IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 27, 2020, accepted June 8, 2020, date of publication June 16, 2020, date of current version June 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3002940

Detection of Social Network Spam Based on Improved Extreme Learning Machine

ZHIJIE ZHANG[1], RUI HOU[1], AND JIN YANG[2]
[1]School of Information Engineering, Lingnan Normal University, Zhanjiang 524048, China
[2]School of Medical Information and Engineering, Guangdong Pharmaceutical University, Guangzhou 510006, China

Corresponding author: Zhijie Zhang (zhgwzzj@126.com)

This work was supported in part by the Ministry of Education Higher Education Department Industry-Academic Cooperation Collaborative Education Project under Grant 201901240036, and in part by the Lingnan Normal University Talent Special Project under Grant ZL1824.

ABSTRACT With the rapid advancement of the online social network, social media like Twitter has been increasingly critical to real life and become the prime objective of spammers. Twitter spam detection refers to a complex task for the involvement of a range of characteristics, and spam and non-spam have caused unbalanced data distribution in Twitter. To solve the mentioned problems, Twitter spam characteristics are analyzed as the user attribute, content, activity and relationship in this study, and a novel spam detection algorithm is designed based on regularized extreme learning machine, called the Improved Incremental Fuzzy-kernel-regularized Extreme Learning Machine (I2FELM), which is used to detect the Twitter spam accurately. As revealed from the experience validation results, the proposed I2FELM can efficiently identify the balanced and unbalanced dataset. Moreover, with few characteristics taken, the I2FELM can more effectively detect spam, which proves the effectiveness of the algorithm.

INDEX TERMS Social network, spam detection, spam features, machine learning, I2FELM.

I. INTRODUCTION

Over the past few years, the Internet has been leaping forward, and the intelligent terminals have been progressively popularized. Under such background, Online Social Networks (OSN) turns out to be a critical channel for people to acquire information, disseminate information, and make friends and get entertained. For the complexity of the online social network structure, the large-scale nature of the group, and the massive, rapid, and difficult traceability of information generation, the effects of user adoption, content creation, group interaction and information dissemination on online social networks thoroughly impact social stability, organizational management models, as well as people's daily work and life [1], [2]. Take Twitter for an example, the detection of Twitter spam can facilitate the process of analyzing, guiding and monitoring social network events, as well as regulating the management of networks.

At present, the research challenges of Twitter spam are presented as follows, namely the feature selection and detection algorithm selection. The details are characterized below: 1) in feature selection, predecessor research often selects the identical type of characteristics e.g., content-based and user profile-based characteristics for detection. On the whole, since many types of characteristics of social network abnormal users are different from those of normal users, and it is not enough to accurately express the state of the data. 2) In algorithm selection, researchers primarily use supervised machine learning algorithms to deal with spam detection in social networks. Based on the idea of classification, the researchers have designed numerical form characteristics to identify spam users. The supervised machine learning algorithm can be split into a single classification algorithm and an integrated classification algorithm (e.g., Support Vector Machine (SVM) [3], [8]–[11], [13], [14], meta-classifiers (Decorate, Logit Boost) [4], Naive Bayesian (NB) [6], [9], [11], Back Propagation Neural Network (BP) [16], Radial Basis Function (RBF) [18], Extreme Learning Machine (ELM) [8], [22], K-nearest Neighbor (KNN) [9], [19], Decision Tree (DT) [9], [20], Random Forest (RF) [5], [7]–[9], [23]–[26] and eXtreme Gradient Boosting (XGBoost) [31], [32]). 3) The real dataset of social networks exerts a long tail effect, i.e., it is an unbalanced dataset with a number of non-spam far exceeding the spam. When those supervised machine learning

The associate editor coordinating the review of this manuscript and approving it for publication was Inês Domingues.

algorithms are detected on unbalanced dataset, their performance will decline. Accordingly, an algorithm capable of effectively exploiting multi-dimensional characteristics and exhibiting continuous feasibility in the face of imbalance datasets should be adopted.

By understanding and summarizing the research achievements of predecessors, four novel characteristics are proposed to express the Twitter datasets accurately and improve supervised machine learning algorithm to deal with unbalanced datasets to detect Twitter spam effectively. The details are illustrated below: 1) How to select the full category feature and pay attention to the correlation between the characteristics of the social network account helps enhance the accuracy of identifying spam users. This study considers the Twitter spam attributes composed by the user attribute, content, activity and relationship to express the user characteristic and detect the spam accurately. 2) This study proposes a novel incremental Twitter spam assessment algorithm, termed as the Improved Incremental Fuzzy-kernel-regularized Extreme Learning Machine (I2FELM) to enhance the accuracy in dealing with the unbalanced data. 3) I2FELM is capable of enhancing the performance using Cholesky factorization without square root and composite kernel function. Besides,, it can automatically determine the optimal number of hidden layer nodes by gradually adding new hidden nodes one by one. 4) The I2FELM introduces the fuzzy weight as a method to address the unbalanced problem, which can apply to each input and facilitate the learning of output weights. 5) On the public dataset and the collected dataset, a range of index parameters and experimental verification methods are adopted to ascertain the performance of I2FELM, and spam is assessed based on the imbalance data problem and few characteristics.

The article structure is arranged as follows. Section II presents the relevant work. Section III illustrates the novel Twitter spam detection model. Section IV discusses the experimental procedure, and Section V draws the conclusion of the study.

II. RELATED WORK

Extensively studied, several approaches related to social spam detection have been proposed (e.g., spam characteristics and assessment algorithm).

Benevenuto *et al.* [3] considered two attribute sets, namely, content attributes and user attributes, to distinguish one user class from the other and exploited the mentioned characteristics as attributes of SVM process to classify users as either spam or non-spam. Lee *et al.* [4] conducted the statistical analysis of the properties of the mentioned spam profiles to create spam classifier to actively filter out existing and novel spam. Based on the mentioned profile characteristics, the authors developed meta-classifiers (Decorate, Logit Boost, etc.) to identify previously unknown spam. Stringhini *et al.* [5] initially created a set of honey net accounts (honey-profiles) on Twitter and then identified multiple characteristics that allow authors to detect spam. Lastly, the RF model was built to detect spam and employed in a Twitter dataset. Wang [6] developed the novel content-based characteristics and graph-based characteristics to facilitate spam detection; besides, a Bayesian classification algorithm was adopted to distinguish the suspicious behaviors from normal ones. Chu *et al.* [7] presented the collective perspective and focused on identifying spam campaigns that manipulate multiple accounts to spread spam on Twitter. An automatic classification system was designed based on RF and a variety of characteristics, i.e., individual tweet/account levels to classify spam campaigns. In Meda *et al.*'s work [8], a standard Principal Component Analysis (PCA) algorithm was exploited to reduce the dimensionality of the 62 feature to the 20 characteristics, 10 characteristics, and 5 characteristics, and then three different machine learning algorithm (SVM, ELM, RF) were adopted to support spam detection in Twitter. Wang *et al.* [9] studied the suitability of five classification algorithms of Bayesian, KNN, SVM, DT, and RF at the detection stage; they took four different feature sets of user characteristics, content characteristics, n-grams, and sentiment characteristics to the social spam detection task. Zheng *et al.* [10] extracted a set of characteristics from content-based and user-based feature and applied into SVM-based spam detection algorithm. Chen *et al.* [11] built a hybrid model that uses SVM and NB to distinguish suspect users from normal ones based on the user-based characteristics and content-based characteristics. During the assessment, the authors assessed the impact of different factors on spam detection performance, covering discretization of functionality, size of learning data, and data related to time. Chen *et al.* [12] proposed an Lfun approach to identify the "Spam Drift" problem in statistical features based Twitter spam detection. They compared Lfun to four traditional machine learning algorithms and evaluated the performance of Lfun approach in terms of overall accuracy, F-measure and Detection Rate. He *et al.* [13] proposed an analysis approach based on information entropy and incremental learning to study how various features affect the performance of an RBF-based SVM spam detector, through this effort, they attempted to increase the awareness of a spam by sensing the features of a spam. Teng *et al.* [14] proposed a self-adaptive and collaborative intrusion detection model is built by applying the Environments classes, agents, roles, groups, and objects (E-CARGO) model. Wu *et al.* [15] found that most of current spam detection techniques are based on feature selection and machine learning classification (e.g. DT, RF and NB). Liu *et al.* [16] reviewed the schemes and systems proposed to deal with an increasing number of cyber security threats. The work can extract information from data sources and applied analytics/algorithm (e.g. machine learning) to make a decision. Sun *et al.* [17] presented an overview and research outlook of the emerging field, i.e., cybersecurity incident prediction. They also extracted and summarized the research methodology at critical phases of predicting cybersecurity incident. In the research of Coulter *et al.* [18], a new research methodology of data-driven cyber security (DDCS)

was demonstrated, and its application in social and Internet traffic analysis was studied. DDCS shows the strong link between data, model, and methodology during the review of key recent works in Twitter spam detection and IP traffic classification.

Dayani *et al.* performed the KNN on user-based characteristics and NB on the word cloud acquired in the pre-processing step to detect tweets spreading rumors [19], which demonstrated how appropriate preprocessing improves rumor detection substantially. Sheu *et al.* [20] aimed to propose an efficient spam filtering mechanism based on the simple decision tree data mining algorithm that finds association rules about spams from the training e-mails. Liu *et al.* [21] proposed an embedded feature selection method using our proposed weighted Gini index (WGI), which used a decision tree splitting criterion as a feature selection method.

Zheng *et al.* [22] first built the labeled dataset through crawling Sina Weibo data and manually classified corresponding users into spam and non-spam categories. Subsequently, a set of characteristics were extracted from message content and user behavior and then substituted in the ELM-based spam classification algorithm. In Meda *et al.*'s research [23], the system randomly taken, as relevant, 1/6 of the originally available 54 characteristics, to simulate a real case study in which the intrinsic correlation of different characteristics is not easily understandable, causing an ineffective configuration of the probability distribution by the analyst. Next, a variant of the Random Forests Algorithm was exploited to identify spam inside Twitter traffic. The spam detection performances of 9 mainstream algorithms were compared to identify the optimal algorithms on account-based characteristics and tweet content-based characteristics datasets by Lin *et al.* [24]. Though experimental verification, RF achieved the optimal performance under a range of conditions.

Liu *et al.* [25], [26] exploited twelve characteristics to express Twitter spam and developed an ensemble learning approach that learns more accurate single classifiers from imbalanced data following three steps. In the classification step, the RF exhibited a better performance in dealing with different ratios of imbalanced data. During the final step, a majority voting scheme was introduced to combine the assessed results from the second step classification models. Wang [27] improved the precision of the liquid steel temperature prediction in Ladle Furnace by the random forest method on the large sample set accumulated from the production process. Tang *et al.* [28] analyzed the characteristics of spammers in Weibo and proposed fuzzy-logic-based oversampling and cost-sensitive support vector machine algorithmic levels. Wang *et al.* [29] presented a drifted twitter spam classification method by using multiscale drift detection test (MDDT) on K-L divergence.

He *et al.* [30] proposed another form of deep learning, a linguistic attribute hierarchy, embedded with linguistic decision trees, for spam detection. Such approach can improve the performance of spam detection when the semantic attributes are constructed to a proper hierarchy, while efficiently overcoming 'curse of dimensionality' in spam detection with massive attributes.

Saini *et al.* [31] extracted different textual characteristics from text reviews and used XGBoost to build the classifier. In Xu *et al.*'s study, the feature extraction was performed on existing normal and malicious requests, and XGBoost classification algorithm was adopted to identify abnormal requests. By experimental comparison, XGBoost was found exerting better recognition effect of abnormal HTTP requests than the random forest, which supports vector machine [32].

Based on the previous research results, researchers are paying attention to the problem of abnormal users in social networks. In the process of detecting spam, researchers extracted various features to describe the characteristics of spam. The spam feature description is a complex task, which can be described in terms of the user's personal information, published content and favorite features. And, supervised machine learning algorithms were widely used in the detecting of spam due to their superior performance, high prediction accuracy, and strong generalization performance.

III. MODEL

Nowadays, the Twitter spam attributes primarily focus on the tweet-based characteristics and user-based characteristics. The assessment algorithms refer to general machine learning methods based on the relationship between spam characteristics and detection. For instance, the methods adopted are primarily SVM, DT, RF, BP, RBF, ELM, and XGBoost, etc. In the face of the multi-dimensional characteristics and the imbalance dataset, the performance of the mentioned algorithms requires enhancement.

This study proposes the Twitter spam attributes consisting of user attribute, content, activity and relationship characteristics to detect spam exactly; each feature can be captured in the Twitter to ensure its integrity and reliability. Besides, I2FELM is designed to address the multi-dimension and non-balance problem to achieve the high assessment accuracy.

The procedure of Twitter spam detection is illustrated in Fig. 1. First, dataset from Twitter is collected to form user attribute, content, activity and relationship characteristic sets. Second, the collected dataset is preprocessed for labeling each user as a spam or non-spam. Third, the proposed I2FELM is adopted to tackle down the unbalanced problem. An optimal function of I2FELM is formed by training and testing phase. Based on the formed optimal function, I2FELM can effectively assess Twitter spam of novel dataset in the classification phase.

A. FEATURE SET

In this study, the feature set is composed of user attribute, content, activity and relationship in the online social network, and the details are listed in Table 1. To be specific, the user attribute feature refers to the period of the existence of the account, the number of registered locations, the number of

TABLE 1. The Twitter feature set.

Feature	Description
User attribute	Age of account
	Number of registered locations
	Number of lists
	Number of tweets sent
Content	Number of retweets
	Number of favorites
	Number of hashtags
	Number of URLs
	Number of characters
	Number of digits
	Number of mentions
	Number of spam words
	Content similarity score (mean, maximum
	and minimum, standard deviation)
Activity	Time of tweet created
	Duration of tweets sent
	Time information entropy
	Location of tweet created
	Source of tweet created
	Time between tweet
	Number of tweet per day
	Time of tweet mentioned
	Number of replies
	Time between replies
	Number of repetitions
	Number of uses of URL revised
	Number of uses of hashtag revised
	Number of uses of mention revised
Relationship	Number of followers
	Number of following
	Number of favorites
	Clustering coefficient (concentration of
	time when activity occurs)

lists added by the user, and the number of tweets sent by the user. Besides, the content feature covers the numbers of retweets this tweet, favorites this tweet received, hashtags and URLs this tweet included, characters and digits in this tweet, the mentioned time of this tweet, as well as spam words in this tweet, content similarity score. The activity feature is associated with the user behavior information when the user creates the tweet, covering the time of this tweet created, time interval between two tweets, the number of tweets created each day, the time of this tweet mentioned, the location and source of this tweet sent, the number of this user replied, the

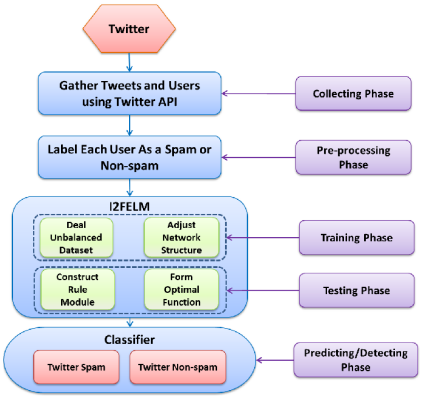


FIGURE 1. The procedure of Twitter spam detection.

number of repetitions of this tweet, the number of uses of URL, as well as hashtag and mention this user modified. The relationship characteristic refers to the user's interaction with other people (e.g., the number of followers, the number of following and clustering coefficient).

B. DETECTION ALGORITHM

In an online social network, the number of non-spam is significantly greater than that of spam, leading to the problem of unbalanced data. Accordingly, the I2FELM is proposed to solve the problem based on RELM. The proposed algorithm can effectively improve the accuracy using fuzzy membership, as an attempt to optimize the learning of output weights in various aspects and increase operation efficiency based on Cholesky factorization without square root and composite kernel function for the non-balance of datasets.

1) RELM

Extreme learning machine (ELM) was proposed for training single hidden layer feedforward neural networks (SLFNs); it can act as an efficient learning solution for regression problem [33]. The essence of ELM is that: unlike the common understanding of learning, the hidden layer of SLFNs should not be tuned. Considering N training data $\{(x_i, t_i) \,|x_i \in R^n, t_i \in R^m\}_{i=1}^N$, if an SLFN with L hidden nodes can approximate the mentioned N samples with zero error, it implies the existence of β, w and b; thus, it yields

$$f(x_i) = h(x_i)^T \beta = \sum_{j=1}^{L} \beta_j G(w_j, b_j, x_i), \quad i = 1, \ldots, N \tag{1}$$

where $\beta_j = [\beta_{j1}, \ldots, \beta_{jm}]^T$ denotes the vector of the output weights between the hidden layer and the output layer, $w_j = [w_{j1}, \ldots, w_{jn}]^T$ is the input weights connecting input nodes with the jth hidden node, b_j represents the threshold of the j hidden node, and $G(w_j, b_j, x_i)$ is the activation function (e.g., $G(w_j, b_j, x_i) = 1 \Big/ \left(1 + \exp\left(-\left(w_j^T \cdot x_i + b_j\right)\right)\right)$) satisfying ELM universal approximation capability theorems.

To enhance the generalization ability of the traditional SFLNs based on ELM, Huang *et al.* [34] proposed the equality constrained optimization-based ELM. In their approach, structural risk considered as the regularization term is introduced. The so-called RELM is capable of regulating the proportion of structural risk and empirical risk using the parameter C. The proposed constrained optimization can be formulated as

$$\begin{aligned} &\min \Gamma_{RELM} = \frac{1}{2}\|\beta\|^2 + C\frac{1}{2}\sum_{i=1}^{N}\|\xi_i\|^2 \\ &s.t.\ h(x_i)^T\beta = t_i - \xi_i \quad i = 1,\ldots,N \end{aligned} \tag{2}$$

where ξ_i denotes the slack variable of the training sample x_i and C controls the tradeoff between the output weights and the errors. Eq. (2) is similar to the classical optimization problem of SVM, despite the simpler constraints, and it is valid for regression, binary, and multiclass cases [35]. Thus, (2) achieves a solution in the closed form

$$\beta = H^T\left(HH^T + \frac{I}{C}\right)^{-1}T \tag{3}$$

where $H = [h(x_1),\ldots,h(x_N)]^T_{N\times L}$ denotes the hidden layer output matrix, I indicates the identity matrix and $T = [t_1,\ldots,t_N]^T_{N\times m}$. The RELM output function can be further derived as

$$f(x_i) = h(x_i)^T\beta = h(x_i)^T H^T\left(HH^T + \frac{I}{C}\right)^{-1}T \quad i = 1,\ldots,N \tag{4}$$

2) I2FELM

The I2FELM is proposed for training single hidden layer feedforward neural networks (SLFNs) based on RELM. The essence of I2FELM is that the hidden layer of the generalized SLFNs should not be tuned. Therefore, it can be applied in regression and multiclass classification applications directly.

I2FELM consists of three layers of nodes: an input layer, a hidden layer and an output layer. In the input layer, the input dataset should be dealt with the different weights for imbalanced problem [36]. Each input data x_i is provided with a weight s_i, $\delta \le s_i \le 1$. The value of s_i is assigned according to the ratio of abnormal users to normal users in the dataset.

Therefore, the prediction problem for the constrained-optimal-based improved incremental fuzzy kernel regularized extreme learning machine can be formulated as

$$\begin{aligned} &\min \Gamma_{I2FELM} = \frac{1}{2}\|\beta\|^2 + C\frac{1}{2}\sum_{i=1}^{N}S_i\|\xi_i\|^2 \\ &s.t.\ h(x_i)^T\beta = t_i - \xi_i \quad i = 1,\ldots,N, \end{aligned} \tag{5}$$

wherein, the values of $\beta_j, \xi_i, x_i, C, h(x_i), t_i$ are consistent with the values of RELM.

Based on the Karush-Kuhn-Tucker (KKT) theorem, the corresponding Lagrange function of the I2FELM optimization (5) is

$$\begin{aligned} \Gamma_{I2FELM} &= \frac{1}{2}\|\beta\|^2 \\ &\quad + C\frac{1}{2}\sum_{i=1}^{N}S_i\|\xi_i\|^2 - \sum_{i=1}^{N}\alpha_i\left(h(x_i)^T\beta - t_i + \xi_i\right) \end{aligned} \tag{6}$$

The KKT corresponding optimality conditions as follows:

$$\frac{\partial\Gamma_{I2FELM}}{\partial\beta} = 0 \Rightarrow \beta = \sum_{i=1}^{N}\alpha_i h(x_i) = H^T\alpha \tag{7a}$$

$$\frac{\partial\Gamma_{I2FELM}}{\partial\xi_i} = 0 \Rightarrow \alpha_i = CS_i\xi_i \quad i = 1,\ldots,N \tag{7b}$$

$$\frac{\partial\Gamma_{I2FELM}}{\partial\alpha_i} = 0 \Rightarrow h(x_i)^T\beta - t_i + \xi_i = 0 \quad i = 1,\ldots,N \tag{7c}$$

By substituting (7a) and (7b) into (7c), the equations can be equivalently written as

$$\left(HH^T + \frac{S}{C}\right)\alpha = T \tag{8}$$

wherein the fuzzy matrix $S = \begin{bmatrix} \frac{1}{S_1} & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{S_2} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{1}{S_N} \end{bmatrix}_{\mathrm{N*N}}$

From (7a) and (8)

$$\beta = H^T\left(HH^T + \frac{S}{C}\right)^{-1}T \tag{9}$$

Thus, the input dataset with weight matrixes can make important contributions to the learning of the output weights β for imbalanced dataset. Then, the output function of I2FELM is

$$\begin{aligned} f(x) &= h(x_i)^T\beta \\ &= h(x_i)^T H^T\left(HH^T + \frac{S}{C}\right)^{-1}T \\ &\quad i = 1,\ldots,N \end{aligned} \tag{10}$$

In order to improve the operation efficiency of I2FELM and reduce the run time, Cholesky decomposition without square root [37] will be used to calculate the value of β.

The Cholesky decomposition of β is shown as follows

$$\begin{cases} A\cdot\beta = b & (11) \\ A = HH^T + \dfrac{S}{C} & (12a) \\ b = H^T T & (13) \end{cases}$$

In (12a), the kernel methods [38] that satisfy Mercer's condition can be adapted to calculate inner product, so as to reduce the complexity of algorithm. The (12a) can be written

as (12b), while the kernel function can be calculated with the composite kernel function

$$\begin{cases} A = \left(HH^T + \dfrac{S}{C}\right) = \left(\Omega + \dfrac{S}{C}\right) \\ \Omega = HH^T : \Omega = h\left(x_j\right) \cdot h\left(x_k\right) = K\left(x_j, x_k\right) \\ = (1-t) \cdot \left(x_j - x_k\right) + t \cdot \exp\left(-\left\|x_j - x_k\right\|^2 \Big/ \sigma^2\right) \\ 0 \le t \le 1. \end{cases} \quad (12b)$$

From (12a), we can get an equation of A

$$A^T = \left(HH^T + \frac{S}{C}\right)^T = \left(HH^T + \frac{S}{C}\right) = A \quad (12c)$$

For any vector V, the quadratic form of A can be expressed as

$$\begin{aligned} V^T AV &= V^T \left(H^T H + \frac{S}{C}\right) V \\ &= \sum_{i=1}^{N} \left(f\left(a_i x_1 + c_i\right) v_i\right)^2 + \cdots \\ &\quad + \sum_{i=1}^{N} \left(f\left(a_i x_k + c_i\right) v_i\right)^2 + \frac{S}{C} \sum_{i=1}^{N} v_i^2 > 0 \end{aligned} \quad (14)$$

From (14), A is a positive definite matrix.

Thus, Cholesky decomposition of the matrix A can be obtained

$$A = LDL^T \quad (15)$$

wherein,

$$A = \left[a_{ij}\right] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \quad (16)$$

$$L = \begin{bmatrix} l_{11} & & \\ \vdots & \ddots & \\ l_{n1} & \cdots & l_{nn} \end{bmatrix} \text{ and } D = \begin{bmatrix} 1/l_{11} & & \\ & \ddots & \\ & & 1/l_{nn} \end{bmatrix} \quad (17)$$

L is a lower triangular matrix whose diagonal elements are all positive numbers, L^T is the transpose of L, and

$$l_{ij} = a_{ij} - \sum_{k=1}^{j-1} l_{ik} l_{jk} \Big/ l_{kk}, \quad i \ge j \quad (18)$$

Substituting (15) into (11), thus leading to

$$LDL^T \cdot \beta = b \quad (19)$$

Denote

$$F = L^T \beta \quad (20)$$

Substituting (20) into (19)

$$LDF = b \quad (21)$$

Using (17) and (21), we have

$$f_{ij} = \begin{cases} b_{ij}, & i = 1 \\ b_{ij} - \sum_{n=1}^{i-1} l_{in} f_{nj} \Big/ l_{nn}, & i > 1 \end{cases} \quad (22)$$

According to (18), (20), (22), we can further obtain

$$\beta_{ij} = \begin{cases} f_{ij} \Big/ l_{ii}, & i = m \\ \left(f_{ij} - \sum_{n=1}^{m-i} l_{i+n,i} \beta_{i+n,j}\right) \Big/ l_{ii}, & i < m \end{cases} \quad (23)$$

Thus, β is calculated by a simple four arithmetic operation to accelerate the learning speed of the I2FELM.

Finally, the incremental method is introduced to calculate the number of hidden layers of I2FELM. When the number of hidden layers is added from L to $L+1$, the newly hidden layer matrix H_{L+1}

$$H_{L+1} = \begin{bmatrix} H_L \\ h_{L+1} \end{bmatrix} = \begin{bmatrix} h_1 \cdots h_L \\ h_{L+1} \end{bmatrix} \quad (24)$$

And

$$A_{L+1} \beta_{L+1} = b_{L+1} \quad (25)$$

$$F_{L+1} = L_{L+1}^T \beta_{L+1} \quad (26)$$

Then, b_{L+1} is shown as follows

$$b_{L+1} = H_{L+1}^T T = \begin{bmatrix} b_L \\ h_{L+1}^T T \end{bmatrix} \quad (27)$$

$$\begin{aligned} A_{L+1} &= H_{L+1}^T H_{L+1} + \frac{S}{C} \\ &= \begin{bmatrix} H_L \\ h_{L+1} \end{bmatrix}^T \begin{bmatrix} H_L \\ h_{L+1} \end{bmatrix} + \frac{1}{C} \begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \dfrac{S}{C} + H_L^T H_L & h_{L+1} H_L^T \\ h_{L+1}^T H_L & h_{L+1}^T h_{L+1} + \dfrac{1}{C} \end{bmatrix} \\ &= \begin{bmatrix} A_L & Q_{L+1}^T \\ Q_{L+1} & P_{L+1} \end{bmatrix} \end{aligned} \quad (28)$$

where $Q_{L+1} = h_{L+1}^T H_L = \left[h_{L+1}^T h_1 \ldots h_{L+1}^T h_L\right]$.

From (15), (17), (28), L_{L+1} is

$$L_{L+1} = \begin{bmatrix} L_L & 0 \\ l_{L+1} & l_{L+1,L+1} \end{bmatrix} \quad (29)$$

where $l_{L+1} = \left[l_{L+1,1} \cdots l_{L+1,L}\right]$, and

$$l_{L+1,j} = a_{L+1,j} - \sum_{k=1}^{j-1} l_{L+1,k} l_{jk} \Big/ l_{kk} \quad j = 1, \ldots, L+1 \quad (30)$$

From (21), (27), (29), we can get

$$F_{L+1} = \begin{bmatrix} F_L \\ f_{L+1} \end{bmatrix} \quad (31)$$

$$L_{L+1} D_{L+1} F_{L+1} = \begin{bmatrix} L_L & 0 \\ l_{L+1} & l_{L+1,L+1} \end{bmatrix} \begin{bmatrix} D_L & 0 \\ 0 & d_{L+1,L+1} \end{bmatrix}$$

$$= \begin{bmatrix} L_L D_L F_L \\ l_{L+1} D_L F_L + f_{L+1} \end{bmatrix}$$
$$= \begin{bmatrix} b_L \\ h_{L+1}^T T \end{bmatrix} \quad (32)$$

In the further step,

$$f_{L+1,j} = b_{L+1,j} - \sum_{k=1}^{L} \frac{l_{L+1,k} f_{kj}}{l_{kk}}, \quad j = 1, \ldots, L \quad (33)$$

Therefore, β_{L+1} can be calculated by (23) and I2FELM prediction model is built by (10).

To summarize, I2FELM has better scalability and runs at much faster learning speed, which can work with a widespread type of feature mappings and less human intervention. It can be summarized as in Algorithm 1.

Algorithm 1 I2FELM(N, L, S)

1: $s = s_i\ (0 < s_i \leq 1, i = 1, \ldots, N)$;
//given the fuzzy membership
2: **for** ($L = 1$ to $K - 1$) **do**
3: **if** ($L \geq 2$) **then**
4: $l_{L+1,j} = a_{L+1,j} - \sum_{k=1}^{j-1} l_{L+1,k} l_{jk} / l_{kk}$;
5: $f_{L+1,j} = b_{L+1,j} - \sum_{k=1}^{L} \frac{l_{L+1,k} f_{kj}}{l_{kk}}$;
6: **end if**
7: $\beta_L = \begin{cases} f_{ij} / l_{ii}, i = m \\ \left(f_{ij} - \sum_{n=1}^{m-i} l_{i+n,i} \beta_{i+n,j} \right) \Big/ l_{ii}, i < m \end{cases}$;
8: $H = [h(x_1), \ldots, h(x_N)]_{N \times L}^T$
9: $f(x) = h(x_i)^T \beta$;
// use (10) to build I2FELM model
10: $R_L = \frac{1}{2} \|\beta\|^2 + C \frac{1}{2} \sum_{i=1}^{N} S_i \|\xi_i\|^2$;
// calculate the total risk of I2FELM
11: **if**($L \geq 5$) **then**
12: $\gamma = \left| (R_{L-i} - R_{L-i-1}) / \max(R_1, \ldots, R_L) \right|$;
13: **if**($\gamma \leq \varepsilon$) **then**
14: $K = L$;
15: **end if**
16: **end if**
17: **end for**

IV. EXPERIENCE

A. DATASET COLLECTION

In this experiment, two datasets are exploited to compare the experimental results.

The first dataset is the public dataset, namely, the Aponador dataset [39]. Such dataset was collected with Brazil's famous location-based social network and covers both normal users and spam users, in which each record contains 59 characteristic and 2 classifications.

The second dataset is harvested by this study using the Twitter API and Twitter4J library, which cover 43 million tweets posted by around 16 million accounts that contain daily popular trends in June of 2017. The method of [40] is employed to label the Twitter spam and non-spam accounts during the pre-processing phase for I2FELM in dataset collected by ourselves. The method [40] proposed a hybrid technique, combining a blacklist augmented with algorithms fitting social networks to the problem of identifying spam and malicious Tweets. To be specific, it is concluded based on the collected data that blacklisting, in conjunction with other analytical tools, can effectively identify malicious Tweets. Accordingly, the spam can be blocked by blacklists. Using the graphical approach, a set of users involved in a round-robin approach will yield a bipartite clique in the graph. Hence, bipartite cliques in such a graph are very suspicious – the probability of real users behaving this way in the normal course of events is extraordinarily small. The blacklist is augmented with a clique-discovery approach that can also effectively identify spam. Finally, 0.81 million accounts have been identified and labeled as spam or non-spam, where each record contains 62 characteristic.

B. EXPERIMENTAL SETUP

The experiment is run in Matlab2012b environment, computer memory is 8GM RAM, and CPU is 2.40GHz. Randomly select 60% of the first or second datasets as training set and 40% as testing set. The fuzzy weight of each data sample is determined by the imbalance ratio of the training set.

The proposed I2FELM algorithm in this study pertains to supervised learning in machine learning. For this reason and given previous research results, the SVM, DT, RF, BP, RBF, ELM, and XGBoost are introduced to compare the experiment results to assess the performance of I2FELM using the accuracy, true positive rate (TPR), precision and F-measure [41], [42]. The details are elucidated below:

TABLE 2. The assessment matrix.

	Assessment	
	Spam	Non-spam
Actual spam	TP	FN
Actual non-spam	FP	TN

(1) An assessment matrix [43] is illustrated in Table 2 as an effective measurement method to assess the experimental results. In this matrix, the true positive (TP) reveals that the spams are correctly classified, the false negative (FN) means that the spams are misclassified into non-spams, the false positive (FP) denotes that the non-spams are misclassified into spams, and the true negative (TN) reveals that the non-spams are classified accurately.

(2) Under the assessment matrix, the accuracy, TPR, precision, and F-measure as a set of metrics to assess the effectiveness of SVM, DT, RF, BP, RBF, ELM, XGBoost, and I2FELM.

The accuracy is indicated by the percentage of correctly identified examples in the total number of examined

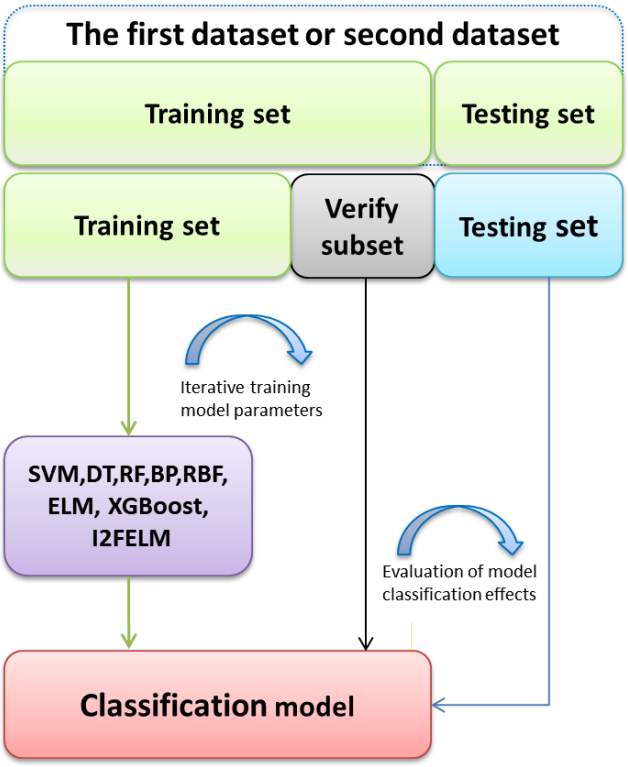


FIGURE 2. The steps of the experiment.

examples, as expressed by Eq. (34).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{34}$$

The TPR is the ratio of correctly classified spams to the total number of actual spams, as defined by Eq. (35).

$$TPR = \frac{TP}{TP + FN} \tag{35}$$

The precision is indicated by the proportion of correctly classified spams to the total number of tweets that are classified as spams, as expressed in Eq. (36).

$$Precision = \frac{TP}{TP + FP} \tag{36}$$

The F-measure is the assessment accuracy combining both the precision and TPR, as calculated by Eq. (37).

$$F - measure = \frac{2 * TPR * Precision}{TPR + Precision} \tag{37}$$

C. EXPERIMENTAL RESULT AND COMPARISON

In the present section, the three experiments are performed in first and second datasets.

All assessment results are obtained by repeating the identical experiment 10 times and calculating the average value, thereby avoiding the accidental results of the experiments. The specific experimental steps are shown in Fig. 2.

1) CLASSIFICATION RESULTS FOR BALANCED DATASETS

In the first experiment, a balanced datasets are established to verify the performance of the eight algorithms in the first and second datasets.

As suggested in Fig. 3 and Fig. 4, the efficiency of the eight algorithms is assessed using the accuracy, TPR, precision, and F-measure as metrics in the first and second datasets. In the balanced datasets, the index parameters of the eight algorithms all exhibit high performance, and I2FELM is the optimal performance.

2) CLASSIFICATION RESULTS FOR UNBALANCED DATASETS

In the second experiment, the unbalanced datasets are constructed to verify the performance of the eight algorithms.

In the first and second datasets, three unbalanced datasets proportions are built, 1:10, 1:20, and 1:50. Moreover, the accuracy, TPR, precision, and F-measure are exploited to evaluate the efficiency of the eight algorithms. The experimental results are shown in Fig. 5, 6, and 7.

From Fig. 5, 6, and 7, the assessment accuracy of the SVM, DT, RF, BP, RBF, ELM, and XGBoost algorithms tends to decline when the imbalance rate of the dataset increases. Besides, the variety of multiple parameter values of SVM and BP are the most obvious. For instance, the accuracy of SVM and BP drops from about 0.7692 and 0.7731 with the imbalance rate of 10 to 0.4886 and 0.5135 with the imbalance rate of 50 in the first dataset. The DT, RF and RBF perform the second poor, and the changes rate of DT, RF and RBF are relatively close. For instance, the reduction rate of TPR of DT, RF and RBF is 23%, 25% and 24% respectively, the accuracy of DT, RF and RBF changes from 0.8085, 0.8366 and 0.8168 in the case of imbalance rate equaling to 10 into 0.5492, 0.5618 and 0.5594 in the case of imbalance rate equals to 50 in the second dataset. The alterations of ELM and XGBoost generally exhibit an imbalance rate. For instance, the drop rate of accuracy is 30% and 26% with the imbalance rate ranging from 10 to 50 in the first dataset, and the precision of XGBoost decreases from 0.8831 in dataset 1 to 0.3985 in second dataset. The proposed I2FELM keeps the identical trend and the values of the five parameters change less. It is therefore reveals shows that the assessment performance of SVM, DT, RF, BP, RBF, ELM, and XGBoost algorithms on the unbalanced dataset requires enhancement, and I2FELM exhibits a better detection performance on the unbalanced dataset to introduce the fuzzy weight as a method to address the unbalanced problem, which can apply to each input and contribute to the learning of output weights.

3) FEATURE SELECTION DETECTION RESULTS

In this experiment, the tweet feature set in Table 1 is taken to train the classification model.

The SVM, DT, RF, BP, RBF, ELM, XGBoost, and I2FELM algorithms are tested using the top N (N=10 or 20) characteristics and a range of types of characteristics in Table 1. Among them, the information entropy method [44] is adopted

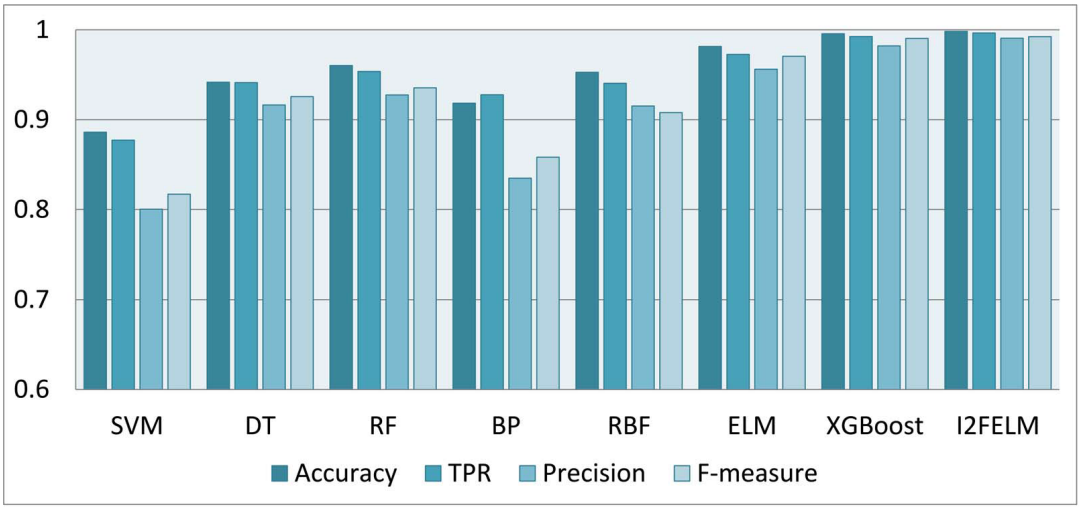


FIGURE 3. The comparison results of the first dataset.

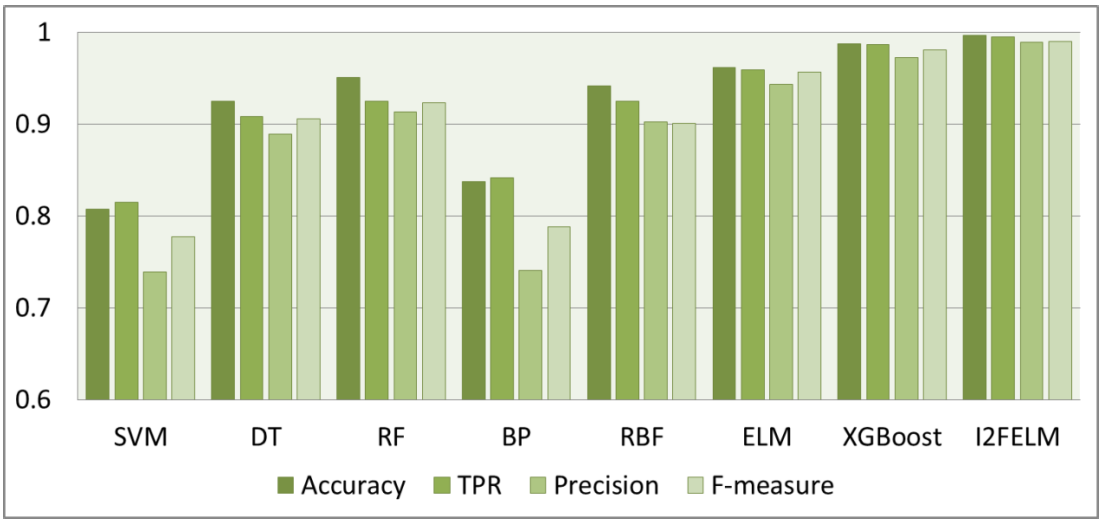
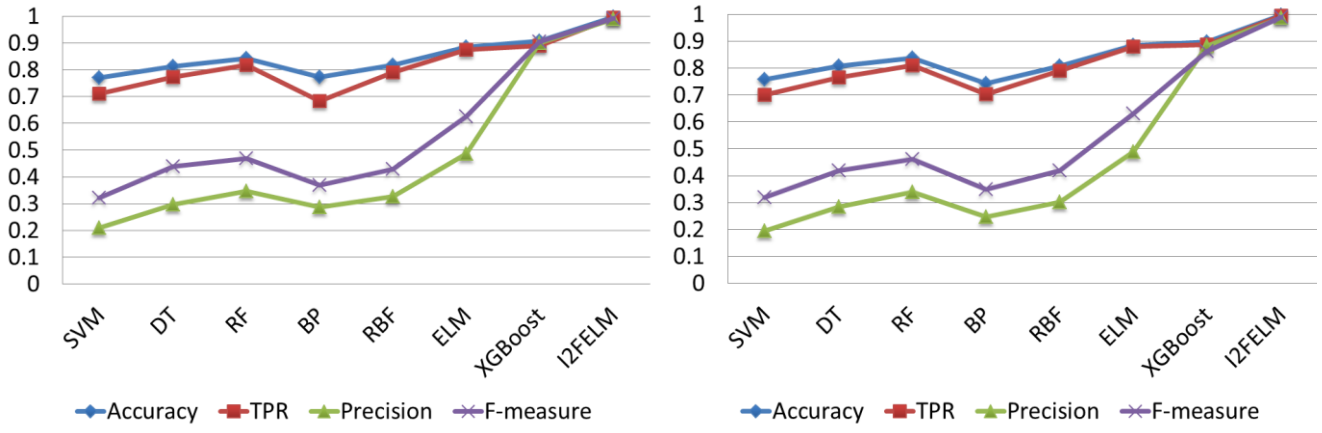


FIGURE 4. The comparison results of the second dataset.



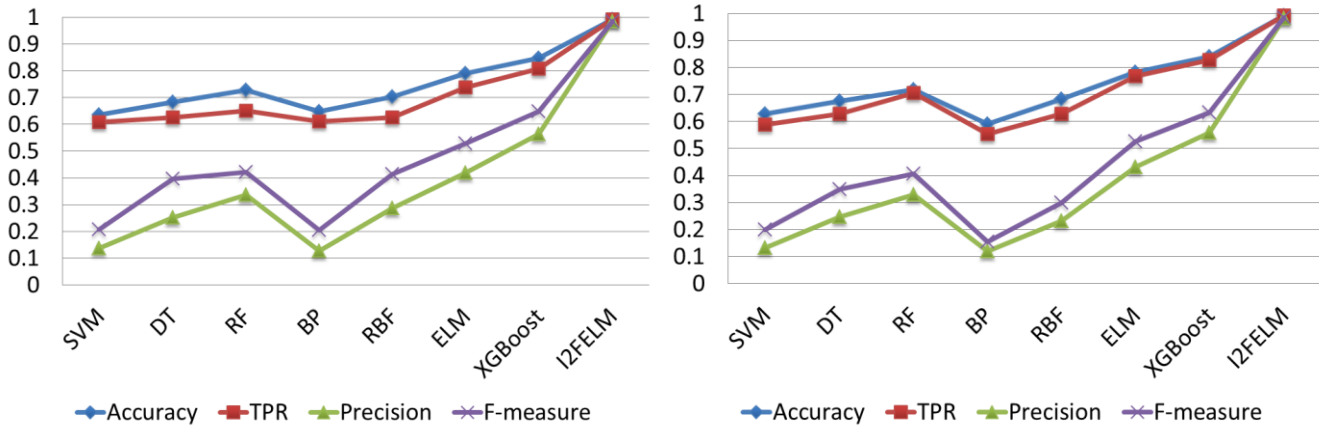
(a) the first dataset

(b) the second dataset

FIGURE 5. The comparison results with an imbalance ratio of 1:10 in two datasets.

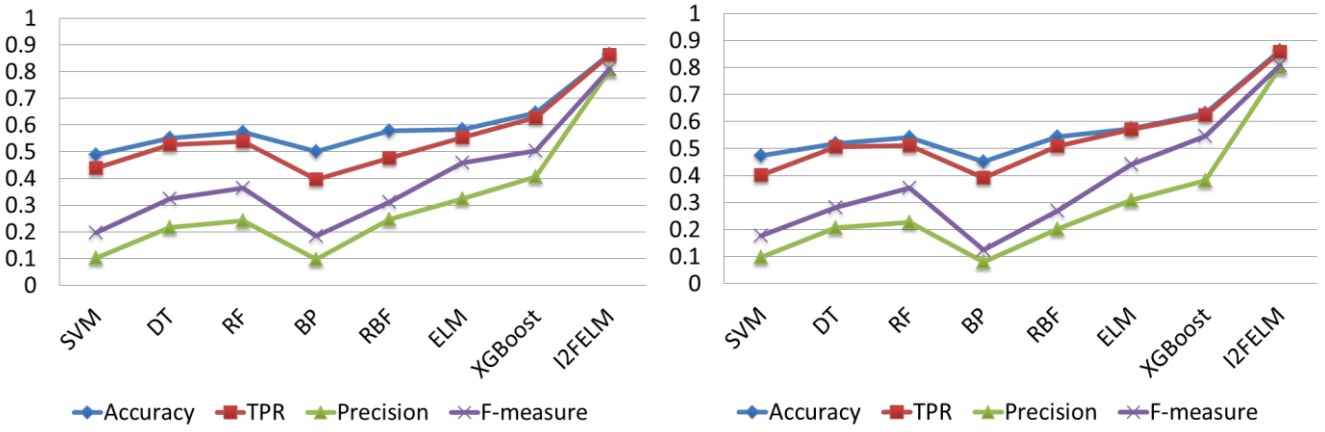
to calculate the top 10 and top 20 characteristics in Table 1. The average value of the results of 5 repeated experiments is extracted, and the classification effect is listed in Table 3 and Table 4.

Experiments show that certain classification characteristics can also be exploited to achieve certain classification effects. For instance, by selecting only 20 characteristics with the I2FELM method, the accuracy of more than 89% can be



(a) the first dataset (b) the second dataset

FIGURE 6. The comparison results with an imbalance ratio of 1:20 in two datasets.



(a) the first dataset (b) the second dataset

FIGURE 7. The comparison results with an imbalance ratio of 1:50 in two datasets.

TABLE 3. The classification results from different kinds of features in first dataset.

Algorithm	Accuracy (%)					
	Top 10	Top 20	Content	Activity	User attribute	Relationship
SVM	60.35	71.47	61.85	58.29	50.93	47.24
DT	66.29.	77.63	68.14	64.17	54.73	55.08
RF	70.43	80.55	72.67	66.25	56.92	57.63
BP	62.27	73.64	58.42	60.33	52.51	48.67
RBF	69.81	81.39	68.73	65.84	55.19	58.06
ELM	72.86	82.10	73.37	67.01	57.44	58.71
XGBoost	73.17	82.75	73.91	67.84	57.63	58.49
I2FELM	**82.14**	**90.06**	**82.57**	**75.29**	**64.91**	**66.52**

achieved in two datasets, which is close to the classification result achieved by exploiting all characteristics; With only the first 10 important characteristics, it can still achieve an accuracy of more than 81%, and the assessment accuracy is higher than any type of feature set individually. It is therefore proved that in the process of identifying spam users in social networks, comprehensive selection of a range of characteristics can achieve more effective assessment results than selecting a certain type of characteristics alone, and also proves the effectiveness of I2FELM feature selection.

TABLE 4. The classification results from different kinds of features in second dataset.

Algorithm	Accuracy (%)					
	Top 10	Top 20	Content	Activity	User attribute	Relationship
SVM	58.41	69.05	58.47	57.10	47.52	45.81
DT	65.33.	76.07	65.29	62.57	51.80	53.46
RF	68.97	79.01	71.15	65.24	53.73	55.82
BP	57.49	73.55	59.42	57.07	45.29	46.74
RBF	69.83	79.64	69.71	64.85	54.62	55.91
ELM	72.09	81.75	73.16	66.40	56.71	57.26
XGBoost	72.85	82.27	73.42	66.90	57.11	58.28
I2FELM	**81.73**	**89.70**	**82.13**	**74.86**	**63.52**	**66.17**

V. CONCLUSION AND FUTURE WORK

This study presents a novel Twitter spam detection method, in which the feature set consists of user attribute, content, activity and relationship in the online social network for identifying the real spam. Moreover, the spam assessment algorithm is I2FELM, which uses fuzzy weights to resolve an unbalanced data problem for the accuracy enhancement. Furthermore, Cholesky factorization without square root and composite kernel function are employed to enhance performance. Also, the reasonable number of hidden nodes can be automatically determined. By the validation of experience, the proposed I2FELM can apply to the multi-dimension balanced or unbalanced datasets, and it has achieved high performance to assess the spam in the online social network.

In the subsequent study, the emphasis will be placed on the following research directions. First, more factors will be considered to identify spam precisely (e.g., semantic analysis and emotion analysis). Also, we plan to exploit feature selection method and oversampling [21], [28], [29] to select a proper feature sets and improve model adaptation. On the other hand, to address insufficient labeled data in the social network, semi-supervised learning method will be substituted into I2FELM model to detect Twitter spam automatically based on a small amount of labeled data.

REFERENCES

[1] M. Chakraborty, S. Pal, R. Pramanik, and C. Ravindranath Chowdary, "Recent developments in social spam detection and combating techniques: A survey," *Inf. Process. Manage.*, vol. 52, no. 6, pp. 1053–1073, Nov. 2016.

[2] R. K. Dewang and A. K. Singh, "State-of-art approaches for review spammer detection: A survey," *J. Intell. Inf. Syst.*, vol. 50, no. 2, pp. 231–264, Apr. 2018.

[3] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in *Proc. CEAS*, vol. 6, 2010, p. 12.

[4] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in *Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR)*, 2010, pp. 435–442.

[5] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2010, pp. 1–9.

[6] A. H. Wang, "Don't follow me: Spam detection in Twitter," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Jul. 2010, pp. 1–10.

[7] Z. Chu, I. Widjaja, and H. Wang, "Detecting social spam campaigns on Twitter," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Cham, Switzerland: Springer, 2012, pp. 455–472.

[8] C. Meda, F. Bisio, P. Gastaldo, and R. Zunino, "A machine learning approach for Twitter spammers detection," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2014, pp. 1–6.

[9] B. Wang, A. Zubiaga, M. Liakata, and R. Procter, "Making the most of tweet-inherent features for social spam detection on Twitter," 2015, *arXiv:1503.07405*. [Online]. Available: http://arxiv.org/abs/1503.07405

[10] X. Zheng, Z. Zeng, Z. Chen, Y. Yu, and C. Rong, "Detecting spammers on social networks," *Neurocomputing*, vol. 159, pp. 27–34, Jul. 2015.

[11] C. Chen, J. Zhang, Y. Xie, Y. Xiang, W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian, "A performance evaluation of machine learning-based streaming spam tweets detection," *IEEE Trans. Comput. Social Syst.*, vol. 2, no. 3, pp. 65–76, Sep. 2015.

[12] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, "Statistical features-based real-time detection of drifted Twitter spam," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 914–925, Apr. 2017.

[13] H. He, A. Tiwari, J. Mehnen, T. Watson, C. Maple, Y. Jin, and B. Gabrys, "Incremental information gain analysis of input attribute impact on RBF-kernel SVM spam detection," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jul. 2016, pp. 1022–1029.

[14] S. Teng, N. Wu, H. Zhu, L. Teng, and W. Zhang, "SVM-DT-based adaptive and collaborative intrusion detection," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 108–118, Jan. 2018.

[15] T. Wu, S. Wen, Y. Xiang, and W. Zhou, "Twitter spam detection: Survey of new approaches and comparative study," *Comput. Secur.*, vol. 76, pp. 265–284, Jul. 2018.

[16] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[17] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1744–1772, 2nd Quart., 2019.

[18] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, and Y. Xiang, "Data-driven cyber security in perspective–intelligent traffic analysis," *IEEE Trans. Cybern.*, early access, Oct. 15, 2019, doi: 10.1109/TCYB.2019.2940940.

[19] R. Dayani, N. Chhabra, T. Kadian, and R. Kaushal, "Rumor detection in Twitter: An analysis in retrospect," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommuncations Syst. (ANTS)*, Dec. 2015, pp. 1–3.

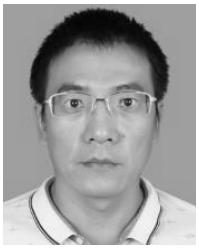
[20] J.-J. Sheu, Y.-K. Chen, K.-T. Chu, J.-H. Tang, and W.-P. Yang, "An intelligent three-phase spam filtering method based on decision tree data mining," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4013–4026, Nov. 2016.

[21] H. Liu, M. Zhou, and Q. Liu, "An embedded feature selection method for imbalanced data classification," *IEEE/CAA J. Automatica Sinica*, vol. 6, no. 3, pp. 703–715, May 2019.

[22] X. Zheng, X. Zhang, Y. Yu, T. Kechadi, and C. Rong, "ELM-based spammer detection in social networks," *J. Supercomput.*, vol. 72, no. 8, pp. 2991–3005, Aug. 2016.

[23] C. Meda, E. Ragusa, C. Gianoglio, R. Zunino, A. Ottaviano, E. Scillia, and R. Surlinelli, "Spam detection of Twitter traffic: A framework based on random forests and non-uniform feature sampling," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Aug. 2016, pp. 811–817.
[24] G. Lin, N. Sun, S. Nepal, J. Zhang, Y. Xiang, and H. Hassan, "Statistical Twitter spam detection demystified: Performance, stability and scalability," *IEEE Access*, vol. 5, pp. 11142–11154, 2017.
[25] S. Liu, Y. Wang, C. Chen, and Y. Xiang, "An ensemble learning approach for addressing the class imbalance problem in Twitter spam detection," in *Information Security and Privacy*, vol. 9722. Sydney, NSW, Australia: Springer, 2016, pp. 215–228.
[26] S. Liu, Y. Wang, J. Zhang, C. Chen, and Y. Xiang, "Addressing the class imbalance problem in Twitter spam detection using ensemble learning," *Comput. Secur.*, vol. 69, pp. 35–49, Aug. 2017.
[27] X. Wang, "Ladle furnace temperature prediction model based on large-scale data with random forest," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 4, pp. 770–774, 2017.
[28] W. Tang, Z. Ding, and M. Zhou, "A spammer identification method for class imbalanced weibo datasets," *IEEE Access*, vol. 7, pp. 29193–29201, 2019.
[29] X. Wang, Q. Kang, J. An, and M. Zhou, "Drifted Twitter spam classification using multiscale detection test on K-L divergence," *IEEE Access*, vol. 7, pp. 108384–108394, 2019.
[30] H. He, T. Watson, C. Maple, J. Mehnen, and A. Tiwari, "A new semantic attribute deep learning with a linguistic attribute hierarchy for spam detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, May 2017, pp. 3862–3869.
[31] M. Saini, S. Verma, and A. Sharan, "Multi-view ensemble learning using rough set based feature ranking for opinion spam detection," in *Advances in Computer Communication and Computational Sciences*. Singapore: Springer, 2019, pp. 3–12.
[32] X. Di, "A method for identifying malicious HTTP requests based on XGBoost," *Telecommun. Eng. Technol. Standardization*, vol. 31, no. 12, pp. 27–32, 2018.
[33] G.-B. Huang, Q.-Y. Zhu, and C.-K. Siew, "Extreme learning machine: Theory and applications," *Neurocomputing*, vol. 70, nos. 1–3, pp. 489–501, Dec. 2006.
[34] G.-B. Huang, H. Zhou, X. Ding, and R. Zhang, "Extreme learning machine for regression and multiclass classification," *IEEE Trans. Syst., Man, Cybern., B, Cybern.*, vol. 42, no. 2, pp. 513–529, Apr. 2012.
[35] T. Evgeniou, M. Pontil, and T. Poggio, "Regularization networks and support vector machines," *Adv. Comput. Math.*, vol. 13, no. 1, pp. 1–50, 2000.
[36] C.-F. Lin and S.-D. Wang, "Fuzzy support vector machines," *IEEE Trans. Neural Netw.*, vol. 13, no. 2, pp. 464–471, Mar. 2002.
[37] D. S. Bernstein, *Matrix Mathematics: Theory, Facts, and Formulas with Application to Linear Systems Theory*, vol. 41. Princeton, NJ, USA: Princeton Univ. Press, 2005.
[38] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[39] H. Costa, L. H. Merschmann, F. Barth, and F. Benevenuto, "Pollution, bad-mouthing, and local marketing: The underground of location-based social networks," *Inf. Sci.*, vol. 279, pp. 123–137, Sep. 2014.
[40] J. Oliver, P. Pajares, C. Ke, C. Chen, and Y. Xiang, "An in-depth analysis of abuse on Twitter," *Trend Micro*, vol. 225, pp. 1–22, Sep. 2014.
[41] D. M. W. Powers, "What the F-measure doesn't measure: Features, flaws, fallacies and fixes," 2015, *arXiv:1503.06410*. [Online]. Available: http://arxiv.org/abs/1503.06410
[42] H. S. Hota and A. K. Shrivas, "Data mining approach for developing various models based on types of attack and feature selection as intrusion detection systems (IDS)," in *Intelligent Computing, Networking, and Informatics*. Cham, Switzerland: Springer, 2014, pp. 845–851.
[43] S. Varadarajan, P. Miller, and H. Zhou, "Region-based mixture of gaussians modelling for foreground detection in dynamic scenes," *Pattern Recognit.*, vol. 48, no. 11, pp. 3488–3503, Nov. 2015.
[44] J. Zhao, X. Lei, X. Yang, and L. Guo, "A new method for identification of essential proteins by information entropy of protein complex and subcellular localization," in *Proc. Int. Conf. Swarm Intell.* Cham, Switzerland: Springer, 2019, pp. 282–291.

ZHIJIE ZHANG received the M.S. degree from Central China Normal University, China, in 2008, and the Ph.D. degree from the South China University of Technology, China, in 2017. She is currently a Lecturer with the School of Information Engineering, Lingnan Normal University, China. She has hosted and participated in many national and provincial scientific research projects. Her current research interests include social networks, machine learning, big data, and mobile computing.



RUI HOU received the master's degree from Chongqing University, China, in 2005. He was a Visiting Scholar with the South China University of Technology, China, in 2016. He is currently a Lecturer with the School of Information Engineering, Lingnan Normal University, China. His current research interests include machine learning, social networks, spatial reasoning, and qualitative reasoning. He is a member of the China Computer Federation.

JIN YANG received the Ph.D. degree from the School of Computer Science, College of Computer Science and Engineering, South China University of Technology, China, in 2017. He is currently an Associate Professor with Guangdong Pharmaceutical University, China. His current research interests include machine learning, evolutionary computation, global optimization, and multi-objective optimization.