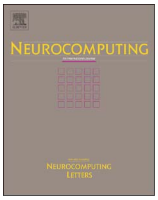
Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom



Discovering social spammers from multiple views

Hua Shen[a,d], Fenglong Ma[c], Xianchao Zhang[b,*], Linlin Zong[a,b], Xinyue Liu[b], Wenxin Liang[b]

[a] *School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China*
[b] *School of Software, Dalian University of Technology, Dalian 116620, China*
[c] *SUNY at Buffalo, Buffalo, NY 14221, USA*
[d] *College of Mathematics and Information Science, Anshan Normal University, Anshan 114007, China*

ARTICLE INFO

Communicated by Peng Cui

Keywords:
Social spammer detection
Multi-view learning
Social regularization term

ABSTRACT

Online social networks have become popular platforms for spammers to spread malicious content and links. Existing state-of-the-art optimization methods mainly use one kind of user-generated information (i.e., single view) to learn a classification model for identifying spammers. Due to the diversity and variability of spammers' strategies, spammers' behavior may not be completely characterized only by single view's information. To tackle this challenge, we first statistically analyze the importance of considering multiple view information for spammer detection task on a large real-world Twitter dataset. Accordingly, we propose a generalized social spammer detection framework by jointly integrating multiple view information and a novel social regularization term into a classification model. To keep the completeness of the original dataset and detect more spammers by the proposed method, we introduce a simple strategy to fill the missing data for each view. Experimental results on a real-world Twitter dataset show that the proposed method outperforms the existing methods significantly.

1. Introduction

Online social networks (OSNs), such as Twitter and Facebook, have become popular platforms to disseminate and share information [1]. Unfortunately, social spammers take advantage of those platforms to spread phishing scams, publish malicious content and links, and promote commodity information [2–4]. According to a study by Nexgate [5], the number of social spam grew more than 355% from January to July of 2013, which means that one in two hundred social messages was a spam, and 15% of all spams contained URLs linking to risky websites. Spammers are so sophisticated and concealed that they change spamming strategies irregularly and try to disguise as legitimate users. Moreover, to increase their influence and be undetected, spammers collude with each other to construct the criminal communities [6]. The malicious behavior of spammers has not only hindered the OSNs' development largely [7], but also threatened information security and personal privacy [8]. Therefore, it is crucial to design effective and novel spammer detection methods for the development of social systems.

Traditional approaches for combating spammers mainly focus on analyzing and extracting users' features, and then applying the existing classification methods to detect spammers or spam campaigns [3,9–11]. As the spamming strategies evolve, these methods only relying on the features could not effectively detect spammers with new spamming strategies. Ranking schemes are also employed in some anti-spam measures using social network information, which can decrease the spammers' impact on legitimate users [12,13]. However, these ranking methods are hard to distinguish legitimate users and spammers only depending on network information.

The state-of-the-art approaches employ supervised machine learning techniques to train an optimization model using both user-generated content and network structures [14–16,8], which identify spammers more accurately than the traditional approaches. However, these optimization methods only rely on one kind of user-generated information, such as text features, URLs or hashtags (i.e., *single view*). As we all known, spam strategies are diverse and protean so that the single view information may not characterize spammers' behavior completely. For example, some spammers may post legal text but adding unfriendly shorten URLs or tempting hashtags to achieve their malicious purposes. Consequently, these spammers would not be correctly identified by existing approaches. Thus, it is more reasonable and challenging to take multiple perspectives of spammers’ behavior (i.e., *multiple views*) into consideration when detecting spammers.

To tackle the aforementioned challenges, we propose a generalized spammer detection framework, named **Multi-View Learning for Social Spammer Detection** (MVSD), by taking advantage of multiple view information of users and network information as shown in Fig. 1. We first statistically analyze the distribution differences between

* Corresponding author.
E-mail address: xczhang@dlut.edu.cn (X. Zhang).

http://dx.doi.org/10.1016/j.neucom.2016.11.013
Received 23 March 2016; Received in revised form 18 October 2016; Accepted 7 November 2016
Available online xxxx
0925-2312/ © 2016 Published by Elsevier B.V.

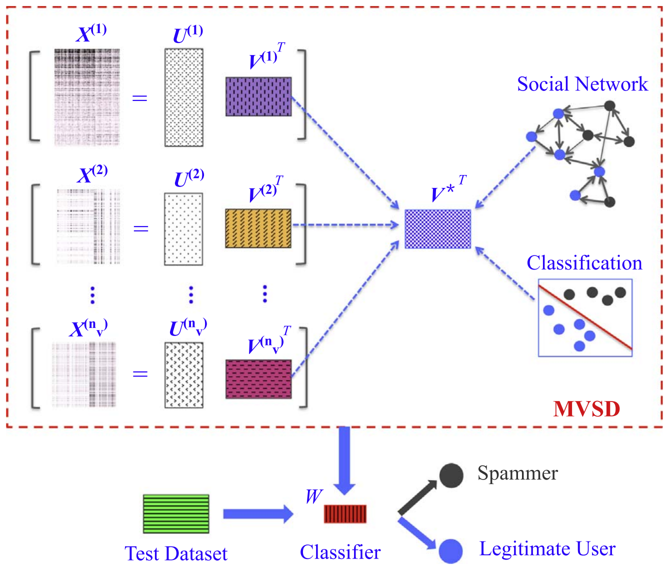


Fig. 1. The Framework of MVSD.

spammers and legitimate users from three views (text, URL and hashtag information) extracted from users' tweets. Based on the statistical analysis, we observe that different information has different ability to characterize users. Thus, we employ multi-view learning, which assigns different weight to each view. Since the values of features are non-negative, multi-view NMF can be used to learn a consensus matrix representing users' features. The proposed MVSD also takes social relationships into consideration, which measures the pairwise interactions among users. Different from existing work [14–16], we model all types of social relationships between legitimate users and spammers. Furthermore, in order to keep the completeness of the dataset, we use a simple method to fill in all the missing feature values. Finally, we jointly integrate users' multiple features and social relationships into a classification model to learn the classifier iteratively on the complemented dataset.

In summary, the contributions of this paper are as follows:

- The paper makes in-depth empirical analysis on a large real-world Twitter dataset, and the statistical results show that different views' feature distributions between legitimate users and spammers are different. Thus, it is reasonable to consider multiple view information of users when detecting spammers.
- The novelty of the paper is proposing a generalized spammer detection framework[1] by jointly modeling multiple view information and a novel social regularization term into a classification model. Through iteratively learning among multiple view information, social regularization and classification model, the proposed MVSD can train an accurate classifier.
- The experimental results on a real-world dataset show that the proposed framework can identify more spammers compared with baseline approaches. We conduct experiments to demonstrate the significance of taking multiple view information into consideration and validate the effectiveness of the new social regularization term. Finally, the importance of complementing missing values for spammer detection task is illustrated by the experimental results.

The remained of this paper is organized as follows: Section 2 analyzes different information from multiple views in OSNs. Section 3 formally defines the problem of multi-view spammer detection. In Section 4, we propose a multi-view learning model based on joint nonnegative matrix factorization. Section 5 demonstrates our evaluation process and experimental results. Section 6 reviews the related work on social spammer detection. The last section concludes the discussion.

2. Data analysis

We first introduce the dataset used in this paper, then statistically demonstrate the rationality of using multi-view method, and finally illustrate the importance of handling missing values for spammer detection task.

2.1. Dataset

In order to validate the proposed method impersonally and fairly, we select a standard and public dataset, Twitter Social Honeypot Dataset [17]. It has been used in [16,18,9], which provides the ground truth data, i.e., labeling users as spammer or legitimate ones, but only a *part* of following relationships. In order to complete the whole following relationships among users, we use the other public dataset, the Kwak's dataset [19][2]. We filter the non-English tweets and the users who posted less than one tweet. We also parse the shortened URLs to the original formats (i.e., long URLs) and only leave the hostname for each long URL. After processing, the final dataset contains 10,080 users (4,414 spammers and 5,666 legitimate users). For each user, we extracted features of text (9,749), URL (4,410) and hashtag (3,491) information.

2.2. Importance of multiple view information

Previous researches have shown that text information can be used to detect spammers effectively [15,16,20,21]. However, we find that not only text information but URLs and hashtags can also help to identify spammers as well. Moreover, they have different abilities to characterize spammers' behavior. For example, some spammers try to post duplicate or similar tweets to increase the probability of successfully alluring legitimate users, i.e., text spamming. Though some spammers publish normal text, the malicious URLs are embedded in the tweets, which is difficult to be detected. This is URL spamming. The third type of spamming is using hashtags, which adds the trending hashtags in the tweets to lure legitimate users to read or retweet them. These three spamming strategies are commonly used by spammers. Thus, we select text, URL and hashtag features as different views to describe users.

To further demonstrate the rationality of applying multiple view information to detect spammers, we first give an intuitive analysis by matrix graph [22] shown in Fig. 2. For each subfigure, X-axis represents users' features that we extracted for each view and Y-axis denotes users' classes (spammers and legitimate users). Each point in the matrix graph represents a feature's attribute value of each user in a single view. Ideally, the greater the color difference of points between the two classes of users, the better the classification performance of the view. We can observe that the distributions of spammers and legitimate users in text view are more similar compared with those in the other two views. It means that URLs and hashtags can be used to characterize the difference between spammers and legitimate users more effectively and separate the users into different classes more easily.

From statistical perspective, a non-parametric method, Spearman rank test, is employed to measure the difference of different views between spammers and legitimate users. The coefficient of spearman rank test r is from −1 to +1. Ideally, the closer the coefficient is to −1, the easier it is to separate users into different classes. Let n_i denote the number of the i-th attribute (word/URL/hashtag) posted by legitimate users and s_i denote the number of the i-th attribute published by spammers. We randomly select 10,000 pairs of such attributes (i.e.,

[1] The code can be downloaded from http://www.acsu.buffalo.edu/fenglong/.

[2] Note that this dataset is only used to complete the following relationships as [18].

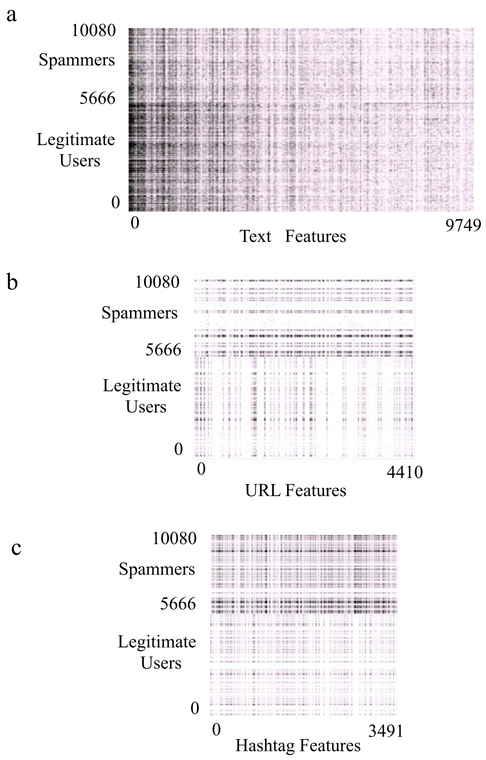


Fig. 2. Matrix Graph of Three Views.

$\{n_i, s_i\}_{i=1}^{10000}$) as the sample set. Then, we calculate the spearman coefficient r on this sample set. For text information, the coefficient r is 0.562 with significant level (2-tail) $\alpha = 0.01$ and $p < 0.001$, which means that it is difficult to determine a user's label based on text information. However, the coefficients are −0.602 and −0.569 with significance level (2-tail) $\alpha = 0.01$ and $p < 0.001$ for URLs and hashtags correspondingly. It means that the feature distributions of legitimate users and spammers are different and separate moderately, i.e., we can use URL or hashtag information to distinguish users easily.

The statistic analysis indicates that we should consider multiple complementary information simultaneously to improve the performance of spammer detection.

2.3. Significance of information complement

Based on the above analysis, we know that URLs and hashtags play important roles when identifying spammers. However, not all the users have URL or hashtag information, i.e., existing missing values in the dataset. Fig. 3 shows the cumulative distribution function (CDF) of users' URL and hashtag information. We can observe that over 10% users do not post any URLs and over 20% users do not publish any hashtags in their tweets, which means that we need to remove at least 20% users to keep all the three views with the same size of non-empty data. Therefore, we should complement these missing values to keep data completeness and identify more spammers.

However, complementing multiple views' data simultaneously is a big challenge. Intuitively, we can complete the missing data based on homophily theory [23,24], i.e., the user's feature distributions should be similar with their neighbors' on the social networks. We extract the three non-negative feature matrices from the different views in the dataset. For text view, we use bag-of-words and take tf-idf as feature's values. For URL and hashtag views, the frequency of each URL or hashtag posted by users is extracted as their features' values. Accordingly, we propose a simple measure to fill the missing values. The complementing procedure works as follows. We consider users without feature distributions of either URL or hashtag. The only information we can use is the text distributions. We calculate the similarities between the user and its neighbors using Euclidean distance, then select the most similar user's distribution as the user's. For those users with two kinds of information (text and URL/hashtag), we calculate the similarities for the user with its neighbors on text distributions and URL/hashtag distributions respectively. Top-N (N=10) most similar users are selected as the candidates from two sets separately. If common users exist in the two Top-N sets, then we select the distributions of the user with the minimum distance as the missing value user's. If the intersection is empty, we simply select the distribution of the user with the minimum distance in the two Top-N sets as the user's.

3. Problem definition

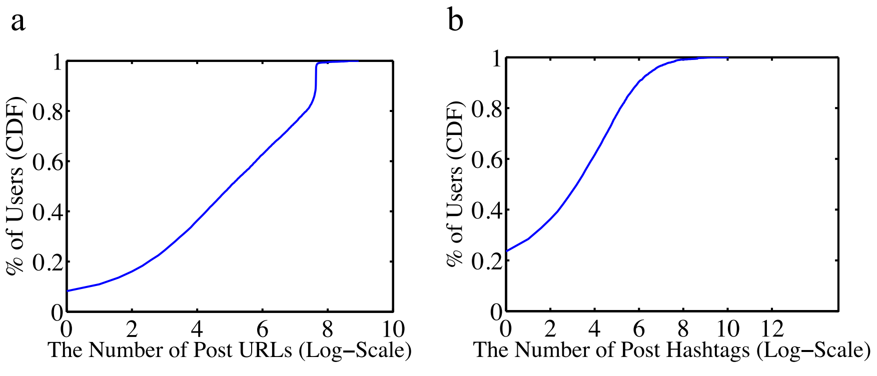
In this section, we introduce the terminologies used in this paper firstly and then formally define the problem of multi-view spammer detection.

Input

The inputs of the proposed model are multiple views' information X, social network information R and labeled data set Y.

Definition 1. The multi-view information is denoted by $X = \{X^{(1)}, X^{(2)}. \ldots, X^{(n_v)}\}$, where n_v is the number of views and $X^{(v)}$ is the non-negative feature matrix of the v-th view. For each view, $X^{(v)} \approx U^{(v)}(V^{(v)^T})$, where $U^{(v)} \in \mathbb{R}^{|U^{(v)}|\times K}$ is the latent feature matrix, $V^{(v)} \in \mathbb{R}^{N\times K}$ is the latent user matrix, $|U^{(v)}|$ is the number of attributes of the v-th view, K is the number of latent features, and N is the number of users (i.e., all the views have the same number of users).

Definition 2. Social network information $R = (V, E)$ denotes users' following relationships, where V is the user set and E is the edge set. $v_j \in Friends(v_i)$ means that user v_i follows user v_j, i.e., there is a direct edge from v_i to v_j.



URLs

Hashtags

Fig. 3. The Number of Post URLs and Hashtags.

Definition 3. $Y \in \mathbb{R}^{l \times c}$ denotes the identity labeled matrix (supervised information), where $l\,(l < N)$ represents the number of labeled users and c represents the number of classes. In this paper, we focus on the binary classification problem, i.e.,c=2. The users will be classified as spammers or legitimate users. If user u_i is a spammer, $Y_i = (-1\ 0)$; otherwise, $Y_i = (0\ 1)$.

Output

The goal of our work is to learn a classification model W which can be used to identify unknown malicious or legitimate users.

Definition 4. W is a classifier learned by the proposed method to detect social spammers with multiple views' information.

With the given notations, we formally define the problem of social spammer detection as follows:

Problem 1. Given the multi-view information X, social network information R, and labeled information Y, our task is to learn a classifier W to automatically classify unknown users as spammers or legitimate users.

4. Multi-view learning for social spammer detection

The basic idea of the proposed model is making full use of multiple view information and social relationships to train an effective classifier. As shown in Fig. 1, each view's information $X^{(v)}$ $(v \in 1,\ldots,n_v)$ can be factorized into $U^{(v)}$ and $V^{(v)}$, and then $\{V^{(v)}\}_{v=1}^{n_v}$ can be modeled into a consensus matrix V^* by considering social network information and the provided labels. Through the iterative learning, we can obtain a reasonable and accurate classification model for detecting spammers. The advantage of this framework is that multi-view learning and labeled information can help the classifier achieve better performance, and in turn, labeled information and classification can guide a better factorization of multi-view learning.

In this section, we first discuss how to model a consensus matrix from multiple view information and then propose a new social regularization term to model social network information. Finally, a novel and generalized spammer detection framework is proposed, which integrates multi-view learning, social regularization and classification simultaneously.

4.1. Multi-view learning

Based on the observation in Data Analysis (Section 2), we know that text, URL and hashtag information all can be used as features to train a classifier effectively. Next, a concrete example is given to illustrate the importance of considering multiple view information when detecting spam.

Example 1. There is a tweet extracted from the Twitter Social Honeypot Dataset, “Earth friendly beauty #sale http://tinyurl.com/3yznmhs”.

The content of this tweet is “Earth friendly beauty”, which is very similar to the legitimate users'. So, it is hard to identify this spammer only depending on the text features. However, we observed that the hashtag “sale” is posted by spammers frequently, and the shortened URL actually links to a promoted website which few legitimate users post. Obviously, simultaneously taking multiple views' features into account may improve the performance, i.e., identifying spammers more accurately.

A straightforward method is concatenating all the features or views together, but this simple approach may fail: (1) The scale or type of each feature is different. Some features may be boolean, such as URL or Hashtag, but some features may be numerical values, such as the frequency or TF-IDF of words. It may lead to training an incorrect classifier and cannot achieve a good predicting performance. (2) The weight of different features may be unequal. Since there exist many kinds of spamming strategies, some spammers post spam terms, but some publish unfriendly URLs. Therefore, it is important to distinguish the weight of views to capture spammers with different types.

Based on the above analysis and motivated by MultiNMF [25], we integrate multiple views' features into a consensus feature matrix. Different from MultiNMF, a clustering method, the final goal of our task is to learn a classifier for identifying spammers. So, we modify the objective function of MultiNMF by adding regularization terms to avoid overfitting when training the classifier. The objective function of multi-view learning is as follows.

$$
\begin{aligned}
O_M = {} & \frac{1}{2}\sum_{v=1}^{n_v} \beta^{(v)}[\|X^{(v)} - U^{(v)}(Q^{(v)})^{-1}Q^{(v)}(V^{(v)})^T\|_F^2 \\
& + \lambda^{(v)}\|V^{(v)}Q^{(v)} - V^*\|_F^2] + \frac{\lambda_f^*}{2}\|V^*\|_F^2 \\
& + \frac{\lambda_f}{2}\sum_{v=1}^{n_v}(\|U^{(v)}\|_F^2 + \|V^{(v)}\|_F^2) \\
s.\,t.\ \ \forall\ \ & 1 \le v \le n_v,\ U^{(v)} \ge 0,\ V^{(v)} \ge 0,\ V^* \ge 0,\ \sum_{v=1}^{n_v} \exp^{-\beta^{(v)}} = 1, \\
Q^{(v)} = {} & Diag\left[\sum_{i=1}^{M} U_{i,1}^{(v)}, \sum_{i=1}^{M} U_{i,2}^{(v)}, \ldots, \sum_{i=1}^{M} U_{i,K}^{(v)}\right]
\end{aligned}
\tag{1}
$$

where $\beta^{(v)}$ is the weight of view v, $\lambda^{(v)}$, λ_f^* and λ_f are the regularization coefficients, and $Q^{(v)}$ is a diagonal matrix. From Eq. (1), we can observe that it is to normalize each latent feature matrix $V^{(v)}$ and then unify them into the consensus matrix V^*, which satisfies the above analysis. If let $\beta^{(v)} = 1$ and $\beta^{(v')} = 0$ $(v' \in \{1,\ldots,v-1, v+1,\ldots,n_v\})$, then $V^* = V^{(v)}$, which is the same as the input of existing methods. Therefore, V^* can be seen as the linear combination of all the feature matrices.

4.2. Social regularization

For online social network users, they can construct following relationships easily. Previous studies have shown that users' social relationships could be exploited to regularize the decomposition of the feature matrix [14,16], which leads to improving the performance of identifying spammers.

There are four kinds of relationships between legitimate users and spammers as shown in Fig. 4(a): legitimate user → legitimate user ($L_1 \rightarrow L_2$ and $L_2 \rightarrow L_1$), legitimate user → spammer ($L_2 \rightarrow S_2$), spammer → legitimate user ($S_1 \rightarrow L_1$) and spammer → spammer ($S_1 \rightarrow S_2$ and $S_2 \rightarrow S_1$). Fig. 4(b) shows the social relationships used in [14]. They

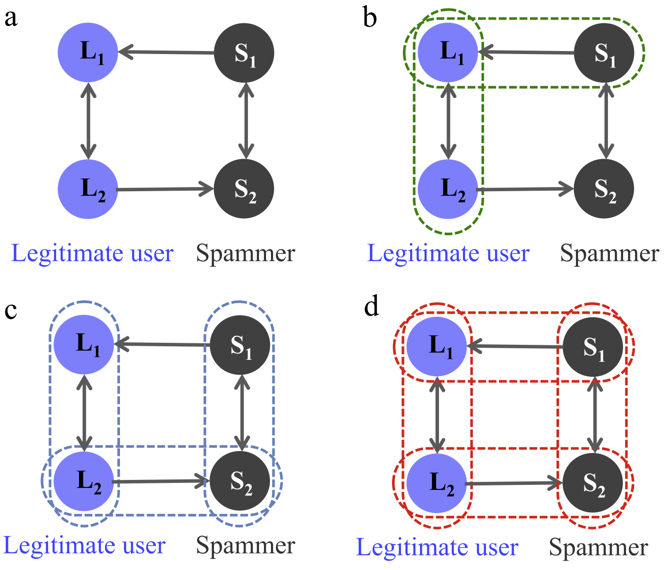


Fig. 4. Social Relationships among Users.

claimed that spammers' behavior is different from their friends' significantly, and conversely, legitimate users usually have similar behavior with their friends. It means that they considered two relationships: legitimate user → legitimate user and spammer → legitimate user. However, spammers may construct sophisticatedly their inner communities for hiding themselves, and many legitimate users could follow spammers for amassing their social influence or out of courtesy [12,13]. So, we need to consider the other two types of relationships. In [15,16], they considered three types of relationships: legitimate user → legitimate user, legitimate user → spammer and spammer → spammer (Fig. 4(c)), and the social regularization term will incur a penalty if two users who have different **predicted labels** when they are close to each other in the graph. Since we employ **the real labels** into the social regularization term, their approaches are quite *different* from [14] and the proposed model.

Based on the above analysis, we all know that it is vital to provide different methods to model the all four types of users' relationships as shown in Fig. 4(d). Different from existing social regularizations, we proposed a novel social regularization as follows.

$$O_S = \sum_{v_i} \sum_{v_j \in Friends(v_i)} [\mathbf{I}(Y_i, Y_j)(V_i^* - V_j^*)(V_i^* - V_j^*)^T \quad + 2\mathbf{I}'(Y_i, Y_j) \\ V_i^*(V_j^*)^T] \tag{2}$$

where $\mathbf{I}$ and $\mathbf{I}'$ are:

$$\mathbf{I}(Y_i, Y_j) = \begin{cases} 1 & \text{if } Y_i = Y_j \\ 0 & \text{otherwise} \end{cases}, \mathbf{I}'(Y_i, Y_j) = \begin{cases} 1 & \text{if } Y_i \neq Y_j \\ 0 & \text{otherwise} \end{cases}.$$

We can see that if both user v_i and v_j belong to the same class, i.e., Y_i=Y_j, the distance of these two users would be reduced; otherwise, the distance may be enlarged. Hence, the proposed social regularization term satisfies the above analysis to provide different types' constraints of user pairs on social networks.

4.3. MVSD: multi-view learning for social spammer detection

The ultimate goal of the proposed method is to learn an accurate and effective classifier by integrating multiple view information and utilizing social relationships to predict unlabeled users' categories. We employ Support Vector Machines (SVM) with smoothing hinge loss as the classification model. Hence, the final objective function builds on Eqs. (1) and (2) with SVM, i.e.,

$$O = O_M + \frac{\lambda_s}{2} O_S + \alpha \sum_{i=1}^{\ell} h(Y_i(W(V_i^*)^T)) + \frac{\lambda_w}{2} \|W\|_F^2 \tag{3}$$

where the smoothing hinge loss function is

$$h(z) = \begin{cases} \frac{1}{2} - z & z \le 0 \\ \frac{1}{2}(1 - z)^2 & 0 < z < 1, \\ 0 & z \ge 1 \end{cases}$$

where λ_s is the coefficients of social regularization, α is the coefficient of classification, and λ_w is the regularization coefficient.

Using the objective function Eq. (3), we can obtain all the users' consensus vector $\{V_n^*\}_{n=1}^N$. For a new unknown user u_k, we can use the learned V_k^* and the trained classifier W to predict its label. The u_k's label is obtained from $W(V_k^*)^T$. The output of $W(V_k^*)^T$ is a weight vector $(w_1\ w_2)^T$. If $w_1 + w_2 < 0$, the user u_k will be predicted as a spammer; otherwise, u_k will be predicted as a legitimate user.

From Eq. (3), we can observe that the consensus matrix V^* learned by multi-view learning can influence the performance of classification, in turn, the accurate classification model W can lead to learning a better consensus matrix V^*. Also, the social regularization can provide constraints to help multi-view learning and classification procedures. Therefore, the proposed MVSD can simultaneously learn among the three parts to achieve better performance.

4.4. Optimization

In the process of optimization, we apply an iterative updating procedure to solve the objective function Eq. (3) until its convergence as follows. First, we minimize O to get $U^{(v)}$ and $V^{(v)}$ by fixing V^* and $\beta^{(v)}$. Then, using gradient descent method updates V^* and W by fixing $U^{(v)}$, $V^{(v)}$ and $\beta^{(v)}$. Finally, $\beta^{(v)}$ is updated by using $U^{(v)}$, $V^{(v)}$ and V^*. The details are introduced in the following.

Computing $U^{(v)}$ and $V^{(v)}$: Since $U^{(v)}$ and $V^{(v)}$ are non-negative and only appear in O_M(Eq. (1)), we can use multiple update rules to solve them. Multiplicative update rules [26] are a good compromise between speed and ease of implementation for solving NMF. Following the multiplicative and alternating updating rules introduced in [25,26], we can use the following updating rules to solve $U^{(v)}$ and $V^{(v)}$ by fixing V^*.

$$U_{i,k}^{(v)} \leftarrow U_{i,k}^{(v)} \frac{\beta^{(v)}(X^{(v)}V^{(v)})_{i,k} + A}{\beta^{(v)}(U^{(v)}(V^{(v)})^T V^{(v)})_{i,k} + B} \tag{4}$$

$$V_{j,k}^{(v)} \leftarrow V_{j,k}^{(v)} \frac{\beta^{(v)}((X^{(v)})^T U^{(v)})_{j,k} + \lambda^{(v)}\beta^{(v)}V_{j,k}^*}{\beta^{(v)}(V^{(v)}(U^{(v)})^T U^{(v)})_{j,k} + \lambda^{(v)}\beta^{(v)}V_{j,k}^{(v)} + \lambda_f V_{j,k}^{(v)}} \tag{5}$$

where

$$A = \lambda^{(v)}\beta^{(v)} \sum_{j=1}^{N} V_{j,k}^{(v)} V_{j,k}^*, B = \lambda^{(v)}\beta^{(v)} \sum_{l=1}^{M} U_{l,k}^{(v)} \sum_{j=1}^{N} (V^{(v)})_{j,k}^2 + \lambda_f U_{j,k}^{(v)}.$$

Computing V^* and W: Since V^* is related to not only $U^{(v)}$ and $V^{(v)}$ but also W, it is difficult to solve V^* by employing multiplicative update rules. Thus, we use stochastic gradient descent (SGD) to update V^* and W sequentially. We derive the gradients of V^* and W as follows.

$$\frac{\partial O}{\partial V_i^*} = \sum_{v=1}^{n_v} (-\lambda^{(v)}\beta^{(v)}(V_i^{(v)}Q^{(v)} - V_i^*)) + \alpha h'(Y_i(W(V_i^*)^T))Y_i W \\ + \lambda_s \sum_{v_j \in Friends(v_i)} [\mathbf{I}(V_i^*, V_j^*)(V_i^* - V_j^*) + \mathbf{I}'(V_i^*, V_j^*)V_j^*] + \lambda_f^* V_i^* \frac{\partial O}{\partial W} \\ = \alpha \sum_{i=1}^{n} h'(Y_i W(V_i^*)^T) Y_i V^* + \lambda_w W$$

where the gradient of the smoothing hinge loss $h(z)$ is

$$h'(z) = \begin{cases} -1 & z \le 0 \\ z - 1 & 0 < z < 1. \\ 0 & z \ge 1 \end{cases}$$

The solutions of $V^{(*)}$ and W lead to the following update rules:

$$V_i^* \leftarrow V_i^* - \eta \frac{\partial O}{\partial V_i^*} \tag{6}$$

$$W \leftarrow W - \eta \frac{\partial O}{\partial W} \tag{7}$$

where η is the learning rate in the procedure of SGD.

Computing $\beta^{(v)}$: Based on Lagrange multiplier, $\beta^{(v)}$ has the solution as follows.

$$\beta^{(v)} = -\log \frac{RE}{\sum_{v=1}^{n_v} RE} \tag{8}$$

where

$$RE = \|X^{(v)} - U^{(v)}(Q^{(v)})^{-1}Q^{(v)}(V^{(v)})^T\|_F^2 + \lambda^{(v)}\|V^{(v)}Q^{(v)} - V^*\|_F^2.$$

We present the proposed algorithm of multi-view learning for social spammer detection in Algorithm 1.

Algorithm 1. *MVSD Algorithm*

```
Input: Multiple view information { $X^{(1)}, X^{(2)}, \ldots, X^{(n_v)}$}; Views' weight { $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(n_v)}$}; Social relation matrix $R$; Labeled data $Y$;
```

```
Number of latent features $K$; Learning rate $\eta$
    Normalize each view $X^{(v)}$ such that $\| \sum_j X_j^{(v)} \| = 1$;
    Initialize $U^{(v)}$, $V^{(v)}$ and $V^*$ $(1 \le v \le n_v)$;
    while $O$ not converged do
    for $v$=1 to $n_v$ do
        while $O$ not converged do
        Update $U^{(v)}$ according to Eq.(4);
        Normalize $V^{(v)}$ and $U^{(v)}$;
        Update $V^{(v)}$ according to Eq.(5);
        end while
    end for
    while $O$ not converged do
        Update $V_i^*$ according to Eq.(6);
        Update $W$ according to Eq.(7);
    end while
    Update $\beta^{(v)}$ according to Eq.(8);
    end while
Output: Basis matrices $\{U^{(1)}, U^{(2)}, \ldots, U^{(n_v)}\}$; Coefficient matrices
$\{V^{(1)}, V^{(2)}, \ldots, V^{(n_v)}\}$; Consensus matrix $V^*$; View weight vector
$\{\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n_v)}\}$; Classification weight matrix $W$
```

5. Experiments

Extensive experiments are conducted to illustrate the effectiveness of the proposed method MVSD in this section. We first introduce baselines and experimental setup. Next, experimental results on spammer detection are shown that the performance of MVSD is better than that of baselines. Finally, we qualitatively analyze the importance of complementing the missing values. The complemented form of the dataset is used for all methods, except experiments in Section 5.5 (i.e., Clean Dataset).

5.1. Baselines and experimental setup

We compare the proposed MVSD with three categories' methods to demonstrate the advantage of employing multiple view information for spammer detection task.

- **Single view methods** TEXT$_{svm}$, URL$_{svm}$ and HASHTAG$_{svm}$ use single view's information as features respectively and SVM as classification method to identify spammers.
- **Optimization methods** SMFSR [14] and SSDM [15] are the two state-of-the-art optimization methods to detect spammers. In the following experiments, we use text information as their input. The details of these methods are introduced in the related work part.
- **Combination methods** CONCATENATE$_{svm}$ is a simple baseline, which only combines three views' information into one feature matrix as SVM's input. MULTINMF+SVM learns the consensus matrix V^* according to Eq. (1) and the social regularization (Eq. (2)) firstly, then we apply SVM on V^* to train the classifier, and finally unlabeled users are identified base on the learned classifier.

We use precision, recall and F$_1$-score to measure the performance of methods. Also, we empirically set $\lambda^{(v)} = 0.5$, $\lambda_s = 0.2$, $\lambda_w = 0.3$, $\lambda_f^* = 0.1$, $\lambda_f = 0.2$, $\alpha = 0.1$, K=800 and $\eta = 0.001$ in the following experiments.

5.2. Performance evaluation

Table 1 shows experimental results of the proposed MVSD and baseline methods on the real-world Twitter dataset. We vary the size of training dataset to observe the performance's trend, where “Training Data One (30%)” means that we randomly select 30% data from the whole dataset as training set and the remaining 70% data as testing set. All the results listed in Table 1 average the results of 10 runs of the experiment under different random splits.

From Table 1, we can observe that the precision and F$_1$-score of the proposed MVSD outperform those of all the baseline methods on different size of the training set, especially on “Training Data One (30%)”. Though the single view's methods (TEXT$_{svm}$, URL$_{svm}$ and HASHTAG$_{svm}$) can identify spammers effectively, they ignore other useful information to improve the performance. Also, the results of URL$_{svm}$ and HASHTAG$_{svm}$ can validate the assumption we discussed in Data Analysis (Section 2), i.e., the performance of URL (on recall) and hashtag (on precision, recall and F$_1$-score) is better than text information's when detecting spammers. Moreover, we observe that the recall of URL$_{svm}$ is better than MVSD. This is because URL$_{svm}$ may label a user as spammer if the user ever posted a few malicious URLs. Thus, most of these users are identified as spammers, which leads to a high recall for URL$_{svm}$, but the precision is low. As shown in Table 1, the precision of URL$_{svm}$ is the worst. However, MVSD takes advantage of three views' complementary information instead of only URL information. It makes that the proposed MVSD could balance the precision and recall.

Compared with the state-of-the-art optimization methods (SMFSR and SSDM), the precision of MVSD is greater over 10% than theirs. The F$_1$-score of MVSD is better than SMFSR's (over 9%) and SSDM's (over 6%) on different training set. The recall of MVSD is also better than optimization methods' on the larger size of training set. The reason is that SMFSR and SSDM only use text information to train the classifier. Also, they do not fully consider the social relationships' constraints between different types of users in social regularization term, which is discussed in Section 4.3. Therefore, they cannot achieve better performance. However, MVSD not only takes multiple useful information into consideration, but also takes advantage of different types of constraints among users as well as complements the missing values to improve the performance significantly.

For the combination methods, CONCATENATE$_{svm}$ simply puts all the features together. Compared with single view's methods, the performance is better than text's, which can also illustrate that URL and hashtag information is useful to detect spammers. However, this simple combination cannot characterize spammers' features correctly. Therefore, the performance of MVSD is better than that of CONCATENATE$_{svm}$. We also can observe that MVSD's performance is better than MULTINMF+SVM's. That is because MULTINMF+SVM trains the classifier separately. The two parts cannot help each other. In contrast, the proposed MVSD learns multiple views' information and classifier simultaneously, which leads to the two parts promoting each other greatly and learning the classifier correctly. Thus, MVSD can achieve better performance compared with baseline methods.

5.3. Multi-view learning evaluation

From the Data Analysis in Section 2, we observed that considering multiple view information can improve the performance of social spammer detection. To validate the effectiveness of multi-view learning in quantity, we conduct the following experiment. We first select several methods as baselines: TEXT$_{\mathrm{SR+SVM}}$, URL$_{\mathrm{SR+SVM}}$ and HASHTAG$_{\mathrm{SR+SVM}}$, which use single view's information as one feature matrix respectively, the social regularization (Eq. (2)) and SVM to train the corresponding classifier; CONCATENATE$_{\mathrm{SR+SVM}}$ combines the three views' information into one feature matrix, and then we apply the social regularization (Eq. (2)) and SVM on this matrix to learn the classification model. The experimental results are shown in Table 2.

From Table 2, we observe that though these methods all exploit the *same* social regularization and SVM, the precision and F$_1$-score of MVSD are better than baselines'. Since single view's information may not be enough for comprehensive identification of social spammers, the performance of single view methods is worse than that of using

Table 1
Social spammer detection results.

Method	Training data one (30%)			Training data two (50%)			Training data three (80%)		
	Precision	Recall	F$_1$-score	Precision	Recall	F$_1$-score	Precision	Recall	F$_1$-score
TEXT$_{svm}$	0.633	0.889	0.740	0.646	0.891	0.749	0.687	0.895	0.777
URL$_{svm}$	0.534	**0.955**	0.685	0.556	0.952	0.702	0.575	**0.948**	0.716
HASHTAG$_{svm}$	0.651	0.898	0.755	0.701	0.903	0.789	0.744	0.915	0.821
SMFSR	0.637	0.892	0.742	0.648	0.901	0.754	0.691	0.906	0.784
SSDM	0.659	0.860	0.746	0.716	0.894	0.795	0.743	0.908	0.817
CONCATENATE$_{svm}$	0.666	0.951	0.783	0.703	**0.956**	0.810	0.772	0.914	0.837
MULTINMF+SVM	0.770	0.915	0.836	0.781	0.928	0.848	0.792	0.931	0.856
MVSD	**0.836**	0.857	**0.846**	**0.838**	0.909	**0.872**	**0.848**	0.912	**0.879**

Table 2
Performance of Multiple-View Learning Validation.

Method	Precision	Recall	F$_1$-score
TEXT$_{\text{SR+SVM}}$	0.722	0.873	0.790
URL$_{\text{SR+SVM}}$	0.609	0.927	0.735
HASHTAG$_{\text{SR+SVM}}$	0.758	0.904	0.825
CONCATENATE$_{\text{SR+SVM}}$	0.782	0.906	0.839
MVSD	0.848	0.912	0.879

multiple view information. CONCATENATE$_{\text{SR+SVM}}$ considers multiple view information, but this method simply puts all the views' information into a feature matrix equally without distinguishing the importance of different views. Compared with baselines, the proposed multi-view learning method not only takes the significance of different views into consideration, but also models the different importance of different views. Thus, the proposed method can achieve the best performance.

5.4. Social regularization evaluation

In Section 4.2, we analyzed the importance of employing the four kinds of social relationships when detecting spammers and proposed a new social regularization term. In this subsection, we verify the performance of the new social regularization term. We select MULTINMF$_{\text{SVM}}$ and MVSD$_{\text{LS}\to\text{L}}$ as baselines. MULTINMF$_{\text{SVM}}$ applies the multi-view learning (Eq. (1)) and SVM to train the classifier, i.e., removing the social regularization (Eq. (2)) from MVSD. Also, we employ the *same* multi-view learning and SVM in MVSD$_{\text{LS}\to\text{L}}$, whose social regularization term is the same as [14]'s, i.e., considering two kinds of relationships: legitimate user → legitimate user and spammer → legitimate user.

Table 3 shows the performance of the above methods. The precision and F$_1$-score of MULTINMF$_{\text{SVM}}$ are worse than those of using social regularization, and the performance of the proposed social regularization is superior to that of the others. The results not only indicate that social regularization term can help spammer detection approaches to identity more spammers, but also validate that modeling all types of users' relationships in social regularization term can improve detection performance than other regularization terms only considering partial users' relationships.

Table 3
Performance of Social Regularization Term Validation.

Method	Precision	Recall	F$_1$-score
MULTINMF$_{\text{SVM}}$	0.788	0.909	0.844
MVSD$_{\text{LS}\to\text{L}}$	0.827	0.901	0.862
MVSD	0.848	0.912	0.879

Table 4
Information Complement Performance.

	Precision	Recall	F$_1$-score
Clean Dataset (50%)	0.789	0.887	0.835
Complemented Dataset (50%)	0.838	0.909	0.872
Clean Dataset (80%)	0.812	0.898	0.853
Complemented Dataset (80%)	0.848	0.912	0.879

5.5. Information complement evaluation

Here we illustrate the importance of complementing the missing values by comparing with the method that deletes the users with empty features in any of the three views. The compared dataset, named Clean Dataset, contains 6,432 users (2,412 spammers and 4,020 legitimate users). Table 4 shows the experimental results on precision, recall and F$_1$-score. "Clean Dataset (50%)" means that we randomly select 50% of the whole Clean dataset as training set and the remaining data as testing set. From Table 4, we can observe that the proposed method MVSD performs well on the complemented dataset, which indicates that complemented the missing users' features helps the proposed method to detect more spammers effectively as well as keeps data completeness. The reason is that filling in missing data makes the users information more sufficient and complete, which leads to learning an accurate consensus matrix V^* (described in Section 4). When V^* is close to the real distribution of users, the classifier W is learned more accurate.

6. Related work

Since Heymann et al. [27] firstly surveyed potential solutions and challenges on social spammer detection, many different methods have been proposed to combating social spammers. Jiang et al. [28] offered an overview of the existing methods and future directions for suspicious behavior detection.

The state-of-the-art approaches employed **supervised machine learning** methods to train a classifier to detect spammers. SMFSR [14] jointly modeled user activities' information (single view) and social network information to learn a classifier. SSDM [15] incorporated users' text information (single view) and social network information into an efficient spare supervised model for spammer detection. Hu et al. [16] proposed a model for online social spammer detection. Hu et al. [18] also proposed an interesting approach which incorporated emotional analysis into spammer detection task and achieved better performance. Wu et al. [8] utilized the posting relations between users and messages to co-detect social spammers and spam messages. In addition, they incorporated the social relations among users and the connections among messages into their framework as regularization terms.

There are also some work to train classifiers only **using users' features** extracted from users' behavior [4,29,30]. [9,31] mainly analyzed and extracted the distinguishing features for identifying spammers. Zhang et al. [32] proposed some features to distinguish promoting and spam campaigns from the legitimate ones. Chu et al. [11] utilized the collective detective approach with the features to capture spam campaigns. Ahmed et al. [33] identified the generic statistical features to detect spam profiles with different classification algorithm on Facebook and Twitter. Yang et al. [10] analyzed the evasion tactics of Twitter spammers and further designed the new users' features to detect more spammers. Zheng et al. [3] proposed the user's content and behavior features and applied them into SVM based algorithm for spammer classification. Zhu et al. [34] presented a model based on logistic regression considering content attributes and behavior attributes of users in social networks. Jiang et al. [35] proposed an approach, CrossSpot, to discover the suspicious behaviors in multimodal data. CatchSync [36] exploited two group-level behaviors, synchronicity and normality, to catch suspicious nodes in large directed graphs. LockInfer [37] learned connectivity patterns in large graphs and detected users' lockstep behaviors. Ali et al. [38] used ensemble learning method combining the outputs of the multiple classifiers to detect spam, which is different from the proposed MVSD.

Different from extracting features, some work only considers **social network information** to identify spammers. Ghosh et al. [12] investigated link farming on Twitter and proposed a ranking scheme to deter spam. Yang et al. [13] proposed a criminal account inference algorithm by exploiting criminal accounts' social relationships. Cao et al. [39] presented the SybilRank algorithm relying on social graph properties to rank users. Cui et al. [40] proposed a Hybrid Factor Non-Negative Matrix Factorization method to incorporate the predictive factors for user-post specific social influence prediction.

Multi-view clustering is used to group objects into different clusters based on their features extracted from different perspectives, i.e., views [41]. NMF is one of the commonly used techniques in multi-view clustering. Akata et al. [42] extended traditional NMF to the joint factorization of different data matrices. Greene et al. [43] assumed that clustering results could be obtained from each view, and employed matrix factorization over the clustering results. Liu et al. [25] developed a joint matrix factorization algorithm to incorporate not only individual matrix factorizations but also inconsistency between each view's coefficient matrix and the consensus. Liu et al. [44] proposed a clustering method by automatically learning each view's weight to balance the result of the consensus. Li et al. [45] proposed the partial multi-view clustering approach to handle partial examples, which worked based on NMF. Our proposed multi-view learning in this paper is different from the above methods, which integrates the NMF based multi-view learning and labeled information into a joint classification model.

All the discussed methods cannot train a classifier using both multiple view information and social network information. To the best of our knowledge, we are the first to build a joint supervised optimization model as well as consider the users with empty features in any kind of information.

7. Conclusion

In this paper, we propose a generalized framework by taking advantage of multiple views' information for social spammer detection. Different from the existing methods that utilize single view's information, the proposed method MVSD integrates multiple social information based on NMF with classification model into a learning model. Moreover, we introduce a simple strategy to complement the missing values of different view to predict more users, thus improving the performance of detection spammers. Experimental results on a real dataset show that MVSD obtains the better detection performance than the existing methods even with a small number of training data.

Acknowledgments

The authors would like to thank the anonymous reviewers and the editor for suggesting various changes. This work was supported by the National Natural Science Foundation of China (61272374, 61300190), the Key Project of Chinese Ministry of Education (313011) and the Foundation of Department of Education of Liaoning Province (L2015001).

References

[1] Y. Han, B. Fang, Y. Jia, Predicting the topic influence trends in social media with multiple models, Neurocomputing 144 (2014) 463–470.

[2] S. Fakhraei, J. Foulds, M. Shashanka, L. Getoor, Collective spammer detection in evolving multi-relational social networks, in: Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2015, pp. 1769–1778.

[3] X. Zheng, Z. Zeng, Z. Chen, Y. Yu, C. Rong, Detecting spammers on social networks, Neurocomputing 159 (2015) 27–34.

[4] Z. Li, X. Zhang, H. Shen, W. Liang, Z. He, A semi-supervised framework for social spammer detection, in: Advances in Knowledge Discovery and Data Mining, Springer, 2015, pp. 177–188.

[5] 2013 state of social media spam, Tech. rep., Nexgate, ⟨http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf⟩(2013).

[6] D. Liu, B. Mei, J. Chen, Z. Lu, X. Du, Community based spammer detection in social networks, in: Proceedings of the Web-Age Information Management, Springer, 2015, pp. 554–558.

[7] C. Cao, J. Caverlee, Detecting spam urls in social media via behavioral analysis, in: Proceedings of the Advances in Information Retrieval, Springer, 2015, pp. 703–714.

[8] F. Wu, J. Shu, Y. Huang, Z. Yuan, Co-detecting social spammers and spam messages in microblogging via exploiting social contexts, Neurocomputing 201 (C) (2016) 51–65.

[9] K. Lee, J. Caverlee, S. Webb, Uncovering social spammers: social honeypots+ machine learning, in: Proceedings of the 33rd international ACM SIGIR Conference on Research and Development in Information Retrieval, 2010, pp. 435–442.

[10] C. Yang, R. Harkreader, G. Gu, Empirical evaluation and new design for fighting evolving twitter spammers, IEEE Trans. Inf. Forensics Secur. 8 (8) (2013) 1280–1293.

[11] Z. Chu, I. Widjaja, H. Wang, Detecting social spam campaigns on twitter, in: Proceedings of the 10th International Conference Applied Cryptography and Network Security, Vol. 7341, 2012, pp. 455–472.

[12] S. Ghosh, B. Viswanath, F. Kooti, N.K. Sharma, G. Korlam, F. Benevenuto, N. Ganguly, K. P. Gummadi, Understanding and combating link farming in the twitter social network, in: Proceedings of the 21st International Conference on World Wide Web, 2012, pp. 61–70.

[13] C. Yang, R. Harkreader, J. Zhang, S. Shin, G.Gu, Analyzing spammers' social networks for fun and profit: a case study of cyber criminal ecosystem on twitter, in: Proceedings of the 21st International Conference on World Wide Web, 2012, pp. 71–80.

[14] Y. Zhu, X. Wang, E. Zhong, N.N. Liu, H. Li, Q. Yang, Discovering spammers in social networks, in: Proceedings of the National Conference on Artificial Intelligence, 2012, pp. 171–177.

[15] X. Hu, J. Tang, Y. Zhang, H. Liu, Social spammer detection in microblogging, in: Proceedings of the 23rd International Joint Conference on Artificial Intelligence, 2013, pp. 2633–2639.

[16] X. Hu, J. Tang, H. Liu, Online social spammer detection, in: Proceedings of the 28th AAAI Conference on Artificial Intelligence, 2014, pp. 59–65.

[17] K. Lee, B.D. Eoff, J. Caverlee, Seven months with the devils: A long-term study of content polluters on twitter, in: Proceedings of the 5th International Conference on Weblogs and Social Media, 2011, pp. 1–8.

[18] X. Hu, J. Tang, H. Gao, H. Liu, Social spammer detection with sentiment information, in: Proceedings of the IEEE International Conference on Data Mining, 2014, pp. 180–189.

[19] H. Kwak, C. Lee, H. Park, S. Moon, What is twitter, a social network or a news media?, in: Proceedings of the 19th International Conference on World Wide Web, 2010, pp. 591–600.

[20] X. Hu, J. Tang, H. Liu, Leveraging knowledge across media for spammer detection in microblogging, in: Proceedings of the 37th international ACM SIGIR Conference on Research and Development in Information Retrieval, 2014, pp. 547–556.

[21] P.P. Chan, C. Yang, D.S. Yeung, W.W. Ng, Spam filtering for short messages in adversarial environment, Neurocomputing 155 (2015) 167–176.

[22] J.T. Wang, M.J. Zaki, H.T. Toivonen, D. Shasha, Data Mining in Bioinformatics, Springer, London, 2005.

[23] J. Weng, E.-P. Lim, J. Jiang, Q. He, Twitterrank: finding topic-sensitive influential twitterers, in: Proceedings of the 3rd ACM International Conference on Web Search and Data Mining, 2010, pp. 261–270.

[24] M. McPherson, L. Smith-Lovin, J.M. Cook, Birds of a feather homophily in social networks, Annu. Rev. Sociol. (2001) 415–444.

[25] J. Liu, C. Wang, J. Gao, J. Han, Multi-view clustering via joint nonnegative matrix factorization, in: Proceedings of the 13th SIAM International Conference on Data

Mining, Vol. 13, 2013, pp. 252–260.

[26] D.D. Lee, H.S. Seung, Algorithms for non-negative matrix factorization, in: Proceedings of the Advances in Neural Information Processing Systems, 2001, pp. 556–562.

[27] P. Heymann, G. Koutrika, H. Garcia-Molina, Fighting spam on social web sites - a survey of approaches and future challenges, IEEE Internet Comput. 11 (6) (2007) 36–45.

[28] M. Jiang, P. Cui, C. Faloutsos, Suspicious behavior detection current trends and future directions, IEEE Intell. Syst. 31 (1) (2016) 31–39.

[29] J. Cao, Q. Fu, Q. Li, D. Guo, Leveraging behavior diversity to detect spammers in online social networks, in: Proceedings of the Algorithms and Architectures for Parallel Processing, Springer, 2015, pp. 323–336.

[30] A.A. Amleshwaram, A.L.N. Reddy, S. Yadav, G. Gu, C. Yang, CATS: characterizing automation of twitter spammers, in: Proceedings of the 5th International Conference on Communication Systems and Networks, 2013, pp. 1–10.

[31] F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida, Detecting spammers on twitter, in: Proceedings of the Collaboration, Electronic Messaging, Anti-abuse and Spam Conference, Vol. 6, 2010, pp. 1–9.

[32] X. Zhang, S. Zhu, W. Liang, Detecting spam and promoting campaigns in the twitter social network, in: IEEE Proceedings of the 12th International Conference on Data Mining, 2012, pp. 1194–1199.

[33] F. Ahmed, M. Abulaish, A generic statistical approach for spam detection in online social networks, Comput. Commun. 36 (10–11) (2013) 1120–1129.

[34] X. Zhu, Y. Nie, S. Jin, A. Li, Y. Jia, Spammer detection on online social networks based on logistic regression, in: Web-Age Information Management, Springer, 2015, pp. 29–40.

[35] M. Jiang, A. Beutel, P. Cui, B. Hooi, S. Yang, C. Faloutsos, Spotting suspicious behaviors in multimodal data: a general metric and algortihms, IEEE Trans. Knowl. Data Eng. 28 (8) (2016) 2187–2200.

[36] M. Jiang, P. Cui, A. Beutel, C. Faloutsos, S. Yang, Catchsync: catching synchronized behavior in large directed graphs, in: Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2014, pp. 941–950.

[37] M. Jiang, P. Cui, A. Beutel, C. Faloutsos, S. Yang, Inferring lockstep behavior from connectivity pattern in large graphs, Knowl. Inf. Syst. (2015) 1–30.

[38] H. Ali, M.-B. Behrouz, Multi-view learning for web spam detection, J. Emerg. Technol. Web Intell. 5 (4) (2013) 395–400.

[39] Q. Cao, M. Sirivianos, X. Yang, T. Pregueiro, Aiding the detection of fake accounts in large scale social online services, in: Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation, 2012, pp. 197–210.

[40] P. Cui, F. Wang, S. Liu, M. Ou, S. Yang, L. Sun, Who should share what? Item-level social influence prediction for users and posts ranking, in: Proceedings of the 34th international ACM SIGIR Conference on Research and Development in Information Retrieval, ACM, 2011, pp. 185–194.

[41] S. Bickel, T. Scheffer, Multi-view clustering, in: Proceedings of the 4th IEEE International Conference on Data Mining, 2004, pp. 19–26.

[42] Z. Akata, C. Thurau, C. Bauckhage, Non-negative matrix factorization in multi-modality data for segmentation and label prediction, in: Proceedings of the 16th Computer Vision Winter Workshop, 2011, pp. 1–8.

[43] D. Greene, P. Cunningham, A matrix factorization approach for integrating multiple data views, Lect. Notes Comput. Sci. 5781 (2009) 423–438.

[44] J. Liu, J. Han, HINMF: A matrix factorization method for clustering in heterogeneous information networks, in: Proceedings of the 2013 International Joint Conference on Artificial Intelligence Workshop, 2013, pp. 1–3.

[45] S. Li, Y. Jiang, Z. Zhou, Partial multi-view clustering, in: Proceedings of the 28th AAAI Conference on Artificial Intelligence, 2014, pp. 1968–1974.

Hua Shen is a Ph.D. candidate in computer science at Dalian University of Technology. She received a master's degree in Computer Applied Technology from Dalian Maritime University. She is currently an associate professor at College of Mathematics and Information Science, Anshan Normal University, China. Her research interests include data mining and machine learning.

Fenglong Ma is a Ph.D. student in Department of Computer Science and Engineering, the State University of New York at Buffalo. He received M.E. and B.E. from Dalian University of Technology in China. His research interests broadly are data mining and machine learning, including truth discovery, healthcare data mining and probabilistic graphical model.

Xianchao Zhang is a full professor at Dalian University of Technology. He got his scholar and master degrees in mathematics from National University of Defense Technology, China, in 1994 and 1998, respectively. He got his Ph.D. in computer science from University of Science and Technology of China in 2000. From 2000 to 2003, he worked as a research and development manager in some international companies. He joined Dalian University of Technology in 2003. His research interests include design and analysis of algorithms, machine learning, data mining, and information retrieval.

Linlin Zong is a Ph.D. candidate in computer science at Dalian University of Technology. She got her scholar degree in software engineering from Dalian University of Technology in 2011 and started her PhD program since then. Her research interests include machine learning and data mining.

Xinyue Liu is an associate professor at School of Software, Dalian University of Technology, China. She got her B.S and M.S from Northeast Normal University, China, and got her Ph.D. from Dalian University of Technology, China. Her research interests include data mining, machine learning and information retrieval.

Wenxin Liang received his B.E. and M.E. degrees from Xi'an Jiaotong University, China in 1998 and 2001, respectively. He received his Ph.D. degree in Computer Science from Tokyo Institute of Technology, Japan in 2006. He was a Postdoc Research Fellow, CREST of Japan Science and Technology Agency (JST) and a Guest Research Associate, GSIC of Tokyo Institute of Technology from Oct. 2006 to Mar. 2009. His main research interests include Big Data, Data Mining, Social Networks, etc. He is currently an associate professor at the School of Software, Dalian University of Technology, China. He is a senior member of China Computer Federation (CCF), and a member of IEEE, ACM, ACM SIGMOD Japan Chapter and Database Society of Japan (DBSJ).