IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

A Review on Multi-attribute Watermarking Technique for Relational Data

Ms. Vrushali B. Patil[1], Prof. P. M. Yawalkar[2]

PG Student, Computer Engineering, MET BKC Adgaon, Nashik, Savitribai Phule Pune University, Maharashtra, India[1]

Professor, Computer Engineering, MET BKC Adgaon, Nashik, Savitribai Phule Pune University, Maharashtra, India[2]

Abstract: The Relational Databases contain the valuable information of various organizations and institutes. In the world of Information Technology and Internet Based services the Copyright protection or Ownership rights protection of Relational Database is critical issue. When data is used in collaborative environments for information extraction; consequently, they are vulnerable to security threats concerning ownership rights and data tampering. Due to unauthorized access to the data may change the originality it result in significant losses of the organization. Watermarking is used to protect the ownership rights of shared Relational Data and also providing the solution for tackling and tampering of data. Watermarking is most often used for images, audio, video etc. However, by considering the use of Relational Database in shared environment and its security, When Ownership rights are preserved using watermarking, the underlying data also gets modified; as a result of which, the data originality gets compromised.

Keywords: Watermarking, Ownership right protection, Data Recovery.

I. INTRODUCTION

Nowadays due to the increasing use of the internet and cloud computing data is excessively generated. This data is then stored in different digital formats such as audio, video, images, natural language texts and relational data. In particular, the Relational data is shared extensively by the owners with research communities and in the cloud virtual data storage locations. The piracy of digital assets such as software, images, video, audio and text has long been a concern for owners of these assets. Protection of these assets is usually based upon the insertion of digital watermarks into the data. The watermarking software introduces small errors into the object being watermarked. The increasing use of databases in applications is creating a need for watermarking databases. In the life sciences industry, the primary assets of companies such as Celera are the databases of biological information. The Internet is exerting tremendous pressure on these data providers to create services (often referred as web services) that allow users to search and access databases remotely. While this trend is a boon to end users, it is exposing the data providers to the threat of data theft. They are therefore demanding capabilities for identifying pirated copies of their data.[12]

Ownership protection and data recovery is ensured by Reversible watermarking techniques. A guilty agent is identified as the source of data leakage by the digital watermarking. Watermarking has the property that it can provide ownership protection over the digital content by marking the data with a watermark unique to the owner. The embedded watermark can subsequently be used for proving and claiming ownership. Watermarking is commonly known about a multimedia content. In image watermarking, the messages were transmitted from sender to receiver by exploiting redundancy in common image formats. The watermarking of relational data and the multimedia content differs because of difference in the properties of the data. Multimedia data is highly correlated and continuous whereas relational data is independent and discrete. The advantages of the modern copyright protection and information hiding techniques, ownership rights of the relational data are protected. However a major drawback of these techniques is that the loss of data quality occurs as they modify the data to a very large extent. There is a strong need to preserve the data quality in watermarked data so that it is of sufficiently high quality and fit for use in decision making as well as in planning processes in different application domains. Data quality is nothing but the appropriateness of data for its intended applications [6].

The problem of data quality degradation is overcome by Reversible watermarking technique. In reversible watermarking technique, original data is recovered along with the embedded watermark information and the data is kept useful for knowledge discovery. In this process the modifications in the data are made such that the quality of the data before embedding watermark information and after extracting is acceptable for knowledge extraction process. To overcome the problems of Reversible watermarking techniques in the presence of malicious attacks no work has been conducted. Reversibility is the ability to recover the watermark and the original data. Robustness and reversibility are two features that are potentially conflicting because a reversible watermark string also makes it an easier target for attack. Therefore, the most appropriate watermark bandwidth that ensures maximum watermark robustness without significant loss of information that may result by watermarking is chosen. The motivated problem is a constrained optimization problem, this (CO) allows one to optimize a single or multiple objectives with respect to certain variables that are bounded by some constraints. Ownership rights of

DOI 10.17148/IJARCCE.2015.412112

these databases need to protect from malicious recipients; in the presence of data quality constraint.

II. 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.

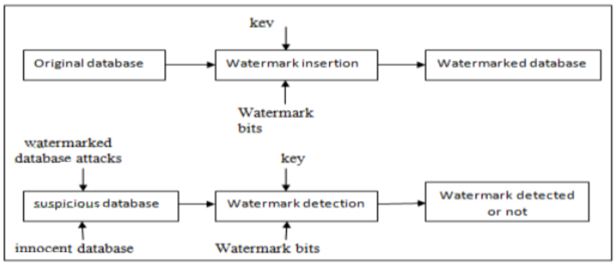

Figure 2: Watermarking scheme [12]

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

DOI 10.17148/IJARCCE.2015.412112

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.RELATED WORK

Watermarking is used to protect the ownership rights of shared Relational Data and also providing the solution for tackling and tampering of data. The relational database watermarking is of various types as, Reversible watermarking, Irreversible watermarking technique based on various constraints like, Particle swarm optimization, Difference expansion, Difference expansion of triplets, difference expansion based on SVR prediction, . This technique selects the watermark from the features of the dataset which is too strong to attack. As the watermarking make some changes in the original data bits hence this technique overcomes this problem by reversible watermarking [12].

JACK T. BRASSIL proposed a marking technique for Electronic distribution of text documents. This technique is used for the Copyright Protection of Electronic data. Three techniques have been described for encoding information into text images:

- Line-shift encoding;
- Word-shift encoding;
- Character modification

In line shift encoding, a mark is embedded on a page by vertically displacing an entire text line. Here a line is moved up or down, while the line immediately above or below (or both) are left unmoved. The unmoved adjacent lines serve as reference locations in the decoding process. He suggests that vertical line displacements of 1/300 in and less are not noticed by readers. In Word shift encoding, a mark is embedded by horizontally shifting the location of a word within a text line. Here a word is displaced left or right, while the words immediately adjacent are left unmoved. These unmoved words can then serve as reference locations in the decoding process. For word shift encoding it is suggested that horizontal word displacements of 1/150 in and less are not noticed by reader. The Character modification is a class of techniques which embed a mark by altering a particular feature of an individual character. Correlation decoding is necessary for word-shift encoding when distortion is present, while centroid decoding is adequate for line-shift encoding [1].

Fabien A. P. Petitcolas presents a study of watermarking scheme Evaluation in which a duality approach is used to the watermarking evaluation problem. The evaluation criterion is split into two (independent) groups: functionality and assurance. The first group represents a set of requirements that can be verified using agreed series of tests. The basic functionalities discussed are Perceptibility, Reliability, Capacity, speed, Statistical Undetectable. The second group is a set of levels to which each functionality is evaluated. These levels go from zero or low to very high [3].

Agrawal and Kiernan have proposed the first method of irreversible watermarking technique for relational databases. The following are the major contributions of this paper:
Identification of the rights management of relational data through watermarking as an important and technically challenging problem for database research.

- Articulation of the desirable properties of a watermarking system for relational data. Enunciation of the various forms of malicious attacks from which the watermark inserted in a relation must be protected.
- First proposal of a watermarking technique specifically geared for relational data.
- Extensive analysis and empirical evaluation of the robustness and effectiveness of the proposed technique to demonstrate the feasibility of watermarking real life datasets.

This technique ensures that some bit positions of some of the attributes of some of the tuples contain specific values. The tuples, attributes within a tuple, bit positions in an attribute, and specific bit values are all algorithmically determined under the control of a private key known only to the owner of the data. This bit pattern constitutes the watermark. Only if one has access to the private key can the watermark be detected with high probability. Detecting the watermark neither requires access to neither the original data nor the watermark. The watermark can be detected even in a small subset of a watermarked relation as long as the sample contains some of the marks. This technique is not useful for non-numeric attributes and also fails to identify the culprit in cases where there can be multiple sources of piracy [4].
Adnan M Alattar proposed a reversible watermarking algorithm based on the difference expansion of colored images. This is an image watermarking technique which is

DOI 10.17148/IJARCCE.2015.412112

used to recover the original image. To hide pairs of bits spatial and spectral triplets of pixels are used. A spatial triplet is any three pixel values selected from the same spectral component, while a spectral triplet is any three pixel values selected from different spectral components. The algorithm is recursively applied to the rows and columns of the spectral components of the image and across all spectral components to maximize the hiding capacity Simulation results show that the hiding capacity of the algorithm is very high and the resulting distortion is low. Test results of the algorithm indicate that the amount of data one can embed into an image depends highly on the nature of the image [5]. D. M. Thodi and Jeffrey J. Rodriguez proposed a reversible watermarking technique for images. The algorithm exploits the correlation inherent among the neighboring pixels in an image region using a predictor. The prediction-error at each location is calculated and, depending on the amount of information to be embedded, locations are selected for embedding. Data embedding is done by expanding the prediction-error values. A compressed location map of the embedded locations is also embedded along with the information hits. This algorithm exploits the redundancy in the image to achieve very high data embedding rates while keeping the resulting distortion low [6].

R. Sion, M. Atallah, and S. Prabhakar uses Statistical-property watermarking algorithm. In this algorithm, watermark bits are embedded in actual data distribution properties of subset of tuples. The whole database is divided into a maximum number of unique, non-overlapping subsets of tuples. A watermark bit is embedded in each selected subset of tuples by making slight difference in some of the data values. Then average value of subset and variance values are reach some value which is depending on whether the watermark bit is 0 or 1.The data partitioning concept is vulnerable to watermark synchronization errors, particularly in the case of tuple insertion and deletion attacks, because the position of marker tuple is disturbed by these attacks. Such errors may be reduced if marker tuples are stored during watermark embedding phase and that same stored marker tuple will used for the data partitions again during watermark decoding phase. But this violates the concept of "blind decoding" of watermark. Furthermore, the threshold selection for bit decoding includes arbitrarily chosen thresholds without following any optimality criteria. This will results in error in the decoding process. The concept of usability bounds on data is used in this technique to control distortions introduced in the data during watermark embedding. However, an attacker can corrupt the watermark by launching large scale attacks on large number of rows. The decoding accuracy is depend on the usability constraints defined by owner of the data. Hence decoding accuracy is degrade if an attacker violates these bounds. An important shortcoming of this approach is that the data owner needs to specify usability constraints separately for application that will use data every time [7].

- The proposal and definition of the problem of watermarking categorical data
- The discovery and analysis of new watermark embedding channels for relational data with categorical types
- The design of novel associated encoding algorithms

The first reversible watermarking scheme for relational databases was proposed by Yong Zhang in The reversible watermarking scheme for relational databases proposed in this paper provides an exact and lossless method to authenticate the relational databases, especially suitable for sensitive data requiring no permanent distortions. The scheme takes advantage of the uneven distribution of errors between neighboring randomly generated values in the same attribute to realize reversibly watermarking, and show ability to limit the watermarking distortion to requirement of practical applications by taking partial real values to calculate errors using initial digit specification. Beside database, this scheme shows great advantage in reversible watermarking for other low correlated data like encrypted data, images heavily polluted by noises, and noise data itself. In this technique, histogram expansion is used for reversible watermarking of relational database. Zhang et al. proposed a method of distribution of error between two evenly distributed variables and selected some initial nonzero digits of errors to form histograms. Histogram expansion technique is used to reversibly watermark the selected nonzero initial digits of errors. This technique is keeps track of overhead information to authenticate data quality. However, this technique is not robust against heavy attacks (attacks that may target large number of tuples) [8].

Gupta and Pieprzyks' proposed reversible watermarking technique introduces distortions as a result of the embedding process. In this paper, they have proposed a reversible and blind database watermarking model. The maximum distortion introduced to the attributes is limited to the tolerance parameter X. It is, in practice, desirable to have distortion on the higher side since the watermarking is reversible. The distorted database is available to everyone and the accurate database can be purchased upon payment by users by reversing the watermarking. The proposed scheme is successful in achieving the major objective of eliminating the shortcomings of irreversible schemes. The capacity of the proposed watermarking scheme is high and the attack resistance probability between 89 and 98 percent. But here the watermark carrying capacity and level of attack resistance is comparatively less [9].

E. Sonnleitner, proposed a robust, blind, resilient and reversible, image based watermarking scheme for large scale databases. In this paper, they have shown that whites- pace substitution for the purpose of information hiding within database relations offers significant potential for watermarking scenarios. Although all experimentally simulated attacks lead to a notable decrease in the watermark detection rate, the perceptual verification level hardly drops below the 90 $% $ mark, even after attacks which heavily distort the original relation [10].

K. Jawad and A. Khan have used GA to improve the capacity of DEW in databases, while keeping distortion

DOI 10.17148/IJARCCE.2015.412112

tolerance fixed. GA introduces some randomness in DEW technique, thus making it difficult for the attacker to predict attributes. Security of the watermarking system is also enhanced by reducing the distortion and minimizing abrupt changes caused by DEW. This is achieved by two measures added in the fitness function of GA, first by using the knowledge of the neighborhood values of the relational database, second by minimizing the distortion introduced by selecting attributes resulting in minimum distortion. Results are also showing improvement in capacity of watermark. Consequently, more watermark bits can be embedded in database, while distortion introduced in it is minimalized. This provides more comfort for the user and leaves fewer options for the attacker to destroy the watermark. Detection technique of GADEW resolves problem of reshuffling attacks on attributes. It is also robust against addition, deletion, sorting, bit flipping, tuple and attribute-wise-multifaceted, and additive attacks. It has also solved problem of false positive rate at detection side. In future, we intend to develop a reversible watermarking technique, which can handles both integer and floating point values present in a single relation [11].

M. Kamran, Sabah Suhail, and Muddassar Farooq uses Random bit pattern watermarking algorithm. They proposed a method for numeric data. It is a robust against various attacks and efficient watermarking scheme for relational databases. In this method, a robust watermark algorithm is used to embed watermark bits into the original data set. The watermark embedding algorithm takes a secret key and the watermark bits as input and converts an original data set into watermarked data set. Watermark bits are generated from UTC (Coordinated Universal Time) date time which is the primary time standard used to synchronize the time all over the world. These bits are given as an input to the watermark encoding function. Then dataset is partitioned into non-overlapping partitions by using the secret key in conjunction with a cryptographic secure hash function. To minimize distortions, only few tuples are selected for watermarking. Then watermark bits are embedded in the selected tuples using a robust watermarking function.

This technique embeds each bit of the watermark in every selected tuple of each partition; as a result, it is robust against malicious attacks even only one watermarked row is left in the data after an attack. The watermarked data set is delivered to recipient where an attacker aims at destroying the watermark by launching different types of attacks. The decoding algorithm is blind and its decoding accuracy does not depend on the usability constraints. As a result, 100 percent decoding accuracy is achieved irrespective of the amount of data alterations made by an attacker in the watermarked data. But the decoding accuracy may decrease in case of combination of different attacks. And if an attacker alters the original data to some signed or zero-valued data then the decoding accuracy might be decreased. This technique is best suited for data sets that contain unsigned numeric attributes. This scheme depends critically on presence of primary key attribute. If there is no primary key or if attackers alter/destroy key then scheme will not work [12].

Watermarking relational databases is a relatively new research area that deals with the legal issue of copyright protection of relational databases. Therefore, literature in this area has been very limited, and focused on embedding short strings of binary bits in numerical databases. Watermarking is most often used for images, audio, video etc. However, by considering the use of Relational Database in shared environment and its security, When Ownership rights are preserved using watermarking, the underlying data also gets modified; as a result of which, the data originality gets compromised. 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 [13].

Reversible watermarking is used to protect data originality along-with data recovery. However, such techniques are not vigorous against various types of attacks and do not have a provision for selectively watermark a particular attribute based on their importance in knowledge recovery. Therefore, the Reversible watermarking must provide; a) Watermark Encoding and Decoding by considering the role of attribute feature in knowledge recovery with provision to watermark multiple attribute, b) Recovery of original data in case of active malicious attacks.

In this paper, a novel robust and reversible technique for watermarking numerical data of relational databases is presented. The main contribution of this work is that it allows recovery of a large portion of the data even after being subjected to malicious attacks. RRW is also evaluated through attack analysis where the watermark is detected with maximum decoding accuracy in different scenarios. A number of experiments have been conducted with different number of tuples attacked. RRW is not applied for shared data used in distributed environment and for non-numeric data stores.

IV. OVERVIEW OF SYSTEM

Nowadays the huge amount of data is generated. This data is of several forms as image, video, text and relational data. Such a relational data is given to the various organizations for analysis. In this process the data sent through the communication channel (let's say attacker channel) may prone to some attacks. This may contaminate the data or make changes in data. Hence to prevent these things we need to provide the security to this data. This is done using the watermarking of the selected features through the data.

The watermarking of relational data previously was done only on the single attribute, which was too easy to attack. So it is required to get such a watermarking technique which is robust against the attacks, and if attack occurs then this technique must be able to recover the lost bits. Hence here the requirements are fulfilled, that is the

DOI 10.17148/IJARCCE.2015.412112

watermark is generated using the GA which is more robust and the watermarking technique is reversible. So original data is recovered by removing the watermarked bits.

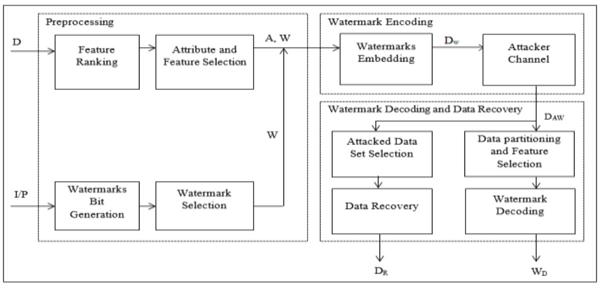

Figure 2: System Architecture [13]

An optimal watermark value is created through the GA and inserted into the selected feature of the relational database in such a way that the data quality remains intact. In this technique mutual information is used to select a suitable (candidate) feature from the database for watermarking. The knowledge of mutual information for every candidate feature is also used to compute the watermark information. Thus, it is ensured that the data quality will not be affected. Consequently, this technique provides a robust solution for data recovery that is reversible and resilient against heavy attacks. This technique mainly consist of following steps

- Data preprocessing phase
- Watermark encoding phase
- Attacker channel
- Watermark decoding phase and
- Data recovery phase

In data preprocessing phase, secret parameters are defined and strategies are used to analyses and rank features to watermark. An optimum watermark string is created in this phase by employing Genetic Algorithm. In the watermark encoding phase, the watermark information is embedded in the selected feature(s). Two parameters, β the optimized value from the GA and η_r change matrix are used in the watermark encoding and decoding phases. Finally, the watermarked data for intended recipients is generated. The attacker channel comprises subset alteration, subset deletion and subset insertion attacks generated by the adversary. These malicious attacks modify the original data and try to degrade its quality. In the watermark decoding phase the embedded watermark is decoded from the suspicious data. In order to achieve this preprocessing step is performed again, and decoding strategies (feature selection on the basis of MI, β the optimized value from the GA and η_r the change matrix) are used to recover the watermark. In data recovery phase, original data is recovered through post processing steps for error correction and recovery. The major contribution is on

- The design of an intelligent reversible watermarking technique for relational data that ensures data recovery without compromising data quality.
- A robust data recovery scheme that is resilient against subset alteration, subset deletion and subset insertion attacks.

Different techniques on watermarking relational databases that embeds the watermark bits in the relational database set by partitioning it are reviewed. In most of the Irreversible watermarking techniques data quality was compromised at the time of recovery. Such data quality problems are handled by Reversible watermarking techniques, which recover the original data from watermarked data and also maintains the data quality up to some extent. However, these techniques are not robust against malicious attacks. Most of these techniques use a single attribute of a tuple to embed a watermark. Embedding the same watermark at different attributes at different places. Hence provide additional security and it will make it difficult for attacker to remove watermarks from different places from the database. A novel robust and reversible technique for watermarking numerical data of relational databases allows recovery of a large portion of the data even after being subjected to malicious attacks. This technique is able to recover both the embedded watermark and the original data. One of the future concerns is to watermark shared databases in distributed environments where different members share their data in various proportions and to extend this technique for non-numeric data set.

ACKNOWLEDGMENT

The author is thankful to MET’s Institute of Engineering Bhujbal Knowledge City Nasik, HOD of computer department, guide and parents for their blessing, support and motivation behind this work.

REFERENCES

[1] G. Salton and C. Buckley, “Term-weighting approaches in automatic text retrieval,” In Information Processing & Management.Journal, vol. 24, no. 5, pp. 513–523, 1988.

[2] J. T. Brassil, S. Low, and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text documents,” In Proc. IEEE, vol. 87, no. 7, pp. 1181–1196.Jul. 1999.

[3] F. A. Petitcolas, “Watermarking schemes evaluation,” IEEE Signal Process. Mag., vol. 17, no. 5, pp. 58–64, Sep. 2000.

[4] R. Agrawal and J. Kiernan, “Watermarking relational databases,” In Proc. 28th Int. Conf. Very Large Data Bases, pp. 155–166. 2002.

[5] A. M. Alattar, “Reversible watermark using difference expansion of triplets,” In Proc. IEEE Int. Conf. Image Process., pp.I–501, vol. 2003.

[6] D. M. Thodi and J. J. Rodriguez, “Prediction-error based reversible watermarking,” in Proc. IEEE Int. Conf. Image Process. vol. 3, pp. 1549–1552, 2004.

[7] R. Sion, M. Atallah, and S. Prabhakar, “Rights protection for categorical data,” In IEEE Trans. Knowl. Data Eng., vol. 17, no. 7, pp. 912– 926, Jul. 2005.

[8] Y. Zhang, B. Yang, and X.-M.Niu, “Reversible watermarking for relational database authentication,” J. Comput., vol. 17, no. 2, pp. 59–66, 2006.

[9] G. Gupta and J. Pieprzyk, “Reversible and blind database watermarking using difference expansion,” In Proc. 1st Int. Conf. Forensic Appl. Tech. Telecommun., Inf., Multimedia Workshop, p. 24, 2008.

[10] E. Sonnleitner, “A robust watermarking approach for large databases,” In Proc. IEEE First AESS Eur. Conf. Satellite Telecommun., pp. 1–6. 2012.

[11] K. Jawad and A. Khan, “Genetic algorithm and difference expansion based reversible watermarking for relational databases,” J. Syst. Softw., vol. 86, no. 11, pp. 2742–2753, 2013.

[12] M. Kamran, Sabah Suhail, and Muddassar Farooq, "A Robust, Distortion Minimizing Technique for Watermarking Relational Databases Using Once-for-All Usability Constraints" In IEEE Transactions on Knowledge and Data Engineering, VOL. 25, NO. 12, DECEMBER 2013.

[13] SamanIftikhar, M. Kamran, and Zahid Anwar, “RRW—A Robust and Reversible Watermarking Technique for Relational Data,” In IEEE Trans. on knowledge and Data Engineering, VOL. 27, NO. 4, APRIL 2015.

DOI 10.17148/IJARCCE.2015.412112