IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 6 (Jul. - Aug. 2013), PP 16-19
www.iosrjournals.org

Detecting Spam Tags Against Collaborative Unfair Through Trust Modelling

N.Shravani[1], Dr.P.Govardhan[2]
[1]*computer science / vardhaman college of engineering, India*
[2]*Information technology, Vardhaman college of engineering, India*

Abstract : *In the past few years sharing photos, within social networks has become very popular .In order to make these huge collection easier to explore, images are usually tagged with representative keywords such as persons, events, objects, and locations. In order o speed up the time consuming tag annotation process, tags can be propagated based on the similarity between image content and context .In this paper, daily and continuous communication implies the exchange of several types of content, including free text, image, audio and video data. Based on the established correspondences between these two image sets and the reliability of the user, tags are propagated from the tagged to the untagged images. The user trust modeling reduces the risk of propagating wrong tags caused by spamming or faulty annotation. The effectiveness of the proposed method is demonstrated through a set of experiments On an image database containing various landmarks. Tagging in online social networks is very popular these days as it facilitates search and retrieval of multimedia content .However, noisy and spam annotations often make it.*
Keywords – *annotation process, audio and video data, trust modeling, tagging, spams.*

I. Introduction

The past few years have witnessed an increasing popularity of social networks, digital photography and web-based personal image collections. A social network service typically focuses on building online communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. Most social network services are web-based and provide a variety of ways for users to interact. They have become also a popular way to share and disseminate information, e.g. users upload their personal photos and share them through online communities asking other people to comment or rate their content. This has resulted in a continuously growing volume of publicly available photos ,e.g. Flicker.

One of the key features of social information systems is their reliance on users as primary contributors of content and as annotators and raters of other content. this reliance on users can lead to many positive effects, including large-scale growth in the size and content in the community (e.g., YouTube, Wikipedia), bottom-up discovery of "citizen-experts" with specialized Social networks and multimedia content sharing Web sites have become increasingly popular in recent years. Their service typically focuses on building online communities of people who share interests and activities, or are interested in exploring the interests and activities of others. At the same time, they have become a popular way to share and disseminate information. For example, users upload their personal photos and share them through online communities, letting other people comment or rate them. This trend has resulted in a continuously growing volume of publicly available multi- media content on content sharing Web sites like Flickr, Picasa and YouTube as well as social networks like Face book, which have created new challenges for access, search, and retrieval of the shared content. For instance, Flicker has hosted more than 6 billion photos since August 2011,and Facebook has approximately 100 billion photos stored on its servers. Every minute, 48 h of video are uploaded to YouTube .and 20 million videos are uploaded to Face book every month.

Trust provides a natural security policy stipulating that users or content with low trust values should be investigated or eliminated. Trust can predict the future behavior of users to avoid undesirable influences of untrustworthy users .Trust- based schemes can be used to motivate users to positively con- tribute to social network systems and/or penalize adversaries who try to disrupt the system. The distribution of the trust values of the users or content in a social network can be used to represent the health of that network.

II. Tag Prpogation.

The goal of the tag propagation module is to propagate the geo tags from the tagged to the non-tagged images according to the matching scores, provided by the object duplicate detection module. As a result, labels from the training set are propagated to the same object found in the test set. The geographical metadata (geo tags) embedded in the image file usually consist of location names and/or GPS coordinates, but may also include altitude, viewpoint, etc. Two of the most commonly used metadata formats for image files are EXIF and IPTC. In this paper, we consider the existing IPTC schema and introduce a hierarchical order for a subset of the

available geo tags, namely: city (name of the city where image was taken) and sub location (area or name of the landmark).

Our system supports two application scenarios as shown in Fig. 2.Inthe closed set problem, each test image is assumed to correspond to exactly one of the known (trained) landmarks. Therefore, the image gets assigned to the most probable trained landmark and the corresponding tag is propagated to the test image. This is comparable to an identification task in biometrics. However, in the open set problem the test picture may correspond to an unknown landmark. This problem is comparable to a watch list task in biometrics where the goal is to distinguish between known and unknown persons (landmarks) and to propagate the tags only for the known ones. For example, we assume that the system is trained with only three known landmarks: Budapest (Parliament), Belgrade (Church St. Sava) and Tokyo (Tower). Given the input test image of Paris (Eiffel Tower), the system gives different results for the closed and open set problems. In the closed set problem, our system finds that Tokyo (Tower) is the most suitable model for the test image. If we consider the open set problem, the system does not retrieve any of the trained models since the matching scores between the object models and the test image do not exceed a predefined threshold. The open and closed set problems are separately evaluated in Section 4 as detection and recognition tasks, respectively.

In this paper ground truth data are used for the estimation of the user trust ratio. However, for a real photo sharing system, such as Panoramic, it is not necessary to collect ground truth data since user feedback can replace them. The main idea is that users evaluate tagged images by assigning a true or a false flag to the tag associated with an image. If the user assigns a false flag, then he/she needs to suggest a correct tag for the image. The more misplacement a user has, the more untrusted he/she is. By applying this method, spammers and unreliable users can be efficiently detected and eliminated. Therefore, the user trust ratio is calculated as the ratio between the number of true flags and all associated flags over all images tagged by that user. The number of misplacements in Panoramic is analogous to the number of wrongly tagged images in our approach.

In case that a spammer attacks the system, other users can collaboratively eliminate the spammer. First, the spammer wants to make other users un trusted, so he/she assigns many false flags to the tags given by those other users and sets new, wrong, tags to these images. In this way, the spammer becomes trusted. Then, other users correct the tags given by the spammer, so that the spammer becomes un trusted and all of his/her feedbacks in the form of flags are not considered in the whole system. Finally, previously trusted users, who were untrusted due to spammer attack, recover their status. Following this scenario, the user trust ratio can be constructed by making use of the feedbacks from other users who agree or disagree with the tagged location. However, due to the lack of a suitable dataset which provides user feedback, the Xu et al. introduced the concept of "authority" in social bookmarking systems, where they measured the goodness of each tag with respect to a content by the sum of the authority scores of the users who have assigned the tag to the content. Authority scores and goodness are iteratively updated by using hyperlink-induced topic search (HITS), which was initially used to rank Web pages based on their linkage on the Web .In contrast, Krestel and Chen iteratively updated scores for users only. They proposed to use a spam score propagation tech-nique to propagate trust scores through a social graph, similar to that shown in Figure 1, where edges between nodes (in this case, users) indicate the number of common tags supplied by users, common content annotated by users and/or common tag-content pairs used by users. Starting from a manually assessed set of nodes labeled as spammers or legitimate users with the initial spam scores, a TrustRank metric is used to calculate.

III. Trust Modelling.

When information is exchanged on the Internet, malicious individuals are everywhere, trying to take advantage of the information exchange structure for their own benefit, while bothering and spamming others. Before social tagging became popular, spam content was observed in various domains first in e-mail, and then in Web search networks have been also influenced by malicious peers, and thus various solutions based on trust and reputation have been proposed, which dealt with collecting information on peer behavior, scoring and ranking peers, and responding based on the scores Today, even blogs are spammed. Ratings in online reputation systems, such as eBay, Amazon, and Epinions, are very similar to tagging systems and they may face the problem of unfair ratings by artificially inflating or deflating reputations. Several filtering techniques for excluding unfair ratings are proposed in the literature. Unfortunately, the countermeasures developed for e- mail and Web spam do not directly apply to social networks

3.1 Content Trust Modeling

Content trust modeling is used to classify content (e.g., Web pages, images, and videos) as spam or legitimate. In this case, the target of trust is a content (resource), and thus a trust score is given to each content based on its content and/or associated tags. Content trust models reduce the prominence of content likely to be spam, usually in query-based retrieval results. They try to provide better ordering of the results to reduce the expo- sure of the spam to users. Koutrika et al. proposed that each incorrect content found in a system could

be simply removed by an administrator. The administrator can go a step further and remove all content contributed by the user who posted the incorrect content, on the assumption that this user is a spammer (polluter).

Approaches for content trust modeling utilize features extracted from content information, users' profiles and/or associated tags to detect specific spam content proposed an algorithm called Trust Rank to semi automatically separate reputable from spam Web pages. Trust Rank relies on an important empirical observation called approximate isolation of the good set: good pages seldom point to bad ones. It starts from a set of seeds selected as highly qualified, credible, and popular Web pages in the Web graph, and then iteratively propagate trust scores to all nodes in the graph by splitting the trust score of a node among its neighbors according to a weighting scheme. Trust Rank effectively removes most of the spam from the top-scored Web pages, however it is unable to effectively separate low-scored good sites from bad ones, due to the lack of distinguishing features. In search engines, Trust Rank can be used either solely to filter search results, or in combination with Page Rank and other metrics to rank con- tent in search results.

3.2 User Trust Modeling

In user trust modeling, trust is given to each user based on the information extracted from a user's account, his/her interaction with other participants within the social network, and/or the relationship between the content and tags that the user contributed to the social tagging system. Given a user trust score, the user might be flagged as a legitimate user or spammer.

User trust can be established in a centralized or distributed manner In centralized trust systems, users' trust models are maintained by one central authority, i.e., manager, while in distributed trust systems each user maintains his/her own trust manager based on the previous interactions with other users. Distributed trust models are mainly used in P2P networks while social networks usually use centralized systems .user trust modeling has a disadvantage of "broad brush," i.e., it may be excessively strict if a user happens to post one bit of questionable content on otherwise legitimate content. The trust-worthiness of a user is often judged based on the content that the user uploaded to a social system, and thus "subjectivity" in discriminating spammers from legitimate users remains an issue for user trust modeling as in content trust modeling.

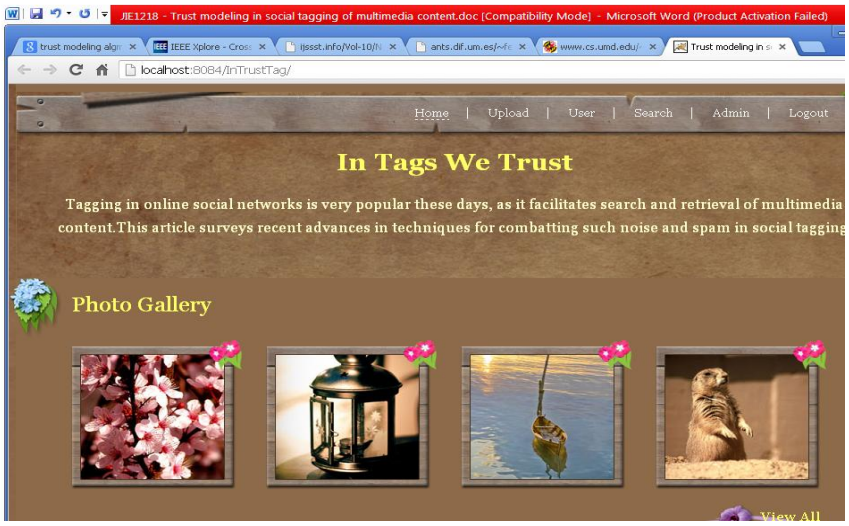

Fig 1

IV. Open Issues And Challenges:

There have been a variety of data sets from different social networks and even different data sets of one social network for evaluation of trust modeling approaches, as shown in the "Evaluation" section. However, publication of such data sets is rarely found, which makes it difficult to compare results and performance of dif- ferent trust modeling approaches. Therefore, it would be desirable to promote researchers to make their data sets publicly available to the research community, which can be used for comparison and benchmarking of different approaches. Furthermore, most of the data sets provide data for evaluating only one aspect of trust modeling, either user or content trust modeling, while evaluation of the other aspect requires introducing simulated objects in the real-world social tagging data sets (e.g., [20] and [29]). However, fo r the thorough

evaluation of a trust model it is necessary that real-world data sets have ground- truth data for both users and content.

Most of the existing trust modeling approaches based on text information assume monolingual environments. However, many social network services are used by people from various countries, so that various languages simultaneously appear in tags and comments. In such cases, some text information may be regarded as wrong due to the language difference. Therefore incorporating the multilingualism in trust modeling would be useful to solve this problem.

V. Conclusion:

In this article, we dealt with one of the key issues in social tagging systems combating noise and spam. We classified existing studies in the literature into two categories, i.e., content and user trust modeling.

Representative. we dealt with one of the key issues insocial tagging systems: combating noise and spam. We classified existing studies in the literature into two categories, i.e., content and user trust modeling. Representative techniques in each category were analyzed and compared. In addition, existing databases and evaluation protocols were re viewed. An example system was presented to demonstrate how trust modeling can be particularly employed in a popular application of image sharing and geo tagging. Finally, open issues and future research trends were prospected. As online social networks and content sharing services evolve rapidly, we believe that the research on enhancing reliability and trust worthiness of such services will become increasingly important.

Currently the user trust model relies on predefined ground truth to estimate the user trust ratios. Future work will focus on automatic ground truth generation using Word Net and Wikipedia to obtain tagged image samples. In addition, we will work on developing new approaches for creating user trust models by considering user trust values assigned by particular user to other users and employing some ranking algorithm such as Page Rank. we aim to achieve hybridization through aggregating with the system that was proposed in and that isbased on extracting association rules from navigation sessions. Therefore, in future works.

References

[1] kyuoo, and D. Su, "Towards the semantic Web: Collaborative tag suggestions," in Proc. ACM WWW, May 2006, pp. 1–8.
[2] ive sources in a hyperlinked environment," JACM, vol. 46, no. 5, pp. 604–632, Sept. 1999
[3] page, s.brin, r. motwani, and t.winograd. the pagerank citation ranking:bringing order to the web. technical report, stanforduniversity, 1998.
[4] m. richardson, r..agrawal, and p. domingos. trust management for the semantic web. in web, proceedings of the second international semantic web conference,2003.
[5] K, J.-S. Lee, L. Goldmann, and T. Ebrahimi, "Geotag propaga- tion in social networks based on user trust model," Multimedia Tools Applicat., pp. 1–23, July 2010.
[6] ML. von Ahn, B. Maurer, C. Mcmillen, D. Abraham, and M. Blum, "reCAPTCHA: Human-based character recognition via Web security measures," Science, vol. 321, no. 5895, pp. 1465–1468, Aug. 2008.
[7] petrusel, r.. stanciu, p.l.: making recommendations for decision processes based on aggregated decision data models. in abramowicz, w. et al.(eds.): bis 2012, lnbip 117, pp. 272–283. springer-verlag berlin heidelberg (2012)