ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Implementation of Reversible Watermarking Techniques on Relational Database

Jaishri Chaudhari [1],Nilesh Chaudhari[2]

P.G. Student, Department of Computer Engg., Godavari College of Engg, Jalgaon, Maharashtra, India[1]

Associate Professor, Department of Computer Engg., Godavari College of Engg, Jalgaon, Maharashtra, India[2]

ABSTRACT: A reversible watermarking scheme for relational databases is proposed in this paper to achieve lossless and exact authentication of relational databases via expansion on data error histogram. This reversible watermarking scheme possesses the ability of perfect restoration of the original attribute data from the untampered watermarked relational databases, thus guaranteeing a "clear and exact" tampered-or-not authentication without worry about causing any permanent distortion to the database. In this scenario, only the secret key owner possesses the capability to exactly restore the database's original state. Simulations demonstrate the scheme's security and feasibility for low-correlated data in typical databases

KEYWORDS: reversible watermarking, security to relational database.

I. INTRODUCTION

In recent times, a large amount of data is generated because of growth of internet and cloud computing[1]. Availability of data is in various formats. Reversible Watermarking techniques allows data recovery and provides ownership protection.it provides the ownership protection by marking format such as images, audio, and relational databases .A large number of organizations today have relational database and their security is of utmost importance. Reversible Watermarking techniques allows enforcement of ownership rights and prevents data from being tampered. As data is available in various formats out of which relational data is structured which is difficult to retrieve as compared to multimedia data. Some primitive techniques were use such as Cryptography, Fingerprinting, and Steganography. These techniques however are not robust however achieving robustness is a very difficult task for these reversible watermarking technique is used .Some of the earlier watermarking techniques are as follows:-Histogram Techniques Problem:-In that system firstly Histogram technique is used. But at time of heavy attack this technique is fully exposed. In histogram, by considering a method of distribution of error between two distributed variables and selected some initial nonzero digits of errors to form histograms. For authenticating data quality, Histogram technique is keep track of overhead information. Histogram technique is not robust against heavy attacks.. Reversible watermarking technique prevents data quality from getting degraded. Difference Expansion Watermarking Technique. : This technique is better than Histogram technique, but also having some drawbacks. This technique exploits methods of arithmetic operations on numeric features and performs transformations[3]. The watermark information is normally grouped in the Least Significant Bite of features of relational databases to minimize distortions. . But, in RRW, a GA based optimum value is embedded in the selected feature of the dataset with the objective of preserving the information and data quality while reducing the data distortions as a result of watermark embedding. Another reversible watermarking technique considered is depend on difference expansion and support vector regression (SVR) prediction to protect the database from being tampered. This technique is similar only exception as Difference Expansion, only difference is that it uses support vector regression. The design of these techniques is to provide and ensure ownership proof. Such watermark techniques are vulnerable to modification attacks as any change or modification in the expanded value will not able to detect watermark information and the original data. This technique is not able to recover original data. Technique used to solve problem:- System is not able to work correctly in heavy attacks. Also fail to detect watermark information and the original data. In order to overcome these problems, A difference expansion watermarking technique is used which

DOI: 10.15680/IJIRCCE.2018. 0612038

is based upon genetic algorithm. This is proposed reversible and robust solution for database. This technique improves upon the drawbacks mentioned above by minimizing distortions in the data,and increasing watermark capacity .

The remainder of the paper is organized as follows. Section 3 presents the context aware in ICN. The message delivery probability with context aware is evaluated in Section 4. Finally, some conclusions are given in Section 5.

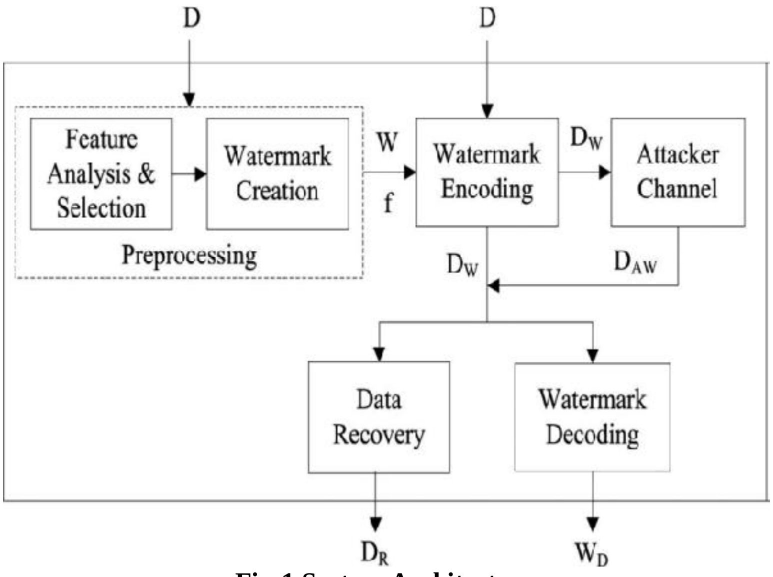

Fig:1 System Architecture

II. RELATED WORK

WATERMARKING RELATIONAL DATABASE

The basic database watermarking technique of relational databases is shown in Figure 1. Watermark embedding phase includes a private key K (known only to the owner) which is used to embed the watermark bits into the original database to form watermarked database. The watermarked database is then made publicly available. To verify the right ownership of a doubtful database, the verification process is performed. In this process the mistrustful database is taken as input and by using the private key K which is used during the embedding phase, the embedded watermark (if present) is extracted from watermarked database and it is compared with the original watermark information.

The watermarked database must preserve the following properties:

Robustness: Watermarking process should be robust against different types of malicious attacks. The watermarking algorithm should be developed in such a way that it should be difficult for an attacker to delete or alter the watermark from database without violating the knowledge of the data.

Usability: Watermarking technique should not results in distortion of data and knowledge in the databases should be preserved. i.e. Data should be useful after watermark embedding process.

Blindness: Watermark extraction should not require the knowledge of the original database and watermark itself.

Security: Watermarked tuples, attributes, bit positions that are selected for embedding watermark bits should be kept secret and it should be only known by having the knowledge of a secret-key. (i.e. Owner of the database)

III. PROPOSED METHODOLOGY

The architecture of RRW is shown in Fig. 1. RRW includes the following four major phases:

(1) watermark preprocessing;

(2) watermark encoding;

(3) watermark decoding; and

DOI: 10.15680/IJIRCCE.2018. 0612038

(4) data recovery.

WatermarkPre-processing Phase
In the pre-processing phase, two important tasks are accomplished:
(1) selection of a suitable feature for watermark embedding;
(2) calculation of an optimal watermark.

Watermark Encoding Algorithm:
Input: Database, watermark string, β
Output: Watermarked database, matrix
1. For all watermark bits 1 to length l
2. For all the tuples of the data
3. If watermark bit is 0, then compute changes using equation (1).
4. Watermark data using equation (3).
5. Insert ηr into the matrix.
6. End if.
7. If watermark bit is 1, then compute changes using equation (1).
8. Watermark data using equation (2).
9. Insert ηr into the matrix.
10. End if
11. End For
12. End For

Watermark Decoding
The Watermark decoding phase recovers watermark information effectively for detection of the embedded watermark. In this phase the percent change in the watermarked data is calculated using equation (4). After this, the difference between the original data change and the watermark detected change amount is calculated using equation (5). Final watermark information is retrieved through a majority voting scheme using Equation

$$\eta dr = D'W * \zeta$$

$$\eta \Delta r = \eta dr - \eta r$$

$$WD \leftarrow mode(dtW(1,2,\ldots..,l))$$

Watermark Decoding Algorithm:
Input: Watermarked Database, matrix containing change in the data values, length of watermark string
Output: Decoded Watermark
1) For all tuples of the watermarked data
2) For all watermark bits b from 1 to length l of the watermark
3) Compute percent change in the watermarked data using equation (4)
4) Compute the difference between original data change amount and the watermark detected change amount using equation (5)
5) If difference computed using equation (4) ≤ 0
6) Detected Watermark bit is 1
7) Else if difference is > 0 and ≤ 1
8) Detected Watermark bit is 0
9) End If
10) End For
11) End For
12) Compute final watermark string using equation (6)

Watermark Recovery

After detecting the watermark string, some post processing steps are carried out for error correction and data recovery. The main responsibility of post-processing is to use the decoded watermark bits, and convert these bits into the watermark information that was embedded as the watermark. If the detected watermark bit is 0, the data is recovered using equation (7). If detected watermark bit is 1, then data is recovered using equation

Performance Evaluation

For Performance evaluation of the approach we measure it based on 2 parameters i.e precision and recall . Precision and Recall are defined in terms of a set of retrieved documents (e.g. the list of documents produced for a query) and a set of relevant documents (e.g. the list of all documents that are relevant for a certain topic)

Total Relevant	Retrieved	Relevant Retrieved	Precision	Recall	F-Measure
25	24	23	95.83	92	93.87
50	49	45	91.83	90	90.90
75	74	71	95.94	94.66	95.30
100	98	93	94.89	93	93.93
200	197	188	95.43	94	94.71

Table 1: Results

Above Table 1 shows the relevant data retrieved, total relevant and total retrieved which will eventually help to generate precision, recall and f-measure calculation.

Precision :

Precision is the fraction of retrieved documents that are relevant to the find.

$$\text{precision} = \frac{|\{\text{relevant documents}\} \cap \{\text{retrieved documents}\}|}{|\{\text{retrieved documents}\}|}$$

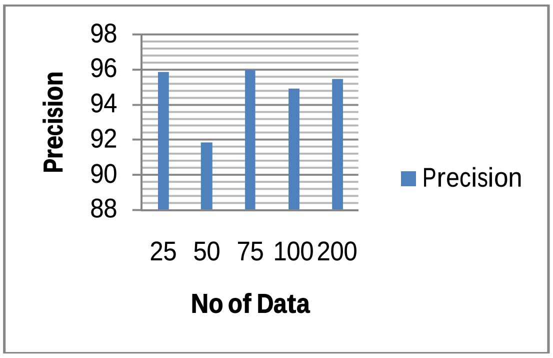

Fig 2: Precision

Recall :

Recall in information retrieval is the fraction of the documents that are relevant to the query that are successfully retrieved.

$$\text{recall} = \frac{|\{\text{relevant documents}\} \cap \{\text{retrieved documents}\}|}{|\{\text{relevant documents}\}|}$$

DOI: 10.15680/IJIRCCE.2018. 0612038

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

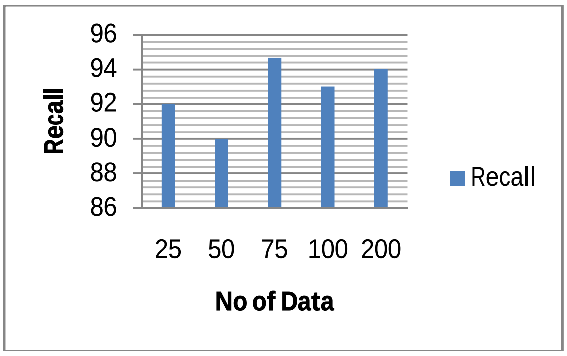

Fig 3: Recall

F-Measure:-

F-Measure is generated from precision and recall.

F-Measure= 2*precision * recall / (precision + recall);

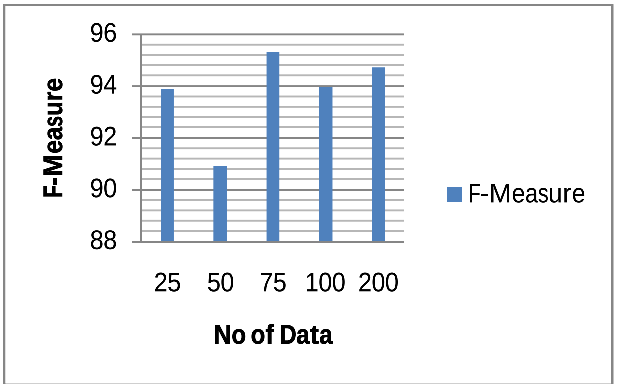

Fig 4: F-Measure

IV. CONCLUSION

Irreversible watermarking techniques make changes in the data to such an extent that data quality gets compromised. Reversible watermarking techniques are used to cater to such scenarios because they are able to recover original data from watermarked data and ensure data quality to some extent. However, these techniques are not robust against malicious attacks—particularly those techniques that target some selected tuples for watermarking. In this paper, we presented a new approach to watermark a non- numeric attribute in the relational database. This algorithm can be used effectively where a huge amount of relational data is transferred between owner and authenticated users. Out experiment results proved that the system is highly efficient and having high accuracy and performance. One of our future concerns is to watermark shared databases in distributed environments where different members share their data in various proportions. A robust and distortion free watermarking technique has been proposed that is capable of recovering the original data. It allows recovery of large amount of the data and embedded watermark even after being subjected to malicious attacks

DOI: 10.15680/IJIRCCE.2018. 0612038

REFERENCES

[1] Saman Iftikhar, M. Kamran, and Zahid Anwar, "RRW—A Robust and Reversible Watermarking Technique for Relational Data" , IEEE Transactions On Knowledge And Data Engineering, Vol. 27, No. 4, APRIL 2015.

[2] Udai Pratap Rao, Dhiren R. Patel, Punitkumar M. Vikani, "Relational Database Watermarking for Ownership Protection", 2nd International Conference on Communication, Computing & Security [ICCCS-2012]

[3] G.Shyamala, I.Jasmine Selvakumari Jeya, M.Revathi, "Secure and Reliable Watermarking in Relational Databases", *International Journal of Computer Trends and Technology (IJCTT) – volume 11 number 1 – May 2014*

[4] Jun Ziang Pinn and A. Fr. Zung, "A new watermarking technique for secure database", International Journal of Computer Engineering & Applications, Vol. I, No. I

[5] Theodoros Tzouramanis,"A Robust Watermarking Scheme for Relational Databases", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates 2011 IEEE

[6] G. Shymala, C. Kanimozhi, S. P. KAVYA, "An Efficient Distortion Minimizing Technique for Watermarking Relational Databases", International journal of scientific research and Technology research, Vol.04,Issue.11,May-2015

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[8] I. Cox, M. Miller, J. Bloom, and M. Miller, "Digital Watermarking".Burlington, MA, USA: Morgan Kaufmann, 2001.