Publishing House
AKAPIT

COMPUTER METHODS IN MATERIALS SCIENCE
Informatyka w Technologii Materiałów

Vol. 14, 2014, No. 3

DETECTION OF VIRTUAL MULTI-IDENTITIES

ANDRZEJ OPALIŃSKI

AGH University of Science and Technology, Kraków, Poland
Corresponding author: andrzej.opalinski@agh.edu.pl

Abstract

Last decade is a time of rapid evolution of the Internet. Various human's life areas are migrating into the cyberspace, where people exist and act through virtual identities - personalization of themselves. Groups of virtual identities with their relations and context form cybersocieties. Due to the unique cyberspace's structure, virtual identities are characterized by relatively high anonymity level. This cause the phenomena of the virtual multi-identities, where a single physical person incarnates a few virtual identities. This entails both positive and negative effects, and presented article concerns a negative one, which is deceptive opinion spam, generated by multi-identities of a single person. This problem constantly increases as relaying on the opinions from the WEB becomes very common. This article presents the concept which combines elements from various domains, linked in order to solve this problem and detect virtual multi-identities hiding in social networks such as web forums, blogs or recommendation portals. The paper describes a general concept and the architecture of the implemented system. At the end, the evaluation of the solution is carried out, based on the examples from the recommendation portal and web forum.

Key words: virtual-identities, cybersociety, opinion spam

1. INTRODUCTION

During the last decade, a phenomena of rapid WEB network development encounter is widely encountered. It is caused partially due to the evolution of the Internet into the WEB2.0 model, where any user can create and publish his own content using social networks, homepages, blogs, web forums or content share portals. On the basis of this phenomena there is a fact of spreading Internet access services and its cost reductions. It is estimated, that at the end of 2012 the access to the Internet was provided to 2,4 billion of people, whereas in the Europe this ratio was about 63% and in the North America almost 78%. Comparing to the begin of the century, the ratio increased for more than 500% (ITU, 2012; MMG, 2012).

Along with the popularization and increasing access of the Internet, it appears also, that various human's life areas are migrating into the cyberspace. Banking, trades, communication, entertainment, social relations are subsequent aspects of human life, that are reflected in the virtual reality. Within the cyberspace people are represented by their virtual identities, which combine with their context and relations and forms cybersociety (Musiał & Kazieńko, 2012). Due to the unique structure of the cyberspace and the cybersociety, mapping of human's characteristics and its relations from real life is not accurate. One of the main attributes of the virtual society is high anonymity of virtual identities and relatively low possibility of verification of authenticity of features describing virtual identities (van Koksvijk, 2010). This situation results with both positive and negative effects. As a positive, there can be mentioned ex. to facilitate personal relations for people with low self-esteem or to allow experimenting with socially non-accepted behaviors (Christopherson, 2007). It also promote the freedom of speech, which is crucial in regions with radical religious or totalitarian political systems. However, simultaneously with positive effects come negative sides of high anonymity of WEB's virtual identities. Some of them are inter alia: broad meaning, sexual deviations like pedophilia, racial or religious hatred, black PR (compromising photos) or cybercrime such as: trafficking in illicit goods or coordination of criminal or terrorist groups. (Thomas & Loader, 2000). One of the negative effects of high anonymity of virtual identities in the WEB is deceptive opinion spam spreading. It happens when a single person uses a number of virtual identities to create many similar opinions about some products, brands, services or companies. Those opinions are usually highly emotional, in order to create an impression that they could reflect people's real choices and remarks about those objects. People, who generate these opinions are usually employed by crowdsourcing portals, which offers such services (Chen et al., 2011; Jindal & Liu, 2007). Importance of this issue rises, along with increasing number of people relaying on Internet opinions, found on recommendation portals or web forums.

This phenomena concerns also industrial part of WEB resources. There are number of industrial knowledge and information exchange portals, which connect groups of domain specialists, for their experience exchange purposes. While it is very useful source of information for many people, it also can be a target of opinion frauds about industrial products, brands and services. Resolving that problem would be very desirable, and will increase value of information acquired from such sources, as engineering forums or industrial portals.

The paper presents the solution, that could be utilized to counteract the deceptive opinion spam, by detecting users which are hiding in the WEB under multiple virtual identities. In order to achieve this objective, a combination of various existing methods and new ideas was applied, what resulted in promising effects.

The second chapter of this paper describes existing solutions in a domain of detecting multi-virtual identities, opinion spam and related research domains. The third chapter contains description of global concept and system's architecture implemented as a realization of this idea. Subsequent, the fourth chapter describe the experiment and the evaluation of methods applied to assess the solution's effectiveness. The fifth chapter contains results of the test and the last chapter present conclusions and plans for further works in this research area.

2. RELATED WORKS

The deception spam opinion is relatively new phenomena but various methods and research domains are already applied in searching for a solution. The most popular approaches aggregate solutions derived from crime-related duplicate identities detection (Wang et al., 2005) or text authorship analysis (Stamatatos, 2009a; Juola, 2007). However, none of those solution cannot be applied directly, due to significant differences related to deceptive opinion spam context. Methods of detecting multi-identities in databases relays usually on personal data, which does not appears in context of opinion spam or which are deliberately falsified. Solutions applied in text authorship analysis base on relatively wide text body, describing a small group of authors. In the area of deceptive spam opinion this ration is reversed, which makes those method ineffective.

Some surveys from text authorship analysis were applied also to data from the WEB. It includes n-gram based approach, presented by Stamatatos (2007) which was effective for group of 50 authors and it was used to detect plagiarism (Stamatatos, 2009b). Another features utilized to detect criminal activities, based on data from WEB resources were also style markers, text structure or keywords (Zheng et al., 2003). Also emails (Zheng et al., 2005) and web forums (Pillay & Soloiro, 2010) were data sources in the surveys related to text authorship analysis. All these solutions decrease an effectiveness with increasing authors number.

Classical spam detection from WEB resources, is another research area, which provides efficient methods, that can be utilized in resolving deceptive opinion spam issue (Jindal & Liu 2007). It was applied on data from recommendation portals, web forums and social networks (Wang et al., 2011; Mukherjee et al., 2012). The drawback of this approaches is that they function as a binary classifier, classifying content as a spam or not. Multi-identities detection is not supported by these solutions.

Social context and virtual identities' relations are subsequent feature used to detect multi-identities from WEB resources (Li et al., 2010). Social roles and activity types related with crime records were also employed to identify duplicated identities (Xu et al., 2007), although those methods were also based on personal data.

User's time activity combined with polarization of their comments were another method of detecting groups of users who spread opinion spam (Xie et al., 2012). However, this solution neither concern user's text content, nor detect multi-identities of a single person.

To summarize, current solutions for detecting virtual multi-identities and methods from related research domains have several drawbacks, that prevent from finding an effective solution for deceptive spam opinion issue. Methods derived from duplicated multi-identities detection are mainly based on personal data. Those derived from text authorship analysis researches are effective only for a small group of authors. Presented concept aggregates a group of various methods in order to create a solution that is effective for Internet data from WEB. These types of resources are characterized by a great number of authors described by short text bodies and lack of personal data. The effect of implementation and utilization of proposed concept is the IT system that support for detecting virtual multi-identities of a single person based on its features.

3. SYSTEM ARCHITECTURE

The overall system's architecture, which embody an implementation of presented concept is presented on a figure 1. System consists of the three main modules:

- crawl and data storage module,
- features and measures module,
- identity similarities detection module.

Details and the description of functional features are presented in subsequent parts of this paper. The system is implemented in JavaEE technology, based on JBoss application server and MySQL database engine. Universal interfaces are defined between all main modules, which allows to substitute single modules or components independently to hardware platform or programming language.

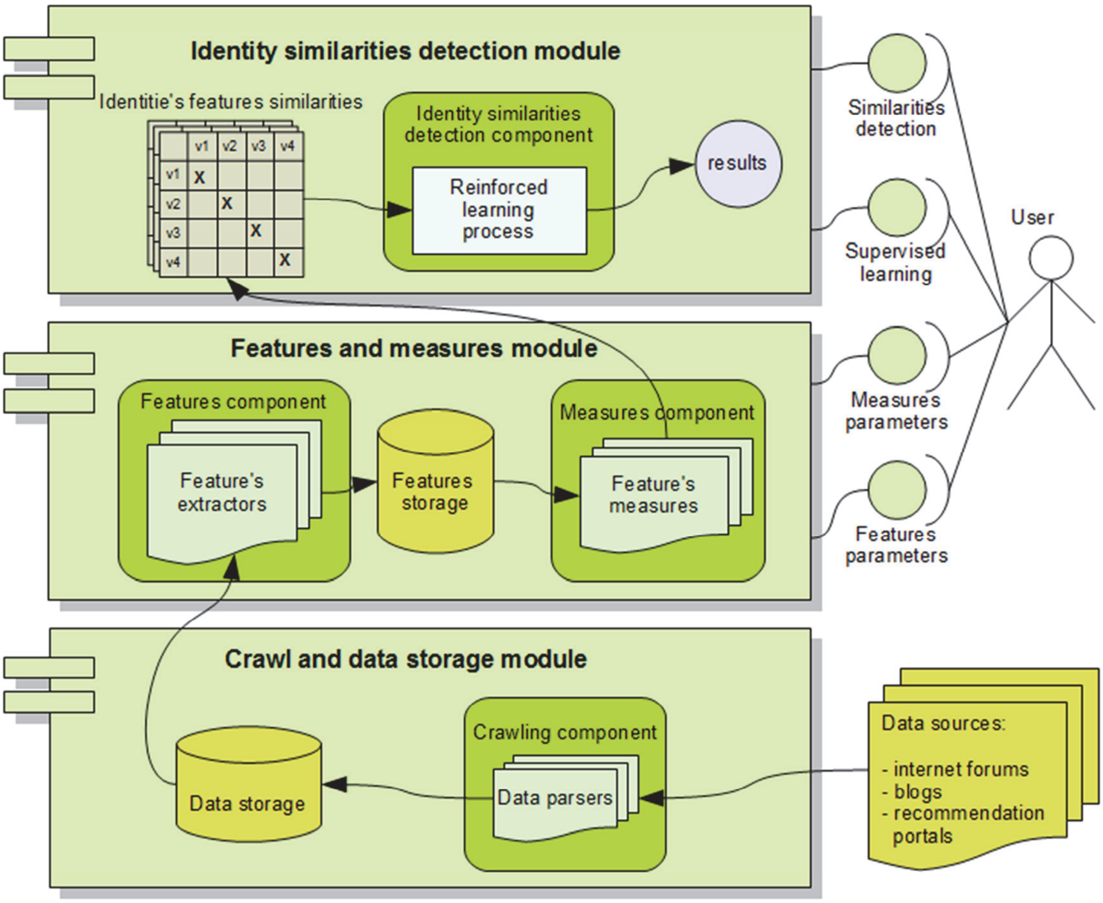


Fig. 1. Main system architecture

3.1. Crawl and data storage module

It is the first module within the process of data processing by the system, which consists of two main components: crawl component and database management system.

Crawl component provides functionality of processing resources from WEB and acquiring information, useful in subsequent data processing operation. Within this component, there were implemented data parsers and extractors, which acquire information from various resource types: web forums, blogs, recommendation portals.

Data acquired by crawl component are stored in the database management system, which pass them further, for the module of features and measures.

3.2. Features and measures module

Second main module within data processing process is features and measures module. First main functionality of this module is an extraction of features, which characterize all virtual identities, found during crawling process and stored in system database. Second main functionality is to compute similarities between all the pairs of those virtual identities, based on previously defined measure algorithms.

There are implemented 20 various virtual identity features within the system. It could be separated into the characteristics based on:

- text features,
  - number of posts, sentences, words, digits, characters,
  - frequency of an occurrence of punctuation marks and words containing following chars: %~@#$^&-_+=?[]{}/;,
  - function words (Zheng et al., 2005) and content related words (de Vel et al., 2001) - features based on text authorship approach ,
  - emotional polarization (sentiment) (Maciołek & Dobrowolski, 2013).
- common time activity points - compares users' activity timestamps,
- common object's links,
  - outgoing links included in user's posts,
  - source specific objects (threads, products, etc.).

The measure functions, also called "metrics", are implemented with purpose of a comparison of a pair of virtual identities based on a single feature. Metrics compute a similarity value for a pair of virtual identities (based on a single feature), which is a floating point number in the range of [0,1]. 0 value represents total lack of similarity and 1 value is computed for two identical virtual identities (considering a single feature).

Various measure's algorithms are applied in the system, depending on the feature's type. Equation 1 is applied for the numerical values:

$$S_m(i,j) = 1 - \frac{|f_m(i) - f_m(j)|}{\max(f_m) - \min(f_m)} \qquad (1)$$

For sets and the categorical values, similarity is computed by Jaccard's measure as in equation 2 below:

$$S(A,B) = \frac{|A \cap B|}{|A \cup B|} \qquad (2)$$

Similarities for all pairs of virtual identities are computed considering every feature, and the results are stored in the similarities matrices. Every feature refers to a corresponding matrix, where the matrix size is the number of virtual identities stored in the system.

3.3. Identity similarities detection module

The last phase in the data processing is executed by the Identity similarities detection module. It utilizes single feature based on a similarity values of pairs of virtual identities, that were computed by previous module, and which are stored in similarity matrices.

Within this module, there are three main methods of computing similarities of virtual identities:

- weighted sets of a similarity measures method (WSSM),
- hierarchical method,
- hybrid method.

Weighted sets of a similarity measures (WSSM) is the most general method, providing with results for wide set of data sources. It is described in details in the next part of this chapter. Hierarchical method is applied in cases where the priority of features set is known in advance. It is usually efficient, when reliable personal data are available, and are set at the top of prioritized list of features. The hybrid method is a combination of a pair of previous methods. It is applied when the number of virtual identities, or computational complexity of measure for any of features extends the capabilities of the system.

WSSM method computes the similarity of a pair of virtual identities based on all features available within the system. The general equation for this method is presented in equation 3:

$$S_p(t_i,t_j)=\sqrt{\frac{\sum_{w_a\in W_S} w_a * m_a(ch_i,ch_j)^2}{|W_s|}} \qquad (3)$$

where:
W – set of weights for features, $w_a \in W$
W_s – relevant set of weights, that:
$\forall w_a \in W_s$: $w_a \in$ W, $w_a > 0{,}1$

Weights from equation 3 are established during the supervised learning process, assisted by the system's administrator. Schema of the supervised learning process for the WSSM method is presented in figure 2.

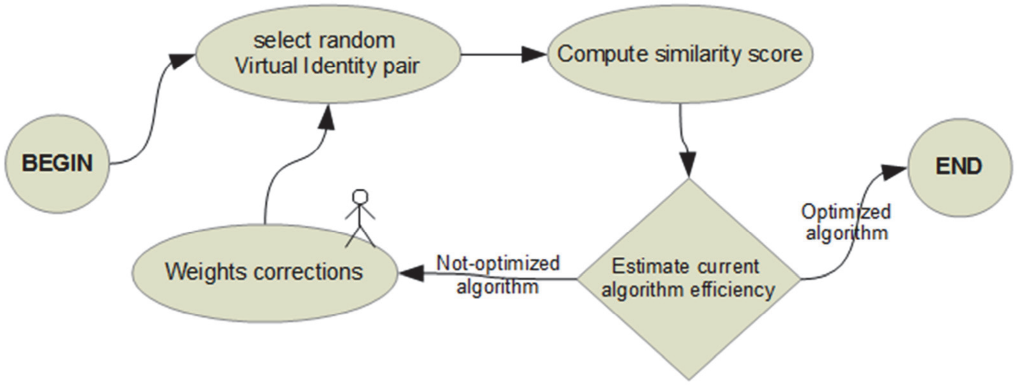


***Fig. 2.** Supervised learning algorithm schema*

Supervised learning schema starts with set of weights to 1 value. In the main loop of the learning process the supervisor assess the computed value of similarity for a random pair of virtual identities. If value does not reflect the real similarity of virtual identities, supervisor select the weights of features, that should be increased or reduced. Then, the loop is repeated. The values of weights are modified by 10% of their previous value. Whenever any feature's weight reaches the 0,1 level, the feature it is eliminated from the set of features. Supervised learning process finishes, when for the 10 subsequent drawings supervisor agree with the computed similarity value.

4. TESTBED AND EVALUATION METHODS

Well known issue in multi-identities detection and deceptive opinion spam researches is a lack of a gold standard data, which could be used in the verification of experiments (Ott et al., 2011; Jindal & Liu, 2008). There is a number of solutions applied in order to solve this problem. The first method utilized in researches in this area is to employ group of people, using the crowdsourcing portal and outsource them the task of generating training data representing unfair principals (Ott et al., 2011; Mukherjee et al., 2012). Another solution is the selection of verification set of data, based on the authors experiences gained during working as a crowdsourcer (Chen et al., 2011) or based on the fulfillment of certain assumptions. It could be for example high Google rank for a profile photo and deletion of an account from a social network, which may indicate potential fraud attempt (Wang et al., 2012).

Next method of results assessment for deceptive opinion spam research is a verification by a human arbiters group (Yang & Padmanabhan, 2010; Weimer et al., 2007; Kim et al., 2006). Despite potentially subjective human assessments, it has been proved, that applying group verification method significantly increases the effectiveness of this verification method (Le et al., 2010). A broadly used method of this type is called "Skeptic judge" and base on considering majority of votes, after exceeding the fixed threshold value (Ott et al., 2011).

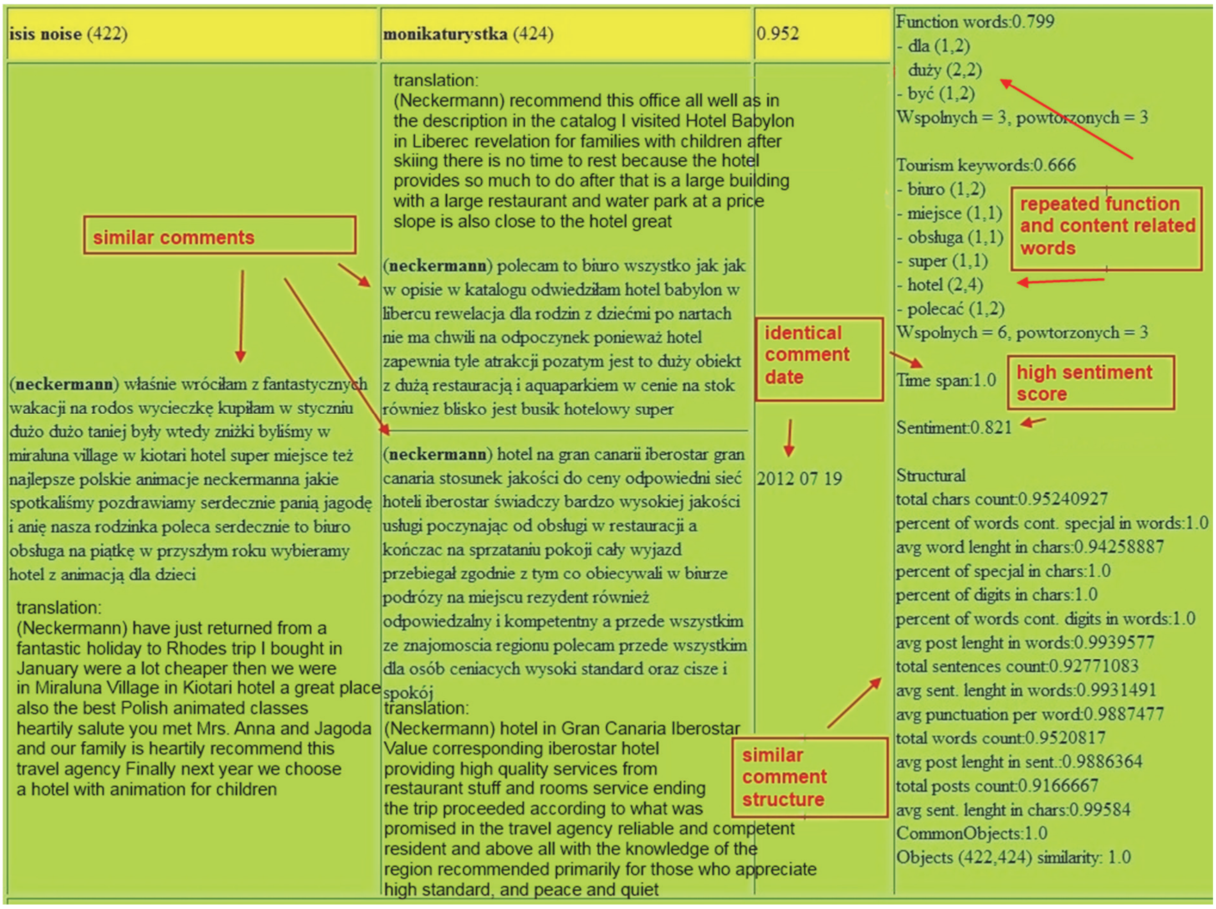
This paper presents results of two experiments:

Due to a lack of "gold standard data" for system's effectiveness evaluation, author browsed the Internet web forums and recommendation portals to gather data, that could be used for the results verification purposes.

First is based on data acquired from polish-language tourism related recommendation portal oceniacz.pl. For the tests purposes crawler module acquired 2034 opinions about 93 tourism agencies created by 1784 virtual identities. Verification of detection of multi-virtual identities is carried out by the "Skeptic judge" model consisting of a group of volunteer arbiters. System's assessment is considered to be correct when it matches with at least 3 of 4 judges answers.

Second experiment bases on polish-language web forum forumnasze.pl. System collected 1913 posts related to 281 forum threads created by 860 virtual identities. The results assessment is verified based on an examples of user accounts, that has been removed from forum due to "multi-account" violating regulation.

The second verification method, requires an information about banned multi-accounts, published by forum's supervisor. It's very rare within polish WEB resources, and couldn't been found on any industry related web forum. That is the reason, why a universal web forum were selected for testing purposes.



isis noise (422)

monikaturystka (424)

0.952

(**neckermann**) właśnie wróciłam z fantastycznych wakacji na rodos wycieczkę kupiłam w styczniu dużo dużo taniej były wtedy zniżki byliśmy w miraluna village w kiotari hotel super miejsce też najlepsze polskie animacje neckermanna jakie spotkaliśmy pozdrawiamy serdecznie panią jagodę i anię nasza rodzinka poleca serdecznie to biuro obsługa na piątkę w przyszłym roku wybieramy hotel z animacją dla dzieci

translation:
(Neckermann) have just returned from a fantastic holiday to Rhodes trip I bought in January were a lot cheaper then we were in Miraluna Village in Kiotari hotel a great place also the best Polish animated classes heartily salute you met Mrs. Anna and Jagoda and our family is heartily recommend this travel agency Finally next year we choose a hotel with animation for children

translation:
(Neckermann) recommend this office all well as in the description in the catalog I visited Hotel Babylon in Liberec revelation for families with children after skiing there is no time to rest because the hotel provides so much to do after that is a large building with a large restaurant and water park at a price slope is also close to the hotel great

(**neckermann**) polecam to biuro wszystko jak jak w opisie w katalogu odwiedziłam hotel babylon w libercu rewelacja dla rodzin z dziećmi po nartach nie ma chwili na odpoczynek ponieważ hotel zapewnia tyle atrakcji pozatym jest to duży obiekt z dużą restauracją i aquaparkiem w cenie na stok równiez blisko jest busik hotelowy super

(**neckermann**) hotel na gran canarii iberostar gran canaria stosunek jakości do ceny odpowiedni sieć hoteli iberostar świadczy bardzo wysokiej jakości usługi poczynając od obsługi w restauracji a kończac na sprzataniu pokoji cały wyjazd przebiegał zgodnie z tym co obiecywali w biurze podrózy na miejscu rezydent również odpowiedzalny i kompetentny a przede wszystkim ze znajomoscia regionu polecam przede wszystkim dla osób ceniacych wysoki standard oraz cisze i spokój

translation:
(Neckermann) hotel in Gran Canaria Iberostar Value corresponding iberostar hotel providing high quality services from restaurant stuff and rooms service ending the trip proceeded according to what was promised in the travel agency reliable and competent resident and above all with the knowledge of the region recommended primarily for those who appreciate high standard, and peace and quiet

2012 07 19

Function words:0.799
- dla (1,2)
duży (2,2)
- być (1,2)
Wspolnych = 3, powtorzonych = 3

Tourism keywords:0.666
- biuro (1,2)
- miejsce (1,1)
- obsługa (1,1)
- super (1,1)
- hotel (2,4)
- polecać (1,2)
Wspolnych = 6, powtorzonych = 3

Time span:1.0

Sentiment:0.821

Structural
total chars count:0.95240927
percent of words cont. specjal in words:1.0
avg word lenght in chars:0.94258887
percent of specjal in chars:1.0
percent of digits in chars:1.0
percent of words cont. digits in words:1.0
avg post lenght in words:0.9939577
total sentences count:0.92771083
avg sent. lenght in words:0.9931491
avg punctuation per word:0.9887477
total words count:0.9520817
avg post lenght in sent.:0.9886364
total posts count:0.9166667
avg sent. lenght in chars:0.99584
CommonObjects:1.0
Objects (422,424) similarity: 1.0

similar comments
identical comment date
repeated function and content related words
high sentiment score
similar comment structure

***Fig. 4.** Top 10 results: pair of virtual multi-identities*

5. RESULTS

The first experiment based on recommendation portal oceniacz.pl consists of series of tests verified by "Skeptic judge" model. One of the major tests is the TOP10 test, based on verification of 10 top from all 1,5 billion classified pairs of virtual identities, sorted with regards to their similarity value. Efficiency of the system is computed using popular classification estimator methods based on TruePositive, FalsePositive, TrueNegative and FalseNegative values (de Vel et al., 2001; Chen et al., 2004; Zheng et al., 2003). The Precision value is the final efficiency indicator, which is computed as in equation 4:

$$Precision = \frac{TruePositive}{TruePositive + FalsePositive} \tag{4}$$

For top 10 pairs of virtual identities 8 results was classified as TruePositive, 1 as FalsePositive and 1 as unresolved, when judges voted 2 vs 2. This results in Precision equals to 0,89 value, which is considered as a good classification efficiency.

Figure 4 presents exemplary pair of virtual identities found in set of TOP10 results. The features that results high similarity value (0,952) could be observed on the picture. Those are: similar comments content, repeated function and content related keywords, similar text's structure, identical comments' date and high sentiment's value.

The second experiment based on web forum data, was verified by 3 pairs of "multi-account" virtual identities. The similarities for all 369 000 of pairs of virtual identities were computed, and the position of the multi-accounts pairs constituted basis for verification, considering equation 5:

$$Eff = \frac{np - lp + 1}{np} \cdot 100\% \qquad (5)$$

where:
np – number of pairs
lp – positon on the sorted list

The results for 3 pairs of multi-accounts are presented in table 1.

Table 1. *Multi-accounts similarity results*

Virtual identity pair	Similarity value computed by the system	Position on the sorted list	Efficiency (Eff)
rozowaradosc x tomaszkrol	0,91	8	99.99%
tomaszkrol x princkaania	0,741	3 725	98,99%
rozowaradosc x princkaania	0,735	4 388	98,81%

Relatively high rank of multi-account pair of virtual identities confirms high system's efficiency. Considering 369 000 pairs of virtual identities the verification examples results in effectiveness of about 99%. The difference between first and next two pairs results from the fact, that the account "princkaania" was registered 9 days before the other two, which reduced similarity values for pairs containing this account.

6. CONCLUSIONS

The paper presents a concept of the solution that emerge the methods from various research domains and enrich them with some new elements: weighted sets of a similarity measure followed by supervised learning process. On the basis of tests carried out it can be stated, that the presented approach is correct, and the system is able to effectively detect hiding virtual multi-identities from WEB resources. It maintains the efficiency for a large number of authors and does not require the use of personal data.

The mechanism of supervised learning enables efficient application of universal WSSM method for various data sources from the WEB. Results of experiments indicate that system can be successfully used to detect standard cases of deceptive opinion spam, characterized by similar text content created in short period of time.

The system is an promising platform for a development of solutions in domain of detecting multi-identities and testing another approaches from various research domains.

REFERENCES

Chen, H. C., Goldberg, M., Magdon-Ismail, M. 2004. Identifying multi-ID users in open forums, *Intelligence and Security Informatics*, 176-186.

Chen, C., Wu, K., Srinivasan, V., Zhang, X. 2013. Battling the internet water army: Detection of hidden paid posters, *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 116-120.

Christopherson, K.M., 2007, The positive and negative implications of anonymity in Internet social interactions: On the Internet, nobody knows you're a dog, *Computers in Human Behavior*, 23(6), 3038-3056.

de Vel, O., Anderson, A., Corney, M., Mohay, G., 2001, Mining e-mail content for author identification forensics, *ACM Sigmod Record*, 30(4), 55-64.

International Telecommunication Union, 2012, Measuring the Information Society 2012, Place des Nations, CH-1211 Geneva Switzerland.

Jindal, N., Liu, B., 2007, Analyzing and Detecting Review Spam, *Data Mining, ICDM* 2007, October 28-31, 547-552.

Jindal, N., Liu, B., 2008, Opinion spam and analysis, *Proceedings of the International Conference on Web Search and Web Data Mining*, 219-230.

Juola, P., 2007, Authorship attribution, *Foundations and Trends in Information Retrieval*, 1(3), 233-334.

Kim, S.M., Pantel, P., Chklovski, T., Pennacchiotti, M., 2006, Automatically assessing review helpfulness, *Proc. of the 2006 Conference on Empirical Methods in Natural Language Processing*, 423-430.

Le, J., Edmonds, A., Hester, V., Biewald, L., 2010, Ensuring quality in crowdsourced search relevance evaluation: The effects of training question distribution, *SIGIR 2010 Workshop on Crowdsourcing for Search Evaluation,* 21-26.

Li, J., Wang, G.A., Chen, H., 2010, Identity matching using personal and social identity features, *Information Systems Frontiers*, 13(1), 101-113.

Maciolek, P., Dobrowolski, G., 2013, CLUO: Web-Scale Text Mining System for Open Source Intelligence Purposes, *Computer Science*, 14(1), 45. DOI:10.7494.

Miniwatts Marketing Group: World internet usage and population statistics, 2012, available online at: http://www.internetworldstats.com.

Mukherjee, A., Liu, B., Glance, N., 2012, Spotting Fake reviewer groups in consumer reviews, *Proc. of the 21st Int. Conf. on WWW*, 191-200.

Musial, K., Kazienko, P., 2013, Social networks on the internet, *World Wide Web*, 16 (1), 31-72.

Ott, M., Choi, Y., Cardie, C., Hancock, J. T., 2011, Finding deceptive opinion spam by any stretch of the imagination, *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies,* 1, 309-319.

Pillay, S.R., Solorio, T., 2010, Authorship attribution of web forum posts, *In: eCrime Researchers Summit* (eCrime), 1-7.

Stamatatos, E., 2007, Author identification using imbalanced and limited training texts, *18th International Workshop on DEXA 2007*, 237-241.

Stamatatos, E., 2009a, A survey of modern authorship attribution methods*, Journal of the American Society for information Science and Technology*, 60(3), 538-556.

Stamatatos, E., 2009b, Intrinsic plagiarism detection using character n-gram profiles, *3rd PAN Workshop on Uncovering Plagiarism, Authorship and Social Software Misuse,* 38.

Thomas, D., Douglas, T., Loader, B., eds., 2000, *Cybercrime: Law enforcement, security and surveillance in the information age*, Psychology Press.

Wang, A. G., Atabakhsh, H., Petersen, T., Chen, H., 2005, Discovering identity problems: A case study, *Intelligence and Security Informatics,* 368-373.

Wang, D., Irani, D., Pu, C., 2011, A social-spam detection framework, *Proceedings of the 8th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference*, 46-54.

Wang, G., Mohanlal, M., Wilson, C., Wang, X., Metzger, M., Zheng, H., Zhao, B., 2012, Social Turing Tests: Crowdsourcing Sybil Detection, *arXiv preprint:1205.3856.*

Weimer, M., Gurevych, I., M¨uhlh¨auser, M., 2007, Automatically assessing the post quality in online discussions on software, *Proceedings of the 45th Annual Meeting of the ACL*, 125-128.

Xie, S., Wang, G., Lin, S., Yu, P.S., 2012, Review spam detection via temporal pattern discovery, *Proceedings of the 18th ACM SIGKDD*, 823-831.

Xu, J., Chau, M., Wang, G.A., Li, J., 2007, Complex problem solving: identity matching based on social contextual information, *Journal of the Association for Information Systems*, 8(10), 525-545.

Yang, Y.C., Padmanabhan, B., 2010, Toward user patterns for online security: Observation time and user identification, *Decision Support Systems*, 48(4), 548-558.

Zheng, R., Qin, Y., Huang, Z., Chen, H., 2003, Authorship analysis in cybercrime investigation, *Intelligence and Security Informatics,* Springer Berlin Heidelberg 59-73.

Zheng, R., Li, J., Chen, H., Huang, Z., 2005, A framework for authorship identification of online messages: Writing-style features and classification techniques, *Journal of the American Society for Information Science and Technology*, 57(3), 378-393.

DETEKCJA WIRTUALNYCH MULTI-TOŻSAMOŚCI

Streszczenie

Ostatnia dekada jest okresem dynamicznego rozwoju sieci Internet. Różne dziedziny życia ludzkiego stopniowo przenoszą się do cyberprzestrzeni, w ramach której ludzie reprezentowani są poprzez swoje wirtualne tożsamości. Grupy wirtualnych tożsamości, ich relacje oraz kontekst środowiskowy tworzą jako całość cyberspołeczeństwo. Z uwagi na unikalną strukturę cyberspołeczeństwa, wirtualne tożsamości charakteryzują się stosunkowo wysokim poziomem anonimowości. Jest to przyczyną występowania zjawiska wirtualnych multi-tożsamości, kiedy to jedna fizyczna osoba jest reprezentowana poprzez wiele tożsamości wirtualnych. Prowadzi to zarówno do pozytywnych jaki i negatywnych skutków, a jednego z tych negatywnych, dotyczy prezentowany artykuł. Jest to konkretnie zjawisko oszustwa opiniotwórczego, generowanego przez pojedyncze fizyczne osoby przy użyciu wielu tożsamości wirtualnych (multi-tożsamości). Problem ten nieustannie narasta, jako że sieć WEB jest coraz bardziej popularnym źródłem opinii. W pracy zaprezentowano koncepcje systemu łączącego rozwiązania z wielu dziedzin badawczych, mającego na celu pomóc w rozwiązywaniu problemu wykrywania multi-tożsamości, ukrywających się sieciach społecznych typu forum dyskusyjne, blog lub portal rekomendacyjny. W pracy zawarto opis koncepcji, architektury oraz części implementacyjnej systemu. Ocena skuteczności systemu przeprowadzona została w oparciu o przykłady z portalu rekomendacyjnego i forum dyskusyjnego.

Received: October 23, 2014
Received in a revised form: November 28, 2014
Accepted: December 12, 2014