mathematics

MDPI

Article

Hybrid Fake Information Containing Strategy Exploiting Multi-Dimensions Data in Online Community

Huiru Cao [1], Xiaomin Li [2,*], Yanfeng Lin [2] and Songyao Lian [3]

[1] Department of Information Engineering, Guangzhou Institute of Technology, Guangzhou 510725, China
[2] College of Mechanical and Electrical Engineering, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China
[3] Department of Electrical and Computer Engineering, Nanfang College of Sun Yat-sen University, Guangzhou 510970, China
* Correspondence: lixiaomin@zhku.edu.cn

Abstract: It is well-established that, in the past few years, internet users have rapidly increased. Meanwhile, various types of fake information (such as fake news or rumors) have been flooding social media platforms or online communities. The effective containing or controlling of fake news or rumor has drawn wide attention from areas such as academia to social media platforms. For that reason, numerous studies have focused on this subject from different perspectives, such as employing complex networks and spreading models. However, in the real online community, misinformation usually spreads quickly to thousands of users within minutes. Conventional studies are too theoretical or complicated to be applied to practical applications, and show a lack of fast responsiveness and poor containing effects. Therefore, in this work, a hybrid strategy exploiting the multi-dimensional data of users and content was proposed for the fast containing of fake information in the online community. The strategy is mainly composed of three steps: the fast detection of fake information by continuously updating the content comparison dataset according to the specific hot topic and the fake contents; creating spreading force models and user divisions via historical data, and limiting the propagation of fake information based on the content and user division. Finally, an experiment was set up online with BBS (Bulletin Board System), and the acquired results were analyzed by comparison with other methods in different metrics. From the extracted results, it has been demonstrated that the proposed solution clearly outperforms traditional methods.

Keywords: fake information; online community; social network; multi-dimension data

MSC: 68M11

Citation: Cao, H.; Li, X.; Lin, Y.; Lian, S. Hybrid Fake Information Containing Strategy Exploiting Multi-Dimensions Data in Online Community. *Mathematics* **2022**, *10*, 3265. https://doi.org/10.3390/math10183265

Academic Editor: Zhao Kang

Received: 8 August 2022
Accepted: 5 September 2022
Published: 8 September 2022

1. Introduction

In recent years, with the continuous popularization and improvement of the network infrastructure, the internet has developed rapidly worldwide [1–3]. As a result, millions of smart terminals are connected to the internet, especially as far as mobile devices are concerned [4]. It has been reported that the number of internet users is more than 5 billion, which implies that 60% of the world population is being affected by the quick increase in mobile phones [5]. Meanwhile, the number of active social media users is larger than 4.2 billion, and a growing number of people enjoy "smart" services from different applications, for example, BBS, Twitter, and WeChat [6–9]. As a result, information release, acquisition, and discussion are transferring from offline to online formats. In addition, the constantly increasing online community has become the main channel for exchanging opinions and messages [10,11].

It is also well-known that the online community plays a significant role in news or information spreading. As in the real world, fake news, misinformation, and rumors are quickly spread on the internet [12]. Differently from traditional fake information spreading,

some significant features of fake news can be detected on the internet [13,14]. Firstly, the spread of fake information takes place at a relatively faster speed. It is obvious that the user can more easily connect to the internet than to conventional mediums, such as through newspapers or magazines, while the internet could accelerate the spreading speed at a lower cost. Consequently, fake information is rather prone to be quickly spread in cyberspace. Secondly, fake information is propagated more widely. As billions of people are in the same cyberspace, fake information can easily impact and infect more users. Thirdly, fake information can easily infect other users. With the rapid development of the internet, fake news or rumors are easily and repetitively flooding our daily life through different channels. Thus, fake news is rendered even more confusing and more difficult to identify.

As fake information through the vast network of the internet has the above-mentioned new features, it can cause harm and losses [15]. On the one hand, once the influence of false information is formed, it is difficult to be removed quickly. Furthermore, once the fake information (especially rumors) runs deep and begins to threaten public safety, it has the potential ability to form a gap among people. On the other hand, when fake information gets worse, it is anticipated to cause huge economic and life losses. Moreover, from the academic perspective, there are interactive relationships between false information research and natural language processing and sentiment analysis [16,17]. It is known that fake information detection is one of the main subtopics of natural language processing, and fake information-related studies are the basis for internet sentimental analysis. Meanwhile, natural language processing and sentiment analysis provide the necessary support for research into false information. Therefore, it is meaningful to contain and control the internet's fake information.

An elevated number of studies focusing on this topic can be found in the literature. These studies can be divided into the following aspects: fake information spreading models [18], detection [19,20] and containing [21]. As far as the containing of fake information is concerned, the studies have gone through several stages [22]. More specifically, in the beginning, complex systems theory and mathematical models were used in the majority of the reported works to solve the problem. However, these works are more complex than real applications. Then, with the introduction of machine learning and deep learning techniques into the domain, more studies began to exploit ML (Machine Learning) and DL (Deep Learning) to deal with the problem. However, the implementation of such types of methods is wise after the event given lack of a fast response for containing the fake news or the rumor in online communities, since most ML and DL are based on the massive degree of fake information data labeling that takes place after the event. It is interesting to notice that there are still several problems with containing fake news, including the fast detection of fake information, the selection of the potential and meaning of fake information, and the development of a reasonable and effective containing algorithm.

According to the previously reported studies, exploiting multi-dimensional data for a hybrid approach to containing or controlling fake information in the online community was proposed. This strategy can be divided into the three following phases: Fast detection of the fake information based on the user number difference and content comparison. Then, a fake information-related spreading force (SF) mathematical model was established based on the utilization of the users' multi-dimensional data, and fake information was contained differently based on the user behavior and content fakeness degree. At last, an experiment was carried out to assess the performance of the proposed strategy.

Against this background, this work has been organized as follows: The related work is introduced in Section 2. The fake news-containing framework is presented in Section 3. The details of the proposal containing misinformation are given in Section 4. Meanwhile, experimental and results analysis are provided in Section 5. Finally, the extracted conclusions are presented in Section 6.

2. Related Work

2.1. Fake Information Detection

It is well-known that the detection of fake news or rumor is key to monitoring or controlling its spread. For that reason, an increasing number of studies can be found in the literature that seek to solve this problem. The various fake information detection methods can be categorized into two groups, namely, machine learning and deep learning [23]. In reference [24], based on the implementation of the K-nearest Neighbor algorithm, the authors designed a classifier to detect fake news. Then, the experiment was finished using the Facebook news post dataset. In reference [25], the authors used the multinomial naive Bayes (MNB) and support vector machine (SVM) classifiers to detect Bangla fake news. From the experimental outcomes, it was proven that SVM exhibits a higher degree of accuracy than MNB methods. To further improve the detection accuracy, various works in the literature began to use a hybrid model by merging different machine learning methods. For example, a hybrid method using a recurrent neural network (RNN) and SVM was established to find real and fake news in reference [26]. With further development in the field, deep learning-based techniques for attaining better performance in this area have been proposed [27]. More specifically, in reference [28], a new deep learning model was designed, which combines convolutional and recurrent neural networks to discover fake contents. In reference [29], based on the implementation of a bi-directional long short-term memory (Bi-LSTM) model, a classifier was presented for detecting real or fake news. Although the above-mentioned studies present different choices for the subject, most detection methods are based on a large number of labeled datasets and complicated models, which take up a lot of time in completing the training and detection procedures, and this is not suitable for controlling the spread of fake information in real-life applications.

2.2. Method of Containing Fake Information

It is well-established that social media facilitates a higher spreading speed of real or fake information than traditional platforms. Hence, containing or controlling fake information to reduce unnecessary loss [30] has become a hot research issue. Therefore, a great number of works in the literature focus on the domain. In reference [31], a rumor-spreading model for social networks was built, and then a rumor-containing algorithm was presented that can solve model optimization problems. In reference [32], the fake information containment problem was modeled as an optimization problem, and an isolation–conversion strategy was proposed based on the utilization of the complex network theory. The above-mentioned rumor or fake information models are mostly based on graphs and complex network theories, while the controlling algorithms are too idealistic, and exceed practical conditions. A growing number of works in the literature focus on social media spreading rules or models to control the adverse impacts of fake news [33]. Based on the counterpart of real life, an anti-rumor message-sending mechanism, that consults reputable authorities and trusted friends, was proposed in reference [34]. In reference [35], a discrete particle swarm method was used to select the influential node in an online social network, and a soft dynamic quarantine strategy was applied in rumor propagation control based on the most influential nodes. Although the above-mentioned works provide the necessary characteristics for rumor or fake information control, most studies do not consider the impacts of online social networks for real applications, such as the lack of key ideal data or parameters, which can hinder the practical implementation of these strategies.

3. Framework for Containing Fake Information

From the social media platform management perspective, it is of great importance to build a novel fake information containment strategy based on available data from real-life applications. Therefore, an effective and fast fake information containing method was proposed according to the utilization of multiple parameters, such as content, user behavior, spreading force and impact of the fake information. As can be observed from Figure 1, the framework consists of five different parts: platform monitoring, information feature

analysis, fake information discrimination and selection, fake information classification, and fake information containing.

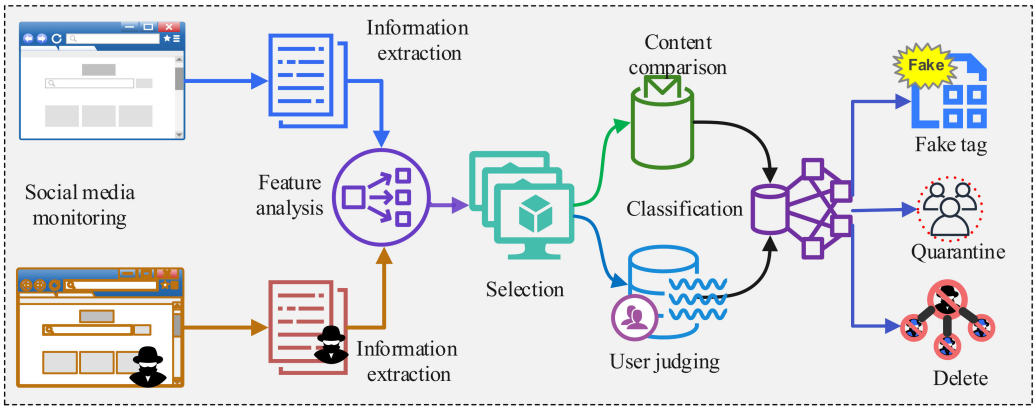

Figure 1. Framework of the proposed fake information containing strategy.

The framework introduced fake information with many aspects, while the working process of the strategy can be described as follows: Firstly, the social media management system monitors the released content and new posts created by the users. In addition, the related parameters, such as visiting number, replier number, time label, etc., are collected and stored in the related database. Secondly, information extraction is completed by the management system (for example, text and event), which also completes the feature analysis of these monitoring contents. Then, the most popular post or content is extracted to determine the change in the user number during the interval. Thirdly, the contents are selected by content comparison with a live updating fake content dataset, and the users are divided by behavior and other indexes. Then, the fake spreading force is computed in line with the content and users. Finally, the system deals with the fake content by different approaches (such as fake news tagging, user or content quarantining and deleting), which are based on the fake content spreading force, content, and user division.

In order to derive a good content dataset, several methods are available. Firstly, the initial dataset is created by different types of users who provide different fake information content on the same topic. The different types of users can balance the user bias. Secondly, during the online learning process, if the false information without labels (or that which is matched as "non-fake") appears several times or in the next monitoring period, the fake information is evaluated again and added into the dataset.

4. Multi-Dimension Data-Driven Fake Information Method

4.1. Mathematical Model

In this section, a mathematical model has been built from social media platforms (for example, BBS (bulletin board system), talk web, etc.) for containing the propagation of the fake information. The social media content follows time serials. Therefore, the content monitoring method can be divided into many time intervals. By assuming that $T = \left\{t_1, t_2, \cdots, t_{|T|}\right\}$ is the time intervals set and $O = \left\{o_1, o_2, \cdots, o_{|O|}\right\}$ is the talking or discussion topic, the current time interval can be set as $t(t \in T)$. Without loss of generality, $S = \left\{s_1, s_2, \cdots, s_{|S|}\right\}$ was regarded as the set of newly created posts or web pages during time t on the same topic $o(o \in O)$. Moreover, $U = \left\{u_1, u_2, \cdots u_{|U|}\right\}$ represents the user of S. Hence, we derive the following equation:

$$U = V + R \tag{1}$$

where V and R refer to the viewers and repliers of S, respectively.

For any $s_i (i \in [S])$ ([•] is the total element number of •), $n_v^{s_i}(t), n_r^{s_i}(t)$ were considered as the numbers of viewers and repliers of s_i , respectively. Therefore, the total number of viewers and repliers of S in time t can be formalized as follows:

$$N_v^S(t) = \sum_{i \in [S]} n_v^{s_i}(t) \tag{2}$$

$$N_r^S(t) = \sum_{i \in [S]} n_r^{s_i}(t). \tag{3}$$

According to the above-mentioned assumptions and Equations (1)–(3), it is easy to derive the total number of users $N(t, o)$ contributing to topic $o (o \in O)$ in time t, which can be described as follows:

$$N(t, o) = \left| U \right| = N_v^S(t) + N_r^S(t). \tag{4}$$

Based on real-life applications, fake information is usually hidden within a popular topic for optimal spread and impact. In addition, fake information on hot topics can quite easily cause damage and losses. Therefore, the acquisition of the most popular topic is considered the most essential first step. In this work, based on the differential concept, the difference of $N(t, o)$ can be derived as follows:

$$\Delta N(t, o) = N(t, o) - N(t - 1, o) \tag{5}$$

where $N(t - 1, o)$ is the total user number of topic $o (o \in O)$ in time $t - 1$.

Topic o is a hot topic that easily includes more fake information when the difference of $\Delta N(t, o)$ is larger than the threshold value. Specifically, the value $\Delta N(t, o)$ can be obtained from historic data on the online community user number of a similar hot topic. In other words, $\Delta N(t, o)$ is the average of the total user number of a hot topic within time t. The following formulation was used:

$$\Delta N(t, o) \geq N_0(t, o). \tag{6}$$

After determining the hot topic, all content on said topic o_{hot} can be collected as content set $C = \left\{ c_1, c_2, \cdots, c_{|C|} \right\}$. By assuming that $\Delta = \left\{ \Delta_1, \Delta_2, \cdots, \Delta_{|\Delta|} \right\}$ is the standard or initialized fake content set of the hot topic o_{hot}, for any content $c (c \in C)$ (that means c is any content), the content comparison can be employed for determining whether the content c is fake information or not, which can be formulated using the following equation:

$$\cos\theta = \frac{L \times \Delta_k^T}{\left| L \right| \times \left| \Delta_k^T \right|} = \frac{\sum\limits_{i \in n} (\iota_i \times \delta_i^k)}{\sqrt{\sum\limits_{i \in n} l_i^2} \times \sqrt{\sum\limits_{i \in n} (\delta_i^k)^2}} \tag{7}$$

where L is the word vector of $c (c \in C)$, Δ_k denotes the k-th word vector of the standard fake information of the hot topic o_{hot}, l_i denotes the i-th word of L, and δ_i^k denotes the i-th word of Δ_k. Usually, the standard fake content set can be continuously updated by inserting new fake content according to Equation (7). Then, the fake value of content c can be determined by computing the max value of Equation (6):

$$fv(c) = \mathrm{Max}(\cos\theta(\Delta_k)) \quad (k \in [\Delta]). \tag{8}$$

Then, to evaluate the fake content, the fake degree of social media is used, according to the fake value that was mentioned above.

Definition 1. *The fake degree ($fd(t, o_{hot})$) is the average fake value of all content C for the hot topic o_{hot} during time t. Therefore, the fake degree of the topic o_{hot} can be defined as follows:*

$$fd(t, o_{hot}) = \sum_{i \in |C|} fv(c_i)/[C]. \tag{9}$$

According to Definition 1 and Equations (8) and (9), the fake degree was used to measure the fake information content of a hot topic. It is well-known that fake information's impact includes the fake information itself and its spreading impact [36]. Therefore, the two factors should be considered using a good method, and so our proposed model considers not only the fake degree, but also the spreading force, in containing fake information. From the social media platform management point of view, it is easy to access some user historical data, such as users' friends or followers, the number of users participating in fake information spreading, and so on. Furthermore, the user's historical behavior data can be used to build the spreading model.

Consequently, according to the historic user data, the fake information spreading coefficient of the user u can be calculated as follows:

$$fs = fs_0 + \lambda \frac{n_f(u)}{N_f} - \eta \frac{n_r(u)}{N_r} \tag{10}$$

where fs_0 is the start value, N_f, N_R represent the values of the spreading of fake and real information on a recent hot topic, respectively, $n_f(u), n_R(u)$ stand for the numbers of u users taking part in fake and real information spreading, respectively, and λ, η represent the fake and real information spreading coefficients. $n_e(u)$ is the number of friends of u, and p is the spreading probability of u, which can be estimated by the statistical data of the social media platform. Specifically, p is the ratio of the number of user u's friends who spread hot topic information to other friends to the total number of friends. Then, the spreading force of u can be calculated as follows:

$$F_s(u) = p \cdot fs(u) \cdot n_e(u). \tag{11}$$

Apparently, there are often malicious users on various platforms. The data related to recent fake information spreading times were employed to discover malicious users. By assuming that $m_v(u, t), m_r(u, t)$ represent the numbers of views of and replies to fake information in the time intervals t of user u, the malicious user evaluation function $\varphi(u)$ can be calculated as follows:

$$\varphi(u) = \alpha \sum_{t \in T} m_v(u, t) + \sum_{t \in T} \beta m_r(u, t) \tag{12}$$

where α, β are constant coefficients for viewing and relying on fake information, respectively.

4.2. Hybrid Fake Information Containing Method Based on Multiple Perspectives

In light of the given assumptions and the model provided in Section 4.1, a hybrid fake information-containing method has been presented here based on the fake information content, users' historical behavior data, and so on. The method can be divided into two sub-algorithms: potential fake information selection and fake content determining, and fake information user containment. The main goal of the first algorithm is to find the potential fake information by considering the hot topic and popular content, and selecting valuable and potentially interesting newly created topics and content on social media. The underlying reason for identifying the hot topic is that popular content is usually tainted with fake information seeking a wider spreading range and greater impact.

The proposed sub-method can be divided into the following steps, and the details can be checked in Algorithm 1. Firstly, Algorithm 1 initializes the parameters. Lines 2–11 were

incorporated to select the potential hot topic set $OHot$ by counting the user numbers of different topics O based on their first-order difference. Lines 12–22 were used to determine whether the hot topic includes fake information via a fake content comparison, and the fake degree of $OHot$ was calculated. Thirdly, the containing topic set (O_F) with a relatively high fake degree was selected by comparison with the threshold value. Finally, according to O_F, the fake tagging of the content was implemented. It is also known that the complexity of Algorithm 1 is $O(|OHot| \cdot \max(|\Delta(o_{hot})|) \cdot \max(|c(o_{hot})|))(o_{hot} \in OHot)$.

Algorithm 1. Potential fake information selection and fake content determination.

Input: O, S, U
Output: O_F, C_F
1: **Initialize** $OHot$, fd_0, O_F, C_F
2: **for** o = 1: [O] // selecting the potential topic having the fake information
// [•] is the total element number of •
3: **for** i = 1:[S]
4: $N_v^S(t,o) \leftarrow \sum_{i \in |S|} n_v^{s_i}(t,o), N_r^S(t,o) \leftarrow \sum_{i \in |S|} n_r^{s_i}(t,o)$
//getting the total replying and view number for topic o.
5: $N(t,o) \leftarrow N_v^S(t) + N_v^S(t)$ //collecting the total user for o.
6: $\Delta N(t,o) \leftarrow N(t,o) - N(t-1,o)$
//computing first-order difference of user numbers
7: **end for**
8: **if** $\Delta N(t,o) \geq N_0(t,o)$
9: $O_{Hot} \leftarrow O_{Hot} + o$
10: **end if**
11: **end for**
12: **for** o_{hot} = 1:[o_{hot}] //determine o_{hot} whether includes fake information
13: Collecting $C(o_{hot})$ and input $\Delta(o_{hot})$
14: **for** i = 1:[$\Delta(o_{hot})$]
15: **for** k = 1: [$\Delta(o_{hot})$]
16: Computing $\cos\theta(c_i, \Delta_k)$ using Equation (7)
17: **end for**
18: Update $\Delta(o_{hot})$
19: $fv(c_i) \leftarrow \mathrm{Max}(\cos\theta(c_i, \Delta_k))$
20: **end for**
21: Repeating steps 14–18 several times for getting reasonable $fv(c_i)$
22: $fd(t, o_{hot} \leftarrow \sum_{i \in |C|} fv(c_i)/[C]$ //computing fake degree of o_{hot}
23: **if** $fd(t, o_{hot}) \geq fd_0$ // Create the fake information topic set in time t
24: $O_F \leftarrow O_F + o_{hot}$
25: **if** $f_v(c_j) \geq fv_0$// // Create the fake content that needs to be controlled
26: $C_F(o_{hot}) \leftarrow C_F(o_{hot}) + c_j$
27: **end if**
28: **end if**
29: **end if**
30: fake information tagging of $C_F(o_f)(o_f \in O_F)$
31: **Return** O_F,C_F

The applied user controlling strategy is given in Algorithm 2 for containing the fake information. The presented sub-method can be described by the following steps; the details can be viewed in Algorithm 2. Firstly, the inputs O_F, C_F are derived from Algorithm 1, and the users' state values are initiated ($State(U_f(o_f))$), as is shown in Lines 1–2. Then, the rate of fake or real information spreading about a recent hot topic is collected. Secondly, according to the content of the topic, the normal $U_R(o_f)$, fake content users $U_f(o_f)$ are identified, as demonstrated in Lines 3–6. Additionally, the spreading coefficient and spreading force of the fake content user are computed by the above-mentioned equations, as described in Lines 8–9. Thirdly, according to the spreading force threshold value, the fake content users are

further divided into infection and susceptible users, and different user management functions are employed, as shown in Lines 11–17. Fourthly, the function $\varphi(u)$ is run to select the malicious users, responding to the relevant management method deployed in Lines 18–21. Finally, the user state value vector is updated and returned for the next usage in Lines 22–26. It is known that the complexity of Algorithm 2 is $O([O_F] \cdot \max(U(o_f)))(o_f \in O_F)$.

Algorithm 2. Fake information users controlling strategy.

Input: O_F, C_F
Output: $State(U_f(O_f))$
1: Initialize fs_0, $State(U_f(O_f)) = 1$
2: Count (N_f, N_R)
//collect the rate of fake or real information spreading of a recent hot topic
3: **for** o_f = 1:$[o_f]$
4: $C_R(O_f) \leftarrow C(O_f) - C_f(O_f)$ //collect real content of topic o_f.
5: $U_R(O_f) \leftarrow Map(C_R(O_f))$ //search the normal users
6: $U_f(O_f) \leftarrow U(o_f) - U_R(o_f)$ //find the fake content users
7: **for** u = 1:$U_f(O_f)$ //evaluate the fake content users
8: $f_s(u) \leftarrow fs_0 + \lambda n_f(u)/N_f - \eta n_r(u)/N_r$
//computing the spreading coefficient of user u
9: $F_s(u) \leftarrow fs(u) \cdot p \cdot fs(u) \cdot n_e(u)$
//computing the spreading force of user u
10: Compute $(m_v(u,t), m_r(u,t))$
//Compute () is a function for determign the numbers of viewing and replying to fake information of user u
11: **if** $F_s(u) \leq F_s(0)$
//Judge spreading force threshold value
12: Remind(u) //Remind () is a function to remind the infection users
13: $State(u)$ = 0 //change the state of user
14: **else**
15: Quarantine(u) // Quarantine () is a function to quarantine the susceptible users
16: $State(u) = -1$
17: **end if**
18: $\varphi(u) \leftarrow a \sum_{t \in T} m_v(u,t) + \sum_{t \in T} \beta m_r(u,t)$
// running the malicious user evaluation function
19: **if** $\varphi(u) \geq \varphi_0$
20: Delete(u) //delete malicious user
21: $State(u) = -2$
22: **end if**
23: **end for**
24: Update ($State(U_f(o_f))$) //Update the state value of user
25: **end for**
26: **Return** ($State(U_f(o_f))$

5. Experiment and Results

5.1. Experiment Setting

In this section, based on a BBS (Baidu Tieba—https://tieba.baidu.com/ (accessed on 1 January 2020)), a fake information dataset regarding three topics was created with 187,000 items of text for evaluating fake information detection. Then, the fake information was implemented on campus BBS to deliberately contain the fake information about course selection at a different time to evaluate the performance of the presented containing strategy.

First, our proposed method, called CCSP (potential fake information selection and fake content comparing), was compared with LSTM (long short-term memory), RNN-SVM [26], Text-CNN (Convolutional Neural Network) and Bi-LSTM [29] for evaluating the fake information detection performance by taking into account two metrics, namely, time and

accuracy. Then, our presented method CCUM (content containing and user management) was compared to a classical method of anti-rumor message sending (ARMS, such as [34]) and fake information user quarantine (FIUQ, such as [35]) by analyzing the performance of the metric spreading force and the proportion of false information. The main experiment settings are summarized in Table 1.

Table 1. Parameter configuration of the experiment.

Parameters	Value	Description
t	1 h	Time interval
$N_0(t,o)$	100	The hot topic threshold value
fs_0	10	The start value of spreading coefficient
λ, η	1	The fake or real information spreading coefficient
fd_0	0.4	The fake information hot topic judging threshold value
fv_0	0.6	The fake content threshold value
$F_s(0)$	200	The fake spreading force threshold value
φ_0	5	The malicious user evaluation threshold value
α, β	1, 0.3	The constant coefficient for viewing and relying to the fake information of malicious users

5.2. Results and Analysis

A. *Model training or creating time and fake information detection time*. Figure 2 shows the model training or creating time results of the different methods with the same training dataset. It is obvious that LSTM spends the most time finishing model training. Meanwhile, the textCNN and RNN-SVM methods exhibited better performances than the BiLSTM and LSTM approaches. On top of that, the proposed method CCSP spends less time creating a model. The deep learning models have convolution and pooling steps, which would eventually require more time. However, a simple content comparison method was employed in the proposed CCSP. It is interesting to note that CCSP can reduce the time requirements by about 45%, 20%, 8% and 5% compared with LSTM, BiLSTM, textCNN and RNN-SVM. In other words, the CCSP method performs best in terms of creating or training model time.

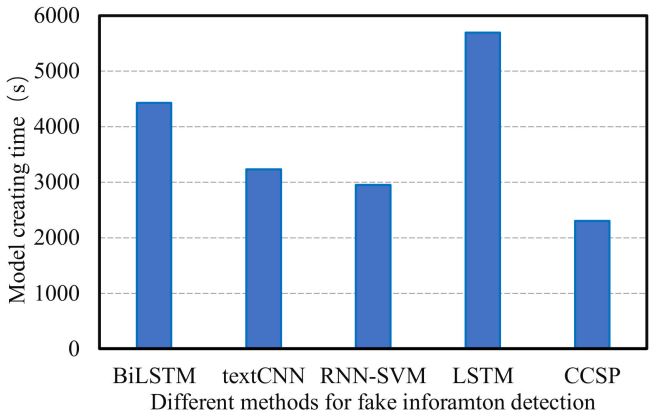

Figure 2. Model training or creating time.

Figure 3 displays the results related to total fake information detection time for 10,000 different texts. Obviously, the BiLSTM method requires the most detection time, as this model has a more complicated network structure. Meanwhile, the textCNN, LSTM, and RNN-SVM methods also waste much time. In the same way, during fake information detection, CCSP would not spend time on the convolution, pooling or other steps. Therefore, the proposed algorithm clearly outperforms others in the metric of fake information detection time.

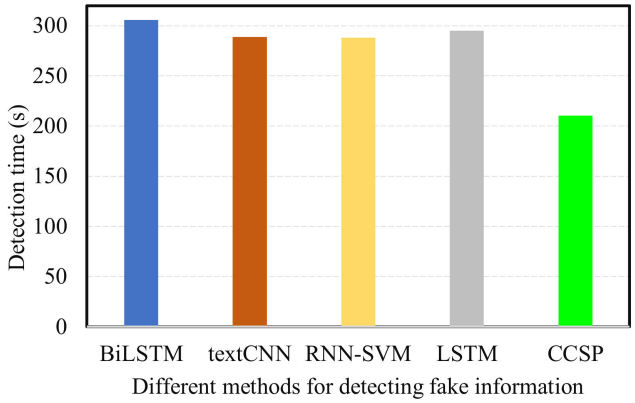

Figure 3. Fake information detection time.

B. *Fake information detection accuracy and spreading force.* Detection accuracy is regarded as a key index to evaluate the methods of fake content detection. Figure 4 contains the related results for three topics (S1, S2, S3). It is well-established that the BiLSTM method has the best detection accuracy, and the textCNN, RNN-SVM and LSTM techniques show relatively poor performance. As CCSP introduces a constantly updating comparative fake content dataset mechanism, it achieves similar performance in terms of accuracy compared to the BiLSTM method. When considering the time constraints, the CCSP method is suitable for controlling the spread of fake information in the context of real social media platform management.

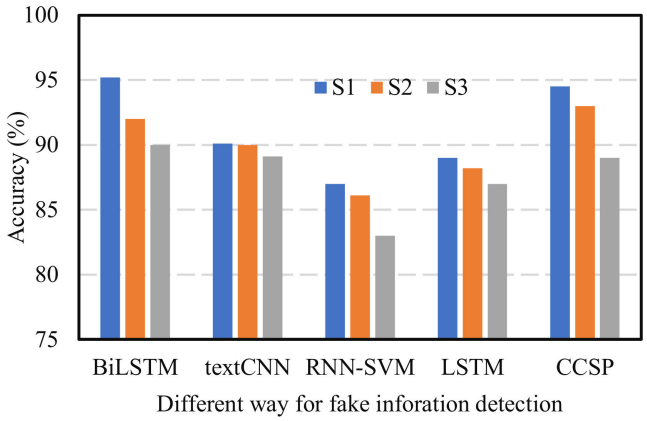

Figure 4. Fake information detection accuracy.

Figure 5 presents the extracted results on spreading force with different fake information containment strategies after five hours of implementation. It is quite clear that the proposed CCUM method ensures the lowest spreading force of fake content. The reason for this is that the CCUM method is a hybrid fake information controlling strategy, combing content tagging and user's management. Besides this, the FIUQ method still ensures a high spreading force as it only employs the quarantining of users, meaning normal users can still easily believe and spread fake content. Meanwhile, the ARMS method shows a better performance.

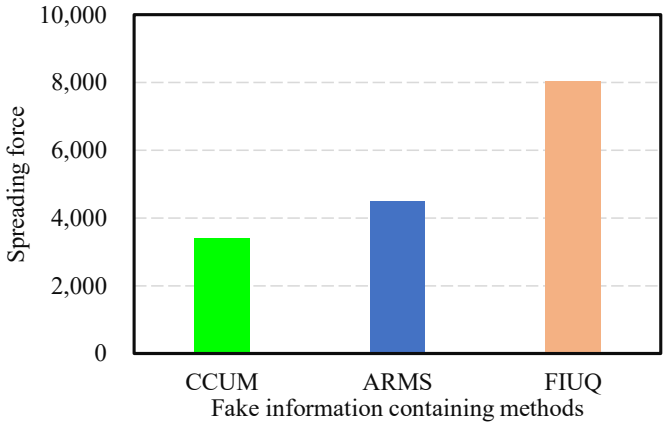

Figure 5. Spreading force of the different methods.

C. *Number of users and proportion of fake information*. In order to evaluate the algorithm objectively and comprehensively, the number of users and the proportion of fake information after the employment of different containing methods were assessed at different times, and the results are given in Figures 6 and 7. More specifically, Figure 6 shows that the user number would change with time. Obviously, with the CCUM method, the user number decreases with time. Additionally, the ARMS method shows the second-best performance in this metric. In other words, with this method, a lower number of users would discuss the fake content and related topics. Meanwhile, the FIUQ method exhibits the peak user number, as a single user-quarantining method could easily attract other users towards the topic.

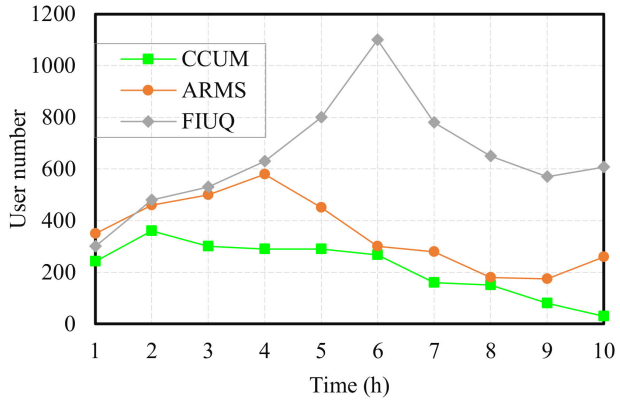

Figure 6. The number of users.

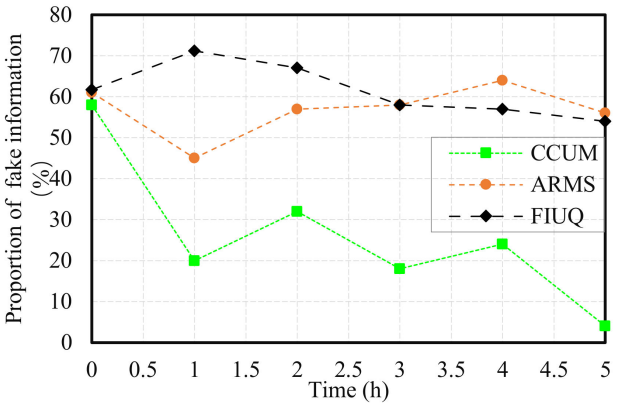

Figure 7. The proportion of fake information.

Figure 7 displays the changes in the fake information proportion under different methods with time. As a whole, the CCUM method ensures a reduction in fake information proportion. There is also a reduced change with both the ARMS and FIUQ methods. The reason for this effect is that a hybrid of fake information containing methods is used in CCUM. The CCUM approach not only tags the fake information, but also control users according to their behaviors.

6. Conclusions

Fake information has a great impact on social media users. However, the traditional schemes are facing many challenges related to real social media applications. Thus, in order to improve the performance of fake information containment, a study of this domain has been reported in this work, from the social media platform management perspective. Based on the implementation of multi-dimension historical data, a hybrid method has been presented that addresses fake content and social media users. According to real requirements, a potential fake information selection and fake content determination method has been constructed from the difference in user numbers and a content comparison. Then, a user management method has been proposed in light of user behaviors and division. The performance of the proposal has been evaluated through a real dataset and experiments with different metrics. The results demonstrate that the proposed method has the ability to contain fake information. In the future, the present methods should be applied to other datasets and platforms in order to evaluate the performance, and at the same time improve the related parameters, detect fake information and contain bot networks.

Author Contributions: H.C. conceived and wrote the manuscript; S.L. and Y.L. analyzed the data and performed the experiments; X.L. analyzed the experimental results. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Ministry of Education in China Liberal Arts and Social Sciences Foundation under Grant No.20YJCZH004, the College Students Innovation and Entrepreneurship Training Fund of the Guangzhou Higher Education Teaching Quality and Teaching Reform Project under Grant No. 2022CXCYJH017, and the undergraduate's Innovation Fund in 2022 of Zhongkai University of Agriculture and Engineering under Grant No. 2022CX19.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yang, H.; Wang, S.; Zheng, Y. Spatial-temporal variations and trends of Internet users: Assessment from global perspective. *Inf. Dev.* **2021**, 02666669211035479. [CrossRef]
2. Stilinovic, M.; Hutchinson, J. The Internet regulation turn? Policy, Internet and technology. *Policy Internet* **2022**, *14*, 6–12. [CrossRef]
3. Zhang, W.; Tian, Z.; Zhang, G.; Dong, G. Spatial-temporal characteristics of green travel behavior based on vector perspective. *J. Clean. Prod.* **2019**, *234*, 549–558. [CrossRef]
4. Batalla, J.M.; Krawiec, P.; Mavromoustakis, C.X.; Mastorakis, G.; Chilamkurti, N.; Negru, D.; Bruneau-Queyreix, J.; Borcoci, E. Efficient media streaming with collaborative terminals for the smart city environment. *IEEE Commun. Mag.* **2017**, *55*, 98–104. [CrossRef]
5. Kemp, S. Digital in 2018: World's Internet Users Pass the 4 Billion Mark. We Are Social. 2018. Available online: https://wearesocial.com/blog/2018/01/global-digital-report-2018 (accessed on 1 January 2020).
6. Sunhare, R.; Shaikh, Y. Study of security vulnerabilities in social networking websites. *Int. J. Manag. IT Eng.* **2019**, *9*, 278–291.
7. Lyu, H.; Chen, L.; Wang, Y.; Luo, J. Sense and sensibility: Characterizing social media users regarding the use of controversial terms for COVID-19. *IEEE Trans. Big Data* **2020**, *7*, 952–960. [CrossRef]
8. Dong, G.; Luo, Y.; Liu, Y.; Wang, F.; Qin, H.; Vilela, A.L. Percolation behaviors of a network of networks under intentional attack with limited information. *Chaos Solitons Fractals* **2022**, *159*, 112147. [CrossRef]
9. Dong, G.; Qing, T.; Du, R.; Wang, C.; Li, R.; Wang, M.; Tian, L.; Chen, L.; Vilela, A.L.; Stanley, H.E. Complex network approach for the structural optimization of global crude oil trade system. *J. Clean. Prod.* **2020**, *251*, 119366. [CrossRef]

10. Ridings, C.M.; Gefen, D. Virtual community attraction: Why people hang out online. *J. Comput. -Mediat. Commun.* **2004**, *10*, JCMC10110. [CrossRef]
11. Han, E.; Kim, K.K.; Lee, A.R. Contributors to exchange structures and their effects on community solidarity in online communities. *Internet Res.* **2019**, *299*, 1410–1442. [CrossRef]
12. Scheufele, D.A.; Krause, N.M. Science audiences, misinformation, and fake news. *Proc. Natl. Acad. Sci. USA* **2019**, *116*, 7662–7669. [CrossRef] [PubMed]
13. Posetti, J.; Matthews, A. A short guide to the history of 'fake news' and disinformation. *Int. Cent. J.* **2018**, *7*, 2018-07.
14. Zhang, X.; Ghorbani, A.A. An overview of online fake news: Characterization, detection, and discussion. *Inf. Processing Manag.* **2020**, *57*, 102025. [CrossRef]
15. Kanekar, A.S.; Thombre, A. Fake medical news: Avoiding pitfalls and perils. *Fam. Med. Community Health* **2019**, *7*, e000142. [CrossRef] [PubMed]
16. Oshikawa, R.; Qian, J.; Wang, W.Y. A survey on natural language processing for fake news detection. *arXiv* **2018**, arXiv:1811.00770.
17. De Oliveira, N.R.; Pisa, P.S.; Lopez, M.A.; de Medeiros, D.; Mattos, D. Identifying fake news on social networks based on natural language processing: Trends and challenges. *Information* **2021**, *12*, 38. [CrossRef]
18. Bodaghi, A.; Oliveira, J. The theater of fake news spreading, who plays which role? A study on real graphs of spreading on Twitter. *Expert Syst. Appl.* **2022**, *189*, 116110. [CrossRef]
19. 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]
20. Manzoor, S.I.; Singla, J. Fake news detection using machine learning approaches: A systematic review. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 230–234.
21. Pundir, V.; Devi, E.B.; Nath, V. Arresting fake news sharing on social media: A theory of planned behavior approach. *Manag. Res. Rev.* **2021**, *44*, 1108–1138. [CrossRef]
22. Figueira, Á.; Oliveira, L. The current state of fake news: Challenges and opportunities. *Procedia Comput. Sci.* **2017**, *121*, 817–825. [CrossRef]
23. Tolosana, R.; Vera-Rodriguez, R.; Fierrez, J.; Morales, A.; Ortega-Garcia, J. Deepfakes and beyond: A survey of face manipulation and fake detection. *Inf. Fusion* **2020**, *64*, 131–148. [CrossRef]
24. Kesarwani, A.; Chauhan, S.S.; Nair, A.R. Fake news detection on social media using k-nearest neighbor classifier. In Proceedings of the 2020 International Conference on Advances in Computing and Communication Engineering (ICACCE), Las Vegas, NV, USA, 22–24 June 2020; pp. 1–4.
25. Hussain, M.G.; Hasan, M.R.; Rahman, M.; Protim, J.; Hasan, S.A. Detection of bangla fake news using mnb and svm classifier. *arXiv* **2020**, arXiv:2005.14627.
26. Albahar, M. A hybrid model for fake news detection: Leveraging news content and user comments in fake news. *IET Inf. Secur.* **2021**, *15*, 169–177. [CrossRef]
27. Sahoo, S.R.; Gupta, B.B. Multiple features based approach for automatic fake news detection on social networks using deep learning. *Appl. Soft Comput.* **2021**, *100*, 106983. [CrossRef]
28. Nasir, J.A.; Khan, O.S.; Varlamis, I. Fake news detection: A hybrid CNN-RNN based deep learning approach. *Int. J. Inf. Manag. Data Insights* **2021**, *1*, 100007. [CrossRef]
29. Bhattacharya, P.; Patel, S.B.; Gupta, R.; Tanwar, S.; Rodrigues, J.J.P.C. SaTYa: Trusted Bi-LSTM-Based fake news classification scheme for smart community. *IEEE Trans. Comput. Soc. Syst.* **2021**, 1–10. [CrossRef]
30. Cao, J.; Guo, J.; Li, X.; Jin, Z.; Guo, H.; Li, J. Automatic rumor detection on microblogs: A survey. *arXiv* **2018**, arXiv:1807.03505.
31. Pan, C.; Yang, L.X.; Yang, X.; Wu, Y.; Tang, Y.Y. An effective rumor-containing strategy. *Phys. A Stat. Mech. Its Appl.* **2018**, *500*, 80–91. [CrossRef]
32. Zhao, J.; Yang, L.X.; Zhong, X.; Yang, X.; Wu, Y.; Tang, Y.Y. Minimizing the impact of a rumor via isolation and conversion. *Phys. A Stat. Mech. Its Appl.* **2019**, *526*, 120867. [CrossRef]
33. Bodaghi, A.; Goliaei, S.; Salehi, M. The number of followings as an influential factor in rumor spreading. *Appl. Math. Comput.* **2019**, *357*, 167–184. [CrossRef]
34. Askarizadeh, M.; Ladani, B.T. Soft rumor control in social networks: Modeling and analysis. *Eng. Appl. Artif. Intell.* **2021**, *100*, 104198. [CrossRef]
35. Liu, Z.; Qin, T.; Sun, Q.; Li, S.; Song, H.H.; Chen, Z. SIRQU: Dynamic Quarantine Defense Model for Online Rumor Propagation Control. *IEEE Trans. Comput. Soc. Syst.* **2022**, 1–12. [CrossRef]
36. Roets, A. 'Fake news': Incorrect, but hard to correct. The role of cognitive ability on the impact of false information on social impressions. *Intelligence* **2017**, *65*, 107–110.