finished only using the open data and the common classification algorithms can be used directly.

The new algorithm has three steps. First, a serious of classifiers is trained by using the original data. Then, new samples are generated randomly. Finally, we use the classifiers trained in the first step predict the category of the samples generated in the second step. Using experiments, we demonstrated that our new method can maintain good data utility while preserving privacy.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the National Nature Science Foundation of China (51407012) and the Chang'an University's Fundamental Research Funds (0009-2014G6114024).

REFERENCES

[1] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-preserving data publishing: a survey of recent developments", *ACM Computing Surveys*, vol. 42, pp. 14:1-14:53, 2010.

[2] E. Bertino, I. Fovino, and L. Provenza, "A framework for evaluating privacy preserving data mining algorithms", *Data Mining and Knowledge Discovery*, vol. 11, pp. 121-154, 2005.

[3] V. Verykios, E. Bertino, I. Fovino, L. Provenza, Y. Saygin, and Y. Theodoridis, "State-of-the-art in privacy preserving data mining", *SIGMOD Record*, vol. 33, pp. 50-57, 2004.

[4] B. Fung, K. Wang, and P. Yu, "Anonymizing classification data for privacy preservation", *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, pp. 711-725, 2007.

[5] K. Babu, N. Reddy, N. Kumar, M. Elliot, and S. Jena, "Achieving k-anonymity using improved greedy heuristics for very large relational databases", *Transactions on Data Privacy*, vol. 6, pp. 1-17, 2013.

[6] S. Kisilevich, L. Rokach, Y. Elovici, and B. Shapira, "Efficient multidimensional suppression for K-anonymity", *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, pp. 334-347, 2010.

[7] B. Pinkas, "Cryptographic techniques for privacy-preserving data mining", *ACM SIGKDD Explorations Newsletter*, vol. 4, pp. 12-19, 2002.

[8] F. Emekci, O. Sahin, D. Agrawal, and A. Abbadi, "Privacy preserving decision tree learning over multiple parties", *Data & Knowledge Engineering*, vol. 63, pp. 348-361, 2007.

[9] S. Xu, J. Zhang, D. Han, and J. Wang, "Singular value decomposition based data distortion strategy for privacy protection", *Knowledge and Information Systems*, vol. 10, pp. 383-397, 2006.

[10] J. Wang, J. Zhang, S. Xu, and W. Zhong, "A novel data distortion approach *via* selective SSVD for privacy protection", *International Journal of Information and Computer Security*, vol. 2, pp. 48-70, 2008.

[11] J. Wang, W. Zhong, and J. Zhang, "NNMF-based factorization techniques for high-accuracy privacy protection on non-negative-valued datasets", in: *Proceedings of the 6th IEEE International Conference on Data Mining - Workshops*, Hong Kong, pp. 513-517, 2006.

[12] I. Witten and E. Frank, Data Mining: *Practical Machine Learning Tools and Techniques* (3rd ed), Massachusetts: USA, 2011.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014