Detecting Online Counterfeit-goods Seller using Connection Discovery

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

With the advancement of social media and mobile technology, any smartphone user can easily become a seller on social media and e-commerce platforms, such as Instagram and Carousell in Hong Kong or Taobao in China. A seller shows images of their products and annotates their images with suitable tags that can be searched easily by others. Those images could be taken by the seller, or the seller could use images shared by other sellers. Among sellers, some sell counterfeit goods, and these sellers may use disguising tags and language, which make detecting them a difficult task. This article proposes a framework to detect counterfeit sellers by using deep learning to discover connections among sellers from their shared images. Based on 473K shared images from Taobao, Instagram, and Carousell, it is proven that the proposed framework can detect counterfeit sellers. The framework is 30% better than approaches using object recognition in detecting counterfeit sellers. To the best of our knowledge, this is the first work to detect online counterfeit sellers from their shared images.

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, deep learning

ACM Reference format:
Ming Cheung, James She, Weiwei Sun, and Jiantao Zhou. 2019. Detecting Online Counterfeit-goods Seller using Connection Discovery. *ACM Trans. Multimedia Comput. Commun. Appl.* 15, 2, Article 35 (May 2019), 16 pages.
https://doi.org/10.1145/3311785

1 INTRODUCTION

In the past, it was hard to become an online seller as technical knowledge of system design and programming were required. Recently, thanks to social media and e-commerce platforms, sellers have become able to set up an online store conveniently, with just a few clicks, and share their product images with suitable tags online. Such images are made widely accessible to others so that

This work was supported in part by HKUST-NIE Social Media Lab., HKUST, and the Macau Science and Technology Development Fund under Grants No. FDCT/022/2017/A1 and No. FDCT/077/2018/A2, and in part by the Research Committee at the University of Macau under Grants No. MYRG2016-00137-FST and No. MYRG2018-00029-FST.
Authors' addresses: M. Cheung, J. She, Room 2430, HKUST, Clear Water Bay, Sai Kung, Hong Kong; W. Sun, and J. Zhou, E11-2024a, Faculty of Science and Technology, University of Macau, E11, Avenida da Universidade, Taipa, Macau, China.

1551-6857/2019/05-ART35 $15.00
https://doi.org/10.1145/3311785

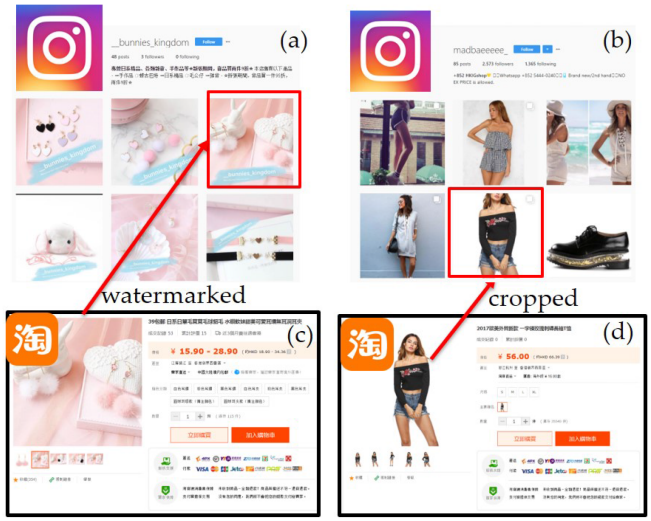

Fig. 1. User interface (UI) on (a, b) Instagram and (c, d) Taobao. The product images on (a) and (b) are from (c) and (d), respectively.

potential customers can easily access them by searching their tags, or customers can follow sellers to receive new product images. The number of online sellers has grown rapidly in the past few years. Products available range from ornaments and electronics to almost anything. It is estimated that the Asian e-commerce platform Carousell, which launched in 2012, has more than 57 millions products listed for sales.[1] These products include second-hand goods, self-made products, and resale products.

As it is very easy to become a seller on such platforms, the number of counterfeit products being sold online has increased substantially. Most online sellers do not have an offline store, and it is not possible to investigate their goods before buying them, which makes detecting such products difficult. E-commerce giants like Amazon and Alibaba dedicate significant effort to removing counterfeit products. However, they are still widely accessible as counterfeit goods must be manually flagged and removed.[2] This approach creates challenges for e-commerce platform owners, brand owners, and customs officers. Using manual effort to detect a small number of counterfeit sellers from among the hundreds of thousands of sellers is inefficient, and it is not scalable to the rapid growth of online sellers. An effective detection framework may help reduce the search space by identifying potential counterfeit sellers for further investigation.

Traditionally, detecting counterfeit sellers has been conducted by searching suitable tags and then browsing sellers whose products contain those tags. However, such sellers may use disguising text such as “toy watch” or “high-quality shoes,” meaning a text-based detection system will perform poorly at detecting these sellers. In contrast, the images used on posts are more consistent than texts. Similar images are used for the same product across sellers, to attract customers. Figure 1 shows two examples of how sellers use images from other sources, such as Taobao, to display their products on Instagram. Sellers often process the product images from their source, with techniques such as watermarking, cropping, and so on, before posting them on their own store. In recent years, a lot of progress has been made in object recognition using convolutional neural networks (CNNs), which are designed to automatically learn features that are sensitive to

[1] https://blog.carousell.com/2017/01/26/a-new-year-a-new-home-and-a-new-blog/.
[2] https://consumerist.com/2017/03/22/amazon-steps-up-effort-to-rid-site-of-counterfeit-products/.

the targeted objects using given samples for training. The extracted features can also be used for connection discovery using user-shared images for applications such as follower/followee recommendation [5]. A framework is hence proposed to detect counterfeit sellers through a CNN using images from sellers who have been previously convicted or reported for selling counterfeit goods.

This article conducts an intensive study on counterfeit and non-counterfeit sellers on social media using connection discovery. The sellers are labelled manually by surveying 40 experienced online shoppers to mark each seller independently. Hence, a classifier is built based on a fine-tuned CNN through their connections. The following contributions are made in this article: (1) We collect 473K shared images from Taobao, Instagram and Carousell. (2) We analyse the behaviors of counterfeit sellers using object recognition and connection discovery approaches and prove that related sellers share more similar images. (3) We propose an optimised framework to detect counterfeit sellers using connections discovered from their shared images. (4) We conduct a showcase to prove that the proposed framework can work even if the counterfeit sellers edit the images using various methods.

This article is organised as follows: Section 2 presents related works, followed by the proposed framework in Section 3, where we discuss how connections can be discovered. Section 4 introduces the dataset and measures the characteristic of it. Section 5 gives the experimental results, and Section 6 concludes the article.

2 RELATED WORKS

Detecting abnormal users on social networks has been studied for a long time. Researchers have tried various ways to detect various kinds of abnormal users. Some works are dedicated to discovering influential [18, 25] or key users [10], while others are working to discover negative users, for example, detecting paid posters on social media [4], sexual predators [17], or fake reviewers on Amazon [16]. The methods for detecting abnormal users are varied. The most common technique is to investigate the social information among users. If a user is a spammer, or a fake account, then their social graph will be significantly different from that of other users [21]. Accordingly, a series of methods for detecting spam or spammers have been proposed [23, 26, 29, 30]. For example, the social graph of a normal user can be clustered based on their common friends, while this is not the case for spammers. However, such patterns may not be observed among counterfeit sellers as their accounts are generated by individuals instead of computers, or social information is not available on platforms such as Amazon and Taobao.

Another solution is to locate the supply chain in social networks to identify the counterfeiting activity parties [24], such as their supply chain. However, it is observed that most counterfeit sellers are independent, and their supply chain is offline and difficult to find with this method. Another approach is to analyse the content shared by users. The credibility of users can be used to detect cyberbullying in social networks [20] by understanding the information sent or posted by users. However, this technique prefers to process text, and the feature extraction is based on keyword extraction, which makes it difficult to apply to counterfeit seller detection. Fake reviewers can also be detected through understanding their content sharing behaviors, such as by analysing the content similarity [4, 16]. The content shared by fake reviewers is similar, as they are copying each other without making changes. Counterfeit sellers also copy content from official sellers or other sources, as they do not want to reveal to customers that they are selling counterfeit products, but they will modify images to prevent being detected. Figures 1(a) and 1(b) show two Instagram sellers who are posting images from another website, Taobao, and the original images are shown in Figures 1(c) and 1(d). The Instagram sellers have watermarked and cropped the images before posting them.

Recently, discovering connections from shared images on social media has proven to be effective for many applications, such as follower/followee recommendation and gender prediction [5, 7]. As

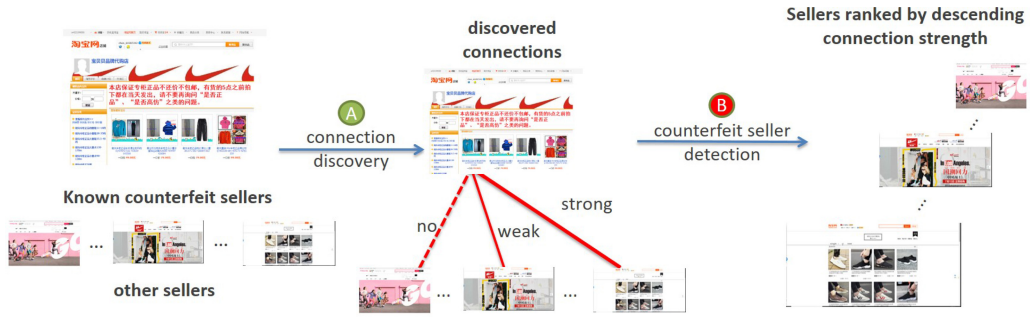

Fig. 2. System flow of the detection.

the products sold by counterfeit sellers are similar to those of official sellers, the connections among them can be discovered through their shared images. Hence, this article utilises deep learning techniques [3, 12] to detect the connections among sellers, and identify potential counterfeit sellers for further investigation.

The goal of the CNN training is to make images of related users more likely to be annotated with the same machine-generated label, and images from unrelated pairs likely to be tagged with very different labels. The optimization can be conducted by a Siamese network [2, 13, 28], for which the objective is that the output of the CNN is a vector that maximises the distances between images of unrelated pairs, and minimises the distances between images of related pairs. Siamese networks have been used in many applications, such as tracking [2], face recognition [8, 11] and multimedia data retrieval [14, 27]. However, one of the drawbacks of Siamese network is that the number of samples is much larger than that for classification. Hence, this article applies classification, by putting all images from counterfeit sellers into one class, and the images from non-counterfeit sellers into another class. The layer before classification is extracted for encoding images.

This article extends our previous work [6] in the following ways: (1) a new framework that can classify sellers into counterfeit and non-counterfeit; (2) optimization of the CNN for connection discovery and a better result in seller classification; (3) a new dataset from Taobao, and counterfeit and non-counterfeit sellers are labelled; and (4) measurements to show the differences among counterfeit and non-counterfeit sellers.

3 COUNTERFEIT SELLER DETECTION AND CONNECTION DISCOVERY

The goal of this article is to detect those that are likely to be counterfeit sellers. This section introduces the proposed method to identify counterfeit seller using machine generated labels. Figure 2 shows the flow of the proposed framework. The images are first encoded as vectors, followed by a clustering process to group similar images, and the images among the same cluster are assigned with the same label.

3.1 Image Encoding using Convolutional Neural Network

Recently, CNNs have become the most successful techniques in visual object recognition [3, 12]. CNNs are inspired by the human visual system, in which neurons are arranged to respond to small spatial regions. The structure of a CNN comprises several layers of non-linear feature detectors, which are handcrafted with learnable weights and biases from data. The CNN is trained in a supervised manner, in which once the network architecture is defined, the training is just to give the input (images) and the desired output (objects in an image). Different from hand-crafted features, a CNN is capable of locating visual features based on the objective function, such as detecting

social signals from images. Images are encoded using a CNN, as it provides the best performance in object recognition. As the CNN is trained and designed for object recognition, images are encoded such that they are sensitive to objects in images. However, this may not be possible in the case of counterfeit seller detection, as the difference between non-counterfeit and counterfeit sellers may not be the objects in their shared images. Hence, we are motivated to investigate how to optimise the weight of a CNN, $\mathbf{W}$, for counterfeit seller detection.

A novel idea proposed in this section is to optimise $\mathbf{W}$ so that it is sensitive to visual features that can help to detect counterfeit sellers. One of the possible objectives is to minimise the distance among images of counterfeit sellers, and to minimise that among non-counterfeit sellers, as well as to maximise that between counterfeit and non-counterfeit sellers. As a result, the images from related pairs are more likely to be annotated with similar machine-generated labels, while the images from unrelated pairs are less likely to be annotated with the same machine-generated labels. Hence, counterfeit sellers have a more similar seller profile, and training a classifier to identify those sellers would be more effective. The distance between two images, x_1 and x_2, can be computed by

$$D(x_1, x_2, \mathbf{W}) = ||f(x_1, \mathbf{W}) - f(x_2, \mathbf{W})||, \tag{1}$$

where $f(, \mathbf{W})$ is the encoded vector of an image using a CNN with weight $\mathbf{W}$. It is desirable to obtain a $\mathbf{W}$ such that the distances among images of related sellers are small, and the distances among images of unrelated sellers are large.

Conventionally, $\mathbf{W}$ can be optimised by using a Siamese network, in which $\mathbf{W}$ is optimised by minimising the distance between images of related pairs, and maximising the distance between images of unrelated pairs. However, one of the drawbacks of Siamese network is that the training does not always give reasonable results, for example, all the images are encoded to zeros, which cannot be used for further computation. As well, the number of samples is much larger than that for classification. Hence, this article applies classification, by putting all images from counterfeit sellers into one class, and the images from non-counterfeit sellers into another class. The layer before classification is extracted for encoding images.

3.2 Discovering the Connections among Sellers

The connection between any two sellers is defined as their similarity $S_{i,j}$. Each image is encoded into a feature vector using image processing and computer vision techniques, as shown in step 1 of Figure 3. All feature vectors of the user-shared images from every user are clustered [15] into K clusters, and annotated by a unique machine-generated label that represents the cluster it belongs to, as shown in steps 2 and 3 of Figure 3. A seller i is then profiled by a K-dimensional vector, L_i, that describes the distribution of K unique labels on the images shared by this seller:

$$L_i = (l_{i,1}, \ldots, l_{i,k}, \ldots, l_{i,K}), \tag{2}$$

where $k \leq K$, $l_{i,k}$ is the frequency of the kth label in the profile, L_i, and K is the total number of unique labels in the system, as shown by step 4 of Figure 3. If the images are encoded using object-based encoder, such as ResNet [9], then the images in the same cluster are more likely to be with the same objects. Given the profiles, L_i and L_j, of seller i and j, their similarity, $S_{i,j}$, can be evaluated through their shared images by

$$S_{i,j} = S(L_i, L_j) = \frac{L_i \cdot L_j}{||L_i|| \cdot ||L_j||}, \tag{3}$$

where $\cdot$ is the dot product of two vectors and $||.||$ is the L2 norm of a vector.

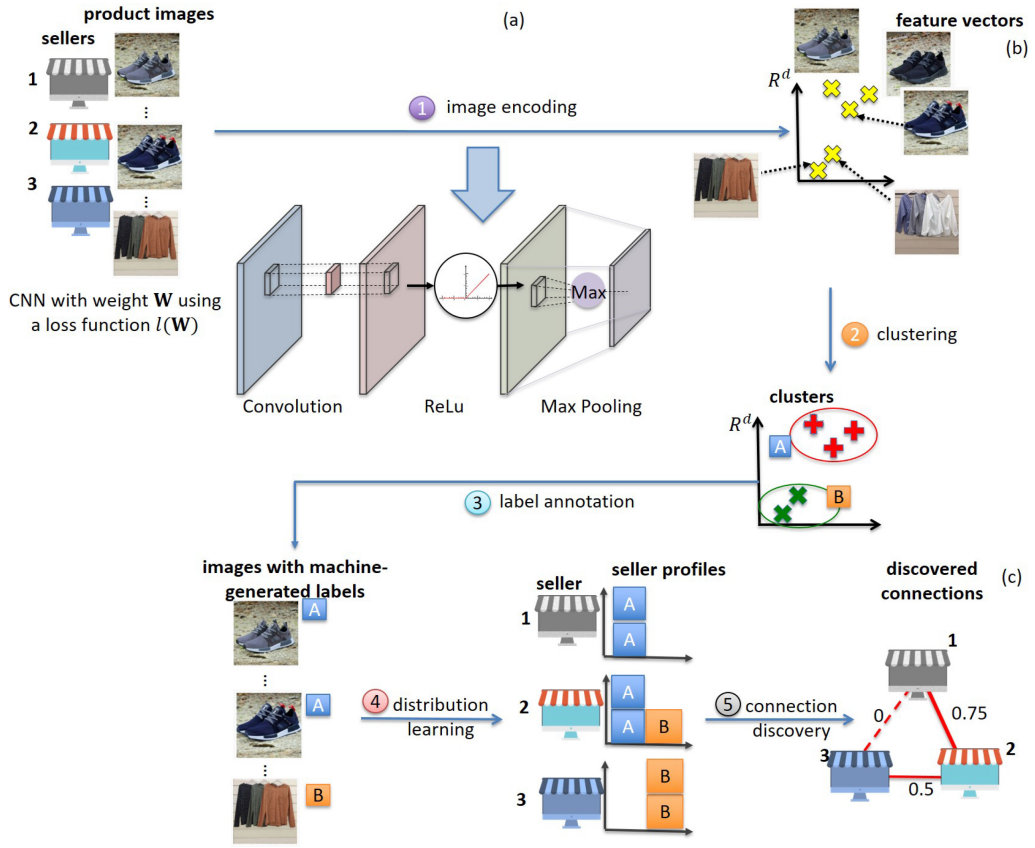

Fig. 3. System flow of the connection discovery.

3.3 Hypothesis Testing of Counterfeit Seller Detection

This section introduces hypothesis testing of how counterfeit sellers can be detected. We consider the following two hypotheses:

(1) H_0: The seller i is a counterfeit seller;
(2) H_1: The seller i is not a counterfeit seller.

The first, H_0, is the null hypothesis that seller i is a counterfeit seller, while the second one, H_1, is that i is not a counterfeit seller. Given the two hypotheses, there are four possible outcomes when a decision is made. The decision is called a true positive when the algorithm selects H_1 when H_1 is, in fact, true. However, if the algorithm chooses H_0, it is called a false negative. Likewise, when H_0 is, in fact, true, picking H_1 constitutes a false positive. Finally, picking H_0 when H_0 is true is true negative.

A binary classifier is proposed for hypothesis testing. In the training of the binary classifier, a seller is labelled as a counterfeit or a non-counterfeit seller, with an expected output, Λ, of 1 and 0, respectively. Hence, the binary classifier gives an output range from 0 to 1, with 0 representing certainty that a user is a non-counterfeit seller, and 1 representing certainty that a user is a counterfeit seller. If Λ is greater than a threshold, α, then H_0 is accepted; otherwise, it is rejected.

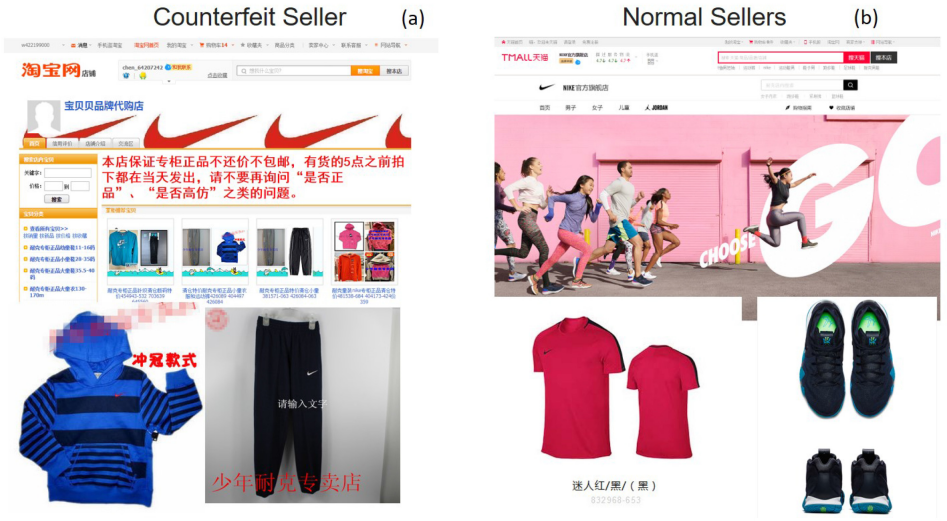

Fig. 4. Examples of images from (a) a counterfeit seller and (b) a non-counterfeit seller.

4 SHARED IMAGES AND COUNTERFEIT SELLERS

This section presents a quantitative measurement of the shared images from sellers from the object recognition and connection discovery perspectives and concludes how and why the proposed framework helps to detect counterfeit sellers.

4.1 Dataset

Data is collected from Taobao, a popular Chinese e-commerce platform. On Taobao, there are individual sellers and famous brands, so it contains a wide range of products. Figure 4 shows examples of images shared by counterfeit sellers and non-counterfeit sellers, as well as the page of their stores on Taobao. It is observed that these are not similar. As shown in Figure 4, the store of the counterfeit seller is simpler and contains more words. However, the store of the non-counterfeit seller looks more attractive. There are differences in their product images also. Although the products and objects in the images of the two sellers in Figure 4 are similar, a human can easily tell that they are not in the same style. Images from counterfeit sellers are not professionally taken, and watermarks are added. The images from a non-counterfeit seller are clean and do not have a background. Hence, it is interesting to investigate the differences.

The collected data can be divided into two categories, shoes and cosmetics, which are commonly found on Taobao. The information, including the prices and images of the products are collected using Octopus.[3] For each seller, 80 products are selected from their product list, and all images of each product is collected. To avoid the interference of thumbnails and advertising images, we set the minimum size of the captured images to 400×400. In total, 101,090 and 51,870 images are collected from 93 and 100 shoes and cosmetics sellers, respectively. There are 38 counterfeit and 55 non-counterfeit sellers among the shoe sellers, while there are 23 counterfeit and 77 non-counterfeit sellers among the cosmetics sellers. The sellers are labelled manually by surveying 40 experienced online shoppers to mark each seller independently by considering the seller's pages, images, and price. Finally, the statistical value of the survey results is used as the label for each seller.

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

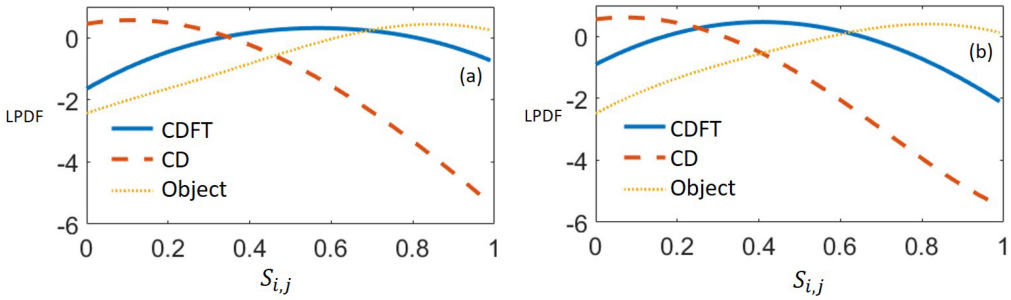

Fig. 5. Measurement of object recognition and connection discovery on (a) shoe sellers and (b) cosmetics sellers.

4.2 Discovering Connections Using Object Recognition

Object recognition is a very common way to detect what a seller is selling. It is conceivable that among the same types of sellers, the goods they sell must have a certain relevance. This section shows measurements between counterfeit and non-counterfeit sellers from the object recognition perspective. All images are encoded with ResNet [9] with 1,000 class labels, and user profiles are built based on the occurrences of the 1,000 labels. These profiles are further used to calculate $S_{i,j}$ for related and unrelated pairs using Equation (3), and the logged PDF (LPDF) of related pairs are shown in the dot line (Object) in Figures 5(a) and 5(b), for shoe and cosmetics sellers, respectively. The method of density estimation [22] is applied to estimate the LPDF from the observed discrete data with a kernel estimator with a window width of 0.2. It is observed that most related pairs have a high similarity for both shoe and cosmetics sellers. One of the reasons is that the sellers are selling the same types of goods, and hence $S_{i,j}$ is high among them.

4.3 Discovering Connections Using Machine-generated Labels

This section shows measurements between counterfeit and non-counterfeit sellers using discovered connections from machine-generated labels. The flow in Figure 3 is applied to tag every image with a machine-generated label, and user profiles are built based on the occurrence of the labels, and $S_{i,j}$ is computed using Equation (3). The first approach uses the connection discovery (CD) [7], which encodes images from sellers with a pre-trained CNN. The images are encoded using ResNet, and the classification layers are removed, with K equal to 1,000. The logged probability density functions (PDF) of related pairs are shown by the broken line in Figures 5(a) and 5(b), for shoe and cosmetics sellers, respectively, using density estimation. Different from Object, most of the pairs have a relatively small $S_{i,j}$, and only a few pairs have a high $S_{i,j}$. This shows an advantage of the proposed approach: As images are grouped based on the feature vectors, if images are similar (e.g., similar objects), two images have to be very similar to be tagged with the same label. However, if images are not similar (e.g., very different objects), two images can be tagged with the same label even though they contain different objects.

Hence, it is interesting to fine-tune the CNN such that it is sensitive to counterfeit images. The connection discovery using a fine-tuned CNN (CDFT) targets extracting features that are sensitive to connections. This article applies classification for the training by putting all images from counterfeit sellers into one class, and the images from non-counterfeit sellers into another class. The layer before classification is extracted for encoding images and using the flow above to compute $S_{i,j}$. The results are shown by the solid line in Figures 5(a) and 5(b). It is observed that most pairs have a similarity of 0.4 to 0.5. This motivates us to investigate how these methods will affect the detection, and the results are presented in the next section.

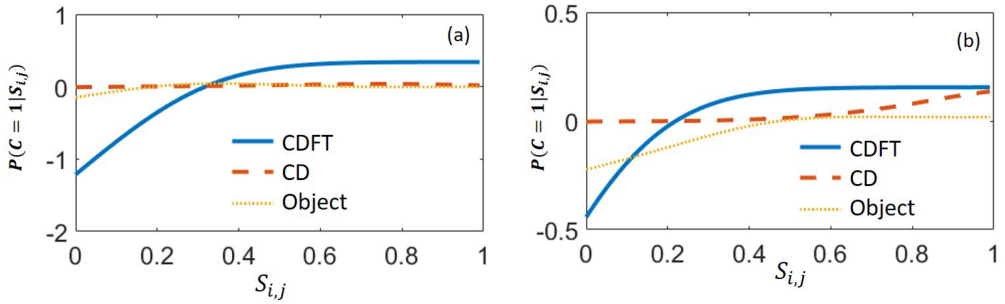

Fig. 6. The increasing trend among (a) shoe sellers and (b) cosmetics sellers. Higher $S_{i,j}$ implies a higher probability that two sellers will be collected.

4.4 Rising Trend of Related Pairs

It is interesting to investigate if Λ is an increasing function. Figures 6(a) and 6(b) show the measurement of logged Λ using density estimation employing different methods: Object, CD, and CDFT. It is observed that only CDFT gives a clear trend, in which the chance that a pair of users is counterfeit sellers is higher when the two users have a higher $S_{i,j}$. However, Object and CD do not show a clear trend in the figure. Hence, when using CDFT, it is observed that they are all increasing functions, which means that the probability that the two sellers belong to the same class will also increase with $S_{i,j}$.

This section has investigated the relationship among sellers using different methods. Given the rising trend, we are motivated to investigate how counterfeit sellers can be detected using classification. The next section presents the experimental results and the discussions.

5 EXPERIMENTAL RESULTS

This section discusses the dataset, experiment settings, and results of an experiment to test the proposed framework. The goal of the experiment is to identify sellers that are likely to be counterfeit sellers.

5.1 Experimental Settings

As proposed, classifiers are built to identify counterfeit sellers. All images are encoded with different approaches: The first is CD, in which the images are ResNet [9], with the same network structure by taking the layer before softmax as the base. The second one is CDFT, in which the network is fine-tuned by considering that images from counterfeit sellers belong to one class and images from non-counterfeit sellers belong to another class. The encoded images are clustered using K-means++ [1]. Seller profiles are built by the occurrence of machine-generated labels, which are the cluster labels. The occurrence of the labels of a seller's images is the profile of the seller. To better evaluate the performance, the third approach is Object, which makes use of the 1,000 classes in ResNet to build the seller profile. The user is split into training and testing sets, and the result is evaluated by $F1$ [19] as

$$F1 = \frac{2pr}{p + r}. \tag{4}$$

$F1$ gives a good balance between precision p and recall r. If only confidence recommendations are made (e.g., pairs with a high $S_{i,j}$), then a high precision can be achieved with a low recall.

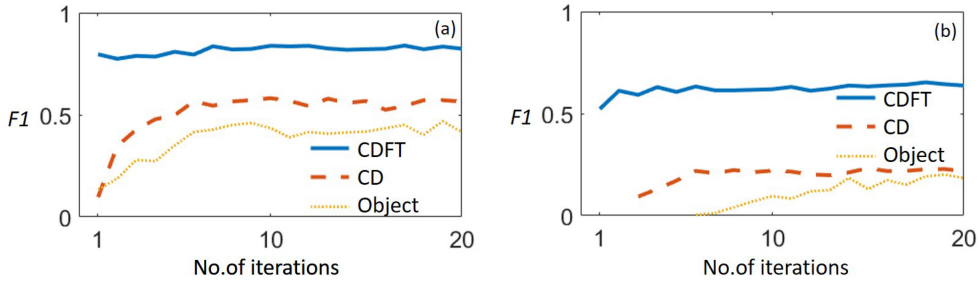

Fig. 7. Precision of detection for number of iterations in training: (a) shoe sellers and (b) cosmetics sellers.

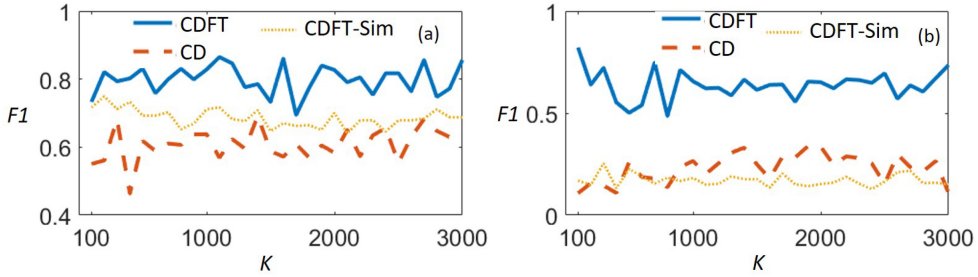

Fig. 8. Precision of detection for different values of K for (a) shoe sellers and (b) cosmetics sellers.

5.2 Experimental Results

Figures 7(a) and 7(b) show the results of counterfeit seller identification, with the number of iterations in training, for shoe and cosmetics sellers, respectively. The experiment is repeated 100 times, and the mean is taken among the 100 results. In each trial, 90% of users are randomly selected as the training set, and the rest are the testing set. Note that CD and CDFT use $K = 1{,}000$ for comparison with Object, which has 1,000 class labels. It is observed that the performance improves with more iterations, and CDFT out-performs the other two approaches, with about 80% accuracy for both shoe and cosmetics sellers. CD is the second-best performer, as Object fails to represent users. More discussion can be found in the next section. Hence, it also interesting to investigate how K affects the performance of the detection.

Figures 8(a) and 8(b) show the results of counterfeit seller identification with different K for shoe and cosmetics sellers, respectively. The experiment is repeated 20 times, and the mean is taken among the 20 results. In each trial, 90% of users are randomly selected as the training set, and the rest are the testing set. The performance of the 10th iteration is used for the evaluation. The result is also compared with siamese network (CDFT-Sim) [2, 13, 28], for which the objective is that the output of the CNN is a vector that maximises the distances between images of unrelated pairs, and minimises the distances between images of related pairs. It is observed that CDFT out-performs the CD and CDFT-Sim approaches for any values of K. The performance is similar with different values of K. More discussion on finding an optimised K can be found in the later section.

Figures 9(a) and 9(b) show the p of counterfeit seller identification with different α for shoe and cosmetics sellers, respectively. The training is repeated 100 times, and the Λ of all data in the testing sets are recorded, and tested against different values of α. It is observed that p increases with α, and reaches a maximum of 0.94 and 0.95 when α equals 0.99. This means that for sellers with Λ equal to 0.99, about 95% are counterfeit sellers. Note that a high p will result in a low r, and a lot of counterfeit sellers are not detected.

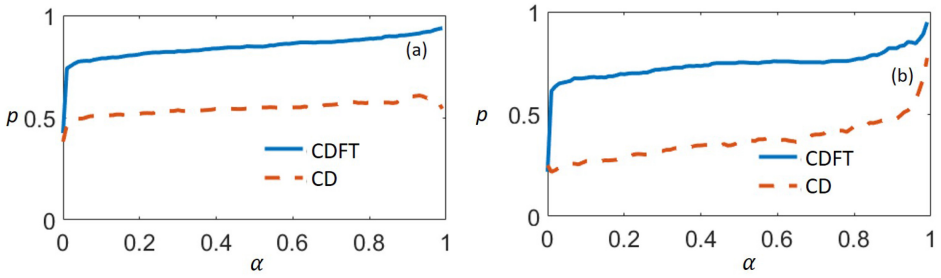

Fig. 9. Precision of detection for different values of K for (a) shoe sellers and (b) cosmetics sellers.

The effectiveness of the proposed framework has been proven in this section. On other social media platforms, however, counterfeit sellers may not take images of their products but will use the images from non-counterfeit sellers. Hence, it is interesting to synthesise a dataset for experiments to evaluate if the proposed framework works for such sellers, and the results are presented in the next section.

5.3 Showcase: Counterfeit Sellers Detections

The experiment involves discovering connections between known counterfeit sellers and other sellers, and aims to recommend sellers for further investigation. An Instagram dataset and a Carousell dataset are collected for the experiment. Instagram is an image-oriented social media platform, while Carousell is an e-commerce platform with social network features. On both platforms, sellers post their products' details, including images, prices and other text descriptions. Both sellers and customers may follow others to get their latest product posts. The Instagram dataset includes 60,018 images from 138 sellers on Instagram. Sellers are Hong Kong-based, and are searched manually using tags, such as "#hkonlinestore." The Carousell dataset includes 259,926 images from 785 sellers. Sellers are also Hong Kong-based, and are searched through four of the categories listed on Carousell: "Men's Tops," "Women's Tops," "Design & Craft," and "Everything Else." Images are scraped using the Scrapy[4] framework, as there is no API available.

The steps are shown in Figure 2. Counterfeit sellers are synthesised with observations of how such sellers share images, as shown in Figure 1. Images are likely to be downloaded from other sources, and they are processed by counterfeit sellers before they are posted. Figure 1 shows how images are processed by counterfeit sellers. Some common methods are cropping, flipping, shrinking, color-tuning, or watermarking. Using this observation, known and target counterfeit sellers in the experiment are synthesised from collected sellers as follows: (1) a seller is randomly selected as a known counterfeit seller; (2) 50% to 100% of the images of the known counterfeit seller are then randomly selected; (3) selected images are processed using common processing methods to become photos posted by synthesised counterfeit sellers; and (4) steps (1)–(3) are repeated until the desired number of counterfeit sellers are synthesised. The detection is conducted using CD, without classification.

Figure 10 shows the results of the experiments. The proposed framework (proposed) is compared with manual searching (manual). It is observed that the proposed framework can provide an accurate list of potential counterfeit sellers. While there are only 8 target counterfeit sellers, the framework maintains p of 0.3 or above and achieves r of at least 0.8 within 20 recommendations. Instead of scanning all sellers, 7 out of 8 counterfeit sellers are located within 20 recommendations, which translates to a saving of 95% of the manual effort. This result proves the proposed

[4]https://scrapy.org/.

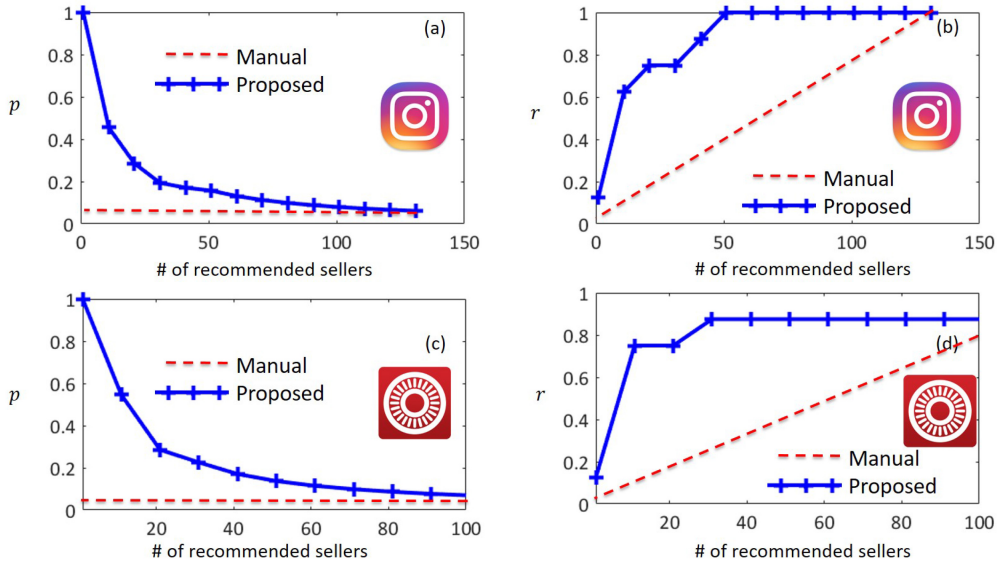

Fig. 10. Results of counterfeit sellers detection: (a) p and (b) r.

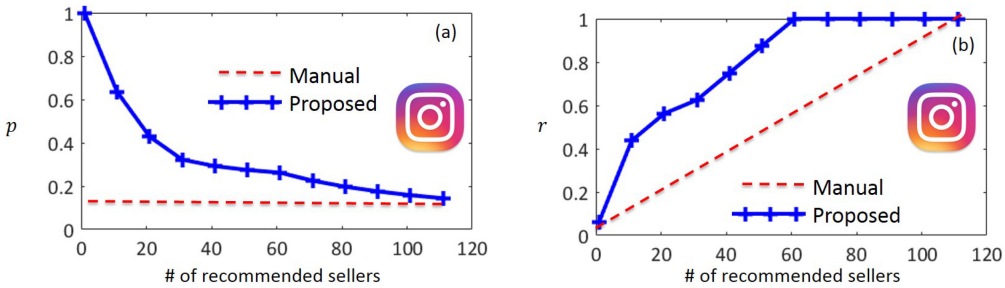

Fig. 11. Results of Taobao sellers detection: (a) p and (b) r.

framework can reduce the loading of manual screening by recommending sellers with a higher chance of being counterfeit sellers.

5.4 Showcase: Taobao Seller Detection on Instagram

A showcase is conducted to show how to detect Taobao sellers using the proposed framework. The images from each seller are checked manually, and a seller is labelled as a Taobao seller if the seller has more than 50% of their product images from Taobao. In total, there are 33 Taobao sellers, of which 17 are regarded as known Taobao sellers and are used to locate the rest of the Taobao sellers by discovering connections using the same framework. The result is shown in Figure 11. It is observed that at 20 recommendations, over 60% of Taobao sellers can be detected. This result shows that the proposed framework can find potential Taobao sellers on other social media.

5.5 Error Analysis

This section shows cases in which the proposed algorithm, as well as others, fails to detect counterfeit sellers. In such cases, pairs of normal and counterfeit sellers have a high $S_{i,j}$, and examples are shown in Figure 12. Under Object, two users with similar objects have a high $S_{i,j}$, as shown in

Fig. 12. Error analysis on: (a) Object, (b) CD, and (c) CDFT.

Figure 12(a). However, the differences are obvious to a human: images from non-counterfeit sellers are taken against a white background, while the images from counterfeit sellers are taken against various backgrounds. Object recognition approaches cannot give a good classification result, as the tags on the images of non-counterfeit and counterfeit sellers are very similar, and hence so are their profiles. Figure 12(b) shows a pair of non-counterfeit and counterfeit sellers with a high $S_{i,j}$ under CD. It is observed that they share visually similar images, and hence it is not easy for CD to tell the difference without fine-tuning. Figure 12(c) shows another pair of normal and counterfeit sellers with a high $S_{i,j}$ under CDFT, and it is observed that the images shared by the counterfeit and non-counterfeit sellers are similar. As the sellers are labeled by information, such as seller page and price, more than images, it is not possible for CDFT to tell the difference between non-counterfeit and counterfeit sellers. One of the solutions is to consider information besides the shared images from the sellers.

5.6 Discussion

The proposed approach makes use of known counterfeit sellers to optimize the CNN for detecting counterfeit sellers. The approach can capture patterns on images that could be added by counterfeit sellers. The proposed approach shows promising results in detecting counterfeit sellers, but it is limited to the training sets. While manually effects are required to verify whether there are new types of images among counterfeit sellers, the proposed approach could detect most of the counterfeit sellers and learn the new type through continuous training. As the proposed approach can be optimized with more data, there is no intrinsic relations between the experimental results and the products in the dataset. Shoe and cosmetic sellers are selected as they are very common commodities, but the proposed approach is applicable to any goods selling online.

The approach, CDFT-Sim, only slightly increases the performance of CD, while CDFT improves the result significantly. Possible reasons are that CDFT-Sim requires more data for training, and

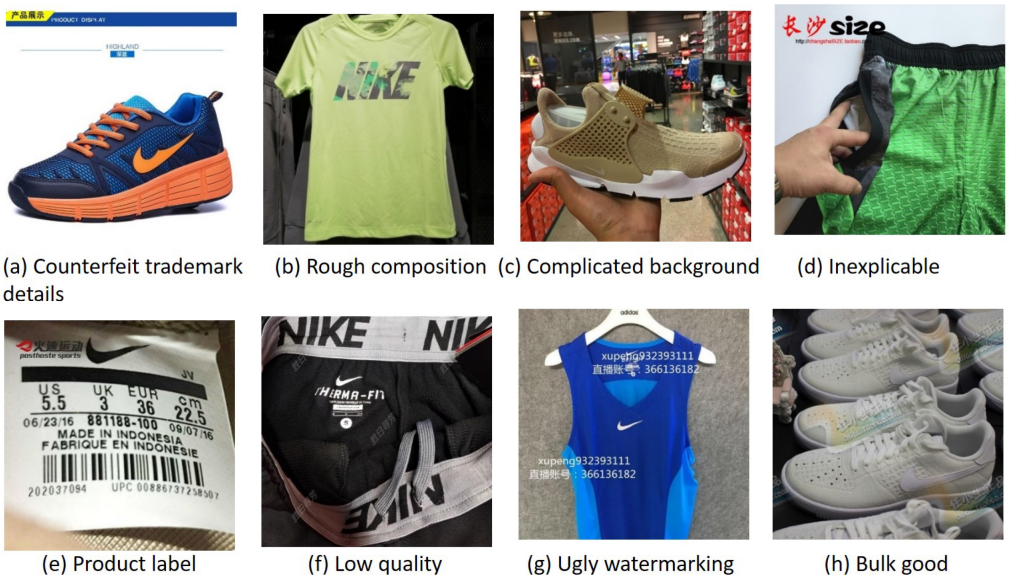

Fig. 13. Example images from of counterfeit sellers.

CDFT-Sim may generate unstable results. As well, CDFT-Sim is more computationally intensive. Hence, CDFT-Sim is more suitable for tasks that cannot be trained by CDFT, such as optimizing a CNN for follower/followee recommendation. In the follower/followee recommendation, images from related users should be closer while images from unrelated users should be father away. For three users, there could be one related and two unrelated pairs, and images cannot be classified into two classes.

Figure 13 shows examples of images from counterfeit sellers. There are various types, such as low image quality, ugly watermarking, complicated background, and so on. In general, the traditional detection methods are based on some unique features and can only handle a small part of these counterfeit-goods sellers' images, e.g., use text detection-based method to recognize some watermarked image or use image quality detection-based method to find the low-quality images. However, they are not applicable as these images are the features extracted and not ubiquitous. However, CNN can be optimized for extracting these features for detecting sellers who share images with these features.

There are two directions to improve performance. The first is to incorporate Object with CDFT. Although Object cannot help to classify counterfeit and non-counterfeit sellers, it can help to group sellers who are selling similar products, and the CDFT can be built based on the results. The second direction is to investigate different parameters, such as K, the number of unique machine-generated labels. Although it is proven that the proposed algorithm works with different K, it is not clear how to optimise the selection. An optimised value of K could give a better performance.

6 CONCLUSION

This article proposes a framework to detect online counterfeit sellers, who previously had to be manually detected. A CNN-based connection discovery framework is proposed. It utilises the trend to detect counterfeit sellers and is fine-tuned for discovering connections among sellers, and hence detecting them. Experiments are conducted with real-life datasets with over 450K shared images from the social media and e-commerce platforms Taobao, Instagram, and Carousell, and the

effectiveness of the proposed framework is proven. The framework can achieve over 90% in $F1$ score for detecting counterfeit sellers. With the rapid growth of online sales, there is a great need for detecting counterfeit sellers. The proposed framework greatly reduces the manual effort currently needed to detect them. To the best of our knowledge, this is the first work to detect online counterfeit sellers from their shared images.

REFERENCES

[1] David Arthur and Sergei Vassilvitskii. 2007. k-means++: The advantages of careful seeding. In *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms*. Society for Industrial and Applied Mathematics, 1027–1035.

[2] Luca Bertinetto, Jack Valmadre, João F. Henriques, Andrea Vedaldi, and Philip H. S. Torr. 2016. Fully-convolutional siamese networks for object tracking. In *Proceedings of the European Conference on Computer Visualization*. Springer, 850–865.

[3] 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*.

[4] Cheng Chen, Kui Wu, Venkatesh Srinivasan, and Xudong Zhang. 2013. Battling the internet water army: Detection of hidden paid posters. In *Proceedings of the IEEE/ACM International Conference on Advances Social Network Analysis Mining (ASONAM'13)*. IEEE, 116–120.

[5] 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.

[6] Ming Cheung, James She, and Lufi Liu. 2018. Deep learning-based online counterfeit-seller detection. In *Proceedings of theIEEE Conference on Computer Communication Workshops (INFOCOM'18)*. IEEE.

[7] Ming Cheung, James She, and Ning Wang. 2017. Characterizing user connections in social media through user shared image. *IEEE Trans. Big Data* (2017).

[8] Haoqiang Fan, Zhimin Cao, Yuning Jiang, Qi Yin, and Chinchilla Doudou. 2014. Learning deep face representation. *arXiv preprint arXiv:1403.2802*.

[9] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Visualization and Pattern Recognition*. 770–778.

[10] Julia Heidemann, Mathias Klier, and Florian Probst. 2010. Identifying key users in online social networks: A pagerank based approach. In *Proc. 31st Inform. Syst. Int. Conf.* 79.

[11] Junlin Hu, Jiwen Lu, and Yap-Peng Tan. 2014. Discriminative deep metric learning for face verification in the wild. In *Proceedings of the IEEE Conference on Computer Visualization and Pattern Recognition*. 1875–1882.

[12] 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 *Proceedings of the ACM International Conference on Multimedia*. ACM, 675–678.

[13] 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.

[14] Venice Erin Liong, Jiwen Lu, Yap-Peng Tan, and Jie Zhou. 2017. Deep video hashing. *IEEE Trans. Multimedia* 19, 6 (2017), 1209–1219.

[15] Andrew McCallum, Kamal Nigam, and Lyle H. Ungar. 2000. Efficient clustering of high-dimensional data sets with application to reference matching. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery Data Mining*. ACM, 169–178.

[16] Arjun Mukherjee, Bing Liu, and Natalie Glance. 2012. Spotting fake reviewer groups in consumer reviews. In *Proceedings of the 21st International Conference on World Wide Web*. ACM, 191–200.

[17] Arjun Mukherjee, Vivek Venkataraman, Bing Liu, and Natalie S. Glance. 2013. What yelp fake review filter might be doing? In *Proceedings of the International Conference on Web and Social Media (ICWSM'13)*. 409–418.

[18] Florian Probst, Laura Grosswiele, and Regina Pfleger. 2013. Who will lead and who will follow: Identifying influential users in online social networks. *Busin. Info. Syst. Engin.* 5, 3 (2013), 179–193.

[19] C. J. Van Rijsbergen. 1979. *Information Retrieval* (2nd ed.). Butterworth-Heinemann, Newton, MA.

[20] Geetika Sarna and M. P. S. Bhatia. 2017. Content based approach to find the credibility of user in social networks: An application of cyberbullying. *Int. J. Mach. Learn. Cybernet.* 8, 2 (2017), 677–689.

[21] David Savage, Xiuzhen Zhang, Xinghuo Yu, Pauline Chou, and Qingmai Wang. 2014. Anomaly detection in online social networks. *Social Netw.* 39 (2014), 62–70.

[22] Bernard W. Silverman. 1986. *Density Estimation for Statistics and Data Analysis*. Vol. 26. CRC Press.

[23] 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 *Proceedings of the IEEE 32nd International Conference on Distributed Computer Systems (ICDCS'12)*. IEEE, 305–314.

[24] S. L. Ting and Albert H. C. Tsang. 2014. Using social network analysis to combat counterfeiting. *Int. J. Prod. Res.* 52, 15 (2014), 4456–4468.
[25] Michael Trusov, Anand V. Bodapati, and Randolph E. Bucklin. 2010. Determining influential users in internet social networks. *J. Market. Res.* 47, 4 (2010), 643–658.
[26] Alex Hai Wang. 2010. Don't follow me: Spam detection in Twitter. In *Proceedings of the International Conference on on Security and Cryptography*. IEEE, 1–10.
[27] Jiang Wang, Yang Song, Thomas Leung, Chuck Rosenberg, Jingbin Wang, James Philbin, Bo Chen, and Ying Wu. 2014. Learning fine-grained image similarity with deep ranking. In *Proceedings of the IEEE Conference on Computer Visualization and Pattern Recognition*. 1386–1393.
[28] Sergey Zagoruyko and Nikos Komodakis. 2015. Learning to compare image patches via convolutional neural networks. In *Proceedings of the IEEE Conference on Computer Visualization and Pattern Recognition*. 4353–4361.
[29] Qunyan Zhang, Haixin Ma, Weining Qian, and Aoying Zhou. 2013. Duplicate detection for identifying social spam in microblogs. In *Proceedings of the IEEE International Congress on Big Data*. IEEE, 141–148.
[30] Xianghan Zheng, Zhipeng Zeng, Zheyi Chen, Yuanlong Yu, and Chunming Rong. 2015. Detecting spammers on social networks. *Neurocomputing* 159 (2015), 27–34.

Received September 2018; revised December 2018; accepted February 2019