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

Survey on 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 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.

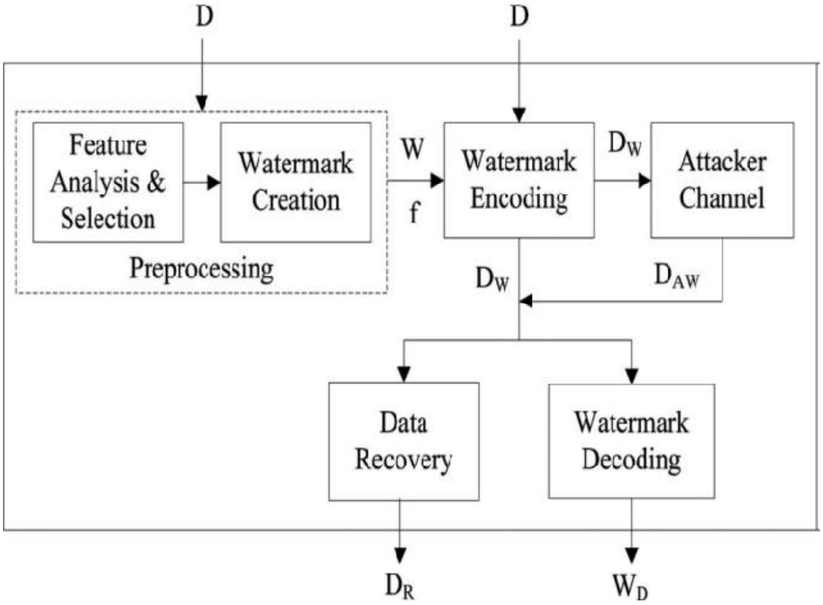

Fig:1 System Architecture

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)

A. Application of Digital Watermarking for Relational Databases

Digital Watermarks for relational databases are useful in many applications:

1) **Ownership Assurance:** For ownership protection watermarking can be used. To assure ownership of a relational database, Owner of the database can embed a watermark into his data by using some private parameters which is known only to him. Then watermarked database can be made publicly available. Later, suppose Owner suspects that

the data published by someone else has pirated from his data. To avoid ownership confusion, Owner can proved the presence of his watermark in attacker's data. Hence watermark detection have to be used to survive against various malicious intentions [4].

2) **Fingerprinting:** Fingerprinting is used to identify a betrayer. The applications where content is publicly available over a network, the owner of data would like to discourage unauthorized distribution and duplication of data by embedding a distinct watermark in each copy of the content. If unauthorized copies of the data are found, then the original data can be determined by extracting the fingerprint [4].

3) **Fraud and Tamper Detection:** Critical applications such as commercial transactions or medical applications use data, it will originate from a specific source and it will not been modified, manipulated or destroyed. This can be achieved by embedding a watermark in the underlying data of the database. The watermark is extracted by using private parameter associated with the source. Fraud in the data is verified by checking the integrity of original data to that of extracted watermark [7]

B. Different Attacks

In fragile watermarking, integrity verification is done while in robust watermarking, the embedded watermark should be robust against various types of attacks. This attack includes removing or distorting the watermark. The watermarked database may suffer from various types of attacks which are created intentionally and unintentionally and it may damage or erase the watermark. [13]

1) Benign Update: In this type of attack, the marked tuples may be inserted, removed or updated. It may make embedded watermark detectable or undetectable. This may do unintentionally.

2) Value Modification Attack: In this type of attack, watermarks are destroyed by altering one or more bits in the watermarked data. Success of this attack depends on the estimation of how many bit positions are involved in the watermarking. Underestimation of it may cause the attack unsuccessful, whereas overestimation may cause the data useless.

3) Subset Attack: Attacker may consider a subset of the tuples or attributes of a watermarked relation. Attacker may delete or update tuples or attribute and hope for watermark has been lost.

4) Collusion Attack: This attack requires the attacker to have access to multiple watermarked copies same content.

5) Majority Attack: This attack creates a new relation with the same schema as the copies but with each bit value computed as the majority function of the corresponding bit values in all copies so that the owner cannot detect the watermark.

6) False Claim of Ownership: This type of attack, attacker may claim for ownership by adding his own watermark in owner's data.

7) Subset Reverse Order Attack: In this type of attack, attacker exchanges the order or positions of the tuples or attributes in data which may remove or disturb the watermark.

C. Classification of Watermarking Techniques

In this paper, we try to cover the details of various watermarking techniques. To limit the survey area we classify techniques based on: [13]

1) Watermark Information: Different watermarking embeds different types of watermark information into the database. (e.g. image, text, sound etc.)

2) Distortion: Watermarking may be distortion-based or distortion- free depending on whether the marking introduces any distortion to the data. Distortion-based watermarking techniques includes slight changes in the original data during embedding phase but the degree of change should be tolerable and should not make the data useless. In distortion-free watermarking scheme, the watermark insertion phase does not depend on any specific type of attribute and does not introduce any distortion in the original data

3) Cover Type: Watermarking can be classified based on the type of the cover i.e. type of attributes into which watermark bits is embedded.

4) Granularity Level: The watermarking can be performed by modifying or inserting information at bit level or higher level (e.g. character level or attribute level or tuple level).

5) Verifiability: The verification process may be deterministic or probabilistic in nature, it can be performed blindly or non-blindly, it can be performed publicly (by anyone) or privately (by the owner only).

6) Intent: Different watermarking schemes are designed for various purposes, namely, integrity and tamper detection, localization, ownership, traitor detection etc.

III. PROBLEM DEFINITION & OBJECTIVES

Motivation

- Watermarking techniques mainly used to protect publicly available data from being tampered, protect ownership [13] of that data, ensure integrity [14] and such other purposes.
- Watermarking may has the threat of malicious attack which may cause alteration, deletion, or false insertion.

Problem Definition

The irreversible watermarking technique may causes alternation or modification of underlying data at the certain extent[2].To overcome such problem reversible watermarking employed which results in lossless and exact authentication of relational databases.

This reversible watermarking technique acquire the capability of exact restoration of the original attribute data from the watermarked relational databases[3].

Objective

- Watermark accounting so as to encode and interpreting for the part of the considerable number of components in information disclosure b) Normal information restoration in the presence of energetic malicious attacks.
- The robust watermarking scheme possesses the exact recovery also in the existence of active malicious attack
- The additional feature is involved that allows selective watermarking of required particular attribute which involves selection of suitable feature for the embedding through the watermark
- Digital watermarking of multimedia content is more commonly known. Particularly image watermarking—a derivative of Steganography is an age-old practice allowing covert transmission of messages from one party to another by exploiting redundancy in common image formats.
- Our focus is to develop an information model through a statistical measure that identifies such features that do not have a significant effect on the decision making process.
- The goal is to make the data item must be secured from vulnerabilities and threats and to provide data quality and data recovery from malicious attacks.

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. 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

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.