# Social Network Analytic-based Online Counterfeit Seller Detection using User Shared Images

MING CHEUNG, Social Face Limited, China
WEIWEI SUN, Department of Computer and Information Science, Faculty of Science and Technology, State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau
JAMES SHE, HKUST-NIE Social Media Lab, Hong Kong
JIANTAO ZHOU, CORRESPONDING AUTHOR, Department of Computer and Information Science, Faculty of Science and Technology, State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau

Selling counterfeit online has become a serious problem, especially with the advancement of social media and mobile technology. Instead of investigating the products directly, one can only check the images, tags annotated by the sellers on the images, or the price to decide if a seller sells counterfeits. One of the ways to detect counterfeit sellers is to investigate their social graphs, in which counterfeit sellers show different behaviour in network measurements, such as those in centrality and EgoNet. However, social graphs are not easily accessible. They may be kept private by the operators, or there are no connections at all. This paper proposes a framework to detect counterfeit sellers using their connection graphs discovered from their shared images. Based on 153K shared images from Taobao, it is proven that counterfeit sellers have different network behaviours. It is observed that the network measurements follow Beta function well. Those distributions are formulated to detect counterfeit sellers by the proposed framework, which is 60% better than approaches using classification.

CCS Concepts: • **Social and professional topics** → **Computer crime**; • **Applied computing** → **System forensics**; • **Human-centered computing** → *Social media*; • **Computing methodologies** → Neural networks.

Additional Key Words and Phrases: Counterfeit seller detection, Social network analytic, Deep learning

## 1 INTRODUCTION

With the continued ubiquitousity of the Internet and the promotion of e-commerce platforms, online shopping becomes easy and popular around the world. In recent years, the number of online sellers and consumers has grown rapidly as well as the turnover. Millions of items are traded every day creating great business value. The Asian e-commerce platform, Carousell, has more than 100 millions products for sales since its launch in 2012 [1]. The product images are shared by the sellers, and potential customers can easily search the images by tags, or follow the sellers to receive notifications for new products. Due to the convenience and low cost of setting

[1]https://blog.carousell.com/2017/01/26/a-new-year-a-new-home-and-a-new-blog/

Authors' addresses: Ming Cheung, Social Face Limited, Hong Kong, China, ming@socialface.ai; Weiwei Sun, Department of Computer and Information Science, Faculty of Science and Technology, State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau, YB57457@umac.mo; James She, HKUST-NIE Social Media Lab, Hong Kong, eejames@ust.hk; Jiantao Zhou, Corresponding author, Department of Computer and Information Science, Faculty of Science and Technology, State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau, jtzhou@umac.mo.


1551-6857/2022/3-ART $15.00
https://doi.org/10.1145/3524135

an online store, considerable unscrupulous merchants sell counterfeit goods on various e-commerce platforms. Unlike physical stores, it is not possible to investigate the products from online sellers directly. With the high volume of transactions, it is difficult to locate sellers that misbehave, such as selling counterfeits. E-commerce giants like Amazon and Alibaba pay a lot of attention to fight counterfeit products. As removing those counterfeit products requires manual flag, counterfeit products are still accessible[2]. Using manual efforts to detect counterfeit products is not effective, and it can only detect a small number of counterfeit sellers from the hundreds of thousands of sellers. A scalable approach is required to suit the needs of a rapidly growing number of online sellers. One of the possible approaches is to reduce the manual efforts by ranking potential counterfeit sellers for further investigation.

As counterfeit sellers generate their shared images differently, they could be obtained using their network measurement and the profiles. Using social graphs and social network analytic (SNA) to detect abnormal sellers have been used for years, but is not useful in some platforms, such as Taobao in which their sellers do not declare their connections. In this paper, a SNA-based framework for online counterfeit seller detection is proposed, using discovered connections from their shared images. The connections are discovered from images using convolutional neural networks (CNNs), which are designed to automatically learn features that are sensitive to the targeted objects using given samples for training. The features are extracted using CNN for connection discovery in applications such as follower/followee recommendation [11][14]. Hence, connection graphs can be discovered using the similarity among user-shared images. The network features of each seller are measured, including direct measurements, degree centrality, betweenness centrality, closeness centrality and eigenvector centrality. The EgoNet of each seller, or the connection graph formed by the connected sellers, is also considered. The EgoNet mean degree, EgoNet density and EgoNet principal eigenvalue are measured, and they are appropriately formulated for counterfeit seller detection. We conduct an intensive study on sellers on e-commerce platforms using connection discovery, on counterfeit and non-counterfeit ones, respectively. With real-life datasets of over 153K shared images from social media and e-commerce platforms Taobao, the proposed framework is proven to be effective. Distributions of network features are modelled and formulated, and counterfeit sellers are detected by computing the probability that a seller is a counterfeit one, comparing to the probability that a seller is a normal one.

The rest of this paper is organized as follows. Section 2 presents related works. In Section 3, it is proposed the connection discovery among sellers. Section 4 introduces the proposed framework for counterfeit seller detection. Section 5 shows the measurement of the collected data. Experimental results are provided in Section 6 to show the superior performance of our proposed framework. Finally, the paper is concluded in Section 7.

## 2 RELATED WORKS

Detecting anomalies in a network has high-impact applications and has been studied for a long time. This technology affects many areas such as law enforcement, privacy protection, and risk assessment, such as detecting XSS attack [32], fake profiles on social media [30, 31]. In past years, researchers have proposed a variety of methods and technologies to handle such a problem for anomaly detection on graphs. Those users include influential users [29][38][21], paid posters [7], sexual predators [27], or fake reviewers on Amazon [26]. One of the ways to detect abnormal users on social media is to investigate the user's network features, such as centrality[17][5]. There are four common centralities: degree, closeness, betweenness and eigenvector centrality. They can be used to localize socially important users [25], spammer detection [45], content filtering [4] and more[44]. It can be applied in other types of networks, such as biological [23], webpage [28], and even airport network [19]. Those centralities follow similar distributions. Another common method is to investigate the properties of the EgoNet, the sub-graph formed by the connected users of a user[15]. Applications, such as friend

[2]https://consumerist.com/2017/03/22/amazon-steps-up-effort-to-rid-site-of-counterfeit-products/

recommendation and community detection[36], are possible with the use of EgoNet. Spam or spammers can be detected with social graphs [37, 39, 47, 48] as the graphs are significantly different from normal ones [34]. For example, normal users are not connected randomly; they form clusters with their common friends, while this kind of strategy is ineffective for spammers. It is interesting to investigate whether the connections among counterfeit sellers are significantly different from normal ones. Although network analysis has many applications and is very powerful, in many platforms, the connection between users could be missing, either hidden by the operators, such as Facebook, or ignored by the users of the network, such as Taobao.

Recently, using user shared images to discover connections has proven to be effective for follower/followee recommendation and gender prediction [10],[14]; but it is not clear whether the connections can be used for counterfeit seller detection. As abnormal users share more similar contents [7] [26], discovering connections among users is possible with their shared images to detection them. Counterfeit sellers copy and modify the images from the official sellers to prevent being detected by their customers[12]. Fig. 1 (b) and (c) show the shared images of Taobao sellers, and Fig. 1(a) shows the shared images by NIKE official store website. It is observed that the images of the Taobao sellers are from the official store, while adding a watermark or being copy-moved on the original images. As counterfeit sellers would share some similarities among their shared images, the connections can be discovered accordingly. Hence, in this work, we employ deep learning techniques [22],[6] for detecting connections among sellers, and then identify those potential counterfeit sellers for further investigation. Deep learning has been proven to be effective to classify images from social media [24, 46]. It has been used for abnormal detection[18, 43]. The deep features are extracted for encoding the images, based on which the images are clustered. The same unique label is assigned to the images within the same cluster, and the connections are discovered based on the occurrence of those labels on the images of a seller. As a result, SNA techniques, such as centrality measurements can be conducted, even without the social graphs from the sellers.

This paper extends our work [13] in the following ways: 1) we extend the framework to discover the network features among counterfeit sellers to form connection graphs; 2) we measure and formulate the network features from the social graphs using social network analytic; and 3) we utilize the formulated features to detect counterfeit sellers, and prove that the proposed framework achieves better detection performance.

## 3 CONNECTION DISCOVERY FROM SHARED IMAGES

This section introduces the proposed framework to discover the connection among counterfeit seller using machine generated labels.

### 3.1 Image Encoding using Convolutional Neural Network

Recently, Convolutional Neural Networks (CNNs) have been used for visual object recognition [22],[6]. A CNN is formed by several layers of non-linear feature detectors, with trainable weights and biases. Usually, a CNN is trained in a supervised way by using a large number of training data. Different from the conventional handcrafted features, the deep features are automatically learned and extracted from the training data through optimizing a certain objective function. Since a CNN is designed and trained for object recognition, the extracted features are essentially sensitive to objects in images. Under this circumstance, we propose to use the deep features for encoding the images for the subsequent counterfeit seller detection. Based on the extracted deep features, the images are clustered and the same unique machine-generated label is generated for images within the same cluster. This paper applies ResNet[20] to encode the images for clustering but training the CNN from scratch.

### 3.2 Discovering the Connections among Sellers

Naturally, we define the connection between any two sellers $i$ and $j$ as their similarity $S_{i,j}$. For conventional detection, the social graph is collected online, and abnormal users are detected accordingly, as shown in Fig. 2 (a).


Fig. 1. User interface shows product images on Taobao. The original product images are given in (a), while (b), (c) and (d) show examples of images of the same product on other sellers.

However, as social graphs are not available among sellers, connections are instead discovered from their shared images. More specifically, all the shared images from sellers are encoded into feature vectors, which are then clustered into $K$ clusters and annotated by the same unique machine-generated label that represents the cluster it belongs to. Such procedure is illustrated in Fig. 2 (b). Let $\mathbf{L}_i$ be the $K$-dimensional vector that describes the distribution of $K$ unique labels on the images shared by the seller $i$. Mathematically, it reads:

$$\mathbf{L}_i = (l_{i,1}, \ldots, l_{i,k}, \ldots, l_{i,K}), \tag{1}$$

where $l_{i,k}$ is the frequency of the $k$-th label in the profile $\mathbf{L}_i$ and $K$ represents the total number of unique labels, as illustrated in step 1 of Fig. 2 (b).

Given the profiles $\mathbf{L}_i$ and $\mathbf{L}_j$ corresponding to sellers $i$ and $j$, the similarity $S_{i,j}$ can be computed as follows:

$$S_{i,j} = S(\mathbf{L}_i, \mathbf{L}_j) = \frac{\mathbf{L}_i \cdot \mathbf{L}_j}{||\mathbf{L}_i|| \cdot ||\mathbf{L}_j||}, \tag{2}$$

where $\cdot$ denotes the dot product of two vectors and $||.||$ is the $\ell_2$ norm.

### 3.3 Connection Graph from Similarities

The connections are discovered based on $S_{i,j}$. Instead of using a threshold to define a connection between 2 sellers, the list of sellers with the highest $S_{i,j}$ to seller $i$ are considered to be connected with user $i$. Hence, the connection between 2 users, $i$ and $j$, can be defined as:

$$e_{i,j} = \begin{cases} 1 & \text{if } rank_i(j) \leq N_{top} \text{ or } rank_j(i) \leq N_{top} \\ 0 & \text{if otherwise,} \end{cases} \tag{3}$$

where $rank_i(j)$ is the rank of the $S_{i,j}$ of user $j$ among all values of $S_{i,.}$. $N_{top}$ is the number of sellers to be considered as connected per seller. Note that the connections is undirected, which means that if user $j$ is in the top list of sellers of user $i$, $i$ and $j$ are connected whether or not $i$ is in the top list of $j$. As a result, sellers have a different value of degree centralities.

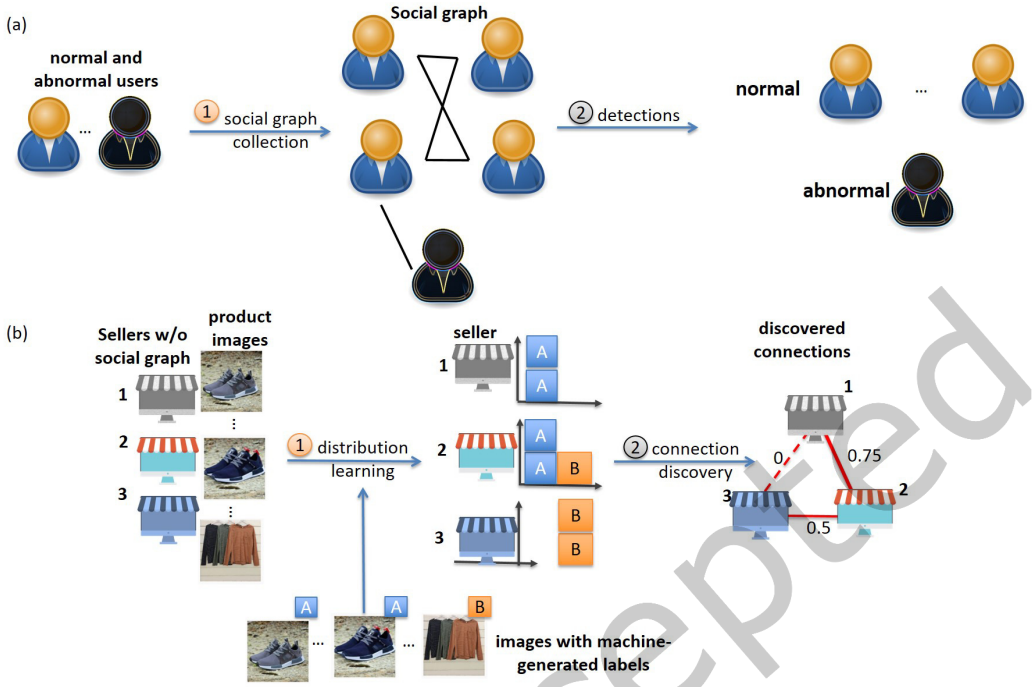


Fig. 2. Abnormal detection from connections: (a) from social graph collected and (b) discovering connections from user shared images



## 4 PROPOSED FRAMEWORK FOR DETECTING COUNTERFEIT SELLERS

This section discusses how to detect counterfeit sellers from the discovered connections. As shown in Fig. 3, the first step is to discover connections from their shared images, as introduced in the last section. The second step is to measure the network features among sellers based on the connection graph, and the third step is to fit the distribution of those features using Beta distribution for counterfeit and normal sellers. The fourth step is to utilize those fitted distributions for detecting counterfeit sellers. The details regarding the second to fourth steps are given below.

### 4.1 Network Features Measurements

We now describe the network measurements in terms of centrality and EgoNet. Fig. 4 shows an example of connection graph with 9 users, labeled with 1 to 9.

#### 4.1.1 *Centrality Analysis.*

***Degree Centrality***: The degree centrality for a node $i$ counts the number of nodes connecting to node $i$. A high degree centrality means that a node connects to many other nodes. The values are normalized with respect to the maximum possible degree, that is, the number of nodes in $G$ minus 1 :

$$C_D(i) = \frac{\sum_{j \neq i} e_{i,j}}{N-1}. \tag{4}$$

Nodes 4, 5 and 6 in Fig. 4 have the highest degree as they have the most number of connections.

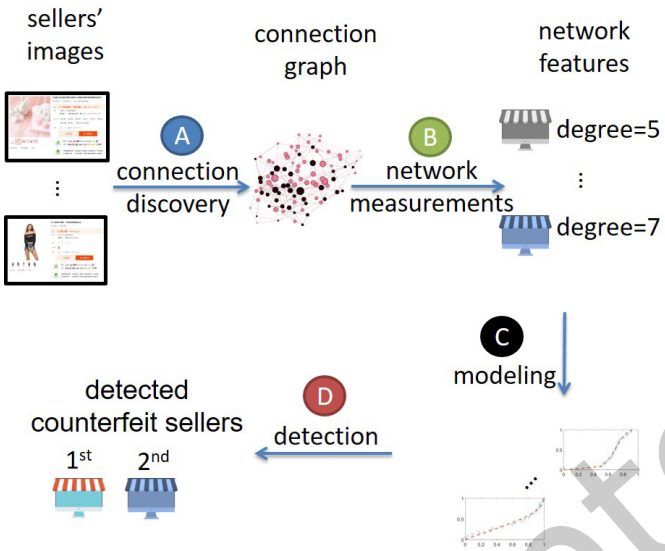


Fig. 3. Proposed framework for counterfeit seller detection.

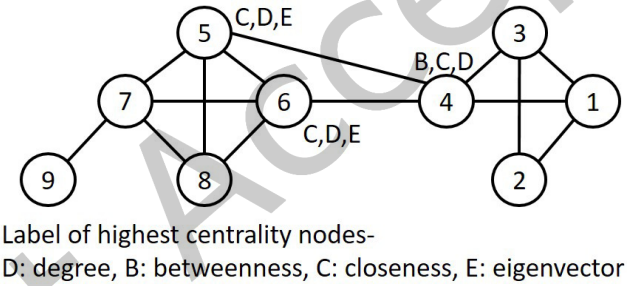


Fig. 4. Social importance in a social graph. The nodes with the highest centralities are labelled.

***Closeness Centrality***: Closeness centrality of a node $i$ is the mean of the shortest distances from $i$ to all other nodes in the graph. A high closeness centrality value implies that a node is close to many others, and it is at the centre of a connection graph. Since the sum of distances depends on the number of nodes in the graph, closeness is normalized by the sum of the minimum possible distances $N-1$.

$$C_C(i) = \frac{N-1}{\sum_{j=1}^{N-1} d(i,j)}, \tag{5}$$

where $d(i,j)$ is the shortest-path distance between $i$ and $j$, and $N$ is the number of nodes in the graph. Nodes 4,5 and 6 in Fig. 4 have the highest $C_C(i)$ as they are at the centre of the connection graph.

***Betweenness Centrality***: Betweenness centrality of a node $i$ is the sum of the number of shortest paths that pass through $i$, for all possible node pairs in the graph. Hence, a node with a high betweenness centrality is a node that connects very different nodes, such as those from different communities. Betweenness centrality can

be computed as:

$$C_B(i) = \sum_{j,v \in \mathcal{V}} \frac{\sigma(j,v|i)}{\sigma(j,v)}, \tag{6}$$

where $\mathcal{V}$ is the set of nodes, $\sigma(j,v)$ is the number of shortest $(j,v)$-paths, and $\sigma(j,v|i)$ is the number of hose paths passing through some node $i$ other than $j,v$. If $j=v, \sigma(j,v)=1$, and if $i \in \{j,v\}, \sigma(j,v|i)=0$. Node 4 in Fig. 4 has the highest $C_B(i)$ as it is between the 2 major communities on the connection graph.

***Eigenvector Centrality***: Eigenvector centrality for a node $i$ is based on the centrality of its neighbours. A high value of eigenvector centrality means that a node has many important connected nodes. The eigenvector centrality of all nodes, $\mathbf{C_E}$, is

$$\mathbf{AC_E} = \lambda \mathbf{C_E}, \tag{7}$$

where $\mathbf{A}$ is the adjacency matrix of the graph $G$ with eigenvalue $\lambda$. There is a unique and positive solution if $\lambda$ is the largest eigenvalue associated with the eigenvector of the adjacency matrix $\mathbf{A}$. Nodes 5 and 6 in Fig. 4 correspond to the highest values in $\mathbf{C_E}$, as they have the highest number of important connections.

*4.1.2 EgoNet.* An EgoNet is formed by the connected nodes to a node, including the original node, and all the connections among these nodes [2]. For a given node, $i$, its EgoNet is a sub-graph, $G^{(ego)}(i)$, of the connection graph, $G$, that all nodes in the sub-graph are connected to node $i$. Hence, the edge of $G^{(ego)}(i)$, $e^{(ego)}_{j,v}(i)$, is 1 if node $j$ and $v$ are connected in $G$. By the above definition, 3 measurements are defined: EgoNet mean degree, EgoNet density and EgoNet principal eigenvalue. EgoNet mean degree of node $i$ can be defined as:

$$C^{(ego)}_D(i) = \frac{1}{C_D(i)} \sum_j \sum_{j \neq v} e^{(ego)}_{j,v}(i), \text{ where } e_{i,j}=1. \tag{8}$$

Similarly, the EgoNet density of user $i$ can be defined as:

$$C^{(ego)}_{Den}(i) = \frac{\sum_j \sum_{j \neq v} e^{(ego)}_{j,v}(i)}{C_D(i)(C_D(i)-1)}, \text{ where } e_{i,j}=1. \tag{9}$$

Note that although the definitions of $C^{(ego)}_D(i)$ and $C^{(ego)}_{Den}(i)$ are similar, they have a different term, $(C_D(i)-1)$, which depends on user $i$. The third measurement is the EgoNet principal eigenvalue of $G^{(ego)}(i)$ [1].

Once these features are obtained, the next step is to model the distributions according to their labels, that is, counterfeit or normal sellers. The details can be found in the coming section.

## 4.2 Distribution Fitting for Probability Computation

The 7 features from graphs are selected and fitted accordingly based on the discovered connections. The goal here is to estimate the probability that a seller is a counterfeit one, given the feature of a seller. Hence, the question can be formulated using a Bayesian approach as:

$$P(C_i|f_i) = \frac{P(f_i|C_i)P(C_i)}{P(f_i)}, \tag{10}$$

where $f_i$ is a feature measured based on the connection graph, and $C_i \subset [0,1]$. Seller $i$ is a counterfeit seller if $C_i=1$, while $C_i=0$ means that seller $i$ is a not a counterfeit seller, that is, a normal seller. Hence, the likelihood ratio of a seller being a normal seller and a counterfeit seller, $\Psi$, can be defined as:

$$\Psi_i = \frac{P(f_i|C_i=1)P(C_i=1)}{P(f_i|C_i=0)P(C_i=0)}. \tag{11}$$

If $\Psi_i$ is greater than 0.5, it implies that user $i$ is more likely to be a counterfeit seller.


Fig. 5. Example images from of counterfeit sellers

### 4.3 Hypothesis Testing using Fitted Distribution

As it is not possible to obtain $\Psi_i$ of a user, $i$, directly from data and (11), it is desirable to fit the distribution of each feature, so as to compute $\Psi_i$. Considering a feature, the value of $\Psi_i$ can be computed as:

$$\Psi_i = \frac{g^{(c)}(f_i)\, P(C_i = 1)}{g^{(n)}(f_i)\, P(C_i = 0)}, \tag{12}$$

where $g^{(c)}(.)$ and $g^{(n)}(.)$ are the probability density function (PDF) of a feature. If $\Psi_i$ is greater than 0.5, seller $i$ is more likely to be a counterfeit seller. In the next section, the details of the computation of (12) will be introduced.

## 5 IMAGE SHARING BEHAVIORS OF SELLERS

This section introduces the Taobao dataset involved in this paper, and how connections are discovered from their shared images. Then, the distribution of the features in the connection graph is measured and formulated. The importance of features is also investigated.

### 5.1 Dataset

As the most popular e-commerce platform in China, Taobao has attracted a huge number of sellers, including individual operators, purchasing agents, brand official stores, and so on. Various sources of sellers and products make it an ideal testing platform, and hence, we collect our test dataset from Taobao. Two common commodities, shoes and cosmetics, are selected as the testing targets while the collected data is constituted by the images and prices of the online products. We browse 93 shoes stores and 100 cosmetics stores via a data collection tool Octopus[3]. Each store contributes up to 80 products. Totally, we collect 101090 images from shoes stores and 51870 images from cosmetics stores. The ground truth of these sellers is obtained manually via a surveying procedure. 40 experienced volunteers are invited to visit and mark all these online stores independently. We

[3]https://www.octoparse.com/

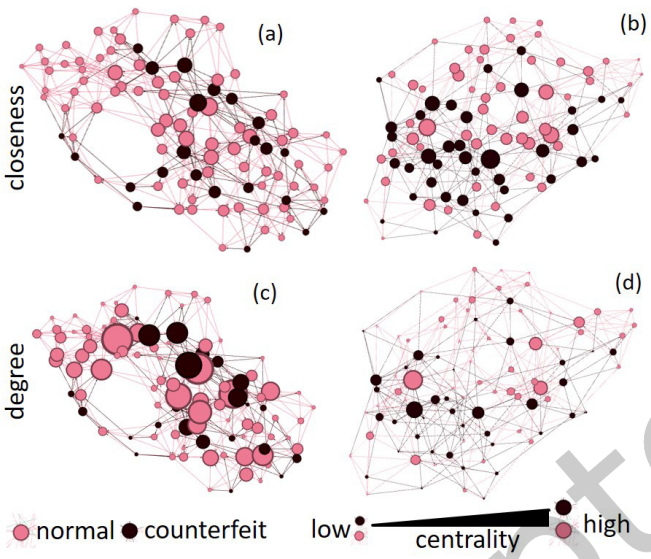


Fig. 6. Connection graphs for: (a) closeness of shoe sellers, (b) closeness of cosmetics sellers, (c) degree of shoe sellers, and (d) degree of cosmetics sellers



aggregate the marks given by these volunteers to determine the true identity of each seller. Finally, the shoes sellers are identified into 55 normal ones and 38 counterfeit ones while the cosmetics sellers are identified into 77 normal ones and 23 counterfeit ones.

Now, we give an intuitive view of the counterfeit products; some representative examples are illustrated in Fig. 5. As can be seen, various types of counterfeit product images exhibit different characteristics, making it difficult to detect counterfeit sellers via some traditional feature based methods. Usually, the exiting detection method only works on a small part of images. For example, detect and recognize the special ugly watermarking, or identify some low-quality product images. More discussions can be found in the subsequent sections.

## 5.2 Connection Graphs

The connection graphs are discovered from shared images. Fig. 6 (a) and (c) show connection graphs discovered among shoe sellers, while Fig. 6 (b) and (d) show connection graphs from cosmetic sellers. They are discovered by setting $N_{top} = 5$ and $K = 100$. It is observed that for closeness in Fig. 6 (a) and (b), normal and counterfeit sellers are different. There is a higher portion of high closeness sellers (those bigger green nodes). On the other hand, the degree of normal and counterfeit sellers shows a similar pattern, as observed in Fig. 6 (c) and (d). It is motivated to investigate if any network features can tell whether a seller is a counterfeit one. The next section discusses how those distributions can be modelled.

## 5.3 Trends of the distributions

It is interesting to investigate the trends of the distribution and how they can be modelled. The diamonds in Fig. 8 (a) to (g) are the values of the cumulative distribution function (CDF) of different features, for shoe and cosmetics

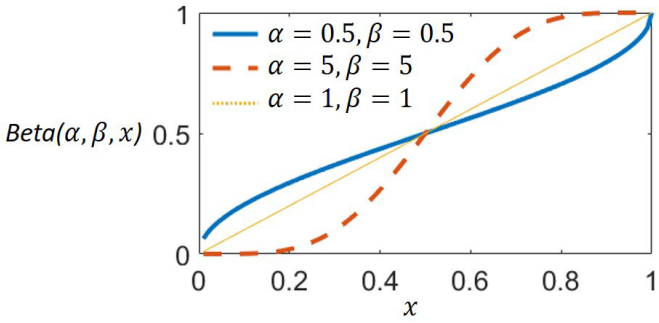


Fig. 7. Curves of the Beta function with different parameters.

sellers, respectively. It is observed that they follow a Beta distribution, as defined below:

$$Beta(\alpha, \beta, x) = \int_0^1 \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} dx, \tag{13}$$

where $\Gamma(.)$ is the gamma function. Note that $Beta(\alpha, \beta, x)$ is 0 when $x$ is less than 0, and 1 when $x$ is greater than 1. Hence, $\Psi_i$ can be computed as:

$$\Psi_i = \frac{Beta(\alpha_c, \beta_c, x_i)}{Beta(\alpha_n, \beta_n, x_i)}, \tag{14}$$

where $(\alpha_c, \beta_c)$ a and $(\alpha_n, \beta_n)$ are the parameters learned from counterfeit and normal sellers, respectively. $x_i$ is the value of a feature, such as the degree of user $i$. As Beta function is 0 if $x_i < 0$ and 1 if $x_i > 1$, the centrality values are divided by the maximum number of that centrality before fitting to the Beta distribution. Fig. 7 shows examples of $Beta(\alpha, \beta, x)$ with different values of $\alpha$ and $\beta$. It is observed that $Beta(\alpha, \beta, x)$ can fit different distributions, such as fast/slow increase in the beginning/ending.

Fig. 8 and Fig. 9 show examples of fitted curves and the corresponding data, where $K$ is 1000 for all features. The fitting results are the solid lines, while the measurements from data are represented by the diamond shaped markers. It is noticed that the curves fit the data well. The fitting can be evaluated by the root-mean-square error (RMSE):

$$rmse = \sqrt{\frac{\sum_{i=1}^{B}(y_i - \hat{y}_i)^2)}{B}} \tag{15}$$

where $y_i$ and $\hat{y}_i$ are the true and predicted values from the model, respectively, and $B$ is the number of points. Fig. 10 (a) and (b) give the error of fitting with different values of $K$, for shoes and cosmetics sellers, respectively. The error rate is measured in terms of $rmse$. It is observed that $rmse$ is relatively small among different values of $K$.

## 5.4 Feature Importance

To measure the importance of different features, precision and recall are common measurements. A high precision means that the sellers who are identified as counterfeit ones are mostly counterfeit sellers. A high recall means that most of the counterfeit sellers are identified as counterfeit ones. However, using a feature that gives a high recall may not be good, as those counterfeit sellers are covered by others. Using a feature that gives a low recall may not be bad, as it may cover sellers that cannot be identified by other features. For example, even one feature can achieve 80% of recall; it may be covered by other features that make the features less valuable. On the other

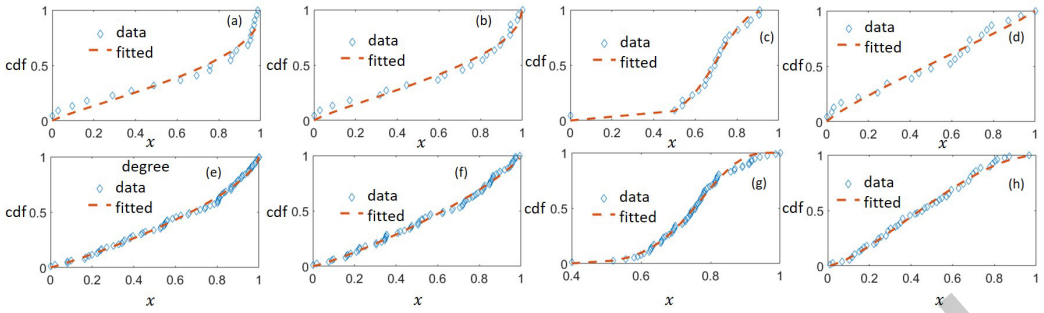


Fig. 8. CDF and the fitted curves: (a) degree of counterfeit sellers, (b) betweenness of counterfeit sellers, (c) closeness of counterfeit sellers, (d) eigenvector of counterfeit sellers, (e) degree of normal sellers, (f) betweenness of normal sellers, (g) closeness of normal sellers, and (h) eigenvector of normal sellers.

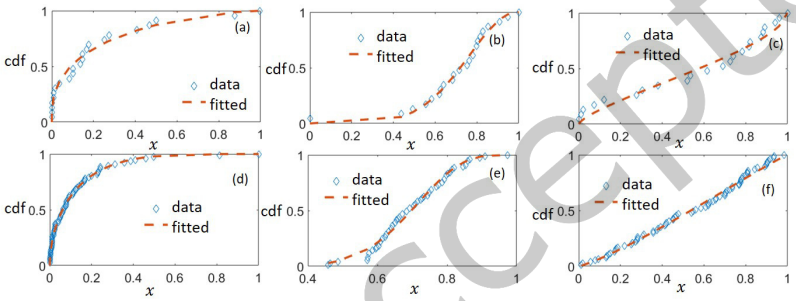


Fig. 9. CDF and the fitted curves: (a) EgoNet mean degree of counterfeit sellers, (b) EgoNet eigenvalue of counterfeit sellers, (c) EgoNet density of counterfeit sellers, (d) EgoNet mean degree of normal sellers, (e) EgoNet eigenvalue of normal sellers, and (f) EgoNet density of normal sellers.

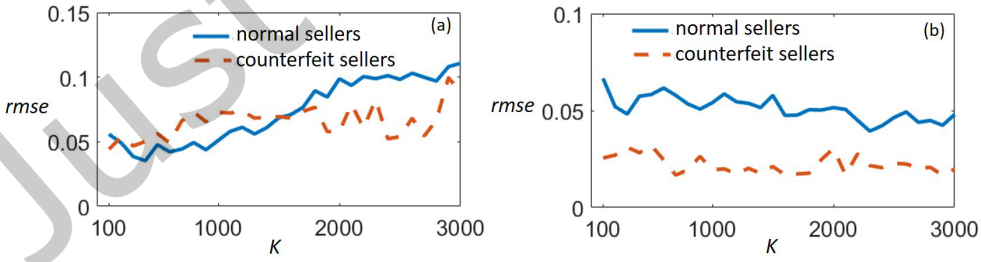


Fig. 10. Error measurement of the fitting with different values of $K$: (a) shoes sellers and (b) cosmetics sellers.

hand, one feature that has 10% recall may be more useful, as this part of counterfeit sellers cannot be detected from other features. Hence, it is motivated to measure the importance of different features besides their recall. Normalized recall, $r_N$ is defined as follows:

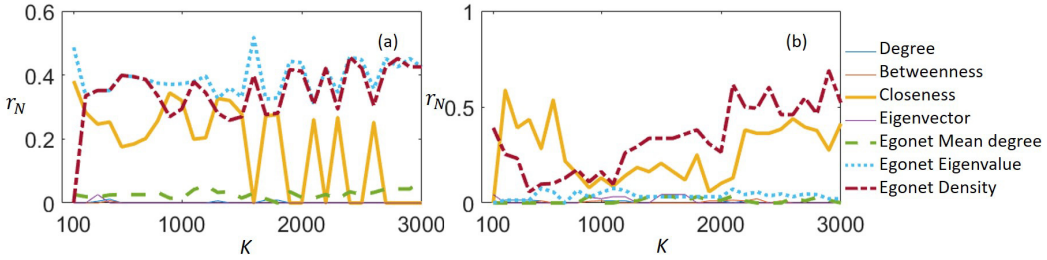


Fig. 11. Sensitivity analysis of different features with different values of $K$: (a) shoes sellers and (b) cosmetics sellers.

$$r_N = \sum_i \frac{1}{\text{Card}(\{j|\Psi_i^{(j)} > threshold_j\})}. \tag{16}$$

where $i$ and $j$ are indices of user and network feature, respectively. Here, Card$(\cdot)$ returns the cardinality of the given set. $\Psi_i^{(j)}$ is the measurement of user $i$ on the $j$-th importance, and $threshold_j$ is the threshold for that feature. With (16), a counterfeit seller that can only be detected by a feature, will result in a high $r_N$ for that feature. On the other hand, if a counterfeit seller can be detected by many features, $r_N$ will only increase slightly. Measurement is conducted to investigate which features are more sensitive to tell whether a seller is a counterfeit or normal one. The result is shown in Fig. 11. It is observed that not all features contain the same level of importance for detecting counterfeit sellers. Among those features, betweenness, degree centrality, principal eigenvalue and density of EgoNet, give higher $r_N$, which means that they are more sensitive to counterfeit seller detection. In the coming sections, these 4 features are selected for counterfeit seller detection.

## 6 EXPERIMENTAL RESULTS

We now experimentally evaluate our proposed framework. We first give the details of our system and parameter settings. In our experiments, we are attempting to identify whether an online seller is selling counterfeit-goods. This section also presents the error analysis, followed by a discussion.

### 6.1 Experimental Settings

As proposed, the labelled sellers are applied to fit the distributions of counterfeit and normal users using the 4 types of measurements developed in the previous section. We encode all images using ResNet[20]. The layer before the softmax is chosen as the base. We then use $K$-means++ [3] to cluster the encoded images. Furthermore, the occurrence of machine-generated labels is used to build each seller's profile. Each cluster corresponds to a unique label, which will be used to tag all the images from such a cluster. Note that all images are involved in the clustering process, as it does not require any counterfeit seller labels. In real operation, new images can be tagged using existing clusters [9], and the profile can be obtained accordingly. The seller's profile is composed by the occurrence of the labels of his belonging images. The connection among sellers is discovered accordingly, and a number of top users are the connection of a user (see (3)). Note that the connections in the experiments have no direction. Baselines are implemented to compare the performance of the proposed framework. It is the approach directly using the seller profiles to train a classifier[13].

The users are split into training and testing sets, in which 70% of data are used as the training set, while the

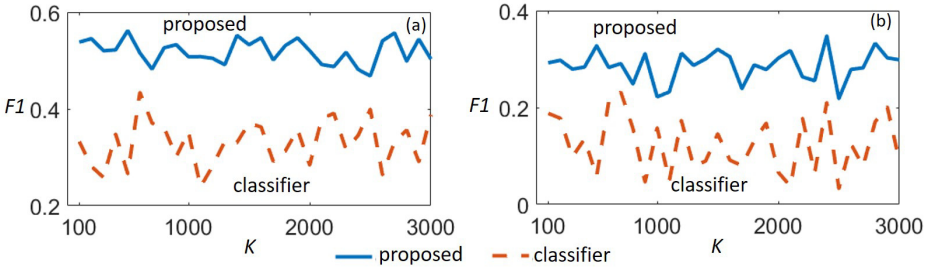


Fig. 12. Results with different values of $K$: (a) shoes sellers and (b) cosmetics sellers.

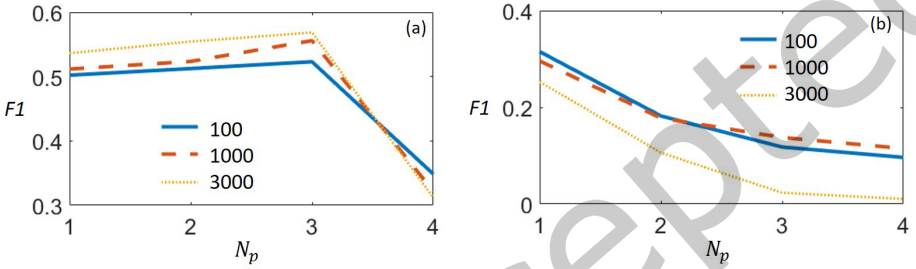


Fig. 13. Results with different $N_p$: (a) shoes sellers and (b) cosmetics sellers.

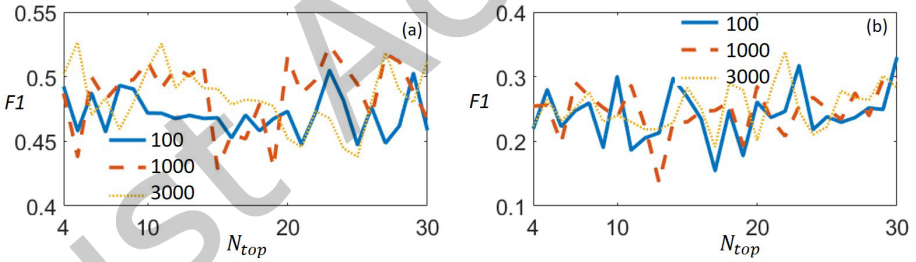


Fig. 14. Results with $N_{top}$: (a) shoes sellers and (b) cosmetics sellers.



rest are in the testing set. Each experiment is repeated for 100 times. The result is evaluated by $F1$ score[33] as:

$$F1 = \frac{2pr}{p+r}. \tag{17}$$

where $p$ and $r$ denote the precision and recall, respectively. If we would like to achieve high precision with a low recall, confidence recommendations, e.g., pairs with large $S_{i,j}$, is needed. A higher $r$ may result in a low $p$, resulting in a low $F1$ score. Clearly, $F1$ can give a good trade off between recall $r$ and precision $p$.

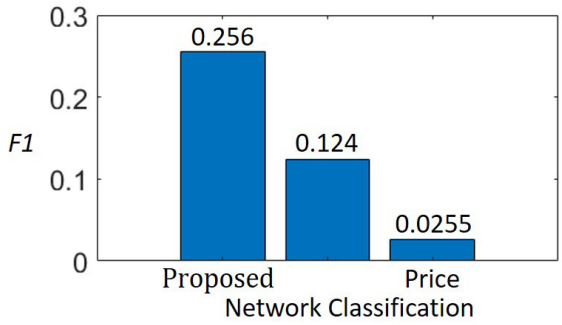


Fig. 15. Showcase: Proposed approach vs. network feature classification and pricing with cosmetic sellers.

## 6.2 Results

The counterfeit seller identification results of shoes and cosmetics with different $K$s are illustrated in Fig. 12 (a) and (b), respectively. We repeat the experiment 100 times and take the mean vale of the corresponding 100 results. It is observed that the performance of the proposed framework outperforms other approaches.

Fig. 13 (a) and (b) illustrate the identification results of shoes and cosmetics counterfeit sellers with different thresholds and $K$, respectively. Note that $N_p$ is the number of features that are greater than 0.5. It is observed that $F1$ is high when the threshold is small. It implies that if $N_p$ is large, there are too few counterfeit sellers that can be detected, and $F1$ drops significantly. Hence, $N_p$ is set to be 1 for better performance.

Fig. 14 (a) and (b) are the results of counterfeit seller identification. The results of shoes and cosmetics sellers are the $F1$ of with different values of $N_{top}$, respectively. It is observed that there is no clear trend for different values of $N_{top}$ and $K$, which means that the proposed framework is not sensitive to the 2 parameters.

## 6.3 Showcase: Price and Classification

It is a conventional wisdom that the prices of counterfeit-goods are mostly lower than non-counterfeit-goods. It is interesting to investigate whether it is the case on Taobao. Another conventional way to identify counterfeit sellers is classification using the network features. Hence, an experiment is conducted using price and network features for classification. The sellers are represented by the histogram of their products and network features, which are used to build the seller profile. 70% of the sellers are used as the training set, and the rest as the testing set. A classifier is trained using support vector machine, and the experiment is repeated for 100 times on cosmetic sellers. The result is shown in Fig. 15. As can be seen, our proposed method outperforms the ones based on price and network features. The price of a product from a normal and counterfeit seller can be very similar, as a counterfeit seller could seller expensive goods, while a normal seller could sell a cheap but official product.

## 6.4 Showcase: Ranking Counterfeit Sellers

In detection, whether the framework can rank counterfeit sellers high is also important for the platform operator. This ability enables the operator to check only the top ranked sellers, and this can save a lot of their manual efforts for checking one by one. An experiment is conducted to check whether the top ranked sellers by different approaches are counterfeit sellers. 70% of the sellers are used as the training set, and the rest as the testing set. Two baselines are built, the first one is a support vector machine for regression using the kernel of “RBF". Another one is a sequential deep learning model with 3 layers using “ReLU" as the activation function. The experiment is repeated for 100 times. The $r$ and $p$ of different number of sellers detected are recorded, and the result is shown

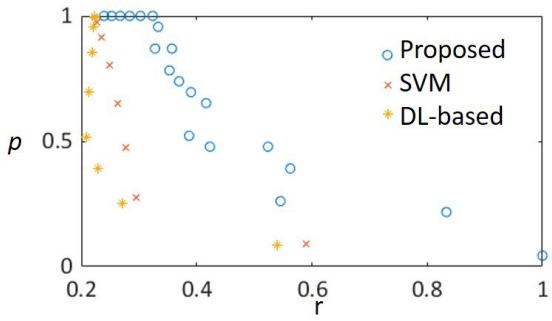


Fig. 16. Showcase: Proposed approach vs. other approaches on $r$.


Fig. 17. Error Analysis.

in Fig. 16. It is observed that $r$ of the proposed approach has outperformed the 2 baselines. It will greatly reduce the manual efforts of the platform operator.

## 6.5 Error Analysis

This section discusses the cases that different approaches cannot detect counterfeit sellers, and show the images from representative users. Fig. 17 (a) shows error cases when using classification approach. It is obvious that the latter sells counterfeit goods, but it is unrealistic to distinguish the difference between counterfeit and normal sellers. The images shared by a counterfeit seller could be well taken as from a normal seller. Such a situation is indistinguishable by methods based on object recognition. Fig. 17 (b) shows error cases when using price. As

observed from these images, the counterfeit and normal sellers have shared images of similar products, that is, socks, hats, shoes, and bags. However, the bags and shoes that the counterfeit seller sells are leather ones, and the average price of the product for the counterfeit seller is even higher than the normal sellers. In other words, counterfeit sellers do not necessarily have cheaper prices than normal sellers. Fig. 17 (c) shows error cases when using the proposed approach. The left one is MUJI, a well-known brand who sells a wide variety of things on Taobao. However, such a product span makes his connection with most stores very weak. That is why it is easy to be classified into counterfeit sellers. In contrast, a counterfeit seller who only sells high imitation shoes can easily be classified as normal sellers after well processing their images. Since the image provides partial information of the product, the classification based on the image is more or less biased.

### 6.6 Discussions

The proposed framework makes use of network features of known counterfeit sellers to detect counterfeit sellers using the connection graph discovered from their shared images. The training sets are learned from labelled counterfeit sellers, such as those found by the operators, and those flagged by users of these e-commerce platforms. Even the behaviors of the sellers may change with time, the proposed framework could learn the new behaviours by the labelled counterfeit sellers. Hence, the proposed framework can rank the counterfeit sellers, and the operators can focus on those sellers with new image sharing pattern. Note that we select the shoes and cosmetic sellers as the examples because they are very common commodities. Our proposed framework can be applied to any online selling products.

We also identify three possible future directions that may further improve the counterfeit detection performance. First of all, it is interesting to improve how the labels are generated. Currently, $k$-means is used as the clustering process, and other clustering algorithms could be adopted as well. Hence, another direction is how to apply other clustering algorithms that are more sensitive to counterfeit sellers. In addition, other inputs from models and sources can be used to improve the result. By integrating objects, user and opinion with the machine-generated labels [16], a better user profile can be formed and hence the discovered connections can be improved. The social information [42], such as commenting and the user interests [41] are also possible extensions. The third one is to study the network evolvement [35]. Unlike most social networks, the discovered connections keep changing with the images, as the edges are defined by the $N_{top}$. As a result, some edges will be added while some will disappear, even with the same set of sellers. It is interesting to investigate how the evolving network affects the counterfeit seller detection.

During the experiments for building classifiers for classify sellers, we have also implemented more complicated baselines, such as graph neural networks(GNN)[40] and Wide&Deep[8]. For GNN, the result is that it always predicts sellers to be non-counterfeit sellers. There is a similar observation for Wide&Deep. One of the reasons is that the data size is too small for model training. As well, the connections in the inputs of GNN are formed by the seller profiles but confirmed by users. Hence, they are not suitable for counterfiet detection in this paper.

## 7 CONCLUSION

In this work, we have proposed a framework to detect the online counterfeit sellers based on the connection graphs discovered from users shared images. By utilising a framework of CNN-based connection discovery, it is proven that counterfeit and normal sellers have different network features in the connection graph. The distribution of these features are modelled with a Beta function, and counterfeit sellers are detected based on the fitted distribution. Extensive experiment results based on the real Taobao environment with over 153K shared images are provided to validate the effectiveness of the proposed framework, where 60% in F1 score can be achieved for identifying counterfeit sellers. The proposed framework can be enhanced with object detections, and incorporating with network evolvement. With the surge of E-commerce, the requirement of detecting counterfeit

sellers becomes critical and imminent. Our proposed framework can be used as an effective preliminary screening tool, and can greatly reduce the manual detection efforts.

## ACKNOWLEDGEMENT

This work was supported in part by HKUST-NIE Social Media Lab., HKUST, and Macau Science and Technology Development Fund under SKL-IOTSC(UM)-2021-2023, 0072/2020/AMJ, and 0060/2019/A1, by Research Committee at University of Macau under MYRG2020-00101-FST, and by Natural Science Foundation of China under 61971476.

## REFERENCES

[1] Leman Akoglu, Mary McGlohon, and Christos Faloutsos. 2010. Oddball: Spotting anomalies in weighted graphs. In *Proc. Pacific-Asia Conf. Knowl. Discovery Data Mining*. Springer, 410–421.

[2] Leman Akoglu, Hanghang Tong, and Danai Koutra. 2015. Graph based anomaly detection and description: a survey. *Data mining knowl. discovery* 29, 3 (2015), 626–688.

[3] David Arthur and Sergei Vassilvitskii. 2007. k-means++: The advantages of careful seeding. In *Proc. annual ACM-SIAM symp. Discrete algor.* Society for Industrial and Applied Mathematics, 1027–1035.

[4] Hila Becker, Mor Naaman, and Luis Gravano. 2011. Selecting quality twitter content for events. In *Proc. 5th Int. AAAI Conf. Weblogs Social Media (ICWSM)*.

[5] Phillip Bonacich and Paulette Lloyd. 2001. Eigenvector-like measures of centrality for asymmetric relations. *Social Netw.* 23, 3 (2001), 191–201.

[6] Ken Chatfield, Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. 2014. Return of the devil in the details: Delving deep into convolutional nets. *arXiv preprint arXiv:1405.3531* (2014).

[7] Cheng Chen, Kui Wu, Venkatesh Srinivasan, and Xudong Zhang. 2013. Battling the internet water army: Detection of hidden paid posters. In *Proc. IEEE/ACM Int. Conf. Advances Social Netw. Anal. Mining (ASONAM)*. IEEE, 116–120.

[8] Heng-Tze Cheng, Levent Koc, Jeremiah Harmsen, Tal Shaked, Tushar Chandra, Hrishi Aradhye, Glen Anderson, Greg Corrado, Wei Chai, Mustafa Ispir, et al. 2016. Wide & deep learning for recommender systems. In *Proceedings of the 1st workshop on deep learning for recommender systems*. 7–10.

[9] Ming Cheung, Xiaopeng Li, and James She. 2017. An efficient computation framework for connection discovery using shared images. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 13, 4 (2017), 1–21.

[10] Ming Cheung and James She. 2019. Detecting social signals in user-shared images for connection discovery using deep learning. *IEEE Trans. Multimedia* 22, 2 (2019), 407–420.

[11] Ming Cheung, James She, and Zhanming Jie. 2015. Connection Discovery Using Big Data of User-Shared Images in Social Media. *IEEE Trans. Multimedia* 17, 9 (2015), 1417–1428.

[12] Ming Cheung, James She, and Lufi Liu. 2018. Deep learning-based online counterfeit-seller detection. In *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*. IEEE.

[13] Ming Cheung, James She, Weiwei Sun, and Jiantao Zhou. 2019. Detecting online counterfeit-goods seller using connection discovery. *ACM Trans. Multimedia Comput. Commun. Appl. (TOMM)* 15, 2 (2019), 1–16.

[14] Ming Cheung, James She, and Ning Wang. 2018. Characterizing User Connections in Social Media through User-Shared Images. *IEEE Trans. Big Data* 4, 4 (2018), 447–458.

[15] Alessandro Epasto, Silvio Lattanzi, Vahab Mirrokni, Ismail Oner Sebe, Ahmed Taei, and Sunita Verma. 2015. Ego-net community mining applied to friend suggestion. *Proceedings VLDB Endowment* 9, 4 (2015), 324–335.

[16] Wenqi Fan, Yao Ma, Qing Li, Yuan He, Eric Zhao, Jiliang Tang, and Dawei Yin. 2019. Graph neural networks for social recommendation. In *The World Wide Web Conference*. 417–426.

[17] Linton C Freeman. 1978. Centrality in social networks conceptual clarification. *Social Netw.* 1, 3 (1978), 215–239.

[18] Sahil Garg, Kuljeet Kaur, Neeraj Kumar, and Joel JPC Rodrigues. 2019. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective. *IEEE Trans. Multimedia* 21, 3 (2019), 566–578.

[19] Roger Guimera, Stefano Mossa, Adrian Turtschi, and LA Nunes Amaral. 2005. The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proceedings National Academy Sci.* 102, 22 (2005), 7794–7799.

[20] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep residual learning for image recognition. In *Proc. IEEE Conf. Comput. Vis. Pattern Recogn. (CVPR)*. 770–778.

[21] Julia Heidemann, Mathias Klier, and Florian Probst. 2010. Identifying key users in online social networks: A pagerank based approach. (2010).

[22] Yangqing Jia, Evan Shelhamer, Jeff Donahue, Sergey Karayev, Jonathan Long, Ross Girshick, Sergio Guadarrama, and Trevor Darrell. 2014. Caffe: Convolutional architecture for fast feature embedding. In *Proc. ACM Int. Conf. Multimedia (MM)*. ACM, 675–678.

[23] Dirk Koschützki and Falk Schreiber. 2008. Centrality analysis methods for biological networks and their application to gene regulatory networks. *Gene regulation systems biology* 2 (2008), GRSB–S702.
[24] Yuncheng Li, Liangliang Cao, Jiang Zhu, and Jiebo Luo. 2017. Mining fashion outfit composition using an end-to-end deep learning approach on set data. *IEEE Trans. Multimedia* 19, 8 (2017), 1946–1955.
[25] Abderrahmen Mtibaa, Martin May, Christophe Diot, and Mostafa Ammar. 2010. Peoplerank: Social opportunistic forwarding. In *Proc. INFOCOM*. IEEE, 1–5.
[26] Arjun Mukherjee, Bing Liu, and Natalie Glance. 2012. Spotting fake reviewer groups in consumer reviews. In *Proc. 21st Int. Conf. World Wide Web (WWW)*. ACM, 191–200.
[27] Arjun Mukherjee, Vivek Venkataraman, Bing Liu, and Natalie Glance. 2013. What yelp fake review filter might be doing?. In *Proc. 7th Int. AAAI Conf. Weblogs Social Media (ICWSM)*.
[28] Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. 1999. *The PageRank citation ranking: Bringing order to the web.* Technical Report. Stanford InfoLab.
[29] Florian Probst, Laura Grosswiele, and Regina Pfleger. 2013. Who will lead and who will follow: Identifying Influential Users in Online Social Networks. *Busin. Inf. Syst. Engin.* 5, 3 (2013), 179–193.
[30] Shailendra Rathore, Vincenzo Loia, and Jong Hyuk Park. 2018. SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook. *Applied Soft Comput.* 67 (2018), 920–932.
[31] Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, and Jong Hyuk Park. 2017. Social network security: Issues, challenges, threats, and solutions. *Inf. sci.* 421 (2017), 43–69.
[32] Shailendra Rathore, Pradip Kumar Sharma, and Jong Hyuk Park. 2017. XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs. *J. Inf. Process. Syst.* 13, 4 (2017).
[33] C. J. Van Rijsbergen. 1979. *Information Retrieval* (2nd ed.). Butterworth-Heinemann, Newton, MA, USA.
[34] David Savage, Xiuzhen Zhang, Xinghuo Yu, Pauline Chou, and Qingmai Wang. 2014. Anomaly detection in online social networks. *Social Netw.* 39 (2014), 62–70.
[35] James She, Chen Zhao, Ming Cheung, and Hao Liang. 2017. From Densification Power Law to Degree of Separation: A Case Study. In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 278–285.
[36] Fatemeh Sheikholeslami, Brian Baingana, Georgios B Giannakis, and Nikolaos D Sidiropoulos. 2016. Egonet tensor decomposition for community identification. In *Proc. Global Conf. Signal Inf. Process. (GlobalSIP)*. IEEE, 341–345.
[37] Enhua Tan, Lei Guo, Songqing Chen, Xiaodong Zhang, and Yihong Zhao. 2012. Spammer behavior analysis and detection in user generated content on social networks. In *Proc. Int. Conf. Distr. Comput. Syst. (ICDCS)*. IEEE, 305–314.
[38] Michael Trusov, Anand V Bodapati, and Randolph E Bucklin. 2010. Determining influential users in internet social networks. *J. Market. Research* 47, 4 (2010), 643–658.
[39] Alex Hai Wang. 2010. Don't follow me: Spam detection in twitter. In *Proc. int. conf. on Secur. crypt.* IEEE, 1–10.
[40] Xiang Wang, Xiangnan He, Meng Wang, Fuli Feng, and Tat-Seng Chua. 2019. Neural graph collaborative filtering. In *Proceedings of the 42nd international ACM SIGIR conference on Research and development in Information Retrieval*. 165–174.
[41] Yinwei Wei, Xiang Wang, Weili Guan, Liqiang Nie, Zhouchen Lin, and Baoquan Chen. 2019. Neural multimodal cooperative learning toward micro-video understanding. *IEEE Transactions on Image Processing* 29 (2019), 1–14.
[42] Yinwei Wei, Xiang Wang, Xiangnan He, Liqiang Nie, Yong Rui, and Tat-Seng Chua. 2021. Hierarchical User Intent Graph Network for Multimedia Recommendation. *IEEE Transactions on Multimedia* (2021).
[43] Ke Xu, Tanfeng Sun, and Xinghao Jiang. 2019. Video anomaly detection and localization based on an adaptive intra-frame classification network. *IEEE Trans. Multimedia* 22, 2 (2019), 394–406.
[44] Erjia Yan and Ying Ding. 2009. Applying centrality measures to impact analysis: A coauthorship network analysis. *J. American Society Inf. Sci. Techn.* 60, 10 (2009), 2107–2118.
[45] Chao Yang, Robert Chandler Harkreader, and Guofei Gu. 2011. Die free or live hard? empirical evaluation and new design for fighting evolving twitter spammers. In *Proc. Int. Workshop Recent Advances Intrusion Detection*. Springer, 318–337.
[46] Zhaoquan Yuan, Jitao Sang, Changsheng Xu, and Yan Liu. 2014. A unified framework of latent feature learning in social media. *IEEE Trans. Multimedia* 16, 6 (2014), 1624–1635.
[47] Qunyan Zhang, Haixin Ma, Weining Qian, and Aoying Zhou. 2013. Duplicate detection for identifying social spam in microblogs. In *Proc. IEEE Int. Congr. Big Data*. IEEE, 141–148.
[48] Xianghan Zheng, Zhipeng Zeng, Zheyi Chen, Yuanlong Yu, and Chunming Rong. 2015. Detecting spammers on social networks. *Neurocomputing* 159 (2015), 27–34.