Abstract

In this paper a comparison is performed on two of the key methods for graph anonymization and their behavior is evaluated when constraints are incorporated into the anonymization process. The two methods tested are node clustering and node modification and are applied to online social network (OSN) graph datasets. The constraints implement user defined utility requirements for the community structure of the graph and major hub nodes. The methods are benchmarked using three real OSN datasets and different levels of k-anonymity. The results show that the constraints reduce the information loss while incurring an acceptable disclosure risk. Overall, it is found that the modification method with constraints gives the best results for information loss and risk of disclosure.

References

Privacy and authentication) Vol. 1, Issue 1, pages 102-114.

- Leskovec, J., Kleinberg, J., Faloutsos, C. 2007. Graph Evolution: Densification and Shrinking Diameters, ACM Transactions on Knowledge Discovery from Data (ACM TKDD), 1(1).

**Index Terms**

Computer Science  
Applied Mathematics

**Keywords**

Data privacy  
information hiding  
graphs and networks  
online social networks  
anonymization

information loss

risk of disclosure