ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016

A NEW WATERMARKING APPROACH FOR RELATIONAL DATA

A.Usha Nandhini,M.Phil Final Year,
Department of Computer Science,
Mother Teresa University,
Chennai- 15

Dr.Mrs.R.Janaki,MCA.,M.Phil.,Ph.D.,
Assistant Professor
Department of Computer Science,
Queen Mary's College (A),
Chennai-600 004

Abstract— the hurried hike of the net and connected technologies has offered a new ability to access and spread digital contents. In such a context, executing information possession is a very important demand, which needs articulated solutions, surrounding technical, structure, and legal aspects. Though we have a tendency to square measure still far away from such comprehensive solutions, within the last years, watermarking techniques have occurred as a very important building block that plays an important role in addressing the tenure downside. Such techniques permit the owner of the info to enter an un hearable watermark into the info. A watermark defines info which will be used to prove the possession of knowledge like the owner, origin, or recipient of the content. Secure embedding needs that the embedded watermark should not be simply tampered with, forged, or aloof from the watermarked information. Watermarking techniques are established for video, images, audio, and text information and additionally for package and tongue text. Watermark implanting for relative information is formed potential by the very fact that real information will fairly often tolerate a little quantity of error with none vital deprivation with relation to their usability. In explicit, our projected technique is resilient to tuple deletion, alteration, and insertion

Key words: Watermarking, relational database, information security, ontology.

I. INTRODUCTION

The rapid evolution of the Internet and related technologies has offered an extraordinary ability to access and reallocate digital contents. In such a context, imposing data ownership is an important requirement, which requires articulated solutions, surrounding technical, organizational, and legal aspects. Although we are still far from such comprehensive resolutions, in the last years, watermarking techniques have developed as an important building block that plays a crucial role in addressing the tenure problem. Such techniques allow the owner of the data to embed an undetectable watermark into the data. A watermark defines information that can be used to prove the tenure of data such as the owner, origin, or receiver of the content. Secure implanting requires that the embedded watermark must not be easily obstructed with, fake, or removed from the watermarked data. Imperceptible embedding means that the presence of the watermark is unremarkable in the data.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016

EXISTING SYSTEM

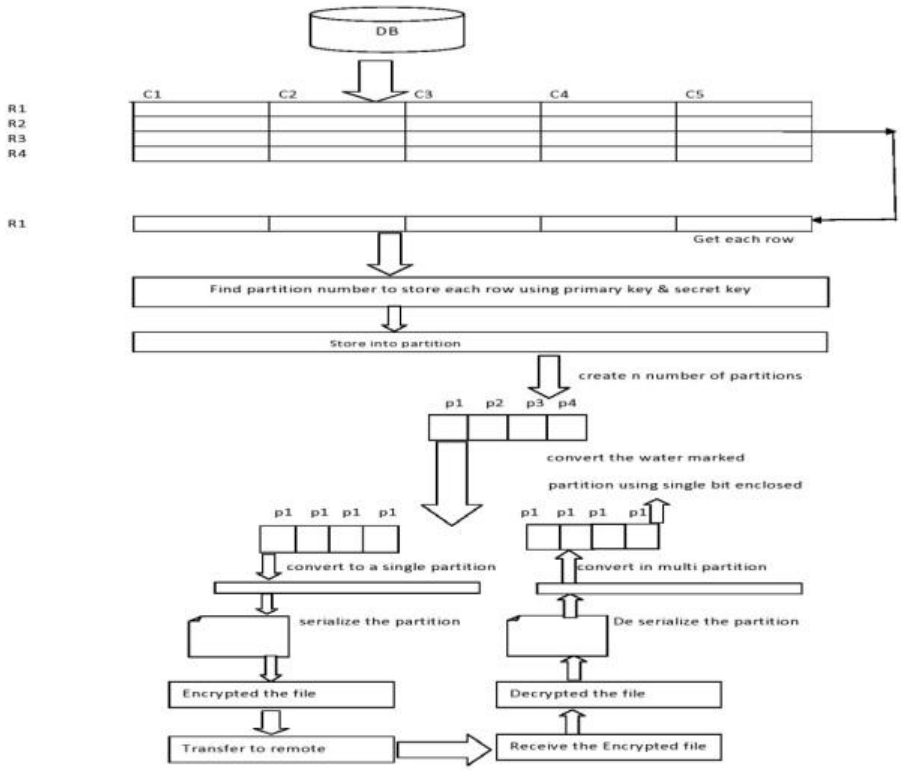
Watermarking in least noteworthy bits(LSB).This technique implants the watermark bits in the least significant bits of selected qualities of a selected subset of tuple's. It uses secret key in watermarking. For each tuple's a safe message, authentic code is calculated using the top-secret key and tuple's primary key. The computed MAC is used select candidate tuple's attributes and the LSB places in the designated attributes.

PROPOSED DESIGN:

In this paper, we lecture the original problem of strongly transmitting provenance for data streams using MD5 algorithm. Then we encode the segregated data using Triple DES algorithm. Least Significant Bit (LSB) Single Bit Encoding is used for Encrypting process. Data set will make Divider and group for programming for dispensation However, unlike outdated watermarking approaches, we implant provenance over the inter packet delays (IPDs) it escapes the problematic of data degradation due to watermarking. We propose a spread-spectrum watermarking-based solution that embeds derivation over the inter packet delays. The security features of the system make it able to survive against various networks or flow watermarking attacks

Watermarking implants ownership information in digital content. Watermark defines information that can be used to prove the proprietorship of relational database. Here the embedding is hidden that the presence of watermarking is invisible to the user.

System Architecture:



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016

Technique Explanation

The technique used to partition the data is based on message authentication code (MAC) using cryptographic hash function Message Digest 5 (MD5). This algorithm is similar to the algorithm proposed by Mohamed Shehab, only MD5 is used as cryptographic hash function. The data partitioning algorithm that partitions the data set based on secret key Ks. The data set D is a database relation with scheme D(P,A0,A1…….Av-1) where P is the primary key attribute, A0,A1…….Av-1 are v attributes which are candidates for watermarking, and |D| is the number of tuples in D. The data set D is to be partitioned into m non overlapping partitions, namely, {S0; . . . ; Sm-1}, such that each partition Si contains on the average |D| / m tuples approx. from the data set D. Partitions do not overlap, that is, for any two partitions Si and Sj such that i □ j ,we have Si □ Sj = { }. For each tuple r € D, the data partitioning algorithm computes a MAC (Message Authentication Code), which is considered to be secure cryptographic hash function.

MODULES

1) Data Partitioning

Data partitioning in social data warehouse can applied by objects partitioning of base tables, clustered and non-clustered indexes, and index views. Range dividers refer to table partitions which are defined by a customizable range of data. The conclusion manipulator or database administrator can define the divider function with boundary values, partition scheme having file cluster mappings and table which are mapped to the partition scheme. By using Watercourse the data set is separated into several non-overlapping partitions**.** Christo Ananth et al. [10] proposed a system in which the complex parallelism technique is used to involve the processing of Substitution Byte, Shift Row, Mix Column and Add Round Key.

2) Watermark Embedding

A watermark bit is entrenched in each divider by Single Bit Encoding algorithm. Watermarking is a technology for implanting various types of information in digital content. In general, evidence for protecting copyrights and showing the cogency of data is embedded as a watermark. Watermarks are added to images or audial data in such a way that they are invisible or imperceptible unidentifiable by human eye or ear. Furthermore, they can be entrenched in content with a diversity of file formats. Watermarking is the content guard method for the multimedia era.

3) Optimal Threshold Evaluation:

The bit implanting statistics are used to compute the ideal threshold that minimizes the possibility of decoding error. The optimization technique used in this research is pattern search technique (PS). PS methods are straight search methods for non-linear optimization. It starts at an early point and samples the impartial function at a prearranged design of points centered about that point with the goal of generating a new better iterate

4) Dataset Partitioning:

By using the data partitioning algorithm, the data partitions are engendered from watermarked dataset**.**

5) Threshold Based Decoding:

The statistics of each divider are evaluated, and the entrenched is decoded using a threshold based scheme based on the optimal threshold. The probability of bit decrypting error is denied as the probability of an embedded bit decrypted incorrectly. The deciphering threshold T_ is

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016

nominated such that it minimizes the possibility of decoding error. The bit embedding stage is based on the enlargement or minimization of the tail count; these optimized hiding function values computed during the programming stage are used to compute the optimum threshold T.

CONCLUSION:

In this project, we have presented a resilient watermarking technique for relational data that embeds watermark bits in the data statistics. The watermarking problem was articulated as a constrained optimization problem that maximizes or diminishes a whacking function based on the bit to be embedded. GA and PS techniques were employed to solve the proposed optimization problem and to handle the restraints. Furthermore, we presented a data partitioning technique that does not be contingent on special marker tuples to locate the partitions and proved its resilience to watermark synchronization errors. We established an efficient threshold-based technique for watermark detection that is based on an optimal threshold that diminishes the possibility of decoding error. The watermark flexibility was improved by the repeated embedding of the watermark and using mainstream voting technique in the watermark decoding phase. Moreover, the watermark resilience was amended by using numerous attributes.

A proof of concept implementation of our watermarking technique was used to conduct experiments using both synthetic and real-world data. A evaluation our watermarking technique with previously posed techniques shows the dominance of our technique to deletion, alteration, and insertion attacks.

REFERENCE

[1] R. Agrawal and J. Kiernan, "Watermarking Relational Databases,"Proc. 28th Int'l Conf. Very Large Data Bases, 2002.

[2] M. Atallah and S. Lonardi, "Authentication of LZ-77 Compressed Data," Proc. ACM Symp. Applied Computing, 2003

[3] M. Atallah, V. Raskin, C. Hempelman, M. Karahan, R. Sion, K. Triezenberg, and U. Topkara, "Natural Language Watermarking and Tamperproofing," Proc. Fifth Int'l Information Hiding Workshop,
2002.

[4] G. Box, "Evolutionary Operation: A Method for Increasing Industrial Productivity," Applied Statistics, vol. 6, no. 2, pp. 81-101, 1957.

[5] E. Chong and S. Z_ ak, An Introduction to Optimization. John
Wiley & Sons, 2001.

[6] D. Coley, "Introduction to Genetic Algorithms for Scientists and Engineers," World Scientific, 1999.

[7] C. Collberg and C. Thomborson, "Software Watermarking: Models and Dynamic Embeddings," Proc. 26th ACM SIGPLANSIGACT Symp. Principles of Programming Languages, Jan. 1999.

[8] I. Cox, J. Bloom, and M. Miller, Digital Watermarking. Morgan Kaufmann, 2001.

[9] E. Dolan, R. Lewis, and V. Torczon, "On the Local Convergence of Pattern Search," SIAM J. Optimization, vol. 14, no. 2, pp. 567-583,
2003.

[10] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016

[11] D. Gross-Amblard, "Query-Preserving Watermarking of Relational Databases and XML Documents," Proc. 22nd ACM SIGMOD-SIGACT-SIGART Symp. Principles of Database Systems (PODS '03), pp. 191-201, 2003