Procesamiento del Lenguaje Natural, Revista nº 57, septiembre de 2016, págs. 125-132 recibido 30-03-2016 revisado 21-04-2016 aceptado 03-02-2016

Using Personality Recognition Techniques to Improve Bayesian Spam Filtering

Uso de Técnicas de Reconocimiento de la Personalidad para Mejorar el Filtrado Bayesiano de Spam

Enaitz Ezpeleta, Urko Zurutuza
Mondragon University
Goiru Kalea, 2
20500 Arrasate-Mondragón, Spain
{eezpeleta, uzurutuza}@mondragon.edu

José María Gómez Hidalgo
Pragsis Technologies
Manuel Tovar, 43-53, Fuencarral
28034 Madrid, Spain
jmgomez@pragsis.com

Resumen: Millones the usuarios se ven afectados por las campañas de envío de correos eléctrinicos no deseados al día. Durante los últimos años diferentes técnicas de detección de spam han sido desarrollados por investigadores, obteniendo especialmente buenos resultados con algoritmos de aprendizaje automático. En este trabajo presentamos una base para un nuevo metodo de filtrado de spam. Durante el estudio hemos validado la hipótesis de que las técnicas de reconocimiento de personalidad pueden ayudar a mejorar el filtrado Bayesiano de spam. Usando estas técnicas de filtrado, añadimos la característica de personalidad a cada correo, y después comparamos los resultados del filtrado Bayesiano de spam con y sin personalidad, analizando los resultados en terminos de exactitud. En un segundo experimento, combinamos las características de personalidad y polaridad de cada mensaje, y comparamos los resultados. Al final, conseguimos mejorar los resultados del filtrado Bayesiano de spam, alcanzando el 99,24% de exactitud, y reduciendo el número de falsos positivos.
Palabras clave: spam, personalidad, polaridad, PLN, seguridad

Abstract: Millions of users per day are affected by unsolicited email campaigns. During the last years several techniques to detect spam have been developed, achieving specially good results using machine learning algorithms. In this work we provide a baseline for a new spam filtering method. Carrying out this research we validate our hypothesis that personality recognition techniques can help in Bayesian spam filtering. We add the personality feature to each email using personality recognition techniques, and then we compare Bayesian spam filters with and without personality in terms of accuracy. In a second experiment we combine personality and polarity features of each message and we compare all the results. At the end, the top ten Bayesian filtering classifiers have been improved, reaching to a 99.24% of accuracy, reducing also the false positive number.
Keywords: spam, personality, polarity, NLP, security

1 *Introduction*

Millions of users per day are affected by unsolicited email campaigns. Spam filters are capable of detecting and avoiding an increasing number of emails, but according to Kaspersky Lab data, the average of spam in email traffic stood at 55.28% in 2015[1]. This mass mailing of unsolicited emails are used both for the sale of products such as online fraud, and it reports billionaire benefits. Thanks to spam campaigns a market share sufficient to enrich a sector devoted to fraudulent activity in achieved. These facts make those types of activities one of the biggest threats to Internet security.

To deal with this problem different spam detection systems have been designed and developed by researchers during the last years, spending on cyber-security technologies over \$83.6 billions in 2015[2] for example.

This paper provides a baseline for a new

[1]https://securelist.com/analysis/kaspersky-security-bulletin/73591/kaspersky-security-bulletin-spam-and-phishing-in-2015/

[2]http://www.bloomberg.com/news/articles/2016-01-19/e-mail-spam-goes-artisanal

ISSN 1135-5948

spam filtering method. The objective is to demonstrate that personality recognition of email messages can help in Bayesian spam filtering. In this paper we hypothesize that being spam an email that generally aims at selling services or products, analyzing its meaning, and specially the personality of the spam, can bring similar personality functions such that classification systems are improved.

We take into account the results published by (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) related to Bayesian spam filtering, and we aims to improve them. First of all, applying personality recognition techniques to a dataset we create a new tagged (personality) dataset. Then, we apply the best ten classifiers of the mentioned study to the new dataset and we analyze the obtained results. In the second experiment we combine the best sentiment classifiers used by (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) with personality and a new combined dataset is created. One more time, we apply the best classifier to the new dataset and we compare all the results in order to give our conclusions.

The remainder of this paper is organized as follows. Section 2 describes the previous work conducted in the area of spam filtering, personality recognition, natural language processing and sentiment analysis. Section 3 describes the process of the aforementioned experiments, regarding emails personality recognition and spam filtering using personality feature. In Section 4, the obtained results are presented, showing the results of the different experiments carried out during the study. Finally, we summarize our findings and give conclusions in Section 5.

2 Related Work

2.1 Spam filtering techniques

Different techniques to detect spam have been developed during the last years (Nazirova, 2011). Among all proposed automatic classifying techniques, machine learning algorithms have achieved more success (Cormack, 2007). In (Tretyakov, 2004) the authors obtained precisions up to 94.4% using those type of techniques.

In this study we focus on a specific section of machine learning algorithms; content-based filters. Those filters are based on analyzing the content of the emails in order to split messages in spam or legitimate emails as it is explained in (Sanz, Hidalgo, and Cortizo, 2008). Content-based spam filters can be separated in several types such as heuristic filtering, learning-based filtering and filtering by compression.

A comparison between various existing spam detection methods is presented in (Savita Teli, 2014): rule-based system, IP blacklist, Heuristic-based filters, Bayesian network-based filters, white list and DNS black holes. As a conclusion they define Bayesian based filters as the most effective, accurate, and reliable spam detection method.

Some of the content-based filtering techniques are also studied and analyzed in (Malarvizhi and Saraswathi, 2013), and again, the Bayesian method is selected as the most effective one (classifying correctly the 96.5% of messages). Furthermore, in (Eberhardt, 2015) authors demonstrated that although more sophisticated methods have been implemented, Bayesian methods of text classification are still useful.

2.2 Personality recognition techniques

As authors defined in (Vinciarelli and Mohammadi, 2014) personality is a psychological construct aimed at explaining the wide variety of human behaviours in terms of a few, stable and measurable individual characteristics. As an effort to formalize it, two main models has been defined (Celli and Poesio, 2014): in the first one, called Myers-Briggs personality model (Briggs Myers and Myers, 1980), four dimensions are used to define the personality: Extroversion/Introversion, Thinking/Felling, Judging/Perceiving and Sensing/iNtuition; Meanwhile, in the Big Five 5 (Costa and McCrae, 1992) traits are used to define the personality: Openness to experience, Conscientiousness, Extroversion, Agreeableness and Neuroticism.

Personality recognition became a potential tool for Natural Language Processing as it is possible to extract a lot of information about the personality of the authors from every text (Mairesse et al., 2007). Several research in the last years has been published related to personality recognition in blogs (Oberlander and Nowson, 2006), offline texts (Mairesse et al., 2007) or online social networks (Bai, Zhu, and Cheng, 2012; Rangel et al., 2015).

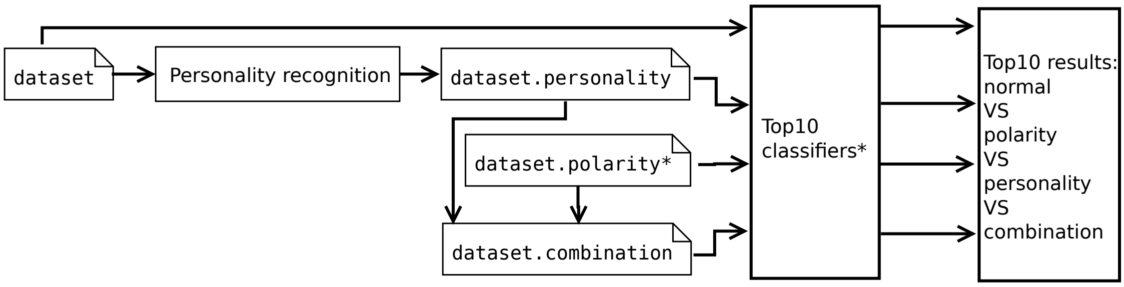

Figure 1: Full process of the study

Email authors personality prediction is possible as it is shown in (Shen, Brdiczka, and Liu, 2013). Authors prove that personality prediction is feasible, and their email feature set can predict personality with reasonable accuracies. This last research is taken into account by the authors as a baseline in spam filtering.

2.3 Sentiment analysis

A brief definition of Natural Language Processing (NLP) is given in (Liddy, 2001), as a theoretical motivated range of computational techniques for analyzing and representing naturally occurring texts at one or more levels of linguistic analysis. It aims to achieve human-like language processing for a range of task or applications. Those techniques are becoming more and more useful for spam filtering, as it is demonstrated in (Giyanani and Desai, 2013) using sender information and text content based NLP techniques.

Researchers in (Echeverria Briones et al., 2009) and (Lau et al., 2012) confirmed that it is possible to create an application or a system to detect spam in different formats using text mining techniques and semantic language model respectively.

During the last years Sentiment Analysis (SA) has been used in several research areas, although there has been a continued interest for a while. In (Liu and Zhang, 2012) the most important research opportunities related to SA are described. Based on that, in (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) authors selected document sentiment classification topic as a possible option to improve spam filtering. They tagged a dataset with polarity (positive, neutral or negative) score of each message using sentiment classifiers, and then authors compare spam filtering classifiers with and without the polarity score in terms of accuracy. As the results were positive, authors aim at improving these results adding more semantic features to the text.

3 *Design and Implementation*

This research has been carried out following the procedure of the figure 1, which is divided in two main experiments.

Taking as a baseline the top ten classifiers identified in (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a), on the one hand, we analyze the influence of the personality in spam filtering comparing the results of the ten classifiers applied to the dataset with and without personality. And on the other hand, we combine personality feature with polarity feature (in the dataset) in order to analyze if it improves Bayesian spam filtering results.

Those experiments are carried out using the 10-fold cross-validation technique and the results are analyzed in terms of false positive rate and accuracy, being the accuracy the percentage of testing set examples correctly classified by the classifier.

$$Accuracy = \frac{(True\ Positives\ +\ True\ Negatives)}{(Positives\ +\ Negatives)}$$

3.1 Dataset

To carry out this study, we use a publicly available dataset called *CSDMC 2010 Spam Corpus*[3]. This dataset is composed by 2,949 legitimate email messages and 1,378 spam messages.

3.2 Bayesian spam filtering

To analyze if personality recognition techniques improve Bayesian spam filtering. First of all we generate Bayesian spam filters as a baseline for the rest of the experiment.

As in (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) the best ten classifiers for spam

[3]http://www.csmining.org/index.php/spam-email-datasets-.html

#	Name	Normal FP	FN	Acc
1	BLR.i.t.c.stwv.go.wtok	13	24	99.15
2	DMNB.c.stwv.go.wtok	21	17	99.12
3	DMNB.i.c.stwv.go.wtok	21	17	99.12
4	DMNB.i.t.c.stwv.go.wtok	21	17	99.12
5	DMNB.stwv.go.wtok	21	17	99.12
6	DMNB.c.stwv.go.stemmer	22	19	99.05
7	DMNB.i.c.stwv.go.stemmer	22	19	99.05
8	DMNB.i.t.c.stwv.go.stemmer	22	19	99.05
9	DMNB.stwv.go.stemmer	22	19	99.05
10	BLR.i.t.c.stwv.go.ngtok.stemmer.igain	14	28	99.03

Table 1: Baseline results

filtering are defined. In table 1, the best results presented in the mentioned study are shown.

During this paper, our main objective is to improve those results using the selected classifiers. To understand the settings of each classifier, table 2 shows the nomenclatures used.

	Meaning
DMNB	DMNBtext
BLR	Bayesian Logistic Regression
.c	idft F, tft F, outwc T
.i.c	idft T, tft F, outwc T
.i.t.c	idft T, tft T, outwc T
.stwv	String to Word Vector
.go	General options
.wtok	Word Tokenizer
.ngtok	NGram Tokenizer 1-3
.stemmer	Stemmer
.igain	Attribute selection using InfoGainAttributeEval

Table 2: Nomenclatures

3.3 Personality recognition

The objective of the next phase is to apply personality recognition technique to each email in order to add this feature to the original dataset and create a new dataset. To do that, we followed the personality recognition process presented in (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016b).

One of the most trusted personality recognition assessment is used in this study: Myers-Briggs personality model. To determine the personality of each emails, it is mandatory to use the four different dimensions of this model: Extroversion/Introversion, Thinking/Feeling, Judging/Perceiving and Sensing/iNtuition. In this case, publicly available machine learning web services for text classification, hosted in *uClassify*[4], are used to calculate each feature. Among all the possibilities offered in this website, we focus on the Myers-Briggs functions developed by Mattias Östmar.

As author explains, each function determines a certain dimension of the personality type according to Myers-Briggs personality model. The analysis is based on the writing style and should not be confused with the Myers-Briggs Type Indicator (MBTI) which determines personality type based on self-assessment questionnaires. Training texts are manually selected based on personality and writing style according to (Jensen and DiTiberio, 1989).

Those are the used functions:

- *Myers-Briggs Attitude:* Analyzes the Extroversion/Introversion dimension.
- *Myers-Briggs Judging Function:* Determines the Thinking/Feeling dimension.
- *Myers-Briggs Lifestyle:* Determines the Judging/Perceiving dimension.
- *Myers-Briggs Perceiving Function:* Determines the Sensing/iNtuition dimension.

Each function returns a float within the range [0.0, 1.0] per each pair of characteristics of the dimension. For example, if we test a certain text and we obtain X value for Sensing, the value for iNtuition is 1-X. Thus, we only record one value per each function: Extroversion, Sensing, Thinking and Judging.

In order to create a new dataset, those four values of each email message are added

[4]https://www.uclassify.com

	Total	Extroversion	Sensing	Thinking	Judging
ham	2949	975	2439	313	1908
spam	1378	591	918	301	915
Percentage(%)					
ham	100	33	83	11	65
spam	100	43	67	22	66

Table 3: Descriptive analysis of the dataset.

to the original dataset. This new dataset is used during the tests to evaluate the influence of the personality in spam filtering. To do that, we apply the top ten classifiers mentioned previously to the original dataset and to the new one, and we compare the results.

3.4 Combination

Once we analyzed the results of the first experiment, in the second part our objective is to explore the possibilities to improve the results published by (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) where authors used polarity feature in Bayesian spam filtering.

We decided to combine both personality and polarity. First, we use the best sentiment classifier defined in the mentioned work and we analyze each email to create a dataset tagged with the polarity of each email. Once we created this dataset, we apply the top ten classifiers in order to obtain the results using the polarity feature. Finally, we create a new dataset adding the personality and the polarity of each email, and we apply the classifiers to compare all the results.

4 Experimental Results

In this Section the results obtained during the previously explained study are shown. To carry out the following experiments the dataset called *CSDMC 2010 Spam Corpus* is used.

4.1 Descriptive analysis

Once the dataset is selected, we perform a descriptive experiment of the dataset. The objective of this step is to analyze the personality features of the authors (spammers and legitimate email writers) applying the previously explained (Section 3.3) personality recognition functions. During this step the personality features are added to the original dataset creating a new tagged dataset, and we extract statistic about the personality. This information is shown in table 3.

Analyzing the data presented in the descriptive table, it is possible to see that there are differences between the emails types. The biggest difference according to Myers-Briggs personality model between spam emails and legitimate emails is given by the Perceiving Function. Taking into account only this dimension, the percentage of *sensing* legitimate emails is 16 point higher than spam emails.

In the next steps different experiments are carried out to see the real influence of personality feature in Bayesian spam filtering.

4.2 Using personality

As we explain in the previous Section, to see if personality improves Bayesian spam filtering, we apply the top ten classifiers to the labelled (personality) dataset, and we compare the results with the results obtained applying the same classifiers to the original dataset.

The results obtained during this experiments are presented in table 4.

	Normal			Personality		
#	**FP**	**FN**	**Acc**	**FP**	**FN**	**Acc**
1	13	24	99.15	14	26	99.08
2	21	17	99.12	22	16	99.12
3	21	17	99.12	22	16	99.12
4	21	17	99.12	22	16	99.12
5	21	17	99.12	22	16	99.12
6	22	19	99.05	22	21	99.01
7	22	19	99.05	22	21	99.01
8	22	19	99.05	22	21	99.01
9	22	19	99.05	22	21	99.01
10	14	28	99.03	13	26	99.10

Table 4: Comparison between normal and personality

Results show that only in one case the previous result is improved (from 99.03% to 99.10%), while in other four cases we obtain the same results (99.12%) and in the other five the results are worst than applying the classifiers to the original dataset.

So, adding the four personality dimensions to the dataset it is not helpful. But if we take into account the information obtained in the descriptive part, we can see that the

	Normal		Polarity		Sensing		Combination	
#	**FP**	**Acc**	**FP**	**Acc**	**FP**	**Acc**	**FP**	**Acc**
1	13	99.15	14	99.12	15	99.03	15	99.03
2	21	99.12	22	99.21	21	99.12	**19**	**99.24**
3	21	99.12	22	99.21	21	99.12	**19**	**99.24**
4	21	99.12	22	99.21	21	99.12	**19**	**99.24**
5	21	99.12	22	99.21	21	99.12	**19**	**99.24**
6	22	99.05	22	99.15	22	99.08	23	99.05
7	22	99.05	22	99.15	22	99.08	23	99.05
8	22	99.05	22	99.15	22	99.08	23	99.05
9	22	99.05	22	99.15	22	99.08	23	99.05
10	14	99.03	14	99.03	14	99.08	14	99.10

Table 5: Comparison between all techniques

differentiator dimension is Sensing/iNtuition.

4.2.1 Myers-Briggs Perceiving Function

To see if the mentioned dimension affects in the Bayesian spam filtering, a new dataset is created. We use only the Myers-Briggs Perceiving Function in order to add the *sensing* characteristic of each message to the dataset.

The followed procedure is the same than in the previous experiment: we apply the best ten classifiers to the new dataset and we compare the results with the original ones.

Table 6 summarized the new results.

	Normal			Sensing		
#	**FP**	**FN**	**Acc**	**FP**	**FN**	**Acc**
1	13	24	99.15	15	27	99.03
2	21	17	99.12	21	17	99.12
3	21	17	99.12	21	17	99.12
4	21	17	99.12	21	17	99.12
5	21	17	99.12	21	17	99.12
6	22	19	99.05	22	18	99.08
7	22	19	99.05	22	18	99.08
8	22	19	99.05	22	18	99.08
9	22	19	99.05	22	18	99.08
10	14	28	99.03	14	26	99.08

Table 6: Results using *sensing*

In this case we obtain better results in terms of accuracy than using all the dimensions of the Myers-Briggs personality model. The results are improved in five cases, in four of them the same results are obtained, and only in one case the result is worst.

Those results give a baseline to see the possibilities that personality recognition techniques can improve Bayesian spam filtering. But to confirm that the *sensing* characteristic can be helpful, we carry out one more experiment combining personality feature (sensing) with the polarity of each email.

4.3 Combinational experiment

During this experiment we apply the best ten Bayesian classifiers to the following datasets:

- Original dataset.
- Original dataset with the polarity information of each email. The best sentiment classifier identified in (Ezpeleta, Zurutuza, and Gómez Hidalgo, 2016a) is used to calculate the polarity score of each email.
- Original dataset with the *sensing* feature (as in the previous experiment).
- Original dataset with the polarity and the *sensing* feature of each email (combining the two previous dataset).

We compare the obtained results in terms of accuracy and false positive number, as it is possible to see in table 5.

According to the obtained results, we can say that combining sentiment analysis techniques with personality recognition techniques the best result obtained in Bayesian spam filtering is improved in terms of accuracy. The combination improves (99.24% of accuracy) both the top result of the original dataset (99.15%) and the top result of the polarity analysis (99.21%). Moreover, in those cases where the best result is achieved, the combination of sentiment analysis and personality techniques reduces the false positive number.

5 Conclusions

In this work, we give the initial ground for improving spam filtering techniques.

Results show that with the combination of personality recognition techniques (*sensing*) and sentiment analysis techniques allows it is possible to obtain better results than using those techniques separately. This combination obtains the best results within all different experiments reaching to a 99.24% of accuracy, reducing the false positive number from 21 to 19.

Despite the difference in percentage does not seem to be relevant, from 99.15% to 99.24%, if we take into account the amount of real spam traffic, the improvement is significant.

In addition, we conclude that it is possible to improve spam filtering classifiers adding the *sensing* feature to each email message, as in our experiments 5 results out of the best 10 classifiers are improved and in other 4 cases the same result is obtained. Although using the four dimensions of Myers-Briggs personality model the results are not not significant, using a specific characteristic we demonstrate that those techniques are helpful in spam filtering.

Furthermore, this work presents a new filtering method (combining polarity and personality) that gives to the research community the opportunity of detecting non evident intent in spam emails.

Moreover, taking into account that the personality recognition functions used are independent from the text, the use of manually tagged (personality) emails during the learning process of the function might improve the results.

Finally, taking this work as a reference, several directions can be explored: for example, in order to validate those results a repetition of the experiments using a different dataset; more algorithms and filters settings can be used to obtain more results; analyze different types of spam in order to see if the behaviour of the spammers is the same (SMS spam, blog spam,...).

Acknowledgments. This work has been partially funded by the Basque Department of Education, Language policy and Culture under the project SocialSPAM (PI_2014_1_102).

We thank Mattias Östmar for the valuable tools developed and published. And we thank Jon Kågström (Founder of uClassify[5]) for the opportunity to use their API for research purposes.

[5]https://www.uclassify.com

References

Bai, S., T. Zhu, and L. Cheng. 2012. Big-five personality prediction based on user behaviors at social network sites. *CoRR*, abs/1204.4809.

Briggs Myers, I. and P. B. Myers. 1980. Gifts differing: Understanding personality type.

Celli, F. and M. Poesio. 2014. Pr2: A language independent unsupervised tool for personality recognition from text. *arXiv preprint arXiv:1402.2796*.

Cormack, G. V. 2007. Email spam filtering: A systematic review. *Foundations and Trends in Information Retrieval*, 1(4):335–455.

Costa, P. T. and R. R. McCrae. 1992. Normal personality assessment in clinical practice: The neo personality inventory. *Psychological assessment*, 4(1):5.

Eberhardt, J. J. 2015. Bayesian spam detection. *Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal*.

Echeverria Briones, P. F., Z. V. Altamirano Valarezo, A. B. Pinto Astudillo, and J. D. C. Sanchez Guerrero. 2009. Text mining aplicado a la clasificación y distribución automática de correo electrónico y detección de correo spam.

Ezpeleta, E., U. Zurutuza, and J. M. Gómez Hidalgo. 2016a. Does sentiment analysis help in bayesian spam filtering? In *Hybrid Artificial Intelligent Systems: 11th International Conference, HAIS 2016, Sevilla, Spain, April 18-20, 2016*. Springer.

Ezpeleta, E., U. Zurutuza, and J. M. Gómez Hidalgo. 2016b. Short messages spam filtering using personality recognition. In *Proceedings of the 4th Spanish Conference in Information Retrieval*.

Giyanani, R. and M. Desai. 2013. Spam detection using natural language processing. *International Journal of Computer Science Research & Technilogy*, 1:55–58, August.

Jensen, G. H. and J. K. DiTiberio. 1989. *Personality and the Teaching of Composition*, volume 20. Ablex Pub.

Lau, R. Y. K., S. Y. Liao, R. C.-W. Kwok, K. Xu, Y. Xia, and Y. Li. 2012. Text mining and probabilistic language modeling for online review spam detection. *ACM Trans. Manage. Inf. Syst.*, 2(4):25:1–25:30, January.

Liddy, E. 2001. Natural language processing. *Encyclopedia of Library and Information Science, 2nd Ed.*, NY. Marcel Decker, Inc.

Liu, B. and L. Zhang. 2012. A survey of opinion mining and sentiment analysis. *Mining Text Data*, pages 415–463.

Mairesse, F., M. A. Walker, M. R. Mehl, and R. K. Moore. 2007. Using linguistic cues for the automatic recognition of personality in conversation and text. *J. Artif. Int. Res.*, 30(1):457–500, November.

Malarvizhi, R. and K. Saraswathi. 2013. Content-based spam filtering and detection algorithms-an efficient analysis & comparison 1. *International Journal of Engineering Trends and Technology*, Vol. 4, Issue 9, September.

Nazirova, S. 2011. Survey on spam filtering techniques. *Communications and Network*, 3(3):153–160.

Oberlander, J. and S. Nowson. 2006. Whose thumb is it anyway?: Classifying author personality from weblog text. In *Proceedings of the COLING/ACL on Main Conference Poster Sessions*, COLING-ACL '06, pages 627–634, Stroudsburg, PA, USA. Association for Computational Linguistics.

Rangel, F., F. Celli, P. Rosso, M. Potthast, B. Stein, and W. Daelemans. 2015. Overview of the 3rd Author Profiling Task at PAN 2015. In *Working Notes Papers of the CLEF 2015 Evaluation Labs*, CEUR Workshop Proceedings. CLEF and CEUR-WS.org, September.

Sanz, E. P., J. M. G. Hidalgo, and J. C. Cortizo. 2008. Email spam filtering. *Advances in Computers*, pages 45–114.

Savita Teli, S. B. 2014. Effective spam detection method for email. *IOSR Journal of Computer Science*, pages 68–72.

Shen, J., O. Brdiczka, and J. Liu. 2013. Understanding email writers: Personality prediction from email messages. In *User Modeling, Adaptation, and Personalization*. Springer, pages 318–330.

Tretyakov, K. 2004. Machine learning techniques in spam filtering. In *Data Mining Problem-oriented Seminar, MTAT*, volume 3, pages 60–79.

Vinciarelli, A. and G. Mohammadi. 2014. A survey of personality computing. *Affective Computing, IEEE Transactions on*, 5(3):273–291.