

# An Improvement of Privacy-Preserving Scheme Based on Random Substitutions

Ju-Sung Kang

Department of Mathematics, Kookmin University, KOREA  
jskang@kookmin.ac.kr

## 1 Introduction

Data perturbation techniques are one of the most popular models for privacy-preserving data mining due to their practical utility [1]. In a typical data perturbation, before the data owner publishes the data, they randomly change the data in certain way to disguise the private information while preserving some statistical properties for obtaining meaningful data mining models.

Agrawal and Haritsa [2] have proposed a generalized matrix-theoretic framework of random perturbation that facilitates a systematic approach to the design of random substitutions. They used a privacy measure called  $\rho_1$ -to- $\rho_2$  privacy breach [5], and chose a special type of optimal perturbation matrix called the  $\gamma$ -diagonal matrix. Agrawal and Haritsa [2] explored their framework in the context of privacy-preserving association rule mining, and Dowd et al. [4] extended the results to privacy-preserving decision tree mining. Also the authors of [4] explained that random substitution with  $\gamma$ -diagonal matrix is fundamentally different from adding noise and it is secure against data-recovery attacks of [7] and [6].

In this research we discuss a theoretical upper bound of the estimation error for the matrix-based random perturbation method, and concretely examine the relationship among the parameters used in the random substitutions by  $\gamma$ -diagonal matrices. Moreover we propose a method of improving the accuracy of random substitutions and theoretically analyze its effect of improvement on the view point of the estimation error.

## 2 Main results

We can obtain the relationship between the estimation error and three parameters, namely the privacy assurance metric  $\gamma$ , the dimension size  $N$  of transition matrix, and the total number  $n$  of data records. We consider

the standard deviation of the estimator  $\hat{X}$ ,

$$\sigma_{\hat{X}} = \sqrt{\text{Var}(\hat{X})} = \sqrt{E[\|\hat{X} - X\|^2]},$$

as the estimation error of reconstruction procedure.

**Theorem 1.** *Let  $X = (X_1, \dots, X_N)$  and  $Y = (Y_1, \dots, Y_N)$  denote the random vectors representing frequency of  $(u_1, \dots, u_N)$  in the original data set  $D = [d_1, d_2, \dots, d_n]$  and the perturbed data set  $\tilde{D} = [\tilde{d}_1, \tilde{d}_2, \dots, \tilde{d}_n]$  of  $n$  records, respectively, and  $\mathbf{P} = (p_{ij})$  be the  $\gamma$ -diagonal transition matrix satisfying the condition  $p_{ii} = \gamma/(\gamma + N - 1)$ , and for  $i \neq j$ ,  $p_{ij} = 1/(\gamma + N - 1)$ . Then the standard deviation of the estimator  $\hat{X} = Y\mathbf{P}^{-1}$  satisfies the following inequality: for any  $\gamma > 1$ , and positive integers  $N$  and  $n$ ,*

$$\frac{\sigma_{\hat{X}}}{\|X\|} \leq \frac{\sqrt{N(N-1)(N+2(\gamma-1))}}{(\gamma-1)n^{1/2}}.$$

Recently Agrawal et al. [3] mentioned the relationship between the database size  $n$  and accuracy. They obtained a probabilistic upper bound on the normalized deviation and proposed the multiple independent perturbations as a method of achieving the desired accuracy. We have independently studied slightly different multiple random substitutions and concretely examined their effect of improving accuracy on the view point of the estimation error.

## References

1. R. Agrawal and R. Srikant, *Privacy-preserving data mining*, Proc. of ACM SIGMOD International Conference on Management of Data, May 2000.
2. S. Agrawal and J. Haritsa, *A framework for high-accuracy privacy-preserving mining*, Proceedings of the 21st International Conference on Data Engineering (ICDE 2005), IEEE, 2005.
3. S. Agrawal, J. Haritsa, and B. A. Prakash, *FRAPP: a framework for high-accuracy privacy-preserving mining*, Data Mining and Knowledge Discovery, Springer, Vol. 18, No. 1, 2009, pp. 101-139
4. J. Dowd, S. Xu, and W. Zhang, *Privacy-preserving decision tree mining based on random substitutions*, ETRICS 2006, LNCS 3995, Springer-Verlag, 2006, pp. 145-159.
5. A. Evfimievski, J. Gehrke, and R. Srikant, *Limiting privacy breaching in privacy preserving data mining*, ACM Symposium on Principles of Database Systems, ACM, 2003, pp. 211-222.
6. Z. Huang, W. Du, and B. Chen, *Deriving private information from randomized data*, ACM SIGMOD International Conference on Management of Data, ACM, 2005, pp. 37-47.
7. H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, *On the privacy preserving properties of random data perturbation techniques*, IEEE International Conference on Data Mining, 2003.