Detection of E-commerce Fake Reviews Using Core Diagram and Metric Weight Measurement Algorithms

Junsheng Song[1*], Chunyan Wu[2], Juan Li[3]
[1]Security Office, Shandong Labor Vocational and Technical CollegeJi'nan, 250022, China
[2]Department of Senior Technician, Shandong Labor Vocational and Technical College, Ji'nan, 250022, China
[3]Continuing Education Center, Shandong Labor Vocational and Technical College, Ji'nan, 250022, China
E-mail: sjs091240@163.com, yanzi691177@126.com, liyajing828@163.com
[*]Corresponding author

Keywords: legal perspective, fake review groups, core diagram, metric weight measurement, label propagation

Received: November 19, 2024

In today's digital age, e-commerce platforms have become an essential part of daily life. However, the convenience and openness of online shopping has also led to numerous legal and ethical issues. Dishonest merchants, in pursuit of higher profits, often hire fake reviewers to post misleading comments, undermining consumer trust and violating trade laws. Therefore, in response to the detection of such fraudulent activities in the e-commerce environment, this study proposes a method that uses core diagrams and metric weight measurements to identify fake reviews. By evaluating the relevance of users based on rating levels and temporal correlation, a user relationship graph was constructed, which served as the basis for the detection algorithm. The method improved the accuracy of fake review detection by employing a multi-label propagation strategy and integrating an algorithm that combined entropy and analytic hierarchy process methods for metric weight measurement. The experimental setup was conducted on four real-world datasets—Amazon, YelpChi, YelpNYC, and YelpZip. The results showed that the proposed method achieved an average accuracy of 0.88, a precision of 0.88, a recall rate of 0.85, and an F1 score of 0.87 on the Amazon dataset, significantly outperforming other methods. These findings highlight the applicability and reliability of the model proposed in this study in the field of e-commerce fake review detection, providing a strong solution to protect consumer interests and maintain fair competition in the online market.

Povzetek: Razvita je metoda za zaznavanje lažnih ocen v e-trgovini, ki uporablja jedrne diagrame in algoritme merjenja uteži metrik. Z ocenjevanjem relevantnosti uporabnikov na podlagi ocen in časovne korelacije je bil zgrajen graf uporabniških odnosov. Metoda izboljšuje zaznavanje lažnih ocen z uporabo strategije propagacije z več oznakami in algoritma, ki združuje metode entropije in analitičnega hierarhičnega procesa za merjenje uteži metrik.

1 Introduction

With its characteristics of convenience, speed, and affordability, online shopping is gradually becoming the mainstream of mass consumption. With the proliferation of online shopping platforms, the content of reviews is growing at an astonishing rate, making it difficult for users to distinguish between real and fake reviews. In addition, the virtual and open nature of the Internet has led to numerous legal issues in online shopping [1]. Many unscrupulous merchants, driven by profit motives, engage in the dissemination of false evaluations online to promote their own products or denigrate competitors. In particular, fake reviews refer to the hiring of fake accounts to publish deceptive comments by certain enterprises, aiming to promote their own products or discredit those of competitors [2]. As review information is a crucial basis for consumer purchasing decisions, erroneous decisions can impact the legitimate interests of consumers. Allowing such behavior to proliferate would seriously harm consumer interests and jeopardize internet security [3]. As mentioned by Lecue F in his study, the existing methods are deficient in feature extraction and evaluation index weight assignment [4]. At the same time, they are also deficient in effectively identifying target users, which may lead to unsatisfactory recognition results. For example, Ji S. et al. pointed out in their study that existing methods such as support vector machines (SVM), random forests (RF), and convolutional neural networks (CNN) still had limitations in recognizing user behavior patterns [5]. These problems ultimately lead to unsatisfactory detection results. To further optimize the effectiveness of e-commerce fake review detection, this study proposes a method based on core diagram (CD) and metric weight measurement. The innovations of this research include following points. (1) Proposing a label propagation algorithm for fake review group detection based on CD.

(2) Addressing the disparity in the importance of various metrics in fake review group detection by introducing a metric weight measurement algorithm that integrates entropy method (EM) and analytic hierarchy process (AHP). This study is divided into four sections. (1) Literature review, which reviews the current status of CDs and existing fake review detection technologies. (2) Research methodology, which provides a detailed discussion of the core technologies in this study. (3) Experimental verification, which conducts simulation experiments on the proposed method. (4) Conclusion, which summarizes and provides future prospects for the entire research.

2 Related work

CD is a graph model composed of user relationships. Research on graph models has attracted attention from scholars across various fields. Berahmand K and colleagues proposed a novel CD algorithm and applied it to simulate the spread of popular epidemics. This algorithm had advantages such as linear temporal ordering, local information utilization, and independence from any parameters, making it one of the most popular community detection algorithms in recent years [6]. On a legal level, such algorithms can help identify groups of fake reviewers, provide evidence for legal proceedings. It can enhance the regulatory capacity of e-commerce platforms, and protect consumer rights. Compared to other advanced attribute graph clustering methods, this approach is more efficient and accurate. Graham S et al., building on the CD method, introduced a knowledge graph embedding model applied to detecting anomalous transactions in the trade of cultural artifacts. The study employed semantic annotation tools to construct a CD model related to cultural artifact trade. Through supervised machine learning, they transformed CD into a knowledge graph embedding model, demonstrating significant potential in uncovering concealed aspects of illegal cultural artifact trade [7]. Wang Y et al. proposed an indoor positioning system based on an adaptive robust factor CD model, suitable for smartphone indoor positioning. This method, grounded in CD, integrated Wi-Fi and PDR location information, effectively addressing issues such as low network update frequency, Wi-Fi coarse errors, and PDR error accumulation. It achieved precise positioning for multiple unknown points indoors [8]. Zhong Y et al. presented a CD partitioning algorithm based on heterogeneous perception. This method considered differences in network bandwidth, computing node capabilities, and resource competition among kernels in high-speed networks. Compared to existing methods, the proposed algorithm demonstrated improvements in distributed and heterogeneous clustering. Experimental results confirmed its effectiveness in addressing graph node allocation issues in distributed and heterogeneous clustering [9]. Feng L et al., approaching from the perspective of service trade, constructed a service trade network based on the CD model and complex network theory. This model proved useful for analyzing the openness of national service trade, urbanization rates, and mutual influencing factors [10].

The rapid development of e-commerce platforms has intensified competition among merchants, leading to a proliferation of fake reviews. Therefore, scholars from various fields have shown interest in methods for detecting fake reviews. Cheng J et al. proposed a semi-supervised generative adversarial network with an integrated attention mechanism for fake review detection. This model, incorporating an attention mechanism, exhibited ample semantic expressive capability and relied on a small number of labeled samples for detecting fake reviews. Experimental results indicated that when the number of labeled samples is limited, this method outperformed currently popular semi-supervised pseudo-review detection methods [11]. Bathla G et al. proposed a fake review detection method that combines CNN and LSTM networks, considering existing methods to be time-consuming and inefficient. This method effectively extracted user features from comments and utilizes user sentiment information for fake review identification. Experimental results demonstrated the superior performance of this method in handling complex computations [12]. Alsubari S et al. developed a fake review detection system based on n-grams and reviewer sentiment scores for more accurate detection of fake reviews. This method input n-grams of comment text into the constructed model, automatically identified user comments, and assessed their authenticity. Simulation experiments validated the superiority of the proposed method in terms of accuracy [13]. Vidanagama D et al. compiled prominent techniques proposed to address the fake review detection problem, aiming to provide a theoretical basis for subsequent fake review detection by analyzing existing methods in depth, clarifying their characteristics, advantages, and limitations [14]. Mutemi A et al. addressed the lack of research on fraud detection in e-commerce by conducting a systematic review and meta-analysis of preferred reporting items for research. By exploring the effectiveness of machine learning and data mining techniques for fraud detection in digital marketplaces and broader e-commerce environments, research opportunities were identified, providing industry stakeholders with insights into key technologies and trends [15].

In summary, the existing methods for detecting fake reviews are based on the CD model and have achieved good results. These studies provide different technical means to identify and combat fake review behavior in a legal context, thus protecting consumers from fraud and misinformation and maintaining a level playing field in the e-commerce marketplace. This is important for effective regulation by regulators with limited resources, and provides technical support for identifying and proving fraudulent behavior in legal proceedings. However, existing studies have neglected the impact of fake review behavior on consumer rights and the competitive environment of the market, as well as how to effectively regulate and combat it through legal means. In addition, existing techniques do not take into account the different importance of evaluation indicators when identifying fake review groups, resulting in inaccurate and inefficient detection results. Therefore, this study aims to improve the effectiveness of fake review detection in e-commerce by proposing a method based on CD and metric weight measurement. A comparative summary of existing methods is shown in Table 1.

Table 1: Comparative analysis of existing methods

References	Methodology	Data sets	Inadequacies
Berahmand K et al [6]	CD	Epidemiological data	No consideration of comment content and user behavioural pattern analysis, limited applicability to the legal context
Graham S et al [7]	CD-based knowledge graph embedding model	Cultural artwork transaction data	Lack of in-depth research on anomalous transaction detection in a legal context
Wang Y et al [8]	Adaptive robust factor CD model	Smartphone data	High computational complexity
Zhong Y et al [9]	CD segmentation algorithm for heterogeneous sensing	High-speed network data	High computational complexity
Feng L et al[10]	CD modelling and complex network approach	One Belt One Road data	High computational complexity
Cheng J et al [11]	Semi-supervised generative adversarial networks	E-commerce review data	Dependent on a small number of labelled samples with limited generalisation ability
Bathla G et al [12]	A combination of CNN and LSTM networks	E-commerce review data	High computational complexity, low efficiency, difficult to cope with large-scale data sets
Alsubari S et al [13]	Based on n-gram and sentiment scores	E-commerce review data	Large errors in the detection of fake comments
This study	Detection of false e-commerce reviews based on CD and indicator weight metrics	Four labelled real datasets	-

3 E-commerce fake review detection model based on CD and metric weight measurement

To enhance fake review detection in e-commerce, this study proposes a CD-based label propagation algorithm for fake review group detection. Initially, the study constructs a CD-based label propagation fake review detection method. Subsequently, entropy weighting and AHP are introduced to measure the weights of various indicators of fake reviews.

3.1 CD-based label propagation algorithm for detecting fake review groups

Customer reviews on e-commerce platforms have a significant impact on consumer behavior. However, misleading reviews due to language bias can result in merchants making undue profits, violating commercial laws such as the Anti-Unfair Competition Law and the Consumer Rights Protection Law, and infringing on consumers' rights [16]. These laws clearly stipulate the principle of good faith in commercial activities and the basic rights of consumers, including the right to know and the right to choose. By providing false or misleading information, misleading reviews undermine the fair competitive environment in the market and harm the legitimate rights and interests of consumers, and therefore must be regulated and combated by legal means. The effective identification of false comments on the Internet is an urgent problem that demands resolution.

Despite the fact that a considerable number of studies have been dedicated to the identification of fake comment groups, extant methods include semi-supervised generative adversarial networks by Cheng J et al., Bathla

G et al.'s method combining CNN and LSTM, and Alsubari S et al.'s system based on n-grams and sentiment scores. These methods face efficiency bottlenecks when dealing with large datasets, complex computations, and distinguishing between similar fake comments, and have limited application in legal contexts because they fail to deeply analyze the content of comments and user behavior patterns [17]. Therefore, this study proposes a CD-based algorithm for detecting clusters of label-propagating fake comments. The method analyzes the ratings of users in fake review clusters for their characteristics, including abnormal consistency of ratings, temporal concentration, similarity of language patterns, and abnormal user behavior. Based on the analysis, the algorithm establishes a user relationship graph by examining the closeness between users through rating levels and temporal correlations. Subsequently, utilizing CD as a foundation and employing a multi-label propagation approach, the algorithm groups users in the graph, yielding candidate groups [18]. Finally, the algorithm uses multiple fake review group detection indicators to classify and identify fake review groups within these candidates. The research examines user relationships from two perspectives: similarity in review content and similarity in user behavior. The closer the relationship between two reviewers, the more likely they are to belong to the same fake review group [19]. The formula for calculating the correlation between a user's product rating and review time is presented in Equation (1).

$$tn(a,b,m)=\begin{cases}0, & \left|S_a^m-S_b^m\right|\geq 2\vee\left|t_a^m-t_b^m\right|>\tau\\ 0.5\times\left(1-\dfrac{\left|S_a^m-S_b^m\right|}{2}\right) & \\ +0.5\times\left(1-\dfrac{\left|t_a^m-t_b^m\right|}{\tau}\right), & otherwise\end{cases}\qquad(1)$$

In Equation (1), S_a^m, S_b^m represent the ratings given by reviewers a,b for product m, while t_a^m, t_b^m) represent the review times of reviewers a,b for product m. The formula for calculating the closeness between reviewers is defined in Equation (2).

$$tns(a,b)=\frac{\left|P_a\cap P_b\right|}{\left|P_a\cup P_b\right|}\times\sum\nolimits_{m\in P_a\cap P_b}tn(a,b,m)\,(2)$$

In Equation (2), P_a represents the product reviewed by reviewer a, P_b represents the product reviewed by reviewer b, and $tn(a,b,m)$ represents the correlation between a user's product rating and review time. $tns(a,b)$ is mapped to the range $[0,1]$, as shown in Equation (3).

$$W(a,b)=\frac{2}{1+e^{-tns(a,b)}}-1\qquad(3)$$

In Equation (3), the correlation quantifies the extent to which two users share the same product review in the overall review. A higher percentage of reviewer a,b's sharing of the same product review implies that the two users are more correlated in their review behavior [20]. Given the high uncertainty in the label propagation process, the study, based on the CD method, assigns the same label to nodes within the same CD. Nodes not belonging to any of these cores are assigned an independent label. In graph theory, every weighted graph has a global density, and this study assumes that when the closeness of two nodes exceeds the graph's density, these nodes are considered to be on the same CD. The graph density is defined as shown in Equation (4).

$$\rho(WG)=\frac{\sum\nolimits_{x,y\in V}W_{xy}}{|E|}\qquad(4)$$

In Equation (4), WG represents the user relationship graph, which can reflect the average weight of the edges in the graph. Therefore, it can provide the algorithm with a measure of the closeness of the relationship between the nodes in the graph. V represents all nodes in the graph, and E represents all edges. W_{xy} represents the weight between nodes x and y. Therefore, the operation process of the CD algorithm is shown in Figure 1.

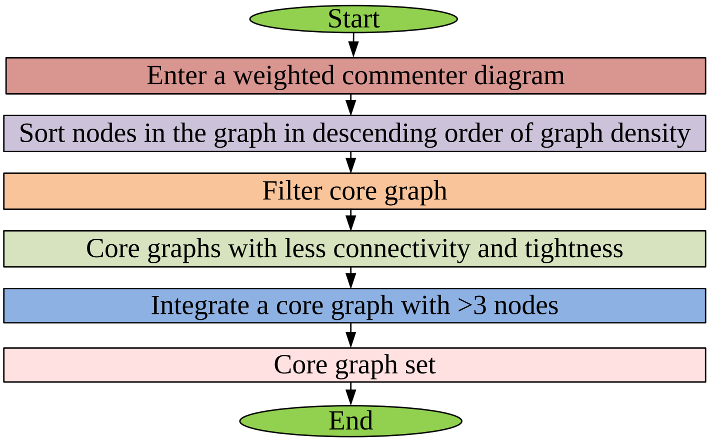

Start
Enter a weighted commenter diagram
Sort nodes in the graph in descending order of graph density
Filter core graph
Core graphs with less connectivity and tightness
Integrate a core graph with >3 nodes
Core graph set
End

Figure 1: Operation process of CD algorithm

During label propagation, the strength of communication between nodes can be measured using the weights of the edges in the user-associated graph. For propagation, the connectivity between nodes is more important than propagation strength. Therefore, this study introduces $anklevalue$ automatic label filtering to mitigate the impact of propagation strength [21-22]. $anklevalue$ can identify points of sharp change in a sequence of numbers and filter them. It is assumed that the label ownership degree sequence is $\left(d_1,\ldots,d_i,\ldots,d_n\right)$, define two lines as le_1,le_2. Connect d_1 to d_i and d_n. Among them, d_i denotes the label ownership degree of the i th node. Label ownership degree is the likelihood or confidence that a node is assigned to a particular label. $anklevalue$ can be represented as the maximum angle between the two lines, as shown in Equation (5).

$$\tan\theta = \left(\left|k_1 - k_2\right|\right) / \left(1 + k_1 \times k_2\right) \tag{5}$$

In Equation (5), k_1,k_2 represent the slopes of le_1,le_2, and their calculation formulas are given by Equation (6).

$$\begin{cases} k_1 = \left(d_i - d_1\right) / \left(i-1\right) \\ k_2 = \left(d_n - d_i\right) / \left(n-i\right) \end{cases} \tag{6}$$

Substituting Equation (6) into Equation (5) yields the expression shown in Equation (7).

$$\theta = \arctan\frac{\left|\left(d_i - d_1\right)\left(n-i\right) - \left(d_n - d_i\right)\left(i-1\right)\right|}{\left(i-1\right)\left(n-i\right) + \left(d_i - d_1\right)\left(d_n - d_i\right)} \tag{7}$$

Based on the above description, this study does not unconditionally accept labels from surrounding nodes in node propagation. Instead, it uses propagation strength to propagate more accurately. Additionally, $anklevalue$ is used to automatically filter node labels during label filtering, avoiding the direct setting of filtering thresholds to prevent inappropriate threshold settings from affecting propagation results. The candidate group identification algorithm constructed in this study mainly consists of two parts. The first step is to initialize node labels: use the CD algorithm to initialize nodes and set nodes with close relationships to the same label. The second step is the judgment of candidate fake comment groups: based on the initial labels, iterate over the labels of each node, and finally obtain the label sets to which each node belongs. Labels with the same mark are considered a group, and users belonging to a single label are removed, as the goal is to identify groups. The core diagram-tag propagation false comment group detection algorithm (CD-TPFGD) process is shown in Figure 2.

3.2 Fusion of CD and metric weight measurement in CD-TPFGD

After obtaining a set of fake reviews, the task is to identify true fake review groups from the candidate set. True fake review groups refer to those groups of fake review publishers that actually exist and are organized to manipulate online reviews of a product or service by posting false reviews for the purpose of unfair competition. These groups typically share some common characteristics, such as similarity in review content, concentration of posting times, and unusual consistency in ratings. This study utilizes the Fake Review Group Index to rank the suspicion level of candidate groups, with higher-ranking groups being more likely to be fake [23]. Numerous scholars have developed various detection methods for fake reviews in existing research [24]. In this study, specific evaluation metrics, as shown in Figure 3, are selected based on the characteristics of fake review groups and the proposed model.

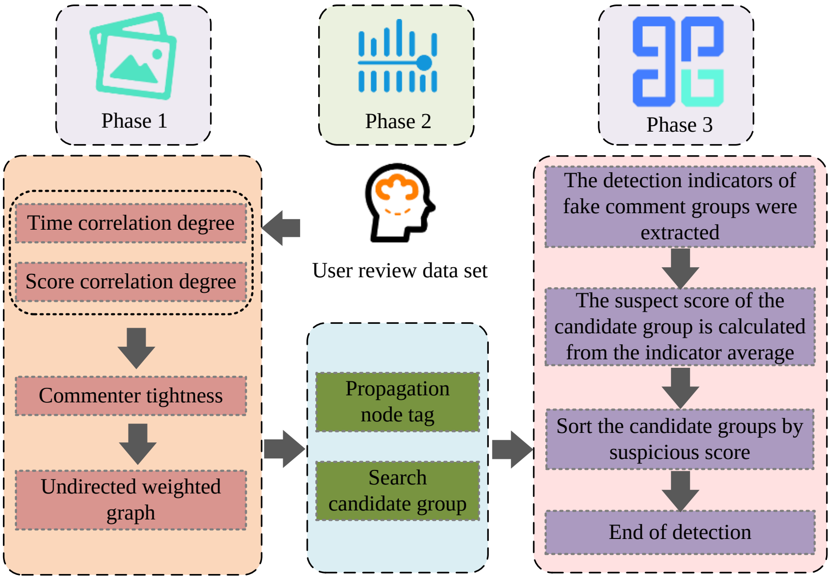
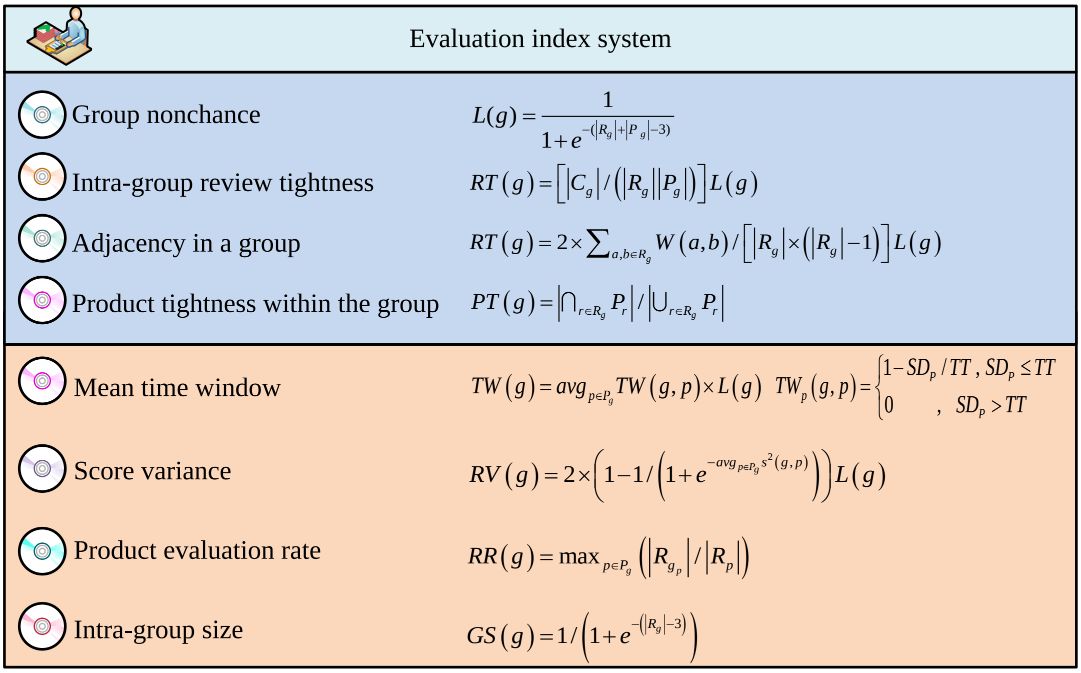

Phase 1
Phase 2
Phase 3
User review data set
Time correlation degree
Score correlation degree
Commenter tightness
Undirected weighted graph
Propagation node tag
Search candidate group
The detection indicators of fake comment groups were extracted
The suspect score of the candidate group is calculated from the indicator average
Sort the candidate groups by suspicious score
End of detection

Figure 2: CD-TPFGD test flow



Evaluation index system	
Group nonchance	$L(g)=\frac{1}{1+e^{-(\lvert R_g\rvert+\lvert P_g\rvert-3)}}$
Intra-group review tightness	$RT(g)=\left[\lvert C_g\rvert/\left(\lvert R_g\rvert\lvert P_g\rvert\right)\right]L(g)$
Adjacency in a group	$RT(g)=2\times\sum_{a,b\in R_g}W(a,b)/\left[\lvert R_g\rvert\times\left(\lvert R_g\rvert-1\right)\right]L(g)$
Product tightness within the group	$PT(g)=\left\lvert\bigcap_{r\in R_g}P_r\right\rvert/\left\lvert\bigcup_{r\in R_g}P_r\right\rvert$
Mean time window	$TW(g)=avg_{p\in P_g}TW(g,p)\times L(g)\quad TW_p(g,p)=\begin{cases}1-SD_p/TT\,, & SD_p\le TT\\ 0\,, & SD_p>TT\end{cases}$
Score variance	$RV(g)=2\times\left(1-1/\left(1+e^{-avg_{p\in P_g}s^2(g,p)}\right)\right)L(g)$
Product evaluation rate	$RR(g)=\max_{p\in P_g}\left(\lvert R_{g_p}\rvert/\lvert R_p\rvert\right)$
Intra-group size	$GS(g)=1/\left(1+e^{-(\lvert R_g\rvert-3)}\right)$

Figure 3: Evaluation index system of fake reviews

All the metrics presented in Figure 3 are derived from the features of fake review groups. Among them, $L(g)$ denotes group non-contingency. $RT(g)$ denotes intra-group comment closeness. $NT(g)$ denotes intra-group neighbour closeness. $PT(g)$ denotes the product closeness within the group. $TW(g)$ denotes the mean time window. $RV(g)$ denotes the rating variance. $RR(g)$ denotes the product being rated rate. $GS(g)$ denotes the group size. R_g denotes a reviewer in cluster g. P_g denotes a reviewed product in cluster g. C_g denotes all reviews by reviewers in the cluster for the product in the group. P_r denotes a reviewer r reviewing the product. SD_p denotes the standard deviation in time of the reviews by reviewers in cluster g for the product p. TT denotes 30 d. $TW(g,p)$ denotes a time window for a single product. $S^2(g,p)$ denotes the variance of the ratings by reviewers in cluster g for the product p. R_p denotes the variance of the ratings by all reviewers in the dataset for the product p. R_{g_p} denotes all reviewers in cluster g who reviewed product p.

For a fake review group, it constitutes an organized and planned entity with a common purpose. Therefore, compared to general groups, there is greater cohesion among group members, similarity in the content of reviews, and similarity in the products being reviewed. This research considers seven indicators to calculate the final suspicion degree *GSD* of a group, as shown in Equation (8).

$$GSD = \left(RT(g)+NT(g)+PT(g)+TW(g)+RV(g)+RR(g)+GS(g)\right)/7 \quad (8)$$

Equation (8) represents the average of the seven detection indicators. Considering these seven features collectively, groups with higher values are considered more likely to be fake review groups. In previous studies, when detecting multiple fake review groups, researchers often use the mean value as the final suspicion level of the group without considering the differing importance of each indicator, which can affect the overall accuracy of the detection [25]. To better measure the weights of each indicator, this study proposes a metric weight measurement algorithm based on EM and AHP. EM is an objective weighting method based on information entropy, which evaluates the effectiveness of indicators by calculating the entropy value of each indicator. The higher the information entropy, the greater the information entropy of the indicator, the richer the amount of information it carries, and the greater the impact on decision-making. Therefore, the EM method can objectively reflect the importance of each indicator in detecting misjudgment. AHP is a subjective weighting method based on expert judgment, which determines the relative weight of each indicator by constructing a judgment matrix and calculating the consistency ratio. The AHP method can synthesize the subjective judgment of experts to complement the EM method, ensuring that both objectivity and subjectivity are taken into account when determining the weights. Based on EM and AHP, it can effectively combine objective data and experts' experience to improve the accuracy and reliability of misjudgment detection. In AHP, subjective judgment refers to an expert's assessment of the relative importance between indicators based on his or her understanding of the domain and the data. This judgment is subjective because it relies on the expert's experience and intuition. However, by using the EM results as a starting point, this subjective bias can be reduced because the EM results provide an objective basis based on data. It is assumed that there are n candidate fake review groups, each with (M) fake review group indicators. The normalization process for the indicators is represented as Equation (9).

$$z_{ij} = \frac{x_{ij} - \min\left(x_j\right)}{\max\left(x_j\right) - \min\left(x_j\right)} \quad (9)$$

In Equation (9), x_{ij} represents the value of the j-th indicator for the i-th group. x_j represents the score set of the j-th indicator across all groups. z_{ij} represents the normalized value of x_{ij}. These values are the basis for calculating the entropy values, which reflect the distribution of each indicator in the different pseudo rating groups. Normalization produces a dimensionless value that more intuitively reflects the importance of the indicator in the different dummy rating groups. The weight calculation for the j-th indicator under the i-th group is computed as shown in Equation (10).

$$r_{ij} = z_{ij} / \sum\nolimits_{i=1}^{n} z_{ij} \quad (10)$$

In Equation (10), n represents the total number of candidate dummy assessment groups. The entropy calculation Equation for the j-th indicator is shown in Equation (11).

$$en_j = \left(-\sum\nolimits_{i=1}^{n} r_{ij} \ln r_{ij}\right) / \ln n \quad (11)$$

The entropy value is calculated to measure the uniformity of the distribution of the values of each indicator. A larger entropy value indicates a more uniform distribution of the group's values on the indicator, and a smaller amount of information. Conversely, a smaller entropy value indicates a more concentrated distribution and a larger amount of information. The entropy weight calculation Equation for each indicator is presented in Equation (12).

$$ws_j = \left(1 - en_j\right) / \sum\nolimits_{j=1}^{s} \left(1 - en_j\right) \quad (12)$$

The result of Equation (12) does not represent the final measurement of the importance of indicators. Rather, it serves as a preliminary calculation of the importance of each indicator. This calculation provides an objective basis for establishing the consistency matrix of the AHP. The information entropy weights obtained from the entropy weight method are then employed to facilitate a comparative analysis of various evaluation indicators. The weights are calculated to measure the informativeness of each indicator, i.e. the more informative the indicator, the lower its entropy value and the higher the corresponding weight. According to this study, indices with higher entropy weights are considered more important. Based on the comparative results, a consistency matrix is constructed, as shown in Equation (13).

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{bmatrix} \quad (13)$$

In Equation (13), A represents the judgment matrix, and a_{ij} represents the result of comparing the importance of indicator i with indicator j. The construction of matrix A is based on the subjective assessment of the relative importance of the indicators by the experts. By constructing the judgment matrix, the weights of the indicators can be calculated, which in turn assesses their relative contribution to the detection of misclassifications. In addition, the judgment matrix is used for consistency testing to ensure that the experts' judgments are consistent, thereby improving the reliability of the weight calculation. After constructing the judgment matrix, it is necessary to test whether the matrix is a consistency matrix. The consistency test coefficient is represented as shown in Equation (14).

$$CR = CI / RI \tag{14}$$

In Equation (14), CI represents the consistency index, and RI represents the random consistency index. CI is a measure of the consistency of the judgment matrix. It is calculated based on the difference between the largest eigenvalue of the judgment matrix and the size of the matrix, then divided by the size of the matrix minus one. The smaller the value of CI, the better the consistency of the judgment matrix, i.e., the more consistent the judgments of the experts are. RI is based on the average consistency index of a large number of randomly generated judgment matrices. The value of RI depends on the size of the judgment matrix. If $CR < 0.1$, it indicates that the matrix meets the standard. Otherwise, the judgment matrix needs to be reconstructed. The calculation Equation for group suspiciousness is shown in Equation (15).

$$sd_i = \sum_{j=1}^{s} x_{ij} B_j \tag{15}$$

In Equation (15), B_j represents the weight of the j th indicator. In the misperception test, different metrics have different weights. By multiplying the value of each metric by its weight, the contribution of each metric to the group suspicion can be determined. These contributions are added together to produce a composite measure, the group suspicion level, which reflects the overall performance of the group on all relevant indicators. This approach ensures that the more important metrics are given greater weight in the final assessment of the level of suspicion, thereby improving the accuracy and effectiveness of misclassification detection. In this study, the importance of indicators is first calculated using the EM. Then, based on this calculation, the weight vector is determined using the AHP. By integrating the EM and AHP, this research ultimately obtains the proportion of weights for each indicator. This method effectively addresses the objectivity issues of EM and the subjectivity issues of AHP. In summary, this study constructs a weighted user association graph, based on which the target group's candidate groups are identified using the label propagation algorithm. Subsequently, the entropy method-analytic hierarchy process (EM-AHP) algorithm is employed to measure the indicators and obtain a sorted list of groups. This results in the final algorithm for detecting fake review groups (CD-TPFGD-EM-AHP), and the system framework is illustrated in Figure 4.

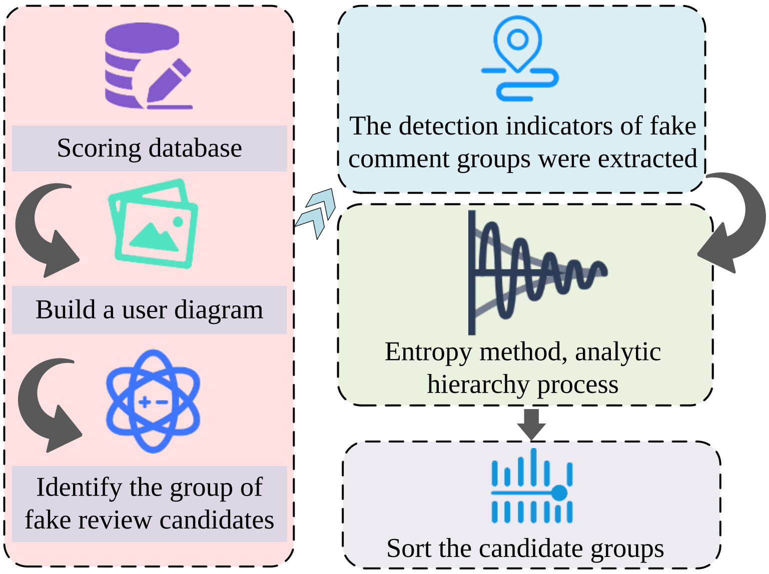

Scoring database
Build a user diagram
Identify the group of fake review candidates
The detection indicators of fake comment groups were extracted
Entropy method, analytic hierarchy process
Sort the candidate groups

Figure 4: System framework of CD-TPFGD-EM-AHP

According to the process shown in Figure 4, CD-TPFGD-EM-AHP is able to demonstrate a clear superiority in terms of accuracy of false rating detection as well as running time. The method first constructs a user relationship graph, determines the similarity between users by analyzing their rating data and timestamps, and establishes links accordingly. Next, the user relationship graph is processed by applying the CD algorithm to identify a core group of users, which are grouped by iterative label propagation and community structure analysis. Then, EM-AHP is used to measure the weights of different indicators, where EM is used to objectively evaluate the information content of the indicators, and AHP adjusts the weights by combining the subjective judgment of experts. Finally, these weighted indicators are combined to calculate the suspicion level of each user group, and based on the suspicion level ranking, the user groups most likely to be fake review groups are identified.

This process improves the accuracy and efficiency of fake review detection, providing e-commerce platforms with more effective tools to identify fake reviews.

4 Performance validation of fake review detection method based on CD-TPFGD-EM-AHP

The experiment initially delves into the discussion of parameters influencing CD-TPFGD-EM-AHP and compares the operational performance of CD-TPFGD-EM-AHP with CD-TPFGD. Subsequently, to better highlight the superior performance of CD-TPFGD-EM-AHP, the experiment introduces two other algorithms of the same type for comparative validation.

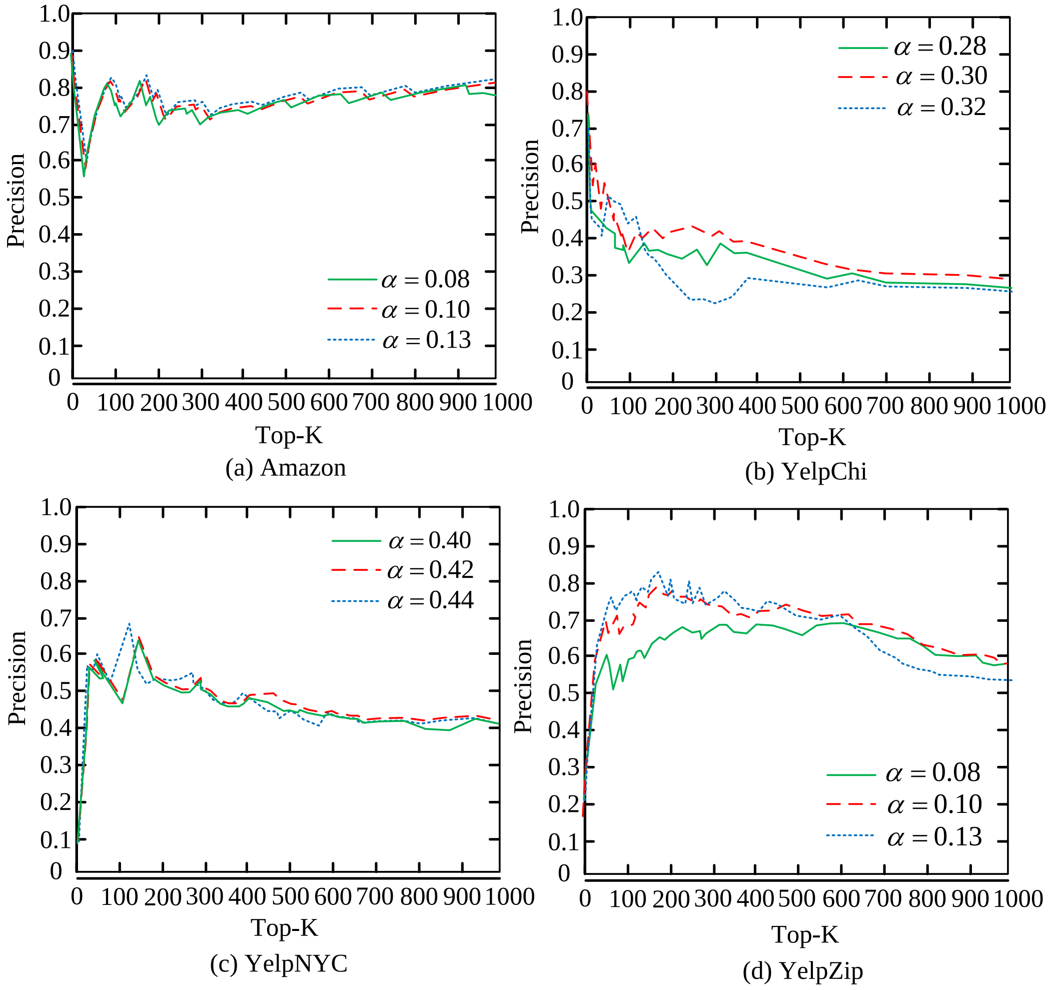
4.1 Impact of experimental parameters on the performance of CD-TPFGD-EM-AHP

To evaluate the algorithm proposed in this study, four labeled real-world datasets are used as experimental data-one from Amazon and three from Yelp. Amazon and Yelp are both well-known online shopping and review platforms where user reviews have a significant impact on consumers' purchase decisions. These datasets are well suited to illustrate the prevalence and complexity of the problem of fake reviews in the e-commerce domain. Furthermore, the selection of datasets from diverse platforms can enhance the generalizability of the experimental results. Amazon's primary focus is on merchandising, whereas Yelp specializes in local service reviews. This diversity in the datasets facilitates the evaluation of the algorithm's applicability in various scenarios. False online reviews not only violate business ethics, but also a variety of legal requirements, such as anti-unfair competition and consumer protection laws. The review content and rating behavior in these datasets are directly related to the scope of legal regulation and are therefore of high legal relevance. Experiments with these datasets can assess the effectiveness of algorithms in practical legal applications and provide technical support to e-commerce platforms in legal proceedings. Table 2 provides detailed statistics on the datasets. On this basis, the data are pre-processed by cleaning, text processing, score normalization, time erratic processing, and various density thresholds and time parameters are performed to determine the optimal parameters of the algorithm. The study is conducted using an Intel (TM) 7-3700 3.4GHz CPU and 8GB of RAM. The software is developed using Microsoft Windows 7 operating system and JDK1.8 development environment. Analysis tools such as SPSS and Eclipse 4.6.0 are also installed on the system. JDK 1.8 has good backward compatibility to support third-party libraries and frameworks used in the study, ensuring smooth transitions and fewer compatibility issues during development. A number of density thresholds are tested to determine the value that will best improve detection accuracy. Optimal parameter settings are selected by comparing performance at different thresholds. At the same time, the size of the time window is adjusted to assess changes in user behavior patterns over different time scales.

Figure 5 illustrates the accuracy versus Top-K for different α values for four different datasets (Amazon, YelpChi, YelpNYC, YelpZip). The red curves are the final choices of the experiments, which usually maintain higher accuracy in the Top-K region, especially when K is small. In this figure, the weight parameter has little effect on the algorithm in the Amazon database with a higher degree of association. The degree of association of the data at different thresholds reaches 0.9. In contrast, for Yelp data, which lacks such a close relationship, the impact is more significant. The density of a dataset is defined as the frequency of interactions between users and the degree of concentration of product reviews. Specifically, the density of a dataset can be measured by metrics such as the consistency of user ratings, the concentration of review time, and the frequency of interactions between users. Weighting parameters, on the other hand, are parameters used in the algorithm to adjust the impact of different features (e.g., user ratings, timestamps, etc.) on the final results. In denser datasets, such as the Amazon dataset, adjusting the weighting parameters has less impact on the algorithm's detection results due to the higher concentration of interactions between users and product reviews. This is because in high-density datasets, the consistency of user behavior is higher, allowing the algorithm to more consistently identify groups of false reviews and maintain a high accuracy rate even when the weighting parameters are changed. In low-density datasets, such as the Yelp dataset, where interactions between users and product reviews are more dispersed, the adjustment of the weighting parameters has a greater impact on the algorithm's detection results. This is because in low-density datasets, the consistency of user behavior is lower, and the adjustment of the weighting parameters may affect the algorithm's identification of user behavior patterns and the detection of false review groups. Therefore, this suggests that the degree of influence of the weighting parameters on the dataset is closely related to the density of the dataset.

Table 2: Experimental data set

Data set	Comments (article)	Commenters (individual)	Product (unit)	Time frame
Amazon	53778	5051	17607	2016.04-2022.08
YelpChi	67396	38061	199	2011.10-2022.10
YelpNYC	359050	160223	921	2011.10-2022.01
YelpZip	608597	260275	5041	2011.10-2022.01



(a) Amazon

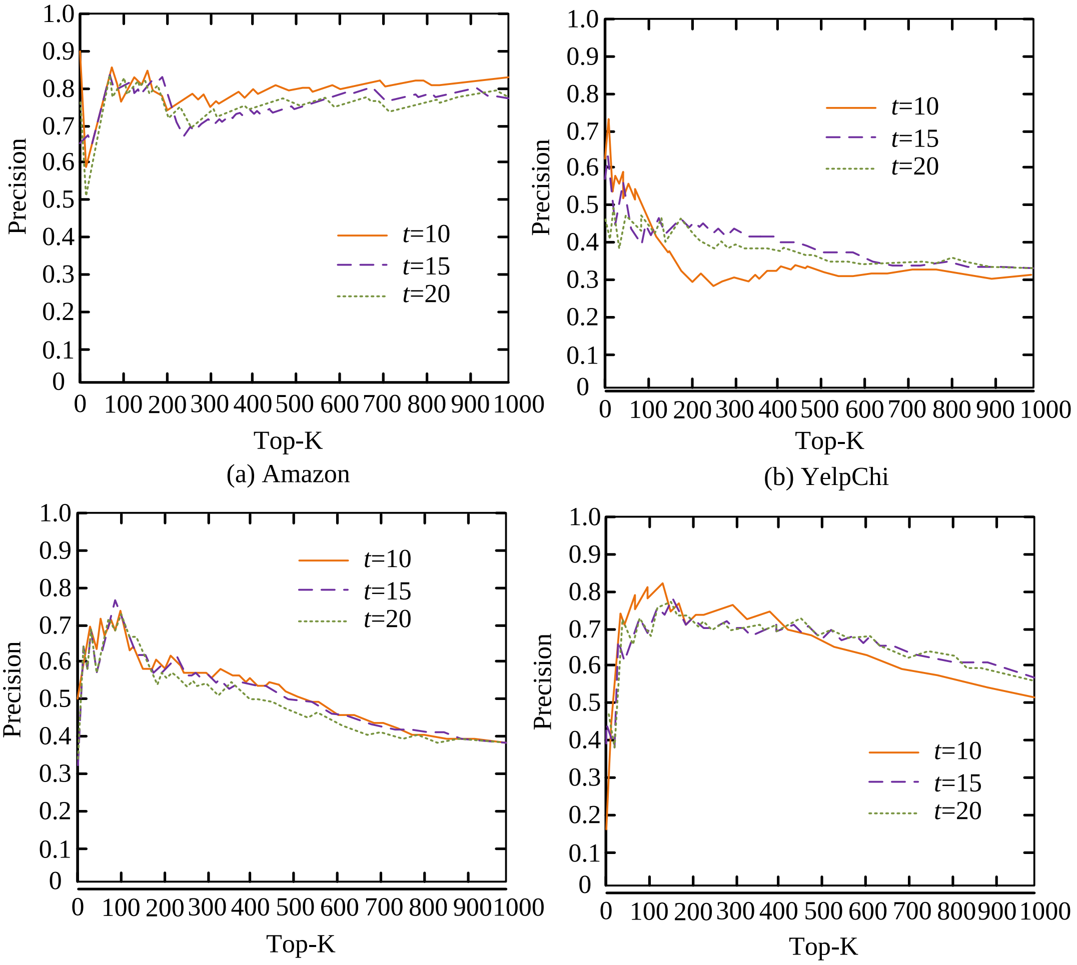
(b) YelpChi

(c) YelpNYC

(d) YelpZip

Figure 5: Influence of tightness thresholds of different values on test accuracy

As illustrated in Figure 6, the effect of varying time parameter values on test accuracy is evident for each dataset, with the legend denoting time intervals. The time interval is defined as the difference between the timestamp of a user's comment and the timestamp of the earliest or latest comment in the dataset. This time range is employed to analyze user behavior patterns over time. Similar to the weight parameters, the values corresponding to the red curve in this figure are the final results of this chapter. In this graph, unlike the weighted parameters, the time parameter has a minimal impact on test accuracy. For the YelpZip dataset, the effect of the time parameter is more important for the top 300 reviewers. This may be due to the fact that the behavior of these reviewers is more concentrated and therefore the time parameter is better able to capture changes in this behavior. The influence of the time parameter decreases as the number of reviewers increases, which may be due to the fact that as the number of reviewers increases, the diversity of user behavior increases and the influence of the time parameter on the overall behavior patterns is relatively weaker.



(a) Amazon

(b) YelpChi

(c) YelpNYC

(d) YelpZip

Figure 6: Influence of different time parameters of each data set on test accuracy

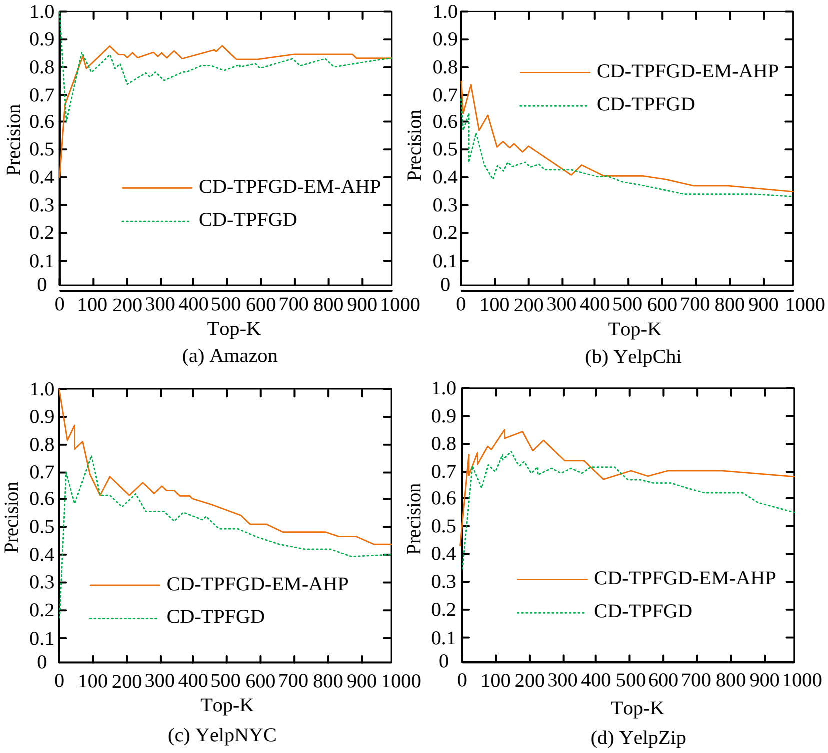
Table 3: The impact of label filtering on algorithm performance

Datasets	Enable tag filtering		Turn off tag filtering	
Amazon	Precision	0.88	Precision	0.78
	Recall	0.85	Recall	0.75
	F1 score	0.87	F1 score	0.76

Additionally, the study further analyzes the impact of label filtering *anklevalue* on algorithm performance. Using the Amazon dataset, the CD-TPFGD-EM-AHP algorithm is run with and without label filtering, and the recognition accuracy, recall rate, and F1 scores are recorded. As shown in Table 3, with label filtering enabled, there is a noticeable improvement in the accuracy, recall rate, and F1 scores of the algorithm. The accuracy increased from 0.78 to 0.88, the recall rate increased from 0.75 to 0.85, and the F1 score increased from 0.76 to 0.87. This indicates that label filtering effectively improves the detection performance of the algorithm.

On this basis, in order to validate the effectiveness of the CD-TPFGD-EM-AHP method in detecting false reviews in e-commerce, the detection accuracy of the two methods, CD-TPFGD and CD-TPFGD-EM-AHP, are first compared. The experiment selects the top 1000 users for testing to validate the accuracy of the algorithm (Figure 7). The validation results of the CD-TPFGD algorithm outperform the CD-TPFGD-EM-AHP algorithm for the Amazon dataset with Top-K of 50-52 segments, the YelpNYC dataset with Top-K of 80-110 segments, and the YelpZip dataset with Top-K of 390-450 segments, indicating that there may be a misclassified cluster where the test precision is low. Overall, the CD-TPFGD-EM-AHP algorithm gives better results.

4.2 The performance comparison verification of the fake comment detection model based on CD-TPFGD-EM-AHP



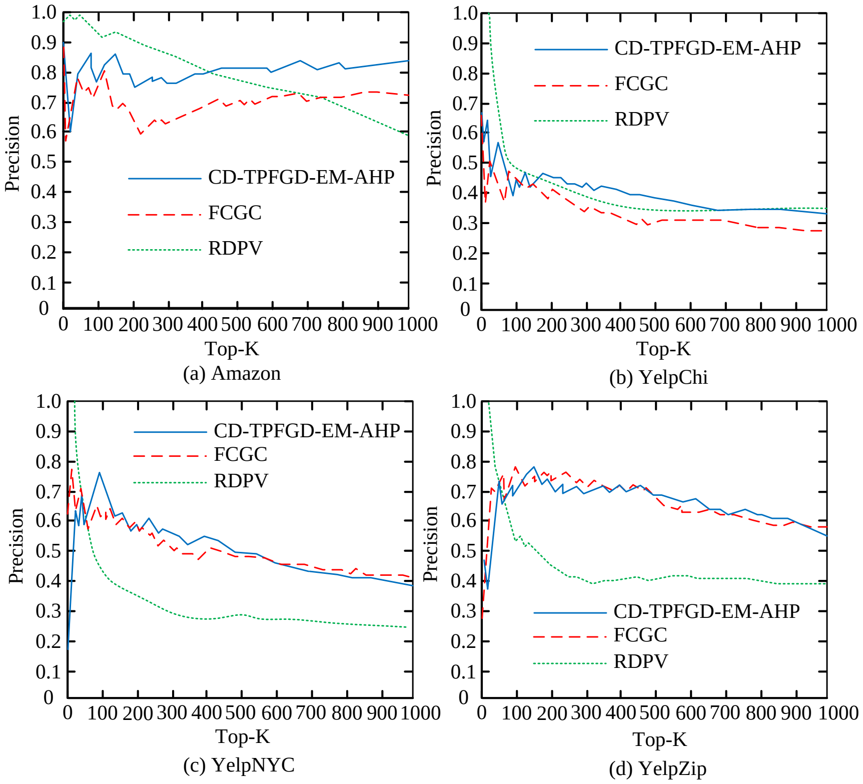
(a) Amazon

(b) YelpChi

(c) YelpNYC

(d) YelpZip

Figure 7: Difference in detection accuracy between CD-TPFGD and CD-TPFGD-EM-AHP



(a) Amazon

(b) YelpChi

(c) YelpNYC

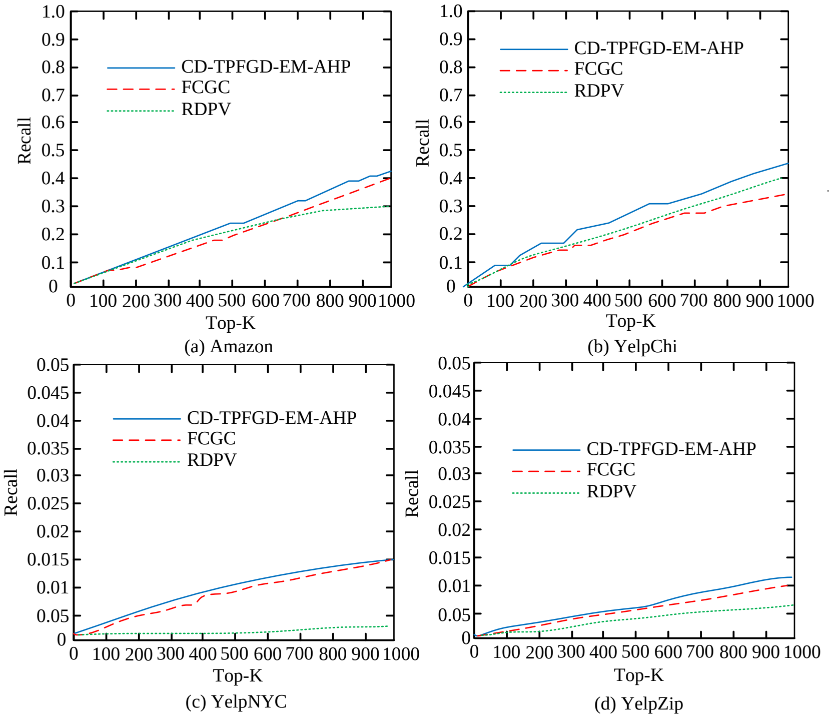
(d) YelpZip

Figure 8: Test accuracy results of three methods on four different data sets

To comprehensively assess the performance of the CD-TPFGD-EM-AHP method and demonstrate its potential in practical applications, the study further selected two currently popular false comment detection methods for comparative analyses. This is done to more clearly demonstrate the advantages of the CD-TPFGD-EM-AHP method in terms of accuracy, efficiency, and applicability. These methods are the found fake comment groups in graph clustering (FCGC) and the user ranking method based on doubtful probability values (RDPV). The accuracy of these three methods on four different datasets is illustrated in Figure 8. The CD-TPFGD-EM-AHP method has been demonstrated to exhibit consistent and reliable performance across various datasets. This finding suggests that the CD-TPFGD-EM-AHP method can be effectively applied to multiple datasets and can achieve effective fake comment detection on these datasets. On the Amazon, YelpNYC, and YelpZip datasets, the CD-TPFGD-EM-AHP method showed better detection and accuracy, with accuracies of about 0.88, 0.42, and 0.71, respectively. It suggests that the CD-TPFGD-EM-AHP method has a high degree of stability and applicability on these datasets. However, on the YelpChi dataset, CD-TPFGD-EM-AHP is slightly less accurate than RDPV, with an accuracy of about 0.31, while RDPV performs slightly better on this dataset. This difference may be due to the unique characteristics of the YelpChi dataset. Overall, the CD-TPFGD-EM-AHP method showed better detection and accuracy on the Amazon, YelpNYC, and YelpZip datasets.

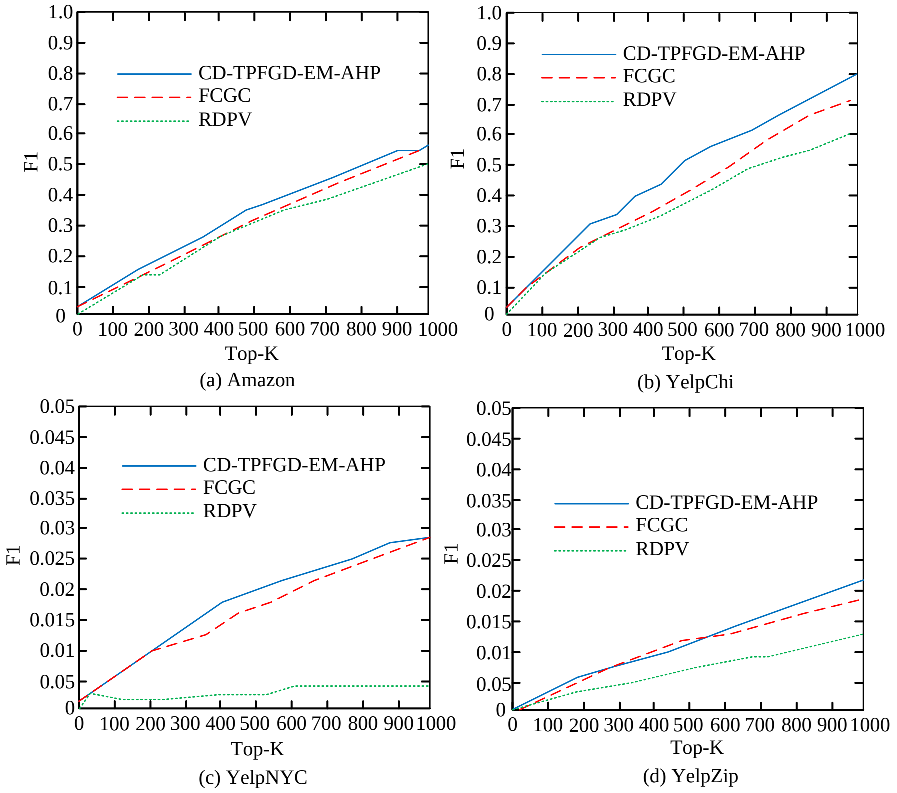
Figure 9 illustrates the recall of the three methods on the four datasets. On the YelpChi dataset, the recall of CD-TPFGD-EM-AHP is slightly lower than that of RDPV, which is consistent with the trend of accuracy observed in Figure 8. On the YelpZip dataset, CD-TPFGD-EM-AHP has a recall comparable to that of RDPV in most cases, but lower than RDPV at some points. On the other datasets, CD-TPFGD-EM-AHP has a high recall, suggesting that it is able to efficiently identify fake reviews in most cases.

Figure 10 illustrates the F1 scores of the three methods across four datasets. Through an analysis of these four datasets, it is observed that CD-TPFGD-EM-AHP outperforms RDPV and its effectiveness gradually increases with an increase in the number of viewers. RDPV performed poorly, especially on the YelpNYC dataset. The F1 score of CD-TPFGD-EM-AHP is superior to FCGC, but slightly lower compares to RDPV. Overall, CD-TPFGD-EM-AHP exhibits higher F1 scores compared to other methods in detecting false comment groups. The CD-TPFGD-EM-AHP algorithm does not perform as well on the YelpChi dataset as it does on other datasets. This may be due to the unique characteristics of the YelpChi dataset. YelpChi mainly contains reviews of localized services, which may differ significantly from the other datasets in terms of language style and review content. The reviews in YelpChi contain more local expressions and slang, which affects the effectiveness of the algorithm's feature extraction based on linguistic patterns.



(a) Amazon (b) YelpChi (c) YelpNYC (d) YelpZip

Figure 9: Recall rates of the three methods on the four data sets



(a) Amazon (b) YelpChi (c) YelpNYC (d) YelpZip

Figure 10: F1 values for three methods on four datasets

Table 4 presents a comparison of the running time of the three algorithms on four different datasets. The arithmetic mean of the 10 experimental running times is calculated to ensure the reliability of the results and to minimize the effect of random errors. This is due to the RDPV algorithm's inherent randomness in processing data, which can lead to variability in outcomes across iterations. To obtain a stable and reliable performance metric, 10 experiments are repeated, and the average running time of these experiments is calculated. The table indicates that CD-TPFGD-EM-AHP shows a significant advantage in computational speed compared to the RDPV algorithm. On the YelpChi dataset, the computational time for CD-TPFGD-EM-AHP is longer than that of FCGC, reaching 142.11 seconds. However, CD-TPFGD-EM-AHP demonstrates lower computational time and better results when dealing with other types of data. Furthermore, an analysis of the relationship between the sample sizes of the four datasets and the running time of the algorithms reveals a direct correlation between the increase in the speed of the CD-TPFGD-EM-AHP operation and the increase in the sample sizes. This correlation stands in contrast to the performance of algorithms such as FCGC and RDPV. Therefore, CD-TPFGD-EM-AHP has minimal impact on computational speed, indicating better identification effectiveness compared to FCGC, RDPV, and similar methods.

Table 4: The results of running time comparison of 3 algorithms on 4 data sets

Data set	CD-TPFGD-EM-AHP	FCGC	RDPV
Amazon	28.12s	42.03s	3601.11s
YelpChi	142.11s	85.99s	301.45s
YelpNYC	41.11s	1201.56s	24001.11s
YelpZip	164.12s	1419.11s	48021.01s

Note: Running time is one of the key metrics for measuring the usefulness of an algorithm. Although accuracy is the core criterion for evaluating the performance of an algorithm, the running time of an algorithm is also crucial in practical applications, especially when dealing with large datasets. An algorithm, even with high accuracy, may fail to deliver results in a reasonable amount of time if the running time is too long, limiting its use in real-time or large-scale application scenarios.

Table 5: Comparison of baseline models

Data sets	SVM	RF	LSTM	CD-TPFGD-EM-AHP	P-value
Amazon	0.82	0.83	0.83	0.88	0.00
YelpChi	0.77	0.79	0.75	0.79	0.03
YelpNYC	0.73	0.76	0.71	0.83	0.00
YelpZip	0.67	0.70	0.65	0.75	0.00

Finally, in order to further confirm the effectiveness of the proposed method, the study introduces three baseline models, SVM, RF, and LSTM, to compare the performance with the proposed method. The details are shown in Table 5.

In Table 5, the detection accuracy of the proposed CD-TPFGD-EM-AHP in this study is significantly higher than that of the three baseline models, SVM, RF and LSTM, for the four dataset types ($P<0.05$). This indicates that the use of CD in combination with indicator weighting metrics is reasonable and superior for the detection of misclassification. It also indicates the positive effectiveness of the proposed improvement strategy of the study.

5 Discussion

The CD-TPFGD-EM-AHP method proposed in the study demonstrated superior detection performance on the Amazon, YelpChi, YelpNYC, and YelpZip datasets compared to methods such as RDPV, FCGC, SVM, RF, and LSTM. By integrating label propagation based on CD with metric weight measurement using EM and AHP, this method could more accurately identify user relationships and review patterns, improving the accuracy of fake review detection. The CNN+LSTM method presented in reference [12] exceled at capturing sequential patterns, but had limitations in simulating complex user interactions and the subtleties of review context, making it difficult to distinguish between real and fake reviews. The n-gram-based system in reference [13] was effective for text classification tasks, but struggled with the nuances of detecting carefully crafted fake reviews.

The high recall rate in YelpZip indicated that the CD-TPFGD-EM-AHP effectively captured dense relationships in review data, but could face challenges in sparsely connected datasets. This was due to the algorithm's reliance on user interaction density and review consistency, which were less common in sparse datasets. In dense datasets like YelpZip, where user interactions and review patterns were more frequent and consistent, the proposed method could more accurately identify fake review groups. Future work will focus on improving the robustness of the model in such scenarios by integrating alternative data sources or developing hybrid models that can adapt to different data densities.

In terms of algorithm parameter selection, the weight parameter adjusted the impact of different features on the final results, having a smaller impact on dense datasets like Amazon, but a larger impact on sparse datasets like Yelp. The time parameter, which represented the timestamp difference between user reviews, had a small impact on the overall accuracy of the test, but was more important for capturing behavioral patterns in certain datasets. These results underscored the importance of carefully tuning parameters based on specific dataset characteristics. High accuracy ensured the reliability of the model's detection results, and precision indicated the proportion of identified fake reviews that were actually false. Together, these metrics affected the credibility of reviews presented to consumers and the reputational and financial impact on merchants and e-commerce platforms. However, while the model provided a good balance, improving the sensitivity of fake review detection without sacrificing the model's sensitivity may require more computational resources. The model needed further testing on a wider range of datasets to confirm its broad applicability. The model could struggle with reviews that closely mimic real user language, or when faced with new fake review strategies, and further optimization of error case review is needed.

6 Conclusion

In the present day, numerous unscrupulous e-commerce entities employ a large number of fake accounts to publish misleading reviews, attempting to boost their profits through this method. This violates commercial laws and harms consumer interests. To enhance the detection of fake reviews, this study proposed an e-commerce fake review detection method based on CD and metric weight measurement. The performance of the proposed model was validated in this study, and the experimental results indicated that the impact of weighted parameters on the dataset was related to the dataset's density. The detection accuracy of CD-TPFGD-EM-AHP surpassed that of CD-TPFGD. This study compared CD-TPFGD-EM-AHP with two other methods, FCGC and RDPV. The results demonstrated that CD-TPFGD-EM-AHP achieved detection accuracy of approximately 0.88, 0.31, 0.42, and 0.71 for the Amazon, YelpChi, YelpNYC, and YelpZip datasets, respectively, with stable detection outcomes. The recall and F1 score results for the three methods indicated that CD-TPFGD-EM-AHP exhibited superior performance compared to FCGC and RDPV. Additionally, the running time of CD-TPFGD-EM-AHP on the four datasets is better than the other two methods, with the shortest running time being 28.12 seconds. The limitation of this study lies in its failure to discuss sparse datasets using the proposed model, which could be considered as a direction for future research.

References

[1] A. Mewada, and R. K. Dewang, "Research on false review detection methods: A state-of-the-art review," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 9, pp. 7530-7546, 2022. https://doi.org/10.1016/j.jksuci.2021.07.021

[2] H. Paul, and A. Nikolaev, "Fake review detection on online E-commerce platforms: a systematic literature review," Data Mining and Knowledge Discovery, vol. 35, no. 5, pp. 1830-1881, 2021. https://doi.org/10.1007/s10618-021-00772-6

[3] P. K. Roy, and S. Chahar, "Fake profile detection on social networking websites: a comprehensive review," IEEE Transactions on Artificial Intelligence, vol. 1, no. 3, pp. 271-285, 2020. https://doi.org/10.1109/TAI.2021.3064901

[4] F. Lecue, "On the role of knowledge graphs in explainable AI," Semantic Web, vol. 11, no. 1, pp. 41-51, 2020. https://doi.org/10.3233/SW-190374

[5] S. Ji, S. Pan, E. Cambria, P. Marttinen, and P. Yu, "A survey on knowledge graphs: Representation, acquisition, and applications," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 2, pp. 494-514, 2021. https://doi.org/10.1109/TNNLS.2021.3070843

[6] K. Berahmand, S. Haghani, M. Rostami, and Y. Li, "A new attributed graph clustering by using label propagation in complex networks," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 5, pp. 1869-1883, 2022. https://doi.org/10.1016/j.jksuci.2020.08.013

[7] S. Graham, D. Yates, A. El-Roby, C. Brousseau, J. Ellens, and C. McDermott, "Relationship prediction in a knowledge graph embedding model of the illicit antiquities trade," Advances in Archaeological Practice, vol. 11, no. 2, pp. 126-138, 2023. https://doi.org/10.1017/aap.2023.1

[8] Y. Wang, Z. Li, J. Gao, and L. Zhao, "Deep neural network-based Wi-Fi/pedestrian dead reckoning indoor positioning system using adaptive robust

factor graph model," IET Radar, Sonar & Navigation, vol. 14, no. 1, pp. 36-47, 2020. https://doi.org/10.1049/iet-rsn.2019.0260

[9] Y. Zhong, C. Huang, and Q. Zhou, "HaSGP: an effective graph partition method for heterogeneous-aware," Computing, vol. 105, no. 2, pp. 455-481, 2023. https://doi.org/10.1007/s00607-022-01132-y

[10] L. Feng, H. Xu, G. Wu, and W. Zhang, "Service trade network structure and its determinants in the Belt and Road based on the temporal exponential random graph model," Pacific Economic Review, vol. 26, no. 5, pp. 617-650, 2021. https://doi.org/10.1111/1468-0106.12378

[11] J. Cheng, and Y. Wang, "Semi-supervised fake reviews detection based on aspamgan," Journal of Artificial Intelligence, vol. 4, no. 1, pp. 17-36, 2022. https://doi.org/10.36548/jaicn.2022.1.002

[12] G. Bathla, P. Singh, R. Singh, E. Cambria, and R. Tiwari, "Intelligent fake reviews detection based on aspect extraction and analysis using deep learning," Neural Computing and Applications, vol. 34, no. 22, pp. 20213-20229, 2022. https://doi.org/10.1007/s00521-022-07531-8

[13] S. N. Alsubari, S. N. Deshmukh, A. A. Alqarni, N. Alsharif, T. H. Aldhyani, F. W. Alsaade, and O. I. Khalaf, "Data analytics for the identification of fake reviews using supervised learning," Computers, Materials & Continua, vol. 70, no. 2, pp. 3189-3204, 2022. https://doi.org/10.32604/cmc.2022.019625

[14] D. U. Vidanagama, T. P. Silva, and A. S. Karunananda, "Deceptive consumer review detection: a survey," Artificial Intelligence Review, vol. 53, no. 2, pp. 1323-1352, 2020. https://doi.org/10.1007/s10462-019-09697-5

[15] A. Mutemi, and F. Bacao, "E-Commerce fraud detection based on machine learning techniques: systematic literature review," Big Data Mining and Analytics, vol. 7, no, 2, pp. 419-444, 2024. https://doi.org/10.26599/BDMA.2023.9020023

[16] Q. Guo, F. Zhuang, C. Qin, H. Zhu, X. Xie, H. Xiong, and Q. He, "A survey on knowledge graph-based recommender systems," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 8, pp. 3549-3568, 2020. https://doi.org/10.1109/TKDE.2020.3028705

[17] Z. Li, H. Liu, Z. Zhang, T. Liu, and N. Xiong, "Learning knowledge graph embedding with heterogeneous relation attention networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 8, pp. 3961-3973, 2021. https://doi.org/10.1109/TNNLS.2021.3055147

[18] L. Dong, J. Cheng, X. Zhang, and Y. Na, "Research on disease diagnosis method combining knowledge graph and deep learning," Journal of Frontiers of Computer Science and Technology, vol. 14, no. 5, pp. 815-824, 2020. https://doi.org/10.3778/j.issn.1673-9418.1908018

[19] D. Sardana, and R. B. Bhatnagar, "Graph algorithm to find core periphery structures using mutual k-nearest neighbors," International Journal of Artificial Intelligence & Applications, vol. 12, no. 1, pp. 1-18, 2021. https://doi.org/10.5121/ijaia.2021.12101

[20] P. Rathore, J. Soni, N. Prabakar, M. Palaniswami, and P. Santi, "Identifying groups of fake reviewers using a semisupervised approach," IEEE Transactions on Computational Social Systems, vol. 8, no. 6, pp. 1369-1378, 2021. https://doi.org/10.1109/TCSS.2021.3085406

[21] M. Burczaniuk, and A. Jastrz bska, "On the improvements of metaheuristic optimization-based strategies for time series structural break detection," Informatica, vol. 35, no. 4, pp. 687-719, 2024. https://doi.org/10.15388/24-INFOR572

[22] S. Moon, M. Y. Kim, and D. Iacobucci, "Content analysis of fake consumer reviews by survey-based text categorization," International Journal of Research in Marketing, vol. 38, no. 2, pp. 343-364, 2021. https://doi.org/10.1016/j.ijresmar.2020.08.001

[23] S. Saumya, and J. P. Singh, "Spam review detection using LSTM autoencoder: an unsupervised approach," Electronic Commerce Research, vol. 22, no. 1, pp. 113-133, 2022. https://doi.org/10.1007/s10660-020-09413-4

[24] A. Islam, F. Othman, N. Sakib, and H. Babu, "Prevention of shoulder-surfing attack using shifting condition with the digraph substitution rules," Artificial Intelligence and Applications, vol. 1, no. 1, pp. 58-68, 2023. https://doi.org/10.48550/arXiv.2305.06549

[25] V. Uluçay, I. Deli, and S. A. Edalatpanah, "Prioritized aggregation operators of GTHFNs MADM approach for the evaluation of renewable energy sources. Informatica, vol. 35, no. 4, pp. 859-882, 2024. https://doi.org/10.15388/24-INFOR570