Image Analysis for Privacy Assessment in Social Networks

Joaquin Taverner, Ramon Ruiz, Elena del Val, Carlos Diez, and Jose Alemany

Universitat Politècnica de València,
Camino de Vera s/n, Valencia, Spain
{joataap, raruidol, edelval, cardieal, jalemany1}@dsic.upv.es

Abstract. Nowadays, the concern about privacy in online social networks has increased. However, the definition of an appropriate privacy policy might be a complex task, especially when several users are involved and have different privacy preferences. This problem usually appears when a user publishes a photo. In this paper, we propose a tool to automatically define the audience of a photo based on a trust metric. This metric uses a set of features (i.e., distance between users, number of people, emotions, etc.) obtained by the image analysis provided by *IBM Cloud Visual Recognition Service*. In a preliminary experiment considering 40 photos of 4 users, the results show that the proposed trust metric approximates the real trust relationships between users. We plan to integrate the tool into a real online social network.

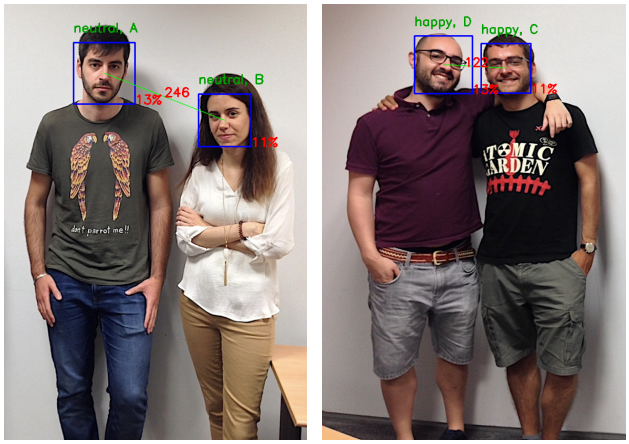
Keywords: Image analysis, privacy negotiation, social networks, trust

1 Introduction

One of the problems that arises when sharing content (e.g., photos) in an online social network is the definition of the privacy policy [1,7,10]. This problem becomes more complex if there are more than one user involved in the shared content (e.g., various users appearing in the same photo) [11,4]. Consider the next scenario where a user A decides to publish a photo where (besides him) other people appear (users B and C). In that moment, a dilemma may arise to the user A: should I publish the photo using my privacy policy? or it would be better if I publish according to the privacy concerns of the users involved? which is the most suitable privacy policy? As each user has his own concern about privacy, it is necessary to reach an agreement.

Taking this problem into consideration, this proposal aims to provide an automatic privacy policy assessment for photo sharing in social networks. In order to achieve this goal, we propose to use a trust model to define the relationships between the users based on feature extraction from published images.

The proposed model consists of the following modules: (i) Image Feature Extraction, (ii) Trust Estimation, (iii) Privacy Policy Recommendation. The



(a) (b)

Fig. 1: Examples of the results obtained by the Image Feature Extraction process.

Image Feature Extraction module analyzes the image and detects the faces that appear in the photo. This module uses the *IBM Cloud Visual Recognition* service [2] to identify the users associated with the faces, and estimates the degree of trust between them. To calculate their degree of trust, the module analyzes the following features: the distance between the users that appear in the photo, the sentiment of each user, the number of people, the type of photo (e.g., close-up photography, portrait, etc.) (see Figures 1a and 1b), and finally, the number of times users appear together in a photo. Based on these features extracted from the image, the Trust Estimation module estimates the degree of trust for each pair of users that appear in the photo. Each time a new photo is added to the online social network, the degree of trust of the users identified in the photo is updated.

The degree of trust is used by the Privacy Policy Recommendation module to assist in the decision-making process of which is the most suitable privacy policy for publishing a photo. The module creates a personalized list of users that could see the photo based on their degree of trust. Considering the previous scenario where user A publishes a photo, the audience list that is going to see the photo is automatically created. The members of this list are a subset of the user's A friends, user's B friends, and user's C friends that have a trust value with the co-owners of the photo (A, B, and C) over a trust threshold. The value of the trust threshold is established considering the most restrictive value of trust of the users involved.

To test the Image Feature Extraction and the Trust Estimation modules, we design an experiment. For this experiment, we considered forty photos from four users (ten for each one). These photos were analyzed to calculate the trust

values between users. For example, in Figure 1 we can see the results of this process. The top label represents the emotion detected in the face, followed by the user identifier (in this case we use A, B, C, and D). The bottom label is the total percentage of the face in the image to estimate the distance to the camera. And the label on the line indicates the distance between the users. We can observe that users A and B (Figure 1a) have a neutral emotion and the distance between both is higher than the users C and D, that are expressing happiness. Therefore, if we only take into account this two images we can deduce that there is a higher level of confidence between users C and D than between users A and B.

Then, we compare the calculated trust with the real trust values between users. The real trust values were obtained using a questionnaire previous to the experiment. The results are shown in Table 1. As can be noted from the table, the trust relationship between users is not symmetric. Asymmetry occurs because of the nature of the human relationships and differences in peoples' perceptions, opinions, beliefs, and expectations [6,8]. In our case, the asymmetry is due to the users' emotions shown in the photos.

Users	A	B	C	D
A	-	0.6	0.8	0.6
	-	0.66	0.67	0.71
B	0.6	-	0.4	0.0
	0.7	-	0.23	0.0
C	0.6	0.6	-	0.8
	0.68	0.65	-	0.71
D	0.6	0.0	1.0	-
	0.72	0.0	0.84	-

Table 1: Comparison between the real trust values (above) and the trust values obtained by the proposed model (below).

Finally, to evaluate the Privacy Policy Recommendation module, we plan to integrate it in the PESEDIA social network designing an experiment with real users. With this experiment, we want to test if the audience list associated with the photo by our proposal corresponds to the users' expected audience obtained by an initial questionnaire.

2 Conclusions

In this work, we propose a tool to assist users in the privacy decision making process when sharing a photo on a social network. This tool consists of three modules: Image Feature Extraction, Trust Estimation, and Privacy Policy Rec-

ommendation.

The majority of direct social trust metrics are based on the activity in social networks [3] such as the number of comments, number of likes, or number of tags [8,9]. In this paper, we propose a metric based on image features. This metric could be complementary to other existing approaches [5] to estimate the trust value in a more informed way. We have created a recommendation module based on the proposed trust metric. This module allows the automatic definition of the audience of a publication where more than one user appears.

Acknowledgements

This work is partially supported by the Spanish Government project TIN2017-89156-R, by the FPI grants BES-2015-074498 and ACIF/2017/085, and the Post-Doc scholarship with the Ref. SP20170057.

References

1. J. Alemany, E. del Val, J. Alberola, and A. García-Fornes. Estimation of privacy risk through centrality metrics. *Future Generation Computer Systems*, 2017.
2. B. Bhattacharjee, S. Boag, C. Doshi, P. Dube, B. Herta, V. Ishakian, K. Jayaram, R. Khalaf, A. Krishna, Y. B. Li, et al. Ibm deep learning service. *IBM Journal of Research and Development*, 61(4):10–1, 2017.
3. S. P. Marsh. Formalising trust as a computational concept. 1994.
4. Y. Mester, N. Kökciyan, and P. Yolum. Negotiating privacy constraints in online social networks. In *Advances in Social Computing and Multiagent Systems*, pages 112–129. Springer, 2015.
5. S. Nepal, W. Sherchan, and C. Paris. Strust: A trust model for social networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 841–846. IEEE, 2011.
6. J. Sabater and C. Sierra. Reputation and social network analysis in multi-agent systems. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: Part 1*, pages 475–482. ACM, 2002.
7. M. Shehab and H. Touati. Semi-supervised policy recommendation for online social networks. In *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*, pages 360–367. IEEE, 2012.
8. W. Sherchan, S. Nepal, and C. Paris. A survey of trust in social networks. *ACM Computing Surveys (CSUR)*, 45(4):47, 2013.
9. M. Šitum. Analysis of algorithms for determining trust among friends on social networks. *Vienna, June*, 2014.
10. A. C. Squicciarini, F. Paci, and S. Sundareswaran. Prima: a comprehensive approach to privacy protection in social network sites. *annals of telecommunications-annales des télécommunications*, 69(1-2):21–36, 2014.
11. J. M. Such, J. Porter, S. Preibusch, and A. Joinson. Photo privacy conflicts in social media: a large-scale empirical study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3821–3832. ACM, 2017.