncse.com.cn

\* Correspondence: lijun@bistu.edu.cn

**Abstract:** The existing deep learning-based detection of fake information focuses on the transient detection of news itself. Compared to user category profile mining and detection, transient detection is prone to higher misjudgment rates due to the limitations of insufficient temporal information, posing new challenges to social public opinion monitoring tasks such as fake user detection. This paper proposes a multimodal aggregation portrait model (MAPM) based on multi-model joint representation for social media platforms. It constructs a deep learning-based multimodal fake user detection framework by analyzing user behavior datasets within a time retrospective window. It integrates a pre-trained Domain Large Model to represent user behavior data across multiple modalities, thereby constructing a high-generalization implicit behavior feature spectrum for users. In response to the tendency of existing fake user behavior mining to neglect time-series features, this study introduces an improved network called Sequence Interval Detection Net (SIDN) based on Sequence to Sequence (seq2seq) to characterize time interval sequence behaviors, achieving strong expressive capabilities for detecting fake behaviors within the time window. Ultimately, the amalgamation of latent behavioral features and explicit characteristics serves as the input for spectral clustering in detecting fraudulent users. The experimental results on Weibo real dataset demonstrate that the proposed model outperforms the detection utilizing explicit user features, with an improvement of 27.0% in detection accuracy.



**Citation:** Li, J.; Jiang, W.; Zhang, J.; Shao, Y.; Zhu, W. Fake User Detection Based on Multi-Model Joint Representation. *Information* **2024**, *15*, 266. <https://doi.org/10.3390/info15050266>

Academic Editor: Arkaitz Zubiaga

Received: 28 March 2024

Revised: 24 April 2024

Accepted: 24 April 2024

Published: 9 May 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** fake user detection; deep learning; domain large model; user behavioral clustering; cyberspace security

## 1. Introduction

Social media plays a crucial role in today's society, serving as a primary platform for information dissemination, social interaction, and opinion propagation. Weibo is one of the most popular social media platforms in China. It allows users to publish short text messages, as well as various media formats including images, videos, and audio. Users on Weibo can follow others and be followed by others. Content on Weibo can be interacted with through retweets, comments, and likes. Massive amounts of data are generated on a daily basis, among which the proliferation and dissemination of fake news are prevalent, posing one of the serious challenges faced by social media platforms. Past research has mainly focused on analyzing fake news itself. Typically, these studies emphasize single modality, specifically text and visual information recognition. Additionally, some studies employ multimodal methods to identify fake news, with existing fake news detection approaches largely integrating both image and text modalities. Studies on single-modal fake news detection mainly include text-based fake news detection [1–4] and visual-based fake news detection. Integrating multiple modalities is one of the key challenges in multi-modal fake news detection. Methods that map different modal information to the same

feature space and fuse them into classifiers for identifying fake news [5–8]. Many scholars believe that if news images do not match the textual content, the news is considered fake. Based on such assumptions, methods for identifying fake news through modal contrasts are employed, utilizing thresholds set for image-text similarity to achieve fake news recognition. Similarly effective methods include enhancing multimodal information through co-attention mechanisms [9] and assisting fake news detection by extracting user features for credibility [10].

For detecting fake users on social media platforms, various methods have been proposed, most of which analyze features in users' profiles [11–13] or utilize machine learning methods combining text features with user profiles. However, with the emergence of high-quality generative models such as ChatGPT, BigGAN, etc., there is a growing trend of more realistic and human-likeness of fake users on social media platforms. These advanced generative models endow fake users with more sophisticated and realistic machine-generated capabilities, making them increasingly difficult to distinguish on social media platforms, thereby further increasing the threat of widespread dissemination of fake information.

In this paper, we adopt a multi-modal joint representation strategy and propose the Multi-Modal Aggregation Portrait Model (MAPM) based on this strategy for detecting fake users. Specifically, the MAPM model consists of three parts: (1) Using the Chinese version of Pegasus [14] to extract text summaries as input for the Chinese CLIP pre-training module [15,16], which analyzes text and image similarity using multi-modal information. Utilizing the BERT pre-training module [17] to classify blogs posted by users. Introducing the HiFi-NET network module [18] to determine whether blog images have undergone AI synthesis or tampering. (2) Designing a Sequence Interval Detection Net (SIDN) module based on Sequence to Sequence [19] architecture to model the time interval sequences of user blog posts, representing implicit time behavior features. (3) Adjusting the output size of the feature extraction module to a user-level scalar and mapping it to the same feature space. Combining implicit behavioral features with explicit user features, constructing a spectral clustering-based unsupervised classification module [20] to achieve multi-modal detection of fake users.

The main contributions of this paper are as follows:

1. MAPM utilizes large models like CLIP, BERT, and HiFi-NET transfer learning modules to aggregate explicit and implicit features across multiple dimensions such as text, images, and user data, thereby achieving a concrete fusion of user behavior characteristics.
2. We propose a Time Interval Detection Network aimed at representing potential temporal characteristics of user posting behavior, enhancing the model's capability to detect unusual user behavior.
3. By combining implicit behavioral features with explicit user features, we construct a spectral clustering-based unsupervised classification module to further classify fake users, providing a potential approach for public opinion analysis in social media management.

The structure of the remaining part of the paper is as follows: Section 2 will discuss current popular methods for identifying fake news and fake users. Section 3 will delve into the theoretical foundations of building the model and detail the representation of user behavior. Section 4 will introduce the experimental classification results of the model and discuss the data preparation work. Finally, Section 5 will provide the conclusion of this paper.

## 2. Literature Review

### 2.1. Fake News Detection

The narrow definition of fake news refers to intentionally falsified information that can be verified as false and may mislead readers [21]. This definition has two key features: truthfulness and intent. Firstly, fake news includes falsified information that can be verified. Secondly, fake news is characterized by the intent to mislead readers, a definition widely adopted in recent research [22]. Broadly speaking, fake news is defined as news that is

deceptive in terms of either the truthfulness of its content or the intent of its publisher, even if it is satirical news. Satirical news, despite being entertainment-oriented, still contains false content [23]. Additionally, broad fake news may also cover other forms of deceptive news, such as serious fabrications, hoaxes, and other news that can have a misleading effect [24]. Formally, we define fake news as news that contains untrue information. There are several reasons for choosing a broad definition. Firstly, this study identifies users who have posted articles on military-related topics. Compared to regular news, the dissemination of fake military news can have more serious and complex consequences. Regardless of the intent of the disseminator, misleading reports may shape unjust perceptions of the country, leaders, or policies. Secondly, the broad definition of fake news helps enhance the model's generality because content posted on social media platforms often has a certain entertainment value. Such a definition enables the model to better adapt to the diversity of social media platforms.

Currently, significant progress has been made in the research on detecting fake news based on text and visual information, with effective methods proposed to address this issue. In the field of text-based fake news detection, Ma et al. [25] first applied deep learning techniques to fake news detection. Their method inputs sentences into a Gate Recurrent Unit (GRU) to represent news information using the hidden layer vectors of recurrent neural networks. In subsequent work, they introduced the idea of multi-task learning into fake news detection [26]. Nan et al. proposed the MDFEND model, which applies the pre-trained BERT model to text encoding, aggregates the outputs of expert layers through domain gates into a classifier, and finally uses softmax for binary fake news classification. Liu et al. [27] proposed a fake news filtering algorithm based on generative adversarial networks. Qi et al. [28] proposed the fake image discriminator MVNN, which uses frequency domain features to determine whether images have been manipulated using image editing software and uses spatial domain features to recognize the semantic information of images. The above research indicates that single-modal information detection is effective in fake news detection tasks, but single-modal methods may overlook crucial information contained in other modalities, resulting in an incomplete understanding of the overall situation.

The key issue in multi-modal fake news detection is coordinating text and visual features. Singhal et al. employed the Visual Geometry Group (VGG) model and XLNET to effectively classify fake news using a cross-modal approach. Zhou et al. [29] used image2text to map textual and visual information into the same vector space, then compared the similarity between visual and textual information. Meng et al. [30] noticed the neglect of interactions between single and multi-modalities in existing research and proposed establishing intra-modality and inter-modality attention mechanisms to capture high-level interactions between text and visual domains. Qi et al. [31] comprehensively considered the complementary information of multi-modality and fused textual and visual information using co-attention. Raza et al. [32] leveraged a Transformer model combining news content with heterogeneous auxiliary information, aiming to conduct early detection of fake news. Ying et al. [33] proposed the BMR model, which treats consistency between text and image as an auxiliary discriminant factor for fake news, combines multi-task models to adaptively weight features from multiple modalities, and ultimately determines whether it is fake news. These research achievements provide valuable examples for improving classification performance in the field of fake news detection. There have been significant advances in detecting fake news. Social media platforms emphasize user participation and creation [34], but previous work has not fully addressed user characteristics in social media platforms [35].

In recent years, research on deep learning-based fake news detection has mostly come from social media platforms. Weibo is China's largest social media platform, where users are not only receivers of information but also important sources of information. In this context, some research works assess the credibility of users by utilizing their personal profiles and posting histories. Lu et al. [36] extracted user features from user profiles and social interactions on Twitter, learned user propagation representations based on user

features using CNN and RNN, and proposed a dual co-attention mechanism to learn the correlation between source tweets and retweet propagation and the mutual influence between source tweets and user interactions. Dou et al. [37] identified user credibility using user posting history as an intrinsic factor. At the same time, this work regarded the propagation of news as an extrinsic factor and used intrinsic and extrinsic factors together for fake news detection.

Current fake news research focuses on detecting visual and textual information, neglecting the widespread participation and influence of users in social media networks, or treating user behavior only as an auxiliary task for fake news detection rather than the core of the detection task. We believe that combining users' historical behaviors with user characteristics is a key clue to revealing fake news.

## 2.2. Fake User Detection

The key to identifying fake users lies in mining and analyzing features. Extracting user profile information as features combined with low-dimensional user behavior features is a common method in fake user detection [38–40]. Common low-dimensional behavioral features include the number of stopwords, emojis, posting frequency, etc. Building classification models based on comprehensive social network features and user interaction behaviors enables more comprehensive consideration for fake user detection [41,42]. Implicit features of users refer to their underlying behavioral patterns. These features are not directly visible like explicit features and require algorithms and analysis to reveal deeper characteristics of users, such as “posting patterns” and “correspondence between text and images”. Yang et al. [43] noticed that traditional user detection focuses on identifying individual anomalous users and proposed an anomaly detection framework based on bipartite graphs and co-clustering to identify abnormal users. However, due to the singular form of abnormal user samples, it is difficult to address anomaly detection in different social environments. Heidari et al. [44] explored the impact of sentiment features mined from text sentiment classification networks on the accuracy of detecting fake users on social media but failed to fully characterize user behavior. Furthermore, Mohammad et al. [45] utilized the first tweet of each user as input to a convolutional neural network for identifying bot users. However, a single tweet lacks temporal information. Therefore, there is a need to design a detection method that can fully represent user behavior and has generalizability.

On another front, automated users on social media platforms refer to social entities implemented by programs to mimic human social interaction norms [46–48]. Malicious bot accounts manipulate user influence by engaging in behaviors such as commenting, follower boosting, and reposting, thereby manipulating public opinion, disseminating harmful information, and posing serious threats to the online environment [49–51]. The core focus of this study lies in analyzing user behaviors on social media platforms. Therefore, the research focus is on identifying automated users and conducting fine-grained classification of fake users based on different automation behaviors.

Firstly, the first category of fake users mimics the daily posting behavior of genuine users, and actively participate in platform giveaways to seek rewards while evading detection of their deceptive nature by automated systems or manual checks. Secondly, the behavior of the other category of fake users primarily involves automatically reposting multimedia messages sourced from multiple platforms, such as images, videos, or other content. The operations of these machine users typically aim to widely disseminate specific types of information, potentially involving promotion, propaganda, or other purposes. Their automated nature enables them to efficiently execute large-scale message reposting behaviors. In this study, these two categories of users are respectively referred to as lottery users and repost users, and they are collectively referred to as fake users. In past research, there has been limited algorithmic analysis of user behavior features [52–54], and it is difficult to identify fake user behaviors combined with generative models using traditional machine learning algorithms. Therefore, the proposed method jointly analyzes

text information, visual information, multimodal information, and temporal information using multiple models to fully characterize user behaviors.

### 3. Methodology

This paper proposes the MAPM for multimodal joint representation and detection of fake users, the architecture of MAPM is shown in Figure 1. The core work of this study focuses on characterizing user behavior. Firstly, all textual and image content from individual users’ blogs is analyzed. Specifically, we fine-tuned the BERT model for domain classification of text, identifying the proportion of blog content in different domains. Subsequently, the HiFi-NET module is introduced to detect whether images are AI-generated or tampered, calculating the mean probability of image forgery for all images. Due to the text length limitation of the CLIP module, we first input the blog text into the Pegasus module to extract Chinese text summaries, which are then used alongside blog images as inputs to the CLIP module to extract consistency scores between text and images. Next, user posting richness features are extracted using the entropy formula. Secondly, the SIDN module is introduced to analyze time interval sequences, representing user posting behavior features. Finally, the text domain vectors extracted by the BERT module are flattened into scalars, combined with consistency scores between text and images, mean forgery probabilities, posting richness, and time behavior feature scores, to form user behavior features. These features are combined with existing explicit user features to create individual user feature sets. Subsequently, spectral clustering algorithm is utilized to cluster different users with similar feature performances, enabling the detection of fake users.

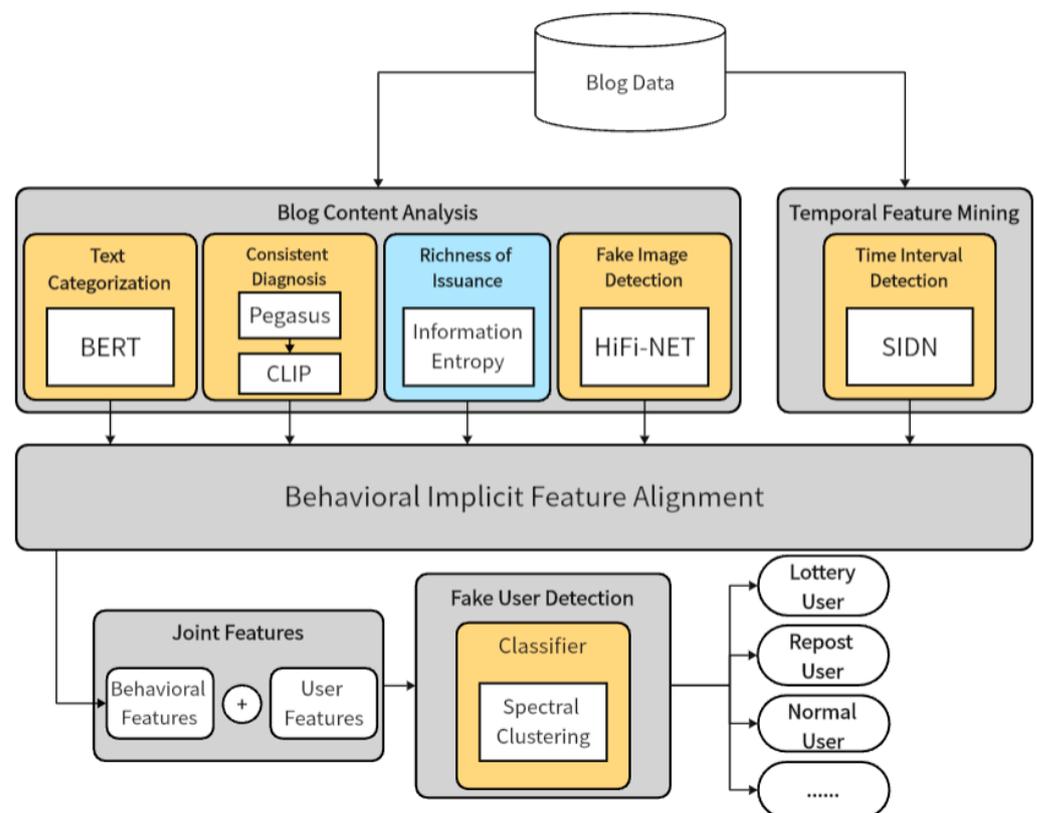


Figure 1. Network architecture of MAPM.

#### 3.1. The Window User Feature Space

Let the user  $\theta = [U, B_n] \in D$  where  $U$  denotes the user characteristics,  $B_n$  denotes the collection of blog content published by the user,  $n$  denotes the number of blogs contained in  $B$ , and  $D$  denotes the dataset.

First, break down the components of  $U$ , including membership level, number of blogs, number of follows, number of fans, number of likes, number of retweets, and number of comments.

$$U = \{U_v, U_n, U_a, U_f, U_l, U_r, U_c\} \tag{1}$$

$U_l, U_r, U_c$  denote the number of likes, retweets, and comments summed up for each blog by the user.

The  $B$  composition rule in  $\theta$  is:

$$B_n = \{(P_{t_1}\&T_1\&I_1), (P_{t_2}\&T_2\&I_2), \dots, (P_{t_n}\&T_n\&I_n)\} \tag{2}$$

In which,  $\&$  represents the concatenation symbol in the string, the triple  $S_n = (P_{t_n}\&T_n\&I_n)$  represents the  $n$ th blog of the user in the dataset, where  $P_{t_n}, T_n, I_n$  respectively represent the posting time, text content, and image of the  $n$ th blog of the user. Here, images are linked to  $T_n$  in the form of text.

In the user behavior analysis stage,  $S_n$  is extracted for preprocessing, and a method using regular expressions is employed to remove text tags and emoticons from  $T_n$  on the Weibo platform.

On the Weibo platform, blogs from bot users exhibit a high degree of similarity in style. Some bot users' blogs are all accompanied by images, while others are all in text form. Therefore, we introduce information entropy to measure the diversity of user blogs. The presence of images in blogs from the majority of normal users cannot be predicted, hence showing higher information entropy. The formula for calculating the richness of users' blogs is as follows, where  $p(x)$  denotes the proportion of blogs with pictures:

$$H(x) = -\sum_{i=1}^n p(x) \log p(x) \tag{3}$$

In the text classification task, we used the "bert-base-chinese" model.  $\prod$  stands for the indicator function. During pre-training, the model parameters were frozen, and a linear layer was used for the output, with the output length being the same as the number of categories in the text domain.  $T_n$  was extracted, and based on punctuation marks, it was truncated as input to the model. Finally, the involvement of various domains in the textual part of user blogs was analyzed in percentage terms.

The output of the pre-trained BERT model is:

$$i_{\max} = \sum_i^N \prod_i ((Wx + b)_i = \max(Wx + b)) \cdot i \tag{4}$$

In the formula, the output layer of the pre-trained model is fully connected. After linear operation represented by  $Wx + b$ , the predicted category  $i_{\max}$  represents that the text information is classified into the  $i$  category.  $W$  is the weight parameter, and  $x$  represents the hidden state of the last layer of the model except for the output layer. The indicator function  $\prod$  is used to calculate the maximum index in the output list and map it to the category. The feature output is:

$$P_j = \frac{1}{n} \sum_{i=1}^n \prod_i (Map(i_{\max}) = class_j) \tag{5}$$

In the equation, we define a mapping function  $Map$  to map this index to the predefined categories of the text. Next, we use an indicator function to count the category for each sentence. Then, we sum up this indicator function and divide by the total number of sentences  $n$  to obtain the percentage distribution  $P$ .

In visual tasks, we use HiFi-NET to detect whether the image is generated by CNN or by stitching and synthesizing, and output the probability. Given the image  $X$ , the logarithm

of the output of branch  $\theta b$  and the predicted probability are represented as  $\theta b(X)$  and  $p(yb|X)$ , respectively. The formula for predicted probability is:

$$p(yb|X) = \text{softmax}(\theta b(X) \odot (1 + p(yb - 1|X))) \tag{6}$$

In the multimodal task, we freeze the parameters of Pegasus and `cn_clip`. Due to the text input length limitation of the CLIP pre-trained model, we utilize the Chinese version of the Pegasus [55] model to extract text summaries of the blogs. This approach not only effectively overcomes the text length limitation of the CLIP model, but also helps standardize the textual information of the blogs. We use Pegasus to extract text summaries, and these summaries, along with images, are jointly used as inputs to the `cn_clip` model. The output of the model is as follows:

$$s_i = \text{scale} \times f_{img} @ f_{text} \tag{7}$$

In the equation,  $s_i$  represents the calculation of the cosine similarity between vectors, where  $f_{text}$  and  $f_{img}$  are the text embedding vector and image embedding vector, respectively. Here, `@` denotes matrix multiplication.

### 3.2. Sequence Interval Detect Net

Liu et al. extracted the time interval sequence of blogs to obtain the modified conditional entropy for each user. The study found that the modified conditional information entropy of bot users is significantly lower than that of regular users, indicating a strong regularity in the tweeting behavior of bot users. It is speculated that the timing of bot users' blogs is controlled by automated script algorithms, which may manifest certain patterns in the intervals between blogs. In Ying Q. et al.'s study on the posting behavior of users on online social networks (OSNs), it was observed at a macro level that social media platforms exhibit two distinct peaks in traffic. The first peak occurs during morning working hours, while the second peak occurs in the evening. For users who frequently post, the evening peak is more pronounced [56]. Considering the clustering of user posting times, it is challenging for a multilayer perceptron to capture such complex behavioral patterns, and the availability of datasets for modeling time interval sequences is limited. Therefore, the study adopted the seq2seq network architecture from recurrent neural networks. This network structure can better consider information from multiple time steps and is suitable for capturing the temporal patterns of users' posting behavior on social media platforms.

Specifically, for each user, we extract  $Pt$ , calculate the time interval  $it_i$  by subtracting the previous  $Pt_{i-1}$  from the current  $Pt_i$ , and combine all its values to form a time interval sequence  $IT = (it_1, it_2, \dots, it_n)$ . Then, we delete the first element to obtain a new sequence  $\overline{IT} = (it_2, it_3, \dots, it_n)$ , which serves as the expected output data for the Decoder.

We have improved the architecture of the seq2seq network, as shown in Figure 2 to model the time interval sequence.

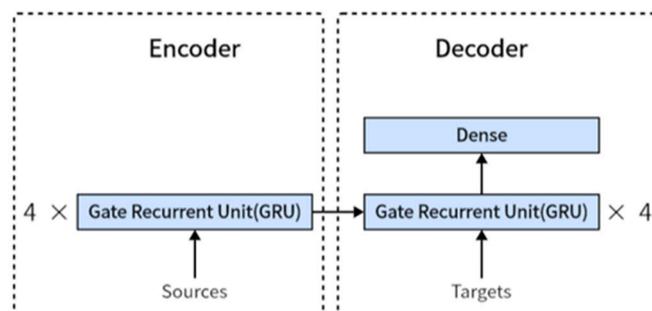


Figure 2. Network architecture of SIDN.

SIDN is divided into Encoder and Decoder, with their embedding layers removed. In the encoder part, we use 4 layers of GRU. Similarly, the decoder also utilizes 4 layers of

GRU, and the update process for the hidden state at each time step in a single-layer GRU is as follows:

$$h_t = (1 - z_t) \odot h_{t-1} - 1 + z_t \odot \tanh(W_h \cdot [r_t \odot h_{t-1}, x_t]) \tag{8}$$

In the equation,  $h_t$  represents the current hidden state,  $(1 - z_t) \odot h_{t-1}$  denotes the old hidden state being partially forgotten, and  $z_t \odot \tanh(W_h \cdot [r_t \odot h_{t-1}, x_t])$  represents the new candidate's hidden state being partially added.  $z_t$  is the output of the update gate in GRU,  $r_t$  is the output of the reset gate, and they compute by concatenating the current input  $x_t$  with the previous hidden state  $h_{t-1}$ , and  $W$  is their weight matrix.

In each time step of the Decoder's computation, the expectation is to obtain the output of the next time interval, which is ultimately output through a linear layer. The training process is illustrated in Figure 3. Since the training data is continuous, the mean squared error loss function is utilized, defined as:

$$L(\bar{it}, \tilde{it}) = \frac{1}{n} \sum_{i=1}^n (\bar{it} - \tilde{it})^2 \tag{9}$$

where  $\tilde{it}$  represents the elements of the model's predicted output. To detect anomalies in the time series, the data is inputted into the model, and  $L(\bar{it}, \tilde{it})$  is extracted as the reconstruction error, which is used to quantify the anomalies exhibited by user posting behavior over time.

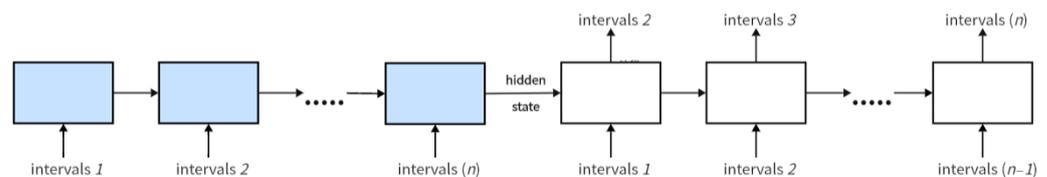


Figure 3. The reasoning process of SIDN.

### 3.3. Classifier Module of MAPM

The behavior features extracted by the deep learning model are concatenated with explicit features to obtain the window user feature space  $X$ :

$$X_i = \{U_i, H_i, C_i, P_i, S_i, Lt_i\} \tag{10}$$

Consider a user  $\theta$ , whose explicit features are represented by  $U$ , the richness of user-generated content is denoted by  $H$ ,  $C = \{c_0, c_2, \dots, c_{10}\}$  represents the text classification results, consisting of eleven categories indicating the composition of text domains. Additionally,  $P$  represents the probability of image forgery,  $S$  represents the similarity between text and images, and  $Lt$  represents the reconstruction error of the time series.

Spectral clustering algorithm, as a kind of unsupervised learning method based on a data graph, can fully utilize the input feature information in mining the inherent structure of data, and capture the potential cluster structure in high-dimensional space. Spectral clustering is unaffected by sample distribution, as its optimization objective solely focuses on measuring similarity between samples. In contrast, imbalanced datasets often exhibit a more concentrated distribution pattern. The similarity calculation formula for two user samples  $x_i$  and  $x_j$  is as follows:

$$\text{similarity}(x_i, x_j) = \exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right) \tag{11}$$

The equation  $\|x_i - x_j\|$  represents the Euclidean distance between samples  $x_i$  and  $x_j$ , the calculation formula is referred to as:

$$\|x_i - x_j\| = \sqrt{\sum_{k=1}^d (x_{ik} - x_{jk})^2} \tag{12}$$

where  $d$  denotes the feature dimension of the samples,  $x_{ik}$  and  $x_{jk}$  represent the values of sample  $x_i$  and  $x_j$  on the  $k$ -th feature, respectively, and  $\sigma$  is the parameter of the Gaussian kernel function, which controls the decay rate of similarity. Subsequently, by utilizing the similarity, a Laplacian matrix is constructed, followed by eigenvalue decomposition, and clustering of the data is performed based on the eigenvectors.

## 4. Experiments

This section will introduce the datasets used in the work, analyze the performance of different modules, and employ ablation experiments to validate their effectiveness.

### 4.1. Data Sets

#### 4.1.1. BERT Text Categorization Dataset

When fine-tuning BERT for text classification, the dataset used was the THUC-News [57] from Tsinghua University, consisting of 740,000 news documents. Based on the original Sina Weibo news classification system, it was reorganized into 10 candidate categories: politics, finance, real estate, stocks, education, science, society, sports, games, and entertainment. Building upon this, we developed a topic-specific web crawler dedicated to fetching blog content. To expand the “military” category, additional text data was collected, including over 6700 training samples, more than 1200 testing samples, and over 1600 validation samples.

#### 4.1.2. Weibo User Dataset

We developed a web crawling tool in-house specifically for collecting data from Weibo user profiles. With this automated tool, we obtained a large amount of relevant information about Weibo users, including their posted content, social context information, and social media metrics. After applying data cleaning methods such as deduplication and removing low-quality data, we constructed a Weibo user dataset consisting of 2076 user records and 198,705 blogs. Figure 4 is a feature heatmap of different user categories in the dataset, used to reveal patterns of feature values across different user categories. Darker colors indicate higher values. After averaging the features for the three user categories, the averaged data is merged and normalized. For aesthetics in the legend, the textual composition features extracted by BERT, which encompass proportions from 11 different domains, are omitted from the heatmap. In the figure, red font denotes implicit user features, while “Avg” represents the mean values. Additionally, “Consistency”, “Forgery”, and “Time Feature” respectively denote the text-image consistency, AI image probability, and temporal reconstruction error extracted by the cn\_clip, HIFI-NET, and SIDN feature extraction modules.

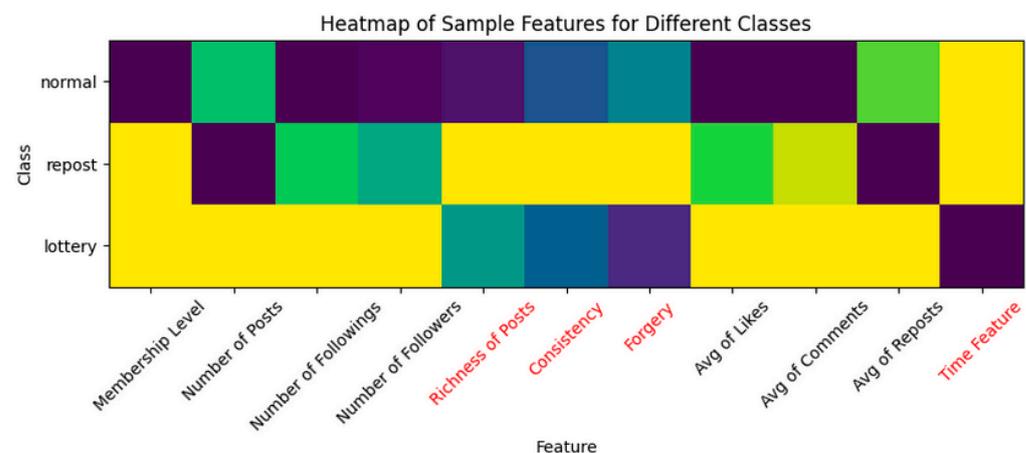


Figure 4. Heatmap of sample features for different classes.

Through the heat map, it is evident that the repost users exhibit relatively low posting frequency, text-image consistency, and image forgery probability, which aligns with our previous findings. This category of users tends to share blogs with rich multimedia content, albeit often with a mismatch between text and image descriptions. Lottery users demonstrate higher values in time-related features, thus the features extracted by the SIDN network offer robust support in identifying them. These users exhibit relatively lower metrics on social media platforms, consistent with their behavioral objective of not publishing valuable content, but rather participating solely in reposting and lottery activities. The color diversity in the blocks of normal users indicates that their behavior lies between the low activity of lottery users and the high activity of repost users to some extent.

#### 4.2. Analyzing Module Performance

After fine-tuning on the expanded THUCNews, we obtained experimental results for the BERT model. The results clearly demonstrate that the pre-trained BERT model exhibits high accuracy in Chinese text classification across eleven domains. To validate the classification performance of BERT, we selected multiple benchmarks for comparison, including composite-CNN [58], classical CNN, traditional machine learning methods, and THUCTC. Specifically, classical CNN includes single-layer convolutional neural network (CNN-1) and multi-layer convolutional neural network (CNN-3), while traditional machine learning methods include naive Bayes (NB), k-nearest neighbors (KNN), and support vector machine (SVM). The classification results of different models are shown in Table 1.

**Table 1.** Data set statistics.

Model	Precision	Recall	F1 Score
NB	0.819	0.816	0.814
KNN	0.855	0.853	0.849
SVM	0.874	0.876	0.874
CNN-1	0.925	0.924	0.924
CNN-3	0.919	0.918	0.917
composite-CNN	0.937	0.937	0.937
THUCTC	0.886	0.829	0.856
BERT	0.933	0.930	0.930

This indicates that BERT performs second only to the domain-specific model composite-CNN in Chinese text classification tasks.

When extracting time intervals from the dataset of Weibo users, we observed a significant right-skewed distribution of the data. This is attributed to the irregular activity patterns of Weibo platform users, resulting in the collected time interval data exhibiting extremely long-tail characteristics. Figure 5 illustrates the box plot of the time interval sequence, with the time series represented in minutes. By setting the maximum value to 2880 and applying two logarithmic transformations to all data, we effectively alleviated the right-skewness of the data. This processing strategy helps avoid excessive weights during training, thereby maintaining the stability of the model. The blue points in the left plot represent outlier samples. The right plot shows the box plot of the time interval sequence after processing.

We utilized kernel density estimation plots to reveal patterns in posting times among different user categories. Due to the highly skewed nature of the time interval data, to prevent the curves from being overly flattened, we capped the maximum value at 2880, as shown in Figure 6.

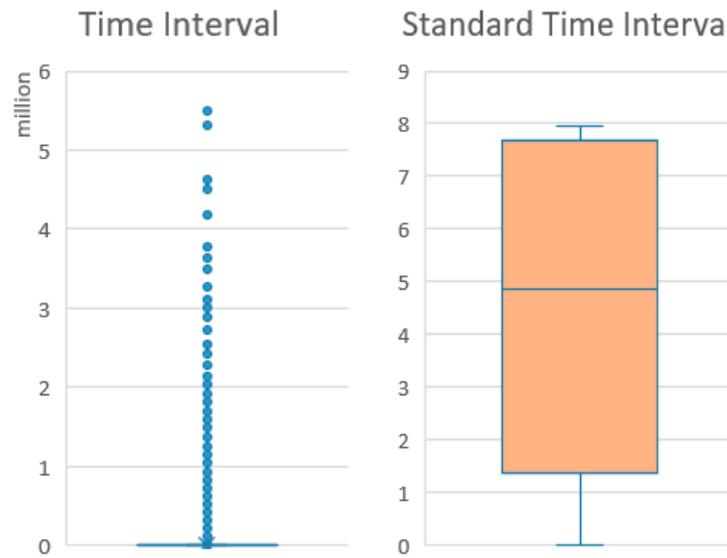


Figure 5. Box plots of time interval data.

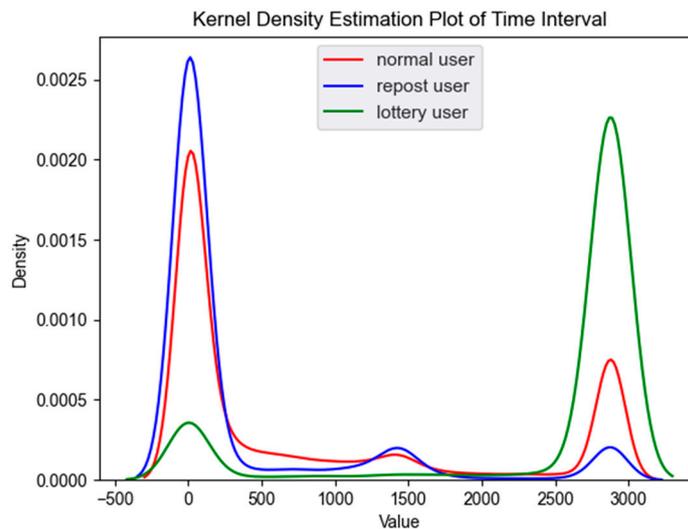


Figure 6. Kernel density plot of time intervals for different user categories.

Reposting users require continuous tweeting to maintain a high level of engagement, with the characteristic of frequent tweeting within short time intervals being particularly prominent. In contrast, lottery users exhibit a posting frequency closer to that of inactive users, with a relatively uniform pattern observed in the posting frequency within the time intervals of 500 to 2500 min.

#### 4.3. Data Sample Distribution and Evaluation Methods

##### 4.3.1. The Influence of Implicit Features on Sample Distribution

Before applying clustering algorithms, it is crucial to observe the distribution of samples in space. Figure 7 illustrates the impact of removing individual features on the distribution of samples in space, while also presenting the measurement results for selecting the Davies–Bouldin Index (DBI). The DBI is a metric used to evaluate clustering quality, considering both cluster cohesion and separation. A DBI coefficient closer to 0 indicates better clustering results. The observation from clustering metrics and T-SNE distributions indicates a noticeable deterioration in clustering effectiveness upon the removal of all latent features, with no distinct user delineation boundaries discernible. The incorporation of temporal analysis assists clustering algorithms in better discriminating between repost

users and normal users. Analysis of text composition in blog content and the diversity of posting reveal clear classification boundaries between normal users and repost users, suggesting discernible distinctions in posting behavior between repost users controlled by automated programs and normal users. Lottery users exhibit relatively uniform patterns both in posting format and content, such as the consistent absence of image content in blogs and the lack of opinions or viewpoints in blog content.

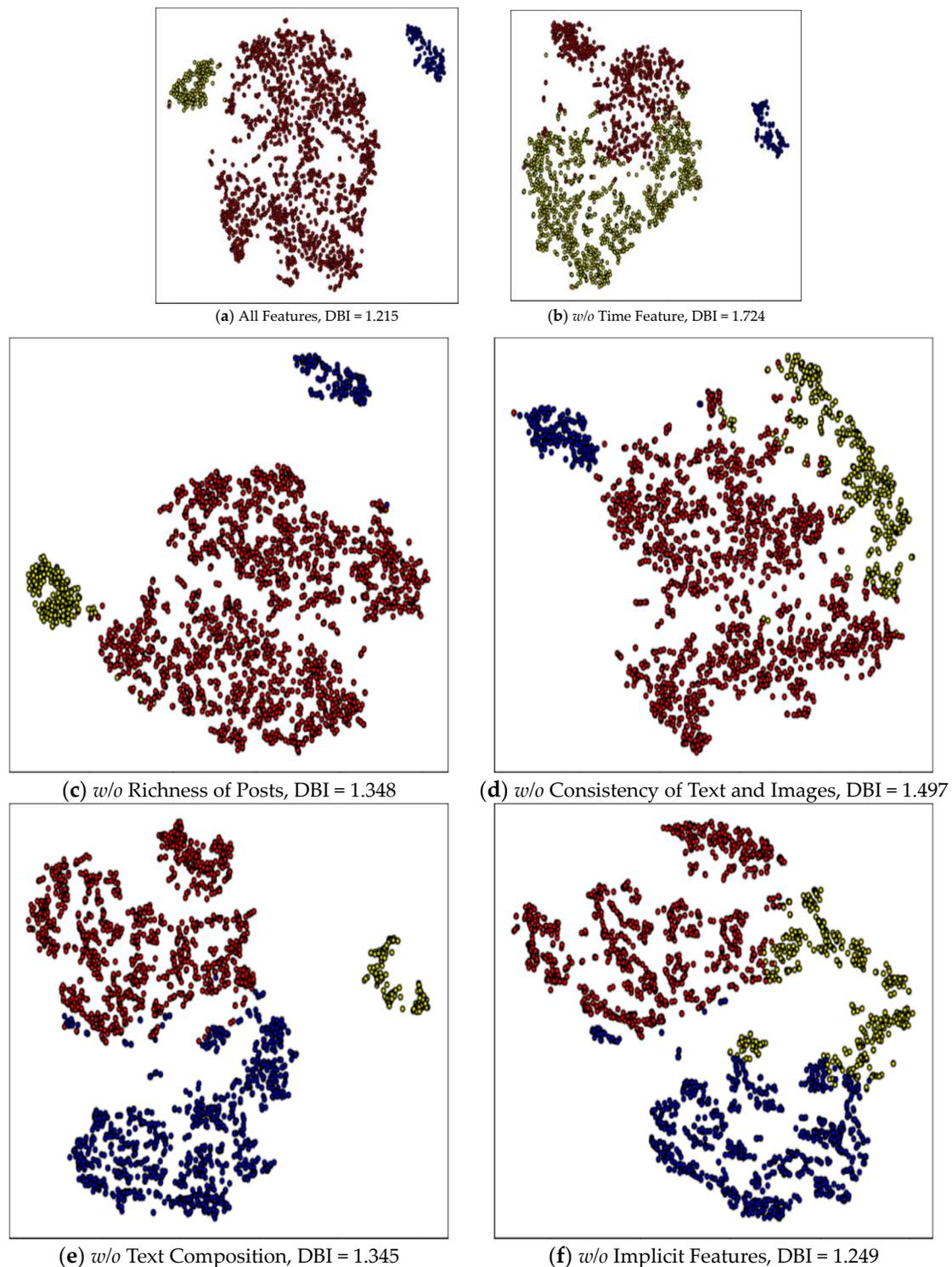


Figure 7. T-SNE data distribution plot when excluding certain features as clustering features.

#### 4.3.2. Performance Evaluation Metrics on Weibo User Dataset

The experiment used metrics such as Precision, Recall, and F1 Score to validate the performance of MAPM on the Weibo user dataset. Precision represents the model's ability to correctly predict positives, Recall measures the model's ability to identify all positives, and F1 Score combines Precision and Recall. Table 2 shows the Precision, Recall, and F1 Score for the three categories. When manually annotating user categories, we often encounter situations that are difficult to judge. A minority of reproduced users and lottery users exhibit signs of artificial manipulation under certain circumstances. In response to such cases, we categorize them uniformly as automated users. Because manual annotation introduces biases, it can potentially lead to a small amount of data bias.

**Table 2.** Precision, Recall, and F1 Scores for Three Categories.

User Category	Precision	Recall	F1 Score	Sample Size
Normal User	0.983	0.993	0.988	1756
Reproduce User	0.957	0.852	0.901	155
Lottery User	0.909	0.903	0.906	165

#### 4.3.3. Dissociation Experiment

To further demonstrate the superiority of multi-model joint representation in extracting user behavior features, this paper designed a dissociation experiment. By removing certain modules and comparing them with common internal measurement metrics used in clustering algorithms, the results of the dissociation experiment are shown in Table 3, where:

- MAPM: Includes all modules;
- *w/o* SIDN: Removes time series features;
- *w/o* BERT: Removes text composition features;
- *w/o* clip: Removes text-image consistency features;
- *w/o* DEEP: Disables all deep learning modules, retaining only explicit user features;
- Normalize Scores: Uses normalized Davies–Bouldin scores plus Calinski–Harabasz scores minus Silhouette scores to obtain Normalize Score scores.

**Table 3.** Internal metrics for ablation experiments.

Methods	Behavioral Analysis Module			Internal Metrics			
	SIDN	cn Clip	BERT	Davies	Calinski	Silhouette	Normalize Score
MAPM	✓	✓	✓	<b>1.224</b>	297.014	0.109	<b>−0.245</b>
<i>w/o</i> SIDN	×	✓	✓	1.497	<b>296.480</b>	0.043	1.002
<i>w/o</i> BERT	✓	✓	×	1.463	609.496	0.227	0.924
<i>w/o</i> clip	✓	×	✓	1.452	340.384	0.137	0.501
<i>w/o</i> DEEP	×	×	×	1.367	580.108	<b>0.234</b>	0.476

Table 3 highlights the scores of the most superior models in each category. The clustering indicators show the most significant decrease after disabling SIDN, indicating the crucial role of time series features mined by the SIDN network in detecting fake users. The overall clustering scores of the module without behavioral features are lower than those of the MAPM model, demonstrating that introducing the multi-model joint representation method in the model can effectively improve the clustering performance of the classifier.

#### 4.4. Exploration of Implicit Features and Hyperparameter Selection Effects

To further validate the contribution of implicit user features to user classification decisions and the optimality of spectral clustering cluster parameter selection, we present

the visual results of the experiments. Figure 8 displays the comparison results of disabling individual deep learning modules on the weighted average precision and recall of samples. The vertical axis represents the variation of their precision.

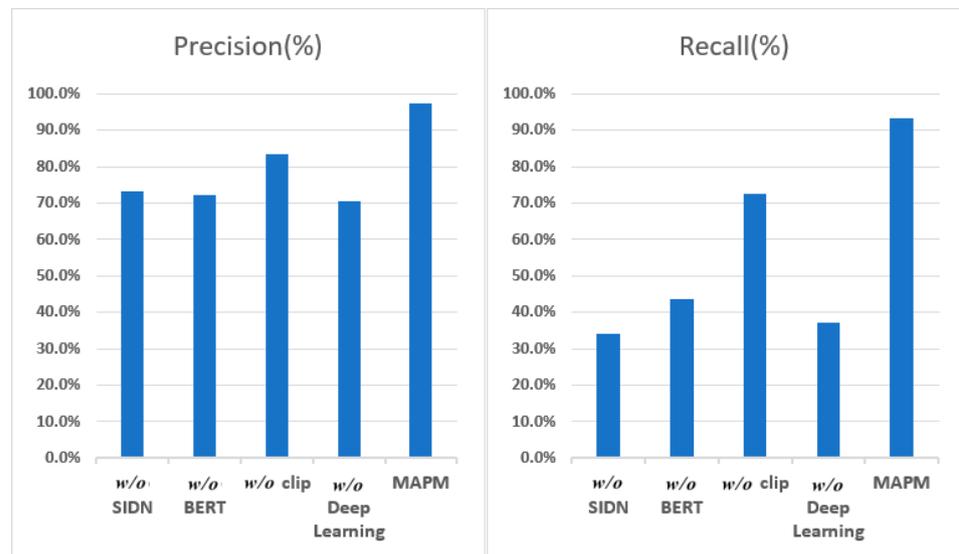


Figure 8. The visualization results of the ablation experiment’s accuracy and recall.

In Spectral Clustering, the affinity parameter is used to determine the similarity or connectivity between samples. The choice of this parameter directly impacts the final effectiveness of the clustering algorithm, and its proper selection can significantly enhance the performance and efficiency of the clustering algorithm. Figure 9 illustrates the impact of selecting different parameters on the model’s classification performance, measured using macro-averaged Precision, Recall, and F1 score.

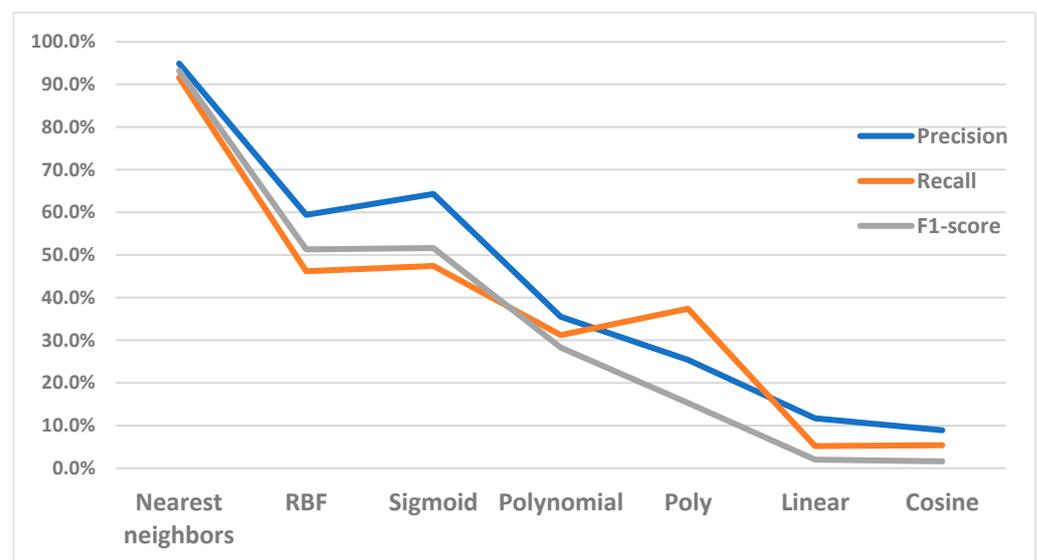
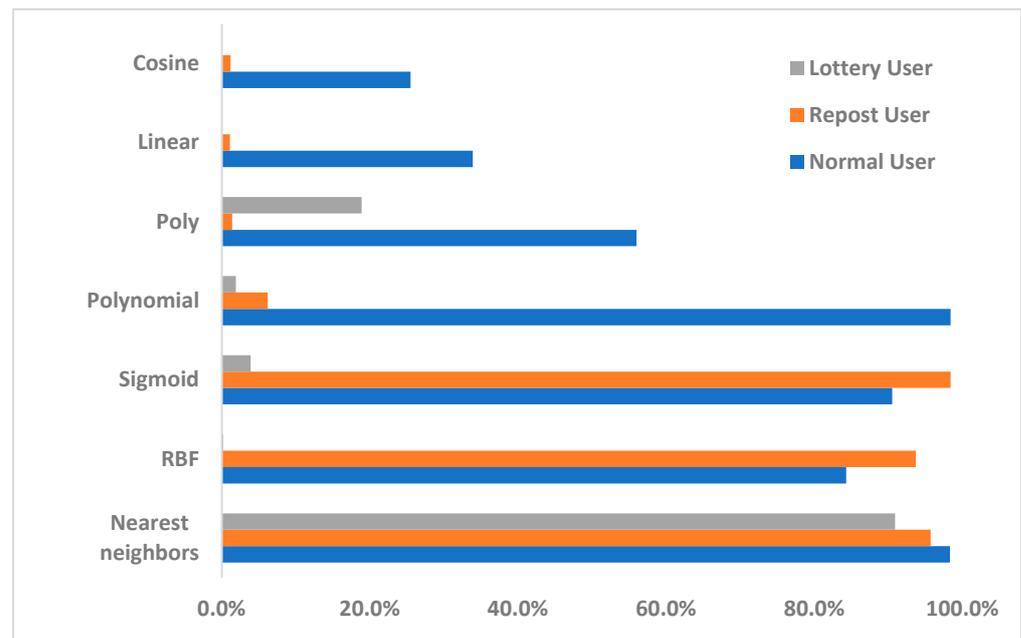


Figure 9. The impact of different parameters on model performance.

Figure 10 is used to demonstrate the impact of different parameters on the model’s accuracy across different categories. We chose “nearest neighbors” as the strategy for quantifying similarity between samples, as it yielded the best clustering performance for the classifier.



**Figure 10.** The accuracy across different categories.

From the experimental results, we observe that compared to disabling the behavior analysis module, the MAPM version performs better in terms of prediction accuracy and recall. For example, in the user classification dataset, the performance of the MAPM version is nearly 27.0% higher than that of the classification model using only explicit features for classification. Therefore, we can confidently say that compared to traditional fake user detection schemes, the multi-model joint representation strategy is more suitable for fine-grained detection of fake users.

## 5. Conclusions and Future Work

This paper proposes a scheme for detecting fake users on social media platforms based on multi-model joint characterization and introduces a multi-modal aggregation portrait model for detecting fake users. It combines multiple models that perform best in the field to characterize the behavior of users posting blogs on social media platforms. Specifically, we introduce the SIDN network module to capture the temporal patterns of fake user postings. Experimental results on the Weibo user dataset demonstrate the significant role of the SIDN network architecture in extracting user behavior features in the field of fake user identification, while the MAPM model performs well in the task of fake user detection. In addition, there are some limitations to this study. Since the training corpora for BERT and cn\_clip only contain Chinese text, MAPM cannot be applied to non-Chinese data samples. The use of multiple deep learning models for feature extraction results in slower model inference speed. Furthermore, constrained by insufficient data samples, MAPM is still unable to detect a broader range of user types.

Discriminant analysis technology that integrates the results of multiple large models provides an excellent opportunity for upgrading artificial intelligence technology for online content analysis and user mining on social platforms. In this sense, vertical domain analysis technology that aggregates large models represents the vertical development of machine learning, which can be applied to a wider range of scenarios by more people. We hope that this framework design will provide a new idea for previous social multi-modal content data analysis, and it may open up new research space for more general false information detection and mining tasks.

**Author Contributions:** Investigation, Software, Writing Original Draft, Validation, Methodology, W.J.; Conceptualization, Methodology, Supervision and Writing—Review and Editing, J.L.; computing resources and automated data collection, J.Z.; data curation and writing, Y.S. and W.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by Basic Research Project of the National Defence Science and Industry Bureau (Project No. JCKY2022405C010), the Translational Application Project of the “Wise Eyes Action” (Project No. F2B6A194) and Beijing Information Science and Technology University Education Reform (Project No. 2024JGYB35). We would like to express our deepest gratitude to these organizations for their generous funding and support.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The datasets presented in this study are available at <https://github.com/JackPotProject/User-Clustering> (accessed on 15 February 2024).

**Acknowledgments:** We would like to express our gratitude to Yanhua Shao (The Sixth Research Institute of China Electronics and Information Industry Corporation) for providing computational resources and support.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Nan, Q.; Cao, J.; Zhu, Y.; Wang, J.; Li, M. DFEND: Multi-domain fake news detection. In Proceedings of the 30th ACM International Conference on Information & Knowledge Management, Virtual, 1–5 November 2021; pp. 3343–3347.
2. Ma, J.; Gao, W.; Wong, K.F. Detect rumors on twitter by promoting information campaigns with generative adversarial learning. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 3049–3055.
3. Vaibhav, V.; Annasamy, R.M.; Hovy, E. Do sentence interactions matter? leveraging sentence level representations for fake news classification. *arXiv* **2019**, arXiv:1910.12203.
4. Cheng, M.; Nazarian, S.; Bogdan, P. Vroc: Variational autoencoder-aided multi-task rumor classifier based on text. In Proceedings of the Web Conference 2020, Taipei, Taiwan, 20–24 April 2020; pp. 2892–2898.
5. Singhal, S.; Kabra, A.; Sharma, M.; Shah, R.R.; Chakraborty, T.; Kumaraguru, P. Spotfake+: A multimodal framework for fake news detection via transfer learning (student abstract). *Proc. AAAI Conf. Artif. Intell.* **2020**, *34*, 13915–13916. [CrossRef]
6. Wang, Y.; Ma, F.; Jin, Z.; Yuan, Y.; Xun, G.; Jha, K.; Su, J.; Gao, J. Eann: Event adversarial neural networks for multi-modal fake news detection. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, UK, 19–23 August 2018; pp. 849–857.
7. Khattar, D.; Goud, J.S.; Gupta, M.; Varma, D. Mvae: Multimodal variational autoencoder for fake news detection. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 2915–2921.
8. Jin, Z.; Cao, J.; Guo, H.; Zhang, Y.; Luo, J. Multimodal fusion with recurrent neural networks for rumor detection on microblogs. In Proceedings of the 25th ACM International Conference on Multimedia, Mountain View, CA, USA, 23–27 October 2017; pp. 795–816.
9. Wu, Y.; Zhan, P.; Zhang, Y.; Wang, L.; Xu, Z. Multimodal fusion with co-attention networks for fake news detection. In Proceedings of the Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021, Online, 1–6 August 2021; pp. 2560–2569.
10. Jiang, S.; Chen, X.; Zhang, L.; Chen, S.; Liu, H. User-characteristic enhanced model for fake news detection in social media. In Proceedings of the Natural Language Processing and Chinese Computing: 8th CCF International Conference, NLPCC 2019, Dunhuang, China, 9–14 October 2019; Springer International Publishing: Cham, Switzerland, 2019; pp. 634–646.
11. Chen, L.; Ruan, S.; Chen, X.; Wang, H. Research on Intelligent Detection of Social Media Robot Accounts. *Netinfo Secur.* **2019**, *19*, 96–100.
12. Akyon, F.C.; Kalfaoglu, M.E. Instagram fake and automated account detection. In Proceedings of the 2019 Innovations in intelligent systems and applications conference (ASYU), Izmir, Turkey, 31 October–2 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–7.
13. Liu, K.; Yuan, Y.Y.; Liu, P. Weibo bot-users identification model based on random forest. *Acta Sci. Nat. Univ. Pekin.* **2015**, *52*, 290–300.
14. Zhang, J.; Zhao, Y.; Saleh, M.; Liu, P. Pegasus: Pre-training with extracted gap-sentences for abstractive summarization. In Proceedings of the International Conference on Machine Learning, PMLR, Virtual, 13–18 July 2020; pp. 11328–11339.
15. Yang, A.; Pan, J.; Lin, J.; Men, R.; Zhang, Y.; Zhou, J.; Zhou, C. Chinese clip: Contrastive vision-language pretraining in chinese. *arXiv* **2022**, arXiv:2211.01335.
16. Radford, A.; Kim, J.W.; Hallacy, C.; Ramesh, A.; Goh, G.; Agarwal, S.; Sastry, G.; Askell, A.; Mishkin, P.; Clark, J.; et al. Learning transferable visual models from natural language supervision. In Proceedings of the International conference on machine learning, PMLR, Virtual, 18–24 July 2021; pp. 8748–8763.

17. Devlin, J.; Chang, M.W.; Lee, K.; Toutanova, K. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv* **2018**, arXiv:1810.04805.
18. Guo, X.; Liu, X.; Ren, Z.; Grosz, S.; Masi, I.; Liu, X. Hierarchical fine-grained image forgery detection and localization. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Vancouver, BC, Canada, 17–24 June 2023; pp. 3155–3165.
19. Sutskever, I.; Vinyals, O.; Le, Q.V. Sequence to sequence learning with neural networks. *arXiv* **2014**, arXiv:1409.3215.
20. Von Luxburg, U. A tutorial on spectral clustering. *Stat. Comput.* **2007**, *17*, 395–416. [[CrossRef](#)]
21. Allcott, H.; Gentzkow, M. Social media and fake news in the 2016 election. *J. Econ. Perspect.* **2017**, *31*, 211–236. [[CrossRef](#)]
22. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake news detection on social media: A data mining perspective. *ACM SIGKDD Explor. Newsl.* **2017**, *19*, 22–36. [[CrossRef](#)]
23. Rusidn, V.L.; Conroy, N.J.; Chen, Y.; Cornwell, S. Fake news or truth? using satirical cues to detect potentially misleading news. In Proceedings of NAACL-HLT, San Diego, CA, USA, 12–17 June 2016; pp. 7–17.
24. Rusidn, V.L.; Chen, Y.; Conroy, N.K. Deception detection for news: Three types of fakes. *Proc. Assoc. Inf. Sci. Technol.* **2015**, *52*, 1–4.
25. Ma, J.; Gao, W.; Mitra, P.; Kwon, S.; Jansen, B.J.; Wong, K.F.; Cha, M. Detecting rumors from microblogs with recurrent neural networks. In Proceedings of the 25th International Joint Conference on Artificial Intelligence (IJCAI 2016), New York, NY, USA, 9–15 July 2016; pp. 3818–3824.
26. Ma, J.; Gao, W.; Wong, K.F. Detect rumor and stance jointly by neural multi-task learning. In Proceedings of the Companion Proceedings of the Web Conference 2018, Lyon, France, 23–27 April 2018; pp. 585–593.
27. Liu, J.; Lu, W.; Huang, G.; Ma, N. Research on Internet false information recognition based on deep learning. *Intell. Eng.* **2022**, *8*, 86–99.
28. Qi, P.; Cao, J.; Yang, T.; Guo, J.; Li, J. Exploiting multi-domain visual information for fake news detection. In Proceedings of the 2019 IEEE International Conference on data mining (ICDM), Beijing, China, 8–11 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 518–527.
29. Zhou, X.; Wu, J.; Zafarani, R. Similarity-Aware Multi-modal Fake News Detection. In Proceedings of the Pacific-Asia Conference on Knowledge Discovery and Data Mining, Singapore, 11–14 May 2020; Springer International Publishing: Cham, Switzerland, 2020; pp. 354–367.
30. Meng, J.; Wang, L.; Yang, Y.; Lian, B. Multi-modal deep fusion for false information detection. *J. Comput. Appl.* **2022**, *42*, 419.
31. Qi, P.; Cao, J.; Li, X.; Lian, B. Improving fake news detection by using an entity-enhanced framework to fuse diverse multimodal clues. In Proceedings of the 29th ACM International Conference on Multimedia, Virtual, 20–24 October 2021; pp. 1212–1220.
32. Raza, S. Automatic fake news detection in political platforms—a transformer-based approach. In Proceedings of the 4th Workshop on Challenges and Applications of Automated Extraction of Socio-Political Events from Text (CASE 2021), Online, 5–6 August 2021; pp. 68–78.
33. Ying, Q.; Hu, X.; Zhou, Y.; Qian, Z.; Zeng, D.; Ge, S. Bootstrapping multi-view representations for fake news detection. *Proc. AAAI Conf. Artif. Intell.* **2023**, *37*, 5384–5392. [[CrossRef](#)]
34. Kaplan, A.M.; Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. *Bus. Horiz.* **2010**, *53*, 59–68. [[CrossRef](#)]
35. Roy, P.K.; Chahar, S. Fake profile detection on social networking websites: A comprehensive review. *IEEE Trans. Artif. Intell.* **2020**, *1*, 271–285. [[CrossRef](#)]
36. Lu, Y.J.; Li, C.T. GCAN: Graph-aware co-attention networks for explainable fake news detection on social media. *arXiv* **2020**, arXiv:2004.11648.
37. Dou, Y.; Shu, K.; Xia, C.; Yu, P.S.; Sun, L. User preference-aware fake news detection. In Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval, Online, 11–15 July 2021; pp. 2051–2055.
38. Yuan, D.; Zhang, Y.; Gao, J.; Sun, H. Anomaly User Detection Method in Sina Weibo Based on User Feature Extraction. *Comput. Sci.* **2020**, *47*, 364–368+385.
39. Durga, P.; Sudhakar, T. The use of supervised machine learning classifiers for the detection of fake instagram accounts. *J. Pharm. Negat. Results* **2023**, 267–279.
40. Khaled, S.; El-Tazi, N.; Mokhtar, H.M.O. Detecting fake accounts on social media. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 3672–3681.
41. Van Der Walt, E.; Eloff, J. Using machine learning to detect fake identities: Bots vs. humans. *IEEE Access* **2018**, *6*, 6540–6549. [[CrossRef](#)]
42. Viswanath, B.; Bashir, M.A.; Crovella, M.; Guha, S.; Gummadi, K.P.; Krishnamurthy, B.; Mislove, A. Towards detecting anomalous user behavior in online social networks. In Proceedings of the 23rd Usenix Security Symposium (Usenix Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 223–238.
43. Yang, W.; Shen, G.W.; Wang, W.; Gong, L.Y.; Yu, M.; Dong, G.Z. Anomaly detection in microblogging via co-clustering. *J. Comput. Sci. Technol.* **2015**, *30*, 1097–1108. [[CrossRef](#)]
44. Heidari, M.; James, H., Jr.; Uzuner, O. An empirical study of machine learning algorithms for social media bot detection. In Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.

45. Mohammad, S.; Khan, M.U.S.; Ali, M.; Liu, L.; Shardlow, M.; Nawaz, R. Bot detection using a single post on social media. In Proceedings of the 2019 Third World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, UK, 30–31 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 215–220.
46. Uppada, S.K.; Manasa, K.; Vidhathi, B.; Harini, R.; Sivaselvan, B. Novel approaches to fake news and fake account detection in OSNs: User social engagement and visual content centric model. *Soc. Netw. Anal. Min.* **2022**, *12*, 52. [[CrossRef](#)] [[PubMed](#)]
47. Zhang, Y.; Lu, J. Discover millions of fake followers in Weibo. *Soc. Netw. Anal. Min.* **2016**, *6*, 16. [[CrossRef](#)]
48. Cresci, S.; Di Pietro, R.; Petrocchi, M.; Spognardi, A.; Tesconi, M. Fame for sale: Efficient detection of fake Twitter followers. *Decis. Support Syst.* **2015**, *80*, 56–71. [[CrossRef](#)]
49. Zhang, Z.; Jing, J.; Li, F.; Habib, A.; Khan, A. A review of research on detection, dissemination and control of false information in online social networks from the perspective of artificial intelligence. *J. Comput. Sci.* **2021**, *44*, 2261–2282.
50. Shao, C.; Ciampaglia, G.L.; Varol, O.; Flammini, A.; Menczer, F. The spread of fake news by social bots. *arXiv* **2017**, arXiv:1707.07592.
51. Kondeti, P.; Yerramreddy, L.P.; Pradhan, A.; Swain, G. Fake account detection using machine learning. In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020*; Springer: Singapore, 2021; pp. 791–802.
52. Bharti, K.K.; Pandey, S. Fake account detection in twitter using logistic regression with particle swarm optimization. *Soft Comput.* **2021**, *25*, 11333–11345. [[CrossRef](#)]
53. Wang, X.; Zheng, Q.; Zheng, K.; Sui, Y.; Cao, S.; Shi, Y. Detecting social media bots with variational autoencoder and k-nearest neighbor. *Appl. Sci.* **2021**, *11*, 5482. [[CrossRef](#)]
54. Shreya, K.; Kothapelly, A.; Deepika, V.; Shanmugasundaram, H. Identification of Fake accounts in social media using machine learning. In Proceedings of the 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 26–27 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–4.
55. Zhang, J.; Gan, R.; Wang, J.; Zhang, Y.; Zhang, L.; Yang, P.; Chen, C. Fengshenbang 1.0: Being the foundation of Chinese cognitive intelligence. *arXiv* **2022**, arXiv:2209.02970.
56. Ying, Q.F.; Chiu, D.M.; Venkatramanan, S.; Zhang, X. User modeling and usage profiling based on temporal posting behavior in OSNs. *Online Soc. Netw. Media* **2018**, *8*, 32–41. [[CrossRef](#)]
57. Li, J.; Sun, M. Scalable Term Selection for Text Categorization. In Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL), Prague, Czech Republic, 28–30 June 2007; pp. 774–782.
58. Zhang, Y.; Liu, K.; Zhang, Q.; Wang, Y.; Gao, K. A combined-convolutional neural network for Chinese news text classification. *Acta Electronica Sin.* **2021**, *49*, 1059.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.