Abstract

Information age demands omnipresence of data. Large data sets are created, maintained and outsourced to the third party experts for data mining. Knowledge and patterns are extracted by using advanced data mining algorithms that assist the decision makers to ensure quick, correct and effective decisions to be made in this world of competition. The outsourcing of these large data sets faces the problem of theft and loss of ownership. The problem of data theft can be handled by fingerprinting i.e. embedding buyer specific marks along with ownership identification marks which further leads to the challenge of knowledge preservation. Thus, a technique which performs fingerprinting with knowledge preservation on numeric relational data to be outsourced is proposed here. It is ensured that the usability constraints are not violated. Knowledge preservation is achieved by optimizing the error to be inserted using Particle Swarm Optimization (PSO), a nature – inspired optimization algorithm. Collusion attack is very well-known in the context of fingerprinting techniques. Here, the proposed system provides a mechanism for avoiding collusion. The proposed system is independent of the primary key.
References


6. Radu Sion, Mikhail Atallah, Sunil Prabhakar "Rights Protection for Relational Data" IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 06, June 2004, pp. 1509-1525.


**Index Terms**

Computer Science  
Security

**Keywords**

Watermarking, Fingerprinting, Collusion, Knowledge preservation, Optimization.