International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-2, December 2011

Compression of Watermarked Relational Database for Security and Optimization of Storage Consumption

Abha Tamrakar, Vinti Nanda

Abstract— Today's competitive world demands speed. If we are slow then we will be a loser. Providing security speedily is the aim of this paper. Relational database are very important for satisfying today's informational needs. More crucial phase is preventing its ownership rights. In earlier existing system security was provided by sending the encrypted relational database to the client system without compressing its size hence doesn't increases the speed of transfer rate. To overcome this limitation we are using compression technique which will provide security as well increases the speed of data transfer between clients to server system.

Keywords-Compression, ownership rights, Speed, watermarked relational data.

I. INTRODUCTION

The rapidly growing internet and related technologies has offered an unprecedented accessibility and redistribution of digital contents. . Proving ownership rights is very difficult especially in case of internet and related applications. The concept of watermarking is about several hundred years ago. The idea of digital watermarking is to embed a small amount of secret information –the water mark into host digital production such as image, audio, relational database so that it can be extracted later for the purpose of copyright assertion, authentication and content integrity verification. Digital watermarks are usually invisible to human eyes and can be detected by specially designed detector. The difference between watermarking and cryptography is that cryptography provides no protection after the content is decrypted, digital watermarking become inseparable constituent after embedding. Because of these characteristics, digital watermarking requires no secret channel for communicating the digital signature that cryptography does. So in the last decade, digital watermarking has attracted numerous attentions among researchers and is regarded as a promising technique in the field of information security.

Manuscript published on 30 December 2011.
***** Correspondence Author (s)
Abha Tamrakar*, Department of Computer Science and Engineering, Chhattisgarh Swami Vivekananda Technical University, Raipur, India, 09993844951, (e-mail: tamrakar.abha@gamil.com).
Vinti Nanda, Department of Computer Science and Engineering, Chhatrapati Shivaji I nstitute of Technology, Bhilai, India, 09907142531., (e-mail: vintinanda@csitdurg.in).

Various types of watermarking schemes have been developed for different application. According to their nature, digital watermarking schemes could be classified into three categories: fragile watermarking, semi-fragile watermarking and robust watermarking. The main difference between fragile and semi fragile watermarking is that semi-fragile watermarking is tolerant to non-malicious attack such as lossy compression while fragile watermarking is intolerant to many manipulations. Robust watermarking on the other hand is indented for application of copyright protection. Ours watermarking approach is robust watermarking where in watermarks should survive attacks aiming at weakening or erasing the attack.

In contrast to it the problem of watermarking relational data has not been given appropriate
attention.
The main steps in our approach are Table Partitioning, Watermark Embedding, Compression, Decompression, Watermark Detection, and Reverse Partitioning.
The first three steps are the part of server side.

- During table partitioning step the table is partitioned on the basis of column. Each column contains one row of the table.
- During step of watermark embedding the watermarked bits as per the owners convenience is embedded into the relational database table so that the changes that will be made after embedment of the bits in the table is acceptable as per single bit encoding algorithm criteria.
- In the third step watermarked embedded table serve as a input and on that input OLTP table compression algorithm given by Oracle 11g is applied.

The next three steps are performed at the receiver side.

- In the next step compressed watermarked relational table serve as a input and on that input OLTP table decompression algorithm is applied.
- During this step of watermark detection the watermarked bits is detected into the relational database table by single bit decoding algorithm criteria.
- During reverse table partitioning step the table is unpartitioned so as to get original final table.

In earlier existing system security was provided by sending the encrypted watermarked relational database to the client system without compressing its size hence reducing the speed of transfer rate between client and server system. To overcome

this limitation we use compression technique which will provide security as well increases the transfer rate.

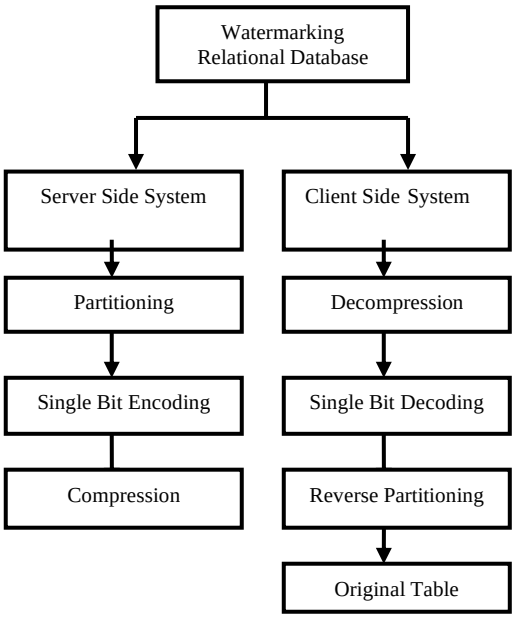

Fig 1.Block Diagram of Proposed System

II. LITERATURE REVIEW

Fernando Perez-Gonzalez and Juan R. Hernandez, [10] proposed a mechanism that was resilient or insensitive to additive attacks,to embed and detect watermark in relational database. In additive attack the attacker simply inserts his/her own watermark in original data. In their proposed system they can draw graphs and original ownership claim can be resolved by locating the overlapping regions of the two watermarks in which the bit values of the marks conflict and determining which owner's mark win.

M. Atallah and S. Lonardi[7] proposed a system, in which a simple variation on the classic LZ-77 algorithm that allows one to hide, within the compressed document, enough information to warrant its authenticity and integrity. The design is based on the unpredictability of a certain class of pseudo-random number generators, in such a way that the hidden data cannot be retrieved in a reasonable amount of time by an attacker (unless the secret bit-string key is known).

Agrawal[8] proposed a watermarking algorithm that embeds the watermark bits in the least significant bits (LSB) of selected attributes of a selected subset of tuples. This technique does not provide a mechanism for multibit watermarks; instead only a secret key is used. For each tuple, a secure message authenticated code (MAC) is computed using the secret key and the tuples primary key. The computed MAC is used to select candidate tuples, attributes and the LSB position in the selected attributes. Hiding bits in LSB is efficient. However, the watermark can be easily compromised by very trivial attacks. (2003).

Gross-Amblard[4] proposed a watermarking technique for XML documents and theoretically investigates links between query result preservation and acceptable watermarking alterations. Another interesting related research effort is to be found in where the authors have proposed a fragile watermark technique to detect and localize alterations made to a database relation with categorical attributes (2003).

Radu Sion[3] proposed a watermarking technique that embeds watermark bits in the data statistics. The data partitioning technique used is based on the use of special marker tuples which makes it vulnerable to watermark synchronization errors resulting from tuple deletion and tuple insertion; thus such technique is not resilient to deletion and insertion attacks. Furthermore, R. Sion recommend storing the marker tuples to enable the decoder to accurately reconstruct the underlying partitions; however this violates the blinded watermark detection property. The data manipulation technique used to change the data statistics does not systematically investigate the feasible region; instead a naive unstructured technique is used which does not make use of the feasible alterations that could be performed on the data without affecting its usability. (2004).

Wilfred Ng and Ho-Lam Lau[6], "Effective Approaches for Watermarking XML Data. presented two different watermarking schemes on XML data: the selective approach and the compression approach. The former technique embedded non-destructive hidden information content over XML data. The latter takes verbosity and the need in updating XML data in real life into account. We conduct experiments on the efficiency and robustness of both approaches against different forms of attack, which shows that our proposed watermarking schemes are reasonably efficient and effective (2005).

Yingjiu Li, Vipin Swarup, and Sushil Jajodia[2] presented a technique for fingerprinting relational data by extending Agrawal watermarking scheme.The primary new capability provided by their scheme is that, under reasonable assumptions, it can embed and detect arbitrary bit-string marks in relations. This capability, which is not provided by prior techniques, permits their scheme to be used as a fingerprinting scheme and then presented quantitative models of the robustness properties of our scheme. These models demonstrate that fingerprints embedded by our scheme are detectable and robust against a wide variety of attacks including collusion attacks (2005).

Ms. Arti Deshpande and Mr. Jayant Gadge[5] presented a mechanism that is resilient or insensitive to additive attacks, how to embed and detect watermark in relational database. In additive attack the attacker simply inserts his/her own watermark in original data. In their proposed system one can draw graphs and original ownership claim can be resolved by locating the overlapping regions of the two watermarks in which the bit values of the marks conflict and determining which owner's mark win. The attacker must have inserted the watermark later. Clearly having more marked tuples increases collisions and hence we can easily identify the owner of the data (2009).

Nagarjuna. Settipalli, R Manjula[1] proposed a paper "Watermarking Relational Databases Using Optimization-Based Techniques .According to him in earlier existing systems the relational data will be watermarked and directly send to the client system, in these systems while sending relational data from server to client attacker easily copy the data and create same copy of relational data. Here there is no security to watermarked relational data. In their proposed system before sending the watermarked relational data to client side he encrypted the relational data and send it to the client side, at client side decryption will be done to get

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

the original watermarked data. Because of using this encryption technique even an attacker copy the data he/she may not read the watermarked relational data (2011).

But the problem with the above paper is that though encryption algorithm provides security but didn't speaks anything about reduction in storage space of watermarked relational data as well about the transfer time of data between sender and receiver. To overcome this problem we have introduced the concept of compression technique which indulges security as well as optimizes storage space.

III. Our Approach

In my approach I have used compression algorithm which provides security and reduces transfer time of watermarked relational data between sender and receiver system.

A. The following steps are involved in my approach:-

a. Data Set Partitioning: In this module the data set is partitioned into number of non-overlapping partitions.

b. Watermark embedding: In this module the bits are embedded by using single bit encoding.

c. Compression: The OLTP table compression algorithm given by Oracle 11g is for compressing the relational database table

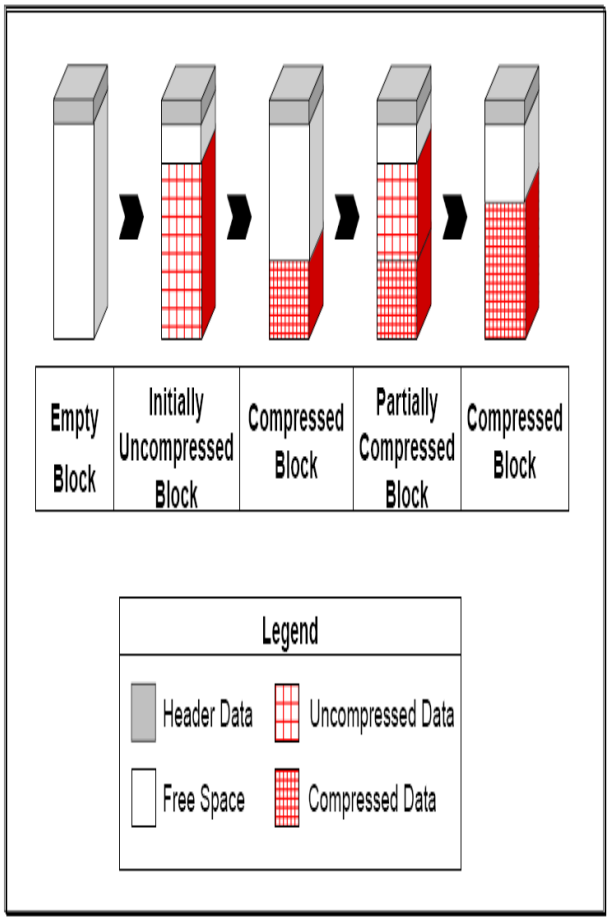

Fig 2.Steps Involved in compression Process

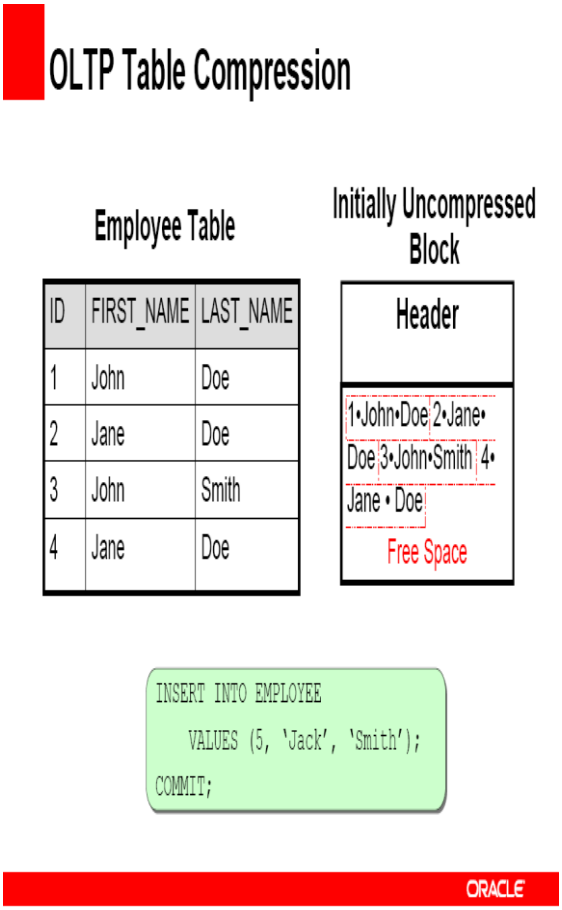

Fig 3.OLTP Table Compression Technique

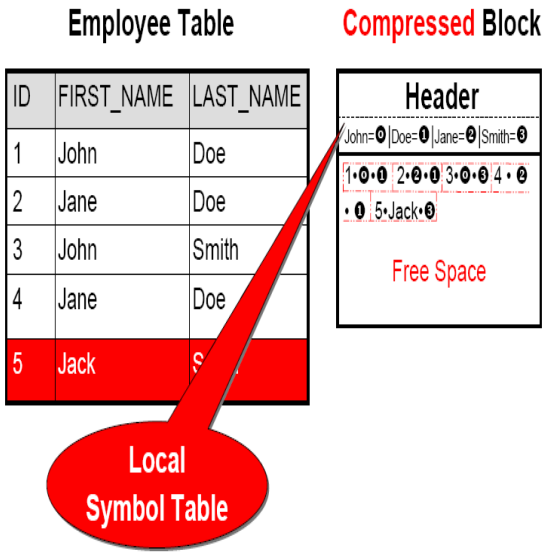

Fig 4.Free Space available after applying OLTP

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table Compression Algorithm

Algorithm for OLTP Table Compression

1. *Read the relational database to be compressed.*
2. *Initialize line=first tuple of the table*
3. *while (line!=null)*
4. *{*
5. *a. variable word=different tokens in each line.*
6. *b .while (word has more tokens)*
7. *{add each token in iterator Set}*
8. *}*
9. *Close the table.*
10. *Open the intermediate table.*
11. *Store the distinct words in intermediate table.*
12. *Close the intermediate table.*
13. *Open the original table to be compressed*
14. *Line=read the first tuple.*
15. *Open the output table which is the compressed table.*
16. *While (line! =null)*
    {
    Word=obtain different tokens
    While (tokens are not over)
    {Open the intermediate table which contains one word per line.
    Compare word with each line (word) in Intermediate table
    if (word =line)
    place the corresponding word no. (line no.) of the intermediate table in the compressed output table.
    end if}
    line=read next tuple
    }
17. *Close all the tables*

Fig 5. Algorithm for OLTP Table Compression

A. The advantages of OLTP Table Compression Algorithm is:

•Structured/Relational data Compression.
•Unstructured data compression
•Compression for backup data
•Network transport compression
•Reduces resource requirements and costs.
•Storage System
•Network Bandwidth
•Memory Usage

IV CONCLUSION

The compression technique used in our approach secures as well as compresses the watermarked relational database which provides security as well as optimizes storage consumption which in turn reduces transfer time of data between sender and receiver. In the previous systems the task of compression was not performed, and directly send it to the client side system so here the concept of optimization of storage consumption was not fullfilled.This drawback is removed in our compression approach.

ACKNOWLEDGEMENT

I would like to thank Ms Vinti Nanda, Asst. Professor in Csit, Durg (C.G). Secondly I would also like to express my sincere thanks to Mrs. Tripti Sharma, Head of department of Computing Science and Engineering, Csit, Durg(C.G) for her continuous efforts in encouraging and guiding us to become successful engineers

REFERENCES

1. N.Settipalli, R Manjula, ‘‘Securing Watermarked relational
2. Encryption and Decryption” ARPN Journal Vol. 1,pp. 70-74, May 2011.
3. Y. Li, V. Swarup, and S. Jajodia, “Fingerprinting Relational Databases: Schemes and Specialties.” Vol. no. 2, pp. 456-460, March 2005.
4. R. Sion, M. Atallah, and S.Prabhkar, “Right Protection for Relational Data.” IEEE Trans. Knowledge and Data Engineering, Vol. 16 no.6, June 2004.
5. D. Gross-Amblard, “Query-Preserving Watermarking of Relational Databases and XMLDocuments.” In PODS ‘03: Proceedings of the 22nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, pp. 191-201. ACM Press, 2003.
6. A. Deshpande, J. Gadge, “New Watermarking Technique for Relational Databases.” Department of Computer Engineering, Thadomal Shahani Engineering College, Mumbai, ICETET-2009.
7. W. Ng and H. Lau, “Effective Approaches for Watermarking XML Data.” Department of Computer Science, the Hong Kong University of Science and Technology, Hong Kong, 2005.
8. M. Atallah and S. Lonardi. “Authentication of LZ-77 Compressed Data.” In Proceedings of the ACM Symposium on Applied Computing, Florida, USA, 2003.
9. R. Agrawal, J. Kiernan, “Watermarking Relational Databases.” IBM Almaden Research Center, china, 2002.
10. F. P. Gonzalez and J. R. Hernandez, “A Tutorial on Digital Watermarking.” Dept. Tecnologıas de las Communications, ETSI Telecom., Universidad de Vigo, Spain, 1999.
11. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on Copyright Marking System.” Notes in Computer Science, Portland, Oregon, USA, 14 17 April, 1998.

AUTHOR PROFILE

ABHA TAMRAKAR: I received my B.E in Computer Science and Engineering from Shri Shankaracharya College of Engineering and Technology of Chhattisgarh State, India in 2009. I am now Pursuing my M.Tech at Chhattrapati Shivaji Institute of Technology State, India. My area of interest includes watermarking, security, image processing.

VINTI NANDA: She received her M-TECH in Computer Science and Engineering from Rungta College of Engineering and Technology of Chhattisgarh State, India in 2010.She received her B.E in Computer Science and Engineering from Shri Shankaracharya College of Engineering and Technology of Chhattisgarh State, India in 2005.She is working as Asst. Professor in Chhattrapati Shivaji Institute of Technology(CSIT), DURG(C.G).

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)