Association for Information Systems
AIS Electronic Library (AISeL)

Proceedings of the XI Brazilian Symposium on Information Systems (SBSI 2015)

Brazilian Symposium on Information Systems (SBIS)

5-2015

Recognition of Compromised Accounts on Twitter

Rodrigo Augusto Igawa
Londrina State University, igawa.rodrigo@gmail.com

Alex Marino Gonçalves de Almeida
Londrina State University, alex.marino.almeida@gmail.com

Bruno Bogaz Zarpelão
Londrina State University, brunozarpelao@gmail.com

Sylvio Barbon Jr
Londrina State University, barbon@uel.br

Recognition of Compromised Accounts on Twitter

Rodrigo Augusto Igawa
Londrina State University
PR 445 Km 380
Londrina-PR, Brazil
igawa.rodrigo@gmail.com

Alex Marino Gonçalves de Almeida
Londrina State University
PR 445 Km 380
Londrina-PR, Brazil
alex.marino.almeida@gmail.com

Bruno Bogaz Zarpelão
Londrina State University
PR 445 Km 380
Londrina-PR, Brazil
brunozarpelao@gmail.com

Sylvio Barbon Jr
Londrina State University
PR 445 Km 380
Londrina-PR, Brazil
barbon@uel.br

ABSTRACT

In this work, we propose an approach for recognition of compromised Twitter accounts based on Authorship Verification. Our solution can detect accounts that became compromised by analysing their user writing styles. This way, when an account content does not match its user writing style, we affirm that the account has been compromised, similar to Authorship Verification. Our approach follows the profile-based paradigm and uses N-grams as its kernel. Then, a threshold is found to represent the boundary of an account writing style. Experiments were performed using a subsampled dataset from Twitter. Experimental results showed that the developed model is very suitable for compromised recognition of Online Social Networks accounts due to the capability of recognize user styles over 95% accuracy.

Categories and Subject Descriptors

I.2.7 [**Natural Language Processing**]: Text analysis; I.5.4 [**Applications**]: Text processing; K.4.2 [**Social Issues**]: Abuse and crime involving computers

General Terms

Measurement, Security, Verification

Keywords

Authoship Verification, Compromised Accounts, N-grams

1. INTRODUCTION

Online Social Networks (OSNs) are environments where people discuss and express thoughts and opinions about any subject [26]. Currently, OSNs represent a relevant resource of information and researches in areas such as Customer Relationship Management (CRM) and Opnion Mining (OM). Knowledge obtained from OSNs such as Twitter and Facebook has shown to be extremely valuable for marketing research companies, public opinion organisations, and other Text Mining purposes [1, 25, 28, 19]. Since millions of opinions on a certain topic are expressed with simplicity, posting provide rich, easy and unbiased content comprehension [9]. Therefore, the contents of OSNs are a valuable dataset for decision making on marketing research, business intelligence, stock market prediction and image monitoring [15, 10].

The OSNs wide popularity and ease of access have resulted in the misuse of their services. In addition to the privacy preserving issues, OSNs face the challenge of dealing with undesirable users and their malicious activities, spamming for product promotion being one of the most common [2]. To address the problem of malicious activity on social networks, researchers have focused the detection of fake accounts (i.e., automatically created accounts for only spreading malicious content). However, the problem persists once systems that solely detect fake accounts do not discriminate between fake and compromised accounts. A compromised account is a legitimate account which has been taken over by an attacker to publish fake and harmful content [1] [2]. Accounts can be compromised in many different ways, for example, by exploiting a cross-site scripting vulnerability or by using a phishing scam to steal the users credentials. Also, bots have been increasingly used to obtain credentials information for social networking sites on infected hosts [6, 8].

Since fake accounts were mainly created with proposal to cause harm in OSNs, once they are detected, the simplest solution is to delete them. In the meantime, compromised accounts need engaging in a credentials recovery process to give back the accounts control to their respective owners [6]. Moreover, a study performed through Twitter revealed that only 16% of the spamming accounts were indeed fake accounts, while the remaining quantity were all compromised accounts [8]. The same reality also was seen on Facebook where 97% of malicious accounts were not originally created to solely spamming porpose [7].

In this paper, we present a first of its kind study to recognize compromised accounts using just text as resource. Our approach is based on N-grams Authorship Verification (AV) and we focus on recognition of a user based on its writing

[1] http://www.bbc.com/news/world-us-canada-30853311
[2] http://www.bbc.com/news/world-us-canada-30785232

SBSI 2015, May 26th-29th, 2015, Goiânia, Goiás, Brazil

style. When the writing style of a given user does not match its boundary based on a threshold, then, a warning alarm could be sent out to inform the account owner and malicious posts could be blocked. Also, as seen in [13, 23, 15] Preprocessing can either contribute or disturb text mining tasks, therefore, we also conducted experiments concerning Preprocessing and Corpus size to study their relevance in results. Our experiments were performed using a Twitter dataset and results ranging from 94% to 95% accuracy were achieved.

The remaining of the work is organized as follows: Section 2 presents an overview towards compromised accounts and Authorship Verification along N-grams. In Section 3 details about the proposed aproach are described. Section 4 presents the experimental settings to perform our tests. Section 5 discusses our results. Section 6 states our conclusions.

2. RELATED WORK

Compromised accounts initially became the object of research interest in e-mail and web services as seen in [22, 12]. In a similar scenario to OSNs, users credentials are stolen using malicious link or phishing techniques [14, 22]. Concerning e-mails, researches already conducted work in user levels by using social engineering to emphasize user awareness [12], while another different approach combined network information, machine learning and content analysis in order to detect harmful content [22].

Some other approaches detected intrusion and compromised accounts in short messages by applying text mining techniques as Authorship Attribution (AA) and AV [5, 4]. Their main contribution was to aid the search for cyber criminals [27] or to increase cyber space security and reliability [5].

In order to achieve so, both AA and AV were based on one of two strategies: Stylometry and N-grams. The first one describes text content through attributes which represent writing-style markers as lexical, syntactic, content-specific, and idiosyncratic style markers. Lexical attributes are words and character based statistical measures like sentence length. Syntatic attributes include part-of-speech tagger measures. Content-specific attributes are represented by keywords of a given text and idiosyncratic markers are represented by misspellings and grammatical mistakes [11, 18].

N-grams, on the other hand, consist in obtaining frequent co-ocorrent patterns in words or character level. A set of most frequent N-grams represents the textual description of a given author, hoping that most frequent patterns would occur more often [13, 21].

Regarding the few existent works addressing compromised accounts on OSNs, studies already stated that malicious content are almost completely spread by compromised accounts that were victims of phishing attacks. The detection of malicious accounts is achieved by extracting features from text, webdata and network information to then, classify it based on machine learning approaches like Random Forest, SVM and Logistic Regression [7, 20].

3. PROPOSED APPROACH

The proposed approach is grounded on AV to analyse if an account has been compromised. In order to represent the legitimate user, it is necessary to extract features from textual content. These contents are calculated using N-grams, as seen in in Figure 1.

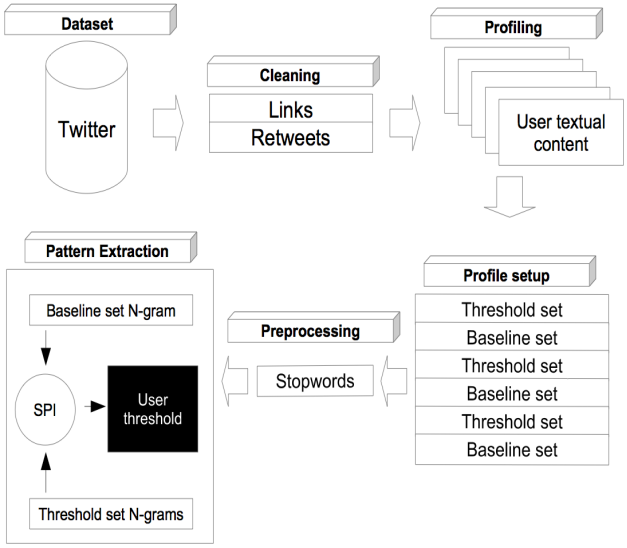

Figure 1: Proposed Approach for User Threshold Estimation

The main idea behind our proposal is to address compromised accounts problem as a document representation model. By doing so, it would be possible to apply Text Mining tasks to analyze the user writing style.

First step is dataset acquisition. Considering Text Mining approach only text features will be used and, therefore, none additional information beyond the tweets content and their respective authors username are required for our proposal.

Second step is about Cleaning. Normally, it would be possible to consider any textual content as a part of a document produced by an author. However, as this approach is created to be applied on Twitter users, links and *retweets* (thirdy part contents) were removed due to not represent any textual authorship mark.

All remaining text productions are considered authorship samples. Therefore, all contents are concatenated cumulatively following the profile-based paradigm described in [17]. The result of this step, called Profiling, is a document containing all terms writen by the user.

Then, in Profile Setup, each user is represented as a document whose content is subsampled at the same fraction in two distinct parts: Baseline set and Thresholding set. Each fraction of document subsampled has the same size and is interspersed as shown in Figure 1. This way, subjects discussed by the user during the time will be equally distributed in both sets. This is important to our approach because both sets must have subjects balanced so that the boundary of the writing style can be properly found.

The Baseline set is the text portion which represents user account. This set is used to extract the usual writing style of an user and is kept as one single document as described by the profile-based paradigm in [17]. The Thresholding set is a portion used to find a Simplified Profile Intersection (SPI) threshold to delimitate the user writing style and different from Baseline set, each portion subsampled becomes an distinct sample instance. The SPI similarity measure was used in [17, 13] and is stated to be suitable to diferent sample

sizes. The SPI is calculated as seen in Equation 1, where N_1 and N_2 are two distinct sets of N-grams. Note that SPI is basically a count of N-grams that exist in both sets.

$$SPI(N_1, N_2) = |N_1 \cap N_2| \quad (1)$$

After Profile Setup process, Preprocessing techniques can be performed to improve the effectiveness of our approach. In this work, we explore some combination of Preprocessing concerning precision and accuracy to recognize accounts textual content.

In order to obtain the SPI threshold in Writing Style Extracion step, most frequents N-grams are extracted from Baseline set and most frequents N-grams are also extracted from each fraction in Thresholding set. Then, SPI is used to calculate similarity between Baseline set and Thresholding set N-grams. The minimal similarity obtained is considered the SPI threshold. Any future portion of text posted in this account that presents similarity measure lesser than threshold is considered an intrusion and the account is compromised.

4. METHODOLOGY

Twitter, the OSN used in this work, is known as a micro blogging service. Unlike other social media, Twitter is known by short posts (140 characters at maximum) done by users expressing thoughts, opinions and feelings [26]. These short texts, named tweets, are available publicly as default, and are immediately broadcasted to the users followers [3].

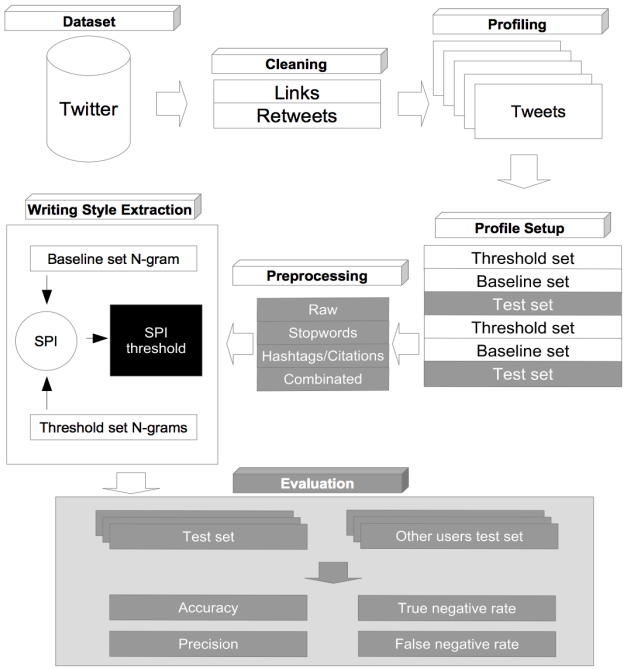

Figure 2: Experimental Settings Overview

The Twitter Developer Team offer a streaming service that delivers other developers low latency access to Twitter's global stream of data. The tweets sets used as samples in our experiments were collected by [24] using this service.

In our experiments, only a subsample from original Dataset was used. This was done in order to simulate the few samples available in a more critical scenario. From this part, all tweets were grouped by authors username cumulatively following profiling step described in Section 3. As specified in our approach, links and retweets were removed since they do not infer any information about its user writting pattern. All remaining textual content was included in our tests.

In Figure 2, gray parts represent the experimental settings. The Profile Setup process was performed to separate textual contents in 3 distincts parts: Baseline set, Thresholding set (as proposed in Section 3) and Test set. The last set is used to evaluate our method's efficiency and is a representation of future portions of text posted. The user's Test set is completelly used along randomly selected Test set instances from other users to check how adequate is the obtained threshold. Our intention to use other users test set among the own user test set is to simulate a situation where the legitimate account has been compromised and harmful posts are writen, therefore, it is desirable to obtain SPI measures in instances from other users test set lesser than threshold, while own user test set are intended to present SPI greater than threshold.

Another concerning towards the Profile setup is to study the size of each splited part. This is considered an important issue of this work once the size used presenting better results would be the amount of words necessary to recognize accounts textual contents. In our experiments, were used 11 difrent sizes ranging from 50 to 100 words.

Also, concerning Preprocessing, 4 tests concerning their influence were performed: a) Raw (i.e, no preprocessing), b) *Hashtags* and *Citations* removal, c) Stopwords removal and d) Combinated preprocessing (i.e, *Hashtags*, *Citations* and Stopwords removal). The idea behind these tests is to study the influence of disposable terms concerning precision and accuracy to recognize account textual content.

One last issue experienced in our tests was the N used on N-grams. Following results from [13] we used values to N equals to 4, 5 and 6. These setting were also applied including the Corpus size and preprocessing settings.

Therefore, the complete experimental setting consists in 132 experiments covering our 3 diferent N-grams values, 11 combination towards Corpus size the 4 combination dealing 2 preprocessing techniques.

In order to keep experiments always balanced to enable comparisons to each other, we defined that each Test set and Threshold set were composed by 10 instances of same size (ranging from 50 to 100 words). In the Evaluation step, the user being recognized always used its entire Test set (i.e, 10 instances of text) along 10 instances randomly selected from other users Test sets.

To evaluate our method eficiency, we used 4 well known statiscal measures found in [16] and their equations are shown in Table 1 where TP are user test set instances presenting SPI greater than threshold, TN are other users test set presenting SPI lesser than threshold, FN are user test instances presenting SPI lesser than threshold and FP are other users test intances presenting SPI greater than threshold. Analysis results and discussion towards all experiments are presented in Section 5.

5. RESULTS AND DISCUSSION

As described previously, 132 experiments were performed concerning all possible combinations within $N = 4, 5, 6$; Corpus size in each splited portion ranged from 50 to 100 words

Table 1: Measures used to evaluate recognition rate

Name	Equation
Precision	$\frac{TP}{TP+FP}$
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
False Negative Rate	$\frac{FN}{FN+TP}$
True Negative Rate	$\frac{TN}{TN+FP}$

Table 3: The influence of text Preprocessing techniques on compromised accounts recognition

Preprocessing	Mean	Standard Deviation
Raw	91.90%	7.21%
Hashtags/Citations Removal	86.10%	10.56%
Stopwords Removal	95.80%	8.78%
Combinated Preproc.	85.22%	12.15%

and 4 combinations of text preprocessing. Table 2a and 2b shows our highest and lowest results in accuracy terms independently of its setting. It is notable that the top settings achieved excelent results, ranging from 94.10% to 95.80% accuracy (i,e. correctly classified instances) and also presentend excelent results in terms of true negative rate ranging from 88.40% to 91.60% which indicates that our method is capable of infer when the content does not correspond to its legitimate user writting pattern.

Another important issue to be observed is the combinations of preprocessing in both Table 2a and Table 2b. All 10 top results achived their results without removing hashtags and citations. On the other hand, all 10 least accurate experiments applied hashtags and citations removal achieving poor results. Our first conclusion by overviewing the experiments is that hashtags and citations carry information about the writting style of an user textual content, once they indicate subjects discussed and people frequently contacted.

Still concerning the preprocessing issue, a detailed result from the top 1 experimental setting in Table 2a using Corpus size = 100 and $N = 6$ is shown in Table 3 in terms of accuracy. Just by removing hashtags and citations, a loss in accuracy is found, falling from 91.90% to 86.10% precision. By removing only stopwords it is still possible to increase 5.0% accuracy. This implies that pronouns, articles and prepositions used do not help to recognize an user writing style using our approach. One last observation about preprocessing is: a combination of hashtags/citations and stopwords removal achives the lowest results of the 4 combinations once it uses only a little part of writing not including stopwords, hashtags and citations.

A discusion towards the top 1 setting in Table 2a is ilustrated by Figure 3 and shows accuracy considering each user. The setting achieved 100% of correctly recognized in many cases, however, to account number 4, 15, 25 and 27 obtained accuracy bellow 80%. These users presented a very unstable writing style using a high quantity of prepositions and almost nothing of jargons and emoticons making their writting dificult to distinguish. In all other cases the setting obtained satisfactory results.

Corpus size influence on our approach is illustrated by Figure 4. Before any discussion about this view, it is necessary to observe that the Corpus size is not used only to split in Profile Setup process, but also implies in the number of words necessary to perform proposed approach with satisfactory results. Considering so, the fact that none setting size used in our experiments presented ourliers and also presented balanced quartiles, having a good result. It implies that our method have a stable range of accuracy independently of amount of text used. A descending gradient observed on accuracy using 100 to 50 words is justifiable once less words also means less n-grams to be extracted and possibly less accuracy. Therefore, the boxplot states that the most considerable size to be used in our dataset is 100 words while the most inapropriate is 50.

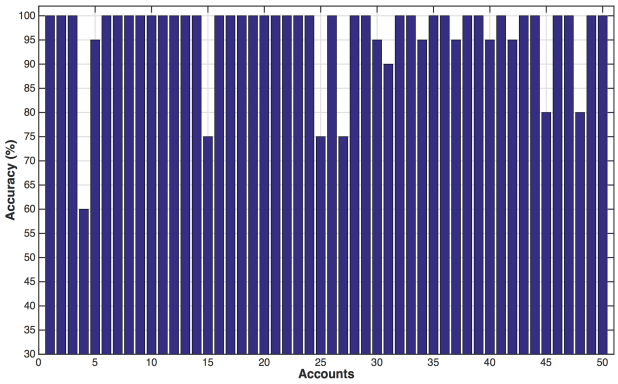

Figure 3: Individual accuracy on recognition of compromised accounts

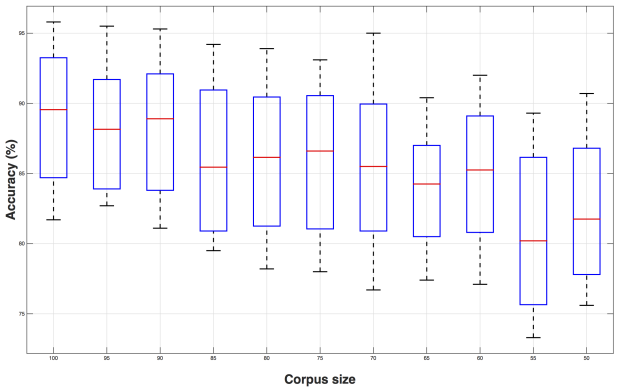

Figure 4: The influence of Corpus size on baseline accuracy

One last consideration towards our approach is threshold value and its relation to each user writing style. Most part of users obtained 100% accuracy as shown in Figure 3. These users are represented in Figure 5, as Case III, where the obtained threshold is suitable to separate writing styles from the legitimate user and other users. Case I and II represent users that by presenting too many stopwords as part of their writing styles and using a small quantity of emoticons, jargons, hashtags or citations obtained a threshold value unable to correctly separate writing styles and, therefore, obtained a signicant number of false negative (i.e, writing style from different users being recognized as the user in question).

6. CONCLUSION AND FUTURE WORK

Table 2: Overview on accounts recognition accuracy

(a) Top results in accuracy

N	C. Size	Precision	Accuracy	TNR	FNR	Hashtags/Citations	Stopwords
6	100	93.97%	95.80%	91.60%	0.00%	Not removed	Removed
5	100	93.43%	95.70%	91.40%	0.00%	Not removed	Removed
6	95	93.59%	95.50%	91.00%	0.00%	Not removed	Removed
6	90	93.64%	95.30%	90.80%	0.20%	Not removed	Removed
5	90	93.36%	95.10%	90.40%	0.02%	Not removed	Removed
6	70	92.72%	95.00%	90.20%	0.02%	Not removed	Removed
4	100	92.28%	94.60%	89.20%	0.00%	Not removed	Removed
5	70	92.45%	94.60%	89.40%	0.02%	Not removed	Removed
6	85	92.57%	94.20%	89.00%	0.06%	Not removed	Removed
5	95	91.39%	94.10%	88.40%	0.02%	Not removed	Removed

(b) Lowest results in accuracy

N	C. Size	Precision	Accuracy	TNR	FNR	Hashtags/Citations	Stopwords
6	55	72.31%	77.60%	55.40%	0.20%	Removed	Removed
6	65	73.75%	77.40%	61.20%	6.40%	Removed	Not removed
6	50	75.08%	77.20%	63.20%	8.80%	Removed	Not removed
4	60	75.47%	77.10%	64.40%	10.20%	Removed	Not removed
4	70	74.53%	76.70%	61.80%	8.40%	Removed	Not removed
4	55	71.73%	76.60%	53.80%	0.60%	Removed	Removed
5	50	74.03%	76.10%	60.60%	8.40%	Removed	Not removed
4	50	73.89%	75.60%	60.20%	9.00%	Removed	Not removed
4	55	71.30%	74.70%	55.80%	6.40%	Removed	Not removed
6	55	70.97%	73.80%	55.40%	7.80%	Removed	Not removed
5	55	70.62%	73.30%	55.00%	8.40%	Removed	Not removed

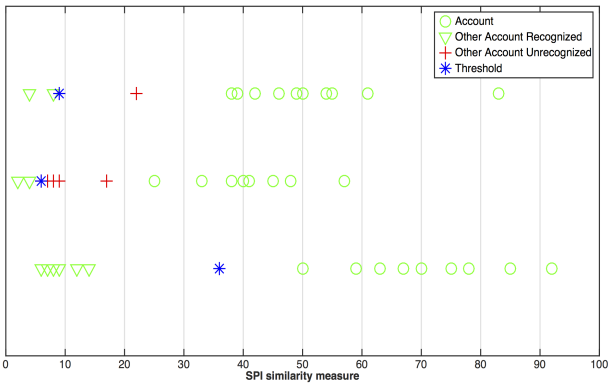

Figure 5: Threshold testing for compromised accounts recognition

One advantage from our approach is that only text is used as resource once it is grounded on Text Mining. Although it was tested on Twitter in our experiments, our developed method is applicable in any OSN. Also, due to the fact that this work is the first to depend only on text to recognize compromised accounts, our approach concerned about the Corpus size necessary to recognize compromised accounts, desirable preprocessing to obtain better results and which N use in N-grams calculation to improve the approach results.

In this work one important consideration during the entire process is that warning systems should not incorrectly recognize a legitimate user as an invasor to claim compromised account. Therefore, we studied and comproved that the top experimental setting presented in Table 2a (N=6, Corpus size = 100, Stopwords removal only) obtains very good results in terms not only of precision and accuracy, but also very few occurrences of false negative. That implies that our method would rarely claim compromised accounts by content when actually it was not compromised.

Considering Twitter's very short texts scenario, the need to use 100 words is also aceptable. The tweets used in experiments have a mean of 14.6 words. In practice, between 6-10 tweets, depending of how much per tweets is writen, is possible to recognize an user by its text, with 95% accuracy along 91% true negatives.

For future works it would be of great interest to study a method dealing only with those cases of low accuracy presentend in Figure 5 and Figure 3. This way, our methods accuracy could be increase. This study could be towards other N-grams measures focused on special cases of authors.

7. REFERENCES

[1] S.-A. Bahrainian and A. Dengel. Sentiment analysis and summarization of twitter data. In *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on*, pages 227–234. IEEE, 2013.

[2] S. Y. Bhat and M. Abulaish. Community-based features for identifying spammers in online social networks. In *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social*

Networks Analysis and Mining, pages 100–107. ACM, 2013.

[3] C. A. Bliss, I. M. Kloumann, K. D. Harris, C. M. Danforth, and P. S. Dodds. Twitter reciprocal reply networks exhibit assortativity with respect to happiness. *Journal of Computational Science*, 3(5):388–397, 2012.

[4] M. L. Brocardo, I. Traore, S. Saad, and I. Woungang. Authorship verification for short messages using stylometry. In *Computer, Information and Telecommunication Systems (CITS), 2013 International Conference on*, pages 1–6. IEEE, 2013.

[5] J. A. Donais, R. A. Frost, S. M. Peelar, and R. A. Roddy. Summary: A system for the automated author attribution of text and instant messages. In *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*, pages 1484–1485. IEEE, 2013.

[6] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. Compa: Detecting compromised accounts on social networks. In *NDSS*, 2013.

[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pages 35–47. ACM, 2010.

[8] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @ spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 27–37. ACM, 2010.

[9] A. Hassan, A. Abbasi, and D. Zeng. Twitter sentiment analysis: A bootstrap ensemble framework. In *Social Computing (SocialCom), 2013 International Conference on*, pages 357–364. IEEE, 2013.

[10] L.-C. Hsieh, C.-W. Lee, T.-H. Chiu, and W. Hsu. Live semantic sport highlight detection based on analyzing tweets of twitter. In *Multimedia and Expo (ICME), 2012 IEEE International Conference on*, pages 949–954. IEEE, 2012.

[11] S. Keretna, A. Hossny, and D. Creighton. Recognising user identity in twitter social networks via text mining. In *Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on*, pages 3079–3082. IEEE, 2013.

[12] S. Khanna and H. Chaudhry. Anatomy of compromising email accounts. In *Information and Automation (ICIA), 2012 International Conference on*, pages 640–645, June 2012.

[13] R. Layton, P. Watters, and R. Dazeley. Authorship attribution for twitter in 140 characters or less. In *Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second*, pages 1–8. IEEE, 2010.

[14] C.-H. Li, F.-H. Hsu, S.-J. Chen, C.-S. Wang, Y.-H. Chen, and Y.-L. Hwang. Hawkeye: Finding spamming accounts. In *Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific*, pages 1–4. IEEE, 2014.

[15] M. M. Mostafa. More than words: Social networks' text mining for consumer brand sentiments. *Expert Systems with Applications*, 40(10):4241–4251, 2013.

[16] D. L. Olson and D. Delen. *Advanced data mining techniques*. Springer Science & Business Media, 2008.

[17] N. Potha and E. Stamatatos. A profile-based method for authorship verification. In *Artificial Intelligence: Methods and Applications*, pages 313–326. Springer, 2014.

[18] R. Ramezani, N. Sheydaei, and M. Kahani. Evaluating the effects of textual features on authorship attribution accuracy. In *Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on*, pages 108–113. IEEE, 2013.

[19] J. Smailović, M. Grčar, N. Lavrač, and M. Žnidaršič. Stream-based active learning for sentiment analysis in the financial domain. *Information Sciences*, 2014.

[20] T. Stein, E. Chen, and K. Mangla. Facebook immune system. In *Proceedings of the 4th Workshop on Social Network Systems*, page 8. ACM, 2011.

[21] J. Sun, Z. Yang, P. Wang, and S. Liu. Variable length character n-gram approach for online writeprint identification. In *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, pages 486–490. IEEE, 2010.

[22] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song. Design and evaluation of a real-time url spam filtering service. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 447–462. IEEE, 2011.

[23] A. K. Uysal and S. Gunal. The impact of preprocessing on text classification. *Information Processing & Management*, 50(1):104–112, 2014.

[24] J. Yang and J. Leskovec. Patterns of temporal variation in online media. In *Proceedings of the fourth ACM international conference on Web search and data mining*, pages 177–186. ACM, 2011.

[25] S. J. Yu. The dynamic competitive recommendation algorithm in social network services. *Information Sciences*, 187:1–14, 2012.

[26] M. Zappavigna. Ambient affiliation: A linguistic perspective on twitter. *New Media & Society*, 13(5):788–806, 2011.

[27] C. Zhang, X. Wu, Z. Niu, and W. Ding. Authorship identification from unstructured texts. *Knowledge-Based Systems*, 2014.

[28] X. Zhou, S. Wu, C. Chen, G. Chen, and S. Ying. Real-time recommendation for microblogs. *Information Sciences*, 279:301–325, 2014.