International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

Data Recovery Using Reversible Watermark Technique

Mr.Bhausaheb C.Sanap[1],Mr.Vaibhav M.Pagare[2], Mr.Aditya A.Pardeshi[3], Mr.Udayraj P.Anwekar[4]

[1] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[2] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[3] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*
[4] *Sir Visvesvaraya Institute Of Technology, Department of Computer Engineering, Savitribai Phule Pune University Nashik, India*

Abstract - *Databases often contain vital information which is used for decision support sys-tem. Unauthorized changes to the data may have serious consequences and result in significant losses for the organization. Watermarking is a candidate solution that pro-tects databases shared with purposive receiver. Most of the study available in this field is focused on images, audio, video etc. The contribution of this work is to design and implement an intelligent watermarking technique for enforcing owner rights on relational databases. Proposed technique embeds the same watermark for different attributes at different places. Hence, it will difficult for an attacker to remove watermarks from the database. As relational database watermarking changes numeric data to some extent and this change in numeric data may lead to loss in knowledge of the data, proposed strategy causes minimum distortion in data and hence preserves the knowledge in data due to lesser information loss. We presents scheme for embedding and detecting water-mark in database relations without relying on primary keys. It can watermark relations that have no primary keys and is capable of retaining attribute values even if their primary keys are altered in attacks.*

Key Words: Knowledge preservation, Owner rights, Watermarking

1.INTRODUCTION

For calculation of an optimal watermark, the watermark preprocessing phase computes different parameters. For watermark encoding and decoding, these parameters are used. To embed watermark information in such a way that it does not affect the data quality, the main focus of watermark encoding phase. To the available bandwidth (or capacity) of the watermark information, during watermark embedding, data gets modified according. To ensure robustness but not so large that it destroys the data quality, The bandwidth of the watermark should be sufficiently large. To introduce tolerable distortion into the data, the data owner decides the amount of data modification such that the quality is not compromised for a particular database application before-hand and therefore defines usability constraints. MAGIC Gamma Telescope dataset and PAMAP2 Physical Activity Monitoring dataset, the datasets used in our research, are taken from UCI machine learning repository, including, Cleveland Heart Disease dataset. RRW is not dependent on any particular dataset or feature, it is to note that these datasets were used for evaluation purposes. Numerical features can be taken under consideration from any dataset and a suitable feature is determined to embed watermark on the basis of mutual information. to be insecure and termed as the “attacker channel” in this research domain, after watermarking, the data is released to the intended recipients over a communication channel that is assumed. The data may undergo several malicious attacks in the attacker channel. To subset insertion, alteration and deletion attacks, The efficiency and effectiveness of RRW is described through robustness analysis determined by its response. For detection of the embedded watermark, the Watermark decoding phase recovers watermark information effectively. The important task of successful recovery of the original data, data recovery phase mainly comprises. In subsequent sections, different phases of RRW are discussed.

2.OBJECTIVE

On the decision making process, Our focus is to develop an information model through a statistical measure that identifies such features that do not have a significant effect. Statistically measures the amount of information

that one feature contains about the other features in a database, mutual Information, a well known information theory. To select a suitable (candidate) feature from the database for watermarking, mutual information is used. Do not take into account the mutual information measure for determining relative importance of features, according to literature, existing reversible watermarking techniques. To compute the watermark information, the knowledge of mutual information for every candidate feature is also employed. Thus, it is ensured that the data quality will not be affected. Consequently, RRW provides a robust solution for data recovery that is reversible and resilient against heavy attacks.

3.LITERATURE SURVEY

For relational databases was proposed by Agrawal and Kiernan, the first irreversible watermarking technique. for relational databases was proposed, the first reversible watermarking scheme. For reversible watermarking of relational database, in this technique, histogram expansion is used. Proposed a method of distribution of error between two evenly distributed variables and selected some initial nonzero digits of errors to form histograms.

To reversibly watermark the selected nonzero initial digits of errors, histogram expansion technique is used. To authenticate data quality, this technique is keeps track of overhead information. However, this technique is not robust against heavy attacks.

Exploit methods of arithmetic operations on numeric features and perform transformations, difference expansion watermarking techniques. To minimize distortions. Whereas, in RRW, The watermark information is normally embedded in the LSB of features of relational databases. To protect the database from being tampered, another reversible watermarking technique proposed in is based on difference expansion and support vector regression (SVR) prediction. To provide ownership proof, the intention behind the design of these techniques. To modification attacks as any change in the expanded value will fail to detect watermark information and the original data, such techniques are vulnerable. In a proposed robust and reversible solution for relational databases, Genetic algorithm based on difference expansion watermarking (GADEW) technique is used. Increasing watermark capacity and lowering false positive rate, GADEW improves upon the drawbacks mentioned above by minimizing distortions in the data. To increase watermark capacity and minimize introduced distortion, To this end, a GA is employed. To search the optimum one for watermarking, this is because the watermark capacity increases with the increase in number of features and the GA runs on more features. In watermarked tuples, however, watermark capacity decreases with the increase. To control distortions in the resultant data, GADEW used the distortion measures. When AWD and TWD are given high values, the robustness of GADEW can be compromised. To select candidate pixels or features for embedding of watermark information, Prediction-error expansion watermarking techniques (PEEW) like incorporate a predictor as apposed to a difference operator. As the watermark information is embedded in the fractional part of numeric features only, the PEEW proposed technique by Farfoura and Horng is fragile against malicious attacks. To preserve the usefulness of the data, in this particular scenario, the scheme works because the intention of the attacker. He can easily compromise the fractional part. RRW is robust, as the watermark information is embedded in the values of numeric features, to make the scheme resilient against such attacks.

Architecture Diagram

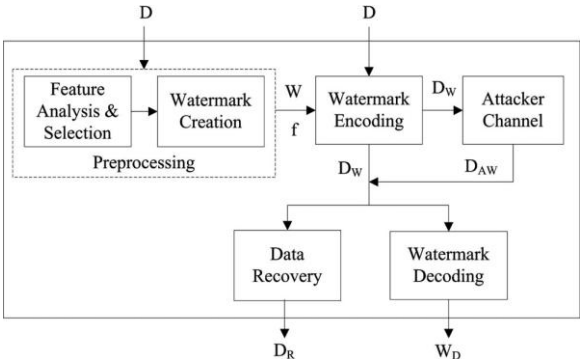

Fig -1: Basic Watermarking Technique

4. CONCLUSIONS AND FUTURE WORK

In this paper, we reviewed different techniques on watermarking relational databases that embeds the watermark bits in database set by partitioning it. Every author worked for the robustness of the technique. Many watermarking techniques are based on different watermark information, most of these techniques are

designed for numerical database and are distortion based. There are almost similar steps to identify attribute then tuple and then marking position for the watermark. Finally, we observe that usability of the watermarked database and deterministic detectability leaves so many queries in mind for future research. Most of these techniques used a single attribute of a tuple to embed a watermark. So, this work will be extended towards embedding the same watermark at different attributes at different places. Therefore, it will be difficult for attacker to remove watermarks from different places from the database. Most of these techniques are also depend on presence of primary key. So we will also extend the work to find solution if there is no primary key.

REFERENCES

1. *Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, "A method for trust management in cloud computing: Data coloring by cloud watermarking," Int. J. Autom. Comput., vol. 8, no. 3, pp. 280–285, 2011.*
2. (2012, Feb. 4).Walmart to start sharing its sales data. [Online]. Available: http://nypost.com/p/news/business/walmart-opens-up
3. I. Cox, M. Miller, J. Bloom, and M. Miller, Digital Watermarking. Burlington, MA, USA: Morgan Kaufmann, 2001.
4. (2012, Feb. 4).Walmart to start sharing its sales data. [Online]. Available: http://nypost.com/p/news/business/walmart-opens-up
5. P. W. Wong, "A public key watermark for image verification and authentication," in Proc. IEEE Int. Conf. Image Process., 1998, vol. 1, pp. 455–459.